Internet Infrastructure Review

IIJ
Internet Initiative Japan

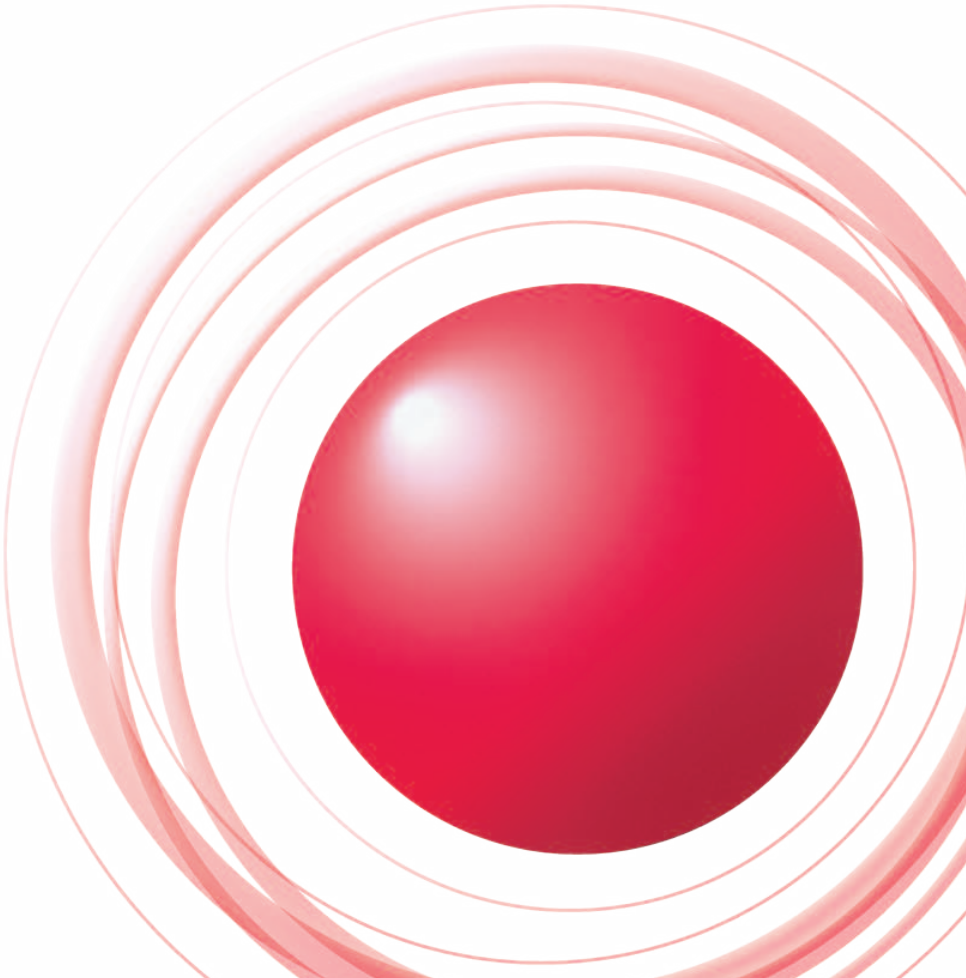
Vol.7

May
2010

インフラストラクチャセキュリティ
標的型攻撃とOperation Aurora

インターネットオペレーション
経路制御の現状と異常経路検出時の対処

メッセージングテクノロジー
メールアドレスの国際化アプローチに対する考察



Internet Infrastructure Review Vol.7 May 2010

■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

インターネットは未だに日々成長を続けているネットワークです。総務省が発表した2009年11月時点での日本国内のダウンロードトラフィック量は、１年前と比べて約1.4倍の1.3Tbpsとなりました。また、利用者数に関しても、同じく総務省発表のデータによれば、2009年は前年から317万人増えて9,408万人となり、割合としては小さいですが増加傾向は続いています。そして、トラフィック量の増加率とユーザ数の増加率を比べてみると、一人当たりのトラフィック量は1年で平均30%程度増加している事が解ります。この増加の原因としては、インターネットの利用方法の多様化や、流通しているコンテンツのリッチ化などが考えられます。

それに伴い、インターネットインフラストラクチャーの状況も日々刻々と変化しています。昨日まで安全だと考えられていた利用方法にセキュリティ上の問題が見つかったり、新たな機能の実現や利便性の向上の為の施策に思わぬ落し穴が隠れていたりします。IIJを始めとするインターネットプロバイダはこのような問題や落し穴をできる限り速やかに発見し対策を取る為に、日々問題の調査・解析や、その対策のための技術開発を積み重ねています。

本レポートは、IIJがインターネットというインフラを整備・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1月から3 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、Gumblar型の攻撃スキームを持つ「ru:8080」についての詳細レポート、2010年1月に公表された標的型攻撃「Operation Aurora」についての解説、そして、IIJが実施しているマルウェア対策活動である「MITF（Malware Investigation Task Force）」の概要についてご紹介します。

「インターネットオペレーション」の章では、ISP間で用いられる経路制御プロトコルであるBGPの動作概要を示し、経路数の現状や「権威なき広報」の問題について触れ、日本国内での異常経路検出の為の取り組みや、ルータが受け取った経路情報が正しいかどうかを判別する為の仕組みであるRPKI（Resource Public Key Infrastructure）の展開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１月から３月までの12週間の迷惑メールの状況の推移や、送信ドメイン認証の導入状況についての報告を行います。また、メールアドレスの国際化の取り組みであるEAI（Email Address Internationalization）について紹介し、そのアプローチの問題点を考察します。

また、「インターネットトピック」として、IIJが2010年2月から実施しているモジュール型エコ・データセンター実証実験について簡単にご紹介しています。

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。

標的型攻撃とOperation Aurora

今回は、2010年1月から3月に発生したインシデントに関する報告とともに、昨年12月以降発生しているGumblar類似の事件と、米国の企業を対象にした標的型攻撃について解説し、IIJのマルウェア対策活動MITFとその技術について取り上げます。

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1月から3月までの期間では、前回のレポートで取り上げた、IDとパスワードを盗み取るマルウェアGumblarとその類似のインシデントの発生が継続し、関連するWebサイトの改ざんが数多く報告されています。また、脆弱性に関しても、Webブラウザに関連するものやサーバに影響を与えるものが相次いで発見されています。このほかのインシデントとして、DNS情報を不正に操作したサービスの乗っ取りや、天災に便乗したSEOポイズニング事件などが発生しています。そして、米国の複数の大手企業を対象にした標的型攻撃が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1月から3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]。

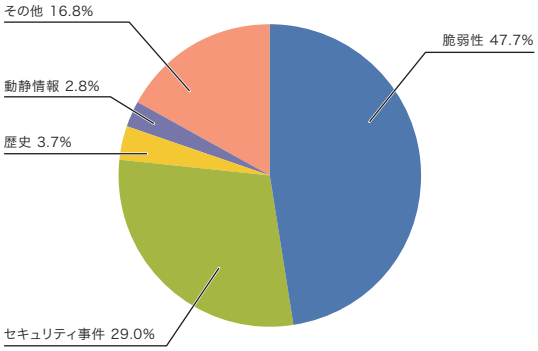


図-1　カテゴリ別比率（2010年1月～3月）

＊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では、マイクロソフト社のInternet Explorer[*2][*3]、アドビ社のAdobe ReaderとAcrobat[*4][*5]、Flash Player[*6][*7]、製品のアップデートに利用されているAdobe Download Manager[*8]、リアルネットワークス社のReal Player[*9]やオラクル社のJava Runtime Environment（JRE）[*10]など、Webブラウザ自体とそのプラグインに関する脆弱性が数多く発見され、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、DNSサーバのBIND9[*11]、プロキシサーバに利用されるSquid[*12]、Oracle Database[*13]等、広く利用されているサーバや、Linux Kernel[*14]やMac OS[*15][*16]等のOSに関する脆弱性、ジュニパーネットワークス社のJUNOS[*17]やシスコシステムズ社のCisco IOS[*18]等のルータ製品に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、2月に開催されたバンクーバーオリンピックなどに注目しましたが、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す。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上では直接関連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、中国の検索サイトである百度（Baidu）のDNS情報が不正に操作され、別のWebサイトに誘導される事件[*19]が発生しました。またハイチ地震やチリ地震などの自然災害の発生に付け込んで、検索エンジンなどの検索結果から詐欺的ソフトウェア（スケアウェア）に誘導する事件も発生しています[*20]。さらに、P2Pファイル共有ネットワーク上の著作権法違反のコンテンツに対し、著作権団体を装ったり、マルウェアを悪用して金銭を請求する事件も報告されています[*21]。

＊2　マイクロソフト セキュリティ情報 MS10-002 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム（978207）（http://www.microsoft.com/japan/technet/security/Bulletin/MS10-002.mspx）。
＊3　マイクロソフト セキュリティ情報 MS10-018 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム（980182）（http://www.microsoft.com/japan/technet/security/Bulletin/MS10-018.mspx）。
＊4　Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB10-02（http://www.adobe.com/jp/support/security/bulletins/apsb10-02.html）。
＊5　Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB10-07（http://www.adobe.com/jp/support/security/bulletins/apsb10-07.html）。
＊6　Adobe Flash Player用セキュリティアップデート公開 APSB10-06（http://www.adobe.com/jp/support/security/bulletins/apsb10-06.html）。
＊7　マイクロソフト セキュリティ アドバイザリ（979267）Windows XPで提供される Adobe Flash Player 6の脆弱性により、リモートでコードが実行される（http://www.microsoft.com/japan/technet/security/advisory/979267.mspx）。
＊8　Adobe Download Manager用セキュリティアップデート公開 APSB10-08（http://www.adobe.com/jp/support/security/bulletins/apsb10-08.html）。
＊9　RealNetworks, Inc.、セキュリティ脆弱性に対応するアップデートをリリース（http://service.real.com/realplayer/security/01192010_player/ja/）。
＊10　JavaTM SE 6 アップデートリリースノート（http://java.sun.com/javase/ja/6/webnotes/6u19.html）。
＊11　JVNVU#360341 BIND 9のDNSSEC検証コードに脆弱性（http://jvn.jp/cert/JVNVU360341/index.html）。
＊12　Squid Proxy Cache Security Update Advisory SQUID-2010:1 Denial of Service issue in DNS handling（http://www.squid-cache.org/Advisories/SQUID-2010_1.txt）。
＊13　Oracle Critical Patch Update Advisory - January 2010（http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html）。
＊14　JVNVU#571860 Linux カーネルの IPv6 jumbogram 処理に脆弱性（http://jvn.jp/cert/JVNVU571860/index.html）。
＊15　セキュリティアップデート 2010-001 について（http://support.apple.com/kb/HT4004?viewlocale=ja_JP）。
＊16　セキュリティアップデート 2010-002 ／ Mac OS X v10.6.3のセキュリティコンテンツについて（http://support.apple.com/kb/HT4077?viewlocale=ja_JP）。
＊17　PSN-2010-01-623:JUNOS kernel cores when it receives an crafted TCP option.（https://www.juniper.net/alerts/viewalert.jsp?actionBtn=Search&txtAlertNumber=PSN-2010-01-623&viewMode=view）（参照にはユーザ登録が必要）。
＊18　Cisco Systems, Inc. Summary of Cisco IOS Software Bundled Advisories, March 24, 2010（http://www.cisco.com/JP/support/public/ht/security/107/1076221/cisco-sa-20100324-bundle-j.shtml）。
＊19　この件に関しては次のトレンドマイクロ社のBlogに詳しい。 Iranian “Cyber Army” Strikes at China’s Search Engine Giant, Chinese Hackers Retaliate（http://blog.trendmicro.com/iranian-cyber-army-strikes-at-china%e2%80%99s-search-engine-giant-chinese-hackers-retaliate/）。
＊20　ハイチ地震に関するSEOポイズニングについては次のエフセキュアブログに詳しい。ハイチ地震：新たなローグがニュースを悪用（http://blog.f-secure.jp/archives/50335541.html）。
＊21　この事件についてはエフセキュアブログに詳しい。ICCP著作権財団は偽物（http://blog.f-secure.jp/archives/50388533.html）。

