# Internet Infrastructure Review

IIJ
Internet Initiative Japan

Vol.10

February
2011

インフラストラクチャセキュリティ

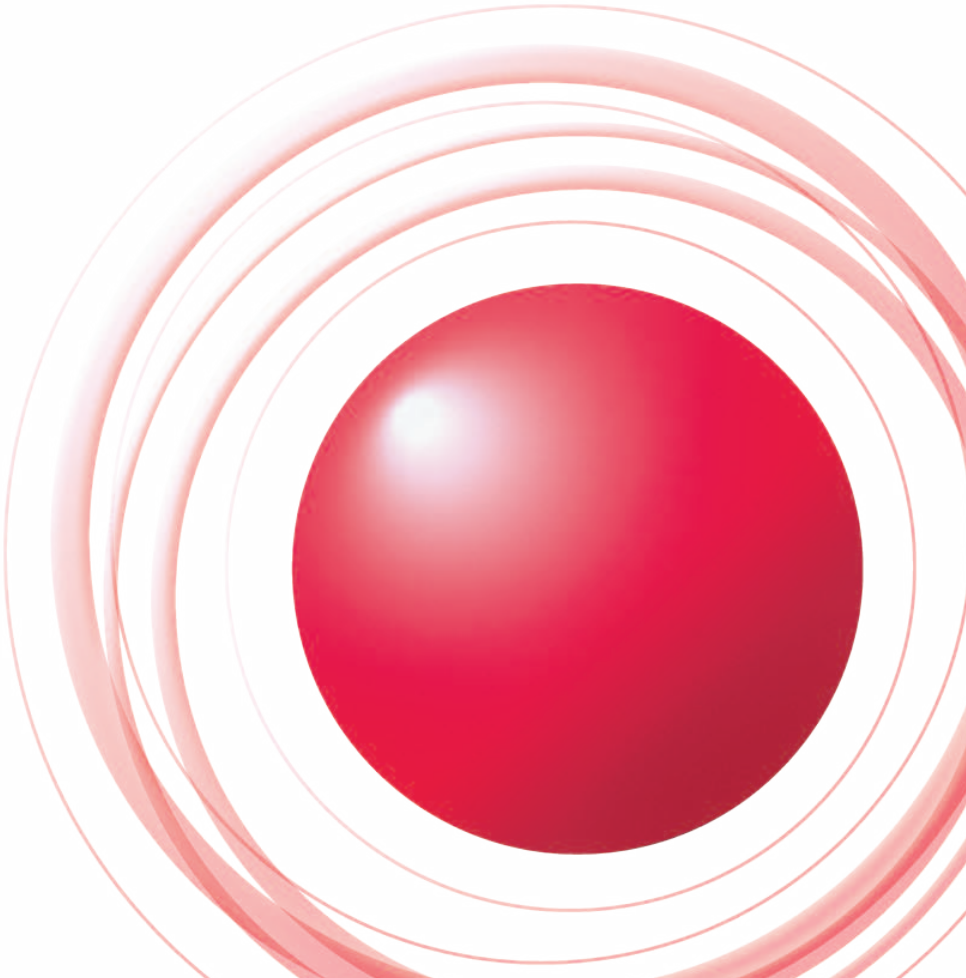
**マッシュアップコンテンツに起因したマルウェアの大量感染**

メッセージングテクノロジー

**送信ドメイン認証技術と迷惑メールの関係を考察**

インターネットオペレーション

**IPv4アドレス枯渇問題を知り、備える**



Internet Infrastructure Review Vol.10 February 2011



■IIJホームページ(http://www.iij.ad.jp/development/iir/)に、最新号及びバックナンバーのPDFファイルを掲載しております。併せてご参照ください。

# エグゼクティブサマリ

2011年2月3日に、未使用の/8 のIPv4アドレスブロックの最後の5つが、IANAから5 つの地域IR に1つずつ割り振られ、ついにIPv4の大元の在庫が枯渇を迎えました。地域IR の在庫が無くなるまでには数ヶ月の時間的余裕があるとはいえ、いよいよIPv4 の枯渇問題をどう乗り越えていくのか、本格的な対策の推進が必要な時期になりました。

インターネットの対人口での普及率を見てみると、2010年6 月の時点では、世界全体で28.7%で、特にアジア太平洋地域では全体よりもやや少ない21.9%となっています。この数字から考えると、インターネットは、ネットワークインフラとしてさらに今の数倍の規模にまで拡大する可能性を持っているという事ができるでしょう。

しかし、今後も拡大を続けるインターネットでIPv4を使い続けるためには、グローバルアドレスを複数ユーザでシェアしたり、不要になったIPv4アドレスを組織間で譲渡したりするような状況が考えられ、そうなると従来IP アドレスベースで行なわれていたユーザの認証などの仕組みが非常に繁雑になったり、そもそも意味をなさなくなる事も考えられます。

IPv6 に移行するといっても、プライベートアドレスにNAT が大前提となっている今のIPv4のネットワークをどのように安全に移行できるかなど、運用面やセキュリティ面での課題がまだまだ多いのが現状です。

このように、IPv4アドレスの枯渇を乗り越えて、インターネットを全人類を繋ぐ安心かつ安全なコミュニケーションインフラへと成長させるためには、今後も継続的な技術開発と事業者やユーザが相互に協調した運用体制を維持することが不可欠になるでしょう。

本レポートは、IIJがインターネットというインフラを持続的に整備・発展させ、お客様に安心・安全に利用し続けて頂く為に継続的に取り組んでいるさまざまな調査・解析の結果や、技術開発の成果、ならびに、重要な技術情報を定期的にとりまとめ、ご提供するものです。

「インフラストラクチャセキュリティ」の章では、2010年10月から12 月末までの3 ヶ月間を対象として、継続的に実施しているセキュリティインシデントの統計とその解析結果をご報告します。また、対象期間中のフォーカスリサーチとして、2010年9月の一連の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、マルウェア対策研究人材育成ワークショップ2010（MWS2010）についてご紹介します。

「メッセージングテクノロジー」の章では、2010年9月末から1月初頭までの14週間の迷惑メールの割合の推移と送信地域の分布、主要迷惑メール送信地域の推移を示します。また減少傾向にある迷惑メールの割合の推移に関する考察や、送信ドメイン認証技術による認証の結果と迷惑メールとの関係についての解説を行います。

「インターネットオペレーション」の章では、いよいよ第一段階が始まったIPv4 アドレス枯渇の意味や影響について解説し、ISPや企業がその対策に取り組む際に検討しなければならない項目や課題を示します。

「インターネットトピック」としては、日本国内におけるシーサート（Computer Security Incident Response Team: CSERT）組織の協調や情報交換を通じて会員組織の事案対応能力向上を目指す団体である、日本シーサート協議会の概要と活動内容についてご紹介します。

IIJでは、このような情報を定期的なレポートとしてお届けするとともに、お客様に、企業活動のインフラとしてインターネットを安心・安全、かつ、発展的に活用して頂くべく、さまざまなソリューションを提供し続けて参ります。

執筆者：
**浅羽 登志也（あさば としや）**
株式会社IIJイノベーションインスティテュート代表取締役社長。1992年、IIJの設立とともに入社し、バックボーンの構築、経路制御、国内外ISPとの相互接続等に従事。1999年取締役、2004年より取締役副社長として技術開発部門を統括。2008年6月に株式会社IIJイノベーションインスティテュートを設立、同代表取締役社長に就任。

# 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関係す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IIJ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

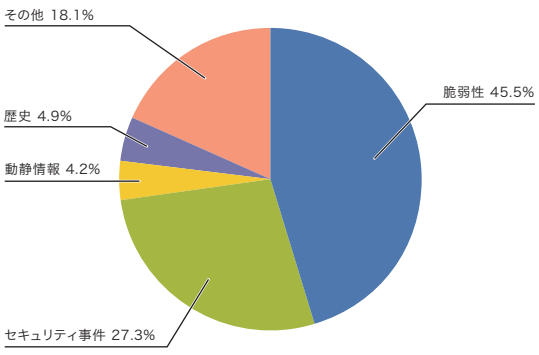



**図-1　カテゴリ別比率（2010年10月～12月）**

＊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）ドライバーの脆弱性により、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　APSB10-28 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　APSB10-26 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

IIJ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、IIJの設備やIIJ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継続しています[*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/detailvulnId=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!? ー“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、公開されたことで[*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とりまとめた「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

IIJ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。

### 1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生しています。DDoS攻撃の内容は、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、2010年10月から12月の期間にIIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、正確な攻撃の実態を把握することが困難なため、ここでは集計対象から除外しています。

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[*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。

