標的型攻撃の全貌をひと目で把握する高速フォレンジック技術

High-Speed Forensic Technology for Promptly Analyzing Damage after Targeted Attacks

● 海野由紀　● 及川孝徳　● 古川和快　● 森永正信　● 武仲正彦

あらまし

政府官公庁や特定の企業，個人を標的として情報窃取を行うことを目的とした標的型攻撃は年々増加を続けており，その攻撃の手口はますます巧妙化している。標的型攻撃では，攻撃者は標的を十分に事前調査して執拗に攻撃を仕掛けるため，組織内ネットワークにマルウェア(悪意のある不正なコード)が侵入するリスクが高くなる。そのため，マルウェアが侵入することを前提にした対策の必要性が高まっている。万が一，マルウェアが組織内ネットワークに侵入したとしても，可能な限り早い段階でその攻撃活動を検知し，攻撃が広がる前に適切に対処して被害を最小限に抑えることが重要である。この適切な対処の実現を目的として，筆者らは攻撃を見つけた後に被害の状況を迅速に分析する高速フォレンジック技術を開発した。

本稿では，これまで長い時間がかかっていたセキュリティ事故の分析が短時間で実現でき，被害が拡大する前に迅速に包括的な対策を講じることを可能とする高速フォレンジック技術について述べる。

Abstract

The number of targeted attacks aiming to steal information from government and municipal offices, specific enterprises, and individuals is growing year by year, and the attack methods are becoming more and more clever. In a targeted attack, the attacker stubbornly attacks the target after thoroughly investigating it beforehand. The risk of malware (malicious and illegal code) infecting an internal network is thus increasing. Therefore, there is a pressing need for countermeasures against malware infection that detect attack activity as soon as possible and respond effectively to prevent or minimize damage before the attack proceeds further. We have developed high-speed forensic technology that promptly analyzes the situation after an attack has been detected. Previously, such analysis took a long time. Application of this high-speed forensic technology enables inclusive countermeasures to be promptly implemented before the damage expands.

ま え が き

政府官公庁や，特定の企業，個人を狙った標的型攻撃では，ひとたび組織内ネットワークにマルウェア（悪意のある不正なコード）が侵入してしまうと，攻撃者はそのマルウェアを遠隔操作して感染を拡大させて，ネットワークや端末の情報を収集し目的の情報を探す。最悪の場合，機密情報や個人情報が組織外に流出し，標的となった組織やその組織の取引先に多大な損害を発生させてしまう。

多くの組織では，組織内ネットワークと組織外ネットワークとの境界にファイアーウォールやIPS（Intrusion Prevention System）などの侵入防御装置を設置し，また端末にアンチウイルスソフトウェアを導入するなどして，マルウェアが組織内に侵入するのを防いでいる。しかし攻撃者は，一般にファイアーウォールを通過するように設定しているHTTP（Hypertext Transfer Protocol）やSMTP（Simple Mail Transfer Protocol）などの通信経路を利用して，RAT（Remote Access Trojan/Remote Administration Tool）と呼ばれる遠隔操作型マルウェアを組織内ネットワークに送り込む。そして，人間の心理的な隙や行動のミスに付け込むソーシャルエンジニアリングと呼ばれる方法を使い，巧妙に感染させる。

攻撃者は，アンチウイルスソフトウェアなどの検知を回避したり，標的のネットワーク環境に対応させたりするカスタマイズを行ったRATを送り込むため，気付かれることなく諜報活動を開始できる。また諜報活動は，OS標準のコマンドを使うなど通常の業務に紛れて目立たないように行われる。このため，攻撃が進行した後に第三者の監視センターなど，外部の組織から通報を受けて初めて攻撃に気付くケースも多い。

これまでに，富士通研究所では標的型攻撃の被害を最小限に抑えることを目的として，RATによる諜報活動を早期に検知する技術を開発してきた。[(1), (2)] この技術では，組織内通信を収集・分析し，攻撃者とRAT感染端末間の遠隔操作通信と，感染端末から別の端末に侵入してコマンドやプログラムを実行する内部攻撃通信とを，それぞれの特徴から抽出してひも付けを行うことで諜報活動を検知する。[(3), (4)]

