異なる組織間でのセキュア文書流通アーキテクチャ

西村　知也†　　島津　秀雄‡
NECシステムテクノロジー株式会社†‡

1．はじめに

本稿では、コンテンツセキュリティにおいて、異なる組織をまたがってビジネス文書をセキュアに流通させるアーキテクチャについて述べる。これまで多くの対策が講じられながらいまだに続く情報漏洩問題を根本的に解決する方法として、デジタル権利管理(Digital Rights Management, DRM)[1]を使い、文書ファイル単位にそのファイルへのアクセス権リストとともに暗号化して管理する（カプセル化）コンテンツセキュリティの手法がある[2][3]。筆者らは、総務省でＨ１９年度から開始された「情報の来歴管理等の高度化・容易化に関する研究開発」の一環として、従来のコンテンツセキュリティモデルに比べて来歴管理能力を向上させた権限委譲型モデルを昨年度提案した[4]。このモデルは、文書の「作成者」と「所有者」を分離し、文書の権限管理をより厳密に行うことが特徴である。ただ、Ｈ１９年度の成果は、イントラネットに代表されるような同一の認証システムの環境下のみで実現されるモデルであり、異なる組織間での文書流通には利用できないという問題があった。今年度は、同モデルを発展させ、異なる組織をまたがってセキュアに文書を流通させるアーキテクチャに発展させたので、その詳細を報告する。

2．権限委譲型モデル

権限委譲型モデルでは、組織に属するある人（作成者）が文書を作成しアクセス権を定義すると、その時点で文書の所有権がその組織に譲渡される。つまり、元の作成者は、その文書の作成者であるという記録は保持されるが、その文書のアクセス権（編集権、参照権、印刷権、カプセル解除権など）の制御（誰に付与するか）は、については所属する組織に一切譲渡することになる。従って、元の作成者は、カプセル解除権を持たなければ、自分で勝手にカプセルを解除することはできなくなる。図１に権限委譲型モデルの動作例を示す。ここでは、被譲渡者である組織は、エージェントとして表現されている。このモデルでは、エージェントのみが、ＤＲＭサーバへ直接指示（カプセル化、カプセル解除、アクセス権変更等）するので、コンテンツセキュリティの操作に関する一元管理が可能になり、その結果、来歴管理が厳密に行なえることになる。

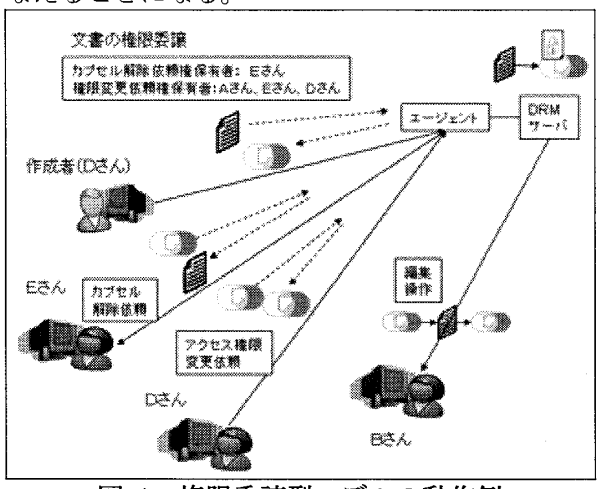

図１　権限委譲型モデルの動作例

3．組織をまたがる文書流通への適用での問題

異組織間での連携プロジェクトを遂行する時に、一社で権限委譲型モデルを採用していても、他の組織では採用していない場合、他組織に文書を流通させる時にはカプセルを解除しなくてはならないが、これでは情報漏洩の可能性を高めてしまう。もちろん、他組織でも権限委譲型モデルを導入してくれれば首尾一貫した管理は可能になるが、独立した別組織に対して情報システムの置換を依頼（命令）するのは現実的ではない。そうなると、従来の権限委譲型モデルを異組織間での運用には使えないという問題になる。

4．異組織での文書流通向け権限委譲型モデル

この問題を解決するために、本稿の提案では、異なる組織が共通してアクセスできる環境に権

The secure document distribution architecture among the different organizations
†Tomonari Nishimura, ‡Hideo Shimazu
NEC System Technologies ,Ltd

限委譲型システムを構築し、新たに「外部送信依頼権」という概念を導入した。これにより、異組織間でもカプセル化したままで文書が流通でき、かつ組織を超えての文書の来歴情報を一元管理することが可能になった。

