Internet Infrastructure Review

IIJ
Internet Initiative Japan

Vol.5

November
2009

インフラストラクチャセキュリティ

米国および韓国における大規模DDoS攻撃

メッセージングテクノロジー

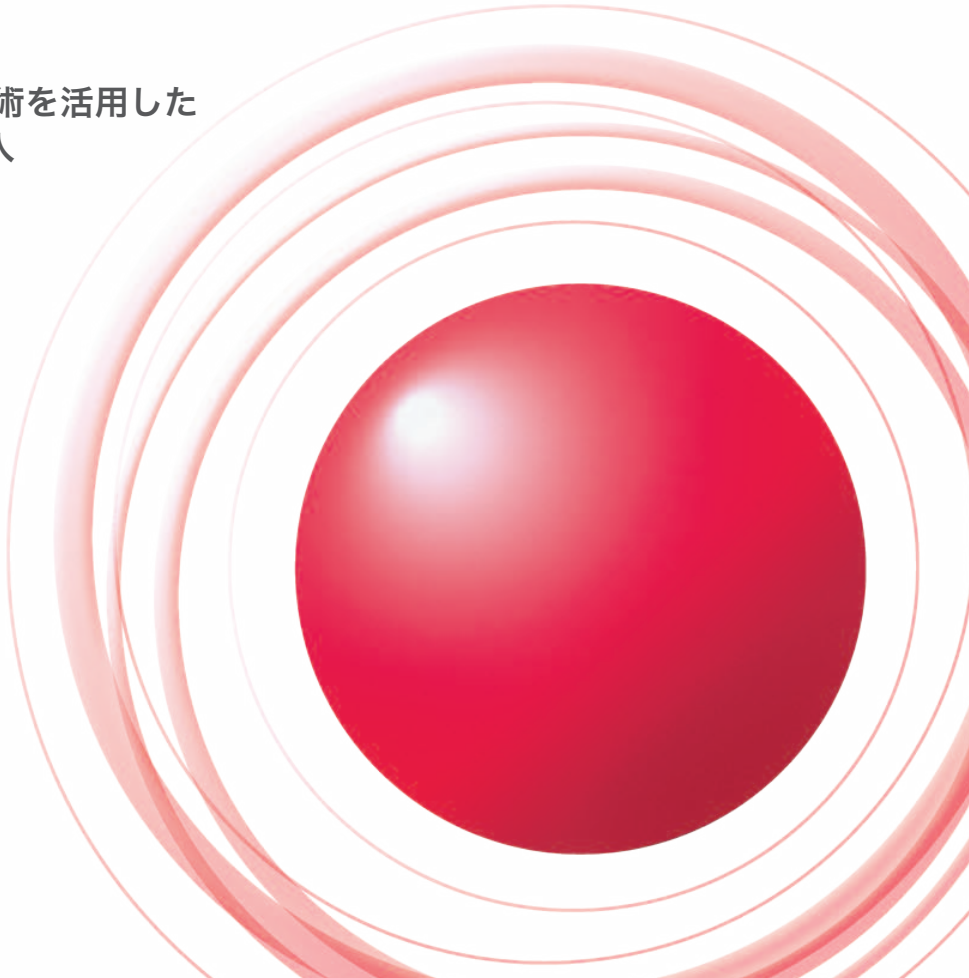
アジア地域を迷惑メール送信元にし続けないために、今すべきことは何か

クラウドコンピューティングテクノロジー

移動通信機能NEMO BSを用いたゲスト計算機のライブマイグレーション

サービスインフラストラクチャ

遠隔データセンタと、仮想化技術を活用した次世代サービス基盤NHNの導入



Internet Infrastructure Review Vol.5 November 2009

■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

平成21年8月17日に総務省から「日本のICTインフラに関する国際比較評価レポート」が発表されました。レポートによると対象24ヶ国中日本は総合評価で1位でした。各評価項目に注目すると、ブロードバンド料金、光ファイバ比率、ブロードバンド速度が第一位で、速くて安いインフラが整備されていることが解ります。

一方、社会基盤性を表すとされるインターネットホスト数は11位、ICT 投資割合が13位となっており、ネットワークは整備されているものの、サーバインフラやそれを利用したサービス面の整備や投資に遅れが見られるということが読み取れます。日本の速くて安いネットワークインフラの上に、クラウドコンピューティングのインフラ構築と事業の立ち上げが、日本のICT インフラ整備と競争力の向上の為に、まさに必要であると言えるのでしょう。

昨年から今年にかけて立ち上がり始めたクラウドコンピューティングに象徴されるように、インターネットは、ネットワーキングとコンピューティングの融合体と言うことができ、そのインフラを構成する要素は多岐に渡り、さまざまなレイヤからなる複雑なシステムとして動作しています。この複雑な系を安定して運用しながら、ICT基盤として発展させ続けるためには、さまざまな要素やレイヤーに関する挙動の監視や解析、そして、新たな利用の実現に向けた継続的な技術開発が必要不可欠です。

本レポートでは、IIJがインターネットというインフラを整備し発展させる為に行なっているさまざまな監視・解析、ならびに、新たな技術開発に関する情報をご提供しています。

安心・安全面では、2009年7月から9月末までの3ヶ月間を対象として、「インフラストラクチャセキュリティ」では、セキュリティインシデントの統計とその解析結果や、フォーカスリサーチとして、米国および韓国の複数のWebサイトに対するDDoS攻撃や、TCPの脆弱性に関する考察、そして、SIPを用いたVoIP サービスに対する攻撃の状況分析についてご報告します。また、「メッセージングテクノロジー」では、迷惑メールの状況分析と、送信ドメイン認証技術の導入への取り組みや普及状況についてご報告します。

技術開発面では、IIJのサービス用インフラのクラウド化を目指した「NHN」に関する技術解説と、サーバ仮想化環境においてゲストコンピュータをネットワーク単位でマイグレーションさせる機能を、Mobile IP技術を応用して実現する実験と検証結果についてご報告します。

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

執筆者:
浅羽 登志也(あさば としや)
IIJ 取締役副社長。WIDEプロジェクトメンバー。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、同代表取締役社長を兼務。

米国および韓国における大規模DDoS攻撃

今回は、2009年7月～9月の期間にIIJが対応したインシデントに関する報告とともに、米国と韓国で複数のWebサーバを対象に発生した大規模なDDoS攻撃の詳細、CERT-FIで発表されたTCPの脆弱性の内容、SIPによる無言電話発生の仕組みを取り上げます。

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7月から9月までの期間では、米国および韓国の複数のWebサーバに対する大規模なDDoS攻撃が発生しました。また、脆弱性に関しては、Webブラウザ関連の脆弱性が相次いで発見され、DNSサーバ等インターネット上での利用度が高いサーバの脆弱性も報告されました。加えて、多くの実装に影響するTCPの脆弱性が発表されています。このほか、偽のセキュリティソフトウェアやDDoS攻撃を伴った恐喝事件等、直接金銭被害を与える事件が継続しています。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7月から9月までの期間にIIJが扱ったインシデントと、その対応を示します。この期間に扱ったインシデントの分布を図-1に示します*1。

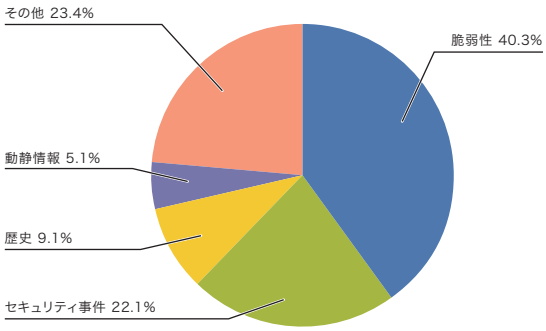


図-1　カテゴリ別比率（2009年7月～9月）

＊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、対策等の作業が該当する。
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：イベント等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の脆弱性[*2]、SMB2.0の脆弱性[*3]、Visual StudioのActive Template Libraryの脆弱性[*4]等、ユーザが利用するアプリケーションに関する脆弱性への対策が発表されました。また、ActiveXのkillbitに関する脆弱性[*5]、Jscriptに関する脆弱性[*6]、Adobe Flash PlayerやAdobe Acrobat Readerの脆弱性[*7]、Apple QuickTimeに関する脆弱性[*8]等、Webブラウザに関係する脆弱性にも多数対策が実施されています。

これらに加えて、BIND9[*9]、Squid[*10]等、サーバとしてよく利用されるソフトウェアにも、安定動作に影響するような脆弱性が発見されています。また、Cisco社製ルータのBGPに関する脆弱性[*11]や、IOSの定例アップデートがあり、複数の脆弱性[*12]が修正されています。さらに、TCPにかかわる脆弱性が公開され、多くの実装に影響するとされています。TCPの脆弱性に関する詳細は、「1.4.2 TCPの脆弱性(Sockstress)」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、第45回衆議院議員総選挙や消費者庁の発足等、日本国内の動きに注目しましたが、関連する攻撃は検出されませんでした。

■ 歴史

この期間には、日本における終戦記念日や太平洋戦争終結日等が含まれます。この時期には、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等が発生しており、各種の動静情報に注意を払いました。しかしながら、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、7月初旬に米国および韓国の複数のWebサーバに対する大規模なDDoS攻撃が発生しました。この件に関する詳細は、「1.4.1 米国および韓国におけるDDoS攻撃」を参照してください。また、クラウド環境からP2P

＊2　マイクロソフト セキュリティ情報 MS09-034 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(972260)（http://www.microsoft.com/japan/technet/security/bulletin/ms09-034.mspx)。
＊3　マイクロソフト セキュリティ情報 MS09-050 - 緊急 SMBv2 の脆弱性により、リモートでコードが実行される(975517)（http://www.microsoft.com/japan/technet/security/Bulletin/MS09-050.mspx)。
＊4　マイクロソフト セキュリティ情報 MS09-035 - 警告 Visual Studio の Active Template Library の脆弱性により、リモートでコードが実行される(969706)（http://www.microsoft.com/japan/technet/security/bulletin/ms09-035.mspx)。および、Adobe Flash Playerに関するセキュリティ情報APSA09-04（http://www.adobe.com/jp/support/security/advisories/apsa09-04.html)等。
＊5　マイクロソフト セキュリティ情報 MS09-032 - 緊急ActiveX の Kill Bit の累積的なセキュリティ更新プログラム(973346)（http://www.microsoft.com/japan/technet/security/bulletin/MS09-032.mspx)。
＊6　マイクロソフト セキュリティ情報 MS09-045 - 緊急JScript スクリプト エンジンの脆弱性により、リモートでコードが実行される(971961)（http://www.microsoft.com/japan/technet/security/bulletin/ms09-045.mspx)。
＊7　Adobe Reader、AcrobatおよびFlash Playerに関するセキュリティ情報 APSA09-03（http://www.adobe.com/jp/support/security/advisories/apsa09-03.html)。Adobe Flash Player、Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB09-10（http://www.adobe.com/jp/support/security/bulletins/apsb09-10.html)。
＊8　QuickTime 7.6.4 のセキュリティコンテンツについて(http://support.apple.com/kb/HT3859?viewlocale=ja_JP)。
＊9　BIND Dynamic Update DoS (https://www.isc.org/node/474)。この脆弱性はプライマリサーバとしてゾーン情報を持つBINDサーバが対象となる。キャッシュ機能のみを提供するサーバでもlocalhostなどのゾーン情報を持つことが多いので注意が必要。
＊10　Squid Proxy Cache Security Update Advisory SQUID-2009:2（http://www.squid-cache.org/Advisories/SQUID-2009_2.txt)。
＊11　Cisco Security Advisory: Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities (http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml)
＊12　Cisco Security Advisory: Summary of Cisco IOS Software Bundled Advisories, September 23, 2009（http://www.cisco.com/warp/public/707/cisco-sa-20090923-bundle.shtml)。

ファイル共有ネットワークへの攻撃*13、Twitterに対するDDoS攻撃*14等が発生しました。さらに、8月にはDDoS攻撃を行った上で対策費用と称して金銭を要求する事件*15の発生も確認しています。

■ 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、台湾における台風の影響によって複数の国際海底ケーブルが損傷し、通信に影響を与えたことが注目されました*16。また、複数のアンチウイルスソフトウェアで2010年度版がリリースされ、それらにそっくりな偽のソフトウェアが登場して話題になりました*17。同様に、マイクロソフト社の無償アンチウイルスツールMicrosoft Security Essentials*18のリリースに伴い、検索エンジンの検索結果から詐欺的ソフトウェア(スケアウェア)に誘導される事件も起こっています*19。

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7月から9月までの期間にIIJ DDoS対策サービスで扱ったDDoS攻撃の状況を示します。

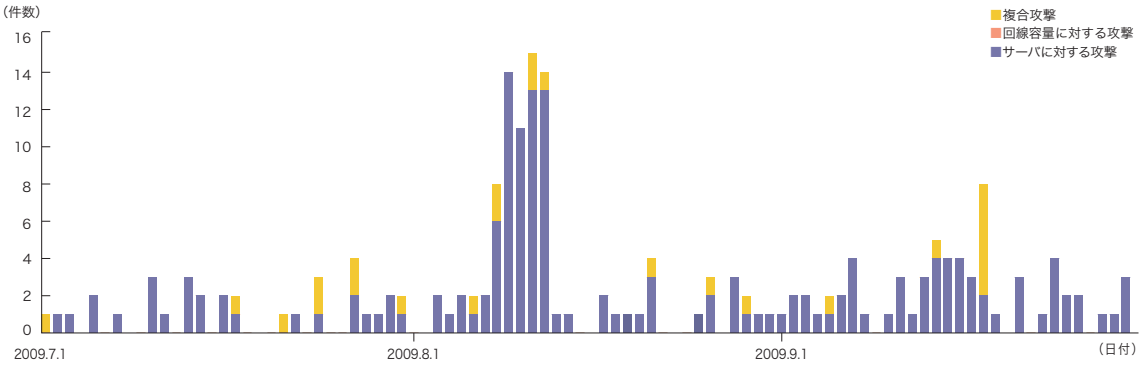


図-2　DDoS攻撃の発生件数

＊13 cNotes による「Amazon Web Serviceを利用したShareネットワークへの攻撃」(http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=Amazon+Web+Service%A4%F2%CD%F8%CD%D1%A4%B7%A4%BFShare%A5%CD%A5%C3%A5%C8%A5%EF%A1%BC%A5%AF%A4%D8%A4%CE%B9%B6%B7%E2)。

＊14 次は攻撃の様子を示すtwitterによるツイート(http://status.twitter.com/post/157191978/ongoing-denial-of-service-attack)。通信量の減少については次のArbor Networks社のblogに詳しい「Where Did All the Tweets Go?」(http://asert.arbornetworks.com/2009/08/where-did-all-the-tweets-go/)。

＊15 同様の事件については、例えばトレンドマイクロ社による次の記事を参照のこと「日本国内にも広がるボットネットによる恐喝事件(DDoS攻撃)」(http://blog.trendmicro.co.jp/archives/1385)。

＊16 本件については、例えば次の報道がある。NetworkWorld社による "Asian undersea cable disruption slows Internet access" (http://www.networkworld.com/news/2009/081209-asian-undersea-cable-disruption-slows.html)。

＊17 Symantec社の製品にそっくりな偽ソフトウェアに関するblog Symantec Security Blogs:Nort “what” AV? (http://www.symantec.com/connect/blogs/nort-what-av)。

＊18 Microsoft Security Essentials(http://www.microsoft.com/security_essentials/)。