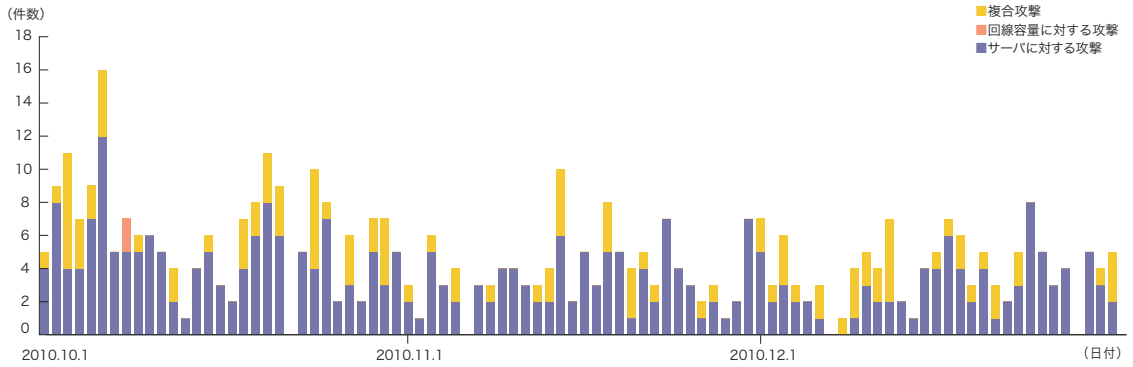



**図-2　DDoS攻撃の発生件数**

＊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、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24.8%、複合攻撃が74.7%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のパケットによって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。

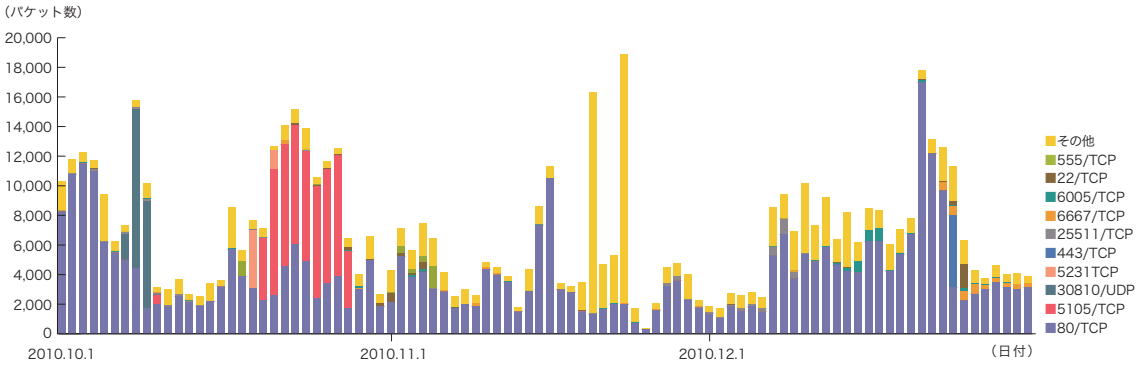



**図-3　DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)**

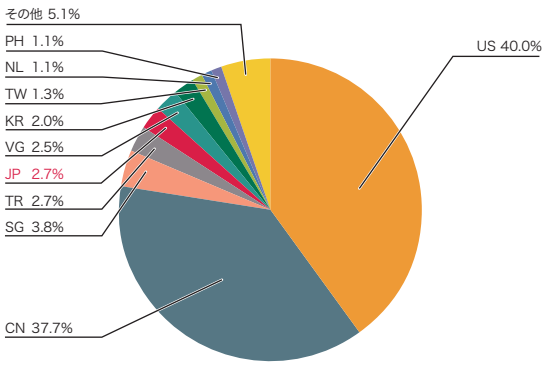



**図-4　backscatter観測によるDDoS攻撃対象の分布(国別分類、全期間)**

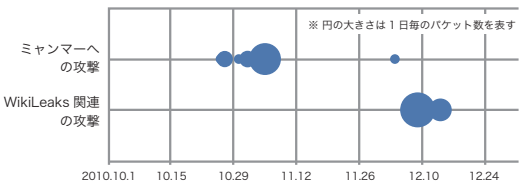



**図-5　backscatter観測によるミャンマーへのDDoS攻撃とWikiLeaks関連のDDoS攻撃**

＊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.iij.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、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[*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。

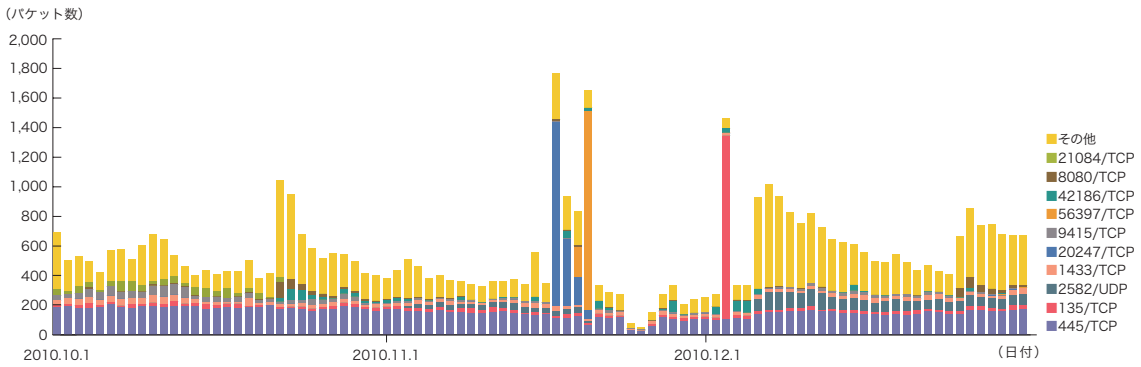



**図-6　ハニーポットに到着した通信の推移（日別・宛先ポート別・一台あたり）**

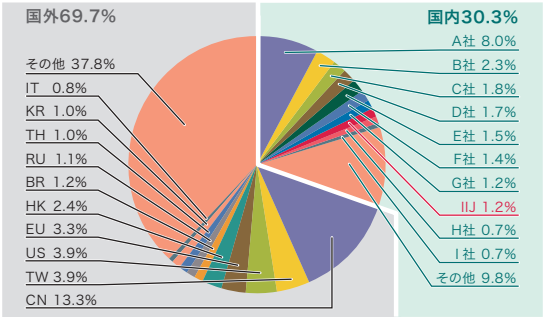



**図-7　発信元の分布（国別分類、全期間）**

＊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、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%、ボット型40.1%、ダウンローダ型3.1%でした。また、解析により、25個のボットネットC&Cサーバ[*47]と29個のマルウェ

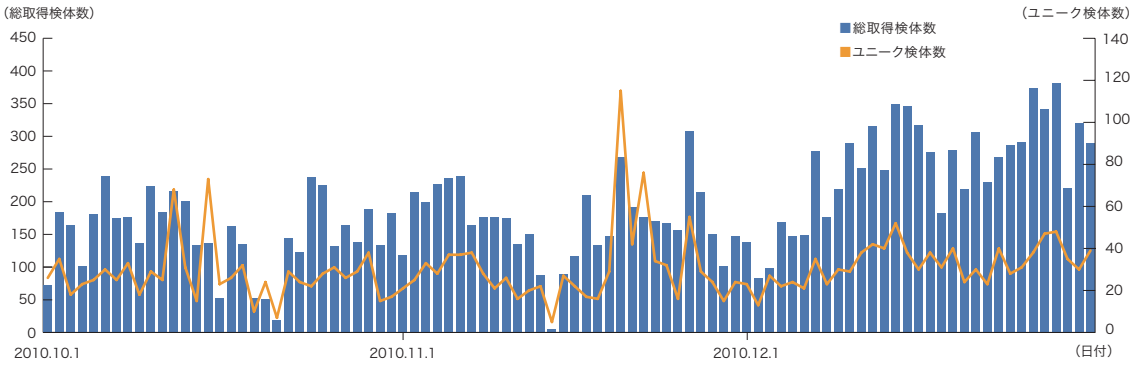



**図-8　取得検体数の推移(総数、ユニーク検体数)**

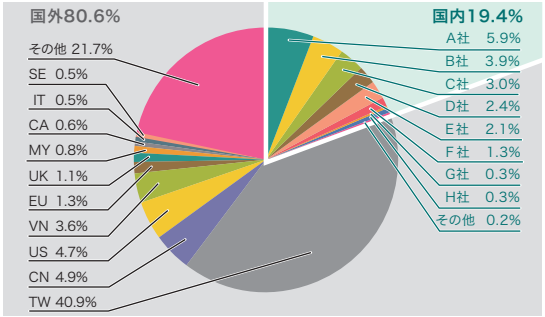



**図-9　検体取得元の分布(国別分類、全期間)**

＊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。

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

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[*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、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、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。

