組織内通信・ログ分析による サイバー攻撃対策技術

Cyber Attack Countermeasure Technology Using Analysis of Communication and Log in the Intranet

● 森永正信　● 野村祐士　● 古川和快　● 天満尚二

あらまし

サイバー攻撃の脅威は増加し続けており，大きな社会問題となっている。特に，標的型攻撃と呼ばれる特定の企業や個人を標的として情報窃取を行うことを目的としたサイバー攻撃は，より巧妙で執拗（しつよう）になってきている。ファイアーウォールやアンチウイルスソフトウェアなどの従来の「入口対策」や「エンドポイント対策」では，マルウェアの組織内部への侵入を完全に防ぐことはできない。

本稿では，標的型攻撃を組織内で検知し，その攻撃の影響範囲を特定する「内部対策」技術について紹介する。本技術は，組織内ネットワークを流れる大量のパケットを効率的に解析するための高速キャプチャー技術，組織内ネットワークに侵入したマルウェア通信のコンテキストの分析による攻撃検知技術，マルウェアの検知情報と周辺機器のログ情報の分析により攻撃の影響を検証する技術から成る。これらの技術を組み合わせることにより，標的型攻撃に対する高度な対策ソリューションを実現できる。

Abstract

The threat of cyber attacks is continuously on the increase and causing major social issues. In particular, cyber attacks intended for information theft by targeting specific corporations and individuals, which are called targeted attacks, are becoming increasingly clever and persistent. With conventional entrance and end point measures such as firewalls and antivirus software, it is not possible to completely prevent malware from intruding into organizations. This paper presents internal countermeasure technology that detects any targeted attack in an organization and identifies the extent of impact of the attack. This technology is composed of high-speed capture technology for efficiently analyzing a large number of packets that flow in the intranet, attack detection technology based on analysis of the context of malware communications that intruded into the intranet and technology for verifying the impact of the attack by analyzing malware detection information and peripheral device log information. An advanced countermeasure solution against targeted attacks can be realized by combining these technologies.

ま え が き

サイバー攻撃の脅威は増加し続けており，大きな社会問題となっている。特に，標的型攻撃と呼ばれる特定の企業や個人を標的として情報窃取を行うことを目的としたサイバー攻撃は，より巧妙で執拗になってきている。標的型攻撃は，複数の攻撃手法を組み合わせたステルス性の高い攻撃であることが多く，標的とする企業や個人に特化した攻撃を仕掛けてくる。そのため，ファイアーウォールやアンチウイルスソフトウェアなどの，従来の「入口対策」や「エンドポイント対策」では，マルウェアの組織内部への侵入を完全に防ぐことはできない。更に，一旦組織内部へ侵入したマルウェアは，感染拡大しながら不正アクセスを繰り返す諜報活動を開始するが，これらの対策では対処できない。そのため，マルウェアが侵入することを前提にした新たな「内部対策」が必要となる。内部対策は，内閣サイバーセキュリティセンター（NISC）の「政府機関の情報セキュリティ対策のための統一基準」[(1)]の中でもその重要性が示されており，できる限り早期に攻撃を検知して，被害を最小限度に抑えることが重要である。富士通では，攻撃の初期潜入から，侵入後の組織内ネットワークでの諜報活動という標的型攻撃の各進行段階を意識し，標的型攻撃の検知から対処まで総合的に対応している。

本稿では，巧妙な標的型攻撃への内部対策を実現する，組織内の通信とログの分析による新たなサイバー攻撃対策技術について紹介する。まず，分析する情報の基となる組織内ネットワークを流れる大量のパケットを効率的に収集する高速キャプチャー技術について述べる。次に，収集情報から組織内ネットワークに侵入したマルウェア通信のコンテキストを抽出する攻撃検知技術について述べ，最後に，マルウェアの検知情報と周辺機器のログ情報の分析により攻撃の影響を検証する技術を紹介する。

組織内通信を監視するためのキャプチャー技術

パケットキャプチャーとは，サーバ・クライアント・ネットワークの種類に依存せず負荷も与えない，という優れた特長を持つデータ収集技術である。本章では，マルウェア通信を分析するパケットキャプチャー技術について述べる。