マルウェアの活動では、昨年より継続しているGumblarとそれに類似した事件[*22]が活発になり、多くの企業のWebサイトで改ざんによる被害が確認されました。この事件に関しては「1.4.1 Gumblar型の攻撃スキームを持つ ru:8080」を参照してください。

また、Pushdoと呼ばれるボット型マルウェアによる目的不明なSSLの通信が、特定多数のWebサーバに対して行われていることも確認されています[*23]。さらに、ボットネットmiraposaを運用していたグループがスペインで摘発されたり[*24]、ボットネットWaledacに対しマイクロソフト社がサーバをテイクダウンする[*25]など、ボットネットに対する取り組みが複数行われました。加えて、Internet Explorerの脆弱性を利用した標的型攻撃[*26]により複数の米国企業で被害が発生しています。この標的型攻撃に関しては「1.4.2　標的型攻撃とOperation Aurora」を参照してください。

■ その他

その他の事件としては、国内の利用者が多いインターネット掲示板が3月に大規模な攻撃を受け、利用に支障が生じる等の影響が発生しました。

その他のセキュリティに関係する情報としては、まず、スマートフォンに対する攻撃手法の研究が続けて発表されました[*27]。また、昨年発見されたTLSのrenegotiation機能に関係するプロトコルの脆弱性[*28]に対して、この脆弱性を修正した通信プロトコルを規定するRFC5746が発行されました[*29]。さらに、昨年度発生したセキュリティ事件をまとめた文書「2010年版10大脅威」がIPAから発表[*30]されています。

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います。ここでは、そのうちDDoS攻撃、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います。DDoS攻撃の内容は、状況により多岐にわたりますが、一般には、脆弱性等の高度な知識を利用した攻撃ではなく、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。図-2に、2010年1月から3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。

＊22 JPCERT/CC Alert 2010-01-07:Webサイト改ざん及びいわゆるGumblarウイルス感染拡大に関する注意喚起（https://www.jpcert.or.jp/at/2010/at100001.txt）。
＊23 この攻撃に関する詳細は次の報告などが詳しい。Shadowserver Foundation:Pushdo DDoS'ing or Blending In?（http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20100129）。
＊24 この事件についての詳細は次のPanda Security社のブログに詳しい。 Panda Security Japan ブログ:史上最大規模、Mariposaボットネットの摘発（http://pandajapanblogs.blogspot.com/2010/03/mariposa.html）。
＊25 この件については次のマイクロソフト社のブログに詳しい。The Official Microsoft Blog:Cracking Down on Botnets（http://blogs.technet.com/microsoft_blog/archive/2010/02/25/cracking-down-on-botnets.aspx）。
＊26 米国ではこの脅威に対してUS-CERTが注意喚起を行うなど重大な脅威として取り扱っている Technical Cyber Security Alert TA10-055A:Malicious Activity Associated with "Aurora" Internet Explorer Exploit（http://www.us-cert.gov/cas/techalerts/TA10-055A.html）。
＊27 BlackBerryとiPhoneに関する独立した研究がそれぞれ別のカンファレンスで発表された。Tyler ShieldsによるBlackberry Mobile Spyware - The Monkey Steals the Berries（http://www.shmoocon.org/presentations-all.html#monkeyberry）およびNicolas Seriotによるiphone Privacy（http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html#Seriot）。
＊28 この脆弱性については本レポートのVol.6「1.4.2 SSLおよびTLSのrenegotiation機能の脆弱性を利用した中間者攻撃」にて解説を行っている。（http://www.iij.ad.jp/development/iir/pdf/iir_vol06.pdf）。
＊29 IETF RFC5746 Transport Layer Security（TLS）Renegotiation Indication Extension（http://www.rfc-editor.org/rfc/rfc5746.txt）。
＊30 IPA（独立行政法人情報処理推進機構）による「2010年版 10大脅威」（http://www.ipa.go.jp/security/vuln/10threats2010.html）。

ここでは、IIJ DDoS対策サービスの基準で攻撃と判定した通信異常の件数を示しています。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、正確な攻撃の実態を把握することが困難なため、この集計からは除外しています。

DDoS攻撃には多くの攻撃手法が存在します。また、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*31、サーバに対する攻撃*32、複合攻撃（1つの攻撃対象に対して同時に数種類の攻撃を行うもの）の3種類に分類しています。

この3ヵ月間でIIJは、227件のDDoS攻撃に対処しました。1日あたりの対処件数は2.52件で、平均発生件数は前回のレポート期間のものと大きく変わっていません。

DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0%、サーバに対する攻撃が86%、複合攻撃が14%でした。今回の対象期間で観測されたもっとも大規模な攻撃は、サーバに対する攻撃に分類したもので、3万ppsのパケットによって105Mbpsの通信量を発生させたものです。また、攻撃の継続時間は、全体の86%が攻撃開始から30分未満で終了し、14%が30分以上24時間未満の範囲に分布しています。今回の期間中では24時間以上継続する攻撃は見られませんでした。

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ています。これは、IPスプーフィング*33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*34の利用によるものと考えられます。

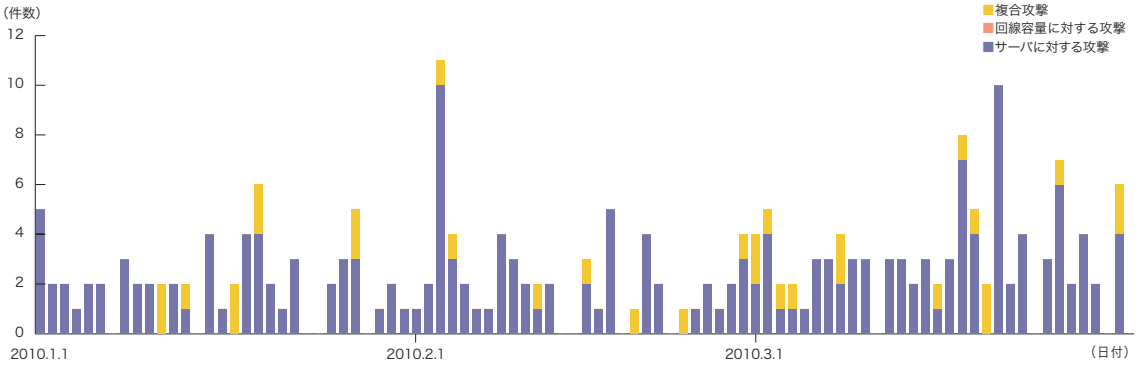


図-2　DDoS攻撃の発生件数

＊31 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。

＊32 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。

＊33 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、発信すること。

＊34 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。

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*35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*36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1月から3月までの期間中に、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-3に、その発信元IPアドレスの国別分類を図-4にそれぞれ示します。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、前回のレポート期間と同様に、シマンテックのクライアントソフトウエアが利用する2967/TCP、SSHで利用する22/TCPに対する探索行為が観測されています。一方で、2582/TCP、11999/TCP等、一般的なアプリケーションで利用されていない目的不明な通信も観測されました。発信元の国別分類を見ると、中国の17.9 %、日本国内の15.9%、ベトナムの9.9%が比較的大きな割合を占めています。

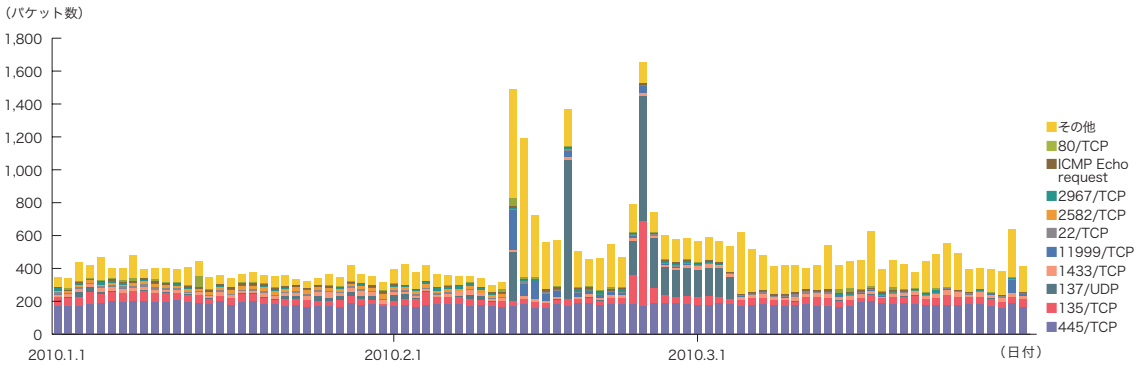


図-3　ハニーポットに到着した通信の推移（日別・宛先ポート別・一台あたり）

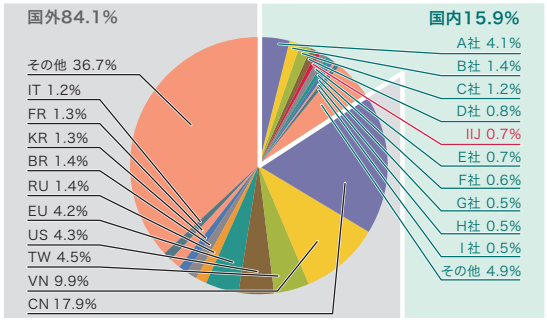


図-4　発信元の分布（国別分類、全期間）

＊35 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。

＊36 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。

■ 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-5に、マルウェアの検体取得元の分布を図-6にそれぞれ示します。図-5では、1日あたりに取得した検体[*37]の総数を総取得検体数、検体の種類をハッシュ値[*38]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479、ユニーク検体数が37です。前回の集計期間での平均値が総取得検体数で623、ユニーク検体数で44でした。今回は、総取得検体数、検体の種類を表すユニーク検体数ともに、前回より減少傾向が見られました。

検体取得元の分布では、日本国内が61.3%、国外が38.7%でした。このうちIIJのユーザ同士のマルウェア感染活動は0.1%で、前回の観測期間に続いて低い値を示しています。

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。この結果、この期間に取得した検体は、ワーム型が14.3%、ボット型が84.6%、ダウンローダ型が1.1%となりました。また、この解析により、42個のボットネットC&Cサーバ[*39]と96個のマルウェア配布サイトの存在を確認しています。

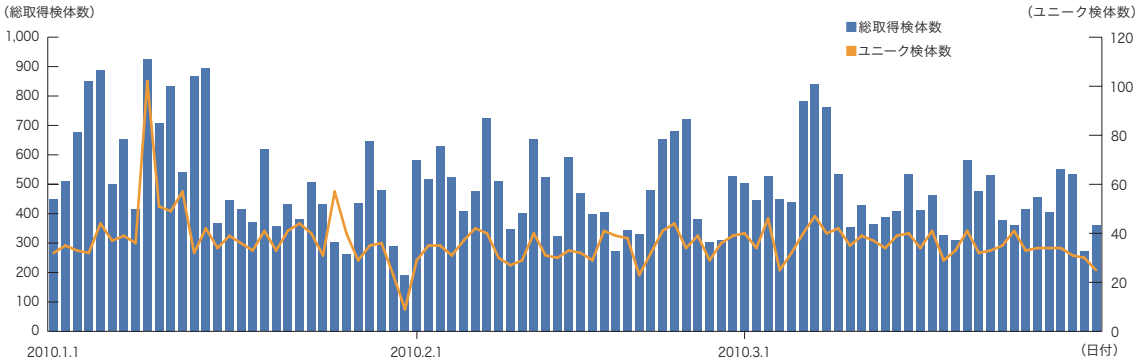


図-5　取得検体数の推移(総数、ユニーク検体数)

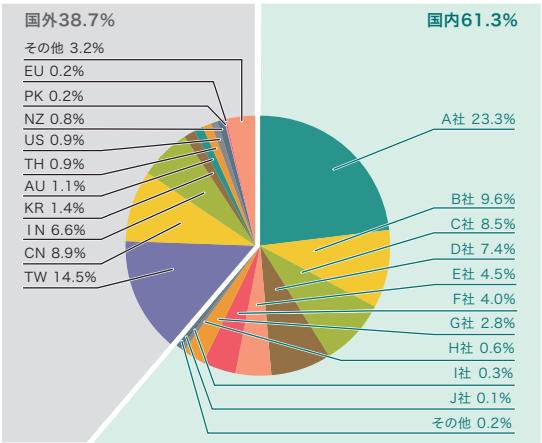


図-6　検体取得元の分布 (国別分類、全期間)

