博士論文(要約)

論文題目　　情報を対象とする捜査手続の在り方

氏　　名　　劉　芳伶

目　次

参考文献・資料

・本稿では，**太字**で示した形に略して引用する。
・以下は，略語(＝**太字**)の５０音順(和文)・画数順(中文)・アルファベット順(欧文)に並べる。
・改訂のあったものは，原則として，最新版を挙げる。
・雑誌論文などで発表後に単行本にまとめられた場合，付記する。

和文文献・資料

あ行

あ

青柳幸一「基本権の侵害と比例原則」芦部信喜先生還暦記念論文集刊行会編『憲法訴訟と人權の理論：芦部信喜先生還暦記念論文集』599 頁以下（有斐閣，1985 年）

青柳文雄「『**文書**の押収，捜索』について」ジュリスト 228 号 28 頁以下(1961 年)

青柳文雄『日本**刑**事訴**訟**法論――**国民性**の視角から』(立花書房，1970 年)

青柳文雄**ほか**編『**註釈**刑事訴訟法**(1)**』（立花書房，1976 年）

青柳文雄『刑事訴訟法**通論(上)** 五訂』(立花書房，1976 年)

青柳武彦『サイバー監視社会 ： ユビキタス時代のプライバシー論』（電気通信振興会，2006 年）

秋山規雄「捜索差押許可状に**被疑事実**を記載することの適否」新関雅夫ほか著『増補令状基本問題(下)』259 頁以下(判例時報社，2006 年)

秋山規雄「**令状**に**記載**された物以外の物件を差押えたのではないかが問題となった事例」新関雅夫ほか著『増補令状基本問題(下)』243 頁以下(判例時報社，2006 年)

秋山規雄「捜索差押許可状における**目的物の特定**」新関雅夫ほか著『増補令状基本問題(下)』234 頁以下(判例時報社，2006 年)

秋山規雄「遠隔地における緊急逮捕と**迅速な令状**請求手続の一方法」新関雅夫ほか著『増補令状基本問題(上)』175 頁以下(判例時報社，2006 年)

浅田和茂「**科学的尋問**と取調べ」井戸田侃ほか編『総合研究被疑者取調べ』369 頁以下（日本評論社，1991 年)

浅田和茂『科学捜査と**刑事鑑定**』(有斐閣，1994 年)

浅田和茂「刑事司法の**科学化**」ジュリスト 1148 号(1999 年)

芦部信喜『**現代人権論**：違憲判断の基準』(有斐閣，1974 年)

芦部信喜『憲法Ⅱ人権(1)』(有斐閣，1978 年)

芦部信喜「**包括的基本権(2)**」法学教室 128 号 69 頁以下(1991 年)

芦部信喜『憲法学Ⅱ――**人権総論**』(有斐閣，1994 年)

芦部信喜『**憲法**(新版／補訂版)』(岩波書店，1999 年)

足立進「押収・捜索及び検証」團藤重光編『法律実務講座刑事編（第 2 巻）』308 頁以下（有斐閣，1953 年）

渥美東洋「**鑑定**をめぐる諸問題」鴨良弼ほか編『刑法と科学――法律編：植松博士還暦祝賀』745 頁以下（有斐閣，1971 年）

渥美東洋『**捜査**の原理』(有斐閣，1979 年)

渥美東洋「**自動車検問**の法律構成について」判例タイムズ 423 号 13 頁以下（1980 年）

渥美東洋『**レッスン刑事訴訟法(上)**』(中央大学出版部，1985 年)

渥美東洋「**情報犯罪**の規律と捜査」『ネットワーク社会と法(ジュリスト増刊)』77 頁以下(有斐閣，1988 年)

渥美東洋「**テレビカメラ**による不穏な状況と犯罪状況の警察による擁影・録画を適法とした事例――東京高裁昭和六三年四月一日判決，本誌六八一号二二八頁――」判例タイムズ 684 号 36 頁以下(1989 年)

渥美東洋『**刑事訴訟法(新版)**』(有斐閣，1990 年)

渥美東洋「**電気通信網**による通信・会話の傍受について」判例タイムズ 43 巻 13 号 9 頁以下（1992 年）

渥美東洋『刑事訴訟における**自由と正義**』(有斐閣，1994 年)

渥美東洋『**(全訂)刑事訴訟法**』(有斐閣，2009 年)

マイケル・アドラー(著)**新保史生(訳)**「インターネット上の**デジタル禁制品の捜索**と修正 4 条」公法学研究(駒沢大学大学院)23 号 157 頁以下(1997 年)

荒木伸怡『刑事訴訟法読本――冤罪・誤判の防止のために』(弘文堂，1996 年)

有倉遼吉＝**小林**孝輔**編**『別冊**法**学**セ**ミナー(122 号)基本法**コンメ**ンタール**憲法**(第三版)』(日本評論社，1986 年)

有倉遼吉『**公共の福祉**』法学セミナー53 号頁 12 以下(1960 年)

安東美和子「捜索・差押え――検察の立場から」三井誠ほか編『新刑事手続法Ⅰ』325 頁以下（悠々社，2002 年）

アンドリュー・S.タネンバウム著 ； 水野忠則［ほか］訳『コンピュータネットワーク（第 4 版）』（日経 BP 社，2003 年）

アンドリュー・S.タネンバウム(ほか＝マールテン・ファン・スティーン)著 ； 水野忠則［ほか］訳『**分散システム**原理とパラダイム（第 2 版）』（ピアソン・エンデュケーション，2009 年）

い

飯島泰「フロッピーディスク等の内容を確認せずに，その差押えが許されるとした事例」警察公論 54 巻 6 号 89 頁以下（1999 年）

五十嵐清『**人格権**論』(一粒社，1989 年)

池上政幸「盗聴」三井誠ほか編『刑事手続(上)』159 頁以下(筑摩書房，1988 年)

池田修「フロッピーディスク等につき内容を確認せずに差押えることが許されるとされた事例」法曹時報 53 巻 2 号 520 頁以下（2001 年）→(法曹会『**最**高裁判所**判**例**解**説刑事篇**(平成 10 年度)**』(2001 年)**78 頁以下**)

池田修**＝前田**雅英『**刑**事**訴**訟法**講義**(**4 版**)』(東京大学出版会，2012 年)

池田公博「**電磁的記録**を含む証拠の収集・保全に向けた手続の整備」ジュリスト 1431 号 78 頁以下(2011 年)

池田公博「被疑者方居室を令状により捜索中に同人あてに配達された荷物について捜索することの可否：最高裁平成 19 年 2 月 8 日第一小法廷決定(平成 18 年(あ)第 1733 号覚せい剤取締法違反被告事件)(刑集 61 巻 1 号 1 頁,判時 1980 号 161 頁)」『(**平成 19 年度**)**重**要**判**例**解**説(ジュリスト 1354 号)』200 頁以下(有斐閣，2008 年)

池田公博「**共犯者の供述**による立証」井上正仁＝酒巻匡(編)『三井誠先生古稀祝賀論文集』629 頁以下(有斐閣，2012 年)

池田弥生「携帯電話の位置探索のための令状請求」判例タイムズ 1097 号 27 頁以下(2002 年)

石尾登「科学捜査力の強化」警察学論集 40 巻 1 号 30 頁以下(1987 年)

石川元也「立法的提言―手続について」日本弁護士連合会刑法改正対策委員会編『コンピュータ犯罪と現代刑法』207 頁以下(三省堂，1990 年)

石川才顕「**令状主義**と捜索差押の必要性判断」法律時報 41 巻 2 号 77 頁以下(1969 年)

石川才顕「**押収**すべき物の範囲･意義」熊谷弘ほか編『捜査法大系(Ⅲ)捜索・押収』114 頁以下(日本評論社，1986 年)

石川才顕『**通説刑**事**訴**訟法』(三省堂，1992 年)

石川才顕「捜索・差押の**必要性判断**の帰属――いわゆる国学院大学映研フイルム差押事件に対する特別抗告審の判断を契機として」日本法学 35 巻 1 号 92 頁以下(1994 年)

石川才顕「**建築物**を証拠物としてなす差押処分とその必要性判断の基準」ジュリスト 669 号 92 頁以下(1978 年)

石川弘**＝増井**清彦「証拠収集と立証の新展開（1）――防犯カメラ，盗聴，音声識別，臭気選別等」『現代刑罰法大系(第五巻)刑事手続Ⅰ』203 頁以下（日本評論社，1983 年)

石川健治『自由と特権の距離――カール・シュミット「制度体保障」論・再考(増補版)』(日本評論社，2007 年)

石毛平蔵「令状問答(第三問)差押許可状に**場所の記載**は必要か」捜査研究 20 巻 4 号 31 頁以下(1971 年)

石毛平蔵『捜査官のための**令状問答**』(東京法令出版，1980 年)

石毛平蔵『**捜査・令状**の基本と実務――令状裁判官と警察実務家とのＱ＆Ａ』(東京法令出版，1992 年)

石村耕治「監視カメラ社会化をどう考えるべきか――市民が“監視”できる法制づくりが急がれる」法学セミナー580 号 54 頁以下(2003 年)

石村善治**＝奥平**康弘**(編)『知る権利** マスコミと法』(有斐閣，1974 年)

石村善治**＝堀部**政男**(編)**『**情報法**入門』(法律文化社，1999 年)

石山豊太郎『犯罪捜査と司法的抑止(司法研究報告書第五輯第二号)』(司法研修所，1952 年)

板倉宏『現代型犯罪と刑法の論点』(学陽書房，1990 年)

井田良(**ほか**＝田口守一＝植村立郎＝河村博)**編著**『**事例**研究刑事法**Ⅱ刑**事**訴**訟法』(日本評論社，2010 年)

伊丹俊彦『Ｑ＆Ａ――**実例**――捜索・差押えの実際』(立花書房，2005 年)

出射義夫「捜査の方法」団藤重光『法律實務講座(刑事編 第 3 巻)』583 頁以下(有斐閣，1954 年)

井戸田侃『刑事手続の構造序説』(有斐閣，1971 年)

井戸田侃『**刑**事**訴**訟法**要説**』(有斐閣，1993 年)

伊藤栄樹『刑事訴訟法の**実際問題** ： 捜査と証拠をめぐる **95 問** 』（立花書房，1967 年)

伊藤栄樹**ほか**著『**注釈**刑事訴訟法**(新版)**第二巻』(立花書房，1997 年）→初版：青柳文雄［ほか］著『註釈刑事訴訟法』全 4 巻（立花書房，1976-1981 年；増補版 1978 年)

伊藤栄樹**ほか**著『**注釈**刑事訴訟法**(新版)**第三巻』(立花書房，1997 年)

株式会社 NTT データ経営研究所『電子文書証明－**e ドキュメント**の原本性確保』(NTT 出版株式会社，2001 年）

伊藤正己「**プライバシーの権利**」(岩波書店，1963 年)

伊藤公一「環境権との関連における**憲法一三条**の一考察」広岡隆ほか編『憲法と環境問題：一圓一億博士還暦記念論文集』21 頁以下(中央書房，1976 年)

稲垣隆一「情報と捜査―捜索差押え実務上の問題点」多賀谷一照＝松本恒雄編『情報ネットワークの法律実務』5001 頁以下(第一法規，1999 年)

井上伸雄ほか共著『新通信情報早わかり講座３』（日経コミュニケーション，1999 年)

井上伸雄『基礎知識からクラウド，モバイル，次世代通信まで〔図解〕**通信技術のすべて**』（日本実業出版社，2011 年)

井上弘通「フロッピーティスクに入力された情報の収集と令状の発付」『(増補)令状基本問題(下)』331 頁以下(判例時報社，2006 年)

井上正治『**全訂**刑事訴訟法原論』(朝倉書店，1952 年)

井上正仁『刑事訴訟における**証拠排除**』(弘文堂，1985 年)

井上正仁「**科学捜査**の限界―盗聴を中心にして―」法学教室 114 号 16 頁以下（1990 年)

井上正仁「捜索差押の際の**写真撮影**と準抗告の適否(最決平成 2.6.27）」警察研究 64 巻 2 号 34 頁以下(1993 年）**＝井上・強制・任意 348 頁以下**

井上正仁「**電話逆探知**の適法性」松尾浩也＝芝原邦爾編『刑事法学の現代的状況：内藤謙先生古稀祝賀』485 頁以下(有斐閣，1994 年）**＝井上・強制・任意 191 頁以下(**※元の題名が「電話の逆探知」に変更された。)

井上正仁『捜査手段としての通信・会話の**傍受**』(有斐閣，1997 年)

井上正仁「**捜索・押収**と令状主義(特集 捜索・押収と令状主義)」刑法雑誌 36 巻 3 号 409 頁以下(1997 年)

井上正仁「**令状主義**の形成過程」司法研修所論集（創立五十周年記念特集号）第 3 巻（刑事編）200 頁以下（1997 年)

井上正仁**＝佐藤**英彦「〈**対談**〉刑事訴訟法施行 50 年と刑事警察の課題」警察学論集 52 巻 1 号 1 頁以下(1999 年)

井上正仁「**コンピュータ・**ネットワークと犯罪捜査 **(1) ～ (2・**完**)** 」法学教室 24４号／245 号 (2001 年)

＝井上・強制・任意 240 頁／272 頁以下

井上正仁＝**池田**公博長「コンピュータ犯罪と捜査」松尾浩也＝井上正仁編『刑事訴訟法の争点(第 3 版)ジュリスト増刊』88 頁以下(有斐閣，2002 年)

井上正仁「任意捜査と強制捜査の区別」松尾浩也＝井上正仁編『刑事訴訟法の**争点**(第 3 版)ジュリスト増刊』 46 頁以下(有斐閣，2002 年) **＝井上・強制・任意 2 頁以下**

井上正仁『**強制**捜査と**任意**捜査』(有斐閣，2006 年)

今村成和「基本的人権と公共の福祉」小嶋和司編『憲法の争点(新版)』66 頁以下(有斐閣，1985 年)

指宿信「**インターネット**を使った**犯罪**と刑事手続」法律時報 69 巻 7 号 1 頁以下(1997 年)

指宿信「**インターネット盗聴**と暗号問題」法学セミナー518 号 125 頁以下(1998 年)

指宿信「**ベッコアメ**顧客データ差押事件」別冊ＮＢＬ79 号 66 頁以下(2003 年)

指宿信「変わる捜査の対象：**モノからデータへ**――サイバー刑事法制の諮問を契機として」法律時報 75 巻 7 号 1 頁以下(2003 年)

指宿信「**サイバースペース**における証拠収集とデジタル証拠の保全――2011 年改正法案を考える」法律時報 83 巻 7 号 84 頁以下(2011 年)

岩崎和彦「差押許可状における『差押えるべき物』の特定」警察公論 36 巻 2 号 36 頁以下(1981 年)

岩田二郎「**コンピュータ関連犯罪**の手続問題**(捜査手続**上の問題**)**」日本弁護士連合会刑法改正対策委員会編『コンピュータ犯罪と現代刑法』190 頁以下(三省堂，1990 年)

う

植松健一「連邦刑事庁(BKA)・ラスター捜査・オンライン捜査(2)」島大法学 53 巻 2 号 1 頁以下(2009 年)

植松健一「2009 年度 島根大学法政研究会実施報告 第 5 回 植松健一(憲法) 『国家』が"Hacker"になるとき!?--ドイツ連邦憲法裁判所"**オンライン捜索**"違憲判決とその周辺 」島大法学 54 巻 1・2 号，203 頁以下(2010 年)

植村立郎「盗聴・秘密録音について」河上和雄ほか編『(講座)日本の警察(第二巻)刑事警察』219 頁以下(立花書房，1993 年)

上村卓也「社会と刑事法--捜査差押えをめぐる最高裁判例 2 題--フロッピーディスクの包括的差押えの可否など」警察時報 53 巻 11 号 93 頁以下(1998 年)

右崎正博「憲法一三条と自己情報コントロール権」愛敬浩二＝水島朝穂＝諸根貞夫編『現代立憲主義の実践と認識：浦田賢治先生古稀記念論文集』274 頁以下(日本評論社，2005 年)

宇藤崇「違法収集証拠排除による基本的人権の保障についての一考察―『**規範的瑕疵**効果論』の展開を手掛かりとして―」光藤景皎先生古稀祝賀論文集編集委員会編集『光藤景皎先生古希祝賀論文集（上巻）』505 頁以下（成文堂，2001 年）

宇藤崇「被疑者の容ほう等の**ビデオ撮影**が適法とされた事例」『(平成 20 年度)重要判例解説（ジュリスト，

臨時増刊 1376 号）』208 頁以下(有斐閣，2009 年)

え

株式会社**エディックス(訳)**Robert　Jones(著)『インターネットフォレンジック――ネット犯罪を解決する電子証拠の収集と分析』(オライリー・ジャパン，2006 年)

遠藤誠「捜索･差押状における目的物の特定及び罪名の記載」司法研修所報 28 号 153 頁以下(1962 年)

榎原猛**(編)**『**プライバシー**権の総合的研究』(法律文化社，1998 年)

お

大家重夫(編著)『最新肖像権関係判例集』(ぎょうせい，1989 年)

大谷直人「司法警察員が捜索差押の際にした写真撮影によって得られたネガ及び写真の廃棄又は引渡を求める準抗告が不適法とされた事例」法曹時報 43 巻 7 号 1628 頁以下(1991 年)

大野正博「携帯電話による位置認識システムの活用とプライヴァシー」朝日法学論集第 39 号 77 頁以下(2012 年)

岡田薫「科学捜査の歴史と現実――科学捜査の先進国から後進国へ」警察学論集 60 巻 11 号 4 頁以下(2007 年)

岡部宏泰「捜索・差押の執行をめぐる諸問題(下)」警察学論集第 29 巻 10 号(1976 年)

岡村久道＝**新保**史生『電子**ネットワーク**と個人情報保護』(経済産業調査会，2002 年)

小木曽綾「新たな刑事手続と警察捜査」「警察行政の新たなる展開」編集委員会編『警察行政の新たなる展開(下巻)』187 頁以下(東京法令出版株式会社，2001 年)

奥平康弘「**表現の自由**」田中二郎ほか編・小林直樹ほか執筆『日本国憲法体系：宮沢俊義先生還暦記念――基本的人権Ⅰ――第七巻』53 頁以下(有斐閣，　1965 年)

奥平康弘『**知る権利**』(岩波書店，1979 年)

落合義和**＝辻**裕教『**刑**事**訴訟法**等の**一部**を**改正**する法律及び刑事訴訟規則等の一部を改正する規則の**解説**』(法曹会，2010 年)

小野清一郎『刑事訴訟法**講義(全訂**第 **3 版)**』(有斐閣，1924 年)

小野清一郎『新刑事訴訟法**概論**』(法文社，1948 年)

小野清一郎ほか著『(**ポケット**注釈全書)刑事訴訟法**(上)**新版』(有斐閣，1986 年)

小田中聡樹「成田空港開港阻止闘争拠点『**横堀第二要塞**』に対する差押処分を必要性の枠をこえるものとして取り消した事例――成田空港横堀第二要塞差押取消決定」判例時報 909 号(判例評論 240 号)150 頁以下(1979 年)

小田中聡樹「**コンピュータ関連犯罪**の手続問題(公判手続上の問題)」日本弁護士連合会刑法改正対策委員会編『コンピュータ犯罪と現代刑法』201 頁以下(三省堂，1990 年)

小田中聡樹「**盗聴**立法**の違憲性**――事務局参考試案の検討」**小田中**聡樹(**ほか**＝村井敏邦＝川崎英明＝白取祐司(著)『**盗聴立法批判**――おびやかされる市民の自由』(**＝小田中ほか・盗聴立法批判**)58 頁以下(日本

評論社，1997 年）
大澤裕「捜索場所・押収目的物の**特定**(特集 捜索・押収と令状主義)」刑法雑誌 36 巻 3 号 431 頁以下(1997 年)
大澤裕「コンピュータと捜索・差押え・検証--インターネット・プロバイダからの**顧客データ差押え**事件を素材として（特集 新世紀の法とコンピューター--21 世紀の法律学を展望する)」月刊法学教室 244 号 44 頁以下(2001 年)
大橋充直『図解・実例からのアプローチ：ハイテク犯罪捜査入門――**基礎編**』(東京法令，2004 年)
大橋充直『図解・実例からのアプローチ：ハイテク犯罪捜査入門――捜査実務編』(東京法令，2005 年)
大橋洋一「**法律の留保**学説の現代的課題―本質性理論（Wesentlichkeitstheorie）を中心として―」國家學會雜誌 98 巻 3・4 号 241 頁以下(1985 年)
小川新二「磁気のディスクと捜索差押え」平野龍一ほか編『新実例刑事訴訟法Ⅰ』251 頁以下(青林書院，1999 年)
小川憲久「**知的財産権**の保護と自力救済」法とコンピュータ 23 号 39 頁以下(2005 年)
小倉秀夫「Ｐ２Ｐに関する法律問題」法とコンピュータ 23 号 19 頁以下(2005 年)
小倉利丸「監視社会とプライバイー－グローバル化のなかでの新たな危機(特集＝プライバシーの再検討)」法律時報 78 巻 4 号 33 頁以下(2006 年)
小倉利丸**(編)**「**監視社会**とプライバイー」（ンパクト出版会，2001 年）
尾崎久仁子「批判」法律のひろば 50 巻 7 号 71 頁以下(1997 年)
小津博司「令状による差押え(2)――フロッピーディスクの差押え」松尾浩也＝井上正仁編『刑事訴訟法判例百選(第 7 版)別冊ジュリスト 148 号』54 頁以下(有斐閣，1998 年)
鬼頭季郎「捜索証明書・押収目録の交付」熊谷弘ほか編『捜査法大系(Ⅲ)捜索・押収』100 頁以下(日本評論社，1986 年)
王志安「越境コンピュータ捜索の法的地位――サイバー犯罪条約が残した課題」駒澤法学 3 巻 3 号 132 頁以下(2004 年)

か行

か

甲斐行夫「新判例解説 フロッピーディスク等につき内容を確認せずに差し押さえることが許されるとした事例(最高裁判決平成 10.5.1)」研修 605 号 13 頁以下（1998 年）
戒能通孝**＝伊藤**正己『**プライヴァシー**の権利』(松岳社，1962 年)
戒能通孝「**肖像権**と警察権」法学セミナー169 号 2 頁以下(1970 年)
香川喜八朗「**プレインヴィユー**法理の展開」高岡法学 4 巻 1 号 51～52 頁(1992 年)
香川喜八朗「写真撮影の適法性とコミュニティ・セキュリティ・カメラ」『日本刑事法の理論と展望――佐藤司先生古稀祝賀(下巻)』65 頁以下(信山社，2002 年)。
香川喜八朗「**所持品検査**の限界」法学新報 112 巻第 1・2 号(渥美東洋先生退職記念論文集)111 頁以下(2005 年)。

書上由紀夫「差押えに関する一考察――いわゆる横堀要塞差押事件特別抗告決定について――(最高裁昭和53年7月26日第三小法廷決定)」法律ひろば31巻10号12頁以下(1978年)
柏木千秋『**刑**事**訴**訟法』(有斐閣，1970年)
各和吉四郎「コンピュータ犯罪と捜査」警察学論集28巻3号51頁以下(1975年)
梶川住友「暴力団の実態解明(11月30日発行臨時増刊特集暴力団犯罪)」捜査研究27巻12号193頁以下(1978年)
粕谷友介「憲法一三条前段の『個人尊厳』」法学教室89号13頁以下(1998年)
加藤晶「科学捜査の必要と限界――戦後における科学捜査生成の中から」佐々木史朗ほか編『刑事訴訟法の理論と実務(別冊判例タイムズ7号)』124頁以下（判例タイムズ社，1988年)
亀山継夫「**刑事**関係**立法**過程はこのままでよいか」ジュリスト852号165頁以下(1986年)
亀山継夫「**刑**事**訴**訟法における判例**と立法**の役割」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版)』24頁以下(有斐閣，1991年)
鴨良弼「捜索･差押**許可状の記載**要件」『憲法判例百選(旧版)』91頁以下(有斐閣，1963年)
鴨良弼『刑事訴訟における**技術**と**倫理**』(日本評論社，1964年)
鴨良弼「捜査と**肖像権**」 我妻栄(代表)編『刑事訴訟法判例百選**(初版)**』26頁以下(有斐閣，1965年)
鴨良弼「**特殊**犯罪と**捜査**」 鴨良弼ほか編『刑法と科学――法律編：植松博士還暦祝賀』613 頁以下(有斐閣，1971年)
鴨良弼『刑事**証拠法**』(日本評論社，1972年)
鴨良弼『**刑**事**訴**訟**法**の**新展開**』(日本評論社，1973年)
鴨良弼『**新版刑**事**訴**訟法**講義**』(青林書院新社，1981年)
鴨良弼『**刑**事**訴**訟法の**基本理念**』(九州大学出版会，1985年)
川出敏裕「令状による**捜索(1)範囲**」松尾浩也＝井上正仁編『刑事訴訟法判例百選(第7版)別冊ジュリスト』48頁以下(有斐閣，1998年)
川出敏裕「**フロッピーディスク**等の内容を確認せずに差し押さえることの可否」ジュリ1157号181頁以下（1999年)
川出敏裕「**組織犯罪**と刑事手続」ジュリ1148号238頁以下（1999年)
川出敏裕「**コンピュータ犯罪**と捜査手続」法曹時報53巻10号1頁以下（2001年)
川出敏裕「**行政警察活動**と捜査」法学教室259号73頁以下（2002年)
川出敏裕「**任意捜査**の限界」『刑事裁判論集(下巻)：小林充先生佐藤文哉先生古稀祝賀』23頁以下（判例タイムズ社，2006年)
川出敏裕「**物の占有**とプライバシー」研修 753号3頁以下(2011年)
川出敏裕「**新たな捜査手法**の意義と展望」刑事法ジャーナル29号3頁以下(2011年)
河上和雄「**捜索差押**をめぐる問題について」捜査研究20巻4号97頁以下(1971年)
河上和雄「捜索・差押令状による**捜索，差押上の諸問題（**その**一）**」警察学論集28巻6号146頁以下(1975年)
河上和雄「捜索・差押令状による**捜索，差押上の諸問題(**その**三)**」警察学論集28巻9号150頁以下(1975年)
河上和雄「捜索・差押令状による**捜索，差押上の諸問題(**その**四)**」警察学論集28巻10号143頁以下(1975年)

河上和雄「捜索・差押**令状請求**上の諸問題**(**その**二)**」警察学論集 28 巻 5 号 157 頁以下(1975 年)
河上和雄『**証拠法ノート (1)** 捜索・差押』（立花書房，1979 年）
河上和雄「**強制捜査**の新展開」石原一彦ほか編『現代刑罰法大系(第五巻)刑事手続Ⅰ』173 頁以下(日本評論社，1983 年)
河上和雄(**ほか**＝渥美東洋＝中山善房＝古川定昭)**編**『**警察実務**判例解説(捜索・差押え篇)別冊判例タイムズ 10 号』(判例タイムズ社，1988 年)
河上和雄「**捜索・差押の範囲**」佐々木史朗ほか編『刑事訴訟法の理論と実務(別冊判例タイムズ 7 号)』283 頁以下(判例タイムズ社，1988 年)
河上和雄「**任意捜査**の限界――検察の立場から」三井誠ほか編『刑事手続(上)』308 頁以下(筑摩書房，1988 年)
河上和雄(**編**)『刑事**裁判実務大系(11)**犯罪捜査』（青林書院，1991 年）
河上和雄(**ほか**＝渥美東洋＝中山善房＝泉幸伸)**編**『**警察実務**判例解説**(取り調べ・証拠**篇**)** 別冊判例タイムズ 12 号』(判例タイムズ社，1992 年)
河上和雄(**ほか**＝中山善房＝古田佑紀＝原田國男＝河村博,＝渡辺咲子)**編**『**大コンメンタール**刑事訴訟法**第２巻**〔第二版〕』(青林書院，2010 年)
→補遺〔情報処理の高度化等に対処するための刑法等の一部を改正する法律〕（青林書院ホームページ(最新情報)2012/02/15：**河上和雄［ほか］編**『**大コンメンタール**刑事訴訟法〔**第二版**〕』に「**補遺**」を PDF 形式にて登載**[吉田**雅之執筆**]**。平成 24 年施行の一部改正法（平成 23 年法律 74 号）を緊急解説。既刊の 第２巻，第３巻，刊行予定の第４巻，第１０巻に関連。)http://www.seirin.co.jp/pdf/009100s-rev-2.pdf
川上宏二郎「行政法における比例原則」成田瀬明編『行政法の争点(法律学の争点シリーズ 9)』24 頁以下(有斐閣，1980 年)
川島武宜『日本人の**法意識**』(岩波新書，1994 年)
川崎英明「**差押**の範囲」村井敏邦＝後藤昭編著『現代令状実務 25 講』51 頁以下(日本評論社，1993 年)
川崎英明「盗聴立法の**憲法的問題点**」法律時報 69 巻 4 号 47 頁以下(1997 年)＝**小田中ほか・盗聴立法批判 87 頁以下**
川崎英明「**盗聴**の問題性格と理論性格」小田中聡樹(**ほか**＝村井敏邦＝川崎英明＝白取祐司著)『**盗聴**立法**批判**――おびやかされる市民の自由』**＝小田中ほか・盗聴立法批判** 125 頁以下(日本評論社，1997 年)
川崎英明『現代**検察官論**』(日本評論社，1997 年)
河原俊也「フロッピーディスクの包括的差押え」田口守一＝寺崎嘉博編『判例演習刑事訴訟法』68 頁以下(成文堂，2004 年)
河原峻一郎『基本的人権の研究』(有斐閣，1957 年)
川端亮二『データプライバシー』(ぎょうせい株式会社，1989 年)
河村博『公判に強い**捜査実務 101 問(改訂**第 **4 版)**』(立花書房，2009 年)
上口裕『**刑**事訴**訟**法(第 **3 版**)』(成文堂，2012 年)

き

菊井康郎「民事不介入」成田瀬明編『行政法の争点(法律学の争点シリーズ 9)』238 頁以下(有斐閣，1980 年)

貴志浩平「**ハイテク犯罪**の捜査に関する諸問題」警察論集 51 巻 7 号 99 頁以下(1998 年)
貴志浩平「ハイテク犯罪と**捜査手続**」捜査研究 564 号 18 頁以下(1998 年)
岸盛一『刑事訴訟法**要義（新版）**』（廣文堂書店，1962 年）
北村篤「**ハイテク犯罪**に対処するための刑事法の整備に関する要綱（骨子）」ジュリスト 1257 号 6 頁以下（2003 年)
北村篤「令状による差押え(3)――**相当性**」井上正仁編『刑事訴訟法判例百選(第 8 版) 別冊ジュリ 174 号』56 頁以下(有斐閣，2005 年)
北村滋「**写真**撮影，**ビデオ撮影**」河上和雄ほか『(講座)日本の警察(第二巻)』173 頁以下(立花書房，1993 年)
北村滋「捜索・差押えの状況の**写真撮影**」河上和雄(ほか＝渥美東洋＝中山善房＝古川定昭)編『警察実務判例解説(捜索・差押え篇)別冊判例タイムズ 10 号』64 頁以下(判例タイムズ社，1988 年)
木村順吾『**情報政策**法』(東洋経済新報社，1999 年)

く

久保田ぬき子「**プライバシーの権利**」田中二郎ほか編・小林直樹ほか執筆『日本国憲法体系：宮沢俊義先生還暦記念――基本的人権Ⅰ――第七巻』**145 頁以下**(有斐閣，1965 年)
熊谷弘「捜索・差押許可状の記載事項」『刑事訴訟法判例百選(新版)別冊ジュリスト 32 号』58 頁以下(有斐閣，1971 年)
熊本典道「**令状の意義**と種類(特集・捜査と人権)」判例タイムズ 296 号 18 頁以下（1973 年)
熊本典道「**憲法三五条**の意義」『昭和 48 年度重要判例解説（ジュリスト，臨時増刊 565 号）』158 頁以下(有斐閣，1974 年)
熊本典道「捜索令状・差押**令状の記載**」熊谷弘ほか編『捜査法大系Ⅲ捜索・押収』42 頁以下(日本評論社，1986 年)
栗田正「捜索押収令状の記載事項――日教組本部捜索事件の特別抗告」ジュリスト 162 号 19 頁以下(1958 年)
栗田正「憲法 35 条と捜索差押許可状の記載事項」『**最**高裁判所**判**例**解**説刑事篇**(昭和 33 年度)**』555 頁以下(法曹会，1959 年)
栗本一夫『新刑事訴訟法上の諸問題』(立花書房，1952 年)
金隆史「当事者の立会」熊谷弘ほか編『捜査法大系(Ⅲ)捜索・押収』75 頁以下(日本評論社，1986 年)

け

経済**産**業**省報告書**「欧州評議会**サイバー犯罪条約**と我が国の**対応**について(サイバー刑事法研究会報告書)」(2002 年)【www.meti.go.jp/policy/netsecurity/.../Cybercriminallawreport.pdf にて入手できる。本報告書は，経済産業省は，2001 年 8 月から欧州評議会サイバー犯罪条約への国内対応等を検討するために，山口厚東京大学教授が座長を務めているサイバー刑事法研究会を開催し検討を進めていた結果として取りまとめて公表したものである。】
警察庁情報システム安全対策研究会・不正アクセス対策法制分科会「**不正アクセス対策法**制に関する調査研究**報告書**」平成 10 年 3 月 http://www.npa.go.jp/cyber/research/h10/housei/nsreport.html

警察庁生活安全局生活安全企画課「**ハイテク犯罪**等に係る**被害状況**の調査《**報告書**》」平成 15 年 3 月 http://www.npa.go.jp/cyber/research/h14/image/higaicyousa.pdf

警察庁生活安全局情報技術犯罪対策課「**不正アクセス行為**対策等の**実態調査**(調査**報告書**)」平成 20 年 2 月 http://www.npa.go.jp/cyber/research/h19/H19countermeasures.pdf

警察庁刑事局『遂条**解説　犯**罪**捜**査**規範(6 版)**』(東京法令出版社，1991 年)

警察庁刑事部捜査課編『**適正な捜査**運営のために(刑事警察資料 41 巻)』(警察庁，1956 年)

刑事裁判資料 140 号：『刑事手続法規に関する通達・質疑回答集(追補Ⅱ)』(最高裁判所事務総局，1952 年)

刑事裁判資料 176 号：『令状関係法規の解釈運用について(下)』(最高裁判所事務総局，1967 年)

こ

小磯武男「医学鑑定――その現状と課題」判例タイムズ 1294 号 23 頁以下(2009 年)

香城敏磨『警察権限法の判例理論』河上和雄ほか編「講座――日本の警察――第二巻(刑事警察)」(立花書房，1993 年)

小杉修二「広域捜査力及び特殊事件捜査力の強化について」警察学論集 40 巻 1 号 74 頁以下(1987 年)

後藤昭「捜索差押の際の**写真撮影**」法律時報 58 巻 7 号 97 頁以下(1986 年)

後藤昭『**捜査法**の論理』(岩波書店，2001 年)

小林直樹「**基本権**への原理的視角」田中二郎ほか編・小林直樹ほか執筆『日本国憲法体系：宮沢俊義先生還暦記念――基本的人権Ⅰ――第七巻』1 頁以下(有斐閣，1965 年)

小林直樹「自動車ナンバー自動読取システム(N システム)事件」獨協法学 68 号 96 頁以下(2006 年)

小林充「マンションの一室を**捜索場所**とする捜索令状により，廊下，階段，エレベーター，共用駐車場等についてまで捜索することができるか，右部分に立ち入ることはどうか」新関雅夫ほか著『増補令状基本問題(下)』218 頁以下(判例時報社，2006 年)

小林充「**貸金庫**・コインロッカーに対する捜索令状とその執行」新関雅夫ほか著『増補令状基本問題(下)』223 頁以下(判例時報社，2006 年)

小林充『**刑**事**訴**訟法(**新訂**版)』(立花書房，2009 年)

小山雅亀「写し」井上正仁編『刑事訴訟法判例百選(第 8 版) 別冊ジュリ 174 号』196 頁以下(有斐閣，2005 年)

小山松吉『刑事訴訟法提要(合本)』(法政大學，1929 年)

小山剛ほか(訳)ユーゼフ・イーゼンゼー(著)「保護義務としての基本権」ドイツ憲法判例研究会編訳；栗城壽夫ほか(編集代表)『保護義務としての基本権』129 頁以下(信山社，2003 年)

根本渉「電話傍受のための令状の諸問題――検証説に対する批判的考察」警察研究 64 巻 6 号 24 頁以下(1993 年)

さ行

さ

斉藤豊治「アメリカの刑事鑑定制度」上野正吉ほか編『刑事鑑定の理論と実務――情状鑑定の科学化をめざして』37 頁以下(成文堂，1977 年)

佐伯仁志「プライヴァシーと名誉の保護――主に刑法的観点から**(1) ／(2) ／(3) ／(4 完)**」法学協会雑誌 101

巻 7 号 981 頁以下／8 号 1158 頁以下／9 号 1406 頁以下／11 号 1675 頁以下(1984 年)。
酒井吉栄「委任立法の限界」小嶋和司編『憲法の争点(新版)』156 頁以下(有斐閣，1985 年)
坂倉宏「情報化時代のコンピュータと法」ジュリスト 707 号 138 頁以下(1980 年)
阪本昌成「憲法と**プライバシーの権利**」神戸法学雑誌 22 巻 1 号 43 頁以下(1972 年)
阪本昌成「**プライバシー**の権利」奥平康弘＝杉原泰雄編『憲法学Ⅱ』14 頁以下(有斐閣，1976 年)
阪本昌成「**プライヴァシー権**」法学教室 41 号 6 頁以下(1984 年)
阪本昌成『**プライヴァシー権論**』(日本評論社，1986 年)
阪本昌成『憲法理論(Ⅱ)』(成文堂，1993 年)
阪本昌成「プライヴァソーと**自己決定の自由**」樋口陽一編『講座憲法学３　権利の保障〈１〉』220 頁以下(日本評論社，1994 年)
佐久間修「企業**秘密の侵害**における客体の財物性」産大法学 19 巻 3 号 49 頁以下(1985 年)＝**佐久間・無形的財産の保護 67 頁以下**
佐久間修「**無形的財産**の刑法的保護」産大法学 21 巻 1・2 号 69 頁以下(1987 年)＝**佐久間・無形的財産の保護 170 頁以下**
佐久間修『刑法における**無形的財産の保護**』(成文堂，1991 年)
笹倉宏紀「フロッピーディスク等につき内容を確認せずに差押えることが許されるとされた事例」ジュリスト 1191 号 80 頁以下(2000 年)
酒巻匡「いわゆる『**緊急差押**』について―『プレイン・ヴュー（plain view）』法理の検討」松尾浩也＝芝原邦爾編『刑事法学の現代的状況：内藤謙先生古稀祝賀』431 頁以下(有斐閣，1994 年)
酒巻匡「**捜索・押収**とそれに伴う処分」刑事雑誌 36 巻 3 号 444 頁以下(1997 年)
酒巻匡「新しい証拠収集手段――**提出命令**について」ジュリスト 1228 号 125 頁以下(2002 年)
酒巻匡「令状における**条件の付加**について」研修 658 号 3 頁以下(2003 年)
酒巻匡「刑事手続における**任意手段の規律**について」法学論叢(京都大學法学会)162 巻 1＝6 号 91 頁以下(2008 年)
佐藤幸治「**プライヴァシー**の**擁護**」中央公論 4 月号(1970 年)
佐藤幸治 「**プライヴァシー**の権利(その**公法的側面**)の憲法論的考察--その比較法的検討**(1)／(2)**」法学論叢（京都大学法学会） 86 巻 5 号 1 頁以下／同巻 6 号 1 頁以下 (1970 年)
佐藤幸治「**プライヴァシー**の権利」小嶋和司編『憲法の争点』92 頁以下(有斐閣，1978 年)
佐藤幸治「**通信の秘密**」芦部編『憲法Ⅱ――人権(1)』365 頁以下(有斐閣，1978 年)
佐藤幸治「**権利としてのプライバシー**」ジュリスト 742 号 158 頁以下(1981 年)
佐藤幸治「**プライバシーと知る権利**」法学セミナー395 号 18 頁以下(1984 年)
佐藤幸治「明白かつ現在の**危険**」小嶋和司編『憲法の争点**(新版)**』76 頁以下(有斐閣，1985 年)
佐藤幸治「**プライヴァシー**の権利」小嶋和司編『憲法の争点**(新版)**』114 頁以下(有斐閣，1985 年)
佐藤幸治『**憲法（第 3 版）**』（青林書院，1999 年)
佐藤功『憲法』(有斐閣，1955 年)
佐藤文哉「令状によらない捜索・差押(一)」熊谷弘ほか編『捜査法大系(Ⅲ)捜索・押収』7 頁以下(日本評

論社，1986 年）
佐藤文哉「**盗聴**」『刑事訴訟法判例百選（新版）』別冊ジュリスト 32 号 32 頁以下(有斐閣，1971 年)
佐藤隆一「別罪証拠の差押―**プレイン・ヴュー**の法理」現代刑事法現代刑事 5 巻 5 号＝通巻 49 号 31 頁以下（2003 年）

し

Bill Nelson ほか著 **SITE J1 訳**『コンピュータフォレンジックス入門―不正アクセス，情報漏洩に対する調査と分析』（トムソンラーニング，2005 年）
塩入みほも**(訳)**ユーゼフ・イーゼンゼー(著)「意見表明の自由の統制下における名誉保護」ドイツ憲法判例研究会編訳・栗城壽夫ほか(編集代表)『保護義務としての基本権』245 頁以下(信山社，2003 年)
椎橋隆幸『刑事弁護・捜査の理論』(信山社，1993 年)
椎橋隆幸『**刑**事**訴**訟法(第 **4 版**)』(不磨書房，2012 年)
鹿野伸二「時の判例」ジュリスト 1371 号 99 頁以下(2009 年)
實原隆志「ドイツ版『N システム』の合憲性」自治研究 86 巻 12 号 149 頁以下(2010 年)
下山瑛二「行政手続と人権保障」小嶋和司編『憲法の争点**(新版)**』132 頁以下(有斐閣，1985 年)
篠原弘志「捜索・差押え**(4)**――執行をめぐる諸問題」警察公論 38 巻 4 号 122 頁(1983 年)
島伸一「**写真撮影**」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版)』82 頁以下(有斐閣，1991 年)
島伸一『**捜索・差押**の理論』（信山社，1994 年）
島田仁郎「**科学捜査**と人権――ポリグラフ・麻酔分析・盗聴」松尾浩也編『刑事訴訟法の争点』82 頁以下(有斐閣，1979 年)
島田仁郎「電話の盗聴をするにはどのような令状が必要か」新関雅夫ほか著『増補令状基本問題(上)』52 頁以下(判例時報社，2006 年)
白取祐司「**科学捜査**と人権」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版)』別冊ジュリスト 78 頁以下(有斐閣，1991 年)
白取祐司『**刑**事**訴**訟法(第 **7 版**)』(日本評論社，2012 年)
白藤博行「リスク社会下の警察行政」ジュリスト 1356 号 82 頁以下(2008 年)
城綮「体液の**強制採取**」警察公論 36 巻 2 号 110 頁以下(1981 年)
洲見光男「修正４条の適用判断と『明白な準則』――『捜索』該当性判断を中心として」三原憲三先生古稀祝賀論文集編集委員会編集『三原憲三先生古稀祝賀論文集』695 頁以下（成文堂，2002 年）
新保佳宏「コンピュータをめぐる刑事手続法上の諸問題」『コンピュータ犯罪等に関する刑法一部改正(註釈）改訂増補版』145 頁以下(成文堂，1989 年)
新保史生(訳)マイケル・アドラー(著)『インターネット上の**デジタル禁制品の捜索**と修正第四条』駒沢大学大学院公法学研究 23 号 157 頁以下(1997 年)
新保史生『**プライバシー**の権利の生成と展開』(成文堂，2000 年)
法制**審議会**刑事法（**ハイテク**犯罪関係）会議**第** 1 **回**～8 回議事録**＝審議会（ハイテク）第〇回議事録**

す

須加憲子「人格的利益と不法行為―権利＝救済：制度的思考から脱却」法律時報 78 巻 8 号 49 頁以下(2006 年)

杉原泰雄「大学研究室の捜索と大学の自治―『和光大学事件』をめぐって・**(1)／(2)／(3)／(4)（5・完）**」法律時報 43 巻 7 号 121 頁以下／8 号 92 頁以下／10 号 76 頁以下／11 号 138 頁以下／12 号 120 頁以下(1971 年)

杉山治樹「**外国における捜査**活動の限界」平野龍一ほか編『新実例刑事訴訟法Ⅰ』50 頁以下(青林書院，1999 年)

杉山徳明**＝吉田**雅之「『**情報処理の高度化**等に対処するための刑法等の一部を改正する法律』について」警察学論集 64 巻 10 号 1 頁以下(2011 年)

杉山徳明**＝吉田**雅之「『**情報処理の高度化**等に対処するための刑法等の一部を改正する法律』について**(下)**」法曹時報 64 巻 5 号 55 頁以下(2012 年)

鈴木義男「差押許可状における差押物件の特定」法学ゼミな 34 号 74 頁以下(1959 年)

鈴木義男「刑事訴訟法における**比較法の意義**」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版)』16 頁以下(有斐閣，1991 年)

鈴木茂嗣「**憲法と刑**事**訴**訟法との関係」松尾浩也編『刑事訴訟法の争点』4 頁以下(有斐閣，1979 年)

鈴木茂嗣『**刑**事**訴**訟法(**改訂**版)』(青林書院，1990 年)

鈴木茂嗣『続**刑**事**訴**訟の**基本構造(上**巻**)**』(成文堂，1996 年)

鈴木秀美［訳］Rosler Albrecht 「翻訳 「オンライン捜索」についての連邦憲法裁判所判決--二〇〇八年二月二七日第一法廷判決 」阪大法学 58 巻 5 号 1235 頁以下(2009 年)

須藤陽子『比例原則の現代的意義と機能』(法律文化社，2010 年)

せ

関根廣行「警察における**デジタルフォレンジック**」警察政策 10 巻 229 頁以下(2008 年)

関正晴『Next 教科書シリーズ　**刑**事**訴**訟**法**』(弘文堂，2012 年)

そ

警察大学校刑事訴訟法研究会編『**捜査**手続法**資料(改訂**版**)**』(立花書房，1986 年)

警察大学校刑事教官室編『**捜査手続総合判例集**』(警察図書出版株式会社，1965 年)

た行

た

高原賢治「社会国家における財産権」田中二郎［ほか］編；小林直樹［ほか］執筆『日本国憲法体系：宮沢俊義先生還暦記念-基本的人権Ⅰ-第七巻』239 頁以下(有斐閣，1965 年)

田上穣治「基本的人権と**公共の福祉**」一橋大学一橋学会『一橋大学創立八十周年記念論文集(下巻)』217 頁以下 (勁草書房，1955 年)

田上穣治「行政作用法における**比例原則**」田中二郎ほか編『行政法講座(第六巻)』1 頁以下(有斐閣，1966 年)

大政正一「捜索差押許可状における目的物の特定方法」判例タイムズ 213 号 69 頁以下(1968 年)＝河村澄

夫(ほか＝柏井康夫＝古川實)編『刑事実務ノート(第 3 巻)』336 頁以下(判例タイムズ社，1988 年)
高木光「比例原則の実定化――『警察法』と憲法の関係についての覚書」樋口陽一ほか編『現代立憲主義の展開（下）』211 頁以下(有斐閣，1993 年)
髙杉顕「情報セキュリティにおける**暗号**の位置付けについて――暗号の常識，非常識」警察学論集 64 巻 7 号 134 頁以下(2011 年)
高田卓爾「憲法三五条と捜索差押**許可状の記載**事項」大阪市立大学法学雑誌 5 巻 4 号 124 頁以下(1959 年)
高田卓爾『**刑**事**訴**訟法[**2 訂版**]現代法律学全集 28』(青林書院新社，1984 年)
高田卓爾**編**『(別冊**法**学**セ**ミナー122 号)基本法**コンメ**ンタール**刑**事**訴**訟法(第三版)』(日本評論社，1993 年)
高橋正明『CCTV 監視システム基礎講座(改訂新版)』(産業開発機構株式会社，2004 年)
高橋正俊「通信の秘密」小嶋和司編『憲法の争点(新版)』104 頁以下(有斐閣，1985 年)
高橋誠志『電子的個人**データ保護**の方法』(信山社，2007 年)
高橋和之「憲法学からみた刑事訴訟法」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版)』10 頁以下(有斐閣，1991 年)
高橋明男『**比例原則**審査の可能性』法律時報 85 巻 2 号 17 頁以下(2013 年)
高橋勝「**通信の秘密(１)／(２・**完**)**」郵政調査時報 13 巻 2 号 1-25,39 頁以下,／郵政調査時報 13 巻 3 号 47 頁以下(1972 年)
高部道彦「捜索差押の際の写真撮影」研修 496 号 47 頁以下(1989 年)
高柳賢三(**ほか**＝大友一郎＝田中英夫)**編**著『日本憲法の制定過程――連合国総司令部側の記録による――Ⅰ**原文と翻訳**』(1972 年)
高柳賢三(**ほか**＝大友一郎＝田中英夫)**編**著『日本憲法の制定過程――連合国総司令部側の記録による――Ⅱ**解説**』(1972 年)
瀧川幸辰(**ほか**＝平場安治＝中武靖夫)著『**刑**事**訴**訟法（法律學体系 1 部**コンメ**ンタール篇 10)』(日本評論社，1950 年)
瀧波宏文「『サイバー犯罪に関する条約』について（上）手続法及び国際協力規定」警察学論集 55 巻 9 号 150 頁以下(2002 年)
田口守一「(二)強制採尿令状に『医師により医学的に相当な方法で行わしめること』を条件とする旨の記載がない場合に，これによって得られた証拠の証拠能力が認められた事例」判例評論 397 号(＝判例時報 1406 号)190 頁以下(1992 年)
田口守一「**検証**証許可状**による電話傍受**」田口守一＝寺崎嘉博編『判例演習刑事訴訟法』114 頁以下(成文堂，2004 年)
田口守一『**刑**事**訴**訟法(**6 版**)』(弘文堂，2012 年)
田口精一「私人相互間における権利保障」小嶋和司編『憲法の争点』46 頁以下（有斐閣，1978 年)
竹中勲「『新しい人権』の承認の要件」法学教室 103 号 42 頁以下(1989 年)。
田中開「捜査手続と準抗告」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版)』104 頁以下(有斐閣，1991 年)
田中輝和「鑑定」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版)』196 頁以下(有斐閣，1991 年)
田島泰彦**(監修)・清水**知子**(訳)**『９・１１以後の監視』(明石書局，2004 年)

種谷春洋「日本国憲法第13条後段の『**公共の福祉**』概念」岡山大学法経学会雑誌13巻2号1頁以下(1963年)
種谷春洋「**生命・自由**および**幸福追求**権」芦部編『憲法Ⅱ――人権(1)』130頁以下(有斐閣，1978年)
種谷春洋「**司法権の限界**」小嶋和司編『憲法の争点(新版)』171頁以下(有斐閣，1985年)
種谷春洋「**幸福追求**の権利」小嶋和司編『憲法の争点(新版)』76頁以下(有斐閣，1985年)
田宮裕「**強制捜査**」佐伯千仭＝団藤重光編『総合判例研究叢書――刑事訴訟法(16)』65 頁以下(有斐閣，1965年)
田宮裕「犯罪捜査と**写真撮影**――判例をめぐって」ジュリスト323号40頁以下(1965年)
田宮裕「捜査における**肖像権**とその限界――最高裁判例の意義――」判例タイムズ243号14頁以下(1970年)
田宮裕**編著**『**刑**事**訴**訟**法Ⅰ**――捜査・公訴の現代的展開(有斐閣大学双書)』(有斐閣，1975年)
田宮裕**編**『**刑**事**訴**訟**法Ⅰ**――捜査・公訴の現代的展開』(有斐閣，1975年)
田宮裕『**注釈刑**事**訴**訟法(付)刑事訴訟法規則』(有斐閣，1983年)
田宮裕**＝多田**辰也共著『セミナー　刑事**手続法**　捜査編』(啓正社，1990年)
田宮裕**編**『改訂新版　**ホーンブック　刑**事**訴**訟法』(北樹出版，1995年)
田宮裕『**刑**事**訴**訟法**(新版)**』(有斐閣，2000年)
田村武志『図解・情報通信ネットワークの基礎(2版)』(共立出版株式会社，2000年)
壇上弘文「フロッピーディスク等につき捜索差押の現場で内容を確認せずに差し押さえることが許されるとされた事例」捜査研究571号50頁以下(1999年)
壇上弘文「**サイバー関係**をめぐる刑事訴訟法の一部改正について」刑法ジャーナル30号33頁以下(2011年)
団藤重光『**[旧]** 刑事訴訟法**綱要**』(弘文堂書房，1943年)
団藤重光『**訴訟状態**と訴訟行為――刑事訴訟における――』(弘文堂，1949年)
団藤重光『**条解**刑事訴訟法**(上)**』(弘文堂，1950年)
団藤重光「**刑**事**訴**訟法の**一部**を**改正**する法律――批判と解説」法律時報280号863頁以下(1953年)
団藤重光『**新**刑事訴訟法**綱要(7**訂版**)**』(創文社，1972年)

つ

警察庁警察大学校刑事判例研究会「**通信関係書類の押収捜索**」警察学論集8巻7号85頁以下(1955年)
警察大学校編「**通信**関係書類の**押収捜索**について」警察学論集8巻7号85頁以下(1955年)
辻裕教「検証許可状による電話の傍受が適法とされた事例」研修582号21頁以下(1996年)
土屋彰久**(訳)**Colin J.Bennett(著)『プライバシー保護と行政の対応』(文真堂，1994年)
土屋真一「捜索差押令状の**捜索場所の特定**及び違法収集証拠の証拠能力」研修339号59頁以下(1976年)
坪内利彦「写真撮影」三井誠ほか編『刑事手続(上)』151頁以下(筑摩書房，1988年)

て

寺崎嘉博「電磁的記録に対する包括的差押え」廣瀬健二＝多田辰也編『田宮裕博士追悼論集(下巻)』11頁以下(信山社，2003年)

寺崎嘉博『**刑**事**訴**訟法(第**2版**)』(成文堂，2008 年)
寺中良則「逮捕に伴う捜索・差押え」警察公論 36 巻 2 号 29 頁以下(1981 年)
電気通信法制研究会編『逐条解説電気通信事業法』(第一法規出版，1987 年)

と

藤乗一道「サイバー犯罪等への対処―情報処理の高度化等に対処するための刑法等の一部改正案」立法と調査 316 号(2011 年)
戸波江二「**人権**の性格と限界」法学教室 141 号 24 頁以下(1992 年)
戸波江二「**自己決定**権の意義と射程」樋口陽一ほか編『現代立憲主義の展開(上)：芦部信喜先生古稀祝賀』325 頁以下(有斐閣，1993 年)
戸波江二・**嶋崎**健太郎**(訳)**ユーゼフ・イーゼンゼー(著)「解釈者のエートスについて――規範解釈の主観的要素とその立憲国家への包含」ドイツ憲法判例研究会編訳；栗城壽夫ほか(編集代表)『保護義務としての基本権』3 頁以下(信山社，2003 年)

な行

な

内藤丈夫「執行時刻の制限」熊谷弘ほか編『捜査法大系(Ⅲ)捜索・押収』89 頁以下(日本評論社，1986 年)
中井憲治「体液の採取」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版)』84 頁以下(有斐閣，1991 年)
中下晴興「捜索・差押えと必要な処分」警察公論 36 巻 2 号 45 頁以下(1981 年)
中武靖夫**＝高橋**太郎(編)『**捜査法**入門』(青林書院新社，1978 年)
中村睦男「法定手続の保障と明確性原則」法学教室 89 号 6 頁以下(1988 年)
永田秀樹**＝松本**和彦**＝倉田**原志**(訳)**ボード・ビエロート＆ベルンハルト・シュリンク(著)『現代ドイツ基本権』(法律文化社，2001 年)
長沼範良「犯罪・差押目的物の存在の**蓋然性**」刑法雑誌 36 巻 3 号 420 頁以下(1997 年)
長沼範良「**ネットワーク犯罪**への手続法的対応」ジュリスト 1148 号 212 頁以下(1999 年)
長沼範良「**電磁的情報**に関する捜索・差押え」現代刑事法 5 巻 5 号＝通巻 49 号 45 頁以下(2003 年)
長沼範良「**コンピュータ犯罪**と新たな捜査手法の導入」L&T(エル・アンド・ティ)26 号 12 頁以下(2005 年)
長沼範良**＝山田**利行「コンピュータと捜査(最二小決平成 10 年 5 月 1 日刑集 52 巻 4 号 275 頁)」法学教室 334 号 46 頁(2008 年)
中野次雄**(ほか)編**『判例とその読み方(三訂版)』(有斐閣，2009 年)
中野目善則編著『法の機能と法解釈』(八千代出版，1994 年)
中山研一**＝神山**敏雄**(編)**『コンピュータ犯罪等に関する刑法一部改正(註釈) 改訂増補版』(成文堂，1989 年)
中利太郎「令状の記載事項の変更ないし追加は許されるか」平野龍一・松尾浩也編『刑事訴訟法(新版)実例法学全集』12 頁以下(青林書院新社，1997 年)
夏井高人『裁判実務とコンピュータ――法と技術の調和をめざして』(日本評論社，1993 年)

奈良恵一「米国における捜査機関相互間及び捜査機関と行政機関相互間における捜査協力，情報共有について」警察学論集 58 巻 12 号(2005 年)
名取俊也「**コンピュータ**・システムと捜査――検察の立場から」三井誠ほか編『新刑事手続法Ⅰ』389 頁以下（悠々社，2002 年）
名取俊也「**写真**・ビデオ嫌影」三井誠ほか編『新刑事手続法Ⅰ』349 頁以下（悠々社，2002 年）
鍛越溢弘「DNA 型鑑定」井上正仁編『刑事訴訟法判例百選(第 8 版）』別冊ジュリスト 174 号 152 頁以下(有斐閣，2005 年)
成田秀樹「捜査と**プライバシーの保護**」現代刑事法 6 巻 4 号 34 頁以下(2004 年)
成田秀樹「**電子的捜査**とプライバシー」刑法雑誌 45 巻 1 号 142 頁以下(2005 年)

に

西村好順「捜索･差押令状の範囲」河上和雄編『刑事裁判実務大系(11)犯罪捜査』264 頁以下(青林書院，1991 年)
西村法「公務所･大学･労組等の捜索――責任者の立会」熊谷弘ほか編『捜査法大系(Ⅲ)捜索・押収』82 頁以下(日本評論社，1986 年)
庭山英雄＝**森井**暲(**編著**)『法学基本講座　**刑**事**訴**訟法 **100 講**』(学陽書房，1986 年)
庭山英雄＝**岡部**泰昌『**刑**事**訴**訟**法**(第 **3 版**)』(学陽書房，1986 年)

ね

根森建「人権としての個人の尊厳」法学教室 175 号 52 頁以下(1995 年)
根森建「人格権の保護と『**領域理論**』の現代」『人権と憲法裁判』75 頁以下(成文堂，1993 年)
根森建「『**人間の尊厳**』の具体化としての『精神の自由』：福岡ゲルニカ事件再訪」『ドイツ公法理論の受容と展開――山下威士先生還暦記念』365 頁以下(尚学社，2004 年)

の

能勢弘之『論点法律学　**刑**事**訴**訟法 **25 講**』(青林書院，1987 年)
野中俊彦(**ほか**＝中村睦男＝高橋和之＝高見勝利）著『**憲法Ⅰ(5 版)**』(有斐閣，2012 年)
野本靖之「ネットワーク利用形態の多様化と**デジタルフォレンジックの課題**」警察政策 12 巻 227 頁以下(2010 年)

は行

は

「**ハイテク犯罪**に対処するための刑事法の整備に関する要綱［骨子］――平成 15 年 9 月 10 日：法務省の法制審議会答申とその**関連資料**」ジュリスト 1257 号 34 頁以下（2003 年）
ハインリッヒ・**ショラー(著)／嶋崎**健太郎**(訳)**「基本権論における領域論と保護区域論」自治研究 69 巻 4 号 68 頁(1993 年)

橋本公亘『現代法学**全集**２**憲法(改訂版)**』(**青林書院新社**，**1976** 年)

橋本公亘「**プライヴァシー**の権利」芦部信喜ほか編『アメリカ憲法の現代的展開Ⅰ：人権』3 頁以下(東京大学出版会，1978 年)

橋本公亘『日本国**憲法(改訂版)**』(有斐閣，1988 年)

長谷川正安『**憲法解釈**の研究』(勁草書房，1974 年)

長谷部恭男『(新法学ライブラリ―2)憲法(第 3 版)』(新世社，2004 年)

濱田純一「マルチメディアと〈情報に対する権利〉」マス・コミュニケーション研究 No. 52，67 頁以下(1998 年)

馬場義続「占領下における刑訴法制定雑感」ジュリスト 551 号 21 頁以下 (1974 年)

早川武夫「適正法定手続」小嶋和司編『憲法の争点(新版)』128 頁以下(有斐閣，1985 年)

林頼三郎『刑事訴訟法要義・各則(上巻)』(東京中央大学，1924 年)

原田国男「**磁気テープ**の証拠能力」平野龍一ほか編『続刑事訴訟法 (実例法学全集) 』317 頁以下 (青林書院新社，1980 年)

原田國男「**コンピュータ**，クレジット，カード等を利用した犯罪」石原一彦ほか編『現代刑罰法大系――経済活動と刑罰(第 2 巻)』223 頁以下(日本評論社，1983 年)

原田尚彦「正当な補償」小嶋和司編『憲法の争点(新版)』122 頁以下(有斐閣，1985 年)

原田三朗(**ほか**＝日笠完治＝鳥居壮行)『**新・情報**の法と倫理』(北樹出版，2003 年)

ひ

日沖憲郎「電気は物か」『判例百選』ジュリスト 200 号 (ジュリスト臨時増刊 4 月号)2 頁以下(1960 年)

樋口陽一［**ほか**］共著『**注釈**日本国**憲法 (上巻)** 』(青林書院新社，1984～1988 年)

樋口陽一(**ほか＝**佐藤幸治＝中村睦男＝浦部法穂)共著『**注解**法律學全集Ⅳ**憲法Ⅰ**』(青林書院，1994 年)

久岡康成「科学的捜査」法律時報 61 巻 10 号 26 頁以下(1989 年)

平松毅「**通信の秘密**」『憲法判例百選Ⅰ』66 頁以下(有斐閣，1980 年)

平田勝雅「刑訴法 **111 条**の必要な処分の意義」判例タイムズ 296 号 417 頁以下(1973 年)

平田勝雅「刑訴法 **129 条**の必要な処分の意義」判例タイムズ 296 号 420 頁以下(1973 年)

平野大＝渡辺脩「電位的記録の定義規定(コンピュータ犯罪新設規定の遂条解説)」日本弁護士連合会刑法改正対策委員会編『コンピュータ犯罪と現代刑法』90 頁以下(三省堂，1990 年)

平場安治『**改訂**刑事訴訟法**講義**』(有斐閣，1954 年)

平場安治『**刑**事**訴**訟法の**基本問題**』(有信堂，1960 年)

平場安治「捜索差押**許可状の特定**に関する二つの東京地裁決定」判例評論 14 号(＝判例時報 158 号)1 頁以下(1958 年) **＝平場・刑訴基本問題 224 頁以下**

平野龍一「**人身の保障**――特に刑事手続における―」国家学会雑誌 64 巻 2・3 号 37 頁以下(1950 年)

平野龍一『**刑**事**訴**訟法Ⅲ・完(法律学**講座**Ⅷ)』(弘文堂，1953 年)

平野龍一『**刑**事**訴**訟法(法律学**全集** 43)』(有斐閣，1958 年)

平野龍一「**日教組**差押捜索事件」『続判例百選(旧版)』(ジュリスト臨時増刊 10 月号)158 頁以下(1960 年)

平野龍一『**刑**事**訴**訟法**概説**』(東京大学出版会，1968 年)
平野龍一「**罪刑法定主義**の感覚――コピーの偽造に関して」警察研究 49 巻 2 号 3 頁以下(1978 年)
平野龍一＝**松尾**浩也**編**『**実例**法学全集　続　**刑**事**訴**訟法』(青林書院，1980 年)
平場安治**ほか**著『**注解**刑事訴訟法**(上巻)**』(青林書院新社，1968 年)
平場安治［**ほか**］共著『**注解**刑事訴訟法**(全訂新版)上巻**』(青林書院新社，1982 年)
廣畑史朗「コンピュータ犯罪と**鑑定**」警察学論集 40 巻 12 号 23 頁以下(1987 年)
廣畑史朗「コンピュータ犯罪と**検証**」警察学論集 40 巻 11 号 1 頁以下(1987 年)
廣畑史朗「コンピュータ犯罪と**捜索**，**差押え**」警察学論集 41 巻 3 号 65 頁以下(1988 年)
廣畑史朗「コンピュータ犯罪と**証拠法**」警察学論集 41 巻４号 83 頁以下(1988 年)
平良木登規男『**捜査法**』(成文堂，1996 年)
平良木登規男『**刑**事**訴**訟**法Ⅰ**』(成文堂，2009 年)
平良木登規男(**ほか**＝椎橋隆幸＝加藤克佳)**編**『**判例**講義**刑**事訴**訟**法』(悠々社，2012 年)

ふ

藤井俊夫『憲法訴訟の基礎理論』(成文堂，1981 年)
藤永幸治＝河上和雄＝中山善房［**ほか**］**編**『**大コンメンタール**刑事訴訟法**(第二巻)**［第 57 条～第 188 条の７］』(青林書院，1994 年)→同書 2010 年(第二版) ＝**河上ほか編・大コンメンタール第２巻**
藤田潔「電気通信とプライバシー(通信の秘密の保護)」堀部政男編『ジュリスト増刊　情報公開・個人情報保護』224 頁以下(有斐閣，1994 年)
藤野英一「写真撮影」熊谷弘ほか編『捜査法大系(Ⅲ)捜索・押収』263 頁以下(日本評論社，1986 年)
藤原静雄「西ドイツ国勢調査判決における『**情報の自己決定権**』」一橋論叢 94 巻 5 号 138 頁以下(1985 年)
不正アクセス対策法制研究会編著『遂条不正アクセス行為の禁止等に関する法律（補訂第 2 版)』(立花書房，2008 年)
福井厚「差押物の特定」村井敏邦・後藤昭編著『現代令状実務 25 講』27 頁以下(日本評論社，1993 年)
福井厚『**刑**事**訴**訟法**講義(5 版)**』(法律文化社，2012 年)
古田佑紀「コンピュータネットワーク上の捜査と**第三者の保護**」芝原邦爾＝西田典之＝井上正仁編集『松尾浩也先生古稀祝賀論文集(下巻)』187 頁以下(有斐閣，1998 年)
古田佑紀「**犯罪の発生時期**と捜査の開始時期判例」タイムズ 528 号 52 頁以下(1984 年)
古田佑紀**(監修)**『任意捜査の限界 101 問』(立花書房，1996 年)
舟田正之「**情報の取引とプライバシー――NTT のデータベース事業をめぐって**」『ネットワーク社会と法(ジュリスト増刊)』77 頁以下(有斐閣，1988 年)

ほ

法學協會編『**註解**日本國**憲法(上)**』(有斐閣，1948 年)
法曹会編『**例題**解説刑事訴訟法(六)』(法曹会，1997 年)
「電気窃盗に就て」**法律新聞 86 号** 257 頁以下 (1902 年)

法務省刑事局刑事訴訟法研究会編『**実務刑**事**訴**訟法』（立花書房，1994 年）
穂積陳重『穂積陳重遺文集第二冊』（岩波書店，1932 年）
堀部政男**（編著）**『**インターネット**社会と法』（新世社，2003 年）

ま行

ま

前田雅英「刑事訴訟における**相当性判断**」井上正仁＝酒巻匡編『三井誠先生古稀祝賀論文集』495 頁以下（有斐閣，2012 年）
牧野英一『**刑**事**訴**訟法**（改訂**版**）**』（有斐閣，1940 年）
牧野二郎「**イ**ンター**ネ**ットと**盗聴**」右崎正博ほか編『盗聴法の総合的研究――通信傍受法と市民的自由』124 頁以下（日本評論社，2001 年）
幕田英雄「捜索差押現場における写真撮影――捜索差押現場の状況等の写真撮影は，どこまで許されるか」捜査研究 31 巻 2 号 79 頁以下（1982 年）
幕田英雄『実例中心**捜査法解説**　捜査手続きから証拠法まで』（東京法令出版，1989 年）
幕田英雄『実例中心**捜査法解説**（**3 版**）捜査手続きから証拠法・公判手続入門まで』（東京法令出版，2012 年）
増井清彦『**犯罪捜査** 101 問**（補訂**第 **5 版）**』（立花書房，2005 年）
松井茂記『**情報コントロール権**としてのプライバシーの権利』法学セミナー404 号 37 頁以下（1988 年）
松井茂記「**自己決定権**について**（二・**完**）**」阪大法学 45 巻 5 号 717 頁以下（1995 年）
松井茂記『**インターネット**の憲法学』（岩波書店，2002 年）
松井茂記『公共の安全と**インターネット**上の**人権**』法とコンピュータ 23 号 3 頁以下（2005 年）
松井茂記『日本国憲法〔第 3 版〕』（有斐閣，2007 年）
松沢栄一「**通信ログ**の保全　刑事訴訟法の改正」法とコンピュータ 23 号 53 頁以下（2005 年）
松浦秀寿「写真撮影」判例タイムズ 296 号（特集：捜査と人権――令状事務の理論と実務）46 頁以下（1973 年）
松浦一夫『**ドイツ基本法**と安全保障の再定義』（成文堂，1998 年）
松岡正章「当事者主義と鑑定」上野正吉ほか編『刑事鑑定の理論と実務――情状鑑定の科学化をめざして』107 頁以下（成文堂，1977 年）
松倉豊治『改訂捜査法医学』（東京法令出版，1971 年）
松尾浩也**＝田宮**裕『**刑**事**訴**訟法の**基礎知識**〔質問と回答〕』（有斐閣，1979 年）
松尾浩也「**刑**事**訴**訟法**（上）新版**」（弘文堂，1999 年）
松尾浩也（監修）『**条解**刑事訴訟法**（第 3** 版**増補**版**）**』（弘文堂，2006 年）
松尾浩也（監修）『**条解**刑事訴訟法（第 **4 版）**』（弘文堂，2009 年）
松本和彦「**基本権の保障と制約（一）／（二・完）**――ドイツにおける防禦権のドグマーティクの法的構造」民商法雑誌 111 巻 1 号 25 頁以下／同 2 号 223 頁以下（1994 年）
松本和彦「**基本権の保障**と論証作法**（一）／（二）／（三）／（四・完）**――ドイツ連邦憲法裁判所の国勢調査判決を素材にして」阪大法学 45 巻 1 号 53 頁以下／同 2 号 339 頁以下／同 5 号 791 頁以下／同 6 号 981 頁以下（1995 年）

松本和彦「**法律**による基本権の**保障(二・完)**」大阪学院大学法学研究 24 巻 2 号 1 頁以下(1998 年)
松本和彦(訳)ユーゼフ・イーゼンゼー(著)「**防禦権**としての基本権」ドイツ憲法判例研究会編訳；栗城壽夫ほか(編集代表)『保護義務としての基本権』51 頁以下(信山社，2003 年)
的場純男「コンピュータ犯罪と捜査」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版)』94 頁以下(有斐閣，1991 年)
丸谷定弘「捜索・差押令状の執行方法」熊谷弘ほか編『捜査法大系(Ⅲ)捜索・押収』58 頁以下(日本評論社，1986 年)

み
三浦守「写真撮影」井上正仁編『刑事訴訟法判例百選(第 8 版) 別冊ジュリ１７４号』20 頁以下(有斐閣，2005 年)
三浦守(ほか＝松並孝二＝八澤健三郎＝加藤俊治)『**組織的犯罪**対策関連**三法**の**解説**』(法曹会，2001 年)
三浦正充「警察捜査と刑事手続をめぐる若干の論点について」警察学論集 52 巻 1 号 37 頁以下(1999 年)
水谷規男「第 9 条～第 18 条」右崎正博ほか編『盗聴法の総合的研究――通信傍受法と市民的自由』224 頁以下(日本評論社，2001 年)
三島聡「第 1 条～第 8 条；附則・別表」右崎正博ほか編『盗聴法の総合的研究――通信傍受法と市民的自由』184 頁以下(日本評論社，2001 年)
三島聡「人権保障の確実性の要請と**盗聴立法(上)／(下)**」法律時法 70 巻 2 号 50 頁以下／同 70 巻 3 号 89 頁以下(1998 年)
三島聡「**盗聴法**を**解剖**する」法学セミナー539 号 52 頁以下(1999 年)
水町和寛「自動車ナンバー自動読取システムの研究開発の概要」警察学論集 40 巻 2 号 115 頁以下(1987 年)
三井誠**＝酒巻**匡『**入門**刑事**手続法**(第 **5 版**)』(有斐閣，2010 年)
三井誠『刑事**手続法(1)[新版]**』(有斐閣，1997 年)
三井誠**ほか編『刑事手続(上)**』(筑摩書房，1988 年)
三井誠「科学的捜査[１]――**写真撮影**」法教 147 号 74 頁以下(1992 年)**＝三井・手続法(1)[新版]114 頁以下**
三井誠「**捜査・総説**[２]」法学教 140 号 94 頁以下(1992 年) **＝三井・手続法(1)[新版]79 頁以下**
三井誠「捜索・差押え・検証に関する諸問題〔３〕――**盗聴**」法学教 138 号 33 頁以下(1992 年) **＝三井・手続法(1)[新版]69 頁以下**
光藤景皎『**口述刑**事**訴**訟法**(上)**』(成文堂，2005 年)
光藤景皎『**刑**事**訴**訟法Ⅰ』(成文堂，2007 年)
緑大輔「捜査機関が公道上およびパチンコ店内において被告人の容ほう等をビデオ撮影した活動および捜査機関による公道上のごみ集積所に排出されたごみの領置が適法と判断された事例」法学セミナー増刊・速報判例解説第 3 巻 213 頁以下(2008 年)
緑大捕「刑事手続上の**対物的処分**における権利・利益の帰属**と強制処分性**」刑法雑誌 51 巻 2 号 147 頁以下(2012 年)
緑大捕「無令状捜査押収と**適法性判断(1)**――憲法 35 条による権利保障――」修道法学 28 巻 1 号 452 頁以

下(2005 年)
緑大輔「対物的強制処分の執行――『**必要な処分**』の法的規律」法学セミナー669 号 112 頁以下(2010 年)
三林宏「権利客体としての情報――情報保護の民事法的規制を中心に(上)」明治大学法科大学院論集 7 号 163 頁以下(2010 年)
三堀博『**犯罪捜査**法』(花立書房，1952 年)
美濃部達吉『逐條憲法精義(全)』(有斐閣，1927 年)
宮沢俊義『**憲法Ⅱ[旧版]**』(有斐閣，1959 年)
宮沢俊義『**憲法Ⅱ(新版)**』(有斐閣，1971 年)
宮澤俊義『日本国**憲法(**法律學体系・**コンメ**ンタール篇**)**』(日本評論新社，1995 年)
宮本英脩『刑事訴訟法大綱』(松華堂，1936 年)
宮下明義『新刑事訴訟法逐条解説Ⅱ捜査・公訴』(司法警察研究会公安発行所，1949 年)
三好幹夫「令状の記載事項の追加ないし変更の許否」新関雅夫ほか著『増補令状基本問題(上)』28 頁以下(判例時報社，2006 年)

む

武藤文雄「新警察と刑事警察」警察研究 20 巻 1 号 53 頁以下 (1949 年)
棟居快行「**プライヴァシー**概念の**新構成**」神戸法学雑誌 36 巻 1 号 1 頁以下(1986 年)
棟居快行「監視カメラの憲法問題」神戸法学雑誌 43 巻 2 号 391 頁以下(1993 年)
棟居快行『**人権論**の新構成(改版新装)』(信山社，2008 年)
村井敏邦「令状主義はだれのもの」法学セミナー435 号 100 頁以下 (1991 年)
村井敏邦編著『**現代刑**事**訴**訟法**(**第 **2** 版**)**』(三省堂，1998 年)
村井敏邦**＝後藤**昭**(編著)『現代令状**実務 25 講』(日本評論社，1993 年)
村上健「**任意捜査**における有形力行使の限界」松尾浩也＝井上正仁編『刑事訴訟法の争点(新版) 別冊ジュリスト 6』 50 頁以下(有斐閣，1991 年)
村瀬均「将来発生する犯罪事実についての令状発付の可否」『(増補)令状基本問題(上)』34 頁以下(判例時報社，2006 年)
村田正幸『マルチメディア情報ネットワークー：コンピュータネットワークの構成学』 (共立出版株式会社，1999 年)

も

森井暲「写真撮影」『刑事訴訟法判例百選(5 版)』26 頁以下(有斐閣，1986 年)

や行

や

矢口俊昭「科学技術の発展と自己決定権――安楽死・尊厳死を中心に」法学教室 21 号 22 頁以下(1998 年)
山内一夫「脅迫電話の逆探知の合憲性」判例時報 376 号 6 頁以下(1964 年)

ローレンス・レッシグ（著）；**山形浩生，柏木亮二（訳）**『コード・バージョン 2.0』（翔泳社，2007 年）
山川健「インターネットの世界はどうなるか」法学セミナー539 号 62 頁以下(1999 年)
山口和人「海外法律情報 ドイツ--「オンライン捜索」の合憲性をめぐる争い 」ジュリス 1359 号 66 頁以下（2008 年）
山口厚「企業秘密の保護」ジュリスト 852 号 46 頁以下(1986 年)
柳川重規「最新重要判例評釈(10)フロッピーディスク等につき内容を確認せずに差し押さえることが許されるとされた事例--最二小決平成 10.5.1 刑集 52・4・275」現代刑事法 1 巻 5 号 79 頁以下（1999 年）
柳俊夫「捜索・差押え――検察の立場から」三井誠ほか編『刑事手続(上)』291 頁以下(筑摩書房，1988 年)
柳瀬良幹「憲法と補償--憲法第 29 条に関する臆説-**(1)**／**(2)**／**(3・完)**-」自治研究 25 巻 7 号 9 頁以下／8 号頁 44 以下／9 号 3 頁以下(1949 年)
山下義昭「『比例原則』は法的コントロールの基準たりうるか――ドイツにおける『比例原則』論の検討を通じて――**(一)**」福岡大学法学論叢 36 巻 1・2・3 号 139 頁以下（1991 年）
山田晟『ドイツ**法律用語**辞典(改訂増補版・第 4 版)』(大学書城，2001 年)
山田道郎「フロッピーディスクの包括的差押え」『平成 4 年度重要判例解説（ジュリスト，臨時増刊 1024 号）』192 頁以下(有斐閣，1993 年)
安富潔「**コンピュータ犯罪の捜査**と証拠」法とコンピュータ 6 号 28 頁以下（1988 年）
安富潔『刑事手続と**コンピュータ犯罪**』(慶応義塾大学法学研究会，1992 年)
安富潔「刑事訴訟法と**判例の機能**」刑法雑誌 33 巻 1 号 73 頁以下(1993 年)
安富潔「**科学的捜査**と証拠**(一)**」警察学論集 46 巻 7 号 167 頁以下（1993 年）
安富潔『**演習**講義　**刑**事**訴**訟法』(法学書院，1993 年)
安富潔『演習講座　**捜査**手続**法**』(立花書房，1994 年)
安富潔「**フロッピーディスク**等につき内容を確認せずに差し押さえることが許されるとされた事例」判例評論 487 号(判例時報 1679 号)242 頁以下（1999 年）
安富潔『**ハイテク犯罪**と刑事手続』(慶応義塾大学法学研究会，2000 年)
安富潔『**刑**事**訴**訟**法**』(三省堂，2009 年)
安富潔『**刑**事**訴**訟法**講義(2 版)**』(慶應義塾大学出版会，2009 年)
山本未来「自動車ナンバー自動読取システム(N システム)の許容性と根拠――従来の判例理論に対する行政調査の視点からの分析」明治学院大学法科大学院ローレビュー6 号 95 頁以下(2007 年)

ゆ

結城光太郎「正当な補償の意味」公法研究 11 号 82 頁以下(1954)
アメリカ自由人権協会(編著)**YOUR RIGHT TO PRIVACY 和訳会(訳)** 青木宏治，高嶌英弘監訳「プライバシーの権利 ： 情報化社会と個人情報保護」(株式会社教育史料出版会，1994 年)
郵政省編『郵政関係新聞雑誌記事集(郵政百年史資料 21 巻)』(吉川弘文館，1971 年)

よ

横井大三「犯罪捜査に関する**裁判官の権限(一)**」警察研究 21 巻 1 号 27 頁以下(1950 年)
横井大三「判例研究――捜索差押**令状の記載**要件――」研修 123 号 72 頁以下(1958 年)
横井大三「**押収・捜索**」法学セミナー57 号 42 頁以下(1960 年)
横井大三「捜索差押許可状の発付とその**必要性の判断**」研修 160 号 57 頁以下(1961 年)
横井大三「捜索差押**許可状の記載**」研修 212 号 37 頁以下(1966 年)
横井大三『**刑訴裁判例ノート(1)**：捜査』(有斐閣，1971 年)
横井大三「**各別の令状**の意義その他」研修 296 号 53 頁以下(1973 年)
横井大三『**刑訴裁判例ノート(6)**：捜査・証拠・公訴・公判・上訴・その他』(有斐閣，1973 年)
横田安弘＝**高橋**省吾『刑事抗告審の運用上の諸問題〔増補〕』司法研究報告書 36 輯 1 号(司法研修所，1991 年)
吉田統宏「フロッピーディスクの包括的差押」研修 580 号 63 頁以下(1996 年)
吉田昭『判例学説中心　**捜査手続**法精義(四訂版)』(東京法令，1995 年)
吉田作穂『各種令状に関する研究』(有恒社，1950 年)
吉田淳一「捜索差押許可状の請求をするに際しての資料の提供及び場所の特定」平野龍一＝松尾浩也編『刑事訴訟法(新版)実例法学全集』69 頁以下(青林書院新社，1997 年)
吉川経夫**＝小田中**聡樹『**治安と人権**』(法律文化社，1974 年)
吉川澄一『**刑事鑑識**』(立花書房，1955 年)
吉村徳則「**科学的捜査**――検察の立場から」三井誠ほか編『刑事手続(上)』129 頁以下(筑摩書房，1988 年)
ホセ・**ヨンパルト**「『人間の尊厳』と『個人の尊重』」法学教室 88 号 48 頁以下(1988 年)
米澤慶治**(編)**『**刑法**等一部**改正**法の**解説**』(立花書房，1988 年)

ら行

り

劉芳伶「『情報の差押』という制度の在り方について」法律時報 82 巻 2 号＝通巻 1018 号 91 頁以下(2010 年)

れ

裁判所書記官研修所編修『**令状事務(第 1 版)**』(法曹会，1981 年)
裁判所書記官研修所編修『**令状事務(再訂**版**)**』(法曹会，1995 年)
司法研修所検察教官室実務研究会編著『**令状請求の実際 101 問**』(立花書房，1996 年)

わ行

わ

和田英夫「国家権力とプライヴァシー　―その公法的側面」戒能通孝ほか編著『プライヴァシー研究』129 頁以下(日本評論社，1986 年)
和田英夫(**ほか**＝原田三朗＝日笠完治＝登板治彦)『**情報**の法と倫理』(北樹出版，1999 年)
和田康敬「強制採尿に関する最高裁決定について」警察公論 36 巻 2 号 22 頁以下(1981 年)
渡辺咲子『刑事訴訟法講義(第 6 版)』(不磨書房，2012 年)

渡辺直行『刑事訴訟法[補訂版]』(成文堂，2011 年)
渡邊一弘「覚せい剤取引に使用されていた電話の通話内容を検証許可状に基づき傍受･録音することが達意，違法ではないとされた事」警察学論集 46 巻 1 号 161 頁以下(1993 年)
渡辺脩「『財産的情報』と刑法」日本弁護士連合会刑法改正対策委員会編『コンピュータ犯罪と現代刑法』2 頁以下(三省堂，1990 年)

中文文献・資料

四画

王兆鵬「自**令状原則**論我國相關規定之缺失」刑事法雜誌 44 卷 4 期 32 頁以下(2000 年)
王兆鵬『**搜索扣押**與刑事被告的憲法權利』(自己出版，2000 年)
王兆鵬「**新修**訂刑訴法之緊急**搜索**」月旦法學雜誌 72 期 99 頁以下(2001 年)
王兆鵬『**刑**事**訴**訟**講義(一)２版**』(元照，2003 年)
王兆鵬「重新定義**高科技**時代下的**搜索**」『新刑訴・新思維』57 頁以下(元照，2004 年)
王兆鵬『**刑**事**訴**訟法**講義**』(元照，2010 年)
王郁琦「**生物辨識技術**之應用對隱私權之影響」科技法律評論 3 卷 2 期 49 頁以下(2006 年)
王俊文「我國憲法上**隱私權**相關問題之釐清」東吳法研論集 2 卷 189 頁以下(2006 年)
王郁琦「無線射頻辨識系統(ＲＦＩＤ)之應用對**隱私權**之影響」科技法律評論 4 卷 2 期 97 頁以下(2007 年)
王勁力「**電腦**網路**犯罪**偵查之數位證據探究」檢察新論 13 期 13 頁以下(2013 年)
王澤鑑『**人格権**法――法釋義學・比較法・案例研究』(自己出版，2012 年)

六画

朱石炎『**刑**事**訴**訟法論**(修**訂**二**版**)**』(三民，2009 年)
江舜明「**監聽**在刑事程序法上之**理論**與**實務**」法學叢刊 168 期 99 頁以下(1997 年)
江舜明「論**通訊**保障及**監察**法第三條之立法妥當性」法學叢刊 50 卷 3 期 101 頁以下(2005 年)

七画

李榮耕「**電磁紀錄**的搜索及扣押」臺大法學論叢 41 卷 3 期 1055 頁以下(2012 年)
李榮耕「**明確性原則**與機動性通訊監察」政大法學評論 126 期 105 頁以下(2012 年)

李鴻禧「**資訊**，憲法，**隱私權**」『憲法與人權(六版)』(台灣大學，1991 年)

李震山「從**憲法觀點**論身體不受傷害權」李建良・簡資修(編)『憲法解釋之理論與實務(第二輯)中央研究院中山人文社會科學研究所專書 48』497 頁以下(中研院，2000 年)

李震山「從公共場所或公眾得出入之場所普設**監視錄影**器論個人資料之保護」東吳法律學報 16 卷 2 期 45 頁以下(2004 年)

李震山「來者猶可追——正視**個人資料保護**問題」台灣本土法學 76 期 222 頁以下(2005 年)

李震山「**資訊權**——兼論監視錄影器設置之法律問題」『多元寬容與人權保障』193 頁以下(元照，2007 年)

李震山「論**資訊自決權**」『人性尊嚴與人權保障』219 頁以下(元照，2012 年)

李知遠『**刑**事**訴**訟法**釋論**(修訂 **3 版**)』(一品文化，2008 年)

李如霞老師工作室編著『新編**犯罪偵查**精粹含警察偵查犯罪手冊及特別刑法(２版)』(士明圖書，2011 年)

李建良「基本權利與國家**保護義務**」李建良・簡資修(編)『憲法解釋之理論與實務(第二輯)中央研究院中山人文社會科學研究所專書 48』325 頁以下(中研院，2000 年)

李建良「**人權維護者**的六十回顧與時代挑戰」廖福特(編)『憲法解釋之理論與實務(第六輯)中央研究院中山人文社會科學研究所專書 8』467 頁以下(中研院，2009 年)

李雅萍『**概括的權利**保障——德國基本法第二條第一項與我國憲法第二十二條之研究』(輔仁大學碩士論文，1995 年)

李惠宗「裁判書上網公開與個人**資訊自決權**的衝突」月旦法學雜誌 154 号 21 頁以下(2008 年)

李惠宗『**憲法**要義(**五版**)』(元照，2009 年)

吳秋宏『照相錄影於刑事程序之運用及容許性界限』(東吳大學**博**士**論**文，2011 年)＝**吳**秋宏『**照相錄影**與刑事程序』(自己出版，2012 年)

吳庚『**憲法**的解釋與適用**３版**』(三民，2004 年)

吳庚「社會**變遷**與**憲法**解釋」湯德宗(主編)『憲法解釋之理論與實務(四輯)中央研究院法律學院研究所籌備處專書(1)』１頁以下(中研院，2005 年)

吳兆琰「論**網路**環境下的**通訊監察**法制」科技法律透析 17 卷 2 期 36 頁以下(2005 年)

何賴傑(ほか＝林鈺雄＝陳運財)著『**刑**事**訴**訟法**實例**研究』(學林，2000 年)

巫聰昌『我國**勘驗法制**之研究』(東海大學碩士論文，2005 年)

八画

法務部保護司『**電腦犯罪**問題研討會實錄(第**４版**)』(法務通訊雜誌社，1993 年)

「刑事訴訟法**強制處分**部分條文**修正**研討會」臺灣法學 19 期 60 頁以下(2001 年)

周叔厚『**證據**法論』(三民書局，1995 年)

林俊益『**刑**事**訴**訟法**概論(上)11 版**』(新學林，2010 年)

林紀東『中華民國**憲法**逐條釋義**(一)**冊**８版**』(三民，1998 年)

林世宗「**隱私權**」全國律師 5 巻 4 期 33 頁以下(2001 年)

林永謀『**刑**事**訴**訟法**釋論(上)**改定版』(自己出版，2010 年)

林山田『刑事**程序法**(增訂**５版**)』（五南，2004 年）

林裕順『**基本人權**與司法改革』(新學林，2010 年)

林富郎『**通訊監察**法制化之研究』司法研究年報 21 輯 12 篇(司法院，2001 年)

林榮耀『**刑**事**訴**訟法**釋論**』(自己出版，1981 年)

林雅惠「**資訊隱私權**之重塑」科技法律評論 1 卷 1 期 93 頁以下(2006 年)

林鈺雄「逕行搜索與扣押之**合理依據**」台灣本土法學 28 期 104 頁以下(2001 年)

林鈺雄「**搜索修法**之回顧與前瞻(二)研究報告』臺灣法學 21 期 53 頁以下(2001 年)

林鈺雄「搜索及強制處分部分修建議條文(**乙案**)」臺灣法學 19 期 30 頁以下(2001 年)

林鈺雄『**搜索扣押**註釋書』(自己出版，2001 年)

林鈺雄「**干預保留**與門檻理論」政大法學評論 96 期 189 頁以下(2007 年)

林鈺雄『刑事訴訟法(上冊)總論篇』(自己出版，2007 年)

林鈺雄『**檢察官**論』(1999 年)

林鈺雄『**刑事程序**與國際人權(二)』(元照，2012 年)

林紀東『中華民國**憲法**逐條**釋義７版**』(三民，1993 年)

林三欽(他＝陳愛娥＝郭介恆＝陳春生**)**「**通訊監察**與秘密通訊之自由學術研討會」憲政時代 23 卷 2 期 4 頁以下(1997 年)

范姜真女微「企業內電子郵件之監看與員工**隱私權**」台灣本土法學 60 期 7 頁以下(2004 年)

李志仁「**電信**資訊匯流下之法律爭議——以 Skype 為例」科技法律透析 18 期 12 号 43 頁以下(2006 年)

范清銘「略談刑事搜索之證物**過度扣押**問題」刑事法雜誌 52 卷 5 期 1 頁以下(2007 年)

法治斌**＝董**保城『**憲法**新論**３版**』(元照，2008 年)

九画

洪俊義『警察執行**搜索・扣押**之**實務研究**』(輔仁大學碩士論文，2013 年)

柯耀程「**強制處分**基礎思維」月旦法學教室 76 期 88 頁以下(2009 年)

柯耀程『**刑事程序**理念與重建』(元照，2009 年)

柯耀程「**扣押問題**的定性與思辯」高大法學論叢 6 卷 2 期頁以下(2011 年)

柯慶賢「論**修正**之**搜索扣押(上)(下)**」法律評論 67 卷 4～6 期 2 頁以下／67 卷 7～9 期 2 頁以下(2001 年)

十画

「**搜索修法**之回顧與前瞻(一)研討會記錄」臺灣法學 20 期 109 頁以下(2001 年)

「**搜索修法**之回顧與前瞻**(二)**議題討論」臺灣法學 21 期 105 頁以下(2001 年)

翁岳生「**憲法解釋**與人民自由權利之保障」李建良・簡資修(編)『憲法解釋之理論與實務(第二輯)中央研究院中山人文社會科學研究所專書 48』1 頁以下(中研院，2000 年)

十一画

張耀中「**無線**網路溢波**盜用**之法律議題初探」科技法律透析 18 卷 9 期 16 頁以下(2006 年)

張國清「**隱私保護**概念的比較探討」全國律師 5 卷 6 期 4 頁以下(2001 年)

許文義『**個人資料保護**法論』(三民書局，2001 年)

許義寶「論**公共**場所**監視**器設置之法律程序(上)」法令月刊 57 卷 2 期 14 頁以下(2006 年)

陳新民『**憲法基本權**利之基本理論**(上)４版**』(三民，1996 年)

陳新民『中華民國**憲法釋論４版**』(三民，2002 年)

陳宏毅『追訴犯罪與**法本質**之研究』(鼎茂圖書，2003 年)

陳宏毅『**刑**事**訴**訟**法**理論與實務 3 版』(三民，2005 年)

陳慈陽『**憲法**學**２版**』(元照，2005 年)

陳河泉『**隱私權**在我國法制之規範現況與未來展望』全國律師 5 卷 6 期 21 頁以下(2001 年)

陳瑞仁「刑事訴訟法**改革**對案系列研討會之七——如何由法制面提升**警察**辦案品質」月旦法學雜誌 56 号 46 頁以下(2000 年)

陳瑞仁「搜索門檻『**相當理由**』之內涵」司法周刊 1038 期 2 頁以下(2001 年)

陳瑞仁「**新法**下**搜索扣押**之理論與實務」台灣本土法學 26 期 51 頁以下(2001 年)

陳正根「**警察資訊**作用之正確性」月旦法學雜誌 198 期 213 頁以下(2011 年)

陳樸生『**刑**事**訴**訟法實務**(重訂十版)**』(自己出版，1995 年)

陳運財「偵查之基本原則與**任意偵查**之界限」東海大学法學研究 9 期 281 頁以下(1955 年)

陳運財『刑事訴訟與**正當**之法律**程序**』(月旦，1998 年)

陳運財「**監聽**之性質及其法律規範」東海法學研究 13 期 137 頁以下(1998 年)

陳通和「論**情報自己決定權**與警察資料蒐集活動之法的統制」警政論叢 4 期 275 頁以下(2004 年)

陳志龍『檢察官之**偵查與檢察**制度(國科會專題研究)』(法務部，1998 年)

陳愛娥「**基本權**作為客觀法規範——以『組織與程序保障功能』為例檢討其衍生的問題——」李建良・簡資修(編)『憲法解釋之理論與實務(第二輯)中央研究院中山人文社會科學研究所專書 48』235 頁以下(中研院，2000 年)

黃清德**＝陳**斐鈴「公共場所**監視錄影**器設置與基本人權的關係——以資訊自決權為討論中心」警察學報第 3 卷 6 期 75 頁以下(2006 年)

黃清德「論警察利用**科技**方法**蒐集個**人**資**料與基本人權之保障」警專學報 4 卷 3 期 269 頁以下(2008 年)

黃清德「位置資料蒐集與基本人權保障以警察利用**衛星定位**系統 GPS 蒐集資料為探討中心」警專學報 4 卷 5 期 119 頁以下(2009 年)

黃翰義「論**緊急搜索**在我國刑事訴訟法上之適用」月旦法學雜誌 124 号 154 頁以下(2005 年)

黃東熊**＝吳**景芳『**刑**事**訴**訟**法論(上)**修訂 7 版**』(三民書局，2009 年)

黃東熊『**刑**事**訴**訟法論』(三民書局，1999 年)

黃朝義「**偵查**概念與原則」月旦法學教室 14 期 66 頁以下(2003 年)

黃朝義「**勘驗**與鑑定」月旦法學教室 12 期 74 頁以下(2003 年)

黃朝義『**刑**事**訴**訟法**(三版)**』(新學林，2013 年)

黃慧娟「設置防範監視器與**個人資料保護**」警學叢刊 40 卷 4 期 115 頁以下(2010 年)

許鴻基「**電磁記錄搜索扣押**之法制面建構——以美國法為中心」(文化大學碩士論文，2006 年)

許玉典『**憲法**』(元照，2008 年)

許志雄(他＝陳銘祥＝蔡茂寅＝周志宏＝蔡宗珍**)**『現代**憲法**論』(元照，2008 年)

許宗力「論**法律保留**原則」『法與國家權力(一)』頁以下(元照，2006 年)

張明貴『中華民國**憲法**新論』(商鼎文化，2002 年)

十二画

程明修「**資訊自決權**——遺傳基因訊息」法學講座 19 期 1 頁以下(2003 年)

傅美惠「**勘驗**之思與辯——我國勘驗法制之評析」刑事法雜誌 52 卷 5 期 105 頁以下(2008 年)

傅美惠『**偵查**法學』(元照，2012 年)

傅雅秀「**資訊隱私權**」書府 13 号 43 頁以下(1992 年)

褚劍鴻『**刑**事訴**訟**法論**(上**冊**)四**次修訂**版**』(2000 年)

曾正一『**偵查**法制專題研究』(元照，2007 年)

十四画

廖元豪「建構以**平等公民權**(Equal Citizenship)為基礎的憲法權利理論途徑——對傳統基本權理論之反省」廖福特(編)『憲法解釋之理論與實務(第六輯)中央研究院中山人文社會科學研究所專書 8』365 頁以下(中研院，2009 年)

蔡墩銘『**刑**事**訴**訟法論(**增訂五版**)』(2002 年)

蔡震榮**＝張**維平「**電腦犯罪**證據之研究」刑事法雜誌 44 卷 2 期 49 頁以下(2000 年)

蔡聖偉「**妨害秘密**罪章的新紀元**(上)(下)**」月旦法學雜誌 70 期 151 頁以下／71 期 96 頁以下(2001 年)

蔡宗珍「**人性尊嚴**之保障作為憲法基本原則」月旦法學雜誌 45 期 99 頁以下(1999 年)

蔡耕榮「I Am Linstening to you(上)釋字 631 號解釋，令狀原則及**修正後通訊**保障及監察法——」台灣本土法學 104 期 47 頁以下(2008 年)

十五画

鄧湘全「**通訊監察**之合憲性探討」月旦法學雜誌 40 期 102 頁以下(1998 年)

鄭玉波**(他**＝林紀東＝蔡墩銘＝邱聰智＝古登美＝蘇永欽**)**編『**新編六法**全書』(五南，2002 年)

劉靜怡「網路社會的**資訊隱私權**保護」二十一世紀 63 期 17 頁以下(2001 年)

潘兆娟「APEC 電子資料**隱私保護**原則與分析」政大智慧財產權評論 6 卷 2 期 95 頁以下(2008 年)

十七画

謝咏庭「**合理隱私期待**與搜索概念」（台灣大學碩士論文，2004 年）

十八画

簡彥匡「司法警察**搜索**票聲請**要件**之研究」（中央警察大學碩士論文，2004 年）

欧文文献・資料

Akhil Reed **Amar**, The Constitution and Criminal Procedure—First Principles（Yale University Press, New Haven and London, 1997）

Michael **Adler**， Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Searc,105 Yale L.J. 1093(1996)

RiOLG Dr. Wolfgang **Bär**；TK-Überwachung§§100a-101StPO mit Nebengesetzen Kommentar(Carl Heymanns Verlag, 2010)

Burkhard Schröder**＆Claudia** Schröder， Die Online-Durchsuchung Rechtlicht Grundlagen, Technik, Medienecho, Heise(2008)

Rolando V. Del **Carmen**, Criminal Procedure --Law and Practice, Wadsworth, 8th(2009)

Fourth Amendment Issues Raised by the FBI' **"Carnivore" Program**, Hearing before the Subcommittee on the Constitution of the committee on the Judiciary House of Representatives One Hundred Sixth Congress, Second Session, JULY 24, 2000, Serial No. 137(Prepared Statement of Donald M. Kerr, Lab Division, Federal Bureau of Investigation)

Eoghan **Casey**， Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet， Academic Pr; 2th(2004)

William R. **Casto**， Photostatic Copies and the Best Evidence Rule: Time for a Change，40 Tenn. L. Rev. 709, 1973。

Julie E. **Cohen**, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373 (2000)

Sherry F. **Colb,** CORRESPONDENCE: A WORLD WITHOUT PRIVACY: WHY PROPERTY DOES NOT DEFINE THE LIMITS OF THE RIGHT AGAINST UNREASONABLE SEARCHES AND SEIZURES, 102 Mich. L. Rev. 889(2004)

Craig Ball, Computer Forensics for Lawyers Who Can't Set the Clock on THeir VCR, in 6 ON FORENISICS(2005)

Darien A. McWhirter ＆ **Jon** D. Bible, PRIVACY AS A CONSTITUTIONAL RIGHT : SEX, DRUGS, and the

RIGHT to LIFE(QUORUM BOOKS, 1992)

Susan W. **Dean**, Government Surveillance of Internet communications: Pen Register and Trap and Trace Law Under the Patriot Act, 5 Tul. J. Tech. & Intell Prop. 97(2003)

Dorothy E. **Denning**, William E. **Baugh**, Jr., **ENCRYPTION AND EVOLVING TECHNOLOGIES** AS TOOLS OF ORGANIZED CRIME AND TERRORISM,May 15(1997)

(http://www.cs.georgetown.edu/~denning/crypto/oc-abs.html)

Dorothy E. **Denning** and William E. **Baugh**, Jr. **CASES INVOLVING ENCRYPTION** IN CRIME AND TERRORISM, Last Updated October 10, 1997 (http://www.cs.georgetown.edu/~denning/crypto/cases.html)

DOJ, Computer Crime & Interllectual Prop. Sec., Field Gruidance on New Authorities that Relate to computer Crime and Electronic Evidence Enacted in **the USA Patriot Act of 2001(Nov. 5, 2001)** available at http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm.

Dreier, in Dreier Hrsg., Grundrechte-Kommentar, Bd. I. Aufl., Art. 2.(2004)

Umberto **Eco**, **Zeichen**, Einführung in einen Begriff und seine Geschichte(Frankufurt, 1977)

Dr. jur. Ulrich **Eisenberg**, Beweisrecht der StPO Spezialkommentar,(Verlag C. H. Beck München, 2002)

A. L. Dipioetro, Anticipatory Search Warrants, **FBI** Law Enforcement **Bulletin**(July 1990)

Susan **Freiwald**, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 Ala. L. Rev. 9(2004)

M. -E. **Geis,** Der Kernbereich des Personlichkeitsrechts, JZ, S. 112(1991)

Marco **Gercke**, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007(S.250)

Corinne L. **Giacobbe**, Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data, 57 Wash & Lee L. Rev. 257(2000)

W. Schmitt **Glaeser**, Schutz der Privatsphäre, in J. Isensee/ P. Kirchhof（Hrsg.), Handbuch des Staatsrechts, Bd. VI, S.41(1989)

Dr. Jürgen P. **Graf**, StPO Kommentar(Verlag C.H. Beck München, 2010)

Dr. Jürgen P. **Graf**, **Internet**: Straftaten und Strafverfolgung(DriZ 1999)

Leon **Green**, The Right of Privacy, 27 ILL. L.Rev. 237(1932)

Statt vieler **Günter Dürig**, Art. 2 GG, in： Maunz／Dürig／Herzog／Scholz, Grundgesetz Kommentar(1990)

Rich **Haglund**, Comment, Applying Pen Register and Trap and Trace Devices to Internet Communications: As Technology Changes, Is Congress or the Supreme Court Best-Suited to Protect Fourth Amendment Expectations of Privacy?, 5 Vand. J. Ent. L. & Prac. 137, 145 (2003)

editor in chief, Kermit L. **Hall** ; editors, James W. Ely, Jr., Joel B. Grossman , The Oxford companion to the Supreme Court of the United States, Oxford University Press(2005)

LG **Hanau**, Beschlagnahme von E-Mails, NJW, S.3647(1999)

Hans—Carl Nipperdez, Freie Entfaltung der Persönlichkeit, in：Bettermann／Neumann／Nipperdez(Hrsg.) , Die Grundrechte ：Handbuch der Theorie und Praxis der GrundrechteⅣ, 2 . Band, .Halbband, 1962,

Hans Robert **Hansen**／Gustaf **Neumann**, Wirtschftinformatik 1—Grundlagen und Anwendungen. 9 Auflage(Stuttgart, 2005)

Heal **Hartzog**, THE“MAGIC LANTERN”REVEALED: A REPORT OF THE FBI’S NEW “KEY LOGGING”TROJAN AND ANALYSIS OF ITS POSSIBLE TREATMENT IN A DYNAMIC LEGAL LANDSCAPE, 20 J. Marshall J. Computer & Info. L.287(2002)

Hegmann, BeckOK StPO § 110 Rn 13 ～15(Beck Edition: 6, 2010)

Burkhard **Hirsch**, In dubio pro libertate ; Frederik Roggan(Hrsg.), Online-Durchsuchungen － Rechtliche und tatsächliche Konsequenzen des BverfG-Urteils vom 27. Februar 2008 , S. 9ff(BWV・BERLINER WISSENSCHAFIS-VERLAG, 2008)

BGH Manfred **Hofmann**, Die Online-Durchsuchung—staaliches „Hacken“ oder zulässige Ermittlungsmaßnahme? NstZ,S.121-125(2005)

Cerrit **Hornung**,Ein neues Grundrecht—Der verfassungsrechtliche Schutz der “Vertraulichkeit und Integrität informationstechnischer Systeme“, CR ,S.229(2008)

STEVEN P. SMITH ET AL., **IIT R**ESEARCH **I**NSTITUTE, INDEPENDENT REVIEW OF THE CARNIVORE SYSTEM -- FINAL REPORT A.2 (2000) [hereinafter **IITRI REPORT**], *available at* http://www.usdoj.gov/jmd/publications/ carniv_final.pdf (last visited May 5, 2004)

JIM KEOGH, THE ESSENTIAL HULDE TO COMPUTER HARDWARE 140(2002)

Sonia K. **Katyal**, The **New Surveillance**, 54 Case W. Res. 297(2003).

Sonia K. **Katyal, Privacy vs. Piracy,** 7 Yale J. L. & Tech. 222(2004 / 2005).

Orin S. **Kerr**, INTERNET SURVEILLANCE LAW AFTER THE USA PATRIOT ACT: THE **BIG BROTHER** THAT ISN'T, 97 Nw. U.L. Rev. 607(2003)

Orin S. **Kerr**, Lifting the **"Fog" of Internet Surveillance**: How a Suppression Remedy Would Change Computer Crime Law, 54 Hastings L.J. 805 (2003)

Orin S. **Kerr**, A User's **Guide to** the **S**tored **C**ommunications **A**ct, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208(2004)

Orin S. **Kerr**, THE FOURTH AMENDMENT AND NEW TECHNOLOGIES: **CONSTITUTIONAL MYTHS** AND THE CASE FOR CAUTION, 102 Mich. L. Rev. 801(2004)

Orin S. **Kerr**, CORRESPONDENCE: TECHNOLOGY, PRIVACY, AND THE COURTS: **A REPLY TO COLB AND SWIRE,** 102 Mich. L. Rev. 933(2004)

Orin S. **Kerr**, SEARCHES AND SEIZURES IN A **DIGITAL WORLD**, 119 Harv. L. Rev. 531(2005)

Orin S. **Kerr, DIGITAL EVIDENCE** AND THE NEWCRIMINAL PROCEDURE, 105 Colum. L. Rev.279(2005)

See Orin S. **Kerr** , THE COEXISTENCE OF PRIVACY AND SECURITY: CONGRESS, THE COURTS, AND NEW TECHNOLOGIES: **A RESPONSE TO PROFESSOR SOLOVE** , 74 Fordham L. Rev. 779(2005)

Tobias **Korge**, Die Beschlagnahme elektronisch gespricherter Daten bei privaten Trägern von Berufsgeheimnissen(Springer, 2009)

Kutscha: Verdeckte „Online-Durchsuchung“ und Unverletzlichkeit der Wohnung, NJW 2007 Heft 17, S.1169

Oliver **Lepsius** , Das Computer-Grundrecht : Herleitung-Funktion-Überzeugungskraft ; Frederik Roggan(Hrsg.), Online-Durchsuchungen － Rechtliche und tatsächliche Konsequenzen des BverfG-Urteils vom 27.

Februar 2008, S. 21ff(BWV・BERLINER WISSENSCHAFIS-VERLAG, 2008)

Lawrence **Lessig,** CODE version 2.0(Basic Books, New York, 2006)

E. Casey **Lide**, BALANCING THE BENEFITS AND PRIVACY CONCERNS OF MUNICIPAL BROADBAND APPLICATIONS11 N.Y.U. J. Legis. & Pub. Pol'y 467(2008)

David **Lyon**, Surveillance after september 11(Polity,2003)

Charles W. **Morris**, Grundlagen der **Zeichentheorie**(München 1972)

Charles W. **Morris**, **Zeichen**, Sprache und Verhalten(Düsseldorf ,1973)

Robert **Moore**, Cybercrime: Investigation High-Technology computer Crime (Matthew Bender & Company, Inc; 2005)

James **McClintick,** WEB-SURFING IN CHILLY WATERS: HOW THE PATRIOT ACT'S AMENDMENTS TO THE PEN REGISTER STATUTE BURDEN FREEDOM OF INQUIRY,13 Am. U.J. Gender Soc. Pol'y & L. 353(2005)

Jürgen **Müller**, Auswirkungen der unterschiedlichen Auffassungen zum Rechtscharakter der Art. 2 Abs. 1 GG und dessen Schranken, Diss. Münster(1970)

John Schwartz, Privacy Debate Focuses on F.B.I. Use of an Internet Wiretap, **N.Y. Times, Oct. 13, 2001, at A14.**

Paul **Ohm**, THE FOURTH AMENDMENT RIGHT TO DELETE, 119 Harv. L. Rev. F. 10(2005)

Stefanie **Olson,** Patriot Act Draws Privacy Concerns (Oct. 26, 2001) ("Part of the new legislation includes the expansion of Internet eavesdropping technology once known as Carnivore."), at http://news.com.com/2100-1023-275026.html.

Franz **Palm**, Rudolf **Roy,** Der BGH und der Zugriff auf Mailboxen, NJW 1997(S.1904)

Dr. Fredrik **Roggan**, Das neue BKA-Gesetz : Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, NJW 2009(S.259)

Roxin/Schünemann, Strafverfahrensrecht, 26. Auflage, verlag C.H. Beck München (2009)

Johannes **Rux**,Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden : Rechtsfragen der Online-Durchsuchung, JZ 6 ,S.285(2007)

Omar **Saleem**, THE PHYSICS OF FOURTH AMENDMENT PRIVACY RIGHTS, 32 T. Marshall L. Rev. 147,(2007)

Richard P. **Salgado**, FOURTH AMENDMENT SEARCH AND THE POWER OF THE HASH, 119 Harv. L. Rev. F. 38 (2006)

Sarah **Salter,** Storage and Privacy in the Cloud: Enduring Access to Ephemeral, Messages, 32 Hastings Comm. & Ent. L.J. 365(2010)

Pamela **Samuelson**, Privacy as Intellectual Property? 52 Stan. L. Rev. 1125 (2000)

W. **Schmidt,** Die Bedrohte Entscheidungsfreiheit, JZ, S.241(1974)

Schmidt/Seidel, Grundrechte, 2. Aufl. (2001)

Andrea **Schnabl**, Strafprozessualer Zugriff auf Computerdaten und die Cybercrime Konvention(Jura 2004)

Computer Crime and Intellectual Property Section, Criminal Division, U.S. Dep't of Justice, **Searching and Seizing Computers** and Obtaining Electronic Evidence in Criminal Investigations (2002)

Ulrich **Sieber**, **Informationsrecht** und Recht der Informationstechnik, NJW 1989(S. 2569)

Ulrich **Sieber**, Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichtsin dem Verfahren 1 BvR 370/07zum Thema der **Online-Durchsuchungen**(2008)

Graham B. **Smith**, NOTES AND COMMENTS: A CONSTITUTIONAL CRITIQUE OF CARNIVORE, FEDERAL LAW ENFORCEMENT'S NEWEST ELECTRONIC SURVEILLANCE STRATEGY,21 Loy. L.A. Ent. L. Rev. 481(2001)

Daniel J. **Solove**, Marc **Rotenberg**, Paul M. **Schwartz**, Privacy, information, and technology(Aspen Publishers, 2006)

Daniel J. **Solove**,THE COEXISTENCE OF **PRIVACY AND SECURITY**: FOURTH AMENDMENT CODIFICATION AND PROFESSOR KERR'S MISGUIDED CALL FOR JUDICIAL DEFERENCE,,74 Fordham L. Rev. 747(2005)

Daniel J. **Solove**, THE FUTURE OF **INTERNET SURVERVEILLANCE LAW** : a SYMPOSIUM TO DISCUSS INTERNET SURVEILLANCE, PRIVACY & THE USA PATRIOT ACT: SURVEILLANCE LAW : ,RESHAPING THE FRAMEWORK: Electronic surveillance law, 72 Geo. Wash. L. Rev. 1264 (2004)

Daniel J. **Solove**, **DIGITAL DOSSIERS** AND THE DISSIPATION OF FOURTH OF FOURTH AMENDMENT PRIVACY, Vol. 75（NO. 5）SOUTHERN CALIFORNIA L. Rev.531(2002)

Riichard **Stone,** The law of Entry, Search, and Seizure, 4th edition, OXFORD UNIVERSITY PRESS, 2004.