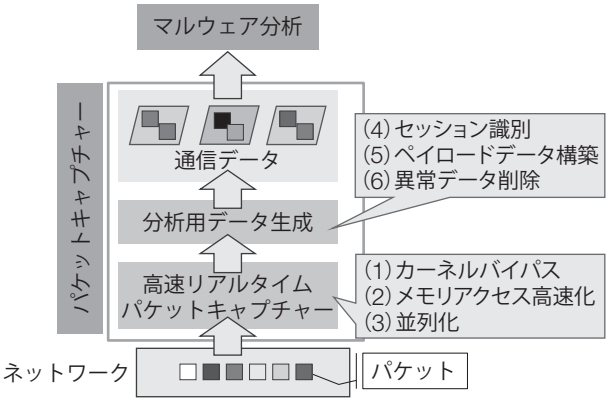

図-1　パケットデータの収集基盤

● パケットキャプチャーにおける課題

通信パケットはデータ量が多く，ソフトウェアで全てを処理しようとするとCPUの処理負荷が高いという問題がある。また，従来の汎用ハードウェア上のソフトウェア処理では全データの一部しか処理ができず，全データが必要なマルウェア通信の分析には利用が難しかった。加えて，パケットキャプチャーにCPUやメモリリソースを多く使うと，マルウェア通信の分析に必要なリソースが不足するという問題も生じるため，マルウェア分析用に適したデータのみを提供する必要があった。

● 高速リアルタイムパケットキャプチャー技術

富士通研究所では，これまでに汎用ハードウェア1台で200 Gbpsの通信パケットをリアルタイムに解析できる技術を開発した[(2)]。この技術をマルウェア分析のパケットデータ収集基盤として活用している（**図-1**）。

従来のlibpcapインターフェース[(注)]は，汎用ハードウェア上でのパケットキャプチャーに広く活用されているが，キャプチャー性能が低いという問題があった。これを解決するために以下の三つの技術を開発し，低負荷でパケットを受信できるようになった。

(1) 処理負荷の高いOSカーネルレベルのTCP/IPパケット受信処理をバイパスするパケット受信高速化処理

(注)　通信パケットをキャプチャーするための標準的なAPI（Application Programming Interface）。

(2) 不要なパケットデータコピーを防ぐメモリアクセス高速化
(3) 複数のCPUコアを効果的に活用できる並列化

● **分析用データ生成機能**

前述のlibpcapインターフェースのように，パケットを時系列順にキャプチャーする機能だけではマルウェア分析に必要十分なデータのみを抽出できない。そこで，以下の三つの機能を開発した。

(4) パケットヘッダーをデコードし，通信セッションを識別
(5) マルウェア通信の分析機能には，パケットのペイロードなど必要なデータのみを提供するデータ構築
(6) パケットロスや不通などの通信異常を発見し，異常データを削除

● **効果**

以上の技術と機能により，低負荷でパケットをキャプチャーするだけでなく，マルウェア分析機能からは通信パケットを意識した分析ロジックやデータアクセスも不要になる。これにより，パケットキャプチャーおよびデータ生成性能が向上するとともに，稼働する汎用ハードウェアの小型・省リソース化にも寄与している。

マルウェア通信を分析・検知する技術

標的型のサイバー攻撃では，RAT（Remote Access Trojan/Remote Administration Tool）と呼ばれる遠隔操作型のマルウェアが利用される。攻撃者は，標的型攻撃メールなどの方法を用いて，標的とする組織内のホストコンピュータ（以下，端末）をRATに感染させる。更に，この端末を踏み台として組織内の別の端末に侵入し，コマンドやプログラムを実行することで情報を盗む諜報活動を繰り返す。本章では，このようなRATの諜報活動を，組織内通信の関係性から検知する技術について紹介する。

● **解決すべき技術課題**

諜報活動における通信は，攻撃者と踏み台端末間のRATによる遠隔操作の通信（RAT通信）と，踏み台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通信（内部攻撃通信）に分けられる。RAT通信は，通常のWebアクセスに偽装した暗号化通信で行われることが多いため，このRAT通信を高い精度で検知することは難しい。また，組織内での別の端末へ侵入するために行われる内部攻撃通信も，一般的に利用される管理ツールやコマンドを悪用することが多い。このため従来の技術では，正規の管理者の操作とRATによる諜報活動との判別が困難であった。

● **組織内でのRAT活動検知技術**

富士通研究所では，組織内通信を収集・分析し，RAT通信と内部攻撃通信をそれぞれの特徴から抽出してひも付けることにより，諜報活動を検知する方式を開発した。[3]

RATの遠隔操作では，踏み台端末が攻撃者からの指示を待ち受けて，指示が来ると即座に応答して結果を返すという特徴がある。更に，いつでも指令を受け付けられるように，一度構築した通信コネクションを維持するという特徴がある。これらの特徴を利用することで，通常のWebアクセスからRAT通信の候補を絞り込める。

