2ZA-2

仮想計算機モニタを用いた クライアントコンピュータの証拠保全システムの設計と実装

小川　拡†　　平野　学‡

豊田工業高等専門学校 専攻科 情報科学専攻†‡

1　はじめに

米国では 2006 年に連邦民事訴訟規則が改正され，訴訟における電子情報開示（e-discovery）に関する法律が整備された．日本企業が米国で訴訟を起こされた場合，原告から開示要求された電子データを裁判所に提出しなくてはならない．意図的に証拠を提出しない場合には裁判所からの制裁や判決に不利となる可能性もあるため，訴訟に必要な情報を迅速かつ改ざんされていない状態で提出する必要がある[1]．米国の連邦民事訴訟規則の改正に加えて，エンロン社等の企業の不祥事から 2002 年にサーベンス・オクスレー法（SOX 法）が制定され企業経営者に対する決算情報の開示に関する規制が強化された．日本でも金融商品取引法により同様の規制が強化された．このため組織で扱われる重要なデータを適切に管理することが求められている．

本研究では，組織で特に重要な情報を管理している個人の電子データが，間違いなくその本人が作成したものであることを証明するシステムを提案する．提案システムには仮想計算機モニタをトラステッドコンピューティング基盤として利用する．実現にはストレージへの書き込みを補足して，複数のセクタ単位でハッシュ値を作成し，個人の IC カードにより電子署名を自動的に生成して保管する方法を用いる．本稿では開発途中のシステムの設計と実装を報告する．

2　証拠保全システム

開発中の証拠保全システムの処理の流れを図 1 に示す．本研究では仮想計算機モニタをトラステッドコンピューティング基盤として利用する．仮想計算機モニタを利用することで既存 OS に手を加えずに証拠保全の機能を追加する．安全の鍵となる仮想計算機モニタと証拠保全システムの実行コードが改ざんされていない状態で確実にロードされることを，Intel 社の Trusted Execution Technology（TXT）対応ハードウェアで確認することも検討する．

Design and Implementation of an Evidence Preservation System using Virtual Machine Monitor

† Hiromu OGAWA ‡ Manabu HIRANO †‡ Department of Information and Computer Engineering, Toyota National College of Technology

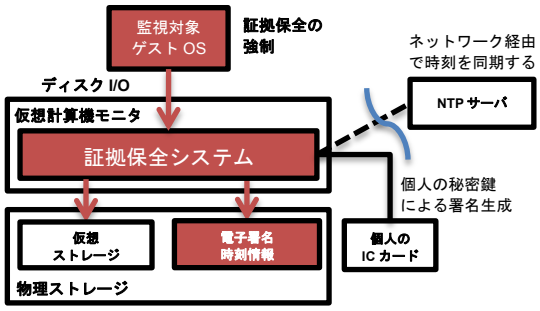

図 1　証拠保全システムの処理の流れ

提案システムの対象者は組織で重要な情報を扱う個人である．提案システムでは，組織が個人に対して証拠保全システムの利用を強制することを想定する．このために，事前に IC カードと証拠保全システムをインストール済みのパソコンを個人に配布しておく．利用者が提案システムを利用している間は，仮想ファイルシステム全体に対する電子署名を自動的に作成するため，個人が作成したファイルや電子メールなど全てについて証拠保全が行われるようになる．

提案システムは監視対象ゲスト OS が書き込みを行った仮想ストレージのセクタ位置を監視する．まず，ゲスト OS の書き込み命令をそのまま実行させることで証拠保全システムの影響を与えずに通常通りの書き込みを完了させる．一方，証拠保全システムは書き込みの発生時に該当セクタ位置のフラグを立てておき，定期的に更新のあった複数セクタ領域のハッシュ値を更新する．最終的に全てのハッシュ値を連結した内容のハッシュ値を元に仮想ストレージ全体の電子署名を作成する．電子署名は個人の IC カードに格納された本システム用の秘密鍵を用いてバックグラウンドで生成する．以上で IC カードの電子署名による仮想ストレージに対する否認防止を実現する．更に証拠保全の観点から，証拠保全システム内部の時刻を定期的に NTP サーバと同期させておき，時刻情報を含めた電子署名を作成することで，作成時刻を証明することも可能になる．

