Vol.2010-DPS-142 No.54
Vol.2010-CSEC-48 No.54
2010/3/5

ディスク擬似書き込みと仮想マシンモニタによる機密情報閲覧作成環境の実現

栗本裕司[†1]　齋藤彰一[†1]　松尾啓志[†1]

計算機の普及にともない，機密情報が計算機上で扱われることが多くなっている．しかし，インターネットや内部不正者による機密情報の漏洩の事件が多発しており，機密情報の保護が最大の懸案事項となっている．本稿では，ディスク擬似書き込みと仮想マシンモニタによる機密情報閲覧作成環境を提案する．提案手法では，機密情報を安全に保存するために機密情報を作業 OS の外側に保存する．機密情報の閲覧作成時にはディスク擬似書き込みによるディスク書き込みの無効化とネットワークの無効化によって機密情報の漏洩を防止する．また，提案手法を実装し，性能の評価と実際の攻撃の対処法の考察した．

A Secure Environment for Sensitive Files with Pseudo-writing and Virtual Machine Monitor

Yuji Kurimoto,[†1] Shoichi Saito[†1]
and Hiroshi Matsuo[†1]

A sensitive file is regularly written and read on computers today. However many information leaking incidents are caused by insiders and attackers in the Internet. Protection of sensitive files becomes a big problem. We propose a secure environment for sensitive files by pseudo-writing and virtual machine monitor in this paper. This environment saves secure files outside of a working OS. When sensitive files are read and written, the information leaking is prevented by pseudo-writing and stopped network of the proposed system. This paper is described implementation, performance evaluations and safety of the proposed system.

†1 名古屋工業大学
Nagoya Institute of Technology

1. はじめに

現在，機密情報が計算機上で扱われることが一般的になっている．しかし，インターネットや記憶デバイスの紛失による機密情報の漏洩の事件が頻繁に発生し，漏洩による被害が甚大となっている．このため，機密情報の保護が計算機システムにおける大きな課題である．

ファイアウォールや暗号化といった従来のセキュリティ対策のほとんどは，侵入やマルウェアといった外部からの不正アクセスから情報を守ることが主目的としている．そのため，内部者による情報漏洩に対して従来のセキュリティ対策は完全ではない．なぜなら，内部者の中には機密情報を扱う権限を持つユーザがいるためである．もし，権限を持つユーザが意図的に漏洩をさせようとした場合には，従来のセキュリティ対策では防ぐことはできない．例えば，権限をもつユーザが USB メモリ等のリムーバブルメディアやネットワークを用いて機密情報を持ち出す漏洩では，従来のセキュリティ対策では正常な動作とみなされるため情報の漏洩を発見することはできない．また，機密情報を持ち出せない場合でも，権限を持つユーザは閲覧することは可能なため，情報の複製は容易であり簡単に漏洩することができる．例えば，機密情報をビューワで閲覧している際に表示内容をコピーして別ファイルにペーストして複製された場合，複製されたファイルは機密情報ではない．この複製を持ち出すことで，容易に漏洩してしまう．

このような問題を防ぐために，機密情報を安全に取り扱うシステムが必要となる．ここでいう安全とは，機密情報を取り扱う作業中に，機密情報の内容がどこにも漏れないことを指す．機密情報を安全に取り扱うためには，次の 3 点が必要である．1 つ目に機密情報を安全に保存できること，2 つ目に機密情報を安全に閲覧できることそして，3 つ目に機密情報を安全に作成できることである．

ファイアウォールや暗号化といった従来のセキュリティ対策の他に，不正ファイルアクセス防止システム[1] が存在する．しかし，外部からの攻撃しか想定していないため権限をもつユーザからの漏洩を防止できない．また，機密情報を安全に閲覧できる手法[2] がある．しかし，閲覧だけに限っているため，作成については考慮されていない．さらに，機密情報をサーバで管理して閲覧作成要求があった場合，データの表示のみおこなう手法[3] がある．しかし，ユーザの権限によっては，データを持ち出すことが可能であるため悪意あるユーザが権限を持っていた場合には漏洩を防ぐことはできない．そして，計算機の所持者や使用者であってもデータの改竄や持ち出しを防ぐ手法[4] も存在するが，使用するアプリケーション等が制限されておりユーザビリティに欠けるという問題点がある．

Vol.2010-DPS-142 No.54
Vol.2010-CSEC-48 No.54
2010/3/5

本稿では，機密情報を安全に扱うことができる機密情報閲覧作成システムを提案する．提案手法は，仮想マシンモニタを用いて管理用のオペレーティングシステムを独立して設ける．機密情報の閲覧作成時には，ユーザの権限に関係なく，ディスクやネットワークといった出力デバイスを無効化することで漏洩を防ぐ．また，機密情報の作成には，ディスク擬似書き込みによる任意のアプリケーションを使用可能とする．そして，仮想マシンモニタのスナップショット機能を用いて機密情報の閲覧作成中の状態を残さない．以上により，機密情報作成閲覧後の主記憶内容の覗き見による漏洩を防ぎ，り機密情報を安全に扱うことが可能となる．

