メール添付ファイルのトレースシステムの試作

高　杰　園田俊浩　片山佳則　津田宏
株式会社富士通研究所

1. はじめに

電子メールは、ファイルを共有する最も簡単な手段の一つとしてよく使われる。しかし、企業においてはメール誤送信による機密情報や顧客情報の漏えい事件も大きい問題となっているのも事実である。NPO 日本ネットワークセキュリティ協会によると、2008 年の個人情報漏えいインシデント 1,373 件のうち、Email による漏えい件数は 8.1%（約 112 件）と 4 番目に多い[1]。

メールからの情報漏えい対策(DLP: Data Loss Prevention)として、富士通研究所では、宛先タイプミスや規定ポリシーに合わないメールをチェックするメールフィルタ、およびテキスト特徴を利用したフィンガプリントに基づいた機密文書テキストの類似性(コンテンツシグネチャ)技術を開発した[2]。

しかし、このような DLP 技術では、ファイルを相手に送信した後、それがいかに扱われたか、送信者は把握できない。複数の組織によるプロジェクトで一定期間だけ情報を交換する場合や、組織内で機密情報がどのように利用されたか監査する場合には不十分である。

そこで、我々は送信後にも添付ファイルの操作履歴を送信者がトレースできるトレーサビリティシステムを試作した。本稿では、本システムの概要について述べる。

2. 従来技術の課題と解決手段

送信後でもファイルを保護する手法として、ERM (Enterprise Rights Management)技術がある。ERM では、ファイルそのものは暗号化し、利用時にポリシーサーバからライセンスを付与することで、一定期間だけファイルにアクセスすることを許可するなどが可能である。ただし、ERM はファイルフォーマットが限定的だったり、複数のファイル内容を組み合わせて新たなファイルを作る場合のトレースが難しいなどの課題がある。

これに対して、我々のトレーサビリティシステムは、操作イベント収集、ネットワーク経由のイベントルーティング、およびイベントモニタリング技術の組み合わせにより、特定のメンバー間でのメール添付ファイルの操作をトレースできる。本システムは、Windows API とフックを利用し、アプリケーションに依存せずにファイルに対する操作を監視する。さらに、ファイルのハッシュ値とテキスト特徴に基づいたコンテンツの類似度を計算することで、ファイルの一部を流用して組み合わせる場合でもトレースすることができる。

3. 実現方法

3.1 概要

本トレーサビリティシステムの構成を図 1 に示す。これは、送信者 A があるファイルをメールに添付し受信者 B に送信し、受信者 B は共有サーバや USB メモリ等により同ファイルを第三者である共有者 C に渡すというシーンを示している。B や C の PC には操作監視エージェントがあり、添付ファイルの操作イベントを検知し、イベント送信装置がそのイベントをイベント管理サーバ経由で送信者 A に通知する。送信者 A はファイルの操作履歴をイベントモニタでトレースすることができる。

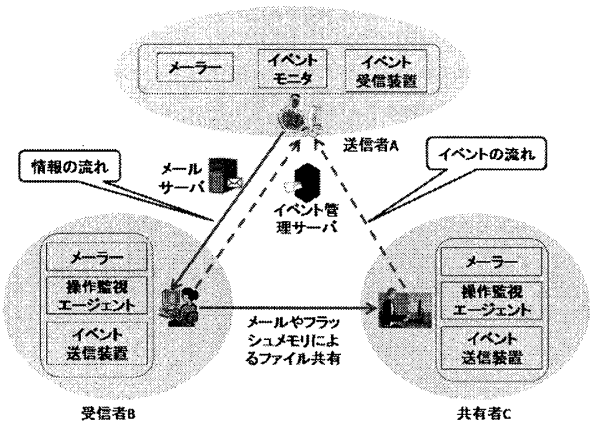

図 1. 本システムの全体図

3.2 操作イベント収集

送信後の添付ファイルをトレースするために

A System for Tracing E-mail Attachment
Jie Gao, Toshihiro Sonoda, Yoshinori Katayama, Hiroshi Tsuda
Fujitsu Laboratories LTD.

