Internet Infrastructure Review

IIJ
Internet Initiative Japan

Vol.6

February
2010

インフラストラクチャセキュリティ

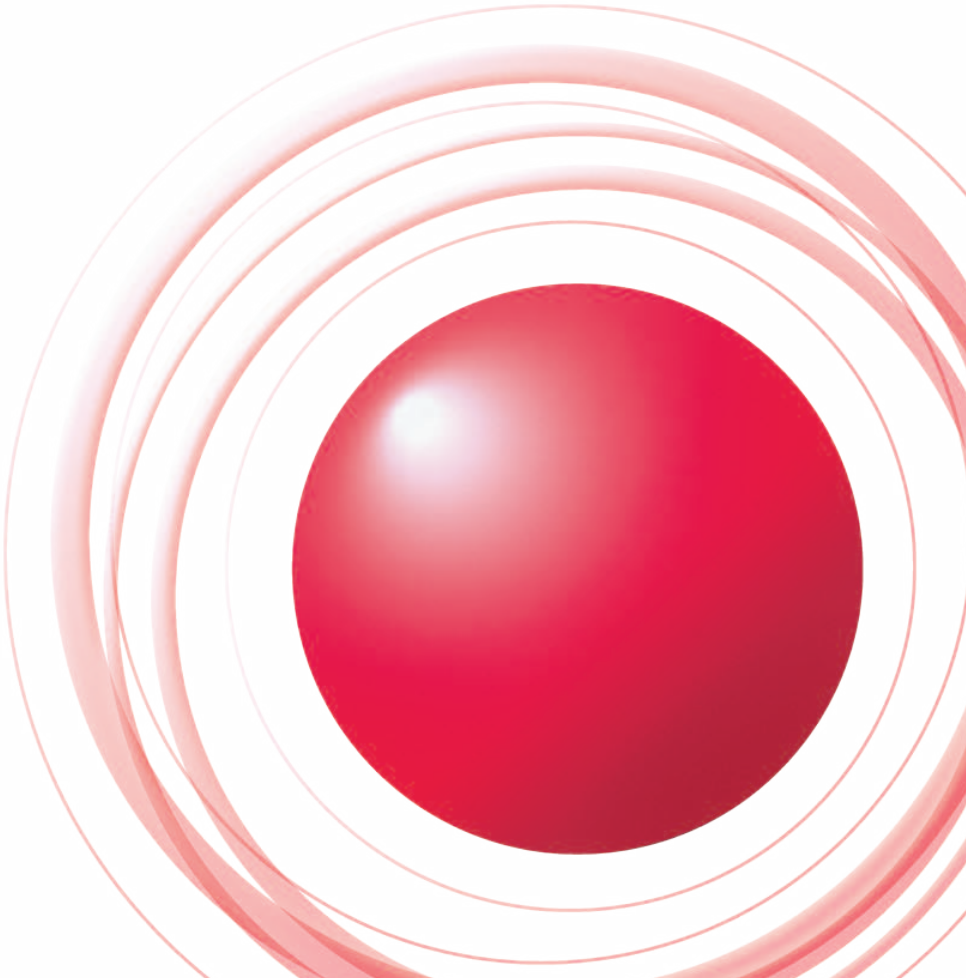
Gumblarの再流行

メッセージングテクノロジー

送信元の地域特性に合わせた迷惑メール対策の必要性

インターネットバックボーン

インターネット上での到達性の計測



Internet Infrastructure Review Vol.6 February 2010

エグゼクティブサマリ 3

1.インフラストラクチャセキュリティ 4
1.1 はじめに 4
1.2 インシデントサマリー 4
1.3 インシデントサーベイ 6
1.3.1 DDoS攻撃 6
1.3.2 マルウェアの活動 8
1.3.3 SQLインジェクション攻撃 10
1.4 フォーカスリサーチ 11
1.4.1 Gumblar の再流行 11
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 13
1.4.3 P2Pファイル共有ネットワークの調査技術 15
1.5 おわりに 17

2.メッセージングテクノロジー 18
2.1 はじめに 18
2.2.1 迷惑メールの割合の推移 19
2.2.2 迷惑メールの送信元 19
2.2 迷惑メールの動向 19
2.2.3 迷惑メールの送信傾向 20
2.2.4 送信ドメイン認証技術の導入状況 21
2.3 メールの技術動向 22
2.3.1 DKIM ADSP とその経緯 22
2.3.2 DKIM ADPS の概要 22
2.3.3 DKIM のアップデート 23
2.4 おわりに 23

3.インターネットバックボーン 24
3.1 はじめに 24
3.2 /25はどこまで伝搬するのか 25
3.3 default経路の利用状況 26
3.3.1 ASのタイプによる変化 28
3.3.2 default経路の影響 29
3.4 dual probingによる到達性の検査 30
3.4.1 間違ったbogonフィルタの検出 32
3.5 計測結果の確からしさに影響する項目 33
3.5.1 トポロジー上でカバーする範囲 33
3.5.2 IPアドレスとAS番号のマッピング 34
3.5.3 どの計測ツールを使うか 34
3.6 結論 34

インターネットトピック: 迷惑メール対策推進協議会 35

■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

インターネットはそもそも、全体を統括するような主体を持たず、部分同士が自発的に繋がりあって徐々に成長していく自律分散型のシステムです。その振舞いにはある程度の法則はありますが、どこかに全体の設計図やシナリオがあり、それに沿って動いているわけではありません。その時々の社会情勢や世界経済の動向、それらによる利用者の振舞いの変化や利用形態の変化など、さまざまな要因が影響を及ぼし、それが重なり合うことで、インターネットの挙動や性質は刻々と変化していきます。

このような自律的に成長し変化するインフラストラクチャを安定して運用するためには、継続的にその振舞いを複数の視点から計測して分析し、どのような動きが起こっているかを常に把握した上で、迅速かつ適切に対応していく必要があります。その際に、計測する方法やデータを解釈する方法が適切でなければ、そこから得られる情報が不確かなものになり、適正な運用ができなくなってしまいます。

したがって、インターネットを構築し運用するための技術開発も重要ですが、稼働状況を計測し、得られたデータを解析し、そこから有益な情報を取り出し、運用にフィードバックするための取り組みや仕組み作りも非常に重要であると認識しています。

本レポートは、IIJがインターネットというインフラストラクチャを整備し発展させるために行っているさまざまな計測や解析の成果と、それに関連する技術項目の情報を定期的に提供するものです。

「インフラストラクチャセキュリティ」では、2009年10月から12月末までの3か月間を対象として、セキュリティインシデントの統計とその解析結果を報告します。また、フォーカスリサーチとして、10月に再流行し現在も継続している「Gumblar」の詳細、11月に公表された「SSL/TLS の脆弱性」に関する情報、そして、「P2Pファイル共有ネットワークの調査技術」の解説も行います。

「メッセージングテクノロジー」では、2009年一年間の迷惑メールの状況の推移や、迷惑メール対策の普及に向けた国際的な協調の取り組みについて報告します。また、電子署名方式の送信ドメイン認証技術であるDKIMについても解説します。

「インターネットバックボーン」では、実際にインターネットの広い範囲を複数の手法で計測した結果を比較検討しながら、インターネットの到達性を計測するためにこれまで広く利用されてきた方法の持つ問題点を指摘し、その改善策について議論します。

IIJ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、企業活動の基盤としてインターネットを安心、安全に、また、発展的に活用していただけるように、さまざまなソリューションを提供し続けていきます。

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。

Gumblarの再流行

今回は、2009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、10月以降に再発しているGumblarに関する事件、暗号化通信に広く利用されているSSLおよびTLSのプロトコルの脆弱性の解説、P2Pファイル共有ネットワークとその調査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2009年10月から12月までの期間では、IDとパスワードを盗み取るマルウェアGumblarが再発し、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、脆弱性に関しては、Webブラウザに関連するものが相次いで発見され、暗号化通信に広く利用されているSSLおよびTLSのプロトコルにも問題が見つかっています。このほか、DNS情報を不正に操作した乗っ取り事件や、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。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、2009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。

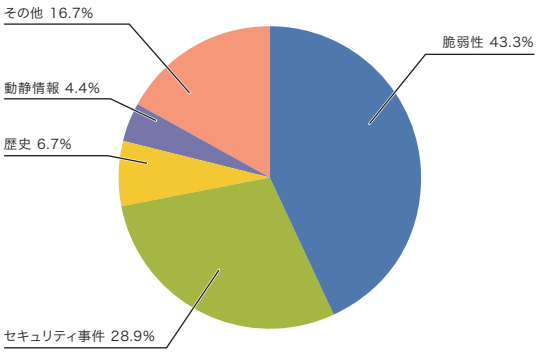


図-1　カテゴリ別比率（2009年10月～12月）

＊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]、アドビシステムズ社のAdobe AcrobatとAdobe Reader[*3]、Adobe Flash PlayerとAdobe AIR[*4]、Adobe Shockwave Player[*5]、オラクル社のJava Runtime Environment（JRE）[*6]等、Webブラウザに関係する脆弱性が数多く発見され、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されました[*7]。

また、時刻同期に利用されるNTPサーバ[*8]やDNSサーバのBIND9[*9]等、広く利用されているサーバにも脆弱性が発見され、対策されています。加えて、多くのサービスで暗号化通信のために利用されている、SSLおよびTLSプロトコルに脆弱性[*10]が発見されました。この脆弱性に関しては「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」を参照してください。

■ 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、11月のオバマ米国大統領や12月の習近平中国国家副主席といった外国要人の来日の動きに注目しましたが、関連する攻撃等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、アップル社のiPhoneに感染するマルウェアが発見[*11]されました。また、SNS として広く利用されている twitter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[*12]が発生しました。検索エンジンなどの検索結果で詐欺的ソフトウェア（スケアウェア）に誘導される事件も継続して起こっています[*13]。

加えて、10月初旬以降、4月に大規模な活動が認められたGumblar[*14]の活動再開が確認されました。この件に関する詳細は、「1.4.1 Gumblar の再流行」を参照してください。

＊2　マイクロソフト セキュリティ情報 MS09-072 - 緊急Internet Explorer用の累積的なセキュリティ更新プログラム（976325）（http://www.microsoft.com/japan/technet/security/bulletin/ms09-072.mspx）。
＊3　Security updates available for Adobe Reader and Acrobat APSB10-02（http://www.adobe.com/support/security/bulletins/apsb10-02.html）。
＊4　Adobe Flash Player用のセキュリティアップデート公開 APSB09-19（http://www.adobe.com/jp/support/security/bulletins/apsb09-19.html）。
＊5　Security updates available for Shockwave Player APSB09-16（http://www.adobe.com/support/security/bulletins/apsb09-16.html）。
＊6　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/6u17.html）。
＊7　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。例えば、この期間中Adobe ReaderおよびAcrobatの脆弱性について、Gumblarもしくはその類似の事件で修正が公開される前に悪用されていることをIIJでも確認している。この脆弱性は、修正が公開される前であっても、Adobe ReaderおよびAcrobatの設定でJavaScriptの利用を禁止することで一時的な対処とすることができた。
＊8　NTPにおけるサービス運用妨害（DoS）の脆弱性 JVNVU#568372（http://jvn.jp/cert/JVNVU568372/index.html）。特殊な要求パケットをNTPサーバに送ることで、応答と要求を無限に繰り返すループを作り出すことができる。
＊9　BIND 9のDNSSEC検証処理における脆弱性 JVNVU#418861（http://jvn.jp/cert/JVNVU418861/index.html）。DNSSEC利用時にキャッシュポイズニングの危険がある。
＊10 SSLおよびTLS プロトコルに脆弱性 JVNVU#120541（http://jvn.jp/cert/JVNVU120541/index.html）。
＊11 このワームの詳細についてはエフセキュア株式会社のblogに詳しい。初のiPhoneワームを発見（http://blog.f-secure.jp/archives/50301814.html）。
＊12 この攻撃の影響については次の公式blogに詳しい。Twitterブログ 昨日のDNS障害についての追加情報（http://blog.twitter.jp/2009/12/dns_19.html）。
＊13 検索エンジンの評価アルゴリズム等を利用し、特定の語句の検索結果として、悪意あるサイトへのリンクが上位に表示されるよう工夫することをSEOポイズニングと呼ぶ。例えば、次のトレンドマイクロ社のBlogでは、クリスマスシーズンに検索されると思われる単語について調査と解説を行っている。トレンドマイクロ社　SEOポイズニング：不正サイトもSEO対策？（http://blog.trendmicro.co.jp/archives/1255）。今回は 2009年9月30日に発生したサモア諸島付近の地震に関連する語句がSEOポイズニングの対象となった。
＊14 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」でも解説を行っている（http://www.iij.ad.jp/development/iir/pdf/iir_vol04_infra.pdf）。

■ その他

直接セキュリティに関係しないインシデントとしては、10月に、利用者の多いインターネット掲示板が複数のISPに対して大規模なアクセス制限を行い、一般ユーザの利用に支障が生じる等の影響が発生しました。

また、この期間においては、ユーザが利用するアプリケーション、特にWebブラウザのプラグインの脆弱性を利用した攻撃が数多く発生していたため、アプリケーションやプラグインのバージョンを確認するためのツールがリリースされています（IPA MyJVNバージョンチェッカ[*15]やFirefox PluginChecker[*16]等）。さらに、マイクロソフト社の新しいオペレーティングシステム Windows7が発売され、セキュリティ機能の向上の観点からも注目されました。

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、2009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。

＊15 MyJVN バージョンチェッカでは、利用しているPCにインストールされている対象ソフトウェアのバージョンが確認できる（http://jvndb.jvn.jp/apis/myjvn/）。

＊16 Mozilla Firefox にて次のURLを参照のこと（https://www-trunk.stage.mozilla.com/en-US/plugincheck/）。また、機能としては「ツール（T）」「アドオン（A）」から更新有無の確認を行うこともできる。本機能はFirefoxの機能であり、他のブラウザ、例えばMicrosoft Internet Explorerのプラグインに関しては別の手法での確認が必要となる。

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*17、サーバに対する攻撃*18、複合攻撃（1つの攻撃対象に対し、同時に数種類の攻撃を行うもの）の3種類に分類しています。

この3ヵ月間でIIJは、185件のDDoS攻撃に対処しました。1日あたりの対処件数は2.01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りはありません。

DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0.5%、サーバに対する攻撃が87.6%、複合攻撃が11.9%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で、65万ppsのパケットによって245Mbpsの通信量を発生させています。また、攻撃の継続時間は、全体の77%が攻撃開始から30分未満で終了し、23%が30分以上24時間未満の範囲に分布しています。今回の期間中で最も長い攻撃は、約12時間継続していました。

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*19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*20の利用によるものと考えられます。

