スマートフォンのセキュリティ

今回は、SSL/TLS、SSHで利用されている公開鍵の多くが他のサイトと秘密鍵を共有している問題について解説すると共に、スマートフォンに関するセキュリティ事情と、標的型攻撃対策のための情報提供に関する議論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2012年7月から9月までの期間では、国内においては特に太平洋戦争の歴史的日付や、竹島や尖閣諸島などの領土問題に関連した、ホームページ改ざん、DDoS攻撃などが複数発生しました。また、利用者情報を不正にもしくは不必要に取得するスマートフォンアプリケーションが立て続けに発見され、大きな問題となりつつあります。同時にスマートフォン用のOSや機種固有の問題も明らかとなり、悪用の可能性が大きくなっています。加えて、国外においてはAnonymousなどのHacktivismの活動も継続しています。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。

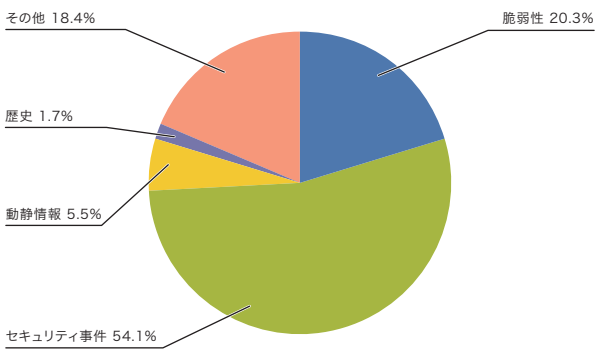


図-1 カテゴリ別比率(2012年7月〜9月)

1.2 インシデントサマリ

ここでは、2012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]。

■ Anonymousなどの活動

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、多数の国の企業や政府関連サイトに対するDDoS攻撃や情報漏えい事件が発生しました。

7月には、オーストラリア政府によるインターネット上の規制強化の動きに反対し、Anonymousが複数の政府系Webサイトを改ざんして抗議しました。更にこれに関連してオーストラリアのISPやクィーンズランド州政府から不正に取得した大量のデータを公開しました(OpAustralia)。また8月には、ロンドンのエクアドル大使館に亡命を認められたWikiLeaks代表のJulian Assange氏の動向に関連して、Anonymousは同氏を逮捕しようとするイギリス政府に抗議し、複数の政府系Webサイトへの攻撃作戦OpFreeAssangeを実施しました。9月には、The Pirate Bayの共同創業者がカンボジアで逮捕されたことを受け、Anonymousによる報復作戦OpTPBが行われました。これにより複数のカンボジア政府のWebサイトが改ざんされたり、情報が漏えいする事件が発生しました。

なお、今年はじめに欧州各国で起きた激しい反対運動の結果、6月に欧州議会で否決されたACTA(偽造品の取引の防

*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、ソフトウェアなど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など、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:歴史上の記念日などで、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、対策などの作業を示す。
セキュリティ事件:ワームなどのマルウェアの活性化や、特定サイトへのDDoS攻撃など、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など、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。

止に関する協定）が、9月に日本の衆議院本会議で可決、締結することが承認されました。批准を決めた国は日本が初めてとなります。このため、国内においても一部で反ACTAデモなどが行われましたが、目立った攻撃活動などは観測されませんでした。

■ 動静や歴史的背景による攻撃

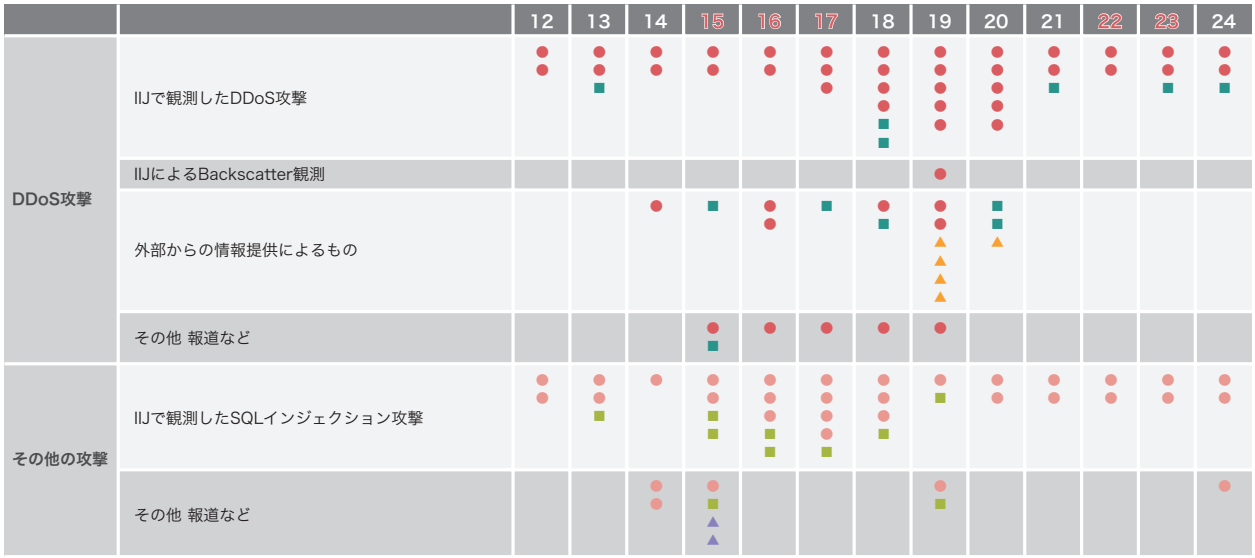
この期間では、7月から開催されたロンドンオリンピックや、9月にロシアで行われたAPEC首脳会議など、国際的なイベントが複数行われました。このようなイベントの開催に伴ったネットワーク上での攻撃が発生する場合があるため注意していますが、この期間において、これらのイベントに関連する攻撃は、IIJの設備及び顧客のネットワークでは検出していません。

一方で、この期間では毎年、太平洋戦争の歴史的日付や、竹島や尖閣諸島などの領土問題に関連したインシデントが発生しています。特に本年は、8月に発生した中国人活動家による尖閣諸島への不法上陸事件に端を発し、国内の複数のWebサイトに対する改ざん事件が発生しました。

更に、9月11日に日本政府が尖閣諸島の国有化を発表したことを受け、中国国内で大規模なデモが発生すると共に、日本国内の複数の政府機関や民間企業のWebサイトに対し、大規模な改ざんとDDoS攻撃が多発的に発生しました。攻撃予告などの情報から、この動きに関連すると判断した攻撃を表-1にまとめます。本年の特徴として、昨年の攻撃に比べ、Webサイトの改ざん被害が多数発生していることが挙げられます。DDoS攻撃については攻撃による被害は少なくなっています。Webサイト改ざんを目的とした攻撃は、政府機関だけでなく金融機関や一般企業に対しても行われました。この攻撃はSQLインジェクションや、ブルートフォースなどによる侵入によって行われていたと考えられます。

攻撃対象には多数の政府機関や民間企業が挙げられていましたが、IIJで観測した攻撃では、対象や発生件数はあまり多くありませんでした。9月18日午後10時過ぎ（日本時間）には、複数の対象への同時多発攻撃を確認しています。この攻撃では最大で1ヵ所に650Mbps、240KppsのUDP FloodとSyn Floodを観測しました。DDoS攻撃の種類としてはHTTP GET FloodやConnection Floodなど、サーバに対する攻撃が多く観測されています。この期間内におけるDDoS攻撃としては、最大で800Mbps、110Kppsの複合攻撃を観測しています。また、攻撃の継続時間は最大で1時間程度でした。

表-1 一連の攻撃の様子（2012年9月）



期間中にIIJが認知した攻撃のうち、攻撃予告と対応する攻撃をDDoS攻撃とその他の攻撃に分けて集計した。
Webサーバに対するSQLインジェクション攻撃やWeb改ざんについてはその他の攻撃に分類している。
特定のサーバに攻撃が発生した日にマークして、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つとした。
ただし、DDoS攻撃とその他の攻撃ではそれぞれ別に集計を行っているため、1つのサーバにDDoS攻撃とWeb改ざんが同時に行われた場合には2つマークされている場合もある。

● 政府官公庁関係/DDoS攻撃　● 政府官公庁関係/その他の攻撃
▲ 教育関係/DDoS攻撃　▲ 教育関係/その他の攻撃
■ 一般企業・団体など/DDoS攻撃　■ 一般企業・団体など/その他の攻撃

7月のインシデント

1 他 **1日**：協定世界時の調整のため、うるう秒の挿入が日本時間8時59分60秒に行われた。
独立行政法人情報通信研究機構(NICT)、「「うるう秒」挿入のお知らせ ― 今年の7月1日は1秒長い日となります ―」(http://www.nict.go.jp/press/2012/01/31-1.html)。

2

3 他 **3日**：Twitter社は、Transparency Report(各国の政府機関などからのユーザ情報の開示請求などの状況をまとめたレポート)を初めて公開した。今回のレポート期間となった2012年1月から6月では、ユーザ情報の開示請求で日本は米国についで2番目であることなどが確認できる。
"Twitter Transparency Report"(https://support.twitter.com/articles/20170002)。

4 他 **3日**：日本は「サイバー犯罪に関する条約」の受諾書を寄託した。これにより本年11月1日より効力が発生することとなった。
外務省、「サイバー犯罪に関する条約」(http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html)。

5

6 他 **4日**：政府の情報セキュリティ政策会議が行われ、標的型攻撃などの高度な攻撃に対する対策の強化や、スマートフォンやクラウドなど新しい情報通信技術への対応などを謳った、「情報セキュリティ2012」が決定した。
内閣官房情報セキュリティセンター、「情報セキュリティ２０１２」(http://www.nisc.go.jp/active/kihon/pdf/is2012.pdf)。

7

8 他 **9日**：日本時間13時1分に、FBIが運用していたDNS Changer感染者向けのDNSサーバの運用が停止された。
DNS Changerについて対策を行っていたDCWGによる発表は次のとおり。"DCWG Ends Clean DNS Function"(http://www.dcwg.org/dcwg-ends-clean-dns-function/)。

9

10 脆 **10日**：Microsoft社は、2012年7月のセキュリティ情報を公開し、MS12-043を含む3件の緊急と6件の重要な更新をリリースした。
「2012 年 7 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-jul)。

11

12 他 **12日**：総務省と経済産業省は、サイバー攻撃の実態を把握し、その結果を関係省庁、重要インフラ事業者等に提供することを目的として、関連4団体と共にサイバー攻撃解析協議会を発足した。
総務省「サイバー攻撃解析協議会の開催」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000021.html)。第1回の議事要旨は次の経済産業省のホームページで確認できる。経済産業省「サイバー攻撃解析協議会」(http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#cyber_attack)。

13

14 他 **13日**：日本国内のドメインレジストラが、規約違反の利用者へのDNSサービスを一時停止したことにより、該当ドメインで提供されていたサービス利用者に影響が生じ、問題となった。

15

16 他 **17日**：情報処理推進機構(IPA)は、内部不正の現状や内部不正に関する意識調査をまとめた、「組織内部者の不正行為によるインシデント調査」の報告書を公開した。
「組織内部者の不正行為によるインシデント調査」報告書の公開(http://www.ipa.go.jp/security/fy23/reports/insider/index.html)。

17

18 脆 **18日**：Oracle社はOracleを含む複数製品について、四半期ごとの定例アップデートを公開し、合計87件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - July 2012"(http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html)。

19 セ **19日**：世界で3番目に大きいと言われているGrum BotnetのC&Cサーバがテイクダウンされ、活動を停止した。
例えば、このテイクダウンに参加したThe Spamhaus Projectに詳しい。"Spam botnets: The fall of Grum and the rise of Festi"(http://www.spamhaus.org/news/article/685/spam-botnets-the-fall-of-grum-and-the-rise-of-festi)。

20

21 脆 **20日**：権威DNSサーバの実装の1つであるNSDに、特殊なDNSパケットを受信することで異常終了する脆弱性(CVE-2012-2978)が見つかり、修正された。
NLnet Labs、"NSD denial of service vulnerability from non-standard DNS packet from any host on the internet. [VU#624931 CVE-2012-2978]"(http://www.nlnetlabs.nl/downloads/CVE-2012-2978.txt)。

