Vol.2012-DPS-150 No.20
Vol.2012-CSEC-56 No.20
2012/2/29

# 標的型サイバー攻撃と APT に関する考察

二木 真明[†]　佐藤 元彦[††]　山崎 文明[†††]　内田勝也[††††]

明確な目的を持ち、特定の、あるいは極めて狭い範囲に対して行われるサイバー攻撃が増加している。また、こうした攻撃は、極めて高度な技術を持ち豊富な資源を有する攻撃主体によるものも多い。本稿では執拗に行われるこれらのサイバー攻撃とその対策について考察する。

# Consideration about Targeted Cyber Attack And Advanced Persistent Threat

Masaaki Futagi[†]　Motohiko Sato[††]
Fumiaki Yamasaki[†††]　Katsuya　Uchida[††††]

Recently, Confident and highly targeted cyber attacks are evolving. Some of those are performed by entity that has extremely high technologies and available resources. This study is a consideration about those continuous cyber attacks and countermeasures.

## 1. はじめに

昨今、標的型攻撃やAPT①への対策が情報セキュリティ分野の課題になっている。しかし、これらの言葉は使う人により必ずしも同じでないため、混乱も発生している。

本論文では、関連する言葉の定義を改めて行った上で、それらの特徴及びその対策について考察を行う。

[†] SCSK(株)　SCSK Corp.
[††] 伊藤忠テクノソリューションズ(株)　IT OCHU Techno-Solutions Corp.
[†††] ネットワンシステムズ(株)　Net One Systems Co., Ltd
[††††] 横浜市CIO補佐監／情報セキュリティ大学院大学名誉教授 Assistant to CIO,City of Yokohama,Emeritus Proffessor at Institute of Information Security

① Advanced Persistent Threat

### 1.1 標的型サイバー攻撃とは？

サイバー攻撃は、CNSS②の定義では、「サイバー空間を通じて、企業のサイバー空間利用を標的とし、そのためのコンピュータシステムやインフラの機能停止、破壊、悪意による制御、またはデータの完全性の破壊やアクセス制限された情報の窃取などをする攻撃」[10]とされている。

この定義に従えば、コンピュータウイルスやワーム、トロイの木馬等のマルウェアやウェブ改ざん、サービス妨害（DoS攻撃やDDoS攻撃③）、個人情報盗取等の行為も全てサイバー攻撃と言える。更に、サイバー攻撃を行う前段階での必要な情報収集等の活動もサイバー攻撃の企図行為と考えられる。

また、いわゆる「標的型サイバー攻撃」（以下、「標的型攻撃」という）は、その使われ方から、サイバー攻撃を特定の目的に特化し、それに即した形で特定の対象に狙いを定めて行われる行為と定義される。たとえば、2001 年に発生したCodeRedワームの大量感染事件[1]は、無差別的なサイバー攻撃でありながらも一方で、感染した結果として、米国ホワイトハウスWebサイトへのサービス妨害攻撃を引き起こしており、標的型攻撃としての性格も併せ持つと言える。

標的型攻撃は、その手段としてマルウェア（コンピュータウイルス、ワーム、トロイの木馬等）が使われることが多い。このため、マルウェアやそれを含むメールによる攻撃だけが標的型攻撃と言われる場合があるが、本稿では、より広い定義として、特定の目的、特定の対象に狙いを定めたサイバー攻撃とする。

### 1.2 APT(Advanced Persistent Threat)とは？

NIST④がSP-800-39 文書の中で行っている定義[3]では、APTは、

高度（Advanced）で
執拗（Persistent）な（サイバー）攻撃が行なわれる（能力を有する）
脅威（Threat）」＝「攻撃主体」

を意味するとされている。

本定義に基づくと、APT とは、攻撃そのものでなく、高度で執拗な攻撃を行う脅威である。このような性格を有する主体は、豊富な経済的、人的、技術的リソースを活用でき、組織的かつ継続的に攻撃を続行できる能力を有すると推察される。

本稿では、標的型攻撃を仕掛ける主体のうち、高度な手法を用い、目的を達するために執拗なサイバー攻撃を行う主体を APT と定義する。

② The Committee on National Security System
③ Denial of ServiceおよびDistributed Denial of Serviceの略、サービス妨害と分散型サービス妨害の意
④ National Institute of Standards and Technology

Vol.2012-DPS-150 No.20
Vol.2012-CSEC-56 No.20
2012/2/29

The advanced persistent threat:
i. pursues its objectives repeatedly over an extended period of time;
ii. adapts to defenders' efforts to resist it; and
iii. is determined to maintain the level of interaction needed to execute its objectives.

