Internet Infrastructure Review

IIJ
Internet Initiative Japan

Vol.9

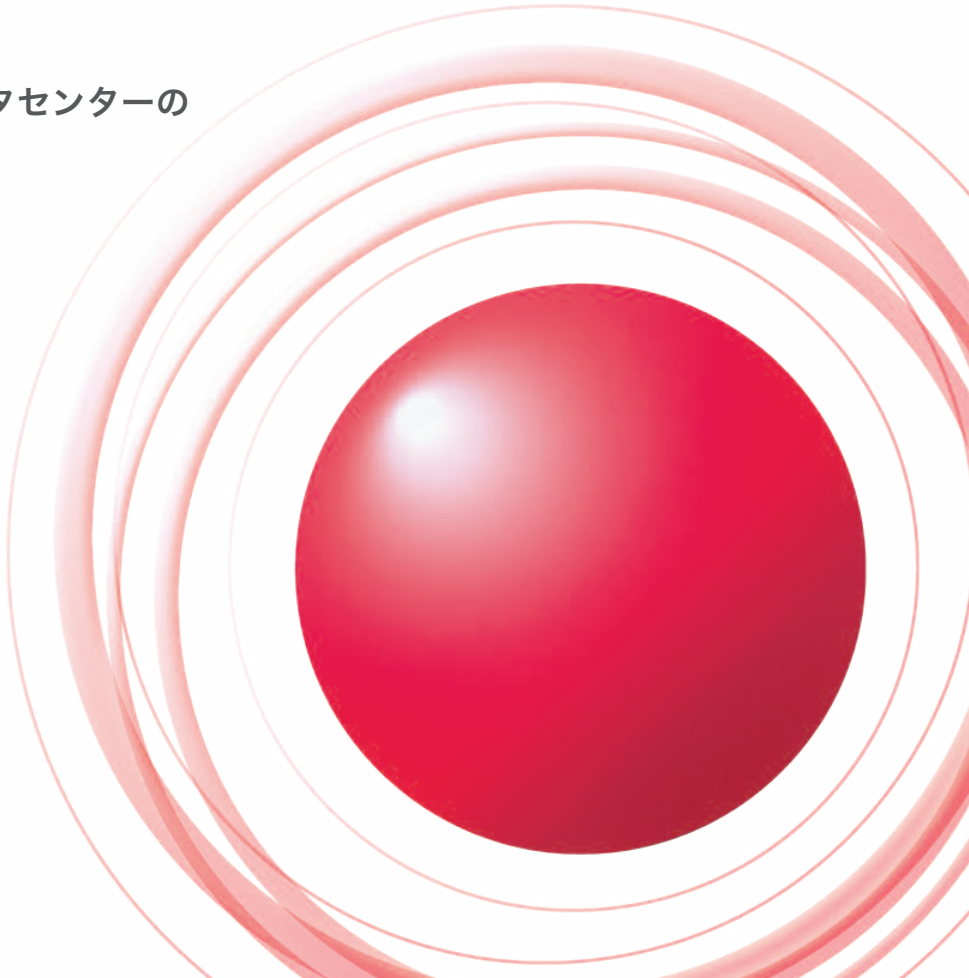
November
2010

インフラストラクチャセキュリティ
DDoS攻撃への備え

インターネットオペレーション
DNSSECの導入にむけて

メッセージングテクノロジー
送信ドメイン認証技術の送信側導入状況はやや停滞

モジュール型エコ・データセンター
次世代モジュール型エコ・データセンターの実証実験報告



Internet Infrastructure Review Vol.9 November 2010

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

エグゼクティブサマリ

ここ数年来のクラウド化の流れは、インターネットを、単なる情報通信のためのオープンでシンプルなネットワークシステムという位置付けから脱皮させ、これまではネットワークの外にあった情報システムやそれにより実現される情報サービスまでネットワークの内側に取り込み、今日の高度情報化社会に関わるさまざまなコンテクストをも呑み込んでしまおうとしているように感じられます。

本年5月に公表された総務省のスマート・クラウド研究会の報告書によると、米国では56.2%の企業がクラウドを利用しているのに対して、日本では14.8%とクラウド利用において日本は遅れを取っているようです。しかし、同報告書では、今後は日本の市場も拡大し、5年後の2015年には国内のクラウドコンピューティング市場は、2010年比で3.2 倍の約2兆4千億円まで膨らむという予想をしています。

このような流れの中で、インターネットというインフラは、もはやネットワークだけのインフラではなくなり、情報システム全般をも内包するインフラとして、今後の発展を考えなければならない時代になってきているのでしょう。

実際に昨年から今年にかけてIIJを始めとする多くの事業者がクラウドサービスを開始し、その上でのビジネスも動き始め、そして、それに必要なシステム、機器、インフラなどの開発や構築も進み始めています。それに伴い、クラウド利用の基盤であるネットワークの安全性や信頼性の確保もますます重要になっています。

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

「インフラストラクチャセキュリティ」の章では、2010年7月から9 月末までの3 ヶ月間を対象として、継続的に実施しているセキュリティインシデントの統計とその解析結果をご報告します。また、対象期間中のフォーカスリサーチとして、小規模システムでのDDoS攻撃への備え、クラウドコンピューティング等の共用システムにおけるセキュリティの検討、そして、デジタルフォレンジックの概要についてご紹介します。

「インターネットオペレーション」の章では、インターネットの利用に必要不可欠なサービスであるDNSの応答が正しいかどうかを検証可能にする、DNSSECという技術の概要と導入時に必要な作業について解説します。

「メッセージングテクノロジー」の章では、2010年6月末から9月末までの13週間の迷惑メールの割合の推移と送信地域の分布、主要迷惑メール送信地域の推移を示します。またメールの技術動向として、送信ドメイン認証技術の導入や、ボットネット対策の状況について、報告を行います。

「モジュール型エコ・データセンター」の章では、IIJが、外気冷却方式のコンテナユニットによる次世代モジュール型エコ・データセンターを開発するために行なった実証実験の、実験システム構成と実験結果について詳しく解説しています。

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

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

DDoS攻撃への備え

今回は、2010年7月から9月に発生したインシデントに関する報告とともに、小規模システムでのDDoS攻撃への備え、クラウドコンピューティング等の共用システムにおけるセキュリティの検討と、デジタルフォレンジックの概要を取り上げます。

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2010年7月から9月までの期間では、前回に引き続きWebブラウザとそのプラグインに関係する複数の脆弱性が悪用されました。また、SIPを悪用して有償の通話を行うことで金銭被害を及ぼす事件が発生したことに続き、9月には社会情勢に応じて日本国内の複数のWebサーバに対する同時多発的な攻撃が発生しました。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

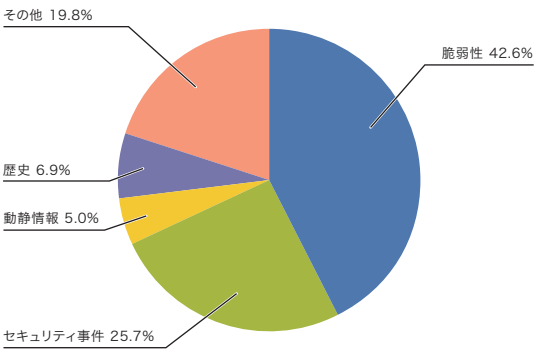


図-1　カテゴリ別比率(2010年7月～9月)

1.2 インシデントサマリー

ここでは、2010年7月から9月までの期間にIIJが取り扱ったインシデントと、その対応を示します。この期間に取り扱ったインシデントの分布を図-1に示します*1。

■ 脆弱性

今回対象とした期間では、マイクロソフト社のWindowsを対象とした脆弱性*2*3*4*5と、アドビ社のAdobe ReaderとAcrobat*6*7、Flash Player*8*9、アップル社のQuickTime*10等のアプリケーションに数多くの脆弱性が発見され、修正されています。これらの脆弱性のいくつかは、対策が公開される前に悪用が確認されました。また、Linux kernelにおいても脆弱性*11が修正されています。さらに、DNSサーバのBIND*12やDHCPサーバであるISC DHCP*13といったサーバアプリケーション、シスコシステムズ社のCisco IOS等のルータ製品でも複数の脆弱性*14*15が修正されています。加えて、携帯電話等のファームウェアとして利用される、アップル社のiOS*16においても脆弱性が修正されています。

■ 動静情報

IIJは、国際情勢や時事に関連する各種動静情報にも注意を払っています。今回対象とした期間では、9月初旬に発生した中国の船舶による海上保安庁の巡視船への衝突行為等に注目しました。

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

＊2　マイクロソフトセキュリティ情報MS10-042-緊急ヘルプとサポートセンターの脆弱性により、リモートでコードが実行される (2229593)（http://www.microsoft.com/japan/technet/security/bulletin/ms10-042.mspx)。

＊3　マイクロソフトセキュリティ情報MS10-046-緊急Windows シェルの脆弱性により、リモートでコードが実行される (2286198)（http://www.microsoft.com/japan/technet/security/bulletin/ms10-046.mspx)。

■ 歴史

この期間には、過去に歴史的背景によるDDoS攻撃やホームページの改ざん事件が発生したことがあります。今回は、9月18日（満州事変の日）に攻撃予告の情報があり、IIJの設備やIIJのお客様のネットワークに対する攻撃行為に注意を払いました。本件に関連した攻撃により、複数の政府官公庁関連組織や、一般の企業、事件とは関係ない団体のWebサイト等に対し、DDoS攻撃や改ざんの試みが発生しました。

■ 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、シーメンス社製の産業用制御システム[*17]を標的として活動を行うマルウェアが発見[*18]されています。また、以前から発生しているSIPの不正な通信の増加が確認[*19]されています。さらに、Twitterにクロスサイトスクリプティング脆弱性[*20]が発見され、悪用[*21]されたり、広告配信サーバの脆弱性を悪用し、一部のデータを改ざんしてスケアウェアへ誘導する事件[*22]も発生しています。

■ その他

その他セキュリティに関係する動向としては、DNSSECの導入に関して、DNSの最上位階層であるルートゾーンへの署名が実施[*23]され、日本でも2011年1月にJPドメイン名サービスにおけるDNSSECを導入することが発表[*24]されました。また、TLSのrenegotiation機能に関係するプロトコルの脆弱性に伴って規定されたRFC5746を実装した修正プログラム[*25]が、マイクロソフト社から提供されました。さらに、9月には毎日未修正の脆弱性を発表する試みが行われ、実際に多くの脆弱性情報が公開されました[*26]。

＊4　マイクロソフトセキュリティ アドバイザリ（2269637）安全でないライブラリのロードにより、リモートでコードが実行される（http://www.microsoft.com/japan/technet/security/advisory/2269637.mspx）。
＊5　マイクロソフトセキュリティ情報MS10-070-重要ASP.NETの脆弱性により、情報漏えいが起こる（2418042）（http://www.microsoft.com/japan/technet/security/bulletin/ms10-070.mspx）。
＊6　APSB10-17 Adobe ReaderとAcrobatに関するセキュリティ情報（http://www.adobe.com/jp/support/security/bulletins/apsb10-17.html）。
＊7　APSB10-21 Acrobatおよび Adobe Readerセキュリティアップデーターの公開（http://kb2.adobe.com/jp/cps/871/cpsid_87135.html）。
＊8　APSB10-16 Flash Player用セキュリティアップデート公開（http://www.adobe.com/jp/support/security/bulletins/apsb10-16.html）。
＊9　APSB10-22 Flash Playerに関するセキュリティアップデート公開（http://www.adobe.com/jp/support/security/bulletins/apsb10-22.html）。
＊10 QuickTime 7.6.7のセキュリティコンテンツについて（http://support.apple.com/kb/HT4290?viewlocale=ja_JP）。
＊11 JVNDB-2010-002118 64-bitプラットフォーム上で稼働しているLinux kernelのcompat_alloc_user_space関数における権限昇格の脆弱性（http://jvndb.jvn.jp/ja/contents/2010/JVNDB-2010-002118.html）。
＊12 RRSIG query handling bug in BIND 9.7.1（http://www.isc.org/software/bind/advisories/cve-2010-0213）。
＊13 DHCP: Fencepost error on zero-length client identifier（http://www.isc.org/software/dhcp/advisories/cve-2010-2156）。
＊14 Cisco Security Advisory: Cisco IOS XR Software Border Gateway Protocol Vulnerability（http://www.cisco.com/JP/support/public/ht/security/109/1091094/cisco-sa-20100827-bgp-j.shtml）。
＊15 Cisco Security Advisory: Summary of Cisco IOS Software Bundled Advisories, September 22, 2010（http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml）。
＊16 iPhoneおよびiPod touch用のiOS 4.1のセキュリティコンテンツについて（http://support.apple.com/kb/HT4334?viewlocale=ja_JP）。
＊17 SCADA: Supervisory Control And Data Acquisitionの一種。コンピュータによるシステム監視とプロセス制御を行う監視制御システムで、主に工場等で利用されている。
＊18 このマルウェアに関する詳細報告は複数あるが、例えば次は日本シーサート協議会による解説。マルウェア Stuxnet（スタクスネット）について（http://www.nca.gr.jp/2010/stuxnet/index.html）。
＊19 不正なSIP着信 24（http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=%C9%D4%C0%B5%A4%CASIP%C3%E5%BF%AE+24）。cNotesでは不定期にSIPに関する観測情報が提供されている。
＊20 この脆弱性については次の公式blogに詳しい。Twitterブログ「マウスオーバーの」問題についての全容（http://blog.twitter.jp/2010/09/blog-post_22.html）。
＊21 この件についての詳細は次のエフセキュアブログに詳しい。「Twitter.com」に放たれたワーム（http://blog.f-secure.jp/archives/50446597.html）。
＊22 この事件については次のトレンドマイクロ株式会社の Blogでも紹介されている。Adobe製品へのゼロデイ攻撃、広告配信システムを通じた「Webからの脅威」－2010年9月の脅威動向を振り返る（http://blog.trendmicro.co.jp/archives/3700）。
＊23 ルートゾーンへの署名導入に関する報告（http://www.root-dnssec.org/2010/07/16/status-update-2010-07-16/）。
＊24 JPRSによるサービス案内JPドメイン名サービスへのDNSSECの導入予定について（http://jprs.jp/info/notice/20090709-dnssec.html）。
＊25 TLS renegotiation機能に関する修正は次の更新プログラムに含まれている。マイクロソフト セキュリティ情報 MS10-049-緊急SChannelの脆弱性により、リモートでコードが実行される（980436）（http://www.microsoft.com/japan/technet/security/bulletin/ms10-049.mspx）。この問題に関しては本レポートVol.6（http://www.iij.ad.jp/development/iir/pdf/iir_vol06.pdf）の「1.4.2 SSL及びTLSのrenegotiation機能の脆弱性を利用した中間者攻撃」にて解説している。
＊26 MOAUB (Month of Abysssec Undisclosed Bugs)。この試みで発表された脆弱性については次のAbysssec Security Research blogにまとめられている。MOAUB - Day by Day(http://www.abysssec.com/blog/2010/09/moaub-1/)。

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攻撃と、ネットワーク上でのマルウェアの感染活動、Webサーバに対するSQLインジェクション攻撃の実態について、その調査と分析の結果を示します。

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生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。しかし、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。

■ 直接観測による状況

図-2に、2010年7月から9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。

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。

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模（回線容量やサーバの性能）によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*27]、サーバに対する攻撃[*28]、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つに分類しています。

この3ヵ月間でIIJは、622件のDDoS攻撃に対処しました。1日あたりの対処件数は6.76件で、平均発生件数は前回のレポート期間に比べて3倍に増加しました。DDoS攻撃全体に占める割合は、回線容量に対する攻撃が1%、サーバに対する攻撃が72%、複合攻撃が27%でした。これは、9月10日から9月30日までの期間に、複数のWebサーバへの攻撃数が大幅に増加したためで、この3週間に発生した攻撃は全体の46%を占めています。

今回の対象期間で観測された最も大規模な攻撃は、回線容量に対する攻撃に分類したもので、最大27万5千ppsのパケットによって1.4Gbpsの通信量を発生させるものでした。また、攻撃の継続時間は、全体の66%が攻撃開始から30分未満で終了し、20%が30分以上24時間未満の範囲に分布しています。最も長く継続した攻撃は12日間（291時間）にわたり、最大で12万ppsのパケットにより670Mbpsの通信量を発生させた複合攻撃でした。

