

マッシュアップコンテンツに起因したマルウェアの大量感染

今回は、2010年10月から12月に発生したインシデントに関する報告とともに、2010年9月に発生した一連のDDoS攻撃の状況、マッシュアップコンテンツによるマルウェア感染事件、ソフトウェア配布パッケージの改ざん事件と、マルウェア対策 研究人材育成ワークショップ 2010 (MWS2010) の模様を報告します。

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2010年10月から12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係る複数の脆弱性が悪用され、携帯端末に関する脆弱性とその悪用が現実の脅威となりました。また、SIPを悪用した金銭被害事件も継続的に発生しています。国際的には大規模なDDoS攻撃が複数件発生しました。さらに、WikiLeaksに代表される内部告発や情報漏えい事件が非常に大きな話題となりました。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

1.2 インシデントサマリー

ここでは、2010年10月から12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。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。

■ 脆弱性

今回対象とした期間では、マイクロソフト社のWindows*2*3*4、Internet Explorer*5、Office製品*6、ア

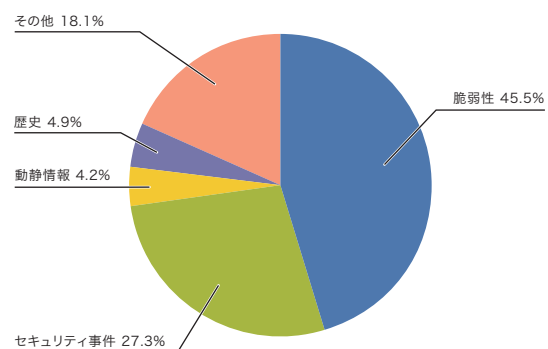


図-1 カテゴリ別比率(2010年10月～12月)

*1 このレポートでは取り扱ったインシデントを、脆弱性、動静情報、歴史、セキュリティ事件、その他の5種類に分類している。

脆弱性: インターネットやユーザの環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェア等の脆弱性への対応を示す。

動静情報: 要人による国際会議や、国際紛争に起因する攻撃等、国内外の情勢や国際的なイベントに関連するインシデントへの対応を示す。

歴史: 歴史上の記念日等で、過去に史実に関連して攻撃が発生した日における注意・警戒、インシデントの検知、対策等の作業を示す。

セキュリティ事件: ワーム等のマルウェアの活性化や、特定サイトへのDDoS攻撃等、突発的に発生したインシデントとその対応を示す。

その他: イベントによるトラフィック集中等、直接セキュリティに関わるものではないインシデントや、セキュリティ関係情報を示す。

*2 マイクロソフト セキュリティ情報MS10-070 - 重要 ASP.NETの脆弱性により、情報漏えいが起こる(2418042) (<http://www.microsoft.com/japan/technet/security/bulletin/MS10-070.mspx>)。

*3 マイクロソフト セキュリティ情報MS10-091 - 緊急 OpenTypeフォント(OTF)ドライバの脆弱性により、リモートでコードが実行される(2296199) (<http://www.microsoft.com/japan/technet/security/bulletin/MS10-091.mspx>)。

*4 マイクロソフト セキュリティ情報MS10-092 - 重要 タスク スケジューラの脆弱性により、特権が昇格される(2305420) (<http://www.microsoft.com/japan/technet/security/bulletin/MS10-092.mspx>)。

*5 マイクロソフト セキュリティ情報MS10-090 - 緊急 Internet Explorer用の累積的なセキュリティ更新プログラム(2416400) (<http://www.microsoft.com/japan/technet/security/bulletin/MS10-090.mspx>)。

*6 マイクロソフト セキュリティ情報MS10-087 - 緊急 Microsoft Officeの脆弱性により、リモートでコードが実行される(2423930) (<http://www.microsoft.com/japan/technet/security/bulletin/MS10-087.mspx>)。

*7 APSP10-28 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/apsb10-28.html>)。

*8 APSP10-26 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/apsb10-26.html>)。

ドビ社のAdobe ReaderとAcrobat^{*7}、Flash Player^{*8}、Shockwave Player^{*9}、アップル社のQuickTime^{*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。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、オラクル社Oracle Database^{*12}、DNSサーバのBIND^{*13}、DHCPサーバであるISC DHCP^{*14}、Adobe Flash Media Server^{**15}、CMS^{*16}として利用されるWordPress^{*17}やMovable Type^{*18}といったブログソフトウェア等のサーバアプリケーションや、UNIX系OSで利用されているglibc^{*19*20}や仮想化ソフトのVMware^{*21}等、影響範囲の広いソフトウェアでも脆弱性が修正されています。加えて、この期間にはアップル社のiOS^{*22}、Android端末のFlash Player^{*23}等、携帯電話等のファームウェアやアプリケーションでも複数の脆弱性が修正されています。

■ 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、ノーベル平和賞の受賞者決定、横浜で開催されたAPEC JAPAN

2010^{*24}、北朝鮮による韓国への砲撃等の動きに注目しましたが、関連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、アクセス解析サービスを経由したマルウェア感染事件が発生しました^{*25*26}。この件の詳細は「1.4.2 マッシュアップコンテンツに起因したマルウェア感染」を参照してください。また、以前から発生しているSIPの不正な通信も引き続き確認^{*27}されており、不正利用に対する注意喚起が行われました^{*28}。TwitterやFacebook等のSNSを悪用し^{*29}、情報を詐取したりマルウェアを感染させようとする試みも続いています^{*30}。さらに、この期間には、ミャンマーでの選挙に