CASS R. **SUNSTEIN**, Infotopia /How Many Minds Produce Knowledge(OXFORD UNIVERSITY, 2006)

Peter P. **Swire**, KATZIS DEAD. LONG LIVE KATZ, 102 Mich. L. Rev. 904(2004)

K. **Vogelgesang**, Grundrecht auf informationelle Selbstbestimmung (Baden-Baden : Nomos Verlagsgesellschaft, 1987)

Warren, Samuel D. ;**Brandeis**, Louis D, THE RIGHT TO PRIVACY.,4 Harv. L. Rev. 193 (1890)

André **Weiß**, Online-Durchsuchungen im Strafverfahren(Verlag Dr. Kovač Hamburg, 2009)

Alan **Westin**, Privacy and freedom(Athenaeum New Yor,1967)

James Q. **Whitman**, The Two Western Cultures of Privacy : Dignity Versus Liberty, 113 Yale L.J. 1151（2004）

J. **Wintrich**, Die Problematik der Grundrechte (1957).

Raphael **Winick**, Searches and Seizures of Computers and Computer Data, 8 HARV. J. L. & TECH. 75 (1994)

Wiss. Assistent Stephan Schlegel (Aufsatz),"Online-Durchsuchung light" – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, HRRS Januar , S26(2008)

《 序 論 》

コンピュータの普及とコンピュータ・ネットワーク(とりわけ，インターネット)[1]の急速な拡大と共に[2]，コンピュータ・ネットワーク・システムは，現代社会のインフラとなりつつあり，それに伴い，情報技術(ＩＴ)を悪用する新型の犯罪――サイバー犯罪，ハイテク犯罪ないしコンピュータ・ネットワーク犯罪など[3]――を生み出すことになった[4]。それは，ＩＴ技術を多用する各国に共通する現象である。

その一例として，最近，日本において大きな話題となった，PC遠隔操作によるなりすましの犯行予告の書き込み事件を挙げることができる。同事件では，犯人が，ウイルス感染などの手法により他人のパソコンを遠隔操作し，感染したパソコンの持ち主４名が，被疑者として誤認逮捕された[5]。本件は，コンピュータ・ネットワーク犯罪の典型例といえるが，それに対する捜査手続においては，デジタル証拠の収集・保全の手続の困難さが示されることになった。

すなわち，まず，ＩＰアドレスが発信端末を割り出すための重要な手掛かりであるのは間違いないが，それだけで必ず発信端末を確定できるという保障はないし，また，PC遠隔操作などの可能性もあるから，ＩＴシステムにおいてなされた行為は，必ずしも発信端末ないしかかる端末の持ち主と関係があるものでもない。そのため，発信端末を割り出すだけで

---

[1] コンピュータ・ネットワークとは，複数のコンピュータを接続する技術，または，接続されたシステム全体を意味し，インターネットとは，TCP/IPというプロトコルを利用するコンピュータ・ネットワークの一種類である。そのほかに，デジタルテレビ放送システム，ATMシステム，クレジットカードショッピング決算システム，鉄道パスカードシステム，航空誘導システム・衛星GPSシステムなどが，そこに含まれる(アンドリュー17～18，39～40，53～76，504～526頁，石村＝堀部(編)・情報法[吉居]102～107頁，井上伸雄12頁など参照)。

[2] 日本の総務省「平成22年通信利用動向調査」によると，平成22年末までに，パソコンの個人利用率は67.4%となった。インターネットの利用者数(平成22年末まで)を見てみると，同「平成22年通信利用動向調査」によれば，「それは，平成21年末より54万人増加して9,462万人（対前年比0.6%増），人口普及率は78.2%（前年から0.2ポイント増）となった。また，個人がインターネットを利用する際に使用する端末については，モバイル端末での利用者が7,878万人（対前年比1.7%減），パソコンからの利用者は8,706万人（対前年比2.3%増）となった。そのうちに，インターネット利用端末の種類（平成22年末）につき，パソコンからの利用者は8,706万人(92.0%)となった。」とのことである。平成23年版『情報通信白書』186頁以下，堀部(編著)・インターネット[堀部]1～4，74～76頁も参照。

[3] ハイテク犯罪，サーバー犯罪，コンピュータ・ネットワーク犯罪などの用語のそれぞれの概念並びにその出処につき，指宿・サイバースペース84～85頁(同頁脚注5，6)，井上・コンピュータ(1)63頁注(18) ＝井上・強制・任意245頁注(18)，川出・コンピュータ犯罪21頁注(2)，安藤＝遠藤12頁，安富・コンピュータ犯罪7頁注(5)，安富・ハイテク犯罪10頁注(6)参照。他方で，台湾においては，コンピュータ犯罪などの用語についての一致した定義が存在しないが(法務部・電腦犯罪27頁。学説の整理については楊・電腦犯罪127 頁以下，蔡＝張・電腦犯罪51頁以下，王勁力・電腦犯罪14～17頁を参照)，台湾の内政部警察署の頒布した「警察の犯罪捜査のための手引き(警察偵査犯罪手冊)」(以下は「捜査手引き」と略称する)の222条は，「コンピュータ犯罪」を，「コンピュータ，ネットワーク及びその周辺の設備をその主な道具あるいは目的として利用し行う犯罪の行為」と定義している（法務部・電腦犯罪26～28，80～81，95～97，170～172頁をも参照)。また同文10～11頁は「コンピュータ犯罪」を，「全ての犯罪，調査あるいは起訴の過程においてコンピュータ技術の知識を必要とする不法行為」と定義しつつも(この定義が通説でもある。李茂生・電腦犯罪176 頁参照)，「コンピュータ犯罪は，その本質上は，その他の全ての犯罪と異なるものとして考えるべきではないのである。実際には，ほぼすべての犯罪の形態がコンピュータと関連する」と強調している。

[4] 井上・コンピュータ(1)50～51頁＝井上・強制・任意242～243頁，川出・コンピュータ犯罪1頁参照。

[5] http://news.livedoor.com/article/detail/7052676/(読売新聞 2012年10月17日14時33分)。

も大変な手間がかかるうえに，仮にそれを割り出したとしても，それだけでは真犯人を明らかにすることができない場合が多いのである。

他方で，遠隔操作のウイルスやプログラムの種類は豊富で，かつ，その入手も困難ではなく，また普通の素人であっても容易に操作できるという特徴があるうえに，役割を終えた遠隔操作のウイルスを素早く消去することも可能だと言われている[6]。

このように，コンピュータ・ネットワーク犯罪の事案では，デジタルデータが主な捜査の手がかりないし最終的な証拠となる点に特徴があり，そのデジタル証拠は，電磁的記録媒体と物理的に結合していないため，有体物たる記録媒体とは別に，無形のデータ自体を対象とする処分を想定しやすいし，また，その実際上の必要性もある，という指摘もなされている[7]。仮に，法律により，無体のデータ自体を対象とする強制処分が認められれば，オンラインで，遠隔操作のウイルスを消去されてしまう前に，デジタル証拠であるかかるウイルスを確保しておく法的な手段を講じることが可能になるし，真犯人を割り出すために，端末を対象とするオンラインでの追跡のみならず，無体の情報である「遠隔操作の痕跡」（オンラインで発信端末に辿り着いたルート）自体を強制処分の対象としたうえで，それを解明し，証拠化することもできる。

以上に示した「デジタル証拠の収集・保全の手続」を巡る問題については，既に国際的な対応がなされている。それが， 2001 年 11 月 8 日に，欧州評議会閣僚委員会会合で正式採択されたサイバー犯罪に関する条約である[8]。同条約は，同年 11 月 23 日に開催された署名式典で各国に開放され，日本も署名した。同条約の国内法化に向けた法整備として，2011 年に，ＩＴの発展に対応するための捜査手続の整備などを盛り込んだ「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（以下，「改正法」という）が成立した[9]。

他方，台湾でも，無線ネットの盗用によるなりすましなどのコンピュータ・ネットワーク犯罪への手続上の対応に関わる問題が生じている[10]。それに対する法的対応としては，

---

[6] http://www.asahi.com/national/update/1011/OSK201210110070.html（朝日新聞デジタ 2012／10／11／15 時 42 分）：「遠隔操作ウイルスに感染した大阪と三重の男性のパソコン（PC）からネット上に犯行予告が書き込まれた事件で，大阪の男性の PC に感染していた遠隔操作ウイルスが，犯行予告メールを送信した直後に PC 上から消えていたことがわかった。大阪府警は，ウイルス検知の危険性を避けるため，発信者が役割を終えたウイルスを素早く消去した疑いがあるとみている。」

[7] 川出・コンピュータ犯罪 1～2 頁。

[8] Convention on Cybercrime (ETS no. 185, Budapest, 23 XI. 2001), I. L. M., vol. 41, 2001, p.282. また，欧州評議会の設置並びにサイバー犯罪に関する条約の採択についての邦文での簡要な説明につき，堀部(編著)・インターネット[岩隈]233～234 頁を参照。

[9] 2003 年に，サイバー犯罪条約の署名を受けて，法務大臣から法制審議会に対して，「ハイテク犯罪に対処するための刑事法の整備に関する諮問」（諮問第 63 号）(法務省ホームページ http://www.moj.go.jp/shingi1/shingi_030324-2.html 参照)がなされ，刑事法部会での審議を経た後，「ハイテク犯罪に対処するための刑事法の整備に関する要綱(骨子)」の答申がなされた(法務省ホームページ http://www.moj.go.jp/shingi1/shingi_030910-5.html。北村・ハイテク犯罪 6 頁をも参照)。その後，2004 年に，同答申に基づき，「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」（http://www.shugiin.go.jp/itdb_gian.nsf/html/gian/honbun/houan/g16305022.htm 参照)が，国会に提出された。2011 年に成立した改正法は，ハイテク犯罪関係の法整備については，上記法律案とほぼ同じ内容であるが，若干の修正が加えられている。改正法の成立の経緯については，指宿・サイバースペース 84～85 頁参照。

[10] 2004 年に起きた，クレジットカードの不正利用などの目的で，有効なセキュリティが設定されていない他人無線ネッ

2001 年に行われた刑訴法の改正をあげることができる。同改正により，「電磁紀錄」(以下では，日本語に対応させて「電磁的記録」とする)という文言が，捜索・差押えの対象として，旧来の条文(台湾の刑事訴訟法 122 条 1 項と同条 2 項[11]。以下では，台湾刑訴法〇条〇項と略称する)に追加された。

しかし，2001 年の台湾刑訴法改正の主たる目的は，日独米の制度を参考に，日本でいう令状主義を導入すること，すなわち，過去には検察官が持っていた捜索(差押え)令状[12]の発付権限を剥奪し，中立の裁判官しか捜索令状を発付することができないという制度に代える点にあり，立法の背景[13]ないし審議当時の議論については，「コンピュータ・ネットワーク犯罪と手続上の対応」というテーマとは，全く関係ないものであった。

実際にも，上記の「電磁的記録」という文言の条文への追加は，最後の三読会[14]において唐突になされたものであって[15]，その追加の経緯ないし理由が一体何であったのかについても，当時の審議記録には何も残されていない[16]。ただし，その後，2001 年の改正刑訴法に合わせて，同年 4 月に軍事審判法(軍審法)が改正されることになり，その改正案の 1 つであ

トを盗用したケースにおいて，警察はＩＰアドレスを追跡したが，結局，なりすましの被害者，すなわち，無線ネットの加入名義者の身元しか特定できなかった(張・無線盗用 17，19 頁)。これに対して，台湾の行政院(日本の内閣府に該当する機関)は，個々の端末器機における識別番号であるMACアドレス(Media Access Control address)が唯一性を持つことを理由に，それを人間の指紋にたとえ，この番号さえ掌握しておくことができれば，上記の無線ネットの盗用によるなりすましの捜査の難点を克服することができると提言していた(2005 年 4 月 20 日に行政院國家資通安全會報の主催した「2005 年無線網路安權策略座談會」；また張・無線盗用 19～20 頁をも参照)。しかし，前述した日本のコンピュータの遠隔操作によるなりすましの場合には，このMACアドレスを確保しておいたとしても意味はない。というのも，警察が追跡・確保しておくことが可能なのは，通常は，真犯人により遠隔操作された被害者の所有する端末のMACアドレスだけだからである。

[11] 同条 1 項は，「被告人あるいは犯罪嫌疑者の身体，物件，電磁的記録及び住宅あるいはその他の場所に対して，必要があるとき，それを捜索することができる」と，同条 2 項は，「第三者の身体，物件，電磁的記録及び住宅あるいはその他の場所に対して，被告人もしくは犯罪嫌疑者または差し押さえるべき物もしくは電磁的記録が存在すると信じられる相当の理由があるときであるかぎり，それを捜索することができる」と定めている。

[12] 台湾では，日本と異なり，独立した差押え令状が存在しておらず，差し押さえるべき物が，捜索令状に記載されるという形になっている(台湾刑訴法 128 条 1 項。そして，黄＝呉・刑訴法論(上)7 版 196，206 頁，林永謀・刑訴釋論(上)433 頁をも参照)。

[13] 2001 年の台湾の法改正のきっかけとなったのは，2000 年 8 月 16 日に台南地検(台南地方裁判所に配置された検察署)の検察官(黄朝貴)が，国会議員の廖福本の研究室を捜索したことであるとされる。さらに，当時国家安全局の官員である劉冠軍の汚職事件に端を発した秘密漏洩罪に関わる事案を捜査するため，検察が同年 10 月 3 日(中国時報系が成立した 50 周年の翌日)に中時晩報(中国時報系の傘下の新聞社であって夕刊を担当する)を捜索したが，それが，新聞業界における権力者である余紀忠を怒らせ，中国時報系が「捜索権限を裁判所に帰せ！」というスローガンを打ち出して裁判所の発付する令状による捜索という制度を構築すべきと強く主張したことが，この法改正の動きを成熟させた最も重要な推進力になったとされる。以上につき，強制處分修正 66 頁の林鈺雄の発言，林山田・程序法５版 339 頁及び同頁注 59 を参照。

[14] 台湾の立法は，草案を国会に上程し，一読会，二読会，三読会という３回の審議の過程にわたる必要があり，三読会により法律案が成立し，大統領が成立した法律を公布することにより，当該法案が正式発効するという形になっている。2001 年の法改正は，一読会を省略して，直ちに，二読会に進み，まもなく，三読会に入り，極めて迅速かつ異例なスピード(立法関係者の発言によると，多くの条文は三読会の夕方からはじめて協議し，当日の夜にただちに通過させ，かかった総時間はわずか６時間しかないものであった)で通過させたものである(捜索修法 109 頁以下陳瑞仁の発言。また，林山田・程序法５版 339 頁，林鈺雄・捜索修法 55 頁の説明をも参照)。

[15] 三読会以前各政党に提出された個々の修正の草案には，「電磁紀錄」という文字はなかったのである(立法院公報 90 卷 5 期 200 頁以下参照)。

[16] 立法院公報 90 卷 5 期 303 頁以下参照。

る李慶雄(台湾の国会議員)の提出した草案における説明の別紙である「刑事訴訟法部分修正新旧条文対照及び説明」[17]では，「電磁的記録」という文字の追加に関して，次のような立法参考理由をあげている。

「最近のコンピュータ及びネットワーク科学技術の発達により，コンピュータ・ネットワークの伝送は，常に犯罪の道具として使われるから，もし電磁的記録に対して捜索することができないと，ある新型の犯罪の捜査に必ず困難が起こることとなるがゆえに，電磁的記録をも捜索の客体として列挙することにし，これをもって概括できようにする。」[18]

しかしながら，電磁的記録という文字の追加をするだけで，果たして，問題の解決に向けて，電磁的記録に対する捜査の文脈のもとにおけるあらゆる場面を概括することができるかについては，大きな疑問がある。すなわち，2001 年の法改正以前に，電磁的記録を捜査の対象とする場合に如何なる問題が提起されてきたかをいえば，次の５つのものにまとめられる[19]。①高機能のコンピュータ・ネットワークからなる高度化・複雑化するＩＴシステムのスペースは極めて広汎であるため，現在の捜査技術では，効率かつ有効的にこのスペースを探索したりその中に存在した標的となるデータを割り出したりすることは，山の中にある１本の細い針を見つけようとするような極めて困難な作業である。②かようなＩＴシステムに対する捜索を，捜査官でなく，鑑定人としてのコンピュータアナリストに任せることができるか。③コンピュータ操作やＩＴセキュリティ解除との関係で，対象となる電磁的記録を割り出したりするためには被処分者の協力を必要とする場面が少なくないが，かような協力を得られない場合，どう対応すればよいか。④コンピュータ操作を被処分者に任せると，証拠隠滅・改ざんの恐れがあるから望ましくはないものの，技術上の理由で，かかる操作を被処分者に任せざるを得ない場合，どのように証拠を保全するか。⑤対象となる電磁的記録を記録した媒体全体を差し押えると，同媒体に蔵置された膨大な対象でないデータも捜査機関に取られてしまう点がプライバシーへの厳重な侵害となるから妥当でない[20]。

このうち，電磁的記録をも捜索・差押えの対象として列挙している現行法のもとにおいても，過去と同様に，対象となる電磁的記録を記録した媒体を丸ごと差押えることができるから，⑤の問題点は今でも未解決のままである。①～④の４つの問題点に関しては，電磁的記録という文字の追加により解決されるものではないことは明らかである。

---

[17] 原文用語は,「刑事訴訟法部分修正新舊條文對照暨説明」である。これは法務部が国会議員の協商により通過された版を参照し整理したものであって，2001 年刑訴法改正の正式的な立法理由ではないのである。

[18] 立法院第四届第五會期司法委員會第五次全體委員會會議(2001 年 4 月 23 日)の資料，林鈺雄・捜索扣押 330 頁の附録１に収録されている。

[19] 法務部・電脳犯罪４版 55 頁以下，林合民・電脳資訊捜索扣押 41 頁以下をも参照。

[20] この点に関して，前注の林合民論文 46～47 頁は，「……わが国刑事訴訟法の捜索・差押えに関する規定は完全ではなく，実務上は捜索・差押えを行う際に，捜索令状の記載はあまりにも簡略すぎるし，また，検察・警察がコンピュータに対する知識が足りず，先例あるいは規定を欠いているから，適切な程度を超えた過度の捜索・差押えが行われる場合が稀でなく，それにより人権の侵害となるかについての争いを引き起こしている。」と指摘し，「法務部が，アメリカ司法部の頒布した『連邦コンピュータの捜索及び差押えの準則』(1994 / Federal Guidelines for searching and Seizing Computers)を参考に，わが国の関連する規定及び裁判所の事例に合わせて，わが国の検察・警察が従える準則を用意することにより，検察・警察がコンピュータ及び情報に対する捜索・差押えを行う際に，もっと効率的となり，かつ，人権の保障にも資する」と提案する。

そればかりか，電磁的記録という文字の追加は，解釈論上の新たな問題点を引き起こしている。そのうち，もっとも重要な争点は，2001 年の法改正以後，果たして，無体の電磁的記録自体が，現行法の差押えの対象となっているのかである。この点，台湾刑訴法 122 条 2 項に定められた「差し押さえるべき物もしくは電磁的記録」という法的用語については，文言上は２つの読み方が考えられる。その１つは，「差し押えるべき物」もしくは「電磁的記録」という読み方，もう１つは，「差し押えるべき物」もしくは「差し押えるべき電磁的記録」という読み方である。前者の理解であれば，電磁的記録は捜索の対象だけであって，差押えの対象にはなっていないことになるし，後者の理解であれば，差押えの対象でもあることになる。立法者が考えていたのは，一体どちらであるかは不明である。先行研究においても，2001 年の法改正は単に電磁的記録という文字を追加しただけであり，捜索・差押えの対象は，一体，電磁的記録それ自体であるか，それとも，電磁的記録を記録した媒体であるかについては，依然として曖昧不明であり，明らかにされていないと指摘されている[21]。

この点につき，学説は分かれている。一方で，仮に，電磁的記録という文言が有体の電磁的記録媒体をさすものであるとすれば，かような追加は意味を失ってしまうことを理由に，2001 年の法改正により無体の電磁的記録も差押えの対象となっているとする見解がある[22]。他方で，2001 年の法改正により，捜索の客体には無体物が含まれることになったが，刑訴法はそれを差押えの対象としてはないとする見解もある[23]。

この問題の核心は， 2001 年の法改正は電磁的記録をも差押えの対象として列挙しているが，電磁的記録には占有の剥奪を観念することができないという点にある。というのも，占有の剥奪を観念できない電磁的記録を差押えの客体としているように見える 2001 年の刑訴法の改正と，占有の剥奪という従来の差押えの定義との間には齟齬があるからである。

以上のとおり，無体の情報を対象とする新しい立法論を構築するためにはもちろんのこと，現行法の解釈論としても，占有の剥奪という観念がありえない電磁的記録を対象とする場合に相応しい新たな差押えの定義を改めて探求することが必要となる。ここでの問題の核心は，如何なる条件をもって，占有の剥奪を観念できない電磁的記録という無体の情報が差し押さえられるといえるかという点にある。具体的には，有体物を対象とする場合には，差押えにより侵害される法益は財産権であり，その法益侵害の態様は有体物に対する占有の剥奪となるのに対して，無体の情報は必ずしも財産権にかかわるものでないし，また，財産権にかかわる情報であれ，そうでない情報であれ，それらのいずれに対しても占有の剥奪をすることが不可能であるから，情報が差し押さえられることによって一体如

---

[21] 李・電磁紀錄 1057～1058 頁。

[22] 林鈺雄・刑訴(上)353 頁，簡・捜索要件 30 頁，柯慶賢・修正捜索扣押(上)7 頁，王勁力・電腦犯罪 17 頁などを参照など参照。また，2001 年法改正以前にも，アメリカ法の状況を参考に，台湾の場合にも，無体の情報をも捜索・差押えの標的であると解する論者がある(林合民・電腦捜索扣押 44 頁)。

[23] 黄朝義・刑訴三版 234～235 頁参照。前述した「刑事訴訟法部分修正新旧条文対照及び説明」における立法参考理由においても，「電磁的記録をも捜索の客体として追って列挙する……」と述べているだけであり，電磁的記録は差押えの対象であるかどうかという点を言及していないのである。

何なる法益が侵害されるのか，及びこうした場合の法益侵害の態様は如何なるものとなるか，という２つの点を明らかにしておかなければならない。

これらの問題点を検討するためには，台湾における関連する判例や学説は乏しいから，外国の議論を参考にする必要がある。そこで，以下では，日本と並んで，「コンピュータ・ネットワークと捜査手続」というテーマについての豊富な研究の蓄積があるドイツとアメリカにおける関連議論をもとりいれた比較法的研究アプローチを採用し，下掲の２つの問題に取り組むことにしたい。

第１は，コンピュータ・ネットワークの発達によって刑事手続上生じてきた，あるいは，これから生じうる問題点は何なのかである。この点，前述したとおり，台湾における議論は不十分であるので，以下で，まずは，本稿の主な比較法的研究の考察素材である日本における問題状況を考察し，そのうえで，台湾の立法論として解決すべき問題を洗い出す。それにより，2001 年の法改正により追加された「電磁的記録」という法文の解釈に資する示唆を得ることも期待できよう。具体的には，次の３つの点を検討課題とする。

①日本においては，ＩＴ技術の発展に伴い生じた，情報を処分の対象とする場面において解決すべきとされる捜査上の諸課題につき，これまでいかなる問題点が指摘され，検討されてきたか。そして，これらの指摘・検討から，台湾にとって，如何なる有益な示唆が提供されるか。

②それぞれの問題点に対して，これまではいかなる対応がなされてきたか。また，日本で今回の改正法が成立した後，これまでの対応にいかなる変化が生じているか。そのうえで，仮に，この改正法を台湾に導入した場合，台湾のこれまでの問題状況は如何に変わりうるか。

③改正法を含めた日本の現行法の下で，なお解決されていない問題点は何であるのか。これらの問題点は，台湾の場合にもあてはまるものなのか。

そのうえで，第２に，第１の問題の検討より洗い出した台湾の立法論として解決すべき問題点に対応するために必要な解決策を探ってみたい。すなわち，本稿は，日本法の問題状況を踏まえて，ドイツとアメリカにおける関連議論を採り入れつつ，問題の所在を改めて再検討しながら，日独米の三カ国を素材にした比較法的考察により得られた台湾の解釈論及び立法論に資する示唆を抽出し，それに基づいて，有体物と並んで，無形の情報をも独立した強制処分の直接の対象とする捜査手続を規制するためにあるべき新制度を構築しようとするものである。

以上の枠組みに従って，具体的に検討すべき内容は，(1)「蔵置されたデータと捜査手続」，及び(2)「伝送中のデータと捜査手続」という２つのカテゴリに区分される。この区分を必要とする理由は，次の点にある。すなわち，ここでの主な比較素材である日本の改正法は，サイバー犯罪に関する条約の趣旨に沿って制定されたものであるとされているが，「伝送中のデータ」を対象とする部分については，既存の通信傍受という処分の枠内にあると考えられたため，条約上の「データ」という用語は使わず，それより狭い意味での「電磁的

記録」という用語を採用している。つまり，日本の改正法は，「蔵置されたデータ」のみを対象としたものなのであり，したがって，台湾との比較上も，「蔵置されたデータ」と「伝送中のデータ」とに分けて検討するのが妥当だと考えるからである[24]。

そこで，以下では，まず，第１章において，「蔵置されたデータと捜査手続」を，次に，第２章において，「伝送中のデータと捜査手続」を検討し，最後の第３章において，「新制度の内容」を敷衍し，本研究の結論を示すものとする。

[24] 学説上は，電磁的記録，データ，情報という３つの概念が厳密に区別されることなく，ほとんど同義語として使われる場合が少なくない(例えば，黄清德・衛星定位 120 頁脚注 2，渡辺脩 7 頁，米澤(編)・刑法改正解説[的場＝河村]70 頁注(3)など参照)。これに対して，日本の改正法の審議過程では，「情報」を「一定の観念」と，「データ」を「一定の観念を表現するデジタルのあらゆる形式」と，「電磁的記録」を「一定の観念を表現するデジタルの保存の形式(すなわち，蔵置されたデータ)」とされている(審議会(ハイテク)第 3 回議事録参照)。この部分は，主に実体法の場面でなされた定義であるが，同法律案で提案された手続法も同じ定義を採用していると考えられる。これに対して，台湾における電磁的記録の意味を説明すると，まず，台湾の刑法 10 条 6 項は，「電磁的記録とは，電子，磁気，光学あるいはその他の類似する方式により作られ，電子計算機の処理に供せる記録を意味する」と定められている。また，最高法院 81 年度第 11 次刑事庭會議決議は「電磁紀錄物とは，永続する状態中，磁気テープやフロッピーティスクなどの媒体上の意思あるいは観念を意味する」とする。こうして，台湾でいう電磁的記録も，前掲した日本のいう「一定の観念を表現するデジタルの保存の形式」をさすものと考えてよい。

第１章　蔵置されたデータと捜査手続

日本の今般の改正法成立前の，蔵置されたデータと捜査手続をめぐる問題の核心は，データを保全・取得するためにはいかなる手段によるべきかという点にあった。というのも，無体のデータのみを保全・取得するためには，有体物のみを対象とする捜索・差押えなどの既存の処分だけでは十分に対応できないという点が，捜査実務の大きな問題とされてきたからである[25]。この点は，台湾においても同様に問題となっている。

この問題を解決するために可能な対応策を，令状による規制を基準に分類すると，①令状による直接強制処分，②令状による間接強制処分，③令状によらない直接強制処分，④令状によらない間接強制処分，の４つのものとなろう[26]。このうち，本研究は，以下の理由で，①を検討対象とする。

まず，すでに指摘したとおり，台湾の刑事手続における強制処分は，その運用について相当な混乱状況を呈しているため，強制処分の制度を改めて徹底的に検討することが，刑事手続法制及び実務の重要課題となっているとされる[27]。とりわけ，令状による直接強制処分についての抜本的な検討は，もっとも根本的かつ重要なものであると考えられる。というのも，2001年の法改正により，台湾においても捜査機関が強制処分を行うには令状によるべきものという原則がとられたからである。

また，前述した，デジタル証拠のみを収集・保全することが必要な場合に，既存の処分だけでそれに対応することは困難であるという点については，日本においても，改正法が成立したことにより問題が完全に解決されたとはいえない。なぜなら，後の検討で明らかにするように，改正法は，有体物のみを対象とする現行法の枠組みを維持しているし，また，「蔵置されたデータを保全・取得する」という場面における問題点にしか対応していないものだからである。この点からも，令状による直接強制処分という制度の在り方を改めて再検討する必要があるということができる。

他方，捜査機関は，被処分者ないし事件に精通していると思われる者の協力が得られないと，無体のデータなどの客観的な証拠を保全したり取得したりすることができない場面が多くなってきている。これに応じて，日本の学説上は，間接強制処分の新設による立法

---

[25] 審議会（ハイテク）第２回議事録（立法当局の説明）参照。岩田・コンピュータ関連犯罪（捜査手続）194～200 頁，井上・コンピュータ(2)53～54 頁，指宿・サイバースペース 88 頁，夏井 203 頁をも参照。

[26] ここでいう直接強制処分とは，捜査機関が，被処分者の明示ないし黙示的な意思に反して，法に付与される権限をもって自ら捜査の目的を実現することができる処分を指す。たとえば，捜索・差押えという制度がその例としてあげられる。これに対して，間接強制処分とは，捜査機関が自ら捜査の目的を実現することができるのではなく，捜査の目的を実現するために必要な協力の要請に応じない被処分者には罰則などの法的な不利益を与えることにより，捜査の目的を実現することができるように協力をさせる処分を意味する。台湾においても日本においても，現行法上はかような制度は用意されていない。

[27] 柯・刑事程序 180～181 頁。というのも，台湾において，現行法上，強制処分の権限の配分は妥当ではないため，具体的な適用上の在り方を捉まりかねる一方，学理的な研究も足りないに加え，実務的操作上も恣意的な解釈がなされてきているため，強制処分の具体的な運用はすでに常軌から離れているし，また，立法上は刑事手続における強制処分の根本的な意味を理解しておらず，不適切な規定がなされてきているからである（柯・同文同頁参照）。

的な対応が望ましいという提案も一部でなされている[28]。この提案は台湾にも参考となるものがあると思われるが，しかし，被処分者が処罰を甘受し，協力を拒否する場合には，やはり，直接強制処分による対応が必要となる。そして，そのうえで，直接強制処分たる差押えをもって媒体の占有を剥奪したからといって，媒体に施されたＩＴセキュリティなどによる支障がそれによって排除されるわけはないのである。それゆえ，これらの問題に対応するためには，既存の令状による直接強制処分という制度を見直すことが必要となろう。

以上の通り，今後は，有体物と並んで，データなどの無体の情報も含んだ意味での客観的な証拠を保全・取得するための法的手段の在り方を改めて検討しなければならないのであり，その中でも，①の令状による直接強制処分に関わる制度の見直しと整備が，もっとも重要な課題であるといえよう。

そこで，以下では，まず，今回の改正の対象となった「蔵置されたデータの保全・取得」に関わる問題から議論を展開していきたい。その際に，改正法の記録命令付差押え(日本の刑事訴訟法99条の2；以下，日本刑訴法○条○項と略称する)並びに協力・保全要請(同111条の2，197条3項)などの規定については，問題状況を明らかにするに必要な限度で言及するに留める。というのも，これらは，いずれも間接処分に属するものであり，本稿の検討においては副次的なものにすぎないからである。

第１節　プロバイダーに対する情報保全・開示の要請

第１款　直接強制処分という制度の不備とその対応

前述したとおり，今回新設された協力・保全要請(日本刑訴法111条の2，197条3項)という制度は間接処分にあたるものであるが，ここで検討すべきは，かかる制度と，本稿の研究課題である令状による直接強制処分との間に如何なる関係があるかである。この点については，既存の令状による直接強制処分には不備があると指摘されてきたから，その対応策として協力・保全要請などの間接処分という新制度が導入されたとされている。そこから，次の３点が検討対象となる。すなわち，①令状による直接強制処分という制度には如何なる不備があるか，②かかる不備を補うために，なぜ，今回新設された協力・保全要請というような間接処分の制度を新たに導入する必要があるのか，③かような間接処分の導入によって，果たして，既存の直接強制処分における問題点を抜本的に解決することができるのかである。

以上の３点を具体的に検討するために，以下では，プロバイダーなどの通信業者が被処分者である場面を中心に，具体例をあげて検討を進めていきたい。なぜならば，今回新設

[28] 酒巻・提出命令 125 頁以下参照。

された協力・保全要請の規定は，主に，プロバイダー[29]などの通信業者が被処分者となる場合を想定しているからである。具体例は，以下のようなものである。

【例 1】麻薬密輸捜査事件

マレーシアから入国した日本国籍の男性Aが，ヘロイン約982グラム（末端価格およそ5,900万円）を隠し持っているのが税関検査で発見され，関税法並びに麻薬及び向精神薬取締法違反で現行犯逮捕された。

Aは，捜査官の取調べを受け，「『ただで海外旅行に行けるし，お金ももらえるから，なかなかお得な仕事でしょう……』と言葉巧みに誘われてやってしまったが，貨物の中身がヘロインである可能性を全く認識していなかった。何も知らないうちに運び屋に仕立てられてしまった。また，貨物の提供者が誰なのかも全く知らない。これまでは，『Mark@docoxx.ne.jp』というメールアドレスを使っている，面識のないマークと呼ぶ人物とメールでやり取りをしており，指示を受けながら行動していただけである。」と供述した。

以上のような前提で，日本において，本件の捜査がどのような展開をたどるかを考えてみよう。まず，Aの上記供述により，マークという人物がヘロインの卸元である疑いが強いため，マークの身元を突き止めるのが，本件捜査の第一歩となるであろう。そこで，捜査機関は，まず，任意捜査の一環として，「docoxx.ne.jp」というドメイン名[30]が示す，docoというプロバイダーに対して，「Mark」というアドレス名を使用している加入者の身元情報及び「Mark@docoxx.ne.jp」の通信履歴[31]の提供を要求する捜査関係事項照会(日本刑訴法第197条2項)を行った[32]。ここで問題となるのは，doco社は，こうした捜査関係事項照会に任意に応じることができるかである。

この点，通信の秘密とは，通信に関する事項の私生活の秘密を指すから，通信の内容はもちろん，そうでないものも，それが私生活の秘密である限り，例えば，通信の履歴についても，通信の秘密にあたるとする立場が通説である[33]。他方で，個々の通信とは切り離さ

---

[29] 正式名称は，「インターネット･サービス･プロバイダー」(Internet Service Provlder)であるが，一般には，ISPと略称され，通信業界では，単に「プロバイダー」と呼ばれることが多いが，「商業プロバイダー」とも呼ばれる(大橋・基礎編7頁，松沢・通信ログ55頁，60頁参照)。

[30] ドメイン名の登録者などに関する情報を，誰でも参照できるサービス「WHOIS」（フーイズ）を利用すれば，「doco」というプロバイダーの連絡先を手に入れることができる。「WHOIS」とは，インターネット上でのドメイン名・IPアドレス・Autonomous System（AS）番号の所有者を検索するためのプロトコルであり，それが，ドメイン登録情報の管理を行う組織(レジストリ)またはドメイン登録の仲介を行う組織(レジストラ)より提供されているものである(ウィキペディア―サーチワード：WHOIS〈フーイズ〉参照)。

[31] 通信履歴は通信ログの同義語として使われている(松沢・通信ログ55頁)。また，通信ログの種類として，主に，①接続ログ，②課金ログ，③メール送受信記録，④HP更新・閲覧記録などのものが挙げられる(松沢・通信ログ57頁)。

[32] こうした捜査の流れは，日本の実務の慣行になっているようである。この点についての詳細は，審議会(ハイテク)第2回議事録(ニフティからの参考人の陳述)参照。

[33] 佐藤・憲法(3版)576頁，山内7頁，井上・強制・任意207～208，254頁，宮澤・憲法(コメ)248～249頁，宮沢・憲法Ⅱ[旧版]373頁，佐藤・通信の秘密641頁，佐藤・憲法(3版)576頁，野中ほか・憲法Ⅰ(5版)［中村]397頁，電気通信法制研究会23頁，高橋正俊104頁，電気通信事業における個人情報保護研究会35頁，中村385頁，大阪高判昭和41年2月26日高刑集19巻1号58頁，美濃部380～381頁，松井・インターネット291頁，平松・通信の秘密67頁，三井・手続法(1)[新版]57頁，審議会(ハイテク)第7回議事録，杉山＝吉田・情報処理の高度化(下)113頁，木村・情報政策190頁など参照。

れた形での加入者の氏名，住所等は，通信の秘密には含まれないものとされてきた[34]。平成23年に改定された「電気通信事業における個人情報保護に関するガイドライン」の解説においても，「加入者の氏名，住所，生年月日等の当該加入者に関する情報……は，メール内容，送信相手，送信日時，送受信場所，送信回数等の事実に関わるものではなく，個別のメール送信に係る情報ではないため，通信の秘密に属する情報には当たらないと解される」[35]とされている。以上によれば，プロバイダーは，捜査関係事項照会に任意に応じて，通信の秘密にあたらない「Mark」という加入者の身元情報を捜査機関に提供することができるという結論が導かれる。

これに対して，通信事業者が，通信の秘密にあたる特定された個別のメール送信に係る送信者情報，すなわち「Mark@docoxx.ne.jp」の通信履歴を，捜査機関に任意に提供できるかは疑問がある。通信の秘密の保護という観点からすると，doco社が前掲した捜査関係事項照会に任意に応じて，通信の秘密にあたる「Mark@docoxx.ne.jp」の通信履歴を捜査機関に提供できないという帰結になる[36]。

これに対して，台湾では，日本刑訴法第197条2項のような規定がないが[37]，内政部の警察署が頒布した「警察の犯罪捜査のための手引き(警察偵査犯罪手冊)」(以下は「捜査手引き」と略称する)においては，「警察機関は，個人資料保護法[38]及び関連法令の規定により，プロバイダーなどの通信業者，学校あるいは関連業者に対して，個人のユーザーの資料あるいは記録を問い合わせることができる」という，捜査のための問い合わせの規定（捜査手引き224条）がある[39]。他方，中華民国憲法12条(以下「台湾憲法〇〇条」と略称する)において，「人民は秘密の通訊の自由を有する」と定められている[40]。また，通説によると，本

---

[34] 井上・強制・任意 254 頁，井上・電話逆探知 498 頁＝井上・強制・任意 207 ～208 頁，電気通信事業における個人情報保護研究会 37 頁，審議会(ハイテク)第 4 回議事録参照。

[35] 平成 16 年総務省告示第 695 号(最終改正平成 23 年総務省告示第 465 号)平成 23 年 11 月 2 日版：28 条解説(3)(http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html)参照。

[36] 通信の秘密に対しては犯罪捜査のための通信傍受に関する法律(以下，通信傍受法という)により一般の令状より厳格な要件を要求される傍受令状による保障がなされている現行法の体系を鑑みれば，捜査機関の照会書に任意に応じて通信の秘密にあたる通信履歴を提供することを認めると，両者はアンバランスという感じがせざるを得ない。他方，前掲した総務省のガイドライン解説においても，「通信履歴は，通信の秘密として保護されるので，裁判官の発付した令状に従う場合等，違法性阻却事由がある場合を除き，外部提供は行わないこととする。法律上の照会権限のある者からの照会に応じて通信履歴を提供することは，必ずしも違法性が阻却されないので，原則として適当ではない」(同注 35 の 28 条解説(4))とされている。

[37] 台湾刑訴法においては，247條で，「捜査の事項に関して，檢察官が所管機關に必要な報告を請求することができる。」と，278條で「裁判所は，審判期日の前に，必要の事項に対して，所管機關にそれを報告することを求めることができる。」と定められているだけである。つまり，警察官が通信秘密に当たらない通信履歴の提供を要求する捜査関係事項照会を出すというような権限は規定されていない。

[38] 個人資料保護法 20 条は，「公務機関でないものは，第 6 条第 1 項に定められた資料を除き，収集の特定の目的に沿って必要な範囲内に，個人の資料に対する利用を行うべきである。但し，下掲の事情の 1 つに該当する場合，特定の目的外の利用を行うことができる。一、法律の明文規定。二、公共利益を増進させるため。……四、他人の權益の重大な危害を防ぐため。……」犯罪の捜査については，一般に，二や三に該当するものがある。そして，法律の明文規定とは，前掲した台湾刑訴法 247(捜査における所管機関の報告義務)や同法 278 条(審判における所管機関の報告義務)があげられる。

[39] しかし，捜査手引きはあくまで行政院の内政部の警察署が頒布した行政規則にすぎない。

[40] そして，台湾でも，日本と同様に，通信の秘密に対しては一般の令状より厳格な要件を要求される傍受令状による保

条の保障する通信の秘密の範囲には，通信の内容のほかに，通信の対象・時間・方式や履歴なども含まれているとされる[41]。そこで，基本的には，台湾の解釈論としても，前述した日本の場合と同様に，通信の秘密にあたる通信履歴を捜査機関に提供できないが，通信の秘密に当たらないものであるならば，それを提供することができるという帰結になろう。

このように，日本においては，捜査関係事項照会に応じて，特定の対象者の通信履歴を捜査機関に提供しないということであれば，捜査機関としては，差押えないし検証に基づき関連情報を取得するという強制的手段をとるしかない[42]。この点は，台湾の場合も同様である。そうすると，次に検討すべきは，差押えや検証[43]などの強制的手段がとられる場合に，いかなる問題が生じてくるのかである。以下では，日本の場合での問題状況を明らかにしたうえで，それを参考に，台湾の場合にあてはめて考えるべき問題点を洗い出してみよう。

Ⅰ．既存の強制処分の保全機能の不備

第１の問題は，当該媒体に蔵置されたデータが既に削除されてしまっている場合には，かかる手段が機能しないという点である。というのも，検証であれ，差押えであれ，それらはいずれも，直接強制処分であって，相手方に一定の要求(作為ないし不作為)を命じることを内容とするものではないから，蔵置されたデータを削除しないように要求できるといった保全機能を有するものではないからである。

こうした問題が生じる背景としては，プロバイダーなどの通信業者は，一般的に，そのサーバー記憶媒体の容量とＩＴシステムの効率性に鑑み，大量の通信ログを，日々，記録したり削除したりしているため，捜査機関がサーバー記録媒体を差し押さえたときには，対象となる通信ログが既にプロバイダーにより業務行為として削除されてしまっていることが少なくないという点があげられよう[44]。

障がなされている(台湾の「通訊保障及監察法」参照)。

41 司法院大法官会議解釈 631 号，何賴傑(他)・刑訴實例 65～66 頁[陳運財]，林鈺雄・干預保留 219 頁，江舜明・通訊監察 116～117 頁，林三欽(他)・通訊監察 5 頁，林富郎・通訊監察 11 頁。

42 松沢・通信ログ 57 頁は，「通信の秘密に該当する情報は，強制処分の場合以外は提出しないのが通常であろう。但し，現に犯罪が差し迫っているなどの正当事由がある場合は，任意でも提出することはありうる」とし，「捜査機関は，……『捜査関係事項照会書』などのものを提示してプロバイダー側に情報を求めるが，個別の通信に関する情報については，通信の秘密を守る観点から，回答しないことが多い。そのため，捜査機関は求める情報を差押えるための手続きをとる」とする。井上・コンピュータ(1)56 頁＝井上・強制・任意 256 ～257 頁をも参照。

43 台湾における検証の定義は日本のそれと同じであるが(陳樸生・刑訴重訂十版 251 頁参照)，それは，令状によるものではなく，裁判所や検察官の職権によるものである(台湾刑訴法 212 条参照)。また，それが強制処分にあたるかどうかについても争いがある(呉・博論 14 頁＝呉・照相錄影 33 頁参照)。通説はそれを強制処分であるとされてきたのに対して(黃＝呉・刑訴法論(上)7 版 225 頁，蔡・刑訴增訂五版 255 頁，黃朝義・勘驗 74，77 頁)，検証(五官による認識)を，証拠を取得するための任意的な手段と位置づけ，強制的な五官による認識の捜査行為は捜索に帰属させるべきとする説が有力である(柯・刑事程序 276 頁脚注 9 参照。また同頁脚注 10 及び同氏・強制處分 93 頁をも参照。同解として，巫聰昌・勘驗法制 77 頁，傅・勘驗 106，108，119，133，134 頁参照)

44 通信履歴記録の保存期間は，業界ではまちまちであるとされる(井上・コンピュータ(1)56頁＝井上・強制・任意257頁)が，多くの場合は通信履歴を短期間ごとに削除していくのが業界の実態になっているのは間違いないようである(審議会(ハイテク)第2回，5回議事録参照。警察庁・ハイテク犯罪被害状況報告書205頁，警察庁・不正アクセス行為実態調査報告書167頁，松沢・通信ログ58頁，杉山＝吉田・情報処理の高度化(下)113頁をも参照されたい)。また，通信履歴な

以上の問題は，台湾においてはあまり指摘されていないが，将来の立法論として，考えておくべきものがあると思われる。というのも，台湾におけるプロバイダーなどの通信業者の運営の実態も日本のそれと異ならないように思われるし，台湾の差押えや検証という制度は，いずれも，直接強制処分にあたるものであるから，前述したような保全機能がないことは明らかだからである。

Ⅱ．占有の剥奪による過剰な処分

次に，記録媒体に蔵置されたデータが削除されていない場合にも，以下のような問題がある。

まず，記録媒体を対象とする差押えの執行により，媒体の占有が剥奪され，通信業者がその業務に甚大なダメージを被るという問題点が指摘されてきた[45]。同時に，媒体が差し押さえられたプロバイダーと契約している広範囲の市民にも，大きな不便ないし甚大な被害が生じるおそれがある。

これに対しては，現行法上の対応策として，差押えによらず，検証という手段をとればよいという反論が考えられる。というのも，検証は，差押えと異なり，媒体の占有が終局的に剥奪されることはないからである。しかし，検証であっても，その執行に際して，捜査機関が当該媒体を一時的に占有する形になっているのは間違いなく，場合によっては，それが長時間にわたることもありうるとすれば，検証の執行も，差押えの執行と同様に，プロバイダーなどの通信事業者の業務ないし契約加入者である市民に不利益を与えるものである。その意味で，それは，差押えによる終局的な占有の剥奪との間に質的な差異があるわけではなく，程度の差異にすぎないと思われる。

以上の指摘は台湾にも当てはまるものだと思われる。というのも，捜査手引き228條は，「コンピュータに対する差押えを執行する際に注意すべき事項：……（二）コンピュータの差押えは，比例原則に沿ったものでなければならず，とりわけ，プロバイダーなどの通信業者に与える影響の範囲を特別に注意しなければならない。」と定められているし，また，学説上，差押えに相応しくない場合か，それともそれに適合しない場合には，検察官や裁判所の職権による強制的な検証ないし警察官による任意的な検証を取るのが望ましいとされてきたからである[46]。

どを一切記載・保存しない業者もあり，例えば，利用料金につき定額制を取っている業者などがあげられる(井上・コンピュータ(1)56頁＝井上・強制・任意257頁参照)。

45 井上・コンピュータ(1)56 頁＝井上・強制・任意 257 頁，河上ほか編・大コンメンタール第二版補遺[吉田]9 頁，審議会(ハイテク)第 2 回議事録(ニフティからの参考人の発言)，福井・刑訴講義 5 版 149 頁，幕田・捜査法解説 3 版 228 頁，東京地決平成 10 年 2 月 27 日判時 1637 号 152 頁など参照。

46 黄＝呉・刑訴法論(上)7 版 225 頁。

Ⅲ．差押えによる技術的な支障の解決の可能性

捜索・差押えないし検証を行う際のコンピュータなどの機械の操作について，捜査側に専門的な知識・技術が欠如する場合には，捜査目的を十分に達成できないという問題点がある[47]。具体的には，まず，技術的な支障[48]が存在するがゆえに現場で電磁的記録媒体の内容が点検できないことが実務上は稀でなく，かような場合には，とりあえず媒体に蔵置されたデータを保全するために，当該媒体を差し押さえておく必要が認められる。こうした場合は，関連性を確認できないという点が問題となるが，後述する「蓋然性による差押え」が，その対応策として考えられている。

しかし，蓋然性に基づいて媒体を差し押さえることができるからといって，技術的な支障などの問題がそれによって解決されるわけではない。そして，その問題が解決できないままである限り，差押えを行った後，同媒体からデータを取り出したりアウトプットしたりすることはできず，捜査の終局的な目的を達成することはやはりできない。そうである以上，こうした場合の蓋然性による差押えの実施は，捜査の終局的な目的にとっては，実益が薄いものと言わざるを得ないと思われる。

これに対し，台湾においては，通説によると，差し押さえるべき物に当たるかどうかの判断にあたっては，現場で発見した物それ自体の内容を確認するという方法のほかに，当該物の存在する方式・状態などから推測するという方法も認められるとされる[49]。このことからは，台湾の場合にも，日本の蓋然性による差押えと同様に，現場で発見した媒体に関連性のあるデータが存在するかどうかを確認せずに，取りあえず一括して当該媒体を差し押さえておくことが認められると解されよう[50]。しかしここで，前述したように，問題は，媒体の中身を見ないで取りあえずそれを一括して差し押さえておいたからといって，技術的な支障などの問題がそれによって解決されるわけではない。

Ⅳ．改正法の対応とその問題点

以上示した３つの問題点につき，日本の改正法の対応を検討すると，まず，保全要請（日

---

[47] 河上ほか編・大コンメンタール第二版補遺［吉田］9 頁。台湾の場合にも同じ問題が指摘されてきた（法務部・電腦犯罪４版 150 頁）。

[48] その例としては，機械のランゲージが異なる場合のほか，被処分者が持っている機器やソフトのバージョンが極めて古いがゆえに捜査機関がそれを持っていない場合，被処分者が使用している機器やソフトが改造されたものである場合などが考えられる。

[49] 林鈺雄・捜索扣押 206 頁参照。また，陳樸生・刑訴重訂十版 214 頁は「……当該物件が証拠となるものあるいは没収できるものにあたるように思われる場合，それを差し押さえることができ，当該物件は果たして証拠物あるいは没収できる物であることを必要としない」とする。

[50] 陳瑞仁・新法捜索扣押 70 頁；また，捜査手引き 228 條は，「コンピュータの差押えを執行する際に注意すべき事項：（一）差押えを執行する際にコンピュータの設備の全セットを差し押さえておいたほうがよい［。］……（四）フロッピーディスク，CD等のコンピュータ補助記憶媒体の数を確かめておき，それを差押物一覧表に詳しく記載すべきである」と定められている。

本刑訴法197条3項)は，第Ⅰの点への対応策と考えられよう。本規定は，差押えの準備処分として位置づけられるものであり，令状によることなく，捜査機関の要請だけで行われるものとされる[51]。次に，第Ⅱと第Ⅲの点について，学説上は，提出命令などの間接強制処分の新設による対応が提案されてきた[52]。今回の改正で新設された記録命令付き差押え(日本刑訴法99条の2)は，「一種の提出命令」と位置づけられているから[53]，上記の提案が一部実現されたものともいえよう[54]。

もっとも，これらの制度は，いずれも強制力を持たないため[55]，現実的な問題を解決するには限界があることも否定できない事実である[56]。

以上の問題点をさけるため，台湾の立法論としては，日本の改正法の関連規定を一部で導入しつつも，強制力を与えることにすることも考えられるかもしれない。しかし，そうすると，台湾憲法12条の通信の秘密という基本権への過度な侵害にもなりかねないという問題点がある[57]。

第２款　「各別の令状」原則と「概括令状」の許容性

以上のとおり，①保全機能の不備，②一時ないし終局的な占有の剥奪による過剰な処分，③終局的な占有の剥奪による技術的な支障の排除不能，という既存の令状による直接強制処分の３つの不備を補うために，間接強制処分を導入する必要があったものの，日本の今

---

[51] 杉山＝吉田・情報処理の高度化(下)116 頁，121 頁(注 2)，審議会(ハイテク)第 2，7 回議事録参照。

[52] 酒巻・提出命令 125 頁以下参照。

[53] 田口・刑訴 6 版 114 頁，福井・刑訴講義 5 版 151 頁。

[54] 「記録命令付き差押え」には，それに違反した場合の罰則がない点で，提案されてきた間接強制手段たる提出命令とは異なっている。

[55] ただし，被処分者が命令に応じない場合には，別途で差押え令状をとり，それによって，必要な電磁的記録が記録されている記録媒体自体を差し押さえることが可能であるから，被処分者がそれを回避しようとして命令に従うことが期待されるので，この意味で，記録命令付き差押えは，「間接強制処分的な性格をもつ処分」であると言われる（杉山＝吉田・情報処理の高度化(下)77 頁(注 3)，河上ほか編・大コンメンタール第二版補遺[吉田]10～11 頁，指宿・サイバースペース 87 頁，福井・刑訴講義 5 版 152 頁)。

[56] 類似の指摘として，池田公博・電磁的記録80～81頁。杉山＝吉田・情報処理の高度化(下)72頁及び73頁(注5)参照。ただし，記録命令付き差押えについては，強制力はないものの，捜査機関の判断だけで要請できる保全要請とは異なり，裁判官が発付する令状による点で，問題を解決するのに有益なものと評価されている(長沼・コンピュータ犯罪15頁，審議会(ハイテク)第2回議事録(ニフティからの参考人の発言)，福井・刑訴講義5版151～152頁，指宿・サイバースペース87頁参照)。というのも，令状に基づくものであることから，データを提供した場合の，第三者との関係での免責的効果をもつことになると考えられ，捜査関係事項照会(197条2項)よりも，通信事業者による協力が得やすくなるからである。

[57] これにより，日本の改正法が罰則を設けないことの実益もわかろう。すなわち，罰則による制裁がないことにより，通信の秘密への不当の制約という批判を回避できるということである(杉山＝吉田・情報処理の高度化(下)113～114 頁参照)。これに加えて，前掲注 55 で示した通り，別途，差押え令状による対応が可能であるし(杉山＝吉田・情報処理の高度化(下)77 頁(注 3)参照)，また，保全要請はそもそもプロバイダーなどの通信業者のみを対象としており，通常はその協力を期待できると思われることも理由としてあげられている。しかし，技術的な理由で，被処分者の協力がないかぎり，別途で差押令状をとって媒体の占有を剥奪したからといって必ず当該媒体から対象となる電磁的記録を取り出すことができる保障はないし，また，台湾の通信業者の協力意識は日本のそれと比べると格段の差があり，「通常はその協力を期待できる」とまではいいかねるものがあるから，少なくとも，台湾の立法論にかぎっていうと，罰則などの強制力が与えられなければ，立法の実効性は薄いと言わざるを得ないであろう。

回の改正法は，通信の秘密への過度な侵害にならないようにするという配慮から，法による罰則という間接的な強制力を持たない間接処分という形にしたわけである。

間接強制処分につきさらに問題となるのは，各別の令状という原則との緊張関係が生じうるという点である。具体的には，次のような事例が問題となる。

【例 2】匿名伝送メールに対するトレース捜査

捜査機関は，【例 1】のＡ(麻薬密輸の運び屋)が提供した『Mark＠docoxx.ne.jp』というメールアドレスを doco 社に確認してもらったが，当メールアドレスは，いわゆる匿名伝送メールであることが判明した。匿名伝送メールの仕組みは，例えば，最初の発信者であるＸが，特定のメールアドレス(Mark＠docoxx.ne.jp)に届くメールを，自分の携帯メールアドレス(Xman@maxixx.com.my)に転送するよう設定するというものである[58]。その伝送の具体的なイメージは，次のものになる[59]。

【ステップ１：Ｘの送信】

From:　Xman@maxixx.com.my
To:　　Ａ(A@ntxx.ne.jp)
Subject: Subject: ただで海外旅行に行けるお得な派遣仕事ご紹介♪
　ただで海外旅行に行けるし，お金ももらえるお得な仕事をご紹介いたしますので，ご興味がある方，是非，このメールに御返信下さい。
　御返信をお待ちしております。担当者：マーク

↓

【ステップ２：Ａの受信】

From:　Mark＠docoxx.ne.jp
To:　　Ａ(A@ ntxx.ne.jp)
Subject: Subject: ただで海外旅行に行けるお得な派遣仕事ご紹介♪
　ただで海外旅行に行けるし，お金ももらえるお得な仕事をご紹介いたしますので，ご興味がある方，是非，このメールに御返信下さい。
　御返信をお待ちしております。担当者：マーク

このように，ステップ２で，「From」の部分が，「Xman@maxixx.com.my」ではなく，「Mark＠docoxx.ne.jp」に変化している。これが，いわゆる匿名転送メール・サービスのアドレス変換機能である。そして，Ａがステップ２の「Mark＠docoxx.ne.jp」からのメールにそのまま返信すると，ヘッダーの部分は，「To:Mark＠docoxx.ne.jp; From:Ａ(A@nttxx.ne.jp)」になる。すなわち，Ｘが，Ａに携帯のメールアドレスを知られることなく，やりとりが続けられることになる。

そのため，結局，doco 社が提供した情報だけでは，卸元であると疑われる最初の発信者

[58] http://mail.marine.ne.jp/scripts/tokumeisetumei.asp を参考にした。その他の仕組みもあるが，例えば，リメーラ・サービス（remailers service）を利用する(http://en.wikipedia.org/wiki/Anonymous_remailer)。
[59] 同前注。

を割り出すことができなかった。それでは，匿名伝送メールに対して，捜査機関はいかなる捜査を行うべきであろうか。

１つの可能性として考えられるのは，いわゆるトレース・バック捜査[60]である。具体的には，捜査機関が，doco 社の通信履歴データから１つ前の発信元は maxi 社であることを割り出したうえで，その maxi 社に連絡し，最初の発信者の身元を突き止めていく形になる。この手法をとる際に問題となるのは，中継サーバーの経由は，技術的には，いくらでも設定可能であるが，１つの長いチェーンに対して，従来の１通の令状によって対応することができるかである。そこからは，1 つの令状――間接強制力付きの開示命令状が考えられる――により，対象となる特定のデータ転送の全過程をカバーできるような制度(以下は，概括令状と称しよう)を設ける必要性があることが容易に想像できる。しかしながら，既に指摘されている通り，各々のデータが異なる場所にあり，それぞれ別々の主体によって管理されているため，かような制度が，果たして日本国憲法 35 条によって要求されている対象の特定・明示ないし各別の令状などの要件にかなうのかという問題がある[61]。

トレース・バックという手段は，ＩＴシステムにおける捜査にあたっては必ず必要不可欠なものと言っても過言ではないが，かような手段を認めるために必要な「概括令状」は，各別の令状の原則に反するものであるとされる。そこで，今般の改正法は，間接強制力付きの開示命令状という方策をとらずに，間接強制力が付かない開示義務を設ける程度にとどめることにしたわけである。というのも，こうすれば，前述の難点を回避することができるからであり，逆にいえば，上記の問題につき，立法的な解決は図られていないわけである。

ところで，対象となる特定のデータ転送の全過程をカバーできるような令状は，間接的強制処分という側面のみならず，直接的強制処分という側面においてもそのニーズがある。というのも，間接強制力付きの開示命令状を設けたとしても，相手方が法の処罰という不利益を甘受する場合には，直接的強制処分を行うしかないからである。ここでいう直接的強制処分は，対象となる特定のデータ転送の全過程をカバーできるような概括令状をもって，転送の全過程におけるすべてのＩＳＰないし経由点のシステムにアクセスしたり，それぞれのシステムに蔵置されたデータを検索したり，ダウンロードしたりするような新型の捜査手法を意味する。

以上をもとに，台湾の立法論を考えてみると，次のようなものになろう。すなわち，中華民国憲法においては，日本国憲法 35 条のような条文はない。そのため，学説上は，捜索(差押え)という制度に関して令状原則を採用するかどうかは，憲法の問題にはならず，あ

---

[60] トレース・バック捜査とは，伝送経路が多重中継になっている場合，多重中継チェーンのうち，最終の受信先プロバイダーであるＸ社の通信履歴データから，１つ前の中継サーバーが，例えば例えばM_1というプロバイダーであることを割り出し，次に，そのM_1の通信履歴データから，さらに１つ前の中継サーバーM_2であることを割り出し，同じようにして最後最初の発信プロバイダーであるＹ社を突き止めるという捜査の手法を指す(井上・コンピュータ(1)57 頁＝井上・強制・任意 259 頁参照)。また，大橋・基礎編 51 頁の説明をも参照。

[61] 井上・コンピュータ(1)57 頁＝井上・強制・任意 260 頁の説明を参照されたい。

くまで「立法政策」の問題にすぎないという理解が多数説である[62]。そうだとすれば，台湾においては１つの概括令状をもって，転送の全過程におけるすべてのＩＳＰないし経由点のシステムにアクセスしたりそれぞれのシステムに蔵置されたデータを検索したりダウンロードしたりするような捜査手法を新設することが憲法上の問題にはならないことになる。

しかし，これに対しては，台湾憲法は，令状原則を明示していないが，憲法の精神から，それを導き出すことができるとする見解も有力である[63]。これによれば，捜索・差押えは，人民のプライバシーないし財産などの基本人権に関わるものであるから，政府が人民の基本権利を制限することができるかは，当然に，「中立かつ超然の機関」が判断すべきとされる[64]。

かかる見解は，アメリカ憲法修正４条に関わる議論を参考に，台湾憲法の精神から，捜索・差押えを正当化するためには，中立かつ超然の機関が発付する令状が必要であるという憲法上の原則を導き出しているが，ここでいう憲法上の令状原則が，日本における各別の令状という原則をもその一内容とするものであるかどうかについては言及されていない。かりに，そこまでの内容を含んでいないとすれば，前述した多数説のそれと同様に，概括令状を設けることが台湾憲法の精神に反するものでないということになるが，逆に，もしそれを含むのだとすると，同憲法の精神に反すると解されることになろう。

第２節　電磁的記録媒体に対する捜索・差押え・検証

第１款　大容量の電磁的記録媒体に対する捜査

以上のとおり，通信の秘密の中核をなす部分については，旧来の捜査関係事項照会ないし今回新設された協力・保全要請というような規定によって，捜査機関がその部分に関するデータを入手することができない。言い換えれば，この部分のデータに関しては，令状の発付がない限り，プロバイダーなどの通信業者はそれを捜査機関に提供することができないのである。

これに対して，日本の今般の改正法は，いわゆる記録命令付差押状(日本刑訴法 99 条の 2)を新たに設けることによって対応している。だが，この新設令状には強制力が与えられていないため，相手方がこの記録命令付差押状に応じない場合には，新たな問題が生じるとなる。具体例をあげると，次のようなものとなる。

---

[62] 林鈺雄・乙案 41～42 頁，同・捜索扣押 20 頁脚注 1，27 頁，128 頁脚注 17 参照。捜索修法 139 頁，柯・刑事程序 174～181 頁をも参照。

[63] 令状原則という理念は，中外西東を問わずに，法治国であるかぎり，認めるべきものであるとし，台湾の憲法からもその精神に沿って解釈すれば，捜索・差押えを行うには中立かつ超然の司法機関の発付する令状によるべきものであると解されようとされる(王・令狀原則 46～47 頁，同・刑訴講義 91～92 頁参照)。同見解として，曾・偵査 60 頁。

[64] 同前注。

【例 3】記録命令付き差押状に応じない場合に取られる措置とその問題点

前例にも登場した doco 社の通信履歴データから，１つ前の発信元は maxi 社であることを割り出した捜査機関は，maxi 社が保有している，「Xman」というアドレス名を使用している加入者の身元情報及び「Xman@maxixx.com.my」の通信履歴の提供を要求する旨の捜査共助要請書を作成したうえで，国交のあるマレーシアの外務省に対して当該要請書を提出した[65]。その結果，maxi 社も１つの中継サーバーにすぎず，最初の発信元は，「Yman@chanxx.co.jp」であること，及び chan 社はアメリカ人が日本国内で日本の会社法に基づいて設立・登記した会社であることが明らかになった。

そこで，捜査機関は，chan 社に対して，捜査関係事項照会書(日本刑訴法 197 条 2 項)をもって，「Yman」というアドレス名を使用している加入者の身元情報及び「Yman@chanxx.co.jp」の通信履歴の提供を要求し，これに応じて，chan 社は，Yman(ユーザー名)という加入者の身元情報を提供したが，通信履歴は既に削除されていたため，関連データは提供されなかった。これを受けて，捜査機関は，chan 社に対して，これからは「Yman@chanxx.co.jp」に関連する通信履歴を削除しないよう依頼した[66]。

その３ヶ月後，捜査機関は，chan 社に対して，「Yman@chanxx.co.jp」の通信履歴並びに同アカウントに蓄積されているメールの内容の提供を要請した。これに応じて，chan 社は通信履歴の提供をしたが，メールの内容については，通信の秘密の中核をなす部分であるから，令状の発付がない限り提供できないと回答した。そこで，捜査機関は，記録命令付き差押状を得たうえで，chan 社に対して対象となるメールの内容を記録媒体に記録することを命じた。これに対し，chan 社は，「Yman@chanxx.co.jp」というアカウントの関連データの抽出作業に長時間がかかるうえに，こうした作業を完全に自動化することはできず，手作業を含めて行う必要があり[67]，抽出費用が高額となるため，命令に応じることはできないとの回答をした。

この場合，捜査機関として，「Yman@chanxx.co.jp」というアカウント関連データが本件捜査のために重要性が高く，それをどうしても手に入れなければならないと考えているとすれば，同アカウントが設定された chan 社のサーバー記録媒体を差し押さえるべき物又は検証すべき物として，当該媒体に対する捜索差押令状又は検証令状の発付を請求し，自ら chan 社に赴いて強制捜査を行うことになる。その際には，以下の点が問題となる。

Ⅰ．データを取得する場面

改正法のもとにおいても，従来と同様に，無体のデータ自体は差押えの対象になっていないから,【例 3】において,捜査機関が捜索差押令状を請求する際には,「Yman@chanxx.co.jp」

[65] 日本における国際捜査共助の実務上の処理につき，杉山・外国における捜査 69～64 頁参照。

[66] これは日本の実務上の標準手順になっているようである(審議会(ハイテク)第 2 回議事録のニフティからの参考人の説明参照)。

[67] 審議会(ハイテク)第 2 回議事録(ニフティからの参考人の発言)及び松沢・通信ログ 58 頁の説明参照。

というアカウントやその中にあるメールではなく，同アカウントが設置されている chan 社のサーバー記憶媒体を捜索差押令状の直接の処分の対象とすることになる。すなわち，改正法は，電磁的記録を保全・取得するための措置を講じつつも，基本的には捜索・差押えの対象が有体物に限られるという従来の理解をそのまま維持するものである。

これに対し，台湾においては，2001 年の法改正により，無体の電磁的記録も捜索の対象として列挙されており，一般論としては，無体の電磁的記録も差押えの対象であると解されている。しかし，既に指摘されているとおり，従来の捜索・差押えの定義が変わっていないのに，捜索・差押えの対象には電磁的記録を含めるというような法改正は明らかに不当である[68]。つまり，台湾においては，通説によると，差押えは物の占有を強制的に取得する処分と定義されるため，その(直接の)対象は，有体物に限られるとされている[69]。また，捜索[70]は，差し押さえるべき物を発見するための手段と位置づけられるため[71]，その対象も，有体物に限られると解されてきた[72]。

こうした前提のもとで，2001 年の法改正は，形式的に電磁的記録を対象とするのみで，電磁的記録それ自体が捜索・差押されたといえるための基準を示していないがゆえに，有体物を対象とする場合にとられてきた従来の基準，すなわち，捜索とは物理的な場所に入ったりすることであり，差押えとは有体物の占有を剥奪することであるという基準が，そのまま適用されることにならざるをえないのである。

しかし，警察官がＩＴシステムに入ったり，そのなかに置かれた何かを触ったりすることはありえないし，また，データに対しては占有の剥奪を観念することもできないから，結局のところ，一体，何をもって電磁的記録それ自体が捜索されたといえるのかは明らかでないばかりでなく，占有剥奪のできない電磁的記録それ自体が差し押えられたといえる場面もほとんどないとすれば，かような立法は意味が薄いといわなければならない。実際にも，裁判例や学説上， 2001 年の改正によって追加された「電磁的記録」に言及する際に，その例として一般的にはノートパソコンやコンピューマシンなどの有体の記録媒体をあげている程度にとどまっており，こうした場合の捜索・差押えの(直接の)対象は，一体，有体の電磁的記録媒体なのか，それとも，無体の電磁的記録なのかという問題についての説明を回避している[73]。他方で，捜査実務上も，証拠となる無体のデータのみならず，有体の

---

[68] 林裕順・基本人權 152 頁；捜索修法(二)131～132 頁(林鈺雄・蔡秋明・蔡兆誠の発言)。

[69] 黄＝呉・刑訴法論(上)7 版 200 頁，陳樸生・刑訴重訂十版 213 頁，黄朝義・刑訴三版 234～235 頁。

[70] 台湾では，人に対する捜索と物に対する捜索との２つの制度があり，後者は狭義の捜索であり，両者を併せて広義の捜索とされる(林山田・程序法５版 338 頁)。ここでは，狭義の捜索を指す。

[71] 林・概論(上)11 版 295 頁，黄＝呉・刑訴法論(上)7 版 195 頁。

[72] 確かに，2001 年に，従来の差し押さえるべき物と並んで，電磁的記録をも捜索の対象としている点からいえば，捜索の位置づけは，差し押さえるべき物並びに電磁的記録を発見するための手段に変わるものであろう(朱・刑訴(修二)121 頁脚注 1 参照)。とすると，電磁的記録を見つけようとする場合，捜索の対象は有体物に限らないと解する可能性があるかもしれない。しかし，占有の剥奪という差押えの定義は変わっていないから，電磁的記録には占有の剥奪を観念することがありえない以上，それを取得する捜査行為の法的性格は何なのかは不明のままである。もし，かかる行為も差押えにあたるものと考えると，結局のところ，差し押さえるべき電磁的記録を発見するための捜索の対象はやはり占有の剥奪という要素により制限されることになってしまい，有体物に限られるという帰結になるはずだろうと思われる。

[73] 林・概論(上)11 版 297 頁。台湾の最高法院 94 台上 3200 判決をも参照。日本でいう判例は，判決の先例の略称である

コンピュータなどの電磁的記録媒体自体を差し押さえることが基本方針となっている[74]。それゆえ，結局のところ，上記の【例 3】では，法文上は電磁的記録をも捜索(ないし差押え)の対象としている台湾刑訴法の場合にも，捜査の実態としては，有体物のみを対象とする日本刑訴法の場合と同様に，chan 社のサーバー記憶媒体そのものを差し押さえておくことになる。

しかしここで問題となるのは，サーバー記憶媒体の容量は非常に膨大であって，その中の，極めて僅かの容量しかない「Yman@chanxx.co.jp」というアカウントにおける特定のメールのデータを取得するためだけに，数千ないし数万さらにそれ以上の数のアカウントが設置された超大容量のサーバー記憶媒体全体の占有が剥奪されてしまう点にある。これにより，業者の営業に大きな支障を生じさせると同時に，同媒体内に蔵置された他の多数の無関係な加入者の身元ないしアカウントの関連データをも一括して捜査機関の手に入ってしまうため，適切ではない[75]。

以上の問題は，「実質的な過大差押え」と称することができよう。というのも，かような場合になされる差押えは，形式的には台湾の現行刑訴法の規定に反しないようにみえるものの，中華民国憲法 23 条における比例原則から導かれた，「処分が必要最小限度でなければならないという原則」(いわゆる最小化原則)[76]に適合しないからである。つまり，技術的には，「電磁的記録(データ・情報)のみを取得する」ことが可能であり，かつ，犯罪立証のためにそれだけで足りる場合であるにもかかわらず，有体物である媒体と無体の情報である記録とを同時に差し押さえることになるため，最小化原則に適合しない過剰な処分にあたることになるからである。

この点で，従来は，情報とその記録媒体との間に物理的な不可分性が認められたために[77]，処分の直接の対象を記録媒体などの有体物に限ったとしても，法規定の上でも，また，法執行の場面においても，最小化原則に反するとまではいえなかったかもしれない。しかし，現在の技術では，上記の意味での不可分性は解消されているため，情報自体の差押えが可能である[78]。そして，帳簿やコンピュータなどの「記録媒体の差押え」と比べると，記録媒

のに対して，台湾でいう判例は特別の意味をもち，すなわち，法院組織法 57 条(判例の選択編集及び変更)は，「最高裁判所の裁判においては，その法律的見解は判例として取り上げる必要がある場合，院長[裁判所の長]，廷長[法廷の長]及び裁判官からなる民事廷会議，刑事廷会議あるいは民・刑事廷総会のそれぞれにより決議されたあと，[その決議の結果を]司法院に報告し査察の備えをすべきである。(第一項)」と定められている。つまり，院長，廷長及び裁判官からなる民事廷会議，刑事廷会議あるいは民・刑事廷総会の決議により選ばれた特に優れた法律的見解を示した最高裁の判決の先例を，判例といい，それ以外の最高裁の判決の先例は判例ではなく，判決あるいは裁判例と呼ぶ。

[74] 捜査手引き 228 条，同 229 条参照。范・過度扣押 9～10 頁をも参照。

[75] 井上・コンピュータ(1)60～61 頁＝井上・強制・任意 267～268 頁，経産省報告書・サイバー犯罪条約・対応 52 頁。

[76] 立法院公報(院会記録)二讀(逐條討論) 90 卷 5 期 3139 號一冊 165 頁(會議日期 2001 年 1 月 2 日)は「憲法 23 条から導かれた『比例原則』は刑事訴訟法の指導原則であり，人民の基本権利に対する国家の干渉の手段とその目的の間に，『最小の干渉』を原則としなければならない(http://lis.ly.gov.tw/ttscgi/lgimg?@900501;0163;0301)」とする。また，林・刑訴概論 11 版 212，215～218 頁，林鈺雄・捜索扣押 35 頁，180 頁以下，陳・憲法基本權(上)4 版 239 頁，241～242 頁をも参照。

[77] 川出・コンピュータ犯罪 1 頁。

[78] 劉 92 頁。

体に記録された関連情報のみをコピーする，いわば「情報の差押え」という選択肢は，権利の侵害の程度がより緩やかな手段であるから，そのような手段をとる必要性も認められるのである[79]。

以上指摘した実質的な過大差押えの問題は，台湾では十分に意識されていないのが現状であるのに対して[80]，日本においては，これまで，後述する，①差押えの「必要性」の否定，②検証の活用，③差押えの代替的処分としてのアウトプット物(紙媒体の印刷物あるいは電磁的記録媒体の転写物)の作成，という３つの手段により対応がなされてきた。これに加えて，④今回新設された差押えに代える処分(日本刑訴法 110 条の 2)もかかる問題に対応しようとするものと位置づけられる。

そこで，以下では，この４つの対応により，実質的な過大差押えの問題が，どのように，いかなる程度で解決されてきているのか，そして，そのうえで，なお残されている未解決の問題点は何なのかを検討しておくことにする。

１．必要性と利益衡量論

実質的な過大差押えの問題につき，学説上は，コンピュータ等の記録媒体全体を差し押さえることにより，大量の情報が一括して捜査機関の手に移転してしまうことは深刻な問題であるとの指摘がなされてきた[81]。また，電磁的記録媒体を差し押さえると第三者に対して過度の負担になるような場合，記録媒体に対する捜索・差押えの「妥当性」を疑問視すべきであるという主張もなされてきた[82]。一般論として，処分が過剰になる場合には，「相当性」の観点から差押えが認められない場合もあるとされており[83]，裁判例においても，被疑事実と関連性のあるデータが僅かであり無関係の第三者の個人データが多数入っている電磁的記録媒体に対する差押えの「必要性」を否定したものが存在する[84]。

以上の通り，「妥当性」，「相当性」，「必要性」などの異なる用語が使われているが，それらは，いずれも，憲法で要求されている最小化原則[85]を体現するものといえるから，実質的な意味内容

---

[79] 同前注。

[80] 台湾の先行研究においては，対象となる電磁的記録を取得するためにそれを記録した媒体自体を差し押さえるのは，過度な差押えの問題があると学説上は一部で指摘されてきたが（李・電磁紀錄 1057 頁以下，范・過度扣押 8～10 頁参照），これらの問題は，これまで実務上はあまり重視されていないため，あるべき対応もなされていない。

[81] 酒巻・提出命令 128 頁，椎橋刑訴 4 版 99 頁のほかに，前掲注 45 に挙げた文献をも参照。台湾においても，コンピュータ媒体自体を丸ごとに差し押さえると，それによって，かかる媒体の使用者が権益を損されると同時に，同媒体に蔵置された会社の営業秘密などにかかわる情報が洩れるという問題点が指摘されてきた(法務部・電腦犯罪 4 版 150 頁参照)

[82] 安富・コンピュータ犯罪 152 頁以下。古田・第三者の保護 191 頁も参照。

[83] 長沼＝山田 60 頁。

[84] 東京地決平成 10 年 2 月 27 日判例時報 1637 号 152 頁(ベッコアメ顧客データ差押え事件)。

[85] この最小化原則の憲法上の根拠については，台湾の場合には，前述したように，中華民国憲法 23 条に求められる。日本の場合は，憲法 13 条が根拠となると思われる。すなわち，まず憲法分野では，日本国憲法 13 条は，「必要最小限度の規制の原則」を宣明しているとされる(野中ほか・憲法Ⅰ(5 版)258 頁，田上・公共の福祉 225 頁，今村 55 頁など参照)。また，刑事法分野においては，通信傍受の合憲性につき，日本国憲法 35 条に要求される特定性の要請の趣旨を，アメリカでいう「最小化(minimization)」原則に類するものとして捉えている見解がある(井上・傍受 186 頁)。福井・刑訴講義 5 版 13 頁は，日本国憲法 13 条と並んで，同法 31 条の「法律の定める手続」による基本的人権(同法 11 条参照)の制

が異なるものでないと思われる。そこで本稿では,「必要性」という用語を採用することとする。

令状発付の必要性に関して,裁判官にはその判断権限があるかについてかつては争いがあったが,最高裁は,いわゆる国学院大学ファイル事件(最三決昭和 44 年 3 月 18 日刑集 23 巻 3 号 153 頁)において,裁判官は様々な要素を総合的に考量したうえで令状発付の必要性を判断する権限があることを肯定した[86]。これにより,この問題に決着が付けられた。

この判例で示された「総合的な考量」という判断手法は,学説上は,「比較衡量論」や「利益衡量論」と称される[87](本稿は,「利益衡量論」という)。

この利益衡量論は,台湾の場合にも活用することが可能であろう[88]。というのも,それは,中華民国憲法 23 条に要求されている最小化原則が体現されたものだと考えられるからである[89]。しかし,利益衡量というのは,情報の要保護性のみを配慮するものではなく,令状の発付ないし捜査の執行などの事項の全般にわたって妥当する一般的な原則であるから,被疑者や被告人が被処分者である場合にも適用されることになる[90]。とはいえ,実際には,この利益衡量論は,実質的な過大差押えという文脈のもとにおいては,被処分者が被疑者や被告人である場合には機能しにくいように思われる。

なぜなら,まず,被疑者や被告人が協力の意思表示をしたとしても,捜査官としては,被疑者や被告人の真意は協力ではなく,コンピュータなどの記憶媒体を操作するふりをしつつ証拠を隠滅するつもりではないかと疑うことは一般的に合理性があると考えられるからである[91]。それに加えて,データが瞬時に移動・削除できる特性をもつため電磁的記録媒体を捜査の対象とする場合には証拠隠滅が一般の事案のそれよりも容易に実行されるという実状に鑑みると,捜査官として,最も妥当な捜査の執行の方法は,コンピュータなどの電磁的記憶媒体全体の占有を取得した

限も,「合理的な必要最小限度の制限」でなければならないとする(同 90 頁,108 頁をも参照)。以上のとおり,台湾の憲法のいう最小化原則の内実と日本の憲法のいうそれの内実とは異なるものでないと考えられる。

[86] 本件は「差押は『証拠物または没収すべき物と思料するもの』について行なわれることは,刑訴法 222 条 1 項により準用される同法 99 条 1 項に規定するところであり,差押物が証拠物または没収すべき物と思料されるものである場合においては,差押の必要性が認められることが多いであろう。しかし,差押物が右のようなものである場合であっても,犯罪の態様,軽重,差押物の証拠としての価値,重要性,差押物が隠滅毀損されるおそれの有無,差押によって受ける被差押者の不利益の程度その他諸般の事情に照らし明らかに差押の必要がないと認められるときにまで,差押を是認しなければならない理由はない。したがつて,原裁判所が差押の必要性について審査できることを前提として差押処分の当否を判断したことは何ら違法でない」とする。

[87] 杉原(4)146 頁。

[88] 実務上も,コンピュータを差押えの対象とする場合には,証拠保全における利益衡量が問題となると指摘されている。すなわち,証拠を保全するために対象となるコンピュータを差し押さえた場合,それによって損害されうる利益が,当該捜査対象となった事案における被害を超える場合にも,それを差し押さえるべきであろうかという問題である(法務部・電脳犯罪 4 版 82 頁。林永謀・刑訴釋論(上)471 頁をも参照)。これに対して,「わが国の刑訴法上,逮捕令状に関しては,日本の刑訴法 199 条 2 項のいう『明らかに逮捕の必要がないと認めるときは』というような文言がないため,台湾の場合には,日本のように,裁判官には必要性を審査する権限があると解することができない。」(陳瑞仁・新法捜索扣押 60 頁)とする少数見解がある。

[89] 中華民国憲法 23 条のいう比例原則は,刑訴法のみならず,法律全般に渡って妥当する一般的原則とされており,刑事手続における比例原則の適用についても,電磁的記録の文脈のもとに限られないものである(たとえば,智慧財産法院刑事判決 98 年度刑智上訴字第 19 號参照)。

[90] 千葉地決昭和 53 年 5 月 8 日判例時報 889 号 20 頁,福岡地決昭 46 年 5 月 1 日判夕 264 号 349 頁のほか,福井・刑訴講義 5 版 137 頁注 1 に挙げられた数多くの判例をも参照。

[91] 河原 72 頁。また,平良木ほか編・判例刑訴[壇上]63 頁,渡辺直行 105～107 頁をも参照。

上で,被疑者や被処分者にパスワードを提供させたり,データの選出の方法を教示させたりして,自ら操作するという形か[92]，あるいは，コンピュータ・フォレンジック[93]の専門家に依頼するという形になるであろう[94]。

それゆえ，結局のところ，被疑者や被告人が被処分者である場合には，利益衡量論を活用したとしても，その結果は，ほとんどの場合，記録媒体全体を差し押さえるべきであるという結論になるように思われる[95]。

２．検証の差押え的性格の活用

改正法以前に捜査機関が特定のデータを取得する方法としては，差押えと検証という２つの手段があった[96]。まず，通説によれば，差押えの対象は有体物に限られるから，データを複写することは差押えにあたらないとされるので[97]，差押えという手段をとる場合は，電磁的記憶媒体に対する占有の剥奪を通じて，対象となるデータをも含んだ，媒体に蔵置された全部のデータを一括して保全・取得するという形になる[98]。他方，検証という手段をとると，必要な処分として，関連するデータを他の電磁的記録媒体に転写したりプリントアウトしたりするという「検証の結果の記録」の形で，対象となるデータのみを保全・取得することになる[99]。

以上の通り，差押えの媒体に対する占有の剥奪ないし検証の結果の記録(関連性のあるデータをコピーすること)などの手段により,媒体内に蔵置されたデータを取得することが可能である。検証の結果の記録という手段は,データ自体のみを差し押さえるのと同様の機能を果たすもので

---

92 台湾の実務では,捜査人員自らが操作することが原則とされているばかりでなく(捜査手引き 225 条参照),被処分者がコンピュータに接触しファイルや証拠を削除することを避けるためには当該者がコンピュータと近づかないよう注意しなければならないという規定もある(捜査手引き 227 条参照)。

93 コンピュータ・フォレンジックとは，特定のデータを探索したり解析したりするために行うコンピュータの鑑識分析技術を意味する(See JIM KEOGH, at140～144 ; Craig Ball, at 4ff ; Kerr, DIGITAL WORLD, at 539 n26。エディックス(訳)1 頁をも参照)。かかる技術は，日本法においては，刑訴法でいう鑑定や，捜査機関が行う鑑識と位置づけられる。また，安富・刑訴講義 2 版 268 頁は，「デジタル・フォレンジック」と称し，それを，「犯罪の立証のための電磁的記録の解析技術及びその手続」と定義する。

94 河原 72 頁参照。

95 同前注。

96 井上弘通 332 頁，川出・コンピュータ犯罪 4 頁，小林充・刑訴新訂 103 頁参照。また，寺崎・刑訴 2 版 107 頁は「情報を発見・収集・保全するための処分として，検証や鑑定，証人尋問がある」とする。

97 通説は，名取・コンピュータ 390 頁，上口・刑訟 3 版 140 頁，白取・刑訴 7 版 134 頁，田宮・刑訴(新版)102 頁，柳 306 頁，寺崎・刑訴 2 版 121 頁，幕田・捜査法解説 3 版 228 頁，田口・刑訴 6 版 88，110 頁，松尾・条解 4 版 204 頁，平良木・捜査法 245～236 頁など参照。反対説がある(伊藤ほか・注釈(新版) 2 巻[藤永]151 頁＝初版：青柳ほか・註釈(1)[藤永]379 頁，安富・ハイテク犯罪 164 頁，同・コンピュータ犯罪 150 頁など参照)。

98 関・刑訴法 79 頁，椎橋・刑訴 4 版 101 頁参照。

99 川出・コンピュータ犯罪 5 頁。白取・刑訴(7 版)134 頁(脚注 44)及び 139 頁，田口・刑訴 6 版 88 頁をも参照。ただ，こうした場合は，媒体が検証の直接の対象である点には異論がないが，無体の電磁的記録それ自体も検証の直接の対象になりうるか，それとも，それがあくまで間接的な対象(実質的な処分の対象)にすぎないかについては争いがある。この点，ここで挙げた川出論文 5～6 頁は「……検証の対象が，有体物たる電磁的記録媒体であることは明らかである」とし，同 4 頁は「現行法上，電磁的データを強制的に取得する手段としては，差押えと検証が考えられるが，いずれについても，処分の対象は有体物に限られるため，無形のデータそれ自体はその対象とならない」とする(同見解として，松尾・条解 4 版 203～204，242 頁をも参照)。これに対して，石川／増井 216 頁は「現行法の解釈としては，……『検証』と考えれば刑訴法は検証の対象を特に有体物とは限定していない」とする。

あるので，実質的な過大差押えの問題を解消する手段となりうると考えられる[100]。

以上を台湾の場合に当てはめて考えてみると，次のようになる。まず，差押えの部分は，日本の場合と同様に解してよいと思われる。これに対し，検証の部分については，台湾では，証拠の保全ないし証拠調べの方法としての検証(勘驗)という制度があるが[101]，警察による捜査の手段としての検証(令状)という制度は存在しないから，せいぜい任意処分としての検証(警察機関による実況見分)という手段を活用する程度に止まるだろう[102]。

そこから，日本の検証令状という制度を台湾にも導入することも考えられないわけではなかろう。しかし，そうすると，次の点がまた問題となる。すなわち，捜査機関が検証によることなく，媒体の差押令状の発付を請求する場合に，裁判官が，捜査機関に対して，データを検証する手段をとれば十分であるとして，差押令状の請求を却下し，検証令状を発付することが可能なのかである。

この点について，許可状という差押令状の性質からみれば，それは，捜査機関の固有権である捜査権限の行使を裁判官が許可するだけであって，捜査機関が請求する差押令状の代わりに検証令状を発付することはできないと解すべきであろう。とはいえ，裁判官は，捜査官に対して，媒体を検証しその中に対象であるデータのみをコピー(検証の結果の記録)する手段で十分である旨を示したうえで，改めて検証令状の請求を勧めることができないわけではないであろう。

以上の通り，検証令状という制度を台湾にも導入したうえで，それを活用することにより，ある程度，実質的な過大差押えの問題に対応するのが可能であると思われるものの，そこには，解釈論としての限界並びに司法の役割による二重の制限があるから，問題解決のためには必ずしも十分ではない。

3．差押えの代替的処分

日本の捜査実務上，データを電磁的記録媒体からアウトプットしてプリントアウト文書を作成したり，他の記録媒体に関連データを転写したりする慣行があるとされている[103]。かような慣行により，記録媒体全体を差し押さえる必要がなくなるとすれば，実質的な過大差押えが解消されるということができる。この意味で，媒体に対する差押えを本来の処分と，プリントアウト文書ないし転写記録媒体の作成を差押えの代替的処分と位置づけるこ

---

[100] 川出・コンピュータ犯罪 7 頁。

[101] 本条の位置づけにつき，法の体系上は，証拠物を収集するための強制処分でなく，証拠調べのところに置かれているが(台湾刑訴法 212 条参照)，学説上，検証(勘驗)も証拠(物)を収集するための強制処分の一種と位置づけられる(林裕順・基本人權 115 頁，黄＝呉・刑訴法論(上)7 版 225 頁)。これに対して，検証を，証拠を収集するための任意的な手段であるとする説もある(柯・刑事程序 276～277 頁，傅・勘驗 106 頁)。

[102] 台湾の刑訴法においては，強制処分である検証(勘驗)は，検察官あるいは裁判官の職権により，令状なしでそれを行うことができると定められているから(台湾刑訴法 212 条)，司法警察官には，本条の強制性を帯びる検証を行う権限がないという点については異論がない(黄＝呉・刑訴法論(上)7 版 255 頁参照)。任意処分としての検証(「臨場檢查」あるいは「實況勘察」と呼ばれ，いわゆる日本でいった「実況見分」という概念にあたるものである)を行うことは，現行法上認められているかどうかについては争いがある。この点，否定説としては，林山田・程序法 5 版 470 頁，褚・刑訴(上)四版 336 頁，19 年上字 1359 判例があげられる。肯定説は，黄＝呉・刑訴法論(上)7 版 225 頁脚注 139 参照。

[103] 審議会(ハイテク)第 4 回議事録，井上・コンピュータ(1)61 頁＝井上・強制・任意 269 頁，貴志・ハイテク犯罪 110 頁，長沼・コンピュータ犯罪 13 頁参照。

とができる。そこで，以下では，かかる慣行により，実質的な過大差押えの問題がどこまで解消されており，なお残されている未解決の問題点は何なのかについて検討を行いつつ，それに照らして台湾の問題状況を明らかにし，将来の立法のあるべき方向を考えておきたい。

(1) これまでの実務の慣行

プロバイダーを被処分者とする場合においては，原則的に，サーバー記憶媒体全体に対する差押えの代わりに，プロバイダーにプリントアウト文書ないし関連データの転写記録媒体を作成してもらい，それのみを取得するという措置が取られている[104]。その具体的な手順は，以下のようになる。

まず，令状への記載事項として求められる「差し押さえるべき物」の内容を，捜査機関とプロバイダー側が確定する作業を行い，その上で，「差し押さえるべき物」の内容確定後は，プロバイダー側の担当者が，差押え目的物たる通信ログなどを紙媒体に印字したものや，記録媒体(フロッピーディスクやCD―R)に格納したものを所持しておくことになる[105]。最後に，捜査機関は，令状をプロバイダー側担当者に呈示し，プロバイダー側担当者はあらかじめ準備しておいた，印字済紙媒体，データが格納された記録媒体などを提出し，押収品目録の交付を受ける[106]。

これに対し，被処分者がプロバイダーでない場合は，処理は異なったものとなる。この点について，警察大学特別捜査幹部研修所教授である名和吉四郎氏は，次のような説明を行っている。

「この種事犯[コンピュータ犯罪を指す]の捜査では，犯罪を立証するために，プログラムとかデータを入力してある磁気ディスク，磁気ドラム，磁気テープの内容を明確にしなければならない。しかし，これらのものそれ自体を押収してきてもそれだけでは足りず，その内容を人間の目で見読できるようにする必要がある。例を磁気テープにとると，それに入力されているデータは，ラインプリンターによって印字されてはじめて，その内容が捜査員の目でみられるわけである。この場合，磁気テープそのものを押収してきて，捜査機関の保有する機械によってアウトプットすれば足りるものと考えるかもしれないが，それは不可能である。というのは，コンピュータは，それぞれの機械に特有のランゲージがあって，同機種同号数の機械であっても，ランゲージが異なると，Aという機械で読み込んだデータを収めている磁気テープの内容を，Bという機器にかけてアウトプットすることはできないからである。そのため，磁気テープを差し押さえる場合には，差押えの現場で，そこにある機械を使って，テープの内容をラインプリンターに印字しなくてはならなくなる」[107]。

---

[104] 審議会(ハイテク)第2回議事録(ニフティからの参考人の発言)参照。
[105] 松沢・通信ログ57～58頁。前注をも参照。
[106] 同前注。
[107] 名和68頁。また，廣畑・捜索，差押え70～71頁，河村・捜査実務101問(改訂4版)100頁をも参照。

加えて，既に指摘されている通り，現場では，「プログラムの作成やコンピュータでの分類作業などに相当な技術，人力，時間などを必要とし，かえって問題を生ずることにもなる」[108]から，捜査実務としては，関連性を確認するための分類作業を行うことなく媒体を丸ごと差し押さえておくか，あるいは，対象となるデータとそうでないものとを選別せずにとりあえず大雑把な大量のデータをアウトプットしておき，その後に，それをゆっくり見ながら関連性の有無を確認するという形になっているようである[109]。

また，公判廷で，プリントアウト文書ないし当該転写記録媒体が，確かに対象たるデータを正確にアウトプットして紙に印字したり別の電磁的記録媒体に転写したりしたものであるかが争われる可能性があるから，そのために媒体自体を差し押さえておく必要があるとされる[110]。もっとも，この点に関して，学説では，「電磁的記録を一定のプログラムに従ってアウトプットした者がその成立の真正を公判廷で証言すれば足りる」[111]とする見解があり，これによれば，媒体自体を差し押さえる必要性は否定されうる。しかし，他方で，この同一性(あるいは真正性)は，元の電磁的記録の保管状況，アウトプットしたコンピュータの機械的正確性，プログラムの信頼性，印字の正確性等について，鑑定人の尋問その他の方法により慎重に認定されなければならないという意見もある[112]。さらに，電磁的記録の原本は何なのかについても争いがあるし[113]，また，現行法上，プリントアウト文書ないし関連データの転写記録媒体の位置づけに関する明文の規定も設けられていない。これらの点を考慮すれば，媒体を一括して確保しておこうという捜査実務の基本方針は[114]，賢明であると評価できよう。

このように，アウトプットの慣行については，理論的には，それにより，関連性があるデータのみを取得することが可能となるし[115]，そのような方向での運用が望ましいと思われるものの，捜査の実際は，それができない場合も少なくないのである。

以上示した日本の状況にてらして台湾の問題状況を検証すると，次のようになる。台湾では，プロバイダーなどのインターネット通信業者を被処分者とする場合に行われる差押えは比例原則によるべきであるという捜査手引き 228 条の規定がある。これによれば，台湾の実務上も，プロバイダーなどを被処分者とする場合には，そのサーバー記憶媒体全体に対する差押えの代わりに，プロバイダーにプリントアウト文書ないし関連データの転写記録媒体を作成してもらってそれらのみを取得するというような措置が望ましいと考えられる。他方で，捜査手引き 227 条 4 号は「コンピュータファイルである証拠を現場でプリントアウトしたうえで，被処分者に署名及び押印を求めるべきである」としているものの，

---

[108] 丸谷 65 頁。
[109] 大橋 283 頁参照。
[110] 大橋・基礎編 5，10，189 頁参照。
[111] 安富・ハイテク犯罪 261 頁，新保 161 頁，坂倉 148 頁。
[112] 小田中・コンピュータ関連犯罪 203 頁。
[113] 詳細は，安富・コンピュータ犯罪 227～228 頁＝同・ハイテク犯罪 261～262 頁 ，廣畑・証拠法 89 頁参照。
[114] 大橋 283 頁参照。
[115] 廣畑・検証 11～12 頁，河村・捜査実務 101 問(改訂 4 版)100 頁，的場 96 頁，平良木・刑訴法 I 193 頁参照。

同 228 条 1 号は，「差押えを執行する際にコンピュータの設備の全セット(コンピュータ器機，モニター，キーボード，電源ケーブルなどの設備を含む)を差し押さえておいたほうがよい」と定めている。これらの規定の趣旨は，前掲した名和吉四郎氏の述べたのと同じものであろうと思われる。実際にも，学説上は，犯罪立証という目的には電磁的記録それ自体こそが重要であると述べておりつつも，アメリカの議論を参考に，日本の名和吉四郎氏の述べた技術上の難点と同じ内容の理由をあげているほかに，現場でコンピュータの中にあるデータをアウトプットすることには，作業環境の不良や捜査機関の操作のミスなどが理由でデジタル証拠を毀損させてしまうおそれがより高くなるし，また，長時間を要する場合も稀ではないということも理由に，目標となるデジタル証拠を取り出して可視化・可読化したりすることは現場で行うのは適切でなく，まず目標データを記録した媒体を差し押さえておいた上で，その後，警察機関の実験室などの適切な別の場所に行うほうが望ましいとする見解も一部でなされている[116]。

以上のとおり，アウトプットの慣行は，日本においても台湾においても，プロバイダーを被処分者とする場合を除き，差押えの代替的処分として，実質的な過大差押えを解消するという機能を果たしていないように思われる。

これに対しては，技術上の支障の解消や証拠化のために媒体全体を差し押さえておく必要があるという場合には，媒体と情報の両方を獲得する必要があるわけであるから，そもそも実質的な過大差押えという問題が生じないのではないかという疑問があるかもしれない。しかし，必ずしもそうではない。

確かに，こうした場合においては，技術上の問題や証拠化の必要性という理由から，媒体をも確保しておくという前段階の処分には正当性があるが，だからといって，かような前段階の確保処分としての媒体の差押えによる終局的な占有剥奪の効力が，そこに記録された情報についてまで，当然に及ぶと考えるべきではないからである。つまり，前段階の媒体の差押えに伴い，捜査機関が取得した「情報」については，それを，媒体とは独立した処分の対象となると考えれば，立法論的としては，媒体の差押え後に，その内容を調査するためには，別個の令状を必要とする制度も考えうる。そして，こうした制度を採用すれば，前述した捜査のニーズに対応すると同時に，中華民国憲法23条から導かれる最小化原則をより貫徹することができる。それにもかかわらず，台湾の現行法のもとにおいては，単に法文上は形式的に無体の電磁的記録をも捜索(ないし差押え)の対象としているだけで，かような措置が用意されていないのであり，その点で，媒体と情報の双方を獲得する必要がある事例においても，実質的な過大差押えの問題が生じているのである。

(2)アウトプット物の作成権限と占有剥奪の根拠について

前述した通り，プロバイダーが被処分者である場合，実務上は，相手方のプロバイダーに対象となるデータのみをアウトプットしてもらったうえで，アウトプット物のみを差し

[116] 李・電磁紀錄 1062～1063 頁。

押さえるという形がとられる。これに対し，個人や一般の会社ないしその他の団体が被処分者である場合には，現場で警察官自らがアウトプットを行うということになるが，その法的位置づけは，捜索・差押えないし検証に必要な処分と考えられる[117]。この理解は，捜索・差押えの部分では，台湾の法解釈論としてもそのまま適合するものと考えられる。というのも，台湾刑訴法 144 条 1 項は，「捜索・差押するために鍵・封緘を開けたりしてあるいはその他の必要な処分を行うことができる」と定められており，この規定の趣旨と，日本刑訴法 111 条[118]のそれとは異なるものでないからである。

しかし，必要な処分に当たらない場合にはどう対応すればよいかという点が問題であるし[119]，また，もとより，必要な処分に当たる場合であっても，だからといってアウトプット物を作成するために捜査機関が当然に被処分者のコンピュータなどの設備ないし紙などの消耗品を使ってもよいというわけではないから，捜査側がそれらを使用するための現行法上の根拠は何なのかが問題となる。さらに，現場で作成されたアウトプット物は令状に記載されていない以上，いかなる根拠でそれを差し押さえることができるのかについても問題がある。

これらの問題は，台湾では，あまり意識されておらず，類似する規定をもった日本の関連議論を参照に，台湾の立法論として考えるべき問題点を洗い出したい。その際に，アウトプット物を作成するための転写媒体が捜査機関の物である場合とそれが被処分者の物である場合とに分けて考える必要がある。

A. 捜査機関が持参する場合

日本刑訴法 99 条を根拠に，電磁的記録媒体等を差し押さえずに，目的のデータだけを，あらかじめ捜査機関が持参した用紙ないしフロッピーディスクに印刷したり転写したりすることができるであろうか。

ここでのアウトプット権限について，学説上は，すくなくとも捜査機関が用紙ないしフロッピーディスクを用意し，持参することを，捜索差押令状請求段階において裁判所に対し疎明を行った場合には，もともと令状発付の段階から，被処分者のコンピュータを使用

---

117 的場 95 頁，池田＝前田・刑訴講義 4 版 179 頁脚注(7)参照，安富・捜査法 199 頁，白取・刑訴 7 版 135 頁，安富・刑訴講義(2 版)108 頁。

118 すなわち，第 111 条の前段は「差押状、記録命令付差押状又は捜索状の執行については、錠をはずし、封を開き、その他必要な処分をすることができる。」と定められている。他方，台湾では，記録命令付差押という制度がないが，ここでの論旨には差し支えない。

119 この点，改正法以前の議論を回顧すると，実質的な過大差押えの問題を解消するために捜査機関がアウトプット物を作る場合は，本来の目的物の差押え，あるいはそれに必要な処分とは言えないので，そのような目的でアウトプットすることはできないという見解が多数説であった(河上ほか編・大コンメンタール第二版補遺[吉田]14 頁。井上・コンピュータ(1)62 頁＝井上・強制・任意 269～270 頁，大澤・顧客データ差押え 46 頁，長沼・電磁的情報 46 頁，貴志・ハイテク犯罪 110 頁，新保 148 頁，長沼・46 頁をも参照)。これに対して，いわゆる縮小法理――「大なる令状によって，それに含まれている軽い執行ができる」――によって，差押えに代わってアウトプットすることは当然認められるし，比例原則の要求からも，物に対する差押えの必要がない場合はアウトプットを行うべきであるという帰結になるという少数説が存在していた(審議会(ハイテク)第 4 回議事録参照(括弧内は議事録の発言の引用である)。同少数見解として，的場 96 頁参照。

してアウトプットすることが予定されていると解することができるとする見解がある[120]。また，アウトプット作業を行うことを捜索差押許可状の条件として付記すれば可能であるとの考え方もある[121]。

このうち，前者は，アウトプットを令状の本来的効力の一環として捉えるものであり，後者は，令状に執行の条件を付けるという点にその根拠を求めるものであって，これらの理解によれば，必要な処分という概念を介在する必要はなくなる。しかし，前者については，疎明が行われなかった場合にはどうなるのか，後者については，裁判官が令状に条件を付することができるのかという問題が残る[122]。

以上に照らして台湾の議論を整理すると，次のようになる。まず，前掲した台湾刑訴法144条1項については，従来，それを捜索・差押えという処分における「内在的な」効力であって，本来は，かような規定がなくても差し支えないと理解されてきた[123]。なぜならば，捜索・差押えという本体処分を執行するために鍵や封緘をあけるなど付随処分を行うことは，新たな権利侵害にはならず，本体処分の授権範囲内にあると解されるからである[124]。こうして，台湾の理解では，令状の本来的効力の一環という理解と，必要な処分という理解とが，軌を1つにしたものになる。

他方で，台湾における2001年の法改正の際に，刑訴法128条2項により，裁判官に，捜索(差押え)令状において執行人員に対して適当な指示を行う権限が新しく与えられた。これは，日本の概念に代えて言い換えれば，裁判官が令状に条件を付することができるというものになる。しかし，本条項のいう適当な指示に，捜索・差押えの執行方式の指示まで含まれるかという点については争いがある。この点につき，否定説は，アウトプットというのは執行方式の問題であるから，それを行う権限は本来捜索・差押えという処分における内在的な効力により認められているものであって，その要否についても，現場で捜索・差押えを執行する人員が判断すべき事項であるから，裁判官により指示されるものでないとする[125]。これに対し，肯定説は，アウトプットは執行方式にあたり，捜索・差押えという処分の一環として認められているとする点では，否定説と同様の立場に立ちつつも，裁判官が令状に条件を付けるという形でアウトプットなどの執行方式の要否ないしその順序を指示してもよいとしている[126]。

いずれにしても，アウトプット権限は認められるが，だからといって，当然に，それによって作成されたアウトプット物の占有を剥奪することが認められるわけでない。という

---

[120] 的場95頁。
[121] 小川264頁。
[122] 酒巻・条件の付加8頁以下参照。
[123] 林鈺雄・捜索扣押254頁参照。
[124] 同前注。
[125] 陳・刑訴法3版199～200頁は，本条項のいう適当な指示とは，「捜索の手続きと目的あるいはその範囲をより明確させるものにとどまる」とする。
[126] 林鈺雄・捜索扣押98頁は「各々異なる捜索は，往々として特別な執行方式に絡んでおり，そこで，裁判官は，捜索令状に特別な指示を行うことができる」とする。同見解として，陳瑞仁・新法捜索扣押64～65頁参照。

のも，被処分者のコンピュータなどの設備ないし紙などの消耗品を利用することと，それらの占有剥奪を行うことは，法的には異なる次元での権利侵害とされているからである。つまり，「利用」だけであれば，それを，令状の本来効力の一環か，それとも，必要な処分かと見ることや，条件の付記という形によりそれを正当化することも考えられないわけではないが，「占有剥奪」に至れば，新たな権利侵害が生じることになるから，別個の差押令状が要求されると解すべきだからである。

しかし，台湾においては，独立した差押え令状が存在しておらず，捜索令状による差押えという形となっているから，捜索する必要がない場合には，別個の差押えの行為を行うことができなくなる。この問題を解決するには，新しい立法をもって，日本のように，捜索令状と独立した差押え令状を設けることが考えられよう。

もっとも，ここでの議論の前提は，捜査機関が持参した用紙ないしフロッピーディスクへのアウトプットであるから，被処分者に対して新たな財産権の侵害が生じることはないし，また，電磁的記録媒体の全体を差し押さえられる場合の侵害程度と比べると，その媒体に記録された目的のデータ（アウトプット物）のみを取られる場合の侵害程度がより低いといえるとすれば，日本でいう捜査比例の原則[127]により捜査機関はかかるアウトプット物を持ち帰ることができるという考えもあろう[128]。この考えは，台湾にも適合するであろう。というのも，中華民国憲法 23 条から導かれた比例原則は法の全般に渡った一般的妥当性を有するものである以上は，当然，警察行政の指導的原則にもなるからである[129]。

しかし，こうした考えをとった場合には，次に，差押令状に対象として記載されている電磁的記録媒体自体を差し押さえず，アウトプット物だけを持ち帰るという行為は，法的にいかなる位置づけになるのかという問題が生じる。言い換えれば，かかる行為は，差押えといえるか，それとも，単なる事実行為にすぎないのかである。

この点につき，台湾においては，一般論としては，2001 年の法改正以後は電磁的記録も捜索・差押えの対象となるとされる[130]。しかし，差押えの法的定義は変わっていないから，結局のところ，アウトプットすることだけでは，占有の剥奪が発生することはない以上，それを差押えとはいえないという帰結になる。

これに対して，日本では，差押の段階では，無体物であっても，一定の用紙にプリント

---

[127] ここでいう捜査比例の原則は，行政法の原則であって，憲法の原則でない。すなわち，日本の場合では，従来，行政法学においては，比例原則を日本国憲法から導かれる法原則として位置づけようとする試みがなされてきたが，憲法学においては，ドイツ憲法学における比例原則をめぐる議論が紹介されることは数多くあるものの，比例原則を日本国憲法上の法原則として位置づけるものは少ない（須藤 259～260 頁，高木 211 頁）。また，そもそも，「比例原則」という用語自体も，通用のものにはなっていない（須藤 14 頁，田上・比例原則 2 頁）。

[128] 審議会（ハイテク）第 4 回議事録参照。これに対して，無体物自体は現行法のもとで差押えの対象となっていないから，媒体に対する差押えに代えて，電磁的記録のみを入手することはありえないと示す見解がある（椎橋・刑訴 4 版 101 頁）。

[129] 実際にも，学説上は，日本の「捜査の比例原則」という用語を，中国語である「偵査比例原則」と訳し，それが台湾の刑訴法の重要な原則であると論じる論者がある（たとえば，陳運財・任意偵査 292 頁＝陳運財・正當程序 153 頁，黄朝義・偵査 70 頁，傅・偵査 60 頁）。

[130] 林裕順・基本人權 152 頁，吳・博論 270 頁脚注 30 頁＝吳・照相錄影 308 頁脚注 30 参照。反対説がある（李・電磁紀錄 1057～1058 頁，黄朝義・刑訴三版 234～235 頁参照）。

アウトした時点で有体物に転化することには疑問がなく，したがってこれを一体的・総体的にとらえれば，最終的には有体物を差し押さえたことになるという見解がある[131]。もっとも，これを台湾の現行法に適用し，無体の電磁的記録を一定の用紙にプリントアウトして転写した有体物の占有を剥奪することを，無体の電磁的記録に対する差押えであると捉える考え方もありうる。

しかし，捜査機関が持参する転写用の電磁的記録媒体ないしプリントアウト用の紙媒体などの有体物自体は，被処分者の物でなく，捜査機関の所有物であって，差押えを執行するために必要なツールとしてすでに占有している以上，かかるツールに対してさらにその占有を剥奪することは観念できない。それゆえ，それは差押えの対象物としての適格がないということになろう[132]。

それでは，差押えではなく，検証として行うという方法は[133]どうであろうか。確かに，検証による場合，電磁的記録媒体に目標たるデータを転写させたり，紙媒体に印字したりすることは，検証の結果を記録する行為であるから，捜査機関が電磁的記録媒体や紙媒体を持参したうえで，それに記録するのが，むしろ自然であるといえる。

しかし，このように解すると，捜査側がデータの内容を全く認識することなく，そのすべてをコピーするような場合は，検証を行ったとはいえず，そのコピーの結果である転写物やプリントアウト文書を検証の結果の記録と解することはできないのではないかという問題が生じる。

B. 被処分者の財産である場合

次に，アウトプットしたデータの転写媒体が被処分者の財産である場合について検討する。この場合に，データをアウトプットして，被処分者の財産である媒体に転写したうえで，その占有を剥奪することができるであろうか。

この点，複製物やプリントアウトした用紙そのものの取得を目的として，その作業を可能にする条件を捜索差押許可状に付することも，台湾刑訴法 128 条 2 項のいう「適当な指示」と認められるとすれば，令状に条件を付すことにより，それが可能となると考えられないわけではなかろう[134]。さらに，オリジナルの記憶媒体が押収されることに比較すれば被処分者の不利益はより小さいのが通常であるから，令状にかような条件が付されていなくても，被処分者の財産である，データを転写した媒体の占有を取得することが認められる

---

[131] 新保 148 頁。類似する見解として，的場 95 頁，安富・ハイテク犯罪 164 頁，同・コンピュータ犯罪 150 頁参照。

[132] 前注参照。そして，長沼・電磁的情報 46 頁，的場 96 頁をも参照。また，台湾刑訴法 133 条 1 項は「証拠になる物あるいは没収できる物を差し押さえることができる」と定められており，その旨は日本刑訴法 99 条のそれと異ならないものであろう。

[133] 的場 96 頁は「捜査官側の用意した記憶媒体や印字用紙等を用いてこれらの作業を行うときは，結局差押物はないという結果になる上，いかなる情報が捜索差押手続によって捜査官側に渡ったかを明らかにする手段がないことにもなるので，捜索・差押えとしてではなく，検証として行うべきであろう。」とする(同 97 頁の説明をも参照されたい)。また，井上弘通 338 頁も参考になる。

[134] 林鈺雄・捜索扣押 86 頁及び的場 96 頁の説明が参考になる。

とする見解もある[135]。

しかし，いずれの見解についても疑問視すべき点がある。まず，前者の見解については，前述した通り，台湾において，令状に執行方式に関してまで条件を付すことができるのかについて争いがある。また，後者の見解については，オリジナルの記憶媒体が押収されることに比較すれば被処分者の不利益が小さいからといって，当然に，アウトプット物を占有してもよいとはいえないであろう。というのも，アウトプット物は，オリジナルの記憶媒体とは別の有体物であり，それを差し押さえることによって新たな法益の侵害が生じるので，そのためには別個の令状が必要となるはずだからである。

次に，日本のいう検証令状を台湾にも導入することによる対応の可能性を検討すると，既に指摘されているように，検証自体はプリントアウト物の占有取得を内容とするものではないから[136]，検証令状をもって，被処分者の所有する用紙に情報をプリントアウトした上で，それを差し押さえることはできないであろう。

もっとも，検証許可状の請求に際して，同時に，プリントアウト物を対象とする差押許可状を請求し，発付を受けておけば，プリントアウト物を仕上げた上でそれを差し押さえることはできる[137]。このことは，差押えの場合にも妥当し，差押令状に，本体の記録媒体のみならず，「被疑事実と関連性のあるプリントアウト文書」も差し押さえるべきものとして明記しておけば問題がないと解される[138]。実務上も，そのような運用がなされているようである[139]。

しかし，台湾では，独立した差押令状が存在しておらず，捜索令状による差押えという形になっている。そこで，台湾にも，日本のような独立した差押令状という制度を導入することが考えられる。しかしながら，そうすると，同時に差押え令状を請求していない場合，同時に請求したが差押え令状の発付が認められなかった場合，あるいは，令状申請の手続に落ち度があったがゆえに差押令状に「被疑事実と関連性のあるプリントアウト文書」などの明記がなされなかった場合には，どのように対応すればよいのかという問題が生じる。

4．改正法について

以上の通り，改正法が成立する前にも，データのアウトプットという捜査手法はすでに慣行として行われていたが，その法的根拠については争いがあった。そのため，立法により，かかる手法のための明確な法的根拠を定める必要があるという指摘もなされていた[140]。今回の改正で新設された「差押えに代わる処分」（日本刑訴法 110 条の 2，222 条 1 項）[141]は，

---

[135] 的場 96 頁。

[136] 小川 265～266 頁，黄＝呉・刑訴法論（上）7 版 255 頁。また，河原 72 頁，井上弘通 339 頁をも参照。

[137] 同前注。

[138] 的場 95 頁，河村・捜査実務 101 問（改訂 4 版）101 頁参照。

[139] 前注のほかに，井上・コンピュータ（1）62 頁＝井上・強制・任意 270 頁，貴志・ハイテク犯罪 110 頁をも参照。

[140] 長沼・コンピュータ犯罪 12～14 頁参照。

[141] 日本刑訴法 110 条の 2 の規定は，以下の通りである。「差し押さえるべき物が電磁的記録に係る記録媒体であるとき

かかる指摘を実現したものと考えられる[142]。これに対して，台湾では，かような手法は，当然可能なものとして行われてきている。これは，法の明確性からいって，望ましくないと思われる。この意味で，日本において今度新設された差押えに代わる処分は，台湾にも参考するに値するものがある。それにとどまらず，以下に述べる通り，かかる規定の新設は，従来の慣行の明文化を超えた価値をもつものであると考えられる。

(1)「差押えに代わる処分」の新設の実益

前述した通り，実質的な過大差押えの問題に対しては，台湾においても，日本と同様に，プロバイダーを被処分者とする場合においては，サーバー記録媒体などに対する差押えを行うことを出来る限り避けるために，事前の連絡と調整により，プリントアウト文書ないし別の転写記録媒体の作成を先行するほうが望ましいとされている。実務上も，捜査に差し支えない範囲内において，この方向へ進んでいくように思われる。

しかし，実質的な過大差押えという問題は，プロバイダーの場合のみならず，銀行その他の大型コンピュータセンター(例えば，中小企業の会計帳簿などの作成管理の業務を営む企業)が所持する記憶媒体を差し押さえる場合においても同様に生じうるものである[143]。にもかかわらず，実務上，かような場合には同様な配慮を払っていないのが台湾の現状である。

この問題に関して，日本では，プロバイダーでない第三者の場合にも，事前の連絡と調整によるプリントアウト文書ないし別の転写記録媒体の作成を原則とすべきとする見解が有力となりつつあるが，どのような場合にそれが要求されるかについては差異がある。例えば，コンピュータ会社に処理を委託しているような場合あるいは１台のコンピュータを数社で使用している場合のように，第三者に「大きな損害」を与える可能性がある程度で十分であるとする見解がある一方で[144]，例えば，被疑者の取引状況を確認するために，直ちにかかるデータを含むと思われる電磁的記録媒体を差し押さえることにより，銀行の業務を麻痺させ，取引秩序に重大な混乱を招く事態になる場合のように，第三者に「致命的な損害」を与える可能性がある程度を想定する見解もある[145]。

は，差押状の執行をする者は，その差押えに代えて次に掲げる処分をすることができる。公判廷で差押えをする場合も，同様である。　一　差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し，印刷し，又は移転した上，当該他の記録媒体を差し押さえること。　二　差押えを受ける者に差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写させ，印刷させ，又は移転させた上，当該他の記録媒体を差し押さえること。」

142 審議会(ハイテク)第４回議事録参照。というのも，こうした法根拠の問題につき，今般新設された差押えに代わる処分の関連規定により抜本的な解決がなされたからである(河上ほか編・大コンメンタール第二版補遺[吉田]14～15 頁)。すなわち，この規定の新設の立法趣旨は，アウトプット物の作成自体ないしそのために被処分者の器機(コンピュータ設備など)ないし媒体(フロッピーディスクや紙など)を利用すること，及び最後にできたアウトプット物を占有することなどのすべてを，一連の手続を強制的に行うものと見なした上で，かかる一連の手続の全過程を，１つの差押えの処分に当たるものと擬制して認めたものである(杉山＝吉田・情報処理の高度化(下)61 頁，108 頁(注 7)参照。)。

143 柳 307 頁。

144 安富・コンピュータ犯罪の捜査 30 頁参照。

145 原田・コンピュータ 225～226 頁参照。

ここで問題となるのは，以上に示した，プロバイダーの場合とそうでない場合との区別，大きな損害ないし致命的な損害が生じる場合とそうでない場合との区別が，果たして合理的なのかである。

この点については，プロバイダーの営業は，その規模によって，数千ないし数万あるいはそれをはるかに超えた人数の市民の利益が絡むという特色があるのに対して，一般の個人，会社，企業ないしその他の団体などを対象者とする場合には，このような特色がないということから，その区別の合理性を基礎づける見解もありえよう。つまり，プロバイダーを対象者として記録媒体を差し押さえる場合には，それによる法益の侵害性は他の場合より重大であると同時に，その要保護性を判断するための基準も明白であるので，プロバイダーの場合に対してのみ特別に取り扱うということである。このような立法は，比例原則と並んで法の明確性の原則[146]にかなうものとして合理性があると考えられる。

もっとも，プロバイダーにも小規模のものもあり，そのような場合には，数千ないし数万あるいはそれをはるかに超えた人数の市民の利益が関係するという特色がなくなるため，それを区別して扱うことが，比例原則及び明確性の原則にかなうということが言えなくなる。つまり，プロバイダーの場合であっても，ケースバイケースによる対応が必要となる場面があるとすれば，プロバイダーを特別に取り扱う合理性が成り立ちえなくなるということである。

今回新設された差押えに代わる処分の関連規定の趣旨は，第三者への過大な処分の回避にあるとされ，そこでは，プロバイダーなどの通信業者が想定されているのは間違いないが[147]，少なくとも文言上はかような区別は取られていない。そして，前述した通り，プロバイダーの場合だからといってその侵害性が必ずしも重大でない場合もあるから，その規定の適用をプロバイダーの場合に限定して解釈する正当性もないと思われる。

このような理解のもとにおいては，改正法は，プロバイダーでない場合及び致命的な損害といえない場合における実質的な過大差押えの問題にも対応するものということになる。そうだとすれば，改正法は，これまでの実務慣行によってカバーされていない保護の間隙を補う機能を有するものと評価することができよう。

これに対して，台湾では，2001 年の法改正により，電磁的記録も捜索・差押えの対象としたため，電磁的記録をアウトプット(あるいはコピー)することは，差押えに代わる処分とは解されない。しかし，他方で，占有の剥奪という従来の差押えの定義は変わっておらず，電磁的記録をアウトプットやコピーすることだけでは何も奪われていないから，結局のところ，それを，無体の電磁的記録に対する差押えとはいえなくなるのである。以上の

---

146 アメリカ連邦憲法修正 5 条と同修正 14 条の系譜に連なるとされる日本国憲法 31 条は，適正手続を保障する一般的規定とされると同時に，「法律の留保の原則を宣言したもの」でもあるとされており ，その内容は，実質的には，ドイツでいう法の明確性・特定性(Normenklarheit und Normenbestimmtheit)の原則――法律の留保の原則(Grundsatz des Gesetzesvorbehalts)とも呼ばれる――と異ならないものと思われる(下山(新版)132 頁，早川 131 頁，橋本・全集憲法(改訂)245 頁，井上正治・全訂 30 頁，中村 6 頁，高橋和之 10 頁参照)。

147 河上ほか編・大コンメンタール第二版補遺[吉田]14 頁，審議会(ハイテク)第 6 回議事録，壇上・サイバー関係 35 頁，幕田・捜査法解説 3 版 228 頁参照。

とおり，2001 年の法改正は，解釈論上の混乱を招いており，立法として適切なものだとは思われない[148]。

これに対し，日本の場合には，アウトプットやコピーすること自体は，差押えではなく，差押えに代える処分――すなわち，差押えの執行の一方法――と位置づけられているがゆえに，従来の差押えの定義を維持することができるとともに，解釈論上の混乱を生じさせることもない。それと同時に，日本の今般の改正法によれば，前述した２つの問題が，以下のように解決されている。

すなわち，まず，①捜査機関が持参したフロッピーは，被処分者のものでなく，捜査機関の職務上の所有物であるので，台湾の現行法のもとでは，それには差押の対象物の適格がない，という問題点については，日本の改正法が，差押えの適格がない捜査機関の持参物を，差押えの適格がある物件と擬制するという趣旨であるとすれば，捜査機関の職務上の所有物であっても，差し押さえることができるという帰結になる。

次に，②電磁的記録媒体の内容を全く認識することなく，そのなかにあるすべてのデータをコピーしておくような場合は，このコピーの結果――転写物やプリントアウト文書――を検証(五官の作用による認識)の結果の記録と解しかねる，という問題点については，新設された差押えに代わる処分の規定を適用すればよいから，検証という制度を利用する必要がなくなり，転写物やプリントアウト文書を検証の結果の記録と解すことができないという問題は生じない。

(2)残された問題点

以上の通り，今回の差押えに代わる処分の新設は，日本におけるこれまでに存在した問題への有益な対応であり，台湾の立法論にも参考となるものがあると思われるものの，そこには，なお以下のような問題点が残されている。

A. 無形のアウトプットへの不対応

デジタル証拠の収集・保全の手続の問題に対応するには，無形のデータ自体を処分の対象とする必要性があるとの指摘がなされてきたが，今般の改正法は，基本的には，有体物のみを対象とする現行日本刑訴法の枠をそのまま維持するものである。このことは，「差し押さえるべき記録媒体に記録された電磁的記録を複写し，印刷し，又は移転させた他の記録媒体を差し押さえる」とする日本刑訴法 110 条の 2 における「差し押さえるべき記録媒体」，「他の記録媒体」という文言からも窺える。同条の性質は，差押えをするものが，差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写するなどして取得するという一連の手続を強制的に行うものであって，当該他の記録媒体の取得過程全体として「差押え」に当たるものだとされているのである[149]。つまり，改正法によると，差し

[148] 実際にも，学説上は類似する指摘がなされている(林裕順・基本人權 156 頁参照)。
[149] 河上ほか編・大コンメンタール第二版補遺[吉田]17 頁。

押さえるべき記録媒体を「占有」しながらそこにあるデータを転写した物(すなわち，日本刑訴法 110 条の 2 の「他の記録媒体」)に対する「占有」をも差押えの一環としたうえで，終局的に「有体物である転写物」の「占有」を剥奪することにより，有体物の占有を剥奪するという差押えの従来の定義が当てはめられるわけである。

確かに，このような設計によって，現場で紙媒体ないし電磁的記録媒体を利用する「有形のアウトプット」の場合には，ある程度，問題に対応できるであろう。しかし，それは，例えば，オンラインでデータをダウンロードしたりするなどの「無形のアウトプット」の場合には対応できないという問題がある。

これに対しては，無形のアウトプットの根拠としては，検証が考えられるから，そもそもそれに対応する必要はないという反論があるかもしれない。実際にも，学説上，データを検索したりダウンロードしたりするような捜査の手法を検証と解すことができるとすれば，オンラインでの検証(すなわち，無形のアウトプット)が現行法上認められるという見解が一部で現れてきている[150]。もしこの見解が正しいとすれば，台湾の場合にも，裁判官や検察官の職権による(無令状の)検証という制度があるから，無形のアウトプットに対応するために新しい立法をする必要性が薄くなると解されうる。

しかし，オンラインで膨大なデジタルデータをダウンロードしたりするというような捜査手法は「人の五官の作用による認識」という検証の従来の定義には当てはまらないから[151]，無形のアウトプットという捜査手法を検証と解すことはやはりできないと思われる。というのも，かような捜査手法においては，人の五官は全く関与しておらず，プログラムによる自動的作業が行われるという形になるし，また，そもそもデジタル値は人の五官では認識できないものだからである[152]。

これに対して，台湾の場合には，形式的には，電磁的記録をも捜索・差押えの客体としているようにみえるため，オンラインでデータを取得することを，電磁的記録への差押えと解釈する余地があるかもしれない。しかしながら，差押えの定義は，いまでも占有の剥奪とされているから，かような解釈は，従来の差押えの定義ないしその適用の基準・原則と調和せず，法解釈と法の文言との間に不一致と混乱を引き起こしてしまうから，妥当ではない。さらに問題となるのは，もしこの解釈が認められるとすれば，オンラインでデータを取得する範囲を画定するための基準が，現行法上は全く用意されていないため，無制限の一般的・探索的差押えをみとめるものとなってしまうことである。他方で，検証については，台湾の職権による検証の定義は，日本の令状による検証と異なるものではないから，結局のところ，日本の場合と同様に，台湾の場合にも，オンラインでデータを見たり取ったりすることを検証とは解しがたい。そこで，台湾において，無形のアウトプットに対応するためには，新たな立法を考える必要がある。

---

[150] 井上・コンピュータ(2)53～54 頁＝井上・強制・任意 276～277 頁を参照されたい。

[151] この点，井上教授自身も明確に意識されておられる(前注参照)。

[152] 井上・コンピュータ(2)53～54 頁＝井上・強制・任意 276～277 頁。

B. 事後救済の欠如

次に指摘すべき改正法の問題点は，事後救済が設けられていないという点である。この点につき，日本刑訴法 110 条の 2 の法的位置づけを「差押えの擬制」とする見解があり[153]，この理解によれば，差押えに代わる処分も準抗告の対象になりうると解する余地がある[154]。

しかし，立法当局の説明によると，本条は，「あくまで通常の差押えの執行方法として位置づけられるもの」[155]，すなわち，執行方式の選択肢としての代替的処分にすぎないとされている[156]。そのうえで，立法過程においては，「準抗告につきましては，これは，現行法では，いわば特別な財産権侵害のパターンの場合の特別な救済手続として設けられておりますので，基本的に複写の場合には，財産権侵害がない――準抗告で救済しようとしている意味での財産権侵害はないということで，基本的には準抗告の対象にはならないということになると考えております。」[157]との説明がなされている。

以上の通り，日本の改正法のように，有体物のみを対象とする改正前の法的枠組を維持すると，準抗告を認めるか否かの基準は財産権の侵害の有無に求められることになるから，データを複写・転写する行為は，有体物に対する占有の剥奪を前提とする財産権の侵害にはならず，理論的に事後救済を認めることができないことになってしまうのである。

これに対して，2001 年の台湾刑訴法改正は，電磁的記録をも捜索(差押え)の対象として旧来の条文に追加し列挙しているから，形式的には，電磁的記録をコピーするだけでも，現行刑訴法 416 条の準抗告の対象となりうると解される[158]。しかし，上記のとおり，電磁的記録をコピーするだけでは，通常は，財産権上の損害に伴わないし，また，占有の剥奪が発生しないから，結局のところ，電磁的記録をコピーすることを，416 条の「差押えの処分」にあたると解するのは，やはり困難である。

ここで問題の核心は，仮に，電磁的記録それ自体を捜索・差押えの対象としようとすれば，旧来の捜索・差押えの定義ないしその適用の基準・原則も電磁的記録の特性に沿って適切な調整を行う必要があるのに，2001 年の法改正はこのような調整を行っていないという点にある。

その解決策としては，日本のように，有体物のみを対象とする枠組みを維持しながら，別途，差押えに代わる処分を新設することが考えられる。このような立法設計をとること

---

153 指宿・サイバースペース 86 頁。審議会(ハイテク)第 6 回議事録をも参照。

154 審議会(ハイテク)第 6 回議事録参照。

155 河上ほか編・大コンメンタール第二版補遺[吉田]16 頁。

156 審議会(ハイテク)第 6 回議事録参照。この点，学説も，同調である(杉山＝吉田・情報処理の高度化 19 頁)。

157 審議会(ハイテク)第 6 回議事録。そして，田中 104，107 頁をも参照。

158 実際にも，学説的には，台湾刑訴法 122 条の規定は，無体の電磁的記録を捜索・差押えの客体として列挙している以上，文書の内容を撮影しそのデジタルの画像ファイルを取得することは，実質上は差押え処分に準じるものであるから，それに対しての準抗告を認める余地があるように思われるとする見解がある(呉・博論 270 頁脚注 30＝呉・照相錄影 308 頁脚注 30 参照)。しかし，捜査機関が証拠となり得る有体物の文書を撮影する行為は，既存の電磁的記録を取得するものでなく，新しい電磁的記録を改めて作成するものであるから，こうした場合でいう電磁的記録の取得が，果たして 122 条のいう電磁的記録の取得に当たるものなのかは疑問がある。というのも，立法者が想定した 122 条のいう電磁的記録の取得とは，既存の電磁的記録の取得であると思われるからである。

によって，従来の捜索・差押えの定義・基準・原則をそのまま援用することができる。しかし，そうすると，前述したように，事後救済の制度を設けることができなくなるという問題が残る。

そこで，台湾の立法論としては，むしろ，無体の情報の特性に相応しい捜索・差押えの新定義を立て，この新定義に沿って，あるべき適用の基準ないし原則を検討し，無体の情報を対象とする捜索・差押えの制度を構築するほうが望ましいと思われる。これによれば，事後救済の論拠も，有体物に対する占有の剥奪を前提とした差押えという制度のもので理解されてきた財産権の侵害の有無という点ではなく，無体の情報の特性に相応しい捜索・差押えの新たな定義・基準・原則に求められることになる。

C．順序づけと実効性の担保について

最後に，今般改正された日本刑訴法 110 条の 2 が「代替的執行と本来的処分との間に順序づけの規定をおかなかった」[159]という指摘について検討することにしたい。この点に関し，法制審議会刑事法部会において立法当局は次のような説明を行っている。

「現行法が物を対象にした体系をとっているから，それを踏まえてというだけではなくて，物についても証拠として意味を持っているのはそこに含まれている情報なのですね。しかし，それを確実に，ほかから引き離して保全する。完全な形で，オリジナルとして保全するためには，物自体を押さえるのがベストなので，そういうことでやっているわけです。それと同じことが，データなどについても言えるのではないか。そういう意味で，証拠としての完全性を維持しながら，捜査機関なら捜査機関の保管のもとに置くというのが，正に現行法で言っている証拠の保全手段としての差押えであり，それが基本になるだろう。だけれども，保全の完全性という点で一歩譲っても他の利益を優先させるべき場合があるとすれば，次善の策として中身を複写する形で保全してきてもいい，そういうことなのです。」[160]

かような実務の考えからすると，順序づけは令状の執行方法に属する事項である以上，それは捜査機関に任せられるべきものであるから，「順序づけ等の規定をおかなかった」わけではなく，「順序づけ等の規定をおく必要はない」ということになろう[161]。

しかし，そうすると，本条には，実効性の担保が欠けているという点が問題となってくる。というのも，順序づけは捜査機関の判断に委ねられるものであるとすれば，捜査機関への制約にはならないからである[162]。

これに対し，台湾の場合には，仮に，刑訴法128条2項にいう「適当な指示」の範囲に「執

---

[159] 長沼・コンピュータ犯罪 14 頁。

[160] 審議会(ハイテク)第 6 回議事録。

[161] 河上ほか編・大コンメンタール第二版補遺[吉田]15 頁，杉山＝吉田・情報処理の高度化 19 頁参照。

[162] 長沼・コンピュータ犯罪 14 頁参照。これに対して，差押えに代わる処分をとるかの選択は差押を執行する者に委ねられるが，本来の差押による場合は「処分の相当性」ひいては憲法 35 条 1 項にいう「正当な理由」を欠く処分として，準抗告で取り消されることもあり得るとする見解もある（福井・刑訴講義 5 版 150 頁。同解として，田口・刑訴 6 版 113 頁参照)。

行方法」も含まれるという立場にたつと，上記の問題が解消されよう。というのも，その順序につき，裁判官が個別事案ごとに指示する形になる以上，法が順序付けの規定を用意する必要がなくなる一方，捜査機関は裁判官が令状に命じた順序付けに関わる適当な指示を遵守しなければならず，この意味で，捜査機関への制約となるからである[163]。しかし，裁判官が順序付けに関する指示をしなかった場合はどうすればよいかという問題は残る。

Ⅱ．データを検索・検閲する場面

続いて，蔵置されたデータを検索・検閲する場面を検討する。ここでの議論を展開するに先立ち，まずは，用語の意味を明らかにしておこう。ここで，「検索」とは，フロッピーディスクなどの電磁的記録媒体の中から目的の情報(データ)を探し出すまでの手段を指す[164]。そして，「検閲」とは，コンピュータのモニターに映ったり紙媒体にプリントアウトしたりしたデータを見ながらその内容を認識することを意味する。

最初に日本の問題状況からみていくと，改正法成立以前に，こうした検索・検閲を行うための手段としては，捜索と検証が考えられてきたが，それぞれにつき，以下のような問題点があった。

まず，捜索とは，日本刑訴法99条1項に規定する証拠物又は没収すべき物を発見するために探し出す行為と理解されており，そのため，捜索の対象は，差押えの対象に限られるとするのが通説である[165]。そして，検証とは，「五官の作用により物(人の身体を含む)の存在及び状態を認識することである」[166]と定義されてきた。

こうした定義を見るかぎり，捜索も「五官の作用による認識」――例えば，何かを探し出すために，まず見たり聞いたりすること――の要素を含んでいるのは間違いないが，捜索の場合の「五官の作用による認識」は，あくまで，捜索の本来の目的である証拠物ないし没収すべき物の発見のための一手段にすぎない[167]。これに対して，検証の本来の目的は，証拠物などの発見ではなく，既に発見された証拠物を対象として，五官の作用によりその外形，状態ないし内容を認識することであるから，五官の作用による認識内容の証拠化自

---

163 檢察機關實施搜索扣押應行注意事項§15「捜索あるいは差押えを実施する際に，裁判官の捜索令状において執行人員に対する指示を守らなければならず，捜査事件の犯罪事実[を解明するため]のニーズに応じて捜索を執行し，標的を特定せず漫然としての捜索を行ってはならない。」(警察機關執行搜索扣押應行注意要點§11もこれと同じ内容が定められている)。また，林鈺雄・捜索扣押98頁以下をも参照。

164 井上弘通339頁。

165 日本刑訴法102条2項の規定が，明文で，「押収すべき物」という限定を置いているという点が主な理由になる(井上・傍受99～100頁参照)。台湾でも，同様に解されている（林富郎・通訊監察16，40頁注22参照。通説であり，そして，主な論拠は，台湾刑訴法122条は明文で「物件(同条1項)」「差し押さえるべき物(同条2項)」という限定が置かれている点に求められる)。

166 小野・ポケット(上)285頁。同494頁以下をも参照。同解として，黄＝呉・刑訴法論(上)7版255頁，陳樸生・刑訴重訂十版251頁参照。

167 河村・捜査実務101問(改訂4版)108頁参照。最決昭和55年10月23日刑集34巻5号300頁をも参照。同解として，鄭(他)・新編六法の台湾刑訴法212条矢印部分の説明参照。

体が目的である[168]。

以上の日本の理解は，基本的には台湾の場合にもそのまま適合するものであるように思われる。というのも，台湾でいう捜索・差押えないし検証は，制度上は日本のそれとは相違点があるけれども，その定義自体は，日本における定義と異ならないものだからである。

台湾の現行法のもとで，データを検閲しようとするのであれば，捜索ではなく，検証によるべきことになろう[169]。というのも，こうした場合，その処分の本来の目的は，データの内容を認識することにあるので，(裁判所や検察官の職権による)令状によらない検証という制度の目的に合致しているからである[170]。もっとも，データの内容の認識は，物理的な現象の認識にはあたらないので，それが五官の作用による認識と定義された検証という制度に適合するかどうかという点は問題として残る。

他方で，以上に述べたのとは異なり，データを検索しようとするのであれば，検証ではなく，捜索によるべきことになろう。なぜなら，その本来の目的が，検閲(検証)の対象となるデータを発見するという点にあるからである。そうすると，日本のいう，いわゆる検証のための捜索は認められるかどうかという問題が生じる。

この点，台湾では，無体の電磁的記録それ自体も捜索の対象であると，現行法上，明示されているから，文言上は，捜索令状さえあれば，検証のための捜索が認められていると解されうる。

これに対し，日本の通説によれば，捜索の対象は，差押対象物に限られ，無体のデータ自体は，差押えの対象にはならないから，それを発見するための捜索を行うことはできない[171]。また，検証の対象であるデータを発見するための捜索，すなわち，検証のための捜索も，現行法上は認められないことになる[172]。もっとも，検証の対象となるデータを探す行為がおよそ認められないわけではなく，それが検証に必要な処分として認められる場合もあると解されているが[173]，しかし，それが実質的な意味での捜索という程度にまで至る場合には，検証に必要な処分として認められる範囲を超えており，許されないことになるのである[174]。この日本の理解から台湾の現行法を再考すると，次の２点の示唆が得られる。

第１に，台湾の現行法は，電磁的記録を捜索の対象として定めているとはいえ，捜索・差押えの定義は従来のままである。従来の捜索・差押えの定義からすると，前述の日本の

---

168 同前注。

169 証拠の「発見」という文字は検証の意義に合わないとされる(鄭(他)・新編六法の台湾刑訴法 212 条矢印部分の説明を参照)。これに対して，学説上，現行法の検証を任意的な処分と解する立場の論者が，強制的な検証を行う場合は検証でなく，捜索によるべきであると主張する(柯・刑事程序 276 頁脚注 9 参照)。この主張からすると，証拠を「発見」するための手段である捜索をもって，発見した証拠の内容を五官で「認識」するための処分である検証を行うことになり，検証と捜索とのそれぞれの定義との間には齟齬があるように思われる。

170 検証の目的は，既に発見された証拠物件を五官の作用による認識で直接に調べるものである(黄＝呉・刑訴法論(上)7 版 255 頁，及び鄭(他)・新編六法の台湾刑訴法 212 条矢印部分の説明を参照)。

171 井上・傍受 99～100 頁。前掲注 97 に挙げた文献をも参照。

172 井上・傍受 99～100 頁参照。反対の論者(少数説)として，井上弘通 339～340 頁参照。

173 川出・コンピュータ犯罪 6 頁。

174 井上・コンピュータ(1)62 頁＝井上・強制・任意 271 頁。同解として，長沼・コンピュータ犯罪 13 頁，田口・刑訴 6 版 113 頁参照。

通説と同様に，「捜索の対象は，差押対象物に限られ，無体のデータ自体は，差押えの対象にはならないから，それを発見するための捜索を行うことはできない」という帰結になるはずである。それにもかかわらず，法律上は，電磁的記録も，捜索・差押えの対象としている点で，理論上の一貫性を欠いていると言わなければならない。

第２に，台湾において，検証という制度は，通説によると，無令状での検察官の職権による強制処分であると位置づけられており，日本においては認められていないと解されている検証のための捜索というものが，台湾の場合には，当然に認められるものとして行われてきている[175]。ここで考えるべき問題は，次の２点である。①捜査中における強制的な検証の権限を，実質的な捜査の主体となっている警察官には当たらず，形式的な捜査の主体である検察官にのみ付与するという現行法の設計は，立法論として，果たして妥当なのか。②検察官も，捜査機関であるのは間違いないのに，それを中立の審判機関である裁判官と同視し，令状なしでの職権による強制的な検証を行う権限を与える立法を正当化することができるのか。

以上の２点を考える際に，日本の関連議論から有益な示唆が提供される。そのうち，とりわけ，井上教授がなされた，「多数の加入者の受信ファイルが収録・管理されているコンピュータないし記憶媒体につき，果たして目的の通信を識別するための捜索ないし点検を行うことができるかには，疑問も感じられなくはない」[176]，及び「サーバー……記憶媒体内に蓄積されている被疑者宛のメールの中に関連性のあるものが含まれている蓋然性があるからといって，それらをすべて，検証という形で点検することが許されるものかは，疑問なしとしない」[177]という指摘が興味深いものである。

この指摘は，日本の問題状況並びに改正法の問題点を明るみに出しており，台湾の立法論にとっても極めて有益な示唆に富むものである。そこで，以下では，井上教授のこの指摘をもとに，この問題をより深く掘り下げて検討することにしたい。

１．検証令状による場合

(1)関連性・蓋然性がある場合

検証令状により，前掲の【例 3】におけるＹの「Yman@chanxx.co.jp」アカウントに蔵置されたメールを点検・検閲することができるであろうか。この点につき，井上教授は，次のような指摘をされている。

「……[最初の発信元の被疑者であるＹ宛]のメールの中に関連性のあるものが含まれている蓋然性があるからといって，それらをすべて，検証という形で点検することが許され

---

[175] これに対し，反対説があり，すなわち，検証は任意的な処分に限られるとされ，強制性を帯びる場合は，検証でなく，捜索という制度によるべきであるとされる(柯・刑事程序 276 頁脚注 9 参照)。これによると，検察官がその職権により，強制性を帯びる検証のための捜索を行うことができないという帰結になるはずだろう。

[176] 井上・コンピュータ(1)60 頁＝井上・強制・任意 265 頁。

[177] 井上・コンピュータ(1)62 頁＝井上・強制・任意 271 頁。

るのかは，疑問なしとしない。そのような点検はまさに捜索にほかならないのであるが，検証のための捜索ということは，現行法上は認められていないのである。」[178]。

仮に，媒体自体が検証の対象であるならば，プロバイダーのサーバーないし記憶媒体内に蓄積されている「Y宛のメールの中に関連性のあるものが含まれている蓋然性がある」以上，当該媒体全体を検証することができるという結論になるはずであろう。なぜなら，有体物のみを直接の処分の対象とする日本刑訴法のもとにおいては，当該プロバイダーのサーバーないし記憶媒体という有体物の全体が検証の対象になるのであり，検証の対象である有体物が既に発見された場合に，さらに，実質的な検証の対象であるデータを発見するための「検証のための捜索」を観念する必要はないと解されるからである。

しかし，前述した実質的な過大差押えの問題を視野に入れた場合，有体物たる媒体は検証の形式的な対象にすぎず，同媒体に記録されたデータこそが検証の実質的な対象であると解するのであれば，検証のための捜索という問題が生じてくるのである。

ここから，台湾の解釈論にも有益な示唆が提供されよう。まず，台湾でいう捜査としての強制処分の検証とは，日本のそれと異なり，検察官が職権で令状なしに行うという形になっているが，基本的にはその対象が有体物とされ，かつ，捜査事件に関わる場所ないし物件に限られるとされるという点で，日本でいう検証の場合の同様である。そして，従来は，膨大なデータを記録した電磁的記録媒体も，一般の物件と同様に，そこに証拠となるデータが存在する蓋然性さえあれば，媒体の全体を検証することができるとされてきた[179]。しかし，前掲した井上教授の見解から再考すると，かような蓋然性があることが，電磁的記録媒体の全体を１つの検証の対象である「物件」とみなしてよいという従来の理解については，実質的な妥当性を欠く場合もあるとすれば，すくなくとも立法論的には再検討の余地があるように思われる。すでに指摘されているように，犯罪の立証にとって実質的に意味があるのは，媒体ではなく，その中に記録された無体の情報であるし[180]，また，電磁的記録とその記録媒体が物理的に結合していないことからも[181]，関係する情報を記録した蓋然性のある媒体全体を１つの検証の対象とする台湾の現行法は不合理であるということができる。

(2)関連性・蓋然性を確認するための場合

次に，「被疑事件に関連するかどうか分からない段階で，まさにそのような関連性があるかどうかを判別する目的で，多数の電子メールの内容を閲覧するということが，現行法の検証の枠内で果たしてできるか」[182]という点を検討する。【例 3】についていえば，最初の発信元の被疑者であるＹのアカウントが設置された媒体が特定できないために，捜査機

---

[178] 井上・コンピュータ(1)62 頁＝井上・強制・任意 271 頁。井上＝池田 89 頁，長沼・コンピュータ犯罪 13 頁も参照。
[179] 検証は「事件に関係する物件を検査する」（台湾刑訴法 213 条 5 号）ことを行うことができる。
[180] 川出・コンピュータ犯罪 4 頁。
[181] 川出・コンピュータ犯罪 1～2 頁。
[182] 井上・コンピュータ(1)62 頁＝井上・強制・任意 271 頁。

関がそれを確認するため，媒体に蔵置された多数のメールを見ようとするような場合が，これに該当する。

こうした場合は，被疑事件に関連するかどうかが分からない段階であるから，媒体自体は未だ検証の対象にはなっていない。それゆえ，媒体に記録されたデータの確認は，当該媒体が検証の対象であるかどうかを判断するために必要な手段であり，それは，日本のいう「検証に必要な処分」と位置づけることが可能であろう[183]。これを台湾の制度に照らして言い換えれば，台湾刑訴法 213 条 6 号のいう「(職権による無令状の強制的な)検証の処分」を行うために「その他の必要な処分」になる[184]。

ここで問題となるのは，関連性のあるデータが存在している蓋然性を確認するために，検証に必要な処分を超えて実質的な意味での捜索を行わなければならない場合もありうるとすれば[185]，こうした場合を台湾刑訴法のいう「その他の必要な処分」といい難いということである。というのも，もし，かようなデータを確認する処分の性質が実質的な意味での捜索に該当する場合には，それを行うには検察官の職権による無令状の検証によってはならず，捜索令状によらなければならないと解されるはずだからである[186]。すなわち，普通容量のフロッピーディスクを対象とするならば特に問題が生じない場合が多いかもしれないが，大容量の記録媒体(例えば，サーバー記録媒体)の場合には，ほとんどの場合に実質的な意味での捜索が行われることになるのではないかと思われる。そうだとすれば，被疑事件に関連するかどうかを確認するために行う措置には，「その他の(検証に)必要な処分」として認められない場合があるという帰結になる。

以上に検討した問題については，今般の日本の改正法では，これについて何らの対応もなされていないが，これに対し，井上教授は，次のような提案を行っている。

「検証という方法が，差押えに比べ穏やかな方法であるうえ，無形の情報の保全という目的に性質上最も適した処分であることは確かであるから，立法論的には，捜索と検証とを組み合わせた処分を新設するということを考えてもよいのではないかと思われる。」[187]

確かに，この提案は傾聴に値するものと思われる。実際にも，台湾の先行研究においては，2001 年の法改正により電磁的記録を捜索・差押えの対象とすることは有体物のみを対象とする現行法に合わないと指摘したうえで，かかる規定を廃止すべきと主張しながら，無体の電磁的記録を保全するには，上記の井上教授の提案が妥当だとする見解が一部でなされてきた[188]。しかし，この見解をとると，検証には事後救済がないという点が問題となる。

---

[183] 川出・コンピュータ犯罪 6 頁，井上弘通 339 頁参照。

[184] 同条柱書きは「検証には以下の処分を行うことができる」としたうえで，その 1 号は「犯罪の現場あるいはその他の事件に関係する場所を探査すること」と，2 号は「身体を検査すること」と，3 号は「死体を検視・調査すること」と，4 号は「死体を解剖すること」と定めている。本条の内容を日本法の概念に照らして考えてみると，1 号～5 号(5 号は前掲注 179 参照)は検証行為それ自体に関わる定めであるが，6 号はいわゆる検証に必要な処分となる。

[185] 井上弘通 339 頁参照。

[186] 台湾では，法文上，電磁的記録も捜索の対象とされているし，また，2001 年以後，検察官や裁判官が行う捜索の場合であっても，捜索令状を必要とすることになっている。

[187] 井上・コンピュータ(1)62 頁＝井上・強制・任意 271 頁。

[188] 林裕順・基本人權 156，158 頁参照。同文に引用された文献は，井上＝池田 89，90 頁である。

これに対しては，新設した処分において事後救済を設ければよいとの反論がなされるかもしれない。しかし，そうすると，捜索と検証とを組み合わせた新設の処分と，既存の検証との間の，体系上の一貫性ないし統合性という問題が生じうる。また，新しい技術に応じて既存の処分を組み合わせた処分を新設していくことになると，個別の処分が肥大化し，そして，肥大化すればするほど，それぞれの適用関係は複雑化するという点も問題となる[189]。これらの点から，台湾の立法論としては，日本の制度をそのまま受け入れることはできず，以上指摘した諸問題点に対応するために必要な対策を検討するべきであると考えられる。

２．捜索・差押令状による場合

日本においては，情報を検索・点検したりする行為の目的が，差し押さえるべき物であるかどうかを判断する点にあれば，かかる行為は，「捜索の一環ないしそれに必要な処分」になると解されている[190]。というのも，こうした場合の検索行為は，情報の内容の認識それ自体を目的とするわけではなく，関連性のある情報が存在しているかどうかを確認することを通じて，捜索の対象たる媒体が差し押さえるべき物に当たるかどうかを判断することを目的とするものだからである。この理解は，台湾の場合にもそのまま通用する。というのも，かかる理解の前提となる，捜索が差し押さえるべき物を発見するために行われるものであるという日本の通説は[191]，台湾の通説でもある[192]からである。

これに対し，井上教授は，「多数の加入者の受信ファイルが収録・管理されているコンピュータないし記憶媒体につき，果たして目的の通信を識別するための捜索ないし点検を行うことができるかには，疑問も感じられなくはない」[193]と指摘されている。しかし，教授自身も，目的の通信を識別するための捜索ないし点検の許容性を全面的に否定するわけでない。すなわち，教授は，前掲した指摘をしつつも，「まず開披してみなければそのような証拠物等にあたるかどうかが分からない」という点については，データを対象とする場合と，日本刑訴法 100 条の郵便物の場合とが同じであることを述べたうえで，「プロバイダーの受信用サーバーや記憶媒体についても，［被疑者や被告人］の専有の受信ファイルが他と区別して特定可能である限り，そこに収録されているメールに限って，被疑事件との関連性を判別するため，その内容を点検することは許されるものと考えることができよう」と述べている[194]。

確かに，目的の通信（情報）を識別するための検索行為の目的が，差し押さえるべき物で

---

[189] 個別立法の肥大化と適用関係の複雑化という問題は，第２章で述べるように，アメリカが既に経験しているところである。日本においても，今回の改正法によって新設された処分と，既存の検証及び通信傍受という制度との間にいかなる関係があるのかについては，かなり複雑かつ錯綜のものがあるのであり（田口・検証による電話傍受 114 頁以下，庭山＝岡部・刑訴法 3 版 68 頁，後藤・捜査法 53 頁以下など参照），将来，検証のための捜索に対応する個別の処分を新設するとすれば，かような問題は一層深刻になるのではないかと思われる。

[190] 井上・コンピュータ(1)58 頁＝井上・強制・任意 262 頁。

[191] 井上・傍受 99～100 頁。

[192] 林・概論（上）11 版 295 頁，黄＝呉・刑訴法論（上）7 版 195 頁。

[193] 井上・コンピュータ(1)60 頁＝井上・強制・任意 265 頁。

[194] 井上・コンピュータ(1)59～60 頁＝井上・強制・任意 265～266 頁。

あるかどうかを判断する点にあるとすれば，井上教授の見解は台湾の場合にも適切であろう。というのも，「［被疑者や被告人］の専有の受信ファイルが他と区別して特定可能である限り」という制限が，台湾刑訴法 135 条 1 項 2 号の「被告人から発し，または被告人に対して発したもの[郵便物]」（日本刑訴法 100 条 1 項に相当する規定である）という制約と同様に考えられるとすれば，井上教授の見解は，台湾の現行法の枠組みと一致し，差し押さえるべき物であるかどうかを判断するための捜索（台湾刑訴法 122 条）ないし（検察官の職権による無令状の）検証（同法 212 条）の範囲を合理的に制限することができると思われるからである。

しかし，第２章で検討する通り，そもそも日本刑訴法 100 条 1 項の合憲性自体に争いがあるところである。そうであれば，同じ趣旨が定められた台湾刑訴法 135 条 1 項 2 款の実質的正当性についてもなお再検討の余地があるように思われる。また，「専有の受信ファイルが他と区別して特定可能である」といっても，受信ファイルの容量はそれぞれ異なり，大容量の場合には，必ずしも台湾刑訴法 135 条 1 項 2 款のいう有体の郵便物と同視できないのではないかという疑問もある。

第２款　蓋然性による差押え

続いて検討するのは，捜査機関が，現場で，大容量の電磁的記録媒体並びに大量の小容量の電磁的記録媒体を発見した場合，これらの媒体の容量の大小の如何をとわずに，すべての媒体に対して，それぞれの内容を確認することもなく，一括して差し押さえることができるかである。この点を検討するための具体例としては，次のようなものが考えられる。

【例 4】電磁的記録媒体の内容を確認せずそれを差し押さえる事例

前掲の【例 3】において，chan 社のサーバー記録媒体から取得したＹの関連資料により，捜査機関は，Ｙの身元を確認し，その所在を突き止めた。そこで，Ｙの住宅を捜索すべき場所とし，差し押さえるべき物を「組織的犯行であることを明らかにするための磁気記録テープ，光磁気ディスク，フロッピーディスク，パソコン一式」等とする令状を請求し，その発付を得た。

その後，同令状に基づき，Ｙの住宅に赴いて捜索を行ったところ，W型パソコン１台，大容量のＨＤ２台及びを 108 枚のフロッピーディスクが発見された。しかしながら，パソコン及びＨＤにはＩＴセキュリティがかかっているため，現場でそれらを起動させることができなかった。また 108 枚のフロッピーディスクにつき，現場で一枚ずつ点検するには長時間を要し，困難であると判断された。加えて，Ｙが，端末が権限者の設定しておいた以外の方法により起動されるとそこに記録された情報が瞬時に消去されるコンピュータソフトを開発しているとの情報もあった。

そこで，捜査機関は，捜索の現場で内容を確認することなく，上記のパソコン，ＨＤ及

び大量のフロッピーディスクを一括して差し押さえた。このような差押えは，現行法上，認められるであろうか。

Ⅰ．判例による解決とその問題点

【例 4】における問題の核心は，捜索の現場で，媒体(コンピュータ等)の内容を確認することなく差し押さえた点が，差押えのために要求される差押物と被疑事実との「関連性」という要件を満たしているかという点にある。

この点，最二決平成 10 年 5 月 1 日刑集 52 巻 4 号 275 頁(以下，「平成 10 年決定」という)は「令状により差し押さえようとするパソコン，フロッピーディスク等の中に被疑事実に関する情報が記録されている蓋然性が認められる場合において，そのような情報が実際に記録されているかをその場で確認していたのでは記録された情報を損壊される危険があるときは，内容を確認することなしに右パソコン，フロッピーディスク等を差し押さえることが許されるものと解される。」という見解を示している。これによれば，電磁的記録媒体の中に被疑事実に関する情報が記録されている蓋然性が存在している限り，内容を確認しなくともそれを差し押さえることが認められる。この意味で，かような差押えを，「蓋然性による差押え」と称することができよう。同決定により，電磁的記録媒体に対する蓋然性による差押えの許容性につき，実務上は決着が付いた。

以上をもとに，本事例が，台湾ではどのように処理されるかを検討する。まず，台湾刑訴法 152 条(別件差押え)[195]により，捜索あるいは差押えを執行するときに発見した別件の差し押さえるべき物をも差し押さえることができるから，台湾の現行法のもとでは，元の事件と関連性のないものを差し押さえることが認められている。そこで，台湾では，この 152 条が合憲であるとすれば，平成 10 年決定において提起された「蓋然性による差押え」の可否という問題を検討する必要はなくなる[196]という見解が一部で現れてきた[197]。

これに対し，学説上は，台湾刑訴法 152 条は，刑事手続の本質に違背し，人民の権利を侵害するものであるから，立法論的には廃止すべき条項であるとする見解が有力である[198]。

---

[195] 本条は「捜索あるいは差押えを執行するとき，別件の差し押さえるべきものを発見した場合，それをも差し押さえることができ，そのうえでそれぞれを所管裁判所あるいは検察官に渡すべきである。」と定められている。

[196] 台湾の「別件差押え」の 152 条の規定の趣旨と日本の「蓋然性による差押え」の概念とは，論理的には，次元が異なるものである。というのも，日本でいう蓋然性による差押えの問題の核心は，関連性を確認せずに蓋然性によって差し押さえることができるかという点に帰結するのに対して，台湾でいう別件差押えについては，その趣旨は，関連性を確認しなくてもよいというものではないのであり，すなわち，現場で発見したある物件は本件と関連性がないという点はすでに確認されたことを前提に，かような別件にかかわる証拠物に対しても差押えことができる趣旨だからである。しかし，152 条の運用としては，一般的・探索的な捜索を行った上で，関連性を確認せずに大量な無差別の押収，つまり，現場で関連性を確認することもなく別件の証拠や本件の証拠をも区別せずに怪しそうなものと思われたらそれらをすべて押収しておくことが行われている(洪・捜索扣押實務研究 41，126 頁及び強制處分修正 65 頁柯耀程の発言，范・過度扣押 8～9 頁参照)。

[197] 林裕順・基本人權 146 頁。

[198] 林山田・程序法 5 版 355 頁。152 条を批判するその他の見解として，黃東熊・刑訴 245～246 頁，柯耀程・扣押問題 120 頁をも参照。これらの批判する見解に対する再反論として，柯慶賢・修正捜索扣押(下)6～7 頁参照。

これによれば，蓋然性による差押えの許容性を検討することが必要となる[199]。その際には，前述の平成 10 年決定の論旨が参考になる。

しかし，同決定の射程は必ずしも明確ではなく，未解決の点がなおいくつか残されている。まず，仮に，記録された情報が損壊される危険はなく，単に，現場での確認作業に時間が非常にかかる場合や，現場でＩＴセキュリティが解除できない場合には，結論は変わるであろうか[200]。次に，電磁的記録媒体ではなく，極めて大量の書籍・帳簿などについても，同決定を根拠に，その内容を確認することなく，蓋然性による差押えを実施することができるのかという点も問題となる[201]。さらに，同決定に基づく蓋然性による差押えと，日本刑訴法 100 条 1 項(台湾刑訴法 135 条 1 項 2 号がそれと同じ趣旨のものである)による郵便物に対する差押えとの関係についても必ずしも自明ではない[202]。

Ⅱ．問題の再考

台湾の立法論との関係では，さらに，以下の２つの問題点を検討すべきである。

(1)コンピュータ・フォレンジックについて

【例 4】の事実を変更し，捜査官が捜索現場でパソコンの中身を確認したところ，そこに関連性のあるデータが記録されていることが判明したという事例【例 4-1】を考えてみる。この場合，パソコン自体は関連性のある証拠物である以上，台湾の現行法のもとでは，その全体を差し押さえることができるから，これは，日本のいう蓋然性による差押えではなく，一般の差押えにあたるものである。しかし，こうした場合においても，蓋然性による差押えの場合と同様に，パソコンの中に蔵置された無関係の大量なデータが一括して捜査機関に取得されるから，実質的な過大差押えの問題が生じうる。

この問題に対し，今回の改正法で新設された「記録命令付差押え」(日本刑訴法 99 条の2)や「差押えに代える処分」(同 110 条の2)などの規定を台湾に導入することにより対応することが考えられるが，前述したように，それによって問題が完全に解決されるわけではない。

もっとも，相手方がプロバイダーである場合には，台湾の捜査実務上も，まずはその協力を求めるべきであるという方針が確立されつつあるとすれば，いきなりプロバイダーの

---

[199] 法務部・電腦犯罪４版 55～56 頁でも，コンピュータに対して捜索・差押えを執行するに際して，何が差し押さえるべきものにあたるのかを判断することに困難があると指摘されている。

[200] 記録された情報を損壊される危険があるという要件を必要とする説は，寺崎 252 頁，池田 269 頁＝同・最判解（平成 10 年度）89 頁などを，同要件を必要としない説は，柳川 83 頁，安富・フロッピーディスク 244～245 頁，小津 55 頁，飯島 94 頁，壇上 54 頁，甲斐 20 頁などを参照。

[201] この点に関して，井田良ほか編著・事例Ⅱ刑訴[真田]465～466 頁，同頁脚注(13)(14)(15)(16)に挙げられた文献及び池田・最判解(平成 10 年度)89 頁の説明を参照されたい。

[202] 両者の関係についての説明は，川出・フロッピーディスク 182 頁，井上・コンピュータ(1)59～60 頁＝井上・強制・任意 264～266 頁参照。

記憶媒体全体を差し押さえることは稀であるという反論がなされるかもしれない。

しかし，現実には，プロバイダーのサーバー記憶媒体を差し押さえる必要が生じる場合があることを否定できない[203]。また，捜査機関の指定するデータを探し出すためにコンピュータ・フォレンジックを行うと，極めて高い費用が発生する可能性があるとも言われている[204]。そのような場合においては，合理的な通信業者であるならば，それに協力しないという選択肢を選ばざるをえないことになろう。

さらに，私人であるプロバイダーは捜査に精通していないので，それによるコンピュータ・フォレンジックの結果が必ずしも捜査機関が求めるものと合致するとはかぎらない。そのような場合には，捜査機関自らがコンピュータ・フォレンジックを行う必要がある[205]。また，プロバイダーの使えるコンピュータ・フォレンジック技術が，捜査のニーズないし令状の要求に対応できるレベルに達していないという問題点もある[206]。

以上から，台湾の立法論としての在り方を考えてみると，次の２つのことがいえよう。第１は，捜査機関が自ら行うコンピュータ・フォレンジックを直接に規制する制度を設ける必要性があることであり，第２は，実質的な過大差押えという点に着目すれば，一般の差押えの場面と，蓋然性による差押えの場面のいずれについても，事後規制が必要となる場合はあるということである。

(2)電磁的記録でない場合について

蓋然性による差押えの問題は，電磁的記録媒体の差押えに特有なものではない。ここでは，【例 4】の事実を，電磁的記録媒体のみならず，Ｙの麻薬密売の組織的犯行に関する書類(例えば帳簿など)及び組織が取り扱う麻薬も，差し押さえるべき物として令状に明記されており，現場で，大量の書類及び５パックの白い粉末が発見されたという事実【例 4-2】に変更して考えてみる。

この設例で発見された書類は，１つの広い部屋に置かれた数万冊の帳簿であり，その量が極めて多く，現場での確認は困難である。他方，５パックの白い粉末は，それぞれの色ないし形状に差があり，それらが麻薬であるかについては，現場での捜査官による予試験だけでは確認できず，専門家に鑑定(鑑識)をしてもらわないと分からない。このように，【例 4-2】も，電磁的記録媒体を対象とする【例 4】と同様に，現場で，差し押さえるべき物――大量の書類ないし５パックの白い粉末――の内容(関連性)を確認せずに一括して差し押さえる必要がある事例である。それにもかかわらず，日本も台湾も，従来にはこのような事案における差押えの適否は全く問題視されていないようである[207]。

---

[203] 松沢・通信ログ 57～58 頁，河原・72 頁，松井・インターネット人権 14 頁参照。

[204] 審議会(ハイテク)第 2 回議事録(ニフティからの参考人の説明)，Giacobbe，at 265 参照。

[205] Kerr，BIG BROTHER，at 651～654.