表 1　NIST SP800-39 での APT 定義

## 2. 標的型攻撃の特徴

標的型攻撃のシナリオは様々だが、その性質から考えられる攻撃の形態を考察する。

### 2.1. ソーシャルエンジニアリング

ここでいうソーシャルエンジニアリングとは人間の心理的な弱さを利用し、必要な情報の取得を試みるような手法をいう。この手法は、多くの場合、標的となる攻撃対象に関する情報収集の段階で使用される。標的となる組織の関係者全員が対象になりえ、物理的（人的）接触、電話、FAX、電子メール等様々な手段により情報収集が試みられる。ここで使われる手法は、旧来より使われてきた詐欺的な手口が中心である。また、関係者の弱みを握り脅迫したり、利益誘導を行ったりして協力者にし、必要情報を聞き出すこともある。[7]ソーシャルエンジニアリングそのものは、サイバー攻撃とは言えないが、実際にサイバー攻撃にあたっての情報収集段階では多用されることから本稿でも取り上げる。

### 2.2. マルウェアによる準備

標的型攻撃においては、その攻撃のシナリオをプログラミングした専用のマルウェアが組み合わせで使われることも多い。最近発生した標的型攻撃においては、こうしたマルウェアが攻撃者のプログラミングに基づいて、侵入したネットワーク内を活動し、目標となるサーバを探索したり、システムに関する情報を収集したりしていたことが報告されている。また多くの場合、この様な目的のマルウェアは、OS に標準のコマンドを活用したり、一般的なソフトウェアの機能を活用したりするなどし、市販のウイルス対策ソフトで検知できない。これは、そのマルウェアがその組織のためだけに作られるなど、ウイルス対策ソフトベンダが検体を入手できないことや、標準的なネットワークコマンドを活用する安全なソフトウエアのように見せかけられているため、ウイルス対策ソフトが正常な動作か判断ができないことがある。

また、市販のウイルス対策ソフトを攻撃者が入手して、検知できないことをあらかじめ検証することが可能である。

多くの組織が、ネットワークからのマルウェアの直接的な侵入に対しては、対策を講じているが、上記の理由から標的型攻撃の端緒となるマルウェアの侵入に気づけない可能性がある。

標的にマルウェアを侵入させる主な方法としては以下のようなものが考えられる。

(1) 電子メールに添付して送付し、受信者に実行させる。
(2) 電子メールでURLを送付してマルウェアが置かれたサイトに受信者を誘導しマルウェアをダウンロードさせる⑤
(3) マルウェアが保存された可搬メモリ（USBメモリ等）やUSB接続周辺機器⑥にマルウェアを自動起動する仕組みを組み込み、接続させる。[4]

一旦システム内に侵入したマルウェアは、システムの情報を得るために、まずは感染に成功した PC を足がかりに、管理の甘さなども利用して徐々に感染を広げたり、組織内を移動したりしながら情報を得ていく。

### 2.3. 隠密行動

情報の収集を目的とする標的型攻撃では、可能な限りひっそり情報を収集する。

(1) PC やサーバに感染したマルウェアはリソースを大量に消費せず、正常なプログラムを偽装して内部に留まる
(2) PC 内やネットワーク探索は、キーロギング、パケットキャプチャなど受動的な方法が使われることも多い。また外部との通信にあたっては、巧妙に通信を偽装し、通常の通信と見分けがつかないようにする[9]
(3) 検出を困難にしたり、機能を変更したりするため、マルウェア自身を定期的に更新する。また必要に応じて他のマルウェアを追加ダウンロードする
(4) HDD やネットワークへのアクセスは他のアクセスやトラフィックが多い時を狙い、それにまぎれて行う
(5) 目的達成後、可能な限り痕跡を残さないようにする。マルウェア自体は自己消滅し、HDD 上のログやマルウェア自身のコードの痕跡を消去する。最近のマルウェアでは痕跡が完全に消去される場合も増加しており、事後の解析を困難にしている
(6) 発覚時の対処を行う。いくつかのマルウェア間で相互通信をして異常を検知

⑤ この手法を「ドライブ・バイ・ダウンロード」と呼ぶ。最近では、有名なWebサイトが改ざんを受け、マルウェアのダウンロードに使用される事例が増加している。
⑥ USB接続周辺機器には、サポートソフトウエアなどの自動インストールのため、初期設定時にUSBメモリとして機能するものがあり、マルウェアを媒介することがある。（参考文献[4]参照）

Vol.2012-DPS-150 No.20
Vol.2012-CSEC-56 No.20
2012/2/29

したら一斉に消滅、もしくはその時点で探索を中止し、そこまでの結果を短時間で持ち出すなどの行動を起こす。また、時限式にしておき、潜伏しているスリーパーマルウェアが一定期間経過後に新たな活動を開始する