＊37 ここでは、ハニーポット等で取得したマルウェアを指す。

＊38 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。

＊39 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。

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*40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-7に、攻撃の発信元の分布を図-8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、日本が60.4%、中国が10.0%、米国が9.5%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生状況は、前回と同様の発生数となっています。

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

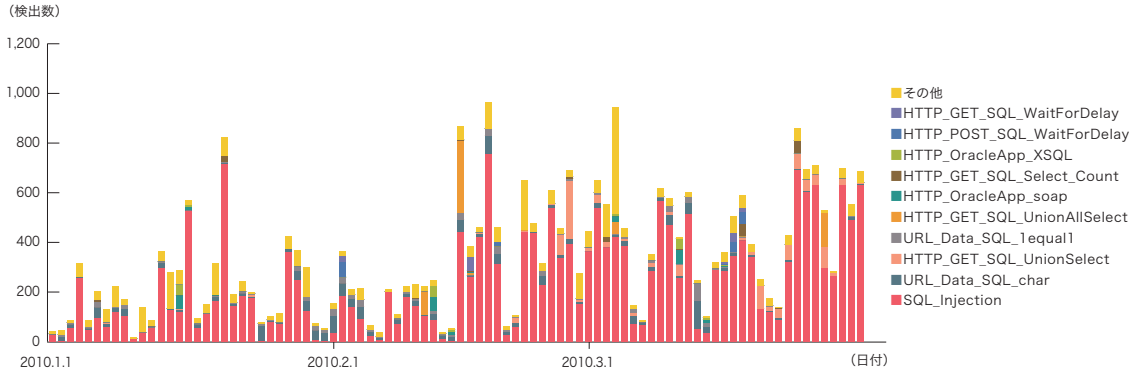


図-7　SQLインジェクション攻撃の推移（日別、攻撃種類別）

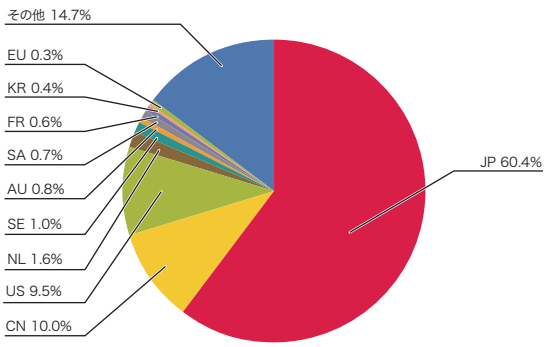


図-8　SQLインジェクション攻撃の発信元の分布（国別分類、全期間）

＊40 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行うことで対策につなげています。ここでは、この期間に実施した調査のうち、Gumblar型の攻撃スキームを持つru:8080、標的型攻撃とOperation Auroraについて解説します。また、IIJが実施しているマルウェア対策活動MITFについても、その概要を示します。

1.4.1 Gumblar型の攻撃スキームを持つ ru:8080

ru:8080の攻撃スキームはGumblar[*41]と同様のものです。攻撃者は、あらかじめ盗み出しておいたFTPのIDとパスワードを悪用し、Webコンテンツを改ざんします。そして、そのWebコンテンツを閲覧したユーザを悪意のあるサイトに誘導し、マルウェアに感染させ、さらにIDとパスワードを盗み出して改ざんを繰り返し、被害を拡大します。この事件は2009年12月から活性化[*42]し、有名企業を含む多数のWebサイトが改ざん被害に遭ったため、Gumblarと同様に報道等でも取り上げられました[*43]。ただし、使われたマルウェア、盗み出すIDやパスワードの種類やその手法、脆弱性の悪用手法など、ru:8080は多くの点でGumblarと異なっています。

■ Gumblarとの相違点

ru:8080は、FTPのIDとパスワードを盗み出すだけでなく、HTTP、SMTP、POP3のIDとパスワードも盗み出します。その際、通信の盗聴に加えて、Webブラウザ やFTPクライアントに保存されている認証情報も盗み出す[*44]ことが大きな特徴です（図-9）。特に、Webブラウザに保存されたWebサイトの認証情報には、SNS、Webメール、オンラインショッピング、オンラインバンキング等で使用される、金銭や個人に関する重要な情報を管理するための認証情報が含まれているため、直接金銭や個人情報等の被害につながる可能性があります。

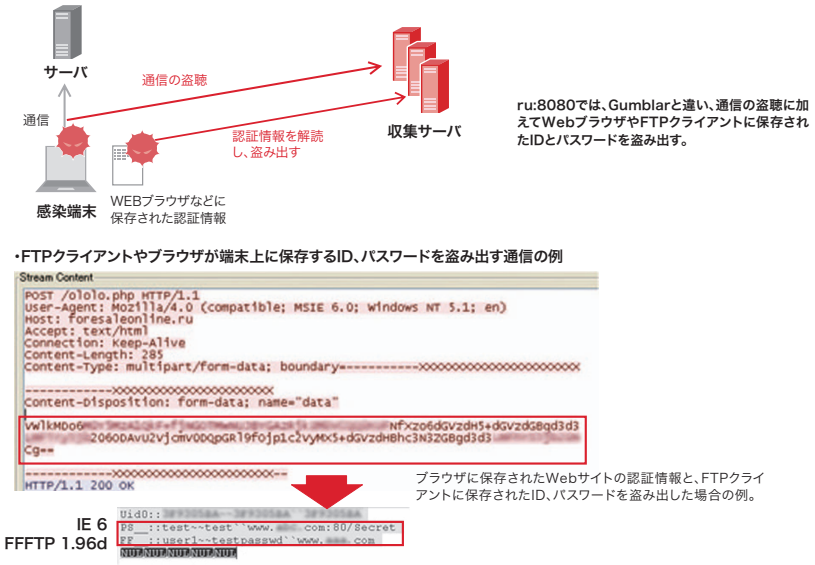


図-9　ru:8080がIDとパスワードを盗み出す手法

＊41 Gumblarについては本レポートの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）、及びVol.6「1.4.1 Gumblarの再流行」（http://www.iij.ad.jp/development/iir/pdf/iir_vol06.pdf）において解説している。

＊42 ru:8080は本稿執筆時点（2010年4月）でも活動を継続している。また2009年12月末に鎮静化したGumblarも2010年2月に活動を再開している様子が観測されている。

＊43 この事件ではGumblarと同様にFTPアカウントを盗み出すことから、Gumblar亜種や新型Gumblar、カタカナでガンブラー等と表記され、報道等では一緒に扱われることもあった。また、挿入するスクリプトのコメントにGNU GPLという文字列が入っていたことからGNU GPL マルウェアと呼ばれたり、誘導先のFQDNがロシア（ru）に帰結（ただしそのIPアドレスのほとんどはフランスなどの４つのAS番号に存在）し、TCPポート8080番が使われていることからru:8080、Gumblar.8080等とも呼ばれていた。しかし専門家の間では、悪用する脆弱性の種類やマルウェアなどが全く異なることから、Gumblarとは別のものとして扱うことも多い。本レポートではオリジナルのGumblarと区別するために、ru:8080という名称を用いる。

＊44 JPCERT/CCの調査で、多くのFTPクライアントやWEBブラウザに保存された認証情報を盗み出すことが確認されている。FTP アカウント情報を盗むマルウエアに関する注意喚起（http://www.jpcert.or.jp/at/2010/at100005.txt）。この問題への対策として、現在保存しているIDとパスワードの情報を削除したとしても、利用しているクライアントソフトウェアによっては、設定ファイルやレジストリにID、パスワードが残されたままになっている場合もあるので注意が必要である。

その他にもボットをインストールして迷惑メールを送信したり、スケアウェア*45をインストールしてユーザを騙して金銭を直接詐取しようとするなど、その悪性活動は多岐に渡ります。また、感染手法もGumblarに比べて強化されています（表１）。特に、Adobe Readerの脆弱性への攻撃は、悪用時には対策が存在しない0-day攻撃であったため、被害がより大きくなったと考えられます*46。

■ マルウェアの動作

ru:8080で使われているマルウェアは、ダウンローダ型*47のマルウェアであり、感染後にサーバから２～５種類のマルウェアをダウンロードします*48。これらマルウェアのいくつかは、ファイルとして保存されない*49ため、発見が困難です。また、ダウンロードされるマルウェアの数や種類も時間の経過とともに変化しています。2010年1月初旬にru:8080のマルウェアがダウンロードしたマルウェア群の一覧を図-10に示します。この時点では、IDとパスワードを盗み出すマルウェアとともに、ボット（Waledacや後にPushdo等）、スケアウェア（Security tool）、rootkitなどをインストールしています。

ソフトウェア	バージョン	脆弱性	Gumblar	ru:8080
Internet Explorer	== 7	MS09-002	●※	
Microsoft Video ActiveX Control	<= XP SP3	MS09-032		●※
Microsoft Office	<= 2003 SP3	MS09-043	●	
MDAC	<= 2.8 SP2	MS06-014	●	●
	<= 2.8 SP2	MS07-009	●	
Microsoft Access Snapshot Viewer	-	MS08-041		●
Adobe Flash	< 9.0.124	CVE-2007-0071	●	
	<10.0.23	CVE-2009-1862	●	
Adobe Reader / Acrobat	< 8.1.1	CVE-2007-5659		●
	< 8.1.2	CVE-2008-0655	●	
	< 8.1.3	CVE-2009-0927	●	
	< 8.1.3	CVE-2008-2992	●	●
	< 9.2.1	CVE-2009-4324		●
Java（JRE）	< 1.6.11	CVE-2008-5353	●	●
AOL Radio AmpX ActiveX	<= 2.4.0.6	BID:35028		●

赤字は 事件発生時点で 0-day 攻撃であった脆弱性　※IIJ では未確認

表-1　Exploitに利用される脆弱性の比較

■ 対策にむけて

ru:8080とサーバ間の通信内容はエンコードされ、復号キーはRFCに違反したHTTPヘッダとして追加されています*50。この通信をWAFやIPSなどで検知して防御することで、マルウェアの動作を実質的に無力化できます*51。IIJでは、取得したマルウェアを解析してえられたこれらの特徴を、サービスでのアクセス制御に反映しています。また、さまざまな団体の活動*52に積極的に参加し、複数の事業者間でより効果的な対策を実施するための情報交換や対策手法も検討しています。

Gumblarやru:8080に限らず、今後も同種の事件は発生し続けると考えられます。このため、状況の変化に応じながら、継続的に予防や対策の活動を行っていくことが必要です。特に、ru:8080では、アプリケーションに保存したパスワードが盗まれるという点が大きな脅威となっています。アプリケーションごとに保存された情報の安全性を個別に評価し、対策を実施することは困難であることから、パスワード管理ツール等の利用で包括的に防御することが考えられます。

＊45 金銭を詐取する詐欺行為を手助けするソフトウェア。スケアウェアについてはIIR Vol.3の「1.4.3 スケアウェア」において解説している（http://www.iij.ad.jp/development/iir/pdf/iir_vol03.pdf）。

＊46 この脆弱性は2010年1月12日に修正がリリースされている。Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB10-02（http://www.adobe.com/jp/support/security/bulletins/apsb10-02.html）。

＊47 主にサーバから追加機能をダウンロードするためのマルウェア。機能をダウンロードと実行のみに限定して小型化することで、ウイルス対策製品等による検知を迂回する狙いがある。従来のGumblarはドロッパ型であり、情報の盗難を行うマルウェアを内部に格納しているため、Gamblarが実行されると即座に情報が盗み出される可能性があった。ru:8080ではこのような機能を別途マルウェアをダウンロードして実行するため、ダウンロードに利用されるHTTP等の通信を阻害することで情報盗難の被害を比較的容易に防ぐことができる。