[206] Id.

[207] 日本の状況につき，石毛・令状問答 238 頁以下，三堀・犯罪捜査 147 頁，井田良ほか編著・事例Ⅱ刑訴[真田]473 頁参照。台湾の状況について，洪・捜索扣押實務研究 41～42 頁，陳瑞仁・新法捜索扣押 70 頁参照。

以上により，日本において提起されてきた，電磁的記録媒体を対象とする場合に行われる蓋然性による差押えの許容性という問題意識は，かかる問題を十分に意識していない台湾の立法論に対しては啓蒙的なものがあると同時に，同問題に対応するためになされた今回の改正法の関連規定は台湾にも参考になる箇所が含まれていると思われる。しかし，電磁的記録媒体以外を対象とする場合にも，蓋然性による差押えの性質を有する差押えが行われているのに，なぜ，電磁的記録媒体のみを特別に取り扱うのかという疑問もあり，そのような立法の合理性については，なお再吟味する余地があるように思われる。

第３節　遠隔操作によるデータの検索・検閲と取得

日本でいうリモート・アクセスという捜査手法は，さらに次の２つの場合に分けることができる。第１は，オンラインで繋がった別の端末機器の存在を予想したうえで，それを令状にあらかじめ記載しておく場合である[208]。第２は，オンラインで繋がった別の端末機器の存在を事前に予想しておらず，捜索や検証に着手した後に初めて，そのことがわかった場合である[209]。

以下は，第１の予見できる場合の問題点のみを取り上げることとする。というのも，改正法は第１の場合にのみ対応しているものであるし，また，本稿は令状制度の再構築を検討するものであるため，予見できない場合を取り上げる必要はないからである。

ここでの問題の核心は，捜索・差押えの対象となる場所及び記録媒体と，リモート・アクセスの対象となる媒体及びかかる媒体が所在する場所が如何なる関係にあるか，そして，法はかような関係をいかに評価すべきか，という２つの点に帰結することができる。この２つの点を説明するために，以下のような具体例を想定してみる。

【例 5】住居の捜索・差押えからリモート・アクセスへ発展する事例

捜査機関は，【例 4】において，蓋然性に基づき一括して差し押さえたW型パソコン１台，ＨＤ２台及び 108 枚のフロッピーディスクを鑑識に付した。技官が当該W型パソコン及びＨＤ２台を鑑識したところ，被疑者Ｙが頻繁にアクセスしていたいくつかのＩＰアドレス[210]を割り出した。そのうち，123・13・12・111[211]という「固定ＩＰアドレス」(static Internet Protocol address)により定義されたある送受信器機[212]は，W型パソコンで作成若しくは変

---

208 井上・コンピュータ(2)52～53 頁＝井上・強制・任意 277～278 頁。

209 井上・コンピュータ(2)54 頁＝井上・強制・任意 281 頁。

210 IPアドレス（Internet Protocol address）とは，Internet Protocol（IP)における送受信機器を判別するための番号，言い換えれば，特定の送受信元のネット上の所在を示す「位置情報」である。IPアドレスには，接続する度にIPアドレスが変わる動的IPアドレスと，何度接続してもIPアドレスが変わらない固定IPアドレスがある(「Request for Comments (RFC)」―search word: Internet protocol suite／static IP address／Dynamic IP Addresses，ウィキペディア―サーチワード：IPアドレス参照)。

211 IPアドレスは，「xxx.xxx.xxx.xxx」という 3 桁までの 4 つの数値の組み合わせ（IPv4 の場合/32 ビット）の形になっているが，その範囲は，「0.0.0.0～255.255.255.255」に限られる(出処は同前注参照)。

212 厳格にいえば，「IPアドレスにより定義された送受信器機」という言い方は正確ではない。というのも，個別の送受

更をした電磁的記録又は同パソコンで変更若しくは消去することができることとされている電磁的記録を保管するために使用されている蓋然性があることが判明した。捜査機関は，当該ＩＰアドレスを手掛かりに，当該器機は， Nex 社(クラウド型リモート・ストレージ・サービス株式会社)が所持する Wz1 型ホストコンピュータであることを突き止めた。

Ｙの上記パソコンの過去のアクセス履歴からは，これとは別に，「23・000・123・XXX」という形の複数の「動的(非固定)ＩＰアドレス」（dynamic Internet Protocol address）が見つかったが，当該ＩＰアドレスにより定義された送受信器機自体を特定することはできなった。なぜならば，「XXX」の部分は，いわゆる動的ＩＰアドレスの割当分であり，それは，プロバイダーが保有するユーザー用のＩＰアドレスの中から，接続した時点でその都度割り当てられる番号であって固定していないものだからである[213]。

そこで，「23・000・123・XXX」という形の複数の動的ＩＰアドレスを特殊なソフトにかけて計算した結果，1500 組のアクセス可能なＩＰアドレスが得られた。これらのＩＰアドレスを，本件の地縁関係及び接続の時間によりさらに絞り込んだところ，マレーシア及び日本の２つの地域内において，本件と関係あると疑われる送受信をしたものが 10 組あることがわかった。そして，この 10 組は，いずれも，個人のユーザーによるものである確率が高いと判断された。

また，２台のＨＤのうちの１台から，もう１つ固定ＩＰアドレスである 21・223・224･112 にアクセスした履歴記録が割り出された。捜査機関は，当該ＩＰアドレスから，ネットワーク管理者ないしホスト名などの情報を手に入れたが，それらはいずれも国交のない外国に所在する法人であり，関連照会文書を出したが回答を断わられたため，当該ＩＰアドレスにより定義された送受信器機自体を特定することはできなった。だが，鑑定により，送受信器機自体を特定しなくても，オンラインで 21・223・224･112 のＩＰアドレスに対応する遠隔地にある不明の器機(Z)にアクセスする可能性があり，かつ，同器機からデータを閲覧したりダウンロードしたりすることも可能であることが明らかになった。

以上の前提のもとで，以下の３つの問題を検討する。

(1)捜査機関は，差し押さえたW型パソコンないし警察庁が所有するコンピュータから，

信機器を識別する番号は， IPアドレスではなく，MACアドレス(Media Access Control address)だからである。 IPアドレスから得られるのは，ネットワーク管理者ないしホストなどの情報だけであって，個別のユーザーの個人情報ないし該当ユーザーが使用した発信端末の詳細を手に入れようとすれば，当該ネットワーク管理者に問い合わせる必要がある。もっとも， IPアドレスとMACアドレスの対応付けなどがプロトコルで定義されているという意味では，「IPアドレスにより定義された送受信器機」といっても誤りとまではいえないかもしれない。とはいえ，IPアドレスはネットワーク上のインターフェースに与えられるものであるから，個別の機器を取り換えても不変であり，厳格な意味で器機を定義するのはMACアドレスであって，IPアドレスではないという点には注意が必要である。以上につき，「Request for Comments (RFC)」―search word: IP Addresses／MAC address，ウィキペディア―サーチワード：IPアドレス参照。

[213] 一般には， IPアドレスさえわかれば，発信元端末である遠隔地にあるコンピュータを特定することができると考えられているようであるが，これは誤解である。なぜなら，前述した通り，IPアドレスだけでは発信元端末が一義的に特定されるとはいえないし，また， IPアドレスには，固定式と非固定式(動的 IPアドレス)の２つがあり，このうち固定式の場合には，IPアドレスを手掛かりに，発信元端末を割り出すことが可能であるが，非固定式の場合には， IPアドレスだけで,それはできないからである(See「Request for Comments (RFC)」―search word: IP Addresses. And see Moore, at 127 ～134；井上・コンピュータ(1)53 頁＝井上・強制・任意 279 頁をも参照)。

リモート・アクセスという手法により，遠隔地にある特定された Wz1 型ホストコンピュータに記録されたデータの検索・検閲ないし取得を行うことができるか。

(2)10 組の 23・000・123・XXX のＩＰアドレスにより定義される遠隔地にある不明の器機(q)，及び 21・223・224･112 のＩＰアドレスにより定義される遠隔地にある不明の器機(Z)が，差し押さえられたW型パソコンで作成若しくは変更をした電磁的記録又は同パソコンで変更若しくは消去をすることができることとされている電磁的記録を保管するために使用されている蓋然性がある場合に，捜査機関が，遠隔地にある特定されていない器機にアクセスし，その内部に蔵置されたデータを閲覧したりダウンロードしたりすることができるか。

(3)上記の(1)ないし(2)の捜査を行うに際して，遠隔地にある器機にアクセスしデータを取得するために，技術的な手段をもって，アクセス先にかかっているパスワードないしその他のＩＴセキュリティを解除することができるか。

以上の３点につき検討するにあたり，まず，日本の現行法においてそれらについていかなる対応が可能であろうかを考察したうえで，それを参考に，台湾の立法論として検討すべき問題点を洗い出し，将来の立法のあるべき方向を探ることにしたい。

第１款　リモート・アクセス，ネットワークと端末

上記の問題点を検討するに先立ち，日本の改正法が成立する前の状況がどうであったのかを概観しておく。

改正法が成立する前の捜索・差押えにあたっては，リモート・アクセスの手段により遠隔地にあるコンピュータに蔵置されたデータを検索・検閲ないし取得することはできないと解されていた[214]。他方で，現行法上，オンラインでの検索・検閲とダウンロード・コピーを，検証のため捜索(検証に必要な処分)，検証，検証の結果の記録という一連の処分と解することができるとすれば，検証という制度が，かような捜査を行うための根拠として考えられるかもしれないという指摘もなされていた[215]。

仮に，オンラインで検証を行うことが，現行法上認められていると解することができるとすれば，それは，被処分者のコンピュータから行う場合であれ，警察庁が所有するコンピュータから行う場合であれ，いずれも許されることになろう。というのも，上記の見解

---

[214] 川出・コンピュータ犯罪 9 頁は「……あるコンピュータの中に特定の被疑事実に関連するデータが保存されている蓋然性があるということで，その取得のための強制処分を実施するという場合，そのデータ自体が処分の対象であれば，その強制処分それ自体に関する限り，その実施時点において，当該データが当初想定したのとは異なる他のコンピュータに移動していた場合でも，その執行が可能である。しかし，記録媒体たるコンピュータが処分の対象である場合には，データがそこから移動してしまえば，当初の処分の執行として，他のコンピュータ内にあるデータを獲得することはできないということにならざるをえないと考えられる[。]」とする。同解として，井上・コンピュータ(2)53～54 頁＝井上・強制・任意 280 頁，指宿・サイバースペース 88 頁，経産省報告書・サイバー犯罪条約・対応 52 頁などを参照。

[215] 井上・コンピュータ(2)54 頁＝井上・強制・任意 280 頁。

によると，オンラインでの検証の実質的な対象は，目の前のコンピュータでも，遠隔地にあるコンピュータでもなく，データ自体であると考えられ，そうだとすると，その検証を被処分者のコンピュータから行わなければならないとする理由はないはずだからである。

これに対し，改正法は，リモート・アクセスによる差押え(日本刑訴法 99 条 2 項，218 条 2 項，219 条 2 項)を設けており，この規定は，リモート・アクセスによりデータを取得するための法的根拠を提供したものと考えられる。しかし，99 条 2 項の文言から見ると，その適用は，差し押さえられた被処分者のコンピュータからのリモート・アクセスの場合に限られている[216]。また，日本刑訴法 107 条の 2 項の規定によれば，その電磁的記録を複写すべき遠隔地にある電磁的記録媒体の範囲を令状に明記しなければならないとされる。

それによれば，差し押さえるべき物である被処分者のW型パソコンとオンラインで繋がっている,遠隔地にある特定の Wz1 型ホストコンピュータの範囲を令状に明記しておけば，現場で，リモート・アクセスにより，W型から Wz1 型に蔵置されたデータの検索・検閲ないし取得を行うことができるが，W型コンピュータを差し押さえた後に，別の場所でリモート・アクセスを行うことはできず，ましてや，警察が所有するコンピュータから同様のリモート・アクセスを行うことはできないことになろう[217]。つまり，改正法のリモート・アクセスによる差押え関連規定の適用は，「現実に当該電子計算機を差し押さえた場合に限ることとはされていない」[218]とされるが，差し押さえるべき物たるコンピュータなどの媒体を差し押さえる前に，電磁的記録の複写が行われることが，前提となっている[219]。

以上の通り，リモート・アクセスによる差押えの新設は，オンラインでの検証の可否についての解釈論上の争いを回避するという実益があると評価できるものの，そこには，第１に，警察が所有するコンピュータからはかかる捜査を行うことができず，第２に，電磁的記録の複写が，媒体を差し押さえる前に行われなければならないという制約がある。以上を前提に，前掲の３つの問題についての検討を行いたい。

まず，問題(1)については，リモート・アクセスは，警察が所有するコンピュータからはそれを行うことができず，現場でW型パソコンを利用しなければならないということになる。しかし，これは不合理だと思われる。なぜなら，技術的には，遠隔地にある特定のWz1型ホストコンピュータにアクセスしデータを取得することは，必ずしもW型パソコンからではなく，捜査機関の端末からでも可能であるし，また，場合によっては，捜査機関の端末から行う必要性ないし実益もあるからである。例えば，現場でW型パソコンが突然に故障した場合が，それが必要な例として挙げられよう。こうした場合に，捜査官が，W型パソコンから得られた情報を手掛かりに，捜査機関の端末から，Wz1型ホストコンピュータに

---

[216] 池田・電磁的記録 82 頁は「本項の処分の対象となる電子計算機は，99 条 1 項の要件を満たしている必要があるため，例えば，それ自体差し押さえるべき物に当たらないコンピュータから，何らかの方法によりネットワークを介して記録媒体を操作し，電磁的記録を複写することが可能となるものではない」とする。

[217] 河上ほか編・大コンメンタール第二版補遺[吉田]8 頁，杉山＝吉田・情報処理の高度化(下)105 頁。

[218] 同前注。

[219] 同前注。また，上口・刑訴 3 版 150 頁をも参照。

アクセスするという方法が容易に想定されるが，改正法は，かような場合を全く想定していないようである。

また，それを捜査機関の端末から行う実益としては，被処分者の財産権と差押えの必要性との調和をとるという点が挙げられる。というのも，リモート・アクセスによる差押えを行うためにW型パソコンの利用が不可欠ではない以上，被処分者の財産であるW型パソコンを利用することをできるかぎり避け，警察機関のコンピュータを使うべきと考えられるからである[220]。

これに対して，台湾の場合には，2001 年の法改正により電磁的記録自体も捜索(差押え)の対象とされている以上,警察の所有するコンピュータからオンラインで証拠となる電磁的記録にアクセスしたり，それをダウンロードしたりすること，――すなわち，リモート・アクセスという捜査手段が，現行法上認められていると解する見解が一部で現れている[221]。しかし，現行法上，このリモート･アクセスの範囲を限定するための関連規定が完全に欠如しているという問題がある。

さらに，かような捜査手段が，現行法上の捜索・差押えという概念に該当するかどうかという点にも大きな疑問がある。この点，上記の見解は，オンラインで遠隔端末にアクセスしたり，そのなかにあるデータを捜したりする行為は，捜索に該当すると明言しているが，①無体の電磁的記録それ自体が現行法上の差押えの対象であるかどうか,②オンラインでデータをダウンロードすることは差押えにあたるかどうか,という２つの点については明らかにしていない[222]。確かに，現行法は，捜索を，犯罪嫌疑者や差し押さえるべきものあるいは電磁的記録を発見するための手段であると明示的に定めているので，オンラインでのサーチという捜査行為を，現行法のいう捜索に該当すると解するのは特に不都合がないようにみえる。これに対して，差押えについては，依然として占有の剥奪がその定義とされているため[223]，ダウンロードすることは，それにより占有の剥奪が発生しない以上，それを差押えに該当するものとは解しえない。また，無体の電磁的記録それ自体は差押えの対象にならないとすると，ダウンロードは取得行為であるから，発見する行為である捜索の概念に包摂させることも困難である。

以上のとおり，無体の電磁的記録をも捜索・差押えの対象としている台湾刑訴法によれば，現場で発見したW型パソコンを利用しなければならないという日本刑訴法の不合理性を回避することができるようにみえるが，それは，①オンラインで捜索・差押えを行うにあるべき範囲を画定するための規定の欠如，及び②差押えの従来の定義との齟齬による法解釈上の不一貫性の発生という２つの問題を抱えている。これに対して，日本の今回新設されたリモート・アクセスによる差押え関連規定は，オンラインでの捜索・差押えの範囲を限定する機能ないし差押えの従来の定義との調和性という２点で，台湾の現行法より優れているものがあると評価できよう。

---

[220] 経産省報告書・サイバー犯罪条約・対応 52 頁の説明が参考になる。

[221] 林鈺雄・搜索扣押 95 頁参照。これに対して，反対説がある(搜索修法(二)131 頁蔡秋明の発言参照)。

[222] 同前注。

[223] 同前注 197 頁参照。

以上のように，オンラインで行う捜索・差押えにつき，その適正な範囲の限定の在り方，及びその法的位置づけと差押えの従来の定義との調和を図るには，日本刑訴法のリモート・アクセスによる差押え関連規定には長所があるが，それには，現場でのW型パソコンの利用を必ず必要としているという短所もある。それゆえ，この短所を除いてその長所のみを残す可能性を模索しなければならない。

第２款　遠隔地にある端末ないしその範囲の特定

続いて，問題(2)の検討に移る。この事例における，10 組の「23・000・123・XXX」という形のアクセス可能なＩＰアドレスにより定義されている遠隔地にある器機(q)，及び「21・223・224･112」のＩＰアドレスにより定義されている遠隔地にある器機(Z)は，器機自体が不明で，特定されていないため，従来の理解によれば，日本国憲法 35 条に要求される「特定性」の要件を満たしていないと解すべきことになろう。というのも，従来，対象の特定とは，物理的な意味で，対象となる物とそうでない物とを区別することであるとされてきたのに対して，遠隔操作の場合は，ＩＰアドレスはネットワーク上のインターフェースに与えられるものにすぎず，個別の機器を取り換えても不変であるので[224]，ＩＰアドレスだけでは，　個別の器機を特定することができず，(q)と(Z)は，物理的な媒体の次元で特定されてはいないからである。

この点に関して，リモート・アクセスを対象とした日本の改正法 107 条 2 項は，令状に，「その電磁的記録を複写すべき遠隔地にある電磁的記録媒体」ではなく，当該記録媒体の中の「その電磁的記録を複写すべきものの範囲」を特定して記載すべきとしている。このような記載により，果たして日本国憲法 35 条の特定性の要件が満たされるであろうか。以下では，この点を中心に，【例 5-1】を，捜査官が，W型パソコンに対する差押えを行う現場でリモート・アクセスを行う事案に修正したうえで，問題(2)について検討していきたい。

Ⅰ．107 条 2 項に基づく対象の特定について

改正法の元となった要綱(骨子)を採択した法制審議会刑事法部会においても，「差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であって，その電磁的記録を複写すべきものの範囲」をどのように特定すべきかが問題となった。この点につき，事務当局は，遠隔地である場所や，遠隔地にある記録媒体までを特定する必要はなく，差し押さえるべき電子計算機の所在地及びリモート・アクセスしようとする範囲を明記すればよいと回答している[225]。

この説明を【例 5-1】の事案に当てはめてみると，W型パソコンを対象とした差押令状を

---

[224] 例えば，Yahooや MSNなどのサイトは，固定 IPアドレスを取っているが，端末機器が交換されても，Yahooや MSNの固定式 IPアドレスが変更されることはない。というのも，IPアドレスとMACアドレスの対応付けがプロトコルで定義されており，機器が変更されてMACアドレスが変わっても，その対応付けを変更するだけですむからである。

[225] 審議会(ハイテク)第 4 回議事録参照。

請求する際に，「W型パソコンを差し押さえる現場において，10 組の『23・000・123・XXX』のＩＰアドレス，及び『21・223・224･112』のＩＰアドレスでアクセスできるリモート・ストレージ器機を調べる」旨を明記すれば，新設されたリモート・アクセスによる差押えを行うことができると解される。この場合，リモート・ストレージ器機自体は特定されていないが，「10 組の『23・000・123・XXX』のＩＰアドレス，及び『21・223・224･112』のＩＰアドレス」の明記によってアクセスできるリモート・ストレージ器機は間接的に限定されており，これによって 107 条 2 項の特定性の要件が満たされていると解しうると同時に，以下の問題点も解決される。

すなわち，仮に，法が，遠隔地にある媒体自体を特定することを要求しているとすれば，【例 5-1】で令状に明記されたのは Wz1 型ホストコンピュータである以上，その後に，Wz1 型が Wz2012 型に取り替えられた場合には，令状に明記されていない Wz2012 型に対してリモート・アクセスによる差押えを行うことができないことになろう。しかし，ネット上の位置表示(ＩＰアドレス)は，Wz1 型も Wz2012 型も，同じく「123・13・12・111」であり，捜査機関は，それらが所在する場所に赴くことなく，リモート・アクセスによる差押えを行うから，通常は，目的の端末が Wz2012 型に変わったことはわからない。そうすると，Wz1 型を対象とした令状によって，対象でない Wz2012 型に対してリモート・アクセスがなされることになるという問題がある。

これに対して，改正法 107 条 2 項では，もともと，令状において Wz1 型や Wz2012 型というリモート・ストレージ器機自体を明記することは要求されておらず，令状に明記されたＩＰアドレスと繋がっているあるリモート・ストレージ器機のなかの，コピーできるデータの範囲さえ明示・特定されればよいので，かような問題は生じないのである。つまり，改正法の下では，令状において，例えば，「『123・13・12・111』という ＩＰアドレスにより特定されうる媒体」といった記載をするだけで十分であって，したがって，令状請求時には，上記のＩＰアドレスと繋がっているのは Wz1 型ホストコンピュータであったが，令状を執行する際には，同じＩＰアドレスと繋がっているのが，Wz2012 型ホストコンピュータになっているとしても，Wz2012 型をアクセスする対象としリモート・アクセスによる差押えを行うことは差し支えないことになる。この改正法の設計と改正前のそれとを図式で比較すると，次のようなものになる。

図１　データを取得できる範囲についての改正前後の比較

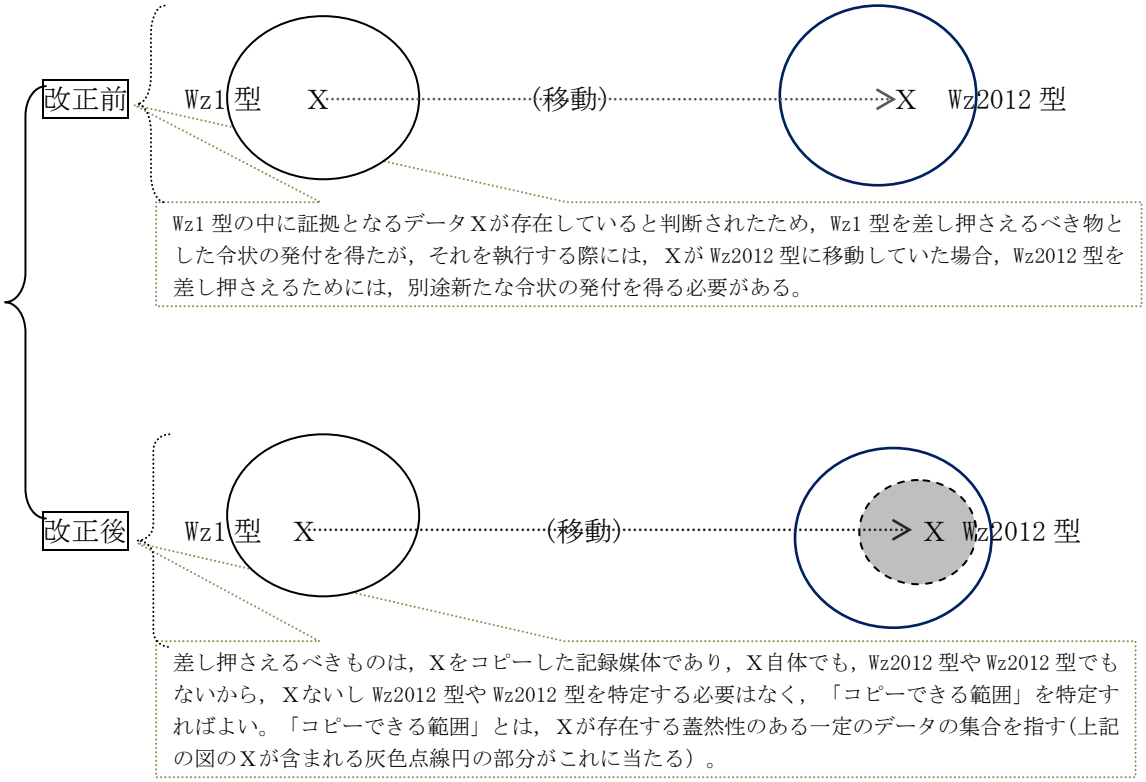


図１に照らして 107 条 2 項の「差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であって，その電磁的記録を複写すべきものの範囲」という文言を評価すると，２つの見方が考えられる。その１つは，従来は，Wz2012 型を処分(差押え)の対象としようとすると，別個の令状が必要とされたのに対して，改正法では，Wz2012 型を処分(アクセス)の対象とする場合にも，別個の令状は不要となるから，その意味で，従来の有体物を対象とする特定性要件が緩和されているという見方である。これによれば，107 条 2 項は，「拡張機能」を持つといえる。もう１つは，従来は，別個の令状さえあれば，Wz2012 型全体を差し押さえることができるので，その中のデータもすべて取得されることになるのに対して，改正法では，Wz2012 型のなかにあるすべてのデータを取得することが認められず，その中の，図１の灰色点線円の部分のみを取得することができるから，従来の有体物を対象とする特定性要件よりも，その対象をより限定しているという見方である。この意味で，107 条 2 項は，「限定機能」を果たしているということができる。

以上の議論を台湾の場合に当てはめると，次のようになる。

まず，現行法は電磁的記録も捜索・差押えの対象としているという一般論から出発すれば，対象となる電磁的記録Ｘをあらかじめ特定することができ，それが捜索(差押え)令状に明記されている場合であるならば，特に問題がないようにみえる。しかし，前掲の例で

いえば，捜査機関は，それらが所在する場所に赴くことなく，リモート・アクセスによる差押えを行うから，通常は，目的の端末が Wz2012 型に変わったことはわからないので，Wz2012 型自体があらかじめ令状に明記されることはまずない。また，捜査の段階では，通常は証拠となる電磁的記録Ｘ自体を特定できないのが現実であるから，結局のところ，電磁的記録それ自体をも捜索・差押えの対象とするだけでは，問題の解決にはならず，その実益は薄いと言わざるを得ない。

これに対して，前述した日本の改正法 107 条 2 項の「拡張機能」によれば，これらの問題点に対応することが可能であると考えられる。というのも，107 条 2 項によれば，Wz2012 型自体をあらかじめ令状に明記する必要はなくなり，それと同時に，証拠となる電磁的記録Ｘ自体を特定しておく必要もなくなるからである。

もっとも，台湾においては，前述した別件差押えという制度のほかには，付随差押え[226]という制度があるし，また緊急捜索[227]の制度も用意されているから，結局のところ，令状に記載されていない物件ないし場所ではあるが，それらに対しても差押・捜索をすることが現行法上は認められているので，日本刑訴法 107 条 2 項の「拡張機能」というような制度を導入する必要が本来にはないと反論されうるかもしれない。

しかし，前述したように，別件差押えの規定を廃止すべきという主張が有力であるし，また，別件差押え・付随差押え・緊急捜索の３つの緊急処分の制度の運用は，一般的・探索的令状を認めていることと等しいという批判もなされてきているから[228]，立法論としては，むしろ，令状原則の遵守を前提とした日本の改正法 107 条 2 項の「拡張機能」をある程度で採り入れつつ，既存のこの３つの緊急処分の制度を全面的に見直したほうが望ましいであろう。

前述した改正法の「限定機能」により，Wz2012 型のなかにあるすべてのデータを取得することが認められず，その中の，図１の灰色点線円の部分のみを取得することができるということになる。これに対して，台湾では，付随差押え・別件差押えないし緊急捜索が認められていることに加え，前述したように，実務上は現場で関連性を確認せずに無差別の大量な差押えが行われているといわれているから，令状において明記された Wz1 型はもちろんのこと，令状に明記されていない Wz2012 型にもアクセスがなされ，そこにあるすべてのデータが取得されることになりかねない。この意味で，改正法の「限定機能」は台湾に導入するに値する価値があるものであるように思われる。

---

[226] 台湾刑訴法 137 条 1 項は「検察官，検察事務官，司法警察官あるいは司法警察は捜索あるいは差押えを執行するときに，捜索令状に記載されていない本件の差し押さえるべき物を発見する場合，それをも差し押さえることができる。」と定めている。

[227] 台湾刑訴法 131 条 2 項は「検察官は，捜査中，即時に捜索を行わなければ，証拠を偽造・変造・隠滅や隠匿されたりするおそれがあり，緊急を要する場合と認められる相当な理由があるかぎり，直ちに自ら無令状で捜索を行うか，それとも，検察事務官，司法警察官あるいは司法警察を指揮しそれらに捜索を行わせることができる。」と定めている。

[228] 洪・捜索扣押實務研究 41，126 頁及び強制處分修正 65 頁(柯耀程の発言)参照。

Ⅱ．台湾への導入に先立ち検討すべき問題点

以上の通り，「拡張機能」と「限定機能」の双方を持ち合わせている日本の改正法107条2項は，台湾の立法論にも参考となるものがある。しかし，その導入に先立ち，まずは，以下の３つの点を確認しておくべきである。

１．拡張機能について

ここで検討すべきは，「拡張機能」を認める改正法の設計が果たして合理的であるのかである。例えば，Ａ社が，独禁法違反事件で摘発されたＢ社を買収し，顧客流出を防ぐために，Ｂ社のネットショップの固定ＩＰアドレスである「123・13・12・111」をそのまま使うことにしたが，同アドレスと繋がっている端末は，Ｂ社のWz1型コンピュータではなく，Ａ社のWz2012型コンピュータに取り替えられたという事例を想定しよう。

この場合，Ａ社のWz2012型コンピュータの中身は，Ｂ社のWz1型コンピュータのそれとは全く異なるが，Ａ社のWz2012型コンピュータが令状に明記された「123・13・12・111」というＩＰアドレスで繋がっているものであるかぎり，改正法の「拡張機能」により，それに対しても，同令状をもってリモート・アクセスによる差押えを行うことができることになろう。これは，不合理ではないかと思われる。

そこで，台湾の立法論との関係で検討すべきは，この「拡張機能」を導入するとして，この不合理を如何に解消することができるのかである。

２．限定機能について

次に，「限定機能」という側面を検討すると，そこでは，第１に，いかなる形で，前掲した図１の黄色の部分（証拠となるデータＸが存在する蓋然性が認められる一定の範囲のデータの集合）を画定することができるのか，そして，第２に，その部分をコピーすることにより，証拠ではないデータも取得されることになるが，それはなぜ許されるのか，という２つの点が問題となる。

まず，第１の，データの集合部分を画定する方法については，立法担当者によれば，改正法99条2項によりオンラインで複写することができる電磁的記録は，差押対象物たる電子計算機に電気通信回線で接続している記録媒体に記録されている電磁的記録のすべてではなく，「当該電子計算機で作成若しくは変更をした電磁的記録」又は「当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録」に限られるものとされ[229]，そのうえで，かかる記録は，通常，被疑事実との関連性があると思料されるものと考えられるから，個々の電磁的記録について，個別に被疑事実との関連性の有無を判断しなければならないわけではないと考えられるとされている[230]。

---

[229] 河上ほか編・大コンメンタール第二版補遺[吉田]6 頁，杉山＝吉田・情報処理の高度化(下)103 頁。

[230] 同前注[吉田]7 頁，杉山＝吉田 103 頁。

つまり，改正法は，従来の「差し押さえるべき物の特定性」という要件を緩和しつつも，その代わりに，「接続している状態」並びに「電磁的記録の属性」を制限するという形で，間接的に差押えが許される範囲を限定しているわけである。しかし，かような制限だけで，果たして差押えの許容範囲が適切に限定されているといえるのかについては疑問がないわけではない。それゆえ，台湾の立法論を考える際に，「接続している状態」「電磁的記録の属性」の２つの制限要素は参考になるものであると思われるものの，なお他の可能性はないのかを改めて検討する必要がある。

さらに問題となるのは，上記の立法担当者の説明のうち，「個別に被疑事実との関連性の有無を判断しなければならないわけではない」という部分である。この点につき，立法担当者により，次のような補足的な説明が付されている。

「差押えの現場において，このような電磁的記録について，被疑事実との関連性の有無を逐一確認するよう要求するのは，捜査における迅速性の要請に反するだけでなく，不可能を強いることにもなりかねず，現実的ではないと考えられる。なお，最決平10・５・１集52巻4号275頁は『フロッピーディスク等の中に被疑事実に関する情報が記録されている蓋然性が認められる場合において，そのような情報が実際に記録されているかをその場で確認していたのでは記録された情報を損壊される危険があるときは，内容を確認することなしに……フロッピーディスク等を差し押さえることが許されるものと解される。』と判示している。しかし，他方で，差押えの現場において，被疑事実との関連性があると思料される電磁的記録とそれ以外の電磁的記録との区別が容易である場合に，捜査機関が，明らかに被疑事実との関連性がないと思料される電磁的記録の複写を殊に行うことは許されないものと考えられる」[231]。

これによれば，リモート・アクセスによる差押えにおいては，「当該電子計算機で作成若しくは変更をした電磁的記録」又は「当該電子計算機で変更若しくは消去をすることができることとされている電磁的記録」にあたる限り，その内容を確認することなしに，それを転写したうえで，記録媒体を差し押さえることができる。その意味で，改正法のかかる規定は，【例4】でいう蓋然性による差押えの性質を帯びるものといってよかろう[232]。

このように，オンラインの場合にも蓋然性による差押えをみとめてもよいかという点は，台湾の立法論としてはなお慎重な検討を要する問題である。というのも，オフラインの場合においては，すくなくとも，物理的な場所という制約があるのに対して，オンラインの場合には，このような制限が働かなくなる結果，オンラインでの蓋然性による差押えの範囲が広がりすぎるとすれば，それが果たして中華民国憲法23条のいう比例原則に適合するものであるのかは疑問だからである[233]。

---

[231] 同前注[吉田]7 頁，杉山＝吉田 107 頁(注 6)。

[232] 杉山＝吉田・情報処理の高度化(下)102 頁の説明をも参照されたい。

[233] オフラインの場合には，捜査機関が蓋然性により取られるものの「最大限」は，あくまで，一定の物理的な区切りにより限定された「一定の空間である場所内」に置かれた「すべて」のものであるに対して，オンラインの場合となると，理論的には，無限連結が技術上は可能であるから，かような限定さえないのでそれにより取られる情報量が予想しかね

３．リモート・アクセスの対象とその範囲について

最後に，改正法 107 条 2 項の規定が，果たして現代の情報社会の実情にかなうものであるかを検討してみたい。すなわち，立法担当者が想定している，前掲の図１のような形態，つまり，１つのＩＰアドレスが１つの端末に対応するような状況は，一般的なものではなく，実際には，むしろ，同一のＩＰアドレスで，多数のパソコンと接続しながら通信していることが，現代の情報社会の実情である。

この点を検討するために，設例を，図１のように，令状の発付から執行までの間に，Wz1 型が Wz2012 型に取り替えられたという場面ではなく，Wz1 型に加えて Wz2012 型が追加されたという場面に変更して考えてみる。この場合，107 条 2 項の下では，Wz1 型や Wz2012 型自体を特定することは必要ではなく，ＩＰアドレスを特定すればよいから，Wz1 型も Wz2012 型も，「123・13・12・111」というＩＰアドレスに対応するものである以上，それを記載したリモート・アクセスによる差押令状の効力の範囲内に入っていることになる。つまり，改正法の考え方は，ＩＰアドレスの特定によって，間接的にではあるが，Wz1 型や Wz2012 型が特定されると擬制するものといってよいであろう。

しかし，ＩＰアドレスが特定されたからといって，Wz1 型や Wz2012 型が特定されたわけではないし，また，同じＩＰアドレスと繋がっている端末の数は，令状発付から令状執行までの間において変動する可能性があるから，上記の意味での擬制に基づく立法が，果たして，憲法上の最小化原則にかなったものであるかについては，なお検討する余地があるように思われる。この問題点は，クラウドコンピューティングの場合を考えるとより明らかになる。まず，クラウドの大まかなイメージは，次の図２に示されたようなものである。

図２について、インターネット公表に対する著作権者からの許諾が得られていないため，非公開とする。

図２　グラウトの概念図[234]

図２において，Ａ社のクラウドのシステムに繋がっているすべての端末(例えば，数百台のPCやプリンターやファクシミリなど)に対して，１つの同じ固定ＩＰアドレスを与えることができる。そのイメージは，次のようなものになる(以下の「21・223・224･112/○○」は，「システムの共通ＩＰアドレス番号/システム内の割当番号」を意味する)。

るという意味での「無限」といっても過言ではないだろう。

[234] 図２は，2013 年（平成 25 年）１月３日［木曜日］NHK の WEB 特集 「大丈夫？ あなたの“クラウド”」(http://www3.nhk.or.jp/news/web_tokushu/1228.html)の挿絵に若干手を加えたものである。

→21・223・224･112/PC1

→21・223・224･112/PC2

↓

→21・223・224･112/PC323

→21・223・224･112/プリンター1

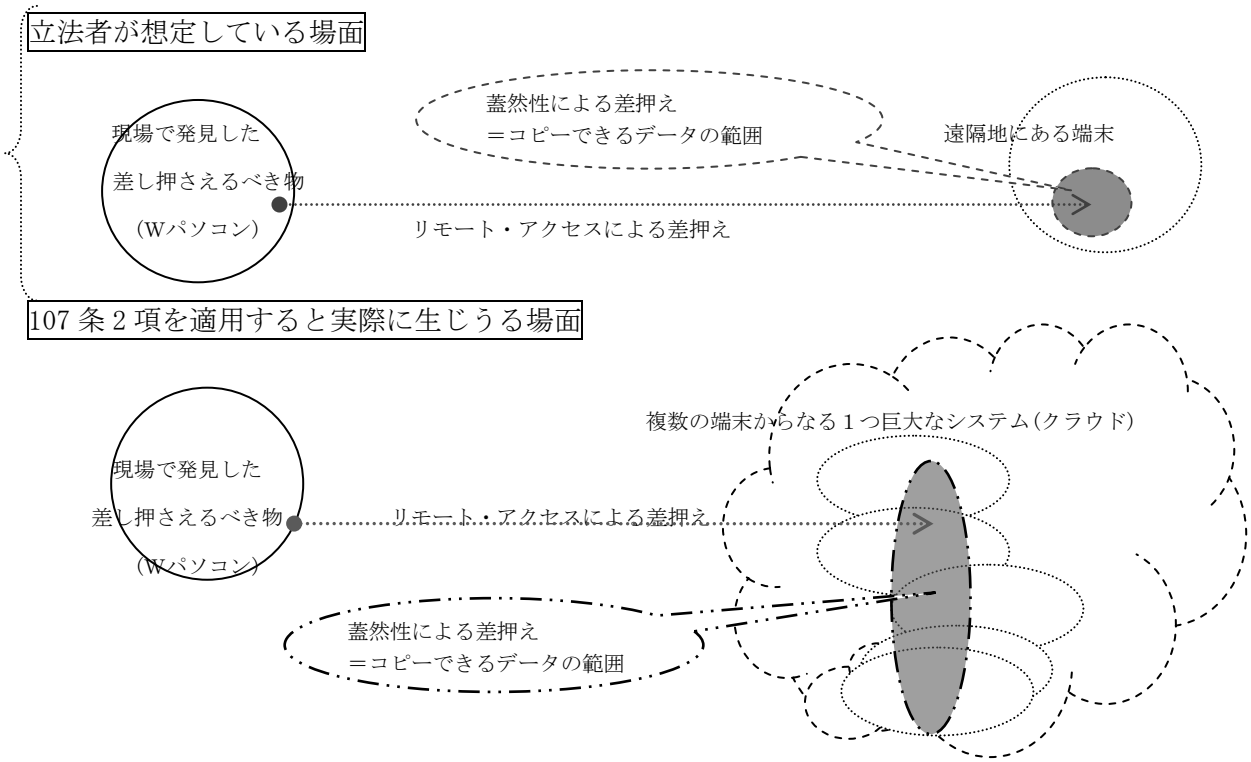
→21・223・224･112/プリンター2

↓

→21・223・224･112/プリンター70

以上の例に，改正法 107 条 2 項の文言を適用すると，リモート・アクセスによる差押えを行うことができる「範囲」には，323 台のサーバーコンピュータ及び 70 台のプリンター内部の記憶媒体が含まれることになる。言い換えれば，「『ある』リモート・ストレージ器機のなかの，コピーできるデータの範囲」という場合の，「ある」の部分は，「323 台のサーバーコンピュータ及び 70 台のプリンター」になり，これらの複数の器機からなる「１つの巨大なシステムの集合体」のうちにおいて，「コピーできるデータの範囲」を画定することになる。この点を図式化すると，次のようなものになる。

図３　リモート・アクセスによる差押えの範囲についての立法者の想定と実際の比較



以上の通り，クラウド・サービス・システムに対するリモート・アクセスの場合，当該システム内部に含まれる情報は，すくなくとも，クラウド・サービスを提供する会社，同社の顧客及び同社の連携社ないし照会・支援・認証先のものが含まれ，かつ，前述した通り，リモート・アクセスによる差押えは蓋然性による差押えの性質を有するものである。それゆえ，この場合には，107 条 2 項の「の範囲」という文言は，前述した「限定機能」の側面をもちつつも，実際には，その「拡張機能」が前面に出てくる。

このように，立法担当者の説明では，１つのＩＰアドレスが１つの遠隔地にある端末に対応し，リモート・アクセスによる差押えは，かかる端末の中にある画定された一定の範囲のデータの集合のみを取得することが想定されているが，107 条 2 項の文言を技術の実態に照らして理解すると，実際には，１つのＩＰアドレスに対応する複数の端末がアクセスの対象となる。とりわけ，クラウド技術のもとでは，複数の端末が１つの巨大なシステムを構成していると同時に，データを保存する態様は多種多様であって，１つのデータが分割されたり圧縮されたりして，システム内のどこにも存在しうることになっているため[235]，結局のところは，この１つの巨体なシステムの集合体がリモート・アクセスによる差押えの対象となる。それゆえ，改正法には，そのなかにある一定の範囲のデータの集合しか取得できないという制限がなされているとしても，その範囲は，やはり広すぎると思われる。

それゆえ，立法論としては，接続の範囲がかなり限定される非常に小規模のシステムの場合であるなら，日本の改正法の関連規定を導入することによってそれに対応してもよいかもしれないが，クラウドのような，複数の端末から結成された１つの巨大なシステムの場合になると，かような対応は不十分であるから，他の可能な対策を検討すべきである。

第３款　リモート・アクセスによる差押えのための捜索

続いて，リモート・アクセスによる差押えのための捜索という問題点を検討したい。前掲の【例 5-1】のような，より複雑な事案においては，リモート・アクセスによる差押えを行うために捜索することが必要となる場合が容易に想定されるし，また，かような事例は決して非現実なものではないから，この問題は重要であり，それを検討する必要があると考える。しかし，日本の改正法は，リモート・アクセスによる差押えのための捜索[236]を全く想定していないようである[237]。

---

[235] アンドリューほか著・分散システム 497～553 頁，井上伸雄・通信技術のすべて 12～16 頁参照。

[236] 従来，捜索とは，差押えの前段階として差し押さえるべきものを発見するための手段と理解されてきた。そうすると，リモート・アクセスによる差押えも差押えである以上，理論的には，リモート・アクセスによる差押えのための捜索を観念することができるはずであろう。例えば，W型パソコンに対する差押えを行う現場で，W型パソコンと接続している遠隔地にある Wz1 型ホストコンピュータの中にあると想定される情報(データ)を取得(複写)するために行うデータの検索ないし検閲があげられよう。

[237] 前述した通り，リモート・アクセスによる差押えは，蓋然性による差押えの性質を帯びるものであるから，アクセス先のコンピュータ内のデータの内容を確認することは不要であるし，また，立法担当者が挙げる，リモート・アクセスの具体例からみても，リモート・アクセスによる差押えのための捜索の場面は考慮されていないように思われるからである(河上ほか編・大コンメンタール第二版補遺[吉田]12 頁，杉山＝吉田・情報処理の高度化(下)100，102，107，109

その理由としては，リモート・アクセスによる差押えのための捜索の問題は，既存の捜索・差押えないし検証という制度の解釈論により解決されているものであるということが考えられる。つまり，この問題に対しては立法による対応を図る必要がないのである。仮にそうであれば，それは，台湾における捜索・差押え・検証という制度の解釈論にも参考になるものだろう。そこで，以下では，台湾の立法論の前提問題として，リモート・アクセスによる差押えのための捜索を認めるための，現行法上可能な根拠は何なのかについての解釈論上の可能性を検討しておく必要がある。

まず，その１つの可能性としては，リモート・アクセスによる差押えのための捜索は，リモート・アクセスによる差押えという処分を構成する要素として認められるという考え方があげられよう。しかし，台湾では，現行法上，独立した差押令状が存在しておらず，捜索令状において差し押さえるべきものを明記するという形になっている点に鑑みると，独立した令状を有する捜索を，独立した令状のない差押えの一要素と見ることはあり得ないであろう。

それでは，別個の令状によって対応することは可能であろうか。この点，日本においては，捜索の対象は差押えの対象である有体物に限られるとするのが通説であり，この点は，改正法の成立後も変わらないであろう。というのも，新設されたリモート・アクセスによる差押え関連規定の直接の処分の対象は，アクセス先の Wz1 型ホストコンピュータでも，そこに蔵置された情報でもなく，当該情報を転写した記録媒体だからである。そうすると，差押えの対象を発見するために行う処分と定義された捜索という制度をもって，差押えの対象にはならない無体のデータを発見(検索ないし点検)する行為を正当化することはできないという帰結が導かれるであろう。

これに対して，台湾の場合には，法文上は，差し押さえるべき物と電磁的記録とを並列し双方とも捜索の対象として認められているから，捜索という制度により，リモート・アクセスによる差押えのための捜索を正当化することは可能であろう。しかし，このようなバーチャル空間において行われる捜索の態様は，伝統的な住居等の捜索のそれとはかなり異なる特徴を持つものである[238]。それにもかかわらず，2001 年の台湾刑訴法改正はそれに対する規制についは何らの規定も設けていないため，物理的な場所を対象とする旧来の捜索の制度のもとでなされてきた原理・原則をそのまま援用する形になるがゆえに，物理的な場所という概念を観念することができないバーチャル空間における捜索の範囲を適切に

頁参照。幕田・捜査法解説 3 版 234 頁，田口・刑訴 6 版 115 頁，安富・刑訴法 190 頁，井上・コンピュータ(2)53～54 頁＝井上・強制・任意 280 頁をも参照されたい)。他方で，杉山＝吉田・情報処理の高度化(下)105 頁(注１)は，「本処分は，差押えの一環として行うものであり，これを行うために，差し押さえるべき電子計算機をネットワークに接続する作業等は，差押えに『必要な処分』として行うことができると考えられる(同法 111 条 1 項)」としているが，ここでいう「接続する作業」に，「リモート・アクセスによる差押えのための捜索」が含まれるとは考えがたい。なぜなら，情報通信分野においては，不正アクセスを検討するにあたって，「接続」と「侵入」とが同義語として使われており(和田ほか・情報 193 頁＝原田三朗ほか・新情報 216 頁)，「捜索」は「侵入」した後の段階を指すものだからである。

[238] 従来捜索すべき範囲は，物理的な場所という要素をもってそれを劃定するものであるが，リモート・アクセスの場合では，前に日本の改正法 107 条 2 項を検討したところで見たように，かような要素の限定機能が働かなくなる。

画定することができなくなるという問題点が残っている。

それでは，検証による対応は可能であろうか。この点，前述した通り，検証とは，物理的な意味での「五官の作用による認識」と定義されているから，同制度により非物理的な意味でのデータの検索ないし点検を正当化しようとすれば，従来の定義との間に齟齬が生じてくる。さらに，体系上の整合性の問題もある。というのも，現行法の基本的な枠組みは，差押えの対象物を発見するための手段として捜索を，発見した物を認識する手段として検証を定めているからである。そうすると，リモート・アクセスによる差押えの対象たる「転写媒体の構成部分にあたる電磁的記録」を発見することが目的であるのに，捜索によらず，検証という手段を使うのは，体系的な整合性を欠くことになるからである。

以上のとおり，問題に対応するには，無体の電磁的記録それ自体を捜索・差押えの対象とする必要があるが，それだけでは足りず，伝統的な捜索と異なる特徴をもつリモート・アクセスによる差押えのための捜索の範囲を画定するための規制ないしその適用基準を用意しなければならないのである。台湾の現行法上はかような手当てがなされていないから，リモート・アクセスによる差押えのための捜索を適正に規制するためには新たな立法による対応が必要となる。

第４款　必要な処分とＩＴセキュリティの解除権

最後に取り上げるのは，リモート・アクセスによる差押えを行うために，捜査機関が自ら，技術的な手段をもって，アクセス先にかかっているパスワードその他のＩＴセキュリティによる支障を解除することができるかという問題である。

この点が，改正法の下でどのように処理されるかは必ずしも明らかではない。というのも，新設されたリモート・アクセスによる差押え関連規定の適用は，捜査機関が既にパスワードやＩＤなどを知っていることを前提としたものだからである[239]。言い換えれば，これまで想定されてきたいくつかの例は，捜査機関が，リモート・アクセスによる差押えを行うために，オンラインでＩＴセキュリティを解除することを必要としない場面ばかりであるようにみえるからである。

もっとも，学説の中には，「対象者の協力が得られない限りリモート・アクセスによりデータを取得することが困難な場合も予想される。そうした事態に対処するためにも，次

[239] 井上・コンピュータ(2)54 頁＝井上・強制・任意 281 頁，河上ほか編・大コンメンタール第二版補遺[吉田]12 頁，杉山＝吉田・情報処理の高度化(下)109 頁参照。また，杉山＝吉田・情報処理の高度化(下)107 頁(注 5)は「第 107 条 2 項……その範囲の特定については IDを用いることが考えられるところ，例えば，当該電子計算機に複数のID・パスワードを使用した痕跡がある場合であっても，『その電磁的記録を複写すべきものの範囲』を特定するために令状に掲げられている IDが，痕跡として残っている IDの一部にすぎないときは，そこに掲げられていない IDに対応する記録媒体からは複写はできないこととなる。」とする。また，「 IDが事前に判明しておらず，『被疑者が使用する ID』という限度でしか特定することができない場合」には，何らかの手段――例えば，「差押えの現場で被処分者から説明を受けるなど」――をもって「『被疑者が使用する ID』を具体的に特定することができるときは，令状の記載としては，具体的な ID までは特定せずに，『被疑者の使用する ID』という限度で特定することも許容されると考えられる」としている。

に見る『協力要請』の導入が図られたものと思われる。……法案でいう『その他の必要な協力』要請には暗号鍵やパスワード等の提示も当然含まれると考えられるが，我が法では現段階では暗号鍵の提示について間接強制を導入するまでには至っていない」と指摘したうえで，捜索差押許可状の呈示に先立ってホテル客室のドアをマスターキーで開けて入室した措置が適法と判断された最一決平成 14 年 10 月 4 日刑集 56 巻 8 号 507 頁を引用し，同決定によりマスターキーの利用による入室が必要な処分として認められているから，「パスワード解読解除ソフトやハッキング・ツール等を用いて当該コンピュータのディスクスペースに侵入こともゆるされるかどうかが問題となるだろう。また，上記決定……を，サイバースペース上でも可能と考えるなら，前もって差押え対象となっているコンピュータにハッキング行為で侵入した上で，その直後に被処分者に令状を提示することも許されることになるのかという新しい問題に直面することとなろう。」とするものがある[240]。

以上の問題につき，台湾においては十分な議論がなされていないが[241]，台湾刑訴法 144 条 1 項が，捜索・差押えのために鍵をあけること，その他の必要な処分を行うことができると定めていることから，上記の日本の学説は受け入れやすいように見える。

しかし，「ドアに対するマスターキーの使用」と「端末に対するセキュリティの解除」を対比できるかについては，大きな疑問がある。というのも，ある端末からＩＴシステムに侵入するためにハッキング・ツールなどを利用するのは，個室に侵入するためにマスターキーを使用するというような容易なものではないし，また，ＩＴシステムへの侵入によって生じうる損害は，場合によっては，個人の巨大な財産的・経済的損失の発生，さらに，大手の会社の倒産というような事態に至ることもありうるからである。

もっとも，上記の論者の見解は，リモート・アクセスによる差押え関連規定の場面においてかかる問題を検討しているわけではなく，新設された協力要請（日本刑訴法 111 条の 2）の文脈のもとでの言及である。そこでは，リモート・アクセスによる差押えを行うために，プロバイダーなどの第三者に協力を求め，ＩＴセキュリティによる支障を解除してもらうことはできるが，捜査機関自らがＩＴセキュリティを解除することはできないということが暗黙の前提になっているとも解しうる。

これに対しては，通常，現場に赴いて，サーバーコンピュータに対しオフラインでの捜索・差押えないし検証を行うためにかかる媒体のＩＴセキュリティを解除することは，必要な処分として認められているから，リモート・アクセスによる差押えはオンラインで行うとはいえ，それも差押えの一種である以上，オフラインの場合と同様に解することができるはずではないかという反論がありえよう[242]。

---

[240] 指宿・サイバースペース 89 頁。

[241] 台湾において，学説上は，電磁的記録をも捜索・差押えの対象としていることから，オンラインで電磁的記録をアクセスしたり取ったりするために，ハッカーのような手法（裏口による侵入やパスワードの解読など）を利用することも現行法上認められているとする見解がある（林鈺雄・捜索扣押 62 頁参照）。

[242] 小木曾 204 頁は「押収された記憶媒体に保存された情報の暗号解読は，住居等に立ち入るのに錠をはずすことができるのと同様，必要な処分として許されると解してよい[。]」とする。

しかし，オンラインの場合は,遠隔操作という方法によるものであるから,複数のネットワークを経由し，最後にリモート・アクセス先に到達するという形になる。言い換えれば,リモート・アクセスの場合のＩＴセキュリティの解除の対象は，遠隔地にあるリモート・アクセス先である端末のみならず，それと繋がった範囲をあらかじめ特定しておくことができない複数の階層のネットワークも含まれることになる。これに対して，オフラインの場合は，既に占有しているサーバーコンピュータのみを対象に,そのセキュリティを解除すればよいという重要な違いがある。

以上の通り，オフラインの場合には，ＩＴセキュリティの解除という処分の対象は捜査機関が占有した媒体という特定の有体物に限られているから，その処分の侵害性の程度が本体の処分である捜索・差押えないし検証を超えていないかぎり，台湾の現行法のもとでも必要な処分としてそれを認めてもよかろう。しかし，オンラインの場合は,リモート・アクセス先である端末だけでなく，それと繋がっている特定されていない複数の階層のネットワークも解除処分を実施される対象となりうるから,技術上にも，処分者の利益侵害にも,オフラインの場合よりも遙かに複雑，かつ深刻なものがある。それゆえ，リモート・アクセスの場合にＩＴセキュリティの解除を行うことが，果たして台湾刑訴法のいう必要な処分として認められるかについては大きな疑問があるのである。

第４節　差押えの場面に対応するために必要な基礎的理論の構築

以上のとおり，有体物のみを対象とする従来の捜索・差押え・検証という制度だけでは,無体の情報を保全・取得・探索・検閲する場面において生じてきている諸問題に対応するには不十分であり，そのためには，情報自体を対象とする必要性がある。しかし，台湾のように，有体物とともに，無体の電磁的記録も捜索・差押えの対象として旧来の条文に追加するだけでは，問題の解決にはならないばかりでなく，かえって法解釈上の不一致と混乱を招致してしまうことになる。そこで，この不一致と混乱を是正するために，次のような立法提案がなされている。

「伝統的には，差押えは，国家機関が対象者の特定の『有体物』（tangible objects）に対する占有を剥奪したうえで，当該物を占有することと理解されてきたため，コンピュータ鑑識人員は媒体内に記録された無体の情報あるいはファイルを差し押さえることができず，その内容を知ったり，その複製を取得したりすることができるだけである。そこで,本条[台湾刑訴法133条]2項2款を，『捜索すべき，被告人，犯罪嫌疑者，電磁的記録あるいは差し押さえるべきもの。』と修正すべきである。そのうえで，現行同条項3款の規定により捜索票上記載すべき事項は『捜索すべき場所，身体，物件あるいは電磁的記録』であるが，本款は，裁判所が令状において捜索の客体（あるいは対象）を詳しく記載すべきであることを要求するものである。しかしながら，電磁的記録は，『電子，磁気，光学あるいはその他の類似する方式により作成し，コンピュータの処理に供する』情報にすぎず(台湾

刑法10条6項参照)，捜索(検索)を実施する対象ではないのである。ファイルあるいは情報の検索(コンピュータ鑑識)を行う本当の客体(所在)は，電磁的記録を記載した媒体である。そこで，本款を『捜索すべき場所，身体，物件あるいは電磁記録媒体。』と修正すべきである。」[243]

確かに，かような提言により，差押えの定義と法文上の文言との間にある不一致及びそれにより招かれた法解釈上の混乱を免れることができる。しかし，かかる提言は，問題の解決には意味が薄いものであると言わざるをえない。というのも，もし，捜索・差押えの直接の客体は，媒体自体であるとすれば，媒体はすでに物件という概念により包摂されているものであるので，かような修正(台湾刑訴法133条2項3款)は不必要であるし，また，現行法133条2項2款のいう「差押えるべき物あるいは電磁的記録」の文言について２つの理解可能性があり，その１つは，「差押えるべき物」あるいは「差し押さえるべき電磁的記録」であり，もう１つは，「差し押さえるべき物」あるいは「電磁的記録」であるので，この意味で，解釈論によっても解決されうるとすれば，前掲の立法提言の必要性は低くなると言わざるを得ないからである。

仮に，どうしても有体物のみを強制処分の直接の対象とする従来の法の枠組みを維持しようとするのであれば，上記の立法提言を取るよりも，むしろ，ここまでに紹介した日本の枠組みを採用するほうがより妥当であろう。というのも，日本の今度の改正法は，有体物のみを対象とする刑訴法の旧来の建前を維持しつつも，有体の媒体を通じて無体のデータを間接的な処分の対象とする形で，電磁的記録の場合に特別な規定を設けており，これによって，前述した台湾の現行法上の不一致ないし混乱という問題を解消することができると同時に，意味が薄い立法となってしまうという問題点もなくなるからである。しかし，以上の検討によっても明らかにされたように，改正法をも含めた日本の現行法のもとにおいては，なお未解決の問題点が数多く残されている。

それゆえ，本稿では，日本の議論状況を参考にするだけでは足りず，日本と並んで，情報と刑事手続というテーマに関する先進国でもある独米における関連議論をも採り入れる必要性があると考える。すなわち，台湾の立法論としては，情報を独立した(強制)処分の(直接の)対象としたうえで，情報を対象とする場合に相応しい強制処分の定義ないしその適用の基準・原則を探求し，有体物を対象とする場合と統合できるような，新しい刑事手続法を構築する必要がある。具体的には，日本法と並んで，アメリカとドイツにおける問題状況ないし関連議論を検討し，日独米三カ国の比較法の視点から，「情報に対する捜索・差押え」という新制度を検討し。

以下では，こうした「情報に対する捜索・差押え」という新制度の内容を具体化していくが，まずは，以下の理由で，「情報の差押え」という制度から議論を展開していく。

以上の設例により示されたとおり，無形の情報を対象とする場合，データを取得・保全するという差押えの場面のみが問題となるわけではなく，データを検索・検閲するという

[243] 李・電磁記録 1094 頁。

捜索の場面でも問題が生じうる。それにもかかわらず，日本においても，台湾においても，実務的に問題として浮上しているのは，差押えの場面ばかりであるし，また，日本の今回の改正法も，差押えという側面で生じてきた問題のみを対象としており，捜索という側面に関わる諸問題(たとえば，検証のための捜索やリモート・アクセスによる差押えのための捜索などの問題)に対応していない。それは，次のような理由によるものである。

日本においても，台湾においても，占有の剥奪を必要とするという差押えの従来の定義は変わっていないため，捜査機関にとっては，対象となるデータを取得するためにもっとも便利(時間ないし技術上)かつ妥当(証拠保全上)と思われる手段は，有体の媒体に対する差押えという選択肢となる。つまり，「コンピュータ・ネットワークと捜査」という文脈のもとで，ほとんどの場合は，前述した蓋然性による差押えが先行する形になる。そうすると，すでに合法的に占有が剥奪された媒体の中身に対して検索・検閲を行うことの法的な位置づけは，捜索でなく，証拠調べの方法としての「鑑定」(台湾刑訴法 197 条以下参照)ないし警察機関が職務行為として行う「鑑識」というものになる。その結果としては，この後段階の鑑定(ないし鑑識)は，実質的には捜索の性質を有するものであるにもかかわらず[244]，令状による規制もなしに，媒体に蔵置されたデータに対して隅から隅まで検索・検閲することができることになってしまう。言い換えれば，蓋然性による差押えを実施する場合には，検証のための捜索という問題は，理論上は重要なものであるにもかかわらず，実務上は，それが実際の問題となる可能性は極めて低い，ないし皆無であるといえよう。言葉を換えて言えば，有体物を対象とする場面での捜査の順序は，「捜索→(関連性による)差押え」であるのに対して，無体の情報を対象とする場面では，順序が逆転し，通常は「(蓋然性による)差押え→捜索(鑑定・鑑識)」となるため，従来の捜査の順を前提に想定された規制によって対応できない点が問題である。そこで，この問題を解決するには，まずは，差押えの在り方を再検討する必要があると考える。

以上のとおり，「情報に対する捜索・差押え」という制度を構築するには，「情報の差押え」という制度から議論を展開するべきである。そして，「情報の差押え」という制度を作るために必要不可欠な３つの基本的問題がある。

(1)なぜ，立法論として，有体物と並んで，無形の情報をも差押えという制度の直接の対象とすべきなのか。

(2)無形の情報は，有体物のように物理的に支配・管理することが不可能であるとされてきた。そうだとすれば，立法論として，情報を差押えという制度の直接の対象とすることは可能なのか。

(3)仮に，無形の情報をも差押えの直接の対象とすることは必要かつ可能であるとすれば，情報を物と同程度に保護するためには，新たな法益侵害の判断基準，そして，その前提となる新たな法益論が必要となる。というのも，仮に，従来の物に対する法益侵害の判断基

[244] 類似する見解として，李・電磁記録 1064～1066，1068 頁。だが，その理論の構成のなかみは，本稿のそれとは異なるものがある。

準，すなわち占有剥奪という基準を，情報を対象とする場合にもそのまま適用すると，情報をコピーするだけでは占有剥奪があるとは言えない以上，侵害がないことになるから，情報の要保護性が事実上否定されてしまうからである。そうだとすれば，立法論的としては，この新たな法益・基準の具体的な中身は何なのかである。

第１款　情報を差押えの対象とすることの必要性

ここまでの検討をもとに，情報を差押えという処分の直接の対象とする必要があると考える。その理由としては，次の４つのものが挙げられよう。

Ⅰ．実質的な過大差押えへの対応

実質的な過大差押えの問題に対しては，前述した通り，日本においては，これまで，①利益衡量論，②検証の差押え的性格の活用，③アウトプットという実務の慣行，の３つの対応策が考えられ，また，改正法により，差押えに代わる処分の規定が新設された。これらの対応策は台湾にも参考となるものが含まれていると思われるものの，それらによる問題の解決には限界があり，すべての問題が解決されているわけではない。

もっとも，実質的な過大差押えという問題は，電磁的記録の場合に特有なものではないのである。例えば，前掲の【例 4-2】の事例で，警察官Ｆが，別の部屋で，もう一冊の厚い帳簿（1200 頁)を発見し，その中身を見たところ，その第 19 頁の第 1 行目から第 3 行目までの部分のみ被疑事件と関係があったとしよう。この場合，現行の台湾刑訴法のもとにおいては，第 19 頁の第 1 行目から第 3 行目までの部分のみ捜査事件と関係があるにもかかわらず，1200 頁の帳簿全体を差し押さえることができる。

従来は紙媒体と文字とが物理的に不可分であったから，このような差押えも特に問題とされてはこなかった。しかし，現在，デジタルカメラないしスキャン技術を利用すれば，文字の撮影やスキャンという物の情報化の手段により情報のみを取得することが可能になっている。この意味で，有体物である書類を対象とする場面においても，電磁的記録につきデータのみを取得するだけで十分な場面で見られた，実質的な過大差押えと同じ問題が生じるということができよう。つまり，情報を独立した処分の対象とする刑事手続の在り方を考えるに際しては，情報を対象とすることの必要性にのみ着目するのではなく，物と並んで情報をも対象とすることの必要性にも着目する必要があると考える。

Ⅱ．事後救済制度の整備

日本の現行法のもとにおいては，物が捜査機関に取得された場合には，還付及び準抗告

という救済策があるのに対して，情報――例えば，顔写真――が取得された場合には，そのための救済手段が用意されていない[245]。

これに対して，台湾では，2001 年に刑訴法が改正され，電磁的記録も捜索・差押えの対象として追加されることになったため，顔写真という情報がすでに電磁的記録という形で存在しており，それが政府に取得(コピー)された場合，理論的には，電磁的記録の差押えとして，準抗告などの事後救済の規定が適用されると解することができるように思われる。しかし，前述したとおり，2001 年以後にも旧来の差押えの定義ないし適用の基準自体は全く変わっていないから，電磁的記録をコピーするだけで通常は占有の剥奪が発生せず，物理的な意味での財産権上の損害も生じない以上，デジタルコピーを，電磁的記録に対する差押えとはいえないから，結局のところ，事後救済の規定を適用することができないという帰結になると思われる。

情報が政府に取得された場合も，物が押収された場合と同様に，事後の救済策を用意すべきであり，そのためには，情報自体を独立した処分の対象とする必要がある。そのうえで，情報が政府に処分されたといえるための基準は何なのかを探求しなければならない。

ところで，日本では，情報のみを取得された者に比べ，当該物件全体の占有を奪われた者の被る被害はより大きいから，物のみを保護の対象とする現行法(日本刑訴法 420 条 2 項・430 条 1 項，2 項)には合理性があるとして[246]，情報のみを取得する処分を当該物件全体の占有を取得する押収と同一視することには理論上，なお飛躍があるという見解が有力である[247]。また，一定の場合に救済手段を認めるとしても，無体の情報が捜査機関に取得された場合，情報自体をそのまま返還することはありえないから，それを記録した媒体を廃棄ないし引き渡すという方法によらざるをえないが，そうすると，捜査機関が持参した媒体に転写した場合，被処分者である情報主には，その媒体の所有権や占有権がないため，その廃棄ないし引き渡しを要求する権利はないとされてきた[248]。

確かに，情報と媒体との間の物理的な結合関係を前提とすれば，「物件(媒体)＋情報＞情報」という公式が成り立つので，上記の理解は妥当であり，差押えを占有の剥奪と定義している台湾の現行法の解釈論としても通用すると思える。そして，書類や小容量の記録媒体のように，情報と媒体の価値にそれほど差がない場合には，実質的にもそれが妥当する。しかし，現在の情報社会においては，情報が媒体より遙かに高い価値を持つ場合（例

---

[245] 最小(二)決平成 2 年 6 月 27 日刑集 44 巻 4 号 385 頁。

[246] 大谷 1641 頁。

[247] 井上・強制・任意 367 頁。ただし，井上教授は，結論としては，情報の押収が現行法の下では許されないとしても，それが事実として行われた場合に，その行為が押収としての性格を持つとして，かような場合には，準抗告による救済の対象となると解すべきであるとしている。また，写真撮影によって押収に匹敵するほど重要な継続的権利侵害が生じるような場合には，「押収に準ずる処分」として準抗告を認めるべきとする見解もある(後藤・捜査法 27 頁，福井・刑訴講義 5 版 158 頁参照)。

[248] 高部 55 頁，北村滋・写真撮影 67 頁，横田＝高橋 327 頁。井上教授は，基本的に，同見解を支持しつつも，少なくとも，当該情報に対する捜査機関などの支配を完全に排除する適切かつ確実な措置(例えば，裁判所に問題のファイル等を提出させ，廃棄することなども考えられよう)が取られることを求めることはできると解されると述べている(井上・強制・任意 373 頁)。

えば，新しく開発した高価なソフトウェアとそれを保存する媒体との関係）も稀ではなく，かかる場合には，「媒体＋情報」と「情報のみ」の価値が同程度となることもある[249]。そうだとすれば，事後救済の制度を設ける際にも，この点を視野に入れる必要があろう。言い換えれば，その重点を，転写媒体に対して被処分者である情報主に所有権や占有権があるかどうかという点に置くべきではなく，媒体と情報との結合関係及びそれぞれの（価値）構成比例という点に着目すべきである。

そして，かような考え方が成り立つことの前提として，情報は，媒体に付属する構成成分ではなく，媒体と対等の位置にある独立した処分の客体であることを認めなければならない。言い換えれば，物と並んで，情報をも独立した直接の処分の対象とすることが必要となるのである。

Ⅲ．事後規制の実現

前述したように，通常の差押えであれ，蓋然性による差押えであれ，それらのいずれについても事後規制が必要となる場合が生じる。しかしながら，日本の現行法のもとでは，事後規制は働かない。というのも，従来，差し押さえられた物について，その内容等を点検する行為は，性質としては，その物の検証にあたるが，それは，差押えという処分の中に当然に含まれていると考えられており，その部分について別途に令状は必要とされないと理解されてきたし[250]，この理解は，改正法のもとにおいてもそのまま適合するものだからである。言い換えれば，現行の差押えという制度は，有体物のみをその処分の直接の対象とするので，適法に占有を取得した記録媒体である以上，蓋然性による差押えか否かを問わず，差押え後に，当該媒体の内容を確認することは，媒体に対する新たな侵害にはならないからである。

かような理解は，差押えを（有体物に対する）占有の剥奪と定義している台湾の現行法のもとにおいても，そのまま当てはまるものであろう。というのも，台湾刑訴法144条1項のいう捜索・差押えのために必要な処分の目的は，差し押さえるべき物を発見しその占有を剥奪することにあると解されてきたため，すでに差し押さえられた物に対する検証をここでいう必要な処分と解することはできないが[251]，前述の見解によると，適法に占有した物を検証することは，差押えという処分における本来の効力のなかに当然に含まれており，差

---

[249] 佐久間・無形的財産の保護 192 頁以下（とりわけ 194，200，210～211 頁）参照。

[250] 川出・物の占有 6 頁。

[251] これに対して，日本においては，押収したフィルムを現象することを，「当該押収物の性質上」，これに対する必要な処分であると解した東京高判昭和 45 年 10 月 21 日高刑集 23 巻 4 号 749 頁によると，差押え後も必要な処分を認める余地があると解されよう。言い換えれば，日本の場合には，捜索・差押えのために必要な処分の目的は，差し押さえるべき物を発見しその占有を剥奪するために限らないと解される。しかしこれに相対し，媒体のシステムを利用し複写又は印刷を行うのは，媒体の差押えとは違った管理権の侵害を伴う行為であるし，差押え後の処分であるので，これを直ちに差押えに必要な処分ということはできないとの指摘がなされていたのであるとする論者がある（古田・第三者の保護 193～194 頁。杉山＝吉田・情報処理の高度化（下）57 頁をも参照）。

押えの一環として捉えてよいという帰結になるからである[252]。

以上の理解は，差押えを占有の剥奪と定義している台湾の現行法のもとでは正しいものといえるだろう。しかし，逆に，媒体と並んで，情報それ自体をも独立した強制処分の直接の対象とすることを前提としたうえで，情報に対する差押えといえるための基準が，有体物に対する占有の剥奪ではないとすれば，技術的な問題ないし捜査のニーズなどの理由で，とりあえず記録媒体を差し押さえたというような場合に対しては，媒体に対する占有の剥奪によって，その内部に蔵置された情報も当然に差し押さえられたわけではないと解する余地があるから，それに対する別途の事後規制を設けることも可能になると思われる。

Ⅳ．オンラインで行う処分の場合への対応

ここまでの検討により，単に，電磁的記録という文字を既存の法文内に追加するだけである台湾の現行法は，リモート・アクセスで捜査を行う場面に対応できないことは明らかである。これに対して，日本のリモート・アクセスによる差押え関連規定はオンラインで行う処分の場合に対応するものと考えられるが，それも有体物のみを対象とする現行の日本刑訴法の枠の維持を前提としているものであるから，問題の解決には十分だとはいえない。ここで確認すると，次の４点が重要である。

１．物理的な基準の局限性

日本のリモート・アクセスによる差押え関連規定は，有体物のみを対象とする現行法の枠を維持していることから，差押えには，何らかの形での有体物という物理的な基準を介在させなければならず，そのために，リモート・アクセスは現場で差し押さえた被処分者の媒体からでなければならないという限定が設けられることになった。つまり，アクセスできる範囲は，一定の物理的な場所に置かれた有体の電磁的記録媒体により限定されている。

しかし，問題は，技術的にも，また法的にも，リモート・アクセスを被処分者の媒体からしなければならない必然性があるわけではないし，また，対象者の財産権の保護の観点からしても，警察機関の所有する媒体から行う方が妥当だと思われるから，かような限定の実質的な妥当性については疑問の余地があるように思われる。そうだとすれば，この設計は，台湾の立法論として，最良策とはいいがたいであろう。

２．オンラインとオフラインとの相違

オンラインの場合とオフラインの場合との間には以下のような重要な相違点があるから，

[252] 実際にも，林鈺雄・捜索扣押 254 頁は，捜索・差押えという本体処分を執行するために必要な処分を行うことは，新たな権利侵害にはならないかぎり，明文の規定がなくても，それを，本体処分の授権範囲内にあるものであると解することができるとする。

日本の今回の改正法のように，オフラインの場面で適用される「蓋然性による差押え」という概念を，そのままオンラインの場面，つまり，リモート・アクセスによる差押えの場面に採り入れると，一般令状となってしまう懸念がある。

というのも，オフラインの場合には，有体物である媒体を直接に接触する形になるから，従来の場所基準をそのまま適用するか，それとも，類推適用することが可能である。つまり，オフラインで電磁的記録を捜索する可能な範囲を，捜索すべき場所で発見される対象となる電磁的記録が存在する蓋然性があるすべての電磁的記録媒体に限ることができるのに対して，オンラインの場合には，物理的な空間である捜索すべき場所という概念を観念することすらできないから，上記のような解釈をとることによる制限ができなくなるため，この意味で，一般令状となる懸念があるからである。

そこで，前述したとおり，技術上ないし捜査のコスト(時間や人力など)上の理由で，無体の情報を対象とする場合には，「(蓋然性による)差押え→捜索(鑑定)」という順になる場合があるため，日本の「蓋然性による差押え」という概念は，台湾にとっても制度としての必要性があるが，立法論としては，かかる概念の適用については，オンラインの場合とそうでない場合とを区別する必要性があるかどうかを考えるべきである。

3．オンラインで行う捜索への不対応

オンラインの場合は，対象となる電磁的記録を探索・取得するに先立ち，まずは該当記録が存在する蓋然性がある一定のＩＴシステムの範囲にアクセスしなければならない[253]。ここでは，オンラインの場合に，理論的に無限に連結可能なバーチャル空間において，捜査機関がアクセスできる範囲を限定するための基準は如何なるものであるか，言い換えれば，いわゆる「リモート・アクセスによる差押えのための捜索」をいかに規制すべきかという点が重要な問題となる。

それにもかかわらず，日本でのリモート・アクセスによる差押えは，有体物のみを対象とする現行法の枠組みを維持しているものであるから，オンラインで捜索を行う必要はない場面にのみ対応している。

それゆえ，台湾の立法論としては，むしろ，情報をも独立した強制処分の対象としたうえで，正面から，リモート・アクセスによる差押え並びにリモート・アクセスによる差押えのための捜索の在り方を思案すべきことになろう。

---

[253] 台湾において，学説上，「会員制のわいせつサイトを検挙するため，当該サイトのサービスマシンにアクセスして，ダウンロードの方式でその電磁的記録の証拠を取得したい場合，捜索令状に，『URLのhttp://www.enjoysex.com.tw のHP，わいせつ画像ファイル及びインターネットマシン内に記録された顧客の取引資料』という記載をすればよい」というような例があげられている(林鈺雄・搜索扣押 95 頁)。これは，物理的な空間でいう住所の概念をそのままインターネットの世界に当てはめるもの――URLをネット上の住所と考えてよいとされる――と考えられるが，しかし，【例 5】であげたような複雑な事例では，かような限定が働かなくなる。

４．各別の令状原則の意味の再考

オンラインで行う処分の類型は，リモート・アクセスだけではなく，前にも言及した概括令状によるトレース・バック捜査もその一例として考えられる。ここでは，次の２点が重要である。すなわち，①立法論的には，プロバイダーなどの通信業者が間接強制処分の罰則を甘受し，協力しない可能性もあるとすれば，捜査機関は，1 つの概括令状をもって，みずから転送の全過程におけるすべてのＩSP ないし経由点のシステムにアクセスしたり，それぞれのシステムに蔵置されたデータを検索したり，ダウンロードしたりするような新型の捜査手法――つまり，オンラインで情報を独立した捜査の対象とする直接強制処分――を設けることが必要となる。②かような概括令状は，複数のプロバイダーなどのネットワーク管理者を対象とするものであるから，いわゆる一場所一令状原則（各別の令状原則）[254]に反するおそれがある。というのも，かかる複数の管理者が常に複数の異なる場所に散在し，各場所は異なる管理権に服するものだからである。

しかしながら，もし，処分の対象が，有体物ないし物質空間[255]ではなく，無体の情報ないしそれが存在するバーチャル空間[256]となると，各別の令状原則を，従来のとおり，一場所一令状と理解する合理性が欠ける。というのも，バーチャル空間においては，物質空間のように物理的な場所という概念を観念することができないからである。

Ⅴ．小結

以上のとおり，ここまでに指摘した数々の問題点を解決するには，最終的には，物と並んで，情報をも独立した強制処分の直接の対象とする立法を行う必要がある。

そのための具体的な検討課題としては，①実質的な過大差押え，②蓋然性による差押え，③リモート・アクセス，④直接強制力付き概括令状によるトレース・バック捜査，という４つのものがあげられよう。このうち，本章においては，①と②を取り上げ，③と④については，第２章において取り扱うことにしたい。

---

[254] 各別の令状とは，通説によれば，「一場所一令状」と理解されてきた（小野・ポケット（上）256頁，伊藤ほか・注釈（新版）２巻［佐藤］178頁＝初版：青柳ほか・註釈(1)［佐藤］392頁，松尾・条解4版218，220頁，田宮・強制捜査268頁，田宮・注釈刑訴129～130頁，田宮・捜査・公訴［荻原］347頁，藤永ほか編・大コンメンタール（二）［渡辺］341頁，瀧川・刑訴コメ146頁，樋口ほか・注釈憲法（上巻）［佐藤］756頁，熊本・憲法三五条160頁，法務省・実務刑訴126頁）。これに対して，反対説がある（河上・証拠法ノート(1)3頁，横井・各別の令状62頁。また，大澤・特定435頁をも参照）。

[255] 本稿でいう「物質空間」とは，下述する「バーチャル空間」に対峙する概念であり，「実体を伴い，物体や生物など実在する一切のものを資源として利用・消耗することによって動いている人間の生活環境」を意味する。

[256] バーチャル空間とは，「実体を伴わず，コンピュータの計算結果を，数字で表示する仮想的環境」と定義される。

第２款　支配・管理の可能性

ここでは，無形の情報を差し押さえることは，果たして可能なのかという問題点を検討する。

この点，有体物に対しては，それを支配・管理するために，占有の剥奪という手段が取られる。しかしながら，無体の情報については，その占有の剥奪を行うのは不可能である。

しかし，無形の情報について，それを支配・管理するための手段を，有体物と同様に，占有の剥奪に求める必然性はない。そこで，以下では，物理的な場面と非物理的な場面とを分けて，無形の情報に対する支配・管理の可能性を検討する。

Ⅰ．物理的な場面

日本において，情報が強制処分の対象にならないとされる論拠の核心は，差押えに関する刑訴法 99 条 1 項の文言による制限にある。このことは，逆に，立法によれば，情報を強制処分の対象とすることは否定されないことを意味する。そして，現代社会の実情に鑑みれば，情報を独立した差押えの対象とする実益があるし，科学技術を使用すれば，その特定や管理が困難であるとはいえないという評価も一部でなされつつある[257]。しかし，それらも情報の差押えという制度を正面から支持するものではない。

これに対して，台湾刑訴法 133 条 1 項の文言は，日本刑訴法 99 条 1 項のそれと類似しており，通説によると，「物」という用語は，特別な定義がなされていないかぎり，「有体物」を意味するから，133 条 1 項でいう「物」は有体物をさすとされてきた[258]。しかし，2001 年の台湾刑訴法改正は，133 条 1 項の文言を従来のままにして，同法 122 条 2 項において，電磁的記録は，「差押えるべき物」と並んで，捜査機関が捜索(差押え)令状により捜索できる対象として列挙している。そこで，電磁的記録は有体物ではないが，それも差押えの対象であると解されている。

しかし，現行法上の差押えとは，占有の剥奪を必要不可欠な要素とする点は，いまでも全く変わっていないから，結局のところ，占有の剥奪を観念できない無体の電磁的記録に対しては，それが差し押さえられたといえる場面はほとんどないではないかという疑問が残る。つまり，台湾では，2001 年の法改正により形式的には電磁的記録も捜索・差押えの対象として列挙されていることになったけれども，一体何をもって，無体の電磁的記録が差し押さえられたといえるのかは不明であるから，実際には当該法改正も情報の差押えという制度を正面から支持するものではないのである。

このように，情報の差押えを観念する可能性があることを認めながら，情報の差押えと

---

[257] 井上・科学捜査27～28頁，井上・傍受92頁，川出・コンピュータ犯罪1～2頁，新保147頁以下，壇上52頁，指宿・モノからデータへ1～2頁等参照。

[258] 林富郎・通訊監察 16 頁，陳仟萬・監聽 9 頁。

いう制度を正面から支持しないのは，一体なぜなのか。その理由は，従来，刑事手続における強制処分の対象に対する支配・管理は，物理的な意味でなされなければならないとされてきたことに求められるであろう。というのも，同じく無体物である光，熱，電気等のエネルギーは，実存する物質であり，物理的な支配・管理が可能であるのに対して[259]，情報は，実存する物質ではなく抽象的な観念としての仮想的な存在に過ぎず，それ自体を直ちに物理的に支配・管理するのは不可能であって，ある媒体に組み込まれて実存する物質になって初めて，物理的な支配・管理が可能になるからである。

そうすると，仮に，強制処分の対象には物理的な支配・管理可能性を必要とするという前提に立つとすれば，立法論としては，無体物であるエネルギー等を独立した強制処分の対象とすることが限度であって，物理的な支配・管理を観念できない無体の情報を独立した強制処分の対象とすることは困難であるという帰結になろう。

しかし，そもそも，なぜ，情報を独立した強制処分の対象とする場合においても，物を強制処分の対象とする場合と同様に，物理的な支配・管理可能性を要求しなければならないのかは疑問である。むしろ，非物理的な支配・管理可能性という観点から，情報の独立した強制処分の対象としての適格性を再検討する必要があると思われる。

Ⅱ．非物理的な場面

非物理的な支配・管理可能性とは，情報に対して独立した処分の対象としての適格性を認めるために必要な法的定義ないし保護要件として実定法化された，科学技術上並びに法的概念上の支配・管理可能性を意味する。具体的には，著作権法においては，無体の情報に創作の価値としての法益の要保護性が認められ，そのような保護の対象とすべき法益を含む情報には著作権が発生すると定められていること[260]，民事手続においては債権の差押えという制度が設けられていること[261]などが，その例として挙げられる。

刑事手続においても，同様の法技術を採用することができるはずであり，かつ，そうすべきであろう。というのも，現在，自動記録，自動分析，自動探索といった科学技術によれば，犯罪立証に役立つ情報を，非物理的な意味での支配・管理に服させることが可能になっており，かつ，物理的な支配・管理を観念できない無体の情報と，物理的な支配・管理を観念できる有体物ないし無体物とは，それぞれの特徴が異なる以上，必ずしも，両者について，強制処分の対象としての適格を認めるための法的な定義及び保護法益の構成要

---

[259] 無体物は強制処分の対象にならないとする通説（前掲注 97 のほか，伊丹編著・実例 3 頁，幕田・捜査法解説 3 版 182 頁をも参照されたい）に対峙し，現行法の下で，電気，熱などの無体物であっても，管理可能であれば，差押えは可能であるとする見解もある（書上 12 頁，伊藤ほか・注釈（新版）2 巻［藤永］151 頁＝初版：青柳ほか・註釈(1)［藤永］370 頁，松尾・条解（第 3 増補）171 頁〈しかし，同・条解 4 版 203 頁は，「エネルギーも物理的に管理可能なら差押可能……」という部分の文字を削除した〉，安富・刑訴法 137 頁）。また，林鈺雄・捜索扣押 200 頁§133/11 によると，一般の物件のほかには，指紋や気体なども物理的に管理可能なので，差押えの対象と解される。

[260] 日本の著作権法 17 条 1 項，同 51 条 1 項；台湾の著作権法 10 条，同 30 条参照。

[261] 日本の民事執行法 145 条 1 項及びその民事保全法 12 条 1 項 4 号；台湾の強制執行法 115 条 1 項，同 115 条の 2 参照。

件を同じにする理由はないからである。

そうだとすれば，仮に，物理的な支配・管理という従来の観点と異なる，非物理的な支配・管理を具体化することさえできれば，正面から，物と並んで，あらゆる類型の情報をも独立した強制処分の対象とする立法を行うことは可能であるはずである。というのも，非物理的な支配・管理の具体化をもって，情報に対する支配・管理可能性を実定法化することができるからである。

第３款　あるべき法益論の構築

続いて，情報が差押えの対象として支配・管理された場合，それにより侵害される法益は何なのかという点を検討する。

前述した通り，情報の差押えという制度を創設することが立法論的に困難とされる理由は，差押えの定義が，占有の剥奪を必要不可欠な要素としてきたという点にあった。無体の情報に対しては，有体物のように，占有を剥奪するという形により物理的な支配・管理を行うことが不可能である以上，それを，差押えの直接の対象とすることの可能性も否定されてしまうわけである。

しかしながら，物と情報は異なる性質を持ち，それぞれに対する侵害の態様は異なるから，両者に同じ基準を適用する合理性はないと考えられる。

この点，従来は，有体物のみが証拠として扱われる現行台湾刑訴法の下では，占有剥奪が有体物である証拠を確保する唯一の手段とされてきた[262]。そこでは，差押えという制度により侵害される法益は，有体物に対する財産権であると解され，かかる法益が侵害されたといえる基準は，財産権をなす１つの要素である「占有」が剥奪されたという点(以下，「占有剥奪基準」という)に求められてきたのである[263]。

しかし，情報を差押えの対象とするには，必ずしも，有体物のように占有剥奪を必要な要素としなければならないわけではない。というのも，従来の占有剥奪基準の採用は，有体物が差押えの対象である場合を前提とするものであるから，かかる基準を，情報を差し押さえる場面にそのまま適用する必然性はないからである。そうすると，次に，占有剥奪に匹敵する新たな法益侵害の判断基準，そして，その前提となる新たな法益を探求する必要が生じる。

これに対しては，新たな法益や新たな法益侵害の判断基準を探求しなくても，占有剥奪基準を準用すれば足りるとする見解も存在する(以下，「準用説」という)。そこで，まずは，Kerr に代表される準用説の内容とその問題点を明らかにしておくことにしよう。

---

[262] 范・過度扣押 10 頁は，電磁的記録をコピーすることは差押えの概念に当たらないとする。田宮・注釈刑訴 123 頁，松尾＝田宮・刑訴基礎知識 75 頁，鈴木茂嗣・刑訴改訂 86 頁をも参照。

[263] 同前注。

Ⅰ．準用説の内容と問題点

Kerrは，情報も修正４条の捜索・差押えの対象になりうるというKATZ事件の判断を前提としながら，手書きで情報を記録するだけでは差押えに当たらないとしたHICKS事件[264]の判断を是認している[265]。ここでいうHICKS事件の判断とは，ステレオのシリアル番号を単に記録することは，被告人が捜査機関によって終局的にステレオを奪われる過程の最初の段階に過ぎず，被告人の財産に対する意義ある干渉にあたらないから，それは差押えを構成しないという判示を指す[266]。

アメリカでは，ここで示された「財産に対する意義ある干渉」が，物理的財産権を基礎として理解され，物理的な剥奪(すなわち，占有剥奪)があって初めて「意義ある干渉」に該当すると理解されているがゆえに，KATZ事件が情報も捜索・差押えの対象になり得ると判示した後も，差押えに占有剥奪が必要とされているのである[267]。

Kerr は，このような占有剥奪を必須要素とする差押え概念の理解に賛成しつつも，HICKS の射程は限定すべきであると主張する[268]。すなわち，HICKS が示した通り，手書きで番号をコピー(記録)するだけでは差押えに該当しないとするのは正当であるが，少なくとも，原本と複製との同一性が担保できるビット連続コピー（a bitstream copy）[269]の場合には情報の差押えに該当しうるから，HICKS 判決の射程外と解すべきであるというのである[270]。

しかし，コピーをするだけで占有を剥奪していないという点は，手書きであってもビット連続コピーであっても，同じである。それにもかかわらず，なぜ，ビット連続コピーの場合のみを，差押えに当たると解することができるのか。

この問題に対し，Kerr は，占有剥奪基準を準用することによって対応する。すなわち，ビット連続コピーが情報の差押えに該当するかどうかを判断するための基準は，データに対する占有剥奪の有無ではなく，媒体の占有に対する侵害の程度に求めるべきというのである[271]。具体例で説明すれば，ビット連続コピーをするためにわずかな時間しかかからない

---

[264] ARIZONA v. HICKS (1987) 480 U.S. 321. 本件の概略は以下の通りである。弾丸がアパートに発射されたという緊急状況の下，警察官が被告のアパートに入ったところ，警察官のうちの１人が高価なステレオ器材２セットに気づいた。彼はこのような高級なものがそのアパートの汚さにふさわしくないことから極めて怪しいと考え，この器材のシリアル番号を読んで記録しようとして，シリアル番号を探すために器材を少し動かした。そして，本部に数回の電話をかけ，その器材のうちターンテーブルが武装強盗によって盗られたものであることを確認した後，当該器材を差し押さえた。被告人は強盗罪で起訴されたが，最高裁は器材を動かすことは弾丸事件の捜索と異なる別個の捜索であるとした。そして，本件はプレイン・ヴュー原則を適用するための相当な理由がないため，このような捜索は修正第４条によって合理的とはいえないから，証拠排除すべきだとした。

[265] Kerr, DIGITAL WORLD, at 561～565.

[266] Id., at 324.

[267] See Maryland v. Macon, 472 U.S. 463, 1985; United States v. Jacobsen, 466 U.S. 109, 1984 (Cited by Macon, supra.). And See Carmen, at 194, Ohm, at 11.

[268] Kerr, DIGITAL WORLD, at 561～565.

[269] オリジナルの記録メディアから１ビットずつコピーする方式による「完全コピー」と定義されている(SITE J1 訳 43, 45, 46 頁参照)。And see Kerr, DIGITAL WORLD, at 541。

[270] Kerr, DIGITAL WORLD, at 561～565.

[271] Id., at 561～562.

場合は差押えに該当しないが，何時間にもわたって媒体を占有しコピー作業を行う場合には差押えに当たりうるということになる[272]。こうして，Kerr は，媒体の占有に対する侵害の程度を基準とすることにより，情報を強制処分の対象として認めた KATZ 判決の判断を維持しつつ，占有剥奪を核心要素とする差押えの従来の定義をも維持できるとするのである[273]。

このように，準用説は，従来の占有剥奪基準をそのまま強制処分の対象たる情報(データ)に適用することはできないが，情報を記録した媒体を通じて情報に準用することはでき，媒体の占有に対する侵害の程度の大きなものをデータの差押えとみなすという考え方である。

確かに，Kerr の準用説は，コンピュータ媒体を占有しながらビット連続コピー作業を行う場合には，いかなる場合に対象たる情報が差し押さえられたといえるのかを判断するために役立つものと考えられる。しかし，この説の考え方は，以下の問題点を抱えているため，適切だとは思われない。

第１に，媒体の占有に対する侵害の程度を判断する客観的な基準はなく，恣意的判断になる可能性がある。例えば，コピー作業を何時間行えば情報の差押えに該当するのかについて，Kerr は何ら回答を提供していない。

第２に，被処分者の媒体を占有する必要がない場合には，規制ができなくなってしまう[274]。例えば，警察機関が保有するコンピュータを使いインターネットを通じて被疑者のパソコンに侵入しデータをコピーする場合は，被疑者の媒体の占有に対して何らの侵害もなされないまま，大量の情報が政府に取得されてしまうが，準用説はかかる行為を規制できない。これは，媒体を占有した上でコピーを行う場合と比較して，不均衡と言わざるを得ない。

もっとも，後述するとおり，Kerr は IT 技術におけるプライバシーの基本権性を否定し，オンラインでデータを取得するというような場合に対応する必要はそもそもないとする立場であるから，この点を説得的な批判と受け取らないかもしれない。しかし，後に検討するように，本稿は Kerr と異なり， IT 技術におけるプライバシーを含めた人格権にかかる諸利益の基本権性を肯定し，オンラインとオフラインのいずれに対しても同程度の保護を与えるべきと考えるから，オンラインで行う捜査手法に対応しない Kerr の準用説を採用することはできないのである。

Ⅱ．情報の終局的処分権

以上に示した Kerr の準用説に反対する代表的論者が Ohm である。Ohm は，デリート権という概念を修正４条に取り入れれば，Kerr の準用説によらなくても，HICKS 判決に反することなく，コピーすることを差押えと解することができるとする[275]。以下では，この Ohm

---

[272] Id.

[273] Id.

[274] 劉 93 頁。

[275] Ohm, at 12.

の議論を参考にしつつ，差押えの場面における新たな保護法益と新たな法益侵害の判断基準について検討する。

１．保護法益

Ohmによれば，情報をコピーするだけで差押えにあたるかという問題の核心は，この場合にも，有体物に対する差押えにおける物理的な占有の剥奪のような消極的効果を観念することができるかという点にある[276]。

そして，Ohmは，差押えにより侵害される法益を観察する際に，物の占有による利用という側面よりは，むしろ物に対する終局的処分という側面こそが重要であると述べる[277]。その上で，終局的処分に照準を合わせると，自己のデータのコピーを政府に保有され，データの所有者がそれに対してコントロールを及ぼすことができなくなることにより，「自分のデータをデリートする権利」（終局的処分を行う権利）を失う場面と，有体物の占有が政府に剥奪され，当該有体物の所有者がそれに対してコントロールを及ぼすことができなくなることにより，「自分の所有物を破壊する権利」（終局的処分を行う権利）を失う場面との法益保護上の構造は完全に同じである以上，修正４条は両場面に同様の保護を与えるべきことになるとする[278]。

このように情報の差押えと物の差押えの共通点を終局的処分という要素に見出すべきであるとすれば，両者の終局的処分における権能はそもそも異なるから，物を破壊する権能を失わせる占有剥奪という要素を，情報をデリートする権能の場合に適用する必要はないという帰結が導かれよう。

本稿は，Ohmのこの見解を支持する。すなわち，従来は，差押えという制度により侵害される法益は，物に対する占有・使用権限にあるとされてきたが，差押えの目的は，被処分者の物に対する利用・使用・収益の権限を奪うことではなく，証拠物を保全すること，すなわち，被処分者によって当該証拠物が終局的に処分されない，言い換えれば，証拠隠滅されないようにすることにあり，裏返していえば，終局的処分を行う権限がここで侵害される法益だと理解すべきである。この意味で，物に対する利用・使用・収益の権限の剥奪は，終局的処分の権限が奪われたことに付随する事実上の不利益にすぎないことになろう。

ここでいう終局的処分の権限とは，物が処分の対象になる場合であれば，中華民国憲法15条の財産権を意味し，情報が処分の対象になる場合であれば，Ohmが提案したデリート権を意味する。そして，ここでいうデリート権については，台湾においても，憲法により保護されている基本権にあたるものであると考えられる。その論拠は次の通りである。

---

[276] Id., at 11.
[277] Id., at 12, 14, 18.
[278] Id., at 11, 12, 14.

(1)新しい人権を承認するための要件

まず，検討すべきは，ある利益が中華民国憲法上の基本権として保護すべき法益といえるために必要な条件は何なのかである。

この点につき，学説を整理すると，憲法上の基本的人権性の承認要件としては，①普遍性(すべての人間に認められるもの)[279]，②無条件性(権利をもつための条件は人間ということのみであり，特定の能力を有することは要件とされないこと)[280]，③憲法上の根拠(憲法典のいずれかの条文により根拠づけること)[281]，④実定法的権利性(権利の行使主体ないし権利行使の範囲及びその要件が特定されなければならないこと)[282]，⑤基本性・重要性(個別的独立的存在たる人間の生き方にとって基本的で重要なものでなければならないこと)[283]，⑥社会に対する中立性(基本権の存在が社会に対して有益なものであることが必要ではなく，単に，社会に対して害にならないだけでよいこと)[284]という６つのものが挙げられる[285]。それらは，さらに，以下の２つの類型に区分することができる。

すなわち，台湾の通説によると，憲法上に明文がない基本権の性質については２つのものがある。その１つは，自然権の性質を持つものであり，これは国家に先立ち普遍的に存在する固有権であるから，憲法上の規定を待つまでもなく，人間として当然に享有するものである。したがって，この場合には，上記の③の要件は不要となる。たとえば，人性尊厳，生命権，身体が傷害を受けない権利などがこれに属する[286]。もう１つは，人類社会，国家が発展するがゆえに新たに生まれてきた新しい基本権（非固有権）であり，たとえば，知る権利，環境権，情報自己決定権などがあげられる[287]。

Ohm がＩＴ技術と修正４条の適用解釈というテーマの文脈のもとで提案したいわゆるデリート権は，台湾においてもすでに権威ある中華民国司法院大法官解釈により認められてきたいわゆる情報自己決定権(情報プライバシー権，または，情報自己コントロール権とも呼ばれる)[288]と同様に，ＩＴ技術の進展に伴い生じてきた憲法により保護すべき法益であるといえる。それは，非固有権の性質を有するものに属するから，もしそれを基本権として認めようとすれば，前述の６つの要件を満たさなければならないこととなる。

Ohm の説明によれば，デリート権は，この６つの要件のうち，①②④⑥の４つの要件を満

---

279 陳愛娥・基本權 238 頁，李震山・個人資料保護 225 頁，竹中 33～34 頁，石川健治 56 頁参照。
280 陳愛娥・基本權 238 頁，竹中 33～34 頁，石川健治 56 頁参照。
281 竹中 33～34 頁，石川健治 56 頁参照。
282 同前注。
283 李震山・個人資料保護 225 頁，竹中 33～34 頁，石川健治 56 頁参照。
284 李惠宗・憲法 326 頁。
285 竹中 33～34 頁。石川健治 56 頁も参照。
286 李震山・憲法觀點 505 頁，蔡宗珍・人性尊嚴 100 頁。
287 李震山・憲法觀點 505 頁。
288 司法院大法官会議解釈 603 号は「プライバシー権は，憲法上に明文で列挙された権利ではないが，人性尊厳及び個人主体性の維持並びに人格の発展の完全性に基づき，それと同時に，個人の生活の私的領域が他人の侵害を受けないこと及び個人情報を主体的にコントロールすることを保障するために必要不可欠な基本の権利であり，それは憲法 22 条により保障されるものである」とする。

たしているのは明白である。それゆえ，ここで検討すべきは，③と⑤の２つの要件である。

A. 基本性・重要性という要件の意味とその判断基準

デリート権という法益が，基本性・重要性という要件を満たしているのかについては，Ohm の立場からすれば，それが肯定されるであろう。しかし，如何なる法益が基本かつ重要といえるかは，各々の国や社会によって異なるし，同じ国や社会においても人によって変わるものである。それゆえ，デリート権が，憲法上保護すべき基本権として認められるのかについては，再検討の余地がある。前述したアメリカの議論をも踏まえて，日独の議論状況を概観してみると，次のようになる。

まず，ドイツにおいては，権利保護の概括条項としては，その基本法 2 条 1 項があげられるが，その保護範囲の射程に関しては，核心的な人格的利益(すなわち，精神的・道徳的な人格の核心の部分)に限られるか，それとも，一般的な行為の自由もそれに含まれるかについて論争がなされてきた。

現在の通説及び裁判例の多数は，同条項を，一般的な行為の自由に対する保護の定めと見なしている[289]。その主たる理由は，一般的な行為の自由が保護されることは，基本法上の明白な文言から導かれるものであり，核心的な人格的利益のみを保護するという主張は，基本法上の文言を無視し，許されない方式をもって当該条項の保護範囲を狭くさせてしまうので認められないというものである[290]。というのも，基本法上は，「精神的・道徳的な人格」や「人格核心」という用語は見当たらず，文言上は，単に，「人格」に言及しているだけであるし，また，基本法 2 条 1 項でいう「人格」の意味は，「人」とは異なるものではないからである[291]。

この通説の考えに従えば，Ohm のいうデリート権については，それを，精神的・道徳的な人格の核心の部分に当たるものであるとは言い難いとしても，少なくとも，現代社会の日常生活ないし経済活動の形態に鑑みると，個人が生きていくためにはコンピュータなどのＩＴ技術を使わなければならないのが現状である以上，それは，基本法２条１項のいう基本権として認められるものといえよう。

これに対して，日本においては，一般人格権が判例・学説上認められてきたドイツと異なり，幸福追求権を根拠として一般人格権を認める見解は少数にとどまる[292]。その理由としては，「人格権は多岐にわたる人格的利益を包摂し，その外延は明確でないので，もしそれを総称して憲法 13 条を根拠とする一般的人格だと解すると，例えば，それから派生する憲法上の保護を受ける人格的自律権ないし自己決定権……も，広汎な行為に及んでゆく可能性があり，それは……幸福追求権の性格[その保護範囲を，『個人の人格的生存に不可欠

---

[289] Vgl. Günter Dürig S.11ff; Schmidt/Seidel,S.97ff,106ff; Dreier,S.288 . Und vgl. BverfGE 6, 32ff. そして，李雅萍・概括的権利101頁，李震山・資訊權220～222頁の説明をも参照。

[290] Vgl. Günter Dürig, S.12 ; Hans,S. 770ff.

[291] a. a. O.

[292] 芦部・人権総論 359 頁。

な利益』に限定すべきとする通説の立場を指す]に適合しないからである。」[293]という点があげられる。

この日本の通説の立場からすると，Ohm のいうデリート権を，「個人の人格的生存に不可欠な利益」にあたるものということができるのかは疑問であろう。むしろ，デリート権の基本権としての資格が否定される可能性がより高いように思われる。

それでは，台湾は，一体，どちらの立場を取るべきであろうか。その検討に先立ち，台湾の議論状況を概観してみよう。

まず，憲法分野における主流的な見解は，ほぼ前掲したドイツの通説の見解をそのまま受け入れている[294]。

しかし，これに対して，次のような批判がなされてきた。すなわち，中華民国憲法上は，基本権という用語が見当たらない以上，ドイツの議論のように，基本性・重要性を憲法により保護される権利の必要な要件とする必要はない[295]。なぜならば，如何なる基準をもって，ある権利を，基本的かつ重要的な権利であるといえるのかは明らかでないし，また，基本性・重要性のあると評される権利に対してのみ憲法上の保護を与えるのは，結局のところ，多数の利益のみを保護し，少数の利益を犠牲にする傾向を持つから[296]，少数の利益を保護すべきという憲法の役割に反するものとなるからである[297]。

以上に基づき，本稿の立場を説明すると，次のようなものとなる。まず，基本権という用語を従来の通り使い続けても構わないと思われるが，基本権を構成する１つの要素である基本性・重要性という要件を厳しく解することは必ずしも中華民国憲法の文言に合致しないし，また，そうすると，憲法が多数の利益のみを保護し，少数の利益を犠牲にする傾向があることになるとすれば，かかる要件を厳格に解釈することは少数の権利・利益を守るべき憲法の重要な機能に適合しないものである。それゆえ，当該要件については，日本の通説ないしドイツの有力説のように，それが，「個人の人格的生存に不可欠な利益」や「精神的・道徳的な人格の核心の部分」に限られるといった狭い解釈をとるべきではなく，「一般的な行為の自由」も含まれるものであると，より広く理解するほうが妥当であると考える。

基本的・重要的な権利とそうでない権利とを区別するための基準が不明確であるという問題については，ある権利ないし利益に対して，憲法上の保護を与える必要性はないことが明らかである場合にのみ，かかる権利ないし利益は，基本性・重要性をもたないという基準を立てることにより，適用が容易になろう。

これに対しては，その基準によると，基本権として認められる権利ないし利益の範囲が

---

[293] 芦部・人権総論 360 頁。これに対して，反対説がある(阪本・自己決定の自由 223～224，244～246 頁，根森・人間の尊厳 372～373 頁参照)。

[294] 呉庚・憲法３版 128～130 頁，李震山・資訊自決權 236～237 頁，陳慈陽・憲法２版 504～506 頁，法＝董・憲法３版 167，177～178 頁，李惠宗・憲法５版 365 頁等参照。

[295] 李雅萍・概括的権利 115～116 頁。また林紀東・憲法(一)８版 333～338 頁をも参照。

[296] というのも，少数にのみ関係する利益は，常には基本や重要と思われない傾向があるからである。

[297] 李雅萍・概括的権利 115～116 頁。また，類似する指摘として，廖・平等公民權 375～385 頁をも参照。

無制限に広がるおそれがあるとの批判がなされるかもしれない。しかし，前述したとおり，基本権を承認するためには，その他の要件を必要とされているため，かような懸念は妥当しないと思われる。とりわけ，実定法的権利性という要件は重要である。実定法化できる程度の具体的な権利や利益ではないと，基本権として認める余地がないからである。

さらに，基本権であっても，無制約の絶対の権利ではないから，基本権としての資格の有無という前段階について認定の基準を厳しくしなくても大きな問題は生じないといえる。これに対しては，前段階の基本権としての資格の認定の範囲を広くしても，その後，認定された基本権に対する制約を厳しくするのであれば，基本権性を認めることの意味が失われてしまうではないかという疑問があるかもしれない。しかし，ある権利ないし利益が基本権として認められた場合には，立法による制約に対して，憲法訴訟を提起するかたちで権利の救済を受けることが可能であるから，基本権としての資格の認定自体にも意味があるのである。

B. 中華民国憲法 22 条を適用するための要件

残る③の要件についても，一般規定としての中華民国憲法 22 条がその根拠として考えられる。

中華民国憲法 22 条は，「人民のその他の自由及び権利については，社会の秩序ないし公共の利益を妨害しないものであるかぎり，そのすべてが憲法の保障を受ける」と定めている。通説によると，この規定は，憲法がすべての自由・権利を保障し，この要件を満たす自由・権利であるならば，それは憲法の保障を受けるものであり，法律によってそれを侵害してはならないと解されている[298]。これは，学説上，「憲法直接保障主義」と称されている[299]。

そして，「憲法直接保障主義」を適用するための要件としては，①憲法上列挙された権利保障のリストにおいて保護間隙が存在すること，②かかる保護間隙を埋める必要があること，③22 条以外には保護間隙を補填する可能な憲法上の条項が見つからないこと，という３つのものが考えられる[300]。この３つの要件に照らして，デリート権の憲法上の保障について検討すると，次のようになろう。

まず，①については，中華民国憲法上においては，有体物に対する終局的処分権(つまり，権利主体が権利対象物を処分・破壊する権利)については，住居不可侵を保障する同法 10 条と並んで，財産権を保護する同法 15 条があげられる。これに対して，無体の情報に対する終局的処分権(つまり，デリート権)に関しては，憲法上の明文が欠けている。言い換えれば，デリート権に関する保護間隙が存在している。

それから，②については，コンピュータ・インターネットなどのＩＴ技術と並んでさまざ

[298] 李惠宗・憲法 325～326 頁。

[299] 同前注。

[300] Vgl. Müller, s.123.そして李雅萍・概括的權利 31 頁，李震山・個人資料保護 225～226 頁の説明をも参照。

まな科学技術の設備(たとえば，写真撮影や録画の器機など)が普及している現代社会においては，無体の情報が有体物である媒体の価値を超えた無体財産権上の価値をもつ場合があることに鑑みると，無体の情報に対する終局的処分権という保護間隙を補填する必要性が高いといえよう。というのも，かかる間隙を埋めないと，社会の実情に合わないと同時に，無体物である情報の価値より低い有体物である媒体の場合にのみ憲法上の保護を与えるというアンバランスが生じているため，中華民国憲法 23 条のいう比例原則に適合しないと思われるからである。

最後に，③の要件については，前に論じたアメリカ憲法修正 4 条を根拠とした Ohm の理論の内実を，中華民国憲法の既存の条項にあてはめた上で再検討する必要がある。

まず，Ohm のいうデリート権の具体的な内実は，２つの点からなる。その１つは，この権利は，修正４条の保護法益であるプライバシー権から派生した情報プライバシーをその根拠とするものであること，もう１つは，無形の情報にも，有体物の財産と同様に，それを終局的に処分する権限が考えられるので，それにも同様程度の修正４条の保護を与えるべきであることである。後者の点については，前述したので，ここでは，前者の点について述べることにする。

まず,Ohm によれば,デリート権は,これまでは確認されていない修正４条の法益であり,自分のデータを支配・コントロールする権利であるとされる[301]。そして,デリート権がいわゆる情報プライバシー権から派生するものであることを説明するため,Ohm は,いわゆるプレイン・ヴュー法理の適用を中心に,以下の３つの例を挙げている[302]。まず，①警察官が捜索の現場の状況を写真撮影する場合や，②GPS 設備をもって公道上の車両を追跡する場合には，デリート権は発生しない。なぜならば，これらの例はいずれも，プレイン・ヴューの状況にあたるものであり，情報プライバシー権が存在しないものだからである。これに対して，③前述した HICKS 事件の事例は，警察官がステレオを移動しないと，そのシリアル番号を見ることができず，その意味で，この事例はプレイン・ヴューの状況に該当しないから，デリート権が発生するとされる[303]。

以上により，Ohm のいうデリート権については，①憲法上の根拠となる条項は，住居不可侵の保護並びに不合理な捜索・差押えの禁止を定める修正４条であること，②保護法益は，修正４条における情報プライバシー権であること，③プレイン・ヴューの場合，言葉を換えていえば,すでに公開された情報を対象とする場合には,デリート権が存在しないこと，④有体物の財産権と同様に終局的に処分する権限があること，という４つの要素が重要である。

これに対して，中華民国憲法においては，アメリカのいう不合理な捜索・差押えの禁止，つまり令状主義を定める条項は存在しない。上記の４要素を中華民国憲法の規定に照らし

[301] Ohm, at14.

[302] Id., at16.

[303] 但し，後述するとおり，Ohm の結論としては，手書きだけでは，デリート権の侵害にはならないと述べている。

て考えると，類似する根拠としては，住居不可侵を定める同法 10 条，プライバシー権の一般的な根拠とされた同法 22 条[304]，及び財産権を定める同法 15 条，という３つのものが考えられる。

しかし，単純に住居不可侵という実体的な法益を保護する中華民国憲法 10 条であれ，単純に財産権という実体的な法益を保護する同法 15 条であれ，それらはいずれも，適切ではないのは明らかであろう。というのも，10 条や 15 条などの実体的な法益を保護する条項からは令状主義という手続的な権利を導き出すことは無理であると言わなければならないからである。

他方で，Ohm は，権利保護の概括条項からではなく，権利保護の個別条項である修正４条における既存の情報プライバシー権から新しくデリート権を導き出している。アメリカでは，中華民国憲法 22 条のような権利保護の概括条項が存在しない。すなわち，アメリカでいうプライバシー権は，「もっとも包括的な権利」[305]としての「一般的権利」[306]と理解されてきたが，それは憲法上の特定の規定を根拠とするものではなく，様々な条項の解釈によって導かれた権利の総称である[307]。ここで言及した，修正４条の保護法益としての情報プライバシー権も，Ohm のいうデリート権も，包括的な権利としてのプライバシー権の１つの類型に過ぎない。

ところで，我が国においても，権威ある大法官解釈は，憲法 22 条を根拠に，アメリカのいう一般的権利であるプライバシーを認めた上で，情報プライバシー権もその一環として憲法 22 条により保護される法益であるとしている[308]。この点からすると，Ohm の立場に従えば，プライバシー権の一環としてのデリート権という法益に憲法上の保護を与えようとすれば，我が国憲法 22 条にその根拠を求めるべきであるという帰結になろう。

しかし，本稿は，個人は，自分の無体の情報に対しても，自分の有体物の財産と同様に，終局的に処分する権限をもつという点においては Ohm の見解を支持するが，彼が，かかる権利の法益性の根拠を，既存のプライバシー権ないし情報プライバシー権(すなわち，ドイツのいういわゆる情報自己決定権)に求める部分に対しては，反対である。というのも，デリート権は，情報に対する終局的処分権をその核心の要素とするものである以上，理論的には，(情報がすでに知られたかどうかという意味での)プライバシー権と完全に両立する

---

304 司法院大法官会議解釈 603 号参照。

305 アメリカでいうプライバシー権は最初「the right to be let alone」と定義され，一般に，「ひとりにしておかれる権利」や「一人でほっておいてもらう権利」と翻訳されてきた。これは， 1890 年のウォーレン＝ブランダイスの論文［Warren／Brandeis, at 1 ff.］により提唱されたものである。この「the right to be let alone」は，「最も包括的な権利」とも呼ばれてきた(See OLMSTEAD ET AL. v. UNITED STATES, 277 U.S. 438(1928), at 478～479［MR. JUSTICE BRANDEIS, dissenting］。伊藤・プライバシーの権利 33～35，61，70 頁及び久保田 145，148 頁をも参照されたい)。また，プライバシー権を包括的な権利と称する日本の論者として，和田 131～132 頁，橋本・憲法(改訂版)425 頁，同・プライヴァシー32～35 頁などがあげられる。

306 Warren／Brandeis, at 7, 15； 和田131～132頁；橋本・憲法(改訂版)425頁，同・プライヴァシー32～35頁以下をも参照。

307 Lide, at 481；and see Stone, at 4.

308 司法院大法官会議解釈 603 号参照。

ことができるし，また，その必要性もあると思われるからである。例えば，自分の情報が警察官に見られたからといって，かかる情報を見た警察官が当然に当該情報を保持(コピー・記録・取得)することができるわけではないし，また逆に，警察官がある情報を見なくてもそれを保持することもできる。それゆえ，デリート権とプライバシー権との両者の法益における異なる性質を無視しそれらを１つのプライバシーの概念のもとで包摂させるOhmの見解は，理論的に一貫していないという批判を免れないと思われる。というのも，Ohmの理論が，自分のデータのコピーが政府により保持されると，個人はかかるコピーを削除することができなくなり，それによって，自分の情報に対する終局的な処分の権限を政府により剥奪されるというものであるとすれば，プレイン・ヴューの場合であってもその法益侵害の状況は同様であるからである。つまり，データがすでに政府に見られたが，データのコピーが取られていない段階であれば，デリート権は生じないという結論になるのに対して，コピーまで取られた場合には，前述の Ohm の説明からすると，デリート権が発生すると解すべきと思われるからである。

他方で，プライバシー権をデリート権の法益性の根拠とする Ohm の立場は，情報に対する捜索・差押えという制度の構築にも不適切であると思われる。というのも，ここまでの検討でも示されたように，情報を対象とする捜索・差押えの場合は，従来の有体物を対象とする場合とは異なり，「捜索→(関連性による)差押え」という順序でなく，「(蓋然性による)差押え→捜索(鑑定・鑑識)」という順序となる。それにもかかわらず，捜索を差押えの前段階とする従来の理解を，そのまま，「差押え→捜索」の順序に適用させると，この順序で前段階となる差押えでは関連性を確認していないし，また後段階となる捜索は形式的に鑑定や鑑識となるため規制がないこととなるから，結局のところ，捜査に対するコントロールを失ってしまうこととなる。そこで，物に対する捜索・差押えという制度と並んで，情報に対する捜索・差押えという制度を構築するには，「捜索→差押え」という順序に捉われることなく，「捜索」「差押え」という２つの制度の独立性を確立したうえで，両者の執行の順序は，有体物や無体物を対象とするそれぞれ異なる場面に応じて組み合わせることができるという形にすべきである。

以上のとおり，情報に対する終局的処分権は，これまで認められている保護法益(プライバシー権ないし情報プライバシー権など)とは，全く異なる新たな人権であるから，中華民国憲法22条という権利保護の概括条項からしか導くことができないということができよう。

(2)「終局的処分権」という提案の実益

以上のとおり，情報に対する終局的処分権は，中華民国憲法上の基本的人権性の承認要件を充足するものであり，その根拠は，同法22条に求められる。

そのうえで，差押えという制度について，「終局的処分権」(物の破壊あるいは情報のデリートを行う権限)という点に着目することの実益は，次の点に求められる。

第１に，終局的処分権に着目すれば，情報を物と同程度に保護すべきという立場を正当

化することができる。というのも，物を強制処分の対象とする場面でも，情報を強制処分の対象とする場面でも，終局的処分を行う権利が政府に剥奪されるという構造は同じである以上，憲法は両場面に同様の保護を与えるべきだからである。

第２に，終局的処分権に着目すると，意義ある干渉という従来の差押えの定義をそのまま維持した上で，物と情報の両者を同じ定義の下に包摂させることも可能になる。すなわち，ここでいう意義ある干渉を，「終局的処分権を剥奪すること」と理解すれば，物を対象とする場合も，情報を対象とする場合も，終局的処分権を奪った場合に意義ある干渉が認められ，それぞれの場合に応じて物ないし情報の差押えと評価されるのである。

２．法益侵害の判断基準

もっとも，物と情報は，それに対する権利行使の態様が異なるので，終局的処分権を奪われたかどうかを判断する基準，すなわち，差押えの該当性を判断する基準は，有体物が処分の対象となる場合と情報が処分の対象となる場合とは異なるものであると思われる。Ohmもこの点を指摘しているが[309]，終局的処分権を奪われたかどうかを判断する基準，言い換えれば，情報をデリートする権能を失わせる要素が何なのかについては明らかにしていない。そこで，以下では，この点についての更なる検討を行いたい。

(1)物の場合

物の財産権を行使するには，占有が不可欠である。物を利用・使用・収益する場合にはもちろんのこと，終局的に処分するためにも，当該物を直接や間接的に占有しなければならない。この点からは，物を終局的に処分する権利を奪われたかどうか，言い換えれば物の差押えにあたるかどうかを判断するには占有剥奪を基準とするのが適切であると考えられる。

そして，物の所有権ないし合法的な占有権限とは抽象的な観念に過ぎず，外見からその存否を判断するのが法執行機関にとっては困難ないし不可能であるという点からも，事実状態としての占有が剥奪されたという物理的な現象を差押えの該当性を判断する基準としている現行の有体物に対する差押えという制度には，合理性が認められよう。

(2)情報の場合

これに対して，情報を利用する場合には，物理的な占有を観念する余地がないから，占有剥奪を情報の差押えの該当性を判断する基準とすることは適切ではない。

そして，前述した通り，情報を処分の対象とする場合の差押えという制度は，占有した物を終局的に破壊する権利の行使を抑制するのではなく，デリート権の行使を防ぐことがその目的である。言い換えれば，ここで情報の差押えという制度により侵害される法益は，

---

[309] Ohm, at 10ff は，占有の権限に特徴付けられている物を差押えの対象とする場合，「占有剥奪」という要素をそのまま維持すべきであるが，それは，占有を特徴としない情報にふさわしくないとする。

物に対する占有，利用ないし処分の権利ではなく，情報を終局的に消滅する権利(デリート権)である。すなわち，捜査機関に自己の情報のコピーを取得された場合，被処分者は当該情報を利用し続けることはできるが，捜査機関がデータの複製を所持していることにより，世の中から当該データを完全に消去(デリート)することはできなくなり，この意味で，被処分者は自己のデータに対する終局的処分権を政府に奪われた，すなわち，情報(データ)が差し押さえられたといえる。

そうすると，次の問題は，いかなる場合に，デリート権，すなわち情報の終局的処分権が剥奪されたとして，情報の差押えに該当するといえるかである。以下，この問題を検討する。

A. 科学技術の使用との関係

デリート権が剥奪されたといえるための条件は何なのかについて，Ohm は具体的な回答を示しておらず，単に，デリート権の剥奪を認めるには科学技術の使用を必要とすると述べているだけである[310]。そのうえで，手書きをするだけでは差押えに当たらないとした HICKS の結論は正しいとしている[311]。

ここからは，科学技術を用いた機械的記録の場合には，デリート権の侵害が認められ情報の差押えに該当するのに対し，科学技術を使わない非機械的記録の場合には，デリート権の侵害が認められないから情報の差押えには該当しない，という判断基準が考えられるかもしれない。

しかし，いかなる科学技術を用いた機械的記録の場合にデリート権が侵害されたといえるのかは必ずしも明らかではない。というのも，前述した通り，Kerr の見解によると，一般のデジタルコピー技術だけでは差押えにはならず，ビット連続コピーの場合のみが情報の差押えに当たりうるとされるのに対して，Ohm は，ビット連続コピーというようなハイテク技術の使用に限る必要はなく，普通のローテク技術によるコピーでも情報の差押えに該当しうるとしているからである[312]。

ここからは，Ohm は，ハイテク技術の使用に着目しているのではなく，コピーされた情報と原始の情報との同一性を担保するために科学技術の使用が必要になると考えているように思われる。仮にそうだとすると，デリート権の侵害の有無を判断する究極の基準は，コピーされた情報と原始の情報に同一性が担保されているかという点にあることになるが，かかる担保のために科学技術の使用が不可欠というわけではない。例えば，次のような事例が想定されよう。

麻薬密売組織のボスＹが，密売取引先と電話しながら連絡先ないし取引条件を紙にメモした上で，担当の子分Ｘに当該メモを渡すと同時に取引の用意ができたらすぐ当該メモを

[310] Ohm, at 16.

