

東日本大震災に関連したセキュリティ事件

今回は、マルウェア観測の実装とマルウェアによるフォレンジック回避の手法について解説するとともに、東日本大震災にともなう日本国内の通信状況と関連するセキュリティインシデントについて紹介します。

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IJ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、IJ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1月から3月までの期間では、前回に引き続きWebブラウザとそのプラグインに関する脆弱性が悪用され、携帯端末やクラウドコンピューティングに関する事件も増えています。また、中東の政変に関連した攻撃や、韓国でマルウェアを利用したDDoS攻撃も発生しています。さらに、日本で発生した東日本大震災に関連し、国内の通信状況の変化や、震災に便乗した攻撃も発生しています。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。

1.2 インシデントサマリ

ここでは、2011年1月から3月までの期間にIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します*1。

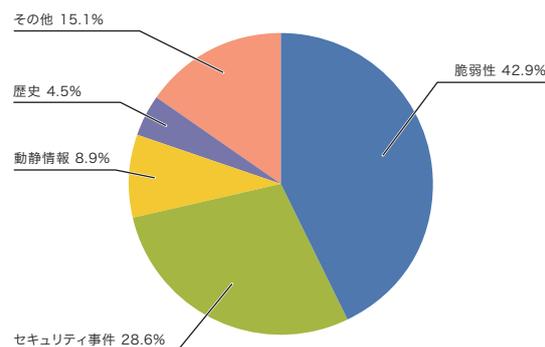


図-1 カテゴリ別比率(2011年1月～3月)

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

■ 脆弱性

今回対象とした期間には、マイクロソフト社の Internet Explorer^{*2}、Windows^{*3*4*5}、アドビ社の Adobe Reader と Acrobat^{*6*7}、Flash Player^{*8*9}、Shockwave Player^{*10}、オラクル社の JRE^{*11}等、Webブラウザやアプリケーションに数多く脆弱性が発見され、対策されています。アップル社の Mac OS X^{*12}でも、複数の脆弱性が修正されています。これらの脆弱性のうちいくつかは、対策が公開される前に悪用が確認されました。

また、マイクロソフト社のインターネット インフォメーション サービス (IIS) の FTP サービス^{*13}、Linux 等で利用されている FTP サーバの vsftpd^{*14}、データベースサーバとして利用されているオラクル社の Oracle Database^{*15}、DNS サーバの ISC BIND^{*16}、CMS として利用されている WordPress^{*17}等、サーバアプリケーションでも多くの脆弱性が修正されました。さらに、携帯電話等のプラットフォームとして利用されているアップル社の iOS^{*18}でも脆弱性が発見され、修正されています。

■ 動静情報

IJ は、国際情勢や時事に関連する各種動静情報にも注意を払っています。今回対象とした期間では、チュニジアやエジプトで発生した政変に伴って、インターネット回線の遮断や^{*19}、大規模な DDoS 攻撃^{*20}が発生して話題になりました。しかし、IJ の設備や IJ のお客様のネットワーク上では直接関係する攻撃は検出されませんでした。

■ 歴史

この期間には、過去に歴史的背景による DDoS 攻撃やホームページの改ざん事件が発生したことがありました。このため、各種の動静情報に注意を払いましたが、IJ の設備や IJ のお客様のネットワーク上で直接関係する攻撃は検出されませんでした。

■ セキュリティ事件

動静情報に結びつかない突発的なインシデントとしては、携帯端末のプラットフォームとして利用される Android OS を標的としたウイルス^{*21}が海外で確認さ

-
- *2 「マイクロソフト セキュリティ情報 MS11-003 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2482017)」 (<http://www.microsoft.com/japan/technet/security/bulletin/ms11-003.mspx>)。
 - *3 「マイクロソフト セキュリティ情報 MS11-006 - 緊急 Windows シェルのグラフィック処理の脆弱性により、リモートでコードが実行される (2483185)」 (<http://www.microsoft.com/japan/technet/security/bulletin/MS11-006.mspx>)。
 - *4 「マイクロソフト セキュリティ アドバイザリ (2501696) MHTML の脆弱性により、情報漏えいが起こる」 (<http://www.microsoft.com/japan/technet/security/advisory/2501696.mspx>)。この脆弱性は4月に「マイクロソフト セキュリティ情報 MS11-026 - 重要 MHTML の脆弱性により、情報漏えいが起こる (2503658)」 (<http://www.microsoft.com/japan/technet/security/bulletin/ms11-026.mspx>) により修正された。
 - *5 「マイクロソフト セキュリティ情報 MS11-015 - 緊急 Windows Media の脆弱性により、リモートでコードが実行される (2510030)」 (<http://www.microsoft.com/japan/technet/security/bulletin/MS11-015.mspx>)。
 - *6 AP SB11-03: 「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/apsb11-03.html>)。
 - *7 AP SB11-06: 「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/apsb11-06.html>)。
 - *8 AP SB11-02: 「Flash Player 用セキュリティアップデート公開」 (<http://www.adobe.com/jp/support/security/bulletins/apsb11-02.html>)。
 - *9 AP SB11-05: 「Adobe Flash Player 用セキュリティアップデート公開」 (<http://www.adobe.com/jp/support/security/bulletins/apsb11-05.html>)。
 - *10 AP SB11-01: 「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/apsb11-01.html>)。
 - *11 「Java™ SE 6 アップデートリリースノート」 (<http://java.sun.com/javase/ja/6/webnotes/6u24.html>)。
 - *12 「Mac OS X v10.6.7 のセキュリティコンテンツおよびセキュリティアップデート 2011-001 について」 (http://support.apple.com/kb/HT4581?viewlocale=ja_JP)。
 - *13 「マイクロソフト セキュリティ情報 MS11-004 - 重要 インターネット インフォメーション サービス (IIS) の FTP 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 (2489256)」 (<http://www.microsoft.com/japan/technet/security/bulletin/ms11-004.mspx>)。
 - *14 JVNDB-2011-001378: 「vsftpd の vsf_filename_passes_filter 関数におけるサービス運用妨害 (DoS) の脆弱性」 (<http://jvndb.jvn.jp/ja/contents/2011/JVNDB-2011-001378.html>)。
 - *15 "Oracle Critical Patch Update Advisory - January 2011" (<http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html>)。
 - *16 BIND "Server Lockup Upon IXFR or DDNS Update Combined with High Query Rate" (<http://www.isc.org/software/bind/advisories/cve-2011-0414>)。
 - *17 「WordPress 3.0.5 (そして、3.1 リリース候補 4)」 (<http://ja.wordpress.org/2011/02/08/wordpress-3-0-5/>)。
 - *18 「iOS 4.3 のセキュリティコンテンツについて」 (http://support.apple.com/kb/HT4564?viewlocale=ja_JP)。
 - *19 この件に関しては、例えば Arbor networks 社の "THE ARBOR NETWORKS SECURITY BLOG: Egypt Loses the Internet" (<http://asert.arbornetworks.com/2011/01/egypt-loses-the-internet/>) に詳しい。
 - *20 この件に関しては、例えば SOPHOS 社のブログである nakedsecurity 等に詳しい。"Egypt versus the internet - Anonymous hackers launch DDoS attack" (<http://nakedsecurity.sophos.com/2011/01/26/egypt-versus-the-internet-anonymous-hackers-launch-ddos-attack/>)。
 - *21 独立行政法人 情報処理推進機構 (IPA) 「Android OS を標的としたウイルスに関する注意喚起」 (<http://www.ipa.go.jp/security/topics/alert20110121.html>)。

れたり、正当に署名されたファイルを利用して正規ソフトウェアのように振る舞うスケアウェアが報告されたりしました^{*22}。また、大手サイトのSSL証明書が不正に発行され^{*23}、その悪用を防ぐためにWebブラウザでこれらの証明書を失効させるためのアップデートが行われました^{*24}。

