公開鍵証明書の不正発行事件

今回は、Apacheの脆弱性とその対応について示すとともに、金銭目的の攻撃プラットフォームとして多く利用されるようになっているSpyEyeの解析と、公開鍵証明書の不正発行事件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7月から9月までの期間では、サーバやブラウザに関する脆弱性が複数発見され対応されています。また、香港証券取引所への攻撃に代表される各国企業や政府関係組織へのDDoS攻撃等も数多く報告されています。さらに、日本国内において軍事産業企業への標的型攻撃の発生が９月後半に報告されました。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。

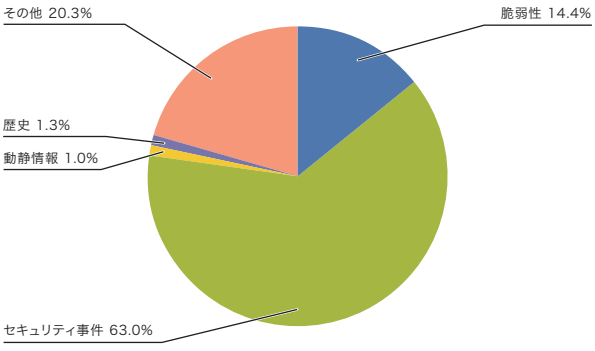


図-1 カテゴリ別比率(2011年7月～9月)

1.2 インシデントサマリ

ここでは、2011年7月から9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]。本稿より、IIJが直接対応したインシデントだけでなく、間接的な情報、例えば諸外国で発生した事件で日本国内にも影響する可能性のあるもの等を集計の対象としています。

次に、この期間に発生した主な事件について紹介します。

■ Anonymous等の活動

この期間においてもAnonymousに代表されるHacktivist[*2]の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、インド、チリ、コロンビア、メキシコ等の政府関連サイト、政府関連団体や企業のサイトに対するDDoS攻撃が発生しました。7月中旬から8月にかけて、複数のAnonymous関連サイトへの攻撃が発生していますが、行為者は不明です。同時に、非常に多くの政府関連サイト、企業サイトから情報漏えいが発生しています。

例えば、8月にはサンフランシスコの鉄道公社BARTの事件をきっかけに、駅におけるデモ、BART関連サイトへのDDoS攻撃、Webサイトからの情報漏えい等が発生しています。またニューヨークのウォール街で実施されていたデモに関連した活動は、本稿執筆時点でも継続しています。

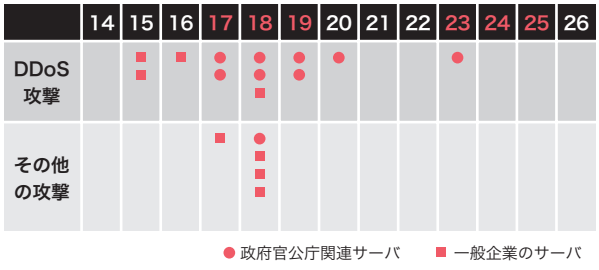
＊1　このレポートでは取り扱ったインシデントを、脆弱性、動静情報、歴史、セキュリティ事件、その他の5種類に分類している。
脆弱性:インターネットやユーザの環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェア等の脆弱性への対応を示す。
動静情報:要人による国際会議や、国際紛争に起因する攻撃等、国内外の情勢や国際的なイベントに関連するインシデントへの対応を示す。
歴史:歴史上の記念日等で、過去に史実に関連して攻撃が発生した日における注意・警戒、インシデントの検知、対策等の作業を示す。
セキュリティ事件:ワーム等のマルウェアの活性化や、特定サイトへのDDoS攻撃等、突発的に発生したイン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

＊2　Anonymousとその関連の活動については、IIR Vol.12「1.4.1 連続する企業や政府関係組織への攻撃」(http://www.iij.ad.jp/development/iir/pdf/iir_vol12.pdf)で紹介している。

■ 動静や歴史的背景による攻撃

昨年9月18日、尖閣諸島における船舶衝突に端を発した一連の事件として、国内複数のサイトに対する大規模なDDoS攻撃が同時多発的に発生しました[*3]。本年もこの日を中心として、複数の攻撃が観測されました。攻撃予告等の情報から、関連すると判断した攻撃を表-1にまとめます。このように、昨年の攻撃に比べるとその攻撃対象や発生件数は少なかったことが分かります。攻撃の最大規模は、635MbpsのUDP floodで、複合攻撃では1.2Mpps/600MbpsのSYN floodとHTTP GET floodを観測しました。最大の攻撃継続時間は2時間程度でした。

また本年の特徴として、金融機関等一般企業への攻撃が発生したことと、DDoS攻撃と同時に、SQLインジェクション、パスワードブルートフォース等による侵入や情報漏えい、改ざんを目的とした攻撃が多く発生していたことが挙げられます。



期間中にIIJが観測した攻撃で、攻撃予告と対応する攻撃を集計した。Webサーバに対するSQLインジェクション攻撃やFTPサーバに対するブルートフォース攻撃によるパスワード探索等を「その他の攻撃」として分類している。特定のサーバに攻撃が発生した日にマークしている。1つのサーバに1日で複数回攻撃が発生していてもマークは1つ。

表-1 一連の攻撃の様子(2011年9月)

■ 標的型攻撃

8月に入り、日本国内の大企業において組織内ネットワークにおけるウイルス感染が見つかり、メールを媒体とした標的型攻撃によるものであることが公表されました。またその後、同じ業種の複数の企業において同様の攻撃が発生したことが報じられました。

この攻撃に対して、官公庁主導の複数の対策活動が検討、または実施されています。また、この攻撃の公表に先立って公開されたIPAによるガイドライン[*4]に提案された出口防御[*5]の概念が、実効力のある対策として注目されています。

■ 脆弱性とその対応

この期間中では、マイクロソフト社のInternet Explorer[*6]、Adobe社のAdobe Reader及びAcrobat、Adobe Flash Player、Adobe Shockwave Player、Apple社のQuickTime等の、Webブラウザやユーザ利用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。

また、DNSサーバのISC BINDや、WebサーバのApache HTTPD Serverに脆弱性が見つかっています。特にApacheでは、未修正の脆弱性がApache Killerという名の検証プログラムとして発表されたため、修正が公開される前に悪用されたことが確認されています。本脆弱性については「1.4.1 Apache Killerとその対応」も併せてご参照ください。これら以外にも、CMSとして利用されるWordpress、マイクロソフト社のWindows DNSサーバー[*7]で脆弱性が修正されています。データベースサーバとして利用されているOracleでは四半期ごとに行われている更新が提供され、複数の脆弱性が修正されています。さらに、シスコ社から定例のアップデートが公開され、ルータのファームウェアについて、東日本大震災の影響を考慮して公開が延期された修正を含め複数の脆弱性が修正されました。

*3 昨年同時期の一連の攻撃については、IIR Vol.10「1.4.1 2010年9月に発生した大規模DDoS攻撃の概要」(http://www.iij.ad.jp/development/iir/pdf/iir_vol10.pdf)で紹介している。
*4 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)。
*5 出口防御とは、組織内ネットワークからインターネットに対する通信を制御することで、組織内に感染しているマルウェアの動作や外部からの操作を止めたり、情報漏えいを阻害したりする。マルウェアの解析により明らかになったサーバのブラックリスト等により実現する。より詳しくは「新しいタイプの攻撃」の対策に向けた設計・運用ガイドのP17「4. 新しい脅威に立ち向かうポイント」以降を参照のこと。IIJのサービスでは、IIJセキュアWebゲートウェイサービスにおいて2009年8月よりこの機能を提供している。
*6 「マイクロソフト セキュリティ情報 MS11-057 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(2559049)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms11-057)。
*7 「マイクロソフト セキュリティ情報 MS11-058 - 緊急 DNS サーバーの脆弱性により、リモートでコードが実行される(2562485)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms11-058)。

7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

他 **1日**：Googleは.co.ccサブドメインのサイトに不正な利用が多いことからインデックスから削除し、検索結果に表示されないようにした。
この方針については6月の次のGoogle Online Security Blogにより公表されている。"Protecting users from malware hosted on bulk subdomain services"(http://googleonlinesecurity.blogspot.com/2011/06/protecting-users-from-malware-hosted-on.html)。

他 **1日**：JNSAよりオフィス節電のための「在宅勤務における情報セキュリティ対策ガイドブック」が公表された。
JNSA、「在宅勤務における情報セキュリティ対策ガイドブック」(http://www.jnsa.org/result/2011/zaitaku_guide.html)。

他 **1日**：JNSAより「2010年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」が公表された。
JNSA、「2010年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」(http://www.jnsa.org/result/incident/2010.html)。

セ **4日**：FTPサーバアプリケーションのvsftpdが、Backdoorを含むパッケージに改ざんされていたことが判明した。改ざんされたパッケージは署名を確認することで検知が可能であった。
"Alert：vsftpd download backdoored"(http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html)。

脆 **5日**：BIND 9.7.3-P3 がリリースされ、悪用されるとDNSサーバに対してDoS攻撃となるCVE-2011-2464を含む複数の問題が修正された。
Internet Systems Consortium、「ISC BIND 9の権威およびキャッシュサーバに対する遠隔サービス妨害攻撃」
(https://www.isc.org/software/bind/advisories/CVE-2011-2464-JP)。

セ **8日**：国内通信事業者が、5月に発生した関西での大規模通信障害について、業務委託先の元社員による内部犯行であることを発表した。

セ **10日**：警察庁のWebサイトに対しDDoS攻撃が発生し、一時的にホームページが閲覧できなくなる。
この事件については次の警察庁の発表がある。「平成23年７月の警察庁に対するサイバー攻撃への対応について」
(http://www.npa.go.jp/keibi/biki3/230826kouhou.pdf)。

脆 **13日**：マイクロソフト社は 2011年7月のセキュリティ情報を公開し、1件の緊急と3件の重要な更新をリリースした。
「2011年7月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms11-jul)。

他 **14日**：Janog 28にて東日本大震災におけるインターネット等の通信への影響について議論が行われた。
Janog Meeting、「日本のインターネットは本当にロバストだったのか」(http://www.janog.gr.jp/meeting/janog28/program/robust.html)。

他 **14日**：米国国防総省が新しいCyber Security戦略を発表。同時に、3月に起きた国防関連企業への他国からの攻撃によって、24,000のファイルが漏えいした事実を公表。
"Lynn:Cyber Strategy's Thrust is Defensive"(http://www.defense.gov/news/newsarticle.aspx?id=64682)。

他 **20日**：「タコイカウイルス」作者が器物損壊容疑に問われた裁判で実刑判決が言い渡された 。
TrendLabs SECUITY BLOG、「『タコイカウイルス』作者に実刑判決」(http://blog.trendmicro.co.jp/archives/4377)。

脆 **20日**：Oracleが四半期毎の定例アップデートを公開し、合計78件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - July 2011"(http://www.oracle.com/technetwork/topics/security/cpujuly2011-313328.html)。

セ **21日**：7月14日に施行されたいわゆるウイルス作成罪を含む改正刑法に基づき、不正指令電磁的記録保管容疑で初の逮捕者が出た。

脆 **23日**：MacBookのバッテリーの管理インタフェースに脆弱性があり、マルウェア等に悪用された場合、機能停止や過熱といった被害が出る可能性が指摘された。
ISC Diary、"Apple Battery Firmware Default Password"(http://isc.sans.edu/diary.html?storyid=11248)。

脆 **25日**：iOS4.2.10/4.3.5がリリースされた。CVE-2011-0228で指摘されているSSL関連の問題の修正が含まれる。
「iPhone用iOS4.3.5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/HT4824?viewlocale=ja_JP)。

セ **25日**：osCommerce利用サイトで大規模改ざん事件が発生した。
Armorize Malware Blog 、"willysy.com Mass Injection ongoing, over 8 million infected pages, targets osCommerce sites"
(http://blog.armorize.com/2011/07/willysycom-mass-injection-ongoing.html)。