- *9 APSB10-25 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/apsb10-25.html>)。
- *10 QuickTime 7.6.9 のセキュリティコンテンツについて (http://support.apple.com/kb/HT4447?viewlocale=ja_JP)。
- *11 Oracle Corporation, JavaTM SE 6 アップデートリリースノート (<http://java.sun.com/javase/ja/6/webnotes/6u22.html>)。
- *12 Oracle Corporation, Critical Patch Update - October 2010 (http://www.oracle.com/technology/global/jp/security/101015_92/top.html)。
- *13 BIND: cache incorrectly allows a ncache entry and a rrsig for the same type (<http://www.isc.org/software/bind/advisories/cve-2010-3613>)。
- *14 DHCP: Server Hangs with TCP to Failover Peer Port (<http://www.isc.org/software/dhcp/advisories/cve-2010-3616>)。
- *15 APSB10-27 Adobe Flash Media Server用セキュリティアップデート公開 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-27.html>)。
- *16 CMS: Content Management System コンテンツマネジメントシステムの略。Webサイトやポータルサイトに利用されている。
- *17 WordPress 3.0.2 (<http://ja.wordpress.org/2010/12/01/wordpress-3-0-2/>)、WordPress 3.0.3 (<http://ja.wordpress.org/2010/12/09/wordpress-3-0-3/>)、3.0.4 重要なセキュリティアップデート (<http://ja.wordpress.org/2010/12/30/3-0-4-update/>)。
- *18 [重要]セキュリティアップデート Movable Type 5.04および 4.28の提供を開始 (<http://www.sixapart.jp/movabletype/news/2010/12/08-1100.html>)。
- *19 Vulnerability Note VU#537223 GNU C library dynamic linker expands \$ORIGIN in setuid library search path (<http://www.kb.cert.org/vuls/id/537223>)。
- *20 CVE-2010-3856 glibc: ld.so arbitrary DSO loading via LD_AUDIT in setuid/setgid programs (<http://web.nvd.nist.gov/view/vuln/detail?vulnid=CVE-2010-3856>)。
- *21 VMware hosted products and ESX patches resolve multiple security issues (<http://www.vmware.com/security/advisories/VMSA-2010-0018.html>)。
- *22 About the security content of iOS 4.2 (<http://support.apple.com/kb/HT4456>)。
- *23 脚注*8で示したAPSB10-26のセキュリティアップデートにはAndroid端末のFlash Playerも含まれている。
- *24 アジア太平洋経済協力Asia-Pacific Economic Cooperation: APEC (<http://www.mofa.go.jp/mofaj/gaiko/apec/2010/>)。
- *25 JPCERTコーディネーションセンター アクセス解析サービスを使用した Webサイト経由での攻撃に関する注意喚起 (<http://www.jpCERT.or.jp/at/2010/at100028.txt>)。
- *26 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。アフィリエイトによる金銭取得が目的か!? - "mstmp"lib.dll"攻撃続報 (<http://blog.trendmicro.co.jp/archives/3728>)。
- *27 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、攻撃元のIPアドレスやbruteforceに使われたID一覧等。不正なSIP着信 32 (<http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=%C9%D4%C0%B5%A4%CASIP%C3%E5%BF%AE+32>)。
- *28 JPCERTコーディネーションセンター 不適切な設定で Asteriskを利用した場合に発生し得る不正利用に関する注意喚起 (<http://www.jpCERT.or.jp/at/2010/at100032.txt>)。
- *29 これらにはソーシャル・スパムと呼ばれる手法が利用される。ソーシャル・スパムについては次のエフセキュアブログ等が詳しい。ソーシャル・スパム Q&A (<http://blog.f-secure.jp/archives/50501967.html>)。
- *30 例えば、次のMicrosoft Malware Protection Centerのblogで報告されている事例ではビデオへのリンクを装って不正なファイルを実行させる試みが行われていた。It's NOT Koobface! New multi-platform infector (<http://blogs.technet.com/b/mmpc/archive/2010/11/03/its-not-koobface-new-multi-platform-infector.aspx>)。

関連した攻撃^{*31}、WikiLeaks関連^{*32}や米国の年末商戦に関連した攻撃^{*33}等、大規模なDDoS攻撃が複数発生しています。

■ その他

直接インシデントに関係しない動向として、10月にJPゾーンにおけるDNSSEC署名^{*34}、12月にjpゾーンへのDNSSEC導入準備としてルートゾーンにjpゾーンのDSレコードが登録、公開されたこと^{*35}、日本国内におけるDNSSEC利用の基盤準備が進みました。さらに、サービス妨害攻撃への対応等を取りまとめた「サービス妨害攻撃の対策等調査」報告書がIPAから公開されました^{*36}。

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きています。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。

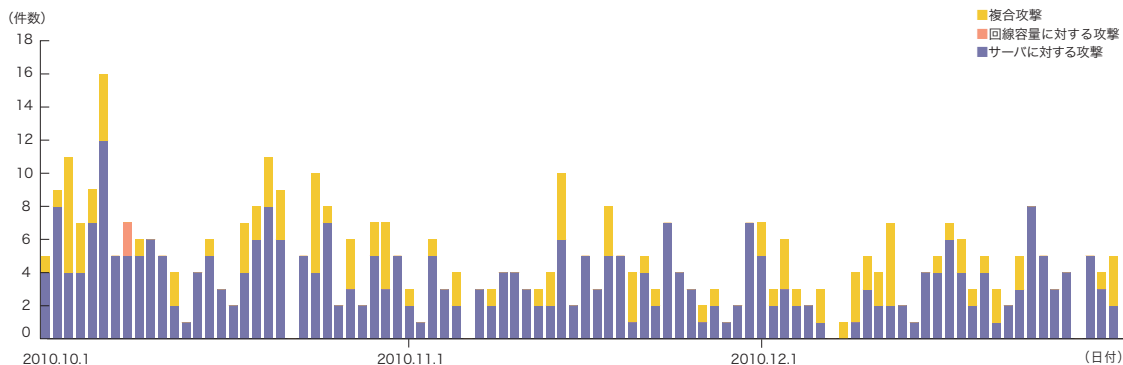


図-2 DDoS攻撃の発生件数

*31 この件に関しては、例えばArbor networks社のTHE ARBOR NETWORK SECURITY BLOG: Attack Severs Burma Internet (<http://asert.arbornetworks.com/2010/11/attac-severs-myanmar-internet/>)に詳しい。

*32 詳細に関しては例えば次のPanda Security社のブログに詳しい。Panda Security Japan ブログ、ザ・シーズン・オブ DDoS (<http://pandajapanblogs.blogspot.com/2010/12/ddos.html>)。

*33 アカマイ、米国ショッピング・シーズン中にDDoS 攻撃から大手小売業者を防御 (http://www.akamai.co.jp/enja/html/about/press/releases/2010/press_jp.html?pr=122110)。

*34 JPゾーンにおけるDNSSEC署名の開始による影響について (<http://jprs.jp/tech/notice/2010-10-15-jp-dnssec.html>)。

*35 ルートゾーンへのjpゾーンのDSレコード登録・公開に伴う影響について (<http://jprs.jp/info/notice/20101210-ds-published.html>)。

*36 IPA(独立行政法人情報処理推進機構)「サービス妨害攻撃の対策等調査」報告書について (<http://www.ipa.go.jp/security/fy22/reports/isec-dos/index.html>)。

*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と呼ばれる、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。

この3ヵ月間でIIJは、430件のDDoS攻撃に対処しました。1日あたりの対処件数は4.67件で、平均発生件数は前回のレポート期間と比べて減少しています。DDoS攻撃全体に占める攻撃手法の割合は、回線容量に対する攻撃が0.5%、サーバに対する攻撃が74.7%、複合攻撃が24.8%でした。

今回の対象期間で観測された最も大規模な攻撃は、サーバに対する攻撃に分類されるもので、最大4万2千ppsの packets によって168Mbpsの通信量を発生させるものでした。また、最も継続時間が長かった攻撃も、この攻撃で、15時間20分にわたりました。攻撃の継続時間については、開始から終了までが30分未満のものが全体の81.9%、30分以上24時間未満のものが18.1%でした。

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^{*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。

■ 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^{*41}によるDDoS 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。

