標的型攻撃　対策指南書

(第 1 版)

株式会社ラック

LAC ともに、イキル

変更履歴

日付	変更内容
2015 年 7 月 28 日	第 1 版　発行

目次

はじめに

この「標的型攻撃　対策指南書」は、対症療法的に局所的なセキュリティ対策を施しただけでは攻撃の回避や被害の発生を防ぐことはもちろん、攻撃を受けたことに気がつくことすら困難な、「標的型攻撃」に企業や団体がいかにして対抗すべきかという課題に対して、当社の考えを整理しまとめた資料です。

本書をまとめるにあたり、企業の経営者や事業責任者にとって、複雑でわかりにくい表現となりがちな技術レポートを、可能な限り概要を理解しやすく、対策の必要性や困難さを感じられるよう、文章表現や構成を工夫しました。いわゆるセキュリティの専門家や IT 技術者にとっても、標的型攻撃に対する準備や対策技術、事故発生時になすべきことや継続的な対策の予算化措置までの取り組みを網羅した参考資料となることを目指しています。

どのような組織であっても、標的とされ執拗に狙われてしまった場合、完全に防御することは残念ながら不可能です。攻撃者は、標的とした組織の IT システムを陥落させるためにあらゆる手段をとることができ、攻撃に使う時間・人員も潤沢に投下することができます。対して防御する我々は、限られた予算の中で限られた技術力と人数で運用を行っており、防御には限りがあります。

ただし、攻撃を受け（ウイルスの侵入を許し）ても被害を最小限に抑え、実害を可能な限り小さくすることは可能です。更に、攻撃の対象になりにくくし被害からの速やかな復旧を行うなど、多方面からの対策を効率よく採用することでより有効な対策をとることが出来ます。この「多層防御」こそが根本的な考え方であり、**標的型攻撃の対策の基本は、「現実的なセキュリティ対策の総合力」**であると当社は考えています。

本書は、セキュリティ対策の総合力とは何を指しているのかを、網羅性をもって指し示します。

なお本書は、対策から抜け落ちていた内容や、標的型攻撃の進化に伴い開発された新しい対策に関しても継続的に改訂増補していきます。標的型攻撃と戦う組織の皆様が、今後も継続的に閲覧いただける資料を目指します。

1. 標的型攻撃の理解と対策の流れ

サイバー攻撃において使用されるコンピュータウイルス（以下ウイルス）は、黎明期のインターネットで「Morris Worm」が半ば実験的に感染を広げた[1]のを皮切りとして、ネットワークを介して攻撃を行う犯罪に用いられることで急速に凶悪化しました。今では、ウイルスを攻撃者自身が遠隔操作し、企業内部を蝕ことが一般的になってきています。

ここでは、日本において危険視されているだけでなく、実害の激増が確認されている「標的型攻撃」とは何かを整理します。

1.1. 標的型攻撃とは

標的型攻撃は、海外では APT（Advanced Persistent Threat）と呼ばれるサイバー攻撃の手法の一つです。日本においては、情報セキュリティ対策推進会議[2]が定義した「高度サイバー攻撃」[3]に含まれる攻撃手法を指します。

なお、標的型攻撃の詳細に関しては、「Cyber GRID View vol.1」をご覧ください。

標的型攻撃の攻撃者は、狙いを定めた組織からまずは様々な情報を窃取しますが、そのためには手段を選びません。その手口は年々巧妙化・多様化し、目的を達するまでは執拗に繰り返します。現在においてもメールにウイルスを添付して直接送り付ける手法が多く悪用されていますが、2013 年に入り、未知の脆弱性を悪用[4]し、特定の攻撃対象組織からの閲覧者に限ってウイルス感染させるようにウェブサイト改ざんを「水飲み場型攻撃」[5]が日本でも初めて確認されました。

下の表 1 は、2014 年 12 月に当社が公開した「Cyber GRID View vol.1」に掲載した、標的型攻撃事案からの抜粋です。言うまでもなく、これらは氷山の一角にすぎません。

攻撃者は、メールでのウイルス添付や、利用者が普段よく訪れるウェブサイトの改ざん、ソフトウェアのインストール・更新時の悪用など、あらゆる手段で標的対象組織のパソコンにウイルスを仕込もうとします。いまでは、ウイルスに感染したことのない組織はまず見当たらないと言っていいでしょう。

日付	報道された主な標的型攻撃の内容
2009/11	世界の石油・天然ガスなどのエネルギー関連企業や製薬会社などへのサイバー攻撃
2010/1	Google を含む米国企業へのサイバー攻撃
2010/6	イランの核燃料施設を標的としたサイバー攻撃
2011/4	ソニーの米国子会社へのサイバー攻撃により個人情報が流出

[1] https://ja.wikipedia.org/wiki/Morris_worm

[2] 現在のサイバーセキュリティ対策推進会議。

[3] 標的型攻撃などを含む、組織的・持続的な意図をもって外部から行われる情報の窃取・破壊等の攻撃（「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（平成 26 年 6 月 25 日 情報セキュリティ対策推進会議）

[4] ソフトウェアベンダからの脆弱性情報や修正プログラムの公開前に、その脆弱性を悪用して攻撃すること。また、脆弱性そのもののこと。

[5] 正規のウェブサイトを改ざんし、そこに標的対象とする組織の利用者が訪れた時のみウイルス感染させる攻撃手法

2011/9	三菱重工へのサイバー攻撃
2011/10	衆議院へのサイバー攻撃によるウイルス感染で議員のパスワードが流出
2012/5	原子力安全基盤機構における情報流出
2012/7	財務省でウイルス感染による情報流出
2012/11	三菱重工（宇宙関連の事業所）におけるウイルス感染
2013/1	農林水産省から TPP 関連などの機密情報が流出
2013/2	外務省ネットワークから外部への情報流出
2013/5	Yahoo! JAPAN への不正アクセスにより、最大 2200 万件の ID や 148 万件のパスワード（ハッシュ）、およびパスワードを忘れてしまった場合の再設定に必要な情報が一部流出の可能性
2014/1	高速増殖炉もんじゅ および国立がん研究センターが、GOM Player の利用時におけるアップデート通信で不正なプログラムを実行される[6]
2014/2	はとバス・ヤマレコに IE のゼロデイの脆弱性を悪用する攻撃コードが埋め込まれる[7]
2014/8	日本で、インターネットサービスプロバイダ（ISP）、学術機関、大学関係者などを対象とする EmEditor の更新チェッカーを悪用した水飲み場攻撃[8]
2015/6	日本年金機構に標的型攻撃。125 万件の個人情報が流出[9]

表 1 メディアで報道された国内外の標的型攻撃の一覧

標的型攻撃では、攻撃者は例えば、標的組織やそこに所属する社員について情報収集し、その組織や関連組織の社員、外部から問い合わせをする人などになりすまし、ウイルスに感染させるためのメールを“継続して（執拗に）”送ります。

組織内のパソコンがたった 1 台でもウイルス感染させられると、攻撃者はそのパソコンとネットワークに関する情報を収集し、それを踏み台に組織内の他のパソコンへの不正アクセスを繰り返します。最終的には社内のシステム管理者などの高い権限を取得して組織内の複数のパソコンを制御し、以降、継続的に組織を観察し、メールや文書ファイルの窃取などを行います。管理者権限が得られない場合でも、感染時の利用者の権限で窃取可能な、Web ブラウザに登録されているアカウント情報やメールや文書ファイルなどの情報を盗み取ります。

[6] http://www.lac.co.jp/security/alert/2014/01/23_alert_01.html
http://www.jaea.go.jp/02/press2013/p14022801/
http://www.ncc.go.jp/jp/information/20140206.html
[7] http://internet.watch.impress.co.jp/docs/news/20140226_637153.html
[8] http://jp.emeditor.com/general/更新チェックによるウイルス感染の可能性/
[9] http://itpro.nikkeibp.co.jp/atcl/column/14/346926/060300268/

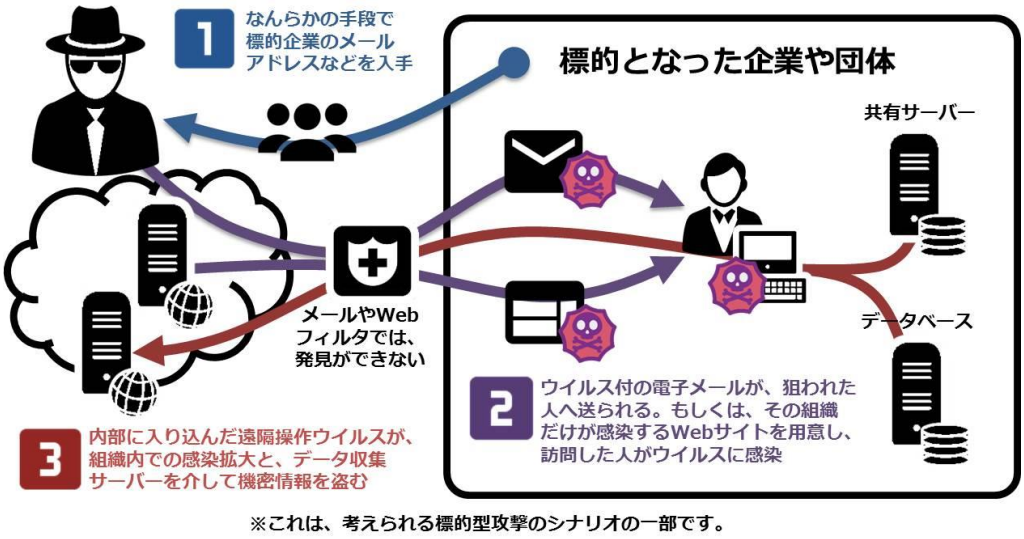

図 1 代表的な標的型攻撃のシナリオ

標的型攻撃で標的型メール（成りすましメール）が使われた場合の、当社サイバー救急センターが実際に対応した被害企業で確認された添付ウイルスの割合は、図 2 になります。

確認された標的型メールのうち、実行ファイル（拡張子が exe、LNK やマクロファイルなど）のように利用者による直接実行を狙ったものが全体の 76%を占めており、利用ソフトの脆弱性を悪用し感染を狙うものより大幅に多く「利用ソフトを最新にしておく」という企業の管理者側の管理では感染を止められない実態が明らかになっています。つまりメールによる攻撃の標的となっているのは実行ファイルの区別が付かない IT リテラシーの低い利用者であることが明白です。

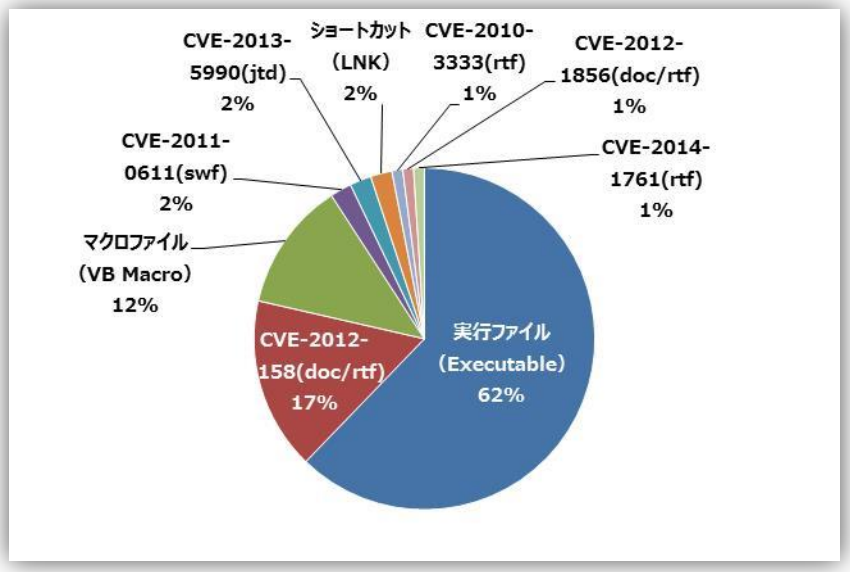

図 2 悪性のファイルの種類・脆弱性の内訳

1.2. 標的型攻撃対策の流れ

従来のセキュリティ対策は、ウイルス対策ソフトやファイアウォールなどの境界防御、セキュリティ修正プログラム（利用ソフトを最新にしておく）による脆弱性対策など、防御機能の実装が主体となっていました。しかし、「1.1 標的型攻撃とは」で示したように、いまや標的型攻撃を万事未然に防ぐことは不可能であることを理解してください。つまり、攻撃を防ぐ取り組みを行いながらも、事故（感染）発生を前提とした対策を考える必要があります。

