コンテンツセキュリティにおける網羅性の実現

坂本久　足尾勉　小林香織　稲垣嘉信　北村晃一　笹鹿祐司　島津秀雄
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

コンテンツセキュリティは、デジタル権利管理基盤（Digital Rights Management, DRM）[2]を使って電子文書をカプセル化して管理するもので、情報漏えい対策の切り札として注目されている[1]。しかし、コンテンツセキュリティでも「為すべきことを網羅的に行う」ことをしないと情報漏えいが発生する点では他のセキュリティモデルと同じである。コンテンツセキュリティの場合は、カプセル化の徹底が「為すべきこと」だが、組織でその構成員一人ひとりに対して、それを徹底するには工夫が必要である。本稿では、それを極力自動化して網羅的に実行する仕組みについて述べる。

2. カプセル化徹底への課題

カプセル化徹底の課題として以下をあげることができる。

(1) 電子文書に対するアクセス権の設定

１つ１つの文書ごとに対する適切なアクセス権の設定が必要である。例えば、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、などの設定である。しかし、このアクセス権リストの設定を個々の文書に対して作成者自身が行なうことを徹底させるのは困難であり代替手段の提供が課題である。

(2) 電子文書のカプセル化

文書ごとにアクセス権を設定した後には、文書のカプセル化操作を行わなくてはならない。その中には、受信したメールに添付されてきた文書ファイルを利用者の PC に格納する場合のように、利用者が意識しないうちに新しい文書を作成している場合も含まれる。しかし、文書を新規作成するたびに人手で陽にこの操作を行なわせるのは現実的に困難であり、代替手段の開発が課題である。

(3) 電子文書の状況変化への対応

文書は、その所属や秘匿性の程度が、時間に応じて変化する場合が一般的である。例えば、新製品の広報資料は、作成開始時は、作成者本人のみが編集可能であるが、その後、開発部門や広報部門で共有され、更に、社外でも公開可能な情報になる。文書のアクセス権も、この状況変化に対応して、改訂されていくべきであるが、作成者や利用者がこの改訂を文書１つ１つに対して行なっていくのを徹底するのは現実的に困難であり、代替手段の開発が課題である。

3. カプセル化網羅性の実現

筆者らは、これらの課題を解決しコンテンツセキュリティを網羅的に実現する仕組を開発した。以下に、図１を参照しながら解決の施策を説明する。

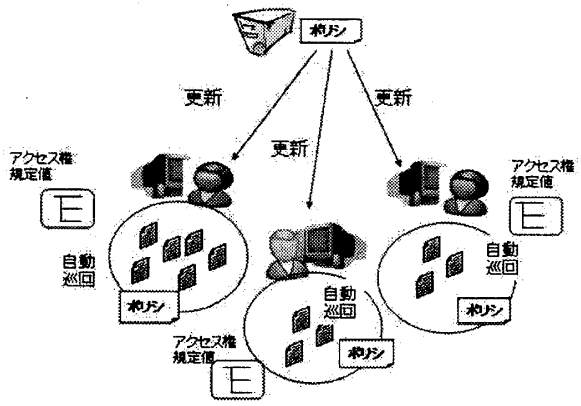

図１：網羅性の為の３つの施策

(1) フォルダ単位のアクセス権管理

同一のプロジェクトや特定業務に関する事柄、のように共通の属性を持つ文書群、あるいは個人用途の文書群、などのように、通常は、かなりの文書は、ある意味を持つカテゴリごとに分類することが可能である。利用者は、通常このカテゴリごとにファイルシステムの階層構造（フォルダ）を使って文書ファイルを配置して整理している。筆者らは、この運用方法に注目

On Robust Operation for Business Content Security
Hisashi Sakamoto, Tsutomu Ashio, Kaori Kobayashi, Yoshinobu Inagaki, Koichi Kitamura, Yuji Sasaka, Hideo Shimazu
NEC System Technologies Ltd.

