標的型攻撃とその対応

今回は、昨年9月以降大きく話題となった標的型攻撃について解説すると共に、不正に発行された証明書の悪用について解説します。

1.1 はじめに

このレポートは、インターネットの安定運用のためにIIJ自身が取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、IIJが対応したインシデントについてまとめたものです。今回のレポートで対象とする2011年10月から12月までの期間では、前回の期間に続いてAnonymous等のHacktivismによる攻撃が複数発生しており、企業や政府関係組織を狙った標的型攻撃も相次いで発覚しています。また、米国で水道システムへの侵入事件が発生する等、重要インフラに対する攻撃が明らかになりました。加えて、スマートフォン利用者の増大に伴い、特に利用者にかかわる情報の取り扱いについて、問題となることが増えてきました。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

1.2 インシデントサマリ

ここでは、2011年10月から12月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

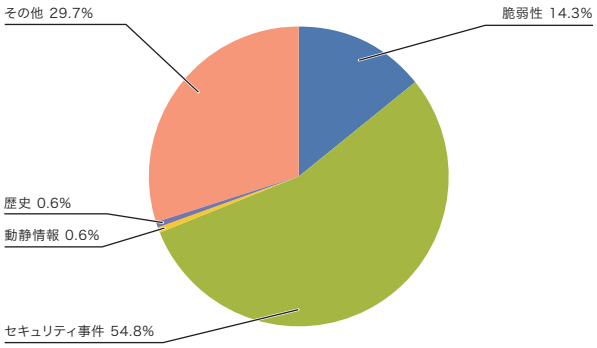


図-1 カテゴリ別比率(2011年10月〜12月)

*1 このレポートでは取り扱ったインシデントを、脆弱性、動静情報、歴史、セキュリティ事件、その他の5種類に分類している。
脆弱性:インターネットやユーザの環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェア等の脆弱性への対応を示す。
動静情報:要人による国際会議や、国際紛争に起因する攻撃等、国内外の情勢や国際的なイベントに関連するインシデントへの対応を示す。
歴史:歴史上の記念日等で、過去に史実に関連して攻撃が発生した日における注意・警戒、インシデントの検知、対策等の作業を示す。
セキュリティ事件:ワーム等のマルウェアの活性化や、特定サイトへのDDoS攻撃等、突発的に発生したインシデントとその対応を示す。
その他:イベントによるトラフィック集中等、直接セキュリティに関わるものではないインシデントや、セキュリティ関係情報を示す。

■ Anonymous等の活動

この期間においてもAnonymousに代表されるHacktivistによる攻撃活動は継続しています。様々な事件や主張に応じて、米国、イスラエル、イタリア、ポルトガル、コロンビア、エルサルバドル等、その他にも多数の政府系サイトに対するDDoS攻撃や情報漏えい事件が発生しました。特に米国内においては、複数の政府関連団体及び企業からの大規模な情報漏えい事件が発生しています。

2011年9月にニューヨークのウォール街を中心に始まったデモ活動であるOccupy Wall Streetは格差是正等を訴えて支持を拡げ、10月以降になると米国内にとどまらず世界中にデモ活動が拡大していきました。Anonymousもこの活動への支持を表明し、大手金融機関の経営陣の個人情報を漏えいしたり、これら金融機関からの資金移動を呼び掛けたりしました。

また11月になると、米国議会において審議中の法案SOPA(Stop Online Piracy Act)への反対を表明し、SOPA支持を表明している企業への攻撃や、米国政府への攻撃等を表明しました。SOPAは様々な反対運動が実施された結果、法案の審議は延期されましたが、Anonymousによる攻撃活動は本稿執筆時点においても継続しており、今後の動向に注意する必要があります。

12月に発生したStratfor社(Strategic Forecasting Inc.)への攻撃では、Webサーバに侵入して、サーバ上にあったレポートを購読していた顧客のクレジットカード情報を含むリストが漏えいし、その一部が公開されました。更に、このリストを利用して慈善団体への寄付が行われる等の金銭的被害も発生しました[*2]。

■ 標的型攻撃とその対策活動

9月に大手企業で発覚した標的型攻撃が、他の大手企業や複数の政府機関に対しても発生していたことが明らかになりました。この期間においては、特に、複数の政府関係組織において標的型攻撃を受けていたことが相次いで判明しました。ある事例では、利用者のIDとパスワードの流出、及びメールの内容が漏えいしていたことが被害として報告されています。このように政府機関での被害が相次いで判明したことから、12月に内閣官房から注意喚起が行われました[*3]。

標的型攻撃が相次いだことにより政府機関を主導とした対策活動が多く実施されました。まず、この問題についての情報セキュリティ対策の強化について内閣官房長官からメッセージ[*4]を出すと共に、情報セキュリティ政策会議[*5]において政府における取組みの説明が行われました。また、各省庁が主導する対策活動も複数実施されています[*6]。加えて、一般企業に向けた対策活動として、JPCERTコーディネーションセンターから、標的型メール攻撃に関する注意喚起[*7]が行われたり、IPAでは「標的型サイバー攻撃の特別相談窓口」を設置[*8]する等、情報の把握と対策を支援する体制が整えられつつあります[*9]。この問題については「1.4.2 標的型攻撃とその対応」も併せてご参照ください。

＊2　この事件に関しては次のエフセキュアブログ等に詳しい。「『Anonymous』、寄付および慈善団体について」(http://blog.f-secure.jp/archives/50644771.html)。
＊3　内閣官房情報セキュリティセンター(NISC)、「標的型攻撃対策としての適切な管理者権限管理について」(http://www.nisc.go.jp/press/pdf/hyoutekigata_press.pdf)。
＊4　情報セキュリティ政策会議議長である内閣官房長官が出したメッセージは、次の首相官邸ホームページを参照のこと。「情報セキュリティ対策の強化について」(http://www.kantei.go.jp/jp/tyokan/noda/20111007message.html)。
＊5　情報セキュリティ政策会議(http://www.nisc.go.jp/conference/seisaku/index.html)。
＊6　例えば、警察庁による「サイバーインテリジェンス対策に係る警察の取組について」(http://www.npa.go.jp/keibi/biki3/230804kouhou.pdf)、経済産業省による「サイバー情報共有イニシアティブ(J-CSIP)」(http://www.ipa.go.jp/security/J-CSIP/index.html)、総務省による「テレコムアイザック官民協議会」等。民間企業の間でも、セキュリティオペレーション事業者や、重要インフラ企業の間で同様の検討が行われている。
＊7　JPCERTコーディネーションセンター、「JPCERT/CC Alert 2011-10-28 標的型メール攻撃に関する注意喚起」(http://www.jpcert.or.jp/at/2011/at110028.html)。
＊8　IPA、「『標的型サイバー攻撃の特別相談窓口』の設置」(http://www.ipa.go.jp/about/press/20111025.html)。
＊9　その他の活動としては、民間主導の活動として、国内の重要インフラ企業で構成されたCEPTOAR Councilにおける活動や、日本セキュリティオペレーション事業者協議会(http://www.jnsa.org/isog-j/)の標的型攻撃対策検討WG等がある。

10月のインシデント

1
- セ **1日**：国内においてAndroidアプリ開発者向けに提供されていたSDKで端末内の情報を不適切に取得していることがわかり、問題となった。

2
3
4
- 脆 **2日**：HTC製Androidスマートフォンの一部にインストールされているTCLoggersに、任意のアプリが個人情報等を読みとれるという不具合が発見された。この不具合に対して、10月7日に日本でのパッチ提供が行われている。
  Android Police "Massive Security Vulnerability In HTC Android Devices（EVO 3D, 4G, Thunderbolt, Others）Exposes Phone Numbers, GPS, SMS, Emails Addresses, Much More"
  （http://www.androidpolice.com/2011/10/01/massive-security-vulnerability-in-htc-android-devices-evo-3d-4g-thunderbolt-others-exposes-phone-numbers-gps-sms-emails-addresses-much-more/）。

5
- 他 **3日**：IPAより「『標的型攻撃メールの分析』に関するレポート」が公開された。
  「IPA テクニカルウォッチ『標的型攻撃メールの分析』に関するレポート」（http://www.ipa.go.jp/about/technicalwatch/20111003.html）。

6
7
- 脆 **5日**：Apacheでmod_proxyを利用し、特定の設定を行っているリバースプロキシの動作に脆弱性（CVE-2011-3368）があり、内部サーバが参照できるという不具合が修正された。
  "Apache HTTP Server：mod_proxy reverse proxy exposure（CVE-2011-3368）"（https://bugzilla.redhat.com/show_bug.cgi?id=769844）。

8
- 他 **5日**：商業的な活動をしているボットネットの1つであるAldi Botに関する調査結果が公表された。
  The Arbor Networks Security Blog、"DDoS Watch: Keeping an Eye on Aldi Bot"（http://ddos.arbornetworks.com/2011/10/ddos-aldi-bot/）。

9
10
- セ **7日**：6日に逝去したスティーブ・ジョブズ氏のニュースに便乗した攻撃が確認された。
  TrendLabs SECURITY BLOG、「スティーブ・ジョブズ氏死去報道に便乗した詐欺、Facebook上で確認」（http://blog.trendmicro.co.jp/archives/4532）。

11
- 他 **7日**：政府の情報セキュリティ政策会議で政府機関の職員およそ5万人に対して、標的型不審メール訓練を実施することを決定した。
  内閣官房情報セキュリティセンター、「第２７回会合 参考資料１ 政府機関における標的型不審メール訓練について」
  （http://www.nisc.go.jp/conference/seisaku/dai27/pdf/27shiryous1.pdf）。

12
13
- セ **11日**：Anonymousの呼びかけにより、ニューヨーク証券取引所に対するDDoS攻撃が発生した。
  IIJ-SECT Security Diary、「Anonymousによる NYSEへの DDoS攻撃」（https://sect.iij.ad.jp/d/2011/10/127533.html）。

14
- 他 **11日**：RIMの「BlackBerry」でインターネット接続やメッセージ送受信ができなくなる大規模サービス障害が発生した。この障害は世界各地で3日間続いた。
  "BlackBerry Service Update"（http://www.rim.com/newsroom/service-update.shtml）。

15
- 脆 **12日**：Apple社のiOS 5ソフトウェアで任意のコード実行や情報漏えいを引き起こす複数の脆弱性があり、修正された。
  「iOS 5 ソフトウェア・アップデートのセキュリティコンテンツについて」（http://support.apple.com/kb/HT4999?viewlocale=ja_JP）。

16
17
- 脆 **12日**：Apple社のOS X Lionに任意のコード実行や情報漏えいを引き起こす複数の脆弱性があり、修正された。
  「OS X Lion v10.7.2およびセキュリティアップデート 2011-006 のセキュリティコンテンツについて」
  （http://support.apple.com/kb/HT5002?viewlocale=ja_JP）。

18
- 脆 **12日**：Microsoft社は 2011年10月のセキュリティ情報を公開し、2件の緊急と6件の重要な更新をリリースした。
  「2011年10月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms11-oct）。

19
20
- セ **14日**：Stuxnetに類似したコードを持ち、リモートアクセスによる情報取得を狙ったマルウェアDuquが発見された。
  シマンテック セキュリティレスポンスブログ、「W32.Duqu：次なる Stuxnet の前兆（http://www.symantec.com/connect/blogs/w32duqu-stuxnet）。

21
- 脆 **18日**：Oracle社のJava SE JDK及びJREに任意のコードが実行可能な脆弱性（CVE-2011-3544）があり、修正された。
  "Oracle Java SE Critical Patch Update Advisory - October 2011"
  （http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html）。

22
- 他 **18日**：米国土安全保障省がAnonymousによる産業制御システム（ICS）を狙ったサイバー攻撃に対して注意喚起を行っていることが判明した。
  public intelligence、"(U//FOUO) DHS Bulletin: Anonymous Hacktivist Threat to Industrial Control Systems (ICS)"
  （http://publicintelligence.net/ufouo-dhs-bulletin-anonymous-hacktivist-threat-to-industrial-control-systems-ics/）。

23
24
- セ **22日**：オープンソースのアプリケーションサーバ「JBoss」を対象としたワームが発生し、感染を拡げているとの注意喚起が行われた。ワームが利用している脆弱性は2010年4月に修正されている。
  SANS ISC Diary、"JBoss Worm"（http://isc.sans.edu/diary.html?storyid=11860）。

25
26
- セ **25日**：The Hacker's Choiceが脆弱性のあるHTTPSサイトに対しSSLの再ネゴシエーションを利用したDoS攻撃を行うツールを公表した。
  SANS ISC Diary、"The Theoretical "SSL Renegotiation" Issue gets a Whole Lot More Real !"（http://isc.sans.edu/diary/11893）。

27
- セ **25日**：正規のAndroidアプリケーションのアップデートを利用した感染手法を使うマルウェアが発見された。
  エフセキュアブログ、「『DroidKungFu』がアップデート攻撃を利用」（http://blog.f-secure.jp/archives/50634684.html）。

28
- セ **25日**：国内で7月に政府関連組織に対する標的型攻撃が発生していたことが報道された。

29
30
- セ **26日**：韓国でソウル市長選の選挙管理委員会や候補者のWebサイトへのDDoS攻撃が発生した。

31
- 脆 **28日**：WordPressのプラグインであるWPtouchにSQL Injectionが可能な脆弱性が見つかり、修正された。
  EXPLOIT-DB、"WordPress wptouch plugin SQL Injection Vulnerability"（URL:http://www.exploit-db.com/exploits/18039）。