22

23 脆 **25日**：Android 4.0.4以前のDNS実装でソースポートとTXIDのランダム性に問題があり、DNSポイズニング攻撃が可能な脆弱性(CVE-2012-2808)が見つかり、修正された。
詳細については、次のIBM Application Security Insiderを参照のこと。Android DNS Poisoning:Randomness gone bad(CVE-2012-2808)(http://blog.watchfire.com/wfblog/2012/07/android-dns-poisoning-randomness-gone-bad-cve-2012-2808.html)。

24

25 脆 **25日**：BIND 9.xに大量のDNSSEC validationを受信することでサービス停止が可能な脆弱性(CVE-2012-3817)が見つかり、修正された。
Internet Systems Consortium、"CVE-2012-3817:Heavy DNSSEC Validation Load Can Cause a ""Bad Cache"" Assertion Failure in BIND9"(https://kb.isc.org/article/AA-00729)。

26 脆 **25日**：BIND 9.9.xに大量のTCP問い合わせを受信した場合にメモリリークが起こり、サービス停止が発生する可能性のある脆弱性(CVE-2012-3868)が見つかり、修正された。
Internet Systems Consortium、"CVE-2012-3868: High TCP Query Load Can Trigger a Memory Leak in BIND 9"(https://kb.isc.org/article/AA-00730)。

27

28 脆 **29日**：米国で行われたセキュリティイベントで、暗号化通信の認証などに利用されているMS-CHAPv2の既知の脆弱性を利用して、短時間に安い料金で認証情報を突き止めるクラウドサービスが発表された。
詳細については次の発見者のBlogを参照のこと。CloudCracker::Blog、"Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate"(https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/)。

29

30 脆 **30日**：5月に公表されたロジテック社製無線LANブロードバンドルータの一部で見つかった脆弱性について、テレコム・アイザック推進会議より注意喚起が行われた。
「【注意喚起】ロジテック製ルータの脆弱性、および、利用者が行うべき必要対策」(https://www.telecom-isac.jp/news/news20120730.html)。

31

[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

■ 未修正の脆弱性を悪用した攻撃

この期間では、未修正の脆弱性が発見され、悪用される事例が複数確認されました。8月26日にはOracle社のJava7に、任意のOSコマンドが実行可能な未修正の脆弱性（CVE-2012-4681）があり、既に攻撃に悪用されていることが報告されました[*2]。PoC（Proof of Concept）も公開されており、この脆弱性を悪用した攻撃が複数のアンチウイルスベンダーから報告されていたため[*3]、Oracle社は8月31日に定例外でこの脆弱性の修正プログラムを公開しました。この脆弱性は最新バージョンのJava7に対してのみ機能し、古いバージョンであるJava6には影響しないことが確認されています。9月18日には、Internet Explorerで未修正の脆弱性が報告されました[*4]。この脆弱性についても公表時点で既に悪用が確認されており、Microsoft社は、9月22日に修正プログラムを公開しています[*5]。

このような未修正の脆弱性を悪用した攻撃は頻繁に発生しており、修正が行われるまでの間は攻撃に対して無防備な状態となってしまいます。このため、ベンダーが推奨する影響を低減するための対策を行うことや、その攻撃による影響が大きいと考えられる場合には、一時的に利用を停止する、代替となるソフトウェアを使用し脆弱性を含むソフトウェアをアンインストールするなど、ユーザ側での対応が必要となります。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*6*7]、Office[*8*9]、Internet Explorer[*10]などで修正が行われました。7月11日に公開されたMicrosoft XMLコアサービスの脆弱性のセキュリティ更新プログラム（MS12-043）では、公開時には対応していなかったMicrosoft XMLコアサービス 5.0に対応した更新プログラムが8月に再リリースされています。Adobe社のAdobe Reader及びAcrobat、Adobe Flash Player、Oracle社のJavaでも更新が行われ、多くの脆弱性が修正されています。また、Apple社のiOSでも、新バージョンのリリースに合わせて、脆弱性の修正が行われました。

スマートフォンやタブレットなど携帯端末のOSとして利用されているAndroidでは、DNS参照の実装にDNSポイズニングが可能な脆弱性が発見され修正されています。

サーバアプリケーションでは、データベースサーバとして利用されているOracleで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ました。また、DNSサーバのBINDでは特定のリソースレコードにより、サーバの異常停止などを引き起こすといった複数の脆弱性が修正されています。DNSでは権威サーバの実装の1つであり、ルートサーバにも採用されているNSDでもサーバの異常終了を引き起こす脆弱性が見つかり、修正されました。

＊2　FireEye Malware Intelligence Lab、"ZERO-DAY SEASON IS NOT OVER YET"（http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html）。
＊3　例えば、次のTrendMicro社のSECURITY BLOGなどでこの脆弱性を悪用した不正プログラムの動作解説がされている。「JRE 1.7に存在するゼロデイ脆弱性を狙った攻撃、バックドア型不正プログラムをもたらす」（http://blog.trendmicro.co.jp/archives/5850）。
＊4　「マイクロソフト セキュリティ アドバイザリ (2757760) Internet Explorer の脆弱性により、リモートでコードが実行される」（http://technet.microsoft.com/ja-jp/security/advisory/2757760）。
＊5　「マイクロソフト セキュリティ情報 MS12-063 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2744842)」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-063）。
＊6　「マイクロソフト セキュリティ情報 MS12-043 - 緊急 XML コアサービスの脆弱性により、リモートでコードが実行される (2722479)」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-043）。
＊7　「マイクロソフト セキュリティ情報 MS12-053 - 緊急 リモート デスクトップの脆弱性により、リモートでコードが実行される (2723135)」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-053）。
＊8　「マイクロソフト セキュリティ情報 MS12-046 - 重要 Microsoft Visual Basic for Applications の脆弱性により、リモートでコードが実行される (2707960)」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-046）。
＊9　「マイクロソフト セキュリティ情報 MS12-060 - 緊急 Windows コモン コントロールの脆弱性により、リモートでコードが実行される (2720573)」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-060）。
＊10「マイクロソフト セキュリティ情報 MS12-052 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2722913)」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-052）。

8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 **9日**：Oracle社より、Java6のサポート終了期限が2012年11月から2013年2月に延長することが発表された。
"Java 6 End of Public Updates extended to February 2013"(https://blogs.oracle.com/henrik/entry/java_6_eol_h_h)。

脆 **10日**：米国で行われたセキュリティカンファレンスで、SSL/TLS、SSH で利用されている公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題が発表された。
詳細については次の21st USENIX Security Symposiumの発表を参照のこと。"Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices"(https://www.usenix.org/conference/usenixsecurity12/mining-your-ps-and-qs-detection-widespread-weak-keys-embedded-devices)。

動 **10日**：韓国大統領による竹島訪問が行われた。

脆 **15日**：Microsoft社は、秘密鍵の解読される可能性の高い、長さ1024ビット未満のRSAキーを使用した証明書の使用を制限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 (2661254) 証明書の鍵長の最小値に関する更新プログラム」(http://technet.microsoft.com/ja-jp/security/advisory/2661254)。

脆 **15日**：Microsoft社は、2012年8月のセキュリティ情報を公開し、MS12-060を含む5件の緊急と4件の重要な更新をリリースした。
「2012 年 8 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-aug)。

脆 **15日**：Adobe Flash Playerに、不正終了や任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「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/apsb12-18.html)。

脆 **15日**：Adobe Reader及びAcrobatに、不正終了や任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「Adobe ReaderおよびAcrobat用セキュリティアップデート公開」(http://www.adobe.com/jp/support/security/bulletins/apsb12-16.html)。

動 **15日**：中国人活動家が尖閣諸島に不法上陸し、逮捕される事件が発生した。

セ **15日**：AT&Tの2ヵ所のDNSサーバがDDoS攻撃を受け、顧客へのサービス提供に影響が生じた。

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。

脆 **17日**：SamsungとHTCのAndroid携帯端末で、ユーザによって入力された情報が参照可能な脆弱性が見つかり修正された。
US-CERT"Vulnerability Note VU#251635 Samsung and HTC android phone information disclosure vulnerability"(http://www.kb.cert.org/vuls/id/251635)。

セ **19日**：尖閣諸島に上陸した中国人活動家の逮捕に関連して、国内で複数のWebサイトが改ざんされる。

脆 **22日**：Adobe Flash Playerに、DoS攻撃を受けたり、任意のコードを実行される可能性がある複数の脆弱性が見つかり、修正された。
「Adobe Flash Player用のセキュリティアップデート公開」(http://www.adobe.com/jp/support/security/bulletins/apsb12-19.html)。

他 **23日**：警察庁から、セキュリティサービス事業者と共に情報窃取を企図したとみられるサイバー攻撃事案に係る情報を共有することにより、被害を防止する目的で「サイバーインテリジェンス対策のための不正通信防止協議会」を設置したことが発表された。
「サイバーインテリジェンスに係る最近の情勢(平成24年上半期)について」(https://www.npa.go.jp/keibi/biki3/20120823kouhou.pdf)。

セ **26日**：地方公共団体のホームページに殺人予告の書き込みをしたとして、男性が威力業務妨害容疑で逮捕された。その後、ウイルス感染による第三者による犯行だったことが判明し、釈放された。

脆 **27日**：Oracle社のJava7に、任意のOSコマンドが実行可能な未修正の脆弱性(CVE-2012-4681)があり、既に攻撃に悪用されていることが公表された。
FireEye Malware Intelligence Lab、"ZERO-DAY SEASON IS NOT OVER YET"(http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html)。

セ **28日**：請負業者を解雇された元従業員が、取引先の日本法人の米国子会社の重要情報を不正に入手したとして告訴された。
Sophos Naked Security Blog、"Toyota says it was hacked by ex-IT contractor, sensitive information stolen"(http://nakedsecurity.sophos.com/2012/08/29/toyota-says-it-was-hacked-by-ex-it-contractor-sensitive-information-stolen/)。

セ **30日**：独立行政法人理化学研究所は、計算科学研究機構が共催するイベントの招待を装った標的型攻撃メールが発生しているとして注意を呼び掛けた。
「計算科学研究機構の名前を騙った標的型攻撃メールについての注意」(http://www.riken.go.jp/r-world/topics/120830/index.html)。

脆 **31日**：Oracle社は、Java7で発見された未修正の脆弱性に対し、修正をリリースした。
"Oracle Security Alert for CVE-2012-4681"(http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html)。

動 **31日**：衆議院外務委員会で偽造品の取引の防止に関する協定(ACTA)が承認された。

[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

■ DNS Changerマルウェアへの対応

FBIにより運用されていた暫定DNSサーバの停止期限が7月9日となっていたDNS Changerマルウェア*11については、日本時間7月9日13時1分をもって停止されました。しかし、日本や各国で一般に向けた注意喚起の取り組みが大規模に行われた成果もあり、特に大きな混乱は確認されませんでした。

DCWG(DNS Changer Working Group)*12による感染PCのユニークIP数の集計では、最大で80万台以上(2011年11月16日)が感染していましたが、最終的には21万台と、約4分の1程度にまで減少しています。また、7月8日時点の国別IPアドレス数では、日本での感染数は5,522台でした。

DNS Changerの脅威は、その感染者数の多さだけでなく、感染端末上のDNSサーバの設定を書き換えるという手法でインターネットの利用に不可欠なDNSの仕組みを乗っ取ることにあります。このようにして感染者を悪意のあるサーバに誘導することで、広告トラフィックの奪取やスケアウェアの配布などを行い、実際に金銭被害を出しました。DNSサーバの設定を書き換える手法については他にもブラジルでホームルータに対する攻撃などが確認されています*13。このような参照先のDNSサーバを変更する手法は、利用者やISPが気づくことは困難なため、今後も同様の手法が悪用される可能性があります。

