JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

高度サイバー攻撃（APT）への備えと対応ガイド

～企業や組織に薦める一連のプロセスについて

一般社団法人 JPCERT コーディネーションセンター

2016 年 3 月 31 日

JPCERT CC®

著作権・引用や二次利用等について

本資料の内容に関するお問い合わせ

一般社団法人 JPCERT コーディネーションセンター
エンタープライズサポートグループ
E-mail：es-info@jpcert.or.jp

更新履歴

2013 年 7 月 25 日	Ver.1.0	初版
2013 年 10 月 1 日	Ver.1.1	コラム内容を修正
2015 年 3 月 16 日	Ver.2.0	第 2 版 章構成を変更、対応手順のフローチャート化など
2016 年 3 月 24 日	Ver.2.1	Web 公開版

JPCERT CC®

「高度サイバー攻撃（APT）への備えと対応ガイド」Web 公開版 まえがき

JPCERT/CC は、日本国内の企業や組織に対し、APT を理解し準備と対応を促すことを目的に、2012 年に APT（Advanced Persistent Threat、先進的で執拗な脅威）への対応事例を豊富に持つ米国デルタリスク社（Delta Risk LLC）に作成依頼した"Initial Procedures and Response Manual for Countering APT -Enterprise Processes and Actions-"を、我が国の企業や組織の実態に精通するコンピュータインシデント対応に関する専門家で構成される「APT 攻撃初動対応マニュアルの国内利用に関する検討委員会」において、国内の企業や組織が効果的に利用できるよう検討した内容をとりまとめたものを「APT への備えと対応ガイド」として作成し、2013 年に初版をリリースした。

その後 2015 年に、サイバーセキュリティに関するガバナンスやマネジメントの実装について明確化した『NIST Cybersecurity Framework[1]』や『The Critical Controls for Effective Cyber Defense（CSC）v5.1[2]』等のフレームワークの概念や内容を本ガイドに取込むなどの改訂作業を行い、第 2 版としてリリースした。

これらの版は、内容を非公開としたうえで国内の企業や組織に個別に配付していたが、昨今では、APT によるものと思われるインシデント事例の報道の増加に伴って、国内の企業や組織においても「標的型攻撃」と呼ばれる概念を含む APT の脅威と対策の重要性について理解が浸透してきている。こうした現状を鑑み、より広く国内企業と組織に向けて、APT の活動を妨害し情報資産を防御するための具体的な活動目標の参考資料として利用していただくことを目的として、第 2 版の内容を一部修正して Web 公開版を作成した。

本ガイドは、従来の一般的なサイバー攻撃やコンピュータインシデントへの対応能力がある組織が、APT と呼ばれる高度なサイバー攻撃に備え対応するために、戦略やポリシー、手順を検討する際の参考文書として利用することを意図して書かれている。

本ガイドの目的は、以下のとおりである。

- 組織のインシデント対応チームやセキュリティチームの知識を高め、APT に備えたシステム環境を構築することを支援する
- APT に対する準備、検知と分析、そして封じ込めの一部に集中的に取り組むことに役立ち、組織内ネットワークに APT が存在することに気付いた時の初動対応手順を備え、効果的なインシデント対応措置を確実に行うことを可能にする
- APT の実態を把握しインシデントに対応できるよう、攻撃の有無について過去に遡って調査するために組織が準備しておくべきことを明らかにする

[1] IPA が翻訳文書を公開している。タイトルは、『重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0 版（Framework for Improving Critical Infrastructure Cybersecurity Version 1.0）』

[2] SANS を中心とするセキュリティ専門家団体の共同研究により作成されたサイバー攻撃対策にフォーカスしたフレームワーク。Council on CyberSecurity（現在は Center for Internet Security に改称）が原文を公開している。

- 企業や組織が、JPCERT/CC をはじめとする業界内の情報共有機関や他の組織の CSIRT[3]と協働するための汎用的な手順を整備し、APT に対する迅速かつ的確なインシデント対応ができるようにすることを支援する

本ガイドは、一連の APT インシデント対応プロセスにおいてどのように対処すべきかについて記載している。特に、APT 活動の発見からインシデント対応の間に企業や組織に何ができるかについて、焦点をあてている。

[3] CSIRT（Computer Security Incident Response Team、シーサート）は、コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行なう。CIRT や IRT という場合もある。

ガイドの構成

本ガイドは、以下の 3 部から構成されている。
第 1 章　APT の定義と活動モデル
第 2 章　APT 対応のための事前準備
第 3 章　インシデント対応プロセス

「第 1 章　APT の定義と活動モデル」では、本ガイドにおける APT の定義に触れ、その活動モデルを、準備・潜入・横断的侵害・活動の 4 段階アプローチを使って説明する。また、APT 対応のための事前準備やインシデント対応に際して、インディケータ[4]情報を入手し、適切に利用することにより、攻撃の検知・検証が可能になる。第 1 章の後半では、インディケータ情報の定義や内容を説明するとともに、インディケータ情報の交換やインディケータ情報をインテリジェンス情報と統合して他の専門組織と共有するための継続的な仕組みを持つことの重要性について述べる。

「第 2 章　APT 対応のための事前準備」では、組織が APT のリスクを特定するために行うこと、また APT の活動を妨害し、組織の情報資産を守るために取るべき手段について解説する。サイバーセキュリティの取り組みにおいて、上級経営陣を巻き込んだガバナンス活動とビジネスプロセスレベルでのマネジメント活動の 2 つが同時にうまく機能することがグッドプラクティスと考えられている。識別したリスクの許容度の評価、守るべき資産の特定についての取り組みについて紹介する。また、迫りくる脅威を特定するための取り組みとして、脅威の理解、情報共有、予防的なログの保持と定期的な分析活動について解説する。効果的に防御策を実施しインシデントに対応するための事前準備として、ポリシーやガイドラインの整備、インシデント対応機能の整備と人材育成、CSIRT の設置、トレーニングおよび演習の実施、インシデント対応計画の検証の実施を推奨する。

「第 3 章　インシデント対応プロセス」では、組織がログの監視によりマルウェア感染や C&C サーバへのアウトバウンド通信を検知することにより APT の可能性を認知した時点、あるいは、外部組織から通知を受けた時点から、インシデント対応チームが侵入に対処するまで、APT に対応する際の重要なポイントについて順を追って解説する。組織はどのような場合に自社のネットワーク上に存在する APT について外部から通知を受けるのか、攻撃者の活動を長期的に追跡するためのデータを確実に収集するにはどのようにすればよいか、APT の活動を認知した際の初動として何をすればよいか、インシデント対応中にどのような措置を検討すべきか、どのような措置を避けるべきか、外部のインシデント対応チームによる支援の導入に関して、導入を決定するしきい値をどのようにして定めるか、導入の効果を高めるにはどのような備えが必要かを紹介する。

「付録 A：事前準備のために利用するチェックリスト」、「付録 B：インシデント対応フロー及びチェックリスト」は組織における APT 対応の準備状況や対応プロセスの確認に使用できる。これらのチェックリストやフローは、組織が持つ特定のニーズに合わせて修正して利用していただくことを想定している。

また、APT への効果的な対応を実現するための重要な要素であるログの管理についての参考として、「付録文書：ログ保管に関する分析レポート」の中でログ保管の推奨値について紹介する。

[4] 「インディケータ」は、APT の可能性がある攻撃、または、攻撃の準備活動を選り分けるためのデータまたは情報のことをいう。

JPCERT CC®

目次

ガイド作成の背景

JPCERT/CC が 2010 年に行った APT に関する実態調査では、長期間にわたって社内で攻撃者による活動が行われていてもその兆候を検出できなかった事例がほとんどであった。またログの保持や保全状況に問題があり、企業や組織が APT 活動下にあると気付いたものの、いつ頃始まったのか、侵入経路や攻撃手口はどのようなものだったのかを特定することは困難な場合が多かった。

APT による攻撃にあった企業や組織は、情報セキュリティ対策を何も実施していなかったわけではなく、ベースラインとなる基本的な対策（アンチウイルスソフトの導入、パッチマネジメントの実施等）は行っている企業や組織が多かった。

本ガイドは、企業や組織が APT に備え対応するためのガイドとして利用することを想定して作成された。原著の執筆者であるデルタリスク社（Delta Risk LLC）は、JPCERT/CC の連携先やサービス利用者らに APT による侵入に対処するための知識・プロセスを提供する目的で、マンディアント社（Mandiant）およびロッキード・マーティン社（Lockheed Martin）から提供された、APT への対応に関する豊富な専門知識と経験についての情報を、インシデント対応に関するベストプラクティスとして本ガイドの内容に反映した。これらの情報は、企業や組織が確実なセキュリティを実装するために役立つ事実、手順および考察を明らかにする上で重要かつ不可欠なものである。

ガイドは組織が CSIRT または同等の機能を有することを前提とした記載となっている。本文中には「セキュリティチーム[5]」や「インシデント対応チーム[6]」として、セキュリティ管理策の実施主体やインシデント対応実施主体が登場する。セキュリティチームの中にインシデント対応機能を包含する場合もあるが、組織により実装は異なるため、ガイドの中ではこれらの用語を使い分けている。

[5] 「セキュリティチーム」は、企業や組織内のセキュリティオペレーション機能全体（コンプライアンス、パッチ管理、トレーニング等）を指す。

[6] 「インシデント対応チーム」は、実際のインシデント対応者を指す

第1章.　APT の定義と活動モデル

1.1.　APT の定義

ある脅威が APT（先進的で執拗な脅威）とみなされるためには、攻撃者が戦略的かつ組織的に攻撃活動を行い、標的とする特定の企業や組織に対し執拗に関心を持ち続ける[7]ということが条件となる。この定義に基づくと、APT には少なくとも以下のような特徴がある。

- 明確な長期目標に基づく作戦行動のような活動が見られる
- 活動を遂行するために巧妙に仕組まれたインフラ／プラットフォームがある
- 標的とする組織の従業員に対する諜報活動を行う能力がある
- 目的達成のために、様々なテクニックやソフトウェアを組み合わせることができる
- 侵入検知や各種インシデント対応措置に対して速やかに適応し攻撃手法を改変する能力がある

当初「APT」は、国家が後押しするスパイ行為を表す特定の脅威となる侵入や攻撃手口として定義された[8]。本ガイドでは、**先進的で（Advanced）、執拗な（Persistent）、脅威（Threat）**の用語を以下のように定義する。

表 1：APT の定義

先進的で：攻撃者は目的達成のために必要な最小限のツールを使用し行動する。そのため、一連のイベント自体が「先進的」と見なされる。

執拗な：攻撃者は ネットワークに長期にわたって居座り続ける。繰り返しアクセスを図り、何年にもわたってアクセスを維持することもある。

脅威： 攻撃者は長期的な活動を実施するためのリソースが必要である。このような活動をおこなう攻撃者には、国家が支援する者や先進的なサイバー犯罪者が含まれる場合がある。

・攻撃者は、**先進的なツールとテクニック**を用いて**高度に組織化された活動を展開する**
・標的を攻略しアクセスを維持するために、**複数の手法、ツールやテクニックを組み合わせる**ことが多い

・攻撃者は**長期的に活動を継続する**ために、侵入に成功した組織への**足場の構築・維持**を図る
・**機密情報**の収集にフォーカス
・長期の活動可能な攻撃インフラを構築
・目立たずゆっくりしたアプローチ

先進的で(Advanced)　執拗な(Persistent)　脅威(Threat)

APT 攻撃者は、明確な攻撃の**目的**と実行**能力**を有し、**組織化され、十分な資金を持ち**、また**豊富な経験を**有する者が**連携**して活動する。

リスク	想定される攻撃者
・評判を失う	・競合他社、ハクティビスト
・競争優位性を失う -ID の窃盗 -交渉内容の漏洩	・国家スパイ、産業スパイ
・内部情報の売買	・犯罪組織
・事業能力の低下	・競合他社、国家が後押しする団体

APT は、重要性の高い情報、あるいは、組み合わせることで重要性の高い情報になるデータを取得し、企業や組織に深刻な脅威をもたらす。APT は、役員の個人情報のほか、組織の独自のビジネスプロセスや事業戦略といった知的資産を狙うことがある。

APT 攻撃者は、ネットワークへの侵入技術に長けており、侵入後はアクセスを維持するためにシステムを改ざんすることもできる。執拗にアクセスし続けることで、APT はネットワークやビジネスプロセスに関する知識を得て、断片的な情報を再構成し、組織が持つ重要性の高い情報や資産を奪取

[7] BITS Malware Risks and Mitigation Report（マルウェアのリスクと低減に関するレポート）、2011 年 6 月

[8] セキュリティ業界の一部では「APT」を、国家やその他の組織が後押しする攻撃者の行為に限らず、特定の標的を狙う「標的型攻撃」全般と混用して称する場合があるが、本ガイドの定義によればそれは誤用となる。

し、場合によっては破壊活動を行う。そのため APT 攻撃者は、強大な軍事力を持つ政府やサイバー犯罪組織、その他の豊富なリソースを持つ組織など、資金力と政治権力を擁した組織からの任務を請け負い活動を行うものと考えられている。

US-CERT によると、APT は標的とする組織に対して執拗かつ長期的に活動を行うため、一度でも狙われた組織は、今後も狙われる可能性が非常に高いとされる。その活動には、**攻撃者**、**標的**、**目的**という次の 3 つの要素が必ず含まれている。

- **攻撃者**：攻撃者は、長期にわたり標的とする組織のネットワークへの侵入を試みる。その際、ネットワークのアーキテクチャや事業運営に関する情報を収集しながら、一般とは隔離されたシステムや情報資産に対して継続的にアクセスできるように、ネットワーク全体に活動範囲を広げる。その手段として、攻撃者は、活動のための足場を構築・維持し、組織内部のシステムを横断的に侵害し、正規のユーザの認証情報の奪取を試み、証明書による信用情報を悪用するなど様々な戦術を用いる。最終的に、ホストとなる PC を悪用し、サービス妨害、偽の電子メールを使った「スピアフィッシング（いわゆる、標的型メール）」など、およそ考え付く限りのサイバー攻撃を行う。彼らのメンバは若干の増減はあり得るが、その基本的な性質は変わることがない。
- **標的**：標的とされた組織は、攻撃者による調べあげられ、システムや情報に対する侵害が行われる。攻撃者は獲得したアクセス手段を維持し、政府機関や軍事組織あるいは他の資金力のある組織など、攻撃の指示者の目的に応じて攻撃方法を柔軟に変更する。標的は 1 つである必要はなく、攻撃者は時間差を作って複数の標的を設定したり、一つの組織内に複数設定する場合もある。
- **目的**：APT の活動において最も重要なのは、その活動と時間などのリソースを投入する動機となる目的である。APT は長期的な目標を達成するために活動すると考えてよい。APT の目的は、時間とともに変化することもあるが、最終的な目的は重要性の高い情報の収集、データの破壊・削除による事業活動の妨害、APT 活動を継続するためのアクセス手段の維持などが代表的なものである。ただし攻撃者自身の知的探求や、役員スケジュールの確認など、これまでに挙げた APT の特徴とは必ずしも一致しない動機にもとづく場合もある。

1.2. APT の活動モデル

APT 活動モデルの作成

APT 活動モデルの作成は、攻撃者に係わる情報を統合し、防御手段や他の留意事項を実際の運用にまで発展させるための準備をする際の重要なステップである。本ガイドでは APT の活動を形容するために、4 段階アプローチを用いる。この 4 段階アプローチは以下のステップで構成される。

- **第 1 段階：　準備** ― 攻撃者は標的組織への侵入の前に入念に調査し侵入の手筈を整える。
- **第 2 段階：　潜入** ―攻撃者は標的組織のセキュリティ防御を破り侵入する。
- **第 3 段階：　横断的侵害** ―攻撃者は組織内の侵害を広げ目的とする重要資産に近づく。
- **第 4 段階：　活動** ―攻撃者は重要資産に対しデータの窃盗、改ざんなどの行為を行う。

第 1 段階：準備

準備段階では、攻撃者は、活動の障害となりうる要素を極力排除するべく周到な準備をおこなう。この段階では、いくつかの事象は観察可能である。攻撃者は、実際の所在地や目的を掴まれにくくするためにグローバル規模の分散型インフラを構築する。攻撃者はまた、標的組織の機密情報を収集し、過去の活動からの教訓を基に侵入経路や攻撃手口を改善する。広く報道された「ナイトドラゴン（Night Dragon）」作戦行動では、複数の国際的なエネルギー企業を狙った組織的な攻撃が長期に渡り行われたが[9]、C&C サーバ[10]は、実際に攻撃を受けた組織のものが使われ、攻撃者はエネルギー業界固有の企業間トラストチェーンを巧みに利用した。攻撃者は、活動ができるだけスムーズに行われるように活動手順を徹底的に検証する。

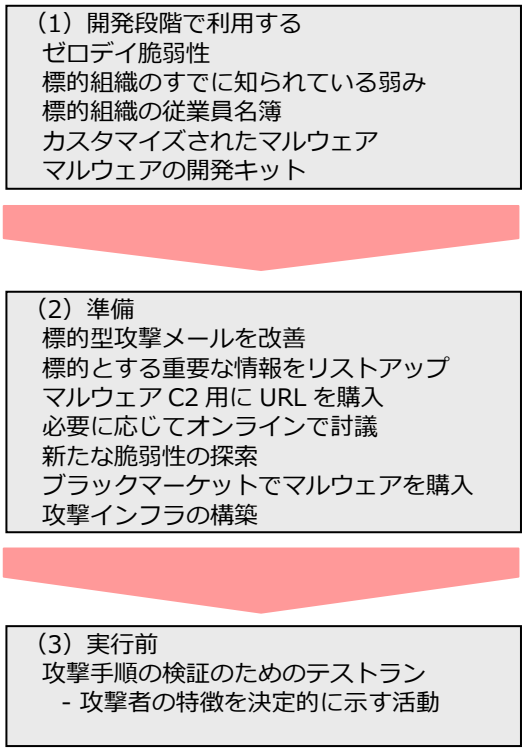


図 1：攻撃者の準備作業

興味深いことに、APT はまた、可能であれば防御側の法律的な制約を利用する。例えば米国では、米国防総省が米国民に関する機密情報を収集することは法で禁じられている。そのため APT は国防総省を狙う際には米国のインフラを使う。国防総省がこうしたシステムを合法的に捜査することができないためである。また欧州では、セキュリティ関係者がトラフィックの監視を行うことについて欧州プライバシー法やその他の各国の法規制による制約を受ける場合があるため、攻撃者は盗んだ情報を欧州内のゲートウェイを通じて国際組織に送ることが多い。APT はその活動の中で技術的な戦術と法的な戦術を組み合わせて用いるため、技術的な方法による防御だけでは対処が大変難しくなることがある。

この段階で攻撃者は、情報収集システム、電子メールシステム、ツールのレポジトリ、マルウェア保存レポジトリ、C&C サーバ、および情報の引き出しに使うサーバ、あるいは Dropbox 等の外部クラウドサーバなどを用意し攻撃用のインフラを構築する。攻撃者はこれらのインフラを世界中に存在す

[9] Global Energy Attacks: “Night Dragon” （グローバルなエネルギー攻撃「ナイトドラゴン」）、McAfee、 2011 年 2 月

[10] C&C サーバ（Command & Control Server）は、指令（command）を送り、制御（control）の中心となるサーバ、「C2 サーバ」と表記されることもある。

るデバイスに分散させ、その制御を維持することができる。攻撃者は、こうしたインフラ用に独自にドメイン名を作成、登録することもある。このようなドメイン名は他の既知の攻撃用ドメインに関連したものであることがある（すなわち、ドメインはそれが APT であることを決定的に示すインディケータとなる）。

次に、攻撃に利用可能な文書（PDF, DOC など）を収集する。この文書の収集のために Web サイトに入ってくるトラフィックの発信元 IP アドレスの範囲もまたインディケータとなる。収集した文書は、標的型メール攻撃などに利用される。こうした文書の内部に存在するメールアドレスが最初の標的として利用される可能性がある。標的を定める他の方法としては、従業員のソーシャルメディアアカウント、電子メールアドレス、従業員満足度に関する情報を利用することもある。これら攻撃者が作成した構成要素の動作を確認するため、テストラン（検証のための試験的な攻撃）を実施する場合があり、このときの攻撃の発信元 IP アドレスやドメイン情報を特定できれば、それらは重要なインディケータとなる。

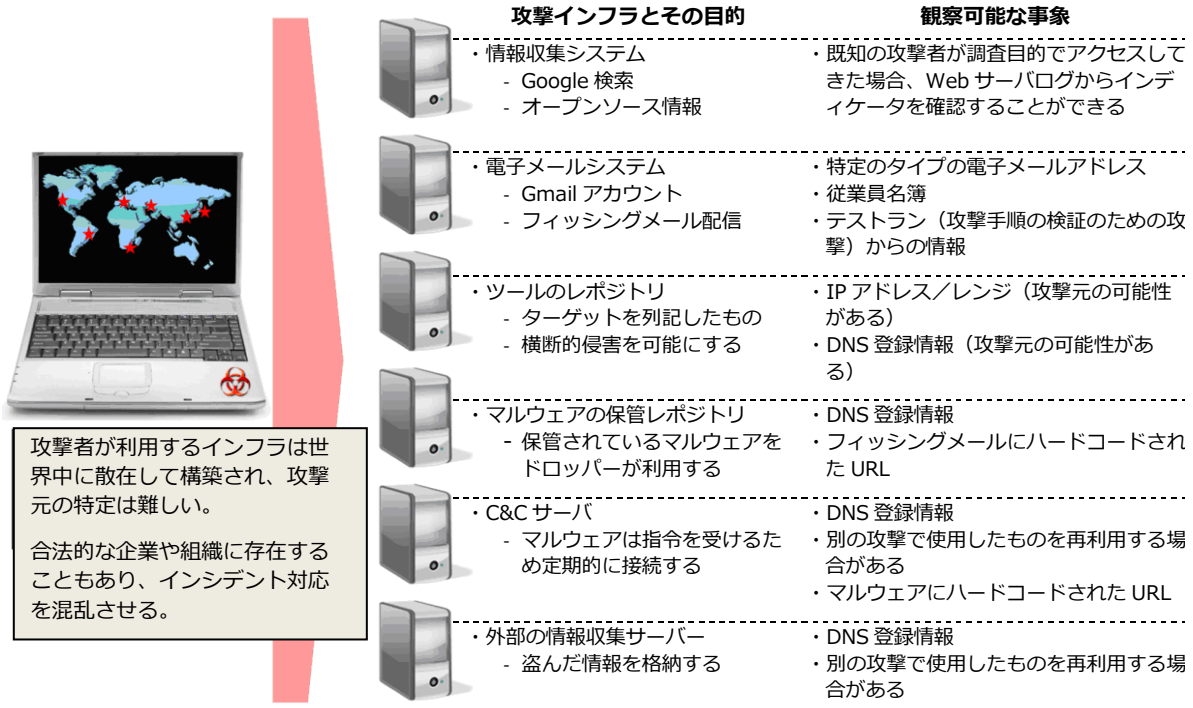


図 2：攻撃者が利用するインフラの特徴

第 2 段階：潜入

潜入段階の攻撃者の活動は、ネットワーク境界のファイアウォール、IDS デバイスや他の配置されているセンサを侵害するため、非常に目立つ。攻撃者が標的型攻撃メールを利用した潜入戦術を使う場合、用心深いユーザに気づかれる可能性がある。この時点では、最新のアンチウイルスソフトやホストベースの IDS によって潜入は阻止される場合もある。資金力が十分ある APT 攻撃者は標的組織に対する事前の調査により、組織にどのような防御体制が敷かれているか、それをどうやって回避するか、組織内の誰を標的とするか、ネットワークはどのような構成になっているか、そして大きなセキュリティ上の欠陥が存在するかどうかを把握している。APT 攻撃者は、露出を最小限にして捕捉されないようにし、目的を遂行しようと考える。最新の高度な手口では、IDS などのセンサで検知されることなく侵入するために、正規の認証情報を盗みそれを使用する。こうした特定の侵入経路や手口

に対しては適用可能な対処方法が存在する。一方で、リモートアクセスや認証情報の管理に対しては強固な方策が必要となる。

攻撃者がネットワークに侵入するのに利用する一般的な方法がいくつかある。フィッシングメールによってユーザを騙し偽の Web サイトからマルウェアをインストールさせたり、脆弱な周辺システムを攻撃し、周辺システムと標的組織のネットワーク内のシステムの間に存在するトラストチェーンを利用するなどにより、ネットワークに直接侵入しようとする。さらに攻撃者は、ネットワーク内に接続されたまま残っている共有モデム（特に SCADA システムでは一般的にみられる）や監視されていないゲートウェイ接続など、利用可能な他のアクセス方法を把握している可能性もある。最近では攻撃者は高度なツールを使って正規の認証情報を取得し、VPN などの正当なアクセス方法で組織内ネットワークにアクセスする例もみられる。

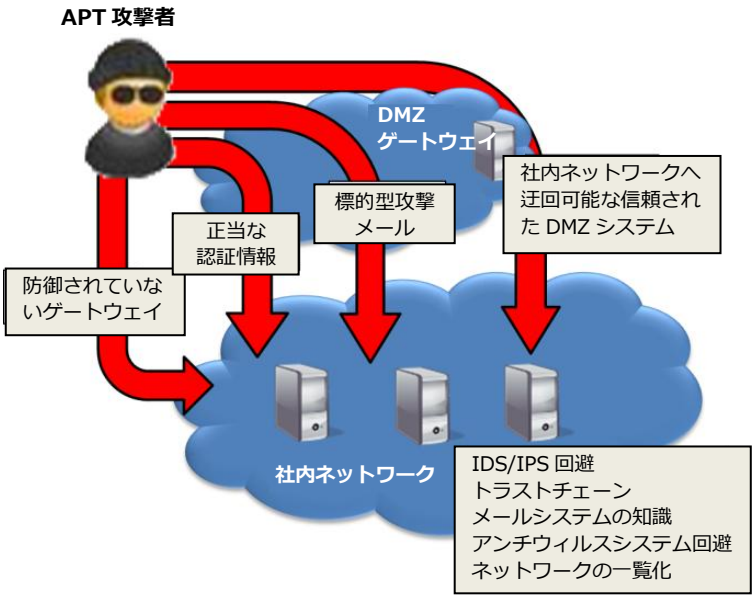


図 3：APT の侵入経路や攻撃手口

気づかれることなくネットワークへの侵入に成功すれば、これ以後の活動段階でも攻撃者は成功裏に進める可能性が高まる。ネットワークセキュリティ部門は最初の侵入を検知できなければ、他に有効な機能を持ち合わせない限り、攻撃者の活動を完全に見失う可能性がある。

第 3 段階：横断的侵害

攻撃者は組織のネットワークに最初の足場を築いた後、横断的侵害をおこなう。通常、攻撃によって最初に侵害されたシステムには APT が狙っているものが存在しない。攻撃者は別の戦術を用いて、ネットワークの構造を把握し、他の脆弱なシステムを横断的に侵害する。最初の侵入は最も明らかで目立つ行為であるが、その後の他システムへの周回と、感染したノードに横断的侵害のためのより大きな活動基盤を作り上げる行為は、最初の感染に比べほとんど目立た

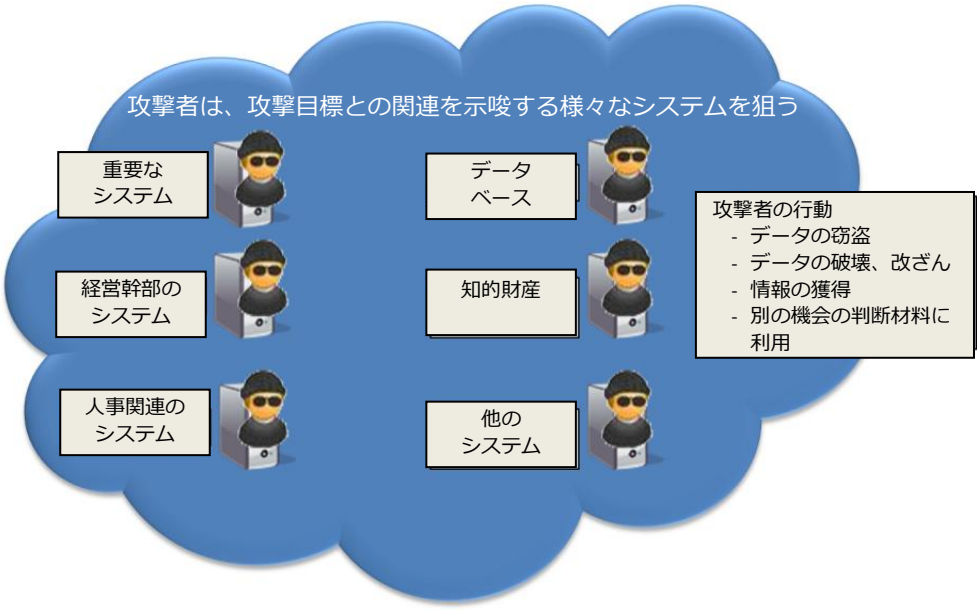


図 4：攻撃者が狙うシステム

ず、その動きは検知されにくい。攻撃者はこのようにしてネットワーク内のシステムへの侵害を広げた後、やがて重要な資産や重要な人物に属するシステムに到達する。

APT 対策や従来のセキュリティ管理策の典型的なベストプラクティスとして、重要なシステムの隔離、センサを使ったネットワークモニタリング、トラフィックの難所の設置が挙げられる。横断的侵害は、APT 活動のうち最も検知が難しいものの一つである。これはネットワークの入口は監視するが、ネットワークの出口に検知システムを採用しないでよいと考えてきた従来のネットワークセキュリティに対する甘さに原因がある。この段階で攻撃者は、継続してネットワークや侵害されたホストにアクセスすることができるようシステム内に複数の裏口を作る。

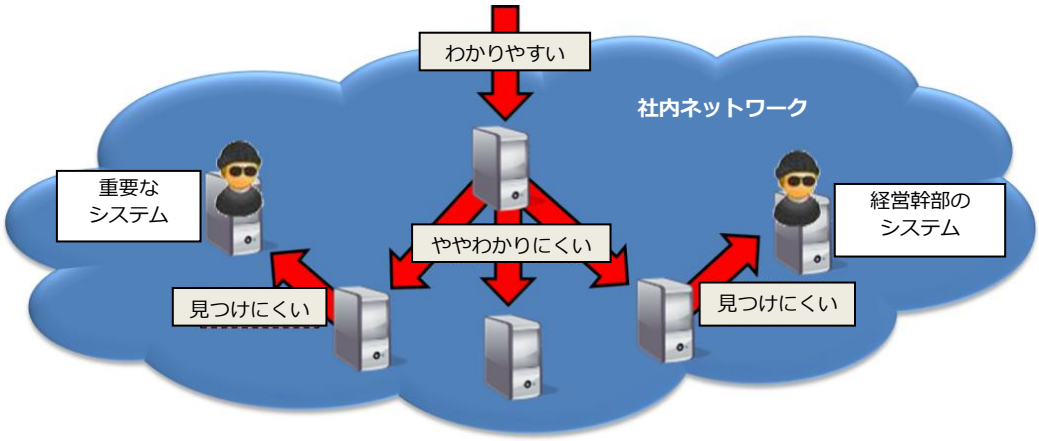


図 5：APT の横断的侵害

第 4 段階：活動

やがて、APT は活動を開始する。この段階では、APT の活動は時間と共に様々に変化する。最も一般的な活動は、知的財産、スケジュール、業務マニュアル、電子メールファイルなどの価値のあるデータの窃盗または収集である。それらのデータは企業や組織の状況認識を把握するための情報、標的組織と新たに発見された他の組織とのトラストチェーンに対する攻撃計画の立案に役立つ情報となることもある。時間が経過してもアクセスは維持され、組織が保有する情報の窃盗や何らかの効果を狙った情報の改ざんが引き続き行われる。データを破壊し、組織に遅延や困難をもたらし、攻撃者が優位に立つようにすることもある。この段階では多くの目標が実行されるが、攻撃者が指示を受けた目標は達成までの期限が非常に短い可能性が高い。したがって、攻撃者にとって標的への継続的なアクセスは非常に重要となる。なぜなら、標的組織に潜入するのに非常に長い時間かかるため、目的達成は短時間で行う必要が出てくるからである。攻撃者のこのようなサイクルを理解し、防御手段によってサイクルを破壊することができれば、攻撃者のリソースを消費させることができる。

モデル作成の際のその他の留意事項

これらの 4 段階アプローチは、APT の全体像を役員やサイバーセキュリティ関係者以外の一般従業員に説明する際には効果がある。しかしセキュリティチームにはもう少し精度の高いものが必要である。マンディアント社（Mandiant）の攻撃者に関する説明やロッキード・マーティン社（Lockheed Martin）の「キルチェーン（Kill Chain）[11]」など、APT による攻撃のモデルがいくつか存在する。組

[11] Intelligence-Driven computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains（敵対者の作戦行動と侵害キルチェーンの分析に基づく、機密情報を対象としたコンピュータネットワークの防御）、LM-CIRT、 2011 年

織が攻撃者のプロファイリングをもっと徹底的に行いたい場合、攻撃者を適切に分類するためにこうしたモデルの一つを実装する必要があるだろう。

ハイレベルな取り組み事例

「APT プロファイル」の作成

脅威について理解し、どのようにして様々なインディケータに注意するかを把握した後、セキュリティチームは、自組織を狙っているとみられる APT に関するプロファイルを構築したいと考えるだろう。プロファイルは、今後の侵入について攻撃者の特定に役立てるために、APT 活動の特徴を明らかにする試みである。プロファイルは極めて機密性が高いものと考え、必要な場合にのみ共有するようにする。こうしたプロファイルに侵入者がアクセスできないように、細心の注意を払う必要がある。

APT プロファイルを可視化することにより、アナリストは最新の脅威状況について優れた理解を持つことになるだろう。そのためにも相関エンジンなどを用いて APT プロファイルのデータベースから情報を得られるようにし、SIEM がプロファイルデータベースに情報を提供できるようにすべきである。

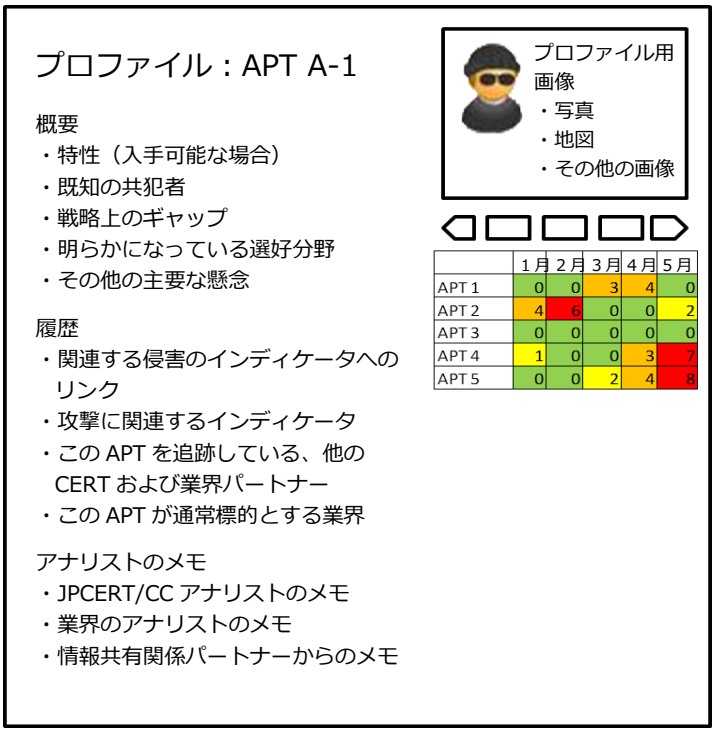


図 6：APT プロファイルの概念図

1.3. インディケータ情報の共有

インディケータ情報の重要性

本ガイドではインディケータを「APT の可能性がある攻撃、または、攻撃の準備活動を選り分けるためのデータまたは情報」と定義する。攻撃と侵害の兆候を示す情報は、APT に対する効果的なインシデント対応計画において重要な要素である。

下記にインディケータの種類を挙げる[12]。列挙した各インディケータは、種類毎の特性が異なる他、誤検出率や、攻撃者が防御を回避するためのアプローチを考え出す難易度からの影響を受ける。