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

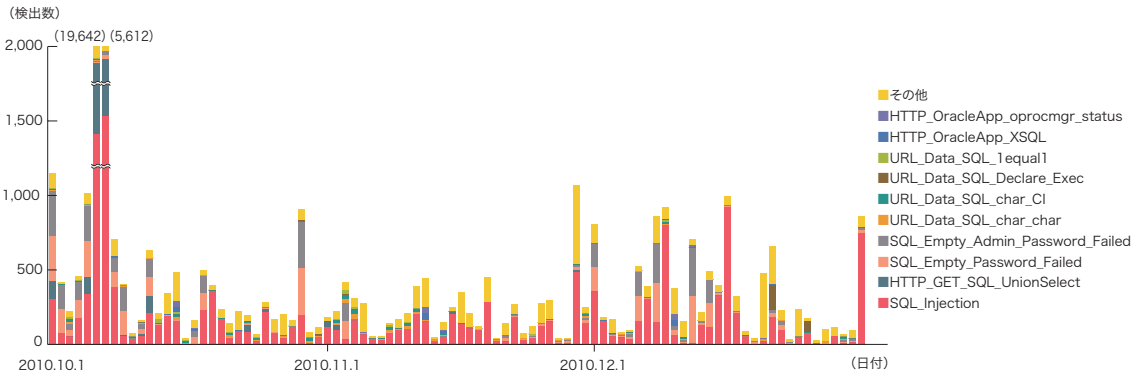



**図-10 SQLインジェクション攻撃の推移(日別、攻撃種類別)**

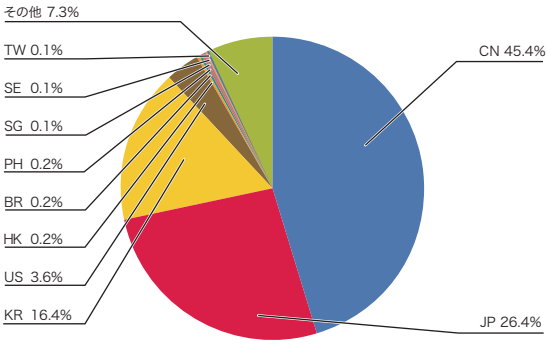



**図-11 SQLインジェクション攻撃の発生元の分布(国別分類、全期間)**

＊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。

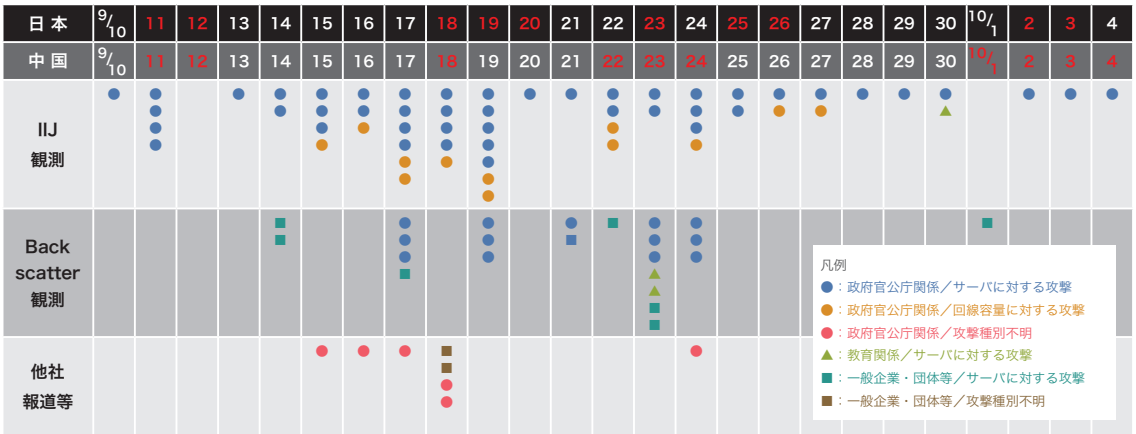
#### ■ 攻撃の発生状況

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をこえる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**




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。しかし、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。IIJ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)。

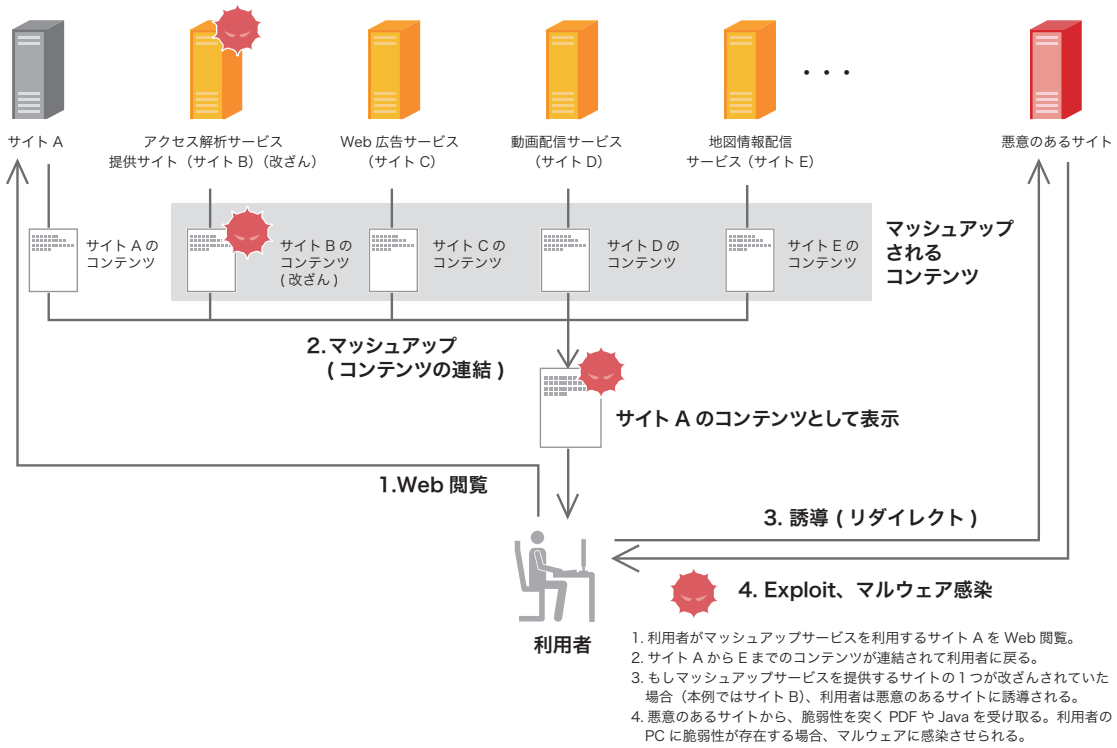



**図-12 マッシュアップコンテンツに起因したマルウェア感染**

＊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、日本国内で少なくとも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。IIJ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、IIJ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 |

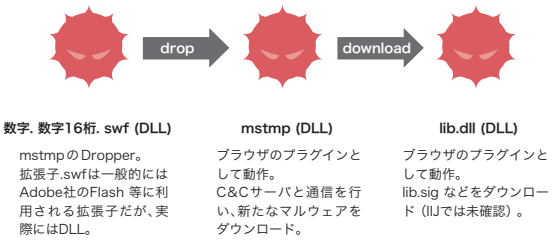



**図-13 mstmp感染後のマルウェアの変遷**

＊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.iij.ad.jp/development/iir/pdf/iir_vol04.pdf）、Vol.6 1.4.1 Gumblar の再流行（http://www.iij.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.iij.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する脅威。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.iij.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/2010/10/18/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ては意味がないため、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。

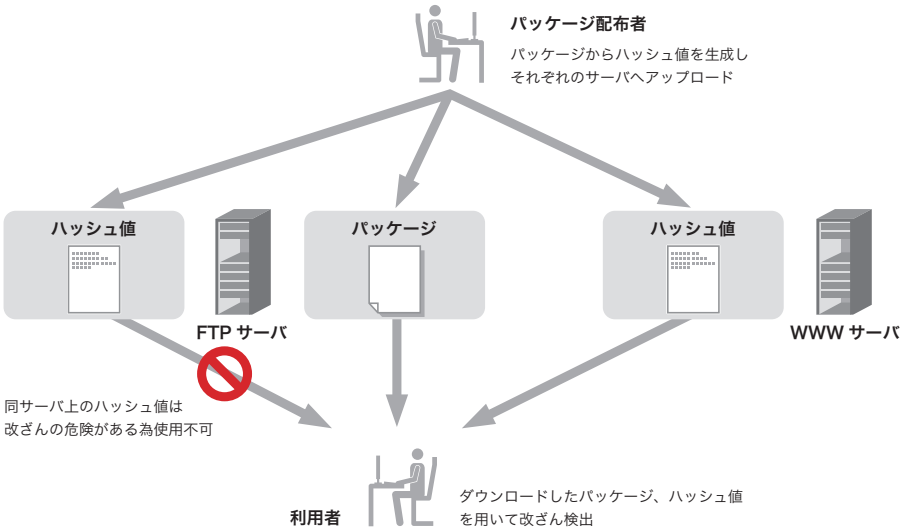



**図-14 ハッシュ値を用いた改ざん検出の例**

＊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.iij.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、ProFTPD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て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、解析対象の種類の面でも大幅に拡充されました。