■ スマートフォンの状況とマルウェアの増加

この期間では、Samsung社のAndroid端末の一部で、リモートから工場出荷時設定へのリセットが可能な脆弱性が公表されました*14。アプリケーションでも、Android端末向けのYahoo!アプリにあった脆弱性を悪用し、アプリケーションで利用しているメールアカウントを乗っ取り、スパムメールを送信する事件が発生しています*15。iOSでは、アプリケーション内課金を迂回することができる不具合が見つかっています*16。日本のSNS事業者が提供しているHTMLベースのAndroidアプリケーション向けSDK(Software Development Kit)では、WebViewクラスに関する脆弱性が発見され、他の不正なAndroidアプリケーションを使用した場合に、該当SDKを利用したアプリケーションのデータ領域にある情報が漏えいする脆弱性が発見され、修正が行われました。

ウイルスやマルウェアなどの脅威も大きくなってきています。4月に日本の利用者をターゲットとした不審なAndroidアプリケーションが見つかり話題となりましたが、この期間でも模倣したと考えられるアプリケーションが多く見つかっています。これらの多くは、「電池が長持ちする」「インストールすることで電波状況が改善する」など、利用者の不満解消をうたっているものでした。このため、IPAからこのようなアプリケーションの解析結果を元に不正なアプリケーションの動作の一例を解説した注意喚起が行われました*17。この中では、これらのアプリケーションでは、誘導する手口として、正規のメールか確認しにくい携帯端末へのスパムメールなどを利用して、不正なサイトへ誘導したり、SNSを利用する手口が確認されているとしています。このようなスマートフォンに関する問題については「1.4.2 安全なスマートフォンの利用」も併せてご参照ください。

---

*11 DNS Changerマルウェアについては、本レポートのVol.15(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol15.pdf)の「1.4.2 DNS Changerマルウェア」も参照のこと。

*12 各国のチェックサイトは次のDCWGで確認できる。"How can you detect if your computer has been violated and infected with DNS Changer?"(http://www.dcwg.org/?page_id=381)。

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

*14 エフセキュアブログ、「Samsung TouchWizデバイスの脆弱性」(http://blog.f-secure.jp/archives/50680598.html)。

*15 Trend Micro SECURITY BLOG、「Android端末用Yahoo!のアプリに存在する脆弱性、スパムメール送信に利用される」(http://blog.trendmicro.co.jp/archives/5590)。

*16 9to5mac、"Apple's in-app purchasing process circumvented by Russian hacker"(http://9to5mac.com/2012/07/13/apples-in-app-purchasing-process-circumvented-by-russian-hacker/)。

*17 IPA、「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/2012/09outline.html)の「情報を抜き取るスマートフォンアプリに注意!」を参照のこと。

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

セ **5日**：BitCoinの交換サイトから、24,000BTC（25万ドル相当）が盗まれる。サーバに侵入し、HDD内の暗号化されていない領域に保存されていたバックアップからキーを見つけて盗んだとされている。

他 **5日**：IPAは、2012年8月のコンピュータウイルス・不正アクセスの届出状況をまとめ、国内のスマートフォンユーザを狙うアプリケーションが増加しているとして注意喚起を行った。
「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/2012/09outline.html）。

他 **6日**：衆院本会議で偽造品の取引の防止に関する協定（ACTA）が可決承認された。

他 **8日**：Google社は、セキュリティサービスを提供しているVirusTotal社を買収することを発表した。
VirusTotal、"An update from VirusTotal"（http://blog.virustotal.com/2012/09/an-update-from-virustotal.html）。

セ **11日**：ドメイン登録業者の米国Go Daddyグループで数時間のサービス停止が発生した。この事件ではAnonymousが犯行声明を出したが、Go Daddyグループでは攻撃ではなく内部ルータの障害が原因と公表している。
"Go Daddy Site Outage Investigation Completed"（http://www.godaddy.com/newscenter/release-view.aspx?news_item_id=410）。

セ **11日**：パソコンの画面に画像を表示させるウイルスを配布したとして不正指令電磁的記録供用の疑いで中学生が摘発された。同容疑の未成年への適用は初めてとなる。

脆 **13日**：BIND 9.xで外部からサービス停止可能な脆弱性（CVE-2012-4244）が見つかり、修正された。
Internet Systems Consortium、"CVE-2012-4244: A specially crafted Resource Record could cause named to terminate"
（https://kb.isc.org/article/AA-00778）。

脆 **13日**：Microsoft社は、2012年9月のセキュリティ情報を公開し、2件の重要な更新をリリースした。
「2012 年 9 月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-sep）。

セ **14日**：Microsoft社は、マイクロソフトデジタルクライムユニット（DCU）により、Nitolボットネットのテイクダウン（Operation b70）が実施されたことを公表した。
次の日本のセキュリティチームのブログに詳しい。「販売されている PC に組み込まれた Nitol ボットネットのTakedown（オペレーション b70）」
（http://blogs.technet.com/b/jpsecurity/archive/2012/10/02/3523720.aspx）。

セ **17日**：CloudFlare社は、65GbpsのDDoS攻撃とその対処についての解説を公表した。
CloudFlare blog、"How to Launch a 65Gbps DDoS, and How to Stop One"（http://blog.cloudflare.com/65gbps-ddos-no-problem）。

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

セ **19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などにあったことが報じられた。
例えば、警察庁では被害状況の概要を発表している。「尖閣諸島問題等と関連したとみられるサイバー攻撃事案について」（http://www.npa.go.jp/keibi/biki3/20120919kouhou.pdf）。

脆 **20日**：iOS6がリリースされ、任意のコード実行が可能な脆弱性を含む複数の脆弱性が修正された。
Apple社、「iOS 6 のセキュリティコンテンツについて」（http://support.apple.com/kb/HT5503?viewlocale=ja_JP）。

脆 **22日**：Microsoft社は、不正なWeb閲覧による任意のコード実行を含むInternet Explorerの複数の脆弱性に関する更新プログラムを公開した。
「マイクロソフト セキュリティ情報 MS12-063 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2744842)」
（http://technet.microsoft.com/ja-jp/security/bulletin/ms12-063）。

脆 **22日**：アルゼンチンで行われたセキュリティカンファレンスで、TLS/SSLに対する新たな攻撃手法CRIMEが発表された。

脆 **26日**：Android端末の一部バージョンで、リモートから工場出荷時設定へのリセットなどが可能な脆弱性が公表された。
詳細については例えば次のSophos Nakedsecurity Blogなどを参照のこと。"Are Android phones facing a remote-wipe hacking　pandemic?"
（http://nakedsecurity.sophos.com/2012/09/26/are-android-phones-facing-a-remote-wipe-hacking-pandemic/）。

セ **26日**：SourceForgeのミラーサイトの1つでトロイの木馬が含まれたphpMyAdmin 3.5.2.2が見つかり、修正が行われた。
"phpMyAdmin corrupted copy on Korean mirror server"（http://sourceforge.net/blog/phpmyadmin-back-door/）。

セ **26日**：IEEEで暗号化されていないユーザ情報を含むログファイルがFTPサーバで誤って公開され、10万人分のユーザ情報が漏えいした。
"IEEE Statement on Security Incident"（http://www.ieee.org/about/news/2012/25september_2_2012.html）。

他 **27日**：総務省は、ポータル事業者が発表した、利用者のメール内容を解析した結果を利用した新しい広告サービスに関し、懸念されている通信の秘密との関係について見解を示した。
「ヤフー株式会社における新広告サービスについて」（http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000122.html）。

脆 **29日**：Adobe社は、同社製品のコードサイニング証明書がマルウェアに悪用されていることが発見されたとして、証明書を無効化する措置を10月に実施すると発表した。
「重要なお知らせ　コードサイニング証明書について」（http://helpx.adobe.com/jp/x-productkb/global/certificate-updates.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

■ 政府機関の取り組み

政府機関の取り組みとしては、情報セキュリティ政策会議が行われ、標的型攻撃などのサイバー攻撃に対する対策の強化や、スマートフォンやクラウドなど新しい情報通信技術への対応などを踏まえた「情報セキュリティ2012」が決定しています。また、9月中旬からの、政府機関などに対するWebサイト改ざんやDDoS攻撃などのサイバー攻撃が多数発生していることを受け、情報セキュリティ対策推進会議幹事会が開催され[*18]、各府省庁で管理する情報システムなどの再点検や、障害や事故の発生に備えた体制の充実などの要請が行われました。

また、警察庁、総務省及び経済産業省は、インターネット利用者が参照できるサイトとして、情報セキュリティに関する情報を集約したポータルサイトを開設する[*19]など、インターネット利用者への啓発活動を行っています。更に、情報セキュリティ上の脅威に対し、国境を越えて海外諸国と協力して取り組むことの重要性から、毎年2月に開催している「情報セキュリティ月間」に加え、10月から「情報セキュリティ国際キャンペーン」として、アジア、欧米をはじめとする諸国と国際連携を活用した行事や、情報セキュリティ対策に関する情報提供を実施し、国際連携の推進と国内における情報セキュリティ対策の一層の普及を図る取り組みを行うことを決定しています[*20]。

■ 暗号の強度や証明書の利用に関する問題

この期間では暗号アルゴリズムの危殆化や証明書の利用に伴う問題がいくつか話題となりました。

7月には米国のセキュリティイベントで、企業のVPN接続で利用されているPPTP(Point-to-Point Tunneling Protocol)などの認証に使われているMS-CHAP v2の認証情報を解読するツールが公開されました。このツールは、以前から指摘されていた、MS-CHAP v2プロトコルで使われている暗号アルゴリズムの強度に起因する問題を利用しています。Microsoft社では、この問題について、PEAPを併用することやL2TPなど他のプロトコルの利用を推奨するアドバイザリを公開しました[*21]。

8月に行われた別の米国のセキュリティカンファレンスではSSL/TLSやSSHで利用されている公開鍵の多くが、意図せず他のサイトと秘密鍵を共有している問題が発表されました。この問題に関しては、「1.4.1 SSL/TLS、SSHで利用されている公開鍵の多くが他のサイトと秘密鍵を共有している問題」も併せてご参照ください。

また、Microsoft社は、8月15日に、鍵長1024ビット未満の暗号キーをブロックする更新プログラムを公開しました。これはリスクを理解して利用すべきであると認識されている、1024ビット未満のRSA鍵の問題への対策として実施されたものです。この更新プログラムはユーザによる更新作業が必要でしたが、10月10日より、自動更新に含まれるようになりました。

9月にはAdobe社のWindows版アプリケーションで利用しているコードサイニング証明書に不正利用と思われる報告があったことが公表され、7月11日以降に署名された、該当するソフトウェアに含まれる証明書を失効させる措置が10月5日に実施されました。

＊18 内閣官房情報セキュリティセンター、「情報セキュリティ対策推進会議幹事会の開催について」(http://www.nisc.go.jp/press/pdf/kanjikai_press.pdf)。
＊19 「ここからセキュリティ！」(http://www.ipa.go.jp/security/kokokara/)。
＊20 この取り組みに当たっての内閣官房長官メッセージは次のとおり。「情報セキュリティ対策の一層の普及について～情報セキュリティ国際キャンペーンの実施に当たって～」(http://www.kantei.go.jp/jp/tyokan/noda/20120928message.html)。
＊21 「マイクロソフト セキュリティ アドバイザリ (2743314)カプセル化されていない MS-CHAP v2 認証により、情報漏えいが起こる」(http://technet.microsoft.com/ja-jp/security/advisory/2743314)。

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、日常的に発生するようになっており、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、脆弱性など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、2012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[*22]、サーバに対する攻撃[*23]、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、853件のDDoS攻撃に対処しました。1日あたりの対処件数は9.27件で、平均発生件数は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0.1%、サーバに対する攻撃が86.5%、複合攻撃が13.4%でした。

この期間では、領土問題に関連した事件が複数発生しました。IIJではこれらに関連すると考えられるDDoS攻撃も検知しています。例えば8月15日から8月31日の間に検知した249件のうち89.2%が、9月10日から9月21日に検知した326件のうち、85.0%が官公庁を含む公的機関への攻撃でした。