［ 凡 例 ］ 脆 脆 弱 性　セ セキュリティ事件　動 動 静 情 報　歴 歴　史　他 そ の 他

※日付は日本標準時

■ 脆弱性とその対応

この期間中では、クライアントとして用いるMicrosoft社のWindows[*10]、Adobe社のAdobe Reader及びAcrobat[*11]、Adobe Flash Player[*12]、Adobe Shockwave Player[*13]、Oracle社のJRE[*14]等のアプリケーションで多くの脆弱性が発見され、修正されています。これらの脆弱性のいくつかは修正が行われる前に悪用されていることが確認されました。サーバアプリケーションでは、DNSサーバのISC BIND[*15]や、WebサーバのApache HTTPD Server[*16]に脆弱性が見つかっています。これ以外にも、Microsoft社のWindows[*17]、FTPサーバのProFTPD[*18]でも脆弱性が修正されています。また、ドイツのハッカーグループによりWebサーバのSSL再ネゴシエーションの問題を突くDoSの実証ツールが公開されています[*19]。加えて、ドイツで行われた、28th Chaos Communication Congressで、PHPをはじめとする多くのWebアプリケーション開発プラットフォームに対してDoS攻撃を行う手法が公表されました[*20]。

■ 脆弱性を悪用したWebコンテンツの改ざん

不正侵入による改ざん事件も多く発生しました。Webアプリケーションサーバ JBossの既知の脆弱性（CVE-2010-0738）を悪用して感染するワーム[*21]の発生や、CMSのWordPressのプラグインであるTimThumb、ASP.net[*22]、Plone CMSやphpThumb.php等[*23]、特定のシステムで明らかになった脆弱性を狙う攻撃が増加していることが確認されています。特にTimThumbのケースではexploit kitの1つであるBlackhole Toolkitに取り入れられていることが判明[*24]しました。

このようなWebサーバアプリケーションは導入が容易で機能も豊富なため、広く利用されるようになっていますが、一方で今回のように脆弱性を機械的に攻撃する手法により数多くの改ざんが確認される事件がたびたび発生しています。インターネット側に公開するサーバについては、適切なアクセス権限の設定やセキュリティアップデートに迅速に対応する必要があります。

＊10 「マイクロソフトセキュリティ情報 MS11-087 - 緊急Windowsカーネルモードドライバーの脆弱性により、リモートでコードが実行される（2639417）」（http://technet.microsoft.com/ja-jp/security/bulletin/MS11-087）。

＊11 「APSB11-30：Windows版Adobe Reader 9.x及びAcrobat 9.xに関するセキュリティアップデート公開」（http://kb2.adobe.com/jp/cps/927/cpsid_92703.html）。なお、Adobe Reader X及びAdobe Acrobat Xの修正は2012年1月10日に行われた「APSB12-01：Adobe Reader及びAcrobatに関するセキュリティアップデート公開」（http://kb2.adobe.com/jp/cps/928/cpsid_92823.html）。

＊12 「APSB11-28：Adobe Flash Player用セキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb11-28.html）。

＊13 「APSB11-27：Adobe Shockwave Player用セキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb11-27.html）。

＊14 "Oracle Java SE Critical Patch Update Advisory-October 2011"（http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html）。

＊15 Internet Systems Consortium、"BIND 9 Resolver crashes after logging an error in query.c"（http://www.isc.org/software/bind/advisories/cve-2011-tbd）。

＊16 Red Hat Bugzilla、"Bug 740045-（CVE-2011-3368）CVE-2011-3368 httpd:reverse web proxy vulnerability"（https://bugzilla.redhat.com/show_bug.cgi?id=750935）。

＊17 「マイクロソフトセキュリティ情報 MS11-083 - 緊急TCP/IPの脆弱性により、リモートでコードが実行される（2588516）」（http://technet.microsoft.com/ja-jp/security/bulletin/MS11-083）。

＊18 "Response pool use-after-free memory corruption error"（http://bugs.proftpd.org/show_bug.cgi?id=3711）。

＊19 このツールに関しては次のSANS ISC Diary等に詳しい。"The Theoretical "SSL Renegotiation" Issue gets a Whole Lot More Real !"（http://isc.sans.edu/diary.html?storyid=11893）。

＊20 この手法の詳細については次の発表を参照のこと。"Effective Denial of Service attacks against Web application platforms"（http://events.ccc.de/congress/2011/Fahrplan/events/4680.en.html）。なお、この発表を受けて各プロダクトで修正が行われているが本稿執筆時点では一部で修正が行われたのみとなっている。

＊21 このワームについては次のJBoss Communityのブログに詳しい。"Statement Regarding Security Threat to JBoss Application Server"（https://community.jboss.org/blogs/mjc/2011/10/20/statement-regarding-security-threat-to-jboss-application-server）。

＊22 ASP.NETを狙った事件についての詳細は、例えば次のArmorize Malware Blog等がある。"http://jghui.com/urchin.js mass infection ongoing"（http://blog.armorize.com/2011/10/httpjghuicomurchinjs-mass-infection.html）。

＊23 IBM Tokyo SOC Report、「Plone CMS及びphpThumbへの攻撃増加を確認」（https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/plone_phpthumb_attack_20111226?lang=ja_jp）。

＊24 詳細については次のAVAST! Blogを参照のこと。"Following WordPress into a Blackhole"（https://blog.avast.com/2011/10/31/following-wordpress-into-a-blackhole/）。

11月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

セ **1日**：WordPressの脆弱性を利用してページを改ざんし、訪問者をマルウェアに感染させる攻撃が多数確認された。
Avast! Blog、"Following WordPress into a Blackhole"（https://blog.avast.com/2011/10/31/following-wordpress-into-a-blackhole/）。

セ **2日**：10月に報道された政府関連組織とは別の政府関連組織も同時期に標的型攻撃を受けていたことが報道された。

セ **4日**：マレーシアのSSL認証局が暗号強度の低いSSL証明書を発行していたことが判明した。
Entrust, Inc.、"Entrust Bulletin on Certificates Issued with Weak 512-bit RSA Keys by Digicert Malaysia"（http://www.entrust.net/advisories/malaysia.htm）。

セ **5日**：オランダのSSL認証局でサーバ上にDDoSツールが見つかり、調査のため一時的に証明書発行業務を停止した。
Kaspersky Lab SECURELIST Blog、"Dutch CA suspends issuance of digital certificates"
（http://www.securelist.com/en/blog/208193210/Dutch_CA_suspends_issuance_of_digital_certificates）。

セ **7日**：ブラジルで大規模なDNSキャッシュポイズニング事件が発生した。
Kaspersky Lab SECURELIST Blog、"Massive DNS poisoning attacks in Brazil"
（http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil）。

脆 **8日**：Juniperルータの脆弱性により広範囲にネットワークがダウンする障害が世界各地で複数発生した。
この障害については次のNANOG mailing listでのスレッド等で報告されている
（http://mailman.nanog.org/pipermail/nanog/2011-November/041653.html）。

脆 **8日**：Adobe Shockwave Playerにリモートからコード実行可能な複数の脆弱性が見つかり、修正された。
「APSB11-27：Adobe Shockwave Player用セキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb11-27.html）。

セ **8日**：イリノイ州の水道設備でポンプ障害が発生した。この事件は当初ロシアからのサイバー攻撃によるものと報道されていたが、後に攻撃ではなかったことが発表された。
ICS-CERT、"ICSB-11-327-01?ILL INOIS WATER PUMP FAILURE REPORT"（http://www.us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf）。

脆 **9日**：FTP サーバのProFTPDにリモートからのコード実行可能な脆弱性（CVE-2011-4130）が見つかり、修正された。
bugs.proftpd.org、"Response pool use-after-free memory corruption error"（http://bugs.proftpd.org/show_bug.cgi?id=3711）。

脆 **9日**：Microsoft社は 2011年11月のセキュリティ情報を公開し、緊急に分類されるMS11-083と2件の重要、1つの警告となる更新をリリースした。
「2011年11月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms11-nov）。

セ **9日**：自治体向けサービス提供会社にDDoS攻撃が発生し、このサービスを利用している全国200の自治体に影響が出た。

脆 **10日**：Adobe Flash Playerにリモートからのコード実行を含む複数の脆弱性が見つかり、修正された。
「APSB11-28：Adobe Flash Player用セキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb11-28.html）。

他 **10日**：一般社団法人インターネットコンテンツセーフティ協会（ICSA）は、報道機関向けに児童ポルノのブロッキングの運用状況を公表した。
一般社団法人インターネットコンテンツセーフティ協会（ICSA）（http://www.netsafety.or.jp/）。

脆 **11日**：Microsoft社はDigiCert Sdn. Bhd.の脆弱なSSL証明書の対策として、2つの中間証明機関による証明書を失効する更新プログラムをリリースした。
「マイクロソフト セキュリティ アドバイザリ（2641690）不正なデジタル証明書により、なりすましが行われる」
（http://technet.microsoft.com/ja-jp/security/advisory/2641690）。

セ **14日**：マレーシア政府の関連組織の署名鍵で署名されたマルウェアが発見された。
エフセキュアブログ、「政府の署名鍵で署名されたマルウェア」（http://blog.f-secure.jp/archives/50638015.html）。

セ **15日**：2011年8月に発見されたWordPress Pluginの脆弱性を利用したWebサイトへの改ざん攻撃が増加しているとの報告がされた。
IBM Tokyo SOC Report、「WordPressを利用したWebサイトへの改ざん攻撃の増加」
（https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/wordpress_injection_20111115?lang=ja）。

脆 **16日**：BIND 9にリモートからサーバ停止が可能な脆弱性（CVE-2011-4313）が発見され、修正された。
ISC、"BIND 9 Resolver crashes after logging an error in query.c"（http://www.isc.org/software/bind/advisories/cve-2011-tbd）。

セ **19日**：テキサス州の水道設備システム（SCADA）に侵入したとするpr0fを名乗る人物が証拠として複数の制御画面のスクリーンショットを公開した。
Kaspersky Lab Threatpost、"Hacker Says Texas Town Used Three Character Password To Secure Internet Facing SCADA System"
（http://threatpost.com/en_us/blogs/hacker-says-texas-town-used-three-character-password-secure-internet-facing-scada-system-11201）。

他 **25日**：IPAは、公開した注意喚起情報をリアルタイムに配信するサイバーセキュリティ注意喚起サービス「icat」を公開した。
「サイバーセキュリティ注意喚起サービス『icat』の公開」（http://www.ipa.go.jp/security/vuln/icat.html）。

セ **28日**：携帯電話会社によりスマートフォンにインストールされていたアプリケーションCarrier IQがスマートフォンの利用データを収集して送信していたことが研究者より発表された。

他 **30日**：IPAより「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド改定第2版」が公開された。
「『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）。

［ 凡 例 ］ 脆 脆 弱 性　セ セキュリティ事件　動 動 静 情 報　歴 歴　史　他 そ の 他

※日付は日本標準時

■ 重要インフラへの攻撃

この期間には重要インフラに対する攻撃がいくつか発生しました。まず、テキサス州の水道設備で利用されていたSCADAシステムが侵入され、証拠として制御画面の画像が公開されました[*25]。日本でも複数の自治体の電子申請システムが収容されているサーバ群が攻撃され、申請業務に影響がでる事件が発生しています。テキサス州の事件の前に、イリノイ州の水道システムにロシアを発信源とする攻撃が発生したと報道されましたが、この事件は誤解であったことが後に発表されています。

■ 証明書発行機関への侵入と不正な証明書の取得

証明書発行機関に対する侵入事件と、それにより不正な証明書が発行される事件についても引き続き発生しています。オランダのKPN社では警察によるDDoS事件の調査の過程で自社サーバ上にDDoSツールが見つかったとして、調査のため一時的に証明書発行業務を停止しました[*26]。更にKPN社の子会社でオランダの自治体や警察等にセキュリティコンサルティングや認証技術を提供していたGemnetに対し、phpMyAdminを介した侵入事件が発生しました[*27]。侵入されたデータベースにはこれらの顧客に関連したネットワーク情報等が含まれていたとされています。これらの事件については「1.4.1 公開鍵証明書発行に関するいくつかの問題」も併せてご参照ください。

マレーシアの証明書発行機関であるDigiCert Sdn.社では、同組織が発行した22通の証明書の暗号強度が低く、失効情報が含まれていない等、問題のある証明書であったことが判明し、Microsoft社やMozilla等で中間認証局の信頼を取り消す対応[*28]が行われました。

また、ComodoHackerによる一連の事件で侵入を受けたとされたGMOグローバルサイン社が調査結果をまとめ、不正な証明書の発行や認証局のインフラに対する侵害はなかったとする最終報告書を公表しました。

■ DDoS攻撃

韓国では、10月に行われたソウル市の市長選の際に、候補者や選挙管理委員会のWebサイトに対するDDoS攻撃が発生し、選挙会場の確認ができない等の混乱が発生しました。また、この攻撃を行ったとして与党国会議員の秘書とIT会社の社長等が逮捕されています[*29]。選挙に関連したDDoS攻撃はロシアでも発生し、ラジオ局や独立系選挙監視団体等のWebサイトが攻撃を受け、アクセスができなくなる事件が発生しています。

■ フィッシング事件の国内動向

この期間では、メールやSNSを利用したフィッシング事件も継続して発生しています。特に銀行を装ったフィッシングでは類似の手口による攻撃が複数の銀行に対して確認されており、金銭被害も発生しています。攻撃手法としては、メールに添付したプログラムを利用するものと、フィッシングサイトに誘導する2つのパターンが確認されています[*30]。いずれの場合も、第2認証として利用される情報等の入力を促す画面が表示されます。

また、金融機関のIDやパスワードだけではなく、SNSやオンラインゲームのアカウントを狙ったフィッシング事件も発生しており、ポイントを不正に利用される等の被害が発生しています。

