Vol.90 No.03 294-295

Professional Report

企業情報を守る漏洩防止技術

Data Leakage Prevention Technologies Protecting Enterprise Information

鮫島 吉喜　Yoshiki Sameshima

個人情報保護法の制定に伴い，顧客情報をはじめとする秘密情報の漏洩に対する社会の見方が厳しくなっている。日立ソフトウェアエンジニアリング株式会社の情報漏洩防止ソリューション「秘文AE」は情報の暗号化と外部媒体への書込みを制限することで，PCや媒体の紛失/盗難による情報漏洩を防止している。その特徴は既存PCの使い勝手を変えないことである。「秘文ME」は秘文AEによる漏洩防止のほかに，ウイルス感染防止の対策状況を可視化することにより，管理者による現状把握，改善によるセキュリティマネジメントを支援する。

二系統端末は未知のウイルス/攻撃への対策であり，仮想化技術とセキュアOSという二つの古くからあり最近注目を浴びている技術を利用している。ウェブ2.0，SaaS（Software as a Service）など，新しいネットワーク利用時代の情報漏洩に対応する。これらにより，現在および近い将来に必要とされる情報セキュリティを確保することができる。

1986年 日立ソフトウェアエンジニアリング株式会社 入社
技術開発本部 研究部 所属
現在，情報セキュリティの研究に従事
電子情報通信学会会員，情報処理学会会員，日本セキュリティ・マネジメント学会会員，USENIX会員

1　はじめに

1990年代半ばからのインターネット普及に伴い，ウイルス対策をはじめとするセキュリティ対策は，企業にとっても一般利用者にとっても必須となった。ここ10年余りを振り返ると，最初の脅威となったのは，1990年代後半のマクロウイルスである。電子メールを使って簡単にオフィス文書のやり取りができるようになったことで，ワープロや表計算ソフトのマクロ機能を利用して感染を広げ，文書を破壊するコンピュータウイルスが流行した。現在ではワクチンソフトを利用したウイルスの検知，駆除が常識となっている。

2000年初めに中央官庁のホームページ改竄（ざん）事件やサービス妨害攻撃が発生し，不正アクセスに対する脅威が再認識された。ウェブやメールサーバをはじめ，組織のネットワークをインターネットに接続する際のファイヤウォール設置が進むとともに疑似攻撃によるサーバの診断が普及する契機となった。

ファイヤウォールさえ導入しておけば安全という当時の常識を打ち砕いたのは，2003年のBlasterやSlammerワームであった。インターネットに接続していたサーバには，OS（Operating System）やアプリケーションのセキュリティパッチを当てていた。しかし，直接インターネットに接続していないクライアントPCは，ワクチンソフトを利用したウイルス対策はしていても，パッチは当てていなかった。このために，社外でウイルスに感染したノートPCを社内ネットワークに接続した途端に一気に感染が広まり，業務が停止状態となったのである。これ以来，Windows Update※1を使ったソフトウェアの脆（ぜい）弱性対策の必要性が周知となる。

次の脆弱性は利用者が関係していた。個人情報保護法制定の動きに伴い，顧客や住民など，個人情報の特に機密性確保に注目が集まった。さらに，2005年に官公庁や原子力発電関連の秘密情報がP2P（Peer to Peer）ネットワークへ漏洩（えい）する事件が多発し，個人情報以外の秘密情報保護に対する意識も一気に高まった。これらの事件では，PCや記憶媒体の紛失，ルールに違反した秘密情報の個人所有PCへの保管など，利用者に原因があったケースが多い。

ここでは，日立ソフトウェアエンジニアリング株式会社（以下，日立ソフトと言う。）が取り組んでいる企業な

※1　Windowsは，米国およびその他の国における米国Microsoft Corp.の登録商標である。

どの組織向けの情報漏洩対策として，「秘文AE」[1] の漏洩防止技術，「秘文ME」[1] による対策状況の可視化，さらに二系統端末[2] によって今後予想される未知のウイルスによる漏洩を防止する技術について述べる。

