標的型攻撃の脅威と対策についての考察

A Study on the Threat of Targeted Attacks and Countermeasures

助川賢二，大冨哲也，佐野　至

要　約　2005 年頃から政府や一部の大手企業を対象に行われていた標的型攻撃が，個人情報の漏えいにより注目されることとなった．これに合わせるように企業規模や業種を問わずに攻撃を受けることが目立つようになってきている．その一方で，標的型攻撃対策ソリューションは費用対効果がわかりにくく，一般企業ではソリューションによる対策を実施しにくい状況である．

本稿では，標的型攻撃がどのようなものかを改めて示すとともに，ネットワークの観点およびサーバーと端末の観点で，標的型攻撃からシステムを防護することができる設計・設定を紹介する．

Abstract　Targeted attacks that have been made since 2005 to target the government and some of the leading companies, was noted by the leakage of personal information. At the same time, it has become prominent that attacks being made regardless of the company size and category of industry. On the other hand, many of the targeted attacks countermeasure solution is expensive, considering the cost-effectiveness, it is difficult for general companies to implement countermeasures by Solution.

In this document, by showing the method of targeted attacks, the design of Network and the settings of Client / Server are introduced to protect the system from the targeted attacks.

1. はじめに

標的型攻撃は 2005 年ごろから発生しており，政府系機関や大手企業などが攻撃を受けていたが，広く知られるものではなかった．これは，過去にあった標的型攻撃による被害が大規模な個人情報を含むものではなかったことにより，メディアで大きく報道しなかったことが要因である．しかし，2015 年 5 月に日本年金機構への標的型攻撃による約 101 万件の大規模な個人情報漏えいが発生し，メディアがこの事件を大きく報道したことにより，状況が一変し，国内で標的型攻撃に対する関心が急激に高まった．この事件により，標的型攻撃がどこかで起きている脅威から身近で発生しうる脅威に変わったのである．

企業の規模や業種に関係なく標的型攻撃を受ける可能性があり，すべての企業，団体でできる限り早く標的型攻撃対策を実施する必要がある．一方で，様々な標的型攻撃対策ソリューションが存在するが，高額な上に効果もわかりにくいものが多く，一般企業が標的型攻撃対策をすぐに実施できる状況は整っていないと考えられる．本稿では，2 章で標的型攻撃について説明し，3 章では，ネットワーク，サーバー/端末，その他の防護領域で，システム構成やセキュリティー設定を見直すことによって，標的型攻撃対策の一助となる施策を紹介する．

2. 標的型攻撃とは

標的型攻撃の被害が拡大した社会的背景には大きく以下二つの要因が考えられる．

1） インターネットの利用を前提としたライフスタイルの変化に伴う情報収集・発信・保管方法の変化

2） 個人情報や企業情報の電子化が進むとともに，ビッグデータ活用で情報が連結されることによる，情報が持つ価値の上昇

本章では，標的型攻撃について説明する．

2.1 ウイルスから標的型攻撃への変遷

1990年代，日本ではプロバイダーの設立やWindows95の発売などにより，インターネットおよびインターネットメールが普及した．これに伴い，メールを媒体とするウイルスが登場すると，その感染力が飛躍的に増大した．その後2000年頃になると，Windowsのセキュリティーホールを利用するウイルスが出現し，大きな話題となった．この時代までのウイルスは，「作成者の技術力の高さのアピールと自己満足」の意味合いが強く，不特定多数をターゲットに派手に拡散し，注目を浴びることで作成者の目的を達成していた．

2003年にボットウイルス[*1]が出現し，2004年にボットネットが日本で話題になるころからウイルスの目的が「作成者の自己満足」から「悪意ある攻撃者の攻撃」に変化している．また，ブラックマーケットではボットウイルスで構成されたボットネットが売買され，「経済活動」のひとつとして成り立っているとも言われる．

ボットネットによって「経済活動」が成り立つ状況になったことにより，目的が「自己満足」時代の感染影響がわかりやすいウイルスから，感染がより判別しにくいマルウエア[*2]へと変遷してきた．これに加え，不特定多数をターゲットにした攻撃から特定の企業や個人にターゲットを限定した攻撃に変化した．これが“標的型”と呼ばれる攻撃である．