攻撃を検知した後の対処の一つとして，アメリカ国立標準技術研究所（NIST：National Institution of Standards and Technology）が作成したセキュリティ標準であるNIST SP800-61 Computer Security Incident Handling Guide[(5)]において，インシデントレスポンスのライフサイクルが示されている。これによると，攻撃が検知された後にはマルウェアの活動を封じ込め，諜報活動の根絶と組織内ネットワークの復旧を実施するための分析作業が必要である。早期に攻撃を検知し，更にこの分析フェーズを迅速に行って，被害が拡大する前に適切な対処を実施すれば，甚大な損害の発生を防止できる。そこで，筆者らは攻撃を見つけた後の被害の状況を迅速に分析する，高速フォレンジック技術を新たに開発した。この技術により，攻撃を受けた端末の範囲と各端末が受けた攻撃の内容を迅速に把握できる。

本稿では，従来の標的型攻撃分析方法と攻撃分析における技術課題について述べた後，高速フォレンジック技術の特長と効果について説明し，本技術を適用した統合分析システムについて紹介する。

従来の標的型攻撃分析方法

標的型攻撃の分析には，デジタルフォレンジックと呼ばれる方法が採られている。デジタルフォレンジックとは，攻撃者がネットワーク機器や端末に残した痕跡を解析する手段である。本章では，組織内ネットワーク諜報活動の分析における，一般的なデジタルフォレンジックの方法について説明する。

（1）不審な外部通信の分析

組織内ネットワークに潜入したRATは，HTTP/HTTPS（Hypertext Transfer Protocol Secure）などの通信経路を利用して，攻撃者が外部に設置したC2サーバ（Command and Control Server）に接続する。その後，攻撃者はC2サーバからRATに対して諜報活動の指令を出し，感染端末やその周辺のネットワークおよび端末の情報を収集し，感染を拡大させていく（**図-1**）。したがってインシデント対応者は，DNS（Domain Name System）サーバのログに不審な名前解決の問い合わせがないか，

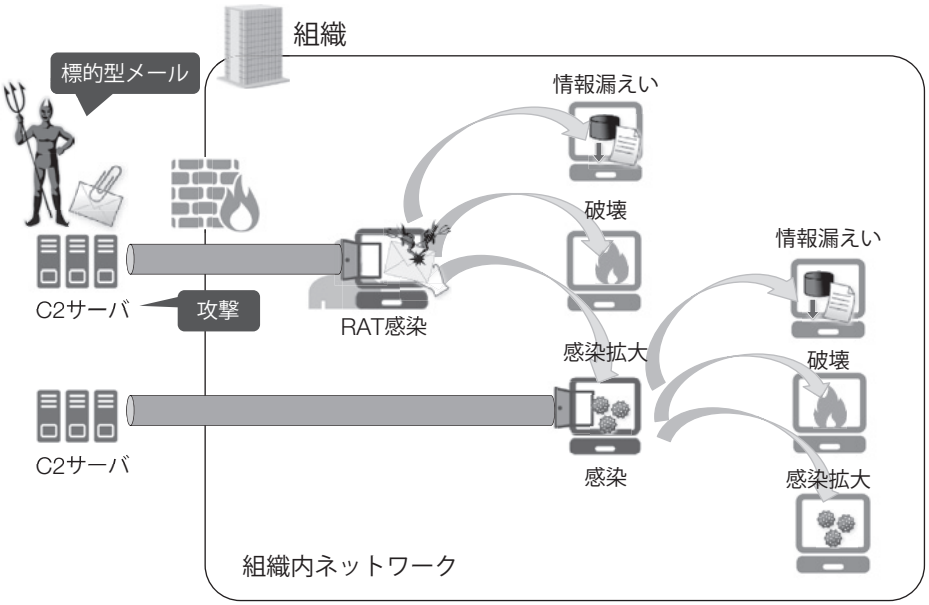

図-1　典型的な標的型攻撃

プロキシサーバのログに不審なURL，IPアドレス，ポート番号，ユーザーエージェント（User Agent）の通信がないかについて調査する。[6], [7]

（2）アカウントの不正利用の分析

OSは不正利用を防ぐために認証・認可の仕組みを備えている。攻撃者がOS標準のコマンドを実行する際や，攻撃者が送り込んだマルウェアを実行する際にもその認証・認可の機構が働いているため，実行にはアカウント名，パスワード，チケットなどの認証情報が求められる。したがって多くの場合，攻撃者はRATが装備しているキーロガー機能や，WCE（Windows Credentials Editor），mimikatzなどのセキュリティ検査ツールを利用して正規の認証情報を盗み，OS標準のコマンドやフリーツールを実行してネットワークや周囲の端末から情報を窃取している。このようなアカウントの不正利用の状況を調査するために，Active Directoryなどの認証サーバの監査用イベントログや,[8] Windows端末の監査用イベントログに残る認証の成功・失敗，特権の利用などの認証ログを分析する。