さらにMTAのExim等のように特定のサーバの脆弱性を狙った攻撃^{*25}やSIPサーバに対する不正な通信^{*26}についても引き続き確認されており、これらを利用した外部公開サーバに対する不正利用が発生しています^{*27}。韓国では、2009年7月に発生したDDoS攻撃と類似した攻撃が3月3日に再び発生しました^{*28}。メールやSNSを利用してマルウェアに感染させようとする試み^{*29}や、クラウド環境を悪用した攻撃も数多く発生しています^{*30}。

■ その他

その他のインシデントとしては、2月にニュージーラン

ドで発生した地震や、3月の東日本大震災等の自然災害に関連する動向に注目しました。これらの大震災に便乗したSEOポイズニング攻撃^{*31}や標的型攻撃^{*32}の発生を確認しています。また、セキュリティ関連の動向としては、12月にルートゾーンに.jpゾーンのDSレコードが登録され、1月にはJPのドメイン名サービスにDNSSECが導入されました^{*33}。

また、IANA (Internet Assigned Numbers Authority) が管理している未割り振りのIPv4アドレスがすべて放出され、IPv4アドレスの枯渇が現実のものとなりました^{*34}。さらに、2010年に発生したセキュリティ事件をまとめた文書「2011年版10大脅威 進化する攻撃…その対策で十分ですか?」がIPAから発表されたり^{*35}、電気通信事業者がDoS攻撃等の大量通信を識別し、その対処を適法に実施するためのガイドライン「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」が電気通信事業関連5団体より公表されたりしています^{*36}。

- *22 Symantecセキュリティレスポンスブログ「信頼済みのソフトウェアを悪用する不正行為」 (<http://www.symantec.com/connect/ja/blogs-161>)。
- *23 詳細については例えば次のエフセキュアブログに詳しい。「不正なSSL証明書(Comodoケース)」 (<http://blog.f-secure.jp/archives/50581423.html>)。
- *24 証明書発行機関のシステムが不正に利用されて発行されてしまった有名Webサイトに対する証明書は、証明書失効リスト(CRL)に追加されたが、Webブラウザの実装や設定によっては、偽のWebサイトを正当なものとして判断してしまう可能性があり、これらの証明書を個別に不正と判断する仕組みがブラウザ修正として配布された。例えば、「マイクロソフト セキュリティ アドバイザリ (2524375) 不正なデジタル証明書により、なりすましが行われる」 (<http://www.microsoft.com/japan/technet/security/advisory/2524375.mspx>) や、Mozilla Firefoxの「セキュリティアップデート (3.6.16/3.5.18) を公開しました」 (<http://mozilla.jp/blog/entry/6491/>) 等がある。
- *25 この件に関しては、次のIBM社の東京SOCによる報告に詳しい。Tokyo SOC Report「Eximの脆弱性を悪用してサーバにBotを感染させようとする攻撃」 (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/exim_attack_20110309?lang=ja)。
- *26 cNotesでは不定期にSIPに関する観測情報が提供されている。例えば、2011年になってからの攻撃元のIPアドレスや国の分類等を掲載。「不正なSIP着信42 2011年に入って」 (<http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=%C9%D4%CO%B5%A4%CASIP%C3%E5%BF%AE+42+2011%C7%AF%A4%CB%C6%FE%A4%C3%A4%C6>)。
- *27 JPCERTコーディネーションセンター(JPCERT/CC)「主に UNIX/Linux 系サーバを対象としたインターネット公開サーバのセキュリティ設定に関する注意喚起」 (<http://www.jpccert.or.jp/at/2011/at110002.txt>)。
- *28 「アンラボ、韓国で40のWebサイトを対象にしたDDoS攻撃への注意喚起」 (http://www.ahnlab.co.jp/company/press/news_release_view.asp?searchWord=&movePage=&seq=5568)。
- *29 詳細については以下のトレンドマイクロ社のセキュリティブログに詳しい。「地震、津波、原発、節電などのファイル名の不正プログラムが国内で流通」 (<http://blog.trendmicro.co.jp/archives/4001>)。
- *30 2010年に発生したクラウドからの攻撃については、例えば次のIBM社の東京SOCからの報告で詳しく解説している。Tokyo SOC Report「クラウドを悪用した攻撃」 (https://www-950.ibm.com/blogs/tokyo-soc/entry/cloud-attack_20110216?lang=ja)。
- *31 詳細については以下のトレンドマイクロ社のセキュリティブログに詳しい。「東北地方太平洋沖地震に便乗したSEOポイズニングを確認。「FAKEAV」へと誘導」 (<http://blog.trendmicro.co.jp/archives/3981>)。
- *32 例えば、トレンドマイクロ株式会社のマンスリーレポートで報告されている。「インターネット脅威マンスリーレポート【2011年3月度】～震災に便乗したサイバー攻撃、心理的な隙を狙う手法に注意を～」 (http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20110406083423.html)。
- *33 株式会社日本レジストリサービス(JPRS)「JPRSがJPドメイン名サービスにDNSSECを導入」 (<http://jprs.co.jp/press/2011/110117.html>)。
- *34 社団法人日本ネットワークインフォメーションセンター(JPNIC)「IANAにおけるIPv4アドレス在庫枯渇、およびJPNICの今後のアドレス分配について」 (<http://www.nic.ad.jp/ja/topics/2011/20110204-01.html>)。
- *35 独立行政法人情報処理推進機構(IPA)「2011年版 10大脅威 進化する攻撃… その対策で十分ですか?」 (<http://www.ipa.go.jp/about/press/20110324.html>)。
- *36 インターネットの安定的な運用に関する協議会は電気通信事業関連の5つの業界団体により構成されている。このガイドラインの策定については次を参照のこと。社団法人日本インターネットプロバイダー協会(JAIPA)「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドラインの改定について」 (http://www.jaipa.or.jp/other/mtcs/info_110325.html)。

1.3 インシデントサーベイ

IJでは、インターネット上で発生するインシデントのうち、インフラストラクチャ全体に影響を与える可能性があるインシデントに注目し、継続的な調査研究と対処を行っています。ここでは、そのうちDDoS攻撃と、ネットワーク上でのマルウェアの感染活動、Webサーバに対するSQLインジェクション攻撃の実態について、その調査と分析の結果を示します。

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になっています。

■ 直接観測による状況

図-2に、2011年1月から3月の期間にIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。ここに示す件数は、IJ 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です。IJでは、ここに示す以外の攻撃にも対処していますが、正確な攻撃実態の把握が困難なため、集計対象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^{*37}、サーバに対する攻撃^{*38}、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カ月間でIJは、585件のDDoS攻撃に対処しました。1日あたりの対処件数は6.5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攻撃全体に占める攻撃手法の割合は、回線容量に対する攻撃が0%、サーバに対する攻撃が24%、複合攻撃が76%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5万7千ppsのバケットによって163Mbpsの通信量を発生させるものでした。また、攻撃の継続時間は、開始から終了までが30分未満のものが全体の85%、30分以上24時間未満のものが15%に分布しており、24時間以上継続した攻撃はありませんでした。なお、今回の期間中で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、6時間にわたりました。攻撃元の分布としては、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^{*39}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^{*40}の利用によるものと考えられます。

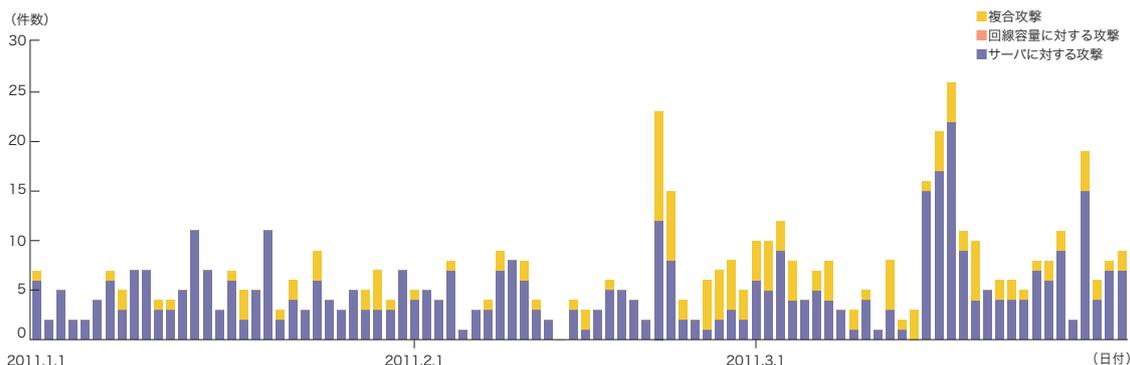


図-2 DDoS攻撃の発生件数

*37 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。

*38 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消費させる。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。