標的型攻撃の対策は、「はじめに」に記したように、セキュリティ対策における総合力の高さが重要となります。
総合力とは、図 3 にあるようにセキュリティ対策を、組織体制、情報収集、抑止、防御、検知、事故対応、復旧対応、活動評価と予算確保、社員教育の各充実度を示すことで評価されます。

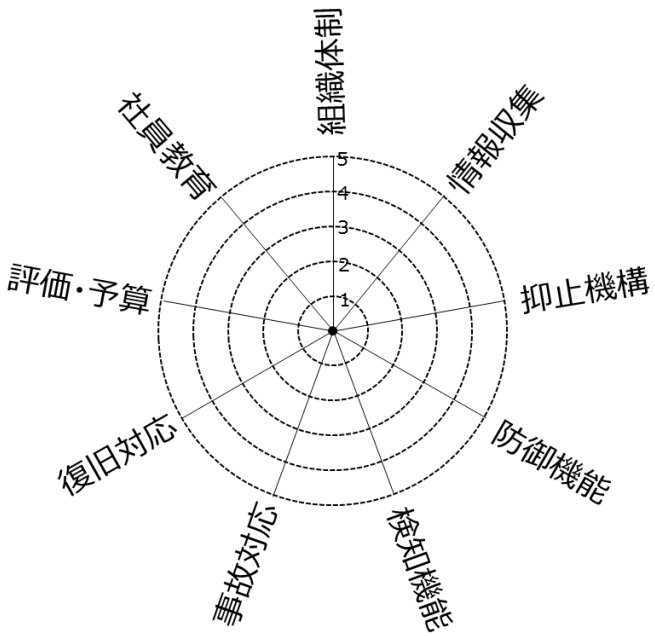

図 3　セキュリティ対策における評価要素

- 組織体制は、包括的なセキュリティ対策を行ううえでの一丁目一番地といえます。セキュリティ対策の知識がある担当者を核として、企業や団体のセキュリティ対策全体のとりまとめを行い、計画し、遂行します。

- 情報収集は、日進月歩で進むセキュリティ上の脅威と対策等に関する最新の情報を、信頼できる情報筋から入手することです。自社の状況を共有しながらも円滑な対策を進める上での貴重な情報を得るための仕組みを社内外に構築します。

- 抑止策は、セキュリティ対策において最も効果的な取り組みです。攻撃者に対して、自社をターゲットとして気がつかせない、攻撃により得るものが少ない、もしくは攻撃をするとダメージを負ってしまう、あるいは攻撃者が攻撃対象としている技術（オペレーティングシステムやミドルウエア、アプリケーションなど）以外のものを利用するといった策を検討します。

- 防御策は、多くの企業が現在行っている、標的型攻撃を含む脅威そのものに対して、そのリスクを最小化するための取り組みです。

- 検知策は、攻撃によりなんらかの被害が発生していないか、また、通常の運用環境で水面下に隠れて暗躍しているようなウイルスがいないかを、あぶり出しをするなどの取り組みです。検知するための仕掛けは、既存の機器に仕掛けを施す、専用の機器を導入して運用する、社員が異変に気づくなどの内部だけではなく、警察や JPCERT/CC などの外部機関から連絡が入るなどもあるため、一番最初に議論すべき策です。

- 事故対応は、実際に防御線が突破され、検知策などでウイルスによる監視や情報の窃取が疑われたり確認された際の、被害拡大防止や被害の封じ込めのための業務停止の判断、技術調査、対外発表、関係機関への報告など、システムと事業のダメージコントロール（被害を最小限に抑えること）を行う取り組みです。

- 復旧策は、事業を復旧させる際に、調査結果や影響等を踏まえ、関係者の事業継続を優先し最短の時間で最低限の機能から復旧させ、事業継続を図る取り組みです。

- 評価・予算は、半年、もしくは一年間のセキュリティ対策の状況の振り返りと、次年度のセキュリティ対策に関する方針や実施内容、予算計画について検討を行うもので、継続的な活動には欠かせない取り組みです。

- 社員教育は、組織を構成する社員全員が、情報セキュリティの理解と対策の重要さを理解し実施することを目指して行われる取り組みです。その為には最低限の情報技術に関わる利用技術（IT リテラシー）教育は欠かせません。特にデータの取扱い技術は必須となっていることを理解しましょう。

標的型攻撃への対処は、防御の困難さに比例して対策そのものの難易度も上昇します。
次章より、対策の流れに沿ってわかりやすく説明します。

2. 標的型攻撃の対策

標的型攻撃の対策は、セキュリティ対策の総合力であり、これをやれば大丈夫というような特効薬は存在しません。なぜなら、そもそも標的型攻撃とは、特定の「標的」に対し、情報窃取や業務妨害等の明確な目的を持った上で、労を惜しまずに執拗に狙い続けるものであり、標的となる組織や団体の弱点を調査した上で攻撃手段が選定されるからです。とは言え、標的型攻撃においてよく見られる攻撃パターンは存在します。本章では、これらに対する対策、更にセキュリティ対策の総合力という観点からも求められる対策にも踏み込んで、当社の考える対策の網羅的な姿を示します。

なお、専門技術的な内容は一般の方にも極力わかりやすく、難解な箇所にはさらに注釈を加えておりますので参考にしてください。

2.1. 推進体制の整備

標的型攻撃の対策を考えたとき、事故発生を前提とした対策の設計が必要であるという考え方は、本書では何度も登場します。たとえば、企業経営を行う中で、製品のリコールをはじめとした品質の問題や不祥事のリスクというものが存在することは広く理解されており、それに対応する準備が行われています。では、情報セキュリティの事故が発生したときの準備ができている企業はどれほどあるでしょうか？

ここでは、標的型攻撃への対策を推進する、原動力となる組織体制の話をまとめます。

セキュリティは、すでに経営課題。経営者の参画は必須

情報セキュリティに関わるリスクは、いまや企業の存亡にかかわる大きな課題であることに議論の余地はありません。特に標的型攻撃の対策は、IT 技術者だけが自身の領域で解決できる範囲を超えており、組織のセキュリティ推進体制には経営層の参画が必須と言えます。

その多くがサイバー空間で発生する情報セキュリティの事故に対して、IT の専門家ではない経営層はどのようなかかわりを持てばよいでしょうか。お手本となる企業の経営層は次のような姿勢で臨んでいます。

- セキュリティ対策の推進への積極的な参画と支援
  情報システムを活用し、ネットワークを介した事業の活性化や効率化を図るとき、そこには情報セキュリティ面のリスクが伴います。そしていまやこのリスクは経営レベルでの判断が必要であるほどになりました。「100%安全」ということなどあり得ない中で、放っておけばリスクに関する悪いニュースは入ってこなくなり、セキュリティは無視されていきます。セキュリティリスクへの危機感は、トップダウンで対応しなければ失われていくのです。経営者は人員と費用の投資や社員への理解促進により、セキュリティ対策を積極的に支援します。

- 企業内セキュリティ推進組織(以下 CSIRT[10])からの報告を理解する
  次節に述べる、CSIRT を構築することはもちろん、CSIRT が作成するレポートの内容を理解し、経営としてどのような判断をするべきかを検討します。逆の言い方をすれば、セキュリティリスク対応が経営課題である以上、経営層が理解できる内外のセキュリティ状況に関するレポートがきちんと提出されているかどうかが企業として重要です。あなたの組織では、自組織がどの程度のリスクを抱えているか、きちんと経営層に見えているでしょうか。

- 事故対応におけるリーダーシップ
  万が一標的型攻撃による被害の疑いが確認された場合、社内が混乱することは避けられません。そんな中、経営層には CSIRT および事業責任者と協調し、事業や企業活動の一時停止に関しての決断を行うなど、リーダーシップを発揮する必要があります。
  社会的な説明責任を伴う問題が発生した場合には、関係者に対して状況の説明を行い、組織の責任者として対応の矢面に立つ覚悟をし、備えをします。
  そしてそれは、「万が一」のことではもはやないのです。

こうした行動は、一朝一夕に整備できるものではありませんが、認識は直ちに必須です。情報セキュリティ実施の意思を持つ経営層を円滑にサポートするには、IT 部門や総務部門の枠組みにとらわれないセキュリティ専門組織を整備することが有効です。

企業や団体の中に、専門化集団を組織する

最近、標的型攻撃の被害を受けていることに警察や JPCERT/CC のような外部からの指摘によってはじめて気づくというケースが相次いで発生しています。あなたの組織の代表窓口にそのような連絡が入った時、あなたの組織では誰がどこに連絡し、どのような役割分担で、何を調査して事実確認を進めるべきでしょうか。

たとえばそれが誤報であったと仮定して、自信と証拠を持って反論することはできるでしょうか。

標的型攻撃の手法で、2015 年 7 月現在の代表的なものはウイルスメールの添付、および Web サイトを介してウイルスを送り込む水飲み場攻撃です[11]。しかしこれらの攻撃手法は日進月歩で進化しており、いつまでも同じではありません。例えば、出張先のホテルの無線通信を使用したらウイルスに感染した[12]、ソフトウェアを更新したら正規の更新情報にウイルスが潜んでいた[13]、といった事案も発生しています。レガシーな侵入の常套手段である USB メモリを通じて侵入やサイトをハッキングされた侵入と言ったことも見逃してはいけません。

[10]シーサート：Computer Security Incident Response Team の略で、事故対応チームを指します。
[11]http://www.lac.co.jp/security/alert/2013/10/09_alert_02.html
[12]https://blog.kaspersky.co.jp/darkhotel-apt/5392/
[13]http://www.lac.co.jp/security/alert/2014/01/23_alert_01.html

今、企業や団体には、日々悪質化する手口を理解し、翻って自社組織内の対策状況とのギャップを把握し、予算やビジネス要件と折り合いをつけながら優先順位を付けて対応していくことが求められています。

こうしたセキュリティ推進組織の活動は、決して簡単なものではありません。そのため、活動の中心には、サイバーセキュリティ上の脅威を深く理解し、かつビジネス推進との間での最適解を見極められる専門チームが必要です。

多くの日本企業の間で、CSIRT（シーサート）と呼ばれる組織が立ち上がっていることをご存知でしょうか。CSIRT とは、いわばサイバー事故対応の専門チームで、サイバー攻撃手法や防御に関する知見と経験を持つ、「サイバー空間の自衛消防隊のようなもの」とされてきました。

しかし、今必要な標的型攻撃との戦いというのは、専守防衛ではあっても本質は「サイバー戦」であり、従来の知見と経験に加えて、「敵」の手法や狙いを把握していることが決定的に重要です。

