〈ソリューション〉

オフィスセキュリティ（情報漏えい対策）

Secure Office System （Information Leak Prevention Method）

大瀧　潔* 山井忠則* 福田光司** 宮崎義昭**
Kiyoshi Otaki Tadanori Yamai Koji Fukuda Yoshiaki Miyazaki

要　旨

近年，機密情報の漏えいに関する様々な事件がマスコミなどから報道され，その影響の大きさが広く社会に認知されるに従い，社会問題となってきています。さらには個人情報の保護などに関する法律の施行が間近となり，個人情報も含めた情報の漏えい対策の必要性が高くなっています。これらの漏えいの多くは内部に大半の原因があることが報告されており，オフィスの内部のセキュリティ対策が重要であることは論を待ちません。本稿では，このようなオフィスセキュリティのなかでも「情報漏えいを防止する」という観点からその原因と具体的対策を議論します。

In recent years, various incidents about disclosure of confidential information are reported from newspapers, TV programs, etc. It is becoming a social problem as the largeness of its influence is widely recognized in the society. It is reported that many of these disclosures have causes inside of office. Therefore, the security measure inside of office is important for argument. This paper discusses the cause and measure from a viewpoint of “preventing an information leak” for such office security.

1. はじめに

数十万といった大規模な個人情報の漏えい事件が新聞やテレビを騒がし，いっこうに収束する気配がありません。このような，情報の漏えい問題は，古くて新しい問題であるといわれています。業務活動の様々な情報がITで管理される以前から，漏えい事件は発生していたといわれています。たとえば，紙の台帳でファイルされていた会員情報がコピーされて持ち出されたといったことは頻繁に発生していました。

ここ数年にわたり，大規模な流出事件がITを経由して発生したり，個人情報の管理に対する社会意識が高まったことから機密情報の漏えい問題が社会の大きなテーマの1つとして取り上げられることが多くなってきています。現在では，個人情報や設計情報，取引情報などの多くの情報資産が，ITを活用して収集，操作，管理されており，サーバなどに大量に蓄積され万一漏えいとなった場合はその影響は非常に大きいと考えられます。すなわち，情報漏えい対策はITの重要なキーポイントとなったといえます。

2. 対策の必要性

このような，情報漏えい問題の7～8割は内部に起因する要因で発生しているといわれており，この問題はまずオフィス内部のセキュリティレベルを上げることから対策が始まるといっても過言ではありません。しかしながら，総務省の統計[1)]では，媒体などの持ち出し制限は自治体では約半数，上場企業においては20％足らずしか実施していないなど，内部における漏えい対策は十分とはいえない状況です。

情報漏えい事件が発生した場合の事業に与える影響としては以下の点があります。

1）漏えいされたことに端を発した直接の損害賠償責任

これは特に個人情報漏えいに関しては，判例として一人当たり1万円という事例があります。また，大規模漏えいの場合見舞金として500円を支払うという例が報告されています（合計で十数億円）。

2）サプライチェーンやデマンドチェーンさらにはCRMといった企業間・団体間などの連携業務や研究の枠組みから参加を拒否されるという問題

いくつかの企業においては，サプライチェーン参加の条件に一定の情報セキュリティ強化を指定するところも多くなってきています。

3）遵法の精神，コンプライアンス

個人情報の保護などに関する法律や不正アクセス防止法等の関連する法律への遵守が企業市民として求められ，事件発生時は監督官庁からの指導も発生する可能性があります。

このように個人情報の保護などに関する法律の施行が

＊ ソフトウェア販売推進本部
Software Promotion Division

＊＊ ユビキタスソフトウェア事業部
Ubiquitous Software Division

2005年に迫った今，情報の保全が必要となっており，機密情報を保持する官公庁，企業，団体にとってはまさしく，情報漏えい問題への対応は「待ったなし」といえます。

3. 情報漏えい事件に見る対策の指針

情報セキュリティは非常に幅の広い分野での対策が必要であること，またその費用予算は必ずしも潤沢でない場合が多い[1]ことから，対策は「①どんな種類の対策」を「②どこまで，どこに」やればよいのかというのが常に情報セキュリティの担当者にとって頭の痛い問題となっています。守るべき情報資産の内容，場所，管理方法は様々であり，経営環境もバラバラです。したがって，漏えい対策もそれに応じて千差万別であるのは当然ですが，一方では，ある程度の指針も必要となっているのです。

「①どんな種類の対策」を打つのかの指針を検討する場合には発生した情報漏えい事件のなかで，対策を分析し，それ参考にしながら立案することが1つの方法です。公開された事件と対策を整理し，必要となる要素にまとめたものが図1です。この図では，以下の3つのポイントを対策の種類の例としてあげています。