(7) 得られた情報をもとに、特定の攻撃対象だけを攻撃するよう指令するなど、総当りの攻撃ではなく、システム情報に依拠した攻撃を実施する

### 2.4. 攻撃者の意識から見た特徴

従来型攻撃者と標的型攻撃者の考え方を整理すると以下の様になり、従来型は自分の力を誇示する傾向、標的型攻撃は身元や攻撃自体の発覚を避ける傾向がある⑦。

**表２ 意識から見た従来型攻撃と標的型攻撃の相違の例**

| 従来型攻撃 | 標的型攻撃 |
|---|---|
| 実力を誇示するために、より困難な攻撃対象を狙う傾向がある<br>• 未発見の脆弱性の発見と攻撃コードの作成<br>• 仮想化システムのハイパーバイザーの脆弱性を使った攻撃など<br>• マルウェア大量感染の数を競う<br>• 有名サイトをあからさまに改ざんする | 攻撃者にとってのリスクを最小化し、安全・確実な手段を選ぶ<br>• アカウント盗取して、正当な利用者になりすます<br>• SQL インジェクション等、攻撃が容易な脆弱性利用し、情報盗取やマルウェア組み込みのための表面上は見えないウェブ改ざんを行う<br>• 管理ネットワークに侵入し、管理システムのアカウントを奪取してシステムの制御を奪うことで、セキュリティを無効化したり痕跡の消去を狙ったりする |

この特性は APT であればより強い傾向を示し、攻撃元の機関や国さえも発覚を避ける方策を講じていると考えられる。

## 3. 標的型攻撃からの防御

### 3.1. 基本的な考え方

標的型攻撃で利用される手法の多くが、既に長年使われ、実証されたものが基本になっている。これは、先に述べた攻撃者の特性からも推測できる。従って、防御策のベースラインは、これまでに確立されている情報セキュリティのベストプラクティスの確実な実装にほかならない。しかし、一方で標的型攻撃に対しては既存のベストプラクティス実装の限界も見えている。現在、ベストプラクティスの実装は多くの組織においてベースラインアプローチで行われているため、高リスクの業務を守ろうとすると、比較的リスクの低い業務においては、業務効率が損なわれる危険がある。また、こうした効率低下を抑えようとすると、高リスクの業務においては効果が十分でない可能性が高い。このことは、異なるリスクの業務を扱う組織において、単一のベストプラクティス実装が困難であることを意味する。

従って、最低限、いずれの業務にも必要なレベルのベースライン対策を確実に実装した上で、さらに、そこから高リスクの業務を分離して個別に、そのリスクに応じた対策を上積みしていく、いわゆるリスクベースアプローチが必要になる。とりわけ、APT による攻撃においては、既存のベストプラクティス実装ではなお不十分な場合もあり、標的となる情報資産と業務を識別して、個別に追加対策を実装していくことが必要である。このようなリスクベース対策の未整備が、最近の標的型攻撃事例で指摘される対策の不十分さの一因ではないかと考える。

従って、以後の考察では、APT が行う標的型攻撃の目標となりうるような高リスクの業務への対策実装について考えることとする。

### 3.2. 保護対象の隔離とリスク評価のあり方

高リスクの情報資産と関連する業務に対して必要なレベルの保護策を講じるためには、これらの資産と業務が、個別に他の業務から隔離されていることが必要である。隔離は、物理的な作業場所や情報保管場所、組織構成、人員構成、IT 機器やネットワークなど、その業務に関わるすべてが対象となる。とりわけ、APT を想定した防御においては、これらのすべてについて、厳重に隔離することが求められる。

隔離されるべきレベルは、想定されるリスクによって異なるが、最も厳重な場合、組織とその構成人員やそれらに付随する一般的な業務も含めて完全に分離することも検討されるべきである。こうした検討の前提には、適切なリスク評価のプロセスが必要になる。何をリスクと考えるかという点においては多面的な視点が必要になる。組織自身の目的や存在意義に対してのリスクは、一般企業であれば、そのビジネスそのものを直接的に阻害する可能性である。たとえば、業務の直接的な妨害や、保有している重要な情報資産に対する侵害などが考えられる。一方、APT を想定したリスク分析では、社会的なリスクも考慮が必要である。組織自身の被害は限定的でも、それが侵害されることで、他者に大きな被害をもたらすような可能性である。たとえば、個人情報の漏洩は、漏洩させた組織の存亡にかかわる結果を招くことは

⑦ 例外的に、昨年のソニー系列企業での大量情報漏えいのように、目的がその企業への社会的ダメージを狙ったものの場合は、攻撃側がその事実を公表することもあるが、一般には秘匿する傾向にあると言える。

Vol.2012-DPS-150 No.20
Vol.2012-CSEC-56 No.20
2012/2/29

少ないが、漏洩された個人に生命の危険をもたらす場合もある。重要インフラや国家にとっての機密情報、業務が侵害された場合、社会や国全体に被害が及ぶ可能性もある。たとえば、民間企業に対する APT の攻撃は、後者のリスクをもたらすことのほうが多いと考えられる。

社会的なリスクの大きさの評価は、そのリスクについてのステークホルダー間で合意され、共有される必要があるだろう。たとえば、組織自身へのリスクについては、現場だけではなく経営陣や場合によっては株主などとも共有されるべきである。組織外にあたえるリスクについては、それらの関係先との共有が必要である。そういう意味で、APT に関するリスクは社会的、国家的に共有され、評価されるべきだろう。

