脅威分析に基づいたプロアクティブな防御モデル

Proactive Defense Model Based on Cyber Threat Analysis

● 大迫剛史　● 鈴木智良　● 岩田洋一

あらまし

サイバー攻撃対策として，多層防御とともに，インシデント発生時の対応組織「CSIRT（Computer Security Incident Response Team）」が設置されてきているが，対策を講じたとしても，防御できずに被害を受けるケースが日々増加している。更なる防御の強化のためには，攻撃を受けた後に行うリアクティブな防御に加えて攻撃を緻密に分析して行うプロアクティブ（先回り）な防御に転じていく段階にきている。同じ攻撃者による攻撃には，特有の癖があると考えられる。この癖を「脅威情報」とし，様々な攻撃の予兆や痕跡から脅威情報を抽出することを「脅威分析」と定義する。これらの定義に基づいたプロアクティブな防御モデルの確立は，従来のセキュリティ対策では検出・防御が困難であり，近年増加している標的とする組織に合わせたカスタムメイドの攻撃検知に有用であると考えられる。

本稿では，マルウェア分析などの脅威分析手法や脅威情報の標準化，および脅威情報を活用することで，将来のサイバー攻撃に対してプロアクティブに防御を実現するモデルを紹介する。

Abstract

As a measure against cyber attacks, enterprises are establishing computer security incident response teams (CSIRTs) and ensuring they have defense in depth. Even these measures, however, may not be sufficient for perfect defending against attacks and the number of cases of damage is increasing day by day. It has reached the stage where, to further strengthen protection, it is necessary to carry out reactive defense after being attacked but also proactive defense to closely analyze attacks. Attacks by the same adversary are considered to show certain peculiarities. They are seen as features of attacks, which are defined as "Cyber Threat Intelligence," and extracting this Cyber Threat Intelligence out of various signs and traces of attacks is defined as "Cyber Threat Analysis." Establishing a proactive defense model based on these definitions seems to be useful to detect attacks that target a specific organization, which have been increasing in recent years and are difficult to detect and defend against with existing security measures. This paper describes the standardization of Cyber Threat Analysis techniques including malware analysis and how to express Cyber Threat Intelligence. It also describes a model that realizes proactive defense against future cyber attacks by utilizing Cyber Threat Intelligence.

ま え が き

2014年，日本では「サイバーセキュリティ基本法」[(1)]が成立した。本法律には，サイバーセキュリティ戦略本部の設置や，国内セキュリティ産業の発展を推進する点などが明記されており，サイバー空間におけるセキュリティ対策がますます重要視されている。

近年，サイバー攻撃のレベルは高度化し，密かに行われるとともに，ターゲット領域の拡大や，インシデント（攻撃によりサーバやパソコンが侵害される事象）の発生件数も増加している。そのため，企業や組織は侵入されないような対応から，侵入を前提とした対応へと移行せざるを得ない状況となってきている。たとえ侵入されたとしても，影響範囲を局所的にして，被害を拡大させないことが重要である。これには，隔離環境でファイルを動作させて不審な挙動を検知するサンドボックスなどの新しい技術を用いた多層防御を行うとともに，インシデント発生時の対応組織「CSIRT（Computer Security Incident Response Team）」の設置が一般的に有用である。

しかし，こうした対策を講じたとしても，防御しきれずに情報漏えいなどの被害が発生している。[(2)] この背景には，APT（Advanced Persistent Threat）攻撃と呼ばれる，攻撃者が標的組織や世間の対策状況に関する情報を収集し，緻密な戦略のもとにカスタムメイドの攻撃を繰り返し行うようになってきたことが理由として挙げられる。そこで富士通は，APT攻撃を分析し，その攻撃の背景や，インフラ，手法などの情報を認知することで，新たな対策を講じていく段階にきていると判断し，このような対策に向けた取組みを開始している。

本稿では，攻撃の目的，インフラ，手法，ツールなどを分析し，そこから得られる攻撃の特徴を利用して，プロアクティブ（先回り）な防御を実現するモデルについて紹介する。

APT攻撃への対策と課題

APT攻撃の特徴を，攻撃フェーズごとに整理する。各攻撃フェーズにおける代表的な攻撃と対策を**表-1**にまとめる。[(3)] 各攻撃フェーズは以下のとおりである。