---

*25 この事件については次のKaspersky Lab社のThreatpostに詳しい。"Hacker Says Texas Town Used Three Character Password To Secure Internet Facing SCADA System"(http://threatpost.com/en_us/blogs/hacker-says-texas-town-used-three-character-password-secure-internet-facing-scada-system-11201)。

*26 KPN社の公式発表は次のとおり。"KPN stopt uit voorzorg uitgifte nieuwe veiligheidscertificaten"(http://www.kpn.com/corporate/overkpn/Newsroom/nieuwsbericht/KPN-stopt-uit-voorzorg-uitgifte-nieuwe-veiligheidscertificaten.htm)。

*27 この事件について、例えば次のSophos社のnakedsecurityに詳しい。"Second Dutch security firm hacked, unsecured phpMyAdmin implicated"(http://nakedsecurity.sophos.com/2011/12/08/second-dutch-security-firm-hacked-unsecured-phpmyadmin-implicated/)。

*28 Microsoft社やMozillaでの対応は次のとおり。Microsoft "Untrusted Certificate Store to be updated"(http://blogs.technet.com/b/msrc/archive/2011/11/03/untrusted-certificate-store-to-be-updated.aspx)。Mozilla Security Blog、"Revoking Trust in DigiCert Sdn. Bhd Intermediate Certificate Authority" (http://blog.mozilla.com/security/2011/11/03/revoking-trust-in-digicert-sdn-bhd-intermediate-certificate-authority/)。

*29 Sophos、nakedsecurity "Election-day cyber attack scandal rocks South Korea's ruling party"(http://nakedsecurity.sophos.com/2011/12/08/election-cyber-attack-scandal-south-korea/)。

*30 これらのフィッシングについては次のIPAの報告でも解説されている。「コンピュータウイルス・不正アクセスの届出状況[9月分および第3四半期]について」(http://www.ipa.go.jp/security/txt/2011/10outline.html)。

12月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

セ **1日**：.usドメインのレジストラであるabout.usが、WordPressの脆弱性により9月から改ざんされていたことが判明した。

セ **4日**：韓国で2011年10月26日に発生した選挙管理委員会Webサイトへの DDoS攻撃の容疑で与党議員の秘書等が逮捕された。

セ **4日**：ロシアの下院投票日に複数のラジオ局や野党系ニュースサイトに対してのDDoS攻撃が発生した。
Harvard University、Internet & Democracy Blog "Coordinated DDoS Attack During Russian Duma Elections"
(http://blogs.law.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/)。

セ **7日**：コンゴでGoogle等、主要なWebサイトに対するDNSキャッシュポイズニングが観測された。

脆 **7日**：Adobe Reader及びAcrobatに未修正の脆弱性が発見された。
「APSA11-04：Adobe Reader および Acrobat に関するセキュリティ情報」(http://kb2.adobe.com/jp/cps/926/cpsid_92600.html)。

セ **9日**：オランダKPN社の子会社の認証局で、不適切な設定によるデータベースへの侵入事件が発生した。
Sophos、nakedsecurity "Second Dutch security firm hacked, unsecured phpMyAdmin implicated"
(http://nakedsecurity.sophos.com/2011/12/08/second-dutch-security-firm-hacked-unsecured-phpmyadmin-implicated/)。

脆 **13日**：Oracle社からJava SE 6u30がリリースされた。
"Update Release Notes JavaTM SE 6 Update 30"(http://www.oracle.com/technetwork/java/javase/6u30-relnotes-1394870.html)。

脆 **14日**：Microsoft社は2011年12月のセキュリティ情報を公開し、3件の緊急と10件の重要な更新をリリースした。
「2011年12月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms11-dec)。

セ **14日**：GMOグローバルサイン社は2011年9月に判明したComodohackerによる不正アクセスについての最終報告を公表した。
「不正アクセスに関する調査と分析についての最終報告」(http://jp.globalsign.com/information/important/2011/12/399.html)。

他 **15日**：警察庁はインターネットバンキングでのフィッシング事件や不正アクセス禁止法違反等事件の発生状況について公表した。
「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)。

脆 **16日**：Adobe Reader 9及びAcrobat 9の公開されていた脆弱性が修正された。
「APSB11-30：Windows版 Adobe Reader 9.x および Acrobat 9.x に関するセキュリティアップデート公開」
(http://kb2.adobe.com/jp/cps/927/cpsid_92703.html)。

脆 **20日**：DNSキャッシュサーバのUnboundにサービス不能の脆弱性が見つかり、修正された。
"Unbound denial of service vulnerabilities from nonstandard redirection and denial of existence [VU#209659 CVE-2011-4528]"
(http://www.unbound.net/downloads/CVE-2011-4528.txt)。

セ **20日**：北朝鮮総書記死去のニュースに便乗した標的型攻撃が確認された。
IBM Tokyo SOC Report、「北朝鮮総書記死去のニュースに便乗した標的型メールを確認」
(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/targeted_attack_20111220?lang=ja_jp)。

他 **22日**：内閣官房情報セキュリティセンターより、標的型攻撃によるネットワーク利用者を管理するサーバへの攻撃について注意喚起が行われた。
内閣官房情報セキュリティセンター、「標的型攻撃対策としての適切な管理者権限管理について」
(http://www.nisc.go.jp/press/pdf/hyoutekigata_press.pdf)。

他 **23日**：ドメイン登録業者の米国Go Daddyグループが反対運動を受けてSOPAへの支持を撤回すると発表した。
"Go Daddy No Longer Supports SOPA"(http://www.godaddy.com/newscenter/release-view.aspx?news_item_id=378)。

セ **26日**：Anonymousが米大手シンクタンクを攻撃し、サーバに登録されていた個人情報が流出した。

脆 **29日**：ドイツで行われたセキュリティイベントで、PHPをはじめとする多くのWebアプリケーション開発プラットフォームに対して効率的にDoS攻撃を行う手法が発表された。
28C3、"Efficient Denial of Service Attacks on Web Application Platforms"
(http://events.ccc.de/congress/2011/Fahrplan/attachments/2007_28C3_Effective_DoS_on_web_application_platforms.pdf)。

セ **29日**：AnonymousがSOPAに関連してソニーに対する攻撃(OpSony)を再び実施すると公表した。

脆 **30日**：Microsoft社は、.NET Frameworkに任意のコード実行を含む脆弱性が見つかり、修正をリリースした。
「マイクロソフト セキュリティ情報 MS11-100 - 緊急 .NET Framework の脆弱性により、特権が昇格される (2638420)」
(http://technet.microsoft.com/ja-jp/security/bulletin/MS11-100)。

[凡例] 脆 脆弱性　セ セキュリティ事件　動 動静情報　歴 歴史　他 その他

※日付は日本標準時

■ Duquマルウェア

Duquと命名されたマルウェアがStuxnetに酷似した構造を持つことが発見されました[*31]。Stuxnetは2010年に見つかった特定の産業用制御システムを対象に感染するマルウェアで、その感染対象の独自性と複雑な構造で話題となりました。今回発見されたDuquは産業用システムを対象とはしておらず、感染させたPC内の情報を盗むという活動をします。その後の分析で用いられたドライバファイルに盗まれた複数の電子署名が使われていること[*32]や、感染にWindowsカーネルの未修整の脆弱性を利用していることが判明しました[*33]。

■ DNSキャッシュポイズニング

ブラジルで大規模なDNSキャッシュポイズニングが発生し、銀行のIDやパスワードを狙ったトロイの木馬をインストールさせようとする事件が発生しました[*34]。また、コンゴでも主要なWebサイトに対するDNSキャッシュポイズニングが観測されました。DNSはインターネットを利用する上で欠かせない仕組みの1つであり、DNSキャッシュポイズニングが成功した場合、不正なサイトへ誘導されたり、Webやメールの盗聴・改ざんといった重大な問題が発生します。

■ スマートフォンアプリの問題とマルウェアの拡大

スマートフォンの普及に伴い、これらを対象としたマルウェアも複数発見されています。その目的として端末内の情報や金銭を狙ったものが増えてきています。特に海外においては、Androidを対象としてプレミアムSMS[*35]を悪用するマルウェアが多く発生しており、中には公式アプリとしてマーケットで配布される事例[*36]も出てきています。

また、一般のアプリにおける利用者情報の取り扱いについて、問題となることが増えてきました。CarrierIQという端末の情報を取得して携帯キャリア側で情報を収集するツールが、複数のスマートフォンにプリインストールされていることが判明し、ユーザ側が知らないうちに様々な情報を送信していたことから問題となりました[*37]。更にアプリを作成するときに利用するSDKについても、必要以上のアクセス権を要求したり、場合によっては利用者が意図しない利用者情報の外部送信等をするものが見つかり話題となりました。

このような問題に対し、総務省の研究会「スマートフォン・クラウドセキュリティ研究会」[*38]では、12月に中間報告をまとめ[*39]、スマートフォンの情報セキュリティレベルの向上のために早急に講ずべき対策について公開しています。

■ その他の動向

IPAによる標的型攻撃の分析レポートが発行され、実際に標的型攻撃に悪用されたメールについて事例を詳細に紹介しています[*40]。また、同じくIPAの「新しいタイプの攻撃」の脅威とその対策をまとめたガイドラインが改訂され、「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド改定第2版」として公開されました[*41]。また同時に、第1版の英語版も公開されています。

---

*31 このマルウェアはハンガリーの大学の研究室であるCrySySで最初に発見された。Budapest University of Technology and Economics, Laboratory of Cryptography and Systems Security(CrySyS)"Duqu: A Stuxnet-like malware found in the wild" (http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf)。

*32 署名には台湾のメーカから盗まれた鍵やSymantec社の顧客から盗まれたコードサイニング証明書が用いられた。経緯については次のSymantec Authentication (Business)Blogに詳しい。"Duqu: Protect Your Private Keys"(http://www.symantec.com/connect/blogs/duqu-protect-your-private-keys)。

*33 Microsoft社は2011年12月の更新でこの脆弱性の修正を行った。「マイクロソフトセキュリティ情報 MS11-087 - 緊急Windowsカーネルモードドライバーの脆弱性により、リモートでコードが実行される(2639417)」(http://technet.microsoft.com/ja-jp/security/bulletin/MS11-087)。

*34 Kaspersky Lab SECURELIST Blog、"Massive DNS poisoning attacks in Brazil"(http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil)。

*35 プレミアムSMSとはSMS(Short Message Service)を利用して課金を行う仕組み。通常はユーザが課金確認のメッセージに返信することで課金が発生する。

*36 エフセキュアブログ、「Androidマーケットの詐欺アプリ」(http://blog.f-secure.jp/archives/50644769.html)。

*37 この件については、例えば次の発見者のblog等が参考となる。Android Security Test "CarrierIQ"(http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/)。

*38 総務省、「『スマートフォン・クラウドセキュリティ研究会』の開催」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_01000009.html)。

*39 総務省、「『スマートフォン・クラウドセキュリティ研究会』の中間報告の公表」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000015.html)。

*40 IPA、「IPAテクニカルウォッチ『標的型攻撃メールの分析』に関するレポート」(http://www.ipa.go.jp/about/technicalwatch/20111003.html)。

*41 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)。

1.3 インシデントサーベイ

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が日常的に発生しており、その内容は多岐にわたります。しかし、攻撃の多くは、脆弱性等の高度な知識を利用したものではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にすることでサービスの妨害を狙ったものです。

■ 直接観測による状況

図-2に、2011年10月から12月の期間にIIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。ここでは、IIJ DDoS対策サービスの基準で攻撃と判定した通信異常の件数を示しています。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、攻撃の実態を正確に把握することが困難なため、この集計からは除外しています。

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*42]、サーバに対する攻撃[*43]、複合攻撃(1つの攻撃対象に対し、同時に数種類の攻撃を行うもの)の3種類に分類しています。

この3ヵ月間でIIJは、450件のDDoS攻撃に対処しました。1日あたりの対処件数は4.9件で、平均発生件数は前回のレポート期間と比べて減少しています。DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0%、サーバに対する攻撃が79.3%、複合攻撃が20.7%でした。

今回の対象期間で観測された中で最も大規模な攻撃は、複合攻撃に分類されるもので、最大3万1,764ppsのパケットによって157Mbpsの通信量を発生させる攻撃が14時間10分継続しました。攻撃の継続時間は、全体の86.7%が攻撃開始から30分未満で終了し、11.8%が30分以上24時間未満の範囲に分布しており、24時間以上継続した攻撃は1.5%でした。なお、今回もっとも長く継続した攻撃は、サーバに対する攻撃に分類されるもので39時間26分にわたりました。12月に複合攻撃の割合が期間中の他の月と比べ、大きく増加していますが、これは一部の攻撃先に対し、主に中国からの断続的な攻撃が続いていたためです。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング[*44]の利用や、DDoS攻撃を行うための手法としてのボットネット[*45]の利用によるものと考えられます。