また、最近、一般的にリスクを機密性の観点のみから評価する傾向があるが、評価対象によっては、完全性、可用性などの面で大きなリスクが生じるものがある点に留意すべきである。また、業務プロセス自体へのリスクを考えるならば、効率性を低下させたり、成果の品質を低下させたりするようなリスクも考慮されるべきだろう。

### 3.3. 業務プロセスの見直し

高リスクの情報資産を扱う業務については、業務の流れにおいてのリスクを評価しておく必要がある。業務プロセスの中で誤りや悪意が入り込む可能性を洗い出し、必要に応じて業務の流れを変えたり、コントロールを追加したりすることが必要になる。高リスク資産へのセキュリティ対策を十分に強化するためには、こうした業務プロセスの改善が必須となる。これを行わないとセキュリティ対策自身が、業務効率の低下という別のリスクをもたらしかねない。

### 3.4. 多層防御と攻撃シナリオの分析

標的型攻撃に対しては、その特質故に既存のベストプラクティスの予防的効果は限定的である。そのため、予防的な対策に加え、それが機能しなかった際に侵害の事実を発見することや、被害拡大防止や可能な場合の復旧策などをあわせて考えておく必要がある。

また、実際に侵害が発生した場合、それを早期に発見し対処するためには、あらかじめ攻撃シナリオを想定しておく必要がある。こうしたシナリオをできるだけ多く想定し、それが実際に発生した場合に起きであろう事象を時系列に特定し、それらの連鎖から侵害の発生を推定するようなしくみが重要になる。とりわけ APT による攻撃を想定するならば、攻撃側も複数のシナリオを準備している可能性が高い。一度防御に成功しても、次には違うシナリオで攻撃される可能性がきわめて高いので常に防御側もシナリオの見直しを行い、対策をレベルアップしていくことが重要である。

## 4. 対策モデルの考察

いくつかの切り口で、標的型攻撃に対する予防、発見、対応について具体的に考察する。前提として、APT の標的にされるような極めて高いレベルの保護を必要とするような業務を行う環境を想定する。

### 4.1. 物理的、組織的、人的な隔離

保護対象はコンピュータ上のデータだけでなく、紙やオフライン媒体、作業者の知識など様々な情報が対象になる。例えば、デジタルデータ以外の情報の紛失、盗難や作業中の会話などによる情報の漏洩を防ぐには、作業区画を分離し、入退室を制限するなどの管理が必要になる。高度な保護が必要な業務従事者は、専任とし、組織的に分離することが望ましい。要員のモティベーション低下にも常に注意を払う必要がある。高いレベルの保護が必要な情報を扱う業務では、メンタル面も含め、より緻密なマネジメントが必要で、それがないと、システム上の対策も無意味になる可能性がある。

また物理的に保護された区画の入退室管理に加え、物品や情報の移動も常にチェックされるべきである。

### 4.2. ネットワークの隔離

高リスクの業務を行うコンピュータ等を接続するネットワークは、他の一般のネットワークから物理的、あるいは論理的な分離をすることが望ましい。ネットワーク機器の安全性も考慮するのであれば、これらも含めた物理的分離が必要で、原則として、保護されたネットワーク以外には接続できなくし、全ての作業をその中で行う。

ただし、現在の IT 利用環境では、完全な隔離が不可能、あるいは作業効率を低下させる可能性がある。そのため作業効率の大幅な低下を避けるには、最低限の接続を残さざるを得ないこともある。但し、そのように物理的に接続されている場合でも、接続点の機器制御は保護されたネットワーク側からのみ可能とし、通信も保護されたネットワークへ外部からのアクセスを完全に封鎖し、例外を認めないことで対応できる。全ての作業はネットワークの内側からのみ可能にする。一般ネットワ

Vol.2012-DPS-150 No.20
Vol.2012-CSEC-56 No.20
2012/2/29

ークへ保護ネットワーク側から接続できる場合でもインターネットへのルーティングは行わず、デフォルトルーティングはオフにし、明示的に指定されたルートしか通信できないようにする。保護側から一般ネットワーク上の他ユーザが利用できる機器（例：ファイルサーバ等）への直接接続は、マルウェアの伝播等を防ぐため、禁止する。

一般事務作業等を考慮すると、保護された業務環境だけでなく、一般環境へのアクセスが必要になる。2 台の PC で事務用と作業用に分けることがあるが、コスト面のみならず、保護区画内に一般のネットワークが引かれていると事故の原因になる可能性がある。事務区画を作業区画外に置くことも効率性やスペース確保（費用）面の問題もある。