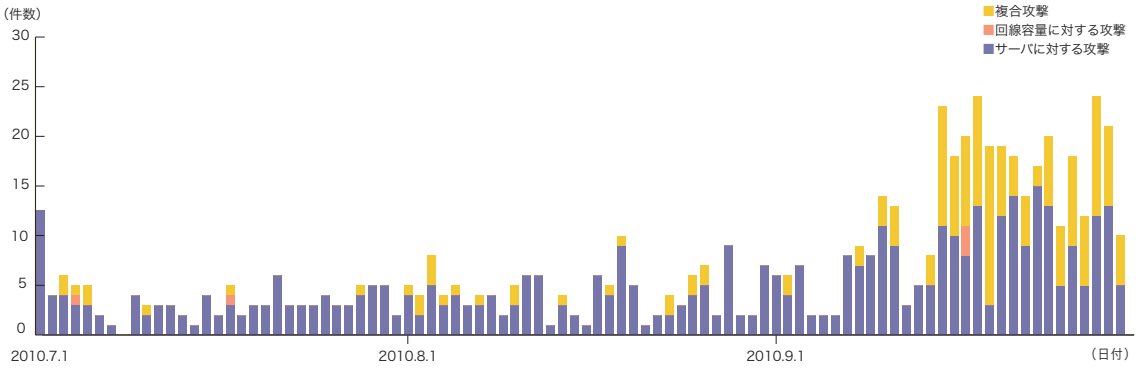


図-2 DDoS攻撃の発生件数

＊27 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。

＊28 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。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング[*29]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[*30]の利用によるものと考えられます。

■ backscatterによる観測

次に、IIJでのマルウェア活動観測プロジェクトMITFのハニーポット[*31]によるDDoS backscatter観測の結果を示します[*32]。backscatterを観測することで、外部のネットワークで発生したDDoS攻撃の一部を、それに介在することなく第三者として検知できます。

2010年7月から9月の期間中に観測されたbackscatterについて、ポート別のパケット数推移を図-3に、発信元IPアドレスの国別分類を図-4に示します。

観測されたDDoS攻撃の対象ポートのうち最も多かったものは、Webサービスで利用される80/TCPで、全期間における全パケット数の58.4%を占めています。また、リモートデスクトップで利用される3389/TCPへの攻撃も観測されています。これらに加えて、5218/TCP、5224/TCP等、一般的なアプリケーションで利用されないポートも多く観測されました。図-4で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、中国の44.8%と米国の29.5%が比較的大きな割合を占めており、日本国内のIPアドレスも2.1%を占めていました。また、特に多数のbackscatterパケットが観測された、8月20日の5224/TCPと9月19日の5218/TCPを対象ポートとするパケットは、すべて中国の同一IPアドレスが攻撃対象となっています。

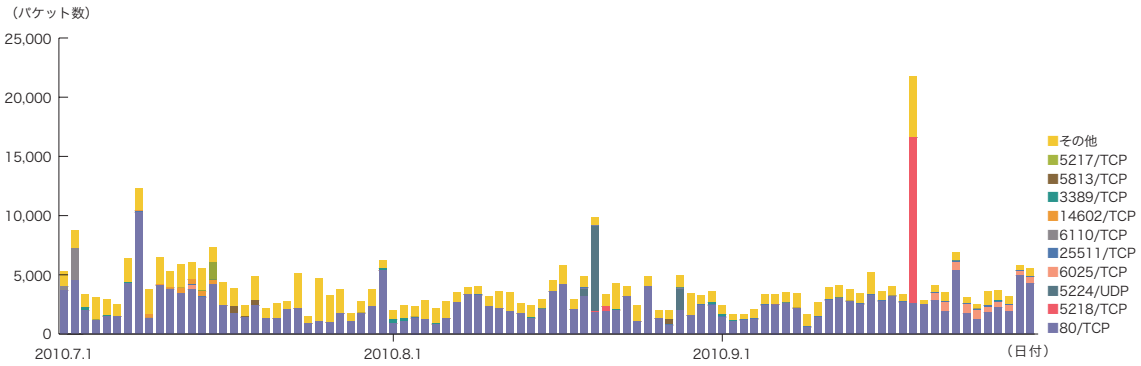


図-3　DDoS攻撃によるbackscatter観測（観測パケット数、ポート別推移）

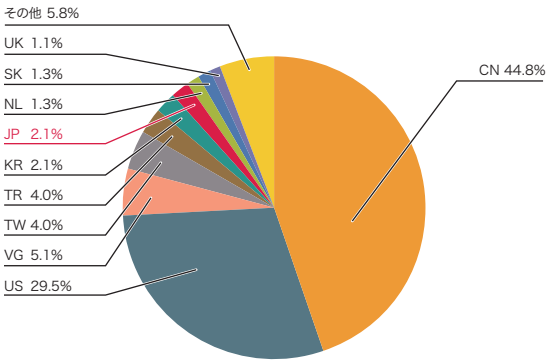


図-4　backscatter観測によるDDoS攻撃対象の分布（国別分類、全期間）

＊29 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。

＊30 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。

＊31 IIJのマルウェア活動観測プロジェクトMITFが設置しているハニーポット。「1.3.2 マルウェアの活動」も参照。

＊32 この観測手法については、本レポートのVol.8（http://www.iij.ad.jp/development/iir/pdf/iir_vol08.pdf）の「1.4.2 DDoS攻撃によるbackscatterの観測」で仕組みとその限界、IIJによる観測結果の一部について紹介している。

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[*33]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[*34]を利用して、インターネットから到着する通信を観測しています。そのほとんどがマルウェアによる無作為に宛先を選んだ通信か、攻撃先を見つけるための探索の試みであると考えられます。

■ 無作為通信の状況

2010年7月から9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-5に、その発信元IPアドレスの国別分類を図-6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、同社のSQL Serverで利用される1433/TCPや、telnetで利用される23/TCPに対する探索行為も観測されています。これらに加えて、5121/TCP、31795/TCP、23502/TCP、9415/TCP等、一般的なアプリケーションでは利用されない目的不明な通信も観測されました。 図-6で発信元の国別分類を見ると、日本国内の30.4%、中国の15.9 %、台湾の6.0%が比較的大きな割合を占めています。

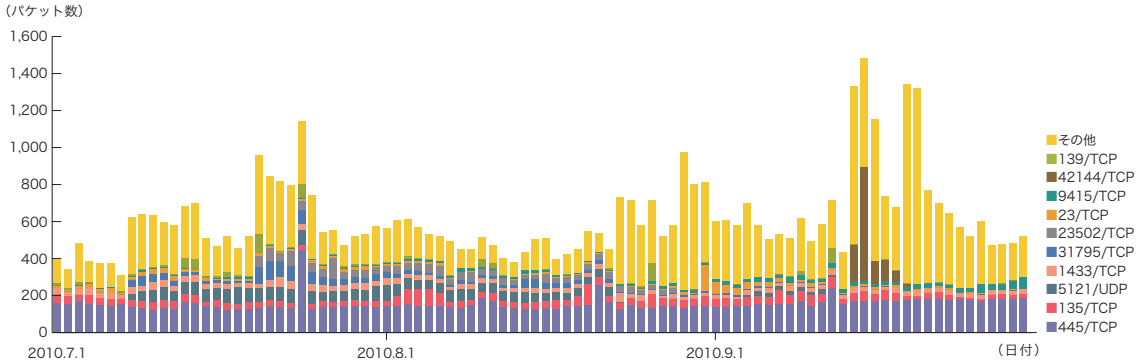


図-5　ハニーポットに到着した通信の推移（日別・宛先ポート別・一台あたり）

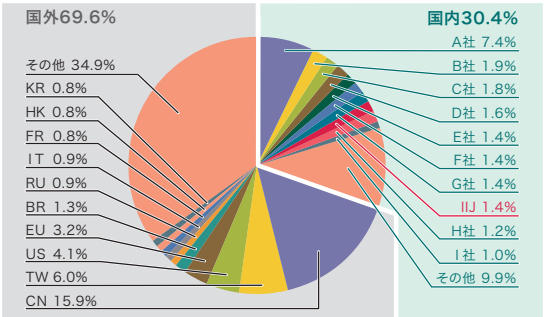


図-6　発信元の分布（国別分類、全期間）

＊33 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。

＊34 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-7に、マルウェアの検体取得元の分布を図-8にそれぞれ示します。図-7では、1日あたりに取得した検体[*35]の総数を総取得検体数、検体の種類をハッシュ値[*36]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371、ユニーク検体数が41です。前回の集計期間では、平均値が総取得検体数で378、ユニーク検体数で32でした。今回は、総取得検体数に減少傾向が見られますが、検体の種類を表すユニーク検体数が前回より増加傾向にあります。総検体取得数が9月19日以後急激に減少しているのは、世界中でSdbotとその亜種の活動が見られなくなったことによります。このSdbotの活動停止の原因は不明です。

図-8に示す検体取得元の分布では、日本国内が38.7%、国外が61.3%でした。なお、台湾が47.8%と前回に引き続き大きな割合を占めています。これは、台湾においてSdbotとその亜種の活動が活発であったためですが、他の国の状況と同様に9月19日以後は活動が見られなくなっています。

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。今回の調査期間に取得した検体は、ワーム型14.0%、ボット型84.8%、ダウンローダ型1.2%でした。また、解析により、26個のボットネットC&Cサーバ[*37]と276個のマルウェア配布サイトの存在を確認しました。今回、マルウェア配布サイトの検出数が大幅に増加していますが、これは前回減少傾向が見られた複数の配布サイトにアクセスする検体が増加したためでした。

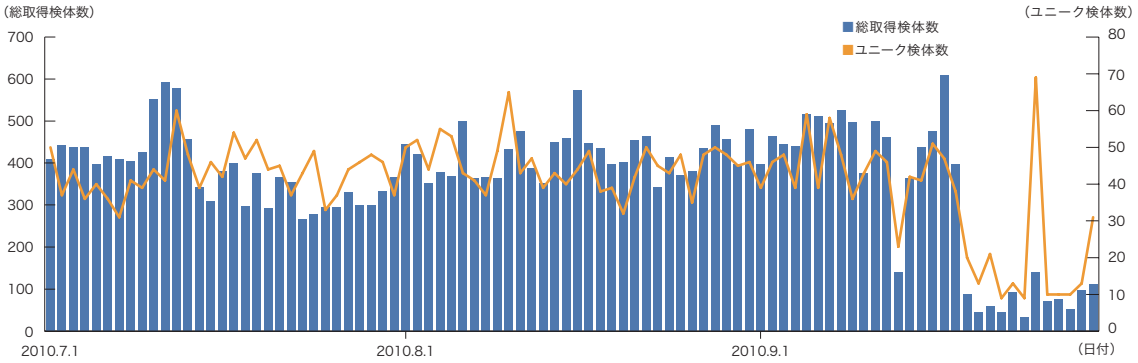


図-7　取得検体数の推移(総数、ユニーク検体数)

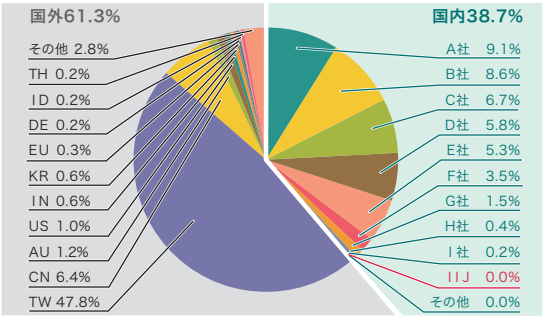


図-8　検体取得元の分布(国別分類、全期間)

＊35 ここでは、ハニーポット等で取得したマルウェアを指す。

＊36 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。

＊37 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*38について継続して調査を行っています。SQLインジェクション攻撃は、過去にもたびたび流行し話題になった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

2010年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-9に、攻撃の発信元の分布を図-10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40.0%、中国36.7%、米国7.1%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、前回からあまり変化が見受けられませんでした。しかし、9月30日に主に中国から特定の攻撃先に対しSQLサーバに侵入を試みる攻撃があったため、全体に対して中国からの攻撃が占める割合が増加しています。

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

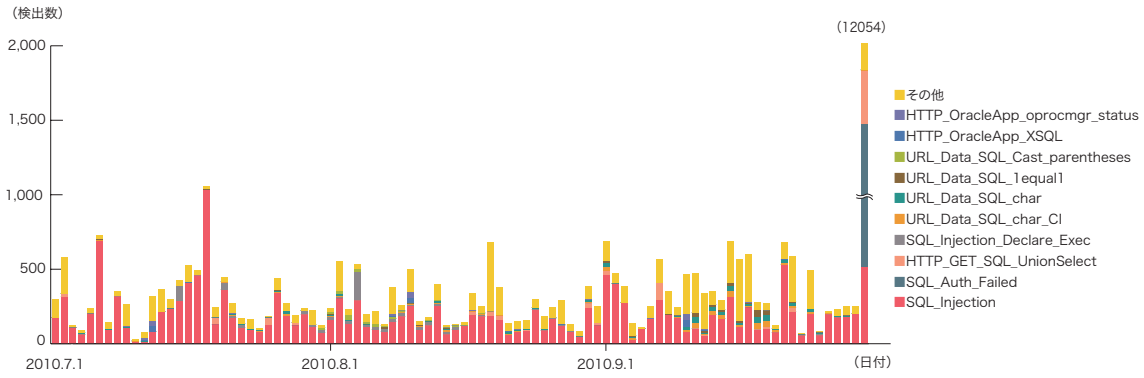


図-9　SQLインジェクション攻撃の推移(日別、攻撃種類別)

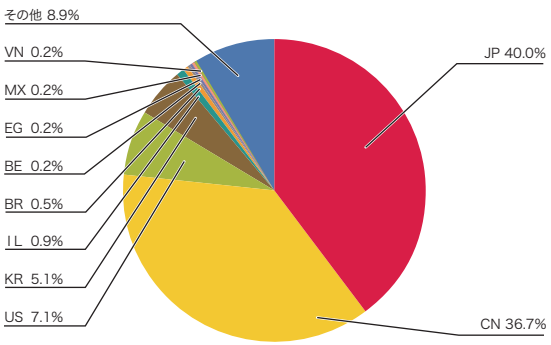


図-10 インジェクション攻撃の発信元の分布(国別分類、全期間)

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

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、小規模システムでのDDoS攻撃への備え、共用システムにおけるセキュリティ、デジタルフォレンジックの概要を示します。

1.4.1 小規模システムでのDDoS攻撃への備え

「1.3.1 DDoS攻撃」に示した通り、本レポートの対象期間の9月に複数のWebサーバへのDDoS攻撃が発生しました。この攻撃では、日本の官公庁に加えて民間企業のWebサーバ等も攻撃対象になりました。この事件に限らず、DDoS攻撃は攻撃対象のサーバの所有者に対する抗議や自己主張の一つとして行われます。また近年では、DDoS攻撃を行いながら金銭を要求する恐喝事例なども発生しています。現在のDDoS攻撃には、専用の攻撃ツールやボットネット等が利用され、攻撃自体を代行する者も存在しています。つまり、攻撃の意図を持つ者に知識や技術がなくても比較的容易に攻撃が行える状態になっています。このため、インターネット上に公開しているサーバは、その規模の大小にかかわらず、DDoS攻撃の対象となる可能性があります。ここでは、特に小規模システムでのDDoS攻撃への備えについて検討していきます。

DDoS攻撃には、サーバ自体を直接過負荷にする攻撃と、サーバが利用している回線を通信で埋めつくす攻撃の2つがあります。しかし、どちらの攻撃も、インターネットに接続しているサーバが突然利用できなくなることに変わりはありません。攻撃発生時に有効となる対策を検討するためには、サーバの重要度に基づく対策方針の策定、サーバの耐性向上、異常検出の仕組みの構築、他組織への協力要請等の準備が必要です。

■ 対策方針の策定

DDoS攻撃を受けた場合、サーバはその役割を果たすことができなくなります（可用性に対する脅威）。このため、検討対象のサーバが停止したときに、業務にどのような影響があるかを明らかにします。その上で、サーバの機能の回復目標を定めます。例えば、全面停止していても問題のないシステムなのか、通信できる範囲を特定の領域（日本国内や業務上の提携相手のみ等）に限定しても構わないのか、通信の品質を下げて（特定のアドレスからの接続数を制限したり、全体に帯域制御をかけたりして）も問題にならないか、といったことを検討します。どうしても可用性が求められるサーバについては、専用のDDoS対策装置の導入や対策サービスの利用を検討します。