今回の対象期間で観測された中で最も大規模な攻撃は、複合攻撃に分類したもので、最大11万ppsのパケットによって800Mbpsの通信量を発生させる攻撃でした。攻撃の継続時間は、全体の69.8%が攻撃開始から30分未満で終了し、29.3%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も0.9%ありました。なお、今回最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1日と3時間10分(27時間10分)にわたりました。

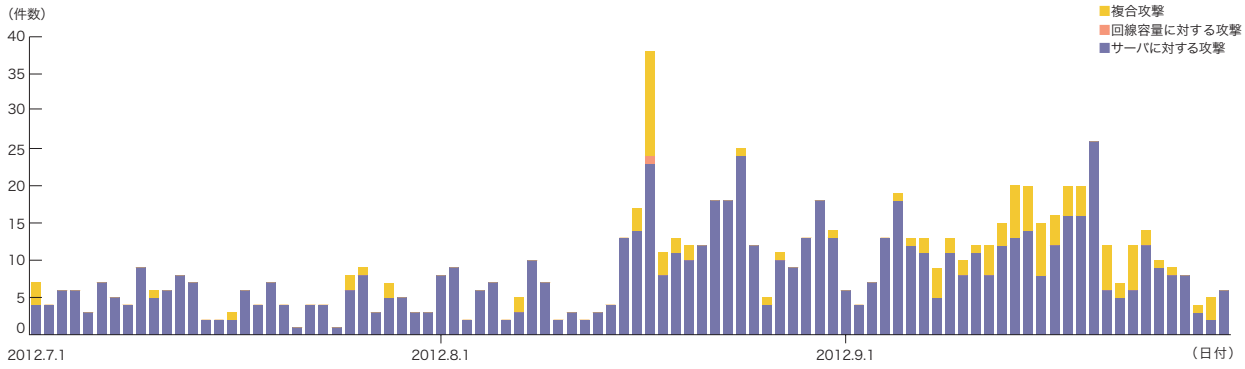


図-2 DDoS攻撃の発生件数

*22 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。

*23 TCP SYN floodやTCP connection flood、HTTP GET flood攻撃など。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など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[*24]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[*25]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[*26]によるDDoS攻撃のbackscatter観測結果を示します[*27]。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。

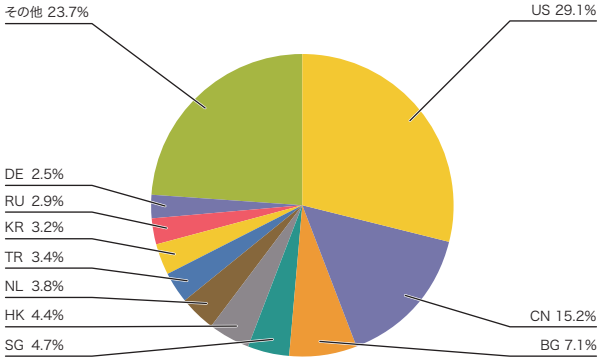


図-3 backscatter観測によるDDoS攻撃対象の分布（国別分布、全期間）

2012年7月から9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。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46.5%を占めています。また、HTTPSで利用されている443/TCPやリモートデスクトップで利用される3389/TCP、SSHで利用されている22/TCPなど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、米国29.1%、中国15.2%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、Webサーバ（80/TCP）への攻撃としては、7月26日に香港のホスティング事業者への攻撃が観測されています。この日はこれ以外にも米国と中国のIPアドレスからのbackscatterを多く観測しています。

8月14日にも香港からのbackscatterを観測していますが、こちらは香港のDDoS対策サービス事業者のものでした。9月1日や9月5日、9月7日にWebサーバ（443/TCP）への攻撃が多く発生していますが、これらの攻撃はシンガポールのホスティング事業者の複数のサーバに対する攻撃でした。9月23日には米国のDDoS対策サービス事業者の

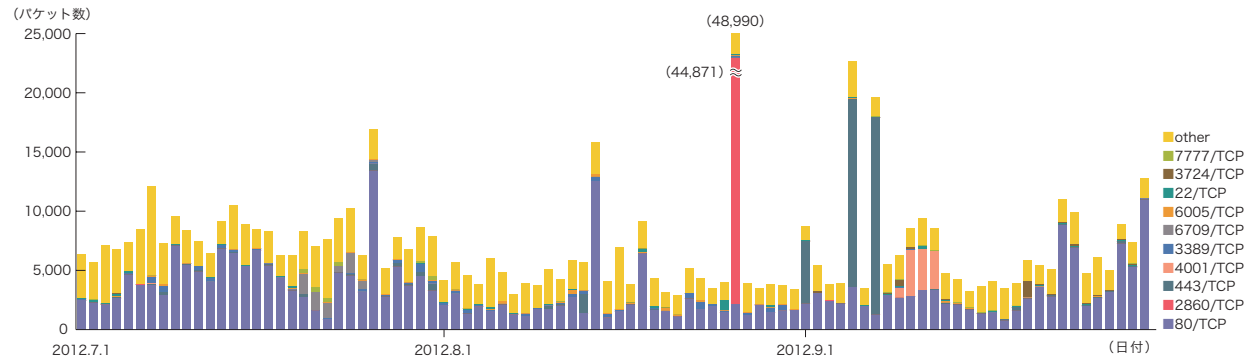


図-4 DDoS攻撃によるbackscatter観測（観測パケット数、ポート別推移）

＊24 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。

＊25 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。

＊26 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。

＊27 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。

Webサーバに対する攻撃を観測していますが、こちらは金融機関への攻撃でした。

9月30日には、複数のWebサーバからのbackscatterが観測されており、フィリピンと米国のWebサーバへの攻撃を観測しています。この2つは同じブックメーカのWebサーバでした。また同じ日に、香港のDDoS対策サービス事業者とトルコのアダルトサイトのWebサーバへの攻撃を観測しています。

8月26日には、ブルガリアのサーバに対する2860/TCPの攻撃を4万件以上観測しています。9月9日から9月12日にかけては、米国内のオンラインゲームに関連するサーバに対する4001/TCPへの攻撃を、合計で1万件以上観測しています。これらのポートは通常のアプリケーションで利用するポートではないため、それぞれの攻撃の意図は不明です。

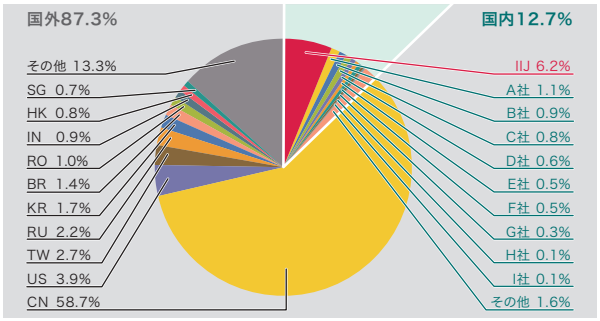


図-5 発信元の分布(国別分類、全期間)

また、今回の対象期間中に話題となったDDoS攻撃のうち、IIJのbackscatter観測で検知した攻撃としては、7月に発生したTheWikiBoatによると考えられる米国のネオナチサイトへの攻撃、9月に発生した何者かによるPastebinへの攻撃、同じく9月に発生したAnonymousによると考えられるスペインの警察への攻撃によるbackscatterをそれぞれ検知しています。

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[*28]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[*29]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

2012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台あたりの平均を取り、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。

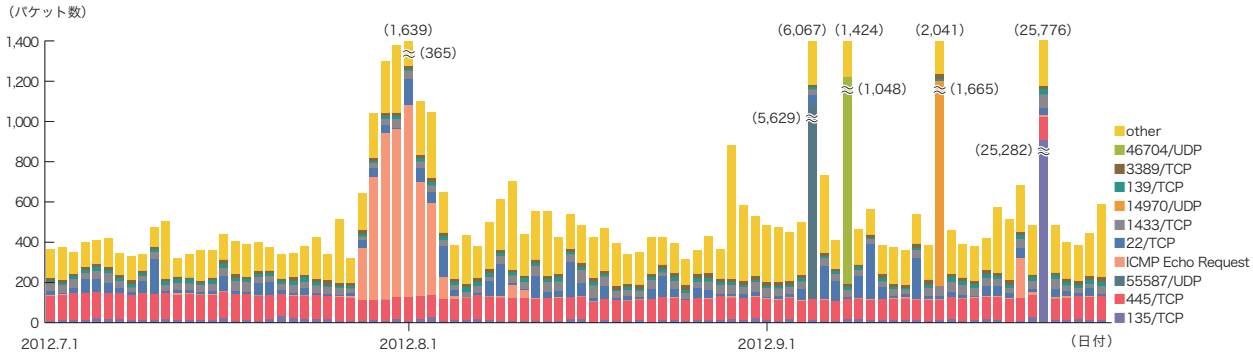


図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

*28 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。

*29 脆弱性のエミュレーションなどの手法で、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Windowsのリモートログイン機能である、RDPで利用される3389/TCP、SSHで利用される22/TCP、telnetで利用される23/TCP、ICMP Echo Requestによる探査行為も観測されています。これらに加えて、55587/UDPなど、一般的なアプリケーションでは利用されない、目的が不明な通信も観測されました。

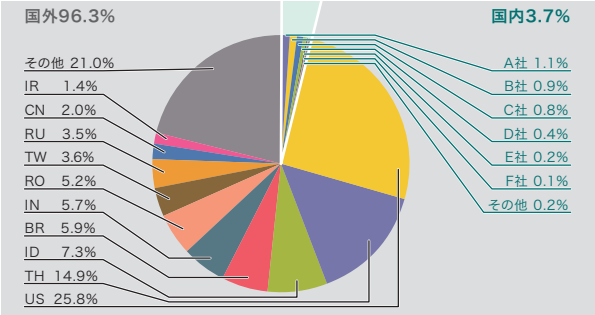


図-7 検体取得検体元の分布（国別分類、全期間、Conficker を除く）

期間中、135/TCPが9月25日に急増しました。これは中国に割り当てられた1つのIPアドレスから大量の通信が行われたものです。また、7月28日から8月4日まで、ICMP Echo Requestが一時的に増加しています。これは、IIJの1つのIPアドレスから特定のハニーポットに対して通信が行われたものです。この他に、9月5日に55587/UDP、9月8日に46704/UDP、9月16日に14970/UDPに対して、中国に割り当てられている多数の送信元から特定のハニーポットに、数時間だけ集中的に到着していますが、その目的は不明です。

■ 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

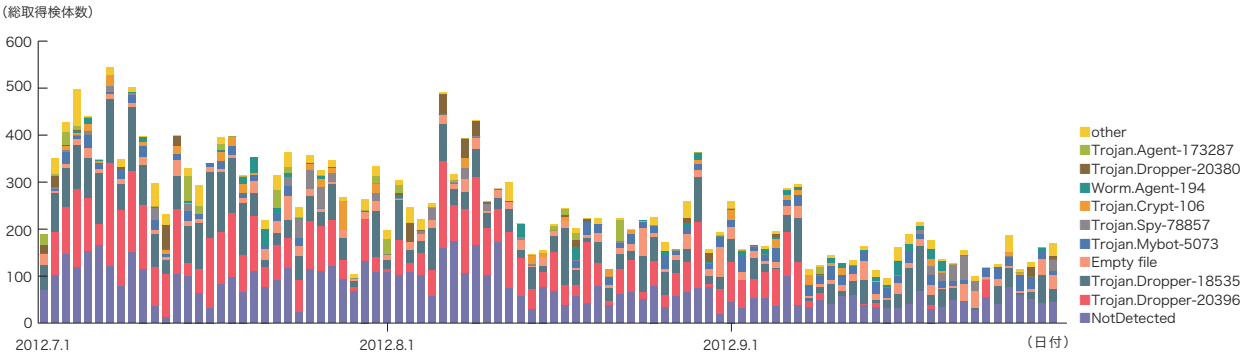


図-8 総取得検体数の推移（Conficker を除く）

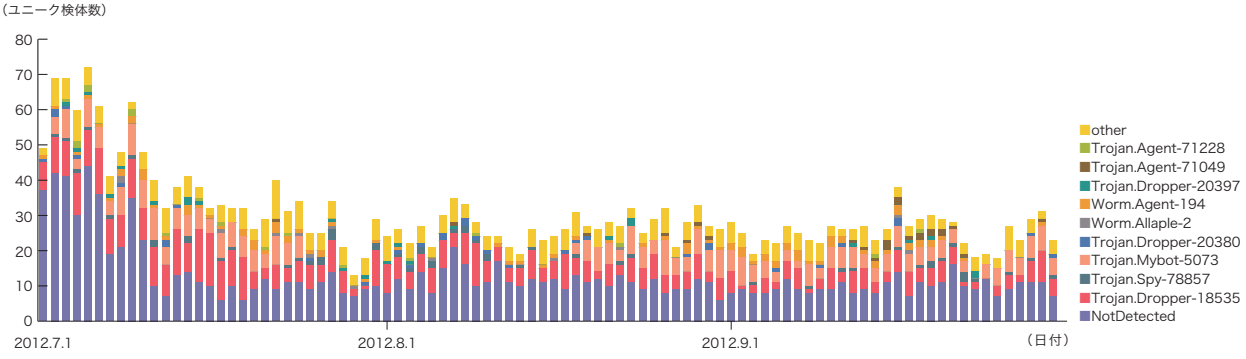


図-9 ユニーク検体数の推移（Conficker を除く）

図-8と図-9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。なお、図-8と図-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。