- **基本的インディケータ**は、最も基本的なレベルのインディケータで、攻撃元の IP アドレスや通信先の URL などの単純に判断できる情報である。ただし、攻撃者はこの情報が示す要素を容易に変更できる。このタイプのインディケータは非常に具体的で、インシデントに直接関係している。
- **複雑なインディケータ**は、分析の結果から生みだされるインディケータである。通常、IDS シグネチャやファイルのハッシュ値など、算出・創出されたものがこのタイプに分類される。
- **パターンによるインディケータ**は、一般的に観察可能な、特定の攻撃者の存在を示している可能性のあるインディケータである。このタイプのインディケータには、攻撃者が通常標的型攻撃メールを送りつける従業員のタイプやマルウェアのポート使用パターン、DNS 登録のパターン、その他の攻撃者固有の行動様式から観察可能な性質などがある。

表 2：インディケータの種類

種類	例	使い方	メリットとデメリット
基本的インディケータ	IP アドレス、URL	監視または阻止	防御者は単純に判断できる。攻撃者は簡単に変更できる。急速に陳腐化する。
複雑なインディケータ	ファイルのハッシュ値、IDS 署名	インスタンスの検索	信頼性は高い。攻撃者が値を迅速に変更することが幾分困難になる。
パターンによるインディケータ	侵入経路や攻撃手口、使用するポート、固有の特性、レジストラのパターン	攻撃者に係る情報の分析、APT プロファイルの構築、侵入範囲の確定	高い誤検出率が影響する。効果を得るためには他のインディケータと組み合わせる必要があるかもしれない。攻撃者が変えることは非常に難しい。

APT モデルの種類と段階を実際のインディケータに対してメタタグとして利用すれば、収集したインディケータを管理するための一種のマトリクスを構築することができる。企業や組織は特定の使用のために「基本」または「複雑」の種別のインディケータのみを抽出したいと思う場合がある。一方で、攻撃者に関する情報の分析者は行動様式に関するインディケータに関心を抱くかもしれない。また、特定の攻撃段階に関係するインディケータにのみアクセスしたいと分析者が望むときがあるかもしれない。

次の表は、APT による侵入の記述に用いられる可能性のあるインディケータのサンプルを示している。APT は急速に変化するため、この表がすべてを包括しているわけではない。

[12]本定義は、ロッキード・マーティン社のネットワークセキュリティへのキルチェーン（Kill Chain）アプローチで使われるインディケータの種類を参照。

表 3：APT 侵入の記述に用いられる可能性のあるインディケータの例

インディケータ	検知メカニズム	種類	段階
IP アドレス（偵察）	ISP の NetFlow、外部センサ	基本	準備
IP アドレス（攻撃）	外部センサ	基本	潜入
IP アドレス（C2）	外部センサ	基本	横断的侵害
IP アドレス（情報引出し）	アウトバウンドセンサ	基本	活動
URL	DNS／プロキシ	基本	さまざま
フィッシングメールの特徴	メールサーバ、ユーザ	パターン	潜入
マルウェアのファイル名	フォレンジック／ホスト	基本	さまざま
マルウェアのハッシュ値	フォレンジック／ホスト	複雑	さまざま
マルウェアの行動様式	攻撃者に係わる情報の分析／ホスト	パターン	潜入
マルウェア の違い	横断的侵害を示すアーティファクト（サイバー攻撃の痕跡[13]）	パターン	横断的侵害
好んで使用するゼロデイ脆弱性	インシデント対応	複雑	潜入
使用されるインフラ	インシデント対応／ISP の情報提供	複雑	準備／活動
ホップポイント[14]	警察、法執行機関／ISP の情報提供	パターン	活動
DNS レジストリの詳細	WHOIS 分析	パターン	さまざま
レジストラのパターン	攻撃者に係わる情報の分析	パターン	準備
ポートのパターン	インシデント対応	パターン	潜入/横断的侵害
C&C サーバの特性	攻撃者に係わる情報の分析（カスタムメイドか、盗まれたものか）	複雑	準備／潜入
標的となる従業員（攻撃の初期段階）	フィッシングメールの受取人	パターン	準備／潜入
標的となる従業員（組織内での移動や拡大）	インシデント対応	パターン	横断的侵害
標的となる従業員（重要情報や重要機能）	インシデント対応、DLP	パターン	活動
標的となるデータ種別	インシデント対応、DLP	パターン	活動
補完された戦略的ギャップデータ	攻撃者に係わる情報の分析	パターン	活動

インディケータ情報の活用

APT が侵入に成功しネットワーク内に深く入り込むにつれて、防御・根絶ははるかに難しくなる。様々なタイプのネットワークトラフィックにおいて認識される APT 活動の特徴がインディケータとなる。インディケータにより、攻撃者がたどる経路について洞察を得ることができ、セキュリティチームは早期に APT を阻止できる可能性が高まる。

以下の質問に答えることで、攻撃アプローチの各段階についての洞察と潜在的なインディケータが得られるかもしれない。セキュリティチームが以下の質問に対し自組織の状況に照らして考えれば、状況の変化にともなって、質問のリストは時とともに増えていくことが分かるであろう。

- 自組織が所有しているもののうち、攻撃者が欲しいものは何か。
- 攻撃者が情報を得るために狙うシステムはどれか

[13] サイバー攻撃の技法や攻撃の痕跡を「アーティファクト」という。攻撃の客観的な証拠となる。

[14] 遠隔操作のためのマルウェアが利用する踏み台サーバを「ホップポイント」という。

- どのようにして自組織のシステムに侵入できるのか
- 自組織のシステムに侵入するために攻撃者はどのようなツールを必要とするか
- 攻撃者はどのような外部資源を利用しているのか
- 攻撃者は攻撃中にどのような種類の観察可能な痕跡を残すのか
- 潜在的攻撃者はどのようなテクノロジーギャップを持ち、それをどのように補おうとするのか
- 攻撃者は盗んだ情報を理解するために、どのような技術的専門知識が必要か

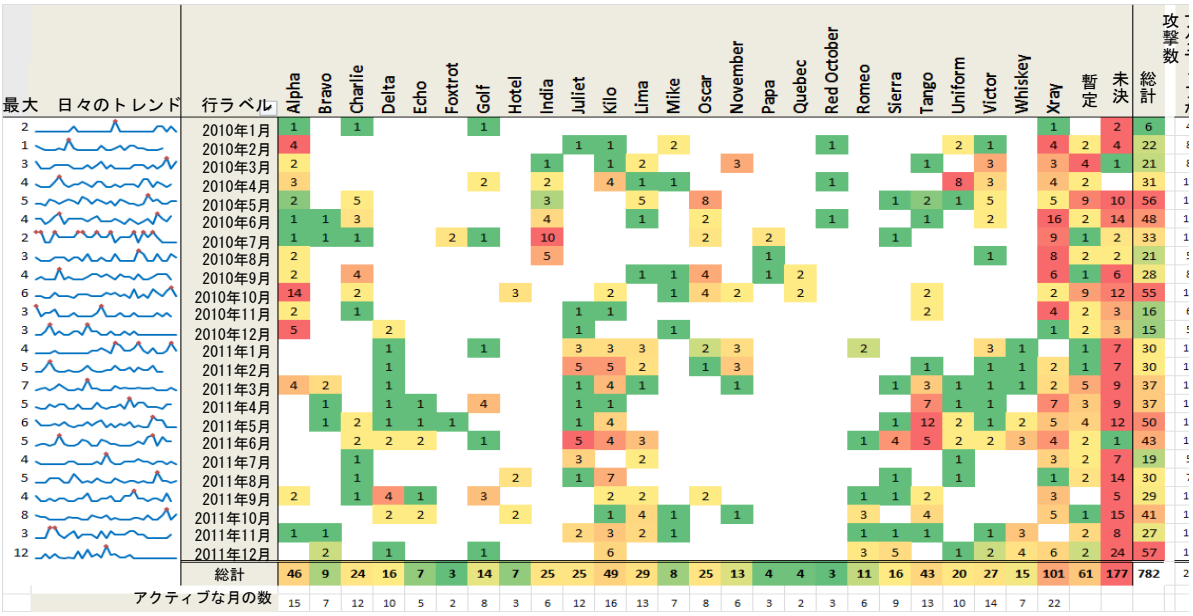
モデルを適用することで、侵入の段階に基づいてインディケータを分類することができる（あるインディケータは潜入段階に、横断的侵害段階に、または活動段階にのみ存在するなど）。インディケータがどの段階の活動に関連するのかを把握することは、インシデント対応手順により正確な情報を提供することになる。得られたインディケータが 100%確かなものと思われない場合は、JPCERT/CC や他の外部組織からの情報、他の攻撃者関連情報源、オープンソース・リサーチ等を利用して、意思決定プロセスに役立てるための適用可能なインディケータが他にないかを調べる必要があるだろう。追加のインディケータを取得できれば、侵入が APT であるかどうかを判断するのにさらに役立つ。得られるインディケータが多ければ多いほど、自組織のネットワーク内に潜む攻撃者を探すのにより大きな助けとなる。攻撃者に係る情報交換の対象には、検知方法、仮想化、攻撃システム、データ侵害、等に関する APT 攻撃者のプロファイリングに役立つ可能性のある様々な項目が含まれる。

APT のための事前準備、インシデント対応プロセスの実践のためには、企業や組織はインディケータ情報の交換やインディケータ情報をインテリジェンス情報と統合して継続的に他の専門組織と共有することを推進する必要がある。JPCERT/CC をはじめ、業界内外の信頼できる情報共有組織とインディケータ情報を自動的にやり取りするレベルになることが理想的である。

ハイレベルな取り組み事例

「ヒートマップ」を使った攻撃予測

ロッキード・マーティン社は様々な可視化能力を活用しており、その中には一定の期間の APT の活動を詳細に示すヒートマップがある。これにより、同社は APT の長期的な影響を理解し、休止状態であった APT が活動を再開した際の潜在的予測分析を行っている。以下は、このようなヒートマップが長期的にどのようになるかを示した例である。



最大	日々のトレンド	行ラベル	Alpha	Bravo	Charlie	Delta	Echo	Foxtrot	Golf	Hotel	India	Juliet	Kilo	Lima	Mike	Oscar	November	Papa	Quebec	Red October	Romeo	Sierra	Tango	Uniform	Victor	Whiskey	Xray	暫定	未決	総計	攻撃数
2		2010年1月	1		1				1																		1		2	6	
1		2010年2月	4									1	1		2					1				2	1		4	2	4	22	
3		2010年3月	2								1		1	2			3						1		3		3	4	1	21	
4		2010年4月	3						2		2		4	1	1					1				8	3		4	2		31	
5		2010年5月	2		5						3			5		8						1	2	1	5		5	9	10	56	
4		2010年6月	1	1	3						4			1		2				1			1		2		16	2	14	48	
2		2010年7月	1	1	1			2	1		10					2		2				1					9	1	2	33	
3		2010年8月	2								5							1							1		8	2	2	21	
4		2010年9月	2		4									1	1	4		1	2								6	1	6	28	
6		2010年10月	14		2					3			2		1	4	2		2				2				2	9	12	55	
3		2010年11月	2		1							1	1										2				4	2	3	16	
3		2010年12月	5			2						1			1												1	2	3	15	
4		2011年1月				1			1			3	3	3		2	3				2				3	1		1	7	30	
5		2011年2月				1						5	5	2		1	3						1		1	1	2	1	7	30	
7		2011年3月	4	2		1						1	4	1			1					1	3	1	1	1	2	5	9	37	
5		2011年4月		1		1	1		4			1	1										7	1	1		7	3	9	37	
6		2011年5月		1	2	1	1	1				1	4									1	12	2	1	2	5	4	12	50	
5		2011年6月			2	2	2		1			5	4	3							1	4	5	2	2	3	4	2	1	43	
4		2011年7月			1							3		2										1			3	2	7	19	
5		2011年8月			1					2		1	7									1		1			1	2	14	30	
4		2011年9月	2		1	4	1		3				2	2		2					1	1	2				3		5	29	
8		2011年10月				2	2			2			1	4	1		1				3		4				5	1	15	41	
3		2011年11月	1	1								2	3	2	1						1	1	1		1	3		2	8	27	
12		2011年12月		2		1			1				6								3	5		1	2	4	6	2	24	57	
		総計	46	9	24	16	7	3	14	7	25	25	49	29	8	25	13	4	4	3	11	16	43	20	27	15	101	61	177	782	
		アクティブな月の数	15	7	12	10	5	2	8	3	6	12	16	13	7	8	6	3	2	3	6	9	13	10	14	7	22				

図 7：ヒートマップの例（ロッキード・マーティン社）

第2章. APT のための事前準備

2.1. サイバーセキュリティフレームワーク

常に進化、変化する攻撃者から企業や組織の情報資産を防御し、ビジネス目標を効果的に達成していくためには、サイバーセキュリティの領域においても、PDCA サイクルを導入することが効果的であると考えられている。

2013 年 2 月の米国大統領令（Executive Order: EO）13636 号 を受け、米国商務省傘下の国立標準技術研究所（NIST: National Institute of Standards and Technology）を中心に、産官学のサイバーセキュリティに関する有識者が APT を考慮したサイバーセキュリティフレームワークについて検討を開始し、2014 年 2 月に**「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」**が発行された。

このフレームワークでは、組織におけるサイバーセキュリティリスクを管理し、インシデント対応能力を定着・発展させるためには、次の 2 つのサイクルが必要とされている。

- **ガバナンスのサイクル**—経営からの指示と必要なリソース（人・物・金）を確保するための経営への定期報告
- **マネジメントのサイクル**—現場でのリスクアセスメントと対策実施、そのための必要リソースの投入

これらのサイクルは、IT 戦略やシステムリスク管理と同じであるが、サイバーセキュリティ対応として、下記の特殊性がある。

- 自社に有用な情報収集
- 情報の分析
- サイバーセキュリティとしてのリスク評価
- フレームワーク作り
- CSIRT 及びシステム運用・システム開発要員のサイバーセキュリティスキル
- 有用なソリューションの確保

組織が中長期的な事業目標の達成を支援するためには、サイバーセキュリティへの取り組みを組織にとっての事業上のモチベーションにつながるものにすることと、サイバーセキュリティリスクを組織のリスク管理プロセスの一環としてとらえることに重きをおくべきである。

APT に対応するためには、セキュリティチームがソリューションを確保し、攻撃を防御・検知すればよいというものではない。攻撃の防御・検知に失敗する可能性も高い。そのタイミングではじめて上級経営陣がインシデントに関与するようでは、被害を極小化することは難しいと考えられる。

あらかじめ、組織においてどのようなセキュリティインシデントの発生が想定されるのか、その影響を予測した上で、次の一連の活動が、事前準備のベストプラクティスとして推奨されている。

1) 現状のサイバーセキュリティへの取り組みをまとめる
2) 被害極限目標のためのサイバーセキュリティ対策を明確にする
3) 継続的かつ繰り返し実施可能なプロセスを整備・運用し、サイバーセキュリティ改善の機会を 見つけた場合は、実行にあたっての優先順位付けを行う
4) 目標達成までの進捗を評価する
5) 社内外の利害関係者とサイバーセキュリティリスクについて情報交換を行う

特に、上級経営陣によるリスク許容度の評価が実施されているか否かが、APT 対応の成否を分けることになる。IT や情報セキュリティ部門を管轄する役員だけでなく、事業部門を管轄する役員、管理部門の役員が、自組織の環境を考慮した上で、他社事例を参照し、サイバー攻撃が発生した場合のリスクと対応について[15]事前検討し、合意形成しておくことが重要である。

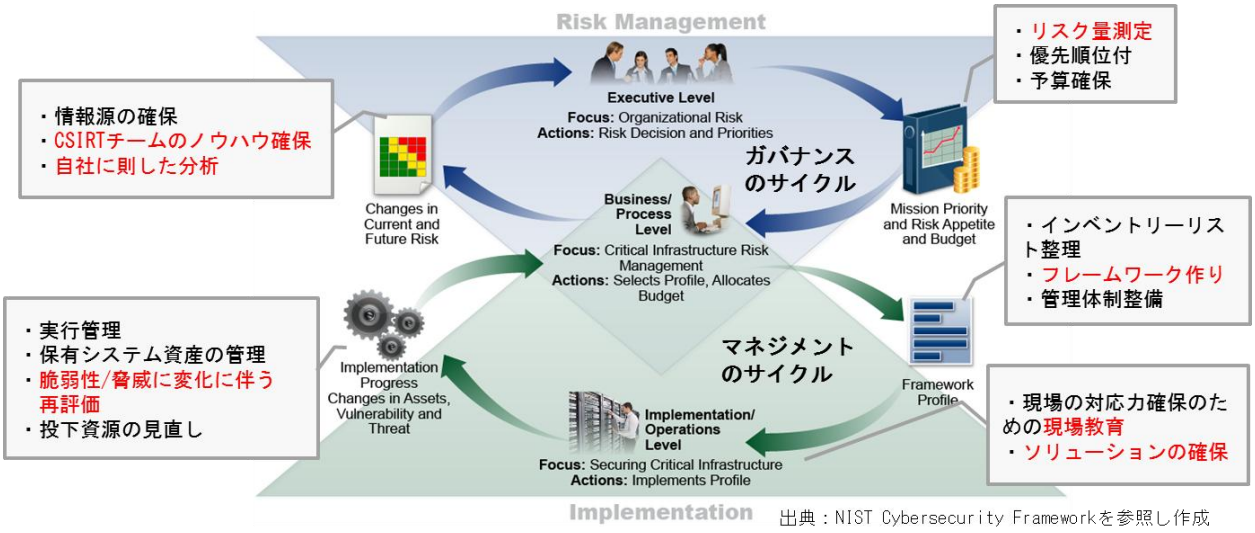


図 8：サイバーセキュリティの PDCA モデル

[15] 経営層の関与については、JPCERT/CC の研究・調査レポート『**経営者が知っておくべきセキュリティリスクと対応について**』を参照。https://www.jpcert.or.jp/research/aptrisk.html
（本報告書は、いち早く APT への対処に取り組んだ米国の企業等が、経営者および経営幹部に APT がもたらすリスクの概要を説明し、被害の最小限化等の適切な対応をとるために経営者が自ら果たすべき責任について示唆することを目的としてまとめたレポートを、日本国内の企業や組織向けに翻訳し一部修正したもの。）

2.2. インシデント対応プロセスの全体図

NIST が発行する SP800 シリーズ（Special Publication）の SP800-61「*コンピュータセキュリティ・インシデント対応ガイド*」[16]は、インシデント対応チームの助けとなるべく作成されている。この文書は、インシデント対応の準備からインシデント収束後に報告をまとめるまでに有用な手順、チーム体制などを説明している。また、サービス妨害、悪意のあるコード、不正アクセスおよび不適切な使用など、主要なインシデントを分類した上で詳しい説明がなされている。この文書には、インシデント対応能力を強化するための基本的な事項もまとめられており、基本的な指針として有益であろう。

NIST のインシデント対応プロセスは、大別すると**準備、検知および分析、封じ込めおよび根絶、インシデント後の活動の 4 段階**に分類される。企業や組織がこれをどのように適用するかは、ネットワークやシステム、アプリケーションのいずれを重視するかによって異なり、これを図 9 に示すような**6 段階に拡張**して使っている企業や組織も少なからず存在する。

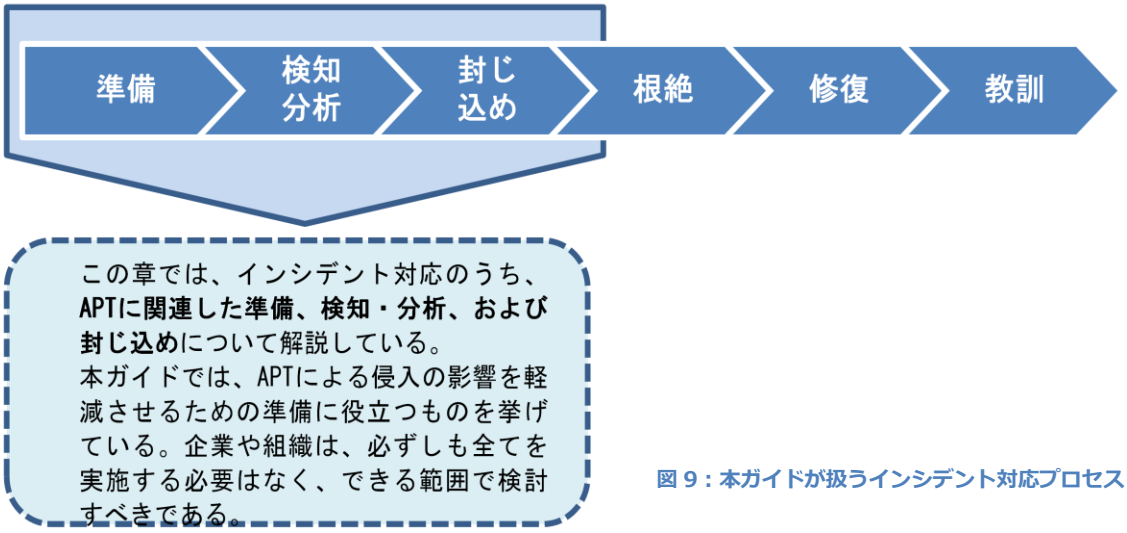


図 9：本ガイドが扱うインシデント対応プロセス

本ガイドは、インシデント対応プロセスのごく一部を扱っているにすぎない。プロセス全体は、**準備、検知・分析、封じ込め、根絶、修復、および教訓**で構成されており、それぞれのプロセスにおいて考慮すべきポイントが数多く存在するが、全てが APT に焦点を当てたものではない。本ガイドは、APT に対する準備、検知および分析、そして封じ込めの一部に集中的に取り組むことに役立ち、企業や組織が、ネットワーク上に APT が存在することに気がついた時点での対処（以降、「初動対応」という。）手順を備え、効果的なインシデント対応措置を確実に行うことを可能にする。

APT は執拗に繰り返し攻撃をおこなうため、インシデント対応においては完全な封じ込めや根絶は困難であることを常に留意する必要がある。対応費用の問題や知識不足により、検知できた端末のマルウェア感染への対応を実施しただけでインシデント対応を終えてしまった場合は、攻撃者のネットワークへの侵入を排除できず、その後の長期間にわたり、潜入・横断的侵害・活動を継続され、企業や組織の事業にとって重要な情報を窃取、改ざんされることにつながりやすい。

[16] NIST SP 800-61, "*Computer Security Incident Handling Guide*（コンピュータセキュリティ・インシデント対応ガイド）"
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

2.3. リスク許容度の評価と管理策の実装

準備段階では、リスク許容度の評価結果に基づき、様々な管理策を検討した上で実装することになるが、絶対確実な管理策は存在せず、残存リスクは避けられない。そのため、インシデント発生時にすみやかに報告するなどの仕組みが重要である。組織内でインシデントの影響を押さえ込むことも重要であるが、APT を含む深刻度の大きなインシデントの場合は、防御・復旧のために外部組織との連携の必要性が高まる可能性がある。最終的にインシデント対応が終了した後に、対応に要したコストや手順の不備などを再確認し、将来に向けたインシデント防止のための取り組みについて検討するための報告書を作成することも重要である。

2.4. 事前準備のポイント

準備段階のポイントは、以下の３つが挙げられる。

- **ベースラインの確保**—リスク低減措置（攻撃対象領域を縮小する管理策）を実施する
- **セキュリティ訓練の実施**—セキュリティチームおよび従業員に対し、脅威への理解を深める
- **トレーニングおよび演習**—セキュリティチームのメンバが、最新のツール・脅威に精通しているようにする

適切にインシデント対応を行うためには、組織のセキュリティ管理策、ネットワークの監視および管理、運用に対して、要員、プロセス、技術に適用できるようなベースラインを整備することが重要である。

３つのうち重要なのは要員である。高度な訓練を受けたアナリストは、新しい事態に遭遇しても対処可能な技術とプロセスを有しており、APT に対しても十分な情報に基づいて判断することができる。

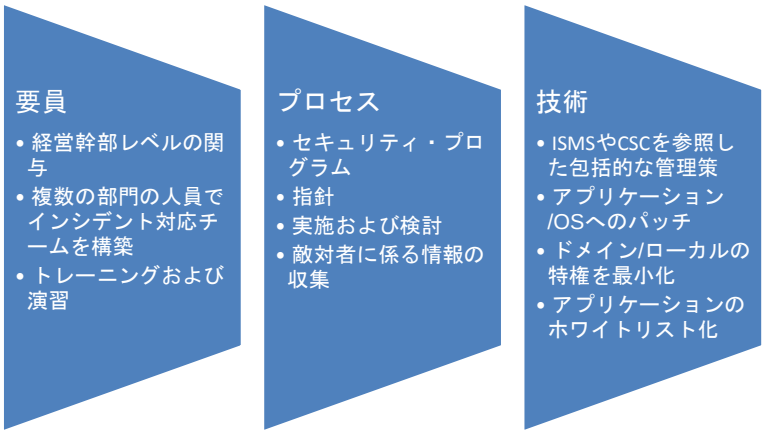


図 10：要員、プロセスおよび技術

セキュリティ全般についての検討は、APT の攻撃機会を阻止するという面でも有効である。組織が強力なセキュリティ管理策を実施するならば、侵入の大半は容易に対処できるという統計が米国・国防防衛産業基盤（DIB）からも報告されている。

米国では、NIST SP800-53 モデルが APT 攻撃に対する対抗策としてよく利用されている。日本では ISO/IEC 27001（情報セキュリティマネジメントシステム（ISMS）の国際規格）といった ISO 規格を使う傾向が強い。ISMS は、多くの侵入の試みを未然防止することが期待できるが、サイバーセキュリティのための完全なソリューションではないことに留意が必要である。従来型の攻撃の成功を防止できるが、標的となった組織は依然として侵害活動に脅かされる恐れがある。「The CIS Critical Controls for Effective Cyber Defense」[17]のようなサイバーセキュリティのリスクを効果的に低減する

[17] Centers for Internet Security “CIS Critical Security Controls” https://www.cisecurity.org/critical-controls.cfm

ためのフレームワークを参照し利用することで、セキュリティチームの能力を向上させ、優先度を考慮した上で、優良な実践策を導入し運用できるようになる。

企業や組織は、セキュリティが確保されていない環境でのリスクを特定する必要がある。IT 資産管理、ビジネス環境の理解、ガバナンスとリスクアセスメント、リスク管理戦略への取り組みが遅れている組織は、リスクの特定を適切に行うことができない可能性がある。多くの組織は現在ある程度侵害されているか、過去に侵害されたことがある。APT に対するインシデント対応措置を準備する際に、特に次のような点を考慮する必要がある。

- どのようにして攻撃を過去に遡って確実に一掃するのか。
- 攻撃を受けている最中に、どのようにして事業運営を持続するのか。
- どのようにして新たなインシデントの発生を阻止するのか。

効果的な準備は、APT に対する防御を構築する際の鍵となる。攻撃者は活動を APT モデルのいくつかの段階（最初の侵入、足場の確保、感染の拡大、機器の一覧化、横断的侵害、持続的なアクセス、目標に対する活動、など）を通して行い、インディケータの一部はその過程の各ステップで明らかとなる。APT の防御に集中的に取り組む場合には、こうしたインディケータを見つけることに力を注ぎ、しかるべき対応を図るべきである。従って APT に対するプログラムを構築・実施する前に、まずはネットワークの管理・監視のための強固なベースラインが必要となる。

ネットワークの監視を効果的に行うためには、パッチ管理、パスワード、その他の管理項目をしっかりと把握し、安定した比較的クリーンなネットワーク環境とする必要がある。このようなベースラインを構築することで、企業や組織は何がインディケータであるのか、インディケータを検知するためにネットワーク資源をどのように有効活用するかを理解することができ、セキュリティチームに検知・対応に関する訓練と演習を実施し、APT 活動の検知・対応能力を発揮させることができる。

APT への効果的な対応を行うためには、対応措置に関する指針となる強固なインシデント対応計画が必要である。この計画の立案のためには、組織は様々なインシデントに対しどのように対応していくのかについて検討しなければならない。そして効果的な防御プログラムのための資金を確保し、優先順位を決定し、組織全体の統合を図るため、上級経営陣による防御プロセス全体の承認・監督が絶対的に重要である。

APT への事前準備として、情報資産と権限の棚卸を定期的に行い組織内の情報やシステムの資産管理を十分に実施することは、攻撃後の復旧フェーズにおいて役に立つ。またこのような組織内の情報資産を発見する能力および情報資産の機能を把握する能力を備えることは、侵入が APT である可能性が高いかどうかの判断や、侵入範囲の確定とその後の攻撃者の排除のために役立つ。資産管理の能力を備えるには様々な実現手段があるが、究極的には、システムの追加を検出した際に、インシデント対応チームがその物理的なシステムの位置を容易に探し出すことができることが重要である。

2.5. 脅威の理解

いくつかの基本的なセキュリティ管理策は、APT 以外の脅威からの混乱を最小限に抑えるのに役立つと同時に、組織が APT の標的となった場合に攻撃者に対しさらに高度な技術と複雑な手順を強制し、攻撃の難易度を上げることを可能性にする。攻撃者が利用できるものを最小限に抑えることで組織の対応能力を強化することが、セキュリティに関する有効な基本姿勢となる。時として、APT に焦点を当てたセキュリティ管理策と一般的なセキュリティ管理策との間にほとんど違いがないことが

ある。だが、APT は特定のエクスプロイト[18]や攻撃手順を好む傾向があるため、APT が嗜好する活動の傾向によって、特定の管理策が他の管理策より重要となってくることがある。

セキュリティ管理策の優先順位リストの作成は、複雑な活動（通常は APT 攻撃者によって行われていると考えられる）の上位 20%をより効果的に縮減する。重要な留意点は、セキュリティ管理策が十分でない場合、APT とそれ以外の一般的な攻撃を区別できなくなるということである。優れたセキュリティ管理策を備えることにより、フォレンジックとインシデント対応に対する適応性が増すだろう。

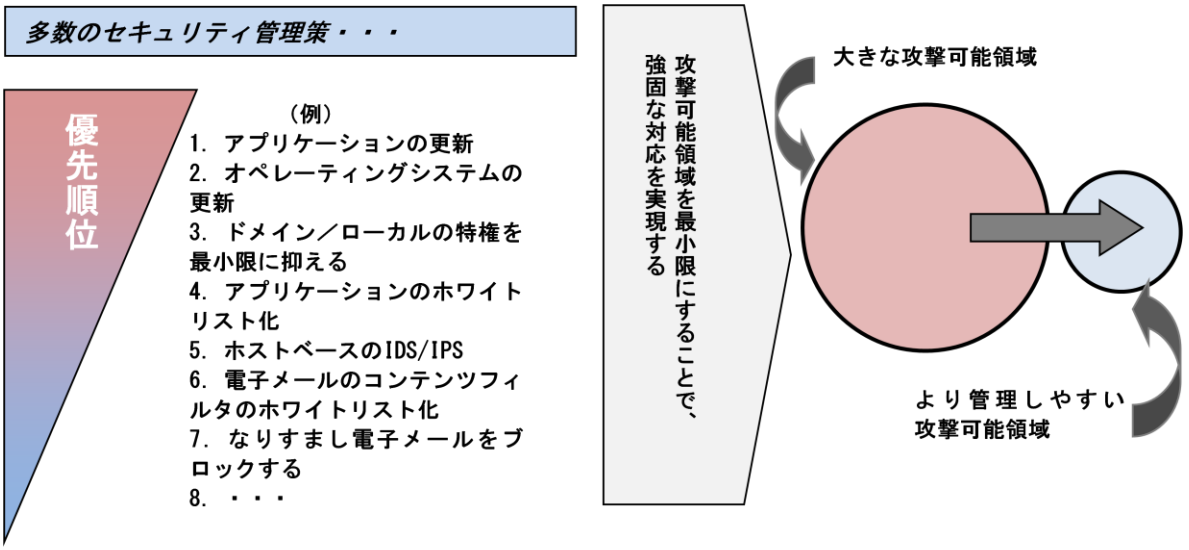


図 11：攻撃可能領域を縮小するためにセキュリティ管理策に優先順位をつける

オーストラリア国防省は、標的型サイバー侵入に対処するための 35 の戦略リストを公表している[19]。このリストを標的型攻撃に対するベースライン防御を確実に自組織に備えるための一例として考慮することが推奨される。米国の主要企業と国際企業がこのリストを、APT に優先順位を付けて対処するために採用している。このリストは、攻撃者の侵害をどの程度防げるかという効果の度合いに応じて順位付けされている。

オーストラリア国防省による、標的型サイバー侵入に対する 35 の戦略のリスト
http://www.asd.gov.au/infosec/mitigationstrategies.htm

さらに、この文書ではリストアップされた様々な戦略を実施する際の具体的な留意点について言及されている。こうした戦略の多くを確実に実施することで、攻撃者が攻撃可能な対象領域を大幅に縮小することができ、その結果 APT 攻撃者はさらに複雑な攻撃方法を使わざるを得なくなり、攻撃側のコストを引き上げることになるだろう。

図 13 は、ISO/IEC 27001 のセキュリティ管理策によって示された様々な重点分野の一部を示しており、こうした管理策を実施した場合どのような状況になるのかを知る上で参考になる。こうしたセキュリティ管理策を実施するためには、環境、アーキテクチャ、脅威情勢などの変化にあわせて情報を

[18] エクスプロイト (exploit)とは、ソフトウェアやハードウェアの脆弱性を利用した悪意ある行為を行うために書かれたスクリプトのこと。

[19] オーストラリア国防省：Strategies to Mitigate Targeted Cyber intrusions（標的型サイバー侵入への戦略）、2011 年 7 月 21 日

更新する必要があるが、有効なベースラインがあれば、こうした情報の更新を比較的タイミングよく実施する事ができるだろう。これらのセキュリティ管理策は、人材に関するセキュリティや、意図的なものとそうでないものを含む内部者による脅威などを扱う。組織、指針、およびリスク管理といった概念についても触れている。主要なセキュリティ管理策には、コミュニケーションや業務管理、資産管理を含む。これらはセキュリティ指針や手順が最新で、且つ現在の脅威に対応したものであることを裏付けるものとして重要である。最後に、コンプライアンスおよび事業継続性を担保することで、事業および利害関係者のニーズにセキュリティの観点から確実に対応することになる。

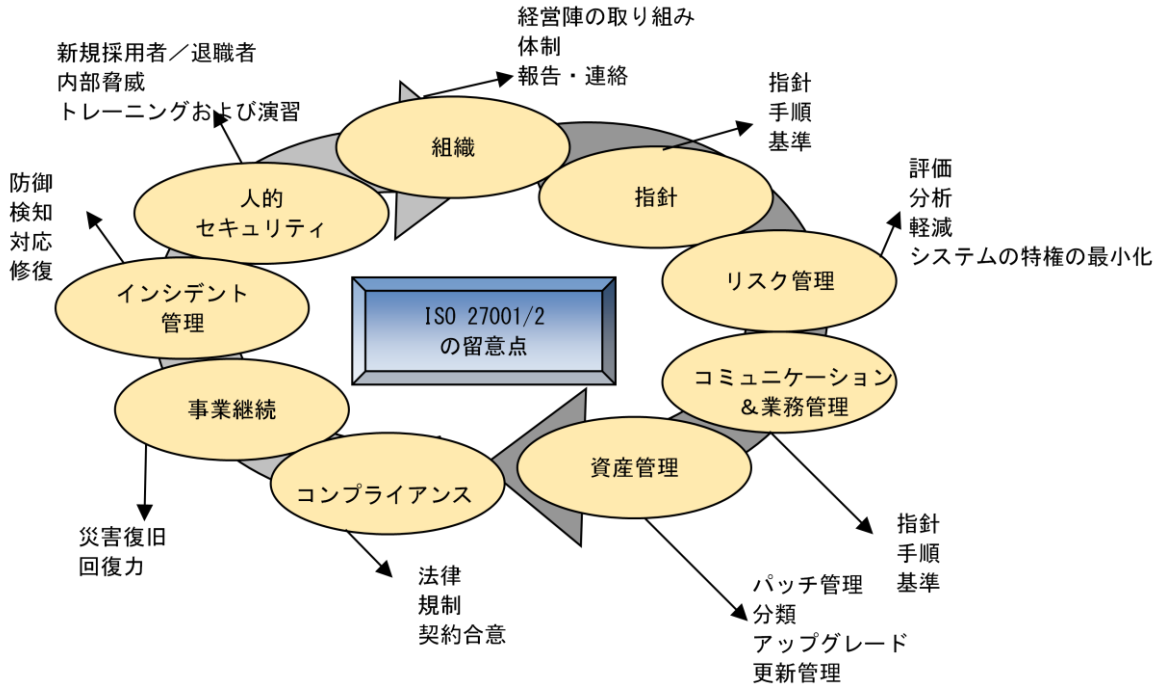


図 12：ISO/IEC 27001 におけるセキュリティ管理策の留意点

2.6. 情報連携と共有

APT 攻撃者に係わる情報を収集および交換する枠組み[20]