■ サーバの耐性向上

DDoS攻撃を受けたときには、回線が通信で埋めつくされたり、サーバが過負荷状態に陥ったりします。このため、無防備なサーバでは、通信状況を確認したり、サーバの動作状況を確認したりすることさえ困難になります。サーバの導入時には、通常の業務で要求される処理能力を検討し、その状態に対してある程度の余裕を持たせることが必要です。あわせて、サーバのOSやアプリケーションでのDDoS対策や資源管理のオプションの導入を検討しておくことも大切です。例えば、

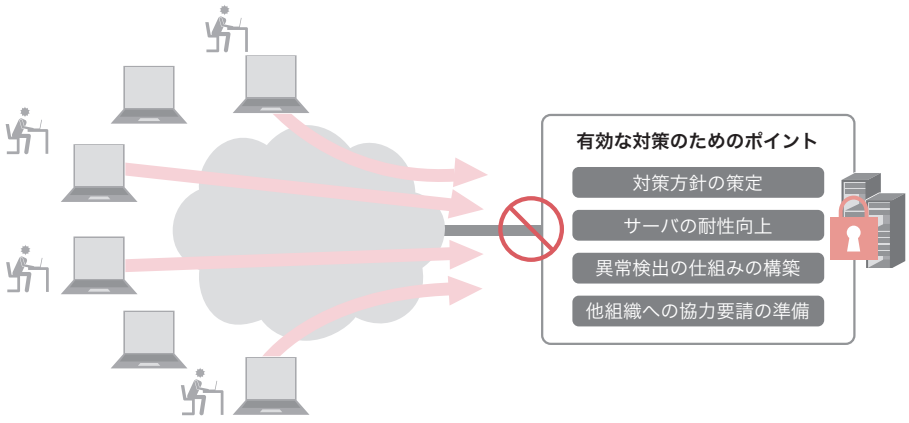


図-11 DDoS攻撃に対する準備

Linuxには、SYN flood攻撃を防御するSYN cookiesの機能[*39]や、アプリケーションごとに接続数を制限する機能[*40]等が搭載されています。HTTPサーバのApacheでも、設定[*41]や各種外部モジュール[*42]を追加することで、同時接続数等を制限する機能が利用できます。このようにハードウェアの性能と、OSやアプリケーションの機能を組み合わせることで、DDoS攻撃に対するサーバの耐性をより強固にすることができます。

■ 異常検出の仕組みの構築

DDoS攻撃を受けた場合に状況を把握しようとしても、日常的に適切なログを取得していなかったり、膨大な量のログを扱わなければならなかったりするため、解析を終えるまでに非常に長い時間がかかる場合があります。このため、日頃から適切なログの記録と通常の通信状態の把握を行い、突発的に発生するDDoS攻撃を異常として検知する仕組みを備えておくことが重要です。また、サーバのログだけではなく、SNMPやNetflow等により通信に関する情報も参照できるようしておくことで、より状況を把握しやすくなります。さらに、大量のログを取り扱うための準備も必要です。例えば、Webサーバとは別にログサーバを用意しておくことで、Webサーバが過負荷な状況でも記録を分析することができます。また、事前に大量のログから概要情報を抽出するスクリプト等を準備しておくことで、異常を検知した時に短時間で状況を把握できます。

■ 他組織への協力要請の準備

回線を通信で埋めつくしたりIPアドレスを詐称したりする攻撃では、攻撃を受けたサーバだけで対処できず、ISP、セキュリティベンダ、CSIRT等の外部組織に対処の協力要請を行うことが必要となる場合があります。この際には、すでに把握している状況を開示することが必要です。また、多くの場合、協力を要請した組織だけでは対策が行えず、攻撃に関する情報を他の組織（攻撃者を収容するISP等）と共有する許可を与える必要もあります。IPアドレス、攻撃の内容、通信の様子等、攻撃に関する個々の情報の開示の可否を事前に定めておくことで、他組織が迅速に対策活動を行えるようになります。このような情報については、JPCERT/CCのインシデント報告フォーム[*43]等が参考になります。

■ まとめ

ここでは、小規模システムを対象にして、DDoS攻撃を受ける前に備えておくべき事柄について説明しました。「1.3.1 DDoS攻撃」のbackscatter観測で示しているように、現在ではWebサーバ以外のサーバに対するDDoS攻撃も観測されており、あらゆるサーバで突然のDDoS攻撃に備えておく必要があります。また、DDoS攻撃は、攻撃者の意図が強く表れるものであり、その発生をある程度予見できます。このために、世間の動向や、所属する組織に関する情報等の自社のかかわるニュースにも注目し、諍いの前兆を早期に発見することも、DDoS攻撃への備えとして役立ちます[*44]。

1.4.2 共用システムにおけるセキュリティ

現在、クラウドコンピューティング（以下、クラウド）の本格的な利用が活発化しています。クラウドでは、さまざまなシステム資源を共用することで、それらを低コストで利用できる反面、共用システム特有のセキュリティに関する問題が懸念されています。ここでは、システム資源の共用から生じるクラウドでの脅威とその対策を検討します。

■ 共用資源における問題

マルチテナントでシステム資源を共用するクラウドでは、利用者間の資源の分離はソフトウェア等により論理的に行われます。このため、論理的な資源の分離が

＊39 SYN cookiesについての詳細は考案者であるダニエル・J・バーンスタインによるSYN cookiesの解説（http://cr.yp.to/syncookies.html）を参照のこと。また、IETFからSYN flood 攻撃についての攻撃原理と対策技術の概要をまとめた文書としてRFC4987 TCP SYN Flooding Attacks and Common Mitigations（http://www.ietf.org/rfc/rfc4987.txt）が発行されている。

＊40 iptablesではlimitやconnlimit等のモジュールが用意されている。例えばiptablesでlimitを利用しsynパケットに制限を加えることでアプリケーションが処理可能な新規接続数を絞るといった設定ができる。

＊41 例えば、MaxClientsの設定で同時接続数に制限を行える。これ以外にもTimeout、KeepAlive、KeepAliveTimeout、MaxKeepAliveRequests等がありこれらの設定を調整することで攻撃によるリソースの消費を抑制することができる。

＊42 Apacheには多くの外部モジュールが用意されており、例えば、mod_limitipconn（http://dominia.org/djao/limitipconn2.html）では1つのIPアドレスからの同時接続数を制限することができる。

＊43 詳細については次のJPCERTコーディネーションセンターのインシデントの報告（http://www.jpcert.or.jp/form/）を参照のこと。

＊44 その他、DDoS対策で参考となる情報としては例えば、VeriSign, Inc.：DDoS Mitigation - Best Practices for a Rapidly Changing Threat Landscape Whitepaper(要ユーザ登録)（http://www.verisign.com/forms/ddosbestpracticeswp.html?toc=MYUM9-0000-02-00）等がある。

適切であることが大変重要であり、分離している境界が破られることは利用者にとってセキュリティ上の脅威になります。では、実際にどのような脅威が考えられるでしょうか。CSA (Cloud Security Alliance) [*45] は“Top Threats to Cloud Computing V1.0” [*46] において、クラウドの代表的な脅威として7つの項目を挙げています。この7項目の中には、“Shared Technology Issues”という項目があり、CPUやGPUといった共用資源の論理的な分離や分割での違反の事例と影響が紹介されています。また、CSAのレポート以外にも、クラウド特有の脅威として、共有資源の問題が多くのレポートで取り上げられています。さらに、クラウドでは、通信回線や通信機器、ストレージといった資源も共用されるため、これらについても考えなければなりません。ここでは、クラウドのシステム構成を考慮しながら具体的な脅威について考えていきます。

■ クラウドのインフラストラクチャ構成

一般的に、クラウドの構成は公開されていません。このため、ここでは汎用的な機器で構成されているものと仮定し、図-12のような機器で構成されたクラウドシステムを例にクラウドの脅威を考えていきます。

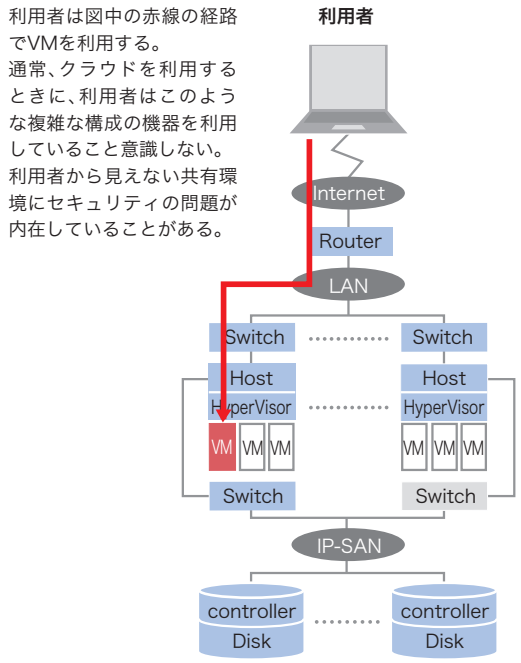


図-12 クラウドのシステム構成例

このクラウドはルータ等を使ってインターネットと接続しています。利用者はインターネットを通じてクラウド上の仮想マシン (VM) にアクセスします (図-12の赤い矢印)。仮想マシンが稼動している物理マシンには他の利用者の仮想マシンが同居しており、物理的な資源を共用しています。物理マシンはサービス提供のために複数のイーサネットポートをもち、インターネット側へのサービス提供や、イーサネットを使ったストレージネットワーク (IP-SAN) に接続されて、ストレージサービスを提供しています。

■ クラウド環境での脅威とその対策

ネットワークの共用は、クラウドだけに限られた話でなく、インターネット自体や、従来からのレンタルサーバ環境でも、複数の利用者がネットワークを共用しているという点で同一です。しかし、クラウドでは、異なるセキュリティポリシーの仮想マシンが同一のL2セグメント上に存在する可能性があります。仮想マシンが不正侵入によって乗っ取られ、ARP poisoning[*47]等により通信の阻害や盗聴が発生する危険性があります。このような脅威への対策として、ハイパーバイザーや、接続先のスイッチでVLAN ID、MAC Address等の詐称対策等を行うことが必要です。

また、クラウドでは、ストレージも仮想化され共用されます。IP-SAN (iSCSI) 等を利用している場合、イーサネットを使ってストレージが接続されるため、人為的に偽のイーサネットフレームを生成することでストレージネットワークを攻撃できます。仮想マシンから到達可能なネットワーク上にストレージのコントローラが存在する場合には、コントローラへの攻撃も可能です。また、ストレージ仮想化のためのID (IQN[*48]) が詐取されたときには、それによって本来は分離されていて、見えないはずのデータ領域が見えてしまったり

＊45 CSA(Cloud Security Alliance)。2008年にクラウドセキュリティのベストプラクティスを広めるために設立された団体(http://www.cloudsecurityalliance.org/)。2010年6月には日本支部として、日本クラウドセキュリティアライアンスが発足している(http://www.cloudsecurityalliance.jp/)。
＊46 “Top Threats to Cloud Computing V1.0”はCSAがクラウドコンピューティングへの代表的な脅威と対策をまとめて文書化したもの(http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf)。
＊47 ARP poisoningとはネットワーク上に偽のARPパケットを流すことにより、別のホストの通信を横取りする攻撃。
＊48 iSCSI Qualified Nameの略。ネットワーク上でiSCSIノードを識別するための名前。

接続できてしまったりする危険性があります。このような脅威への対策として、ネットワークと同様にハイパーバイザーやスイッチでのアクセス制御や詐称対策が必要となります。

さらに、ファイアウォール等の基本機能がサービスとして提供されている場合には、その提供形態によって脅威が変化します。図-13にファイアウォールの構成例を示します。パターン1は、ハイパーバイザーの一機能としてファイアウォールを提供する方法です。この場合、ファイアウォールの安全性は、事業者によって担保されます。パターン2は、利用者に提供される仮想マシンと同じように、ハイパーバイザー上にOSを載せ、ソフトウェアでファイアウォール機能を実現しています。この場合、ハイパーバイザーに脆弱性が存在していると、ファイアウォールもその影響を受けます。パターン3は、専用機器を用意し、VLANやルーティングでネットワークトラフィックを中継させる方法です。この方法は、従来のものと同じですが、コストがかかります。パターン4は、利用者のOS上に実装する方法ですが、不正侵入者によって設定が変更されてしまう危険性があります。パターン5は、Webやメールで用いられることが多い方法で、アプリケーションのproxy機能をSaaSとして利用する方法です。異なる事業者によってサービスが提供されているときには、サービス間の統制は利用者の責任になります。このように、提供形態によって考慮すべき点が異なることをあらかじめ認識しておく必要があります。

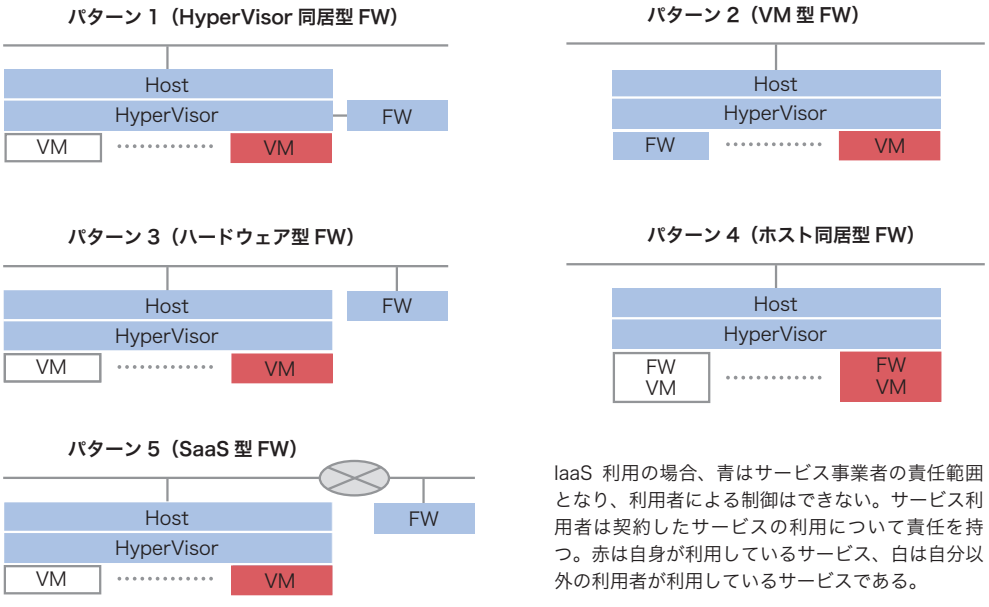
■ まとめ

ここで説明してきた事項は、目新しいものではなく、本来は事業者がそれぞれの脅威を認識して対策を行っていれば、問題になることはありません。

安全性を確認するために利用者自らが内部構成を意識することは有益ですが、サービス利用ではそのような情報が開示されないことも多々あります。利用者は、利用するサービスにおける利用者自身の責任範囲を見極めて必要な対策を行うことに加えて、事業者との間でセキュリティ対策に関する合意を形成していくことが、クラウドの利用において重要です。

1.4.3 デジタルフォレンジックの概要

ITが普及するに伴い、企業や個人が保持する情報の多くがデジタルデータとして保存され、蓄積されるようになっています。また、これによって、デジタルデータが事件の対応や裁判の証拠等に利用されるケースも増えています。デジタルデータは、紙媒体に比べると容易に変更したり消去したりできるため、それを調べる人には適切な技術が求められます。ここでは、デジタルデータの調査技術であるデジタルフォレンジックについて説明します。



IaaS 利用の場合、青はサービス事業者の責任範囲となり、利用者による制御はできない。サービス利用者は契約したサービスの利用について責任を持つ。赤は自身が利用しているサービス、白は自分以外の利用者が利用しているサービスである。

図-13 ファイアウォールの構成例

デジタルフォレンジックは、不正アクセス等を調査するインシデントレスポンス時や、訴訟における電子データの提出時等に、主に企業内で使われる技術[*49]です。解析対象の観点からデジタルフォレンジックを分類すると、コンピュータを対象にしたコンピュータフォレンジック、ネットワークを流れるパケットを対象にしたネットワークフォレンジック[*50]、携帯電話等のモバイル端末を対象としたモバイルデバイスフォレンジック[*51]等に分かれます。

また、デジタルフォレンジックの実施順序は、保全、解析、報告の3つのステップになります。デジタルフォレンジックでは、オリジナルのデジタルデータを使って解析することは、一部の例外を除いて基本的にありません。デジタルフォレンジックを実施するエンジニアは、最初に対象のデータを保全（複製、取得ともいう）する作業を実施します。次に、保全したデータを、そのデータに対応したツールで解析し、インシデント発生時の一連のイベントを可視化して再構築します。最後に、解析結果のデータを元に判明した事実を報告としてまとめます。

