2009－GN－70 (6)
2009／1／22

機密データの伝搬経路可視化手法

中山 佑輝† 稲場 太郎‡ 芝口 誠仁‡ 岡田 謙一†

情報化社会の進展による情報の電子ファイル化によって，機密データが漏洩してしまう危険性が急激に増大した．ゆえに，情報を扱う各組織の管理者にとって，機密データを所持するホストや機密データの送受信・複製を把握するなどの漏洩対策を講じることが重要となっている．そこで，本稿では機密データの伝搬経路を可視化する手法を提案する．本提案手法はスケールの異なる5つの可視化手法を併用することによって，スケーラブルでかつ多様な伝搬方途に対応した可視化を実現した．本手法を用いることによって，管理者は常日頃から機密データの所在を容易に把握でき，それによって漏洩を事前に防止することが可能となる．更には，漏洩が発覚してしまった際の解析作業を支援するツールとしての利用も可能であり，デジタルフォレンジックにおける解析・証拠提示の分野においても本提案手法は漏洩対策に貢献する．

Visualization of Transmission Route of Confidential Data

Yuki Nakayama† , Taro Inaba‡ , Seiji Shibaguchi‡ , and Ken-ichi Okada†

This paper describes a visualization technique for use in tracing confidential data. In recent years, the damage by information leakage is extensive because anyone can copy electoric files, even confidential documents, very easily. Our proposal technique is able to counteract the damage. Concretely speaking, our system enables administrators to figure out that which host has confidential data and how secret information is transmitted, received and duplicated. We also aim to work out a method of a scalable and capable visualization framework. *i.e.* That can meet the diverse size of companies and ways of propagations. As a result, our technique enables to forestall leakage, to analyze transmission routes and to adduce evidences. And this method contributes a countermeasure against information leakage.

1 はじめに

情報化社会の発展に伴い，情報の媒体は紙から電子へとその主流を移行した．時期を同じくして機密情報の漏洩が深刻化し，それに関するニュースが日々世間を賑わすようになった．このような情報漏洩の頻発は電子ファイルのコピー&ペーストによる複製やリムーバブルメディアによる持ち出しが非常に容易であることに由来する．そして，現在に至っても情報漏洩の被害は甚大であり，現代社会の抱える大きな課題のひとつといえる．2008年現在，情報漏洩はセキュリティの10大脅威の第3位に位置づけられている [1]．ゆえに，近年の情報を扱う企業をはじめとする様々な組織にとって，情報漏洩に備えた対策を講じることが必要不可欠となっている．

一般的な漏洩対策はその特性から事前対策と事後対策に大別が可能である．事前対策は漏洩を未然に防ぐことを目的としており，USBメモリの利用を禁止することやプリントアウトを制限することが例として挙げられる．また，機密ファイルの所在を常日頃から把握しておくことも重要な事前対策となる．その理由は，機密情報流出の主たる原因であるPCの持ち出しや盗難による流出 [1] の危険性を知ることができ，機密ファイルを削除させるなど，危険を回避するための対応が可能となるためである．

また，事前対策を講じる際には，それによる作業効率の低下を考慮しなければならない．例えば，PCの持ち出しを禁止することによって漏洩に対するセキュリティレベルは向上するが，同時に従業員の労働時間が制約され生産性も低下してしまう．すなわち，事前対策によるセキュリティ向上と利便性低下のバランスを熟慮する必要がある．

一方の事後対策は漏洩発覚後にその主眼をおいており，早急な原因究明を行うことのできる体制を整えておくことが例として挙げられる．このような体制を整えることによって，関連企業に対する迅速な報告が可能となり，企業の信頼低下を最小限にとどめることができる．更に，裁判などの法的な場においては，解析結果を専門知識のない人に提示する必要が生じる．ゆえに，わかりやすい解析結果の提示も事後対策として重要となる．

事後対策を提供する既存のツールは往々にしてログを収集し，それを管理者が解析するというものである [2, 3]．しかし，ログは膨大な量のテキストデータの羅列であり，その解析には非常に多くの時間と労力を要する．一方で

