企業におけるコンテンツセキュリティ

足尾勉　坂本久　小林香織　稲垣嘉信　北村晃一　笹鹿祐司　島津秀雄
ＮＥＣシステムテクノロジー（株）　システムテクノロジーラボラトリ

１．はじめに

企業では、膨大な量の電子文書が作成され、格納、流通されている。それらの中には、機密性の高い情報が多数含まれている。たとえば、未発表製品の価格表の記載ファイル、人事情報ファイル、公表前の広報用ファイル、他社との連携に関するやりとりが記述された電子メール、などがあげられる。しかし、それらは必ずしも十分に管理されておらず、企業の情報漏えいリスクを増大させている。本稿では、電子文書そのものが「自分で自分の身を守る」コンテンツセキュリティの概念を紹介しそのアーキテクチャを提案する。

２．情報セキュリティモデルの変遷

企業の情報セキュリティモデルの進化は、図１に示すように３段階に見ることができる。最初に登場したのはゾーンセキュリティだった。これは、企業システム全体を壁で囲い、壁の出入り口を厳重に管理しておけば、その内側は、機器もデータも安全と考えるモデルであり、代表例がファイアウォールである。当時は、デスクトップ PC が主流であり、社員によるノート PC の社外への持ち出しや社内持ち込みは頻繁ではなくゾーンセキュリティで十分だった。

その後、ノート PC が主流になり、電子メール、USB メモリなどの普及が進み、ゾーンセキュリティだけでは不十分になった。そこで、PC やサーバ、ネットワーク機器、USB メモリのようなハードウェアを単位として保護するセキュリティシステムが次々に出現した。たとえば、PC にはパーソナルファイアウォールが搭載され、ハードディスクは丸ごと暗号化され、ファイルシステムには、ウィルスチェックのソフトウェアが実装され、さらに電子メールのクライアントソフトウェアにも、その内容やスパイウェアの有無を検査するソフトウェアが実装され、PC 全体が要塞化された。同様に、USB メモリにも、指紋認証装置付きやパスワード認証装置付きにして要塞化させた商品が続々と出現している。これをプラットフォームセキュリティと呼ぶ。

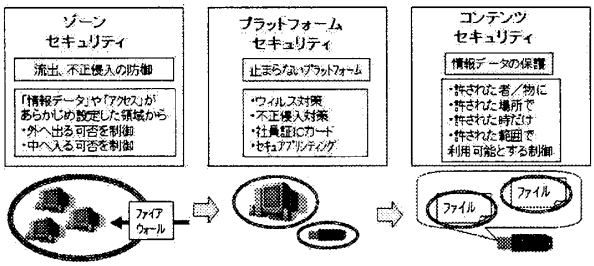

図１　情報セキュリティモデルの変遷

しかし、それらを整備しても情報漏えいの事件や事故はなくなっていない。その理由の１つは、ハードウェア機器のセキュリティ保護の徹底が困難なためである。今日では、ハードウェア機器のコモディティ化、多種多様化が進み、爆発的に普及しており、企業内のハードウェア機器に対してくまなくセキュリティ保護を行うことを徹底するのは不可能になっている。一部の機器がセキュリティ対策を行っていないと、そこから情報漏えいが起こる。ゾーンごとのゲートウェイやハードウェアのチェックポイントでセキュリティの数や種類を増やせば、その分安全になるが、その一方で、チェックポイントを増やすことは、情報システムの管理自体を複雑にするし、本来のパフォーマンスを低下することにもなる。それに、どれだけチェックポイントを増やしても、チェックポイントと別のチェックポイントの間では、情報漏えいの危険性の問題が常に起こる可能性がある。

そこで、電子文書そのものが「自分の身を自分で守る」モデルとして生まれたのが、コンテンツセキュリティである。情報漏えいする単位は、顧客名簿を納めた文書のようなファイルそのものであるから、文書を単位にセキュリティの管理を行うのは自然な考えである。

このように、情報セキュリティモデルの変遷をみると、その保護をする対象の単位が、企業の情報システム全体から、個々のハードウェア

Content Security for Enterprise Document Management
Tsutomu Ashio, Hisashi Sakamoto, Kaori Kobayashi, Yoshinobu Inagaki, Koichi Kitamura, Yuji Sasaka, Hideo Shimazu
NEC System Technologies Ltd.