2　情報漏洩の現状と基本的対策

情報漏洩の現状と対策を以下に述べる。資料[3] をもとに情報漏洩の原因別にまとめたものが**表1**，漏洩経路の媒体別にまとめたものが**表2**である。

表中の「内部犯罪」とは，社員や派遣社員が悪用目的で不正に情報を入手して持ち出した漏洩である。「紛失」とはPCや媒体を紛失または置き忘れた場合であり，「盗難」とは車上荒らしなどPCや媒体が盗まれた場合であり，「誤操作」は電子メールやファクシミリでの宛て先誤りである。「不正アクセス」は外部の第三者がネットワーク経由で侵入して情報を盗んだ場合である。「ウイルス」とはウイルスに感染して情報が漏洩した場合である。ただし，不正に情報を自宅に持ち帰り，ウイルスにより漏洩した場合は含まない。不正に情報を自宅に持ち帰って漏洩した場合の被害人数は約11万1,000人で0.5 %，件数では80件で8 %を占めている。

被害人数ベースでは，「内部犯罪」が約36 %で一番多く，「紛失」約19 %，「盗難」約8 %が続いている。「内部犯罪」は1件当たりの被害人数も約44万5,000人と突出しており，発生した場合の損害が大きいと考えられる。対策の基本はアクセス権限の管理であるが，権限者の不正を防ぐのは困難である。利用者識別子やアクセス権限の定期的見直し，アクセス記録の監査，媒体の持ち出しやネットワークの監視など，総合的な対策が必要である。

一方，発生件数ベースでは，「紛失」が約30 %，「盗難」が約19 %を占め，この二つの原因で約半数となっている。また**表2**に見られるように，「外部媒体」や「PC本体」を経由しての漏洩は，被害人数で約59 %，件数では約19 %を占めている。「紛失」と「盗難」による漏洩は媒体上の情報を暗号化しておくことで，情報自体の盗難や悪用，二次被害を防ぐことができ，有効な対策となる。件数比では「紙」からの漏洩が約44 %を占めており，印刷物に対する対策も必要なことがわかる。

「誤操作」に対しては基本的には利用者の意識向上が必要である。メールの誤送信防止の技術的対策として，一定数以上に送信する際には上長の承認を得るようなフィルタリングを導入する方法が有効である。

「ウイルス」による漏洩は約12 %を占める。基本対策としては，ワクチンソフトの利用やセキュリティパッチの適用しかないが，未知のウイルスに対しては効果が薄いと考えられる。未知のウイルスへの対策については後述する。一方，P2PネットワークのWinny経由で感染するウイルスに関する別の調査では漏洩事件が186件発生しており，個人情報漏洩の18 %を占め，57 %が自宅からの

表1　漏洩原因別の被害人数と発生件数
「内部犯罪」は1件当たりの被害人数が約44万5,000人ときわめて多く，発生した場合の損害が大きい。発生件数では，「紛失」と「盗難」で約半数を占めている。

漏洩原因	被害人数（千人）	発生件数
内部犯罪	8,001	18
紛失	4,132	280
盗難	1,799	176
誤操作	737	144
不正アクセス	562	9
ウイルス	531	115
不明・その他	6,475	207
合計	22,237	949

表2　漏洩経路別の被害人数と発生件数
「外部記憶媒体」や「PC本体」を経由しての漏洩は，被害人数で約59 %，件数では約19 %を占めている。

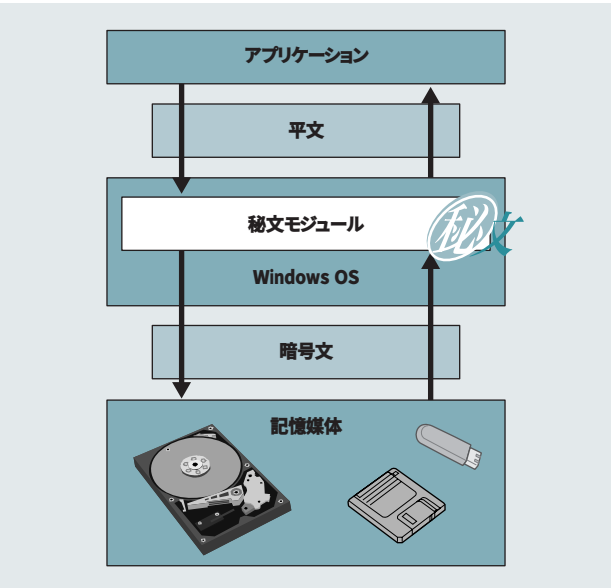
漏洩原因	被害人数（千人）	発生件数
外部記憶媒体	12,558	81
紙	1,571	435
ネットワーク	1,478	218
PC本体	557	106
不明・その他	6,073	153
合計	22,237	993