期間中での1日あたりの平均値は、総取得検体数が249、ユニーク検体数が31でした。今月もタイ及びインドネシアからの未検出の検体取得が特に7月中に出現しています。この未検出の検体をより詳しく調査した結果、IRCサーバで制御されるタイプのボット2種類[*32][*33]、及びトロイの木馬に分類されるマルウェア[*34]が活発に活動していたことが分かりました。

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81.4%、ボット型13.8%、ダウンローダ型4.8%でした。また解析により、18個のボットネットC&Cサーバ[*35]と10個のマルウェア配布サイトの存在を確認しました。

■ Confickerの活動

本レポート期間中、Confickerを含む1日あたりの平均値は、総取得検体数が46,415、ユニーク検体数は955でした。短期間での増減を繰り返しながらも、総取得検体数で99.5%、ユニーク検体数で96.8%を占めています。このように、今回の対象期間でも支配的な状況が変わらないことから、Confickerワームを含む図は省略しています。前回の対象期間中は総取得検体数は13%程度に一時的に減少していましたが、今回の対象期間では18%増加しています。それに対し、ユニーク検体数は前号から3%程度減少しました。

Conficker Working Groupの観測記録[*36]によると、2012年9月30日現在で、ユニークIPアドレスの総数は1,787,998とされています。2011年11月の約320万台と比較すると、約44%減少したことになりますが、依然として大規模に感染し続けていることが分かります。

＊30 ここでは、ハニーポットなど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などにより、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上で指標として採用している。
＊32 Trojan:Win32/Ircbrute（http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute）。
＊33 Win32/Hamweq（http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq）。
＊34 Backdoor.Win32.Azbreg（http://www.securelist.com/en/descriptions/33537389/Backdoor.Win32.Azbreg.ccv）。
＊35 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。
＊36 Conficker Working Groupの観測記録（http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking）。

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[*37]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。

2012年7月から9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-10に、攻撃の推移を図-11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。

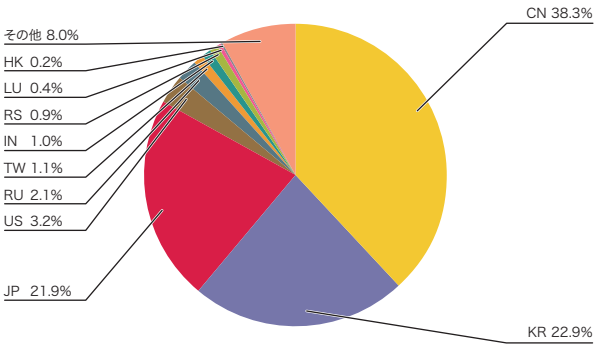


図-10 SQLインジェクション攻撃の発信元の分布

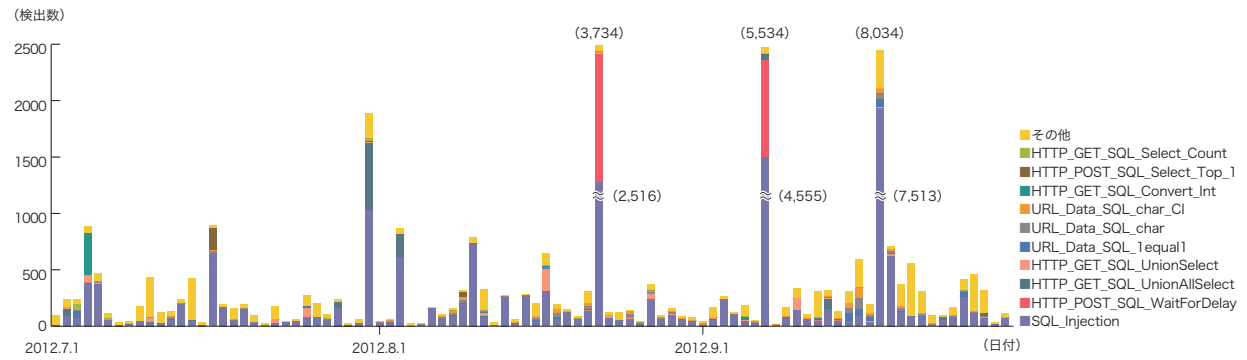


図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)

発信元の分布では、中国38.3%、韓国22.9%、日本21.9%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に比べ増加しています。韓国からの攻撃が2位と上昇していますが、これは韓国の特定の攻撃元から特定の攻撃先への攻撃が一部の日に発生したことによります。攻撃先としては官公庁、オンラインゲーム、金融機関などに対して多く発生していました。

この期間中、9月18日には韓国の特定の攻撃元から特定の攻撃先に対する攻撃が発生しています。この日は、他にも別の複数の攻撃元からそれぞれ特定の攻撃先に対する攻撃が発生していました。9月7日には中国の特定の攻撃元から特定の攻撃先への攻撃が、7月31日や8月22日にもそれぞれ別の特定の攻撃元から特定の攻撃先への攻撃が発生しました。これらの攻撃は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。

*37 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繋げています。ここでは、これまでに実施した調査のうち、SSL/TLS、SSHで利用されている公開鍵の多くが他のサイトと秘密鍵を共有している問題、スマートフォンに関するセキュリティ事情、標的型攻撃対策のための情報提供に関する議論について解説します。

1.4.1 SSL/TLS、SSHで利用されている公開鍵の多くが他のサイトと秘密鍵を共有している問題

インターネット上のIPv4アドレスを広範囲にスキャンして、SSL/TLSやSSHで利用されている公開鍵証明書、DSA署名及びPGP鍵を収集したところ、意図せず他のサイトと秘密鍵を共有していることがLenstraら[*38][*39]とHeningerら[*40]による独立した2グループから報告されました。本節ではこの問題について、現状と問題の本質、対策について取り上げます。

■ Heningerらによる指摘

ここでは、毎年実践的な研究発表が行われるUSENIX Security Symposiumにて本年公開されたHeningerらによる論文[*40]を解説します。

この論文によると、1,280万のSSL/TLSサーバのうち61%が、1,020万のSSHサーバのうち65%が、他のいずれかのホストと同じ秘密鍵(repeated keys)を利用しているとのことです。例えば、負荷分散のためDNSラウンドロビンなどの技術を用いて同じFQDNに複数のIPアドレスを割り当てているケースなど、これらのすべてに問題があるわけではなく、意図的に複数IPアドレスで同じ鍵を利用しているケースもあります。その中でも機器の出荷時のデフォルト鍵をSSL/TLSにおいて利用していると思われるケースが、少なくとも5.23%(670,391ホスト)も見つかっています。出荷時のデフォルト鍵を利用しているデバイスのほとんどがネットワーク機器や組み込み機器で、著者らは現在60のベンダーに連絡を取っているとのことです。そのうち20から何らかの回答がありましたが、アドバイザリを出したのは3ベンダーのみという状況です[*41]。また、この研究とは別に、ネットワーク製品においてデフォルト鍵を利用する脆弱性に関するアドバイザリが公開されたこともあります[*42]。

この論文では、インターネット上のIPv4のIPアドレス空間で443/TCP(SSL/TLS)と22/TCP(SSH)を広範囲にスキャンして、SSL/TLS、SSHで利用されている公開鍵証明書及びDSA署名を収集したところ、SSL/TLSでは5.57%(714,243IPアドレス)、SSHでは9.60%(981,166IPアドレス)が、意図せず他のサイトと同じ公開鍵・秘密鍵を利用していたという結果を報告しています。異なるIPアドレスで同じ公開鍵・秘密鍵を利用しているケースのすべてが問題であるということではありませんが、第三者と同じ秘密鍵を意図せず使用している事例もあることが警告されています。この状況を鑑み、著者らはオンライン鍵チェックサービスの提供を開始しました[*43]。

これらの機器以外にも、Apache WebサーバやCitrixリモートアクセスサーバでもデフォルト鍵を利用している事例が報告されています。そのうち38の証明書がWebブラウザで信頼されている認証機関から発行されています。その中にはFortune 500にリストされている企業、保険会社、法律事務所、公共交通機関、米軍などが含まれており、著者らはできるだけこれらの組織に連絡を取るようにしているとのことです。

---

*38 Arjen K. Lenstra、James P. Hughes、Maxime Augier、Joppe W. Bos、Thorsten Kleinjung、Christophe Wachter、"Ron was wrong, Whit is right"(http://eprint.iacr.org/2012/064)。

*39 Arjen K. Lenstra、James P. Hughes、Maxime Augier、Joppe W. Bos、Thorsten Kleinjung、Christophe Wachter、"Public Keys"(http://www.iacr.org/conferences/crypto2012/abstracts/session11-2.html)。

*40 Nadia Heninger、Zakir Durumeric、Eric Wustrow、J. Alex Halderman、"Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices"(https://www.usenix.org/conference/usenixsecurity12/mining-your-ps-and-qs-detection-widespread-weak-keys-embedded-devices)。

*41 この問題について、各ベンダーが出したアドバイザリがまとめられている。"Security Advisories"(https://factorable.net/advisories.htm)。

*42 "F5 BIG-IP remote root authentication bypass Vulnerability"(https://www.trustmatta.com/advisories/MATTA-2012-002.txt)。

*43 次のサイトでは実際に利用している公開鍵が脆弱かどうか確認できる。もし脆弱鍵を利用していることが判明した場合には、鍵の更新が推奨される。"Widespread Weak Keys in Network Devices"(https://factorable.net/)。

本論文では、このような状況が発生した原因の1つとして「世の中に広く出回っている擬似乱数生成モジュールに問題がある」という点を指摘しています。鍵生成や署名生成時に利用する擬似乱数生成モジュールのエントロピーが不足しているために、十分な鍵空間から鍵が生成されていないため、同じ秘密鍵を共有してしまっているという主張です。

この擬似乱数生成モジュールのエントロピーが不足することに起因する問題は、例えばDebianのOpenSSLにおける脆弱性[*44]として既に知られています。Debianの特定バージョンにおけるOpenSSLを使って鍵生成を行った場合、極端に少ない鍵空間からしか秘密鍵を導出していないという問題がありました。2008年にアドバイザリが発行されていたにも関わらず、現在でもその脆弱な鍵を利用しているサイトがSSL/TLSでは0.03%(4,147ホスト)、SSHでは0.52%(53,141ホスト)存在していることが報告されています。更に著者らは各エンティティに応じていくつかの対策について推奨しています。

- **デバイス製造社向け**
  - ビルトインされたデフォルト鍵や証明書をユーザが利用できる状態にしない。
  - 十分なエントロピーを確保するためにハードウエアによる擬似乱数生成器を利用する。
- **エンドユーザ向け**
  - デバイスが出荷されたときに格納されているデフォルト鍵や最初にブートされた際に生成される鍵を利用せず、十分なエントロピーを確保できる他の環境下で生成した鍵を利用する。
  - 自ら生成した鍵が脆弱かどうか、つまり既に他のユーザに利用されている鍵かどうかをチェックする。
- **公開鍵証明書発行機関**
  - カスタマーが提示した公開鍵が脆弱かどうかチェックし、脆弱な場合には証明書を発行しない。

