“環境管理型”情報漏えい対策の重要性
―セキュリティと利便性を両立させた暗号化ソリューション―

なぜ情報漏えい事故はいつまでもなくならないのであろうか。情報漏えい対策ソリューションの選択肢は増えているにもかかわらず、情報漏えい事故は減るどころか増加傾向にある。本稿では、ヘルスケア分野での情報漏えい対策ソリューションの導入経験に基づいて、企業の現実を見据えた情報漏えい対策、特に暗号化による対策について考察する。

増える情報漏えい事件

世の中にはさまざまな情報漏えい対策ソリューションがあふれている。それにもかかわらず、情報漏えい事件はなくなるどころか増加傾向にある。なぜ情報漏えいは減らないのだろか。

図１は、アイティメディアが公開している、情報漏えいの原因について2010年に行われた調査の結果である。PCやUSBメモリーの紛失など、上位にあげられる原因に共通しているのは、それが人為的なミスによるものだということである。これに比べて外部からの攻撃などは割合としては小さい。人的ミスを完全になくすことはできない。このことが、情報漏えいが減らない大きな要因の１つである。

情報漏えいが減らないもう１つの要因は、情報共有がますます進んでいることである。情報は、それが共有されることによってさらに価値が高まる。企業にとっては、社内で情報を共有し、組織の生産性を高めることはますます重要になっている。

情報を共有する人間が多数おり、人間は必ずミスを犯すという単純な事実が、情報漏えいがいつまでもなくならないことの背景にある。従って、情報漏えい対策にとって肝心なことは、人的ミスの発生を前提とすること、および情報共有の妨げにならないことである。

筆者はヘルスケア分野のシステム導入を専門としている。この分野は医師や患者の個人情報が多く扱われるため、情報漏えいには特に気をつけられている。以下では、野村総合研究所（NRI）がある製薬企業に対して行った情報漏えい対策ソリューション導入の経験に基づいて、あるべき情報漏えい対策について考える。

これまでの情報漏えい対策の問題点

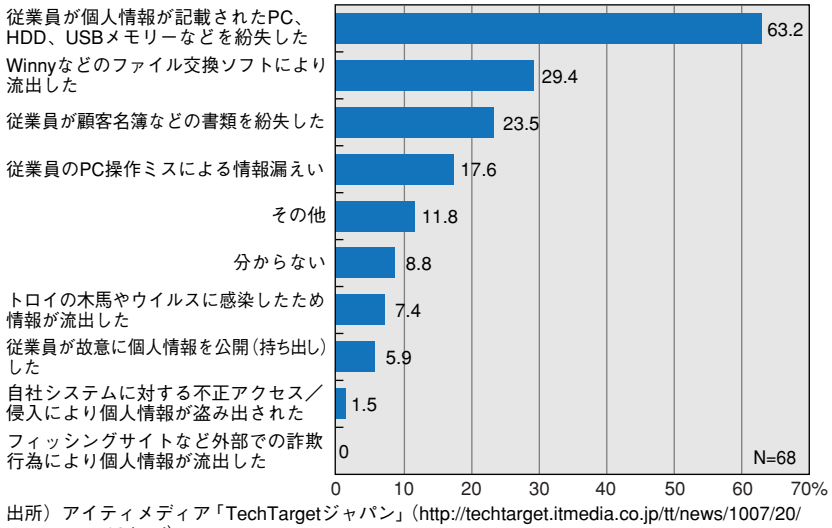
情報漏えい対策として最も一般的なのは、「アクセス権管理」と「暗号化」という２つの方法である。

アクセス権管理は、組織別、機密レベル別のアクセス制限が一般的である。各社員がアクセスできる情報を最小限にすることにより、情報漏えいのリスクは確かに減らすことができる。しかし、少数とはいえ、機密情報にアクセスできる社員がミスによって情報漏えいを起こす可能性は残る。また、リスクを小さくしようとすればするほど情報共有の範囲が狭くなり、組織としての生産性は低下する。