＊19 IIJでは、検索エンジンを英語環境で利用したときに偽のソフトウェアに誘導するリンクが上位に現われることを確認している。

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[*20]、サーバに対する攻撃[*21]、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か月間でIIJは、192件のDDoS攻撃に対処しました。1日あたりの対処件数は2.08件程度で、平均発生件数は前回のレポート期間よりも増加しています。ただし、8月9日から8月12日までの複数の攻撃は特定のサイトに対して断続的に発生したものであり、全体の動向は前回のレポート期間での発生状況と大きく変わりません。

DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0%、サーバに対する攻撃が87%、複合攻撃が13%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、複合攻撃に分類した、14万ppsのパケットによって566Mbpsの帯域を埋める攻撃でした。また、攻撃の継続時間は、全体の80%が攻撃開始から30分未満で終了し、19%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1件で、94時間30分(約4日間)にわたって継続していました。

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[*22]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[*23]の利用によるものと考えられます。

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[*24]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[*25]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、攻撃先を探索するための探索の試みであると考えられます。

＊20 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。

＊21 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。

＊22 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。

＊23 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。

＊24 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。

＊25 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。

■ 無作為通信の状況

2009年7月から9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ポートに対するもので、クライアントへの探索行為でした。また、今回の期間においても、前回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、53248/TCPや20689/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。また、マイクロソフト社の脆弱性を狙った445/TCPへの攻撃は、昨年10月以来継続して観測されています。発信元の国別分類を見ると、日本国内の26.6%、中国の24.4%が比較的大きな割合を占めています。

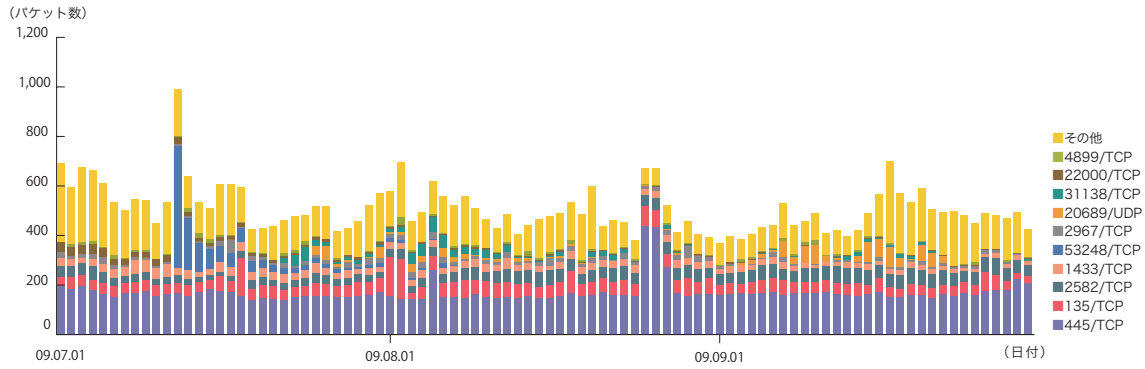


図-3　ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

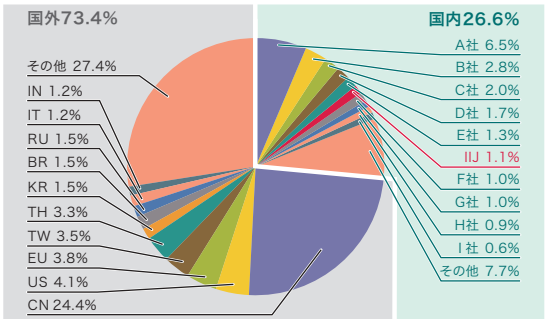


図-4　発信元の分布(全期間)

■ 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[*26]の総数を総取得検体数、検体の種類をハッシュ値[*27]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592、ユニーク検体数が46です。前回の集計期間での平均値が総取得検体数で708、ユニーク検体数で60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減少傾向にありました。

検体取得元の分布では、日本国外が35.6%、国内が64.4%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1.5%です。前回の観測期間では、IIJのユーザ同士の感染が16.8%でしたので、急激に減少しています。マルウェアの種類に注目した分析によると、これは、6月まで活発であったVirut[*28]とその亜種を感染させるための活動や、Sdbot[*29]とその亜種の活動が、IIJの網内で急激に見られなくなったことに起因しています。

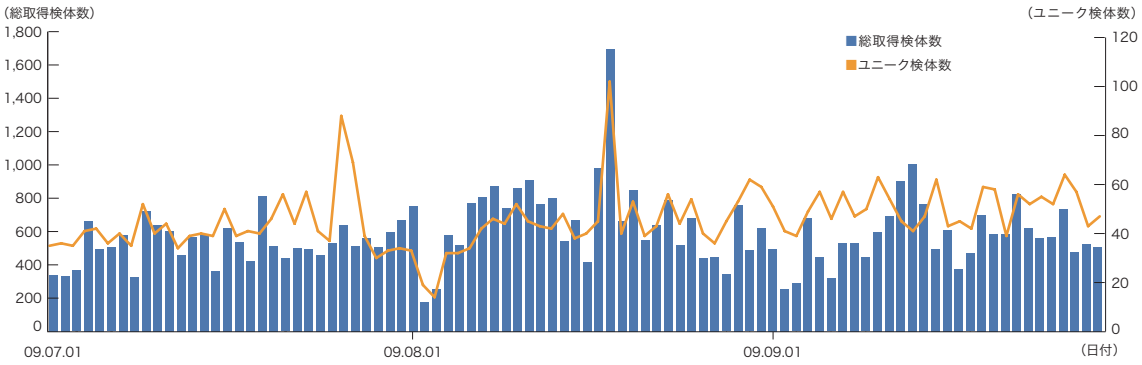


図-5　取得検体数の推移(総数、ユニーク検体数)

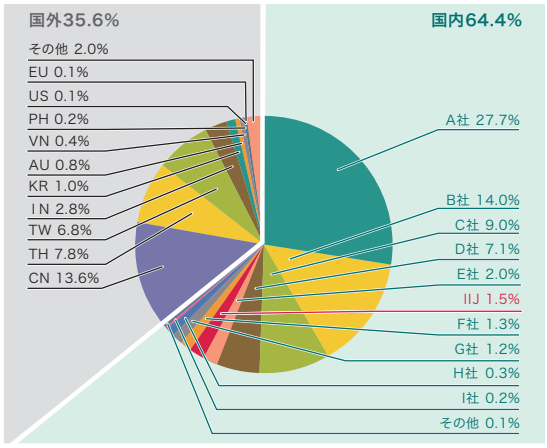


図-6　検体取得元の分布(全期間)

＊26 ここでは、ハニーポット等で取得したマルウェアを指す。

＊27 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。

＊28 Virutはファイル感染型のウイルスで、一般にはネットワークを介した感染は行わないが、脆弱性を利用した攻撃の結果としてこのウイルスを送り込む試みが流行していた。次はトレンドマイクロ社によるVirutの説明(http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=PE_VIRUT.GEN)。次はIPA (独立行政法人 情報処理推進機構)による、Webコンテンツ経由でのVirut感染に対する注意喚起(http://www.ipa.go.jp/security/txt/2009/03outline.html)。サイバークリーンセンターにおいても同様のマルウェアを感染させる試みを検出しており、他のマルウェアの感染活動とも関連するとしている(https://www.ccc.go.jp/report/200907/0907monthly.html)。

＊29 Sdbotはボットの一種で、C&Cサーバと IRCで通信を行う。次はトレンドマイクロ社によるSdbotの説明(http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_SDBOT.GEN)。

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4.5%、ボット型89.6%、ダウンローダ型5.9%となりました。また、この解析により、44個のボットネットC&Cサーバ*30と548個のマルウェア配布サイトの存在を確認しています。

1.3.3 SQLインジェクション攻撃

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃*31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7月から9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67.3%、中国11.6%、米国4.9%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、前回の観測結果に比べて減少が見られました。このため、SQLインジェクション攻撃の総数は減少しましたが、国外を発信元とする攻撃の減少が顕著であったため、日本国内を発信元とする攻撃の割合が大きくなっています。

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、攻撃の試みが継続しているため、引き続き注意が必要な状況です。

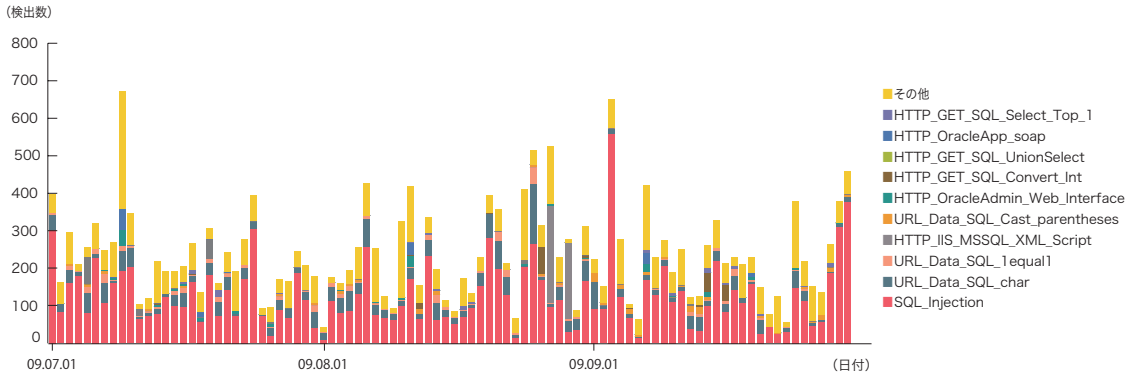


図-7　SQLインジェクション攻撃の推移(日別、攻撃種類別)

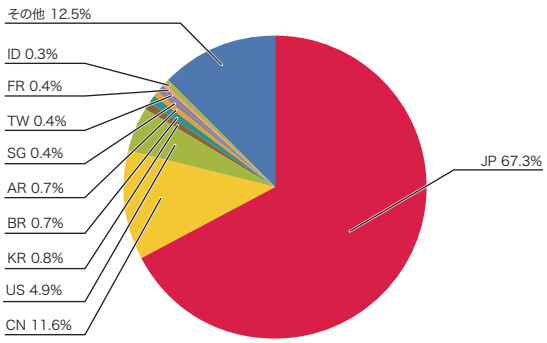


図-8　SQLインジェクション攻撃の発信元の分布

＊30 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。
＊31 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。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い対策につなげています。ここでは、2009年7月から9月までに実施した調査のうち、米国および韓国におけるDDoS攻撃、TCPの脆弱性(Sockstress)、無作為に到着するSIPパケットについて、その詳細を示します。

1.4.1 米国および韓国におけるDDoS攻撃

2009年7月初旬、米国および韓国の複数のWebサイトに対して、同時多発のDDoS攻撃が発生しました*32。ここではIIJが入手した情報を元に、その攻撃の状況を示します。

■ DDoS攻撃の経緯

今回のDDoS攻撃では、昨今DDoS攻撃に広く利用されているボットネットは利用されず、今回の攻撃専用のマルウェアが利用されました。この攻撃専用のマルウェアは、韓国国内でファイル共有を行うWebサイトに置かれたファイルを介して感染したとされています*33。このため、攻撃元のIPアドレスの多くは、韓国国内のものであったとされています*34。また、韓国国外の同様のWebサービスにも同種のマルウェア感染用ファイルが置かれ、韓国以外の国にも感染被害がありました*35。この感染活動がどの程度の期間にわたって行われていたかは不明ですが、アンチウイルスベンダによる発見や対処を避けるために、DDoS攻撃の発生直前に一気に感染活動が行われたものと見られています*36。また、このマルウェアに感染したPCの総数は不明ですが、後日の韓国側からの発表では、韓国国内において約7万8千台の規模の感染があったとしています*37。

DDoS攻撃はまず、韓国時間の7月5日*38および7月6日に、政府官公庁関係を主とした米国の複数のWebサーバに対して発生しました。この後7月7日以降、攻撃は韓国国内の複数のサイトに推移しました。韓国に対する攻撃では、政府官公庁関係に加えて、オンラインバンクやWebメール等、生活に密着したサイトも対象となりました。攻撃の通信面では、マルウェアに感染し攻撃に利用された個々のPCからの通信の量は多くなく、大量の通信によって回線を埋める攻撃よりもサーバに直接負荷を与えるような攻撃が主であったと伝えられています*39。

今回のDDoS攻撃は、7月10日を境に下火となり終息しています*40。これは、約7万8千台の感染PCの95%を4日間で駆除することに成功するなど、韓国国内におけるISPやセキュリティ関係組織や、メディア等の努力によるところが大きいと考えられます*41。このような対策活動の結果、7月10日を経た時点でDDoS攻撃は収束し、マルウェア感染の副作用として発生するHDD破壊も数百台程度であったと伝えられています。

＊32 本DDoS攻撃にて米国のサイトのいくつかがアクセスできなくなっていることをエフセキュア株式会社がブログで報じている(http://blog.f-secure.jp/archives/50255293.html)。また、韓国国内へのDDoS攻撃によっていくつかのサイトがアクセスできなくなっていることは、韓国国内の報道機関によって伝えられていた。

＊33 Web上でのファイル共有サービス(いわゆるアップローダー)は、韓国国内においては、企業や教育機関等で広く日常的に利用されており、マルウェアを感染させるファイルが共有ファイルとして置かれたため、多くの利用者が感染したと伝えられている。

＊34 次の報告では、攻撃に加担したPCは10万台以上で、そのうち韓国からの攻撃は全体の90～95%であったとしている(http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20090710)。

＊35 次は日本国内からの攻撃があったことを示すJPCERT/CCによる注意喚起「韓国、米国で発生している DDoS 攻撃に関する注意喚起」(http://www.jpcert.or.jp/at/2009/at090012.txt)。

＊36 一つの状況証拠として、IIJで入手した検体を調査した結果では、ファイルの作成日は2004年に偽装されているものの、PEヘッダ内のタイムスタンプは例えばperfvwr.dllが2009年7月4日0:38等、いずれのヘッダも攻撃が開始される直前の日付が記録されていた。

＊37 韓国国内の感染台数に関する情報はKRNIC of KISA (Korean Internet & Security Agency)によるAPNIC28での発表に詳しい(http://meetings.apnic.net/__data/assets/pdf_file/0019/14077/lee-ddos-attack.pdf)。

＊38 韓国と日本の間に時差はない。最初の攻撃は韓国時間で7月5日午前2時に開始されたが、米国時間(EDT)では7月4日(独立記念日)の午後13時にあたる。

＊39 例えば、次のKrCERTによる注意喚起にはこのマルウェアによるDDoS攻撃の通信の状況が示されている(http://www.krcert.or.kr/noticeView.do?num=340)。(韓国語の情報)

＊40 トラフィックが正常に戻ったことを受け、7月12日には韓国NCSC(National Cyber Security Center)は警報を"注意"から"関心"に推移させた。

＊41 APNIC28におけるKrNICの発表内容による(http://meetings.apnic.net/28/program/apops/transcript#ji-young-lee)。その他の活動としては、例えば、韓国国内に対するDDoS攻撃が発生した後、攻撃に利用されたマルウェアの情報や、その駆除ツールが複数のアンチウイルスベンダから早期に提供されていた。また、テレビのニュース番組や、多くのユーザが利用するWebサービスのTOPページでの告知等で、この問題に関する注意と対策の情報を広めようとする努力がなされた。さらに、マルウェアの少なくとも1つの亜種によって7月10日にHDDが破壊されるということが判明し、PCの時計を戻す等の一時的な対策手法に関する情報も伝えられていた。

■ 攻撃に利用されたマルウェア

IIJでは、今回の攻撃の発生時から、一般のマルウェア関係の情報源や、関係組織を介して、最初にDDoS攻撃用マルウェア感染を誘導するマルウェア、実際にDDoS攻撃の機能を持つマルウェア、攻撃先を更新するマルウェア等、複数の検体を入手しました。