他 **26日**：JPCERT/CC等が共同で、情報処理の高度化等対処のための刑法等の一部を改正する法律（サイバー刑法、刑事訴訟法）の説明会を実施。
「情報処理の高度化等対処のための刑法等の一部を改正する法律（サイバー刑法、刑事訴訟法）説明会のご案内」(http://www.jpcert.or.jp/event/keiji.html)。

セ **28日**：韓国のポータルサイト（NateとCyworld）で、最大3,500万人分の個人情報が漏えい。ユーザID、名前、携帯番号、メールアドレス、パスワード、住民登録番号が漏えいした。パスワードと住民登録番号は暗号化されていた。
TrendLabs SECUITY BLOG、「韓国で大規模情報漏えい。3500万人の個人情報が盗まれる」(http://blog.trendmicro.co.jp/archives/4426)。
TrendLabs SECUITY BLOG、「【続報】韓国における大規模情報漏えい：被害はより広範囲か」(http://blog.trendmicro.co.jp/archives/4447)。

[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

■ 大規模情報漏えい

韓国では複数のポータルサイトが攻撃を受け、最大で3,500万人分となる個人情報漏えい事件が発生しています。流出したデータは暗号化していたとされていますが、国民の70%にも及ぶ規模と個人情報が流出したときの影響の大きさから問題となりました。

日本国内でも、複数の保険事業者の契約情報等、合計2万5,000人分の個人情報が不正に取得されて第三者に売却されていたことが判明したり、ゲームサーバが不正なアクセスを受け、最大で20万3,000人分のIDとパスワード及びメールアドレスが流出した事件が発生しています。

■ ウイルス作成罪関連

この期間中、7月14日に「情報処理の高度化等に対処するための刑法等の一部を改正する法律」[*8]が施行されました。21日には不正指令電磁的記録保管容疑で初の逮捕者がでています。この法律が施行される前の昨年逮捕された、タコイカウイルスを作成したとされる人物に対して、器物損壊罪での実刑判決が下されています。

これまでウイルスや不正なプログラムの作成等を直接罪に問うことはできませんでしたが、この法律が施行されたことにより、不正な目的のためのウイルスの作成・供用・保管等の行為に対して犯罪として対処できるようになりました。一方で、法律の解釈や運用に不安な点もあるため、JPCERT/CCらが共同主催した説明会等が実施されました。

■ 不正侵入とWebコンテンツやパッケージの改ざん

不正侵入やそれによる改ざん事件も多く発生しています。オンラインショップ構築で利用されているサーバアプリケーションのosCommerceを対象とし、その脆弱性を利用してWebページを改ざんする事件が多数発生しました[*9]。この事件では、訪問したユーザが改ざんされたWebサイトから不正なWebサイトに誘導され、マルウェアに感染させる手法が使われています。この事件で改ざんされたWebページは769万ページに及ぶとされています。この他にもMySQL.comが改ざんされ、同様の手法で訪問者を不正なWebサイトに誘導する事件が発生しています。

また、Linux Kernelを管理しているKernel.orgが侵入され、SSH関連ファイルの改ざんやシステムにバックドアが仕込まれる等の被害が出た事件が起こり、配布されているLinuxのKernelプログラムが改ざんされていないことを確認するために大規模な検証が行われました。関連して、Linux Foundationも同様に侵入されていたことが分かり[*10]、侵入による影響範囲の特定や改ざんの状況についての調査確認のため、一時サイトを閉鎖する等の対応が行われました。さらに、Linux等で利用されているFTPサーバのvsftpdでファイルが改ざんされ、侵入のためのバックドアが含まれたものが配布される事件も発生しています[*11]。正規の配布サイトに不正に改ざんしたソフトウェアが設置される事件は、過去にもたびたび発生しており[*12]、例えば、2002年に発生したSendmailやOpenSSH、2010年に発生したProFTPD等が事例として挙げられます。

今回の事件では、ファイルの署名までは改ざんされておらず、署名やハッシュ値のチェックを行うことで正規のソフトウェアでないことが判別できました。

---

*8 この法律に関しては次の法務省の説明に詳しい。「情報処理の高度化等に対処するための刑法等の一部を改正する法律案」(http://www.moj.go.jp/keiji1/keiji12_00025.html)。

*9 この件については次のArmorize Malware Blogで継続的に報告されている。"willysy.com Mass Injection ongoing, over 8 million infected pages, targets osCommerce sites"(http://blog.armorize.com/2011/07/willysycom-mass-injection-ongoing.html)。

*10 この事件については例えば次のSophos社のニュースリリース等が参考となる。「セキュリティ侵害:Kernel.orgとLinux Foundationのサイト閉鎖が続く」(http://jp.sophos.com/pressoffice/news/articles/2011/09/linux-world-in-security-spinout.html)。

*11 この件についてはvsftpdの作者本人が解説している。"Alert: vsftpd download backdoored"(http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html)。

*12 過去の改ざん事例とその検出方法については本レポートVol.10「1.4.3 ソフトウェア配布パッケージの改ざん」(http://www.iij.ad.jp/development/iir/pdf/iir_vol10.pdf)で解説している。

8月のインシデント

1
- 他 1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」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/about/press/20110801.html)。

2
- 脆 2日：ENISAがHTML5の仕様に脆弱性があることを指摘した。
  "Agency ENISA flags security fixes for new web standards/HTML5"
  (http://www.enisa.europa.eu/media/press-releases/web-security-eu-cyber-security-agency-enisa-flags-security-fixes-for-new-web-standards)。

3
- セ 2日：日本国内においてMasterCardを騙るフィッシングが発生した。

4
- セ 2日：Androidで通話内容を録音する盗聴ウイルスが発見される。
  Total Defense:GLOBAL SECURITY ADVISOR RESEARCH BLOG、"A Trojan spying on your conversations"
  (http://totaldefense.com/securityblog/2011/08/26/A-Trojan-spying-on-your-conversations.aspx)。

5

6
- セ 3日：国内ネットバンクへの不正アクセスが相次いだことに対する注意喚起が発行された。
  IPA、「国内のインターネットバンキングで不正アクセスが相次いでいる問題について」(http://www.ipa.go.jp/security/topics/alert20110803.html)。

7
- セ 3日：複数のウイルス対策ソフトベンダが標的型攻撃Shady RAT攻撃の分析レポートを公開した。
  McAfee、「Operation Shady RATの全貌」(http://www.mcafee.com/japan/security/rp_OperationShadyRAT.asp)。

8
- 脆 4日：QuickTime7.7がリリースされ、CVE-2011-0245を含む複数の脆弱性が修正された。
  「QuickTime 7.7 のセキュリティコンテンツについて」(http://support.apple.com/kb/HT4826?viewlocale=ja_JP)。

9
- 他 8日：イギリスのダブリンにあるデータセンターで大規模電源障害が発生、複数のクラウド事業者のサービスに影響した。

10
- 脆 9日：Adobe Shockwave Playerに関するセキュリティアップデートが公開され7件の脆弱性が修正された。
  APSB11-10：「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/apsb11-19.html)。

11

12
- 脆 10日：マイクロソフト社は2011年8月のセキュリティ情報を公開し、MS11-057・MS11-058等、緊急2件、重要9件、警告2件の修正をリリースした。
  「2011年8月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms11-aug)。
- セ 10日：香港証券取引所にDDoS攻撃が発生し、11日まで2日連続で一部銘柄の取引ができない事態が発生した。
  "Disruption of HKExnews Website Services"(http://www.hkex.com.hk/eng/newsconsul/hkexnews/2011/1108104news.htm)。
  Sophos、nakedsecurity "Hong Kong stock exchange (HKEx) website hacked, impacts trades"
  (http://nakedsecurity.sophos.com/2011/08/10/hong-kong-stock-exchange-hkex-website-hacked-impacts-trades/)。

13

14
- セ 12日：クライムウェアキットである「SpyEye」のソースコードが流出したことが明らかになった。
  DAMBALLA、The Day Before Zero"First Zeus, now SpyEye. Look at the source code now!"(http://blog.damballa.com/?p=1357)。

15
- 脆 12日：仮想化サーバXenにシステムの停止を引き起こすCVE-2011-3131を含む複数の脆弱性が発見され修正された。
  "CVE-2011-3131 kernel:xen:IOMMU fault livelock"(https://bugzilla.redhat.com/show_bug.cgi?id=730341)。

16

17
- 脆 14日：Rubyに複数の脆弱性が発見され修正された。
  "CVE-2011-2686 CVE-2011-2705 CVE-2011-3009 ruby:Properly initialize the random number generator when forking new process"
  (https://bugzilla.redhat.com/show_bug.cgi?id=722415)。

18
- セ 15日：終戦記念日に関連して、日本の大規模掲示板に対する攻撃が発生した。

19
- 他 17日：研究者がAES暗号化アルゴリズムに脆弱性を発見した。ただし、ただちに利用上の安全性が脅かされるものではないことも確認されている。
  マイクロソフトリサーチ、"Biclique cryptanalysis of the full AES"(http://research.microsoft.com/en-us/projects/cryptanalysis/aes.aspx)。

20
- セ 19日：Invoiceを装ったマルウェア添付メールの流行が報告された。
  Sophos、nakedsecurity "Inter-company invoice emails carry malware"
  (http://nakedsecurity.sophos.com/2011/08/18/inter-company-invoice-emails-malware/)。

21

22
- 脆 20日：ApacheにCVE-2011-3192の脆弱性があり修正された。なお、この脆弱性は公表された時点では未修正であった。
  Apache KillerについてはFull Disclosure MLを参照のこと。この脆弱性については次のApache Foundationのアドバイザリに詳しい。"Apache HTTPD Security ADVISORY UPDATE 3 - FINAL"(http://httpd.apache.org/security/CVE-2011-3192.txt)。

23

24
- セ 24日：国内大手サービスプロバイダを騙るフィッシングサイトが確認され注意喚起が行われた。このフィッシングサイトではIDとパスワードを入力させるサイトであったことからなりすましやサービスの不正利用が目的であったと考えられる。

25
- セ 25日：利用者の多い大規模掲示板がApacheの非公開の脆弱性を検証するためのツール、Apache Killerによって攻撃される。

26
- セ 28日：Kernel.orgが1ヶ月程前から侵入されていたことが発覚した。アカウント情報の漏えいやファイル改ざん等の被害が発生した。
  Linux Foundation、"The cracking of kernel.org"(https://www.linuxfoundation.org/news-media/blogs/browse/2011/08/cracking-kernelorg)。

27
- 脆 28日：squidに通信先のgopherサーバにDoS攻撃を引き起こすCVE-2011-3205の脆弱性があり修正された。
  "Squid Proxy Cache Security Update Advisory SQUID-2011:3"(http://www.squid-cache.org/Advisories/SQUID-2011_3.txt)。

28
- セ 28日：RDPによる感染活動を行うMorto Wormの流行が報告された。
  エフセキュアブログ、「Windowsリモートデスクトップワーム『Morto』が拡散」(http://blog.f-secure.jp/archives/50625847.html)。

29
- セ 30日：オランダの認証局DigiNotar社が7月に不正アクセスを受け、大量の偽のSSL証明書が発行されていたことが発覚した。
  エフセキュアブログ、「『Diginotar』がBlack.Spookとイランのハッカーによりハッキング」(http://blog.f-secure.jp/archives/50626009.html)。

30
- 他 31日：スマートフォンで位置情報や通話記録の情報を公開してしまうアプリが、実際の利用者への確認が不十分であったことで問題になった。

31
- 脆 31日：XenにゲストOSからシステムの停止を引き起こす可能性のあるCVE-2011-2901の脆弱性があり修正された。

[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

■ DDoS攻撃

この期間中は大規模なDDoS攻撃も多く発生しており、7月に発生した警察庁のホームページが一時閲覧できなくなる事件や、8月15日には大規模掲示板を狙ったDDoS攻撃等が発生しています。また、IIJにおいても、7月に最大3Gbpsの通信量で、45万ppsのUDP flood攻撃を観測しています。

海外においても、香港証券取引所がDDoS攻撃を受け、2日連続で一部銘柄の取引ができなくなる事件が発生し、重要インフラである金融分野において実際に被害を受けたサイバーテロの事例として注目されました。