インディケータを受け取った時は、それが侵入を発見するために十分詳細なものかを判断する必要がある。もし十分詳細なものでない場合は、外部組織等との情報共有関係を利用して、判断に必要な追加情報を得ることが重要になる。十分詳細である場合は、その侵入が APT である可能性が高いかどうかを判断しなければならない。APT である可能性が低い場合は、標準的なインシデント対応手順を実施することでよいかもしれない。一方で既存の APT プロファイルの中にこうしたインディケータと一致するものが存在する場合は、ネットワーク内で APT が活動していることはほぼ確実であり、本ガイドにあるインシデント対応措置を実施すべきである。

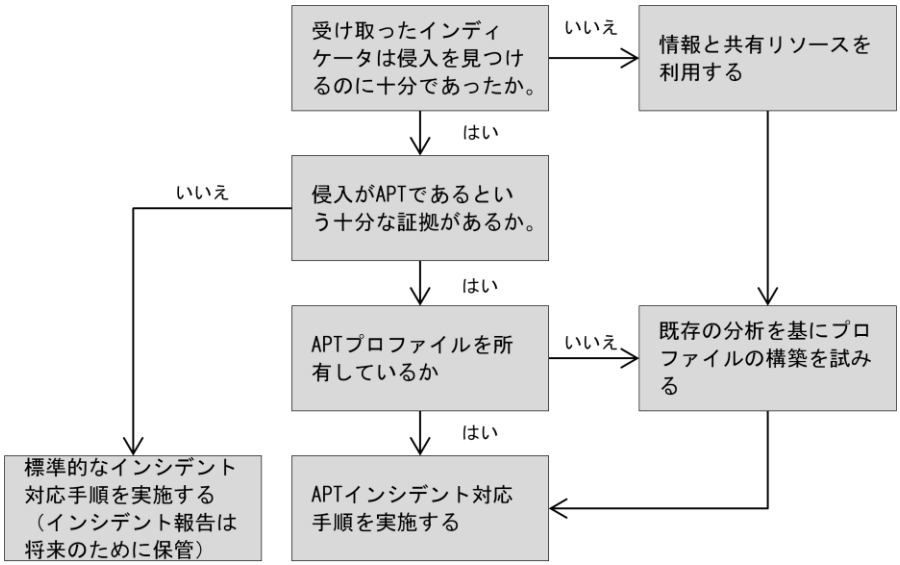


図 13：インディケータを活用したインシデント対応手順の切り分け

攻撃者に係わる情報の収集は重要であるが、外部ベンダから情報を得ている場合は、注意する必要がある。攻撃者に係わる情報のうち、外部ベンダから購入可能な情報や無料で受け取れる情報は、攻撃者に既に知られている可能性がある。

組織内のインシデント対応プロセスの中で抽出された攻撃者に係わる情報については、適切に扱われるように情報の共有・保存のためのセキュリティ管理策を整備し、最善の注意を払う必要がある。これらの情報が攻撃者に知られた場合、攻撃者は使用するマルウェアのコードを更新し、侵入検知・防御システムのシグネチャやアンチウイルスソフトの効果を無効化するかもしれない。

APT は、標的とする企業や組織が、外部のパートナー等との間で、正式な合意に基づいて攻撃者関連情報の共有を行なっているかどうかについて関心を持つだろう。電子メールを使ってやりとりする情報は攻撃者に知られる恐れがあるため、攻撃者関連情報の通知を行う際はまず電話で連絡し、その後に、安全なポータルへのアップロードや、直接対面して情報交換を行う方がよい。

外部ベンダから提供される攻撃者関連情報の使用には、前述のような制約があることを考えると、同じ業界の企業や関係する組織同士で攻撃者関連情報とインディケータを共有することは、大きなメリットがある。ビジネス上の競合相手と情報の共有関係を確立することは、経験にそぐわない考え方かもしれないが、APT は通常、一つの業界全体を狙うことを考えると、情報の共有によって関係者すべての利益を向上させることが可能である。このような共有関係は米国の防衛産業基盤（DIB）では広く見られ、企業が以前は一切交流のなかった競合他社と情報を共有する例がよく見られる。攻撃者が金銭を盗むために金融機関を狙う場合を例にとれば、ある銀行で用いられた攻撃手法は他の銀行に対しても同様に用いられる。ある企業とその競合企業には、相当な損害を一斉に与える能力のある共

[20] 攻撃者の情報を収集し交換するためには、何をどういう形で交換するかをあらかじめ定めておくことが効率的であり、このことを「スキーマの共有」という。

通の攻撃者がいるため、競合企業間で情報の共有関係を築くことで、それらの企業は各々の長期的な成功を強固にできる。

次の疑問は「何を共有するか」となる。この疑問に対する最善の答えは「攻撃および侵害のインディケータ」を共有することである。つまり、組織のネットワークの外における APT 活動（攻撃方法、企業に対する機密情報の収集）を示すインディケータ、および特定の APT 攻撃者が使うツールやマルウェアに関連するインディケータである。 タイムリーであることが、インディケータの価値を決定する上で重要となる。タイムリーな情報共有により、情報共有の枠組みに参加している組織は、データを速やかに解釈・分析することができ、インディケータに関係のある攻撃者を把握し、攻撃者に合わせたより適切な対応をすることが可能となる。対応を実施した後、必要であれば対応結果について組織間で話し合い、情報共有プロセスを向上させることを検討してもよい。

2.7. 予防的なログの保持

予防的なログ保持
-DNS ログ
-プロキシ ログ
-ファイアウォールログ
-NetFlowログ
-サーバ ログ
-ホストログ

図 14：保持を検討すべきログ

APT 対応のための保持しておくべきログの種類

様々なネットワークデバイス、サーバ、ワークステーションから集められたログは、APT の活動が行われた場所を正確に特定するために使うことができる。こうしたログを記録し保存するプログラムを構築する際にいくつか考慮する点がある。

- どのログを保存するのか
- どのようなフォーマットで保存するのか
- どの位の期間ログを保存するのか
- どのようにしてログを保護するのか

APT 侵入の範囲を特定するために、一部のログについては長期間保持する必要がある。個別の状況によっては、ある種のログが他のログより重要度が高くなることがある。企業や組織は、インシデント対応者が攻撃者を探す時に一般的によく参照する様々な種別のログをできるだけ多く維持したいと思うだろう。JPCERT/CC による過去の米国業界のベストプラクティスについての調査では、図 15 に示す 6 つのログ種別が分析において最も有用と判断された。

こうした特定のログは、収集後長期間（1 年以上）保管することで、長期的な時間軸での攻撃者の活動の調査に有効利用できる。推奨されるログ保存ポリシーについて、ベストプラクティスや様々な機関からの情報やその他の要素をもとに検討するべきである。こうしたログは、攻撃のインディケータを見つけるのに使う一般的な手段の一つであり、ログをなるべく長期間残すことで、最初の侵入や、侵入の早い段階での攻撃者の行為に関する証拠の発見につながる可能性がある。こうしたタイプのログの多くは、何年も保管することが可能で、インシデント対応者が現在の侵入の規模を把握するのに役立つとともに、場合によっては、攻撃者が何を目的としているかについての手がかりを提供し、攻撃者の特性を判断するのにも役立つ。

表 4：APT に備えてログを保持した場合のプラス面とマイナス面

ログ種別	プラス面	マイナス面
DNSログ –ネットワーク上のホストからの完全修飾ドメイン名についてのクエリ	比較的容易に取得でき、特定のサイトへの潜在的アウトバウンド・トラフィックについて重要なインディケータを含んでいる。	保存量が限られているため、ログのローテーションが頻繁に行われ、履歴データによる解析ができない。
プロキシログ – LAN上のIPアドレスが要求したサイトやページ、ファイル[21]	比較的容易に取得でき、Web要求に関する重要なインディケータを含んでいる。	保存量が限られているため、ログのローテーションが頻繁に行われ、履歴データによる解析ができない。
ファイアウォールログ– インターネット上のIPアドレスに対するアウトバウンド接続（IPアドレスおよびポート）	簡単に取得でき、長期間保管が容易。アウトバウンド接続の情報を提供する。	SIEM や他の相関関係デバイスやアプリケーションなしには、分析が複雑になりデータの意味を理解することが困難になる。
NetFlow –アウトバウンド接続およびインバウンド接続（IPアドレスおよびポート）のトラフィック種別ごとの概要、およびネットワーク上で非常に頻繁に接続を行う者（トーカー）の概要	容易に取得でき、保存にあまり場所を取らない。セッションおよびホスト間のトラフィック量に関する情報を提供する。	非常に基本的な情報のみ取得する。分析者が必要な情報をすべて提供できるわけではない。
サーバログ – 各サーバ（数は少ないがより重要なシステム）のアクセスおよびログイン要求（成功または失敗）。	他のインディケータと相関関係がある可能性のあるサーバの異常な動きについて詳細な情報を提供する。	重要な警報を引き出せる可能性があるが、大量の不必要な詳細情報に終わってしまう可能性もある。
ホストログ – 各端末（従業員が使う全てのコンピュータ）のアクセスおよびログイン要求（成功または失敗）。（syslogやWindowsのイベントログを含む。）	他のインディケータと相関関係がある可能性のある端末の異常な動きについて詳細な情報を提供する。	重要な警報を引き出せる可能性があるが、大量の不必要な詳細情報に終わってしまう可能性もある。

タイムスタンプに関する留意事項

センサーには信頼できる時刻源が必要であり、NTP 同期時刻源から時刻を取得するように設定し、すべてのイベント（アラート）に、正しい Coordinated Universal Time（UTC; 協定世界時）のタイムスタンプが必要である。タイムスタンプがなければログを正しく分析できない。すべてのログおよびセキュリティシステムへのタイムスタンプには UTC を使用することを検討していただきたい。様々なインテリジェンス情報を含む、多くのレポートでは UTC が使用されている。グローバル展開する企業組織において時刻帯を越えて分散するシステム間でのログの突合せを行う場合や、その他の国際連携を考慮するならば、日頃からタイムスタンプには UTC を使うのが良い。これは連携した活動を促進し、アナリストたちが必要に応じて手作業でログを精査する際にも役立つ。センサーに UTC の他に現地時間を設定できる場合は、現地時間を利用してもよい。

[21] フォレンジックの現場ではファイルサイズが一定の判断基準となることがある。攻撃者によって送信されたファイルが暗号化されその内容を特定できない場合、ファイルサイズが手掛りとなる。ただしファイルの分割により見た目のファイルサイズを小さくしている可能性にも留意すべきである。

侵入の時間軸を再構成できる DNS ログやプロキシログなどのログは有益であるが、時差やタイミングソース（時刻源）の不整合によって起こりうるタイムスタンプの食い違いに留意する必要がある。前述のとおり、ベストプラクティスは時刻帯に関係なく UTC 時間を使っている。タイムスタンプとログは攻撃者によって改ざんされる可能性があるため、ファイルの作成時間、変更時間、アクセス時間については、安全に保管されていない場合は信用しないことである。

ログ収集能力の判定

ネットワーク上の APT 活動を完全に把握し、対処するためには、アーティファクト（サイバー攻撃の痕跡）を追跡するためのシステムが不可欠である。追跡のための強力なシステムは、侵害されたホスト、横断的侵害のインディケータ、ログファイルのレビュー結果、SIEM などで構成される。インシデント対応チームは、このシステムに対するすべての入力、アーティファクトを確認する必要がある。システムはデータベースと同程度に複雑であるかもしれないし、スプレッドシートのような単純なものかもしれない。ベストプラクティスは、ログ取得を適切に行い、ログの一元的集約を図り、関連する証拠をその検出内容、場所と時間および収集方法とともに保存することを薦めている。

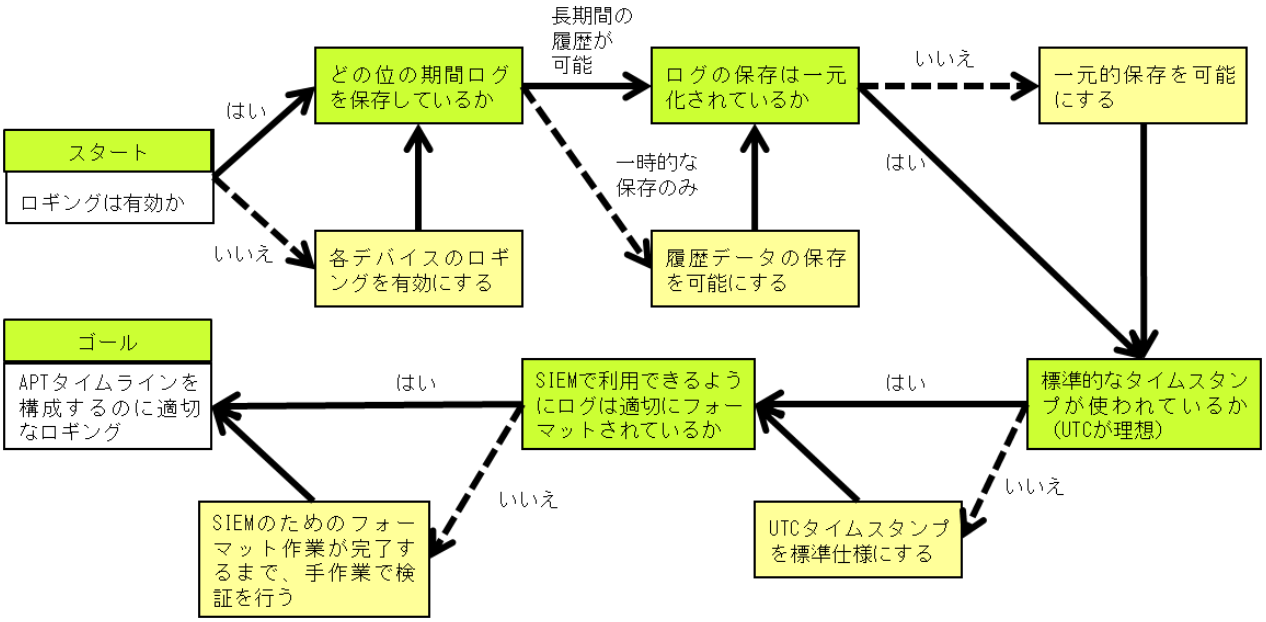


図 15 ログ収集能力の判定

ハイレベルな取り組み事例

ログの一元的集約と SIEM（Security Information and Event Management）ツールの活用

情報を一元的に集約することで検索および相関付けを容易にするため、ログの一元的集約について考慮する必要がある。様々なソースから必要なログを一度に引き出すことはとても不可能である。また、ログがソース上で攻撃者によって改ざんされる可能性もある。ログを集約することで、保存されたログに対して定期的に履歴の解析を行うことも可能になる。

一元的に集約された情報を保護し、攻撃者によるログやインシデント対応記録へのアクセスや改ざんを防ぐことは極めて重要である。防御方法には、閉鎖型ネットワーク、片方向通信の使用、またはセキュリティチームのみがログやインシデント対応記録にアクセスできるようにするためにファイアウォールやアクセス制御機構の適切な配置などが考えられる。どの方法を選択するかはともかく、こうしたログは、それらを見つけ出して利用しようとする APT 攻撃者から防御する必要がある。

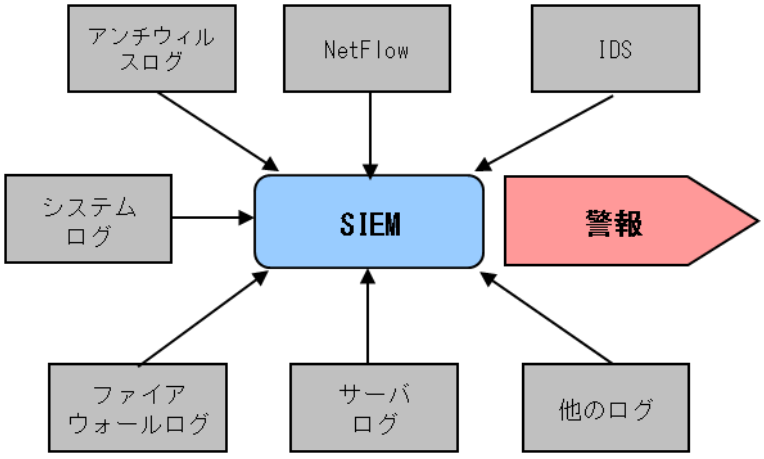


図 16 SIEM はどのように作用するのか

セキュリティ情報イベント管理ツール（通称「SIEM」）は、ログ、侵入検知システム（IDS）、ファイアウォール、および攻撃者の活動の関連づけに利用できるその他のものを含め、多様な情報源から有用なデータを得るために使われる。SIEM の活用によって、アナリストはネットワークを巡る様々な機器やシステムからの情報を結合し、活動のしきい値に基づいて警報を得ることができるため、APT に対処する際の重要な機能となる。以前はネットワーク上の特定の活動を確認するために IDS が主に使われていたが、IDS から得られるデータは検知するためのシグネチャのあるもの、および IDS が設置された場所に限られていた。SIEM を利用することにより、こうしたデータを他のログと結合し、そのパターンに基づいて検知し、検知された事象に関して警報を発することで、セキュリティチームは攻撃者が活動を行っているかを判断することができる。SIEM には、単体の機器やソフトウェアとして販売されているもののほか、セキュリティサービス事業者等がマネージドセキュリティサービスの中で SIEM 機能を提供するものがある。

2.8. ポリシーやガイドラインの整備

企業や組織は、APT を含むサイバー攻撃に対応するため、既存の危機管理や情報セキュリティリスクマネジメントなどの枠組みを補完する、サイバーセキュリティに関する新たなポリシーを整備することがある。サイバーセキュリティ戦略やポリシーを独立した形で整備する必要はないが、どの部署がサイバー攻撃への対応を主管するのか、サイバーセキュリティに関するリスク管理はどの部署が担当するのか、それらの評価はどの部署で行うかなどは、上級経営陣の方針を確認しながら、既存の関係部署の役割を考慮し、組織としてのコンセンサスを得た状態にする必要がある。
サイバー攻撃を想定したインシデント対応について事前にリスクシナリオを検討し、対応計画を立案し、その結果を包括的なガイドライン等の形でまとめることは、インシデント対応プロセスの可視化の観点からも有効である。
企業や組織によっては、リスク管理規程や危機管理規程、事業継続計画、IT-BCP などサイバーセキュリティに限定しない包括的なインシデント対応ガイドラインを整備している場合がある。サイバー攻撃対応のための効果的、かつ、迅速なマネジメントの実現を図るとともに、既存のガイドラインとの整合性を維持し、ガバナンスに矛盾が生じないような着意が必要である。

企業や組織における「サイバーセキュリティに係るインシデント対応ガイドライン」の目次例

１． 総則
　　(ア) 目的
　　計画やガイドラインの目的
　　(イ) 適用対象
　　想定しているサイバー攻撃事案
　　(ウ) 定義
　　用語の定義
２． サイバー攻撃への準備
　　(ア) 体制
　　体制・対応組織の概略
　　(イ) サイバー攻撃事案発生時の連絡先
　　関係者の連絡先リスト
　　(ウ) サイバー攻撃事案対応への準備
　　必要な情報の整理
　　教育・訓練
３． 対応計画
　　(ア) 想定しているサイバー攻撃事案
　　想定事案の解説と対応案
　　(イ) 被害レベル
　　事案ごとの被害レベルの想定
　　(ウ) 個別事案の対応プロセス・体制
　　ウイルス感染の対応
　　標的型メール攻撃への対応
　　社外向け Web サーバで異常を検出した場合の対応
　　他、
　　(エ) 標準対応プロセス・体制（共通的なもの）
　　標準的な対応について記載

2.9. インシデント対応機能の整備と人材育成

インシデント対応機能の整備と人材育成について、ロードマップを作成し、中長期的に取り組む企業や組織も増えている。

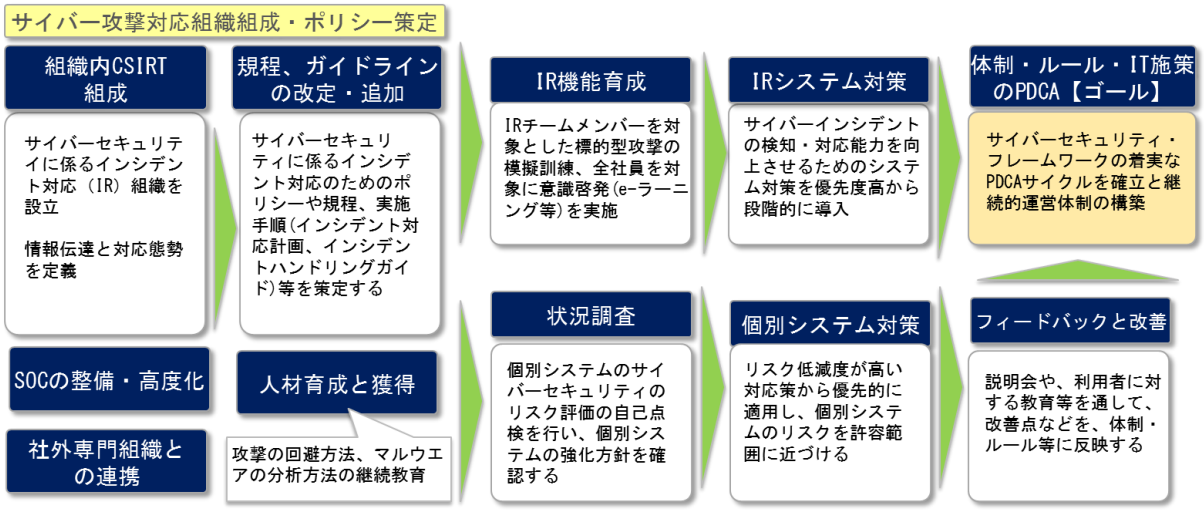


図 17 インシデント対応機能の整備と人材育成に関するロードマップの事例

はじめに、サイバーセキュリティに係るインシデント対応組織を定義し（組織内 CSIRT の組成）、あわせて、SOC（Security Operation Center）を整備し高度化を図る。また、社外の専門組織との連携を同時に開始することが効果的である。

次に、必要な規定やガイドラインの改訂・追加を行うとともに、人材の育成と獲得を行う。サイバー攻撃の回避方法、マルウェア分析方法などを習得した人材を組織内に確保するのは簡単ではないが、必要とされているのは高度サイバーセキュリティ人材である。

さらに、組織のサイバーセキュリティインシデント対応能力を向上させるため、インシデント対応チームを対象とした実機や演習環境を利用した攻撃対応演習や、役職者やシニアマネージメントを対象とした教育訓練の実施が推奨される。インシデント対応のための有用なシステムソリューションを導入することもインシデント対応機能の整備には有効である。

並行して、個別システムのサイバーセキュリティリスクを把握・特定し、もし、安全ではない環境で事業を行っているような状況がある場合は、リスク低減度が高い対策から優先的に導入し、個別システムのリスクを許容度の範囲に近づける必要がある。

これらの一連の改善を通じて、体制・ルール・IT やセキュリティ施策の PDCA サイクル確立と継続的運営体制を構築することがロードマップの最終目標に設定される。

2.10. CSIRT の設置

APT に限らず、サイバー攻撃全般に対応するためには、**① 外部との情報連携、② 内部の各部門へのフォロー、③ セキュリティ管理業務**（サイバーセキュリティや情報セキュリティの区別がない場合も多い）を行う必要がある。これらはいずれも、必ずしも企業や組織に備わっている機能ではないが、近年は、組織全体の対応スピードや品質の向上を目的として、サイバー攻撃のための体制を強化、攻撃を特定・防御・検知・分析するためのツール導入等を行う組織が増加している。

サイバー攻撃への対応体制強化のために、組織内 CSIRT を設置することは大変効果的であると考えられている。ただし、設置のためのリソースを確保することが障害となるケースも多い。

組織内 CSIRT は、図 17 に示すように、リスク管理と危機管理の観点から、インシデントマネジメントを主管し、インシデントハンドリングを実行し危機対応を行う。

CSIRT の有用性の例を以下に記載する。

- 外部とのインシデント対応に必要な信頼関係の構築
- 組織内のインシデントに関する統一された窓口
- 情報セキュリティ（特に、サイバーセキュリティインシデント関連）に関する情報管理

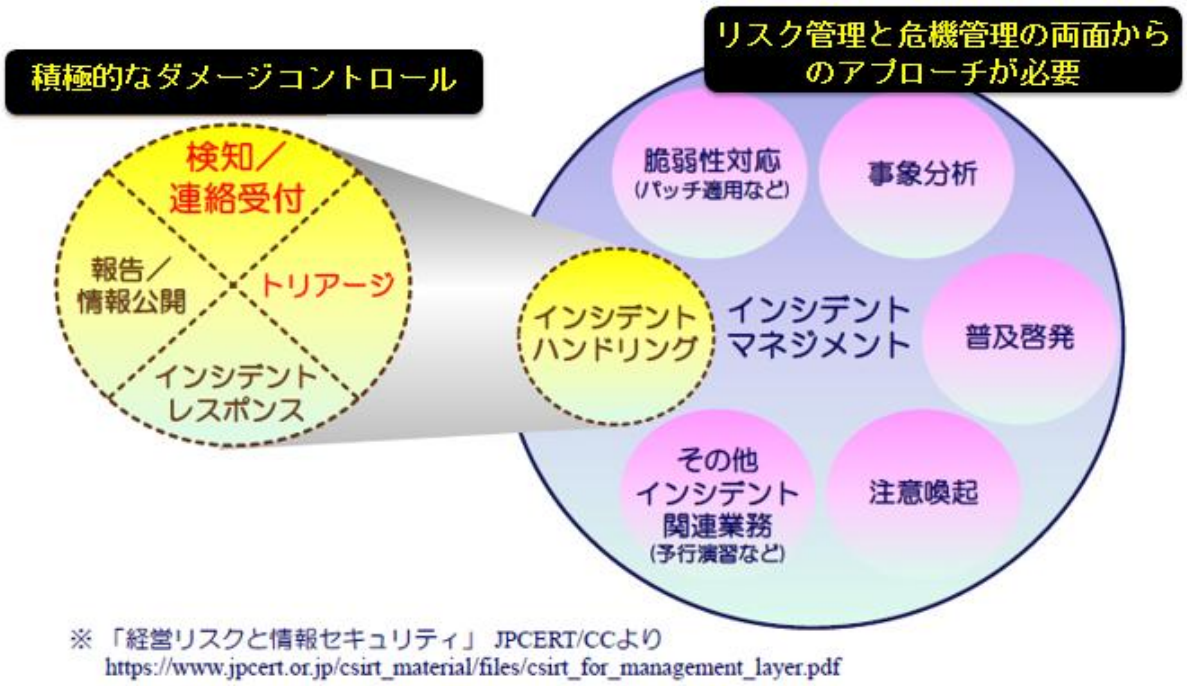


図 17： APT 対応における組織内 CSIRT の位置づけ

2.11. トレーニングおよび演習の実施

トレーニングの実施

トレーニングプログラムは、APT に対する防御を構築、維持、実施するために欠かせない。初動対応のトレーニングにあたっては、スキルと先進的な戦術に焦点を当て、トレーニングを繰り返し行うことにより、セキュリティチームは常にサイバーセキュリティおよび APT 活動の最新動向を認識するようになる。これらの焦点のうちスキルの面では、基礎レベルの知識・スキルを教え、セキュリティチームのメンバ全員のベースラインを合わせるようにする。先進的戦術の面では、メンバに APT に対する監視、検知、対応を行うための深い知識や実施体験を伝える。トレーニングの繰り返しについては、少なくとも年 1 回は APT 防御のために新たに生まれた技術・戦術についてトレーニングを行い、進化する APT 関連の技術・ツールへの認識を高める。APT は絶えず進化しており、社内のセキュリティチームも後れをとらないようにすることが不可欠である。さもなければ、APT 活動を効果的に検知し、対処する能力が損なわれるリスクを生じさせるだろう。

トレーニングと演習

トレーニングと演習は非常に重要である。すべての従業員を対象に検知・対応能力に関する演習を行うことで、プロセスギャップを認識でき、こうしたプロセスに関するトレーニングの成果を実践することができる。
討論を中心とした演習（机上演習、セミナー、ワークショップ、ゲーム）およびオペレーション中心の演習（訓練（ドリル）、機能演習、総合演習）はともに、様々な成熟度にある組織に対し検知・対応能力を評価するために適用できる。また、組織が APT に直面したときに要員、プロセス、技術がどの程度機能するかについての洞察を得る機会を提供する。 演習はトレーニングの一部として利用することも可能である。たとえば、セキュリティチームに対して新しい検知能力のトレーニング用にゲームを使うことができるし、手順や反応時間を向上させることを目的に、既存の検知・対応手順についての訓練（ドリル）を行うことも有効である。トレーニングと演習の重要な違いは、トレーニングは主に個人を対象としており、演習は組織としての対応能力向上を目的としている点にある。
企業や組織は最終的には、既知の APT 攻撃手口に対する防御方法を含む防御戦略文書をどのようにして整備し活用するかを知りたいと思うようになるだろう。何百ものシステムが感染した可能性がある事態に取り組む場合には、不十分なプロセスやその場しのぎの防御戦略では侵入に対処するのは不可能であろう。セキュリティアナリストやシステムの防御の裏をかこうとする高度な侵入に対処するには、確立したトレーニングプログラムや演習プログラムを通じてセキュリティチームが適切な訓練を受けることが非常に重要である。セキュリティチームは訓練を積むことにより反応時間を早め、侵害から対処までの時間を縮小し、データ侵害、窃盗やさらなる侵害のリスクを減少させることができる。またパートナー組織を活用した協働での対処を実践できるようになる。

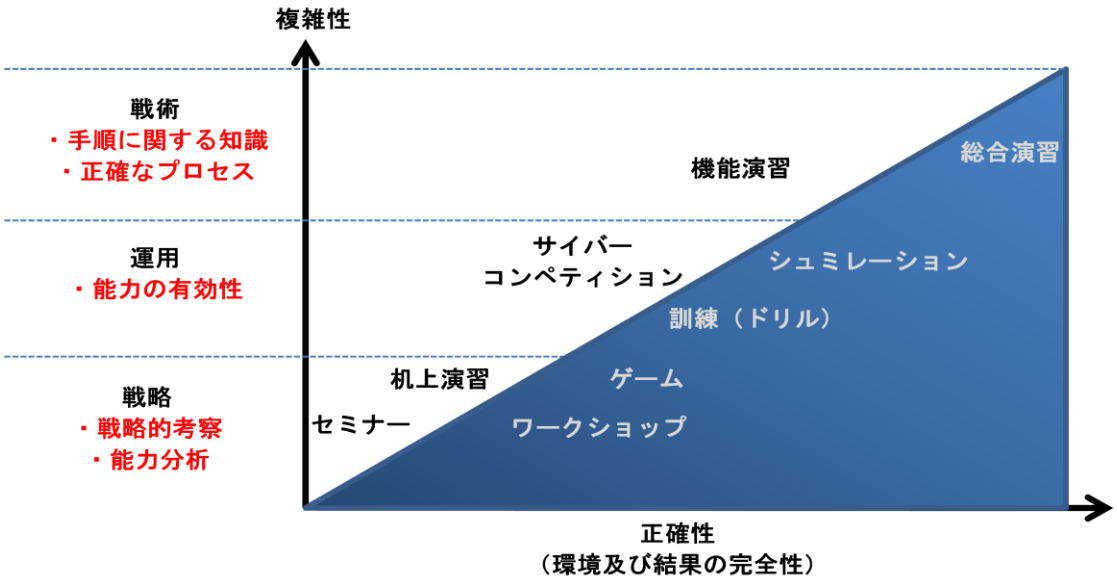


図 18：様々な演習と効果

2.12. インシデント対応計画の検証

インシデント対応計画

サイバーインシデントに備えるための重要なステップは、強固なインシデント対応計画を持つことである。しかし、計画を利害関係者や対応担当者に伝え、実際の対応に沿った方法で検証しその効果を実証しなければ、計画はほとんど意味がない。検証の範囲は、安全と確認されたバックアップを使用した単純な障害復旧以上のものでなければならない。広範囲にわたるインシデント対応計画を検証することで、APT への対処に係わる複雑な問題を把握するのに役立つ。インシデント対応計画の効果的な検証としては、意図的に設けた脆弱性を使って侵入をシミュレーションし、セキュリティチームに実際の攻撃への対処のように対応させるという方法もある。
このプロセスは、組織における変更に関して意思決定権限を持つ上級管理職が管理する必要がある。この上級管理職は通常、インシデント対応計画の検証において発見された弱点や欠陥を補うための人事異動の指示、新技術導入のための支出の承認、組織全体の方向性やビジョンの設定に関する権限と責任を持つ。

① インシデント対応計画の検証の主管となる部課長に対して、作成されたインシデント対応計画を検証できる決定権を与える
② 全社的な業務リスクに基づき、事業における懸案事項と関連する脅威を選別する
③ 全社的な業務リスクに基づき、標的となるシステムを選別する
④ セキュリティ管理者に選別した脅威と標的を伝える
⑤ 現実的なシナリオとなるように、過剰な指図を行うことなく、対応措置を観察する
⑥ 講じられた措置および得られた教訓に関して報告書（レポート）を作成する
⑦ 検証結果を、予想された措置や以前のインシデント報告と比較し、レポートをレビューする
⑧ 得た教訓がすべて組み込まれるように、必要に応じて計画を更新する
⑨ 更新・改善を加えた手順で計画を再度検証する（必要な場合）

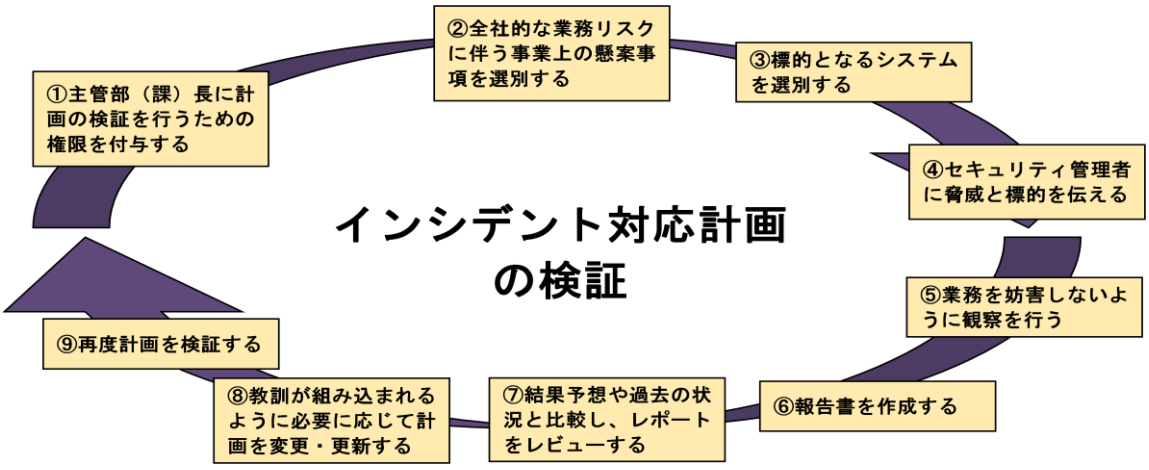


図 19：インシデント対応計画の検証

第3章. インシデント対応プロセス

3.1. APT の検知と初期ステップ

APT の検知

APT は、特定の企業や組織を対象とし、攻撃範囲を選別した手法をとるため、攻撃範囲が限定的であり、従来のような不特定多数を対象とした攻撃とは異なり攻撃の実態を把握するのが難しいという特徴がある。現実のケースでは、外部からの情報でインシデントが発覚することが多い。しかしながら、有用なシステムソリューションを導入し、インバウンドとアウトバウンドの通信について適切なシグネチャを設定した上で、常時分析・監視を行うことで、攻撃や疑わしい通信を検出することが可能となる。