機器へ、そして、そのなかに格納される文書ファイルへ、と徐々に小さな単位へ移行してきていることがわかる。

3．DRMに基づくアーキテクチャ

コンテンツセキュリティの土台になるのはデジタル権利管理(Digital Rights Management: DRM)[1][2]である。DRMはもともと、映像コンテンツや音楽コンテンツなどの有料コンテンツを小額課金で取引きする仕組みとして普及が始まったものだが、これを文書管理の基盤として導入することで、企業の新しい情報セキュリティモデルとして有効となることが期待される。

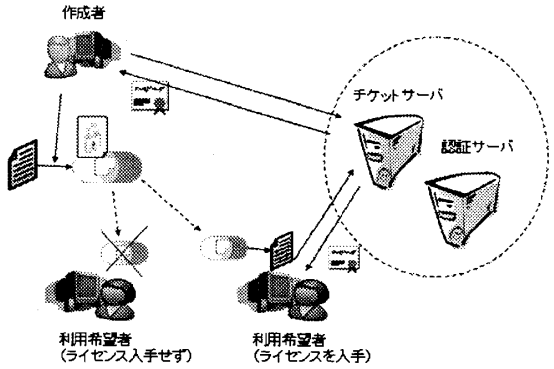

図2　DRMの仕組み

DRMの仕組みを図2に示す。DRMでは、新たな文書が生成されると、まず、作成者が、その利用方法や流通権限などのアクセス権情報を定義したライセンスの登録をDRMのサーバに対して申請して、そのライセンスと文書本体を対にして暗号化する。これをカプセル化と呼ぶ。例えば、「編集権限はプロジェクト構成員のみ可能、社内の人は参照可能、カプセル解除は作成者本人のみ可能、その他の人はアクセス不可能にする。また、アクセス有効期間は今日から1ヶ月間」などのように文書のアクセス権を定義する。ひとたびカプセル化されると、その流通は自由に行われる。カプセル化された文書の利用希望者は、DRMサーバに対して、その利用ライセンス取得を申請する。DRMサーバが許可をすると、利用可能回数、複製可否などの種々の流通に関する属性と制限が記載されたライセンスチケットが利用希望者に渡されるので、その制限の下で利用することができる。ライセンスチケットを不正に複製して利用することはできない。ライセンスチケットの流通を許可せず、利用のたびにDRMサーバへ利用許可を申請させる実現方式もある。このように、文書をDRMで管理することで、情報漏えいしても、漏えい先でDRMサーバへ認証許可を得るか、ライセンスチケットを入手しない限り、文書が解読される心配はなくなる。

企業で運用する場合は、アクセス権の組織的な定義と運用が重要である。アクセス権には、文書が所属する組織やプロジェクトとその構成員によるアクセス権限の種類が規定される。具体的には、組織やプロジェクトの構成メンバーの一覧とそれぞれの人の編集や印刷可否などの操作権限、その組織やプロジェクトで使われるPCや共有ファイルサーバなどのハードウェア機器の一覧、電子文書をどこに置くかの配置管理、などが含まれる。

4．むすび

本稿では、コンテンツセキュリティの必要性とそのアーキテクチャを紹介した。コンテンツセキュリティは、情報漏えいの単位となる文書ごとに管理するセキュリティモデルであり、文書の情報漏えい対策として適している。しかし、コンテンツセキュリティを導入するだけで文書が安全に守られるわけではなく、適切な設定と運用管理をしないと情報漏えいは発生する。コンテンツセキュリティの場合は、文書ファイルのカプセル化の徹底ができるかどうかが鍵になる。組織でそれを徹底するには多くの工夫が必要であり、その1つの提案を坂本他[3]が行っている。

参考文献

[1] Windows Rights Management Services (http://www.microsoft.com/japan/windowsserver2003/)
[2] 森亮一：「ソフトウェア・サービスについて」JECCジャーナル, No.3, pp.16-26 (1983)
[3] 坂本他：「コンテンツセキュリティにおける網羅性の実現」情報処理学会　全国大会, 2008年3月.（準備中）