■ フィッシングと国内ネットバンキングに関する注意喚起

メールによるフィッシングサイトへの誘導や、マルウェアを添付した攻撃についても継続して発生しており、ネットバンク、クレジットカード会社、通信事業者等を詐称したフィッシングサイトや、関連するIDとパスワードを盗むマルウェアが確認されています。特に国内のインターネットバンキングにおいて、不審メールやスパイウェアによりパスワード等の顧客情報が窃取され、実際に振込被害が発生するといった不正アクセスが相次いでいるとして、IPAから不正プログラムや迷惑メールに対する注意喚起が行われています。

■ 内部犯行

5月に関西で発生した携帯電話網の通信障害について、元契約社員が作成した不正プログラムによる人為的なものであったとして、犯人が電子計算機損壊等業務妨害容疑で逮捕されています。また、携帯ソーシャルゲーム利用者130万人分のゲーム情報が改ざんされた事件では、ゲーム開発会社で3月まで派遣業務で働いていた人物が、サーバにアクセス制限を解除できるプログラムを仕込んで不正アクセスを行ったとして、不正アクセス禁止法違反と電子計算機損壊等業務妨害の容疑で逮捕されています。米国では、今年2月に製薬会社の複数の社内用仮想サーバの内容が、解雇された元従業員により削除される事件が発生しました[*13]。これらの仮想サーバには業務システムの多くが収容されていたため、多大な影響があったと報じられています。

内部犯行によるインシデントについては古くから事例の共有や対応策の検討がなされています。たとえば米国のCERT/CCでは2001年より研究が開始され、昨年よりblogによる継続的な情報発信がなされています[*14]。国内においても、昨年度に関連調査が実施されました[*15]。

■ Shady RAT

9月にはShady RATと呼ばれる攻撃について、複数のウイルス対策ソフトベンダから報告されました。まず、この攻撃で用いられた標的型攻撃と不正侵入について、実際の事例に基づいたレポートがMcAfee社から公表されました[*16]。このレポートでは、政府機関を含む複数の組織に対して、5年間に渡りこの仕組みを利用した攻撃が実施されていたと報告されています。また、Symantec社から同じ攻撃に関する詳細な解説が公開されています[*17]。この中では制御用の通信を通常のHTTPのトラフィックに見せかけるために、画像ファイルにコマンドを隠すステガノグラフィーが利用されていたり、HTMLのコメントに暗号化したコマンドを隠す等の手法が明らかにされています。

＊13 この事件の詳細については次の米国司法省の発表に詳しい。(http://www.justice.gov/usao/nj/Press/files/Cornish,%20Jason%20Plea%20News%20Release.html)。

＊14 CERT/CC、"InsiderThreatResearch"(http://www.cert.org/insider_threat/)。

＊15 財団法人 社会安全研究財団 情報セキュリティにおける人的脅威対策に関する調査研究会、「情報セキュリティにおける人的脅威対策に関する調査研究報告書」(http://www.syaanken.or.jp/02_goannai/08_cyber/cyber2203_01/pdf/cyber2203_01.pdf)。

＊16 McAfee社から発表されている「Operation Shady RATの全貌」(http://www.mcafee.com/japan/security/rp_OperationShadyRAT.asp)を参照のこと。

＊17 Symantecセキュリティレスポンスブログ、「Shady RAT、その真相」(http://www.symantec.com/connect/blogs/shady-rat)。

9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

脆 **7日**：OpenSSLで証明書失効リストの検証を回避できるCVE-2011-3207とシステムの停止を引き起こすCVE-2011-3210の脆弱性が修正された。
"OpenSSL Security Advisory[6 September 2011]"(http://www.openssl.org/news/secadv_20110906.txt)。

セ **8日**：ソーシャルゲーム利用者130万人分の情報が改ざんされた事件で容疑者が逮捕された。ゲーム開発会社での派遣業務を終了する際に、サーバにバックドアを仕込み不正アクセスを行った容疑による。

セ **10日**：NBC NewsのTwitterアカウントが不正に取得、悪用され、Ground Zeroについての偽ニュースを流す。Twitterアカウント運用担当3人のうちの1人が標的型メールで攻撃され、キーロガーをインストールされた。
Sophos、nakedsecurity "Script Kiddies"(http://nakedsecurity.sophos.com/2011/09/13/christmas-tree-trojan-blamed-for-nbc-news-twitter-hack/)。

セ **12日**：Kernel.orgの侵入事件に関連してLinux Foundationも侵入されていたことが発覚したためサイトが一時閉鎖された。

脆 **13日**：Adobe Reader及びAcrobatに対する複数の脆弱性を修正したセキュリティアップデート(APSB11-24)が公開された。
「APSB11-24：Adobe Readerおよび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/917/cpsid_91746.html)。

脆 **14日**：ApacheにCVE-2011-3192の脆弱性に関連して、さらに修正を加えた2.2.21がリリースされた。
"Apache HTTP Server 2.2.21 Released"(http://www.apache.org/dist/httpd/Announcement2.2.html)。

脆 **14日**：マイクロソフト社は2011年9月のセキュリティ情報を公開し、MS11-071・MS11-073等、重要5件の修正をリリースした。
「2011年9月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms11-sep)。

セ **18日**：この日の前後に政府機関や民間企業のWebサーバに対する攻撃が複数発生した。

セ **19日**：日本国内の大企業において、メールによる標的型攻撃でマルウェアに感染していたことが発見された。後に他の企業に対しても同様の攻撃があったことが判明する。

セ **20日**：9月18日に発生した日本のWebサイトへの攻撃に関連して、複数のWebサイトが改ざん被害にあったことが報じられた。

セ **20日**：オランダのDigiNotar社が事件による影響で倒産手続きに入った。
ISC Diary、"Diginotar declared bankrupt"(http://isc.sans.edu/diary.html?storyid=11614)。

脆 **21日**：Adobe Flash Playerの複数の脆弱性を修正したセキュリティアップデート(APSB11-26)が公開された。
「APSB11-26: Adobe Flash Playerに関するセキュリティアップデート公開」(http://www.adobe.com/jp/joc/security/apsb11-26.html)。

脆 **22日**：WordPressのクリックジャッキング攻撃が可能な脆弱性が公表された。この脆弱性は、5月にリリースされた3.1.3で保護機能が実装され、修正されている。
Full Disclosure ML、"WordPress <=v3.1.2 Clickjacking Vulnerability Advisory"(http://seclists.org/fulldisclosure/2011/Sep/219)。
「WordPress 3.1.3、WordPress 3.2 ベータ 2」(http://ja.wordpress.org/2011/05/26/wordpress-3-1-3/)。

脆 **24日**：SSL/TLSの脆弱性を攻撃する新たな手法BEASTが発表された。
"BEAST"(http://vnhacker.blogspot.com/2011/09/beast.html)。

脆 **26日**：PostgreSQLにおいて、blowfishアルゴリズムに関連して弱い暗号化でパスワードが保存される脆弱性(CVE-2011-2483)等が修正された。
"PostgreSQL 2011-09-26 Cumulative Bug-Fix Release"(http://www.postgresql.org/about/news.1355)。

セ **27日**：MySQL.comが改ざんされ、この間Webサイトを閲覧した利用者はマルウェア感染サイトに誘導されていた。
"MySQL.com Security Notice"(http://www.mysql.com/news-and-events/news/article_1691.html)。

セ **27日**：マイクロソフト社やウイルス対策ソフトベンダにより「Kelihos」ボットネットの活動が停止された。
"Microsoft Neutralizes Kelihos Botnet, Names Defendant in Case"
(https://blogs.technet.com/b/microsoft_blog/archive/2011/09/27/microsoft-neutralizes-kelihos-botnet-names-defendant-in-case.aspx)。

脆 **27日**：Firefox 7.0がリリースされ、外部から停止を引き起こすことができるCVE-2011-3002を含む複数の脆弱性が修正された。
「Firefox セキュリティアドバイザリ」(http://www.mozilla-japan.org/security/known-vulnerabilities/firefox.html)。

脆 **29日**：Cisco Security Advisoryが公表され、10件の脆弱性が修正された。
"Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication"
(http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep11.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

■ 暗号技術関連動向

８月には暗号に関する国際会議(CRYPTO 2011)にて暗号アルゴリズムAESへの新しい解読攻撃が発表されました[*18]。鍵の総当り攻撃に必要な計算量の理論値と比べ、少ない計算量で暗号を解読する手法ですが、現時点で暗号強度に致命的な影響を及ぼすものではなく、AESの利用に関して、特に問題となるわけではありません。

また、SSL及びTLS1.0の脆弱性を用い、ブロック暗号モードCBCを利用する場合においてCookieを搾取するツールが公開されました[*19]。本問題は2006年に改訂されたRFC4346にて根本的な対処がされており、TLS1.1及び1.2には影響しません。暗号アルゴリズムとしてRC4を利用する、またはCBC以外のモード(例えばCTR)を利用することで攻撃を回避できます。

オランダの認証局DigiNotar社が7月に不正アクセスを受けていた事件では、侵入された認証機関が持つ自己署名証明書を信頼しないという対策が、主要ブラウザにおいて実施されました[*20]。この事件については「1.4.3 公開鍵証明書の不正発行事件」も併せてご参照ください。また、犯人がDigiNotar社だけでなく、その他の認証機関についても侵入をほのめかしたことから、名前の挙がった認証機関では一時的に業務を停止して事実確認が行われる等の対応がとられました。このように、当初の予想を大きく上回る影響が発生したことで、証明書の信頼性そのものが著しく脅かされる事態となりました。

■ その他の動向

その他の動向としては、JNSAから、2010年に発生した個人情報漏えいインシデントについて、独自の調査モデルから集計・分析し結果を報告した「2010年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」と、東日本大震災当時やこの夏の節電で注目された在宅勤務を実施する際のガイドラインとして「在宅勤務における情報セキュリティ対策ガイドブック」が公表されました。

＊18 この手法については次のマイクロソフトリサーチのページで公表されている。"Biclique cryptanalysis of the full AES" (http://research.microsoft.com/en-us/projects/cryptanalysis/aes.aspx)。

＊19 詳細に関しては発表者の一人であるThai DuongのBlogを参照のこと。"BEAST"(http://vnhacker.blogspot.com/2011/09/beast.html)。

＊20 各ブラウザやアプリケーションではアップデートにより証明書の無効化等の手段が取られた。主要なブラウザでの対応については次のとおり。「Mozilla Foundationセキュリティアドバイザリ2011-34」(http://www.mozilla-japan.org/security/announce/2011/mfsa2011-34.html)。「Mozilla Foundationセキュリティアドバイザリ2011-35」(http://www.mozilla-japan.org/security/announce/2011/mfsa2011-35.html)。「11.51でのセキュリティ修正とOperaのフィッシング・マルウェア防止機能」(http://my.opera.com/chooseopera-Japan/blog/2011/09/01/11-51-opera)。"Stable Channel Update"(http://googlechromereleases.blogspot.com/2011/09/stable-channel-update.html)。またOSやアプリケーションでも次の通り、同様の対処が行われている。「マイクロソフトセキュリティアドバイザリ(2607712)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/2607712)。「セキュリティアップデート2011-005 について」(http://support.apple.com/kb/HT4920?viewlocale=ja_JP)。「JPCERT/CC Alert 2011-09-14 Adobe Reader 及び Acrobat の脆弱性に関する注意喚起」(http://www.jpcert.or.jp/at/2011/at110025.txt)。

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、状況により多岐にわたります。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したり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7月から9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[*21]、サーバに対する攻撃[*22]、複合攻撃(両方の攻撃を同時に行うもの)の3種類に分類しています。

この3ヵ月間でIIJは、561件のDDoS攻撃に対処しました。1日あたりの対処件数は6.1件で、前回のレポート期間と比べて増加しています。DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0.2%、サーバに対する攻撃が80.7%、複合攻撃が19.1%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435万ppsのパケットによって1.5Gbpsの通信量を発生させる攻撃が2時間15分継続しました。また、攻撃の継続時間は、全体の84.8%が攻撃開始から30分未満で終了し、残りの15.2%は30分以上24時間未満の範囲に分布しています。なお、今回最も長く継続した攻撃は、複合攻撃に分類されるもので2時間47分にわたりました。攻撃の規模と継続時間の関係では、小規模な攻撃は継続時間も短く、大規模な攻撃になるほど継続時間も長くなる傾向が認められます。

