JPCERT CC®

「標的型攻撃について」

有限責任中間法人 JPCERT コーディネーションセンター

平成 20 年 9 月 17 日（第二版）

JPCERT CC®

改訂履歴

	変更内容	日付
初版		2007 年 6 月 21 日
二版	変更箇所　8 ページ「不祥事への対応について」 変更前　　製造：1 件、情報通信 1 件 変更後　　製造：1 件、情報通信 2 件	2008 年 9 月 17 日

JPCERT/CC®

目次

1. はじめに

目的

本文書では、近年急増していると言われる標的型攻撃(Targeted Attack)について、まず攻撃の定義を試みる(3 章)。次に JPCERT コーディネーションセンター(以下、JPCERT/CC)が行った国内企業へのアンケートから標的型攻撃に関する実情を紹介する。そして最後にそれら攻撃に対して企業・組織が取り得る対策について紹介する。

想定する読者

企業・組織の情報セキュリティ担当者

定義

本調査では、標的型攻撃を以下のように定義している。

> 情報セキュリティ上の攻撃で、無差別に攻撃が行われるものでなく、特定の組織あるいはグループを標的としたもの。攻撃対象となる組織あるいはグループに特化した工夫が行われることもある。

“標的型攻撃”の呼び名について

”Targeted Attack”という言葉は標的攻撃、スピア型攻撃、スピアー攻撃、ターゲットアタックなど様々に翻訳されている。本文書では”標的型攻撃”という訳語を用いる。この表現が比較的定着しており、初見でも漢字から内容を類推することが容易と思われるからである。

2. 要旨

1. 特定の組織あるいは組織グループを標的とした、情報セキュリティ上の攻撃を標的型攻撃と呼ぶ。攻撃対象が限定されているため、各組織が自律的に検知し対策を実施する必要がある。
2. 2006 年には国内組織に向けて日本語ワープロソフトのゼロデイ脆弱性を利用するマルウェアが使用されるなど、日本国内の組織を標的とする攻撃の増加が見受けられる。
3. アンケート調査の結果、製造業やマスコミなども標的型攻撃のメールを受け取った経験があると回答しており、標的となるのは官公庁に限らない。
4. 今回の調査では民間企業を狙う標的型攻撃の存在、及びその増減を把握する事を目標とした。被害の詳細や手口についてはさらなる調査が必要である。
5. 検知しにくい標的型攻撃からの自衛のために、そして攻撃の全容を把握するために相互理解と信頼に基づく情報共有体制が必要である。

3. 標的型攻撃の具体例

今回の調査では、標的型攻撃を以下のように定義した。

> 情報セキュリティ上の攻撃で、無差別に攻撃が行われるものでなく、特定の組織あるいはグループを標的としたもの。攻撃対象となる組織あるいはグループに特化した工夫が行われることもある。

この章では実例やモデルケースを交えて、この定義にあてはまる攻撃について説明する。なお、事務所荒らし・ゴミ箱漁りなど、攻撃に情報システムを必要としない攻撃についてはここでは考慮にいれない。