一つの解決策は、一般ネットワーク側に専用シンクライアントサーバ⑧を配置し、保護区画から、このサービスのみアクセスを認めることである。PC一台で保護対象業務と一般業務の両方を実行できる。シンクライアントサーバが一般ネットワーク側にあれば、ここからインターネットアクセスを許可しても、リスクはかなり低減できる。万一マルウェア感染などが発生してもそれは一般ネットワーク側に留まる。勿論、このサーバとシンクライアント間のファイル転送やリソース共有は禁止し、マルウェア感染伝播の防止と、情報持出防止の観点から必要になる。一方、保護区画内のシンクライアントサーバに対して区画外からアクセスさせることは、外部からの侵入口を作ることになるため好ましくない。

ネットワークを分離しても、例えば、USB メモリ等の媒体経由で、マルウェアが侵入する可能性は無視できない。悪意ある内部者や脅迫･利益誘導等を受けた内部者がマルウェアを持ち込んだり、情報を持出したりする可能性もある。これらへの対策はネットワークレベルのみでは困難だが、ネットワーク側で取り得る対策もある。

例えば、マルウェアの多くはインターネットとの通信や内部ネットワークの探索を行う。先に書いた前提で保護されたネットワークでは、必要外の通信はすべてデフォルトルートに集まる。そこでダミーのデフォルトルートを設定し、流れてくる通信を監視すれば、比較的効率良くマルウェアの通信を発見できる。また、内部ネットワークでは、クライアント相互間の通信を禁止する。例えば、ポート毎やユーザ認証で PC 毎に異なる VLAN を割り当て、サーバ等共用リソースがある VLAN との相互通信のみを認める。これにより、マルウェア感染が発生した場合、ネットワークスイッチ側で隔離し易くなる。ネットワークが切れると活動を停止するマルウェアでは、この方法でネットワークコネクタを抜かずに接続を切り替えてトラフィックを監視し続けられる。また、エンドポイントの検疫システム等との整合性もよくなる。

無線 LAN 等の無線接続は原則として使用しない。どうしても使用する場合は、保護区域の電磁波漏えい対策を講じる。保護区域内に不正なモニタリング機器の持ち込みを想定し、暗号化や認証も十分に強固にし、許可端末以外の接続はできないようにすべきである。

### 4.3. エンドポイントの防御（作業用 PC など）

Windows PC にはウイルス対策を含むセキュリティソフトを導入し、集中管理する必要がある。パターンファイルの更新等は管理サーバ経由で行い、定期的にフルスキャンを実施する。これはリアルタイムスキャンだけで発見できないマルウェアを防ぐためである。感染当初は検知ができなくても、後から検知できるようになる可能性もあるため、こうしたセキュリティソフトウエアは必ず導入し、機能を活用する。

Windows PC は、Active Directory（以下 AD という）を使用して集中管理する。利用者のシステム権限は限定し、利用者独自のソフトウエアはインストールさせず、管理者のみ、確認済みソフトウエアをインストールできるようにする。また、USB メモリ等の機器の利用を制限する。外部記憶装置を使用する場合、接続時の自動実行を禁止すれば、マルウェア感染のリスクを減らせる。また、AD で既定のプログラムフォルダ以外からのプログラム実行を禁止すれば、外部メディアや既定のプログラムフォルダ以外に感染したマルウェアの実行を防止できる。セキュリティ更新プログラムも AD サーバ経由で一括適用する。放置された脆弱性はマルウェアに悪用される可能性があり、標的型攻撃では、新しい脆弱性が利用される可能性も高く、セキュリティ更新はできるだけ早く行う必要がある。

Windows 以外の PC でも、可能なものにはマルウェア対策を行う。集中管理ツール等がある場合、それで全体を管理する。Linux 等の OS の PC でも利用サービスのセキュリティ更新は可能な限り早急に適用する。

OS組込みのファイアウォール機能や不正操作防止機能も有効にし、必要に応じて例外設定を行うホワイトリスト方式⑨の運用を行うとよい。

⑧ 端末（クライアント）側では画面表示のみを行い、処理はすべてサーバ側で行うような形態のサービス。情報を端末側に保存する必要がないため、近年、情報保護目的で多用されている。ここでは逆に、外部からのマルウェア侵入を、このサーバまでで食い止めるための方策として利用することを想定している。

⑨ たとえば、アクセスを原則禁止とし、必要なアクセスのみを明示的に許可する方式。逆に原則許可として不都合な通信のみを拒否する方式をブラックリスト方式と言う。

Vol.2012-DPS-150 No.20
Vol.2012-CSEC-56 No.20
2012/2/29

保護区域外から保護区域内、又は逆方向へのPCやストレージ機器の移動は禁止し、移動の場合、HDDの完全消去⑩とOSのクリーンインストールを行い、マルウェア等の持込や情報流出を防ぐ。モバイル機器は保護区域内のネットワーク接続を禁止する。高リスクの情報／システムを扱う業務は在宅勤務や外出先からの作業を行わない。ノートPC等も情報持ち出しを容易にする可能性があるため、保護されたネットワークへの接続は禁止する。