*39 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。

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

■ backscatterによる観測

次に、IJJのマルウェア活動観測プロジェクトMITFのハニーポット^{*41}によるDDoS攻撃のbackscatter観測の結果を示します^{*42}。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1月から3月の期間中に観測された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34.0%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、米国26.4%、アルゼンチン21.4%、中国21.3%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。

なお、2月の後半からその他に分類される攻撃の増加が見られますが、その多くがアルゼンチンの複数のアドレスの、数多くのポートに対する攻撃です。特定のアドレスについてポートを昇順に攻撃しており、通信の様子はポートスキャンと似ていますが、IPスプーフィングにより攻撃者が応答を得ることができないため、意図は不明です。

今回の対象期間中には、エジプト等の中東諸国でのDDoS攻撃(1月後半)や、wordpress.comへの攻撃(3

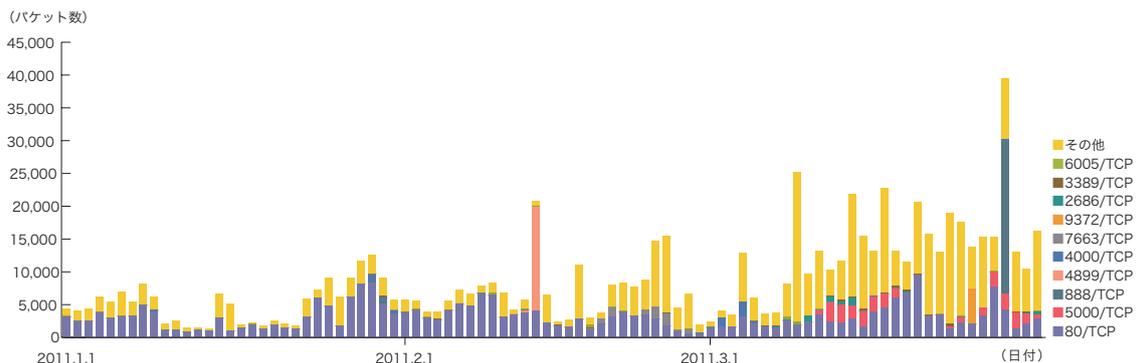


図-3 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

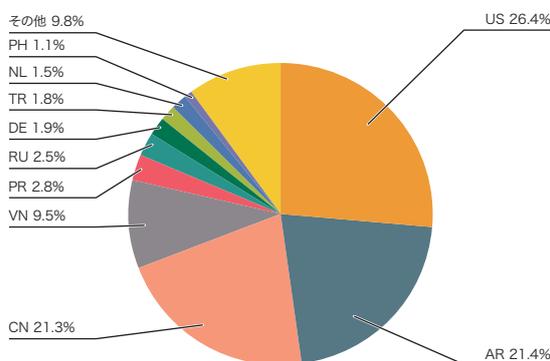


図-4 backscatter観測によるDDoS攻撃対象の分布(国別分類、全期間)

*41 「1.3.2 マルウェアの活動」も参照のこと。

*42 この観測手法については、本レポートのVol.8 (http://www.ijj.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、IJJによる観測結果の一部について紹介している。

月初旬)、韓国におけるDDoS攻撃(3月3日)等が発生しましたが、この観測では、エジプトの2サイトに関する攻撃を検出しています。他の攻撃については、IPスプーフィングをともなわない種類の攻撃が行われたか、攻撃にIJの観測装置のアドレス以外のアドレスを利用されたと考えられます。

1.3.2 マルウェアの活動

ここでは、IJのマルウェア活動観測プロジェクトMITF^{*43}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^{*44}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行為による通信であると考えられます。

■ 無作為通信の状況

2011年1月から3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。

ハニーポットに到着した通信の多くは、マイクロソフト社の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、HTTPで利用される80/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、9230/UDP、28002/TCP等、一般的なアプリケーション

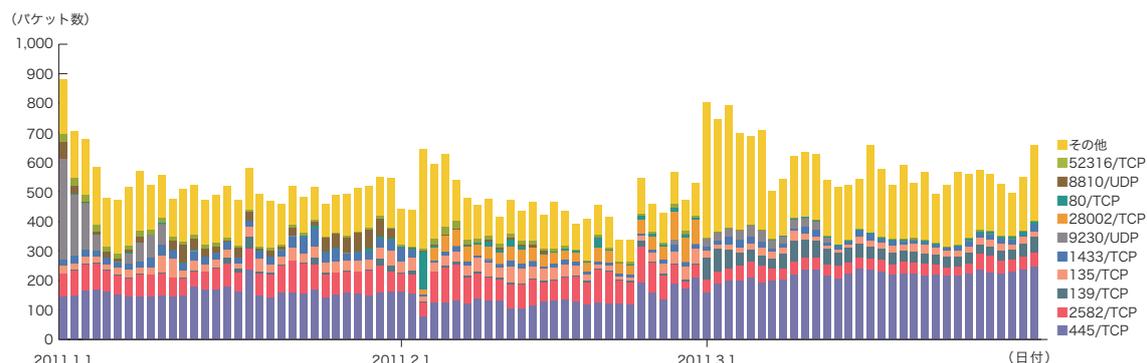


図-5 ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

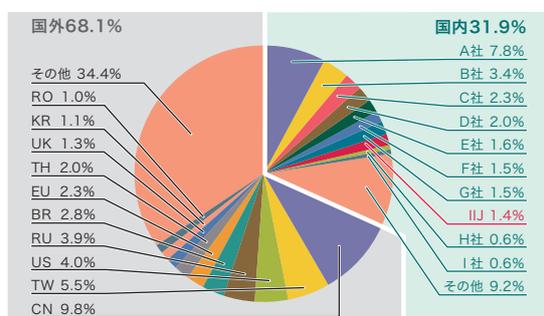


図-6 発信元の分布(国別分類、全期間)

*43 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。

*44 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。

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の発信元の国別分類を見ると、日本国内の31.9%、中国の9.8%が比較的大きな割合を占めています。

■ 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取得検体数の推移を図-7に、マルウェアの検体取得元の分布を図-8にそれぞれ示します。図-7では、1日あたりにハニーポットで取得したマルウェア検体の総数を総取得検体数、検体の種類をハッシュ値^{*45}で分類したものをユニーク検体数として示しています。

期間中での1日あたりの平均値は、総取得検体数が307、ユニーク検体数が37でした。前回の集計期間では、平均

値が総取得検体数で190、ユニーク検体数で30でした。

図-8に示す検体取得元の分布では、日本国内が10.5%、国外が89.5%でした。なお、前回までと同じく、台湾が28.8%と引き続き大きな割合を占めています。これは、この期間中にMybotとその亜種の活動が活発化し、特に台湾における活動が顕著であったためです。

MITFでは、マルウェアの解析環境を用意し、取得した検体について独自の解析を行っています。今回の調査期間に取得した検体は、ワーム型48.7%、ポット型44.3%、ダウンロード型7.0%でした。また、解析により、48個のポットネットC&Cサーバ^{*46}と59個のマルウェア配布サイトの存在を確認しました。