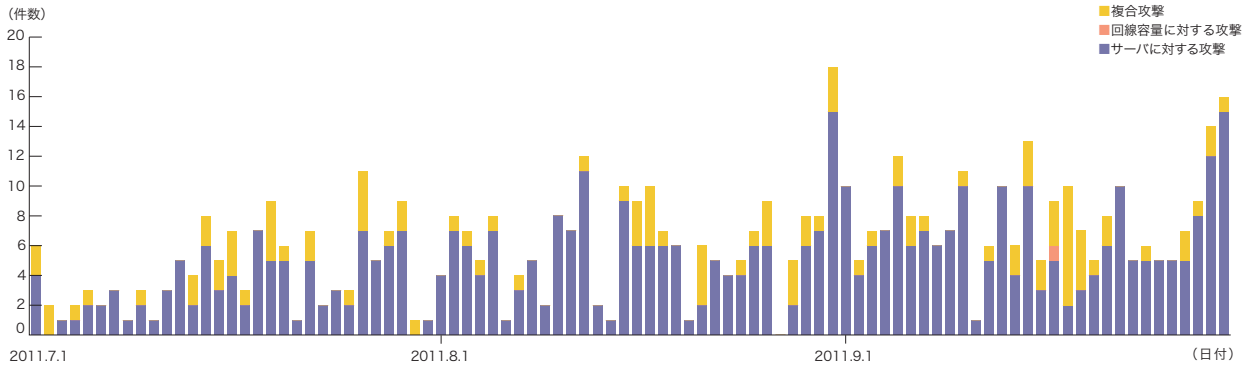


図-2 DDoS攻撃の発生件数

*21 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。

*22 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。

攻撃元の分布は、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[*23]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[*24]の利用によるものと考えられます。

■ 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[*25]によるDDoS攻撃のbackscatter観測結果を示します[*26]。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7月から9月の期間中に観測したbackscatterについて、ポート別のパケット数推移を図-3に、発信元IPアドレスの国別分類を図-4にそれぞれ示します。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71.4%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、FTPで利用される21/TCP等への攻撃も観測されています。図-4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42.4%、米国28.6%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。

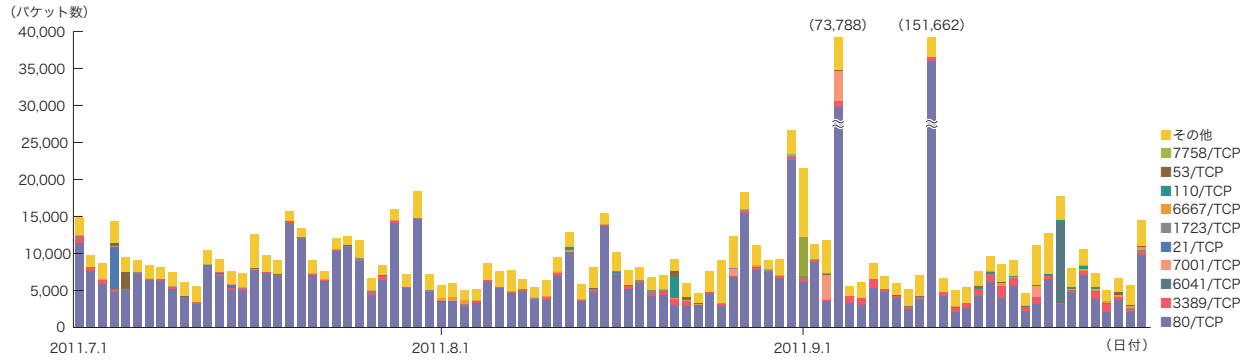


図-3 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

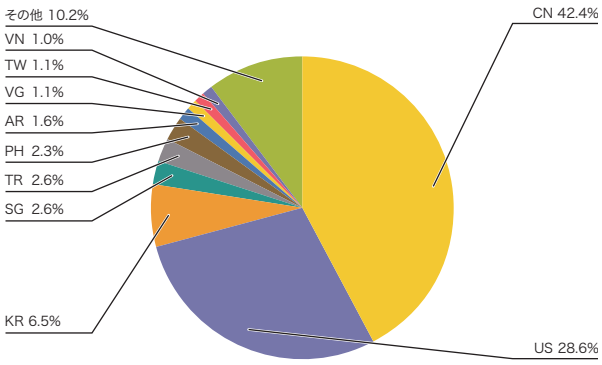


図-4 backscatter観測によるDDoS攻撃対象の分布(国別分類、全期間)

*23 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IPアドレスを付与した攻撃パケットを作成、送出すること。

*24 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。

*25 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。

*26 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。

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、中国国内のWebサーバ(80/TCP)に対する攻撃が9月に2回観測されています。また、7月3日に米国企業のFTPサーバ(21/TCP)への攻撃、7月4日に米国内のDNSサーバ(53/TCP)、POP3サーバ(110/TCP)に対する攻撃を観測しました。9月1日に発生している7758/TCPに対する攻撃と、9月23日の6041/TCPに対する攻撃は、中国国内で発生しています。この2つのポートに対応するアプリケーションは不明ですが、後者はゲーム関連企業のサーバに対する攻撃であることが分かっています。

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[*27]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[*28]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7月から9月の期間中に、ハニーポットに到着した通信の総量(到着パケット数)の推移を図-5に、その発信元IPアドレスの国別分類を図-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。

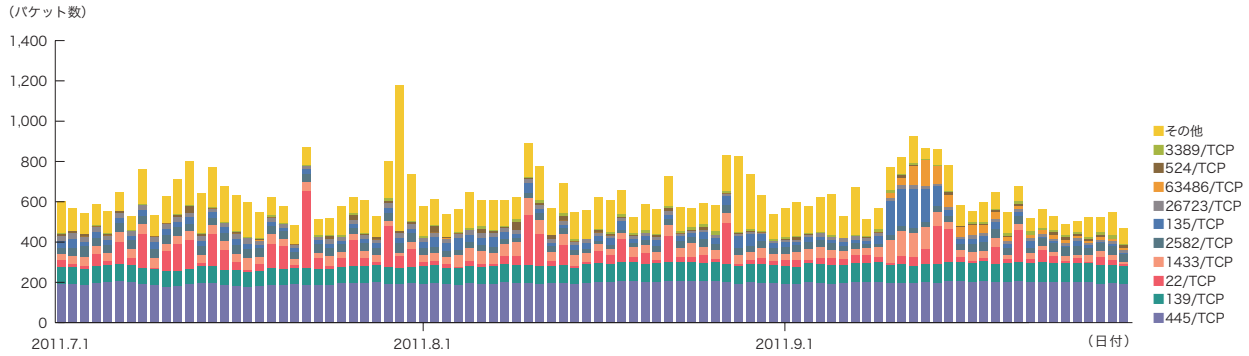


図-5 ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

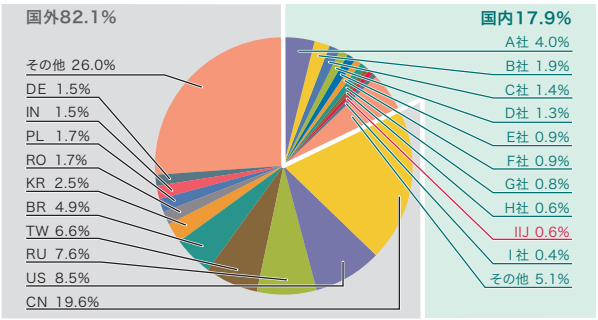


図-6 発信元の分布(国別分類、全期間)

*27 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。

*28 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。

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、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、63486/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-6で発信元の国別分類を見ると、中国の19.6%、日本国内の17.9%が比較的大きな割合を占めています。

9月10日から15日にかけて135/TCP、1433/TCPへ国内の特定のISPと米国からの通信が増加しています。また、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7月22日に中国、8月10日に米国、8月27日にオランダの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。

■ Mortoワーム

また、この期間中にWindowsのリモートログイン機能であるRDPに対して辞書攻撃を行って感染を広げていくMortoワームが発生しました[*29]。図-7はハニーポットに到着したRDP(3389/TCP)の通信です。RDPへの探査行為は日常的に発生していますが、8月5日から13日にかけて増加したのち、8月17日から27日にかけて断続的に増加したことが分かります。また、9月9日から13日、9月18日以降についても、増減を繰り返しながら通常時より高い値で通信が推移しています。これはMortoワームの流行によるものであると判断しています。従来RDPに対する通信は主に中国から発生していましたが、上記の期間においてはその他の国からも到着していることから、このワームが世界中で流行した可能性を示唆しています。

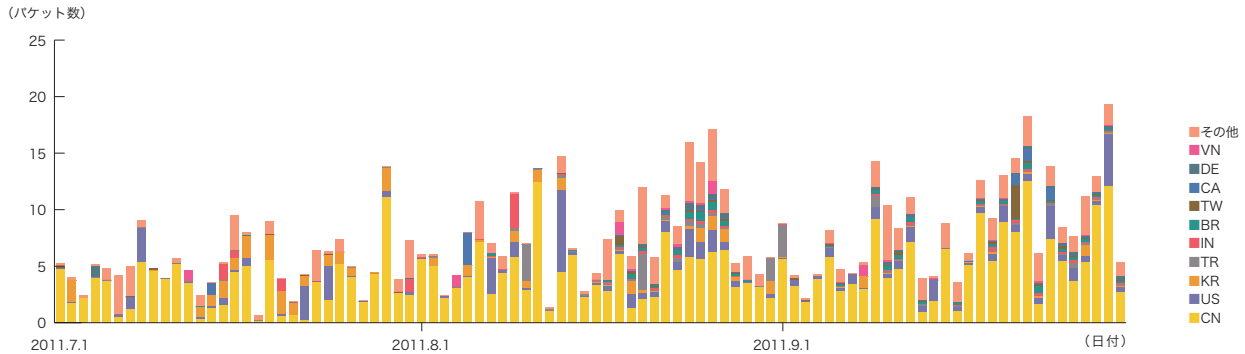


図-7 ハニーポットに到着したRDP(3389/TCP)通信の推移(日別・国別・一台あたり)

*29 次のエフセキュアブログでは「Windowsリモートデスクトップワーム『Morto』が拡散」(http://blog.f-secure.jp/archives/50625847.html)として、このマルウェアの挙動を伝えている。

■ 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-8に、マルウェアの総取得検体数の推移を図-9に、そのうちのユニーク検体数の推移を図-10にそれぞれ示します。このうち図-9と図-10では、1日あたりに取得した検体[*30]の総数を総取得検体数、検体の種類をハッシュ値[*31]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。

期間中での1日あたりの平均値は、総取得検体数が57,352、ユニーク検体数が1,294でした。マルウェアの種類では、Conficker が支配的で、総検体取得数で73.7%、ユニーク検体数で70.1%を占めています。図-8に示す検体取得元の分布では、日本国内が2.9%、国外が97.1%でした。これは、Conficker が主に国外で大規模に活動しているためです。また、期間中にユニーク検体数には変化が見られませんでしたが、総取得検体数には増加傾向が見られます。これは一部のConficker の活動がわずかながら増加傾向にあるためです。