† 慶應義塾大学理工学部
Faculty of Science and Technology, Keio University
‡ 慶應義塾大学院理工学研究科
Graduate School of Science and Technology, Keio University

漏洩発覚に際して，その対応の迅速さは企業の信頼性を大きく左右する．ゆえに，単にログデータを収集するのではなく，その解析作業を容易にすることに大きな意義があると我々は考える．

そこで，本稿では機密データの伝搬経路を可視化する手法を提案する．本提案手法ではスケールの異なる5つの可視化手法を併せ用いることによって，スケーラブルでかつ多様な伝搬方途に対応した可視化を実現した．これにより，機密データを所有するホストを容易に把握することが可能となる．本手法は従業員に対する制約を設けることなく実現されるため，利便性の低下を極力抑えセキュリティレベルの向上を図ることが可能である．また，機密データの伝搬経路を解析する作業を簡素化することが可能となる他，直感的な理解を支援するインタフェースの提供によって，専門知識のない人にも理解が容易である．すなわち，本提案手法は事前対策・事後対策の両面で情報漏洩対策に貢献する．

本稿の以下の構成は次の通りである．まず，2章で関連研究を取り上げる．3章では提案手法の概要を述べ，4章で提案手法のプロトタイプについて記す．5章ではそのプロトタイプを用いた解析の例を示し，6章で将来性について考察する．最後に7章を本稿のまとめとする．

2 関連研究

機密情報の監視を行う関連研究としてSKYSEA Client View [2] とInfoCage [3] がある．SKYSEA Client Viewはファイル追跡をはじめUSBメモリの使用検知や印刷履歴の記録も可能な情報漏洩対策ツールである．当ツールにおけるファイル追跡の解析作業は検索と絞り込みにより行う．しかし，その結果は表1のようなリストとして表示されるため，ファイルの受け渡しの流れなどを直感的に把握することは困難である．一方のInfoCageは国内検疫ツール市場分野において2005 ～ 07年の3年連続シェアNo.1を獲得したツールである [4]．InfoCageでは「協調型セキュリティ」をコンセプトに，PC・ファイル・サーバ・ネットワークといった情報が滞在する箇所それぞれに必要な対策を提供する非常に優れたツールである．しかしながら，解析作業の効率化に関してはアプローチが余りなされていないのも現状である．

一方でセキュリティを脅かす技術が年々高度なものとなってきている．そのためシステム的な対策のみでは十分に対応し切れないことが増えてきた．そこで，判断の一部を人間に託すというアプローチが注目を集めており，関連研究も多々行われている [5, 6, 7, 8]．しかし，システムを人間が直接扱うことは非常に困難である．ゆえに，セキュリティという極めて抽象的で理解の困難なモノを可視化し人間の理解を補佐するツールの開発には大いに

表 1: SKYSEA Client View ファイル追跡の詳細表示

日時	操作ユーザ名	元ファイル	・・・
2008/02/05 18:42:02.250	nakayama	C:...\confidential.xls	・・・
2008/02/05 18:42:08.093	nakayama	C:...\X-File.xla	・・・
:	:	:	:

意義があるといえる．本稿の提案手法は機密データの追跡における視覚化技術の先駆となることを目指す．

3 機密データ伝搬経路可視化手法

本章では，素早い状況把握と容易な解析作業および解析結果の提示を可能とする提案可視化手法の概要について記す．本提案手法はスケールの異なる5つの可視化手法を提供する．そして，それらをツリー状に配置することによって，多様な組織規模に対して柔軟に対応可能な視覚化を実現する．また，多様な伝搬手段を視覚化の対象とし，それらの直感的な理解を可能とする．

3.1 可視化の課題

機密データを追跡し可視化するに際しては以下のような問題がある．

スケーラビリティ 何台のPCを（あるいは，いくつの機密ファイルを）監視対象として収容可能であるかという問題．導入する組織の規模に対して柔軟に対応することが可能な視覚化が要求される．