我々は、CSIRT が「敵」をよく知ることにより、事故が起きた時の対応に留まらず、常日頃から標的型攻撃対策推進を主導する組織になるべきだと考えています。

それでは標的型攻撃に対応した CSIRT は、組織のセキュリティ推進・運営の中で具体的にどのような機能を担うべきでしょうか。その一例を、表 3 に示します。

分類	業務機能	内容
情報セキュリティ企画業務 ＝事前対応＝	体制、権限などの整備	・情報共有すべき連絡先の整理 ・暫定対応時の被害遮断等の権限整備 ・事故対応手順書などルール集の策定、整備 ・証拠保全、警察等へ提出する情報の収集対象・手順の整備
	システム状態評価	・セキュリティ文書（スタンダード、ガイドライン、チェックリスト等）の所管 ・ネットワーク構成情報、システム構成情報、対策実施状況の収集と管理 ・脆弱性診断実施計画の企画、立案、実施結果の評価、対策の推進 ・システム安全性評価、リスク分析の企画、立案、実施結果の評価、対策の推進
	教育・訓練の企画・推進	・セキュリティ教育、啓発、訓練の企画、推進、結果の評価
	新サービスの評価	・第三者の専門家によるリリース評価
	脆弱性情報の収集と活用	・プログラムバージョン、セキュリティパッチ適応状況の把握 ・外部からの脆弱性情報収集と活用 ・脆弱性情報に基づいた、注意喚起や脆弱性対応の通達
外部侵害監視 ＝早期検知＝	攻撃動向の把握 情報収集力強化	・外部からの攻撃動向情報収集と活用 ・既存ベンダ情報の収集と活用 ・注意喚起情報の展開、追加対策の実施を提言
	ログ管理の強化推進	・攻撃動向より管理対象ログ、解析手法等の改善提言
外部侵害事故 ＝事後対応＝	連絡体制の設置	・対応態勢の確認 ・受付窓口の設置
	外部侵害発生時 の対応支援	・状況把握、証拠保全、対処 ・広報、当局報告、経営報告の支援 ・外部に対する協力依頼、外部機関への報告
	再発防止策の検討	・再発防止策の検討、評価

表 3　CSIRT の果たすべき機能(※JPCERT/CC の資料をもとに、当社にて修正加筆)

このように、組織が、サイバーセキュリティにおいて「敵を知り、己を知れば、百戦あやうからざる」状態を目指すとき、CSIRT の果たすべき役割は非常に広範なものとなります。

それでは、こうした大役を担う CSIRT を整備する上で、どういったポイントがあるでしょうか。

当社は、これまでに多くの企業の CSIRT の設立支援や運用改善支援をし、現在も多くの CSIRT 関係者とお話しする機会がありますが、活動が充実しているチームと、活動が不十分なチームでは、表 4 のような違いがあります。

「名ばかり」CSIRT		「本物」CSIRT
事故対応はするが、検知は外部通報頼みで口をあけてまっている	モニタリング	モニタリングの仕組みがあり、「検知」の仕組み、トリガーがある
「○×通報制度」のように、窓口はあるが連絡の敷居が高くなってしまっている	コミュニケーション	各部門に、face to face で顔が売れており、色々な相談が舞い込む下地がある
個々の脆弱性情報の収集等にとどまっていて、「リスク」をとらえきれていない	情報収集	内部の情報、業種コミュニティの情報、外部の情報、海外動向等広く収集している
「何をしなさい」という情報にしか反応できない	情報分析	収集した情報から、的確に自社へのインパクトや取るべきアクションが判断できる
事故対応チームの機能に拘泥し、情報発信が無い	情報発信	社内、そして社外に対して警戒情報をはじめとした情報発信をおこなっている
事務色が強くなってしまっており、専門スキルが低い	スキルレベル	フォレンジックをはじめとした技術的専門スキル、調整能力、情報整理力がバランス良くそなわっている
技術的な事実しか答えない、答えられない	スキルエリア	時には推論や示唆を踏まえ、ITセキュリティ脅威の理解と共にビジネスを理解した上でアドバイスができる
方針が無いと決められない、要件が無いと決められない、100%確かではないと決断ができず、火急の時も動きが遅い	マインド 仕事の流儀	80%完成度、80%確からしさ、200%スピード

表 4　名ばかり CSIRT と本物の CSIRT の比較

これらはすべて本質的な考え方の違いを表しています。CSIRT は、考え方や目標の異なる各組織に根ざすものであり、もし「名ばかり CSIRT」に該当するような問題があっても一朝一夕に改善できることはなく、また共通する万能策や雛形というものももちろんありません。

とはいえ、CSIRT を機能的に活動させるためには、組織整備上注意すべきポイントがあります。例えば次のようなことです。

- 社内に宣伝する、売り込む

  CSIRT に社内の情報が集まり、またその意思決定に対して理解を得るためには、社内に活動内容が浸透していることが重要です。そのためには、社内からセキュリティ上の悩み事、相談事、気になることを気軽に連絡できることが大事であり、平素からの顔の見えるコミュニケーション、情報の発信といった活動を意識的に組み込んで設計することが重要です。

- 詳細なマニュアル例を用意する

  「○○攻撃対応マニュアル」は、できるだけ詳細なレベルで用意します。

  これに沿って対応を円滑に行うためと思われるでしょうか。実はそうではありません。実際の事故対応は、マニュアル通りになど進みません。また、そもそも「マニュアルが無いから対

応できなかった」ということでは困ります。想定外の事態が起こることを考えなければならないからこそ、CSIRT が必要なのですから。
ある想定攻撃シナリオに沿ってマニュアルを書くことの本質は机上訓練であり、事故対応の優先順位や思想、求められる役割等の認識を共有する作業なのです。

- 権限は比較的厳密に規定する

マニュアル対応に収まらない CSIRT の活動を円滑にするポイントは、権限だけは明確にしておくことです。事故は全員がそろっている平日の昼間に起きるとは限りません。社内における CSIRT の位置づけと権限の範囲を事前に明確にしておくことで、事業責任者が不在等の状況でも、被害の拡大防止が可能になるのです。例えば、ネットを遮断する、パソコンを隔離し調査する、プロキシサーバのログやメールの記録を調べるなど、夜間や休日に実施しなければならないのは当然です。それらと、それらが誤報であることも前提とした権限の定義を決めておきましょう。

現在、標的型攻撃対策を推進する組織が無い場合、この際 CSIRT という形で IT セキュリティ対策の推進力を整備・強化することは、とても有効な手段です。

社員の理解と参画

企業や団体の経営層の皆様や、セキュリティの専門家である CSIRT が組織化されたからといって、標的型攻撃の撃退は可能なのでしょうか？ 企業には、CISRT 以外にも大勢の社員がおり、標的型攻撃の多くは人事部門や総務部門を含む社員全体を対象としている事実を考えると、セキュリティ対策に関する一般社員の理解の促進は大変重要です。

2015 年 6 月 1 日に発表された日本年金機構の情報流出事件においては、情報系ネットワーク（通常のオフィスエリア）における個人情報取扱いに関わるルール違反の結果、個人情報流出事件に至ったと言われています。

社員に情報セキュリティの重要さの理解促進（リテラシー教育や標的型攻撃メールの訓練、事故対応訓練など）やセキュリティ対策の実施の徹底のほか、経営層や CSIRT の要請に応じ事故の的確な報告など指導をすることも重要です。

2.2. 情報収集と情報共有

標的型攻撃は、国家のように高度で強い意志が働いている組織の仕業であり、知的好奇心や自らの功名心で行われる犯罪ではないと考えられています。攻撃の多くは日本国外から到達しており、外交機密、防衛機密、重要技術情報や莫大な金銭的価値のある情報、更なるターゲット攻略への足がかりとなる情報を求めて攻撃が行われていると考えられています。

日本の産業競争力をはじめとした国力を守るために、というのは少し大げさかもしれませんが、ある業界で、A 社から情報が流出し、同じ手法で B 社からも情報が流出し、C 社からも流出し、といった展開を許してしまうことは決して国益にかなったものではなく、また業界全体の利益にも、そして個々の会社の利益にも悪影響があることは明白です。

例え A 社からしか情報が流出しなくても、いつのまにか外国企業の技術力があがっていて、市場競争環境が悪化するということがあれば、B 社、C 社にとっても望ましいことではないはずです。

公平な競争環境という、経済活動の土台そのものが、無策でいては保証されないのです。

標的型攻撃対策を考えるとき、彼らの違法な情報収集を許してはいけません。その為には個々での「情報収集」が重要であることは自明ですが、「敵を広く知らしめる」ためには企業を超えた「情報共有」に踏み込む必要があります。特にある業界全体が標的になった例は多く見られ、業界内部での情報共有の仕組みの重要性が高まっています。その為には単なる攻撃だけではなく、攻撃基盤ともいえる指令サーバ[14]や水飲み場攻撃の使われた改ざんサイトなどの情報を共有することを考えなければなりません。つまりは、自分が標的型攻撃の対象になったときだけではなく、その踏み台になったことが発覚したときにこそ、情報共有の第一歩が始まります。勇気を持って詳細に調査する、警察や JPCERT/CC に協力し適切な情報共有が行われるように協力する意思を決めておかねばなりません。

CSIRT による情報収集

CSIRT が収集すべき情報には、大きく分けて社内の情報と社外の情報がありますが、社外の情報の収集だけに絞っても次のようなものが挙げられます。

- 脆弱性情報
- セキュリティ事故発生状況
- 攻撃予告等の早期警戒情報
- 感染調査するための情報（指令サーバやウイルスの特徴等）

CSIRT には、これらの具体的情報を収集し、自組織に対するインパクトを的確に判断する能

[14]コンピュータに侵入したウイルスを遠隔操作するためのサーバ。C&C サーバとも呼ばれる。

力が求められます。また、これら「点」の情報を有機的に解釈し、サイバーセキュリティ動向を示唆する情報として分析することも必要でしょう。しかし実際には、多くの企業の CSIRT では、比較的容易かつ定型で収集できるソフトウェア等の脆弱性情報を収集することだけで、その先の分析までは行いきれていません。

当社は、海外を含めたセキュリティ事故事例を日常的に収集し、自社で調査している事案との関連性などを分析していますが、情報が正しく入手できた場合には、考えられる原因や手法、とるべき対策について推測することが可能です。

これが可能なのは、分析技術や事故対応経験も関係しますが、日常的にセキュリティ事故情報を注視し、考えられる攻撃シナリオや脆弱性について分析し、そして自組織にあてはめた場合に何が起こるかをシミュレーションし続けていることが背景にあるためです。

攻撃予告等の早期警戒情報については、公的機関からの連絡、セキュリティ企業からの連絡等で知ることが多いでしょう。実際には、攻撃予告が行われる攻撃については、技術的に想定できる範囲の手法[15]であることが多く、適切なセキュリティ対策が行われていれば過度に恐れることはありません。とはいえ予告情報が手に入れば何もしないわけにはいかないのが現実です。

こうした攻撃予告情報は、確実に入手できるように準備しておくことが重要です。入手した場合は確実に対応することが CSIRT の錬度を高め、標的型攻撃対策の総合力アップにつながってゆきます。

CSIRT による情報共有

「はじめに」に記載したとおり、標的型攻撃対策では、攻撃手法の情報、相手の用いている武器（ウイルス添付メールの文面や、ウイルスファイル、その通信先等）の「敵の動き」をつかみ、お互いの防御に活かす必要があります。