外部との情報共有によりインディケータ情報を入手し、インバウンド通信の発信元やアウトバウンド通信の送信先の IP アドレスをブラックリストに登録しておくことで、該当の攻撃の検知につながる。

組織が APT による攻撃を検知するきっかけは、ファイアウォールやプロキシなどの通信ログ、特に、内部から外部へのアウトバウンド通信や内部システム間の通信を分析した際にインディケータ情報と一致する通信があった場合や、端末の振る舞い検知型のウイルスチェックソフトで異常を検出した場合、IT 資産管理システムがネットワーク上にホワイトリストに無いハードウエアを検知した場合などがある。APT による攻撃では、ソーシャルエンジニアリングによってユーザの認証情報が標的となる場合も多い。通常とは異なる時間帯にログオンしたり、異なる場所で同時にログオンするなどのユーザ認証が行われた時間に矛盾がないか等のモニタリングも APT の検知には有効である。

攻撃の検知に成功した場合でも、初動の段階で APT による攻撃の可能性があると判定しないまま対応を終了し、その後の被害を拡大するケースも多い。

実際に自組織のネットワークに侵入され被害を生じた組織からは、次のような反省があった。

- ✓ 8 ヶ月前に他の組織との間で情報共有ができていれば侵入され続けることはなかった。**情報集約と情報共有の取組み**があれば、もっと早く気付けていたかもしれない。
- ✓ 最初の処置で他のバックドアを駆除できていれば 3 日後以降に再侵入されることはなかった。**ネットワークやシステムの構成把握**ができていれば、再侵入を防ぐことができたかもしれない。
- ✓ ユーザや端末の情報以外にもデータを持ち出された可能性はあるが内容は特定できていない。**情報資産の把握・保護**が不十分なため、被害は何だったのか、攻撃者の狙いが判らないままで終わっている。
- ✓ 「攻撃は繰り返され、インシデントは再発する」と考えるべき、と外部ベンダから言われたが、いつ終息宣言をだせばよいのか。**脅威との共存を意識した環境作り**と言われてもどう取り組んでよいか分からない。

攻撃の防御・検知に有用なシステム面での対策

APT に備え対応するためには、事前準備として IT 資産構成（ハードウェア、アプリケーション、ID 管理）を徹底することや、APT による攻撃を想定した高度な防御・検出技術を利用することが重要である。有用なソリューションは、防御機能と検知機能の両方を有することが多い。具体的には、次のようなレイヤで適用が可能である。

- 次世代ファイアウォール（NGFW: Next Generation Firewall）
- 侵入防御デバイス（IPS/IDS）
- 高度な脅威防御アプライアンス

- Web アプリケーションのセキュリティ
- 電子メール・コンテンツのセキュリティ
- Web コンテンツのセキュリティ[22]
- エンドポイントのセキュリティ
- IPsec 及び SSL VPN のリモートアクセス接続

これらに加えて、自動モニタリングや、相関分析を行うことで分析能力を改善する目的で、SIEM を導入する組織は増加傾向にある。

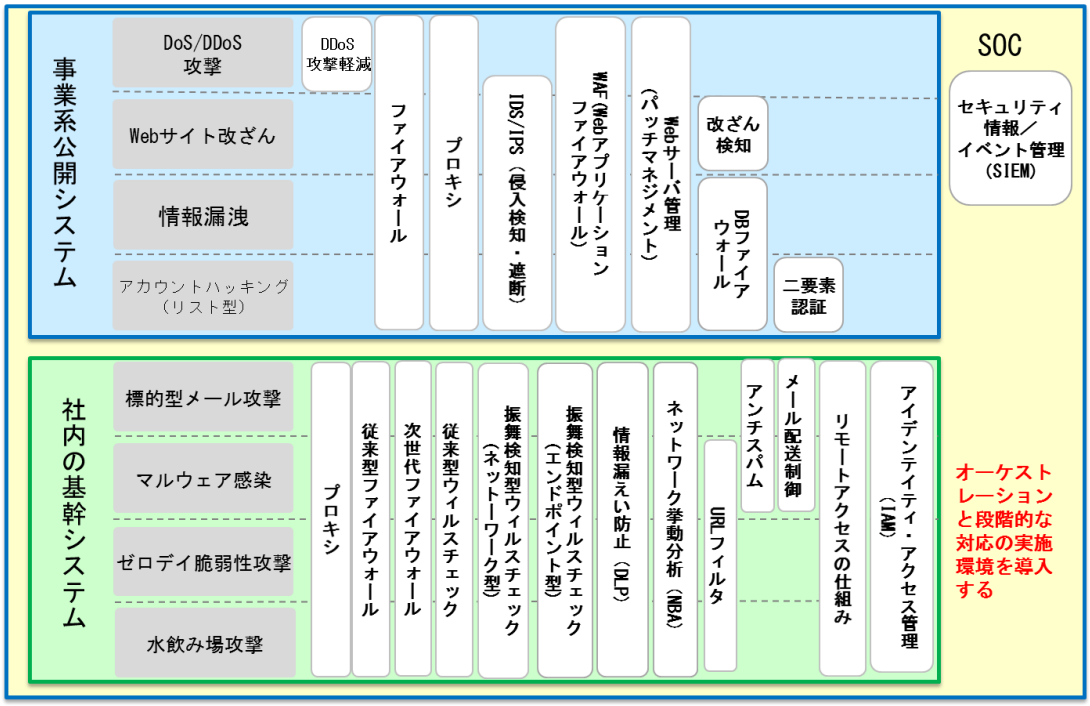


図 20: 攻撃の防御・検知に有用なシステム対策の適用例

[22] インターネット通信のフィルタリングやモニタリング、URL フィルタリング設定、疑わしいホストのブロッキングなど。Secure Web Gateway（SGW）と呼ぶこともある。

3.2. APT 攻撃に関する通知と検証

企業や組織は、自社のネットワーク上で APT が活動していることを様々な手段で知らされる可能性がある。本セクションではこうした通知への初動対応措置について説明する。最初の通知を受け取った時に、慎重に計画された対応プロセスが実行されるようにすることが重要である。措置には、取るべき措置、避けたほうがよい措置がある。APT の疑いのある活動に対しては、それが実際に APT であることを確認するために「トリアージ」を行うべきである。いったん APT であると認識されたら、組織はインシデント対応にリソースを結集し、APT 攻撃者に対する措置を実行する場合は、実行結果に対するリスク評価を行う。この際の留意点を本節で示す。最後に、内部 （従業員）および外部（マスコミ）とのコミュニケーションについて留意点を述べる。 組織は、APT 対応を開始する前に本節で述べる留意点について討議することで、タイムリーに計画を立て対応を行うことができる。

米国では「通知の 94%は政府からで、そのほとんどが電話による」とマンディアント社は述べている。CERT や法執行機関等は様々な企業の POC（Point of Contact: 連絡窓口）のリストを保有しており、それらの組織と直接連絡を取っている。

先進的な企業では組織間の情報の共有に専用のポータルを使うまでに進歩している。しかしこれには次のようなリスクが内在する。情報共有ポータルが侵害された場合、攻撃者は侵害を受けた企業のアナリストが見ているのと同じ情報にアクセスできることになる。またポータルに対するサービス妨害（DoS）攻撃により、連携先やサービス利用者のポータルへのアクセスが不可能になるかもしれない。ポータルにアクセスする個々の登録メンバのアカウントが攻撃者に侵害され、攻撃者が重要性の高い情報にアクセスできるようになるかもしれない。総じて、こうした問題からのリスクを軽減するため、攻撃者に係わる情報を保管した機器を他のネットワークアーキテクチャから隔離するように、十分に注意する必要がある。

情報共有関係を強固で信頼できるものとするには、それを構成するすべての企業や組織は、それぞれの組織において誰が関与しているかを互いに把握しておく必要がある。攻撃者は高度なソーシャルエンジニアリング手法を使い、標的とする組織になりすます可能性があり、組織内のプロセスに精通し、そのプロセスを利用して情報共有組織間の情報のやりとりを模倣し攻撃に用いる可能性がある。したがって、連携先やサービス利用者や JPCERT/CC からの連絡はすべて、それが真正なものであるかどうかを認証する手順を整えておく必要がある。たとえば電話で連絡を受けた際には、情報や姓名、電話の時刻を記録した後に電話を一旦切り、あらかじめ整備してある連絡先リストにある連絡方法を使って通知してきた組織に電話をかけ直す。攻撃時にインターネットアクセスが遮断される場合を考慮して、そのような場合でも攻撃者に係わる情報源や情報共有の枠組みで運用されるポータル等にアクセスできるように、連絡先リストのローカルコピーを保持するか、連絡先リストを別のインターネット接続方法を備えた独立したシステムに保存するほうがよい。連絡先リストの情報は機密性が高いものであるため、企業や組織は、リストに対する侵害や窃盗のリスクを低減するためにスタンドアロンシステムに保存することを考慮したほうがよい。連絡先リストのハードコピーも安全な場所に保管しておくべきである。

APT 侵害下における通知の扱い

APT 攻撃者は、セキュリティチームが APT 活動について通知を受けたときに使う手順を把握している可能性がある。APT 攻撃者はこの手順やソーシャルエンジニアリングで得た情報を、調査の妨害や、企業がどの程度攻撃を把握しているかを探るために巧みに利用するかもしれない。これはサイバー犯罪者やハクティビスト（社会的・政治的な主張を目的としたハッカー）などの組織にとってはリスクが高いものの、前例がないわけではない。通知の取扱いに関する強力なプロトコルを持つことは、優れたセキュリティを実現するために有益である。

情報共有の関係にある組織間の連絡に関して、通知をおこなう相手の組織がネットワーク侵害されている可能性がある場合、電子メールによる連絡は必ずしも薦められる方法ではない。メール個人フォルダが盗まれるか傍受された場合、攻撃者に組織間の通知情報がフィードバックされる可能性があるからだ。JPCERT/CC や業界のパートナー、外部 CSIRT 等の情報共有パートナーとの間に安全なコミュニケーション方法があるならば、それが情報交換に利用可能な標準外のコミュニケーション方法として容認されるだろう。さらに、適切に安全管理されている情報共有ポータルがある場合、それを協力連携の関係にあるメンバ間や JPCERT/CC への情報の伝達を行うための、標準外のコミュニケーション手段として利用することも可能だ。こうしたコミュニケーション例を以下に示す。

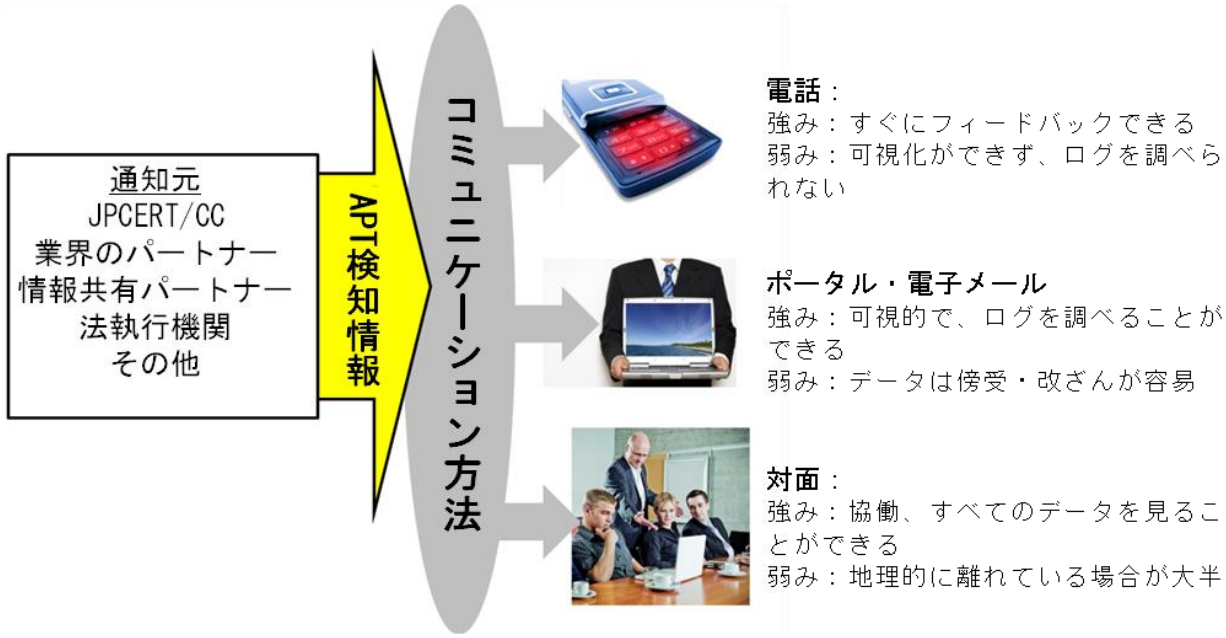


図 21：コミュニケーション方法別の留意点

通知元の組織から攻撃を受けている組織へのコミュニケーションを開始するいくつかの方法がある。最も一般的な方法は、電話、標準外の電子メールコミュニケーション、共有するポータルを使う方法、または直接会って連絡する方法である。連絡方法の選択は、通知する内容の重要度や、通知先の組織がその方法に対応しているか否かに依存する。

- ネットワークへの高度な侵入に関する通知は、電話で行われることが多い。第一段階は組織内の連絡窓口を見つけることである。情報は直接電話で提供すべきではなく、侵入について討議するための直接の面談またはリモート会議を設ける。
- ポータルにも限界があり、またポータル自体が攻撃者に狙われる可能性がある。ポータルが安全に運用されているならば、場合によっては追加的な標準外のコミュニケーション手段となり得る。
- 対面でのコミュニケーションは時間が長くかかり、情報量が限られる可能性がある。対面は一般的に、APT がほぼすべてのネットワークのセキュリティ管理策を奪い、信頼できるコミュニケーション手段がないという最悪のシナリオのために留保される。

ある侵入行為が APT であるかを判断する際には、APT が 3 つの基本的な要素－標的、目的、攻撃者－が必要であることを考慮し、この 3 つの要素を分析する必要がある。とはいえ、こうした判断を行うのは、その組織が狙われているか否かを示す材料に基づいて行われる極めて複雑な作業である。

APT の最終的な標的と目的は、攻撃対象である企業や企業パートナーに対する競争優位性を得るために利用するための何かかもしれないし、一つの業界全体から搾取するための大計画の一部であるか

もしれない。侵害の標的と目的をともに分析することは、その侵害が APT に関連したものであるかを判断する上で役立つ。企業の合併・買収に係わるファイルは、その情報の機密性の高さゆえに APT の標的とされやすい。パスワードファイルは最も機密性が高い情報であるが、APT だけでなく他の一般的な攻撃においても標的とされ、常に APT による侵害を示唆するものではない。APT 活動を示唆するものとしては、データ窃取、企業情報や専有データの窃取、データの破壊や削除が考えられるが、APT が将来の活動のためのアクセスを確保すること自体が目的となる可能性もある。重要なシステムへの直接攻撃や横断的侵害は APT を示唆するかもしれない。反対に、Web サイトの改ざんが目的である場合は通常 APT によるものではない。

検知した攻撃について、これまでに自組織または他組織で検知された攻撃との関連付けと比較を行う必要がある。このステップは重要であるが、高度なインテリジェンス能力を要求されるため、単独組織での実施には限界がある。JPCERT/CC や ISAC などの情報共有組織と連携し、情報を収集し判断する必要がある。

通知において最も重要な留意点の一つは、通知の結果次に何が起こるかを把握することである。潜在的な影響を適切に分析することができなければ、間違いが起こり、結果的に侵入が長く続く可能性がある。優れたインシデント対応計画と状況の綿密な分析を組み合わせることにより、侵入への対応が組織内だけで処理できない場合に外部のインシデント対応チームのリソースをタイムリーかつ適切に投入することができる。組織の能力および侵入の複雑性についての適切な判断材料を収集できることが、外部のインシデント対応チームを導入するタイミングのしきい値を決定するために重要である。これについては、別のセクションで後述する。

様々な情報源からの通知は、得られる情報量に限りがあり、また組織内のシステムやネットワークに直接当てはまらないかもしれない。初動のトリアージにおいては、通知された情報がどのくらいの即時性をもってもたらされたものであるかを検討する。JPCERT/CC や法執行機関からの情報については、その情報はすでに検知されている可能性が高い攻撃に関するものであるという事実を考慮に入れる。これらの情報を利用するためには、情報共有関係にある同業者や攻撃者関連情報サービスから収集した情報とは少々異なるアプローチが必要となるだろう。通知された情報が自組織に当てはまるかどうかを検討するため、過去のログを調べる必要があるためである。

初動トリアージのチェックで何も見つからなかったとしても、組織は依然として危機に晒されている恐れがある。一つの業界を狙った APT による攻撃は常に同時に起こるとは限らない。APT が近い将来に同様の侵入経路や攻撃手口を使って組織を狙う可能性があるため、トリアージからの情報を保持し、そこからインディケータを整理し、監視を続け、予防的に防御する。

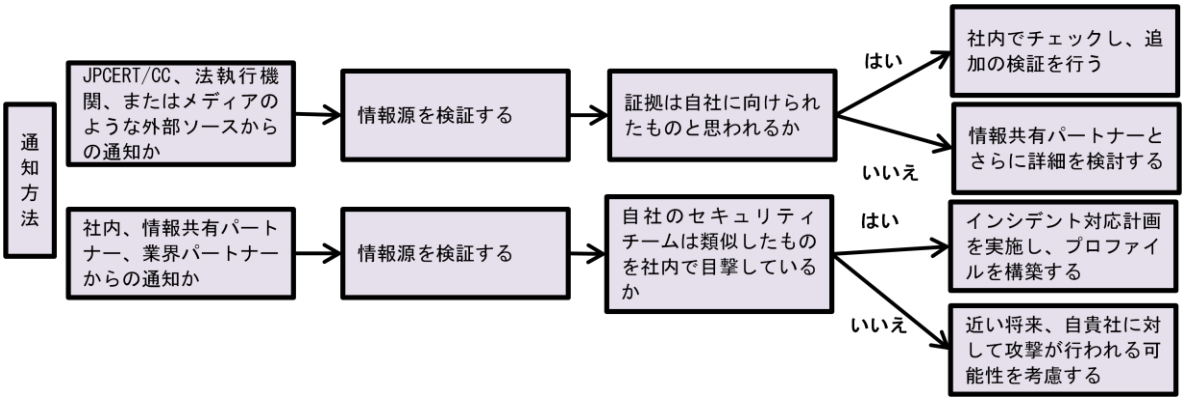


図 22：通知に関する留意点

ハイレベルな取り組み事例

マスコミへの配慮

組織間の APT に関する通知についての最後の留意点は、従業員、マスコミおよび国民に対してこうした情報をどのように扱うべきかという問題である。適切なメッセージを適切なときに発表できるようにするためには、IT、セキュリティ、および広報部門の良好な関係が重要となるだろう。企業や組織に広報部門がない場合は、役員、IT あるいはセキュリティ部門の者がその任務を負う必要が出てくる。マスコミが関係してくる場合、マスコミが発表するものの多くは一部の事実に基づいているだろうが、不正確な仮定や間違った事実が入り込む可能性がある。マスコミへの対処は慎重におこない、メッセージが事実に関して正確であるようにする。メッセージは完全なものである必要はないが、正確でなければならないことに特に注意を払うべきである。組織にとってセンシティブであると判断される事項や、まだ事実が把握できていない事項は、トピックから外すべきである。さらに、マスコミは組織内の人員にインタビューを行おうとするかもしれない。このような時のためにインシデント対応計画やコミュニケーション指針が重要となる。マスコミからのこうした要請はすべて会社の連絡窓口か事前に任命された者が対処し、セキュリティチームがその場その場で対処してはならない。だがマスコミは執拗に、不用意にインタビューに応じてしまう従業員を探し出すかもしれない。マスコミへの情報提供に関する組織的な指針を持つべきである。従業員は一般的にマスコミからの質問を適切な部署に回すべきであるが、中には質問を受けたいと思う従業員もいれば、マスコミに捕まり答えなければならない状況に陥る従業員もいるかもしれない。企業は、従業員がマスコミと話をした場合の副次的影響に対して準備しておく必要がある。企業のマスコミへの情報提供に関する指針は、少なくとも以下の質問にどのように答えるかを扱う必要がある。

- 攻撃者は誰か
- なぜこの攻撃がなされたのか
- いつ起こったのか
- どのようにして攻撃してきたのか
- 攻撃はどの程度の範囲に及んでいるのか
- 組織のセキュリティ対策は攻撃に対して不十分であったのか
- 何が起こったのかを判断し、今後の発生を防ぐために、どのような手段を取るのか
- 今回のインシデントの影響は何か
- 個人情報が漏えいしたか
- 今回のインシデントに関して、どの位のコストが予想されるか

マスコミが極めて具体的な質問をする可能性があり、不適切な回答は組織に甚大な被害を及ぼしかねない。従業員全員がマスコミからの問い合わせへの対処方法を認識し、訓練を受けるようにする。日本では、盗まれたデータに関する質問が非常に一般的である。さらに以下の質問も対処できるようにしておくべきである。

- どのようなデータが盗まれたのか
- 何台のシステムが侵害されたのか
- 盗まれたデータは重要な機密情報か

3.3. ログおよび各種データの保全

自組織のネットワーク上の APT 攻撃者について通知を受けたならば、すぐにログおよび各種データを保護し、インシデント対応チームが活動するための準備を整えるべきである。証拠として保全すべきデータの種類は、攻撃方法・侵入経路や、侵害に関わったシステムから実際に収集できるものによって決まる。データ収集中に発生する可能性のある変動要因を理解し、より正確な状況認識を得るためには、データ収集の方法もまたインシデント対応者にとって重要な問題となる。

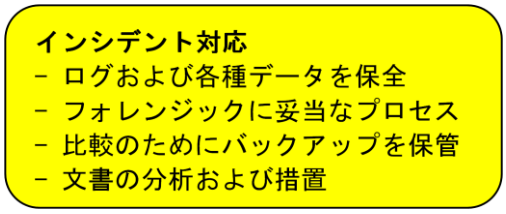


図 23: インシデント発見時の対応措置

ログおよび各種データの保全に際して、以下の事項を考慮する必要がある。

- **標的型攻撃メール：**メールのオリジナルをヘッダ、添付ファイルと共に保存する。標的型攻撃の一部分であるダウンロードされたファイルや実行ファイルは、パケットキャプチャデータの中から見つかるかもしれない。パケットキャプチャデータ全体は非常に大きく、多くの組織ではこうしたデータを長期間保存していないため、インシデント対応チームは必要な時にデータを速やか取得できるように準備する必要がある。
- **SIEM データ：**SIEM データには、インシデント対応チームが必要とするものが含まれていない。SIEM は通常、問題の存在を報告するだけである。インシデント対応チームが侵入の状況を把握するためには、SIEM が解釈する前の実際のログが必要となる。SIEM の警報は、対応チームに実際に何が起こっているかを知らせるわけではなく、どこを調べたらよいかを教えるだけである。ログが保存されていなければ、SIEM が解析した証拠を確認する方法はなく、SIEM の警報自体がインシデント対応者にとってほとんど役に立たないものとなる。
- **タイムスタンプ：**「2.7 予防的なログの保持」の中で述べたように、すべてのログ種別が、同期し連携した正確なタイムスタンプを持つことにより、インシデント対応チームは素早く行動することができる。チームが一連の事象を順序付けていくにつれて、侵入の範囲に関する証拠をより深く理解できるようになる。このように証拠の断片をつなぎ合わせることで、APT を排除するために必要な、集中的な作戦行動に焦点を当てた対応を行うことが可能になる。
- **インシデント対応記録：**インシデント対応関連のデータや記録は、機密性が高い情報であるので、安全で、法的に利用可能な（法的紛争・訴訟に際して利用可能な）方法で取り扱う必要がある。これは APT がこうした記録を侵害し、検知からの回避に利用することを防ぐだけでなく、起訴、事業継続計画、さらなる侵入の脅威への対応に関する法的要求事項を満足する。このような記録は安全な場所で作成・保管し、調査のトリアージの期間中はそのまま残しておくべきである。インシデント対応チームの対応記録と相関付けされたログをもとに、長期および短期の傾向変動分析を実施することができる。記録媒体は暗号化し、必要がなくなったらシュレッダーにかけるか、削除する。
- **法的に利用可能な（法的紛争・訴訟に際して利用可能な）証拠：**メモやバックアップ、証拠に対し、それらの収集方法について注記を付けることは、ベストプラクティスであるだけでなく、法廷で証拠として採用されるために必要である。フォレンジックの証拠として、問題になっているシステムのハードディスクのビットイメージコピーは、システムファイルの変更をチェックできることから重要である。一連の分析過程におけるすべてのステップは、システムに対してとられた措置とともに、文書化されなければならない。必要な証拠のメタデータには以下のものがある。
    - 保管した日時（時刻、分まで記録）
    - 保管場所

- デバイスタイプ、容量、メーカー、モデルおよび 製造番号
- MD5 および SHA-1 のチェックサム
- 証拠の引き渡しや処分における管理人と証人の署名

システムのハードディスクのビットイメージコピーについても、同様の情報が推奨される。

- **バックアップ：**ログおよびインシデント対応記録のバックアップは、定期的に実施し、安全に保管する必要がある。バックアップは定期的にテストし、読み込み可能であることを確認する。バックアップは複数のコピーを複数の場所に保管する。その理由としては、内部からの脅威への耐性を高める、物理的損傷に対するデータの維持能力を高める、実データや他のバックアップと比較使用するなどがある。バックアップは、タイムスタンプ、アクセスログ、システムファイルなどのメタデータが攻撃者によって改ざんされていないことを証明するために重要となる。この検証は、何かが変更される度にファイルを収集し MD5 ハッシュを作成・比較することで完全なものになり得る。この手法は、オフラインで保管され変更されないログおよびデータに適用される。こうした静的ログのハッシュに変化が見られる場合、ログが改ざんされた可能性がある。

組織が外部のインシデント対応チームの支援を要請する可能性がある場合、外部のインシデント対応チームに引き渡すために保持しておかなければならないログが数多くある。こうしたログには、ファイアウォール周辺のログ、ホストのエンドポイントのログ、およびオペレーティングシステムでの詳細プロセスを追跡できるイベントログなどがある。マンディアント社およびロッキード・マーティン社によると、DNS ログは次の理由により時系列を掴み調査を進めるために重要である。ログのサイズが小さいため長期間の取得がしやすくログ全体を分析しやすいこと、また多くの APT 攻撃者が攻撃プロセスやマルウェアの中で様々な URL を使用すること。APT の初期段階の攻撃活動は数カ月～数年に渡りおこなわれるため、DNS ログを取得できる期間が長いほど組織が APT の活動を発見できる可能性が高まる。加えて、すべてのネットワーク接続ログ、特に RDP（リモートデスクトッププロトコル）ログやプロキシログも重要である。Web サーバログを含め、エンドポイント、オペレーティングシステムのリスト、DMZ サーバに関する情報は、すべてインシデント対応チームにとって有益なものとなるだろう。

ログを保存する際、ログの相関分析によって何が起こったかを掌握できるように必要な情報を確保することが重要である。ログには、どのユーザまたはシステムがリクエストを投げたか、リクエストの目的、リクエストが発行された時刻を示すものが必要である。DNS やプロキシがユーザに代わってリクエストを発行したなら、両方のログをレビューし相関分析する必要がある。

追加情報が有用となることが多いので、ストレージの制約が許す限りログはできるだけ詳細に取得するのが最善である。もしストレージが問題であれば、一部のログはあらかじめ除外してもよい。例えば、アンチウィルスベンダとの通信、OS のアップデート、通常のビジネスパートナーの Web サイトとの通信など、ログのトラフィックの多くを占めるものがそれに該当する。

多くの場合プロキシはログを役立てやすい形式では記録しない。そのようなシステムではログが適切に収集されるよう設定変更するべきである。ログには参照されたデータ、タイムスタンプ、すべてのリクエストに関する情報（送り返されたファイルの種別を含む）が含まれるべきである。プロキシのログについては、上り（アップロード）、下り（ダウンロード）のデータサイズ（ヘッダ＋ボディ）を記録しておいた方が良い。もしプロキシにリクエストを拒否する設定が組み込まれているなら、拒否されたリクエストのログも取得するべきである。それはセキュリティチームが調査するに値する有用な情報となる。

3.4. APT インシデント対応手順

APT インシデント対応に先立ち、組織が所有している検知、分析および対応用のツールを調査しリストを作ることが大切である。ツール、その能力、使用条件、およびアウトプットを特定し、使用法を把握しているセキュリティチームのメンバのリストを作成するべきである。侵入への対応中に、こうしたツールを使って行った措置をすべて文書化する。これによりセキュリティチームおよびインシデント対応チームは、どの措置がすでに取られどの措置がまだ実施されていないかを把握することができる。

APT の痕跡が残る場所
-ファイアウォール周辺
-システム利用者のログ
 -詳細なプロセス、ログイン、OS
-ネットワーク／リモート接続
-各種ログ
-DNS：各クエリ
-DMZ

図 24：APT の痕跡が残る場所

標準的な手順は、侵入前の予防的な監視および侵入中・侵入後の監視を行いながら、ログの収集を続け一元的に保存する。こうしたログには、ファイアウォールの周辺ログ、ホストログ、詳細なプロセスログ、ログイン、オペレーティングシステムログ、ネットワーク接続およびリモート接続ログ、活動が検知される前のすべての DNS クエリ、DMZ ログがある。前項で述べたとおり、理想的にはこうしたログをすべて一元的に安全な隔離領域に保存し、セキュリティチームが事件の時間軸を作成できるようにすべきである。

ネットワーク上で APT が活動しているという通知を受けて、企業が直ちに取るべき措置がいくつかある。反対に避けるべき措置もある。たとえばもし攻撃者が検知されたことを知り、より検知が難しい活動手法を採用すれば、組織に弊害がもたらされるだろう。同様に、攻撃者がもし個々のシステムが修復されていることを知れば、攻撃者は他のシステムに横断的に侵害し代替の通信経路を設定することで対応者の対策を阻止するだろう。そしてインシデント対応チームは文字通り何も得ることなく資源を浪費することになる。組織は、何を行い、何を行わないかの決定を、準備段階で行っておくべきである。

APT はネットワーク上での活動中にアクセスや情報をさらに得ようとするだろう。したがって、侵入の規模を判断し、タイムリーに正しい方法で対応することが非常に重要である。セキュリティチームの目標は、攻撃者の活動プロセスのなるべく早い段階で対処することである。また、データが盗まれただけでは、必ずしも攻撃者の活動が終わったとは言えないことも考慮したい。攻撃者には他の目標や目的があるかもしれない。攻撃者はさらなるデータ窃取か他の目的を達成するために、ネットワークに執拗に居すわり続けるだろう。

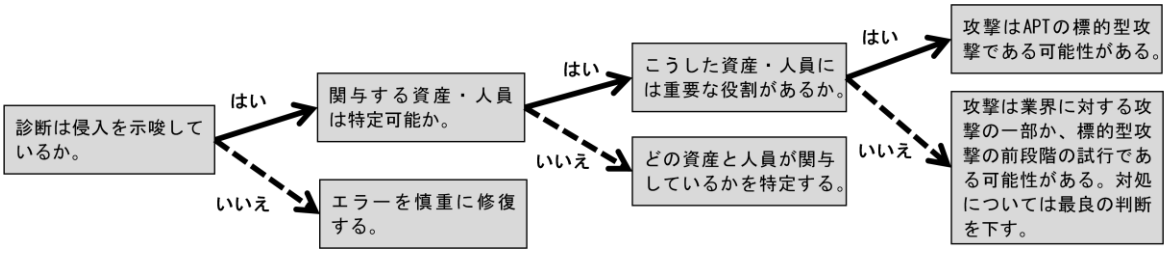


図 25：侵入の診断フロー

リスク許容度に基づく措置

企業や組織は、APT のネットワーク上での活動を知った時点で、どのレベルの措置をとるかを決めるために、あらかじめ整備されたリスク管理およびセキュリティ指針をもとに検討する必要がある。

一刻を争う迅速な対応が求められる性質のものであるため、こうしたリスク管理やセキュリティ指針は APT による侵入が起きる前に用意しておく必要がある。そうしておかなければ、侵入への対処に使えるはずの時間が手順の決定に費やされてしまうことになる。リスク管理の判断は、関連する経営上の考慮事項を把握し、意思決定の権限を持っている取締役会や上級経営陣がおこなうのが最善と考えられる。

APT への対応において、取るべき措置を決定する際には、「リスク」「リスク許容度」「脅威を直ちに排除する必要があるのか」「脅威を直ちに排除しないとき、侵入範囲を完全に把握できるか」について検討する。リスク許容度が低い、すなわちリスクを許容できないと判断した場合、マルウェアを除去する目的でのシステム遮断、システムの隔離、およびマルウェアのフォレンジックの実施を検討する。

リスクをどう許容するかについて、セキュリティチームおよび各リスク責任者は討議する必要がある。重要な情報資産に対する攻撃の脅威の排除を、侵害の範囲を完全に特定することより優先するかどうかの判断は、究極的には経営判断の問題である。攻撃への対処のために特定のシステムを遮断したことにより生じる混乱や悪影響により、コストが増加する恐れがある。対処したにもかかわらず攻撃者は引き続き円滑に活動を続けるかもしれない。APT 攻撃者が横断的にネットワークを侵害し、他のシステムを感染させ、戦術を変更した結果、セキュリティチームが APT をネットワークから排除することがますます困難になり、時間と人的資源の面で高コストとなることも考えられる。

リスク許容度が高い、すなわちリスクを許容できる場合は、 次の工程で検討を行う。（順序は状況によって変化し得る。）

① 手順の漏れがないようにチェックリストに従い工程をすすめる。工程には、インシデント対応計画の実行や、逸脱（逸脱は必ず発生する）を承認できるように権限のある者とともに調整を行うことも含まれる。
② SIEM などのツールを使って収集したログを精査する。ローカルに保管されていないログや SIEM に取り込まれていないログが存在する場合は、手作業での検討が必要となる。その場合でも何らかの方法で個々のイベントについて調査すべき時間枠を絞り込むことができれば、分析しなければならないログの量を減らすことが可能となる。
③ 攻撃者のプロファイルを構築し、相関関係があるかどうかを見るため、既存のプロファイルと比較する。多くの場合、セキュリティチームはすぐには活動を APT プロファイルに当てはめることはできないだろう。インディケータを収集し、多くの事例を蓄積する必要がある。事例の蓄積が進展するにつれて、既存のプロファイルとの関連が現れ、探すべき他のインディケータを見つけるのが容易になるだろう。
④ 横断的侵害の証拠を調査する。こうしたデータは、メモリ、接続データなど揮発性の情報を調べることで特定することができるかもしれない。見つけるのは容易ではないが、何者かがシステム間を横断的侵害した証拠はどれも重要なインディケータとなるだろう。
⑤ 重要な資産とその間のトラストチェーンを監視し、このような標的に対するいかなる行為が起きても警報が出されるようにする。重要な資産とのトラストチェーンがあるシステムが侵害された場合は、トラストチェーンが悪用されていないかどうかを判断するため、調査を必ず行う。
⑥ 侵害されたとみられるシステム上で圧縮ファイルや暗号化ファイルを探す。これは、盗まれたデータをパッケージ化する標準的な方法であるため、こうしたパッケージ化の方法、ファイルの命名規則、および保管場所の特定は、同じ APT 攻撃者が他のシステムを侵害した可能性がある場合、調査すべき項目の手がかりとなり得る。
⑦ 攻撃者に関する特徴的な情報をできる限り共有する。攻撃を受けた企業は、自身が受けた攻撃に対して他の企業が準備を整えるのを支援することができる。また標的となった他企業の

アナリストが、追加的なインディケータやセキュリティチームが注視する事象についての分析情報を提供することができれば、それらの情報はさらに役に立つ可能性が高い。

最後に、リスクへの適切な対処を決定したらすぐに必要な措置を実施する。こうした措置には、遮断、マルウェア・フォレンジック、システム隔離などが含まれる可能性がある。おそらく、協働関係にある他のアナリストから得た経験・教訓を基に留意点をすべて検討した時点で、計画が形になってくるだろう。