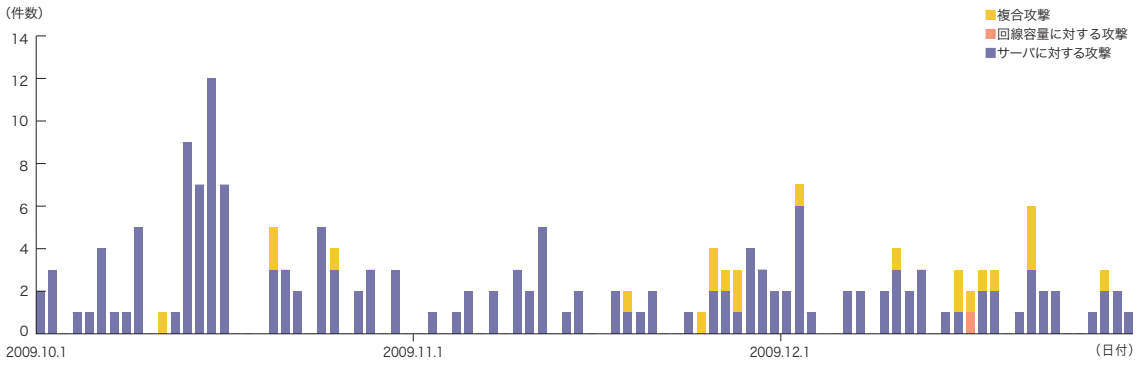


図-2　DDoS攻撃の発生件数

＊17 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。

＊18 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。

＊19 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。

＊20 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[*21]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[*22]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

2009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-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、PCリモート管理ツールが利用する4899/TCPに対する探索行為が観測されています。一方で、2582/TCP、31138/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の通信も観測されました。発信元の国別分類を見ると、日本国内の22.6%、中国の20.0%が比較的大きな割合を占めています。

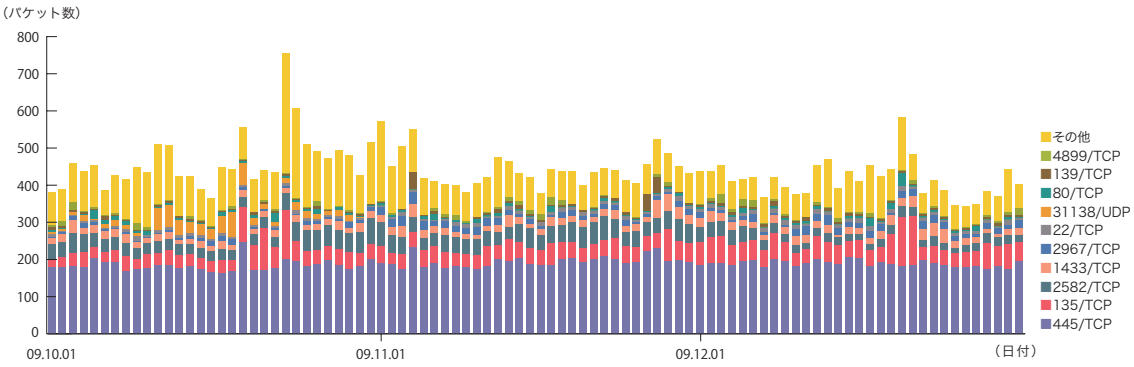


図-3　ハニーポットに到着した通信の推移（日別・宛先ポート別・一台あたり）

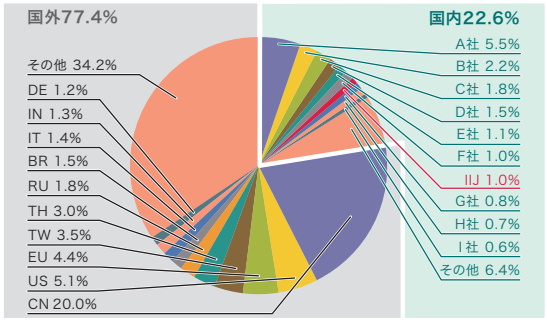


図-4　発信元の分布（国別分類、全期間）

＊21 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、流行状況や技術情報を把握し、対策につなげる試み。

＊22 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[*23]の総数を総取得検体数、検体の種類をハッシュ値[*24]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623、ユニーク検体数が44です。前回の集計期間での平均値が総取得検体数で592、ユニーク検体数で46でした。今回は、総取得検体数においても、検体の種類を表すユニーク検体数においても前回と同程度の値でした。

検体取得元の分布では、日本国内が60.2%、国外が39.8%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3.0%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4.3%、ボット型93.1%、ダウンローダ型2.6%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[*25]と519個のマルウェア配布サイトの存在を確認しています。

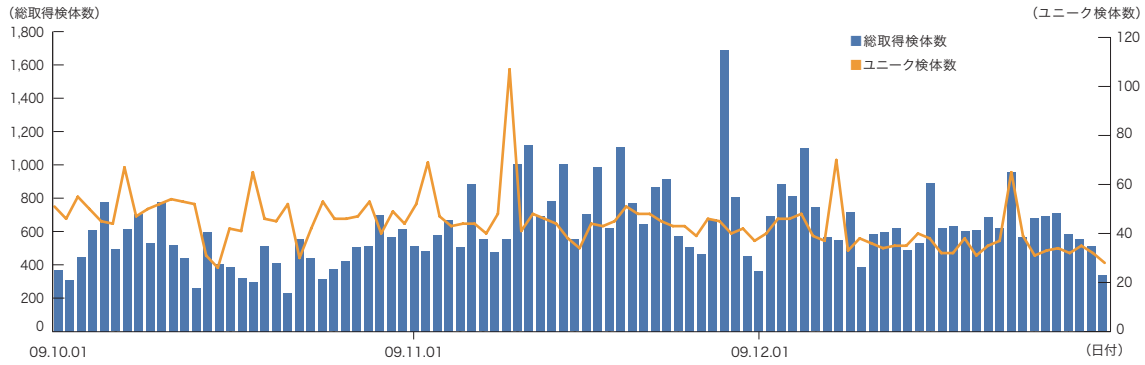


図-5　取得検体数の推移(総数、ユニーク検体数)

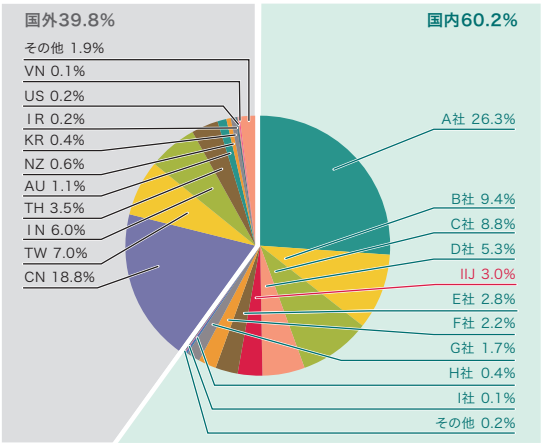


図-6　検体取得元の分布 (国別分類、全期間)

＊23 ここでは、ハニーポット等で取得したマルウェアを指す。

＊24 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。

＊25 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*26について継続して調査を行っています。SQLインジェクション攻撃は、過去にもたびたび流行し話題となった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

2009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-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61.7%、中国6.7%、米国5.3%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。散発的にみられる攻撃の増加は、特定の攻撃元から複数の宛先への攻撃を検知したものです。

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。

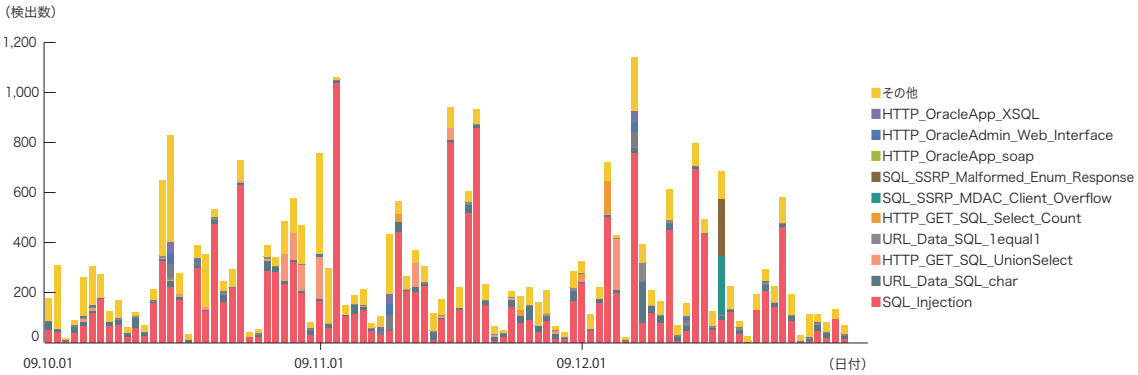


図-7　SQLインジェクション攻撃の推移（日別、攻撃種類別）

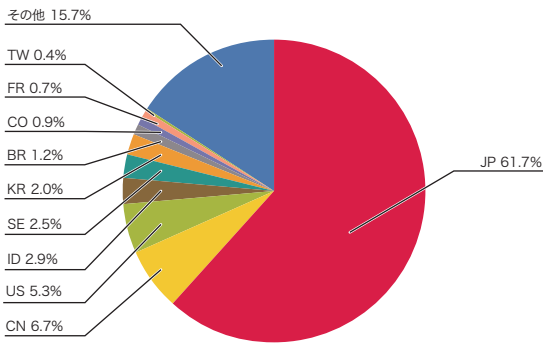


図-8　SQLインジェクション攻撃の発信元の分布（国別分類、全期間）

＊26 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の再流行、SSLおよびTLSのrenegotiation機能の脆弱性を利用した中間者攻撃、P2Pファイル共有ネットワークの調査技術について、その詳細を示します。

1.4.1 Gumblar の再流行

2009年4月以降に流行したマルウェアGumblarが2009年10月から12月にかけて再流行し、被害が拡大しました。ここでは、最近の事件について、前回のGumblarとの違いに着目して解説します*27。

■ 新しいGumblar

Gumblarは、事前に盗み取ったFTPアカウントを悪用したWebコンテンツ改ざんに始まる、マルウェア感染事件です。感染したマルウェアによってIDとパスワードが盗まれ、それが次の改ざんに悪用されることで被害が拡大します。この事件は、複数のWebサイトと複数のマルウェアが関係する複雑な事件です*28。今回の流行は、10月12日頃に複数のWebサイトが改ざんされたことで明らかになり*29、本稿執筆時点でも断続的に発生し続けています。

前回と同様に、今回再発した事件においても、複数のWebサイトを経由してマルウェア感染に誘導する流れは変わっていません。前回はマルウェア配布サイトが専用に用意された少数のサーバでしたが、今回は改ざんされた多数のWebサイトが悪用されています。このため、今回の流行では、マルウェア配布サイトへのアクセスを禁止したり、そのサイトを停止（テイクダウン）したりすることで被害拡大を食い止めることが困難となりました（図-9）。

今回改ざんされたWebサイトや、盗み取られたIDやパスワードの総数は不明ですが、その活動の規模を示す情報が、いくつか公開されています。例えば、マルウェア感染に誘導するように改ざんされたWebサイト数が約8万（日本国内に3千以上）、マルウェア配布サイト数としては2千以上（日本国内に約80）が存在したという報告があります*30。

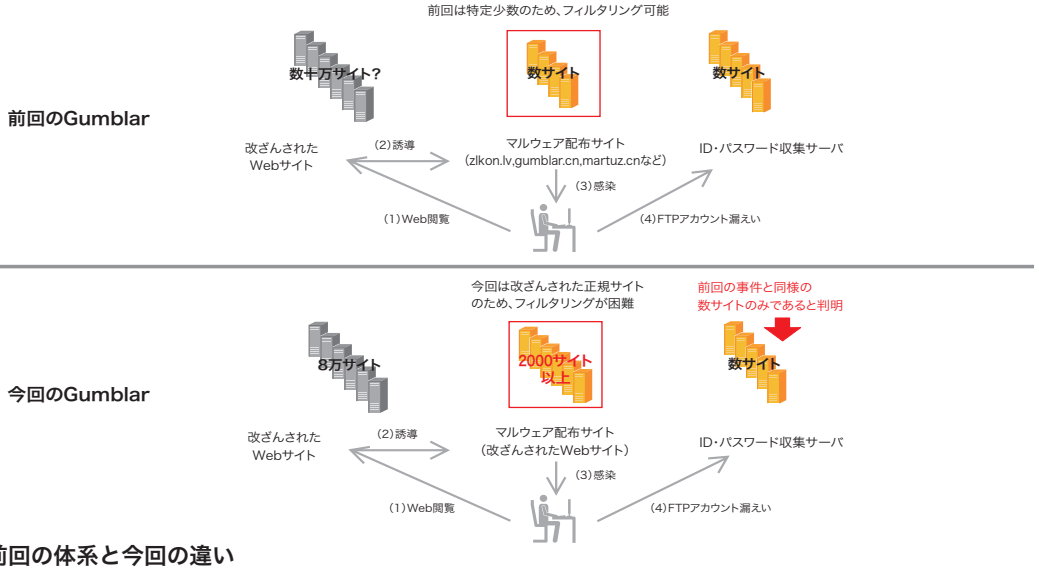


図-9　前回の体系と今回の違い

＊27 Gumblarとは2009年4月～5月当時マルウェア配布Webサイトのドメイン名（gumblar.cn）の一部。本稿では関係するWebサイトやマルウェアなど、全体を示す名前としてGumblarを使う。一般には、今回の流行を前回と区別するために、Gumblar.Xと呼ぶこともある。

＊28 Gumblarにかかわる Webサイトの役割やマルウェアの動作解析結果等、4月に流行した事件の詳細については、IIR Vol.4「1.4.2 ID・パスワード等を盗むマルウェア Gumblar」を参照のこと（http://www.iij.ad.jp/development/iir/pdf/iir_vol04_infra.pdf）。

＊29 cNotesでは、10/12にこの攻撃が観測され始めていることを伝えている。「zlkon、gumblar、martuz 再臨（http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=zlkon%A1%A2gumblar%A1%A2martuz+%BA%C6%CE%D7）。

＊30 本文中のサイト数は次のKaspersky Labs社のblogによるAnalyst's Diary,"Gumblar infection count"（http://www.viruslist.com/en/weblog?weblogid=208187923）。

■ 今回利用されたマルウェアと対策

IIJでは、今回利用されたマルウェアの複数の検体を解析しました。その結果、前回のマルウェアに複数の機能が追加されたものが悪用されていることを確認しています[*31]。また、盗んだIDとパスワードをサーバに送る通信も、前回と同様に行われています。この通信では、通常のHTTPリクエストには出現しない、RFCに違反した特徴的なヘッダが使用されています。このため、これらをProxyサーバやIDSなどで監視することで、感染者を発見したり、IDやパスワードの漏えいを防止したりすることが可能になります(図-10)。盗み取ったIDやパスワードをアップロードするサーバが前回と同様に少数であることが判明したため、これらのサーバについて停止[*32]を行うことで対策を試みました。しかし、すぐに別のサーバを利用して活動が再開したことが確認されています。

