概要

近年，情報社会の発展とともにインタネットを通じたデータの配信が増加している．しかし，そのデータの中には機密データや著作物など扱いに制限がかかっているものもあり，それらのデータに対しては，クライアント側でデータの不正な解析や改ざんが行われないことをサーバー側に対して保証する必要性がある．そのため近年プラットフォーム認証に関する関心が高まって来ている．

TCG ではセキュリティモジュールである TPM を用いた遠隔認証を提案している．しかし，TPM を用いた遠隔認証は，認証に用いるプラットフォームの情報の完全性を確立するための制約の固さなどの問題点があり，実際には利用されていない．

本論文では，ソフトウェアによるタンパを防ぐ機能を持つ耐ソフトウェアパンパ・プロセッサを用い，さらにその機能を拡張させることで遠隔認証を可能とする手法について提案する．耐ソフトウェアタンパ・プロセッサにプロセッサと Secure DMA 専用の非発揮性メモリを追加し，さらに Secure DMA にハッシュ演算機構を追加することで，Secure DMA が転送を行いながらハッシュ値を取得できるようにする．また，耐ソフトウェアタンパ・プロセッサのアクセス保護機能や拡張 Secure DMA のメモリへのアクセスを保護することで計測したプラットフォームの情報の完全性を確立する．また，サーバーは認証の対象となるコンポーネントの計測をサポートする検証プログラムを保護データを配布する前に配布することで遠隔認証をサポートする．耐ソフトウェアタンパ・プロセッサは認証に用いる情報を保存しておき，認証後の保護データの実行時に再認証を行うことで認証後のプラットフォームの改ざんやなりすましを防ぐことができる．