基盤技術

企業におけるコンテンツセキュリティ

島津 秀雄

要　旨

企業では、膨大な量の電子ドキュメントが作成され、個人のPCやファイルサーバに格納され、流通されており、そこには機密性の高い情報が多数含まれています。それらは、必ずしも十分には管理されておらず、情報漏えいのリスクを増大させています。
本稿では、電子ドキュメントが「自分で自分の身を守る」コンテンツセキュリティのアーキテクチャを紹介します。コンテンツセキュリティの導入により、電子ドキュメントの情報漏えいに対する防衛能力が大幅に向上します。

キーワード
●電子ドキュメント　●情報漏えい　●コンテンツセキュリティ　● Digital Rights Management

1. はじめに

企業では、膨大な量の電子ドキュメントが作成され、個人のPCやファイルサーバに格納され、流通されています。そのなかには、機密性の高い情報が多数含まれています。たとえば、未発表製品の価格表が記載された表計算ソフトのデータファイル、人事情報などが記載されたワープロファイル、公表前の広報用プレゼンテーションファイル、他社との連携に関する機密情報のやりとりが記述された電子メール、などが含まれます。しかし、それらは必ずしも十分に管理されていないのが実態であり、企業の情報漏えいのリスクを増大させています。

本稿では、電子ドキュメントそのものが「自分で自分の身を守る」コンテンツセキュリティのアーキテクチャを紹介します。コンテンツセキュリティを導入することで、電子ドキュメントの情報漏えいへの防御能力が大きく向上します。

2. 情報セキュリティモデルの変遷

情報セキュリティの進化は、**図1**に示すように3段階に見ることができます。最初に登場したのは、ゾーンセキュリティでした。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ものでした。この仕組みの代表例がファイアウォールです。当時は、デスクトップPCが主流であり、PCの社内外持ち出し/持ち込みは頻繁ではなくこれで十分でした。

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りました。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ました。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全体が要塞化されました。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ます。これらをプラットフォームセキュリティと呼びます。

残念ながら、それらを整備しても情報漏えいの事件や事故はなくなりませんでした。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す。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ます。一部の機器がセキュリティ対策を行っていな

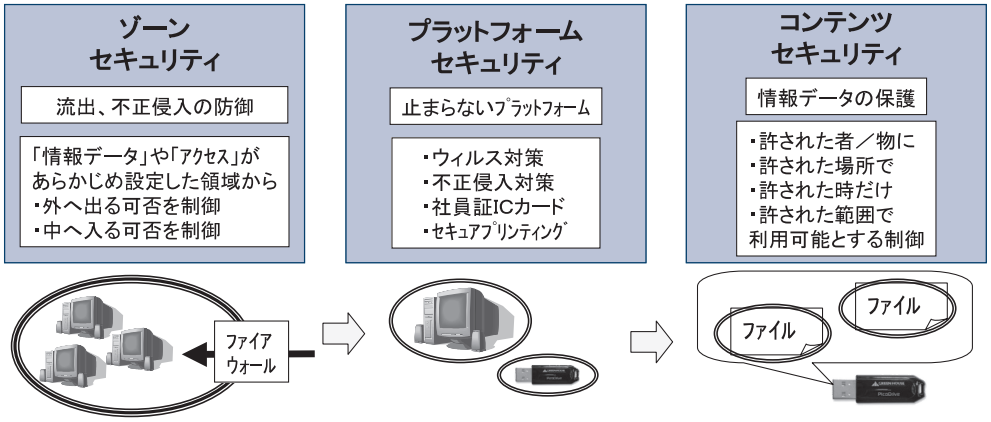

図1　セキュリティの3つの保護領域

いと、そこから情報漏えいが起こります。

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、その分安全になりますが、一方では、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しますし、情報システムの本来のパフォーマンスを低下することにもなります。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ります。そこで、電子ドキュメントそのものが、「自分の身を自分で守る」仕組みを持てばよい、という考え方が出てきました。これに基づく情報セキュリティが、コンテンツセキュリティです。このように、情報セキュリティの変遷をみると、その保護をする対象の単位が、企業内の情報システム、個々のハードウェア機器、そのなかに格納される電子ドキュメント、と徐々に小さな単位へ移行してきていることが分かります。

3. 企業における電子ドキュメントの活用プロセスとセキュリティ面の課題

本章では、企業内の電子ドキュメントの扱いを観察し、セキュリティ面の課題を検討します。

(1) 電子ドキュメントの属性管理

電子ドキュメントは、様々な属性が付与され、それが守られているかを検査される必要があります。誰が、どういう権限で、どういう範囲の操作(参照なのか、編集なのか、印刷可能なのか、複製は可能か等)が許可されるべきか、その有効期限はいつまでか、などです。これらの管理は、人手で遺漏なく管理するのは困難であり、何らかの属性管理と検査の自動化の仕組みが不可欠です。

