1D-5

CyebrTrace:OS イベントのリアルタイム解析による高精度機密情報監視

†坂本　久　　†喜田　弘司　　‡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　‡サーバソフトウェア事業部

1. はじめに

現在、情報漏えい対策の一つとしてコンピュータ上での操作を監視するシステムが多数存在する。しかしながら、そのほとんどは実際に情報漏えいに関係する操作を特定することは難しく、監視結果を有効に活用できていない。この原因は、従来の監視システムは OS からの低水準なイベントをそのまま大量のログとして記録することにある。大量のログから利用方法の仮説をたて、ひとつひとつ検証する作業は、膨大な時間と労力が必要である。

我々は、従来の監視システムが情報漏えい操作の検出にあまり効果がない原因の本質は、ログが大量の低水準な監視結果であることにあると考える。そこで、より高次の必要最小限の監視結果をログに残すことが重要であると考える。本稿では、ファイルの生成、編集、複製、移動メール添付、共有などの操作事象を高精度に監視する方式とそれに基づくシステム CyberTrace および、その評価結果を説明する。

2. 監視システムの分析

従来の監視システムは OS が発生する低水準イベントを記録（ファイル I/O、ウインドウタイトル変化等）とファイル名を基にした監視を行っていた。その問題は以下の事柄がある。

ログ量問題：OS からの低水準イベントをそのまま記録するため大量にログが出力される。大量のログからファイルの移動／コピーを特定することは極めて困難である。また大量のイベントを処理することでパフォーマンスの低下も引き起こす。

ファイル名問題：ファイル名をベースに機密文書を識別しているため、ファイル名だけでは特定できない移動／コピーに関しては追跡できない。例えば、添付メールによるファイル配布のように、ネットワークを経由したファイルの移動／コピーは追跡できない。

アプリケーション操作によるファイル操作問題：ユーザによるアプリケーションの GUI 操作に伴うファイルの移動／コピーは追跡できない。（例：名前を付けて保存）

A proposal of a high-level monitoring method with analyzing realtime events generated operating system
Hisashi Sakamoto, Koji Kida, Hiroyuki Takahashi,
NEC System Technologies, Ltd.

3. CyberTrace による高精度機密情報監視

CyberTrace では以下の２つの課題を解決する。

（１）１台のコンピュータに注目し、このコンピュータ内で発生したファイルの移動やコピーを正確に監視

（２）ファイルが複数のコンピュータに跨って移動した場合にも正確に監視

以下では、前者の技術「ファイル操作／システム挙動照合技術」と、後者の技術「ファイル追跡電子透かし技術」を説明する。

3.1. ファイル操作／システム挙動照合技術

必要最小限の監視結果をログに残すために、低水準な監視結果をリアルタイムに解析して、その意味を推定しログに出力する。低水準なイベントは、ユーザの GUI の操作イベントとファイルアクセスイベントである。意味を推定するためにアプリケーションの振る舞いをモデル化した「*AP 知識*」を利用する。AP 知識は、GUI の操作イベントの系列に対してその意味を割り当てたデータである。低水準イベントの系列に対してＡＰ知識を使って整合性のある解釈を作成することにより高次な監視ができる（図１）。