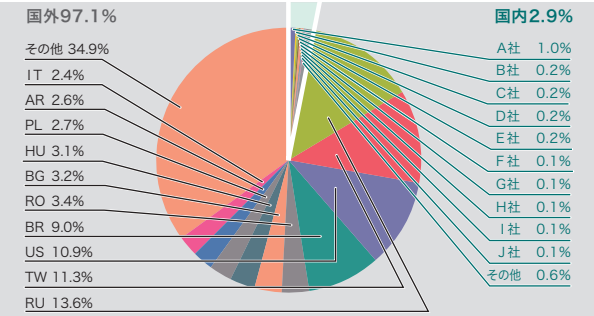


図-8 検体取得元の分布（国別分類、全期間）

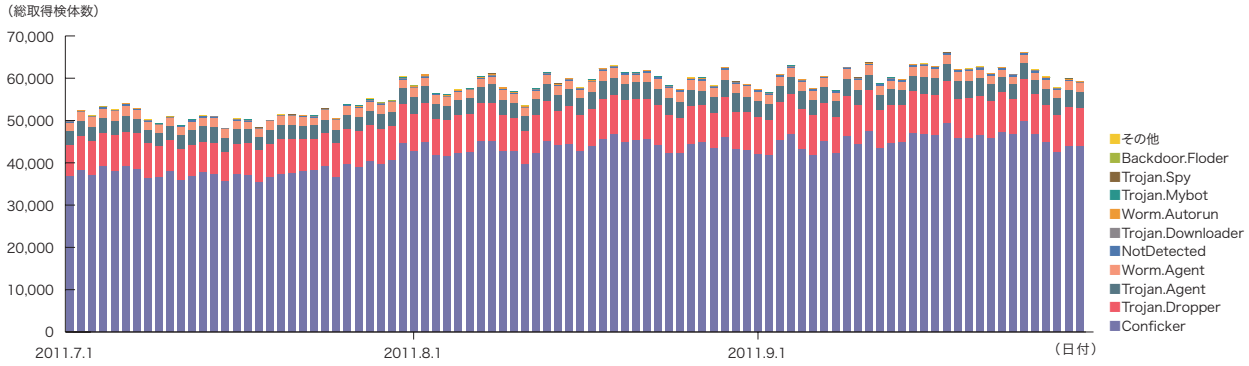


図-9 総取得検体数の推移

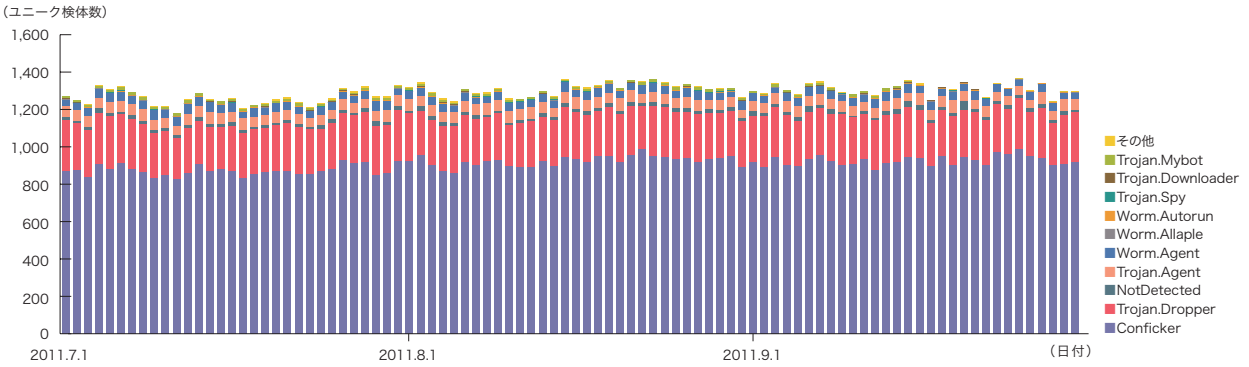


図-10 ユニーク検体数の推移

＊30 ここでは、ハニーポット等で取得したマルウェアを指す。

＊31 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、本節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。

次に同様の期間中、後述の手法でConfickerと判定された検体を除いた、マルウェアの検体取得元の分布を図-11に、マルウェアの総取得検体数の推移を図-12に、そのうちのユニーク検体数の推移を図-13にそれぞれ示します。このうち図-12と図-13では、1日あたりに取得した検体の総数を総取得検体数、検体の種類をハッシュ値で分類したものをユニーク検体数としています。図-11では、タイからの検体取得の割合が27.6%と多くの割合を占めています。これは1〜2日間だけ活動した検体が多く見られたためです。また、図-12では、Mybotの感染活動が行われているのが確認できます。これらの多くは台湾に割り当てられているIPアドレスからの活動でした。ただしMybotは9月16日に原因不明で全世界中で一斉に活動を停止しました。図中で最も大きな割合を占めている未知の検体(NotDetected)の内訳は実行形式のファイルが87.1%、HTML、XML等のテキスト形式のファイルが11.6%、それ以外の不明なバイナリデータが1.3%でした。

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86.9%、ボット型1.4%、ダウンローダ型11.7%でした。また、解析により、16個のボットネットC&Cサーバ[*32]と16個のマルウェア配布サイトの存在を確認しました。

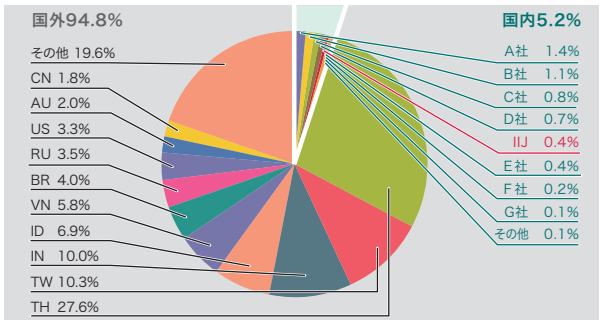


図-11 検体取得元の分布(国別分類、全期間、Confickerを除く)

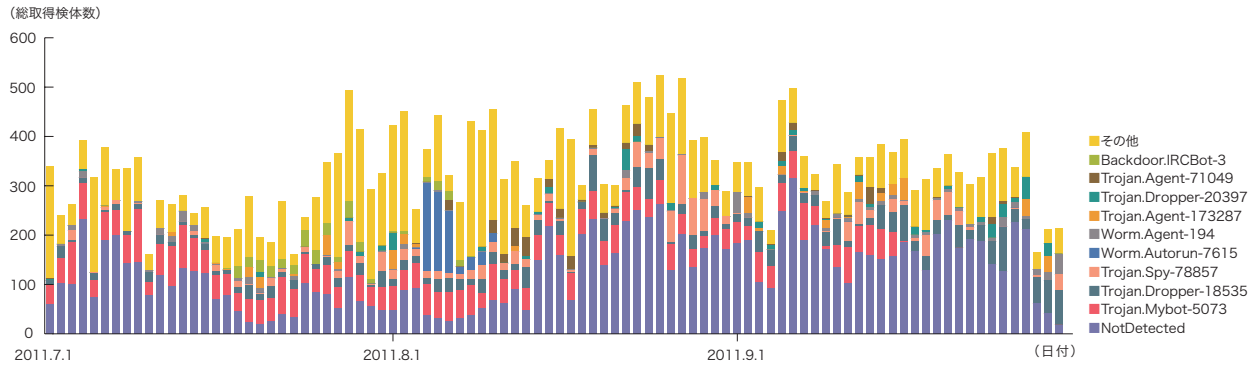


図-12 総取得検体数の推移(Confickerを除く)

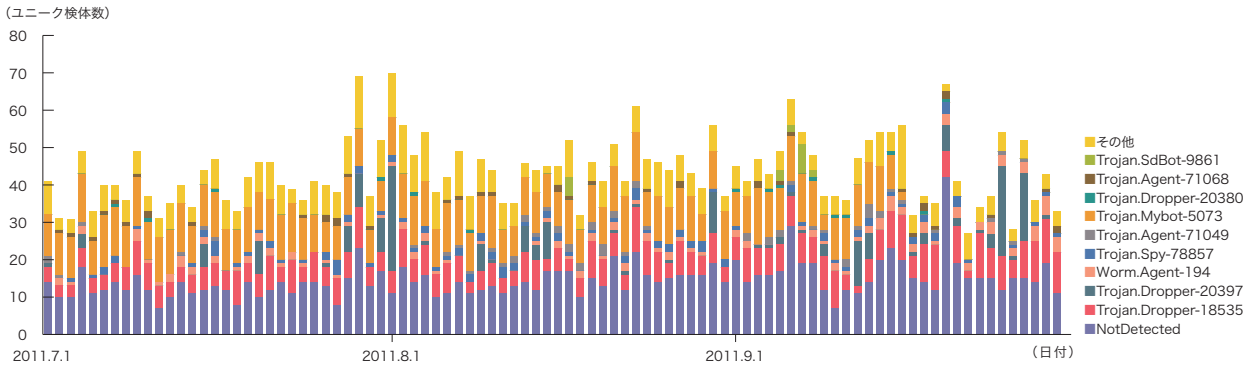


図-13 ユニーク検体数の推移(Confickerを除く)

*32 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司令を与えるサーバ。

■ Conficker の同定

本レポートでは、複数あるウイルス対策ソフトウェアのうちClamAVによる検出を利用してきました。しかし、このソフトウェアで他のマルウェアであると判定された検体に、Confickerと同様の動作を行う検体があることが分かりました。そこで、今回は複数のウイルス対策ソフトウェアの検出名による多数決でConfickerかどうかの判定を実施しました。この処理の結果、総取得検体数の99.4%、ユニーク検体数の96.6%がConfickerであると判定され、その結果を用いて図-11から図-13を作成しました。

ウイルス対策ソフトウェアは、マルウェアを早期に発見して駆除することを目的としたソフトウェアであり、名称に関わらず検体をマルウェアと判定できれば駆除は可能です。つまり、特定の検体に対する判定の違いは、検出処理の速度や負荷を考慮した上での検出方法の違いによるもので、ウイルス対策ソフトウェアの性能の違いを表すものではありません。一方で、本レポートのようにネットワーク上で活動するマルウェアの実態を表現しようとする目的では、一意な名称を継続的に利用することが重要で、このために1つのウイルス対策ソフトウェアによる判別結果を利用してきました。しかし、世界で猛威を振るっているConfickerについて実態を示せないことが明らかになったため、本稿からこの方式を採用することにしました。

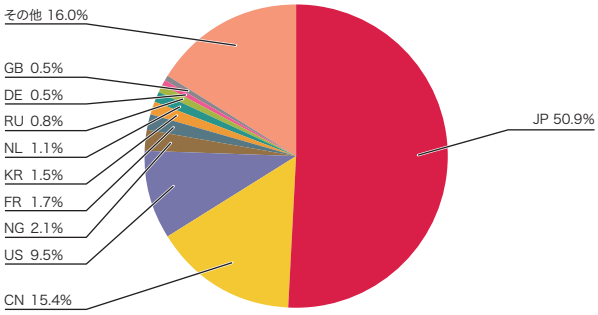


図-14 SQLインジェクション攻撃の発信元の分布

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[*33]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7月から9月までに検知した、攻撃の発信元の分布を図-14に、Webサーバに対するSQLインジェクション攻撃の推移を図-15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。

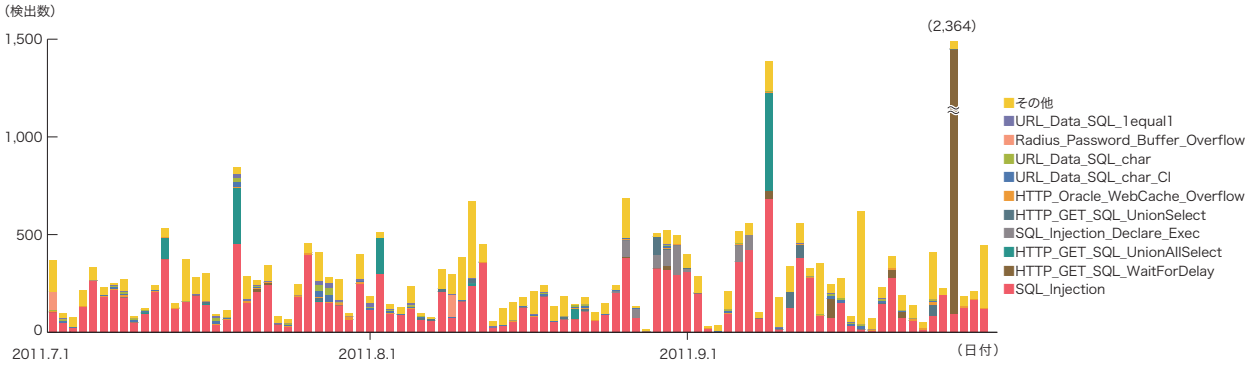


図-15 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*33 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。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。

発信元の分布では、日本50.9%、中国15.4%、米国9.5%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。