(1) 認証の強化

業務システムやネットワークの利用における基本的な概念としての認証を強化します。たとえば退社した社員のIDを速やかに無効にするとか，部門でIDを共用するといった問題を解決すると同時に，パスワードという記憶認証手段だけではなくICカードや生体認証といった異なる種類の認証を加えることで，認証の強化につながります。

(2) 操作記録の取得と保全

万が一漏えい事件が発生した場合にその原因を特定するため，また不正行動を抑止するためにも操作記録の取得は非常に有効です。

(3) 情報のアクセスの制限や暗号化

情報の持ち出しのリスクが一般に高いので，その持ち出しを制限したり，持ち出した場合でも権限のない人には見せないようにする（暗号化）が必要となります。

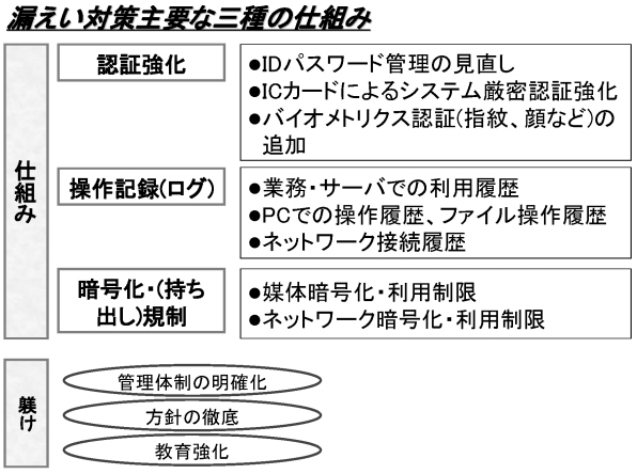


図1　対策例に見る情報漏えいの取り組み
Fig.1　Patterns of measure against information leak.

4. 情報漏えい対策パタン

オフィスセキュリティとしての情報漏えい対策は，オフィス内部を対象としていることから，人，利用しているPC，サーバ，ネットワークなどの管理すべきポイントが広範囲に渡ってしまいます。そのため，守るべきポイントの選定が難しく，「どこまで，どこに」という問題が発生する原因になっています。そこで，オフィス内部のセキュリティレベルを3つ（図2参照）に分類，その境界を通過する情報に注目し，対策をパタン化することで分かりやすくしています。これらの対策は以下の6つの対策となります。

(1) ICカードなどを利用した個人認証強化対策

社員証/職員証ICカードを利用し，ネットワークの認証を始めとして，入退管理やパソコンの利用者認証を行なうことで，本人以外の不正な利用を防止（図3）。

(2) 外部持ち出し情報保護対策

パソコンのハードディスクや，USBメモリ・フロッピー

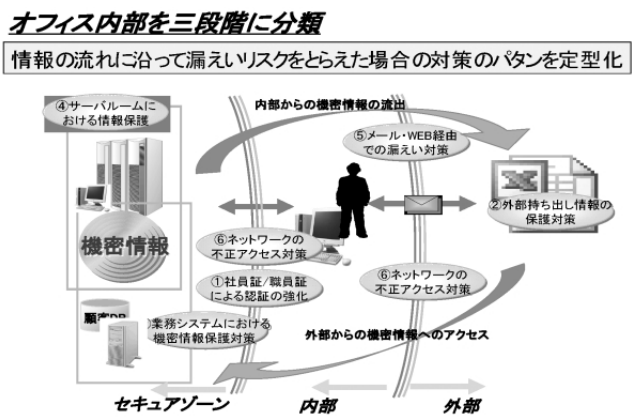


図2　オフィスセキュリティ（情報漏えい対策）の対策パタン
Fig.2　Security risks in office.

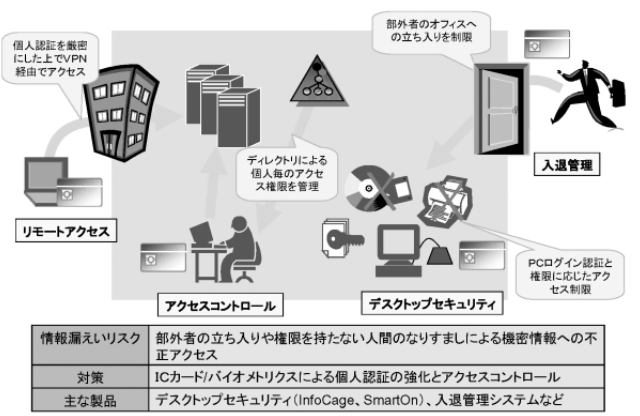


図3　社員証ICカード個人認証強化対策
Fig.3　Strengthening of individual authentification.