また，内部攻撃通信では，業務での操作を装うために，Windows標準の管理サービスが悪用されることが多い。このようなサービスでは，SMB（Server Message Block）プロトコルが利用される。SMBパケットのヘッダー情報を用いて，アクセスするユーザーの権限や操作内容を解析することで，ファイル共有やネットワーク探索などの業務通信から，攻撃の可能性がある管理操作の通信を絞り込める。更に，抽出したRAT通信と内部攻撃通信の候補を，IPアドレスや時間的な関連性に基づいてひも付けることで，RATの遠隔操作と関連するSMBの管理操作を諜報活動として検知する。

● **複数センサーの連携による検知範囲向上**

実際のネットワークでは，セグメントをまたぐ諜報活動に対して，1台の監視センサーでRAT通信と内部通信の両方が観測できない場合がある。富士通研究所は，ネットワーク内に複数配備した監視センサーがそれぞれRAT通信と内部攻撃通信を抽出し，連携サーバに情報を収集してひも付けることで，監視センサーの検知範囲を拡大する連携検知技術を開発した（**図-2**）。[4]

連携検知技術では，ネットワークの出入口と監視対象のセグメントに監視センサーを設置し，各監視センサーは候補となる通信の情報をサーバに送信する。サーバは，監視センサーから受信した

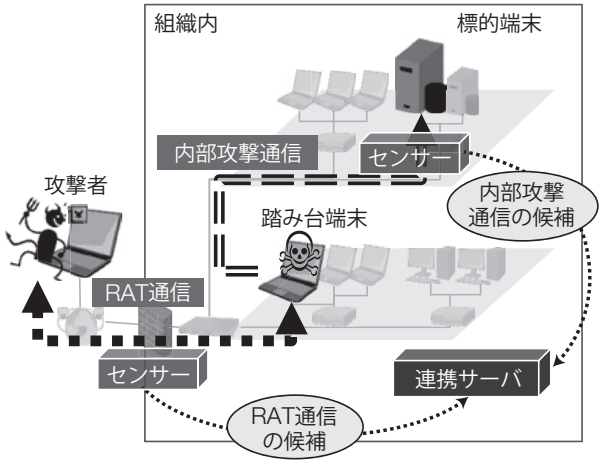

図-2　RATによる諜報活動の検知技術

情報を分析し，必要に応じて別の監視センサーに追加の情報を問い合わせる。このようなインタラクティブな協調によって，監視センサーを配置したセグメントに対する諜報活動を網羅的，かつリアルタイムに検知する。

● **効果**

開発した検知技術を用いることで，入口対策やエンドポイント対策を擦り抜けて組織内に侵入したRATの諜報活動を検知し，攻撃の被害が深刻になる前の対処が期待できる。

マルウェアの影響を特定する技術

前章で述べたように，標的型サイバー攻撃は組織内のマルウェアに感染した端末を踏み台として，別の端末/サーバに諜報活動を繰り返し，被害を拡大させる。標的型サイバー攻撃は，最初のマルウェア感染から被害発覚まで平均205日[(5)]であり，その間に非常に多くの端末/サーバに蔓延（まんえん）し，様々な重要情報が窃取されると言われている。

サイバー攻撃を受けたことが発覚した組織は，組織内の被害の全容を明らかにし，対処する必要がある。これには，セキュリティ専門家によるサービスを利用することが一般的であるが，調査には時間がかかり，その間の業務停止を余儀なくされる。一方で，あらかじめ全ての端末にエージェントソフトウェアをインストールすることで端末の詳細な情報を把握し，被害発覚時に短期間で調査が可能となる新しい製品が発売されている。しかし，こういった製品では被害発覚時の調査期間を短縮できる代わりに，全端末の管理が必須であり，平常時に大きな運用リソースが必要となる。

本章では，このような標的型サイバー攻撃の被害検証において，セキュリティ専門家と同等の調査を自動的に処理し，組織内に残る影響の特定を高速に実現する全く新しい対処技術を紹介する。

● **通常の標的型サイバー攻撃被害の調査**

一般に標的型サイバー攻撃検知技術は，感染した端末の検知のみが可能であり，その先の諜報活動の標的となった端末/サーバについては調査できない。このため，セキュリティ専門家による被害調査ではまず感染端末を特定し，そこから諜報活動対象の標的や，更にその先の標的を繰り返し調査する。また，このときの端末の調査では，マルウェアのスキャン，ファイルやレジストリー，ログなどに残された痕跡の調査，見つかったマルウェア検体の静的・動的検証などにより，その端末で何が起きたかを検証する。そのため，このような専門家による作業は，半年から1年ほどかかると言われている。こうしたことから，現状では大きな事件でもない限りこのような調査が行われることは少なく，感染した端末の初期化のみの対処を行い，感染再発を繰り返していた。