[311] Id.

[312] 劉 94 頁の説明をも参照されたい。

処分するよう指示していることを知った覆面捜査官Ａは，Ｙがメモした密売取引関連情報を手に入れるために，Ｙがメモする際にいつも使っているテーブルのテーブルクロスの下に，複写紙ともう一枚の紙を重ねてこっそり入れておき，Ｙがメモする度に，当該複写紙と紙を回収したうえで，また新しいものと取り替えるということを行った。

この事例で，複写紙の使用を科学技術の使用とすることは困難であるから，上記の捜査手法においては科学技術が用いられていないという帰結になろう。しかし，複写紙によりコピーされた情報は，明らかにＹがメモした原始の情報との間に同一性を有するものである。その意味で，デリート権の侵害を判断する究極の基準である，コピーされた情報と原始の情報との同一性は満たしているといわなければならない。そうだとすれば，複写紙の使用だけであっても，それは情報の差押えにあたりうることになる。

このように，科学技術を使わない限り，情報の差押えには該当しないという主張は説得力がない。ビット連続コピー，普通のデジタルコピーや複写紙ないし手書きなどの違いは程度の差にすぎず，これらを質的に区別することはできないからである。

B. 情報の終局的処分権の剥奪

そこで，次に，情報の終局的処分権の侵害を判断する基準，すなわちコピーされた情報と原始の情報に同一性が担保されているかという基準の内容をより具体的に検討し，情報の差押えの該当性判断基準を明らかにしたい。

(A)原始情報の性質

まず，原始情報は「自己の情報」でなければならないが，情報の終局的処分権（デリート権）はプライバシー権ではないから，保護される「自己の情報」はプライバシーに関するものに限定されない。

この点，物を対象とする場合との比較によりも基礎付けられよう。物を差押えの対象とする場合，たとえ利用価値が全くない物(例えば，ごみ)であっても，占有がなお残っている限り，所有者はそれを完全に破壊し，棄ててしまうという終局的処分権を依然として有している[313]。この意味で，所有者は，当該ごみに対して所有権を主張することができる。この理解は民法の理解とも一致している。というのも，民法でいう物に対する所有権は，経済的な価値の有無とは関係なく，物に対する帰属関係及び支配・利用・収益・処分関係により定義されるものだからである。それゆえ，たとえごみであっても，それに対する終局的処分権が所有者に残っているから，ごみという物に対する占有が政府に剥奪されたときに，物に対する差押えの保護法益である財産権が侵害されたといえ，物に対する差押えに該当することになる。

かかる理解は，物と情報を同程度に保護すべきとする前提からすれば，情報の差押えの法益であるデリート権にも同様に妥当するものということができよう。すなわち，たとえ

[313] 川出・物の占有9頁。古田(監修)126～127頁をも参照。

個人のプライバシーと全く関係ない情報――例えば，著作権侵害事件の捜査を行う目的に基づき政府により撮影された，ある大学院生の未公刊の論文の原稿の内容(写真の画像)――であっても[314]，当該大学院生は当該原稿を完全に破壊し棄ててしまうという終局的処分権を依然として有しているから，前述した情報の差押えの保護法益であるデリート権を政府に奪われない権利を主張することができると解すべきである。言い換えれば，デリート権は，プライバシーに関わる情報であるかどうかを問わず，自己の情報である限り，あらゆる情報に対して認められるものである。

(B)自己の情報の範囲

次に，検討すべきは，いかなる情報が自己の情報といえるかであるが，この点は，強制処分の対象としての情報の定義に関わる問題であり，後述する第５節の「情報の差押え」という制度の前提問題になるから，この点についての詳細は，そこでの検討に譲ることにしたい。

(C)原始情報との同一性に対する合理的信頼価値

最後に検討すべきは，いかなる場合にかかる情報の終局的処分権が政府によって剥奪されたといえるかという問題である。

Ohm の理論によれば，原始情報(自己の情報)のコピーを政府に保有され，被処分者が政府の占有するコピーにコントロールを及ぼすことができなくなることにより，自己の情報に対する終局的処分権を失うことになる。そして，このように被処分者が終局的処分権を失ったといえるためには，政府によってコピーされた情報と自己の情報との間の同一性が担保されている必要がある。

例えば，捜査官による記憶や個人的なメモは不確実で，原始の情報との同一性が担保されておらず，その信頼性にも問題があるため，被告人は「かかる記憶ないし記録は，自分とは関係がない」と否認すればよいから，かかる不確実な記憶・記録は，ここでいう「自己の情報」にあたらない[315]。それゆえ，それを政府に保有されたとしても，情報の終局処分権の剥奪には該当しないと考えられる。これに対して，その形式において原始情報との同一性について信頼性を有する記録（例えば，ビット連続コピー，デジタルコピー，複写紙記録）であるならば，たとえ被告人がどのように否認したとしても，それが受け入れられ

---

[314] 英米においては，台湾において一般に理解されてきた意味での「私事」とは全く関係のない知的所産としてのプライバシーを認めた例がある。例えば，イギリスにおいては，医師である講師の了承を得ていないにもかかわらず，ある学生が勝手にかかる講師の外科医講義の内容をメモした自分の筆記を雑誌に載せて公表した事案で，かかる公表行為が講師のプライバシーを侵害したものと判断された Abernethy v. Hutchinson(1825)3 L. J. Ch.209 が存在する。また，アメリカにおいても，仕事や学問上の研究成果などやその他の知的所産を，いわゆる「個人の知識・思想に関するプライバシー」ないし「知的所産プライバシー」(intellectual privacy)として捉える見解がある(See Katyal, The New Surveillance, at 253ff, 353ff; Katyal, Privacy vs. Piracy, at 222ff)。しかし，台湾においては，私事と関係がない知的所産をプライバシーと捉える議論は見当たらない。

[315] 劉 95 頁参照。

る可能性は低い。したがって，このような記録は「自己の情報」のコピーに該当し，政府によるその記録の保有は情報の終局処分権の剥奪に該当することになる[316]。

ここでの議論で示唆されている通り，コピーされた情報が原始情報と同一のものとして扱われるかは一般人の合理的な判断にかかっているから，コピーされた情報と原始情報との同一性の有無を判断する基準は，合理的一般人が当該情報の記録(コピー)と原始情報の間に同一性があると考えるかどうかに求めるべきと思われる。裏返していえば，合理的一般人が原始情報と同一性を有すると考える情報のコピーには，原始情報との同一性について「合理的信頼価値」が認められるといえよう。

このように，コピーされた情報と原始情報の同一性を一般人の合理的判断に基づいて決定する。すなわち，コピーされた情報が原始情報との同一性について合理的信頼価値を有する場合に情報の終局的処分権の剥奪を認めるという立場に立つと，政府による情報取得の態様，言い換えれば，情報を記録する方式(例えば，手書きのメモか，それとも機械によるコピーか)は，情報の差押え該当性判断において決定的な意味を持たなくなる。つまり，仮に，情報を記録する方式は手書きであっても，当該記録に社会的・一般的に信頼されている私的ないし公的な機関による認証が付されているならば，合理的な一般人は，当該手書きの記録と原始情報との間に同一性があると考えるであろうから，原始情報との同一性について合理的信頼価値があると評価できる。

反対に，情報を記録する方式が機械的記録である写真撮影であっても，撮影された記録と原始情報との間に同一性がないと判断される場合もありうる。例えば，監視カメラに映った容疑者の映像は，赤いＴシャツを着た茶髪の男性であるが，撮影当時は天候が悪く，周辺で祭りも開催されていたことが判明した場合，監視カメラに映ったＴシャツ及び髪の色と被疑者が実際に着ていた服及び髪の色との間にズレがある可能性が高い。かかる場合に，合理的な一般人は，監視カメラ画像(原始情報のコピー)と被疑者の容貌（原始情報)との間に同一性があるとは考えないであろうから，写真撮影であっても原始情報との同一性について合理的信頼価値が認められず，情報の差押えに該当しないという帰結になる。

第５節　「情報の差押え」という制度について

第１款　押収の新定義

差押えは，提出命令，領置と並ぶ押収の一類型であるから，差押えの定義との関係で，押収，提出命令ないし領置についての定義もあわせて言及する。

さて，本章第４節で示した「情報の終局的処分権」という法益論によれば，押収とは，「証拠になりうる物若しくは没収すべき物又は証拠になりうる情報若しくは没収すべき情報を確保するために，物の占有又は情報の終局的処分権を取得し，又は占有の剥奪若しく

[316] 同前注。

は情報の終局的処分権の剥奪を継続する処分」と定義される。

この押収の新しい定義をもとに，現行刑訴法のもとで定められた，差押え(台湾刑訴法133条1項)[317]，提出命令(同133条2項)[318]，領置(同143条)[319]の３つの類型の押収を再定義すると，次のようになる。

Ⅰ．差押えについて

差押えは，「証拠になりうる物若しくは没収すべき物，又は証拠になりうる情報若しくは没収すべき情報を確保するために，直接的な強制力により，物の占有又は情報の終局的処分権を取得したうえで，占有の剥奪又は情報の終局的処分権の剥奪を継続する処分である」と定義される。

この新しい定義をもとに，以下では，情報の一時的な取得は差押えにあたるかという問題点を取り上げたい。

台湾においても，従来は，現場で物を利用するために，一時的に物の占有を剥奪したとしても，その場合の占有の剥奪は，捜査の終局的な目的ではなく，あくまで現場での物の利用という目的を遂行するための手段として行われただけであるから，差押えには当たらないと解されてきた[320]。ここで問題となるのは，一時的な占有剥奪であるといっても，占有剥奪に当たるものである点に変わりはないのに，なぜそれを差押えとしないことができるのかである。この点は，電磁的記録を対象とする場合に特有な問題ではないし，また，台湾の先行研究においてはそれを特に問題として指摘する見解も見当たらないから，以下は，日本の関連議論を素材にここでの検討を進める形にしたい。

日本においては，捜査機関が，現場で，被処分者のコンピュータ及びプリンターを利用し目標となるデータをアウトプットするというような場合，対象者はその所有物の占有を一時的に捜査機関に奪われてはいるが，現場でアウトプットのために利用されただけであるから，それは差押えではなく，差押えないし検証に必要な処分と解されてきた[321]。

さらに，学説においては，差押えの対象となる物件を選別するために，差押対象物である蓋然性を有するすべての物件を現場から持ち去ったとしても，それがあくまで一時的な措置であって，選別が終わったら，即時に当該物を被処分者に返還するならば，差押えと解する必要がなく，捜索に必要な処分と解することができるとする主張もなされている[322]。

---

317 「証拠となるあるいは没収できる物は，それを差し押さえることができる。」

318 「差し押さえるべき物の所有者・所持者若しくは保管者に対して，それを提出あるいは交付するよう命じることができる。」

319 「被告人，犯罪嫌疑者若しくは第三者が犯罪の現場で遺留した物，または所有者若しくは保管者が任意に提出あるいは交付する物を領置することができる。こうした場合は，前四条の規定[差押えが行われた後の処置並びに差し押さえられた物の還付に関わる規定]を準用するものとする。」

320 朱・刑訴(修二)134 頁。

321 新保 149 頁，小川 264～265 頁。

322 酒巻匡・捜索・押収 447～453 頁，長沼範良・電磁的情報 47～48 頁。平野・刑訴全集 112 頁も参照。

他方,直接に差押えの問題を扱った事例ではないが,いわゆるNシステム[323]の問題につき,走行車両の搭乗者の容ぼう等を撮影したとしても,その撮影した画像を長時間記録,保存する予定がない場合には,肖像権に対する侵害が生じないとしたものがある[324]。写真撮影は情報の差押えという性格を持つものであるから[325],仮に,撮影画像の保存が短時間の場合においては肖像権への侵害とはいえないという理解[326]が,一時的な情報の取得は実質的な情報の差押えとはいえないということを意味するのだとすれば,それは,一時的な占有の剥奪は(物に対する)差押えに当たらないという前述の理解と同一の考え方に基づくものと位置づけることができよう。

これに対して,本稿の理解によれば,占有が剥奪された時点で,物は差し押さえられたといい,情報の終局的処分権が剥奪された時点で,情報が差し押さえられたといえる。それゆえ,一時的な占有の剥奪だけであっても,物の差押えに該当するし,一時的な保存により情報の終局的処分権が一時的に剥奪されただけであっても,情報の差押えにあたることになる。

もっとも,本章第４節で検討した通り,物と情報とは異なる性質をもつものであるから,物の占有剥奪を内容とする法の原理・原則をそのまま情報を取得する場面に適用することは不適切である。何が差押えに該当するかというここでの問題に即していえば,情報の「一時的な取得(複製・記録)」は差押えに当たるが,「一瞬の取得」は差押えに当たらないと考えられる。なぜならば,情報が取得された時点と,取得された情報が削除された時点がほぼ同時となる一瞬の取得の場合には,情報の終局的処分権の剥奪に該当しないと解すべきだからである。

すなわち,情報の終局的処分権の侵害の構造は,個人が自己情報の記録(コピー)を政府に取られると,当該取得された情報の記録をデリートすることができないため,自己情報を終局的に処分する権利が侵害されるというものである。しかし,一瞬の取得の場合においては,被処分者が当該取得された情報の記録に対してデリート権を主張する実益は全くない。なぜならば,情報の取得とその削除とがほとんど同時に発生する一瞬の取得の場合においては,情報を政府に取得された時点で生じる被処分者のデリート権は,発生する時点と同時に消滅することになるからである。

---

[323] Ｎシステムという名称は,ドイツで先駆けて用いられた「自動車ナンバー自動読取システム」の Number の頭文字であるＮをとって作られた略称である 。日本においてこのシステムが開発された経緯ないし運用の実態につき,實原 156 頁,水町 115 頁三浦 49 頁,警察白書昭和 60 年版,平成 10 年版,平成 11 年版,平成 12 年版参照。

[324] 東京高判 17 年 1 月 19 日判例時報 1898 号 157 頁。東京地判平成 13 年 2 月 6 日判例時報 1784 号 114 頁をも参照。

[325] 写真撮影を伴う検証について,それが継続的な侵害性を有するものである点に着目し,一定の場合には,それを実質的な情報の差押えであると見る見解が有力となりつつある(井上・強制・任意 348 頁以下収録 370 頁,酒巻・捜索・押収 455 頁注 18,最二決平成 2 年 6 月 27 日刑集 44 巻 4 号 385 頁〈藤島昭裁判官の補足意見〉,名古屋地決昭和 54 年 3 月 30 日警備実務判例集第 1 巻 443 頁参照)。

[326] 前掲注324参照。同注に挙げた東京高裁平成17年判決は,「Nシステム……によって撮影された画像には,一時的に走行車両の搭乗者の容ぼう・姿態が写っている可能性があるが,この画像は瞬時にコンピュータ処理によって車両ナンバープレートの文字データとして抽出されることになり,搭乗者の容ぼう・姿態が写っている可能性のある画像そのものが記録,保存されることはない」としている。

これに対しては，そうであるならば，物を差押えの対象とする場合においても，同様に解すべきではないかという疑問があるかもしれない。しかし，物に対する差押えの場合においては，「一瞬の占有剥奪」ということは，観念上はありうるが，現実的には存在しないであろう。というのも，捜査機関が，情報を取得したと同時にそれをデリートすることができるのは，情報をスキャン(一瞬的な保存)したり照合したり削除したりするという一連の作業が，高度計算能力を持つコンピュータの自動作業によれば，一瞬で完成させられるのに対して，被処分者からある物を取得(占有剥奪)した場合には，その中身の確認が人間の能力[327]により実行されるものであるかぎり，それを一瞬で完成させるのは不可能であって，物を取得すると同時にそれをを還付するということはできないからである。

Ⅱ．提出命令について

提出命令は，間接強制処分[328]の一種であり，それを，「物の所有者，占有者ないし情報の終局的処分権の所有者，情報の管理権者等に対して，処分の対象となる物ないし情報の提出義務を生じさせ，その義務を履行しない場合は法的な制裁を課す処分である」と定義することができよう。

しかし，現行法の提出命令は，ここでいう間接強制処分としての提出命令ではない。現行法の提出命令に応じないときには，「差押えが予定されている」という意味で「間接的な強制」が存在するとされているが[329]，ここでいう“間接的な強制力”とは，命令に応じない場合に法的な制裁を課すという意味での強制とは異なるものだからである[330]。

このように，現行法においては法的な制裁を課すという意味での間接強制処分が認められていないが，被処分者に協力してもらうニーズがないわけではない。この点は，とりわけ，電磁的記録媒体への捜索・差押えの文脈において顕在化してきている。具体的には，捜査機関が，被処分者ないし事件に精通していると思われる者に電磁的記録のアウトプットないしそれへの協力をしてもらうことができるのかが問題となる[331]。この問題点に対しては，日本においてなされてきた以下のような解釈論と立法論が台湾にも参考となると思われるので，その中身を紹介しておきたい。

１．解釈論の提案とその問題点

まず，河上検事は，「内容がわからぬ以上，すべての磁気テープ類をとりあえず差し押さえざるをえないということになるし，この場合，被差押人側としても，それを避けるために必要な処

---

[327] エックス線検査機や麻薬犬などのツールを用いて人間の能力を増強する場面をも含む。

[328] 間接強制処分の定義につき，前掲注 26 参照。

[329] 柯慶賢・修正捜索扣押(上)3 頁参照。また，台湾刑訴法 138 条は「差し押さえるべき物の所有者，所持者あるいは保管者が正当な理由もなく提出若しくは交付することを断ったりまたは差押えを抵抗したりする場合は，強制力を持ってそれを差し押さえることができる。」と定めている。また，藤永ほか編・大コンメンタール(二)[藤永]230 頁，[渡辺]254 頁；平場ほか・注解(上)[高田]331 頁，田宮・注釈刑訴 123 頁，岸・要義 143 頁をも参照。

[330] 酒巻・提出命令 129 頁。

[331] 新保 152 頁以下参照。

分のアウトプットに協力させざるを得ないということで事実上解決されるのではないか」と述べている[332]。

かかる見解によれば，被処分者が捜査に協力する場合においては，関連性のある物件のみを提出すればよいのに対して，協力しない場合には，関連性のあるものとそうでないものを含めて，そのすべてを，とりあえず差し押さえられてしまうということになるから，協力しない場合には，協力した場合に生じる，関連性のある物に対する占有の喪失という不利益の他に，関連性のない物に対する占有までも失ってしまうという不利益が加えられることになる。この意味で，関連性のない物に対する占有の喪失の部分は，事実上，捜査に協力しないことの処罰とも評価できるものである。

しかしながら，そのような不利益を課すことは，現行法が予定した直接強制処分[333]の侵害強度をこえてしまうのではないかと思われる。というのも，直接強制処分である差押えによっても，基本的には，関連性のないものを差し押さえてはならないからである。

実際にも，この見解は，学説の多数では支持されていないし[334]，それを「法律議論とはいえない暴論」とする厳しい意見が実務家の間からもなされている[335]。また，河上検事の見解に近いようにみえる実務家も，かなり謙抑的な姿勢を示している。例えば，原田判事は「差押え自体が適法である場合，差押えをひかえて，それを背景に相手方にアウトプットを協力するように働きかけることは，不当な強制にわたらない限り許される」[336]とされる。

その結果として，協力義務という問題に対する抜本的な解決は，新たな立法に委ねるのが本筋であるという考え方が，学説ないし実務家の多数を占めている[337]。そこで，次に検討すべきは，立法的解決の具体的な中身は何なのかである。

２．立法提案とその問題点

電磁的記録のアウトプットという場面に止まらず，暗号化などのＩＴセキュリティ技術の急速な進展・普及に伴い，データを保管している対象者の協力がなければ，目標たるデータを検索・検閲ないし保全・取得することが困難となっているという現状がある。かような現状を踏まえて，学説では，もっとも妥当な方策として，新しい立法により，間接強制力付きの協力義務に関する規定――具体的には，間接強制処分としての提出命令という制度が挙げられている――を設けるべきであるとの提案がなされている[338]。

しかしながら，実際には，間接強制処分だけでは，被処分者に協力してもらえないという問題を抜本的に解決することはできない。すなわち，従来の議論では，まず，①対象者が協力しないとＩＴセキュリティの解除が不可能であることを前提に，直接的強制処分であ

---

[332] 河上・証拠法ノート(1)87 頁。
[333] 直接強制処分の定義につき，前掲注 26 参照。
[334] 安富・コンピュータ犯罪161頁，新保156頁。
[335] 廣畑・捜索・差押え 71 頁。
[336] 原田・コンピュータ 226 頁。
[337] 新保 153～154 頁。ほかには，廣畑・捜索・差押え 71 頁，安富・コンピュータ犯罪 161 頁，柳 307 頁をも参照。
[338] 酒巻・提出命令 128 頁。そして，新保 153～154 頁，柳 307 頁をも参照。

る差押えをしたとしても，警察側(技官や専門家等との連携をも含む)自らがＩＴ技術などの支障を排除し捜査の目的を遂行することができないから意味がないという問題点が指摘される[339]。そして，この問題点への対応として，②間接強制処分(提出命令や協力義務に関する規制など)が提案される[340]。その上で，被処分者が②の間接強制処分を甘受した場合には，③直接強制処分である差押えを終局的手段とし，警察側が媒体の占有を剥奪したうえで，それに対し自らアウトプットをしたりコンピュータ・フォレンジクをしたりすることにより対応することができるという対策が挙げられている[341]。

このように，②は①の対応策であり，③は②の対応策であるが，③の対応策は結局①の問題点に戻るものにすぎないから，③の対応策は，②の問題の解決策にはならないのである。この点を意識しているかどうかは明らかではないが，②の問題点につき，捜査を断念するしかないという可能性を明言している論者もいる[342]。しかし，それ以上に，この問題を解決するためにあるべき対応策は何なのかについては，具体的な議論がなされていない。

３．可能な解決策について

この問題に対しては，迂回型の情報取得という捜査の手法が対応策として考えられる。ここでいう迂回型の情報取得とは，被処分者の意思の如何を問わずに，解除できないＩＴセキュリティを迂回しながら目標たるデータを直接に取得することができるという，オンラインでの捜査手法をさす。この迂回型の捜査手法により，オンライン侵入技術を利用し対象者の端末に侵入したうえで，まだ暗号化されていないコードを取得したり，対象者の暗号を解読するための秘密鍵を取得したりすることができる。つまり，正面から暗号を解読する必要がなくなるわけであり，それゆえ，かかる捜査手法は間接強制処分という制度に含まれた欠点の解決策となりうるのである。

それでは，かような迂回型の捜査手法は，台湾の現行法上，認められているものであろうか。この点，前述したように，現行法は，その文言上，形式的には，電磁的記録をも捜索・差押えの対象としているが，いまでも，差押えの定義は，占有の剥奪を必ず必要不可欠な核心の要素としているから，オンラインでデータを取得することを差押えであるとは言い難い。また，迂回型の捜査手法を行うためには，オンラインでアクセスしたりＩＴセキュリティを解除したりする必要がある。この点，まずはアクセスすることを捜索であると言えるのかが疑問である[343]。かりにそれを捜索と位置づけることができるとしても，そのアクセスの範囲をいかに画定することができるのか，言い換えれば，令状の記載の在り方は何なのかが必ずしも明白でないし，それについての規定も，学説上の理論の蓄積も欠けている。また，ＩＴセキュリティの解除の法的位置づけも問題となる。それを捜索・差押えに

[339] 新保 153～154 頁。そして，酒巻・提出命令 128 頁をも参照。
[340] 同前注。
[341] 同前注。
[342] 新保 153 頁。
[343] 肯定説は，林鈺雄・捜索扣押 95 頁を，否定説は，捜索修法(二)131 頁蔡秋明の発言を参照。

必要な処分であるとする考え方もありうるが，既に論じた通り，データにアクセスしたり，それをコピーしたりすることを捜索差押えと言えるのかという点自体に疑問が残されているし，また，巨大なＩＴシステムのセキュリティを解除することにより侵害されうる利益は，場合によって，本体処分であるアクセスないしコピーという行為により侵害されるものよりも重大となる可能性もあるから，かような解除行為を果たして必要な処分と解することができるのかについては，大きな疑問がある。

そこで，立法論的には，かような迂回型の捜査手法を導入しようとすれば，2001年の台湾刑訴法改正のように，占有の剥奪という概念を核心とした既存の有体物に対する捜索・差押えを準用するという形をとることだけでは問題の解決には意味がなく，迂回型の捜査手法を実定法化するための前提としては，正面から，占有の剥奪という概念から離脱した，情報に対する捜索・差押えという制度を新たに構築すべきである。というのも，ここまでの検討により示されたとおり，この新制度のもとで，差押えの定義について，有体物を対象とする場合には，占有の剥奪を核心の要素とする旧来の理解をそのまま維持することができるのに対して，無体物を対象とする場合には，終局的処分権を核心の要素とするものであるので，差押えの定義との衝突が解消されるからである。また，捜索についての詳細は第２章において検討する予定であるが，情報に対する捜索・差押えという制度は，情報それ自体を処分の直接の対象とすることを前提としているから，正面から，アクセスしたりＩＴセキュリティを解除したりするなどのような捜査行為を規制することも可能となる。

Ⅲ．領置について

前述した新たな押収の定義からすると，領置は，「物の占有又は情報の終局的処分権を取得する過程において物理的ないし非物理的な強制力の使用を伴わずに，差押えの効果が発生する処分」と定義される[344]。

このように，領置は，物の占有又は情報の終局的処分権を取得する過程が任意であるものの，一旦，それらが政府に取得されれば，物や情報を提出する者の意思に反しても，強制的に「占有の剥奪」あるいは「情報の終局的処分権の剥奪」状態を継続できるので，この意味での法的な強制の効果は，差押えの場合と異ならない[345]。

---

[344] 証拠になりうる物若しくは没収すべき物，又は証拠になりうる情報若しくは没収すべき情報でなくとも，領置の対象になりうる(法務省・実務刑訴126頁注3は「領置は押収の一種であるが，差押えと異なり，令状を必要としないことはもとよりとして『証拠物又は没収すべき物と思料するもの』以外の物もその対象となる。」とする。また，永谷11頁～12頁をも参照)。ただし，証拠になりうる物若しくは没収すべき物，又は証拠になりうる情報若しくは没収すべき情報ではないことが明らかである，又は，捜査には何の役にも立たないと判断された際には，領置することができない。また，領置した物・情報が，証拠になりうる物若しくは没収すべき物，又は証拠になりうる情報若しくは没収すべき情報ではないこと，又は捜査には何の役にも立たないことが判明したときは，直ちに還付しなければならない。

[345] 陳樸生・刑訴(重訂十版)213 頁は領置の場合にも差押えの場合と同様に物の占有を取得しかかる占有の状態を強制的に維持することができるから，それも強制処分である押収の一態様であるとする。また日本においては，領置を強制処分とするのが多数説である(鈴木茂嗣・刑訴改訂 90 頁，石川・通説刑訴 139 頁)が，これに対して，任意処分と解する見解も少なくはない(河上ほか編・大コンメンタール第２巻 300 頁，警察庁・解説犯捜規範(6 版)187 頁，最三決昭 29 年 10 月 26 日刑集 99 号 531 頁，小林充・刑訴新訂 98 頁，安富・刑訴法 134 頁等)。

第２款　差押えの対象

Ⅰ．差押えの対象としての情報

１．情報の構造――記号論からの視点

情報を(強制)処分の対象とすることを認めるためには，まず，処分の対象にあたる「情報」の具体的な中身は何なのかという問題を検討しておく必要がある。以下では，記号論(Semiotik)の視点に基づき，ここでいう「処分の対象としての情報」の構造を明らかにする。情報は無形であって，「記号」により定義しなければならないものであるので，この意味で，記号論により情報の構造を明らかにすることが適切かつ可能だと思われる。

ここでいう記号論は，基本的に，ドイツの Morris の理論に基づくものであるが，本稿は，彼の理論をそのまま受け入れるわけではなく，彼が提案したいくつかの重要な概念を借りて，情報の意義を明らかにするするものである。Morris によると，記号論は，構文論(Syntaktik)，意味論(Semantik)，及び語用論(Pragmatik)という３つのカテゴリーからなるものであるとされる[346]。これを踏まえ，本稿は，情報の構造を，構文，意味と語用の３つの要素からなるものとする。具体的には，次の通りである。

(1)「構文，意味，語用」の３つの要素について

A.「構文」要素

「構文」要素とは，「定着させられた記号の組み合わせ」と定義される。例えば，それをデジタルデータの場合に当てはめると，「コールサイン(das Zeinchen)[347]により組み合わせられた０と１との配列」を意味する。また，手書きの場合でいえば，人間の言語――例えば，日本語，中国語，ドイツ語，英語など――の文法に基づき文字という記号を組み合わせた表現と説明することができる。

そして，コールサインであれ文法であれ，それらはいずれも，一定の規則からなるものであって，これらの規則に沿って組み合わせた記号の集合が定着(固定)しているといえよう。この意味で，記号の組み合わせの構造を示す「構文」要素は「定着性」を有するものということができる。

---

[346] この分類は,Morrisが1946年に提出したものであって,その後,学界に広く受け入れられてきたとされる(Vgl. Morris, Zeichentheorie, S.26； Morris, Zeichen, S. 324ff； Eco, Zeichen, S. 32；und vgl. Weiß, S.8)。そして，この分類は，オンライン捜索などの，情報を直接の対象とする捜査手法の議論において，刑事法の学者によく利用されている。例えば，Weiß, S.10は，この３つの分類をもとに，オンライン捜索における研究の対象を，証拠としての価値を有する情報と定義する；あるいは，Sieber, Informationsrecht, S.2572はこの３つの分類を，法的な規制と結びつけながら，司法的な目的利用に適合するものであるとする。

[347] コールサインとは，１と０を組み合わせるための法則であり，人間の言語に喩えて言うと文法にあたる。ドイツにおいて最初に知られたのは，1968年Bob Bernerにより導入された米国標準情報交換コード(ASCII)であって，その後に広がったのは，ウィンドス及びその応用プログラムに利用された米国規格協会コード(ANSI-Code)であるとされる(Vgl. Korge, S.7。Und vgl. Computer-Lexikon, “ANSI-Zeichensatz”, http://www.lexitron.de/main.php?detail=true&eintrag=1355)。

B. 「意味」要素

「意味」要素は，「記号の形成(Gebilde von Zeichen)により伝えられる『具体化された内容』を表すメッセージ」と定義される。この定義でいう「具体化された内容」における「具体化された」という言葉は，「記号の組み合わせにより定着させられた」と言い換えることができる。そして，ここでいう「内容」とは，喩えて言えば，著作権法でいう「アイデア」にあたる。

そして，「構文」要素と「意味」要素との関係を，著作権法の概念に喩えて説明すると，著作権法は，「構文」要素である「定着させられた記号の組み合わせ」――すなわち，表現――を保護するが，「意味」要素である「具体化された内容」――すなわち，アイデア――を保護しないというふうに考えてよいと思われる。

このように，アイデアは抽象的・主観的なものであって，それ自体は「定着性」を持たないものの，「構文」要素である「特定の記号の組み合わせ」により間接的に定着させられうるという意味で，「意味」要素は「準定着性」を有するといえよう。

C. 「語用」要素

「語用」要素は，「各々の受け手の，記号に対する異なる理解と感銘」と定義される。この「語用」要素は，記号を組み合わせた人が伝えようとするメッセージと，組み合わせられた記号を受け取った人が理解(感銘)したメッセージとの間が，必ずしも一致しているわけではない一方で，同じ(組み合わせられた)記号の集合により表れたメッセージに対する解読(力)には人によって個人差がある，という点に特徴がある。例えば，同じ判決に対して異なる評釈が出てくることが，その例である。この場合，評釈の対象は，同一の，裁判官が組み合わせた判決文の文字(記号)の集合であるものの，当該文字の集合により裁判官が一体何を伝えようとしているかという点については，学者ごとに異なる解読がなされるのは決して稀ではない。このように，同一の，定着性を持つ組み合わせられた記号の集合に対して，解読上の個人差が生じうることを，「語用」要素の「非定着性」ということができる。

(2)示唆

以上から，以下の３点の示唆が得られよう。

第１に，情報を定義する際には，「定着性」をもつ「構文」要素に照準を合わせるべきである。なぜなら，情報を差押えの対象とする場合において非物理的な支配・管理を可能にしようとすれば，まず，物理的な支配・管理でいう物の「定着性」に匹敵する，情報の「定着性」から出発しなければならないからである。

第２に，「意味」要素は，情報の本質を構成するものであると同時に，「構文」要素により定着させられうるものである。つまり，「意味」要素自体は，「準定着性」しか持たないから，「情報の終局的処分権」の客体にはならないので，「情報の終局的処分権」を

主張しようとすれば，「構文」要素により定着させられた「意味」でなければならない。

第３に，情報の不特定性は，個別の受け手ごとに異なる「語用」要素に由来する。言い換えれば，「語用」要素の介入により「構文」要素が改変されると，「構文」要素の定着性を喪失することになる。ただし，注意すべきは，前述した，同じ判決に対する異なる評釈が出てくるというような例は，「語用」要素の介入により「構文」要素が改変されるわけではないという点である。というのも，学者らが判決文をどう解読するかはともかく，すべての学者が同じ構文の判決を読んだことは間違いないからである。逆に，学者が自分の理解――「語用」要素――をもとに，判決文――「構文」要素――を整理したりサマリーしたりするのは，「語用」要素の介入により「構文」要素が改変される一例といえる。

２．定義と基準

ここで，前述した「構文，意味，語用」の３つの要素をもとに，「物の差押え」の核心要素である「占有剥奪」に対応する，「情報の差押え」の核心要素である「情報の終局的処分権」に照準を合わせて，「差押えの対象としての情報」の中身を明らかにしたい。

(1)物の構造と情報の構造との比較

物の構造と情報の構造とを比較すると，【表１】のようになる。

【表１】

<table>
<tr><th></th><th colspan="3">物の構造</th><th colspan="2">情報の構造</th><th>両者の異同</th></tr>
<tr><td rowspan="8">構成</td><td rowspan="8">物質</td><td rowspan="5">有体</td><td>目で見える外見(定着性[i])</td><td rowspan="8">記号
↓
無体</td><td rowspan="3">「構文」要素
(定着性)</td><td rowspan="8">定着性につき，物と情報との両者の間に程度は差があるものの，基本的には，両者はいずれも定着性の要素をもつと同時に，非定着性の要素も存在する。</td></tr>
<tr><td>例えば，包丁，篳篥など</td></tr>
<tr><td>目で見えない内部(定着性)</td></tr>
<tr><td rowspan="3">無体</td><td>五官で感知できる物質（準定着性[ii]）</td><td rowspan="2">「意味」要素
(準定着性)</td></tr>
<tr><td>例えば，光，電気等のエネルギー</td></tr>
<tr><td>固定された外見がない(非定着性[iii])</td><td>「語用」要素
(非定着性)</td></tr>
<tr><td rowspan="4">支配の形式</td><td colspan="3">物理的な支配・管理可能性あり</td><td colspan="2">×</td><td rowspan="2">準定着性は，物理的ないし非物理的な支配・管理可能性が実現される限り，法の定着性[iv]に転換することが可能である。</td></tr>
<tr><td colspan="3">目で見える外見(定着性)</td><td colspan="2">固定した構文(定着性)</td></tr>
<tr><td colspan="3">五官で感知できる 物質(準定着性)</td><td colspan="2">一定の構文により表れた一定の意味(準定着性)</td><td>排他性の有無：異
→判断基準を異にすべき</td></tr>
<tr><td colspan="3">占有による排他性のある利用の剥奪
→「占有」の剥奪</td><td colspan="2">×</td><td>終局の処分：同
→同等に保護すべき</td></tr>
<tr><td colspan="3">終局の処分(破壊する権原)の剥奪
→「占有」の剥奪</td><td colspan="2">終局の処分(デリート権)の剥奪→「情報の終局的処分権」の剥奪</td></tr>
</table>

【表１】の注と説明

※ 注：

[i] (物の)定着性：「物に対する人間の五官による物理的な直接の支配・管理の可能性」を意味する。例えば，包丁や箪笥等の有体物は，目で見えるし，手で移動させたりすることができる。

[ii] (物の)準定着性：「物に対する何らかの方法(ツールや技術)による物理的な間接の支配・管理の可能性」を指す。例えば，光，電気等のエネルギーなどの無体の物質は，直接には目で見えず手で掴めないが，適切なツール(エネルギーの貯蔵器など)を使えば，間接的にではあれ，それも一般の有体物のように所持(貯蔵)したり利用したりすることができる。

[iii] (物の)非定着性：「物に対する人間の五官による物理的な直接の支配・管理の不可能性」を意味する。

[iv] 法の定着性：「立法技術をもって定義や要件等を工夫することにより，『(物ないし情報の)準定着性』を『(物ないし情報の)定着性』とみなすこと」を意味する。例えば，「本法の差押えの規定は，何らかの方法による物理的な支配・管理が可能な光熱，電気等のエネルギーにも適用する。」というような規定においては，法は，定着性をもつ一般の有体物を対象とする差押えの規定を，本来定着性を持たず準定着性しか持たない光熱，電気等のエネルギーにも適用させている。この意味で，「法の定着性」とは，「立法技術によって擬制された(物ないし情報の)定着性」(以下は，「立法技術による擬制の定着性」という)と言い換えることができよう。

※ 説明：

情報の定着性(及びその準定着性と非定着性)につき，「本章第５節第２款Ⅰの１の(1)の A～C」の説明に加え本表の中身をも踏まえて，これからはさらなる検討を加える。

【表１】をもとに，以下では，物の定着性と匹敵する情報の定着性に着目し，差押えの対象としての情報を定義しながら，「情報の終局的処分権の剥奪」という基準をさらに具体化してみたい。

(2)情報の定着性について

前に述べた通り，差押えなどの処分には，処分の範囲を特定・明示するためにその処分の対象に対する支配・管理の可能性が要求されている。物を処分の対象とする場合において，その支配・管理の可能性は，「目で見える外見」という定着の要素ないし「五官で感知できる物質」などの物理的な準定着の要素に求められる。これに対して，情報を処分の対象とする場合には，情報は，「目で見える外見」がないし，「五官で感知できる物質」でもないため，物理的な支配・管理は不可能であるが，【表１】で示した通り，「構文」という非物理的な定着の要素及び「意味」という非物理的な準定着の要素を持つ。とすると，「構文」という定着の要素に着目し，「意味」という準定着の要素をも加味すれば，情報にも，物と同様に，法の定着性(立法技術による擬制の定着性)[348]を認めることが可能だと思われる。

A. 処分の対象としての情報の３層構造

こうして，情報を独立した強制処分の対象とする場合でいう法の定着性とは，「強制処分の対象としての情報の定着性」を意味する。そして，「強制処分の対象としての情報の定着性」の構造は，「構文」という定着の要素に着目し，「意味」という準定着の要素をも加味すれば，次の３層構造からなるものになる。

すなわち，第１に，「記号の組み合わせの集合」自体が「一定の構文」により定着させられたものでなければならないこと，第２に，「記号の組み合わせの方式」は「一定の法

[348] 法の定着性の定義及び物を対象とする場合でいう法の定着性の例につき，本章【表１】の注の「[iv]」参照。

則」により定着させられたものでなければならないこと，そして，第３に，「記号の組み合わせにより表れる意味」は，一定の法則に基づきなされた一定の「記号の組み合わせの集合」により定着させられたものでなければならないこと，である。

B.「差押えの対象としての情報」の定義

「構文」要素に照準を合わせると，「差押えの対象としての情報」は，「証拠になりうる定着させられた一定の記号の組み合わせの集合又は法の要求に基づき削除すべき定着させられた一定の記号の組み合わせの集合[349]」と定義される。そのうえで，「意味」要素をも取り入れると，上記の定義の「定着させられた一定の記号の組み合わせの集合」という部分に，一定の法則により一定の「意味」を表すものでなければならないという限定がかかることになる。ここでいう一定の法則としては，例えば，前述した，人間の言語の文法あるいは機械語のコールサインなどがあげられる。

C.「差押えの対象としての情報の定着性」の定義と具体化

情報を差押えの対象とする場合における法の定着性とは，「差押えの対象としての情報の定着性」を意味する。

そのうえで，前に述べた３層構造に従って「差押えの対象としての情報の定着性」を定義すると，次のようになる。すなわち，「情報を取得(複製・記録)するには，情報の構造における一定の『構文』要素並びに当該『構文』要素により定着させられた『意味』要素のみを複製・記録することであり，複製・記録の過程において『語用』要素の介入により『構文』要素が改変されてはならない」。

この定義を，「占有の剥奪」という要素に対応する「情報の終局的処分権の剥奪」という要素に照らして，さらに具体化することができるが，その前提として，本章４節３款における情報の終局的処分権についての検討結果を確認しておく。

第１に，情報の差押えに対して保護される法益であるデリート権が侵害されたといえるための基準は，「情報の終局的処分権の剥奪」である。第２に，「情報の終局的処分権の剥奪」が発生したといえるための基準は，政府により取得された「情報の複製・記録」が「原始の情報」との間に同一性があると見られる「合理的信頼価値」を有しているかという点にある。そして，第３に，「合理的信頼価値」を有するといえるための基準は，合理的な一般人であれば，当該「情報の記録」と「原始の情報」との間に同一性があると考えるか(合理人基準)，に求められる。

そのうえで，これらと，ここでいう「差押えの対象としての情報の定着性」との繋がりを説明すると，次のようになる。

複製・記録の過程において「語用」要素が介入していない場合，言い換えれば，「構文」

[349] 「法の要求に基づき削除すべき定着させられた一定の記号の組み合わせの集合」とは，没収すべき物に対応する概念であり，それを，没収すべき情報と言い換えることができる。具体的には，ネット上の児童ポルノなどの違法情報が考えられる。

要素が改変されていない場合，合理的な一般人であれば，当該「情報の記録」と「原始の情報」との間に同一性があると考えるから，「情報の複製・記録」と「原始の情報」との同一性についての「合理的信頼価値」が認められるので，このような「情報の複製・記録」が政府に取得されたときに，「情報の終局的処分権の剥奪」が発生したということができる。

逆の例をあげると，例えば，警察官が容疑者Aの容ぼう，行動のスタイルないし名前，住所などの個人情報についての聞き込み調査を行うというような事案では，聞き込み調査の記録においてAの個人情報を記載していたとしても，この記録自体は，情報の差押えには当たらない。というのも，このような記録は，専ら「意味」という準定着要素を対象とし，情報の差押えといえるために必要不可欠な「構文」という定着要素が欠けているからである。

この点についてより具体的にいうと，まず，当該情報を記録する過程においては「語用」という非定着の要素が，次に示す通り，五重も介入している。すなわち，当該記録は警察官が自分の個人的認知(第二重「語用」)により理解(第三重「語用」)した見聞(第一重「語用」)の「意味」要素を，自分の陳述能力(第四重「語用」)に基づき再度組み合わせた(第五重「語用」)記号の集合にすぎない。とすると，この例は，明らかに，前述した「複製・記録の過程においては『語用』要素が介入していない」という命題に反しており，それゆえに差押えの対象としての情報にあたらないのである。

以上の通り，「構文」が改変されるかどうかという定着要素により，抽象的な合理人基準を具体化すると同時に，差押えの対象としての情報にあたる範囲とそうでない範囲を適切に区画することができる。

(3) 自律産出情報について

以上の検討をもとに，次に，コンピュータやネットワークのユーザー自身は，往々にして，どのような自律産出情報[350]が，いつ，どこで産出されたかを全く知らないのに，なぜ，自律産出情報を自己の情報といえるのかという問題点を検討する。

この点については，情報の終局的処分権の主体と，情報を産出した主体とは，そもそも一致する必要がないので，ユーザー自身は，どのような自律産出情報が，いつ，どこで産出されたかを全く知らなくても，情報の終局的処分権の所有者として権利を主張することは可能であるということができよう。

確かに，情報の終局的処分権の主体と情報を産出した主体とは一致するのが通常であるが，一致しない場合も決して稀ではない。このことは，写真撮影の例を考えてみれば明らかである。すなわち，人や物自体は，「定着させられた一定の記号の組み合わせの集合」ではないから，差押えの対象としての情報に当たらない。しかし，ファイルの記録ないしデジタル画像データにより表現される人の容ぼうないし物の状態は，「一定の『構文』要

[350] コンピュータの設定・計算・処理により自動的に産出されたあるユーザーに関わる情報をさす。

素により定着させられた『記号の集合』」に該当し，差押えの対象としての情報にあたることになる。というのも，「人の容ぼう」ないし「物の状態」を「一定の『構文』要素」により表記すると，当該「構文」要素を表す記号の集合自体であれ，当該記号の集合を形成する法則であれ，それらはいずれも，定着したものになるからである[351]。

以上をもとに，「人の容ぼう」ないし「物の状態」の写真撮影による捜査という場面に照らして，「自律産出情報」を自己の情報であるといえるのかという問題点を再考してみよう。まず，情報を産出した者(撮影者)は警察官であるが，情報の終局的処分権の主体は被撮影者であるという点については争いがないだろう。他方，撮影が密かに行われた場合，被撮影者は，自分の情報が，いつ，どこで撮影(産出)されたかを全く知らないが，その場合であっても，被撮影者が，警察に撮られた「自分の容ぼう」の写真に対して，情報の終局的処分権の主体としての地位に立っていることは変わらない。そうだとすれば，自律産出情報の場面においても，同様に解することができるはずだと思われる。

以上により，情報の差押えの具体的な方法としては，前述した「(情報の)複製・記録」のほかに，「(情報の)産出」もあげられるのである。

(4)情報に対する権利の具体化

ところで，前述した自分の容ぼうの写真というような例では，情報の終局的処分権という法益によらず，既存のプライバシー権や情報自己決定権などの法益もその根拠としては考えられるのではないかという疑問があるかもしれない。

それはその通りであるとはいえ，独立した基本権としての情報の終局的処分権を承認することに全く差し支えはない。というのも，情報の終局的処分権と従来に認められてきた複数の基本権の保護範囲とが一部で重なっていることと，情報の終局的処分権が独立した基本権として認められるかということとは別の次元の問題であり，両者は両立することができるものだからである。

この点については，第２章において，情報の終局的処分権の具体的な中身及びそれと従来のプライバシー権ないし情報自己決定権との相違を明らかにしている。そこで述べた通り，複数の基本権の間に競合関係が生じうること自体が問題視されることはない。というのも，プライバシー権，知る権利，表意自由，名誉権ないし情報自己決定権などの基本権の間にも競合関係があるが，だからといってそのうちのどちらかが否定されることはないからである。

以上の通り，競合関係の存在自体は問題にはならず，真剣に検討すべきは，競合する複数の基本権の間における適用関係をどのように決めるべきかである。この点につき，一般論としていえば，競合する複数の基本権それぞれの核心的な保護法益に沿って，それぞれ

[351] 人の容ぼうないし物の状態を表記する一定の記号の集合の意味をより具体的にいえば，例えば，アナログの場合であるなら，磁気テープの＋−記号の一定の組み合わせの集合を指し，デジタルの場合であれば，コードの一定の組み合わせの集合を指す。他方，記号の集合を形成する法則とは，写真撮影技術に使われた記号の組み合わせを決めるためのルールを指す。

の具体的な中身を形成するのに必要な要件を確認したうえで，それぞれの法的位置づけに基づき，適用関係を決めるべきであるということになるが，それを具体例によって敷衍すると，次のようになろう。

例えば，公道上の個人の行動を録画する場合，従来のプライバシー権の理解からすると，公道上の行動である以上プライバシーの領域ではないから，プライバシー権が否定されるという結論になる。そうすると，それには自己情報決定権の保護も及ばないことになる。というのも，自己情報決定権の保護対象は，プライバシーに関わる私的な情報に限られていると解されてきた[352]からである。また，こうした場合は，個人の行動を録画していたとしても，対象者の顔を特写するのでないかぎり[353]，録画の角度ないし器械の性能との関係で，顔自体は識別できる程度綺麗に映っていないことがよくあるとすれば，肖像権によっても保護は困難になろう。

これに対して，前述した通り，情報の終局的処分権は，プライバシーや肖像権ないし情報自己決定権などを保護するものではなく，「処分の対象としての情報の三層構造」が情報の終局的処分権の保護法益の具体的な内実である。

この三層構造の理論からすると，前掲の事案では，顔自体は識別できる程度に綺麗に映っておらず，かつ，公道上の行動ではあるが，個人が，「自分が，ある時間帯に，ある場所で，ある行動を行った」という原始情報を産出・複製・記録されたときは，かかる産出・複製・記録の過程において「語用」要素が介入していない場合であるかぎり，「情報の終局的処分権」により保護されることになる。というのも，こうした場合は，録画された，「誰が，どこで，いつ，何をしていた」という「原始の情報」を表す「一定の『構文』要素により定着させられた『記号の集合』」がそのまま産出・複製・記録されており，「語用」要素が介在していない以上，かかる「記号の集合」と原始の情報との間に同一性があることについて「合理的信頼価値」が認められるので，このような「記号の集合」が政府に取得(産出・複製・記録)されたときに，「情報の終局的処分権の剥奪」が発生したと評価できるからである。

つまり，公道上の録画のケースのような場面では，プライバシー権や自己情報決定権ないし肖像権の侵害にはならないが，「情報の終局的処分権」からすれば，基本権を侵害する強制処分になりうるのである。

他方，仮に，長時間の録画でなく，瞬時的・断片的な写真撮影にすぎない事案であるならば，顔自体は識別できる程度綺麗に映っていないし，また一断面の画像だけであるから，映されたのは一体誰か，そして何をしていたかが明らかではない以上，原始の情報がその原始の構文の通り記録されておらず，語用の要素が介在している記録にすぎないから，そ

---

[352] 司法院大法官会議解釈 603 号参照。

[353] 公道上の行動であるならば，行動者が自ら肖像権を放棄すると解する見解（大阪高判昭和 31 年 4 月 19 日刑事裁判資料 123 号 180 頁）に対して，新しい見解として，デモ行進や暴走族の共同走行は集団としての表現行為の限度でプライバシーを放棄していると見るべきであって，参加者の個々の容貌について捜査官憲がこれを撮影することを許すまでにプライバシーを放棄しているとは見るべきでないとするものがある(大阪高判昭和39年5月30日高刑集18巻2号14頁，同解として，古田(監修)96，107 頁の説明をも参照されたい)。

れによっては「情報の終局的処分権の剥奪」が発生したとはいえないので，それは強制処分にはあたらないことになる。

このように，「情報の終局的処分権」を適用した結果が従来の理解からの結論と同じになる場合もあるが，その理由は異なるものである。

Ⅱ.「関連性」要件について

続いて，2001 年の台湾刑訴法改正により導入された令状主義のもとにおいて要求される，いわゆる「関連性」要件につき，情報を，差押えの直接の対象とした場合には，いかなる問題が生じうるかを検討し，その解決策を模索してみたい。

この関連性要件は，差押えの範囲を画定するための基準として機能するものであり，その根拠は，台湾刑訴法 133 条 1 項(日本刑訴法 99 条の定めに相当するもの)に求められるとされる[354]。言い換えれば，関連性要件の要求により，捜査の対象である犯罪と関係のある物ないし情報しか差し押さえられない。ここで，関連性を判断できれば特に問題はないが，問題となるのは，その判断ができない場合においては差押えの対象をどう決めるべきなのかという点である。

この問題点は，とりわけ，フロッピーディスク等の内容を確認せずに差し押さえる場面で顕在化するという指摘が学説上は一部でされてきた[355]。しかも，この指摘をした論者は，かような場面で行う差押えの正当性を認めるべきであると結論付ける[356]。その理由としては，①技術的には，コンピュータ鑑識を行い現場で内容を確認することが困難ないし不可能であること，②仮に，かかる鑑識の現場での実施が技術上は可能であるとしても，それを行うと時間が大変かかること，③伝統的な家宅捜索の場合においても同じ性質の差押えがなされてきたこと（例えば，内容を見ることもなく大量の文書を一括して差し押さえておくのが実務上は必ずしも稀ではない），という３つのものがあげられている[357]。

しかし，この論拠を確認すると，単に，捜査上の必要性があること(①と②の理由)，及び，これまでも同じ形態の差押えをやってきたから，電磁的記録の場合にも同じ処理をしてよい(③の理由)というものとなる。そうだとすれば，その妥当性についてはなお再検討の余地があると考える。というのも，捜査上の必要性があるからといって必ずしも権利侵害を正当化することができないし，また，従来行われてきたことだからといって，その正当性が当然に認められるわけではないからである。

この問題に関して，台湾においては参考となる裁判例が見つからないが，日本においてはリーディングケースとされる最二決平成 10 年 5 月 1 日刑集 52 巻 4 号 275 頁（以下，「平成 10 年決定」という）が挙げられる。本決定は，結論としては，前掲の台湾の先行研究の見解と同様に，フロッピーディスク等の内容を確認せずに差し押さえることができる旨を

---

[354] 李・電磁記録 1078 頁。
[355] 同前注。
[356] 同前注。
[357] 同前注 1079～1080 頁。

判示したものであるが，本決定を検討対象とした日本の先行研究は豊富であり，より精密な検討がなされているから，フロッピーディスク等の内容を確認せずに差し押さえることの正当性・許容性を再考するための有益な示唆を与えるものと考えられる。そこで，以下では，平成 10 年決定並びにそれに関連する議論を検討し，そのうえで，台湾への示唆を洗い出したい。

そのために，まずは，フロッピーディスク等の内容を確認せずに差し押さえることをどのように称すべきかを確認しておく必要がある。日本の学説上，それを「包括的差押え」と称する見解は数多くあり[358]，かかる用語を使った裁判例もある[359]。また，台湾においても，日本の学説を参考に，「包括的差押え」という用語を，中国語である「概括性的扣押」と訳したうえで援用している論者がある[360]。しかし，包括的差押えという用語には以下のような問題点があるため，不適切だと思われる。

１．日本における議論について

(1)「包括的差押え」という用語について

包括的差押えを文言通り解すれば，複数の電磁的記録媒体を一括して差し押さえるという意味で捉えるのが自然であろう。しかし，実際には，この問題は，一枚の電磁的記録媒体の場合にも生じうる。というのも，一枚の電磁的記録媒体であっても，現場で当該媒体の中に被疑事実と関連性のあるデータがあるかどうかを確認することができない場合，それを確認せずに差し押さえる必要が生じうるからである。この意味で，包括的差押えの問題の核心は枚数とは関係がなく，複数を語意とする「包括的」という用語は必ずしも妥当でないと思われる。

もっとも，前掲の平成 10 年決定は，108 枚のフロッピーが押収された事案であるから[361]，仮に，問題が枚数だけであるとすれば，複数のフロッピーを差し押さえた事案である限り，包括的差押えと称しても，違和感がないかもしれない。しかし，包括的差押えという用語は，枚数の問題に止まらず，さらに次の見解が指摘するような問題点を含んでいる。

「逆にいえば，関係記録がある蓋然性がある物件と，あるとは認められない物件が混在する場合に，それらを一括して差し押さえることまでを当然には許容していないと思われます。もし，そのようなものも含めて『包括的差押え』という言い方でこれを許容するとすれば，それは適切ではないし，そういう表現の仕方自体ややミスリーディングなところがあるようにも思われます。」[362]

---

[358] 河原 65 頁，山田 192 頁，井上弘通 336 頁，吉田 63 頁，上村 93 頁，寺崎 249 頁，伊藤ほか・注釈(新版) 2 巻[藤永] 151 頁，松尾・条解 4 版 204 頁，井田良ほか編著・事例Ⅱ刑訴[真田]464 頁，光藤・刑訴法Ⅰ150 頁，平良木・刑訴法Ⅰ203 頁等。

[359] 大阪高判平成 3 年 11 月 6 日判タ 796 号 264 頁。

[360] 林裕順・基本人權 146 頁。

[361] ところで，前掲注 335 に挙げた平成 3 年の判決も複数のフロッピーディスクが押収された事案である。

[362] 長沼＝山田 54 頁(長沼)発言。

ここで述べられている「関係記録がある蓋然性がある物件と，あるとは認められない物件が混在する場合に，それらを一括して差し押さえること」は，前に引用した「内容がわからぬ以上，すべての磁気テープ類をとりあえず差し押さえざるをえないということになる」という河上検事の見解と同じものであろうと思われる。前述した通り，この河上検事の見解に対しては学説から厳しい批判がなされており，前掲の指摘も同じく批判的な立場に立っているものである。

他方，平成 10 年決定以前になされた，「全部のフロッピーディスクを包括的に差し押さえる」という表現を使った大阪高判平成 3 年 11 月 6 日判タ 796 号 264 頁（平成 3 年判決）は，文言上からみるかぎり，河上検事の見解に近いものであるようにみえる。この点につき，山田教授は，平成 3 年判決に関して，次のような見解を述べている。

「『結局内容がわからぬ以上，すべての磁気テープ類をとりあえず差し押えざるを得ない』とする見解もあるが，そのような包括的差押えは一般令状禁止の趣旨からは疑問であろう。……本件判決は，包括的差押え許容のもうひとつの根拠として被処分者による罪証隠滅のおそれをあげ，本件において，具体的な罪証隠滅工作がなされたことを認めている。……本件判決は，コンピュータ機器の捜索･差押えにおける捜査機関側の困難とともに被処分者による罪証隠滅のおそれを重視して，捜査の必要を優先させたものと判断される。フロッピーディスクの包括的差押えの適否に関しては，本件判決が重要な先例的意義をもつとされる……ことから，今後ますますふえると予想されるこの種の捜査への影響も大きいと考えられる。一般令状禁止の趣旨が十分理解されるならば，できるかぎり包括的差押えは避けるべきで，選別のための合理的な努力がなされなければならない。そのためには，専門家の養成･補助が不可欠であり，また，必要性判断に際しては，罪証隠滅のおそれの他に，特に，被疑者と被処分者の関係や被処分者の業務の種類･性格･規模などを考量したうえで，被処分者が受ける不利益への十分な配慮が必要とされよう。」[363]

山田教授のこの指摘は，平成 3 年判決を，前述した河上検事の考えと同様に，関係記録がある蓋然性があるとは認められない物件が混在する場合にも，それらを一括して差し押さえることを認めたものという理解に立つものであろう[364]。

以上に対し，この大阪高裁の平成 3 年判決は，最高裁の平成 10 年決定と表現が異なるものの，基本的な考え方には大きな違いがないだろうと解する見解もある[365]。

ともあれ，最高裁の平成 10 年決定では，既に，蓋然性による差押えが認められる旨を明示している以上，現在では，現行法のもとにおいて蓋然性のない物まで含めて包括的に差し押さえることは認められないと解すべきであることに疑問はないと思われる。

以上のとおり，包括的差押え(台湾のいう概括性的扣押)という用語は，蓋然性のないも

---

[363] 山田 193 頁。

[364] 山田教授と類似する見解として，伊藤ほか・注釈(新版) 2 巻[藤永]151 頁は「……捜索差押えの現場でフロッピーディスクの内容を確認して選別することが実際上極めて困難な場合には全部のフロッピーディスクを包括的に差し押さえることもやむを得ない措置として許容される(大阪高判平成３・11・6 判タ 796・264)」とする。

[365] 池田 268 頁＝最判解（平成 10 年度）88 頁。

のに対する差押えまで許容されるという誤解を招致するおそれがあるものであるから，本稿では，「蓋然性による差押え」という用語を用いることとする。

(2) 蓋然性による差押えについて

平成 10 年決定が，蓋然性による差押えの許容性を認めた具体的な論拠は，次の通りである。

「本件は，自動車登録ファイルに自動車の使用の本拠地について不実の記録をさせ，これを備え付けさせたという電磁的公正証書原本不実記録，同供用被疑事実に関して発付された捜索差押え許可状に基づき，司法警察職員が申立人からパソコン一台，フロッピーディスク合計一〇八枚等を差し押さえた処分等の取消しが求められている事案である。原決定の認定及び記録によれば，右許可状には，差し押さえるべき物を『組織的犯行であることを明らかにするための磁気記録テープ，光磁気ディスク，フロッピーディスク，パソコン一式』等とする旨の記載があるところ，差し押さえられたパソコン，フロッピーディスク等は，本件の組織的背景及び組織的関与を裏付ける情報が記録されている蓋然性が高いと認められた上，申立人らが記録された情報を瞬時に消去するコンピュータソフトを開発しているとの情報もあったことから，捜索差押えの現場で内容を確認することなく差し押さえられたものである。令状により差し押さえようとするパソコン，フロッピーディスク等の中に被疑事実に関する情報が記録されている蓋然性が認められる場合において，そのような情報が実際に記録されているかをその場で確認していたのでは記録された情報を損壊される危険があるときは，内容を確認することなしに右パソコン，フロッピーディスク等を差し押さえることが許されるものと解される。」

この判示につき，蓋然性による差押えとの関係で検討すべき問題点は，以下 A と B で示す２つの点である。

A.「蓋然性」要件を正当化するための論拠

第１に検討すべきは，蓋然性と関連性との関係である。すなわち，関連性は，従来，差押えに必要な要件(差押えの理由)とされてきたのに対して，平成 10 年決定は，「令状により差し押さえようとするパソコン，フロッピーディスク等の中に被疑事実に関する情報が記録されている蓋然性が認められる」場合に差押えを認めており，それが，関連性という要件を満たさない差押えの許容性を認めたものだとすれば，一般令状禁止原則に反するものではないかという疑問が生じるからである。

この点に関する学説の見解は，大きくは，①内容が確認できない以上，とりあえずすべての電磁的記録媒体を包括的に押収することができるとする立場，②蓋然性による差押えは一般的探索的押収に当たるので許されないとする立場，③一定の要件の下に蓋然性による差押えを認めることができるとする立場，の３つに区分できる[366]。

[366] 柳川 81 頁，池田 265 頁＝最判解（平成 10 年度）85 頁。

このうち，①を検討する必要はないと思われる。というのも，前述した通り，平成10年決定の旨は，蓋然性のない物をまでも差し押さえられるという意味での包括的差押えを認めるものではないからである。また，②については，検討の余地があるが，ここでの検討は，蓋然性による差押えは一般的探索的押収に当たらないとする平成10年決定の立場を前提とするものであるので，②についての詳細な検討は後に行うことにしたい。

以上より，③がここでの検討対象となる。その問題の核心は，なぜ，関連性によらず蓋然性だけでも差押えが認められるのかという点に帰結する。以下では，まず，従来の見解の内容を検討し，その問題点を洗い出したうえで，私見を述べる。

(A)関連性緩和説

関連性緩和説とは，電磁的記録媒体に対する蓋然性による差押えでいう蓋然性を，「推認された関連性」と捉えたうえで，それを，日本刑訴法 99 条が要求する「確認された関連性」という原則を緩和したものであると解する立場を指す[367]。この説は，学説上の多数を占めているように思われる。

通常の場合，差押処分を執行するには処分の対象の中身を見た上でそれと被疑事実との関係の有無を判断しておかなければならず，関係があると判断されたものしか差し押さえられない。これが，一般に言われる「関連性」要件であり，それを「確認された関連性」と呼ぶ。これに対して，捜査機関が，差押えの対象の中身を見ていないにもかかわらず，何らかの事情に鑑み，それが被疑事実と関係があるのではないかと推測されただけでも，その対象を関連性のある差し押さえるべき物とみなして，その占有を剥奪することが認められることを，「推認された関連性」と呼ぶ。これを平成10年決定に当てはめれば，「蓋然性」要件ということになる。

問題は，なぜ，例外的にではあれ，「蓋然性」要件だけで差し押さえることが認められるのかである。この点に関して，川出教授が次のような説明を提供している。

「『正当な理由』を基礎付ける関連性の程度は，令状執行の際の具体的状況によって変動しうるものであるというわけである。刑訴法上も，例えば，100条1項では，通信官署が保管又は所持する郵便物等で，発信人又は受信人が被告人であるものにつき，通常は開披してみないと証拠物か否かが判断できないという特殊性を考慮して，その内容を確認することなく一律に差し押さえることができるとしており，この規定は，まさに，関連性の程度が低くても差し押さえが認められる一例であるということになろう。」[368]

---

[367] 寺崎・252 頁，壇上・54 頁，柳川 82 頁，小川 261 頁，秋山・令状記載 251 頁，甲斐 20 頁，小津 55 頁，川出・フロッピーディスク 182 頁など。もっとも，これらの見解の間にも論者によっては異なるニュアンスが含まれるものであるが，ここでの整理は，あくまで，「処分の対象の中身を見た上で関連性を判断すべきということを原則としてあげながら，中身を見ることができないという場合には，従来理解されてきた『関連性による差押え』の例外として，中身を見ていないままの『蓋然性による差押え』を認めるべきとする」という最大公約数的な意味で，関連性緩和説というカテゴリーに帰納させたものである。

[368] 川出・フロッピーディスク 182 頁(川出教授は，このような考え方を挙げているに止まり，それを支持するかどうかについては明白にされていない)。

蓋然性による差押えは，電磁的記録媒体の場面に特有の問題ではなく，現行法においても，郵便物に対する蓋然性による差押えを定めた日本刑訴法100条1項が存在する，という川出教授の説明からは，電磁的記録媒体に対する蓋然性による差押えを論じる際に，100条1項との比較検討が有益かつ必要であるという示唆が得られよう。そこで，以下では，100条1項の合憲性の論争を検討しつつ，電磁的記録媒体に対する蓋然性による差押えと100条1項の郵便物に対する蓋然性による差押えとを比較しながら，論点を洗い出すことにしたい。

①日本刑訴法 100 条 1 項の合憲性と蓋然性による差押え

日本刑訴法100条1項の合憲性についてのこれまでの学説を整理すると，次の６つの立場に分けることができる。

すなわち，①「差押えの対象は，証拠物又は没収すべき物でなければならない」という日本刑訴法99条の一般原則を前提に，被告人から発し，又は被告人に対して発した郵便物だからといって，それが直ちに証拠物又は没収すべき物にあたるものではないのに，無条件で差し押さえることができるとする日本刑訴法100条1項は，一般的・探索的差押えにあたり，違憲であるとする立場である[369]。

②郵便物は，被告人から発し，又は被告人に対して発したものであれば，一応，被疑事実と関係のあるものであると推定することができるから，日本刑訴法100条1項は同法99条の関連性の要件を緩和したものであるが，違憲ではないとする立場である[370]。

③日本刑訴法100条1項には明示されていないが，同法99条が適用される結果，100条1項によって差し押さえることができるのはやはり証拠物或いは没収すべきものに限られるので，違憲の問題にはならないとする立場である[371]。

④郵便物の占有を一括して取得するものの，無関係な郵便物であることが判明したら直ちに返還するため，それは差押えではなく，したがって，日本刑訴法100条は差押えの要件を緩和したものでないから違憲の問題にならないとする立場である[372]。

⑤郵便物は開披してみないと証拠物であるかどうかが判断できないので，日本刑訴法100条1項は，それを開披できるように，捜索と同じ条件で差押えを認めたものと解する立場である[373]。

⑥日本刑訴法100条は，同法99条の要件を緩和した特別規定であるが，開披しなくても犯

---

[369] 団藤・条解(上)202 頁，平場・改訂講義 302 頁，高田・刑訴法(2 訂版)173 頁，平場ほか・注解(全訂新版)上巻 322 頁(旧版：平場ほか・注解(上巻)315～316 頁)，瀧川ほか・刑訴コメ 139～140 頁，鈴木・刑訴法 86 頁，滝川＝竹内・刑訴講義 141 頁，佐藤・憲法(3 版)576 頁，法協・註解憲法(上)624 頁等。

[370] 足立 315 頁，伊藤・実際問題 95 問 189 頁，藤永ほか編・大コンメンタール(二)[渡辺]269～270 頁＝河上ほか編・大コンメンタール第２巻[渡辺]289～290 頁等。

[371] 小野・ポケット(上)244 頁，高田編・法セコメ刑訴(三版)[田口]95 頁，三井・手続法Ⅰ[新版]57 頁，田宮・注釈刑訴 124 頁，田宮・刑訴(新版)102 頁，松尾・条解 4 版 208 頁，福井・刑訴講義 5 版 142 頁，野中ほか・憲法Ⅰ(5 版)425 頁[高橋]など参照。

[372] 河上・令状請求(二)162 頁(河上検事自身が④の見解を支持するわけでなく，単に学説上このような見解があるとして列挙したものである)。

[373] 小野・ポケット(上)244～245 頁，平野・刑訴全集 112～113 頁。

罪と無関係であることが明らかな場合，差押えの必要性がない場合，及び郵便物が全く特定されていない場合には，同100条1項の適用がないとする立場[374]である。

ここからは，関連性緩和説の考えは，基本的には上記の②の見解と異ならないものであることがわかろう。というのも，川出教授が指摘した通り，「通常は開披してみないと証拠物か否かが判断できないという特殊性」に着目すれば[375]，可読性・可視性のない電磁的記録の場合と日本刑訴法 100 条 1 項の郵便物の場合とを同様に考えてよいからである。

しかしながら，関連性緩和説には，以下のような問題点があり，妥当とは言い難いと思われる。

②関連性緩和説の問題点

まず問題となるのは，電磁的記録媒体に対する蓋然性による差押えの場合には日本刑訴法 100 条 1 項のような特別の定めがないから，その現行法上の根拠は何なのかである。

また，同 100 条 1 項の場合には，「被告人から発し，又は被告人に対して発したもの」という点から，一応，被疑事実と関係のあるものであると推定することができる(すなわち，「推認された関連性」が存在する)といえるのに対して，電磁的記録媒体に対する蓋然性による差押えの場合であるならば，一体，何をもって，「推認された関連性」が存在するといえるのかが必ずしも明らかでない。

さらに，関連性緩和説には，100 条 1 項に関する前述の②の見解と同様に，日本国憲法 35 条との関係で，なぜ，差押えの理由につき，従来の「関連性」要件を「蓋然性」要件へと緩和することができるのかという問題がある。

この点について考えられる理由としては，次の２つのものがある。その１つは，電磁的記録媒体の特殊性ゆえに，現場で関連性を確認することができないということであり，もう１つは，平成 10 年決定で示された「証拠滅失の恐れ」の存在である。

しかしながら，この２つの理由は，いずれも，捜査の必要性を示すものにすぎず，それだけでは論拠にならないと言わざるを得ないであろう[376]。関連性緩和説の理論的な論拠を構築しようとすれば，その第一歩として，関連性を蓋然性に緩和したとしても，日本国憲法 35 条の関連性という要件によって基本権に対して提供された保護の内容ないし程度が縮減することはないということを論証しておかなければならないと思われるが，関連性緩和説の論者からはこの点について十分な説明がなされていない。

---

374 河上・令状請求(二)162 頁。

375 飯島 91～94 頁をも参照されたい。

376 この点は，「『必要性は法を持たない。』necessitas non habet legem. この法諺は有名である。必要性それ自体では法にはならない。必要性には，本来的に行き過ぎ，法のきびしい枠を破る危険要因が多分にある。その行き過ぎを合理的に抑制する規範的要因が作用しないかぎり，必要性それ自体は法をなさない。」とする鴨・刑訴基本理念 101 頁の指摘の通りであろう。

(B)必要な処分説

「蓋然性による差押え」を認めるもう1つの有力な見解として，必要な処分説を挙げることができる。この見解の代表的な論者である酒巻教授によると，「蓋然性による一時的な占有剥奪」は，差押えでなく，捜索・差押えの目的を遂行するために必要な処分である[377]。なぜならば，関連性の選別を必ず現場で行わなければならないわけではなく，現場での選別が不可能ないし不適切である場合は，関連性を確認するために，とりあえず，その中に関連性のあるデータが存在する蓋然性がある電磁的記録媒体である限り，当該媒体を，一時的に，他の適当な場所に移すという必要な移動行為をすることができ，これは差押えではないからである[378]。

このように，必要な処分説によると，蓋然性による差押えは，差押えではないから，関連性の問題は生じないという帰結になる。

この見解は，基本的に，前述した100条1項の合憲性に関する④の立場と同じものであると考えられる。しかし，蓋然性による差押えの正当化の論拠としては，必要な処分説であれ，④の立場であれ，それらのいずれにおいても以下のような問題を含んでいるため，妥当とは言い難い。

①定義に関わる問題点

まず，前述した④の立場によると，100条1項は郵便物を一時的に移動することを認めているだけであるから，それは捜索の一環として捉えるべきであり，差押えではないとされてきた。しかし，100条1項は，その「一時的な移動」を「差押え」と明示的に定めているから，このような説明は，条文の文言に明らかに反する。

また，一時的な移動だから物の差押えに該当しないと解するのは，差押えの定義とも整合しない。というのも，一時的な移動とはいえ，それによって占有剥奪が発生しており，従来，占有剥奪と定義されてきた物の差押えという概念に当てはまることは明らかだからである。

他方，電磁的記録媒体を対象とする場合においては，100条1項のような規定はないが，差押えの従来の定義を維持するかぎり，必要な処分説も，前述した④の立場と同様な問題点を抱えているといえる。前述した平成10年決定も，占有剥奪を核心の要素とした差押えの従来の定義に従い，蓋然性により電磁的記録媒体の占有を一時的に剥奪したことを，差押えであると明示的に述べている。

②執行の適正ないし事後の救済に関する問題

さらに，④の立場に従って，蓋然性による差押えを差押えではないと解した場合，差押えの執行中の適正手続を担保するための規定ないし事後救済等の関連規定の適用ができな

[377] 酒巻匡・捜索・押収444頁以下。また，小林充・刑訴新訂103頁をも参照。
[378] 酒巻匡・捜索・押収447～453頁。同解として，長沼・電磁的情報47～48頁参照。

くなってしまうという問題点がある。具体的には，被処分者に対して押収目録の交付もなされず，準抗告も許されないことになる。当然，必要な処分説も同じ問題点を抱えている[379]。

この点に対して，必要な処分説からは，解釈により，あらかじめ令状裁判官が押収目録の交付などの適当と認める条件を附けることが可能であり，占有の一時的な取得も，押収に関する処分として準抗告の対象になりうるとされる[380]。

確かに，明文規定が欠如していても，司法的法創造のアプローチによって解決することが可能であるとすれば，この点は重大な問題にならないとする余地があるかもしれない。しかし，現行法のもとにおいては裁判官が令状に条件を付することができるのかという点自体については争いがあるし[381]，また，強制処分法定主義のもとでは，司法的法創造のアプローチによる対応はむしろ例外とすべきであろう。そうだとすれば，電磁的記録媒体に対する蓋然性による差押えの場面においても，このようなアプローチを活用することの適切性については，慎重な吟味を要する。

以上により，執行中の適正手続の担保及び事後救済の規定が欠如している点は，やはり，必要な処分説の大きな問題点であるといわなければならない。この点をも考慮に入れると，現行法の解釈論としては，蓋然性による差押えは，やはり，差押えと解する方が適切であると思われる。

(C)私見：「関連性＝蓋然性」という構造

以上の通り，日本における「蓋然性による差押え」を正当化する見解である，関連性緩和説と必要な処分説との２つの学説は，一時的な占有の取得(剥奪)を差押えと見るか否かという点で異なるものの，関連性要件が満たされるためには，対象物の中身を見て関連性の有無を確認しなければならないことを前提とするものである。

ここに，問題を解決するために必要な鍵が提供されている。すなわち，ここでの問題の核心は，関連性要件を定義するには，対象物の中身を見ることをその前提とすべきであろうかという点に帰結することができる。

本稿は，関連性要件により権利に対して提供される保護の内容ないし程度が縮減することはないという保障が，法により実質的に担保されているかぎり，そもそも，関連性要件が満たされるためには，中身を見ながら関連性の有無を確認しておくことを必要としないと考える。すなわち，最小化原則による実質的保障(すなわち，同じ程度の保障が実質的に担保されることをさす)を前提に，確認された関連性であれ，推認された関連性であれ，それらは，いずれも，関連性要件を充足するということであり，従来のように，関連性による差押えが原則で，蓋然性による差押えが例外であるという区分は必要でなくなる。この考え方を，「『関連性＝蓋然性』という構造」と称する。

---

379 この点，寺崎 256 頁参照。そして，長沼＝山田 58 頁(山田発言)においても同様の指摘がなされた。

380 寺崎 256 頁，酒巻・捜索・押収 455 頁の注 18 参照。

381 酒巻・条件の付加 8 頁以下参照。

この構造のもとにおいては，蓋然性は低度の関連性であるが，台湾刑訴法133条1項[382]で要求される関連性要件を緩和したものでなく，本来同条で予定されている関連性の一態様にすぎないがゆえに，蓋然性による差押えが認められるという帰結になる。そして，中身を見た上で処分の対象にあたるかどうかについての判断を行うことは，あくまで，処分の対象を最小化するための１つの可能な手段にすぎないから，他の手段によって処分の対象が最小化されているという点が担保されるのであれば，それに固執する必要はないのである。

この「『関連性＝蓋然性』という構造」の実益としては，次の点が挙げられる。

①理論上の利点

台湾においても，関連性緩和説と似たような見解が存在している。前に引用した，技術上ないし時間のコストなどの捜査の必要性を理由に，膨大な情報が入った電磁的記録媒体に対して，蓋然性による差押えを行うことの正当性を認めた台湾の学説がそれにあたるものと考えられよう。

本稿が提案したいわゆる「関連性＝蓋然性」という構造のもとにおいては，蓋然性による差押えは，そもそも，台湾刑訴法133条1項本文の関連性による差押えそのものであるから，他の特別な規定を根拠とする必要はない。とすると，関連性緩和説に対して提起された，電磁的記録に対する蓋然性による差押えの場合の刑訴法上の特別な根拠は何なのかという問題点が解消されよう。

それと同時に，電磁的記録媒体に対する蓋然性による差押えの場合には，一体，何をもって，「推認された関連性」が存在するといえるのか，及びなぜ関連性を緩和することができるのか，という２つの問題点も解決される。というのも，「関連性＝蓋然性」という構造のもとにおいては，蓋然性が関連性の一態様であり，関連性を緩和したものではないので，「推認された関連性」（関連性の例外としての蓋然性）というような概念を観念する必要は全くないからである。

他方で，台湾においては，日本でいう必要な処分説と類似の見解は見当たらないが，刑訴法上，捜索・差押えのために必要な処分を定めた規定[383]が用意されていることに鑑み，この必要な処分説を台湾の解釈論にも採り入れることが可能であるという見方もありうる。

これに対して，本稿の提案である「関連性＝蓋然性」という構造によると，必要な処分説のように，一時的な移動は占有剥奪である差押えではないというような技巧的な説明によらなくても，蓋然性による差押えの許容性を認めることができる。それゆえ，必要な処分説が抱えていた差押えの定義との不整合の問題が解消されることになる。

また，「関連性＝蓋然性」という構造は，蓋然性による差押えは「差押え」であることを前提とするものであるから，執行の適正手続の担保ないし事後救済という点も問題にはならない。

---

[382] 「証拠となる若しくは没収できる物は，それを差し押さえることができる。」

[383] 台湾刑訴法 144 条 1 項は，「捜索・差押するために鍵・封緘を開けたりしてあるいはその他の必要な処分を行うことができる。」と定めている。

②台湾刑訴法 135 条と職権による差押えの立法妥当性への再考

台湾刑訴法135条1項2款[384]は，日本刑訴法100条1項と類似するものと考えられる。しかし，日本の状況を検討したところで見た同100条1項の合憲性にかかわる争いは，台湾の場合は生じていない。すなわち，殆どの学説は，台湾刑訴法135条の合憲性を無批判に受け入れてきた[385]。というよりも，大多数の学説は，このような問題意識すら持っていないというのが台湾の現状であるといっても過言ではない。その理由としては，次の２点が考えられる。第１に，台湾の場合には，通信の秘密は中華民国憲法12条により明文で保護されているが，令状による捜索・差押えを定めた日本国憲法35条のような条文がないこと，第２に，台湾においては，独立した差押状が存在しないことである。この２つの点を更に敷衍すれば，次のようなものとなる。

まず，第1の点については，前にも言及したとおり，中華民国憲法においては令状主義を示す明文条項が存在しない点は異論がないところであるが，令状主義というものはあくまで立法政策の問題であって憲法上の原則ではないとする多数説と，憲法の精神からも令状主義が憲法上の原則であることを導き出すことができるとする有力説とが対峙している。しかしながら，ここで注意しなければならないのは，この争いの核心は，令状を発付する権限を，裁判官にのみ付与すべきであろうか，それとも，検察官にも与えることが可能であろうかという点にあることである。

換言すれば，ここでの検討課題である関連性という要件については，有力説はもちろんのこと，多数説であっても，本件と関係があると思料されるものしか差し押さえられないこと――すなわち，差押えの関連性要件――が憲法上の要求であると認められており，その根拠は，日本でいう憲法上の原則としての令状主義でなく，中華民国憲法23条の比例原則から導かれた最小化原則[386]に求められている[387]。この点に関して，令状主義はあくまで立

---

[384] 「郵政若しくは電信機関，または郵電事務を執行する人員が所持若しくは保管する郵便物，電報については，下掲する事情のいずれに該当する場合，それを差し押さえることができる。

一　本件と関係があると信じられる相当な理由がある場合。

二　被告人から発し，又は被告人に対して発した場合。但し，弁護人との往来の郵便物，電報については，犯罪の証拠が隠滅，偽造あるいは変造されたり，若しくは共犯あるいは証人と通謀されたりするおそれがある場合，または被告人が既に逃亡された場合に限るものとする。

前項の差押えを行うする場合，即時に，郵便物，電報の差出人あるいは受取人を通知すべきである。但し，訴訟手続に妨害を与える場合，この限りでない。」

[385] 確かに，同 135 条 1 項 2 款に対して合憲性の疑問を呈する少数説もあるが，しかし，その論拠は，令状主義のいう関連性要件とは全く関係ないものである(林永謀・刑訴釋論(上)475～476 頁)。

[386] 確かに，日本においては「……我が国における比例原則の位置づけはなお不明確である。即ち，行政法学においては，比例原則が憲法 13 条に『実定化』されているものとする立場のほか，特に憲法の条項に言及することなく，『法の一般原則』として『不文法源』の１つにあげるものがあり，さらに，『条理』としての妥当を説くものがみられ，これら理由づけの複数があげられることもある。……他方，憲法学においては，比例原則という用語自体がそれほど一般的なものではないようにみうけられ，教科書をいくつか繙いてみても，比例原則という言葉はほとんど見当たらないのが現状である」とされてきた(高木 211 頁。須藤 10 頁及び 14 頁をも参照されたい)。他方，刑事法の分野においては，「手続の適法性に関する判例が用いる『諸事情の総合判断』『相当性』」につき，「比例原則」という用語を用いてそれを表す論者があり(前田・相当性判断 497 頁)，また，「警察比例の原則」を，行政法でいう「比例原則」の一環として捉えられる学説もある(川出・行政警察活動 76 頁)。これに対して，台湾では，比例原則は中華民国憲法 23 条に実定化されているとす

法政策の問題であって憲法上の原則でないと主張する代表的な論者とされる林鈺雄教授は，135条1項2款に対して次のような批判を述べている。

すなわち，「135条1項2款[日本刑訴法100条1項に相当するもの]により要求される差押えのハードルは133条1項[日本刑訴法99条に相当するもの]のそれ[すなわち，日本のいう関連性要件の要求]よりも低いものではある。これは，立法の錯誤であろうか。この点は，解釈論による解決の道を探求することができよう。すなわち，133条1項の規定は，差押えのハードルの『下限』を定めているものであって，その他の規定は，それに『付加』された制限にすぎない。これによると，135条1項2款の場合にも，同様に，当該郵便物・電報は証拠ないし没収すべきものにあたると信じられる合理的な根拠がある場合にかぎり，その差押えが認められると解すべきである。」[388]

この理解は，基本的には，前掲の日本刑訴法100条1項の争いにおける③の立場と同じ論旨をとるものと考えられる。すなわち，台湾刑訴法135条1項2款には明示されていないが，同法133条1項が適用される結果，同135条1項2款によって差し押さえることができるのは当然には証拠物或いは没収すべきものに限られるので，違憲の問題にはならないという理解である。

以上より，台湾においては，中華民国憲法23条の最小化原則から導かれた憲法レベルでの差押えの関連性要件が認められているといえよう。この意味では，台湾も日本と同様に，憲法上の要求としての差押えの関連性要件という視点に基づき，刑訴法135条1項2款の合憲性問題を検討するための土台があるということができよう。

しかし，台湾の場合には，同条項の合憲性に係る問題意識の種を培養するために必要な土台はあるが，その種を開花させることができてはいない。というのも，前述したとおり，台湾においては，独立した差押状という制度が存在していないので，この最小化原則という土台に埋められたかかる問題意識の種を開花させるために必要な養分が非常に貧弱なものであるからである。

この点をさらに検討すると，まず，なぜ，台湾の立法者が独立した差押状を必要としないかを検討しておく必要がある。この点の理由は，従来は，捜索は差押えの手段であり，差押えは捜索の目的であるので，両者は密接な関係があるから，両者を一体化する――すなわち，差し押さえるべき物を捜索令状に記載し，捜索令状をもって差押えを行うという形をとることをさす――ほうが妥当だという点にあるとされてきた[389]。かような立法モデルに対しては，次のような批判がなされている。

すなわち，「かかる立法モデルは便利であるが，捜索・差押えは同じ属性のもの(捜索＝差押え)であると誤解させやすいし，また，2001年法改正後，捜索令状を発付する権限を裁判所にのみ与えることとなったのに，差押えの部分はそれに応じて調整していないため，

るのが通説であるし，かかる用語を，憲法学の分野においても刑訴法学の分野においても，通用するものである。

[387] 林鈺雄・捜索扣押 35～36 頁。

[388] 同前注 217 頁(脚注 4)。

[389] 林榮耀・刑訴釋論 188 頁，黃朝義・刑訴三版 234，255 頁。

数多くの未解決の問題が残されている。」[390]

ここでの検討との関係でいえば，2001年以後，検察官は，捜索令状の発付権限を奪われたが，捜索が不要な場合においては，検察官の職権による(無令状の)差押えの権限が依然として保持されている点が重要である。すなわち，もし，捜索を行わないと，差し押えるべき物を探し出すことができない場合，つまり，捜索令状が必要な場合には，検察官は裁判官の発付する捜索令状がなければ差し押さえることができないのに対して，差し押えるべき物の所在が明らかである場合，つまり，捜索が不要な場合，例えば，売店で児童ポルノDVD(法禁物)を見つけた場合，あるいは，町で怪しいと思われるバイクのナンバーを確認してみたらそれが盗難車であることを発見した場合であるならば[391],検察官は,職権により,DVDないし盗難車を差し押さえることが現行法上認められているのである[392]。

以上により，2001年以後に，台湾の立法論としては，差押えも，捜索のように，司法令状による審査の制度を設けるべきであると考える[393]。これを実現するには，日本のように，独立した差押令状を設けることが考えられる。というのも，捜索を必要とする場合は，捜索令状を差押令状とみなしてもよいが，捜索を必要としない場合には，現行法上は独立した差押状が存在しないため，この部分についての検察官の職権による差押えの権限がそのまま残されているからである。

③台湾刑訴法 135 条 1 項 2 款の立法価値について

前述したとおり，台湾においても，前掲の日本刑訴法100条1項の争いにおける③の立場と同じ論旨をとるものがある。すなわち，台湾刑訴法135条1項2款(日本刑訴法100条1項に相当するもの)には明示されていないが，同法133条1項(日本刑訴法99条に相当するもの)が適用される結果，同135条1項2款によって差し押さえることができるのは当然に証拠物或いは没収すべきものに限られるので，違憲の問題にはならないという立場である。

本稿の提案である「関連性＝蓋然性」という構造のもとでは，蓋然性による差押えを，この③の立場と同様に，台湾刑訴法135条1項2款は同法133条1項の適用に反しないものであると解することができるが，本稿の理論と③のそれとは全く異なるものであるから，下掲する③に対する批判ないし再反論は，いずれも当てはまらない。

まず，③説に対しては，学説上，そのような見解によると，日本刑訴法100条1項の規定はその存在する理由を完全に失ってしまうのではないかという批判が一部でなされてきた[394]。この批判を，台湾の場合に当てはめると，台湾刑訴法135条1項2款の立法価値がなくな

---

390 黄朝義・刑訴三版 255 頁。類似する批判として，傅美惠・偵査 250 頁をも参照。

391 ここで，バイクのナンバーを確認すること自体を，捜索に該当するものであるとも考えられる筈ではないかという疑問が生じうるかもしれないが，台湾の現行法のもとにおいては，誰でも見られるバイクの番号をみることは捜索に当たらず，捜査官が既に合法に見た番号をさらに盗難車両番号の登録システムに照合することの性質は，鑑識(情報照合)と位置づけられており，これも捜索に該当しない。

392 林鈺雄・捜索扣押 224 頁。同見解として，陳瑞仁・新法捜索扣押 68～69 頁参照。

393 これに対して，反対説がある(柯・刑事程序 216 頁，傅・偵査 250～253 頁参照)。

394 平場・注解(上巻)316 頁。

ってしまうこととなる。この批判に対し，③説の論者は，日本国憲法21条2項の定めがあるから，とくに確認的には100条1項の規定を設けたのであると反論してきた[395]。だが，この反論に対してはまた，100条1項は確認的な規定に過ぎないとすればその価値が非常に薄いものであると再反論されうるだろう。この議論は，台湾刑訴法135条1項2款の解釈論にも適合するものと考えられる。

これに対して，本稿の「関連性＝蓋然性」という構造のもとにおいては，台湾刑訴法135条1項2款の規定は，単なる確認的な規定にとどまらず，同法133条1項の関連性を類型化したものとして，存在意義が十分に認められる。言い換えれば，135条1項2款の要件は133条1項に由来するものであるとはいえ，それをさらに具体化した要件であり，133条1項の要件と同じものではないからである。

そして，こうした具体化した要件としては，135条1項2款によれば，①原則として郵便物に対しては捜索することができないこと，及び②「被告人から発し，又は被告人に対して発した郵便物」という制限が付けられること，の２つのものが挙げられよう。この点をより具体的に説明すると，次のようになる。

まず，①の原則として郵便物に対しては捜索することができないという点については，台湾刑訴法135条1項2款の法文ではなく，同135条1項2款と同じ構造を持った日本刑訴法100条1項に関わる日本の通説を台湾の解釈論にも採用すべきであるというのが私見である。

この点，日本の通説によると，日本刑訴法100条1項の法文上は，「…被告人から発し，又は被告人に対して発した郵便物…を差し押さえ，又は提出させることができる」と定められているから，そうでない郵便物を差し押さえてはならず，そして，この選別は，捜査機関ではなく郵便局員に行わせるべきであると解される[396]。言い換えれば，原則としては，捜査機関が100条1項の差押えを行うために捜索することが禁じられている。この見解を台湾刑訴法135条1項2款に当てはめると，捜査機関が同135条1項2款の差押えを行うために捜索することが原則的に認められないこととなる。

こうして台湾刑訴法135条1項2款の構造を再整理すると，それは，「郵便局員の協力による捜索」(通信の秘密の保護のために不可欠な最小化の措置：蓋然性の確認)→「差押え」(蓋然性による占有剥奪)→「捜査機関による捜索」(関連性の確認)，という３段階の仕組みになる。この３段階の仕組みにより，135条1項2款の要件と133条1項のそれとは異なること，及び135条1項2款の価値は，単なる確認的な規定を超えたものであることの２つの点が立証されよう。

B.「証拠滅失の恐れ」という要件について

次に検討すべきは，平成 10 年決定は，「蓋然性」要件の他に，「記録された情報を損壊

[395] 三井・手続法(1)[新版]57 頁。

[396] 藤永ほか編・大コンメンタール(二)[渡辺]271 頁。また，通信関係書類の押収捜索・87 頁，高橋勝・通信の秘密(2)60 頁，警察庁・適正な捜査 172～173 頁の説明をも参照されたい。

される危険がある」という要件（以下，「証拠滅失の恐れ」[397]という）をも挙げているが，「蓋然性」と「証拠滅失の恐れ」という２つの要件の間の関係は何なのか，言い換えれば，証拠滅失の恐れは，蓋然性による差押えを認めるために不可欠の要件なのかである。

これを肯定する見解からは，その理由として，関連性を緩和するのはあくまでも例外であるので慎重さを必要とするという点が挙げられる[398]。これに対して，「証拠滅失の恐れ」は，押収の必要性の有無を判断する要素の１つに過ぎず，蓋然性による差押えに必要不可欠の要素ではないとする否定説がある[399]。

まず，肯定説の立場が，「証拠滅失の恐れ」という要件があってはじめて関連性を緩和した蓋然性が認められるというものであるとすれば[400]，理論的には疑問が残る。というのも，前述した通り，「証拠滅失の恐れ」という要件は捜査の必要性を示すものにすぎず，それ自体が直ちに理論的な論拠にはならないからである。また，捜査の必要性は多種多様であるのに，「証拠滅失の恐れ」が存在する場合にのみ緩和が認められるとすれば，それは一貫性を欠いているものであると思われる。

そして，関連性ではなく蓋然性により差押えが行われた場合に，関連性という要件によって基本権に対して提供された保護の内容ないし程度が実質的には縮減されないように担保することさえできれば，「証拠滅失の恐れ」という要件を不要とする否定説を採用するとしても，必ずしも人権保障を害するものではないように思われる。

以上に対し，本稿の「関連性＝蓋然性」という構造によると，証拠滅失の恐れという要件による制限は不必要なものである。というのも，蓋然性による差押えはもともと台湾刑訴法 133 条 1 項(日本刑訴法 99 条に相当するもの)でいう関連性による差押えの一態様であって，その例外ではない以上，証拠滅失の恐れというような要件をもって適用範囲を減縮する必要はないからである。

C. 台湾への示唆

以上により，立法論としては，次の２点が重要である。

(A)蓋然性により差し押さえた後の規制の必要性について

台湾においても，これまでは，捜査機関が適法に占有を取得した物であるならば，その内容を確認するのに別個の令状は不要であるというのが一致した見解である[401]。しかし，前述した通り，蓋然性による差押えは，従来の「捜索(関連性の確認)」→「差押え(関連性の

---

[397] 学説上は，「罪証隠滅」や「証拠隠滅」とするものが多いが，電磁的記録媒体の場合には，被処分者，捜査官が現場で操作ミスをすることによりデジタル証拠を損壊してしまう可能性が十分ありうるから，こうした場合には，意図的な行為を意味する「隠滅」という用語は適切でなく，より中性的な「滅失」という用語を使ったほうがよいと考える。

[398] 寺崎 252 頁。池田 269 頁＝最判解(平成 10 年度)89 頁，光藤・刑訴法 I 150 頁，庭山＝岡部・刑訴法 3 版 55 頁などをも参照。

[399] 柳川 83 頁，安富・フロッピーディスク 244～245 頁，小津 55 頁，飯島 94 頁，壇上 54 頁，甲斐 20 頁など参照。

[400] 池田 269 頁＝最判解(平成 10 年度)89 頁。

[401] 朱・刑訴(修二)134 頁。

ある物のみの占有剥奪)」という順序でなく，「差押え(蓋然性による一時的な占有剥奪)」→「捜索(関連性の確認)」という順序になる。

このように，「差押え→捜索」という順序になる「蓋然性による差押え」を行う場合は，蓋然性により差し押さえた時点では関連性が確認されていないうえに，その後の内容の確認にも令状は不要であるということになり，捜査への規制を失ってしまうので，適切とは言いがたい。それゆえ，立法論として，蓋然性により差し押さえた後の確認段階に対して，別個の令状による規制が必要であると考えられる。

そして，この後の確認段階に対する規制の必要性は，とりわけ，蓋然性による差押え性格をもつ新設されたリモート・アクセスによる差押えの場合に顕在化している。というのも，リモート・アクセスによる差押え関連規定が，オンラインでの蓋然性による差押えをした後の段階に対するあるべき規制を用意してはいない点は，オフラインのそれと同様であるが，前に検討した通り，オンラインでの蓋然性による差押えは，オフラインでの蓋然性による差押えと比べると，ＩＴシステムの広さが理論上は無限に拡張可能なのであるために，一般的探索的差押えになってしまう懸念がより一層深刻化するからである。

(B)「蓋然性を確認するための捜索」の規制について

以上に見た通り，電磁的記録媒体に対する蓋然性による差押えの場合には，日本刑訴法100条1項の郵便物に対する蓋然性による差押えの場合の「郵便局員の協力による捜索」という段階が欠けている。つまり，電磁的記録媒体の場合には，捜査機関が，自ら蓋然性を確認するための捜索を行うことができ，その点についての規制が加えられていない。

しかし，「関連性＝蓋然性」という構造によると，電磁的記録媒体に対する蓋然性による差押えと日本刑訴法100条1項で定められた蓋然性による差押えとは，その本質においては異なるものでない。そうだとすれば，電磁的記録媒体に対する蓋然性による差押えの場合においても，台湾の立法論としては，日本刑訴法100条1項の構造を参考に，例えば，「専門家の協力による捜索」→「蓋然性による差押え」→「捜査機関による捜索」といった規制を採用することが考えられよう。

そして，立法論上，「蓋然性を確認するための捜索」についての規制を必要とする理由としては，後に詳論するように，中華民国憲法23条から導かれた最小化原則をより貫徹できるという点が挙げられよう。というのも，蓋然性による差押えが不可避であるとすれば，捜査機関が自ら蓋然性を確認するための捜索を行うよりも，専門家が蓋然性を確認するための捜索を行う方が適切な最小化の手段であるといえるからである。

２．アメリカにおける議論について

以上の通り，蓋然性による差押えを巡る諸問題を解決するためには，新しい立法により，蓋然性による差押え後とその前との双方の段階に，法的規制を加える必要があると考える。そして，この２つの点に対応する立法を考えるにあたっては，ここまで紹介した日本法に

加えて，アメリカの関連議論を考察する実益ないし必要性があるようにも思われる。というのも，アメリカでは，既に情報を独立した処分の対象としているし，また，台湾においても，日本国憲法 35 条の母法と言われてきた修正４条[402]に関わる議論は常に捜査手続における立法論ないし解釈論の両面で活かされてきているからである。

そこで，これからは，前に検討した日本の状況をも踏まえて，蓋然性による差押えの検討との関係で日米の比較法的視点に基づく更なる考察を行い，そのうえで，台湾への示唆を洗い出したい。以下では，まず，日本とアメリカと比較するにあたって注意すべき点を敷衍しておこう。

(1)比較法的研究を展開するために

まず，用語については，日本でいう「蓋然性による差押え」を，アメリカの理解に照らして言い換えれば，「選別のための差押え」といってよかろう。だが，それぞれの法的理解には，以下のような差異がある。

A. 差押えの対象の差異について

物と並んで，情報をも強制処分の対象としているアメリカでいう選別のための差押えとは，現場では，差し押さえるべきデータとそうでないデータとを選別することができない場合に，選別のために，とりあえず，すべてのデータあるいはデータを記録した媒体を一時的に一括して差し押さえておくという手法である。

これに対して，有体物のみを強制処分の対象とする日本でいう蓋然性による差押えとは，ある電磁的記録媒体の中身を現場でみることは困難ないし不可能であるため，かかる媒体が差し押さえるべき有体物であるかどうかを直ちに確認することができないが，何らかの事情に鑑み，そこに関連性のあるデータが存在する蓋然性があると推認されうる媒体であるならば，そのような媒体を，関連性のある差し押さえるべきものであると見なした上でとりあえず一括して差し押さえておくことを意味する。

台湾の場合は，前記の日本の理解と接近するものと考えられるため，蓋然性による差押えと称してよかろう。

また，日本においては，電磁的記録媒体に貼られたラベルを見て，当該媒体が差し押さえるべき物であると判断された場合は，当該媒体の内部に被疑事実と関連性のあるデータがあるかどうかを確認する必要はなく，当該媒体全体を適法に差し押さえることができることになる[403]。こうした場合には，有体物のみを対象とする日本の現行法のもとでは，蓋然性による差押えの問題が生じることはないのである。

これに対して，アメリカにおいては，媒体も情報も捜索・差押えの対象になりうるから，

---

[402] 法協・註解憲法(上)326，328 頁(同旨として，樋口ほか・注釈憲法(上巻)[佐藤]748，750 頁，栗本 144，150 頁の注(11)，高柳ほか編・原文と翻訳 228，230 頁及び同・Ⅱ解説 186～187 頁，安富・コンピュータ犯罪 150 頁，佐藤隆一・プレイン・ヴュー32 頁参照。

[403] アメリカ法を参考に，反対説も一部で見当たられている。

発付された捜索(差押え)令状[404]に明記された対象が「データのみ」である場合は，電磁的記録媒体の外部のラベルを見て当該媒体に被疑事実と関連性あるデータを含んでいる可能性があることがわかったとしても，直ちに媒体を差し押さえることはできず，当該媒体から関連性のあるデータを選出しそれのみを取得するという形にしなければならないことになる。

ここで，台湾の状況を確認すると，法文上，形式的には，電磁的記録をも捜索差押えの対象としているから，理論的にはアメリカのやり方に接近するものとなるはずであるが，実際には，捜索・差押えの従来の定義は全く変わっていないし，また，実務上も，捜索(差押え)令状に明記された対象が「データのみ」となる場合は殆どないと思われる。言い換えれば，台湾の現状も日本のそれと同様に，電磁的記録媒体に貼られたラベルを見て，当該媒体が差し押さえるべき物であると判断された場合は，直ちに当該媒体全体を差し押さえるほうが通常であろうし，それは，当然には適法と評価されるものである。

B. 台日米の用語の対応関係について

アメリカで選別のための差押えを認めた先例としては，Sissler 事件[405]が挙げられる。Sissler 事件によれば，パスワードがかけられていること等により，現場で「正当な理由」(probable cause；すなわち，かかる媒体に被疑事件と関係するデータが記録されていること)を確認することができない場合，警察官は媒体の中に事件と関係あるデータが存在することを信ずる「合理的な理由」(reasonable believe)がある限り，現場で「正当な理由」を確認せずに，すべての記録媒体を一括して差し押さえておくことができるとされている[406]。

このように，アメリカの Sissler 事件と前述した日本の平成 10 年決定とを対照すると，同事件でいう「probable cause」という要件は，日本法でいう「関連性」に，同事件でいう「reasonable believe」とは，日本法でいう「蓋然性」に，それぞれ対応するものであると考えられよう。

以上に対し，台湾では，用語について，やや混乱が生じているようにみえるが[407]，差押えの場面でいえば，日本のいう関連性と蓋然性の概念と同じ内容のものが使われてきている。すなわち，台湾においても，差押えの対象は，証拠物あるいは没収できるものに限られると定められている(台湾刑訴法 133 条 1 項)ので，ここでいう証拠は本件と関係があるもの

---

[404] アメリカにおいては，捜索・差押は捜索令状(search warrant)により行われ，日本の如く差押状と捜索状との区別はない(Carmen at 195;栗本 150 頁注 12)参照。

[405] See United States v. Sissler, 1991 U.S. Dist. LEXIS 16465, at *10～*12.

[406] Id.

[407] アメリカのいう「probable cause」を「相当な理由」と訳するものとして，王兆鵬・捜索扣押 25 頁以下；陳瑞仁・相當理由 2 頁参照。この訳語に対し，それは，台湾刑訴法 122 条 2 項でいう「相当な理由」と混同するものであるし，被告人に対する場合には「probable cause」はいらないと誤解されてしまうおそれがあると批判しつつ，「合理の根拠」は，台湾刑訴法 122 条 1 項のいう「必要の時」及び同条 2 項のいう「相当な理由」の 2 つの用語の上位の概念であり，それを，必ずしもアメリカのいう「probable cause」の概念と同視することができないものであると述べている(林鈺雄・捜索扣押 65 頁)。他方，「probable cause」を「合理の根拠」と訳する論者がある(黄東熊・刑訴 234 頁)。

に限られるものと解される[408]。言い換えれば，本件との関連性が，差押えを発動させるための要件であるとされるから，この意味で，それを，関連性要件と称してもよかろう。また，前述したように，台湾の実務上も，日本と同様に，電磁的記録媒体を差し押える場合に，現場でその内容を確認することが困難な場面が稀ではないから，媒体の内容を確認せずに，本件と関連する証拠となるデータが存在する蓋然性がある媒体を差し押さえておくことが認められてきている。この意味で，こうした場合の差押えの発動要件を，蓋然性要件と称することができよう。

C. 関連性と蓋然性との関係について

ところで，アメリカの修正４条においては，２つの原則があるとされる。その１つは令状原則，もう１つは合理性原則である。両原則のいずれが第１原則であるかが争われてきたが，現在は，合理性原則が第１原則であるという見解が支配的であるとされる[409]。

そして，reasonable believe により差し押さえること(台湾と日本でいう蓋然性による差押えに相当する)は，probable cause により差し押さえること(台湾と日本でいう関連性による差押えに相当する)の一態様であると理解されている[410]。つまり，reasonable believe により差し押さえる場合も，probable cause を，reasonable believe に緩和したものではなく，probable cause の１態様である。というのも，第２原則である令状主義によって要求される probable cause の程度は，そもそも第１原則である合理性原則により調整されうるものだからである。

(2)問題の核心

ここまでの検討により，台湾と日本でいう蓋然性による差押えの許容性を巡る論争のもとにおいて最も核心的な問題とされてきたいわゆる「関連性と蓋然性との関係」という争点は，アメリカの議論においては，副次的な問題として取り扱われてきたにすぎないことがわかる[411]。

そうすると，次に問うべきは，アメリカの議論においては，選別のための差押え(台湾と日本でいう蓋然性による差押え)を巡る問題の核心は，一体何なのかである。この点については，蓋然性による差押えを行う時点においては関連性が確認されておらず，その後の内容の確認にも令状が不要であるとすれば，捜査への規制を失ってしまうということが，ここでの問題の核心であるとされる。

アメリカにおいても，日本と同様に，捜査機関が適法に占有を取得した物であるならば，その内容を確認するのに別個の令状は不要であるという原則が存在している。同原則は，

---

[408] 林永謀・刑訴釋論(上)471，477～478 頁。

[409] Amar，at 8～9，43～45，Solove，DIGITAL DOSSIERS，at 1118～119；and see Carmen，at 195.

[410] Id.

[411] 日本でのもう１つの争点である「証拠隠滅の恐れ」は，アメリカにおいては全く問題とされておらず，選別のための差押えを行うには，証拠隠滅の恐れは必要な要件とされていない。

自動車に対する無令状の捜索・差押えに関するROSS事件[412]により確立されたものである。本件の争点は，令状によらない合法的な捜索・差押えの権限が自動車内に置かれた容器にも及ぶのかという点にある。法廷意見は，捜査機関が合法的に自動車を占有した以上，車内にある容器の中身を確認するために別個の令状は不要であるとしつつ，自動車の内部に対する無令状の捜索を無制限に行うことができるわけではなく，それは場所・サイズにより適切に制限されているとする[413]。ここでいう場所・サイズによる制限とは，自動車の中にあるすべての容器を捜索してはならず，差し押さえるべき物が存在する蓋然性がある容器しか捜索できないことを意味する。例えば，拳銃を探すために車内の封筒(けん銃のサイズにはあわないもの)を開けてはいけないという意味で，捜索できる範囲が制限されているということである。

しかしながら，バーチャル空間であるＩＴシステムにおいては場所・サイズを観念できないため，場所・サイズによる制限は働かない。そこで，アメリカの議論では，コンピュータに対する選別のための差押えの場合には，伝統的な事案でなされるそれとは区別すべきであり，捜査機関が適法に占有したコンピュータの内容を確認するためには，別個の令状を必要とするという主張がなされてきた。その代表的な論者としては，Winick が挙げられる[414]。Winick は，TAMURA 判決[415]を理論構成の起点とし，コンピュータに対する選別のための差押えを行った場合においては，その後に第２段階の令状による規制が必要であると主張する。この意味で，Winick の理論を「(コンピュータに対する特別の)２段階令状論」と称してよかろう。

そして，この２段階令状論は，単なる１つの学説にとどまらず，これを明示的に採用した裁判例が既にいくつか現れている。とりわけ，1999 年の CAREY 判決[416]は，Winick の 1994 年の「コンピュータとコンピュータデータに対する捜索・差押え」[417]という論文を明示的に引用した上で，コンピュータデータに対する捜索・差押えの場合には，特別なコンピュータ令状を必要とすると判示した。その後，2004 年の ILLINOIS 決定[418]も，CAREY 判決を引用しながら，Winick の見解を取り入れたものとしてあげられる。

以上により，Winick の２段階令状論は，前に指摘した，蓋然性により差し押さえた後の規制の必要性という問題を考えるうえで有益な示唆を提供するものと考えられよう。そこで，以下は，Winick の理論を紹介しながら，台湾にとって参考になる部分を抽出したい。

---

412 UNITED STATES v. ROSS, 456 U.S. 798(1982).

413 ROSS, id., at 824～825.

414 Winick, at 80 ff.

415 UNITED STATES of AMERICA v. LEIGH RAYMOND TAMURA (694 F.2d 591; 1982 U.S. App. LEXIS 23412).

416 UNITED STATES OF AMERICA v. PATRICK CAREY. 172 F.3d 1268(1999).

417 Winick, at 75ff.

418 UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION, In the Matter of the Search of. 3817 W. WEST END, FIRST FLOOR CHICAGO, ILLINOIS 60621, 321 F. Supp. 2d 953(2004). But ILLINOIS, supra, is overruled by United States v. Gocha(N.D. Iowa Aug. 10, 2007)2007 U.S. Dist. LEXIS 58962.

(3) Winick の２段階令状論について

Winick の理論の起点となった TAMURA 判決は，従来の「混雑的文書のコントロール・ルール（The rule controlling searches of intermingled documents）」（以下，混雑文書ルールと略称する）をコンピュータなどの電磁的記録媒体に対する捜索・差押えの場合にも適用することができるとする[419]。ここでいう混雑文書ルールとは，被疑事実と関連性のあるドキュメントとそうでないドキュメントが混在している物理的な文書，書籍，ファイルなどの媒体は，その中に令状に記載された差し押さえるべきドキュメントを含んでいる限り，関連性のあるドキュメントと関連性のないドキュメントとが不可分であることから，それらを選別することなしに媒体の全体(すべてのドキュメント)を差し押さえることができることを意味する[420]。

しかしながら，アメリカにおいては，令状に記載されていないドキュメントをも含めて，それらをさらに詳しく調べるために，関連性のあるドキュメントと関連性のないドキュメントとを一括して差し押さえるという「無差別的差押え」（the wholesale seizure）は，原則として修正４条により禁止されている[421]。とすると，混雑文書ルールの適用は，正当な理由に由来する特定性・関連性という２つの令状原則の要求を満たしていないから，修正４条に反する無差別的差押えにあたるのではないかという点が問題となる。

この点について，TAMURA判決は，以下の理由で，混雑文書ルールの適用は修正４条に反しないと結論付けた。すなわち，現場では関連性のあるドキュメントと関連性のないドキュメントとを選別することができないか，あるいは分割しがたい場合に，公判前の準備手続で治安判事に一層詳しい調査の許可を請求する――言い換えれば，関連性のあるドキュメントを選び出し，それに対してのみさらに詳しく調べる――ため，現場で選別せずに記録媒体(紙媒体の文書)の全体(すべてのドキュメント)を一時的に一括して占有することは，令状における正当な理由(すなわち，特定性・関連性の要件)を満たすために必要かつ合理的な一時的無差別的差押えであり，修正４条が禁止する無差別的差押えにはあたらず，修正４条に反しないというのである[422]。

このTAMURA判決の見解は，修正４条の第１原則は合理性原則であるとする支配説と合致しているものであると思われる。なぜならば，TAMURAの見解は，正当な理由に由来する特定性・関連性の要件は，あくまで第２原則である令状主義の要求にすぎず，合理性原則により柔軟に調整することができるという理解に基づいているものと考えられるからである。

このように，合理性原則が第１原則であるとする見解の支配しているアメリカにおいては，選別のための差押えが特定性・関連性の要件を満たしているかどうかよりも，むしろ，①選別のための差押令状を発付するための要件は何なのか，及び②選別のための差押え後の規制はどうあるべきか，という２つの問題こそが重要である。そして，Winick は，この

---

[419] TAMURA, supra note 415, at 596～597.

[420] Id. And see United States v. Beusch, 596 F.2d 871 (9th Cir. 1979).

[421] Id. And see United States v. Abrams, 615 F.2d 541, at 543 (1st Cir. 1980).

[422] TAMURA, supra note 415, at 596～597.

２つの問題点に対応し，次のように２段階令状論を構築してきたのである。

A. 第１段階の令状

Winick は，前記の混雑文書ルールを認めた TAMURA 判決を根拠に，警察官は，コンピュータの中にある関連性のあるドキュメントと関連性のないドキュメントを区別することができない場合には，これらのドキュメントを選別(捜索)するために，治安判事の許可を受けて，コンピュータ全体あるいはすべてのドキュメントを占有することができるとする[423]。

これは，Winick が提案した２段階令状論の第１段階となる「選別のための差押え」であって，日本の議論に照らして言い換えれば，「蓋然性による差押え」に類似するもののように見えるが，こうした選別のための差押えの実質と日本の蓋然性による差押えのそれとは全く異なるものである。すなわち，蓋然性による差押えとは，あくまで，通常の差押令状の執行の一方法にすぎず，それ自体が独立した令状の種類ではないのに対して，Winick が提案する選別のための差押えとは，令状の執行という次元を超えて，１つの独立した令状の種類とされる。

そして，Winick によると，選別のための差押えという段階の重点は，関連性のある記録と関連性のない記録が混在しているため，現場で選別することができないと予想される場合，警察が，関連性のある記録を選出しそれについてのみさらに詳しく調べるために，その中に関連性のある情報が存在する蓋然性があるすべての記録に対する一括した占有取得を目的とする令状を，あらかじめ治安判事に請求することができるという点にある[424]。

次に検討すべきは，選別のための差押令状には，普通の差押令状と比べていかなる異なる要件が含まれているかである。この点の詳細は，以下の通りである。

(A)関連性要件について

①合理性原則と蓋然性

Winick によると，正当な理由(台湾と日本でいう関連性要件を意味する。以下では，台日米比較の便宜上，アメリカ法でいう「正当な理由」をも「関連性」と称する)は不要であり，関連性のあるデータが存在する蓋然性があれば十分であるとされる[425]。

このように，第１段階の選別のための差押令状には関連性を必要とせず蓋然性だけで足りるとすることが修正４条に反しないといえる理由は，前述した，修正４条の第１原則である合理性原則に求められる。

まず，修正４条の令状原則によれば，被疑事実と関連性を有するものしか差し押さえることができないとされるが，デジタルデータの場合には，それぞれをクリックしてみないと中身を知ることができないという特徴があるため，従来の令状原則に固執することは不

[423] Id. And see Winick, at 105.
[424] Winick, at 105.
[425] Id., at 104～106.

合理であるとされる。というのも，デジタルデータの場合にはサイズなどの物理的な特徴がなく，事前に中身を予知することもできない以上，コンピュータに対する選別のための差押えの場合においては，捜索・差押えの対象とするデジタルデータと被疑事実との関連性の確認を求めない方が合理的といえるからである。

もっとも，合理性があるからといって，令状原則を守らなくてもよいというわけではなく，修正４条の実質的な保護の程度が下げられてはならない。この点，Winick によると，警察が，選別のための差押令状により適法に一括して差し押さえたコンピュータデータの内容を捜索する際には，あらかじめ，治安判事から，当該捜索が関連性のあるドキュメントにしか及ばないことを担保することができる，「第２段階の令状」(second warrant)を得ることが前提条件となり[426]，治安判事は，一般的・探索的な捜索を避けるために，条件を付すことによって捜索の範囲を制限しなければならないとされる[427]。この意味で，修正４条の実質的な保護の程度が維持されていると評価することができよう。

こうして，第１段階である選別のための差押令状の発付には，関連性という要件は不要であるが，その後に，蓋然性により適法に差し押さえたコンピュータの中身を確認(捜索)するには，確認(捜索)の範囲を制限する別個の第２段階の令状が必要とされるから，全体として修正４条による従来の保護の程度を下げることはないので，合理性原則によれば，修正４条に反しないということができる。

②従来の差押えと蓋然性による差押えの比較

以上を確認すると，日米の異同は，以下の【表２】で示すものになる。

【表２】

アメリカ	第１段階	第２段階	修正４条の保護の程度
ROSS 判決	従来の差押え↓ 関連性を確認した上で自動車を合法的に占有した。	占有した自動車の内部を捜索するために別個の令状は不要である。	
規制要素	関連性の確認→厳格	「場所・サイズ」基準→柔軟	厳格＋柔軟
	蓋然性の確認→柔軟	別個の令状→厳格	柔軟＋厳格
Winick	蓋然性による差押え↓ 関連性を確認せずに，電磁的記録媒体を占有できる。	占有した電磁的記録媒体の内部を捜索するために別個の「第２段階の令状」が必要である。	
日本	差押え段階	内容検視段階	憲法 35 条の保護の程度
	従来の差押え	占有した物の中身を確認するために別個の令状は不要である。	厳格＋柔軟
	蓋然性による差押え		柔軟＋柔軟

[426] Id., at 107.

[427] Id., at 107～108.

表２の灰色の部分で示されているように，Winick の見解により，関連性を確認せずに行われる蓋然性による差押えを認めても，修正４条の実質的な保護の程度を下げることはないといえよう。これに対して，日本においては，第１段階・第２段階という区分をしないため，右下の「憲法 35 条の保護の程度」欄の部分で示されているように，蓋然性による差押えの保護程度は，明らかに，従来の関連性による差押えのそれよりも低いものであることがわかろう。

③蓋然性の判断基準について

Winick によれば，蓋然性の判断の基準は，従来のように，「合理的な一般人基準」によらなければならないわけでなく，「合理的な警察官基準」による判断で十分だとされる[428]。ここでいう「合理的な一般人基準」とは，差押え当時に存在していた客観的な根拠に基づき，理性を持った一般人ならば誰でも蓋然性が存在すると思われるという程度を指す[429]。他方で，「合理的な警察官基準」とは，差押え当時に存在していた客観的な根拠に照らして，警察官が，その仕事上得られた経験，訓練，専攻ないし当該分野に関する知識――例えば，外国人犯罪や麻薬密輸事件など――により判断すれば，蓋然性が存在すると思料される程度を指す[430]。

これに対して，日本においては，判例・通説は，「警察官基準」を採用してきた[431]。それゆえ，日本の場合には，電磁的記録媒体に対する蓋然性による差押えの場面であるかどうかを問わず，また蓋然性や関連性ないし特定性などの要件とも関係なく，「警察官基準」がそのまま適用されることになる。

この点，台湾では，通説・実務の見解は，前述した日本の状況と同様である[432]。

(B)特定性要件

Winick によれば，令状の特定性要件も不要であるとされる。Winick は，その理由を特に論じていないが，TAMURA 判決の意見を引用した Winick にとっては当然の帰結といえるだろう。というのも，令状主義の合理性原則によれば，修正４条による従来の保護の程度を全体として下げることがないかぎり，令状主義の個別の要件としての特定性も，関連性要件と同様に，柔軟に調整されうるものだからである。

---

428 Id., at108.

429 Brinegar v. United states, 338 U.S. 160(1994)；Maryland v. Pringle, 540 U.S. 366(2003)；Carmen, at 67～68；Hall, at 681～682.

430 Id. And see United States v. Ortiz, 422 U.S. 891(1975).

431 最判昭和 33 年 7 月 29 日刑集 12 巻 12 号 2776 頁，横井・刑訴裁判例ノート(1)248 頁(同 272 頁，同・押収・捜索 44 頁，同・令状の記載 77 頁，栗田・最判解(昭和 33 年度)561 頁をも参照)。ただ，警察官基準に反対し，一般人(合理人／通常人)基準こそ妥当であるとする少数説がある(熊本・令状の記載 50 頁。東京地決昭和 33 年 6 月 12 日判例時報 152 号 20 頁，中武＝高橋・捜査法 171 頁等をも参照)。

432 林鈺雄・捜索扣押 206～207 頁，黄朝義・刑訴三版 258 頁，黄翰義・緊急捜索 157 頁参照。

(C)「現場での選別困難ないし不能」についての疎明義務

そのうえで，Winick は，選別のための差押令状を発付するには，現場での選別が困難ないし不可能であると予想されること及びその根拠を疎明することが必要であるとしている[433]。すなわち，Winick によれば，第１段階の選別のための差押令状の発付を請求する際に，捜査官は，関連性のある記録と関連性のない記録とを現場で選別しがたい，あるいはそれができないことが予想される旨及びその予想を支える根拠を，令状を発付する治安判事に疎明しなければならないということである。

具体的にどのような場合が，「現場での選別困難ないし不能」にあたるのかについて，Winick は特に言及していないが，理論的には，以下の４つの可能性をあげることができる。

すなわち，①客観的不能（例えば，ＩＴセキュリティが解除できない場合），②主観的不能（例えば，捜査官の誤信や誤判断で不能と思い込んだ場合），③執行効率上の困難（例えば，現場での確認作業に膨大な時間を要するなどの事情がある場合），④捜査目的遂行上の困難（例えば，現場で確認作業を行うと記録された情報を損壊される危険がある場合）である。Winick の理論から推論すれば，①～④のうちのいずれかがあれば十分であろうと思われる。

(D)補充性要件

選別のための差押令状の最後の要件として，Winick は，「補充性」を挙げている[434]。補充性とは，他の有効かつより侵害性が低い捜査手段が存在しない場合に限って選別のための差押令状を発付することができることを意味する。

具体的には，捜査官にとっては現場で選別困難ないし不能であるが，仮に被処分者にコンピュータを操作してもらえれば，それによって選別困難や不能の問題を回避できるという事例で，被疑者と全く関係のない第三者である被処分者からあらかじめ捜査に協力したいという申出がなされていたにもかかわらず，捜査官が，合理的な理由もなく，協力の申出を無視し，選別のための差押えを行うために第１段階令状を請求するというような場合が，ここでいう補充性要件を満たさない一例として考えられる。

B. 第２段階の令状

第１段階の選別のための差押えを認めるにはその後の捜索段階を規制しなければならないとする Winick は，捜索のためには第２段階の令状を得ることが必要であるとし，かかる令状の発付要件として，①証拠存在の蓋然性，及び②関連性のある記録を選別するための執行方式の提案，の２つを挙げている。具体的には，①は，警察が，標的とする記録が捜索の範囲内で発見できると考えられる「合理的な理由」を提示しなければならないことを，②は，関連性のある記録と関連性のない記録とを選別することができる捜索の「執行方式」

[433] Winick, at 105～106.

[434] Id.

を提案しなければならないことを意味し，この２つの要件のいずれかが欠けると第２段階の令状を発付することができないとされる[435]。

このうち，②の要件は，従来の判例の立場と完全に異なる，Winick の学説の最も特徴的な箇所であり，２段階令状論の核心をなすものであると思われる。その理由は次の通りである。

まず，アメリカにおいても，日本と同様に，従来は，執行方式は現場の状況によって決めなければならない場合が多いので，それを令状で事前に限定しておくと捜査の実効性を害するおそれがあるため，現場で執行にあたる警察官の裁量判断に任せるべき事項であるとされてきた[436]。

しかし，前述した通り，コンピュータに対する選別のための差押えを行う場合には，差し押さえる際に関連性を確認していないから，その後に，差し押さえたコンピュータの内容を捜索することには何らの制約も受けないとすれば，捜査への規制を失ってしまう。この問題点に対応するため，従来は警察官の裁量事項とされてきた「執行方式」を工夫すべきという Winick が提案した②の要件は，非常に斬新な発想であると評することができると思われる。

他方，Winick によると，第１段階の選別のための差押令状が修正４条に反しないといえるためには，その後，第２段階の令状，すなわち，選別のための差押え後の捜索を規制するための令状が必須の条件であるとされている。この意味で，「執行方式」の工夫という点に特徴付けられている第２段階の令状という提案こそが，２段階令状論のもっとも核心的な部分であるといえよう。

(4)台湾への示唆

A. ２段階令状論の有益性

このように，一部の裁判例でも受け入れられている，２段階令状論という Winick の提案からも，蓋然性による差押えを行う際に関連性を確認せず，その後の内容の確認にも令状が不要であるとすることにより捜査への規制を失ってしまうという台湾の現状は適切でないという評価が支持されると思われる。それゆえ，この２段階令状論を立法論としてある程度採り入れ，蓋然性による差押えに対する規制を設けることが妥当であろう。

もっとも，前述した通り，台湾においては，蓋然性による差押えは，単に差押えの執行方法の一態様として扱われてきたのに対して，Winick の提案によれば，それは，通常の差押えと異なる種類の「選別のための差押え」令状として捉えられており，通常の差押えの場合と異なる令状発付の要件が設けられている。したがって，立法論的には，蓋然性により差し押さえた後の段階を別個の令状により規制する必要があるのにとどまらず，蓋然性による差押えという段階自体も令状制度をもって規制すべきであるということになる。

---

[435] Winick, at 108.

[436] DALIA v. UNITED STATES, 441 U.S. 238(1979).

B. 情報の膨大性と混雑性

前述したように，蓋然性による差押えは，電磁的記録媒体に対する差押えの場面に特有の問題ではない。それにもかかわらず，伝統的な事案においてなされる蓋然性による差押えは，問題視されていない[437]。例えば，現場で５本の包丁が発見されたが，その５本の中から令状に記載された「凶器である１本の包丁」を選出するために鑑定を必要とするというような事案では，従来の議論によれば，１本の凶器である包丁と４本の凶器でない包丁を一括して差し押さえることができるとされる。

この点，日本では，電磁的記録媒体ないし郵便物を対象とするような場合には，蓋然性による差押えは，被疑事実と関連性のあるデータを含まない電磁的記録媒体ないし被疑事実と関係ない郵便物まで差し押さえられてしまう点が問題視されてきた。これに対して，台湾では，かかる問題があまり重視されていないが，学説上は，大容量の媒体に対して蓋然性による差押えを行う場合には，被疑事実と関係ない郵便物まで差し押さえられてしまうため，プライバシー権への過度の侵害に繋がりかねないとしつつも，伝統的な事案においても，実際には蓋然性による差押えが行われてきた点をも１つの正当化理由として，電磁的記録媒体に対する蓋然性による差押えの正当性を認めることができるという主張が一部で現れてきた。

この点，Winick によれば，その差異は，コンピュータにおいて保存している情報の量の膨大性及びその質の混雑性という点に求められる[438]。具体的には，まず，現場で発見された複数の包丁の中に凶器である包丁があるという蓋然性が存在する限り，それらを一括して差し押さえたとしても，その後，差し押さえた包丁の中身を確認することにより開示されうる情報の量は極めて限定された範囲のものでしかないと同時に，その質もかなり限られている。これに対して，コンピュータの場合であるならば，開示されうる情報は極めて大量であるばかりでなく，その質も極めて混雑的なものである。

つまり，蓋然性により差し押さえられた包丁の内容を確認する段階でさらに別個の令状により保護すべきとする必要性が極めて低いばかりでなく，このような別個の令状を要求すると，かえって無駄な手続になってしまい，捜査に余計な支障を招くと同時に，刑事司法資源の浪費に繋がるのに対して，コンピュータの場合には，その後の内容の確認は別個の令状による規制の必要性が極めて高いものであると説明されよう。

しかし，情報の膨大性ないし混雑性という特徴は，大量の書類の捜索・差押えなどの場合にも同様にあてはまる一方，電磁的記録媒体だからといって必ずしも大容量ないし混雑のものとは限らないのであるから，特別コンピュータ令状という Winick の用語自体が適切でない。コンピュータだからといって必ずしも２段階の令状により保護すべきであるわけでなく，反対に，コンピュータ以外の場合であっても，２段階の令状により保護すべき場合があるはずである。つまり，ここでの終局的な判断基準は，コンピュータであるかどう

[437] 李・電磁記録 1079～1080 頁。石毛・令状問答 238 頁以下(とりわけ，247 頁)，三堀・犯罪捜査 144，147 頁をも参照。
[438] Winick, at 89.