■ コンピュータフォレンジック

次に、実施頻度が高いコンピュータフォレンジックの保全と解析について説明します。

コンピュータは、CPUやメモリ、ハードディスク等によって構成されています。ハードディスクやCD-ROMに残っているデータは、コンピュータの電源を落としても消えることがない不揮発性のデータです。これに対して、CPUやメモリ上のデータは、電源を落とすと消えてしまう揮発性のデータです。 RFC3227 “Guidelines for Evidence Collection and Archiving”[*52]では、保全を実施する際には「揮発性の高いデータから順に保全する」ように推奨されています。したがって、調査対象のコンピュータがサーバであり、オンライン状態（電源が入っていて動いている状態）であったときには、まずメモリ上にあるデータ等の揮発性データを保全し、その後にディスクやその他のバックアップメディアを保全することが望ましいと言えます。

揮発性データの収集方法には、対象マシン上で揮発性データ収集ツールキットを実行する方法と、メモ

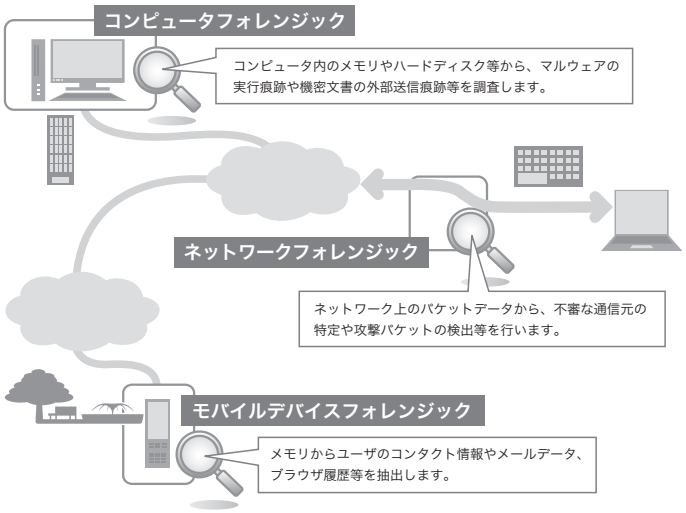


図-14 フォレンジックの概要

＊49 特定非営利活動法人のデジタル・フォレンジック研究会は、デジタルフォレンジックを「インシデントレスポンスや法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」としている（http://www.digitalforensic.jp/wdfitm/wdf.html）。

＊50 遠隔から対象のコンピュータを調査・分析する手法をネットワークフォレンジックと呼ぶ場合もある。

＊51 モバイルデバイスフォレンジックについては、欧米で利用されているフォレンジックツールが日本の携帯電話の規格に対応していないため、法執行機関を除いて実施されることはほとんどなかったが、最近では徐々に増えてきたスマートフォンを対象としたツールを国内でも利用できるようになってきた。例えば、Oxygen Software社のモバイルデバイス解析ツールOxygen Forensic Suiteは、サイバーディフェンス研究所で取り扱っている（http://www.cyberdefense.jp/company_profile/prerelse10001.html）。

＊52 RFC3227 "Guidelines for Evidence Collection and Archiving" (http://www.ietf.org/rfc/rfc3227.txt)では、セキュリティインシデント発生時の証拠の収集手順や注意点を述べている。日本語訳にはIPAによる「証拠収集とアーカイビングのためのガイドライン」（http://www.ipa.go.jp/security/rfc/RFC3227JA.html）等がある。

リイメージを取得した後に解析する方法の2つがあります。例えば、揮発性データ収集ツールキットとしてはSysinternals Suite[*53]があります。このツール群は、対象のマシン上で実行され、その結果をテキストファイル等に出力します。一方、メモリイメージは、メモリの内容をそのままダンプしたバイナリファイルのことです。メモリイメージの取得には、対象のマシン上でメモリの内容をダンプするツールの実行だけを行い、その後にそのメモリイメージを別のマシンに移動して解析し、揮発性の情報を抽出します。メモリイメージの取得は、必ず揮発性データ収集ツールキットの実行よりも前に実施します[*54]。

不揮発性データの取得方法には、オンライン状態での保全とオフライン状態（電源を落とした状態）での保全の2つがあります。また、保存データの形式には、物理ディスク単位で保全する物理ディスクイメージや、論理ボリューム単位で保全する論理ディスクイメージ等があります。基本的に、不揮発性データはオフライン状態で保全します。ただし、ディスクが暗号化されていたりRAID構成が設定されていたりして、論理ボリュームで保全したほうが都合のよいときには、オンライン状態で保全することもあります。また、保全したデータは、保全後のデータの完全性を保証するために、保全時のハッシュ値を計算しておきます。これによって、保全後のデータが変更されたり改ざんされたりしても、それを検出できます。

保全した揮発性データを解析することで、ログオンしていたユーザの情報、実行中のプロセスの通信状態や開始時刻、プロセスがオープンしていたファイルや読み込んでいた共有ライブラリ、ARPテーブル、ルーティングテーブル、DNSキャッシュの情報等を得ることができます。また、メモリイメージファイルを解析することで、過去に実行されたプロセスの情報やすでにクローズした通信の情報等も得られる場合があります。

不揮発性データの解析で得られる結果は多岐にわたります。不正侵入時やマルウェア感染時には、関係する実行ファイルやログが隠ぺい目的によって削除されてしまうことが多いため、削除ファイルの復元を行ったり未使用領域内にあるログの断片を調べたりします。また、システムログやイベントログ、レジストリ等からインシデントに関係する操作やファイルを検出できれば、操作が行われた時刻や該当するファイルのタイムスタンプ（作成時刻や修正時刻等の情報）に近い別のイベントを調べていくことで、インシデント発生時期や被害範囲を推定することもできます。

さらに、揮発性か不揮発性にかかわらず保全したデータ内をキーワード検索することで、外部へのデータ送信痕跡を確認したり他システムへのアクセス有無を確認したりできます[*55]。

■ デジタルフォレンジックの課題

このようなデジタルフォレンジックにおける課題には、次のようなものがあります。

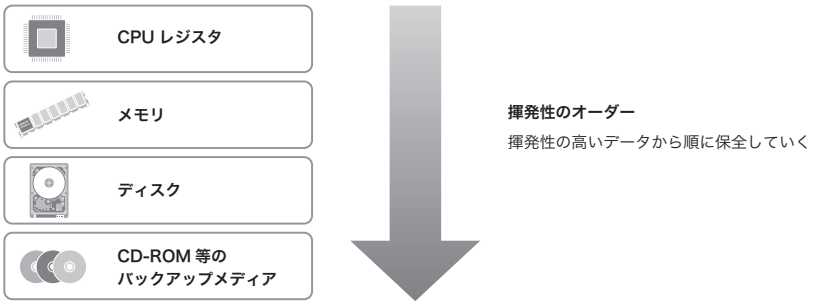


図-15 揮発性のオーダー

＊53 Sysinternals Suiteには実行中プロセスの情報を表示するPsListやTCP接続の状態を表示するTcpView等揮発性のデータを収集する多数のプログラムが含まれる（http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx）。

＊54 揮発性データ収集ツールキットは、数多くのプログラムで構成されており、それらの実行によるスワップ発生などで、メモリイメージの内容に影響を与える可能性がある。

＊55 ここで示したようなデータ解析を行うためのツールとしては EnCase（http://www.guidancesoftware.com/）、FTK（http://www.accessdata.com/）、TSK（http://www.sleuthkit.org/）等がある。

●複数ソースのログの集約
●アンチフォレンジックへの対応
●メディアの大容量化や暗号化への対応

複数ソースのログの集約に関する課題の例として、情報漏洩による機密情報の拡散範囲の調査があります。この場合には、コンピュータフォレンジックに加えて、ネットワークフォレンジックの実施も必要です。具体的には、ファイアウォール、ルータ、IDS等の各ネットワーク機器のログやパケットデータをコンピュータ側の情報と突き合わせる必要があります。しかし、各機器のログのフォーマットが異なっていたり、設定されている時刻にずれが生じていたとき等には、この突合せ作業は大きな負担となります。

アンチフォレンジックは、デジタルフォレンジックによる検出を逃れるための手法です。例えば、ファイルシステムのタイムスタンプを元に関係するファイルを調べていく手法から逃れるために、作成したファイルの時刻情報としてランダムな時刻をセットし直すマルウェアがあります。そのようなアンチフォレンジックに対しては、ファイルシステム以外のタイムスタンプ[*56]を活用する必要があります。

保全対象となるメディアのサイズも年々増大しています。できるかぎり短い時間でデータを保全するためには、保全する機器やソフトウェアの性能向上を待つしかありません。しかし、十分な時間を確保できないときには、保全前にプレビュー（対象のメディアを読み取り専用でマウントして直接調べる）を活用することも１つの手段になります。また、大容量のメディアを効率よく解析するためにプロセスを自動化できることも望まれています。加えて、最近ではメディアが暗号化されているケースも多く見受けられます。このようなときには、オンライン状態で保全するか、オフライン状態で保全した後に復号化する手段を確保しておく必要があります。

■ まとめ

デジタルフォレンジックをインシデントレスポンスに活用することで、重要な手がかりとなるデータを見逃すことなく、インシデントの発生原因やその影響範囲を調査することが可能です。IIJでは、今後もデジタルフォレンジックでの課題の解決方法を検討していくとともに、常に最新技術動向を調査しその知見を対応方法に取り入れていきます。

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、インシデント対応に必要な準備として、小規模システムでのDDoS攻撃への備え、クラウドコンピューティング等の共用システムにおけるセキュリティと、デジタルフォレンジックの概要を取り上げました。

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

執筆者:
齋藤 衛（さいとう まもる）
IIJ サービス本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発等に従事の後、2001年よりIIJグループの緊急対応チームIIJ-SECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会、Webで感染するマルウェア対策コミュニティ等、複数の団体の運営委員を務めるとともに、安心ネットづくり促進協議会 児童ポルノ対策作業部会 技術者SWG、IPAサービス妨害攻撃対策検討会等においても活動も行う。

土屋 博英（1.2 インシデントサマリ）
土屋 博英 鈴木 博志 永尾 禎啓（1.3 インシデントサーベイ）
齋藤 衛 土屋 博英（1.4.1 小規模システムにおけるDDoS攻撃への備え）
加藤 雅彦（1.4.2 共用システムにおけるセキュリティ）
春山 敬宏（1.4.3 デジタルフォレンジックの概要）
IIJ サービス本部 セキュリティ情報統括室

協力:
須賀 祐治　吉川 弘晃　小林 直　齋藤 聖悟　IIJ サービス本部 セキュリティ情報統括室

＊56 他のタイムスタンプとしては、ファイル自身が内部に持つ情報や、ショートカットファイルが持つオリジナルファイルの情報、レジストリキーの情報等がある。Webブラウザやメール経由でのマルウェア感染時にはブラウザ履歴やメールの送受信日時等も手がかりになる。

DNSSECの導入にむけて

**DNSは、インターネットに欠くことができないサービスです。
ここでは、DNSの役割を改めて振り返るとともに、昨今懸念されているDNSへの
脅威に対応する技術、「DNSSEC」について導入の課題と展望について説明します。**

2.1 DNSの役割

DNSは、問い合わせに対応したリソースレコードを応答するという単純なサービスですが、インターネットで事実上必要不可欠なサービスです。例えば、ユーザ自身はあまり認識していませんが、Webブラウザでのページ閲覧やメールの送受信など、日常的なインターネット利用の舞台裏でもDNSが活躍しています。もちろんDNSがなくても通信はできます。ただし、通信先のIPアドレスを覚えておく必要があるなど、インターネットの利便性が大きく損なわれてしまうため、現実的には多くのユーザがDNSに依存していると言ってもよいでしょう。

DNSでは、ゾーンと呼ばれる範囲ごとに分散管理できるようになっています。インターネットではルート(.)ゾーンを頂点とし、必要に応じてサブドメインを設定して管理を権威委譲することで、ツリー状の分散管理が実現されています。例えば.jp ccTLDは株式会社日本レジストリサービス(JPRS)に権威委譲され、登録されたドメインはJPDNSと呼ばれるコンテンツDNSサーバ群を通じて公開されています。問い合わせを行う側は、このツリー状に権威委譲され、分散管理されているコンテンツDNSサーバをたどって必要なリソースレコードを見つけます。

多くの場合、手元の端末はこの作業を自分自身で行わずに、ISPやネットワーク管理者の運用するキャッシュDNSサーバに要求します。キャッシュ DNSサーバは、端末からの要求に応じてコンテンツDNSサーバをたどって必要なリソースレコードを検索し、結果を端末に返します。DNSが正常に稼働していないと、目的のサービスにアクセスできないといった障害が発生してしまいます。実際に、DNSのトラブルによってWebサイトにアクセスできないといった障害は、世界中でたびたび発生しています。

2.2 DNSSECの必要性

さて、DNSサーバの運用で一番起こしてはならないトラブルは何でしょうか。それは「嘘を答えること」です。誤ったリソースレコードを応答してしまうと、応答を受け取った側はそれを信じてしまうため、間違いの内容によってはかなり困った状況になってしまいます。世の中には悪いことを考える人がいるもので、この嘘の応答を意図的に注入する攻撃が存在しています。この攻撃が成功すると、あるWebサイトにアクセスしようとするユーザを、まったく別な任意のWebサイトに

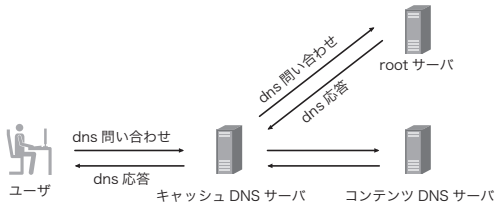


図-1 DNSへの問い合わせと応答

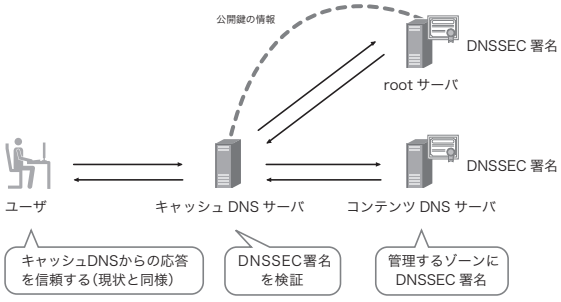


図-2 DNSSECの導入

誘導できてしまいます。これによって、アカウント情報を盗まれるといったような被害が容易に想像できます。さらに悪いことに、この攻撃は、現在の端末の性能や回線速度であれば実現可能です。

このような攻撃を想定して、DNSの応答が正しいかどうかを検証可能にする技術が検討されてきました。それがDNSSECです。DNSSECでは、公開鍵暗号方式を用いた電子署名をDNS応答に付加することで、応答の送信者を認証し、応答内容の完全性を確認できるようにしています。

DNSSECでは、ゾーンごとに電子署名を行います。この署名を検証するためには、それぞれの公開鍵の情報が必要です。DNSSECでは、サブドメインで署名に利用した公開鍵の情報をリソースレコードとしてゾーンに登録できます。このようにすることで、あるゾーンの公開鍵の情報を手に入れれば、その配下のドメインに関しては、登録された公開鍵の情報をたどることで検証可能になります。この信頼の連鎖によって、任意のゾーンからDNSSECを検証することも可能ですし、信頼の連鎖がきちんと繋がっていればルート(.)の公開鍵の情報さえ得ていれば、署名されたゾーンすべてが検証可能になります。

2.3 DNSSEC対応のための作業

ゾーンの管理者としてDNSSECへの対応を考えたときには、2つの作業が必要になります。1つはゾーンへの署名作業で、もう1つは署名に利用した公開鍵の情報を上位ゾーンに登録する作業です。ゾーンへの署名作業は、鍵の運用と密接な関係にあり、公開鍵暗号の知識、継続的な鍵の更新と署名の実施が必要になります。また、上位ゾーンに公開鍵の情報を登録する際には、上位ゾーンを管理するレジストリでのDNSSEC対応はもちろんのことですし、登録窓口となっているレジストラのDNSSEC対応も必要となります。.jp ccTLDでは、2010年10月17日にJPゾーンのDNSSEC署名を開始し、2011年1月16日にレジストリでの対応、つまり公開鍵の情報登録受け付け開始を予定しています。