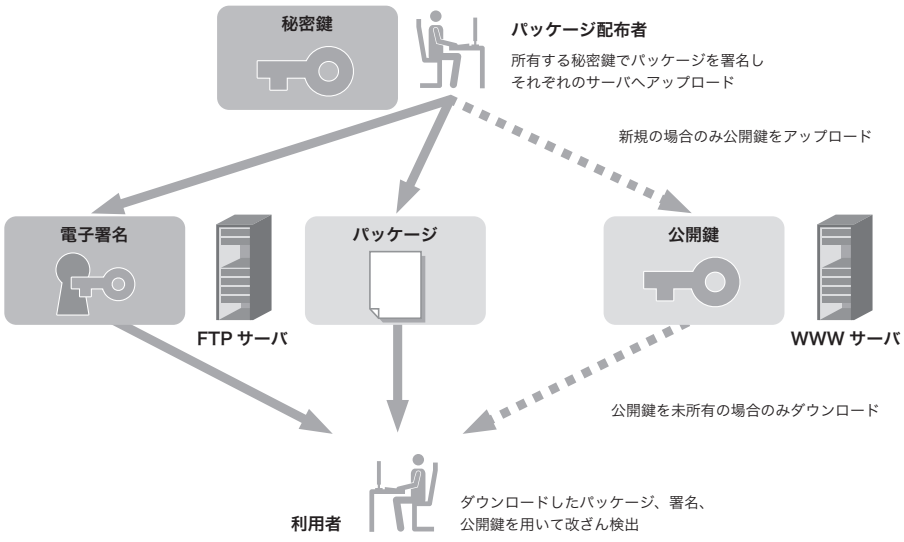



**図-15 電子署名を用いた改ざん検出の例**

＊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ボ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.iij.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件発表されました。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。

IIJ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。IIJ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。IIJ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、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、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の模様を紹介しました。

IIJでは、このレポートのようにインシデントとその対応について明らかにし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まいります。

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

# 送信ドメイン認証技術と迷惑メールの関係を考察

**今回は、2010年第39 ～ 52週での迷惑メールの推移を報告します。迷惑メールの送信元地域は、前回に引き続いて米国が1位でした。今回は、迷惑メールと認証結果の関係についても考察します。**

## 2.1 はじめに

このレポートでは、迷惑メールの最新動向やメールに関する技術解説、IIJが関わるさまざまな活動についてまとめています。今回のレポートは、多くの企業の第3四半期にあたる2010年第39週（2010年9月27日～ 10月3日）から第52週（2010年12月27日～ 2011年1月2日）までの14週間分のデータを対象としています。

## 2.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IIJのメールサービスで提供している迷惑メールフィルタが検知した割合の推移と、迷惑メールの送信元に関する分析結果を中心に報告します。

### 2.2.1 2010年後半から迷惑メールの減少が続く

前回のIIR Vol.9では、9月以降迷惑メール割合の減少が続いていると報告しました。今回の調査範囲でも、この減少傾向が続いています。今回の調査範囲である2010年第39週から第52週までと、その前年同時期を含む1年3 ヶ月分（66週）の迷惑メール割合の推移を図-1に示します。

今回の調査期間での迷惑メール割合の平均は72.1%でした。前回（2010年第26 ～ 38週）から6.9%減少し、2009年同時期（2009年第40 ～ 53週）に比べても9.3%減少しています。今回の迷惑メールの割合の推移では、平均値が減少していることからも明らかなように、2009年の同時期に比べて大きく変化し、その傾向も減少しています。特に、2010年最終週である第52週は、63%まで減少しています。これは、IIR Vol.2で報告したMcColo社のネットワーク遮断による影響が見られた2008年第47週よりも低い割合です。今回の迷惑メールの減少に関しては、セキュリティベンダからのレポートや、その内容を引用したニュース記事でも、2010年後半からメール流量が減少していることが報告されています。原因は、迷惑メールの主要な送信手法であるボットネットの活動が低下しているためと推測されています。2008年にMcColo社のネットワーク遮断の詳細を報告し、ワシントンポスト紙の

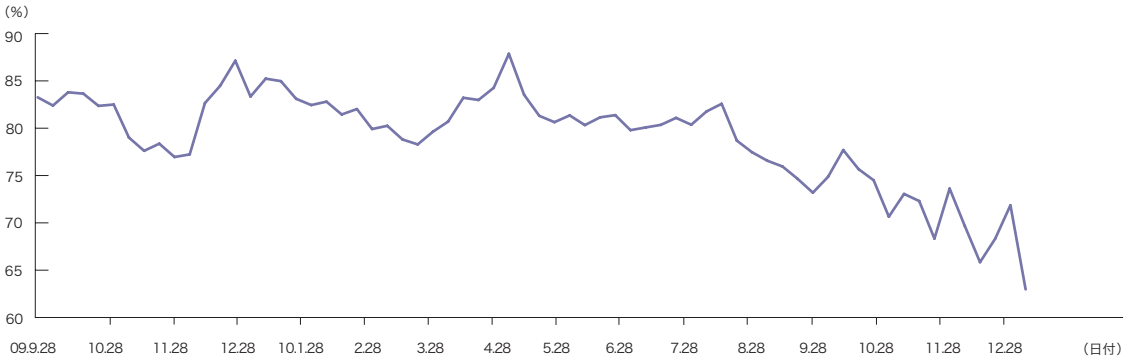



**図-1　迷惑メール割合の推移**

＊1　KrebsonSecurity (http://krebsonsecurity.com/2011/01/taking-stock-of-rustock/)

記者だったBrian Krebs氏のブログ[*1]でも、2010年8月からのスパム量の減少と、ボットネットのRustockとの関係性が報告されています。このように迷惑メールの割合が減っていくことは、メールサービスを運用する者にとっては望ましいことですが、残念ながらあまり長続きはしないようです。まだ速報値のレベルですが、2011年第2週あたりから迷惑メールの割合が再び上昇してきています。

### 2.2.2 送信元1位は米国、日本の割合も上昇

今回の調査期間での迷惑メール送信元地域の分析結果を図-2に示します。今回の調査では、迷惑メールの送信元地域の1位は、前回に引き続き米国（US）で、迷惑メール全体の10.3%を占めていました。ただし、前回からは1%減少していますし、迷惑メール全体の割合も減少していますので、実際に受信されたメール数も減少したことになります。2位は中国（CN）の10.2%で、前回の3位から上昇しています。3位はインド（IN）の6.2%で、前回2位であったときの割合（7.4%）から減少しています。4位はロシア（RU、5.4%）、5位は日本（JP、4.7%）です。日本は、前回の8位から上昇しました。以下、ブラジル（BR、4.6%）、ベトナム（VN、4.6%）、英国（GB、4.2%）が続いています。

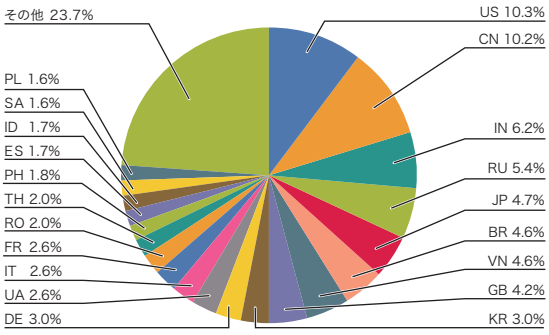



**図-2　迷惑メール送信元地域の割合**

### 2.2.3 ボットネットと送信元地域の関係

迷惑メール送信元地域で日本の順位が上がった原因は、日本発の迷惑メールがボットネットの活動の影響をあまり受けなかったためだと考えられます。ボットネットの活動が低下し全体の迷惑メール量が減少しました。しかし、日本発の迷惑メールは、ボットネットを利用した動的IPアドレスでなく、固定IPから送信されるものがほとんどです。このため、日本の順位が上がったものと思われます。中国の順位が上がった原因も同じ理由であると推測しています。以前IIR Vol.6で、日本や中国では特定の送信元からの迷惑メール量が多いという分析結果を示しました。この傾向は現在も続いています。このため、日本と同様にボットネットの活動の影響を受けなかったものと考えています。　図-3に、これら迷惑メール送信元の上位7地域（US、CN、IN、RU、JP、BR、VN）での割合の推移を示します。中国（CN）の割合が第44週（11月11日の週）に急上昇しています。これは、特定の送信元からの迷惑メール数が増加したことが原因です。これに対して第50週（12月13日の週）と第51週（12月20日の週）の割合が大きく減少しています。これらは、それまで続いていた特定の送信元からの迷惑メールが送信されなくなったことによるものです。第52週（12月27日の週）に中国（CN）の割合が再び急上昇し、米国（US）の割合が激減しています。図-1に示した全体の割合で、この週は迷惑メール量が極端に少なかった時期です。この原因が米国（US）からの送信量の減少であることが図-3から読み取れます。一方、中国（CN）やロシア（RU）の割合が上昇していますが、これは実際の送信数が増えたのではなく、全体の迷惑メール数が少なかった上に米国（US）の割合が極端に減ったことが影響しています。こうした傾向から、ボットネットの種類別に地域的な分布状況を分析できるかもしれません。