■ より新しい事件

この事件と並行し、12月初旬からまったく異なる改ざん内容や感染手段と、新しいマルウェアおよび異なる通信手段を利用した事件が発生しています[*33]。マルウェアを感染させる手段が高度になり、Java実行環境の脆弱性[*34]や、Adobe Reader(Acrobatを含む)の新たな脆弱性[*35]等が悪用されています。また、感染させられるマルウェアは、FTPクライアントの設定等からもIDとパスワードを盗んだり、ボットのような動きをすることも確認されています。この事件では、2009年末から2010年初めにかけて多数のWebサイトが改ざん被害に遭っています。

以上のように、Gumblarは現在も継続中の事件であり、引き続き、クライアントのOSやソフトウェアのバージョン管理、パスワード管理、Webコンテンツ改ざんに注意が必要な状況です。

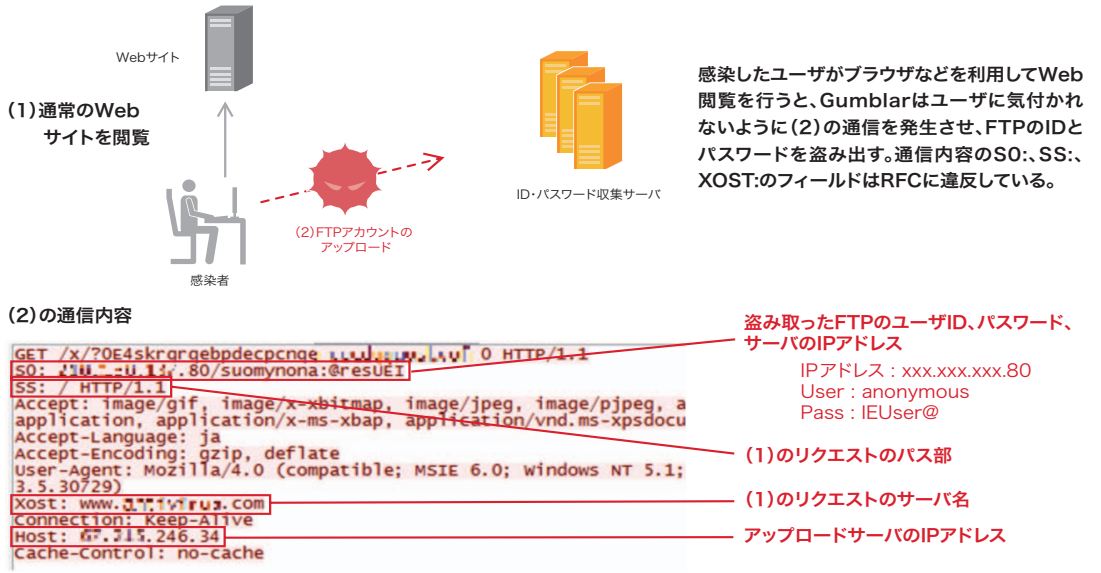


図-10 GumblarによるFTPアカウントを盗む通信

＊31 レジストリの隠ぺいや特定Webサイトへの通信妨害、rootkit検査ツールの起動の妨害など。rootkitとは、元々UNIX上のroot権限を奪取するために使われるツールのこと。この行為を隠ぺいするツールも同時に利用されることが多く、権限奪取と隠ぺいのツールを総称してrootkitと呼ぶようになった。GumblarはID・パスワードを盗むためにAPIのフックや特定レジストリの存在の隠ぺいなど、rootkit的な動作をするため、rootkit検査ツールによる発見を阻害しようと試みている。

＊32 IIJが確認したサーバについては、JPCERT/CCに停止依頼を行った。このような悪性活動を行うサーバの停止依頼等は、JPCERT/CCの「インシデント報告の届出」から行うことができる(http://www.jpcert.or.jp/form/)。

＊33 マルウェア感染に誘導する改ざんの様子と、利用されているマルウェアが異なるため、この事件をGumblarと呼ばないこともある。改ざんの様子からGNU GPL(CODE1, LGPL)、ru:8080、8080等様々な呼ばれ方をしている。

＊34 Java RuntimeEnvironment (JRE)の脆弱性が使われていることがIBM ISSのTokyo SOC Reportで伝えられている(http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1333966?cntxt=a1010214)。

＊35 Adobe AcrobatとAdobe Readerの脆弱性が利用されていることは、同じく、IBM ISSのTokyo SOC Reportで続報として伝えられている(http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1333971?cntxt=a1010214)。この脆弱性は、悪用された時点で、修正の公開されていない問題で、0-day攻撃となっていた。本稿執筆時点では、"Security updates available for Adobe Reader and Acrobat"(http://www.adobe.com/support/security/bulletins/apsb10-02.html)として修正されている。

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

■ 背景

2009年11月、SSLおよびTLSプロトコル*36*37に中間者攻撃*38を成立させる可能性のある脆弱性がMarsh Ray、Steve Dispensa、Martin Rex によって公表されました*39。SSLとTLSは、IP層とアプリケーション層の間に位置し、アプリケーションデータの暗号化とデータの完全性を保証し、通信相手をX.509公開鍵証明書によって認証する機能を提供します。HTTP、SMTP、POPなどのアプリケーション層の通信プロトコルと合わせて用いられるため、本脆弱性は多くのアプリケーションやシステムに影響を及ぼします。

特にHTTPS（HTTP over SSL）プロトコル*40は、多くのWebブラウザとWebサーバに実装されていますし、Marsh Rayらの報告でもHTTPSを用いた攻撃方法が例として紹介されています。さらに、これをTwitter APIに適用して攻撃者のTwitterアカウントにパスワード情報を投稿させる方法*41が公開されるなど、実際に悪用可能であることが示されました。HTTP以外のプロトコルへの適用可能性については、Thierry Zollerによって検討されています*42。FTPS、SMTPSは脆弱であり、EAP-TLSは影響を受けないことが示されていますが、POPやLDAPなど影響を受けるかどうかが明らかになっていないアプリケーションプロトコルも残っています。

本脆弱性は、SSLとTLSのプロトコル仕様そのものの問題に起因します。OpenSSL*43やApache*44などで修正が公開されていますが、その多くが問題となるrenegotiation機能を単に無効にするという修正です*45。根本的な対処のためには、現仕様を更新し、新仕様にあわせた実装に移行する必要があります。IETF*46もこの認識にあり、現在、対策を策定したRFC化を目指してインターネットドラフト*47が異例の速さで検討されています。本脆弱性は、TLSのすべてのバージョンのプロトコルに加えてSSLバージョン3.0にも影響します。SSLの仕様はIETFで策定されていませんが、新仕様ではTLSと同様に適用可能と記されています（当該ドラフト4.5節）。

■ renegotiation 機能を悪用した中間者攻撃

SSLとTLSは、アプリケーションデータを安全に送受信する前に、ハンドシェイクプロトコルにて暗号アルゴリズムや鍵情報などを共有します。renegotiation機能は、クライアントとサーバの間で合意されたアルゴリズムや鍵情報などを更新するために利用されます。今回の報告では、renegotiation機能の仕様上の問題を利用すると、中間者攻撃により、SSLやTLSの通信に割り込むことが可能であることが示されました。具体的なケースとして、セッション途中でクライアント認証（公開鍵証明書を用いたクライアント認証）に切り替えるケースが指摘されています。

＊36 Alan O. Freier, Philip Karlton, Paul C. Kocher, "The SSL Protocol Version 3.0", Internet Draft (http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00)。

＊37 Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246 (http://www.ietf.org/rfc/rfc5246.txt)。

＊38 中間者攻撃（Man in the middle attack）とは、通信に対する攻撃手法で、通信を行う2者の間に攻撃者が存在することで成立する攻撃のこと。その結果として、通信の傍受と改ざん（通信を行う2者それぞれに対する成りすましを含む）などが発生する。この攻撃手法が成立するかどうかを検討したり、対策を検討したりするうえで、あらかじめ中間に存在する攻撃者を仮定して検討する。実際に中間者攻撃を成立させるためには、その攻撃手法だけではなく、通信の間に割り込むための別の手法（例えばインターネットでは経路ハイジャック等）を併用しなければならない。

＊39 Marsh Ray, Steve Dispensa, "Renegotiating TLS" (http://extendedsubset.com/Renegotiating_TLS.pdf). 本脆弱性はCVE-2009-3555 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555)およびJVNVU#120541 SSL および TLS プロトコルに脆弱性(http://jvn.jp/cert/JVNVU120541/index.html)として管理されている。

＊40 E. Rescorla, "HTTP Over TLS" (http://www.ietf.org/rfc/rfc2818.txt)。

＊41 Twitter APIの問題を指摘するAnil Kurmusのblog "TLS renegotiation vulnerability (CVE-2009-3555)" (http://www.securegoose.org/2009/11/tls-renegotiation-vulnerability-cve.html)。ここで指摘された問題はTwitterによってすぐに修正された。

＊42 Thierry Zoller, TLS & SSLv3 renegotiation vulnerability (http://www.g-sec.lu/practicaltls.pdf)。

＊43 OpenSSL Security Advisory(http://www.openssl.org/news/secadv_20091111.txt)。

＊44 http://www.apache.org/dist/httpd/patches/apply_to_2.2.14/CVE-2009-3555-2.2.patch

＊45 renegotiation が無効になっているかどうかは次のTLS Renegotiation Testで確認することができる。TLS Renegotiation Test (http://netsekure.org/2009/11/tls-renegotiation-test/)。

＊46 Internet Engineering Task Force。インターネットに関する通信プロトコルやデータフォーマットなどの技術の標準化を行う組織。標準化仕様を規定する文書Request for Comments(RFC)の発行を行う。

＊47 RFCの草稿段階の文書をインターネットドラフトと呼ぶ。本稿執筆時点では、この問題への対策に関するインターネットドラフトは次のものであった(http://tools.ietf.org/html/draft-ietf-tls-renegotiation-03)。この文章は、後の2010年2月13日にRFC5746（http://www.ietf.org/rfc/rfc5746.txt）として発行された。本稿はインターネットドラフトをもとに執筆したもので、状態名等をRFCの内容に合わせてある。

HTTPSにおける攻撃の例を図-11に示します。この攻撃により、中間者である攻撃者は、クライアントとサーバ間での暗号化された通信に割り込むことができます。この結果、攻撃者のHTTPリクエストと正当なユーザによるリクエストを結合し、サーバに送信することが可能になります。このとき、正当なユーザのアプリケーションデータは暗号化されたままであり、攻撃者による改ざんやデータ搾取が行われない点に注意してください。攻撃者のリクエストと正当なユーザの既存のリクエストがHTTP Cookie等で結び付けられる場合、サーバは一連のリクエストが同一ユーザによるものであると解釈し、攻撃者のリクエストを受領して処理する可能性があります。

■ 仕様の改変点

次に、RFC化が予定されているインターネットドラフトでの改変点を紹介します。このドラフトでは、TLSの拡張タイプの値としての“renegotiation_info”と、本来ならば暗号アルゴリズムを表現するCipher Suiteの状態として"TLS_EMPTY_RENEGOTIATION_INFO_SCSV"が導入されています。renegotiation_info拡張を用いてrenegotiationを安全に行う実装であることを通信相手に宣言できます。具体的には、クライアントとサーバがともにハンドシェイクプロトコルで安全に共有した情報を保存しておきます。renegotiationを行う際にrenegotiation_info拡張を用いて、お互いしか知りえない情報を交換することで、それまで接続していた通信相手であることを確認します。また、renegotiation_info拡張を処理不能なTLS拡張と認識し、通信を中断する実装が存在するため、"TLS_EMPTY_RENEGOTIATION_INFO_SCSV"を用いる方法も準備されています。

■ 対策と後方互換性の問題

このインターネットドラフトがRFC化され、新たに対策された実装が普及し今回の問題が解消されることが望まれますが、移行には時間がかかると考えられます。後方互換性の観点から現バージョンとの互換性を確保すべきですが、旧実装からrenegotiationが行われた場合、正しい相手からのリクエストであるかどうかを安全に確認する手段はありません。このため新実装では、旧実装からのrenegotiation要求を拒否することが推奨されています。これは、現在の一時的な対策に相当するもので、renegotiation機能を利用することはできません。つまり、安全にrenegotiationを行う必要がある利用形態では、新しい仕様がRFC化された後、クライアントとサーバで、ともに新仕様に対応した新しい実装を導入する必要があります。