重要な資産へのアクセスが変更・隔離された時は、攻撃者はそれに気付くだろう。これは、上級経営陣が扱うべきリスク許容度の問題である。たとえば、以下のような点である。データは、アクセス方法を変更することで、検知していることについて攻撃者に気付かれてもよいほど重要か。攻撃者に関する他のインディケータを探り出すために、その動機、目的、戦術についてさらに情報が得られることを期待して、その行動を監視し続ける価値があるか。より一般的な手順は、データの持ち出しを阻止するために、マルウェアのコミュニケーション方法（もし分かっている場合に）を妨害してデータを保護することである。残念ながら、個々の状況には違いがあり、常に適用可能な措置というのは存在しない。企業や組織は、リスクを分析し、それぞれの侵入に対する対処方法を決定する必要があるだろう。だが、こうしたリスク分析の一部は、対応プロセスを迅速化するために、事前に決定することが可能である。

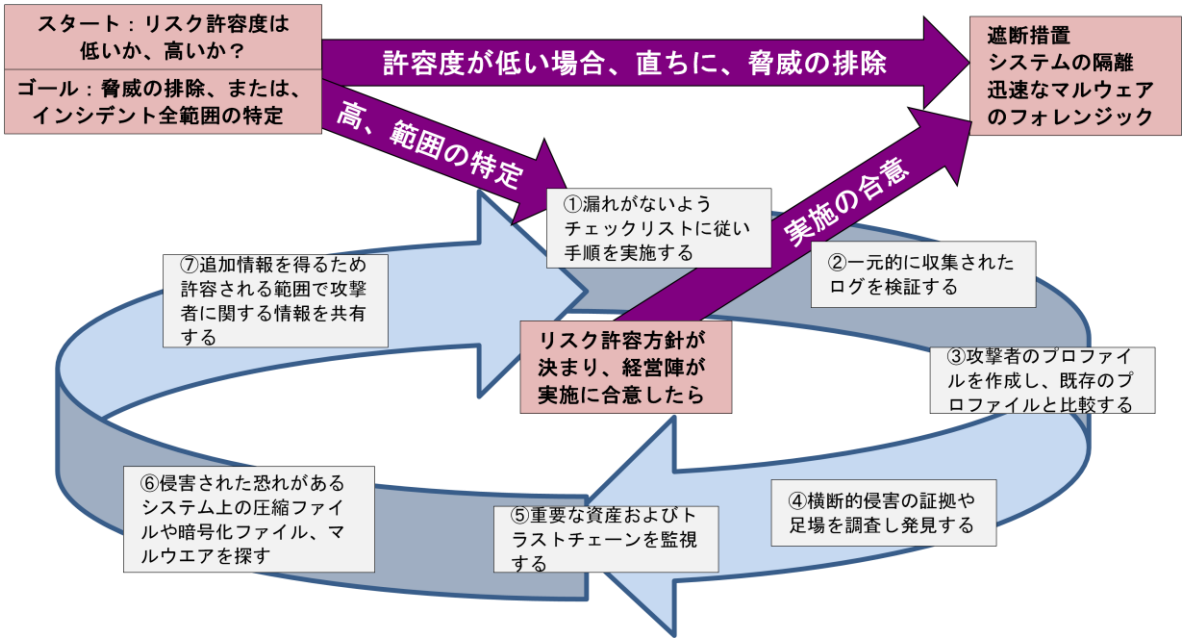


図 26：リスク許容度に応じた対応手順

リスク分析を予防的に実施するに当たって、以下の質問は役に立つかもしれない。

- 守る必要のある重要な資産は何か
- 重要資産に関して、すでに把握されているコンピュータセキュリティ問題は何か
- どのようなタイプの対応が必要か、資産は（今後の）侵害を阻止するために遮断してもよいほど重要か
- どのようなプロセスが必要か、プロセスにおける活動は誰が実施するのか
- 通知やエスカレーション（上位の担当者に対応を要請）のプロセスには誰が関与する必要があるか

初動対応中に参照する主なリソースには、以下のものがある[23]。

- セキュリティチームと事態を認識する必要のある部門（たとえば、リスク責任者）とのコミュニケーションを確実にするための、企業や組織全体および各部門の組織図
- 優先順位を付けるための、重要なシステム、資産および情報のリスト
- 既存の災害復旧計画および事業継続計画
- 業界規制および法規制（該当する場合）

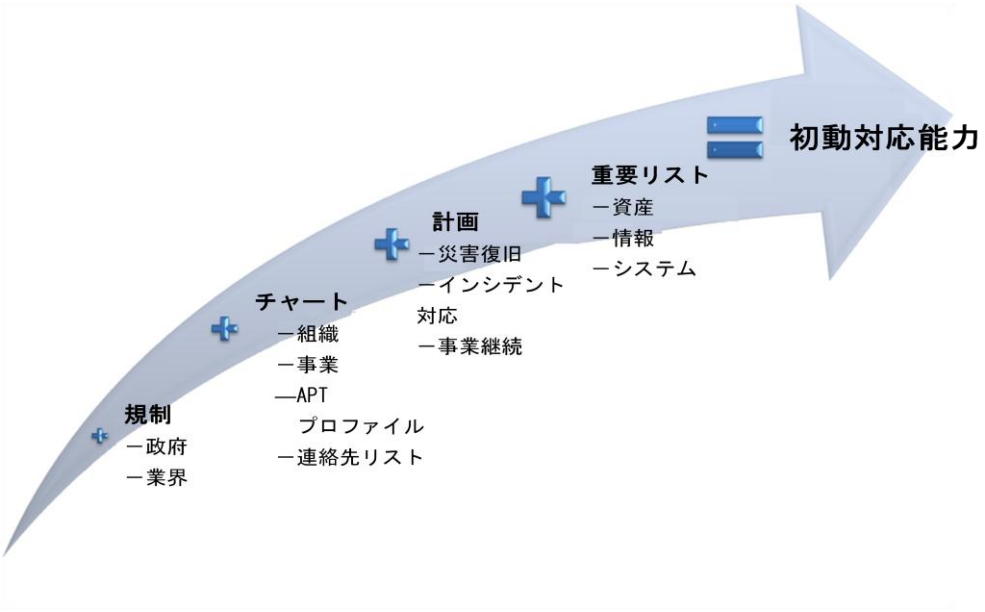


図 27：初動対応能力の決定

インシデント対応におけるチェックリストの利用

インシデント対応のための基本的な項目を含む既成のチェックリストを利用することから始めてもよいが、こうしたチェックリストは組織の実態に合わせて大きな修正や調整が必要となる。組織の運用方法にあわせ修正を繰り返し、組織の具体的なニーズをチェックリストに含めるようにする。

侵害を検知した初動段階においては、チェックリストによる統制の効いた対処が重要である。多くの企業や組織では、遮断措置、システムの隔離、迅速なマルウェアのフォレンジックなどで侵入に速やかに対処することが標準的な作業手順として定められているが、マルウェアがマルウェアの操作者とのコミュニケーションをとる可能性は考慮されていない。遮断とシステム隔離は、それによって攻撃者が戦術を変更しネットワークに潜伏し続けることを考慮すれば、必ずしも最善の解決方法ではない。本ガイドには、実際に既に使われ、検証されたチェックリストおよび手順を付録として添付している。これらは APT による侵入の範囲を適切に特定し脅威の排除を行うことを支援するだろう。

[23] Software Engineering Institute. “*Creating and Managing Computer Security Incident Handling Teams (CSIRTs)*”（ソフトウェア工学研究所「コンピュータセキュリティ・インシデント対応チームの設置と管理」）

ハイレベルな取り組み事例

APT に備えた高度なチェックリストの利用

米国では多くのセキュリティベンダが APT に備えて高度なチェックリストを用意している。場合によっては、組織的な対応に関するチェックリストが外部のインシデント対応チームのプロセスを補うこともある。組織が外部のインシデント対応チームと連携する場合は、既存のチェックリストについて本書を補完または修正できるものがあるかチェックすべきである。マンディアント社は現在、顧客が社内チェックリストプログラムを作成・改善するのを支援する事業部門を立ち上げており、他社も同様の事業を行うと思われる。その目的は、よく知られたベストプラクティスをモデルにプロセスを作成し、顧客の従業員を訓練し、顧客自身がプロセス・手順をカスタマイズできるようにすることである。

対応の作戦行動中に侵入範囲を特定するのは複雑な作業になり、繰り返しがほぼ不可能である。マンディアント社の対応事例では、同社は顧客側での高度な準備がほとんど必要ない内製ツールをインシデント対応に活用しているが、顧客のセキュリティチームは多くの場合、いくつかの対処手順を独自で実施したがり衝突を生む。組織がインシデントに直面する前に問題を慎重に検討することは、取るべき措置および回避すべき措置に関して適切な判断を下す助けとなるだろう。

APT の活動中の関連リスク

企業や組織は、ネットワーク内の攻撃者の存在を把握していることを攻撃者に知られたくないと考えるだろう。一方で、攻撃者の侵入に完全に対処するためには迅速に対応しなければならない。ネットワーク内の攻撃者は企業や組織に害を及ぼすことに注力していることが明白であることを考えれば、企業がすべきことを厳密に決定することは難しいだろう。

いくつかの措置は、企業や組織が APT の存在を把握していることを暴露し、APT が戦術を変更しさらに高度な活動を行うようにさせる可能性があるため、組織は APT 対応中にそれらの措置を取ることを望まないかもしれない。APT が高度な活動に移行すると検知がさらに難しくなり、攻撃者の定着化を促進する結果となり得る。以下のセクションでは、企業や組織が APT の存在に対して迅速に対処する必要があるという事実を認識しつつ、APT に情報を与える可能性のある対応措置を制限するための留意点を挙げる。

侵入を検知した時点で、脅威に対して無計画な措置を取り始めない。多くの場合、最も重要なことは、「何をしないか」ということである。ある措置は当初は予防的なものとみえるかもしれないが、長期的な状況改善の妨げになることがある。また、別の措置は予防的なものとみられるが、適切でない時点で使

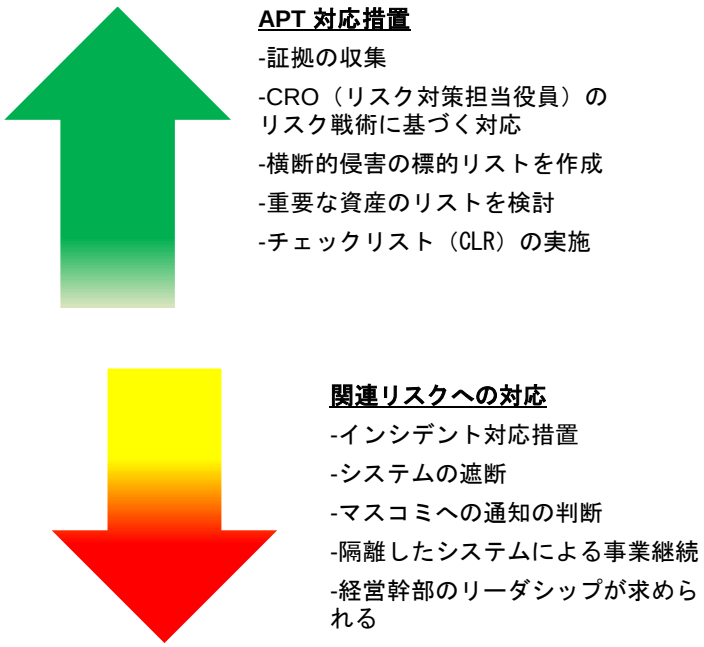


図 28：APT 対応措置と関連リスク

われると修正が妨げられる可能性がある。こうした措置としては、IP ブロッキング、システムの実ネットワークからの隔離、マルウェアのリバースエンジニアリングの試み、検索、調査および無力化のためのコールバックドメインへのアクセスなどがあり得る。整備されたチェックリストに従い、適切なリスク分析を行う事が重要である。こうした措置を実施すべき状況もあり得るが、APT に対処するためには慎重に考慮する必要がある。

第一の考慮事項は、APT 攻撃者を扱う際には、標準的なインシデント対応に使うチェックリストとは別のチェックリストを作成・使用することである。攻撃が本当に APT であるかどうかを判断するのは最も難しい部分である。人を欺き、ひそかに行動するという攻撃の性質を考えると、対応チームが当初から、侵入が APT によるものであると確信することはまれである。またこのチェックリストは、企業が検知していることを APT に知られるというリスクに基づいて措置を分類するべきである。

次に考慮する点は、機密情報の保持は、報告が必要な企業や組織では難しいことがあるという点である。たとえば、侵害されている状況で、上層部に侵入に関して報告を行う必要がある場合、攻撃者がその報告内容を獲得し、すでに取られた措置や今後計画されている対応を知る可能性がある。これまでの経験では、攻撃者は、企業が取る対応措置に対し速やかに適応する能力を示している。

さらに、従業員に送られた侵入に関する情報は、様々な理由で攻撃者に知られてしまう可能性がある。攻撃者によるトラフィックの傍受やセキュリティチームの行動に関する情報収集もその一つであるが、APT への対応活動に従事していない熱心すぎる従業員やセキュリティ専門家が、調査の一部を買って出るかもしれない。組織がその存在を知っていることを、こうした「積極的な」従業員の活動によって APT に気付かれることを防ぐことは非常に重要である。組織における手順は、APT に関する知識の拡散をできるだけ小さくし、この知識を必要とする者にのみ提供するために、どのように共有・配布していくかについて取り上げるべきである。攻撃者は、ネットワーク上で重要資産にアクセスできなくなったことを知り、組織を攻撃するためのアプローチ・戦術を変える可能性がある。APT の存在が疑われる場合、重要資産を隔離する前に多くの検討・リスク分析を行う必要がある。APT は執拗であり、将来さらに情報を持ち出していくと考えられ、APT が深く身を隠した場合、排除はさらに難しくなるだろう。初動においてこのバランスを決定するのは不可能で、セキュリティチームが事後分析において初めて、適切な決定だったかどうかを知ることになる。これが、セキュリティチームが、事業上のニーズとセキュリティ上の懸念を比較してリスク決定を行うことのできる上級幹部とリスク責任者の支援を求める理由である。

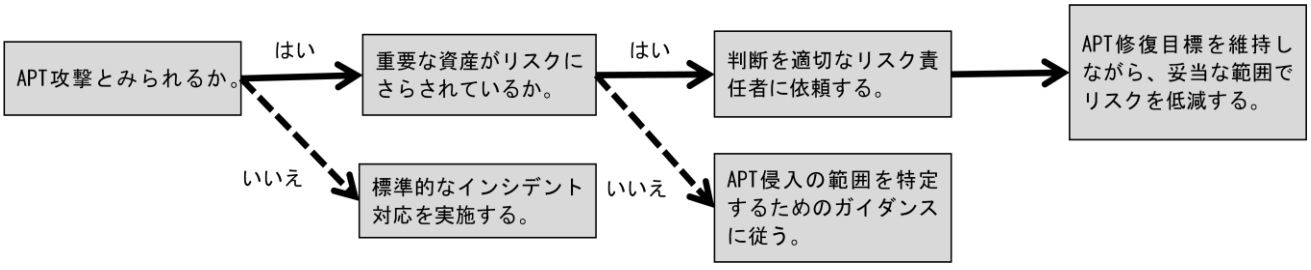


図 29：APT が存在するときに取る措置を理解する

3.5. インシデント対応支援のアウトソーシング

外部からの支援を得る決定は、最終的には上級経営陣が行う必要がある。最初の APT 攻撃の検知時に予防的に導入する場合もあれば、社内の選択肢がすべて失敗に終わったときに外部リソースを導入する場合もある。企業はセキュリティや対応プログラム、指針、セキュリティ管理策の現状を評価するために外部リソースを予防的な利用することもできる。このタイプの支援による最も一般的な成果は、侵入テストやリスク評価であるが、APT 活動に先立つ効果的な監視プログラムや予防的な防御プログラムの構築に重点を置いたものになることもある。

外部のインシデント対応チームを初動対応のために利用するのは、一般的な戦術である。侵入を検知した時点では、組織はどこから対応を始めるべきかわからないかもしれない。そのとき、外部のインシデント対応パートナーが手助けとなる。攻撃が横断的侵害やデータの持ち出しにエスカレートする前に、または長期にわたって被害をもたらす前に、外部のインシデント対応パートナーは攻撃を阻止できる可能性がある。

外部リソースの支援を利用するもう一つの一般的な理由は、社内の選択肢がすべて失敗に終わったことである。この時点で、政府やマスコミが攻撃を発見し、それらからの問い合わせが来ている可能性もある。組織はアウトソーシングを決定する前に、一定期間独力で APT からの修復を試みたかもしれない。官公庁が連絡をしてくるまで、専門のインシデント対応チームの導入を行わない組織もある。官公庁の監督の回避はインシデント対応支援をアウトソーシングする理由としてよく言及される。これは多くの場合、サイバーインシデントに対処できないと見做された企業に対しては、政府の監督が強化されることがよくあるためである。

外部に支援を求めることを決定する際には、上級経営陣が考慮しなければならない要素がいくつかある。最も基本的な質問は「我が社はどの程度のリスクを取る用意があるか」である。APT に対して用意がなく無防備な状態が長く続けば続くほど、より大きなリスクが発生する。そのような組織の多くは、自組織の中核機能にサイバーセキュリティや APT 分析が含まれていないことを思い知らされることになり、会計などの専門分野で行うのと同じように、サイバーインシデント対応の専門家の支援の必要性を理解する。

もう一つの要素は、組織内外で侵入について知っている者がどれだけいるかという点である。一般的には、侵入について知っている者の数が増えるにつれて、プロセスを管理するのが難しくなることが懸念される。この情報がマスコミに漏れるのに、不注意な者や不満を持つ従業員が一人いれば十分なのだ。マスコミに対応する最も一般的な方法は、事後に「問題があったが解決した」と言ってすませることである。

さらに追加的な要素として、組織は、非常に機密性が高いデータを外部委託先に任せることを懸念するかもしれない。 また、外部委託先自体が侵害されていないことを確信できないかもしれない。組織は、このような機能をアウトソーシングする際には、評判の高い信頼のおけるインシデント対応チームを選ぶことが推奨される。

外部のインシデント対応チームを選ぶ際の留意事項

- レポートの充実度とタイミング
- 外部とのパートナー
- 対応時間
- 身元保証
- 業界での経験
- 監視の容易さ

図 30：外部のインシデント対応チームを選ぶ際の留意事項

外部の支援を求める決定がなされた後、組織と外部委託先との間で、委任する業務の範囲を明確に定義し、合意し、文書化する必要がある。組織はすでに自らが把握している問題を解決したいだけなのか。外部委託先が徹底的に調査を行い、発見した活動をすべて排除することを望むのか。または、侵

入の問題を解決し、自組織のセキュリティプログラムを全面的に改修してほしいのか。業務の範囲を決定することは重要であるが、その決定は組織と外部委託先の双方に明確に伝えられ、すべての関係者が外部委託先の実際の活動について十分理解していなければならない。

外部委託先は、効果的に業務を行うために、十分なアクセス権を与えられる必要がある。組織が外部委託先をあまりにも細かく管理すると、侵入を解決するのに必要な時間が大幅に伸びる可能性がある。また、外部委託先の問題解決能力を全体的に妨げることにもなりかねない。しかしこれは、経営陣が定義し、契約期間を通して監督する必要のある、微妙な境界線である。

最後に、組織のセキュリティ能力と対応能力の成熟度を考慮する必要がある。組織の能力についてあまり確信がない場合には、外部に業務を委託したり、支援を求めたいと思うだろう。これは、組織のネットワーク上で APT が本当に活動している場合には重要であろう。もし組織が、APT がネットワーク上に居すわり続けることを許すならば、損失は大きなものとなろう。APT は時間とともにさらにデータや知的財産を持ち出し、組織の競争力が損なわれるだろう。そして APT はネットワーク上にさらに居続けることになり、その排除はよりいっそう難しくなるだろう。

侵入に対して社内で取り組むか、外部の支援を求めるかの決定に関係なく、JPCERT/CC や外部の CSIRT との間でインディケータ等の情報を共有するための情報共有の枠組みへの参加を考慮すべきである。情報共有の枠組みへの参加により、情報交換、インディケータの収集が可能となる。たとえセキュリティチームと外部のインシデント対応チームが現在この情報共有の枠組みに関与していない場合でも、組織は JPCERT/CC へのインシデント報告（等の情報共有）を検討すべきである。インシデント報告（情報共有）は APT に対処するすべての業界に役立つからである。他の組織は分析から恩恵を受け、分析結果を使って追加的なインディケータを発見し、そうしたインディケータが今度は情報共有の枠組みにおいて共有される可能性がある。他の組織はこの新情報を防御措置に活用することができ、情報共有の枠組みへの参加者全体を向上させる。セキュリティチームと外部のインシデント対応チームが継続して情報共有の枠組みに参加している場合、交換される情報は、標準的なインシデント報告より内容が濃いものとなり、特定の攻撃者に狙われているかもしれないすべての参加組織に役立つ可能性がある。各組織が互いに協力し合って共同の防御を行うことで、すべての参加組織は共有された情報から恩恵を受け、各組織が個々に非常に複雑な防御プログラムを作成・維持する必要がなく、進化する APT 活動の常に先を行くことができる。

一部の組織が留意すべき別の事項として、インシデント対応機能が外部委託されているかどうかがある。組織は、情報共有の枠組みにインシデント対応の委託先のチームが加わることを望むかもしれない。外部のインシデント対応サービスプロバイダは APT に対する防御において重要な役割を果たすのであり、戦略の一部として定義された手順・プロセスに精通しているべきである。組織はリスクの観点から、同業界のどの企業と自組織の記録や情報を比較したらよいのか知りたいと思い、また様々な組織から通知を受け取る場合に、収集された攻撃者関連情報の匿名性と信頼性を確保したいと思うだろう。また、サービス内容合意書（SLA）を使ってリスク機能を外部委託先のチームの活動に組み入れたいと思うだろう。これらにより組織は、ネットワークに侵入した APT をどのように処理するかについて洞察を得て、重要な資産を防御するための一定の能力を有することになる。

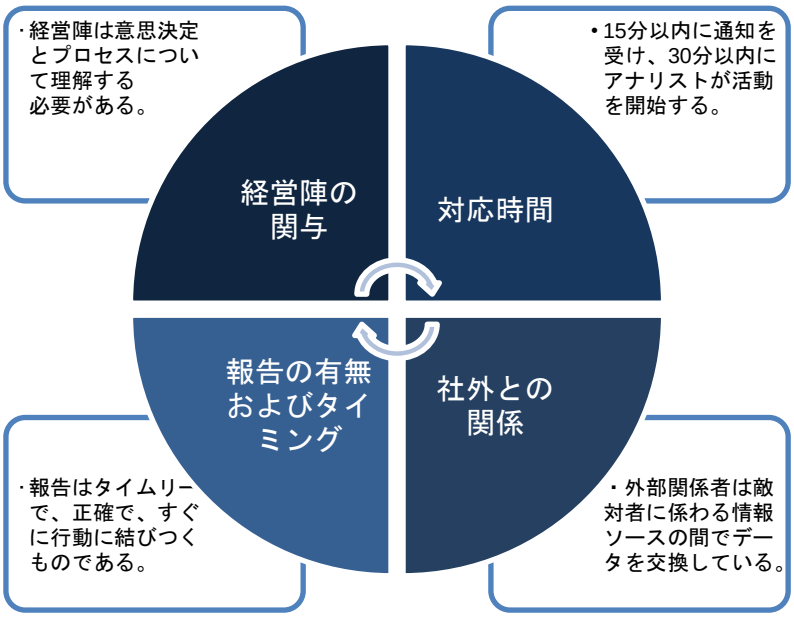


図 31：インシデント対応をアウトソーシングする際の優位事項

3.6. 外部のインシデント対応チームの活動

外部のインシデント対応チームは、委託を受け業務を開始次第、手順に従った対応を実施するだろう。まず、外部のインシデント対応チームは、検知、分析、および対応措置に関与した従業員とのインタビューを実施する。どのステップが完了したのか、どのツールを使ったのか、いつ措置を実施したのか、そしてこうした措置への反応と成果について知ろうとするだろう。また、実施されている予防的な措置、取得された関連ファイルやログについても知ろうとするだろう。このため、組織はインシデント対応措置の最中に詳細な記録を取ることが極めて重要である。

外部インシデント対応チームは組織の記録を活用する際、すべてについて評価し直すのが普通である。これは一般的な手順であり、組織の措置が不十分であったことを示唆していると解釈するべきではない。外部インシデント対応チームは結果を検証する場合があるため、記録に加えて、証拠のオリジナルとバックアップにアクセスできることも重要となる。適切に取られた記録によって、外部インシデント対応チームは集められた証拠を使い、迅速に検出事項を再構成することができる。ログが十分でない場合は、データをそのままの意味に解釈し使用する。これはチームが感染源を把握し、侵入範囲を特定し、修復を開始するために重要である。

マンディアント社は、高度な APT による侵害からの修復を独力で完全に行える能力のある組織をまだ見たことがないとしている。APT による侵害からの修復のための技術・プロセスにかかる費用は非常に高額となる可能性があり、同社は、いくつかの企業は、最長 1 年にわたり独力で APT 侵害と戦おうとしたが、結局は完全に修復することができず、外部インシデント対応チームの支援を導入せざるを得なかったと述べている。この点で、経営上の明確な決定を行う必要がある。特定のタイプの侵入に対処する自社の能力について確信がなければ、アウトソーシングするほうが道理にかなっている。APT に限って言うならば、組織内に高度なインシデント対応能力がある企業は社内での対応を考えても良いが、そうでない場合には、アウトソーシングあるいは、外部のインシデント対応支援サービス利用を検討した方が良い。

付録 A：事前準備のために利用するチェックリスト

チェックリストの章構成

大項目	中項目	小項目～	本文関連箇所
カテゴリ1 守るべき資産の特定	**A. リスク許容度の評価と管理策の実装**		2.3 リスク許容度の評価と管理策の実装
		1 組織のプロファイリング	
		2 リスク判断によるビジネスインパクトの整理	
		3 とくに自動化すべき資産管理策	
		3.1 ハードウェア管理	
		3.2 ソフトウェア管理	
		3.3 アイデンティティ管理	
カテゴリ2 迫りくる脅威の理解	**B. 脅威の理解**		2.5 脅威の理解
		1 業界のセキュリティ動向の検討	
		2 外部脅威　攻撃者に係わる情報の収集と交換	
		2.1 攻撃者に係わる情報収集能力の構築	
		2.2 攻撃者に係わる情報 を共有する際の留意点	
		3 内部脅威　脆弱性スキャンとペネトレーションテスト	
		3.1 脆弱性スキャンの実施	
		3.2 ペネトレーションテストの実施	
カテゴリ3 具体的防御策の検討	**C. 予防的なログの保持**		2.7 予防的ログの保持
		1 ログの取得と保守ポリシー	
	D. ポリシーやガイドラインの整備		2.8 ポリシーやガイドラインの整備
		1 セキュアな構成	
		1.1 サーバおよび端末のハードウェア、ソフトウェアのセキュアな構成	
		1.2 ネットワーク機器のセキュアな構成	
		1.3 特権ID、アクセス権のセキュアな構成	
		2 モニタリング	
		2.1 無線LANのモニタリング	
		2.2 アカウントのモニタリング	
		2.3 外部データ送信のモニタリング	
	E. インシデント対応機能の整備と人材育成		2.9 インシデント対応機能の整備と人材育成
		1 インシデント対応機能の整備	
	F. トレーニングおよび演習の実施		2.11 トレーニングおよび演習の実施
		1 トレーニングの実施	
		2 演習の実施	
		3 演習後の対応に関する留意点	
	G. インシデント対応計画の検証		2.12 インシデント対応計画の検証
		1 インシデント対応計画の検証	

想定される使用方法

一連のチェックリストは、APT 攻撃者によるネットワークへの侵入を排除するために、組織が準備を整え、APT に関する詳細な情報を得ることができるように考慮されている。これらのチェックリストを理解することで、APT に関する通知を受ける前から、適切な準備を行うことができるだろう。

カテゴリ 1　守るべき資産の特定

チェックリスト内容			補足解説	Check
A. リスク許容度の評価と管理策の実装				
A. リスク許容度の評価と管理策の実装	**1　自組織のプロファイリング**			
	1.1	組織のプロファイルを作成しているか	組織の特徴には、例えば次の内容が含まれる。 ・規模（例：所在地、従業員、収益など） ・複雑さ（例：製品、サービス、プロセス、管理体制、サプライチェーン・パートナーなど） ・保有する知的財産の価値 ・IT への依存度（IT なしで遂行できる事業活動に関する分析） ・システムダウンの影響範囲 ・システムエラー、管理エラー、処理エラーの影響範囲 ・組織的な変化の度合い ・多国籍企業かどうか ・利害関係者および株主の期待 ・規制のレベル ・評判への依存度 ・外部委託の依存度 ・各事業の活動地域（危険度別）	
	2　リスク判断によるビジネスインパクトの整理			
	2.1	組織のサイバーセキュリティ防御能力について記述した文書を作成しているか		
	2.2	守らなければならない製品、サービスおよびプロセスを定めているか		
	2.3	資産を防御する理由について定めているか	資産には情報、技術、施設、要員なども含まれる。	
	2.4	資産が保護されなかった場合、発生しうるリスクを把握しているか		
	2.5	潜在的なリスクにおいて、対処の必要があるもの、および対処に必要なコストを把握しているか		
	2.6	対処が必要となる前に、どの程度まで資産の減損が許容できるか定めているか		
	2.7	対処後の残存リスクを把握しているか		

	チェックリスト内容		補足解説	Check
A. リスク許容度の評価と管理策の実装	**3 とくに自動化すべき資産管理策**			
	3.1 ハードウェア管理			
	3.1.1	組織内のパブリックネットワークおよびプライベートネットワークに接続されたシステムの資産リストが存在するか	IT 資産インベントリ検出ツールを利用する。 検出ツールの利用の際は、特定のネットワークアドレスの範囲をスキャンするアクティブツール、およびトラフィックの分析に基づいてホストを特定するパッシブツールの両方を採用する必要がある。	
	3.1.2	資産リストの管理と未登録機器の検出を行っているか	DHCP サーバのロギング機能等を利用することで検出が可能。	
	3.1.3	承認されたデバイスのみがネットワークに接続されているか	機器の取得に伴って資産リストを定期的に更新し、アクセス監視の際に確認する。	
	3.2 ソフトウェア管理			
	3.2.1	システムに対してホワイトリストに登録されているソフトウェアのみの実行を許可し、その他すべてのソフトウェアの実行が防止されているか	ホワイトリストを用いて、システム上で一部のソフトウェアのみの利用を強制することは最大のリスク低減であると言える。 ホワイトリストは（ホワイトリストベンダーから入手可能）、一般的なソフトウェアを使用する場面で不便と感じることはないよう非常に広範囲に及ぶ場合もある。一部の専用システム（必要なビジネス機能を提供するために少数のプログラムのみが稼働するシステム）では、ホワイトリストは限定的なものになる。	
	3.2.2	さまざまなサーバ、ワークステーション、およびラップトップを含む、各タイプのシステムについて、組織で必要かつ許可されているソフトウェア/バージョンのリストがあるか	許可されたソフトウェア/バージョンのリストは、その内容が不正に変更されていないかどうかを検証するファイル完全性チェックツールでモニタする必要がある。	
	3.2.3	システムで無許可のソフトウェアが検出された場合に検知できる仕組みがあるか	定期的なスキャンを実行して無許可のソフトウェアの有無を確認できる環境が必要。システム上の変更またはソフトウェアのインストールを管理するため、厳密な変更管理プロセスを実装する必要もある。これには、次の内容などが含まれる。 ・認識できないバイナリ（実行ファイル、DLL、その他のライブラリなど）がシステムで検出された場合（圧縮アーカイブ内で検出された場合を含む）にアラートを生成する。 ・ファイルのハッシュ値を比較してソフトウェアの未認識バージョンまたは変更されたバージョンを調べる。（攻撃者は、よく知られたソフトウェアを改ざんしたものを利用して継続的な攻撃をおこなう。ファイルハッシュの比較によって、ソフトウェアコンポーネントが侵害されたかどうかを判別可能。）	

チェックリスト内容				補足解説	Check
A. リスク許容度の評価と管理策の実装		**3.3**	**アイデンティティ管理**		
		3.3.1	すべての従業員に関する ID のアクセスコントロールリストを定義しているか	アクセスコントロールリストは例外条件を極力減らした、単純かつ強力なものが望ましい。	
		3.3.2	アクセスコントロールリストに基づいて、各データへのアクセス制限が実行されているか		
		3.3.3	アクセスコントロールリストの棚卸を定期的に行っているか		

カテゴリ 2　迫りくる脅威の理解

			チェックリスト内容	補足解説	Check
B. 脅威の理解					
	1　業界のセキュリティ動向の検討				
		1.1	自組織が属する業界を攻撃するような攻撃者のタイプを分析しているか		
		1.2	自組織が持つ情報の中から、攻撃者が関心を持つ情報が特定されているか		
		1.3	重要な資産・データを特定し、それらに対するリスクを識別しているか		
		1.4	重要な資産を保護するためのプロセスを定めているか		
		1.5	重要なシステムに対し適用可能なセキュリティ管理策はすべて実施されているか		
		1.6	情報の機微度に応じて、「高、中、低」の格付けが実施されているか	情報の格付けを行うことで、APT が狙う場所について合理的な推測が可能となる。	
		1.7	自組織におけるセキュリティ方針・計画の中で、情報システム・重要データが扱われているか		
	2　外部脅威　攻撃者に係わる情報の収集と交換				
		2.1	攻撃者に係わる情報収集能力の構築		
		2.1.1	攻撃者に関する情報の生データにアクセスする役割、およびデータに基づいて意思決定を行う役割をそれぞれ定義しているか		
		2.1.2	アナリストに各種情報源の利用許可をどの程度認めるかを定義しているか	情報源には少なくとも以下の情報を含む。 ・APT プロファイル ・公開情報調査の結果 ・過去のインシデント報告 ・アナリストのメモ等	
		2.1.3	APT プロファイルは、常に最新の状態に更新されているか	月に 1 回は検証を行うことが推奨される。	
		2.1.4	APT プロファイルには、必要な情報がすべて含まれているか	APT プロファイルには次の情報を含む。 ・標的となった文書 ・嗜好性 ・活動時間帯 ・マルウェアやツールキットの分析結果 ・周辺からのインシデント報告および入手可能な全ての記録	
		2.1.5	異なる複数の APT プロファイルについて、相互関連の有無を定期的に検証しているか		
		2.1.6	アナリストは、収集したデータと攻撃者に係わる情報の間の関連付けを実施することを許可されているか		
		2.1.7	初期侵入段階で判明した情報と APT プロファイルを活用し、状況を特定するための手順が定義されているか		

			チェックリスト内容	補足解説	Check
		2.1.8	防御ツールを評価する場合は、攻撃者との間に存在する能力差を考慮に入れて実施しているか	攻撃者によって駆使する攻撃手法は変わるため、想定されている攻撃者が行うであろう攻撃手法に対して、それを防ぐことができるかどうかに評価項目を絞ることができる。	
		2.1.9	攻撃者が目標を達成するために必要と考えられる技術に対し、組織の対処方法は定義されているか		
		2.1.10	組織から盗んだ情報を理解するために、攻撃者が必要とする専門知識は何かを把握できているか		
		2.2	**攻撃者に係わる情報 を共有する際の留意点**		
		2.2.1	情報共有のための高いレベルの関係を構築し維持している競合他社を含む業界内外のパートナーを特定しているか		
		2.2.2	競合他社を含む業界内外のパートナーから得た情報には、機密保持に関する注意事項が注記されているか		
		2.2.3	競合他社を含む業界内外のパートナーとの情報共有は安全な方法で実施されているか	安全な方法とは、例えば次のような特徴が含まれる。 ・パートナーと共有される情報がネットワークを介して傍受されない ・傍受された場合でも、解読できない	
		2.2.4	技術情報の交換の場やワーキンググループ等に積極的に参加しているか	参加者には各組織の CISO レベルの責任者が含まれることが望ましい。最新のインディケータや事例の共有ができるように定期的に参加する必要がある。	
		2.2.5	パートナーや競合他社から提供された情報について、透明性の高いフィードバックを行うための手続きが整備されているか		
		2.2.6	組織が侵害された場合の、法執行機関への通知と連携、マスコミへの対応についてのプロセスが整備されているか		
B. 脅威の理解	**3**		**内部脅威　脆弱性スキャンとペネトレーションテスト**		
		3.1	**脆弱性スキャンの実施**		
		3.1.1	ネットワーク上のすべてのシステムにおいて、毎週またはそれ以上の頻度で脆弱性スキャンが実行されているか	スキャンには SCAP により検証済みの脆弱性スキャナを使用することが望ましい。このスキャナは、コードベースの脆弱性と、構成ベースの脆弱性の両方を検出することが可能である。 最も重要な脆弱性の優先リストと、システム管理者と各部門がリスクを削減する際の効果を比較したリスクスコアを、各担当システム管理者に配布しておくことが望ましい。 ※SCAP - Security Content Automation Protocol：セキュリティ設定共通化手順	