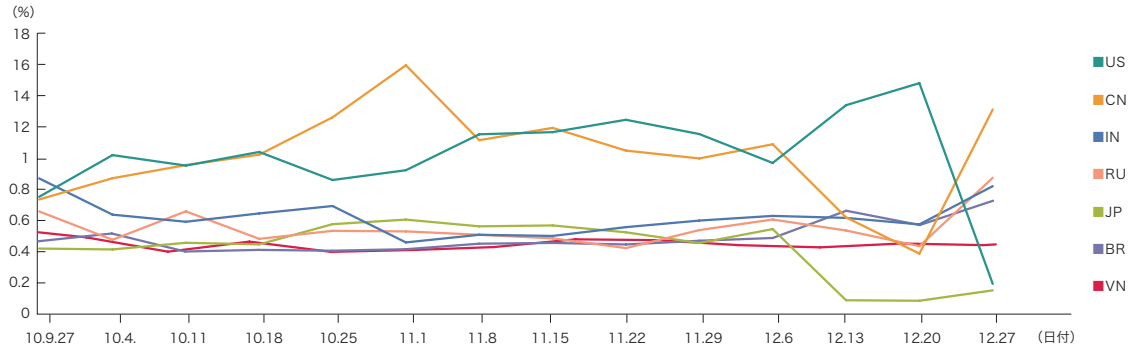



**図-3　迷惑メール送信元のうち上位7地域の推移**

## 2.3 メールの技術動向

IIJが提供するメールサービスでは、メールの受信時に送信ドメイン認証を標準で行っています。特に個人向けに提供しているIIJ4UとIIJmioブランドで提供しているメールサービスでは、SPF（Sender Policy Framework）とDKIM（Domain Keys Identified Mail）の2つの技術による認証を行っています。これまで、この認証結果を利用した送信ドメイン認証フィルタを提供してきましたが、2010年12月1日からはより簡単な設定で利用できる「なりすましメールフィルタ」の提供を開始しました[*2]。今回も送信ドメイン認証技術の普及状況について報告します。

### 2.3.1 流量ベースのSPFの導入が増加

今回の調査期間（2010年10月～12月）に受信したメールのSPFによる認証結果の割合を図-4に示します。送信側のドメインがSPFレコードを宣言していないことを示す認証結果“none”の割合は、今回50.2%でした。この結果は、前回IIR Vol.9で報告したものに比べて5.5%減少しています。したがって、送信側のSPFレコードの宣言率、すなわち送信側のSPFの導入割合が5.5%増えています。しかし、今回の調査期間では、迷惑メールの全体量も減少しているために、SPFの導入割合が見かけ上増加したのではないかと考えることもできます。これに対しては、認証結果“pass”の割合が23.6%と、前回から4.8%増加したことを挙げることができます。

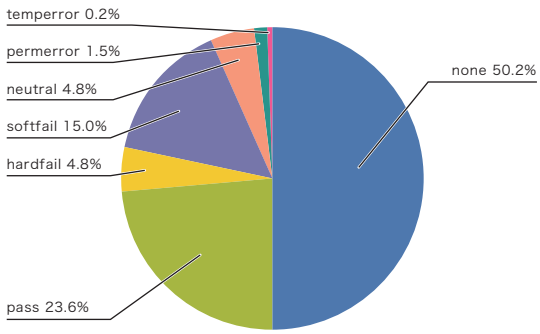



**図-4　送信ドメイン認証結果の割合**

### 2.3.2 認証結果と迷惑メールの関係

いまだに一部の人々の間で誤解されることが多いため、認証結果と迷惑メールの関係について改めて補足しておきます。認証結果が“pass”となった送信者情報のメールが迷惑メールでない、とは必ずしも言えません。同様に、“fail/hardfail”や“softfail”となったメールが必ずしも迷惑メールであるとも限りません。送信ドメイン認証技術が普及する以前は、多くの迷惑メールで、広く知られているドメイン名が送信者情報（配送プロトコルでの送信者情報や、メール本体のFrom:ヘッダに記述されているメールアドレス）に利用されていました。古くは、送信者情報を利用した受信ブロックを回避したり、実際の送信元を隠蔽したりするために、よく使われているドメインが嘘の情報として利用されました。また最近では、フィッシングなど、そのドメイン名を使っているWebサービスの偽サイトに誘導して個人情報などを搾取する目的で、受信者を騙すために送信者情報が利用されることがあります。このようなことから、送信者情報を詐称できないようにするために、送信ドメイン認証技術が開発され、普及されてきました。その一方で、認証結果だけを使うフィルタリングを回避するために、認証結果が“pass”となるドメインを送信者情報に利用する迷惑メールも増えてきました。母数が多いデータについての分析はまだ終えていませんが、個人で受け取っている迷惑メールについて調べてみると、最近の認証結果の半数以上が“pass”となっていました。この原因として、2つのことが考えられます。1つは、正規のメールサーバを踏み台にして、迷惑メールが送信されている可能性です。最近では、メールの送信時に送信者認証（SMTP-AUTH）を実施するメールサービスが増えました。しかし、この認証に利用するパスワードに、認証IDと同じ文字列が使われていたり、不正プログラム（マルウェア）によって搾取された認証IDが悪用されたりしているケースなどが考えられます。もう1つは、ドメイン名を

＊2　新しい送信ドメイン認証フィルタ「なりすましメール対策フィルタ」の提供及び従来の送信ドメイン認証フィルタの廃止について（https://www.iij4u.or.jp/info/iij/20101201-1.html）（https://www.iijmio.jp/info/iij/20101201-1.html）

詐称せず、堂々と独自のドメインを取得し、それに送信ドメイン認証技術を導入して送信しているケースです。前者の場合は、安易なパスワードを設定しないようにしたり、ウイルスチェックをこまめに実施したりするなどの啓発による対策が重要です。後者の場合については、元々送信ドメイン認証技術に関する議論の中で、こういった可能性があることが指摘されていました。ただし、このようなドメイン名は、自らが迷惑メール送信者だと名乗っているようなものなので、粛々とフィルタリング等を行えばよい、ということになります。つまり、認証結果だけで判断せずにドメイン名と合わせてフィルタリングするべき、ということです。確かに紛らわしいドメインが取得され、正規のドメインになりすましているようなケースもあります。しかし、このようなドメインは、ブラックリストなどで機械的に判断することができます。　このように認証結果が“pass”というだけでは、迷惑メールかどうかを判断することはできません。したがって、送信ドメイン認証技術が迷惑メール対策の1つであるとは、単純には言えません。認証されたドメイン名の情報と組み合わせることで対策が可能になる、いわば基盤のような技術であると言えます。また、きちんと管理されたドメインであれば、そのドメイン名と“pass”の認証結果を併せてホワイトリストとし、他のフィルタリング処理を省略してメールシステムの負荷を軽減させることも可能なはずです。このように、メールを受け取りやすくするためにも、メールの送信側で送信ドメイン認証技術を導入し、送信しているメールに迷惑メールが含まれないようにする、といった管理が必要になります。　また、正規のメールでの認証に失敗するケースについては、メールの再配送時に生じるなど、運用形態の一部で発生することが分かっています。このような問題は、技術的に解決可能であることをこれまでのIIRで解説してきていますので、参照にして頂ければと思います。

## 2.4　おわりに

前回、特電法（特定電子メールの送信の適正化等に関する法律）とその改訂に関する研究会のワーキンググループが開催されていることに触れました。報道機関による12月17日の発表によれば[*3]、この法律の違反容疑で東京の出会い系サイトの運営会社が逮捕されたそうです。報道内容から、今回の容疑は、送信者情報を偽って無差別に大量にメールを送信したことと、受信者の同意を得なかったこと（オプトイン規制）が要件となっているようです。いずれの容疑も、前回の法律改正時に強化された部分ですので、改正の意義があったと言えるでしょう。また、今回の迷惑メールの送信は、中国やフィリピンなどの海外から行われたと報道されています。もちろん、海外から送信されたとしても、日本に届く迷惑メールは日本の法律の対象になるため、逮捕することが可能です。海外から送信された理由は、これまでIIRで述べてきたとおり、OP25B（Outbound Port 25 Blocking）の導入などのISPの努力の結果、日本からは送信しにくくなったためだろうと考えています。前回の法律改正で、外国の執行機関に対して情報提供することも、一定の条件で可能になりました（第三十条）。ただし、外国の法律や執行制度には日本と異なる部分があるため、この法律改正だけで違法な業者の摘発が増えていくとは限りません。しかし、言うまでもなくインターネットは全世界をつなぐ基盤システムですので、今後もよりグローバルな視点で協力しあっていくことが重要だと考えています。その意味で、この部分の改正に関しても意義があったと考えています。　IIJは、今後も引続き、技術面や法的な側面を含め、よりグローバルな分野でよりよいインターネット環境実現のために貢献していきたいと考えています。