(2) 電子ドキュメントの所属の管理

社員が電子ドキュメントのファイルを作成すると、作成時点ではその作成者がそのファイルの所有者になります。しかし、それが、その作成者本人ではなく、その人が所属する組織やプロジェクトに関連する電子ドキュメントの場合は、そのファイルは、本来ならば、その組織やプロジェクトに所属するものと扱われるべきですし、組織やプロジェクトで決めた規則でそのファイルの属性も決定されるべきです。たとえば、未発表製品の仕様書であれば、その開発プロジェクト内でのみ流通し、同じ社内でも他の部門には開示できないという場合が相当します。

(3) ファイル形式以外の電子ドキュメントの管理

企業システムのなかで電子ドキュメントのうちファイル以外で重要な形式としては、データベースのレコードと電子メールの本文があります。データベースの場合、データベースからその一部のレコードを取り出して表計算ソフトやテキストファイルへ出力すると、そのファイルにはセキュリティ保護がされないので、情報漏えいの危険性が高くなりますから、そこに電子ドキュメントの情報保護の仕組みが必要になります。

一方、電子メールの場合、機密性の高い情報を本文に記載し、それがメールアドレスの誤記によって無関係の人に送られてしまう場合に情報漏えいが起こります。これを防ぐには、電子メールの本文を一時的に暗号化ファイルとして

取り扱い、保護する仕組みが必要となります。

4. コンテンツセキュリティのアーキテクチャ

第3章で述べたセキュリティ面の課題は、電子ドキュメント自身が「どういう属性を持つか」「どこに所属するか」を知り、「自分の身を自分で守る」仕組みを持たせたコンテンツセキュリティを導入すれば、解決することが可能です。コンテンツセキュリティのアーキテクチャは、コンテンツの権利管理、所属管理、流通管理、の3つの特徴を持っています。

(1) コンテンツの権利管理

土台になるのはデジタル権利管理(Digital Rights Management : DRM)の仕組みです。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り引きする仕組みとして普及が始まったものですが、これを、企業の電子ドキュメントの管理に対しても適用できます。

DRMの仕組みを図2に示します。DRMでは、新たな電子ドキュメントが生成されると、まず、作成者が、その利用方法や流通権限などの属性情報を規定したライセンスの登録をDRMのサーバに対して申請します。その時、電子ドキュメントに対しても属性情報を付与して暗号化を行います。これをカプセル化と呼びます。ひとたびカプセル化されると、その流通は自由に行われます。暗号化された電子ドキュメントの利用希望者は、DRMサーバに対して、その利用ライセンス取得を申請します。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ます。ライセンスチケットは、勝手に複製して不正に電子ドキュメントを利用することはできない仕組みになっています。また、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場合もあります。

電子ドキュメントを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、カプセル化されたファイルの内容が解読される心配はなくなります。

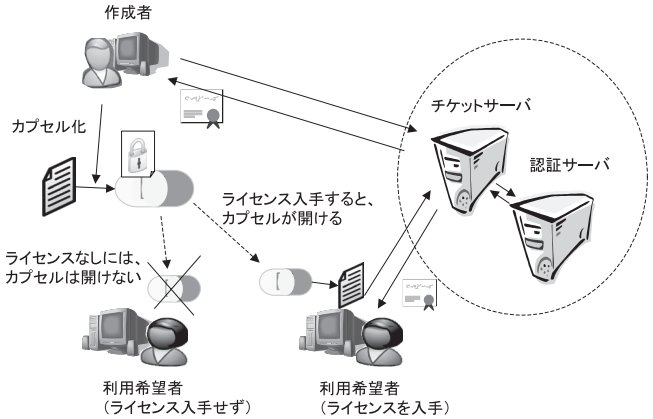

図2　DRM(Digital Rights Management)の概念

(2) コンテンツの所属管理

電子ドキュメントは、それが所属する組織やプロジェクトが規定され、各種の属性を付与されます。属性項目としては、1) 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、2) 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、3) 電子ドキュメントをどこに置くかの配置管理、などがあります。これらの機能は、機密性の高い電子ドキュメントを遺漏なくDRMで管理するために必須な機能群です。