問い合わせ側においては、まずISPやネットワーク管理者の運用するキャッシュDNSサーバでDNSSEC検証が行われ、端末がその検証結果を信頼するというモデルが普及すると考えられます。このようなDNSSEC検証を行うキャッシュDNSサーバでは、検証したい範囲に応じて信頼の拠り所となる公開鍵の情報を得ておく必要があります。ルート(.)がDNSSEC署名された現状では、ルートの公開鍵の情報を設定しておく方法が簡単な運用方法だと考えますが、運用ポリシによっては必要な範囲のみを検証可能にすることもありえるでしょう。いずれにせよ、これらの公開鍵の情報は、鍵の更新タイミングに追従して更新していく必要があります。

実際には、DNSSEC運用に関わるトラブルがすでに数多く報告されています。その内容は、更新作業を怠ってしまったという単純なケースから、運用ツールに問題があったというケースまでさまざまです。DNSSECでトラブルが発生すると、ほとんどの場合で署名検証に失敗し、キャッシュDNSサーバがエラーを応答します。すると、ユーザ側では、DNSから必要な応答を得られません。実際に、前述のトラブルでは、多くのユーザがWebサイトにアクセスできないといった大きな影響がありました。せっかくセキュリティ向上を目指してDNSSECを導入しても、きちんと運用できなければ、アクセスできないなどのトラブルを発生させてしまいます。

DNSSECでは、公開鍵暗号の知識や継続的な更新作業が必要であり、これまで以上にきちんとDNSを運用する必要があります。残念ながら現状では、気軽に導入できるようなものではありません。それでもDNS応答を検証できる機能は、重要なものであり、DNS応答を偽られたときに大きな被害が出るサービスにとっては、運用体制を作って導入を検討する価値があるものです。IIJでは、これまでにDNSSECの導入に向けてさまざまな試験や調査を行ってきました。また、いくつかのトップレベルドメインでのDNSSEC導入にも積極的に協力してきています。今後、これらの知見を生かして、DNSSECによるより安全な利用環境を提供できればと考えています。

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

送信ドメイン認証技術の送信側導入状況はやや停滞

今回は、2010年第26～38週での迷惑メールの推移を報告します。迷惑メールの送信元地域は、中国に代わって米国が1位になりました。また、今回は、送信ドメイン認証技術の導入状況とボットネット対策についても考察します。

3.1 はじめに

このレポートでは、迷惑メールの最新動向やメールに関する技術解説など、IIJが関わるさまざまな活動についてまとめています。

今回のレポートでは、2010年の第2四半期にあたる第26週（2010年6月28日～7月4日）から第38週（2010年9月20日～9月26日）までの13週間分のデータを対象としています。

3.2 迷惑メールの動向

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

3.2.1 前年までとは異なり、9月以降も迷惑メールは増えず

2010年第26週から第38週までの91日間に検出した迷惑メールの割合は、平均79.0%でした。前回（2010年第13～25週）の平均が81.3%、2009年同期（第27～39週）が82.2%でしたので、いずれも若干の減少という結果になります。今回の調査期間を含めた2009年第27週からの迷惑メールの割合の推移を図-1に示します。

これまでの調査では、日本の連休期間に重なる第32週（8月9日～15日）に、通常のメール流量が減少することで迷惑メールの割合が高くなり、その後に減少するものの9月以降に再び高くなるという傾向が続いていました。今回も8月までは同じような割合で推移し、第32週がこの期間でもっとも高い割合である82.6%を示

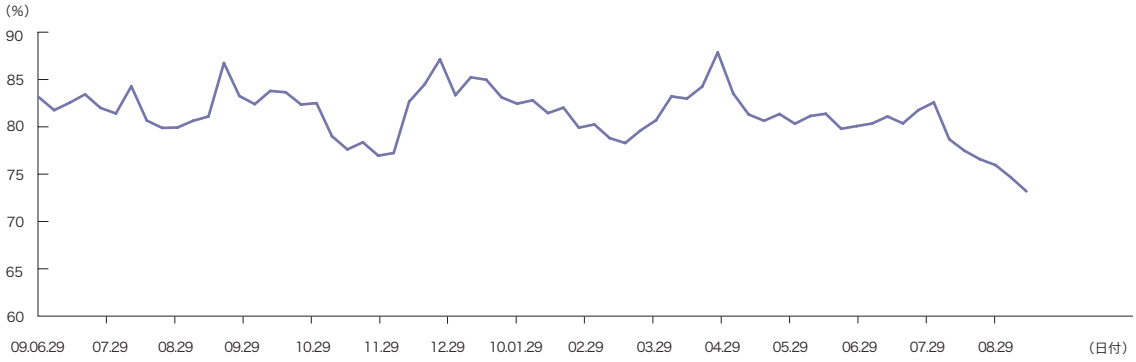


図-1 迷惑メール割合の推移

しました。しかし、9月以降になっても低い割合が続いたため、この期間全体の迷惑メールの平均値が低くなっています。この減少が一時的なものなのか、何かの理由によって今後も迷惑メール量が減少していくのかは不明です。今後の分析とともに調査していきたいと考えています。

3.2.2 中国に代わって米国が迷惑メール送信元1位に

今回の調査期間での迷惑メールの送信元地域の分析結果を図-2に示します。今回の調査では、迷惑メールの送信元地域の1位は米国（US）で、迷惑メール全体の11.3%を占めていました。前回の2位から順位を上げ、再び首位に戻りました。2位はインド（IN）の7.4%で、前回の3位から上昇しています。3位は前回首位だった中国（CN）で7.1%でした。また、前回上昇傾向を示していた欧州の英国（GB）とドイツ（DE）は、それぞれ5位（5.0%）と7位（4%）となり、引き続き高めの傾向にあります。その他は、ブラジル（BR）が4位（5.2%）、ベトナム（VN）が6位（4.8%）と、これまでも割合が高かった地域が引き続き上位を占めています。日本は、割合が0.1%微減して順位を8位（3.8%）に後退しています。

図-3に、これらの迷惑メール送信元の上位6地域（US、IN、CN、BR、GB、VN）での割合の推移を示します。前回1位だった中国（CN）は、7月に低下していますが、8月以降は上昇傾向にあり、今後再び上位送信地域になる可能性があります。今回1位であった米国（US）は、調査期間中を通してほぼ1位であったため、全体でも首位になりました。これら以外の上位4地域（IN、BR、GB、VN）は、大きな変動はありません。ただし、今回2位であったインド（IN）は、時期によって1位や2位になっているため、引き続き注意が必要と考えています。

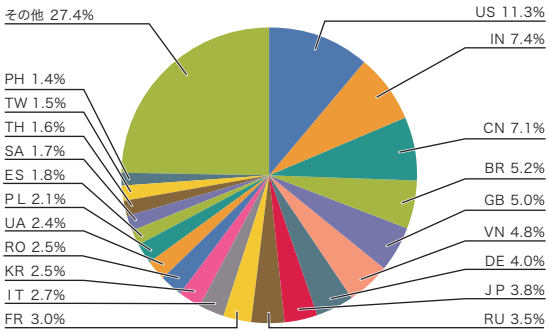


図-2　迷惑メール送信元地域の割合

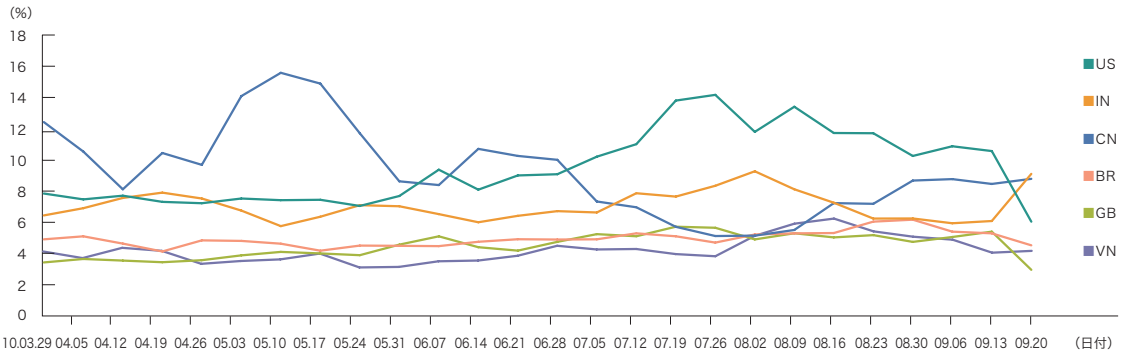


図-3　迷惑メール送信元のうち上位6地域の推移

3.3 メールの技術動向

前回に引き続いて今回も、広く普及している送信ドメイン認証技術の一つであるSPF(Sender Policy Framework)の導入状況について報告します。また、今回は、迷惑メール送信の主な原因であるボットネットを根絶させるための活動事例についても報告します。

3.3.1 送信ドメイン認証技術

IIJが提供しているメールサービスでは、メール受信時の送信ドメイン認証をほぼ標準で行っています。図-4に、今回の調査期間(2010年7～9月)での認証結果の割合を示します。この期間に受信したメールの認証結果は、全体の55.7%が“none”でした。これは、受信メールの約44.3%のドメインでSPFレコードが宣言されていたことを表しています。この結果は、前回の調査結果に比べて0.8%の微減になります。また、JPドメインだけを調査しても減少していました(図-5)。WIDEプロジェクトの調査[*1]でも、以前に比べて横ばい傾向にあるため、導入ドメイン数があまり伸びていないことが予想できます。

総務省では、IIJを含めた電気通信事業者6社でのSPFの認証結果の割合の推移を、2009年8月から統計データとして公表しています[*2]。最新データの2010年8月では、認証結果のうち“none”が約18%でしたので、受信メールの約82%のドメインがSPFレコードを宣言していることになります。

この結果は、本レポートでの結果と大きく異なっています。これは、メールサービスの利用者層や集計ポイントの違いによるものと考えられます。例えば、携帯電話では、受信メールの多くが携帯電話から送信されたものです。携帯電話事業者のほとんどのドメインがSPFレコードを宣言しているため、高い認証結果になることが予想できます。このことから、送信ドメイン認証技術の導入傾向を把握するためには、それぞれのデータの絶対値を比較するのではなく、それぞれの割合の時間的な推移で判断したほうがよいと思えます。
データの集計開始時点での導入割合が元々高かったこともあり、いずれの結果でも、最近の傾向として導入が進んでいるとは言い難い状況が続いていることがわかります。

3.3.2 ボットネット対策

今回報告した迷惑メールの送信元地域で7位のドイツ(DE)では、迷惑メールの主な送信手法であるボットネットを根絶するために、The German Anti-Botnet Initiative[*3]を今年9月に立ち上げました。これは、ドイツのインターネット産業協会であるecoと連邦政府組織であるBSI(The Federal Office for Information Security)の協力の元に運営されるプロジェクトで、不正プログラムに感染した一般ユーザに警告を発し、正常に戻るまでインターネットへのアクセス制限なども行う対策です。このプロジェクトでは、不正プログラムを駆除するツールを提供したり、電話サポートを行ったりすることで、ユーザのPCをクリーンにしようと計画してい

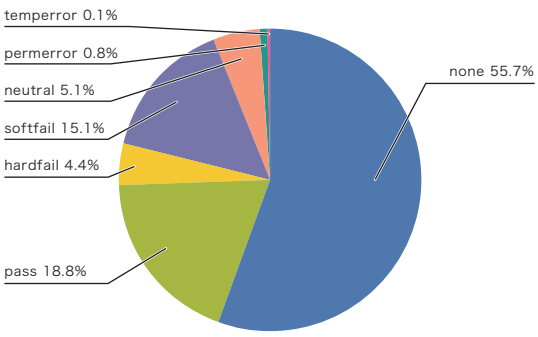


図-4　送信ドメイン認証結果の割合

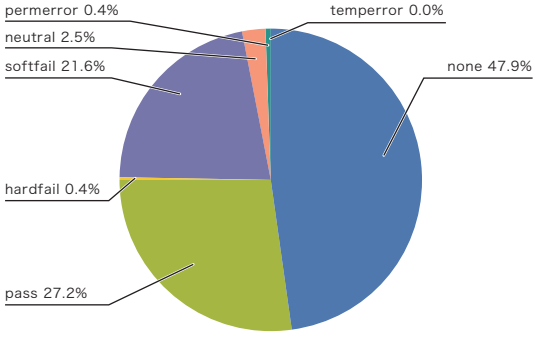


図-5　送信ドメイン認証結果の割合(JPドメインのみ)

＊1　2010年8月現在でのJPドメインにおけるドメイン認証技術のおおよその普及率(http://member.wide.ad.jp/wg/antispam/stats/index.html.ja)
＊2　http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei
＊3　http://www.oecd.org/dataoecd/42/50/45509383.pdf

ます。日本のCCC（Cyber Clean Center）[*4]での取り組みに非常によく似ていると思われるかもしれません。実際に、このプロジェクトに関わっているecoのメンバーがCCCの関係者にヒアリング等を行っていますので、かなりの部分を参考にしたのではないかと思います。また、今年の6月に開催されたMAAWGのGeneral Meetingでも、CCCの活動が報告されました。

迷惑メールの送信を止めるだけであれば、日本で広く導入されている、動的IPアドレスからの直接メール送信を止めるOP25B（Outbound Port 25Blocking）が非常に効果的な方法になります。ボットネットは、迷惑メールの送信だけでなく、不正プログラムの配布元やDDoS攻撃の発信元になったり、不正プログラムによってPC内の個人情報を搾取したりすることに使われるなど、より深刻な被害の原因になります。このため、ボット化されるときの主な原因である、不正プログラムが添付された迷惑メールの流通を抑えるために、まず通信事業者がOP25Bを導入することが必要です。そして、そこでブロックした情報や、不正プログラムが指令を受けるために使用したDNSの問い合わせ情報などから、感染したPCを特定します。また、おとりホストを運用し、不正アクセスの送信元を検知することもできます。さらに、CCCやThe German Anti-Botnet Initiativeでの活動のように、駆除ツールを配布し、ボット化の原因である不正プログラムを除去します。

このように、ボットネットを根絶するための手順は、ある程度確立されつつあります。しかし、不正プログラム駆除のためには、それ相当のコストがかかります。日本やドイツのプロジェクトでは、主に政府が費用を負担していますが（ドイツは初年度）、最終的にはそれぞれの国の国民がこのコストを負担していることになります。こうした負担を軽減するためにも、個々の利用者がボット化されないように日頃からの注意が重要です。

3.4 おわりに

日本における迷惑メール対策法ともいえる「特定電子メールの送信の適正化等 に関する法律（特電法）」には、施行3年後の見直し規定が盛り込まれています。平成14年に公布された特電法は、平成17年と平成20年にそれぞれ改正され、今回も特電法の施行の状況等を踏まえつつ、今後の迷惑メール対策として必要な措置を検討するための会合が今年の9月から開催されました。今回は、「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」の下に「迷惑メールへの対応の在り方に関する検討WG」が設置され、このWGの会合で検討が行われています[*5]。IIJでは、この特電法の見直しのための検討に継続して参加しており、今回は本レポートの報告者が構成員として参加しています。

前回の改正では、特定電子メール（いわゆる広告宣伝メール）を送信するためには事前の同意が必要なオプトイン規制が導入されるという、大きな変更がありました。しかし、個人的に受信するメールをみても、オプトインした覚えの無い、様々な勧誘を行う広告宣伝メール的な迷惑メールが相変わらず届く状況が続いています。こうした状況が続く背景には、様々な要因があるわけですが、そもそもメールの送信者を明確に特定することができないことが大きな原因の一つと考えています。

送信ドメイン認証技術を普及させることによって、こうした問題をある程度改善していけるのではと考えています。IIJでは、技術的な問題解決だけでなく、こうした法的な側面を含め、今後も迷惑メール対策に積極的に関わっていく予定です。

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

＊4　http://www.ccc.go.jp/
＊5　http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html

次世代モジュール型エコ・データセンターの実証実験報告

IIJでは、次世代モジュール型エコ・データセンターを構築するために、中部地方にて2010年2月から1年間にわたり外気冷却方式のコンテナユニットによる実証実験を行っています。ここでは、実証実験の目的、実験に用いたシステムの構成とともに、実験結果を説明します。

4.1 外気冷却方式の実証実験に至った理由

4.1.1 空調方式見直しの必要性

データセンターは、大量のサーバなどのIT機器を効率よく設置できる環境を実現するために、大容量の電気設備や空調設備を備えています。しかし、現在のデータセンターには、サーバから排出される熱が当初の設計時の想定を大きく上回り、十分に冷却できないという問題があります。これは、IT機器の処理能力や集積度が向上し、機器あたりの消費電力とともに発熱量が増えていることが原因です。当初、サーバを設置するラックあたりの消費電力は、実効値で1 ～ 3kVA程度と見積もって設備を設計していたのですが、現状は4 ～ 6kVAが当たり前になりつつあり、将来は10kVA以上になる可能性があります。