### 4.4. エンドポイントの防御（サーバ）

サーバも、ウイルス対策を含むセキュリティソフトを導入するが、クライアントに導入されているセキュリティソフトと異なるベンダの製品を選択する。パターン更新タイミングや検出ロジックが異なるため、補完効果を期待できる。管理は多少煩雑だが、対象範囲を絞ることで運用負荷を抑えることもできる。必要なアクセスログ等が取得できる OS やプラットホームを選択し、OS の標準ログ取得機能が改ざんされる可能性も考慮し、市販のログ取得ソフト等が使えれば、それを利用する。

サーバ上で起動するサービスは必要最低限にする。また、各サービスは認証を行い、どのユーザのアクセスかを明確にする。利用者には、業務上必要な最小限のアクセス権限のみを与え、アクセスが不要なクライアントからのアクセスは可能な限り禁止する。

データベースサーバ等、アプリケーションからのみアクセスされるようなサーバは、サーバ専用ネットワークに分離し、アプリケーションサーバからしか、アクセス出来ないようにする。

OS やアプリケーションの脆弱性も、緊急度の高いものは、可能な限り早く修正プログラムを適用する。サーバの更新適用は可用性を損なう恐れがあり敬遠されがちだが、搭載アプリケーションやシステム構成を吟味することで、リスクを軽減できる可能性もある。OS ベンダが公開している互換性に関する情報も参考にできる。PC 同様、集中管理できる仕組みがあれば利用する。Windows サーバでは、PC と併せて AD で管理する。

最も注意が必要なサーバは、ADにおけるドメインコントローラのような集中管理サーバである。集中管理は全体のセキュリティレベルを均一化できるが、一方で管理サーバが侵害を受けた場合には致命的である。最近の事例では、マルウェアがPCに感染した後で、ドメインコントローラを探索し侵入するケースが増加している。[8]

⑩ ディレクトリ上の論理的削除ではなく、メディア上の痕跡も含めて完全に消去することを言う。

### 4.5. モニタリング（監視）とログ管理

監視はネットワークや機器に関する監視は、必要に応じてリアルタイムに、または定期的に行う。

リアルタイム監視は主にネットワーク上の通信とPCやサーバの異常動作の監視を行う。保護されたネットワーク上の通信は、ネットワークスイッチのミラーポート⑪等を使用し常時監視する。対象となる通信は一定期間全て保存し、解析できるようにする。また、監視機器のチェック機能（IDS⑫機能等）を使用し、マルウェア等に起因する通信を検知する。ただ、一般に提供されている検知機能の標的型攻撃への効果は限定的であり、最終的には、専門技術者の判断になるだろう。なお、監視部分は専門業者に委託可能だが、日常行われている作業に伴う通信の洗出しや真に発見したい挙動を見つける方法は、委託先と委託元が共同で考え、その後も継続的なコミュニケーションを通じて改善していくべきである。このため、委託元にも、専門技術者と会話できるだけの知識を持ち、自社の業務やシステムに通じた担当者が必要になる。こうした担当者の育成は、直近の最重要課題の一つである。

もし、区画外への通信を許可している場合、接続点にファイアウォールを設置し、ログを取得・監視が必要になる。ファイアウォールは必要最小限の外向き通信のみを許可する。許可されなかった通信にマルウェア等によるものが含まれている可能性があり、通信拒否ログの監視は重要になる。また、デフォルトルートへの通信もダミー機器に流して、全て監視、保存し、⑬その中にマルウェアやなんらかの不正アクセスに起因する通信が含まれないかを常にチェックする。

PC やサーバで、セキュリティソフトに起因するアラートは、常時監視する。 AD の認証ログも取得し、認証失敗の頻発やアカウントロック等のイベントはリアルタイムで検知する。PC やサーバの起動、再起動、シャットダウン等の記録も有用で、サーバではリアルタイム監視の対象とする。なお、作業用 PC もマルウェア感染などにより再起動する可能性があるため、イベントログなどを定期的に検査する。ファイルサーバは共有ファイルのアクセスログを取得し、重要ファイル（フォルダ）へのアクセスはリアルタイムに検知出来るようにする。これらの監視はイベントログを中心に監視するが、必要があれば市販の監視エージェントプログラムの導入も考慮する。重要情報を扱う Web サーバやアプリケーションへのアクセスログも取得する。各サーバは管理者アカウントでの操作の監査ログを必ず取得する。ログは全て、

⑪ トラフィック監視用に設定されたポート
⑫ Intrusion Detection Systemの略
⑬ 明示的に指定された以外のネットワーク経路への通信はデフォルトルートに流れるため不審な通信を見つけやすい