現在では、各社の CSIRT を主体として、様々な情報共有スキーム、情報共有団体が生まれています。これらは従来から日本でも組織されている「職能団体」や「業界団体」です。

代表的な情報共有団体には、例えば NCA(日本 CSIRT 協議会)、各業界の ISAC 団体（Information Sharing And Analysis Center, 情報共有分析センター）、国際的な枠組みでは FIRST(Forum of Incident Response and Security Teams)などがあり、実際に脅威の封じ込めに直結する情報を含めた活発な意見交換・情報共有が行われています。海外の情報共有団体に参加すれば、「次に日本に来るサイバー攻撃」の予測ができることも大きな利点となるでしょう。

「そんなに頼もしい団体があるのか、ぜひ入って情報を今すぐ入手したい」と思われたでしょうか。これらの団体は、基本的に情報交換のフレームワークを提供するもので、情報共有そのものは参加している企業や団体が自発的積極的に進めるものです。誰かが音頭を取ってくれるような枠組

[15] ただし、とにかく大量の通信を投げつけて対象を麻痺させる DoS 攻撃等、単純ではあるが防ぐことが難しい攻撃というものも存在します

みではありません。重要なことは、自ら進んで情報を提供し、議論に加わることです。
　もしあなたが自組織に対して行われたサイバー攻撃情報を共有しても良いと考えるとしたら、それはどんな相手に対してでしょうか。答えはおそらく、同じように情報を提供してくれる相手とでしょう。

「職能団体」や「業界団体」を円滑に運営するには、会で率先して貢献することは人付き合いの上で基本です。情報交換の場での貢献は、自社で把握した情報を信頼する仲間に共有し、そのフィードバックを得ることであり、仲間の事案に対する自らの考えを発言することです。情報は寂しがり屋とも言います。持っているところに集まるのです。
　もちろん、自組織に対して行われた攻撃の検知や、調査・分析を行うため、CSIRT の組織化とスキルアップは必要になりますが、情報共有をする意思があれば、仲間が支援してくれます。それが互助会の良い点です。

「そうは言っても、いきなりはなかなか」という声も聞きますが、そうした場合には、同業種の特定社の CSIRT チームとまずは意見交換をするという方法があります。普段はライバル企業同士であっても、共通の敵に対しては利害が一致している筈です。
　当社では、設立のお手伝いをした CSIRT チームのご担当者間の意見交換会等をコーディネートすることがありますが、セキュリティ推進担当から、互いにとても参考になったというご意見を頂きます。

世界的注目を浴びる東京オリンピック・パラリンピックのような大イベントの際には、様々なサイバー攻撃が日本を襲うことは間違いありません。今後情報共有の仕組みの堅牢性、スピード等の重要性は増すばかりですが、大変残念なことに、サイバー攻撃の事実をいち早く発表・共有しても「面倒なことが増えるばかり」という状態にあります。そのような環境の中、生きた情報が十分に流通するためには、人間的な相互信頼と「互助の精神」に頼らざるをえないのです。

2.3. 抑止策の実装

これまでの標的型攻撃の対策として語られている多くは、本資料の「2.4. 標的型攻撃と被害拡大の防御機能の実装」もしくは「2.5. 標的型攻撃と被害発生の検知機能の実装」に集約された技術的な部分や、もしくは「2.6. 標的型攻撃による被害の対処とダメージコントロールへの備え」のような事故発生時の緊急対応、そして技術者育成といったものでした。

標的型攻撃とは、その名のとおり攻撃対象を特定し、被攻撃者に合わせ効果的な方法で攻撃を行います。周到な計画の上で行われるこれら攻撃行為を防ぐことが困難な理由は、この攻撃の個別対応（カスタム化）にあると考えています。

それでは、攻撃を甘んじて受けなければならないのでしょうか？

たとえば自組織に標的型攻撃が行われることを抑止することはできないのでしょうか？

ここでは、これまでほとんど語られていない、標的型攻撃の抑止策についてまとめます。

標的の抑止が効果的な組織か否かの判断

2011 年に当社は、「ソニーの情報漏えい事件で我々は何を学ぶか」と題して、情報漏えい事件を題材に、攻撃者のプロファイリングをしました。その後当社も様々な事件を経験し攻撃者を以下のように分類できると考えています。

- 愉快犯（高い技術を持ち技術的好奇心から脆弱性の発見やハッキングをする）
- ストーカ（恨み等により執拗に個人に付きまとう）
- 主義主張者（アノニマスのようなハッカー集団や政治的主張を行うキャンペーン等、自らの正義感により、国家や企業を攻撃する）
- 金銭目的の犯罪者（こそ泥、詐欺師、恐喝犯、インサイダー、強盗など）
- 国家等による権益拡大（国家やそういったレベルの組織が行う諜報活動や破壊行為等）

攻撃者がどのような立場で、何を目的に行っているのかを考えると、標的となる抑止の取り組みに効果があるのか否かを判断できるでしょう。

たとえば、以下のような属性を持っている、または攻撃者がそう考える企業や組織は、非常に強い意図をもった攻撃者により攻撃される可能性があると考えられ、抑止の効果は期待できない可能性があります。

- 国家機密にかかわる情報や事業を行っている
- 大規模プロジェクトに関わる事業を行っている
- 大量の個人情報を持っている
- 人や会社を脅すための情報を持っている
- 金銭などのトラブルに発展しやすい事業を行っている

- 反社会的と誤解を受けやすい事業を行っている

※ほかにも機微情報や攻撃を呼び込みやすい属性があります。

たとえば、ある国家が他国の軍備情報を秘密裏に閲覧したいと考えた場合、国家機密および軍備に関連した企業などを狙うことが考えられ、このような要求に対して抑止は働きません。

しかし、オンライン販売を行う EC サイトの顧客情報を窃取したいという動機を受け、複数ある事業者のなかでどこを標的にするかを決定するときに、リスクや手間が高く、成果が少ない企業よりは、リスクや手間が少なく、成果が高い事業者を狙うことになるでしょう。このように複数の攻撃対象がある中で標的から逃れることを考えた場合、抑止の取り組みは効果を上げる可能性があります。

標的にされないための 2 つの考え方

標的型攻撃を受ける前に、そもそも標的にされないということを考えるとき、「積極策」と「消極策」が考えられます。

「積極策」：その企業や組織のことを知らせた上で、攻撃をすることを躊躇させたり、攻撃が無意味であることを知らせたりする方法です。

「消極策」：その企業や組織そのものの存在を目立たせず、攻撃の対象になることを免れる方法です。

それでは、これら 2 種類の抑止方法について、実現性の有無や可能性の高低を考慮せずに列挙します。

積極的な標的型攻撃抑止策

積極的な抑止策とは、攻撃者が自社を攻撃対象から外すための材料を公表するか、攻撃しても得られるものが少ないと判断させる材料を公表するものです。

1. 情報をあえて小さく掲載する
   契約数や実績数など、貴重な情報が集まっているという印象持たせないよう、あえて競合他社に比べて小さく掲載し、目立たないように工夫します。もちろん、上場企業等に課せられた情報開示義務に抵触しないことが条件となります。

2. 報復することを表明する
   攻撃を受けた場合、攻撃者を特定して報復措置をとることを表明し、リスクがあることを認知させます。ただし、攻撃者の特定の技術的な課題や報復の連鎖、報復に関する倫理的な問題が残るため安易には実施できません。

3. 懸賞金を公表する
   攻撃を受けた場合に、懸賞金をかけて犯人を探し出すことを公表し、リスクがあることを

認知させます。海外においては、ウイルス開発者の摘発に懸賞金を掛ける事例があり、公表をすることに一定の抑止効果は考えられます。しかしながら、国際犯罪組織に対する取り組みを行うことになることが想定され、現実に実施するには多くの課題が残ります。

4. 攻撃の分析情報を公開する
   攻撃を受けた技術情報を公開し、自社の調査能力をアピールすることにより、攻撃者に厄介な攻撃対象であるという印象を与えます。この取り組みは、当社も「脅威分析情報の公開」で実施しています。さらに踏み込んで攻撃組織のプロファイルまで行い世間を見方につけて社会的に非難するキャンペーンを行う方法も考えられます。しかし、ネットワークやコンピュータのフォレンジック技術に対応できる体制を用意することは容易ではありません。

消極的な標的型攻撃抑止策

消極的な抑止策とは、攻撃者に対して企業や組織を目立たなくさせ、攻撃の矛先が向かないよう情報のコントロールを行うものです。

1. 情報を隠蔽する
   自社の事業について、契約顧客数や取引先情報などを公表しないことで、企業や組織が価値のある情報を保有し、大きな事業を展開していることを悟られないようにします。しかし企業の透明性や企業のアピールを展開する活動との相性が悪く、現実の実行は困難です。一般の企業であれば、ウェブサイトのログを隠蔽することにより特定組織を狙った水飲み場攻撃の踏み台にさせられることを抑止できる可能性があります。

2. 大きな話題となる目立つ発表やコミュニケーション方法を考慮する
   話題性をもったアピールや、派手で目立つコミュニケーションスタイル、奇抜な発想の主張など、目立ちすぎる話題の提供や攻撃者を刺激するアピールには、不要な攻撃のきっかけを与えるため、それを実施すべきかどうか考慮することが重要です。

現実的に標的型攻撃の抑止は可能か

ここまで、抑止の方法に関するアイディアを紹介しました。海外企業において取り入れられている手法なども含め、日本国内で有効に機能させられる取り組みは限られています。しかし標的型攻撃の深刻さは今後も低減するとは考えにくく、ますます加速するという観点に立った場合、抑止策の可能性を検討することも現実には必要かもしれません。

現実世界においては、警備会社や警察立ち寄り所などの掲示や、企業イメージを意識した慎重なコミュニケーション手法、警察との協議による懸賞金など、組織に対する犯罪行為の抑止手段は実装されています。サイバー分野においても、今後抑止施策は検討の課題になると考えています。

2.4. 被害拡大の防御策の実装

標的型攻撃では、ターゲットの最も脆弱な部分を狙って、複数の経路で攻撃が行われます。一般的には、メールによる攻撃が最も多く、次に Web 経由での攻撃が続きます。この 2 つの経路は、どこの企業・組織に対しても利用しており、インターネットから直接に利用者の端末にウイルスをダウンロードさせたり、実行させたりすることができます。そのため、メールと Web については、できる限りウイルスを内部に入れないような対策が防御策となります。

本項においては、代表的な対策として知られる手段の概要をまとめます。防御策は多岐にわたりますので、今後の改訂により網羅性を高め、詳細な対策法を整理してまいります。

必ず実施すべき最低限の対策

ウイルスの感染を対象のパソコンで防御するためには、既存のウイルス対策製品では基本的にはウイルスのパターン[16]が存在しないと検知・防御することができません。標的型攻撃で使われるウイルスは、ウイルス対策ソフトでは検知することがないことを確認した、使い捨てのウイルスで突破を試みるからです。ただし、パターンが更新されれば検知・防御できる可能性があるため、ウイルス対策製品は必ず導入します。また、実際に被害が発生した場合、ウイルス対策製品を導入していなかったという事実が大きな脅威となります。言い訳が出来ないためです。

このように標的型攻撃で使用されるウイルスは、攻撃者も手に入れることが出来る一般的なパターン検知による市販のウイルス対策製品で防御することは困難であるため、攻撃者側は入手しづらい振る舞い検知機能を持つウイルス対策製品を導入します。