これら複数の検体を解析し、実証実験を行ったところ、今回の攻撃に利用されたマルウェアは図-9に示すような動作を行うことが分かりました*42。

まず、発端となるマルウェア(msiexec*.exe等)は、2種類のマルウェア(perfvwr.dll (もしくはwmiconf.dll)と、wmcfg.exe)をドロップ(生成)します(1)。マルウェアperfvwr.dll (もしくはwmiconf.dll)はまず、攻撃に先立って感染したPCのパーソナルファイアウォールを停止します。また、3か所のサーバに接続し、攻撃のための設定ファイル(uregvs.nls)を生成します(2)。マルウェアのうちperfvwr.dllとwmiconf.dllは、設定ファイルに従ってDDoS攻撃を行います(3)。設定ファイルには、DDoS攻撃の期間、対象とするサーバ、攻撃の種類、回数が記述されています。このマルウェアによる攻撃は、この設定ファイルに従って図-9の(4)のように行われます。IIJにおける実証実験の結果、1台あたりの攻撃の通信量は、TCP syn floodで110pps、TCP ACK floodが110pps、UDP FloodおよびICMP floodで216Kbps程度、HTTP GET floodもしくはHTTP POST floodで107cps(command per sec)となりしました。また、プログラム上の一時停止命令によって、これらの通信が断続的に増減しながら発生する様子が観測されています。

一方でwmcfg.exeは、さらにmstimer.dllとwversion.exeをドロップします(5)。mstimer.dllは、複数のWebサーバからflash.gifという名前のファイルをダウンロード(6)し、そのファイル内からwversion.exeを抽出してアップデート(7)すると同時に、複数の宛先に迷惑メールを送信します(8)。一方でwversion.exeは、mstimer.dllと自分自身を削除する等、痕跡を消去する活動を行います(9)。ただし、アップデートされた後は、ハードディスク内部の特定の拡張子を持つファイルを検索して破壊したり(10)、ハードディスクのMBR*44周辺に特定の文字列を書き込み、PCを起動不能にする機能が追加されます(11)。

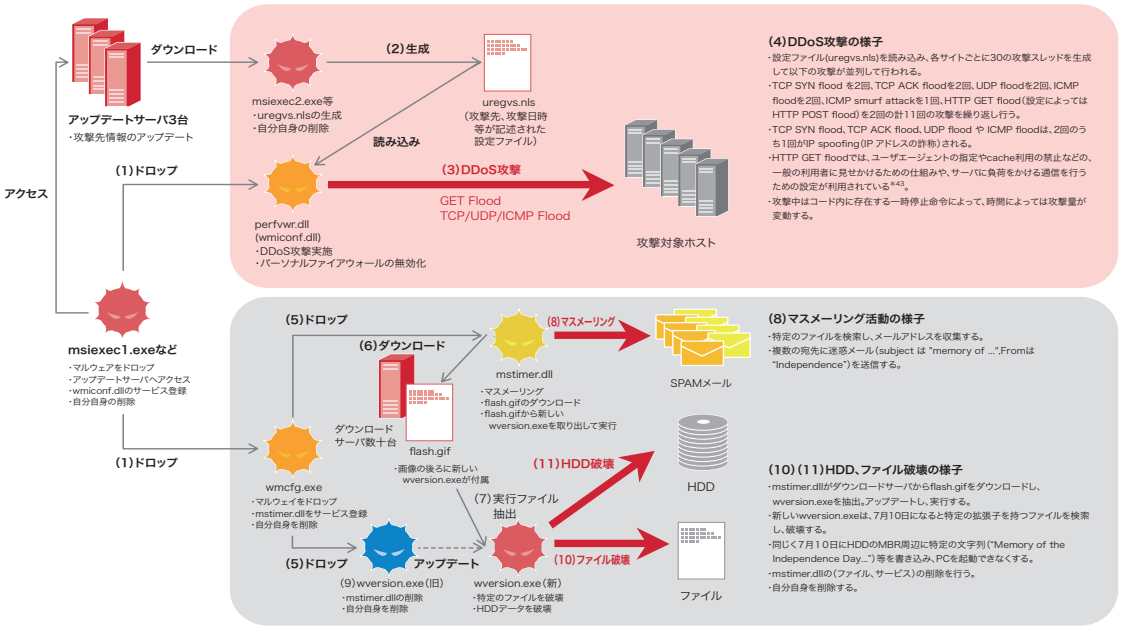


図-9　DDoS攻撃に利用されたマルウェアの動作

＊42 この動作の様子は、極力直接得た情報をもとに取りまとめているが、DDoS攻撃発生当時のインターネット上の各種サーバ等の役割や状況については、IIJで直接確認していない情報も含んでいる。

＊43 User-AgentヘッダにはfirefoxやIE7.0、IE8.0に見せかける文字列が存在し、様々なパターンがある。Accept-Languageヘッダにはko (韓国語)が指定される。またCache-Controlヘッダにはno-store, must-revalidateが指定されるが、すべてのリクエストに必ず付加されるわけではない。

＊44 MBR:Master Boot Recordの略。ハードディスクの先頭にある領域で、通常はこの領域にOSの起動用のプログラムが格納される。

■ 攻撃の全体像

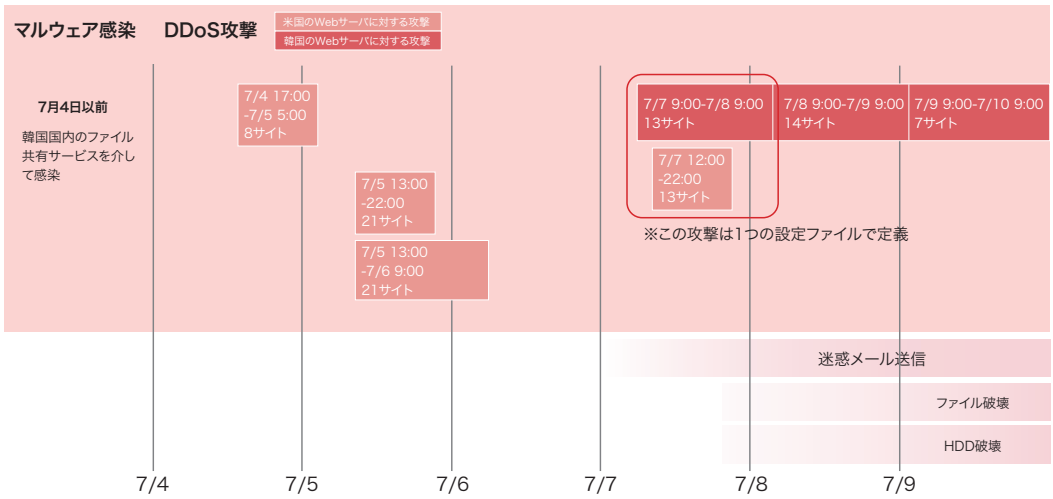
今回発生した事件における、攻撃対象の推移や関連する事象を時系列順でまとめ、図-10に示します。

通常、DDoS攻撃は、特定のサイトに対する嫌がらせ等、明確な狙いを持って行われることが多く、インターネット上で発生するインシデントの中では、比較的その意図がわかりやすいものの１つです。しかし、今回のDDoS攻撃は、主に韓国国内で攻撃用マルウェアが広まったこと、攻撃先が米国から韓国に推移した*45こと、介在したマルウェアが2つの独立したマルウェアに分かれること等、複雑で意図が読み取りにくい攻撃となっています。

■ 今回のようなDDoS攻撃への対策

ここでは今回のDDoS攻撃の被害を受けたときの対策について、通常のDDoS攻撃への対策との差異に注目して検討します。今回の攻撃は、多くのマルウェア感染PCの一斉動作によるもので、攻撃の通信を発生させているPCのIPアドレスについて個別にアクセス制御や帯域制御を行うことは困難です。しかし、攻撃の通信の多くは、一つの国の国内から発生しており、ネットワーク単位でアクセス制御や帯域制御を行うことは、一時的な対策として有効であったと考えられます。また、今回は個々のマルウェア感染PCからの攻撃の通信量が小さく、特に攻撃にかかわるWebのリクエストはマルウェアにより利用者の挙動を真似るように偽装されているため、正常な通信と攻撃による通信の判別が比較的難しくなっていることが特徴でした。DDoS 対策装置等を利用できる場合でも、異常検知のしきい値や動作モードの設定等に工夫が必要になる状況が考えられます。

最後に、IIJとしては、今回の事件のような仕組みで日本国内からDDoS攻撃が発生した状況を想定し、対処方法を検討しておく必要があると考えています。攻撃に利用されたマルウェアは事前に配布される設定にしたがって攻撃を実施することから、一元的に管理されるボットネット等への対策とは異なり、攻撃が開始された後はマルウェアに感染したPCから個々にマルウェアを駆除するより他に攻撃を止める方法はありません。韓国で実際に行われたように、多くのPCから早期にマルウェアを駆除するためには、多くの組織による連携した活動が必要です。このためには、関係組織での間で日常から有事に備え、いざというときの対策において相乗効果を発揮できることが重要となります*46。



攻撃対象の数は報道等の情報にIIJで確認した攻撃先を加えたもの

図-10 米国および韓国に対するDDoS攻撃: 時系列で整理(UTC)

＊45 取得した検体から、米国13サイトへの攻撃(2009年7月7日18:00から7月8日18:00)と韓国13サイトへの攻撃(2009年7月7日 21:00から7月8日7:00)が同一設定ファイル内で行われ、これを境に攻撃全体が韓国国内への攻撃に推移したことが分かっている。

＊46 日本では、総務省による「電気通信事業分野におけるサイバー攻撃対応演習」(http://www.soumu.go.jp/menu_news/s-news/2006/061201_4.html)や日本データ通信協会Telecom-ISAC Japan (https://www.telecom-isac.jp/)等で、サイバー攻撃に対する演習が行われており、また国際的にはAPCERTによる演習(http://www.apcert.org/documents/pdf/APCERT-drill-2008.pdf)等がある。IIJはこのような場に積極的に参加している。

1.4.2 TCPの脆弱性(Sockstress)

2009年9月、フィンランドのCSIRT組織であるCERT-FIにより、TCPに関する脆弱性への対応状況が発表され、報道等でも大きく取り上げられました*47。ここでは、このTCPの脆弱性とその対応について説明します。

■ 経緯

今回発表された脆弱性そのものは、発表の1年以上前である2008年9月に、スウェーデンに本拠地を置くセキュリティベンダOutpost24社の2名の研究者によって、その存在が指摘されたものです。この研究者たちは、ネットワーク上の監査を高速化するツールUnicornscan*48を開発し、その利用中にTCPの不審な挙動に気づき、その動作を狙って通信を行うツールSockstress*49を作成しました(このツール自体は非公開になっています)。

この脆弱性の存在を示す情報を受け、CERT-FIを中心に製品開発者間に対策を促進するためのコミュニティが組織されました。日本では、情報セキュリティ早期警戒パートナーシップ*50で取り扱われています。

■ 脆弱性として指摘された問題

脆弱性を攻撃するためのツールSockstress自体は非公開であり、今回指摘された脆弱性の全容は公開されていません。ここでは、もっとも大きく取り上げられたゼロウィンドウサイズの問題について解説します。

ゼロウィンドウサイズの指定による攻撃は、次の順序で発生します。

1. クライアントからサーバに対してTCP接続を確立する。
2. 通信の途上にクライアント側で受信ウィンドウサイズ0の指定を行い、「受信バッファに空きがなく、これ以上はデータを受け取れない」と宣言する。この状態で、サーバ側は当該TCP接続によるデータ転送を一時停止する。サーバ側は、クライアント側に現在の受信ウィンドウサイズをある間隔で問い合わせ、応答がある限り接続を保持し続ける。
3. クライアント側からサーバに対して上記の1と2を多量に繰り返す。
4. サーバ側の資源が埋め尽くされ新しいTCP接続を受け入れられない状態になる。

実際には、サーバ側の実装や資源の量等によって、攻撃が成立するまでの時間は変化します。また、高負荷にはなるものの、攻撃が成立しないことも考えられます。

ゼロウィンドウサイズの状態で接続が保持されること自体は、TCPの規格RFC793*51やRFC1122*52に記載されている正常な動作です。TCPによる通信を利用する通常のクライアントでも、正常な通信制御としてゼロウィンドウサイズの指定を行うことがあります。今回の指摘では、ゼロウインドウサイズの指定が、システム資

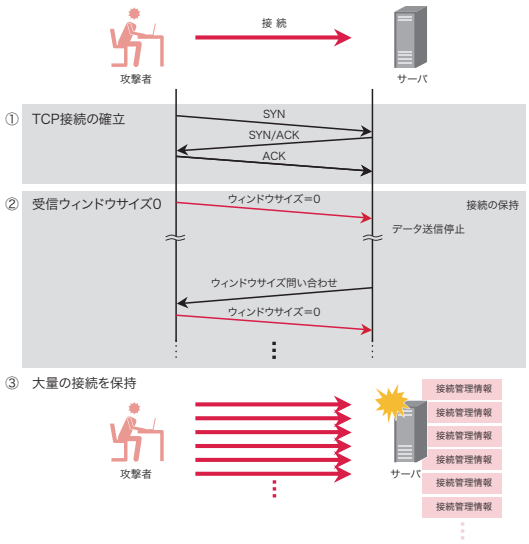


図-11 ゼロウィンドウサイズの指定によるサーバ側のスタック

*47 TCPに関する脆弱性への対応状況(https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html)、(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4609)、(http://www.microsoft.com/japan/technet/security/bulletin/ms09-048.mspx)など。
*48 Unicornscan(http://www.unicornscan.org/)。
*49 Sockstress自体は非公開とされているが、関連情報は次にまとまっている(http://sockstress.com/)。
*50 情報セキュリティ早期警戒パートナーシップは経済産業省告示に基づく製品開発者への脆弱性情報流通の仕組み。このパートナーシップでは、IPA(http://www.ipa.go.jp/security/vuln/report/)が脆弱性情報の受付機関として、JPCERTコーディネーションセンター(http://www.jpcert.or.jp/vh/)が製品開発者との調整機関として活動している。 取り扱われた脆弱性に関する情報はJVNにて公開される(http://jvn.jp/)。IIJはルータ等の自社製品の製品開発者としてこのパートナーシップに参加している。
*51 RFC793 Transmission Control Protocol(http://www.ietf.org/rfc/rfc793.txt)。
*52 RFC1122 Requirements for Internet Hosts - Communication Layers(http://www.ietf.org/rfc/rfc1122.txt)。

源を超える量のTCP接続を保持させるための手法として、攻撃に悪用可能であることが示されました。ただし、このゼロウィンドウサイズによる攻撃は、新しい手法ではなく、例えばIETF*53のTCPMワーキンググループ*54でSockstress登場前の2006年7月頃から話題に上っています*55。

■ プロトコルの問題か実装の問題か

すでに示したようにゼロウィンドウサイズの指定は、プロトコル規格上は正常な状態ですが、これを大量に引き起こすことが問題視されています。この問題を解決するために、TCPプロトコルそのものに変更を加えるか、タイムアウト値の設定や調整等実装上の回避策を行うかという議論がありました。

先に述べた過去のIETF TCPMワーキンググループでの議論では、この種の攻撃はOSやサーバ実装の資源管理上の問題であり、プロトコル規格ではなく実装時に個別の事情に応じた解決をすべきというのが大方のコンセンサスでした。こうした状況もあり、今回の件は実装上の対応を行う方向で対処されました。

■ 対策の有効性

今回のゼロウィンドウサイズの問題に関して、マイクロソフト社の対策を例にとり、対策を施す前の実装と、対策後の実装で実証実験を行いました。この実験の結果を図-12に示します*56。