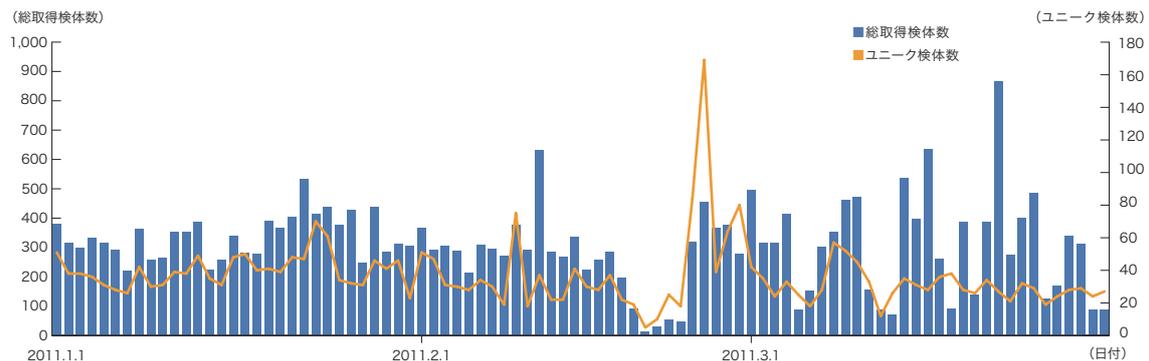


図-7 取得検体数の推移(総数、ユニーク検体数)

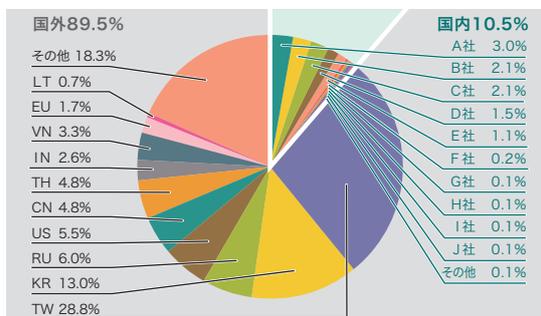


図-8 検体取得元の分布(国別分類、全期間)

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

*46 Command & Controlサーバの略。多数のポットで構成されたポットネットに指令を与えるサーバ。

1.3.3 SQLインジェクション攻撃

IJ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^{*47}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1月から3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推移を図-9に、攻撃の発信元の分布を図-10にそれぞれ示します。これらは、IJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、日本48.2%、米国21.2%、中国5.1%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には、前回からあまり変化は見受けられませんでした。ただし、1月29日に米国からの特定サーバに対する大規模攻撃が発生し、3月2日、3月8日、3月22日に別のサーバに対して国内外からの攻撃が発生する等、いくつかのサーバに対して集中的に攻撃が発生しました。このため、全体に占める日本と米国の割合が増加し、中国や韓国等からの攻撃件数の割合が減少しています。また、この期間にSQLインジェクションによるWebサイト改ざん攻撃として話題になったLizaMoon^{*48}攻撃については、2月4日から中旬にかけて小規模な攻撃が複数のサーバに対して試みられていました。

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

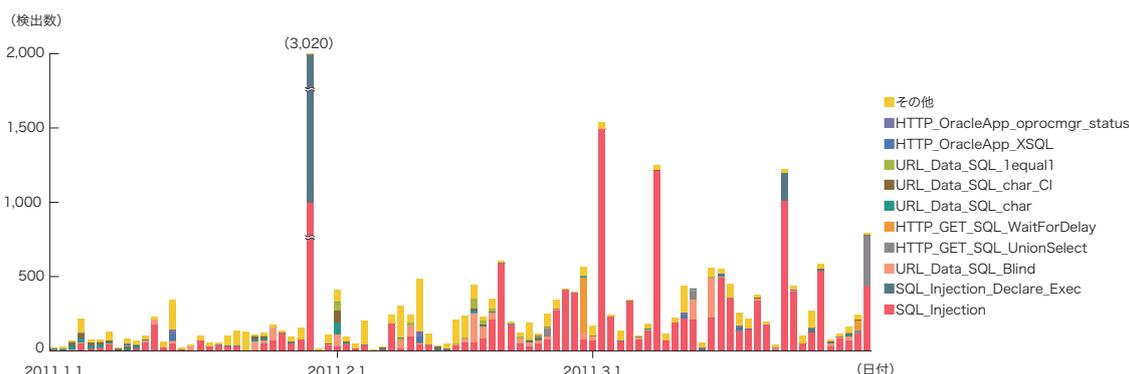


図-9 SQLインジェクション攻撃の推移(日別、攻撃種類別)

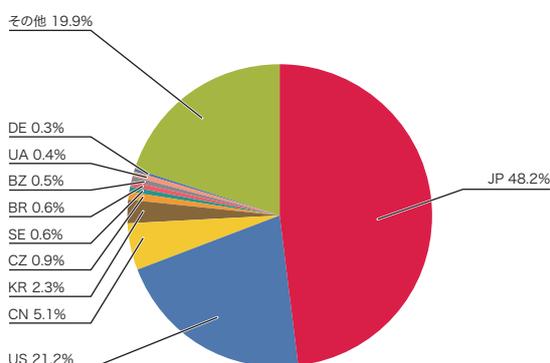


図-10 SQLインジェクション攻撃の発生元の分布(国別分類、全期間)

*47 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。

*48 LizaMoon攻撃については、例えば次のIBM社の東京SOCによる報告に詳しい。Tokyo SOC Report「新しいタイプのWebサイト改ざんSQLインジェクション攻撃」(https://www-304.ibm.com/blogs/tokyo-soc/entry/sqlinjection_20110401?lang=ja_jp)。

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、IJ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、今回新たに採用したdionaeaハニーポットと、マルウェアによるアンチフォレンジックについて解説するとともに、東日本大震災による日本の通信事情への影響と関連する攻撃について紹介します。

1.4.1 dionaeaハニーポット

IJでは、2007年5月よりマルウェア対策活動MITF (Malware Investigation Task Force) を行っています^{*49}。この活動の一端としてハニーポット^{*50}システムを構築し、IJの網を攻撃するワームやポットの活動を直接観測しています。これまで、この観測にnepenthes^{*51}を利用していました。ここでは、新しいハニーポットシステムとして稼働を開始したdionaea^{*52}の機能や特徴を説明します。

■ dionaeaの特徴

dionaeaは、nepenthesの後継となる実装として2009年5月末に公開され、現在も開発が活発に継続されているハニーポット用ソフトウェアです。dionaeaは、nepenthesに比べてマルウェア取得やログの取得等の

機能が強化されています。また、IPv6に対応していたり、pythonベースの実装により拡張が容易といった特徴を備えています。ここでは、dionaeaの特徴のうち次のものの概要を示します。

- マルウェア取得機能
- 攻撃検出の精度向上
- ログ取得機能の強化

マルウェア取得の機能強化としては、新しい脆弱性のサポートを上げることができません。nepenthesは、MS05-017までしか脆弱性をエミュレートしていませんでした。これに対してdionaeaでは、攻撃に使用される事が少なくなった古い脆弱性のサポートを廃止し、MS08-067^{*53}等の新しい脆弱性に対応できる検出方法に変更されました。

nepenthesでは、攻撃の通信のペイロードに対するパターンマッチングによって攻撃検出を行っていました。このため、SMB等の複雑なプロトコルを用いた通信の後に攻撃が行われるような場合、それをエミュレートすることが難しいという欠点がありました。dionaeaでは、SMBとMSRPCのプロトコルエミュレーションを実装することで、この課題を解決しています。また、x86エミュレータであるlibemu^{*54}と連動してペイロード内のshellcodeを自動検出することで、未知の脆弱性を悪

*49 MITFに関しては、IIR vol.7 「1.4.3 マルウェア対策活動MITF」にて解説している (http://www.ij.ad.jp/development/iir/pdf/iir_vol07.pdf)。

*50 ハニーポットとは、攻撃者の手法を観察するための仕組みで、脆弱性を持つソフトウェアや脆弱なシステムをエミュレートするlow interaction型と、実際のOSやソフトウェアを用いるhigh interaction型がある。