また、従来のパソコン上でのウイルス対策に加え、ネットワーク上でのウイルス検知機能を持った機器(FireEye など)の導入も有効です。

メール

メール経由のウイルス感染は、組織のパソコン利用者のメールアドレスを何らかの方法で入手します。その後、メールを受信した利用者に対して直接ウイルスを送り込み、利用者がうっかり送り込まれたウイルスを実行してしまう[17]と感染被害につながります。また、メールシステムは元来、送信元情報を偽装[18]できるため、取引先の担当者の名前を騙るなどの手段で信用させます。メールの文章も簡単には見分けがつかない完成度の高い内容や実際に使用されたものであることが多く、メールを受信したパソコン利用者は、疑念を抱くことなく、ウイルス感染させられてしまうケースがほとんどです。

1. メールによるウイルスの感染で最も多いのは、Windows の実行形式のファイル（拡張子が".exe"のファイル）を添付して、受信した利用者に実行させる方法です。実行形式のファイルを受信した場合には、メールサーバで添付ファイルを削除するか、受信を拒

[16]シグネチャともいう、ウイルスの特徴を集めたデータベースで、ウイルス対策ソフト毎に提供されています。

[17]パソコン利用者の多くは、実行ファイルとは何かを認識せずにパソコンを利用しているのが実態です。

[18]メールシステム(SMTP)は、送信者情報を送信者が設定する仕組みのため、別人を装った送信も可能です。

否するなどして、利用者までメールが届かないようにします。或いは Windows 以外のパソコンで添付書類を開きます。

2. 不正な文書ファイル（例：拡張子が".doc", ".docx", "pdf"のファイル）を送り、利用者にファイルを開かせることにより、Office や Adobe Reader といったソフトウェアの脆弱性を悪用することで、ウイルスに感染させます。パソコンで使用しているソフトウェアは常に最新の状態にします。或いは正規のソフト以外の閲覧ソフト或いは Windows 以外のパソコンで添付書類を開きます。

3. メールに Web サイトのアドレスを書いて送り、利用者にクリックして実行させた際に、ブラウザや Flash Player や java などの脆弱性を悪用することで、悪意あるプログラムを実行してウイルスに感染させます。パソコンで使用しているソフトウェアは常に最新の状態にします。また、Web のウイルス対策もあわせて実施します。或いは Windows 以外のパソコンでリンクをクリックします。

4. 送信元ドメインや送信元メールアドレスを偽装してメールを送信し、メールを受信する使用者をだまします。送信ドメイン認証である SPF（Sender Policy Framework）を使用し、正しいドメインからメールが送信されているかチェックします。

Web

Web 経由攻撃は、不正な Web ページを用意し閲覧者のパソコンにウイルス感染させる手段として使われます。メールに比べれば、不正な Web サイトに利用者を誘導する手間が必要ですが、通常の Web サイトが改ざんされ不正なプログラムが埋め込まれるなど、見た目で不正な Web サイトと気づくのはほとんど不可能です。

1. インターネット上の任意の Web サイトを使用する必要のない業務や利用者の場合には、ホワイトリスト[19]による指定したドメインへのアクセスに限定します。

2. Java や Flash Player など、ブラウザのプラグインとして実行される特定のアプリケーションは、危険度の高い脆弱性が存在することが多く、ウイルスの感染に悪用されることが多いため、これらの機能を無効化、もしくは可能であれば削除します。業務で必要な場合は、そのサイト利用時のみに該当の機能を有効にします。

3. ２.を実施しても、攻撃者はブラウザなどのソフトウェアの脆弱性などを突いて、ウイルスに感染させることができます。そのため、パソコンで使用しているソフトウェアは常に最新の状態にします。

[19]ブラックリストの反対で、接続や実行を許可しているサイトのリスト

4. 攻撃者は、Web サイトに埋め込まれた不正なコードや、不正なプログラムをダウンロードさせることで、ウイルスに感染させることができます。そのため、Web 用のウイルス対策製品を導入して、HTTP でダウンロードしたコンテンツのスキャンを行います。

5. Windows 若しくは Window 上で動作するソフトの脆弱性が悪用されることが多いため、メールやサイト閲覧などだけであればパソコンを使用しない方法を取ります。

その他ネットワーク経由の攻撃

ウイルスのネットワーク経由の侵入経路としては主にメールか Web ですが、自組織以外のネットワークとの境界では、ウイルスに限らず不正侵入を防御するために対策が必要です。ネットワーク境界には、ファイアウォールなどによるアクセス制御のほかに、攻撃を防御するような製品を導入します。

1. 自組織とインターネットとの境界では、次世代ファイアウォールによりアクセス制御を行い、必要な通信のみ許可します。さらに、公開 Web サーバなど、任意の第三者がアクセスする場合には、侵入防止システム（以降 IPS）を導入して攻撃から防御します。

2. 自組織と他組織との境界（例：自社とグループ会社）でも、次世代ファイアウォール[20]によりアクセス制御を行い、必要な通信のみ許可します。他組織のネットワークが信用できない場合は、IPS を導入して攻撃から防御します。

また、このような防御システムはシステム内に侵入したウイルスの活動を発見できる役割を負わせることも出来るため（むしろその役割のほうが有効であるため）運用できるならば試してほしい対策である。

外部記録媒体経由での攻撃

ウイルスの感染は、大半がネットワーク経由で行われますが、稀に USB メモリや DVD 等の外部記録媒体経由でも行われます。

1. 信頼できない人物や方法（例：拾った USB メモリ）によって入手した外部記録媒体に保存されたウイルスなどを実行しないように、DVD 等のメディアの自動再生を無効にし、USB などのデバイスについては認められたデバイスのみ接続を許可するように設定もしくは製品を導入します。

2. 信頼できない機器や人物に信頼している媒体を渡さないようにします。

システム管理者パソコンの保護

[20]従来のファイアウォール機能に加え、アプリケーションレベルでのセキュリティ機能が充実している製品

攻撃の多くはシステム管理者のパソコンが侵害されています。組織のシステム全体の管理権限を持つシステム管理者のパソコンが侵害されるとパスワード管理表やパソコン管理表などの重要な情報も攻撃者の手に渡ってしまうことになります。組織のシステムを防御する上でシステム管理者のパソコンの保護は欠かせません。しかし、多くの被害現場ではシステム管理者のパソコンの保護が十分ではありません。システム管理者のパソコンが上述したようなメールや Web 経由でウイルスに感染し、システムの重要情報が盗まれています。

システム管理者のパソコンを保護するために以下の対策が重要です。

1. システム管理者のパソコンはシステム管理専用のパソコンを用意し、システム管理者としての技術情報収集などのパソコンとは分離し、当然のことながら社員や職員の通常の業務パソコンと分離する

2. システム管理用のパソコンではインターネット閲覧や組織外部とのメール送受信をできるだけ避ける

3. システム管理用のパソコンは管理専用のネットワークを用意し、業務ネットワークと分離し、アクセス制御を実施する

ウイルス感染しても、被害を広げないための対策

ウイルスに感染すると、外部の指令サーバに接続を試み、接続に成功すると指令サーバから送られた命令を実行します。指令サーバとの接続は、一般的には HTTP[21]もしくは HTTPS[22]が使われますが、稀にその他の通信が使用されます。そのため、まず自組織からインターネットに出て行く通信を必要な通信に限定します。特に、HTTP および HTTPS については、必ず自組織のプロキシ[23]経由でのアクセスに限定し、プロキシ経由以外の HTTP および HTTPS についてはファイアウォールで拒否します。以下は一例です。

- パソコンからインターネットへの通信は全てファイアウォールで拒否する。
- HTTP および HTTPS は、自組織のプロキシ経由のみファイアウォールで許可する。
- DNS は、自組織内の DNS サーバ経由のみファイアウォールで許可する。
- SMTP は、自組織内の SMTP サーバ経由のみファイアウォールで許可する。メール送信を許可するクライアントは、SMTP サーバで制限をする。
- FTP や SSH は、自組織のゲートウェイ経由のみファイアウォールで許可する。FTP や SSH を許可するクライアントは、ゲートウェイで制限をする。

プロキシもしくは Web 用のウイルス対策製品では、URL フィルタリングにより不正なサイトへの

[21]Web システムで利用される通信の手続き方法が規定されたもの

[22]上の Web システムで利用される通信規定を、暗号化するために規定されたもの

[23]代理サーバのことで、ブラウザからの要求を一旦受け取り、ブラウザの代わりにサーバにアクセスする仕組み。

アクセスのほか、Flash Player など特定の（脆弱性があり危険なソフトウェアで閲覧する）コンテンツをブロックします。また、前述したようにホワイトリストによるアクセス制御を行う場合には、URL フィルタリングの機能を用いて、許可したドメインのみアクセスを許可します。

プロキシでは、利用者認証を導入することで、利用者認証を行わないウイルスが指令サーバに接続できないようにします。ただし、パソコンから認証情報を盗んで、プロキシで利用者認証を行った上で、プロキシ経由で指令サーバと接続することも可能である点に注意してください。

ウイルスに感染し、指令サーバへの接続に成功すると、感染の拡大や権限の昇格・奪取が行われます。特に、Active Directory が導入されている場合には、Active Directory のドメイン管理者権限が狙われます。そのため、ドメインコントローラーには、特に最新のセキュリティ更新プログラムを適用してください。その他のパソコンやサーバに対しても同様で、最新のセキュリティ更新プログラムを適用してください。

ウイルスに感染したパソコンから他のパソコンに感染することを防止するために、使用者のパソコン同士の通信を制御することが重要です。従来のシステム設計では使用者のパソコン同士の通信を制御する思想が含まれておらず、多くのシステムではそのような設計になっていません。しかし、多くの標的型攻撃の事案では多数のパソコンがウイルスに感染しており、被害を受けたすべてのパソコンの調査を実施することができず、被害範囲を特定することが難しくなっています。被害拡大防止の観点でも使用者のパソコン同士の通信を Windows ファイアウォールや L2 スイッチなどで制限することを検討するべきです。使用者のパソコンとサーバ、使用者のパソコンと複合機は通信ができる必要がありますので、システムに必要な要件を検討して実施してください。

2.5. 被害発生の検知策の実装

標的型攻撃では、最初のターゲットを遠隔操作型のウイルス[24]に感染させ、他のホストやサーバへの感染および権限奪取を行い、最終的には機密情報の漏洩など、企業・組織に多大な被害を与えます。ウイルスの感染を完全に防ぐことは困難ですが、ウイルスの侵入と感染をできる限り早く検知することで、被害の影響を抑えることができます。逆を言えば、検知が遅くなればなるほど、被害は甚大になります。

本項においては、代表的な対策として知られる手段の概要をまとめます。検知策は多岐にわたりますので、今後の改訂により網羅性を高め、詳細な対策法を整理してまいります。

ウイルスの侵入および感染をいち早く検知するためには、侵入経路として最も多いメールおよび Web 経由でのウイルスを検知する仕組みを導入します。このとき、それぞれの侵入経路に対して、できる限り多層的な対策を実施します。

メール・Web の侵入検知

ウイルス対策機能を備えたゲートウェイによりウイルスを検知・駆除します。これらの製品は、未知のウイルスには無力ですが、既知のウイルスには有効に機能します。

未知のウイルスに対しては、サンドボックス型のウイルス対策製品を使用します。これらの製品は、メールや Web で疑わしいファイルを受信・ダウンロードすると、サンドボックスと呼ばれる仮想 OS の上でファイルを実行させ、プログラムの動作からウイルスの判定を行い、ウイルスを検知・駆除することができます。

ホストの侵入検知

メールや Web などの経路で侵入したウイルスは、対象のホストにファイルがダウンロードされ、ユーザーによって実行するか、脆弱性により自動的に実行されることで感染します。そのため、ファイルがダウンロードされた時、もしくはファイルを実行した時に検知・防御するために、ホストにウイルス対策製品を導入します。