この実験結果が示すように、対策後の実装では、対策前の実装よりも今回の攻撃に対する耐性が強化されています。ただし、この対策では、新しいTCP接続を受け入れるために、既存のTCP接続を強制的に終了することで資源を解放しており、重要な接続を切断してしまう可能性を否定できません。また、この攻撃を完全に防ぎきるものではありません。マイクロソフト社に限らず、「対策済み」としている多くの実装においても同じように有限の資源の利用法を調整することで対策としている状況にあります。

ここまで紹介したように、今回の問題は実装の脆弱性として取り扱われましたが、TCPの規格から見て攻撃の接続と正常な接続を区別できない以上、本質的には、大量の接続を受けるシステムの資源管理の問題であると言え

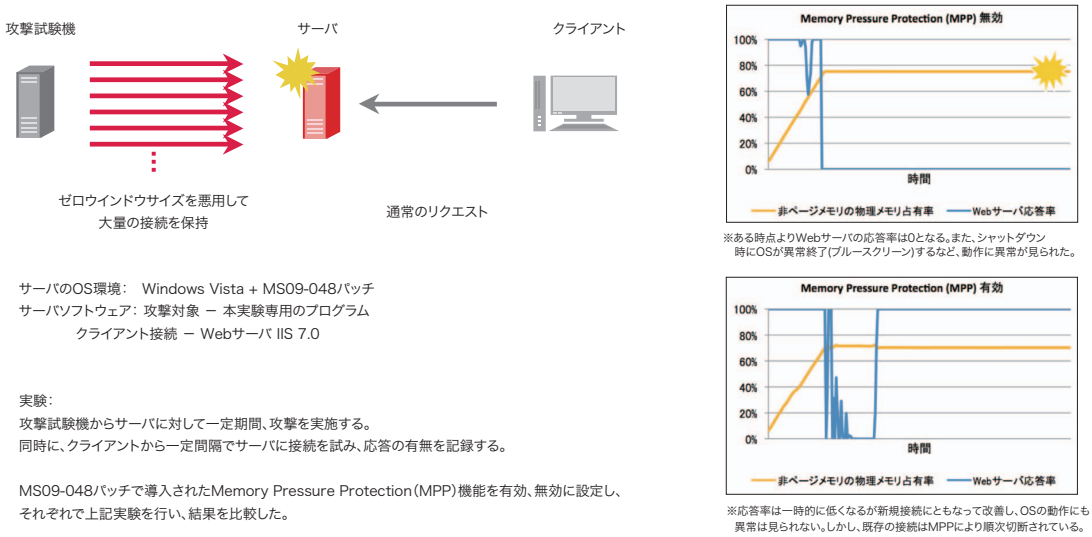


図-12 実証実験とその結果

＊53 IETF Internet Engineering Task Force の略。インターネット技術の標準化を推進する組織（http://www.ietf.org/）。
＊54 TCPMワーキンググループ TCP Maintenance and Minor Extensions Working Group（http://www.ietf.org/dyn/wg/charter/tcpm-charter.html）。
＊55 TCPM WGメーリングリストでの（http://www.ietf.org/mail-archive/web/tcpm/current/msg02189.html）に始まる議論や、その後提出されたInternet Draft、「Clarification of sender behaviour in persist condition」（https://datatracker.ietf.org/drafts/draft-ananth-tcpm-persist/）等。
＊56 実際にはマイクロソフト社のWebサーバ、インターネット インフォメーション サービス（IIS）には、OSの負荷状況によりWebの応答を調整する機構が備わっており、Webサービスに対して今回の攻撃を行うだけでは、OSの動作異常までは至らなかった。このため、今回の実験ではWebサービス以外のサービスに対して攻撃を行って負荷をかけている。

ます。このように、実装の修正による根本的な対策ができない問題は他にも存在し[*57]、今後も新たに発見される可能性があります。したがって、インターネット上に公開しているサーバについては、引き続きその負荷等に注意して運用していく必要があるのです。

1.4.3 無作為に到着するSIPパケット

■ 不正なSIPの通信

IIJでは、昨年よりハニーポットに到達するSIP（Session Initiation Protocol: セッション確立プロトコル）[*58]のパケットを断続的に観測しています。これらのSIPパケットは、インターネット上の不特定多数に対して送信されていて、SIPを解釈することのできる端末への接続が試みられています。一部のVoIPルータやIP電話端末では、設定によってSIPのパケットが到着しただけで着信音を鳴らす等の反応を起こすことがあります。このような理由による無言電話の事例が多く報告[*59]されています。

■ SIPによるVoIP通信の仕組み

SIPは、その名前が示すとおり、セッションの制御に使われるプロトコルの1つで、HTTPと同様にリクエストとレスポンスを基本としています。SIPは、IP電話サービス等VoIP通信で利用されています。ただし、HTTPがデータの配送まで規定しているのに対して、SIPはVoIP機器間でのセッションの開始、変更、終了の3つの制御をするだけで、音声等はRTP（Real-time Transport Protocol[*60]）等の別のプロトコルで配信されます。図-13に、IP電話でのSIPの通信例を示します。

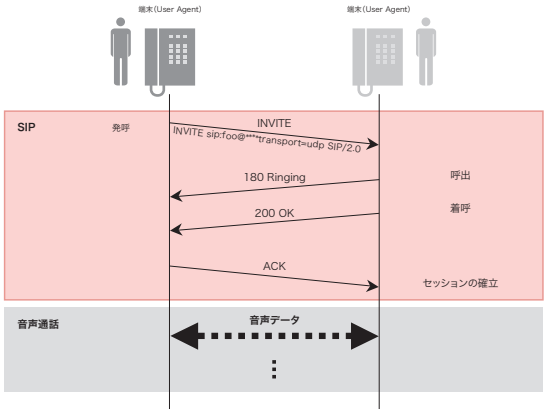


図-13 SIPによる音声通話確立の様子

① IP電話で電話をかけるときには、まず、発信元の端末（UA: User Agent）が通話先に対してINVITEメッセージを送信する。
② 着信側の端末は、INVITEメッセージを受け取ると、着信ベルを鳴らして人に知らせる。同時に、呼出中であることを意味する（180Ringing）をINVITEメッセージの発信元に返答する。
③ 通話先で人が受話器を取ると、着信側端末は200 OKを発信元に送信する。
④ これを受け取った発信元は、着信側にACK応答を返しセッションを確立する。

これは基本的な動作で、一般的には、接続する際に直接端末同士で通信せず、SIPサーバ[*61]等を利用します。

■ IP-PBXを狙った攻撃

最近では、企業等においても、導入コストや維持費等を抑えるため、従来のPBX[*62]による回線交換網の利用をやめ、IP-PBX[*63]を利用したIP電話システムを導入する事例が増えてきています。安価なIP-PBXアプライアンス製品も登場しているため、今後このような導入がますます増えると考えられています。

IP-PBXは、コスト抑制等の導入メリットが大きい半面、これまでの電話網と異なり、インターネットや閉域IP網等、他の通信が行われていたり、VoIP機器以外の機器が接続されているネットワークに接続します。この

＊57 例えば、英国CPNIによるTCPの頑健性に関する調査報告書（https://www.cpni.gov.uk/Docs/tn-03-09-security-assessment-TCP.pdf）やIPAによるTCP/IPの既知の脆弱性をまとめた調査報告書（http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html）では、こうした問題を複数示して、開発者向けにTCP/IPプロトコルスタックを実装する上での注意点を解説している。また、後者の報告書には運用者向けのガイドも記述されている。
＊58 無作為なSIPのパケットについては本レポートのVol.4においても紹介している（http://www.iij.ad.jp/development/iir/pdf/iij_vol04.pdf）。
＊59 例えばcNoteによる「INVITE Flood?不正なSIP着信」（http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=INVITE+Flood%3F++%C9%D4%C0%B5%A4%CASIP%C3%E5%BF%AE）。
＊60 Real-time Transport Protocolはデータストリームをリアルタイムに配送するためのデータ転送プロトコル。音声や動画の転送などに利用され、VoIP機器の多くはRTPをサポートしている。
＊61 SIPサーバには中継（プロキシ）・転送（リダイレクト）・登録（レジスター）等の機能があり、通常はSIPサーバを経由することで相手との通信を行う。
＊62 PBX（Private Branch eXchange）は主に企業等に導入されている構内交換機のこと。内線と外線（公衆電話回線網）とを接続し、その発着信の制御を確立する。
＊63 VoIP機能に対応したPBXのこと。例えばAsterisk（http://www.asterisk.org/）等が知られている。

ため、従来のPBXに比べると、外部や内部からの攻撃を受けやすい点を考慮する必要があります。また、現在のVoIP製品の多くがUDP上でSIPを利用しているため、IPアドレスや発信元の電話番号等を詐称したSIPパケットを容易に作成できる状況にあります。実際に、海外では脆弱性を悪用してIP-PBXを不正に操作し、IP電話サービスの契約情報を取得して悪用する試み[*64]や、番号を詐称して着信履歴を残すことで折り返し有料電話サービスに電話をかけさせて料金をだまし取ろうとした事例[*65]が発生しています。IIJで観測した無作為のSIPパケットに関しても、無言電話を引き起こすことが目的ではなく、悪用可能な脆弱性を持つIP-PBXを探査する狙いがあったと考えられます。

■ VoIPのセキュリティ対策

このような被害を受けないためには、どのような脅威があるかを正しく理解し[*66]、利用しているVoIP機器のベンダで推奨している設定や製品に関する情報を定期的に確認したり、利用しているISP等によるサービス利用上の注意事項を確認する等、常に機器を適切に運用することが大切です。また、利用できるようであれば、VoIP機器の暗号化機能を設定したり、特定のSIPサーバからのみSIPパケットを受け取るように設定する等、不特定多数からのSIPメッセージを受け取らないよう、機能や設定で適切なアクセス制御を行います。さらに、VoIPに対応したファイアウォール、IDS、IPSを導入したり、セッションボーダーコントローラ[*67]を導入することも有効です。

個人向けIP電話や企業でのIP-PBX等、VoIPは今後ますます普及すると考えられます。見ず知らずな電話番号からの着信は不用意に折り返さないなど、従来の電話での脅威に対する対応と同様に、これら新たな脅威に対しても適切な対応を行うことが必要です。

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、IIJが直接関与していないインシデントですが、米国と韓国におけるDDoS攻撃について大きく取り上げました。このように他国で発生した事件についても、情報を収集し解析を行うことで、将来日本において同様のインシデントが発生したときに迅速に対処できるように備えておくことも、我々の使命だと考えています。

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。

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米国および韓国におけるDDoS攻撃)
永尾 禎啓 須賀 祐治(1.4.2 TCPの脆弱性(Sockstress))
土屋 博英(1.4.3無作為に到着するSIPパケット)
IIJ サービス事業統括本部 セキュリティ情報統括部

協力:
大原 重樹 サービス事業統括本部システム基盤統括部システム開発課
加藤 雅彦、根岸 征史 IIJ サービス事業統括本部 セキュリティ情報統括部

＊64 例えば、米国の法執行機関(連邦捜査局等)と連携してサイバー犯罪に取り組んでいるIC3(Internet Crime Complaint Center)から注意喚起が出ている(http://www.ic3.gov/media/2008/081205-2.aspx)。
＊65 例えば エフセキュア株式会社のブログ「ワン切り詐欺にご用心」(http://blog.f-secure.jp/archives/50260210.html)。
＊66 既知の脆弱性とその脅威に関しては、例えば以下の報告書等を参照のこと。IPAによる「SIPに係る既知の脆弱性に関する調査報告書 改訂第2版」(http://www.ipa.go.jp/security/vuln/vuln_SIP.html)。
＊67 VoIPネットワークの境界等に設置され、SIPパケットの内容に応じて必要なポートの制御を行ったり、NAT環境下でも正常にVoIPの通信が行えるように制御を行う装置。

アジア地域を迷惑メール送信元にし続けないために、今すべきことは何か

今回は、2009年第27週〜第39週に検知した迷惑メールの割合の推移や送信元地域の分析とともに、迷惑メール対策のために行われている国際的な活動の状況と、送信ドメイン認証技術の普及度調査の結果を解説します。

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情報、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、さまざまな視点で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、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27週(2009年6月29日〜7月5日)から第39週(2009年9月21日〜9月27日)までの13週間、延べ91日間を対象にしています。また、前号(Vol.4)でIIR発行開始から1年が経過しましたので、これまでのデータを一部まとめて示します。

迷惑メール対策の動向としては、国際的な取り組みに関する話題を紹介します。IIJは、これまでもMAAWG(Messaging Anti-Abuse Working Group)を中心に、国際的な議論の場で活動してきました。今回は、これ以外の組織や取り組みについて、その概要を報告します。また、メールの技術動向としては、前号に続いて送信ドメイン認証技術を取り上げ、実際の普及がどの程度まで進んでいるのかを報告します。

2.2 迷惑メールの動向

ここでは、迷惑メールの動向として、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。今回の調査対象である2009年第27週から第39週を含めた、過去1年間69週分での推移を図-1に示します。

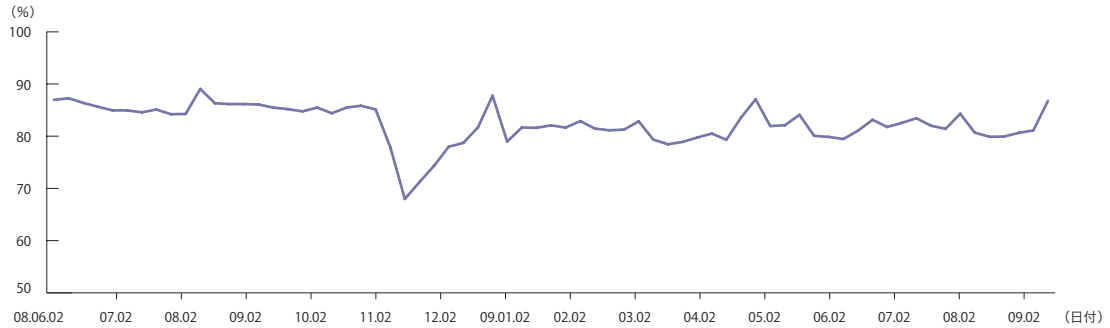


図-1 迷惑メールの割合の推移

2.2.1 迷惑メールの割合の推移

2009年第27週から第39週までの91日間で検出した迷惑メールの割合は、平均82.2%でした。前回(2009年第14～26週)の平均値が81.6%でしたので、0.6%微増したことになります。この期間もっとも検出割合が高かった週は、第39週(2009年9月21日～9月27日)で、その値は86.7%でした。第39週には、連休期間が含まれているため、通常のメール流量が減少したことによる影響が表れたものと考えます。ただし、これまでの経験上から、秋以降に迷惑メール量が増加する傾向があるため、今後も注意が必要だと考えています。

最近では、不正プログラムを添付ファイルとして送りつける迷惑メールがたびたび増加し、不正プログラムの亜種の更新頻度も高く、ウイルス検知ソフトウェアが対応できていないことがあります。このため、添付ファイルを不用意に解凍したり実行したりしない等の注意が必要です。

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、前回と同様にブラジル(BR)で、全体の12.1%を占めていました。ブラジルは、前回に引き続いて1位であり、割合も0.3%増加しているため、迷惑メール送信が多い原因やその対策などの検討が必要と考えています。これ以外の上位地域には若干の変動がありました。これまで常に最上位にあった米国(US)が7.1%と前回から4.3%減少し、4位に順位を下げています。前回報告したように、FTC (米連邦取引委員会)など消費者行政に関する執行機関の対策活動が効果を上げているのかもしれません。