かではなく，情報の膨大性ないし混雑性という特徴が存在するかどうかにこそあるのである。

３．あるべき立法について

以上をもとに，情報の差押えという制度のあるべき内容を具体化するにあたって取り上げるべき問題点としては，次の３つのものがあげられる。

第１に，「関連性＝蓋然性」という構造は，一般的・探索的差押え禁止原則に反するものであるのかである。というのも，令状主義が，中華民国憲法上の原則であるかどうかについては争いがあるが，同法 23 条の最小化原則から導かれた一般的・探索的捜索・差押え禁止原則が憲法上の要求である点には異論がないし，また，日本刑訴法 100 条 1 項及び台湾刑訴法 135 条 1 項 2 款の合憲性に関わる問題を検討したところで見た通り，蓋然性による差押えが，証拠物又は没収すべき物にあたらないものを，無条件で差し押さえることができるとするものであるとすれば，違憲の一般的・探索的差押えに当たる可能性を否定できないからである。

第２に，この合憲性の問題がクリアされた場合には，次に，「関連性＝蓋然性」という構造を前提にした「最小化原則による実質的保障」が基盤となる情報の差押えの制度と現行法の差押えの制度との関係を明らかにしておく必要がある。具体的には，①「関連性＝蓋然性」という構造を前提にした「最小化原則による実質的保障」という本稿の理論を，現行台湾刑訴法 133 条 1 項の文言に採り入れることは可能か，及び②情報の差押えという制度を新しく創り出すという選択肢のほかに，個別の特別な立法による対応の可能性もあるのに，なぜ後者が選択されないのか，という２つの点が問題となる。

その上で，第３の問題は，関連性(蓋然性)要件との関係で，情報の差押えという制度がどうあるべきかである。

(1)合憲性の問題

本稿が提案した「関連性＝蓋然性」という構造は，中華民国憲法 23 条(最小化原則)から導かれた一般的・探索的差押え禁止原則に反するものではないと考える。その理由は，以下の通りである。

まず，「関連性＝蓋然性」という構造は，最小化原則による実質的保障を実現することを終局的な目的とするものであり，後述する内在的制約が加えられているから，中華民国憲法 23 条の最小化原則から導かれた一般的・探索的差押え禁止原則に反することはない。この点を説明するためには，まず，ここまでの検討を確認しておく必要がある。

第１に，アメリカにおいては，普通の物件に対する差押えの場合であるならば，すでに適法に占有した物の内容を確認するために別個の令状は不要であるという点は台湾の理解と異ならないが，蓋然性による差押えの場合においては，それが修正４条の一般令状禁止原則に反しないといえるためには，蓋然性により差し押さえた後の捜索の範囲を別個の令

状により規制しなければならないという見解が現在は有力となっている。

第２に，台湾では，通常の差押えであれ蓋然性による差押えであれ，すでに適法に占有した物の内容を確認するために別個の令状は不要であるという原則はそのまま適用されている。

第３に，台湾の理解のもとで行われる蓋然性による差押えは，何らの規制もなされていないため，こうした場面での保護の程度は，明らかに，関連性を確認したうえで行われる従来の伝統的な家宅捜索における差押えの場面で行われるそれよりも低くなるものである。

以上を踏まえて，本稿は，蓋然性による差押えを正当化するための根拠につき，「関連性＝蓋然性」という構造を提案した。かかる構造に基づく蓋然性による差押えが，一般的・探索的差押え禁止原則に反しないものであるといえるためには，蓋然性により差し押さえた後の捜索の範囲を別個の令状により規制する必要があり，これによって蓋然性による差押えにおける低下した保障の水準を回復させなければならない。

そして，「関連性＝蓋然性」という構造をもって，蓋然性による差押えが合憲であるといえるためには，中華民国憲法 23 条の最小化原則から導かれた一般的・探索的差押え禁止原則の一部を構成する関連性要件によって基本権に対して提供された保護の内容ないし程度が縮減することはないという保障を，法により実質的に担保しなければならない。具体的には， Winick の提案した第２段階の令状による規制が，その一例として考えられる。

しかし，本稿は Winick の提案を参考としつつも，それとは，次の２点において差異がある。第１に，本稿も，蓋然性による差押えの後段階の規制を必要としているが，その根拠は，中華民国憲法 23 条の最小化原則から導かれた「法による実質的な保障を回復できる内在的制約」という点に求められるのに対して，Winick が打ち出した第２段階の令状の提案は，修正４条の第１原則とされるいわゆる「合理性原則」から導かれているものである。第２に，Winick が打ち出した第２段階の令状は，専ら，コンピュータデータを選別するための差押えという場面にのみ対応するものであるとされるのに対して，本稿の考え方は，コンピュータデータが対象である場面に限られないのである。というのも，ここまでの検討により示されたとおり，蓋然性による差押えとは，コンピュータデータを対象とする場合に特有な問題点ではないからである。

(2)現行法との関係

「関連性＝蓋然性」という構造を前提に，中華民国憲法 23 条の最小化原則から導かれた差押えの関連性要件を再定義すると，それは，「差し押さえるべき物ないし情報と被疑事実との間に立証関係ないし準立証関係が存在する蓋然性」ということになる。ここでいう「立証関係」とは，差し押さえるべき対象が「証拠物」や「証拠たる情報」であることを意味する。「準立証関係」とは，差し押さえるべき物ないし情報それ自体は，証拠にはならないが，証拠物ないし証拠たる情報を取得するために必要不可欠な存在であることである。具体的にいえば，その中に証拠である情報が存在する蓋然性がある媒体自体は，証拠

物ではないが，現場で当該媒体から証拠である情報を取り出すことができないため，証拠である情報を取得するためにとりあえず媒体を差し押さえることが必要になる。この意味で，かかる媒体は，被疑事実との間に準立証関係が存在する蓋然性があるものといえる。

問題は，このような関連性の再定義は，果たして現行の台湾刑訴法 133 条 1 項の「証拠となる物あるいは没収できる物は，それを差し押さえることができる。」という文言に適合するものなのかである。以下では，この点についての更なる検討を行う。

まず，同条でいう関連性要件の解釈には，２つの方法がある。１つは，「関連性を確認する方法」に照準を合わせた解釈である。この場合には，関連性とは，「処分の対象の中身を見ておくこと」(すなわち，関連性を確認する方法)を，その必要な前提とする。言い換えれば，関連性を確認する方法も，関連性要件の内実をなす一部になる。

そうすると，蓋然性による差押えの場合は，捜査官が媒体の中身を確認しておらず，必要な前提を満たしていないため，かかる媒体を，関連性があるものとはいえないという帰結になる。これを同条の文言に当てはめて言い換えれば，媒体の中身を確認していない以上，「証拠物又は没収すべき物と思料するもの」とはいえないということになろう。

このように，「関連性を確認する方法」という点も関連性要件の一内容として採り入れ，135 条 1 項の文言を解釈すると，ある媒体が証拠物になりうる蓋然性があるという推測・推定(確認されていない関連性)に基づく差押えは認められないという帰結になる。言い換えれば，135 条 1 項でいう差押えは，「立証関係があると確認された関連性」による差押えに限られ，「準立証関係があると推認された関連性」(蓋然性)による差押えは認められていないことになる。

しかし，このような解釈によると，情報の膨大性ないし混雑性という特徴をもたない，包丁や麻薬などを対象とした蓋然性による差押えも認められないという「規制過剰」の結果になってしまうので，適切とは言い難い。これに対し，もう１つの解釈の方法は，関連性要件を理解するには「関連性を確認する方法」を考慮する必要はないというものである。すなわち，関連性要件を満たしているといえるために，中身を見た上で関連性を確認しておくことを必要としない。このように解すると，ある媒体が証拠物になりうる蓋然性があると推測されるという「蓋然性による差押え」，言い換えれば「(確認されておらず)推認された関連性」の場合も，「証拠となる物又は没収できる物」という 133 条 1 項の文言範囲内に包摂されることになる。

しかし，こうした解釈をとると，情報の膨大性ないし混雑性という特徴をもつ，蓋然性により差し押さえた後の捜索について更なる規制を行うべき場合すら，現行法の 133 条 1 項により差押えができるという「規制不能」の結果になってしまうので，適切とは言い難いのである。

(3)個別的な立法の問題点

以上の通り，133 条 1 項の文言の２つの解釈は，規制過剰か規制不能の結果を生じさせる

ものであり，これを解消しようとすれば，新しい立法によるしかない。

もっとも，新しい立法にも様々なパターンがある。まず考えられるのは，例外規定の新設といった個別立法によるアプローチである。この選択肢にも，さらに次の２つの可能性がある。

その１つは，前述した第１の解釈を前提とした上で，133 条１項の特別の定めとして例外規定を設けることにより規制過剰の問題に対応するというものである。

もう１つは，それと逆に，前述した第２の解釈をとった上で，133 条１項の規定を厳しくする特別な定めを設けることにより，規制不能の問題を解決するというものである。

しかし，この２つの方策は，いずれも，妥当ではないと思われる。というのも，蓋然性による差押えは，電磁的記録に特有の問題ではないし，また，あらゆる電磁的記録媒体において情報の膨大性ないし混雑性という特徴が含まれるわけではない一方で，電磁的記録媒体でないからといって，必ず情報の膨大性ないし混雑性という特徴を持たないわけでもないから，個別立法という方策を採用すると，宿命的に，類型化の困難に遭遇すると同時に，あるべき例外規定を設けきれないという問題を抱えてしまうことになるからである。

それゆえ，あるべき立法としては，やはり，情報の差押えという制度の新設が挙げられよう。具体的には，まず，現行法の 133 条 1 項の文言において，明示的に，前述した関連性の新定義を取り入れたうえで，蓋然性による差押えという段階への令状による規制，及びその後の捜索の範囲を画定するための令状による規制を用意すべきである。

(4)最小化原則による実質的保障の実現

以上をもとに，以下では，「関連性＝蓋然性」という構造に基づく「最小化原則による実質的保障」を基盤とした情報の差押えという新たな制度を具体化する。そのためにまずは，この新制度の核心となる「最小化原則」の意味を明らかにしておく必要がある。

A. 最小化原則の意味

本稿の提案した「関連性＝蓋然性」という構造の基盤(または前提)となる最小化原則は，憲法上の原則であり，行政法規としての警察法において成立･発展した「警察比例の原則」[439]ないし「捜査比例の原則」[440]とは異なるものである。言い換えれば，それは，行政法における警察比例の原則ないし捜査比例の原則の次元を超えた「憲法上の原則」であって，その

[439] 須藤・比例原則 8 頁以下，石毛・令状問答 45 頁，川出・行政警察活動 76 頁，井田ほか編着・事例Ⅱ刑訴[真田]380 頁以下，平良木・捜査法 48，280 頁参照。警察比例の原則について，通説によると，それは，行政法上の原則であるとされるが，これに対して，それを，「自然法的ないし超実定法的な内在的制約的原理」と捉える見解もある(庭山＝森井編著・刑訴 100 講[渡辺]45 頁)。

[440] 警察比例の原則を，刑事手続の場面に当てはめて，「捜査比例の原則」と言い換えるものがある(三井・手続法(1)[新版]75 頁，小林充・刑訴新訂 111～112 頁，福井・刑訴講義 5 版 90 頁，田宮・刑訴(新版)64 頁，平良木・捜査法 44 頁，平良木・刑訴法Ⅰ98～99 頁)。通説として，捜査比例の原則とは，憲法上の原則でなく，行政法上の原則とされるのに対して，「憲法 31 条の要請として，捜査比例の原則(目的と手段の均衡が必要)が妥当する」とする見解がある(安富・刑訴法 38 頁)。

根拠を，通説と実務により認められたいわゆる中華民国憲法 23 条の最小化原則に求めることができる。これによって，蓋然性により差し押さえる段階自体並びにその後の(捜索)段階につき，それぞれを別個の令状により規制すべきとする本稿の提案が，憲法上の位置づけを獲得することになる。

すなわち，かりに，最小化原則を，警察比例の原則ないし捜査比例の原則の次元で理解するに止めると，これに応じた実定法的な対応も，法の制度という形――例えば，令状制度――による規制でなく，捜査機関の裁量権限に任せる――例えば，台湾の現行法上のように蓋然性による差押えを令状の一種の執行方式と位置づける――という形で処理されることとなる。これに対して，本稿の立場からすると，憲法上の原則としての最小化原則がその根拠となるものであるから，例えば蓋然性による差押えという問題を考える際に，最小化原則を忠実に実現するためにはそれを単なる「令状の執行」の問題として捉えるだけではたりず，「多段階の令状による規制」という制度を用意すべきことになるのである。

B. 規制に係るジレンマの解消

以上をもとに，前述した，台湾刑訴法 133 条 1 項の解釈論における規制過剰と規制不能というジレンマ[441]を解消するためにあるべき立法論の具体的な内容について述べる。

(A)規制過剰について

まず，規制過剰の問題に対応しようとすれば，台湾刑訴法 133 条 1 項における「証拠物」という文言を「証拠になりうる物又は情報」と修正することが考えられる。というのも，この修正は，情報を独立した処分の対象とする趣旨を表明するほかに，次の２つの意味をもつからである。第１に，これは，蓋然性による差押えを正当化するための論拠は何なのかという問題につき，「関連性＝蓋然性」という構造を採用する立法者の意思表明となる。第２に，「関連性を確認する方法」(原則的には処分の対象の中身を見ながら関連性を確認しておかなければならないことをさす)に照準を合わせて同 133 条 1 項の文言を厳格に解することにより生じうる規制過剰の問題を防ぐことができる。

(B)規制不能について

続いて，規制不能[442]の問題を解決するには，以下の３つの段階からなる法的対応が必要となる。すなわち，(ア)蓋然性による差押えの前段階（蓋然性を確認するための捜索)，(イ)蓋然性による差押え自体，(ウ)蓋然性による差押え後の段階である。そして，（イ）の段

441 規制過剰と規制不能の意味について再確認すると，規制過剰とは，「処分の対象の中身を見た上で関連性を確認すべき」という原則に照準を合わせて台湾刑訴法 133 条 1 項に要求される関連性要件を解すると，従来全く問題視されていない，包丁や麻薬などに対する蓋然性による差押えさえ認められなくなることをいう。これに対して，規制不能とは，「関連性を確認する方法」に照準を合わせず同 133 条 1 項の文言を緩やかに解すると，蓋然性により差し押さえた後の捜索について更なる規制をすべき場合すら，現行法の 99 条により差押えができるという帰結になることをいう。

442 前注参照。

階では，Winick が提案した選別のための差押令状が，（ウ）の段階では，関連性を確認するための第２段階の捜索令状が必要とされる。

そのうえで，(ア)(イ)(ウ)の関係を説明すると，次のようになる。まず，(イ)と(ウ)の関係については，(イ)を認めることの前提として，(ウ)が必須である。というのも，コンピュータなどの記録媒体を占有した後，当該媒体の内容を確認する段階に関する規制を設けることにより，対象でない情報が侵害されないように配慮することが可能となり，かつ，令状主義のいう関連性要件により提供される従来の保護程度を維持するための憲法上の比例原則における最小化の要求からも，そうすべきだからである。言葉を換えていえば，(イ)を認めながら(ウ)を設けないと，蓋然性による差押えの場面の規制程度は，中身を見たうえで関連性を確認しておくという従来の差押えの場面のそれよりもより下がることになるので，「関連性＝蓋然性」という構造の内在的制約である法による実質的な保障の要求をも満たしておらず，憲法上の最小化原則に反し違憲になるからである。

これに対して，(ア)と(イ)の関係については，憲法上の最小化原則をより一層精緻化しようとすれば，(イ)の前段階に，(ア)の規制を加えるのは妥当だと考えられる。言い換えれば，(ア)を設けないと，直ちに，(イ)の規定が最小化原則に反し違憲になるわけではなく，(ア)を設けるかどうかは立法者の裁量権の範囲内にある。なぜなら，仮に，(ア)の規制を設けないとしても，(ア)段階の(蓋然性を確認するための)捜索も「捜索」である以上，結局のところ，そこにも，(ウ)段階の(関連性を確認するための)捜索に対するのと同様の規制が及ぶことになり，「関連性＝蓋然性」という構造の内在的制約である法による実質的な保障の要求を満たすことができ，最小化原則に反しないものといえるからである。

この多段階規制を具体化するには，日本刑訴法 100 条 1 項から導かれた「郵便物に対する蓋然性を確認するための捜索禁止原則」が台湾にも参考となるが，本稿の理論からそれを敷衍すると，次の表のようになる。

【表３】

<table>
<tr><th></th><th colspan="2">(ア)蓋然性を確認するための捜索</th><th>(イ)蓋然性による差押え</th><th>(ウ)関連性を確認するための捜索</th></tr>
<tr><td>100条1項</td><td colspan="2">捜査機関による郵便物(封筒)の捜索→禁止
郵便局員によるあらゆる郵便物(封筒)の全面的な点検(捜索)→許容</td><td>△
差押えの執行の１方法：
別個の令状→不要</td><td>×</td></tr>
<tr><td rowspan="2">本稿の提案</td><td>３段階規制</td><td>捜査機関による郵便物(封筒)の捜索→禁止
郵便局員によるあらゆる郵便物(封筒)の全面的な点検(捜索)→許容
※「(捜索)計画書」の提出→不要</td><td>○
独立した差押えの処分：
別個の令状→必要
↓
蓋然性による差押令状</td><td>○
独立した捜索の処分：
別個の令状→必要
↓
関連性を確認するための捜索令状
↑
令状発付の請求:(関連性を確認するための捜索)計画書の提出→必要</td></tr>
<tr><td>２段階規制</td><td>蓋然性を確認したうえで蓋然性による差押えを行う。
すなわち(ア)段階と(イ)段階が実質的に融合すること。
捜査機関による郵便物(封筒)の捜索→許容
※但し，蓋然性による差押令状の発付を請求する際に，蓋然性を確認するための捜索の範囲を最小化する手段を明記する「(蓋然性を確認するための捜索)計画書」を裁判官に提出しなければならない。
(捜査機関の補助としての)郵便局員によるあらゆる郵便物(封筒)の全面点検(捜索)→禁止</td><td>○
独立した捜索の処分：
別個の令状→必要
↓
関連性を確認するための捜索令状
↑
令状発付の請求:(関連性を確認するための捜索)計画書の提出→必要</td></tr>
</table>

前述したように通り，立法者は，３段階規制のパターンにするか，２段階規制のパターンにするかの裁量権をもつ。そして，２段階規制のパターンが選択される場合，(ア)段階には，３段階規制のパターンのような特別な規制(捜査機関による郵便物(封筒)の捜索の禁止)が加えられていないが，しかし，その段階が何らの規制も受けないわけではなく，「(捜索)計画書」による規制が適用されることになる。つまり，「(捜索)計画書」による規制は，政府によるあらゆる態様の捜索行為に適用可能な一般規定であり，(ウ)段階の捜索の態様にのみ適用されるわけではないが，特別な規定が設けられる場合，その適用順位は劣後になる。また，この２つのパターンを比較すると，両者の規制要件はそれぞれ異なるから，どちらがより厳しいかは一律に言いきれない。

以上を踏まえて，以下では，Winick の選別のための差押令状を参考に，(イ)の蓋然性による差押えの段階の規制について述べる[443]。

①疎明の義務と令状の明示

立法により，「捜査機関は，現場での選別が困難ないし不能であると予想され，選別のために，とりあえず，関連性を確認せずに膨大な若しくは混在する情報又はこのような情報を含む蓋然性のある媒体を一括して確保しておく必要があると思料されるときには，令状の発付を請求する際に，その旨及び具体的な根拠を疎明しなければならない。裁判官が令状を発付するときは，当該疎明の要旨を令状に明記すべきである」という規定を設ける

[443] (ア)(ウ)は捜索の問題であるから，それらの詳細は第２章において論じる。

べきである。

この規定により，包丁のような物件を前掲の規制の範囲外から排除すると同時に，大量書類ないし電磁的記録媒体のような物件であれば，この規制に服させることができる。これによって，前述した規制不能と規制過剰のジレンマが解消されよう。

また，ここでいう「現場での選別困難ないし不能」という命題は，前述した，客観的不能，主観的不能，執行効率上の困難，捜査目的遂行上の困難，の４つの可能性を包摂しているものであるが，許可するかどうかは，令状発付裁判官の裁量により決められるのである。

最後に，現場での選別困難ないし不能などの事情を予見できない場合も当然ありうるが，その場合は，事前に疎明がなされていない以上，蓋然性による差押えは認められないという帰結になる[444]。

②最終手段性とその他の必要な規制

関連性を確認せずに膨大な若しくは混在する情報又はこのような情報を含む蓋然性のある媒体を一括して確保しておくという捜査手法は，情報の終局的処分権に対する重大な侵害であるのみならず，媒体をも同時に取得する必要がある場合には，媒体の財産権も侵害することになる。この点に鑑み，法に，「このような捜査手法の使用は，捜査目的を遂行するために必要不可欠なものであり，かつ，その他のより緩やかな代替手段がない場合に限る」旨を明示すべきである。

そのうえで，前述した通り，(イ)蓋然性による差押えという段階と(ウ)関連性を確認するための第２段階令状という段階とは密接不可分割の関係があるため，次の２つの条項を用意する必要がある

第１は，「条件の付加による限定」条項である。これは，「必要があれば，関連性を確認せずに膨大な若しくは混在する情報若しくはこのような情報を含む蓋然性のある媒体を一括して確保しておく範囲を最小化するために適切な条件の記載を付することができる」旨を定めるものである。

第２は，「捜査(選別)計画の提案による限定」条項である。これは，「必要があれば，取得しようとする証拠になりうる物又は情報のうち，証拠物又は証拠である情報とそうでない物又は情報とを選別するために予定される方策につき，捜査機関に疎明させることができる」旨を定めるものである。

Ⅲ.「特定性」要件について

以上の通り，差押えという制度における「関連性」要件を検討した。次に，「特定性」要件を論じたい。ここでいう特定性は，「差し押さえるべき対象とそうでない対象とを区

444 この場合への立法論的な対応としては，本稿の検討課題である令状制度でなく，いわば緊急処分などの制度の新設があげられる。

別することができる程度に，差し押さえるべき物ないし情報を令状に明示すること」と定義してよかろう。これを前提に，特定性との関係で検討すべき問題点を洗い出しておこう。

１．有体物と特定性要件

無体のデータは，有体物のように，物理的に支配・管理することが不可能である。そこから，これまでの検討は，無体の情報を特定することは困難であるという点に焦点を当ててきたが，実際には，この問題は，電磁的記録の場面にのみ存在するものではない。例えば，第２章において後述するように，傍受の対象となる無体の通信会話を如何に特定することができるのかが難問として指摘されてきた。また，有体物を対象とする伝統的な家宅捜索・差押えの場面においても同様に，特定困難という問題が生じうる。

つまり，台湾においては，通説によると，「捜査段階の証拠は手続の発展に従い徐々に収集していくものであるので，この段階においては個別の物件の特定を要求することは確かに困難があるから，その関連する事項を具体的に表明すれば十分である。国家の刑罰権の実現及び個人の利権保障の観点から，それを適当に調和し，その特定の程度が判定される。」[445]。他方で，実務上も，これまでは慣行として，捜索令状における「差し押えるべき物」の記載については，抽象的かつ概括的に，「犯罪と関係がある証拠」「○○犯罪(または○○捜査事件)と関係する証拠」と記載されてきただけである[446]。

これに対して，台湾の最高裁判所は，2008 年に，著作権法違反事件で，「差し押さえるべき物」欄に，単に「商標法，著作権法の違反に関する証拠物」と記載されただけである点を，「概括捜索令状禁止原則」に違反するおそれがあるものであると指摘した[447]。この事件では，上訴人が，この点に対して原審で繰り返して争ったにもかかわらず，原判決はそれを深く探求することもなく，詳細な説明をせずに，直ちに「捜索を執行するまえには具体的な差し押さえるべきものを予知することがありえない」と述べて，「かかる概括的な記載を違法なものであるとは言い難い」としたのに対し，それは「理由不備の違法に属するものである」と判断したのである[448]。その具体的な論拠は，次の通りである。

「[2001 年の法改正以前にも]刑事訴訟法 128 条 2 項において，明文で捜索令状の法定の必要な記載事項を列挙しており，[2001 年の]修正後は捜索令状の発付につき裁判官留保原則を採用するとともに，……捜索令状における記載すべき事項を新設している。これは，捜索令状において記載すべき事項にかかる規範であり，すなわち，いわゆる『概括捜索令状禁止原則』そのものである。そのうち，とりわけ，捜索令状上の『差し押さえるべき物』及び『捜索すべき場所』は，いずれも，事前に合理的かつ具体的に特定・明示しておかなければならず，これをもって，捜索の対象と範囲を明確に画定する要求を満たすといえると同時に，捜索差押えが濫用され一般的捜索の禁止原則に違反することを防ぐ。そこで，

---

445 林永謀・刑訴釋論(上)452 頁。同解として，范・過度扣押 6～7 頁。

446 洪・捜索扣押之實務研究 126 頁。

447 最高法院 97 年台上字 1509 號判決。陳瑞仁・新法捜索扣押 61～62 頁をも参照。

448 同前注。

捜索令状における記載すべき事項が，漠然としたものにすぎないか，あるいは，概括的な記載にすぎない場合には，それは合理・明確性の要求に反するものである。」[449]

差し押さえるべき物を明示・特定しておかなければならないという定めは，2001 年法改正以前にもすでに現行法上は存在していたものであるが，当時は，検察官も令状を発付する権限をもっていたため，「概括的な記載」が正当と認められてきたのに対して，最高裁は，2001 年に刑訴法に導入された令状主義を，「裁判官留保による概括(捜索)令状禁止原則」と理解したうえで[450]，「概括的な記載」がかかる原則に違反するものであるから現行法上は認められないと判断したのである。 つまり，裁判官留保による概括令状禁止原則のいう特定性要件の認定基準は，検察官による令状のいう特定性要件のそれよりも高くなるものである。

それでは，概括的な記載が裁判官留保による概括令状禁止原則に反するものでありそれが認められないとして，如何なる記載であれば認められるのか。この点，最高裁は，例として，「本件でいうと，その差し押さえるべき物を，『著作権を侵害することにかかわるCD，CDバーナー，コンピュータ，ラベル，説明書，包装などの証拠物』と記載することができる」としている。

しかし，裁判官留保による概括令状禁止原則が現行法上採用されているからといって，「〇〇事件にかかわる証拠物」というような概括的な記載が，現行法上はおよそ認められないものであるとしなければならないかについては，なお再検討する余地があるように思われる。

この点，日本の先行研究においてすでに指摘されてきたとおり，住居等の捜索・差押えは「事件の内容も固まっておらず，時には犯人さえ判らない段階において，強制捜査の第一歩として必要となることが多いのであるから，その時までに差押え物件を個別的に特定することは，多くの場合に極めて困難であり，それが不可能な場合さえしばしば生じるであろう。……捜査段階における差押えの本質からくる要請によって，憲法の規定をもう少し柔軟に，ただし一そう合理的に解釈する必要が生じてくる。」[451]

ここに示されている通り，特に捜査の初期段階では，流動的かつ不明確な要素が多く，処分の対象を特定することがそもそも容易ではない。日本の実務でも，一般に「その他本件に関係ありと思料せられる一切の文書及び物件」という差押え目的物についての令状の記載の慣行が存在しており[452]，そしてこの慣行は，すでに最決昭和 33 年 7 月 29 日刑集 12

---

[449] 同前注。

[450] 台湾では，独立した差押状がないため，用語上は，概括捜索令状禁止原則となるが，その中身は当然，捜索・差押えの両面とも含まれるものであるから，これからの検討では概括令状禁止原則と称する。

[451] 鈴木 74 頁。同旨として，岩崎 38 頁，秋山・目的物の特定 236 頁，令状事務(1 版)336 頁，三井・手続法(1)[新版]37 頁なども参照。

[452] 大政 70～71 頁参照。東京地決昭和 33 年 6 月 13 日，札幌地決昭和 38 年 5 月 17 日下級裁判所刑事裁判例集 5 巻 6 号 621 頁，東京高判昭和 40 年 10 月 29 日判例時報 430 号 35 頁，令状事務(1 版)337 頁をも参照。これに対して，この慣行を認めなかったように見える裁判例としては，東京高裁昭和 47 年 10 月 13 日判例時報 703 号 108 頁，名古屋地裁昭和 54 年 3 月 30 日判例タイムズ 389 号 157 頁があげられる。

巻 12 号 2776 頁(以下，「昭和 33 年決定」という)により承認されている。

このように考えると，台湾の最高裁のいう裁判官留保による概括令状禁止原則における特定性要件の認定基準をより柔軟に解釈する余地があるように思われる。 というのも，前にも言及したとおり，日本では，一般令状禁止原則の根拠については，日本国憲法 35 条という明文の定めがあるのに対して，台湾の最高裁のいう裁判官留保による概括令状禁止原則については，中華民国憲法上はそれについての明文が存在していないため，学説上は，かかる原則の導入は憲法上の要求でなく，立法政策にすぎないと解するのが多数説だからである。

また，実際にも，台湾の最高裁は，2011 年に，児童及少年性交易防制條例に違反する事件で，「刑事訴訟法 128 条 2 項は，明文で捜索令状の法定記載事項を列挙しており，それは，捜索令状における記載すべき事項を規範するものであり，すなわち，学説上のいう『概括捜索令状禁止原則』そのものである。その第 2 款のいう『差し押さえるべき物』については，それを事前に，合理・具体的に特定・明示しなければならず，これによっては，捜索の対象と範囲を明確に画定する要求を満たさせ，捜索・差押えが濫用され一般的(または魚釣り式)捜索の禁止原則に反することを防ぐことができる。ここでいう差し押さえるべき物とは，同法 133 条 1 項の規定に照らして，証拠となる物あるいは没収できる物を指す。合理・明確性の要求を満たすためには捜索令状における『差し押さえるべき物』をいかに記載すべきかについては，外国の実務を参考にすると，日本最高裁判所昭和 33 年 7 月 29 日裁定によれば，偽造文書の事件で，差し押さえるべき物を，『会議議事録，闘争日誌，指令，通達類，連絡文書，報告書，メモ，及びその他本件に関係ありと思料せられる一切の文書及び物件』と記載することを，明確性が欠けていないものであると認められる[。]……本件第一審裁判所が発付した捜索令状は，その差し押さえるべき物欄においては単に『犯罪にかかわる贓物，証拠物及び犯罪で得られた物』と記載されただけであり，その記載は空漠としたものにすぎず，はたして明確性の要求を満たしているのかについては……疑問がないとはいえない。」[453]

以上のとおり，台湾の最高裁の基本的な立場も，日本の最高裁のそれと同様に，単なる「〇〇事件にかかわる証拠物」というような概括的な記載が現行法上は認められないとするものであると解されるが，「会議議事録，闘争日誌，指令，通達類，連絡文書，報告書，メモ，及びその他本件に関係ありと思料せられる一切の文書及び物件」というような「例示による概括的表示」の形をとる場合であるならば，この場合での概括的な記載の適法性が認められるものとなる。言い換えれば，必ずしも 2008 年判決の台湾の最高裁のあげた「著作権を侵害することにかかわるCD，CDバーナー，コンピュータ，ラベル，説明書，包装などの証拠物」というような具体的な記載を必要としない。更に言葉を換えていえば，2008 年判決があげたものは，あくまで明示・特定の要求を満たすための一例にすぎず，「例示による概括的表示」という形での記載の許容性が否定される論旨ではないと思われる。

[453] 最高法院 100 年台上字 5065 號判決。

他方で，日本の裁判例上は，「例示による概括的表示をもってする等の記載方法が実際上一般に行われるところであるが，かような記載方法も捜査の性質上，法の根本趣旨を没却しない限り，是認せられるものといわなければならない」[454]という制限がなされている。言い換えれば，いくら概括的な記載が捜査の実務としてはやむを得ず必要な措置であるとしても，その記載自体は日本国憲法 35 条に示された令状主義の根本的な精神に反してはならないのである。

この見解は，前掲の昭和 33 年決定を前提としたものであるから，台湾の場合にも適合するものと考えられる。というのも，台湾の最高裁は，特定性という要件を判断する際に，日本の昭和 33 年決定を引用したからである。しかし，台湾においては，日本国憲法 35 条というような条文がないから，台湾のいう令状主義の根本的な精神の具体的な中身は何なのかについては，より精密な検討が必要となる。具体的には，いかなる基準をもって，令状主義における法の根本趣旨を没却しないといえるのかを明らかにする必要である。そのために，日本においてこれまで提案されてきた基準の内容を検討しておくことは，台湾にとっても必要かつ有益なものであると考える。

(1)関連性と特定性との関係

日本においては，有体物を対象とする場合であっても，特定性要件を満たしにくい場合があるということを背景に，関連性と特定性とは，異なる機能を有する２つの独立した要件ではあるけれども，差し押さえるべき対象を特定するには,憲法 35 条の「正当な理由」に対応する広義の「関連性」(被疑事実，罰条，罪名)を令状に明記すべきであろうかという問題が提起されてきた。

もとより，「正当な理由」の記載自体は，処分を受ける者に対して，いかなる理由で差押えが行われるかを知らせ，差押えの執行に対する異議ないし事後救済を申し立てる際に必要な情報を与えるという重要な役割を担うことから[455]，関連性要件には,対象物を特定するという機能(特定性要件)とは別に独立した存在の価値があるといえよう。

それにもかかわらず，前述の昭和 33 年決定は，「憲法三五条は，……令状が正当な理由に基いて発せられたことを明示することまでは要求していない[。]」としている。

この昭和33年決定に対して学説上は批判的な見解が多数を占めているが[456]，その後，論争の焦点は，差し押さえるべき対象を特定するために，正当な理由(広義の関連性要件)を記載すべきであろうかという点に移行した。そして，この問題の核心は，罰条ないし被疑事実の記載の要否という点に帰結される[457]。

---

[454] 東京高判昭和 40 年 10 月 29 日判例時報 430 号 33 頁。横井・許可状の記載 40 頁も参照。

[455] 遠藤 160，162～163 頁の説明を参照されたい。

[456] 高田・許可状の記載124頁以下，鴨・許可状の記載91頁以下，平野・日教組158頁以下，田宮・強制捜査265頁以下，遠藤158頁，熊本・令状の記載42頁以下，柏木・刑訴66頁，田宮＝多田・手続法137頁等参照。

[457] というのも，日本刑訴法上，罪名の記載が要求されているからである。

A. 罰条の記載による特定の機能

捜索する場所や押収する物件の特定との関係での罰条の記載の要否について，昭和33年決定は，「捜索差押許可状に被疑事件の罪名を，適用法条を示して記載することは憲法の要求するところでなく，捜索する場所及び押収する物以外の記載事項はすべて刑訴法の規定するところに委ねられており，刑訴219条1項により右許可状に罪名を記載するに当つては，適用法条まで示す必要はないものと解する。そして，本件許可状に記載された『本件に関係ありと思料せられる一切の文書及び物件』とは，『会議議事録，闘争日誌，指令，通達類，連絡文書，報告書，メモ』と記載された具体的な例示に附加されたものであつて，同許可状に記載された地方公務員法違反被疑事件に関係があり，且つ右例示の物件に準じられるような闘争関係の文書，物件を指すことが明らかであるから，同許可状が物の明示に欠くるところがあるということもできない。」としている。

このように適用法条まで示す必要はないとした昭和33年決定の判旨に対しては，ほとんどの学説は反対している[458]。しかし，反対する理由は，罰条の記載が捜索すべき場所ないし差し押さえるべき物件を特定するために絶対の要件であるからというわけではなく，「罪名は，それによってその内容である構成要件をおおむね特定できるようなものでなければならない」[459]という点にある。つまり，罪名は，捜索する場所や押収する物件を特定するためにもその充分な表示が必要であることを前提に，罪名を具体化するための１つの方法として，罰条(適用法条)の記載が挙げられる。具体的には，「刑法235条と書かなくても窃盗と書けばよい」けれども，昭和33年決定の事実である「地方公務員法違反」というような場合には，「地方公務員法違反というだけでは，ほとんど犯罪事実を特定させる効果はない」ということである[460]。

B. 被疑事実の記載による特定の機能

昭和33年決定によると，正当な理由の記載も罰条の記載も不要とされるから，被疑事実の記載も当然不要であるという帰結になる[461]。他方で，学説に目を向けると，そこでは，次の４つの議論が代表的なものとして挙げられよう。

第１は，捜索・差押えは常に被疑事実が確定されていない捜査の初期に行われることから,物件の特定のために被疑事実が果たす役割が低いことを理由に，その記載を不要とする見解である。すなわち,「逮捕状の場合には令状記載の事実について無関係である旨弁解し誤った拘束から直ちに解放される準備をするために被疑事実の記載が必要とされるが，差押捜索の場合には，差押捜索に立ち会った者が，その書類等が被疑事実と無関係であるとして差押に異議を述べたところで，逮捕状の場合と異なって，無関係かどうかということ

458 平野・日教組 159 頁，熊本・令状の記載 49，53～54 頁，鴨・許可状の記載 92 頁，大政 71 頁，遠藤 158 頁。
459 平野・日教組 159 頁。大政 71 頁，鴨・許可状の記載 92 頁をも参照。
460 平野・日教組 159 頁参照。
461 もっとも,実務上は,捜索差押許可状に被疑事実の要旨を記載する例も少なくないとされる(田宮･注釈刑訴 130 頁)。

はそれ程明確ではなく，無限の段階をもつ関連性を意味し，それに情状に関する資料や，捜査展開に要する資料をも加えるときは被疑事実の記載だけでは限定的な意味をもたないように思われる。従ってこの種の令状に被疑事実の記載を必要としなかったことは，それによって差し押さえるべき物，捜索すべき場所の特定に支障がない限り解釈論としても立法論としても相当である。」[462]とされる。

もっとも，この見解も，「それによって差し押えるべき物，捜索すべき場所の特定に支障がない限り」と述べているから，そこから逆に推論すれば，それによって差し押えるべき物，捜索すべき場所の特定に支障がある場合には，解釈論としても立法論としても不相当であるという帰結になろう。それゆえ，この説によっても，被疑事実の記載による特定の機能が完全に否定されるとまではいえないであろう。

第２に，「捜査の秘密，被疑者の名誉を重視する立場にたてば，これらが害されるおそれがある場合には被疑事実を記載すべきではなく，そのおそれがない場合で差し押さえるべき物をより特定するのに必要であれば被疑事実を記載してよい」[463]という折衷説がある。

これに対し第３に，捜査秘密の維持ないし被疑者の名誉の保護などの問題は別にして，差し押さえるべき対象を特定するために，被疑事実を記載すべきであるとする積極的な立場がある[464]。その代表的な議論として，平野教授の次の見解が挙げられよう。

「そこで差し押えるべき物をできるだけ特定するために，いろいろの工夫が必要になってくる。その１つに，いくつかの物を例として掲げ，『その他』として，総括的なことは書き加える方法がある。…もう１つのやり方は，犯罪事実との関係で特定する方法である。例えば，殺人の具体的事実を述べて，その証拠となる物とすれば差し押さえるべきものにも，かなりの限定が加えられることになる。このどちらも，それだけで十分に差し押えるべき物を特定することは難しいのが，むしろ普通だろう。しかし，この２つを組み合わせると，いくらかよくなる。」[465]

ここで注目するに値するのは，「正当な理由」による限定と「例示の物件」による限定との２つの要素を組み合わせることにより差押えの範囲を限定すべきという点である。言い換えれば，「正当な理由」による限定と「例示の物件」による限定との２つの要素は，同等に重要である。

これに対し，第４に，「捜索・差押えを受ける者が，目的物に含まれるかどうか，被疑事実の内容を知っていて実際に判断しうる状態にあったか否かを基準とすることは妥当ではなく，やはり，当該許可状の記載自体によって決すべき」[466]とする消極説がある。そして，

---

[462] 青柳・文書29頁（また，類似の見解として，石毛・捜査・令状218頁参照）。これに対して批判説がある（遠藤163頁。田宮・注釈刑訴130頁をも参照）。

[463] 中武＝高橋・捜査法 179 頁。

[464] 平野教授のほか，秋山・被疑事実 260 頁，石毛・令状問答 255，259～260 頁，福井・刑訴講義 5 版 146 頁，及び福井同頁関連説明に引用された諸文献をも参照されたい。

[465] 平野・日教組 158 頁。

[466] 岩崎 37 頁。同解として，吉田昭・捜査手続 364 頁，及び「差し押えるべき物が特定されているか否かは，結局，当該許可状の記載自体によってこれを決するのほかはないものというべきである。」とする東京高裁昭和 47 年 6 月 29 日

この説のうち，「例示の物件」による限定という要素の重要性をとりわけ強調する論者がある。その代表として鈴木検事が挙げられよう。鈴木検事は，「差押えを受ける者とくに被疑者以外の第三者にとっては，差し押さえられようとする物が例示の物件に『準じられるような』物かどうかを判断する方が，それと犯罪事実との関係の有無を判断するよりもはるかに容易であるといわなければならない。この意味において，犯罪事実との関係よりも例示の物件との関係を重視する……方が，一そう常識にも合し，憲法の趣旨に適うものといえるであろう」[467]と述べている。

(2)「例示の物件」による限定とその問題点

この鈴木検事の立場は，「例示の物件」により差押えの範囲を限定する機能にとりわけ重点を置き，それによって，前掲の昭和 33 年決定を支持するものといってよかろう。その具体的な論拠は次の通りである。

「これまでの実務において……とくに，許可状の執行においては，その事件に関係があるかどうかを唯一の基準として差押え物件の範囲が定められてきたのである。そして，これがそのまま許されるものとすれば，令状主義に関する憲法の保障は，ほとんど無意味になってしまうであろう。今回の決定［前掲の昭和 33 年決定を指す］において，このような実務の現状に対する最高裁の明確な判断が示されなかったのは残念であると言わなければならない。ただ，決定の趣旨を合理的に推測することが許されれば，『その他本件に関係があると思われる一切の文書及び物件』という記載方法が憲法に合致するのは，それが『例示の物件』を意味する限りにおいてであると解することもできるのであって，そうとすれば，この決定は，これまでのややルーズな実務の現状を単純に肯定したというより，これに重大な反省を強いるものといってよいであろう。」[468]

つまり，これまでの実務における令状の記載は概括的記載にすぎないため，許可状の執行においては，その事件に関係があるかという点が，差押えの範囲を画定するための唯一の基準とされてきたということである。

それでは，なぜ，このような実務のやり方がそのまま許されるものとすれば，令状主義に関する憲法の保障が，ほとんど無意味になってしまうといえるか。この点について，鈴木検事は，「『その他本件に関係があると思われる一切の文書および物件』という表現は，これよりはるかに広い意味にも解される。すなわち，例示の物件をはじめ，あるいは，例示の物件はもちろん，その事件に関係あると思われさえすれば，どんな文書や物件でもすべてここに含まれるという趣旨にもとることができる。むしろ，そう解する方が自然でさえあるといってよい」[469]と述べている。

すなわち，従来の実務の運用としては，「その他本件に関係があると思われる一切の文

判決東高刑時報 23 巻 6 号 119 頁参照。

[467] 鈴木 75 頁。

[468] 同前注。

[469] 鈴木 75 頁。

書および物件」という表現が極めて広い意味に解されており，「例示の物件」という要素は差押えの範囲を限定する基準として機能していなかったとのことである。

確かに，かような実務の理解を前提とすると，「被疑事実の記載」があったとしても，「例示の物件」による限定機能が働かないかぎり，鈴木検事が指摘したように，どんな文書や物件でも「その他本件(被疑事実)に関係があると思われる」枠内に入ってしまうことになるという意味で，差し押さえるべき物件の範囲が広すぎる。そうだとすると，鈴木検事の提案のように，仮に，昭和 33 年決定の判旨を，「その他本件に関係があると思われる一切の文書及び物件」という記載方法が憲法に合致するのは，それが例示の物件を意味する限りにおいてであると解することができれば，例示の物件の記載が差押えの範囲を限定する基準として機能することを期待できるかもしれない。しかし，この鈴木検事の提案は，以下のような難点を含んでいる。

(A)法的な実効性の担保の欠如

まず，昭和 33 年決定の趣旨を，例示の物件により特定すべきであるという意味であると解する鈴木検事のような理解は，最高裁により否定されているように思われる。このことは，昭和 33 年決定後に出た，最一判昭和 42 年 6 月 8 日判例時報 487 号 38 頁(以下，昭和 42 年判決という)の判旨から明らかである。本判決は，「差し押さえるべき物：本件に関係ありと思料される帳簿，メモ，書類等」として発付された捜索差押え許可状に基づき警察官が麻雀屋を捜索し，「麻雀牌及び計算棒」を差し押さえたという事案につき，「本件麻雀牌及び計算棒が，令状にいう差し押さえるべき物に包含されるとした原審の判断は正当である」と判示した。

「麻雀牌及び計算棒」の部分については，令状の文言からみれば，それを含まないと解するのが寧ろ自然であるし，また，それらは「帳簿，メモ，書類」という例示の物件ないしそれに準ずるものにも当たらないのが明らかであるにもかかわらず，昭和 42 年判決は，それらも差し押さえる物に包含されると判断したのである。言い換えれば，前掲の例示の物件による制限という鈴木検事の理解を，最高裁が採用していないことは明らかである。

(B)正当な理由と例示の物件との関係につき

もとより，正当な理由を記載せずに，例示の物件のみで，果たして限定の機能があるのかについては大きな疑問がある。これは，鈴木検事の提案の最大の問題点であると思われる。

この点につき，「差し押えようとする目的物だけに備わっている特徴を具体的に明示するのが最も望ましい。例えば，カメラについている製品番号のようにその物に固有の物理的特徴があるときはその特徴を，また盗難被害品の着物が質入れされているという場合のように，着物に固有の物理的特徴はないが，何某から×月×日に質入れされた着物というように質屋の受入手続上の特徴があるときには，その特定事項等を示すことができれば最も

明確に特定することができ望ましい。しかし，差押え目的物には右のような明確な固有の特徴のない場合がむしろ通常である(例えば，帳簿，伝票，メモ，賭具)[ため，]……目的物の表示方法については，これを令状に明示すべきものと定めた法の趣旨に反しない限度内で，ある程度概括的，抽象的に記載することもやむを得ないものとしなければならないであろう」[470]という指摘がなされている。

これによると，仮に，「『会議議事録，闘争日誌，指令，通達類，連絡文書，報告書，メモ』その他本件に関係ありと思料せられる一切の文書及び物件」というような昭和 33 年決定で見たパターンを，鈴木検事が提案した通り，例示の物件である「会議議事録，闘争日誌，指令，通達類，連絡文書，報告書，メモ」ないしこれらに準じる文書及び物件に限ると解することができるとしても，これらの例示物件自体は明確な固有の特徴を持たないため，正当な理由(とりわけ，被疑事実)を記載しない限り，差し押さえるべき物が特定されたとは言いがたい。

というのも，「会議議事録，闘争日誌，指令，通達類，連絡文書，報告書，メモ」は例示の物件であるとはいえ，それらも多種多様であるから，捜査の対象とする被疑事実，罰条などの正当な理由によって限定しないと，本件に関係あるかどうかを判断できず，結局のところ，捜査の対象外の「会議議事録，闘争日誌，指令，通達類，連絡文書，報告書，メモ」まで差し押さえるべき物になってしまうおそれがあるとすれば，それは，一般令状禁止原則に反し，差し押さえるべき物が特定されたとはいえないと考えられるからである。

この意味で，やはり，「正当な理由」による限定と，例示の物件による限定との２つの要素を組み合わせることにより差押えの範囲を限定すべきであるとする平野教授の見解が妥当だと思われる。

２．あるべき立法へ

以上に述べたことは，次の３点にまとめられる。①台湾の最高裁が引用した日本の最高裁の昭和 33 年決定は，日本では，学説においてあまり評価されていない。②昭和 33 年決定に対する批判の核心は，差し押さえるべき物を特定するためには罰条及び被疑事実をも記載すべであるという点にあるが，台湾の最高裁は，この点に全く言及していない。③例示の物件による限定があったからといって，必ずしも概括令状禁止原則(または一般令状禁止原則)の要求を満たすわけでない。

ここでまず検討すべきは，台湾の最高裁がいう概括令状禁止原則の具体的な中身及びその中華民国憲法上の位置づけは何なのかである。これは，立法論の前提問題となるものである。

また，前掲の３つの点に対応するには，罪名，罰条並びに被疑事実などの正当な理由の記載(すなわち関連性要件の記載)による限定と，例示の物件による限定との２つの要素を

[470] 秋山・目的物の特定 235～236 頁。とりわけ，差押目的物が現金など代替物の場合は，その自体に個性がないため，特定困難な場合が多いと指摘されている(令状事務(1 版)338 頁)。

組み合わせることにより差し押えるべき物を特定するという平野教授の提案が適切なものであると考えられる。しかし，立法論として，当然に関連性要件(罪名，罰条ないし被疑事実など)を令状に記載しなければならないという帰結になるのかについてはなおより深い検討の必要がある。

最後に指摘したいのは，関連性要件による限定と，例示の物件による限定との２つの要素を組み合わせるという方策が有益であるとはいえ，これだけで問題が完全に解決されるわけでないという点である。この点は，日本の改正法 107 条の 2 項を検討したところであげたクラウド・サービス・システムの例を想起すれば明らかである。というのも，クラウドのような，複数の端末から結成された１つの巨大なシステムの場合においては，例示の物件という概念を観念できないし，また，関連性要件による限定はＩＴシステムなどのバーチャル空間においても考えられるが，関連性要件による限定は，あくまでも，差し押さえるべき物ないし当該物件が存在する場所などの物理的な特徴による限定を補完する機能を果たすものにすぎず，主な限定要素である物理的な特徴が機能しない場合には，補完的な限定要素である事件との関連性を明記したとしても，特定性の要件を満たすことはないからである。とすると，この部分は，やはり立法論による解決を図るしかないだろう。言い換えれば，バーチャル空間における情報を対象とする場合には，従来の物理的な限定要素(例えば，例示の物件による限定)が失効してしまうから，その代わりに，物理的な特徴に依存しないバーチャル空間及びそこにある情報に相応しい「非物理的な限定要素」を提案する必要がある。

それゆえ，以下で検討すべき問題は，(1)台湾における概括令状禁止原則の中身と法の位置づけは何なのか，(2)差し押さえるべき物を特定するために，立法論として，関連性要件を必要な記載事項とすべきか，及び(3)バーチャル空間における差押えの対象となる情報を特定するためにあるべき非物理的な限定要素の具体的な中身は何なのか，という３点である。

(1)概括令状禁止原則について

ここまでの検討により，問題の核心は，情報が記録された媒体の種類が何なのかではなく，これらの媒体から捜査機関が取得する情報の量及びその質を，いかに「最小化」すべきかという点にあることが明らかになった。言い換えれば，正当な理由であれ，関連性要件であれ，特定性要件であれ，それらは，いずれも，この最小化の目的に奉仕するものである。そしてこの最小化の目的を達成することは，情報の差押えという制度の核心をなす部分でもある。

以上により，台湾の最高裁のいう概括令状禁止原則の中身を具体化すると，それは，物あるいは情報に対する差押令状をもって，捜査機関が取得する物あるいは情報の量及びその質を最小化しなければならないという法的要求であると定義することができる。

次に検討すべきは，ここでいう最小化の法的要求は，法律のレベルにとどまるか，それ

とも，憲法の次元に達するものであるかである。この点，日本の場合は，ここでいう最小化の法的要求の根拠が，憲法 35 条における令状主義に求められ，アメリカの場合は，憲法修正４条のいう令状原則がその根拠として考えられるのに対して，台湾の場合には，これに対応する憲法上の明文規定がないのである。

とはいえ，台湾においては，捜索・差押えについての令状主義(または原則)はあくまで立法政策にすぎず，憲法上の要求ではないと主張する論者も，中華民国憲法 23 条の比例原則から導かれた最小化原則は捜索・差押えという制度を支配する憲法上の要求であることを認めている[471]。言い換えれば，現行刑訴法が採用した裁判官留保による令状原則という制度は，捜索・差押えの範囲を最小化しなければならないという憲法上の要求を満たすために１つの可能な手段にすぎないというのである。

基本的には，台湾の憲法の文言解釈としては，かような理解が正しいと言わざるを得ないのであろう。とはいえ，憲法解釈の方法は，文言解釈だけではないから，中華民国憲法の精神からは，裁判官留保による令状原則が憲法上の要求であることを導き出すことができるという見解があり，それも説得力があるものであろうと思われる[472]。そして，この見解を支えるために必要とされる憲法上の条項としては，前にも論じた概括的権利保護条項とされる憲法 22 条が考えられる。というのも，同条は，実体法上の権利にかぎらず，手続法上の権利も含むものとされるからである。

つまり，①令状主義(または原則)の核心は，最小化原則にあるとすれば，かかる原則は中華民国憲法 23 の比例原則から導かれるから，その意味で，令状原則を憲法上の要求であるといえること，及び②捜査機関が，この憲法上の要求に従い最小化の目的を忠実に実現することを担保するためには，中立かつ超然な司法機関による審査・監督のメカニズムを構築する必要があること，という２点が重要である。

ところで，解釈論としては，②の根拠は，中華民国憲法 22 条にそれを求めることも考えられないわけではないが，この部分については，学説上争われてきているから，法の明確性という観点に鑑みると，新しい憲法改正をもって明文の根拠を改めて設けるほうが望ましいと考える。

(2)関連性要件の記載の要否

次に，立法論としては，差し押さえるべき物を特定するために関連性要件(罪名，罰条な

---

[471] 比例原則が基本的に３つの部分原則から構成されていることは，台湾の学説ないし実務上においては，ほぼ一致をみている。すなわち，ドイツから発展されてきた，いわゆる，①適合性(Geeignetheit)の原則，②必要性(Erfoderlichkeit あるいは Notwendig-keit)の原則，③狭義の比例原則(Der Grundsatz der Verhältnismäßigkeit im engeren Sinne あるいは Proportionalität)，という３つのものである 。適合性の原則とは，目的の実現に対し手段(措置)が「質的」に適合であること ，言い換えれば，目的も，手段も，それ自体は正当であり，かつ，目的と手段との間に正当な関連性を有することを意味する。これに対して，狭義の比例原則とは，同様に目的と手段との関係を問うものであるが，質的な視点ではなく，量的な評価を行うという相違がある 。最後に，必要性の原則は，「最小の侵害の原則」，「最も緩やかな手段の原則」，「最も侵害的・規制的でない手段」などとも呼ばれており ，本稿のいう「憲法上の原則としての最小化原則」そのものを指す。

[472] 王・令状原則 34 頁以下参照。蔡耕榮・修正後通訊 52 頁以下，大法官解釈 535 号をも参照。

いし被疑事実など)をも法定の必要な記載事項とすべきかという問題を検討する。そのために，以下では，関連性要件と特定性要件との関係を敷衍しておく。

まず，特定性要件については，ここまでの検討を踏まえてそれを再定義すると，次の２つの視点に基づく可能性がある。その１つは，対象の識別可能性という視点であり，もう１つは，一般令状禁止原則(または概括令状禁止原則)という視点である。

まず，対象の識別可能性という視点を徹底すると，場所の捜索や物の差押えとは，事件を離れて，純粋に物理的に，ある場所で何かを捜すこと，ある物の占有を取得することであるから，場所ないし物を特定するには，場所ないし物自身の特徴により行うべきであって，関連性要件(正当な理由)とは関係がないという帰結になる[473]。

しかし，かような徹底した見解をとると，実情にそぐわない不都合が生じてくるため，この見解を正面から支持するものは見当たらない。その代わりに，同様に対象の識別可能性という視点から出発するものであるが，原則的には特定性の要素を場所ないし物件自体の特徴に求めるべきとしつつ，捜査の秘密性ないし被疑者の名誉を害することがないかぎり，場所ないし物件を特定するために関連性(正当な理由)も一要素として考えられるという折衷的な見解が，日本の実務上は支配的な見解であるとされる[474]。

これに対して，一般令状禁止原則という視点によると，関連性(正当な理由)と特定性との間には密接不可分の関係があるから，処分の対象を特定するに当然は関連性をも考量に入れるべきものであるという結論が導かれよう。なぜならば，一般令状禁止原則からすると，捜索・差押えが許されるのは，正当な理由が存在する場所・物に限られなければならないので，正当な理由を離れて独立に対象の識別可能性の有無を論じることが考えられないという帰結になるはずだからである[475]。

このように考えると，関連性も特定性も，正当な理由に由来するものであって，一般令状禁止原則を実践するための一要素にあたるという点で共通しているといえよう。この意味で，関連性と特定性は表裏一体の関係を有するものといえよう。この見方は，最小化原則を令状原則の核心としている本稿の立場と一致している。言い換えれば，特定性要件を定義するには，一般令状禁止原則(台湾の最高裁のいう概括令状禁止原則)，言い換えれば，最小化原則という視点から出発すべきものである。

しかし，だからといって，立法論的には，当然に，関連性要件(罪名，罰条ないし被疑事実など)をも令状に記載しなければならないという帰結になるわけではないのである。ここでの問題の核心は，令状に要求される特定性とは，一体誰に対して要求されるものであろうかという点に帰結する[476]。この点については，次の３つの立場が考えられる。

すなわち，①特定性は執行者の警察官に対するものであり，警察官さえ正当な理由を分かればよいから，それを令状に記載する必要がないとする立場，②令状発付者の裁判官に

---

[473] 横井・刑訴裁判例ノート(1)242 頁の説明を参照されたい。

[474] 横井・刑訴裁判例ノート(1)243 頁，令状事務(第 1 版)335～336 頁，捜査資料(改訂)184 頁の④参照。

[475] 大澤・特定 433～434 頁。

[476] 平場・許可状の特定 5 頁。

対して特定すればよいから，令状請求書に表せば十分だとする立場，③被処分者に対するものであるから，令状に明記しなければならないとする立場である。

このうち，①と②は，令状の発付及び執行に必要不可欠なものである。というのも，憲法 35 条に明記されている通り，令状は正当な理由に基づき発しなければならないが，裁判官が正当な理由を分からないと，令状を発付することは不可能であり，また，警察官が正当な理由を分からないと，令状を執行することができないからである。逆に言えば，令状に罪名のみを記載し，罰条ないし被疑事実を記載しないという形にした場合，被処分者ないし立会人の現場での即時の異議ないし事後の不服申立てなどの救済手続の保障が侵害されることになるが，令状の発付ないし執行には全く差し支えがないのである。

しかしながら，事後の不服申立ての点はともかく，被処分者ないし立会人の現場での即時の異議は，単なる権利救済の側面という意義に止まらず，捜査機関による令状執行の適正性を監督したり国家行為の恣意を防止したりするという重要な機能を果たしている。この機能が，一般令状禁止原則の目的を遂行するために必要な機能であるとすれば，令状には，罪名，罰条はもちろんのこと，被疑事実をも詳しく記載しなければならないという帰結になるはずだろう。

とはいえ，仮に，被処分者の権利救済の保障及び捜査機関の令状執行の適正性を監督したり国家行為の恣意を防止したりするために十分な制度上の配慮を行うことさえできれば，③の部分を緩和することも許されると思われる。例えば，被疑事実の詳細を令状に記載する代わりに，捜査機関が被疑事実の詳細について説明する義務を課したり，被処分者ないし立会人がそのような説明を求める権利を与えたりするという方策が考えられよう。

これに対しては，捜査の秘密を理由として，被疑事実についての十分な説明を尽くすことはありえないという反論もありうるだろうが，こうした場合においては差押えが許されるかを裁判官の判断に任せるという形にするのはどうであろうか。具体的には，被処分者ないし立会人が，現場で，令状を発付した裁判官に電話して，被疑事実に関する捜査機関の説明が不十分であるため，自分の所持品が押収されたことに納得できず，それに不服を抱いているというような趣旨を述べる権限を認めることが考えられないわけではないだろう[477]。このような権限の行使により，被処分者の権利救済の保障及び捜査機関の令状執行の適正性を監督したり国家行為の恣意を防止したりするという目的を達することができると同時に，正当な理由を既に分かっている裁判官であるならば，被処分者の抗弁を聴取したうえで，差し押さえるべきものに当たるという捜査機関の判断が令状の本旨にかなうかどうかを判断する能力があるし，また捜査の秘密を害するおそれもないと考えられる。

しかし，これに対しては，差し押さえるべきものに当たるかどうかという判断は捜査の本質と関連する強制処分の執行裁量権限であって，裁判所にこれをコントロールさせることは妥当でないという反論がありうる。それゆえに，ここでの問題の核心は，どの段階ま

[477] 秋山・迅速な令状 176～177 頁が参考になる。

での，またどの程度の関与を裁判官に認めることができるかにある[478]。この問題は，法の権限分配に関する体系によって解決されることになろう。

この点，本稿は，立法の在り方としては，捜査の段階においても，当事者主義に基づく「訴訟」的構造――言い換えれば，捜査構造の対審化[479]――を採用すべきであると考える。というのも，裁判官は，被処分者が異議を出したときに，直ちに「差し押さえるべきものに当たるかどうか」を判断するわけではなく，両方の当事者――警察の判断の理由及び被処分者の異議の理由――を聴取したうえで，両当事者の主張のどちらがより令状の本旨にかなうかを判断するという捜査構造の対審化の設計は，強制処分の執行裁量権限を侵害するものと思われないし，また，現代の通信技術によれば，即時の異議に対する迅速な処理も可能であるから，捜査の効率性にも害しないものだからである。

これに対して，各々の媒体や情報の量が膨大である場合には，それに対して異議の機会を与えることはありえないという反論があるかもしれない。しかし，こうした場合は，適用される制度は一般の差押えではなく，前に打ち出した前段階の蓋然性による差押えという制度となるから，大きな問題が生じない。というのも，本稿の理論によると，捜査機関が，差し押さえる対象が大量の媒体ないし情報であること，及び捜査の便宜性ないし時間のコストなどを理由に現場で蓋然性による差押えを実施する必要性があることを，令状の発付を請求する際に，令状発付裁判官に疎明すれば，前段階の蓋然性による差押え令状を得ることが可能だからである。つまり，こうすれば，前段階の蓋然性による差押えの実施により証拠となり得る媒体ないし情報がすでに確保されている以上，蓋然性による差押えの後段階においては対審構造を採用することが可能となり，それと同時に，中立の裁判官が捜査側と被処分者側との双方の意見を聴取したうえで「差し押さえるべきものに当たるかどうか」を判断することが考えられるからである。

(3)非物理的な限定要素

以上のとおり，仮想的な場所であるバーチャル空間における無形の情報を対象とする場合には,特定性要件は,「非物理的な限定要素」をもって,差し押さえるべき対象の範囲を最小化しなければならないことと定義される。そこで，次に検討すべき問題点は，ここでいう「非物理的な限定要素」は何なのかである。

A. 正当な理由

従来，有体物を対象とする場合の差押令状発付の正当な理由(台湾の場合では，相当な理

[478] 渥美・テレビカメラ37頁が参考になる。

[479] 日本における捜査の構造についての代表的な議論としては,①弾劾的捜査観(平野・刑訴全集 83 頁以下。同解として，三井・手続法(1)[新版]177～178 頁をも参照)，②訴訟的捜査観(井戸田 2，3 頁。同解として，石川・刑事手続と人権 193 頁以下；同・捜査における弁護の機能 11 頁以下をも参照)，③糺問的捜査観(河村・捜査実務 101 問(改訂 4 版)3 頁，金 77 頁。関連として，川崎・検察官論 21 頁，同論文 24 頁の注 17 に挙げられた参考文献並びに同 32 頁～36 頁の説明，鴨・刑訴法新展開 76 頁をも参照)，④修正された弾劾的捜査観(松尾・刑事訴訟の原理 252 頁)，の４つの立場が挙げられよう。本稿が提案した捜査構造の対審化とは，基本的には，①を基盤とするものである。

由とも呼ばれる)とは，①特定の犯罪の嫌疑が存在すると認められること，②差し押さえるべき物が被疑事実と関係すると思料されること，及び③差し押さえるべき物が一定の場所に存在すると信じられることを意味する[480]。

これに対して，情報を対象とする場合の正当な理由とは，①一定範囲の人の集合の中に，犯罪の嫌疑のある人ないし犯罪と関わる第三者が存在する蓋然性があること，②差し押さえるべき情報が被疑事実と関係するか，被疑事実の解明に資するものと推測する合理的な根拠があること，及び③差し押さえるべき情報が，物理的な媒体若しくは仮想的なバーチャル空間に存在する蓋然性があること，と解することができる。その論拠としては，次の２つのものが考えられる。

第１に，ＩＴシステムなどのバーチャル空間においては，場所という概念がないことに加え，分散システムが採用されているため，犯罪の嫌疑がある人を特定し，その犯罪と関連性を有する情報のみを対象とするのは，現時点の技術では不可能であるから，情報が対象である場合に，その内容を有体物が対象である場合と同様に解するのは明らかに不合理である。

第２に，本稿の「関連性＝蓋然性」という構造においては，前述した「法による実質的な保障を回復できる内在的制約」が含まれており，前段階の正当な理由という部分での要求のレベルは，従来の有体物を対象とする場合のそれよりは低くなるけれども，その後の段階に加えられる法的制約により，前段階で低くなった保障の程度が実質的に回復できるので，上記の内容の，情報が対象である場合の正当な理由を採用したとしても，中華民国憲法 23 条の最小化原則から導かれた一般的・探索的差押禁止原則に反することはない。

B. 関連性

次に，「関連性」については，従来は，物理的な特徴を前提に，「関連性」要件は，「差し押さえるべき物が被疑事実と関係すると思料されること」と定義され，それが，「五官の作用」により確認されると理解されてきた。

しかし，ＩＴシステムなどのバーチャル空間においては，関連性を確認するために自動徹底検索技術の利用を必要とする場面がほとんどであろう。このような技術の利用は，五官の作用とは関係ないから，前掲の従来の理解はこうした場合には適合しないものとなる。

それゆえ，関連性の確認のために自動徹底検索技術が用いられるという非物理的な特徴に照らして，こうした場合の「関連性」の意味を考えると，それは，人の五官により処分の対象が犯罪証明に必要な証拠としての価値・重要性を有するものであることが確認されたということではなく，「科学技術の利用や一定の方法により，当該事件の捜査にとって必要ないし有益な情報が存在する蓋然性があると推測されうること」と解されることになる。

[480] 王・刑訴講義 99～100 頁，林鈺雄・刑訴(上)394 頁，李・明確性原則 114 頁。また大澤・特定 433～434 頁をも参照。

C. 特定性

最後に，特定性については，従来，差し押さえるべき物が一定の場所に存在すると信じられることが令状の発付要件の１つとされてきたが，当該場所を対象とした令状さえあれば同場所に置かれたすべての物件を差し押さえることが認められるわけではなく，当該場所において発見しうる物件の名称，外見や特性等の「物理的な要素」により，差し押さえるべき対象とそうでない対象とを区別することができる程度に，差し押さえるべき物を令状に明示することが，(差し押さえるべき物の)特定の意味であるとされてきたのに対して，Winick の理論からすると，(差し押さえるべき情報の)特定とは，「差し押さえるべき情報を取り出すための『執行方策』の提出」[481]などの「非物理的な要素」により，差し押さえるべき情報が存在する蓋然性がある「一定の情報の集合(体)」若しくは「一定の非物理的な空間(システム)の構成(体)」の範囲と，そうでない範囲とを区別することができる程度に，情報を押収(記録・複写・産出)しようとする範囲を明示しなければならないという理解になる。

(4)新たな立法の内容

以上をもとに，新たな立法についての私案を敷衍すると，次のようになる。

A. 記載の程度に関わる原則と例外

正当な理由の記載の程度につき，次のような原則と例外を設けておくべきである。原則としては，罪名，罰条のみならず，被疑事実をも記載すべきであり，そのうえで，被疑事実の記載は，対象となる事案とそうでないものとを区別することができる程度にすべきである。

ただし，例外的な場面では，被疑事実の記載を不要にするか，あるいは，その記載の詳しさの程度を緩和するかのどちらかを許容する。同時に，被処分者の即時異議ないし事後の不服申立ての権利をどのように担保するか，及び捜査機関の執行の適正性をどのようにコントロールするかという２つの点について，立法上の措置を用意しておかなければならない。

B. 直接強制処分と間接強制処分

直接強制処分を採用するとやむを得ず関連性のない部分をも一括して取得することになる場合には，間接強制処分を先行させる可能性を考慮しなければならない旨を，立法により，裁判官に指示しておくべきである。

そのうえで，裁判官があらゆる資料を勘案し総合的な判断により直接的強制処分の採用

[481] ここでいう執行方策の提出の例として，例えば，利用する予定の検索ツールの技術的な特徴や，かかるツールをもって検索しようとするシステムの技術的な特徴，ないしかかるツールにより開示されうる情報の技術的な特徴(例えば，拡張子の種類など)を明記することが考えられる。

が妥当だと判断したときには，関連性のない部分をも一括して取得した後，関連性のある部分と関連性のない部分とを選別するための行為(すなわち，第２段階の捜索の範囲)を規制しなければならないという趣旨の規定を設けなければならない。

第６節　問題点の解決

以上のとおり，本稿が打ち出した「情報に対する終局的処分権」という新しい法益論により，2001 年の台湾刑訴法改正により生じた，差押えの従来の定義と，無体の電磁的記録をも差押えの対象とする法文との間における法理論上の齟齬を解消することができる。すなわち，本稿の理論によると，有体物を対象とする場合に，従来のとおり，占有の剥奪という差押えの定義をそのまま維持することができるのに対して，音声や電磁的記録などの無体の情報を対象とする場合には，占有の剥奪ではなく，情報に対する終局的処分権が剥奪されたことが，情報に対する差押えとなる。

これによると，電磁的記録に対しては占有剥奪をすることが不可能であるから電磁的記録をも差押えの対象とする立法は適切ではないという現行法に対する台湾の先行研究の指摘はその論拠を失う。それと同時に，終局的処分権に着目すると，物と情報の両者を同じ定義の下に包摂させることも可能になるから，有体物を対象とする場合の定義との不調和性も解消されよう。というのも，有体物を終局的に処分しようとすれば，その占有を剥奪するという形になるのに対して，情報を終局的に処分しようとすれば，原始情報及びその全てのコピーを完全にデリートすることとなるが，それらは，いずれも，終局的処分権という概念により統括することができるものだからである。

そのうえで，本稿は，情報を差押えの対象とする場合にあるべき差押令状の発付要件ないしその判断基準・原則を打ち出している。これにより，以下のとおり，ここでの検討課題である，実質的な過大差押え及び蓋然性による差押えという２つの問題が解決される。

第１款　実質的な過大差押えについて

Ⅰ.「物(媒体)のみを取得する」だけで十分な場面

実質的な過大差押えの問題は，従来指摘されてきた「情報のみを取得する」だけで十分な場面のみならず，「物(媒体)のみを取得する」だけで十分な場面にも生じうる。というのも，「情報のみを取得する」だけで十分な場面であるのに，現行法が適用されると，常に，情報と媒体との両方が政府に取得されてしまうことになる点と，「物(媒体)のみを取得する」だけで十分な場面であるにもかかわらず，現行法のもとでは，当然情報も媒体と一緒に政府に取得されてしまうことになる点とは，異曲同工だからである。しかし後者に関しては，これまでは，問題が完全に見過ごされてしまっている。

これに対して，本稿の考え方によれば，「情報のみを取得する」差押令状により，前者の問題点が解決され，他方，後者の問題点には，「物(媒体)のみを取得する」差押令状をもって対応することができる。このうち，後者の「物(媒体)のみを取得する」差押令状の内容は，ノートパソコンを鈍器として人を殺害したというような事例を考えてみると明らかになる。すなわち，このような例では，ノートパソコンという機器のみを取得すれば十分であるから，ノートパソコンを差し押さえる際に，被処分者がノートパソコンに蔵置されたデータを他の媒体に転写したり削除したりする権限を認めた上で，「捜査機関はデータの削除されたノートパソコンしか差し押さえられない」，若しくは，「技術を以てデータをロックしないと差し押さえることが認められない」といった規定を設けるべきである。

Ⅱ．本稿の提案の必要性と有益性

台湾の場合においても，(検察官の職権による無令状の)検証という手段により，データのみを取得することが可能であり，これが，いわゆる実質的な過大差押えという問題への１つの対応策として考えられるかもしれない。しかし，そうであっても，現行法のもとでは，有体物である大容量の端末機器を差し押さえることができるという点に変わりはない。

この点に対応するため，立法論的には，日本のように，差押えに代える処分を新たに設ける方策も考えられるが，しかし，これは，差押えの執行の一方法と位置づけられるものにすぎず，問題が完全に解決されるとはいえない。というのも，この差押えに代える処分という執行方法をとるかどうかを判断する権限は，裁判官ではなく，捜査機関にあるため，日本では，改正法の成立後も，裁判官が実質的な過大差押えの問題に介入しようとすれば，結局のところ，従来と同様に，利益衡量論を活用するという微調整の手段をとるしかないからである。

そして，さらに問題なのは，被疑者や被告人が被処分者であるときには，現行の台湾刑訴法の単一段階の令状制度を前提とするかぎり，利益衡量論を適用した結果，ほとんどの場合は，記録媒体全体を差し押さえることに合理性があると認められることになるであろう。というのも，デジタル証拠の隠滅の容易性に加え，被疑者や被告人の協力の真摯性には常に疑問符が付くために，プロバイターを除く一般の場合には媒体全体を差し押さえておくことが基本になっているのが捜査の実情であるし，また，技術上の問題や証拠化の必要性などの理由で，媒体と情報の両方を獲得することが必要となる場合が稀ではないからである。

他方で，記録媒体全体を差し押さえておくべきと判断される場合においては，そもそも，実質的な過大差押えというような問題が生じることはないのではないかという疑問があるかもしれない。というのも，単一段階の令状制度しか用意されていない現行法のもとでは，媒体と情報の両方を獲得する必要があると判断される以上，両方を差し押えることは正当だといえるからである。

しかし，多段階規制論(前段階の蓋然性による差押えに対する規制と後段階の関連性を確認するための捜索に対する規制)に基づく本稿の考え方からこの点を改めて分析すると，そこにも実質的な過大差押えに該当しうるものがあるという異なる帰結が導かれる。

まず，前述の通り，犯罪の立証にはデータのみで十分であるが，媒体と情報の両方を獲得する必要があるといえる理由としては，主に，①デジタル証拠の隠滅の可能性ないし被疑者や被告人の協力の真摯性が疑われるため，及び②技術上の理由ないしデジタル証拠の可視化・可読化のため，という２つの場合が挙げられている。

このうち，まず，①の場合は，現行法のもとでは，データ自体が差押えの対象にはならないし，また，単一段階の令状しかないから，媒体と情報の両方を獲得する必要があるという帰結にならざるを得ない。これに対して，本稿の理論からすると，被疑者の協力の真摯性に問題があり，デジタル証拠の隠滅を防止する必要性がある場合には，「情報のみを取得する」差押令状をもって，関連性のあるデータが存在する蓋然性があると思料される媒体であるかぎり，かかる媒体の中のすべてのデータを一括してコピー(蓋然性による差押え)しておけばよいから，媒体と情報の両方を獲得(差押え)する必要はないことになる。

このように，本稿の理論のもとでは，「情報のみを取得する」差押令状と「媒体のみを取得する」差押令状の２つの制度が用意されているから，媒体と情報の両方を獲得する必要がある場合にあたるかどうかは，有体物のみを差押えの対象とする現行法よりもより厳格な基準によって判断されることがわかろう。言い換えれば，現行法のもとでは，媒体と情報の両方を獲得する必要があるといえる場合であっても，本稿の提案によれば，それが必要でないと解される場合があり，この意味で，現行法は実質的な過大差押えの問題を抱えていると言えよう。

次に，②の場合は，本稿の理論からも媒体と情報の両方を獲得する必要があるという帰結になるが，本稿の対応と，現行法のそれとは，全く異なるものがある。具体的には，まず，本稿の理論からすると，捜査機関は，前段階(すなわち，電磁的記録媒体に対する蓋然性による差押えという段階)においては，一般の差押令状(関連性による差押え)ではなく，いわば「蓋然性による差押令状」をもって，「準立証関係」が存在する蓋然性があると思料される媒体ないし情報の両方を差し押さえておくことができる。しかし，同令状をもっては，蓋然性により一時的・一括的に差し押さえられた媒体に蔵置されたデータを検索することはできず，そのためには，別個の「関連性を確認するための捜索」令状[482]を必要とすることになる。

このように，多段階令状を設けることが可能であり，かつそうすべきであるのに，かような用意がなされていない現行法には，媒体と情報の両方を獲得する必要がある場合の実質的な過大差押えの問題に対応できていないという不備があるといってよかろう。これに対して，多段階令状という制度を適用すれば，最小化原則を徹底し，実質的な過大差押え

[482] この令状は，捜索という制度にかかわるものであるから，その具体的な発付要件と判断基準・適用原則についての詳細は第２章において論じる予定である。

の問題を抜本的に解決することが期待できる。というのも，多段階規制論を前提とした情報に対する捜索・差押令状という制度のもとにおいては，裁判官に実質的な過大差押えの問題に介入する権限(捜査の各々の段階に応じて，物ないし情報に対するあるべき捜索・差押令状を発付する権限)が付与されているから，いかなる場合に実質的な過大差押えの問題が存在するといえるか，そして，かかる問題を解決するにはいかなる手段をとるべきかなどについての判断が，捜査機関の恣意により左右されることはないだけでなく，裁判官自身も，場当たり的な判断を行うことができず，情報ないし物に対する各段階の捜索・差押令状の定義，要件と基準に従い，法的判断をしなければならないからである。

以上により，本稿の理論のもとにおいては，実質的な過大差押えの問題に対応するために台湾の現行法の解釈論として考えられる，①検察官の職権による無令状の検証の活用，②利益衡量論による微調整，及び③アウトプット物の作成という実務の慣行，という３つの方策をとる必要はなくなる。それゆえに，前述した，この３つの対応策に関わる種々の問題点も解消されるのである。

Ⅲ．アウトプットの規制の在り方

１．事後救済という制度の構築について

現行法のもとでは，捜査機関が持参した物(転写媒体)に対して「占有剥奪」を行い，差し押さえるということは観念できない一方で，占有剥奪の発生を伴わない「データを転写する」という行為は，差押えに該当せず，「検証の結果の記録」にあたるものにすぎないとされているので，それに対する事後救済を主張することができない。

これに対して，本稿の理論によると，コピー行為自体が情報の差押えにあたるため，実務上これまでは行われてきたアウトプットの慣行自体は，情報の差押えと解されることとなり，占有の剥奪という意味での財産上の損害がなくても，政府にコピーされた自分の情報を削除したり返却させたりするという事後救済を設けることが，理論上可能となる。

２．無形のアウトプットについて

現行法の条文上は，電磁的記録も差押えの対象とされているが，占有の剥奪という差押えの従来の定義が全くは変わっていない。その前提で，アウトプット行為を差押えと解釈することができるのかが問題となる。この点につき，現場で一定の用紙ないし有体の媒体にアウトプットする，いわゆる「有形のアウトプット」の場合には，解釈論的にもある程度対応できるかもしれない。有形のアウトプット物の占有を剥奪する行為を差押えであると解するのである。しかし，このような解釈の手法は，オンラインでデータをダウンロードしたりするというような「無形のアウトプット」の場合には対応できなくなる。

これに対して，本稿の理論によると，情報を差押えの対象とする場合，情報の終局的処分権が剥奪されることが，情報の差押えにあたるから，現場で作成した転写媒体というよ

うな有形のアウトプット物を介在させる必要はなくなるので，オンラインの場合であれ，オフラインの場合であれ，それらのいずれにも対応することができる。

他方で，台湾の先行研究においては，オンラインでデータにアクセスしたり，それをダウンロードしたりする「無形のアウトプット」を電磁的記録に対する捜索・差押えと解する理解も一部にある。しかし，これは，理論上の一貫性を欠くという批判を免れないばかりでなく，このような理解によると，オンラインでの捜索・差押えの範囲をいかに制限することができるのかについて，現行法上そのために必要な規定が用意されていないため，結局のところ，憲法上の最小化原則から導かれた一般的・探索的捜索・差押禁止原則に反する結果に繋がるという問題がある。

これに対して，本稿の立場は，次のようなものとなる（捜索の部分については，第２章で検討するため，ここでは，差押えの部分についてのみ述べる）。すなわち，本稿は，終局的処分権という新しい法益論により差押えを再定義しており，それによると，有体物に対する終局的処分権の剥奪は占有の剥奪という形となるのに対して，情報に対する終局的処分権の剥奪は情報をデリートするという形となって，理論上の一貫性が維持されている。そのうえで，情報を対象とする場合の正当な理由，特定性及び関連性要件と，有体物を対象とする場合のそれとは異なる点があるが，このような相違点に応じて，本稿は，情報の差押えの範囲を最小化するための非物理的限定要素を打ち出す一方で，多段階の規制をも用意しているから，最小化原則に反する一般的・探索的差押えになることはないのである。

第２款　蓋然性による差押えについて

以下では，蓋然性による差押えについて，本稿の理論と従来のそれとの重要な差異のみを敷衍する。

Ⅰ．多段階規制に基づく視点の有益性

単一段階の令状制度を採用している現行法のもとにおいては，蓋然性による差押えは，一般の差押令状の執行方法の１つとして扱われるにすぎず，また，その後に差し押さえられた物の中身を確認するにも別個の令状は不要であるとされている。しかし，この章で論じた通り，なぜ関連性を確認せずに蓋然性によって電磁的記録媒体を差し押さえることが認められるといえるのかについて，理論上は解決困難な点が残されているうえ，前段階の差押えでは関連性が確認されておらず，後の段階の捜索にも別個の令状が不要であるとすると，捜査への規制が失われてしまうという点(規制不能)が問題となる。

以上に対し，本稿の主張からすると，包丁というような物件に対し蓋然性による差押えを行う場合には，かかる物件には情報の膨大性ないし混雑性という特徴が存在しないため，

かような蓋然性による差押えは，一般の差押令状の執行方法の１つとして扱ってよく，また，その後にかかる物件の中身を確認するにも別個の令状は不要であるのに対して，サーバー記憶媒体などの大容量の記憶媒体ないし大量の書類に対する蓋然性による差押えの場合には，媒体の財産権と独立した，大量かつ混在する情報(電磁的記録媒体のデータ情報ないし書類の文字情報)に対する終局的処分権という法益があるため，蓋然性による差押えは，令状の執行方法ではなく，独立した処分になるから，それを行うには，一般の差押えと異なる要件が要求されるいわば「蓋然性による差押令状」を必要とし，そのうえで，その後に差し押さえられた媒体の中身を確認するためには，別個の情報に対する捜索令状が必要であることになる。

以上の通り，本稿の理論によると，後の段階による制約が用意されており，それによって，従来の関連性要件により提供される保護が実質的には維持されているかぎり，前段階における関連性の未確認という瑕疵が治癒されるから，従来の関連性要件に固執する必要はなくなる。

これにより，前述した２つの問題点が解決されると同時に，包丁などの物件を対象とする蓋然性による差押えの場合と大容量の電磁的記録媒体ないし大量の書類などの媒体に対する蓋然性による差押えの場合との区別を正当化するための理論上の論拠も提供される。

Ⅱ．従来の判例・学説との差異

本稿は，「関連性＝蓋然性」という構造を採用しているから，蓋然性による差押えの問題に決着を付けた日本の最高裁の平成 10 年決定並びに学説上の関連性緩和説と，蓋然性による差押えの許容性を認めるという結論部分では一致しており，この部分に限っては，それが台湾にも参考となるものがある。

しかし，本稿の理論は，この日本の見解とは，以下のような重要な相違点がある。すなわち，本稿の立場からすると，蓋然性による差押えの許容性を認めるための前提として，蓋然性により一時的・一括的に差し押さえられた媒体の内容を確認するという段階は，別個の令状により規制しなければならないのに対して，日本の理解は，蓋然性による差押令状という制度が存在せず，また，多段階令状による制約もなく，蓋然性による差押えを一般の差押えと同視したうえでその許容性を認めるものである。台湾の現行法は，この部分に関しては，この日本の理解と一致している。それは，中華民国憲法 23 条の最小化原則の要求を満たしていないものであると言わざるをえないのであり，それを是正するには新しい立法をもって蓋然性による差押令状並びに多段階令状という制度を導入しなければならない。

第２章　伝送中のデータと捜査手続

ここまでは，「蔵置されたデータ」を対象とする場面を検討したが，これからは，ここまでの議論をも踏まえたうえ，捜索・差押え及び検証という制度と並んで，捜査の手段としての通信傍受という制度も視野に入れて，「伝送中のデータ」を対象とする場面の検討に移りたい。

第１節　通信傍受とＩＴシステム

台湾においては，日本でいう「犯罪捜査のための通信の傍受に関する法律」（通称は，通信傍受法である）に相当するものと考えられる，いわゆる「通訊保障及監察法」（以下，通保法[483]という）という法律がある[484]。しかし，日本の通信傍受法が，専ら，伝送中のデータを対象とするものであるのに対して，台湾の通保法については，その文言上からみれば，伝送中のデータのみならず，一定の設備に保存されたデータをも対象とされているようにみえる[485]。ここで検討すべき問題としては，次の２つのものがあげられる。その１つは，保存されたデータを対象とする場合に，通保法に定められている通信傍受という制度が適用されるのか，それとも，刑訴法のいう電磁的記録に対する捜索・差押えという処分にあたるのかである。もう１つは，現行通保法は，果たして，ＩＴシステムにおいて流れているデータ通信を傍受するために機能するのかである。この２つの問題点を検討するに，日本における関連議論は台湾にも参考となると思われる。そこで，以下の検討では，日本の通信傍受法を主な比較の素材とすることにしたい。そのための具体例をあげると，以下のものとなる。

【例 6】「えさのメール」に対する傍受

Ｈは，「新規サービスへの移行のため，ＩＤ及びパスワードの再入力をお願いします」などと，Ｌ社のウェブサイトを装った偽のフィッシング・ウェブサイトへのＵＲＬリンクを貼った「えさのメール」をＬ社の会員に送りつけ，そのクレジットカード番号やイーバンク

---

[483] 通監法と略称するものがある（黄朝義・刑訴三版 286 頁）。

[484] 台湾の通保法と日本の通信傍受法との間には以下の２つの相違点があることを注意してほしい。第１に，通保法でいった「通信」とは，通信傍受法でいう電気通信のほかには，また，「郵便物及び書信」「言論及び会話」という２つの種類が用意されている（通保法 3 条参照）。ここでの検討では，電気通信以外の種類を論じる必要はない。第２に，本来，日本語でいう「傍受」という用語は，通保法のいう「監聴（すなわち，監視しながら盗聴することを意味する）」という中国語に対応するものであるが，この「監聴」は通保法のいう「通信監察」という行為の１つの「執行の方法」しかない。すなわち，通保法 13 条 1 項は，「『通信監察』の執行は，キャッチ，傍受（監聴），録音，録画，撮影，開封，検査，コピーあるいはその他類似する必要な方法をもって行う」と定められている。しかし，日本語では，台湾の通保法のいう「通信監察」という中国語に完全に対応する用語が存在しないし，また，ここでの検討は，電気通信の場面しか論じないから，翻訳上は中国語の「通信監察」を日本語の「通信傍受」と訳してもよいかと考える。

[485] 通保法 3 条 1 項 1 号においては，通信傍受の対象となる「通信」が，「電気通信設備を利用し，文字，映像，音声，あるいはその他の信号を発送，保存，伝送，あるいは接収する有線あるいは無線の電気通信」と定義されている。

のID及びパスワードを入手し，不正な送金や預金の引き下ろし，クレジットカードの偽造などに利用したりして，巨額の不法利益を得た。被害を受けた多数のＬ社の会員からの被害届を受けて，警察が捜査を開始した。

本件捜査により，「えさのメール」は，いわゆる匿名転送メールの仕組みを利用し，最初の発信元を隠しているものであることが判明した。捜査機関は，いかなる行動をとるべきであろうか。

第１款　メール傍受の捜査上の諸難点

まず，「えさのメール」は匿名転送メールである以上，第１章の【例 2】で論じた通り，最初の発信者を突き止めるために，トレース・バック捜査を行うことが必要となる。また，「えさのメール」の発信者Ｈが使っているメールボックスに残っているメールの内容を点検・検閲ないし取得しようとすれば，台湾において，実務上は，司法警察(官)が捜索(差押え)令状をもって当該メールボックスが設置されているサーバー記憶媒体に対する捜索・差押えを行うか[486]，それとも，検察官による無令状の検証という方法をとることになる。しかし，読み出したメールがすべて犯罪者のユーザーにより削除されてしまうことが多いから，通信履歴の保全要請や記録命令付き差押えだけでは足りず，メールに対する傍受が必須になる場合がある。

この点，日本の通説によれば，通信傍受法の要件を満たしている限り，メールに対して傍受を行うことが可能であるとされる[487]。しかしながら，既に指摘されてきたように，匿名メールの経路は多重の転送という形になっており，極めて複雑なものであるから，最初の発信者が特定できないため，こうした場合においては，傍受ができなくなるのである[488]。また，匿名メールの場合，仮に最初の発信元がわかったとしても，傍受すべき多重の転送経路を特定しておくのは現在の技術ではほぼ不可能であるから，日本の通信傍受法 6 条の要求する「傍受すべき通信」の特定ができなくなるではないかという点も問題である。

以上の指摘は台湾にも当てはまるものであると考えられる。というのも，メールに対する傍受の根拠は，通保法 3 条に求められており[489]，その一方で，同法 11 条３号により「傍受すべき通信」の特徴――具体的には，転送経路の種類(たとえば，携帯電話か市内電話か)やそれを示す番号(たとえば，電話番号)などがあげられる――の明記が要求されているが，傍受すべき多重のメールの転送経路を特定しておくのは現在の技術ではほぼ不可能であるとすれば，通保法の要求する「傍受すべき通信の特徴を明記しておく」こともできなくな

---

[486] 李如霞・犯罪偵査 4－83～4－84 頁参照。

[487] 井上・コンピュータ(1)58 頁＝井上・強制・任意 262 頁。また，水谷 189 頁，松井・インターネット人権 14 頁，田口・刑訴 6 版 104 頁をも参照。

[488] 牧野二郎・イー盗聴 131 頁参照。

[489] 林富郎・通訊監察 161～162 頁，呉兆琰・網路通信監察 37 頁。そして通訊保障及監察法施行細則 2 条をも参照。

るのではないかと思われるからである[490]。この意味では，現行通保法は，メールに対する傍受に十分に対応できていないということができよう。

第２款　電話回線通信傍受との差異

さらに，電話回線を対象とする傍受とコンピュータ・ネットワークを対象とする傍受との差異に着目して，通保法の適用範囲を再考すると，通保法の規定が，果たして，メールに対する傍受のような場面に適合するものかについてはなお再吟味の余地がある。というのも，通保法制定の過程において，コンピュータ・ネットワークからなるデジタル通信にかかわる問題については本格的な議論が全くなされておらず，実際にも，当時，立法当局がイメージしたのは，電話に対する盗聴というものであって[491]，デジタル通信の仕組みないしそれへの傍受の方法に関して，立法当局者も審議委員会のメンバーもほとんど理解していなかったのである[492]。こうして，通保法が，そもそも，電話通信回線に対する傍受のみを念頭に置いたものだとすれば，同法の規定を，そのまま，電話通信回線と異なる技術的な特徴をもつコンピュータ・ネットワークの傍受(監視・記録)に適用すると，噛み合わない部分が出てくることが当然に予想される。

この点，日本においても問題背景としては類似するものがある。すなわち，すでに指摘されているように，「通信傍受法制定の過程でインターネットの問題が本格的に議論の対象となったのは，衆議院の最終盤の審議に入ってからであった。それまでは，インターネット通信の認識は希薄で，立法当局者，法制審議会メンバーにはほとんど理解できていなかった。立法当局の頭にあったのは，通常の固定電話の会話の盗聴であって，今まで『検証令状』で行ってきた行為であった。」[493]

以上のとおり，日本と台湾とは，問題背景としては共通するし，また，傍受するために必要な法的根拠の内容についても似ている箇所が見られる。そこで，以下では，電話回線通信システムとＩＴ通信システムの差異に着目し，日本における通信傍受法を巡る関連議論を参考に，台湾における通保法の問題点を改めて検討してみたい。その際に，ここでの検

---

490 類似する指摘として，李・電信 54 頁の説明(スカイプを傍受する事例)をも参照されたい。

491 立法院公報 82 卷 48 期 2647 號下冊 253 頁[趙少康(国会議員)發言]，同公報 82 卷 48 期 2647 號下冊 252 頁以下[陳癸淼(国会議員)発言，林錫堯(立法当局代表＝法務部参事官)発言，蘇煥智(国会議員)発言]参照。

492 立法院公報 83 卷 74 期 2748 號下冊 97～98 頁[蘇煥智(国会議員)発言]参照。

493 牧野二郎・イー盗聴 124 頁。また実際にも，日本においては，国会への通信傍受の実施状況報告をみると，インターネット傍受に関する報告は１件もない(「通信傍受の実施状況等に関する公表」につき，海上保安庁HP (広報資料：報道発表資料：平成 12 年中～同 24 年中)， 厚生労働省HP (報道発表資料：平成 13 年中～同 24 年中)や法務省HP (プレスリリース：平成 21 年中～同 24 年中) にて入手できる(調査日：2013/03/27)。これまでの公表結果を簡要に整理したものとして，田口・刑訴 6 版 109 頁参照)。台湾の場合にも，インターネット傍受に関する報告は一件もない(台湾では，通信傍受の実施に関する公表の義務が付けられていないが，2002 年に公布された法務部年度通訊監察報告及び 2008 年～2012 年の司法統計年報参照。また，李如霞・犯罪偵查 4-20～4-21 頁，李・電信 54 頁；呉兆琰・網路通信監察 58 頁をも参照されたい)。

討に必要な程度においてかぎり，捜索・差押え及び検証に関わる部分をも言及する。

Ⅰ．待ち受け型の傍受

ＩＴ通信システムの一種類であるインターネットを傍受しようとする場合,その１つの手段として，いわゆる「待ち受け型の傍受」が挙げられる。ここでいう待ち受け型の傍受とは，通信経路を対象として伝送中のデータをとるという厳格な意味での傍受ではなく，通信の到着先であるメールボックスを対象として着信したばかりのデータを取得するという意味での傍受である。

この点，既に指摘されている通り，待ち受け型の捜査も，検証としては，既に電話の検証において認められているところであるから，それが，一般的なネットワーク通信において認められないという理由はないであろう[494]。そして，こうした待ち受け型の傍受は，「伝送中のデータ」を対象とするものではないから，それは現行の通信傍受法によって規制するところでないと解されている[495]。

この日本の理解は，台湾にも解釈論の１つの可能性として取り入れることが考えられるはずだろう。というのも，台湾のいう捜査の手段としての検証は，令状によらない点で日本のそれと異なるものであるが，その定義自体は，日本の検証のそれと同様であるし，また，通信の秘密のいう「通信」は，従来は，進行中のコミュニケーションに限られると解されてきたからである[496]。

しかし，台湾の先行研究において，一般論としては，通保法３条の文言により，同法は，伝送中のデータのみならず，一定の電気通信設備により保存されたデータをも対象としていると解されてきた[497]。これに従えば，待ち受け型の傍受は，「伝送中のデータ」を対象とするものではないが，それは，現行通保法のいう「保存されたデータ」を対象とする場面にあたるものであると解されうる。しかし，他方で，2001 年の台湾刑訴法改正により，電磁的記録も捜索・差押えの対象として列挙されていることからは，ＩＴ通信システムにおける「保存されたデータ」を対象とする待ち受け型の傍受を，現行刑訴法の検証ないし捜索にあたるものであると解する可能性もあると言わなければならない[498]。そこで，学説上，保

---

494 川出・コンピュータ犯罪 24 頁注(22)。

495 日本の通説によれば，メールボックスに到着した未読のメールは，基本的に，私書箱に届いた郵便物と同様に考えてよく，通信傍受の対象ではないとされる（井上・コンピュータ(1)59 頁，安富・刑訴法 183 頁，小木曾 211 頁，審議会(ハイテク)第４回議事録参照)。

496 林富郎・通訊監察 8～9 頁参照。

497 蔡耕榮・修正後通訊(上)52～53 頁。これに対して，本稿は，通保法のいう「保存」を，「伝送のために保存された通信のデータ」と解すべきであろうと考えている。というのも，ITシステムにおける情報を伝送する仕組みは，一連のコピー(言い換えれば，一時的な保存)の繰り返しによるものであるし，また，このように解すると，憲法上の権利としての通信の秘密のいう通信の定義にも叶うものだからである。

498 もちろん，傍受は，物理的な侵入を必要な要件とした伝統的な家宅捜索のいう捜索の定義に該当しないが，先行研究においては，アメリカの合理的なプライバシーの期待をもって台湾刑訴法のいう捜索を再定義したうえ，傍受も刑訴法のいう捜索の一態様にあたるものと解する論者がある(謝・合理隱私期待 160 頁)。

存されたデータを対象とする場合には，通保法あるいは刑訴法のどちらを適用すべきかという点が問題として提起されている[499]。

それゆえ，捜査機関が，「えさのメール」の発信者Hのメールボックスを監視しながらその中身をキャッチしようとするここでの例を，台湾の場合に当てはめて採用可能な捜査手段を考えると，検証，捜索ないし傍受という３つの選択肢があげられる。というのも，検証や捜索という手段をとる場合には，形式的には「伝送中のデータ」を対象とする意味での通信傍受にならないが，「到着したばかりのデータ」をキャッチすることができるとすれば，実質的には，「伝送中のデータ」を対象とする意味での通信傍受と接近する，ないし同じ効果を有するものと評価することができる一方で，「到着したばかりのデータ」が通保法のいう「保存されたデータ」にあたるものと考えられるからである。こうして，検証，捜索や傍受のいずれに対しても，実質的には同じ効果を持っているものであると評価することが可能なのだとすれば，通保法よりも，検証または捜索による待ち受け型の傍受のほうがより魅力的であるということができよう。というのも，検証のほうは，検察官の職権だけで行われるものであって令状は不要であるし，また，捜索令状を取る場合，その発付要件は，通保法により要求される通信傍受令状のそれよりもはるかにクリアしやすいものだからである。そうすると，ここで問題の核心は，到着したばかりのデータをキャッチする場合にも検証ないし捜索による待ち受け型傍受を活用することが認められるとすれば，これによって，通保法の要求される厳格な傍受令状の要件が回避されることになるのではないかという点にある。

しかし，台湾においては，通保法成立以前の電話傍受の根拠につき，その理解は，日本のそれとは異なるものがある。当時は，その根拠は一応刑訴法に求められると解されてきたが[500]，具体的には一体同法の何条がその根拠になりうるかについては争いがあった。主に，①対人処分（現行犯逮捕の台湾刑訴法 88 条 1 項，緊急逮捕の同法 76 条及び 88 条の１）の類推適用説[501]，及び②対物強制処分（家宅捜索の同法 122 条 1 項，有体物に対する差押えの同法 133 条）の類推適用説[502]の２つの立場が対立していた。つまり，台湾の場合においては，

---

499 陳瑞仁・新法捜索扣押 55 頁，許・電磁記錄捜索扣押 123～124 頁参照。

500 通保法以前にも電話傍受という捜査手法がすでに頻繁に使われており，しかしその法的な根拠は何のかについては厳重に疑問視されていたが，当時法務部は刑事訴訟法を根拠に，「検察機関が通信傍受の作業を実施するための執行の要点」「国内犯罪のための通信傍受の作業の執行」という２つの行政命令を頒布し，それをもって，通信傍受という手法を正当化するための根拠としていた（林富郎・通訊監察 8～9 頁，江・監聽理論實務 111 頁参照）。これに対して，行政命令による通信傍受は憲法の保障する通信の秘密の自由（中華民国憲法 12 条）を侵すものとして厳しく批判されていた（林山田・程序法５版 359 頁，林富郎・通訊監察 154 頁，鄧湘全・通訊監察 106 頁参照）。そこで，1999 年に通保法が新設されたことに至った。

501 これは，当該者の身柄拘束さえ認められれば，その人の犯罪のために使われた道具である電話を傍受することもできるという理解である。これに対して，対人処分の対象は人であり，これと，電話傍受の対象とは異なるから，類推適用をしかねるとする論者がある（林富郎・通訊監察 18，143～144 頁，また同 8，9，14 頁をも参照）。

502 すなわち，電信局の電話を捜索・差押することさえできれば，その電話の内容を処分の対象にしてもよいという理屈である。これに対して，同前掲注林富郎論文 143～144 頁は，捜索・差押えは有体物を対象とし，その実施は一回でかつ公開性を有するのに対して，傍受は無体物を対象とし，継続的かつ密かに行われるので，両者は異質のものであるから，類推適用ができないと批判する。同見解として鄧湘全・通訊監察 106 頁参照。

もともと，日本でいう，いわゆる検証による電話傍受という発想が存在していなかったのである。その理由としては，次のようなものが考えられよう。

まず，台湾のいう検証は，日本のいう検証と同様に，捜査の手段としての強制処分の実質を有するものの，それは令状によらないものであるし，また，条文の配置も，対物強制処分でなく，証拠調べのところに置かれている。加えて，検証には，その対象は有体物に限られ，その目的は，犯罪証拠の発見でなく，すでに発見した証拠物の内容を認識する点にあると解される[503]。そこで，台湾では，検証という制度は，本質的には，無体の会話を対象として犯罪証拠の発見を目的とする通信傍受という手法には相応しくないものであると考えられてきた。

以上によれば，台湾の現行法のあるべき解釈論としては，検察官による無令状の検証という形での待ち受け型傍受を行うことはできないと解されるべきであろう。このように解すると，前述した，通保法で要求される厳格な傍受令状の要件が回避されるという点が問題でなくなる。

他方で，台湾刑訴法の(電磁的記録に対する)捜索による待ち受け型傍受と解することは可能なのか。この点，特別法が一般法を優先する法理により，通保法の規定(保存されたデータを対象とする傍受の類型にあたる)が適用されるという考えもありうるであろう[504]。しかし，このように解すると，到着した後，既に一定の時間に渡って一定の媒体に蔵置されたデータを点検・取得するような場合においてすらも，通保法の通信傍受令状が適用されてしまうという帰結となり，これは捜査に対する不適切かつ不必要な過剰規制であるといわなければならない。というのも，こうした場合に侵害される法益の内実は，到着したばかりのデータのキャッチを内容とする待ち受け型傍受の場合に侵害されるそれとは異なり，むしろ家宅に置かれたコンピュータ媒体に蔵置された電磁的記録を点検・取得される場合に侵害される法益の内実に接近するものだからである。つまり，これは傍受の実質を持たない場合であるので，こうした場合を厳格な傍受令状により規制する必要性ないし正当性はないと考えるからである[505]。

以上により，台湾の現行法のもとにおいて提起されてきた，「保存されたデータを検索・取得することが一体，刑訴法のいう捜索・差押えや検証に該当するか，それとも，通保法のいう通信傍受に属するか」という法適用の問題を解消しようとすれば，日本法の設計が

---

503 陳樸生・刑訴(重訂十版)252 頁。

504 実際にも，先行研究においては，通保法という法的根拠がある以上，傍受を行うには，捜索令状によってはならず，通保法のいう「監察書」(すなわち，日本の場合の通信傍受令状)の発付を得るべきであると解するものがある(簡・捜索要件 30～31 頁)。

505 この点，井上教授が指摘した通り，「通信傍受の手続がそのようにより厳格なものとされたのは，通信秘密を侵害する処分だからということではなく，むしろ，傍受が行われる通信設備において傍受期間内にいかなる範囲の人の間でどの程度頻繁に通信がなされるかを確実に予知することはできず，その意味で，対象が物理的に一定の範囲に限定されている通常の捜索や検証の場合に比べ，プライバシー侵害の範囲がより広く及び得るという点に主たる理由があったというべきであります。(井上・コンピュータ (1) 59 頁。同・傍受 50～52 頁をも参照。)」。これによれば，到着した後既に一定の時間に渡って一定の媒体に蔵置されたデータを点検・取得する場合は，「傍受が行われる通信設備において傍受期間内にいかなる範囲の人の間でどの程度頻繁に通信がなされるかを確実に予知することはできない」という特徴が存在しないので，プライバシー侵害の範囲がより広く及び得ることにはならないから，通常の捜索や検証の場合と同じ規制をすればよく，厳格な傍受令状による規制は必要ではないという帰結になる。

参考になるだろう。すなわち，立法論としては，保存されたデータは，電磁的記録として，刑訴法における捜索・差押えないし検証という制度により対応されるものとするのに対して，通保法の規制対象を，もっぱら，伝送中のデータに限るものとすることにより，前述した法適用の問題がなくなると思われる。しかしこのような立法設計をとると，傍受の実質を持つ，いわゆる待ち受け型の傍受は，形式的には伝送中のデータを対象とするものではないから，それは通信傍受に当たらないという帰結にならざるを得ない以上，通保法で要求される厳格な令状の要件が回避されてしまうという点が問題となってくる。

Ⅱ．一網打尽型の傍受

前述した匿名転送メールの場面にかぎらず，インターネットの仕組みの特徴ゆえに，一般のメールないしデータの伝送の場面においても，複雑な多重の転送経路になりうる。この場合，傍受すべき多重の転送経路を特定しておくのは技術上ほぼ不可能であるが，あらゆる可能な経路の経過点に専用プログラムをインストールしてインターネットの全体には引き網を張って傍受(監視・記録)を行うことは，技術的に可能であるし，実行上も困難ではない。かような手法を「一網打尽型の傍受」と呼び，これが， インターネットの傍受のもう１つの手法として考えられる。この一網打尽型の傍受を採用すれば，【例 6】の「えさのメール」傍受が可能になる。

ここで検討すべきは，通保法を，複雑な多重の転送経路になっているインターネットの場面に適用させるために，一網打尽型の傍受を認めてもよいかという問題である。この点，台湾の通保法 8 条でいう「傍受すべき通信」が，固定電話の個別の通信回線を単位として特定されるものであるとすれば[506]，すべての(ネット上の仮想)回線を対象とする一網打尽型の傍受は同法の範囲外にあるものと解すべきではないかと思われるが，従来は，この点についての議論は十分に尽くされていない。

Ⅲ．物理的な特徴に依存する必要性の有無

前にも指摘したように，通保法は，立法当時は，電話傍受の場面を主にイメージして作られたものであるから，通信傍受という捜査の手法は無体の情報(会話やデータなど)を対象とするものであるといいつつも，結局のところ，その適用はやはり電話回線やその設備などの有体物にかかわる物理的な特徴に依存することが前提とされている。そのため，通保法は，物理的な特徴に依存しない場面には十分に対応できていないという問題点がある。

この点をより具体的にいえば，まず，通説によると，通保法による傍受の対象は，無体物と有

506

http://www.lawtw.com/article.php?template=article_content&area=&job_id=161187&parent_path=,1,2169,1481,&article_category_id=2206&article_id=88622(法務部檢察司 99 年6 月8 日新聞稿)，林富郎・通訊監察 145～146 頁参照。

体物との双方が含まれているとされる[507]。前者について，具体的には電話通信会話が想定されているが，後者なら，電話器機などの通信設備が考えられる。他方，同法は，通信傍受令状(通訊監察書)において明記すべき事項として，「①案由[508]・罰条，②傍受すべき対象者，③傍受すべき通信の種類及び番号など識別に資する特徴，④傍受すべき場所，⑤傍受すべき理由[509]，⑥傍受の時期及びその方法，⑦傍受(令状)を請求する機関，⑧(傍受を)執行する機関，⑨(傍受の)設備を整える機関[510]。」(通保法 11 条 1 項)の 9 つのものがあげられている。

以上のとおり，無体の「傍受すべき通信」は，通保法における処分の対象であるとされつつも，それ自体は，令状の必要的記載事項となっていないのである。そうすると，傍受の対象となる通信それ自体も特定すべきなのかという点が問題となる。この問題は，通保法の審議の当時にすでに提起されており[511]，具体的には，次のような発言がなされた。

「傍受すべき対象者[512]に対して傍受を行うとき，傍受の範囲[傍受の対象となる通信それ自体の範囲をさす]を明らかにしておくべきではないでしょうか。……細則のなかにおいて……傍受の事項・範囲を説明すべきであって，そうしないと，必ず濫用される。(台湾の国会議員の蘇嘉全の発言)」[513]

しかし，結局のところ，最後に成立した細則においても，傍受の対象となる通信自体を特定するような規定は置かれないことになった。なぜならば，立法当局は，傍受の対象となる通信の範囲は，すでに同法 11 条 1 項 3 号傍受すべき通信の種類ないし番号などの識別特徴(前掲③)及び同条項 6 号の傍受期間及び方法(前掲⑥)により画定されているものである以上，通信自体(たとえば如何なる内容の通信会話)をさらに特定する必要はないと考えていたからである[514]。

しかし，後述する日本の関連議論に照らして再考すると，現行の通保法が要求するこの程度で，果たして，傍受できる通信の範囲がすでに特定されているといえるのかについてはなお再検討の余地があるように思われる[515]。

まず，日本の通信傍受法の立法過程においては，傍受の対象となる通信をどの程度特定すべきかが争われてきた[516]。学説上は，「どのような内容の通話・会話かを具体的に記載することが要

---

507 林富郎・通訊監察 16 頁。

508 これを日本法で言い換えればと，「罪名」に該当する概念であり，具体的にいえば，「違反毒品危害防制條例由(麻薬や覚せい剤などによる危害を防止するための条例に違反する事件)」がここでいう「案由」の一例としてあげられる(林鈺雄・搜索扣押 91 頁を参照)。

509 ここでいう「理由」とは日本の場合の「犯罪事実」に近い概念である。

510 傍受の内容に接触することもなく，単純に傍受するために必要な器機設備やソフトなどを提供する機関をさす(林・刑訴概論(上)11 版 354 頁参照)。

511 立法院公報 83 卷 4 期 2678 號下冊 83 頁。

512 被疑者や被告人以外には関係第三者にも含まれるとされる(通保法 4 条，5 条，7 条参照)。

513 立法院公報 83 卷 4 期 2678 號下冊 83 頁。

514 立法院公報 83 卷 4 期 2678 號下冊 83 頁[林錫堯(立法当局代表＝法務部参事官)の発言]参照。

515 林裕順・基本人權 135 頁は，現行通保法の規範内容は「無体物」をいかに明確・特定するかという点を明らかにしていないのが問題であると指摘する。

516 通信傍受法第 6 条で，「傍受令状には，……傍受すべき通信，傍受の実施の対象とすべき通信手段，傍受の実施の方法及び場所……」を記載すべきものと定めている。これによれば，広い意味での通信傍受の対象には，「傍受すべき通信」と「傍受の実施の対象とすべき通信手段」の 2 つが含まれることになる。ここでいう「傍受すべき通信」とは，通信会話という情報を意味し，「傍受の実施の対象とすべき通信手段」の具体的な例としては，電話回線などの通信設備が想定

求される」とする少数説もあった[517]。これによれば，前掲③と⑥(通保法 11 条 1 項 3 号と 6 号)だけでは，傍受の対象となる通信自体はまだ特定されていないと言わなければならない。

これに対し，日本において支配的なものであるとされる，井上教授が示した以下のような見解は，台湾の通保法の立法当局側の考えに近い立場であるように思われる。

「……電気通信や会話の傍受についても，従って，当の通信設備(電話機･回線等)や場所が専ら当該犯罪の実行や準備，共犯者間の連絡などに用いられており，それを介して行われる通信，あるいはそこで行われる会話はすべて，当該犯罪に関係するものである蓋然性があると認められる場合には，その通信設備あるいは場所が特定されている限り，そこにおけるすべての通信ないし会話を傍受することを許したとしても，特定性の要件に欠けるところはないといってよいように思われる……いずれにせよ，しかし，少なくとも，『事件』の内容が適切に示されていれば，上記のような受け皿的語句でも，特定性の要件を満たし得るという点では，大方の意見は一致しているのである。これと同様に考えると，電気通信や会話の傍受についても，被疑事実が特定され，その性質･内容や当該通信設備ないし場所との関係などから，当該事件に関連する一定の趣旨･性質の通信ないし会話がなされる蓋然性があると認められる場合には，例えば，『〔これこれの趣旨の〕通信ないし会話』，さらには，『本件犯行に関係する通信ないし会話』といった表示でも，それに該当する通信ないし会話を合理的に識別できると認められる限り，特定性の要請は充たされているといってよいように思われる。」[518]

この見解は，「傍受の実施の対象とすべき通信手段」(通信設備)ないし「傍受すべき場所」などの物理的な特徴の明記に加え，「事件」をも記載することにより「傍受すべき通信」と「そうでない通信」とを合理的に識別できると認められる限り，対象となる通話・会話自体を具体的に特定する必要がないというものである。つまり，当該通信設備ないし場所を特定すること及び事件との関連性を媒介として，傍受すべき通信が特定される――特定性の要件を満たすといえる――という理解になろう。

以上に示した井上教授の見解を台湾の場合にあてはめると，傍受すべき通信を特定するための要素としては，通保法の立法当局の説明においてあげられた前述した③と⑥だけでなく，その①②④⑤⑨も含まれるものとなる。すなわち，井上教授の見解に従い分類すると，①②⑤を「事件との関連性」というカテゴリーに，③④⑨を「通信設備ないし場所」というカテゴリーにいれることができ，そしてこの２つのカテゴリーをもって，傍受の対象となる通信が特定されるといえる。

しかし，このように解すると，ＩＴシステム通信の傍受のように，通信設備ないし場所などの物理的な特徴に依存しない場面で行われる通信傍受については，現行の通保法は対応

される。

[517] 三島219～220頁。同趣旨の見解として，小田中・盗聴の違憲性61～62，74～78頁；川崎・憲法的問題点49～52頁(小田中ほか・盗聴立法批判87頁以下収録93～95，99～102頁)；川崎・盗聴129～130，133～134，148～150頁；三島・盗聴立法(下)90～91頁等がある。

[518] 井上・傍受 43，46～47 頁。

できないのではないかという疑問が生じる。この点，まず，台湾の先行研究においては，通保法による傍受の範囲を画定するには，前述した井上教授が提供した２つのカテゴリーに沿って，日本の現行通信傍受法のもとにおいて打ち出されてきた，①外形的な限定，②通信・会話の性質や当事者別などによる限定，③スポット・モニタリングによる限定，という３つの最小化の方策[519]を採り入れているようにみえる論者がある。すなわち，「傍受を執行する捜査員は，傍受を始める際に，会話の内容を大雑把に審査しておくことができ，それによってはかかる会話が対象犯罪と関係があるかどうかを判断し，関係があることが確定された場合にのみ，当該通信に対する傍受を継続することができるが，逆に，それが対象犯罪と関係がないと判断された場合には，通保法においてはそれについての明文がないものの，かかる傍受を即時に切断しなければならないと解すべきである。」[520]

しかしながら，この見解が示した最小化の方策は，以下に分析するとおり，有体の電話回線や無体の物理的なエネルギーであるアナログの音声などの物理的な要素や特徴に依存しないＩＴシステムの場合には役立たないものになってしまうのである。

１．外形的な限定

伝統的な電話回線の場合においては，通信回線をあらかじめ確保しておく仕組みになっており，傍受の対象とする通信経路を事前に予測することができるので，「目的とする通信・会話がなされる蓋然性の高い時間帯に絞って傍受を行わせる」[521]こと(外形的な限定)[522]が可能である。

これに対して，分散システムかつパケット交換技術を採用しているＩＴシステムの場合には，(仮想的な)回線をあらかじめ確保しておらず，コンピュータ・システムの自律性により最も効率的な伝送経路を送出の時点で自動的に判断し，その判断と同時に当該経路でパケットを送出するという情報伝送の仕組みになっているので，それを傍受する場合に，その時間帯や経路を事前に予測しておくことは，現時点の技術では不可能である[523]。それゆえ，ＩＴシステムの場合に，目的とする通信・会話がなされる蓋然性の高い時間帯に絞って傍受を行わせることはできない。

２．通信・会話の性質や当事者別などによる限定

伝統的な電話回線の場合，その対象は無体物であるが，当該無体物は物理的なエネルギーであってすなわち人間が認識できるアナログ量の音声であるから，電話回線を傍受する

---

519 井上・傍受 186 頁。

520 黄朝義・刑訴三版 308 頁。

521 同前注。

522 かかる外形的な限定という方策は，「傍受の実施に当たっては，警察本部長は，あらかじめ，次に掲げる事項について，捜査主任官に対し，文書により指示しなければならない(柱書き)。…三　前二号に掲げるもののほか，傍受の実施の適正を確保するための事項」と規定する通信傍受規則６条１項１号により実現することができる。

523 See Lessig, at 63＝邦訳：山形浩生，柏木亮二（訳）89 頁；また，大橋・基礎編 61 頁(注 49)及び同 222 頁以下の説明，井上伸雄 12 頁；同・通信技術のすべて 122～125 頁；村田 6，31，118 頁；ウィキペディア―サーチワード：ルーティング，パケット通信，データリンク層，ルーターをも参照。

場合には，人間の捜査官が自分の耳で音声を聞きながら，当該通話と被疑事実との関連性を判断することができる。この意味で，「当該事件の性質や規模，目的とする通信・会話の性質，予想されるその当事者などと対照し，個々の通信・会話の当初の内容から推認される当該通信会話の性質やその当事者などからみて，無関係であると認められるときは，傍受を打ち切らせる」[524]という最小化の方策も，ある程度役立つだろうと思われる。

これに対して，ＩＴシステムは分散システムとパケット交換技術を採用しており，伝送するデータをパケットに分解し，これらの分解した複数のパケットをネット上にある複数の通過点を経由し同時あるいは非同時に送出する仕組みになっているため[525]，人間の捜査官が，五官を用いて自らパケットの内容を感知しながら，当該パケットと被疑事実との関連性を判断していくことはありえない。

また，回線電話は回線伝送及び中央システムを採用しているから，傍受の対象たる通信の回線を事前に予想することができ，それのみを対象に傍受を実施すれば済むのに対し，ＩＴシステムの場合には，仮想的な回線として利用される可能性のある複数の通過点に地引き網を張って複数の人々のすべてのパケットをスキャン（傍受）しておかなければ，傍受の目的を遂行することができない。

このように，通信・会話の性質や当事者別などによる限定という方策は，ＩＴシステムの場合，全く機能しないと言える。

３．スポット・モニタリングによる限定

最後に，スポット・モニタリングによる限定という方策については，これも前述した「２．通信・会話の性質や当事者別などによる限定」のところと同様の構造上の問題点を持っている[526]。

まず，伝統的な電話回線の傍受の場合には，人間が認識できるアナログ量である音声を対象とするから，警察官の耳で音声の意味を認識することができるので，断続的に聞いたり関連性を確認したりすることが可能である。この点は，前述した通り，通信・会話の性質や当事者別などによる限定という方策が機能する前提であると同時に，スポット・モニタリングによる限定という方策が機能する前提にもなっている。

これに対し，ＩＴシステムを傍受する場合は，傍受の過程に捜査官の五官が全く関与せず，

---

[524] 井上・傍受 186 頁。この通信・会話の性質や当事者別などによる限定という方策は，前掲注 522 に挙げた通信傍受規則 6 条 1 項 1 号の規定に加え，「前二号に掲げるもののほか，傍受の実施の適正を確保するための事項」という同条項 2 号の規定，及び「スポット傍受に当たっては，犯罪の組織的背景，既に傍受をされた通信の内容その他スポット傍受をしている通信の該当性判断に資する事項を考慮しなければならない」と規定する同規則 11 条 2 項ないし「スポット傍受をしている場合において，第四項各号のいずれにも該当しない通信であって傍受すべき通信に該当しないことが明らかであるものが行われていると認めるに至ったときは，直ちに，スポット傍受を終了しなければならない」と規定する 11 条 7 項等により実施することが可能であろう。

[525] 非同時送出とは，コンピュータ・システムの自律性により，伝送の効率に鑑み，パケットの一部だけを先に送って残りを待たせる必要があると判断される場合をさす（井上伸雄・通信技術のすべて 124～125 頁参照）。

[526] 三島・盗聴法解剖 55～56 頁にも，電子メール傍受の場合にはスポット・モニタリングが不可能であると指摘していたが，かかる不可能の技術上の理由を敷衍していない。

すべてをネットワーク・スニーフェル・プログラムのようなツールによる自動作業に任せることになるので，聞きながら関連性を確認し，関連性がないと判明された時点で聞くことを打ち切らせることは全く不可能である。

さらに，ＩＴシステムの場合には，流通中のすべてのパケットをスキャン(監視・傍受)しておく必要があるところ，「断続的に聞く」(断続的にスキャン)という方式にすると，元のデータに還元するために必要なパケットを取り落としてしまう危険性があり，ＩＴシステムの傍受という目的を達成することもできなくなってしまう。

このように，スポット・モニタリングによる限定という方策も，ＩＴシステムの場合においては機能しないものである。

４．小結

以上から，次の２つの点が明らかになった。

第１に，確かに，事件との関連性という要素は，ＩＴシステムの場合にも適用されうるものであろう。しかし，台湾の現行法のもとで，事件との関連性という要素による限定は，あくまでも，傍受の実施の対象とすべき通信手段(通信設備)ないし傍受すべき場所などの物理的な特徴による限定(特定)を補完する機能を果たすものにすぎない。言い換えれば，主な限定要素である「物理的な特徴」が機能しない場合には，補完的な限定要素である「事件との関連性」を明記したとしても，特定性の要件を満たすことはできないのである。

第２に，確かに，伝統的な電話通信を傍受の対象とする場合においては，有体の電話回線や無体のアナログの音声などの物理的な特徴に依存しているから，①外形的な限定，②通信・会話の性質や当事者別などによる限定，③スポット・モニタリングによる限定，という３つの物理的な限定方策をうまく組み合わせれば，ある程度，傍受すべき電話通信を最小化することが可能である。これに対して，ＩＴ通信に対する傍受の場面では，物理的な特徴に依存しないから，この３つの物理的な限定方策のいずれについても役立たないものとなってしまう。

第２節　ＩＴ通信の多様性に対応しきれない捜査の苦境

インターネットの傍受は，メールに対する傍受に限らず，その類型は多様多端に渡るものであるから，現行の通保法ではそれらに対応しきれないのが現状である。これを説明するに１つの典型例をあげると，次のようなものとなる。

【例７】ブログに対する傍受

ある男性Ｋは，「ウタマロの波動砲」というハンドルネームを使用したいわゆる「買春ブログ」を開設し，300 回以上行った自らの買春行為をブログで詳しく紹介するとともに，

デジカメで撮影したわいせつ画像 1700 枚と，体験記 150 編を同ブログで掲載していた。同ブログは極めて人気があり，捜査官が当件捜査に着手した時点までのアクセス数は 42 万 5000 件にも達していた。Kは毎回，写真付きという形で，買春した場所，値段，交通手段，セックスしてもらった相手の特徴及びそれへのコメント，セックスの行為の過程などを詳細に書きこんでいたことから，捜査機関はKのブログを手掛かりに売春組織の摘発にも乗り出そうとしている。

以下では，この事例において捜査官はいかなる捜査を展開すべきであろうかを検討する。

第１款　インターネットにおける通信と通信当事者の意味

日本において通説によれば，メール等のインターネット通信に対する傍受も，通信傍受法の適用対象であるとされ[527]，この点，台湾の通説も同解である[528]。しかし，ブログ，掲示板などについては，果たして，現行の通保法をもって，それらへの傍受(監視・記録)を行うことができるかは疑問があるように思われる。というのも，従来の電話回線でいう通信とは，1 名の発信者と 1 名の受信者間におけるコミュニケーションと理解される[529]のに対して，インターネットの場合の通信ないし通信当事者の意味は，電話回線の場合のように明瞭ではないと思われるからである[530]。

この点，前掲の【例 6】のメール傍受の例は，1 名の発信者と 1 名の受信者間におけるコミュニケーションという定義にあてはまる。また，日本においては，通信傍受法は，必ずしも，1 名の発信者と 1 名の受信者間におけるコミュニケーションに限らず，複数の特定個人間の閉ざされた情報の送受信にも適用されると解されてきた[531]。もし，この理解が台湾の通保法にも適合するものだとすれば，前述した定義の問題が解決されるかもしれない。

しかし問題は，【例 7】の事案は，1 名の発信者と 1 名の受信者間におけるコミュニケーションにあたらないのはもちろんのこと，複数の特定個人間の閉ざされた情報の送受信にも該当しないのである。というのも，インターネットの通信は，そもそも，「特定」，「閉ざされた情報」という２つの要件を満たさないものだからである[532]。

ブログにはさまざまな種類があり，それぞれに公開範囲(アクセス権限)を設定できるオプションが提供されている。そこで，本件の「ウタマロの波動砲」ブログのアクセス権限設定機能として，①「公開」(インターネット上で誰でもアクセスできる)，②「限定」(ア

---

527 水谷 189 頁。松井・インターネット人権 14 頁，田口・刑訴 6 版 104 頁をも参照。

528 林富郎・通訊監察 162 頁。

529 Korge, S. 11.

530 阪本・プライヴァシー権論 232～233 頁及び新保史生・プライバシー380，381 頁でなされた通信の定義は，いずれも，送受信者をコミュニケーションする主体(通信当事者)として，それらを通信手段の運営者から区別する点で共通している。

531 松井・インターネット人権 11 頁。和田ほか・情報 103 頁＝原田三朗ほか・新情報 146 頁をも参照。

532 松井・インターネット 292～293 頁，堀部(編著)・インターネット[堀部]38 頁。

ドレス帳におけるすべての知り合いがアクセスできる，あるいはアドレス帳におけるお気に入りの知り合いのみがアクセスできる)，③「非公開」(自分しかアクセスできない)との３つの選択肢が用意されているものと仮定しよう。Kは，前述のわいせつ画像 1700 枚のうち，1500 枚は，アドレス帳におけるすべての知り合いがアクセスできるパターンに，この 1500 枚をも含めた 1600 枚は，アドレス帳におけるお気に入りの知り合いのみがアクセスできるパターンに設定したが，残りの 100 枚は，「非公開」にした。また，体験記 150 編については，そのすべてをアドレス帳におけるお気に入りの知り合いのみがアクセスできるパターンに設定した。ただ，同 150 編のタイトルのみは，「公開」設定をした。

本件が検挙されるに至ったきっかけは，「ウタマロの波動砲」というハンドルネームを不審に思った捜査官Ｓがさらに体験記 150 編のそれぞれのタイトルを見たところ，それはいずれも一見明白のわいせつ性をもつ怪しいものであったことである。Ｓは，当のブログは，いわゆるわいせつの記述や写真の散布ないし売春紹介に関するブログであると判断し捜査に着手すると同時に，Kのブログを手掛かりに売春組織の摘発にも乗り出すことになった。

Ｓは，Kの身元の突き止めを急ぐと同時に，同ブログを監視・記録(傍受)する捜査にも着手した。ここで取り上げるのは，捜査機関が，通信傍受法をもって，Kのブログを傍受(監視・記録)することができるかという問題点である。この点を，前述したアクセス権限設定機能の３つのオプションに沿ってさらに具体化すれば，次のようなものになる。

まず，①の場合は，インターネット上で誰でもアクセスできるように設定しているから，その監視・記録は任意処分となる。しかし，だからといって，捜査機関が長期間にわたって，常時，体験記の更新履歴及び内容(タイトル)を監視・記録してもよいのであろうか。この点，日本の判例・通説は，任意処分であっても，警察活動一般を規律する警察比例の原則による制約があり，社会通念上相当と思われる合理的な範囲内に限られなければならないとしている[533]。この見解に従えば，本件の体験記の更新履歴及びタイトルは，「公開」設定とされているのみならず，わいせつな内容を含んだものであり，Kの犯罪ないしその背後の売春組織の摘発という正当な目的に基づくことから，それに対する捜査官の長期間の監視・記録行為は，警察比例の原則ないし社会通念にかなうものと解されるだろう。

この日本の理解は，以下の理由で，台湾の場合にも通用するものであると考えられる。まず，台湾においては，刑訴法上は，任意捜査の原則が明示的に定められていないけれども，同原則は中華民国憲法 23 条に求められるし，また，実際にも，台湾刑訴法 228 条 2 項，同法 101 条，同法 122 条などの規定からは捜査が任意処分を原則とすべきという帰結が導かれるとする見解が学説上は一部で現れている[534]。他方，実務上も，原則的には任意的な捜査が行われてきているとされる[535]。それから，任意処分と強制処分との区別の基準について

[533] 川出・任意捜査 32～39 頁，最三決昭和 51 年 3 月 16 日刑集 30 官 2 号 187 頁，坪内 155 頁参照。
[534] 陳運財・正當程序 145～146 頁，洪・搜索扣押實務研究 25 頁。
[535] 洪・搜索扣押實務研究 27 頁，97 頁，137 頁参照。

は，従来は，それが物理的な強制力の有無という点に求められてきたが，現在は，日本の通説(いわゆる重要な権利・利益侵害説[536])及び有力説(いわゆる実質的権利・利益侵害説[537])という２つの立場による混合説が，台湾において支持が得られつつある[538]。そのうえ，台湾にも警察比例の原則(捜査比例の原則とも呼ばれる)[539]が認められているからである。

次に，②の設定の場合は，アクセス権限の設定がかかっているから，技術的な方法をもって当該設定を解除しなければ，それぞれの内容を監視・記録することができないので，それは強制処分といえるものであろう。問題は，こうした監視・記録が，果たして，現行の通保法でいう通信傍受にあたるかのである。

まず，ここでの通信当事者は誰なのかが問題となる。というのも，ブログの仕組みと，電話ないしメールのそれとは，全く異なるものだからである。より具体的にいうと，ブログの場合，そのコミュニケーションの仕組みは，次のようなものになる。すなわち，Kが関連記事ないし写真を当該ブログにアップロードすると，アップロードの内容がホストコンピュータを運営しているプロバイダーWへ送信されてKのブログの画面に表示され，その後，アドレス帳におけるすべての知り合いやお気に入りの知り合いがそれぞれのアクセス権限によりKのブログの画面の記事を閲覧したり，写真をダウンロードしたりコメントを付したりするという形になる。

かような形態のもとでは，通信傍受令状において，誰を被処分者(傍受すべき対象者)として書くべきであろうか(通保法 11 条 1 項 2 号参照)。この点，前にも言及したが，通保法は「伝送中のデータ」と並んで「保存されたデータ」をも対象としている。伝送中のデータが対象である場合には，上記の形態の中で，データが伝送されているのは，Kによるアップロードの内容がホストコンピュータを運営しているプロバイダーWへ送信されている段階であるから，傍受すべき通信は，伝送中のアップロードの内容であり，通信当事者，すなわち傍受すべき対象者は，Kと通信業者のWになる。

そして，保存されたデータが対象である場合にも同様に，傍受すべき対象者はKや通信業者のWになるが，こうした場合は伝送中のデータを対象とする場合と異なり，KとWの両方とも傍受の対象とする必要はなく，その片方だけで十分である。というのも，ＩＴ通信は一連のコピー(保存)の繰り返しにより情報の伝送を完成させるという仕組みになっているため，KのところもWのところも，同じデータのコピーが残されうるからである。

しかし，以上示したブログの場面の２つの状況を，電話回線やメールの場面のそれと比較すると，違和感が生じる。というのも，電話回線やメールの場面においては，通信業者

---

[536] 最三決昭 51 年 3 月 16 日刑集 30 巻 2 号 187 頁。井上・争点 48 頁＝井上・強制・任意 10～11 頁参照。

[537] 三井・手続法(1)[新版]81 頁。安富・演習刑訴 5 頁をも参照。

[538] 陳運財・正當程序 169 頁，吳・照相攝影 119～120，175 頁，林富郎・通訊監察 21～22 頁。また，日本の先行研究を挙げていないが，こうした混合説とほぼ同じ内実をとる見解があり、すなわち，強制処分を，基本権(つまり重要または実質的な権利)を干渉(つまり侵害)する行為であるという理解として，黃朝義・刑訴三版 140 頁，林山田・程序法 5 版 266 頁，柯・刑事程序 165 頁，同氏・強制處分 93 頁参照。

[539] これも中華民国憲法 23 条から導かれたものである(陳運財・正當程序 153 頁，洪・搜索・扣押之實務研究 25 頁参照)。

は，通信当事者や傍受すべき対象者にはならないと理解されているからである[540]。この３つの場面のそれぞれの過程を対比すると，次のようになる。

(1)電話回線：発信者K→通信業者(電話会社)→受信者Y

(2)メール　：発信者K→通信業者W(KのISP)→通信業者Z(YのISP)→受信者Y

(3)ブログ　：発信者K→通信業者W(KのISP)→受信者K(アップロード完了画面表示)
↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑
複数のアクセス権限者のそれぞれが契約したISP
↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑↑
Kが許容した複数のアクセス権限者

上記の「→」の部分は，リアルタイムのコミュニケーションにあたるが，「↑」の部分は一方的なアクセスであるから，リアルタイムのコミュニケーションにはあたらない。つまり，「↑」の部分こそが発信者Kが意図したコミュニケーションの部分であるのに，アクセス権限者はリアルタイムのコミュニケーションの受信者になっていない。このように，通保法は，コミュニケーションの相手方と通信伝送の受信者との間にしばしばずれが生じるコンピュータ・ネットワーク通信の場面に対応できていないのである。

そのうえで，捜査機関が，「↑」の部分(Kが許容した複数のアクセス権限者のアクセス履歴，閲覧記録及びコメント)まで監視・記録しようとすれば，KとプロバイダーWないしKの知り合いと彼らが契約しているそれぞれのプロバイダーを対象とし，それらの間の多対多通信を傍受(監視・記録)するしかないだろう。しかし，かような傍受が，果たして，通保法でいう傍受令状によってなしうるものであるのかには大きな疑問がある。

さらに問題となるのは，仮に，多数のファンないし友だちのうちの誰か，捜査機関に対して当該ブログにおけるコミュニケーションを密かに監視・記録をすることに同意したとすれば，当該同意は，通信傍受法でいう「一方当事者の同意がある場合」に当たるか，そして，同意の範囲は，他のアクセス権限者による閲覧履歴ないし通信の内容(コメントを付けた場合)にまで及ぶかである。また，発信者Kが意図したコミュニケーションの相手方ではないが，リアルタイムのコミュニケーションの伝送の受信者になっているプロバイダーWが，かような同意をすることができるのかという問題もある。これらの点についても，現行の通保法のもとにおいては明確な答えが提供されていない。

最後に，③の「非公開」設定の場合，自分しか見られない記事とはいえ，Kがそれを同ブログに書き込むと，それはプロバイダーWのサーバーに送信されることになる。しかし，自分しかアクセスできないブログ記事を書き込んだKは，誰かを相手方としてコミュニケ

[540] 阪本・プライヴァシー権論 233 頁，藤田 224 頁，渥美・情報犯罪 82 頁参照。

ーションをする意思は全くないのであるから，この場合は，有体物である日記や個人の書類などの場合と異ならないので，それを双方向性のコミュニケーションの通信と解すべきではないであろう。しかし，この点についても，現行法上は明確でないのである。

第２款　多重転送と自動的受信応答

【例 7】から転じて，Kが，未成年者の売春紹介により金を稼ごうと企図して，ブログに掲示板機能を付し，自動的受信応答サービスを利用していると仮定しよう。具体的には，Kは売春や援助交際をしようとする多数の未成年女子を自分のブログの会員として募っており，顧客がKのブログに掲載された気に入った女の子の写真を選択すると，掲示板の画面に変換し，その予約欄に顧客が希望日時及び連絡方式を書き込むと，自動的に受付の返信がなされ，その後，女の子から顧客に連絡をし，性的取引を行うという仕組みになっている。

この事例で，顧客と自動的受信応答システムとの間の(予約ないし受付のやり取りの)通信は，通信傍受の対象となりうるであろうか。この点については，発信者と受信者の間のコミュニケーションとは，必ずしも人と人との間の通信を意味するものではなく，コンピュータ通信により，自動的に受信応答等を行う場合(相手方が自動的に対応するＦＴＰサーバのファイルや銀行口座へのアクセスなど)も含まれると解されている[541]。

確かに，コンピュータ通信により，自動的に受信応答等を行う場合，その機械ないしシステムは，あくまで，Kという人間の意思を執行するツールにすぎないとすれば，それも「特定された発信者対受信者におけるコミュニケーション」という「通信」の定義にあてはまるといえる。しかしながら，多重転送の場面においてかような理解をとると，法的には，以下のような不都合が生じうる。

まず，経由点としての自動発送信のコンピュータも通信当事者になるとすれば，単に転送するために経由点として利用される中継サーバーも通信当事者となり，それすら捜査機関が他人の通信を傍受することに同意することができるという結論に至る[542]。例えば，プロバイダー契約及び経路の設計ゆえに，最初の発信者Ａが，通信の相手であるＦに送信するためには，ＢＣＤＥの４つの中継サーバーを経由しなければならないという例を想定すると，この場合の経路は，Ａ→Ｂ→Ｃ→Ｄ→Ｅ→Ｆになる。この場合，ＢＣＤＥはコンピュータ通信により自動的に受信応答等を行う単なる経由点にすぎないが，前述した見解によれば，ＢＣＤＥも通信当事者になるから，それらすらＡとＦの間の通信を傍受することに同意することができることになってしまうが，こうした結論は，一般の通信利用者として

[541] 三島 190 頁。『第 145 回国会参議院法務委員会会議録』18 号 31 頁，19 号 23～24 頁，三浦守ほか・組織的犯罪三法解説 443 頁注(3)も参照。
[542] 通信当事者の同意による傍受につき，通保法 29 条 1 項 3 号参照。

納得しがたいものであろう。

他方で，多重転送の設定が，技術的な理由によるものではなく，ハッカーが攻撃の発信源を隠匿しようとするなどの動機で行われたものであるような場合であるとすれば，上記のＢＣＤＥがＡ(加害者)とＦ(被害者)の間の通信を傍受することに同意することができるとしても，一般の通信利用者は違和感をもたないばかりか，むしろ，システムの安全性を守る観点からは望ましいと考えるであろう[543]。

このように，顧客とＫの自動的受信応答システムとの間のやり取りを，顧客とＫとの通信とみなすことは妥当であるが，単なる技術的な理由による多重転送の自動的受信応答の設定などの場合は，必ずしも，そのように言い切れるものではない。こうした問題についても，現行の通保法は十分に対応していない。

第３節　捜索の場面に対応するために必要な基礎的理論の構築

以上から，次の３点が明らかになった。

①ＩＴシステムにおける移動可能なデータを捜査の対象とする場合には，考えられる捜査の態様は非常に変化多端なものであるから，既存する通信傍受という捜査手段によりそれらを完全に包摂させることが困難ないし不可能であるといえる[544]。②電磁的記録を刑訴法の捜索(差押え)の対象とする同時に，一定の電気通信設備に保存されたデータを通保法のいう通信傍受の対象とする台湾の現行法のもとにおいては，捜索と傍受を如何に区別するのかは，判断困難な問題である。③待ち受け型の傍受は，一定の電気通信設備に保存されたデータを対象とする場合の一例としてあげられるが，こうした場合は，リアルタイムで伝送中のデータを対象とする傍受の場合と同じ法益侵害の内実を持つものと評価することができるから，傍受令状により規制するのが妥当だと考えられるが，そうでない場合，つまり，リアルタイムでの傍受の実質を持たない場合にすらも傍受令状が適用されると，中華民国憲法 23 条の比例原則に適合しない，捜査に対する過剰な規制となるので，適切でない

---

[543] See also Kerr, BIG BROTHER at662～666.