本稿では，2 章で既存手法について述べる，3 章で提案手法について述べる．4 章で提案手法の実装について述べ，5 章で提案手法の評価について述べる．そして，6 章でまとめる．

2. 関連研究と問題点

機密情報漏洩防止についての関連研究について述べ，問題点について整理する．

2.1 関 連 研 究

SAccessor[1] は，仮想マシンを用いた不正ファイルアクセス防止システムである．SAccessor は仮想マシンを用いてユーザが使用する作業 OS とファイルサーバとなる認証 OS を動作させ，認証 OS でファイルアクセス制御をおこなう．また，認証 OS は作業 OS に対して認証をおこない，正当なユーザのみがファイルの変更を許される．これにより，OS が乗っ取られても正常にファイルアクセス制御が動作し，正当なユーザのみがファイルを変更することが可能となる．しかし，SAccessor は攻撃者は遠隔地にいることを想定しており内部者の攻撃については考慮していない．よって，認証できるユーザであれば漏洩を許す．

VOFS[2] は，仮想マシンを用いた機密情報の閲覧のみを許可するシステムである．VOFS は機密情報を安全に保存するために，使用する OS とは別の仮想マシンに機密情報を保存する．機密情報の閲覧時には，ディスク書き込みとネットワークを無効化する．これにより，機密情報を安全に閲覧することが可能となる．しかし，VOFS では機密情報の閲覧のみを対象としているため機密情報の作成については考慮されていない．また，閲覧以外の行為の無効化の開始は手動でおこなうため，ユーザビリティに欠ける．

DOFS[3] は，リモートデスクトップを用いた機密情報漏洩防止システムである．DOFS はサーバで機密情報を一括管理し，機密情報の閲覧作成要求には，リモートデスクトップを用いて要求内容を表示する．これにより，ローカル計算機に機密情報のデータ内容は渡らない．よって，機密情報のデータ内容の複製による漏洩は不可能となる．しかし，DOFS は権限のあるユーザに対して機密情報を持ち出すことを許可している．よって，悪意あるユーザが権限をもっていた場合，機密情報は漏洩する．

HiGATE[4] は計算機の所持者や使用者であってもデータの改竄や持ち出しを防止する計算機ベース型大容量耐タンパ装置である．HiGATE は計算機のケースを開いていないことを証明する機能でメモリ内容の盗み見を防ぎ，HDD の暗号化で HDD の持ち出しによる漏洩を防止している．また，使用するプログラムの起動制御をおこなうことで不正プログラムによる漏洩を防止している．しかし，HiGATE は使用するプログラムを制限するため，任意のプログラムを使用することはできない．よって，ユーザビリティに欠ける．

2.2 問 題 点

本稿では，機密情報を安全に取り扱うための要件として，機密情報を安全に保存できること，機密情報を安全に閲覧できること，機密情報を安全に作成できること，の 3 点を挙げた．この 3 点がすべて満たされた場合のみ，機密情報を安全に取り扱うことができるといえる． 1 つ目の機密情報を安全に保存できることについては，機密情報が保存された場所から不正持ち出しを防止する必要がある．従来のシステムでは，OS によるファイルアクセス制御により不正アクセスを防いできた．しかし，OS にも脆弱性が報告されており，不正者が脆弱性を攻撃してファイルアクセス制御を無効化することも考えられ，同一 OS 内で保存することは危険である．この点については，関連研究のすべてが満たしているといえる．SAccessor と VOFS では仮想マシンを用いて別 OS で保存し，管理している．また，DOFS ではサーバで機密情報を一括管理しており，HiGATE は耐タンパ領域内で管理する．

2 つ目の機密情報を安全に閲覧できることと，3 つ目の機密情報を安全に作成できることについては，機密情報の閲覧，作成中における漏洩を防止する必要がある．ビューアを用いた機密情報の閲覧や，エディタを用いた機密情報の作成時には，ディスプレイ上に機密情報の内容が表示される．一般的なアプリケーションを用いた場合，表示内容をコピーすることを許可されているため容易に機密情報の内容をコピーできる．また，主記憶内にはアプリケーションデータが存在するため，主記憶内からアプリケーションで表示中の機密情報の内容を盗み見ることができる．これらの手段から機密情報の内容をコピーできた場合，容易に機密情報を複製することが可能となり，情報が漏洩する．これらの点については，HiGATE は所持者や使用者であってもデータの改竄や持ち出しを防ぐことができるため満たしているといえる．しかし，SAccessor や DOFS では権限を持つユーザであれば容易にファイルを複製できる．VOFS は閲覧のみこの点を満たすが，作成については考慮していないのため，完全に満たしているとはいえない．

Vol.2010-DPS-142 No.54
Vol.2010-CSEC-48 No.54
2010/3/5

HiGATE は機密情報を安全に取り扱う 3 点を満たしているが，使用するプログラムを制限しているため，ユーザビリティに欠ける．ユーザビリティに欠けると使用者に使用法を強いるため，非常に使いにくいものになる．これは VOFS の閲覧以外の行為の無効化の開始は手動であることも同様である．