伝搬方途の多様性 データの伝搬にはネットワークを介したものや外部デバイスを用いたものなどがあり，更にクライアント内での移動や編集・複製といった伝搬も含めると，その手段は多岐にわたる（図1）．このことも解析作業および視覚化を困難なものとしている要因として挙げられる．ゆえに，多彩な漏洩経路を分かりやすく可視化することが重要となる．

図 1: 機密情報の追跡

3.2 課題の実現

本提案手法ではグループ，ネットワーク，クライアント，ディレクトリ，アプリケーションをそれぞれベースとした5つの可視化手法を併用することでこれらの課題を克服した．5つの可視化手法の位置づけを図2に示す．この図は一組織のネットワークをマクロからミクロへと順にその構成要素で分解し階層表示したピラミッドと，その構成要素と提案手法との対応を示すものである．下位2つの手法はネットワークを介した伝搬を，上位3つは各クライアントにおける伝搬をそれぞれ可視化の対象

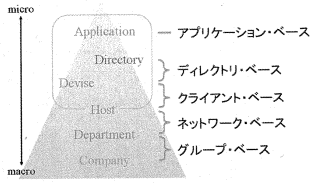

図 2: 5 つの可視化手法の位置づけ

としている．具体的には，グループ・ベース手法では複数のホストで構成されるグループの間におけるファイル交換を可視化し，ネットワーク・ベース手法では各ホスト間でのファイル交換を可視化する．また，クライアント・ベース手法は各クライアントにおけるファイルの出入りを，ディレクトリ・ベース手法はホスト内におけるファイルの移動の流れを監視する．アプリケーション・ベース手法は機密ファイルが開かれているときのアプリケーションやユーザの挙動を監視する．そして，スケールの異なるこれらの可視化手法を図 3 のようにツリー状に配置する．このように 5 つの可視化手法を設計することによって，スケーラブルでかつ多様な伝搬方途に対応した可視化を実現した．尚，巨大企業で監視対象の PC 数が膨大な場合においても，いくつかのグループの集まりをひとつのグループとする可視化を取り入れることで対応が可能である．

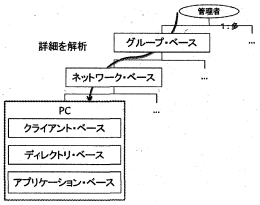

図 3: 各手法の配置と解析作業

4 FileTracingViewer

本章では，提案手法のコンセプトをもとに，Windows 環境で動作するよう構築したプロトタイプである FileTracingViewer におけるシステム構成と 5 つの可視化手法について詳述する．

4.1 システム構成

システムの全体像を図 4 に示す．提案手法では監視対象となる PC に監視プログラムを予めインストールしておくことを想定している．また，追跡すべき機密データを特定するための情報や監視アプリケーションの情報，セキュリティポリシーに基づいたネットワーク情報・遵守事項といった情報をデータベース化しておく．監視プログラムはこのデータベースを参照すると共に機密データの送受信・複製といった動作の監視を行い，得られた監視データを管理サーバに送信する．こうして集積されたデータを可視化し管理者に提供する．

