3A-6

情報漏洩防止ソリューション(3)
- ファイル暗号化 -

中嶋　春光[†]　　今井　功[†]　　宮崎　一哉[†]　　近藤　誠一[†]　　遠藤　淳[‡]

[†]三菱電機株式会社　　[‡]三菱電機インフォメーションシステムズ株式会社

1.　はじめに

近年、企業等において、情報のデジタル化が進み、利便性が向上する一方で、本来、機密保持すべき技術情報や顧客情報等、内部情報の漏洩が問題視されている。

我々は、このような内部情報の漏洩防止を目的に、ユーザ認証、アクセス制御、ファイル暗号化などの情報セキュリティと、入退室管理システムなどの物理セキュリティを統合したトータルソリューション[1]を開発した。

本稿では、本ソリューションにおいて、人事情報に連動する役割ベースのアクセス制御に基づいて、内部情報の漏洩を防止するファイル暗号化技術について説明する。

2.　ファイル暗号化

一般に、企業等で、複数の組織やユーザによって共有される内部情報は、イントラネット上のファイルサーバや Web サーバで管理される。このとき、この内部情報は、システム外部からの不正アクセスや、システム内部のユーザによる故意または過失によって外部流出してしまう危険を抱え持っている。また、その流出する内部情報の形態として、電子化されたファイルの形で流出してしまう場合だけでなく、印刷された紙の形で流出してしまう場合もある。

このような危険に対して、内部情報を管理するシステムでは、それぞれの内部情報に適切なアクセス制御情報を設定し、そのアクセス制御情報に従って、内部情報を保護することが要求される。さらに、システムを利用する組織やユーザが多い大規模システムの場合には、運用管理の効率化のため、このアクセス制御情報を、人事情報に連動した役割ベースで管理することが要求される。

本ソリューションでは、これらの要求を満足するよう、人事情報に連動した役割ベースのアクセス制御情報に基づいて内部情報を保護する 2 つのコンポーネントを開発した。

1 つが、サーバで管理する共有ファイルを暗号化することで、内部情報を保護する「ファイル暗号化システム」であり、もう 1 つが、Web コンテンツを対象に、ユーザによる印刷の可否等、その利用権を制御することで内部情報を保護する「コンテンツ不正流出防止システム」である。

以下、それぞれのコンポーネントにおいて、統合管理サーバが管理するアクセス制御情報に基づいて、内部情報の漏洩を防止するファイル暗号化技術について説明する。

2.1.　ファイル暗号化システム

ファイル暗号化システム（図 1）では、複数の組織やユーザによって共有され、かつ、編集され得る共有ファイルを暗号化することによって、内部情報の漏洩防止を実現する。

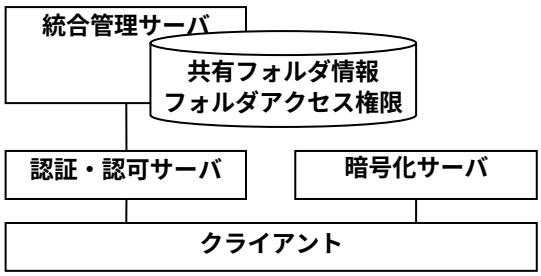

図 1 ファイル暗号化システム

暗号化サーバは、共有フォルダ（Windows 共有フォルダ）単位で暗号化ファイルを管理する。このとき、統合管理サーバは、暗号化サーバの共有フォルダ情報と、そのフォルダに対するアクセス権限を管理する。

クライアントは、Windows ログイン時、認証・認可サーバにログインし、ユーザにアクセス権限が与えられている共有フォルダのリストと、フォルダ固有の鍵情報を、認証・認可サーバを介して、統合管理サーバから取得する。

クライアントにおいて、ユーザがこの共有ファイルにアクセスすると、暗号化・復号機能を実装したファイルフィルタドライバ（暗号フィルタ）が、ファイル書き込み時、フォルダ固有の鍵でデータを暗号化し、ファイル読み込み時、同鍵で暗号化データを復号する（図 2）。

Information Leak Prevention Solution (3) – File Encrypted –
Harumitsu Nakajima[†], Isao Imai[†], Kazuya Miyazaki[†],
Seiichi Kondo[†] and Jun Endo[‡]
[†]Mitsubishi Electric Corporation
[‡]Mitsubishi Electric Information Systems Corporation