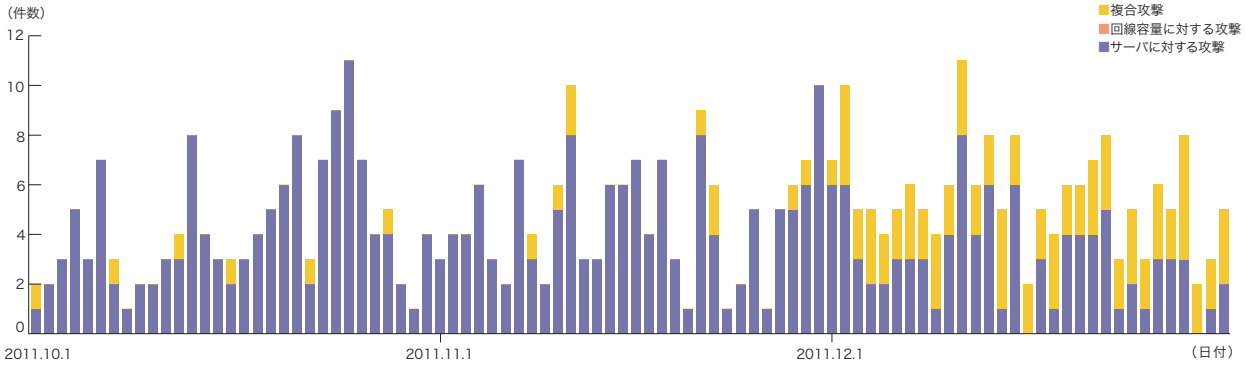


図-2 DDoS攻撃の発生件数

＊42 攻撃対象に対し、本来不必要な大きなサイズのIPパケットやその断片を大量に送りつけることで、攻撃対象の接続回線の容量を圧迫する攻撃。UDPパケットを利用した場合にはUDP floodと呼ばれ、ICMPパケットを利用した場合にはICMP floodと呼ばれる。

＊43 TCP SYN floodやTCP connection flood、HTTP GET flood攻撃等。TCP SYN flood攻撃は、TCP接続の開始の呼を示すSYNパケットを大量に送付することで、攻撃対象に大量の接続の準備をさせ、対象の処理能力やメモリ等を無駄に利用させる。TCP connection flood攻撃は、実際に大量のTCP接続を確立させる。HTTP GET flood攻撃は、Webサーバに対しTCP接続を確立したのち、HTTPのプロトコルコマンドGETを大量に送付することで、同様に攻撃対象の処理能力やメモリを無駄に消費させる。

＊44 発信元IPアドレスの詐称。他人からの攻撃に見せかけたり、多人数からの攻撃に見せかけたりするために、攻撃パケットの送出時に、攻撃者が実際に利用しているIPアドレス以外のアドレスを付与した攻撃パケットを作成、送出すること。

＊45 ボットとは、感染後に外部のC&Cサーバからの命令を受けて攻撃を実行するマルウェアの一種。ボットが多数集まって構成されたネットワークをボットネットと呼ぶ。

■ backscatterによる観測

次に、IIJでのマルウェア活動観測プロジェクトMITFのハニーポット[*46]によるDDoS攻撃のbackscatter観測結果を示します[*47]。backscatterを観測することで、外部のネットワークで発生したDDoS攻撃の一部を、それに介在することなく第三者として検知できます。

2011年10月から12月の期間中に観測したbackscatterについて、発信元IPアドレスの国別分類を図-3に、ポート別のパケット数推移を図-4にそれぞれ示します。

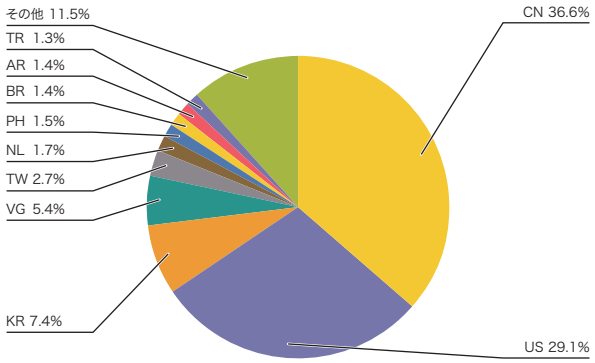


図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類

観測されたDDoS攻撃の対象ポートのうち最も多かったものは、Webサービスで利用される80/TCPで、対象期間における全パケット数の53.7%を占めています。また、リモートデスクトップで利用される3389/TCPや、リモートアクセスVPNのPPTPで利用される1723/TCP、FTPで利用される21/TCP等への攻撃も観測されています。図-3で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、中国36.6%、米国29.1%が比較的大きな割合を占めており、以下その他の国々が続いています。

特に多くのbackscatterを観測した場合について、攻撃先のポート別にみると、まず、米国内にある中国語ニュースサイトのWebサーバ(80/TCP)への攻撃が10月7日に観測されています。10月14日から19日にかけて中国国内のサーバに対する46045/TCPと46049/TCPへの攻撃が観測されました。また、10月25日には80/TCPへの攻撃が多く観測されましたが、これらは中国国内のサーバを対象にした攻撃と、英領バージン諸島にある動画ストリーミングサイトのWebサーバを対象にした攻撃でした。後者のWebサーバ(80/TCP)への攻撃は、10月から11月にかけて断続的に観測されています。11月23日にも80/TCPへの攻撃が多く観測されていますが、ほとんどは米国内のホスティング事業者が持つIPアドレスを攻撃対象としたものでした。他にも、米国オンラインストアのWebサーバ(80/TCP)に対する攻撃が10月末からクリスマス直前まで継続して観測されています。

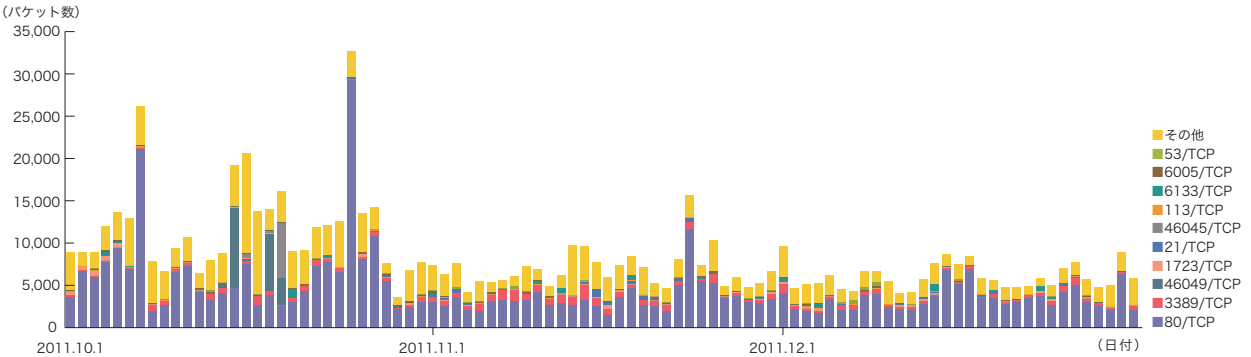


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

＊46 IIJのマルウェア活動観測プロジェクトMITFが設置しているハニーポット。「1.3.2 マルウェアの活動」も参照。
＊47 この観測手法については、本レポートのVol.8(http://www.iij.ad.jp/development/iir/pdf/iir_vol08.pdf)の「1.4.2 DDoS攻撃によるbackscatterの観測」で仕組みとその限界、IIJによる観測結果の一部について紹介している。

1.3.2 マルウェアの活動

ここでは、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*48]による観測結果を示します。MITFでは、一般利用者と同様にインターネットに接続したハニーポット[*49]を利用して、インターネットから到着する通信を観測しています。そのほとんどがマルウェアによる無作為に宛先を選んだ通信か、攻撃先を見つけるための探索の試みであると考えられます。

■ 無作為通信の状況

2011年10月から12月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に、その総量(到着パケット数)の推移を図-6にそれぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均をとり、到着したパケットの種類(上位10種類)ごとに推移を示しています。また、この観測では、MSRPCへの攻撃のような特定のポートに複数回の接続を伴う攻撃は、複数のTCP接続を1回の攻撃と数えるように補正しています。

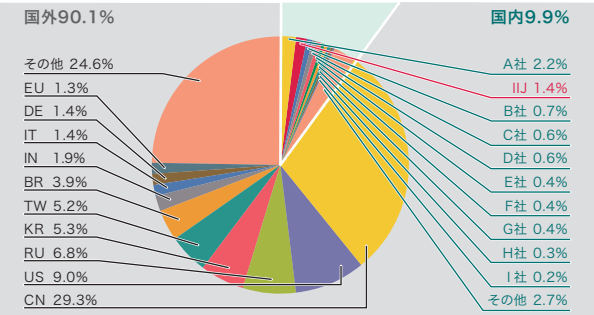


図-5 発信元の分布(国別分類、全期間)

ハニーポットに到着した通信の多くは、Microsoft社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQL Serverで利用される1433/TCPやWindowsのリモートログイン機能であるRDPで利用される3389/TCP、RAdminと呼ばれるWindows用リモート管理ソフトが使用する4899/TCPへの通信、SSHで利用される22/TCPに対する探索行為も観測されています。これらに加えて、2582/TCP、26723/TCP等、一般的なアプリケーションでは利用されない目的不明な通信も観測されました。図-5で発信元の国別分類を見ると、中国の23.9%、日本国内の9.9%、米国の9.0%が比較的大きな割合を占めています。

SSHの辞書攻撃と思われる通信も断続的に発生しており、例えば10月7日に米国、11月16日、21日に韓国、11月30日に中国、12月23日に韓国と中国のIPアドレスからそれぞれ集中的に通信が発生しています。また11月4日には、2582/TCPの通信がみられなくなり、これに関する原因は不明ですが、2582/TCPの95.6%が日本国内からの通信であるため、日本固有のアプリケーションからの通信ではないかと推測しています。RDPについては前号で紹介したMortoワームの活動が活発化して以降、上位10位以内に現れるようになっています。特に本期間中は中国からの接続が大部分を占めていました。

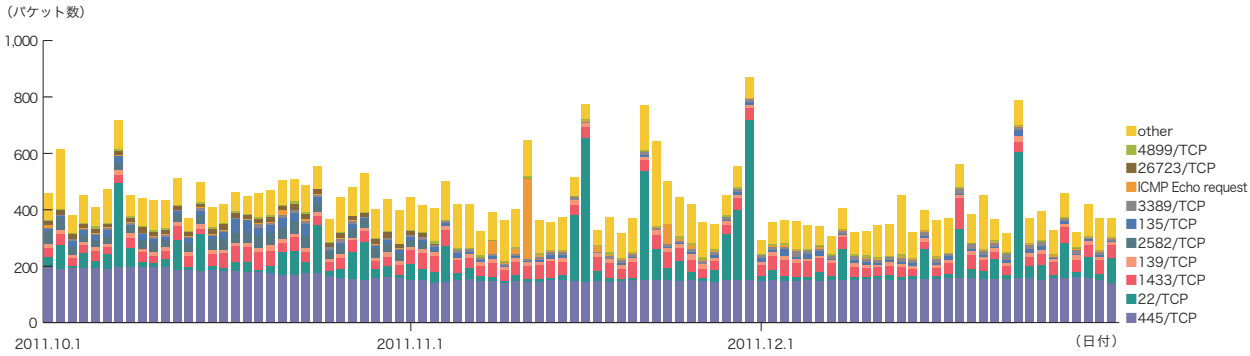


図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

＊48 Malware Investigation Task Forceの略。MITFは2007年5月から開始した活動で、ハニーポットを用いてネットワーク上でマルウェアの活動の観測を行い、マルウェアの流行状況を把握し、対策のための技術情報を集め、対策につなげる試み。

＊49 脆弱性のエミュレーション等の手法で、攻撃を受けつけて被害に遭ったふりをし、攻撃者の行為やマルウェアの活動目的を記録する装置。

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの検体取得元の分布を図-7に、マルウェアの総取得検体数の推移を図-8に、そのうちのユニーク検体数の推移を図-9にそれぞれ示します。このうち図-8と図-9では、1日あたりに取得した検体[*50]の総数を総取得検体数、検体の種類をハッシュ値[*51]で分類したものをユニーク検体数としています。また、検体をウイルス対策ソフトで判別し、上位10種類の内訳をマルウェア名称別に色分けして示しています。なお、図-7から図-9は前回同様に複数のウイルス対策ソフトウェアの検出名によりConficker判定を行い、Confickerと認められたデータを除いて集計しています。

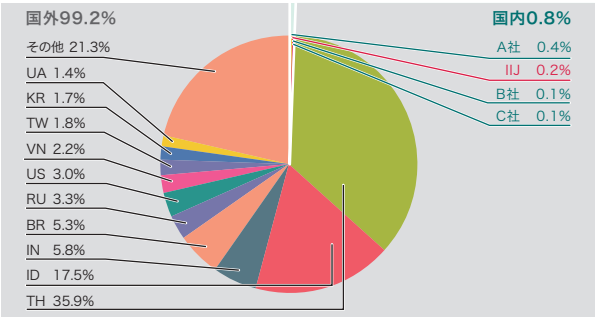


図-7 検体取得元の分布(国別分類、全期間、Confickerを除く)

期間中での1日あたりの平均値は、総取得検体数が343、ユニーク検体数が32でした。図-7では、タイ及びインドネシアからの検体取得の割合がそれぞれ35.9%、17.5%と多くの割合を占めています。

MITFの独自の解析では、今回の調査期間中に取得した検体は、ワーム型66.7%、ボット型25.3%、ダウンローダ型8.0%

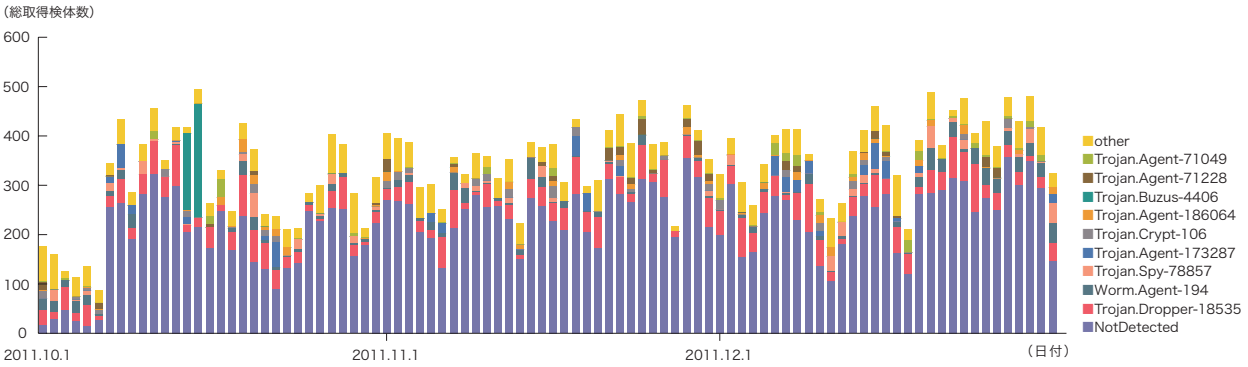


図-8 総取得検体数の推移(Confickerを除く)