標的型攻撃の種類について

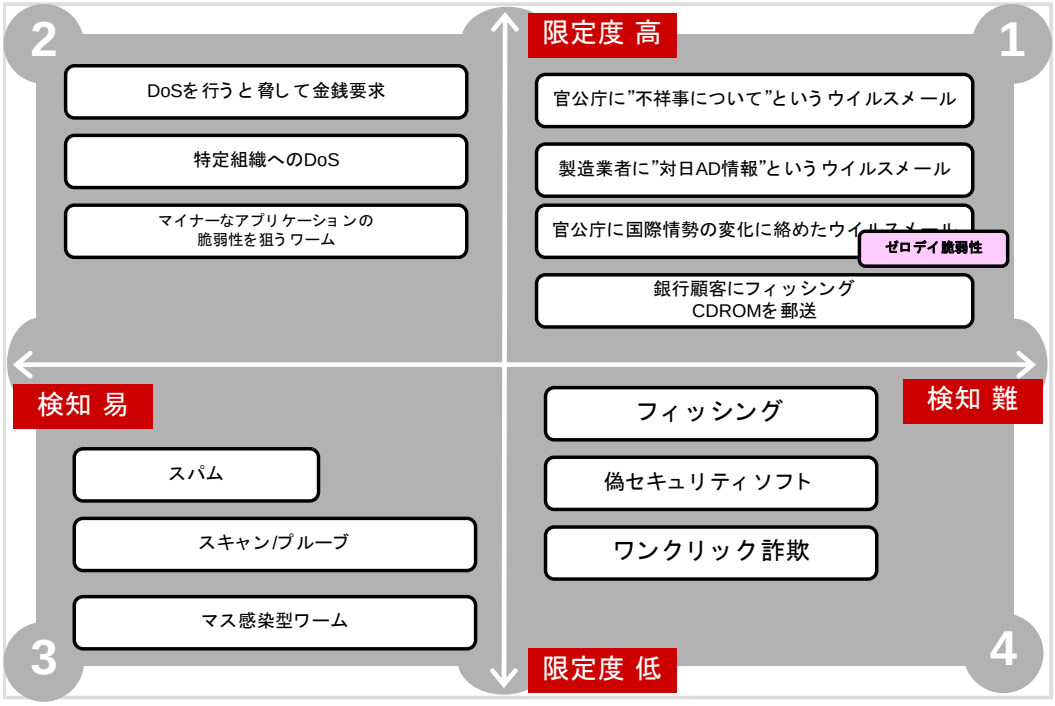
本調査では標的型攻撃を”攻撃対象となる組織あるいはグループに特化した工夫”の有無を基準に 2 つに分けて考えた。

1、 限定度が高く、検知が易しい標的型攻撃

たとえば「特定の企業 A 社を狙った DDoS 攻撃」は特定の組織を標的としているものの、その攻撃の手口に A 社に特化した工夫はされていない。このようなタイプは高度な工夫が行われていないため、比較的検知が易しいと考えられる。特に DDoS に関して言えば攻撃が成功すれば、被害者が攻撃に気づかないことは考えにくい。下図では第 2 象限がこのタイプの攻撃にあたる。

2、 限定度が高く、検知が難しい標的型攻撃

下図の第 1 象限に位置するタイプの攻撃は、標的となる組織に特化した工夫がされている。攻撃が成功した場合、被害者は攻撃を受けたことに気づきにくい。たとえば標的となる組織に特化した差出人や文章を使ったフィッシングを”スピアフィッシング”というが、これは限定度が高く、検知が難しい標的型攻撃の 1 つである。



限定度について

攻撃対象の限定度には様々なレベルが考えられる。現実に発生している事例を調べると、特定個人を狙った攻撃、一企業を狙う攻撃、特定業種の複数企業を狙った攻撃、特定ドメイン利用者を狙った攻撃、特定国への攻撃などが確認されている。
今回の調査では何らかの形で標的を限定していれば標的型攻撃と見なした。大量感染型のワームや、不特定多数を狙うフィッシングやワンクリック詐欺などの無差別攻撃は標的型攻撃には含まれない。

検知 難易度について:

図の横軸は検知の難易度を示している。前述の通り、標的型攻撃の中でもスピアフィッシングやゼロデイ脆弱性を悪用するウイルス付きメールなど攻撃が成功した場合、攻撃に気づかない可能性がある。対して DDoS 等は攻撃が成功すれば、誰もが異常に気づく。

具体的な事例

一口に標的型攻撃と言っても、攻撃の内容には様々な形が見受けられる。攻撃の手口は常に変化を続けているため体系的な整理は困難である。ここでは確認されている過去事例から特徴的な攻撃について例示する。

1. オフィスアプリケーションの脆弱性を狙う攻撃
   Microsoft Office やジャストシステムの一太郎など
2. 主に特定地域で使用されているアプリケーションの脆弱性(もしくはユーザ)を狙う攻撃
   QQ(インスタントメッセンジャー、中国)、zeroboard(掲示板ソフト、韓国)、一

太郎(ワードプロセッサ、日本)、Winny(ファイル共有ソフト、日本)