（3）攻撃手順と被害の範囲の分析

（1），（2）で述べた個々のログの調査では，断片的な情報しか把握できないため，攻撃の有無や詳細な調査が必要かどうかの判断はできても，攻撃の全貌を把握することは難しい。それを補うために，ハードディスクをコピーし，そのファイルシステムを解析することで，ファイルの復元や電子メール，Web閲覧，デバイス接続の履歴などの採取を行う。また，復元したマルウェアを解析して具体的に何を行ったのかを把握する。この方法では詳細な攻撃手順が把握できるが，セキュリティに関する高度な知識と技術を有する人材が必要不可欠である。更に，攻撃を受けた可能性がある端末の台数分解析を繰り返し行うため，攻撃の全貌を把握するまでに数週間から数か月の時間がかかる場合もある（**図-2**）。

攻撃分析における技術課題

組織内へ侵入したマルウェアによる攻撃の被害を明らかにするために，組織内ネットワークを流れる通信データを常時そのまま蓄積しておき分析する方法が考えられる。しかし，ネットワークを流れる通信量は膨大であり，大量の記憶媒体が必要となる。過去の事例から，標的型攻撃の検知から遡ると攻撃期間は約1年以内であることから，内閣サイバーセキュリティセンター（NISC）では，ログを1年以上保存することを推奨している。[9] これに従って，仮に全ての通信データを1年以上保存すると，数ペタバイトから数十ペタバイトのデータ蓄積量となる場合もあり，記憶媒体の確保や管理に多大なコストがかかることが予測される。加え

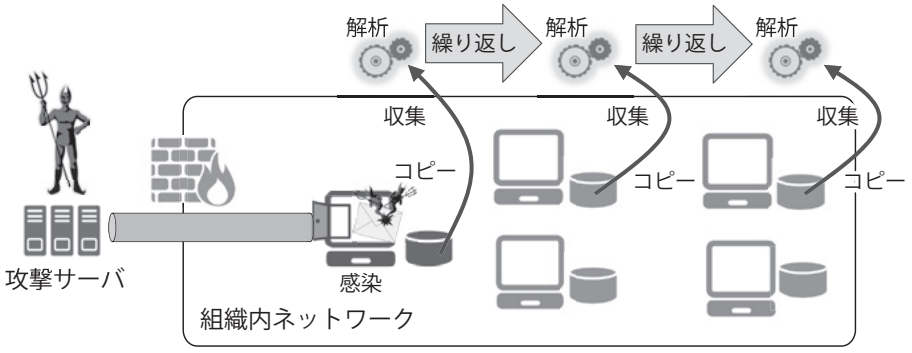

図-2　従来の攻撃分析方法

て，膨大な通信データの中から解析すべきデータの範囲を特定することも困難である。

また，上述した分析には様々なネットワークプロトコルの仕様に関する知識が必要である。このため，通信データから誰が何をしたのか（例：アカウントAがOSにログインした）という操作のレベルに読み解くことは容易ではなく，時間がかかる。更に，諜報活動において実行されるOSの標準コマンドやマルウェアの内部で利用されているプロトコルは，通常の業務で利用されるプロトコルと共通であるため，操作の通信を単体で見ても攻撃かどうかを判定できない。

高速フォレンジック技術の特長と効果

前章の技術課題を解決するため，リアルタイムにコマンドレベルで証跡を収集する技術，アカウントと操作を自動的にひも付けする技術，および攻撃進行状況をひも付けする技術から成る高速フォレンジック技術を開発した（**図-3**）。それぞれの技術の特長と効果を以下に述べる。

(1) リアルタイムのコマンドレベル証跡収集技術

ネットワーク中を流れる通信データを常時取得し，その通信データに含まれている内部攻撃通信に共通のプロトコルを解析する。通信データの基本単位であるパケットの特徴を判定し，端末で実行されたリモート操作コマンドを特定して，実行結果（成功・失敗）を付加して収集する。膨大な通信データをコマンドのレベルに要約して記録することにより，証跡ログのサイズの圧縮が可能となる。利用している通信データのプロトコル分布によるが，通信データを約1万分の1のサイズに圧縮して蓄積できる。