Vol.2012-DPS-150 No.20
Vol.2012-CSEC-56 No.20
2012/2/29

いつ、誰が（どの機器が)、何を、どうしたかを分かるようにする。各利用者を識別できるように共用アカウントや共用 PC は廃止する。

アラートやログのリアルタイム監視は、対象が多岐にわたり、形式も異なるため、これらを共通化して扱える統合監視システム（SIEM⑭）の導入や監視事業者のサービスを利用して効率化する。SIEMの利用により、想定した攻撃シナリオに沿って時系列にイベントをとらえた形での攻撃判定をある程度自動化できる。[9]

リアルタイム監視対象以外のログも、認証系ログ、特権操作関連ログを中心に定期的にチェックする。これも、SIEM 等の検索機能を利用したり、簡単なフィルタプログラムを書いたりして自動化･効率化する。

ログは可能な限り長期間オンライン保存し、インシデント対応時の原因調査時間を短縮する。ログ保存用には比較的安価なHDDストレージと定期バックアップを併用することで、コストを押さえ要領を確保できる。定期的にバックアップを行い、必要に応じて複数世代のバックアップを保持しておく。一旦バックアップしたデータも 1 年半～2 年程度、オンラインで残すことで、問題発生時の検査の迅速性とログ消去、改ざんなどが発生した際の保全の両立ができる。仮想化されたシステムの場合は、仮想マシンイメージのスナップショット⑮を定期的に取得しておくといい。ネットワークデータのキャプチャは、モニタリング範囲により、膨大なデータ量になり、保存期間はストレージコストとのバランスになるが、キャプチャデータはインシデント対応に大きな役割を果たす。キャプチャ装置は様々なオプションがあり、特定通信をフィルタしたり、パケットの一部のみ保存したりすることも可能で、これらを適宜利用し、容量を減らしつつ、可能な限り長期間保持する。標的型攻撃は攻撃開始から長期間発見できないこともあり、長期間保持のログは極めて重要になる。

ログの保存は専用サーバを用意し、ログ取得対象システムに権限を持つ利用者以外の者をログサーバの管理者にし、悪意のログ改ざんを防ぐと同時に相互牽制を行う。

### 4.6. インシデントの発見と対応

ここでいう「インシデント」は、監視での異常検知から実際のセキュリティ事故、事件までを含む。

監視からインシデンを効率よく発見するには、事前にシナリオを想定し、そのシナリオに沿って発生する一連のイベントを推定する。単一のアラームやイベントから、標的型攻撃が発見できることは稀で、一見正常なイベントも一定条件下で発生した場合、異常と考えなければならないこともある。例えば、正当な利用者のファイルアクセスも平日勤務時間のアクセスと深夜･休日のアクセスでは注目度が違う。そのアクセス後、アクセス元 PC からデフォルトルート宛通信が発生していたら更に注目しなければならない。事前にこの様な攻撃手法に通じた外部の専門家を交え、シナリオの検討を行い、それらのシナリオに沿ったイベントを時系列に並べる。実際に、イベントがこの時系列に沿って発生すれば、インシデント発生の可能性は大きい。SIEM を利用し、時系列検知を自動化することもできるが、シナリオでのイベントは、機械的に検知できるものばかりではない。不審な電話やメールの増加もインシデント発生を推測する要因になる。疑わしい情報を人的なネットワークで収集する仕組みの構築も必要である。

実際、インシデントの疑いが強い場合や確実になった場合、まず拡大防止策を講じる。しばらく泳がせて挙動を確認する方法もあるが、泳がせた結果が重大な損失にならない対策を最初に講じておく。それが攻撃であることが強く示唆される場合、攻撃の目的や攻撃者の意図を推定することは、その後の対応にとって重要である。特に APT による攻撃が疑われる場合、同時に複数の攻撃が進行している可能性や、引き続き別の攻撃が行われる可能性が高いので、それらも想定した対応が必要になる。

マルウェア感染が疑われる場合、PC がポート毎に VLAN 接続であれば、VLAN 接続を切り替え、隔離する方法がある。ネットワークコネクタを抜くと、マルウェアは活動を停止し消滅する可能性がある。ネットワーク機器の一連の設定を簡単に変更できるようなスクリプトを用意するといいだろう。

実際の対応は一意ではないが、インシデント発見のシナリオ作りと発見された場合の対応手順も作ると対応を効率化できる。シナリオ作りの利点は初動をすばやく行える点で、特に、監視とインシデント対応の多くを外部に委託する場合、初動を外部に頼ると手遅れになることが多い。あらかじめ決めたシナリオに沿って、初動を委託元で出来れば、初動遅れのリスクを低くでき、手順が用意されていることで作業ミスも低減できる。

APT による攻撃では攻撃者は対策の裏をかいてくる可能性も高いが、想定されたインシデント対応の負荷は大幅に低減でき、そのリソースを想定外の警戒にあてることができる。

⑭ Security Information and Event Management system : SIM とも呼ばれ、異なるベンダやプラットホームの機器から発生するアラームやログを一括管理し、リアルタイム分析を行うシステムの総称