● **マルウェアの影響を特定する技術**

開発した技術は，端末で動作するエージェントを使用せず，セキュリティ専門家と同様の調査を自動で行うことが特長である。これを実現するために，情報の収集と分析の二つのフェーズでの効率化技術を開発した。収集フェーズでは，調査に必要な情報を極小化する。専門家の調査では，マルウェアの分類や振舞いなどの対処に不要な情報の収集も行っている。そこで，マルウェアのプロセスやそれがアクセスしたファイルなどの対処に必要不可欠な情報に絞って収集する。

分析フェーズでは，感染した端末のアドレス以外の情報を活用して高精度な分析を実施する。前章の技術では，マルウェア通信を分析するため，感染した端末のアドレス以外に悪用されたアカウントやツール名が取得可能である。これをキーに収集した情報を分析することで，高精度で諜報活動対象の標的を特定できる。調査に必要な情報は，Windows標準の機能などを使ったリモート収集が可能である。そのため，これらの技術を利

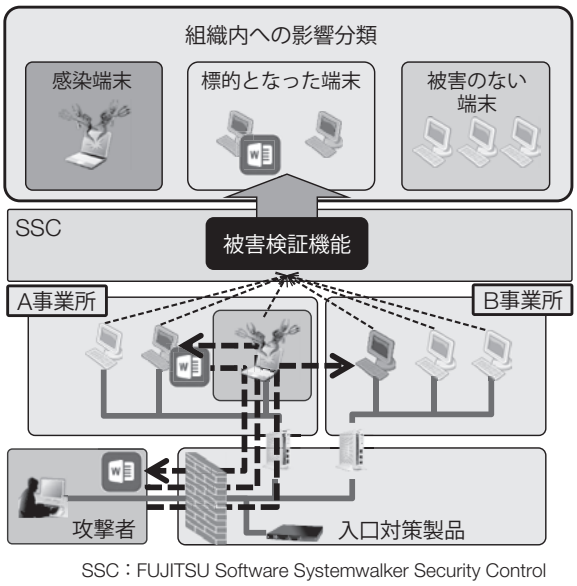

図-3　影響特定機能

用した影響特定機能は，感染端末を起点とする組織内へのサイバー攻撃の影響調査を自動化できる（**図-3**）。

● **効果**

開発した技術を適用することで，全ての端末へのエージェントソフトの導入が不要となり，被害発覚時に組織内に残る影響の特定をセキュリティ専門家による調査と同等のレベルで高速に実現できる。筆者らの試算では，影響特定までに半年以上必要であった調査期間を数時間から数日程度に短縮可能であり，これまで不可能であった感染した端末から先の諜報活動の標的になった端末にも対処できる。

む　す　び

本稿では，標的型攻撃を組織内で検知し，その攻撃の影響範囲を特定する内部対策技術として，富士通が開発した高速キャプチャー，攻撃検知，影響検証の各技術を紹介した。これらの技術を組み合わせることで，組織内ネットワークを流れる膨大なパケットを漏らさず解析し，攻撃の早期段階で被害範囲や情報流出の証跡を確実に検証する高度な対策ソリューションを実現できる。

本研究の一部は，総務省委託研究「サイバー攻撃解析・検知に関する研究開発」により実施したものである。

参考文献

(1) 内閣サイバーセキュリティセンター：政府機関の情報セキュリティ対策のための統一基準(平成26年度版). http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf
(2) 野村祐士ほか：200 Gbpsの超高速通信をリアルタイムにソフトウェアで解析する技術．FUJITSU, Vol.66，No.5，p.41-45（2015）. http://img.jp.fujitsu.com/downloads/jp/jmag/vol66-5/paper06.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（SICS），2015.
(5) FireEye：M-Trends® 2015：A View from the Front Lines，March，2015. https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html

著者紹介

森永正信（もりなが　まさのぶ）
知識情報処理研究所
サイバー・システムセキュリティプロジェクト 所属
現在，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）
知識情報処理研究所
サイバー・システムセキュリティプロジェクト 所属
現在，サイバーセキュリティに関する研究開発に従事。

野村祐士（のむら　ゆうじ）
ソフトウェア研究所
運用管理ソフトウェアプロジェクト 所属
現在，ICTシステムの運用管理に関する研究開発に従事。

天満尚二（てんま　しょうじ）
データセンタプラットフォーム事業本部 所属
現在，NFV方式，ネットワークセキュリティ，IoTの研究開発に従事。