3. 特定銀行の利用者に限定して、フィッシングサイトへと誘導する CD-ROM を送付
4. 「金銭を払わなければ、Web サイトに DDoS 攻撃を行う」という恐喝
5. ソーシャルエンジニアリングの手法を組み合わせる
   新聞社を騙る、顧客を装う、企業/組織の役員の名前を騙る
   件名・本文に大きな時事問題に便乗した内容を含める

特に 5 番目のソーシャルエンジニアリングについては、この他にも様々なバリエーションで標的を欺く巧妙な手口が確認されている。

4. 被害状況　JPCERT/CC 調査から

調査の目的と手法

2006 年度、JPCERT/CC では標的型攻撃の実態を把握するための調査を行った。この調査では、まず国内外の公開情報の整理、国内のセキュリティベンダにヒアリングを行い実態についての状況を伺った。その結果をふまえた上で、国内企業を対象に無記名アンケート調査を行った。

事前の調査では「標的型攻撃が急増しており、官公庁がターゲットになっている」という意見・報道が散見された。そこでアンケートでは以下 2 つを目的とした。

1. 標的型攻撃の増加しているのであれば、それを定量的なデータで示す。
2. ターゲットは官公庁のみであるのか、あるいは一般企業もターゲットになっているのかを確認する。

無記名アンケート調査に関する詳細は以下の通りである。

- 調査時期: 2007 年 3 月 2 日から 23 日
- 送付先: 企業(東証一部・二部上場企業、店頭公開企業)、電気通信事業者、医療関連(病床数 100 以上の病院を対象)、教育関連(国立・私立大学)、行政サービス(市町村役所)。
- 宛名:「情報セキュリティ担当者様」とした。
- アンケート送付数: 2000 社
- 回答数: 282 社 (回答率 14.1%)
- 回答者構成:

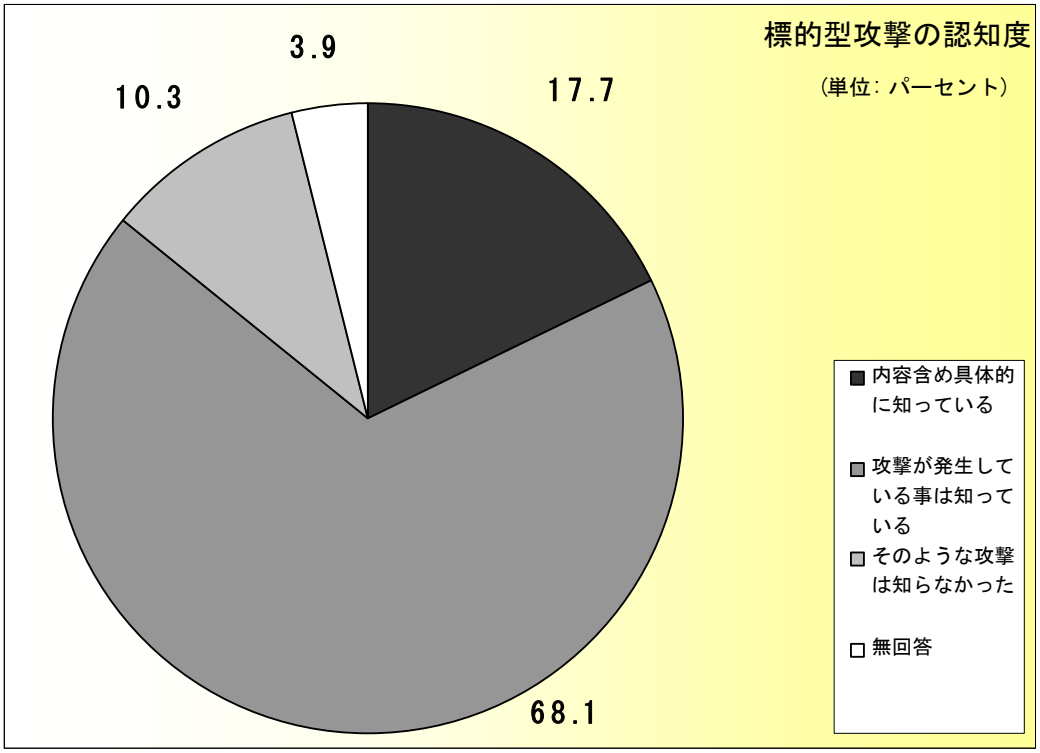
	回答数	構成比(%)
農林水産	1	0.4%
製造	50	17.7%
不動産	13	4.6%
金融	21	7.4%
エネルギー	4	1.4%
運輸	10	3.5%
情報通信	43	15.2%
サービス	51	18.1%
教育	44	15.6%
行政	38	13.5%
業種無回答	7	2.5%
全体	282	100.0%