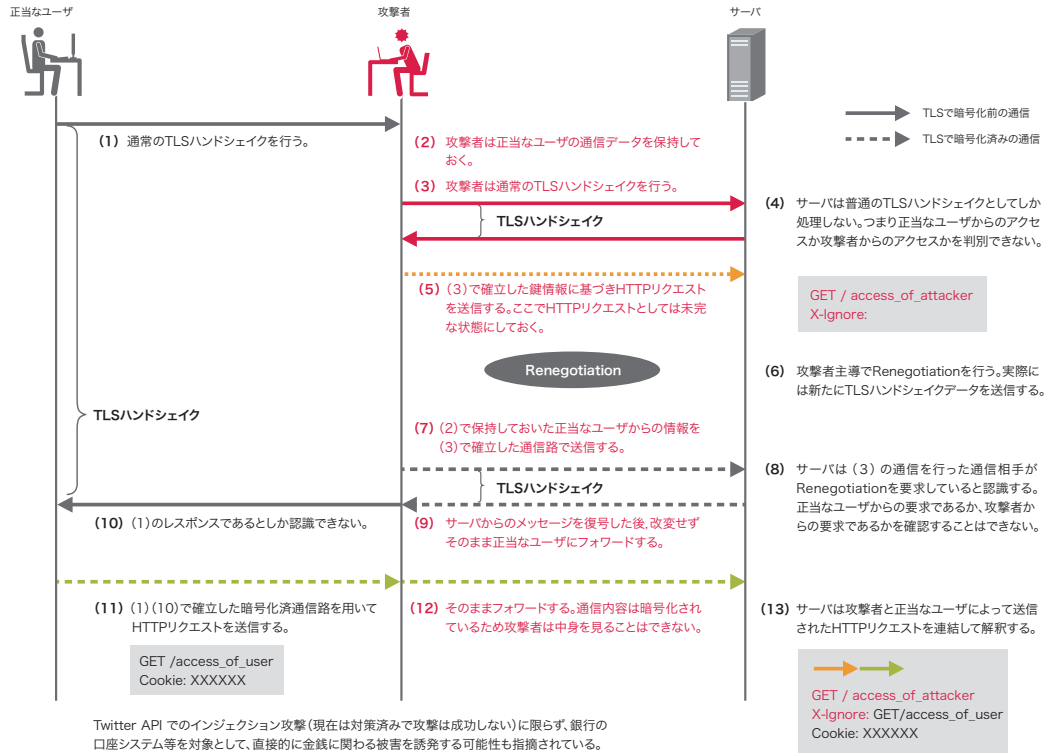


図-11 攻撃シナリオ

1.4.3 P2Pファイル共有ネットワークの調査技術

■ はじめに

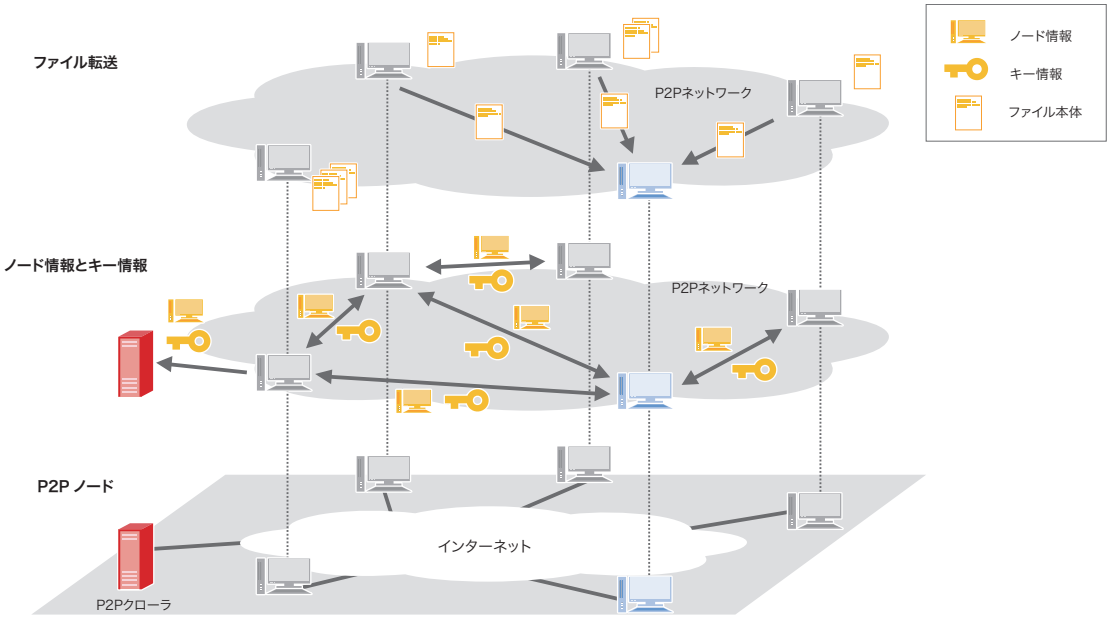
IIJでは、情報漏洩への対策の検討と通信の特性調査の2つの観点から、WinnyやShareといったP2Pファイル共有ソフトウェアが構成するP2Pネットワークの調査技術に注目し、2006年頃から関連する研究会等[*48]に積極的に参加しています。

また、2010年1月1日に施行される改正著作権法[*49]では、いわゆる「ダウンロード違法化」の規定が盛り込まれるため、著作権侵害行為との関連からP2Pファイル共有ネットワークが再び注目されています。ここでは、これを機会に、WinnyやShareといったP2Pファイル共有ソフトウェアの仕組みと、そのネットワークの調査技術についてまとめます。

■ P2Pファイル共有ネットワークの仕組み

P2Pファイル共有ネットワークには、ファイルを共有するためにファイルを公開する機能、ファイルを検索する機能、ファイルをダウンロードする機能が備わっています。P2Pノードは、希望するファイルを効率よく検索するために、どのノードがどういったファイルを持っているかを示す「キー情報」を頻繁に交換します。このキー情報交換の仕組みは、自分が公開しているファイルを他のノードに通知するためにも利用されます。

また、P2Pファイル共有ネットワーク全体でのダウンロード効率を上げるための工夫として、ダウンロードが完了したファイルを「キャッシュ」として残し、他のノードに対して自動的に公開します。ユーザ自らがダウンロードしなくても、ファイル転送の中継などによって自動的にキャッシュが作られ、公開される仕組みも備えています。この仕組みによって、「人気のある」ファイルは自動的に多くのノードで公開されるのです。そして、ピュアP2P方式で不特定多数のノードが自由に参加したり離脱したりできるようにするために、どのノードも他ノードの情報を交換し蓄積してP2Pファイル共有ネットワークを維持しています。以上の説明をまとめたものを図-12に示します。実際のP2Pファイル共有ソフトウェアは、ユーザの指定するキーワード等をもとにして、自動的にファイルを収集します。このため、P2Pファイル共有ネットワーク上でキー情報の収集とファイル転送を行う通信が常時発生し、通信量を増加させることがあります。



インターネットに接続したP2Pノード（下段）は、ノード間で接続してP2Pネットワークを構成し、ノード情報やキー情報を交換、蓄積する（中段）。ファイルをダウンロードしたいノード（図中の青いノード）は、蓄積されたキー情報からファイルを検索してファイル（もしくはその一部）を持つノードを特定し、そのノードに直接接続してファイルを転送してもらう（上段）。一方で、P2Pクローラは、ノードへの接続と、ノード情報とキー情報の収集までを行い（下〜中段）、ファイル転送は行わない。

図-12 P2Pファイル共有ネットワークの仕組み

＊48 例えば、安心・安全インターネット推進協議会 P2P研究会（http://www.scat.or.jp/stnf/）等。
＊49 著作権法の条文は、法令データ提供システム（http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi）から閲覧できる。

■ P2Pファイル共有ネットワーク調査技術

P2Pネットワークでは、全体の一元管理を行うサーバは存在しません。このため、その全体像を調べるときに、クローリング手法が用いられます[*50]。クローリングによる調査では、クローラが実際にP2Pノードに接続してP2Pファイル共有ネットワークのプロトコルで通信し、他ノードの情報を取得します。そして、そこで知り得たノードに接続し、さらに他ノード情報を取得する作業を繰り返し、P2Pファイル共有ネットワーク上のノードを網羅的に調査します（図-13）。

クローリングによる調査で、ノード情報と同時に収集されるキー情報を分析することで、どのノードでどのようなファイルが公開されているかも知ることができます。このようなクローリング手法による調査では、ファイルの拡散などの副作用を起こすことなく、P2Pファイル共有ネットワークの全体像を把握できるメリットがあります。

■P2Pネットワークの実態

P2Pファイル共有ネットワークの実態調査の例[*51]として、IIJが外部の組織と協力して実施している調査から、その結果の一部を紹介します。この調査で、IIJのネットワーク内にはWinnyのノード全体の約2%、Shareのノード全体の約3%が存在していることがわかっています。また、これらのノードがIIJのネットワークの外にあるノードとの通信で発生させている通信量を把握することで、ネットワーク全体に対する影響を評価しています。この調査の結果明らかになったWinnyとShareのノード数の推移[*52]を図-14に、IIJのネットワーク内のノードがIIJのネットワークの外にあるノードとの通信で発生させている通信量を調査した結果を図-15に示します。

これらの結果が示すようにWinny、Shareともにノード数は減少傾向にありますが、現時点でも常時約6Gbpsの帯域を占有する通信量を発生させていることがわかります。

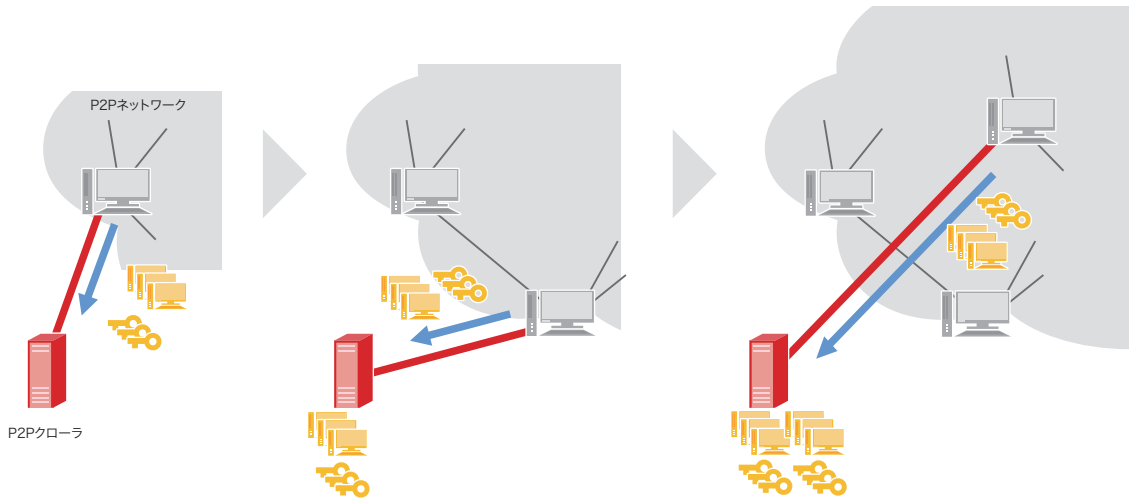


図-13 クローリング手法の概要

＊50 クローリング調査については、例えば、次の論文にも報告がある。寺田ら: クローリング手法を用いたP2P ネットワークの観測, 情報処理学会 コンピュータセキュリティ 研究報告 Vol.2007 No.48, pp.51-56（2007）（http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/CSEC07037009.pdf）。実際にこのような調査を行う製品としては、株式会社フォティーンフォティ技術研究所（http://www.fourteenforty.jp/）のWinny RadarおよびShare Radarがある。

＊51 P2Pファイル共有ネットワークの実態調査には、例えば株式会社クロスワープによる P2Pの現状 ~Winny、Shareネットワーク状況調査報告~ (http://www.scat.or.jp/stnf/contents/p2p/p2p080910_2.pdf)等がある。安心・安全インターネット推進協議会の主催による2008年9月の情報セキュリティセミナーでは、こうした実態調査が他にも複数報告され、現在はWebページから発表資料を入手できる(http://www.scat.or.jp/stnf/contents/p2p080910.html)。また、次回のセミナーは2010年3月2日に開催が予定されている(http://www.scat.or.jp/stnf/contents/p2p100302/P2P.htm)。

＊52 2010年1月1日の改正著作権法の施行日の前後では、Winny、Shareともにノード数が2割前後減少している様子が観測されている。この図が示すノード数は減少後の数値であることに注意が必要。

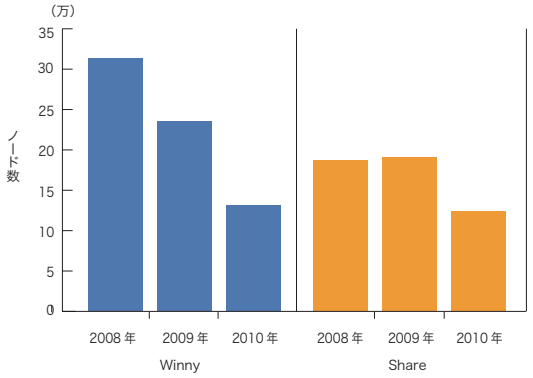
ここでは、継続的に調査を行っているWinnyとShareについて、その状況を紹介しました。P2Pファイル共有ネットワークには、まだ他にも実装があり、利用状況の変化に伴って、今後も通信特性が大きく変わる可能性があります。IIJでは、安定したネットワーク基盤を提供しつづけるために、今後もこのような調査を継続していきます。

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。

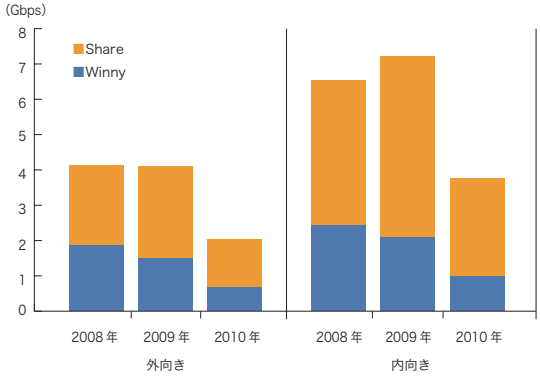
今回は現在でも継続中の事件であるGumblarの続報と、通信プロトコルであるSSLおよびTLSの脆弱性、P2Pファイル共有ネットワークの調査技術についてまとめています。特に、P2Pファイル共有ネットワークについては今日話題となったことではなく、発生させる通信量、匿名性、情報漏洩、著作権侵害等、様々な議論が重ねられているテーマであり、IIJでも長期にわたり調査を行っています。今回は調査手法と通信量への影響という形でその一部を示しましたが、今後も調査は継続しますし、別の切り口についても機会があれば紹介していきたいと思います。

IIJでは、このレポートのようにインシデントとその対応について明らかにして公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を継続してまいります。



各年1月のある1週間を対象に調査した。24時間ごとに重複を除きノードを数えて1日のノード数とし、7日間の平均をとってその年のノード数とした。

図-14 WinnyとShareの1日平均ノード数の比較



各年1月のある1週間（図-14と同一）の平均通信量を算出した。
外向きはIIJのネットワークの内から外部へ出ていく通信を、
内向きはIIJのネットワークの外から内部へ入ってくる通信を示す。

図-15 WinnyとShareの通信量（1週間の時間平均）

執筆者:
齋藤 衛(さいとう まもる)
IIJ サービス事業統括本部 セキュリティ情報統括部 部長。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の再流行）
須賀 祐治（1.4.2 SSLおよびTLS renegotiation機能の脆弱性を利用した中間者攻撃）
齋藤 衛 永尾 禎啓　（1.4.3 P2Pファイル共有ネットワークの調査技術）
IIJ サービス事業統括本部 セキュリティ情報統括部

協力:
加藤 雅彦　IIJ サービス事業統括本部 セキュリティ情報統括部

送信元の地域特性に合わせた迷惑メール対策の必要性

今回は、2009年第40週〜第52週を加えた2009年一年間での迷惑メールの割合の推移とともに、同期間での送信元地域の分析結果を示します。
また、迷惑メールの主要な送信元地域での送信傾向を推測し、地域特性に合わせた対策の必要性を解説するとともに、送信ドメイン認証技術DKIMの関連技術を解説します。

2.1 はじめに

ここでは、迷惑メールの最新動向、迷惑メール対策に関連する技術、IIJ が深く関わっているさまざまな活動などについてまとめています。迷惑メールの動向については，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機能から得た各種情報を元に、さまざまな分析を行った結果を示します。ただし、メールの流量は、提供しているサービスの対象によって曜日ごとに変動します。このため、ここでは、よりよく傾向を把握できるようにするために、一週間単位でデータを集計し、その変化に着目して分析しています。今回の調査は、2009年第40週（2009年9月28日〜 10月4日）から第52週（2009年12月21日〜 12月27日）までの13週間を加えた、2009年一年間のデータを対象にしています。

迷惑メールの動向では、地域ごとの迷惑メールの送信傾向の違いについて取り上げます。日本発の迷惑メールは、OP25B[*1]により劇的に減少しましたが、こういった対策技術が有効に機能する地域と、個別に対処していくべき特定の地域の違いが明らかになりました。さらに、迷惑メール対策のための基礎となる技術、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。

メールの技術動向では、電子署名技術に用いる送信ドメイン認証技術DKIMに関して、その署名方針を表明する DKIM-ADSPを解説します。また、DKIM-ADSPを含めてDKIMの仕様が一部改訂されたため、その改訂ポイントも示します。