3. 提 案 手 法

本章では，提案手法について述べる．まず，提案手法の概要を述べ，提案手法の前提条件について述べる．そして，提案手法の実現するシステムの構成について述べる．

3.1 概　　要

2.2 節で述べた問題点を解決し機密情報を安全に扱うためには，機密情報のファイルアクセスを外部で制御し，機密情報の閲覧作成中にその内容を漏らさないことが必要である．本稿ではこれらの問題点を解決する機密情報閲覧作成システムを提案する．提案手法では，機密情報を安全に扱うために次の 3 点をおこなう．

- ユーザが使用する OS とは別の OS でファイルアクセスを制御する．
- ユーザが機密情報を閲覧作成する時は，全ユーザに対して，ユーザアプリケーションの漏洩以外の動作を阻害しない出力デバイスの無効化処理を実施する．
- ユーザが機密情報の閲覧作成作業を終了する時に，機密情報の閲覧作成前の状態に戻す．

機密情報をユーザが使用する OS とは別の OS でファイルアクセスを制御することにより，ユーザが使用する OS が乗っ取られてもアクセス制御は正常に機能する．このために，仮想マシンモニタを用いる．以下，一般ユーザが使用する OS を作業 OS，システム全体を管理する OS を管理 OS という．

ユーザが機密情報を閲覧作成する時に，提案手法では管理者を含むすべてのユーザの権限に関係なく，作業 OS に対してディスクとネットワークへの出力の無効化処理を実行する．これによって，ユーザは，機密情報の内容を複製できたとしてもディスク書き込みとネットワークへの流出ができないため情報の漏洩手段がない．よって，ユーザアプリケーションの実行を確保しつつ機密情報を保護できる．

そして，ユーザが機密情報の閲覧作成を終了した時に，作業 OS を機密情報の閲覧作成前の状態に戻す．作業 OS を機密情報の閲覧作成前の状態に戻すことにより，機密情報の閲覧作成中の主記憶内容を残さない．これにより，出力デバイスの無効化が終了した後に主記憶から機密情報の閲覧作成時の内容の盗み見を防ぐことができる．以下，出力デバイス無効化処理と作業 OS の状態復元処理を合わせて，**機密情報漏洩防止処理**という．

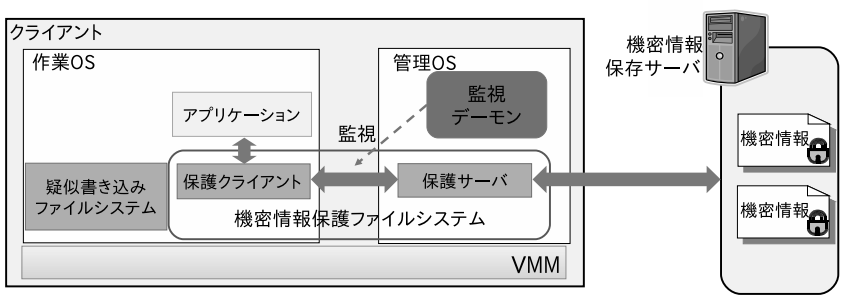

図 1　提案システムの全体構成
Fig. 1　Overview of proposal system

3.2 前 提 条 件

本項では，提案手法における前提条件について述べる．提案手法における前提条件は次のとおりである．

- 計算機内の仮想マシンモニタ，管理 OS，機密情報保存サーバは信頼する
- 攻撃者は任意のアプリケーションを作業 OS で実行可能
- 機密情報の閲覧時に内容を紙に書き写す，画面を写真で撮るといった行為は考慮しない

3.3 提案システムの構成

本節では提案手法を実現するためのシステムについて述べる．提案手法を実現するためのシステム構成を**図 1** に示す．提案システムは機密情報保存サーバとクライアントによって構成する．機密情報保存サーバは，機密情報の保存をおこなうサーバである．クライアント内では仮想マシンモニタを用いて作業 OS と管理 OS の 2 つの OS を動作させる．管理 OS は提案システムを管理する OS で，システム管理者のみが操作可能である．管理 OS は計算機上の物理デバイスや作業 OS を管理する能力を持つ．作業 OS は一般ユーザが使用するもので，ユーザがログインし，一般的な作業をおこなう OS である．以下，提案手法の実現方法について述べる．

3.3.1 機密情報のファイルアクセス制御

提案手法では 3.1 節で述べたように機密情報を安全に保存するために，ユーザが使用する作業 OS とは別の管理 OS で機密情報のファイルアクセスを制御する．これを実現するために，**機密情報保護ファイルシステム**を設ける．機密情報保護ファイルシステムは，仮想マシンモニタの独自の通信機構を用いた遠隔ファイルシステムである．機密情報保護ファイルシ