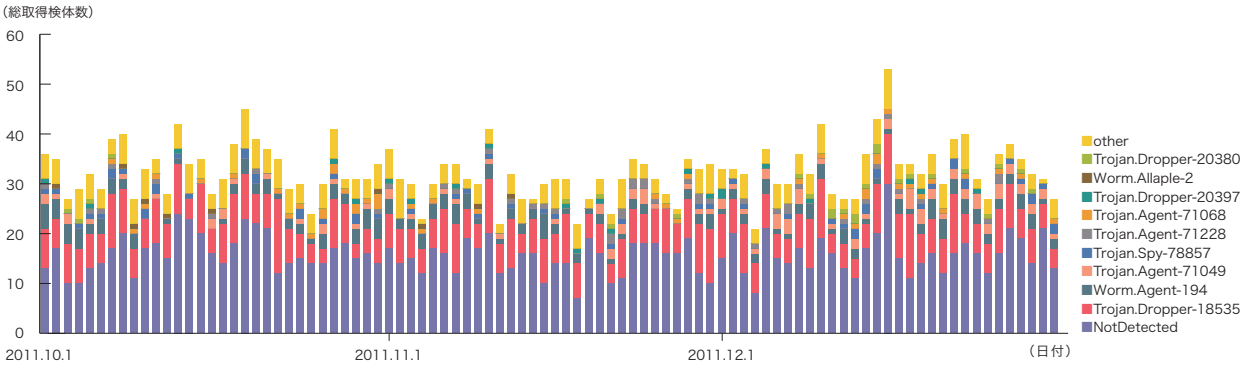


図-9 ユニーク検体数の推移(Confickerを除く)

＊50 ここでは、ハニーポット等で取得したマルウェアを指す。

＊51 様々な入力に対して一定長の出力をする一方向性関数(ハッシュ関数)を用いて得られた値。ハッシュ関数は異なる入力に対しては可能な限り異なる出力を得られるよう設計されている。難読化やパディング等により、同じマルウェアでも異なるハッシュ値を持つ検体を簡単に作成できてしまうため、ハッシュ値で検体の一意性を保証することはできないが、MITFではこの事実を考慮したうえで指標として採用している。

でした。また解析により、21個のボットネットC&CサーバとC&C[*52]と17個のマルウェア配布サイトの存在を確認しました。

■ タイ及びインドネシアからの未知の検体の増加

図-10において10月7日以降に観測され、大きな割合を占めている未知の検体(NotDetected)は、大部分がタイとインドネシアから取得されており、未知の検体全体に対する割合は、それぞれタイが55.4%、インドネシアが26.4%でした。また、これらの検体の内訳は実行形式のファイルが93.4%、HTML、XML等のテキスト形式のファイルが6.6%でした。

より詳しい調査の結果、IRCサーバで制御されるタイプのボット2種類[*53][*54]が活発に活動していたことが分かりました。ハッシュ値による分類では、個々の検体は1日から2日間程度の短い期間のみ活動していたことが観測されています。

■ Confickerの増減

図-11はConfickerを含めた同じ期間中でのマルウェアの総取得検体数の推移を示したものです。Confickerの割合は、全体の99.3%と依然として高い水準を保っています。Confickerは長期間の観測結果から今も活発に活動しており、増減を繰り返していることが分かります。この期間中はロシア、ブラジル、台湾等でこのような増加傾向が顕著に現れていましたが、日本や米国では増減は見られませんでした。このように、各国に割り当てられているIPアドレスによって活動の傾向が異なっています。

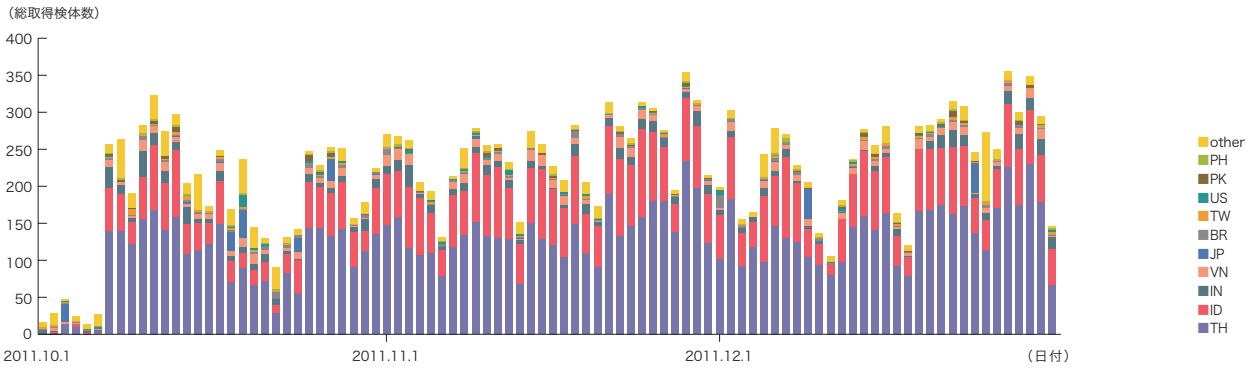


図-10 取得検体数の推移(未検出の検体の国別で分類)

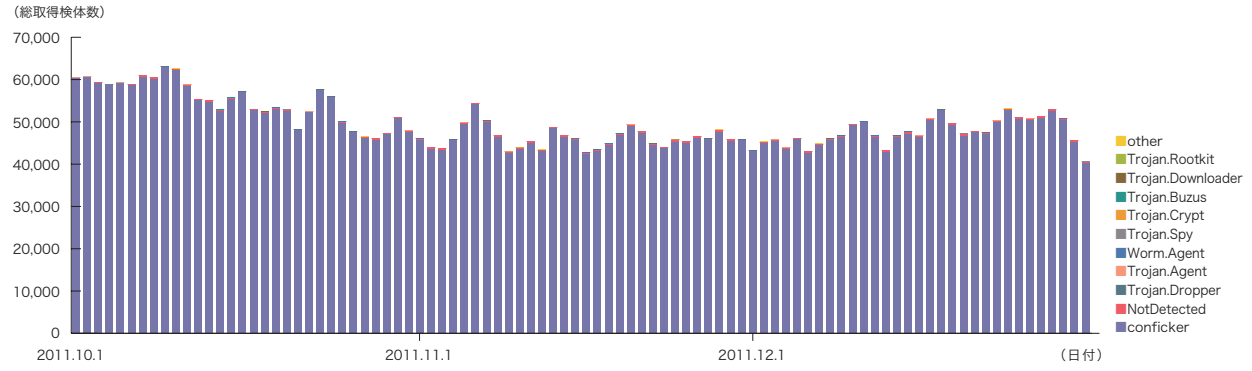


図-11 総取得検体数の推移(Confickerを含む)

＊52 Command & Controlサーバの略。多数のボットで構成されたボットネットに指令を与えるサーバ。
＊53 Trojan : Win32/Ircbrute(http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute)。
＊54 Win32/Hamweq(http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq)。

1.3.3 SQLインジェクション攻撃

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃[*55]について継続して調査を行っています。SQLインジェクション攻撃は、過去にもたびたび流行し話題となった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

2011年10月から12月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-12に、攻撃の推移を図-13にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、日本48.2%、中国16.0%、米国9.0%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生件数は前回からあまり変化していません。

この期間中、10月10日に発生した攻撃は、米国の特定の攻撃元から特定の攻撃先に対するものでした。また、11月30日から12月2日にかけて発生した継続的な攻撃は、主に中国の複数の攻撃元から複数の攻撃先に対するものでした。どちらの攻撃についても、同じ手法の攻撃を繰り返し行っており、Webサーバの脆弱性を探る試みであったと考えられます。

ここまでに示したとおり、各種の攻撃はそれぞれ適切に検出され、サービス上の対応が行われています。しかし、攻撃の試みは継続しているため、引き続き注意が必要な状況です。

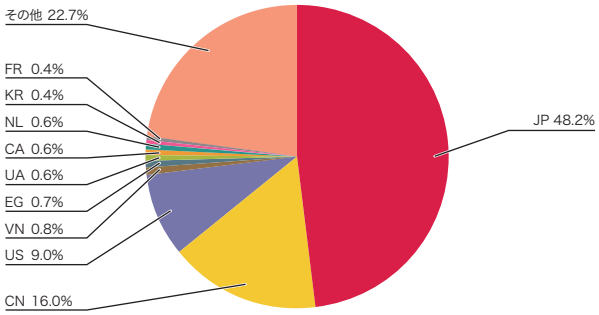


図-12 SQLインジェクション攻撃の発信元の分布

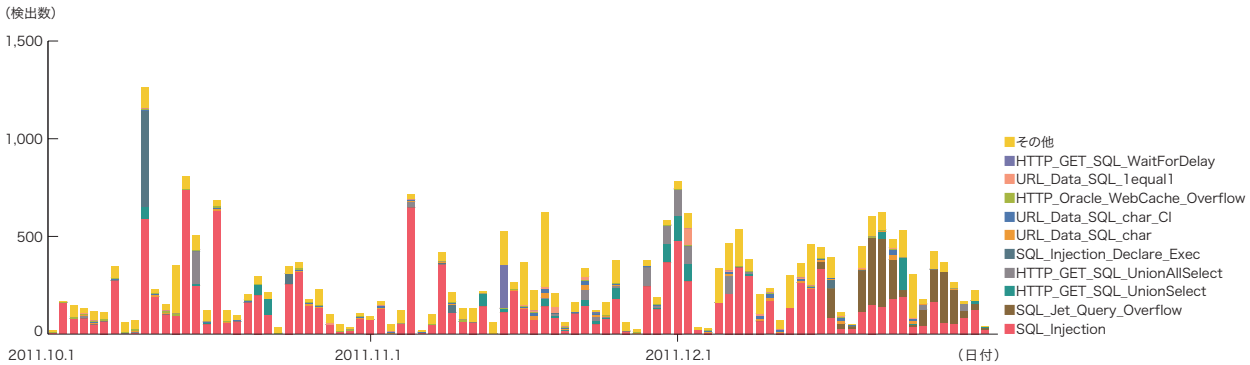


図-13 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*55 Webサーバに対するアクセスを通じて、SQLコマンドを発行し、その背後にいるデータベースを操作する攻撃。データベースの内容を権限なく閲覧、改ざんすることにより、機密情報の入手やWebコンテンツの書き換えを行う。

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、公開鍵証明書発行に関する事件、標的型攻撃とその対応について解説します。

1.4.1 公開鍵証明書発行に関するいくつかの問題

本節では、前号[*56]で紹介したような侵入事件が別の認証機関で発生している事例と、認証機関の発行ポリシーの問題に起因する署名付マルウェアの事例、これらPKIにおける課題に対する業界の対策活動について紹介します。

■ 前号で紹介した不正発行事件について

2011年8月に明らかになったDigiNotar社の事件に関連して、9月に同社が自己破産申告を行いました。当初のプレスでは認証機関業務に関する上半期の収益は10万ユーロ以下であり、侵入事故の影響は軽微なものであるとの見解でしたが、実際には、負債額が3,300万から4,800万米ドルと試算されており、認証機関における信頼失墜が事業そのものに非常に大きな影響を及ぼした事例となりました[*57]。

また、ComodoHackerによる犯行声明において、システムへの不正アクセスが可能であったと名指しされたGMOグローバルサイン社は、調査のため9月6日から15日の間、新規証明書の発行を一時的に停止し、サービス再開にあたり全顧客のアカウントのパスワードをリセットする対策を講じました。12月に公開された最終報告では証明書発行システムには被害がなかったことが報告されていますが、全サービスにおける通常業務再開は10月中旬にまで及ぶといった影響が出ています[*58]。

■ オランダの認証機関における侵入事件

2011年11月、KPN社が運営するオランダの認証機関サービスGemnetが、証明書発行システムへの侵入の痕跡が見つかったため証明書発行業務を停止しました[*59]。サーバログによると4年以上も前に仕組まれていたとの報告がなされています[*60]。11月4日の報告後、9日には部分的に発行業務を再開しています。

KPN社は一般ユーザ向けの証明書の発行業務だけではなく、政府向けの証明書の発行業務を行っています。DigiNotar社と同様に、オランダ政府が利用する認証機関の1つとして認定されている事実[*61]も問題視されています。実際、DigiNotar社での不正発行事件で被害を受けた多くの組織が、KPN社発行の証明書に切り替えていました[*62]。

■ マレーシアの認証機関における発行ポリシーの問題

2011年11月、マレーシアの認証機関DigiCert Sdn. Bhd.社がRSA512ビット鍵に対する証明書、及びExtended Key Usage拡張を含まない証明書を発行しており、これはCPS（Certification Practice Statement：認証機関運用規程）に違反した発行であったとEntrust社が報告しました[*63]。これらの違反した証明書は22枚に及び、DigiCert Sdn. Bhd.社は問題が指摘された中間CA（識別名：Digisign Server ID - (Enrich)）から発行されている512及び1024ビットのRSA鍵を持つ証明書を2048ビットに差し替える方針を打ち出しています。