*51 nepenthes (<http://nepenthes.carnivore.it/>) はlow interaction型のサーバ型ハニーポットで、主にMicrosoft社のWindowsの既知の脆弱性をエミュレートする。現在は開発が停止しており、後継のdionaeaを利用するようにアナウンスがされている。

*52 dionaea (<http://dionaea.carnivore.it/>)。

*53 「マイクロソフト セキュリティ情報MS08-067 - 緊急Server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 (958644)」 (<https://www.microsoft.com/japan/technet/security/bulletin/MS08-067.msp>)。

用された場合の検知も可能になりました。

次にログ関連機能について紹介します。dionaeaでは、テキスト形式のログ出力に加えて、SQLiteによるデータベース形式のログ出力もでき、傾向や分析の把握がより容易になっています。nepenthesでは、各ログが時系列に出力されるだけで、後日の関連付けが難しいという課題がありました。これに対してdionaeaでは、どの通信にどの攻撃が含まれていたか、どの通信が発生したことによってマルウェアが取得されたか関連付けできるようになりました。

このほかにも、いくつかの改良点があります。nepenthesでは、C++を使って機能追加しなければなりませんでした。dionaeaではpythonでモジュールを記述できるため、機能の拡張が容易になりました。また、IPv6に対応する等、ここで挙げた以外にも多くの改良が行われています。

■ dionaeaの評価と採用

初期のdionaeaは、動作が不安定で恒常の運用が困難でした。また、毎日のようにソースコードが変更されていた^{*55}ため、IJではnepenthesと併設してdionaeaの評価と実験を継続してきました。この実験的な観測では、ネットワーク上で活動するマルウェアとしてConficker^{*56}の活動が非常に活発であることが分かりました。しかし、IJ網内での感染件数が少ないことも

あり、観測環境の安定稼働を優先し、このマルウェアを取得できないnepenthesでの観測を継続しながら、同時にdionaeaをMITFに適用させるための検討も進めてきました。また、dionaeaの調査と並行して、他のハニーポットの実装^{*57}についても検討を行ってきました。そして、ハニーポットの能力やコミュニティの活発さ、既存システムとの親和性等を総合的に判断した結果、dionaeaをベースにしたハニーポットシステムの構築を決断しました。

この新しいシステムは、2011年3月より正式に観測システムとして稼働しています。新システムでは、評価で明らかになった問題点、例えば攻撃と取得されたマルウェアと関連付けができない、攻撃コードが含まれるMSRPCの命令が不明である等、機能上不十分な点については、IJが独自に実装を拡張しました。また、IJの観測システムの環境に適用させるためにソースコードの修正も行いました。前述のとおり、複雑なプロトコルエミュレーションを行うようになったため、複数回の通信をとまなう攻撃を観測するようになりました。これにより、特定のポートへの接続の観測量が増えたため、「1.3.2 マルウェアの活動」の集計では、3月分の観測値についてこれらの影響を排除するための補正を行っています。またConficker等一部のマルウェアが特定のハニーポットに繰り返し攻撃を行うことが判明したため、この問題に関するシステムの修正も行いました。

*54 libemu (<http://libemu.carnivore.it/>)。

*55 次のURLに、dionaeaの変更履歴が存在する (<http://src.carnivore.it/dionaea/log/>)。これを見るとわかるとおり、2009年5月末に最初のdionaeaがコミットされた後、2010年の後半までほぼ毎日ソースコードが変更されており、開発の活発さが伺える。

*56 Confickerについては、IJR vol.2「1.4.2 MS08-067を悪用するマルウェア」(http://www.ij.ad.jp/development/iir/pdf/iir_vol02.pdf)、IJR vol.4「1.4.1 マルウェアConfickerの世界的流行」(http://www.ij.ad.jp/development/iir/pdf/iir_vol04.pdf)にて取り上げている。

*57 例えば、BothHunter (<http://www.bothhunter.net/>) や amun (<http://amunhoney.sourceforge.net/>)、argos (<http://www.few.vu.nl/argos/>) 等。

■ 新システムによる観測

新システムによる観測結果として、検体取得総数の日別分布を図-11に、マルウェアの種類別分布を図-12に示します。これらの図では、ClamAVによる識別でマルウェアの名称をまとめています。図-11と図-7の2月までの期間を比較することで、取得状況が大きく変わっていることがわかります。総取得検体数の1日当たりの平均は、従来のシステムの307に対し、25246と大きく増加しました。これはnepenthesとdionaeaでの脆弱性のエミュレーション数や種類の違いによるものです。特に両者で大きく異なる点は、Confickerを取得できるようになったことです。

Confickerは、MS08-067の脆弱性を悪用して拡散するワームです。新システムでの検体取得総数のうち、Conficker(図中のWorm.Kido、及びWorm.Downadup)は71.4%と大きな割合を占めています。その感染源について調査すると、国内が3.7%、IJJの網内では0.03%であり、IJJの網内では大きな脅威ではあ

りませんが、世界規模で見ると依然として活発に活動していることがわかります。

このシステム変更によって、どのマルウェアがどのような脆弱性を利用しているかを把握しやすくなり、より迅速に対策活動が行えるようになりました。また、nepenthesでは取得できなかったマルウェアについても、傾向を把握できるようになっています。現在、IIR上での定期的な公開に向けて、さらにシステムの調整を行っています。IJJでは今後もマルウェア対策を推進するため、状況の変化に応じてシステムを更新し、適切に対応していきます。

1.4.2 マルウェアによるアンチフォレンジック

不正アクセスやマルウェア感染等のインシデントが起こった際には、関係する機器のデジタルデータを調査し解析するデジタルフォレンジック技術^{*58}が用いられます。しかし、近年のマルウェアでは、アンチフォレンジックと呼ばれ、解析による検出を妨害する手法が実装

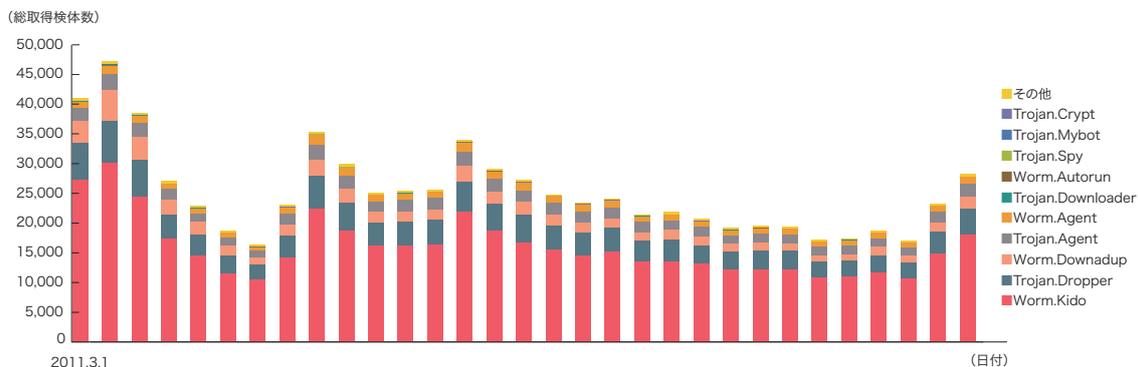


図-11 取得検体数の推移 (日別・新システム・検体別)

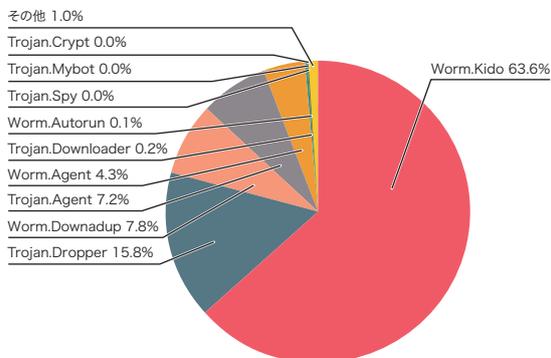


図-12 取得検体の分布 (3月・検体種類別)