(2) アカウントと操作の自動ひも付け技術

通信データに含まれている認証プロトコルを解析し，アカウント名などの認証情報を特定する。そして，特定した認証情報がどのリモート操作コマンドの認証で利用されたかについて効率的にひも付ける。これにより，悪用されたアカウントの停止やパスワード変更など，的確で迅速な対処を検討できる。更に，そのアカウントの権限のレベルを把握することで，被害の範囲を適切に把握できる。

(3) 攻撃進行状況の抽出技術

RATによる遠隔操作によって，感染した端末から周囲の端末に対してリモート操作コマンドが実行されるという点が，標的型攻撃の最大の特徴である。このリモート操作に特徴的な動作の定義を基に，業務による正常な操作と攻撃の可能性の高い操作を識別して分析する。また，攻撃の可能性が高い通信を，操作の方向などの属性によってフィルタリングしながら時系列に連結して抽出する。1日分の通信に関する証跡ログの場合，特定の端末における一連のリモート操作コマンドを数秒から数十秒で分析できるため，数十分から数時間で攻撃全体の進行状況を抽出できる。

技術の適用例：統合分析システム

本章では，前章で説明した高速フォレンジック技術を搭載した統合分析システムについて紹介する。

統合分析システムは，攻撃証跡収集技術を搭載したネット証跡サーバと，攻撃進行状況抽出技術

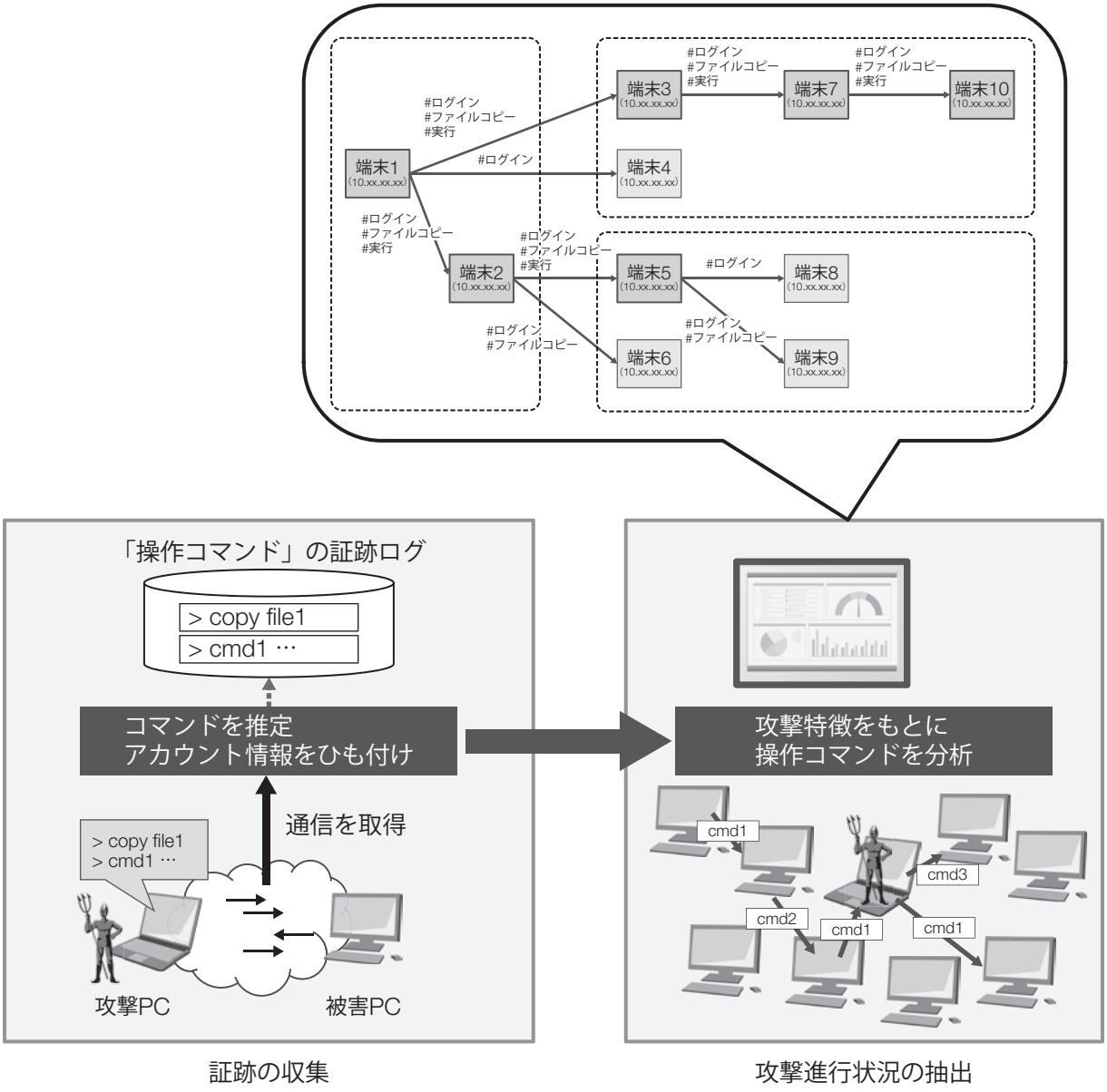

図-3　高速フォレンジック技術

を搭載した証跡分析サーバで構成される。**図-4**のシステム構成の場合，重要な情報が格納されている本社と各支店の間，および各支店間で攻撃者から遠隔操作によって実行される諜報活動の証跡を収集できるように，ネット証跡サーバを設置している。

例として，B支社の端末がRATに感染し，攻撃者に遠隔操作され本社の端末に諜報活動を行ったとする。図-4の例では，RATによる諜報活動を検知する技術を搭載したアプライアンスが，検知と同時に証跡分析サーバにインシデントを登録する。そのインシデントをトリガとして，セキュリティオペレーションセンター（SOC）の分析者は，何が起きたかのを確認するために，本統合分析システムの分析コンソールを利用する（**図-5**）。分析コンソールでは，インシデントに関連する証跡を特定でき，B支社の端末から本社端末に対して行われたリモート操作コマンドの内容を時系列で確認もできる。これにより，攻撃者が悪用したアカウント，リモートからアクセスしたファイルや変更した設定，またそれらが成功したのか失敗したのかなどの詳細な情報が得られる。