は、そのファイルの作成から削除までのライフサイクルを把握する必要がある。本システムは Windows API を用いて、クライアント PC で行われた、添付ファイルの編集や削除等のイベント情報を収集する。また、OS で実行しているプロセスを監視することで、オフィスソフト等のアプリがファイルをオープン・クローズするイベントを取得することができる。

イベント情報には、ファイル内容のテキスト特徴であるハッシュ値およびコンテンツシグネチャを含む。これにより、複数ファイルの一部をコピー&ペーストして別ファイルに流用した場合でも、ファイル間の類似度が計算でき、元ファイルがどのように組み合わされて利用されたかをトレースすることができる。

3.3 イベントルーティング

本トレーサビリティシステムは、ファイル操作イベントを収集した後、必要な操作イベントを適切な宛先に通知するイベントルーティング機能を持つ。本機能は、Publish/Subscribe モデル[3]を活用した。

Publish/Subscribe モデルでは、あるクライアント (Publisher)によって配信されたイベントを、そのイベントに興味があるクライアント(Subscriber)に配信する。ここでは、図 2 に示すように、最初のメール送信者 A が、添付ファイルの属性(ファイル名等)を持つイベントに興味がある旨をサーバに Subscribe する。受信者 B や共有者 C の PC におけるファイル操作イベントはイベント管理サーバに Publish されるが、そのうち Subscribe された属性に一致したイベントだけが、送信者 A に配信される。

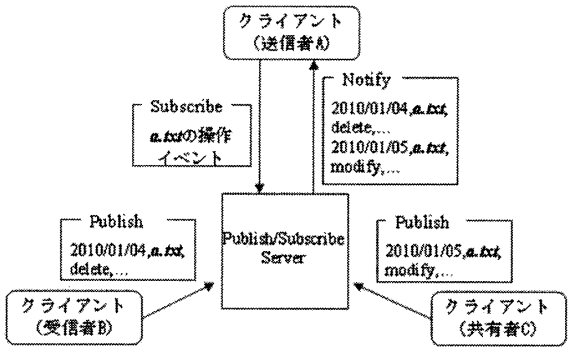

図 2. Publish/Subscribe による
イベントルーティング

3.4 イベントモニタリング

本トレーサビリティシステムは、送信したファイルがいつどのような PC でどのように利用されたかの履歴を、時系列でタイムライン表示するインタフェースを提供する。

図 3 は、送信した添付ファイルが複数クライアントで操作された履歴をモニタした一例を示す。各矩形ブロックはファイルを表す。左上のファイルが、最初に送信したファイルで、それ以外は、これを元に受信者や共有者で操作されたファイルである。ブロックは時間順に並んでおり、2 つのブロックをつなげる矢印は作成・更新・削除などのファイル操作を示す。

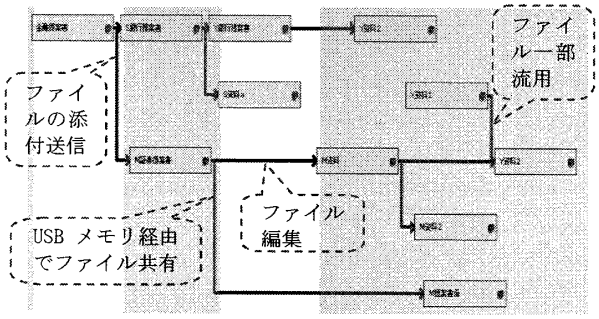

図 3. イベントのモニタ画面

4. まとめと今後の課題

本稿では、メールで送信した添付ファイルが送信後にどのように扱われたかを送信者に通知するトレーサビリティシステムについて述べた。本システムは、メールと連動して相手先でのファイル操作イベントを適切に収集・配信することで実現し、従来の情報漏えい対策技術における送信後のファイルの利用状況を把握できないという課題を解決した。

クラウド技術等の発展により、他社含めた複数組織間での柔軟なコラボレーションが今後ますます重要になってくると考えられる。本研究は、そのような環境での共有情報のトレーサビリティに発展させていく予定である。

参考文献

[1] NPO 日本ネットワークセキュリティ協会: 2008 年情報セキュリティインシデントに関する調査報告書. 2009. http://www.jnsa.org/
[2] 竹林, 津田, 長谷部, 益岡, 情報漏えい防止セキュリティ技術開発への取り組み, Fujitsu, pp. 444-450, Vol. 60, No. 5, 2009. 9.
[3] Eugster, P. T., Felber, P. A., Guerraoui, R., and Kermarrec, A. The many faces of publish/subscribe. ACM Comput. Surv. 35(2):114-131, 2003