執筆者：
**櫻庭 秀次（ さくらば しゅうじ）**
IIJ サービス本部 アプリケーションサービス部 シニアエンジニア。メッセージングシステムに関する研究開発に従事。特に快適なメッセージング環境実現のため、社外関連組織との協調した各種活動を行う。MAAWGメンバ及びJEAGボードメンバ。迷惑メール対策推進協議会及び幹事会構成員、送信ドメイン認証技術WG主査。（財）インターネット協会 迷惑メール対策委員。総務省 迷惑メールへの対応の在り方に関する検討WG 構成員。

＊3　迷惑メールを無差別に数百万通！出会い系を宣伝、容疑の7人逮捕（http://sankei.jp.msn.com/affairs/news/110117/crm11011720130102-n1.htm）

# IPv4アドレス枯渇問題を知り、備える

**数年前から話題になっているIPv4アドレス枯渇問題が現実のものとなりました。ここでは、IPv4アドレス枯渇とはどのような問題なのか、ISPや企業にはどのような対応が求められるのかを解説します。**

## 3.1 はじめに

IP（インターネットプロトコル）を使った通信では、パケットという小さな断片に分けられた情報がやりとりされます。大きな情報であっても小さなパケットに分割して運び、受け手側で元通りに組み立て直すことで、ネットワーク上の機器間でさまざまな情報が伝達されています。パケットには、送り手側と受け手側の機器を示す番号が含まれています。これは、ネットワーク上で機器の位置を示す住所のような情報で、IPアドレスと呼ばれています。

ここでは、IPアドレスに関する話題のうちIPv4アドレス枯渇問題を、ISPと企業ユーザの2つの視点から取り上げます。

## 3.2 インターネットとIPアドレス

インターネット上で通信している機器には、すべてIPアドレスが割り当てられています。インターネットでは、受け手の機器がどんなに遠方にあっても、受け手のIPアドレスを元にパケットが届けられます。これを実現している技術が経路制御やルーティングと呼ばれるものです。インターネットでは、ルータと呼ばれる機器がどのIPアドレスがどこで利用されているかという情報を動的に交換して、常に正しい受け手にパケットが届けられるよう運用されています。

つまり、IPアドレスは、パケットを正しい受け手に届けるためにとても重要な役割を果たしています。受け手の機器がどれほど遠方にあってもIPアドレスだけでパケットが届くということは、インターネットという広大なネットワークでそのIPアドレスに対応する機器が一意に決まるということです。世界中の利用者がそれぞれ勝手にIPアドレスを設定してしまうと、IPアドレスの重複が発生してしまい、正しい受け手にパケットが届かなくなってしまいます。これを防ぎ、IPアドレスの一意性を担保するためには、何らかの管理体系が必要です。

## 3.3 IPアドレスの管理

### 3.3.1 IPアドレスの分配

現在、インターネットでは、階層構造を持つインターネットレジストリを通じてIPアドレスが分配されています。大本の在庫管理は、ICANN（Internet Corporation for Assigned Names and Numbers）によって運用されているIANA（Internet Assigned Numbers Authority）機能が担っています。IANAは、APNIC（Asia-Pacific Network Information Centre）など地域ごとに設立されているRIR（Regional Internet Registry）に、必要に応じてIPアドレスを分配します。実際にユーザへのIPアドレスの割り当てを行っているISPなどのLIR（Local Internet Registry）は、APNICなどのRIRやJPNIC（Japan Network Information Center）などのNIR（National Internet Registry）を通じてIPアドレスの分配を受けています。

ISPは、このようにして分配を受けたIPアドレスを使ってネットワークを構築し、ユーザに接続サービスを提供しています。これまでISPは、専用線やデータセンタといった常時接続サービスで静的なIPアドレスを割り当てる一方、ダイヤルアップ接続など一時的な接続サービスでは接続のつどに動的なIPアドレスを割り当てていました。動的なIPアドレスの割り当ては、需要の大

きさに応じて行えばよいため、実際の契約者数よりも少ない数のIPアドレスで運用できるなどのメリットがあったのです。しかし、ブロードバンド接続の要求が高まるにつれて、インターネットを利用していないときにも契約者からIPアドレスが解放されず、それまでと同じ契約者数でもより多くのIPアドレスが必要になってきています。

この原稿を執筆している時点でも、これまでどおりの分配ポリシによってIPアドレスが分配されています。例えば、ISPは、将来の需要に基づいた必要量を申請し、その内容が審査で認められればIPアドレスの割当てを受けることができます。しかし、現在、1つの大きな問題が生じています。それは、IANAで管理されているIPv4アドレスの在庫が底をついてしまったのです。IPv4アドレスの在庫がなくなってしまうと、「無い袖は振れない」のことわざのとおり、これまでのような需要に応じた分配ができなくなります。現時点ですでにAPNICは、APNICが管理する在庫IPv4アドレス数が一定量以下になった場合、既存の需要に基づく割り振りを停止し、会員であるLIRに対して一律のサイズに限ったIPv4アドレス分配を行うというポリシを採択しています。

### 3.3.2 IPv4アドレス枯渇問題

2月初めにIANAからAPNICにIPv4アドレスの割り振りを行った結果、IANAのIPv4アドレス在庫量が一定以下になりました。これを受けてこれまでの議論で決められていた最後の分配ポリシに基づき、2011年2月3日節分の日に残った在庫を5つのRIRに均等に割り振り、IANAで分配用に持っていたIPv4アドレスはなくなりました。これまでの需要と割り振りの傾向からすると、APNICの在庫は早ければ2011年5月、どんなに遅くても来年中には無くなる見込みです。JPNICは独自の在庫をほとんど持っていないため、APNICの在庫枯渇はそのまま日本でも在庫枯渇を意味します。

IPv4アドレスが枯渇すると、新規に事業を始めようとするISPがサービスに必要なIPアドレスを確保できなかったり、個人向けサービスに新規ユーザが接続できなかったりといった問題が発生すると考えられます。このような状況が発生する時期は、各ISPが保持しているIPアドレスの在庫や利用の伸びによって異なります。しかし、いずれにせよ、新規に顧客を獲得していたり、ネットワークを拡張したりしているISPでは、必ずIPv4アドレスの在庫枯渇が発生します。

中長期的な視点からは、インターネットに接続される機器数に比べてIPv4アドレスの絶対数が足りなくなることが予測されています。このため、IPアドレスの在庫枯渇に対する根本的な解決方法として、IPアドレス数を増やしたプロトコルであるIPv6の導入が必要になります。しかし、残念ながらIPv6はIPv4と互換性がなく、新たなプロトコルを追加するための導入作業が必要です。このような制約から、これまでIPv6の導入はなかなか進んできませんでした。しかし、IPv4アドレス

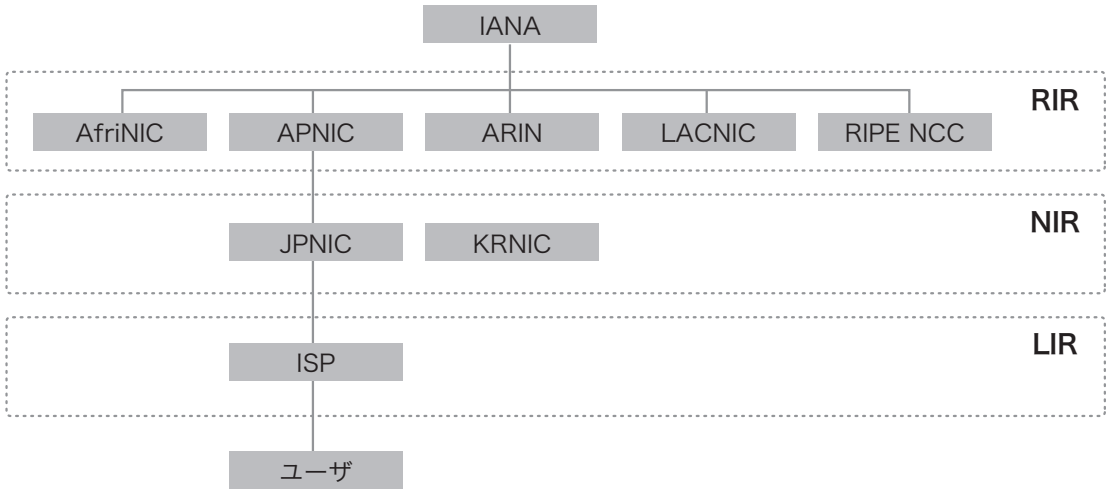



**図-1　階層構造によるIPアドレスの分配**

の枯渇が現実のものとなり、ようやく導入の検討が進み始めたように思えます。

### 3.3.3 ISPでの対応

IPv6の導入が進み始めたといっても、まだまだ多くのサイトがIPv4で運用されています。このような現状では、インターネットに接続したいというユーザにはIPv4の接続性も提供する必要があります。また、メールやWebなどのサービスを提供しているサーバ側でも、当面はIPv4アドレスが必要です。つまり、今後は何らかの方法でIPv4アドレスによる運用を延命していくことが必要になります。このための主な考え方は、IPv4アドレスの効率的な利用とIPv4アドレスの共有になります。