Vol.2010-DPS-142 No.54
Vol.2010-CSEC-48 No.54
2010/3/5

ステムは図 1 のように，作業 OS 側に保護クライアント，管理 OS 側に保護サーバをそれぞれ配置する．保護サーバでは機密情報に対するアクセス制御をおこなう．その後に，機密情報保存サーバに機密情報の取得要求を送り，要求結果を保護クライアントに返す．機密情報保護ファイルシステムは，保護クライアント内にキャッシュを作成しない．これは，すべてのアクセスを保護サーバに要求することで，保護サーバでのアクセス制御を強制するためである．これにより，作業 OS が乗っ取られても，機密情報のファイルアクセス制御は奪われない．よって，機密情報に許可なくアクセスすることが不可能となる．

3.3.2 機密情報漏洩防止処理

提案システムでは，ユーザアプリケーションの実行を阻害せずにディスク出力を無効化するために，**擬似書き込みファイルシステム**を設ける．擬似書き込みファイルシステムは，機密情報閲覧作成時に既存ファイルへの読み書きを可能にしたまま，ディスクへの書き込みを無効化するファイルシステムである．提案システムでは，擬似書き込みファイルシステムを作業 OS のルートディレクトリにマウントして使用する．次に，ユーザが機密情報の閲覧作成作業が終了する時に作業 OS を機密情報の閲覧作成前の状態に戻すためには，仮想マシンモニタのスナップショット機能を用いる．スナップショットは機密情報漏洩防止処理の開始時点で取得し，機密情報漏洩防止処理が終了した時に作業 OS を復元する．

また，機密情報漏洩防止処理は機密情報を閲覧作成しようとした時に実行し，閲覧作成作業が終了した時に終了する．提案システムでは機密情報保護ファイルシステムの通信を監視して，ファイルアクセスの挙動によって機密情報漏洩防止処理の開始と終了を判断する．機密情報を閲覧作成する際にはどのプログラムでもファイルアクセスが発生する．このため，ファイルアクセスの挙動を監視することで，確実に機密情報漏洩防止処理を開始できる．これにより，提案システムではユーザアプリケーションを制限する必要がなくなり，例え不正プログラムが機密情報にアクセスしても機密情報を漏洩できない．提案システムでは図 1 にあるように，管理 OS に**監視デーモン**を作成して機密情報保護ファイルシステムのファイルアクセスを監視する．

4. 実　　装

本章では，3.3 節で述べた提案システムの実装について述べる．本実装において，仮想マシンモニタとして Xen[5] を使用し，管理 OS を domain0，作業 OS を domainU として動作させた．まず提案手法の機密情報保護ファイルシステムについて述べ，次に機密情報漏洩防止処理について述べる．そして最後に，作業 OS の正当性の保証について述べる．

4.1 機密情報保護ファイルシステム

機密情報保護ファイルシステムは，3.3.1 項で述べたように，機密情報を安全に保存するファイルシステムである．本節ではプロトタイプとして開発した，FUSE[6] と Xen のデバイスドライバモデルを用いた遠隔ファイルシステムについて述べる．本プロトタイプでは保護サーバが機密情報保存サーバから機密情報を取得する機能が未実装である．機密情報保存サーバに存在する機密情報を閲覧する場合には，まずユーザが機密情報保存サーバから入手して機密情報保護ファイルシステムに保存する必要がある．なお，機密情報を作成した際には，保護サーバが機密情報保存サーバに自動的にアップロードする機能を有する．以下，機密情報保護ファイルシステムのクライアントとサーバの実装について述べる．

4.1.1 保護クライアント

保護クライアントは FUSE と Xen のデバイスモデルを用いて実現した．FUSE は Unix 系オペレーティングシステムのカーネルモジュールの一種で，ユーザがカーネルコードを修正することなく，独自のファイルシステムを作成できる機能を提供するものである．また，Xen のデバイスドライバモデルは，Xen 内部で仮想マシン間の通信を実現する．このため，通信内容が外部に漏れないという利点を持つ．実装は，ファイルシステムを提供する部分を FUSE，保護サーバとの通信を実現する部分を Xen のデバイスドライバを用いて作成した．保護クライアントは FUSE 部分でファイルアクセスを受け付け，Xen のデバイスドライバモデルを用いてサーバに送信する．そして保護サーバからの実行結果が返信されるまで待ち，結果を受信する．

4.1.2 保護サーバ

保護サーバは Xen のデバイスドライバモデルを用いて実装した．保護サーバは保護クライアントから要求を受信し，その要求を実行する．その後，要求の実行結果をクライアントに送信する．また，保護サーバは AES を用いて機密情報の暗号化と復号をおこなう．作業 OS が機密情報を閲覧する場合には，機密情報を復号して内容を渡す．一方，機密情報を作成する場合には，ファイル作成後に暗号化する．さらに，暗号化されたファイルを機密情報保存サーバにアップロードする．なお，機密情報保存サーバとの通信には，RSA を用いて暗号化する．

4.2 機密情報漏洩防止処理

機密情報漏洩防止処理は，3.3.2 項で述べた出力デバイスの無効化処理と，作業 OS の状態を復元処理の 2 つの基本処理に加えて，監視デーモンによる機密情報漏洩防止処理の開始と終了のタイミング調整処理が必要である．本節では機密情報漏洩防止処理の流れにつ