中国(CN)が9.8%、韓国(KR)が7.2%と、両国とも依然として大きな割合を占め、それぞれ2位と3位になっています。5.6%で6位のベトナム(VN)と合わせて、アジア地域の迷惑メール送信割合を押し上げる要因にもなっています。また、ベトナムは、前回の14位から急速に順位を上げているため今後注意が必要です。ベトナムやブラジルに限らず、経済発展が進むにつれてネットワークなどのインフラが整備されると、迷惑メールの送信元割合が増えるのは世界的な傾向です。6.0%で5位のインド(IN)も前回とほぼ同水準であり、同様のことが言えると推測しています。

今回、日本(JP)は3.1%で9位でした。前回からは、割合も順位も上がっています。割合が増えた原因はいくつか考えられますが、そのひとつとしていわゆるエラーメールの受信が目立ちました。迷惑メールと判定した日本発のメールの中に、主要ISPのメールサーバを送信元とするものが多くありました。ただし、配送上の送信元の情報(エンベロープFrom)や送信期間等から、その大部分が宛先不明メールに対するエラーメール、つまりバウンスメールであったと判断しています。

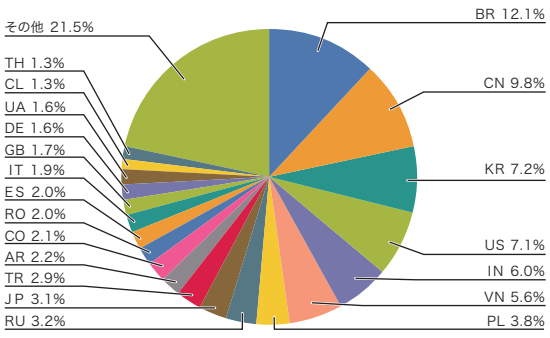


図-2　迷惑メール送信元地域

こういった事例は、IIJの顧客のドメイン名が、迷惑メールの送信元情報として悪用されたことによって発生します。一般的に、このような悪用をドメインの管理側で防ぐことは難しいです。ただし、これまでのIIRで紹介してきた送信ドメイン認証技術を送信側に導入することが、その対策手法の1つとなります。また、メール受信側でも、送信ドメイン認証を行うことで、送信者情報に示されているドメインが正しいメールの出口から送信されたものであるかどうかを判断することも必要になってきます。送信者情報として不正なドメイン名を利用しているメールに関しては、バウンスメールを返さない等の技術を導入することで、こういった事例は防ぐことができます。

図-3に上位6カ国(ブラジル、米国、中国, 韓国、ベトナム、インド)に日本を加えた 7カ国の迷惑メール送信元割合の推移を示します。

この期間の開始当初は、ベトナムは日本より迷惑メールの送信割合が低い国でしたが、その後急速に順位を上げ、8月以降は4位から5位に位置するなど迷惑メール送信元の上位国になっています。

これにより、全体としての順位も押し上げられ、今回の調査期間の全体でも 6位となりました。

このように図-3からは、それぞれの送信元からの迷惑メール量に、時期的な変動があることが読み取れます。しかし、その変動の内容についても同じような動きをしているわけではありません。

例えば韓国(KR)は、今回の調査期間中では第34週(2009年8月17日週)が送信元の割合が最も高く、10%を超えています。

この週での増加分は、同じ送信元(IP アドレス)から大量に送信している送信元が増えたことにより全体として、送信数が増えていました。

一方ブラジル(BR)は、それぞれの週で送信割合が多少変動していますが、ブラジルから送信された迷惑メールだけに着目すると、大量に送信している送信元の割合も、例えば1週間に1通だけしか送信しない少量の送信元の割合とも、あまり変動がありませんでした。

これらのことから、韓国から日本への迷惑メール送信は、大量に送信する特定の送信元の送信数が大きく影響していることがわかり、ブラジル等の地域は、大量に送信する送信元が少ないことから、不正プログラムに感染させられたボットからの送信が多いことが推測できます。

大量に送信する送信元に対しては、それぞれに対して法的措置によってある程度改善することが期待できますが、少量送信元が多数存在する場合には法的措置にも限界があります。

この様に、迷惑メール送信を抑制するには、それぞれの地域及び送信元の特性に応じた対応が必要になってきます。

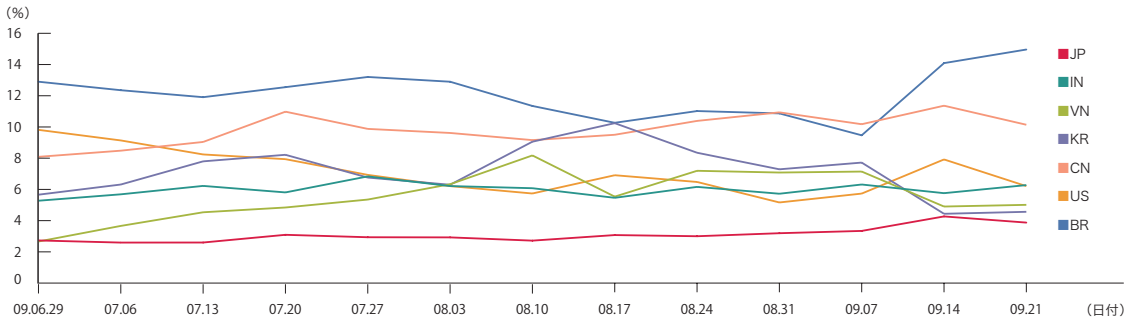


図-3　迷惑メール送信元の推移

2.2.3 国際的な迷惑メール対策活動

これまで示してきた迷惑メールの送信元の分析結果からも明らかなように、日本に向けた迷惑メールの大部分が海外から送信されたものです。特にアジア地域は、世界的にも迷惑メールの送信元地域として不名誉な結果がセキュリティベンダ等によって示されています[*1]。

アジア地域を対象とした、迷惑メール対策のための民間主体の組織に、APCAUCE (Asia Pacific Coalition Against Unsolicited Commercial Email)があります。APCAUCEは、北米を中心としたCAUCE (Coalition Against Unsolicited Commercial Email)のアジア地域版という位置づけで、筆者は2006年と2007年に会合に参加し、日本での取り組みを紹介してきました。しかし、残念ながら2007年のインドでの会合以降、2年間会合が開催されていません。このため、APを接頭語に持ついくつかのアジア地域組織の情報交換会合であるAP*Retreat[*2]会合が、APNIC 28ミーティングに合わせて北京で開催されました。ただし、このときも残念ながらAPCUACEからの参加はありませんでした。しかし、迷惑メール問題は重要なテーマであることから、AP*Retreatの共同議長らの協力により、対策の取り組み状況について日本と開催地の中国から発表が行われました。

こういったボランティアベースの組織は、モデレータの努力に大きく依存してしまう傾向にあり、会合の開催が不定期になることはある意味やむを得ないことかもしれません。しかし、アジア地域での迷惑メール対策は急務であり、日本の代表メンバである(財)インターネット協会などを中心に、まず来年の開催を目指して検討を進めています。

グローバルな民間組織には、前回(Vol.4)のインターネットトピックスで紹介したMAAWGがあります。現状は、参加者が欧米と筆者ら日本などの一部地域であり、アジア地域からの参加者があまり多くありません。MAAWGの会合は、開催地が北米や欧州であり地理的になかなか参加が難しい面もあるため、まずアジア地域での関係者による会合が必要ではないかと考えています。

行政府を中心とした組織としては、グローバルなものとしてLAP[*3]があります。LAPは、執行当局間の情報共有や連携、官民対話の促進等を目的として2004年に合意された行動計画を元に、毎年定期的に会合が開催されています。2007年には、MAAWG、CNSA(Contact Network of Spam Enforcement Authorities)との合同会合も開催されました。また、2009年10月7日から10月10日の3日間、ポルトガルのリスボンにおいて、CNSAとの5回目の合同会合も開催されています。日本からはメンバである総務省が参加し、筆者と(財)日本データ通信協会を含めて日本の取り組みを紹介しました[*4]。

LAPの会合では、各国の迷惑メールに関連する法律の紹介や執行状況、迷惑メールに対する取り組み等が報告されます。筆者も含め民間からも、ドイツのISPの団体であるecoやMAAWGから活動の紹介や今後検討していく法執行機関との協調に関する発表がありました。米国のFTCからは、前回紹介したPricewert社のネットワーク遮断の経緯についての紹介もありました。

＊1　例えばソフォス社によるスパム送信元の大陸別調査では、アジアが全体の約3分の1となっている(http://www.sophos.com/pressoffice/news/articles/2009/07/dirtydozenq209.html)
＊2　AP*Retreat会合の概要はWebサイトを参照(http://www.apstar.org/)
＊3　LAP: London Action Plan(http://www.londonactionplan.org/)
＊4　Workshop CNSA-LAP “Spam-Fighting” (http://www.anacom.pt/render.jsp?contentId=962326)

LAPには、アジアパシフィックからオーストラリアやニュージーランドなどが積極的に参加しています。また、今回、香港、台湾、マレーシアからの参加もあり、比較的アジアからの行政機関の参加は多いようです。同様に、アジアパシフィック地域の行政機関の集まりとして、ソウル-メルボルン スパム対策のための多国間MoU(Memorandum of Understanding)[*5]が2005年に合意され、関係国間で会合が開催されています。日本からは総務省が参加しており、2008年3月には東京で会合が開かれています。

行政府組織間では、こういった組織により定期的に情報交換が行われています。実際に効果を上げるためには、法執行を着実に行うこともちろん大切ですが、ボットネットなど高度化する迷惑メール送信手法に対抗するために、直接的な技術対策も重要です。迷惑メール対策を効果的に行うためには、民間と行政府が連携し、技術面と法執行面の両面が協調し対策を進めて行くことが必要になります。また、日本からの迷惑メール送信がOP25B (Outbound Port 25 Blocking)等の技術的な対策により難しくなり、海外、特にアジア地域に拠点を設けて迷惑メールを送信していると考えられています。こういった送信拠点を無くすためにも、アジア地域で行政府組織と協力して対応をしていくことが重要になっています。

2.3 メールの技術動向

2.3.1 送信ドメイン認証技術の普及状況

これまで送信ドメイン認証技術に関して、ネットワークベースのSPF/SenderIDや、電子署名技術を利用したDKIM技術を紹介してきました。また、普及状況については、WIDEプロジェクトの調査結果[*6]を示し、特にSPFの送信側導入が順調に進んでいることも紹介しました。

今回は、実際に流れているメールにおいて、送信ドメイン認証技術がどの程度普及しているかを調査した結果を紹介します。IIJでは、2005年から送信ドメイン認証技術を導入し[*7]、これまでにSPFに加えてDKIMも順次サービスに導入する等、積極的な取り組みを続けてきています。

IIJが提供するメールサービスの一部ですが、メール受信時の認証結果の割合を図-4に示します。

調査期間は2009年9月いっぱいです。受信したメールのうち、送信者情報に示されたドメイン名をSPF認証した結果、56.2%が“none”でした。これは、受信メールの43.8%のドメインがSPFレコードを宣言していたことを示しています。WIDEでの調査では、2009年10月

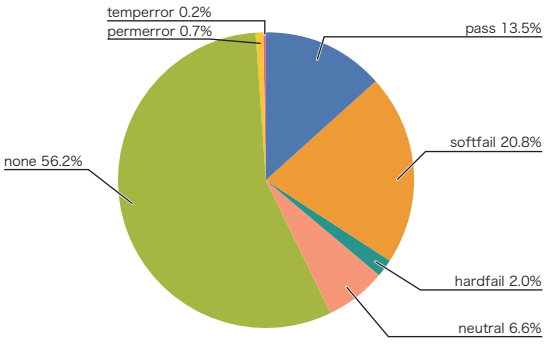


図-4　メール受信時の認証結果(SPF)

＊5　Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Countering Spam(http://www.sm-mou.org/)
＊6　WIDEが公表している送信ドメイン認証技術の普及率の調査結果(http://member.wide.ad.jp/wg/antispam/stats/index.html.ja)
＊7　IIJ、送信ドメイン認証技術の導入を開始(http://www.iij.ad.jp/news/pressrelease/2005/0317.html)

時点での“jp”ドメインの宣言率は36.8%ですので、実際の流量ベースではそれより多いという結果になります。もちろん、受信メールの送信側ドメインには、“jp”以外にも“com”や“net”等、多様なTLD（Top Level Domain）を使っているわけですが、日本での受信メールの分析結果としては比較的SPFが使われていると言えると思います。

SPFの認証結果の割合で、“pass”が13.5%、“softfail”や“hardfail”といった認証に失敗した割合が29.4%となっています。このことから、正規のメールサーバから送信されたメールよりも、送信者情報を詐称したメールのほうが多かったと推測できます。迷惑メールの受信割合が80%を超えている状況では、ある程度納得できる割合です。SPFの場合、転送問題など誤判定の問題があるため、慎重な運用が必要になります。ただし、SPFの宣言率と利用率がこのように高い状況では、SPF認証結果によるある程度のふるい分けは、非常に効果がある手法の1つになると言えます。

次にDKIMの認証結果について図-5に示します。

調査期間は、SPFと同じく2009年9月いっぱいです。受信メール全体に対して、何らかのDKIMに対応した送信者からのメールは0.8%という結果でした。DKIMの場合、送信側の導入がSPFに比べてコスト高になる等の点から、あまり普及していないことが分かります。ただし、DKIMは、ネットワークベースのSPF/SenderIDに比べて比較的誤判定の問題が少ないため、今後より重要なメールに利用されていくと期待しています。受信側の認証コストは、SPFもDKIMも機能追加という点では同じであるため、DKIMに関しては受信側の普及をSPFの受信側認証と同じように進めて行くことが重要だと考えています。

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、迷惑メールの判定割合の推移と送信元の分布について報告しました。さらに、迷惑メール対策として重要な国際協調に関して、民間や行政府組織間での会合情報や取り組みを、グローバルや日本が属するアジアパシフィック地域のそれぞれについて紹介しました。

IIJは、IIRに示すようなデータや技術を国際会議の場でも紹介し、それぞれの地域での取り組みや対策の促進を行っています。今後も、さまざまな場で積極的に迷惑メール対策に取り組んでいきます。

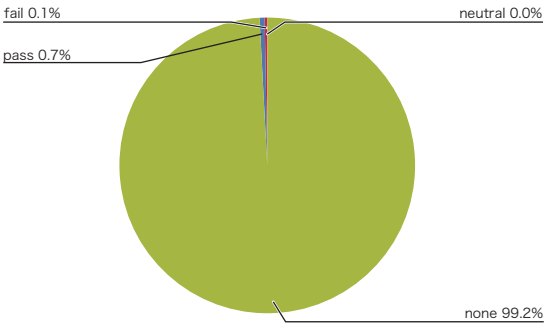


図-5　メール受信時の認証結果（DKIM）

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。（財）インターネット協会 迷惑メール対策委員。

移動通信機能NEMO BSを用いた ゲスト計算機のライブマイグレーション

効率のよい仮想環境を構築するには、仮想計算機の流動性を確保し柔軟に管理する仕組みが必要です。ここでは、IPv6ルータに移動通信機能を追加するNEMO BS技術を利用した、仮想計算機の移動方法を示し、その実験結果を考察します。NEMO BSを使うことで、ネットワークセグメントを越えた仮想計算機の移動が可能になります。