更に，攻撃の全貌を確認するために，攻撃を行ってきたB支社の端末を起点とし，通信が行われた端

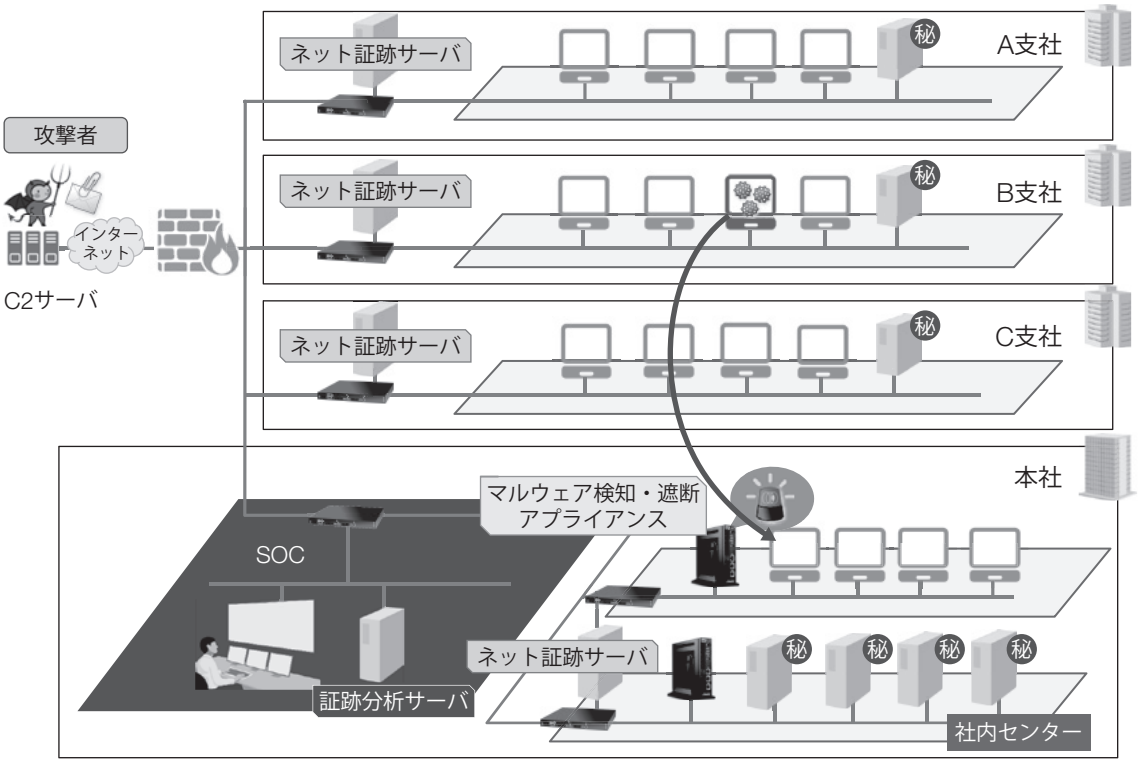

図-4　統合分析システムの構成

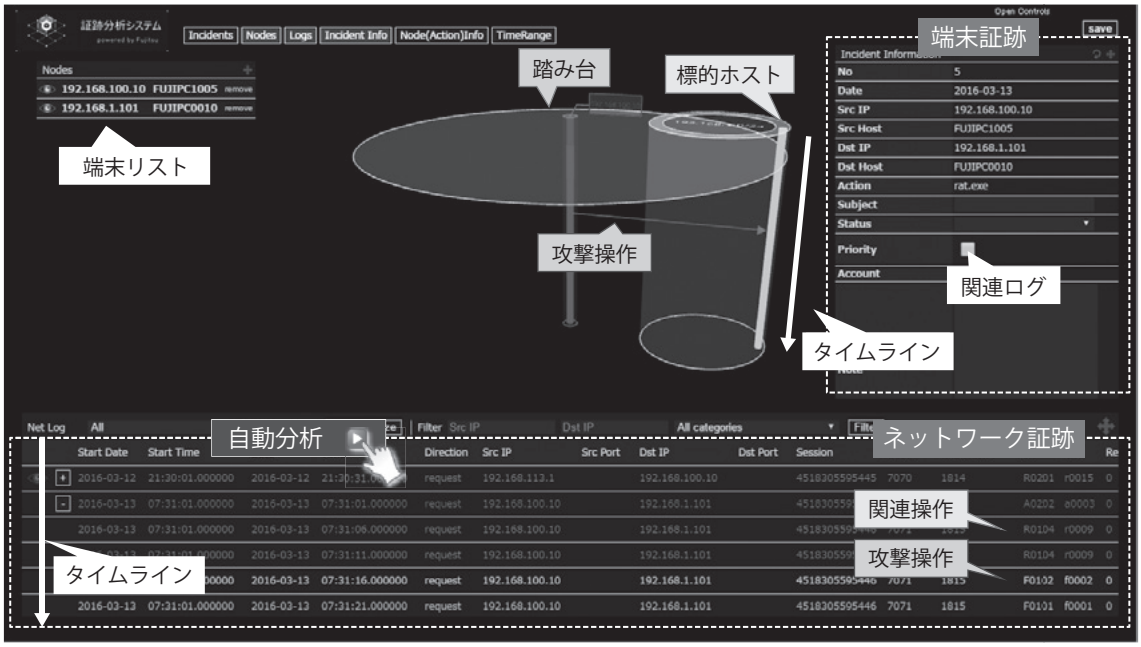

図-5　分析コンソール

末に対して同様の自動分析をすることで，本社の端末のほかに攻撃を受けた端末や，B支社の端末を攻撃した端末に関する証跡を特定する（**図-6**）。このように，起点とする端末を変更しながら同様の自動分析を再帰的に行うことで，攻撃の全体を分析する。これらの分析結果をノードグラフとして自動的に表示することで，攻撃全体を俯瞰できる（**図-7**）。