＊48 ru:8080が接続するダウンロードサイトは数週間ごとに変更されていた。IIJが確認した限りでは、例えば2009年12月28日から2010年1月12日はforhomessale.ru、2010年1月7日から2月10日はyourarray.ru、2月5日から2月27日はexitguide.ru、2月26日から3月18日はstelane.ruなど。

＊49 エンコードしたマルウェアをダウンロードし、ファイルとして保存しないでメモリ上の処理だけでデコードした後、直接ほかのプロセスにインジェクションして実行する。このため通信上でもファイルとしてもウイルス対策製品で検出されにくい。

＊50 HTTPレスポンスにMagic-Number: や Entity-Info: など、RFCに違反したヘッダが追加される。これらのヘッダに付随する情報は、エンコードされたマルウェアを復元するために使われる。

＊51 一般には、HTTPリクエストを".ru:8080"でフィルタすることで効果があるとされていたが、本稿執筆時点では .info等、他のTLDの利用も見られるようになっている。これには4月１日より.ruドメイン取得手続きが厳格化されたことが影響していると考えられる。Coordination Center for ccTLD .RU によるアナウンス（http://www.cctld.ru/en/news/news_detail.php?ID=682）。

＊52 例えばWeb感染型マルウェア対策コミュニティ（http://www.fourteenforty.jp/news/WebMalwareCommunity_PR.pdf）やTelecomISAC Japan（https://www.telecom-isac.jp/）、日本シーサート協議会（http://www.nca.gr.jp/）の各種活動等。

1.4.2 標的型攻撃とOperation Aurora

近年、標的型攻撃による被害が問題視されています。2010年1月にグーグル社は、中国における事業の方針転換を表明した公式ブログ記事*53の中で、2009年12月から標的型攻撃を受けていたことを明らかにしました。この攻撃は、Operation Auroraと名付けられ、大きく取り上げられました。

■ 特定の対象を狙う標的型攻撃

標的型攻撃は、特定の組織や人々を対象とした攻撃です。ネットワークワーム感染のように、不特定多数が対象となる無差別の攻撃とは異なり、攻撃の範囲を限定した上で、標的とする組織や人に合わせた話題を用いる等の手法が使われます。典型的な手口は、なりすましメールによる攻撃です。攻撃対象にとって実際に関係する組織や人を発信者にかたったメールを悪用し、表題、本文、添付ファイルに至るまで、いかにも受信者の業務に関係した内容のように思わせ、添付ファイルを開くように誘います。添付ファイルにはアプリケーションの脆弱性を悪用する攻撃コードが含まれていて、添付ファイルを開くとマルウェアに感染させられます。

このマルウェアには、他のマルウェアをダウンロードする等の手法によって、検知や解析を難しくする仕組みを備えたものが多いようです。これらのマルウェアに感染すると、表面上は何ら症状が見られずにマルウェアに潜伏され、気付かないうちに機密情報が盗み取られていく可能性があります(図-11上段)。

■ 標的型攻撃の事例

標的型攻撃は、2005年頃から広く知られるようになりました*54。当初の攻撃対象は、主に政府機関で、日本でも官公庁を狙ったなりすましメールによる攻撃が報じられました*55。その後、企業の経営層を狙った標的型攻撃も報告され始め*56、民間企業等も攻撃対象になることが広く意識されるようになりました。

2008年6月には、コンピュータセキュリティに関するシンポジウムの論文募集アナウンスをかたる標的型攻撃が発生しました*57。メールの本文は正規の文章を切り貼りして作られ、正規のPDFファイルにマルウェアを埋め込んで作られた添付ファイルとともに送付されました。このときの攻撃対象はセキュリティ専門の研究者

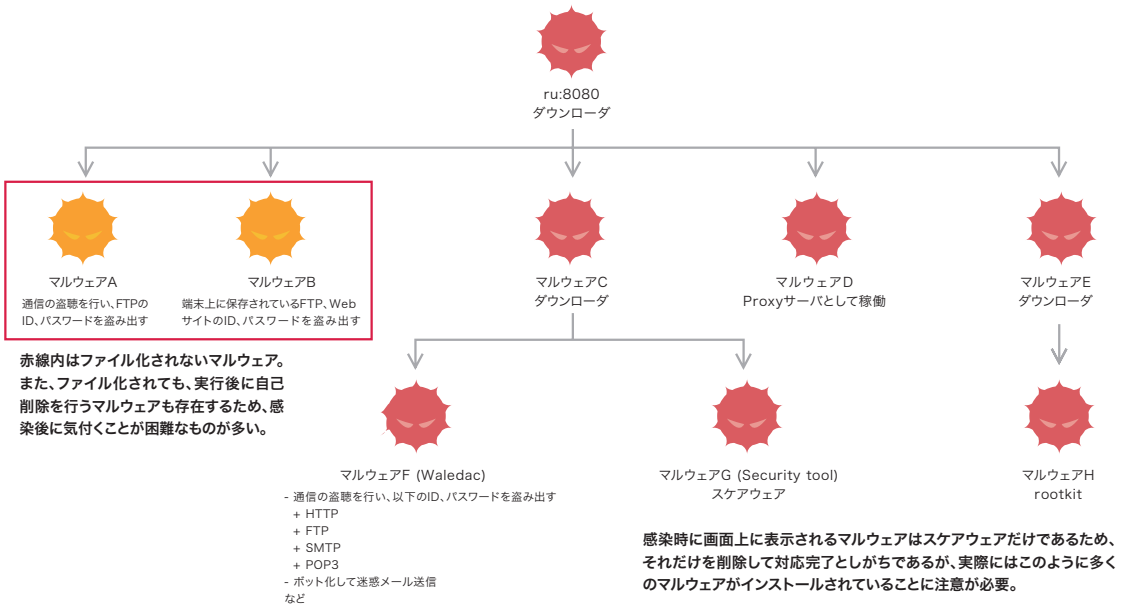


図-10 ru:8080がインストールするマルウェアの一例

＊53 Official Google Blog: A new approach to China (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html)。
＊54 US-CERTによる2005年7月の注意喚起: US-CERT Technical Cyber Security Alert TA05-189A -- Targeted Trojan Email Attacks (http://www.us-cert.gov/cas/techalerts/TA05-189A.html)。
＊55 例えば、外務省による次の注意喚起がある。外務省: 外務省を発信元と詐称するウィルスメールにご注意ください (http://www.mofa.go.jp/mofaj/press/oshirase/18/osrs_0120.html)。
＊56 例えば SANS ISCのHandler's Diary: Better Business Bureau targeted malware spam (http://isc.sans.org/diary.html?storyid=2853)。
＊57 情報処理学会コンピュータセキュリティ研究会による次の報告には、状況推移や対応の記録をはじめ、添付されたマルウェアの解析結果など、詳細な情報がまとまっている。CSS2008のCFPを騙ったウイルスメールに関する情報 (http://www.iwsec.org/csec/css2008-cfp-secinfo.html)。

でした。また、2009年に新型インフルエンザの感染が拡大しつつあった時期に、医療研究機関からの注意喚起を装ったメールが、企業等の組織の新型インフルエンザ対策を担当する人々に送られました*58。

■ Operation Aurora

2010年1月に公表されたOperation Auroraも、民間企業を狙った標的型攻撃と考えることができます。攻撃対象は、グーグル社だけではなく、数十社の米国企業に及んでいます*59。

この事件では、メールやインスタントメッセンジャーを通して悪意のあるWebサイトへのリンクが送られたと言われています。リンクをクリックすると、JavaScriptによりInternet Explorerの未知の脆弱性*60を悪用した0-day攻撃*61が実行され、マルウェアに感染させられました*62。このマルウェアはC&Cサーバに接続し、攻撃者からの命令を受け、ファイルや設定を盗んだり書き込んだりする機能や、新たなマルウェアをダウンロードして実行する等の機能を持っています*63。また、デスクトップ共有の機能も持っており、攻撃者が感染PCの画面を監視でき、自由に操作できる状態になっていました。この様な感染PCを踏み台に、企業内ネットワークにある他のホストの情報にもアクセスされ、ソースコード等の企業秘密が盗まれたとされています(図-11下段)。

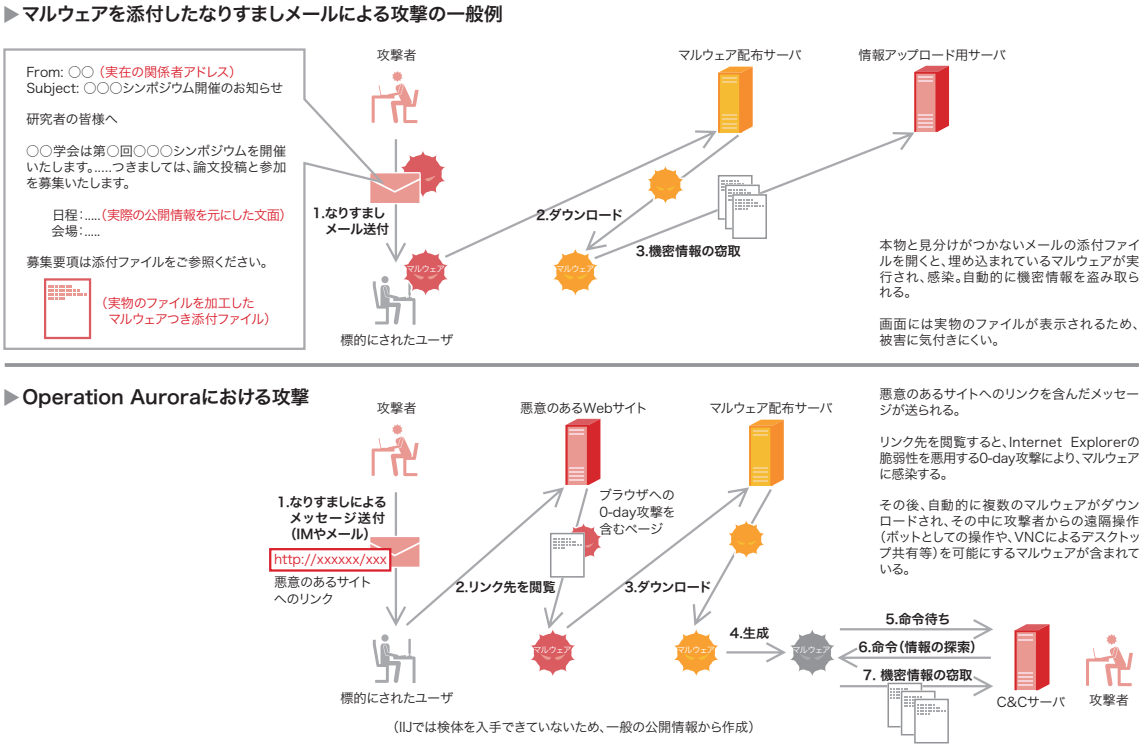


図-11 なりすましメールによる標的型攻撃

＊58 この事例については、本レポートの Vol.4「1.2 インシデントサマリ」で触れている (http://www.iij.ad.jp/development/iir/pdf/iir_vol04.pdf)。
＊59 Operation Auroraについては、US-CERTからも注意喚起のアドバイザリが発行されている (http://www.us-cert.gov/cas/techalerts/TA10-055A.html)。このアドバイザリでは感染ホストの検出に役立つ技術情報も提供されている。
＊60 この脆弱性は、Googleによるブログ記事の公表後、すぐに修正された。マイクロソフト セキュリティ情報MS10-002 - 緊急 :Internet Explorer用の累積的なセキュリティ更新プログラム (978207) (http://www.microsoft.com/japan/technet/security/bulletin/MS10-002.mspx)。
＊61 脆弱性が修正される前に攻撃に悪用されることを0-day (ゼロデイ) 攻撃という。
＊62 この攻撃コードやマルウェアの解析結果は、例えば次のレポートに詳しい。HBGary Threat Report: Operation Aurora (http://www.hbgary.com/press/hbgary-threat-report-operation-aurora/)。
＊63 本件のマルウェアHydraqの解析報告は、例えば次の記事がある。ThreatExpert Blog: Trojan.Hydraq Exposed (http://blog.threatexpert.com/2010/01/trojanhydraq-exposed.html)。