さらにウイルス対策ベンダーとの間で、検体を提供することで迅速にパターンの提供を受けることができるサービスを別途契約します。これらの製品は、未知のウイルスには無力ですが、ウイルス対策製品で検知しないウイルスが侵入してしまった場合でも、検体を提供することで迅速にパターンが提供され、万が一組織内にウイルスが蔓延してしまっても、作成されたパターンを更新することで、ウイルスの検出・駆除を行うことができます。

[24]攻撃のためのツールや自己増殖しない不正なプログラムをマルウェアといいますが、本文書ではウイルスとひとまとめにしています。

未知のウイルス、ゼロデイ脆弱性を突くウイルスに対しては、振る舞い型のウイルス対策製品を導入して検知・防御します。

感染の検知

どんなにウイルス対策を行っても、組織内でのウイルス感染を完全には防ぐことはできません。また、脆弱性や人の関与がある以上、ウイルスが実行されて感染することを防ぎきることはできません。

そのため、ウイルスに感染した際、それにいち早く気づくための検知が必要です。前章で説明したように、自組織から出て行く通信は必要な通信に限定されていることを確認します。その上で、自組織から出て行く通信のログは、許可および拒否したものを含め、全て記録します。標的型攻撃を受けると、長い場合は数年間にわたり不正行為が継続し、その間は外部の指令サーバへの接続が続くなど、何らかの痕跡がログに残るため、追跡に必要なログおよび被害範囲の確認に必要なログを最低でも 1 年間程度保持します。以下は感染を検知する取り組みの例です。

自組織から出て行く通信はファイアウォールでログを残す（許可および拒否）。

- HTTP および HTTPS はプロキシでログを残す（ログの項目は、可能な限り多くとる）。
- SMTP によるメールの送信および受信は、メール本体を含めて全てログを残す（メールのアーカイブを保存する）。
- FTP や SSH などを使用する場合は、ゲートウェイを経由して、送信したファイルやコマンドのログを残す。

指令サーバとの通信は HTTP もしくは HTTPS で行われることが多いため、プロキシサーバのログを定期的に分析し、指令サーバへの通信が発生していないか確認します。

また、ウイルス対策製品や次世代ファイアウォールでは、指令サーバへの通信を検知することができる製品があります。これらの製品を導入して監視を行うことで、指令サーバへの通信を検知した場合は即座に対象のホストを隔離するなど、被害を最小限に抑えることができます。

基本的に指令サーバへの通信を検知した、或いは外部組織から感染連絡により当該通信元を隔離し、当該 PC からの他の不審通信の分析、取り出したウイルスの解析により判明する他の指令サーバ情報の取得により、さらに別の感染 PC 有無を確認しそれを繰り返すことで外部と交信している PC を可能な限り見つけていきます。また、同時に当該パソコンからの他のパソコンやサーバへの不正アクセスを、例えば AT コマンドなどの行使痕跡などにより調査し影響範囲を調査します。

その他のログ

指令サーバへの通信を検知した場合、発信元のホストを迅速に特定して隔離する必要があ

ります。このとき、プロキシやウイルス対策製品のログには、通信の送信元 IP アドレスが記録されます。送信元 IP アドレスからホストを特定する際に、組織内で DHCP を使用していると、IP アドレスからホストの特定ができない場合があります。

そのため、DHCPを使用している場合は、IPアドレスとホスト名などを紐付けるため、DHCPサーバのログが記録されており、最低でも 1 年間のログが残っていることを確認します。送信元 IP アドレスからホストを特定できるのであれば、資産管理ソフトウェアのログなどでも問題ありません。

重要サーバのログ

標的型攻撃では、最初のターゲットがウイルスに感染した後、組織内で Active Directory を使用していた場合は、Active Directory のドメイン管理者権限が狙われます。そのため、Active Directory の監査ログが記録されており、最低でも 1 年間のログが残っていることを確認します。

また、可能であれば監査ログを定期的に分析し、不正なアクセスが発生していないか確認します。

サーバ時刻を合わせる

事故対応時には複数のサーバのログの関連性を相関分析するため、各サーバの時刻を同期しておきます。

2.6. ダメージコントロールと被害の対処への備え

標的型攻撃により組織内ネットワークが侵害された場合、まずは被害拡大を防ぐと共に被害範囲の確認と復旧を行うことになります。以下、組織内における基本的な初動対応について概要を説明します。

なお、具体的な実施方法は、本資料改訂版において増補する予定です。

通信の制限・遮断

組織内の被害範囲をこれ以上拡大させないため、組織内からのインターネットへの接続を制限します。

攻撃者グループは、インターネット上に配置した複数の攻撃拠点となる拠点サーバと、組織内に侵入したプログラムとを通信させることで様々な悪意ある操作を遠隔から行っています。

攻撃者グループの指令サーバへの通信を遮断する

すでに判明している指令サーバ、または不審な通信先と考えられるサーバとの通信を、インターネットとの境界部分で遮断します。一般的にはファイアウォールとプロキシサーバの両方でインターネットとの通信を遮断します。抜け道があり、遮断が効いていない経路が無いかも確認します。

組織外部からの連絡内容から、すでに個人情報が漏洩している、組織内に広く・深く侵入されているなど、被害状況が深刻なケースでは、部分的な通信遮断ではなくインターネットとの接続を完全に遮断することで更なる被害拡大を防ぎます。その場合、事業への影響を事前に見積もっておき最小となるような、遮断可能時間やホワイトリストの定義等を行っておくと同時に、誰がどのような判断で実施するか実際に影響は見積もり範囲か、遮断によってあぶりだすことが可能な他の感染パソコンの特定等の訓練を行っておくことが望ましい。

電子メールの制限

Web へのアクセスを遮断するだけでなく、電子メールなどについても遮断を検討する必要があります。

昨今の標的型攻撃では、メールサーバに関連した認証情報が盗まれ、（被害者に）成りすました電子メールを送る、内部情報を電子メールで外部の攻撃者グループへ送る、といったことが行われる可能性もあるため、Web 以外の通信についても送信遮断を確認してください。その場合、当然のことながら最低限の連絡に必要な経路は事前に考慮しておくべきです。

被害状況を確認するのに必要な情報（準備）

組織内の被害状況を確認するには各種ログの調査が必要になります。被害範囲や原因を調査する前に、必要なログが消えてしまわないように確保します。

被害機器の隔離

攻撃者グループの指令サーバと通信を行っていた機器を特定・隔離するため、プロキシサーバのログを確認します。

すでに判明している指令サーバのアドレスと通信を行っていた機器をプロキシログから特定し、該当機器はネットワークから隔離します。

アカウントパスワードの変更

侵害された機器で利用していたアカウントのパスワードは全て変更します。

OS のログオンパスワードだけでなく、電子メールソフトや Web ブラウザなどで保存していたアカウント情報やパスワードについても変更を行います。特に VPN などを利用するためのパスワードを保存しているケースでは、それらのパスワードも変更が必要です。

被害機器のコピー（証拠の保全）

侵害された機器は、まずネットワークから隔離し、ウイルススキャン等の処置をする前に、完全なコピーを取得し、調査はコピーに対して実施します。

被害機器（コピー）に対するウイルス対策ソフトによるスキャン

調査対象の機器に、ウイルスが存在しているかを確認します。ウイルスが存在するディレクトリなどが特定できていない場合には、コピーに対して複数のウイルス対策ソフトによるスキャンを実施し、ウイルスが存在するか確認します。この場合、いつも使用しているウイルス対策ソフト以外の検知率の高いソフトをセカンドオピニオンとして利用することも効果的です。

ウイルス対策ソフト以外の検出方法

自動実行に登録されているプログラムが正規のアプリケーションであるかを確認します。マイクロソフト社が提供する AutoRuns ツールなどを利用することで、自動起動に登録されているファイルを確認し、正規ファイルであるかを判断します。

ウイルスの取り扱い

自組織で利用しているウイルス対策ソフトでは検知できず、それ以外のウイルス対策ソフトでウイルスを検出できる場合があります。その場合、特定できたウイルスを確保し、自組織で利用しているウイルス対策ソフトベンダへ提供しパターン作成を依頼します。

ウイルスの通信先確認

侵入したウイルスの特定はできているものの、通信先である指令サーバのアドレスが判明していない場合は、ウイルスが通信を行う指令サーバのアドレスを確認します。

情報漏えいの確認

被害機器を特定できた後、事前に確保したコピーを利用して攻撃者グループによる情報の持

ち出しがなかったかを確認します。基本的には遠隔操作された PC やそこから不正操作された PC はフォレンジック調査を行い攻撃者が組織内から集めたファイルの残骸等を探し、被害内容を推測します。

業者への調査依頼

標的型攻撃に対する対応は、組織内だけでは困難なケースがあります。専門業者を利用することで、一般的に次の作業について協力を依頼することができます。

1. インシデントのハンドリング（初動対応の指示）
2. 被害機器のコピー作成（証拠保全：イメージ取得）
3. プロキシサーバのログ調査
4. 被害を受けた機器の詳細なデジタル・フォレンジック調査（原因・影響範囲）
5. ウイルスの解析（通信先の特定など）
6. 監視機器の緊急設置

監視機器の臨時設置

一般的な IDS（侵入検知システム）とは別に、標的型攻撃に特化した監視装置を（一時的にでも）設置し、一定期間監視する方法もあります。

報道発表の判断

標的型攻撃により、個人情報の漏洩が明確になっている場合などは、広報・法務部門などが協力し、記者会見およびプレスリリースについて検討します。

また、平行して警察にも相談し、捜査に必要となる協力を行っていきます。プレスリリースを出す際は、正確に情報提供する必要があります。しかし、発表時点では調査中の箇所も多くなることから、過去の他企業の事例などを参照しつつ、継続的な対応を行っていきます。

2.7. 被害からの復旧手段の確保

標的型攻撃により侵害された機器を特定できた場合には、それらの機器の復旧処理を行います。（後から調査可能なように必要なデータのコピーを取得してから復旧します）

また、組織内ネットワーク全体についても安全を確認し、潜伏しているウイルスが存在しないかを確認します。

復旧のポイント

組織内ネットワーク全体に関する復旧に向けた確認ポイントは次の 3 点です。

1. 組織内ネットワークにウイルスが残っておらず、指令サーバとの通信が無いことを確認する。
2. 正規アカウントの認証情報を悪用し、ウイルス以外の方法（例 VPN など正規のログイン方法）で組織内ネットワークへ侵入されていないことを確認する。
3. 外部でホスティングしているサーバ（例 Web サーバ、メールサーバ等）に、脆弱性が無いか、正規アカウントの認証情報を悪用したアクセスが無いことを確認する。

OS の再インストール

侵害された機器はディスクのフォーマットと OS の再インストールを行い初期化します。

アプリケーションを最新の状態へ

利用するアプリケーションについても、脆弱性が無い最新バージョンへのアップグレードを行います。

データの復元

侵害された機器の記憶装置を初期化した上で OS を再インストールした後、バックアップからデータをリストアします。この際、再びウイルスがリストア[25]されてしまうことが無いように、復元するデータについては複数種類のウイルス対策ソフトによるスキャンを実施します。