一方で上位のルート認証機関を運営するEntrust社はこのDigiCert Sdn. Bhd.社による解決に向けた方針が公開されるよりも早い段階で、遅くとも11月8日までに中間CA証明書を無効にする方針が取られています。この厳しい措置はDigiNotar社等の失敗事例を鑑みた方針であったと考えられます。

＊56 IIR Vol.13「1.4.3 公開鍵証明書の不正発行事件」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol13.pdf)。
＊57 SANS ISC Diary、"Diginotar declared bankrupt"(http://isc.sans.edu/diary.html?storyid=11614)。
＊58 GMOグローバルサイン社、「通常業務再開のご連絡」(http://jp.globalsign.com/information/important/2011/10/388.html)。
＊59 KPN社、"KPN stopt uit voorzorg uitgifte nieuwe veiligheidscertificaten"(https://www.kpn.com/corporate/overkpn/Newsroom/nieuwsbericht/KPN-stopt-uit-voorzorg-uitgifte-nieuwe-veiligheidscertificaten.htm)。
＊60 SANS NewsBites - Volume: XIII, Issue: 89、"Dutch Telecom KPN Halts SSL Certificate Issuing(November 4, 6 & 7, 2011)"(http://www.sans.org/newsletters/newsbites/newsbites.php?vol=13&issue=89&rss=Y#sID300)。
＊61 オランダにおいて電子通信分野を統括する省庁であるOPTAは信頼のおける認証機関リストを作成している。OPTA "Trusted Service List"(https://www.opta.nl/en/tsl/)。
＊62 Kaspersky Lab社、「11月のマルウェア：DuquとStuxnetの類似性、認証機関の信用低下」(http://www.kaspersky.co.jp/news?id=207582793)。
＊63 "Entrust Bulletin on Certificates Issued with Weak 512-bit RSA Keys by Digicert Malaysia"(http://www.entrust.net/advisories/malaysia.htm)。

今回のDigiCert Sdn. Bhd.社において発覚した問題はComodo社やDigiNotar社等で起きた不正発行事件ではありません。しかし、証明書を利用しその内容の確からしさを検証するユーザにおいては、不正に証明書を発行された場合と同様の影響を及ぼしかねません。一般ユーザが証明書の確からしさを検証する場面としては、ブラウザを用いたSSL/TLS通信が多いと考えられます。そのため、各種主要ブラウザベンダーでは、今回の問題に対し、中間CA証明書やその下位証明書を失効させる、つまりブラックリストに載せることで当該証明書の利用を禁止する措置が取られました。

今回無効処理された証明書には、以下に示すように3つの独立した問題がありました。以下それぞれの問題について解説します。

■ 問題1：暗号アルゴリズムの危殆化と公開鍵の鍵長

一般的な証明書発行手順において、証明書の発行対象が証明書発行依頼を行う場合、CSR(Certificate Signing Request)と呼ばれる申請データを認証機関に提出します。認証機関が証明書を発行する際には、CSRに含まれる公開鍵やX.509識別名(Distinguished Name)をチェックします。今回の問題は、認証機関が鍵長に関するポリシーを持っていない、更に鍵長についてチェックしていないことが原因であると指摘されています[*64]。また、EFF(Electronic Frontier Foundation)による公開鍵証明書データベースThe EFF SSL Observatory[*65]を探索することにより、公開鍵がRSA512ビット鍵である証明書がDigiCert Sdn. Bhd.社以外の認証機関からも発行されていたという事実も明らかになりました。RSA512ビット公開鍵による署名・暗号化が信頼できないという背景のひとつには、RSA768ビット公開鍵が既に素因数分解されていることが挙げられます[*66]。現在RSA1024ビット公開鍵も利用されていますが、2048ビットへの移行が推奨されています。

DigiCert Sdn. Bhd.社の緊急対策では、公開鍵暗号アルゴリズムRSAの鍵長だけに着目されていますが、暗号アルゴリズムの危殆化[*67]に関連してデジタル署名に用いられるハッシュ関数アルゴリズムについても留意すべきです。具体的には、MD5の危殆化に伴ってMD5を利用したデジタル署名による証明書は、既に安全ではないという認識ができつつあります。また、現在主流のSHA-1も脆弱であることが指摘されていることから、SHA-2を利用した署名を持つルート証明書への移行が進んでいます。移行にはサーバ、クライアント双方の対応が必要ですが、Webサーバでの対応や証明書のトライアル、更に携帯電話でのSHA-2ルート証明書搭載が報道されており、着実に移行が進んでいることを示しています。

なお、暗号アルゴリズムの移行問題[*68]に関しては、米国の移行計画を一部修正したSP 800-131Aが発表され、各暗号アルゴリズムに関して具体的な指示が与えられました。この文書では当該アルゴリズム(と鍵長)の扱いについて、Acceptable(利用可能)とDisallowed(利用禁止)だけでなくDeprecated(リスクを許容してなら利用可能)やRestricted(制約付きなら利用可能)という状態も定義され、時期に応じて状態が経年変化するように設計されています。

■ 問題2：目的外利用

問題が指摘されている中間CAから発行された政府機関への証明書のうち、マレーシアの政府関連組織のドメイン配下であるanjungnet.mardi.gov.myに対して発行された証明書がAdobe Readerの脆弱性を利用したマルウェアに対して署名を行っているという報告がなされました[*69]。この報告が指摘された時点では既に証明書の有効期限が切れていましたが、署名された8月24日から有効期限の9月29日までの間は、署名検証機能があるOSでも警告なしにマルウェアがインストールされた可能性があります。

＊64 FOX-IT、"RSA-512 Certificates abused in the wild"(http://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/)。
＊65 The EFF SSL Observatory (http://eff.org/observatory)。HTTPSサーバで利用されている公開鍵証明書を広く収集するプロジェクト。CAが発行する証明書に問題がないか監視することを目的にデータセットを公開している。この活動は2010年7月に開催されたDEFCON18で初めて紹介された(https://www.eff.org/files/DefconSSLiverse.pdf)。
＊66 Thorsten Kleinjung et.al、"Factorization of a 768-bit RSA modulus"(http://eprint.iacr.org/2010/006)。
＊67 暗号アルゴリズムの危殆化については、IIR Vol.8「1.4.1 暗号アルゴリズムの2010年問題の動向」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol08.pdf)で紹介している。
＊68 NIST、"SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011"(http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf)。
＊69 エフセキュアブログ、「政府の署名鍵で署名されたマルウェア」(http://blog.f-secure.jp/archives/50638015.html)。

本証明書はRSA512ビットの公開鍵に対するものであったことも問題であると同時に、証明書の用途が制限されていなかったことも問題であることが指摘されています[*70]。証明書の用途を制限する仕組みとしては、X.509 v3拡張の1つであるExtended Key Usage拡張があります。この拡張はRFC5280で規定されており、SSL、code signing、S/MIME等の用途を証明書内に記載することで、利用用途を制限できます。この制限を設ける、つまり本来のサーバ証明書の用途であるSSL通信にのみ制限していれば、検証時に目的外利用であることが検知でき、マルウェアのインストールを防ぐことが可能であったと考えられます。

■ 問題３：証明書の廃棄情報参照先の欠如

公開鍵証明書には、同じ公開鍵を利用し続けることによる暗号危殆化の影響やPKIビジネスモデル上の観点から有効期限が設けられており、1年から数年、ルート証明書の中にはトラストアンカーの差し替えコストを鑑み10年以上の期間、同じ証明書及びそれに対応する秘密鍵が利用されています。一方で、有効期限内に証明書を無効にする仕組みも設けられています。無効にする理由として、秘密鍵の漏えい等が想定されており、オフラインでも検証が可能なCRL（Certificate Revocation List：期限内に無効とする証明書のシリアル番号が列挙されたデータにCAが署名したデータ）とOCSP（Online Certificate Status Protocol：RFC2560で規定されている証明書の失効状態をオンラインで確認するプロトコル）が広く利用されています。

通常、CRLに関する情報はCRL Distribution Points拡張に、またOCSPに関する情報はAuthority Information Access拡張に記載されていることが前述したRFC5280で規定されています。今回問題となった証明書には、これらの証明書有効性を確認する手段に関する情報が含まれていませんでした。そのため認証機関が当該証明書を無効化したと宣言していても、ブラウザ等のアプリケーションにて証明書が廃棄されているかどうかチェックを行うことができず、既に無効な証明書が受け入れられ、処理されてしまう点が問題と考えられます。

■ PKI業界全体の信頼回復のために

今回取り上げたKPN社やDigiCert Sdn. Bhd.社の事件が発生した2011年11月に、PKI業界全体の信頼回復を目指したアクティビティが発表されました。それは、より厳しい発行審査に関する業界統一基準[*71]により発行されるEV SSL証明書の策定を行っているCA/Browser Forumが採択したベースライン要件書[*72]です。11月22日に採択された本文書は2012年7月より施行されることが決まっており、この準備期間中に本フォーラムに参加している企業による実施が期待されています。

要件書にはEV SSL証明書に対する発行要件と同様に、暗号アルゴリズムや鍵長に関する制限や、X.509 v3拡張に関する制限についても、Normativeという位置付けながら規定されています。ここまでに紹介した諸問題を解決する証明書拡張である、Extended Key Usage拡張、CRL Distribution Points拡張、Authority Information Access拡張に、それぞれ記載されるべき内容や、その処理に関しても規定があり、サービスや製品によらず正しく処理できるよう配慮されています。

このように、証明書発行・検証・廃棄等CAが行うプロセスにおいて、満たすべき要件のベースラインを定義することで、各認証機関における発行要件のばらつきを均等化する効果が期待されています。この要件書では、証明書発行・検証機能に関する要件を定めると共に、社員教育、ログ保管、システムセキュリティやリスク評価、秘密鍵保全要件に関しても触れられています。今後も継続的にPKIビジネス信頼回復のための取り組みが行われます。

＊70 Entrust、"512-bit Certificates Abused in the Wild"（http://ssl.entrust.net/blog/?p=1041）。
＊71 CA/Browser Forum、"Guidelines For The Issuance And Management Of Extended Validation Certificates ver1.3"（http://www.cabforum.org/Guidelines_v1_3.pdf）。
＊72 CA/Browser Forum、"Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0, 22 Nov. 2011"（http://www.cabforum.org/Baseline_Requirements_V1.pdf）。

1.4.2 標的型攻撃とその対応

2011年9月に発覚した国内大手企業におけるウイルス感染事例に端を発した一連の「サイバー攻撃」報道により、標的型攻撃という攻撃手法が大きく注目されました。既にこの攻撃手法への対策を謳うセキュリティ製品やセキュリティサービスが登場しており、その多くが特に標的型攻撃メールと悪用されるマルウェアの観点からこの攻撃手法への対策を提供しています。しかし、標的型攻撃には、個別の技術的な対策だけでは防ぎきれない場合があります。ここでは、過去の事例から判明した攻撃に関する情報を元に、攻撃の流れを俯瞰することで、広範囲な対策について検討を行います。

■ 標的型攻撃とその歴史

標的型攻撃は、特定の組織や人物のみが攻撃対象となるような攻撃です。インターネット上で広く流布するWeb感染型マルウェアのように、誰もが感染する可能性のある脅威ではなく、ある時点では世界中で1つの組織だけで発生しているかもしれない事件です。このため、攻撃の発生の事実は把握しにくく、標的となった組織は、孤軍奮闘してこの問題に立ち向かわなければならない状況に追い込まれます。

攻撃の手法としては、利用者が日常的に利用するメールやIM等を悪用することが多く、そのメッセージの内容として、標的となった組織に属する利用者が興味を持ちそうな話題(攻撃の時点で大きく報道されているニュース等)や、業務上のやり取りに似せた内容を用います。これにより、添付ファイルの開封や外部のWebサーバへのアクセスを促してマルウェアに感染させます。つまり、組織内の利用者が日常的に利用する通信にマルウェアを混入することで、ファイアウォール等で構築している組織のセキュリティ境界を越えられてしまうことが、攻撃の第一歩となる場合が多く見られます。

組織のセキュリティ境界を越えた侵入者は、最初にマルウェアに感染した端末を利用して、内部のネットワークの調査を行い、目的とする情報に到達する場合があります。この場合、インターネット側にいる犯人は長い時間にわたって、組織内の感染端末と通信を行います。

標的型攻撃のもう1つの特徴として、攻撃に関する情報の共有しにくさがあります。一般のマルウェア感染事例と比べて事例の数が極端に少なく、また攻撃の発生そのものを示す情報に標的となった組織に関する情報が含まれる場合があることから、被害者が外部への情報提供をしないと判断することがあります。このため、標的型攻撃の発生状況については、インターネット全体や日本国内全体の状況を把握することが難しく、いくつか公開された事例の他には、その発生状況や被害実態もいまだによく分かっていません。

一方で、このような標的型攻撃は昨年突然発生したものではなく、その歴史は公開されているものでも2005年までさかのぼることができます[*73]。この攻撃手法が認知された時点では、ほぼすべての事例が政府官公庁関係で発生しており、国家規模の諜報活動の一環と解釈されていました。ところがこの数年、民間企業に対してこの攻撃手法が用いられている事例が発見されています。

■ 標的型攻撃の過程

ここで、この数年に発生した標的型攻撃の代表的な事例について表-1にまとめます。これらの事例をもとに、標的型攻撃の過程について検討すると、標的型攻撃は、モチベーション、攻撃の準備行為、セキュリティ境界越え、組織内ネットワークでの活動、目的の達成の5段階の過程を経ていると考えられます。以下、それぞれの段階について説明します。