国別の通信傾向としてはナイジェリアを攻撃元とする攻撃が特定の攻撃先に対して発生しており、国別の割合でも4位となっています。この攻撃については特定の日に一時的に発生しているため、特定のWebサーバの脆弱性を探る試みであると考えられます。9月27日に起きた攻撃数の増加も、中国の特定の攻撃元から、特定の攻撃先に対して発生しており、同様の目的であると考えられます。また、この期間に話題となった9月18日前後に発生したDDoS攻撃に関連して、SQLインジェクション攻撃も発生しました。攻撃数そのものの増加は見られませんが、この日のSQLインジェクション攻撃の75%は中国からのものでした。

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。

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、Apacheの脆弱性とその対応について示すと共に、攻撃プラットフォームとして多く利用されるようになっているSpyEyeの解析と、公開鍵証明書の不正発行事件について解説します。

1.4.1 Apache Killerとその対応

■ Apache Killerとは

Apache Killerは広く使われているWebサーバソフトウェアのApache HTTPD[*34]（以下Apache）に対する攻撃のコンセプトを実証するためのツールです。このツールの公開時には未知であった脆弱性[*35]を利用してDoS攻撃を仕掛ける手法を示していますが、簡単な改造で実際の攻撃に悪用することができました。このツールは2011年8月20日に脆弱性情報を取り扱うメーリングリストに投稿されました。

Webサーバに対するDoS攻撃は脆弱性を利用せずとも様々な手段で可能ですが、今回の件において影響が大きくなった要因は、既知のDoS攻撃と比較して、公開時点でサポートされているApacheの全バージョンが対象であったこと、攻撃ツールとして公開されており容易に攻撃が可能であったこと、特定のモジュールや設定に依存する脆弱性ではなく、標準的な構成で影響を受けること、開発者への脆弱性報告に先行して実証ツールが公開されたため対策版が存在しなかったことが挙げられます。

＊34 "The Apache HTTP Server Project"（http://httpd.apache.org/）。
＊35 "Apache HTTPD Security ADVISORY UPDATE 3 - FINAL"（http://httpd.apache.org/security/CVE-2011-3192.txt）。

■ 脆弱性と回避策について

Apache Killerで指摘された脆弱性は、HTTPリクエストにおけるRange:ヘッダの処理に起因しています。通常このヘッダはコンテンツの一部の区間のみを取得したい場合に使われます。2007年の時点でこの区間を複数かつ大量に指定し、コンテンツの増幅が可能な問題[*36]が既に指摘されていました。このようなリクエストを受けた場合の動作は、HTTP 1.1のプロトコルが定義されているRFC 2616[*37]にて定められておらず、Apacheのみではなくマイクロソフト社のIIS等も影響を受けるとの指摘でした。プロトコルについては、現在RFC 2616の修正[*38]が提案されています。

一方、Apache Killerも同一ヘッダに類似した値を指定する点は共通ですが、Apacheの実装に起因する脆弱性であるため、他の製品は影響を受けません。

この脆弱性に対しては、設定によるRange:ヘッダの削除、または多数の区間を指定するリクエストの拒否が回避策となります。Apacheのバージョンにより設定可能な条件が異なりますが、一定数以上の区間が指定された場合に処理を制限する点は共通です。Apache Killerでは、標準設定で最も影響が大きくなる1,300区間程度が指定されていました。

ブラウザやダウンローダ等のソフトウェアでは単一の区間指定のみを利用している場合が多いため、この回避策を設定しても殆ど副作用がありません。一部のソフトウェア、例えばAdobe社のAdobe Readerの古いバージョンにおいて複数の区間指定を行うことが知られていますが、現実的な値の区間数を設定すれば、通信に影響を与えずに防御が可能です。多くの区間を許容するとそれに比例して攻撃を受けた場合の影響も大きくなりますが、例えば100区間程度であれば脆弱性は発現せず、副作用と防御のバランスが取れた値であると考えられます。

■ 既知のDoS攻撃との違い

Webサーバのサービス停止を目的とした攻撃には、大きく分けて2種あります。トラフィックやリクエストを大量に送りつける量による攻撃と、ソフトウェアやプロトコルの脆弱性を悪用する攻撃です。Apache Killerは後者に分類されますが、この種の従来の攻撃手法、例えばSlowloris[*39]とは異なる影響をWebサーバに与えます。

Slowlorisでは、攻撃の影響がHTTPDに限られます。他のプロセスには影響が少ないため、管理者がサーバにログインし問題の確認や対応を行うことが可能です。一方、Apache Killerではメモリを無駄に消費し、Apacheのプロセス肥大化を誘発する脆弱性を用いており、該当プロセスのみならず、サーバ全体のメモリが枯渇する状況に至ります。そのため他のプロセスにおいても、メモリ不足による異常終了や著しい反応速度の悪化が発生します。この場合、管理者はサーバへのログイン等も出来ず、対策も遅れてしまいます。

■ 時系列での動き

次に、Apache Killer公開から対策完了までの時系列の動きを表-2に示します。まず、公開から対策までの経過日数に注目すると、ツールの公開が先行したため、短期間で対応を行った様子がうかがえます。回避策が判明したのは攻撃ツール公開から6日後で、11日後に対策版(バージョン2.2.20)が公開されました。しかし、このバージョンでは脆弱性は修正されましたが、対策前のバージョンでは正常であった機能に問題がありました。完全な対策版(バージョン2.2.21)は25日後に公開されました。

*36 "Vulnerability Summary for CVE-2007-0086"(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-0086)。
*37 "Hypertext Transfer Protocol -- HTTP/1.1"(http://www.ietf.org/rfc/rfc2616.txt)。
*38 "Add limitations to Range to reduce its use as a denial-of-service tool"(http://trac.tools.ietf.org/wg/httpbis/trac/ticket/311)。
*39 "Slowloris HTTP DoS"(http://ha.ckers.org/slowloris/)。

■ 対策の選択

脆弱性の対応として、開発者側から無条件に対策版への更新を勧められる場合があります。しかし、今回の件からも分かるとおり、必ずしもそれが常に最良の選択というわけではありません。Apache Killerについては、提案された回避策では一部のクライアントでの利用に副作用があるため、万能ではありませんでした。しかし、回避策は対策版に比べて遥かに早く提供されており、潜在的なリスクも低く、バージョン2.2.21がリリースされるまでは、回避策の適用が最も安定した対応であったと考えることができます。

一方、対策版は実際にリリースされるまで、修正により動作にどのような影響があるか確認出来ず、リスクの見積もり自体が不可能でした。回避策の適用であれ、対策版へのソフトウエア更新であれ、どちらも実施前に副作用等の検証が必要な点は変わりませんが、ソフトウェアの変更が少なく、早期に対応が開始可能な対策ほど、脆弱性を攻撃される危険を早く排除することができます。

インターネットに公開されるシステムを運用する場合、脆弱性への対応は、攻撃される前に実施しなければならない重要な運用項目です。特に短時間での対応が要求される場合には、必ずしもソフトウェアの更新が最適な手法ではありません。本稿で紹介したように、設定等による回避策を検討し、副作用を把握した上で適用することで、脆弱性からシステムを保護できる場合もあります。脆弱性に対策した結果、本来の機能に問題が発生してしまっては本末転倒ですので、リスクが低く確実性の高い対策手段を選択することが、システムの安定的な運用のためには必要です。

日 付	出 来 事	備 考	経過日数
08.20	**Full Disclosure MLに新しい脆弱性を用いた攻撃ツールApache Killerが投稿される。容易に実行可能であり、対策方法も明らかになっておらずゼロディ攻撃が可能な状態となる。**	**脆弱性公開**	**0**
08.21	Full Disclosure MLにて攻撃ツールの利用する脆弱性や影響を受ける条件等についての議論が進む。Apache 2.2系における攻撃成立が報告される。		1
08.23	Apacheの開発者MLにFull Disclosure MLの情報が展開され議論及び脆弱性の修正が開始される。		3
08.24	脆弱性を公開したと思われる人物によりApacheのBugzilla(バグ管理システム)へ登録される。		4
08.24	CVEのID(CVE-2011-3192)を割り当てた旨がApache HTTPDの開発者よりFull Disclosure MLに投稿される。		4
08.25	**Apacheのセキュリティアドバイザリ公開。設定による回避策が公開される。この時点で公開されている全バージョン(1.3系、2.0系、2.2系)が影響、48時間以内にパッチまたは対策版公開と記載される。**	**回避策公開(1回目)**	**5**
08.25	利用者の多い大規模掲示板がこの脆弱性を利用した攻撃を受ける。		5
08.26	**Apacheのセキュリティアドバイザリ UPDATE 2が公開される。設定による回避策に不備があり、その部分が訂正される。対策版提供は延期され、24時間以内と記載される。**	**回避策公開(2回目)**	**6**
08.27	Apacheのセキュリティアドバイザリ UPDATE 2で宣言した期限。開発者用のMLやリポジトリではコードの修正及び議論が続行中。この時点で再アナウンス等の動きはなし。		7
08.30	Apache 2.2.xのリポジトリへ対策コードがバックポートされる。		10
08.30	DebianのApache2パッケージのセキュリティアップデートが公開される。		10
08.31	Apache 2.2.20のパッケージングが完了し、開発者によるテストが開始される。		11
08.31	DebianユーザからDebian MLへバグが報告される。この時点では情報不足により原因箇所の特定には至らない。		11
08.31	**Apache 2.2.20の開発者によるテストが完了する。リリースノート、パッケージが公開される。**	**対策版公開(1回目)**	**11**
08.31	Apacheの開発者はDebian MLにおけるバグの報告を認知したが、この時点では詳細が不明のままであった。		11
08.31	JPCERT/CCより国内向けのセキュリティアドバイザリが公開される。国内各種報道にて取り扱われる。		11
09.01	Red HatよりApache 2.2.20の修正を元にした対策版パッケージがリリースされる。		12
09.01	CentOSよりRed Hatの修正を元にした対策版パッケージがリリースされる。		12
09.01	Apache 2.2.20のリグレッション(2.2.20にて新規に追加されたバグ)がBugzillaへ登録される。		12
09.01	Apache開発者達が2.2.20におけるバグ報告及びリグレッションへの対応ついて、開発者ML上で議論を開始する。その結果、問題点を修正した2.2.21のリリースが必要との方向で意見が一致するが、他のバグ報告がある可能性を考慮し、リリースは翌週半ばまで待つと判断される。この時点で2.2.20には複数の問題が発見されていたが、アドバイザリ等のアップデートは実施されなかった。		12
09.01	Apacheのセキュリティアドバイザリ UPDATE 3の草稿が公開される。1.3系が影響対象外の記載有り。		12
09.05	Apache 2.2.21のリリースのために2.2.xのリポジトリに対して修正コードのバックポートが開始される。2.2.20におけるリグレッションやRFCに違反した動作が修正される。		16
09.10	Apache 2.2.21のパッケージングが完了し、開発者によるテストが開始される。		21
09.13	Apache 2.2.21の開発者によるテストが完了する。各ミラーサーバへパッケージの同期が開始される。		24
09.14	**Apache 2.2.21のリリースノート、パッケージが公開される。セキュリティアドバイザリUPDATE 3が公開され、正式に1.3系が影響対象外となる。**	**対策版公開(2回目)**	**25**
09.15	JPCERT/CCのセキュリティアドバイザリが更新される。		26

※日付は日本標準時、同日の出来事は早い順で記載。また、注目すべき出来事を太字で記載している。

表-2 Apache Killerに関連する出来事一覧

1.4.2 SpyEye

SpyEyeはCrimeware Kitに分類されるマルウェアです。Crimeware Kitとは、端末からアカウントやパスワード（特に金融関連のもの）等の個人情報を盗み出すマルウェアを生成するためのフレームワークの総称です。先日ソースコードが漏えいしたことでも話題になったZeuS[*40]もCrimeware Kitに分類されます。日本では2011年4月から6月にかけて感染者数が増加したとの情報[*41]もあります。IIJでは独自にSpyEyeのバージョン1.3.10と1.3.45の検体を入手し、調査、解析を行いました。本項では、SpyEyeの機能及び動作の概要について解説すると共に、SpyEyeを検出する方法を検討します。