(3) コンテンツの流通管理

DRMによって電子ドキュメントをカプセル化して管理した場合、それがどのように流通されようと、正当な権利を持つ人以外は、その電子ドキュメントのカプセルを通常のファイルに復号化することはできないので、同じDRMのインフラストラクチャ上では、流通管理は一切不要です。しかし、同一のDRMインフラストラクチャ以外の人との電子ドキュメントの授受になると、DRMの利用は不便になります。このような場合、電子ドキュメントの格納されたカプセル化ファイルを一時的に通常のファイルに逆変換してセキュリティ保護をはずして、次に送付先で利用可能な別のセキュリティ手段に置換して配布することになります。流通管理が便利かどうかで、DRMによる企業間の電子ドキュメント流通の普及が左右されるともいえます。

5. コンテンツセキュリティの具体例

本章では、コンテンツセキュリティについて、実際の具体例を使ってその機能を説明します。コンテンツの権利管理については、マイクロソフト社のWindows Rights Management Services (RMS)を例にして説明します。コンテンツの所属管理については、NECのInfoCageのFileシリーズを例にして説明

します。

(1) RMSによる権利管理

RMSは、Windows上で稼動するDMR基盤です。RMSには、ライセンス管理用のRMSサーバと、利用者のID管理をするActive Directoryサーバが必要です。マイクロソフト社のMicrosoft Office 2003の電子ドキュメントについては、アプリケーションのなかで、RMSサーバと直接連携する機構が組み込まれているので、作成者が、アプリケーションのなかで、編集中のデータファイルをカプセル化することが可能です。一方、利用者がアプリケーションのなかで、RMSで暗号化されたファイルを読み込むと、アプリケーションが直接RMSサーバと交信して、読み込まれたカプセル化ファイルの利用許可を確認し、承認されたら作業を開始できる仕組みになっているので利用者はRMSで暗号化することをほとんど意識せずに利用できます。

(2) InfoCage Fileシリーズによる所属管理

InfoCage Fileシリーズでは、どのような形式のファイルでもカプセル化が可能ですが、RMSとMicrosoft Office 2003の関係のように、アプリケーションの内部でDRMサーバと直接連携する仕組みはありません。

InfoCage Fileシリーズの特徴には、自動巡回機能とポリシに基づく集中管理機能があります。RMSでは、個々のファイルの暗号化は、作成者に任されます。作成者が忘れずに重要なファイルをカプセル化すればよいですが、つい忘れてしまう場合もあります。その点、InfoCage Fileシリーズでは、**図3**に示すように特定のフォルダを指定しておくと、そのフォルダを定期的に巡回するエージェントプログラムが調べて、カプセル化されていないファイルを自動的にカプセル化するので、作成者がカプセル化を忘れた時の情報漏えいの危険度が低くなります。たとえば、データベースの一部を表計算ソフトに読み込んで表計算ソフトのデータファイルとして保存する場合に、このファイルを、自動巡回をするフォルダ上に作成しておけば、定期的な巡回時に、自動的にカプセル化してくれることになります。また、特定の組織やプロジェクト単位に、自動巡回やファイルカプセル化などの制御規則をポリシとして記載しておくと、そのポリシは自動的にメンバーに配布されるので、組織内の制御の統一的管理が容易に実現されます。

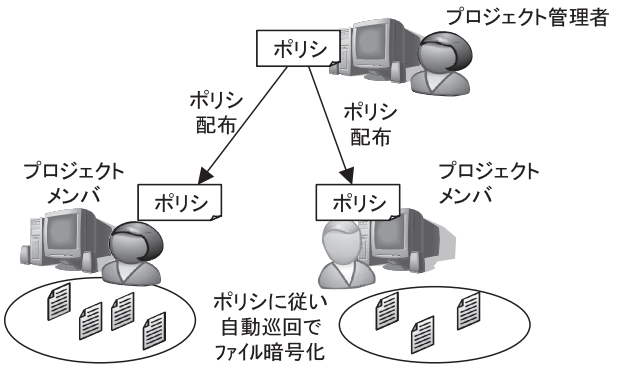

図3　InfoCage Fileシリーズ

6. むすび – 今後の発展 –

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ました。コンテンツセキュリティの考え方は、今後の情報漏えい対策として重要ですが、現在市場に出ている製品群は、コンテンツセキュリティに求められる機能のすべてを網羅しているとはいえません。コンテンツセキュリティを考える上で考慮すべき以下に述べるような検討事項も残されています。たとえば、異なる認証システムやDRMを使用している異なる企業間での電子ドキュメントの流通方法は今後の課題の1つです。これらの検討課題を含め、コンテンツセキュリティを実現する製品の今後の出現が期待されます。

執筆者プロフィール

島津 秀雄
NECシステムテクノロジー
システムテクノロジーラボラトリ
所長