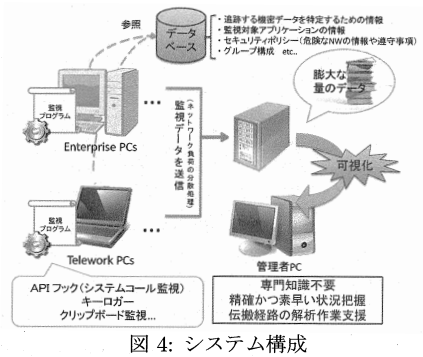

図 4: システム構成

4.2 5 つの可視化手法

4.2.1 グループ・ベース手法（GRP）

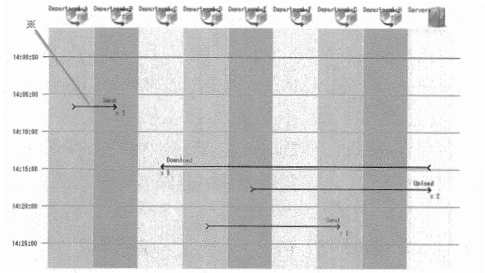

図 5: GRP

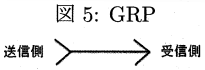

図 6: 送受信のペア表記

数台のホストの集まりをひとつのグループとして扱い，グループ-グループ間およびグループ-サーバ間における機密ファイルのやり取りを可視化したものがグループ・ベース手法（以下 GRP）である．GRP の例を図 5 に示す．縦に広がる 9 個の領域の内，最も右に表示されている領域がサーバ群を表しており，その他の領域はそれぞれがひとつのグループを表している．そして，図 6 に示すような矢印によって送受信グループのペアを表現している．尚，本来ファイル交換をすべきではないグループ間における送受信や危険なネットワーク経由におけるファイル転送の場合，この矢印を赤色で表示し管理者に注意を促す．また，矢印の先端に記された「x 2」等の数字表記は送受信されたファイルの数を表している．監視の対象は，あるグループのホストから他のグループのホストへの Send，サーバからグループ内のホストへの Download，グループ内のホストからサーバへの Upload である．以上のことを踏まえると，図 5 に示す※からは「14 時 7 分頃，グループ A のホストからグループ B のホストに機密ファイルが 2 つ送信された」ことが分かる．

また，GRP はシミュレーション・モニタ（SimMon）とトレーシング・モニタ（TrcMon）を同時に提供する．

それぞれの例を図 7 および図 8 に示す．SimMon では各グループを 2 次元的に配置し，ある時刻における各グループ間のファイル移動を描線によって表現する．更に，線の色でオペレーションを，太さの変化で送信側（細）・受信側（太）を表現している．管理者が任意にシミュレーションを再生することができ，機密ファイルの流れをシミュレートすることが可能である．図 7 は，ある時刻において「グループ 4 からグループ 7 へのファイル送信，グループ 1 からサーバへのアップロード，グループ 3 によるサーバからのダウンロード」が行われたことを表している．シミュレーション再生時には表示が連続的に切り替わり，通信状況を再現できる．これにより，ファイルの流れを直感的に理解することが可能となる．SimMon の特徴として，同時刻における送信を表現する際にも表示が重ならないといった利点がある．一方の TrcMon はひとつの機密ファイルに着目し，そのネットワーク伝搬経路を示す．SimMon では全てのファイル移動の追跡を行ったのに対し，TrcMon ではひとつのファイルのみを可視化の対象としている点が特徴である．線の太さで時間を表現し，色の変化で伝搬経路の分岐を表している．図 8 には，「グループ 1 によってサーバからダウンロードされた機密ファイルがグループ 3 を経由しグループ 5 へと伝搬後，異なる 2 つのグループへと送信され，その後も伝搬する」様子が表現されている．追跡の開始ポイントと追跡の深さを自由に変更可能で，管理者の解析作業を支援する．

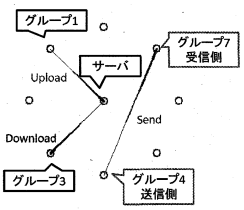

図 7: SimMon

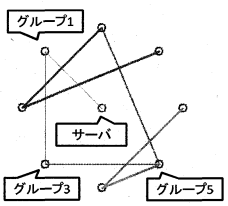

図 8: TrcMon

4.2.2 ネットワーク・ベース手法（NET）

GRP におけるひとつのグループをピックアップし，そのグループに属する各ホスト間における機密データの流れを可視化したものがネットワーク・ベース手法（以下 NET）である．図 9 に例を示す．中央にサーバを配置し，その左に社内 PC，右にテレワーク PC の領域を配置した．監視対象は，Email やメッセンジャーによる Send，FTP による社内ファイルサーバからの Download，FTP による社内ファイルサーバへの Upload，ネットワークの安全性，クライアントの安全性である．クライアントが安全でないと判断された場合，該当するホストの領域に赤い斜線領域を描画することによって管理者に注意を促す（図 9（A））．ネットワークが安全な状態でない場合も同様に黄色い領域の描画を行う（図 9（B））．また，NET も GRP と同様に SimMon と TrcMon を提供する．