し、フォルダ単位に文書に対するアクセス権リストの既定値を定義することで、そのフォルダに文書を置くと、自動的にそのフォルダに付与されたアクセス権リストが文書に転写されカプセル化する仕組を用意した。規定値のアクセス権の例としては、「このフォルダ配下の文書のアクセス権は、A プロジェクト構成員のみが編集可能、B 組織構成員は参照可能、他の人は何もできない」などのように定義する。これにより、利用者は、特定のフォルダに対して１度アクセス権の定義を行ない、その後は、従来の文書の整理方法と同様に操作をしていくだけで、文書に適切なアクセス権が自動的に付与されカプセル化が自動的に行なわれることになる。

(2) 自動巡回によるカプセル化

(1)の仕組みでは、利用者が陽にアクセス権を指定したフォルダ配下の文書に対しては自動的にカプセル化がなされるが、利用者が陽にアクセス権を指定していないフォルダに置かれた文書については何もしない。ところが、一般には利用者の PC には数百個から数千個のフォルダが存在するので、利用者にすべてのフォルダに対してアクセス権の既定値を設定させるのは現実的ではない。しかし、そうなると、網羅性の点で不十分であるため、利用者が(1)で陽に指定していないフォルダに対しても、一括して付与する既定のアクセス権を定義する仕組を用意した。いわば規定値の二重化である。このアクセス権の例としては「本人のみ編集可能、他の人は何も出来ない」や「組織の構成員のみ編集可能」などがある。利用者 PC に組み込まれたエージェントソフトウェアがフォルダを定期的に巡回し、陽に指定されていないフォルダに置かれている文書のうち、指定されたファイル型(例：特定の拡張子を持つファイル) で、かつカプセル化されていないものをみつけると、既定のアクセス権を付与してカプセル化することを行なう。なお、その文書が勝手にカプセル化されては困る場合は、エージェントによる巡回の例外指定を行なうことを許容している。

(3) ポリシ配布による一括定義

個々の利用者が自分の PC 内のフォルダに対して、(1)や(2)の機能を使ってアクセス権の既定値定義をすればよいが、実際には、それすらもすべての利用者に対して徹底させるのは容易ではなく、また、人事異動や組織変更のたびにアクセス権の更新を利用者一人ひとりにさせることも望ましくない。そこで、サーバを準備し、サーバ上に既定のアクセス権をポリシとして定義しておき、個々の利用者 PC から、適当なタイミングでポリシをダウンロードして、そのポリシに沿って、個々の利用者 PC のフォルダのアクセス権定義を自動的に行なう仕組を用意した。この仕組みにより、個々の利用者は、PC からサーバに接続するだけで、(1)も(2)も自動的に設定されることになり、組織変更等によるアクセス権の更新にも追従できるようになり、網羅性の点で完全になった。

4. 今後の課題

本稿で説明した網羅性の徹底の為の施策により、イントラネットにおけるコンテンツセキュリティを徹底できた。今後の課題としては、以下の２つがあげられる。

第 1 は、異なる企業間での安全安心な文書の流通である。個々の企業では、それぞれ独立の ID 管理サーバで利用者の ID 管理を行なっており、DRM 基盤も、ID 管理サーバに認証を依頼している。従って、ある企業から別の企業へカプセル化された文書を送付した場合、受け取った別企業の人間がカプセルを解除するには、VPN を通じて送付側の企業の ID 管理サーバに対して認証を依頼するか、ID 管理サーバ同士が認証を連携する仕組が必要である。第 2 は、多様な形式の文書管理である。単独の文書ファイル以外の形式として、Web ページ、データベースレコード、電子メール本文等がある。これらに対しても、コンテンツセキュリティの考え方で管理することは可能であり、筆者らも今後拡張を計画している。

5. まとめ

コンテンツセキュリティを運用する場合の課題と対策について述べた。これらの施策により利用者に依存せず自動的に網羅性が実現できるため、文書の情報漏洩への防衛能力が大きく向上することが期待できる。

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)