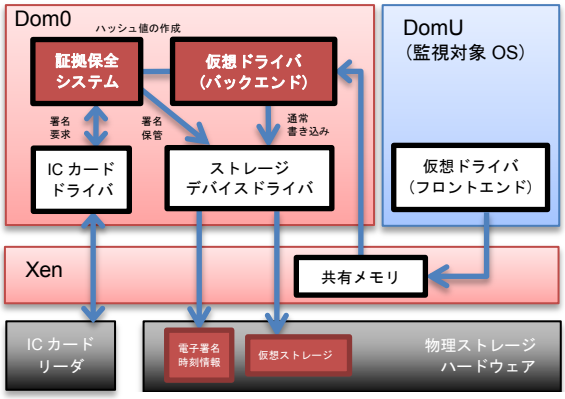

図 2　書き込み捕捉機構

3　利用例

提案システムはクライアントコンピュータにインストールして利用することを想定している．刑事訴訟や民事訴訟で物理ストレージを第三者へ引き渡す場合，電子署名と時刻情報を検証することにより証拠の真正を主張できる．検察等の捜査機関でファイルのタイムスタンプが改ざんされる事件があっても，仮想ストレージ全体に対する電子署名と時刻情報を組織が持っているため改ざんを検出できる．

4　書き込み捕捉機構の実装

仮想計算機モニタの Xen を利用した仮想ストレージへの書き込みの捕捉機構を図 2 に示す．Xen では管理用の仮想計算機をドメイン 0（Dom0），それ以外をドメイン U（DomU）と呼ぶ．提案システムでは監視対象 OS を DomU で動作させ，証拠保全システムは Dom0 の拡張として実現する．証拠保全システムを利用者の影響が及ばない領域に隔離することで外部からの攻撃を受けにくくする．Xen は DomU に対して仮想的なデバイスドライバを提供している．仮想デバイスドライバは DomU 側のフロントエンドと Dom0 側のバックエンドから構成される．フロントエンドとバックエンドのドライバ同士は Xen の共有メモリを通じてアクセス情報を送受信する．提案システムでは，仮想デバイスドライバのバックエンド部分を拡張することで DomU の書き込みを捕捉してハッシュ値を作成する．

5　ハードウェア支援

仮想計算機モニタをトラステッドコンピューティング基盤として用いる場合には，それ自身の信頼性を担保することが何より重要である．これには CPU とチップセットを含むアーキテクチャ全体のサポートが不可欠である．Intel TXT はトラステッドコンピューティング基盤（仮想計算機モニタやセキュリティカーネル）をそれらの起動段階で改ざん検出する仕組みであり，Intel 社の CPU の SMX 命令セットに含まれる SENTER 命令，Authenticated Code（AC）モジュール，Trusted Platform Module（TPM）等の連携により実現される[2]．TXT は要素技術の段階でありアプリケーションは現時点で殆ど登場していない．本研究では TXT の適用可能性を検証する．著者らは過去の研究において仮想計算機モニタ BitVisor [3] のために Static Root of Trust を用いたブート時の検証を試みているが[4]，本研究では Dynamic Root of Trust （Intel 社が Late launch と呼ぶ技術）の実装上の知見が得られると考えている．本研究ではトラステッドコンピューティング基盤実現のためのハードウェア支援に加えて，個人の電子署名を作成するために IC カードをハードウェアトークンとして利用することを述べた．実装には著者らが BitVisor のために開発した IC カードソフトウェアを活用する予定である．

6　おわりに

本研究では仮想計算機モニタを利用した証拠保全システムの設計を示した．今後は実装を進めていくことによりトラステッドコンピューティング基盤を活用したアプリケーション開発の知見を蓄積していくことを目指している．

謝辞

本研究は科学研究費補助金（23700095）の助成を受けたものである．

参考文献

[1] 町村泰貴，小向太郎，実践的 e ディスカバリ，NTT 出版，2010.
[2] James Greene, WHITE PAPER Intel TXT, 2010.
[3] Takahiro Shinagawa, et al., BitVisor: A Thin Hypervisor for Enforcing I/O Device Security, In Proceedings of the 2009 ACM International Conference on Virtual Execution Environments, pp.121-130, 2009.
[4] Manabu Hirano, et al., Portable ID Management Framework for Security Enhancement of Virtual Machine Monitors, Engineering the Computer Science and IT, IN-TECH, pp.477-488, 2009.