*58 デジタルフォレンジック技術についてはIIR Vol.9 「1.4.3 デジタルフォレンジックの概要」を参照のこと (http://www.ijj.ad.jp/development/iir/pdf/iir_vol09.pdf)。

されるようになってきています。アンチフォレンジックは、ディスクやメモリ等のメディアに存在するデータを消去もしくは変更することによって行われます。ここでは、フォレンジック解析によって調べることが最も多いディスク(Windowsファイルシステム)を対象としたアンチフォレンジックの手法を紹介するとともに、解析者の立場で採るべき対策について述べます。

■ ファイルの削除

最もよく見られるアンチフォレンジック手法は、単純にマルウェアの活動に関係するファイルを削除するというものです。ファイルが削除されると、エクスプローラ等の通常利用されているソフトウェアでは、そのファイルが見えなくなります。しかし、ファイルが削除されても直ちにデータ自体が消去されるわけではありません。実際には、ファイルシステムによって管理されている該当ファイルのメタデータの一部が変化する^{*59}だけです。このため、フォレンジック解析に用いるソフトウェア^{*60}によって、削除されたファイルを調べることが可能です。つまり、ファイルが削除されてもデータ自体が別のファイルによって上書きされる前であれば、この手法による隠ぺいに対処できます。

■ タイムスタンプの変更

次によく見られる手法は、ファイルのメタデータであるタイムスタンプを変更するものです。コンピュータのハードディスクドライブは年々大容量化が進み、多くのデータが保存されています。このため、調べる対象のファイルをできるだけ少なくするために、インシデントが発生した期間を絞った解析が行われることがあります。この期間の絞り込みには、ファイルの作成時刻や更新時刻等のタイムスタンプ情報が用いられます。マルウェアは、隠ぺいしたいファイルのタイムスタンプ情報を、SetFileTime API等を用いて本来の時刻とは全く異なる時刻にセットし直すことで、解析対象から逃れようとする。この手法は、3年ほど前からConficker等多数のマルウェアで使われています。

この手法に対しては、2つの対処方法があります。1つは、対象のファイル以外のデータに付属するタイムスタンプを調べることです。例えば、Windowsのレジストリキーは、最終更新時刻を保持しています。このため、サービスとしてレジストリに登録されるマルウェア等に対しては、レジストリの時刻も合わせて調べることで、対象のファイルを検出できます。また、Windowsでは、exeファイルを実行する際にプリフェッチファイルと呼ばれる高速実行のためのファイルが生成されます。このプリフェッチファイルのタイムスタンプ情報をチェックすることで、exeファイルの実行時刻を特定できます。

もう1つの対処方法は、通常は参照されないマイナーなタイムスタンプ情報を期間の絞り込みに使う方法です。WindowsのNTFSファイルシステムは、ファイルのタイムスタンプ情報を含むメタデータをMFT (Master File Table) と呼ばれる構造で保存しています。MFTでは、ファイルのメタデータがエントリの属性として管理されています。通常参照されるタイムスタンプ情報は、Standard Informationと呼ばれる属性が持つタイムスタンプ情報で、SetFileTime等のAPIによって容易に変更可能です。一方、File Nameと呼ばれる属性が持つタイムスタンプ情報は、APIによる変更はできません。したがって、File Name属性のタイムスタンプ情報を用いて絞り込みを行えば、マルウェアによるタイムスタンプ変更の影響を無効化できます

■ 上書き削除

単純なファイルの削除では、メタデータの一部が変更されるだけで、ファイルのデータ自体は削除されません。このため一部のマルウェアは、ファイルのデータ自体をランダムデータで上書きして削除する手法を用います。IJでは、今年3月初めに韓国で流行したDDoS攻撃を行うマルウェアが、この手法を用いていることを確認しています^{*61}。データ自体が上書きされてしまうと、その後のマルウェアの動的解析や静的解析が行えず、マルウェアの性質を把握することが困難になります。ただし、メ

*59 WindowsのNTFSファイルシステムがファイルを削除する際に行うことは、該当するメタデータのレコードが使用中であることを示すフラグと、データが保存されている領域が使用中であることを示すフラグをクリアすることのみ。よって、別のファイルによって上書きされない限りはメタデータとデータの中身の両方が残っている状態になる。

*60 解析に用いるソフトウェアとしては、EnCase (<http://www.guidancesoftware.com/>)、FTK (<http://accessdata.com/>)、TSK (<http://www.sleuthkit.org/sleuthkit/>) 等がある。

*61 このマルウェアはファイル共有サイト経由でダウンロードされ、特定サイトへDDoS攻撃を行うだけでなく、感染端末のハードディスクの破壊等も行った。このマルウェアの挙動に関しては、例えば次のMcAfee Blogに詳しい。McAfee Blog: 「韓国のDDoS攻撃に関する追加情報: データを破壊するペイロードを確認」 (http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1191)。

タデータは残っているため、それを元に関連する活動を調べていくことはできます。また、成功の可能性はあまり高くありませんが、システムの復元機能による自動バックアップ (WindowsのSystem Restore Point等) によって、削除前のファイルが残っていることもあるため、合わせてチェックすべきです。

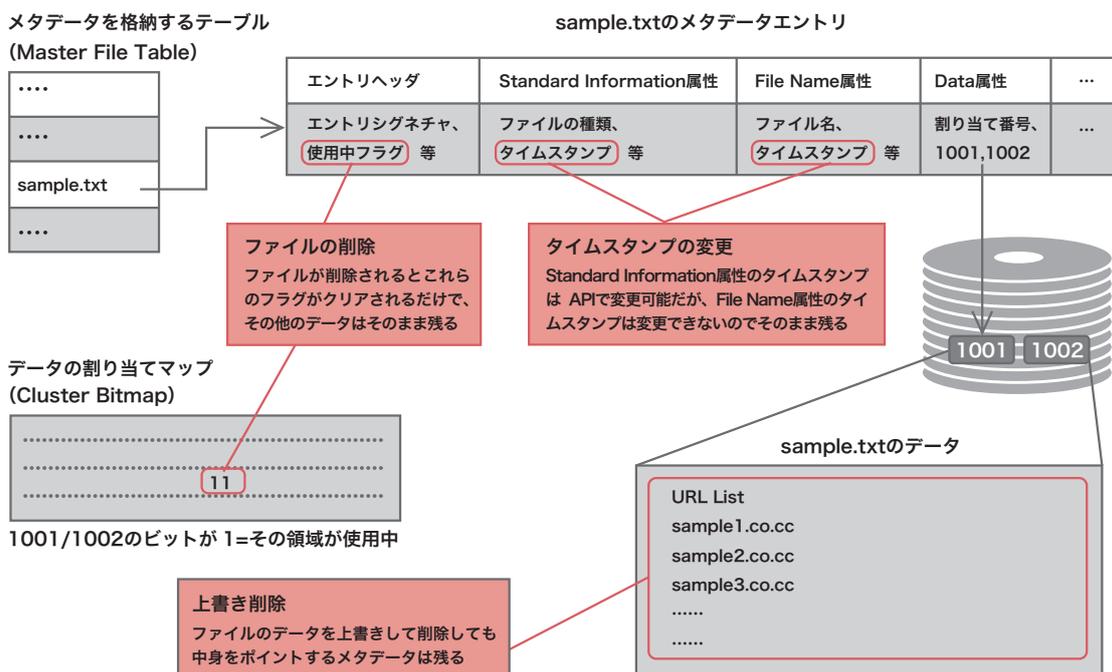
■ ファイルシステムへの直接アクセス

ここまでで紹介してきたアンチフォレンジック手法は、すべてシステムのAPIを用いて削除や変更を行うものでした。これらの手法によって変更される情報を図-13に示します。これを見て分かる通り、いずれの手法が用いられたとしてもファイルシステムのメタデータには何らかの痕跡が残り、メタデータから対象のファイルを検出したり関連する活動を追うことが可能です。