ディスクなどの外部記憶媒体に保存されたデータを暗号化または制限することで，パソコンや外部記憶媒体の盗難・紛失による情報漏えいを防止。また，メールで情報交換を行うファイルを暗号化することで，盗聴などにより第3者への情報漏えいを防止（図4）。

(3) 業務システム機密情報漏えい対策

データベースやファイルサーバへの不正アクセス，業務システムに接続した端末での不正操作を防御もしくは監視することで，機密情報が外部へ持ち出されるのを防止（図5）。

(4) サーバ情報保護対策

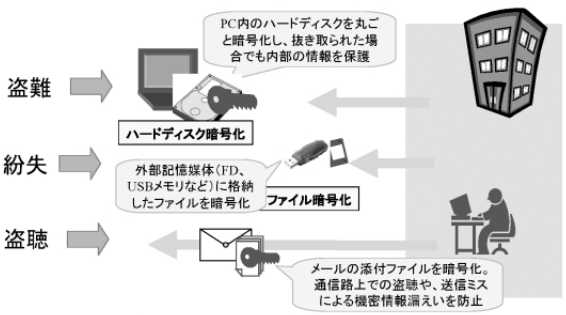
入退室管理など，物理的なものの出入りを管理するとともに，サーバやオペレーション端末へのアクセス履歴を収集・保管し，情報の保全を行う（図6）。

(5) メール/Web経由情報漏えい対策

電子メールの送信や，社内からのWebメール・掲示板・チャットなどへのアクセスを規制することで，インターネット経由での外部への情報漏えいを防止（図7）。

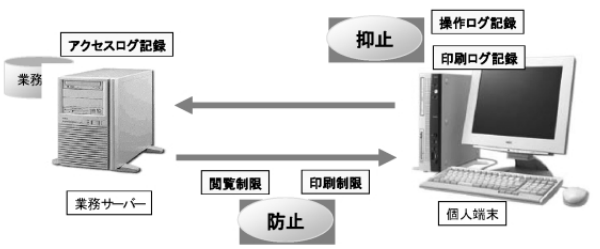
(6) ネットワーク不正アクセス対策

ネットワークへの接続時に，厳密な個人認証を行うことにより，権限をもたない人間が，ネットワーク経由で情報にアクセスし，不正に持ち出すのを防止，さらには権限のないネットワーク機器の接続を防止したり，論理的なネットワークアクセスを実現（SecureVisor，UNIVERGE IP8800シリーズなど）（図8）。



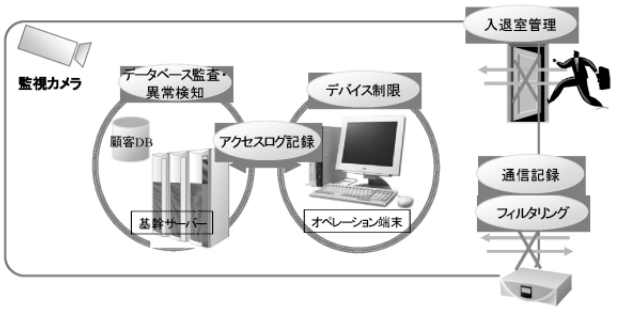
情報漏えいリスク	ノートPCや外部記憶媒体の盗難、紛失による機密情報の漏えい。メールの盗聴による情報の搾取。
対策	ハードディスクやファイル単位での暗号化など
主な製品	SecureWare／ファイル暗号化ツール、InfoCage、DocumenteSecurity他

図4　外部持ち出し情報保護対策
Fig.4　Defencing of carrying-out information.



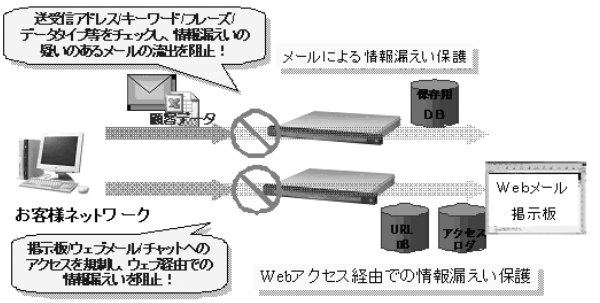
情報漏えいリスク	業務サーバへの不正アクセスと業務用個人端末からのデータの不正操作、個人情報の不正コピー
対策	クライアント操作ログ・印刷ログの採取、データベース書き換え監視、印刷制限
主な製品	デスクトップセキュリティ(InfoCage、SmartOn)、SecureWare

図5　業務システム機密情報漏えい対策
Fig.5　Information leak prevention (operating PC/server).