「外部送信依頼権」とは、従来の権限委譲型モデルに基づいてカプセル化された文書単位に1人以上の利用者に対して付与される権利であり、これを付与された利用者は、その文書を異組織に流通させることができる。具体的には「出稿」「入稿」の２つの操作で構成される。出稿操作とは、文書を異なる組織の特定の人に流通させる為にカプセルに特殊処理をしてもらうことである。一方、入稿操作は、異なる組織の人から戻された文書ファイルの（特殊操作された）カプセルを通常のカプセルに戻すことである。

５．外部送信依頼権とその動作

図２に自組織Ａ社の利用者Ｘが文書を出稿させ、他組織Ｂ社の利用者Ｙが受領してそれに編集を加えたものを再度利用者Ｘに戻す例を使って説明する。ここで、Ａ社は権限委譲型システムを運用しておりそのための DRM サーバを有している。一方、Ｂ社は特段のセキュリティシステムを運用していない。また、流通制御サーバとは、Ａ社、Ｂ社あるいは第３者からもアクセス可能なインターネット空間上に設置され、内部でＡ社とは別の DRM サーバと権限委譲型システムが稼動している。

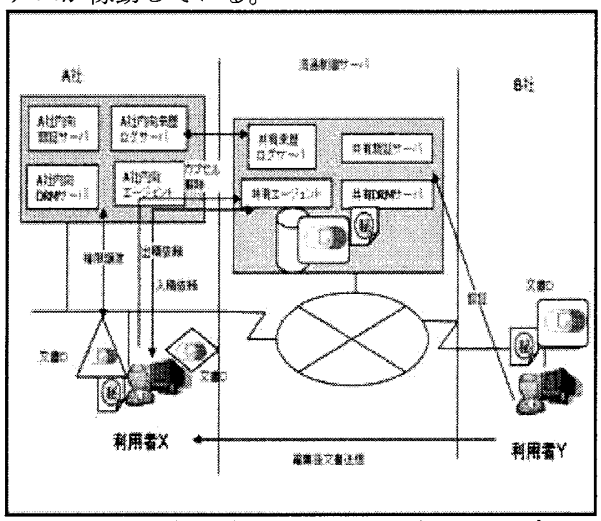

図 2　異組織間流通向けに発展させたモデル

利用者Ｘが文書Ｄを作成すると、それをＡ社内向けに権限譲渡をするが、その時に、利用者Ｙに限定して操作を許可すべく「外部送信依頼権」を自分自身に与えるように指定しておく。利用者Ｘが利用者Ｙに文書Ｄ（カプセル化済み）を流通させるときには、利用者ＸからＡ社のエージェントに対して出稿依頼を発行する。Ａ社エージェントは、文書Ｄのカプセルを解除して流通制御サーバに渡す。流通制御サーバは、自身の DRM サーバに再カプセル化を指示する。利用者Ｙは、この再カプセル化された文書Ｄを入手して編集を行なう。このとき、利用者Ｙの認証は流通制御サーバが行なう。利用者Ｙが編集処理を終えて利用者Ｘに返信するときは、メール等の手段で直接利用者Ｘに返信する。利用者Ｘは、受領した文書Ｄはそのままでは解読できないので、カプセルの再度の付替えを依頼する（入稿操作）。この処理はＡ社エージェントと流通制御サーバの間で協調して行なわれる。

なお、来歴情報については、Ａ社エージェントの記録情報と流通制御サーバ上の記録情報で一貫した管理ができるようになっており、出稿から入稿までのすべての記録が来歴として管理される。

５．まとめ

本稿では、権限委譲型のコンテンツセキュリティモデルで、異なる組織間での文書流通を実現するアーキテクチャと実現方法について述べた。このモデルでは、複数の組織で連携プロジェクトを組む場合、中核組織のみが本モデルで運営されていれば、それ以外の組織には前提とする情報システムの運用が不要であり、現実的なシステム運営が可能である。本研究は、総務省の「情報の来歴管理等の高度化・容易化に関する研究開発」の一環で行なわれたものである。

参考文献

[1] 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)
[2] 足尾他 ：「企業におけるコンテンツセキュリティ」情報処理学会第 70 回全国大会, No. 1, (2008)
[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」情報処理学会第 70 回全国大会, No. 1, (2008)
[4] 西村他 ：「権限委譲型のコンテンツセキュリティ」情報処理学会第 70 回全国大会, No.1 (2008)