しかし、最近ではAPIを用いず、ファイルシステムの構造を解析して感染動作を行うマルウェアも出てきてい

ます。シマンテック社が今年3月に報告したBackdoor.Prioxer^{*62}は、ハードディスクドライブをRAWモードでオープンしてファイルシステムの種類を識別し、そのファイルシステムのアルゴリズムに沿って感染対象のファイルを見つけ出した後、悪性コードを書き込みます。

この手法に対しては、メタデータを用いた調査手法は効果がなく、データの中身に着目した解析を実施する必要があります。例えば、ファイルのデータのハッシュ値を比較します。感染先となるファイルにはシステム標準の実行ファイルが多いため、その実行ファイル群の正常状態でのハッシュ値を事前に計算しておく^{*63}、感染マシン内の実行ファイル群のものと比較することで、感染したファイルを検出できる可能性があります。現在、IJではこの手法を用いるマルウェアは確認していませんが、今後このような手法を実装したマルウェアが発生することが懸念されます。



※この図では代表的なデータを説明している。実際には、例えばNTFSのメタデータエントリの割り当てマップ (MFT Entry Bitmap) 等、ファイル操作にともなって変更される属性が他にも存在する。

図-13 Windowsでのファイル参照の仕組みとアンチフォレンジック手法

*62 「Backdoor.Prioxerlinf: 偶然ながらこれまでにないステルス性を備えた感染型マルウェア」 (<http://www.symantec.com/connect/ja/blogs/backdoorprioxerinf>)。

*63 システム標準の実行ファイルの正常なハッシュ値を得る方法としては、感染していない端末でそれらを事前に計算しておく方法や、パブリックなハッシュ値のデータベースをダウンロードする方法がある。たとえばNIST (アメリカ国立標準技術研究所) は主要なOSの実行ファイルのハッシュ値を含むデータベースを公開している。"National Software Reference Library" (<http://www.nsl.nist.gov/new.html>)。

■ まとめ

ここでは、マルウェアによるいくつかのアンチフォレンジック手法を紹介しました。解析者がメタデータのみでの解析やファイルの中身のみに頼った解析を避け、多面的な解析を実施することで、どのような手法が用いられたとしてもある程度対処することができます*64。また、ここでは端末内の情報だけで検出する対策方法を説明しましたが、ネットワークに流れている通信に異常なものがないかも合わせて調査すれば、被害を早期に検出できる可能性が高まります。

1.4.3 東日本大震災を取り巻く状況

3月11日に発生した東日本大震災は、発端となった大規模地震と津波、原子力発電所の事故等により、多くの人命と生活基盤が失われる大災害となりました。直接の被災地となった東北地方*65のみならず、東京やその近郊を含めた首都圏*66においても、規模の大小に違いはあるものの、この震災の影響を受け、電気、ガス、水道の生活インフラ、公共交通機関、生活必需品やガソリンを含めた物流等に大きな混乱が発生しました。

ここでは、この震災に関連した活動のうち、インターネットを中心とした通信状況とそれに応じた活動と、連日の災害関連情報に埋もれてしまいがちな援助に関する情報、震災に関連した攻撃について紹介します。

■ 震災後の通信状況

震災発生後には、国内の通信やインターネット上でも平時とは異なる通信の状況が見られました。被災地においては地震そのものや津波によって通信設備や電力設備への被害が発生し、通常の通信が行えなくなる状

況が発生しました。国際間海底ケーブルも被害を受けたことが報道されています*67。また、首都圏においては、震災後の安否確認等で発生する大量の通話に対して、固定電話や携帯電話で一時的に発信規制が実施され、通話ができない状況が発生しました。

このような通信状況においては、メール、mixi、Twitter、Facebook等のサーバに情報を蓄積できる通信手段が安否確認等で有効に機能し、一部企業で社員に対する連絡にTwitterを利用する事例も見られました*68。一方で、SNSが原典を示さない不確実な情報が大量に流布する場となっていたとする指摘も見受けられました*69。

また、震災直後はインターネット上の通信量の減少が見られましたが、地方公共団体や電力会社等の特定のWebサーバに最新情報を求めるアクセスが集中し、一時的にアクセス不能となる状況が発生しました。震災当日に公共交通機関が不通となり、徒歩帰宅を強いられた人も多かったことや、震災発生翌週以降において交通機関の安定運行が困難な状況が見込まれたこと等から、社員の在宅勤務を決断した企業も多く、翌週以降においても平常時とは異なる状況が継続しました。

さらに、震災発生翌週以降には、輪番停電の影響により、非常用電源設備を備えていない建物内のWebサーバ等のITシステムが、たびたび停止する事態が発生しました。震災発生後のこのような状況に関わらず、インターネット上では通常通り複数のインシデントが発生しており、マルウェアの活動とその対策や脆弱性対策等、継続的に実施しなければならない状況にありました。

*64 メモリ上のみで感染活動を行うマルウェアは、再起動すると活動できなくなるが、ディスク上には痕跡を残さないで、これまでに紹介したディスクを解析する手法では検出できない。このようなマルウェアに対しては、メモリ上のデータを解析するメモリフォレンジックと呼ばれる手法が有効になる。

*65 今回の震災による直接の被災地については、The New York Timesの次のまとめに詳しい。"Map of the Damage From the Japanese Earthquake" (<http://www.nytimes.com/packages/flash/newsgraphics/2011/0311-japan-earthquake-map/index.html?ref=europe>)。

*66 ここでは東京都及び東京への通勤圏にあたる埼玉県、千葉県、神奈川県、茨城県、栃木県、群馬県及び山梨県等を示す。この圏内の人口は、国土交通省 首都圏白書 (http://www.mlit.go.jp/hakusyo/syutoken_hakusyo/h22/h22syutoken_files/zenbun.pdf) 第2章 第1節「人口等の状況」によると4292万人にのぼる。

*67 国際間海底ケーブルの損傷については、例えば次のNetwork Worldのような報道がある。"Quake damage to Japan cables greater than thought Service is cut off on two segments of a trans-Pacific network" (<http://www.networkworld.com/news/2011/031411-quake-damage-to-japan-cables.html>)

*68 例えば、日本IBMではIBMグループ社員に対して次のようなアナウンスを出している。「社員向け地震関連情報に関するtwitter活用のお願い」 (<http://www-06.ibm.com/jp/news/2011/03/1402.html>)。

*69 例えば、原発の事故に関連してうがい薬を飲むと放射性物質による影響が軽減するとの情報があったが、独立行政法人 放射線医学総合研究所から注意喚起が発表された。「ヨウ素を含む消毒剤などを飲んではいけません・インターネット等に流れている根拠のない情報に注意」 (<http://www.nirs.go.jp/data/pdf/youso-3.pdf>)。

■ 復興支援と通信状況は正の努力

震災直後においては、被災地に対する支援物資や義援金等の直接的な援助だけではなく、安否確認のための掲示板整備、有償のOSや地図アプリケーション等の無償提供等が複数の企業によって行われました。また、被災地に対するサービス課金免除や、クラウドのサーバ無償提供等も実施されています^{*70}。さらに、適切な情報伝達を行うために通信状況を整理しようとする動きが多数見られました。インターネット上に散在する震災対応に有益な情報を一元的にまとめて提供するサイト^{*71}が登場し、アクセス集中や被災等で情報発信が困難なWebサイトにクラウド環境のサーバを提供したり、コンテンツをミラーしたりする動きがこれにあたります。加えて、正確な情報を多くの人に伝えるために、テレビやラジオを番組をインターネット上で再配信がする動きがありました。

情報発信の方法では、内容に対してサイズが大きくなりがちなファイル形式(PDFやExcel等のアプリケーション形式)での情報配信を止め、テキスト形式やCSV形式に置き換えるか併用することが推奨されました^{*72}。あわせて、政府官公庁関係の公式情報がTwitterやFacebook等のSNSで配信されるようにもなりました^{*73}。一方で、インターネット上で流布する不確かな情報(デマ等)に関する自主削除対応について総務省より要請が出されました^{*74}。