調査にあたってはエヌ・アール・アイ・セキュアテクノロジーズ株式会社と株式会社野村総合研究所の協力を得た。

調査結果と考察

標的型攻撃の認知度について

「情報セキュリティ上の攻撃として、無差別かつ広範囲に対して行う攻撃ではなく、『特定の企業・団体等を標的とし、対象ごとに攻撃手段を工夫して行われる攻撃』がなされている事例があることをご存知ですか。」という設問に対する回答は以下の通り。



「知らなかった」とする割合は 10.3%であった。85.8%の回答者はなんらかの形で標的型攻撃の存在を知っていると回答した。回答者は規模の大きい企業の情報セキュリティ担当であることを差し引いても標的型攻撃の認知率は高いと言える。

狙われているのは官公庁だけか

アンケート調査では公開情報を元に既知の標的型攻撃で使用されたメールの件名を調べ、同様のメールを受信した経験について尋ねた。結果、標的型攻撃メールを受信した経験があるとした企業の数と割合は、「小泉首相靖国参拝」: 8 件（2.8%)、「対日 AD 情報」: 2 件（0.7%)、「不祥事への対応について」: 3 件（1.1%）となっている。それぞれの業種別内訳は次の通りである。

「小泉首相靖国参拝」
製造:3 件、情報通信:2 件、行政:2 件、業種不明:1 件
「対日 AD(アンチダンピング)情報」

製造:1 件、情報通信:1 件
「不祥事への対応について」
製造:1 件、情報通信:2 件

複数種類のメールを受け取っているケースが 3 例あるため、いずれかのメールを受信したと回答しているのは 8 企業となる。中央官庁だけでなく、企業・地方公共団体も標的型攻撃を受けている事実が浮かび上がった。また 2006 年 8 月の「小泉首相靖国参拝」関連は他のものと比べ送付範囲が広かったと言える。
なお、上記のようなメールを受信したかどうか「分からない」とする割合はそれぞれ 25%前後である

攻撃は増えているのか

アンケート調査では標的型攻撃を受けた経験について、期間を指定しない過去全ての回数と過去 1 年（2006 年 4 月～2007 年 3 月）の回数を尋ねた。その結果が下図である。