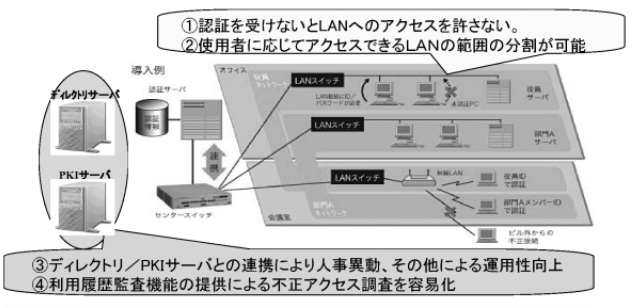
情報漏えいリスク	セキュリティエリア内への部外者の侵入、データの盗聴、持ち出し
対策	入退室セキュリティ強化、操作履歴の保存による抑止、リムーバブルデバイスの制限
主な製品	IPLocks, 入退管理システム、各種ログ管理、ネットワーク構成の見直しなど

図6　サーバ情報保護対策
Fig.6　Information leak prevention (server room).



情報漏えいリスク	ウェブサイト上でのWebメール使用・掲示板書き込みとメール添付ファイルの流出
対策	URLフィルタリングとメールフィルタリングとをセットにしたコンテンツフィルタリング
主な製品	InterSafe、GUARDIAN WALL、MAILsweeper、SecureWare

図7　メール/Web経由情報漏えい対策
Fig.7　Information leak prevention (depend on e-mail/URL).



情報漏えいリスク	権限を持たない人間が、社内LANに接続するだけでイントラネットの不正アクセス
対策	LAN利用時に認証を行い、LANのアクセス可否と利用可能LANをコントロール
主な製品	IP8800/700シリーズ＋ WebSAM VLANaccess Solution Pack CapsSuite　SecureVisor

図8　ネットワーク不正アクセス対策
Fig.8　Network irregular access prevention.

5. ステップバイステップでの展開

オフィスセキュリティの管理する対象がネットワークやサーバといった管理手法が確立しやすいものから，内部の

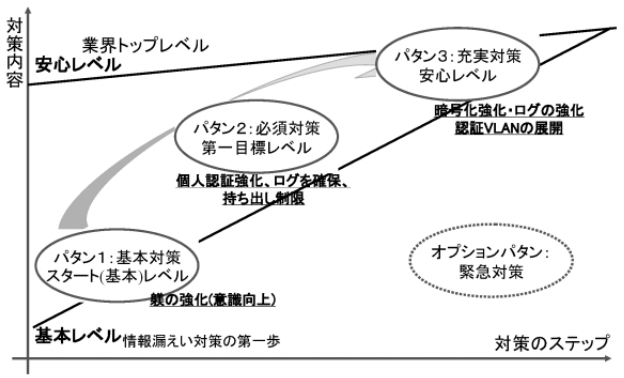


図9　対策のステップ
Fig.9　Step of measure.

社員や職員，内部で活用するPCといった管理手法が確立しにくいものに広がってきています。したがって対策を一気に進めると現場での運用がうまく回らず混乱が発生し，その結果実効のないシステムとなってしまう危険性があります。オフィスセキュリティは運用が回らなければ何の役にも立たないどころか逆に業務効率を下げたり，予期せぬ漏えいにつながる危険を持っています。図9にあるような基本レベルから安心レベルまでステップバイステップで導入を進めることが重要です。

6. むすび

従来の日本のオフィスでは性善説に基づき，情報保全の試みは真剣に行っていなかったのが実態であると思われます。しかし，個人情報に関する法律の制定など，取り巻く環境が変化し，オフィスのセキュリティそのものを見直す必要性が出てきています。情報セキュリティの分野でもオフィスセキュリティは非常に管理が難しいといわれています。しかし，ステップバイステップの方針で前述の対策を確実に実施することで，過去に発生した事件のいくつかは防げていたはずであると考えます。

NECでは，今後もUNIVERGE製品と連携し，オフィスセキュリティ（情報漏えい）対策の施されていないパソコンの検疫をはじめとして，オフィスセキュリティを確実にする新しいソリューションを提案していきたいと考えています。

参考文献

1）　情報セキュリティに関する実態調査（平成16年7月　総務省公表）

筆者紹介

Kiyoshi Otaki
大瀧　潔（おおたき　きよし）　1984年，NEC入社。現在，ソフトウェア販売推進本部グループマネージャー。

Tadanori Yamai
山井　忠則（やまい　ただのり）　1993年，NEC入社。現在，ソフトウェア販売推進本部主任。

Koji Fukuda
福田　光司（ふくだ　こうじ）　1982年，NEC入社。現在，システムソフトウェア事業本部ユビキタスソフトウェア事業部マネージャー。

Yoshiaki Miyazaki
宮崎　義昭（みやざき　よしあき）　1987年，NEC入社。現在，システムソフトウェア事業本部ユビキタスソフトウェア事業部マネージャー。