・攻撃準備：標的とした組織に侵入するための攻撃環境を構築する。
・初期潜入：標的型攻撃メールなどにより，組織内のパソコンを感染させる。
・基盤構築：C2サーバ（コマンド＆コントロールサーバ）との通信を開始し，内部ネットワークやサーバの情報を収集する。
・内部侵入・調査：侵害範囲を拡大し，目的のサーバや情報に近づいていく。
・目的遂行：重要情報の窃取や重要システムの破壊などの目的を遂行する。

このような各攻撃フェーズに対して行われる代表的な対策は一定の効果を示しているが，それらを回避する攻撃手法は既に確認されている。APT攻撃への代表的な対策と確認した最新の攻撃手法を，以下に紹介する。

（1）多種多様な標的型メール

・対策1：標的型メール訓練

代表的な攻撃手法である標的型メールに対する訓練を実施し，社員の標的型メールに対する判断能力を向上させる。

・回避する最新の攻撃手法：やり取り型標的メール

標的組織のお客様相談窓口に対して，客を装い何度かメールのやり取りをした後，マルウェアを添付したメールを送信し，感染させる。

表-1　攻撃フェーズと対策

攻撃フェーズ	攻撃準備	初期潜入	基盤構築	内部侵入・調査	目的遂行
代表的な攻撃	標的型メール C2サーバ	マルウェア感染	バックドア NW環境の調査探索	端末間侵害 サーバ侵入	データ窃取 データ破壊
代表的な対策	対策1. 標的型メール訓練	対策2. サンドボックス	対策3. 不正外部通信対策 対策4. 認証プロキシ		

(2) マルウェアの高度化
・対策2：サンドボックス
　不審な実行ファイルやドキュメントファイルなどの挙動をサンドボックス技術で自動分析し，マルウェアを検知する。
・回避する最新の攻撃手法：サンドボックス検知
　サンドボックス製品で利用される仮想環境をマルウェアが検知し，そのような環境下では不審な挙動を示さず，正常なファイルであるかのように振る舞う。
(3) 不正外部通信の秘匿化
・対策3：不正外部通信対策
　外部への通信を監視し，不審な振舞いの通信を検知・遮断する。
・回避する最新の攻撃手法：通信暗号化
　マルウェアが外部への通信に暗号化通信を使用することで，通信の特徴を検出させない。
(4) 認証プロキシ対応
・対策4：認証プロキシ対策
　認証プロキシサーバの導入により，マルウェアに感染した機器からC2サーバへの通信を遮断する。C2サーバへの通信を遮断することで，攻撃者によるリモート操作や情報漏えいから防御する。
・回避する最新の攻撃手法：認証情報盗聴
　マルウェアが認証プロキシサーバの認証情報を盗聴し，その情報を使用して認証プロキシサーバ経由でC2サーバと通信する。
　このように，攻撃者は様々な手法を用いて対策を回避し，侵入・遠隔操作を経て，標的に甚大な被害を与える。目に見える攻撃への対策のみにコストや運用負荷をかけたとしても，効果は一時的なものであり，すぐに回避され被害を受けてしまうことになる。したがって，今後は目に見えない攻撃や攻撃者の行動を推測する対策が重要になると考えている。

脅威分析と脅威情報

　APT攻撃は，明確な目的を持って繰り返される。富士通では，同じ攻撃者により繰り返される攻撃には，攻撃者の癖があると考えている。攻撃の予兆や痕跡を分析することで，以下のような攻撃者の癖を把握できる。
・攻撃インフラの特徴
・攻撃ツール（マルウェア）の特徴
・攻撃手法の特徴
・攻撃の目的
　攻撃に関するこのような情報を「脅威情報」とし，予兆や痕跡から脅威情報を抽出することを「脅威分析」と定義する。
　富士通は，脅威情報を活用することで，今は目に見えていないほかの攻撃を発見したり，将来発生する可能性のある攻撃を予測したりできるため，攻撃者の行動を推測したプロアクティブな防御が可能になると考える（**図-1**）。
　本章では，いくつかの脅威分析手法と，得られる脅威情報の詳細について述べる。