このような経緯をたどって出現した標的型攻撃は，継続的かつカスタマイズされた複数の攻撃手法を巧妙に用いることで，既存のセキュリティー製品による検知や防御をすり抜けようとしている．また，目的を達成した場合，手間や時間をかけても十分にコストが見合うと考えられ，組織的に攻撃を仕掛けているケースが多いと言われている．

本節で述べた年代に沿った攻撃手法の変化を表1にまとめた．

表1 IT技術の変遷と攻撃手法の変化

	1980年代	1990年代	2000年頃	2005年頃	2010年頃	2015年現在
IT技術の変遷	企業のPC利用加速	インターネットの普及・一般化	SNSの出現・普及	通信用インフラの整備	スマートデバイスの普及	ウェアラブルデバイスの登場
IT利用目的	企業でのデータ管理・基幹システムの動作	PCが一般家庭に普及し、個人利用が加速	個人ブログ/SNSの流行	オンラインゲーム/サービスの普及	クラウドサービスの拡大	PCからスマートデバイスへ利用シーンの移り変わり
攻撃者・ウイルス制作者の主な目的	愉快犯(技術力の誇示)		データ破壊/改ざんによる業務妨害	DoS攻撃のための地盤作り(ボットネットの拡張)	個人/企業情報の取得・売却による金銭目的	
攻撃手法の変化	CD/フロッピー等のメディアからコピー	メール利用による拡散型	Webからの感染	USBデバイスの自動実行機能を利用した感染	SNSを利用したやりとり型攻撃の増加 例：企業の役員・人事部宛に知り合い/一般人を装いパスワード保護されたウイルス付きファイルを添付して内部にウイルスを潜入させる。	
不正攻撃・プログラムの特徴	自分の技術力誇示のため、影響がわかりやすくなっている。			発見されない事が重要視され始めたので、利用者に気付かせない様に活動する。		

2.2　攻撃シナリオ

情報処理推進機構（以下，IPA）の「『高度標的型攻撃』対策に向けたシステム設計ガイド」では，以下 1 ～ 4 の手順が高度標的型攻撃の基本パターンであると記載している．図 1 に示すとともに，本節の各項で説明する．

1.　初期潜入：攻撃対象（標的）に潜入する．
2.　基盤構築：端末にリモートから制御可能なマルウエアを感染させ，バックドア[*3]（コネクトバック通信[*4]）を仕掛ける．
3.　内部侵入・調査：内部システムの情報を収集し，侵入範囲を拡大していく．
4.　目的遂行：金銭的に価値のある“情報”を収集し外部に送出する，データファイルの破壊や暗号化を実行する，など．

攻撃者は，攻撃していることに気づかれないよう，既存のウイルス対策ソフトや侵入検知システム（IDS)/侵入防御システム（IPS）といった脆弱性対策機器に検知されないことを事前に確認したマルウエアを用いている．