Vol.2010-DPS-142 No.54
Vol.2010-CSEC-48 No.54
2010/3/5

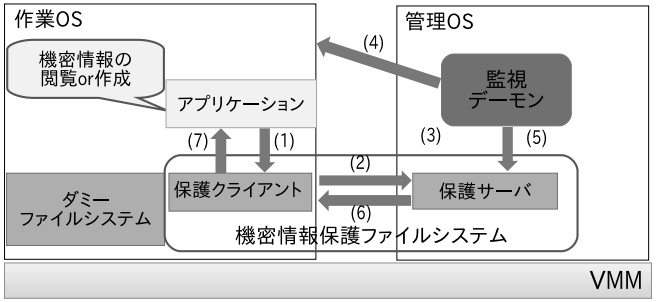

図 2 機密情報漏洩防止処理の流れ
Fig. 2 Flow of leakage prevention processing

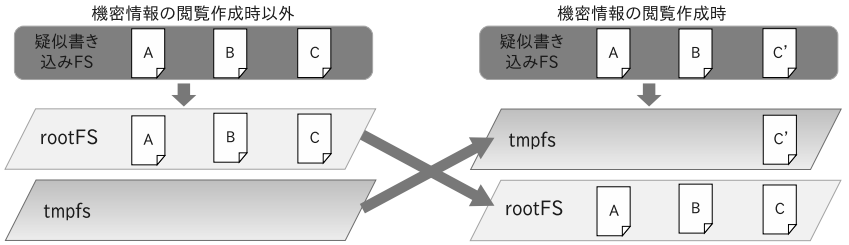

図 3 ディスク擬似書き込みファイルシステム
Fig. 3 Disk quasi-write filesystem

いて述べる．出力デバイスの無効化処理とスナップショットの作成については 4.3 節，監視デーモンによる処理タイミングの判断手法については 4.4 節でそれぞれ詳しく述べる．

機密情報漏洩防止処理の実行の流れを**図 2** に示し，動作について述べる．まず，作業 OS のアプリケーションは機密情報を閲覧もしくは作成するために，保護クライアントが管理するファイルシステムにアクセスする（1）．アクセスを検知した保護クライアントは，保護サーバに対して open 命令を要求する（2）．この時，監視デーモンはこの open 命令を検知する（3）．open 命令を検知した監視デーモンは，作業 OS 側の漏洩の可能性がある出力デバイスの無効化と作業 OS のスナップショットの作成をおこなう（4）．これらの処理がすべて成功した場合にのみ，監視デーモンは保護サーバに対して機密情報の操作を許可する（5）．許可を受けた保護サーバは，作業 OS 内にあるクライアントに対して機密情報のデータを送る（6）．データを受け取った保護クライアントはアプリケーションにデータを渡す（7）．以上により，安全に機密情報の閲覧作成できる．

機密情報漏洩防止処理の実施中に機密情報の閲覧作成作業が終了した時，機密情報漏洩防止処理を終了する．閲覧作成作業の終了の検知は，監視デーモンが機密情報の閲覧作成作業中のプログラムの終了を検知することによって実現する．そして，機密情報を扱うすべてのプログラムの終了を検知した時，監視デーモンは機密情報漏洩防止処理を終了させる．機密情報終了時には，スナップショットによる作業 OS の復元と出力デバイスの有効化をおこなう．

4.3 出力デバイスの無効化とスナップショット

本節では，機密情報漏洩防止処理における出力デバイスの無効化と，スナップショットの実装について述べる．機密情報漏洩防止処理は作業 OS 側の漏洩の可能性がある出力デバイスを無効化する．提案手法において漏洩の可能性がある出力デバイスはディスクデバイスとネットワークデバイスの 2 つである．

以下，擬似書き込みファイルシステムと，ネットワークデバイスの有効化と無効化について述べる．さらに，スナップショットの動作について述べる．

4.3.1 擬似書き込みファイルシステム

擬似書き込みファイルシステムは，ディスク擬似書き込み機能を有するファイルシステムである．ディスク擬似書き込み機能とは，アプリケーションからは通常のディスクデバイスとして読み書き可能であるが，実際にはメモリ上の操作のみでディスクには書き込まない機能である．提案手法では，ディスクデバイスの無効化機能として使用する．

ディスクデバイスの無効化は，全ファイルシステムを読み出し専用にする方法でも実現できる．しかし，ファイルの書き込みを制限することで正常に動作しないプログラムが存在する．これらのプログラムがシステム動作に必要であったり，ユーザに必要なアプリケーションであった場合，システム運用やユーザ利用に支障をきたす恐れがある．このため，全ファイルシステムを読み出し専用にする方法で書き込みを防ぐことはできない．そこで，ディスクに書き込まないが擬似的にファイルを作成することができるディスク擬似書き込み機能を用いる．これにより，ディスク書き込みによる漏洩を防ぐことができ，さらにファイル書き込みが必要なプログラムも正常に動作する．