[544] この点をより具体的にいえばまず，【例6】及び【例7】において指摘したように，一網打尽型の傍受や，通信の当事者は誰なのか，そして自動応答システムの法的性格をどう理解すべきであるのかなどの問題に対応してきていない理由は，現行法は物理的な要素に依存している点に求められる。例えば，通保法の立法に際して規制の対象として立法者が考えていたのは，電話並びに電話回線という有体物を経由して流れている会話に対する傍受に止まっているが，インターネットなどの場合においては，有体物の端末を使うわけではなく，マルチメディアという非定型の多様の端末が使われているため，有体物の電話，電話回線ないしその設備が所在する場所などの物理的な要素を介在させて，間接的に，対象となる会話などの無形の情報を特定するという立法者の考えた設計は機能しないこととなるのである。この場合，様々なマルチメディアを類型化することが，既に大変困難であるのに，それに加えてさらに，種々の捜査の態様をも併せて考慮し，それぞれの場面に対応する定型的処分の実定法化を図ろうとすると，その作業は一層複雑になる。また，こうした個別立法では，日進月歩の科学技術並びに捜査手法の進展に対応することは困難であると言わざるを得ないところである。そこで，立法論としては，媒体の種類ないし捜査の態様を類型化するという選択肢をとるよりは，むしろ，情報それ自体を(独立した)強制処分の(直接の)対象とする方がより現実的かつ効率的であると考えられる。この点からも，情報に強制処分の対象としての適格性を認めたうえで，その有体物と異なる特徴に叶う新しい定義・基準・原則を見つける必要性があるということができる。

[545]。

以上に示した数々の問題点を解決するには，ＩＴシステムなどの仮想的なバーチャル空間において移動可能なデータ――伝送中のものあるいは保存されたものを問わずに――に対して追跡したり，検索・検閲したり，取得・保全したりするという捜査手法を正当化・規制するためにあるべき制度を改めて考案することが必要となる。この点，移動可能なデータを取得・保全するという部分に関しては，第１章に打ち出した情報に対する差押えという制度によりそれを対応することができるが，移動可能なデータを追跡・検索・検閲する場面に対応するためにまずは，捜索すべき場所という概念に，従来理解されてきた物理的な空間のみならず，バーチャル空間をも包摂させる必要がある。具体的には，情報に対する捜索という制度を構築すべきである。

この情報に対する捜索という制度を考案する際の問題の核心は，バーチャル空間でいう“場所”とは，物理的な空間のように実存するものでなく，あくまで「仮想的な場所」を意味するものにすぎないため，従来，捜索の範囲を画定するために用いられてきた，場所・サイズ基準[546]が，バーチャル空間においては有効に機能しない[547]という点にある。

そこで，従来の場所・サイズ基準の代わりに，バーチャル空間を捜索すべき場所とする場合にふさわしい新たな基準を探求する必要がある。そのために，まず検討すべきは，物理的な空間における捜索に対して保護される法益である住居不可侵に対応する，バーチャル空間における捜索に対して保護される法益は何なのかという問題点である。この点を検討するにあたって，アメリカとドイツにおける以下の２つの議論が参考になると思われる。その１つは，アメリカにおける，修正４条の保護は，いわゆる「新しい科学技術におけるプライバシー」にも及ぶのかという問題点に関わる最近の論争である。もう１つは，2008年にドイツ連邦憲法裁判所が創出した新しい人権である，いわゆる「ＩＴ基本権」[548]を巡る論争である(以下，08 年判決[549]という)。

以上の通り，本章では，アメリカの「新しい科学技術におけるプライバシーと修正４条」並びにドイツの「ＩＴ基本権」に関わる判例ないし関連議論を素材にした比較法的考察を行

---

[545] 中華民国憲法 23 条の比例原則の趣旨は，不十分な規制が認められないと同時に，過剰な規制も同条に反するものとして許されないと解されてきた。

[546] 場所・サイズ基準とは，場所の物理的な区切りないし物件のサイズなどの物理的な要素により捜索すべき範囲を画定することをさす。具体的には，例えば，殺人事件を捜査するためにマンションの 101 号室を捜索すべき場所とし令状の発付を得た場合，101 号室内にあるものだからといってすべて捜してみてもよいわけではなく，例えば，凶器である包丁を探すために封筒を開けることは許されない。なぜなら，封筒のサイズに鑑み，その中に包丁が隠されることはありえないからである。

[547] バーチャル空間であるＩＴシステムの範囲は，理論的にネットワークの連結により無限に拡張が可能であるし，また，データは，自由に分割・圧縮できると同時に一定の外見やサイズなどの物理的な特徴をもたないことに加え，拡張子やファイルネームなども内容とは関係なく自由に変更できるから，前注で挙げた例のように，101 号室というような場所の物理的な区切り，ないし 101 号室内にある封筒のサイズと差し押さえるべき物である包丁のサイズとの対応関係などの物理的な要素をもって，捜索すべき範囲を限定することは不可能だからである。

[548] 「ＩＴ基本権」は，08 年判決がいう「情報科学技術システムの秘密性と不可侵性の保障に対する基本権」(das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme) という用語の略称である。

[549] BverfG, 1 BvR 370/07 vom 27.2.2008(Rn1～333) http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

いながら，台湾の立法論にとっての有益な要素を抽出したうえで，情報に対する捜索という制度を構築するために必要となる法益論を検討することとする。

第１款　比較法的考察

Ⅰ．アメリカの問題状況

新しい科学技術におけるプライバシーも修正４条により保護されるか，という論争は，Kerr が，2004 年に発表した論文「修正４条と新しい科学技術」[550]にて提起したものである。同論文に対しては，多くの学者から批判が寄せられた[551]。このうち，代表的なものとして，「プライバシーとセキュリティとの共存」[552]という Solove の論文が挙げられよう。

Kerr と Solove のそれぞれの理論構成及び対立点は以下の通りである。

１．Kerr の理論

Kerr は，修正４条は安定した技術(stable technologies)の場面での問題しか想定していないものであるため，同条によっては，ＩＴ技術などの発展途上の高度で複雑な新しい科学技術の場合には対応できず，そうした場合の問題の解決を図るには新たな立法によるべきものであると述べている[553]。その具体的な論拠は，以下の通りである。

(1)財産権に基づく視点

まず，Kerr は，KATZ 事件[554]では修正４条によって保護されるのは財産権ではなく人のプライバシーの合理的な期待であると判示されたものの[555]，その後の判例の流れをみると，修正４条の適用においては，依然として，「財産権に基づく視点」(the property-based view)を採用したままであるから，修正４条は新しい科学技術におけるプライバシーに対して適切な保護を提供することができないと述べている[556]。

この点をより具体的にいえば，まず，アメリカにおいては，修正４条の理解について，かつては，文言上示された場所や財産への「物理的な侵入」(an actual physical invasion)

---

[550] Kerr, CONSTITUTIONAL MYTHS, at 801ff.

[551] 次の脚注に引用した Solove の論文の他に，Colb, at 889ff ; Swire, at 904ff をも参照されたい。Kerr は，この Colb と Swire の論文に対して反論を加えている(Kerr, A REPLY TO COLB AND SWIRE, at 933ff)。

[552] Solove, PRIVACY AND SECURITY, at 747ff。この Solove の論文に対しても，Kerr は反論している(Kerr, A RESPONSE TO PROFESSOR SOLOVE, at 779ff)。

[553] Kerr, CONSTITUTIONAL MYTHS, at 838～839, 888.

[554] KATZ v. UNITED STATES, 389 U.S. 347(1976).

[555] もっとも，KATZ 判決はプライバシーの保護を重視する立場に移行したに過ぎず，財産的利益の保護を否定したわけではないという指摘がある(佐伯(3)1420 頁以下参照)。

[556] Kerr, CONSTITUTIONAL MYTHS, at 808～839.

は必ず必要である（いわゆる侵入原則 the ″trespass″ doctrine）と解されてきた[557]。かような理解が 1967 年以前の判例の大勢であり，そのリーディングケースとしては 1928 年の OLMSTEAD 事件があげられる[558]。

しかし，この OLMSTEAD 事件は，その後 1967 年の KATZ 事件[559]により明確に覆された。KATZ 判決は，修正４条は「場所ではなく，人を保護するものである」としつつ，無体物の情報(例えば会話など)も修正４条の保護を受けるものであるとしながら，その適用の基準は「物理的な侵入」の有無と関係なく，「憲法上保護された合理的なプライバシー権の期待」（a constitutionally protected reasonable expectation of privacy）の有無により決めるべきであると判示している[560]。

それにもかかわらず，KATZ 事件以後の判例の流れを見みると，修正４条の保護法益はプライバシーであることが確立されたとされつつも，その具体的な判断基準は依然として「場所／財産権」に深く繋がっている。それを示すケースとしては，1978 年の RAKAS 事件[561]が挙げられよう[562]。これは，被告人が捜索を受けた車両の乗客であった事案であるが[563]，法廷意見は，被告人は，車両に対しては「何らかの財産権に関わる利益」[564]を主張することができず，したがって，被告人のプライバシーの合理的期待は認められないので，本件の捜索・差押えが被告人の修正４条の権利を侵害するものではないと判示した[565]。

Kerr は，この RAKAS 事件を引用し，それを踏まえて，いわゆる「財産権に基づく視点」の内実を説明している[566]。すなわち，KATZ 事件以後のプライバシーの保護を判断するための最高裁の基準についていえば，場所ないし物件に対して「何らかの財産権に関わる利益」を主張することができないと，通常はプライバシーが否認されてしまうことになる一方で，逆に，「財産権」ないし「何らかの財産権に関わる利益」があったからといって，必ずし

---

[557] See OLMSTEAD ET AL. v. UNITED STATES, 277 U.S. 438(1928), and see Goldman v. United States, 316 U.S. 129 (1942).

[558] OLMSTEAD, id., at 466～467。法廷意見は，修正４条の文言を拠に，場所や財産などの有体物こそが修正４条の直接の保護対象であるとし，盗聴されたということだけであれば，それは「憲法によって保護された領域」とされる場所や財産に対しては何らの物理的な侵入もなされていないため，修正４条に違反しないと結論した。しかし，反対意見（MR. JUSTICE BRANDEIS, dissenting)は，立憲者が修正４条によって真に保護しようとした法益は財産権ではなく，「ひとりにしておいてもらう権利」(the right to be let alone）でこそあるとした(OLMSTEAD, id., at 478～479)。

[559] KATZ, supra note 554.

[560] KATZ, supra note 554, at 351～352。また同判決の補足意見（MR. JUSTICE DOUGLAS, MR. JUSTICE BRENNAN joins, concurring.）をも参照。

[561] RAKAS ET AL. v. ILLINOIS, 439 U.S. 128(1978).

[562] その他の判例については，Kerr, CONSTITUTIONAL MYTHS, at 815～827 参照。

[563] 本件の概略は以下の通りである。警察がＡの車両を捜索してライフル銃と砲弾を発見し，乗客であった被告人Ｂを逮捕したが，Ｂは，ライフル銃と砲弾の所有者であることを否認した。第一審は，ライフル銃と砲弾を証拠から排除すべきであるというＢの主張につき，Ｂは車両にもライフル銃にも所有権を有していないという理由で，それを却下し，武装強盗罪でＢに有罪判決を下した。控訴審及び州最高裁も，それを維持した。

[564] 「何らかの財産権に関わる利益」とは，法律上認められた所有権や占有権(property or possessory interest）などの財産権に限られるというわけではないとされる(RAKAS, supra note 561, at 143～144)。 例えば，JONES v. UNITED STATES, 362 U.S. 257(1960)で示された，「ある構内・領域に合法的に滞在する権限」のような「充分な財産上の利益」さえあれば十分である(RAKAS, id.)。

[565] RAKAS, supra note 561, at 147～148.

[566] See Kerr, CONSTITUTIONAL MYTHS, at 824.

もプライバシーが認められるわけではないとされる。

もっとも，KATZ 事件においても，補足意見を執筆した Harlan 裁判官は，修正４条の保護対象は，場所ではなく人であるという点は法廷意見の通りであるが，その人に対して，いかなる保護が与えられるかという問題については，その場所に着目することが必要であると述べている[567]。Kerr は，この点にも言及したうえで，修正第４条は，依然として，財産権の客体という意味での物理的な場所と結びついたままであると結論付けている[568]。そのうえで，Kerr は，こうした財産権に基づく視点からは，家屋内に置かれたオフラインのコンピュータ内のＩＴシステムであるならば，それも一般の有体物と同様に修正４条の保護を受けるが，ネットワーク(とりわけ，インターネット)を通じてオンラインで利用するＩＴシステムの場合には，修正４条により保護されないとしている[569]。

(2)プライバシーの合理的な期待の欠如

さらに，Kerr は，KATZ 事件で提示されたプライバシーの合理的な期待の基準に照らしても，新しい科学技術におけるプライバシーを修正４条の下で保護することはできないとしている[570]。

ここでいうプライバシーの合理的な期待の基準とは，KATZ 事件の Harlan 裁判官の補足意見によって示された，①主観的な合理的期待(個人が合理的期待を有すること)，②客観的な合理的期待(主観的な期待が社会的視点から見ても合理的であること)という２つの要件を指す(以下，Harlan 基準という)[571]。

それを前提に，新しい科学技術におけるプライバシーの要保護性を検討するに際して，まず考えられる問題としては，利用者が，インターネットに接続することによってオンラインで侵入される可能性を予見しうるにもかかわらず，ＩＴセキュリティのコスト及び複雑さ，ＩＴセキュリティの実行によりコンピュータの効能及びスピードが落ちることなどを考えて，適切な防御措置を取らずにそのまま接続した場合に，利用者はプライバシーの合理的な期待を主張することができるかという問題が挙げられる。

前述した２つの要件に沿って，この事案を考えると，次のような結論になろう。まず，利用者がオンラインで侵入される可能性を予見しうる以上，主観的な合理的期待は否定される。仮に，当該利用者が，自分の予見能力ないし侵入を防ぐ能力が特別に低いことを理由に，主観的な合理的期待を有すると主張したとしても，社会の一般人はオンラインで侵入されうる可能性を予見しうるため，当該主観的な期待は社会的視点から見て合理的とはいえず，客観的な合理的期待がないと判断されることになる。

---

[567] KATZ, supra note 554, at361.

[568] And see Kerr, DIGITAL EVIDENCE, at 290.

[569] See Kerr, DIGITAL WORLD, at 533 n4; and see Kerr, CONSTITUTIONAL MYTHS, at 831～838.

[570] Kerr, CONSTITUTIONAL MYTHS, at 838ff.

[571] KATZ, supra note 554, at361.

(3)司法による保護の必要性と適切性

もっとも，Kerr は，修正４条では新しい科学技術におけるプライバシーに対して十分な保護を与えることができないと述べるに留まり，かかるプライバシーは何ら保護を与えるに値するものでないとしているわけではない[572]。

そのうえで，Kerr は，新しい科学技術の場面においても修正４条の原則ないし理論を活かす司法による法創造(judicial rulemaking)を必要とするとしても，裁判所は，その構造上かような機能を果たすにふさわしいものであるかについて疑問を呈し[573]，その代わりに，制定法による保護(statutory protections)が必要であり，かつ，立法による方がより手厚い保護を与えられるので適切であるとしている[574]。つまり，Kerr は，立法は，司法より優れた構造上の能力を持っており，とりわけ，高度で複雑な科学技術に関する場面では，司法のもつ構造上の劣勢ゆえに，司法解釈による対応には限界があるから，構造上の優勢をもつ立法により対応すべきであるというのである[575]。

そして，かかる立法と司法の構造上の差異をもたらす要因として，Kerr は，①将来志向(rules ex ante)と過去志向(rules ex post)との差異，②先例による拘束という制約の有無，③クローズド・プロセスとオープン・プロセスとの差異，の３つの点を挙げているが，②は①の一内容として捉えてよいと思われる。

まず，①と②について，将来志向とは，立法が将来に向けられた性格を有すること，過去志向とは，司法が過去に向けられた性格を持つことを意味する[576]。具体的には，立法による法の形成が，過去の判例に拘束されることはなく，その適用は将来の不確定かつ抽象的な事象を対象とするのに対して，司法による法の形成は，過去の判例に拘束されると同時に，その適用は既に発生した個別の具体的な事案を対象とすることを指す[577]。そのうえで，Kerr は，常に変動を続ける科学技術は，過去に経験したことがない問題を提起してくる以上，類似の先例を引用し審理対象たる具体的な個別事案の争点の是非を判断するという司法の過去志向では対応が困難であり，立法の将来志向による対応が適切であると述べる[578]。また，科学技術の新たな問題がすぐに法廷へ持ち込まれることは少なく，法廷へ持ち込まれた後も最高裁の判断を受けるまでにかなりの時間がかかることからすれば，主動性を持たない司法は，変化を続ける新しい技術に迅速に対応することが構造的に不可能であり，必然的に時代遅れになるのに対して，構造上，主動性を持つ立法であるならば，新たな科学技術が登場した時点で直ちにそれに対応する関連規定を設けることが可能であるという

---

572 Kerr, CONSTITUTIONAL MYTHS, at 838～839.
573 Id., at 857.
574 Id., at 809～810, 864～865.
575 Id., at 857ff.
576 Id., at 868～870.
577 Id., at 868～870, 871～875.
578 Id., at 869～870.

[579]。さらに，先例により拘束されることはない立法と比べると，過去の先例により拘束されている司法は，変動している事実に対応するための柔軟性が不十分であるとしている[580]。

次に，③について，クローズド・プロセスとは，裁判官の接触できる情報のソースが極めて限定されているという司法による法形成過程の閉鎖性を，オープン・プロセスとは，立法者が広い範囲の情報を入手することができるという立法による法形成過程の開放性を，それぞれ意味する[581]。すなわち，立法と司法の構造を比較すると，裁判官が判決を作成する過程(すなわち司法による法形成過程)は，自己の部屋にこもり訴訟関連資料を読みながら当該事件に現れた争点の是非を判断するという形であると同時に，一定の時間内に判決を作成しなければならない圧力もあるのに対して，立法による法形成過程は，公開の公聴会を開いたり，大勢の専門家を招いたり，市民の声を取り入れたりするという形になるから，よりオープンなものである[582]。そこから，Kerr は，常に変化を続ける科学技術に関する問題を正しく判断するためには，より多くの関連情報に接触することができる立法のオープン・フロセスの方が望ましいとしている[583]。

２．Solove の反論

かかる Kerr の理論に対して，Solove は，次のように明確な異議を唱えている。

(1)修正４条の適用範囲

まず,修正４条の適用は財産権に基づく視点に限られるという Kerr の理解に対し,Solove は，Kerr の指摘した新しい科学技術に関する問題点は，いずれも，修正４条における情報プライバシー(information privacy)の問題として理解することができると述べる[584]。

Solove によれば，修正４条の保護は，物質空間におけるプライバシー及びバーチャル空間におけるプライバシーのいずれにも及び，また，新しい科学技術の使用に左右されないから，新しい科学技術におけるプライバシーも当然，修正４条でいうプライバシー権として保護される[585]。

そのうえで，問題の核心は，Kerr の議論の出発点となる高度で複雑な科学技術の使用の有無という点にあるのではなく，裁判所が修正４条の保護を情報プライバシーの場面に適用する際にしばしば困難に遭遇している点にこそあるとする[586]。ここでいう困難とは，これまでの修正４条は，物理的な捜索，有体物，及び物理的な侵入を対象とし，場所に侵入して有体物を探すような物理的な方式をその適用指針としていたところ，データを対象とす

---

[579] Id., at 870～871.
[580] Id., at 871～876.
[581] Id., at 875～883.
[582] Id.
[583] Id., at 875～877, 881～883(ただし，Kerr 自身も，立法による法形成過程は万能でないことを指摘している)。
[584] Solove, PRIVACY AND SECURITY, at748～749.
[585] Id.
[586] Id.

る場合にはかかる指針が役立たなくなってしまうという状況を指す[587]。

かかるSoloveの理解によると，KATZ以後の一連の判例において示された財産権に基づく視点が，このような困難を生みだす元凶であって，そもそも情報プライバシーを保護している修正４条にふさわしい基準ではないから，かかる基準を根拠に，修正４条の保護範囲を減縮しようとするKerrの主張は不当ということになる[588]。

(2)立法による保護の不十分性とその難点

次に，新しい科学技術におけるプライバシーは基本権ではなく，それを保護するか否かは，あくまで立法政策に過ぎないというKerrの見解に対して，Soloveは，かかる見解によると，プライバシーに対するバランスの取れた完全な保護を与えることができなくなると同時に，法適用の明確性と柔軟性の問題が一層悪化する懸念があると批判している[589]。

具体的には，情報プライバシー(すなわち Kerr のいう新しい科学技術におけるプライバシー)に関して，これまで作られてきた大量の制定法はいずれも，時代遅れなのであって，プライバシーに対して十分な保護を与えることができず，かつ，その適用も極めて複雑化しているという問題点があることを指摘し，これに対し，修正４条であるならば，現行の制定法[590]と比べて，プライバシーにバランスの取れた完全な保護を提供し，かつ，法適用の明確性と柔軟性の問題にうまく対応することができるとする[591]。

こうしたSoloveの主張を検討すると,彼が挙げた法適用の明確性と柔軟性の問題のうち,柔軟性の部分はバランスの取れた完全な保護の問題に包摂されうるものであると思われるから，以下の検討は，①バランスの取れた完全な保護と②法適用の明確性の問題の２点に分けて論じることにしたい。

まず，①の点について，立法によりバランスの取れた完全な保護が期待できないとされる理由としては，立法の速度を科学技術の進展のスピードに合わせることができないため,制定法による保護が永遠に不完全なままになってしまうという点があげられる[592]。言い換えれば，制定法による保護だけでは，常に保護間隙が生じてしまうという点が問題である。これに対して，裁判所は，修正４条における情報プライバシーという法益により，常に変化を続ける科学技術に柔軟に対応しながら保護間隙を埋めるようにバランスの取れた保護を提供することができるとされる[593]。このように，Solove は．立法の方が司法に比べて新たな科学技術の問題に迅速に対応できるとするKerrの立場とは，全く正反対の理解を示している。

次に，②の点についてSoloveは，法適用の明確性の問題つまり法適用の複雑さは，憲法

---

[587] Id.

[588] Id.

[589] Id.，at766～769.

[590] 主に，後述する the Electronic Communications Privacy Act ("ECPA")を指す。

[591] Solove, PRIVACY AND SECURITY, at 748～749, 760～769.

[592] Id.

[593] Id.

も含めたあらゆる法に存在しているものの，アメリカの現状においては，修正４条の法適用の複雑さよりも，むしろ情報プライバシーの保護を図る大量かつ複雑な制定法の下で現れてきた，法適用上の不明確性・複雑性の方がより深刻かつ複雑だと指摘する[594]。そのうえで，とりわけ，「電気通信におけるプライバシー保護法」（the Electronic Communications Privacy Act＝ECPA)[595]による法適用が複雑化している点を，Kerr 自身も深刻に受け止めているにもかかわらず[596]，制定法による対応が修正４条による対応より優れているとするKerr の主張は事実に合わず不合理であると批判している[597]。

(3)立法の構造上の優位への批判

以上を踏まえて，Solove は，大量かつ複雑な法律の制定により，複数の法の間の適用上の不明確性・複雑性という問題を生み出した立法機関は，Kerr が述べたような新たな科学技術の問題解決に関する構造上の優位を有していないと結論付ける。

まず，Kerr の言及した立法の将来志向に対して，Solove は，確かに，立法は，理論的には，将来志向の性格をもつものであるといえるものの，アメリカにおいて，連邦法を通過させるのは決して容易ではなく，また現行法の改正に対して，国会はかなり保守的な姿勢を示していることなどを指摘する[598]。その一例として，1986 年に成立した ECPA は，2001年に改正されたが，その改正の幅は僅かであり，1986 年から 2001 年までの間に科学技術はかなり進歩していたにもかかわらず，改正までに 15 年以上もかかってしまった事実を挙げている[599]。このように，これまでの情報プライバシーに関連する法改正の経緯に鑑みると，立法は，迅速に科学技術の変化に対応することができないばかりか，仮に法改正がなされたとしても，新法は常に進化を遂げていく科学技術の実情に合わず，時代遅れの問題を解消できていないから，科学技術の問題に対する構造上の優勢を有していないというのである[600]。

次に，オープン・プロセスの立法は，クローズド・プロセスの司法に比べ，科学技術の問題をより良く理解し適切に対処することができるというKerrの主張に対して,Soloveは,かかる主張を支持する論拠は全くないとする[601]。具体的には，現に，これまでの科学技術に関する立法――中心となる 1986 年の ECPA の他に，1934 年の「連邦通信法」（the Federal Communications Act)，1968 年の「包括的犯罪防止及び街路安全法第Ⅲ編」(Title III of the Omnibus Crime Control and Safe Streets Act)，1978 年の「外国諜報監視法」(Foreign

[594] Id.，at766～767.

[595] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as a note to 18 U.S.C. 2510).

[596] Kerr は，ECPA による法の適用の複雑さを「インターネット監視の“霧”」と称している(Kerr, "Fog" of Internet Surveillance, at 805ff)。

[597] Solove, PRIVACY AND SECURITY, at766～767.

[598] Id.，at770～772.

[599] Id.

[600] Id.

[601] Id.，at771～773.

Intelligence Surveillance Act＝FISA)，2001 年の「愛国者法」(the USA-PATRIOT Act)など――の内容を見ると，立法者が規制の対象たる科学技術を十分理解していなかったことは明らかであるばかりではなく，立法者が作った法律は，常にそれによって規制しようとする対象よりも複雑になっているため，法の適用上の難問が多発しているというのである[602]。

その上で，Solove は，立法者が怠慢したり制定法が社会の実情に合わなくなったりする場合，司法でなく立法により対応すべきであるという Kerr の主張によれば，対応を放棄するに等しいではないかという懸念を表明しつつ，そもそも，この問題に対しては，立法と司法の両方による対応が必要であるから，立法のみによる対応，あるいは司法のみによる対応という二者択一の提案自体が不適切であると主張している[603]。

Ⅱ．ドイツの問題状況

続いて，ドイツの 08 年判決が打ち出したいわゆる「ＩＴ基本権」を考察したい。このＩＴ基本権とは，後述するいわゆる「オンライン捜索」(Online-Durchsuchung)[604]という新型の捜査手法の侵害性に対抗するために，08 年判決により創り出された新しい人権である。そこで，ＩＴ基本権を検討するに先立ち，オンライン捜索の意味，仕組みないしその利用上の問題点を明らかにしておく。

１．オンライン捜索について

オンライン捜索という手法は，情報を捜索の直接の対象とする典型例として考えられる。というのも，かような手法を実施するにあたっては，被処分者の記憶媒体の物理的な所在を確認する必要はないし，また当該媒体に接触することもないからである[605]。以下では，オ

---

602 Id.，at769～773.

603 Id.

604 オンライン捜索とは，オンラインでデータを検索・分析・追跡したりするなどの機能を有するものであるから，「捜索」と称されるわけであるが，しかしながら，この捜査手法は，物理的に家宅に侵入することはなくかつ密かに行う特徴があるから，家宅などの物理的な空間を対象とする従来理解された「捜索」という法的概念には当てはまらないものである。他方で，オンライン捜索は，オンラインで情報の取得を目的とする捜査手法でもあるから，この側面からは，かかる手法を，オンライン差押えと呼ばれるべきものであろう。このように考えると，オンライン捜索という用語は必ずしも適切ではないが(同様の指摘として植松 3 頁参照，また同文 35 頁注(10)に挙げられたドイツの先行文献をも参照されたい)，オンライン捜索という用語は既にドイツの判例・実務ないし学説で定着したものであるので，本稿もこの用語を用いることとする。

605 このことは，オンライン捜索という手法の具体例及び稼動の仕組みから明らかである。まず，具体例としては，トロイ木馬(Trojanische Pferde)などのスパイプログラム(Spionageprogramme)を密かに対象者の端末に差し込んでおくことにより，端末にある目標たるデータをオンラインで直ちに取得する方法が挙げられる(Kutscha，S. 1169)。また，その仕組みについては，一致した定義が存在しないとされるけれども，このテーマを取り上げたドイツの関連文献の最大公約数的な理解からいえば，それは，ネットワーク接続のもとにおいて，オンラインで侵入したコンピュータ・システム及びデータ記録媒体にアクセスする捜査手法ということができる(Burkhard&Claudia，S. 13)。ここからわかるように，オンライン捜索の実施にあたっては，媒体との物理的な接触をすることはないし，また媒体を物理的に特定しておく必要もない。

ンライン捜索の問題を検討する前提として，まずは，その問題の背景を示しておこう。

(1)問題の背景

デジタル時代と言われる現在においては，強固な暗号化などの高度のＩＴセキュリティ技術の急速な進展・普及に伴い，各国の捜査の実務において，データを保管している対象者の協力が得られないときに，目標たるデータを見つけ出すことが困難となり，捜査に大きな支障が生じ，場合によっては，捜査を断念せざるを得ない事態に直面している[606]。

これを受け，ドイツにおいては，解読困難ないし不能な暗号等のＩＴセキュリティを迂回できる，いわゆるオンライン捜索という新しい捜査手法が開発されている[607]。この捜査手法によりＩＴセキュリティを迂回することができるのは，オンライン捜索が，直接に端末に侵入し，暗号化されていない段階あるいは暗号が解かれた後の段階のデータを取得するという仕組みによるものであるので，暗号自体が解読できなくても，それを迂回し捜査に必要なデータを取得できるからである[608]。

この点に加えて，以下の２つの点を理由に，ドイツの政府当局は，オンライン捜索は，今や捜査のために必要不可欠な手段であると主張している[609]。第１に，オンライン捜索は，密かな侵入であるから，公開で行われる家宅捜索の場合と異なり，被処分者に処分を事前に知られることはないというメリットがあること，第２に，オンライン捜索により，伝統的な捜査方法で保全できない，変動しているデータ(例えば，パスワード及び被処分者の利用状態履歴に関する詳しい情報のようなデータ)を確保できることである[610]。

これに対し，オンライン捜索という捜査手法の有効性に疑問を投げている論者もいる。例えば，Kutscha は，オンライン捜索は，暗号化などのＩＴセキュリティを取っていない経験の乏しい犯罪者に対してのみ成功できるのではないかと指摘している[611]。

確かに，技術的には，入力の段階でも暗号化させたり，読み終えたら再度暗号化したりすることが可能であり，そして，データの内容を認識するために解号しなければならないように読取権限を設定できるし，また，システムセキュリティを強化することによりオンライン侵入を困難にすることが考えられる[612]。この意味で，暗号化などの様々な工夫をも含

---

606 Rux, S. 285～286, Lessig, at 66～67＝邦訳：山形浩生， 柏木亮二（訳）93～95 頁，酒巻・提出命令 128 頁，山川 63 頁，木村・情報政策 193～195 頁，高杉・暗号 136，139，141，145～146 頁など参照。

607 a. a. O.(BVerfG, Anm.549)Rn.9.他方，ドイツの連邦刑事局の局長である Jörg Ziercke 氏は，2008 年オンライン捜索判決が出た直後の 2008 年 3 月に，ニュース雑誌である DER SPIEGEL の取材に応じて，「我々はすでに特殊なプログラムを開発した。他方，かような捜査手法[オンライン捜索]に資する市販の商業用の製品もある。一旦法的な規制が発効すれば，その時点で，我々はすでに用意してあるソフトウェアを自由に使える」と述べた(Burkhard&Claudia, S. 8)。

608 a. a. O.(BVerfG, Anm.549)Rn.9.

609 a. a. O.(BVerfG, Anm.549)Rn.9.

610 a. a. O.(BVerfG, Anm.549)Rn.11.

611 Kutscha, S.1172。

612 暗号とシステムセキュリティの関係につき，簡単にいえば，セキュリティの問題は，大まかに，①秘密性(secrecy/confidentiality)，②認証(authentication)，③否認防止(nonrepudiation)，④完全性(integrity)の４つのカテゴリーに分類されるが，暗号は，このうちの①に属する。この意味で，システムセキュリティの一部を構成することがありうるが，①～④を組み合わせたシステムセキュリティが破られたからといって暗号が解読されるわけではなく，逆に暗号

んだITセキュリティに常に細心の注意を払っている経験の豊富な犯罪者に対しては，オンライン捜索がどこまで役立つのかという疑問が投げ掛けられるかもしれない。とはいえ，現時点では，入力段階の暗号化はまだ普及していないし，また，データの内容を認識するために解号しなければならないから，すくなくとも解号段階への侵入という意味でのオンライン捜索の有効性は認められる。

他方，Burkhard&Claudia は，08 年判決は個別の事案について判断を下したものに過ぎず，技術及びその効果に関する詳細について触れていないと指摘し，08 年判決を下した連邦憲法裁判所第１部においてなされた口頭審理に出席した連邦刑事局長及び憲法擁護庁の長官が，「必要とされる証言許可」が得られなかったため[613]，本件に対して証言をしていないし，また参照に資する他の先例も存在しないため，08 年判決は，結局のところ，専ら新聞紙の記事あるいはその他のメディアの報道を基礎としたものではないかという批判を展開している[614]。

しかしながら，後述する通り，本件でオンライン捜索が実施されたことは間違いないし，また，法廷に専門家を招き，一般論としてオンライン捜索という捜査技術についての特徴・仕組みを証言してもらっているから，「専ら新聞紙の記事あるいはその他のメディアの報道を基礎としたものではないか」という批判は，必ずしも適切でないと思われる。つまり，08 年判決が，判断の前提として，オンライン捜索の理論上・技術上の有効性を認めた点は妥当だと考える。

(2)オンライン捜索の意味

オンライン捜索の意味を説明するには，以下，08 年判決で争点となった，ノルトライン＝ヴェストファーレン（Nordrhein-Westfalen）州(以下，ＮW州という)の憲法擁護官庁[615]にオンライン捜索の権限を与えた法的根拠である，ＮW州憲法擁護法に基づく規則(VSGNW: Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen)第５条２項 11 号のの内容を確認しておく必要がある。

A. 法的な根拠

VSGNW第５条２項柱書きは「憲法擁護官庁は７条の条件を満たす場合，情報取得のために，情報収集の手段として下記の処分を用いることができる」と定めている[616]。そして，同項 11 号

が解読されたとしても必ずしもシステムセキュリティに侵入されることにならない(アンドリュー677 頁以下，高杉・暗号 145～146 頁参照)。

[613] 両官庁の公務員が何ら陳述をすることの可否につき，それを決定する権限は連邦内務大臣にあるが，連邦内務大臣の Wolfgang Schäuble は，オンライン捜索の実態を明るみに出すことを好まないとされる(Burkhard&Claudia, S. 9)。

[614] Burkhard&Claudia, S. 9.

[615] 連邦法律により，警察の情報・報告制度のために，憲法擁護を目的とする資料と刑事警察の資料を集めるために中央官署を設立することができる(基本法 87 条１項)。憲法擁護の中央官庁としては連邦憲法擁護官庁（Bundesamt für Verfassungsschutz）が設立された(山田晟・法律用語 663 頁参照)。

[616] a. a. O.(BVerfG, Anm.549)Rn.32.

第１文は，「インターネットの秘密的監視及び継続的探索，例えば，コミュニケーションサイトにおいて身元の隠された利用者などを探すこと〈1アトル〉，又は，技術的な手段を利用して情報科学技術システムに密かに侵入すること〈2アトル〉」と規定し，同号第２文は，「第１文の処分が信書，郵便及び通信の秘密に対する侵害を意味する場合，又は，その性質及び程度においてそれに匹敵する場合は，基本法10条に関する規定の必要条件に基づいてのみ許される」と規定している[617]。

以上の通り，１アトルで規定されているインターネットの秘密的監視及び継続的探索がインターネット上を現に流通している不特定多数人の情報を対象とするのに対し，２アトルで規定されているＩＴシステムへの密かな侵入は，特定の端末に既に蔵置された情報を対象とするものである。ここで検討対象とするオンライン捜索は，後者にあたる。

B．定義

オンライン捜索を，前述した規定に従い定義すると，「情報取得のために，情報収集の手段として，技術的な手段を利用しＩＴシステムに密かに侵入する処分」であるということができよう。ここでまず検討すべきは，こうしたＩＴシステムに密かに侵入する処分が，「一回」に限られるのか，それとも「継続」の場合も含まれるのか，という問題点である。

この点について，ドイツの学説には，オンライン捜索の概念を狭く解する立場と広く解する立場がある。このうち，狭義のオンライン捜索とは，蔵置されたデータを取得するため，コンピュータ・システムへ密かに「一回」侵入することを意味する[618]。他方，広義のオンライン捜索は，一回性の侵入行為だけでなく，端末の活動の「継続的な監視」をも含む[619]。言い換えれば，広義のオンライン捜索の概念には，システムへ密かに継続的に侵入する，いわゆる「オンライン監視」（Online-Überwachung）も含まれるものとされる[620]。

これに対して，08年判決は，オンライン捜索の概念について狭義と広義の２つの理解を同時に提示しているが，とりわけ広義の理解に重点を置いている[621]。本稿は，以下の理由で，広義のオンライン捜索概念を採用した08年判決の立場は妥当であると考える。というのは，既に指摘されているように，理論的には一回性処分たるオンライン捜索を観念できるが，実際には，たとえ捜査機関が一回のみ侵入するつもりであったとしても，技術的な困難性ゆえに，通常は，ターゲットとなるシステムへの接続ないし当該システムにある目的のデータの発見に成功するまでに数回ないし一定期間にわたる処分が必要となり，結局のところ，一回性のオンライン捜索は常に継続的監視へ発展する傾向があるからである[622]。

そこで，本稿は，08年判決と同様に，オンライン監視を含んだ広義のオンライン捜索の

---

[617] a. a. O.(BVerfG, Anm.549)Rn.33.

[618] Sieber, Online-Durchsuchungen, S.2；auch vgl. Graf, §102 Rn15.

[619] Weiß, S.18ff；auch vgl. Sieber, Online-Durchsuchungen, S.3.

[620] a. a. O.

[621] a. a. O.(BVerfG, Anm.549)Rn.5, 7.

[622] Sieber, Online-Durchsuchungen, S.４.

定義を採用することとする。そして，オンライン監視でいう監視とは，従来理解された傍受で行われる監視と異なるものであるから[623]，以下では，混乱を避けるために，オンライン監視という用語を用いないことにする。

以上により，本稿は，オンライン捜索を，「オンライン侵入技術を用いて，端末のＩＴシステムに密かに侵入したうえで，当該端末の活動を監視したり，そこに蔵置されたデータを探索・解析・取得したりする捜査手法」と定義する。

このうち，「オンライン侵入技術」とは，スパイプログラムを端末にインストールしておく手法，あるいは，ＩＴシステムの不備や弱点を利用する手法を指す[624]。このうち，ＩＴシステムの不備の例としては，あるべきＩＴセキュリティの措置を取っていない場合，あるいは，コンピュータで利用するソフトウェアないしシステムの新しいバージョンへの更新を行っていない場合が挙げられる[625]。次に，ＩＴシステムの弱点の利用とは，例えば，ユーザーがＩＤやパスワードを忘れてしまった場合に備えてアカウントの設定を変更できる管理者の特権(いわゆるスーパーユーザ権限)が考えられる[626]。この特権を使えばＩＤとパスワードが分からなくてもシステムに侵入することができるのであり，この意味で，それはＩＴシステムの弱点と言えよう。

２．08 年判決について

以上をもとに，オンライン捜索の合憲性について最も権威ある判断をした 08 年判決を検討する。

本件は，ＮＷ州の憲法擁護官庁が，異議申立人らが個人で使用していたコンピュータなどの端末に対して，前述したVSGNW5 条 2 項 11 号 1 文 2 アトルで定められた「オンライン捜索」を実施した事案である。異議申立人らは，ＮＷ州の憲法擁護官庁にオンライン捜索の権限を与えている同規定は違憲であると主張し，本件憲法異議の訴えを提起した。本件の争点及び連邦憲法裁判所の判断は，次の通りである。

まず，争点について，異議申立人らは，オンライン捜索の権限を定めているVSGNW5 条 2 項 11 号第 1 文 2 アトル(以下，2 アトルと略称する)が違憲であると主張した[627]。この主張を支えた具体的な論拠として，以下の６点が挙げられる。

①インターネットの通信機能に着目すれば，オンライン捜索は基本法 10 条により保護された電気通信の秘密を侵害するものであるにもかかわらず，2 アトルは基本法 10 条によっ

---

[623] この点を，メールに対する傍受を例に考えてみると，メールを傍受する場合でいう監視は，送り手がメールを送信した時点から受け手側のメールサーバーに到着する時点までの間の時間帯(すなわち，伝送中のデータ)を対象とするものである。これに対して，オンライン監視でいう監視行為は，①送り手がメールを送信する前段階のデータ入力の時点，②当該メールが受け手側のサーバーに到着してから受け手がメールサーバーに問い合わせるまでの時間帯，あるいは③受け手が自己の端末に保存したデータ，を監視の対象とするものである。このように，オンライン監視(広義のオンライン捜索)において行われる「監視」と伝統的な傍受において行われるそれとは，その対象を全く異にするものである。

[624] Vgl. Weiß, S.16ff.

[625] a. a. O.

[626] a. a. O., S.20～21。また，大橋・基礎編 35 頁以下の説明も参照。

[627] a. a. O.(BVerfG, Anm.549)Rn.119ff.

て要求されている，基本権に対する侵害に必要な条件ないしその範囲についての定めを欠いている[628]。

②オンライン捜索により侵入されたコンピュータが住居に置かれていた場合，基本法 13 条で定められた住居不可侵に関する基本権が侵害されるにもかかわらず，2 アトルは，基本法 13 条 2〜7 項の要求を満たしていない[629]。

③オンライン捜索は，基本法 1 条 1 項ないし 2 条 1 項により保護された「一般人格権」(allgemeine Persönlichkeitsrecht)を侵害する可能性があるにもかかわらず，2 アトルには，「私生活形成の核心領域における個人発展の保護のために十分な規範的予防措置」が欠けている[630]。

④国家によって取得されたデータは広い範囲で加工・流用されたり他の官署に提供されたりする可能性があるにもかかわらず，2 アトルには，それを防ぐための予防措置が欠けている[631]。

⑤2 アトルは，被処分者を保護するための手続的予防措置(例えば裁判官留保原則)を欠いている[632]。

⑥2 アトルは，以上の①〜⑤の不備があるので，「比例原則」（Verhältnismäßigkeits-grundsatz）ないし「規範の明確性原則」（das Gebot der Normenklarheit）に反する[633]。

これらの点をまとめると，本件の争点は次の２点に絞ることができる。第１に，オンライン捜索は，基本法 10 条の通信の秘密，同法 13 条の住居不可侵，同法 1 条 1 項，2 条 1 項の一般人格権，という３つの基本権を侵害するものであるか。第２に，基本権に対する侵害を正当化するための要件及び侵害の許容される範囲ないし被処分者を保護するための手続などの定めが欠如している本件規定は，基本法上の比例原則並びに規範の明確性原則に反するのであるか。

これに対し，08 年判決は次のような判断を下した。オンライン捜索は，必ずしも通信の秘密および住居不可侵に関する２つの基本権の侵害を構成するものではないが，一般人格権から新たに導かれる IT 基本権を侵害するものである。そして，IT 基本権を侵害する処分が認められるためには，比例原則及び規範の明確性原則を満たす法律の規定を必要とするが，オンライン捜索の権限を定めた本規定は，広義の比例原則(すなわち目的との適合性)には反しないものの，狭義の比例原則(すなわち目的と手段との比例性)及び規範の明確性原則に反する。

ここに，情報に対する捜索により侵害される法益は何なのかというここでの検討対象と直接的な関係を有するもののみを検討する。具体的には，08 年判決によると，オンライン

---

628 a. a. O.(BVerfG, Anm.549)Rn.120, 122.
629 a. a. O.(BVerfG, Anm.549)Rn.120, 121.
630 a. a. O.(BVerfG, Anm.549)Rn.120.
631 a. a. O.(BVerfG, Anm.549)Rn.122.
632 a. a. O.
633 a. a. O.

捜索は，基本法 10 条の通信の秘密，基本法 13 条の住居不可侵という２つの基本権を侵害するものではないとされているがその理由は何なのか，及び，なぜ，一般人格権からＩＴ基本権を新しく導き出すことが必要といえるのか，という２つの問題点を取り上げたい。

(1)基本法 10 条との関係

08年判決によると，通信の秘密の保障を定めた基本法10条の保護範囲は，有体物の伝送の場面に止まらず，インターネットのコミュニケーションサービスなどの無形の情報の伝送をも含み，また，通信の内容のみならず，通信の状況(例えば，当該通信が，どのような人により，どのような通信設備の間で，何時，どのように行われたかなどの通信内容以外の部分)にも及ぶが，ＩＴシステムの秘密性と不可侵性には及ばない[634]。

また，基本法10条による通信の秘密の保護は，伝送過程に限られており，コミュニケーションプロセスが終了した後，コミュニケーション参加者が支配する範囲の下で保存された通信の内容及びその状況には及ばないから，既に蔵置されたデータを対象とするオンライン捜索は，伝送過程におけるデータのみを対象とする基本法10条の問題にならない[635]。

(2)基本法 13 条との関係

次に，08 年判決は，基本法 13 条で定められた住居不可侵という基本権の保護範囲は，住居に対する物理的な侵入への防御という場面にとどまらず， 国家が特別な補助的手段(とりわけ，科学技術による補助手段)を用いて，住居内で起こった諸事象を観察したり，それについての関連情報を取得したりするような処分(例えば，住居に対する音声的・光学的監視や漏洩電磁波を測定する処分)にも及ぶとした上で，住居内にあるＩＴシステムの利用を監視する処分もここに含まれるとすれば，家屋内に置いてある端末内のＩＴシステムへの侵入は基本法 13 条でいう住居への侵入に当たる余地があるとする[636]。

しかし，オンライン捜索が家屋などの物理的な場所から離れて移動している端末――とりわけ，ラップトップ，個人デジタルアシスタント(PDAs)あるいは携帯電話などのモバイルのＩＴシステム――を対象とする場合には，住居などの物理的な場所の区切りによって定義された物理的な空間のプライバシーに対する侵害をもたらさないから，かかる場合には 13 条の保護が働かなくなる[637]。

また，オンライン捜索が家屋などの物理的空間に置かれた端末を対象とする場合であっても，当該端末からネットワーク(とりわけ，インターネット)を通じてさらにアクセスできるその他のＩＴシステムを基本法 13 条の保護対象とすることは困難である[638]。というのも，さらにアクセスできるその他のＩＴシステムは，対象となる端末が置かれている場所と

[634] a. a. O.(BVerfG, Anm.549)Rn.182～183.
[635] a. a. O.(BVerfG, Anm.549)Rn.184～186.
[636] a. a. O.(BVerfG, Anm.549)Rn.192.
[637] a. a. O.(BVerfG, Anm.549)Rn.194～195.
[638] a. a. O.

の間に何ら物理的な繋がりを持たないため，それを物理的な場所の保護範囲に含めることはできないからである[639]。

以上により，08 年判決は，基本法 13 条は国家による有形ないし無形の侵入から個人の私的生活空間を守るという保護を提供しているが，ＩＴシステムへの侵入の場合には十分な保護を提供することができないとしている[640]。

(3)その他の基本権との関係

最後に，オンライン捜索が基本法 2 条 1 項及び 1 条 1 項で定められた一般人格権を侵害するかという争点について，08 年判決は，それを肯定した上で，既存の基本権――主に，基本法 10 条と基本法 13 条――，及びこれまで類型化・具体化された一般人格権――主に，プライバシー領域の保護と情報の自己決定に関する権利(以下，「情報自己決定権」と称する)――によっては，オンライン捜索による侵害から人権を守ることができないという意味でのいわゆる保護間隙が存在することを指摘し，かかる保護間隙を埋めるために，一般人格権からＩＴ基本権を新しく導き出す必要があると述べている[641]。

そこで，次に問うべきは，いかなる保護間隙が存在するか，言い換えれば，オンライン捜索により，どのような重要な法益が侵害されているかである。この点，08 年判決は，現代社会においてＩＴシステムが個人の人格の発展には重大な意義をもつという点から出発し，次のような議論を展開している。

A．人格発展におけるＩＴシステムの重要性

08 年判決は，まず，ドイツ連邦政府の統計年鑑を根拠として，①コンピュータがすでに社会に広く普及し，その計算能力(RAMと記録の容量)も高くなっていること，②個人用パソコンは，常に多様な目的に使われており，コンピュータを通信機器とする多様な形態での利用も可能であること，③大部分の人々は日常取扱う多数の物事において常にＩＴ技術的構成要素(例えば，住宅あるいは自動車に設置された電気通信機器あるいはその他の電子機器)を利用していることを指摘して，それらの点から，コンピュータは人格の発展にとってかなり重要な意味をもつものとし，とりわけ，インターネットの利用の急増に伴い，かかる重要性がより一層大きくなっているとする[642]。というのも，複雑なＩＴシステムの一種であるインターネットは，それに接続したコンピュータユーザーが，有用かつ大量の多様な情報(とりわけ，他のネットワークないし別のコンピュータ端末からも検索することができるように設定された情報)にアクセスすることを可能にすると同時に，大量かつ新型のコミュニケーションサービスを自由に使用することも可能にしており，ユーザーはかかるサービスを利用することによって，積極的に社会的な関係網を築いたり保持したりすることが

[639] a. a. O.
[640] a. a. O.(BVerfG, Anm.549)Rn.191.
[641] a. a. O.(BVerfG, Anm.549)Rn. 166～169, 196～200.
[642] a. a. O.(BVerfG, Anm.549)Rn.172～174.

できるばかりか，高度で複雑なＩＴ技術を盛り込んだコンバーターの機能により，遠隔地でのコミュニケーションを，従来のそれより広い範囲で行うことができるようになっているからである[643]。

確かに，現代社会において，人間はコンピュータ及びコンピュータ・ネットワーク，言い換えれば，高度計算機能をもつ複数の端末ないしシステムからなる強大なネットワークの集合の１つの巨大な複合した網状目で結合するＩＴシステムを利用しないと，一般的な日常生活を送りにくくなっている。この点は，08 年判決が，それをオンライン捜索の合憲性を審査するにあたって法的な議論を展開するための立論基礎とすると同時に，ＩＴ基本権の創出を必要と考える重要な背景ともなっている。

B. ＩＴ技術の利用に伴う人格への新たな危険

08 年判決は，最新のＩＴ技術が，前述した意味で，個人の人格の発展に可能性を与えることができると同時に，人格を新たな危険にさらすことにもつながると指摘している[644]。

すなわち，ＩＴシステムには，コンピュータのユーザーが意識的に作成したり保存したりするデータのみならず，ＩＴシステムの自律性によりデータ処理プロセスの中で自動的に生成されるユーザーの行動ないしその特性(属性・傾向)に関する多数のデータも存在し，かつ，これらのデータは，互いに接続したシステムを通じて利用することが可能な状況にあることから[645]，第三者がかかるデータを不正に取得し分析すれば，ユーザーの人格に関するプロフィールの形成に至るような広範囲にわたる帰納的推理をなしうる危険性があるとされる[646]。そして，このような人格に対する新たな危険は，とりわけ，インターネットなどのコンピュータ・ネットワークに接続したＩＴシステムにおいて一層深刻化するとされる[647]。

このように，人間の基本的な生存にとって不可欠な重要性を持つＩＴシステムを利用する際に，ユーザーの人格に関するプロファイルの第三者による形成可能性という人格に対する新たな危険が生じうるのであれば，基本権としての保護を与えることにより，この新たな危険の発生ないしその実害化を防止するべきであることが根拠付けられよう[648]。裏返して言えば，オンライン捜索の侵害性は，その実施によってこの意味での人格に対する新たな危険の発生ないしその実害化がもたらされうるという点に求められることになる。すなわち，オンライン捜索の実施により，ＩＴシステムの強大な資料庫を通じて個人の人格に関するプロフィールを形成することが可能であるとすれば，それによって，「私生活形成の核

643 a. a. O.(BVerfG, Anm.549)Rn.176.

644 a. a. O.(BVerfG, Anm.549)Rn.170, 177.

645 a. a. O.(BVerfG, Anm.549)Rn.170, 178～179.

646 a. a. O.(BVerfG, Anm.549)Rn. 178～179.

647 a. a. O.

648 a. a. O.(BVerfG, Anm.549)Rn.200～206. ここでいう「新たな危険の発生」とは，オンライン捜索によって全人格像を完全に解析されてしまう可能性が存在していること，言い換えれば，まだ完全に解析されていないが，何らかの防止措置が取られないかぎり，将来はそれを完全に解析されてしまう結果に至ることが予見されることを意味する。「その実害化」とは，危険の実現，つまり，全人格像を完全に解析されてしまったことを意味する。

心領域における個人的(人格の)発展」(individueller Entfaltung im Kernbereich privater Lebensgestaltung)という人格権のもっとも核心的な部分が侵害されることになるのである[649]。

こうして，08 年判決は，ＩＴ基本権の必要性を，人間の生存にとって必要不可欠なインフラといえるＩＴシステムを利用するに際して生じうる，個人の人格に関する完全なプロフィールが形成される懸念，及びそれによってもたらされる「私生活形成の核心領域における個人的発展」への侵害に対抗する点に求めている。

C．プライバシー領域論による保護の不十分性

次に検討すべきは，オンライン捜索により引き起こされる人格に対する新たな危険を防ぐには，なぜ，従来の「プライバシー領域論」による保護だけでは不十分なのかである。

この点，まず，ドイツ連邦憲法裁判所の従来の判例においても，アメリカ法でいうプライバシーの領域の保護(すなわち，前述した修正４条における場所に関わるプライバシーの権利)に相当する「私的領域の保護に関する保障」(die Gewährleistungen des Schutzes der Privatsphäre)があり，それは，一般人格権が私的領域を保障しているという理解から導かれてきたものである[650]。本稿では，かかる理解のもとで，一般人格権の具体化として，プライバシーに基本権としての保障を提供する理論を，「プライバシー領域論」と呼ぶ。

08 年判決は，ＩＴシステムにはユーザーが意識的に作り出したデータのみならず，コンピュータの自律的処理の過程により産出されるデータも存在しているため，オンライン捜索に対して保護する必要のあるデータは，ユーザーのプライバシー領域に関するデータに限られないから，従来のプライバシー領域論によってかかる新たな危険の発生ないしその実害化を防ぐことはできないと述べている[651]。つまり，プライバシーに関するデータとそうでないデータの分類は，常に，ＩＴシステムにおける「文脈」[652]に依存し変動しうるものであるため，あるデータがどのような意味を持つか，そして，当該データがさらに他の「文脈」に編入される可能性を有する場合に，そのデータの属性がどのように変化するかを，侵入を受けた被処分者が事前に予想することはできない[653]。そしてまた，システムへの侵入によって必然的に，プライバシーのデータだけでなく，すべてのデータの取得がなされうるから，システムのユーザーの全人格像までが解明される結果になりうるということである[654]。

---

649 a. a. O.(BVerfG, Anm.549)Rn.144, 167, 173, 179.

650 a. a. O.(BVerfG, Anm.549)Rn.170, 196～197. Und vgl. BVerfGE 6, 32(41ff)； 27, 344(350ff)；44, 353(372ff)；90, 255(260ff)；101, 361(382ff)；Glaeser, S.58；Wintrich, S.15ff.

651 a. a. O.(BVerfG, Anm.549)Rn.197.

652 08 年判決がいう「文脈」とは，コンテクスト (Kontext ＝context)を意味する。それは，ＩＴシステムを利用するユーザーの位置，用件，事情，各種の状況とその関連性などについての個別的事情と定義されよう(青柳武彦 31～32 頁参照)。

653 a. a. O.(BVerfG, Anm.549)Rn.197.

654 a. a. O.

D. 情報自己決定権による保護の不十分性

最後に，なぜ，既存の情報自己決定権によって，オンライン捜索による人格に対する新たな危険の発生ないしその実害化を防ぐことはできないかという点を取り上げる。

08 年判決は，情報自己決定権は，プライバシー領域論と同様に，内密の私的情報を保護の対象としているものの，特定の領域を守るのではなく，国家ないし私人による内密の私的情報の徴収・調査ないし分析・利用を防ぐ機能を有するとしている[655]。

そのうえで，ＩＴシステム以外の場面であるならば，かかる情報自己決定権により，被処分者の一定の内密の振る舞いに関する利益を十分保護することができるとされる[656]。しかしながら，ＩＴシステムにおいては，先に述べた通り，プライバシーに関する情報(私的データ)とそれ以外の情報とを区別することは原理的に困難であるから，情報自己決定権がプライバシー領域論と同様に，内密な私的情報を保護対象とする限りにおいては，オンライン捜索による人格への新たな危険の発生ないしその実害化を十分に防ぐことはできない[657]。

他方，情報自己決定権による保護を受けるには，政府が自ら広汎なデータ徴収及びデータ処理(加工，分析，消化，照合など)の処分をすることが必要になるところ，オンライン捜索においては政府によるかかる処分が行われない[658]。というのも，個人は，その人格の発展のためにＩＴシステムを利用する必要があり，そのために個人データをシステムの処理に委ねざるを得ず，かつ，その利用過程において，他のデータもシステムの自律作用により生み出されるため，政府が自ら広汎なデータ収集・処理処分を行う必要はなく，現代情報社会におけるＩＴシステムの日常的な利用及び商業的な発展によって自然に結成された成果を利用するだけで足りるからである[659]。それゆえ，政府による広範なデータ徴収・処理処分を必要としないオンライン捜索は，情報自己決定権の保護範囲外になってしまうという帰結になる[660]。

そしてまた，従来の判例によれば，情報自己決定権とは，「個別のデータの徴集」から被処分者を保護するものとされる[661]。これに対して，オンライン捜索の手法は，情報技術システムの全体に侵入し，そこに蔵置されたすべてのデータを対象とするものであって，その侵害性は個別のデータの徴集の場合よりもはるかに重大であるから，従来の情報自己決定権によっては，オンライン捜索によりもたらされる人格への新たな危険の発生ないしその実害化のリスクに十分に対応できていないとされる[662]。

---

[655] a. a. O.(BVerfG, Anm.549)Rn.198～199.
[656] a. a. O.(BVerfG, Anm.549)Rn.202.
[657] a. a. O.(BVerfG, Anm.549)Rn.197.
[658] a. a. O.(BVerfG, Anm.549)Rn.200.
[659] a. a. O.
[660] a. a. O.
[661] a. a. O.(BVerfG, Anm.549)Rn.198, 200； und vgl. BVerfGE 65, 1 (43)； 84, 192 (194).
[662] a. a. O.(BVerfG, Anm.549)Rn.197, 200, 203, 231～232；und vgl. Burkhard&Claudia, S. 107.

３．いわゆるＩＴ基本権

以上を踏まえ，以下では，ＩＴ基本権の具体的な中身及びその必要性についての更なる検討を行う。

(1)ＩＴ基本権の意義

ＩＴ基本権の中身を具体化するには，08 年判決の判示をもとに，次の３点を明らかにする必要がある。すなわち，①ＩＴシステムに対する侵入という場合の「ＩＴシステム」及び「侵入」とは，それぞれ具体的に何を意味するのか，②ＩＴ基本権が認められるための要件は何なのか，③いかなる要件をもって政府によるＩＴ基本権への干渉を正当化することができるか，の３つの点である。

A. ＩＴシステムの意味

「ＩＴシステム」とは，一体何を指すのかという点に関して，学説上は，ＩＴシステムという用語は，内務省（BMI）から提案されたものであり[663]，それは，現在及び将来の科学技術の発展を概括するために意識的に選ばれた広汎な概念であることを踏まえたうえで[664]，保護範囲を固く技術的に画すことによって将来の技術的な革新が封じられること，及び，事情の変化に応じてそれを再定義しなければならないことを防ぐため，08 年判決でいうＩＴシステムを，電磁的データを処理するあらゆるシステムを包括するものと広く理解されなければならないという見解が主張されている[665]。

これに対して，08 年判決はＩＴシステムの意味を正面から定義していないが，本判決の全文からみると，ＩＴ基本権が保護対象とするＩＴシステムは，コンピュータと同様の高度計算能力を有する端末の系統ないしこのような端末の系統を連結するネットワークの系統あるいはそれぞれの系統の集合に限られているように読める[666]。

しかし，このようにＩＴシステムの概念を具体的に定義すると，保護範囲を固く技術的に画することによって将来の技術的な革新が封じられうること，及び，事情の変化に応じて，それを再定義する必要が生じるという問題があることは，学説が指摘する通りである。

このように，ここでの問題の核心は，ＩＴシステムの概念を固めておくと，保護範囲が限定されてしまう一方，逆に，ＩＴシステムの概念を画定しておかないと，ＩＴ基本権による保護範囲

---

663 BMI が使った原語は「情報科学技術システム」である。

664 Siehe die Antworten des BMI auf den Frasgenkatalog des BMJ, http://asser.netzpolitik.orglwp-uploadlfragen-onlinedurchsuchung-BMJ.pdf. Und vgl. Hornung, S.301～302.

665 Hornung, S.301～302.

666 ここでいうＩＴシステムの端末はコンピュータに限られるわけではなく，高度情報処理が可能な多機能端末であるならば，そのすべてを含むものである。この点について，ドイツ連邦憲法裁判所は，ＩＴシステムへの侵入(例えばオンライン捜索)は人間の生活形成の核心的な部分を洞察したり全人格像を完全な構図にしたりすることさえできるという高度な侵害性を有するものであり，ＩＴ基本権はこのような高度な侵害性に応じて与えるべき特別な基本権保護であり，その保護の適用範囲は，個人用パソコンにとどまらず，広範な機能範囲を通じて自由に利用したり多様な個人データを記録・蔵置したりすることができる携帯電話ないし電子メモ帳などにも及ぶとしている(a. a. O.(BVerfG,Anm.549)Rn.197, 203)。

が不明確になってしまうというジレンマが生じることにある。この点に関して，08 年判決は，ＩＴシステムの概念を正面から定義しないことによって，その概念が固定化されることによるＩＴ基本権の保護範囲の制限の問題を避け，ＩＴ基本権による保護範囲については，いわば排除法によりそれを画定している。ここでいう排除法とは，既存の基本権により保護されていない範囲を洗い出した上で，それらのみをＩＴ基本権の保護範囲とする方法をさす。具体的には，ドイツ連邦憲法裁判所は，従来の通信の秘密に関する基本権，住居不可侵に関する基本権，プライバシーに関する権利及び情報自己決定権によって保護できないかそれとも保護しきれない部分（すなわち，08 年判決がいう「保護間隙」）を，ＩＴ基本権の保護範囲と定義している[667]。

B．侵入の意味

08 年判決によると，ＩＴ基本権は，ＩＴ技術の領域における国家による「侵入」から基本権の享有主体の人格及び私的生活領域を守るものであるが[668]，ここでいう「侵入」とは，単に個別のコミュニケーションプロセスあるいは個々の保存されたデータに対する侵入ではなく，ＩＴシステム（その中にあるすべてのデータを含む）に対する全面的な侵入を意味する[669]。そして，かかるＩＴシステムに対する全面的な侵入を遂行するための具体的な手段として，前述したトロイの木馬などのスパープログラムのほか，キーロガーを使用する方法や，スクリーン又はキーボードから漏洩した電磁波の値を測定する方法などが挙げられている[670]。

ここでいう「全面的な侵入」と，基本法 10 条の住居不可侵の文脈でいわれる「憲法により保護された特定の領域への侵入」とは異なるものである。すなわち，政府がオープン領域において散在している断片的な情報を収集するだけでは[671]，基本法 10 条の「憲法により保護された特定の領域への侵入」に当たらないのに対して，かような収集行為だけであっても，それによってあるＩＴシステムの内実ないしかかるシステムの使用者の人格像が解明されうる場合には，それもＩＴ基本権が規制対象とする「全面的な侵入」に該当しうる。

かかる理解は，前述したＩＴシステムにおけるあらゆるデータの全体を捜索するというオンライン捜索の最大の特徴に対応したものであると思われる。というのも，ＩＴ基本権が全面的な侵入を防ぐ機能を持ってはじめて，すべてのデータに対する全面的な探索を行うオンライン捜索に対抗することができると考えられるからである。

しかしながら，ＩＴ基本権が具体的にはいかなる形でこうした「全面的な侵入・探索」を防ぐ機能を果たすのかについては，08 年判決ははっきりと述べていない。

---

667 Vgl. Burkhard &Claudia, S. 105ff ; und vgl. Lepsius, S.42.

668 a. a. O.(BVerfG, Anm.549)Rn.201.

669 a. a. O.(BVerfG, Anm.549)Rn.201.

670 a. a. O.(BVerfG, Anm.549)Rn.205.

671 例えば，前に言及した 08 年判決が挙げた，スクリーンやキーボードから漏洩した電磁波の値を測定する方法などがその例として考えられる。

C．保護要件

08年判決によると，ＩＴ基本権の保護法益を構成する要件(以下，保護要件という)としては，①保護領域によって把握されるＩＴシステムにおいて生産・加工・保存されるデータの秘密性を維持するというユーザーの利益，及び，②保護されるＩＴシステムの不可侵性という２つの要件が挙げられる[672]。

第１の「データの秘密性」の要件とは，08 年判決が示す通り，システムにおいて，生産・処理・蔵置されたデータの内密性を保持することに関する利用者の利益を意味する[673]。これに対し，第２の「ＩＴシステムの不可侵性」要件の具体的な内容については，08 年判決は明言していないが，学説上は，それは，個別のデータを取得されることから保護するという次元を超えて，ＩＴシステムの能率，機能，及び保存内容に対する侵害から保護することも含むものであり，この要件のもとにおいては個人的データの秘密性が侵害されることを必要としないと解されている[674]。言い換えれば，ＩＴシステムの不可侵性という第２の要件は，第１の要件であるデータの秘密性とは関係がなく，ＩＴシステムの完全性――すなわち，現在の社会において一般に期待されるＩＴシステムの能率・機能が正常に稼動すること，及びそこに保存されたデータが，原状のまま蔵置されており，かつ，利用権限者しかアクセスできないこと――を担保することを，その要保護性の内容とするものである。

この２つの保護要件によってはＩＴ基本権の保護範囲についての学際的な記述を可能にさせる[675]と評価されているが[676]，そこには次の３つの疑問点が残されている。

第１に，ＩＴ基本権の場面でいうデータの秘密性と，情報自己決定権でいうデータの秘密性とは，いかなる点が異なるのかである。この点を明らかにしないかぎり，ＩＴ基本権と情報自己決定権との区別が難しいと同時に，ＩＴ基本権の創出の必要性も説明されない。

第２に，データの秘密性とＩＴシステムの不可侵性の２つの保護要件は，いかなる関係にあるのか，言い換えれば，両者は択一関係なのか，それとも，並立関係なのかである。この点についても，08 年判決の判示は不明確である。

第３に，データの秘密性の有無ないしＩＴシステムの不可侵性の有無を判断するための基準が明らかにされていないという点も問題である。この点，08 年判決は，単に，ＩＴシステムへの侵入が容易であることは，憲法上保護される秘密性及び不可侵性の有無の判断に影響しないと述べているだけであって[677]，それ自体が具体的な判断基準とはいえない。

---

672 a. a. O.(BVerfG, Anm.549)Rn.204.

673 a. a. O.(BVerfG, Anm.549)Rn.204.Und vgl. Hornung, S.302～303.

674 Vgl. Hornung, S.302～303.

675 ＩＴ基本権を理解するには，法学分野の知識だけでなく，通信情報科学技術分野の知識も必要不可欠であり，08 年判決が打ち出した「データの秘密性」と「ＩＴシステムの不可侵性」の２つの要件は，法学及び通信情報科学技術の両分野にまたがった知識要素を採り入れたものであって，この２つの要件によって，ＩＴ基本権の内実をいっそう明確に説明することができるということである。

676 Hornung, S.302～303.

677 a. a. O.(BVerfG, Anm.549)Rn.197, 206.

D. 侵害要件

08年判決では，ＩＴ基本権に対する侵害を正当化するための要件(以下，侵害要件という)として，(A)極めて重大な法益に対する具体的な危険の存在[678]，(B)司法の命令[679]，(C)私的な生活形成の核心領域を保護するための予防措置[680]，(D)高度な科学技術的ハードル[681]，という４つのものが挙げられている。

(A)極めて重大な法益に対する具体的な危険

極めて重要な法益とは，08年判決によると，人の身体，生命，自由，あるいはそれに対する脅威が国の存続あるいは人間の生存の基礎に影響するような公共の利益を意味する[682]。そして，具体的な危険は，根拠のない単なる仮定だけでは足りず，その存在を示すことができる事実上の根拠を有しなければならない，とされる[683]。

かかる定義を前提にすると，犯罪が未だ行われておらず，法益侵害の危険があるにすぎない段階であっても，当該危険の存在を示すことができる事実上の根拠がある限り，基本権を侵害する政府の行為を正当化することができることになる。実際にも，08年判決の審理対象は刑事手続の問題ではなく，治安の維持を目的とする行政法規(VSGNW)に基づいて憲法擁護官庁が行う捜索の合憲性の問題であった。しかし，08年判決は，傍論として，一定の要件のもとで，オンライン捜索を刑事訴追の目的に利用することも認められると明示的に述べている[684]。ただし，この場合に「極めて重大な法益に対する具体的な危険」という要件の代わりに，いかなる要件が課されることになるのかは，明示されていない。

(B)司法の命令

司法の命令という侵害要件は，いわゆる裁判官留保原則と同義である[685]。その意味で，これは，ＩＴ基本権の場面に特有なものではなく，他の基本権も共有している侵害要件であるといえる。したがって，この要件により，ＩＴ基本権の独自の意味を説明することはできないと思われる。

(C)私的な生活形成の核心領域を保護するための予防措置

この侵害要件が，具体的に何を意味するかについて，08 年判決は明示的には述べていないが，この点に関連して，ＩＴシステムにより取得されたデータは広い範囲で流用されたり他の当局へ伝達されたりする可能性があるから，それを防ぐための予防措置(以下，「流用・

---

[678] a. a. O.(BVerfG, Anm.549)Rn. 218, 223, 224, 242, 247, 279.
[679] a. a. O.(BVerfG, Anm.549)Rn. 257, 259.
[680] a. a. O.(BVerfG, Anm.549)Rn. 122, 145, 207, 284, 299.
[681] a. a. O.(BVerfG, Anm.549)Rn. 204.
[682] a. a. O.(BVerfG, Anm.549)Rn. 242, 247, 279.
[683] a. a. O.(BVerfG, Anm.549)Rn. 247, 249～250, 279.
[684] a. a. O.(BVerfG, Anm.549)Rn. 207.
[685] 裁判所保留原則 (Vorbehalt der gerichtlichen Anordnung)とも呼ばれる(a. a. O.(BVerfG, Anm.549)Rn.224；auch Graf, §100a Rn109ff； Roggan, S.259)。

漏洩防止の予防措置」という)を必要とするとしている[686]。この判示からすると，流用・漏洩防止の予防措置は，私的な生活形成の核心領域を保護するための予防措置の一例であるようにも思える。

しかし，前述した通り，オンライン捜索には，ＩＴシステムに全面的に侵入し，全人格像（その中に，要保護性が最も高いとされる「私的な生活形成の核心領域」も含まれる）を完全に解析されてしまう危険性があるからこそ，全面的な侵入に対抗するためのＩＴ基本権が創出されたのであり，このことに鑑みれば，ここでの予防措置も，かかる全人格像の完全な解析を防ぎうるものでなければならないはずである。ところが，流用・漏洩防止の予防措置は，かつては情報自己決定権の場面ですでに提起されてきた対策にすぎず，かかる措置のみで，オンライン捜索による全人格像の完全な解析を防ぐことはできないといわなければならない。

それゆえ，08 年判決のいう私的な生活形成の核心領域を保護するための予防措置は，全人格像の完全な解析を防ぐことができるという意味で，ＩＴ基本権の必要性を説明することが可能であると思われるものの，かかる予防措置の具体的な中身が一体何なのかが，やはり不明確なままであるため，この点をもってＩＴ基本権と情報自己決定権とを区別するのは依然として困難があると言わざるを得ないのである。

(D)高度な科学技術的ハードル

08 年判決は，ＩＴシステムが国家によって侵入された場合には，当該システムの性能，機能及び保存の内容が第三者にも利用されてしまう可能性があるため，システムに対する見張り，監視又は操作に際して高度な科学技術的ハードルを採用しなければならないとしている[687]。

確かに，「第三者にも利用されてしまう可能性がある」という点は，ＩＴシステムに特有の問題である。具体的には，あるＩＴシステムがいったん国家によって侵入されたら，他の第三者がこの国家によるＩＴシステムの侵入に便乗し，当該システムの性能，機能及び保存の内容にアクセスしたりそれらを利用したりする可能性があるということを意味している[688]。

これを踏まえて考えると，08 年判決が示した高度な科学技術的ハードルとは，国家がオンライン捜索を行おうとするならば，まず，対象となるシステムが政府にオンラインで侵入された状態を他の第三者に利用されてしまうという便乗行為の可能性を防ぐために有効な科学技術上の対策を講じておかなければならないということを指すと考えられる。言い換えれば，国家がかかる有効な科学技術上の対策を講じないかあるいはそれができない場合は，ＩＴ基本権への侵害を憲法上正当化することができず，ＩＴ基本権を侵害するオンライン捜索を行うことができないということである。

---

[686] a. a. O.(BVerfG, Anm.549)Rn.122.

[687] a. a. O.(BVerfG, Anm.549)Rn.204.

[688] a. a. O.

この意味で，高度な科学技術的ハードルは，ＩＴ基本権に対する特別な危険を防ぐために，国家によるＩＴシステムに対する見張り，監視，操作行為を規制する特別な侵害要件であるということができ，この点から，ＩＴ基本権と既存の他の基本権との区別が説明されように思われる。

E. 小括

以上を確認すれば，次の３点が重要である。

第１に，08 年判決が作り出したＩＴ基本権とは，ＩＴシステムの全体に対する全面的な侵入並びにシステム内にあるすべてのデータに対する全面的な探索に対抗しようとするものである。

第２に，その法益性（基本権としての要保護性）をなす核心的な要素としては，データの秘密性とＩＴシステムの不可侵性の２つの保護要件が挙げられる。

第３に，全人格像の完全な解析を防ぐために必要な予防措置及び高度な科学技術的ハードルという２つの特別な侵害要件により特徴付けられているものである。

(2) ＩＴ基本権の創出の必要性

前述した通り，08 年判決は，正面からＩＴ基本権の意味ないし保護範囲を画定することなく，排除法をもってそれを行った。そして，既存の基本権によって保護できないかあるいは保護しきれない部分についての 08 年判決の排除法的説明が不十分であったために，ＩＴ基本権を新たに創出する必要性について，ドイツにおいては激しい論争が繰り広げられている[689]。

この点につき，前に挙げた 08 年判決の説明によれば，伝送過程という要素を必要とする基本法 10 条（通信の秘密）や，保護の範囲を物理的な空間に対する有形・無形の侵害に限る基本法 13 条（住居不可侵）によっては，蔵置されたデータを対象としながら物理的な空間という概念から離れているオンライン捜索の問題に対応することはできない。また，プライバシー領域論との関係では，そこでいう領域概念が物理的な空間のみを指すという前提に立つならば，物理的空間に依存しないオンライン捜索の問題に対応することができないという帰結が導かれよう。

しかしながら，通信の秘密の保護が，なぜ伝送過程を必要とするのかについては疑問があるし，また，仮に，領域の概念ないし住居不可侵でいう場所の意味をバーチャル空間にまで拡張することができるとすれば，前述した結論も変わるはずである。

さらに，情報自己決定権によってオンライン捜索に対応することができないという点についての 08 年判決の説明は，通説的な立論とはいえないし，また，論理上も矛盾や不十分な点があるため[690]，この部分は，ＩＴ基本権の創出を必要とする 08 年判決が打ち出した諸々の論拠のうち，

---

[689] Lepsius, S..21ff, Burkhard &Claudia, S. 107ff, Hornung, S. 301ff.

[690] 08 年判決は，情報自己決定権により保護されない部分や保護できない部分をＩＴ基本権の保護範囲とする，いわば排除法を採用しつつも，ＩＴ基本権は情報自己決定権と重なる部分があると認めている。また，ＩＴ基本権は，情報自己決定権を超えて，個人の行動の自由ないしプライバシーに関する憲法上の保護を強化・拡大することを図るという保護強化機能を有すると述べているものの，この保護強化機能の具体的な中身を明らかにしていない。

最も批判されている箇所である[691]。

そこで，以下では，ＩＴ基本権と通信の秘密ないし住居などのプライバシー領域との関係，及びＩＴ基本権と情報自己決定権との関係という２点に絞って，更なる検討を行いたい。

A．通信の秘密，住居不可侵，プライバシー領域との関係

仮に，通信の秘密の保護には伝送過程を必要とせず，また，領域の概念ないし住居不可侵でいう場所の意味をバーチャル空間まで拡張するとすれば，ＩＴ基本権を保障する必要性は変わるのであろうか。この点を検討するためには，その前提として，デジタル通信(例えば，インターネット)において採用されている分散システムとパケット交換の２つの技術の仕組みを把握しておく必要がある。

(A)デジタル通信におけるパケット交換技術の仕組み

分散システムとは，デジタル通信を実現するための伝送システムを指し，伝統的な電話回線システムの採用する中央システムと対置される概念であり，パケット交換技術のルーティング(経路制御)機能により働くものである[692]。

次に，パケット交換技術とは，ルーター(データを異なるネットワーク間に中継する通信器機)間でデータの小包(パケット)をルーティングする通信方式である[693]。具体的には，原始データをPAD(Packet Assembly Disassembly)というマシンによってコピー(一時的蓄積)したうえで，複数のパケットに分解・変換したり，ヘッダーを付加したりして伝送し，交換機の記憶装置に蓄積し，中継伝送路が空いている時間に送り出し，それが受信側の交換機の記憶装置に蓄積された後に送出され，到着後，付加されたヘッダーの部分を削除し，PADで元のデータに還元した上で，受け手の端末に届かせるという仕組みになる[694]。

ここでいうパケットとは，付加されたヘッダー(下掲の図４で示す点線内の方形の灰色の部分)[695]，原始データをコピーしたうえで分割した一部のコード(図４で示す灰色のヘッダーと結合した白色部分)[696]，という２つの部分からなるものを指す。かかる交換過程においては，ビット(Bit)が最小の単位となり，１ ビットの価は１あるいは０により表記され，情報処理手続(EDV)はビットを処理単位とした０と１との組み合わせによって進められる[697]。

また，内容を判読するためのコールサインは，それぞれのビットの組み合わせを割り当

---

691 Burkhard &Claudia, S. 107; Lepsius, S.22, 31.

692 田村6，118頁。パケット交換技術のルーティング機能とは，パケットを伝送するため，コンピュータ・ネットワーク上での最も効率的な経路を見つけだす役割を果たすものである（田村論文同頁のほか，ウィキペディア―サーチワード：ルーティング〈経路制御〉，井上伸雄・通信技術のすべて122～125頁をも参照)。

693 井上伸雄12頁；同・通信技術のすべて122～125頁；村田31頁；ウィキペディア―サーチワード：ルーティング，パケット通信，データリンク層，ルーターを参照。

694 同前注。

695 この部分のコードは，送り手，受け手などの情報やその他の通信処理の記録情報等の，いわゆる「通信履歴情報」の部分を指す。通信履歴情報は，通信内容情報と対置され，「非内容的情報」とも呼ばれる。

696 この部分のコードは，通信の「内容」(content)の部分をさす。

697 Hansen/Neumann, S. 7.；Korge, S.6(n25).

てる必要があり，このようにして割り当てられたビットの組み合わせをコードと呼ぶ[698]。なお，パケットをどのルートで転送するかを決める機能をルーティング機能と言い，具体的には，①転送時間の最小のルートを選択すること，②ネット内のトラフィック量を均等化し，一箇所にトラフィックが集中しないようにすること，及び③伝送路や交換機に障害があれば別のルートを迂回させること，という３つの基準に従って転送ルートが決定される[699]。

以上の説明を図式化したものが，次の図４である。

図４について、インターネット公表に対する著作権者からの許諾が得られていないため，非公開とする。

図４　インターネットにおけるパケット交換技術の具体的な動き方について[700]

ここに示されているように，パケット交換技術は，ルーターというマシンを通じて，中継伝送路の空いている時間にパケットを送り出す機能を有しているから[701]，ＩＴ通信の分散システムにおいては電話回線通信の中央システムと異なり，情報を伝送するために一定の伝送経路をあらかじめ確保しておく必要がないこと，及び，パケット交換は，音声をそのまま伝送する電話回線通信の仕組みと異なり，原始のデータをそのまま伝送するわけでなく，原始のデータをコピー・分解・変換・蓄積・還元する仕組みになっていることが分かる。

(B) ＩＴシステムにおける領域の区画とデータの属性

(A) で示したパケット交換技術の仕組みゆえに，ＩＴシステムを対象にした捜査によって得られるのは，あくまで目標となる情報を構成する部品にすぎず，従来の写真撮影や電話傍受のように，目標となる情報そのものを取得できるわけではない[702]。つまり，写真撮影や

698 Korge, S. 7.

699 田村 118 頁。前掲注 523 に挙げた文献をも参照。

700 この図は筆者が井上伸雄 12 頁の図１をもとに若干手を加えたものである。

701 複数の空いている経路がある場合は最も効率的な経路を選ぶことになる。分散システムのもとでは，システム全体をコントロールする中央センターを観念することができず，最も効率的な経路の選択及び判断は，個々の転送機器（例えば，ルーター，交換ノードなど）によって行われる（田村 118 頁のほか，前掲注 523 に挙げた文献をも参照）。

702 傍受との関係では，次の点が重要である。まず，中央システムの場合には，情報を伝送するために一定の回線をあらかじめ決めて確保しておく必要があるのに対して，分散システムの場合には，情報を伝送するために一定の回線を確保しておく必要はない。他方で，ＩＴシステム通信の場合は，情報が通るルートを予測しておくことができなくなるから，傍受が一層困難となると同時に，単一の原始情報を複数のパケットに分解したうえでシステムにおける複数のルートに

電話傍受を実施する場合には，分割されていない状態での画像や音声をそのまま取得できるのに対して，捜査機関がＩＴシステムにおける伝送中のデータをキャッチしようとする場合には，対象となるデータ全体から分解されたバラバラのコードしか取得できない。この点は，既に端末に蔵置されたデータを対象として，それを遠隔操作により取得する場合(例えば，オンライン捜索)も同様である。それゆえ，少量のバラバラのコードを入手するだけでは，目的たる情報(原始データの全貌)を復元することができず，捜査目的を達成することは不可能になる。

しかし，他方で，捜査機関が取得したコードが一定の量に達すると，適切なツールを使い，それぞれのコードを取得した当時の文脈を手がかりにして，コード同士の組み合わせの可能性を推算することにより，一部のコードからであっても原始情報の全貌を逆推知することが可能となり，ひいては，ＩＴシステムを利用するユーザーの全人格像を完全に解析することすら可能となる[703]。

以上の通り,通信の秘密,住居不可侵,プライバシー領域論による保護を与える前提としては,あらかじめ,通信の秘密にあたるデータとそうでないデータ,住居である領域とそうでない領域,プライバシーに属する範囲とそうでない範囲を確定しなければならないが，ＩＴシステムにおいては，まず，住居を観念することがありえない。また，分散システム並びにパケット交換技術が採用されているため,プライバシー領域とそれ以外の領域を区別することは原理的に不可能であるし，データの属性は文脈ごとに変わってくるので[704]，プライバシーのデータとそうでないデータとの区分が観念できないため,通信の秘密にあたるデータとそれ以外のデータを選別することにも無理がある。

以上により，通信の秘密の保護のために伝送過程を不要とし，また，領域の概念ないし住居不可侵でいう場所の意味をバーチャル空間まで拡張したとしても,それは意味をなさないことがわかる。つまり，通信の秘密，住居不可侵並びにプライバシー領域論における保護間隙は，いずれにしても残るのであり，ＩＴ基本権の必要性が認められるのである。

B. 情報自己決定権との関係

ここで取り上げるべき問題点は，次の３つのものである。

(A)情報自己決定権によってはオンライン捜索の侵害に対抗することができないとする

おいて分散で伝送する仕組みになるので，対象となるデータをキャッチするために，電話回線のように１本の通信回線ごとに傍受の単位とすることも不可能になり，あらゆる(仮想の)通信回線を傍受の対象としなければならないことになる(See Lessig, at 63＝邦訳：山形浩生， 柏木亮二（訳） 89 頁。また，大橋・基礎編 61 頁(注 49)及び同 222 頁以下の説明をも参照)。

[703] 青柳武彦 32 頁，堀部(編著)・インターネット 99～118 頁[李]などを参照。具体的には，住所や誕生日などの個人情報の収集はもちろんのこと，個人の習慣，性格，好みないしその人と関連するあらゆる事柄(例えば，恋人，ペット，家族，仕事など)を解明しながら，それによってさらにその個人の人格に関する全面的なプロファイルを形成・更新していくことまでもができるようになる。

[704] 当初はプライバシー的属性を有さない情報(例えば，単なる断片的なコード)であっても，ＩＴシステムの文脈を通じて，プライバシーに関する情報ないし個人の人格に関する全面的なプロファイルまでにも変容しうる。

08 年判決があげた３つの理由[705]が果たして妥当なのであろうか。

(B) ＩＴ基本権の場面でいうデータの秘密性と従来理解されてきた情報自己決定権でいうデータの秘密性とはいかなる点が異なるのか。

(C)08 年判決は，ＩＴ基本権の保障は，情報自己決定権を越えて，個人の行動の自由ないしプライバシーに関する憲法上の保護の強化・拡大を図ろうとするものである(以下「ＩＴ基本権の保護強化機能」という)と述べている[706]。しかし問題は，08 年判決が，このＩＴ基本権の保護強化機能が，具体的にいかなる内容をもつものかについて，明確に述べていないことである。

(A)08 年判決があげた３つの理由について

①私的データと非私的データの区別の困難性

私的データと非私的データとを区別することが困難であるという 08 年判決があげた第 1 の理由に関して，確かに，当初，情報自己決定権の保護範囲は秘密領域や私的領域に限られるとされてきた[707]。しかしながら，その後の判例の展開は，それらの領域に関わらない場面にも及び，自己決定権(人格的自律権)に焦点を合わせるものであるとされる[708]。そのリーディングケースとして，1980 年代の連邦憲法裁判所による Eppler 決定[709]と Böll 決定[710]があげられており，これらは，いずれも，公の場における発言が問題となった事案であって，秘密や私的領域と関係していない[711]。とりわけ，前者の決定は，情報自己決定権の適用は，「個人の私的領域に限定されない」と明示的に述べている[712]。他方，連邦憲法裁判所は，国勢調査判決において，「自動データ処理を前提とすれば，もはや重要でないデータは存在しない」[713]と指摘して，いわゆる情報自己決定権を明示的に認めており，かかる権利を，「自己決定の思想から導かれる個人の権能であって，個人的な生活状態をいつ，いかなる限界内において打ち明けるかについて，原則として自ら決定する[権利である]」[714]と定義している。

学説においては，以上の判例の発展に鑑み，情報自己決定権を認めたことによって，情報の保護に関しては，「私生活の内密性の保護から自律的決定の保護へと移ってきている」

---

[705] すなわち，前述した，①複雑な IT システムにおいては私的なデータと非私的なデータを区別し難いこと，②オンライン捜索を行うに政府が自ら広汎なデータ徴収・処理をしなくとも，IT システムの自律的作用によって形成された巨大な資料庫を利用することができること，及び③オンライン捜索は，個別のデータに対して徴収を行うわけではなく，システムの全体に侵入しそこにあるすべてのデータを対象とするものであること，という３つの理由である。

[706] a. a. O.(BVerfG, Anm.549)Rn.198.

[707] BverfGE 27, 1(7), und vgl. Vogelgesang, S. 45. 松本和彦・基本権の保障(三)798 頁をも参照。

[708] 松本和彦・基本権の保障(三)798 頁，王澤鑑・人格権 234～238 頁参照。

[709] BVerfGE 54, 148；松本和彦・基本権の保障(三)799 頁をも参照。

[710] BVerfGE 54, 208；松本和彦・基本権の保障(三)799～800 頁をも参照。

[711] 前掲注 709，注 710 参照。

[712] BVerfGE 54, 148(155)；松本和彦・基本権の保障(三) 800 頁をも参照。

[713] BVerfGE 65, 1(45)；また，松本和彦・基本権の保障(二)354～355 頁，永田＝松本＝倉田(訳)127 頁をも参照。

[714] 原文は BVerfGE 65, 1(42)を参照。括弧内の翻訳は永田＝松本＝倉田(訳)128 頁からの引用である。

と評し[715]，さらに一歩進んで，「情報自己決定権によってはじめて，個人情報は，秘密性の有無に関係なく，包括的に憲法の保障対象になった」とする見解も現れている[716]。

このように，私的データと非私的データの区別が，果たして情報自己決定権を適用するために必要なのかには疑問がある。そして，仮に，この要件が不要であるとすれば，情報自己決定権の保護を主張するためには，私的データとそうでないデータとを区別することがその前提条件であるとし，そのうえで，情報の性格を問わずに全面的な保護を図るために，情報自己決定権とは別に，ＩＴ基本権の創出が必要としている 08 年判決は，その論拠を失ってしまうことになる。

この点，ドイツの学説には，情報自己決定権の適用は，必ずしも私的データと非私的データの区別という要件を必要とするものでないのに，08 年判決が情報自己決定権の保護範囲を減縮することにより，ＩＴ基本権の保護範囲のためのスペースを作り出しているという指摘をするものがある[717]。

しかし，さらにひるがえって検討すると，連邦憲法裁判所が，情報自己決定権の適用にあたって，領域理論的思考――これを，ＩＴシステムの場面に照らして言い換えれば，保護される私的領域に関わるデータとそうでないデータの区別を必要な要件とする考え方になる――を放棄し，情報の性格を問わなくなったといえるかどうかについては争いがある[718]。というのも，ドイツにおいては，学説上は現在でも領域理論が依然として支配的であるとされており[719]，判例上においても領域理論が採用されているようにみえるからである[720]。

このように考えれば，情報自己決定権の保護対象を，私的データに限られるものであると理解した 08 年判決は，従来の判例ないし支配的学説に従ったものということになろう。

②広汎なデータ徴収・処理の有無

08 年判決が指摘した通り，高度発展していく自律のＩＴシステムが，自動的かつ継続的に巨大な資料庫を形成しつつあるのが現在の情報社会の実情[721]であるから，オンライン捜索を行う際にＩＴシステムに侵入することさえできれば，政府は，自ら広汎なデータ収集・処理処分を行うことなく，ＩＴシステムの自律性による広汎なデータ収集・処理の成果をそのまま利用することができる。それゆえ，情報自己決定権が侵害されたといえるためには，政府自身による広汎なデータ徴収・処理を必要とするならば，08 年判決の分析した通り，オンライン捜索が広汎なデータ

---

715 松本和彦・基本権の保障(三)794 頁。そしてドイツの関連学説につき，同論文 816 頁注 7 に挙げられた諸文献を参照されたい。

716 松本和彦・基本権の保障(三)804 頁。

717 Burkhard & Claudia, S.107.

718 松本和彦・基本権の保障(三)803 頁。

719 ショラー(著)／嶋崎(訳)の注１及びそこに挙げられた文献を参照されたい。そして，松本和彦・基本権の保障(二)355 頁／同(三)803 頁をも参照。

720 リーディングケースとしては，いわゆる日記決定(BVerfGE 80, 367)があげられる。また，BVerfGE 80, 367(373ff)；und vgl. Geis, S.112ff；そして松本和彦・基本権の保障(三)803～804 頁をも参照。

721 この実情についての詳細は，堀部(編著)・インターネット[李]99～118 頁，石村＝奥平(編)・知る権利[佐藤]168～169 頁の説明を参照されたい。

徴収・処理を必要としないがゆえに，情報自己決定権を侵害しないことを理由に，ＩＴ基本権の必要性を説明することができるだろう。

しかしながら，ドイツの学説の中には，情報自己決定権の侵害を認めるためには，必ずしも広汎なデータ徴収及びデータ処理の処分を必要としないとする見解もある[722]。これによれば，広汎なデータ徴収及びデータ処理の処分という点が，ＩＴ基本権と情報自己決定権とを区別するためのメルクマールにはならない。

さらに，オンライン捜索は，政府が，自ら広汎なデータ収集・処理処分を行うことなく，ＩＴシステムの自律性による広汎なデータ収集･処理の成果をそのまま利用することができるものであるとする 08 年判決の理解に対して，学説には，なぜオンライン捜索による侵害がデータ徴収及び処理に当たらないといえるのかという疑問を提起するものもある[723]。というのも，広汎なデータ収集・処理の成果をそのまま利用することも，一種の広汎なデータ収集・処理処分に当たるものとも考えられるからである。言い換えれば，オンライン捜索を用いてＩＴシステムに侵入することにより，大量のデータを政府が手に入れることも広汎なデータ収集といえるし，また収集したデータをそのまま使える場面もあれば，そうではなく，捜査の目的に合わせて更なる分析や照合などの処理を行うことが必要となる場面もありうるから，その意味でデータの処理にあたるということができるのではないかということである。

③個別のデータの徴収

08 年判決は，情報自己決定権の侵害を認めるためには個別のデータの徴収が必要であることを前提として，１つのＩＴシステムに対する全面的な侵入により，すべてのデータを探索の対象とし，関連性が確認されない大量のデータの徴収を行う場面(すなわち，オンライン捜索)を，情報自己決定権の保護範囲から除外したうえで，それをＩＴ基本権の保護範囲に帰属させている。しかし，個別のデータの徴収という要件の要否については争いがあるし，また，仮にそれを認めたとしても，例えば，１つのＩＴシステムに対する全面的な侵入をするものの，関連性が確認されない大量のデータの徴収を行わずに，個別のデータを単位として徴収することも可能であり，かような個別の徴収のみを捜査の目的とする場合には，ＩＴ基本権と情報自己決定権とを区別できなくなるという指摘もなされている[724]。

また，08 年判決は，情報自己決定権の保護を主張するためには個別のデータの徴収が必要であるとする論拠として，国勢調査判決[725]を挙げている[726]。しかし，これに対しては，国勢調査判決は，情報自己決定権を認めることにより，現代のデータ処理という前提条件のもとにおいて，個別のデータの徴収からのみならず，大量のデータの蓄積・分析により，個人の掌握及び人格の形成を迫られることからも，個人を保護することを意図していると

[722] Hornung, S.301, und vgl. Lepsius, S.29.
[723] Lepsius, S.30.
[724] Burkhard &Claudia, S. 107.
[725] BVerfGE 65, 1(43).
[726] a. a. O.(BVerfG, Anm.549)Rn.198～199.

いう理解もある[727]。

以上の通り，個別のデータの徴収を必要とするか否かで，情報自己決定権とＩＴ基本権とを区別することには，必ずしも合理性がないと思われる。

(B)データの秘密性について

次に，ＩＴ基本権におけるデータの秘密性と情報自己決定権におけるデータの秘密性との異同を検討する。

この点について，もしＩＴ基本権におけるデータの秘密性が，データ自身の属性(性質・性格)に照らして私的データに当たることを意味するのであるならば,それは情報自己決定権におけるデータの秘密性と異ならないものである。しかし，逆に，ＩＴ基本権におけるデータの秘密性とは，必ずしもデータ自身の属性に着目するものでないと考えられるとすれば，ＩＴ基本権と情報自己決定権とは異なることになり，ひいては，ＩＴ基本権の必要性が認められることになる。本稿は，以下の理由で，後者を支持する。

まず，学説上，データの秘密性とシステムの不可侵性の２つの保護要件については，後者こそが目標たるシステムを嗅ぎ出したり監視したりあるいは操作したりすることが許容されるかどうかを判断するための基準であるとする見解がある[728]。他方，08 年判決は，データの秘密性とは，ＩＴシステムにおいて，生産・処理・蔵置されたデータの内密性を保持することに関する利用者の利益を意味するとし，あるデータがどのような意味を持つかはＩＴシステムにおける「文脈」に依存し変動しうるものであると指摘したうえで，それに対応するため，ＩＴ基本権によって，プライバシー領域に関わらないものであるようにみえるデータないし単なる断片的なコードなどの情報にも保護を与える必要があるとしている。

そうすると，08 年判決でいうデータの秘密性は，データ自身の属性に照準を合わせるものではないと思われる。というのも，08 年判決は，データの属性自体も決まったものではなく，プライベットに属するものやそうでないものが文脈ごとに変動しうるものであると指摘しているからである。言い換えれば，システムの不可侵性により保護されるシステムにおいて生産・処理・蔵置されたデータであるならば，それらのすべては秘密性を有するものと見なすというのが 08 年判決の論旨であろう。

以上の通り，ＩＴ基本権の場面でいうデータの秘密性とは，データ自体の属性とは直接の関係がなく，ＩＴシステムの不可侵性により保護されるシステムにおけるすべてのデータは秘密性の保護を享有することを意味するのに対して，情報自己決定権でいうデータの秘密性とは，個々のデータ自体の属性から判断すべきものであり，内密的な属性を有するデータを指す。そうだとすれば，ＩＴ基本権と情報自己決定権は区別できることになる。

[727] Lepsius，S.30.

[728] Burkhard ＆Claudia，S.105.

(C)IT基本権の保護強化機能について

最後に，IT基本権の保障は，いかなる形で，情報自己決定権を越えて，個人の行動の自由ないしプライバシーに関する憲法上の保護を強化・拡大することができるのかという問題を検討する。

①客観的権利保護論

IT基本権と情報自己決定権とを区別する08年判決の結論を正当化しようとすれば，ここまでに検討した08年判決が挙げた理由のほかに，次の理由も考えられよう。

まず，08年判決は，ITシステムは，現在きわめて高度化・複雑化しているため，個人のユーザーが有効な社会的ないし技術的な自己防衛を行うには重大な困難があると指摘し，そこから，ユーザーに自己防衛義務を課すことの正当性を否定している[729]。Lepsiusは，この08年の立場を踏まえた上で，個人がITシステムにより技術的に支配されているため[730]，人格関連に基づく保護目的から解放することが望ましいとして[731]，「主観的権利を超えた事実上的チャンス」は保護するに値すると述べたうえで[732]，08年判決が打ち出したこの新しい基本権(すなわち，本稿のいうIT基本権)は，主観的抵抗権の古典的な基本権的機能[733]ではなく，「客観的基本権思想」の範囲内に帰属するものであるとしている[734]。

このLepsiusの見解を理解するには，ドイツにおける基本権の二重機能論を把握しておく必要がある。まず，ドイツにおいては，基本権には防禦権と保護義務の二重の機能があるとされる[735]。このうち，防禦権とは，人格の主体である個人が国家の侵害を抵抗する権利を有することを意味し，これは，すなわちLepsiusが述べた「主観的抵抗権の古典的な基本権的機能」そのものである。他方，「客観的基本権思想」の論拠は，保護義務という機能に求められる。保護義務とは，国家が一定の法益(人格に関わる利益に限らない)に対し必要な保護を提供すべきという憲法上の要求を意味する。

つまり，08年判決が打ち出したIT基本権が，人格に関わるデータから離れて独立した

---

729 a. a. O.(BVerfG, Anm.549)Rn.108,207.

730 市民は，現代社会においての日常生活を遂行するためにやむをえずITシステムの利用を必ず必要としているという意味での支配をいう。

731人格関連に基づく保護目的については，従来，その要保護性の根拠は，人格的自律権(自由な意思に基づく自己決定の権利)に求められてきたため，仮に，ITシステムの場合にも，かかる保護目的に従うものとすると，ユーザーには自己防衛義務があるという帰結になろう。というのも，ユーザーは，人格的自律権の行使として，インターネットに接続することによりオンラインで侵入される可能性を予見し得るにもかかわらず，適切な防御措置を取らないまま接続するとすれば，かような権利行使による不利益な結果(侵入されたこと)を甘受しなければならないと解されるからである。

732 Lepsius, S.34.「主観的権利を超えた事実上的チャンス」は，「人格的利益を超えた非人格的利益(例えば，ITシステムの利用可能な状態や，かような状態が保持されることにより得られる便利への期待など)」と言い換えることができる。

733 ドイツにおいては，古典的な基本権は，「市民の国家に対する主観的な自由権」(主観的権利)と理解されてきた(永田＝松本＝倉田(訳)50頁)。そして，基本権の古典的機能は，「侵害を予防的に排除する」という点に求められてきた（永田＝松本＝倉田(訳)35頁)参照。

734 Lepsius, S.34. 類似する見解として，Hornung, S.302ffをも参照。

735 松本和彦(訳)・防禦権60頁。

ITシステムの不可侵性の要保護性を主眼とするものであるとすれば，IT基本権は，主観的基本権としての防御権(人格的利益のみを保護の対象とする)ではなく，保護義務(その保護範囲は非人格的利益にも及ぶ)から導かれた客観的基本権であるということになる。このように考えると，客観的権利であるIT基本権は，人格に関連するデータを保護の対象とする情報自己決定権を超えて，人格に関連しないデータや，内部において人格に関わる内密なデータが存在しないと一般に考えられるシステムなどについても，ITシステムの不可侵性という非人格的要保護性要素が存在するといえるかぎりは，保護するものであることになる。この意味で，客観的権利としてのIT基本権は，主観的権利としての従来の情報自己決定権を超える「保護強化機能」を果たすものといえよう。

②権利放棄論の否定

08 年判決以前は，利用者がインターネットに接続することによりオンラインで侵入される可能性を予見し得るにもかかわらず，適切な防御措置を取らずにそのまま接続した場合，家宅内から任意に流出した音声等の情報が誰にでも受け取られてしまう場合と同様に，基本権侵害を主張することはできなくなるとする見解が一般論として存在していた[736]。また，本件における専門家証人の意見によれば，ITシステムへの密かな侵入は困難な作業であり，とりわけ，標的たるITシステムのユーザーが技術的なセキュリティ措置を採用したり，オペレーティング・システムを定期的に更新したりしている場合にはその困難性が顕著になり，少なくとも侵入するまでの所要時間が大幅に長くなるのは間違いないから，現在の技術によれば，ユーザーが効果的な侵入防止措置を講じることが可能であるとされる[737]。これらの点に鑑みると，ユーザーが自ら防御しないという事実を権利放棄と解することも十分可能であるように思われる。

これに対して，08 年判決は，IT基本権を認めるべきであるという前提に立った上で，次のように述べている。すなわち，ユーザーがITシステムへの侵入を防ぐための措置を講じることが可能だとしても，防衛措置を実施するためには高額の支出が必要になるばかりでなく，かかる措置の採用によりシステムの性能が低減する可能性もあるし，また，IT技術の複雑さ及び進展の速さに鑑みると，どのような科学技術による防衛の可能性があるかを正しく予想することができないから，個人のユーザーにかかる措置を講じる義務を課すのは過重負担というべきであり，ユーザーが防衛措置を講じなかったからといって，それを直ちにユーザーによる権利放棄と解することはできない[738]。

このように，IT基本権については，ユーザーが自ら防御しないという事実を権利放棄とは解しないとすれば，IT基本権は，個人の行動の自由ないしプライバシーに関する憲法上の保護を強化・拡大する機能を担っていると言えよう。

---

[736] Vgl. Kutscha, S1170. ;Rux, S.292.

[737] a. a. O.(BVerfG, Anm.549)Rn.10.

[738] a. a. O.(BVerfG, Anm.549)Rn.108, 207.

C．小括

ＩＴ基本権と既存の他の基本権との関係――言い換えれば，ＩＴ基本権の必要性――を確認すると，次の２つの点が重要である。

第１に，ＩＴシステムにおいては，住居という概念を観念したりプライバシー領域とそれ以外の領域とを区別したりすることは原理的に不可能であるし，また，データの属性は文脈ごとに変わってくるものがあるから，住居不可侵に属する領域とそうでない領域，プライバシーに関わるデータとそうでないデータ，ないし通信の秘密にあたるデータとそれ以外のデータ，を区別するのは不可能である。このことからは，伝送過程論ないし物理的な場所などの要件の如何を問わずに，通信の秘密，住居不可侵並びにプライバシー領域論による保護の間隙があることを説明することができる。

第２に，情報自己決定権との関係では，仮に，①私的なデータと非私的なデータの区別困難，②広汎なデータ徴収・処理，③個別のデータに対する徴収，の３つの要件を緩和し，それらをもってＩＴ基本権と情報自己決定権との限界を画そうとする 08 判決の理由付けは適切でないということができるとしても，ＩＴシステムの不可侵性という保護要件からも，ＩＴ基本権と情報自己決定権とを区別することができる。というのも，この新しいＩＴ基本権は，主観的権利の保護を提供するものではなく，客観的権利の保護を図るものであるし，また，ＩＴシステムの不可侵性という要件により保護されるシステムにおいて生産・処理・蔵置されたデータであるならば，それらのデータのすべては秘密性を有するものと見なすため，あらゆるデータに対して保護を与えることができるのに対して，情報自己決定権は，主観的権利であって，かつ，個々の個人データに対する保護しか提供できないものだからである。

Ⅲ．台湾への示唆と検討

以下では，第１章の検討成果をもふまえて，ⅠとⅡにおいて検討したアメリカとドイツの議論の成果を抽出したうえで，情報を捜索の対象とする場合のあるべき法益論について検討することにしたい。

１．新しい科学技術による権利の侵害と保護

ここまでの検討で示された通り，アメリカにおいては，ドイツでいうＩＴ基本権に相当する保護法益(すなわち，Kerr のいう新しい科学技術におけるプライバシー，Solove のいう情報プライバシー)の位置づけについて，制定法により保護すべき法益にすぎず，基本権にはあたらないとする立場(非基本権説)と，憲法により保護すべき法益であって基本権にあたるとする立場(基本権説)が対立している。

そして，その対立の背景には，立法と司法の構造に対する異なる理解がある。すなわち，非基本権説に立つ Kerr は，立法機関には司法機関よりも優れた構造上の能力があるから制

定法(立法)による対応が適切であるとするのに対し，基本権説に立つ Solove は，立法機関にはそのような能力がないし，また，そもそもかかる問題への対応の最善策としては，憲法(司法)と制定法(立法)の両者によって対応すべきであるとする。

これに対して，ドイツにおいてはかような対立状況はなく，現在では基本権説が支配している。かつては異論があったものの，08 年判決が出されて以降，ＩＴ基本権という用語を使う必要があるかどうかという点はともかく，同権利に相当する保護法益の実質をなす①「データの秘密性」と②「ＩＴシステムの不可侵性」という２つの要保護性の要素が基本権性を持つことが，議論の共通の前提となっているので，憲法(司法)と制定法(立法)の両者による対応が取られるべきであるという帰結になる。

この意味で，ＩＴ基本権という新しい権利を作り出すことの必要性についての争いは基本法上の根拠をどこに求めるかという問題にすぎないから，台湾の立法論を考えるにあたって意味を持つのは，むしろ，ＩＴ基本権の必要性を巡る争いで暗黙の前提とされている部分，すなわち，ＩＴ基本権の内実をなす①と②の２つの要保護性の要素が，果たして中華民国憲法においては基本的人権として保護すべき実質を持っているかという点である。

２．財産権に基づく視点と住居不可侵による保護の限界

台湾の先行研究においては，中華民国憲法 10 条における「住居する自由」の意味を，「住居に対して正当な理由もなく侵入あるいは捜索してはならない」という「住居不可侵」の法益を保護するものであると解しつつ[739]，正当な理由(または相当な理由)があることを前提に，住居を侵入ないし捜索するには法律により定められた条件と手続によらなければならないとして[740]，同条をアメリカ修正４条の定めと並べて比較する論者がある[741]。また，本稿の主な比較素材である日本国憲法 35 条は，アメリカ修正４条に由来するものといわれてきた。他方で，前述した通り，Kerr は，アメリカ連邦憲法修正４条における財産権に基づく視点を指摘しているが，これは，ドイツの基本法 13 条で定められた住居不可侵という法益による保護の限界に関わる，従来の理解と同じ内容のものであるように思われる。

以上により，中華民国憲法 10 条の住居不可侵という法益の内実を考えるには，日本の憲法 35 条，アメリカの修正４条及びドイツの基本法 13 条における住居不可侵という法益による保護の限界に関わる理解を検討することが有益である。

この点，まず，Kerr が指摘する，アメリカの修正４条を解釈適用するには財産権に基づく視点が支配的であるという点については，日本でも同様な状況がある。古い裁判例ではあるが，東京高裁昭和 28 年 7 月 17 日決定判時 9 号 3 頁(以下，「昭和 28 年決定」という)は，家屋管理者の承諾により盗聴器を設置し盗聴する場合は場所への物理的な侵入がないため，任意捜査として許されると示した。これは，プライバシー権が日本国憲法 35 条によ

---

739 林紀東・憲法釋義 7 版 145 頁。

740 同前注 145 頁。

741 同前注 138 頁。同見解として，張明貴・憲法 202 頁をも参照。

り保護される法益であることを否定するものであり，OLMSTEAD 判決と同様な立場に立ったものと考えられよう。

しかし，現在では，日本においても，その憲法 35 条の保護法益にはプライバシーも含まれるという点についての見解はほぼ一致している[742]。言い換えれば，修正４条の理解と同様に，日本国憲法 35 条においても，住居などの物理的な場所それ自体にとどまらず，かような場所に係るプライバシーも保護されているから，場所に対する侵入は，物理的な侵入のみならず，盗聴ないし写真撮影などの非物理的な手段にも及ぶ。この意味で，昭和 28 年決定はその先例としての価値を失ったといえよう[743]。Kerr の言葉を借りれば，日本も，「後 KATZ 時代」に入っていることになる。

もっとも，この日本の憲法 35 条の保護法益は，プライバシーであるといわれているものの[744]，プライバシーの概念をさらに具体化すれば，それは「『物理的な場所』における人の振る舞い」というものになるとされるから[745]，結局のところ，同 35 条が適用されるか否かの基準は，アメリカの修正４条のそれと同様に，「物理的な場所ないし物件」，すなわち，Kerr のいった「財産権に基づく視点」に求められることになっている[746]。つまり，修正４条は，人のプライバシーの権利を守るものであるから，それは，物理的な侵入のみならず，科学技術などの使用による無形の侵入をも対象とするものの，ＩＴシステムにおいては，「場所などの物理的な空間」の概念を観念することはできないから，プライベイトな領域を画定できないので，修正４条によってそれを保護することが困難であるというのが Kerr の理解であり，この意味での「場所などの物理的な空間とプライバシー保護との関係」という部分は，日本においてもドイツにおいても現状を支配する主流的な見解であるといえよう。まず，日本では，憲法 35 条は，「物理的な場所における人の振る舞い(プライバシー)」を保護するものであるとされているから，有形の侵入の場合にも無形の侵入の場合にも対応できるが，これらの場合は，いずれも，物理的な場所が存在することを前提とするものである[747]。また，ドイツの場合も，基本法 13 条の住居不可侵の法益にかかわる 08 年判決の示した理解は[748]，基本的には，上記の日本の理解と一致しているものと考えられる。

他方で，Kerr が，こうした財産権に基づく視点という理解を根拠に，さらに一歩進んで，オンラインでのＩＴシステムに関わる(プライバシーないし人格の)利益は，修正４条により保護される基本権ではないと主張しているのに対して，日本とドイツにおける主流的な立場は，こうした Kerr の主張とは異なる。まず，日本の場合は，第１章における改正法のリ

---

742 井上・傍受 14 頁，和田 131～132 頁，渥美・情報犯罪 80 頁，三井・手続法(1)[新版]36 頁など参照。

743 幕田・捜査法解説 112 頁，同・捜査法解説 3 版 138 頁。

744 井上・傍受 12 頁，鴨・刑訴基本理念 76 頁，田宮・注釈刑訴 122 頁，中野目 216～217 頁。

745 井上・傍受 14 頁。

746 同前注。また同井上論文 43，46～47 頁をも参照。

747 井上・傍受 14 頁。和田 131～132 頁，渥美・情報犯罪 80 頁も参照。

748 この点，ここで確認すると，08 年判決が，基本法 13 条をもってオンライン捜索の侵害に対応できないという理由は，オンラインでのＩＴシステムは，対象となる端末が置かれている場所との間に何ら物理的な繋がりを持たないため，それを物理的な場所の保護範囲に含めることはできない，という点に求められる。

モート・アクセスによる差押え関連規定の部分で検討したように，何らかの物理的な要素と繋がる場合であるかぎり，オンラインでのＩＴシステムも憲法 35 条による保護の範囲内にあるものとされる。つまり，刑訴法のレベルでは，物理的な要素との繋がりを介在するという間接的な保護の形になるのではあるが，憲法の次元では，基本的には，オンラインでのＩＴシステムに対しても，基本権としての憲法 35 条の保護を与えるべきであるものとするのが日本における支配的な立場といえよう。

次に，ドイツの状況を確認すると，08 年判決が，基本法 13 条の保護を主張するには，「場所などの物理的な空間」を前提としなければならないとする点では，Kerr の示した修正４条の理解と同様なものだといえるものの，そこから，オンラインでのＩＴシステムに関わる法益の基本権性を否定するものではないばかりでなく，従来の基本権よりも手厚い保護を提供するために，いわゆるＩＴ基本権を新しく創り出している。

以上により，オンラインでのＩＴシステムないしそこに蔵置された情報に関わるプライバシーないし人格の利益に関する要保護性につき，日本の理解は，Kerr の考え方よりも，むしろ，基本権肯定論に立つ 08 年判決の理解ないし Solove の立場に馴染むものであるといえよう。

以上に対して，中華民国憲法 10 条においては，単に，「人民は，住居及び移動をする自由を有する」と定められており，その主な保護の法益としては，日独米の三カ国と同様に，プライバシー権そのものをあげるのが通説である[749]。しかし，同条は，この三カ国と異なり，令状原則の要求を明示的に掲示するものではないのであるから，前述した台湾の学説のいう「正当な理由」及び「法律により定められた条件と手続」というのは，果たして，日独米のいった憲法上の要求としての「裁判官留保」や「令状原則」における「正当な理由」及び「適正な手続」に該当するものなのかについては疑問がある。

この点，まず，前にも言及したが，2001 年の台湾刑訴法改正以前には，検察官は裁判官が発付する令状なしで捜索・差押えを行うことが刑訴法上は認められていた。つまり，令状原則が採用されていなかったのである。確かに，2001 年以後には，台湾においても刑訴法上のレベルでは原則として捜索を行うには裁判官が発付する令状を必要とすることになった。とはいえ，令状原則は果たして中華民国憲法上の要求であるのかについては争われてきた。この点，学説上は，憲法の精神から推論すれば，令状原則は憲法上の要求であると主張する有力説に対して[750]，刑訴法上の令状原則の採用はあくまでも立法政策の選択に過ぎず，憲法上の要求ではないとする立場が多数説である[751]。他方で，現行法上は，いまでも，検察官に逮捕令状を発付する権限があたえられており，捜索によらずに差し押さえる場合[752]にも検察官が令状なしに差し押さえることが認められている[753]。

---

[749] 林紀東・憲法釋義 7 版 138 頁，陳・憲法釋論 4 版 212 頁，江・通訊監察 116 頁，張明貴・憲法 202 頁参照。
[750] 王・刑訴講義(一) 2 版 102～105 頁。
[751] 林鈺雄・搜索扣押 27 頁，搜索修法 139 頁(林山田発言)，柯・刑事程序 174 頁 181 頁。
[752] たとえば，差し押さえるべきものが明確であり，それを捜す必要もない場合があげられる。
[753] 林鈺雄・搜索扣押 221～224 頁参照。

以上のとおり，台湾の場合には,現行法の条文ないし多数説の見解は，むしろ，Kerr の見解に接近するものであるようにみえるが，本稿は，以下の２つの理由で，前述した日独の主流的な見解を台湾の憲法にも採り入れる可能性があると考える。すなわち，①本稿の理論によると，令状主義(または原則)の核心は，最小化原則に帰結すべきであるので，かかる原則は中華民国憲法 23 条の比例原則から導かれるものであるから，この意味での令状原則は，台湾でも憲法上の要求であるといえること,②捜査機関がこの憲法上の要求としての最小化原則を忠実に実現することを担保するためには，中立かつ超然な司法機関による審査・監督のメカニズムを構築する必要があること，という２つの理由である。

３．仮想的な空間における捜索範囲の限定

前述したように，場所ないし物件を観念できないＩＴシステムなどのバーチャル空間においては，従来捜索の範囲を画定するための基準とされてきた場所・サイズ基準が失効してしまうという点が問題となる。この点に関して，Kerr は，オンライン捜索の場合は修正４条の問題にはならないので，場所・サイズ基準は適用されないと解することによって，かかる基準の失効問題も解消されるとしつつ，オンラインでのＩＴシステムを保護しようとすれば，制定法によるべきものであるとしている。

これに対し，Solove は，Kerr 説を強く批判するとともに，従来の場所・サイズ基準が仮想的な空間における捜索範囲を限定するためには役立たないとい問題点にも言及しているが，それに代わる新たな基準を提案していない[754]。

他方，08 年判決が打ち出したいわゆるＩＴ基本権については，十分に検討する価値があると考えられる。というのも，従来の場所・サイズ基準の失効問題を検討するには，それらの基準に代えて，ＩＴシステムなどの仮想的な空間における捜索範囲を限定するためにあるべき基準を探求することが必要となるが，かかる新基準は，ＩＴ基本権における要保護性の一要素である「システムの不可侵性」に求められると考えるからである。

以上に対し，台湾の場合には，2001 年の法改正以前にも，膨大なコンピュータ・システムに対して捜索を行うことに執行上は困難があると指摘されてきたが[755],その問題の焦点は,バーチャル空間における捜索範囲の限定の在り方に置かれていたわけではなく，次の点にあるとされてきた。すなわち，ＩＴシステムは広すぎるため，捜査技術上，如何にそれをより効率的・有効的に探索し標的データを割り出すことができるかという点である[756]。

以上の通り，膨大なコンピュータ・システムを捜索の対象とする場合に困難とされる点には２つの側面がある。１つは，日独米が示唆した，かかる捜査に対する有効な制約の在

---

[754] Solove は，修正４条を科学技術におけるプライバシーの場面に適用するにあたり，合理性原則を第１原則とする判例・通説の立場(Amar， at8～9，43～45)を修正し，オンラインの場合には令状原則を第１原則とすべきであると主張している(Solove，INTERNET SURVERVEILLANCE LAW，at 1301～1304)が，しかし，彼は，具体的に，いかなる方法で令状原則をより貫徹することができるか，そして，物理的な要素を欠くＩＴシステムなどの場合においては捜索・差押えの対象ないし範囲を,いかなる要素ないし基準をもって,適切に画定することができるかについては回答を提供していない。

[755] 法務部・電脳犯罪４版 55～56 頁

[756] 同前注。

り方は何なのかという「捜査の制約」側面であり，もう１つは，台湾の関心事である，かような捜査の効率性をいかに向上させることができるかという「捜査の効率」側面である。

確かに，台湾では 2001 年法改正以後にも，ドイツの裁判官留保という意味での令状原則が憲法上の要求であるかどうかはなお検討する余地がある。しかし，この点は別にして，すくなくとも刑訴法のレベルで，文言上は，無体の電磁的記録をも捜索・差押えの対象としているとともに，捜索・差押えを行うのは原則的には裁判官が発付する令状によるべきものであると定められている。これによると，台湾の将来の立法論の在り方としては，「捜査の効率」側面から「捜査の制約」側面へと転向すべきであろう。この意味で，オンライン捜索を制約するために打ち出された，いわゆるＩＴ基本権における要保護性の一要素である「システムの不可侵性」を検討することは，台湾にも有益なものがあるといえよう。

４．中華民国憲法とＩＴ技術における人格権

前述したように，ドイツにおいては，アメリカでいうような広汎なプライバシー権は認められていないが，一般人格権が認められている。一般人格権の根拠は，基本法 1 条 1 項及び 2 条 1 項に求められる。これに対して，アメリカでは，プライバシー権が，「もっとも包括的な権利」[757]としての「一般的権利」 [758]と理解されてきたが，それは憲法上の特定の規定を根拠とするものではなく，様々な条項の解釈によって導かれた権利の総称である[759]。

本稿の検討対象である修正４条の保護法益としてのプライバシー権も，包括的な権利としてのプライバシー権の１つの類型に過ぎない[760]。この点，アメリカ連邦最高裁によれば，修正４条は，プライバシーに対する憲法上の権利の一般的な根拠にはならず，単に，ある類型の政府の侵入行為から個人のプライバシーを保護するものに過ぎないとされている[761]。また， Solve が述べる情報プライバシー権も，ここでいう包括的な権利としてのプライバシー権から派生したものである[762]。

他方で，ドイツにおけるプライバシー領域の保護は，アメリカの修正４条により保護される住居のプライバシー権と類似するものであると考えてよいし，それにドイツのいう情報自己決定権と，アメリカのいうプライバシー権から派生した情報プライバシーの一環として導出されてきた自己の情報に対するコントロール権とは，本質的に異なるものではないと考えられる[763]。

---

[757] Warren／Brandeis, at 1 ff, 伊藤・プライバシーの権利 33～35, 61, 70 頁, 久保田 145, 148 頁, 和田 131～132 頁, 橋本・憲法(改訂版)425 頁, 同・プライヴァシー32～35 頁等を参照。

[758] Warren／Brandeis, at 7, 15； 和田131～132頁；橋本・憲法(改訂版)425頁, 同・プライヴァシー32～35頁等を参照。

[759] Lide, at 481；and see Stone, at 4.

[760] 修正４条の外には，例えば，修正１条(See, eg, NAACP v. Alabama, 357 US 449, 1958)や修正９条(See, eg, Griswold v. Connecticut, 381 US 479, 1965)などからもプライバシー権の保護が導かれてきている。And see Stone, at 4；久保田 147 頁をも参照されたい。

[761] KATZ, supra note 554, at 350.

[762] Westin, at 7。佐藤・憲法(3 版)455 頁, 右崎 278～279 頁, 奈良 162 頁, 五十嵐・人格権 5, 81, 82, 93, 198～199 頁をも参照。

[763] Westin, 1ff, Und vgl. Schmidt, S.244。また，藤原・情報の自己決定権 145 頁及び松本和彦・基本権の保障(三)803

これに対して，ＩＴ基本権は，プライバシー権や情報自己決定権とは独立した，一般人格権から具体化した個別の基本権である。その一方で，ドイツの一般人格権とアメリカのプライバシーは同源のものであるとの指摘もなされている[764]。そうすると，08 年判決が打ち出したＩＴ基本権は，修正４条のプライバシー権と同じではないが，修正４条のプライバシー権よりも上位の概念である包括的な権利としてのプライバシー権からは，ＩＴ基本権の概念を抽出することは可能である。この意味で，ドイツでいうＩＴ基本権と，アメリカでいう新しいＩＴ技術におけるプライバシー(Kerr の用語)ないしＩＴ技術に関わる情報プライバシー(Solove の用語)などの概念は，いずれも，それを「ＩＴ技術における人格権」と呼ぶことができよう。

以上に従えば，立法論を見据えた法益論を検討するここでの問題の核心は，ＩＴ技術における人格権は，中華民国憲法により保護される基本権であるのか，それとも，基本権ではなく，制定法により保護するに値する利益にすぎないのかという点に帰着することができる。

この点，本稿は，ＩＴ技術における人格権を，台湾の憲法により保護される基本権であると考えている。ここで，ＩＴ基本権という用語を採用するかどうかはともかく，重要なのは，ドイツの 08 年判決が打ち出した，①個別のデータの属性に左右されないデータの秘密性，及び，②システムの不可侵性の２つの保護要件からなるＩＴ技術における人格権を，中華民国憲法により保護される基本権として承認すべきことである。その具体的な理由は，以下の通りである。

(1)新しい人権としての承認の根拠

A. 情報社会の実情

08 年判決が示している通り，現代社会においてはＩＴシステムの利用が人格の発展に非常に重大な意味をもち，ＩＴシステムを利用しないと日常生活を送ることができなくなるといっても過言ではない。こうした状況を鑑みると，家屋内に置かれた端末のオフラインでのＩＴシステムと，物理的な空間から離れたオンラインでのＩＴシステムとを区別し，前者は修正４条により保護することができるが，後者は保護することができないという Kerr の主張は，あまりにも不均衡であり，現代のＩＴ社会の実情には合わないから採用しがたいと思われる。

B. 司法による対応の必要性

Solove が指摘した通り，司法による対応と立法による対応は併用でき，かつその必要性

頁をも参照。

[764] アメリカ法でいう「プライバシー権」は，哲学上の発想としては，ドイツの「人格権」に由来するものであると言われている。すなわち，Whitman の考察によれば，アメリカにおいて，プライバシー権が最初に主張されたのは Warren／Brandies の論文「THE RIGHT TO PRIVACY」(4 Harv. L. Rev. 193, 1890)であるとされるが，Warren／Brandies が提案した人格権の発想(the idea of the personality right)は 19 世紀のドイツの法哲学に遡ることができるということである (Whitman, at1181； Solove/Rotenberg/Schwartz, at 22)。

もある。実際にも，台湾においては， 2001 年の刑訴法の改正により，形式的には，無体の電磁的記録も捜索・差押えの対象とされているが，第１章で指摘したように，従来の捜索・差押えの定義が変わっていないため，問題の解決に資すると評価できないだけでなく，かえって法の解釈・適用の難問ないし混乱を引き起こしてしまい，その一方で，データを保全する側面には全く対応していないし，また，無体のデータを検索・検閲・取得する範囲を適切に劃定できるための基準も用意されていないから，この部分は，司法による対応を期待するしかないのであろう。

さらに，電磁的記録以外の類型の情報に対しても，検索・検閲ないし保全・取得をする必要性がある例は数多くあげられる。例えば，通信会話，写真撮影，ビデオカメラ録画，エックス線検査などである。このうち，通信会話の類型は，2001 年の法改正よりも早く，1999 年に成立した，前にも登場した通保法という個別的な立法による解決がなされた。しかし，他の類型に関しては，法の空白の状態が続いている。かねてより，これは望ましいことでなく，立法により規制すべきであるとの指摘がなされているが[765]，関連する立法の動きは見られない。

その理由として，まず立法の怠慢という点が考えられる。この場合には，国民が主動的に訴訟を提起することによって司法による救済を受ける必要がある。この点に関しては，ドイツにおいても同様な指摘がなされてきた。すなわち，ＩＴ技術におけるプライバシーないし人格に関わる諸法益を「保護することに立法者は重大な怠慢があるので，連邦憲法裁判所[すなわち 08 年判決]は一般人格権を適切に具体化したＩＴ基本権の創出という形でかかる保護義務を引き受けなければならない」[766]とされている。

その他の理由としては，科学捜査はその種類，侵害の態様・程度が多岐に渡るうえに，形成途上にあり，各々の種類に応じた個別的立法では対応しきれないし，類型化も困難であるという点が挙げられる[767]。この点からは，立法が進まないのは，立法者の怠慢というよりも，むしろ，新しいＩＴ技術による捜査を規制するための類型化にかかる立法者の能力には限界があるからということになる。そして，こうした場合にも，同様に司法による対応が必要となる。

以上に示した法の空白による問題に対応するため，台湾においては，これまでは主に捜索・差押えに必要な処分や(強制的性格を帯びる)任意処分ないし検証の活用という解釈論的方策による対応がなされてきた[768]。しかし，必要な処分や任意処分ないし検証と解することが解釈論としては適切であるかどうかについてはなお疑問があるところである。とはいえ，必要な処分や任意処分という概念ないし検証という制度を活用するのが現状であることからは，台湾においても，法の空白を補填するような司法による対応が必要となってい

---

[765] 陳志龍・偵查與檢察 19 頁，林鈺雄・干預保留 220 頁，松尾・刑訴（上）新版 129～130 頁，島田・科学捜査 82 頁，三井・手続法(1)[新版]70 頁参照。

[766] Hirsch S. 9.