■ モチベーション

標的型攻撃事例の多くは、標的とする組織から情報を盗み出すことを目的としています。目的となる情報の多くは企業秘密であり、盗み出した情報を悪用し、金銭を得たり、競争で優位に立ったりすることが本当の目的であると考えられます。次に、他の組織を攻撃するための情報を目的とした攻撃があります[*74]。EMC社の事件では、同社製品を利

＊73 例えば米国US-CERTによる"US-CERT Technical Cyber Security Alert TA05-189A Targeted Trojan Email Attacks"(http://www.us-cert.gov/cas/techalerts/TA05-189A.html)や、英国CPNIによる"TARGETED TROJAN EMAIL ATTACKS"(http://www.cpni.gov.uk/Documents/Publications/2005/2005015-BN0805_Targeted_trojan_email.pdf)等。

＊74 IPA、「標的型サイバー攻撃の事例分析と対策レポート」(http://www.ipa.go.jp/security/fy23/reports/measures/documents/report20120120.pdf)。

用する組織が最終的な標的であり、盗み出した知識を悪用して他の企業への攻撃の試みが行われたとされています。また、国内の事例では、事前に標的となる企業が加盟する業界団体に侵入し、盗んだ情報を悪用し、この２つの組織の間のメールのやりとりに割り込む形でマルウェアを添付したメールが発信されています。

最後に、標的となった企業の信用を失墜させることが目的の場合もありました。HBGary Federal社の事件は、Anonymousに関する調査結果を公表しようとしたことに対する反撃行為で、犯行声明も出ています。最終的にメールサーバに保存されていたメールがすべて盗み出され、広く公開されてしまいました。この目的のためには、盗み出す情報は「盗み出されたことがわかると恥ずかしい」情報であれば何でもよかったと考えることができます。

■ 攻撃の準備行為

標的が定まった段階で、攻撃者は標的に関する知識を様々な方法で事前に入手しているものと考えられます。例えば、インターネットにさらされたシステムの脆弱性を外部から調査することで侵入経路を見つけたり、検索エンジン等を利用して、標的とした組織で外部に公開されている窓口や、個人のメールアドレスを把握し、標的型攻撃メールの送付先として利用したりします。また、組織内で利用するアプリケーションに関する知識も攻撃に利用されやすい情報です。標的となった組織の利用者が、SNSで実名や所属組織を公開している場合、コンタクト情報や日常的な発言の様子等で、利用するアプリケーションの情報を得ることができる場合があります。更に、営業職等、名刺を広く配布する必要のある職種の場合、おのずとその名刺に記載された情報が攻撃者にわたる機会が増えることになります。

表-1 標的型攻撃の例[*75]

日 時	概 要	セキュリティ境界越えの手法	組織内ネットワークでの活動	影 響
2009年11月	Night Dragon 石油･天然ガス等エネルギー関連企業や製薬会社等複数社。	SQL インジェクションに端を発するWeb サーバへの侵入、及び改ざん。改ざんされたコンテンツへのアクセスを誘発する標的型攻撃メール。	RAT(zwShell)のインストール。管理サーバへの侵入。ネットワーク内の調査と他の端末への侵入を繰り返す。	経営者の端末から事業や入札に関する情報等の企業秘密や、メールアーカイブ等が狙われた。
2010年1月	Operation Aurora 米国国内IT系企業数十社。	Web感染型マルウェア感染に誘導するURLつきメールやIMのメッセージ。	インターネット側のC&Cサーバから制御されるマルウェアのインストール。	ソースコードの管理システムへのアクセス等、企業の知財及び関連情報の漏えい。
2011年2月	Anonymousによる HBGary Federal社への攻撃。	CMSやサーバの脆弱性の悪用、パスワードの使い回し等による侵入。	社内システムの脆弱性の悪用や、メールでの対話によって聞き出したIDとパスワードを用いた、内部サーバへの侵入。	企業秘密(メールアーカイブ)の漏えい。漏えい情報のインターネットへの公開による企業信用の失墜。
2011年3月	EMC社に対する攻撃。	採用計画に関係すると模した、一般利用者への標的型攻撃メール。	RAT(Poison Ivy)を悪用してネットワークを調査。認証情報を取得し、社内サーバへの侵入を繰り返した。	同社製品に関する秘密の漏えい。またその秘密を悪用した他社への攻撃。
2011年 4月から9月	Nitro Attacks 人権擁護団体、自動車産業、化学産業、防衛産業等の複数社。	ソフトウェアのセキュリティ更新に模した、もしくはビジネス会合の招待状に模した標的型攻撃メール。	端末への RAT(Poison Ivy)のインストール。端末の情報(パスワードハッシュ含む)を知り、近隣の端末や管理サーバへの侵入。	製品の製造工程等の機密情報が対象となった。

＊75 それぞれの攻撃については以下の情報をもとにまとめた。
Night Dragon：マカフィー株式会社「世界のエネルギー産業を狙うサイバー攻撃:“Night Dragon”」(http://www.mcafee.com/japan/security/rp_Night_Dragon.asp)。
Operation Aurora：HBGary、"HBGary Threat Report: Operation Aurora"(http://hbgary.com/hbgary-threat-report-operation-aurora)及び、IIR Vol.07「1.4.2 標的型攻撃とOperation Aurora」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol07.pdf)。
HBGary Federal："Anonymous speaks: the inside story of the HBGary hack"(http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/)。
EMC：Sophos、nakedsecurity, "RSA release a few details on their big security breach"(http://nakedsecurity.sophos.com/2011/04/04/rsa-release-details-on-security-breach/)。
Nitro Attaks：Symantec、"The Nitro Attacks Stealing Secrets from the Chemical Industry"(http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf)。

■ セキュリティ境界越え

事前に得た標的に関する知識を悪用して、セキュリティ境界を越え、組織内ネットワークに侵入しようとします。このために、業務の内容を装ったり、広く興味を引き付ける話題を含んだ文面を、メールやインスタントメッセンジャー等で送付し、受け取った組織内ネットワークの利用者の動きによりマルウェア感染を誘発します[*76]。実際、Nitro AttacksではAdobe社の製品のセキュリティ更新の注意喚起に模した内容のメールが、EMC社の事件では、翌年度の人員採用計画に関する情報を模したメールが、一般の利用者に送付されたことに端を発していたことが知られています。標的型攻撃メールやメッセージがどの程度の人数に対して送られたかは、事件によって様々です。送付量の大小にかかわらず、宛先となったうちの一人がマルウェアに感染するだけで、攻撃者は組織内ネットワークに攻撃の橋頭堡を確保し、この段階を終えたということができます。

また、インターネットに公開されているサーバの脆弱性を悪用する攻撃が発端となることもあります。Night DragonではSQLインジェクションが、HBGary Federal社ではCMSやサーバOSの脆弱性と、複数システム間でのID・パスワードの使い回しが悪用されました。

■ 組織内ネットワークでの活動

組織内ネットワークの構成や内部システムに関する情報を事前に入手している場合を除き、組織内ネットワークへの侵入後に、攻撃者はより重要なシステムへの侵入や、管理者権限を有する者や経営者等、より重要な人物の利用する端末への侵入を試みます。このために、侵入した端末上に保存されたメールや認証情報等を取得して悪用したり、認証サーバやネットワーク資源の管理サーバを攻撃したりします。実際、表-1に紹介した事件のうちのいくつかと、国内で発生した事件の多くでは、組織内のネットワークの管理をしているActive Directoryのサーバが攻撃され、管理者権限や全利用者のIDとパスワードが盗まれたとされています。

このほか、攻撃が組織内ネットワークに波及する例としては、メールサーバ(保存してあるメールを盗む)、ファイルサーバ(重要ファイルを盗む、またはマルウェアの組織内感染の拠点として利用する)等への攻撃が事例として報告されています。

またこの際、事前に組織内ネットワークへの攻撃をプログラムされたマルウェアを利用するだけではなく、RAT[*77]等のマルウェアを悪用して、インターネット側から逐次命令を送ることにより、手作業に近い形で組織内ネットワークの状況を調査することがあります。この場合、インターネット側の攻撃者と侵入された端末の間の通信が数多く、長期間にわたって発生します。攻撃者は、この通信がセキュリティ境界によって阻害されたり、即座に発見されたりすることを防ぐために、通常の端末が行う通信(HTTP、SSL、SMTP、DNS)等を悪用する場合が知られています。

■ 目的の達成

以上の手順により、攻撃者が標的とした情報にたどり着いたとき、その情報をインターネット側に送信します。いくつかの事例では、内部の侵入したサーバに盗んだ大量の情報を集め、そこからインターネット側に用意されたFTPサーバにアップロードし、その後FTPサーバ上の痕跡を削除したことが知られています。また他の事例では、情報をメールにより外部のメールアドレスに送付することで漏えいさせたことが分かっています。

■ 標的型攻撃の連接

メールによる標的型攻撃の事例には、明らかに様態の異なる2つのタイプがあることが分かっています。1つは、複数の組織の複数の人物に送付されるメールで、もう1つは非常に限定された少人数に対する標的型攻撃メールです。例えば、Nitro Attacksでは、Adobe製品のセキュリティ更新の注意喚起に模したメールが、各企業の利用者100名から500名に送付されると同時に、ビジネス会合の招待状に

＊76 国内で発生した標的型攻撃のメールの例は、次のIPAによるレポートに紹介されている。IPA テクニカルウォッチ、「『標的型攻撃メールの分析』に関するレポート ～だましのテクニックの事例4件の紹介と標的型攻撃メールの分析・対策～」(http://www.ipa.go.jp/about/technicalwatch/20111003.html)。

＊77 RATとはRemote Access TrojanhorseやRemote Access Tool等の略称で、端末の遠隔操作を行うためのツールを指す。代表的なものとしてはGh0st RATやPoison Ivy等がある。標的型攻撃では、これらのツールがそのまま、もしくは改造されて組織内ネットワークの端末を操る目的で悪用されることが多い(例えば、表-1の「組織内ネットワークでの活動」の列を参照のこと)。

模したメールが少人数に送付されたとされています。この違いは、先述の標的型攻撃の過程でも示したように、攻撃者が標的型攻撃に利用するための情報を得るために、別の標的型攻撃を仕掛ける場合があるということから説明することができます(図-15)。

一般に、攻撃者が目的とした情報に近い人物、つまり、システムに対して大きな権限を持つ管理者や企業の機密情報にアクセスできる経営者等のコンタクト情報を、組織外から知ることは困難です。攻撃者はこれらの情報を入手するために、まず、標的とする組織の一般利用者や、関連組織に対して、多くの人が興味を持つ内容のメールを利用して標的型攻撃を仕掛けます。

標的に関する情報の取得に成功すると、次の標的型攻撃が実施されます。この攻撃では、数名程度の少数の宛先に対し、先の攻撃で入手した情報、例えば、日頃メールを送り合う相手からのメールを引用した返信等が利用されます。このため、この標的型攻撃メールの受け取り手からすると、業務上のメールのやりとりが続いているように見え、マルウェア感染に誘導される可能性が高くなります。

標的型攻撃については、大企業や政府官公庁関係組織を対象にした攻撃に関する報道が続いていますが、このように様態と目的の違う攻撃があることを考慮する必要があります。つまり、標的型攻撃は、決して特殊な組織を対象とした他人事ではなく、一般の企業等も対象として発生しうる攻撃なのです。

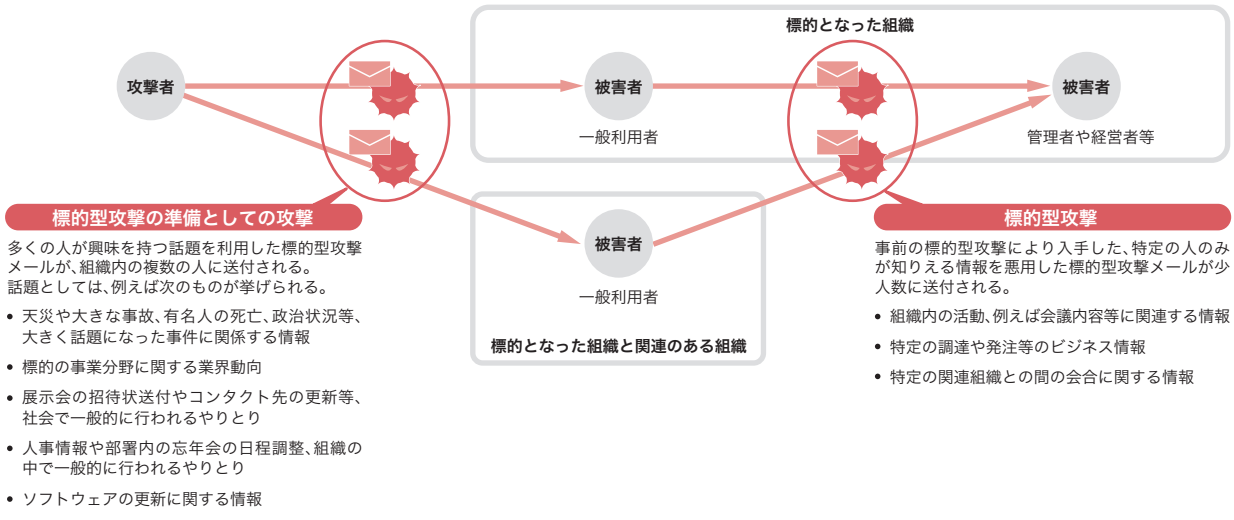
■ 標的型攻撃対策の検討

最後に、これまで紹介してきた標的型攻撃の手法や手順を元に、ここでは、標的型攻撃への対策を検討します。その検討の概要を表-2に示します。

■ 準備行為への対策

インターネット上に公開されている自組織に関する情報で、悪用される可能性のあるものを把握します。DNSやWHOISでの公開情報、公式に外部に公開している窓口のメールアドレス等だけではなく、組織内の利用者に関する情報等が公開されていないかどうかを検索エンジンやSNS等で調査します。外部に公開されていることが判明したシステムやメールアドレス等は、標的型攻撃の突破口として狙われる可能性のある入り口として重点的に保護します。また、過去に標的型攻撃を受けたことのある人については、既に何らかの情報が攻撃者にわたっていると判断できますので、同様に保護します。

