1D-7

CyberTrace:機密情報を高精度に保護・監視・追跡する企業内情報漏えい対策アーキテクチャ

†喜田 弘司　†坂本 久　‡高橋 宏幸
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ー　‡サーバソフトウェア事業部

1. はじめに

近年、情報漏えい事件が多発している。平成17 年の総務省発行の情報通信白書によると情報漏えい事件の件数は 4 年前の 4 倍に達している。個人情報保護法の全面施行に伴い企業は様々な対策を講じているが不十分であると言える。我々はファイルを中心とした情報漏えい対策の方法を研究開発している。

企業にとって「情報」は、人・モノ・カネに続く第四の資産である。すなわち、情報漏えい対策とは「企業資産である情報をきちんと管理すること」と定義できる。ところが、情報はコピー、流通、二次利用が非常に簡単であり、人・モノ・カネと同様の方法で管理することは難しい。本稿ではこの課題に対し機密情報の(1)保護と(2)ライフタイムの高精度な監視・追跡というキーコンセプト CyberTrace を提案する。本稿では全体のアーキテクチャを中心に説明する。

2. 情報漏えい事件の分析

情報漏えい事件が頻発する原因を分析すると、以下のようにまとめることができる。

情報システムアーキテクチャの変化：従来は、外部からアクセスできないようにファイアウォールを設置することがセキュリティ対策の基本であった（図１左）。重要な情報ほど内側に設置し限定された出入り口からアクセスすることにより防御する。ところが最近は便利さを求め、企業情報システムと外部との出入り口が多様化している（図１右）。こうなると漏れないように機器を正しく設定することは非常に難しい。実際、機器の設定ミスや、ソフトウェアのバグによる脆弱な部分から事件が起きている。

機器(ｽﾄﾚｰｼﾞ,ﾈｯﾄﾜｰｸなど）の高性能化：最近の機密情報のほとんどはワープロなどの電子機器で作成されメールなど電子的に流通する。こういった電子機器やネットワークの性能は飛躍的に向上しており、機密情報を持ち出すことは非常に容易い。

A Novel Architecture against Information Leakage That Consists of Protecting, Monitoring and Tracing Confidential Document Lifetime.
NEC System Technologies, Ltd.

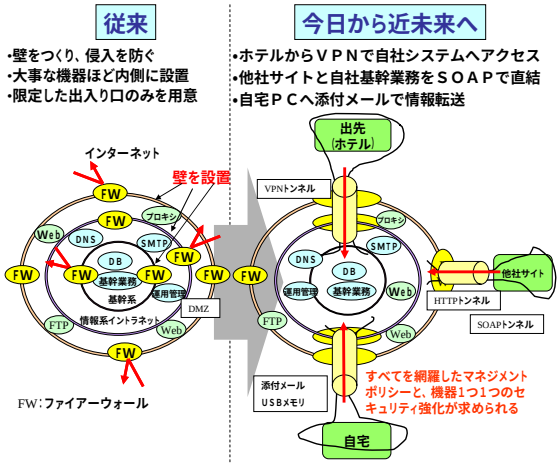

図 1　情報システムアーキテクチャの変化

例えば、2 万人の CSV 形式の顧客情報も数メガバイトのファイルサイズであり USB メモリなどで持ち出すことは簡単である。このように、特殊な技術を必要とせずに持ち出せることが情報漏えいの原因の一つである。

ワークスタイルの変化：軽量なノートＰＣ、無線 LAN など、いわゆるユビキタス環境の普及に伴い、比較的気軽に機密情報を持ち歩き、いつでもどこでも仕事をするワーカが増えている。各ワーカは仕事のモラルの高いワーカであるが、セキュリティ面から考えると非常にモラルの低いワーカである。実際、過去の多くの事件も、外出先での PC の置き忘れなどが原因である。

3. 監視追跡による情報漏えい対策

3.1. 設計方針

上記分析結果をふまえ、我々は情報そのものをきちんと管理することが重要であると考える。従来の対策はファイアウォールやディスクの暗号化など情報を扱う機器の管理に重点が置かれていた。これではワークスタイルの変化に対応できない。今後は、情報そのものの状態を「見える」ようにして管理する時代であると考える。「見える」ための要件をまとめる。