漏洩である。これについては，職場からの持ち出し規則の徹底や媒体利用の制限を課すことが有効であると言える。

3　秘文AE：使い勝手がよい漏洩防止

3.1　ファイルによる漏洩への対策

前述したとおり，紛失，盗難，職場からの持ち出しなど情報漏洩の多くはクライアントPCから漏洩しており，利用者の不注意によるものが多い。漏洩防止には，クライアントPCのハードディスクや外部媒体上のファイルの暗号化，職場にあるPCからの情報の持ち出し制限が効果的であることがわかる。しかし，単純に暗号化や持ち出し制限の機能を実現しただけでは，使いにくいPCになってしまい，機能を使わない，ないしは例外の使い方が常態化するようになってしまう。日立ソフトが開発，販売している「秘文AEシリーズ」は，暗号化と持ち出し制限の機能を実現するにあたり，「PCの操作性を変えない」，「使い勝手がよい」を基本コンセプトとしており，以下の4点を実現している。



注：略語説明　OS（Operating System）

図1 秘文AEの暗号方式

Windowsの中でファイルI/O（入出力）データを暗号化，復号することで，利用者やアプリケーションに暗号を意識させず，従来どおりの使い勝手を実現している。

(1) 利用者データを例外なく暗号化する。操作ミスしても暗号化されないデータが残らない。

(2) 上記(1)を実現するにあたり，従来のPCの操作方法を変えない。特に暗号化，復号のための操作は不要である。

(3) PC外部へのファイル持ち出しを制限する。ただし，組織/グループ内にとどまるファイル持ち出しは制限しない。

(4) 必要があって外部に持ち出す際には，上長，管理者の承認を得たうえで持ち出せるようにする。

「PCの操作性を変えない」，「使い勝手がよい」ファイル暗号を実現するためには，アプリケーションのファイルI/O（Input and Output）をフックして書込み時にデータを暗号化，読込み時に復号する必要がある。このため秘文では図1に示すようにWindowsの中でファイルI/Oを横取りして暗号化と復号を行っている。すなわち，ファイルの種別やフォルダにより，利用者ファイルかシステムファイルかを判別し，利用者ファイルのI/Oデータなら暗号化や復号処理を行うようにしており，利用者が暗号を意識することがなく，上記の(1)と(2)を実現する。あわせて外部媒体への書込み制限による持ち出し制御も行っており，(4)を実現できる。(3)については後述する。

OSを含めてディスク全体を暗号化する方式と異なり，ファイルの位置を意識して暗号化することにより，以下のメリットが得られる。

(1)復号に必要な認証としてプリブート認証が不要であり，Windows認証1回のみでファイルが復号され，アクセスできるようになる。OSは暗号化されていないので，Active Directoryや認証トークン，生体認証などWindowsで利用可能な認証手段が復号に必要な認証として利用できる。

