電子文書の保護流通と来歴の管理

西村　知也†　　島津　秀雄‡

NECシステムテクノロジー株式会社　　システムテクノロジーラボラトリ†‡

1．はじめに

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一昨年度提案した[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。昨年度は、権限委譲型モデルを拡張発展させ異なる組織間でカプセル化ファイルをスムーズに流通できるように拡張させた[5]。今年度は、文書ファイルが、故意または不注意によって、インタネットに流出した場合に、短期間に流出した文書ファイルを見つけるための方法とその探索した文書ファイルから流出経路を推定する方法の検討および評価を行なった。

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、解除権など）の制御（誰に付与するか）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いし、また変更依頼権を持たなければ新たに権限の付与をすることも出来なくなる。図1に権限委譲型モデルの動作例を示す。

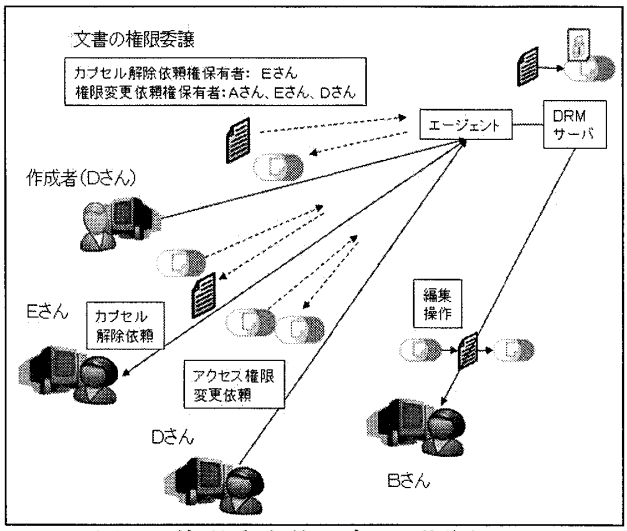

図1　権限委譲型モデルの動作例

3．文書ファイルの流出時の問題点について

文書ファイルがインタネットに流出した場合の問題点を下記に記す。

(1)　文書が開かれ中身を見られることで機密情報や個人情報が漏洩する。(2)　文書が流出してから発見されるまでに時間がかかるため、流出元から多量の情報が漏洩する。(3)　文書の流出元の調査に時間と経費がかかる。(4)　漏洩した情報に対する対応に費用と時間がかかるとともに信頼回復に多大な年月が必要である。

上記問題点のうち、(1)と(4)については、文書ファイルをカプセル化することで文書の中身そのものが保護されるためすでに解決している。そこで今回我々が解決すべき問題点を(2)と(3)に絞り検討を行った。

4．情報の探索・追跡方式についての検討

前記問題点の(2)と(3)を解決するには、流出の早期発見が必要である。そこで文書ファイルに、誰から誰へ、どこからどこへ流通したかという文書ファイルの来歴情報のログ情報の一部を持たせることにした。これにより、流出した文書を探索する場合の鍵とすることができるようになる。ログ情報の肥大化を防ぐため、(a)権限依頼時の情報や版管理番号、(b)文書ファイル

Tracing and monitoring information leakage
†Nishimura Tomonari, NEC System Technologies, Ltd.
‡Shimazu Hideo, NEC System Technologies, Ltd.

自身の最終操作を行った利用者の情報(端末を特定できるネットワークアドレスなど)などの限定した情報のみをカプセル内に記録させる設計にした。これらの情報をキーにして、管理サーバが持つ情報を照合させることで、より詳細な来歴情報を再現できることになる。

５．探索・収集・蓄積の実装モデル

次に、インタネットに流出したカプセル化された文書ファイルを探索し発見するエージェントの設計を行った。これは、特殊な検索エンジンのクローラを設計することに相当する。設計方針としては、ネットワーク上を探索して文書ファイルを収集するための各種プロトコル(http, https, samba, SharePoint など)で構築されたサーバをクローリングしながら探索する検索エンジン(例えば Google-アプライアンスなど)と、(ア)探索サーバが収集した情報(URL やテキスト情報など)に対して、対象ファイルの拡張子を鍵に検索を行い、得られた検索結果の URL を元に実際に文書ファイルを収集する収集部と(イ)蓄積する対象の文書ファイルであるかの解析を行い、それが探索の対象となるカプセル化された文書ファイルであれば、カプセル内に記録された情報の抽出を行う解析・蓄積部と(ウ)蓄積された情報を検索表示する検索・表示部の３つで構成される実装モデルを検討設計した。ここでの特徴は、対象ファイルがカプセル化されているので、ファイルのカプセルの暗号解除を行なうことなしに埋め込んだ来歴情報を外部から読み出すことができる仕掛けを設けた点である。図２は、その実装モデルを示している。

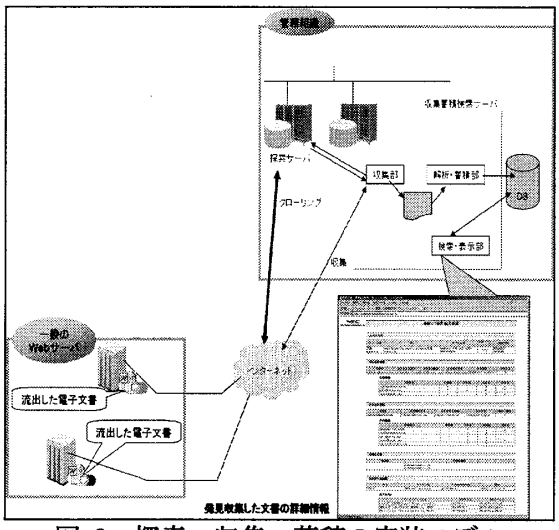

図 2　探索・収集・蓄積の実装モデル

６．実験評価

本実装モデルを元に実験システムを構築して、評価実験を行った。評価環境としては、１２台のサーバ上に各プロトコルで文書ファイル７０個（うち５０個が対象文書）を公開し探索から収集蓄積完了までの時間を計測（１０回計測）しそれぞれの処理時間とした。

評価実験の結果は、各モジュールでの平均的な計測値は、(1)探索エンジン（約４０分）(2)収集部（約１０分）(3)解析・蓄積部（約１０分）であった。

通常インタネットを探索する検索エンジンは、１日１回～２回程度で同一のサイトを巡回して情報収集しており、収集部から解析蓄積をそのサイクルより短く動作させることで、探索結果を効率良く利用して、流出してから半日から１日程度で、文書ファイルの流出を発見することが可能になると思われる。

７．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を基盤とした文書ファイルの流出事故への対処方法として、文書ファイル自身に来歴情報を持たせて追跡する方法とその評価結果を説明した。

本稿で提案する仕組の導入により、カプセル化されている文書ファイルの流出事故が発生した場合の流出ファイルと流出経路の早期発見が可能になることを実証できた。

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)
[5] 西村他：「異なる組織間でのセキュア文書流通アーキテクチャ」情報処理学会第 71 回全国大会, No. 3 (2009)