チェックリスト内容			補足解説	Check
B. 脅威の理解	3.1.2	イベントログと脆弱性スキャンの情報との関連付けはされているか	これには以下 2 つの目標がある。 ・通常の脆弱性スキャンツール自体のアクティビティが記録されていることを確認する ・攻撃検知イベントを前述の脆弱性スキャン結果と関連付けて、特定のエクスプロイトが既知の脆弱な標的に対して使用されたかどうかを判別する	
	3.1.3	各システムで脆弱性スキャンが実行される権限は適切であるか	セキュリティ構成を分析するためには、各エンドシステムでローカルに実行されているエージェントを使用するか、テストするシステムで管理権限を付与されているリモートスキャナを使用して、脆弱性スキャンを認証モードで実行する。 これには認証済みの脆弱性スキャン専用のアカウントを使用する必要がある。このアカウントは、その他の管理作業には使用してはならず、また特定の IP アドレスで特定のマシンに関連付ける。認証されている従業員のみが脆弱性管理ユーザインターフェイスにアクセスできるようにし、役割が各ユーザに適用されていることが必要である。	
	3.1.4	組織内の脆弱性スキャンが検知対象とする脆弱性が月次ベースで更新されているか	脆弱性は常に変化しており、次々に新しい脆弱性が発見されていく。これらの脆弱性を常に認識できるようにするためには、脆弱性情報サービスに登録し、最新の脆弱性情報の把握をしておくことが重要である。 このサービスから得られる情報を利用し組織の脆弱性スキャンが検知対象とする脆弱性の種類を月次ベースで更新することが推奨される。あるいは、使用する脆弱性スキャンツールを、関連するすべての重要なセキュリティ脆弱性で定期更新することで代替が可能である。	
	3.2	**ペネトレーションテストの実施**		
	3.2.1	外部および内部ペネトレーションテストを定期的に実行しているか	ペネトレーションテストは、企業システムを悪用するために使用できる脆弱性と攻撃の軌道を特定することができる。 部外者からの攻撃と内部関係者からの攻撃の両方をシミュレートするために、ネットワーク境界外（インターネットまたは組織での無線周波数）と、ネットワーク境界内（内部ネットワーク）から実行する必要がある。	
	3.2.2	ペネトレーションテストの実行に使用するすべてのアカウントのコントロールおよびモニタリングを行っているか	ペネトレーションテストの実行に使用するユーザアカウントとシステムアカウントが、正当な目的に限って使用されることと、テスト終了後に除去、または通常機能に戻ることを確認する必要がある。	

カテゴリ 3　具体的防御策の検討

チェックリスト内容			補足解説	Check
C. 予防的なログの保持				
C. 予防的なログの保持	1　ログの取得と保守ポリシー			
	1.1	すべてのサーバとネットワーク機器には、NTP が 2 つ以上組み込まれているか	NTP - Network Time Protocol : 定期的に時刻情報を取得する同期化された時刻ソース ログ内のタイムスタンプが整合し、UTC（協定世界時）に設定されるようにする必要がある。	
	1.2	重要な資産に関するログを維持しているか	DNS、プロキシ、ファイアウォールなどが対象となる。	
	1.3	各ハードウェア装置と、そこにインストールされているソフトウェアの監査ログには、必要な要素が含まれているか	必要な要素とは、最低限以下のものを示す。 ・日付 ・タイムスタンプ ・ソースアドレス ・宛先アドレス ・各パケットやトランザクションのさまざまなその他の有用な要素 システムでは、syslog エントリなどの標準化された形式や、Common Event Expression イニシアチブによって概略されている形式でログを記録する必要がある。システムが標準化された形式でログを生成できない場合は、ログを標準化された形式に変換するためにログ正規化ツールを適用が可能である。	
	1.4	ログを格納するすべてのシステムには、生成されるログに適したストレージスペースが用意されているか	ストレージを定期的に確認し、ログ循環間隔の間にログファイルがあふれないようにする必要がある。 ログは、定期的にアーカイブしてデジタル署名することが望ましい。	
	1.5	ログの保守ポリシーは策定されているか	数カ月にわたり組織が侵害されているにも関わらず、その侵害が検出されないことがある。こうした事態を正確に判断するためには、ログを長期間にわたって保持する必要がある。	
	1.6	特に重要なログは、一元管理下におかれているか		
	1.7	ログの一元管理システムは、他のネットワークから保護されているか	ログを格納するデータベースや、SIEM などのツールがアクセスするデータをすべて含む。	
	1.8	ログファイルを参照するタスクに係る作業者は特定されているか、および作業時間がどの程度であるか把握されているか	対象者の一覧や、一般的なタスクに要する時間はインシデント対応チームにとって重要な情報となる。	
	1.9	ログにおける異常を特定するために、最低限、隔週程度のレポートを発行しているか	セキュリティ担当者やシステム管理者は異常を積極的に確認し、判明した内容を文書化する必要がある。	

チェックリスト内容			補足解説	Check
D. ポリシーやガイドラインの整備				
D. ポリシーやガイドラインの整備	**1 セキュアな構成**			
		1.1 サーバおよび端末のハードウェア、ソフトウェアのセキュアな構成		
		1.1.1	自社のオペレーティングシステムに適用するためのセキュアに強化された標準イメージ(※)が存在するか	※標準イメージとは、社内 OA 用 PC へのインストールの際に使用する社内標準 OS、及びソフトウェアの集合体を指す。たいていの場合、OS インストールディスクやイメージファイル(img,iso など)、仮想 OS の状態で保管しておく。予め基盤となる OS に特定のパッチを適応させたり、既定のソフトウェアを同梱しておくなどができる。 標準イメージは、基盤となるオペレーティングシステムと、システムにインストールされているアプリケーションを強化したものである必要がある。 一般的に、この強化には次の処理が含まれる。 ・不要なアカウントの削除（サービスアカウントを含む） ・不要なサービスの無効化または削除 ・実行不能なスタックとヒープの構成 ・パッチの適用 ・開いている未使用のネットワークポートのクローズ ・侵入検知システムおよび侵入防止システムの実装、ホストベースのファイアウォールの使用 これらのイメージは、定期的に検証して更新し、最近の脆弱性と攻撃の軌道に照らし合わせてセキュリティ構成を更新する必要がある。	
		1.1.2	自動化パッチ適用ツールおよびプロセスは、アプリケーションとオペレーティングシステムの両方に実装されているか	古いシステムにパッチを適用できない場合は、アプリケーションを最新バージョンに更新する。古い未使用のソフトウェアはシステムから削除する。	
		1.1.3	管理権限を付与するユーザは、オペレーティングシステムの管理に必要な知識があり、かつ構成変更を業務上必要とする少数のユーザに限定しているか	これにより、無許可のソフトウェアのインストールやその他の管理権限の濫用防止が可能。	
		1.1.4	新規導入されるシステムを構築する際にはセキュアに強化されたイメージを利用し、厳密な構成管理を実施しているか。	既存のシステムのセキュリティが侵害された場合は、セキュアなイメージを適用して再構築することが可能。このイメージに対する定期的な更新または例外を組織の変更管理プロセスに統合する必要がある。また、組織で使用するワークステーション、サーバ、およびその他のシステムタイプのイメージをそれぞれ作成する必要がある。	

		チェックリスト内容		補足解説	Check
D. ポリシーやガイドラインの整備		1.1.5	オペレーティングシステムのマスターイメージは安全に構成されたサーバに格納されているか	完全性チェックツールによる継続的な検証と適切な変更管理により、イメージに対して許可された変更のみを行うようにする。これらのマスターイメージは、本番システムに適用するコピーイメージとともに、本番ネットワークから隔離された環境で保管する。	
		1.2	**ネットワーク機器のセキュアな構成**		
		1.2.1	組織で使用するネットワーク装置のセキュリティ構成は、組織の変更管理委員会によって文書化、確認、および承認されているか	組織で使用中の各種のネットワーク装置用に定義された標準のセキュアな構成と、ファイアウォール、ルーター、およびスイッチの構成とを比較する。 標準の構成または標準の構成への更新からの逸脱をすべて文書化し、変更管理システムで承認する必要がある。	
		1.3	**特権 ID、アクセス権のセキュアな構成**		
		1.3.1	管理権限を最小限に抑え、必要な場合にのみ管理アカウントを使用しているか	管理者権限の使用に関する監査を行い、異常な動作をモニタする。	
		1.3.2	すべての管理者アカウントは上級管理者によって承認されているか	自動化ツールを使用して、すべての管理アカウントのインベントリを作成し、デスクトップ、ラップトップ、およびサーバで管理権限を持つ各ユーザを確認する。	
		1.3.3	すべての管理パスワードのルールは、文字、数字、特殊文字を使用した複雑なものになっており、辞書に載っている単語が使用されないようにしているか	特殊文字と辞書にある単語を複数使用したパスフレーズは、適切な長さである場合には許容する。	
		1.3.4	新規導入する装置は、ネットワーク接続する前に、デフォルトで設定されているパスワードをすべて変更しているか		
		1.3.5	すべてのサービスアカウントには、長く推測しにくいパスワードが設定されているか、またパスワードは定期的に変更されているか		
		1.3.6	すべてのパスワードはハッシュ化または暗号化して保管しているか	ハッシュ化されたパスワードにはソルトを追加し、NIST SP 800-132 の指針または類似の指針に従う。 また、システムがユーザを認証するために必要となるこれらの暗号化またはハッシュされたパスワードが含まれているファイルを、スーパーユーザ権限でのみ読み取り可能にする必要がある。	
		1.3.7	管理者アカウントはシステム管理アクティビティのみに使用させているか	アクセスコントロールリストを使用して、管理者アカウントの使用制限を行う。 電子メールの閲覧や、文書作成、Web ブラウジングに使用されないようにする必要がある。特に Web ブラウザと電子メールクライアントは、決して管理者として実行しないよう構成する。	

チェックリスト内容				補足解説	Check
D. ポリシーやガイドラインの整備		1.3.8	管理者には、管理用アカウントと非管理用アカウントにそれぞれ異なる固有のパスワードを設定させているか	ポリシーとユーザへの啓蒙を通じて、管理者に対して要求する事項である。管理アクセスを必要とする各個人には、独自に別個のアカウントを付与する必要がある。ユーザは、緊急時には、Windows の「administrator」または UNIX の「root」アカウントのみを使用する必要がある。ドメイン管理アカウントは、システム管理に必要な場合に、ローカル管理者アカウントの代わりに使用する必要がある。	
		1.3.9	オペレーティングシステムは、最低 6 か月間はパスワードを再利用できないように構成されているか		
		1.3.10	すべての機密情報は、ファイアウォールによるフィルタリング機能を備え、かつ適切に分離された VLAN に配置されているか	信頼性の低いネットワークを介した機密情報の通信はすべて暗号化する必要がある。	
	2 モニタリング				
		2.1	**無線 LAN のモニタリング**		
		2.1.1	ネットワークに接続されている各無線装置が、許可された構成とセキュリティプロファイルに一致しない場合に、アクセスを拒否しているか		
		2.1.2	ネットワーク脆弱性スキャンツールは有線ネットワークに接続されている無線アクセスポイントを検知するよう構成されているか	ネットワーク脆弱性スキャンツールによって特定された装置は、許可された無線アクセスポイントのリストと照合して一致を確認する。無許可の不正なアクセスポイントは機能しないようにする必要がある。	
		2.2	**アカウントのモニタリング**		
		2.2.1	ビジネスプロセスと所有者を関連付けることができないアカウントは、すべて無効化されているか		
		2.2.2	すべてのアカウントには、有効期限が設定されているか		
		2.2.3	違反者等のアカウントリストを含むレポートが、システムで毎日自動的に作成されるよう設定されているか	違反者等のアカウントリストには次のアカウントを含む。このリストは、関連するシステム管理者にセキュアな方法で送信する必要がある。 ・ロックアウトされたアカウント ・無効にしたアカウント ・パスワードの最大有効期間を超えたパスワードを使用するアカウント ・有効期限がないパスワードを使用するアカウント	
		2.2.4	すべてのアカウントは、従業員の離職または請負業者の解約時に即時に無効化しているか	アカウントを削除する代わりに無効化することで、監査証跡を保持することができる。	
		2.2.5	すべてのユーザアカウントは、一定の未使用期間が経過後に自動的にログオフするよう設定されているか		

チェックリスト内容				補足解説	Check
D. ポリシーやガイドラインの整備		2.2.6	すべてのシステムには、スクリーンロックが設定されているか	無人のワークステーションへのアクセスを制限するために必要である。	
		2.2.7	アカウントの使用状況をモニタして休止アカウントであるかどうかを判別し、ユーザまたはユーザのマネージャに通知する仕組みがあるか	このようなアカウントが不要である場合はアカウントを無効化する。システム復旧または継続的な運用に必要なベンダ保守用アカウントなどの例外が存在する場合は文書化してモニタリングする必要がある。	
		2.2.8	管理者以外のすべてのアカウントは、文字、数字、および特殊文字を使用する強力なパスワードを設定し、少なくとも 90 日ごとに変更するよう設定されているか	最小有効期間は 1 日で、これまでに使用したパスワードを再度使用してはならない。これらの値は、組織の特定のビジネスニーズに基づいて調整してよい。	
		2.2.9	すべてのアカウントは、一定のログイン失敗回数に達した場合に一定期間にわたってロックされるよう設定されているか		
		2.3	**外部データ送信のモニタリング**		
		2.3.1	機密データを保持するモバイル装置とシステムには、認可されたハードドライブ暗号化ソフトウェアが適用されているか		
		2.3.2	社内で利用している暗号化装置と暗号化ソフトウェアは、公的に厳しく検査されたアルゴリズムを使用するように構成されているか		
		2.3.3	暗号化および完全性コントロールを適用する必要がある機密情報は、特定されているか	データ評価を実施することで特定することができる。	
		2.3.4	クラウドプロバイダ（外部委託）のデータ保護に関するセキュリティ対策をレビューを行っているか		

チェックリスト内容				補足解説	Check
E. インシデント対応機能の整備と人材育成					
E. インシデント対応機能の整備と人材育成	**1 インシデント対応機能の整備**				
		1.1	インシデントに対応する担当者の役割の定義を含めた、インシデント対応手順を策定しているか		
		1.2	コンピュータおよびネットワークインシデントを処理するための職種と職務は、特定の個人に割り当てられているか		
		1.3	インシデント対応プロセスをサポートする管理担当者が定義されているか	管理担当者は、重要な意志決定に作用することが求められる。	
		1.4	異常な事象を検知した場合に、インシデント対応チームに報告するための組織全体の標準を規定しているか	組織全体の標準には、次の内容が含まれる。 ・報告に必要な時間 ・報告を行うための仕組み ・インシデント通知に含める情報の種類 この報告内容は、組織がコンピュータインシデントに取り組むためのすべての法的要件または規制要件に従って、JPCERT/CC 等の専門組織へ通知されることが望ましい。	
		1.5	セキュリティインシデントの報告に使用するサードパーティー(※)の連絡先に関する情報を収集、保持しているか	※IPA、JPCERT/CC、監督官庁（警察を含む）等の関連機関やセキュリティベンダーなどを指す。 連絡先には少なくとも電子メールアドレス、Web ページの情報などを含むべきである。	
		1.6	従業員と請負業者を含むすべての担当者を対象に、インシデント対応チームへのコンピュータの異常とインシデントの報告に関する情報を公開しているか	インシデント報告などの情報を日常的に公開することで、従業員の意識向上につながる。	

			チェックリスト内容	補足解説	Check
F. トレーニングおよび演習の実施					
F. トレーニングおよび演習の実施	**1 トレーニングの実施**				
		1.1	全ての対象者に対して、少なくとも年1回の情報セキュリティに関するトレーニングが実施されているか	対象者とは、組織のセキュリティチームとしてインシデント対応を行う従業員を指す。	
		1.2	従業員に対するトレーニングは、常に最新のもので、複数の業務分野がカバーされているか		
		1.3	一般従業員向けのトレーニング では、従業員一人一人の役割や脅威とその対処方法、業務への影響について取り上げられているか		
		1.4	セキュリティチームのメンバには、基本的なネットワークやセキュリティに関するスキルについて資格要件が定められているか	資格を取得するためには、内部教育を同時に行う必要がある。資格要件にはマネージャの場合はCISSP、アナリストの場合には他の技術的資格などが挙げられる。	
		1.5	トレーニングプログラムには実地研修（ハンズオン）を含められているか	最低でも何らかの社内トレーニングプログラムが実施されていることが望ましく、さらに実地研修が含まれていると従業員のより深い理解と意識向上が期待できる。	
		1.6	従業員に必要なスキルと、従業員が守っていない行動に関するギャップ分析を行っているか	分析結果を使用して、全従業員を対象としたベースライントレーニングと意識向上のためのロードマップを策定することが可能。	
		1.7	各従業員のスキルのギャップを解決するためのトレーニングを実施しているか	可能であれば、上級職員がトレーニングを実施する、あるいは、外部の講師を招いてオンサイトトレーニングを実施することが望ましい。	
		1.8	オンラインセキュリティ意識向上プログラムを実装しているか	このプログラムは、以下の特徴を有す。 （1）不正侵入で一般に使用される手法のうち、個人のアクションによってブロック可能なものに重点を置き、 （2）従業員にとって利用しやすい短時間のオンラインモジュールとして提供され、 （3）最新の攻撃テクニックを反映するため頻繁に（少なくとも毎年）更新され、 （4）すべての従業員が少なくとも毎年受講し修了するよう義務付けられ、 （5）従業員の修了状況が確実にモニタされる。	
	2 演習の実施				
		2.1	演習の目的を定めているか		
		2.2	演習計画では範囲、役割、責任、権限などの分界点を明確にしているか		
		2.3	演習を通じて、社内のセキュリティ基本方針、計画のすべてを検証しているか		
		2.4	演習を事前告知するか、あるいは、開示せずに行うかを定めているか		

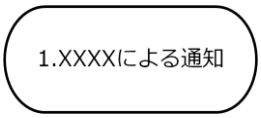
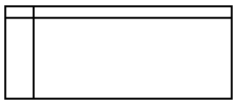
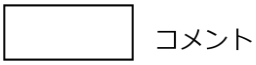
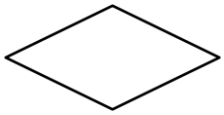
チェックリスト内容				補足解説	Check
F. トレーニングおよび演習の実施		2.5	演習の目的が APT 活動に対する準備、防御、対応に係わる組織の能力評価となっているか		
		2.6	関連するすべての部門が、演習の計画に関与できているか		
		2.7	演習によって、部門間や外部の組織にまたがる情報共有を検証できているか		
	3 演習後の対応に関する留意点				
		3.1	演習実施報告書には、成功点・失敗点、ポリシーやプログラム、および演習の改善方法が網羅されているか		
		3.2	改善が必要とされる分野に、改善プロジェクトの責任者が配置されているか		
		3.3	演習計画および演習実施報告書がプロセスの改善につながっているか		
G. インシデント対応計画の検証					
G. インシデント対応計画の検証	**1 インシデント対応計画の検証**				
		1.1	インシデント対応計画の評価について主管となる部（課）長を任命し、業務の実施に関して決裁権限を付与しているか		
		1.2	事業環境や業務に影響を及ぼすリスクを洗い出しているか		
		1.3	評価の対象となるシステム、機能、またはプロセスは定められているか	これらは、検証内容によって重要度が変化しても良い。複数の事業部門から選択しても良い。	
		1.4	対応計画の評価によって得た教訓を報告書にまとめる手順が確立されているか		
		1.5	報告書内では、トレーニングの実施結果と想定する所要時間を比較されているか		
		1.6	検証の際に、インシデント対応計画の変更・更新が検討されているか		
		1.7	改善されたインシデント対応計画に基づき、対応手順は再度検証されているか		

付録 B：インシデント対応フロー及びチェックリスト

想定される使用方法

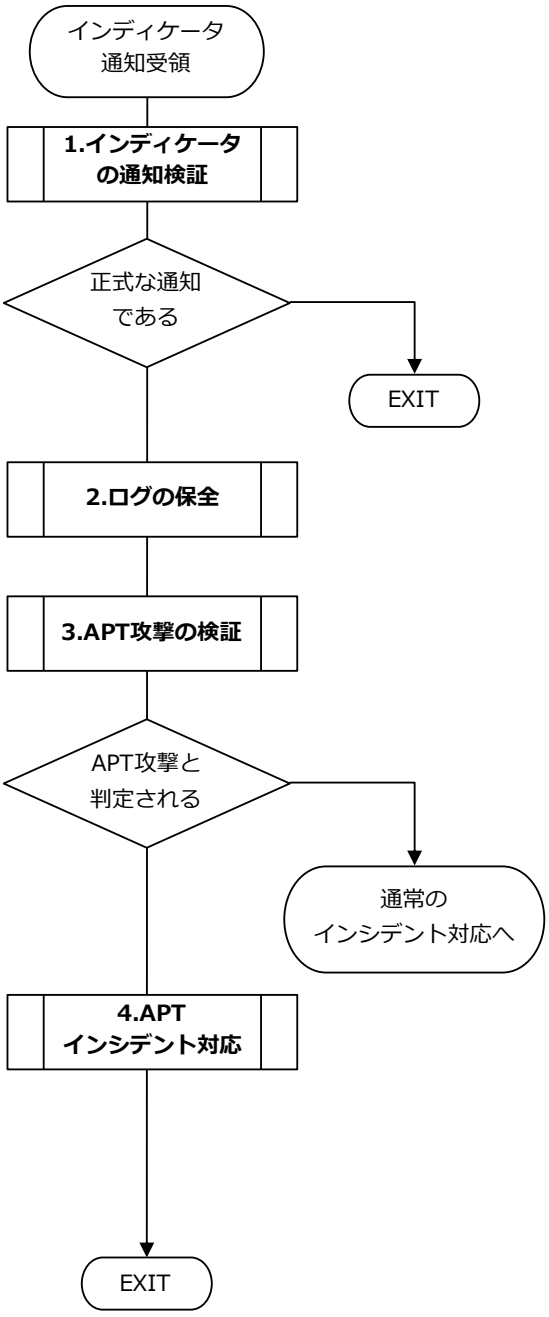
一連のフローは、APT インシデント対応についてまとめたものである。このフローを利用することで、APT への初動対応手順を網羅できる。

フロー凡例

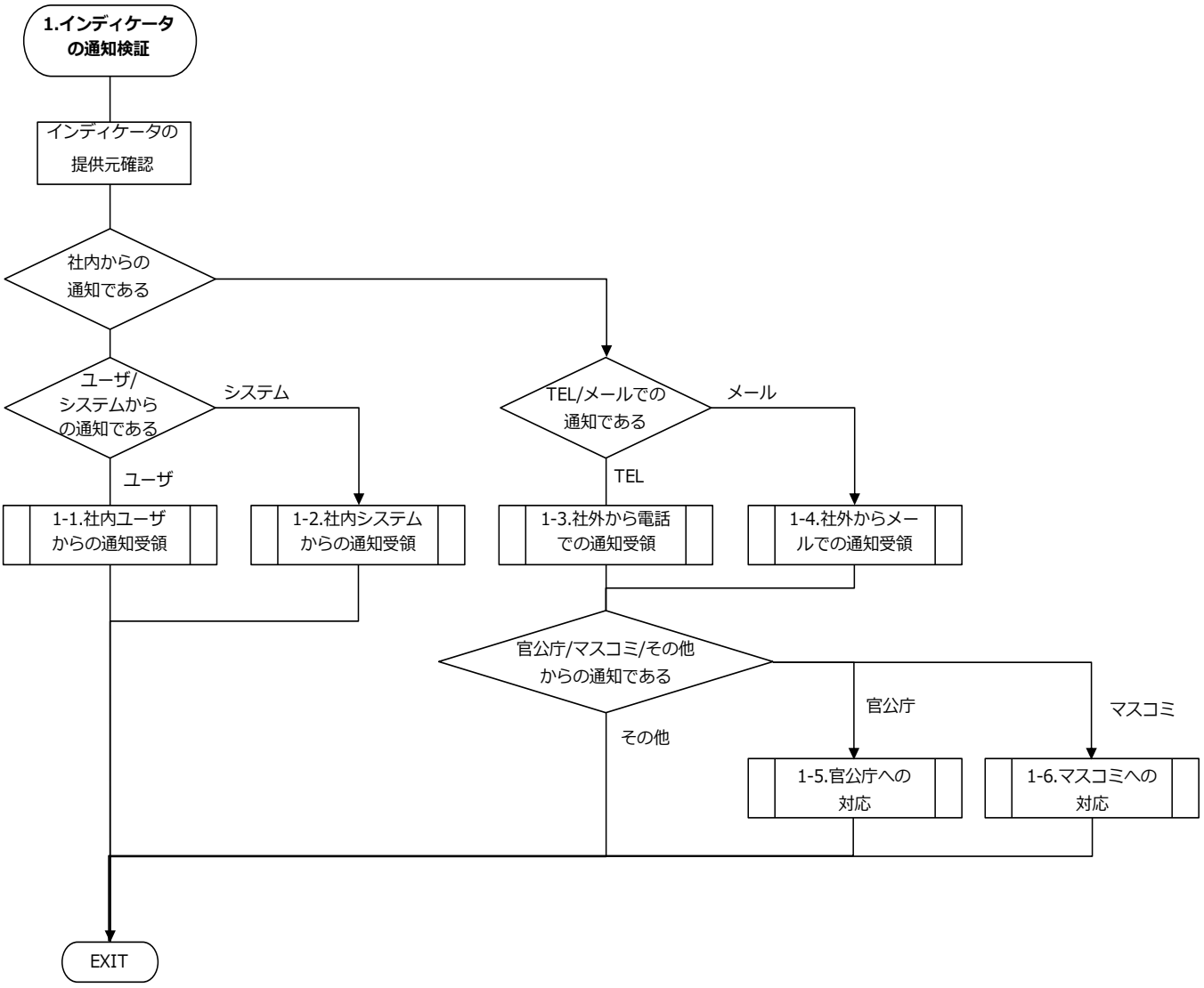
No	区分	記号	呼称	説明
1	開始・終了		作業開始	作業フローの開始を表す。 フローの起点（キック）となるイベントを枠内に記載する。
2			作業終了	作業フローの終了、もしくは呼び出し元のフローへの戻りを表す。
3	作業		手順	作業者が実施する手順を表す。
4			手順上の注意	主に行ってはならない手順や注意事項などを表す。
5			定義済みの手順 （サブルーチンの呼出し）	他で定義されているフローを呼び出す。呼び出したフローが終了すると次処理へ進む。
6			別担当者への連絡・アクション	インシデント対応チーム外の担当者への連絡やアクションを表す。
7			コメント・注釈	各手順に関するコメント・注釈を表す。 手順を表す記号の右横に配置される。
8			判定	Yes（OK）の場合は下へ、No（NG）の場合は横へ分岐する。これ以外に分岐パターンが存在する場合には、判定基準をフロー内に記載する。
9	その他・手段		電子メール	電子メールによる連絡、データ送付
10			電話	電話での連絡

インシデント対応フロー

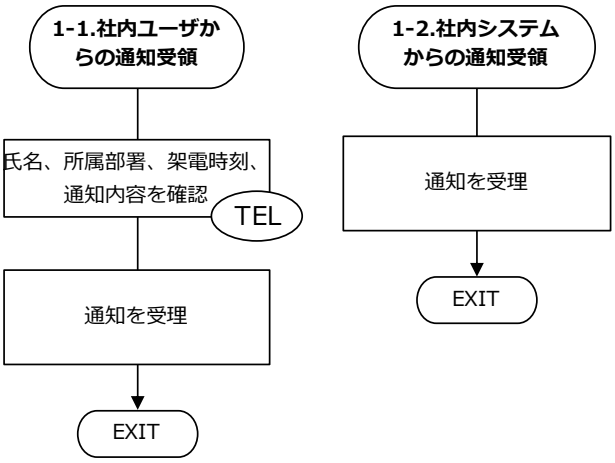
以下のフローはインシデント対応時の全体フローを表す。番号が記載されている各手順は次ページ以降にその詳細フローを記している。

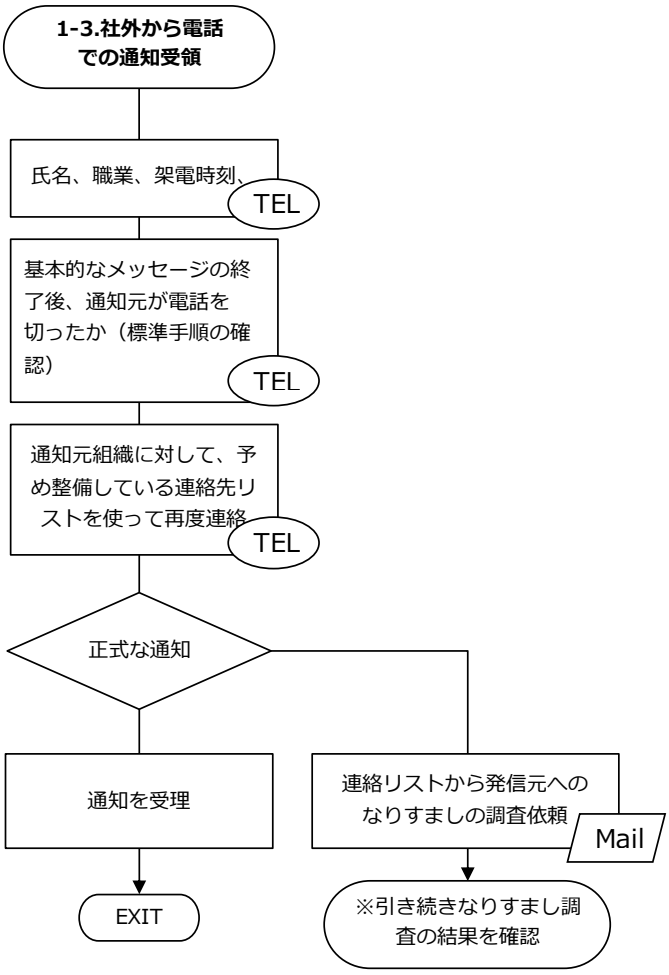


1.インディケータの通知検証(1/3)



1.インディケータの通知検証(2/3)

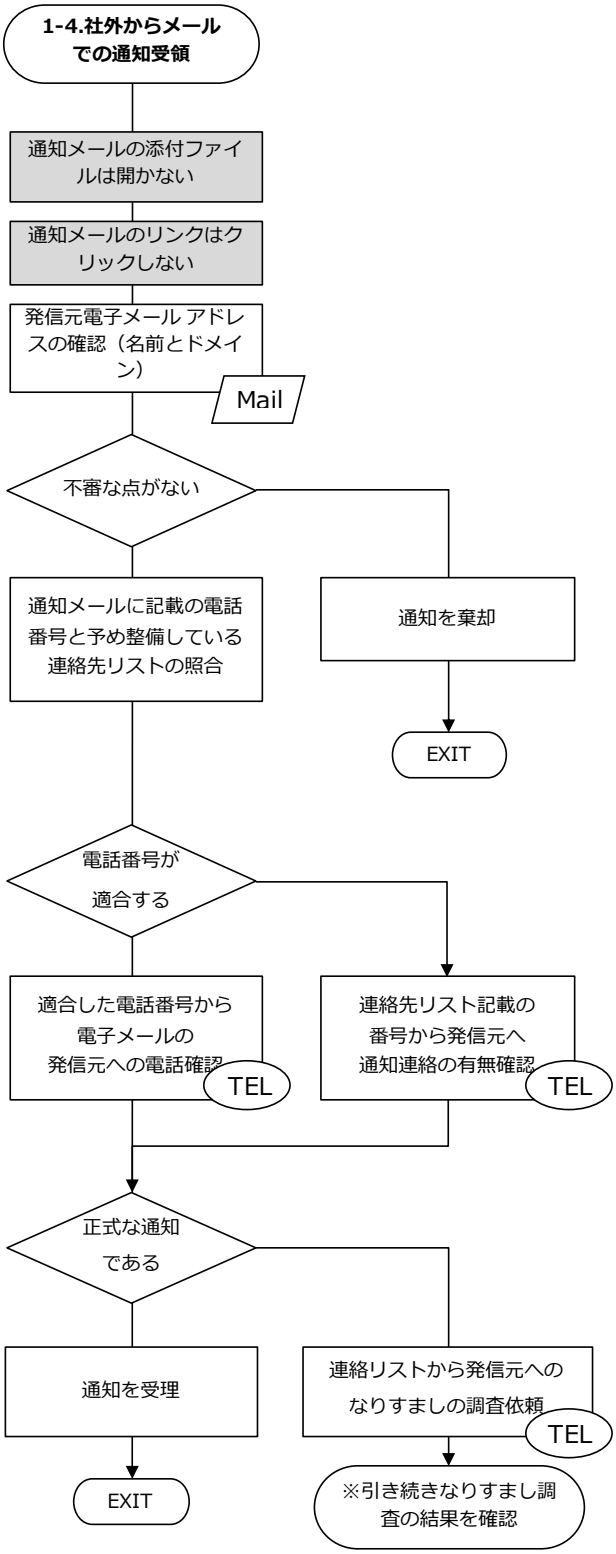




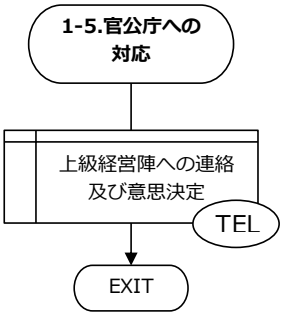
見知らぬ組織からの通知受領

正式な通知を確認する際、各社で予め整備している連絡先リストをもとに通知元を検証するのは有効な手段であるが、これまでコンタクトを取ったことがない組織からコンタクトがあった場合や、直接海外からの情報を受け取った場合などは、信頼できる情報提供であるにも関わらず通知を棄却してしまい、貴重な情報源を失ったり、自組織への風評被害を招く可能性も考えられる。
特定の組織から初めてコンタクトを受け取った場合には、JPCERT/CCやその他の信頼できる組織に問い合わせることも一つの手である。また、初めてのコンタクトを行う場合も、相手企業に無視されることを考慮し、JPCERT/CCやその他の信頼できる第三者を経由して情報伝達を行うことが有用な場合もある。

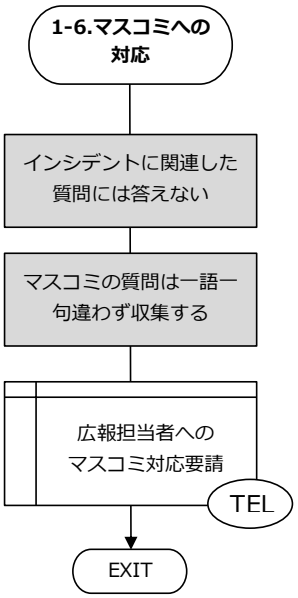
1.インディケータの通知検証(3/3)



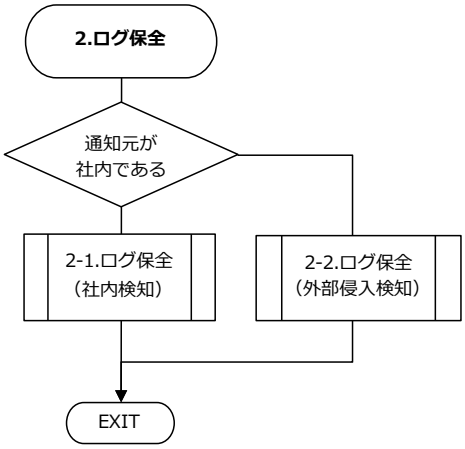
通知されたメールがなりすましの可能性があるため、所持している連絡先リストを用い通知を確認すること