(2)ハードディスクのほかに，外部媒体，外付けディスク，ファイルサーバ上のファイルも暗号化できる。

(3)さらに，情報持ち出し制御としての外部媒体への書込み制御が可能となる。

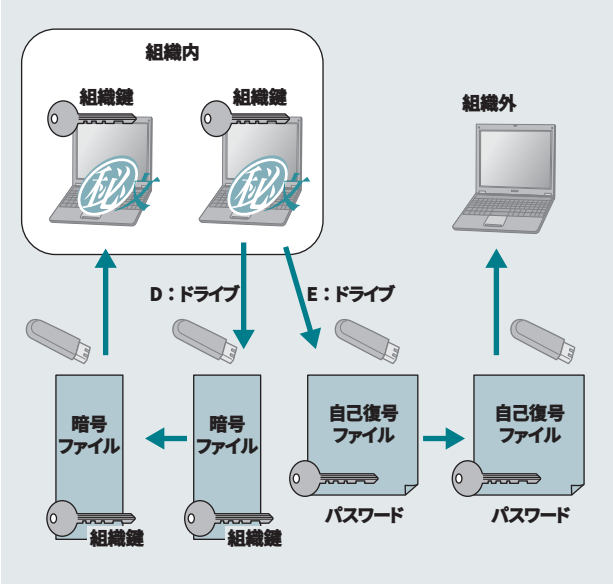


図2 外部媒体への暗号化書き出し
「組織内暗号ドライブD:」に書き出した場合には組織鍵で暗号化，「組織外暗号ドライブE:」に書き出した場合には復号エンジンを含んだファイル形式である自己復号形式に暗号化する。

(4)外部媒体を暗号化するときに，復号エンジンを含むファイル形式(自己復号形式)に暗号化することにより，秘文の利用者でない組織・グループ外利用者向けの暗号化が可能となる。

先の(3)の組織・グループ内にとどまるファイル持ち出しと上記の(4)を補足する。外部媒体への書込みは原則禁止しているが，ファイルを暗号化しておけば問題は生じない。ただし，復号に必要な鍵をどのようにして書込み側PCと読込み側PCで共有するかが問題となる。図2に示すとおり，秘文AEでは，同一組織内ではインストール時に組織鍵を共有することで，組織外では自己復号形式に暗号化して復号用パスワードを利用者間で共有している。こうすることで組織/グループ内では従来どおりの媒体を使ったファイル共有ができる。

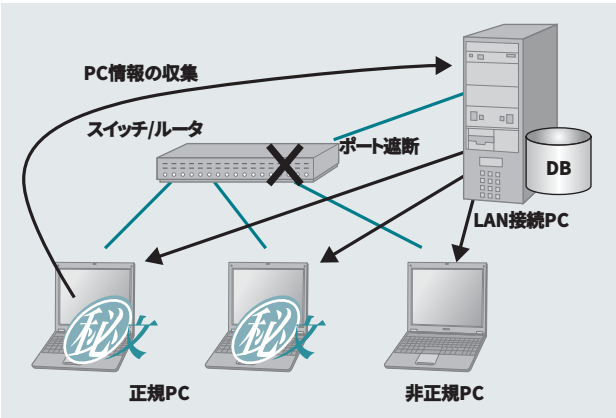
3.2 印刷物による漏洩への対策

前述したとおり，漏洩経路としては印刷物が大きな割合を占める。暗号化だけでは十分な対策とは言えないのが現状である。印刷した情報を暗号化するわけにはいかないが，不要な印刷を制限し，印刷物の取り扱いを喚起するという観点から，印刷制限と透かし入り印刷には効果があると言える。秘文AEでは両機能とも秘文モジュールにおいて，プリンタへのアクセス制限やプリンタへの書込みデータに透かしデータを挿入することで実現している。

4 秘文ME：PC状況の可視化によるPDCAサイクル

秘文AEを用いることで，媒体や印刷物による漏洩を防ぐことができるが，秘文AEをインストールしていないPCからの漏洩を防ぐことはできない。これはウイルス対策についても同様であり，Windows Updateやウイルスパターンファイル更新をしていないPCのウイルス感染を防ぐことはできない。秘文MEを用いることで，情報漏洩防止とウイルス防止の漏れのない対策を実現することができる。秘文MEの概略を図3に示す。

秘文MEのサーバがLAN(Local Area Network)に接続しているPCを自動的に検知して，登録済みの正規PCか否か，秘文MEエージェントのインストールの有無を確認し，非正規PCと判断すると管理者に通報し，スイッチのポートを閉じてLANから遮断する。さらに，正規PCに対しては，秘文AE/MEのインストール状況，Windows Update



注：略語説明 DB（Database），LAN（Local Area Network）
図3 秘文MEを用いた漏洩対策の監視
秘文MEサーバが非正規PCを検知し，通信を遮断する。正規PCからはセキュリティ情報のほかにインストールソフトウェアの情報を収集し，資産管理にも利用できる。