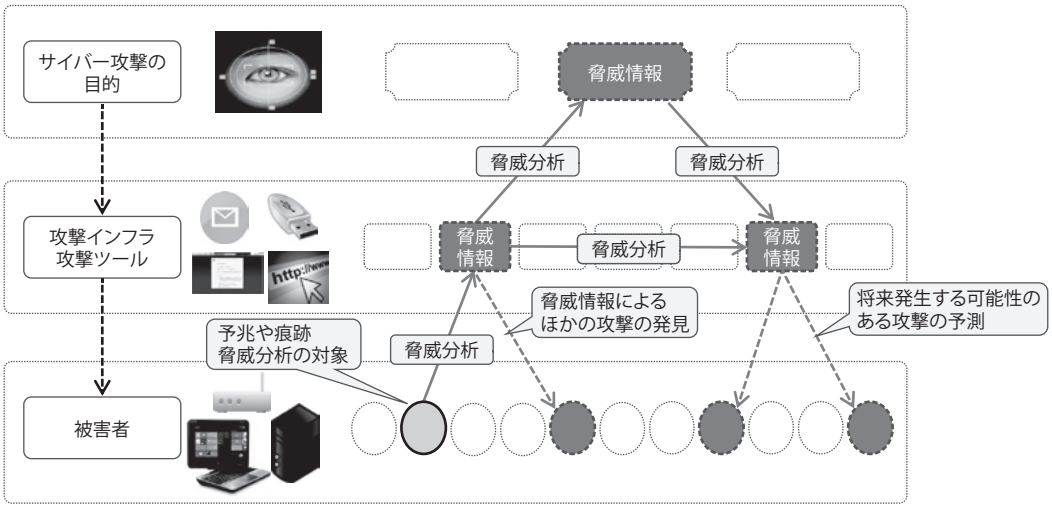

図-1　脅威分析と脅威情報によるプロアクティブ防御

● 攻撃チャネル分析

攻撃者がリモート操作するために，標的組織内の端末にマルウェアを感染させる手法を攻撃チャネルと定義する。以下に例を挙げて，具体的な攻撃チャネルの分析手法を紹介する。

標的としている組織の端末をマルウェアに感染させるために送信される標的型メールが，本分析の対象となる。標的型メールの場合，メールヘッダー情報，本文，添付ファイルを分析する必要がある。この分析によって，以下の脅威情報を抽出できる。

・メール送信元アドレス
・メール送信サーバのホスト名やIPアドレス
・メール件名
・添付されているファイル名
・添付されているファイルの種類

標的としている組織が日常利用しているWebサイトを攻撃者が改ざんし，マルウェアに感染させる「水のみ場攻撃」といった手法も本分析の対象となる。

● マルウェア分析

本分析手法は，攻撃者から送り込まれたマルウェアを主に以下の三つの手順で分析する。

(1) 表層分析

マルウェアを動作させずに，そのファイルの種類やファイル名，バイナリデータ内の文字列などの情報を分析する。

(2) 動的分析

マルウェアを動作させ，その挙動を分析する。分析する対象は，主にファイル操作，レジストリー操作，プロセス，通信の四つである。

(3) 静的分析

マルウェアをリバースエンジニアリング（コンパイル済みのバイナリデータからソースコードを復元すること）し，ソースコードを分析する。ソースコードの分析によって詳細な動作まで明らかにできる。

マルウェア分析を行うことによって，以下の脅威情報を抽出できる。

・マルウェアのファイル名
・マルウェアのハッシュ値
・マルウェアが作成するファイル
・マルウェアが作成するレジストリー
・マルウェアが起動するプロセス
・マルウェアが通信するC2サーバのドメイン名，IPアドレス
・マルウェアが通信するC2サーバとの通信内容の特徴（プロトコル，ヘッダー情報など）
・マルウェアが悪用する脆弱性
・マルウェアの機能（キーロガー，リモートコマンドの実行など）

● C2分析

本分析手法は，以下のような観点でC2サーバに関する分析を行う。

(1) whois情報（IPアドレスやドメイン名の利用者情報）

C2サーバのドメイン名やIPアドレスなどのwhois情報を調べ，同じwhois情報で管理されているサーバを抽出する。これらのサーバも，同じ攻撃者が利用しているC2サーバの可能性がある。

(2) 地域情報

C2サーバの地域情報に関して分析する。C2サーバは，攻撃者が踏み台として設置している場合が多く，攻撃者が頻繁に利用する踏み台には地域性が傾向として表れる。

(3) C2サーバのドメイン名，IPアドレス（パッシブDNS分析により新たに発見した情報）

攻撃者はC2サーバを頻繁に変更することで追跡を回避するため，IPアドレスではなくドメイン名でアクセスさせようとする。仮に，一つのC2サーバのドメイン名情報を入手した場合，このドメイン名に関するDNSサーバへの問合せ結果を継続的にモニタリング・分析することで，攻撃者が乗り換えていく先のC2サーバに関する情報（IPアドレスなど）が得られる。