また、この事件と同一の脆弱性を悪用するWebサイトの発見や、そうしたサイトへのリンクを仕込んだ標的型攻撃のメールも報告され、Operation Auroraに限らず、標的型攻撃の被害拡大が懸念されました。さらに、この事件に便乗して、Aurora関連の情報と称したメールを送付する標的型攻撃まで発生したとの情報もあります*64。

■ 標的型攻撃の対応の難しさ

これらの事例が示すように、個々の標的型攻撃はその対象が限定されています。しかし、その対象は多岐にわたり、現在では誰もが狙われる可能性がある身近な脅威となっています。また、その手口は巧妙で、顕在化しにくいことから、標的型攻撃への対応は難しいとされています。このため、標的型攻撃への備えとしては、まず、なりすましメールにだまされないための対策を行うことが考えられます。教育や演習*65などを通じてユーザの意識を高く保つこと、そして、電子署名や送信ドメイン認証のような発信者の確認に役立つ仕組みを利用することが挙げられます。また、標的型攻撃では、未知の脆弱性や、ウイルス対策製品が対応していないマルウェアが悪用されることがあります。この場合、攻撃に気付いた後の対策として、情報の共有が重要になります。事前にウイルス対策製品ベンダやセキュリティ専門家と相談できる関係を築いておくことや、事後にセキュリティの専門組織に相談*66することが有効です。

1.4.3 マルウェア対策活動MITF

ここでは、IIJが実施しているMITF（Malware Investigation Task Force）について説明します。MITFは、2007年5月から続けているマルウェア対策のための活動です。いくつかの調査において*67、発生するインシデントがネットワークごとに異なる状況にあることが判明し、IIJが運用するネットワークの状況を独自に把握するためにMITFを開始しました。MITFでは、専用の装置でマルウェアの活動を検知し、マルウェアを収集して解析を行い、対策に必要な情報を抽出しています*68。

■ マルウェアを取得するための仕組み

インターネット上のマルウェアの感染活動には、ウイルスなどのファイルを経由した感染だけでなく、ネットワーク上での直接感染、Webコンテンツ経由の感染、メール経由の感染などが考えられます。ここでは、これらの感染活動を観測する仕組みとして、ハニーポットとWebクローラを説明します。

ハニーポットでは、脆弱性のエミュレーション機能を持つホストをインターネットに接続し、外部から無作為に到着する通信を観測します。マルウェアの感染活動がネットワーク経由でこのハニーポットに到着し、脆弱性が適合すると、攻撃元の情報やマルウェアの検体が取得できます*69。MITFでは、IIJが運用する日本全国の網にこのハニーポットを設置し、マルウェアの活動を観測しています。その密度は、IPアドレス空間/23ごとに1台（IPアドレス512個につき1台）としています。

Webクローラは、通常のWebブラウザと同様に、検査対象のURLの一覧に順次アクセスし、脆弱性などを利用した攻撃を含むコンテンツを受け入れます。この結果、実際にマルウェアに感染して、検体を入手します*70。MITFの開始当初、Webクローラは試験的に構築し運用

＊64 エフセキュアブログ:「Operation Aurora」をエサにした標的型攻撃（http://blog.f-secure.jp/archives/50339288.html）。
＊65 例えばJPCERT/CCは擬似攻撃メールを用いた実地調査を行い、その結果を報告している（http://www.jpcert.or.jp/research/#inoculation）。
＊66 標的型攻撃の相談窓口としては、IPAの不審メール110番（http://www.ipa.go.jp/security/virus/fushin110.html）や、JPCERT/CCへのインシデント報告の届出（http://www.jpcert.or.jp/form/）等がある。
＊67 例えばJPCERT/CCの調査研究（http://www.jpcert.or.jp/research/#botnet）等。
＊68 日本国内においてはサイバークリーンセンター（http://www.ccc.go.jp/）が先に同様の活動を開始しており、この活動にはIIJも参加しているが、日本の全体像を把握する試みに加え、IIJの網内をより詳細に調査する必要があると判断した。実際に両者の観測結果には差異があり、その差異について はMWS2009（http://www.iwsec.org/mws/2009/presentation/A2-2.pdf） やIIJ.news（http://www.iij.ad.jp/news/iijnews/2009/__icsFiles/afieldfile/2009/01/07/vol90.pdf）等で公開している。
＊69 ハニーポットの実装としては、例えば、dionaea（http://dionaea.carnivore.it/）等。製品としてはSPECTER（http://www.specter.com/）等がある。このハニーポットとして実際に脆弱性を持つOSのPCを利用する事もあるが、IIJでは、悪用される可能性を極力排除するために、脆弱性をエミュレーションする実装を選択している。
＊70 Webクローラの実装には、例えばHoneySpider（http://www.honeyspider.net/）がある。製品としてはフォティーンフォティ技術研究所のOrigma+（http://www.fourteenforty.jp/products/origma/）等。

していました。しかし、Gumblar に代表されるWebコンテンツで感染するマルウェアの流行に伴い、現在ではマルウェア取得のための重要な構成要素となっています。

MITFでは、これらの他にも迷惑メールからマルウェア感染に誘導される様子を観測するための仕組みや、P2Pファイル共有ネットワーク等で交換されるファイルを観測するための仕組みも利用しています。

■ マルウェアを解析するための仕組み

MITFでは、取得したマルウェアの検体から、対策の検討に必要な情報を抽出する仕組みも用意しています。ただし、ここでの解析の目的は、マルウェアの検知や駆除ではなく、その活動による通信特性(宛先やプロトコル、通信量等)に注目した情報の収集です。

解析手法の1つである動的解析では、外部に接続していない閉じたネットワーク環境で、仮想のインターネットを再現し、そこで実際にマルウェアを動作させることで、動作に伴って発生する通信の様子を観測します[*71]。このため、動的解析環境には、マルウェアからの要求に応答するDNSサーバ、HTTPサーバ、IRCサーバなどの機能が用意されています。また動的解析では、通信の様子とともに、マルウェアによるファイル生成やプロセス生成の様子も観測します[*72]。この解析により、ダウンロードサーバ、アップデートサーバ、ボットネットのC&CサーバのIPアドレスやURLを特定することができます。この手法では、ウイルス対策製品等で判別できない未知のマルウェアに関しても、その活動を阻害するための有益な情報を取得することが可能です。

もう1つの解析手法である静的解析では、まず、取得したマルウェアの検体を複数のウイルス対策製品で検査します。マルウェアの名前や機能に関して参照可能な外部情報があるときには、それらを参考にします。また、閉環境や仮想マシン環境を検知する仕組みを持つマルウェアもあり、動的解析だけでは情報を抽出できないことがあります。この場合には、解析ツールを利用して手作業で解析を行います。さらに、マルウェアの検体は、協力関係にある研究機関やウイルス対策製品ベンダ[*73]にも提供しています。

■ MITFの全体像と今後の予定

図-12に、MITFの全体像を示します。ここに示すように、取得したマルウェアとその解析情報は、セキュリティサービスの設定として還元するなど、お客様のネットワークの保護やIIJのネットワークの安全な運用のために役立てています。

今回説明したMITFの環境では、これまでこのレポートで示してきたものよりも多くの情報が取得されています。たとえば、探索行為を行っている行為者に関する情報や、活動しているマルウェアの種類、IPアドレスを詐称された通信の戻りパケット(backscatter)によるDDoS攻撃の検知等です。今後は、このような情報も提供していく予定です。

また、MITFの開始当初に比べて、ネットワーク上で直接感染するマルウェアの活動は下火になりつつあり、Webコンテンツから感染するマルウェアに推移しています。今後、IPv6の利用推進やクラウド利用の一般化などネットワークの利用方法が変化することで、発生するインシデントの傾向も変わっていくと考えられます。MITFでは、このような変化に適切に対応できるように準備を行っています。

＊71 この閉じた仮想的なインターネットは、IIJで独自に実装したもの。
＊72 このような機能を実現する実装には、例えばProcess Monitor (http://technet.microsoft.com/ja-jp/sysinternals/bb896645.aspx) がある。
＊73 2010年４月の段階では、複数のウイルス対策製品ベンダや、セキュリティ団体、研究機関に対して検体を提供している。IIJでは、IIJの網内で流行しているマルウェアについて、ユーザの利用する可能性のあるウイルス対策製品で適切に対処されることを望んでいる。ご協力いただけるウイルス対策製品ベンダはIIJグループセキュリティコーディネーションチーム (IIJ-SECT) <sect@iij.ad.jp>にコンタクトをお願いします。

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、現在でも継続中であるGumblar類似の事件と標的型攻撃、そしてIIJのマルウェア対策活動であるMITFについて説明しました。

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。

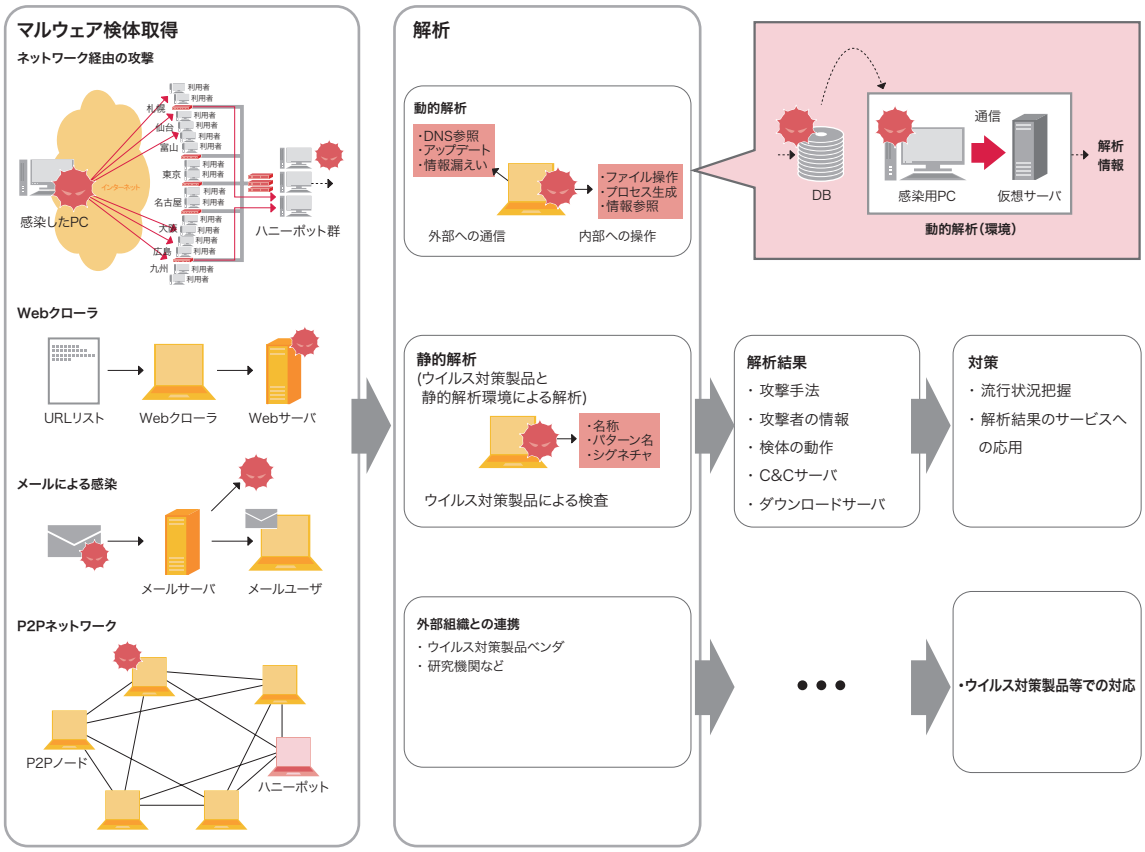


図-12 MITFのフレームワーク

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感染型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。IIJ-SECTの活動は、国内外の関係組織との連携活動を評価され、平成21年度情報化月間記念式典にて、「経済産業省商務情報政策局長表彰(情報セキュリティ促進部門)」を受賞した。