また、業務上関係のある組織(業界団体や出入り業者、利用するシステムのベンダ)等が侵入され、そこで盗まれた情報が自組織への攻撃に悪用されることを想定します。業務上付



図中の矢印は実際のメール配送経路ではなく見せかけの経路を示す。実際には攻撃者から直接配信された詐称メールであることもある。
標的型攻撃メールには、多くの人が興味を持つような内容のものと、関係者しか知りえない内容のものがある。後者については、関係者が事前に攻撃され、盗み出されたメールスプール等の情報を悪用されている。関係者しか知りえない情報が含まれたメールを読んだ場合、最終的な被害者が内容から詐称された攻撃メールであると判断することは困難になる。このように、標的型攻撃は必ずしも政府官公庁や大企業等の特定の組織だけが狙われるような攻撃ではなく、標的となるような組織の関連組織にも波及する。

図-15 標的型攻撃の連接

き合いのある組織のセキュリティ対策の状況を把握したり、そこで事件が発生した場合には連絡をするように調整することで、このような攻撃の連接に備えることができます[*78]。

■ 入口対策の強化

まず、インターネットに公開されているサーバ類で脆弱性の有無を検証します。特に更新の早いソフトウェアについては注意が必要です。

多くの標的型攻撃が、迷惑メールや詐称メールの様態のメールを利用して実行されていますので、迷惑メール対策の導入である程度の効果を期待することができます。業務上メールのやり取りをする必要のある組織に対して、SPFやDKIMの導入を推奨し、自組織においてはメールを受け取った時にその署名等の検証を行う仕組みを導入します。

また、セキュリティ事業者や外部団体等と連携し、標的型攻撃に利用された外部サーバ等の情報を入手し、ブラックリスト化し、そこからのメールを受け取らないように設定することも攻撃の機会を減らす効果があると考えられます。

■ 出口対策[*79]の強化

組織内に侵入したマルウェアはインターネット側に情報を送信したり、インターネット側から命令を受け取って組織

表-2 標的型攻撃への対策

標的型攻撃への対策	概　要	対策方針
準備行為への対策	公開されているシステムの脆弱性対策	インターネットに公開されているシステムのセキュリティ確保について確認する。利用ソフトウェアの脆弱性の有無、ID とパスワードの使い回しの有無等。
	公開情報の確認	自組織についてインターネット上に公開されている情報について確認する。メールアドレス、人物名、利用システム、バージョン等。公開されている情報それぞれについて、攻撃に悪用される前提でセキュリティを強化する。
	他の組織のセキュリティ	業務上付き合いのある他の組織があれば、その組織のセキュリティ確保状況について確認する。
セキュリティ境界越えへの対策（入口対策の強化）	公開システムのセキュリティ強化	インターネットにさらされたシステムが侵入された時に、組織内ネットワークに影響を及ぼさないように十分に分離する。
	詐称メール対策	迷惑メール対策の技術等を利用して詐称メールを受け取らないようにする。
	ブラックリストの活用	過去に標的型攻撃メールを送付してきた IP アドレス等のブラックリスト化を行い、そこからのメールを受け取らないようにする。
セキュリティ境界越えへの対策（出口対策の強化）	マルウェアの通信先のブラックリストの活用	標的型攻撃に利用されたマルウェアの通信先の IP アドレス等の情報をブラックリスト化し、組織内からその通信先に通信を行わないようにする。
	ホワイトリストの活用	インターネットへのアクセスを、業務上必要で信頼できるサーバにのみ限定する。
組織内ネットワークでの活動の妨害	内部サーバの保護	組織内のネットワークの運用に必要な情報と、その情報をつかさどるサーバの保護について見直す。またメールサーバ、ファイル共有サーバ等の重要サーバの保護と、利用者のアクセス権限等についても整理する。
	重要情報保護	組織内の重要な情報とその保護方法について見直す。重要な情報の定義から、組織内におけるそれらの情報への扱いに見直しをかけ、本当に必要なアクセス手段のみに限定する。
標的型攻撃に関する知識	教育	組織内の利用者に標的型攻撃に関する教育を行う。攻撃の存在そのものを伝えると共に、攻撃に利用される手法について知ってもらい、業務上必要ないメールやメッセージを捨てることを推奨する。
	訓練	組織内の職員に標的型攻撃を模したメールを送付すること等で、標的型攻撃への反応を調査するとともに、回数を重ねることで攻撃に対する耐性をつける。
セキュリティオペレーションと緊急対応	セキュリティオペレーション	組織内のシステムの運用において、異常検出等のセキュリティオペレーションを行う仕組みを導入する。運用ツールを利用してセキュリティに関する知識を集める。
	緊急対応	通信異常の検知やマルウェア感染の発見後に、証拠保全、解析、影響範囲の特定を行う緊急対応の機能を組織内に持つ。
情報共有	標的型攻撃に関する情報収集	情報共有のプロジェクト等に参加することで、他の組織で発生した標的型攻撃に関する情報を収集する。特に他の組織への攻撃で利用されたアドレス、マルウェア、メッセージ文面等を入手し、入口及び出口におけるブラックリストへの適用や、利用者への注意喚起を行う。

＊78 例えば内閣官房情報セキュリティセンタでは「標的型攻撃に対して政府が講ずるべき情報共有等に関する対策」の1つとして、調達等に際して調達先に求める情報セキュリティ要件として、情報セキュリティ体制の整備や、秘密保持、セキュリティ侵犯発生時の報告、監査の実施等を盛り込むように指示している。情報セキュリティ政策会議第28回会合（平成24年1月24日）資料1-1「情報セキュリティ対策に関する官民連携の在り方について」（http://www.nisc.go.jp/conference/seisaku/dai28/pdf/28shiryou1-1.pdf）。

＊79 出口対策はIPAの次のガイドによって紹介された概念であり、既存のセキュリティ境界のための仕組みと、マルウェアの動作解析結果を利用してマルウェアの活動を阻害しようとするものである。IPA、「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」を公開（http://www.ipa.go.jp/security/vuln/newattack.html）。

内ネットワークを探索したりします。この際、侵入された端末とインターネット側の攻撃者の間で何らかの通信が発生します。この通信を阻害することで、情報の漏えいや外部からの命令を受け取れなくすることができます。マルウェアによる通信は、多くの組織で端末からインターネットに対して許可されているHTTPやSSL、SMTP等の通信プロトコルを利用します。このため、マルウェアによる通信を阻害するためには、まず、組織内からインターネットに対する通信に制限を設けるような方針を作成し、実施する必要があります。

このためには、従来セキュリティ境界の確保に利用されていたファイアウォールやIPS、HTTP Proxy等の機能を流用することが可能です。例えば、アンチウイルスベンダやセキュリティ事業者等から、標的型攻撃に利用されたマルウェアの通信先の情報を入手し、ブラックリストとして登録することで、組織内ネットワークからそれらのサーバに通信できないようにすることが考えられます。また、組織の業務が許すようであれば、通信先を信頼のおける特定のサーバのみに限定するようなホワイトリスト運用を行うことで、より広範囲なマルウェアによる通信の妨害を行うことが可能となります。

■ 組織内ネットワークでの活動の妨害

多くの事例において、一般利用者の端末に侵入を許したことから、組織内ネットワークの他の端末やサーバへの侵入につながっています。次のステップとしては、侵入に成功したことで得られる情報量の多さを考慮すると、組織内ネットワークの管理サーバが狙われやすいと考えるのが自然です[*80]。組織内ネットワークでは、端末からの攻撃に対して保護されていない管理サーバも多いことから、端末と管理サーバの間の通信を限定し、管理プロトコルを解釈できるセキュリティ装置等を導入することで、端末からサーバに対する攻撃に備えることが必要となります。

また、組織内ネットワークにおいても、複数のセキュリティ境界を設定することで、組織内ネットワークの一部に侵入を許したとしても、重要な情報に到達できないようにすることができます。例えば、一般利用者の端末から重要な情報を保有するシステムへの通信を不可能にすることがこれに当たります。特に、管理サーバへの侵入を許したときに、重要な情報に到達できる権限を与えないように境界や認証を設定することが重要です。

■ 標的型攻撃に関する知識

組織の一般利用者が標的型攻撃メールを受け取った時に、そのメールに対してどういう扱いをするかで、標的型攻撃に強い組織であるか弱い組織であるかが分かれます。例えば、日常的に業務に関係のないメールを許容している組織と、業務のメールのみしか取り扱いを許されていない組織では、後者の方が耐性が強いといえます。

利用者が標的型攻撃という攻撃の存在と、その多くがメールによるものであることを知り、その詐称や文言の傾向等を把握していれば、標的型攻撃メールが到着した際に、添付ファイルを開いたり、URLをクリックしたりしてマルウェアに感染する可能性を減らすことができます。一般の利用者にこのような認識を与えるための手法として、社内教育や、組織内での標的型攻撃メールを模したメールによる訓練は有効だと考えられます。

■ セキュリティオペレーションと緊急対応

組織内からインターネットへの通信を常時監視し、特定の宛先への大量の通信の発生等、異常と考えられる通信を発見できる仕組みを導入することで、組織内に侵入したマルウェアとインターネット側のサーバとの通信を発見することができます。このように、組織内ネットワークの日常的な運用から、セキュリティ上意味のある情報を抽出する仕組みを検討します。

また、異常を検知した時には、緊急対応として、通信を行っている端末の保全を行い、マルウェアの感染の調査、マルウェアの検体解析、通信先や通信内容の調査、マルウェアの通信を阻害するワークアラウンドの設定、マルウェアの感染経路の調査、他の端末やサーバへの攻撃の有無、情報漏えいの有無に関する調査等を実施する必要があります。

＊80 管理サーバが狙われる事例があることから、内閣官房情報セキュリティセンターから各府省庁あてに注意喚起文章が出されている。NISC、「ネットワーク利用者を管理するサーバのセキュリティ対策の徹底について」(http://www.nisc.go.jp/active/general/pdf/ada_kanki_111222.pdf)。

これらの機能を組織内で実現できるように準備することが必要です[*81]。

■ 情報共有

立て続けに明らかになった標的型攻撃の発生をうけ、現在日本国内において複数の情報共有プロジェクトが立ち上がり、事例を基にした知の結集による標的型攻撃への対策が検討されています。このようなプロジェクトのうちのいずれかに参加することで、他組織で発生した標的型攻撃の情報をもとにした対策が実現できます。

一方で、このようなプロジェクトに参加することで、自組織で発生した標的型攻撃に関する情報を提供することが求められることがあります。自組織に対して発生した攻撃に関する情報を、限られた範囲に対してとはいえ公開することには、拒否反応があることも事実です。このために、一部のプロジェクトでは厳格なNDAを締結した上で情報共有を行っていますし、別のプロジェクトでは情報提供のインセンティブについて議論を行っています。

これまでに紹介してきた、入口対策としてのメール送信元のブラックリストによるアクセス制御や、マルウェアの通信に対する出口対策は、既に発生した標的型攻撃に関する知識を利用した対策であり、情報の共有がなければ成立しません。標的型攻撃による被害が継続している現在の状況を打開するためには、現在複数検討されている情報共有プロジェクトのうちのいずれかが成功することが必要不可欠であると考えています[*82]。

■ まとめ

ここまで紹介してきたように、標的型攻撃は1つの問題ではなく、標的になったことに起因して、複合的に起こる問題です。この攻撃に立ち向かうためには、対症療法的な対策だけではなく、複数の対策を効果的に組み合わせる必要があります。

1.5 おわりに

このレポートは、IIJが対応を行ったインシデントについてまとめたものです。今回は、昨年続発した公開鍵証明書に関する事件と、標的型攻撃とその対応についてまとめています。

IIJでは、このレポートのようにインシデントとその対応について明らかにして公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を継続して参ります。

執筆者:
齋藤 衛(さいとう まもる)
IIJ サービス本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発等に従事の後、2001年よりIIJグループの緊急対応チームIIJ-SECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会等、複数の団体の運営委員を務める。

土屋 博英(1.2 インシデントサマリ)
土屋 博英、鈴木 博志、永尾 禎啓(1.3 インシデントサーベイ)
須賀 祐治(1.4.1 公開鍵証明書発行に関するいくつかの問題)
齋藤 衛(1.4.2 標的型攻撃とその対応)
IIJ サービス本部 セキュリティ情報統括室

協力:
加藤 雅彦、根岸 征史、桃井 康成、吉川 弘晃、鈴木 博志、春山 敬宏、小林 直、齋藤 聖悟 IIJ サービス本部 セキュリティ情報統括室

＊81 先に紹介した第28回情報セキュリティ政策会議資料「情報セキュリティ対策に関する官民連携の在り方について」においても、国内すべての政府機関に、このような機能の緊急対応チーム(CSIRT)の設置を求めている。

＊82 例えば、日本セキュリティオペレーション事業者協議会(http://www.jnsa.org/isog-j/)では、標的型攻撃対策のWGで、会員間での情報共有による標的型攻撃の検証に挑戦している。その中間報告「NSF2012 B2 標的型攻撃とセキュリティオペレーション」(http://www.jnsa.org/seminar/nsf/2012/pro.html)によると、過去に発生した標的型攻撃に関する情報の共有と調査を行うことにより、複数のSOC事業者間で共通の攻撃があったことを確認している。このことは、情報共有を実時間で迅速に行うことで、ある種の標的型攻撃への対策を実施することができることを示している。