Internet Infrastructure Review

IIJ
Internet Initiative Japan

Vol.4

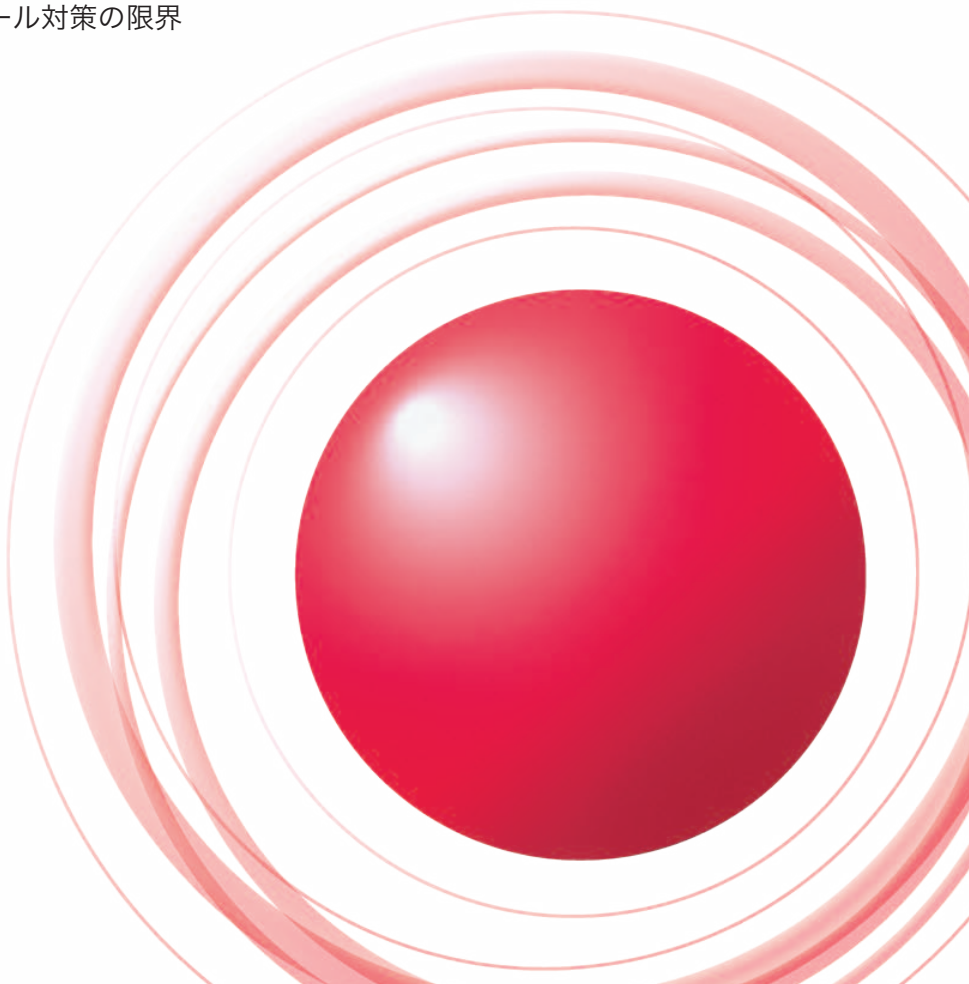
August
2009

インフラストラクチャ セキュリティ
多様化するマルウェア感染

ブロードバンド トラフィック
増大する一般ユーザのトラフィック

クラウドコンピューティング テクノロジー
分散システム dddの実装と活用

メッセージング テクノロジー
ボットネット管理元遮断による迷惑メール対策の限界



Internet Infrastructure Review Vol.4 August 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

7月10日に総務省より公開された情報通信白書平成21年度版では、冒頭に「日本復活になぜ情報通信が必要なのか」という特集が組まれています。この中で、情報通信が経済、社会の成長に寄与できることが示されている一方で、日本は世界最高水準の情報通信基盤を有していながら利活用に遅れが見られ、情報通信を経済力に結び付けられていないと分析されています。さらに、民間部門、あるいは、政府や地方公共団体などの公共部門で、情報通信基盤の利活用促進と、活用に関する不安を払拭することで、経済危機からの脱却を推し進めることができるとの提言がなされています。

この技術レポートIIRも今号で4回目の発行です。このVol.4においては、先の白書で経済発展の鍵とされている、利活用の状況や安全性について、インターネットの技術基盤を担う立場から、主に2009年4月から6月の間の統計情報をもとにまとめています。

まず、利活用の面では「ブロードバンドトラフィック」において、世界最高水準のブロードバンド環境の利用実態について、トラフィック面から解析を行っています。5年前のデータとの比較では、P2Pファイル共有等を利用するヘビーユーザを除いた一般の利用者でも、動画等リッチコンテンツの活発な利用により、1日の平均利用量がダウンロード側で32MBから114MBへと、実に356%もの上昇を示しています。

安全性の面では、「インフラストラクチャセキュリティ」において、大規模な感染が続いているマルウェアConfickerと、Webを閲覧しただけで感染し、情報を盗み出すとともに、変異や証拠の隠滅等の巧妙な活動を行うGumblarについて、解説を行っています。また、「メッセージングテクノロジー」においては、Vol.3に引き続いて、迷惑メールの削減のために、送信側の対策の重要性と送信ドメイン認証技術について現状を説明しています。

また、本号では基盤技術の分野で注目を集めているクラウドコンピューティングについて取り上げています。この分野では、GoogleやAmazon、Microsoft等の海外企業が先行していますが、国内でも官民をあげた活用の検討が開始されており、IIJもその中で大きな役割を果たすべく、技術開発を進めています。「クラウドコンピューティングテクノロジー」では、クラウド環境の基盤となる分散ファイルシステムに関するIIJの取り組みを紹介するとともに、「インフラストラクチャセキュリティ」において、クラウドコンピューティングにおけるセキュリティを取り上げています。

情報通信を有効に活用する上では、安全に活用するためのセキュリティ確保が必要不可欠であることは論を待ちません。7月にはアメリカおよび韓国の政府機関や重要なWebサイトが大規模なDDoS（Distributed Denial of Service）攻撃を受け、一部のサイトがアクセス不能となり、社会活動に大きな影響が生じたと報道がありました。このような事件を防ぎ、情報通信基盤が社会基盤として安定して稼動するためには、IIRで示しているような、実態に関する認識の共有を出発点に、情報通信基盤の運営に携わる各機関での連携した対応が不可欠です。

IIJでは、積極的に新規技術を取り入れながら安定性、安全性を考慮したインターネットの基盤をご提供するとともに、情報発信と関係機関と連携した取り組みを継続し、インターネットが社会を豊かにするためのインフラとして、今まで以上に有益なものとなるよう、努力してまいります。

執筆者：
島上 純一（しまがみ じゅんいち）
IIJ 取締役ネットワークサービス本部長。IIJのバックボーンネットワークや、アジア太平洋地域の各国を相互接続する国際インターネット回線網A-Boneのインフラ構築、運用を行う。現在は、バックボーン運用だけでなく、インターネット接続やメール、WWWのアプリケーションアウトソースなど、IIJのISPサービスを統括する。

1 インフラストラクチャセキュリティ

1.1 はじめに

このレポートは、IIJ自身がインターネットの安定運用のために取得している一般情報や、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もとに、IIJが対応したインシデントについてまとめたものです。

このVol.4では、2009年4月より6月までの3ヵ月間を対象としています。この期間においても様々なインシデントが発生していますが、ここではその中から代表的なものを紹介します。

この期間には、昨年より流行しているマルウェアConfickerの亜種の感染が、数多く報告されています。また、コンテンツ書き換えにより、Webを閲覧するだけで感染し、ID・パスワード等の情報を盗み出すマルウェアの流行がありました。

脆弱性の分野では、Adobe ReaderやApple QuickTimeなど、ブラウザのプラグインとして動作するソフトウェアの脆弱性が相次いで発見され、悪用事例も報告されています。

国際的には、中国で発生したDNSサーバに対する攻撃や、イランの大統領選挙に関連したDDoS攻撃など、多くの利用者に影響を与えるインシデントが発生しています。

IIJの観測では、インターネット上のマルウェアの活動、DDoS攻撃、Webサーバに対するSQLインジェクション攻撃は、従来の規模で継続しています。

以上のように、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

ここでは、2009年4月から6月の期間にIIJが取り扱ったインシデントについて、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、分類の説明について表-1に示します。

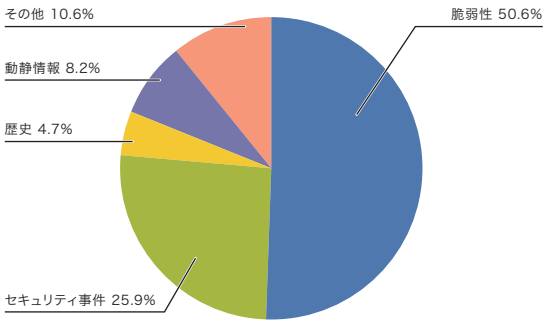


図-1　カテゴリ別比率（2009年4月～6月）

表-1　インシデントの分類

カテゴリ名	内容
脆弱性	インターネットで利用している、または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します。脆弱性そのものや、脆弱性に対する攻撃の情報、ベンダによる脆弱性への対応情報、対応作業等が該当します。
動静情報	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します。要人による国際会議や、国際紛争に起因する攻撃等への対応で、注意・警戒、インシデントの検知、対策といった作業が該当します。
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します。
セキュリティ事件	突発的に発生したインシデントとその対応を示します。ネットワークワーム等のマルウェアの活性化や、特定サイトへのDDoS攻撃等で、原因のはっきりしないインシデントへの対応が含まれます。
その他	上記のいずれにも該当しないインシデントを示します。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等も含まれています。

■脆弱性

この期間では、ワードパッド及びOffice テキスト コンバーターの脆弱性[*1]、Microsoft Office PowerPointの脆弱性[*2]など、ユーザの利用するアプリケーションの脆弱性が発見されています。加えて、Adobe Acrobat及びAdobe Reader[*3][*4]、Apple QuickTimeの複数の脆弱性[*5]等、Webブラウザから起動されるアプリケーションに関連する脆弱性が多く発見され、先に発見されていたFlash Playerの脆弱性[*6]などとともに悪用されました。また仮想化ソフトのVMwareにも複数の脆弱性[*7]が発見されています。

■動静情報

IIJでは、国際情勢や時事に関連した各種動静情報に注意を払っています。この期間では、特に北朝鮮によるミサイル発射関連の動き、新型インフルエンザの世界的な発生、およびイランの大統領選挙等の、国際情勢や各種動静情報に注意を払いました。新型インフルエンザ関連では、国内での感染者発生に伴い、注意喚起を装ったマルウェアの添付されたメールが送られる事例[*8]が発生しました。