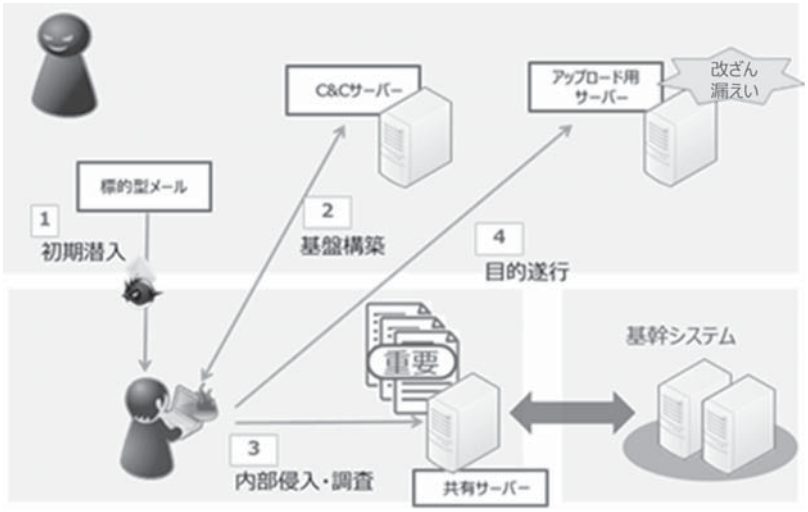

図 1　標準型攻撃の基本パターン

2.2.1　初期潜入

この段階では，公開 Web サーバーの改ざんによる攻撃，可搬メディアを用いた攻撃等，さまざまな手法で侵入を試みる．その中でも，メールによる攻撃は特に多く，攻撃対象内の複数ユーザーに対してメールを送付することにより，潜入を試みる．送付するメールには，「ユーザー操作の陰でマルウエアをダウンロードする URL」を本文に記載する，または，「ユーザー操作の陰でマルウエアをダウンロードする不正なファイル」を添付する，といった手口でユーザーが C&C サーバー[*5] に接続するよう誘導する．送付した複数ユーザーの中で一人でも開封すれば，この攻撃は成功となる．

2010 年頃までは，怪しいメールは開かないように注意喚起することで，被害をできる限り未然に防止しようという対策をとっていたが，最近では，事前に調査してソーシャルエンジニアリング[*6] を用いた標的型メールを送付するため，怪しいメールであることをユーザーが判断

できないメールが多い．このため，「ユーザーがいくら注意しても，標的型メールを見分けることは困難である」と考えなければならない．

2. 2. 2　基盤構築

この段階では，初期潜入段階でダウンロードさせたマルウエアが，バックドアによるコネクトバック通信を確立させる．これにより，侵入端末を攻撃者の支配下に置く．また，C&C サーバーを通じて次の攻撃段階に進むために必要な複数のツールをダウンロードし，端末にキャッシュされているパスワードハッシュの搾取や，Windows 標準のコマンドを実行して端末の環境情報，サーバーの位置情報，ネットワーク環境の情報などを収集する．

2. 2. 3　内部侵入・調査

この段階では，侵入端末を基盤として，前段階で入手したネットワーク情報を基に近隣の端末に侵入し，ID やパスワードを搾取していく．この行為を繰り返すことでより多くの ID とパスワードを入手し，より高い権限を奪いながら内部に指令用端末，侵入拡大用端末，情報送信用端末など様々な役割を持った端末を複数分散させて配置した攻撃基盤を構築する．この攻撃基盤構築により，侵入したシステム全体を攻撃者のコントロール下に置くことができる．また，管理者端末を乗っ取り，リモート管理サービスを利用してサーバーに対して不正アクセスを試みる．

2. 2. 4　目的遂行

この段階では，すでに攻撃者が管理者権限で複数のシステムを自由に操作できる状態である．このため情報漏えいやデータファイルの破壊・暗号化などの実害が発生する攻撃を容易に実行できる状況であり，被害を回避するのは困難な状況であるといえる．

3.　標的型攻撃への対策

標的型攻撃への対策として，前章の攻撃シナリオを認識した上で，「初期潜入」，「基盤構築」，「内部侵入・調査」，「目的遂行」の各段階に応じた対策を多層的に講じることが重要である．本章では，ネットワーク，サーバー・端末，その他の防護領域での標的型攻撃の対策例を紹介する．

3. 1　ネットワークによる対策

本節では，外部からの攻撃の侵入および外部への情報漏えいに対し，システムを構成するネットワーク機器で実現可能な対策について記載する．

3. 1. 1　通信のペイロード内からアプリケーションを特定

従来のパケットフィルタリングやファイアーウォールは，各パケットのヘッダー情報に含まれる IP アドレス，プロトコル，ポート番号を参照し，これらの情報が事前に定義したアクセスルールに合致するかどうかで通信の制御を実施している．この仕組みが有効に機能するには，プロトコルとポート番号の組み合わせでアプリケーションを一意に特定できることが前提になるが，近年のアプリケーションは必ずしもこの前提が成立しない．つまり，例えば HTTP/HTTPS プロトコルを使用してメールやファイル送受信，チャット，ストリーミング

などのサービスを利用できる現状では，意図したアプリケーションをプロトコルとポート番号の組み合わせだけで制御することはできない．

これに対処するために，いわゆる「侵入検知」の機能を応用して，あらかじめアプリケーション毎の特徴を定義したシグネチャーを用意しておき，ペイロード[*7]通信内部のデータパターンや振る舞いからアプリケーションを特定する（図2）．これにより，パケットのヘッダー情報のみを通信制御の判定材料にするのではなく，例えばHTTP上にメール機能を実装したウェブメールや，ポート番号を偽装したアプリケーションも制御できるようになる．