土屋 博英(1.2 インシデントサマリ)
土屋 博英 鈴木 博志(1.3 インシデントサーベイ)
鈴木 博志(1.4.1 Gumblar型の攻撃スキームを持つ ru:8080)
永尾 禎啓(1.4.2 標的型攻撃とOperation Aurora)
齋藤 衛(1.4.3 マルウェア対策活動MITF)
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 吉川 弘晃 IIJ サービス本部 セキュリティ情報統括室

経路制御の現状と異常経路検出時の対処

インターネットでは、ネットワーク間で経路情報が適正に受け渡されることによって、常に正しい宛先にパケットが送られます。ここでは、経路制御のプロトコルを紹介した後、誤った経路情報の広報による問題点を取り上げます。

2.1 経路制御プロトコルの種類と用途

インターネットは、数多くのネットワークの相互接続によって形成され、その状態は常に変化しています。新たなネットワークが接続されるかもしれませんし、何らかの理由で既存の接続が切断されるかもしれません。また、接続されているネットワーク自体も変化します。1つのネットワークが国や地域を越えて広がっていくこともあるでしょうし、事業撤退などでネットワークが縮退することもあります。このような変化の中でも目標とする相手と通信できるのは、きちんとパケットが宛先まで届くように経路制御されているからです。

インターネットでの多くの変化に手作業で対応することは不可能です。このため、自動的に最適な経路を見つけて制御してくれる動的な経路制御プロトコルが必須となります。動的な経路制御によって、需要に応じて分配したIPアドレスを簡単に使えるという利点もあります。組織内などの比較的小さなネットワークでは、RIP（Routing Information Protocol）やOSPF（OpenShortest Path First）といった経路制御プロトコルが採用されることが多いようです。一方、ISP間や大規模ネットワーク間といったインターネットでの経路制御には、BGP（Border Gateway Protocol）が標準的な経路制御プロトコルとして利用されています。

BGPの設計当初は、組織内のネットワークでOSPFやIS-IS（Intermediate System to Intermediate System）等を組織内経路制御プロトコル、IGP（Interior Gateway Protocol）として利用し、ネットワーク間でBGPを組織間制御プロトコル、EGP（Exterior Gateway Protocol）として利用して、IGPとEGP間で経路情報を同期しながら運用するネットワーク構成が想定されていました。しかし、OSPFやIS-ISなどのIGPでは、BGPが扱うような大量の経路情報を処理することが想定されていないため、その構成を変更する必要がありました。このため、BGPの経路情報をIGPに渡すのではなく、BGPとIGPをそれぞれ独立したものとして非同期で運用する構成が標準的な設計として広まりました。

また、最近の大規模なネットワークでは、網内の経路数増加に対応したりIGPの収束速度を早めたりするために、ネットワークのトポロジー（構成）と必要最小限の経路情報のみをIGPで運用し、その他すべての経路情報をBGPで運用するといった構成に変化しています。このためBGPを正しく運用することは、ネットワーク間のみならず、ネットワーク内の経路制御を適切に行う上でも重要なものになっています。

2.2 ネットワークポリシ

各ネットワークは、経路制御のポリシを個別に持っています。すべてを経路制御プロトコルに任せておき一切気にしないというポリシもあるでしょうし、より明確な意思を持って経路を選択しているネットワークもあるでしょう。BGPでは、経路情報を交換する際に、それぞれのネットワークのポリシを設定できます。ただし、設定できることはそれほど多くありません。経路のフィルタと優先度の設定、後処理のために目印を付けるくらいです。BGPで経路制御する際には、これらを組み合わせて上手にネットワークのポリシを実装し、意図したとおりの状態になるように設計する必要があります。

ほとんどのネットワークが標準的に持っているポリシがあります。これは、相互接続する相手の種別に応じたポリシで、カスタマ、ピア、アップストリームの3つです。カスタマは、ピアやアップストリーム等、他のネットワークへの中継（トランジット）を行います。経路制御では、ネットワーク自体が保持する全経路をカスタマに送信することに加えて、カスタマから広報された経路を他のネットワークにも送信します。ピアは、カスタマを含め互いのトラヒックを交換する関係にあり、ネットワーク自体とカスタマの経路のみを互いに交換します。アップストリームは、カスタマとは逆の動きで、他のネットワークへの中継を行ってもらっているネットワークです。アップストリーム向けにはネットワーク自体とカスタマの経路を広報するとともに、アップストリームからは全経路を広報してもらいます（図-1）。

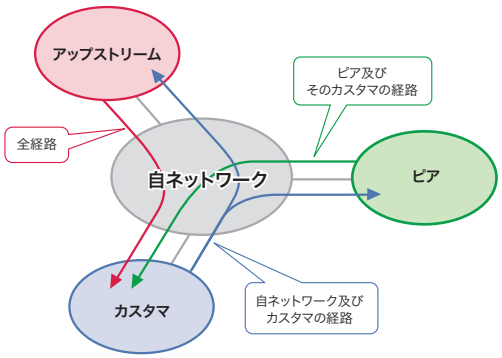


図-1　ピア、カスタマ、アップストリーム

2.3 経路数の現状

BGPで広報した経路情報は、相互接続されたネットワークを通じて世界に伝わっていきます。同様に、世界中のネットワークがそれぞれ経路情報を広報しているため、BGPを運用しているとインターネットに接続しているさまざまなネットワークからの広報を受信することになります。

インターネットでのBGP経路数は、この原稿の執筆時点においてIPv4でおよそ32万経路、IPv6で2300経路程度です。ここ最近、経路数はIPv4とIPv6ともにほぼ線形で増加しています。そして、今後もこの増加傾向は続くと考えられます。経路数の増加要因としては、新たなネットワーク接続やサービス拡充のためのネットワーク追加、トラヒック制御のための経路広報が考えられます。

経路情報の増加は、そのままルータでのメモリ消費につながるため、ルータの増強時期を検討する上でも注意すべき項目です。今後の懸念として、IPv4アドレスの在庫枯渇があります。APNICのミーティングでIPアドレスの移転ポリシが合意に達したこともあり、枯渇前後からIPv4アドレスの利用効率を高めるために、より細かな単位で経路が広報されることが予想されます。これは、さらに経路数が増加することにつながると思われます。

2.4 権威なき広報

BGPでは、経路ハイジャックがたびたび問題になります。これは、主に他人の経路情報を勝手に生成して広報することによる問題で、そのネットワーク宛の通信が関係のないネットワークに送られてしまい通信できなくなるといったトラブルを引き起こしています。このような問題が攻撃手法として利用されたときには、さまざまな悪用方法が考えられます。単純な通信妨害にとどまらず、他者に成りすまして偽のサイトを立ち上げたり、通信内容を盗聴するといったことも考えられます。実際に、2008年に著名な動画投稿サイトがアクセス不能になったり、2010年4月にアジアのあるASが世界中のさまざまな経路情報を数万件も広報してしまうという問題が発生しています。

このような事例では、その発生原因までが明確に報告されることは稀ですが、状況等から考えて意図しないBGPの設定ミスによるものだと推測できます。また、これまで報告された他の事例でも、そのほとんどが設定ミスによるものだと推測でき、「経路ハイジャック」という呼び名がその実態に比べて不穏すぎると思えるため、個人的には「権威なき広報」と呼ぶほうが適当だと考えています。

BGP自体はどのような経路情報が交換されるかを認識していないため、このような権威なき広報が起こってしまいます。どの経路情報を受け取り、どの経路情報を受け取らないかは、すべてポリシ、つまり各ネットワークの経路情報制御の運用に依存します。このため、運用によっては、この権威なき広報を防いだり、その影響範囲を狭めたりできる可能性があります。

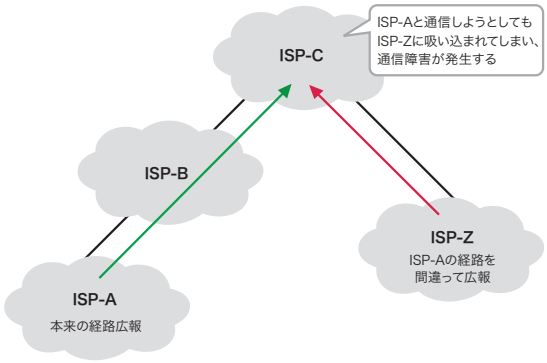


図-2　権威無き経路広報による、通信障害

たとえば、それぞれのネットワークにおいて、カスタマから広報される経路情報を厳密にフィルタリングすれば、権威なき広報で世界中のネットワークに迷惑をかけることはありません。過去には、カスタマ向けの受信経路フィルタを行っていないネットワークにも経路情報を中継した責任があると指摘する意見もありました。IIJは、BGP接続を利用されているお客様には経路情報を広報する前に連絡いただき、厳密な経路フィルタを設定しています。

一方で、権威無き広報を行ってしまったネットワークのアップストリーム内に、経路フィルタを実装していないネットワークが1つでもあったときには、そこから世界中に経路情報が広がってしまう可能性があります。現在でも断続的にこのような問題が発生していることから、いまだにカスタマ向けに厳密な受信経路フィルタを実装していないネットワークが多いと考えられます。より多くのネットワークが適切に経路フィルタを運用することで影響を軽減できる可能性が高まります。今後も、運用者コミュニティ等を通じて、よりよい運用を呼びかけていこうと考えています。

2.5 異常経路の検出

ここまでに示したとおり、他人が自分自身の経路情報を勝手にBGPで広報することは、現状では完全に予防することはできません。このため、権威なき広報が発生したときには、何よりも素早くそれを検知する必要があります。異常経路の検出に関しては、世界中でさまざまな取り組みが行われています。どの検知システムも、正常と見なす経路と実際のBGPでの経路の変動を逐次比較して、違いがあれば異常経路と判断しています。このような仕組みであるため、検知システムには次の2つの課題があります。

- 何をもって正常と見なすかという判断部分
- 比較対象となるBGPの経路情報をどこから得るかという経路収集部分

1番目の「判断部分」に関しては、いくつかの手法が試されています。たとえば、長期間安定して広報されている経路を正しいと見なし、その状態から広報元に変動があったときに異常と見なすシステムがあります。また、手作業で正しい経路の状態を登録しておき、それとの差異が生じたときに異常と見なすシステムもあります。

2番目の「経路収集」に関する課題は、難しい課題です。ネットワークは、それぞれ経路制御のポリシを持っているため、当然保持している経路情報もそれぞれ異なります。また、ネットワークの内部にはBGPが動作しているルータがあります。これらもそれぞれ異なる経路情報を保持している可能性があります。局所的な影響も検知しようとすると、より多くのネットワークやルータから経路情報を得る必要があります。

2.6 日本国内での取り組み

日本国内での異常経路の検知に関する取り組みとして、Telecom-ISAC Japanが運営している経路ハイジャック検知システム「経路奉行」があります。経路奉行は、JPNICが運用するIRR (Internet Routing Registry)、JPIRRに登録されているrouteオブジェクトを正常な経路状態として判断基準に採用し、これと日本国内のISPからシステムに提供されているBGP経路情報とを逐次比較して異常経路を検出するシステムです。routeオブジェクトに登録されている広報元と異なる広報元から経路情報が広報されたときに異常と判定しているため、設定ミスによる異常経路を検出するには有用なシステムです。また、日本国内のISPから経路情報を得ているため、国内での影響をある程度推測することもできます。IIJも当初からこのシステムの運用に参加し、よりよい検出に向けて活動を続けています。また、IIJ自身の経路を監視するという目的のため、利用者としてもシステムを活用しています。これまでには、IIJが広報している経路情報が他ネットワークから広報された際に、経路奉行からの警報を受信したこともあります。

2.7 異常経路検出時の対処方法

警報を受信したときには、まず現在の状態を外部のLooking Glassサイトなどで確認します。これまでのほとんどの事例では、数分間程度で問題の経路情報が消えて復旧しているため、検知システムからの警報を受信したときにはすでに回復している可能性もあります。

しかし、残念ながら、まだ問題の経路広報が継続しているときには、該当経路の広報元への連絡を試みます。その際、こちら側に経路広報の正当性があることを伝えるために、常日頃からIR (Internet Registry) やIRRの登録情報をきちんと更新しておくことが大切です。