3.1 背景

計算機の処理能力、ネットワークやデータストア等の技術進歩により、個々の計算機の能力は飛躍的に進歩しています。一方、計算機単体の速度向上は今後鈍化するという見方もあり、近年は複数の計算機をひとつの計算機資源として取り扱うクラウド技術が注目されています[*1][*2]。また、ひとつの計算機資源を仮想的に分割し、複数の異なる計算機として利用する仮想計算機技術も長年研究されています[*3]。一見異なる方向を目指すように思えるこれらの技術ですが、互いを補うことでより効率よく計算機資源を活用できるものになると考えられています。たとえば、Amazonが提供するEC2[*4]は、複数の計算機資源を組み合わせてひとつのサービスにするクラウド環境を提供していますが、ひとつひとつの計算機資源には仮想計算機技術が用いられています。1台の物理的な計算機という大きな単位での資源管理をやめ、小さく切り出した仮想計算機をひとつの単位として利用することで、効率がよく柔軟な計算機資源の利用を実現し、結果的に仮想計算機に分割したことによる負荷を上回る利便性を提供しています。

このような仮想環境が発展していくためには、仮想計算機を柔軟に管理する仕組みが重要です。クラウド環境からの要求に従って、必要な場所に必要な量の仮想計算機を配置できることが、全体の性能向上や資源の効率よい利用に貢献するからです。ここでは、仮想計算機の再配置の仕組みに注目し、稼働中の仮想計算機を異なるセグメント(オフリンクセグメント)に移動させる手法を提案します。

3.2 ライブマイグレーションの課題

現在、多くの仮想計算機技術が実用レベルで提供されています。その中には仮想計算機を、その親となっている計算機(ホスト計算機)から別のホスト計算機に移動させる機能を提供しているものもあります。VMwareのVMotionやXen[*5]のLive Migrationがこの代表例です。以後、ここではホスト計算機から切り出された仮想計算機を「ゲスト計算機」、ゲスト計算機をホスト計算機間で移動する機能を「ライブマイグレーション」と呼びます。ライブマイグレーション機能を利用すると、稼働中のゲスト計算機をほとんど停止することなく別の機材に移動できます。ただし、現在提供されている機能には、移動元のホスト計算機と移動先のホスト計算機が同一のセグメントに属していなければならないという制限があります。

この制限は、ゲスト計算機に提供されているネットワーク構成方式によるものです。ホスト計算機とゲスト計算機の関係は対等ではありません。通常、ホスト計算機がすべての資源を管轄し、ゲスト計算機にその一部を配分します。ゲスト計算機をネットワークに接続す

＊1　Aaron Weiss. Computing in the clouds. *netWorker*, Vol. 11, No. 4, pp. 16-25, December 2007.
＊2　Brian Hayes. Cloud computing. *Communications of the ACM*, Vol. 51, No. 7, pp. 9-11, July 2008
＊3　Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, et al. Xen and the art of virtualization. In *SOSP '03: Proceedings of the nineteenth ACM symposium on Operating systems principles*, pp. 164-177. ACM, 2003
＊4　Amazon. Amazon Elastic Compute Cloud (Amazon EC2), October 2009. http://aws.amazon.com/ec2/
＊5　Citrix, October 2009. http://www.xen.org/

る場合、図-1に示すようなネットワーク構成が用いられます。図-1の構成(a)では、ゲスト計算機はホスト計算機と同じネットワークに、ホスト計算機が提供する仮想スイッチを経由して接続されます。構成(b)でも、ホスト計算機とゲスト計算機の間に仮想スイッチが設けられます。構成(a)と異なり、この場合、ホスト計算機はゲスト計算機の上流ルータとしても機能します。図-1からも明らかなように、ゲスト計算機のネットワーク構成はホスト計算機に大きく依存します。ライブマイグレーションの実行時には、ゲスト計算機自体の動作環境は変更しません。結果的に、構成(a)でしかライブマイグレーションは実現できません。構成(b)では、仮想スイッチに割り当てられるアドレスがホスト計算機によって異なります。これでは、ゲスト計算機を移動した後、ネットワーク環境を適切に変更しない限り通信を継続できません。また、構成(a)であっても、移動元と移動先のホスト計算機が異なるセグメントに接続している場合、同様の問題が発生します。

ライブマイグレーションによって、仮想計算機が1つのホスト計算機に集中することは回避できますが、その機能は同一セグメント内での移動に限られます。他のセグメントに資源に余裕のあるホスト計算機が配置されていても、それを活用することはできません。また、ゲスト計算機を利用者により近いホスト計算機に移動させるような、性能向上のための資源再配置もできません。

3.3 NEMO BSの概要

NEMO BS (Network Mobility Basic Support)*6は、IPv6ルータに移動通信機能を追加する仕様です。NEMO BS環境では、NEMO BSに対応したMR (モバイルルータ)が固定のネットワークプレフィックスであるMNP (モバイルネットワークプレフィックス)を管理します。MRが提供するネットワークに接続したIPv6ホストは、MNPの範囲にある固定アドレスを利用します。MRはインターネット上のさまざまなセグメントに接続し、接続先のネットワーク環境に応じてインターネットへの接続性を確保します。このとき、MRが管理するMNPは変化しません。MR配下のホストは、MRの位置にかかわらず常に同じネットワーク環境を維持できます。

この機能は、MRと対をなして動作するHA(ホームエージェント)によって実現されています(図-2)。MRは移動先のネットワークで、ネットワーク環境に応じたアドレス(気付アドレス)を取得し、HAとの間に双方向IPv6 over IPv6トンネルを確立します。MNP内のノードで発生したトラフィックは、このトンネルを使っていったんHAに送られ、HAから通信相手に転送されます。一方、MNP内部ノード宛のトラフィックは、HAでいったん受け取られ、トンネルを介してMRに配送された後、最終宛先のホストに転送されます。

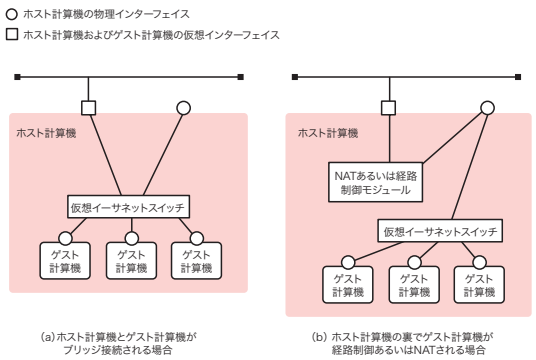


図-1　ゲスト計算機のネットワーク構成

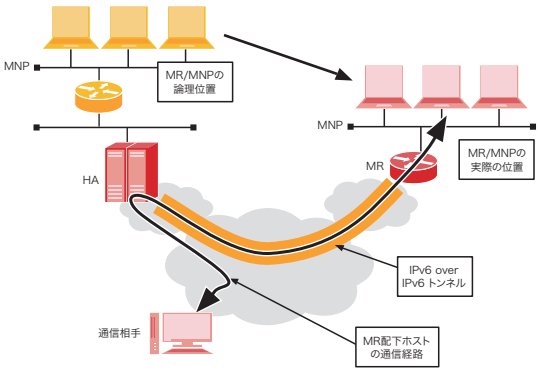


図-2　NEMO BSの動作概要

*6　Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, and Pascal Thubert. *Network Mobility (NEMO) Basic Support Protocol*. IETF, January 2005. RFC3963

3.4 設計

ライブマイグレーションが同一セグメント内での移動に制限される理由は、ゲスト計算機のネットワーク環境がホスト計算機に依存しているためです。つまり、ゲスト計算機のネットワーク環境がホスト計算機によらず一定になるように設計すれば、異なるセグメントに接続しているホスト計算機にもゲスト計算機を移動できるようになります。

ここでは、ゲスト計算機のネットワーク環境を一定に保つ方法として、IPモビリティ技術を用いる方法を提案します。この方法には、ゲスト計算機自体がMobile IPなど[*7][*8]のホスト移動通信機能を備える方法と、ホスト計算機がNEMO BSなどを活用して固定ネットワークをゲスト計算機に提供する方法が考えられます。前者では、ゲスト計算機の改変(IPモビリティ機能の導入)が必要ですが、ゲスト計算機単体での移動が可能になり、計算機資源の細かな制御が期待できます。後者の方法では、これまで利用してきたゲスト計算機を無変更で継続利用できる代わりに、ゲスト計算機の移動とNEMO BSのMRとしてホスト計算機の移動が同期しなければならないという制限が生じます。今回は、既存のシステムで用いられているゲスト計算機をそのまま利用し続けるというシナリオを前提として、後者の方法に注目します。

システムの設計は、ホスト計算機の資源管理の方法によって異なる可能性があります。ここでは、Xenが提供する仮想計算機環境を用いた設計を提示していますが、他のシステムでも大きな変更は必要ないと思います。図-3がその概要です。構成は、図-1の構成(b)を拡張したものになります。ホスト計算機がMRとしての機能を持ち、インターネット接続用と、MNP提供用の2つのインターフェースを提供します。MNP接続用インターフェースは、物理的なインターフェースではなく仮想インターフェースです。仮想インターフェースは、ホスト計算機が提供するゲスト計算機用の仮想スイッチに接続されています。ホスト計算機の仮想インターフェース、および仮想スイッチに接続されたゲスト計算機のインターフェースには、MRが管理する固定アドレスが割り当てられます。NEMO BSの機能により、ホスト計算機が物理的にどこに接続されていても、MNP内のアドレスが変化することはありません。

ゲスト計算機をライブマイグレーションする環境では、複数のホスト計算機がネットワーク上に配置されます。これらのホスト計算機には、MRとして同じMNPが設定されますが、稼働中のゲスト計算機を有していないホスト計算機はMRとして動作しません。ゲスト計算機を移動する場合、まず通常のライブマイグレーションの手順を用いて、移動先のホスト計算機にゲスト計算機を移動します。この時点では、まだゲスト計算機はネットワークから切り離された状態です。その後、移動元のホスト計算機が移動先のホスト計算機に移動完了通知を送り、自分自身のNEMO BS機能を停止します。移動完了通知を受けたホスト計算機は、HAに対して現在位置を登録し、NEMO BSのMRとしての動作を開始します。HAへの登録が完了した段階で、ゲスト計算機が接続している仮想スイッチのMNPが有効となり移動が完了します。

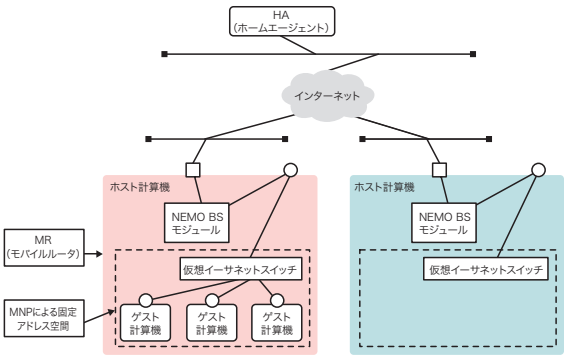


図-3　NEMO BSを用いたゲスト計算機の移動

＊7　Basavaraj Patil, Phil Roberts, and Charles E. Perkins. *IP Mobility Support for IPv4*. IETF, August 2002. RFC3344
＊8　David B. Johnson, Charles E. Perkins, and Jari Arkko. *Mobility Support in IPv6*. IETF, June 2004. RFC3775.

3.5 実験による検証

提案した設計が実現可能であることを確認するため、プロトタイプを実装して稼働実験を行いました。実験環境は、HA、NEMO BS機能を備えMRとして動作する2台のXenホスト計算機、テスト用のストリーミングデータを受信する計算機と、移動の指示を出す制御用計算機の合計5台で構成しました。Xenホスト計算機には1台のゲスト計算機を構築し、ストリーミングサーバとして動作させました。

実情に近い環境で実験するため、これらの機材は実際のインターネット環境上に配置しました。HA、およびMRが利用する固定ネットワークはInterop Tokyo 2009[*9]のために構築された運用ネットワークの一部に設置し、Xenホスト計算機とストリームデータ受信ノードはIIJのネットワーク上に配置しました。それぞれの機材はインターネットを介して相互接続しています。図-4に実験ネットワークの概要を示します。

ゲスト計算機(ストリーミングサーバ)からは、15Mバイト、520Kビット/秒のMPEG4ストリームデータをUDPを使って継続的に送信しました。また、今回、ゲスト計算機のライブマイグレーション開始指示、およびホスト計算機のNEMO BS機能の停止作業と開始作業は、別途用意した制御用計算機からsshを用いて行いました。制御用計算機から、ゲスト計算機のライブマイグレーションコマンドを遠隔実行し、ライブマイグレーションが完了した直後にホスト計算機のNEMO BS移動処理を実行しています。この操作を5分間隔で繰り返し、2台のホスト計算機間でのゲスト計算機の移動を繰り返しました。

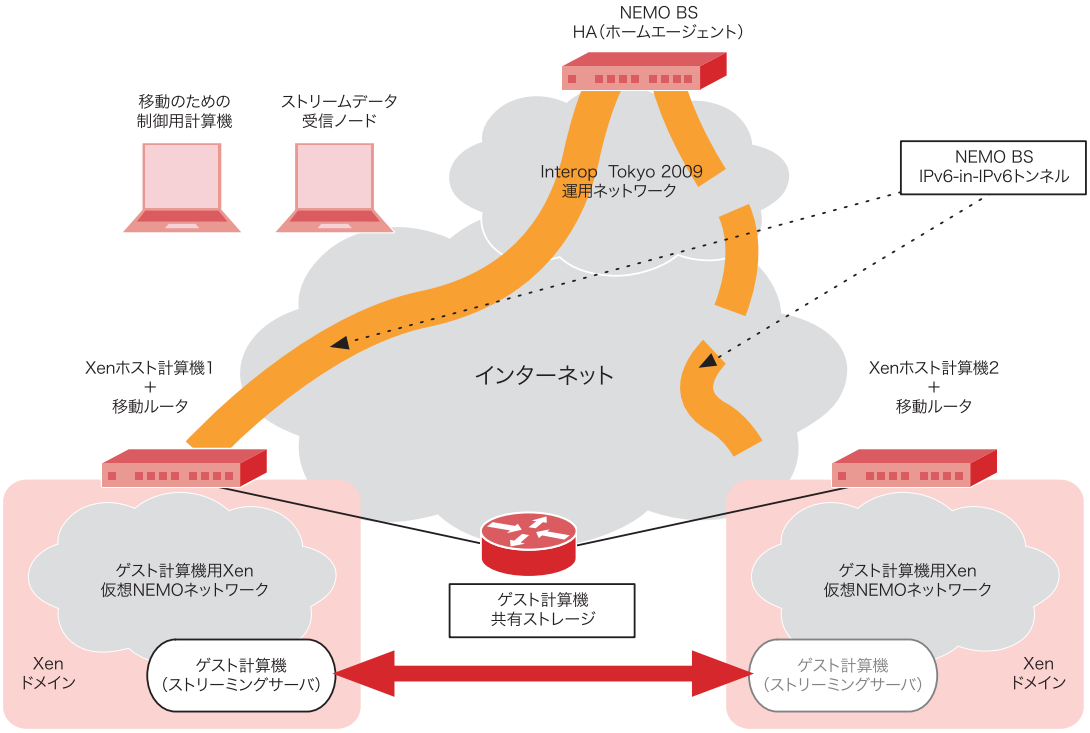


図-4 実験ネットワークの概要

*9 Interop Tokyo 2009, June 2009. http://www.interop.jp/

3.6 評価と課題

ホスト計算機のインターネット側インターフェースでストリームトラフィックをモニタした結果を図-5に示します。5分ごとにゲスト計算機がライブマイグレーションされ、トラフィックグラフが2台のホスト計算機の間を移動していることが確認できます。

ライブマイグレーションでは、仮想計算機のデータを移動先のホスト計算機に複製している間も、移動元の仮想計算機が動作し続けます。切り替え時の停止時間はわずか(数百ミリ秒)です。ただし、今回の構成ではネットワーク層の技術を用いてホスト計算機を移動させたため、ゲスト計算機の移動後にホスト計算機の移動処理も必要でした。トラフィックデータを詳細に調べたところ、一方のホスト計算機がストリーミングデータの配信を停止した後、移動先のホスト計算機がストリーミングデータを送信し始めるまでに6秒程度の時間がかかっていることが判明しました。