野村総合研究所
ヘルスケア・ERPソリューション事業本部
ヘルスケアシステム開発部
主任システムエンジニア
末廣信太郎（すえひろしんたろう）
専門はヘルスケア領域の情報系システム開発

暗号化は、どの部分で暗号化を行うかが問題になる。PCのハードディスクやUSBメモリーなどの機器レベルでデバイスを丸ごと暗号化する対策は一般的になってきている。これは機器の紛失による情報漏えいに対して一定の有効性はあるが、中身のファイルを持ち出されてしまうリスクはなくならない。

図1　情報漏えいの原因



出所）アイティメディア「TechTargetジャパン」（http://techtarget.itmedia.co.jp/tt/news/1007/20/news03.html）

最も確実な方法は、個々のファイルを暗号化することである。ファイルそのものが暗号化されていれば、たとえ持ち出されたとしても情報漏えいは防げる。しかし、ファイルを1つ1つ暗号化する方法では暗号化をし忘れる危険もあり、また権限を設定された人間やパスワードを知っている人間しかアクセスできないため情報共有の範囲が限定される。

複数のソリューションを組み合わせる

上記のように、アクセス権管理、暗号化のどちらも有効な対策ではあるが、それだけでは人的ミスによる情報漏えいを完全には防げず、情報共有の範囲も狭めることになる。

人的ミスの発生を前提とし、情報共有を妨げない単一のソリューションを見つけることは難しい。そのため、複数のソリューションを組み合わせてこれを実現する必要がある。筆者らが採用したのもこの方法である（次ページ図2参照）。

(1) ファイルの自動暗号化

ミスが起きても情報漏えいが起きないようにするためには、暗号化が自動的になされなければならない。筆者らは、製薬企業での情報漏えい対策として、米国Microsoft社のグループウェア「Microsoft Office SharePoint Server」（以下、SharePoint）と暗号化ソリューション「Windows Rights Management Services」（以下、RMS）を組み合わせたソリューションを選定した。

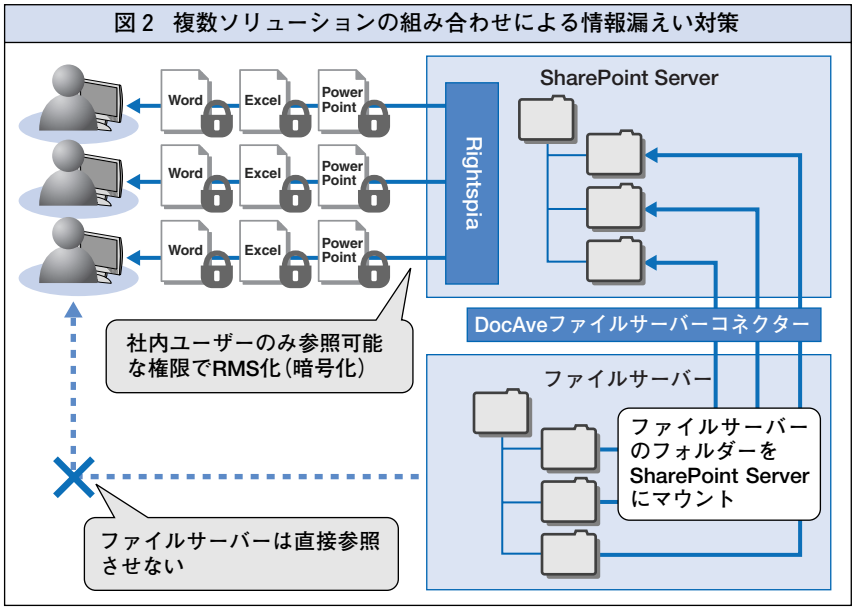
SharePointは企業内の情報共有基盤として普及しつつある製品である。通常のWindows上のフォルダーにアクセスするのと同じ感覚