イランの大統領選挙に関しては、選挙結果における不満からイラン国内に対してDDoS攻撃が発生したという情報がありました[*9]。また、5月及び6月の外国要人来日では警戒を行う等の対応を行いましたが、直接関連する攻撃は検出されませんでした。

■歴史

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などが発生していましたが、この期間においてはIIJの設備及び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、まず、Conficker亜種の感染拡大が観測されています。この件については「1.4.1 マルウェア Conficker の世界的流行」も併せてご参照ください。

また、改ざんされたWebコンテンツを参照することで感染し、ID・パスワード等を盗み出すマルウェアGumblarについて、数多くの感染事例が報告されています。この件についても「1.4.2 ID・パスワード等を盗むマルウェア Gumblar」としてまとめていますので、併せてご参照ください。

＊1　マイクロソフトセキュリティ情報MS09-010、ワードパッド及びOffice テキスト コンバーターの脆弱性（http://www.microsoft.com/japan/technet/security/bulletin/ms09-010.mspx）。
＊2　マイクロソフトセキュリティ情報MS09-017、Microsoft Office PowerPointの脆弱性により、リモートでコードが実行される（http://www.microsoft.com/japan/technet/security/bulletin/ms09-017.mspx）。
＊3　2009年5月Adobeセキュリティ情報APSB09-06（http://www.adobe.com/jp/support/security/bulletins/apsb09-06.html）。
＊4　2009年6月Adobeセキュリティ情報APSB09-07（http://www.adobe.com/jp/support/security/bulletins/apsb09-07.html）。
＊5　QuickTime 7.6.2のセキュリティコンテンツについて（http://support.apple.com/kb/HT3591?viewlocale=ja_JP）。
＊6　2009年2月Adobeセキュリティ情報APSB09-01（http://www.adobe.com/jp/support/security/bulletins/apsb09-01.html）。
＊7　ゲストOS上のユーザが、ホストOS上で任意のコードを実行する可能性がある等（http://www.vmware.com/security/advisories/VMSA-2009-0006.html）。
＊8　国立感染症研究所による注意喚起、「国立感染症研究所」を詐称したブタインフルエンザ関連メールにご注意ください（http://www.nih.go.jp/niid/misc/warning090428.html）。
＊9　攻撃の様子については、例えば次のblog等に詳しい。Arbor network社のTHE ARBOR NETWORK SECURITY BLOG:Iran DDoS Activity: Chatter, Tools and Traffic Rates（http://asert.arbornetworks.com/2009/06/iran-ddos-activity-chatter-tools-and-traffic-rates/）。

4月には、大きなサイズの応答を得るDNSクエリを大量に発生させることで、DNSキャッシュサーバに負荷を与える攻撃が複数観測されています[*10]。また、5月には、中国国内でDNSサーバに対するDDoS攻撃が発生し、数時間に渡って広範囲の障害を起こしています[*11]。加えて、いくつかのHTTPサーバに影響するDoS攻撃ツール[*12]が公開され、イランにおけるDDoS攻撃に悪用されたという情報がありました[*13]。

■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、Googleにかかわる経路情報の不具合により、世界的なトラフィック減があったことが注目されました[*14]。また、IP電話に無言電話が着信する可能性のあるSIPの通信を、断続的に観測しています。

1.3 インシデントサーベイ

IIJでは、インターネット上で発生するインシデントのうち、インフラストラクチャ全体に影響を与える可能性があるインシデントに注目し、継続的に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、調査と分析の結果を示します。

1.3.1 DDoS攻撃

今日では、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ることや、サーバの処理を過負荷にすることで、サービスを妨害するという目的を達成しようとします。

＊10 このDNSキャッシュサーバへの攻撃については、例えば以下から始まるDNS OARCでの議論を参照のこと（https://lists.dns-oarc.net/pipermail/dns-operations/2009-April/003779.html）。

＊11 本件については、例えば次の報道がある（http://www.networkworld.com/news/2009/052109-dns-attack-downs-internet-in.html）。

＊12 この手法では、HTTPリクエストの一部分のみをサーバに送付し、リクエストを完成させないまま接続を保持することでWebサーバの負荷を上げる。技術詳細は作者自身による解説が最も詳しい（http://ha.ckers.org/slowloris/）。この問題の影響を受けるかどうかと、その対策方法は実装により異なるため、利用中のWebサーバの対策情報を参照のこと。

＊13 例えば SANS ISC のHandler's Diary: Slowloris and Iranian DDoS attacks（http://isc.sans.org/diary.html?storyid=6622）。

＊14 この事故による通信への影響については Arbor network社のTHE ARBOR NETWORK SECURITY BLOG: The Great GoogleLapse（http://asert.arbornetworks.com/2009/05/the-great-googlelapse/）に詳しい。Google向けのトラフィックがアジア（日本）に向かったとする情報もあるが、詳細は不明。IIJではこの時間帯に経路情報やトラフィックの異常は観測していない。

ここで、2009年4月から6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、図-2に示します。

この情報は、IIJ DDoS対策サービスの基準で、攻撃と判定された通信異常を件数で示したものです。IIJでは、この他の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。加えて、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、その影響が異なります。図-2の集計では、DDoS攻撃全体を、回線容量に対する攻撃*15、サーバに対する攻撃*16、複合攻撃(1つの攻撃対象に対し、同時に数種類の攻撃を行うもの)の3種類に分類しています。

この3ヵ月の期間中、IIJでは114件のDDoS攻撃に対処しました。1日あたりでは1.25件程度となり、平均発生件数は前回のレポートの期間よりも減少しています。全体の内訳は、回線容量に対する攻撃が1%、サーバに対する攻撃が86%、複合攻撃が13%です。最大規模のSYN floodで67,000pps程度であり、回線への攻撃の最大規模は125Mbps程度でした。この期間中、150,000pps以上のパケット数によるICMP floodが観測されていますが、個々のパケットが小さかったため、回線容量への影響は77Mbps程度となっています。また、攻撃の継続時間については、全体の83%が攻撃開始から30分未満で終了し、17%が30分以上24時間未満の範囲で分布しています。この期間中では、24時間以上継続する攻撃は見られませんでした。

攻撃元の分布については、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*17や、ボットネット*18の利用によるものと考えられます。

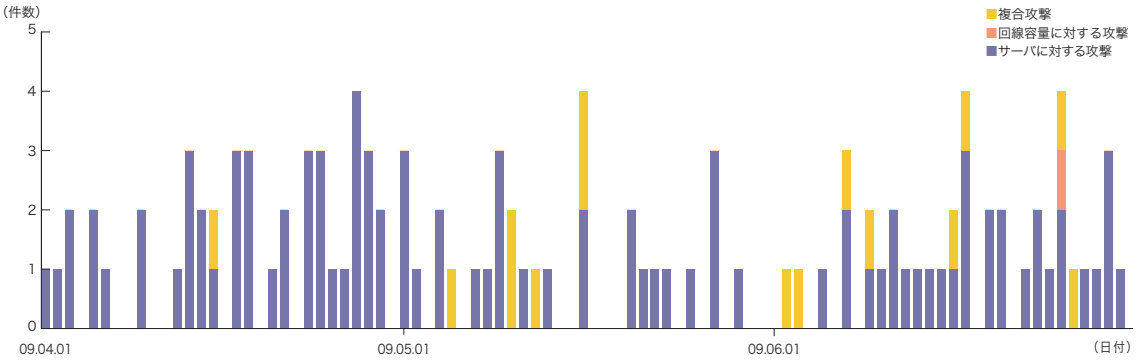


図-2　DDoS攻撃の発生件数

*15 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。

*16 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。

*17 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。

*18 ボットとは、感染後に外部のC&Cサーバからの命令を受けて攻撃を実行するマルウェアの一種。ボットが多数集まって構成されたネットワークをボットネットと呼ぶ。

1.3.2 マルウェアの活動

ここでは、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*19]による観測結果を示します。MITFでは、インターネットに一般利用者と同様に接続したハニーポット[*20]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、攻撃先を探す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

まず、2009年4月から6月の期間中に、ハニーポットに到着した通信の総量（到着パケット数）の推移を図-3に、その発信元IPアドレスの分布を、国別に図-4に示します。ここではハニーポット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）について、全期間の推移を示しています。

この期間では、マイクロソフトのOSで利用されている通信や、P2Pファイル共有ソフトウェアの6881/UDP、PCリモート管理ツール[*21]の4899/TCP、シマンテックのクライアントソフトウエアの2967/TCP等、クライアントに対する探索行為が数多く観測されています。一方で、10044/UDPのように、目的不明の通信も観測されています。また、445/TCPなどMS08-067[*22]で示される脆弱性を狙った攻撃が、昨年10月以来継続しています。

全体の発信元の分布を国別に見ると、中国の29.2%、日本国内の20.3%、が比較的多くなっています。

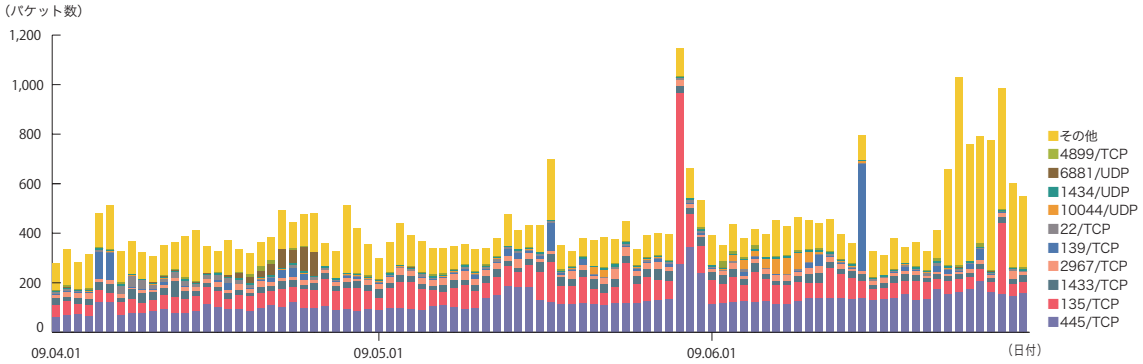


図-3　ハニーポットに到着した通信の推移（日別・宛先ポート別・一台あたり）

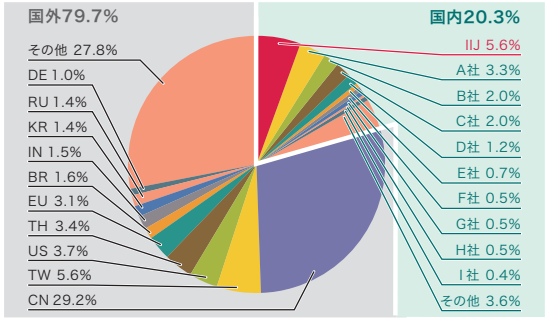


図-4　発信元の分布（全期間）

＊19 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。

＊20 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。

＊21 同様の探索行為については、同時期に他の組織においても観測されている。例えば SANS ISC のHandler's Diary: TCP scanning increase for 4899 (http://isc.sans.org/diary.html?storyid=6637)。