擬似書き込みファイルシステムは，AUFS[7] をベースとして実装した．AUFS は，ブラン

Vol.2010-DPS-142 No.54
Vol.2010-CSEC-48 No.54
2010/3/5

チと呼ばれる分離したファイルシステムのファイルやディレクトリを透過的に重ねて，単一の一貫したファイルシステムを形成する．また，ブランチの優先度を設定でき，優先度が高いブランチにしか書き込みを許さないように指定できる．これにより，コピーオンライト機能を実現することが可能である．本実装では，AUFS を用いて，ブランチに通常のルートファイルシステムと，tmpfs[8] の 2 つをマウントした．tmpfs は擬似書き込みのための一時保存領域である．ここで，擬似書き込みを実現するために，機密情報の閲覧作成時以外ではルートファイルシステムの優先度を高くし，機密情報の閲覧作成時には tmpfs の優先度を高くできるように変更する機構を AUFS に対して追加実装した（**図 3**）．これにより，機密情報の閲覧作成時にはコピーオンライト機能が働きルートファイルシステムにあるファイルの変更はすべて tmpfs に書き込まれる（図 3 の C’）．tmpfs はメモリ上にファイルシステムを形成するため，ディスクに書き込むことがない．しかし，単純にブランチの優先度を変更しただけでは不十分である．これは，カーネル側に状態変更前のファイルキャッシュが存在しているからである．このファイルキャッシュはプログラムに優先的に使用される．もし，状態変更前のファイルキャッシュが使用されると，ディスクに書き込まれる．これを防止するためにはキャッシュを開放すればよいのだが，プログラムが使用している状態ではそのプログラムに支障をきたす恐れがある．このために，本実装ではブランチの優先順位を変更した場合には，ファイルキャッシュにも優先順位を反映させる機構を設けた．

4.3.2 ネットワークの無効化と有効化

ネットワークの無効化と有効化には iproute2 を用いて IP ルーティング操作により実現した．iproute2 は、パケットのルーティングテーブルを操作するパッケージである．本実装では，機密情報漏洩防止処理を開始した時に作業 OS が使用する仮想ネットワークデバイスのルーティングを変更して外部との通信を遮断する．そして，機密情報漏洩防止処理が終了した時にはルーティングを変更して外部との通信を有効化する．

4.3.3 スナップショット作成と仮想マシンの復元

スナップショットの作成と仮想マシンの復元は Xen の機能を使用した．これらの機能を使用する際には，libvirt[9] を通して実行する．本実装では，機密情報漏洩防止処理開始時に作業 OS のスナップショットを取得し，終了時にはスナップショットを用いて作業 OS を機密情報の閲覧作成前の状態に戻す．

4.4 監視デーモン

本節では，監視デーモンによる機密情報漏洩防止処理の開始と終了のタイミングの判断手法とその実装について述べる．監視デーモンは管理 OS のデーモンプログラムとして配置する．4.2 節で述べたように機密情報漏洩防止処理を開始するタイミングは，保護クライアントが保護サーバに対して open 要求を発行した時である．この要求を検出するために，監視デーモンは保護サーバが用いる Xen のデバイスドライバを監視する．監視デーモンは Xen のデバイスドライバで通信している内容を読み取り，機密情報の open 要求が存在した場合に機密情報漏洩防止処理を開始する．

また，機密情報漏洩防止処理の終了は，機密情報の閲覧作成作業をしているプログラムがすべて終了した時である．しかし，監視デーモンは管理 OS 上に存在するため，作業 OS で動作するプログラムの終了を検知することは困難である．そこで本実装では作業 OS 内に機密情報の閲覧作成中のプログラムを監視するプログラムを配置した．このプログラムは保護クライアントを監視し，機密情報に対するアクセスがあった場合，アクセスしたプログラムを順次監視する．そして，機密情報を閲覧作成するプログラムがすべて終了した場合に，監視デーモンに機密情報の閲覧作成が終了したことを通知する．これにより，監視デーモンは機密情報の閲覧作成が終了したことを検知する．通知を受けたデーモンは，機密情報漏洩防止処理を終了する．

機密情報漏洩防止処理のネットワークデバイスとスナップショットについては，4.3.2 項，4.3.3 項で述べたことを監視デーモンがそれぞれ実行する．しかし，擬似書き込みファイルシステムについては作業 OS 側にあるため，監視デーモンは擬似書き込み機能ファイルシステムに対して機密情報漏洩防止処理の開始と終了を直接通知することはできない．そこで，監視デーモンが擬似書き込みファイルシステムに対して機密情報漏洩防止処理の開始と終了を通知する機構を Xen のデバイスドライバモデルを用いて実装した．これにより，監視デーモンから擬似書き込みファイルシステムに機密情報漏洩防止処理の開始と終了を通知することができる．また，擬似書き込みファイルシステムは機密情報漏洩防止処理の開始の通知を受信した場合には，ブランチの優先度を変更してディスク擬似化書き込み機能を有効化する．そして，処理の終了を通知された場合には，擬似書き込みで書かれた内容を破棄してディスク書き込みを有効化する．