で、ファイルサーバーのようにSharePointを利用することが可能である。

暗号化の対象となるのはSharePoint内のMicrosoft Officeファイルで、これを取り出す際に自動的にRMSで暗号化される。

RMSで暗号化したファイルは、権限を持つユーザーのみが開くことができる。暗号化ファイルを開く際には、PCへログインした時に権限が判断されているのでパスワードを入力する必要はない。移動の最小単位であるファイルそのものが自動的に暗号化されるため、例えば電子メールの誤送信などで意図せずファイルが流出しても、情報漏えいが起きるリスクは格段に低い。

図２　複数ソリューションの組み合わせによる情報漏えい対策



(2) 情報共有を妨げない

先に述べたように、暗号化は情報漏えいを防ぐことはできても情報共有を妨げるというジレンマがある。この点ではSharePointとRMSによるファイルの暗号化も課題を残している。SharePointの暗号化機能では、ファイルを開けるのはダウンロードした本人のみであるため、ファイルを社内の別ユーザーと電子メールなどで共有するといったことができないからである。

これを解決するため、筆者らは「社員のみ開ける形での暗号化」を実現した。フォルダーなどの単位で適切なアクセス権管理を行っていれば、ファイル単位の暗号化時に細かく権限を制御する必要性は低い。従って、暗号化は社外への情報漏えい対策と割り切り、社員であれば暗号化を意識せずにファイルを開けるようにしようという考え方である。具体的には、ファイルを暗号化する際の権限設定を変更するソリューション（富士通エフサスの「Rightspia for Secure Documents」）をSharePointと組み合わせることによって実現した。

(3) 大量の既存ファイルを新基盤に移行

情報漏えい対策を真に有効なものとするためには、もう１つ大きな課題がある。それは、大量の既存資産すなわち既存の多数のファイ

ルサーバーと、その中の膨大なファイルをどう守るかということである。

ファイルサーバーは、ほとんどの企業で利用されている情報共有手段であるが、情報量が増えるにつれて必要な情報を見つけにくくなり、活用されないファイルが削除されずにひたすら蓄積されていく傾向がある。大きな問題は、活用されない大量のファイルの中に機密情報や個人情報が含まれ、情報漏えいのリスクが放置されていることである。筆者らが情報漏えい対策ソリューション導入に際して直面したのも、大量の既存資産をどうするかという問題であった。大量のファイルを別基盤に移行するのは非常に時間のかかる作業だからである。

筆者らはこの問題を解決するために、従来のファイルサーバー上のファイルを残したまま、ファイルにアクセスするための入口のみSharePointに置き換えることにした。採用したのは米国AvePoint社の「DocAve」である。これにより、新システムへの移行時間を大幅に短縮することができた。また、利用されていないファイルを一定期間後に自動削除するようにした。

セキュリティ対策は“環境管理型”へ

セキュリティ対策を強化すると、「不便」や「面倒」といった声が社員の間から聞こえてくることがある。これはセキュリティ対策を強いられる社員の本音であろう。セキュリティのために、従来の業務にさまざまな手続きが付け加わり、業務効率や利便性が犠牲にされる。問題が起きるたびにルールや手続きが増え、社員の仕事は増える一方である。

ルールを作り、そのルールを守るよう社員を訓練・監視する従来の“規律訓練型”のセキュリティ対策はもう限界に来ている。これからは、“環境管理型”セキュリティ対策への移行が必要である。

環境管理型セキュリティ対策とは、社員がその環境内で自由に活動しても結果的にセキュリティが守られるような環境を作ることである。忘れてならないのは、セキュリティ対策は企業のビジネスにとって本業ではないということであり、セキュリティのために本業の業務効率が下がることがあってはならない。ソリューションの選択肢が増えている今、複数のソリューションを適切に組み合わせて、利便性とセキュリティを両立させた環境を実現することが可能になってきている。

このような環境を実現するためには、部分最適に陥ることなく、社員を取り巻く環境全体を最適に設計する幅広い視点が必要である。同時に、新しいソリューションを組み合わせる際に起こりやすい問題にも注意を払う必要がある。

本稿で紹介した環境管理型のセキュリティ対策ソリューションが、今後の情報漏えい対策の大きな流れとなっていくことは間違いないであろう。 ■