また、2020年に温室効果ガスの排出量を1990年比で25%削減するという国際公約の実現や、東京都の環境確保条例によってCO2総量削減が義務付けられることなどから、データセンターにおいても消費電力を減らす対策が必要になっています。

データセンターでは、IT機器が最も多く電力を消費します。しかし、空調機器もIT機器と同等の電力を消費しています。このため、消費電力を大幅に削減するには、従来の空調方式を見直し、消費電力量が少ない新たな空調方式を導入する必要があります。

電力の消費を抑えて冷却する方法には、外部環境を利用する次の2つがあります。このうちwater-side economizer（チラーレス水冷方式）のみをフリークーリングと呼ぶことが多いですが、消費電力量を削減して冷却するというという意味ではair-side economizer（外気冷却方式）もフリークーリングに含まれます。

- water-side economizer（チラーレス水冷方式）
- air-side economizer（外気冷却方式）

チラーレス水冷方式では、図-1に示すように、水の気化熱を利用して、より少ない電力で冷却水を作る冷却塔（クーリングタワー）を使用します。これに対して外気冷却方式では、冷たい外気を利用してデータセンターを冷却します。

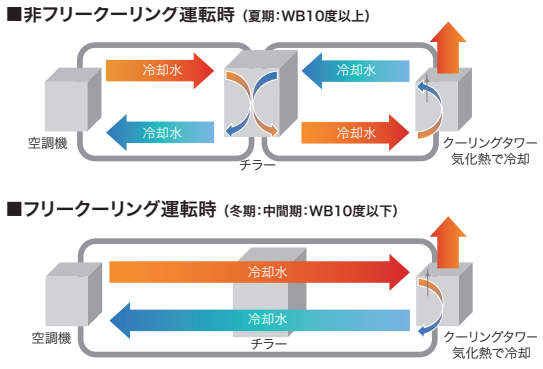


図-1　チラーレス水冷方式の原理

表-1　フリークーリングの方式比較

	Water-side economizer チラーレス水冷方式	Air –side economizer 外気冷却方式
仕組み	水の気化熱（冷却塔）で冷却した冷水で室内を間接的に冷却	外気で室内を直接冷却
湿度、塵埃管理	室内の空気は循環するため、加湿装置、フィルタは簡易ものでよい	外気を直接室内に入れるため、加湿装置、フィルタなどの設備が必要
設備の特徴	冷却塔、冷水配管が必要	サーバールームに外気導入の開口部が必要で既存の建物には導入しにくい
主なランニングコスト	冷却塔で気化する水の補充、冷水を循環させるポンプ動力、室内機の動力	外気導入のファン動力
年間利用可能時間	3500~4000時間/8760時間（東京）	5500~6000時間/8760時間（東京）
日本での導入状況	多数あり	中間期のみ利用することが多く、冬期の導入事例はほとんどない

この2つの方式には、表-1に示すような特徴があります。IIJでは、シミュレーションの結果から、年間利用可能時間が長く、冷却塔などの設備が必要ない外気冷却方式が次世代のデータセンターに適していると判断しました。

しかし、外気冷却方式では、大量の空気を吸排気するための開口部をサーバルームに設ける必要があります。このため、既存のビルに外気冷却方式を導入するためには、解決しづらい大きな問題が存在することになります。そこで、IIJは、空気を吸排気するダクトと筐体を一体化しIT機器を搭載するコンテナモジュールを開発することにしました。

4.1.2 現在の海外動向

巨大なデータセンターの建設で先行している米国では、どのような空調方式が採用されているのでしょうか。これまで、米国ではチラーレス水冷方式が主流と言われていましたが、外気冷却方式の採用も増えています。表-2に、Microsoft、Google、Yahooの各社が最近1、2年に建設したデータセンターの動向を示します。Microsoft社とYahoo社は、外気冷却を主冷却方式にすることに舵を切ったように見受けられます。これに対してGoogle社は、海水による冷却システムを備えたデータセンターをフィンランドに建設するとの報道もあり、チラーレス水冷方式をベースとする方針に変わりがないようです。

Yahooがナイアガラの滝の近郊に2010年9月にオープンしたデータセンターは、公表されている資料から図-2のような構造になっているものと推測されます。建設地のLockportの冷涼な気候を生かし、年間の大部分を外気のみで冷却できるようです。ここで取り上げた3社以外にもNetAppやHPなども自社のデータセンターで外気冷却方式を採用しているとの事例もあり、データセンターにおける外気冷却方式の採用は世界的なトレンドになっているとIIJは認識しています。また、Ashrae（米国暖房冷凍空調学会）TC9.9は、データセンターの消費エネルギー量削減のために、2008年にデータセンターの温湿度条件を緩和しました。IIJは、このことも外気冷却方式の普及を後押しする要因の1つになると考えています。

4.1.3 そして実証実験へ

IIJでは、省エネ性、投資コスト、運用コストなどのメリットと、海外の動向から、現時点においては、外気冷却方式が次世代のデータセンターに適しているという結論に達しました。しかし、海外で実用化されているといっても、日本固有の高温多湿な気候条件で商用に供するためには、実運用に耐えうることの検証が必要と判断し、今回の実証実験を実施することとなったのです。

表-2　米国で最近建設されたデータセンターの動向　　（各種報道資料よりIIJ作成）

会社名	場所	面積	稼働・建設年月	特徴	空調方式
Microsoft	Northlake Illinois, US	51,097㎡	2009年9月　稼働開始	PUE=1.22 1階はコンテナ形式 2階は通常型	水冷
	Quincy Washington, US	9,290㎡	2010年5月　増設工事開始	IT PAC使用 flywheel UPS PUE=1.06	外気
	Dublin, Ireland	28,150㎡	2009年7月　稼働開始	PUE1.25	外気
Google	Hainaut, Belgium	不明	2008年　稼働開始	PUE=1.1	水冷チラーレス
	Hamina, Finland	8,000㎡	2011年春　稼働開始	製紙工場を改修	海水冷却
Yahoo	Omaha Neblasca, US	27,871㎡	2009年　稼働開始	flywheel UPS	外気+チラー
	Lockport New York,　US	14,400㎡	2010年9月　稼働開始	PUE 1.08 flywheel UPS	外気

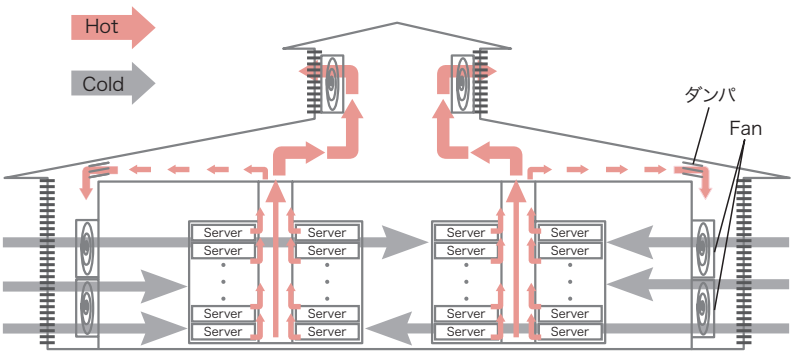


図-2　Yahoo Lockportのデータセンターの構造（IIJ 推定）

4.2 実証実験の目的とシステム構成の概要

外気を利用してサーバ等のIT機器が冷却できることを実証するのが実験の目的ですが、最終的に目指しているものは省エネルギー化であり、今後構築する商用データセンターに採用することにあります。単に外気をIT機器の冷却に利用して「できた」や「できない」という結果を出せばよいのではなく、省エネルギー化が達成されているか、商用データセンターへの利用に耐えうる品質かを定量的に測れることが必要です。

このためIIJでは、各分野のプロフェッショナルとパートナー関係を結び、実証実験システムを構築しました。外気冷却を可能にし、IT機器の冷却に最適化し、自動制御可能な空調機である空調モジュールを、株式会社東芝と共同開発しました。IT機器を収容するためのコンテナユニットであるITモジュールは、日本軽金属グループの株式会社エヌ・エル・エム・エカルに製作を依頼しました。ITモジュール内には、通常のデータセンターと同様に、IT機器を収容するためのラックや、主幹電力線から安全に各ラックに電気を送るための分電盤を備えています。また、省エネルギー化が達成されているかを計測するために、電流や積算電力計のパルス信号を測定する機器も必要です。これらは河村電器産業株式会社より調達しました。

大量の電気を消費するデータセンターでは、火災が最も身近で憂慮される災害です。このため、事前の検知と、万が一発生したときにIT機器にできるかぎり影響がない消火が行える設備が求められます。一般にデータセンター内に吹く風はかなりの量になるため、今回の実証実験システムも同じ状況になることが想定されます。したがって、通常のオフィスで利用される火災検知機は用途に適さないため、防災設備として火災予兆センサーを設置し、ITモジュール内の火災を検知できるかを実験しました。これには能美防災株式会社に協力をお願いしました。また、可能なかぎり実際のデータセンターの環境を再現するために、国際産業技術株式会社からITモジュール内の熱負荷としてサーバ機器を調達し、設置しました。

ここでは、このような実証実験システムを構成する要素を説明していきます。その前にデータセンターのエネルギー指標に関して、その概要をまとめておきます。

PUE (Power Usage Effectiveness) は、米国の業界団体The Green Gridが発表し、世界で最も普及しているデータセンターの電力利用効率を表すための指標です。しかし、今回の実証実験システムは、データセンター全体の設備やシステムを構築するものではありません。このため、PPUE (Partial PUE) の概念を導入することにしました。コンテナユニットの利用などモジュール化指向が進むデータセンターにおいて、PPUEはその名が示すとおりに部分的なPUEを表すためのものです。実証実験システムでは、次の計算式でPPUEを求めることが可能となるように、積算電力計等を配置しています。

$$PPUE = \frac{\text{空調モジュール消費電力} + \text{ITモジュール消費電力}}{\text{ITモジュール消費電力}}$$

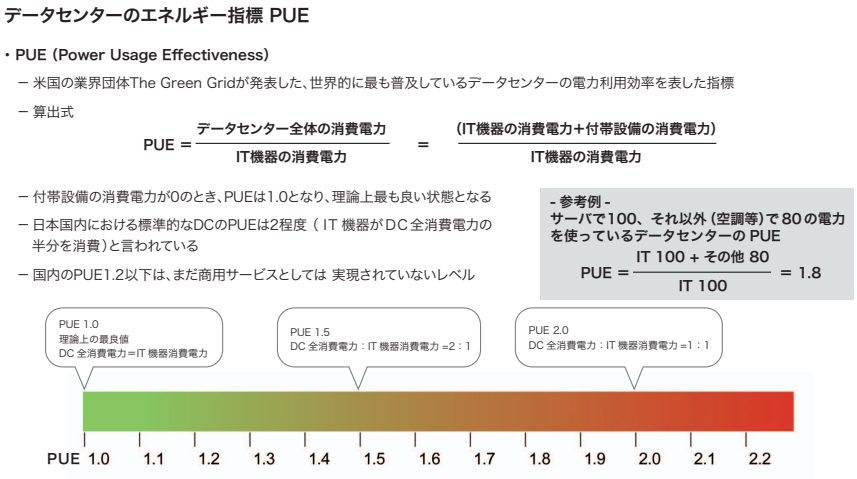


図-3　データセンターのエネルギー指標PUE

4.2.1 空調モジュール

先ほど示した通り、今回の実証実験で用意した空調モジュールは、「外気冷却を可能にし、IT機器の冷却に最適化し、自動制御可能な空調機」です。では、IT機器の冷却に最適化とは、どのような環境状況を指すのでしょうか。今回は、Ashrae（米国暖房冷凍空調学会）技術委員会TC9.9のデータセンター内の温室度条件推奨値（以下、Ashrae2008）を採用することにしました。

図-5のグラフは、横軸に乾球温度［℃］、縦軸に絶対湿度［kg/kg（DA）］を採った簡易的な空気線図です。本来、h＝比エンタルピ［kJ/kg（DA）］、x＝絶対湿度［kg/kg（DA）］の「湿り空気h-x線図」が、空調業界で一般的に使われる空気線図です。空気線図は、大気圧（101.325kPa）を基本として、乾球温度［℃］、湿球温度［℃］、露点温度［℃］、絶対湿度［kg/kg（DA）］、比エンタルピ［kcal/kg（DA）］、相対湿度［%］等の関係を線図で表したもので、このうちの2値が定まれば他の値もすべて線図上で求めることができます。

続いて、空調モジュールの各運転モードを説明します。

■ 外気運転モード

外気運転モードは、最もシンプルな運転モードです。外気運転モードでは、外気の温湿度状態が目的とするAshrae2008内にあるときに、外気をそのままIT機器の冷却に用い、IT機器からの排気はすべて捨ててしまいます。このとき空調モジュールで必要な動力は、外気を取り入れるファンのみで、大幅な省エネルギー化が実現できます。

■ 混合運転モード

混合運転モードは、外気の温湿度状態が低温度、低湿度であるとき用いられる運転モードで、主に冬期に利用されます。混合運転モードでは、外気とIT機器の排気を混合させますが、それぞれの温湿度の状態によって混合比率を可変させ、目的とするAshrae2008の範囲内の空気を作り出します。

混合点が空気線図上のAshrae2008の範囲より下になる場合、つまり湿度が不足しているときには、気化式加湿を行います。気化式加湿は、空気中の熱量を奪いながら加湿するため、空気線図上は右下から左上に空気の状態が遷移します。この結果、Ashrae2008範囲内の空気をIT機器に供給することができます。また、気化式加湿は、蒸気式加湿と違って加湿のために電力を必要としません。このため、外気運転モードと同様に、空調モジュールに関わる動力はファンのみとなり、大幅な省エネルギー化が実現できます。

■ 循環運転モード

外気をそのまま用いたり、またはIT機器の排気と混合させ気化冷却を伴う気化式加湿を行ったりしたとしても、どうしてもAshrae2008の範囲内の空気を作り出すことができない状態に外気がなっていることがあります。この場合には、従来からの方式による冷却が必要となり、コンプレッサーなど電力を多く消費する冷却ユニットを動作させなければなりません。また、消費電力が多いという理由から、その機能をまったく備えないというわけにもいきません。このため、空調モジュールは、循環運転モードのために、

Partial PUE（部分的PUE）

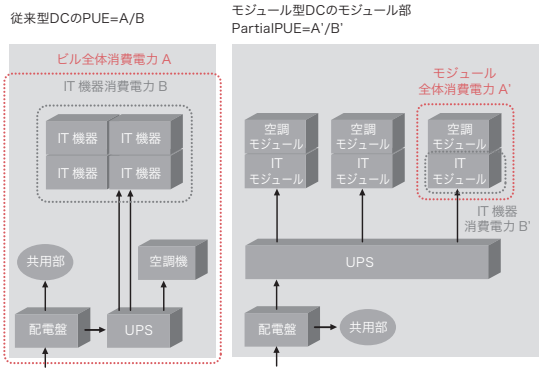


図-4　部分的PUE（PPUE）

	乾球温度	相対湿度	露点温度	備考
Ashrae class1&2 recommended level (2008 Version)	18 - 27℃	60%以下	5.5 - 15℃	DCのエネルギー消費量削減のため、Ashraeが2008年に改訂した機器の吸い込み温湿度条件の推奨値。
Ashrae class 1 allowable level	15 - 32℃	20 - 80%	17℃以下	外気利用等のエコノマイザー利用期間を延ばすために設けられた許容値。ただし、どの程度の期間利用できるかは、IT機器の検証とハードウェア障害の許容度による。

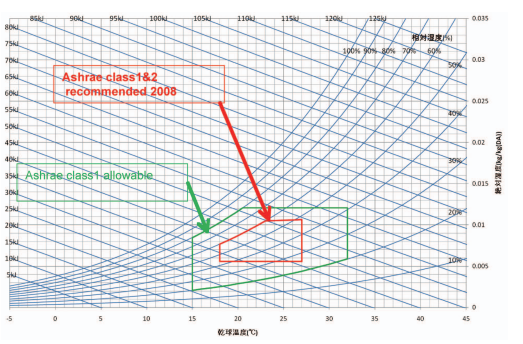


図-5　Ashraeによるデータセンター内温湿度条件推奨値

外気を遮断しコンプレッサーによる冷却を行うための設備を備えています。
循環運転モードの消費電力は、コンプレッサーの冷却能力に依存したものになります。このため、いかに優れた能力の製品を用いるかと、できるかぎり循環運転モードを発動させないように制御できるかが、年間を通じたトータルの省エネルギー化を達成するためのポイントになります。

