

「環境管理型」情報漏えい対策の重要性

末廣信太郎

情報漏えい事故はなぜいつまでもなくなるのであろうか。情報漏えい対策ソリューションの選択肢は増えていにもかかわらず、事故は減るどころか増加傾向にある。その原因は、企業内で組織としての生産性向上のための情報共有が進む一方で、情報にアクセスする社員の人為的なミスは完全になくすることができないことにある。セキュリティ向上のために、企業にとって本業の業務効率を下げることは避けなければならない。今求められているのは、社員が意識しなくても情報漏えいが起こらない「環境管理型」の情報漏えい対策である。

増える情報漏えい

世の中にはさまざまな情報漏えい対策ソリューション(課題解決)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うか。

図1は、アイティメディア(IT media)が公開している、情報漏えいの原因について2010年に行われた調査結果である。パソコンやUSBメモリの紛失など、上位に挙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。人為的なミスを完全になくすることはできない。このことが、情報漏えいが減らない大き

な要因の一つである。

情報漏えいが減らないもう一つの要因は、情報共有がますます進んでいることである。情報は、それら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、社内で情報を共有し、組織の生産性を高めることは一層重要になっている。

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るものの背景にある。したがって、情報漏えい対策にとって肝心なことは、人為的なミスの発生を前提とすること、それが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なければならない。以下では、野村総合研究所(NRI)が、ある製薬企業の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の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。

暗号化は、どの部分で暗号化をするかが問題になる。現在、パソコンのハードディスクやUSBメモリーなどの機器レベルにおい

て、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。これら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ものの、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。

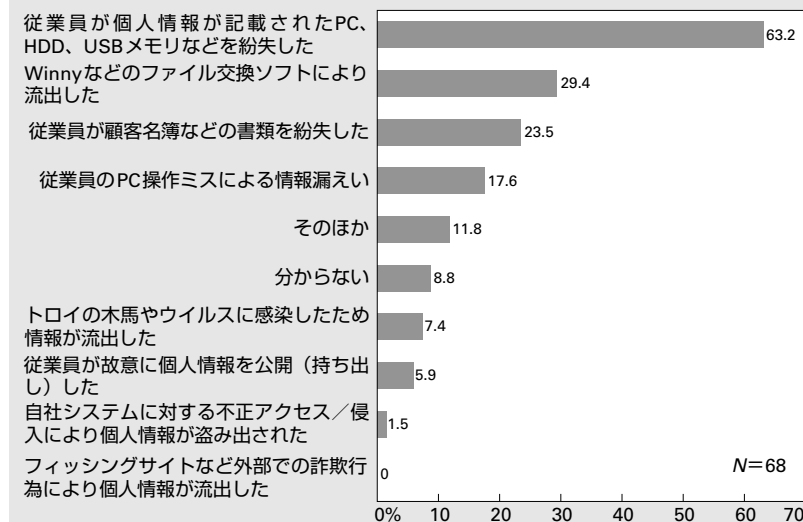
最も確実な方法は、個々のファイルを暗号化することである。ファイルそのものが暗号化されていれば、たとえ持ち出されたとしても情報漏えいは防げる。しかし、ファイルの一つひとつ暗号化する方法では暗号化をし忘れる危険もあり、また権限を設定された人間やパスワードを知っている人間しかアクセスできないため、情報共有の範囲が限定される。

複数のソリューションを組み合わせる「環境管理型」

上述のように、アクセス権管理と暗号化はどちらも有効な対策ではあるが、それだけでは人為的ミスによる情報漏えいを完全には防ぐことができず、情報共有の範囲も狭めることになる。

人為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ることでこれを実現す

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>)

る必要がある。筆者らが採用したのもこの方法である（次ページの図2）。

①ファイルの自動暗号化

人為的ミスが起きても情報が漏えいしないようにするためには、暗号化が自動的になされる必要がある。筆者らは、製薬企業における情報漏えい対策として、マイクロソフトのグループウェア「Microsoft Office SharePoint Server」（以下、SharePoint）と暗号化ソリューションである「Windows Rights Management Services」（以下、RMS）を組み合わせるソリューションを選定し

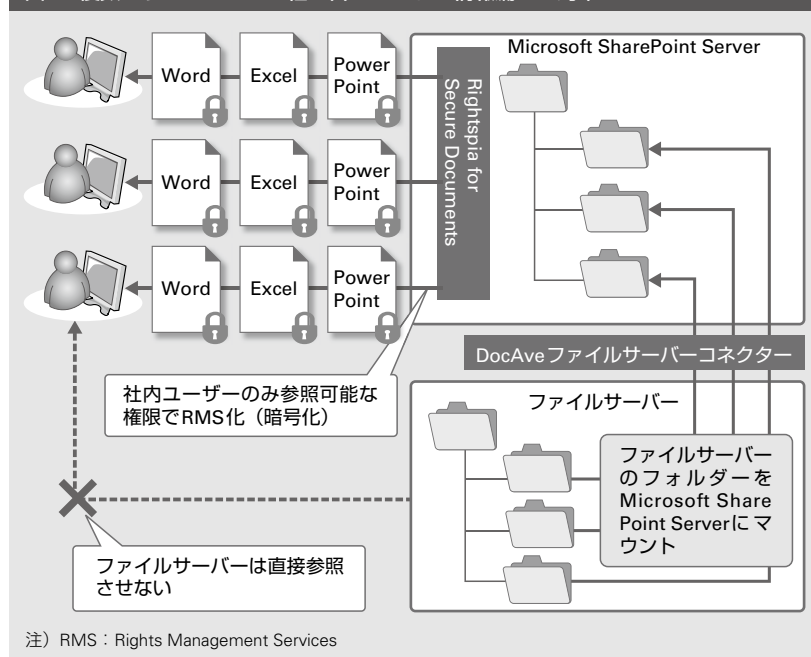
た。

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、ファイルは自動的にRMSで暗号化される。

RMSで暗号化したファイルは、アクセス権限を持つユーザーのみが開くことができる。パソコンにログインした時点で権限が判断さ

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



れているので、暗号化ファイルを開く際には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、たと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。

②情報共有を妨げない

前述のように、暗号化は、情報漏えいを防ぐことはできるが、反面、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、社内の別ユーザーと電子メールなどでファイルを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に筆者らは、「社員のみが開ける形による暗号化」を実現した。通常、フォルダーなどの単位でアクセス権を適切に管理していれば、暗号化時にファイル単位で権限を細かく制御する必要性は低い。したがって、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である富士通エフサスの「Rightspia for Secure Documents」を、SharePointと組み合わせることで実現した。

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、もう一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、そのなか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。

ここでの大きな問題は、活用されない大量のファイルのなか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保護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。採用したのはアブポイント(AvePoint)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もした。

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。

ルールをつくり、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、本稿で述べてきたような、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は保持されるような環境をつくることである。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、セキュリティ保持のために本業の業務効率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、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。

『ITソリューションフロンティア』
2011年5月号より転載

.....
末廣信太郎（すえひろしんたろう）
ヘルスケアシステム開発部主任システムエンジニア