■ Lenstraらによる指摘

ここでは、CRYPTO2012で公開されたLenstraらによる論文による指摘内容を紹介します。彼らはまずThe EFF SSL Observatory[*45]など、公開されている複数の公開鍵証明書データベースから、6,185,372の相異なるX.509証明書と、5,481,332のPGP公開鍵を収集しました。以下、この論文で指摘された結果から、RSAアルゴリズムに関する結果を列挙していきます。

6,185,228のRSA公開鍵を含むX.509証明書のうち、266,729(4.3%)の証明書において他の証明書と同じRSA公開鍵を包含していることが指摘されました。同じ組織体により再利用されている、つまり旧証明書と新証明書で同じ鍵ペアを利用しているケースもあると考えられるため、これらの証明書のすべてが問題であるということではありません。同じ公開鍵を持つ証明書をクラスタリングすると5,989,523に分けることができます。同じクラスタに入っている証明書はそれぞれ同じ公開鍵を持つということを意味します。あるクラスタに含まれる証明書の個数が1である、つまり他の証明書と同じ鍵を共有していないクラスタは5,918,499(98.8%)です。最も証明書数の多いクラスタには16,489の証明書が含まれており、1,000以上の証明書を含むクラスタは14あるとのことです。

次にクラスタリングされた証明書の公開鍵について考察しています。X.509証明書から得られた5,989,523の異なるRSA公開鍵と、同様にしてPGP公開鍵から得られたRSA公開鍵から合計で6,386,984の異なるRSA公開鍵を得たのち、同じ秘密鍵を共有してしまっているケースを調べたところ12,934の公開鍵で秘密鍵を共有していることが明らかになりました。そのうち36の公開鍵は異なる9の秘密鍵の組み合わせで構成されていました。これはHeningerらも同じ状況が観測されており、特定の製品で鍵生成を行った場合の問題があることが指摘されています。

*44 Debian Security Advisory、"DSA-1571-1 openssl -- predictable random number generator" (http://www.debian.org/security/2008/dsa-1571)。
*45 Electronic Frontier Foundation、"The EFF SSL Observatory"(https://www.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。

■ 同じ秘密鍵であることが外部から同定される仕組み

収集された公開鍵からどのようにして同じ秘密鍵を利用していることが第三者に同定されてしまうのか疑問を持つ方もいらっしゃると思いますが、以下の興味深い性質に起因します。RSAアルゴリズム[*46]の安全性の根拠となっている「大きな因数の素因数分解は難しい」一方で「異なる2つの因数のGCD（最大公約数）を見つけるのは簡単である」という性質があります。後者のGCDの算出は紀元前から知られる「ユークリッドの互除法」を用いています。通常RSAではN=pq（素数の積）のモジュラ演算を用いますので、「Nからpまたはqを見つけるのは難しい」けれど「$N_1=p_1q$と$N_2=p_2q$からqを求めるのは簡単」ということになります。そのため、図-12のようにN_1（とe_1）を公開鍵としているエンティティEntity1とN_2（とe_2）を公開鍵としているエンティティEntity2の間では、共通する素数qそしてp_1とp_2もお互い分かってしまう（秘密鍵が漏れてしまう）ことになります。更に、Entity1、Entity2以外の第三者も同じqをシェアしてしまっていることが分かってしまうので、やはりp_1、p_2、qすべてが第三者に同定されてしまいます。

上記例のように、ランダムに選択したつもりの素数qが偶然重なる可能性はRSAアルゴリズムの根本的な問題であることが分かります。しかし、2048ビットRSAで用いられる1024ビット素数の候補は素数定理[*47]から約$2^{1014.53}$個もありますから、容易に重複するものではないことが分かります。しかし、素数生成時のアルゴリズムに偏りがある、つまり$2^{1014.53}$個の全空間から素数を抽出していない場合に問題が起きているということになります。このため、素数生成時に用いられる擬似乱数生成モジュールがその性能を大きく左右することになります。

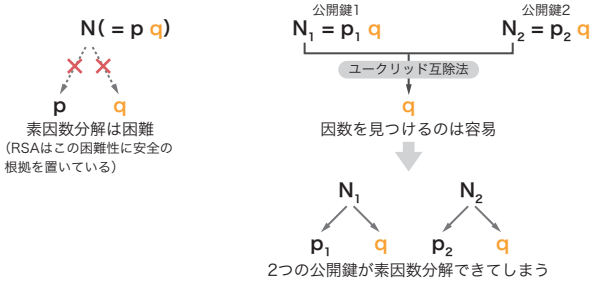


図-12 2つの異なる公開鍵が同じ秘密鍵を持つことが外部から同定される仕組み

■ 秘密鍵を共有していることによる影響

今回の論文で指摘されたような機器のデフォルト鍵を利用している場合、他の同機種を持つユーザも同じ秘密鍵を持つ可能性が高くなります。また、意図せず第三者と秘密鍵を共有してしまった場合には、同じ秘密鍵を持つ者に悪用され、表-2のような問題が発生する可能性があります。

同じ秘密鍵を持つ第三者がいる可能性のある鍵を利用している場合には、現在利用中の鍵を別の鍵に更新して利用することをお勧めします。著者らが提供しているオンライン鍵チェックサービスは、公開鍵が脆弱かどうかチェックできます[*41]。このように、脆弱な公開鍵は外部から判定することができる問題があり、攻撃者も同様な情報を入手することができるということに注意して、影響を受ける可能性がある場合には早急な対策が必要です。

表-2 公開鍵暗号系を利用したアプリケーションにおける秘密鍵が漏えいした場合の影響

影響の分類	詳細
1. 暗号化された通信の暴露	SSL/TLSやSSHサーバとクライアントの通信を傍受できる環境において、暗号化を行っているにも関わらず通信内容を把握できる
2. サーバのなりすまし	DNS詐称やネットワークの乗っ取りが可能な環境において、SSL/TLSやSSHサーバになりすますことができる
3. 不正ログインもしくはクライアントのなりすまし	SSL/TLSでのクライアント認証のように、公開鍵証明書を用いたログインが可能になる
4. 不正プログラムへのコード署名	コードサイニング用の公開鍵証明書の秘密鍵が漏えいすることで、当該証明書によって保証されたプログラムであるかのように見せられる

＊46 例えば2048ビットRSAの場合、1024ビット長の素数p、qを任意に選びN=pq（2048ビット長）とe（通常65537）を公開鍵として公開する。秘密鍵としてed=1 mod(p-1)(q-1)となるdを計算する。このときpまたはqを知っていれば（Nを素因数分解できれば）dは計算可能でありNしか知らない場合はdを得ることは困難である。

＊47 素数定理は自然数の中に素数がどのくらいの割合で含まれているかを近似した値を示しており、n以下の素数の個数Π(n)～n/(ln n + B)ただしB=-1.08366である。RSA2048で利用される1024ビットの素数の個数をΠ(2^{1025}-1)-Π(2^{1024}-1)として計算すると約$2^{1014.53}$が得られる（http://mathworld.wolfram.com/PrimeNumberTheorem.html）。

1.4.2 安全なスマートフォンの利用

スマートフォンの普及に伴い、携帯電話は単なる通話手段としてだけではなく、ソーシャルネットワークを通じて友人と連絡を取り合ったり、ゲームや音楽をダウンロードしたりして楽しむといった、様々な用途で利用されるようになりました。また、スマートフォンはネットワークサービス端末としてPCに近い機能を持っています。そのため、従来の携帯電話にはなかった脆弱性やセキュリティ上の問題が発生しています。ここでは、スマートフォンの事件や問題が発生する理由、更に、安全にスマートフォンを利用するためにはどうすべきかを考察します。

■ スマートフォン関連の事件

既に、スマートフォンを使った多くのセキュリティ事件が発生しています。それらの特徴を分類すると、ウイルス、不正に情報取得を行うアプリケーション、正当なアプリケーションによる情報取得、スマートフォンと連携するサービスからの情報漏えいに分けられます。以下に、それぞれの代表的な事例の概略を紹介します。

■ ウイルス

2010年8月にAndroid端末で初めてのウイルスが確認されました[*48]。Movie Playerというアプリケーションに見せかけていましたが、実際はロシアのショートメッセージサービスに接続し、勝手にメッセージ送信を行うものでした。スマートフォン向けウイルスの多くはAndroid端末上で動作するものですが、iPhoneで動作するIkeeといったウイルスも確認されています[*49]。このように、端末の種別を問わず、ウイルスの脅威は存在しています。

■ 不正に情報取得を行うアプリケーション

2012年4月に端末の電話番号や電話帳を特定のサーバに送信するThe Movieと名づけられたアプリケーションが日本で流行しました[*50]。同様のアプリケーションとしては、2012年9月に、「電波改善」「電池長持ち」と称するアプリケーションに関しての注意喚起が、IPAより行われました[*51]。これらは偽アプリケーションで、実際の動作とは関係のない情報を外部へ送信します。インストール時にユーザが許可したパーミッションを利用して情報を送信するため、脆弱性の有無は関係なく情報漏えいが発生します。

■ 正当なアプリケーションによる情報取得

2011年8月には「カレログ」が大きな話題となりました[*52]。本アプリケーションがインストールされたスマートフォンは、位置情報や通話記録を別のパソコンから確認できるため、プライバシー情報漏えいが懸念されました。

■ クラウドサービスでの情報漏えい

2011年9月にアメリカの女優であるScarlett Johanssonは、利用していたメールサービスの認証情報を窃取され、iPhoneで撮影してアップロードした自身のヌード写真が漏えいしていることを明らかにしました。この事件ではその後、FBIにより犯人が逮捕されていますが、この犯人は他にも50人以上の著名人のアカウントに不正にアクセスしていました[*53]。

■ スマートフォンで事件が増えている理由

なぜスマートフォン関連の事件が増えているのでしょうか。それは、スマートフォンが携帯電話やPCとは異なる特徴を持っていることに起因していると考えられます。ここではスマートフォンの特徴に着目して考察を行います。

■ スマートフォンの機能的特徴

スマートフォンは通話のための電話であると同時に、GPSやカメラを持ち、アプリケーションが自由にインストール可能な高性能端末です。携帯電話ともPCとも異なるスマートフォンの特徴が、従来とは異なる新たな問題を発生させています。

---

*48 詳細については次のKaspersky Lab SECURELIST BLOGに詳しい。「First SMS Trojan for Android」(http://www.securelist.com/en/blog/2254/First_SMS_Trojan_for_Android)。

*49 エフセキュアブログ、「First iPhone Worm Found」に詳しい。(http://www.f-secure.com/weblog/archives/00001814.html)。

*50 IPAから注意喚起が行われている。「コンピュータウイルス・不正アクセスの届出状況[4月分]について」(http://www.ipa.go.jp/security/txt/2012/05outline.html)。

*51 IPAから注意喚起が行われている。「コンピュータウイルス・不正アクセスの届出状況[8月分]について」(http://www.ipa.go.jp/security/txt/2012/09outline.html)。

*52 現在カレログのサービス提供は終了している。「カレログ」(http://karelog.jp/)。

*53 FBIのプレスリリース「Florida Man Arrested in "Operation Hackerazzi" for Targeting Celebrities with Computer Intrusion, Wiretapping, and Identity Theft」(http://www.fbi.gov/losangeles/press-releases/2011/florida-man-arrested-in-operation-hackerazzi-for-targeting-celebrities-with-computer-intrusion-wiretapping-and-identity-theft)。

- **スマートフォンの持つ情報の多様性**
  電話の機能として従来備えられている電話帳や通信記録といった情報はもちろん、アプリケーションで扱われる写真、位置情報、動画、文書といった様々な情報がスマートフォンを使ってアップロードまたはダウンロードされています。スマートフォンはパーソナルデバイスであり、個人に関する多くの情報が保存されやすくなっています。
- **PCと異なる要素**
  利用者の立場からは、スマートフォンの機能はPCに近いものと考えることができますが、セキュリティの観点からみると、セキュリティ確保の技術、ソフトウェア(アプリケーション)の配布方法、OSやアプリケーションのバージョンアップ、デバイスそのものの利用のされ方、通信手段など、多くの違いがあります。