さらに、国外からも被災地に対する災害派遣や、支援物資、義援金等の直接的な援助が実施されました。加えて、特に海外の製品ベンダを中心にして、日本の通信事情に配慮した対応が実施されました。マイクロソフト社は、被災直後に日本のネットワークに負荷をかけないために、米国時間の3月14日に予定していたInternet Explorer 9の公式版のリリースを日本を除いて実施しました^{*75}。また、ISP等多くのネットワーク企業で利用されるルータのベンダであるシスコ社は、被災後の通信維持に注力している日本のISP等に配慮して、年に2回実施しているファームウェアの定期アップデート(米国時間3月23日予定)を半年間延期すると発表しました^{*76}。

■ 震災に関連して発生した攻撃

一方で、この震災に乗じた攻撃も発生しています。まず、震災直後から日本の地震に対するSEOポイズニングや、マルウェア感染に誘導するようなコンテンツによる攻撃が発生しました^{*77}。このためにJapan、Earthquake、Tsunami等の文字列を含むドメインが数多く取得されたことが報告されています。震災の発生当初は、英語による検索キーワードや、被災地の様子の写真や津波の動画等のコンテンツを利用するものが多かったため、日本の状況に興味を持つ日本以外の国の人々を対象とした攻撃であると考えられます^{*78}。また、この種の攻撃は、事件の注目の高さを悪用するものです

*70 企業等による復興支援活動の様子は、例えば次にまとまっている。総務省情報流通行政局情報流通振興課「東日本大震災に係るICT分野での官民の取組の状況」(http://www.soumu.go.jp/main_content/000112455.pdf)。IJでは、被災地への情報発信のためのクラウド環境の無償提供やスケジューラの無償提供、被災地に対する課金措置を行うとともに、被災地の自治体Web等のミラーサイト提供(<http://www.ijj.ad.jp/news/pressrelease/2011/0316.html>)を実施した。

*71 政府としては首相官邸災害対策ページ(<http://www.kantei.go.jp/saigai/>)がある。民間では検索サービスを提供しているGoogle(<http://www.google.co.jp/intl/ja/crisisresponse/japanquake2011.html>)やYahoo!(<http://info.shinsai.yahoo.co.jp/index.html>)等がある。

*72 財団法人地方自治情報センター「国民へ発信する重要情報のファイル形式について」(<https://www.lasdec.or.jp/cms/12.22060.84.html>)。経済産業省でも同様のアナウンスを出している。「東北地方太平洋沖地震に係る情報提供のデータ形式について」(http://www.meti.go.jp/policy/mono_info_service/joho/other/2011/0330.html)。

*73 例えば、Twitterでは首相官邸(災害情報) (@kantei_saigai)、防衛省(災害情報) (@bouei_saigai) や総務省消防庁 (@FDMA_JAPAN) 等の公式アカウントで情報提供を行っている。またFacebookでは首相官邸の公式ページ(<http://www.facebook.com/Japan.PMO>)にて、主に英語で情報発信を行っている。なお、経済産業省では公共機関ソーシャルメディアポータル(<http://smp.openlabs.go.jp/>)を通じ、確認済の政府及び地方自治体のTwitterアカウント一覧や、公共機関がTwitterアカウントを運用する際の指針や手引き等をまとめている。

*74 内閣官房 被災地等における安全・安心の確保対策ワーキングチーム「被災地等における安全・安心の確保対策」(<http://www.cas.go.jp/jp/seisaku/hisaitwiw/honbun.pdf>)を受けて、総務省より「東日本大震災に係るインターネット上の流言飛語への適切な対応に関する電気通信事業者関係団体に対する要請」(http://www.soumu.go.jp/menu_news/s-news/01kiban08_01000023.html)が行われた。この要請により、例えば社団法人テレコムサービス協会では「東日本大震災に係るインターネット上の流言飛語への対応に関する情報提供」(<http://www.telesa.or.jp/taisaku/>)を行っている。

*75 マイクロソフト社「東北地方太平洋沖地震に伴うInternet Explorer (R) 9日本語版の製品版提供の延期について」(<http://www.microsoft.com/japan/presspass/detail.aspx?newsid=3969>)。日本語版のIE9は4/26日より配信が開始された。「Windows (R) Internet Explorer (R) 9日本語版の提供開始」(<http://www.microsoft.com/japan/presspass/detail.aspx?newsid=3995>)。

*76 "Cisco Security Advisories and Notices, March 2011 Bundled Publication Deferred" (http://www.cisco.com/en/US/products/products_security_advisories_listing.html)

*77 震災関連のSEOポイズニングについては、トレンドマイクロ社のセキュリティブログに詳しい。「東北地方太平洋沖地震に便乗したSEOポイズニングを確認。「FAKEAV」へと誘導」(<http://blog.trendmicro.co.jp/archives/3981>)。

*78 Kaspersky Lab社は次のブログで、震災発生後の事件について、国外からの視点で時系列にまとめている。「日本の危機-IT セキュリティを時系列で追う」(<http://www.viruslistjp.com/analysis/?pubid=204792134>)。

が、東日本大震災については震災後1ヵ月を経過した時点でも新しい攻撃が発見されています。

日本国内において日本人を狙った事件としては、震災発生後の1、2週間後から、震災関連のチェーンメール^{*79}や、電話やメールを利用して公的機関等を騙った義援金詐欺や、偽のサイトに誘導するフィッシングが発生し、注意喚起が行われています^{*80}。同じ時期に、震災関連、原子力発電所関連の情報を利用したメールによる標的型攻撃の発生も確認されています^{*81}。

■ まとめ

本稿執筆時点でも余震が継続しており、この震災が今現在も進行中の脅威である中で、関連動向をまとめることは時期尚早かもしれません。しかし、ここで示したように日本のインターネットや通信事情は震災による影響を受けて変化し続けており、依然として安定していない状況にあります。また、震災に便乗した攻撃は今後も継続的に発生する可能性があり、攻撃の発生の事実を知った上で関連情報に継続的に注意していただきたいと思います。

1.5 おわりに

このレポートは、IJ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。今回は新しい観測環境の紹介と、マルウェアによるアンチフォレンジックの解説、そして東日本大震災による日本の通信事情への影響と、それに関連する攻撃について紹介しました。

最後になりましたが、被災者救済活動や復旧と復興に尽力している人々、また国外からの援助協力について、この場をお借りして感謝したいと思います。IJとしても復興に向けた努力を継続してまいります。

執筆者:

齋藤 衛(さいとう まもる)

IJ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後、2001年よりIJグループの緊急対応チームIJ-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とともに、インターネットの安定的な運用に関する協議会、安心ネットづくり促進協議会 児童ポルノ対策作業部会 技術者SWG等複数の団体で活動を行う。

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)

鈴木 博志(1.4.1 dionaeaハニーポット)

春山 敬宏(1.4.2 マルウェアによるアンチフォレンジック)

齋藤 衛(1.4.3 東日本大震災を取り巻く状況)

IJ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、須賀 祐治、小林 直、吉川 弘晃、齋藤 聖悟 IJサービス本部セキュリティ情報統括室

松崎 吉伸 サービス本部 ネットワークサービス部 技術開発課

*79 震災関連の迷惑メールやチェーンメールについては、例えば日本データ通信協会迷惑メール相談センターが注意喚起を行っている (<http://www.dekyo.or.jp/soudan/eq/index.html>)。

*80 例えば消費者庁「震災に関する義捐金詐欺にご注意ください」 (<http://www.caa.go.jp/jisin/110318gienkinsagi.html>) や、フィッシング対策協議会「日本への義援金を騙るフィッシング(2011/3/14)」 (<http://www.antiphishing.jp/news/alert/2011314.html>) 等。

*81 例えば次のIBM社の東京SOCの報告で詳しく解説している。Tokyo SOC Report「東京SOCで検知した最近の標的型攻撃の傾向」 (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/targeted_attack_20110324?lang=ja_jp)。