状況,ワクチンソフトのインストール状況,ウイルスパターンファイルの更新状況などのセキュリティ情報をサーバに収集する。サーバでは収集した情報の要約を見ることができる。これら一連の監視を通じて，ウイルス対策を含めた漏洩防止対策状況を可視化し，管理者が現状を的確に把握して改善につなげることができ，PDCA（Plan, Do, Check, and Action）サイクルによるセキュリティマネジメントを実現する。

5　二系統端末：未知ウイルス対策

5.1　未知ウイルス対策の必要性

今後，問題が大きくなると予想されるクライアントPCからの漏洩の原因として未知のウイルスによる漏洩がある。第一の要因として，ウイルス作成ツールが整い，特別な技術がなくてもウイルスが作成できるようになったことがある。次から次へと新しいウイルスが出現するため，既存ワクチンソフトのウイルスパターンファイルの作成，配布が間に合っていない現実がある。

第二の要因として，ターゲット攻撃と呼ばれる対象を絞った攻撃手法が現れたことにある。個人や役職，組織を絞って攻撃しており，攻撃が目立たないため，ウイルスが発見されにくい。このため，ウイルスパターンファイルに含まれず，ウイルスを検知できない可能性が大きい。

第三の要因はSaaS（Software as a Service）の普及である。従来までは，顧客や売り上げなどの秘密情報はファイヤウォールで守られたLAN上のサーバに置かれていたが，SaaSが普及すればインターネット上に置かれるようになる。従業員のアカウント情報が入手できれば，いつでも，どこからでも秘密情報を盗むことができる。インターネットバンキング向けのフィッシングやキーロガーなどアカウント情報を盗む手段はすでにあり，攻撃対象を変えるだけでSaaSのアカウント情報も入手可能であると言える。

5.2　仮想化技術とセキュアOSによるデータ分離

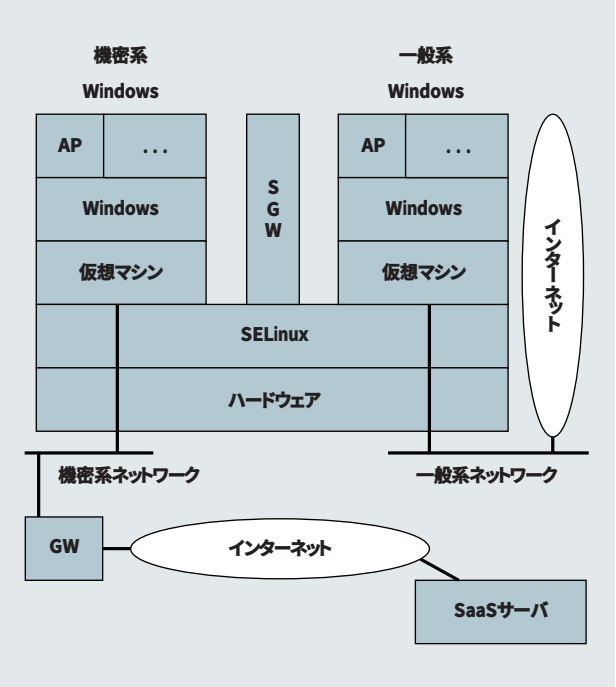
パターン照合による方法のほかに，コードの振る舞いによりウイルスを検知する技術が開発されているが，万全とは言えない。ウイルス作成者はワクチンソフトを入手して，検知方法を分析したり，検知されないようにウイルスのコードをチューニングできるからである。

このような未知のウイルスから秘密情報を守るため，暗号でもウイルス検知でもない別の発想による漏洩対策が二系統端末である。これは「ネットワークにつながなければ安全である」というコンセプトを実現したシステムである。漏洩しては困る秘密情報を扱う機密系Windowsとその他の情報を扱う一般系Windowsを，情報とOSをまとめて二つに分離し，仮想化技術とセキュアOSを使って1台のPCに統合したシステムである。その他の情報にはインターネット上の情報を含む。その構成を**図4**に示す。

二つのWindowsは，それぞれ機密系と一般系のネットワークに接続されている。機密系ネットワークは，他の二系統端末の機密系WindowsのほかにLAN上の業務サーバやゲートウェイを介してSaaSサイトなど秘密情報を扱うサーバとのみ接続する。一方，一般系ネットワークは他の二系統端末の一般系Windowsやインターネットと接続する。このように二つのWindowsはネットワークを含めて仮想的に物理レベルから分離されている。