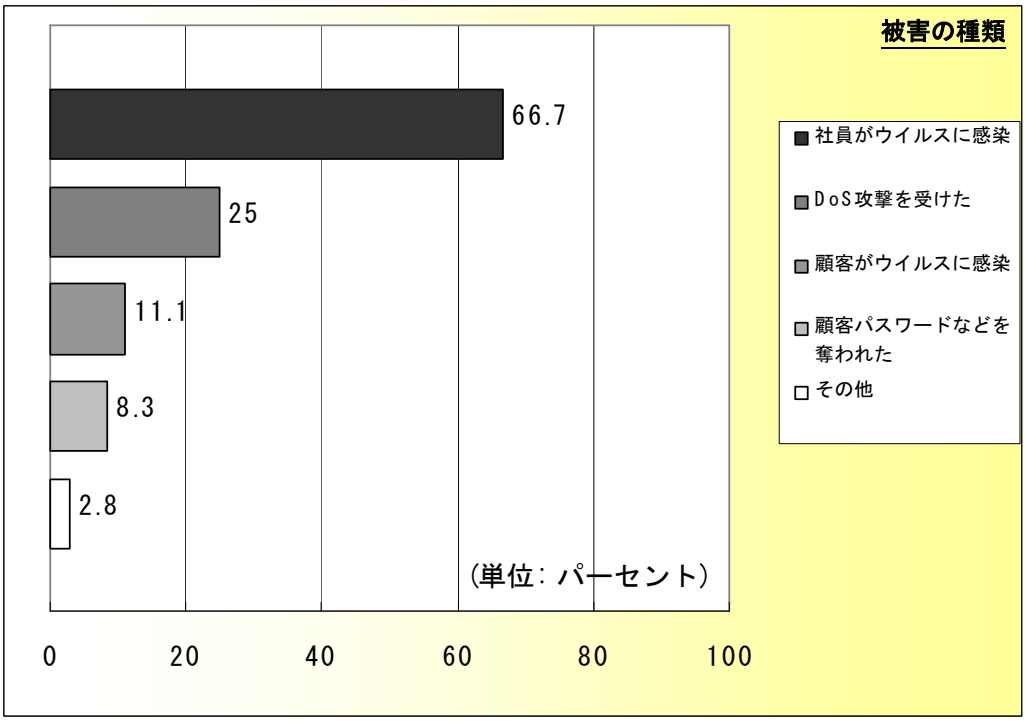
攻撃の例	攻撃を経験したと回答した企業数	回答企業に占める割合
スピアフィッシング	7 (7)	2.6% (2.5%)
関係者を装った社員宛のウィルスメール	18 (15)	6.5% (5.4%)
「DoS をしかける」という脅迫メール	3 (2)	1.2% (0.8%)

()内は過去 1 年間

上記 3 つの標的型攻撃のいずれかを受けたと回答した企業は 8.2%。過去 1 年間に限定すれば 6.4%が被害にあっている。
たとえばスピアフィッシングについてはそのほとんどが 2006 年 4 月から 2007 年 3 月までの 1 年間で発生しており、標的型攻撃の認知件数が急増していると言える。
被害件数に関する報告について業種別の偏りは見られない。

どのような被害が発生しているのか

最も多い事例は自社社員のウイルス感染であり、該当回答者の 66.7%が経験ありと回答している。以下、「DoS（サービス運用妨害）を受けた」（25.0%）が続く。その他の事例としては「サイトが改ざんされた」とする回答があった。アンケートの結果、直接的な金銭被害を受けたという回答は皆無であった。



誰が攻撃をおこなっているのか

標的型攻撃を受けた企業の 6 割以上が「攻撃者の特定ができなかった」と回答している。標的型攻撃であっても攻撃者の特定は困難な現状が伺える。

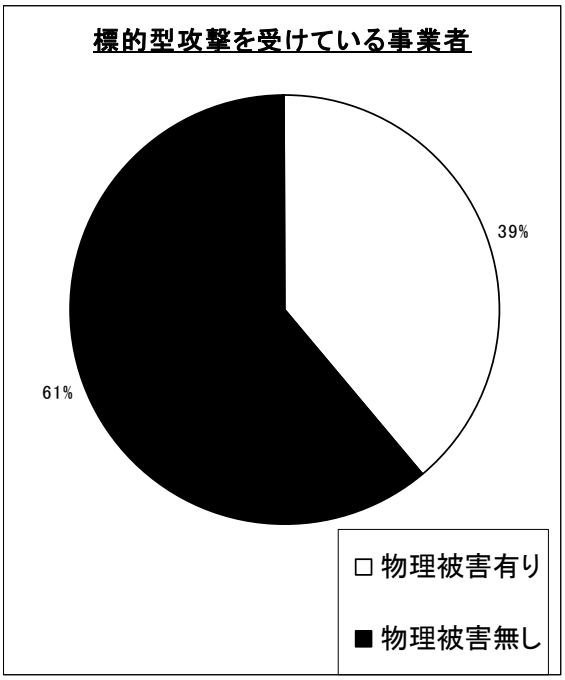
特定できなかった	63.9%
その他、社外の人物	19.4%
特定しようとしなかった	5.6%
社員、あるいは契約社員	5.6%
取引先	2.8%
その他	2.8%
元社員、あるいは元契約社員	0.0%