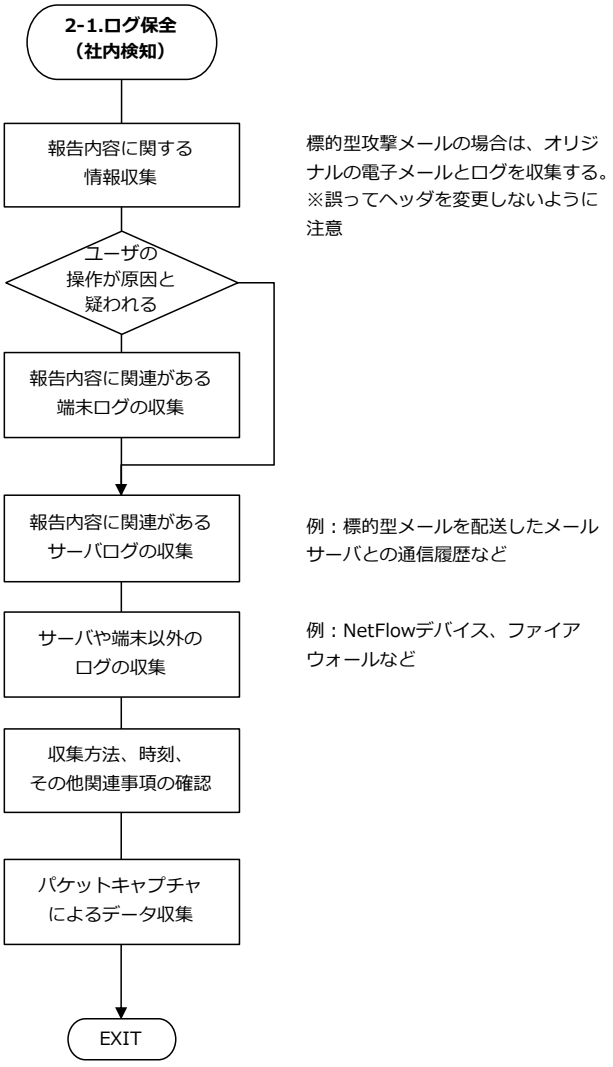


官公庁から通知が来ていることを上級経営陣へ連絡し、対応指示を仰ぐ。
以後のフローにおいても担当部署、上級経営陣への逐次報告を行うなどの適切なアクションが必要である。
（これらについては特にフローには記載しない。）



2.ログ保全

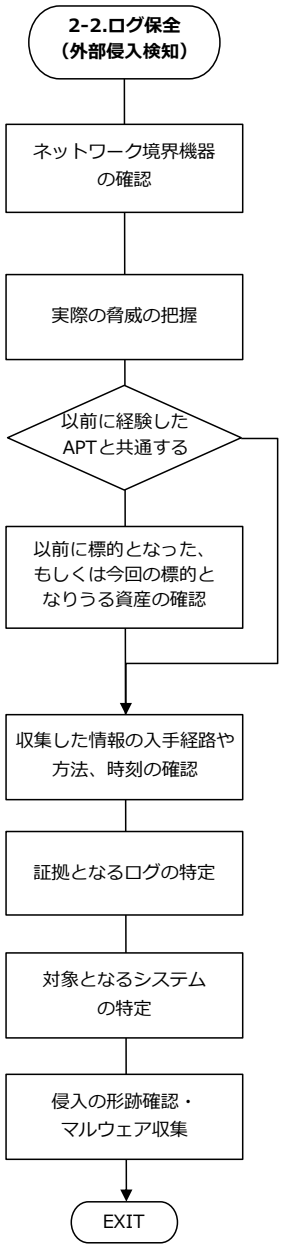




標的型攻撃メールの場合は、オリジナルの電子メールとログを収集する。
※誤ってヘッダを変更しないように注意

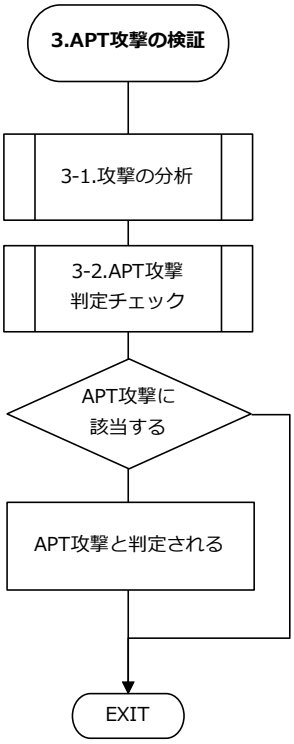
例：標的型メールを配送したメールサーバとの通信履歴など

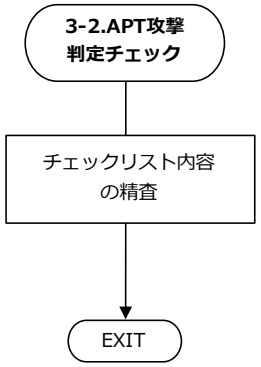
例：NetFlowデバイス、ファイアウォールなど



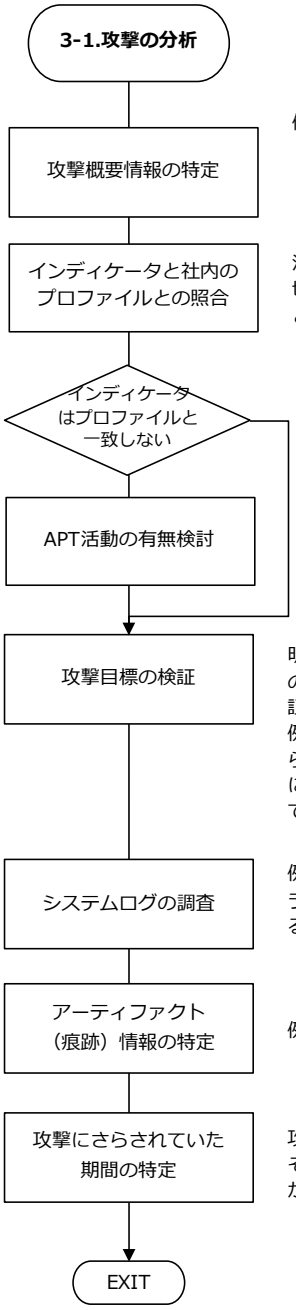
以前に経験したAPTと共通する特徴をもっていないかを確認する。

3.APT 攻撃の検証





次ページに示すチェックリストをもとに攻撃内容の確認を行う。
「Aで該当するものが2個以上」、もしくは「Aで該当するものが1個、Bで該当するものが2個以上」ある場合はAPT攻撃と判定される。



例：
・どのような攻撃（手法・経路等）なのか。
・使われたツールは何か。
・どのような初期情報があるか。

注：企業や組織がプロファイルを適切な状態に維持していることが条件となる。

明確に自社や自組織を標的としたものか、その前段階の試行なのかを検証する。
例：標的型攻撃メールが無作為に送られている。特定のグループを対象にしている。マルウェアを自分以外で検出している。

例：ログインの失敗や不正なプログラム・機能の実行を試したと思われる証拠など、不可解なログ

例：レジストリ情報、マルウェアなど

攻撃が何ヶ月や何週間も続いたのか、それとも数時間や数分で終わったのかなどを確認する。

APT 攻撃判定のためのチェックリスト

(A) APT の可能性が高いインディケータ	
A1	インディケータが、信頼できる攻撃者情報の専門家（法執行機関、JPCERT/CC など）から連絡されたものである
A2	特定されたマルウェアについて、公開情報（Google、ウイルス関連ブログなど）からは情報が得られない
A3	攻撃が新しいものである可能性が高い （APT の活動を示唆するものであるが、信頼できる情報源ですら知らなかった情報）
A4	フォレンジックやマルウェア・サンドボックス分析による挙動分析の結果、脅威であることが示された
A5	システムの利用者や管理者が説明できない圧縮ファイル、暗号化ファイルが、マルウェアとともにシステム上で発見された （攻撃の標的となったことを示すものであり、データが計画的に削除されていることが示唆される）
A6	標的となったシステムは組織の知的財産や重要な情報を格納している
A7	攻撃者が組織内で収集した情報は APT が高い関心を持つものである
A8	検出された活動に、以前に対処した APT インシデントと類似する点がある
(B) APT 可能性が中程度のインディケータ（APT、非 APT それぞれの可能性がある）	
B1	ソーシャルエンジニアリングと思われる手法が攻撃の中に含まれる
B2	標的となったシステムは、組織の業務にとって重要なものである **（例：ドメインコントローラー、エクスチェンジサーバなど）**
B3	狙われたシステムは他のシステムとの間にトラストチェーンを有している （例：他のサーバと通信するための管理上の認証があるなど）
B4	狙われたシステムが、指令を受けるため他のシステムに対して信号を送っていた （APT の活動に関連する C&C との通信の可能性）
B5	システムが、通常とは異なる方法で他の社内システムと通信していた （攻撃者による横断的侵害にシステムが利用されていることが示唆される。）

上記以外にも確認しておくべき点を以下に記す。

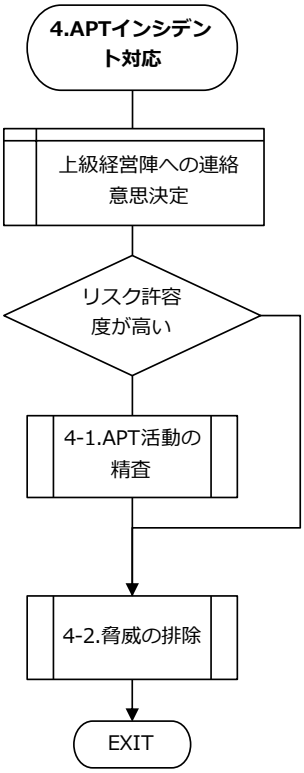
(C) APT との関連が薄いインディケータ	
C1	狙われたシステムは、ウイルス除去ツールや他の APT 用ではないツールによって特定された
C2	パッチ適用が最新の状態ではない （パッチが最新であった場合は、それがマルウェアによってインストールされた可能についても考慮する）
C3	特定されたマルウェアは公開情報から調査可能である （Google 検索、攻撃者に係わる情報サイト、ウイルス対策ブログなどで情報が得られることがある。）

チェックリストと APT 攻撃判定の考え方

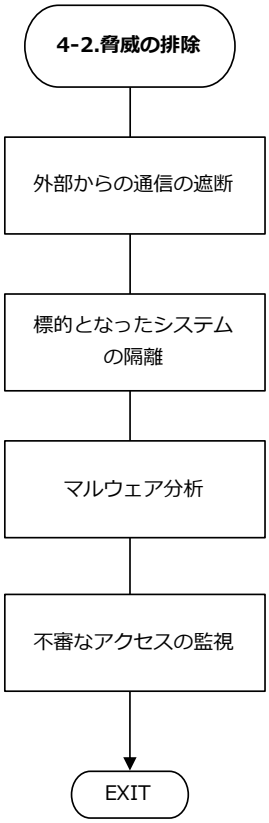
APT による攻撃と判定される場合はチェックリストの該当項目が以下の条件を満たす。

①「A. APT の可能性が高いインディケータ」に該当する項目が 2 個以上
②「A. APT の可能性が高いインディケータ」に該当する項目が 1 個、かつ
「B. APT 可能性が中程度のインディケータ」に該当する項目が 2 個以上

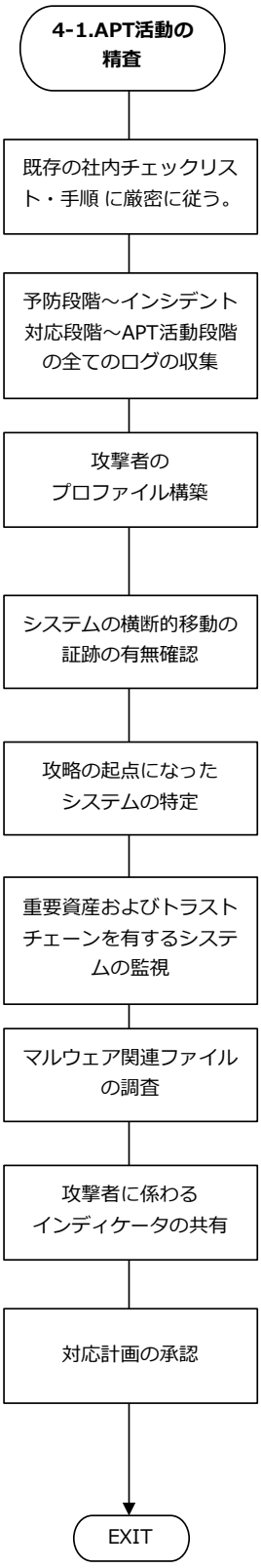
4.インシデント対応



「3.APT攻撃の検証」での調査結果等をもとに、APT攻撃が発生していることを上級経営陣へ連絡し、対応指示を仰ぐ。



APT攻撃が成功している場合、別のアクセス経路を使用し、さらに侵入されるリスクが高い。



チェックリスト・手順にない状況になった場合は、信頼できる情報共有組織や外部の専門家と調整する。

攻撃者について、その手法や動き、潜在的な目標に注目して攻撃者のプロファイルを構築する。また、既存のプロファイルとも比較する。

これまでに検知された活動との類似点を検証する。

圧縮ファイル、暗号化ファイルなど

他の組織との情報共有関係に基づく。共有内容は組織が定めた情報共有の指針に従う。

付録 C：観察可能な詳細

以下の表は、一般的な攻撃ベクター（侵入経路や攻撃手口）と、APT で確認された事象の一部について説明している。

観察可能項目	段階	観察項目の詳細
URL	準備	攻撃者が利用するインフラの 1 つである URL には、登録情報の中に有益な情報が含まれている場合がある。登録者名、メールアドレスおよび住所などを隠すことを目的としたレジストラの選び方自体がインディケータになる場合がある。レジストラが情報を隠ぺいすることがあるため、登録情報には高い信頼を置くことができないが、インディケータまたは攻撃者プロファイルへの付加情報になる場合がある。
インフラ構築	準備	インフラ構築は巧妙に隠ぺいされるため、組織が独力で確認するのは難しい。外部 ISP との接点がある CERT などは、連携によってインフラ構築の兆候を検知できる可能性がある。情報共有の枠組みはこうしたインディケータを組織に提供することができる。
メールアカウントの作成	準備	攻撃者は、標的型攻撃メールの成功率を高めるために、侵入に成功したシステムで新しいアカウントを作成する可能性がある。このような活動は、1 つの業界が攻撃を受けた後で、他の業界にも波及することが多く、情報共有関係を構築していればつぶさに観察可能である。また、ヘッダに含まれるキーワードを利用してインディケータとすることもある（「キーワード」や「フリーメール」に対して警告を表示するか、自動ブロックする）。
外部サイトへの侵入	潜入	攻撃者は、DMZ に置かれたシステムを攻略し、その後トラストチェーンを利用して、侵入したネットワークを横断する。システムを攻略できない場合には、C2 のトラフィックが IDS に検知されたり、アナリストに警告を表示することがないように侵害を行う。この段階におけるインディケータを得るには、組織が保有するサーバのサービスの正常/異常を判定することが重要となる。
標的型メール攻撃	潜入	攻撃者は、標的としている情報にアクセスしやすい個人を把握し、標的型メールによって情報を盗み出すための足がかりを作ろうとする。そのため、標的型メール攻撃の試みを検知しそれを適切に排除する。また標的型メール攻撃が成功した場合の考慮事項について組織内に周知徹底することで、攻撃の難易度が高くなり、攻撃者は別の侵入手段を検討しなければならなくなるだろう。
コールバックドメイン	潜入	多くの組織は、攻撃者が正面玄関から入ってくることを想定してインバウンド通信の対策に重点を置くが、攻撃者が多用するのは、特定の機器との間に設定されたトラストチェーンであり、未知のユーザであっても、このトラストチェーンが維持されることにある。そのため、アウトバウンド通信に注目してトラフィックを監視することは、組織のネットワーク上で発生したマルウェア感染などの検知と対応に役に立つ。インディケータとなりうる項目は、組織が取得するアウトバウンド通信の内容によって異なる。
システムレジストリの詳細	横断的侵害	攻撃の痕跡や攻撃者が辿ったステップを遡るための情報は、システムレジストリに存在することが多い。このレベルで何が起きているかを理解することは、インシデント対応者が APT に対処する際に役立つだろう。
マルウェアのコーディング	横断的侵害	高度なマルウェアは、重要な資産を持つシステムや重要資産へのアクセスを持つユーザのシステム上で見つかることが多い。仮に一般的なマルウェアしか発見できなかったとしても、それは標的型攻撃を成功させるためであったり、他のシステムを探索する際に利用されたと考えるべきである。このようなマルウェアについてフォレンジックを実施し、インディケータ情報を充実させることは、攻撃の先進性について検討する際に有益な場合が多い。

観察可能項目	段階	観察項目の詳細
正当な認証情報の使用	横断的侵害	攻撃者による認証情報の利用は、検知システムを回避される可能性が高く、阻止が最も困難なものであろう。認証情報の管理にはいくつもの製品が市場にあり、これらをコントロールする一連のソリューションも存在するほか、アクセスの時間や場所といった属性を、通常使用時と比較検証する検知方法もある。
重要資産への侵害	横断的侵害	多くの組織は、ネットワーク境界に置かれた機器のみ監視しており、攻撃者による横断的なアクセスを検知することができない。仮にこれらの侵入を検知し除去しても、攻撃者はなおアクセス手段を維持し、活動の検知をより一層難しくしてしまう。この問題に対するベストプラクティスは、重要資産を分離し、ネットワーク上に監視トラップを配備することである。専門のソリューションも市場に存在しており、それらを導入することも有用である。
データ流出	措置	データを窃盗から守る方法は、技術的なコントロールとプロセスによるコントロールを組み合わせたものであり、攻撃者の意図を理解することで標的となっている文書を予想して対策を実施するというものである。データ漏えい防御(DLP)ソリューションなども、データの外部流出を阻止する際に役立つ。
データ の改ざん	措置	攻撃者によるデータ改ざんに対しては、様々なソリューションが市場に出回っているが、注意しなくてはならないのは、改ざんに正当な認証情報が使われた場合、検知が難しいということである。

付録 D：補足資料

セキュリティチーム（SOC）やインシデント対応能力がある組織を構築している、または改善を図っている組織にとって、以下の参考文献は参考になるだろう。こうした文書は著作権で保護されているほか、ボリュームが大きいため本ガイドには添付できない。

(1) ISO/IEC 27001 は、ベストプラクティスとして世界で採用されているセキュリティ管理策の詳細が記載されている。国際標準化機構（ISO）から出版されたこの文書は、理論的には攻撃可能対象領域を縮小でき、セキュリティチームが標的型攻撃に、より集中できるようにする管理策をどのように実装できるか参考になるだろう。

http://www.iso.org/iso/catalogue_detail?csnumber=42103

(2) ソフトウェア工学研究所（Software Engineering Institute）は、「コンピュータセキュリティ・インシデント対応チームの設置と管理（Creating and Managing Computer Security Handling Teams (CSIRTs)）」を作成し一般に公表した。この文書は、セキュリティチームが能力向上のために実施できるプロセスや、CSIRT を構築・維持する際に考慮すべき事項について詳述したものである。

http://www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf

付録 E：その他の参考文書

(1) NIST Cybersecurity Framework
http://www.nist.gov/cyberframework/

(2) 重要インフラのサイバーセキュリティを向上させるためのフレームワーク 1.0 版，IPA
https://www.ipa.go.jp/files/000038957.pdf

(3) “ The CIS Critical Security Controls for Effective Cyber Defense Version 6.0”，Centers for Internet Security
https://www.cisecurity.org/critical-controls.cfm

(4) Malware Risks and Mitigation Report，BITS
http://fsroundtable.org/wp-content/uploads/2015/05/BITSMalwareReportJun2011.pdf

(5) Global Energy Attacks: “Night Dragon”，McAfee
http://www.mcafee.com/in/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

(6) Intelligence-Driven computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains， Lockheed Martin
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

(7) 経営者が知っておくべきセキュリティリスクと対応について，JPCERT/CC
https://www.jpcert.or.jp/research/aptrisk.html

(8) NIST SP.800-61, “Computer Security Incident Handling Guide”
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

(9) コンピュータセキュリティインシデント対応ガイド，IPA
http://www.ipa.go.jp/files/000015367.pdf

(10) Strategies to Mitigate Targeted Cyber Intrusions，The Australian Signals Directorate
http://www.asd.gov.au/infosec/mitigationstrategies.htm

(11) 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， JPCERT/CC
https://www.jpcert.or.jp/research/apt-loganalysis.html

「高度サイバー攻撃（APT）への備えと対応ガイド」付録文書

ログ保管に関する分析レポート

サイバー攻撃への対応のためのログ管理に関する考察

本資料について

本資料は、JPCERT/CC が 2013 年に米国デルタリスク社(Delta Risk LLC)に作成依頼した調査報告書 ” Log Data Retention Analysis Report” を翻訳し国内の企業や組織が利用できるように一部内容を修正したものである。

APT と呼ばれる高度サイバー攻撃への対応における要点となる、各種のログの保管と利用について、「高度サイバー攻撃（APT）への備えと対応ガイド」の内容を補足するものであり、企業や組織が、サイバー攻撃に備え対応するために、ログ保管の戦略やポリシー、手順を検討する際の参考として利用することを想定している。

目次

エグゼクティブサマリ

本レポートは、企業や組織がログ保管に関する戦略とポリシーを作成するにあたり参考とするための背景情報と分析・提言を提示する。

次の３つの分野におけるログ保管プラクティスについて調査を実施した結果を概説する。

・政府／規制
・民間企業のベストプラクティス
・インシデントレスポンスプロバイダの現場での対応

調査結果は、民間企業におけるログ保管の例として技術の高い企業組織のベストプラクティスを代表するものとなった。本レポートで提示するのは、APT とも呼ばれる高度サイバー攻撃に対し強力に対抗するために何が必要か、プラクティスにおいて何が達成されたか、何をしなければならないかについての寸表である。

６つの主要なログ種別（DNS ログ、プロキシログ、IP ログ、Netflow、サーバログ、ホストログ）について個別に検討し適切なログ保存期間とその理由について示す。本レポートは、企業や組織が APT による侵入の理解と対抗機能の実装のための段階的アプローチを開発し実行するため、必要なログ取得のレベルを決定するためのバックグラウンドデータを与える。

さらに APT 対応に役立つ他のログ種別（パケットキャプチャ、E-mail ログ、VPN ログ、アンチウィルスログ）についても考察する。これらのログ種別について、インシデントレスポンスや APT 対応のためのログ管理に関しいくつかの観点から検討をおこなった。これらのログについては、複数の変動要因がストレージ要件に影響するため、ログ保管期間を合理的に決めるのは困難である。

研究アプローチ

民間企業セクタにおけるログ保管のアプローチとインシデントレスポンスサービスのシナリオを理解するため、これらを対象としたインタビューを実施した。民間企業におけるログ保管のプラクティスを決定するため、Lockheed Martin と他のいくつかの匿名企業から、ログ保存期間と脅威別の有益なデータを得る方法についてのデータを得た。この調査結果においては様々な保存期間の組み合わせが示された。これらは APT 対応の成功ケースのシナリオを示している。

さらにインシデントレスポンスプロバイダである Mandiant と CrowdStrike にインタビューをおこない、これらの企業がインシデント対応の現場で調査する際の観点についての情報を得た。

政府／規制に関するデータは公開文書や公開情報から収集した。政府／規制に関するデータについて考慮すべき点は、それらが指示する内容は非常に漠然としていることである。それらが示すログ保管期間を特定することを試みたが、ほとんどの場合ログ保管期間について言及されることはない。

企業ネットワークへの脅威

分析の一部として、脅威の種類によってログ種別が持つ価値の違いについて考察した。インタビューの結果にもとづき、ログの価値を定性的に分析するため、脅威の種別を次の４つにグループ分けをおこなった。４つのグループとは、先進的で執拗な脅威（APT）、サイバー犯罪者、ハクティビズム、日和見的攻撃者である。

先進的で執拗な脅威（APT）：APT は、潤沢なリソースをもつ組織によりスポンサードされ、標的に対し諜報活動をおこなう能力を持つ攻撃者と定義される。APT は様々な目的を達成するためにネットワーク内部に潜伏し続ける。多くの場合、APT は機密情報の窃取を目的とするが、必要に応じて他のオペレーションも実行する。このタイプの脅威に対しては、情報を集めプロファイリングをおこなうことで、攻撃者が用いる攻撃手法や組織内で狙う標的を導き出すことが可能である。

サイバー犯罪者：サイバー攻撃により多額の金銭を得ることを目的とする犯罪者。多くの場合、これらの集団は個人情報、クレジットカード、銀行口座を狙う。ボットネットを操り、スパム送信サービスや DoS 攻撃のサービスを販売するケースもある。最近では、APT のオペレーションからの教訓を彼らのプロセスに採用し、APT 的な手段を取り始めている。これらのタイプの攻撃者に関する情報を集め、攻撃手法を導き出すことは可能である。

ハクティビズム：ハクティビストは社会的あるいは政治的声明を表明することを目的にシステムを侵害する。彼らは通常、既知の攻撃手法や脆弱性を利用する。彼らは通常 IRC や Twitter を使いオペレーションについて会話するため、防御する側にとっては攻撃者をプロファイリングし攻撃を予測することが可能である。ログの活用は、この種の攻撃の検知や緩和にとってあまり有効ではない。

日和見的攻撃者：これらの中には、一般的なハッカー（アマチュア、学生など）を含む。彼らは基本的な脆弱性を利用するがそれらが何をするかについて全てを理解してはいない。彼らの目的は単に侵害するシステムについて学ぶことである。このタイプの攻撃者の活動について積極的なインテリジェンスをおこなうことは非常に難しい。またこのタイプの攻撃者は様々な標的から大量のデータ収集をおこなうため、インシデント対応におけるログの利用価値は低くなる。

本レポートの中でログデータの利用に関して比較するため、これら４つの攻撃者とその能力を理解することは重要である。本レポートではそれぞれの攻撃者グループに対するログの価値について意見を述べる。例えば、ホストログは APT に対抗するには重要だが、日和見的な攻撃手段をとるハクティビストの攻撃に対しては一般的に役に立たない。ハクティビストや日和見的攻撃者は APT と違いネットワークの奥深くに留まろうとしない。

APT 対応のためのログ種別

高度な APT 対応能力を持ついくつかの組織に対しインタビューをおこない多数のベストプラクティスを集めた。それらのベストプラクティスをもとに APT の侵入を検知し被害を軽減するために高い価値を持つログについて考察した。ログ種別には DNS ログ、プロキシログ、ファイアウォールログ、Netflow、サーバログ、ホストログを含む。インタビューの中で価値を持つとされた他のログ（E-mail、アンチウィルス、VPN、DHCP、IDS アラート、パケットキャプチャ）についてもここで考察する。

主要なログについてのレビュー

DNS ログ：DNS はフィッシングメールのコールバックドメインとマルウェアの C&C チャネルを得られるため重要である。特異な DNS トラフィックを発見し相関付けできれば APT による活動の検知に役立つ。APT は古い URL を再利用し別の対象を攻撃するときにも同じインフラを使う傾向があり、whois ルックアップで繰り返し観測されることがある。DNS ログはコールバックドメインを特定し、APT 攻撃者の行動様式に関するインディケータを提供する。

プロキシログ：プロキシログはマルウェアの C&C とコールバックドメインについての追加情報を提供する。この情報はプロキシへの要求を拒否するルールの設定に利用できる。一般的に、ポリシーに基づいて拒否されたトラフィックは関心を持たれないことが多いが、ハッキング、トロイ、マルウェアの活動の調査には、成功した接続に関する情報に加えて拒否トラフィックもまた有用である。ホワイトリストとの比較により分析が必要なレコードの数を減らすことができる。プロキシログはマルウェアのコールバックと感染範囲に関するデータを示すことができる。

IP ログ：IP ログは一般的には firewall で取得される。攻撃者との通信を示唆するす特異な IP トラフィックを探し、IP データを理解することによりトラフィックの行き先についての地理的な絵を描くことができる。IP ログは内部の通信元 IP と外向きの通信先 IP を含む。IP の地理的な位置を特定することにより攻撃者の諜報活動の可能性を示すことができるかもしれないが、高い誤検知率が問題となる。外向き IP トラフィックは、C&C や他の悪意のある活動に使われる既知の IP との比較により、侵害された事実や、マルウェアのコールバックを示す可能性がある。これはイベントの相関付けの一部として利用できる。また、関連の有無をもとにパケットキャプチャ等の追加情報の必要性を判断できる。また特異な IP は、それ自体が攻撃活動のインディケータと紐づけられる。

Netflow：Netflow は組織間のセッションを示す。Netflow データはセッションに依存しトランザクションによりサイズが変動するので、保存されるデータ量を予測するのは難しい。例えば、２拠点間の長期間の通信は２つのフローと認識される。同様に、20 分のビデオストリーミングは１つのフローとされる。多くの異なる通信を長期間カバーするフロー情報を保存するには膨大な量のストレージが必要となる。Netflow のデータはセキュリティ分析者にとっては限られた情報しか提供しないが、より詳細な調査へのスタートポイントとなる。業界平均から大雑把にいえば、おおよそ 2GB のトラフィック毎に 1MB のストレージが必要である[24]。このデータは、データ窃取の可能性を分析するのに使われ、数値は行動様式に関するインディケータとして利用できる可能性がある。

サーバログ：サーバからのイベントやシステムデータは攻撃に関する多くの情報を生む。機密情報を持つサーバや DMZ にあるサーバについては特にそうである。Linux サーバでは syslog サーバを通じて詳細なロギングが可能である。Windows サーバは syslog フォーマットでログをとるよう設定する

[24] Netflow for Incident Detection, Scheck, 2009

ことができるが、すぐにサイズが大きくなる。ほとんどの場合、組織のセキュリティチームが関心を持つのは重要な syslog イベントに限られるので、syslog の保管に必要なストレージ容量を大幅に減らすことは可能である。サーバログを利用することにより特異なサーバ挙動とインディケータとの相関付けが可能となる。

ホストログ：大変有用であるが、効果的な相関付けをおこなうためには相当量のストレージを必要とする。ホストログにはパッチの適用状況、アンチウィルスの状態、その他様々な属性を含むべきである。ホストログを利用することによりシステムにおける特異な挙動とインディケータとの相関付けが可能となる。

主要なログの推奨される保存期間に関する分析

本レポートでは３つの機能エリア（政府／規制、一般企業、インシデントレスポンスプロバイダ）からの情報を提供することを試みたが、政府／規制の要求事項は、能力と特定の機能にフォーカスしており、どのログをいつまで保存すべきかについて明確な指針を与えない。そのため次の表では、先進的な APT 対応能力を備える一般企業のプラクティスと、クリーンナップ作業のために呼ばれるインシデントレスポンスプロバイダの要求事項を比較する。

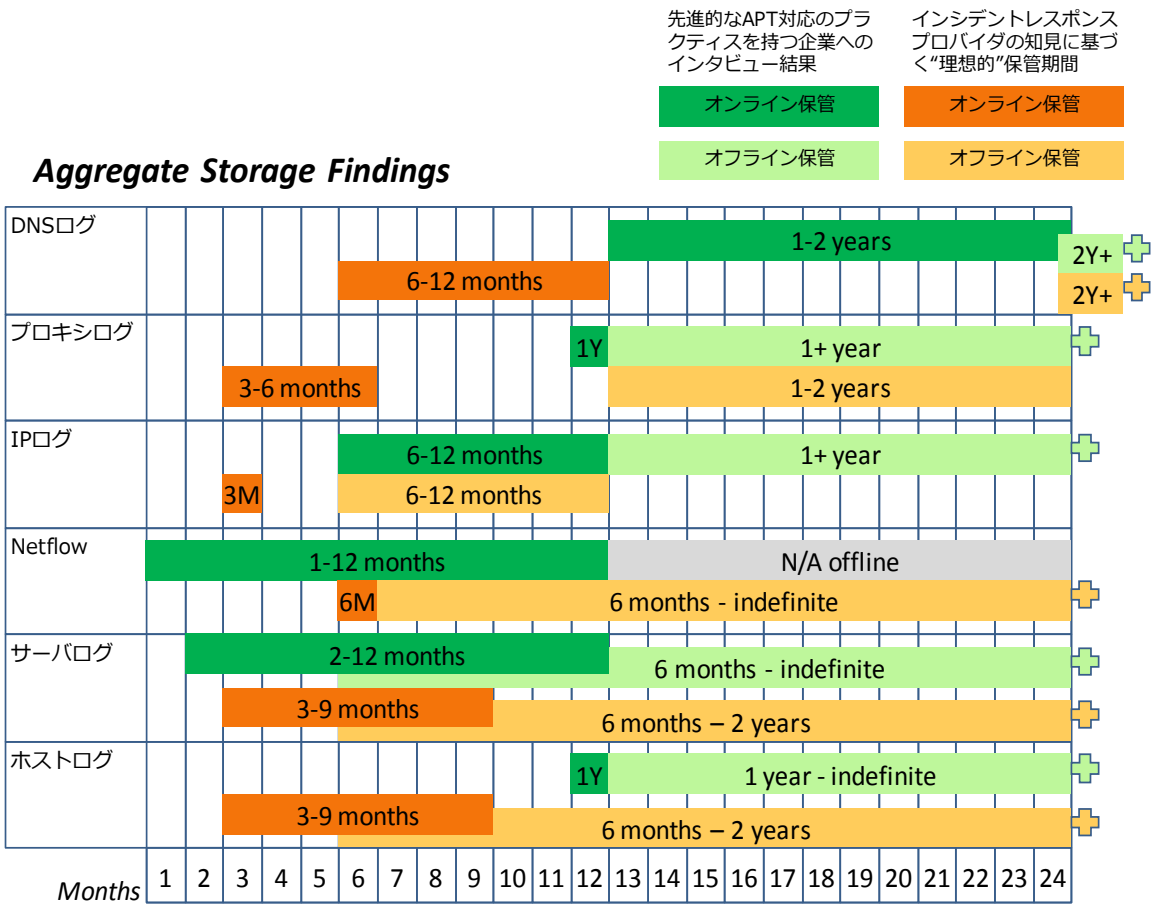


図 1：ログデータ保存期間の分布

上の図は一般企業での知見と、発生したインシデントのうち 80%を駆除した理想的なインシデントレスポンスからの知見を比較している。各エントリの範囲は特定のログ種別における保存期間の最短―最長値を示す。例えば DNS ログのオンラインでの保管は、インシデントレスポンスプロバイダへ

のインタビューによれば理想的企業では 6～12 カ月保存しているが、APT 対応のベストプラクティスをもつ企業へのインタビュー結果では保存期間は 1～2 年間とされる。それらのログはオフラインで 2 年またはそれ以上（いくつかのケースでは永久に）保管される。24 カ月というスケールはログ保管のバリエーションを包含できることから選択された。永久保存されるログには＋の印をつけた。

いくつかのログ種別では、一般企業（APT 対応のベストプラクティスをもつ企業）の平均値は、インシデントレスポンスプロバイダからのデータが示すログ保管期間と同じかそれよりも長期間であるが、そうではないログ種別もある。また、これらのログ種別のいくつかでは、企業がそのログへの価値を置かず、ログ保管の改善のためのプロジェクトも無かったことは注記しておく。後段のセクションではこれら 2 つのエントリは違いを明確にするため独立して記載する。

APT 対応のための追加のログ種別についての検討

以下のセクションでは、調査によって明らかになった、前述のログ以外に役に立つ可能性のあるログ種別について述べる。これらのログのいくつかは、その適正な保存コストが組織構造に大きく依存するため、インタビューからは適切な保存期間についての詳細は得られていない。

VPN ログ：APT の目標のひとつがネットワーク内に強固なアクセス基盤を築くことであるため、VPN ログが重要となるケースがある。APT がこの目標を達成する最良の方法はネットワークへの正当なアクセス手段を得て標的企業に対する活動を長期的に維持することである。攻撃者は正当なリモートアクセスと他の認証情報を獲得し、通常監視されていない正当な通信に紛れ込むことで、目的を達成する可能性を高めることができる。このため防御側では多くの場合、VPN ログの取得と定期的なレビューが必要となる。

