3E-7

メール添付ファイルの伝搬トレース方式に関する検討

張　一凡，　太田　光彦，　安田　武，　徳永　大典

西日本電信電話株式会社

†(tyou.iifan, m.oota, t.yasuda, d.tokunaga)@rdc.west.ntt.co.jp

1. 概要

電子ファイルの情報流通を追跡，可視化するシステムとしてトレーサビリティシステム[1]が考案されている．しかし，従来の取り組みではOS レイヤのファイル操作はトレースできるが，メールなどのアプリケーションによるファイルの拡散をトレースすることができない．この課題に対して，メールによる添付ファイルの送受信操作をログとして生成する機能を用いたトレースの実現方法を提案する．

2. 背景

情報漏洩が企業運営に深刻な影響を与えることは過去の多くの漏洩事件から示されている．漏洩事件が発生した際，損失を与えた企業，顧客への賠償金以外にも，漏洩情報と同じ経路をたどり，他にも漏洩が疑われるファイルの特定に多額の費用がかかるケースが多い．漏洩経路や影響範囲の特定を容易かつ高速に実現するシステムとして，ファイルの操作を追跡し，その拡散経路，ライフサイクルを可視化するトレーサビリティシステムが提案されている．

既存のトレーサビリティシステムにおけるファイルの操作追跡を行う技術としては,OS レイヤにファイル操作監視機能を配置することにより監視対象 OS 上で生じた操作を記録する手法が一般的である．特に DaaS に代表されるユーザに管理者権限が渡されない利用環境では監視機能を回避することが困難であるため，ファイルの追跡を実現しやすく，有効な利用シーンとして想定される．

しかし，OS レイヤのファイル監視機能ではメーラやブラウザ，FTP などのアプリケーションレイヤで行われるファイル伝搬を把握することはできない．アプリケーションによる外部へのファイル転送手段は多数存在するが，本研究では企業内でのファイルの伝達経路として利用頻度の高いメールによる伝搬をトレースする方式の実現に取り組む．

A study about tracing transmission of mail attached file
Tyou Iifan, Ota Mitsuhiko, Yasuda Takeshi, Tokunaga Daisuke
NIPPON TELEGRAPH AND TELEPHONE WEST CORPORATION

3. 課題

メール添付によるファイルの伝搬，拡散のトレースを実現するための技術課題として次の 2 点を抽出した．

課題 1. メール添付監視機能の実装，配置方法
課題 2. 既存のファイル操作トレースとの連結

トレースは操作ログを元に実施されるため，操作を監視しログ生成する方式の検討が必要となる．方式を整理するため，既存のファイル操作監視とメール添付ファイルの操作監視を比較しながら考えたい．ファイル操作監視では，コピー，変更，削除，生成などの操作を OS レイヤで監視し，その操作をログとして生成する．これに対して，メール添付監視ではメール作成，添付，送信，削除，転送などの操作を何らかの手段で監視し，ログを生成する必要がある．この機能の実現には上記メール操作の監視機能を実装できるレイヤ(配置箇所)を定め，実装方法検討することが課題 1 である．

課題 1 で示したメール操作の監視機能を実現するには，出力されるログをトレースする機能が必要となる．既存のファイル追跡システムではファイル追跡に特化して，大規模サービスでの実用レベルまでの高速化 [2]を実現している．同等規模のサービスを実現するためのトレースアルゴリズムの開発，既存システムとの連携のためのシステム構成の整理検討が課題 2 である．

4. 提案手法

本章では，3 章で整理したそれぞれの課題について，対応方法を検討し，実現方式を提案する．

提案 1. メール添付監視機能の実装，配置方法

メール添付監視機能の実現に向け，図 1 の①～③の手法を検討した．

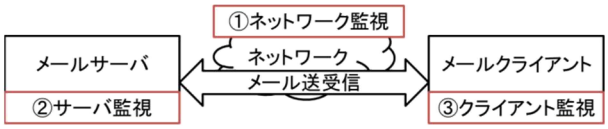

図 1 メール監視ポイント

①のようにネットワークレベルで監視する手法は，暗号化通信を利用した場合に監視できない．また通信内容を監視できても，その通信内容に相当する実在する添付ファイルがユーザの保持するどのファイルかを解決するためのシス