2010年10月から12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。

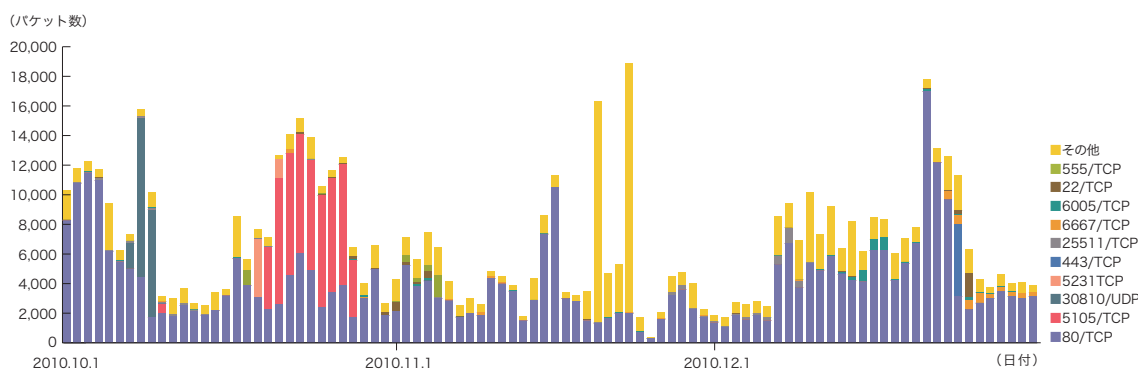


図-3 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

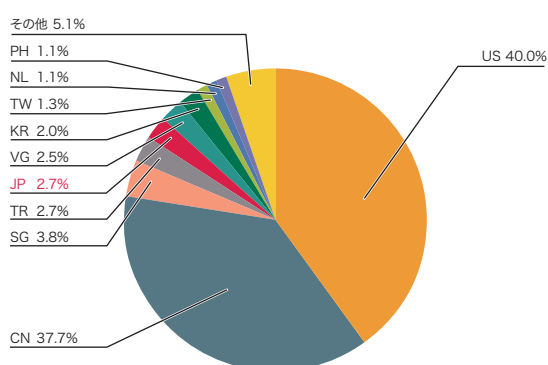


図-4 backscatter観測によるDDoS攻撃対象の分布(国別分類、全期間)

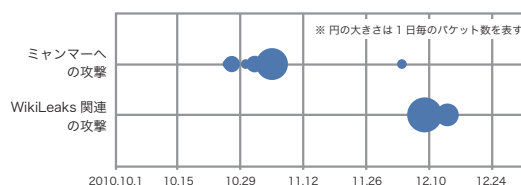


図-5 backscatter観測によるミャンマーへのDDoS攻撃とWikiLeaks関連のDDoS攻撃

*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。

*41 IIJのマルウェア活動観測プロジェクトMITFではハニーポットを設置して、マルウェアの検体取得やインターネットから到着する通信の観測等を実施している。

*42 この観測手法については、本レポートVol.8「1.4.2 DDoS攻撃によるbackscatterの観測」(http://www.iiij.ad.jp/development/iir/pdf/iir_vol08.pdf)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。

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、全期間における全パケット数の58.9%を占めています。また、同じく一般的なサービスで利用される443/TCP、6667/TCP、22/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、米国の40.0%と中国の37.7%が比較的大きな割合を占め、日本国内のIPアドレスも2.7%を占めています。この期間ではミャンマーに対する攻撃と、WikiLeaks関連のDDoS攻撃によると考えられるbackscatterを観測しました(図-5)。ミャンマーへの攻撃によるbackscatterが2010年10月26日から11月5日にかけて断続的に、WikiLeaks関連では、12月9日にはPayPalへの攻撃とWikiLeaks支持者側サイトAnonOps.netへの攻撃が、12月14日にはAmazon.comへの攻撃が、それぞれ観測されました。

1.3.2 マルウェアの活動

ここでは、IJJが実施しているマルウェアの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の試みであると考えられます。

■ 無作為通信の状況

2010年10月から12月の期間中に、ハニーポットに到着した通信の総量(到着パケット数)の推移を図-6に、その発信元IPアドレスの国別分類を図-7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。

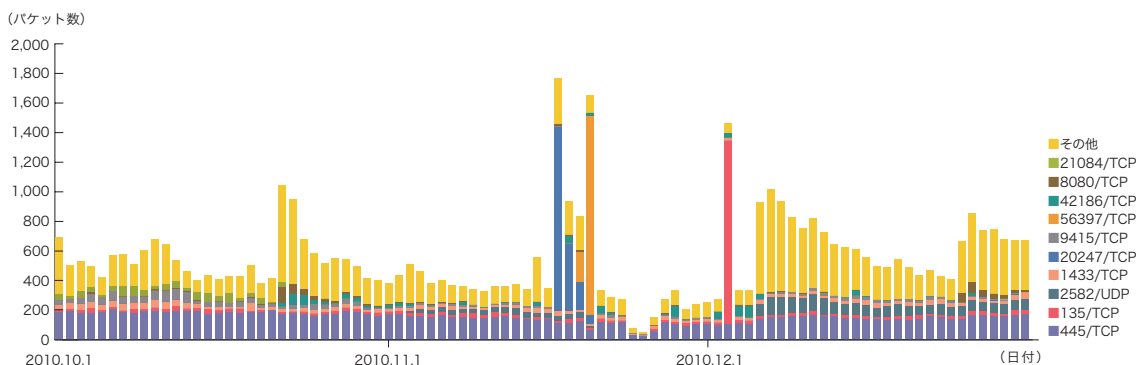


図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

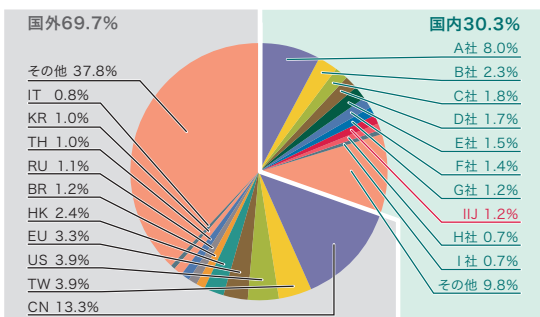


図-7 発信元の分布(国別分類、全期間)

*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て、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、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、proxyで利用される8080/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、20247/TCP、9415/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-7の発信元の国別分類を見ると、日本国内の30.3%、中国の13.3%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-8に、マルウェアの検体取得元の分布を図-9にそれぞれ示します。図-8では、1日あたりに取得した検体^{*45}の総数を総取得検体数、検体の種類をハッシュ値^{*46}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190、ユニーク検体数が30でした。前回の集計期間での平均値が総取得検体数で371、ユニーク検体数で41でした。今回は、総取得検体数、ユニーク検体数ともに減少しています。これは、Sdbotとその亜種の活動が2010年9月末から全く見られなくなったことによります。

図-9に示す検体取得元の分布では、日本国内が19.4%、国外が80.6%でした。なお、台湾が40.9%と前回や前々回に続いて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56.8%、ポット型40.1%、ダウンロード型3.1%でした。また、解析により、25個のポットネットC&Cサーバ^{*47}と29個のマルウェア