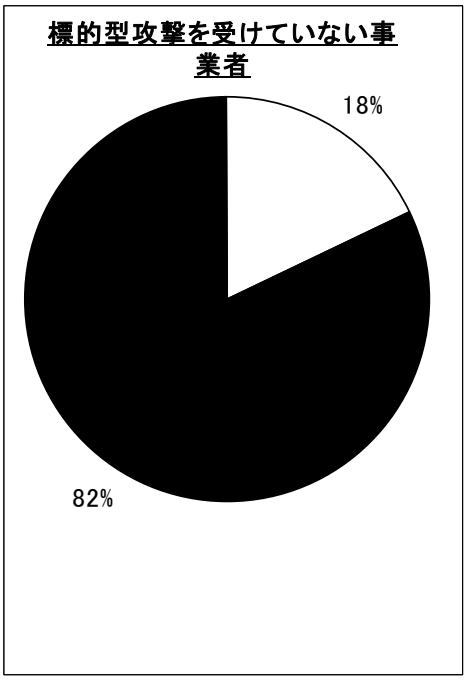
セキュリティ専門家へのヒアリングでも、メールのヘッダが偽造されている可能性や、攻撃元の IP アドレスが特定できても単なる踏み台サーバの可能性もあることから、標的型攻撃の発信元をつきとめることは困難であるという意見が多かった。

インターネットだけが危ないのか

アンケート調査で標的型攻撃を受けたと回答した企業のうち約 4 割は、施設への物理的侵入、窃盗、廃棄物からの情報持ち出しなどの被害を経験している。標的型攻撃を受ける企業が攻撃者にとって魅力的な情報を持っており、攻撃者は手段の 1 つ

として標的型攻撃を行っていると考えることも可能である。





5. 対策

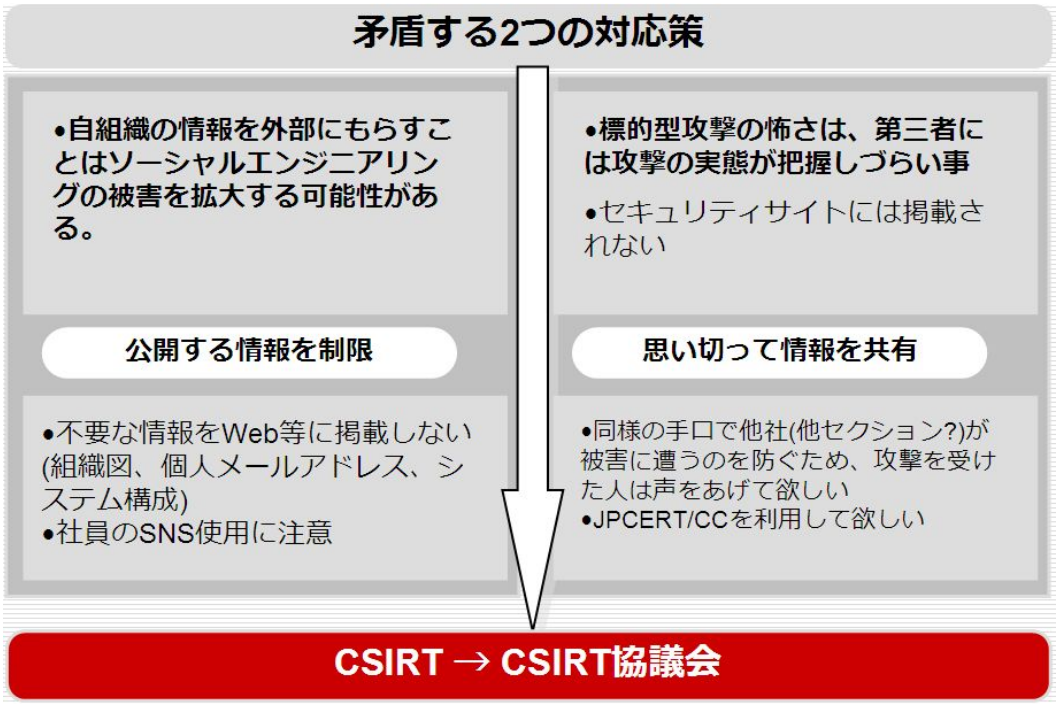
本調査の結果から官公庁や大企業でなくとも、そして業種を問わず、標的型攻撃の対象となる可能性があることが分かった。標的型攻撃は対岸の火事ではないという認識を持つ必要がある。アンケート調査でも回答者の約 9 割がなんらかの標的型攻撃対策を実施することが必要であると認識している。
この章では攻撃者の特定が難しい状況下で如何なる自衛手段が考えられるのかという点について考えたい。