このため，仮にインターネットに接続している一般系Windowsがウイルスに感染しても，機密系Windowsまで感染が広まる危険性はない。仮想マシンに脆弱性があり，仮にこの脆弱性を攻撃するウイルスが現れたとしても，仮想マシンの下位にあるSELinux（Security-Enhanced Linux※2）[4]で攻撃を防ぐことができる。SELinuxは，プロセスにドメイン，リソースにタイプというラベル付けを行い，ドメインからタイプへのアクセスを例外なくポリシーに基づいて制限をかける強制アクセス制御を実現する。このためルート権限があるプロセスでもポリシーに従ったアクセス制限を受け，仮想マシンがウイルスに乗っ取られてもほかの仮想マシンを攻撃することはできない。ポリシーはセキュリティ管理者のみが設定でき，いわゆる

※2　Linuxは，Linus Torvaldsの米国およびその他の国における登録商標あるいは商標である。



注：略語説明　AP（Application），SGW（Security Gateway），SELinux（Security-Enhanced Linux），SaaS（Software as a Service），GW（Gateway：SaaSサーバとの通信のみを許可）

図4　二系統端末の構成
情報とシステムを機密系と一般系に完全に分離することにより，インターネットなど外部からのウイルス侵入を防ぐことができる。

ルート権限があっても変更することはできない。

このように二つのWindowsを分離しておけば，一般系から機密系へのウイルス侵入がなく，逆に機密系から一般系，さらにインターネットへの情報漏洩は起きない。しかし，このままではウェブやメールで得た情報を秘密情報として取り込むことはできなくなってしまう。そこでSGW（Security Gateway）を設けることにより，一般系から機密系へのコピーアンドペーストを実現している。クリップボード経由でコピーできる情報は，利用者が視認して操作できるデータであり，その中にプログラムコードは含まれておらず，ウイルスが含まれる可能性はないと考えられる。「ネットワークにつながなければ安全である。」の原則を守りつつ，使い勝手を向上している。

しかしながら，メールやウェブブラウザは，相手やアクセス先を意識して機密系と一般系を使い分ける必要があり，使い勝手には向上の余地が大きい。メールとウェブに関しては，機密系と一般系のクライアント統合は可能であるが[5]，インターネット電話やインスタントメッセージなど新たなネットワークアプリケーションは課題となっている。

6　おわりに

ここでは，情報漏洩の現状を，原因別に対策方針をそれぞれまとめ，解決策として「秘文AE」によるファイルや印刷物による漏洩の防止，「秘文ME」による漏れのない対策の監視，さらに今後被害が発生すると予想される未知ウイルスによる漏洩への対策として二系統端末について述べた。

個人情報保護法の施行後も個人情報の漏洩事件は発生しており，ゼロになるとは考えられない。また，ウェブ2.0やSaaS，P2Pに見られるように新しい形態のネットワーク利用が普及すれば，新たな経路による情報漏洩や攻撃手法が発生，新たな対策が求められると予想される。ユビキタス情報社会においても，その利点を妨げない，使い勝手のよい情報漏洩対策を含めたセキュリティ技術の開発が求められる。

参考文献など
1）**日立ソフト，秘文，**
http:// hitachisoft.jp/products/hibun/product/
2）**日立ソフト，ニュースリリース**（2007.12），
http://www.hitachi-sk.co.jp/news/news487.html
3）NPO**日本ネットワークセキュリティ協会，**2006**年情報セキュリティインシデントに関する調査報告書** Ver.02.00（2007.10）
4）P.Loscocco,et al.：Meeting Critical Security Objectives with Security-Enhanced Linux, in Proceedings of the 2001 Ottawa Linux Symposium, http://www.nsa.gov/selinux/papers/ottawa01.pdf（2001.7）
5）Y.Sameshima,et al：Windows Vault: Prevention of Virus Infection and Secret Leakage with Secure OS and Virtual Machine, in Pre-Proceedings of the 8th International Workshop of Information Security Applications 2007（WISA 2007）, pp.249-261（2007.8）