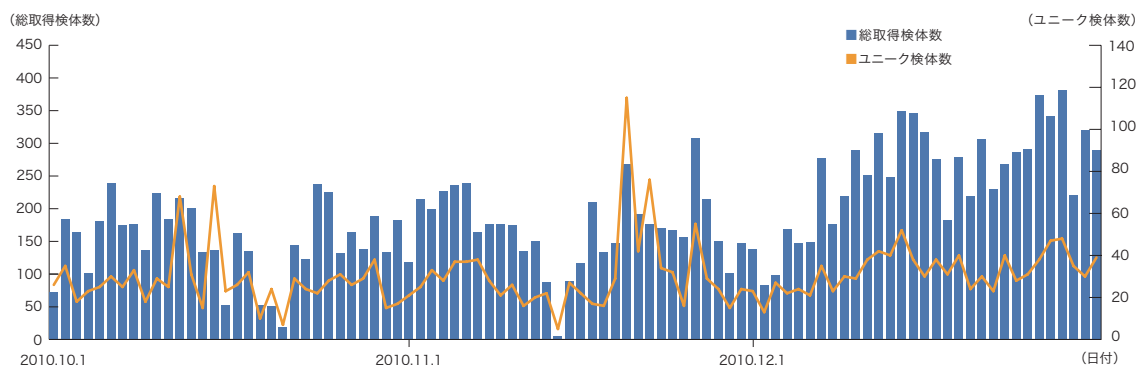


図-8 取得検体数の推移(総数、ユニーク検体数)

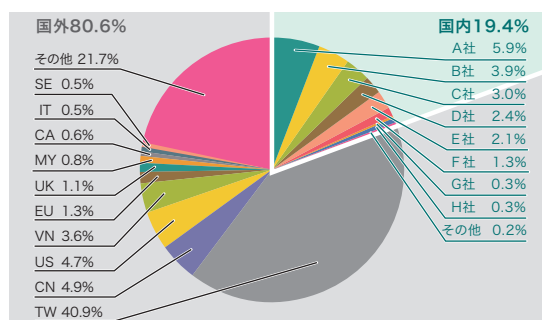


図-9 検体取得元の分布(国別分類、全期間)

*45 ここでは、ハニーポット等で取得したマルウェアを指す。

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

*47 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。

ア配布サイトの存在を確認しました。マルウェア配布サイト数が前回のレポートに比べて減少しています。これは、従来見られていた複数の配布サイトにアクセスする検体が減少したためです。

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^{*48}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になった攻撃です。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。

2010年10月から12月までに検知した、Webサーバに対するSQLインジェクション攻撃の推移を図-10に、攻撃の発信元の分布を図-11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、中国45.4%、日本26.4%、韓国16.4%の順で、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状況は前回からあまり変化が見受けられませんでした。全体に占める中国と韓国からの攻撃の割合が増加していますが、これは10月6日から7日にかけて主に中国や韓国から特定の宛先への大規模な攻撃があったためです。

ここまで示したとおり、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。

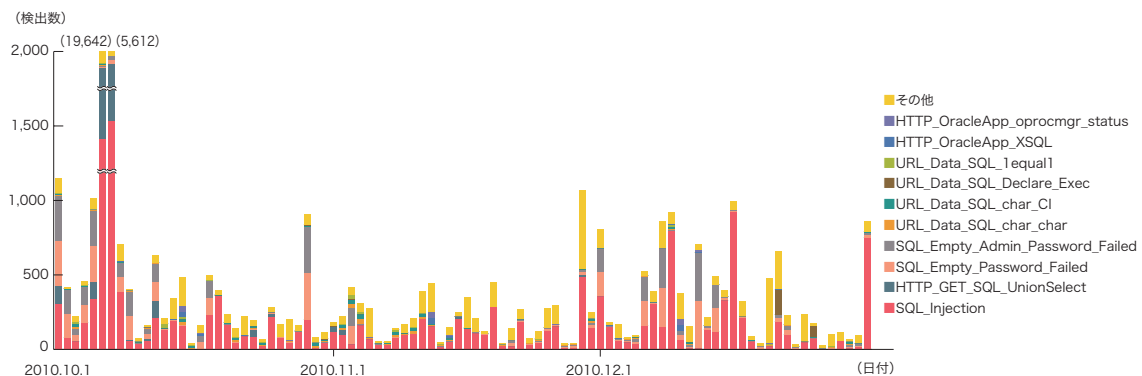


図-10 SQLインジェクション攻撃の推移(日別、攻撃種類別)

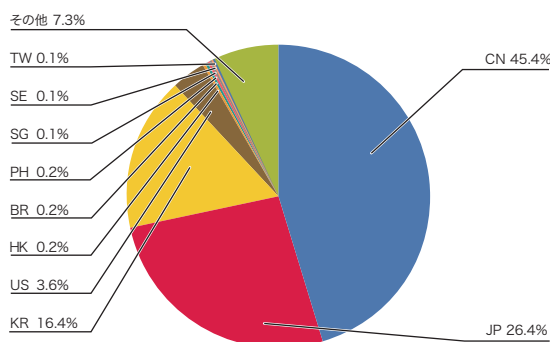


図-11 SQLインジェクション攻撃の発生元の分布(国別分類、全期間)

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

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、2010年9月に発生した大規模DDoS攻撃の概要、マッシュアップコンテンツに起因したマルウェア感染、ソフトウェア配布パッケージの改ざん事件と、10月に行われたマルウェア対策研究人材育成ワークショップ2010の模様を紹介します。

1.4.1 2010年9月に発生した大規模DDoS攻撃の概要

2010年9月から10月にかけて発生したDDoS攻撃は、尖閣諸島沖での海保巡視船と中国船舶の衝突事件に端を発しました。この攻撃は、攻撃の対象や期間が事前にWeb等で予告され、報道等でも取り上げられました。しかし、実際にどのような形でどの程度の攻撃があったかについては、これまで公表されていません。ここでは、この一連の攻撃について、IIJが把握した情報を示します。

■ 攻撃の発生状況

今回の攻撃の発生状況を表-1に示します。9月10日に検出された最初の攻撃以降、さまざまなWebサイトに対して毎日何らかの攻撃が観測されています。その多くはサーバに対する攻撃に分類されるconnection

floodですが、回線容量に対する攻撃に分類されるUDP/ICMP floodも発生しています。IIJが観測した最大規模の攻撃は、サーバに対する攻撃では同時接続数が550万件以上のconnection flood、回線容量に対する攻撃では1.4Gbpsを超えるUDP/ICMP floodでした。また、継続時間については、同一Webサイトで最長291時間となっていました。攻撃の通信は、中国からの直接流入に加えて、中国以外の国や国内他社ISPからの流入も見られ、proxyサーバを悪用した踏み台やボットネットが利用されていたと考えられます。さらに、件数は少ないものの、データの改ざんを狙ったと考えられるSQLインジェクション攻撃や、FTPサーバに対するパスワード総当たり攻撃も発生しました。

■ 攻撃先の遷移

今回の一連の攻撃の特徴として、事前予告されていないWebサイトへの攻撃の波及が挙げられます。特に、攻撃期間の後半には、攻撃先一覧に掲載されているWebサイトからリンクされているサイトにも攻撃が行われました。このようなリンク先のWebサイトは、攻撃対象であったWebサイトを運営する組織とは異なる組織によって運営されているサーバであり、攻撃を受ける理由が把握しづらい状況でした。また、小規模なWebサイトでは、DDoS攻撃に対する準備を行っていないサーバを使用していたこともあり、適切な対策が実施されていない状況も見受けられました^{*50}。

表-1 一連の攻撃の様子

日本	9/10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	10/1	2	3	4	
中国	9/10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	10/1	2	3	4	
IIJ 観測	●	●●●		●	●	●●	●●	●●●	●●●	●●●	●	●	●●	●●	●●	●●	●●	●●	●●	●●	●●	●●		●	●	●
Back scatter 観測					■			●●	●●	●●		●	■	●●	●●							■				
他社 報道等						●	●	●	■						●											