＊22 マイクロソフト セキュリティ情報 MS08-067、緊急:Server サービスの脆弱性により、リモートでコードが実行される (http://www.microsoft.com/japan/technet/security/bulletin/ms08-067.mspx)。

■ネットワーク上でのマルウェアの活動

次に、MITFで観測したマルウェアの活動について示します。同じ期間中における、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に示します。取得検体数の推移では、総取得検体数は、1日あたりに取得できた検体[*23]の総数を示し、ユニーク検体数は、検体の種類をハッシュ値[*24]で分類したものです。

期間中の一日平均としては、総取得検体数で708検体を、種類で60種類程度のマルウェアを取得しています。前回の集計期間では、一日平均の総取得検体数で899検体、種類では44種類でしたので、この期間中では、総取得検体数が減少傾向にありますが、種類においてはその水準を維持しています。

検体取得元の分布では、日本国外が43.2%、国内が56.8%であり、全体のうちIIJのユーザ同士のマルウェア感染活動が16.8%となっています。これは、依然としてマルウェアの感染活動が、非常に局所的であることを示しています。

MITFでは、マルウェアの解析環境を用意し、取得できた検体について独自の解析を行っています。この結果、この期間に取得できた検体の内訳は、ワーム型5%、ボット型59%、ダウンローダ型36%となりました。また、この解析により、81個のボットネットC&Cサーバ[*25]と、528個のマルウェア配布サイトの存在を確認しています。

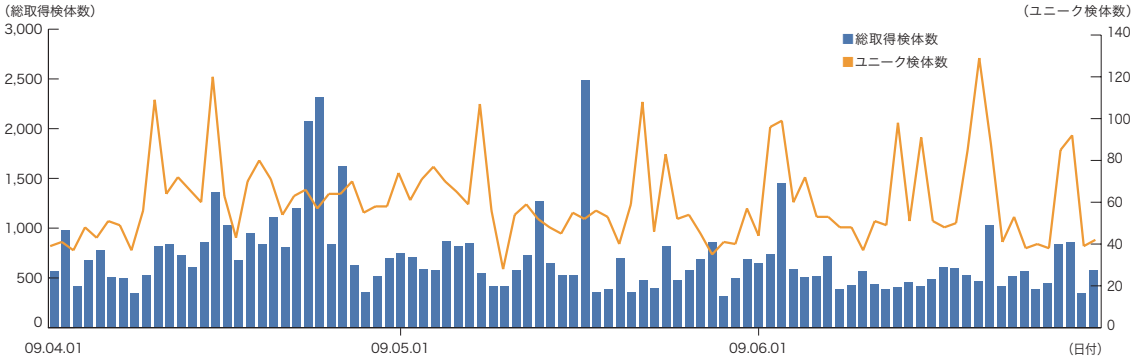


図-5　取得検体数の推移(総数・ユニーク検体数)

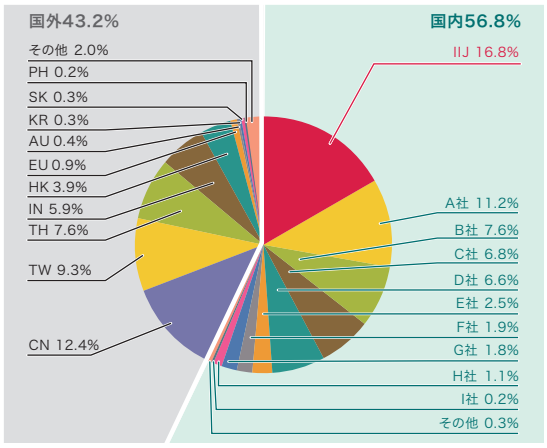


図-6　検体取得元の分布(全期間)

＊23 ここでは、ハニーポット等で取得したマルウェアを指す。

＊24 様々な入力に対して一定長の出力をする一方向性関数(ハッシュ関数)を用いて得られた値。ハッシュ関数は異なる入力に対しては可能な限り異なる出力を得られるよう設計されている。難読化やパディング等により、同じマルウェアでも異なるハッシュ値を持つ検体を簡単に作成できてしまうため、ハッシュ値で検体の一意性を保証することはできないが、MITFではこの事実を考慮したうえで指標として採用している。

＊25 Command & Controlサーバの略。多数のボットで構成されたボットネットに指令を与えるサーバ。

1.3.3 SQLインジェクション攻撃

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃*26について継続的な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ついては、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。

まず、2009年4月から6月の期間中に検知した、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についてまとめたものです。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、前回のレポートの水準を維持しています。4月3日に発生している大量の検出は、特定のWebサーバに対するもので、南米の多数のIPアドレスを送信元とした攻撃が、それぞれの送信元から同じ数だけ観測されており、ボットネットを利用した攻撃であることが窺えます。6月7日に発生した大量攻撃は、中国の特定のアドレスから特定のWebサーバに対するものでした。発信元の分布では、日本39.4%、中国34.4%、米国4.9%となり、以下その他の国が続いています。

以上の攻撃について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おり、引き続き注意が必要な状況です。

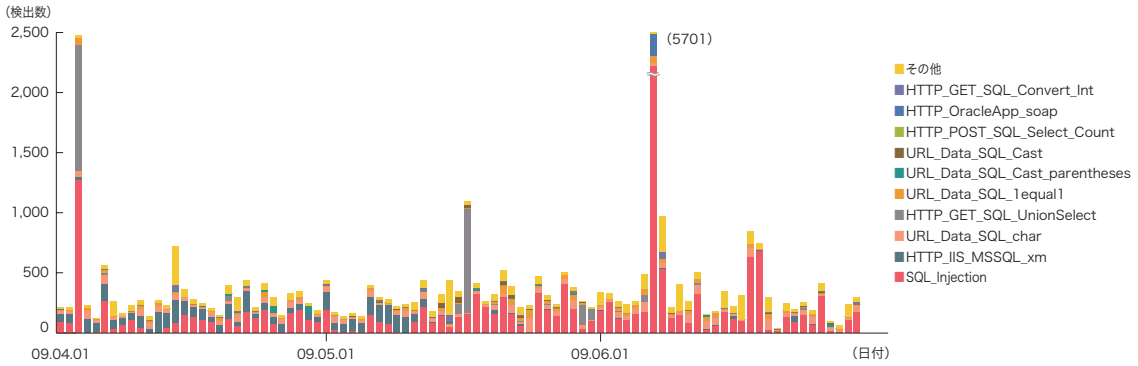


図-7　SQLインジェクション攻撃の推移(日別・攻撃種類別)

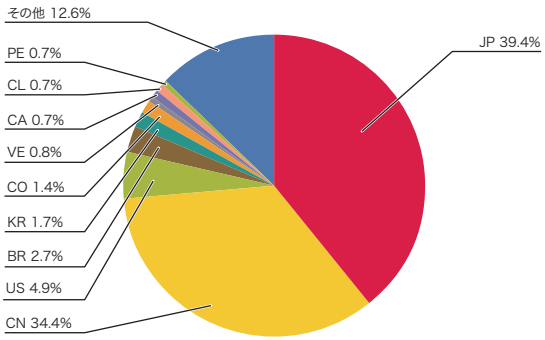


図-8　SQLインジェクション攻撃の発信元の分布

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

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を行うことで対策につなげています。ここでは、この期間に実施した調査のうち、マルウェア Conficker の世界的流行、ID・パスワード等を盗むマルウェア Gumblar、クラウドコンピューティングとセキュリティについて示します。

1.4.1 マルウェアConfickerの世界的流行

■Confickerとは

Confickerは2008年11月から流行しているマルウェアです。数々の亜種の登場により、現在でもその感染規模は拡大しており、5月に米国大統領談話[*27]で言及されるなど、大きく注目されています。ここでは、このConfickerとその感染拡大についてまとめます。

■Confickerの亜種とその動作

本稿執筆時点で存在が確認されているConfickerの亜種と、その特徴について表-2に示します[*28]。以下ではそれぞれの機能について紹介します。

■感染活動

Confickerはまず、MS08-067で示された脆弱性を利用して、ネットワーク経由の感染活動を行います。また、USBメモリ等で利用される自動実行の仕組みを悪用し、ファイアウォール等の、境界防御を設定したネットワークの内部に対する感染活動を行います。さらに、Windowsファイル共有で設定されている管理共有ADMIN$の認証情報に対して辞書攻撃[*29]を行い、成功した場合はファイル共有を通じて組織内ネットワーク上に伝播します。

■制御とアップデート

ConfickerはHTTPを利用してアップデートを行います。アップデートに利用されるWebサーバのURLのドメイン部は、時刻をもとにしてあるアルゴリズムで生成された、複数の文字列によって決定されます（1日あたり250から50,000種類）。感染PCを操ろうとする者は、このアルゴリズムによって、ある特定の日に感染PCがアクセスを試みるURLを事前に知ることができ、そのドメインを取得することで、制御を行います。

表-2　Confickerの亜種

名称	発見日	特徴
Conficker.A	2008/11/21	●MS08-067で示される脆弱性を利用して感染活動を行う。 ●1日あたり250 URLを生成してアクセスし、アップデートを試みる。
Conficker.B	2008/12/29	同上 ●USBメモリなどの自動実行機能を悪用して感染する。 ●Windowsのファイル共有を経由した感染を試みる。
Conficker.C（B++）	2009/2/20	同上 ●P2P通信を実装し、それを通じてアップデートを試みる。
Conficker.D（C）	2009/3/4	●同上だが、1日あたり50,000 URLを生成し、そのうち500 URLにアクセスを試みる。 ●また、P2P通信に変更が加えられた。
Conficker.E	2009/4/8	●同上だがネットワーク経由等の感染機能は持たない。 ●Conficker.C もしくは D から、P2P 通信を利用してアップデートされた。 ●別のマルウェア（例えば Waledac やスケアウェア）をダウンロードする。 ●5 月 3 日に自己削除を行う（5 月 3 日に削除されていないという情報もある）。

＊27 全文は次で参照できる。REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE（http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/）。

＊28 この表は極力直接得た情報をもとに作成しているが、IIJではすべての亜種の検体を取得しているわけでなく、不足している情報については（http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline）などの公開情報をもとにしている。ConfickerはDownadupと呼ばれることもあり、その亜種の呼び方についても、ウイルス対策ソフトベンダや、時期によって異なる場合がある。また、脆弱性とConficker.AについてはIIR Vol2「1.4.2 MS08-067を悪用するマルウェア」も合わせて参照のこと（http://www.iij.ad.jp/development/iir/pdf/iir_vol02.pdf）。

＊29 辞書攻撃とは、あらかじめ用意した辞書（一般名詞や機械的に生成した文字列などで構成される辞書）の内容を、一つずつ試すことで、正当なパスワードを見つけ出す試み。