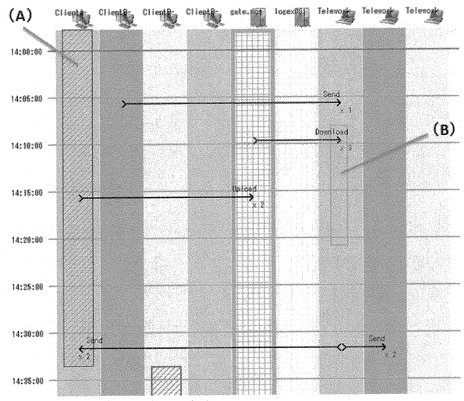

図 9: NET

4.2.3 クライアント・ベース手法（CLT）

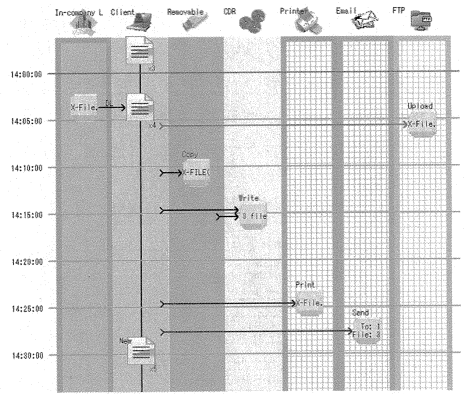

図 10: CLT

クライアント・ベース手法（以下 CLT）は NET における一台のホストに注目し，そのホストを中心とした機密データの出入りを可視化する．図 10 に CLT の例を示す．左端の領域にサーバ群，その右に CLT の主体となるクライアント，以下リムーバブルディスク，CD-R，プリンタ，Email，FTP と続く．クライアント領域内では機密ファイル数の変化が表示されている．監視対象は，社内ファイルサーバからの Download，FTP による Upload，USB メモリ，メモリカード等のリムーバブルメディアへの Copy，CD-R 等の磁気媒体への Write，紙媒体への Print，Email による Send，クライアント内での新たな追跡ファイルの作成（New）である．

4.2.4 ディレクトリ・ベース手法（DIR）

ディレクトリ・ベース手法（以下 DIR）は各ホスト内での機密データの移動・複製を監視する手法である．図 11 に例を示す．ディレクトリ，ごみ箱，プリンタ，Email，FTP の領域が設けられており，それらの間におけるファ

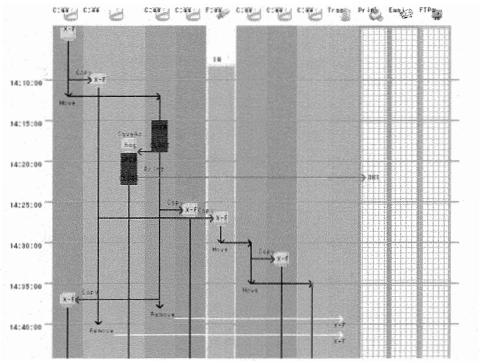

図 11: DIR

イル移動を可視化する．可視化の対象はファイルのコピー，Save As による複製，移動，リネーム，オープン・クローズ，削除・復元，圧縮・解凍，分割・結合，Email による送信，FTP によるアップロードである．