ホスト計算機が接続するネットワークでのルータ広告の間隔は3 ～ 4秒でしたので、ホスト計算機はおよそ2秒間でルータ広告を受信できる環境にありました。NEMO BSの処理の一部である、気付アドレスの重複確認に1秒間かかることを含めても、この環境では3秒程度で移動処理が完了するはずです。今回、それ以上に時間がかかっている理由として次の2点が考えられます。

1. 制御計算機からの遠隔操作スクリプト実行によるオーバヘッド
2. 通常の移動とは異なる手順

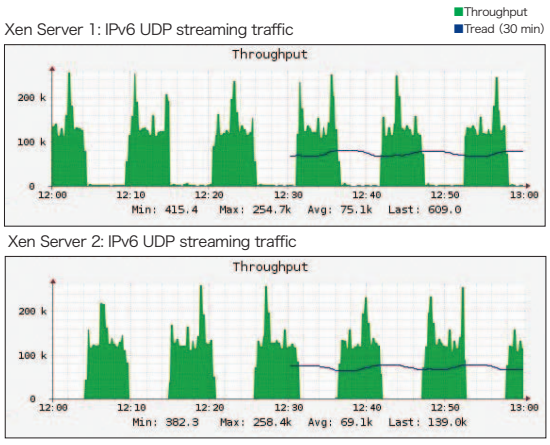


図-5　ストリームトラフィックの推移

NEMO BS機能の停止と開始をsshによる遠隔スクリプトで実行したため、TCP接続のための時間、ホスト計算機でのプロセス生成時間、遠隔コマンドによるNEMO BSデーモンプログラムの制御などの時間が、通常の運用と比較して余計に必要となっています。また、本来ならば単一の移動ノードで実行される移動処理が、今回は2つの異なる移動ノードで協調実行されています。つまり、一方のMRがHAへの登録解除処理を完了した後に、もう一方のMRが登録処理を実行しています。同一MRで移動処理を実行する場合、新しい情報の登録時に古い情報の登録を解除する必要はなく、連続した更新になります。今回は、解除のために余計な時間がかかっています。

3.7 考察

今回の実験は、2つの技術(NEMO BSとXen仮想化)の組み合わせ検証となっています。次に、検証の過程で得た知見を述べます。

3.7.1 ネットワークストレージの問題

仮想計算機環境を提供する仕組みでは、ゲスト計算機のストレージ提供方法として、ホスト計算機のストレージの一部を提供する方法と、ネットワークストレージを提供する方法の2種類が考えられます。ライブマイグレーションを利用する場合、ゲスト計算機を収容するホスト計算機が変わるため、ストレージはネットワーク上に配置しなければなりません。現在想定されている利用方法では、ゲスト計算機が同一セグメントを越えて移動することがないため、ネットワークストレージを利用しても移動前後に大きな環境の変化は生じません。しかし、今回の提案のようにセグメントを越えてゲスト計算機を移動する場合、ネットワークストレージへの到達性、応答性などが問題になる可能性があります。

1つの解決策として、外部ストレージを用いずに、すべてをメモリ上で処理するゲスト計算機環境を構築する方法が考えられます。しかし、この方法ではメモリ上に保持するデータ量が増えるに従って、移動完了までの時間が増加します。また、その構造上、大量のデータを扱うことが困難になります。

別の方法として、インターネット上の複数地点から効率よく透過的に扱えるストレージを提供する方法が考えられます。例えば、ストレージのミラーリング技術を発展させ、複数拠点からの同一ストレージデータへのアクセスを可能とすることで、ゲスト計算機に対する変化を抑えるとともに、ストレージの耐障害性の向上も図ることができるはずです。

3.7.2 利便性の問題

今回移動通信技術としてNEMO BSを用いましたが、この方法には2つの問題点があります。

まず、NEMO BSを含むMobile IP系の移動通信技術一般に言えることですが、HAを介したトンネル通信が前提となってしまう点です。HAが一点障害になるため、HAの多重化技術を導入しなければならない等、別途考慮すべき点が発生します。ただし、この問題は、トンネルを用いない移動通信技術を採用することで解決できる可能性があります。例えば、HIP[*10]やLIN6[*11]、MAT[*12]等を基礎としたMRを用いる方法です。仮想計算機のオフリンクライブマイグレーションを実現するための条件は、仮想計算機が接続する仮想スイッチのネットワーク環境を維持することです。したがって、それを実現する方法がNEMO BSである必然性はありません。

2つ目の問題点は、NEMO BSを利用したことで、すべてのゲスト計算機が同一の固定ネットワークのノードとして管理される点です。これによって、ホスト計算機が移動した場合、関連するすべてのゲスト計算機群も同時に移動しなければなりません。この問題は、次のいずれかの方法で対応可能と考えられます。1つはゲスト計算機がホスト単位の移動通信技術、例えばMobile IPを採用することです。この場合、すべてのゲスト計算機でMobile IPへの対応が必要となり、導入に関する敷居が高くなります。NEMO BSを利用すると、ゲスト計算機の変更が不要になり、標準のゲスト計算機をそのまま利用できるという大きな利点があります。これらの折衷案としてゲスト計算機ごとにNEMO BS環境を提供することが考えられます。一種のMobile IPプロキシのような運用です。この方法を使うと、ゲスト計算機の変更を避けながら、ゲスト計算機単位での移動ができるようになります。

3.8 おわりに

今後到来するクラウド環境において、計算機資源の流動性を確保することが重要です。仮想計算機のライブマイグレーション技術は、資源流動性を確保するための有力な候補です。ただし、現在のライブマイグレーション技術では、移動先が同一セグメント内の別のホスト計算機に限定されています。これは、ゲスト計算機に提供されるネットワーク環境が、ホスト計算機が接続する物理ネットワークに依存するためです。この制限を取り払い、別セグメント、遠隔のセグメントに移動できれば、計算機資源をより流動的に管理できるようになります。ここでは、仮想化技術とNEMO BS技術を用いて、セグメントを共有していない複数のホスト計算機間でゲスト計算機を移動させる手法を提案しました。NEMO BS技術を使い、ホスト計算機の接続ネットワークにかかわらず常に固定のネットワーク環境をゲスト計算機に提供することで、セグメントを越えた移動が可能になります。

最後に、本研究を進めるにあたり、中村雅英氏、Jean Lorchat氏、Martin André氏からLinuxおよびMIPL/NEPLの構成について多くの助言をいただきました。また、実験環境の準備に尽力していただいた三宅喬氏、織学氏およびInterop Tokyo 2009 NOCチームのみなさまに感謝いたします。

執筆者：
島 慶一（しま けいいち）
株式会社IIJイノベーションインスティテュート技術研究所
今後ますます進んでいくインターネット端末のワイアレス化に必要となる、IP移動通信技術の研究開発を進めている。

＊10 Robert Moskowitz, Pekka Nikander, Petri Jokela, and Thomas R. Henderson. *Host Identity Protocol*. IETF, April 2008. RFC5201
＊11 Mitsunobu Kunishi, Masahiro Ishiyama, Keisuke Uehara, Hiroshi Esaki, and Fumio Teraoka. LIN6: A New Approach to Mobility Support in IPv6. In *Wireless Personal Multimedia Communication (WPMC)*, November 2000
＊12 相原玲二, 藤田貴大, 前田香織, 野村嘉洋. アドレス変換方式による移動透過インターネットアーキテクチャ（〈特集〉次世代移動通信ネットワークとその応用）. 情報処理学会論文誌, Vol. 43, No. 12, pp. 3889-3897, 20021215

遠隔データセンタと、仮想化技術を活用した次世代サービス基盤NHNの導入

NHN(Next Host Network)は、IIJが目指す次世代のサービス基盤です。NHNの導入によって、IIJでのサービス開発フローや設備増強のための需要予測が大きく変わろうとしています。ここでは、NHNを導入するにいたった背景、その設計思想や技術要素を説明します。

IIJでは、遠隔データセンタの活用によってデータセンタコストを圧縮しながら、運用自由度の高いサービス基盤を実現しています。現地作業の集約、ラックスペースや電力を無駄なく使う工夫を施し、運用コストの削減を目指した「NHN」(Next Host Network)を2008年度に設計し、新規サービスと既存サービスを移行する基盤として整備しました。ここでは、NHNの導入の背景、設計思想、技術要素について説明します。

4.1 NHN導入の背景

IIJではこれまで、自社サービス用に複数のデータセンタに分散して200ラック以上、数千台のサーバを運用してきました。各ホストはサービス単位でラックを確保して設備を構築していたため、それぞれのラックスペースやネットワーク機器に、将来の需要増に耐えうる余裕を設けており、基盤全体としてのロスが発生していました。このようなサービスごとの縦割りのシステム構成では、計画変更による拡張や、廃止時の設備の転用等が困難で、サービス基盤のコストがかさむうえ、ラックによって機材や配線が異なるため、運用作業の煩雑さも課題となっていました。

また、これまでは障害時の対応等を考慮した結果、物理システムへのアクセスの容易さから東京近郊で立地条件のよいデータセンタを利用し、サーバ運用の最適化を図ってきました。しかしながら、この数年、IAサーバの性能向上と低価格化を背景に、サーバ1台あたりの消費電力は高まり続け、ネットワーク、サーバ、ストレージ等の機器コストよりも、ラックスペース、冷却用の空調費、電気代といったファシリティコストの比率が高い状況になっています。東京都内のデータセンタは、お客様からの引合いが多く、機器の設置スペースはあっても、空調能力、UPS、非常用発電機の容量不足等の制約から十分にサーバを設置できない状況になってきました。

東京近郊のデータセンタにシステムが集中する構成に限界が見えてきたため、IIJでは場所に依存しないサービス用機材は、郊外等ファシリティコストの低い場所に移すことで、抜本的なコスト削減を目指すことにしました。検討にあたっては、コンテナ型データセンタ等、ファシリティコストの圧縮や電源事情の緩和につながるあらゆる方策を検討しています。多重化技術の進化によりネットワークコストも抑えられるようになってきたことも、郊外データセンタの検討を後押ししました。

また検討に際しては、遠隔データセンタを利用しても運用の自由度と機動性を確保できる構成への見直しも同時に進めました。

サービス用機材を郊外のデータセンタに持っていくことでスペース費用、人件費、電気代等を削減し、サービス基盤全体としてコスト削減に繋げること。同時に運用の自由度を向上させることを目指して、NHNの検討はスタートしました。

4.2 遠隔データセンタ利用を視野に入れた設計方針

NHNでは、サーバ運用者の経験を元に、重要視しなければならない部分と、保留できる部分を次のように切り分けました。

- ストレージに関しては、HDD単体故障等想定可能な故障は容認する。ただし、サービス停止に繋がる故障が起きないように、信頼性の高い構成にする必要がある
- サーバ機器はときどき故障する。故障ポイントは多岐にわたり、故障率を下げることには限界があるため、故障しても影響の少ない構成にすることが望ましい
- エッジで利用するネットワーク機器の故障は、これまでの経験上それほど多くない。NIC冗長化設定等は必要なときにのみ実施する

次に、IIJで利用している機器の故障率等を示し、上記の方針に至った経緯を説明します。

4.2.1 ストレージの故障率について

IIJで利用している約100台のDAS[*1]のログを調査したところ、ストレージの台数自体はあまり変わっていないにもかかわらず、HDDの故障数自体が年々減少傾向にあることが確認できました。また、この数年間の傾向として、ストレージの負荷とHDDの故障率に相関関係がほとんどみられなくなってきています。負荷の高さに関係なくHDDの故障は発生し、同一ストレージに搭載したHDDに故障が偏ることは稀なようです。

年	HDD故障数	同一RAIDでのHDD故障数
2005年	32台	7×1台、5×1台、4×1台、[*2] 2×2台、1×12台
2006年	22台	2×3台、1×16台
2007年	16台	2×1台、1×14台
2008年	7台	2×2台、1×3台
2009年	4台	1×4台(2009年9月現在)

HDDの故障率が年々下がっているため、HDD故障以外のストレージ障害、特にサービス停止に直結するものがより目立つようになってきました。具体的には、次のような障害によるものです。

- RAIDコントローラ上のキャッシュメモリの故障による機能停止
- RAIDコントローラの故障が原因と思われる不安定な動作
- SCSIカード等の接続インタフェースの故障
- RAIDコントローラ上のバッテリバックアップユニットの故障もしくは寿命による性能劣化

故障回数は、全体で1年間に数回程度ですが、RAIDコントローラの二重化や接続パスの二重化を行っていない機器で上記のような障害が発生してしまうと、現地で機器交換作業を行うまで復旧できずサービスの停止に直結してしまいます。遠隔データセンタを視野に入れると、ストレージのサービス停止は交換作業完了までに必要な時間が非常に長く致命的であると考えました。このため、現状よりハードウエアコストは増えますが、RAIDコントローラの二重化、接続パスの二重化を必須条件として機器選定を行いました。

4.2.2 サーバの故障率について

サーバの故障率に関しては、サービス復旧を優先して予防交換してしまうことが多く、その後に故障機器を持ち帰って試験しても再現できないこともあり、故障部位別の統計情報は取れていません。

2009年4月から9月までの6か月間で修理したサーバ数、現在予防交換して検査待ちになっている機材の台数から、故障率はおよそ1〜2%程度と推定しています。ただし、この値には、冗長HDDでの片側の故障といった冗長部品の故障は含んでいません。このため、サーバ機器に関しては、かなり多くの台数が故障すると推定しています。

＊1　Direct Attached Storageの略。IIJでは2008年までSCSI I/Fを経由して外部接続する形態のものを中心に利用していました。サーバ上にローカルHDDを載せる形式のHDD故障数は含めていません。
＊2　2005年の同じRAID上で7台、5台、4台の故障が起きているものは、同一タイプの製品かつ同一時期の導入品のため、ロット不良の可能性が高いです。2005年にサービス利用から外しました。

故障理由では、メモリ故障による停止や再起動が目立ちます。また、ファン故障による熱暴走、HDD等の接合部分のバックプレーン故障、電源(VRM)故障、プロセッサ故障等多岐に渡っていました。

ローカルHDDを搭載したサーバ機器で起動不可能な障害が発生した場合、現地に赴いてHDDを故障機材とは別の正常なサーバ機材に移設し復旧する必要があります。データセンタに上記のようなサーバ機器のメンテナンスができるオペレータを常時配置するためには多くの人件費がかかります。そのため、遠隔データセンタを視野に入れると、常時オペレータを配置するとコストが増大し、とはいえ、オペレータを配置しなければ、復旧までに多大な時間を費やさなければならないことを意味します。このため、サーバはローカルデータを持たないディスクレス運用を前提に機器選定を行いました。

4.2.3 ネットワーク機器の故障率について

ホスト等を収容するエッジL2スイッチの故障件数ですが、これまでの経験からあまり多くありません。コンデンサ不良等特定の不良ロットに該当したケースを除けば、稼働数から考えても1%未満です。

NIC冗長化設定による冗長化構成を採ることもできますが、NICやネットワーク機器の追加が必要になりコスト増加の要因となります。また、ロードバランサ等を使ってサーバ間での冗長構成を採ったほうが運用が簡単になることが多いため、基本構成ではサーバ収容スイッチは冗長化せず、より高い信頼性が必要なときにのみNIC冗長化設定を実施する設計にしました。また、エッジL2スイッチの故障時の影響を抑えるときには、ロードバランサ等を使って別のサーバ収容スイッチ配下の機器と冗長構成を組むか、障害発生時に障害サーバ収容スイッチ以下のサーバ機器の中身を遠隔操作で別のサーバ収容スイッチ以下のサーバに移動して対応できるよう設計しました。