4.5 作業 OS の正当性の保証

提案システムでは作業 OS を変更している．前提条件により，管理 OS は信頼できるが作業 OS は信頼することができない．このため，作業 OS が乗っ取られた場合，機密情報漏洩防止処理が正常に動作しない可能性が高い．つまり，機密情報の漏洩が容易になる．この問題点を解決する方法として，作業 OS の正当性の保証をすることによって提案手法の動作が正常に動作することを保証する．作業 OS の正当性は，作業 OS の起動時にカーネルの正当

Vol.2010-DPS-142 No.54
Vol.2010-CSEC-48 No.54
2010/3/5

表 1 ファイルアクセス性能（MB/sec）
Table 1 The performance of file accesses

	ext3	FUSE+Xen	保護 FS
読み出し速度	84.91	48.25	33.13
書き込み速度	72.82	33.53	23.00

性を確認することと，機密情報漏洩防止処理の動作確認の 2 点をおこなうことで実現する．

カーネルの正当性を確認するための処理は，監視デーモンがおこなう．まず，作業 OS の起動時のカーネルの正当性保証として，あらかじめ作業 OS カーネルバイナリハッシュを取得しておき，起動時にカーネルを比較する．次に，機密情報漏洩防止処理の動作確認については，処理が完了したかを判断する機構を設けた．

5. 評価と考察

提案手法の性能の評価と，提案手法に対する攻撃とその対処法についての考察を述べる．

5.1 性 能 評 価

提案手法の性能評価として，機密情報漏洩防止処理開始と終了に要する時間と機密情報保護ファイルシステムの性能について評価する．評価対象の計算機として，Core 2 Quad 2.66GHz の CPU，メモリ 4GB の計算機を使用した．仮想マシンモニタとしては，Xen3.2.1，管理 OS として Linux2.6.25，作業 OS として Linux2.6.24 を用いた．管理 OS にはメモリを 3GB，作業 OS にはメモリを 1GB 割り当てた．

5.1.1 機密情報漏洩防止処理の開始と終了に要する時間

本評価では，スナップショットの保存場所に tmpfs を用いた．計測結果より，ゲスト OS のメモリ量が 1GB で機密情報漏洩防止処理の開始に約 4.5 秒，終了に約 3.5 秒要した．それぞれの所要時間が 5 秒未満であるため，実用には問題ないと考える．

5.1.2 機密情報保護ファイルシステムの性能評価

機密情報保護ファイルシステムの性能評価として，ファイルの読み出しと書き込みのスループットを測定した．スループットの測定方法は，読み出しと書き込みともに，300MB のファイルをブロックサイズを 3KB として速度を測定した．測定結果を**表 1** に示す．機密情報保護ファイルシステム（保護 FS）の比較対象は ext3 と，FUSE と Xen のデバイスドライバを用いたファイルシステム（FUSE+Xen）とした．

表 1 より，ext3 と保護 FS を比較すると約 65%のオーバーヘッドである．ext3 と FUSE+Xen を比較すると約 49%のオーバヘッドがあることから，機密情報保護ファイルシステムのオーバーヘッドのうち 49%が FUSE と Xen のデバイスドライバによるオーバーヘッドで，残りの 16%が AES 暗号を用いた処理のオーバーヘッドである．また，機密情報保護ファイルシステムは ext3 の約 35%程度の速度ながら，読み出し速度が約 33MB/sec であり，書き込み速度は約 23MB/sec であるため，実用には問題ないといえる．

5.2 想定される攻撃とその対処法についての考察

本節では，提案手法に対する攻撃手法とその対応について述べる．攻撃は，大きく外部からの攻撃と内部からの攻撃に分けられる．まず，外部からの攻撃について述べ，次に内部からの攻撃について述べる．

5.2.1 外部からの攻撃

外部からの攻撃として，1 つ目に機密情報の取得時の盗聴が考えられる．提案手法では，機密情報保存サーバから機密情報ファイルをネットワークを介して取得する時に，盗聴される可能性がある．提案手法では，機密情報は暗号化されているため，盗聴されていたとしても盗聴者が復号する鍵を持っていない限り，機密情報の内容を知り得ることは困難である．

2 つ目に不正侵入が考えられる．外部不正者が計算機へ不正侵入をおこない，その後機密情報を漏洩させる攻撃が考えられる．前提条件より，不正者は侵入後，計算機上のすべての情報を知ることが出来るとする．したがって，不正者は機密情報を知ることができる．提案手法では，機密情報ファイルを open した際に機密情報漏洩防止処理によってネットワークが無効化される．このため，外部からリモートで不正侵入しているユーザはその時点で通信が遮断される．よって，不正侵入をおこなう不正者は機密情報を閲覧することができない．