問題の広報元への連絡がうまくいかないときには、そのアップストリームと思われるネットワークに連絡して、対応への援助を求めることも有用です。それでも解決できないときには、周辺のネットワークや運用者コミュニティに適切な連絡先を問い合わせてみたり、助力を求めたりするなどして、解決に向けてできるかぎり対応する必要があります。

短中期的にはこのような運用での対処を行いつつ、長期的にはより簡単に正しい経路であることを判別する方法を検討します。その１つが電子署名を利用して認証を行うRPKI (Resource Public Key Infrastructure) です。RPKIを利用すると、IRからIPアドレスが割り振られる際にリソース証明書と呼ばれる電子署名が発行され、IPアドレスの利用権利を明確にできます。この仕組みを利用してルータで経路情報を認証し、正しい広報元から広報されている経路情報であることを自動的に判別します。すでに、いくつかのルータベンダによる実装が進んでおり、実際に電子署名で経路情報の認証が可能なファームウェアの検証試験も行われています。ただし、証明書の発行や電子署名の運用に関する課題もあり、RPKIの導入までにはいましばらくの時間がかかるとも思えますが、IIJは信頼できる経路制御のために継続的な活動を行くつもりです。

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。

メールアドレスの国際化アプローチに対する考察

今回は、2010年第1週〜第12週での迷惑メールの割合の推移とともに、前年同期との比較結果を示します。また、迷惑メールの主要な送信元地域の傾向の変化、送信ドメイン認証技術の導入状況に加えて、メールアドレスの国際化に対するアプローチの問題点を考察します。

3.1 はじめに

本稿では、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。

今回のレポートでは、2010年第1週(2010年1月4日〜1月10日)から第12週(2010年3月22日〜3月28日)までの12週間分と、2009年一年間分のデータを対象としています。迷惑メールの流量は、時期や迷惑メールの流行のタイミングなど複数の要因で変化しますので、迷惑メールの割合の推移を前年同期と合わせて示すことで、時期的な要因を勘案した比較が可能です。

今回の2.2迷惑メールの動向では、迷惑メールの送信元の分布や、そこからの推測される送信手法などについても分析しました。さらに、迷惑メール対策のための基礎技術である、送信ドメイン認証技術の導入状況についても報告します。

2.3メールの技術動向では、現在IETFで議論されているメールアドレスの国際化と関連する技術動向についてレポートするとともに、EAI(Email Address Internationalization)の問題点を考察します。

3.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IIJセキュアMXサービス等で検知した迷惑メールの割合の推移と、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。

3.2.1 2010年第1週から第12週までの迷惑メールは微増

2010年第1週から第12週までの84日間に検出した迷惑メールの割合は、平均82.1%でした。前回(2009年第40週〜52週)の平均が81.4%、2009年同期(第1週〜第13週)が81.5%でしたので、いずれに対しても微増という結果になります。今回の調査期間を含めた2009年からの迷惑メールの割合の推移を図-1に示します。

今回の調査期間には、長期休暇が含まれているため、これまでの調査結果と同様にその時期に迷惑メールの割合が高くなっています。しかし、これまでは長期休暇の期間が終わると迷惑メールの割合が下がる傾向がありましたが、今回は80%を超える比較的高い期間がしばらく続いています。今回の微増は、この継続の延長が原因で

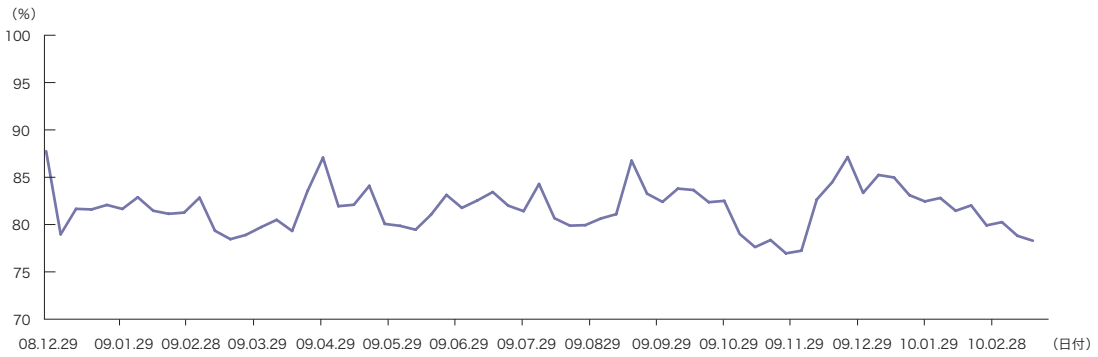


図-1 迷惑メールの割合

あると考えられます。迷惑メールの送信傾向には、時期による要因も影響しますが、送信手法の変化、例えば新たなマルウェア（不正プログラム）の流行に伴うボットネットの増加によって急激に増えることもあります。

近年は、ハードウェアの高性能化やネットワーク帯域の利用増加などもあり、新たな手法が作り出されると、急激に迷惑メールが増える傾向にあります。ISPなどの常に大量のメールを受信する事業者にとって、こうした急激なメールの増加は、安定した運用を阻害する要因になります。ISPのメールサービスで提供されるウイルス対策や迷惑メール判定機能は、主に専門のベンダ企業によるもので、こうした急激な変化への対応が難しくなっています。今後、ISPに対しては、こうした迷惑メール送信手法の動向を把握し、メールシステム全体として素早く対応できる体制が求められます。

3.2.2 迷惑メール送信元1位の地域は、ブラジルから新たに米国に

今回の調査期間での迷惑メールの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位は米国（US）で、迷惑メール全体の9.6%を占めていました。2位は中国（CN）の7.6%、3位はインド（IN）の6.1%でした。これまで連続して首位であったブラジル（BR）は、今回の調査で5.8%となり4位に後退しました。同様に、前回5位だったベトナム（VN）も、今回の調査は3.2%で10位に後退しました。これら2つの国が大きく順位を下げていますが、これは2つの国からの迷惑メールの受信数自体が極端に減少したのではなく、他の上位国からのものが増加したことによる相対的な順位の低下です。図-2のグラフからも、これまでの調査結果と比較して、送信割合が極端に大きい地域が減少していることが分かります。日本の順位は、前回と同様の7位で3.9%、前回より0.1%微増という結果でした。前回の調査でも微増していましたが、その原因は通常のメールサーバと思われる送信元からの迷惑メールが増加していることにあります。

通常のメールサーバから迷惑メールが送信されるケースには、メールサーバが迷惑メール送信の踏み台にされているケースと、転送設定などによって迷惑メールも含めたすべてのメールが転送されているケースが考えられます。このうち踏み台にされているケースでは、外部組織などによるブラックリストに送信メールサーバが登録される可能性が高く、いったん登録されるとそれらを参照している受信メールサーバで受け取りが拒否されてしまいます。日本では、OP25B[*1]の導入時にメール投稿サーバでのSMTP-AUTH[*2]の導入が推奨されているため、簡単にはメールを送信できない仕組みになっています。しかし最近では、迷惑メール送信に利用されるボットPC上の不正プログラムがSMTP-AUTHに対応して迷惑メールを送信しているとの情報もあり、送信時の認証機構だけでは不十分かもしれません。メール投稿時にSMTP-AUTHを利用することに加えて、送信者ごとにメール送信数の上限を設定して大量の送信を防止する、メールログに送信者情報を記録して迷惑メールが送信されてしまった後でも追跡可能にするなどの対応が必要になります。

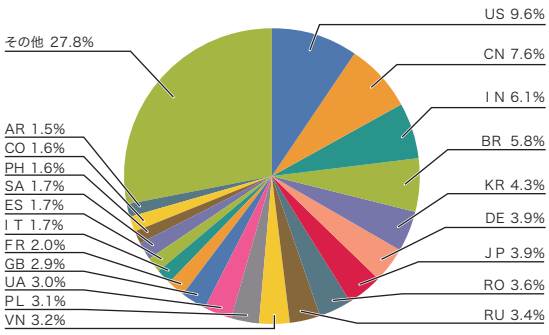


図-2　迷惑メール送信元

＊1　OP25B（Outbound Port 25 Blocking）は、一般のネットワーク利用者に割り当てられる動的IPアドレスに対して、直接外部の受信メールサーバへのメール送信をブロックすることで、迷惑メール送信を抑制する技術です。

＊2　SMTP-AUTHは、メール送信時にSASL（Simple Authentication and Security Layer, RFC4422）の機構を利用して送信者の認証を行います。多くの場合、送信者を特定するAuthentication IDとパスワードによって認証されます。SMTP-AUTHはSMTPの拡張としてRFC4954で仕様が定められています。

3.2.3 送信ドメイン認証技術の導入により、迅速なメール受信を

迷惑メール対策には、迷惑メールを判定する迷惑メールフィルタの導入やアンチウイルス機能の導入など、迷惑メールを排除するための機能と合わせて、正しいメールを遅滞なく受信するための仕組みも重要です。近年の迷惑メールの巧妙化やウイルスメールの多様化、ボットネットなどを利用した新種や亜種の瞬間的な流行に対応するため、迷惑メールを判定するための機能に高度な判定処理が導入される傾向にあります。しかし、判定処理自体に時間がかかり、大量にメールを受信したときに配送遅延などが生じる懸念もあります。例えば、ビジネス上の取引先など、すでにメールの送信元が明らかであるときには、こうした迷惑メールの判定処理の一部分を省略して、迅速にメールを受け取りたいと考えるかもしれません。

これまでは、正しい送信元を判断する基準や方法がありませんでした。しかし現在は、送信ドメイン認証技術を導入することで、この要望に対応できます。これまでのIIRで解説してきたとおり、広く普及しているネットワークベースの送信ドメイン認証技術には、転送などメールの再配送時に送信者を正しく特定できない、という問題点が指摘されています。この問題の解決方法についても、普及するまでに時間が必要です。

ただし、この問題が未解決でも、送信ドメイン認証技術による認証結果を利用できます。メールの再配送での認証の誤判定は、受信メール全体の量に対してそれほど大きな割合ではありません。認証できたドメインからのメールを優先して受け取るバイパス的な配送処理の仕組みが受信側にあれば、より迅速に必要なメールを受け取ることが可能になります。送信ドメイン認証技術の認証結果と、特定の送信者をホワイトリストで取り扱うことにより、信頼のある両者間でより効率的なメールの送受信が可能になります。このような状況を促進するためにも、引き続き送信ドメイン認証技術の普及を訴えていきたいと考えています。

3.2.4 送信ドメイン認証技術の導入は微増、効率の良いメール配送を目指す

ネットワークベースの送信ドメイン認証技術のひとつであるSPFの調査結果として、今回の調査期間(2010年1月〜3月)での特定のメールサービスの認証結果の割合を図-3に示します。この期間に受信したメールの認証結果は、全体の55.6%が“none”でした。これは、受信メールの44.4%のドメインでSPFレコードが宣言されていたことを表します。この結果は、前回の調査に比べて0.7%の微増となります。

また、認証結果が“pass”であった受信メールの割合も16.3%で、0.4%の微増という結果になりました。これは、受信メールの約6分の1の割合ですが、これらをすべてホワイトリストに設定すれば、これらのメールに対してより効率のよい配送が可能になります。ただし、最近は、迷惑メールの送信側でもSPFをパスするようなドメインを利用しているため、ホワイトリストの導入時には、認証結果だけでなく、対象とするドメイン名と合わせて処理するように設定することが必要です。

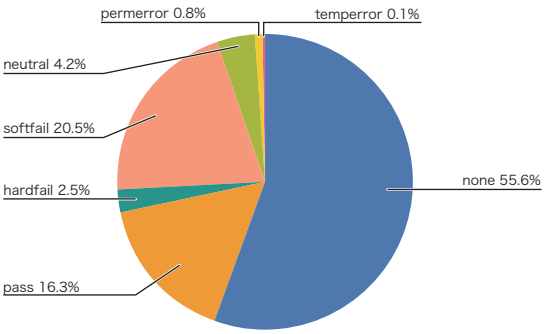


図-3　メールサービスの認証結果の割合

3.3 メールの技術動向

3.3.1 メールアドレス国際化

taro@example.jpといった、インターネットで利用されているメールアドレスは、アットマーク（@）の左右でその役割が分かれています。アットマーク（@）の右側がドメイン名、左側が個々のメール受信者を示すローカルパートです。このような形式のメールアドレスで利用できる文字コードは、基本的にASCII文字列です。アットマーク（@）の右側に置かれるドメイン名の国際化は、すでにIDN（Internationalized Domain Name）という仕組みにより利用可能になっています。IDNの仕組みは、（株）日本レジストリサービス（JPRS）が提供するJPRSトピック&コラムの『No.7 国際化ドメイン名を実現する3つの技術』[*3]に詳しく説明されています。ここでは、その概要を説明します。