凡例

- ：政府官公庁関係/サーバに対する攻撃
- ：政府官公庁関係/回線容量に対する攻撃
- ：政府官公庁関係/攻撃種別不明
- ▲：教育関係/サーバに対する攻撃
- ：一般企業・団体等/サーバに対する攻撃
- ：一般企業・団体等/攻撃種別不明

特定のサイトに攻撃が発生した日にマークしている。1つのサイトに1日で複数攻撃が発生していてもマークは一つ。複合攻撃の場合でも、先に見られた攻撃種別により分類している。「IIJ観測」はIIJが対処した顧客に対する攻撃を示す。「backscatter観測」はIPアドレスを詐称された他者に対する攻撃を示す^{*49}。「他社報道等」は外部情報によるもの。なお、日付の赤字はそれぞれの国における休日(土日や祝祭日等)を示す。

*49 backscatter観測で取得できる情報の範囲とその意味については本レポートVol.8「1.4.2 DDoS攻撃によるbackscatterの観測」(http://www.iij.ad.jp/development/iir/pdf/iir_vol08.pdf)を参照のこと。

*50 小規模なサーバのDDoS攻撃からの防御については本レポートVol.9「1.4.1 小規模システムでのDDoS攻撃への備え」(http://www.iij.ad.jp/development/iir/pdf/iir_vol09.pdf)を参照のこと。

■ 攻撃の影響

実際に2010年9月に攻撃は発生しましたが、その多くはDDoS対策サービス等で適切に対処されたため、被害は少なく、大きな話題にはなりませんでしたが、このような事件では、他サイトの状況を知ることで、攻撃が自サイトへ波及する可能性を考慮し、それに備えることが可能になります。IJでは、今回発生したような攻撃の概要を紹介するとともに、業界団体を通じて他社ISP等との連携を深め、このような事例を収集する仕組みの構築を推進していきます。

1.4.2 マッシュアップコンテンツに起因したマルウェア感染

2010年9月末から11月にかけて、アクセス解析サービスを提供するサーバが断続的に改ざんされ、悪意のあるサイトへ誘導するスクリプトが埋め込まれました^{*51}。このため、このサービスを導入しているサイト(複数の有名サイトを含む)を閲覧したユーザがドライブバイダ

ウンロード^{*52}によってmstmpと呼ばれるマルウェアに感染し、被害が広がりました^{*53}。

■ 事件の特徴

この事件の特徴は、いわゆるマッシュアップ(複数のサイトからのコンテンツを連結し、1つのコンテンツに見せる手法)で作成されたコンテンツの一部が悪用されたことです。現在、さまざまなWebサービスでAPIが公開され、それを通じてサイト間でデータを連携できるようになっています。一般の利用者が日常的に参照するポータルサイト、検索エンジン、ニュースサイト等もマッシュアップを行っていることが多く、複数サイトからのコンテンツが連結されてWebブラウザに表示されています。このため、マッシュアップに利用されているコンテンツが1つでも改ざんされると、そのコンテンツを利用しているWebサイトを閲覧しただけで、マルウェアに感染してしまう可能性が生じます(図-12)。

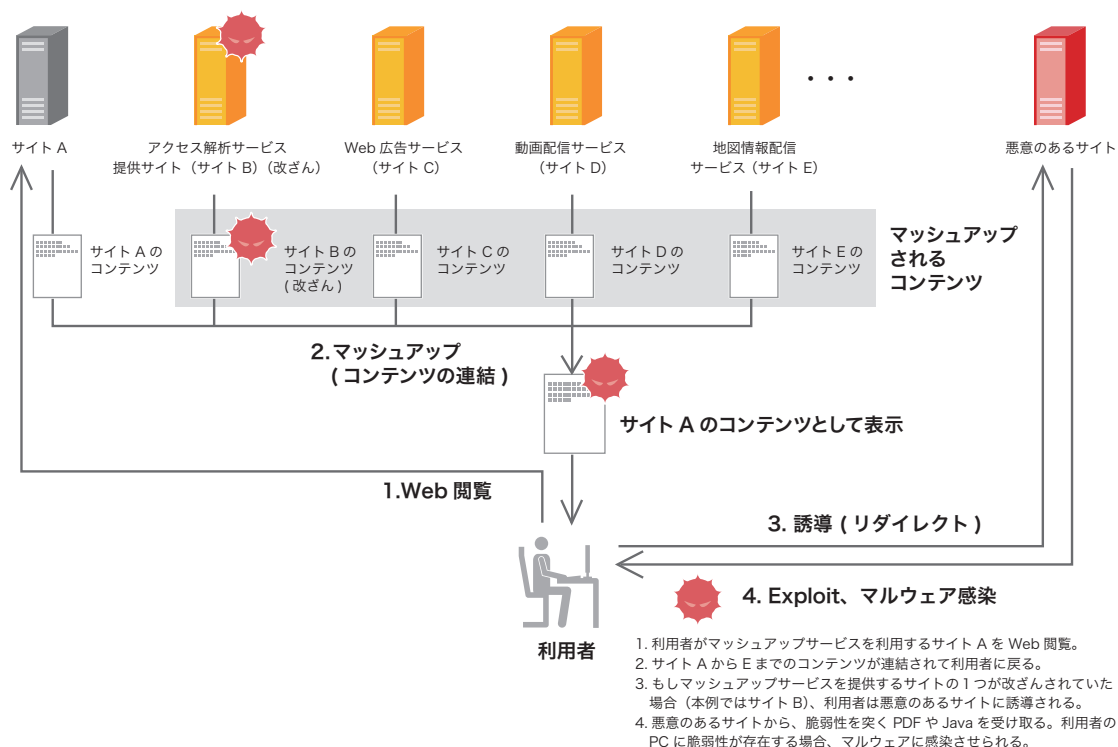


図-12 マッシュアップコンテンツに起因したマルウェア感染

*51 JPCERTコーディネーションセンター アクセス解析サービスを使用した Web サイト経由での攻撃に関する注意喚起 (<http://www.jpcert.or.jp/at/2010/at100028.txt>)

*52 ドライブバイダウンロードとは、ブラウザの脆弱性等を悪用し、Webコンテンツの閲覧者に気付かれないようにマルウェアに感染させる手段のこと。

*53 インストールされたマルウェアのファイル名がmstmpだったことから、報道等でもmstmpという名で扱われることが多い。次のブログでは、国内で少なくとも100社以上が感染被害を受けたことが伝えられている。トレンドマイクロ セキュリティブログ: 国内100社以上で感染被害を確認。"mstmp" "lib.dll" のファイル名で拡散する不正プログラム (<http://blog.trendmicro.co.jp/archives/3723>)。

攻撃者にとって、この手法は非常に効果のあるものになります。一昨年のGumblar事件^{*54}では、大手サイトに広告を出していたWebサイトが改ざんされたことで被害が拡大しました。また、大手広告サイトの改ざんによって、その広告を掲載していたサイトを閲覧したユーザーがマルウェアに感染する事件も複数発生しています^{*55}。今回の事件においても、感染者数が短時間のうちに急激に増加したと報告されています^{*56}。攻撃者は、良く利用されるマッシュアップコンテンツの1つを改ざんするだけで、それを利用するすべてのサイトを改ざんしたときと同等の効果を得ます。このことから、意図的にこのサービスを狙ったことが推測できます。