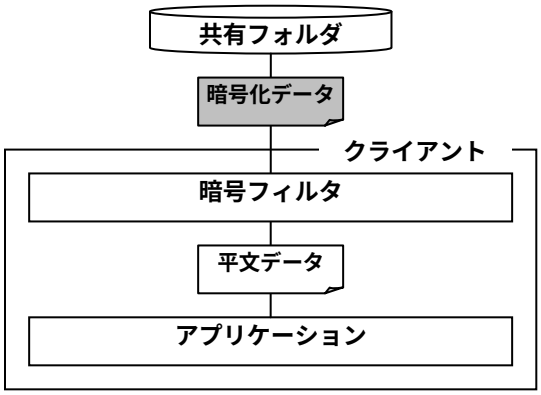

図 2 共有ファイルの暗号化・復号

本ステムでは、保護すべき共有ファイルを常に暗号化することによって、仮に、システム外部からの不正アクセス等により、ファイル自身が外部に流出した場合でも、その情報漏洩を防止する。

2.2. コンテンツ不正流出防止システム

コンテンツ不正流出防止システム（図 3）は、Web コンテンツ（HTML ファイルや画像ファイル）を対象に、ユーザによるコンテンツの使用を制限する利用権（保存可否／印刷可否／コピー可否／画面キャプチャ可否）を管理し、かつ、その利用権に従ってコンテンツの使用を制御することで、内部情報の漏洩防止を実現する。

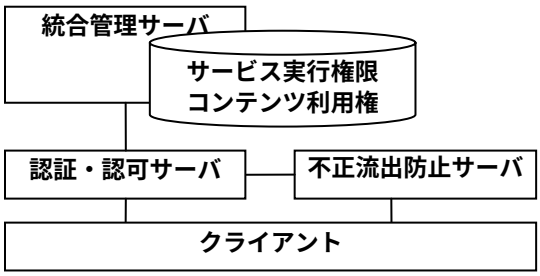

図 3 不正流出防止システム

本システムにおいて、不正流出防止サーバは、特定のユーザ以外の第三者が閲覧できないよう暗号化したコンテンツと、その利用権を一体化（カプセル化）したカプセルファイル[2]を管理し、このカプセルファイルを登録／発行／削除／参照するサービスをクライアントに提供する。また、このとき、統合管理サーバは、これらのサービスに対する実行権限と、ユーザによるコンテンツの使用を制限する利用権を管理する。

不正流出防止サーバは、サービスの実行要求をクライアントから受け付けると、そのユーザに与えられているサービスの実行権限を認証・認可サーバに問い合わせ、その実行権限が与えられていない場合、サービスの実行をキャンセルする。

また、カプセルファイルの発行時には、コンテンツの利用権を認証・認可サーバに問い合わせ、この利用権を格納したカプセルファイルをクライアントに発行する。

クライアントは、Explorer ライクなフォルダビューアで、サービスの実行を不正流出防止サーバに要求し、カプセルファイルを登録、発行等する。また、カプセルファイルに格納されているコンテンツは、Web ブラウザ（IE）で閲覧する。このとき、Web ブラウザにインストールしたプラグイン（IE プラグイン）が、そのプログラム内部で暗号化コンテンツを復号し、かつ、その利用権に従って Web ブラウザを制御する（図 4）。

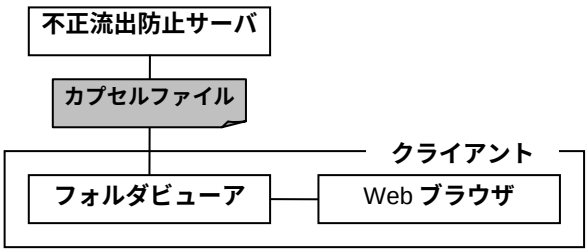

図 4 不正流出防止クライアント

不正流出防止サーバにおいて、コンテンツをカプセル化し、クライアントにおいて、プラグインがその内部で暗号化コンテンツを復号し、かつ、利用権に従って Web ブラウザを制御することで、その情報漏洩を防止する。

3. まとめ

本稿では、本ソリューションが提供する 2 つのコンポーネント「ファイル暗号化システム」、「コンテンツ不正流出防止システム」において、統合管理サーバが管理する、人事情報に連動した役割ベースのアクセス制御情報に基づいて、内部情報の漏洩防止を実現するファイル暗号化技術について説明した。

今後は、不正流出防止システムにおいて、プラグインの機能強化、利用権に基づくデバイス制御の実装により、より強固な情報漏洩防止を実現するとともに、他プラットフォームへの適用についても検討していきたいと考える。

[参考文献]

[1] 二井ほか、「三菱情報漏洩防止ソリューション」三菱電機技報 Vol.78 No.4（2004）
[2] 中嶋ほか、「セキュアコンテンツ制御ライブラリの開発」CSEC 研究報告 Vol.2000 No.030（2000）