また、いくつかの亜種ではP2P通信によるアップデートの機能が搭載されています。この機能を持つConfickerが利用するP2P通信は、初期状態や中央サーバ等を必要としない純粋なP2P通信で、通信の一極集中が発生しないため、発見が困難となっています。実際に、Conficker.EはこのP2P通信により伝播したとされています。

■他のマルウェアの導入

Conficker.Eでは、感染したPCをWaledac[*30]等のボットに感染させようと試みます。この試みが成功すれば、ボットネットの一部として悪用されてしまう可能性があります。

■流行の様子

Confickerは以上の機能を利用して感染を拡大しています。特に国内においては、USBメモリ経由の感染や、ファイル共有を悪用した手法で、企業等の組織内ネットワークにおいて大規模に感染活動を行いました。また、Conficker.Dが4月1日に大きく挙動を変えることが発見され、広く注目[*31]されましたが、IIJでは当日、通信上の異常を確認できませんでした。図-9では、MITFにおけるConficker.Dの感染活動の観測回数の総数を示しています[*32]。この図で示されるように、日本国内においてはほとんど感染活動は見られませんが、中国、ブラジル、ヨーロッパ、ロシア、米国の順で感染活動が多いことが分かります。Conficker Working Group[*33]によると、本稿執筆時点で、すべての亜種の合計感染台数は500万台を越える[*34]としています。

以上にまとめたように、Confickerは現在でも全世界で多数の感染が確認されており、数多くのPCが悪用される状態にあることを示しています。これは、インターネット全体にとって非常に大きな脅威であるといえるでしょう。このため、多くのセキュリティベンダや研究者たちによる、協調対策活動が行われています[*35]。制御の仕組みの問題や対策活動の成果として、現時点では500万台ものPCが、一斉に操られるような事態にはいたっていませんが、予断を許さない状況が継続しています。

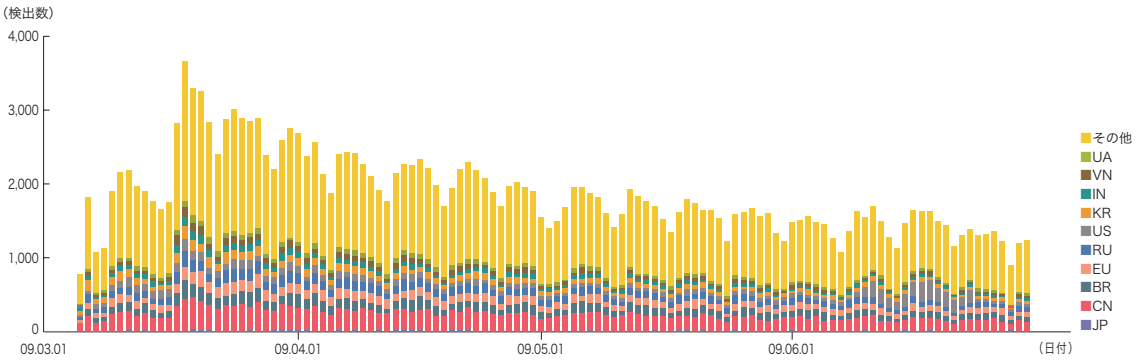


図-9　Conficker.DのP2Pポートへのアクセス（国別）

＊30 Waledacはボットの一種であり、スパムメールを大量に送信することで知られている。ConfickerとWaledacの関係については、たとえば次の情報を参照のこと（http://blog.trendmicro.com/downadconficker-watch-new-variant-in-the-mix/）。

＊31 Confickerに関する、US-CERTのTechnical Advisary（http://www.us-cert.gov/cas/techalerts/TA09-088A.html）。

＊32 Conficker.Dは攻撃先のIPアドレスと時刻をもとに算出されるポート（TCPもしくはUDP）でP2P通信を待ち受ける。この集計は 、このP2Pポートへのアクセスがあった送信元を集計することで作成している（http://nmap.org/nsedoc/scripts/p2p-conficker.html）。この図の作成には、IIJで実験的に運用するハニーポットでの観測情報も採用しているため、他の集計、例えば図-3とは母集団が異なっており、単純に比較できないことに注意。また、日本の様子を見やすくするために、図中の一番下に表示しているが、実際の順位は第26位であった。

＊33 Conficker Working Group とは、Confickerを撲滅するための活動で、セキュリティベンダを含む多くのITベンダや研究機関等が参加している。メンバー構成や活動の詳細については以下のURLを参照のこと（http://www.confickerworkinggroup.org/wiki/）。

＊34 Conficker Working Groupによる感染端末の推移（http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking）。

＊35 たとえば、Confickerがアップデートに使うURLは、日付をもとにしてあるアルゴリズムで生成されるため、対策を実施する側でも特定の日にConfickerがアクセスを試みるURLを知ることができる。このような知識を利用して、Confickerの動作に先行した監視や対応を行っている。

1.4.2 ID･パスワード等を盗むマルウェア Gumblar

4月から5月にかけて、あらかじめ盗まれたFTPアカウントを悪用した、Webサイトのコンテンツ改ざん事件が相次ぎました。この改ざんされたコンテンツは、第三者がアクセスしただけでマルウェア感染を引き起こします。さらに、感染したマルウェアによって、個人情報やID･パスワード等の情報が盗まれるという事態に発展しています*36。

■今回の事件の流れ

はじめに、今回の事件の流れを図-10に示します。以下、本説明中の数字は図-10内の数字に相当します。

■コンテンツ改ざんからマルウェア感染まで

まず、攻撃者はあらかじめ盗んだFTPアカウントを悪用し、Webコンテンツを改ざんします(1)。第三者が改ざんされたWebコンテンツにアクセスした場合(2)、改ざんによって挿入されたJavaScript等により、自動的に悪意のあるWebサイトへ誘導されます(3)。このスクリプトにより、Adobe ReaderやFlash Playerの脆弱性を悪用する、攻撃用のファイルがダウンロードされます。利用者のPCにこれらの脆弱性が存在する場合、ファイル内の攻撃コードが実行され、マルウェアAがダウンロードされます(4)。

■マルウェアの動作

マルウェアAは実行されると、マルウェアBを生成(Drop)し、レジストリに登録した上で、自分自身を削除します(5)。マルウェアBは実行されると、いくつかのAPIをフックし、HTTPやFTP等の通信を盗聴します。また、感染を発見されにくくするために、cmd.exeやregedit.exeを起動できなくします。さらに、別のマルウェア配布サイトにアクセスし、新しいマルウェアをダウンロードして実行する場合もあります(6)。

1. 事前に盗み出したID・パスワードを用い、FTPでコンテンツを改ざんする(スクリプトの挿入)。
2. あるユーザが改ざんされたサイトにアクセスすることで、Webブラウザ上でスクリプトが動作する。
3. ユーザの操作なしに、自動的にマルウェア配布サイトAに誘導される。
4. Adobe Reader や Flash Playerの脆弱性を悪用してマルウェアAをダウンロードし、実行する。
5. マルウェアAはマルウェアBをドロップし、レジストリに登録後、マルウェアA自身を削除する。
6. マルウェアBは新たなマルウェアをダウンロード、実行したり、FTP通信等を盗聴し、アカウント情報等を特定のサーバにアップロードして盗み出す。
7. マルウェアBはさらに、他のマルウェアのダウンロード、活動痕跡の削除、PC内のファイル消去等の破壊を行う場合もある。
8. 盗まれたFTPアカウントは再びコンテンツ改ざんに利用される。
9. 盗まれた情報は、商品購入やオークションの詐欺行為などで悪用される場合もある。

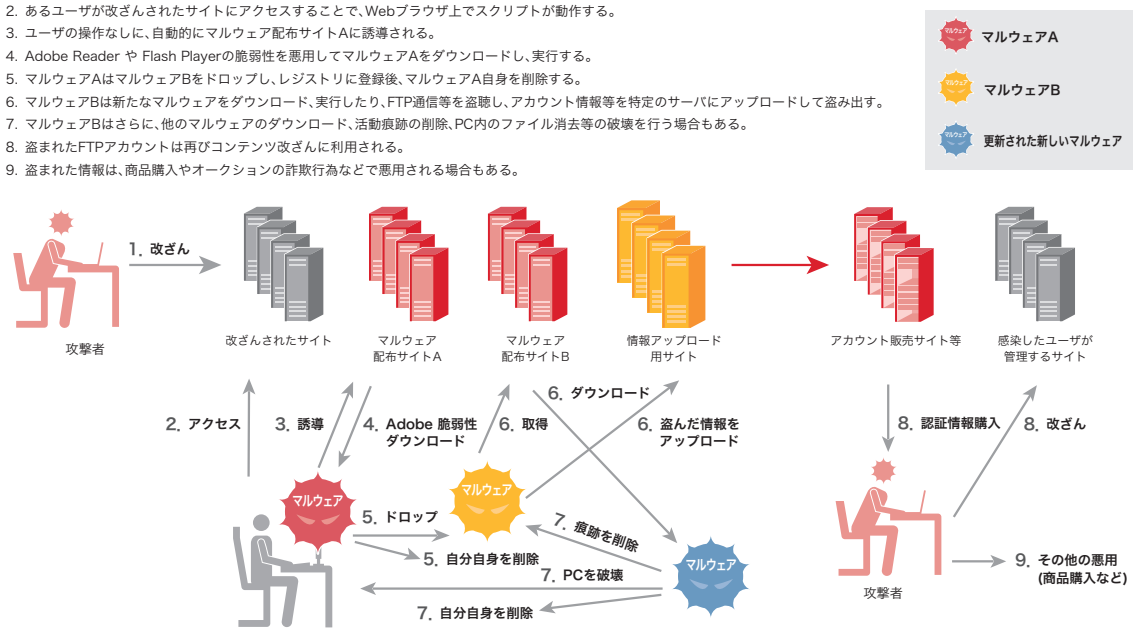


図-10 攻撃の全体像

*36 US-CERT Current Activity:Gumblar Malware Exploit Circulating (http://www.us-cert.gov/current/archive/2009/05/18/archive.html#gumblar_malware_attack_circulating)。
Gumblarとはマルウェア配布Webサイトのドメイン名の一部で、実際には gumblar.cnにアクセスすると感染が発生していた。同様なWebサイトにzlkon.lv, martuz.cnなどがあった。この事件は複雑で全体を示す適切な名前がなく、本稿では関係するWebサイトやマルウェア等、全体を示す名前としてGumblarと呼んでいる。

■情報のアップロードから悪用まで

マルウェアB、もしくは更新された新しいマルウェアは、通信の盗聴や設定ファイル等から盗み出した情報を、外部のサーバにアップロードします(6)。この情報には、個人情報や実際の通信に利用したID・パスワード等の情報が含まれます。また、活動の痕跡となるファイルを削除したり、PC上のOSやデータを破壊したりします(7)。このようにして盗み出された情報は、再びコンテンツ改ざんに悪用され、新たにマルウェア感染に誘導するWebサイトが増えていきます(8)。そして、情報を盗むこととその悪用を、循環的に繰り返すことで拡大し、最終的に多くの利用者が被害を受けていると考えられています。加えて、盗み出した情報は、他人に成りすますために悪用されたり、商品購入等で直接の金銭被害を引き起こしたりしています(9)[*37]。