情報の共有

情報を共有することは標的型攻撃の対策として重要である。高度な標的型攻撃は既存の攻撃と違って目立たず、規模も小さいためセキュリティサイトなどで大々的に報道されることがない。
特定の業種に次々と攻撃をしかけるケースも確認されており、攻撃を受けた企業がその手口を共有することで、同業他社が被害にあうのを防ぐことが出来る可能性がある。

攻撃情報を広く公開することは攻撃者にヒントをあたえることになる。従ってここでは組織間の信頼に基づいた情報共有の仕組みを作る必要がある。たとえば社内に CSIRT をつくり、そこを窓口に他社 CSIRT との情報共有を行うなどの対策が有効である。

※CSIRT: CSIRT（Computer Security Incident Response Team の略）
コンピュータセキュリティインシデントに関わる活動を行なっている組織。インシデント対応及びその支援、分析や教育、研究開発などを含めて様々な活動を行う。



標的型のメール攻撃対策

特に標的を限定して工夫された標的型のメール攻撃については以下のような対策が考えられる

メール以外の通信手段を併用する

メールは送信者の詐称が簡単に行えるという弱点を抱えた通信手段である。標的型のメール攻撃に対しては、例えば電話やインスタントメッセンジャーなどのメール以外の手段を使って、送信者とのコミュニケーションを取ることで詐称に気づく可能性が高まることが期待できる。

送信者の詐称を防ぐ

送信者の詐称を技術的に防ぐ手段として電子メールに署名をする方法がある。現在、メッセージに電子署名をする技術としては PGP や S/MIME が有名である。
また、それとは別にメールサーバでメールの送信ドメインを検証する技術、SPF(Sender ID)あるいは DKIM が考えられる。DKIM は 2007 年に標準化されたばかりであるが、これらの技術が普及することでエンドユーザに対して個別に署名・検証する作業を強いることなく送信者の詐称を見抜くことが可能となる。

予防接種(イノキュレーション)という考え方

特定の相手に向けて工夫されたメール攻撃への対策として、「予防接種」を行うというアプローチも考えられる。
予防接種とは特定組織を対象にファイル削除などの実害を伴わない実行ファイル付きのメールを送信し、メール開封率やクリック率を測定する手法である。最終的に社員に対して不審なメールへの耐性をつけることを目的としている。
ただし予防接種の具体的な手法については情報が少なく、1)対策の効果、2)法的問題、3)倫理的問題などについて検討の余地が少なからず残っている。

6. 謝辞

本調査のヒアリングに協力いただいた各社にこの場を借りてお礼申し上げます。
インターネットセキュリティシステムズ株式会社
株式会社シマンテック
トレンドマイクロ株式会社
マカフィー株式会社
株式会社ラック

またアンケートにご回答いただきました皆様のご協力にあらためて深く感謝いたします。

JPCERT/CC では、コンピュータセキュリティインシデントに関する情報提供を目的としたご報告、及び JPCERT/CC によるコーディネーションの依頼を受け付けております。
情報提供はインシデントの状況の分析に役立てるとともに、統計情報として施策に反映致します。（情報提供元に関する情報は公開致しません。）

ご報告、ご依頼は下記メールアドレスまでお寄せください。
Email：info@jpcert.or.jp
PGP Fingerprint ：BA F4 D9 FA B8 FB F0 73　57 EE 3C 2B 13 F0 48 B8
インシデント報告様式：　http://www.jpcert.or.jp/form/