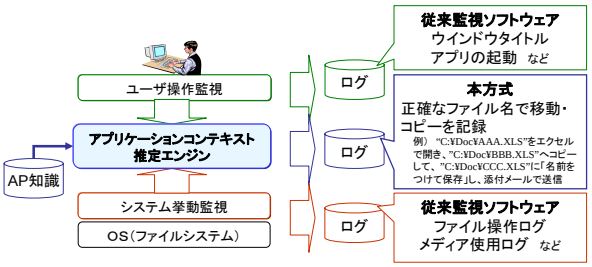

図 1ファイル操作／システム挙動照合技術

AP 知識を使ってコンテキスト推定エンジンが低水準の事象から高水準の事象を組み立てる。このエンジンは以下から構成される。

コンテキスト管理部：AP の各機能を利用する一連の操作において、どこまでユーザが操作をしたかという状態遷移(ｺﾝﾃｷｽﾄ)を AP 知識を使って管理

GUI 操作キュ：ユーザ操作監視結果列を管理

ファイルアクセスキュ：ﾌｧｲﾙｱｸｾｽｲﾍﾞﾝﾄ列を管理

ログ生成：GUI 操作キュのイベント集合とコンテキスト管理部のコンテキストを照合し GUI 操作の解釈を作成。解釈に成功すればファイルアクセス

キュからファイル名を取得して高次なログを生成

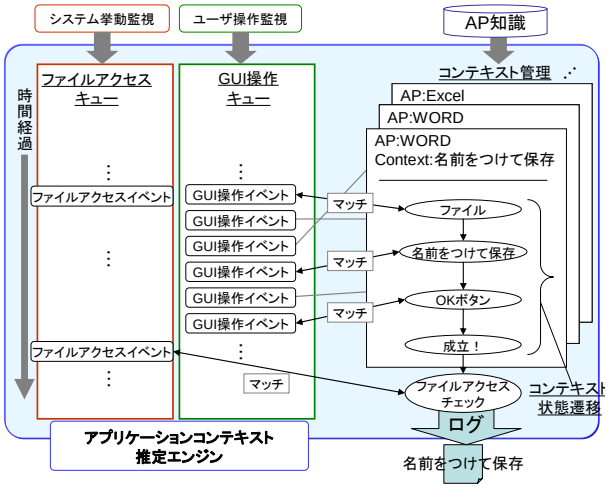

図 2 AP 知識による操作ｲﾍﾞﾝﾄｺﾝﾃｷｽﾄ情報変換

3.2. 動作例

メモ帳（notepad.exe）で「名前をつけて保存」を実行する場合の AP 知識の例を以下に示す。

```
<Application name="notepad">
  <Context name="名前を付けて保存">
    <Operate id=1 type="menu">保存</Operate>
    <Operate id=2 type="button">OK</Operate>
  </Context>
</Application>
```

図 3 「名前を付けて保存」コンテキストの AP 知識

この例では、ユーザが”保存”メニューを選択し、その後表示されたダイアログ上の”OK”ボタンを選択することにより、”名前を付けて保存”コンテキストが成立する。コンテキストが成立した場合は、成立後に発生した特定のファイルアクセスイベントを照合することにより、どのファイルが保存されたかを推定しログに残す。

3.3. ファイル追跡電子透かし技術

複数のコンピュータに跨って機密文章のＩＤを管理できる必要がある。従来技術ではファイル名をベースにしており追跡範囲が限られていた。本方式は、機密文書に文章ＩＤを割り振り、機密文書を配布メディア（メール、USB メモリ、ネットワーク共有）に対してコピーする直前に文章ＩＤを電子透かしとして付加する。機密文書に付加された電子透かしとサーバのログの文章ＩＤをマッチングさせることで高精度に配布経路を追跡できる（図４）。

例えば、電子メールに機密文章を添付して配布した場合、受け取り側では文章ＩＤの電子透かしが埋め込まれた機密文章を受け取ることになる。以後、受け取り側では、この電子透かしから復元した文章ＩＤを受け継いでログに残す。これにより、メール送信者とメール受信者の間の機密文書の流通を監視することが可能になる。

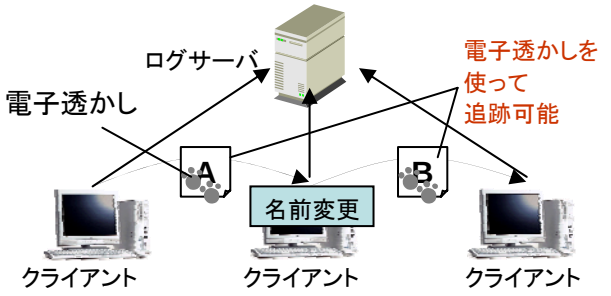

図 4 ファイル追跡電子透かし技術

4. 評価

本方式を従来方式と比較評価する。

従来方式と提案方式で同一操作実行後ログ出力量を測定した。提案方式のログ出力量が従来方式より激減している結果を得られた（表１）。

表 1 ログ出力量の比較

コピー、保存、印刷、メール送信等を含む１４操作	従来方式	提案方式
	６３９行	５８行

これは、本方式が従来方式のように低水準のイベントをそのままログに出力するのではなく、複数の低水準イベントから AP 知識を使ってより高次のログに変換して出力しているためである。

ファイル I/O イベントと GUI 操作イベントを併用した監視や電子透かしによるファイル追跡により、従来方式では出来なかった以下のシチュエーションの追跡が可能になった。

・ファイルコピー：名前を付けて保存
・他のＰＣへのファイルコピー：メール添付
・文書の内のデータのコピー／移動：ＡＰ上でコピー＆ペースト

新方式での監視環境と従来方式での監視環境でファイルの転送性能を測定した。

表 2 ファイルコピー時の転送速度

ファイル(64KByte)連続コピー時の転送速度	従来方式	提案方式
	879KB/sec	1078KB/sec

※PentiumⅢ 833MHz 256M メモリ WindowsXP(SP2)で測定

これにより、新方式が従来方式に比べてシステムに負荷をあまり与えないという結果を得た。

5. まとめ

本稿では、機密情報のライフタイムを高精度に監視追跡する方式を提案した。これは、ファイル操作／システム挙動照合技術とファイル追跡電子透かし技術を新たに開発し実現した。評価実験により、従来方式と比べて必要最小限のログを出力できていることが確認できた。