ドメイン名の国際化対応は、Unicodeによる文字列を使用可能にしたことで実現されています。Unicodeを採用することで、“日本語.jp”などのASCII文字以外を母語の文字とする言語がそのまま使えるようになります。しかし、Unicodeをそのまま利用することは、既存のプロトコル、特にDNSの仕組みへ大きく影響することが懸念されました。そのため、punycodeと呼ばれる変換方式を導入してUnicodeを符号化し、IDNであることを示すACE prefixを付けることで、これまでどおりの英数字とハイフン（-）だけの組合せとなるようにしています。この符号化の仕組みによって、例えばWebブラウザに入力するURLに日本語のドメイン名が含まれていても、Webページを参照するために必要なIPアドレスをWebブラウザがDNSから取得する際に、punycodeによって符号化されたドメイン名で問い合わせることができます。図-4に、punycodeを利用した“日本語.jp”のIDN表記の例を示します。

符号化例:

“日本語.jp”

↓

“xn--wgv71a119e.jp”

図-4　punycodeによる符号化例

ドメイン名の国際化に関しては、さまざまな議論が交わされた結果、既存の仕組みに影響が少ない手法が選ばれました。今後の普及については、実際にどの程度の需要があるかというマーケット面での要因に左右されるでしょう。

Webブラウザと同様にメールでも、メールアドレスに国際化ドメインが使われたときにMUA（Mail User Agent）がWebブラウザと同様に符号化を実施すれば、既存のメールサーバに影響しないため問題はほとんど生じません。しかし、メールアドレスの国際化の現状は、ドメイン名に加えてアットマーク（@）の左側部分のローカルパートも国際化する動きがあります。しかも、Unicodeを符号化せずにそのまま扱おうとしているため、問題をより複雑なものにしています。

現在提唱されているメールアドレスの国際化（EAI: Email Address Internationalization）について、JPRSトピック&コラム『No.11 電子メールアドレスの国際化 ～ Email Address Internationalization（EAI）の概要～』[*4]で詳しく述べられています。IETFからは、EAI全体の枠組みについてはExperimentalとしてRFC4952、メール配送の仕組みであるSMTP（Simple Mail Transfer Protocol, RFC5321）の拡張仕様についてもExperimentalとしてRFC5336がそれぞれ定義されています。

3.3.2 メール関連プロトコルとEAIは深刻な問題を抱えている

SMTPでのEAIの利用では、これまでのSMTPの拡張機能と同様に、SMTPセッションの開始時のコマンド（EHLO）に対する応答により、受信側メールサーバのEAI対応が判断されます。実際には、EHLOコマンドへの応答に“UTF8SMTP”が含まれていれば、受信側のメールサーバがEAIに対応していることになります。EAIに対応していれば、メールの送信者を示すMAILコマンドの引数reverse-pathや宛先を示すRCPTコマンドにUnicodeを含めることができます。同様に、メール本体のヘッダ部分のFrom:ヘッダやTo:ヘッダにも、そのままUnicodeが利用できます。メール配送の開始時

＊3　http://jpinfo.jp/topics-column/007.pdf
＊4　http://jpinfo.jp/topics-column/011.pdf

に利用可能な機能をお互いにネゴシエーションした上で拡張機能を利用するため、ここまでの処理に大きな問題はありません。

EAIで問題になる部分は、メールの受信側がEAIに対応していなかったときの処理です。例えば、EAIに対応したメールの投稿サーバ（MSA: Mail Submission Agent）がMUAからEAIをそのまま受け取ったが、受信側のメールサーバが対応していなかったとします。いったん受け取ったメールを配送できない場合、通常はエラーメールとして送信者にバウンスされます。このような処理は、EAIの段階的な導入時期にメールシステム全体の可用性を下げるかもしれませんが、それほど深刻な問題ではありません。

より深刻な問題は、下位互換性を維持するためにダウングレーディングという変換方法がEAIに用意されていることです。これは、EAIに対応していない受信側のメールサーバにメールを送信するために、エラーとしてバウンスするのでなく、ダウングレードによりできるかぎり配送しようとするものです。細かな部分ではSMTPに関してもいくつかの疑問点がありますが、もっとも深刻な問題はメールヘッダの変換に関するものです。受信側のメールサーバがEAIに対応していない場合、EAIで記述された元のヘッダ情報が“Downgreaded-”で始まるヘッダに書き換えられ、ダウングレードされたメールアドレスによって既存のFrom:ヘッダやTo:ヘッダが書き換えます。この処理での問題は、送信ドメイン認証技術のひとつであるDKIMが、これらの主要なメールヘッダを署名の対象として参照していることです。署名の対象となるヘッダが書き換えられた場合、当然、署名が不正なものと見なされ、認証が失敗することになります。

これまでメールに関連したプロトコルの拡張は、SPF、Sender ID、DKIMなどの送信ドメイン認証技術や、いわゆる添付ファイルに使われるMIME（Multipurpose Internet Mail Extension, RFC2045）などのように、既存のプロトコルにできるかぎり影響を与えず下位互換となるように慎重に行われてきました。こうした努力をまったく無視するように仕様を拡張しているEAI、特にそのダウングレーディングの仕様は、あまりにも乱暴だと言えます。今後、EAIは、国際標準とすべき仕様を目指して検討が行われる予定のようですが、拡張の仕組みやその手順に関しては、より慎重に議論されることを望みます。

3.4 おわりに

今回のメッセージングテクノロジーでは、迷惑メールの動向として、これまでと同様に迷惑メールの割合の推移、送信元地域に関する分析結果、送信ドメイン認証技術のひとつであるSPFの普及状況について報告しました。迷惑メールの割合は、引き続き高い状況が続いており、急増する可能性もあるため、継続した注意が必要です。

メールの技術動向は、これまでの送信ドメイン認証技術に代わり、EAIについて取り上げました。EAIは、送信ドメイン認証技術とまったく無関係なものではなく、むしろその仕様の拡張によって大きな影響を及ぼす可能性がある手法であると考え、今回取り上げました。今回は、EAIの問題点に注目しましたが、本来の目的であるメールの利用者層を広げること自体には賛成です。メール利用者層の広がりを目指して、常日頃ASCII文字を使うことがない地域や民族の人々が、より簡単に電子メールを利用できるようにするための仕組みを模索したり検討したりすることは、むしろ積極的に行うべきです。しかしながら、それを実現する手法が、これまでのプロトコル拡張の積み重ねを無視するような強引なものであるときには、メールの利用環境自体を分断する可能性があります。新たな仕様の導入については、これまでと同様に、より慎重に検討すべきです。あるいは、よく多くの地域や民族の人々が利用するに適したメッセージ伝達のための新たな枠組みが必要になってきているのかもしれません。

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。

インターネットトピック: モジュール型エコ・データセンター実証実験

IIJは、各種サービス機器の設置場所やお客様のITシステムをお預かりする場所として、現在全国15か所でデータセンターを運営しています。これらのデータセンターは、サーバ、ストレージ、ルータなどを安定稼働させるために、堅牢な建物、大容量で高信頼性な電力や空調の設備を備えています。これまでのITシステムは、このような十分すぎる環境で運用されるのが一般的でした。しかし、ここ数年、ITシステムの運用について、従来とは異なる考え方が提唱されてきています。その背景には、ITシステムへのコスト低減の要望やエコロジーという新しい視点があります。

ITシステムのコストには、その開発や構築だけでなく、データセンターの利用料や日々の運用費用が大きな割合を占めています。これらを低減することが、ITシステム全体のTCO（総所有コスト）を下げる上で重要な要素になります。特に、昨今話題に上っているクラウドコンピューティングでは、この傾向がより顕著です。クラウドコンピューティングでは、ITシステムの利用者自身がデータセンターなどのファシリティを意識する必要はありません。しかし、クラウドコンピューティング自体を支える基盤として、依然データセンターは重要な役割を担っています。クラウド化によってソフトウェアやサーバのコストが低減されるため、相対的にデータセンターのコスト比重が高まっています。

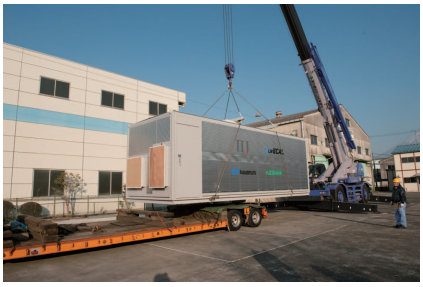
また、現在の環境問題への意識の高まりによって、ITシステムにも「エコロジー」が求められています。従来のデータセンターでは、高性能で高発熱な機器を冷却するために、エアコンなどの空調設備で多くの電力を消費していました。データセンターの効率化に取り組んでいる団体“The Green Grid”による調査では、サーバなどが消費する電力の1.3倍近くの電力が、エアコンや照明といったITシステム以外の設備で消費されています。これは、データセンターで消費される電力のうち、本来の用途に活用されているものが全体の半分にも満たないことを示しています。このような本来の用途以外の電力を削減できれば、省エネルギー化、ひいてはCO2排出量の削減などに大きな効果を上げることができます。また、データセンターで利用される電力を削減することは、ITシステムの維持コストを下げることにもなります。このような観点からも、データセンターでの電力利用の効率化が求められています。

IIJでは、このような状況を踏まえ、次世代のデータセンターとして次の2つの新技術に取り組んでいます。その1つは、需要の増加に応じて迅速に設備を拡張できるモジュール型データセンターの建設です。これは、従来の堅牢な建物の代わりに、運搬可能なサイズのコンテナ内にデータセンターの設備を作り込むことで実現します。もう1つは、サーバなどIT設備の冷却に外気冷却方式を導入することです。外気冷却方式は、従来のエアコンなどによる強制冷却方式に比べて、極めて少ない電力で運用でき、省エネルギーの切り札として期待されています。

しかし、これらの技術の利点を生かすためには、従来までの運用方法を見直す必要があります。コンテナ内に構築したデータセンターでは、従来のビル型データセンターに比べて設置可能な設備のバリエーションが制限されます。また、機器の故障時には個別に機器の修理を行うのではなく、コンテナ単位で交換したほうが効率がよいかもしれません。外気冷却方式は、省エネルギーですが、その冷却能力が周囲の気候や天候に左右されます。四季という変化に富んだ季節がある日本での利用には、高度な制御技術が必要になります。このような運用方法や技術は、世界を見回してもまだ十分に確立されていません。

そこでIIJでは、次世代型データセンターの本格的な建設に先立ち、これらの技術の確立とノウハウの獲得のために実証実験を行います。これは、実際にサーバを搭載して運用可能なITモジュール（コンテナ型データセンター）と、外気を取り込む空調モジュールを建設し、長期間にわたって運用するというものです。実験期間は1年間とし、実際に四季を通じて外気を活用した冷却を行い、どこまで消費電力が低減できるかを観測しながら、実運用に耐えられるIT/空調モジュールの設計ノウハウを追求する予定です。

すでに実証実験のための機器が完成し、2010年2月から運用を開始しています。2月以降、徐々に暖かくなる気候の中で、さまざまなデータが取得できています。想定外のトラブルや設計上の問題もいくつか発見でき、商用設備の設計へのフィードバックも行っています。この実験が新技術の確立に大きな役割を果たすことは間違いありません。IIRの次号では、この実証実験の経過や商用サービスへの展開についてレポートする予定です。ご期待ください。



執筆者:
堂前 清隆（どうまえ きよたか）
サービス本部 データセンターサービス部 事業企画課

Ongoing Innovation

Vol.7 May 2010

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-MKTG019GA-1005KO-08000PR