■Gumblarの特徴

まずGumblarでは、個人のブログ等、比較的参照する人の少ない小規模なサイトに対して改ざん行為が行われていたため、発見が遅れていました。今回の件が大きな事件として取り上げられるようになったのは、ある企業のオンラインショップのコンテンツが改ざんされ、多くの被害が出たことによります。

また、Gumblarには複数のWebサイトや脆弱性、マルウェアが関係していることも特徴として挙げられます。特に悪用されたマルウェアが、シーケンシャルマルウェア[*38]であったことで、発見や解析、対策が困難となっていました。

加えて、マルウェアにより盗み出された情報が、ある程度時間が経過してから悪用されていることも挙げられます。このため、ユーザが改ざんに気づいた時点でウイルス対策ソフトによる検査を行っても、マルウェア自身や痕跡が削除されており、PC上からは異常が発見されにくいケースが目立ちました。

Gumblarについては、現時点で関係した複数のマルウェア配布サイトが停止され、関係するマルウェアもウイルス対策ソフトで検出可能となっているため、すでに過去の事件として考えられています。しかし、一旦感染したユーザの情報は盗まれたままであることを忘れてはいけません。新たなマルウェア配布サーバを用意するだけで、今回と同様の循環を構築することができ、実際に現在でも他のWebサイトやマルウェアを利用した、同様の事件が継続的に起こり続けています[*39]。

■利用者における注意点

この問題に対して、利用者として注意すべき事項は、利用しているPCにインストールされているソフトウェアの脆弱性情報に注意し、常に最新版を利用するように心がけることです。自動更新機能を持っていないソフトウェアや、特にブラウザのプラグインとして提供されているソフトウェア(今回の事例で悪用されたようなAdobe ReaderやFlash Player)は、今後も悪用の対象となる可能性があるため、注意が必要です。もし自分が感染したことに気付いた場合には、その端末上で入力したことのあるすべてのIDとパスワードを変更する必要があります。また、日ごろからIDとパスワードの管理を適切に行うことも重要となってきます[*40]。

1.4.3 クラウドコンピューティングとセキュリティ

ここでは、最近話題となっているクラウドコンピューティング(以下クラウド)の紹介とともに、その利用の観点から、セキュリティに関する考察を示します。

*37 以上のマルウェアの動作は、IIJで入手した検体を解析したうえで再現したもので、マルウェアAやマルウェアBとして、他の多くのマルウェアが介在することを示す情報もあり、必ずしも毎回この通りであるとは限らない。

*38 シーケンシャルマルウェアとは、マルウェアを機能ごとに分割し、必要時に個別にダウンロードし、実行していく仕組み。ウイルス対策ソフトをすり抜けるための手段として使われる。本事件では、リダイレクタ(javascriptマルウェア)、ダウンローダ(PDFマルウェア、マルウェアB)、ドロッパ(マルウェアA)、アカウント盗用マルウェア(マルウェアB)などが利用されており、全体で1つのシーケンシャルマルウェアを構成していると考えることができる。

*39 たとえば Nine-Ball等。以下は改ざんの様子を示すcNotes(http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=molo.tw)。

*40 パスワード管理手法の関連資料については本レポートのvol.3において紹介している(http://www.iij.ad.jp/development/iir/pdf/iir_vol03.pdf)。その他の立場での対策については、独立行政法人情報処理推進機構による今月の呼びかけ「あなたのウェブサイト、改ざんされていませんか?」(http://www.ipa.go.jp/security/txt/2009/07outline.html)等も参考になる。

■クラウドコンピューティングとは

現時点で多くの団体[*41]がクラウドの定義や標準化の議論を行っていますが、例えば、Open Cloud Manifestoでは、クラウドの主な特徴として「必要に応じた処理能力を低コストで確保でき、その能力を手軽に利用できること」としています[*42]。具体的にはAmazon、Google、Microsoftといった例が挙げられます。Amazonは計算環境を提供するEC2[*43]や、ストレージサービスのS3[*44]といった、利用者が自由に組み合わせて、構築、運用できる仕組みを提供しています[*45]。また、GoogleはGmailに代表されるアプリケーションサービスを主に提供しています[*46]。マイクロソフトは Windows Live Mail (Hotmail)や、Windows Update等のサービスを、クラウドの技術を基に提供しています。また、Windows Azureというクラウドプラットフォームサービスを提供することを発表しました[*47] 。このように、同じクラウドと呼ばれるサービスでも、コンピュータ資源の提供、プラットフォームの提供、アプリケーションの提供といった違いがあります。この違いをXaaS (X as a Service) と表記します。Googleのように、ソフトウェア (Software) をサービスとして提供する場合は、SaaS (Software as a Service) と呼び、ハードウェア (Hardware)、インフラストラクチャ (Infrastructure)、プラットフォーム (Platform) を提供するサービスは、それぞれ、HaaS、IaaS、PaaSと表記します。XaaS間の相互の関係を図-11に示します。

また、クラウドはパブリッククラウドと、プライベートクラウドに分類されます。パブリッククラウドとは、主にインターネット上で提供されている環境で、不特定多数の利用者が資源を共用します。一方、プライベートクラウドは、クラウド技術を使い、不特定多数向けではない限定的な用途に利用するクラウドです。

以上のように、クラウドは資源やサービスの提供形態を示しています。一方で、このクラウドと呼ばれる環境を実現するためには、ユーティリティコンピューティング、SOA、Web2.0 、仮想化、そして従来よりも低価格で手に入る潤沢な資源[*48]、といった要素の積み重ねが必要であり、これをクラウドの技術的要素と考えることができます。クラウドは表面的には利用方法の変化に見えますが、膨大な資源をまとめることによる複雑さの増加や、管理に用いる情報量の爆発的な増加といった、技術的に考慮すべき側面を含んでいるのです。

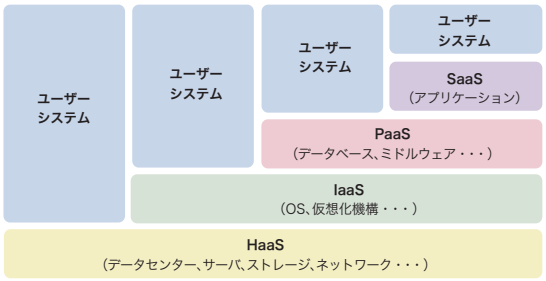


図-11 XaaSの関連図

＊41 クラウドに関する標準化などを推進している代表的な団体は以下の通り。Open Cloud Manifesto (http://www.opencloudmanifesto.org/)、Open Cloud Consortium (http://www.opencloudconsortium.org/)、Cloud Security Alliance (http://www.cloudsecurityalliance.org/),Open Cloud Standards Incubator (http://www.dmtf.org/about/cloud-incubator)。

＊42 原文はopen cloud manifesto (http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf)。ただし、この文章はクラウドの定義ではなく、定義などの議論を行うための整理であるとしている。

＊43 Amazon EC2はElastic Compute Cloudの略で、インターネット上でCPU資源を提供するサービス (http://aws.amazon.com/ec2/)。

＊44 Amazon S3はSimple Storage Serviceの略で、EC2で利用するディスクを提供するサービス (http://aws.amazon.com/s3/)。

＊45 導入事例としてはNASDAQのMarket ReplayやThe New York TimesのTimesMachine等がある。Market Replayは過去の市場動向分析が可能なアプリケーションで、データの保存にS3を利用している (http://aws.amazon.com/about-aws/media-coverage/2008/07/18/nasdaqs-use-of-amazon-s3)。The New York Timesでは過去の新聞のアーカイブ化にEC2を利用し非常に短期間で紙面のPDF化作業を終えた (http://open.blogs.nytimes.com/2007/11/01/self-service-prorated-super-computing-fun/)。

＊46 メールサービスで有名なGmailをはじめ、スケジュール管理を行うGoogleカレンダー、OfficeツールのGoogleドキュメント等が用意されている (http://www.google.com/apps/intl/ja/business/index.html)。

＊47 Windows Azureでは、計算環境やストレージ環境、またはWindows Live等のサービスを自由に組み合わせてシステムを構築する事ができる (http://www.microsoft.com/azure/whatisazure.mspx)。

＊48 CPUのメニーコア化、通信路の帯域、メモリ、ディスク等の記憶装置の容量等。

■クラウド上のセキュリティ問題

ここで､クラウドで利用される､従来とは異なる技術要素を検討した上で､配慮すべき点をいくつかご紹介します。

■境界に関する問題

仮想化技術そのものの脆弱性によって、論理的に分離されている資源の境界を越えて、データへの不正なアクセスが発生する等、脆弱性による影響が従来環境よりも拡大する可能性があります。また、クラウド自体にどのように境界を設定するかが、新たな検討課題となります。パブリッククラウドとプライベートクラウドは、安易に相互接続してはいけません。パブリック側からの不正アクセスを想定するだけでなく、クラウドへの侵入に成功したとき入手できる膨大な資源を、踏み台として悪用されないようにする必要があります。

■APIにかかわる問題

クラウドの制御には、基本的にAPIを利用しますので、そのAPIに脆弱性が発見された場合の影響について、検討が必要です。その影響は、クラウド上の個別のサービスの不正利用だけでなく、クラウド自体への不正な操作（停止も含む）等、従来環境よりも多岐にわたります。APIにアクセスを行うための認証情報を奪われた場合や、クラウド管理用端末に侵入された場合等への対策は、従来のセキュリティ対策課題と同様ですが、クラウドにおいては、その影響が増大すると考えられます。

■デジタルフォレンジック

デジタルフォレンジック*49をどのように行うのかも、大きな問題となります。クラウドでは物理的な実体と、論理的な実体が乖離する場合が多いため、通信の監視やハードディスクのイメージ調査、ログの調査等が非常に困難となります。また、クラウドの構成要素の状態を示す、より多くの管理情報の取得と記録が必要となります。

■クラウドを安全に利用するために

クラウドを利用するということは、様々なデータの管理や処理をクラウドに任せることであり、例えば、クラウドにあるデータのCIA（機密性、完全性、可用性）を、利用者の立場で適切に制御できるかが懸念されます。これは、従来型のアウトソースを利用しても発生する懸念であり、局面によって適切にクラウドを使い分け、契約や運用上のルールで対応することで、従来と同様の対策を考えることができます（図-12）。

但し、先に技術的要素として紹介したように、従来型のアウトソースとクラウドには、仮想化技術によるシステムの複雑さの増加と、資源の管理情報の大容量化の点で違いがあります。逆に言えば、この2点に対処することができれば、クラウドを利用する際に、従来と同程度のセキュリティを求めることができます。前者の課題に対しては、例えば筆者らは、図-13のようなモデルを使って、クラウド上で構成されるシステムのOSや、アプリケーションの依存性、システムの分離分割方法や、アクセス制御構造の把握を行うための研究を行っ