スマートフォンのサービス構造

スマートフォンの機能だけではなく、ビジネス提供形態の変化も従来にない問題を引き起こす1つの理由と考えられます。従来の携帯電話では、通信サービス、端末の開発や提供、アプリケーションの提供などが垂直統合型のビジネスとして行われ、携帯キャリアが総合的にサービスを提供していました。しかし、スマートフォンはこれとは異なり、各サービスを別の事業者が提供し、それらが積み重なることによって最終的なサービスが提供されるという、水平分業型のビジネスとなっています。オープンなプラットフォームが提供される反面、サービスの責任分界が細かく分かれてしまい、全体の整合性が取りやすい垂直統合型と比べて、総合的なプラットフォームとしての安全性を確保することが難しくなっています[*54]。

セキュリティモデルの課題

スマートフォンが備える基本的なセキュリティモデルに、パーミッションとサンドボックス化があります。これらはアプリケーションに対して、不要な機能を利用させない仕組みです。

Androidでは、インストール時にアプリケーションから要求されるパーミッションを利用者が意識的に許可することで、不要な機能の利用を防ぐことができます。インターネットの利用や電話帳の参照といった単位でアプリケーションが利用する機能が定義されており、許可を行わなければアプリケーションはインストールされません。ただし、この機能については次のような問題があります。

- 一度許可すると、アンインストールしない限りパーミッションは変更されない
- 要求されたパーミッションをすべて許可しないと、アプリケーションは利用できない
- パーミッションの分類がOSの機能や処理方法に合わせてあるため、利用者にとって直感的ではない(アプリケーション利用中に着信するために、電話機能にアクセスを許可しなければならない、など)

また、スマートフォンには、OSから隔離された領域でアプリケーションを実行する、サンドボックスというセキュリティ機能が搭載されています。しかし、一般の利用者がサンドボックスの制限を超えて、OSの機能に直接アクセス可能となるアプリケーションが非公式に提供されており、これらを利用することでサンドボックスによる保護機能をバイパスすることが可能となっています。更に、スマートフォンのセキュリティソフトウェアはPCと違い、特権を与えられておらず、サンドボックス上で一般のアプリケーションと同等に動作しています。よって、マルウェアが脆弱性などを突いて特権を取得した場合、検知、防御することが難しい場合があります[*55]。そのため、独自のセキュリティ機能を実装したスマートフォンの開発なども行われています[*56]。

スマートフォンアプリケーション

一般的にスマートフォンアプリケーションは、Google社やApple社、携帯キャリアの運用する公式マーケットなどから入手しますが、非公式なマーケットも多数存在しており、自由にアプリケーションのインストールが可能です。公式

*54 総務省によるスマートフォン・クラウドセキュリティ研究会の最終報告(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html)及びスマートフォン プライバシー イニシアティブの提言(http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html)で言及されている。

*55 詳細な情報が株式会社フォーティーンフォティ技術研究所により公開されている。「Android:設計上の技術的な問題点」(http://www.fourteenforty.jp/research/research_papers.htm)。

*56 パナソニック株式会社「業界初 個人データを保護するスマートフォン向け技術を開発」(http://panasonic.co.jp/corp/news/official.data/data.dir/jn120227-2/jn120227-2.html)。

マーケットはそれぞれのマーケットの方法でアプリケーションの安全性をチェックしていますが[*57]、非公式なマーケットではアプリケーションの安全性の確認が行われていない、もしくは不十分である可能性があります。なお、過去には公式マーケットでも不正なアプリケーションが配布されていたこともあることから、公式マーケットであっても100%安全であるという保証はありません。

事件の事例でも述べたように、公式マーケットで配布されている正当なアプリケーションでも利用者情報の取り扱いに問題が見つかる場合がありますが、現時点ではそのような情報の取り扱いに関する規制は存在しません。総務省による、「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会(平成21年度)[*58]」などでも、利用者の通信に関わる情報や、位置情報などは通信事業者が保有する情報であるとして扱いが検討されています。

また、従来は利用者に関する情報が携帯キャリアに閉じていたことに対して、スマートフォンでは通信インフラ事業者以外に、Google社やApple社といったプラットフォーム事業者や、アプリケーション開発者などによっても利用者情報が取り扱われる可能性があります。これについて総務省では「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」、「スマートフォンを経由した利用者情報の取扱いに関するWG(平成23年度～24年度継続中)[*59]」で検討が行われています。

■ 無線LAN

スマートフォンは、携帯電話規格の通信方式以外に無線LANがサポートされているのも特徴の1つです。スマートフォンは従来の携帯電話に比べ送受信するデータ量が多く、携帯キャリアも通信帯域確保のために無線LANの利用を積極的に推進しています。建屋内といった、携帯電話の電波が届きにくい場所でインターネット接続を行う場合などには非常に便利ですが、誤って不正なアクセスポイントへ接続した場合、通信を傍受されるなどの問題が発生します。

■ OSアップデートやバックアップなどのネットワークサービス

スマートフォンはPCと同様にOSのアップデートが行われます。しかし、脆弱性への対応速度が、現時点ではPCに比べて遅れる傾向にあります。また、基本的にOSやアプリケーションのアップデートや脆弱性対応、バックアップデータの暗号化などはそれぞれ利用者やアプリケーション開発者に任されているため、利用者はそれらのセキュリティ情報に気を遣う必要があります。

また、可用性の観点からバックアップの作成は積極的に行うべきですが、その場合、電話帳やメールなどの個人情報だけでなく、アプリケーションとそのデータといった、スマートフォンの様々なデータが含まれます。このようなバックアップデータが漏えいすると、端末そのものを盗まれた場合と同程度の被害を受けることになります。

■ 利用シーン

スマートフォンは多機能、高性能、高精細画面であり、音声通話以外の利用価値が高く、可搬性に優れることから、場所を問わずに利用されることが多くなっています。そのため、覗き見や盗難におけるリスクは通常の携帯電話よりも高いと考えられます。スマートフォン端末が組織で管理可能であればMDM(Mobile Device Management)を利用することでリスクを減らすことはできますが、利用者個人が注意を払う必要があることは言うまでもありません。

■ スマートフォンを安全に利用するために

現在のところスマートフォンを安全に利用するためには、利用者個人、サービス提供事業者、それぞれの努力が必要です。総務省では利用者視点と事業者視点の両面で検討を行っています。ここではその取り組みを紹介すると共に、利用者がどのようなことに注意をすべきか、事業者は今後どのような対応を行う方向にあるのかといったことをまとめます。

総務省の「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」が取りまとめた提言「スマートフォン プラ

*57 例えばApple社は開発者向けにアプリケーション審査についての情報を公開している。「アプリケーション審査ガイドライン」(https://developer.apple.com/jp/appstore/guidelines.html)。Google社はBouncerという仕組みを用いてアプリケーションの安全性を自動チェックしている。「Android and Security」(http://googlemobile.blogspot.jp/2012/02/android-and-security.html)。キャリア独自の対策としてKDDI株式会社はau one Marketで独自のセキュリティチェックを行っている。「〈お知らせ〉「au one Market」の機能拡張について〈別紙〉」(http://www.kddi.com/corporate/news_release/2010/0831b/besshi.html)。

*58 総務省、「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」(http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html)。

*59 総務省、「スマートフォンを経由した利用者情報の取扱いに関するWG」(http://www.soumu.go.jp/menu_sosiki/kenkyu/riyousya_ict/02kiban08_03000087.html)。

イバシー イニシアティブ」では、利用者が安全安心にサービスを活用できるように、スマートフォン・プライバシーに関する包括的な対策が提案されました。

1. アプリケーション提供者や情報収集モジュール提供者を中心に、アプリケーション提供サイト運営事業者・OS提供事業者、移動体通信事業者などのスマートフォンの関係事業者に広く適用可能な「スマートフォン利用者情報取扱指針」を示す
2. 第三者によるアプリケーション検証の仕組みなど、指針の実効性を上げるための方策を提案
3. 利用者リテラシー向上のための情報提供・周知啓発方策
4. 国際連携の推進

また、スマートフォン・クラウドセキュリティ研究会では、「スマートフォン情報セキュリティ3ヵ条」として、利用者視点で以下の項目を挙げました。

1. OS（基本ソフト）を更新
2. ウイルス対策ソフトの利用を確認
3. アプリケーションの入手に注意

今までに考察したスマートフォンの特徴を元に、PCとスマートフォンの違い、利用時に気をつけるべきこと、改善の方向性を表-3にまとめます。スマートフォンは一見従来の携帯電話よりも便利になった携帯電話に見えますが、実際にはPCと同様のソフトウェア提供形態や動作の仕組みを持っており、様々なセキュリティ上の考慮が必要となっています。個人情報などの重要な情報が保存、送受信されることが多いスマートフォンですが、PCと同等、もしくはそれ以上の安全性を備えているとは現時点では言い難い状況です。利用者自身で情報の重要性を判断し、スマートフォンや関連サービスにその情報を置くべきかどうか、本当にそのアプリケーションを使う必要があるかなどの判断を行うことも重要と言えるでしょう。

表-3 スマートフォン利用時の注意点と改善の方向

	PC	スマートフォン	利用者が注意する点	改善の方向性
OS	• 脆弱性の緊急対応についてはタイムリーなアップデートがある • アップデートでOSに問題が出ることは比較的少ない • 月次で自動的にアップデート	• 脆弱性への対応がPCに比べて遅い • アップデートされたOSの品質に問題 • アップデートは利用者による操作が必要 • JailBreak、Root化の問題がある	• OSの更新を行う • セキュリティについて考慮された端末を利用する	プラットフォーム事業者によりOS仕様が厳密に管理されている場合はプラットフォーム事業者の努力による。オープンなOSでは端末メーカによって独自の対策が行われていることもある
アプリケーション	• アンチウイルスソフトが高い権限で動作している • 主要なアプリケーションは自動アップデートされる • アプリケーションの安全性の評価が比較的容易	• アンチウイルスソフトが一般ユーザ権限で動作している • アップデートはアプリケーション開発者や利用者に任せられている • 非公式マーケット、非公式アプリケーションが存在し、安全性の検証が困難	• ウイルス対策ソフトの利用を確認する • アプリケーションの入手に注意する • アプリケーションがアクセスするデータを確認する • 利用しているアプリケーションの評判を確認する • 不必要な情報の取得があれば、利用を止める • 利用するネットワークサービスの評判を確認する	公式マーケットによるチェックの強化や、キャリアなどによる独自の安全性検証が徐々に強化されつつある
利用者情報	• 利用者情報とアプリケーションの関連性が低い • 利用者自身による保護対策の選択が可能である	• アプリケーションと利用者情報が密接に結合している • アプリケーション利用権限の粒度が荒く、一度許可した権限は以後変更されない	• GPSなどの個人データが付与される機能は、不必要であればオフにする • 利用するネットワークサービスの認証情報を適切に扱う • 作成したバックアップやネットワークサービスにアップロードされたデータは暗号化する	監督官庁の研究会や業界団体などでよりよい利用者情報の扱い方について検討が行われている
無線LAN	• 意識的に接続が必要	• キャリアの提供する機能により、意図していないアクセスポイントに自動接続される場合がある • アクセス先が分からない/分かりづらい	• 無線LAN利用時のアクセスポイントに注意する • 無線LAN利用時には暗号化通信を行う	総務省のスマートフォン・クラウド研究会での問題提起があり、今後の検討課題となっている
端末管理と利用の状況	• 基本的には利用場所、利用シーンが限定される。物理的な固定を前提としてセキュリティワイヤー利用などが可能	• 利用場所や利用シーンが多岐にわたり、可搬性が非常に高い • 携帯電話と同様の感覚で利用されている	• 利用時の周りの状況に注意する。適時、仕事をしてよい状況かどうか判断する • 覗き込まれるような公共の場所では利用しない • 紛失、盗難対策を行う。特に喫茶店などで机の上に置かない	会社利用を前提として、MDMなどの利用で被害状況の軽減が可能である。また、従来どおり、プライバシフィルタなどの対策も有効である