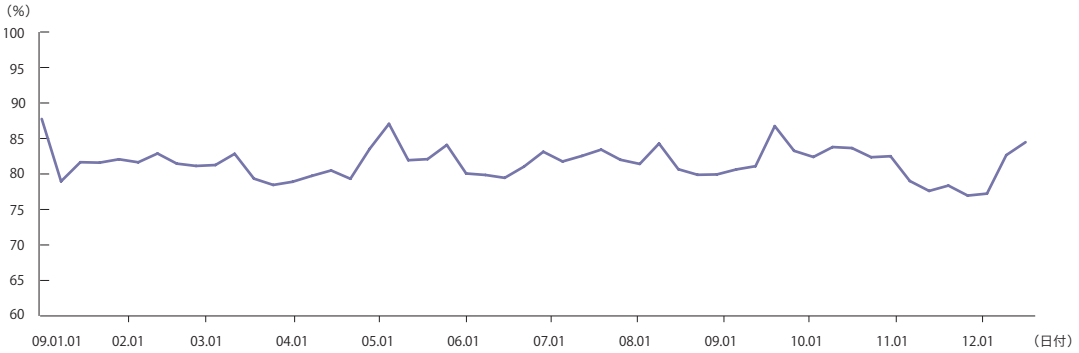


図-1　迷惑メールの割合の推移

＊1　OP25B (Outbound Port 25 Blocking)は、一般ネットワーク利用者に割り当てられた動的IPアドレスが、直接外部の受信メールサーバにメール送信すること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。

2.2 迷惑メールの動向

ここでは、迷惑メールの動向として、迷惑メールフィルタによってIIJが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。

2.2.1 迷惑メールの割合の推移

2009年第40週から第52週までの91日間に検出した迷惑メールの割合は、平均81.4%でした。前回（2009年第27 ～ 39週）での平均値が82.2%でしたので、0.8%減少したことになります。昨年の同時期での平均値が81.5%でしたので、ほぼ同じ傾向が続いていると考えられます。今回の調査期間を含めた2009年一年間での迷惑メールの割合の推移を図-1に示します。

迷惑メールの割合は、通常のメール流量と相対的な関係になります。このため、たとえば長期休暇やイベントなどの活動の有無によって一般的なメール流量に変化が生じると、その影響が迷惑メールの割合に現れます。また、迷惑メールの流量自体にも、時期的な変動が見られます。このため、一般的な迷惑メールの増減傾向を判断するには、長期的な視点での観測が必要です。このような点から、迷惑メールの流量は、昨年から引き続いて高い割合を維持し続けていると言えます。

今回の調査期間に見られる特徴として、11月から12月上旬にかけての迷惑メール割合の減少を挙げることができます。この期間には、迷惑メールの流量自体が減少しています。これは、通常メールとの相対的な関係で減少したものではありませんでした。ただし、その後12月後半から迷惑メールの流量が増加に転じましたので、この減少は一時的なものと考えられます。

2.2.2 迷惑メールの送信元

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、前回と同じくブラジル（BR）で、迷惑メール全体の12.5%を占めていました。ブラジルは、IIR Vol.3で報告した2009年第1四半期に1位となって以降、その位置を保ち続けています。2位から6位までの上位送信地域は、順に中国（CN）の10.4%、米国（US）の7.0%、インド（IN）の5.6%、ベトナム（VN）の5.2%となりました。順位自体は前回のものから変わっていますが、1位から6位までを占める地域は同じです。

これら6か国に日本（JP）を加えた迷惑メールの割合の推移について、これまでIIR Vol.1 ～ 6で報告してきたものを図-3にまとめてみました。このグラフから、米国（US）からの迷惑メールの割合が減少傾向であるのに対して、ブラジル（BR）、インド（IN）、ベトナム（VN）からのものが増加傾向にあることが分かります。また、中国（CN）や韓国（KR）については、時期によって変動しているため傾向を把握し難いですが、減少しているとは言えず、注意が必要です。

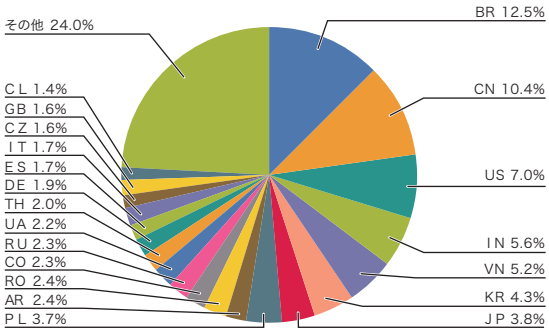


図-2　迷惑メール送信元地域

ここまでに示したように、ブラジルが日本に対する迷惑メールの主要送信元の1つであることから、日本データ通信協会とJPCERT/CCは、ブラジルと迷惑メールに関する情報交換を開始すると発表しました[*2]。この発表資料では、IIRで示してきたデータが引用されています。これまでにIIRで報告してきたとおり、迷惑メールの大部分が海外から送信されているという現状では、迷惑メールの受信量を減らすためにこういった地域の関係当局との連携が必要です。

IIJは、JEAG[*3]などによる活動と連携し、韓国や中国の関係組織と迷惑メール対策、特にOP25Bの導入について意見を交換しています。現在は、それぞれの地域固有の事情もあり、すぐに効果的な対策を実施するには至っていませんが、今後も国内外の関係組織と協力してグローバルな迷惑メール対策に取り組んでいきます。

2.2.3 迷惑メールの送信傾向

今回の調査期間では、先ほど図-2に示したように、日本(JP)は3.8%で迷惑メール送信地域の7位になっています。迷惑メールの送信割合は、前回に比べて0.7%とわずかに増加しています。また、図-3からも明らかなように、迷惑メールの割合は、IIR Vol.1で報告した時期(2008年6月～8月)から少しずつ増加しています。

日本発で迷惑メールと判定されるメールの傾向としては、これまでにも分析してきたとおり、固定IPアドレスを利用して大量送信を目的としたものが依然として多いです。これらの中には、データセンターやホスティング事業のホストと思われる送信元が含まれています。また、OP25Bが対応できていない動的IPアドレスも依然として送信元に含まれています。ただし、その割合は、他の地域に比べて圧倒的に低くなっています。

今回、特定の期間中に迷惑メールの送信元と判定された送信元のうち、迷惑メール数が1日あたり平均1通以下であったものの割合を、主要な迷惑メール送信国ごとに比較してみました。つまり、これは、迷惑メールと判定したメール送信数全体に対して、非常にわずかなメールしか送信していない送信元の割合を示すものになります。比較結果を図-4に示します。

図-4では、中国(CN)、米国(US)、韓国(KR)、日本(JP)がいずれも5%前後であるのに対して、ブラジル(BR)、インド(IN)、ベトナム(VN)が高い割合を示しています。これらの高い割合を示す地域は、いずれも図-3に示したグラフで迷惑メール送信の割合が増えている地域です。近年増加している迷惑メールの送信手法が不正プログラム(malware: malicious software)に感

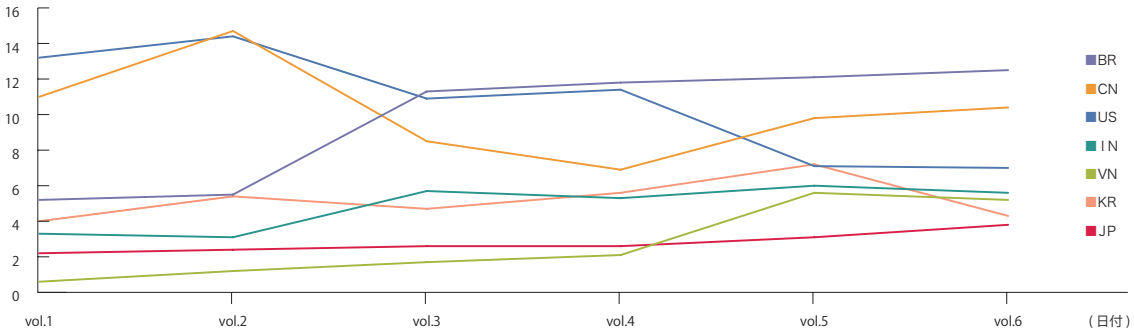


図-3　迷惑メール送信元の推移

＊2　報道資料: ブラジルとの迷惑メールに関する情報交換の開始について(http://www.dekyo.or.jp/soudan/image/n-image/PL_20100108.pdf)
＊3　JEAG (Japan Email Anti-Abuse Group)は、2005年3月に主要ISPや携帯電話事業者を中心に設立された、迷惑メール対策のためのワーキンググループ(http://www.iij.ad.jp/news/pressrelease/2005/0315.html

染させられたボット（bot）と考えられていることから、これらの増加している地域でボットが増えていると考えられます。

ボットに感染しやすいPCは、対策が不十分な個人利用のPCであり、その都度IPアドレスが変わる動的IPアドレスを主に利用します。今回の調査では、これらの地域で同一送信元（IPアドレス）からの迷惑メール送信数が少ないという結果になりました。この理由は、動的IPアドレスにあると考えられます。このような地域では、OP25Bなどのネットワークレベルで迷惑メールを直接送信できないようにする技術の導入が効果的です。

一方、1日にわずかな数の迷惑メールしか送信しない送信元の割合が低いにもかかわらず、迷惑メールの送信割合が高い地域は、特定の送信元が大量に迷惑メールを送信していると考えられます。日本は、OP25Bの導入によって動的IPアドレスからの迷惑メール送信がそれほど多くないため、図-4で示した割合が低いことが説明できます。中国や韓国の割合が低いことは意外かも知れません。これらの日本に近い地域では、特定の送信者が日本に向けて大量に迷惑メールを送信していると考えられます。実際に、2007年に逮捕された迷惑メール送信事業者は、中国国内にPCを設置して日本へ迷惑メールを送信していたと報道されています。こういった地域では、特定の大量迷惑メールの送信元を処分することで、迷惑メールの送信量の減少が期待できます。

このように、即効性のある迷惑メール対策としては、それぞれの地域の事情や特性に合わせた対策が肝要であると考えています。

2.2.4 送信ドメイン認証技術の導入状況

ネットワークベースの送信ドメイン認証技術の一つSPFについて、今回の調査期間（2009年10月～12月）での認証結果の割合を図-5に示します。この期間に受信したメールについて56.3%の認証結果が“none”でした。これは、受信メールの43.7%のドメインがSPFレコードを宣言したいたことを示しています。

この送信元のSPFの導入割合は、前回（vol.6）とほぼ横ばいですが、認証結果“pass”の割合が今回は15.9%となり、前回の13.5% から2.4%増加しました。迷惑メール量の若干の減少が影響しているかもしれません。もう一つの特徴として、認証結果“neutral”の割合が4.3%となり、前回から2.3%減少しました。これは、SPFレコードの末尾に宣言する“?all”部分に適合する割合が減ったことを意味しています。SPFの仕様では“?all”はテスト的な意味を持ちますので、テスト運用のドメインから本格運用に切り替えたドメインが増えていると考えられます。

今後も IIR では、送信ドメイン認証技術の導入状況について調査を継続し、適宜報告していきます。

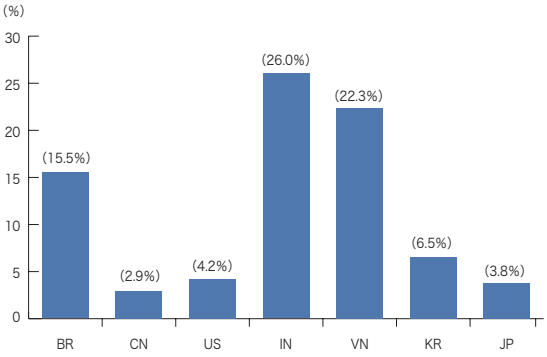


図-4　迷惑メールの送信頻度が低い送信元割合

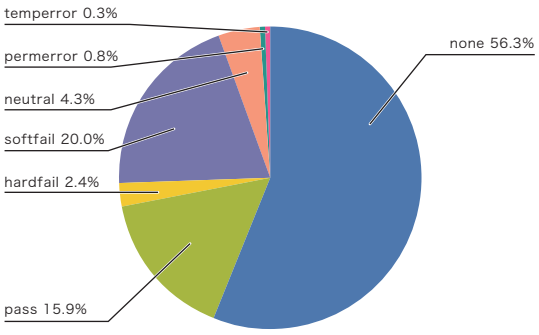


図-5　SPF の認証結果の割合

2.3 メールの技術動向

2.3.1 DKIM ADSP とその経緯

DKIM (DomainKeys Identified Mail) については、すでにIIR Vol.3でその技術を詳細に解説しています。DKIMでは、メールヘッダと本文から電子署名を作成し、それをDKIM-Signatureヘッダとしてメールに添付することで、メール受信者側で認証を行うことができます。また、DKIMには、電子署名を検証するために必要となる公開鍵を送信者側のドメインのDNS上で公開することで、特別な認証機関や配布手段を用意しなくても送信者側のシステムで完結できるという特徴があります。メールの受信者側は、受信したメールのDKIM-Signatureヘッダから署名情報を取得し、それを検証することで送信ドメインの認証を行います。この手順には、SPF/Sender IDなどネットワークベースの送信ドメイン認証技術との大きな違いがあります。

ネットワークベースの技術は、いずれのものも送信者情報として既存の情報 (SMTP上のreverse-pathやFromヘッダなどのPRA情報) を利用しているため、SPFレコードの取得場所が明確であり、SPFレコードの有無を確認することで送信ドメイン認証技術に対応している送信者であるかどうかが判断できます。これに対してDKIMでは、DKIM-Signatureヘッダが存在しているときにはそれを元に認証処理を実行すればよいのですが、ヘッダが存在していないときにはそれが元々DKIMに対応していない送信者によるものなのか、何らかの事情によってそのメールだけにDKIM-Signatureヘッダが付けられていないのかが判断できません。これは、電子署名に利用する公開鍵を取得するためには、DKIM-Signatureヘッダに指定されているセレクタ (selector) 情報が必要であり、送信側のドメイン名だけではDKIMに対応しているかどうかを判断できないためです。

また、ネットワークベースの技術では、SPFレコードの末尾に設定する“all”の前に記述した限定子 (qualifier) の種類によって、認証が失敗したときの強度をメール送信者側が指定できます。

これに対して、DKIM本体の仕様 (RFC4871) だけでは、DKIM-Signatureヘッダが存在しているときには認証の可否は判断できますが、認証が失敗したときに受信者側が振る舞うべき指針を送信者側が指定することはできません。このため、送信者側で署名方針を表明するための手段として、ADSP (Author Domain Signing Practices) がRFC5617として策定されました。

当初、DKIMの仕様検討段階には、こうした送信者側の意思を表明したり、現在のメール利用の流れに沿ったメールの配信者と実際のメール送信者 (作成者) を分離できるような仕組みが必要であることが指摘されていました。しかし、送信者が誰であるかという部分の議論がなかなかまとまらなかったこともあり、普及のためにDKIMの本体部分をまず仕様として出すべきとの判断から、RFC4871が公開されました。その後も、この送信者側の方針部分に関しては、継続して議論が行われましたが、結果としては核となる基本部分だけをADSPとしてまとめることになりました。このため、仕様の名称についても、議論を進める過程で次のように変化していきました。