[767] 加藤 126 頁，劉 96 頁参照。

[768] 呉・照相錄影 150～151，163～171，173，176～177，179～182 頁参照。

ることが示されている。

このことは，高度で複雑な科学技術に関する場面では，構造上が劣勢である司法解釈による対応には限界があり，構造上の優勢をもつ立法により対応すべきであるという，前述したKerrの主張への反論ともなるであろう。というのも，高度で複雑な科学技術による捜査を規制するための類型化にかかる立法者の能力には限界があり，それよりはむしろ，個別事案に応じて臨機的対応ができる司法による解決がより現実的なものと考えられるならば[769]，司法は，かかる問題を解決するために，立法よりも優位するといえるからである。そして，こうした司法による対応が認められる法的な論拠は，憲法上の基本権の保障に求められることになる。

(2)新しい人権の承認の要件とその保護法益の構成要素

新しい人権を承認するための要件については，第１章においても論じたが，ここで確認すると，知る権利，環境権や情報自己決定権などの非固有権の性質を有するものに関しては，それらを基本権として認めようとすれば，①普遍性，②無条件性，③憲法上の根拠，④実定法的権利性，⑤基本性・重要性，⑥社会に対する中立性という６つの要件を満たさなければならない。

以上に従い，前述した08年判決の説明によれば，ＩＴ技術における人格権は，この６つの要件のうち，①②④⑤⑥の５つの要件を満たしていると言えよう。残る③の要件についても，後述するとおり，一般規定としての包括的権利保護条項である中華民国憲法22条から導かれる。

以上のとおり，ＩＴ技術における人格権は，中華民国憲法上の基本的人権性の承認要件を充足するといえよう。言い換えれば，ＩＴ基本権という保護法益の内実は，ＩＴ技術における人格権と呼ぶことができ，それを中華民国憲法上の基本権として保障すべきである。そのうえで，前述した08年判決の検討を踏まえて考えると，ここでいうＩＴ技術における人格権を，従来の基本権(住居不可侵，通信の秘密，プライバシー領域論や情報自己決定権等)には含まれない，①ＩＴシステムの不可侵性と，②不可侵性をもつＩＴシステムの全域におけるすべてのデータの要保護性(以下，「システムデータの要保護性」という)，という２つの新しい要保護性要素からなるものであるといえる。このうち，①は，ＩＴシステム自体の全域において不可侵という要保護性を有することを意味し，②は，プライバシーに関わるデータとそうでないデータとを区別することなく，それらのいずれに対しても同等な保護を与えると同時に，ユーザーが意識的に作ったデータのみならず，ユーザーの知らないうちにコンピュータの自律性により自動的に産出されたものもその保護範囲内に含まれるものとすることをさす[770]。

---

[769] 許宗力・法律保留202頁の説明をも参照されたい。

[770] この２つの要素は，08年判決が打ち出した「データの秘密性」及び「ＩＴシステムの不可侵性」から示唆を得たものであるが，それとは，次の２点で相違がある。第１に，本稿でいう「システムデータの要保護性」は，不可侵性をもつＩＴシステムの全領域におけるデータという限定を加えているから，08年判決の「データの秘密性」とは異なるニュア

そして，両者の関係については，①ＩＴシステムの不可侵性と②システムデータの要保護性は，択一関係でも並立関係でもなく，①が②の前提となっているという意味で，両者は主従関係にあり，①が主で，②が従となる。

第２款　新しい法益論の構築

以下では，ここまでの検討をもとに，情報を捜索という制度の直接の対象とする場面に対応するためにあるべき法益論を敷衍する。その前提として，まず，現行法上，捜索の場面に対応するための法益論においては如何なる保護間隙が存在しているのか，という点を確認しておく必要がある。具体的には，プライバシー権及び情報自己決定権という２つの既存する基本権によって，捜索の対象となる情報に関わる法益を保護することにはいかなる点で不十分であろうかを検討する。

Ｉ．法益保護の間隙

１．プライバシー権説における保護間隙

今日の通説的見解によれば，個人のプライバシー権は中華民国憲法 22 条を一般的な根拠として認められており[771]，また，住居不可侵を保障する同法 10 条の趣旨にはプライバシーの保護も含まれているとされる[772]。そして，台湾においては，任意処分と強制処分の判断基準は何なのかという点については，現行刑訴法により定められてはいないが，従来の理解としては，物理的な強制力の有無がその基準とされてきた[773]。これに対して，物理的な強制力という概念自体は曖昧であるし，また，科学技術の発展により，写真撮影，通信傍受，ポリグラフなどの科学捜査の方式が普及しつつあることに鑑み，これらの捜査活動は客観的には物理的な強制力を伴わないが，それによって実質的には国民の権益に対して与える侵害は捜索・差押えなどの伝統的な強制処分に負けないものがあるのに，多数説の見解によればかような捜査方式に対応することができなくなってしまうと批判したうえで，日本の学説を引用し，任意処分と強制処分の判断基準は有形力の行使や物理的な侵入の有無でなく，「実質あるいは重要な権利・利益への制約の有無」にあるとする見解が現れている[774]。

ンスが含まれている。第２に，用語について，プライバシー権ないし情報自己決定権の場面でいうデータの秘密性ないし情報の内密性と混同されないよう，「データの秘密性」という言葉を使っていない。

[771] 司法院大法官会議解釈 603 号，李惠宗・憲法五版 373～376 頁，許玉典・憲法 321～322 頁，許志雄(他)・憲法 252 頁。

[772] 林紀東・憲法釋義 7 版 137～138 頁，陳・憲法釋論 4 版 212 頁，江・通訊監察 116 頁。

[773] 陳樸生・刑訴(重訂十版)179 頁，黃東熊・刑訴法論239頁参照。

[774] 陳運財・正當程序 168～168 頁。同論文が引用した日本の文献は，井上・争点 54 頁(すなわち，重要権利侵害説。また最三決昭和 51 年 3 月 16 日刑集 30 巻 2 号 187 頁：井上・争点 48 頁＝井上・強制・任意 10 頁以下収録をも参照)及び三井・捜査･総説 85 頁(すなわち，実質権利侵害説)である。これに対して，三井教授の実質権利侵害説を支持する論者がある(呉・博論 120 頁＝呉・照相錄影 148 頁)。また，アメリカのいう合理的なプライバシーの期待の有無を基準とすべきとする見解として，李・電磁紀錄 1066～1067 頁，王・高科技搜索 90 頁参照。

以上のとおり，従来の理解に従えば，住居内のプライバシーに対する侵害は物理的な強制力を伴わない場合，中華民国憲法 10 条(住居不可侵)の保護を主張することができないという帰結になる[775]。かような結果は，現代社会の実情に鑑みると，妥当でないといわなければならない。そうだとすれば，日本でいう「重要(または実質)な権利・利益への制約の有無」という基準は，台湾にも導入するに値するものがあると考える。こうして，中華民国憲法 10 条も，日本国憲法 35 条と同様に，住居に対する侵入は物理的なものに限られず，非物理的な侵害にも対応することが可能であると解することができよう。

しかし，このように解することができたとしても，これにより，ここで指摘した中華民国憲法 10 条のいうプライバシー権における保護間隙の問題が，完全に解決されるわけではないのである。というのも，強制処分と任意処分との区別の基準については「物理的な強制力」という旧来の基準を廃棄し，「重要(または実質)な権利・利益への制約の有無」という新しい基準を採用するとしても，この新しい基準を中華民国憲法 10 条に当てはめて具体的に適用すると，結局のところ，やはり，同条のいう「住居」などの「物理的な場所」により支配されざるを得ないのではないかと思われるからである。

この点，日本の状況を概観すると，その通説によれば，プライバシー保護の必要が認められる場所や空間である限り，そこにおけるプライバシーを侵害するような処分には憲法 35 条の規制が及ぶと解されている[776]。それゆえ，プライベイト領域にあたる物理的な空間において起こる人の活動ないし関連事象である限り，それへの侵害が有形であるか無形であるかを問わず，プライバシー権による保護が認められる[777]。しかし，問題は，①ＩＴシステムの不可侵性，及び②システムデータの要保護性という２つの要保護性の要素においては，「プライベイト領域にあたる物理的な空間」を観念することはできないのである。

こうして，前述した日本の理解を中華民国憲法 10 条に採り入れることにより，物理的な場所に対する非物理的な侵害に対応しかねるという台湾の旧来の理解(捜索を，場所に対する物理的な侵入であると定義する多数説をさす)による問題点が解消されるが，しかし，プライベイト領域にあたる物理的な空間を権利保護の前提にする同 10 条のいうプライバシー権によっては，①ＩＴシステムの不可侵性，及び②システムデータの要保護性という２つの要保護性の要素からなる法益を保護することができないという保護間隙が存在するのである。

これに対して，日本国憲法 35 条でいう侵入は物理的なものに限られないとされているわけであるから，プライベイト領域にあたる物理的な空間という前提における「物理的な空間」という要素も緩和されうるという反論も考えられる。この反論は，かりに，中華民国憲法 10 条の場合にもそのまま適合するものだとすれば，前述した保護間隙を解消する可能

[775] 中華民国憲法 10 条のいう住居不可侵という法益の理解に関しては，無形の侵入もそれに含まれるかという点は争いがあるが，これを否定する一般論に対し，肯定する有力説としては，陳・憲法釋論 4 版 212 頁，江・通訊監察 116 頁があげられる。

[776] 井上・傍受 14 頁。

[777] 同前注。和田131～132頁，渥美・情報犯罪80頁も参照。

であるかもしれない。この点を検討するに，日本の憲法 35 条と同様に住居不可侵を定めたドイツの基本法 13 条についての議論が参考になろう。

すなわち，ドイツにおいては，オンライン捜索の場面への住居の不可侵性に関する基本権の適用可能性を否定した 08 年判決に対して，次のような指摘がなされている。基本法 13 条の保護法益は，従来の判例の理解によると，「そこで私生活を送る場所的空間」であるが，その具体的な内容は必ずしも明白ではなく，それが「場所に関する保護」なのか，それとも，「(人の)振る舞いに関する保護」なのかが争われてきた[778]。仮に，後者の立場からすると，基本法 13 条により保護されるのは，「場所」自体ではなく，そこでの「人間の振る舞い」であると解されると同時に，「物理的な空間」（場所)という要素が必要でなくなり，ITシステムなどの「バーチャル空間における人の振る舞い」も保護されることになる[779]。

他方で，前述したように，日本の憲法 35 条は，アメリカの修正４条に由来するものであるとされてきた。そしてまた，修正４条により保護されるのは，「場所ではなく，人である」と，KATZ 判決は明言している。そうすると，同 35 条の解釈としては，後者の「振る舞いに関する保護」の立場をとるべきであると解されることになろう。そうだとすれば， 物理的な空間に限らず， ＩＴシステムなどのバーチャル空間における人の振る舞いもこの 35 条により保護されるという帰結が導かれる。

確かに，中華民国憲法 10 条における住居不可侵という法益の内実を解釈する際にも，前述した日独米の理解のように，住居不可侵の保護範囲をバーチャル空間にまで拡大することが可能であろう。しかし残念ながら，このような解釈が認められたとしても，かような拡大だけでは，問題の解決には意味が薄いと言わざるを得ないのである。

まず，前述したように，KATZ 判決の Harlan 裁判官の補足意見で，修正４条の適用についてはやはりその「場所」に着目することが必要であると述べられているし，また，KATZ 判決以後の一連の判例の展開をみてみると，修正４条の適用は，依然として「場所」と深く繋がっていることは明らかである。

日本国憲法 35 条の母法とされる修正４条の解釈がこのように推移したとすれば，日本の場合も同様な状況になることが予想される。すなわち，この 35 条の保護範囲をバーチャル空間にまで拡大したとしても，同 35 条によるプライバシーの保護の適格性の有無を判断する基準を，依然として「場所」などの物理的な要素に求める限り，やはり，08 年判決が指摘している保護間隙が生じることになろう。というのも， ＩＴシステムにおいては，場所という概念を観念することができず， プライベイト領域(保護される領域)とそうでない領域(保護されない領域)との区別も不可能だからである。

これに対し，Solove は，修正４条を適用する基準として，そもそも「場所」に着目する

---

[778] Lepsius, S. 24.

[779] Lepsius, S. 25 は「基本法 13 条につき，振る舞いに関する保護に照準を合わせれば，……，住居から離れている情報科学技術システムの利益も，基本法 13 条の保護領域にあるように思われる」とし，a. a. O. S. 26 は「振る舞いに関する保護という立場を……とれば，基本法 13 条の適用範囲を減縮することによって，コンピュータ基本権[すなわち本稿のいう IT 基本権]を新しく作り出した 08 年判決はその論拠を失ってしまう」とする。

必要がないとしている。しかし，Solove は，単に，場所や物理的な要素に依存しないオンラインの場合には，いかなる要素を修正４条の適用基準とするのかは難問であると指摘するにとどまり，具体的な基準が何であるのかについては明らかにしていないのである。

加えて，Solove の考えも，基本的には，保護される(プライバシーに関わる)領域と保護されない(プライバシーに関わらない)領域との区別を前提とするものである。そうすると，かような区別をすることはＩＴシステムにおいては不可能であるから，結局のところ，Solove の主張したデータないしＩＴシステムに対する修正４条による保護が,具体的にいかなる形で実践されうるのかは不明なままである。

このように，ここでの根本的な問題は，空間(場所)に関した保護であれ，振る舞い(人のプライバシー)に関した保護であれ，それらはいずれも，プライバシーの保護を核心としている点にある。というのも，前述した通り，ＩＴシステムの媒体を直接の処分の対象とするオフライン侵入の場合は別にして，ＩＴシステムないしそのなかに流通や蔵置している情報を直接の処分の対象とするオンライン侵入の場合には，デジタル通信におけるパッケト交換技術の仕組みゆえに，ＩＴシステムにおいてプライベイト領域とそうでない領域とを区別するのは原理的に不可能であるし，またデータの属性(プライバシーにかかるものであるかどうか)はそれぞれの文脈に左右されているため常に変動しており，かつ特定の文脈を離れたデータ自体の属性を判断することは何ら意味を持たないからである。

以上により，次の２点が明らかになった。

第１に，中華民国憲法 10 条のいう住居不可侵におけるプライバシー権の保護は，台湾の従来の理解によれば，物理的な侵入に限られるものであるから，当然には，①ＩＴシステムの不可侵性，及び②システムデータの要保護性という２つの要保護性の要素からなる法益には十分な保護を提供できないという帰結になる。

第２に，仮に，前述した，日本国憲法 35 条，ドイツ基本法 13 条及びアメリカ憲法修正４条のプライバシーに関する通説的理解を台湾にも採り入れることが可能だとすれば，これにより解決されうる問題は，せいぜい，住居などの場所に対する非物理的な侵害にも対抗することが可能になるというものにすぎない。言い換えれば，本稿の指摘した核心的な問題――つまり，前述した①と②の２つの要保護性の要素からなる法益には十分な保護を提供できないという保護間隙――は依然として未解決のままである。というのも，プライバシーの保護を主張するには，プライバシーに属するデータ及びスペースと，そうでないデータ及びスペースとの区別が必要不可欠な前提となっているが，ＩＴシステムにおいては,かような区別は理論的・技術的に不可能だからである。

２．情報自己決定権説における保護間隙

次に検討すべきは，情報自己決定権によっては，①ＩＴシステムの不可侵性，及び②システムデータの要保護性という２つの要保護性の要素からなる法益に対し，十分な保護を提供することができるかという問題点である。

まず，前述した 08 年判決の見解をここで確認すると，同判決は，情報自己決定権の適用は，(1)私的なデータと非私的なデータの区別，(2)広汎なデータ徴収・処理，(3)個別のデータに対する徴収，という３つの要件を必要とするものとしたうえで，ＩＴシステムに対してオンライン捜索を行う場合は，私的なデータと非私的なデータとを区別できず，広汎なデータ徴収・処理を行うことなく巨大なデータベースを結成・利用することができるし，また，個別のデータに対する徴収という形でなく，全システムの全領域におけるすべてのデータへの全面的な侵入という形になるから，かかる３つの要件を満たしておらず，情報自己決定権によっては，オンライン捜索によりもたらされる人格への新たな危険の発生ないしその実害化のリスクに十分に対応できていないとしている[780]。

以上に対して，台湾においては，ドイツの 08 年判決のいう「Recht auf informationelle Selbstbestimmung；Informationelles Selbstbestimmungsrecht」という用語は，一般的に中国語である「資訊自決権」と訳されてきた[781]。同用語は，日本語では「情報自己決定権」とされる。そこで，以下では，台湾のいう資訊自決権を，情報自己決定権とする。しかし，台湾の情報自己決定権と 08 年判決のそれとの間には次のような相違点がある。すなわち，台湾の場合には，「広汎なデータ徴収・処理」「個別のデータに対する徴収」という２つの点を必要要件としないのである[782]。よって，以下の検討は，「私的なデータと非私的なデータの区別」という点に絞ることとする。

(1)プライバシーの固有部分と外延部分

台湾においては，情報自己決定権の具体的な中身につき，権威ある大法官解釈 603 号によって次のような理解・定義がなされている。すなわち，情報自己決定権とは，既存するプライバシー権から独立した別の権利ではなく，情報社会の登場を背景にした，プライバシー権から派生する新しい類型のプライバシー，すなわち，いわゆる情報プライバシー(原語は中国語である「資訊隱私權」となる)にかかわる権利であって，「個人情報に対して自主的にコントロールする権利」と理解され，具体的には，「国民がその個人情報を開示するかどうか，そして如何なる範囲で，いつ，どのような方式により，誰に対して開示するかを決定する権利であると同時に，国民がその個人情報の使用の詳細を知る，かつコントロールする権利を有しながら，情報の記載の錯誤を更正する権利でもある」と定義されている。

以上のとおり，情報自己決定権により保護されるのは，プライバシーに関わる個人情報である。

---

[780] 前掲注 648 参照。

[781] 李震山・資訊隱私權 54 頁，同・監視錄影 47 頁，陳正根・警察資訊 219 頁参照。また，李震山・監視錄影 58～59 頁は，「資訊自決權」(情報自己決定権)はドイツの用語であるのに対して，「資訊隱私權」(情報プライバシー)はアメリカの用語であると述べる。この「資訊自決権」という用語は，「自我資訊控制權」(たとえば，范姜・隱私權 10 頁。すなみに，「自我資訊控制權」は日本でいう「自己情報コントロール権」の訳語であるとされる)，「資訊自己(自我)決定権」(たとえば，林鈺雄・刑事程序 237 頁，同・干預保留 192 頁)，「資訊自主権」(たとえば，王郁琦・隱私權 107 頁)，「資訊自主権決定(權)」(たとえば，蔡聖偉・妨害秘密(上)154 頁)とも呼ばれている。なお，日本の文献を引用し，日本語である「情報自己決定権」という漢字を中国語としてそのまま使うものがある(陳通和・情報自己決定權 277 頁)。

[782] 前掲注にあげられた文献のほかに，許文義・個人資料保護 51 頁，陳通和・情報自己決定権 279 頁をも参照。

次に検討すべきは,如何なる基準をもって,ある個人情報を,情報自己決定権の保護対象となるプライバシーに関わる情報であるといえるのかという問題である。この点,大法官解釈は，そのための基準を提供していないが,以下では，日本と台湾における関連する先行研究の理解を検討していきたい。

まず,日本でいう情報自己決定権(情報コントロール権とも呼ばれる)は，アメリカの学説の影響を受けたものとされており[783],その理論の詳細については論者によってニュアンスの差異があるが,その概念の核心的部分は,ドイツでいう情報自己決定権と異なるものではないと思われる。日本の理解によると，情報自己決定権とは，プライバシー権から独立した別の権利ではなく，データバンク社会のニーズに応じてなされたプライバシー権の新しい定義として理解されてきた[784]。これにより，日本の理解と，前述した台湾の大法官解釈 603 号の理解とは同様のものであると考えられる。

また,情報自己決定権の保護対象となるプライバシーに関わる情報とそうでない情報とを区別するための基準につき，日本の情報自己決定権説の代表者とされる佐藤教授は,「その人の道徳的自律の存在に関わる情報」を「プライヴァシー固有情報」(以下,「固有情報」という)と,「個人の道徳的自律の存在に直接かかわらない外的事項に関する個別的情報」を「プライヴァシー外延情報」(以下,「外延情報」という)と称しており，両者を区別したうえで，外延情報に対しては,「正当な政府目的のために，正当な方法を通じて取得･保有･利用しても，直ちにはプライヴァシーの権利の侵害とはいえない」と述べている[785]。

実際にも，台湾の先行研究においては，佐藤教授の提案である「固有情報／外延情報」という基準をそのまま引用する論者が現れている[786]。他方で，同基準と接近する分類を採用する見解があるが[787]，しかし，かかる分類の具体的な使い方は，佐藤教授のそれとは異なるものである。すなわち，この台湾の見解によると,「固有情報／外延情報」(原語は,「敏感資訊／非敏感資訊」となる)という分類は，情報自己決定権の保護範囲を画するための基準として使われるわけでなく,それは,情報自己決定権とプライバシー権との区別の限界を示すための基準とされている[788]。つまり，プライバシー権は,固有情報のみを保護するものであるとされるのに対して,情報自己

---

783 プライバシー権を初めて定義づけた判例としてよく知られている『宴のあと』(東京地判昭和 39 年 9 月 28 日下民集 15 巻 9 号 2317 頁)が示した「いわゆるプライバシー権は私生活をみだりに公開されないという法的保障ないし権利」という定義は，当時は広く学界の支持を得，通説的見解に副うものであったとされるが(五十嵐・人格権 198 頁参照),「その後のコンピュータ社会の出現により，この定義では現在におけるプライバシーの保護のために十分ではないとされ，わが国でもアメリカの学説の影響を受けて，プライバシー権を『自己の情報をコントロールする権利』[情報コントロール権]などと定義する学者が増えている」(五十嵐･人格権 198 頁)。日本におけるコントロール権説の代表的な論者として，佐藤幸治（同・プライヴァシー・公法的側面（1)1 頁以下／(2)1 頁以下，同・権利としてのプライバシー158 頁以下参照）があげられる。

784 佐藤・権利としてのプライバシー162 頁以下。また，阪本・プライヴァシー権論 2～3，8～12，221 頁以下；松井・情報コントロール権 38 頁；棟居・人権論 185 頁以下，同・プライヴァシー新構成 2 頁，同・人権論 173 頁；新保史生・プライバシー129 頁なども参照。

785 佐藤・憲法(3 版)454～455 頁。

786 吳・照相錄影 74 頁(同文は「固有情報／外延情報」を「固有資訊／外延資訊」と訳する)。

787 王郁琦・生物辨識 71～72 頁，陳正根・警察資訊 220 頁。また，台湾の個人資料保護法においても「固有情報／外延情報(「敏感資訊／非敏感資訊」」という分類を採用されている(同法 6 条参照)。

788 前掲注参照。

決定権は,固有情報にかぎらず,外延情報もその保護範囲内に含まれる可能性があるというのが,台湾における一部の学説の理解であるのに対して，佐藤教授によると，情報自己決定権は，原則的には，固有情報を保護するものであるのである。

しかし，前述した台湾の先行研究は，あらゆる外延情報を情報自己決定権の保護対象としようとする立場であるのか，それとも，一部の外延情報も情報自己決定権の保護対象となりうるとする立場であるのかは，必ずしも明瞭でない。前者の立場に立つと，情報自己決定権の保護範囲は広すぎるではないかという批判を免れない一方で，後者の立場をとると，保護対象となる外延情報とそうでない外延情報とを区別するための基準は何なのかという点が問題となる。

これに対し，佐藤教授の提案では，この２つの点とも問題にならないのである。まず，佐藤教授によると，情報自己決定権の保護範囲が原則的には固有情報に絞られているから，保護範囲は広すぎるという問題が生じない。その一方で，教授は，「外的情報［外延情報を指す］も悪用されまたは集積されるとき，個人の道徳的自律の存在に影響を及ぼすものとして，プライヴァシーの権利の侵害の問題が生ずる」[789]とも述べている。また，松井教授は，「収集目的を達成した場合の個人情報の破棄･削除，収集目的以外の利用の禁止に加え，より一層のアクセスの制限やデータ保護が図られることが必要[である]」[790]と主張している。つまり，教授は，場合によって一部の外延情報も情報自己決定権の保護対象となりうるとする立場であるが，こうした場合に保護の対象にあたるかどうかを判断するための基準は,外延情報の悪用ないし集積により個人の道徳的自律の存在に影響を及ぼす可能性があるかどうかという点に求められる。

この佐藤教授の見解は台湾にも参考となるものがあると思われるものの，その前提として，やはり固有情報と外延情報とを区別しておかなければならないから,問題の解決には役立ちかねるものであるといわなければならない。言い換えれば，台湾の先行研究の理解であれ，佐藤教授の提案であれ，それらのいずれにいても，ＩＴシステムの場面に当てはめると機能しないことになると思われる。というのも，前述した通り，デジタル通信におけるパケト交換技術の仕組みゆえに，ＩＴシステムにおいてはプライベイト領域とそうでない領域とを区別することも，特定の文脈を離れてデータの属性の判断を行うことも，原理的には不可能とされるから，プライバシーにかかるデータであるかとの判断を前提に，さらにそれを「固有情報／外延情報」に区別するのは一層無理であると言わなければならないからである。

もとより，ドイツの国勢調査判決が指摘している通り，自動データ処理を前提とすれば，もはや「重要でない」データは存在しないのであるから[791]，自動データ処理を前提とするＩＴシステムの場面でいうかぎりは，固有情報(重要情報)と外延情報(重要でない情報)を区別するのは，正鵠を射ていないと言わざるを得ないであろう。

以上のとおり，ＩＴシステムにおいては，私的データないしスペースとそうでないデータない

---

789 佐藤・憲法(3 版)455 頁。

790 松井 513 頁。

791 BVerfGE 65, 1(45)；また，松本和彦・基本権の保障(二)354～355 頁，永田＝松本＝倉田(訳)127 頁をも参照。

しスペースとの区別,あるいは重要データと重要でないデータとの区別が不可能(または無意味)であるから，情報自己決定権の保護を主張するには,かような区別を必要とするかぎり，前述したプライバシー権と同様に，①ＩＴシステムの不可侵性，及び②システムデータの要保護性という２つの要保護性の要素からなる法益に十分な保護を提供できず,そこに保護間隙が存在することになる。

ところで，台湾の先行研究においては，プライバシーにかかわらないデータも情報自己決定権により保護されるものであると主張する論者がある[792]。これによると，当然には，固有情報も外延情報も保護されるという結論が導かれる。しかしながら，仮に，情報自己決定権論のもとで,私的データや非私的データであれ固有情報や外延情報であれ，それらは，いずれも，一律に保護されるという立場がとられたとしても，以下に述べる理由で，情報自己決定権論のもとで前述した①と②という２つの要保護性の要素からなる法益に十分な保護を提供できないという保護間隙が存在するという結論は，やはり変わらないと思われる。

(2)システムへの不当な侵入

台湾においては，ＩＴシステムに対するオンライン捜索に関する問題について議論が非常に乏しい[793]。したがってまた，台湾におけるプライバシー権論であれ，情報自己決定権説であれ，それらはいずれも，オンライン捜索の問題を念頭に置いていない。

他方で，情報自己決定権説は，コンピュータ社会の出現により唱えられてきたものである[794]。この点からすると，かかる理論の生成とオンライン捜索の文脈のもとでなされたＩＴ基本権の創出とは，異なる背景をもつものではないと思われる。とはいえ，情報自己決定権とＩＴ基本権におけるそれぞれの法益構成の具体的な内容及び問題となった点は全く異なるものである。両者の差異を説明すると，次のようなものになる。

まず，情報自己決定権説の主な狙い――また，その最大の意義――は，データバンク化した行政に対抗する武器を国民に供給しえたという点に求められている一方で[795],自己情報のコントロールの生命部分ともいうべき閲覧・訂正権を市民が行使する際に，いかにして自己情報の存在を知るかにつき周到な用意がされていないとの指摘がなされている[796]。この指摘で示された通り，情報自己決定権の法益構成の具体的な内容としては，知る権利及び自己に関する情報の流通をコントロールする利益という２つのものがあげられる[797]。そして,

---

792 李震山・個人資料保護 228 頁。

793 公刊されているものとして，何賴傑・線上捜索與電子郵件 230 頁以下しか見つからない。これは，08 年判決を簡単に紹介したうえそれに関連する判決及び学説をも一部で若干に言及するものにすぎないし,そのポイントは,電子メールに対する検閲・保全の行為の法的性質は一体通信傍受法に属するものであろうか,それとも,刑事訴訟法の捜索・差押えに該当するものであろうかという点に置かれ，本稿の検討対象とは異なるものである。

794 陳通和・情報自己決定権 278 頁。

795 棟居・人権論 193 頁； 陳通和・情報自己決定権 278 頁脚注 9，李鴻禧・資訊隱私權 481 頁。

796 阪本・プライヴァシー権論 175 頁；司法院大法官会議解釈 603 号；陳通和・情報自己決定権 288～291 頁，李鴻禧・資訊隱私權 490～491 頁参照。

797 司法院大法官会議解釈 603 号。佐藤・権利としてのプライバシー162 頁をも参照されたい。

それが問題となる場面としては，政府による情報の不当な収集(例えば目的外の収集)・開示(例えば，目的外流用や過大開示)，開示された情報に誤りがあるときなどが考えられる。

他方で，確かに，日本において憲法学分野では，1970 年以降，犯罪捜査の目的でなされた盗聴や写真撮影などの事例も，情報プライバシー権(すなわち，情報コントロール権または情報自己決定権)侵害の問題として理解され，日本国憲法 13 条にその規制の根拠を求めることができるとする見解が現われてきた[798]。また，刑訴法の分野においてもかかる見解を受け入れたように見える判例がある[799]。もし，この日本の理解が台湾の場合にも適合するものであるとすれば,いわゆる情報自己決定権説は，データバンク化した行政に対抗する武器という最初の性格から，国家の捜査活動に対抗する武器を被疑者ないし一般市民に与えるものへと変質されよう。そして，こうした場面においては，知る権利という法益とは直接の関係はなく，また，ここで主たる問題とされるのも，もはや閲覧や訂正などの権利の救済という側面でなくなり，情報の収集(例えば，写真撮影や録音などの捜査行為)の合法性に集中するということになる。

これに対して，ＩＴシステムの不可侵性及びシステムデータの要保護性という２つの要保護性の要素からなる法益の場合においては，問題の核心は，知る権利ないし情報の開示及び訂正などの点にあるわけではないのはもちろんのこと，情報の収集という点でもない。そこでもっとも重要とされるのは，「システムへの不当の侵入」という点でこそある。逆にいえば，システムへの不当な侵入という点に特徴付けられている，ＩＴシステムの不可侵性及びシステムデータの要保護性という２つの要保護性の要素からなる法益は，従来理解されてきた，知る権利及び自己に関する情報の流通をコントロールする利益からなる情報コントロール権に含まれないのである。

以上の通り，ＩＴシステムにおいては「私的データとそうでないデータ」ないし「固有情報と外延情報」などの区別の不可能性に加え，システムへの不当の侵入を防ぐという要保護性の独自性からも，情報自己決定権説は，ＩＴシステムの不可侵性及びシステムデータの要保護性という２つの要素からなる法益に十分な保護を提供することができないという帰結になる。

３．新しい基本権の導出とその必要性

続いて，以上のようなプライバシー権論及び情報自己決定権説における保護間隙に対し，いかなる解決策が考えられるかについて，ここまでの考察をも踏まえて検討を加える。

前述した保護間隙への対応策としては，08 年判決が示した，憲法の一般条項から新しい基本権を導き出すという「保護間隙補填モデル」が参考になると思われる。

具体的には，中華民国憲法 22 条から，①ＩＴシステムの不可侵性，及び②システムデー

[798] 佐藤・憲法(3 版)453～455 頁。右崎 278～279 頁も参照。

[799] 最判昭和 44 年 12 月 24 日刑集 23 巻 12 号 1625 頁。

タの要保護性という２つの要保護性の要素を取り入れた新しい基本権――本稿は，これを「情報システム基本権」と呼ぶ――を導き出すことができると考えられる。というのも，前にも言及したが，現在の通説によれば，同 22 条は間隙埋め機能をもつ包括的な基本権であるとされるので，この意味で，同条は，実質的には，ドイツの基本法の一般人格権条項と類似した機能をもつものといえるからである。

以上の主張に対しては，同 22 条から「情報システム基本権」を新しく創り出すまでの必要はなく，従来のプライバシー権ないし情報自己決定権（あるいは情報プライバシー権）などの既存する基本権の保護範囲を拡大するという形で，ＩＴシステムの不可侵性及びシステムデータの要保護性という２つの要保護性の要素を，既存の基本権に取り入れることにより保護するという対策も考えられるという反論もありえよう。そこで，次に検討すべきは，08 年判決が示唆したように一般条項（台湾では，憲法 22 条となる）から新しい人権を導き出すという選択肢を採用すべきか，それとも，既存の具体化した個別の基本権（例えば，憲法 22 条から導かれたプライバシー権ないし情報自己決定権）の内実を拡大するという方法を採用すべきかである。

この点を検討する前提として，まずは，ＩＴシステムの不可侵性及びシステムデータの要保護性という２つの（基本権法益の）構成要素を実質的に保護するためには，既存の基本権――プライバシー権と情報自己決定権――をどのように拡大すべきなのかを具体的に考えておくことにしよう。

(1)プライバシー権との関係

最初に，住居の不可侵性を保護する中華民国憲法 10 条のいうプライバシー権から考えると，かかる問題に対応するためにありうる拡大としては，その対象を物理的な空間に限らず，ＩＴシステムなどのバーチャルの空間にも及ぼすことが考えられる[800]。

しかし，前述した通り，このような拡大解釈を認めたとしても，意味は薄い。というのも，物理的な空間という制限を無くしたとしても，プライバシー権の性質ゆえに，プライバシーに関するデータないしスペースしか保護されないことになるところ，パケット交換技術を利用するＩＴシステムにおいては，プライバシーに関係するデータやスペースとそうでないものとの区別が原理的には不可能である以上，プライバシー権による保護が働かないという点は変わらないと思われるからである。

それから，憲法 22 条のプライバシー権であるならば，そもそも，物理的な空間という制限がないため，かような拡大は不要となる。だが，パケット交換技術を利用するＩＴシステムにおいてはプライバシーに関係するデータやスペースとそうでないものとの区別が原理的には不可能であるという問題は，同様にあてはまるのである。

これに対しては，同 10 条であれ同 22 条であれ，それらの保護範囲を，プライバシーに

[800] 憲法の解釈を時代や客観的諸情勢に応じて変更する立場（吳庚・變遷憲法 5, 7 頁；田宮・強制捜査 308 頁，平野・刑訴全集 113 頁をも参照）からすると，中華民国憲法 10 条における物質性の制限を緩和することができよう。

関係しない部分にまで拡張すれば，かかる難点は解決されうる。しかし，このような解釈によると，「プライバシーではないものをも保護する権利」を，プライバシー権と称することができるのか，それは，プライバシー権とはいえないのではないかという疑問があり，こうした解釈には無理があるといわざるを得ないであろう。

(2)情報自己決定権との関係

次に，情報自己決定権を拡大すると，いかなる形になるのかを検討しよう。この点，前述した通り，台湾では，情報自己決定権は，プライバシー権から派生する新型のプライバシーにかかわる権利とされているから，かかる権利も，プライバシー権と同様に，プライバシーに関するデータやスペースとそうでないものとを区別することが，その適用の前提になることになろう。そうすると，情報自己決定権も，前述したプライバシー権のところと同様な問題を抱えているということができる。

もっとも，情報自己決定権の場合は，プライバシー権と異なり，理論的には，プライバシーでない部分の情報も保護すべきと解釈する余地があるようにも思われるところである。実際にも，先行研究において一般論としては，情報自己決定権(台湾のいう資訊自決權)を，情報プライバシー権(台湾のいう資訊隱私權)から派生する権利であると解するのが主流であるものの[801]，この２つの概念を区別し，前者を適用するには，プライバシー(ないし情報プライバシー)にかかわる情報に限らないとする論者がある[802]。後者の見解を取った場合，情報自己決定権はプライバシー権ではなくなってしまうという問題があるが，この点に関しては，そもそも，情報自己決定権を，プライバシー権から独立した基本権と理解することができるとすれば，この問題は理論的には解消される。

しかし，そうすると，なぜ，個人が，情報に対してコントロール権を有すると主張できるのかという点が問題となる。この点，プライバシー権から導かれた情報自己決定権においては，個人がある情報に対してコントロール権を主張できることの根拠は，当該情報については個人がプライバシー権を享有する点に求められてきた[803]。これに対して，情報自己決定権を，プライバシー権と関係のない基本権と解した場合においては，いかなる情報に対して，そして，いかなるコントロールの内容を主張することができるかについての理論

---

[801] 司法院大法官会議解釈603号，李鴻禧・資訊隱私權485頁，許文義・個人資料保護51頁，吳・博論59頁＝吳・照相錄影71～72頁，王郁琦・隱私權107頁，林雅惠資訊隱私權102～103頁，劉靜怡・資訊隱私權20頁，陳正根・警察資訊220頁，范姜・隱私權10頁，張國清・隱私保護5～6頁，黃慧娟・個人資料保護117頁。これらの論者は，いずれも，「資訊自主權」(情報自己決定権)の保護を主張するにはプライバシーにかかわる情報とそうでない情報との区別を前提とする立場に立っている。同じ立場を取っておりながら，「資訊自主權」という概念と「資訊隱私權」(情報プライバシー)という概念とを同義語として取り扱う論者がある(王俊文・隱私權201頁，陳河泉・隱私權21～22頁)。また，人格権から情報自己決定権を導き出す論者がある(程明修・資訊自決權2頁)。なお，プライバシー権を人格権の延長の一部とみなす見解がある(林世宗・隱私權33～34頁)。

[802] 李震山・個人資料保護 228 頁，同・資訊自決權 246～247 頁参照。同見解として，黃清德・科技蒐集個資 273～275 頁，黃＝陳・監視錄影 89 頁，李惠宗・資訊自決權 24～25 頁参照。

[803] 前掲注 801 にあげた文献のほか，潘兆娟・隱私保護 95 頁，陳通和・情報自己決定権 278～279 頁，松井・情報コントロール権 38 頁及び同・インターネット人権 12 頁，和田ほか・情報 81，111 頁をも参照。

的な根拠を改めて探求しなければならない。この問題点を解決しない限り，プライバシーでない部分の情報も情報自己決定権の保護範囲にあるという解釈をとることには，理論上の難点がある。

さらに，ＩＴシステムの不可侵性という要素が，果たして，個人の自主性を最も核心的な要素とした情報自己決定権の性格[804]にふさわしいものであるかについても疑問があるように思われる。というのも，08 年判決が打ち出したＩＴ基本権は，「個別の(個人)データから離れたシステム保護を目的とするもの」[805]であるので，個人の自主性とは関係ないからである。この点，Lepsius は，データに関する基本権的保護につき，既存する通信の秘密，住居不可侵及び情報自己決定権などの基本権の保護範囲を狭く画定したうえでＩＴ基本権を作り出した 08 年判決が「不必要な限界画定問題」[すなわち，08 年判決がいう保護間隙の問題]に陥ってしまったと批判しつつも，かかる問題は，「情報技術システムの機能性の追加された非人格的な保護の視点」をとる場合にのみ生じうると述べる[806]。言い換えれば，非人格的な保護要素であるＩＴシステムの不可侵性は，人格の主体が個人のデータを自主的にコントロールする権利を意味する――すなわち，人格の主体，個人のデータ，自主性，及びコントロールなどの人格的な保護要素からなる――情報自己決定権とは直接に関係しないものである。とすると，ＩＴシステムの不可侵性という要保護性要素を，情報自己決定権の保護範囲に詰め込むのは，やはり無理があるのではないかと思われる。この点，Lepsius 自身も，この新しい基本権[本稿のいうＩＴ基本権をさす]を「新」といえるには，その力点はこの客観的な保護次元の保障[すなわち，「個別の(個人) データから離れたシステム保護」を指す]にあるとし，それにより，ＩＴ基本権と情報自己決定権との差異が説明されるとしている[807]。

(3)私見

以上の通り，従来のプライバシー権ないし情報自己決定権を拡大することは，抽象的にはありうるが，かような拡大は，実際的な意味をもたないと同時に，解釈論上の首尾一貫性を欠くという問題を生じさせるのである。

これに対して，中華民国憲法 22 条から情報システム基本権という新しい人権を導き出すという選択肢をとると，住居不可侵を保護する同法 10 条における物理的な空間による(保護範囲の)制限が存在しないだけでなく，プライバシーに関わるデータやスペースとそうでないものとを区別する必要もなくなる。加えて，情報システム基本権の法益(要保護性)の核心はシステムの不可侵性にあり，個人情報に対する個別のユーザーのコントロール権の有無とは直接の関係はないので，既存のプライバシー権や情報コントロール権の理論にな

[804] 台湾の先行研究においては，情報自己決定権の具体的な内実(保護範囲)については争いがあり見解が分けられているが，これらの見解は，いずれも，個人の自主性という要素を，自己情報決定権の中身をなす最も核心の部分としているのは間違いない。

[805] Lepsius, S. 32.

[806] a. a. O.

[807] Lepsius, S. 41.

じまない。それゆえ，これらの既存の基本権の理論を根拠とするよりは，むしろ中華民国憲法 22 条から新しい権利を導き出した方こそ適切だと考える。

Ⅱ．情報システム基本権について

以上の通り，中華民国憲法 22 条から，①情報システムの不可侵性と②情報システムデータの要保護性という２つの要素からなる「情報システム基本権」が導き出される。以下では，既存の問題点の解決にあたって，情報システム基本権と，ドイツの 08 年判決が示したＩＴ基本権がどのような差異をもたらすかを説明することにより，情報システム基本権の内容をより一層具体化してみたい。

１．物質空間における場所・サイズ基準の失効

前述した通り，バーチャル空間においては場所・サイズ基準が有効に機能しないが，同じ問題は，物質空間においても生じうる。例えば，少量の麻薬を捜索する場合，麻薬には固定サイズがないから場所・サイズ基準は有効に機能せず，あらゆる場所の全域を捜索してもよいという帰結になるが，これはＩＴシステムに対する捜索の場合で生じうる問題と異なるものではない。

そして，かかる問題への対応策として，例えば，ＩＴシステムに対する捜索において，捜査機関が独自に開発したコンピュータ・プログラムなどの特別な選別ツールを利用し，捜査官が捜索できる範囲を限定する手法が可能であり，かつそれをとるべきものであるとすれば，同じことは，物質空間において行われる少量麻薬捜索事件の場合にも妥当する。具体的には，捜査官の五官による捜索を行うに先立ち，まずは麻薬犬を使うものとし，麻薬が隠匿される蓋然性がある容器(箪笥や引き出し)ないし区切られた空間(地下室や車庫)を確認しながらその範囲を画定しておかなければならない。言い換えれば，捜査官は，麻薬犬などのツールの使用を先行させなければならず，それによって蓋然性の有無を確認したうえで，蓋然性があると判断された容器しか開けることができず，蓋然性があると判断された区切りの空間しか検視できないことになる。

これに対して，ＩＴ基本権という法益から出発すると，それは専らＩＴシステムに着目するものであるため，上記の麻薬犬による蓋然性の捜索といった規制の可能性と必要性は考慮外になってしまうことになる。

２．物質空間における管理権基準の問題点

バーチャル空間(仮想的な場所)の要保護性判断につき，従来の管理権基準をそのまま適用すると，ネットワーク・プロバイダー等の上位の管理権限者を被処分者とする限り，下位の管理権限者である個人のユーザーの利益が無視されてしまうという点が問題として指

摘されてきた[808]。だが，これは物質空間においても生じうる問題である。なぜなら，物質空間においても１つの場所が他の場所を内包することはよくあることだからである。例えば，日本の事例であるが，1 つの研究棟の中に，個別独立した 69 の研究室があり，それぞれの管理権は異なる研究者に属するにもかかわらず，学長が大学に対する包括的な管理権を有するという点を根拠として，１通の令状により，大学研究棟全体への捜索が認められた，いわゆる和光学園事件があげられる[809]。かような捜索は，台湾では常態として行われてきたが，2001 年以前には令状主義が取られていなかったため，訴訟上は争いになることはなかったのである。2001 年以後には令状主義の採用が現行法上は明示されているものの，その具体的な内実についてはなお争いがあり，そのうち，日本でいう各別の令状原則(すなわち一場所一令状原則)が台湾の現行法のいう令状主義の一内容として確立されていないから，かような捜索が争いの対象とされた裁判例がまだ見当らないのが現状である。

ともあれ，以上の通り，１通の令状により１つの大きな場所における複数の小さい場所を捜索することは，物理的な場所であれ仮想的な場所であれ，それらのいずれについても質的な差をつけられない。というのも，１つのシステム(例えば，上層のプロバイダーのシステム)が他のシステム(例えば，下層のプロバイダーないし各々のユーザーのシステム)を内包するというバーチャル空間(たいえば，１つの巨大なＩＴシステム)の構造と，１つの場所(例えば，和光大学の構内)が他の場所(各学部の異なる管理権に所属する独立した建物ないし独立した建物内にある独立した個々の研究室の部屋)を内包するという物質空間の構造は，同質のものといえるからである。この意味で，下層の個々の管理権者(例えば，下層のプロバイダーないし各々のユーザーあるいは研究室の利用者)の権利が，最上層の管理者(例えば，上層のプロバイダーないし学長)を処分の対象者とする令状の発付により否定されることがないようにするための法的な配慮は，ＩＴシステムなどのバーチャルの空間の場合であるか物理的な空間の場合であるかを問わず，適用されるべきである。

これに対して，ＩＴ基本権の理論は，専らＩＴシステムを対象とするものであるから，それをもとに法益論を構築すると，前述した物理的な空間にも生じうる上下層の管理権者の利益の衝突と調和の問題性が看過されてしまい，問題の対応には限界があるということができよう。

３．情報システム基本権の意味

(1)情報システムの定義

ここまでの検討の中でも明らかにしたように，情報システム基本権は，ＩＴシステムに限られないものであるが，その具体的な中身はいかなるものであるかを敷衍すると，次のようなものとなる。

本稿は，情報システムを，「処分の対象としての情報を含む可能性がある，体系的若し

[808] 川出・コンピュータ犯罪 12 頁，林永謀・刑訴釋論(上)452 頁参照。
[809] 東京地決昭和 45 年 3 月 9 日刑月 2 巻 3 号 341 頁。

くは検索可能な情報の集合体又は一定の物理的若しくは非物理的なスペース」と定義する[810]。その典型例は，特定の個人情報あるいは捜査の対象となる情報を容易に検索することができるよう体系的に構成された大量の書類(例えば会計帳簿など)である。その他に，例えば，銀行の保管箱の集合，コインロッカーの集合なども，ここでいう情報システムに該当する。というのも，数百個の保管箱やコインロッカーを捜索する場合も，ＩＴシステムに対する捜索の場合と同様に，検索ツールを用いて蓋然性の確認を先行することは可能だからである[811]。

(2)不可侵性の定義

次の問題は，どのような情報システムが，基本権としての「不可侵性」を有するものと言えるかである。

この点，08 年判決は，ＩＴ基本権の保護範囲は「大量かつ多様な個人データを含むことが可能であり，かつ網目状に結合された複雑なＩＴシステムに限られる」としているが[812]，「網目状の結合」はＩＴシステムに特有な特徴であって，他の情報システムにはふさわしくない。それゆえ，情報システムの不可侵性を構成する核心要素は，むしろ，「システムにおける膨大かつ多様な情報の存在可能性」という特徴に求めるべきである。

この特徴からすると，情報システムだからといって，当然に基本権としての不可侵性を有するわけではなく，例えば，小容量のフロッピーディスクは，個人情報を含む可能性がある情報の集合体という定義にはあてはまるが，そこに大量かつ多様な個人データを含む可能性がないから，システムの不可侵性が認められないことになる。ただし，極めて多数の小容量のフロッピーディスクに対して第１章で指摘した蓋然性による差押えを実施する場合には，大量かつ多様の個人データを含む可能性が生じてくるから，それは情報システムの不可侵性という法益の保護射程範囲内にあるものである。

そのうえで，「不可侵性」とは，前に定義した「処分の対象としての情報を含む可能性がある，体系的若しくは検索可能な情報の集合体又は一定の物理的若しくは非物理的なスペース」の「完全性」を保持する利益を指す。言い換えれば，情報システムの「不可侵性」とは，かかる情報の集合体又は一定のスペースにある，あらゆる情報が探知されうるような状態に置かれないこと，及び，情報の集合体又は一定のスペースの体系，機能ないしその既定する状態が利用・破壊・阻害・改変されないこと[813]，の２つの要素からなる「完全性」の利益を保護するものである。

---

[810] 個人情報の保護に関する法律２条２項を参考にした。

[811] 具体的には，保管箱やコインロッカーの中にある銃を探すそうとする場合，捜索の範囲を最小化するために，まず，金属探知機をもって銃が存在する蓋然性を確定しておかなければならない。また，贓物である花瓶を探す場合には，そのまずはエックス線探査機による探知などのステップを先行させるべきことになる。

[812] a. a. O.(BVerfG, Anm.549)Rn.203.

[813] 「システムの体系，機能ないしその既定する状態の利用・破壊・阻害・改変」の一例をあげると，覆面捜査官がシステムに侵入したうえで犯罪組織の一員Ｘのアカウントの設定を改変し，Ｘの登録を阻害すると同時に，Ｘを装って組織の他のメンバーと接触する，というような捜査の手法が考えられよう。

(3)新たな法益論の実益

情報システム基本権という法益を認めることの実益としては，次の３つのものが考えられる。すなわち，①秘密性(プライバシー)のあるデータとそうでないデータとを区別する必要がなくなること[814]，②物質空間とバーチャル空間に対して，理論上の一貫性を維持した形での規制ができること，及び③法益保護の範囲をより一層拡大すると同時に，法益保護が行われる段階を早めることができることである。このうち，①と②については，既に述べたので，以下では，③のみを取り上げる。

従来の情報自己決定権では，政府の侵入したシステムに個人情報が存在しない場合や，単にシステムに侵入しただけでデータの検索・取得ないし分析などの処理がまだ行われていない場合，情報自己決定権に対する侵害が未だ生じていないため，被処分者は法的な保護を受けられないとされる。これに対して，情報システムの不可侵性を独立の基本権として保護すべきものであるとすると，ここであげた２つの場合は，情報自己決定権への実害は未だ生じていないものの，情報システムの不可侵性という基本権は既に侵害されたと評価できるから，法益保護の段階を早めることができるのである。そして，情報システムの定義にあたるものであるかぎり，ＩＴシステムではない場合も，法益保護段階の早期化という利益を受けることができる。

４．法益侵害の判断基準

最後に，いかなる基準をもって，情報システム基本権が侵害されたといえるかを検討する。この点，前述した通り，情報システム基本権には，①情報システムの不可侵性及び②不可侵性を有するシステムにおける全情報の要保護性の２つの(基本権法益の)構成要素が含まれるが，①が②の前提となるものであるから，以下では，①に絞って，それがいかなる時点で侵害されたといえるかについて検討する。

まず，オンラインでＩＴシステムに侵入するには，オンライン侵入技術を利用する必要があり，また，オンライン侵入技術を利用するために必要な情報を手に入れようとすれば[815]，覆面捜査官，通信傍受ないしその他の探索技術を利用する必要があるため[816]，かかる手順のどの段階で情報システムの不可侵性に対する侵害を認めるべきかについては，それを論理的に決めることが困難である。

---

814 「不可侵性を有するシステムにおける全情報の要保護性」という(基本権法益の)構成要素によれば，情報システムの不可侵性をもつシステムのなかにある情報であるならば，それはプライバシーに属するものであるかどうかを問わずにすべてを保護すべきものとする。

815 具体的には，オンライン侵入技術を実際に利用するために，対象者のインターネット上の活動の詳細や対象者の端末及びその端末が接続しているネットワークのシステムなどの関連情報を手に入れておかなければならない。例えば，スパイプログラムを投与しようとすれば，まず，対象者がインターネットにアクセスする行動を掌握しておく必要がある。また，仮に捜査機関がシステムの脆弱性を利用し対象者の端末に侵入しようとすれば，まず，対象者の端末のシステムないしそれと接続しているネットワークのシステムを十分に理解したうえで攻撃可能な弱点を確認しておかなければならない(Weiß, S.15.)。

816 Weiß, S.15.

さらに，情報システムはＩＴシステムよりも広い概念であるがゆえに，かかる侵害の有無を判断するための基準はより一層複雑になる。というのも，情報システムという概念のもとで観念される「侵入」の対象は，オンラインのＩＴシステムにかぎらず，オフラインのＩＴシステムも含まれるし，さらに，例えば，大量の書類ないしコインロッカーやマンションなどの集合物についても，それらを何らかのツールないし技術により体系的に検索することが可能であるかぎり，ここでいう「侵入」の対象となりうるからである。

もっとも，例えば，住居に対する捜索の場合にも，問題がないわけではない。すなわち，前述した通り，住居などの物理空間に対する侵入行為は，物理的な有形の侵入のみならず無形の侵入も含むが，いかなる条件をもって，住居に対して無形の侵入がなされたといえるかについては，議論の余地がある。この点について，アメリカのKYLLO事件[817]が有益な示唆を与えるものと考えられる。

同事件の概要は，次の通りである。警察官は，室内で大麻を栽培するためには，通常，高熱ランプの利用が必要であることを知り，上告人の家屋内にこのような高熱ランプがあるかどうかを確認するため，令状なしで，公道から上告人の住宅に向けて熱画像形成器を使用し，家屋内の熱が相対的に高く，室内に高熱ランプが存在することを確認した後，上告人の住宅の捜索令状を請求しその発付を得た[818]。

本件の争点は，「令状なしで，公道から上告人の住宅に向けて熱画像形成器を使用し，家屋内の熱が相対的に高いことを見つける」という行為は修正４条に反する不合理な捜索にあたるかである。これについての政府側の主張は，次の２点にまとめられる。第１に，家屋から外に漏れてきた熱を収集する行為は，「壁外での観察(off-the-wall)」にすぎず，「壁を通した監視(through-the-wall)」ではないので，それは住居への侵入行為にあたらず，捜索ではない[819]。第２に，「熱」を収集するだけであって，「私的領域で起こった内密な活動」を探知するわけではない[820]。

これに対して，連邦最高裁は次のように判示した。まず第１の主張に対しては，KATZ 事件で示された通り，修正４条の適用の基準は，「壁外での観察」か，それとも「壁を通した監視」ではなく，「プライバシーの合理的な期待」に求められるから，政府が主張するような区別論は修正４条の硬直的な解釈であって採用すべきではないとする[821]。そして第２の点については，「熱」だけであっても内密な事柄にあたるとし，その理由として，家屋内の「すべての事柄」は内密な事柄であるからだと述べた[822]。

結論として，法廷意見は，政府側の主張を斥け，令状なしで熱画像形成器を利用し公道から個人の家を狙い，家屋の内密な事柄を開示させる行為は，修正４条の禁じる不合理な

---

[817] DANNY LEE KYLLO v. UNITED STATES, 533 U.S. 27(2001)。本判決の詳しい紹介は，洲見 695 頁以下参照。
[818] DANNY LEE KYLLO, id., at 29 ～31.
[819] Id., at 35～36.
[820] Id., at 37～38.
[821] Id., at 35～37.
[822] Id., at 37～39.

捜索にあたる侵入行為であるとした[823]。

このKYLLO事件の判旨と，前述したドイツの08年判決とを比較すると，以下の２点の示唆が得られる。

第１に，家屋内から外へ洩れた熱を収集する行為も侵入行為に該当するとするKYLLO事件の判旨は，電磁波漏洩を収集することによりＩＴシステム内部の情報を探知することもＩＴシステムへの侵入行為にあたると判示した08年判決の立場と同じであると思われる。

第２に，家屋内の事柄であるならば，すべて内密な事柄であるというKYLLO事件の判旨は，ＩＴ基本権をなす１つの要件である「データの秘密性」についての08年判決の論旨は，ＩＴシステムの内部のデータであれば，すべて秘密性を有するものであることを意味するという解釈と一致しているものと考えられる。

以上の検討を踏まえて考えると，「侵入」とは，KYLLO判決で示された通り，ある領域の壁を通ることではなく，当該領域内部における内密な事柄を開示させることと理解すべきである。この理解は，「領域の壁」を観念できない情報システムにもそのまま適用することができる。

また，情報システムの不可侵性に対して，住居の不可侵性と同程度の憲法上の保護を与えるべきであるから，「家屋内の事柄は，すべて内密な事柄にあたる」というKYLLO事件が示した法理は，情報システムの場面にも適用されるべきである。それゆえ，情報システムの内部にあるデータであるかぎりは，個々のデータの具体的な属性の如何を問わずに，そのすべてが秘密性のあるデータと評価されることになる。

以上から，情報システムの不可侵性という法益は，「情報システム内の事柄が開示され始める時点」で侵害されると考えられる。例えば，ＩＴシステムの場合でいえば，オンライン侵入技術を実際に利用し始めたり，ＩＴシステムから洩れた電磁波を収集し始めたりした時点などが考えられるであろう。他方，大量の体系的な情報を結成した紙媒体の資料に対して，現場で関連性のあるドキュメントとそうでないドキュメントを選別できないため，資料の内容を確認せずに一括して差し押さえるような場合は，情報システムの不可侵性の侵害の発生時点は，当該紙媒体が置かれた家屋に立ち入った時点でも当該紙媒体が押収された時点でもなく，警察官が当該情報システムを構成する紙媒体の第１頁を開いた時点になろう。

第４節　「情報の捜索」という制度について

第１款　捜索の新定義

情報システムの不可侵性という法益論を前提とすれば，捜索の概念を，「一定の物理的な空間における物若しくは情報の発見又は一定の非物理的な空間における情報の探知を目

[823] Id., at 36～37.

的として，侵入又は探索し必要な措置をとる強制処分」と新しく定義することができる。

ここでいう一定の物理的な空間とは，場所，容器ないし人の身体などを指すのに対して，非物理的な空間とは，ＩＴシステムなどのバーチャル空間のほかに，情報システムという法理念的な空間をも含むものとする。

次に，「侵入」と「探索」との関係についてであるが，従来，「侵入」の部分は，捜索に必要な処分として，「探索」の部分に吸収されると理解されてきた[824]。というのも，これまでの捜索令状の発付は，家宅などの物理的な空間への侵入を対象とするから，侵入の方式は，通常の方法[825]によるべきであり，そこに大きな問題はないと考えられてきたからである[826]。言い換えれば，従来，「探索」の部分が捜索の核心の部分として理解されてきたのに対して，「侵入」はあくまでこの核心の部分のために必要な処分として捉えられてきたに過ぎない。

しかしながら，家宅などの物理的な空間への侵入を対象とするからといって，侵入の方式が必ずしも通常の方法によるわけではないだろう。例えば，現行法のもとで，捜索のために，大規模の破壊を行うことが果たして認められているかは疑問がないわけでない[827]。さらに，オンライン捜索で見た「オンライン侵入技術」の侵害の強度に鑑みると，捜索という制度の核心が果たして「探索」にあるかについては，再考の余地があるように思われる。以上より，「侵入」部分も「探索」部分と同等な重要性を持つと考えるべきである。ここから，立法論としては，「侵入」部分は「探索」部分に付随する必要な処分ではないから，それについても個別の司法審査を必要とするという帰結が導かれる。とはいえ，侵入の部分を探索の部分から独立し個別の司法審査に服させる必要がない場面もありうるから，そのような場面では，従来のとおり，捜索に必要な処分として扱ってよかろう。そうすると，個別の司法審査を必要とする「侵入」と必要としない「侵入」（すなわち，捜索に必要な処分）とを区別するための基準は何なのかが問題となる。

この問題を考えるにあたっては，オフラインで行う場合とオンラインで行う場合とに分けて検討する必要がある。というのも，第１章において示したとおり，オンラインの場面とオフラインの場面との間には次のような重要な相違点があるからである。すなわち，オンラインの場合は，遠隔操作という方法によるものであるので，複数のネットワークを経由し，

---

824 美濃部 378～379 頁。

825 ここでいう「通常の方法」とは，理性を持った一般人ならば誰でもかような侵入の方式が社会通念に反しない適切なものと考える程度の方法を指す。具体的には，捜索すべき場所に侵入するために，マスターキーが役立たない場合，鍵を破壊したり窓ガラスを割ったりすることがここでいう通常の方法として考えられるのに対して，バックホーなどのビル解体用の工事器機をもって，対象の場所の壁を破壊したりするというような方法は，通常の方法には当たらない。

826 美濃部 378～379 頁。

827 この点について，日本の先行研究においては争いがある。必要があれば日本刑訴法 129 条に例示されている処分もすることができるとする肯定の見解として，団藤・条解（上）218 頁，平場ほか・注解（全訂新版）上巻 364 頁［高田］，伊藤ほか・注釈（新版）２巻［佐藤］201 頁＝初版：青柳・註釈(1)［佐藤］412 頁が挙げられる。これに対して，129 条に例示処分として列挙してきたのに，同法 111 条にかような例示をしなかったことを理由に，反対する見解がある（中下 46 頁，平田 417 頁）。この日本の議論は，台湾刑訴法 144 条（日本刑訴法 111 条に相当するもの）と同法 213 条（日本刑訴法 129 条に相当するもの）との関係上，台湾の場合にもそのまま適合するものである。

最後にリモート・アクセス先に到達するという形になるから，捜索の対象は，遠隔地にあるリモート・アクセス先である端末のみならず，それと繋がっている，範囲をあらかじめ特定しておくことができない複数の階層のネットワーク，及びそれぞれのネットワークとさらに繋がっていくその他の端末も含まれうることになるのに対して，オフラインの場合は，既に占有した端末のみを対象に,その捜索の範囲をあらかじめ特定しておくことが可能である。

Ⅰ．オフラインで行う場合

従来は，捜索すべき場所に置かれた，本件と関係のあると思われる個別の物件(容器)や文書を捜索するには，同場所に対する令状さえあれば十分であり，また別途にそれぞれの物件や文書を対象とする別個の捜索令状の発付を請求するのは不要であると解されてきた。ここでの問題の核心は，ＩＴシステムなどの仮想的な空間を作り出す超大容量のコンピュータなどの電磁的記録媒体も有体の文書や一般の物件と同様に物理的な空間に置かれる有体物であるが，かような媒体に対しても，文書や物件と同様に，同媒体に置かれた場所に対する令状をさえ持っておけば，同令状をもってかかる媒体の中身を探索することが認められると解すべきかにある。この点，前述した通り，アメリカにおいては，コンピュータと一般の物件とを区別し，それぞれに異なる措置をとるべきとする見解が存在している。その代表的な議論としては，TAMURA判決の混雑文書ルールを基礎としたWinickの２段階令状論が挙げられよう。

他方で，日本においては，文書と一般の有体物との相違から，両者で異なる処理をすべきとする見解が存在している。すなわち，青柳教授により，「その物が文書である場合には個人の秘密権が不当に侵害されることもあり得る。このような点は果して押収捜索の令状主義で解決ができるかどうか……」[828]という疑問が提起されてきた。この青柳教授の問題提起は，文書と一般の物件との差異を起点とし，このような差異に対応する上で，既存の単一段階の令状制度による規制だけでは不備があることを意識するものであるといえよう。この意味で，青柳教授の問題意識とWinickの問題意識とは異曲同工と考えられる。というのも，それらは，いずれも，文書は一般の物件と異なる情報量を含んでいるという点に着目し，現行の捜索・押収制度はあくまで一般の物件を対象とするものにすぎず，そのままでは文書に適合しないという発想を起点とするものだからである。とはいえ，問題への解決策としては，青柳教授の提案とWinickのそれとは全く異なるものである。

そこで，以下は，青柳教授の提案とWinickの提案とを主な比較考察の素材に，コンピュータ，文書と一般物件との差異に着目し，オフラインの場面で無体の情報を捜索の対象とする場合の問題点を検討してみたい。

[828] 青柳・文書 28 頁。

１．場所と物件との関係について

ここで検討したいのは，捜索すべき場所に対する令状をもって当該場所に置かれた物件を捜索することができると解されてきたが，こうした場合にその捜索すべき範囲を如何に画定すべきであるのかという点である。以下では，アメリカの状況と日本の状況とを検討し，そのうえで，台湾への示唆を抽出する。

A．アメリカの状況

アメリカの判例及び通説の見解によれば，原則的には，個人は，「閉められた容器（closed containers）」に対するプライバシーの合理的な期待を有し，ある場所に置かれた閉められた容器を捜索するためには令状が必要とされる[829]。そして，この原則のもとで，１つの令状さえあれば，閉められた容器の全体を捜索することができるとされてきた。なぜなら，従来，「閉められた容器」という概念は「範囲が限定された狭い空間」と理解されてきたので，その空間のすべての領域を捜索しても修正４条が禁じる一般的・探索的捜索にはならないと考えられてきたからである[830]。

もっとも，この「閉められた容器」保護の原則に対しては例外がある。すなわち，アメリカ連邦最高裁は，ROSS 判決において，「閉められた容器」保護の原則を認めつつも，ある場所の中に置かれた個別の閉められた容器に対しては，当該容器の中に捜査の対象となる事件の証拠物を発見する蓋然性がある限り，当該場所への捜索令状のほかに，容器に対する別個の捜索令状は要求されないと判示している[831]。

こうした原則とその例外は，伝統的な家宅捜索・差押えというような場面においては，特に問題視されていない。しかしながら，それをコンピュータへの捜索の文脈にそのまま適用すると，一般令状を認めるに等しいから適切ではないと指摘されてきた[832]。ここでの問題の核心は，コンピュータを普通の閉められた容器と見るべきか，それとも，それを場所と見なすほうが妥当なのかという点にあるとされる。

この問題につき，下級審のレベルでは，個人はコンピュータに対し，閉められた容器と

---

[829] See Tex. v. Brown, 460 U.S. 730(1983), and see UNITED STATES v. ROSS, 456 U.S. 798(1982), at 798ff.

[830] Kerr, DIGITAL WORLD, at 550. この点をより具体的にいうと，アメリカにおいては，「閉められた容器」という概念は，従来，「範囲が限定された(閉められた)狭い空間」と理解されてきたのに対して，「場所」という概念は，「範囲がオープンな(閉められていない)広い空間」を意味するものであって，「閉められた容器」自体が，捜索の範囲を制限するための適切な基準であると考えられてきた。それゆえに，「閉められた容器」の範囲内であるならば，そのような，既に制限された狭い範囲の中でさらに捜索すべき範囲を画定する必要がないと理解されてきたわけである。例えば，ペーパーバッグやスーツケースというような，容量の極めて有限な物件である「閉められた容器」の枠内で捜索を行う場合には，その捜索できる範囲はあらかじめ当該容器の「物理的に有限な容量」により適切に限定されている以上，このような極めて狭い「物理的な有限な容量」をさらに最小化する必要はないとされてきた。言い換えれば，従来，「閉められた容器」自体が，「最小化」の単位とみなされてきたといってよい。よって，捜索できる範囲は，既に「閉められた容器」により最小化されている以上，最小化された範囲内にあるすべての内容物をみることは，そもそも，令状主義の理論の下で予定されている権限であるから，そこには一般的・探索的捜索というような問題が生じることはないと解されてきたわけである。

[831] ROSS, supra note 347, at 798ff。

[832] Winick, at 89; Kerr, DIGITAL EVIDENCE, at 301～303；Kerr, DIGITAL WORLD, at 549.

して修正４条の保護を受けることができるという見解が存在した[833]。この見解によると，まず，令状において捜索すべき物件がコンピュータであると明記された場合，当該コンピュータが閉められた容器となるから，その全体(中身)を捜索する(みる)ことができることになる。また，例えば，令状における捜索対象は場所であって，コンピュータが記載されていない場合で，差し押さえるべきものとして児童ポルノ画像という記載がある事例では，別個の令状なしで，当該場所への捜索令状をもって，サイズ等の物理的な特徴がない児童ポルノ画像を発見するために，当該場所に置かれたすべての“電磁的な閉められた容器”(PC, HD, iPho, PDA等)を起動し，その中に蔵置されたすべての情報を捜索することができることになる。

これに対し，Winick は，TAMURA 判決の示したいわゆる混雑文書ルールをコンピュータなどの電磁的記録媒体に対する捜索・差押えの場合にも適用することができるとしつつも，コンピュータを対象とする場合には特別な第２段階の令状による規制を必要としている。これと同時に，Winick は，コンピュータも大量の混雑文書の性格をもち，それを単なる閉められた容器とする見解は，そこに保存されたデータ量の膨大性という特徴を見過ごしており適切ではないと指摘している[834]。この見解は，ある物理的な場所に置かれたコンピュータを捜索する場合には，そこに保存されたデータ量が膨大である限り，それを単なる閉められた容器とみなすことはできず，前述した閉められた容器に対する原則とその例外は適用されないとする。その主張の核心は，次の２点にまとめられる。

第１は，バーチャル空間を仮想的な捜索すべき“場所”と見なすべきであるから，捜索すべき範囲を適切に画定しておかなければならないこと，第２は，この範囲を画定するための基準につき，場所・サイズを観念できないバーチャル空間においては，従来の「場所・サイズ」基準をそのまま適用すると，一般的・探索的捜索になってしまうから，その代わりに新しい基準を探求すべきであることである。

B. 日本の状況

日本においては，アメリカでいう「閉められた容器」保護原則とその例外というような法理が存在しないが，捜索の許容範囲の判断につき，アメリカの理解と同様に，「捜索場所に置かれた物が，原則として，その場所の概念の中に含まれ，場所に対する捜索令状によって，その物の中を捜索できることには争いがない」とされる[835]。そして，その制限も，アメリカと同様に，「場所・サイズ」という基準に求められてきた。すなわち，基本的には，場所にあるすべての閉めら

---

[833] See United States v. Hersch (1994) D. Mass. Sept. 27; United States v. Reyes(10th Cir. 1986)798 F.2d 380; States v. Gomez-Soto(9th Cir.1984) 723 F.2d 649。

[834] Winick, at 89.

[835] 川出・捜索(1)範囲 48 頁(同旨として，松尾・条解（第３増補）186 頁＝松尾・条解４版 221 頁，田宮編著・刑訴法Ⅰ［荻原］376 頁，幕田 86 頁，令状事務(1 版)342 頁，田宮・注釈刑訴 131 頁等参照)。ただ，同じ捜索場所に置かれた物であっても，他の排他的管理権が及んでいる場合(例えば，銀行支店内に設置された貸金庫)，当該捜索場所に対する令状によってはかかる物を捜索することができないとされる(令状事務(1 版)343 頁，刑事裁判資料 140 号 224 頁，三井・手続法(1)[新版]45 頁，松尾・条解４版 221 頁参照)。

れた容器を開けてもよいわけではなく，令状に明記された差し押さえるべき物が見つかると信ずる相当な理由を有する閉められた容器しか開けられないし，また，令状に明記されていない物を差し押さえることはもちろんできない。言い換えれば，日本においても，実質としては，前述したアメリカでいう「閉められた容器」保護の原則とその例外と同じ運用がなされてきているといってよいだろう。

しかし，日本においては，コンピュータは「閉められた容器」であるか，それとも，「捜索すべき“場所”」であるかというような争いはない。なぜならば，このような問題が生じる前提として，情報が独立した処分の対象として認められることが必要になるが，有体物のみを対象とする日本の現行法のもとではこのような前提が満たされていないからである。

もっとも，青柳教授は，物件と文書との差異に着目し，通説と異なるニュアンスを含んだ次のような見解を提供している。「文書の場合は，他の証拠物がその性質形状の検証のために取得保管されるのに過ぎないために何人がこれを検査しても特段の差異をひき起さないのに反して，その内容それ自身のもつ意味が問題なのであって，一定の審判の請求を受けた裁判官がその内容を検討する場合と，その犯人の何らかの犯罪又はこれに関連する犯罪をも捜査の対象としようと欲している捜査機関がこれを検討する場合とでは，その文書のもつ証拠としての価値が異なる。」[836]

この見解は，文書も単なる物件(すなわち，アメリカでいう閉められた容器)であるとする日本の通説と異なるものがあるとはいえ，文書自体を捜索すべき「場所」と観念するわけではなく，単に，一般の閉められた容器と異なる特別な要保護性を持った物件として取り扱うべきというに止まっている。というのも，青柳教授も，有体物のみを対象とするという点では，従来の通説と同様だからである。

２．明示の可能性について

続いて，対象たる文書を明示することの可能性につき，青柳教授は以下のように述べている。

「捜査の必要と秘密権の保障との調和[について]，……本来文書の差押捜索のために案出されたのでない差押捜索令状の制度を用いて完全にこの調和を得ようとすることは不可能に近いことであるまいか。文書はその他の証拠品と異って種々の表題，形状と種類をもつことであり，その事件の捜査に必要な書類は，その犯罪構成要件を証明するものに限定したところで，その明示は極めて困難である。而も情状に関する資料や，その被疑事実の展開に必要な関連事件の資料をも排除はできない以上なおさらのことだからである。その反面に文書は一つのものであってもそこに犯罪事実の資料だけが収められているわけではなく，そこに種々の面から種々の価値を含むものである。……文書の差押え，捜索を裁判官の許可状で制禦しようとするところに，はじめから無理があったと思われる。」[837]

---

[836] 青柳・文書 29 頁。

[837] 同前注 29～30 頁。

ここでは，文書は，固有の物理的な特徴をもたないから，特定が難しいと同時に，１冊の文書の押収は，常に，被疑事実と関連性のある部分(犯罪事実の資料)とそうでない部分(犯罪事実の資料にあたらないその他の種々の価値)とを一括して取得することになるという指摘が重要である。この指摘は，アメリカでいう混雑文書ルールに類するものと思われる。というのも，前述した通り，混雑文書ルールの前提としては，単一の文書の中に，関連性のあるドキュメントとそうでないドキュメントとが分割できずに混在している状況が挙げられるからである。そのうえで，同教授は，文書に対する捜索・差押えについて後述するような最小化の方策を提案している。

３．最小化の方策について

以上の通り，問題となる場面はやや異なるが，文書を検討の対象とする青柳教授の指摘と，電磁的記録媒体を検討の対象とするWinickの指摘とは，問題意識としては同質のものといえる。しかし，両者の対応策は異なる。

すなわち，Winick は，やむをえず，関連性のない部分をも一括して差し押さえる場合には，その後の捜索を規制するための「第２段階の令状」を必須とするという最小化の方策を提案している。これに対して，青柳教授は，文書における情報量と一般の証拠品におけるそれとは異なるから，文書における関連性のない部分の内容の秘密権と捜査の必要性とを適切に調和できるようにするため，一般の証拠品と異なる特別な保護対策をとるべきであるとし，最小化の方策としては，以下のような立法提案をしている。

「それでは立法論としてどのような調和が捜査の必要と秘密権の保護との関係にもたらされるだろうか。裁判官が自ら文書の差押え，捜索の現場に臨まない方がその品位の保持のために望ましいということから現行法の令状主義が生まれているから，旧刑訴の方法に立ち戻ることは相当ではない。そこで文書の差押え捜索には許可状でなく裁判官の命令状を請求し，取得された文書は，捜査機関が直ちに裁判官に提出し，裁判官が被疑事実の重大性と秘密権との調和を考慮した上で関連性があるとしたものを捜査機関の利用に委ねるのが相当であると考える。裁判官が当該被疑事件と関連性がないと判断したものは直ちに還付することにし，差押えを受けた者，利害関係人，検察官はこの判断に対して準抗告できることにしたらよいであろう。さらにもう一つ根本的には捜査機関は文書を特定して裁判官の提出命令を請求できることにし，この提出命令に応じない者は英米法におけると同様裁判所侮辱の一種として秩序罰乃至刑罰を課することができることにし，これに応じて提出された物についても被疑事実との関連性を裁判官が審査の上で，関連性があるとしたものを捜査機関の利用に委ねるのがよいであろうと思う」[838]。

ここでは２つの特別な保護方策が提案されている。第１に，青柳教授は，捜査機関に第２段階の捜索についての具体的な計画書を提出させるべきであるとするWinickの見解より一歩進んで，裁判官が自ら，第２段階の捜索にあたる措置を行うべきであると提案してい

[838] 同前注 30 頁。

る。

第２に，青柳教授は，間接的強制処分――いわゆる提出命令――という方策を提案している。間接的強制処分と直接的強制処分の順位付けについては特に述べられていないが，前に引用した青柳教授の見解から推論すれば，直接的強制処分という方式を採用すると，やむを得ず，関連性のないドキュメントをも一括して取得しなければならないばかりか，その後，また，関連性のないドキュメントと関連性のあるドキュメントとを選別する手間を掛けなければならないから，間接的強制処分という方式を先行させるという方策が考えられよう。

４．台湾への示唆

以上により，以下４つの示唆が得られよう。

第１に，台湾の場合にも，日米と同様に，従来の理解によると，場所に置かれた物件(または容器)を捜索するために別個の令状は不要であるとされてきた[839]。なぜならば，こうした場合，その捜索できる範囲は，いわゆる場所・サイズ基準により制限されており，たとえば，盗難車を捜すためには引き出しを引いたり箪笥や箱をあけたりすることができないから，無制限の一般的・探索的捜索になることはないと解されるからである[840]。しかし，ここでの検討によると，バーチャル空間においては，場所・サイズという概念を観念することができないから，かような空間にも従来の「場所・サイズ」基準をそのまま適用すると，一般的・探索的捜索になってしまう。このように，場所と物件との関係を再考すると，物理的な場所を対象とする捜索令状をもっているからといって，当然にはかかる場所に置かれたコンピュータ器機という物件(または容器)のなかみ(その内部にあるＩＴシステム及びそこに記録されたデータ)を捜索することを正当化することができるわけでもないと考えられよう。

第２に，文書やコンピュータにのみ法の特別な保護を与えるという青柳教授及び Winick の提案は，いずれも妥当ではないと思われる。というのも，媒体が紙であるか，それともコンピュータであるかを問わず，重要なのは，捜査機関が取得しうる情報の量ないしその質であるので，そもそも，保護の対象をコンピュータないし文書に限定する理由はないからである。より具体的にいえば，膨大ないし混雑のデータ情報を記録したコンピュータであれ，大量の文字情報を記録した紙媒体の文書であれ，それらのいずれにおいても，場所にかかわる財産権，管理権ないしプライバシー権と独立した，いわゆる情報システム不可侵という別個の法益が存在しているから，この法益が存在する媒体に置かれた場所に対する令状だけでは，当該媒体を捜索することが認められず，別個の令状の発付を請求することが必要となる。

第３に，捜査機関に第２段階の捜索についての具体的な計画書を提出させるべきである

---

[839] 林鈺雄・捜索扣押 61～62 頁，同 150 頁の説明(捜索の標的による制限と呼ばれる)をも参照。

[840] 同前掲注，また，王・新修捜索 112～113 頁をも参照。

とするWinickの見解から一歩進んで，裁判官が自ら，Winickのいう第２段階の捜索にあたる措置を行うべきであるという青柳教授の提案は，捜査機関が中華民国憲法23条に要求される最小化原則を忠実に実現することを担保するためには中立かつ超然な司法機関による審査・監督のメカニズムを構築する必要があるという本稿の立場に適合しないものである。というのも，裁判官が自ら第２段階の捜索を行うと，それと同時に，中立かつ超然な司法機関という地位を失ってしまうこととなるではないかと考えるからである。

第４に，青柳教授は，間接的強制処分――いわゆる提出命令――という方策を提案している。間接的強制処分と直接的強制処分の順位付けについては特に述べられていないが，前に引用した青柳教授の見解から推論すれば，直接的強制処分という方式を採用すると，やむを得ず，関連性のないドキュメントをも一括して取得しなければならないばかりか，その後，また，関連性のないドキュメントと関連性のあるドキュメントとを選別する手間を掛けなければならないから，間接的強制処分という方式を先行させるという方策が台湾の立法論としても考えられよう。

Ⅱ．オンラインで行う場合

台湾においては，2001 年の法改正により，刑訴法上，電磁的記録をも捜索・差押えの対象としているため，学説上は，オンラインでデータを検索したりダウンロードしたりすることを，電磁的記録に対する捜索であるという論者がある[841]。しかし，同論者は，ダウンロードすることは，電磁的記録に対する差押えにあたるかどうかについては明らかにしていない。

この点，台湾の2001年法改正以後の現行法のもとにおいても，従来と同様に，差押えが占有の剥奪と定義されているから，占有の剥奪が発生しないダウンロードすることを，電磁的記録に対する差押えということはありえないと思われる。そうだとすれば，同じ理屈で，オンラインでデータを検索することを，電磁的記録に対する捜索ということにも論理上の困難があると言わなければならない。というのも，台湾においても，従来は，捜索は，差し押さえるべき物を発見するための手段と位置づけられてきたからである。言い換えれば，井上教授が指摘したとおり，捜索は，差押目的物を発見して差押えにつなげるための処分であり，差押えの対象物は有体物に限られるため，有体物である媒体の占有を剥奪するために対象となる媒体のある現場に捜査機関が出向いて捜索を行う必要がある以上，オンラインでの差押え・捜索を観念できないからである[842]。これに対し，井上教授は，検証であるならば，それは有体物の占有の剥奪を処分の内容としないものであるため，現場に赴かなくてもよいので，「オンライン検証」が観念しうるかもしれないと述べている[843]。

以上のとおり，台湾の先行研究においては，既存する捜索・差押えの定義との調和性を

[841] 林鈺雄・捜索扣押 95 頁。これに対して，反対説がある(捜索修法(二)131 頁蔡秋明の発言参照)。
[842] 井上・コンピュータ(2)54 頁＝井上・強制・任意 280～281 頁。
[843] 同前掲注。

深く考えることもなく，刑訴法の文言を形式的な根拠に，オンラインで捜索を行うことが現行法上は認められていると解する見解が一部で現れてきたが，かような捜索を如何に規制すべきであろうかという問題に対しては精密な検討がなされておらず，またオンラインで検証を行うことの可能性ないし問題点を検討した議論も見あたらない。これに対して，日本の現行法でいう捜索・差押え・検証の制度は台湾のそれとは異なる点があるものの，それぞれの定義自体は，台湾のそれらとは同じものであるから，前述した日本の井上教授が提供した解釈論は，台湾の現行法における捜索・差押え・検証の定義に叶う論理上の一貫性を有するものであると評することができよう。

こうして，台湾の立法論を見据えた，オンラインで捜索を行う場合の問題を検討するには，前に登場したドイツでいうオンライン捜索と並んで，日本でいうオンライン検証をも比較の素材とする必要性ないし実益があると考える。

１．オンライン検証とオンライン捜索

(1) 日独の問題状況

日本でいうオンライン検証と比較するために，ドイツでいうオンライン捜索の特徴をあげると，次の３点が重要である。第１に，オンライン捜索を行うために，オンライン侵入技術を利用し，ターゲットである端末のＩＴシステムに侵入しておく必要があること，第２に，捜査機関は，オンライン侵入技術を持っていれば，必ずＩＴシステムへの侵入に成功できるわけではなく，オンライン侵入技術を実施するためには，まず，対象者がインターネットにアクセスする行動を掌握したり，対象者の端末のシステムないしそれと繋がったネットワークのシステムを十分に理解したり，その攻撃可能な弱点を確認したりしておかなければならないこと[844]，第３に，対象者の行動ないし侵入の対象とするシステムの理解のために必要不可欠な関連情報を取得するための方法として，通信傍受，ポートスキャン[845]，覆面捜査官や捜査協力者という３つの選択肢が挙げられてきたこと，である[846]。

これに対して，日本のオンライン検証においては，オンライン侵入技術の使用に関して全く言及がなされておらず，捜査機関がすでに合法的に対象者のＩＤやパスワードを知っていることが前提とされている[847]。それゆえ，日本でいうオンライン検証とドイツでいうオンライン捜索とは全く別物であることになる。つまり，日本のオンライン検証が，対象者のＩＤやパスワードをあらかじめ知っておりかつ合法的に使えることを前提とするものであるとすれば，オンライン捜索でいう“裏口”(Backdoors)を利用するなどのオンライン侵入技術に頼る必要は全くない。というのも，日本のオンライン検証は，正々堂々，“正門”

---

[844] Weiß, S.15.

[845] ポートスキャンとは，特殊なソフトウェアを利用して，どのような「連絡構造」が許容されるかを明らかにするための技術を指す。また，ここでいう「連絡構造」とは，パソコン本体と周辺機器との間で信号ないしデータを受け渡すための接続端子及びそれぞれの対応関係を意味する。

[846] Weiß, S.15.

[847] 井上・コンピュータ(2)54 頁＝井上・強制・任意 280 頁。

――つまり，端末の系統が設定したルート通り――の“キー”であるパスワードとＩＤをもって，システムに進入(侵入)するものだからである。

他方，ドイツのオンライン捜索は，元々は，解けない暗号に対応するために開発されてきた捜査手法であるとされる。というのも，オンライン侵入技術を利用すると，まだ暗号化されていないコードを取得したりすることができるからである。これに対して，日本では，暗号技術の高度化により捜査には支障が生じているという問題は生じているものの[848]，それへの対応策としては，ドイツとは異なる以下の５つの方策が考えられてきた。

すなわち，(1)被処分者側としては，無関係の物まで差し押さえられてしまうことを避けるために協力させざるを得ないという事実上の解決[849]，(2)協力してもらえなかった場合は媒体の内容を確認せずに関連性のあるデータが存在する蓋然性がある媒体を一括して差し押さえるという対策[850]，そして，(3)暗号解読のために必要な技術力の強化という方策[851]，(4)日本刑訴法 99 条の 2(記録命令付差押え)，同法 111 条の 2(協力の要請)による対応，(5)暗号を規制するという政策[852]，である。

このうち，(1)が機能しない場合の最終結果は(2)になるが，一括して差し押さえたからといって暗号が解けることになるわけではない。(3)は技術の側面からいうと，正道であるが，しかしながら，ここでの問題は，捜査機関の技術力が犯罪者の暗号技術より弱い場合はどうすればよいかという点にあるから，これも，かかる問題の解決策にはならない。また，(4)は，強制力がないため，実効性の担保を欠いているように思われる。(5)は，日本の実態ではなく，1980 年代のアメリカの政策である。具体的には，①「暗号化を禁止・制限する」こと，②「暗号化に使われた鍵を破る」こと，③「なんらかの方法で暗号化の鍵を知る」ことの３つの政策に分けられている[853]。①は，産業界やプライバシー保護団体からの強い反対で頓挫しているとされる[854]。②は，技術上困難とされる[855]。③は，オンライン捜索という手法に似ているようにみえるが，実際には別物である。ここでいう「なんらかの方法で暗号化の鍵を知る」とは，1980 年代の技術を前提とするものであって，近年登場したオンライン侵入技術の利用とは関係がなく，具体的には KES（Key Escrow System）と KRS（Key Recovery System）の２つの政策を指す[856]。この通り，(1)～(5)はいずれも，オンライン侵入技術と無縁なものである。

---

[848] 酒巻・提出命令 128 頁，山川 63 頁参照。
[849] 河上・証拠法ノート(1)87 頁。
[850] 酒巻・提出命令 128 頁。
[851] 井上・コンピュータ(1)52 頁＝井上・強制・任意 247 頁。
[852] 指宿・インターネット盗聴 126 頁。
[853] 同前注。
[854] 同前注。
[855] 同前注。
[856] KES とは「政府機関，あるいは第三者機関が暗号鍵を保管し，裁判所の許可令状を得て政府が情報を解読できるような鍵の管理方式である」ことをさす。KRS とは「暗号鍵を政府に提出する」ことを意味する(同前注)。

(2)台湾への示唆

以上により，以下示す３点の示唆が得られよう。

第１に，台湾の解釈論としても，日本と同様に，検証という制度はオンライン捜索の法的な根拠にならないと解すべきであろう。というのも，台湾の検証も，日本のそれと同様に，五官の作用による認識と定義されてきたので，それは明らかにコンピュータ・プログラムによる徹底的な探索を行うというオンライン捜索の内実に合わないものだからである。

第２に，台湾においても，解読できない暗号が捜査の難問とされてきており，これまでは，(1)事実上の解決，(2)蓋然性による差押え，そして，(3)技術力の強化という３つの対応策が打ち出されてきたが[857]，立法論的には，日本刑訴法における記録命令付き差押え(99条の2)ないし協力・保全要請(111条の2，197条3項)などの制度を台湾にも導入し，それらに間接的強制力を与えるという対策が考えられよう。この対策をとることのメリットとしては，処分対象が有体物であることを前提になされてきた捜索差押えの定義ないしその適用の基準・原則をそのまま維持することができる点があげられるが，被処分者が間接的強制力(法的処罰)を甘受する場合にはやはり直接強制処分が必要となるから，こうした場合の直接強制処分の１つの可能性としては前に論じたドイツのオンライン捜索という手段が考えられよう。しかし，オンライン捜索を導入しようとすれば，強制処分が物理的な空間で行われることを前提にした従来の捜索差押えの定義ないしその基準や原則をそのままバーチャル空間に適用させることができないから，情報をも独立した直接の処分対象としたうえで，情報及びそれが存在するバーチャル空間に相応しい捜索差押えの定義・基準・原則を改めて探求することが必要となる。そこで，本稿は，情報に対する差押えの場面に対応するに，第１章において，情報の終局的処分権という法益を提案したうえで，かかる法益をもとに，情報に対する差押えの新しい定義及びその適用の基準・原則を明らかにしている。そしてまた，捜索の場面に対応するに，本章の第３節第２款において情報システムの不可侵性という法益を打ち出しており，そのうえで，同章の第４節第１款においてこの法益に沿って情報及びそれが存在するバーチャル空間を対象とする場面に相応しい捜索の新しい定義を述べている。これを踏まえてこれからは，情報(ないしバーチャル空間)に対する捜索令状の発付要件及び適用基準・原則を探求してきたい。

第３に，対象者のインターネット上の行動ないし対象たるシステムの詳細などの情報自体は，犯罪事実とは直接の関連性がなく，単に，オンライン侵入を実施するために必要な情報にすぎない。台湾においては，このような，捜査に必要な前提知識である情報を探知するために，通信傍受，ポートスキャン，覆面捜査官や捜査協力者を利用することができるかという点についても大きな疑問があり，なお別個に検討すべき問題であるように思われる。

---

[857] 法務部・電腦犯罪４版15，21頁参照。

２．オンライン捜索とオンライン検閲

(1)日独の問題状況

オンライン捜索との比較をするには，オンライン検閲（Onlinesichtung；Vgl.StPO§110③）という捜査手法にも言及する必要がある。オンライン検閲とは，ドイツの刑事訴訟法110条3項(以下，ドイツ刑訴法〇条〇項という)で定められているものであり，「捜査機関が合法的な捜査により占有した被処分者が所有するオンライン状態の電磁的記録媒体から他の遠隔端末にアクセスしデータを取得する」手法を指すとされている[858]。

ドイツの学説においては,オンライン検閲の規定の適用は「公然の侵入」(offener Zugriff)の処分に限られるから[859]，「密かな侵入」（heimlicher Zugriff）であるオンライン捜索の根拠にはならないとされる[860]。また，多数の意見によれば，オンライン検閲は，捜査機関がオンライン侵入技術を使わずに占有した被処分者のコンピュータから，既存の設定状態のままで他の遠隔保存媒体にアクセスすることができ，かつ証拠保全の必要性がある場合にのみ認められるとされる[861]。これらの点に鑑みると，オンライン検閲はオンライン侵入技術の使用を必要とするオンライン捜索の定義に当てはまらないことが明らかであろう。

これに対して，判例上は，ドイツ刑訴法 102 条以下の家宅捜索に関する規定を根拠としてPCへのオンライン捜索を認めた連邦最高裁の 2006 年の決定(BGH. Beschl.)が存在した[862]。しかし，2007 年のドイツ連邦最高裁の判決(07 年判決)は，オンライン捜索は現行法上予定されていない手法であると判示した[863]。そして，ドイツ連邦憲法裁判所が 2008 年に前述した 08 年判決においてはこの 07 年判決の判断を確認している[864]。つまり，オンライン検閲はオンライン捜索と異なるものであり，その根拠であるドイツ刑訴法 110 条 3 項はオンライン捜索の根拠にならないという理解が，権威ある連邦憲法裁判所の立場である。

以上により，被処分者の端末機器を物理的な占有をしたうえでさらにそこから他の端末にアクセスし目標たるデータを取得するという，日本のオンライン検証は，ドイツのオンライン検閲に類似したものといえよう。この点からも，日本でいうオンライン検証は，ドイツのオンライン捜索に当たらないことがわかる。

そのうえで，日本の理解とドイツの理解との間には次の２つの相違点がある。

第１に，日本でいうリモート・アクセスと，ドイツでいうオンライン検閲とは，行為態様の実質としては同じものであるものの，その性格は異なる。というのも，日本のリモート・アクセスによる差押え関連規定は，緊急処分でなく，令状による差押えの一類型であ

---

858 Hegmann, §110 Rn 13 ～15.

859 「オンライン検閲」は，家宅捜索（StPO§102ff）を前提とするものであり，家宅捜索の行為が公開原則（Grundsatz der Offenheit）により形作られているものであることを意味する。

860 Wiss, S26.

861 Wiss, S.28; Hegmann, § 110 Rn 13.

862 BGH21/02/2006(3―BGs 31/06)BGH Wistra 2007, 28.

863 BGHSt 51, 211；auch vgl. BverfG, 1 BvR 370/07Rn.7; 植松５頁をも参照。

864 BverfG, 1 BvR 370/07Rn.7.

るのに対し，ドイツのオンライン検閲は，令状によらない緊急処分の性質をもつものだからである。すなわち，オンライン検閲の根拠規定であるドイツ刑訴法110条3項は，「捜査を受けた者に属する電子記憶媒体を対象とする検閲には，かかる電子記憶媒体からはさらにアクセスできる空間的に切り離された他の電子的記録媒体において存在する対象となるデータを確保しなければ，かかるデータを滅失させるおそれがある場合，その効力は，空間的に切り離された他の電子的記録媒体にも及ぶものとし，そこにある捜査に役立つデータを取得しておくことができる。こうした場合は，98条2項を準用するものとする。」と定めており，その適用は，捜査に役立つデータないし証拠の滅失を防ぐために限られるとされているのである[865]。

第２に，日本のリモート・アクセスによる差押え関連規定は蓋然性による差押えの性格をもつものであるから，リモート・アクセスを行う際に，データやファイルを検索や検閲したりすることは予定されていない。これに対して，ドイツ刑訴法 110 条 3 項は，書類の検閲（同法 102 条の被疑者に対する捜索若しくは同法 103 条の第三者に対する場合の検閲）を規制する同法 110 条１項の一般的な規定を補充するものとされている[866]。つまり，ドイツでいうオンライン検閲は，差押えでなく，捜索ないし検閲として捉えられている。そして，その理由は，次の点にある。

すなわち，ドイツにおいても，かかる捜査行為により差押えがなされたかが問題とされてきたが，通説によれば，捜査機関が媒体からデータを複製・記録することにより，何らの物理的な剥奪も行われておらず，単に，捜査機関の支配範囲内において，電子データの体現としての新しい物件を作り出すだけであるから，占有の剥奪を核心の要件とした差押えという概念に当たらないものとされてきたのである。つまり，媒体それ自体を差し押さえることなく，単にデータをコピーするだけであるリモート・アクセスは，差押えのカテゴリーには該当しないと判断されてきたわけである[867]。

しかし，その一方で，ドイツ刑訴法 110 条 3 項の第 2 文は，「こうした場合は，98 条 2 項を準用するものとする」と定めている。つまり，データをコピーすることは差押えでないとしつつも，差押えの関連規定を準用することになっているわけであり，この意味で，オンライン検閲は，実質的には差押えの性格をもつ処分であることが認められているともいえよう。

(2)台湾への示唆

以上により，次の２点の示唆が得られよう。

---

[865] Wiss, S.28; Hegmann, § 110 Rn 13; Graf, s.375.

[866] Wiss, S.25.

[867] Wiss, S.24. 通説によれば，ドイツ刑訴法 94 条以下の規定により，データをコピーすることができるとされるが，データをコピーすること自体は差押えではなく，差押えの縮小処分として認められるだけである(Roxin／Schünemann, S. 252～253)．というのも，差押えという概念は従来，「帰属」及び「徴収」 と観念されており，「公開的・司法的な保管機関による占有」という効果の発生を必要とするので，コピーだけでは，このような観念ないし効果を満たすことはないからである(Roxin／Schünemann, S. 253～254)。

第１に，日本でいうオンライン検証とは，①被処分者の端末機器と物理的な接触をすることなく，警察機関の端末機器から直接に目標たるデータを取得するという意味でのオンライン検証，及び②被処分者の端末機器を物理的に占有したうえで，さらにそこから他の端末にアクセスし目標たるデータを取得するという意味のオンライン検証，の２つの類型に分けることができる。このうち，①の類型については，ドイツでいうオンライン捜索と異なる点をここで確認すると，オンライン検証は，オンライン侵入技術を使わないオンラインで行う情報に対する捜索であるのに対して，オンライン捜索は，オンライン侵入技術を使うオンラインで行う情報に対する捜索である。そして，②の類型は，一般にリモート・アクセスと呼ばれており，それが，日本の今回の改正法により明文化されることになった。これにより，次のような立法論上の示唆が得られよう。すなわち，情報に対する捜索という制度につき，それをさらに細分化しようとすれば，「侵入」と「探索」との２つのカテゴリーに分けたうえ，①オンライン侵入技術を使う必要である場合とそうでない場合との区別，及び②警察の端末からアクセスする場合と被処分者の端末からアクセスする場合との区別を基準に，更なる類型化をすることが可能である。

第２に，日本のリモート・アクセスによる差押えと，ドイツのオンライン検閲とは，その捜査行為の実質は同じものであるものの，法的性格が分けられ，すなわち，前者は，差押えと，後者は，捜索ないし検証(または検閲)と位置づけられることからも，捜索・検証(検閲)と差押えの概念が混同する傾向が窺える[868]。しかし，日本もドイツも，かような混同の傾向とその法規制上の意味が十分に検討されておらず，結果として，ある１つの処分の類型に帰属させたうえで規制する形になっている。こうして考えると，既存の処分の類型を超えた複合的処分を必要としており，それを前提に新たな規制を設けるべきであると思われる。そこで，本稿は，類型化の必要性ないし有益性を認めつつ，類型化の不備・欠如に対応するために，オフライン及びオンラインのそれぞれの場面で行われるあらゆる態様の捜索(または検証・検閲)の行為を包摂できるよう，情報に対する捜索という新しい制度を設けることが必要であると考える。

３．オンライン侵入と必要な処分

最後に検討したいのは，台湾の現行法のもとにおいては，捜査の目的でオンライン侵入技術を用いることを認めるための法的な根拠はあるのか，もしあるとすれば，それは何なのか，である[869]。現行法上は，捜査の手段としてのオンライン侵入技術の使用にあてはまる強制処分の類型が存在しないことは明らかであるものの，「必要な処分」という概念を通

---

[868] 実は，この混同の傾向は，コンピュータ・ネットワークという文脈以外の場面でも生じうる。例えば，強制採尿令状を認めた最一決昭和 55 年 10 月 23 日刑集 34 巻 5 号 300 頁は，その典型例として考えられる。これを支持する立場として，和田康敬・強制採尿 26 頁，城毅・強制採取 114 頁など参照。批判的な見解としては，安富・科学的捜査 182 頁以下，白取・科学捜査 80 頁以下，渡辺直行 112～113，116 頁などが挙げられる。

[869] というのも，仮に，現行法上すでにオンライン侵入技術の使用を認める法的根拠があるとすれば，オンライン捜索というような手法をも含めた，情報を直接の対象とする捜索という制度を新たに設ける際，現行法上既存する根拠との整合性に配慮を払わなければならないからである。

じてそれを正当化することが考えられるかもしれない。

この点，日本において，捜索差押許可状の呈示に先立ってホテル客室のドアをマスターキーで開けて入室した措置が必要な処分として適法とされた最一決平成 14 年 10 月 4 日刑集 56 巻 8 号 507 頁(以下，「平成 14 年決定」という)が存在している。台湾においてはかような判決はないが，実務上これまではマスターキーなどの道具でドアを開けて入室するというような捜査の行為が捜索に必要な処分として認められてきている。その根拠を，日本の平成 14 年決定の旨を参考にして考えてみると，捜索に必要な処分を定めた台湾刑訴法 144 条 1 項[870]に求めることが可能であろう。こうして考えると，仮に，ＩＴシステムに侵入するためにオンライン侵入技術を利用することを，物理空間において個室に侵入するためにマスターキーを使用することと同視することができるとすれば，必要な処分としてオンライン侵入技術を使用することも許されると考えられるかもしれない。実際にも，日本の先行研究においてはかような考えを示す見解が学説上は一部で現れている[871]。

しかしながら，ＩＴシステムへの侵入と場所への立入りは全く異質なものであるといわなければならない。というのも，オンライン侵入は，個室に侵入するためにマスターキーを使用するというような容易なものではないからである。より具体的にいえば，オンライン侵入は，その実施により，損害額を予想しかねるほどの重大な侵害をＩＴシステムに対して引き起こす可能性もあることに加え，通信傍受，ポートスキャン，覆面捜査官や捜査協力者などの手段を先行させることが必要になるから，オンライン侵入技術の使用による権利侵害の重大性及びかかる手段の複雑性と，マスターキーの使用のそれとは，格段の差があるものだからである。それゆえ，現行法の「必要な処分」として，オンライン侵入技術の使用を正当化することはできないと解すべきであろう。

とはいえ，前にも論じた通り，日本のリモート・アクセスやドイツのオンライン検閲の場合には，オンライン侵入技術を利用することはない。そうすると，ここでの問題の核心は，ＩＴシステムの場合とそうでない場合との区別というよりは，むしろ，侵入行為の侵害強度という点にこそあると思われる。すなわち，ＩＴシステムにおいてオンライン侵入技術が使用される場合には，その侵害強度は高いと評価されるので，必要な処分に当たらないが，そうでない場合(ＩＴシステムへの侵入行為の侵害強度が低い場合)は，必要な処分により処理してよいといえる。一方で，物理空間の場合であっても，仮に，その侵入行為の侵害強度が高いものだとすれば，必要な処分の枠内で処理することの可能性を否定すべきであるという帰結になる。

以上の通り，「侵入」部分は，個別の司法審査を受ける必要がある場合もあれば，そのような必要はない場合もありうるから，法的には，このような事例の違いに応じて柔軟に対応できる条項を用意すべきであり，また，個別の司法審査を受ける必要性の有無を判断

---

[870] 台湾刑訴法 144 条 1 項は「捜索・差押えをするために鍵・封緘を開けたりしてあるいはその他の必要な処分を行うことができる。」と，日本刑訴法 111 条前段は「差押状，記録命令付差押状又は捜索状の執行については，錠をはずし，封を開き，その他必要な処分をすることができる。」と定めている。

[871] 指宿・サイバースペース 89 頁。

するための基準は，侵入行為の侵害強度に求められるべきであると考える。

台湾において，2001 年に新設された刑訴法 128 条 3 項後段は，「裁判官は捜索令状において執行人員に対して適当な指示を行うことができる」と定めている。この条項のいう「適当な指示」によりオンライン侵入技術の利用を正当化することが考えられるかもしれない。実際にも，学説上は，この新設された「適当な指示」により，「(ＩＴシステムに)進入し木馬プログラムを差し込むことができるというような記載も可能である。」[872]とし，「同条項の適当な指示とは，裁判官が主導的になされるものに限らず，令状発付の請求を行う捜査側からの申出も可能である。この点に関して，法務部[日本の法務省に相当する機関]が頒布した『捜索令状請求書』には，『適当な指示事項申請欄』が欠けており，かような欄を追加すべきである。」[873]と指摘する論者がある。

確かに，オンライン侵入が，裁判官が発付する令状における適当な指示により行われる場合であるならば，個別の司法審査を受けたものであるといえるが，しかし，台湾刑訴法 128 条 3 項後段のいう「適当な指示」は，果たして，オンライン侵入技術の利用を正当化するための根拠となりうるかについてはなお検討の余地があるように思われる。というのも，学説上は，同 128 条 3 項後段のいう適当な指示とは，「捜索の目的あるいはその範囲をより明確させるものにとどまる」[874]とする見解があるし，また，実際にも，捜査実務上の主流の立場はむしろこうした見解に近いものだと思われるからである。更に問題となるのは，この 128 条 3 項後段の規定は簡単すぎるものであるため，オンライン侵入技術の侵害性が低い場合はともかく，もし高度侵害性をもつオンライン侵入技術を利用する場合には，同規定だけではこうした場合を適切に規制することができないのである。

以上のとおり，128 条 3 項後段のいう「適切な規制」についての理解が学説上は分かれているし，また，その規定自体も完全ではないから，高度な侵害性のある「侵入」処分を適切に規制するためには，やはり，より明確かつ完全な法的根拠を用意することが必要となる。そのための立法の内容は，以下のようになる。

(1)個別の司法審査

侵入と探索とに分けて，それぞれ別個の令状により対応することも考えられるが，別個の令状によらず，１通の捜索令状においてそれぞれの審査を行った旨明記しておくという方式でも良いと思われる[875]。他方，侵入できる範囲を適切に規制するために，①侵入の対象，②侵入の方式，③侵入の期間(回数)[876]，を，令状の必要な記載事項として明記しておかなければならない。

---

872 陳瑞仁・新法捜索扣押 65 頁。

873 同前掲注 64 頁。

874 陳宏毅・刑訴法３版 199～200 頁。

875 新保 151 頁，小川 264 頁参照。

876 というのも，オンラインで侵入するには，常に試行錯誤を行う必要があるからである。言い換えれば，捜査機関が一回性処分を行うつもりであったが，一回で必ず対象にうまく侵入することができる保障はない以上，結局のところ，オンラインで侵入・探索する処分は常に継続性の捜査行為へと発展する傾向があるからである。

(2)侵害強度の制限

捜索における侵入の侵害強度に制限を設けるべきである。具体的には，(1)目的の優越性による制限と，(2)侵入による損失の程度に関わる制限が挙げられる。このうち，前者の制限は，探索という目的達成の利益は，侵入により侵害されうる法益よりも優越する価値を有しなければならないことを意味する。また，後者の制限は，侵入の手段の実施により侵害された法益の損失が原状回復できず，かつ損失の補償費用を金銭に換算すると巨額になると見られる場合は，目的の優越性という要件を満たしている場合であっても，当該手段の実施が認められないことを意味する。ここでいう「巨額」にあたるか否かは，国の年度税収を母数に，捜査の合理的な支出費用を概算したうえで，行政規則という形で，その実数を公告する。また，この実数は常に調整可能とする。

もっとも，この侵入による損失の程度に関わる制限には，次の２つの要件を同時に満たす場合に例外が認められる。第１は，「目的の絶対性」要件であり，これは，目的の優越性を満たすだけでは足りず，過去の事件の捜査の目的を遂行すると同時に，さらに，極めて重大な法益の保護又はかような法益の再度被害の防止の目的を達成するためである場合でなければならないことを意味する。第２は，「損失の完全補填」要件であり，これは，侵入により引き出された巨額の損失を完全に補填するための関連規定が用意されねばならないことを意味する。

(3)疎明義務

裁判官が，捜索の侵入の方式について，必要があれば，捜査機関に疎明を求めることができるとする規定を設けるべきである。捜査機関が裁判官の要求に応じないか，それとも，疎明を尽くさない場合には，捜索令状の発付請求を却下すべきものとする。

第２款　捜索の対象

捜索の対象について検討すべき問題点としては，侵入の可否及び探索の範囲という２点が挙げられるが，このうち侵入の可否については既に検討した。その内容を確認すると，次の４点が重要である。

第１に，情報システムの不可侵性という法益でいう「不可侵性」の有無を判断するための基準は，「ある情報システムにおいて，膨大かつ多様な情報が存在する可能性の有無」という点に求められる。

第２に，「ある情報システムにおいては膨大かつ多様な情報が存在する可能性」さえあれば，十分であり，当該システムにおいて実際に膨大かつ多様な情報が存在することは必要ではない。

第３に，「膨大かつ多様な情報が存在する可能性」が認められる情報システムは基本権

としての不可侵性を有するので，当該システムに侵入するためには「情報の捜索」令状を必要とする。

第４に，情報システム内の詳細が開示され始めた時点をもって，情報システムの不可侵性が侵害されたという。

以上をもとに，以下は，探索の範囲という部分の検討に入りたい。

Ⅰ．計画書方策の構築

本稿でいう「計画書方策」は，Winick が提案した第２段階の令状から示唆を得たものであるが，同じものではない。すなわち，この Winick の提案を台湾の場面に照らして説明すると，それは，コンピュータを対象とする場合に限定され，かつ，関連性を確認せずに蓋然性による差押えを行った後の捜索の範囲を限定するための令状であるのに対して，本稿でいう計画書方策は，その内実が，Winick の想定した内容に限られないものであるし，また，その適用範囲は，蓋然性により差し押さえた後の第２段階の捜索という Winick の想定した場面に止まらず，前出したリモート・アクセスやオンライン捜索などの新型の捜査手法にも対応するし，さらに，物理的な空間であっても，場所・サイズ基準が失効してしまう場合には，同方策を生かして対応することが可能である。

ところで，計画書方策とは，令状の請求者側からいう用語であるが，令状発付側からすると，それは計画書審査となる。審査を通過した場合，計画書の内容に基づいた令状が発付される。当該令状を，「計画書審査通過令状」という。

他方，計画書は，当然，計画書審査通過令状の一部になるものであるから，原則として，被処分者ないし関係者に呈示すべきである。しかし，捜査機関の申出により，裁判官が妥当と認めた範囲である限り，一部遮蔽したうえで呈示することができる。ただし，一部遮蔽した場合には，被処分者の即時異議ないし事後の不服申立ての権利をどのように担保するか，そして，捜査機関の執行の適正性をどのようにコントロールすることができるか等についての条件を付すべきである。

以上を前提に，以下では，アメリカの関連議論ないし判例を参考に，計画書の構成について述べる。

１．Winick の理論とその不十分さ

計画書方策は，基本的には，「捜査側が第２段階の捜索令状を請求するには関連性のある記録とそうでない記録とを選別するための『執行方式』を提案しなければならない」という Winick の２段階令状論の核心をなす部分を参考にするものであるが，彼の理論をそのまま採り入れることができないのである。というのも，Winick は，関連性のある記録を選別するための執行方式として，具体的には，①目的となる可能性のあるファイルをおおまかに一通り読む「ルック・スルー」（read through；look through）という方法，②キー

ワードを入力して捜索の範囲を限定する「キーワード・サーチ」（a key word search）という方法，③ファイルのタイプあるいはそのタイトルの特徴によって選別する「ファイルの特徴による検索（print out a directory of the title and file type）」という方法，の３つの可能性を挙げているが[877]，これについてのWinickの理論展開には次のような不十分な点があるからである。

(1)ルック・スルーとキーワード・サーチ

まず，Winick の挙げる３つの執行方式のうち，「ルック・スルー」とは，関連性のあるデータとそうでないデータとを選別するためにすべてのデータをクリックして大雑把にみてみることを意味する。それは，日本でいう「検証のための捜索」という概念に相当するものといえよう。

この点，前述した通り，日本において，検証のための捜索は，検証に必要な処分として認められる場合もあれば，そうでない場合もある。そして，それは，サーバー記憶媒体の場合においては，現行法上，認められてないという井上教授の見解は，学説上，多くの支持を得ているようにみえる。しかし，一般の電磁的記録媒体――個人パソコンやフロッピーディスクなど――が差押えの対象である場合には，必要な処分として，すべてのデータをクリックして大雑把にみてもよいという立場が主流であるようにみえる。

これに対して，Winickは，コンピュータ(個人用のPCであっても)にあるすべてのデータをクリックして大雑把にみてみることは許されず，ルック・スルーの適用の範囲を制限すべきであるとしている[878]。

そうすると，次に，具体的にどのようにルック・スルーの適用の範囲を制限することができるのかが問題となるが，Winick は，この点について明確に述べていない。Winick は，単に，第２の執行方式である「キーワード・サーチ」という方式の重要性を強調し，この方式によって関連情報と無関連情報とを選別することができるならば，コンピュータの中のすべての内容をルック・スルーすることは許されないと述べているだけである[879]。

(2)ファイルの特徴による検索

Winick が挙げた第３の執行方式である「ファイルの特徴による検索」は，コンピュータの中に異なるフォーマットで多様な情報が保存されている場合に，ファイルのタイトルあるいはタイプ（例えば，拡張子）という特徴によって，目的とする情報を捜し出すという方式を指す[880]。具体的には，例えば，仮に捜索の目的物が財務記録であるならば，電話リストというフォーマットのファイルを捜索することは許されないとされる[881]。

---

[877] Winick, at 111.
[878] Id. at 107～108.
[879] Id.
[880] Id.
[881] Id.

この方式によって，目的とするファイルをある範囲で特定することは簡単であるため，実務上しばしば利用されてきているが，しかし，拡張子やファイルの名前を改ざんすることは容易であるし，またそれらと中身との間には必ずしも関連性がない場合もあるから，捜査の実効性を害することがある[882]。

そこで，Winick は，ファイルの特徴による検索方式で捜索の範囲を限定することができない場合には，治安判事は警察側の提案した他の捜索の方式を審査しなければならないと述べている[883]。しかしながら，Winick は，ここでいう他の捜索の方式とは，具体的に何を指すのかを明言していない。

２．Winick の理論の判例上の実現とその問題点

このような Winick の理論を取り入れたのが，CAREY 判決[884]と ILLINOIS 決定[885]である。

(1)CAREY 判決―「閉められた容器」保護例外について

CAREY 判決[886]は，薬物乱用事件で令状によりコンピュータデータを捜索している過程で発見した児童ポルノの画像をダウンロードしたという捜査官の行為が，令状に認められた捜索範囲を超えた違法な捜索であるかという点が争点になった事案である。この争点を巡る法理論上の重要な問題点としては，A. 当該捜索行為は，違法な別件捜索にあたるか，B. 同意捜索の範囲はコンピュータの中のファイルに及ぶのか，という２つの点が挙げられる。

A. 「一番目の JPGファイルのクリック」基準

CAREY 判決は，「ファイルの内容のいずれもが偶然に発見されたものであるので，プレイン・ヴュー法理によれば，違法な別件捜索・差押えにはならない」という警察側の主張を採用しなかった[887]。

同判決は，警察が「一番目の JPGファイル」をクリックして児童ポルノを見たことは偶然

---

[882] Id. 同じ指摘として，Kerr, DIGITAL WORLD, at 545。

[883] Id., at 108.

[884] CAREY, supra note 416.

[885] ILLINOIS, supra note 418.

[886] Supra note 416 . 本件の概要は次の通りである。警察官が，麻薬販売の疑いを受けた被告人を令状逮捕した後，被告人の同意を得て被告人のアパートを捜索していた際に，麻薬販売に関する記録が保存されている可能性のある２台のコンピュータを発見した。この２台のコンピュータを警察署に持って帰った後,「規制薬物の販売と配布に関連する名前，電話番号，元帳，金額，アドレスと他の証拠書類を発見するためにコンピュータのファイルを捜索することができる」という内容の捜索令状によって，コンピュータの中のファイルを検索していたところ，性的暗示のタイトル付き JPG 形式のファイルに気付き，その中の１つをクリックしてみると児童ポルノであることがわかった。警察官は，この１つのファイルにとどまらず，他の JPG 形式のファイルをも１つずつクリックし，ダウンロードした。警察側は，各々のファイルをクリックしてみる前にはその中身を知ることができないし，本件の児童ポルノの発見は完全に偶然によるものであるから，プレイン・ヴュー法理の適用が認められるはずであると主張した。原審では警察側の主張が認められ，被告人の証拠排除の主張が却下された。しかし，上訴審は，原審の判決を破棄し，被告人の主張を認めた。上訴審で主たる争点となったのは，JPG 形式のファイルをクリックしたり見たりした警察の行為が令状で許された捜索の範囲を越えるものであるか，という点にある。

[887] Id., at 1272～1274.

による発見といえるとしても，それにより，それが本件薬物乱用捜査と関係ない児童ポルノであることが判明したのに，さらにその他の同じ JPG形式である複数のファイルを開けた行為には，薬物乱用関連データでなく児童ポルノを探したいという警察の意図が表れているとし，それらの画像は，閉じられたファイルに保存されていたもので，プレイン・ヴューの状況にはないとした[888]。

本件により示された最も重要な示唆は，「一番目のJPGファイルを見た後，それが本件薬物乱用捜査と関係ない児童ポルノであることが判明したのに，さらにその他の同じ JPG形式である複数のファイルを開けてはいけない」という判示部分にある。というのも，この点は，本判決が，ITシステムの場合には，閉められた容器保護原則とその例外の適用がないとする Winick と同様の立場に立ったうえで導かれた結論だと思われるからである。

すなわち，従来の閉められた容器保護原則とその例外によると，閉められた容器全体を捜索してもよいとされるので，閉められた容器であるコンピュータに蔵置されたすべての閉じられたファイルをクリックしてみてもよいことになる。これに対して，Winick の理論によれば，コンピュータは閉められた容器でなく，捜索すべき仮想的な場所であるから，その場所に置かれた閉じられたファイルを閉められた容器と観念することができ，そこから，上記の結論が導かれるのである。

そして，Winick の理論と近い立場から導き出された上記の結論は，プレイン・ヴュー法理の適用範囲を制限する意味をもつものと考えられる。

すなわち，アメリカ連邦最高裁は，HORTON 判決[889]において，修正４条の保護法益は捜索と差押えでは異なり，前者はプライバシー権にあり，後者は財産権にあるとした。そのうえで，プレイン・ヴューの場合には，他の犯罪に関する証拠が既に合法的な捜索の過程中に捜査官により発見された以上，その後の観察ないし差押えによって新たなプライバシーの侵害・制約は生じず，侵害されるのは，証拠物の所持者のこれに対する支配権限のみであるとする[890]。そのうえで，HORTON 判決は，プレイン・ヴューの範囲は「場所・サイズ」基準により制限されているから，一般的・探索的捜索・差押えの問題は生じないとした[891]。しかしながら，ここで問題となるのは，バーチャル空間においては，一定のサイズ・特定の場所という概念がないに加え，デジタルデータは，クリックしてみないとその中身と被疑事実との関連性の有無を判断することができないことから，結局のところ，バーチャル空間における捜索・差押えの場合にも，HORTON 判決が示した従来のプレイン・ヴュー法理をそのまま適用すると，すべてのデータが既に合法的な捜索の過程で捜査官により発見されたといえるので，無制限で捜索・差押えできるに等しいことになるという点である[892]。こ

---

[888] Id.

[889] TERRY BRICE HORTON, PETITIONER v. CALIFORNIA. 496 U.S. 128 (1990).

[890] Id, at 133～135. 酒巻・緊急差押 439～440 頁をも参照。

[891] HORTON, id, at 146～142. HORTON 判決では，一般的・探索的な捜査活動の防止は，当初の捜査官の立入り・捜索がその範囲を特定・明示した令状により限定されるか，または緊急性を理由とする適法な無令状捜索の範囲内に限定されることによって達成することができるとされた。

[892] Kerr, DIGITAL WORLD, at 568～569.

の意味で，CAREY 判決が示した法理は，プレイン・ヴュー法理の適用範囲を制限するといえるのである。

ここから，台湾の議論についても重要な示唆が得られよう。すなわち，アメリカでいうプレイン・ヴュー法理を内容とする現行の台湾刑訴法 137 条 1 項は「検察官，検察事務官，司法警察官あるいは司法警察は捜索あるいは差押えを執行するときに，捜索令状に記載されていない本件の差し押さえるべき物を発見する場合，それをも差し押さえることができる」と定めており，ここでの検討から得られた「一番目の○○類型のファイルをクリックしてみた後関連性のないデータが判明された場合，一番目の○○類型のファイル以後の同類型のファイルをクリックして見てはいけない」という示唆が，この規定の適用上の制限として考えられる。それにとどまらず，この制限は，情報に対する捜索令状における１つの非物理的な限定要素にもなりうると思われる。

B. 同意捜索の範囲――物理的な空間とバーチャル空間

次に，CAREY 事件において，警察側は，プレイン・ヴューの主張の他に，複数の JPGファイルをクリックして見た行為を別件捜索と解されるとしても，それは被告人の同意により行われたものであるから，修正４条によって認められる適法な令状によらない捜索であると主張した[893]。この主張も裁判所は採用しなかった。判決は，被告人はアパートの捜索・差押えに同意したが，その同意の範囲は有体物のコンピュータのボックスには及ぶが，その中の無体物のファイルに及ばないとした[894]。

本判決は，その理由付けとして，同年の Turner 判決[895]を引用したうえで，物理的な証拠への捜索・差押えの同意の範囲は非物理的な証拠に及ばず，本件の被告人の同意は明らかに物理的な範囲にとどまるものであった以上，本件の複数の JPGファイルをクリックしてみた捜索行為は被告人の同意の範囲を超えた違法な捜索であるとした[896]。言い換えれば，「物理的な空間」である場所に対する同意捜索の効力は，「仮想的な空間」である ＩＴシステムに及ばないというのが CAREY 事件の法廷意見である。

以上により，台湾の立法論についても有益な示唆が得られる。すなわち，令状制度の在り方としては，「物理的な空間」（例えば，住居などの場所）と「仮想的な空間」（例えば，コンピュータの ＩＴシステムなど）とを区別すべきであると考える。

そして，この考え方の実益としては，捜索場所に置かれた物は，原則として，その場所の概念の中に含まれるという台湾における通説の理解と異なる，「捜索場所に置かれた電磁計算機などの『物理的な空間と独立した保護を享有する情報システムの不可侵性をもつ媒体』であるならば，原則として，場所の概念の中に含まれず，当該『場所に対する捜索令状』によって，当該媒体を捜索することができない」という帰結を導き出すことができ

[893] CAREY, supra note 416, at 1274.
[894] Id.
[895] United States v. Turner, 169 F.3d 84, 1999 WL 90209 (1st Cir. Feb.26, 1999).
[896] CAREY, supra note 416, at 1273.

る点が挙げられよう。

(2) ILLINOIS 決定――「捜索実施要綱」について

ILLINOIS 決定の概要は次の通りである。令状発付の審査裁判所は，警察側に「捜索実施要綱」(search protocol)の提出を求め，当該要綱の提出はコンピュータに対する捜索の令状発付の必要条件であるとした[897]。この要綱の具体的な構成は，①特定性（コンピュータの中から差し押さえようとする情報を特定すべきであること），及び②選別性（捜査で用いる予定のコンピュータデータの発見方法は，捜査対象の犯罪事実と無関係の他の情報も含めて検視する一般的・探索的な情報検索ではないこと）という２つの要素からなるものである[898]。

これに対して，捜査側は，裁判所が，コンピュータ・ファイルを検索する行動を規制することはできないという理由で，裁判所からの捜索執行要綱の提出という要求を無視した[899]。それに対し，本決定は，政府側が捜索執行要綱を提供しないことを理由に，令状の発付の請求を却下した[900]。法廷意見は，前記の CAREY 判決を含めたいくつかの先例を下敷きにし，コンピュータへの捜索の場合は，「混雑性」という特徴を有するので，このような場合には，令状の「特定性」の要件を特に重視すべきであるとした上で，こういった捜索執行要綱を要求する権限を裁判所が持っていることを確認し，令状の発付に捜索執行要綱という特別なアプローチを必要とすると判示した[901]。

本決定について法理論上検討すべき問題点としては，A. 令状発付の審査裁判所に捜索執行要綱の提出を求める権限があるとする根拠は何なのか，B. 捜索執行要綱を必要とする令状の発付要件は何なのか，という２点が挙げられる。

A. 捜索執行要綱の必要性ないし可能性について

本決定によると，令状を発付する裁判官に捜索執行要綱の提出を求める権限を付与する根拠は，捜索執行要綱の必要性ないし可能性に求められる。その具体的な論拠としては，次の３点があげられる。

第１に，コンピュータへの捜索・差押えは現場での実施に困難をきたす場合が少なくなく，関連性のある記録と関係性のない記録とを選別せず，一時的・一括的な差押え(日本でいう蓋然性による差押え)を認めざるを得ないので，その後の捜索を捜索執行要綱により規制する必要性がある[902]。というのも，蓋然性による差押えの場合には，従来の令状に要求される特定性・関連性という２つの要件が従来通りの程度では機能しないため，差し押さえ

---

[897] ILLINOIS, supra note 418, at 954.
[898] Id.
[899] Id., at 955～956.
[900] Id., at 957～958.
[901] Id.
[902] Id., at 958～959.

た後の捜索の範囲を限定しないと，修正４条の従来の保護の程度が低減されることになるからである。それゆえ，修正４条の従来の保護の程度を維持することが，令状を発付する裁判官にとって譲れない責任であるとすれば，裁判官には捜索執行要綱の提出を求める権限があると解することができよう。

第２に，従来，執行事項は現場での捜査官の判断に任せるべきであるとされてきたが，コンピュータの特徴に鑑み，コンピュータへの捜索に対しては高度の保護を与える必要があるため，捜索執行要綱により保護する必要性がある[903]。なぜならば，現在のコンピュータ技術の発展に伴い，家庭用のパソコンであっても驚異的な量の情報を有し，無関係の個人情報も捜索・差押えを受ける危険性が一層高くなることに鑑みると，コンピュータの中に被疑事実と関連性のある記録が存在すると信じる正当な理由があるとしても，当該コンピュータが本件犯罪にしか使われていないと証明することができる証拠がない以上，被告人の合法的な活動に関する記録も含むことは否定しがたいため，捜索執行要綱の提出が必要である[904]。

第３に，捜索執行要綱の可能性について，本決定は，情報の量の膨大性と混雑性という特徴からデータをすべてプリントアウトする可能性がなく，またタイトルからみて犯罪に関わるデータであることがすぐわかるとも限らないとし，前述の CAREY 判決を引用したうえで，日付やキーワード・サーチあるいはファイルのタイプの指定などのツールによって，捜索の範囲を限定することができるとした[905]。

以上の通り，第１と第２の点からは，令状を発付する裁判官には捜索執行要綱の提出を求める権限があり，そして，第３の点からは捜索執行要綱を提出することが可能であるといえる。このようにして，ILLINOIS 決定は，裁判官には，捜査側に捜索執行要綱の提出を求める権限があるとすると同時に，捜査側は捜索執行要綱により捜索の範囲を限定する義務を負わなければならないと結論付けたのである。

B. 特別コンピュータ令状発付の要件

ILLINOIS 決定が示した捜索執行要綱を必要条件とする特別コンピュータ令状は，Winick の理論に基づくものであるとはいえ，同決定は，Winick が提案した第２段階の令状よりもより厳しい令状発付の要件を要求している。具体的には，ILLINOIS 決定は，Spilotro 事件[906]を引用した上で，本件令状（特別のコンピュータ令状）を発付するときに下記の３点を考慮しなければならないとした。

第１は，令状に明記された一定のタイプの「すべての記録」を差し押さえる「正当な理由」が存在するかである[907]。これに対して，Winick は，「正当な理由」は不要であり，合

[903] Id.
[904] Id.
[905] Id.
[906] United States v. Spilotro, 800 F.2d 959 (1986) at 963.
[907] ILLINOIS, supra note 418, at 959～960.

理的な理由さえあればよいとし，そして，その範囲も，すべてでなく一部の記録のみでよいとしている[908]。

第２は，警察側が，差し押さえるべき関連記録とそうでない記録とを区別することができる客観的な基準を示したかである[909]。これに対して，Winick は，単に，関連性のある記録と関連性のない記録とを選別することができる捜索の執行方式を提案しなければならないと述べているだけであり，客観的な基準までは要求していないと思われる。

第３は，警察側が，令状の発付の時点で，証拠として利用できる情報と考えている差し押さえるべき対象をより一層特定して示すことができるかである。これに対して，Winick は，単に，①証拠存在の蓋然性，及び②関連性のある記録を選別するための執行方式の提案という２つの要件を挙げているだけであり，特定性を特に要求していないと思われる。

以上３つの点を総合勘案した本件の審査結果は，当該コンピュータの中には当該犯罪に関する情報しか存在しないとは限らず，かつ，政府は特定性を充たす執行要綱を提供する能力を有するのに，関連のある記録と関連のない記録を区別することができる客観的な基準を提供しないことを指摘して，本件は執行要綱が提供されておらず令状を請求する政府の行為は修正４条の特定性の要件を充たさないので，令状請求を認められないとした[910]。

しかし，本決定は，政府が特定性を満たす執行要綱を提供する能力を有しない場合に，どう処理すべきなのかという点については明らかにしておらず，このような場合にも，依然として，「捜索執行要綱」を提出することを必要とするかという疑問点が残されている。

３．計画書方策の内容

以上をもとに，以下では，本稿が提案する計画書方策の内容を具体化する。

(1)Winick の理論の不十分さの改善策

Winick の理論の不十分さは，以下の３点にまとめられる。

第１に，具体的な執行方式として，Winick は，①ルック・スルー，②キーワード・サーチ，③ファイル・タイトルという３つのものをあげている。しかし，この３つの方式は，いずれもローテクであって，関連性のあるデータを割り出す保証はないという点が問題である。

第２に，上記の①について，Winick は，コンピュータにあるすべてのデータをクリックして大雑把に見てみることはできず，ルック・スルーの適用の範囲を限定すべきであるとするものの，具体的にはいかなる限定をすべきかについては明確でない。

第３に，Winick 自身も，上記の２つの問題点を意識しており，これらの方法で捜索の範囲を限定することができない場合には，治安判事は警察側の提案した他の捜索の方式を審

---

[908] Winick の第２段階令状の発付要件における「蓋然性」というのは，「何らかの理由でそのように信じる（any reason to believe)」というレベルに達すれば十分とされる(Winick, at 108)。

[909] ILLINOIS, supra note 418, at 959～960.

[910] Id., at 962～963.

査しなければならないと述べている。しかし，ここでいう「他の捜索の方式」とは，具体的に一体何を指すのかについて，Winick は明らかにしていない。

以上の３点については，以下のような対応をとるべきだと考えられる。

A. 非物理的な限定要素

まず，この章の第２款で述べた法益論に照らせば，非物理的な空間とは，Winick が想定したコンピュータにおけるＩＴシステムより広い概念である。具体的には，ＩＴシステムというようなバーチャル空間がそれにあてはまるのはもちろんのこと，大量の書類(例えば，会計帳簿)における体系的な構成の情報の集合体をも含む。

このような非物理的な空間においては，物理的な要素に依存しないため，物理的な空間ないし探知しようとする情報を記録した媒体の物理的な特徴により捜索の範囲を画定するのは不可能である。しかし，①捜索の対象とする情報システムの技術的な特性，②利用しようとする侵入・探索ツールの技術的な特性，③探知の対象とする情報及びこの探知に伴いやむを得ず開示されうる探知の対象でない情報の範囲と性質，という３種類の非物理的な要素により，非物理的な空間である情報システムにおける捜索の範囲を画定することが可能であろう。そこで，具体的な執行方式として，この３つの非物理的な限定要素を提案したい。

このように，本稿の提案と Winick のそれとを比較すると，Winick の提案は，上記の②のカテゴリーのみに言及し，かつ，ローテクのツールをしか挙げていない。そこで，次に検討すべきは，ハイテクのツールとしては，具体的にいかなるものが挙げられるのか，また，①と③の具体的な中身は何なのかという２つの問題である。これらの点は，「C. その他の捜索の方式の具体化」において後述する。

B. ルック・スルー範囲の限定の在り方

次に，ルック・スルーの部分を検討すると，その範囲を画定するためには，次の２つの基準が考えられる。

(A)類型化データによる限定基準

まず，前掲の CAREY 判決が打ち出した基準により，次のようにルック・スルーの範囲を画定することが可能であろう。

すなわち，令状に記載された「〇〇類型のデータ」ではあるが，一番目の〇〇類型のデータをクリックしてみたところ，関連性のないデータと判明した以上，デジタルデータの場合には，クリックしてみないとその中身と被疑事実との有無を判断することができないという前提が破られたから，同類型のデータをさらにクリックしてみていく必要性を否定することにより，ルック・スルーの範囲を画定することができるわけである。これを，「類型化データによる限定基準」と呼ぼう。

これに対しては，拡張子などのデータの類型化の特徴を示すものは改ざんしやすいものであって，いくら類型化に工夫を尽くしたとしても，令状に明記された類型化データ以外のデータに証拠となる情報が存在する可能性があることは否定できないので，類型化データによる限定というような提案は不合理ではないかという批判がありうるかもしれない。

しかし，こうした可能性を支える具体的な根拠がある場合には，これから述べるいくつかの方法を組み合わせることにより対応すればよく，かつそうすべきと思われるから，類型化データによる限定基準を採用しても，捜査に大きな支障をもたらすことはない。

(B)露出されたデータによる限定基準

ルック・スルーの範囲を画定するにもう１つの方策を，Kerr が提案している。すなわち，彼は，ＩＴシステムにおいては，一定のサイズ・特定の場所という概念がないため，すべてのファイルに証拠となるデータが存在する蓋然性があるといえるから，すべてのファイルをクリックする合理性が認められるので，結局のところ，何でもプレイン・ヴューの状況にあたることになってしまい，デジタル証拠に対する一般的捜索が認められるに等しいと指摘する[911]。そのうえで，コンピュータに対する捜索令状が一般令状にならないようにしなければならないとし，そのために，いわゆる「露出されたデータによる限定基準」を打ち出すと同時に，バーチャル空間においてプレイン・ヴュー原則の適用を廃止することが，そのための最善策であるとしている[912]。

この「露出されたデータによる限定基準」とは，ＩＴシステムを，情報を保存する仮想の広い倉庫とみなしたうえで，人間の観察に晒されていないデータを露出させることは，プライバシーの侵害になるから，捜索にあたるのに対して，あらかじめ露出したデータを観察することは，プライバシーの侵害にならないから，捜索にあたらないことを意味する[913]。そして，この基準により，いかなる形で，ルック・スルー範囲を限定することができるかについて，Kerr は次のように述べている。

コンピュータ機器という有体物を基準とすると，同一のコンピュータの中のすべてのデータを見ることができることになり，また，ファイルを基準にすると，同一のファイルの中のすべてのデータを見ることができることになるので，これらの基準は，いずれも，妥当ではない[914]。これに対して，露出されたデータを限定の基準とすると，同じファイルの中にあっても，露出していない関連性のない部分を見てはならないから，それは，捜索の範囲を限定するためのより良い基準となる[915]。そして，露出されたデータの具体例としては，例えば，既にモニターに映っているデータ，あるいは，自動的にモニターに映るデータ[916]な

---

911 Id., at 537, 565～566, 576ff.

912 Id.

913 Id., at 548, 552, 554～556.

914 Id., at 556～557.

915 Id.

916 システムの設定により，電源を入れると，自動的に起動する場合がありうる。例えば，Skype あるいはMSNなどの自動ログインの機能を考えると直ぐ分かろう。こうした機能が設定されていた場合，Skype のSNSのメッセージ

どが挙げられる。

そのうえで,Kerr は,露出されたデータによる限定基準により規制しようとする対象は,「人間の観察」であるから，コンピュータの全体に対してプログラムによる「自動徹底検索」を行う場合には，情報が人間の観察に晒されることはなく，プライバシーに対する侵害が軽微であるので，露出されたデータによる限定基準に反しないとし，それゆえに，自動徹底検索によって捜索の範囲を縮小した上でルック・スルーを行うべきであると述べている[917]。

Kerr の見解をまとめると，①露出していない部分(データ)をさらに見ることは許されないこと，及び②プログラムによる自動徹底検索技術を用いてルック・スルーの範囲を縮小すべきであること，という２点が重要である。

C. その他の捜索の方式の具体化

最後に，これまで述べたような捜索の方式以外のものとして，ハッシュ関数による選別技術というハイテクツールをとりあげる。

ハッシュ関数とは，一方向不可逆性ハッシュ関数とも呼ばれ，デジタルデータをある関数に入力した結果として出力される，短い固定の長さの値を意味する[918]。ハッシュ関数は，ハッシュ値から元のデータを復元するのが不可能であること(いわゆる「一方向性・不可逆性」)，及び異なるデータから同一のハッシュ値が作成される可能性がきわめて低い，ないし科学理論上は不可能であること(いわゆる「唯一性」)の２点によって特徴付けられる[919]。この意味で，ハッシュ関数は「電子指紋」とも呼ばれる。

このような一方向性・不可逆性と唯一性をもつハッシュ関数技術を使うと，ハイテクのレベルで同一性を鑑別することができると同時に，精密な選別を行うことも可能になる。後者の機能につき，アメリカの学者 Salgado は，有用なものを残させ，無用なものを排除することができる仕組みと述べている[920]。この機能を,篩い落とし機能と呼ぶ。Salgado は,このハッシュ関数の篩い落とし機能により「限定性」(対象となる情報しか開示しないことを意味する)を確保することができるから，いわゆる「法禁物の合法的発見法理」を示した CABALLES 判決[921]をハッシュ関数の場合にも適用することができると主張している[922]。

あるいは，MSNのメッセージは，当然捜査官の目に入ることになる。

[917] Kerr, DIGITAL WORLD, at 552.