また、アクセス解析サービスを利用していたサイトは、マルウェア配布を意図した悪性サイトではなく、一般のサイトでした。このため、このサイトをブラックリスト等でフィルタリングすることが困難であったことも、被害が拡大した要因と考えられます。

■ マルウェアの感染とその動き

マルウェアの感染原因は、Webブラウザやそのプラグインの脆弱性を攻撃する悪意のあるサイトにユーザが誘導されたためです。IJでは、表-2に示す脆弱性が悪用されたことを確認しています。図-13に、マルウェア

感染後の挙動を示します。脆弱性の悪用に成功すると、まず「1.1234567890123456.swf」のような数字とピリオドの後に16桁の数字が続く、拡張子.swfのファイルが生成されます。実際には、このファイルの中身はDLLで、mstmpを生成して実行するためのプログラムです。mstmpはWebブラウザのプラグインとして動作し、外部サーバからさらにlib.dll等のマルウェアをダウンロードして、Webブラウザのプラグインとしてインストールします。また、IJでは、「Security tool」というスケアウェア^{*57}とともに、FTPアカウントを盗みだすマルウェアがインストールされ、そのアカウントを悪用して感染者が管理しているWebサイトも改ざんされるという、いわゆるGumblarスキームを持つ事例があったことも確認しています。

■ 対策に向けて

参照したWebサイトを経由したマルウェア感染や、フィルタリングが困難な状況が起こる可能性を認識して、常日頃からブラウザ等のパッチ適用^{*58}を迅速に行うことが一番の対策になります。特にJavaの脆弱性を突いた攻撃が急激に増加しているとも報じられているため^{*59}、近年狙われ続けているアドビ社の製品群と併せて早急な対処が重要です。また、事件が発生した後にファイアウォールやIPS等のログをさかのぼって調査で

表-2 mstmpで悪用された脆弱性

ソフトウェア	バージョン	脆弱性
MDAC	-	MS06-014
HCP (Help and Support Center)	-	MS10-042
Adobe Reader / Acrobat	< 9.4.0	CVE-2010-3631
Java (JRE)	< 1.6.19	CVE-2010-0094
	< 1.6.19	CVE-2010-0840
	< 1.6.20	CVE-2010-0886

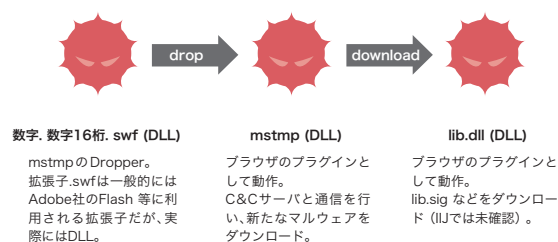


図-13 mstmp感染後のマルウェアの変遷

*54 GumblarやGumblarスキームを持つru:8080に関するレポートは、過去のIIRでたびたび取り上げている。Vol.4 1.4.2 ID・パスワード等を盗むマルウェアGumblar (http://www.ij.ad.jp/development/iir/pdf/iir_vol04.pdf)、Vol.6 1.4.1 Gumblar の再流行 (http://www.ij.ad.jp/development/iir/pdf/iir_vol06.pdf)、Vol.7 1.4.1 Gumblar型の攻撃スキームを持つru:8080 (http://www.ij.ad.jp/development/iir/pdf/iir_vol07.pdf)。

*55 この事件については次のトレンドマイクロ株式会社のブログでも紹介されている。Adobe製品へのゼロデイ攻撃、広告配信システムを通じた「Webからの脅威」・2010年9月の脅威動向を振り返る (<http://blog.trendmicro.co.jp/archives/3700>)。

*56 IBM社の東京SOCでは、数回にわたって急激にマルウェア感染者が増加したのを検知し、紹介している。Tokyo SOC Reprotドライブ・バイ・ダウンロード攻撃で感染する「mstmp」ウイルスについて (https://www-950.ibm.com/blogs/tokyo-soc/entry/dbyd_mstmp_20101027?lang=ja)。

*57 スケアウェアとは、セキュリティソフトウェア等を装い、存在しない警告を発することでユーザを脅して金銭を詐取る脅威。スケアウェアについては本レポートVol.3「1.4.3 スケアウェア」(http://www.ij.ad.jp/development/iir/pdf/iir_vol03.pdf)を参照のこと。

*58 Windows Updateはもちろんのこと、例えばJava (JDK、JRE) やAdobe Reader/Acrobat、Adobe Flash、Apple QuickTime等のブラウザプラグインについても最新版に保つことが必要である。

*59 Javaの脆弱性を突くExploitが急増したとの情報は次のMicrosoft Malware Protection Centerのblogなどで報告されている。Have you checked the Java? (<http://blogs.technet.com/b/mmpc/archive/2010/10/13/have-you-checked-the-java.aspx>)。

きる仕組みや、定期的にログを調査したり解析したりして異常を見つけ出すための仕組みを持つことも役立ちます。

1.4.3 ソフトウェア配布パッケージの改ざん

2010年11月28日から12月2日にかけて、トロイの木馬^{*60}が混入したProFTPD^{*61}のソースコードパッケージが配布されていました^{*62}。これは、公式のサーバが不正に侵入されてファイルが改ざんされたために発生した事件です。このようなソフトウェア配布パッケージの改ざん事件は、今回のものが初めてではありません。1999年にTCP Wrappers^{*63}、2002年にOpenSSH^{*64}とSendmail^{*65}がそれぞれ改ざんされ、トロイの木馬が混入したパッケージが配布されるという同様の事件がありました。ここでは、ソフトウェア配布パッケージの改ざんと、その検出方法の仕組みについて解説します。

■ ProFTPDの配布パッケージ改ざん

今回侵入されたサーバは、一次配布用FTPサーバとミラーサーバ用同期サーバの2つの役割を兼ねていました。このため、改ざんされたソースコードパッケージが、該当期間に同期した複数ミラーサーバに配布され、広く利用者が取得可能な状態にありました。混入されたトロイの木馬の動作は、ビルドされたバイナリファイルにリモートシェルを取得するバックドアを組み込み、ソースコードからのビルド時にその事実を特定のIPアドレスに通知するものでした。

ProFTPDでは、2010年10月29日に深刻な脆弱性^{*66}が公表され、同日に対策済みのバージョンが公開されました。この脆弱性には設定等による回避策が存在せず、2010年11月7日の時点で概念実証コードが公開

され^{*67}、旧バージョンを使用し続けることが非常に危険な状態でした。今回改ざんの対象として狙われたものは、この脆弱性に対策済みのバージョンであり、バージョンアップを目的とした取得が多く見込まれるパッケージでした。しかし、改ざんされたパッケージは、正規のそれと比較したときに、ハッシュ値^{*68}や電子署名^{*69}による検証結果はもちろん、容易に改ざん可能なパッケージ内部のファイルの時刻情報や所有者情報に至るまで、正規の情報と異なっていました。