侵害原因への対処

標的型攻撃による侵入経路・原因を特定します。侵入経路や原因が明確ではない場合、再度の攻撃を防ぐことができず、同様の被害が発生する可能性があります。

侵害原因となる箇所の対処

標的型攻撃による侵入経路の一つとして、自組織の Web サーバや関連組織の Web サー

[25]情報を元の状態に戻すことです。通常は機器の故障からの復旧時に行いますが、ウイルスは自己を再感染させるために行います。

バを改ざんし、ウイルスを送り込むケースがあります。
　これらの Web サーバに脆弱性が無いか、コンテンツ改ざんやウイルスが置かれていないかを確認します。

継続的な不審ログオンの監視

　侵害された機器で利用していたアカウントについては、パスワード情報の変更後も一定期間は不審なログオンが無いかをセキュリティログなどで監視します。

ネットワーク通信の監視と確認

　復旧を行ってから一定期間後、安全性を確認するためにネットワーク上を流れるパケットをキャプチャし、不審な通信が発生していないかを確認します。
　また、プロキシログについても指令サーバとの通信を疑わせるログが無いかを確認します。

Active Directory の完全性を復旧する

　標的型攻撃によりドメインの管理者権限が奪われ、Active Directory サーバ（ドメインコントローラ）も含めドメイン全体が被害を受けているケースでは、Active Directory の再構築を含めて完全性を復旧する計画を立てる必要があります。

手順書・訓練への反映

　事案の収束が確認できた後、一連の対応について手順書の作成・改定を行います。
　標的型攻撃は日々変化するため、手順書の内容も定期的な見直しを行うと共に、手順書に記載されている内容に沿った作業が実施できるか、実地での訓練も定期的に実施します。

通信環境の復旧

「2.4.　被害拡大の防御策の実装」で通信やサーバなどの停止を行っていた場合、本項の回復作業を完了した時点で、通信を復旧させます。

事業の回復

　事業の回復を試みます。復旧された全ての機器を動作させ、事業責任者の確認の下、事業の再開を行います。

企業の信頼性の回復

　標的型攻撃による被害の内容を、警察の捜査などに影響が出ない範囲で可能な限り詳細な情報を公開し、真摯に事件と向き合っていることを知っていただく取り組みを行います。顧客の懸念を全て受け止め、真摯に正直に対応することにより、信頼を回復します。

2.8. 継続的に対策するための実施評価と予算措置

セキュリティ対策に限らず、継続的な取り組みを行う際には、計画、導入・運用、点検・評価、見直し・改善の順で管理する、いわゆる PDCA サイクルが重要とされています。情報処理推進機構(IPA)のサイトにおいても、PDCA サイクルに関して詳しく説明されています。

情報セキュリティマネジメントにおける点検・評価のステップでは、現在の対策技術や体制が、その時点で確認されている脅威に対して有効か否かを評価するものです。本書においては、標的型攻撃という、いつ攻撃が行われるかわからず、しかし対策を中断することができない脅威対策に関して、どのような指針を持って評価を行えば、対策を継続することができるかを整理します。

重要なことは、何を「評価」するか

ほぼ全ての企業や団体で年度毎に予算が組まれ、年度初めから活動の評価が始まることとおもいます。さて、一年の終わり、正確には翌年の予算を検討する際に、どのように該当年度の実施評価をされているでしょうか。導入時には、セキュリティ機器やサービスの導入メリットや運用の仕組みについて検討を繰り返されていることでしょうが、いざ評価の段階になると、何を評価すればよいのか判然としないという自体が見受けられます。

これは、評価の段階に至っても何を評価するのかが明確になっていないことが原因と考えられます。

一般に重要業績評価指標（KPI）を考えたとき、定量的な評価を連想します。一般の IT システムの場合には、導入したシステムをいかに使いこなしているかということは、投資対効果を計る上で有効なため、パフォーマンスやユーザーの利用率などの数値化された評価項目を設けます。

それでは、セキュリティ対策についてはどうでしょうか。当たり前ですが、セキュリティ対策機器が有効に使われるのは、攻撃行為があったときです。攻撃が行われない場合には、セキュリティ機器は反応をすることがありません。よって、一般的な IT システムのような KPI での判定は行いにくいのです。

セキュリティ機器を使い尽くすという視点で見たときには、その運用のありかたが評価の軸になると考えられます。

当社が運営しているセキュリティ監視センター「JSOC」は、850 社ものお客様の環境から 1 日あたり 8 億件を越えるイベントを収集し、独自の相関分析エンジン「LAC Falcon」にて、警戒が必要なイベントを 2000 件程度に絞込み、内部の情報を解析して脅威の判定を行っています。このような機器が発するメッセージを読み解き、自社環境でどのような攻撃があるのかを把握する運用のサービス品質保証を、評価ポイントとするべきです。機器の導入をして満足することなく、余すところなくその能力を活用し、活用した結果を分析することで、その対策が的確に機能しているかを判断します。

一方で、社員の情報セキュリティリテラシー教育や、「IT セキュリティ予防接種」のような標的型メール対策教育サービスの場合には、毎年避難訓練を行うように、定期的に訓練を行うことが重要になります。また、CSIRT の運営維持に関しても、事故に備えた組織対応として継続することが重要になります。

このように、組織の維持や継続的な教育といった取り組みの評価は、継続して実施をすることそのものを目標とした評価とします。

継続的に対策を行うということは、コストとの戦い

標的型攻撃との戦いは、IT システムを活用するうえで避けては通れない課題です。常に継続した対策を維持しなければなりません。しかしながら、IT システムを生産性の向上や売り上げの拡大に活用するのとは異なり、セキュリティ対策は、いつ発生するとも分からない事故と向き合う取り組みのため、とかくコストの面で疑問が出るものです。

標的型攻撃を含むセキュリティ対策は、実施することがすなわち目標であり評価の一つといえます。

継続して機器が発するアラートを分析する。教育を受ける。組織を維持するためのコストは、いつ起こるかわからない事故への「備え」であると考えてください。

2.9. 標的型攻撃を見越した人の教育

標的型攻撃の対策を考えるとき、標的にされる社員など組織を構成する「人」に対する教育は、大変重要です。セキュリティへの危機感を感じセキュリティ対策を進めることも、標的型メールからいつもと異なる「雰囲気」を感じ取るのも、すべて「人」が行うことです。社員や職員といった組織の全員が、セキュリティへの関心と知識を持つことが、ここまで説明してきた対策に必要となります。

ここでは、標的型攻撃対策における人の教育をいかにして進めるかを整理します。

社員はウイルスメールを見分けることはできるのか？

標的型攻撃においては、電子メールにウイルス感染の仕掛けを行うケースが多々見受けられます。その多くは、通常の業務や関連組織からの連絡などに見せかけた「なりすましメール」にウイルスを添付したり、ウイルス感染を引き起こす URL リンクを記載したりして送り付けてきます。社員がなりすましメールに直面した時、ウイルス感染を引き起こすメールであることを見抜き、感染を未然に防止したいと考える方もいらっしゃるでしょう。しかし、どんなに教育や訓練を行ったとしても、確実に見抜く、ということは不可能です。巧みに細工されたなりすましメールには、何段階かの難易度があります。業務に関連するように見せかけられた標的型メールの難易度は、以下のように考えます。

高難易度　ウイルスを使って実際の業務メールを盗み出し、流用している
本文や件名は過去に送受信された業務メールであり、見分けることは困難。
添付書類もゼロデイが使用されるなど見極めは不可能。

中難易度　業務に関連しているように見せかけたメールを攻撃者が作ったもの
IPA などの Web サイトにある記述をそのままコピーして利用したもの。
自分に関わりの無い内容が書かれていた場合は、見分けられる可能性がある。
セミナーの案内等見分けが難しいものもあるが、添付書類は安易な実行ファイルレベル。

低難易度　他国語が混じっていたり、日本語の「てにをは」がおかしいなどの特徴を持つもの
標的型攻撃に使われるなりすましメールの特徴をいくつか知っていれば、見分けられる可能性がある。

標的型メールではないもの
広告メールやフィッシングメールなど、不特定多数の人に送られたもの。
基本的なセキュリティリスクをいくつか知っていれば、見分けられる可能性がある。

真の意味で攻撃対象を「標的」とする高難易度のものを見分けることは、残念ながら不可能です。中難易度や低難易度の場合には、「自分に見覚えが無いメールである」、「論理的に自分に送られてくることがおかしい」、「メールの書き方が社内文化と違う」といった点に気づくこともあります。しかし、どんな組織であっても、ウイルスの開封率をゼロにすることは困難であり、ヒューマ

ンエラーが発生する一定の割合を下回ることはできないと考えます。違和感に気づくための知識を持っていても、急いでいたり、疲労がたまっていたり、一定の期間が経ってウイルスのリスクが薄れたりすることで、うっかりウイルス感染の仕組みに引っかかってしまうからです。定期的な教育は、このような観点から実施されます。

一方で、低難易度のなりすましメールや標的型ではないウイルスメールについて、多くの社員が高確率で感染してしまう場合、社員への教育による知識と意識の底上げが必要です。
「ウイルス対策ソフトが正しく動作していれば全てのウイルスは駆除できる」などの現実と乖離した認識が広まっていると、自分に届いたメールに注意を払うという行動には結びつきません。また、自社の社員がどのレベルのメールを見分けることができるのか、情報システムリテラシーはどの程度であるのかを知るために、疑似ウイルスメールを送付し、開封率を測るのも一つの策として挙げられます。どのレベルのメールを見分けることができるのか、どのくらいの割合で感染してしまうのかを知ることで、その後の教育方針などを明確にすることができます。

ウイルス感染発生時には、社員が気づいたときの報告や連絡、相談などを適切に行うことは重要です。社員への定期教育により正しい知識と行動方法を伝え、疑似ウイルスメールの送付によって、上長や適切な部署への報告、連絡を実施できるかどうかを定期的に確認することができます。

社員への教育や疑似ウイルスの送付に関して注意すべきことがあります。これらの策を実施した際に、「今後感染したら罰則だ」と伝えてしまったり、疑似ウイルスを開封したことを強く非難してしまったりすると、かえってセキュリティ対策上マイナスに働きます。その場合、不審なメールの定義を組織のレベルに応じて具体的に取り決め、そのレベルに応じて継続的に教育訓練を行い、罰則があることを事前に伝えそのうえで、守れない場合は何らかの手段を講じるのが良いでしょう。かねてより発生している日本国内のウイルス感染事例を見ると、一部の組織においては、組織内からの通報、連絡をトリガーに事故対応を始めているケースがあります。高難易度のなりすましメールを使われた際には、社員が気づくことは非常に困難ですが、中難易度以下のなりすましメールやそれらレベルのメールに添付されたウイルスの場合には、社員による報告が可能なこともあるでしょう。もし、ウイルス感染したことを非難していたり、ウイルス感染したこと全てを始末書扱いにしていたりするような場合、社員がウイルス感染の事実に気づいたとしても、隠ぺいしてしまう可能性があります。組織としては、「ウイルス感染」ではなく「ウイルス感染による被害」を防ぐ必要があり、初動対応は被害を最小限に食い止めるための重要なポイントとなります。

コスト面から出口対策などのネットワークの監視による検知策を行っていない場合、社員からの通報は検知のための重要な要素となります。組織としては、如何にして社員が気づいたこと、発見したこと、違和感があったことを報告してもらうかを考えなければいけません。疑似ウイルスの送付という策を、組織を管理する側として開封率の把握を目的に実施するのは良い方法ですが、感染した社員を強く非難するような事後対応が行われることは避けなければなりません。ま

