

概要

情報の流通性の向上により、様々な恩恵が生じている一方で、情報セキュリティ上の脅威、特に情報漏洩は、現代社会で大きな問題となっている。情報漏洩というと、個人情報漏洩事件などの機密情報の漏洩がまず考えられるが、商用コンテンツの無断複製など、情報の配布元が権利を有しているにも関わらず、配布された利用者が権利者の意図に反した漏洩を行うといった事例が、情報漏洩の原因の一角を占めている。

従来の情報漏洩対策手法は、プログラム作成者の悪意の有無や脆弱性の有無、耐タンパ性といった、個々のプログラムの信頼性に依存している。しかし、プログラム作成者が自身のプログラムの信頼性を保証したり、ユーザがそれを判定することは一般的に難しい。さらに、情報の権利者と利用者とは異なる場合において、その状況を適切に表現する手段は少なく、漏洩を防ぐ方法に欠けているのが現状である。

これに対して本論文では、個々のプログラムの信頼性に依存しない情報漏洩対策手法を提案する。従来手法においては、プロセスがアクセスする可能性のある対象にはアクセスを認めざるを得ず、したがって過剰な権限を付与せざるを得ない。それらの問題に対して本論文では、プログラムのアクセス権をアクセス対象に応じて切り替えることで、プログラムの信頼性に依存しない形で情報漏洩対策が出来る手法を示す。