■ SpyEyeの概要

SpyEyeのシステムは大きく分けて2点から構成されています。ユーザの端末に感染後、アカウントや情報を盗み出すボットを作り出すためのビルダと、ボット化した感染端末やそこから搾取した情報を管理するサーバプログラムです。攻撃者はまずこれら2つが同梱されたフレームワークをアンダーグラウンドで製作者から購入して、システムを構築します。SpyEyeによる情報搾取の流れを図-16に示します。

システム構築後、攻撃者はビルダでボットを作成し、ユーザの端末に何らかの手段を用いてインストールさせます。ビルダによって生成されるSpyEye本体には他の端末への感染能力はありません。したがって、攻撃者は別途Exploitkit[*42]のような脆弱性を悪用するためのツールを入手して組み合わせるか、ソーシャルエンジニアリング等の手法を用いる必要があります。

ボットがユーザの端末にインストールされると、そのボットによって他のプロセスにインジェクトされたコードがHTTP/HTTPSによる通信を監視し、ビルド時の設定に基づいてユーザアカウント等搾取した情報を攻撃者のサーバに送信します。攻撃者はその送信された情報をサーバのWeb UIから確認したり、ボットの制御や更新を行ったりすることができます。SpyEyeのWeb UIは、ボットの制御を

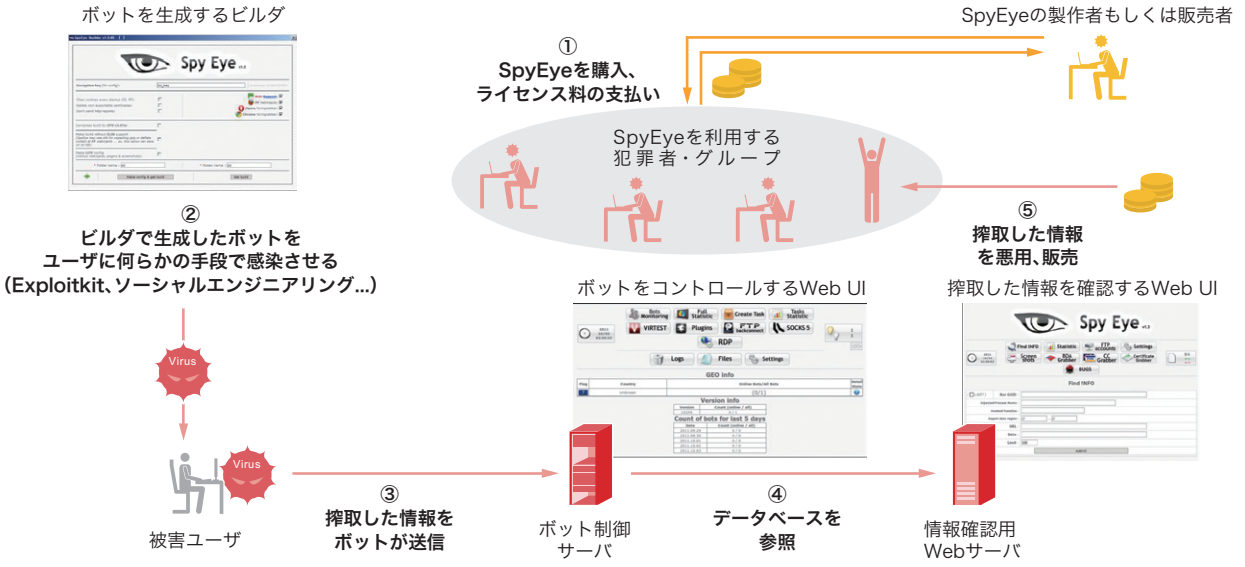


図-16 SpyEyeによる情報搾取の流れ

*40 ZeuSはSpyEyeよりも先行して2007年ごろから確認されているCrimeware Kitであり、今年の5月にはそのソースコードが流出して話題になった。McAfee Blog、「Zeusボットネットについて」(http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1093)。

*41 感染者数の増加はIBMのTokyo SOC Reportのブログや IPAのWebページ等で報告されている。「SpyEyeウイルスの検知件数増加を確認」(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/spyeye_20110425?lang=ja)。「SpyEyeウイルスの検知件数増加を確認（続報）」(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/spyeye_20110817?lang=ja)。「コンピュータウイルス・不正アクセスの届出状況[8月分]について」(http://www.ipa.go.jp/security/txt/2011/09outline.html)。

*42 Exploitkitについては IIJ Technical WEEK 2010の「セキュリティ動向 2010（1）Web感染型マルウェアの動向」でも紹介している(http://www.iij.ad.jp/development/report/2010/__icsFiles/afieldfile/2011/01/31/techweek_1119_1-3_hiroshi-suzuki.pdf)。

行う画面と、搾取した情報を確認する画面が図-16のように完全に分離しており、ZeuSに比べると攻撃の分業化が進んでいることが伺えます。

このように、技術レベルの低い攻撃者でもSpyEyeを購入することで情報搾取の仕組みを簡単に構築可能です。最近はボットのインストールを代行するPPI(pay-per-install)サービスを提供する業者も出現しており[*43]、そのような業者を利用すれば攻撃者が情報を盗むための障壁はさらに低くなると考えられます。

次に、SpyEyeのボットプログラムの特徴を説明します。SpyEyeのボットには、ユーザがWebで送信する情報を単純に搾取する機能のほかに、マウスクリックのタイミングに合わせてスクリーンショットをとる機能や、Webインジェクションと呼ばれる機能があります。スクリーンショットをとる機能は、オンラインバンキング等の認証画面で用いられているソフトウェアキーボードの入力を確認するために使われます。Webインジェクションは、攻撃者が望む情報を追加で搾取するために使われます。例えば、図-17のように、本来であればIDとパスワードの入力のみでログイン可能なサイトにおいて、Web画面の入力フィールドを改ざんすることで、追加で別の情報を搾取できるようにします。この改ざんの設定はビルド時にボット内部に同梱するファイル(webinjects.txt)に記述します。この例のように日本語を含むテキストも挿入可能です。

また、攻撃者はプラグインと呼ばれるモジュールを追加購入することで、ボットにさまざまな機能を付加することができます。例えば、FTPやSOCKS、RDPを使ってバックコネクトを行う機能、クレジットカード情報や証明書を取得する機能、DDoS攻撃を行う機能、USBデバイス経由で感染活動を行う機能等をプラグインとして組み込むことができます。

■ ボットの動作及び特徴

SpyEyeのボットはZeuSと同様にWindows XPだけでなく、Windows 7やVista等のOSでもUAC(User Account Control)[*44]等の警告なしに動作するように設計されています。また、Webインジェクションの設定やボットの接続先のURL、プラグインのDLLや設定ファイルをconfig.bin[*45]として実行ファイルの内部に保持することで、動的な設定変更や機能追加を可能にしています。

ボットの動作概要を以下に示します(図-18)。ボットは最初にインラインの実行ファイルをロードした後に、その

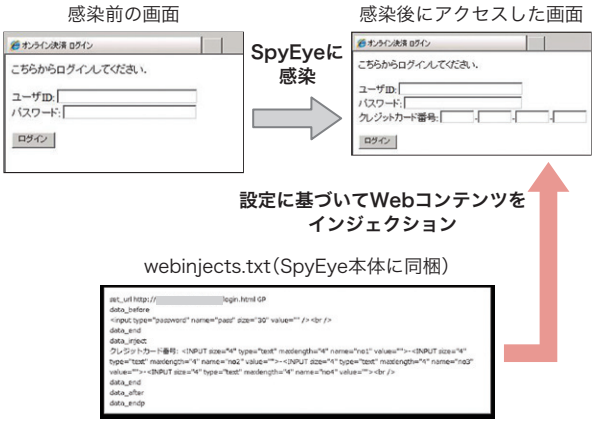


図-17 SpyEyeによるWebインジェクションの例

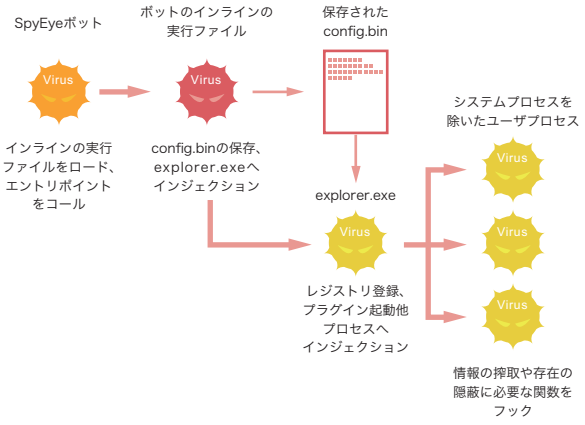


図-18 SpyEyeボットの動作概要

*43 pay-per-installサービスの市場調査や観測については、以下が詳しい。"Measuring Pay-per-Install: The Commoditization of Malware Distribution" (http://usenix.org/events/sec11/tech/full_papers/Caballero.pdf)。

*44 UACとは、Windowsの機能の1つで、管理者レベルのアクセス許可を必要とする変更をプログラムが行ったときに、ユーザに通知することにより、ユーザがコンピュータを制御し続けられるようにする技術を指す。マイクロソフト社、「ユーザー アカウント制御とは」(http://windows.microsoft.com/ja-JP/windows7/What-is-User-Account-Control)。

*45 config.binはパスワード付きzipを即値のXORでエンコードしたバイナリファイルになっている。SpyEyeはこのバイナリファイルを様々なプロセスから参照するため、zipのパスワードを環境変数に保存する。1.3.10ではconfig.binという固定のファイル名だったが、1.3.45ではビルド時の指定フォルダ名や取得したOSバージョン等の文字列を基に生成した数値をファイル名にしている。

エントリポイントをコールします[*46]。そこからの実行では、config.binをファイルに保存するほか、explorer.exeへのコードインジェクションが行われます。インジェクションされたコードは、ボットをシステム起動時に実行するためにレジストリへの登録を行います。また、config.binに含まれているプラグインを起動するとともに、一部のシステムプロセスを除いたプロセスへさらにインジェクションを行い、最終的にそのインジェクトされたコードが情報の搾取やボットの存在の隠蔽に必要な関数をフックすることになります。

SpyEyeは製作者がコードの追加・変更を容易に行えるように工夫されています。具体的には、カスタムリソースからconfig.binや、インジェクションによって実行されるコード等を取得して利用します。また、前述のようにインラインの実行ファイルを動的にロードして内部で実行するのは、初回実行時のインストール動作と二度目以降の本来目的の動作を柔軟に変更できるように、コードを分離することが狙いだと考えられます。

SpyEyeにおいてコードの難読化手法はいくつか使われていますが、最も特徴的な手法は呼び出したいライブラリ関数を、その名前から事前に生成した数値で指定して呼び出すものです[*47]。これは一般的にはシェルコードにおいて用いられる手法です。解析者が呼び出している関数を把握するためには、デバッグで都度実行して確認するか、その数値化のアルゴリズムを解析する必要があります。

■ 検出方法の検討

SpyEyeに感染した端末の検出方法としては、大きく分けて通信からの検出と、ホスト上での検出があります。ここでは、通信からの検出について検討します。

SpyEyeのボットは、主に2種類のサーバと通信を行います。1つはcollectorと呼ばれるプログラムとの通信、もう1つはサーバのWeb UIとの通信[*48]です。collectorとの通信はボットの起動時や盗んだ情報の送信時等に発生します。例えば、ユーザがWebサーバへデータを送信すると、そのデータに加えてボットのIDやプロセス名、フックした関数の情報等がcollectorに送信されます。collectorに送信されるデータは、圧縮処理とXORによる特殊なエンコードが施されており[*49]、IDS/IPS等でリアルタイムで検知することは困難です。

一方で、Web UIとの通信は、ボットのコントロールや生存確認のために、ボットのIDやコンピュータ名、そのボットがサポートしているプラグインの情報等が1.3.10ではGETパラメータ、1.3.45ではbase64でエンコードされたPOSTパラメータとして定期的に送信されるため、こちらの情報を用いた検出は可能だと考えられます。