スマートフォンは登場してからの歴史がまだ浅く、発展途上のプラットフォームです。今後提供者の努力や技術の進歩などにより、安全性が高まるものと期待されますが、技術的な対応策が充実したとしても、利用者による情報管理の必要性や、実際の利用シーンにおいて発生する問題などがなくなるわけではありません。利用者が適切な端末管理と安全な利用を心がけることは継続して必要となります。スマートフォンを安全に利用するためには利用者、事業者、双方の継続的な努力が必要です。

1.4.3 標的型攻撃対策のための情報共有

昨年8月の国内大手企業に対する標的型攻撃の発生以来、その対策のために複数の試みが実施され、様々な対策手法の検討や対策の実施が行われています。ここではこれらの試みの中における標的型攻撃のための情報共有の難しさについて紹介し、その対応を検討します。

■ 標的型攻撃対策のための枠組み

昨年、次々と明らかになった標的型攻撃[*60]に対応するために、様々な観点からこの問題に対策するための活動が行われています。例えば、内閣官房情報セキュリティセンターの情報セキュリティ政策会議[*61]でもこの問題が取り扱われていますし、他にも、各省庁主導の複数の活動[*62]や、民間のセキュリティ関連企業で構成される「日本セキュリティオペレーション事業者協議会(ISOG-J)WG5[*63]」などが、その例として挙げられます。

また、それぞれの活動が開始されてから1年以上が経過した現在、これらの活動との間にも、連携を密にする動き[*64]が生まれてきています。

IIJとしても、重要インフラの1つである通信をつかさどる企業として、標的型攻撃の対象となりうるという考えと、セキュリティ関連サービスを通じて顧客を標的型攻撃から保護するという観点から、これらの活動のほぼすべてに、直接的もしくは間接的に参加しています。

これらの活動はいずれも、標的型攻撃の検出を報告し、その情報を広く伝えることで、対策に役立てることが主眼となっています。

実際、国家や特定の産業に対する攻撃という規模で考えると、情報を集約して全体像を把握することに大きな意味があります。また、いくつかの事例に関する研究の結果、攻撃手法が再利用されている場合が少なからずあるということが判明しています。これらのことから、標的型攻撃対策において、情報の共有は必要であると言えます。

■ 標的型攻撃にかかわる情報提供の難しさ

情報共有を行うためには、その情報が提供されなければ、始められないのですが、標的型攻撃には、一般のサイバー攻撃とは異なった情報提供の阻害要因があります。

例えば、標的型攻撃に悪用されたメールの内容には、標的型攻撃を受けた人の属性(経営者や研究者など)や、その企業の事業内容(防衛産業、重要インフラ)に関する秘密が含まれることがあります。また、成功した攻撃に利用されたマルウェアや脆弱性などの情報が、その企業のITシステムの弱点とも考えられる情報を示すことがあります。このような情報を提供し、多くの組織や人の間で共有することは、情報提供者にとって非常に大きなリスクを伴うものであり、攻撃の防御に成功した場合を除いてあまり情報提供をしようとする気になるものではありません。

また、通信事業者やセキュリティサービス事業者、システムインテグレータにおいては、例えば電気通信事業法など

---

*60 標的型攻撃の説明と、具体的な事件については、IIR Vol.14「標的型攻撃とその対応」(http://www.iij.ad.jp/company/development/report/iir/014.html)をご参照ください。

*61 その検討結果は、例えば、情報セキュリティ政策会議による「情報セキュリティ 2012」(http://www.nisc.go.jp/active/kihon/pdf/is2012.pdf)に「標的型攻撃に対する官民連携の強化等」として公開されている。

*62 サイバーインテリジェンス情報共有ネットワーク(http://www.npa.go.jp/keibi/biki3/230804shiryou.pdf)、サイバー情報共有イニシアティブ(J-CSIP(ジェイシップ))(http://www.ipa.go.jp/security/J-CSIP/index.html)、テレコムアイザック官民協議会、内閣官房情報セキュリティセンター(NISC)、CEPTOAR Council(http://www.nisc.go.jp/conference/seisaku/ciip/dai12/pdf/12siryou04.pdf)など。

*63 日本セキュリティオペレーション事業者協議会、WG5 標的型攻撃対策検討WG(http://www.jnsa.org/isog-j/activities/index.html)。

*64 例えば、J-CSIPやテレコムアイザック官民協議会において、主導的な役割を果たす団体による「サイバー攻撃解析協議会」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000021.html)や、警察庁とISOG-Jによる「サイバーインテリジェンス対策のための不正通信防止協議会」(https://www.npa.go.jp/keibi/biki3/20120823kouhou.pdf)など。

の関連法規における情報管理の規定や、個別の契約における秘密保持条項などにより、顧客の秘密を守るものとされています。これは事業者が顧客を保護するためには当然実施されるべきことですが、一方で標的型攻撃の存在に気付いた事業者が外部に情報提供を行うことができなくなっている要因ともなっています[*65]。

更に、標的型攻撃の検出や対策が実施されている情報を広く公開することにより、攻撃者に攻撃対象の防御能力や検知能力を教えてしまうという副作用があります。標的型攻撃においては、攻撃者は特定の組織の特定の情報を入手しようとするなど、強い目的意識を持っていることが想定されます。このため、攻撃者が攻撃が検出、対処されたことを知った場合、検出可能な手法の利用をやめ、より巧妙な別の手法を用いて攻撃を実施してくる可能性が高くなります。

このように、標的型攻撃に関する情報は、情報の公開範囲や情報を提供された組織が取り扱いを誤ると、情報を提供した組織に新たなリスクを与える可能性があります。その取扱いに十分な注意が必要であり、そのために先に紹介した対策の活動のうちのいくつかでは、情報提供を受ける組織に対して非常に厳格な守秘義務を課して、この問題に対応しようとしています。

■ 標的型攻撃対策のための情報共有の検討例

一方で、情報の提供を受ける組織では、どのような情報を必要とするのでしょうか。ここでは、日本セキュリティオペレーション事業者協議会(ISOG-J)WG5の成果[*66]を例に取り、その検討の様子を紹介します。

ISOG-Jは日本のセキュリティサービス事業者が集まった団体で、その構成メンバーは、何らかの形で顧客にセキュリティを提供している事業者です。このため、標的型攻撃においても、それぞれのメンバーが提供するサービスの機能などでその攻撃を止め、攻撃が成立しなくなることを目的に、WGにて活動しています。このWGの中で、実際にどのような情報が、メンバーの対策活動に役立つのかを検討するために、昨年度、標的型攻撃に関する3つの情報共有の実証実験を行いました。複数の条件において、これらの情報を得られたら、自社のサービスで何がどのような精度や速度で対策できるかという視点で、検討を行っています。

まず、「標的型攻撃のすべての情報を得られた」ことを想定し、標的型攻撃と似た構造を持つ、メール添付型のマルウェアを選び、そのメールヘッダ、宛先、本文、マルウェアといった、すべて実在の情報を共有しました。次に、標的型攻撃に利用されたことの分かっているマルウェアについて、その検体名称で情報を共有しました。そして、最後に、メールの送信元、マルウェアのダウンロードに関わるサーバ、マルウェアの制御に利用されたサーバなど、標的型攻撃に利用された通信の情報に関して共有し、実施しました。

この実験の結果「すべての情報を得られた」ときには、そのメールヘッダやマルウェアの解析に時間を要し、迅速な対応が行えない場合があることが、次にマルウェア検体名称については、各社で利用するウイルス対策ソフトウェアの違いや、名称を付けるタイミングの違いなどにより正規化されておらず、対策のために提供する情報としては適切な情報とは言えないということが分かりました。セキュリティサービス事業者の間では、3つ目の通信に関わる情報が最も取扱いやすく、対処も実施しやすい情報であることが分かりました。

このように、セキュリティ対策のための情報共有においては、必ずしもすべての情報が必要というわけではなく、対策の中で担う役割に応じて適切な情報の範囲があると言えるのです[*67]。

■ 情報共有の成功事例

ここで、日本国内における脆弱性情報流通を例にとり、情報共有の成功事例を紹介します。製品に関する脆弱性を発見した人は、その情報の取り扱いを誤ると、製品開発者との関係が悪化したり、その脆弱性を悪用した事件への関与を

＊65　このような状況を受け、情報提供に関する条項を持つ契約ひな形の検討を開始する動きが出ています。内閣官房情報セキュリティセンター、「情報セキュリティ政策会議資料」(http://www.nisc.go.jp/conference/seisaku/)。
＊66　Network Security Forum 2012「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/data/B2_isog-j.pdf)。
＊67　ISOG-J WG5では、この結果を受け、事業者が対策をしやすい情報の抽出をテーマに事例研究を続けている。

疑われたりする可能性があります。日本においては、その情報の取り扱いを情報セキュリティ早期警戒パートナーシップ[*68]に任せることができます。

この枠組みでは、匿名化による発見者保護、IPAとJPCERT/CCによる脆弱性情報と製品開発者情報の集約と対応責任、事前に登録した製品開発者にのみ脆弱性情報を提供し対策を促す情報共有範囲の制限、そして脆弱性の対策を行ったバージョンの開発期間を調整する情報公開のタイミングの制御、対策済の製品に関する情報公開が一貫して行われています。このため、脆弱性発見者のリスクをなくした上で、脆弱性情報が対策前に漏えいすることを防ぎ、製品開発者に対策期間の猶予を与え、対策が施された製品に関する情報を、即座に利用者に伝えることに成功しています。

■ 標的型攻撃に関する情報共有の検討

この例と同様に、標的型攻撃においても、攻撃にさらされた組織の秘密を守りながら、攻撃手法(メールや脆弱性、マルウェア)の情報、その攻撃者の意図などを共有することで、同じような攻撃が発生した場合に防御できることを目的として、攻撃に関する情報共有を行うことが求められます。これまで紹介してきたように、このためには

- 責任のとれる組織による情報集約
- 被害組織の情報の保護
- 当該標的型攻撃に関する解析、情報抽出
- 対策の能力を持つ組織に対する適切かつ迅速な情報提供
- 攻撃に関する公開タイミングの調整

などが必要となります。先に紹介した複数の情報共有プロジェクトにおいても、これらの点を考慮した情報共有が実現されようとしています。

■ まとめ

標的型攻撃の被害にあう可能性のある多くの組織においては、他の組織で発生した攻撃に関する情報を共有してもらうことで自組織での対策に役立てるために、既に何らかの情報共有の活動に参加していると考えられます。一方で、情報共有の活動を成功させるためには、標的型攻撃にさらされた組織からの情報の提供が必要です。自組織の参加する活動が、ここで検討した項目についてどのように実現しているかを確認した上で、率先して情報の提供を行うことで、情報共有の活動全体の活性化につなげることができるのです。

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、インターネット上に公開されている公開鍵の問題、スマートフォンのセキュリティ、標的型攻撃対策のための情報共有に関する議論についてまとめました。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 サービスオペレーション本部 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などに従事の後、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など、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(1.3 インシデントサーベイ)
須賀 祐治(1.4.1 SSL/TLS、SSHで利用されている公開鍵の多くが他のサイトと秘密鍵を共有している問題)
加藤 雅彦(1.4.2 安全なスマートフォンの利用)
齋藤 衛(1.4.3 標的型攻撃対策のための情報共有)
IIJ サービスオペレーション本部 セキュリティ情報統括室

協力:
根岸 征史、春山 敬宏、小林 直、梨和 久雄、桃井 康成、齋藤 聖悟、吉川 弘晃 IIJ サービスオペレーション本部 セキュリティ情報統括室

*68 情報セキュリティ早期警戒パートナーシップを含めた脆弱性情報の取り扱いについては、IIR Vol.8「1.4.3 脆弱性情報流通動向」(http://www.iij.ad.jp/company/development/report/iir/008.html)をご参照ください。