4.3 NHNの構成

NHNは、遠隔データセンタにも対応できる次のような構成にしました。

- サーバプール方式にして同一スペックのサーバを多数設置する。機器の設置、障害機器の物理交換等の現地作業は、計画作業として月1回等集約できるようにする。
- サーバ構成を画一化して構成管理のコストを抑えるために、物理搭載メモリ量の変更やローカルHDDの搭載等物理構成を変える作業は行わない
- 省電力サーバを利用してラックごとのサーバ収容数を向上
- サービス単位のラック割をやめラックごとのサーバ収容数向上
- 外部業者による機器設置や交換作業をスポットで委託することを想定して、機器や配線を画一化し作業ミスが起きにくいようにする
- Xen、OpenVZ等の仮想化技術と組み合わせ、集約度と自由度を上げる
- VLANを使い、現地での配線変更なしに論理ネットワークを構成できるようにする
- iSCSIを利用して安価なSANを構成する。ストレージは、極力サービス停止が起きないようにRAIDコントローラや接続パスの二重化を必須とする
- ディスクレスサーバは壊れることを前提にする。ハードウエアの障害発生時にはリモートから切り替え作業を行い一次対応が完了できるものを目指す
- ディスクレスサーバの故障発生時に予備サーバへの切り替え完了までの時間がサービス停止として許容できないものであったときには、あらかじめ系の異なる2つのサーバを準備しロードバランサ等を利用して冗長構成を採り、アプリケーション側での冗長構成を実現する
- OSのインストールを含めて、設置以降に必要となる作業をリモートから実行可能にする

次に、それぞれの技術要素について説明します。

4.3.1 iSCSIストレージを利用したIP SANの導入

遠隔データセンタとしての利用を視野に入れた場合、ストレージのサービス停止は長時間の障害に繋がるため、ストレージにはこれまで以上の高い信頼性を求めました。IIJは、IPネットワーク技術に長けていること、またFC SANに比べて安価にシステムが組めることから、iSCSIを利用したシステムを導入しています。そして、RAIDコントローラの二重化、接続パスの二重化を必須条件とすることで、サービス不能に陥るストレージの故障を極力減らすようにしています。

4.3.2 iSCSIストレージと省電力サーバを組み合わせたディスクレスサーバの実現

現行のサーバ機器は、iSCSIブートに対応しているものが少なく、すべてのサーバ機器にiSCSI HBAを装着するとコストがかかります。このため、ほとんどのサーバ機器のオンボードNICが対応しているPXE bootを使い、iSCSIを使ったSAN bootができるよう工夫しています。

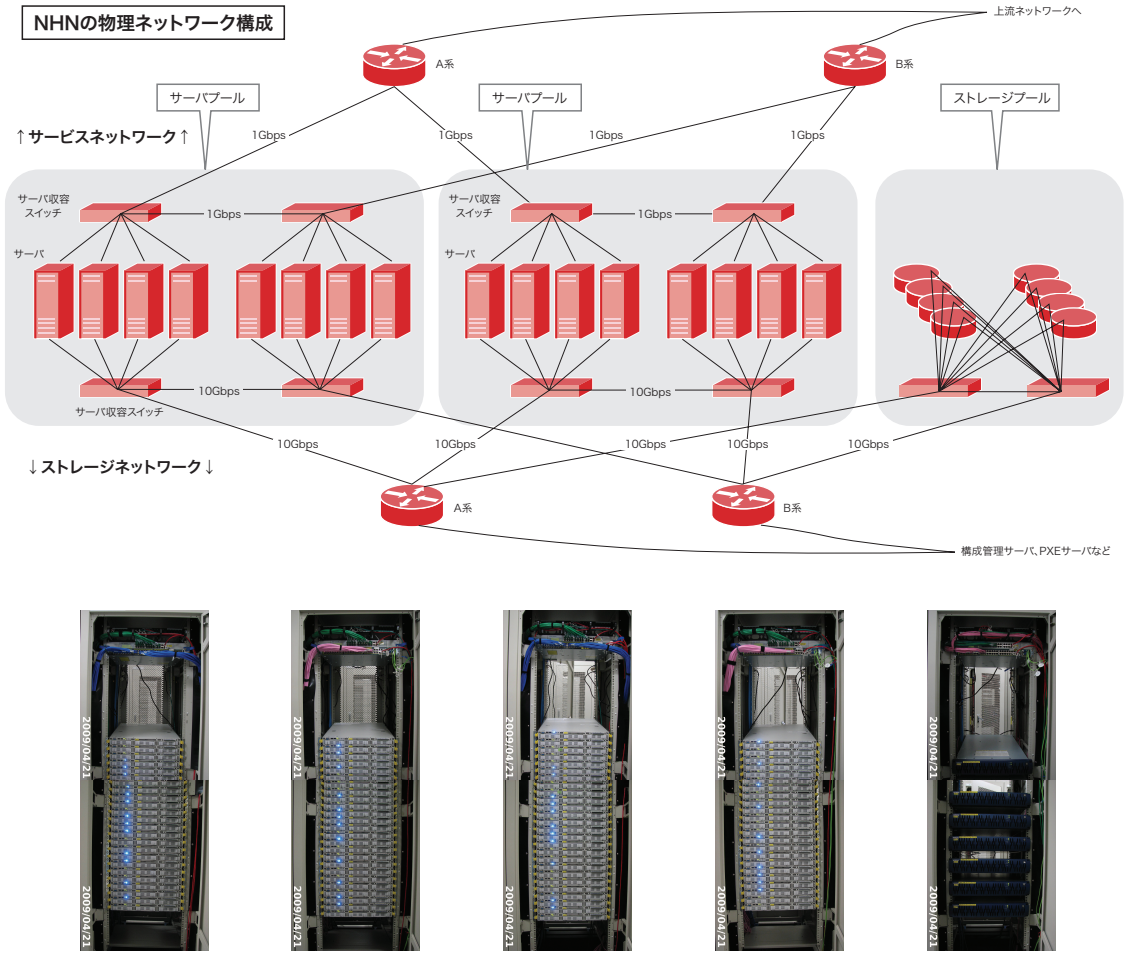
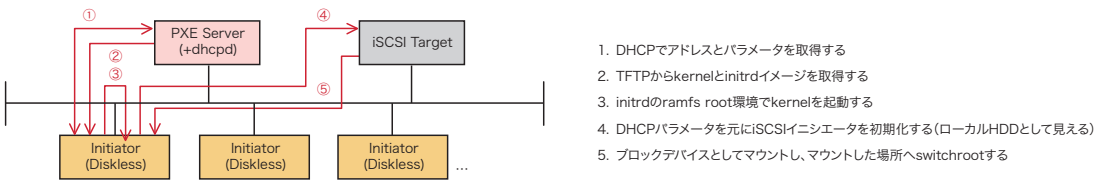


図-1　NHNの物理構成



1. DHCPでアドレスとパラメータを取得する
2. TFTPからkernelとinitrdイメージを取得する
3. initrdのramfs root環境でkernelを起動する
4. DHCPパラメータを元にiSCSIイニシエータを初期化する（ローカルHDDとして見える）
5. ブロックデバイスとしてマウントし、マウントした場所へswitchrootする

図-2　PXE bootとiSCSIによるディスクレスサーバ（Linux）の起動

iSCSIブートに必要なiqn[*3]、IPアドレス等の情報は、DHCPオプションを使って情報を渡します。これによって、構成情報を書き換えて予備サーバを起動することで、故障したサーバ機器と予備機を入れ替えることができます。

サーバ故障に伴う現地作業を回避するため、NHNではサーバ自体をディスクレス構成にしローカルデータを持たないようにしました。仮にサーバ機器の1台に故障が発生したときには、リモートから構成情報を書き換えて再起動することで、すでに設置済みの予備サーバを故障機器のストレージの内容を保持したまま起動できます。

4.3.3 VLANを使った配線変更不要な仮想ネットワークの実現

NHNでは、1本の物理配線に複数のネットワークを同居させることで、現地での配線変更を不要なものにし、リモートのみでの対応を可能にしています。技術的には、サーバごとにaccess VLANとtrunk VLANを使ってネットワークを構成し、必要に応じて1本の物理配線に複数のネットワークを同居させます。

VLAN自体は目新しい技術ではありませんが、NHNではIIJが管理する構成情報と連動して自動的に該当ホストを収容しているサーバ収容スイッチのVLAN設定を書き換える仕組みを実装しました。これにより、ネットワーク機器のVLAN設定のミスを減らし、運用コストを削減しています。

執筆者:
牧野　泰光(まきの やすみつ)
IIJサービス事業統括本部 システム基盤統括部 システム基盤運用課 課長
IIJ法人サービス、個人サービスのサーバインフラ設計、運用業務に従事。2008年度よりサービスホストの設備調達、現地構築業務等をシステム基盤運用課に集約し、基盤システム化していくことで設備の集約、運用の効率化を推進。

花高　信哉(はなたか しんや)
IIJ サービス事業統括本部 システム基盤統括部 システム基盤運用課
小林　直(こばやし ただし)
IIJ サービス事業統括本部 システム基盤統括部 システム基盤運用課

4.4 導入効果

IIJでは、2008年度に今後の遠隔データセンタ利用を視野に入れ「NHN」というキーワードでサービスホスト構成の大幅な見直しを実施し、新規サービスと既存サービス移行のための基盤整備を行いました。

NHNでは、サーバ運用者の視点と経験を元に最新の技術を取り入れ、仮想化、iSCSIを使ったディスクレスサーバ、ホスト情報の集中管理、ネットワーク機器のVLAN設定の動的変更等を導入しました。

NHNを社内サービスに導入した当初、それまでのサービスホスト構成との違いが浸透していなかったため、次のような意見を聞くことがありました。

- 仮想化サーバでは不安。物理サーバにしてほしい
- これほどの性能は必要ないので、もっと安価なサーバにしてほしい
- メモリ量が多すぎるので減らしてほしい
- ローカルディスクに比べてディスク単価が高い

当初はこのような意見が聞かれましたが、個々のサーバが多少高価なものであっても、仮想化の導入による集約、ファシリティ、運用コストまで含めたコストを考慮すると安価になることが理解され、現在では社内導入の敷居は低くなっていると思います。

また、サーバを要求した数日後には利用可能になり、不要になった時点でデータセンタでの物理作業なしに返却できるメリットが浸透してきています。それまでは、サービスごとにばらばらの機器を使って設備を構築していたため、計画変更による他サービスへの転用が難しかったり、急に機器が必要になっても購入待ちや設置待ちですぐに利用できませんでした。NHNの導入によってサービスの開発フローや設備増強の需要予測の仕組みも変わりつつあります。

IIJは、引き続きセキュリティ部分やI/Oの仮想化部分等を詳細に検討し、IIJ GIO等のお客様への提供に向けて完成度をより高めていきます。

＊3　iSCSI Qualified Nameの略。今回はiSCSIターゲットを一意に識別するために利用します

インターネットトピック: マルウェア対策研究人材育成ワークショップ2009について

ここでは、2009年10月26日から3日間にわたって富山国際会議場で開催された、マルウェア対策研究人材育成ワークショップ2009（MWS2009）について紹介します*1。このワークショップは、情報処理学会とサイバークリーンセンター運営委員会が主催する、マルウェア解析に関する研究ワークショップです。昨年のMWS2008*2に続き今年が2回目の開催となり、研究者、学生、企業の技術者など100名以上が参加して発表や議論が活発に行われました。このワークショップは、サイバークリーンセンター*3で取得されたマルウェアの活動の情報（マルウェア検体や通信の情報）を元に、共通の解析対象としてCCC DATAset2009 を作成し、このデータセットに対して解析技術や対策技術の研究成果を共有する試みとなっています*4。

■CCC DATAset2009

発表者には、CCC DATAset2009として次の3種類のデータが提供されます。

● マルウェア検体データ

対象となる10種類のマルウェア検体のハッシュ値（検体は研究者が自ら入手する必要がある）。また、後日解析結果が提供される。

● 攻撃通信データ

ハニーポット2台に対する通信情報2日分（CCC DATAset 2009 では2009年3月13日～ 14日）。実際の通信を示すパケットダンプが提供される。

● 攻撃元データ

ハニーポット94台に対する攻撃通信の記録1年分（CCC DATAset2009では、2008年5月1日～ 2009年4月30日）。ここには、時刻、攻撃元IPアドレス、攻撃先のポート番号、感染したマルウェアに関する情報などが含まれる。

CCC DATAset2009の内容は、昨年の CCC DATAset2008 よりも拡充*5されています。発表者は、自分の研究成果をこれらのデータのいずれかに適用することで、実際の観測データを元にその有効性を検証できます。

■MWS2009の様子

昨年は一般口頭発表が22件（うち学生によるものが8件）でしたが、MWS2009では一般口頭発表30件（うち学生によるものが15件）となり、発表数が大幅に増えています。また、その内容も、マルウェア解析を効率的に行う手法から、ハニーポットの改善手法、マルウェア活動の可視化手法や活動予測の試みまで多岐にわたりました*6。発表数が示すように、学生の活躍が目立ってきたのも今回の特徴でした。IIJでは、自社で運用するMITFのハニーポットでの観測データとCCC DATAset2009の攻撃元データを比較し、観測結果の差異について大局的にまとめた結果を発表しています。同じ時期の複数の観測結果を比較することで、事象の局所性や、観測手法の精度の議論につなげられると考えています。

また、今回初の試みとして、課題として与えられたマルウェアの活動記録データを、限られた時間内に解析し、その解析技術を競う MWS Cup 2009 も開催されました。研究成果として作成したツールや、日々業務で利用する解析環境を会場に持ち込み、当日CDで配付される課題データを解析することで、その解析の早さや精度を競いました。初回にもかかわらず7チームが参加し、上位を大学のチームが占めるなど、ここでも学生の活躍が目立ちました。

マルウェア対策研究人材育成ワークショップは、共通のデータを解析することで、研究成果をフェアに比較できる場として有効なことに加えて、将来のマルウェア対策を担う人材の育成の場でもあると考えることができます。また、IIJとしては、普段あまり意見を交える機会がない学術界との交流の場としても非常に有益であり、次回以降も積極的に参加し協力していきたいと考えています。

MWS Cup 2009 会場の様子

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

＊1　マルウェア対策研究人材育成ワークショップ 2009（http://www.iwsec.org/mws/2009/）。情報処理学会コンピュータセキュリティ研究会主催によるコンピュータセキュリティシンポジウムCSS2009(http://www.iwsec.org/css/2009/)と同時開催。MWS2009の会場の様子は、MWS2009活動記録に掲載されている（http://www.iwsec.org/mws/2009/photo.html）。

＊2　IIJでは、昨年開催のMWS2008に続いて参加している。MWS2008（http://www.iwsec.org/mws/2008/）。また、この開催の様子は IIJ.news Vol.90 に対談として掲載している（http://www.iij.ad.jp/news/iijnews/2009/vol90.html）。

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

＊4　共通のデータを基準として研究成果を共有する試みとしては、DARPA Intrusion Detection Data Sets（1998,1999）（http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html）や Knowledge Discovery and Data Mining Tools Competition（http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html）などがある。

＊5　CCC DATAset2008 は、それぞれ、マルウェア検体データ1種類、攻撃通信データ2日分、攻撃元データ半年分のデータであった。

＊6　MWS2009の発表論文やプレゼンテーションは、著者の許諾が得られた範囲で次に公開される（http://www.iwsec.org/mws/2009/）。

Ongoing Innovation

Vol.5 November 2009

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-MKTG019EA-0911KO-08500PR