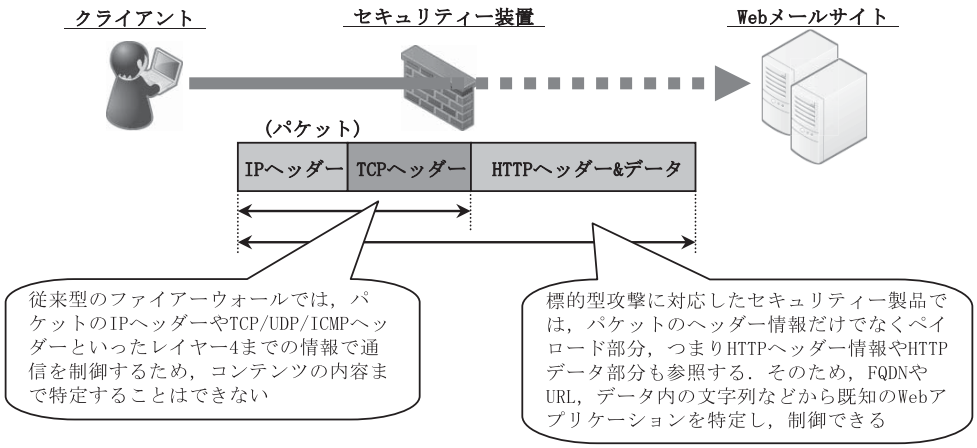

図2　ペイロードを用いたアプリケーションの特定

3.1.2　侵入に成功したマルウエアの検出

システムに対して様々な手段を講じて標的型攻撃に備えたとしても，全ての攻撃を必ず防ぎ切れるとは限らない．外部への情報漏えいを防ぐためには，マルウエアなどの不正なプログラムがシステムに侵入した状況も想定しておく必要がある．システム内に潜伏するマルウエアを発見するのは容易ではないが，多くのマルウエアは侵入後に攻撃者からの命令などを受信する目的でインターネット上のC&Cサーバーと通信を行うケースが多く，この通信をモニタリングすることで，マルウエアに感染したシステム内のノードを発見できる可能性がある．

マルウエアが行う通信は，攻撃対象のネットワークにファイアーウォールが設置されていることを想定して，一般的にファイアーウォールで許可されているHTTP/HTTPSといったプロトコルに割り当てられているポート番号を使用するケースや，自身の通信内容を暗号化することでファイアーウォールやゲートウェー装置のセキュリティー機能を回避するといったケースが考えられる．このような偽装を行うマルウエアの通信を単一の判断材料で特定するのは困難だが，例えば

- 接続先IPアドレスを，これまで収集した攻撃者の接続先IPアドレス一覧と照合
- 未知のアプリケーション（前項のアプリケーション識別機能などを利用）を検出

といった複数の情報から「マルウエアらしさ」を判定し，システム内でマルウエアの侵入が疑われるノードに対して更に調査を行うきっかけにすることができる．

3.1.3　ゼロトラストネットワーク構成

ファイアーウォールのようなゲートウェー型の通信制御機器をネットワークに設置する際，対象のネットワークを「内部（社内 LAN）」「DMZ（外部公開用セグメント）」「外部（インターネット）」といったセグメントに分け，各セグメント間で行われる通信をファイアーウォールで制御する構成が採用されることが多い．この構成では，主な脅威はインターネットなどの外部から侵入するという前提であり，社内 LAN などの内部ネットワーク内での通信は制御の対象にならない（図 3 左）．しかし，昨今の標的型攻撃における侵入経路は，不正に入手されたアカウント情報によるリモート接続や，可搬メディアを経由したマルウエア感染，ソーシャルエンジニアリングによる敷地内への物理的な侵入など，外部ネットワークからのアプローチだけに限定されない．このような背景を考慮すると，社内 LAN のような内部ネットワークを構成する要素は全て信頼できる，という前提は成立しない（ゼロトラストネットワーク[*8]という）．そのため，内部ネットワークの更なるセグメンテーションを行い，図 3 右のようにそれぞれの境界部分に通信制御機器を設置することで，内部における侵入後の脅威の拡大を抑えることが可能になる．