● 攻撃キャンペーン分析

個々の痕跡やインシデントを分析して抽出した脅威情報から，共通値を持つ痕跡やインシデントをグルーピングする。グルーピングした個々の痕跡やインシデントが数多く確認された場合，このグループを一つの攻撃キャンペーンと定義する。攻撃キャンペーンに含まれている個々の痕跡やインシデントは，同じ攻撃者の同じ目的に沿った攻撃によって発生しているものと判断できる。攻撃キャンペーンを認知できた場合，その個々の痕跡から抽出された脅威情報は，今後行われる可能性

のある攻撃を防御するために有用である。

脅威情報の標準化

脅威情報は，攻撃の検知・防御のために，非常に有用な情報であると考えられる。これらの脅威情報を，セキュリティシステム間や組織間で機械的かつリアルタイムに近いスピードで効率的に交換するためには，情報交換のための共通仕様が必要であり，近年様々な仕様が公開されている。本章では，MITRE社が提唱しているCybOX,[4] STIX,[5] TAXII[6]について紹介する。

（1）CybOX（Cyber Observable eXpression）

観測した事象を表すためのフォーマット仕様である。例えば，マルウェアのファイル名や起動されたプロセス，C2サーバのIPアドレスなどに関する脅威情報のフォーマット仕様が，XML形式で定義される。

（2）STIX（Structured Threat Information eXpression）

脅威情報を5W1Hで表すためのフォーマット仕様である。以下の八つの情報から構成され，XML形式で定義されている。

・サイバー攻撃活動（Campaigns）
・攻撃者（Threat Actors）
・攻撃手口（TTPs：Tactics, Techniques and Procedures）
・検知指標（Indicators）
・観測事象（Observables）
・インシデント（Incidents）
・対処措置（Courses Of Action）
・攻撃対象（Exploit Targets）

（3）TAXII（Trusted Automated eXchange of Indicator Information）

脅威情報を交換するための送受信に関するプロトコル（脅威情報を交換するための乗り物）である。CybOXやSTIXで記述された脅威情報の交換をプログラム処理で可能とする。

MITRE社では，これらの標準仕様をサポートする脅威情報の分析・蓄積・共有ができるシステム基盤として，CRITs（Collaborative Research Into Threats）[7]をオープンソースで公開している。CRITsを検証・評価した結果，以下の点において非常に有用であることが分かった。

・脅威分析のための様々な自動分析ツールをサポート
・マルウェアの情報や脅威情報をキーとして，蓄積されている情報から関連する情報の洗い出しが可能であり，この機能によりキャンペーン分析が容易
・CybOX，STIX，TAXIIを使用した脅威情報の交換をサポート

プロアクティブ防御モデル

本章では，APT攻撃に対して，富士通が取り組んでいる脅威情報を活用したプロアクティブな検知・防御を可能とするモデルについて述べる。

最初に，各種センサーやログにより検知された攻撃イベントに関して，痕跡を自動的に保管する。次に，保管された痕跡に対して脅威分析を行い，脅威情報の抽出や蓄積，各種センサーやSIEM（Security Information and Event Management）に対する脅威情報の配信，インシデント発生端末のネットワーク切断などの対処を行う。これらを実現するモデルの概要を**図-2**に示す。各構成要素の定義や機能は，以下のとおりである。