例えば、IPv4アドレスの効率的な利用としては、現在利用されていないIPv4アドレスを回収して他の場所で利用することなどが考えられます。また、組織間でIPv4アドレスを融通し合うことも検討され、すでにAPNICでは会員組織間でIPv4アドレスを移転できるポリシが採択されています。ユーザに提供する接続サービスに関しても、Webやメールといった外部サーバへのアクセス用途が多いとの判断から、ユーザ間でIPv4アドレスを共有するための技術が検討されています。

## 3.4 企業における対応

「うちはIPv4アドレス枯渇問題の対応をしなければいけないのか？」「うちのシステムはIPv6対応が必要なのか？」このような質問を企業の情報システム担当者からよく受けます。企業は、IPv4アドレス枯渇問題に対応する必要があるのでしょうか。企業によるIPv6対応は必要なのでしょうか。次に、一般企業におけるIPv4アドレス枯渇問題の対応方針の考え方や対策の具体例を示します。

### 3.4.1 自社への影響の分析

まず初めにIPv4アドレス枯渇問題を正しく理解する必要があります。そもそもIPv4アドレス枯渇問題とは、一体どのようなものなのでしょうか。IPv4アドレス枯渇の状況はどのようなもので、どのようになっていくのでしょうか。誰にどのような影響があり、それによって世の中はどのようになっていくのでしょうか。このようなことを正確に理解する必要があります。

IPv4アドレス枯渇問題の現状を正確に理解した後は、この問題が自社のシステムにどのような影響を与えるかを把握します。考えるべきことは次の2点です

- 自社でのIPv4アドレスの在庫
- 世の中でのIPv4アドレスの在庫

まず自社でのIPv4アドレスの在庫ですが、現在の在庫量と今後のシステム増強計画などを照らし合わせ、今後もIPv4アドレスの消費が続くのか、自社の在庫がいつまで持つのかといった点を把握します。

しかし、自社のIPv4アドレスの在庫が十分であったからといって、いっさい対応を行わなくてもよいというわけではありません。世の中でのIPv4アドレスの在庫がなくなりIPv6の導入が進んだ場合、自社のシステムがIPv4にしか対応していないのでは、IPv6を使うユーザが接続できません。このため、インターネットによってビジネスを展開している企業はもちろんのこと、一般企業でも少なくとも公開系のサーバ群やDMZへのIPv6導入は必要になります。

また、IPv6の導入がビジネス上のメリットやデメリットになりうるケースも考えられます。例えば、競合他社がIPv6に対応し自社が対応しなかった場合、競合他社にどのようなビジネス上のアドバンテージを取られてしまうのか、また自社がIPv6に対応し競合他社が対応しない場合にどのようなメリットを見いだせるのかといった検討も必要です。コストも重要な検討材料の1つです。IPv6の導入は、情報システム部門の担当者が想像する以上に多大なコストがかかります。ビジネス上のメリットとIPv6導入コストを比較して、IPv6を導入するのかどうかを決定します。

こういった内容を元にしてIPv4アドレス枯渇問題に対応するかどうかを判断します。また、対応する場合には、その対応時期や対応方法を検討する必要があります。

### 3.4.2 企業での対応活動

IPv4アドレス枯渇問題での企業における恒久的な対応方法は、IPv6の導入になります。ただし、IPv6の導入だけではなく、IPv4アドレス在庫の延命処置といった対応も必要です。

IPv4アドレス在庫の延命処置の1つに、管理上はサーバやクライアントに付与されているはずだが、実際には使用されていないIPv4アドレスを回収するといった作業があります。また、無駄なネットワーク分割を最適化することも、IPv4アドレス在庫の延命処置になります。例えば、/29でサブネットを構成しているネットワークでのIPv4アドレスの総数は8個です。ただし、このうちネットワークアドレスとブロードキャストアドレスで2個、デフォルトルートで1 ～ 3個が使用されるため、実際にホストに利用できるアドレスは3個です。/29で構成しているネットワークが多数あるときには、それらをまとめることでIPv4アドレスを節約することができます。未使用アドレスの回収やネットワーク分割の最適化などによってネットワークの棚卸を行うことが、IPv4アドレスの節約につながります。

企業の情報システムにIPv6を導入するときに最も大事なものは、導入計画です。これまでIPv4によってシステムを構築するときには、IPアドレスの付与ルール、DNSの名前の付け方、フィルタポリシなどは、あらかじめ決められたルールに従って設計してきたはずです。IPv6でシステムを構築する際には、このようなIPv4で当たり前のように行ってきたことを、どのように実行するか一つ一つ決める必要があります。次に、具体的な検討項目をいくつか示します。

#### ■ IPv6アドレッシング

IPv6アドレスには、大きく分けてグローバルアドレスとリンクローカルアドレスの2種類があります。また、機器へのIPv6アドレス付与方法には、固定的な割り当てとなる手動方式と、MACアドレスから算出するEUI-64方式があります。このようなことから、各ネットワーク機器に対して、インターフェースにグローバルアドレスを付与するのか、リンクローカルアドレスだけにするのか、IPv6アドレスを手動割り当てにするのか、EUI-64方式とするのか、といったことを検討する必要があります。さらに、サーバ機器やクライアント端末では、IPv6特有の匿名アドレス（RFC3041）の使用を許可するのかどうかの検討も必要です。

#### ■ DNSの名前の付け方

通常、システムをIPv4とIPv6のデュアルスタックにする場合、最も標準的な名前（例えばwww.example.co.jp）をデュアルスタック名に指定するでしょう。ただし、このような名前付けには、サーバを運用しているエンジニア自身がIPv4とIPv6のどちらで通信しているのかが分からないという、運用上の課題が潜んでいます。この課題の解決策には、例えばwww-v4.

**パターン 1：トンネル接続方式**

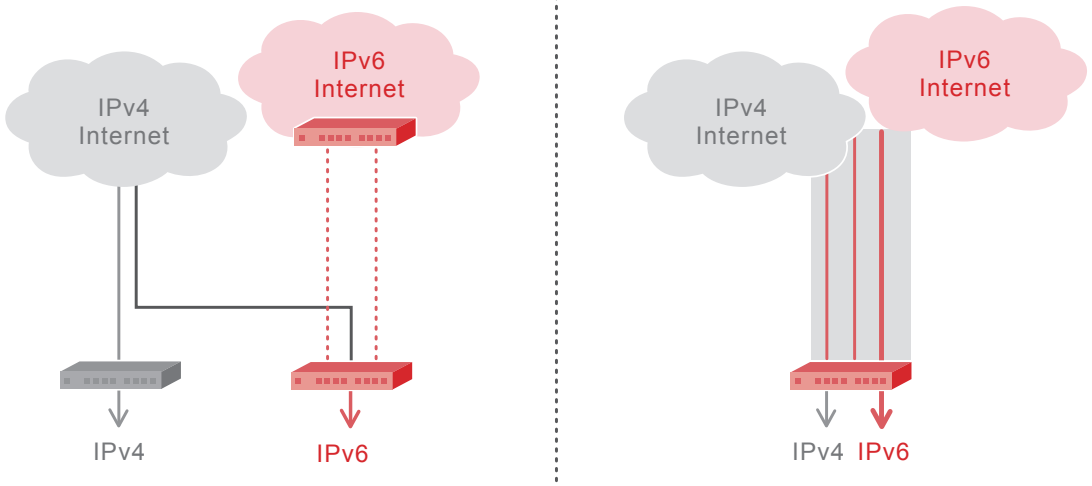



**図-2　ネットワークへのIPv6の導入方法**

example.co.jpをIPv4の名前、www-v6.example.co.jpをIPv6の名前として返すといった命名ルールでの工夫などがあります。

### ■ IPv6スキルアップ

情報システムにIPv6を導入する場合、そのシステムに携わるあらゆる人々がIPv6に関するスキルを身につけておく必要があります。しかし、現状では、多くの企業でIPv6を扱えるエンジニアが不足しているため、社内エンジニアのIPv6スキル向上といった課題があります。

### ■ ネットワークへのIPv6の導入

ネットワークへのIPv6の導入方法は、大きく分けて2つあります。トンネル方式とデュアルスタック方式です。トンネル方式は、既存のIPv4ネットワーク上にIPv6トンネルルータを設置し、IPv6パケットをIPv4でカプセル化して転送する方式です。これに対してデュアルスタック方式は、回線とルータにIPv4とIPv6の両方を混在して転送できるようにする方式です。