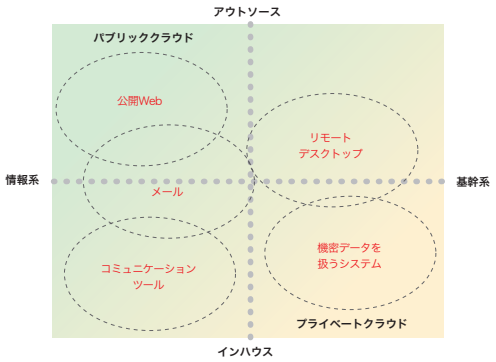


図-12 システムの利用用途によるサービスの使い分け

＊49 特定非営利活動法人デジタル･フォレンジック研究会による定義では「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･技術をいう」としている（http://www.digitalforensic.jp/wdfitm/wdf.html）。

ています*50。後者の課題に対しては、システムをデータモデル化し、コンピュータによる自動管理を推進することが重要です。膨大で複雑な構造をもったクラウド環境をモデル化することで、異常時の影響範囲を自動的に把握し*51、制御するといったことも可能となります。

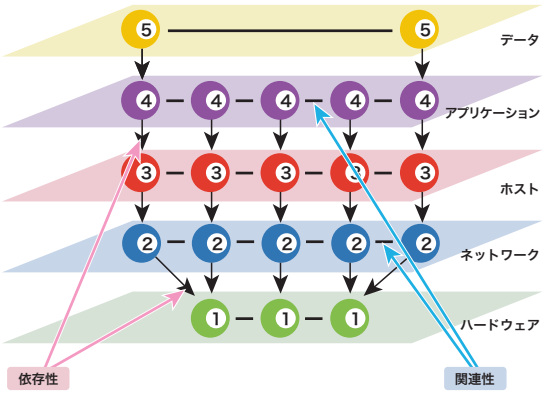
本稿では、クラウドのセキュリティに関する様々な懸念を述べてきました。情報システムの集約化、効率化の流れから、今後必然的にクラウドを利用する機会は増えていきます。ここで示したように、クラウドの仕組みや構造を理解した上で、従来の環境とクラウドの使い分けの検討を行えば、安全性を確保しながらクラウドならではの利点を享受することが可能となります。

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。このVol.4では、今現実に発生している大きな脅威2つについて解説するとともに、クラウドコンピューティングにおけるセキュリティ対策について考察しました。

実際に被害が発生している今日のインシデントに対応していくだけではなく、時々刻々と変化する技術動向を適切に把握し、将来におけるインシデントの予測とその対策を検討することにより、備えを行うことが重要です。

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、公開していくことで、インターネット利用の危険な側面についてご理解いただき、必要な対応策を講じた上で、安全かつ安心して利用できるように、努力を継続してまいります。



番号付きの球は管理対象となる資源を示す。それぞれの資源は属性（装置、OS、アプリケーション名等）を持つ。各レイヤで資源を繋いでいる線は、そのレイヤ内での資源の関連性（アプリケーション間の通信など）を示す。レイヤ間の線は、資源の依存関係を表す。クラウド内の管理対象をこのようにモデル表現することで、たとえばハードウェアの一部が故障したときの影響範囲を把握することができる。

図-13 クラウド上のシステムの論理表現モデル例

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。

土屋 博英（1.2 インシデントサマリ）**永尾 禎啓、須賀 祐治、大原 重樹、鈴木 博志**（1.3 インシデントサーベイ）
鈴木 博志、梅澤 威志（1.4.1 マルウェアConfickerの世界的流行） **鈴木 博志**（1.4.2 ID・パスワード等を盗むマルウェア Gumblar）
加藤 雅彦（1.4.3 クラウドコンピューティングとセキュリティ）
IIJ サービス事業統括本部 セキュリティ情報統括部

協力：
桃井 康成 IIJ ネットワークサービス本部 セキュリティサービス部 サービス推進課
大津 繁樹、牧野 泰光 IIJ サービス事業統括本部 システム基盤統括部
堂前 清隆 IIJ サービス事業統括本部 データセンター事業統括部 事業企画課

＊50 金岡晃，藤堂伸勝，加藤雅彦，岡本栄司：ネットワークシステムの安全性定量化に向けた新たな表現モデルとアクセス制御解析," 暗号と情報セキュリティシンポジウム2008（SCIS2008），（2008）
＊51 加藤雅彦，金岡晃，藤堂伸勝，岡本栄司：ネットワークシステムにおける脆弱性影響度の定量化と可視化," コンピュータセキュリティシンポジウム2008（CSS2008）論文集，pp.551-556，（2008）

2 ブロードバンドトラフィック

2.1 はじめに

本レポートでは、IIJが運用しているブロードバンド接続サービスのトラフィックを分析し、その結果を報告します。

過去5年間の、インターネットのトラフィック量の伸びは、国内及び世界的にも、比較的安定していることが報告されています（参考文献[3] [4] [5] P23参照）。国内ブロードバンドトラフィックの総量については、年率30%程度で増加していて、これは国内バックボーントラフィック全体の約60%にあたります。個人のインターネット利用者の多くはブロードバンド接続を利用しており、ブロードバンドトラフィックの傾向を知ることは、全体のトラフィックを理解するためにも重要です。（参考文献[1] [2] P23参照）。

本レポートでは、利用者の1日のトラフィック量やポート別使用量等をもとに、最近のブロードバンドトラフィックの傾向を見ていきます。P2Pファイル共有等を使うヘビーユーザのトラフィック量は、依然、量的には支配的ですが、あまり増えていません。その一方で、一般利用者のトラフィック量は、ビデオ系コンテンツの増加やウェブサイトのリッチコンテンツ化で着実に増えています。

2.2 データについて

今回利用した調査データは、個人及び法人向けのブロードバンド接続サービスについて、ファイバーとDSLによるブロードバンド顧客を収容するルータで、Sampled NetFlowにより収集したものを使っています。 ブロードバンドトラフィックは平日と休日で傾向が異なるため、一週間分のトラフィックを解析することとし、2009年5月25日から31日の一週間を期間としています。また、比較のため2005年2月21日から27日のデータも用いています。2005年時点ではまだ、YouTubeやニコニコ動画などのビデオ共有サービスは登場していません。

各利用者の使用量は、利用者に割り当てられたIPアドレスと、観測されたIPアドレスを照合して求めています。また、NetFlowではパケットをサンプリングして統計情報を取得しています。サンプリングレートは、ルータの性能や負荷に応じて、1/1024、1/2048、1/4096、1/8192のいずれかに設定されています。 観測された使用量に、サンプリングレートの逆数を掛けることで全体の使用量を推定しています。サンプリングによって、使用量の少ない利用者のデータには少し誤差がでますが、ある程度使用量のある利用者に対しては、統計的に意味のある数字が得られます。

ファイバーとDSLの観測された利用者数を見ると、2005年ではほぼ同数でした。しかし、2009年にはファイバーへの移行が進み、観測ユーザ数の84%はファイバー利用者で、トラフィック量全体の90%を占めるまでになっています。

なお、本レポート中のトラフィックのIN/OUTは、ISPから見た方向を表し、INは利用者からのアップロード、OUTは利用者へのダウンロードとなります。

2.3 利用者の1日の使用量

まずはブロードバンド利用者の、1日の利用量をいくつかの切口から見ていきます。 ここでの1日の利用量は、各利用者の1週間分の1日平均です。

図-1は、利用者の１日の平均利用量の分布（確率密度関数）を、アップロード（IN）とダウンロード（OUT）に分け、利用者のトラフィック量をX軸に、その出現確率をY軸に示しています。X軸はログスケールで、10^4（10KB）

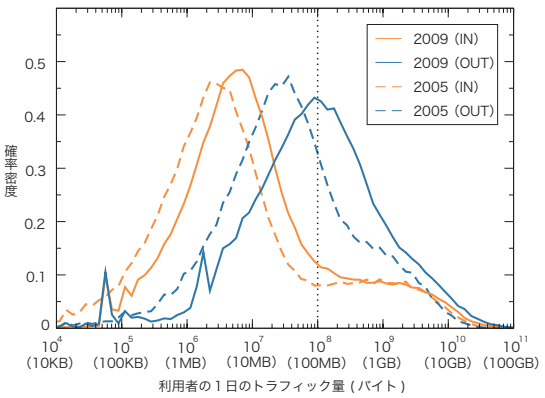


図-1　利用者の1日のトラフィック量分布

から10^{11} (100GB) の範囲を示しています。 一部の利用者はグラフの範囲外にあり、最も使用量の多い利用者は200GBにものぼりますが、概ね10^{11} (100GB) までの範囲に分布しています。2009年のグラフ左側に少しヒゲが出ていますが、これはトラフィックの増加に伴い、サンプリングレートが粗くなった影響のノイズです。

INとOUTの各分布は、片対数グラフ上で正規分布となる、対数正規分布に近い形をしています。これはリニアなグラフで見ると、左端近くにピークがあり右へなだらかに減少する、いわゆるロングテールな分布です。OUTの分布はINの分布より右にずれていて、ダウンロード量がアップロード量より、ひと桁程大きくなっています。平均値はグラフ右側のヘビーユーザの使用量に引っ張られるので、INの平均は2005年で430MB、2009年では556MB、OUTの平均は2005年で447MB、2009年では971MBにもなります。

INの分布の右端を見ると、もうひとつ小さな分布の山があるのに気がつきます。実はOUT側にもメインの分布に重なって、同様の分布の山があります。これらの分布は、INとOUTでほぼ同じ位置にあり、IN/OUT量が対称なヘビーユーザを示しています。そこで便宜上、大多数のIN/OUT非対称な分布を「クライアント型利用者」、右側の小数のIN/OUT対称なヘビーユーザの分布を「ピア型利用者」と呼ぶことにします。

クライアント型利用者の、分布の最頻出値を2005年と2009年で比較すると、INでは3.5MBから6MBに、OUTでは32MBから114MBに増えていて、各利用者のトラフィック量が、特にダウンロード側で大きく増えていることが分かります。それに対して、ピア型利用者の分布では、最頻出値の位置は2005年、2009年ともに2GB付近で大きな変化はありません。つまり、一般利用者の使用量が大きく増えているのに対して、ヘビーユーザの使用量は、一定しています。

図には示していませんが、ファイバーとDSLでそれぞれ同様の分布を調べると、同じ年ではクライアント型とピア型の、分布の位置はほぼ同じですが、ファイバーではピア型利用者の割合が多くなっています。つまり、それぞれの分布の典型的な利用量に差はないのですが、ファイバーではヘビーユーザの割合が多くなっています。なお、ピア型分布の最頻出値の1日に2GBという数字は、ビット／秒換算で185kbpsとなります。