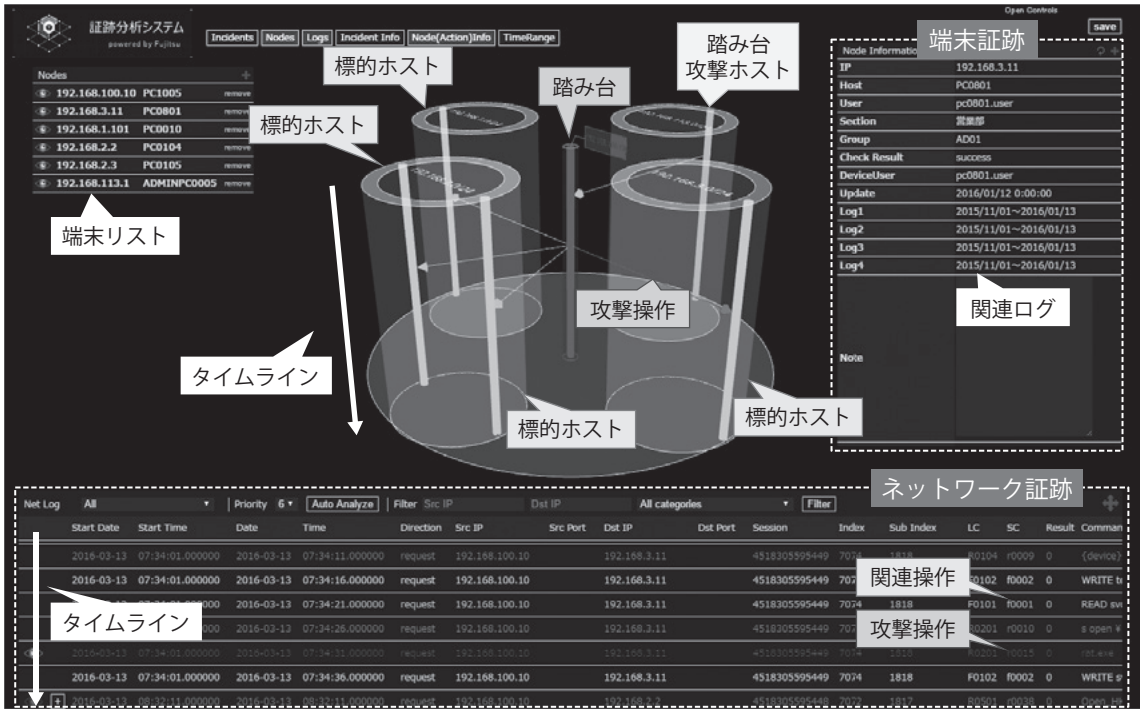

図-6　分析コンソール（自動分析後）

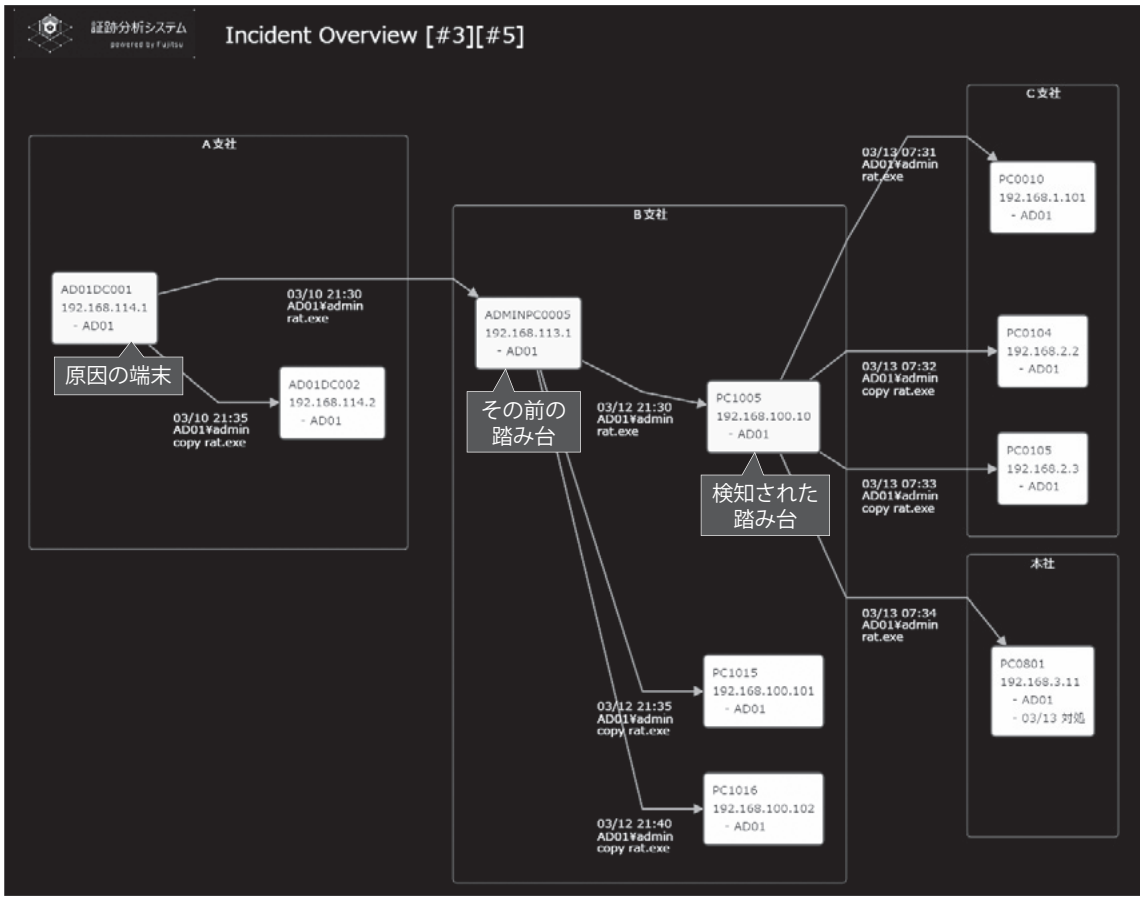

図-7　攻撃全貌図

本統合分析システムを利用することで，高度な知識を有する専門家でなくても分析コンソールでの攻撃内容の確認から攻撃全貌図の作成までを短時間で行うことができる。これにより，迅速かつ適切に対処を実施できる。

むすび

本稿では，富士通研究所が開発した世界初の高速フォレンジック技術とこの技術を搭載した統合分析システムについて説明した。

統合分析システムでは，証跡データのサイズを抑えながら，常時，証跡の収集と攻撃・被害の調査を実施できる。そして，標的型攻撃を検知した際に，攻撃に関係した端末を芋づる式に抽出し，攻撃の進行状況についての俯瞰図を自動的に描画することで，攻撃の全貌をひと目で把握できる。これにより，これまで長い時間がかかっていたセキュリティ事故の分析を，高度な知識を有する専門家でなくとも短時間で実現できるため，被害が拡大する前に迅速で包括的な対策を講じることが可能となる。この統合分析システムは，富士通社内での実証を経て，2017年度中の実用化を目指している。

参考文献

(1) 鳥居 悟ほか：特定の企業や個人を対象にしたサイバー攻撃対策技術. FUJITSU, Vol.64, No.5, p.516-522 (2013).
http://img.jp.fujitsu.com/downloads/jp/jmag/vol64-5/paper09.pdf

(2) 森永正信ほか：組織内通信・ログ分析によるサイバー攻撃対策技術. FUJITSU, Vol.67, No.1, p.63-68 (2016).
http://www.fujitsu.com/jp/documents/about/resources/publications/magazine/backnumber/vol67-1/paper10.pdf

(3) 山田正弘ほか：組織内ネットワークにおける標的型攻撃の諜報活動検知方式. 暗号と情報セキュリティシンポジウム（SCIS），2014.