■ パッケージ改ざん検出の必要性

広く使われているオープンソースソフトウェアでは、そのほとんどが有志によるミラーサーバで世界中に配布されています。このようなミラーサーバが存在することで、一次配布元のネットワークやサーバの負荷が軽減され、ユーザによる取得の際にネットワーク上の遅延が低減される等、さまざまな恩恵が生じています。しかし、それぞれのミラーサーバでの管理体制やシステム構成等は千差万別であり、一次配布元でなくミラーサーバが狙われて侵入されると、そのミラーサーバで配布しているパッケージが改ざんされてしまう可能性があります。また、本来の配布元とはまったく関係のない配布元から偽パッケージを受け取ってしまうことも考えられます。

このため、取得元を問わず、配布パッケージの取得後には改ざんの検知を行うことが重要です。多くの場合、配布パッケージの一次配布元から、改ざん検出のためのハッシュ値や電子署名が提供されています。今回の事件でも、パッケージをダウンロードした利用者が改ざんの有無を適切に検証すれば、被害を受けることはありませんでした。

*60 正規のソフトウェアを偽ったり、一部として混入されることでシステムに入り込むマルウェアの一種。導入後、特定の条件(経過時間や入出力等)を満たした時点で悪性活動を行う。情報の漏洩、システムの破壊、アクセス権限の奪取を目的とする場合が多い。

*61 FTPサーバソフトウェアの一つ。The ProFTPD Project (<http://www.proftpd.org/>)。

*62 この事件に関しては次のProFTPDのホームページで報告されている。ftp.proftpd.org compromised (<http://forums.proftpd.org/smf/index.php?topic=5206.0>)。

*63 CA-1999-01: Trojan horse version of TCP Wrappers (<http://www.cert.org/advisories/CA-1999-01.html>)。

*64 CA-2002-24: Trojan Horse OpenSSH Distribution (<http://www.cert.org/advisories/CA-2002-24.html>)。

*65 CA-2002-28: Trojan Horse Sendmail Distribution (<http://www.cert.org/advisories/CA-2002-28.html>)。

*66 CVE-2010-4221: Telnet IAC processing stack overflow (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4221>)。

*67 Full Disclosure: ProFTPD IAC Remote Root Exploit. (<http://seclists.org/fulldisclosure/2010/Nov/49>)。

*68 よく使われるハッシュアルゴリズムとしてMD5 (Message Digest 5)やSHA-1 (Secure Hash Algorithm 1) 等がある。

*69 例えば公開鍵暗号を利用した電子署名に対応したソフトウェアとしてGnuPG (<http://www.gnupg.org/>) がある。

■ ハッシュ値を用いた改ざん検出

ハッシュ値を用いた改ざん検出の例を図-14に示します。ダウンロードしたパッケージとハッシュ値を比較することで、改ざんの有無が検出できます。しかし、ハッシュ値は簡単に生成できるため、パッケージが改ざんされている場合、ともに配布されているハッシュ値も改ざんされている可能性があります。このため、改ざん検出にハッシュ値を用いるときには、パッケージの取得元とは異なる情報源、例えば一次配布元が運営するWebサーバ等から、ハッシュ値を取得して比較する必要があります。

また、多くの配布パッケージでは、MD5アルゴリズムによって算出されたハッシュ値が提供されています。しかし、MD5アルゴリズムはすでに危殆化しているため、改ざん検出に用いることが危険な状態です。2007年11月30日の時点で同一のハッシュ値を持ちながら、内容の意味が異なるファイルを作成するデモが公開され、MD5アルゴリズムの危殆化が理論上のみでないことが証明されています*70。このため、今回のようなずさんな改ざんは検出できますが、通常利用する検出手法としてはハッシュ値を用いた改ざん検出は不十分です。

■ 電子署名を用いた改ざん検出

電子署名を用いた改ざん検出の例を図-15に示します。電子署名では、生成のために秘密鍵、検証のために公開鍵がそれぞれ必要であり、整合性を保ったままの改ざんは非常に困難です。このため、パッケージとともに配布されている電子署名を用いることで改ざんを検出できます。ただし、注意しなければならない点は、改ざん者自身が別の鍵を生成し、それを使って改ざんしたパッケージに署名することで、整合性が保たれた別の電子署名が生成できる点です。この場合、改ざん者の公開鍵もパッケージとともに配布されていると推測されます。

未知の公開鍵を使用する場合には、鍵の入手元とは異なる情報源から鍵のフィンガープリント*71を取得し、その鍵が信頼できる正しい公開鍵であることを照合する必要があります。初回は公開鍵の正当性調査が必要になるため、ハッシュ値を用いた検出に比べて若干手間がかかります。ただし、電子署名を用いた検出の信頼性は、正当な秘密鍵と公開鍵の組に基づいています。改ざん者の公開鍵を使ってしまっただけでは意味がないため、未知の公開鍵はむやみに信用せず、信頼できる正しい公開鍵を事前に保持しておくようにします。

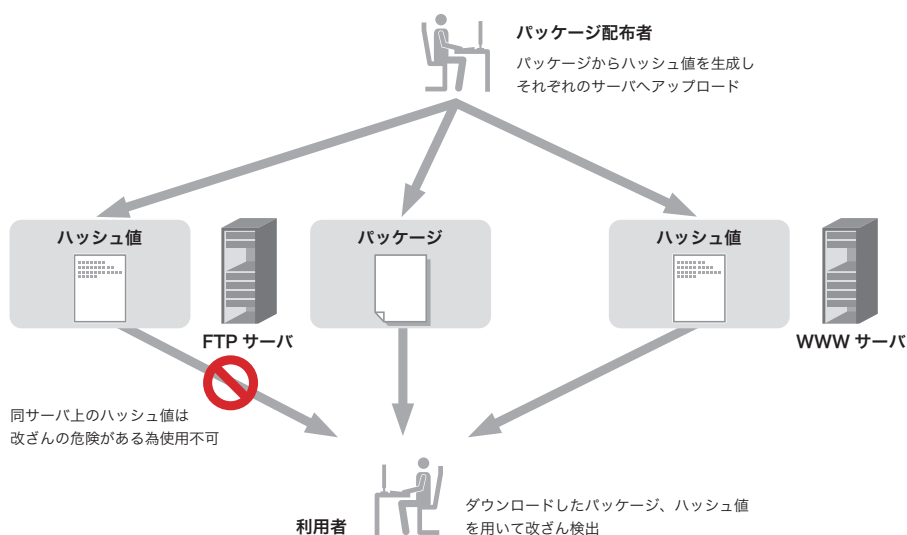


図-14 ハッシュ値を用いた改ざん検出の例

*70 Predicting the winner of the 2008 US Presidential Elections using a Sony PlayStation 3 (<http://www.win.tue.nl/hashclash/Nostradamus/>). 暗号アルゴリズムの危殆化については、本レポートVol.8「1.4.1 暗号アルゴリズムの2010年問題の動向」(http://www.iiij.ad.jp/development/iir/pdf/iir_vol08.pdf)を参照のこと。