図-2は、利用者の1日のトラフィック量を、相補累積度分布にしたものです。これは、使用量がX軸の値より少ない利用者の、全体に対する割合をY軸に、ログ･ログスケールで示したもので、ヘビーユーザの分布を見るのに有効です。グラフの右側が直線的に下がっていて、ベキ分布に近いロングテールな分布であることが分かります。ヘビーユーザは統計的に分布していて、決して一部の特殊な利用者ではないと言えます。

図-3は、利用者間のトラフィック使用量の偏りを示し

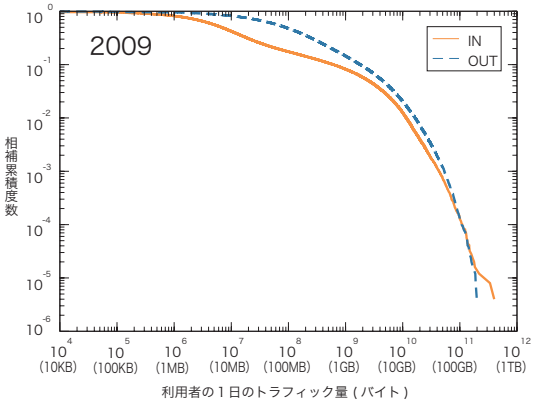


図-2　利用者の1日のトラフィック量の相補累積度分布

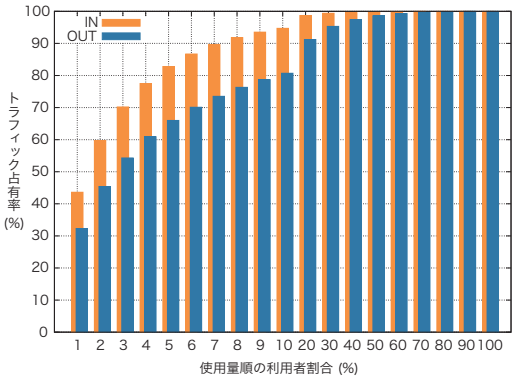


図-3　利用者間のトラフィック使用量の偏り

ます。使用量上位X%の利用者が、全体トラフィック量のY%を占めることを表します。使用量には大きな偏りがあり、結果として全体は一部利用者のトラフィックで占められています。 例えば、上位10%の利用者がOUTの80%、INの95%を占めています。さらに、上位1%の利用者がOUTの30%、INの40%を占めます。上位の利用者の使い方により若干の変動は生じますが、このような偏り方は2005年からほとんど変わっていません。これはロングテールな分布の特徴で、インターネットデータに共通な傾向です。例えば、ピア型利用者を除いた偏りを見ても、やはりほぼ同様な偏りが観測されます。このような偏りは、インターネット以外でも決して珍しいものではなく、単語の出現頻度や富の分布など、大規模で複雑な統計でよく現れることが知られています。

利用者間のトラフィックの偏りは、一見すると一部のヘビーユーザとそれ以外のユーザという、二極化が起きている印象を受けるかもしれません。しかし、使用量の分布はベキ乗則に従っていて、多様なユーザが幅広く存在していることが分かります。

図-4は、利用者ごとのIN/OUT使用量を2005年と2009年で5,000人をランダムに抽出してプロットしています。X軸はOUT（ダウンロード量）、Y軸はIN（アップロード量）で、ともにログスケールです。利用者のIN/OUTが同量であれば対角線上にプロットされます。

ここでは、2つのクラスタが観測できます。対角線の下側に対角線に沿って広がるクラスタは、ダウンロード量がひと桁多いクライアント型の一般ユーザです。もう一方のクラスタは、右上の対角線近辺に広がるピア型のヘビーユーザです。しかし、ふたつのクラスタの境界はあいまいです。これは、実際には、クライアント型の一般ユーザでも、skypeなどのピア型のアプリケーションを利用し、また一方のピア型のヘビーユーザもウェブ等のダウンロード型のアプリケーションを利用しているからです。つまり、多くの利用者は両タイプのアプリケーションを異なる割合で使用しているのです。また、各利用者の使用量やIN/OUT比率にも大きなバラツキがあり、多様な利用形態が存在することが伺えます。

2005年と2009年を比較すると、クライアント型のクラスタは中心が右上に移動していること、ピア型のクラスタは幅が広がり密度が低くなっていることが確認できます。

2.4 ポート別使用量

つぎにトラフィックの内訳を、ポート別の使用量から見ていきます。最近では、ポート番号からアプリケーションを特定することは困難です。P2P系アプリケーションには、双方が動的ポートを利用するものが多く、また、多くのクライアント・サーバ型アプリケーションが、ファイアーウォールを回避するため、HTTPが使う80番ポートを利用します。大雑把に分けると、双方が1024番以上

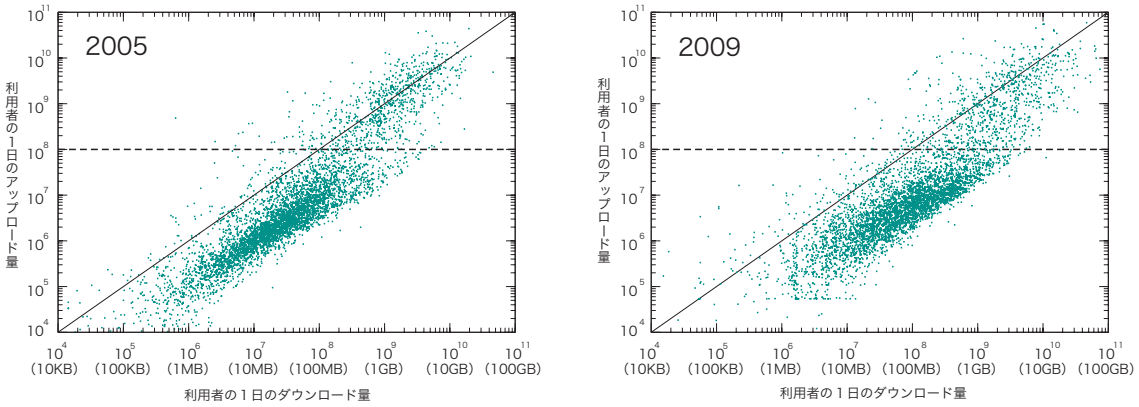


図-4　利用者ごとのIN/OUT使用量　2005年（左）2009年（右）

の動的ポートを使っていれば、P2P系アプリケーションの可能性が高く、片方が1024番未満のいわゆるウェルノウンポートを使っていれば、クライアント・サーバ型のアプリケーションの可能性が高いと言えます。そこで、TCPとUDPで、ソースとデスティネーションのポート番号の小さい方を取り、ポート番号別の使用量を見てみます。

また、全体トラフィックは、ピア型のヘビーユーザのトラフィックに支配されているので、クライアント型の一般利用者の動向を見るために、少し荒っぽいですが、1日のアップロード量が100MB未満のユーザを抜き出して、これをクライアント型利用者とします。 これは図-1では、IN側のふたつの分布の中間にあたり、図-4では、IN = 100MBにある、水平線の下側の利用者にあたります。

図-5はポート使用の概要を、全体とクライアント型利用者について、2005年と2009年で比較したものです。また、表-1にその詳細を数値で示します。

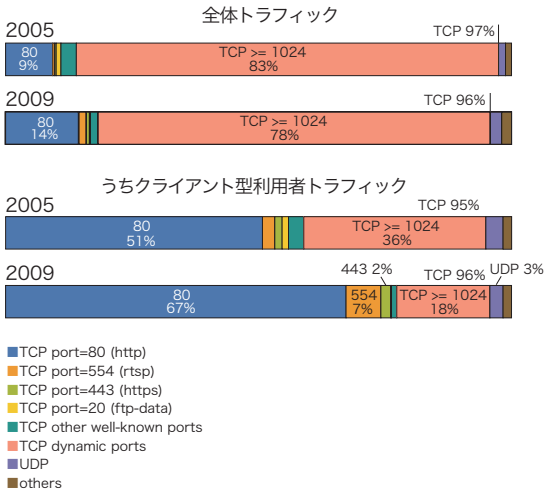


図-5　ポート別使用量概要

トラフィックの95%以上はTCPです。さらに、全体でみるとほとんどはTCPの動的ポートで、2009年には総量の78%が、双方とも動的ポートを使ったトラフィックとなっています。動的ポートでの、個別のポート番号の割合は僅かで、最大のもので総量の1.1%に過ぎません。80番ポートの割合は、2005年の9%から14%に増加しています。

一方、クライアント型利用者に限ると80番ポートが多く、2005年には51%であった割合が2009年には67%にまで増加しています。 逆に、動的ポートの割合は、36%から18%に減少しています。また、2番目に多いのは554番ポートです。これはReal-Time Streaming Protocol（RTSP）で使われるポートで、ビデオコンテンツの増加と関連しています。

これらのデータから、TCP80番ポートのトラフィックが増加傾向にあると言えます。80番ポートには、ビデオコンテンツやソフトウエアアップデート等も含まれているた

protocol　port	2005		2009	
	total (%)	client type	total (%)	client type
TCP　*	97.43	94.93	95.80	95.73
(<1024)	13.99	58.93	18.23	77.31
80 (http)	9.32	50.78	14.46	67.30
554 (rtsp)	0.38	2.44	1.48	6.89
443 (https)	0.30	1.45	0.64	1.91
20 (ftp-data)	0.93	1.25	0.19	0.17
(>=1024)	83.44	36.00	77.57	18.42
6346 (gnutella)	0.92	0.84	1.10	0.60
6699 (winmx)	1.40	1.14	0.70	0.24
1935 (rtmp)	0.20	0.81	0.36	1.51
7743 (winny)	0.48	0.15	0.25	0.03
UDP　*	1.38	3.41	2.24	2.60
53 (dns)	0.03	0.14	0.03	0.07
ESP	1.09	1.35	1.87	1.55
GRE	0.07	0.12	0.07	0.08
ICMP	0.01	0.05	0.02	0.05

表-1　ポート別使用量詳細

め、コンテンツタイプの特定はできませんが、クライアント・サーバ型の通信量が増えていることが伺えます。

図-6は、全体トラフィックのTCPポート利用の週間推移を、2005年と2009年で比較したものです。ここでは、TCPに関して、ポート利用を80番、その他のウェルノウンポート、動的ポートの３つに分けて、それぞれの推移を示しています。トラフィックの絶対量は開示できないので、ピーク時の総トラフィック量を1として正規化して表しています。全体では動的ポートが支配的で、そのピークは23:00〜1:00、土・日には昼間のトラフィックが増加していて、家庭での利用時間を反映しています。

図-7は、クライアント型利用者について同様に、TCPポート利用の週間推移を示します。こちらは、2005年では80番は動的ポートより少し多い程度でしたが、2009年には80番が支配的になっています。また、ピーク時間は21:00〜23:00と少し早くなっていて、土・日は朝からの利用が増えています。