テムがないと実現できず，通信内容から実際送信されたファイルを調べるには，送信され得る全てのファイルを管理できるデータベースが必要になるなど，機能を実現するために必要なシステム規模が増大する．更にこの手法ではメールサーバに蓄積されたデータの利用状況，受信したユーザがメーラの受信ボックスから添付ファイルをどこに何回ダウンロードしたかを特定できない．

②のようにサーバで監視する手法は，①の監視に比べ，暗号化通信により生じた問題が解決される．他にも，サーバによっては，受信メールをローカルの受信ボックスにダウンロードしないようにすることも可能であり，その場合，②の機能単体で添付ファイルを何度ダウンロードしたかを監視できる．しかし，監視できる対象はファイル添付ユーザと添付されたファイルがメインとなるため，送信されたファイルがユーザの保持するどのファイルかを解決できない．

③のようにメーラ機能として監視する手法では，送信メールに添付されたファイルや受信メールからダウンロードされた添付ファイルの保存先がユーザ端末上のどのファイルに対応するかを一意に解決するログを生成できる．受信ボックスからの複数回のダウンロードも API が提供されている限り実装できる．しかし，メーラのアドオンだけではメールサーバ上での転送状態やメールサーバ上での削除などを監視できず，アドオンのない環境のメール受信と添付ファイルのダウンロードを把握できない．

上記を踏まえ，本研究では②，③を組み合わせてトレースログを生成する方式を提案する．①～③の手法を単独で適用するだけでは添付，送受信，ダウンロードの伝達経路全体を監視することができず，トレースの一貫性保証を実現できない．この課題に対し，③のメーラでファイル添付，ダウンロード，受信ボックス操作を監視し，同時に②のサーバアドオンでメールの転送状況を監視することにより，サーバ・クライアント両サイドで一貫性のある添付ファイルの監視を保証できる．

提案 2.既存のファイル操作トレースとの連結

既存のファイルのトレースシステムとの連携方法を検討するにあたり，高速処理が実装されている既存の技術を活用するために，メール操作についても，OS 上のファイル操作の一種となるようなログの生成ができないか考察を行った．

メール送信による情報伝達は，メール内容を記載したファイルをメールサーバのフォルダにコピーする操作に置き換えられる．同様に「メール受信」はメールサーバのフォルダにある「メールファイルをローカルにコピー」に相当し，「メールボックスからの削除」が「ファイルの削除」，「受信ボックスの仕分け」は「ファイルの移動」に相当するなど，メール送受信とファイル操作の対応関係を整理できた．

以上のことから，既存のファイル操作に合わせて，「メールをメールサーバへコピーし，そのファイルを配信サーバへ移動させ，受信者端末が受信の際コピーを作った」という一連のメール送受信操作をファイル操作に置き換えたログを出力することで，ファイルトレースシステムでメールの追跡を可能にする手法を提案する．

5. 実現に向けた課題

トレースシステム実装のため，提案方式の実現性について検討する．提案方式はいずれも手法自体複雑ではないが，開発の難易度は監視対象となるサーバやメーラに依存する．例えば，Exchange サーバであればサーバ側のアドオンの開発は RFC でメール送受信に関する定義がされているため，API の実装検討が容易にできる．しかし，Outlook ではユーザの操作パターンが数多くあり，添付ファイルのダウンロードイベントを取得するための API が不足している．

本方式の実装に向けては，監視対象の精査や不足する情報を補完する仕組みが用意できれば，実現性を確保できる．

6. まとめ

本研究ではメール添付によるファイル伝搬，拡散をトレースするためのログ生成システムとして，メールサーバとメールクライアントへのアドイン開発を提案した．更に，ファイル操作の形式に合わせてメール送受信ログを生成することにより，既存のデータトレースシステムに変更を加えず，メールボックスに残る添付ファイルの特定も実現できる方式を提案した．この手法と既存手法および監視対象を考慮しつつ実現することにより，今後発生するファイル操作とメールへの添付による情報漏洩に対して，効果的な事後対策となると考えられる．本手法の性能等は今後開発を通して検証する予定である．

参考文献

[1] Iifan Tyou, Shinichi Nakahara, “The Accountability of Cloud Services and Traceability Technology” APNOMS2012

[2] 張一凡, 竹内格, “MapReduce を用いたログ間の依存関係ツリーの抽出アルゴリズムの提案” 情報処理学会全国大会 2011