また、ホスト上での検出方法としては、SpyEyeのボットはユーザモードで動作するので、感染しているホスト上からGMER[*50]等のルートキット検出ツールを使ってインストールされたファイルや追加されたレジストリの値をチェックすること等が考えられます[*51]。

■ まとめ

SpyEyeの開発は今も積極的に行われています。今回解析したSpyEyeはバージョンが1.3.10、1.3.45と近いものでしたが、コードの難読化やインジェクションの動作等がより巧妙になっており、今後も注意深くその動向を追っていく必要があります。また、SpyEyeは一度感染すると情報漏えいや金銭被害等の直接的で大きな被害を生むため、感染を防ぐことや、感染を検出することが大事です。Exploitkit等を使ったdrive-by-download攻撃経由での感染を防ぐために、OSやブラウザ、ブラウザプラグインに対するパッチ適用を迅速に行うことやウイルス対策ソフトウェアを導入し、常に最新の状態を保つこと等が重要になります。また、メール等でのソーシャルエンジニアリングによる感染も考えられるので、リンクや添付ファイルを無闇に開かないといったことにも注意が必要です。

＊46 初回起動時は端末の情報を収集し、explorer.exeへコードをインジェクションした後、ビルド時に指定したフォルダの下にボットをコピーするインストール動作を行う。
＊47 1.3.45ではインジェクション対象のプロセス名やインストール後の実行ファイル/config.binの名前、プラグインのエクスポート関数名等の重要な文字列も数値化されている。
＊48 サーバのWeb UIと通信を行うには、customconnectorというプラグインが別途必要。
＊49 圧縮のアルゴリズムを詳細には解析していないが、オリジナルではないかと推測される。また、XORは即値をキーとしていない。
＊50 "GMER - Rootkit Detector and Remover"(http://www.gmer.net/)。
＊51 ただし、作成されるフォルダやファイル名、レジストリの値等は端末ごとに異なる。

1.4.3 公開鍵証明書の不正発行事件

■ 事件の概要と経緯

今年に入り認証機関への侵入行為により不正に証明書が発行される事件が相次いでいます。3月に起きたComodoの事件では9件の証明書が不正に発行され、また8月末に起きたDigiNotarの事件では500以上もの証明書が不正に発行されました。これらは同一犯ComodoHackerによる事件で、後者の犯行声明において、StartComとGlobalSignの2社を含む4つの他の認証機関においても証明書が発行できる状態にあることが発表されました。これを受けてGlobalSign社は事実確認を行うために一時期証明書発行業務を停止していました。これらの事件により、認証機関及びPKI(公開鍵認証基盤)の仕組み自体の信頼性が揺らいでいます。本節では、これらの公開鍵証明書の不正発行の影響と対策について取り上げます。

■ 公開鍵証明書の仕組み

公開鍵証明書は、個人やサーバ等のエンティティを第3者がインターネットを介して認証するために利用されるデータです。証明書内に含まれている公開鍵とエンティティの結び付けの確からしさは、RSAやECDSA等の公開鍵暗号を用いた暗号学的なデジタル署名により保証されます。証明書は信頼のおける認証機関(Certification Authority; CA)がその発行を行います。証明書は階層的に発行可能なため、複数の中間CA証明書を介して最終的にエンドエンティティ向けの証明書が発行されることもあります。発行元から発行先への証明書発行は信用の方向を意味し、その逆方向に証明書検証を行って最終的に自己署名(ルート)証明書まで遡ることでトラストアンカー(信頼点)に行き着くという仕組みで確からしさを確認します[*52]。

通常のインターネットユーザが目にする公開鍵証明書はSSL/TLSプロトコルでアクセスしたサーバの証明書で、X.509仕様[*53]に則った証明書であることがほとんどです。証明書内にはサーバの所在を示すFQDN(Fully Qualified Domain Name)が記載されており、ブラウザを経由してユーザがアクセスしているURLのものと一致するか確認します。CAを信頼することで当該CAから発行されたサーバ証明書を信頼する、という一連の手続きにより安全な通信が成り立ちます。しかし、この時トラストアンカーの設定はプレインストールされているCA証明書群の確からしさをユーザが信頼していると仮定して、OSやブラウザ等のアプリケーションにより行われるのが普通です。ユーザはプレインストールされた証明書群から独自のトラストアンカーを構築することが望まれているのですが、これらのデータを操作するユーザはほとんどいないのが現状です。

今回の事件では、ユーザがベンダの指定するトラストアンカーを鵜呑みにしたために「サーバ認証」を正しく行うことができませんでした。ユーザが所望するサーバとは異なる第3者(攻撃者)と通信してしまうことで、正規の安全な通信を行っているように見えてしまうことが問題です。Webサーバの認証の段階で確からしさが保証できていないのですから、それ以降の秘匿性、完全性といった安全性が正しく確保されていたとしても、その通信は攻撃者サーバに対してセキュアな通信路を確保しているだけで、まったく安全とは言えません。

■ 不正な証明書発行による影響

次に、このような正しいFQDNの保持者に対する証明書が不正発行されたことによる影響について考えます。例えば、攻撃者がexample.co.jpのドメインに対する証明書発行依頼を不正侵入されたCAに対して行い、example.co.jpの保有するFQDNが含まれた不正証明書を取得する場合を考えます。この時、攻撃者は自分の鍵を利用してこの不正な証明書を発行するため、SSL/TLSにおいてこのFQDNについては正しくサーバ認証の処理を行うことができるようになります。しかしexample.co.jpドメイン配下に当該FQDNを持つ攻撃用サーバを置くことができないのであれば、前述したブラウザのFQDNチェックにより(アクセスしているサーバのURLと証明書内のFQDNが異なるため)証明書を受け入れることはありません。そのため攻撃者の前提条件は限定されます。

*52 PKIの仕組みについては以下に詳しい。IPA、「PKI 関連技術解説」(http://www.ipa.go.jp/security/pki/)。

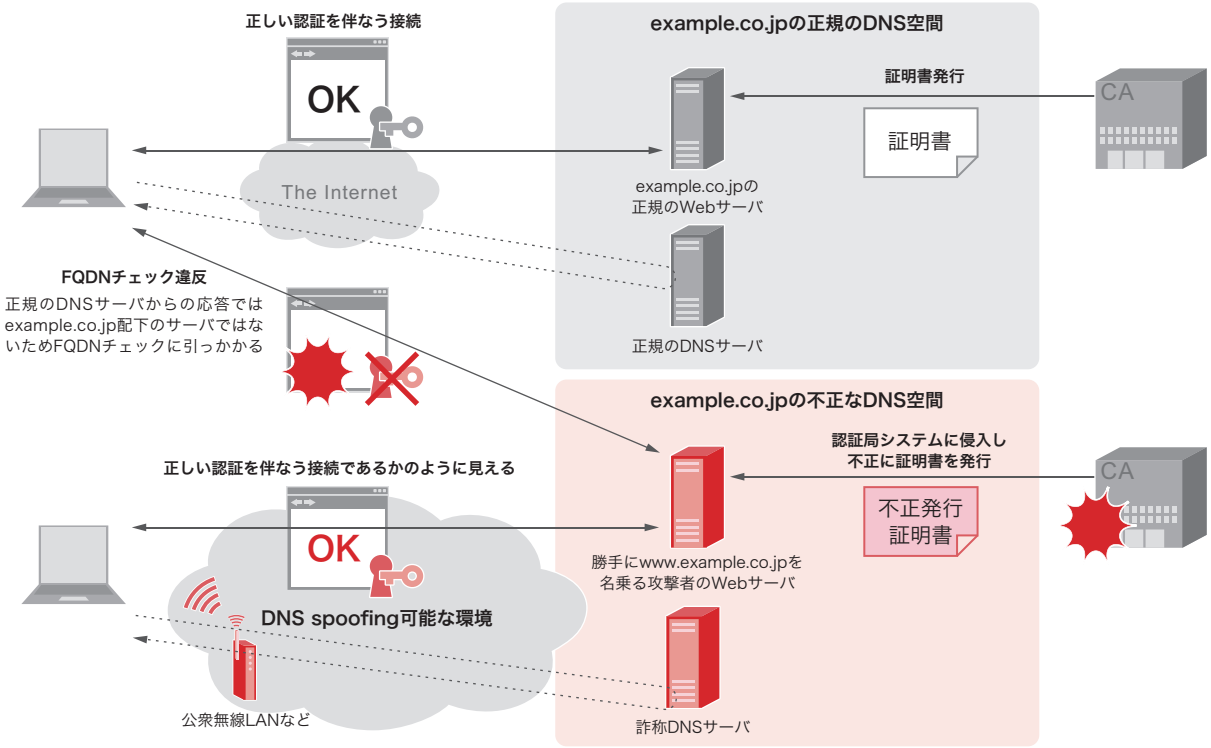
*53 ITU-T Recommendation X.509(08/05)ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory:Public-key and attribute certificate frameworks. 2005.

例えば公衆無線LAN等を利用している際にDNS情報を書き換えるDNSスプーフィングによって攻撃が成功する例を図-19に示します。この例では、example.co.jpドメインのFQDNを攻撃者の保有するサーバのIPアドレスに詐称することで攻撃者サーバに誘導する場合が考えられます。SSL/TLSプロトコルを利用してブラウザで当該サイトにアクセスした場合にはブラウザによるFQDN同定チェックも通過します。DNSスプーフィングのほかにも経路上の乗っ取りにより中間者攻撃サーバを配備することが可能であれば同様の攻撃が可能となります。

DigiNotar事件では、google.comの不正発行証明書に対して約30万アドレスから、オンライン証明書検証プロトコルのひとつであるOCSP(Online Certificate Status Protocol)の通信が行われたことが観測されています[*54]。これはブラウザで不正発行証明書が利用されていたことを示す証拠となっています。OCSPが実装されていない、OCSPの通信を行わないように設定されているブラウザもあることから、実際にはさらに多くのPCで不正発行証明書が受け入れられていたと考えられます。

■ 対策方法

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、証明書を無効化する仕組みが備わっています。証明書が不正発行された今回の事件では、不正発行された証明書を認証機関が無効化することで不正利用をブロックするという対策は理論的には有効であると考えられます。しかし一度正規な証明書として発行されてしまった証明書を無効として扱う仕組みが不十分もしくは全く準備されていない製品群においては、大規模な対策が必要になると考えられます。特に、更新頻度の少ない組み



認証局システムに侵入され、www.example.co.jpについて不正証明書が発行されたとしても、攻撃対象ドメインの配下にサーバを実際に設置するか、何らかのDNSの不正操作と併用しないと攻撃は成立しない。この図はDNS spoofingによりFQDNチェックを迂回する例。

図-19 認証局システムへの侵入による証明書不正発行事件

*54 FOX-IT Interim Report, v1.0, "DigiNotar Certificate Authority breach, September 5, 2011"(http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html)。

込み系製品において、証明書の失効情報の確認を簡素化・省略している場合に留意すべきです。

また根本的な対策方法として現在のPKIと併用して強固にする、もしくは現在のCAの仕組みを置き換える動きがあります。DNSSECを用いて証明書を配送したり証明書とサーバの確からしさを確認したりする機構を持つDANE[*55]や、信頼度を高めるために複数の公証局を配置して確からしさを保証するConvergence[*56]等の提案がそれにあたります。これらの技術が浸透するためにはまだ多くの時間を要すると考えられますが、今回の事件のようにPKIの仕組み自体の信頼性が揺らいでいる今、世論の動きによっては大きくシフトする可能性を秘めています。

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、8月に発見された未公開脆弱性の検証ツールApache Killerとその対応について、世界中で被害をだしているSpyEyeの解析と、公開鍵証明書の不正発行事件とその影響について解説しました。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めています。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)
小林 直(1.4.1 Apache Killerとその対応)
春山 敬宏(1.4.2 SpyEye)
須賀 祐治(1.4.3 公開鍵証明書の不正発行事件)
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、齋藤 聖悟　IIJサービス本部セキュリティ情報統括室

*55 IPA、「情報セキュリティ技術動向調査(2011年上期) 4. DNSを用いた公開鍵の配送技術 - DANE」(http://www.ipa.go.jp/security/fy23/reports/tech1-tg/a_04.html)。
*56 Convergence(http://convergence.io/details.html)。