機密情報を定義できること：企業が管理すべき機密情報を登録できる必要がある。

社外と社内の境界を定義できること：情報漏えいとは、社内から社外へ機密の情報がコピーされる

ことである。すなわち、社内と社外の区別を明確に定義できる必要がある。

機密情報の管理状態を確認できること：機密情報のライフタイム、すなわち、生成、編集、配布、二次利用、削除が正確に把握できる必要がある。

3.2. 機密情報のライフタイムモデル

(1)機密情報の状態

「ドラフト状態」：作成中の機密文書であり、機密であることを正式に登録していない状態。

「社内利用状態」：機密であることを正式に登録された文章であり社内利用されている状態。利用方法は参照、更新、コピー、二次利用である。

「通常文章状態」：機密情報であるといったんは登録されたが、機密ではなくなった情報。例えば、プレスリリースなどは発表されるまでは機密であるが、発表後は通常文章として扱えばよい。

「印刷状態」：印刷は紙の媒体へのコピーと考え、機密文書の状態のひとつとする。

「削除状態」：必要がなくなり削除された状態であり、削除され存在しないことに意味がある。

(2)機密情報の関係

社内利用状態のコピーあるいは二次利用された２つの機密文書の間には*「親子関係」*がある。ただし、親子関係はいろいろな操作で発生することに注意が必要である。例えば、アプリケーションから「名前を付けて保存」を実行した場合、保存前の文章と保存後の文章は親子関係になる。また添付メールによる配布は添付元の文章と受取先で展開した文章は親子関係になる。

3.3. 機密情報の監視・追跡モデル

「監視の開始」：ドラフト状態から社内利用状態になった時点を監視のスタートとする

「監視の範囲」：社内利用状態を監視し親子関係と状態の変化をログに残す。例えば削除したこと、印刷したことなどをログに残す。

「追跡」：親子関係をたどり各ファイルの位置から流通経路を追跡できる。図２にログ分析による親子関係をツリー状に表現した追跡結果の画面例を示す。ファイルの流通経路や、二次利用、印刷されていることなどが追跡できる。

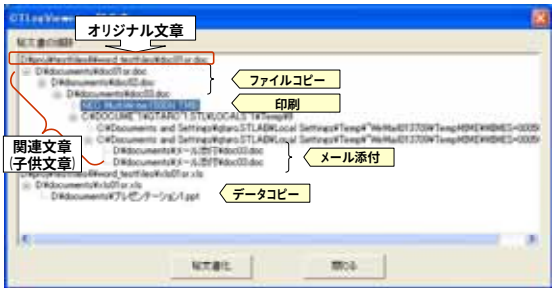

図 2　ログ分析による親子関係の追跡結果

4. CyberTrace 概要

4.1. 特徴

機密情報のライフタイムを追跡するサーバ／クライアント型システムである。機密情報をサーバ上の保護フォルダに格納すると、以後そのライフタイムを隠密にログ記録される。監視の範囲は、監視エージェントが導入されている範囲である。記録する事象はファイルの生成／編集／移動／印刷／複写／親子関係／削除である。

導入の効果として、未許可 PC へのコピー発見や、紛失 PC の機密情報の有無の判別、漏えいした機密情報の足跡から不審性発見（例：競合他社社員へ添付メール）などが期待できる。

4.2. 構成

[クライアント]

「監視エージェント」：クライアントに常駐する監視ソフトウェア。監視エージェントが実行されているＰＣを社内と定義できる。例えば、ノートＰＣを持ち出した場合、監視プロセスが動作していれば、この環境は社内とみなす。

[サーバ]

「保護フォルダ」：機密情報を定義するための共有フォルダ。ワーカはこのフォルダへ情報を登録することでドラフト状態を社内利用状態に変更できる。システムは文章ＩＤを割り振り機密情報として監視対象にする。さらに登録された情報を自動的に暗号化する。

「ログ分析ビューア」：クライアントに常駐する監視エージェントからの監視結果を分析しビューアによりライフタイムを見ることができる。

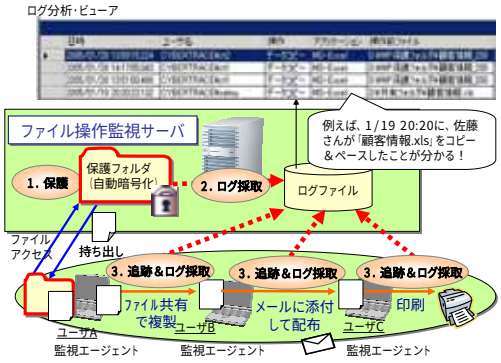

図 3　システム構成図

5. まとめ

機密情報のそのもののライフタイムを高精度に監視・追跡する新しい情報漏えい対策のアーキテクチャを提案した。情報そのもののライフタイムを追跡できることは内部の者からの犯行に対して有効であり、情報漏えい対策の難しさの本質を解決するものである。