表-1　DKIM-ADSP名称の変遷

仕様時期	略称	名称
2006年 1月 10日	SS	Sender Signing Policy
2007年 3月 3日	SS	Sender Signing Practices
2008年 8月 26日	ASP	Author Signing Practices
2009年 1月 3日	ADSP	Author Domain Signing Practices
2009年 8月	ADSP	RFC5617

2.3.2 DKIM ADPS の概要

DKIM ADSP (DomainKeys Identified Mail Author Domain Signing Practices) は、RFC5617としてその仕様が公開されています。ADSPの情報は、DNS上にADSPレコードとして公開することになっています。

具体的には、DNSのTXT資源レコードを利用します。この情報は、メールのFromヘッダ領域に示されているAuthorアドレスのドメイン名（Authorドメイン）を利用して、DNSに問い合わせることで取得します。このときドメインは、DKIM-Signatureヘッダの“d=”タグに示されているドメイン名と同じになります。たとえば、Authorドメイン名が“example.jp”であったときには、次のドメイン名に対してADSPレコード（TXT資源レコード）を問い合わせます。

_adsp._domainkey.example.jp

この例からも明らかなように、ドメイン名は、Authorドメインに“_adsp._domainkey”のサブドメインを付加したものになります。ADSPレコードの記述形式は、“tag=value”（タグ形式）ですが、現在のところ“dkim=”タグだけが定義されています。“dkim=”タグには、次の値（value）が指定できます。また、ここに示す以外の値が設定されていたときには、“unknown”として扱われます。

表-2　DKIM-ADSPの値

Value	意　味
unknown	送信ドメインはメールの全部、または一部に署名している
all	すべてのメールは署名されている
dicardable	すべてのメールは署名されている。署名が正しくないときには、受信者はメールを破棄してもかまわない

2.3.3 DKIM のアップデート

DKIMの仕様は、RFC4871として2007年5月に公開されました。その2年3か月後の2009年8月には、RFC5672として、それまであいまいであったDKIM-Signatureヘッダ上の2つの識別子“d=”と“i=”の部分が整理されました。しかし、DKIMの本質部分である電子署名の作成と検証については変更がなく、それまでもきちんと整理されてこなかった第三者署名に関する有益な変更も加えられませんでした。

2.4　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、迷惑メール割合の推移と、それらの送信元に関する情報を報告しました。また、迷惑メールの主要送信国に関して、同一送信元からの迷惑メール送信数に着目してその違いをまとめ、考察しました。IIJでは、今後も実際に流通されているメールを元に迷惑メールの特徴や傾向を分析し、グローバル環境でそれぞれの特徴に応じた迷惑メール対策について貢献していきたいと考えています。さらに、メールの技術動向では、今後普及が期待される電子署名方式の送信ドメイン認証技術であるDKIMと、その周辺仕様であるADSPの概要について解説しました。IIJが提供するSecureMXサービスは、すでにDKIM ADSPに対応し、送信側に加えて、メール受信時にDKIM ADSPの情報をAuthentication-Resultsヘッダに記録するといった、送受信の両方での最新技術に対応しています。今後もIIJは、常に最新動向を把握し、いち早く有効な技術を提供できるよう努力していきます。

執筆者：
櫻庭 秀次（さくらば しゅうじ）
IIJ ネットワークサービス本部 メッセージングサービス部 サービス推進課シニアプログラムマネージャ。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。

インターネット上での到達性の計測

インターネット上での到達性は、コントロールプレーンやデータプレーンでの計測によって確認できます。ただし、この2つの計測結果には、default経路の利用などによる差異が存在しています。ここでは、コントロールプレーンとデータプレーンの計測結果で差異が生じる理由とともに、より正確な到達性の計測方法としてdual probingによる方法を説明します。

3.1 はじめに

まず、経路制御に関する話題で頻繁に登場する、AS（Autonomous System: 自律システム）とBGP（Border Gateway Protocol）とは何かを簡単に復習しておきます。ASは、単一の管理主体によって単一の経路制御ポリシーの元で管理され運用される範囲のことです。図-1に示すように、通常は1つのASが1つのISPを表しています。ただし、1つのASが2つ以上のISPに属していたり、逆に1つのISPが2つ以上の ASを持っていることもあります。また、ASには、AS番号という32ビットの数値が割り当てられています。このAS番号を使ってISPを呼ぶこともあります。たとえば、IIJのAS番号は“AS2497”ですので、IIJをAS2497と呼ぶこともあります。AS間で経路情報を交換するときには、BGP（Border Gateway Protocol）というプロトコルが使われます。各ASには、IPアドレスの一番左の桁からNビット分が共通であるアドレスのブロックが割り当てられています。これをアドレスプレフィックス、または単にプレフィックスと呼びます。BGPでは、それぞれのASが持つアドレスプレフィックスへの到達性に関する情報が交換されます。また、各ASの共通部分であるNビットをプレフィックスの長さと言います。アドレスプレフィックスの長さだけに着目するときには、/Nのプレフィックスなどと表すことがあります。

インターネットでの最も基本的なサービスは、任意の２点間での到達性の提供です。しかし、私たちは、この基本的なサービスの状況を正確に把握できているとは言い難い状態です。研究者やオペレーターは、BGPのルーティング情報を調べたり（コントロールプレーンでの計測）、pingやtracerouteなどのツールを使い実際の到達性を調べたり（データプレーンでの計測）して、このサービスの状況を把握しようとします。
ここでは、このどちらもがインターネット全体の到達性を把握するには不十分であることを示し、それを補って計測を実施しインターネットでの到達性の状況を把握する方法を示します。なお、本稿は、IIJ特別研究員のRandy Bushと、O. Maennel氏、M. Roughan氏、S. Uhlig氏が共同で実施した調査結果を日本語で解説したものです。ここで示す調査の詳細については、2009年11月ACM SIGCOMM IMC（Internet Measurement Conference）に発表された論文[1]を参照してください。

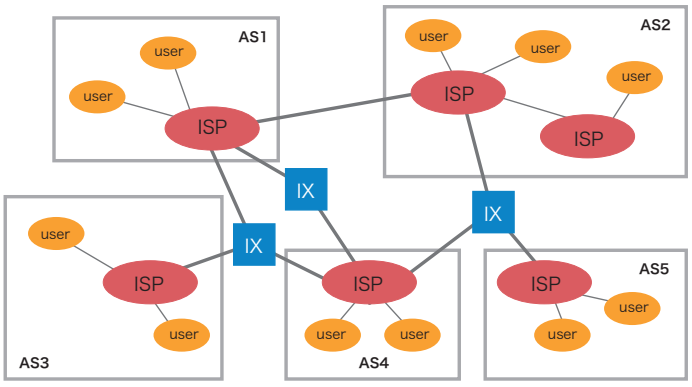


図-1 ASの概要

3.2 /25はどこまで伝搬するのか

ほとんどのプロバイダは、/24より長いプレフィックスの経路情報をフィルタによって受け取らないようにしています。これは、経路情報の処理に費やすリソースの節約や、経路の乗っ取り防止のためです。まず、このようなフィルタが実際にどの程度普及しているかを確かめてみました。

2008年6月22日にAS3130から/25のプレフィックスをアナウンスし、それがどこまで伝搬されたかをコントロールプレーンとデータプレーンの両方で計測しました。このとき、この/25を含む経路情報は、他には存在していませんでした。結果は、コントロールプレーンでの計測結果とデータプレーンでの計測結果がかなり食い違うものになりました。これは、データプレーンでの到達性を調べるときに、コントロールプレーンを調べるだけでは不十分であることを示唆しています。

コントロールプレーンでの到達性の確認は、RouteViewsやRIPE/RISといったBGPの経路モニタを参照して行いました。この結果、11個のASに/25への経路情報が伝搬されていることが確認できました。これは、/25がフィルタによって止められ遠くまで伝搬されないだろうという、私たちが予想したとおりの結果でした。

一方、データプレーンでの到達性の確認は、/25に含まれるIPアドレスをソースIPアドレスとして、インターネット上のさまざまな場所に割り当てられている多数のIPアドレスに対してpingを実行することで行いました。pingへの応答があれば、pingした相手先のIPアドレスからこの/25のネットワークへの経路が存在していることになります。これに対して、応答がないときには、pingした相手先ホストがダウンしているか、相手先ホストから/25に対する経路が確立されていないかは区別できません。このため、ここでは、応答があったときのみを考慮することにしました。

私たちの予想に反して、結果は、1,024個ものASがこの/25への到達性を持っていました。これは、実験を行ったときの全AS数の5%に相当します。インターネット全体において、この割合は大きなものではありませんが、コントロールプレーンであるBGPの経路情報を調べた結果と比べると非常に大きな数字です。

さらに、BGP経路モニタによると、/25に対する経路情報を持っていたASは、AS3130からASホップ数で2ホップ以内であることも分かりました[*1]。つまり、2つ隣のASまでしか届かなかったという事です。ホップ数ごとのAS数の分布を、図-2に実線で示します。経路情報をアナウンスしたAS3130は2つの1次プロバイダに接続されており、この/25はそこからさらに1ホップ先までしか伝搬しなかったので、インターネットの中心部にしか伝わらなかったことになります。

また、pingに応答したIPアドレスまでのASホップ数をtracerouteで測定した結果を、図-2に破線(青色)で示します。こちらは、以前に/20のプレフィックスでの到達性を調べたときの結果(図-2での赤色の破線)とほとんど変わりません。データプレーンでの計測結果は、BGP経路モニタでの結果(最大2ホップ)に比べて、より遠くのAS (最大4ホップ)から/25 に到達可能であることを示しています

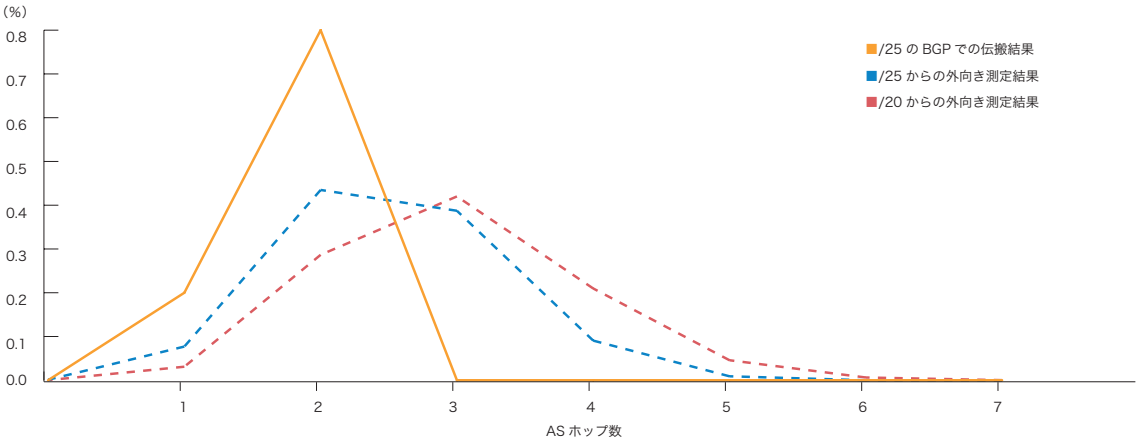


図-2 /25へのASホップ数分布

＊1 本稿では、論文[1]とはホップ数の数え方を変えて、3.3.2節でのホップ数の数え方に統一した。

このような結果から、コントロールプレーンでの計測結果とデータプレーンでの計測結果に食い違いがあることが分かります。ただし、実際のパケットはデータプレーンで運ばれるため、データプレーンでの計測結果が優先されるべきでしょう。
では、なぜ、このような食い違いが生じるのでしょうか。考えられる理由には、次の2つがあります。

- コントロールプレーンにおいて、BGP経路モニタでは観測不能なサイトにも経路情報が届いていた
- default経路によって、/25の経路情報がなくても到達可能なASが存在した

データプレーンで到達可能だったASの75%がいわゆるスタブAS[*2]でした。スタブASではdefault経路が使われる可能性が高いと考えられるため、次にdefault経路に関して調べてみることにしました。

3.3 default経路の利用状況

ここでは、ASパスポイズニングという手法でdefault経路がどの程度使われているかを調べてみます。図-3に示すように、AS3130内の計測用マシンから上位の1次プロバイダに対して、いくつかの実験用プレフィックスに対する経路情報をアナウンスします。ただし、計測対象のASにはこの経路情報が伝搬しないようにするために、ASパスに、計測対象のAS 番号を付加した上でアナウンスします。

たとえば、AS2が計測対象のASであったときには、“3130 2 3130”というASパスを持つ経路情報をアナウンスします。AS2がこの経路情報を受け取ると、自分のAS番号である“2”がすでにASパスに含まれているので、ループ回避のためにこの経路情報の受け取りを拒否します。このようにすることで、AS2がdefault経

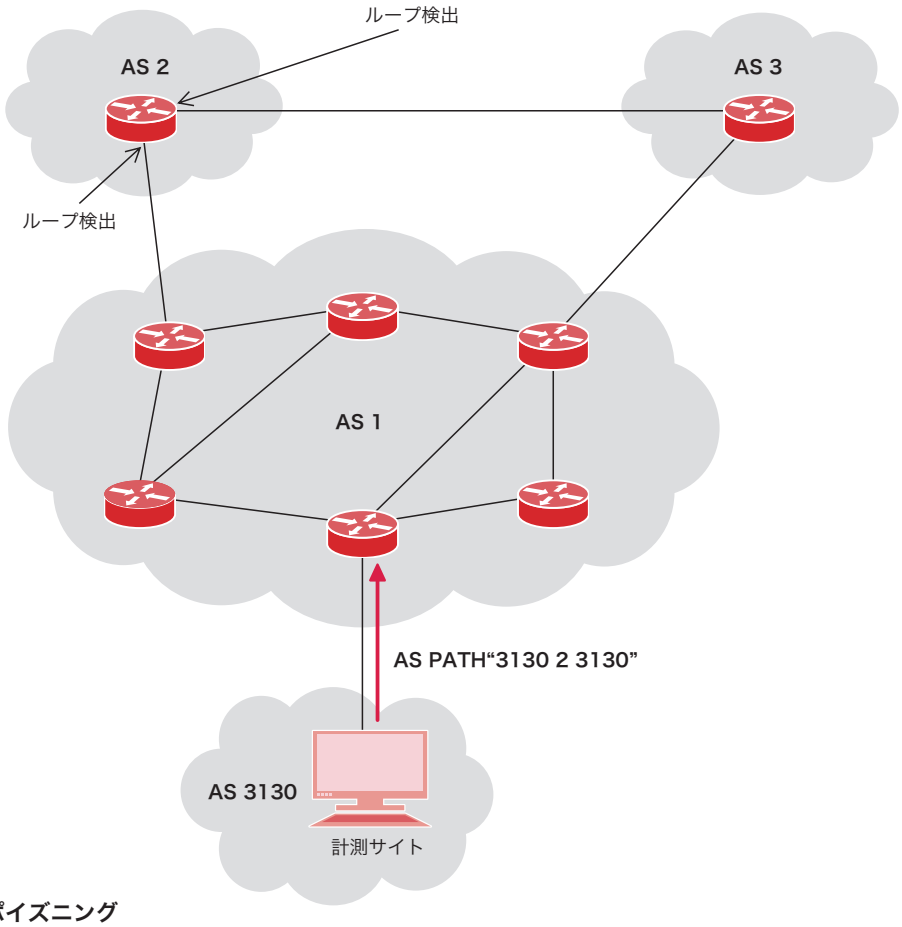


図-3　ASパスポイズニング

＊2　他のAS同士の通信を中継しないASをスタブASと呼ばれる。一方で、他のAS同士の通信を中継するASはトランジットASと呼ばれる。

路を持っていない限り、こちらの実験用プレフィックスに含まれるIPアドレスに到達できない状況を作ることができます。これをASパスポイズニングと呼びます。この方法によって、2009年4月18日～5月1日の13日間に、25,780個のASでのdefault経路の利用状況を調査しました。実験用プレフィックスには98.128.0.0/16を/24に分割して用い、次の順序で、インターネット上の広範囲に対して並行して調査を実施しました。