た、ウイルス感染を 0%にするための策として実施するなどは、言語道断です。不可能な目標を目指していることに加え、仮に 0%を達成できたとしても、本物のウイルスに直面し、社員が感染してしまった場合、感染の疑いがあることに気づいていても社員が隠ぺいしてしまうことが想定されます。これらの誤った策は、「ウイルス感染」という組織上のリスクのほんの一部分だけにフォーカスしてしまっていることが原因の一つと考えられます。組織全体のリスクとして捉えるべきであり、セキュリティガバナンスに基づくリスク管理の中でウイルス感染と感染に関連する事故対応のフローや体制を整えなければなりません。

ウイルス感染というと、普段めったに起きない事故が起きたという印象を持つかもしれませんが、組織のリスクを管理する立場としては、実際にはより身近なところで、頻繁に起きていると考える必要があります。事実、昨今のウイルス感染による被害の報道を見ると、感染したのは半年前であったり、3 か月前であったりという事実が後になって判明したケースが多く見られます。単に見えていなかっただけの可能性があるのです。事故が起きない＝良いセキュリティ、良い策、ではなく、事故が起きても被害が出ない、そして被害を最小限に食い止めることができるのが良いセキュリティ対策であるといえます。逆にセキュリティ対策が向上するとウイルス感染の事実がより発見されることになり、感染件数は増大すると考えて推進するくらいが丁度良いでしょう。

ウイルス感染率と被害発生の関連性は？

電子メールの添付ファイルを開封したことを起因としたインシデントを想定した場合、開封率を下げることができれば被害を食い止められるのかという疑問については、攻撃が行われる目的や意図によって変化するといえます。

まず、単純な被害をもたらす従来のウイルス（後述の標的型と対比してあえてこう表現します。）の場合です。ウイルスは社内ネットワークを通して他のパソコンに感染を広げ、ウイルスの機能によって様々な被害をもたらします。例えば、ウイルス感染したパソコンを拠点に、さらにウイルスメールを送信するなどです。対処としては、感染したパソコンの特定とウイルス駆除、そしてウイルスの種類によってもたらされる被害に合わせて社内対応や対外対応を行います。対外対応の例としては、ウイルス付きのメールが関連企業やお客様に送付された時は、ウイルスメールへの注意を促す連絡を行ったり、情報が漏えいした時は関連する人々や組織への謝罪、二次被害の注意喚起などを行ったりします。その他、感染したパソコンに対しては、OS を再インストールする対応を行ったり、データが消失した場合には、データ復旧の対応を行ったりする必要があります。これらの単純な被害をもたらす従来のウイルスにおいては、ウイルスの種類にもよりますが、感染するパソコンの数がより少ない方が被害は小さくなり、感染率の低下が比較的顕著に効果として現れる可能性があります。もちろん、社内の 1 台のパソコンを起点に、社内ネットワークを通してウイルス拡散がなされる場合には、1 つの侵入口を起点に多数の感染をもたらすため、見方によっては 1 台でも感染すれば大きな被害がでるという見方もできます。ただし、ウイルスが社内ネットワークにおいて感染を広げる原因としては、パソコンのぜい弱性を利用されるケースが多く、パソコンの OS のアップデートや、インストールしているソフトウェアのアップデートを行っていない

場合に発生します。セキュリティ対策として、パソコンの OS やソフトウェアのアップデートは基本であり、ウイルス感染を食い止める対策の一つとして実施すべきことです。仮に 1 台が感染したとしても、アップデートが適切に行われ、さらにウイルス対策ソフトを適切に利用していれば、社内での感染拡大は最小限に食い止められると考えられます。

次に、標的型攻撃の場合です。巧みに作り出されたなりすましメールを送り付けられ、ウイルス感染が発生してしまった場合、その 1 台のパソコンを起点に、攻撃者の人手による遠隔操作により、社内ネットワークの分析や社内パソコン、サーバへのさらなる攻撃などが行われます。このとき、最初のウイルス感染するパソコンは、多くの台数である必要はなく、たとえ 1 台でも感染すればパソコンを遠隔操作することができ、攻撃者は内部での活動が可能となります。標的型攻撃においては、ウイルスの添付ファイルを開封する人数が少なかったとしても、極論を言えば 1 人でも感染してしまうと被害が発生する可能性があります。従来の単純な被害をもたらすウイルスとの大きな違いはこの点にあります。従来のウイルス被害は、より多くのパソコンに感染させることが攻撃者にとっての攻撃の成功ですが、標的型攻撃においては、1 台のパソコンでも良いのでウイルス感染を発生させることができれば、あとは見つからないように延々と攻撃活動を続けられることが、攻撃者にとっての成功と言えます。もちろん、社内ネットワークの構造が複雑な場合、複数のパソコンを遠隔操作できた方が、攻撃者はより攻撃の幅が広がる場合もあります。例えば、特定の部署の 1 台のパソコンにウイルスを感染させることに成功したとしても、組織が行っていたネットワークのアクセス制限により、遠隔操作で分析できる範囲のネットワーク内には目的となる機密情報が無いなどの結果に終わった場合は、また別のパソコン上でウイルス感染を引き起こす必要があります。ただし、その場合においても、1 台のパソコンを遠隔操作することができれば、パソコン上に保存されている過去の電子メールを入手し、それらしいファイル名を付けたウイルスを添付して、遠隔操作しているパソコン上からより高難易度のなりすましメールを社員に向けて送信することができてしまうのです。

標的型攻撃に備えた教育手法

これらのことから、私たちは多くのことを学ぶことができます。標的型攻撃は、手法としてウイルスは使われるものの、従来の単純な被害をもたらすウイルスとは、リスクの種類や傾向が大きく異なることを知る必要があります。その上で、組織としてどのような対策をすべきかを考え、管理する必要があります。従来のウイルスに対しては、パソコンのアップデートやウイルス対策ソフトの利用、exe ファイルに注意するなどの注意喚起が中心でした。社内システムを管理する部門としては、感染が発生した時はパソコンを隔離し、感染パソコンへの対処を行えばよかったのです。これらの対策は、情報システム部門や総務部門主導での社内対策でも十分通用しました。しかし、標的型攻撃に対しては、経営層が中心となって、組織におけるリスクの一つとして捉え、そのリスクへの対策として社内のセキュリティ対策を遂行しなければなりません。さらに、それら経営リスクへの対策が、今現在、組織内で適切に行われているかどうか、時間の経過とともに浮き彫りとなった新たなリスクに対応しているかどうか、システム対策の対応状況はどうか、などを見直す必要があります。これらの考え方はすなわち、情報セキュリティガバナンスに基づいて、セキュリティ対

策のサイクルを適切に回すことに他ならないのです。

その観点から、社内におけるセキュリティ対策を進めます。例えば、疑似ウイルスメールを社員に送付することで、社員はどの程度の知識、スキルを持っているのかの計測や、ウイルスに気づいたときに適切に行動できるのかどうかを知ることができます。疑似ウイルスメールを送付するなどした訓練により感染率 0%を目指したり、開封した人をむやみに非難したりする等の誤った目的で行ってはいけません。

自組織の社員の傾向に基づいて、社員教育を行います。社員教育においては、中難易度や低難易度、標的型ではない不特定多数の人に送りつけられるウイルスについては、メールや添付ファイルに特徴があることを伝え、見分けるためのコツを伝えます。さらに、高難易度のウイルスメールがあることを知り、それらを見分けることは困難であるが、もしも感染に気付くことができた場合には、速やかに報告することが最も適切な対応であることを伝えます。

これらの対策を妨げる社内ポリシーがあった場合、改定するなどの検討を行います。例えば、ウイルス対策ソフトがアラートを上げただけで始末書を提出しなければならない、事後対処が適切で被害は出なかったにもかかわらず、ウイルス感染を引き起こしただけで厳しい社内指導などが行われる、などのルールがある時には見直しを検討します。

その他、ウイルスに感染した時の事後対処を行う、情報システム部門などの担当者の体制や担当者における意識などを見直すことも必要です。ウイルス感染が発生した際に対処を行う部署において、従来の単純なウイルス被害をもたらすリスクをベースに、社内の仕組みやルール、体制を構築している場合、標的型攻撃に対しては適切に事後対処を行えない可能性があります。標的型攻撃への対応を行う場合、従来のリスクの観点から整えた情報システム部門だけでは人員が不足する可能性もあります。また、より高いリスク管理能力や、組織全体のリスクを考慮した事故対応が求められるでしょう。情報システム部門の体制の見直しに加え、情報セキュリティのリスクに対応するための体制を整えることも検討しなければなりません。例えば、経営層も参加する情報セキュリティ委員会や、情報セキュリティ事故が起きた時の司令塔となる CSIRT（Computer Security Incident Response Team、シーサート）体制の整備などです。CSIRT の役割に合わせて、情報セキュリティに関連する情報収集や、他の CSIRT との情報交換、パソコンの分析業務も行う場合には、分析技術を持つ専門の部隊を CSIRT 内に参加させ、デジタル・フォレンジック技術やウイルスに関連する知識をつけさせることが必要となります。標的型攻撃において、経営層、情報システム部門、CSIRT、社員、それぞれがどのような役割、位置づけ、立ち位置となるのかを考え、目的に合わせてセキュリティ教育を実施しなければなりません。

リスクの捉え方とコストバランス

標的型攻撃への対策を考える時、単純な「ウイルス対策」として捉えてしまうと、対策手段に

行き詰ってしまったり、コストとの折り合いがつかなくなってしまったりすることがあります。例えば、標的型攻撃やウイルス感染への対策として「出口対策」というものが挙げられますが、出口の監視となると侵入防御システムや次世代ファイアウォールなどの導入が必要となります。規模の大きな組織では、十分な対策も検討できますが、中小企業で初期費用やランニングコストが大きくかかる対策を実施することは大変な負担となるでしょう。その際、これ以上の対策は実施できないという結論に至ってしまうことは大変危険です。

コストの面から実施が困難である、あるいは、実施できそうな対策が見当たらないという時は、一度視点を変えてみることをお勧めします。「ウイルス」というキーワードから離れ、組織全体を「セキュリティリスク」という広い視点で見直します。標的型攻撃においては、攻撃者は組織が持つ情報を狙い、それらを盗み出していると考えられます。防御側としても、セキュリティ対策におけるアプローチを変え、「ウイルス感染しても情報が漏れない」というシチュエーションを作り出したり、サーバのログなどからそれを証明したりすることができれば、何らかの理由で事故を公表しなければならない時も企業リスクを最小限に食い止めることができます。自組織において、情報セキュリティ上守るべき情報は何かを今一度見直してみましょう。また、日常の業務において、守るべき情報はどのような形で保管され、どのような場所で利用されているかを再確認しましょう。重要な情報ほど、日常の業務では頻繁に利用していることもあります。アクセス制御のかかったサーバや、施錠棚に保管しているつもりが、そのコピーが社員のパソコン上に残っていたり、持ち出し用の USB メモリの中に残っていたりするかもしれません。ウイルス感染した場合、どのような被害が発生するのかを考えてみましょう。どのような経路で守るべき情報に行きつくのか、どこに情報が残っていると被害が大きくなるのかなどを攻撃者の視点から、シナリオベースで考えてみることをお勧めします。

まとめ

本書でまとめた標的型攻撃への対策については、定番として認知されているものから、ある意味荒唐無稽ともいえる対策まで広く取り上げました。一般的な情報セキュリティ対策情報の枠を超えて対策の提案を行った理由は、標的型攻撃がこれまでの常識を超えた狡猾な攻撃方法であり、私たちの知見もまだまだ十分なレベルに至っていないと考えたためです。

これまでになかった範囲と深さの対策方法を必要とする。それが「標的型攻撃の対策」です。

冒頭に記しましたが、本書は継続的に更新を受け、より高い精度と取り上げる対策領域を広げてまいります。

以上