権限移譲型のコンテンツセキュリティ

西村知也[i]　島津秀雄[ii]　足尾勉[iii]　アヌラグ・グプタ[iv]
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

本稿では、権限移譲型のコンテンツセキュリティのアーキテクチャと実現方法について述べる。今日では情報漏えい対策として、電子文書をデジタル権利管理(Digital Rights Management, DRM)基盤を使ってカプセル化して管理する方法が注目され商用化されている[1]。DRMは、電子文書本体とそのアクセス権を分離して管理する超流通モデル[2]を基本にしている。DRMでは、電子文書作成者が、その文書に対して誰がどのような操作を可能にするかを定義したアクセス権リストを記述し、それを文書と同梱して暗号化（これをカプセル化と呼ぶ）する。個々の電子文書作成者がDRMを使いカプセル化していけば情報漏えいの発生は激減するはずであるが、実際には、カプセル化を忘れたり、一度カプセル化した文書を再びカプセル解除したりする可能性があるため、どの文書がどれだけカプセル化されているか、あるいは誰から誰へ流通しているかなどの来歴情報を把握できない点が問題だった。また、企業では特許を作成すると、所属する企業にその権利一切を譲渡する手続きを経てから、企業から出願する業務形態が一般的になりつつある。この場合、特許の「作成者」と「所有者」が切り離されている。企業内の電子文書も、作成する人は個々の社員であるが、その所有権は、社員の所属する組織やプロジェクトに帰属するにもかかわらず、電子文書の作成者と所有者を分離して管理するモデルがこれまで存在しなかった。

そこで、筆者らは、電子文書の作成者と所有者を分離したモデルである権限委譲型モデルを考案しDRM上に実現した。本モデルの採用により、コンテンツセキュリティの情報漏えい対策が、より堅固になることが期待できる。

２．権限移譲型モデル

本モデルでは、図１のように、電子文書は、本体とアクセス権と権限移譲型モデル特有の属性（作成者属性、所有者属性、カプセル解除依頼権保有者属性、権限変更依頼権保有者属性）とから構成される。

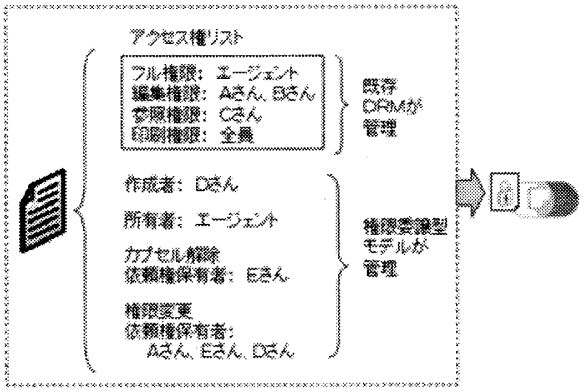

図１：権限委譲型モデルのデータ構造

アクセス権リストには、電子文書の操作を許可する利用者とその権限範囲が定義されDRMが管理する。図１では、フル権限、編集権限、参照権限、印刷権限、が用意されているが、DRMの種類によってそれぞれ異なる。

権限委譲型モデル特有の諸属性には、電子文書本体ではなく、アクセス権リストへの操作を許可する利用者とその権限範囲が定義される。「作成者」属性には、電子文書を新規に作成した人が登録される。「所有者」属性には、作成者がその一切の権利を譲渡する相手が登録される。所有者は、文書のアクセス権変更とカプセル解除を行なえる。「カプセル解除依頼権保有者」属性には、文書のカプセル解除を所有者に依頼する権利を持つ人が登録される。「権限変更依頼権保有者」属性には、アクセス権変更を依頼する権利を持つ人が登録される。なお、所有者は、計算機エージェントが行ない、個々の利用者の端末からアクセス可能なサーバ上に配置される。

図２に権限委譲型モデルの動作の例を示す。ある人（図２ではDさん）が文書を作成し、エージェントに送信し所有権を譲渡する。その時、カプセル解除依頼権保有者(E)と権限変更依頼

Ownership Transfer-based Content Security,
[i] Tomonari Nishimura, [ii] Hideo Shimazu,
[iii] Tutomu Ashio, [iv] Anurag Guputa,
NEC System Technologies, Ltd.