DHCP ログ：DHCP サーバの機能は IP アドレスをクライアントにリースすることであり、探すものを分かっている場合に有用なデータを提供し、診断ツールとして機能する。DHCP ログは監査ログの機能が使えるよう設計されているため、ログファイルサイズやディスク資源を管理するための追加の監視・管理機能を必要としない。DHCP ログは、ID、日付、時刻、説明、IP アドレス、ホスト名、MAC アドレスを記録する。リースされた IP アドレスがいつ更新されたか、または留置されたか、動的更新が成功したか否か、server authorization イベントがあったか否か、それがどのように進行したかを説明することができる。IP アドレスの追跡は特に DoS 攻撃元の追跡に役に立つ。DHCP ログは不正な侵入がいつどこで行われたかを大まかに特定するのに有用だが、ネットワークに数百台のコンピュータがある場合、その中の 1 台を特定するのは難しいかもしれない。それゆえ DHCP ログの利用は、ログをすべて検索して何かを見つけ出すのではなく、探すものが予めわかっている場合に最適である。

IDS アラートデータ：IDS はネットワークやシステム上での悪意のある活動やポリシー違反を監視し、レポートを生成する。攻撃者が標的ネットワークへの攻撃計画を立てるために試験的な侵入を試みる段階の動きをトレースすることにより、攻撃がおこなわれる前に攻撃元を追跡し、IP ネットワークのパケットログ収集とリアルタイムトラフィック分析を開始するために利用できる。プロトコル分析、コンテンツ検索、コンテンツ照合をおこない、探索や攻撃を検知する。IDS は主に 3 つのモードで動作する。スニファ（パケットを読む）、パケットロガー（パケットのログを取得する）、ネットワーク侵入検知（ネットワークトラフィックを監視し定義されたルールセットに違反しているかどうかを分析する）。しかしながら、完璧ではないし、誤検知や見当違いの警告も多い。IDS の警告は有用なソースだが、別方向から検証されるべきである。

パケットキャプチャ（PCAP）：PCAP は実際の生のトラフィックを収集したものである。PCAP の保存における難しい問題は、それが短期間で膨大な量に膨らむということである。リアルタイム分析やインシデントレスポンスにおいては非常に有用だが、多くの組織ではこれを長期間にわたって収集することはできない。

Email ログ：Email は様々な攻撃者にとって一般的な攻撃ベクターである。フィッシング（足場を確保するための大量の試み）、スピアフィッシング（重要な機能エリアへアクセスするための中規模の試み）、whaling（特定の重要人物を狙ったメール）は多くの組織で経験されている。ログデータと Email のオリジナルを管理することは侵入者の初期の行動を特定するのに使える。また、フィッシングメールの受信を報告する人がごくわずかでもいれば、ログをチェックして他の受信者を見つけ、彼らが悪意のあるコンテンツをダウンロードしていないかどうかを確認することができる。

アンチウィルスログ：いくつかの組織では、彼らが遭遇したのがどんなマルウェアかを特定するためにアンチウィルスログをチェックしている。これはシステム上の他の問題を浮かび上がらせ、組織が侵害される最も一般的な方法についてセキュリティチームが理解するのを助ける。組織内のすべてのシステムが最新の定義ファイルにアップデートしていないこともありうる。もし攻撃のキャンペーンを示す妥当なインディケータがあるなら、どのシステムがその侵入を止めたかという情報を得ることはインシデントレスポンスの観点からは重要なことである。

政府／規制の管理ガイダンス

ここでは米国政府の規制と要件に関する様々な検討について述べる。法律はログの管理を求めるが、取得すべきログの種別やその保存期間については通常は規定しない。ログ管理に関するより一般化されたアプローチと理解したほうがよい（すなわち、規制は特定のログ種別を示さず、むしろ「オンラインでX量、オフラインで Y 量を管理できる能力」のようなメッセージが多い）。ほとんどの場合、必要なログは要求事項を実装する組織と管理対象のデータ種別に依存する。またほとんどの場合、ログは監査や法的対応の目的で必要とされる。いくつかのケースでは前述の主要なログ種別が監査証跡の一部として使われる可能性があるが、それらのログ種別が要件として言及されるケースはない。

さらに、ここで述べる規制における要件はすべて、消費者を保護し企業の不正を明らかにするための監査を可能とするためのものである。組織が規制要件をどのように実装するかによるが、実装されたログ管理は APT 対応に有用なものとなり得る。これらの規制や命令に従うことが求められる組織は、APT や他のサイバー脅威に対応するための追加のログ管理手段を必然的に実装することになる。

政府／規制のガイダンスに関する分析

政府や規制団体からのガイダンスは一般的にとても曖昧であり読み方によって様々な意味に捉えられる。これは規制対象となる側の様々な組織からの抵抗に起因する。一般的には、規制する側は「何を行うか（どのように行うか、ではなく）」を命令する。組織は規制に準拠していることを示すことができるなら、それを達成する方法は様々であってよい。この種の規制のもう一つの主要な関心はデータへのアクセスについてのログであり、APT 対抗機能についてはあまり関心がない。

表 1: 政府規制からの要件、目的、保管期間

規制	ログの目的	アクセスストレージ	アーカイブ
米国連邦政府機関	セッションの再構築	7 日	30 日（注記：いくつかの組織では 5 年間の保管を求められている）
PCI DSS	主に監査目的とカード契約者情報の保護	3 か月	1 年
Sarbanes Oxley	監査の準備のためのユーザ権限とグループ管理にフォーカス	N/A	7 年
HIPAA	E メールと他の記録－特に医療情報に関係するものに適用	7 年	N/A
GLBA	金融機関の活動に関する通信と記録に適用	N/A	6 年
NERC	米国の電力会社に適用されるガイドラインと標準	90 日	3 年
FISMA	監査に必要となる重要情報にフォーカス	N/A	3 年
Basel Ⅲ	国際間の銀行業務における様々な記録が求められる	3 年	7 年

政府／規制のガイダンスの詳細

米国連邦政府機関：国土安全保障省（DHS）による連邦政府機関に対する要求事項に基づき、政府機関とインターネットとの間のセッションを再構築しトレースする能力についていくつかの詳細な要件が規定される。連邦政府機関から発するインターネットトラフィックのセッションデータ（FW、ルータ、サーバ、その他のデバイス）は最低 7 日間、またオフラインで 30 日間の保存が義務付けられる。他の政府機関とインターネットとのゲートウェイの役割を司る機関は、セッションデータをオフラインで 5 年間保存することが義務付けられる。（これは一般的な要求事項ではなく特定のクライテ

リアに大きく依存する。）DHS は管理する必要があるログの種類を細かく指定していないが、詳細は各機関にまかせ、セッションの追跡能力を維持することのみを命令している。注目すべきことに、DHS 自身は Einstein システムで各政府機関の Netflow データを保存しているが、その情報がどれくらいの期間保存されているかは公表されていない。確証はないが、おそらく DHS はこの情報を永久に保存するだろう。

PCI DSS：PCI DSS のログ保管に関する要件はセキュリティ関連のログ種別（プロキシログ、Netflow、パケットキャプチャ）を区別しない。PCI DSS の Requirement 10.7 によれば、企業は監査証跡の履歴を少なくとも 1 年間保存し、そのうち直近 3 か月のデータは即時分析に使える（例えばオンラインアーカイブ、バックアップからレストア可能など）ようにしなければならない。[25] さらに、Requirement 10.6 によれば、これらのセキュリティログは日次で自動的にチェックされなければならない。[26] セキュリティログの種別については区別していないが、クレジットカード情報（PIN 番号、CVC など）については細かく規定している。[27]

NIST SP800-93 より：「PCI DSS はクレジットカード所有者のデータを保管、利用、転送する組織に適用される。PCI DSS の要件のひとつはネットワークリソースとカード所有者データへのすべてのアクセスを追跡できること。」

Sarbanes Oxley 法：SOX 法として知られている。監査の準備のためのユーザ権限とグループ管理によりフォーカスする。年間収益 7500 万ドル以上の公開企業について組織の財務レポートに関する情報の管理と保護を求める。

NIST SP800-93 より：「SOX 法は主に財務と会計業務に適用され、これらの実務をサポートする IT 機能を網羅する。セキュリティ違反や攻撃の兆候を見つけるため定期的にログを精査することや、監査人による将来のレビューのためにログそのものとログをレビューした記録を保管しておくことが、SOX 法への準拠の助けになる。」

HIPAA：The Health Insurance Portability and Accountability Act （HIPAA）は医療記録を許可されない者のアクセスから保護する目的で、医療情報に関する E メールと他の様々な記録に適用され、これらの情報をかなりの期間にわたり管理することを求める。現在これらのデータは 7 年間の保存が義務付けられる。このデータのほとんどは医師と患者の双方がアクセス可能でなければならないが、これを実現するためにオフラインのみで長期間保管されるデータをアクセス可能にする方法は不明確である。データは使用可能でなければならず、追加のアーカイブでの保管が必要となると思われる。

NIST SP800-93 より：「HIPAA は医療情報についてのセキュリティ標準を含む。NIST SP800-66 An Introductory Resource Guide for Implementing the HIPAA Security Rule では HIPAA に関連するログ管理の要件についてリストしている。例えば Section 4.1 では監査ログとアクセスレポートの定期的なレビューの必要性について述べられている。また Section 4.22 では活動を文書化し最低 6 年間の保管が必要と規定している。」

GLBA：The Gramm-Leach-Bliley Act（GLBA）は金融機関における消費者の金融情報の守秘義務についての命令であり、監査人に対し脅威や不慮の事故による情報漏洩に対するコントロールが機能していることを示すための詳細情報の提供が可能であることを求める。

[25] PCI Security Standards Council, “ROC Reporting Instructions for PCI DSS v2.0,” Payment Card Industry (PCI) Data Security Standard, September 2011, https://www.pcisecuritystandards.org/documents/PCI_DSS_2.0_ROC_Reporting_Instructions.pdf, 87
[26] Ibid, 86
[27] Ibid, 40

NIST SP800-93 より：「GLBA は金融機関が顧客の情報を脅威から守ることを要求する。セキュリティ違反の可能性を特定し効果的に解決するためにはログ管理が有用である。」

NERC：The North American Electric Reliability Council（NERC）は電力会社に対し Critical Infrastructure Protection Standards に関連するガイドラインと標準を定める。サイバーセキュリティデータ保管の要件が Critical Infrastructure Protection Standards の中で規定されている。CIP-002-1、section D1.3.2 データ保管の項で「コンプライアンス管理者は監査証跡を 3 暦年間にわたり保管する」と述べられている。CIP-007-1, section B.R6 では「責任を持つ組織は電力会社のセキュリティ境界の中にあるすべてのサイバー資産について技術的に可能である限り自動化ツールまたは組織的なプロセス管理によりサイバーセキュリティに関連するシステムイベントの監視を確実におこなえるようにする」、また「責任を持つ組織は Requirement R6 に規定されるすべてのログを 90 暦年間保存する」と述べられている。サイバーセキュリティに関するどのログを管理すべきかは明確には述べられていない。

FISMA：Federal Information Security Management Act（FISMA）は政府機関に対し情報とシステムの機密性、完全性、可用性について集中管理と報告を義務付ける。この要件はインシデントのデータと統計情報について USCERT への報告を含む。

NIST SP800-93より：「FISMAは各政府機関が組織と資産をサポートする情報システムのセキュリティを提供する組織全体のプログラムを開発し、文書化し、実装することの必要性を強調する。NIST SP800-53 Recommended Security Controls for Federal Information Systems はFISMAの支援のもとに作成された。NIST SP800-53は政府機関に推奨されるセキュリティコントロールの第一のソースである。ログ管理（生成、レビュー、保護、監査証跡の保管を含む）についてのコントロールと監査の失敗時のアクションについて記述される。」さらにNIST 800-61 Computer Security Incident Handling Guide, Section 3.4.3, Evidence Retention には「Section 3.4.2で述べたように、General Records Schedule (GRS) 24はインシデントハンドリングの記録は3年間保存されなければならないと規定する。」と書かれている。

Basel Ⅲ：この国際的な規制基準はバーゼル銀行監督委員会によって作成され、銀行法と規制についての推奨事項を提供する。現在第３版であり、1988年の世界中の銀行による審議会として開始されている。

FFIEC：The Federal Financial Institutions Examination Council's（FFIEC）は連邦政府による金融機関の調査のための統一された原則、基準、報告フォーマットを規定し、連邦準備銀行(FRB)、連邦預金保険会社(FDIC)、全米信用組合管理機構(NCUA)、通貨監督庁(OCC)、消費者金融保護局(CFPB)の理事会の監督の下、統一基準を推進するための推奨事項を決める権限を持つ中間的機関である。[28] 1979年3月10日に設立され、2006年にState Liaison Committeeのアドバイザリの投票メンバーとして州の規制当局者の代表を加えた。[29] FFIEC IT Examination handbookはログ取得と保管について規定するが、細かい要件については規定しない。

より詳細な情報については、**NIST SP800-92** Guide to Computer Security Log Management を参照。

[28] “Home Page,” *Federal Financial Institutions Examinations Council*, February 15, 2013, http://www.ffiec.gov/.
[29] “About FFIEC,” *Federal Financial Institutions Examinations Council*, February 15, 2013, http://www.ffiec.gov/about.htm.

企業におけるログ管理のベストプラクティス

投資対効果の評価にもとづいたデータ保管期間についての産業界ベストプラクティスを決めるにあたり、APT 対応のプラクティスを持ついくつかの企業にインタビューを行った。これらの企業は高度な APT 対応プログラムを持ち、APT による侵害を発見し無力化するため様々なログの相関分析能力を持つ。各組織は主要なログ種別をほとんどすべて管理している。さらにそれ以外のログ、パケットキャプチャ、Email、VPN、アンチウィルスログも管理対象としている。

企業におけるログ管理についての相関分析

以下の図はログ種別毎に、オンラインとオフラインでの保存期間の分布を示す。オフラインの保存で図のスケールを超えて保存される、または永久に保存される場合は「＋」記号で示される。これらの企業は成熟した APT 対応プログラムを備えているため、これらの事例はログ管理のベストプラクティスであり一般企業の平均ではないことは注意されたい。

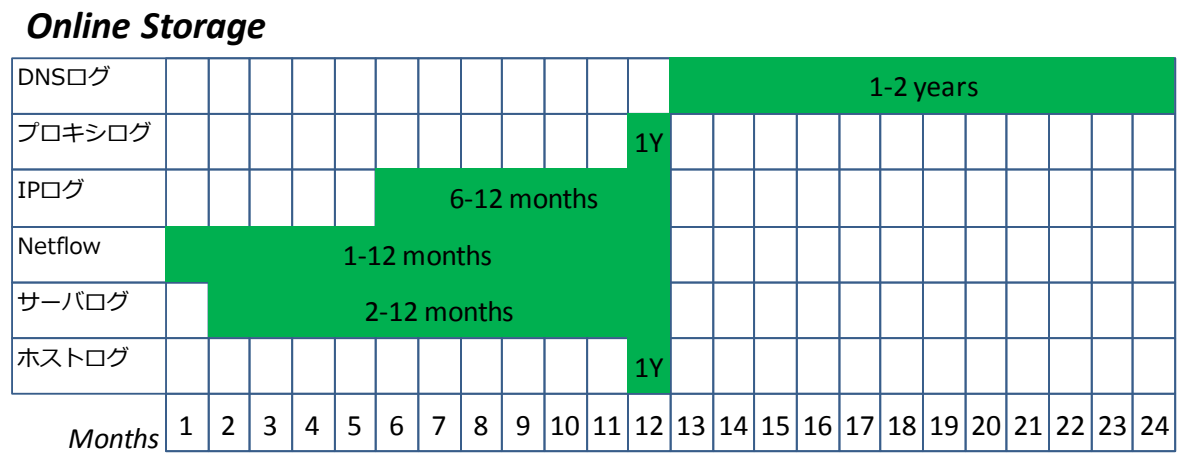


図 2： 企業におけるログ管理（オンライン）

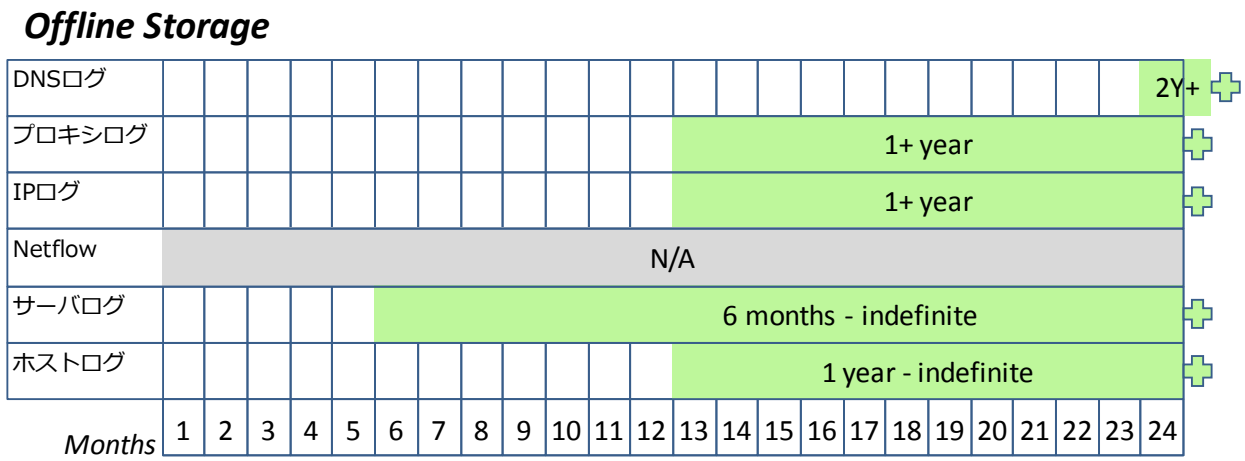


図 3： 企業におけるログ管理（オフライン）

これらの図のスケールは 2 年間となっている。DNS ログの保管は全ての企業にとって最重要とされ、他のログと同等かそれ以上の期間にわたり保存される。個々のログ取得を集中化するか、ログ収集と相関分析を集中化された分析ツールでおこなうか、大量のログを管理するためにどちらかの手法が全ての組織で用いられている。これらのログは相関付けされたものだけではないことに注意すべきであ

る。このセクションの後半で有用な追加のログ種別について論じるが、すべてのケースでそれらのログも相関分析ツールに投入されセキュリティチームに状況認識をもたらすデータを提供する。

企業におけるログ保管の詳細

収集されたログの価値について次の表で示す。ここで提示した価値はインタビュー対象の企業による評価であることに注意されたい。ログ分析をどのようにセットアップするかは、そのログにどれだけの価値を置いているかに影響する。これはログ管理についての考察であり、すべての組織に対するログデータ保管についてのガイダンスを導くものではない。

表 2： 企業のセキュリティチームにおけるログ種別の価値の評価

ログ種別	価値: APT	価値: サイバー犯罪者	価値: ハクティビズム	価値: 日和見的攻撃者
DNS ログ	Very High	High	Medium	Medium
プロキシログ	Very High	Very High	Medium	Medium
IP ログ	Medium	Medium	Medium	Medium
Netflow	High	High	Medium	Medium
サーバログ	Medium	Medium	Medium	Medium
ホストログ	Low	Low	Very Low	Very Low

DNS ログの保管はインタビューしたすべての組織で非常に高いスコアが付けられた。保存期間はオンラインで 1 年から 2 年、オフラインでは無期限まで分布している。ハクティビズムと日和見的攻撃者によるハッキングは、これらの脅威による攻撃ベクターが DNS ヒストリにアーティファクトをそれほど残さないため Medium にランクされている。

プロキシログも非常に高い価値を持つ。プロキシデータはコールバックトラフィックを発したデスクトップ PC を特定する情報を与え、C&C ドメインを特定することもできる。これらのログは DNS ログほど長期間保管されないが、オフラインでは可能な限り長期間保管される。DNS と同様に、ハクティビズムと日和見的攻撃者の脅威に対する価値は Medium とされる。

IP ログのスコアはすべての脅威タイプに対して Medium とされた。IP ログはオンラインで 6～12 か月、オフラインで 1 年～無期限保管される。IP ログは境界情報を提供するのみで、ツールによって相関付けされることで分析結果の妥当性判断に利用されるが、一般にそれ単体で重要なインディケータとなることはない。

Netflow はインタビューしたすべての組織で APT とサイバー犯罪で高いスコアとなった。ハクティビズムと日和見的攻撃者については、それらの脅威は通常ネットワークに深くまで侵入せず DMZ の Web サーバと他の設備にフォーカスするため、Medium とされた。Netflow ログはオンラインで 1～12 か月保管され、長期間保管する組織はなかった。

サーバログはインタビューしたすべての組織で取得され、オンラインで 2～12 か月、1 つの組織では無期限保管されていた。サーバログはインタビューしたすべての組織で、すべての脅威に関して Medium とスコアされた。

ホストログは 1 つの組織で 1 年間取得され無期限保管されていた。1 つの組織ではサイバーセキュリティの目的ではホストログを保管していなかった。しかしながら、ホストログは必要な際にそのホス

ト上で利用できる。これには良い点と悪い点がある。最低限、ログはアクセス可能であるが、しかしながら APT がシステム上に存在する場合ログは侵害・改竄されている可能性がある。

インシデントレスポンスプロバイダによって価値ありとされた追加のログは、VPN ログ、Email ログ、パケットキャプチャ、アンチウィルスログである。これらのログについては次の表で示す。

表 3： 民間セクタのセキュリティチームが指摘した追加のログ種別

ログ種別	オンライン	オフライン	価値
VPN ログ	12 か月	永久保存	Medium
Email ログ	12 か月	永久保存	Very High
パケットキャプチャ	20～90 日	N/A	High
アンチウィルスログ	12 か月	N/A	Medium

VPN ログについては 2 つの組織とも有用とコメントした。1 つの組織では 1 年間取得されテープで無期限保管する。他方の組織は期間については言及しなかった。VPN ログはハクティビズムと日和見的攻撃者に関しては lower とスコアされた。これらの脅威では通常 VPN を使用しないと思われるためである。

Email ログについても双方の組織が有用とコメントした。一方は 1 年間取得しテープで無期限保管する。他方は期間については言及しなかった。Email は非常に一般的に使われる攻撃ベクターであるので、一方の組織は、進行中のインシデントに関係するすべてのフィッシングの試みを発見できることに非常に高い価値を置いている。ハクティビズムと日和見的攻撃者に関しては Email ログの価値は通常低く置かれる。これらの脅威では通常 Email を使用しないと思われるためである。

パケットキャプチャは双方の組織とも取得している。一方の組織は 3 カ月間取得している。他方の組織ではトラフィック量に応じて 20～30 日間の取得能力を持っている。一方の組織でのインタビューによれば、インシデントレスポンス中にパケットキャプチャが使えればそれは最も有用な情報の一つとなる、とのこと。

Antivirus ログは 1 つの組織で取得している。この組織では antivirus ログのレビューの利用を有用なセキュリティプラクティスの一環として位置付けている。どのシステムがウィルスを捕獲し無力化したかを特定し、Email ログと相関付けて侵害されたシステムのリストを生成する。このアプローチはインシデントレスポンスチームの労力を減らし、マルウェアを受け取ったシステムをすべて手作業でチェックする必要がなくなる。

インシデントレスポンスプロバイダの測定値にもとづく理想的なログ管理

データ保管期間の理想値を理解するため、APT への対応と無力化にフォーカスしたインシデントレスポンスサービスプロバイダである Mandiant と CrowdStrike にインタビューした。これらの企業では、データは政府機関や規制団体よりもより細かい粒度で取得され、各ログの統計情報が取得・分析される。

理想的なログ管理についての相関分析

インシデントレスポンスプロバイダに対し、観測した侵入の 80%について適切に対処するための理想的なログ保存期間はどれくらいかを質問した。すべてのケースで、真に理想的なログ保存期間は、どのカテゴリでも「永遠」となる。いくつかのログは長期間保存するには大きすぎるため、これはどの組織においても不可能である。高度な攻撃者は数年にわたり組織のネットワーク内に定着する。最善の状況であっても、セキュリティチームが攻撃者の最初の侵入を明らかにできることはまれである。これらの結果、組織が経験したネットワークへの侵入の大部分のソースを識別できることを十分に期待できるために必要なログ保存期間についての洞察が得られる。

注記：インタビューは収集したデータを集約し全体的な推奨事項にまとめたものである。どの組織も生データを本レポートに含めることを許諾しなかった。

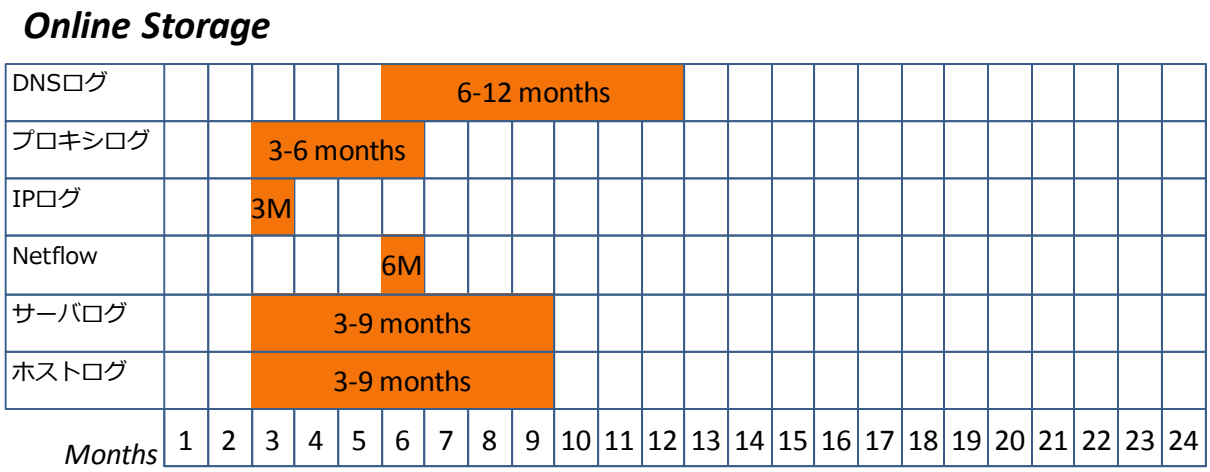


図 4： インシデントレスポンスプロバイダによるオンラインストレージの推奨値

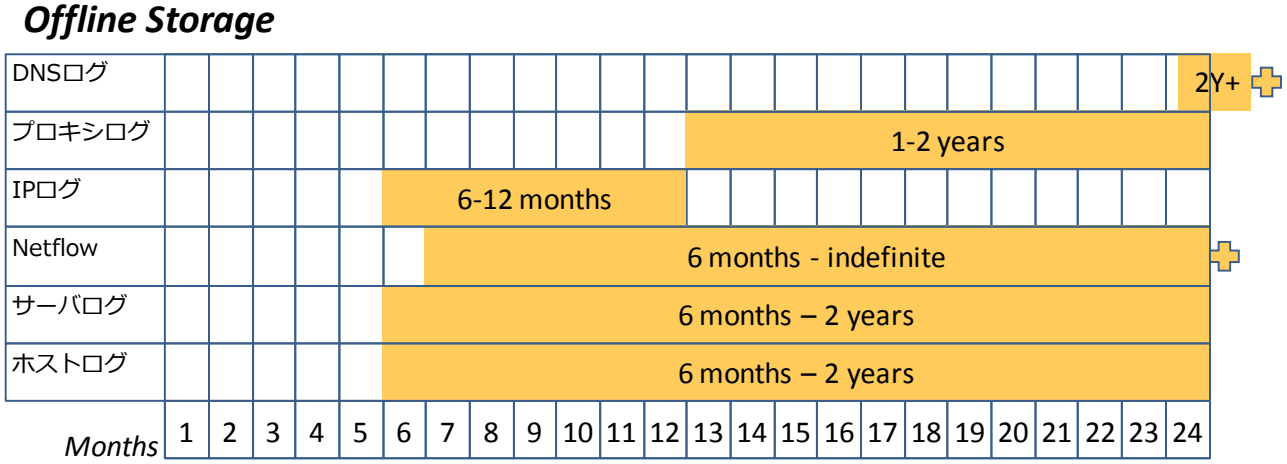


図 5：インシデントレスポンスプロバイダによるオフライン保管に関する推奨値

最初の表は 1 年、2 番目の表は 6 か月～2 年以上のスケールとなっている。興味深いことに、データ種別により推奨値は広くばらついている。注目すべきは、サーバログとホストログの保存能力は、これらのシステムの台数と 1 台あたりが保存するログデータ量（すなわち、ログを全て保存するかまたは重大なアラートだけに絞るか）に大きく依存する。

最も長期間の保存が推奨される 2 つのログは、DNS ログと netflow データである。これは主に、これらのログがとても価値があり、オンライン、オフラインでの保存がそれほど高コストではないことによる。これらの中のとても古いログが、攻撃が開始された時期についての追加的な洞察を与え、APT 活動のタイムラインを推測するのに役立つことがある。

理想的なログ管理の詳細

インシデント対応者にとってログは、攻撃者による過去のイベントを再現することができるため重要である。攻撃者が何をしたか、何の意図でネットワーク全体に広まったのかを理解するために必要となる。ログがインシデント対応よりもリアルタイムのネットワーク防御にとって高い価値を持つこともある。例えばパケットキャプチャは、既に発生したインシデントへの対応よりもむしろ、インシデントが進行中であることを確認するために重要となることがある。次の表は、様々な脅威に対してこれらのログがもつ価値を示す。

注記：次の表はインシデントレスポンスプロバイダの平均的意見のスナップショットを表すが、各インシデントは異なるためある時に価値のある情報が次の時にはそうでないかもしれない。それは真に攻撃ベクターとネットワーク上での攻撃者の活動に依存する。これは 2013 年初期におけるインシデントレスポンスプロバイダの平均的な経験に基づく。

表 4： インシデントレスポンスプロバイダによるログ種別毎の価値評価

ログ種別	価値: APT	価値: サイバー犯罪者	価値: ハクティビズム	価値: 日和見的攻撃者
DNS ログ	Very High	Medium	Medium	Low
プロキシログ	Very High	Medium	Medium	Low
IP ログ	Medium	Medium	Low	Low
Netflow	Medium	Medium	Low	Low
サーバログ	High	Medium	High	Medium
ホストログ	High	Medium	Medium	Medium

DNS ログはインシデント対応者にとって高い価値を持ち、保存も非常に低コストである。しばしば、マルウェアと C&C は攻撃者が登録した URL を用いる。これらのエントリを相関付けして既存の情報や他者によるインテリジェンス情報と比較できることがある。APT は組織的にネットワークへの侵入をおこなうため、この脅威へ対応することは他の脅威への対応よりも一般的に高い価値をもつ。日和見的攻撃者は一般的にフィッシングやマルウェアを攻撃に使わないため、脅威としては低く位置づけられる。

プロキシログは APT 攻撃者に対抗するために非常に大きな価値をもつ。多くの C&C とマルウェアの通信は URL で行われる。DNS ログもこれらの通信を追跡できるが、プロキシログはこれらのアクションを実行するホストを特定できる可能性が高い。ホストログとプロキシログを相関付けすることによりマルウェアやツールの通信先を迅速にレビューすることができる。プロキシログは web コンテンツをキャッシュし DNS レコードが示すよりも多くのホストを示すことができるため重要である。

IP ログはいくつかの理由で少し重要度は落ちる。その理由は、一般的に長期間保存されないということ。さらに、マルウェアと通信チャネルとのビーコンは一般的に IP 上では行われず URL のセットを利用して行われること。IP はセキュリティチームがマルウェアからの DNS クエリを遮断することに成功した場合に代替メカニズムとして利用される。そのため重要度は medium となる。

Netflow の重要度は medium だが、長期間の保存を非常に安価に行える。他の強力なログが生成するようないくつかの重要なコンテキストを欠くが、重要なイベントの時系列のタイムスタンプを提供する。Netflow からの統計情報はマルウェアのビーコンの通信を特定できる可能性がある。

組織が APT やハクティビストの標的となった場合、それらの脅威は情報を探索するためにサーバを狙うため、サーバログが高い価値をもつ。これらのシステムはアクセスされ、ログに攻撃の痕跡を残す。このログを保管する期間は、ネットワーク内で稼働するシステム数に依存する。ログの量はすぐにコントロールできないほどに膨れ上がる。サーバログの管理期間を決定するにはリスク管理の視点が必要となる。このタイプのログは管理のために多大なコストを要する。

ホストログの管理も非常に高コストになる。サーバログとホストログの違いは、サーバよりもホストの方が多くの台数があるということ。組織はある程度の量のログをそのホストシステム自身で保存することがある。この方法は高価なストレージを必要としないが、セキュリティチームがログを集める前に APT によりログを改竄されるリスクがある。

インシデントレスポンスサービスプロバイダにより価値ありとされた他のログは、VPN ログ、DHCP ログ、パケットキャプチャ 、IDS アラートデータである。これらのログの評価について次の表に示す。

表 5：インシデントレスポンスプロバイダによる追加のログ種別の価値評価

ログ種別	オンライン	オフライン	価値
VPN ログ	6～12 か月	2～3 年	High （インシデントに強く依存する）
DHCP ログ	3～6 か月	1 年	High （インシデントに強く依存する）
パケットキャプチャ	1～2 日	90 日	High
IDS アラート	6-12 か月	N/A	Medium

APT は様々なリモートアクセスアカウント（Citrix、VPN 等）を事前に用意し、インシデント対応の完了後も継続的なアクセスを維持することが知られているため、VPN ログは重要である。いくつかのケースでは、リモートアクセス方法の正当性を評価し APT の活動中にどのアカウントが作成・改変されたかを確認するために重要となる。

DHCP ログは、資産管理とインベントリ管理が適切におこなわれていない場合に役に立つ。インシデント対応者は感染ホストを物理的に特定しなければならない。もし DHCP ログがなければ APT がネットワーク内に存在することがわかっても、どのホストが侵害されているのか特定することができない。

パケットキャプチャはセキュリティチームにとって重要なツールとされた。注目すべきことに、インシデント対応者の意見では、パケットキャプチャに対し、何か問題が起きた際にリアルタイムに分析できるための機能を求め、インシデントレスポンスのために用いることをあまり求めない傾向があっ

た。このログは重要であり調査中にその効果を発揮するが、インシデントの早期の段階でより重要度を増す。

IDS アラートは履歴管理の目的で使用される。保管に必要な容量は IDS の設定に依存する。このデバイスは誤検知を避けられず、それゆえ分析時には十分な注意を要する。しかしながら、当初は証拠がないために無視されているイベントが後に重要となり分析が必要になったときに、このデータから侵入の可能性についての追加的な洞察が得られる。

結論と推奨事項

企業や組織にとって効果的なインシデントレスポンスのためのログは、組織がどのようにログを収集するか、組織がどのような脅威に直面しているかによって異なる。本レポートが示すログデータ管理の統計の例は、企業や組織が APT や他の脅威に対抗するための独自の戦略を立てることを支援するためのガイダンスとなる。

以下の表は組織がフォーカスするべき能力についての推奨事項である。いくつかの能力は他とオーバーラップする可能性がある。また、組織が直面する脅威の種類によっては、あるログの取得期間はより短期間で十分かもしれない。これらのログ取得期間はインシデント対応を実施するために利用可能な包括的なデータセットを得るための合理的なゴールを示す。

表 6：ログ保管に関する推奨値

能力	ログ種別	短期	長期
ネットワークへの攻撃を特定する	DNS ログ	6 か月	2 ～ 3 年
	プロキシログ	6 か月	2 ～ 3 年
	IP ログ	3 か月	9 ～ 12 か月
複雑な侵害と履歴データを追跡する	Netflow	2 年	3 年
	DHCP ログ	3 か月	6 か月
	VPN ログ	3 か月	1 年
侵害されたシステムを特定する	アンチウィルスログ	3 か月	1 年
	ホストログ	30 日	6 か月
	サーバログ	30 日	6 か月
	Email ログ	3 か月	1 年
リアルタイム防御を実行する	パケットキャプチャ	7 日	30 日
	IDS アラート	30 日	9 か月

組織においてこれらすべてのログを取得する必要はないが、少なくとも検討は行うべきである。パケットキャプチャなど、いくつかのログは組織にとって取得するコストが高い。さらに、ここにリストされたいくつかのサービスは外部へアウトソースされている可能性もあり、アウトソース先との契約により、ログ取得が困難または不可能となる可能性がある。ここで定義されたクライテリアに見合う能力を備えることが組織にとってのゴールとなる。攻撃に関する完全に包括的な絵を描くためには多くの種別のログが必要となる。さらにデータ収集に加え、これらのログを集約し比較するために、組織は SIEM のような相関分析ツールの導入を検討するべきである。