4.2.5 アプリケーション・ベース手法（APP）

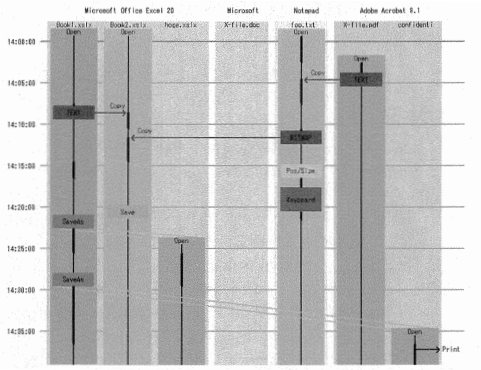

図 12: APP

アプリケーション・ベース手法（以下 APP）では機密情報の記されたファイルが開かれているときのみ監視を行う．その監視対象は実行されている全ウィンドウアプリケーションである．APP の例を図 12 に示す．それぞれのアプリケーションの領域内に個々のファイルの領域が割り当てられる．例えば，「14 時 5 分に Adobe Acrobat 8.1 を用いて X-File.pdf が開かれている」ことが分かる．更に，「14 時 5 分頃，X-File.pdf 内の一部のテキストデータが Notepad で開かれた foo.txt にコピーされた」ことが分かる．また，太線はその時刻における最前面ウィンドウを表している．監視の対象とするオペレーションはコピー&ペースト，キーボード入力，ウィンドウアプリケーションのポジション・サイズ・Z-インデックスである．これらの監視によってコピー&ペーストやスクリーンキャプチャ，キーボード入力によるアナログ的複製などを検知でき，一般ユーザレベルの悪意ある複製行為を検知することが可能となる．

更に，APP ではディスプレイ再現モニタ（DspMon）を提供する（図 13）．DspMon はユーザが操作を行っていた際のディスプレイ状況を忠実に再現するものである．これを用いることによって，管理者はユーザの操作履歴をより直感的に把握することが可能となる．

尚，APP の実現に際して，監視するアプリケーションに関する情報を予めデータベースに登録しておく．監視プログラムはこれを参照することによってアプリケーション監視を行う．このようなシステム構成とすることによって，アプリケーション情報の更新が容易になり，また企業によるアプリケーションの使用制限にも対応が可能となる．

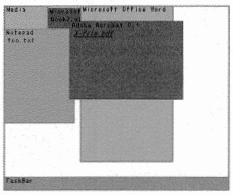

図 13: DspMon

5 解析作業

「漏洩したファイルが判明しており，その漏洩原因を特定したい」状況を想定した解析作業の手順を記す．図 14 に FileTracingViewer の実行画面と解析手順を示した．

まず，実行画面の左上のツリービューから追跡ファイルを決定する．(ツリービューは各ホストやサーバの所持する機密ファイルを表示している．) すると，各手法において選択ファイルに関する情報が選別され表示される．

次に GRP の TrcMon を用いて解析対象とすべきグループを決定する．解析すべき時間帯などが具体的に決まっている際には，GRP のメイン画面を用いて解析対象を絞り込むことが可能である．

解析を行うグループをひとつ決定し，NET を用いてそのグループに関する解析を行う．機密データが危険な

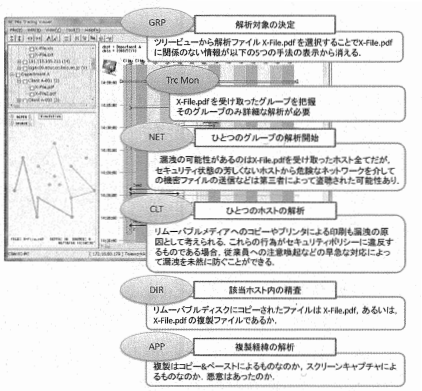

図 14: 解析作業の流れ

ネットワークを経由していなかったか，セキュリティ対策に問題のあるクライアント内に存在していなかったかを確認する．問題があった場合，第三者によって盗まれた可能性があると判断できる．

また，機密データを受け取ったホストに関しても順に調査する必要がある．そこでCLTを用い，リムーバブルディスクに機密データを移していないか，プリンタによって印刷されていないかといった事実確認を行う．これらの行為がセキュリティポリシーに違反するものであれば，漏洩事実の有無に関わらず，対象となる従業員への速やかな注意喚起が必要となる．このようなEmailやポップアップによる注意喚起を行い，監視されているという自覚を従業員に抱かさせることによって，内部犯による漏洩を抑止することも可能である．

CLTによって漏洩の事実が確認された際には，DIRを用いることによって該当ホスト内における機密データの追跡を行い，漏洩に至った経緯を知ることができる．

更に，悪意ある漏洩が発生してしまった際には，先のような解析からは悪意を特定するには至らないことが予想される．そこで，APPを用いることにより，悪意の特定とその証拠確保を行うことが可能である．