権保有者（A、E、D）の名前一覧も同封する。エージェントは、自分が所有者になり、カプセル解除依頼権保有者と権限変更依頼権保有者をアクセス権リストに加えた後、DRM サーバに文書をカプセル化することを指示して生成されたカプセルを作成者に返す。

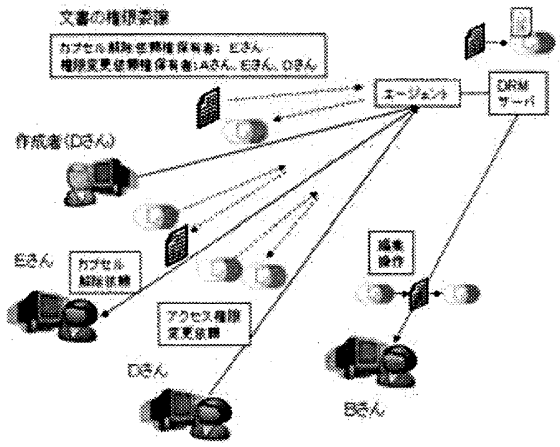

図２：権限委譲型モデルの動作

その後は、そのカプセル化された文書が社内で流通されていく。運用中に、アクセス権リストの変更（例：新規の利用者追加）が必要な時は、権限変更依頼権保有者を通じてエージェントに権限変更の依頼をだしてもらうとエージェントが代行処理をする。同様に、カプセル化解除の場合は、カプセル解除依頼権保有者を通じて行なう。なお、文書の直接操作（編集や参照）の時は、エージェントを介さずに DRM サーバが直接認証を行なう。

３．来歴情報の集中管理

権限委譲型モデルでは、エージェントに渡される権限委譲、アクセス権変更、カプセル解除の依頼情報を来歴情報として集中して収集できるメリットがある。従来の DRM では来歴情報の集中管理は不可能であった。その理由は、電子文書作成者が、自分の権限として、文書のカプセル化、カプセル解除、アクセス権限リストの追加削除を行っていたため、それらの操作の記録を収集しても、せいぜい作成者単位に局所的に保存されるだけであった。その結果、DRM で文書をカプセル化管理しても、それを監視する手段がなかった。

図 3 は来歴情報を収集・分析する画面である。来歴情報としては、誰から誰へどういう権限が付与されたかが記録されている。これにより、個々の電子文書に対して、任意の時間で、どういうアクセス権を存在するかを調べることができる。また、情報漏えいの大きな原因になりかねないカプセル解除の操作をエージェントに対して誰がいつ依頼したかも記録されるため、ある重要な電子文書が情報漏えいした時に、来歴情報のログから、故意または不注意の容疑者を絞り込むことができる。

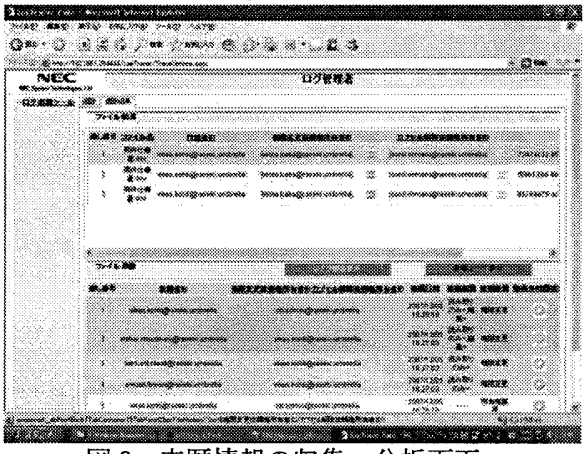

図３：来歴情報の収集・分析画面

４．まとめ

本稿では、権限移譲型のコンテンツセキュリティのアーキテクチャと実現方法について述べた。まず、モデルの必要性を説明し、概要を説明した。次に、本モデルによってカプセルに関連する来歴が集中管理できるメリットを説明した。本モデルの採用により、DRM を基盤としたコンテンツセキュリティの情報漏えい対策が、より堅固になることが期待できる。

なお、本研究は、総務省の H19 年度「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] 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)