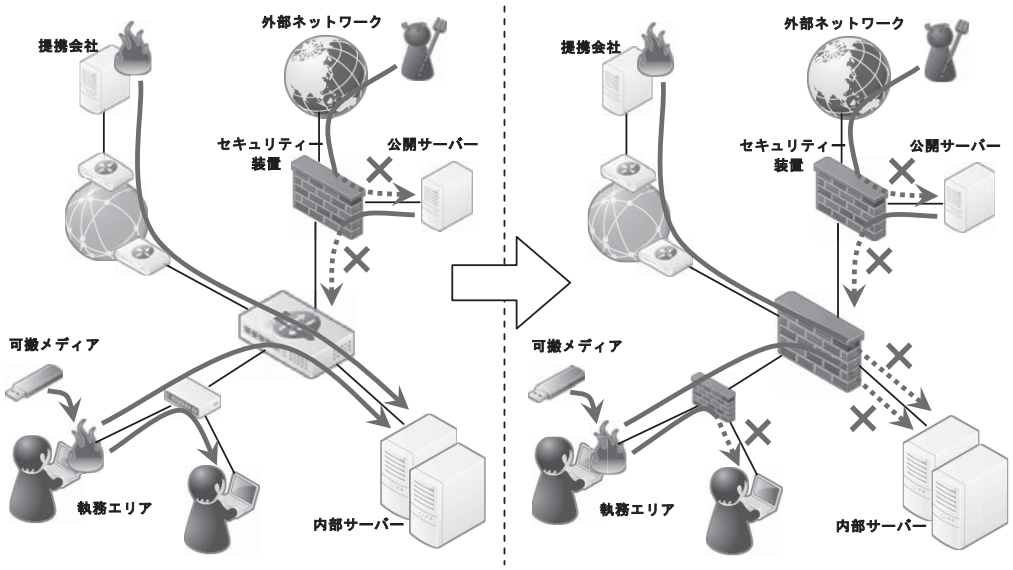

図 3　セグメントの分割によるアクセス制限

3.2　サーバーおよび端末による対策

コネクトバック通信の開設までは，通信を制御するセキュリティー機器が中心の対策であったが，システム内部に侵入された後は，サーバーや端末などの業務・運用機器中心の対策になる．本節では，サーバーおよび端末でできる対策について記載する．

3.2.1　アカウントに関する施策

システムの構築段階では，構築作業の効率化を図るため管理者アカウントのパスワードを同一とすることが多い．また，端末は，同じソフトウエアを導入し，設定が同じものを多数作成することが多いため，マスターイメージから展開することがある．この状況のままシステム運

用に入ってしまうと，「基盤構築」段階で 1 台の端末から奪取された管理者権限情報により，他端末へ侵入し，「内部侵入・調査」段階が容易なものとなってしまう．この対策として，以下の施策が挙げられる．

- 管理者権限を持つローカル ID とパスワードをサーバーおよび端末ごとに変更し，共通の ID を持つアカウントを作成しない．例えば，Windows の管理者アカウントとして広く知られる「Administrator」の ID を変更する．
- 標的型攻撃には，侵入に成功した端末から他端末に対して管理者権限アカウントによるログインを試みる挙動がある．この際，システムに組み込まれたローカル ID による試みがなされるため，この ID を無効状態で存在させることにより，標的型攻撃の兆候をつかむことができる．例えば，Windows では，ID を「Administrator」に設定したゲストアカウントで作成し，無効にしておく．
- 不要なアカウントは作成しない．また，不要になったアカウントは無効にするか削除する．
- 必要なアカウントはパスワードを定期的に変更し，複雑なパスワードを用いる．可能であれば，カード認証や指紋認証などパスワード以外の強固な認証方式を利用する．
- 通常利用するアカウントに管理者権限を付与しない．