### ■ サーバへのIPv6の導入

サーバへのIPv6の導入方法も、大きく分けて2つあります。トランスレータ方式とデュアルスタック方式です。トランスレータ方式では、既存のサーバにいっさい手を加えず、サーバの手前にトランスレータ装置を設置します。トランスレータ装置によってIPv6パケットがIPv4パケットに変換され、既存のサーバに転送されます。これに対してデュアルスタック方式は、サーバ自体でIPv4とIPv6の両方を扱えるようにする方式です。

## 3.5 まとめ

このように、現在、IPv4アドレスの在庫枯渇問題は、目前に迫ったものになっています。在庫の枯渇によってIPv4アドレス分配のポリシが変更され、IPv4アドレスの共有やIPv6の導入でユーザ環境が変わるなど、これまでに経験したことがない変化が起こることが予想されます。IIJは、業界活動等を通して枯渇問題に対応し、IPv6の早期導入によってインターネット全体が今後も魅力あるものであり続けられるように取り組むとともに、お客様が必要とする情報を提供してお客様の組織に合った対応が進められるように支援し続けます。

**パターン 1：トランスレータ方式**

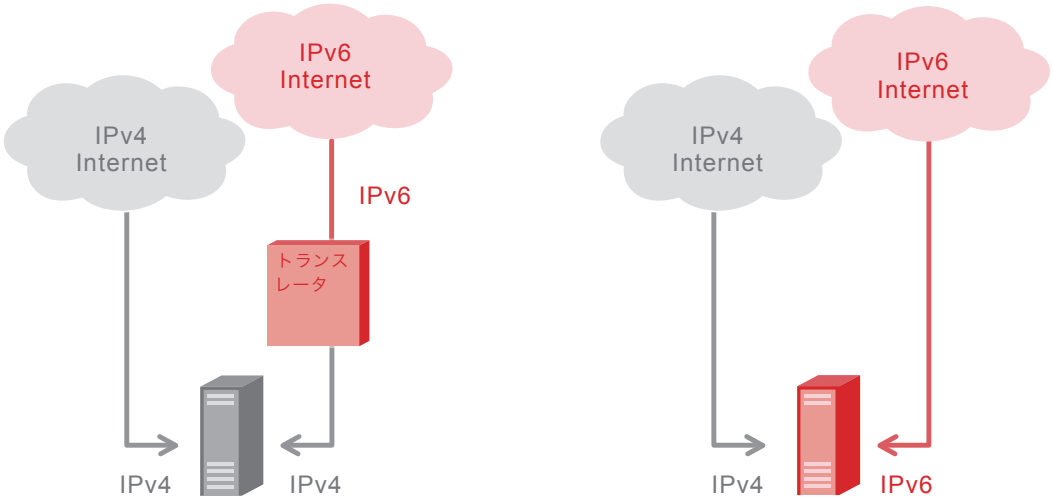



**図-3　サーバへのIPv6の導入方法**

執筆者：
**松崎 吉伸（まつざき よしのぶ）**
IIJ ネットワークサービス本部 ネットワークサービス部 技術推進課 シニアエンジニア。あれこれ面白しろそうな事を見つけては頑張っている。
IIJ-SECTメンバ、The Asia Pacific OperatorS Forum co-chair、APNIC IPv6 SIG chair、JPCERT/CC専門委員。

**加賀 康之（かが やすゆき）**
IIJ サービス本部 サービスインテグレーション部 サービスマネジメント課 コンサルタント。企業ネットワークの構築やコンサルティングに従事。
現在はIPv6導入に関するコンサルティングを担当。

## インターネットトピック: 日本シーサート協議会

### ■日本シーサート協議会とその活動

日本シーサート協議会*1 は、日本国内におけるシーサート(Computer Security Incident Response Team: CSIRT)組織の協調や情報交換を行うことで、会員組織の事案対応能力の向上を目指す団体として 2007年3月に発足しました。協議会発足時は6つのシーサートが会員でしたが、本稿執筆時点では17の組織が加盟しています*2。

一口にシーサートといってもその定義は様々ですが*3、ここでは、保護対象(constituency)となる組織や集団を持ち、そこで発生したセキュリティ事件の解決そのものや、事案の早期検出、分析結果等を用いた注意喚起で保護対象のセキュリティ向上を目的とした活動を行っている組織と考えられています。また、これらの活動のために外部組織との連携窓口機能を持つことも特徴です。現在日本シーサート協議会に集まったチームは、セキュリティ専門企業から、IT系の事業者、IIJのようなISPまで多岐にわたっています。

この協議会では、会員が集って推進するWorking Groupを活動単位としています。その内容としては、実際の事案情報の共有、その対策技術の調査、情報交換方法の検討、現状のシーサートにかかわる課題の検討、外部組織との連携等、広範囲な活動を実施しています。例えば、実際の事案情報の共有については、その情報を会員内で交換するだけではなく、得られた情報をまとめて一般に対する注意喚起として公開しています*4。

執筆者:
**齋藤 衛(さいとう まもる)**
IIJ サービス本部 セキュリティ情報統括室 室長

### ■国際連携ワークショップ

日本シーサート協議会では、外部連携の取り組みとして国内外の他の関連団体と連携を行っています。例えばシーサートの国際団体であるFIRST*5と共同で日本における会合*6を開催したり、昨年は独自に国際連携ワークショップ*7を開催しました。このワークショップでは、Shadowserver Foundation*8とHoneynet Project*9からそれぞれマルウェア対策やボットネット対策の専門家を招き、第一線で得られた観測情報や対処の方法等についてプレゼンテーションを受け、活発な意見交換を行いました。また、会場に構築された閉環境で、実際にマルウェアを捕獲する環境構築や、ボットネット操作者となる疑似体験を行うことで、通常では得られない知見を体得しました(図-1)。

### ■日本シーサート協議会への加盟について

本稿では日本シーサート協議会の活動について、その一端を紹介しました。現在この協議会に参加する組織はIT系の専門組織が多いのが実情ですが、同じ目的で活動する多くの組織の参加を募ることで、一つの事案に対して多様な知見を集約して早期の解決に役立つ相乗効果を得られることが期待されています。例えば、一般の企業の情報システム部門も、ある種のシーサートであると考えることができますので、ここで紹介したような活動に興味がある組織は参加を検討してみてはいかがでしょうか*10。

図-1　国際連携ワークショップの様子
講師のShadowserver FoundationのRichard Perlotto氏(右)とHoneynet ProjectのDavid Watson氏(左)

＊1　日本シーサート協議会 Nippon CSIRT Association (http://www.nca.gr.jp/)。
＊2　日本シーサート協議会 会員一覧 (http://www.nca.gr.jp/member/index.html)。IIJのシーサートであるIIJ-SECTは、この団体の発足時から加盟している。
＊3　例えば米国の CERT/CC による CSIRT FAQ (http://www.cert.org/csirts/csirt_faq.html) や、EUのENISAによる What is CSIRT (http://www.enisa.europa.eu/act/cert/support/guide2/introduction/what-is-csirt) などを参照のこと。IIJのようなISPにおけるCSIRT活動については RFC3013 (BCP46) (http://www.ietf.org/rfc/rfc3013.txt) においても言及されている。
＊4　たとえば、Gumblar対策 (http://www.nca.gr.jp/2010/netanzen/index.html)、PushDo (http://www.nca.gr.jp/2010/pushdo-ssl-ddos/index.html)、Stuxnet(http://www.nca.gr.jp/2010/stuxnet/index.html) 等。
＊5　FIRSTについては本レポートVol.3「インターネットトピック: 21st Annual FIRST Conferenceについて」(http://www.iij.ad.jp/development/iir/pdf/iir_vol03_topic.pdf) を参照のこと。
＊6　Joint Workshop on Security 2008, Tokyo (http://www.nca.gr.jp/jws2008/index.html)。
＊7　詳細はNCA2010イベント 国際連携ワークショップ参加レポート (http://www.nca.gr.jp/2010/event/index.html) を参照のこと。
＊8　The Shadowserver Foundation (http://www.shadowserver.org/wiki/)。
＊9　The Honeynet Project (https://www.honeynet.org/)。
＊10　加盟資格や手続きに関する詳細は、日本シーサート協議会加盟について (http://www.nca.gr.jp/admission/index.html) を参照のこと。加盟には既存会員組織による推薦が必要。この推薦はIIJでも行っている。

Ongoing Innovation

Vol.10 February 2011

**株式会社インターネットイニシアティブ(IIJ)について**

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。

現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービス等、高品質なシステム環境をトータルに提供しています。

また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

**株式会社インターネットイニシアティブ**

〒101-0051 東京都千代田区神田神保町1-105　神保町三井ビルディング
E-mail：info@iij.ad.jp　URL：http//www.iij.ad.jp/



IIJ-MKTG019JA-1102KO-08000PR