[918] Kerr, DIGITAL WORLD, at 541, 546; Salgado, at 38～40；e ドキュメント 60 頁も参照。

[919] e ドキュメント 51，60～61 頁参照。

[920] コンピュータの鑑識分析を行う際に，アナリストは，膨大な量のデータの中から，有用なデータを取り出したり，無用なものを除いたりしなければならない。その際，ハッシュ関数による選別技術により，自動かつ精密的な選別が可能とされる。その具体的な稼動につき，ソート・メカニズム (Sort mechanism)と呼ばれる手順を行ったうえでハッシュ関数を使うと，データの検索範囲を最小化させるという仕組みになる。ソート・メカニズムとは，コンピュータデータを特定の順番で並べ替えることを意味する。(以上の説明につき，Salgado, at 40～41 を参照されたい)。

[921] Petitioner v. ROY I. CABALLES, 543 U.S. 405 (2005).本件の概要は次の通りである。連邦最高裁は，よく訓練された麻薬発見犬を使用すると，人々の目から隠されたままである「非密売・密輸品」を露出させることなく,「密売・密輸品」(麻薬)だけをみつけることができ，さらに，適法な交通検問の間になされたものである以上，かかる政府行為は正当なプライバシーの利益の侵害ではないので，修正４条に反しないと判示した。

法禁物の合法的発見法理とは，①不法性（捜索の対象であるアイテムが法禁物であること），及び②限定性（捜索により発見されうるのは法禁物に限られること）という２つの要件を満たす場合に，開示されうるのは，法禁物や犯罪に関わる情報のみであるため，正当なプライバシーの利益は侵害されていないという原則をいう。

Salgadoによると，データの全体を対象としハッシュ関数をかけて徹底的な自動走査・検索を行う場合にも，法禁物の合法的発見法理が適用されるから，一般的・探索的捜索にはならない[923]。というのも，こうした場合は，ハイテクのハッシュ関数の篩い落とし機能により開示されうるのは，対象となるデータに限られるからである。

しかしながら，Salgadoの理論には次の２つの問題がある。第１に，ハッシュ関数の篩い落とし機能を利用する際には，システムの中にあるすべてのデータをスキャン(自動走査)しておくという仕組みになっているとすれば，ハッシュ関数の使用は必ずしもCABALLES判決の麻薬発見犬の使用と同じでないと思われる。というのも，犬が臭気を嗅いだだけでは何も保存されないのに対して，ハッシュ関数検索を利用する場合，スキャンされたデータはハッシュ値の(自動)照合を行うために一時的な蓄積がなされ，一般には，照合が終わったら直ちにデータを削除し保存しないという設定になっているが，削除せずに保存するように設定することも可能だからである。第２に，犯罪にかかわる情報だからといって，直ちにそれを法的の保護から除外されるわけでないとすれば[924]，法禁物の合法的発見法理の理論上の適切性は疑問視すべきであろう。

以下では，以上の２点について，情報の差押えと情報の捜索との２つの場面に分けて検討を行う。

(A)情報の差押えの場面

前述した通り，一時的な保存(蓄積)であっても，情報の差押えにあたるが，情報に対する「一瞬の取得(保存・蓄積)」という場合には，情報の差押えに当たらない。それゆえ，ハッシュ関数の篩い落とし機能を利用する際に，スキャンされたデータが保存されると同時に削除されたことを，技術及び法の両面で確保することさえできれば，すべてのデータをスキャンしても，情報の差押えに当たらないから，一般令状禁止原則に反しないと解することができる。なぜならば，こうした場合には，情報の終局的処分権に対する侵害にならないからである。

(B)情報の捜索の場面

情報をスキャンすることは，情報の終局的処分権の侵害にならず，情報の差押えに当た

---

[922] Salgado, at 45. ハッシュ関数は唯一性と一方向性の特徴を有するから，ハッシュ値のセットが正しければ，その「篩い落とし」機能の理論上の正確性が百パーセントともいえようが，もし，値が正確ではないなら，ハッシュ技術を使ったとしても，目的のデータとそうでないデータとを正確に選別することができない。

[923] Salgado, at 46.

[924] 井上・電話逆探知 497 頁＝井上・強制・任意 206～207 頁。

らないとはいえ，スキャンは，情報システムの不可侵性という法益を侵害するものであるから，情報の捜索に当たる。というのも，捜索の場合においては，単一のデータに対するスキャンは一瞬といえるが，自動徹底検索技術の利用は，往々にして，膨大な量のデータに対して無選別的・連続的にスキャンしていくという仕組みになり，この仕組みは，一瞬ではなく，長時間かかることになるので，それを「侵入すると同時に退出する」とはいえず，それによって情報システムの不可侵性という法益が侵害されることになるからである。

そこで，次に検討すべきは，膨大な量の情報(例えば，データ)に対して無選別的・連続的に検索(例えば，スキャン)していくことは，一般令状禁止原則に反する情報の捜索に当たるかどうかである。

この点，前述した通り，一般令状禁止原則の根拠は，中華民国憲法23条の比例原則から導かれた最小化原則に求めるべきである。この理解によれば，2001年に導入されたいわゆる令状主義における特定性ないし関連性要件は，この憲法上の最小化原則を具体化したものにすぎず，捜査ツールの高度(精密)な選別機能により，対象となる情報しか開示しないことが保障され，その実質的な保障の程度が有体物を対象とする伝統的な家宅捜索の場合に要求される保障の程度を下回らないと評価できる限り，膨大な量のデータに対して無選別的・連続的にスキャンすることは，同23条から導かれた最小化原則を核心とした一般令状禁止原則に反するものではないと解することができる。

例えば，前述した麻薬犬による臭気選別やハッシュ関数による選別などの捜査ツールを使う場合，犬が臭気を嗅いだり，プログラムがデータをスキャンしたりするに際して，捜査官は，犬が嗅いだ臭いを感じることができないし，プログラムがスキャンしたデータを見ることもできない。また，犬が臭いを嗅いだだけでは何も取得されていないし，プログラムによりデータがスキャンされると同時に削除されるという仕組みになっている限り，事後的にはデータを見ることもあり得ない。こうした場合には，無関係のデータは，実際には，捜査機関の観察に晒されていないということができよう。この意味で，中華民国憲法23条の最小化原則から導かれた一般令状禁止原則に反しないものといえる。

このように，高度(精密)な選別機能を有する捜査のツールの使用は，形式的には，それにより大量の情報に対して無選別的・連続的に検索していく仕組みになるが，実質的には，捜査機関の観察に晒されうるのは，対象となる情報のみであるので，中華民国憲法23条の最小化原則を満たしており，一般的・探索的捜索にならず，立法論的には，同条に基づき明文化される「情報の捜索」令状が発付される限り，合法的に行うことができるのである。

(2)最小化の方策

以上により，最小化の在り方を考えると，次の３点が重要である。

A. バーチャル空間と物理的な空間との共通性

非物理的な空間における捜索の範囲を最小化するための方策としては，「最小化方法に

関する計画書」の提出が挙げられる。この方策は，物理的な空間であっても，物理的な限定要素ないし基準の意味が薄くなる場合には，適用することが可能である。

B. 非物理的な最小化のための前提と限定基準

上記の計画書において具体的にいかなる非物理的な最小化の方策が用意されているかを，ここまでの議論をも踏まえて確認すると，次のようになる。

第１に，「関連性＝蓋然性」という構造の内在的制約を前提とすることである。すなわち，非物理的な空間ないし非物理的な情報を処分の対象とする場合，その憲法上の根拠は，一般令状禁止原則を示す中華民国憲法 23 条に求められる。この場合には，そのための最小化の手段を，立法者が無体の情報並びにそれが存在する仮想なバーチャル空間の特徴に応じて自由に選択できるが，その際には，伝統的な家宅捜索の場合でいう令状主義(または令状原則)が要求する関連性(＝蓋然性)という要件により基本権に対して提供された保護の内容ないし程度が縮減することはないという保障を，法により実質的に担保しなければならない。

第２に，非物理的な限定基準としては，①類型化情報による限定基準，②露出された情報による限定基準，③情報・情報システムに対する一瞬の取得・侵入の場合は基本権の侵害にならない基準，という３つのものが挙げられる。

C. 捜索・差押えの共通性

計画書方策は，捜索すべき範囲を最小化するための対策であると同時に，差し押さえるべき範囲を画定するための基準にもなる。というのも，前述した通り，蓋然性による差押えのように捜索の性格をもつ差押えの類型もあるし，捜索という制度の主な目的は差し押さえるべき物ないし情報を発見することにあるから，捜索すべき範囲が画定されれば，それと同時に，差し押さえるべき範囲も画定されることになるからである。

この意味で，蓋然性による差押えという問題を解決するための３段階の令状規制に関していうと，計画書方策は，捜索すべき範囲を最小化するための方策であるから，第１段階の蓋然性を確認するための捜索，及び第３段階の蓋然性による差押え後の捜索の範囲の制限に対応するものになるが，立法論としては，第２段階の蓋然性による差押えにも準用する可能性がある。

(3)記載すべき事項

計画書には，①捜索対象についての描写，②捜索方式についての描写，③利用目的の限定，④危険性の評価及び安全措置の効果，の４つの事項を記載すべきである。それぞれの具体的な中身は次の通りである。

A. 捜索対象についての描写

捜索対象についての描写とは，主に，「捜索の対象とする情報システムの技術的な特性」と，「探知の対象とする情報及び探知に伴いやむを得ず開示されうる探知の対象でない情報の範囲と性質」の記載を意味する。

具体的には，まず，当該情報システムの系統的構成，その上層管理者と下層管理者，開放性と閉鎖性などについての技術的な属性を描写しなければならない。これらの描写により，対象とするシステムとそうでないシステムとを区別する。

そのうえで，探知の対象とする情報についての技術的ないし内容的な予測を描写しなければならない[925]。このような予測に基づき，当該情報を割り出すために，発受信源，蔵置位置，伝送経路やデータの作成(保存)日付の特定ないしその他の指定要素により，ＩＴシステムなどの捜索対象について捜索できる範囲を限定しなければならない。このような限定ができない場合に，自動徹底検索技術の使用を請求しようとすれば，当該技術の使用により，「情報・情報システムに対する一瞬の取得・侵入の場合は基本権の侵害にならない」という非物理的な限定基準が満たされているといえる理由及び高度な選別機能による限定性を有する捜査のツールであることを明示しなければならない。

他方，探知に伴いやむを得ず開示されうる探知の対象でない情報の範囲と性質を具体的に示したうえで，これらの情報は仮に開示されたとしても，その他の態様での継続的な侵害の蓋然性がないことを技術的・法的に担保することができる点をも説明しなければならない。

B. 捜索方式についての描写

捜索方式についての描写とは，主に，「利用しようとする侵入・探索ツールの技術的な特性」，及び，このようなツールの使用と，前述した「捜索対象についての描写」との繋がりを説明しなければならないことを意味する。そのうえで，利用しようとする侵入・探索ツールが「限定性」を有すること[926]を担保しなければならない。このような担保が技術的に有効といえる理由をも明示しなければならない。

C. 利用目的の限定

利用目的の限定とは，取得しようとする情報をどういう目的に利用しようとしているか

---

[925] ここでいう「技術的な予測」とは，一定の根拠に基づき，目的の情報の技術的な特徴(例えば，「拡張子」，「ファイル名」，「データに付加されたパソコンが記録した作成者の識別ＩＤ」など)を予測しておくことを意味する。例えば，目的のデータが児童ポルノである事例では，その拡張子は，一般には，「jpg.」になる。また，「内容的な予測」とは，一定の根拠に基づき，目的のデータの内容的な特徴を予測しておくことを意味する。これは，主に，Winick の提案したキーワード・サーチの場合に用いられる。例えば，ネット上の誹謗中傷捜査事件において，被疑者のコンピュータの中から誹謗中傷の内容を記録したドキュメントを捜そうとすれば，「被害者の名前」，「誹謗中傷の記事に書かれた人名，地名，時間」などが，目的のデータ(ドキュメント)の内容的な特徴としてあげられる。

[926] ここでいう捜索ツールとは，高度の篩い落とし機能を有する検索ツールをさし，それにより対象となる情報しか開示しないことが技術的に保障されることを，(捜索ツールの)限定性という。

を説明しなければならないことを意味する。その場合，「本件犯罪の成立を立証するために」というような抽象的な記載では足りず，どのような被疑事実を，どのように立証するために用いられるについての簡要な説明を必要とする。その他の捜査目的に役立つという場合には，具体的に，どのような捜査目的のために，どのように役立つのかについての簡要な説明を必要とする。

D. 危険性の評価及び安全措置の効果

「捜索方式についての描写」の部分で明記した「侵入・探索ツール」の使用により，捜索の対象とする情報システムないしその他のシステム，及び探知の対象とする情報ないしその他の情報に損害を与える危険性の有無を具体的に記載しなければならない。また，危険性が生じうる確率及びそれを防ぐ安全措置の可能性を明示しなければならない。

また，「侵入・探索ツール」の使用により，第三者に便乗される危険性の有無及びそれを防ぐための対策も明記しなければならない。

Ⅱ．計画書の審査権限と方式

１．裁判官の適格性

以上のような計画書方策に対しては，コンピュータ・フォレンジックの門外漢である裁判官が，このような複雑な計画書を審査する能力が果たしてあるのかという疑問が提起されうる。

この点について，Kerr は，Winick の理論を批判の対象として，次のように述べている。すなわち，Kerr は，コンピュータ・フォレンジックは極めて複雑であって，最良ツールは往々にして捜査の執行時点でないと決められないばかりか，最良ツールとは何か，さらに，それが存在するのかという点さえ問題となる[927]。それゆえ，最良ツールの判断については，コンピュータの素人である裁判官はもちろん，プロのアナリストであっても判断することが極めて困難であると言わざるを得ず，裁判官の指示に基づく事前のコンピュータ令状により捜査を制約することはプロの仕事を邪魔するばかりであって，採用すべきではない[928]。

確かに，「最良ツールは往々にして捜査の執行時点でないと決められない」という指摘はその通りであろう。実際にも，台湾の先行研究においては Kerr のこの指摘を引用しそれを支持する論者が現れている[929]。しかし，本稿が提案した計画書審査通過令状は，追加・変更が可能なものであると同時に[930]，立法論としては，捜査の現場に臨んで初めて判明した事

---

[927] Kerr, DIGITAL WORLD, at 535, 571～572, 575, 579.

[928] Id.

[929] 李・電磁紀錄 1097 頁。

[930] 従来の理解にも，「令状の記載事項のうち基本的な事項，すなわち裁判の本質的な内容をなす部分については，記載事項の追加変更は許すべきではないが，その他の部分，言い換えれば，裁判の本質的な内容をなさない部分については，特段の弊害さえなければ，新たな令状を発付するまでもなく追加変更を認める」（三好28頁。同解として，伊丹編著・実例19頁参照）とされてきた。令状の追加・変更に関して基本的には，本稿も，この従来の基準に従い処理すればよいと考

情に応じて，ツールの追加・変更ないし修正を行うことを認める「事後追認」制度を設けるべきであると考える。これにより，Kerr の指摘に対応することができると思われる。

また，「最良ツールの判断については，コンピュータの素人の裁判官は勿論，プロのアナリストであっても判断することが極めて困難である」という指摘もその通りであると思われる。しかし，そこから直ちに，「裁判官の指示に基づく事前のコンピュータ令状により捜査を制約することはプロの仕事を邪魔するばかりであって，採用すべきではない」という結論を導き出すのは，論理の飛躍がある。というのも，本稿のいう計画書方策は，捜査側の専門家から提案されるものであって，裁判官が自ら最良ツールを指示するわけではないからである。言い換えれば，裁判官は単に専門家の提案した最良ツールが法の最小化の要求を満たしているかどうかを審査するだけであるし，また，最小化の要求を満たさないと判断された場合のツールの修正も，捜査側の専門家が行うべきであって，裁判官が自ら行ってはならないからである。

もっとも，裁判官に計画書を審査する能力があるかという問題点については，コンピュータについて素人の裁判官に，複雑な計画書を審査する能力がないことは間違いない。よって，令状を発付する裁判官は少なくとも，計画書を理解できる能力を身につけている者でなければならない[931]。この点，日本やアメリカのように法科大学院(ロースクール)を設立することが１つの方法として考えられる。これにより，学部で情報科学通信技術やコンピュータ・ネットワークなどを専攻した方が裁判官となることが可能である。他方で，法学部出身の裁判官は，在職の研修や自学というようなアプローチを通じて，情報科学通信技術やコンピュータ・ネットワークに関わる専門知識を身につけるということがもう１つの方法としてあげられる。

以上に加え，中立かつ権威ある鑑定機構の設立が必要であると思われる[932]。なぜならば，Kerr が指摘した通り，そもそも，最良ツールの判断については，プロのアナリストであっても判断することが極めて困難であるので，制度としては，裁判官の独断により審査するのは妥当ではなく，中立かつ権威ある鑑定機構の審査意見を聴取する必要があると考えられるからである。

える。具体的には，①捜索の対象とする情報システムの技術的な特性，②利用しようとする侵入・探索ツールの技術的な特性，③探知の対象とする情報及び探知に伴いやむを得ず開示されうる探知の対象でない情報の範囲と性質，という３つの種類の非物質性の要素のうち，①と③は，強制処分の対象を明示するものであって，各令状のもっとも基本的な事項であるから，追加変更が認められないが，②は，処分の対象を特定するという側面で補充的な意味をもつ事項であるにすぎず，令状の基本的な事項ではないと考える。そこで，②の部分の追加ないし変更は，審査を通過したもともとの処分の対象との同一性を維持することができる限り，認めても差し支えないと思われる。

931 実際にも，台湾においては，コンピュータ関連事件に対応できる専門の裁判官を養成し，コンピュータ法廷を設立すべきであると唱えられてきた(法務部・電脳犯罪４版 96 頁。同 142 頁，158 頁をも参照)。かかる提案は，公判審理段階の文脈のもとにおいてなされたものであるが，令状発付の文脈のもとにおいてもそのまま適合するものであると考えられよう。

932 もとより，中立かつ権威ある鑑定機構を設立することの必要性に関しては，台湾の先行研究においてかつてよりも既に指摘されてきたが(法務部・電脳犯罪４版 89，103 頁。また，同 96 頁及び 133～134，142，147～148 頁をも参照)，今でもまだ実現されていないのである。

２．審査の重点

このように，適格性を有する裁判官が，中立かつ権威ある鑑定機構の意見を聴取しながら，自らの判断で，捜査側が提出した計画書の内容と法の最小化の要求との合致性を判断するに際して，その審査は，とりわけ，次の３点に重点を置くべきであると思われる。

すなわち，①その他の態様での継続的な侵害の蓋然性があるか，②情報・情報システムに対する一瞬の取得・侵入の場合にあたるか，③ツールの限定性(篩い落とし機能)を視野に入れたうえで，基本権(法益)を保護するためにあるべき段階を決定することである。

第５節　情報と物の関係について

ここまでは，「情報に対する差押え・捜索」という新制度の在り方についての具体的な内容を明らかにした。これを踏まえて，以下では，かかる新制度と現行する物に対する捜索・差押えという既存の制度との間にいかなる関係があるかを述べる。

第１款　物と情報の衝突ないし競合関係

2001 年の台湾刑訴法改正は，形式的には電磁的記録をも捜索・差押えの対象としているが，その他の類型の情報は独立した処分の対象とされていないし，物と情報との衝突ないし競合関係を調整するために必要な規定も用意されていないから，こうした衝突・競合関係が解消・調和されていないのが現状である。そこで，立法論的には，有体物と並んで，あらゆる情報を独立した処分の対象としたうえで，情報と物との衝突ないし競合関係を解消・調和するためにあるべき方策を考案する必要がある。

この点については，情報と物を分割した上で，両者に同じ程度の保護を与えることが，立法論としての最良の調和策であると考えられる。というのも，物と情報とを分割すれば，その衝突ないし競合関係が解消されることになるはずだからである。そして，「物(媒体)のみを取得する」差押令状と「情報のみを取得する」差押令状という制度が，その具体策となる。

このうち，「物(媒体)のみを取得する」差押令状を新設することにより，媒体に蔵置された無関係の情報が捜査機関に取得されることを防止することができるから[933]，この意味で，物と情報との衝突ないし競合関係が解消されるといえよう。「情報のみを取得する」差押令状が，物と情報との衝突ないし競合関係を解消することに機能する原理は，基本的には，

[933] この点，第１章にあげた，ノートパソコンを鈍器として人を殺害した例を想起されると直ぐ分かろう。すなわち，こうした例で，ノートパソコンという機器のみを取得すれば十分であるから，本稿の理論によると，捜査機関が「物(媒体)のみを取得する」差押令状しか得られない。そして，当該令状により，捜査機関はデータがロック若しくは削除されたノートパソコンしか差し押さえられない。それと同時に，削除する前に，被処分者がデータを他の媒体に転写したり削除したりすることができる。

「媒体のみを取得する」差押令状と同じであるが，その具体的な手順はより複雑になっている。以下では，オフラインの場合とオンラインの場合とに分けてそれを論じる。

Ⅰ．オフラインの場合

オフラインの場合とは，対象となるデータを記録した媒体と物理的な接触をすることができる場合を指す。その中には，さらに，「現場での選別が可能なケース」と「現場での選別が不可能なケース」がある。

１．現場で選別が可能なケース

現場で選別可能な場面においては，捜索・差押えの最小化方案に関する計画書を提出し，計画書通過令状の発付を請求しておくことになるが，その令状には，非物理的な限定要素だけでは足りず，物理的な限定要素をも記載しなければならない。というのも，情報を取得するために，まず，物理的な空間に侵入して媒体を探す必要があるからである。

こうした場合，情報は捜索・差押えの対象となるが，媒体は差押えの対象ではなく，捜索の対象にすぎない。他方，前述した「物理的な対象への捜索・差押えの権限の範囲は非物理的な対象に及ばない」という前提のもとでは，物理的な対象への捜索・差押えの部分と非物理的な対象の両方を別々に司法審査に服させなければならないという帰結になる。そして，ここでいう個別の司法審査とは，令状の通数とは直接的な関係はなく，物理的な対象と非物理的な対象のそれぞれに対して個別の司法審査を行い，かつその旨を令状に明記すれば，１通の計画書通過令状という形にしても差し支えない。

２．現場で選別が不可能なケース

現行法のもとでは，電磁的記録という類型の情報を対象とする場合を除き，その他の場合においては有体物のみが差押えの対象とされているから，現場での選別が不可能な場面には，媒体全体――たとえば大量の書類や帳簿などの場面が想定される――を差し押さえるしかない。これに対して，情報自体を独立した処分の対象とする場合には，媒体全体を差し押さえるのではなく，媒体の内部のすべての情報を一括して差し押さえておく――具体的には，紙媒体の書類や帳簿などの中身を見なくてとりあえずそのすべてをコピー(または写真撮影やスキャン)しておくという手段が考えられる――ことになる。

このように，本稿の考え方によると，内容自体を確認せずに，情報の差押えとしてのコピー(または写真撮影やスキャン)をする場合は，蓋然性による情報の差押えに該当する。そこで，計画書通過令状により，蓋然性により差し押さえた後の捜索段階を規制しなければならないことになる。そして，蓋然性による差押えという段階自体に対しては，①捜査機関は，現場での選別が困難ないし不能であると予想され，選別のために，とりあえず，関連性を確認せずに膨大若しくは混在する情報を一括して確保しておく必要があると思料

されるときには，令状の発付を請求する際にその旨及び具体的な根拠を疎明しなければならないこと，②裁判官は令状発付を決定する際に当該疎明の要旨を令状に明記すべきであること，及び，③蓋然性による差押えを認めるための令状の発付は，最終手段性，条件の付加による限定，捜査計画の提案による限定という３つの要求を満たさなければならないこと，という３点からなる規制を用意すべきである。

Ⅱ．オンラインの場合

次にオンラインの場合は，オンライン侵入技術の利用を必要とする場面とそうでない場面とに分けることができる。前者の具体例としては，ドイツでいうオンライン捜索が挙げられる。後者は，日本のリモート・アクセスなどが想定されよう。

前者の場合は，有体物である媒体に接触することなく処分を行うことができるという点に特徴がある。こうした場合には，物と情報との競合ないし衝突の関係が生じない。これに対して，後者の場合は，有体物である媒体を占有したうえで行うという形になっているため，物と情報との競合ないし衝突の関係が生じうる。

まず，有体物の媒体を占有したうえでリモート・アクセスを行う場合において，物と情報の間にいかなる競合ないし衝突の関係が生じうるか。ここでの問題の核心は，令状に明記された被処分者の端末機器を合法的に占有したことにより，それに付帯する――そこから別の端末機器にアクセスする――権限も捜査機関の手に移ったと解することができるか，という点にあるが，特定のコンピュータ内にあるデータへのアクセス権限は，むしろ，そのコンピュータの利用者たる人に帰属する権限であって，コンピュータという物に備わったものではないから[934]，それは否定されるべきである。

それゆえ，次に検討すべきは，立法論として，人に帰属する権限を捜査機関に移転させるという類型の処分を新しく設けることができるか，そして，そうすべきであるのかという問題である。これについては，かような処分を新設すべきであると考える。なぜなら，物に対する捜索差押えであれ，情報に対する捜索差押えであれ，それらはいずれも，被処分者のある権限(物権ないしデリート権)を，一時的に捜査機関に移転させるものと理解することができるとすれば，「アクセス権」を捜査機関に移転させる法律を設けることができないとする理由はないはずだし，リモート・アクセスという問題に対応するためにもこのような法律が必要だからである。

そして，ここでいう「アクセス権」とは，「オンライン侵入技術を使用することなく，システムの設定上認められたユーザーとしての権限で，システムにおいて活動することができる権限」を意味する。こうした「アクセス権」という概念の実益としては，アクセス先ないしアクセスにより取得されるデータを特定する必要がなく，令状により被処分者のアクセス権を捜査機関に移転させるべき範囲さえ特定できればよいという点が挙げられる。

---

[934] 川出・コンピュータ犯罪 10 頁。

また，「アクセス権」の「移転範囲」の特定とは，①当該アクセス権が誰に帰属しているか，及び②捜査機関がいかなる範囲で当該アクセス権を利用することができるか，という２つの要素からなるものである。

それゆえ，立法論としては，「裁判官は，物若しくは情報に対する捜索・差押令状を発付するに際して，捜査機関の請求を受け，かつ，発付すべき物若しくは情報に対する捜索・差押令状の目的を遂行するために必要である限り，被処分者の特定のアクセス権を一定範囲で捜査機関に移転させることができる」といった規定を用意すべきである。

Ⅲ．小結

以上の通り，「物のみを取得する」差押令状並びに「情報のみを取得する」差押令状により，物と情報とを法的に分割することができるので，その衝突ないし競合関係が解消され，また，「情報のみを取得する」差押令状のもとで，さらに「アクセス権の移転」というような類型の処分を設けておけば，リモート・アクセスを行うために，その媒体を占有する必要はなくなるから，物と情報の衝突ないし競合関係が解消される。

それと同時に，これにより，バーチャル空間においては場所という概念がないに加え，遠隔地にあるコンピュータ自体を特定することが困難であるという状況において，リモート・アクセスの範囲を画定するためにあるべき基準は何なのかという問題点が解決される。

それにとどまらず，①情報の内容に証拠としての意味があるとき，すなわち情報と特定の媒体との結びつきが証拠価値の問題として意味が乏しい場合，差押えの方法によるべきか，検証の方法によるべきか[935]，及び②電磁的記録を差し押さえる場合，その客体はデータ自体か，あるいは媒体そのものか[936]という２つの理論上の問題も解消されよう。というのも，「物・情報に対する捜索・差押え」という新制度を導入するに伴い，強制的な捜査手段としての検察官による無令状の検証という制度が存在する必要性はなくなり，廃止すべきという帰結になるし，また，「物・情報に対する捜索・差押え」という新制度のもとにおいて，情報のみを取得する差押えの客体(対象)は，情報であるのに対して，物(媒体)のみを取得する差押えの客体は媒体になるので，この２つの差押えの制度のもとで，電磁的記録を差し押さえる場合の客体はデータなのか，それとも，媒体なのかという問題は生じないからである。

最後に残る問題は，「物と情報とを同時に取得する」差押令状の場合においては，物と情報との衝突ないし競合関係をどう調整すべきであるか，という点である。この場合には，物と情報とを同時に取得する以上，物と情報とを分割することにより両者の衝突ないし競合関係の問題を解消するという前提が成り立たないし，また，電磁的記録を差し押さえる場合の客体はデータなのか，それとも，媒体であろうかという問題が再び登場してくる。

---

[935] 古田・第三者の保護 191 頁。

[936] 李・電磁紀錄 1057～1058 頁；また，新保 147 頁をも参照。

以下では，これらの点を検討していこう。

第２款　多段階規制論の構築

捜索現場において，ＩＴセキュリティの支障等が理由で，情報を選別できないだけでなく，情報を選別せずに一括して記録(コピーや写真撮影)しておくことさえできないこともありうる。それゆえ，「物と情報とを同時に取得する」差押令状という類型はやはり必要となる。このような場合の物と情報との衝突ないし競合関係への調和策として，本稿は，多段階規制論を提案する。その詳細は，次の通りである。

Ⅰ．意義

多段階規制論とは，中華民国憲法 23 条から導かれた最小化原則の要求を満たすために，「制定法の明文による法的な根拠」又は「制定法の授権に基づく司法の判断」をもって，処分を，その執行者，対象，時期ないし範囲などのあらゆる側面で物理的な要素並びに非物理的な要素を基準に，多段階で分割し規制する考え方である。

１．制定法の明文による法的な根拠

「制定法の明文による法的な根拠」とは，多段階の捜査処分を正当化するために立法者が設ける法律を意味するが，そこでは，かかる多段階処分のあるべき段階数並びにそれぞれの段階の処分の執行主体ないし対象(客体)及び処分できる範囲，要件とそれについての判断の基準などを立法者があらかじめ明示しておかなければならない。具体例としては，第１章において検討した日本刑訴法 100 条 1 項から得られた示唆，すなわち，蓋然性を確認するための捜索という段階を規制すべきという発想を採り入れつつ，アメリカの Winick の２段階令状をも考慮に入れた，「(ア)専門家による検索(蓋然性を確認するための捜索)→(イ)蓋然性による差押え→(ウ)捜査機関による検索(関連性を確認するための捜索)→(エ)証拠物又は証拠である情報に対する差押え(関連性による差押え)」という４段階規制の立法例が挙げられよう。このうち，(ア)も(ウ)も，捜索にあたるものであるが，両者の差異は，検索の「執行の主体」と「確認の対象」という２点に求められる。

(1)執行の主体

(ア)の蓋然性を確認するための捜索という段階の主体は，検索の客体ごとに異なるものであり，例えば，郵便物の場合は郵便局職員，電子メールの場合はプロバイダー，会計帳簿の場合は会計士，電磁的記録である電子書類の場合はコンピュータ・フォレンジック・アナリストということになる。

これに対して，(ウ)の関連性を確認するための捜索という段階の主体は捜査機関である。

(2)確認の対象

(ア)の段階の捜索の基準は，蓋然性(低い関連性)のあるものとそうでないものを選別するという意味であるのに対して，(ウ)段階の捜索の基準は，関連性(高い蓋然性)のあるものとそうでないものを選別することである。この点を，次の２つの例で具体的に説明しよう。

A.大量の郵便物の場合

まず，郵便物の例でいうと，(ア)段階でいう蓋然性の選別基準は差出人と宛先人であり，被疑者からの郵便物あるいは被疑者への郵便物とそうでないものが選別され，被疑者からの郵便物あるいは被疑者への郵便物は，被疑事実との関連性が存在する蓋然性が認められるから，(イ)段階の蓋然性による差押えの対象になる。

これに対して，(ウ)段階でいう関連性の選別基準は，それによって被疑事実を立証する関係が有るか否かであり，被疑者からの郵便物あるいは被疑者への郵便物を開封したうえで，その内容を点検しつつ，被疑事実を立証する関係の有無を基準に，被疑事実と立証関係があるものとそうでないものを選別し，被疑事実と立証関係がある郵便物は関連性のあるものとして，(エ)段階の差押えを行うことになる。

B.大量の電磁的記録の場合

次に，大量電磁的記録を例に説明すると，(ア)段階でいう蓋然性の選別基準はコンピュータ・フォレンジックのツールであり，アナリストが捜査機関の提供した事案の内容と関連する情報をもとに設定した指令に該当するコードの集合とそうでない集合を選別する。該当するコードの集合は，被疑事実と関連性のある情報が存在する蓋然性を持つコードにあたるため，(イ)段階の蓋然性による差押えの対象になる。

これに対して，(ウ)段階でいう関連性の選別基準は，被疑事実を立証する関係の有無であり，被疑事実と関連性のある情報が存在する蓋然性を持つコードの集合をアウトプットしたうえで，その内容を点検しつつ，被疑事実を立証する関係の有無を基準に，それがあるものとそうでないものを選別しながら，被疑事実を立証する関係があるコードの集合は，関連性のあるものとして(エ)段階の差押えを行う。

２．制定法の授権に基づく司法の判断

次に，「制定法の授権に基づく司法の判断」とは，多段階令状の発付を指す。例えば，捜査の終局的な目的としては情報のみを取得すれば十分であるが，現場での執行の支障等に鑑み，媒体をも取りあえず確保しておく必要があると判断される場合において，「情報と物とを同時に取得する」差押令状の発付を請求することができる。この差押令状の基本的な構成を示す代表的な例としては，(イ)被疑事実と関連性のある情報が存在する蓋然性がある媒体の取得(蓋然性による差押え)→(ウ)捜査機関による検索(関連性を確認するた

めの捜索)→(エ)証拠物あるいは証拠である情報に対する差押え(関連性による差押え)，という３つの段階からなるものが挙げられる。この意味で，「情報と物とを同時に取得する」令状は，多段階令状の一類型である。

そして，上記の３つの段階は，それぞれの段階で，同じ対象に対して処分できる範囲が異なり，それが各段階を区別する基準ともなる。この点の詳細は，以下の通りである。

(1)「仮差押え」段階

(イ)段階(蓋然性による差押え)では，媒体が取得されると同時に，データに対する情報の終局的処分権も奪われたことになるから，情報と媒体とが同時に差押えという処分の対象となる。

しかしながら，(イ)段階の差押えの目的は，媒体に対する一時的な占有の剥奪により証拠となりうるデータを確保することにとどまるから，(イ)段階の令状をもって差し押さえた媒体に蔵置されたデータを検索することはできない。この意味で，(イ)段階は「仮差押え」といえよう。

(2)「関連性を確認するための捜索」段階

(イ)段階(蓋然性による差押え)で仮差押えをした媒体に蔵置されたデータを検索しようとすれば，(ウ)段階(関連性を確認するための捜索)に入ることになる。(ウ)段階は，捜索に関する最小化の計画書を提出し，別個の計画書通過令状をもって行わなければならない。

(3)仮差押え後の差押えについて

(ウ)段階で，被疑事実を立証する関係があるデータとそうでないものを選別し，それが認められるデータは，関連性のあるものとして，(エ)段階の関連性による差押えを行う。

しかし，問題は，媒体及びその内部に蔵置されたデータは，既に(イ)の仮差押えの段階で一括して確保された以上，仮差押えにあたる「蓋然性による差押え」と「関連性による差押え」とが，観念上区別できるか，また，仮に観念上区別できるとしても，執行上，具体的にはいかなる形になるのかである。これらの点を，さらに敷衍してみよう。

A. 観念上の区別の可能性

前述した通り，政府には仮差押えの段階で令状をもって差し押さえた媒体に蔵置されたデータを検索する権限がない。そして，選別のための検索行為さえできない以上，データの内容をじっくり吟味したり，証拠として利用したりする権限もない。言い換えれば，仮差押えの段階で認められる捜査権限の範囲は，媒体の取得により証拠になりうるデータを確保する点にとどまるのに対し，関連性による差押えの段階で認められる捜査権限の範囲は，データの内容をじっくり吟味したり，証拠として利用したりする権限である。こうして，仮差押えにあたる「蓋然性による差押え」と「関連性による差押え」とは，観念上，区別することができよう。

ところで，この観念の問題と連動し，補足すべき重要な点がある。それは，仮差押えは，「蓋然性による差押え」にあたるが，「蓋然性による差押え」だからといって，必ずしも仮差押えにあたるわけではないということである。というのも，情報システムの不可侵性という法益が含まれない包丁のような物件に対しても蓋然性による差押えを行う必要ないし可能性があるが，この場合の差押えの効力は，一般の差押えの場合のそれと同じであるから，仮差押えではない。それゆえ，(ウ)(エ)という２つの後段階の規制も不要である。

B. 別個の令状の要否

(ウ)の段階で，関連性を確認するために捜索を行うが，そこには２つの場合がある。その１つは，差し押さえるべき情報が未だ特定されていなかったため，計画書通過令状の発付が，捜索に関する部分しか認められなかった場合である。こうした場合，(エ)の段階においては，情報の差押令状を取得しなければならない。もう１つは，差し押さえるべき情報が既に特定されていた場合である。こうした場合，(エ)の段階においては，(ウ)段階で発付された計画書通過令状の差押えを執行することになるから，差押えの執行のために別個の令状は不要である。

C. 押収の効果と執行の方法

仮差押えをされた物(媒体)や情報(データ)には仮押収の効果しか生じないため，その後選び出された関連性のある物や情報が，既に「仮差押え」をした物や情報だからといって，本来の差押えの効果が生じるわけではなく，さらに「差押え」をしなければならない。すなわち，仮差押えにより，情報の終局的処分権は一部(あるいは，一時的に)剥奪され，２回目の「差押え」により，全部(あるいは，最終的に)剥奪されることになる。具体的にいえば，まず，仮差押えにおいても，自分のデータが政府に取得されたという点は変わらないから，被処分者が自分のデータに対してコントロールを及ぼすことができないことになる以上，情報の差押えにあたるものの，政府はこの段階で取得したデータを検索したり分析したり利用したりすることができないという制限があるため，この意味で，情報の終局的処分権は一部(あるいは，一時的に)剥奪されているのである。

これに対して，２回目の「差押え」の対象は，(ウ)の段階の捜索により，(イ)段階で取られたデータを検索したうえで割り出した関連性のあるデータである。それゆえ，この段階では，対象となるデータをコピー(確保)することができるのはもちろんのこと，関連性という制約のもとで当該データをさらに検索したり，分析したり，利用したりすることもできる。この意味で，情報の終局的処分権は全部(あるいは，最終的に)剥奪されているのである。

以上を踏まえて，執行の方法を示すと，次のようになる。すなわち，仮差押えの段階は，情報と媒体とを同時に取得し，その後，関連性を確認するための捜索により関連性のない情報と関連性のある情報を選別した上で，関連性のある情報のみの差押え(コピー)を行い，没収すべき情報がなければ，媒体と共にその内部に蔵置された情報を被処分者に返還する。

そして，差押え(コピー)により押収の効果が生じた以上，押収目録(すなわち，コピー一覧表)を作成し被処分者に交付すべきであることになる。

Ⅱ．機能について

こうした多段階規制論の機能としては，以下の３つのものが挙げられる。

１．物と情報の衝突・競合関係の解消・調和の補完策

各々の段階で同じ対象に対して処分できる範囲が異なるから，仮差押え(蓋然性による差押え)，関連性を確認するための捜索，仮差押え後の差押えの執行(関連性による差押え)という３段階について工夫すれば，物と情報の衝突ないし競合関係を解消・調和することが可能になる。この意味で，多段階規制論は，「物と情報とを同時に取得する」差押令状において生じうる物と情報の衝突・競合関係を補完する方策であるといってよい。

２．仮差押えと一般の差押えとの細分化

仮差押えは，一般の差押えと同様に，物ないし情報を取得することを目的とするものの，当該取得は最終目的でなく，その後更なる選別作業を行うための取得である。現行法のもとでは，このような差異に対応することが困難であるが，多段階規制論によれば，処分の執行者，対象，時期ないし範囲などの諸要素ごとに細分化し更なる規制を行うことが可能になる。

３．最小化原則による実質的保障の維持

現行の単一段階の令状制度のもとにおいては，「正当な理由」，「関連性」，「特定性」等の要件を満たすことができない手段(例えば，膨大かつ混在する情報に対する蓋然性による差押えや自動徹底検索技術の利用など)を捜査に用いることは，一般令状禁止原則に反するものであると解さざるを得ないのに対して，多段階規制論を前提とするならば，ある段階における規制の不十分さ(蓋然性による差押えを行う際に関連性を確認していないこと，自動徹底検索技術の利用がすべてのデータを対象とすることを指す)を，その後の段階で補うことができる(後の段階の捜索を別個の令状により規制することをさす)から，このような多段階を全体と見れば，一般令状禁止原則により提供される従来の保護の範囲ないしその程度を実質的に保持しているといえるかぎり，一般的探索的性格を持つ前段階の措置の許容性が認められるという帰結が導かれる。

このように，多段階規制論のもとにおいては，従来の保護の水準が実質的には維持されることを必要不可欠な前提としたうえで， 捜査の態様に応じた多段階による規制が可能になるため，最小化原則をより貫徹できると同時に，従来の「正当な理由」，「関連性」，「特定性」等の諸要件に固執する必要はなくなるから，捜査のニーズにもより対応できるもの

といえるのである。

Ⅲ．多段階規制論の現実化

多段階規制論を，立法によって実現しようとすれば，次の２つの点を検討しておく必要がある。第１に，裁判官が令状の執行事項につき捜査機関に対して具体的な指示を命ずることができるような立法が正当であるといえるための理論的根拠は何なのか，第２に，「物と情報とを同時に取得する」差押令状における物と情報の競合ないし衝突関係の解消を実現するために，多段階規制論を採用することが必要であるとして，規制段階の決定基準はどうあるべきかである。

１．令状による指示権限とその制約

まず，第１点の令状による指示権限に関しては，2001 年の台湾刑訴法改正により，128 条 2 項後段において「裁判官は捜索令状において執行人員に対する適当な指示を行うことができる」と規定されている。しかし，前にも言及したが，ここでいう適当な指示の許容範囲については争いがある。すなわち，この指示は，捜索の目的またはその範囲をより明確させるものに限られるとする見解と，令状の執行方法までも指示することができるとする見解が対立している。この点の検討は，解釈論と立法論とに分ける必要がある。

(1)解釈論としての分析

台湾刑訴法 128 条 2 項後段の解釈にあたっては，令状における条件の付加の可否という問題についての日本の議論が参考となる。

「仮に令状主義の本旨から『強制処分の範囲程度を減縮させる方向に作用する』条件の付加が許容されるとした場合，捜査機関がこの条件を遵守する限り，処分対象者の被る法益侵害の範囲程度も減縮されるはずであるから，特段の不都合はないように見える。しかし，理論的には次のような問題が想定できなくはない。それは，もし条件の付加がなければおよそ実施できなかったであろう強制処分が条件の付加によりはじめて可能になるような場合である。……これは，法解釈（身体検査令状の規定の検証令状への『準用』）の形式を装った裁判官による実質的な『立法』ではないか。そのような司法部による法創造は許されるのかという疑問が生ずるのである[。]」[937]

「確かに，裁判官が，処分の濫用を防止したり権利の制約を縮減するために，令状に条件を付することは，禁止される理由がないようにも見える。しかし，特定性という令状主義に不可欠の要件に関する限り，条件についての明文の規定がないことは，法律がその確保のために条件を付するということを予定していなかったことの現れと解すべきように思われる。特定性の要件を満たすのに，通常の方法では事足りず，条件を付することが不可欠

[937] 酒巻・条件の付加 8～9 頁。

であるような特別なプライバシー保護を必要とする処分は，そもそも刑訴法が許すことを予定していたものか，疑問とされるべきである。立法者が許そうとした範囲を越える処分であれば，それを新たな立法によらずに許すことは，強制処分法定主義に反するといわなければならない。たとえ実質的に憲法の要求を満たすことができたとしても，既存の強制処分の中に解釈で取り込んでしまうことは，許されないことといわなければならないように思われるのである[。]」[938]

以上のとおり，問題の核心は，司法的抑止論による法創造と強制処分法定主義との対立に帰結する。つまり，司法的抑止論に立つからといって，司法が強制処分法定主義の制限を超えて法創造を行うことができるわけではない。この意味で，強制処分法定主義は司法的抑止論に対する再抑止の機能を担うものであるといえよう。これにより，次の示唆が提供されよう。

すなわち，台湾刑訴法128条2項後段のいう裁判官による適当な指示の立法趣旨を，司法的抑止論による法創造を認めるものであると読むことができるとすれば，それは，捜索の目的またはその範囲をより明確させるものに限らず，令状の執行方法などをも指示することができるという帰結が導かれると同時に，この指示の権限においては，強制処分法定主義に反してはならないという内在的な制約があると解すべきである。言い換えれば，裁判官は128条2項後段によっても強制処分法定主義の制限を超えた法創造を行うことができないのである。

(2) あるべき立法の提案

以上により，台湾にあるべき立法としては，現行台湾刑訴法128条2項後段を次のように修正すべきであると考える。

「裁判官は，本法の所定する強制処分の類型範囲内に限っては，令状において執行人員に対する必要な指示を行うことができる。但し，その指示は，最小化原則を核心とした令状主義の精神に合致しなければならず，かつ，本法の強行規定に反してはならない。」

そのうえで，「(第3項)執行人員は，前項の指示に従わなければならない。但し，令状の執行方式に関わる必要な指示は，強制処分の対象及びその範囲を特定・明示する目的に関わらない場合には，執行人員を拘束しないものとする。(第4項)前項の場合，捜査機関が裁判官の行った必要な指示と異なる執行方式を取ったときには，執行終了後七日以内に令状発付裁判官に対して口頭あるいは書面でその事情を報告しなければならない。(第5項)前項所定期間内に正当な理由もなく当該事情の報告がなされていなかった場合，捜査機関が行った執行方式は違法なものと見なす。」といった内容の規定を新設すべきである。

---

[938] 大澤・特定 440 頁。

２．規制段階の決定基準

最後に，あるべき規制段階の決定基準は何なのかを検討する。それは，立法と司法の２つの次元に分けることができる。

(1)立法の次元

まず，立法の次元からすると，規制段階の決定基準は，侵害されうる基本権に対する特別な保護の要否に求められる。ここでいう「侵害されうる基本権に対する特別な保護の必要性」とは，ある捜査の手法(技術)が，一般的・探索的性格をもつものの，多段階の制約を設けることにより，その合憲性を認める可能性がある場合には，多段階の制約が基本権への侵害を正当化するために必要不可欠な特別保護要件になることを意味する。現行台湾刑訴法 135 条 1 項 2 款(日本刑訴法 100 条 1 項の中身と同じものである)は，その格好の例である。

前にも検討したように，同 135 条 1 項 2 款は，蓋然性を確認するための捜索及び蓋然性による差押えという２重の性格をもつものである。この意味で，それは一般的・探索的性格を帯びているものであるといえよう。この 135 条 1 項 2 款の合憲性の問題を多段階規制論から改めて検討すると，以下の４つの特別保護要件をすべて満たす限り，合憲といえることになる。

A. 情報の終局的処分権

第１の特別保護要件として考慮すべきは，「情報の終局的処分権の剥奪」の有無である。135 条 1 項 2 款に当てはめていえば，同条項により，郵便局職員が，被告人から発し，又は被告人に対して発した郵便物を選び出すために，すべての郵便物の封筒をざっと見るのは一般的・探索的の性格をもつものといえるものの，それだけでは，何も取得(占有の剥奪や複写・記録)されておらず，「情報の終局的処分権」が剥奪されていないので，情報の差押えに当たらない。

B. その他の態様での継続的な侵害の蓋然性

他方で，すべての郵便物の封筒をざっと見ることは，郵便物が大量である場合には，情報システムの不可侵性を害するものであることは間違いない。

しかし，このような検索の結果として，対象郵便物(被告人から発し，又は被告人に対して発した郵便物)に該当しないと判断された郵便物の情報(封筒とその内容)が，捜査機関の目に入ったりするなどの「その他の態様での継続的な侵害の蓋然性」がないことが法的に担保されるかぎり，郵便局職員がすべての郵便物の封筒をざっと見ておくことは一般的・探索的性格をもつものの，違憲とはならない。

しかし，問題は，現行法上，「その他の態様での継続的な侵害の蓋然性」がないことを担保するための法規定が存在していないことである。この点は，立法を行う必要がある。

具体的には，本稿が提案する「蓋然性による差押え」段階への規制に加え，郵便局職員の守秘義務並びに捜査官ないしその補助員の立会の禁止などの措置が考えられよう。

C. 後の段階の規制

このように，郵便局職員がすべての郵便物の封筒をざっと見ておくという検索方法を認める法は，違憲ではないと解することが可能であるが，かかる検索方法が，一般的・探索的性格をもつことは間違いなく，これにより低下した従来の保護水準を回復させるためには，第３の特別保護要件としての，後の段階の規制を必要とする。具体的には，蓋然性により差し押えた後の段階における関連性を確認するための捜索の規制が立法により新しく設けられれば，それが満たされることになる。

D. 蓋然性を確認するための捜索

他方，135 条 1 項 2 款のような明文規定がない場合，あるいは，明文規定はあるが郵便事業者に協力してもらえない場合においては，被告人から発し，又は被告人に対して発した郵便物を割り出すために，大量の郵便物の封筒をすべてざっと見てみるというような「蓋然性を確認するための捜索」を必要とするとしても，司法の判断だけでは，捜査機関にこのような捜索の権限を許可する令状を発付することはできない。

こうした場合には，一般的・探索的性格をもつ選別作業を行うこと自体が認められず，捜査機関が，選別作業の一般的・探索的性格を解消できるような捜索に関する計画書を出さなければならないことになる。すなわち，前述した計画書方策が，ここでの第４の特別保護要件になる。

E. 小結

以上のように，日本刑訴法 100 条 1 項の理解を台湾刑訴法 135 条 1 項 2 款という規定の解釈論にも採り入れることにより，台湾の場合においても，原則としては捜査機関が自ら郵便物の捜索を行うことができないと解することが可能であるので，135 条 1 項 2 款の「蓋然性を確認するための捜索」に関する規制という部分は合憲であるといえるものの，「蓋然性による差押え」という段階自体に対しては規制を設けておらず，また「関連性を確認するための捜索」という後の段階にも必要な規制が欠けているため，「蓋然性による差押え」を認めている部分は違憲であるという帰結になる。

ただし，郵便局職員が，被告人から発し，又は被告人に対して発した郵便物を割り出すために，数量のかなり限定された郵便物の封筒――たとえば，２，３通ぐらいの郵便――をすべてざっと見てみるというような事例においては，膨大かつ多様なデータの存在の可能性がないため，「情報システムの不可侵性」が侵害されるおそれが全くない類型の「蓋然性による差押え」に該当するから，こうした場合の 135 条 1 項 2 款の適用結果は合憲であると解しうる。

(2) 司法の次元

次に，司法の次元から，あるべき規制段階の決定基準を検討すると，それは，立法者の授権と憲法の基準という２点に求めることができる。

A. 立法者の授権

裁判官は，立法者が設けた規制に服しなければならないから，司法の命令により，規制の段階数を増減することができないことはいうまでもない。

しかし，前述した通り，計画書方策を導入するにあたって，立法者が，あらかじめ司法に，令状による指示権限を授権しておくことはできるし，そうすべきである。そして，この指示権限の運用により，実質上，規制の段階数を増減するのと同じ効果をもたらすことは可能であろう。この司法による調整権限の運用は，立法者の授権範囲内である限り，法律の留保の原則に反しない。

B. 憲法の基準

司法による調整権限の行使の基準は，立法者の授権により制約されるほかに，憲法の比例原則に要求される最小化の基準によっても制約される。

第１に，立法者の設けた多段階規制の法が，中華民国憲法 23 条から導かれた最小化原則を満たさない場合，当該法律は違憲となる。

第２に，立法者の定めた多段階規制の法は，憲法の最小化原則を満たしているものの，憲法が要求した保障の水準を維持するために必要とされる最低限の段階数と立法者が設けた段階数とが一致していない場合においては，次の２つの場面に分けてそれぞれを処理すべきである。

まず，立法者の設定した段階数が憲法に要求される最低限の段階数を超える場面では，裁判官は規制の段階数を減らすことができない。というのも，こうした場合は，立法者がある捜査手法に対して特に厳格な規制を行うという意思表明をしているので，司法府はそれを尊重しなければならないからである。

例えば，自動徹底検索技術の使用という段階での執行者は，プロバイダー，会計士，郵便局職員などの専門職業者とすべきであるが，これにより，規制の段階数は，①自動徹底検索技術の使用という段階(蓋然性を確認するための捜索)→②蓋然性による差押え→③関連性を確認するための捜索→④関連性による差押え，という４段階になり，これにより，既に憲法の最小化原則によって要求される最低限の段階数を満たしているものと考えられる。

これに対して，立法者は，自動徹底検索技術を開放式のＩＴシステムにおける通信傍受に使う場合において，上記の４段階による最低限度を超えて，さらに，自動徹底検索技術の使用という段階の前段階，すなわち，自動徹底検索技術の提供という段階での監督メカニ

ズムに関する規定を設けることもできる[939]。

この場合は５段階の規制になる。仮に，立法者が，このような厳しい規制を設けたとすれば，裁判官は，ある捜査手法をとりわけ厳格に規制しようとする立法者の意思を尊重しなければならず，５段階の規制が厳しすぎるからといって規制の段階数を減らすことができない。

次に，立法者の設けた多段階規制の法が，憲法の最小化原則により要求されている最低の規制の段階数を満たしているが，かかる法が具体的な事案に適用されると，実質的に，立法者の設けた段階数よりも下回るものと評価される場合には，裁判所は，計画書方策を生かして立法者の想定している段階数まで補足すべきである。

例えば，個人の端末を探索するための自動徹底検索技術の使用という段階につき，法律では，その執行者がプロバイダーとされているが，プロバイダーが捜査機関の補助機関にならないようにする措置が取られていない場合が考えられる。プロバイダーが捜査機関の補助機関という立場に立つ場合においては，自動徹底検索技術の使用という段階の執行者は，形式的には捜査機関でないものの，実質的には，それを捜査機関が自ら行うことと等しい。とすると，形式的には，①自動徹底検索技術の使用という段階(蓋然性を確認するための捜索)→②蓋然性による差押え→③関連性を確認するための捜索→④関連性による差押え，という４段階になっているが，実質的には，①蓋然性による差押え→②関連性を確認するための捜索→③関連性による差押え，という３段階になるからである。

このような場合，裁判官は，自動徹底検索技術の使用という段階の執行について，捜査機関から完全に独立した中立の鑑定機構により行われるべきだとすることにより，４段階の規制に回復させることができる。

もっとも，注意すべきは，あるべき段階数の提案権は，捜査機関にあり，裁判官にあるわけではないという点である。裁判官は，単に，段階数を増やすことにより，最小化の要求に適合する可能性の有無についての心証を捜査機関に開示すればよい。というのも，前述した通り，計画書通過令状の発付段階は対審化すべきであるし，また，計画書を修正するかどうか，具体的にどう修正すべきかなどの点は，裁判官が具体的な指示を行う必要がないばかりではなく，指示してはならないからである。

---

[939] この規定の具体的な内容としては，次の３点が考えられよう。第１に，捜査機関が開発した自動徹底検索技術をそのまま自動徹底検索技術の使用という段階での執行者であるプロバイダーに提供することができず，当該自動徹底検索技術の仕組みを中立かつ権威ある鑑定機構に公開しなければならないこと，第２に，当該鑑定機構が当該自動徹底検索技術の仕組みの侵害性ないし探索性についての報告書を作成し国会に提出しなければならないこと，第３に，国会が，一定の期間内に，当該自動徹底検索技術の使用禁止に関する法令を出さない場合に限って，次の段階――すなわち，捜査機関が当該自動徹底検索技術をプロバイダーに交付し執行すること――に進むことができることである。

第６節　問題点の解決

台湾において，従来は，捜索は，住居などの場所に対する物理的な侵入・探索の行為と定義されてきたが，現在の最新の見解によれば，捜索は，「捜査機関が犯罪の証拠あるいは犯人を見つけるために，相手方の合理的なプライバシーの期待を有する空間に侵入したうえで，物理的な探索を行う捜査行為」と定義されている。すなわち，捜索の概念を構成する必要な要素は２つのものがあり，１つは，合理的なプライバシーの期待を侵害すること，もう１つは，物理的な探索を行うこと，という２つの要素である[940]。

しかし，2001 年以後，現行刑訴法の文言上は電磁的記録をも捜索の対象とされているので，物理的な探索という第２の要素はそれに当てはまらない。そのため，学説は，電磁的記録を対象とする場合は，第１の要素のみをあげている[941]。だが，問題は，有体物を捜索の対象とする場合には，物理的な侵入・探索の行為をもって，場所ないしそこに置かれた容器に対する合理的なプライバシーの期待が侵害されるというのに対して，電磁的記録が捜索の対象となる場合には，無形の情報に対する合理的なプライバシーの期待が侵害されるといえるための基準は何なのかが，明らかにされていないことである。他方で，通保法３条 2 項の文言上は，明示的に，傍受は，合理的なプライバシーの期待を侵害することと定義されている。とすると，刑訴法のいう電磁的記録に対する捜索と，通保法のいう保存されたデータ(3 条 1 項 1 款)に対する傍受との区別が一層難しくなる点が問題である[942]。更に問題となるのは，ＩＴシステムにおいてはプライベイト領域とそうでない領域との区別若しくは私的データと非私的データとの区別をすること，または，特定の文脈を離れてデータの属性の判断を行うことは，原理的には不可能とされるから，合理的なプライバシーの期待の侵害という定義は，かような場合――たとえば，ＩＴシステムの全体を対象とするドイツでいうオンライン捜索というような手法――には対応することができなくなっているのである。

以上に対して，本稿は，有体物を対象とする捜索を，物理的な侵入・探索行為というのに対して，無体の情報に対する捜索を，情報システムの不可侵性を侵害する非物理性ないし物理性の侵入・探索行為と定義する。そのうえで，情報システムの不可侵性を主張するには，ある情報システムにおいては膨大かつ多様な情報が存在する可能性さえあれば十分であり，当該システムにおいて実際に膨大かつ多様な情報が存在することは必要でないとする。こうして，本稿の理論により保護されるのは，合理的なプライバシーの期待を有する情報に限らないのであるから，無形の情報に対する合理的なプライバシーの期待が侵害されるといえるための基準は不明確であるという問題が解消されると同時に，ＩＴシステム

---

940 陳瑞仁・新法捜索扣押 51～52 頁，同見解として，黃翰義・緊急捜索 155 頁柯慶賢・修正捜索扣押(上)4～5 頁参照。

941 陳瑞仁・新法捜索扣押 51～52 頁

942 台湾の先行研究においては，本稿と異なる理屈で，通保法 3 条 2 項の規定は立法論としては適切でないとするものがある(李惠宗・憲法五版 205～206 頁，江・通訊監察 104，117 頁)。

の全体を対象とするドイツでいうオンライン捜索というような手法に対応することが可能となる。

それから，情報システムの不可侵性という法益侵害の判断基準につき，本稿は，当該法益は，「情報システム内の事柄が開示され始める時点」で侵害されると考える。まず，ＩＴシステムを捜索の対象とする場合においては，オンライン侵入技術を実際に利用し始めたり，若しくは，ＩＴシステムから洩れた電磁波を収集し始めたりした時点などが考えられよう。また，現場で大量の書類の内容を確認せずに一括して差し押さえるような例では，当該紙媒体が置かれた家屋に立ち入った時点でも当該紙媒体が押収された時点でもなく，警察官が当該情報システムを構成する紙媒体の第１頁を開いたときを，情報システムの不可侵性の侵害の発生時点となる。

こうして，本稿の理論のもとにおいては，情報に対する傍受自体は，情報に対する捜索にあたるものであるし，また，捜査行為の侵害強度に合わせてその規制のレベル(段階)を適切に調整することが可能な多段階令状という制度による規制の強度は，現行の傍受令状による規制の強度に負けないものであるから，通保法のような個別立法を設けなくてもよいという帰結になる。この点をより具体的にいえば，ＩＴシステムを傍受する場合には，現在の技術ではあらゆるパケットを一括して保存しておく必要があるが，現行法では，捜索差押令状でなく，通保法の傍受令状をもってかような一括の保存を行うことができると解されており，その後の抽出行為――対象となる通信のデータを割り出したうえで元の通信情報に復元させることをさす――は，形式的には鑑識ないし鑑定と位置づけられるため，別個の令状は不要であるという帰結になるのに対して，本稿の理論によれば，この一括の保存は，情報に対する仮差押にあたるものであるので，蓋然性による差押え令状が必要となり，そして，その後段階である抽出行為は情報に対する捜索にあたるものであるから，また別個の，関連性を確認するための捜索令状を必要とするのである。

以上をもとに，以下では，前に指摘した，ＩＴシステムにおける遠隔操作による移動可能なデータを対象とする場合の問題点についての私見を述べる。具体的には，Ⅰ．端末へのリモート・アクセス，Ⅱ．端末に対する監視・記録，Ⅲ．通信の過程に対する監視・記録(通信傍受)の３つの場面に分けて検討する[943]。

第１款　端末へのリモート・アクセス

現行法は，単に電磁的記録をも捜索・差押えの対象として列挙しているだけであるし，

[943] 端末へのリモート・アクセスと端末に対する監視・記録との間の差異は，前者が，ある端末からある端末へ接近しデータを探索・取得するという捜査手法であるのに対して，後者が，対象たる端末に監視・記録のためのスパイプログラムを差し込んでおき，端末を監視しながらデータを探索・取得するという捜査手法である点にある。

また，単一段階の令状という制度しか用意されていないから，遠隔地にある端末にリモート・アクセスするというような捜査手法を適切に規制することができないのは明らかである。

これに対して，本稿でいうリモート・アクセスによる捜査の範囲は，㋐「リモート・アクセスできる連結経路・システム」及び，㋑「リモート・アクセスできる連結経路・システムのなかにおけるコピーできるデータの範囲」，との２つのものが挙げられる。

このうち，㋐について，捜査機関は，①捜索対象(ここでは，リモート・アクセスできる連結経路ないしシステムあるいは検索しようとする情報それ自体の技術的な特徴をさす)についての描写，②捜索方式についての描写，③利用目的の限定，④危険性の評価及び安全措置の効果，の４つの記載事項を明記した計画書を令状発付裁判官に提出しなければならない。この捜索計画書においては，連結経路を通じて繋がっている遠隔地にある端末それ自体を特定する必要はないから，遠隔地にある端末それ自体を特定することは極めて困難ないし不可能であるという問題が解決される。

次に，㋑の「コピーできるデータの範囲」を画定するには，蓋然性による差押えを行う必要性の有無を検討しておかなければならない。それが肯定される場合には，捜査機関は，情報に対する捜索令状の発付を請求するに際して，それと同時に，証拠となりうる蓋然性のあるデータに対する仮差押令状の発付を請求しておくことができる。この場合の捜索令状は，「蓋然性」を確認するためのものであるから，これをもって確認した蓋然性により「仮差押え」を行った後の段階の，「関連性」を確認するための捜索を行うには別の令状が必要となる。

第２款　端末に対する監視・記録

端末に対する監視・記録という手法としては，ドイツのいうオンライン捜索がその１つの典型例としてあげられる。そして，オンライン捜索は，ＩＴシステムの全体並びにその中に蔵置された「すべて」のデータに対する「全面的な侵入」であるのに対して，台湾の先行研究のいうオンラインで捜索を行うことは，「合理的なプライバシーの期待」を有するデータのみを対象とする「限定的な侵入」である点に違いがある。ここで，「全面的な侵入」という点に着目すれば，ＩＴシステムの全体並びにその中に蔵置された「すべて」のデータを対象とするオンライン捜索は，現行法上は認められていない捜査手法であると解すべきであろう。というのも，現行法の捜索は，あくまでも，個々の電磁的記録を対象とするものしか考えられていないからである。

これに対して，本稿の理論によると，オンライン捜索を，情報に対する捜索・差押えの一態様にあたるものであるということが可能である。ここで確認すると，次の２つの点が重要である。第１に，裁判所は，中華民国憲法 23 条により，自動徹底検索技術を使うオン

ライン捜索の合憲性を認めることができるが，立法者に代わって，オンライン捜索に関する立法を行うことはできないこと，第２に，仮に，裁判所が，オンライン捜索を，情報に対する捜索・差押えであると解し，これによってその合法性を認めようとすれば，計画書方策に要求される捜査の適切な範囲を最小化するための要件を満たさなければならないことである。

第３款　通信の過程に対する監視・記録

Ⅰ．一網打尽型の傍受の規制の在り方

ＩＴシステムの場合においては，分散システムが採用されるとともに，多重の転送経路という形になっていることが少なくないため，現時点の技術では，仮にＩＴシステムを傍受しようとすると，すべてのネット上の仮想回線を対象とする，いわゆる「一網打尽型の傍受」を行うしかないとされているが，こうした一網打尽型の傍受は，「傍受すべき通信」（通保法 11 条）の特定性の要件を満たさない一般的・探索的な傍受に該当する。ただし，これは，あくまで，現行法の単一段階の令状制度のもとから導かれた結論にすぎず，本稿が提案する多段階規制論によれば，その結論は，次のように変わってくる。

まず，傍受段階（取得段階）[944]では，技術上は，ネット上のあらゆる仮想回線において流れているすべてのデータをスキャンしておかなければならないという形（全面捜索）になっているが，本稿の理論からすると，前述した限定性の要求を満たすと同時に，後の段階（抽出段階）[945]の規制を用意しておくかぎり，計画書通過令状さえあれば，一般令状禁止原則に反するものではなく，それを行うことができると解されうる。ここでいう限定性要求については，次の２点が重要である。すなわち，①全面捜索の「過程」において，捜査官の五官が介入してはならないこと，及び②全面捜索の「結果」は，非物理的な（蓋然性に関わる）限定要素[946]により指定された対象のみを確保（仮差押）するという仕組みでなければならないことである。

このうち，①は，かような過程において，情報システムの不可侵性及びそれを前提とし

---

[944] 取得段階とは，傍受しようとするメールから分解されたパケットを取得するために，適切なツールを用い，インターネットにおけるあらゆる仮想回線を流れているすべてのパケットをスキャンしながら，その中から，行き先や種類などを指定の上，指定したパケットのみを抜き出して保存するという「監視・記録の段階」（すなわち，傍受段階）をさす。

[945] 前注において述べたように，取得段階において保存されたパケットは，傍受しようとするメールから分解されたパケットとそうでないものとが混在しているものであるから，当然なことではあるが，そのままでは，捜査に役立つ情報にはならないので，その後，目標たるメールを構成するパケットを割り出したうえで元のメールに復元するために，コンピュータ・フォレンジック作業を行い対象となるメールから分解されたパケットのみを抽出しておく作業が必要となる。この段階を，「抽出段階」と呼ぶ。

[946] 非物理的な限定要素とは，①捜索の対象とする情報システムの技術的な特性，②利用しようとする侵入・探索ツールの技術的な特性，③探知の対象とする情報及び探知に伴いやむを得ず開示されうる探知の対象でない情報の範囲と性質，という３つのものをいう。

たシステムデータの要保護性(擬制的なプライバシー)は侵害されるおそれがないことを，法的にも技術的にも保障しなければならないことを要求するものである。また，②については，現時点の技術では，対象となるメールに関わるパケットのみを精密に指定することは困難であるが，メールの送り先ないし到達先などの限定要素を指定することができる。この意味で，この傍受段階は，蓋然性による差押えの性格を有するものであるといえよう。というのも，送り先ないし到達先などの(蓋然性に関わる)限定要素による指定は，現行台湾刑訴法 135 条 1 項 2 款の規定(「被告人から発し，または被告人に対して発した郵便物……」)とは同工異曲のものだと考えられるからである。よって，ここで適用されるのは，「仮差押令状」(蓋然性による差押え)であり，その後に対象たるメールを割り出すため(抽出段階)には別個の情報に対する捜索令状が必要となる。そして，かような捜索令状を申請するには，捜査機関は，この章に論じた要件の揃った捜索計画書を作成しそれを令状発付裁判官に提出しなければならないことになる。

Ⅱ．ブログを対象とする場合

インターネットの傍受は，メールに対する傍受だけではなく，例えば，ブログに対する傍受もその典型例として考えられる。以下は，本章の【例 7】に関して提起した，ブログを傍受の対象とする事例に関わる理論上の諸問題点につき，本稿の理論から改めて検討すると，次のようなものとなる。

1．「通信」の新しい意味

従来の理解によれば，通信傍受でいう「通信」とは，「特定個人間の閉ざされた情報の受送信」と理解されてきた。その根拠は，おそらくプライバシー権に求められていると思われる。というのも，「特定個人間の閉ざされた情報」の反対概念としては，「不特定個人間のオープンされた情報」があげられるが，「不特定個人間のオープンされた情報」に対してはプライバシーを主張することができず，通信の秘密の保護からは除外されると考えられてきたからである。しかし，ここで問題となるのは，インターネットの通信の場合は，そもそも「特定」及び「閉ざされた情報」という２つの要件を満たさないという点である。

以上に対して，本稿の理論に基づいて考えると，次のようになる。まず，「情報の終局的処分権」については，たとえ個人のプライバシー(私的な情報)と全く関係ないものであっても，個人が当該情報を完全に破壊し棄ててしまう(つまり，デリートすること)という終局的処分権を依然として有しているかぎり，かかる権利の保護を主張することができる。

また，「情報システムの不可侵性」については，それは，物理的な空間における人の活動ないし関連事象という点に特徴付けられるプライバシーの領域の不可侵性とは全く異なるものであり，不可侵性を有する情報システムであるならば，そのシステム内のすべての

情報が保護されるものになる。この意味で，システム内のすべての情報をプライバシー情報と見なすということができるとすれば，それを「擬制のプライバシー」と称してよかろう。

このように，通信傍受でいう「通信」を，本稿の理論から再定義すると，「特定」及び「閉ざされた情報」という２つの要件は必要でなくなることがわかろう。というのも，本稿の法益論は，プライバシーの利益とは無関係なものであるから，かような２つの要件をもってプライバシーとそうでないものとを区別したうえで保護すべきプライベイトな領域を画定する必要はなくなるからである。本稿の理論からすると，あるべき判断の基準は，①かかる通信情報に対して終局的処分権を有するか，及び②かかる通信が流れているシステムは不可侵性を有するのか，という２つの点にある。この２つの基準に従い，【例 7】の問題点を再検討すると，次のようになる。

まず第１に，インターネット上誰でもアクセスできるように設定されている場合であるが，本稿の法益論からすると，かような設定がなされたからといって当然に任意処分にあたるという帰結になるわけではない。というのも，本稿の理論のもとにおいては，「特定」及び「閉ざされた情報」という２つの要件は不要となり，かつ，現在の技術では，ある情報について，コピーはできず，アクセスしたり閲覧したりすることのみが認められるように設定することが可能だからである。つまり，被処分者が，アクセスについては公開設定を行ったが，それにより誰でもアクセス可能な情報については，技術的手段をもってその複写を禁止している場合であるならば，かかる情報に対して情報の終局的処分権を主張することができるのである。

第２は，アクセス権限の設定がかけられている場合である。この場合に被処分者となりうる者としては，①発信者(受信者でもある。というのも，アップロード完了後画面の表示はまた自分宛に戻るからである)，②通信業者(発信者のプロバイダー)，③発信者が許容した複数のアクセス権限者，④複数のアクセス権限者のそれぞれが契約したプロバイダー，の４つのものが考えられる。従来の考え方からすると，プロバイダーなどの通信業者を通信当事者とすることには違和感があるかもしれないが，本稿の理論からすると，重要なのは，情報の終局的処分権の有無及び情報システムの不可侵性の有無という２点であるから，通信傍受法でいう通信の当事者という概念を使う必要はなくなるので．以上の４つのものはいずれも傍受の被処分者となりうるのである。

最後は，「非公開」設定の場合である。こうした場合，発信者には誰かを相手にしてコミュニケーションをする意思は全くなく，その意味で，物理的な日記や個人の書類などの有体物とは異ならないので，それを，双方向性のコミュニケーションと理解されてきた「通信」と解すことは困難である。しかし，これはあくまで，現行法の通信の当事者という概念から導かれた結論に過ぎないのである。本稿の理論からは，重要なのは，情報の終局的処分権の有無及び情報システムの不可侵性の有無であるから，通信傍受法でいう通信の当事者という概念を使う必要はなくなるので，誰かを相手にコミュニケーションをする意思

があるかどうかという点は重要でなくなる。それゆえ，そのような意思がない「非公開」設定の場合も，本稿でいう通信傍受の対象となりうるという帰結になる。

２．自動的受信応答の新しい法的位置づけ

従来の理解によれば，通信傍受でいう通信は，必ずしも人と人との間の通信を意味するものではなく，コンピュータによる自動的受信応答等を行う場合も含まれると解されてきた。しかし，かような理解が多重転送の仕組みを持つインターネットの場面に適用されると，技術的な理由により設定された経由点としての自動送受信のコンピュータは，通信の内容とは何らの関係もなく単に転送するために経由点として利用される中継サーバーであるにすぎないにもかかわらず，その管理者も通信当事者になってしまい他人の通信に対する傍受に同意することができるという不合理な結論に至る。

一方，かような結論を避けるため，中継サーバーの管理者を通信の当事者ではないと解すると，自動的受信応答の位置づけについて解釈論上の一貫性を欠くと同時に，ハッカーが攻撃の発信源を隠匿するために行う自動受信応答などの場合に不都合が生じてくる。

このジレンマを本稿の理論から検討すると，次のようなものになる。

まず，プロバイダー契約及び経路の設計ゆえに，最初の発信者Ａが，通信の相手であるＦに送信するために，ＢＣＤＥの４つの中継サーバーを経由しなければならないというような例では，ＢＣＤＥの管理者は捜査機関による傍受に同意できないという結論が導かれる。なぜならば，それらはいずれも，通信情報の内容とは何らの関係もなく，単なる技術上の理由で経由点とされた中継サーバーに過ぎず，転送する情報に対して終局的なデリートを主張できないので，情報の終局的処分権を持たないものと解されるはずだからである。

他方，多重転送の設定が，技術的な理由によるものではなく，ハッカーが攻撃の発信源を隠匿しようとするなどの理由で行われた場合には，ＢＣＤＥは，いずれも同意できるという結論になる。なぜならば，それらはいずれも，情報システムの不可侵性という法益を侵害された被害者だからである。こうした場合において，ＢＣＤＥは，ハッカー攻撃の目標となる被害者ではないが，それらのシステムをハッカーにより勝手に利用されたことから，システムの不可侵性を侵害されたといえるとすれば，ハッカーの仕業により，勝手に自分のシステムに跳びこんでくる通信の情報(コード)をデリートする権利及びかような侵害状態を原状に戻させる権利(すなわち，情報システムの不可侵性を維持する権利)をもっているということができるからである。このように，本稿の理論によれば，前述した現行法のジレンマが解消されると同時に，解釈論上の一貫性も維持される。

第３章　新制度の内容

第１節　まとめ

第１款　新たな法益論について

本稿の法益論と従来の法益論の異同を比較しながら，情報を独立した強制処分の直接の対象とすることにより保護される法益は何なのかについての結論をまとめると，次のようになる。

Ⅰ.既存の基本権との関係

情報を独立した強制処分の直接の対象とすることにより保護される法益は，「情報システムの不可侵性」及び「情報の終局的処分権」という２つのものである。前者は情報を捜索の対象とする場面に対応するものであるのに対して，後者は情報を差押えの対象とする場面に対応するものである。この２つの法益論に基づく本稿の考え方と，物が処分の対象である制度を前提としたプライバシー権論，物権論ないし情報自己決定権論などの理論との間には，以下のような差異がある。

１．プライバシー権論との差異

まず，物が強制処分の対象となる場合の保護法益であるプライバシーと，情報が強制処分の対象となる場合の保護法益であるプライバシーの差異としては，以下の点があげられる。

物が強制処分の対象となる場合の保護法益であるプライバシーは，プライバシー領域と評価される物理的な空間における人の活動ないし関連事象によって特徴付けられる。かかるプライバシー権は，プライバシー領域と評価される物理的な空間さえ観念できれば，それへの有形の侵入であるか無形の侵入であるかを問わず，それらに対する保護を提供することができる。しかし，一旦プライバシー領域にあたる物理的な空間を観念することができなくなると，その保護を提供することもできなくなる。

これに対して，情報が強制処分の対象となる場合の保護法益であるプライバシーとは，「擬制のプライバシー」ともいうべきものである。というのも，この場合は，プライバシー領域にあたる物理的な空間を観念することができないため，その要保護性の核心は，プライバシーではなく，情報システムの不可侵性に置くべきであり，不可侵性を有する情報

システムであるならば，そのシステム内のすべての情報が保護されるものになるからである。この意味で，システム内のすべての情報をプライバシー情報と見なすものであるため，「擬制のプライバシー」と称しうるわけである。

２．物権性からの離脱

有体物を処分の対象とする場合，その権利侵害の有無，裏返していえば権利の要保護性の有無を判断するためには，物理的な侵入(侵害)を必要条件としないが，物権性[947]という点から完全に離れるわけではない。例えば，銀行が保管する個人の取引に関する紙媒体の商業記録は第三者の銀行の所有物である以上，銀行の所有物に対する捜索・差押えを行う場合は，情報主である銀行の顧客は何らの権利も主張することができないという帰結になる。

確かに，台湾では 2001 年の刑訴法改正により，電磁的記録も捜索・差押えの対象とされているため，学説上は，電磁的記録の場合には，捜索の定義につき，「合理的なプライバシーの期待に対する侵害」という要素だけでよく，「物理的な侵入・探索」という要素は不要であるとする見解がある。しかし，前掲の例は，紙媒体の商業記録を対象とするものであって，電磁的記録とは無関係のものである。

また，電磁的記録の場合であっても，差押えの定義は依然として占有の剥奪とされているし，また，電磁的記録媒体という有体物の利益と同媒体に記録された無体の情報の利益とが競合する場合には，現行法のもとでは，媒体という有体物を優先する点は，2001 年の法改正以後にも変わらないから，結局のところは，電磁的記録と関係する事例――例えば，電磁的記録の形での商業記録やプロバイダーなどの通信業者が保管するデジタルの形での個人の通信記録など――においても同様に，情報主である銀行の顧客やプロバイダーのユーザーは，何らの権利も主張することができないという帰結に至るのである。

他方で，これとは別に，物に記録等された情報の持ち主と物自体の持ち主(所有者)が同一人物であるが，占有者と所有者が別人である場合もある。この場合につき，日本の最決平成 21 年 9 月 28 日刑集 63 巻 7 号 868 頁が格好の事例としてあげられよう。本決定(以下，「平成 21 年決定」という)によれば，合法的に荷物を占有した宅配便業者が捜査機関による借り受けとエックス線検査について承諾したにもかかわらず，本件のエックス線検査は，検証としての性質を有する強制処分に当たるものとされる。

本決定につき，学説には，「捜査機関によって制約される主たる利益が封緘された荷物の『プライバシー』であり，そのプライバシーが荷送人・荷受人のみに帰属している以上，荷送人・荷受人のプライバシーがその意思に反して制約される点で強制処分に該当していると考えたのであろう」[948]とし，「このことは，財産を占有・所持しているだけでは，直ちにプライバシーの利益の放棄が許されるわけではなく，任意提出に基づく領置が常に正当

[947] ここでいう物権性は，民法上の物権より広い概念で，占有などの財産上の利益も含まれる。
[948] 緑・対物的処分と強制処分性 155 頁。

化されるわけではないことを示唆する」[949]とする見解がある。

しかし，平成 21 年決定は，物のみを処分の対象とする日本の現行法の枠内で十分に説明ができるものであると考えられる。というのも，宅配便業者は当該荷物に対して何ら物権的な権利ないし利益を持たず，かつ，かかる法律上の利益関係は外見から一見明白である以上，所有権者である荷送人あるいは荷受人の物権的な権利や利益が優先されることになるからである。

このように，平成 21 年決定の事案では，荷送人や荷受人はかかる荷物に対して財産法上の最も強い物権，すなわち所有権を主張することができる者であるのに対して，前述した銀行やプロバイダーの例では，それらの顧客は銀行が保管する個人の取引に関する商業記録ないしプロバイダーなどが保管する個人の通信記録に対しては何らの物権的な権利ないし利益も主張できない。つまり，平成 21 年決定が荷送人や荷受人のプライバシーの利益を重視していることはその通りであるものの，そのプライバシーの保護の根底にあるものは，プライバシーそれ自体よりは，むしろ有体物である荷物に対する財産上の権利をもつ者を保護しようとする点にある。この意味で，本件も有体物の物権者を優先するという従来の考えに基づくものと考えられるのである。

他方で，日本の最決平成 20 年 4 月 15 日刑集 62 巻 5 号 1398 頁は，ごみにもプライバシーの期待がありうることを認めつつも，公道上のごみ集積所に出したごみである場合，かかるごみへの占有(物の所有権)が放棄されている以上，誰の承諾も得ずに遺留物として領置した捜査機関の行為が適法であると判示している。言い換えれば，情報主に，当該ごみについてのプライバシーの期待があるとしても，かかるごみに対して何ら財産的権利(所有権や占有権など)を主張できない以上，プライバシーの保護を与えないということである。

確かに，以上示した２つの日本の事例を台湾の場合に当てはめて再考すると，台湾の解釈論としても，同様に，強制処分の対象が有体物である場合には，何らかの物権的な権利ないし利益に依存していることを前提にすれば，無体の情報にかかわるプライバシーを保護することが可能であろう。しかし，情報の持ち主が，かかる有体物(記録媒体)に対して何らの財産的利益も主張できない場合が問題となる。かかる問題を解決しようとすれば，物と並んで，情報をも独立した処分の対象としなければならないと考える。というのも，本稿が提案するように，電磁的記録のみならず，あらゆる情報を独立した処分の対象とすれば，物権性を優先するという現行法の建前は崩れ，法的には，物と情報との衝突ないし競合関係を調整するための制度を用意しなければならないことになるからである。

以上をまとめれば，情報が処分の対象となる場合の保護法益はプライバシーに限らないが，それを含んでいる。そして，情報が処分の対象となる場合のプライバシーの要保護性の判断は物権性(または財産権性)に左右されないのに対して，物が処分の対象となる場合のプライバシーの要保護性の判断は物権性に依存するということになる。

---

[949] 同前注 156 頁。

３．情報自己決定権との差異

最後に，本稿の「情報の終局的処分権」「情報システムの不可侵性」と，従来の「情報自己決定権」とを比較する。

このうち，前述した通り，情報システムの不可侵性は，情報が存在している一定の物理ないし非物理的なスペース(システム)に対しては直接の保護を与えるものであって，個人が個々の情報に対するコントロール権に保護を与えるものではない点で，情報自己決定権とは異なることは明らかである。

また，情報の終局的処分権と情報自己決定権との差異を説明するには，台湾における情報自己決定権に対する理解を確認しておく必要がある。この点，自己情報決定権はプライバシー権から派生する権利であって，プライバシーに関わる私的情報のみを保護の対象とするものであるとする見解と，自己情報決定権はプライバシー権と独立した別の基本権であり，その保護の範囲は私的情報に限らないとする見解とが対立している。前者の見解によると，自己情報決定権の保護を主張するには，「私的情報／非私的情報」の区別を前提としなければならないのに対して，後者の理解からすれば，かような区別は不要となる。

これに対して，本稿の理論によると，情報の終局的処分権(デリート権)はプライバシー権ではないので，保護されるのはプライバシーに関するものに限定されないことになるし，また不可侵性をもつ情報システムの全域におけるあらゆる情報を保護するものとするから，その点で，「私的情報／非私的情報」の区別を前提としている前者の理解した情報自己決定権とは，明らかに異なる。そうであるがゆえに，これにより，ＩＴシステムにおいては私的データとそうでないデータとを区別するのが現時点の技術では不可能であるという前者の見解が抱えている難点を解消することができる。

さらに，後者の見解と比較すると，確かに，あらゆる情報を保護の対象とするから「私的情報／非私的情報」という区別が必要でなくなるという点では，本稿の主張と同じものであるようにみえるかもしれない。しかし，同見解は，情報自己決定権の内実をなす必要な要素としては「自主的なコントロール権」をあげているのに対して，本稿のいう情報の終局的処分権の中身は当該要素を必要としないのである。

こうして，コントロール権は漠然した概念であるという指摘も，本来コントロールできない性質をもつ知識･情報をコントロールする対象に取り入れようとしているところに本質的欠陥があるという批判も，本稿の提案する終局的処分権には妥当しないのである。具体的には，まず，自主的なコントロール権という概念についての理解は，論者によって若干微妙なニュアンス上の差異があると思われるが，一般論としては，それが，自己情報の取得・収集から保有・管理・利用を経て，その開示・提供に至る一連の「情報流通の流れ」についての情報主体の同意権ないし決定の自由を意味するものであるとされる。しかし，このコントロール権による権利保護の守備範囲が，「情報流通の流れ」の全般にわたるものであるとすれば，個人が，かような「情報流通の流れ」に対して，果たして自主的にコ

ントロールする権利をもつのかには大きな疑問があるし，とりわけ，情報主体が自己の情報を任意に他人に提供した場合においては，かかるコントロール権を失うという理解が，むしろより素直なものではないかと思われる[950]。

これに対して，本稿が提案する情報の終局的処分権は，「情報流通の流れ」についての情報主体の「同意権」ないし「決定の自由」とは全く異なるものである。つまり，情報の終局的処分権とは，差押えの場面に対応する法益であり，その内実は，財産に対して終局的にそれを処分する権利(すなわち，破壊する権利)に匹敵するものであり，情報に対して終局的にそれを処分する権利(すなわち，デリートする権利)のみを指す。そのうえで，同法益の保護を主張するには，「情報を取得(複製・記録)するには，情報の構造における一定の『構文』要素並びに当該『構文』要素により定着させられた『意味』要素のみを複製・記録することであり，複製・記録の過程において『語用』要素の介入により『構文』要素が改変されてはならない」ことを前提にしなければならない。そして，同法益の権利保護の守備範囲は，「情報流通の流れ」の全般にわたるものではなく，専ら政府が強制的に情報を取得・保有する場面に限定される。それゆえ，情報の終局的処分権論のもとにおいては，自己の情報を任意に他人に提供した場合などの問題は生じないし，また，漠然としたコントロールという用語を使う必要もなくなるのである。

Ⅱ．物と情報の両者の保護の程度について

最後に，情報を強制処分の対象とする場合の法益と，物を強制処分の対象とする場合のそれとの保護程度は同じにすべきである。なぜならば，前述した通り，終局的処分を行う権利が政府に剥奪されるという点に照準を合わせると，強制処分の対象が物であっても情報であっても，その要保護性の構造は同じであるから，憲法上，両者に同様の保護が与えられるべきだからである。

第２款　「情報に対する捜索・差押え」という制度について

最後に，本稿の核心となる検討課題であった「情報令状の在り方」に関わる諸問題についての結論をまとめる。

---

[950] See Adler at 1111(邦訳はアドラー(著)新保史生(訳)198 頁参照)。佐藤・権利としてのプライバシー162 頁で挙げた具体例についての説明をも参照されたい。

Ⅰ．強制処分の対象としての情報

まず，(独立した)強制処分の(直接の)対象としての「情報」という概念の具体的な中身は，「定着させられた一定の記号の組み合わせの集合」と定義される。

そのうえで，情報を強制処分の対象とすることの可能性については，物を対象とする場合と同様に，情報についても支配・管理可能性を必要とする。そして，情報は物と異なり，物理的な特徴を持った定着性はないものの，非物理的な特徴を持った定着性がある。ここでいう「非物理的な特徴を持った定着性」とは，「情報の定着性の３層構造」を指す。それは，第１層：「記号の組み合わせの集合」自体が「一定の構文」により定着させられたものでなければならないこと，第２層：「記号の組み合わせの方式」は「一定の法則」により定着させられたものでなければならないこと，第３層：「記号の組み合わせにより表れる意味」は一定の法則に基づきなされた一定の「記号の組み合わせの集合」により定着させられたものでなければならないことを意味し，この「３層構造」により非物理的な支配・管理が可能となる。

Ⅱ．情報の差押え・捜索といえるための基準

次に，何をもって情報の差押え・捜索といえるかという問題については，以下のような結論になる。

１．差押えについて

情報を対象とする場合の法益と，物を対象とする場合の法益との保護の程度は同じくすべきである。なぜなら，「最終の処分」という点に照準を合わせると，物と情報の基本権としての要保護性の構造は同じである以上，憲法上両場面で同じ程度の保護を与えるべきだからである。

しかしながら，物の利用は，占有によって特徴付けられているため，排他性を有するのに対して，情報の利用には，占有を観念できず，排他性がない。それゆえ，物と情報との保護の程度を同じにすべきであるとはいえ，保護法益が侵害されたかどうかを判断するための基準は異なる。

すなわち，物を差押えの対象とする場合は「占有剥奪」という要素が必要とされてきたが，情報については，「占有剥奪」に匹敵する「情報の終局的処分権の剥奪」がなされたときに，情報が差し押さえられたといえる。そして，政府によりなされた「情報の複製・記録」が「原始の情報」との間に同一性があると見られる合理的信頼価値を有する場合に，情報の終局的処分権の剥奪が発生したといえる。

ここでいう「合理的信頼価値」は，複製・記録の過程において「語用」要素が介入していない――言い換えれば，「構文」要素が改変されていない――という場合に認められる。というのも，情報の定着性の核心である「構文」要素が改変されていない限り，合理的な一般人であれば，誰でも，当該「情報の記録」と「原始の情報」との間に同一性を有すると考えるからである。

２．捜索について

物の捜索といえるための基準は，従来，物理的な空間に立ち入り，物理的な容器を開けたり移したりするという物理的な探索活動に求められてきた。これに対して，情報を対象とする場合は，このような物理的な行動は全く現れないため，捜索にあたるか否かは，次のようなプロセスで判断される。

第１に，物理的な侵入により侵害される「住居不可侵性」という法益に匹敵する法益は，「情報システムの不可侵性」である。

第２に，ここでいう「不可侵性」の有無を判断するための基準は，合理的なプライバシー権の期待とは関係なく，「あるシステムにおいて膨大かつ多様な情報が存在する可能性の有無」でこそある。

第３に，物理的な場所に入った時点で物の捜索が開始されたといえるのに対して，情報の場合は，「情報システム内の事柄を開示し始める時点」が「情報システムの不可侵性」が侵害された時点となる。

Ⅲ．「場所・サイズ」基準以外の最小化の要素

最後に，従来の「場所・サイズ」基準の代わりに，捜索・差押えすべき範囲・対象を特定・明示するために資する基準は何なのかという問題については，次のような結論となる。

まず，従来は，「場所・サイズ」のほかに，「正当な理由」と「例示の物件」の２つの要素の組み合わせにより捜索・差押えの範囲を特定・明示するという考え方が示されてきたが，この２つの要素は，「場所・サイズ」という要素の延長線上にあるものと評価できる。これに対して，本稿は，一般令状禁止原則を，中華民国憲法 23 条から導かれた最小化原則を核心としたものであると理解したうえで，以下のように，非物理的な意味で強制処分の対象を最小化することを提案している。

１．非物理的な３要素と３基準

従来の物理的な「場所・サイズ」基準のかわりに，①捜索の対象とする情報システムの

技術的な特性，②利用しようとする侵入・探索ツールの技術的な特性(すなわち，捜索ツールの限定性)，③探知の対象とする情報及び探知に伴いやむを得ず開示されうる探知の対象でない情報の範囲と性質という３つの「非物理的な限定要素」と，㋑類型化情報による限定基準，㋺露出された情報による限定基準，㋩情報・情報システムに対する一瞬の取得・侵入の場合は基本権の侵害にならない基準，という３つの「非物理的な限定基準」を組み合わせることにより，最小化原則を核心とする一般令状禁止原則の内容が具体化される。そして，こうした３要素・３基準の組み合わせの在り方としては，計画書方策を打ち出している。

これにより，場所・サイズを観念できないＩＴシステムにおいて捜索・差押えの範囲をどう画定すればよいかという問題を解決することができる。

２．３要素と３基準の関係

最後に，前述した非物理的な３要素と３基準がどのような関係にあるのかを説明すると，次のようになる。

３要素も３基準も，非物理的な意味で捜索・差押えの範囲を劃定するものであるが，それぞれの概念をさらに区分すると，３基準は，捜査機関が行う行為が非物理的な意味での捜索・差押えにあたるかどうかを判断するための基準であり，その意味で，捜索・差押えの範囲を画定するための機能も果たす。これに対して，３要素は，ある捜査行為が非物理的な意味での捜索・差押えにあたることを前提に，かような捜索・差押えの範囲を適切に画定するために必要な要件になる。

また，３要素により対応しようとする場面としては，主に，プログラムにより情報を自動的に探索する場面が想定されている。これに対して，３基準のうち，㋑類型化情報による限定基準と㋺露出された情報による限定基準は，人間により情報を探索する場面(例えば，五官によるルック・スルー)に対応するものと考えられる。他方，㋩情報・情報システムに対する一瞬の取得・侵入の場合は基本権の侵害にならないという基準は，プログラムによる自動探索の場面にも，人間による探索の場面にも適用されうる。

こうした３要素・３基準は，計画書の内容を構成するものであるが，これらの要素と基準が必ず同時に計画書に記入されなければならないわけではない。例えば，プログラムによる自動探索という予定があるだけで，ルック・スルーの計画がない場合，㋑ないし㋺の基準を計画書に取り入れる必要はない。

一方で，計画書の内容を構成するものは，この３要素・３基準に限られるわけではない。というのも，物理的な空間であっても，従来の「場所・サイズ」による限定が失効したり，「正当な理由」と「例示の物件」の２つの要素の組み合わせによる対応が機能しなくなったりすることがあるが，こうした場合にも計画書方策により対応できる以上，状況に応じて３要素・３基準の調整を行うことが可能であり，かつそうすべきであるし，また，その

後の科学技術の進展により，新しい要素ないし基準を作り出す可能性も否定されないからである。

第２節　多段階令状制度の応用

続いて以下では，いくつかの重要な事例をとりあげ，現行法との対照という形で，本稿が提案する多段階令状制度による対応はどうなるのかを敷衍する。

第１款　捜索の例：集合物の全体を対象とする場合

ここでいう集合物には，動産のみならず，不動産も含まれる。前者は，貸金庫やコインロッカーがその例としてあげられ，後者は，集合住宅のマンション，大学の構内，ホテルなどが典型例である。これらの例は，その適法性を判断するうえでの争点は同じであるから，以下では，「捜査機関が，『〇〇大学内研究室棟』を捜索すべき場所として捜索令状の発付を請求した場合に，裁判官はそれに応じることができるのか」という設例で代表させる形で検討を行いたい。

このような事例で，台湾においてこれまでは，現行法のもとで当然に認められるものとして行われてきている。確かに，「〇〇大学内研究室棟」などの大型集合物の建物を捜索すべき場所として捜索令状の発付を請求した場合，捜査官が，その建物の構内の様子を知ることが非常にむずかしいから，こうした状況の中で，個々の捜索場所の占有，管理状態がどうなっているかを捜査したうえで，場所ごとの令状請求をするということは，まず不可能といっても過言ではないであろう[951]。そうであるがゆえに，物理的な区切りがなされた複数の独立した場所からなる大型の集合物を捜索すべき場所として１通の捜索令状の発付請求を認めてきている実務上のやり方には理由があったかもしれない。

しかし，本稿の理論からすると，対象となる捜索すべき場所の占有，管理状態を事前に掌握しかねるという問題状況と，蓋然性による差押えの場合のそれとは同様なものと考えられ，第２章に挙げた「仮差押令状」の発付要件に該当するから，研究棟に対する一般的・探索的な性格をもつ捜索・差押令状は発付されてはならず，まずは仮差押を行っておくべきということになる。

具体的には，大学研究室棟に対する仮差押令状を請求し，それにより，研究室棟の全員を退室させたうえで，立ち入り禁止処分をすることにより，当該棟に対する占有を一時的ではあるが完全に警察官の支配のもとに置くことができる。というのも，差押えという制度が不動産にも適用されるという従来の理解は，本稿の理論のもとでもそのまま維持され

[951] 石毛・令状問答 19 頁，東京地決昭和 45 年 3 月 9 日刑事裁判月報 2 巻 3 号 341 頁（和光学園事件）を参照。

るものであるし，また仮差押令状という制度の本旨は，占有の剥奪ではなく，証拠保全にあるので，具体的な差押えの態様ないし手段は，対象となる物ないし情報の状況に応じて証拠価値を保全できるようにすればよいからである。

そして，仮差押である以上，捜査官が当該棟に対して当然に捜索することはできず，仮差押えをした後の捜索をするためには別個の令状を申請する必要がある。その際には，第２段階の捜索計画書令状審査を受けなければならない。この段階に関しては，第２章で論じたように，仮差押が実施された以上，証拠隠滅のおそれはないから，それを対審構造にすることが可能であり，かつそうべきである。そのうえで，対象となる学生ら並びに大学側の関係者にも出席してもらって，個々の捜索場所の占有・管理状態がどうなっているかという点を明らかにするのは困難ではないと思われる。

すなわち，捜索すべき場所は，「対象となる学生らが行動した空間」に限られ，そして，大学側証人の供述および被疑者の供述により，「研究室棟内の学生の自由にされていなかった場所」とそうでない場所を区別することができ，「研究室棟内の学生の自由にされていなかった場所」は，「対象となる学生らが行動した空間」に当たらず，本件の捜索の範囲外となる。

以上のとおり，捜索すべき場所である個々の研究室を特定するのが困難ないし不可能であるというような場合には，現行法によっては対応できないという問題は，本稿が提案する仮差押という制度により解消される。これに対し，捜索すべき場所である個々の研究室を特定するのが困難ないし不可能である場合には，令状の発付自体を抑制すべきという指摘がある[952]。この指摘は，台湾における現行の単一の令状制度のもとにおいては，正しいものと評すべきであろう。しかし，そうすると社会通念にそぐわない結果をもたらすというジレンマがある。本稿の理論によれば，前段階の蓋然性による差押え(すなわち，仮差押)は，あくまで証拠保全のための仮処分であって，その後の段階には別個の捜索令状を必要とするから，令状発付自体を抑制すべきという結論に至ることはないので，かようなジレンマが解消されるのである。

第２款　差押えの例：捜査を目的とした撮影・録画

続いて，以下では，捜査を目的とした撮影・録画という差押えの例を取り上げたい。

Ⅰ．仮差押えとその後の規制

台湾では，現行法上，捜査を目的とする写真撮影・録画を行うための明文の根拠がないが，これまでは，公道上などのオープン領域で行われた場合は任意処分として行われてき

[952] 杉原(4)146 頁。

たのに対して，それが住宅などのプライベイトな領域で行われた場合には，捜索(差押え)令状を執行するために必要な処分，または，検察官による無令状の検証であると解されてきた。

これに対し，本稿の理論からすると，情報の終局的処分権が剥奪されたといえるかぎり，公道上で行われた場合であれ，住宅内で行われた場合であれ，それらはいずれも強制処分である情報に対する差押えに該当するものとなる。というのも，情報の終局的処分権という法益は，プライバシー権とは別物だからである。

また，現行法のもとでは，発生していない犯罪に対する捜査の可否について争いがあるが[953]，本稿にとっては，この点も，そもそも問題にはならない。というのも，「関連性＝蓋然性」という構造に基づく最小化原則による実質的保障説を基盤にした多段階令状制度のもとでは，もっとも重要なのは，中華民国憲法 23 条の最小化原則により基本権に対して提供された従来の保護の内容ないし程度が縮減されることはないという保障を，法により実質的に担保できるかという点にあるからである。かような実質的保障を担保できる後の段階に対する法的制約がなされるかぎり，前の段階においては，一定の犯罪嫌疑，関連性，特定性の３つの要件にこだわる必要はない。

それゆえ，ある犯罪が未だ行われていないが，一定の事実に基づきかかる犯罪が実行されることの蓋然性があり，かつ，写真撮影や録画による証拠保全の必要があると認められるときには，捜査機関は，仮差押令状を申請し，それをもって設備を架設したうえで，撮影ないし録画を開始し，犯罪発生に備えることができる。

そして，この仮差押令状は，あくまで，証拠保全のために認められるものであるにすぎないから，その後，録画・撮影した記録テープやHDなどの内容を確認するためには，「関連性を確認するための捜索令状」を請求しなければならない。その際には，かかるテープやHDに記録された情報は疎明資料にはならず，捜査官は，別途行った聞き込みや見張りなどの手法によって入手した資料をもとに作成した「関連性を確認するための捜索計画書」を，令状発付裁判官に提出しなければならない。

Ⅱ．蓋然性を確認するための措置

仮に，捜査官が，写真撮影ないし録画による証拠保全と同時にその保全(撮影・録画)の過程に対しても五官による監視を行う必要があると考えるきには，仮差押令状だけではたりず，それを申請する際に，同時に，「蓋然性を確認するための捜索令状」の発付を請求しなければならない。そして，その際に，撮影・録画による証拠保全を行うと同時に，その撮影・録画の過程を監視(捜索)することを必要とする理由を具体的に疎明しなければならない。そのうえで，かかる監視(捜索)に伴いやむを得ず開示されうる捜査の対象でない

[953] 鄧湘全・通訊監察 102 頁 108～109，111 頁参照。

情報の範囲と性質を具体的に示すと共に，これらの情報が仮に開示されたとしても，「その他の態様での継続的な侵害の蓋然性」がないようにする技術的・法的な担保が提供されている点をも説明しなければならないものとする。

第３節　新制度の採用に伴う調整

第１款　令状によらない検証の廃止

「物・情報に対する捜索・差押え」という制度の導入に伴い，現行の強制的な捜査手段の一種としての検察官による無令状の検証という制度は必要でなくなり，廃止すべきという帰結になる。というのも，これまでかような検証の手法により処理されてきた各々のケース(例えば，コンピュータ・ネットワーク捜査，写真撮影，ビデオカメラ撮影，エックス線のスキャンなどの捜査手法)のいずれについても，かかる制度のうちの，「情報に対する捜索・差押え」という部分により対応することができるからである。

第２款　新たな救済論について

ここで，次の３点を取り上げる。

第１は，従来，執行中及び執行終了という２つの段階に分けて救済論が論じられてきたのに対して，本稿は，令状発付段階，執行中及び執行終了という３つの段階での救済論を構築すべきであると考える。

第２に，執行中，立会人などが令状をもとに不当・違法の執行に対して異議を申し立てることが認められているが，現場での異議を実効化する規定がないという問題がある。そこで，現場での異議を実効化する規定を用意すべきである。

第３に，従来，事後救済という制度を構築するには差押えのみが対象であることを前提にされてきたが，本稿の理論によると，捜索の場合にも事後救済を与える必要がある。

Ⅰ．令状発付段階での救済論

従来の執行中及び執行終了という２つの段階に加えて，令状発付段階での救済論を構築すべきとする理由は，仮差押え後の段階である計画書通過令状審査手続の構造を対審化することは可能であり，かつ，そうすべきであるという点に求められよう。

しかしながら，ここで，問題となるのは，捜査側の専門家が提出した計画書を争うには，計画書通過令状審査手続の対審構造のもとで，一方当事者である被処分者に相当な専門知識が必要となり，それがない限り，計画書通過令状の発付手続を対審化させたとしても意味がないという点である。

それゆえ，救済を実効化するために，次の２点を提案したい。第１に，一般の被処分者ないし依頼を受けた弁護士も利用できる，中立かつ権威ある鑑定機構を設けること[954]，第２に，当該鑑定機構を利用するために必要かつ合理的な費用に関する規則を定めると同時に，貧困などの理由で費用を負担できないような場合においては，国による補助に関する制度を整備しなければならないことである。

Ⅱ．現場での異議の実効化

現場での異議を実効化する規定として，執行中，電信設備ないしモバイル通信を利用し，捜査機関ないし被処分者が令状発付裁判官（またはその職務の代理人）と連絡を取れるようにすべきである。また，裁判官に対して，現場の異議に応じて即時の裁定をする権限及びかかる裁定の執行に必要な指示を行う権限を認めると同時に，救済に関する準用条項を用意しておくべきである。具体的には，次の３つの条項を法律に規定すべきである。

① 「現場の捜査員が，相手方の異議及び裁判官の裁定・指示の要旨を令状の該当欄に記載したうえ，それを相手方に呈示しなければならない。」[955]

② 「呈示を受けた相手方は，当該欄の記載を閲覧し誤りがないことを確認した後署名する。相手方が署名しない場合，該当欄を記載した捜査員が当該欄の適切な箇所にその事情を明記しなければならない。」

③ 「本法に定められた救済に関する規定は，被処分者の利益のために準用することができる。」

Ⅲ．事後救済について

事後救済は，差押えのみならず，捜索にも設けるべきである。その理由は，次の通りである。

１．取得に関する処分

台湾では，2001 年の刑訴法改正により電磁的記録という類型の情報が差押えの対象とされているが，他の類型の情報は，差押えの対象にはならないと解されているから，電磁的記録でない情報が政府に取得されただけでは，依然として差押えには当たらないため，還付（台湾刑訴法 142 条 1 項）及び仮還付（同法 142 条 2 項），抗告（同法 404 条）及び準抗告（同法 416 条）などの規定は，いずれも適用されないことになる。例えば，自分の容ぼうが政府に撮られた場合，現行法のもとでは，個人がそれに対して抗告・準抗告することができな

[954] 浅田・科学化 102 頁の説明が参考になる。

[955] この点に関して，台湾の法務部が頒布した現行の「捜索令状（発付）請求書」という書式には，「現場異議処理」という欄を追加すべきである。

いのはもちろんのこと，捜査機関が撮った写真のフィルムという有体物は政府の財産である以上，被処分者がそれに対して還付や仮還付を請求することもできない。

さらに，電磁的記録を対象とする場合にも問題がないわけではない。まず，2001 年に追加された電磁的記録という文言は，無体の記録それ自体ではなく，有体の記録媒体をさすとする見解もあり，電磁的記録がコピーされただけで，それに対して抗告ないし準抗告を行うことが，現行法のもとで果たして認められているのかについても，なお検討の余地がある。他方で，占有の剥奪を観念できない電磁的記録が政府によって取得された場合に，有体物に対する占有の剥奪を前提とする現行の還付・仮還付という制度が適用されることはないし，また，2001 年の法改正は，政府に取得された電磁的記録を削除する請求権といった事後救済の規定も用意していない。

これに対して，本稿の理論からすると，情報が政府によって取得されただけであっても，それが情報の差押えに該当するものであるといえるかぎり，還付，仮還付，抗告及び準抗告の規定が適用される。すなわち，有体物を対象とする場合でいう還付，仮還付，抗告及び準抗告という制度により救済されるのは，財産権であるのに対して，情報を対象とする場合でのいう還付，仮還付，抗告及び準抗告という制度により救済されるのは，情報の終局的処分権である。

そのうち，確かに，還付・仮還付という制度については，その前提として占有剥奪を必ず必要とするとすれば，情報を対象とする場合にはそれを観念することができなくなる。しかし，情報を差押えの対象とする場合には，占有剥奪は必要でなくなる。というのも，情報に対する差押えにより剥奪されるのは，情報の終局的処分権だからである。そこで，差し押さえられた情報の還付は，情報の終局的処分権を被処分者に終局的に返す処分であると，差し押さえられた情報の仮還付は，情報の終局的処分権を被処分者に一時的に返す処分であると定義される。

そして，差し押さえられた情報の還付の「方式」については，理論的には，政府により剥奪された情報を削除すれば，情報の終局的処分権を被処分者に返すことになる。というのも，情報の終局的処分権が剥奪された状態を解消しようとすれば，基本的には，差し押さえられた情報を削除すれば十分であり，当該情報を被処分者に引き渡す必要はないと考えられるからである。

しかし，差し押さえられた情報を削除するには，法的処分としての公示手続を必要とするから，差し押さえられた物の還付と同様に，差し押さえられた情報の還付通知書を先行させ，当該通知書において，被処分者が，一定の期間内，当該差し押さえられた情報の複写を請求することができる旨，及び一定の期間経過後あるいは複写手続終了後，差し押さえられた情報を削除する旨を明記すべきである。そして，情報を削除した後，剥奪された情報の終局的処分権がそれによって回復した旨明記する通知書を被処分者に届けなければならない。

以上は，情報のみを取得した場合である。これに対し，媒体と情報とを同時に取得した場合に情報の終局的処分権が剥奪された状態を解消するためには，差し押さえられた媒体を被処分者に還付すべきであり，被処分者の媒体に蔵置された情報を削除してはならない。というのも，還付という制度の終局的な目的は，原状回復という点に求められるからである。

他方，仮還付の場合においては，被処分者は，当該仮還付された情報を終局的に処分する権利が一時的に凍結されることになる。すなわち，仮還付を受けた被処分者には，当該仮還付された情報を原状のままで保管しなければならないという法的義務が課されると同時に，政府の再提出の命令を受けた際に，当該仮還付された情報を原状の通り提出しなければならず，かかる命令に応じない場合，あるいは，前掲保管義務に反したがゆえに命令に応じることができなくなった場合には，不利益(法的処罰や証拠認定上の不利推定効果など)が課されることになる。

２．侵入・探索に関する処分

従来には，捜索は，占有剥奪を必要とする差押えと異なり，何も奪っていないから，事後救済の制度を用意する必要がないとされてきが[956]，2001 年の台湾刑訴法改正により，差押えと並んで，捜索も抗告ないし準抗告の救済対象とされることになった。進行中の捜索がその救済対象である点には異論がないが，すでに終了した捜索もその対象であるかについては争いがある[957]。

これに対し，本稿の理論によると，事後救済の要否を判断するための基準は，①侵害が進行中であるか，及び②原状回復が必要であるかという２点に求めるべきであり，それによれば，以下のとおり，進行中の捜索にも終了した捜索にも，事後救済を与える必要があるという結論が導かれる。

(1)侵害の進行中

一定の期間にわたってＩＴシステムに侵入したり探索したりするというような事例では，被処分者に，このような捜索行為に対して抗告ないし準抗告という救済を与えるべきであろう。

これに対しては，被処分者が侵入に気づいたら，通常は捜査が打ち切られることになるはずだから，救済は不要であるとの反論もありうるかもしれない。しかし，少なくとも，ＩＴシステムへの侵入ないし電話傍受というような場合には，救済を与える必要性があると思われる。なぜなら，ＩＴシステムへの侵入や電話傍受などの場合においては，被処分者が

---

[956] 差押え処分には「(侵害の)継続性」があるのに対して捜索にはそれがないため，立法者が捜索を抗告ないし準抗告の対象から除外していた(林鈺雄捜索扣押 308～309 頁，同 308 頁脚注 7 参照。島・捜索差押 320 頁，福井・刑訴講義 5 版 159 頁。田宮編著・刑訴法Ｉ[田宮]438 頁をも参照)。

[957] 林鈺雄・捜索扣押 309 頁。

このような侵入・傍受行為に気づいたとしても，技術上の複雑さ及び困難さ並びにコストの高さを考えると，自ら捜査機関の侵入ないし傍受の行為を排除することは事実上困難であり，他方で，被処分者が依然としてＩＴシステムや電話を利用する限り，かかる捜査を継続する実益があると考えられるので，捜査機関としては，その捜査を被処分者に察知されたからといって，直ちにかような捜査を打ち切らざるをえないとまではいえないからである。

以上より，被処分者に対し，捜査機関による進行中の侵入・傍受行為に対する不服申出の権限を与えるべきであろう。というのも，被処分者が不服申出を行った時点で，捜査機関が既に事実上侵入・傍受を打ち切っているならば，裁判官は訴えの利益が存在しないことを理由に不服申出を却下すればよく，この却下処分によって被処分者を安心させることができるし，捜査機関が侵入・傍受を継続している場合であれば，訴えの利益が存在していることは明らかだからである。

(2)原状回復の必要性

次に，すでに終了した捜索に事後救済を観念することができるかを検討すると，学説上は，多くの場合，捜索は，救済を提起する際に，すでに終了してしまっているから，もし，こうした場合の捜索を事後救済の対象から排除するとすれば，それは，殆どの捜索を事後救済の対象から排除することと等しいという理由から，同条の対象には，実施中の捜索のみならず，すでに終了した捜索も含まれると解すべきであるという主張が一部でなされてきた[958]。そのうえで，終了後の捜索を対象とする抗告・準抗告については，その法的位置づけを，確認訴訟であるといい，つまり，この訴訟を提起することの前提としては確認利益(Feststellungsinteresse)を必要とされ，例えば，重複的(Wiederholungsgefahr)危険の排除[959]はその典型例としてあげられている[960]。

これに対して，本稿の理論からすると，すでに終了した捜索にも原状回復を観念することができるから，事後救済の制度を設けることが可能であるという帰結が導かれる。すなわち，原状回復の必要性について，差押えの場合には，剥奪された物の占有ないし情報の終局的処分権を被処分者に返すことにより，原状回復がなされたといえるのに対して，捜索の場合も，捜索を受けた対象の原状が変更されることはありうるから，原状回復を観念することができる。例えば，ＩＴシステムなどのバーチャル空間を対象とする場合に，侵入と監視のために差し込んだスパイプログラムの除去及び侵入によりシステムに与えた変化の回復を必要とする事例が考えられる。

以上のとおり，すでに終了した捜索を対象とする事後救済を認めることの実益ないしそ

---

[958] 林鈺雄・捜索扣押 309 頁。

[959] 例えば，同じ捜索あるいは誤り捜索が同じ対象者に対して何回も繰り返してなされる危険がある場合，同対象者が何回も繰り返した捜索あるいは既に終わった誤りの捜索に対して確認訴訟として抗告ないじ準抗告を提起することができる例があげられる。

[960] 林鈺雄・捜索扣押 309 頁。

の正当化の根拠は，原状回復にあり，違法の確認にあるのではない。なぜならば，本稿の理論によると，多段階令状の発付を請求する場合には，それを対審化することになるから，確認の利益を保護するために，事後救済という制度を設ける必要がないからである。言い換えれば，本稿の理論のもとにおいては，被処分者が，対審化された令状の発付段階において，今回の捜索には正当性が欠ける，あるいは，それが捜索の繰り返しであるという主張を行う機会が確保されており，それについての令状発付裁判官の審査がなされるのである。他方，確かに，本稿の理論のもとにおいても，単一段階の令状で済ませる事案がありうるが，こうした場合にも，事後救済としての確認訴訟を認める必要はないと思われる。なぜならば，こうした場合には，本稿が提案する現場での異議という規定が適用されるからである。つまり，被処分者が，今回の捜索には正当性がない，あるいは，今回も前と同じ捜索の繰り返しではないかと思う場合には，執行中，電信設備ないしモバイル通信を利用し令状発付裁判官と連絡をとり，異議を申し立てることができるのである。

ところで，物理的な空間を捜索の対象とする場合にも，錠を破壊したり，引き出しを開けたり，容器を移動させたりすることが予想されている。こうした場合において，理論的には，錠を修復したり，引き出しや容器などを元の場所に戻したりすることにより，原状回復することができるし，そうすべきであろう。それにもかかわらず，現行法のもとでは，かような原状回復のための救済制度が用意されていない。これは適切ではなく，立法論としては，物理空間，非物理空間を問わず，捜索にも，差押えと同様に，原状回復の救済制度を設けるべきである。また，原状回復ができない場合には，被処分者ないしその他の第三者の損失を金銭で補填する「費用償還」の制度を設けるべきである[961]。

第３款　その他の調整

「物・情報に対する捜索・差押え」という制度を採用した場合，①鑑定，②必要な処分，③緊急処分，及び④通信傍受法による通信傍受という４つの既存の制度との関係で，いかなる調整を行うべきであるのかを説明する。

---

[961] 実際にも，現行法上は合法の捜索による損害に対する補償にかかる規定が欠けているし，また，そのための予算も用意されていないから，実務上は，捜索を行うために必要な侵入行為による損害が巨大となる見込みである場合には，捜査を断念することにさせられざるを得ない例もまれではなく，例えば，差し押さえるべき物が船体を構成する板の間に隠されていると思料される合理的な根拠があるにもかかわらず，船体を破壊すると，数百万元(数千万円に相当する)の損失を引き起こしてしまう例，あるいは，差し押さえるべき物である，密かに切って盗まれた「あずき杉(Taiwan Yew；Taxus celebica Li)」(台湾では国宝とされる貴重の樹木)１本が数多くの雑木の中に隠されていると思料される合理的な根拠があるにもかかわらず，その１本のあずき杉を探すためには数多くの非常に重くて巨大な雑木を，工事用の大型の器具によりすべての雑木を一本ずつ下ろして確認しながら探していく手間が必要となるが，そのための費用は数万元ないし数十万円(十万円～九十万円位)にも上る例，という２つのものがあげられる(陳瑞仁・改革警察 65 頁)。これに対して，本稿の提案する費用償還という制度によると，これらの事例が解決されよう。

Ⅰ．鑑定・鑑識について

形式的には鑑定・鑑識ないしそれに必要な処分にあたるようにみえる捜査機関の行為であっても，それが捜索・差押えの実質をもっている限り――例えば，鑑定・鑑識の性格をもちつつも捜査の手段として使われるコンピュータ・フォレンジックが，その例としてあげられる――，物・情報に対する捜索・差押えという制度により規制すべきである[962]。

具体的には，「鑑定若しくは鑑定のために必要な処分を行うには，差押えまたは捜索の実質を有すると判断されるときには，差押え状または捜索状を必要とする」という趣旨の規定を設けるべきである。そのうえで，現行法のもとで認められている検察官の鑑定許可書を発付する権限[963]をなくすべきである。というのも，こうした場合の鑑定に必要な処分は，本稿の理論によると，差押えまたは捜索の実質を有するものであるので，差押令状や捜索令状の発付が必要となるし，また，既に指摘されているとおり，鑑定許可書に基づき鑑定に必要な処分を行うことにより身体及びプライバシーに対して与えられる侵害は，裁判官が発付する令状による家宅捜索の場合の侵害よりも大きいものがあるのに，検察官が発付する許可書だけで行われるのはアンバランス[964]だからである。

それと同時に，本稿の理論により，現行法の下で指摘されてきた以下の問題点も解決される。第１は，ＩＴシステムを捜索する際に，捜査官が行うのではなく，鑑定人としてのコンピュータアナリストに任せることができるかという問題である[965]。本稿の理論によれば，その答えは「できる」となる。但し，この場合に行われる鑑定人の行為は，形式的には鑑定若しくは鑑識にあたるものであるが，捜索・差押えの実質をもっている以上，物・情報に対する捜索・差押令状をとっておかなければならないこととなる。

第２は，一般の鑑定を行う場合においては，その鑑定すべき範囲が通常は本件に関係する部分に絞られるのに対して，コンピュータ・フォレンジックを行う場合には，鑑定の標的であるコンピュータ媒体に記録した本件に関係するデータは僅かであるにもかかわらず，技術上ないし捜査上の必要性があるために，同媒体に記録したあらゆるデータに対する徹底的な捜索を行うことが必要となる場合が少なくないという問題である。こうした場合には，被処分者が，そのコンピュータの中にあるその他のデータの秘密性を保持するため，捜査に協力しないという問題が生じる[966]。この点に配慮して，かかるコンピュータ・フォレンジックの操作を被処分者に任せることも考えられないではないが，そうすると，証拠隠

[962] 実際にも，学説上は，本稿の理論基礎と異なるものの，結論としては，「コンピュータ鑑識手続は，被処分者のプライバシー権を侵害するものであるから，その概念上は，捜索に帰属させるべきである。そこで，刑事手続上は，伝統的な捜索に対する規範と同じレベルの規範を設けるべきである」とする説がある（李・電磁紀錄 1065 頁。同 1069～1070 頁，1085～1087 頁をも参照）。

[963] 現行台湾刑訴法 204 条と同 205 の１条によると，捜査中，鑑定人が検察官による鑑定書許可書を取得しておけば，鑑定のために，身体の検査，場所への進入，相手方の血液，髪や尿などの身体の一部を構成する物質の採取などの処分を行うことができる。

[964] 李・電磁記録 1087 頁

[965] 法務部・電腦犯罪４版 56 頁。

[966] 同前注 57 頁。

滅・改ざんの恐れがあるという問題が生じる[967]。このジレンマに対し，本稿の理論のもとにおいては，２つの対応策がある。その１つは，罰則付きの間接強制処分により被処分者に捜査の協力を強制する方法であり，もう１つは，相手方が処罰を甘受し間接強制処分に応じない場合，または，協力してもらうと証拠隠滅・改ざんの恐れがあると思料される場合に，蓋然性による差押え(仮差押)並びにオンライン捜索のような迂回型の直接強制処分をとる方法である。

なお，裁判官の判断能力を補充するために，専門的分野に関する知識や判断について，裁判所の依頼に基づき，特別の学識経験を有する者に口頭又は書面で報告させる証拠方法と位置づけられてきた[968]，従来の鑑定制度と，本稿が提案する捜索・差押えとしての鑑定(捜査手法)とは併存するものである。

Ⅱ．必要な処分について

前述した通り，捜索のために必要な処分であっても，場合によって，個別の司法審査を必要とするものがある。例えば，高度の侵害性をもつ「オンライン侵入」という行為は，錠を破壊し家に侵入することと同視することはできず，計画書の中にオンライン侵入に関する予定を明記したうえで，裁判官の審査を受けなければならない。

そして，第２章で論じた通り，この点についての具体的な立法提案は，(1)個別の司法審査，(2)侵害強度の制限，(3)疎明義務，の３点である。この３点からすると，現行台湾刑訴法 144 条 1 項前段を，「物ないし情報に対する捜索状又は差押状の執行については，発付された令状により認められた当該段階の処分権限に反せず，かつ，本法が定める多段階令状の規制によって要求される実質的保障を害しない限度で，発付された令状の目的を遂行するために必要な処分することができる」と修正すべきである。そのうえで，同条に，第 2 項として，「発付された令状の目的を遂行するために必要な処分であっても，高度の侵害性を有すると判断されたときには，別個の司法審査を受けなければならない」という規定を追加するべきである。

Ⅲ．緊急処分について

ここまでの検討により，本稿は，付随差押えを定めた台湾刑訴法 137 条 1 項は次のように修正すべきであると考える。

まず，137 条 1 項の「検察官，検察事務官，司法警察官あるいは司法警察員は，捜索あるいは差押えを執行するときに，捜索令状に記載されていない本件の差し押さえるべき物を発見した場合，それを差し押さえることができる」という定めの「捜索令状に記載されていない本件の差し押さえるべき物を発見した場合」という部分を，「捜索令状に記載され

[967] 同前注。

[968] 陳樸生・刑訴(重訂十版)245 頁，最高法院 95 年台上字 6648 号判決。小磯 24 頁をも参照。

ていない本件の差し押さえるべき物が存在することが一見明白である場合」と修正すべきである。この「一見明白」という法文により，本稿の打ち出した「一番目の○○類型のファイルをクリックしてみた後関連性のないデータが判明された場合，一番目の○○類型のファイル以後の同類型のファイルをクリックして見てはいけない」という法理が採用されることになる。

そのうえで，同条項の「……場合」という文字の後には，「証拠隠滅のおそれがあり，即時に対象となる物件ないし情報を保全しなければならない事情があるかぎり」という条件を追加すべきである。それ以外の場合は，別途に別個の差押令状をとらなければならないこととなる。

以上のとおり，現行の 137 条 1 項の内容は，修正すべき箇所があるものの，基本的には本稿の関連性＝蓋然性という構造に反するものではないから，廃止すべきであるという結論に至らない。これに対して，同法 152 条の別件差押えという規定は，関連性＝蓋然性という構造に反しているから，廃止すべきである。というのも，同条によると，捜索あるいは差押えを執行する際に，別件の差し押さえるべき物を発見した場合，それも差し押さえることができるが，それでは，関連性＝蓋然性という構造による制約が全く無意味となってしまうからである。

これに対しては，廃止した場合に，別件差押えという捜査のニーズにどう対応すればよいかという疑問が生じるであろう。これについては，日本の犯罪捜査規範 154 条の「犯罪に関係があると認められる物を発見した場合において，その物の所有者または保管者から任意の提出を受ける見込がないと認めたときは，直ちにその物に対する差押許可状の発付を請求するとともに，その隠匿，散逸等を防止するため適切な処置をとらなければならない。」という定めが台湾にも参考となる[969]。

すなわち，現行の 152 条を，「検察官，検察事務官，司法警察官あるいは司法警察は捜索あるいは差押えを執行する際に，別件の犯罪に関係があると認められる物が存在することが一見明白である場合において，その物の所有者または保管者から任意の提出を受ける見込みがないときは，直ちにその物に対する差押状の発付を請求するとともに，その隠匿，散逸等を防止するため適切な処置をとることができる。」と修正すべきである。

Ⅳ．通信傍受の規制の在り方について

最後に，本稿の立場から，現行の通保法の内容を検討し，通信傍受を規制するためにあるべき立法についての私見を述べる。

まず，前述した通り，伝統的な電話回線を傍受する場合においては，１つの「ライン」(伝送・通信過程)における対象となる会話を特定することができないとしても，少なくとも，

[969] 台湾の現行法のもとにおいては，警察が捜索令状の発付を請求しながら，令状の発付をまっているところ，現場を封鎖しておくことができるのかについては争いがある。学説上は，犯罪が発生した直後ただちに現場を封鎖する場合(台湾刑訴法 230 条 3 項，231 条 3 項)を除き，現行法上はそれについての授権規定が欠けているとされる(林鈺雄・捜索扣押 35 頁。同 193 頁，258～259 頁の説明をも参照)。

対象となる「ライン」自体を特定することができるのは間違いない。これに対して，ＩＴシステムの場合においては，「ライン」さえも特定することができなくなる。というのも，ＩＴシステムは，分散システム及びパケットこう交換技術を使っているからである。それゆえ，現行の通信傍受法が，解釈上はＩＴシステムにも適用されうるとしても，その適用の前提として，傍受の対象は，特定されたある個別の「伝送過程」からのデータでなければならないとすれば，現時点の技術では，このような特定が不可能である以上，現行の通保法をＩＴシステムの場面には適用することはできないと解すべきであろう。

以上の問題を解決するため，ＩＴシステムを傍受の対象とする場合と電話回線システムを傍受の対象とする場合とを分けて，それぞれに個別的な規制を設けるという考え方もありえよう。しかしながら，情報に対する捜索・差押えという制度を構築するにあたっては，この両者を区別する必要はない。というのも，通信傍受の範囲を最小化するための手段は，「多段階規制論」と「計画書方策」に求められるべきであるから，「伝送過程」という要素による最小化が不必要となる一方，対象となるライン(伝送過程)あるいはそこからのデータを特定しておくことも不要となるので，ＩＴシステムを対象とする場面にも，電話回線システムを対象とする場面にも，同様に対応できるからである。

具体的にいかなる対応となるかを説明すると，まず第１段階において，技術的には，対象となる「ライン」を特定することができないが，法的には，「プロバイダー等の通信業者による第１段階の選別」などの制度を設けることにより，捜査機関が不特定の多数のラインを処分の対象とする問題を解決することができる。そして，多段階規制論によれば，こうした規制を正当であるといえるための前提として，その後の段階に対しては別個の令状による規制を必要とするということになる。そのうえで，その段階で令状により認められた処分の対象となる情報とそうでない情報とを選別する作業を最小化する最良策として，計画書方策と多段階令状が挙げられる。

このように，通信傍受も情報に対する捜索・差押えの一態様にあたるものであるから，多段階令状並びに計画書方策という２つの制度により規制されているので，別途に通信傍受に関わる個別の立法を行う必要はないことになる。

もっとも，立法者が，かような個別の立法を行うことは可能である。というのも，本稿が提案する「物・情報に対する捜索・差押え」という制度は，個別の立法の必要ないし可能性を否定しておらず，個別の立法の欠如や不備を補足・調整するためにも機能するものだからである。

ただし，本稿の理論と従来のそれとは全く異なるものであるから，本稿の理論に基づく個別的な立法の内容は，現行の通保法とは異なるものとなる。この点についての詳細は，次の通りである。

１．保護法益について

通説によると，通信の秘密の保障(中華民国憲法 12 条)も個人のプライバシー保護の一環

であるとされてきた[970]。それゆえに，一般論として，公開の演説や講座，会話などは，当事者自身がプライバシーないし秘密性を放棄したものといえるから，この場合の盗聴は強制処分ではないと解されてきたのである[971]。

これに対して，本稿の理論からすると，通信傍受という処分により侵害されるのは，情報の終局的処分権並びに情報システムの不可侵性という２つの法益である。そして，この２つの法益は，プライバシーではないから，「公開の」演説や講座，会話を対象とする場合ではあっても強制処分たる傍受になりうるという帰結になる。というのも，「公開」とはいえ，参加資格に関わる制限を設けることができるし，また，録音・録画を禁止したりすることができるから，前者の場合には情報システムの不可侵性を主張することが可能であり，また，後者の場合には，情報の終局的処分権に対する剥奪が発生しうるからである。

それゆえ，本稿の理論のもとでは，強制処分に該当する「公開傍受」という観念が成り立つことになる。すなわち，仮に，警察官が，参加資格がないにもかかわらず，他人になりすまして出席し，遠隔器機を利用して講演を傍受する場合には，情報システム不可侵性という法益が害されるといえるから，この場合の傍受が，「公開の講演」を対象とするものであっても，それは強制処分に該当する。また，誰でも参加できる公開の講演ではあるが，その講演の内容を録音したり録画したりすることが禁止されている場合には，それに警察官が出席し，遠隔器機を用いて聞くことにより，情報システムの不可侵性という法益が害されたとはいえないが，警察官が，それを録音ないし録画すると，それは，情報の終局的処分権という法益を侵害するものであるといえるから，こうした場合の傍受は，誰でも参加できる「公開の講演」を対象とするものの，これも強制処分にあたることになる。

そのうえで，いうまでもなく，立法者は，通信傍受法という個別立法を行うに際して，こうした公開傍受の場面を除外する裁量権をもっている。しかし，その場合に，警察官がかかる類型の傍受を行おうとすれば，本稿の提案した情報に対する捜索ないし差押令状を請求しておく必要があることになる。

２．処分の目的について

現行の通保法 3 条 2 項によると，傍受の目的は，「合理的なプライバシー期待を有する通信の内容を知る」ことに限られているので，理論的には，通信の内容にあたらない通信履歴や携帯電話の位置を探知するためには，通信傍受によるべきものではないと解すべき

---

970 司法院大法官解釈 631 号，通保法 3 条 2 項，蔡・修正後通訊監察(上)48～49 頁，陳運財・監聽 138 頁など参照。田宮・注釈刑訴 124 頁，平良木・刑訴法 I 227 頁，高橋勝・通信の秘密(1)7～8 頁をも参照。

971 陳瑞仁・改革警察 54～55 頁は「わが国は 1999 年に新設された通保法 3 条 2 項は『前項のいう通信は，事実に基づき，被処分者がその通信の内容に対してプライバシーないし秘密にかかわる合理的な期待を有する場合であると認められる者に限る』と定めている。この規定は，公共の場所に行われる秘録及び通信の一方当事者による秘録の場合を排除しようとするものである。たとえば，警察官が公共の場所において麻薬販売者とその取引相手方との対話を秘録したりあるいは警察側の依頼を受けた捜査協力者が衣服内に隠した録音機器によりかような対話を密かに録音したりするような場合には，通保法のいう傍受令状は不要である。」とする(同 66 頁をも参照)。庭山＝森井編著・刑訴法 100 講[山本]78 頁も参照されたい。

であろう[972]。日本においては，それは検証によるべきものであるとされてきた[973]。

これに対して，台湾の先行研究においては，かような探知を行うための法的根拠が何なのかは争われているが，主に，①刑訴法の捜索・差押え[974]，②刑訴法の任意処分，③警察職権行使法(警職法)11 条 1 項(科学ツールによる情報収集の権限に関わる定め)，④通保法の通信傍受，という４つのものが考えられてきた[975]。

このうち，①については，2001 年の法改正以後，刑訴法上，形式的には，電磁的記録も捜索・差押えの対象とされているから，ＩＴシステムの場合には，このように解することも可能かもしれない。しかし，伝統的な電話回線を傍受の対象とする場合には，かような解釈はできなくなる。さらに，そもそも，刑訴法でいう電磁的記録とは，無体の記録なのか，それとも，有体の媒体をさすのかについては争いがあるところであるから，①の理解自体にも，なお解釈論としての問題点が残っている。

次に，②と③の見解は，それを支持することができない。というのも，通信の内容のみならず，非内容の部分も通信の秘密に含まれるとするのが通説であるから，非内容の部分にあたる通信履歴や携帯電話の位置を探知することは，通信の秘密，つまり通信に関わるプライバシーを侵害するものである以上，それは，明らかに，「権利の侵害にならない処分」という刑訴法の任意処分の定義，及び「プライバシーないし秘密に関する合理的な期待を持たない情報のみを対象とする」という警職法 11 条 1 項の明文と矛盾するからである。

最後に，通保法の通信傍受と解する④の見解は，明らかに同法 3 条 2 項の文言に反するという問題がある。もっとも，ＩＴシステムの場合においては，分散システム及びパケット交換技術が用いられているため，伝送中のパケットをスキャンしたりキャッチしたりする段階(傍受)では技術的に内容と非内容とを区別(分割)することができないし，また，もとより，通信の内容のみならず，非内容の部分も通信の秘密に含まれるとするのが通説であるから，通信傍受の目的を，「内容を知るため」に限るべきではないとも思われる。それゆえ，立法論としては，通信履歴や携帯電話の位置を探知する行為も，通信傍受という処分の一態様になると解すべきである。

その場合，本稿は，ＩＴシステムにおいては，私的情報と非私的情報との区別が理論的には不可能であるという特徴に応じて，情報システムの不可侵性という法益を打ち出しており，かかる法益により保護されるのは，プライバシーに関わる情報に限らないから，立法論的には，通保法の保護範囲を，合理的なプライバシー期待を有する通信に限定する合理性・正当性はないという帰結が導かれる。それゆえ，通保法 3 条 2 項に定められた「合理的なプライバシー期待を有する通信の内容」という文言を，「情報システムの不可侵性という法益を有する通信」と修正すべきである。

---

[972] 安富・刑訴法 183 頁，池田＝前田・刑訴講義 4 版 201 頁脚注(31)，三浦守ほか・組織的犯罪三法解説 436～441 頁参照。

[973] 同前掲注。

[974] 黄朝義・刑訴三版 308 頁。

[975] ②～④は黄清德・科技蒐集個資 44～47 頁参照。

もっとも，立法者が，内容部分の通信の秘密に対してより手厚い保護を与えるため，個別の立法を行うに際して，その目的を「内容を知るため」に限定することは可能である。そして，こうした場合，本稿の理論からすれば，非内容の部分を探知ないし記録するには，刑訴法の検証や任意処分でも警職法の行政処分でもなく，多段階規制論を前提とした情報に対する捜索・差押えという制度が適用されることになる。

———全文完