3. 2. 2　システム構成に関する施策

OS の機能を有効に活用し，適切なアクセス権限を付与することで，「内部侵入・調査」段階での対策ができる．以下に有効と考えられる施策を記載する．

- ホスト型ファイアーウォールを有効にし，必要な通信のみを許可する設定とする．
- 標的型攻撃に利用される不正プログラムは共有フォルダを介してコピーされ，実行されることにより，新たな侵入端末を増やしていく．この動作を回避するため，共有フォルダへの適正なアクセス権を付与するとともに，不要な共有フォルダは停止する．
- 「内部侵入・調査」段階において，Windows に対する攻撃方法の一つとして侵入端末に攻撃対象端末の管理共有をマウントし，Windows 標準のコマンドを用いて攻撃対象端末の情報を収集する手法がある．この手法を回避するため，Windows 標準で設定されているドライブの管理共有に対するアクセス権を明示的に拒否とする．
- 端末で活動しているマルウエアが，アプリケーションの起動や設定の変更を勝手に実行できないように，ユーザアカウント制御を有効にする．
- 不必要な機能やサービスを停止する．特にリモートからのアクセスを許可するサービス（remote registry サービスや Server サービス等）を停止することにより，侵入されてしまう危険性を軽減できる．
- Internet Explorer などブラウザーの一時ファイルおよびキャッシュを削除する．

3. 2. 3　ログ監視

前項の施策を実施したとしても，標的型攻撃による被害を完全に防ぐことはできない．このため，攻撃による異変が発生した場合に検知できるようにシステムを構成することが重要となる．この観点から前項の施策を実施した際に，ホスト型ファイアーウォールのログの記録とログイン/ログアウトに関する成功/失敗のログ，サービスの開始など環境の変更ログ，オブジェクトアクセスログをイベントログに記録する必要がある．これらのログを確認することによ

り，侵入端末から他端末へのアクセスの発生とその結果およびログイン後の挙動が確認できる．さらに，イベントログから外部のログシステムに送信する構成をとれば，攻撃対象となったシステム内で痕跡を消されても，攻撃されたことを確認できる．

3.3　その他の施策

3.1節，3.2節では，ネットワーク，サーバー，端末による対策を示してきた．本節ではそれ以外の対策について示す．

3.3.1　端末システムの分離

一つの端末で様々な業務を遂行している環境が多い．この環境では標的型攻撃の「内部侵入・調査」段階が進行しやすい欠点を持つ．この問題を回避するために端末の役割を分け，標的型攻撃が進行しにくい環境とすることが重要である．端末をどのように分離すれば対策として効果があるかを以下に示す．

1）　通常利用端末システムと運用業務用端末システムの物理的な分離

「内部侵入・調査」段階では，侵入端末に残されたキャッシュ情報を収集し新たな攻撃対象を検索し，攻撃を仕掛ける方法がある．通常利用している端末でシステムの運用管理を行うと，その端末が標的型攻撃により侵入された場合にキャッシュからサーバーの運用アカウントを取得され，サーバーへのログインを容易にしてしまう．

この問題を解消するためには，通常利用端末とサーバーの運用業務用端末をセグメントで分離し，運用業務用端末が接続されたセグメントは，インターネットへのアクセスを遮断するとともに，通常利用端末が接続されたセグメントとの通信ができないように構成することが効果的である．これにより，通常利用端末が感染した場合でも，サーバーの運用アカウント情報が搾取されにくくなり，サーバー上でマルウエアが実行される可能性を減らすことができる．

2）　メールクライアントセグメントとWeb閲覧セグメントの分離

現行システムの多くは，メールとWeb閲覧を同一の端末で行っている．この環境ではメールに添付されたファイルを開くと，HTTP/HTTPSプロトコルを利用してユーザーに気づかれないように実行される新たなマルウエアのダウンロード，C&Cサーバーとの接続等ができ，標的型攻撃が成功することとなる．

この問題を解消するためには，Outlookなどのメールクライアント端末が存在するセグメントとWeb閲覧を行うセグメントをネットワーク的に分離し，メールクライアント端末ではHTTP/HTTPSを利用した外部接続をできないようにすることが効果的である．具体的には，画面転送方式を用いたシステムで提供したWeb閲覧システムのブラウザーをメールクライアントシステムから利用することでセグメントの分離が可能となる．これにより，メールをきっかけとしたマルウエアの侵入を防止すると同時に，メールに添付されたマルウエアの挙動による影響を極小化することが可能となる．

3.3.2　サンドボックスによる監視

ここまで紹介した施策を実施したとしてもマルウエアの侵入が発生する．この侵入を発見するためには，感染しても他のシステムに影響を及ぼさない監視された環境（サンドボックス）を構築し，侵入したプログラムの動作を検査する必要がある．この際，システムの情報やC&C サーバーなどの不正な通信先の情報を用いることでプログラムの動作が不正であるかどうかを判断する．