6 今後の展望

本稿においては提案手法の有用性に関する考察が欠けている．具体的には「本提案手法を充足する監視プログラムが通常の作業に支障をきたさない程度のマシン負荷で実現可能であるか」「監視データの送受信によるネットワーク負荷が通常業務に支障をきたさないレベルであるか」「ログの肥大化で許容以上のストレージ領域を消費しないか」といった事項に関して，シミュレーションに基づく考察が必要である．

そして，将来的には本提案手法に対してインタラクションをとることによって実システムを管理し得るツールの開発を行いたいと考えている．具体的には，本提案手法によって漏洩の危険性を事前に把握できた場合，それに対して直接インタラクションをとることによって，特定の従業員に対する注意喚起を行ったり通信を遮断したりといった処理を行うことを目標としている．我々の目指すファイル追跡技術を形容するなら，現在英国の街中に設置され注目を集めている「話す監視カメラ」である[9]．拉致・暴行・スリなどの犯罪を確認した監視員はこの監視カメラを通じて犯人に話しかけることが可能である．このように犯人に対して語りかけることによって犯罪が未然に防がれるケースが数多く報告されている．すなわち，話す監視カメラは犯罪捜査に重要な証拠保全能力は基より，犯罪に対する抑止力も有する優れたシステムである．機密データの追跡に関しては，本稿の提案手法によって，その所在と伝搬を素早く把握することが可能となった．更に，それに対するインタラクションによって従業員に対する注意喚起を行ったり，強制的に通信を遮断したりといった対策を講じることによって「話すファイル監視」が実現可能であると考えている．

7 まとめ

近年の情報化社会の発展によって，情報の電子ファイル化が急激に進んだ．そして，電子ファイルの複製や持ち出しの容易さゆえ，情報の漏洩事件が多発し現在でもそれは後を絶たない．ゆえに，情報を扱う組織にとって情報漏洩に備えることは必要不可欠である．そこで本稿では機密データの伝搬経路可視化手法を提案した．本手法は5つのスケールの異なる手法を併用することによりスケーラビリティを有し，かつ多様な伝搬方途をカバーし得る可視化に成功した．本提案手法を用いることで機密データを保持するホストを容易に把握可能となり，情報漏洩の事前対策として有効である．更には，漏洩発覚後の解析作業や証拠提示，すなわちデジタルフォレンジックにおいても本提案手法は漏洩対策に貢献する．

参考文献

[1] 独立行政法人 情報処理推進機構．情報セキュリティ白書2008 第II部 10大脅威 ますます進む『見えない化』．2008.5.

[2] SKYSEA Client View. http://www.skyseaclientview.net/. 2008年11月28日確認.

[3] Koji Kida, Hisashi Sakamoto, Hideo Shimazu and Hiroyuki Terumi. "InfoCage: A Development and Evaluation of Confidential File Lifetime Monitoring Technology by Analyzing Events from File Systems and GUIs." Proceedings of the 2nd International Workshop on Security (IWSEC 2007), 2007.

[4] NEC Empowered by Innovation. http://www.nec.co.jp/press/ja/0808/2701.html. 2008年11月16日確認.

[5] Wei-Jan Li, Shlomo Hershkop, Salvatore J.Stolfo. "Email Archive Analysis Through Graphical Visualization." VizSEC/DMSEC '04, October 29, 2004.

[6] Jeffrey B. Colombe, Gregory Stephens. "Statstical Profilling and Visualization for Detection of Malicious Insider Attacks on Computer Networks." VizSEC/DMSEC '04, October 29, 2004.

[7] Glenn A.Fink, Paul Mussig, Chris North. "Visual Correlation of Host Processes and Network Traffic." Workshop on Visualization for Computer Security, October 26, 2005.

[8] William Yurcik, Xin Meng, Nadir Kiyanclar. "NVisionCC: A Visualization Framework for Height Performance Cluster Security." VizSEC/DMSEC '04, October 29, 2004.

[9] 'Talking' CCTV scolds offenders. BBC NEWS. http://news.bbc.co.uk/2/6524495.stm, Wednesday, 4 April 2007. 2008年11月16日確認.