(4) 山田正弘ほか：組織内ネットワークにおける標的型攻撃の振る舞い検知に向けた複数センサ連携手法. 暗号と情報セキュリティシンポジウム（SCIS），2015.

(5) P. Cichonski et al.：Computer Security Incident Handling Guide. National Institute of Standards and Technology, Special Publication 800-61 Revision 2, August 2012.

(6) 一般社団法人 JPCERTコーディネーションセンター：高度サイバー攻撃への対処におけるログの活用と分析方法 1.1版. 2016年10月19日.
https://www.jpcert.or.jp/research/APT-loganalysis_Report_20161019.pdf

(7) 満永拓邦：ログを活用した高度サイバー攻撃の早期発見と分析. 2015年.
https://www.jpcert.or.jp/research/APT-loganalysis_Presen_20151117.pdf

(8) B. Mathers：Best Practices for Securing Active Directory. Microsoft, February 2017.

(9) 内閣官房情報セキュリティセンター：平成23年度政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書. 平成24年3月.

著者紹介

海野由紀（うんの　ゆき）
セキュリティ研究所
ネットワークセキュリティ，サイバーセキュリティに関する研究開発に従事。

及川孝徳（おいかわ　たかのり）
セキュリティ研究所
サイバーセキュリティに関する研究開発に従事。

古川和快（ふるかわ　かずよし）
セキュリティ研究所
サイバーセキュリティに関する研究開発に従事。

森永正信（もりなが　まさのぶ）
セキュリティ研究所
サイバーセキュリティに関する研究開発に従事。

武仲正彦（たけなか　まさひこ）
セキュリティ研究所
情報セキュリティ，暗号実装，サイバーセキュリティの研究開発に従事。