（1）SIEM

各種セキュリティセンサーからのイベントや情報システムの各種ログを集約し，特定のルールや脅威情報に基づいて，インシデントが発生しているかどうかを判定する。

（2）インシデント管理

インシデントの優先度や状況，必要なタスクをチケットとして管理する。

（3）痕跡保管

発生したインシデントに関する痕跡（不審なファイルやログ，メモリダンプなど）を保管する。保管した痕跡は，自動分析や脅威分析において使用される。

（4）自動化エンジン

以下の三つの機能を有する。

・分析

検知したイベントや痕跡に対して自動的に分析する。具体的にはサンドボックスによるマルウェア分析や，蓄積されている脅威情報とのマッチング検索などが該当する。

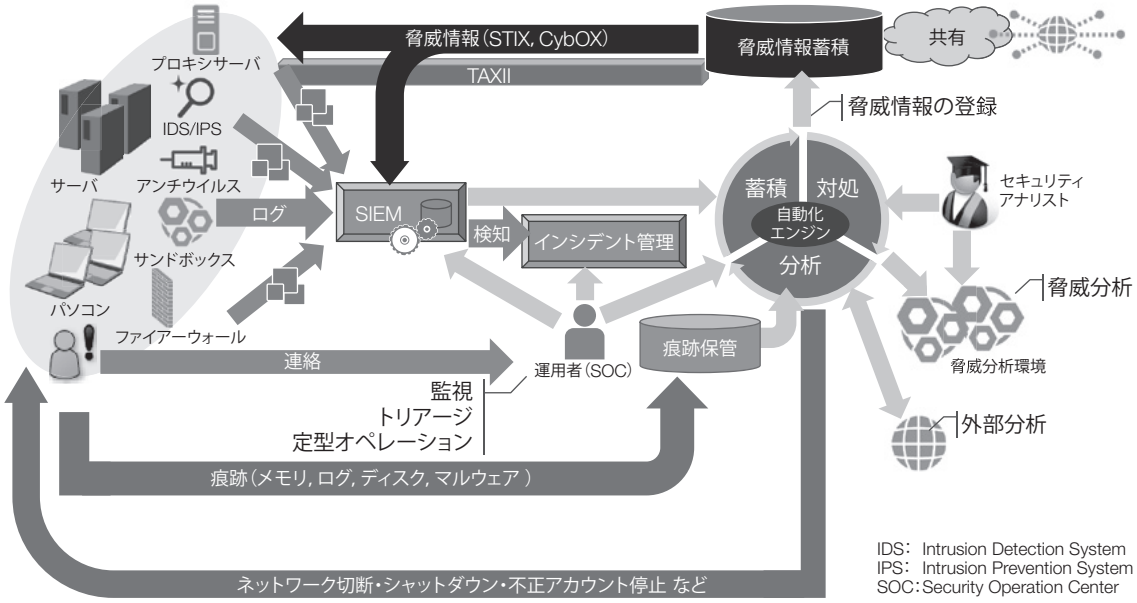

図-2　脅威分析と脅威情報によるプロアクティブ防御モデル

・対処

自動分析の結果や蓄積されている脅威情報に基づいて，対処する。具体的には，脅威情報を各セキュリティセンサーやSIEMへ自動的に配信・適用する。

・蓄積

分析の結果抽出された脅威情報を自動的に蓄積する。

（5）脅威情報蓄積環境

CybOXやSTIX, TAXIIをサポートし，各種セキュリティセンサーや他組織間との共有機能を提供する。

（6）脅威分析環境

脅威分析することで，プロアクティブ防御のための新たな脅威情報を抽出できる。マルウェア分析のための環境や，ログ分析のための環境を含む。

富士通は，一部手動ではあるが，本モデルを適用することで効果が得られることを確認している。したがって，脅威分析によって得られる脅威情報を活用することで，APT攻撃をプロアクティブに防御できると考えている。更に，運用負荷の低減に向けた自動化を実現するためにも有用である。

今後の課題は，より精度の高い脅威情報の抽出と活用である。また，APT攻撃に対抗するためには，富士通のみの脅威情報では不足しており，様々な組織，ベンダー，コミュニティなどとのグローバルな連携が必須である。

む　す　び

本稿では，脅威分析により抽出した脅威情報を基にして，APT攻撃をプロアクティブに防御するためのモデルについて述べた。

今後，お客様のICT環境は，今以上に様々な攻撃の脅威にさらされることが予測される。富士通は，お客様へのセキュリティソリューションに本モデルを適用し，お客様のICT環境の安心・安全な運用を支えていきたい。

参考文献

（1）NISC：サイバーセキュリティ基本法案の概要.
http://www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdf

（2）ベライゾンエンタープライズソリューションズ：2014年度データ漏洩/侵害調査報告書.
http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_ja_xg.pdf

（3）IPA：高度標的型攻撃対策に向けたシステム設計ガイド.
https://www.ipa.go.jp/files/000046236.pdf

（4） MITRE：Cyber Observable eXpression.
https://cybox.mitre.org/
（5） MITRE：Structured Threat Information eXpression.
https://stix.mitre.org/
（6） MITRE：Trusted Automated eXchange of Indicator Information.
https://taxii.mitre.org/
（7） MITRE：Collaborative Research Into Threats.
https://crits.github.io/

著者紹介

大迫剛史（おおさこ　たけし）
セキュリティマネジメントサービス事業本部サイバーディフェンスセンター所属
現在，セキュリティインシデントの調査やセキュリティサービスの開発に従事。

岩田洋一（いわた　よういち）
セキュリティマネジメントサービス事業本部マネージドセキュリティ事業部所属
現在，セキュリティサービスの企画・開発に従事。

鈴木智良（すずき　ともよし）
セキュリティマネジメントサービス事業本部マネージドセキュリティ事業部所属
現在，サイバーセキュリティインテリジェンスの開発に従事。