3 つ目にマルウェアによるクラッキングが考えられる．マルウェアとは，不正かつ有害な動作をおこなう意図で作成された悪意のあるソフトウェアや悪質なコードのことである．マルウェアには計算機に感染後，OS をクラッキングして OS レベルの管理者権限を取得して，感染した計算機内部の情報を使用者に気付かれないようにネットワークに放流して漏洩させる攻撃をするものが存在する．提案手法では，作業 OS の起動時にカーネルをチェックするため，無断でカーネル内容が変更された場合，作業 OS を起動ができなくなり，機密情報の流出を防ぐことが可能である．また，作業 OS 内にある擬似書き込みファイルシステムが改竄されて，機密情報の閲覧作成時に機密情報漏洩防止処理が機能しない場合，監視デーモンが正常動作とみなさないため，機密情報ファイルを open することはできない．

5.2.2 内部からの攻撃

内部からの攻撃として，1 つ目に内部者の不正持ち出しによる漏洩が考えられる．内部者は機密情報を扱う権限を持つため，もし内部に悪意のある者がいれば容易に漏洩する．提案

Vol.2010-DPS-142 No.54
Vol.2010-CSEC-48 No.54
2010/3/5

手法では，機密情報を open した際に機密情報漏洩防止処理が作動し出力デバイスを無効化する．よって，ネットワークを通じて流出させることは不可能である．また，ディスクデバイスやリムーバブルメディアに書き込もうとしても擬似書き込みファイルシステムにより書き込むことは不可能である．

2 つ目に，機密情報の閲覧作成中の内容の複製が考えられる．機密情報を持ち出す権限がないとしても，機密情報を閲覧作成できた場合，機密情報の内容は簡単に複製することが可能である．また，ファイル内容のコピーを無効とするプログラムも存在するが，メモリ内容から情報を読み取ることは可能である．提案手法では，機密情報の閲覧作成中は機密情報漏洩防止処理が動作し，ファイルを作成したとしてもディスク擬似書き込み機能により，ディスクには書き込むことができない．また，機密情報の閲覧や作成が終了した場合，スナップショットを用いて機密情報の閲覧や作成前の状態に戻すため，コピーした内容を主記憶領域内に保持しておくことは不可能である．

3 つ目に，スクリーンショットを取得することが考えられる．スクリーンショットは計算機のモニタ領域をすべて画像として保存することができる．このため，機密情報の閲覧作成時にスクリーンショットを撮った場合，スクリーンショットの画像内に機密情報が記憶される．この画像が外部に流出した場合，機密情報の内容を見ることが出きるため，機密情報が漏洩する．提案手法では，機密情報の閲覧，作成中は機密情報漏洩防止処理が動作し，スクリーンショットを撮ったとしても漏洩させる手段が無い．

以上により，提案手法では機密情報を漏洩させることは困難であり，安全な機密情報閲覧作成環境が実現できるといえる．

6. おわりに

機密情報を安全に取り扱うために仮想化とディスク擬似書き込みによる機密情報閲覧作成システムを提案した．提案手法では，仮想マシンを用いて同一計算機上で一般ユーザが使用する作業 OS とシステムを管理する管理 OS を動作させる．機密情報を作業 OS の外側に存在する管理 OS に保存することで，ファイル制御を独立させて安全に機密情報を保存することができる．また，機密情報の閲覧作成時にはディスク擬似書き込みによる無効化とネットワークを無効化することによって機密情報の漏洩を防ぐ．さらに，スナップショットを用いて機密情報の閲覧作成中の状態を残さないことにより，機密情報閲覧作成中の主記憶内容の覗き見による漏洩を防ぐ．

また，提案手法を仮想マシンに Xen を用いて実装をおこない，評価をおこなった．評価より，実用に耐えうることを確認した．さらに，想定される攻撃に対する対処法の考察をおこい，強固な安全性を確認した．

今後の課題として，機密情報保護ファイルシステムの機密情報保存サーバとの通信部分を完成させて，システムの高速化と安定性の向上を実現する予定である．

参考文献

1) 滝沢裕二，光来健一，千葉　滋，柳沢佳里 : SAccessor: デスクトップ PC のための安全なファイルアクセス制御，情報処理学会論文誌コンピューティングシステム （ACS），Vol.1, No.2, pp.1–9 (2008).
2) Borders, K., Xhao, X. and Prakash, A.: Securing Sensitive Content in a View-Only File System, *DRM '06: Proceedings of the ACM workshop on Digital rights management*, pp.27–36 (2006).
3) Yu, Y. and Chiueh, T.: Display-Only File Server: A solution against Information Theft Due to Insider Attack, *Fourth ACM workshop on Digital Rights Managment*, pp.31–39 (2009).
4) 桜井裕唯，芦野佑樹，吉浦　裕，佐々木良一 : 大容量耐タンパ領域装置 HiGATE の試作と e-Discovery への適用，情報処理学会，Vol.CSS2009-E2-2 (2009).
5) The Xen Project: Xen, http://www.xen.org.
6) SourceForge project: File Space in User Space,http://fuse.sourceforge.net/.
7) SourceForge project: AUFS, http://aufs.sourceforge.net/.
8) Snyder, P.: tmpfs: A virtual memory file system, In Proceedings of the Autumn 1990 European UNIX Users ' Group Conference, pp.241–248 (1990).
9) libvirt community: libvirt: The virtualization API, http://www.libvirt.org.