⑮ 仮想化されたシステムにおいて、動作中の仮想マシンのある時点での状態をすべて記録、保存するようなバックアップ方式を言う。

Vol.2012-DPS-150 No.20
Vol.2012-CSEC-56 No.20
2012/2/29

インシデント対応の体制は重要である。インシデント対応に多くの人員や組織がかかわるため、コミュニケーションや役割分担が対応の成否に影響する。シナリオ作りで、判断と実行主体、それぞれの責任、権限を明確にした対応体制を考えておく。対応のどの段階でも想定外の事態が発生する。その場合、誰が判断するかを明確にする。対応が業務に大きな影響を与えることもあり、誰がその対応を承認するか（できるのか）は重要だが、これはビジネス上の判断であり、経営層や影響を受けるライントップの関与が必要になる。あらかじめ想定されるシナリオや想定外が発生することを十分に説明し、理解を得る必要がある。特に監視や対応の多くを外部委託する場合、対応能力の高い専門業者が選定されていても、ビジネス上の判断が正しくタイムリーにできないと対応が遅れてしまう可能性があることに留意する必要がある。

## 5. まとめと今後の課題

標的型攻撃への対応は簡単ではなく、本稿の記述は一般論を述べるにとどまる。とりわけ APT のような複合的な脅威は、IT 専門家、セキュリティ専門家、ビジネスマネジメントが一致協力して対抗する必要がある。 社内、組織内の連携だけでなく、業界や業界を超えての情報共有や協力、司法、捜査機関の関与も必要になる。

現在、APTによる標的型攻撃は国家の安全にかかわる情報資産や業務にも向けられている。⑯防衛には官民や業種、管轄の枠を超えた連携が必要であろう。こうしたAPTからの攻撃は、一民間企業や組織が負担できるコストで対抗可能なものではない。官民を問わず、すべてのステークホルダーが応分の負担をし、対策に必要なリソースを確保することが重要である。

対応には人材面の不安もある。セキュリティ人材、特に高度な攻撃に対抗できる人材は多くない。IT 技術者全般のセキュリティに関する平均的な知識レベルが低いため、比較的低いリスクのセキュリティ維持に貴重な専門家が携わらざるを得ない現実もある。この問題を解消するためには、セキュリティ人材育成を２つのレベルで考える必要がある。一つは、最新の脅威に対抗できる高度な知識と経験を持った人材。もう一つは、最低限のベストプラクティスを実装できる IT 技術者である。後者は、「セキュリティ人材」でなく、「IT 人材」の基礎的な能力と言える。実際、IT 人材が基礎的な必須科目として、基本的なセキュリティ実装を学ぶことができれば、セキュリティレベルは大幅に向上し、セキュリティ専門家は真に彼らを必要とする業務に専念できる。IT 人材育成は民間の努力だけではなく、政策的な後押しも必要であろう。

標的型攻撃について考察する中で、このような攻撃が、サイバー空間上での出来事であるにもかかわらず、現実世界と強いつながりを持っていることがわかる。実際、我々は IT 側からの視点でこれらを考えるが、攻撃者ははたしてそうだろうか。本来、攻撃者は実世界での目的、意図を持って、その手段として IT を活用しているだけではないのか。それは、我々が実世界での目的を IT で効率よく達成するのとなんら変わらない。そう考えると、これはもはや IT だけの問題ではないだろう。今後、IT 以外の様々な視点から、こうしたサイバー攻撃の考察が行われていくことを期待したい。

⑯ 2011 年に発生した米国ロッキード・マーティン社への侵入事件が象徴的。わが国でも、三菱重工業をはじめとする防衛産業や、衆参両院、複数の省庁などがマルウェアによる攻撃を受けている。

## 参考文献

[1] Gregor Freun d: Beware o f the new breed of hac kers, ZDNet( 2003) http://m.zdnet.com.au/beware-of-the-new-breed-of-hackers-120274471.htm
[2] Joseph Menn, 福森大樹監修：サイバークライム，講談社（2011）
[3] Special Publication 800-39: Managing Information Security Risk, NIST(2011)
[4] (株)バッファロー： ポータブル Wi-Fi ルーター「DWR-PG」一部製品にウイルスが混入 http://buffalo.jp/support_s/dwr-pg/
[5] ナイトミア著 松藤留美子他訳：シークレット・オブ・スーパーハッカー，日本能率協会マネジメントセンター ( 1995)
[6] Knightmare: Secrets of a Super Hacker, Loompanics Unlimited (1994)
[7] ケビン・ミトニック他著、欺術、岩谷宏訳：欺術，ソフトバンククリエイティブ (20 03)
[8] ［特集］侵入されても漏らさない 日経コミュニケーション 201 1 年 12 月号
[9] 「不正プログラム対策と侵入検知」渡辺、二木 Internet Week 2005 チュートリアル T13 資料： http://www.nic.ad.jp/ja/materials/iw/2005/proceedings/
[10] National In formation Assurance (IA) Glossary, CNSS Instruction No. 4009 26 Apr 2010