1. ポインズニングしていないプレフィックスのアドレスから調査対象のASが到達できる状態であることを事前に確認します
2. 次に、実験用プレフィックスのアナウンスを止め、フラップダンプニングの影響が消えるまで1.5時間待ちます
3. そして、相手先ASのAS番号を付加した実験用プレフィックスをアナウンスし、経路情報が伝搬するまで20分間待ちます
4. 実験用プレフィックス内のIPアドレスから、調査対象ASのIPアドレスリストに対してpingを送り調査を開始します

通常、1回の調査に、およそ2～3時間を要します。これを並列して行うことで、多くのASを調査しました。また、調査期間中、実験用プレフィックス以外のアドレスから調査対象ASにpingを送り続け、到達可能な状態が継続していることも確認しました。この結果、99.2%のASが継続的に到達可能な状態でした。

結果は、調査した全IPアドレスリスト中の64%がASパスポイズニングの実施後も到達可能でした。同一のASで複数のIPアドレスをテストしましたので、AS単位では74.8%（19,291個）のASがパスポイズニング実施後も到達可能でした。つまり、多くのASでdefault経路が用いられているということです。

残りのうち20.9%（5,381個）のASからは、まったく応答がありませんでした。また、4.3%（1,108個）のASからは、アドレスによって応答があったりなかったりしました。事前調査段階から到達不能なASも少数ですが0.7%ありました。これは、おそらくbogonフィルタの影響だと思われます。

今回は、応答がない場合は、そのASでdefault経路を使用していないと解釈しました。しかし、AS内のすべてのアドレスでdefault経路を使用していないかどうかはわかりませんので、この解釈は若干不正確かもしれません。また、応答があったりなかったりする場合は、相手先ASで複雑なネットワーク運用を行っていることが考えられます。たとえば、あるASでは、BGPの経路ではdefault経路を採用していないが、IP-TVやVoIPサービスのために一部のルータに手動でdefault経路を書き込んでいるそうです。このように統一されていないポリシーで運用されているASがあることも判明しました。

興味深い点としては、default経路の使用に文化的な差異があったことです。ある調査では、日本のASの60%がdefault経路を使用しておらず、36%が使用し、4%が混在しているという結果が出たそうです。

今回の調査結果は、Webサイトで公開し、調査対象のASからのフィードバックを受け付けました。回答をくれた191個のASのうち、94%が今回の調査結果が正しいことを確認してくれました。また、pingを送ったIPアドレスリストのアドレスが、そのASから他のASに委譲されたアドレスブロックに属している場合もありました。驚くべきことに、自分たちがdefault経路を使用していることを知らなかったAS管理者もいました。これは、たとえば、上位プロバイダから流れてくるdefault経路をフィルタ処理せずに受け取っていたなどの理由によるものです。

3.3.1 ASのタイプによる変化

直観的には、トランジットサービスを提供しているASのほうがスタブASよりもdefault経路の使用率が低そうです。今回の調査結果をこの観点からも分析してみました。ここでは、ASの分類は、参考文献[2]の分類に従って行いました。

表-1　ASカテゴリ別のdefault利用率分布

	調査数	Defaultあり	Defaultなし	混在
スタブ	24,224	77.1%	19.3%	3.6%
小ISP	1,307	44.5%	42.2%	13.3%
大ISP	246	17.1%	60.6%	22.3%

表-1に示すように、スタブ、小ISP、大ISPに移るに従って、default経路の利用率が下がっています。また、自AS内でのdefault経路の利用あり/なしが混在しているケースは、ISPが大きくなるに従って増えています。これは、ISPが大きくなるほど運用が複雑になっていることを表しています。ただし、大きなASになるほど、今回の調査でpingを送ったIPアドレスの個数も増えるため、この点も考慮して結果を解釈する必要があります。

図-4は、今回の調査結果を他のASとのpeerの数の分布で表したものです。少なくとも100個のASとpeerを持つまでは、default経路の利用が減少していくことが分かります。また、20個以下のpeerしか持たないASの80%がdefault経路に依存していますし、300個以上のpeerを持つASでは、default経路を使っているものが15%以下になります。

ASのタイプによってdefault経路の利用率が異なるという調査結果は、非常に興味深いものです。たとえば、スタブASでtracerouteを用いる場合、最初の数ホップは相手への明示的な経路情報がなくてもdefault経路によって進んでいけるが、大きなISPに到達したところでdefault経路が無くなり、そこで止まってしまう場合があるという事です。しかし、これは、tracerouteが止まった地点に問題があったことを示しているわけではありません。そこまでtracerouteが実行できたこと自体が、コントロールプレーンの情報から得た到達性と食い違っているということで、コントロールプレーンでの計測かデータプレーンでの計測のどちらか一方のみでは不十分であるということを示しています。

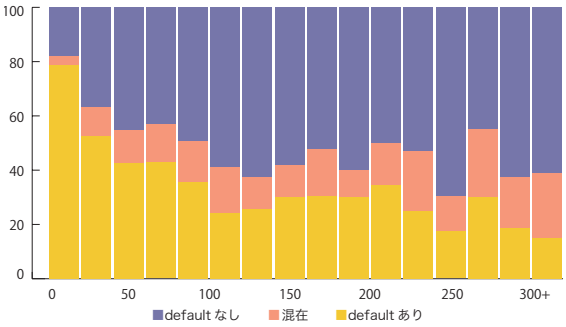


図-4　ASのpeer数ごとのdefault利用率

3.3.2 default経路の影響

default経路の存在がインターネットの計測に対して与える影響を考察するために、参考文献[2]にあるASトポロジーデータを用いたシミュレーションを行いました。シミュレーションでは、今回の測定結果でのdefault経路利用確率を用いて、トポロジーデータ内のスタブASの77.1%、小ISPの44.5%、大ISPの17.1% にそれぞれdefault経路を持たせました。なお、混在のケースはdefault経路なしに含めました。また、default経路を持たせる際にどのASに経路を向けるのかを決める方法として、ここでは2つの方法を採りました。1つはそのASの上位プロバイダからランダムに選ぶ方法(ランダム選択)、もう1つはそのASの上位プロバイダのうち最も顧客数の多いASを選ぶ方法(max選択)です。

シミュレーションでは、1,000個のASを任意に選び、それらからdefault経路のみを使っていくつのASに到達できるかを計算しました。

シミュレーションした結果、default経路のみでは、わずかな数のASにしか到達できませんでした。インターネットの全体構造が比較的フラットなものであるため、スタブASからdefault経路によって上位に移っても、1～3ホップ程度でdefault経路を持たない1次プロバイダに到達して、そこで止まってしまうからです。default経路のみで到達できるAS数は、最大でも5でした。

ここで、自分のプレフィックスに関する経路情報のアナウンスが、1ホップ先の自分の上位プロバイダのみに伝搬し、そこから先のASには伝搬しないようなケースを想定してみます。

図-5は、任意のASから到達可能なAS数の累積分布の補分布(Complementary Cumulative Distribution Function)を示しています。このグラフを見ると、default経路で経路を向けるASをmax選択で選んだ場合、約半数のASが1,000個のASに到達でき、3分の1のASが2,000個のASに到達できることが分かります。また、ランダム選択の場合でも、到達先は減りますが、それでも非常に多くのASに到達可能です。

さらに、図-5には、経路情報のアナウンスが自分から2ホップ先のASまで伝搬すると想定したときの結果も示してあります。この場合、到達可能な範囲は広がり、およそ半数のASが6,000個のASに到達できます。最大で19,000個のASに到達可能な場合もありました。

実際には、3.2の/25の到達性で考察したように、単純なホップカウントのみでなく、各ASが持っている経路フィルタの状況なども考慮しなければなりません。しかし、このシミュレーションにより、/25の経路情報であっても、自分の上位プロバイダにさえ伝搬すれば、そこから先のASにはほとんど経路情報が届いていない状況であっても、インターネットのかなり広い範囲に到達可能になることが解ります。そして、ここでの結果が、コントロールプレーンでの計測では到達できないはずなのに、データプレーンでの計測では到達できてしまうという現象をうまく説明していると考えられます。

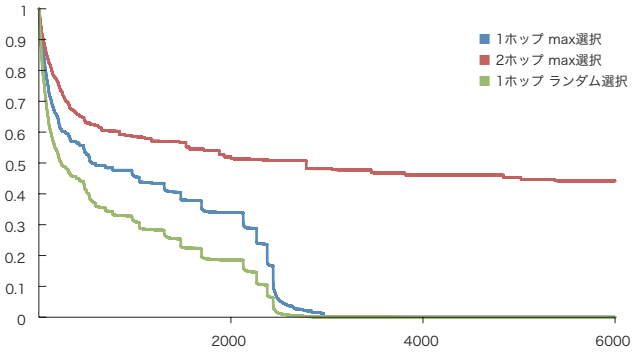


図-5　到達可能なAS数の分布

3.4 dual probingによる到達性の検査

default経路の存在は、コントロールプレーンの観測による予測に限界があることを示しています。コントロールプレーンでの計測のみで何らかの議論を行うときには、この点に注意すべきです。一方、今回の調査で用いてきたデータプレーンでの計測にも限界があります。相手先のホストや経路上に設置された機器などの振る舞いがさまざまに変化する状況下では、pingの結果を解釈することさえ難しい状況が簡単に起こります。
到達性の計測が難しい理由は、次の2つの側面を考慮しなければならないためです。

- 自分から世界がどのように見えるのか
- 世界から自分がどのように見えるのか

前者は、ルータがルーティングプロトコルから得る情報に基づいたものになります。到達性の問題を解決するときにオペレータが知りたい情報は後者のものです。つまり、インターネットの他の部分から自分のネットワークがどのように見えているかということです。しかし、残念ながら、この情報を直接得る方法はネットワーク層に用意されていません。
BGPモニタのようなサービス、looking glassやtracerouteサーバなどを用いれば、外からの見え方を知ることは可能です。しかし、それらは、一部のASのみが公開しているサービスであり、このようなサービスから見えるものをすべて集めても、結局はインターネットの一部からの見え方しか解らないのです。
また、このようなサービスを公開しているASは一般的に大きなISPであり、結果はインターネットの中心部からの見え方に偏ったものになります。たとえば、このような中心に近いISPは、スタブISPに比べると良好な到達性を保っているため、スタブISPの到達性を検証するのには役に立ちません。したがって、インターネット全体のさまざまな視点から到達性を検証できる方法が必要になります。
ここでは、dual probingという、より広範囲な状況に適用可能なデータプレーンでの調査方法を提案します。

あるネットワーク管理者が外のホストから自分のネットワークへの到達性を確認したいとします。単純な方法として、インターネットの広い部分をカバーするIPアドレス群を選び、それらに対してpingを送る方法があります。それらのIPアドレスからpingへの応答があれば、そのIPアドレスの場所からpingを送り出したマシンへの到達性があることになります。この方法を「外向き調査 (out-probe)」と呼びます。

図-6に、外向き調査の考え方を示します。この図に示す黒色の実線は、従来からの方法であり、公開されているlooking glassなどから試験するサイトに向かって内向きに調査する方法です。一方、外向き調査では、緑色の破線で示すように、到達性を試験するネットワークから、広範囲に分布する外のサイトに向かってpingなどで調査パケットを送付します。この際、パケットのソースIPアドレスには試験するアドレス空間に属するIPアドレスを設定します。この場合、到達性があることは、pingを送った相手から自サイトへ応答が戻ってくることで確認できます。
pingに応答がなかったときには、次の理由が考えられます。

- IPアドレスを持つホストがpingに応えなかった
- IPアドレスを持つホストに到達する前に、ファイアウォールなどでpingパケットが落とされた
- IPアドレスを持つホストはpingに応答したが、応答が返ってくる途中で廃棄された
- IPアドレスを持つホストからpingを送り出したホストへの経路が確立されていなかった

3番目と4番目の理由がネットワークの到達性に関連しています。ただし、ICMPのパケットはTCP等の他のパケットに比べて優先度が低いため、3番目の理由を到達性がないことの証拠にするには弱いかもしれません。いずれにせよ、応答がなかったことだけでは情報として不十分だと言えます。
では、あらかじめどのような結果になるかが想定できているときはどうでしょうか。「3.3　default経路の利

用状況」で事前調査を行った後に実際の調査を行ったように、想定される結果に対して実際の調査結果がどのようであったかを比較することで有益な情報を得ることができます。つまり、調査を2回に分けることで、2回目の調査結果をより深く解釈できるのです。また、調査の回数を分けるだけでなく、pingを送る相手のIPアドレスを複数用いることなども可能です。この方法を「dual probing」と呼ぶことにします。ただし、「dual」と言っても、この方法には3つ以上の調査を含めることも可能です。

dual probingでは、実験用プレフィックスからの調査結果と、基準プレフィックスからの調査結果を比較します。基準プレフィックスには、以前から利用し、非常に良好な到達性を持つことが確認できているプレフィックスを選びます。この比較によって、実験用プレフィックスのみの調査に比べて、より深く状況を理解できるようになります。仮に、基準プレフィックスからのpingに応答がなかったときには、実験用プレフィックスから調査する必要はありませんし、どちらに対しても応答があったときには到達性に問題がないことが分かります。また、基準プレフィックスには応答があったが、実験用プレフィックスに応答がなかったときには、pingの送り先のIPアドレスから当該サイトまでのどこかに到達性に関する問題があることが分かります。ICMPの優先度の問題でパケットが落とされている可能性は残りますが、何回か計測を繰り返すことで結論を得られるはずです。