*71 公開鍵暗号方式における公開鍵に対するハッシュ値。

■ 配布パッケージの自動検証

バイナリファイルの配布でも類似の対策が採られています。レッドハット社のLinuxディストリビューションRHEL (Red Hat Enterprise Linux) で使用されているRPM (Redhat Package Manager) 形式のパッケージや、マイクロソフト社のWindowsでは、電子署名が組み込まれ、自動的に検証したり、利用者が配布者を識別することができるようになっています。

■ まとめ

ここでは、ProFTPド配布パッケージの改ざん事件の概要と、改ざんされたパッケージの検出手法について説明しました。脆弱性対策のために行うアップデートで、自発的にトロイの木馬をインストールすることになってしまっは意味がありません。いったん侵入を許してしまうと、その原因を取り除いたとしても安全の確保は非常に困難です。このため、パッケージ導入時には手間を惜しまずに改ざんの検出を実施すべきです。

1.4.4 マルウェア対策研究人材育成ワークショップ 2010

2010年10月19日から21日の3日間にわたって、マルウェア対策研究人材育成ワークショップ2010 (MWS2010)^{*72}が開催されました。サイバークリーンセンター^{*73}運営委員会と情報処理学会が主催するこのワークショップは、共通の研究用データセットを用いてマルウェア対策研究の成果を共有する場として2008年に始まりました^{*74}。

研究対象となるデータセットには、サイバークリーンセンターによるネットワーク感染型マルウェアの観測データを元にしたCCC DATASET 2010が用いられ、昨年までと比較してデータ個数や対象期間の面がさらに充実しました。また、研究者コミュニティから提供された、マルウェア検体動作記録データとWeb感染型マルウェアデータセットが加わり、解析対象の種類の間でも大幅に拡充されました。

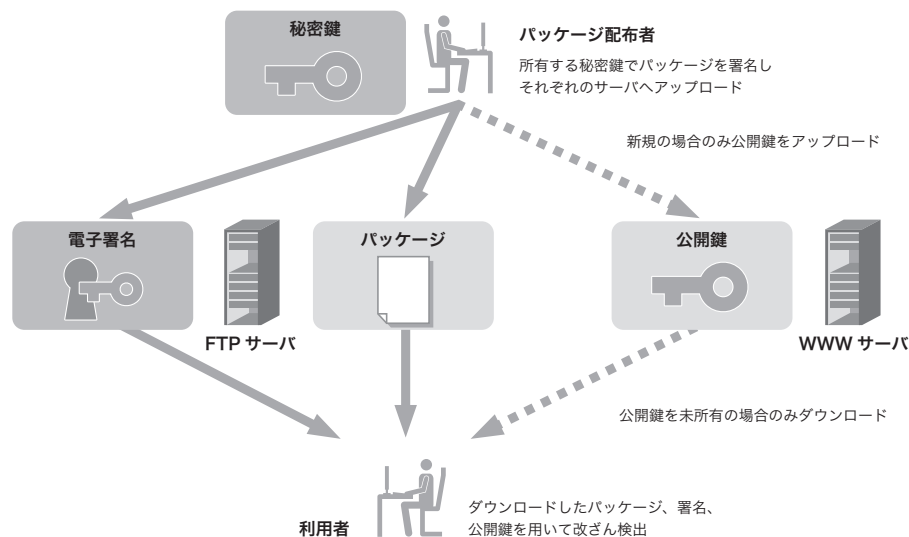


図-15 電子署名を用いた改ざん検出の例

*72 マルウェア対策研究人材育成ワークショップ 2010 (<http://www.iwsec.org/mws/2010/>)。情報処理学会コンピュータセキュリティ研究会によるコンピュータセキュリティシンポジウム2010と合同開催 (<http://www.iwsec.org/css/2010/>)。

*73 サイバークリーンセンターは総務省、経済産業省および各関連団体によるポット対策プロジェクト (<https://www.ccc.go.jp/ccc/index.html>)。

*74 昨年の模様は本レポートVol.5「インターネットトピック：マルウェア対策研究人材育成ワークショップ2009について」(http://www.ij.ad.jp/development/iir/pdf/iir_vol05_topic.pdf)を参照のこと。

■ 研究発表

MWS2010では、22件の口頭発表がありました^{*75}。ここでは、IPアドレスやURLと、これらに付随する属性情報(DNS情報やwhois情報等)から、統計処理によって一般ホストと悪性ホストを特徴づける試みが複数発表されました。また、マルウェアを効果的に解析するための研究として、VMM(Virtual Machine Monitor: 仮想計算機モニタ)やエミュレータの開発や改良による対策手法等、さまざまな視点からの研究発表もありました。他にも、攻撃に関する情報を可視化する手法、未知のマルウェアを検知するための手法、攻撃やマルウェアの分類法、ネットワーク上の距離に基づいてマルウェア活動を分析した結果等、多岐にわたる研究が発表され、活発な議論が行われました。

IJからは、MWS2008、MWS2009に引き続き、MITFのハニーポット網による観測データと、研究用データセットのうちCCC DATASET 2010の攻撃元データを比較し、その差異とこれまでの変化をまとめた結果を発表しました。さらに、一方の観測網で発見された攻撃元アドレスをネットワーク上でフィルタする対策を想定し、フィルタの広さやフィルタ適用までのタイムラグと、防御の成功率の関係をシミュレーションにより求めた結果も発表しました。

■ MWS Cup 2010

昨年と同様に、課題の通信データを規定時間内に解析し、その技術を競うMWS Cup 2010も開催されました。6つの学生チームを含む8チームが競技に参加し、それぞれ持参した解析環境で技術と正確性を競いまし

た。IJも新規開発の解析ツールを持ち込んで参加しました。しかし、学生チームの活躍に敵わず、1位である総合優勝は獲得できませんでしたが、総合2位と技術部門優勝を得ることができました。

マルウェア対策研究人材育成ワークショップでは、最近のマルウェア動向を反映したデータセットと、それに基づく研究成果が共有されます。IJにとっても、通常の業務では交流する機会が少ない学術界の方々と、インターネットをとりまく現在の脅威やその対策について意見交換できる有益な場であり、今後も積極的に参加し協力していきたいと考えています。

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、2010年9月に発生したDDoS攻撃、マッシュアップコンテンツに起因したマルウェア感染、ソフトウェア配布パッケージの改ざん事件について解説しました。また、マルウェア解析の研究発表の場であるMWS2010の様相を紹介しました。

IJ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きます。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、Webで感染するマルウェア対策コミュニティ等、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、IPAサービス妨害攻撃対策検討会等、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)

齋藤 衛 吉川 弘晃 (1.4.1 2010年9月の大規模DDoS攻撃)

鈴木 博志 (1.4.2 mstmp:マッシュアップコンテンツに起因したマルウェアの大量感染)

小林 直 (1.4.3 ソフトウェア配布パッケージの改ざん)

永尾 禎啓 (1.4.4 マルウェア対策研究人材育成ワークショップ2010)

IJ サービス本部 セキュリティ情報統括室

協力:

加藤 雅彦 須賀 祐治 春山 敬宏 齋藤 聖悟 IJ サービス本部 セキュリティ情報統括室

*75 詳細については、次のURLに公開されている論文や発表資料を参照。写真で振り返る MWS 2010 (<http://www.iwsec.org/mws/2010/photo.html>)。