ここまでに示した各運転モードは、空調モジュール内に設置された制御装置によって、外気の状態を元に自動的に制御され、切り替えられます。

次に、空調モジュールに必要な構成要素を説明します。

IT機器(ITモジュール)と空気をやりとりするためのファンは、インバータ制御が可能で、最大風量27,000m3/hを有しています。気化式加湿は、空調モジュール内の風洞に加湿モジュールを設置し、必要な際に給水することで加湿を実現しています。外気の取り入れと、IT機器の排気、外気とIT機器の排気を混合のために、空調モジュール内には複数のダンパが存在しています。混合比率は、これらのダンパの開度をインバータ制御によって調整します。また、循環運転モード時に利用する冷却ユニットとして、空調モジュール外部にそれぞれ28kWの冷却能力を持つ室外機(コンプレッサー)を4台設置し、空調モジュール内の風洞に設置した冷却コイルと冷媒管にて接続しています。室外機はインバータ制御で、きめ細かな制御と省エネルギー化を両立しています。温湿度状態を計るためのセンサーは、外気やITモジュール庫内の必要箇所に設置しています。
そして、これらの各構成要素を制御するためのDDC(Direct Digital Controller: 空調機制御装置)を空調モジュール内に設置し、各運転モードの自動制御を始めとするさまざまな制御を行います。このほかにも、外気を取り入れるという性質上、空調モジュールには中性能フィルターを備え、0.5μm以上の粉塵は除去される仕組みになっています。

なお、空調モジュールは、実証実験のために余裕を持った大きさで設計しています。今後構築する商用データセンターに採用する空調モジュールは、実証実験のものに比べて2/3程度の大きさになる予定です。

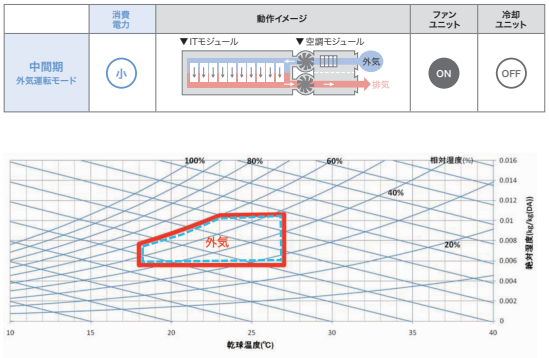


図-6　外気運転モード

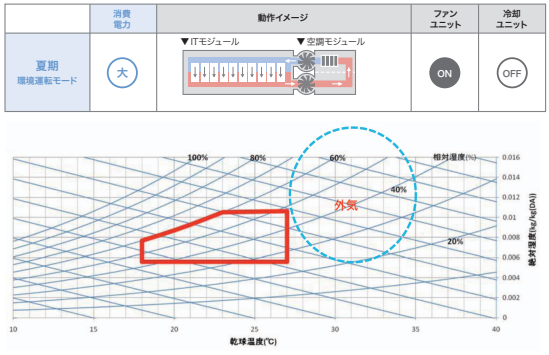


図-8　循環運転モード

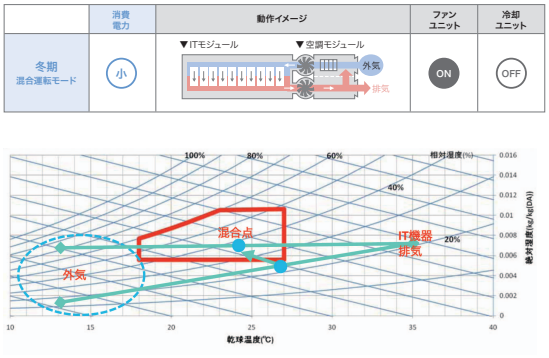


図-7　混合運転モード

図-9　左から、室外機、空調モジュール、ITモジュール

4.2.2 ITモジュール

サーバ等のIT機器を収容するコンテナユニットをITモジュールと呼びます。ITモジュール内は、IT機器を収容するラックを境に、ラック前面をコールドエリア、ラック後面をホットエリアとして区画されています。また、空調モジュールとITモジュールは、2本のダクトで接続され、空調モジュールから「IT機器の冷却に適した空気」がITモジュール内のコールドエリアに送られ、IT機器の排気がITモジュール内のホットエリアから空調モジュールに戻される構造になっています。

今回の実証実験では、サーバ等のIT機器の熱負荷は90kVAを想定しています。クラウド時代のデータセンターにはIT機器収容数の高密度化が求められているため、1ラックの実効電力10kVAが目標となります。これを9ラック備えたITモジュールとしては90kVAの実効電力が利用可能であるべきと考えました。

しかし、今回の実証実験はあくまで外気冷却という空調システムの検証が主目的で、IT機器は熱負荷でしかありません。このため、実際の構築にあたってはさまざまな検討を行いました。用意したラックのうち、熱源を搭載できるスペースは1架あたり約40U程度であり、1Uあたり250VAの電力を消費する必要があります。この熱負荷を安価に準備しようとしたときには、例えば電球を並べることが考えられます。4U程度のスペースに100Wの白熱灯を10個設置できれば、必要相当の負荷を得ることができます。また、ホットプレート（1300W程度）、こたつヒーター（500W程度）、ドライヤー（1200W程度）等も利用できるかもしれません。ただし、いずれの器具にしても外部からの制御が困難で、24時間連続運転したときには火災等の不安があります。また、エアフローに関する懸念もありました。個々のIT機器にはファンが搭載されています。このため、そのエアフローが再現できなければ、いくら単なる熱負荷とはいえ、実証実験と言えないのではないかという意見がありました。

図-10 ラック間を養生テープで目張りし空調効率を高める

このような検討を経た結果、最終的には本物のIT機器（サーバ）を設置して実証実験を行うことに決定しました。サーバには意図して5年ほど前の中古機器を用い、調達コストを圧縮するとともに、1Uあたりの消費電力を稼ぎ出すことにしました。現在のサーバは、省電力指向やその実装が進んでいるため、少し前の古いサーバのほうが消費電力が大きい傾向にあります。サーバは、複数メーカ、複数機種を導入しました。カタログスペック上の定格値が300 ～ 400VAというものが多かったですが、実測してみると平均180 ～ 200VA程度の電力消費となっていました。1Uサーバをメインに利用し、CPUを2個、メモリを最大枚数搭載（容量より枚数が重要）、HDDを2台にすることで、なんとか目標とする1Uあたり250VA程度、ITモジュール全体で最大90kVAに到達できました。

各サーバはあくまで熱負荷という位置づけですが、OSをインストールしネットワークに接続することで、リモートからの制御を可能にしました。OSの起動のみで処理負荷がかかってない状態で、およそ70%の消費電力（ITモジュール全体で約60 ～ 65kVA）、ベンチマークツールによる処理を実行させたときに100%（約90kVA）の負荷を作り出すことができます。また、サーバの物理設置にあたっては、ラックの隙間を完全に養生テープで塞ぐことで、空調効率を最大限まで高めるようにしました。

このほかにも、ITモジュールには随所に工夫を凝らしています。特にセンサー類は数多く設置し、さまざまな情報を取得できるようにしているのが特徴です

4.2.3 PPUEシミュレーション

ここまでの説明で、3つの運転モードを有し、それぞれを自動制御することで、IT機器にAshrae2008範囲内の空気を供給できる空調モジュールと、最大90kVAの熱負荷を作り出すITモジュールが構築できたことはお分かりいただけたと思います。実際に実証実験の結果を説明する前に、今回の実証実験システムを利用した

際にどのようなPPUEになるかをシミュレーションしたため、その結果を紹介します。

気象庁は、気象統計情報として、国内各地の過去の気温、湿度を始めとする気象情報を公開しています。この情報を利用して図-11のような空気線図にプロットすることで、空調モジュールの各運転モードの年間動作時間が算出できます。

また、空調モジュールの各運転モードの消費電力は既にわかっているので、これらの情報により今回の実証実験システムを国内各地で利用したときのPPUEを机上算出することができるわけです。図-12にシミュレーション結果を示します。図-12からも明らかなように、北方の寒冷地では、より低いPPUEが想定できます。しかし、沖縄（那覇）を除き、各地でのPPUEの差は0.1程度の範囲内に収まっています。一方で、寒冷地に設備を構築する際には、冬期の凍結防止や雪害対策などのために初期投資やランニングコストが増大する可能性があります。したがって、今回の実証実験に用いた外気冷却システムは、単純に年間通じて寒い場所に設置すればよいというものではないとも考えられます。

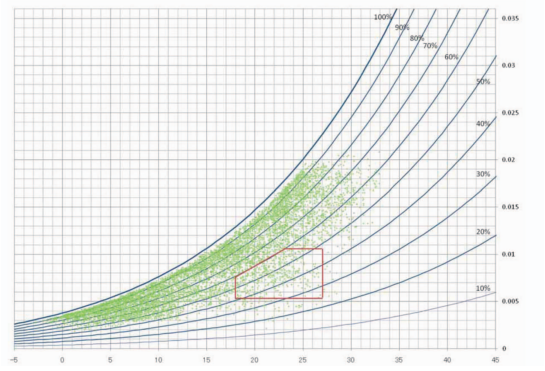


図-11　松江の外気温湿度状況(2009年)を空気線図にプロットした例

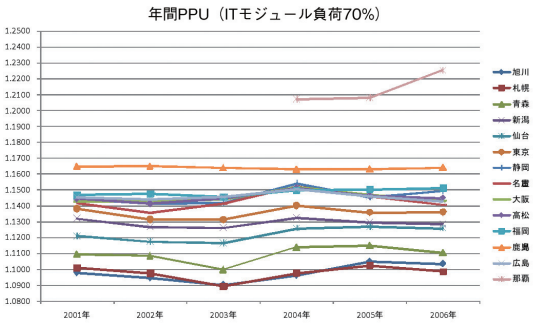


図-12　シミュレーション結果

4.3　実証実験の結果と考察

2010年2月から開始している実証実験では、すでにさまざまなデータを取得し、商用モジュールにフィードバックしています。ここでは、空調モジュールの運転データを元に実証実験の結果の説明と考察を行います。

4.3.1　空調モジュールの消費電力

空調モジュールの消費電力は、S A（Supply Air）ファンと室外機の2つに分けることができます。厳密には、これらに制御機器の消費電力も加わりますが、その量はわずかなため、ここでは取り上げません。

■ SAファンの制御

SAファンは、外気や室外機で作った冷気をＩＴモジュールのコールドエリアに供給し、ホットエリアに出されたIT機器の排気を空調モジュールに循環させる役割を担っています。動作する期間が通年であるため、SAファンの効率化は空調モジュールの省エネルギー化に大きく影響します。

SAファンの回転速度を小さくして風量を低減すると、SAファンの電力が回転速度の三乗に比例して小さくなります。つまり、風量を1/2にすると、電力は1/8になります。SAファンは、インバータ制御によってファンモータの回転速度を調整してコールドエリアへの供給風量をコントロールしているため、ＩＴ機器の冷却に必要な分だけの風量をコールドエリアに供給できれば省エネルギー化に大きな効果を発揮します。

また、ＩＴ機器は、自らのファンでコールドエリアの空気を吸気しホットエリアに排気するため、SAファンの風量としてはＩＴ機器のファン全風量分が常に必要になります。SAファンの風量がＩＴ機器のファン全風量より少なくなると、ＩＴ機器の周辺でショートサーキットが発生します。また、ＩＴ機器のファン全風量より多くなったときには、無駄な風がＩＴ機器内やラックの隙間を通過することになります。したがって、図-13に示すように、SAファンの風量とＩＴ機器のファン全風量が等しいときに、最も効率がよい省エネルギーな運転になります。しかし、ＩＴ機器のファン全風量を算出することは容易ではありません。これは、ＩＴ機器には個々の機種にさまざまなファンが搭載されていることに加えて、ＩＴ機器自体の処理動作（CPUやHDDの

利用状況）や吸い込み温度（コールドエリア温度）の状況による動作状態の変化（温度上昇を防止させるためにファンの回転速度を上げるなど）があるためです。このため、空調モジュールには、ＩＴ機器のファン風量増減を自動的に判断し、SAファンの風量を調整する制御システムの導入が必要です。

■ 室外機の制御

外気を利用しない循環運転モードでは室外機が動作します。通常、室外機は、ＩＴモジュールから戻された高温の空気を冷却するために使われますが、非常時に高温多湿の外気を冷却したり除湿したりする役割も担っています。室外機では、インバータでコンプレッサーモータを制御し、ＩＴモジュールの負荷に合わせて冷却能力を変更してコールドエリアの温湿度をリニアに制御してきめ細かに調整することができます。ＩＴ機器が発する熱は顕熱（温度変化）のみであるため、ビル型データセンターと同様に空調モジュールも高顕熱比で設計しています。

4.3.2 外気運転モードと混合運転モードの実証実験

2月～5月には、混合運転モードと外気運転モードでのさまざまなデータが取得できました。今回は4月6日のデータを元に実証実験の結果を説明します。図-14に、4月6日の運転レポートを示します。

外気運転モード時と混合運転モード時には、室外機が停止しているため、空調モジュールの電力の大部分がSAファンの消費電力になります。SAファンは、先ほど説明したとおりインバータ制御によってＳＡファンの風量（４月６日の平均風量14,627m3/h）を効率よく制御することで、必要最小限の運転を行います。これによって、空調モジュールの電力は、図-15に示すように全電力の4％程度で、PPUE＝1.044になっています。４月６日以外の日での外気運転モードや混合運転モードでもPPUE＝1.04 ～ 1.07を記録しており、想定どおりの省エネルギー化の結果が得られています。

また、図-16は、コールドエリア（青）、ホットエリア（赤）、外気（緑）それぞれの温湿度データを５秒ごとにプロットした空気線図です。コールドエリア（青）のプロットの97.84％がAshrae2008範囲内にあり、残りもAshrae allowable範囲内です。つまり、コールドエリアの温湿度は１日を通じて安定していたことになります。

空調SAファンの制御

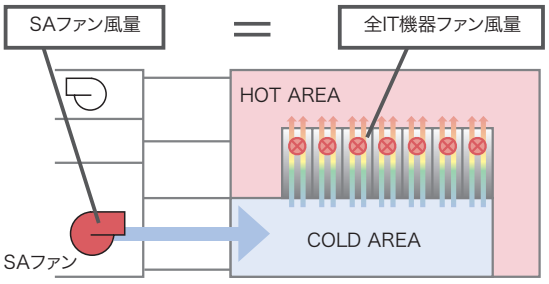


図-13 最も効率的で省エネルギーが実現できる風量の関係

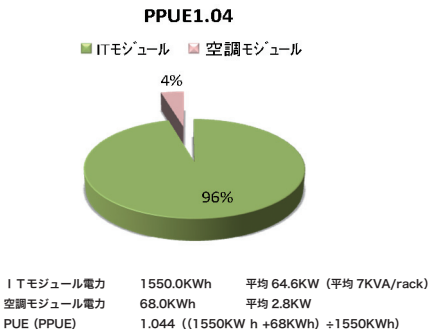


図-15 4月6日のPPUE

■消費電力
IT消費電力 : 1550.0kWh（平均64.6kW）
空調消費電力： 68.0kWh
PUE : 1.044

■空調機運転モード
1.外気 : 29.4% 7時間02分
2.混合 : 70.6% 16時間56分
3.循環 : 0.0% 0時間00分

■FAN風量（SA）
最高風量： 18533m^3/h / 最低風量： 12727m^3/h / 平均風量： 14627m^3/h
加湿器給水量： 0.00m^3

■外気状態
最高気温： 23.5度 / 最低気温： 12.3度 / 平均気温： 17.0度
最高湿度： 92.7% / 最低湿度： 43.5% / 平均湿度： 71.8%

図-14 4月6日の運転レポート

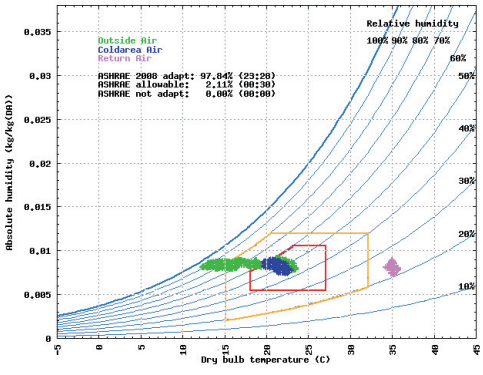


図-16 4月6日の空気線図

さらに、図-17に示すように、混合運転モードと外気運転モードのモード切替時にも温湿度は安定し、Ashrae2008の範囲内にあります。

外気運転モードと混合運転モードでは、図-18に示すようなダンパ制御で温湿度を調整しています。コールドエリアに設置している温湿度センサーの情報をDDC(Direct Digital Controller: 空調機制御装置)がリアルタイムで取得し、外気吸気ダンパ、排熱ダンパ、混合ダンパの開度を調整します。実験結果で温度と湿度が安定しAshrae2008の範囲内に温湿度が収まっているということは、一連のダンパ制御が適正に行われていることを示しています。