多くの標的型攻撃対策ソリューションがシステム内部やクラウド連携などにより，サンドボックスを利用することでマルウエアを検知しようとしている．

4.　まとめ

攻撃の段階に対する防護領域と施策をまとめると表2のとおりとなる．表中の丸印は標的型攻撃の段階に対して効果が期待できる施策を示しており，無印の部分は，その段階の施策としては有効と考えられない施策を示している．

表2　標的型攻撃の段階と効果が期待できる施策

防護領域	攻撃の段階 施策	初期 潜入	基盤 構築	内部 侵入	目的 遂行
ネットワーク	ペイロードによるアプリケーション特定	○	○		○
	侵入したマルウエアの検出		○		
	ゼロトラストネットワーク		○	○	
サーバー/端末	アカウントの施策		○	○	
	システム構成の施策			○	
	ログ監視	○	○	○	
その他	端末セグメントの分離	○		○	
	サンドボックスによる対策		○	○	○

5.　お　わ　り　に

本稿で紹介した施策を実施し，システム運用担当者が日常的にログから標的型攻撃の可能性を検知するのは，不可能ではないものの，運用負荷が非常に高くなってしまう．この運用負荷を軽減するツールとして，標的型攻撃を検知できるソリューションは有効である．本稿で紹介した施策は有効なものであり，あわせて行うことにより，標的型攻撃の脅威からシステムを防御する一助になるものと考える．

標的型攻撃対策の施策は，一度設定を行えばそれでよいというものではなく，定期的に見直し，必要に応じて変更することを継続的に行っていくことが重要となる．そうすることで，新しい脅威への対応が可能となる．

最後に，本稿執筆にあたりご協力・ご指導いただきました皆様に深く感謝し，お礼申し上げる．

＊1　ボットウイルスは，ウイルスの一種で，インターネットを通じて感染したコンピューターを操ることを目的とする．
＊2　マルウエアは，有害な動作を行う目的で作成された不正なソフトウエアの総称．ウイルスもマルウエアに含まれる．
＊3　バックドアは，利用者に気付かれない様秘密裏に構成された通信経路を指す．正規の認証を経ずにセキュリティー対策を回避して通信を行う．
＊4　コネクトバック通信は，侵入対象となるコンピューター側が接続元となって通信を開始し，それに応答する形で侵入用のコンピューターが感染したコンピューターと接続する通信を指す．
＊5　C&C サーバーは，コマンドアンドコントロールサーバーの略でマルウエアに感染したコンピューターに対して命令を行うことを目的としたサーバーを指す．
＊6　ソーシャルエンジニアリングは，セキュリティーの分野では，事前に収集した情報を基に巧妙に偽装し，心理的な隙をつくことでユーザーをだますテクニックを指す．
＊7　通信されるデータから，ヘッダーやメタデータなどを除いた実データをペイロードという．
＊8　ゼロトラストネットワークは，社内システムからの通信であっても「信頼しない」ことを前提に検証を行うネットワークを指す．

参考文献

［1］『高度標的型攻撃』対策に向けたシステム設計ガイド，独立行政法人情報処理推進機構，2014 年 9 月
［2］ サイバーテロ攻撃から組織を守るために　今すぐできる「標的型攻撃」への備え，日本マイクロソフト
https://www.microsoft.com/ja-jp/business/industry/gov/apt/default.aspx（2015 年 11 月 5 日確認）

執筆者紹介

助　川　賢　二（Kenji Sukegawa）
2000 年ユニアデックス(株)入社．システム構築部門にて，Windows/Linux システムの構築に従事．2002 年よりセキュリティー技術部門にてウイルス対策システムの構築を中心にネットワークセキュリティーの提案/構築に従事．

大　冨　哲　也（Tetsuya Ootomi）
2005 年ユニアデックス(株)入社．ネットワーク設計部門にて，主にネットワークセキュリティー製品の構築に従事．2009 年よりネットワーク製品主管部門にて，ネットワークセキュリティー製品の技術主管業務に従事．

佐　野　　至（Wataru Sano）
2008 年ユニアデックス(株)入社．セキュリティー技術部門にてウイルスを中心としたエンドポイントおよびゲートウェーの脅威対策に関する提案/構築に従事．