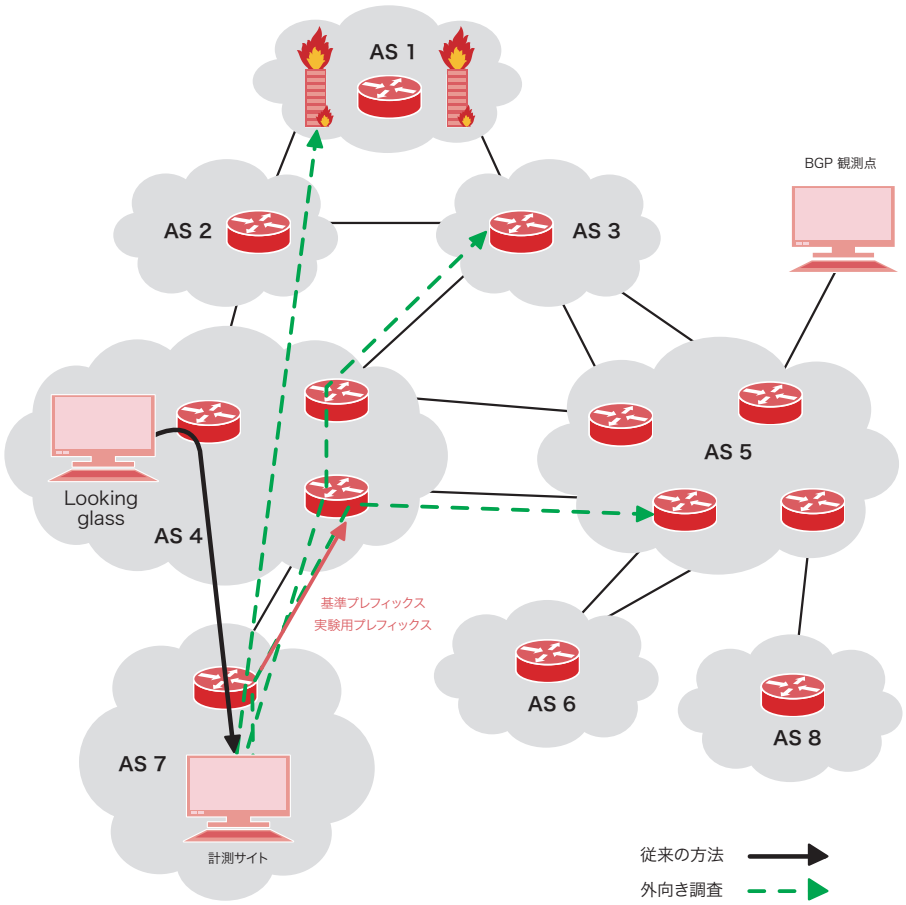


図-6　Dual Probingの考え方

3.4.1 間違ったbogonフィルタの検出

bogonとは、間違った経路情報アナウンスのことです。bogonは、何かの事故によって発生したり、アドレス空間のハイジャックを狙って意図的に送られたりします。したがって、ISPは流されるはずのない経路情報に対して実際にパケット転送が起こらないようにするために、コントロールプレーンかデータプレーンにフィルタを設定しています。通常行われる方法は、まだレジストリからISPに割り振られていないプレフィックスからのトラフィックや経路アナウンスを拒絶するためにフィルタを設定する方法です。ただし、この場合、プレフィックスが割り振られ正当な経路アナウンスが始まっても、フィルタの設定が変更されず、そのプレフィックスへの到達性に問題が起こることがあります。従来の方法では、この間違ったbogonフィルタがどこにあるかを検出することが困難でした。今回、dual probingを応用して、間違ったbogonフィルタを検出する実験を行いました。

実験のために、新たに173.0.0.0/16と174.128.0.0/16をARINから割り振ってもらいました。今回、このアドレス空間に属する5つの小さな実験用プレフィックスを5か所からアナウンスしました。PSGNet（米国、シアトル）、Verio（米国、アッシュバーン）、SpaceNet（ドイツ、ミュンヘン）、CityLink（ニュージーランド、ウェリントン）、そしてIIJ（日本、東京）の5か所です。各ISPに実験用ホストを設置し、ISPが通常利用しているIPアドレスを割り当て、そのIPアドレスを基準アドレスとしました。そして、実験用プレフィックスから実験用IPアドレスを選び、実験用ホストの同じインターフェースにセカンダリーアドレスとして設定しました。

実験は、2008年4月14日、2008年5月27日、2008年6月12日の3つの時期に、それぞれ1週間程度の期間で行いました。1回目の実験は、実験用プレフィックスが割り振られたことをARINが公表する前に行いました。つまり、1回目の実験の目的は、正当なbogonフィルタがどの程度採用されているかを確認することでした。1回目の実験の後に、ARINが新たなプレフィックスを割り振ったので、bogonフィルタ用リストから外すべきであること、が公表されました。そして、私たちは、1回目の実験でフィルタを設定していたASの担当者宛に、フィルタを解除するように電子メールで依頼しました。したがって、2回目の実験で到達性が得られなかったとすると、大きな問題です。3回目の実験は、時間の経過とともに到達性に関する問題がどのように変化するかを観察するためのものでした。

また、到達性に関する問題を正確に把握するため、今回の実験では、基準アドレスに5回以上の応答があるにもかかわらず実験アドレスに1回も応答がないときに

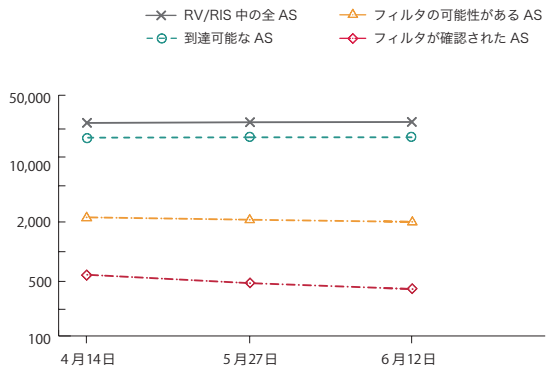


図-7　bogonフィルタ検出実験

限って、到達性に問題があると結論づけることにしました。実験アドレスに1回も応答がなくても基準アドレスへの応答が5回未満であったときには、問題の「可能性がある」とするにとどめました。
図-7に、実験の結果を示します。ここで、黒色の実線が全ASを表しています。また、緑色の破線が問題のなかったASです。bogonフィルタの設置が確認されたASは、赤色の破線で示した、およそ500個でした。また、黄色の破線で示した2,000個近くのASにもフィルタが設定されているようでした。

この実験結果から、インターネット全体の2～7%のASで、新たに割り当てられたアドレスが見えなかったことになります。また、2回目と3回目の実験で、到達性の問題がほとんど改善されていないことも分かります。これは大きな問題です。
図-8は、フィルタの設定が確認されたASと、フィルタがある可能性のあるASの分布を、ASのタイプ別に示しています。この図では、ほとんどがスタブASであり、インターネットの外縁部で問題が発生していることを表しています。ただし、トランジットASに問題があるにもかかわらず、スタブASに問題があると誤解することもあるため、この点には注意が必要です。

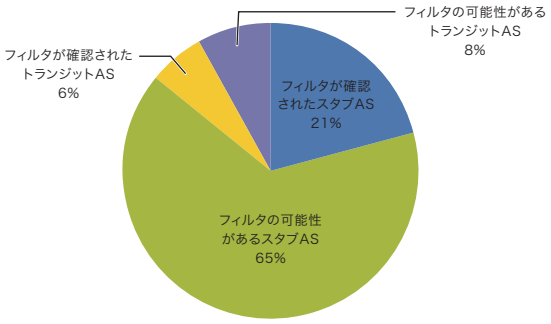


図-8　ASタイプ別分布

3.5　計測結果の確からしさに影響する項目

ここまで、コントロールプレーンからの計測が到達性の状況を正しく表していないこと、そして、データプレーンでの計測によってそれを補えること、を示してきました。しかし、データプレーンでの計測にも限界があります。ここでは、データプレーンでの計測で考慮すべき課題を3つの観点から簡単にまとめます。

3.5.1　トポロジー上でカバーする範囲

外向き計測の実施目的は、BGPモニタやlooking glassではカバーしきれない範囲をカバーすることです。つまり、インターネットの中心部でなく外縁部からの到達性を見ることです。このためには、「3.4 dual probingによる到達性の検査」で用いたようなインターネット全体をカバーするIPアドレスリストを作ることが重要です。このアドレスリストには、広範囲をカバーし、AS内部で統一されていない設定パラメータなども調査できるものであることと、必要最小限の個数であることが要求されます。作成するIPアドレスリストの質によって、実際の計測の質が左右されます。

3.5.2 IPアドレスとAS番号のマッピング

IPアドレスが属するASを決めることも重要な課題です。これには、BGPのルーティングテーブルを参照するなどの方法が採られます。しかし、たとえば、トランジットプロバイダが顧客のプロバイダを接続する際に、自分のASに割り振られたアドレスブロックからIPアドレスを提供することがあります。このとき、この顧客ASのボーダーにあるルータがbogonフィルタ等によって特定のプレフィックスへの到達性を持っていなかった場合であっても、上位プロバイダからの到達性がないと判断してしまう可能性があります。

また、IPアドレスとAS番号の正しい対応表を作った後には、そのメンテナンスも重要です。たとえば、私たちが2007年に作った対応表と、2009年に作った対応表を見比べてみると、同じASに対応するプレフィックスは88%しかありませんでした。IPアドレスとAS番号の対応に誤りがあると、観測結果の解釈を間違えてしまいます。

3.5.3 どの計測ツールを使うか

データプレーンでの計測に用いるツールの選び方も重要です。pingを使うのか、tracerouteを使うのか。また、pingを使うにしても、ICMP、UDP、TCPなど、どのタイプのパケットを用いるかも大切な選択です。今回の調査を実施する際に分かったことは、ICMPでは約70%のIPアドレスに到達可能でしたが、UDPではわずか30%にしか到達できませんでした。これは、ファイアウォールやNATによってフィルタされてしまうためです。TCPでは、さらに状況が悪化し、たった5%しか到達できませんでした。

3.6 結論

ここでは、インターネットでの実際の到達性を知ることが、公開されているBGPサーバなどのデータで見るよりもはるかに複雑なものであり、コントロールプレーンで得られる情報とデータプレーンで得られる情報に食い違いがあることを示しました。また、default経路の使用によって、経路情報が伝搬しないときにもパケットの到達性が提供されることも示しました。さらに、経路情報のポイズニングやdual probingといった到達性を検証するための新たな方法も提案しました。IIJでは、インターネットが安全で安定した社会基盤として機能するよう、自社のバックボーンの安定運用に努めるとともに、本稿で示したような、インターネット全体の安定運用に関する調査と情報発信を継続してまいります。

参考文献

[1] R. Bush, O. Maennel, M. Roughan, S. Uhlig, “Internet Optometry: Assessing the Broken Glasses in Internet Reachability”, ACM SIGCOMM IMC, 2009.

[2] R.Oliveria, B. Zhang, “IRL – Internet Topology Collection,” 2009.

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。

インターネットトピック: 迷惑メール対策推進協議会

日本における迷惑メール対策法の一つに「特定電子メールの送信の適正化等に関する法律」(略称:特電法)*1があります。この法律は、平成14年(2002年)に成立し施行されましたが、3年以内に見直しをすることが条文に含まれていることもあり、これまで平成17年(2005年)、平成20年(2008年)と二度改正されてきました。
いずれの法律改正の前にも、現行の迷惑メール対策全般について検証を行うとともに、今後の方向性を検討を行う目的で、「迷惑メールへの対応の在り方に関する研究会」が開催されました。
直近の研究会は、2007年7月から開催され、2008年8月にそれまでの検討結果をまとめた、最終取りまとめが公表されました*2。
その最終取りまとめの中で、総合的な迷惑メール対策推進のための体制の必要性が述べられており、特電法の国会審議においても同様の主旨の内容が附帯決議されています。

迷惑メール対策推進協議会は、こうした背景から2008年11月27日に設立されました*3。
設立の目的や参加メンバなどは、事務局である(財)日本データ通信協会のウェブページを参照して頂ければ分かりますが、産学官それぞれの有識者からなる幅広い構成員となっています。この第一回の会合では、迷惑メール追放にむけた決意と具体的に講ずるべき措置がもりこまれた「迷惑メール追放宣言」が採択されました。
さらに、協議会発足時に迷惑メール対策に関する実務的な問題や対策の検討を行うために、構成員の一部からなる幹事会が設置されました。
幹事会では、様々な議論と平行して幹事会メンバを中心として、迷惑メールの現状や様々な対策について総合的にまとめる目的で、「迷惑メール対策ハンドブック」を執筆しました。2009年10月2日の2回目の協議会の会合(親会)で、このハンドブックが承認され、10月9日に「迷惑メール対策ハンドブック2009」が公表されました*4。このハンドブックは、迷惑メールの現状から制度的な対策、技術的な対策、様々な組織による対策についての活動などが網羅的にまとめられています。

さらにこの2回目の親会では、迷惑メール対策のための基盤技術である送信ドメイン認証技術の普及促進を目的に、「送信ドメイン認証技術WG」の設置も承認されました。

送信ドメイン認証技術は、これまでIIRでも「メッセージングテクノロジー」で何度か解説してきましたが、既存のメール配送の仕組みとの互換性を保つ一方で、その利用方法及び効果については、正しく理解しなければ誤解を生じかねない部分が幾つかあります。
こういったことから、協議会の送信ドメイン認証技術WGでは、正しく技術を理解し導入してもらうための資料をまず整備するとともに、まずは協議会構成員を中心に導入してもらうための説明会なども開催しています。
WGでは、これらの作業を通して得られた情報を元にさらに広く普及させるための施策を検討しています。

本トピックの報告者は、親会及び幹事会の構成員として、迷惑メール対策推進協議会の活動に貢献しています。
送信ドメイン認証技術WGの設置に際しては、WG の取りまとめる役割を担うことになりました。送信ドメイン認証技術は、IIRでも解説してきた通り複数の技術が存在し、それぞれの利点や欠点、導入にかかるコストなど幾つかの違いがあり、一つの技術だけで容易に目的が果たせるというものではありません。それぞれの技術の特徴を生かし、普及を促進するための段階的な導入や認証結果の利用方法など、実際的な面について検討を重ねています。
IIJは今後も迷惑メール対策に関して、業界においても主導的な役割を果た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 ネットワークサービス本部 メッセージングサービス部 サービス推進課シニアプログラムマネージャ。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。

＊1　特電法: http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#ordinance
＊2　「迷惑メールへの対応の在り方に関する研究会」最終とりまとめの公表: http://www.soumu.go.jp/menu_news/s-news/2008/080828_8.html
＊3　迷惑メール対策推進協議会: http://www.dekyo.or.jp/soudan/anti_spam/index.html
＊4　迷惑メール対策ハンドブック2009」の公表について: http://www.dekyo.or.jp/soudan/anti_spam/image/200910press1.pdf

Ongoing Innovation

Vol.6 February 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-MKTG019FA-1002KO-08000PR