また、外気運転モードや混合運転モードに欠かせない機能に加湿制御があります。図-19は、4月30日の運転レポートです。この日は外気の絶対湿度(乾き空気1 kg中に含まれる水蒸気量)が低かったため、コールドエリアの温湿度をAshrae2008範囲内にするために気化式加湿器が動作しています。

気化式加湿器は、加湿材の上部から水を流し、空気の通過による自然蒸発で加湿します。図-20は4月30日の空気線図です。コールドエリア(青)のプロットがAshrae2008の範囲内を推移していることから、過加湿や加湿不足が発生することなく、加湿制御が適正に行われていることが分かります。

4.3.3 循環運転モード

6月～8月には、循環運転モードでのさまざまなデータが取得できました。ここでは、7月6日のデータを元に実証実験の結果を報告します。図-21に、7月6日の運転レポートを示します。この日は、1日をとおして循環運転モードになっています。

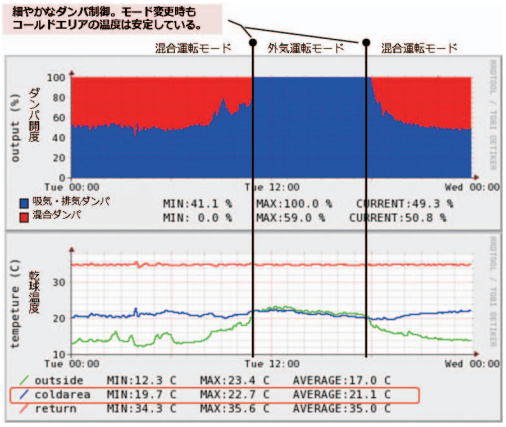


図-17 ダンパ開度と温度推移

図-19 4月30日の運転レポート

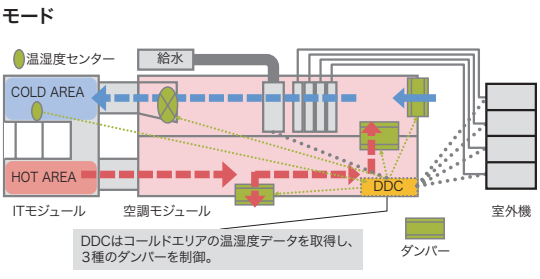


図-18 DDCとダンパ

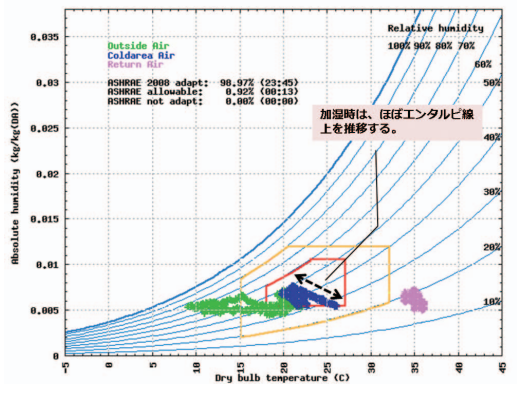


図-20 4月30日の空気線図

外気の最高温度が30.6℃、平均温度が27℃、ITモジュール負荷が63.7KW（最大90KWの70%）であった７月６日の空調モジュール電力は、図-22に示すように全電力の22％で、PPUE＝1.284でした。７月６日以外の日での循環運転モードでは、PPUE＝1.24 ～1.30を記録しています。PPUEの変動が大きい理由は、室外機の電力が「外気温湿度」や「ＩＴモジュール負荷」によって変動するためです。

図-23は、7月6日の空気線図です。コールドエリアの温湿度（青）がAshrae2008範囲内を推移しています。また、図-24に示すとおり、ITモジュールのコールドエリア、ホットエリアの温度、相対湿度、絶対湿度のいずれもが安定しています。

循環運転モードでは、外気を遮断することでより効率のよい運転が可能です。また、何らかの異常によって高湿、高温な外気が流入しても、ITモジュールの温湿度が乱高下しないように、室外機の除湿、冷却機能を制御する機能も実装しています。さらに、室外機の出力と稼働台数を変えて、複数の運転パターンでの実験を行い、室外機の総消費電力が最小となるようにDDCが室外機を制御する機能も実装しています（図-25）。

```
■消費電力
IT消費電力   : 1529.0kWh (平均63.7kW)
空調消費電力:  434.0kWh
PUE          :    1.284

■空調機運転モード
1.外気              :  0.0%  0時間00分
2.混合              :  0.0%  0時間00分
3.循環              : 99.9% 23時間59分
■外気状態
乾球温度 最高: 30.6度 / 最低: 25.5度 / 平均: 27.0度
相対湿度 最高: 99.5%  / 最低: 68.2%  / 平均: 89.9%
絶対湿度 最高: 22.2g  / 最低: 18.1g  / 平均: 20.3g
```

図-21　7月6日の運転レポート

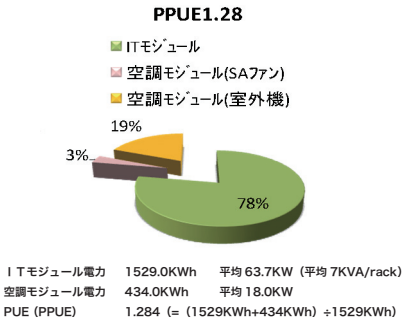


図-22　7月6日のPPUE

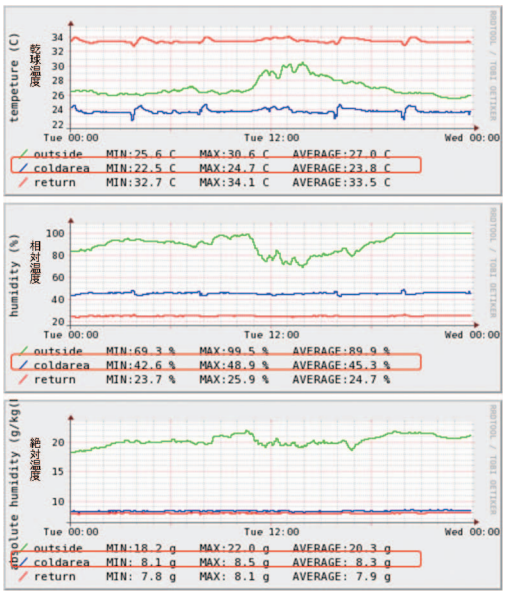


図-24　乾球温度、相対湿度、絶対湿度の推移

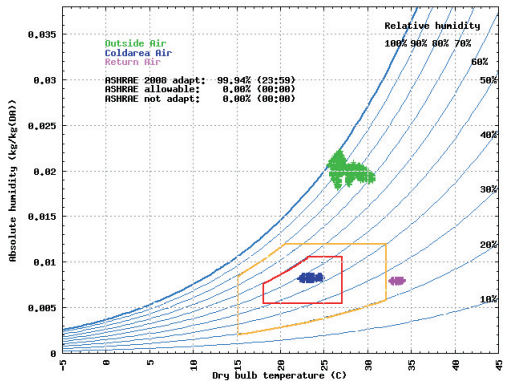


図-23　7月6日の空気線図

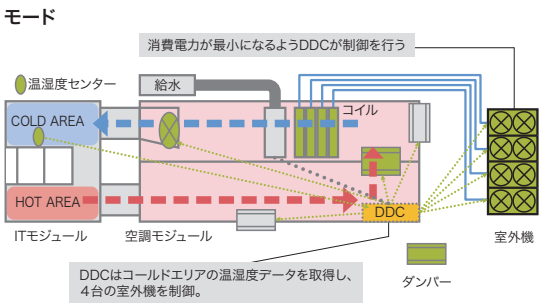


図-25　DDCと室外機

4.4 今後に向けて

4.4.1 さらなる省エネルギー化への課題

外気冷却方式による省エネの実用性のめどはつきましたが、さらなる省エネ化に向けて、次のようなSTEPで中長期的に検討、実証を行っていく予定です。

STEP1 既存の仕組みの拡張（たとえば、夏期も外気運転モードとすることで消費電力を削減する）

STEP2 空調設備とIT機器の融合（たとえば、空調設備とIT機器がそれぞれFANを持ち、独立して温度制御をしているため、一体的に制御させて、二重にあるFANを削減する）

STEP3 カーボンニュートラルデータセンターの実現（たとえば、自然エネルギー（風力、太陽光等）を利用した発電設備とデータセンター設備を一体的に構築運用することにより、CO_2が発生しない電力を利用できる仕組みを作る）

まず、最初のステップとして、2010年8月に行った夏期の外気運転モードでの実証実験の概要を報告します。

夏期でも、循環運転モードを使わずに、消費電力の少ない外気運転モードを使い、通年でPPUEを1.1以下にすることを目標に、複数のIT機器ベンダの協力を得て、実験を実施しました。24時間強制的に外気運転モードにしたため、コールドエリアは外気と同じ温度になり、最高で35度を超える室温となりましたが（そのときホットエリアは45度になります）、表3の通り、PPUEは、1.25から1.06と大幅に改善しました。しかし、消費電力の合計は、70kwが約6%減り、66kwになっただけでした。空調の消費電力が10kw減った分、室温が高温になることでIT機器のFANの回転数が増え消費電力が6kw増えたため（一般にサーバのFANの消費電力は吸い込み口温度が25度を超えると大きく増加していきます）、差し引き4kwしか消費電力は減らなかったのです。空調機器の消費電力が減り、IT機器の消費電力は変わらずに、PPUE1.07になることを期待していたのですが、PPUEは期待通りでも、全体の消費電力は大きくは削減できないということが定量的に測定できたことは大きな成果だと考えています。

表-3 夏期の循環運転モードと外気運転モードの消費電力

	循環運転モード	外気運転モード		
	実測値	期待値		実測値
IT機器消費電力	56kw	56kw	+6kw	62kw
空調機器消費電力	14kw	▲10kw 4kw		4kw
合計	70kw	▲4kw 60kw	+6kw	66kw
Partial PUE	1.25	▲0.19 1.07	▲0.01	1.06

FANの回転数が上がり消費電力が増加した

消費電力は期待値より増加

PUEは期待値を下回った

今後、実験で得たデータの分析を、IT機器ベンダ、空調機器ベンダと進めていきますが、次のステップである空調機器とIT機器の融合につながるデータが得られることを期待しています。

また、従来から言われていることですが、PUEの改善が、必ずしも省エネにつながるものではなく、きめ細やかな省エネを進める場合の指標としては、PUE以外の指標が必要だということを再認識しました。

4.4.2 商用化に向けた松江データセンターパークの構築

実験で実証した技術を実運用に適用すべく、商用として国内初の外気冷却コンテナユニットによるデータセンター「松江データセンターパーク」の構築を、2011年4月の稼動開始を目指し、行政の産業振興施策に基づく投資助成、電力料金補助などのバックアップを受け、2010年9月1日より開始しました。

データセンターパークは、クラウドサービスのニーズに応えるために、建物、電気設備、空調設備、IT設備が融合し、モジュール化された各種リソースが集積する場であり、第１世代である松江データセンターパークは、クラウドサービスIIJ GIOのベースとなるファシリティとして、低コスト、高いサーバ収容効率や容易なスケールアウトを実現する日本初のコンテナ型データセンターで、主な特長は以下の通りです。

- 外気冷却方式の採用
- 独自開発のITモジュール「IZmo（イズモ）」（特許出願中）の利用
- データセンターコンポーネントの効率的な配置

松江データセンターパークでは、実証実験の結果を生かした高効率の外気冷却方式を実装しています。また、ITモジュールでは、外気を供給するダクトとモジュール筐体を一体化することにで、設備コストを低減しています。さらに、モジュール内をホットエリアとコールドエリアに分離することで、空調効率を高め、すべてのラッ

クで実効10KVAまでの電力消費を可能にし、電気代などのランニングコストを低減しています。これらに加えて、モジュール内に設置するラックを傾斜配置することで、ITモジュールの幅を2.5m以下にしつつ、必要な内部スペースも確保しています。これらにより、トレーラー等の特殊車両ではなく通常の大型トラックでの運搬が可能となり、輸送コストを約1/3まで低減できます。

さらに、データセンターに用いるコンテナは、建築基準法第2条の建築物に該当しないことを国土交通省が検討しており、「建築物ではない設備機器」というコンセプトをいち早く取り入れ、IT機器の電源のON/OFFや状態表示ランプの確認などをリモートから行うためのさまざまな機能も実装します。

松江データセンターパークでは、ITモジュールの前後に電気設備と空調モジュールを配置する独自の方式「MISP（Module Inter-connection over the Shortest Path）」を採用しています。これにより、電源配線、冷媒配管などの接続距離を最短にすることができ、配線などから生じるエネルギーロスや設備に関わる投資コストを低減しています。

4.5 おわりに

データセンターの省エネ化を目的とした今回の実証実験は、第一世代の松江データセンターパークの構築という形でひとまず結実しますが、空調設備とIT機器の融合、カーボンニュートラルなデータセンターの実現に向け、商用での運用ノウハウを蓄積し、第２、第3世代のデータセンターパークを実現すべく、今後も先進的な取り組みを継続していきます。

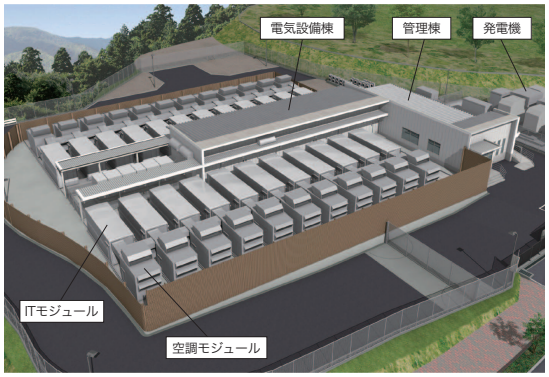


図-26 松江データセンターパークイメージ図

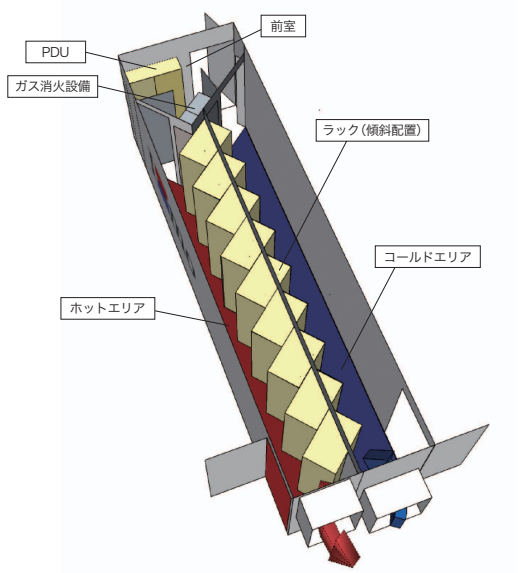


図-27 ITモジュール「IZmo」イメージ図

執筆者：
4.1/4.4
久保 力（くぼ いさお）
IIJ サービス本部 データセンターサービス部 副部長
大手キャリアを経て（株）クロスウェイブコミュニケーションズへ入社し、NTTのダークファイバを使用した相互接続を全国数十箇所で実現（日本初）。2008年IIJへ入社し、既存のデータセンターの運用、拡張を進めるとともに、次世代データセンター構築の統括を行う。

4.2
川島 英明（かわしま ひであき）
IIJ サービス本部 データセンターサービス部 事業企画課 課長
2002年IIJ入社。SEIL/SMFの販売促進、ネットワークインテグレーション部における大規模案件の構築業務を経て、2009年度よりデータセンター事業の企画業務に従事。

4.3
橋本 明大（はしもと あきお）
IIJ サービス本部 データセンターサービス部 事業企画課
キャリア系通信基地局の設計・構築・運用及びデータセンターのファシリティエンジニアを経て2009年IIJに入社。現在は、次世代データセンターの検討・設計・構築に従事。

Ongoing Innovation

Vol.9 November 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-MKTG019IA-1011KO-08000PR