全体とクライアント型との推移を比較すると、夜中を過ぎた後の、トラフィックの減り方に違いがあるのが分かります。80番は夜中を過ぎると急激に減少し、４時頃に最小となります。これに対して、動的ポートの流量は朝にかけて序々に減少し、朝8時頃に最小となります。この理由として、動的ポートを使うP2Pファイル共有で、夜にマニュアルでアップロードされたファイルが、一晩かけて拡散することや、目的のファイルのダウンロードが完了したら、アプリケーションを終了する利用者の行動を反映しているものと推測しています。

2.5 おわりに

これまで見てきたように、P2Pファイル共有に代表されるピア型トラフィックは、量的には依然支配的ですが、2005年から大きな増加は見られません。その原因として、利用者がP2Pファイル共有から、より使い易く魅力あるビデオ共有サイト等の、サービスへ移行していることが挙げられます。また、一時期急速にトラフィックを増やした、P2Pファイル共有が問題視されてきた結果、P2Pファイル共有の仕組みが、過度な帯域使用をしないように修正されてきたことや、ISPによる過度の利用制限の導入等で、利用者の意識が変化してきた影響もあるでしょう。

一方で、一般利用者の使用量が、ビデオコンテンツや他のweb2.0系の、リッチコンテンツによって着実に増加

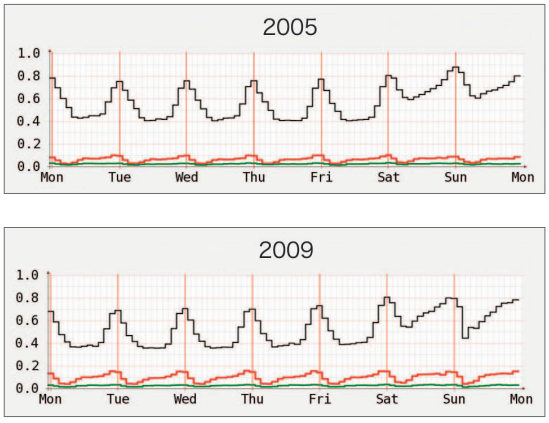


図-6　全体トラフィックのTCPポート利用の週間推移 2005年（上）2009年（下）

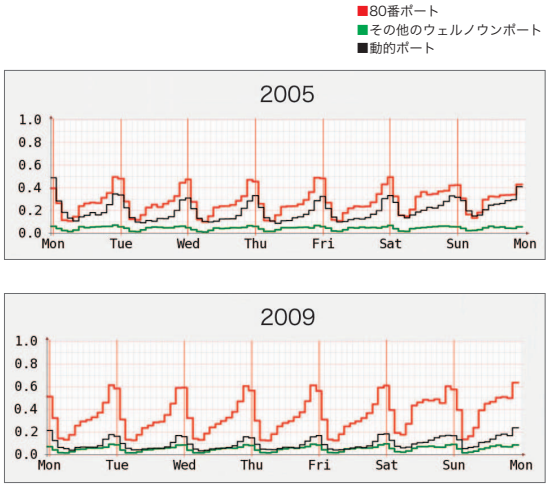


図-7　クライアント型利用者のTCPポート利用の週間推移 2005年（上）2009年（下）

してきています。ビデオコンテンツだけではなく、ユーザが明示的にクリックしなくても、自動的にさまざまな情報を切替えて提供する、あるいはバックグラウンドで、次にユーザが利用する可能性のあるコンテンツを、先回りして取得するようなウェブサイトが増えていて、それに従ってトラフィック量も増えているのです。

2004年頃には、P2Pファイル共有の登場でトラフィックが急増し、回線の逼迫が予測されていました。その後5年間のトラフィック増加は、年率30%程度で安定して増加しています。その一方、バックボーン等のネットワークの容量も、年率50%程度で増強が進んでいると言われています（参考文献- [6]）。そのため、現状マクロレベルでは、回線容量に余裕が生じていると考えられています。

しかし、インターネットのトラフィックに関して、過去のデータをもとに将来を予測をするのは困難です。これは、一部のヘビーユーザの挙動の影響が大きいため、彼らの行動に変化があると、予測が大きくずれることになるからです。また、ユーザのインターネットの利用の仕方は、技術的な要因だけでなく、経済的要因、社会的要因、政治的要因等に大きく影響を受けます。そして、過去にウェブやP2Pファイル共有が登場して、トラフィックが激変したように、新しい技術の登場により、インターネットの使われ方が大きく変わる可能性は常に存在します。これまでは5年ないし10年周期で、トラフィックに大きな変化があったことを考えると、最近のトラフィック成長はある意味、安定し過ぎているとも言えます。近いうちにまた大きな変化が起こるのかも知れません。

IIJでは、インターネットの利用形態の変化に素早く対応できるよう、継続的なトラフィックの観測を行っています。 今後も、定期的にこのようなレポートをお届けしていく予定です。

執筆者：
長 健二朗（ちょう けんじろう）
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 副所長。インターネットがシンプルかつ柔軟な、安定した通信インフラとして発展するため、ネットワークの複雑な挙動の解析、QoS通信、オペレーティングシステムのネットワーク機能の研究等を行っている。WIDEプロジェクトボードメンバー、北陸先端科学技術大学院大学客員教授

参考文献

[1] K.Cho, K.Fukuda, H.Esaki, and A.Kato.
The impact and implications of the growth in residential user-to-user traffic.
In ACM SIGCOMM2006, Pisa, Italy, Aug. 2006.

[2] K.Cho, K.Fukuda, H.Esaki, and A.Kato.
Observing Slow Crustal Movement in Residential User Traffic.
In ACM CoNEXT2008, Madrid, Spain, Dec. 2008.

[3] Cisco. Visual Networking Index - Forecast and Methodology, 2007-2012. June 2008.

[4] Cisco. Approaching the zettabyte era. June 2008.

[5] A.M. Odlyzko. Minnesota Internet traffic studies.
http://www.dtc.umn.edu/mints/home.html.

[6] TeleGeography Research. Globel Internet Geography. 2008.

3 クラウドコンピューティングテクノロジー

3.1 はじめに

クラウドコンピューティングにより、コンピューティングリソースを所有することから利用することへと、パラダイムが移り変わると言われています。IIJでは、莫大なデータの処理や、効率的なインフラの実現のため、数年前から、クラウドコンピューティングを支える技術を開発、運用しています。

ここでは、IIJが独自に開発・実装し、サービス基盤で利用している、クラウド技術基盤の一つである、「ddd」と呼ばれる分散システムについて説明します。

3.2 分散システムとは?

dddについて説明する前に、ここで説明する分散システムを定義しておきます。分散システムの定義は、(1)複数のコンピュータノードで構成されていること、(2)それを利用するユーザからは単一のシステムとして見えること、の2つです。

分散システムの例としては、巨大なデータを保持する分散ストレージや、分散データ処理などが挙げられます。(図-1、図-2)

分散システムの目的は、複数台のコンピュータノード(以下ノード)を用いることにより、一台のコンピュータよりもシステムとしての処理能力を向上させたり、可用性を増大させることです。単純にコンピュータを並べるだけではなく、それらを協調動作させる技術が必要になります。

莫大なデータの保持や処理を、効率的に行うことが期待されているクラウドには、必然的に大量のデータが集まります。また、求められる可用性もますますシビアなものになってきています。クラウドコンピューティングにとって、大規模な分散システムは極めて重要な要素となりつつあります。

3.3 分散システムの実例

分散システムは現在活発に技術開発が続けられている分野です。いくつか有名な例を紹介します。

- Google File System (GFS)
  巨大で大量のデータを扱うためにGoogleで作られた分散ファイルシステム。実装は、Google外部には公開されていない。(http://labs.google.com/papers/gfs.html)
- MapReduce
  Googleで考案された大規模分散処理フレームワーク(詳細は後述)。(http://labs.google.com/papers/mapreduce.html)
- Amazon Dynamo
  Amazonが開発した、分散キーバリューストア(key-

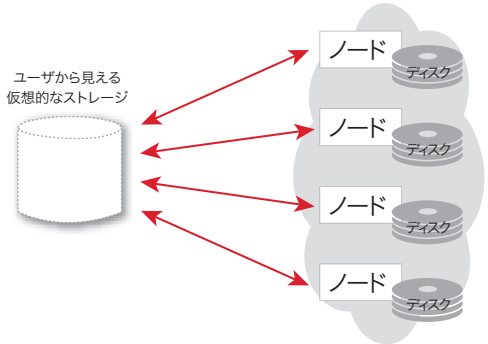


図-1　分散ストレージ

データを複数ノードで分散保持する。ユーザからはひとつのストレージに見える。

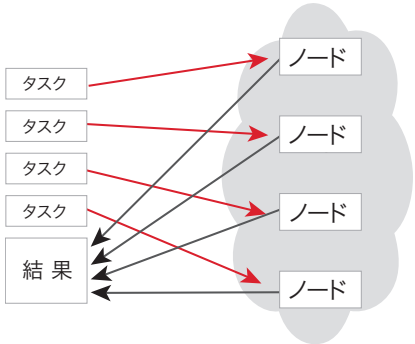


図-2　分散データ処理

データ処理内容をたくさんのタスクに分割し、複数ノードで並列に処理する。

value store)。これも実装は公開されていない。(http://www.allthingsdistributed.com/2007/10/amazons_dynamo.html)

- Hadoop
  上記GFSとMapReduceを参考に作られた分散システム。Javaで記述され、オープンソースとして公開されている。(http://hadoop.apache.org/)

これらの中で、Google File SystemやAmazon Dynamoは分散ストレージに、MapReduceは分散データ処理技術に分類されます。IIJが開発したdddは、その両方の機能を併せ持ったものになっています。

3.4 ddd開発の経緯

dddはdistributed database daemonの略称で、IIJバックボーンを流れる膨大なトラフィックを解析するために作られました。

インターネットサービスプロバイダ(ISP)は、自社のバックボーンを安定運用するために、バックボーンルータのトラフィック情報を取得し、解析しています。多くの場合は、ルータの各インタフェースのカウンタ値を、SNMPで取得してグラフ化するということが行われていますが、インタフェースの単純なIN/OUT情報だけではトラフィックの実態が分からないため、監視や分析をする上で不十分なことがあります。

そこで利用されるのが、フロー情報と呼ばれる、より詳細なトラフィック情報です。ISPのバックボーンで使われているハイエンドなルータやスイッチは、パケットの送信元及び送信先のIPアドレスや、ポート番号等が含まれるフロー統計情報を出力できるものがあり、それを受信して解析することにより、SNMPでは把握できない、詳細な通信状況を監視することができるようになります。

例えば、図-3は、フロー情報を元にトラフィックの宛先となるAS番号別に色分けして表示したグラフです。右端近辺でトラフィックが急に落ち込んでいる部分がありますが、フロー情報を用いて解析すると、一部のAS宛ての通信のみが減少していることが分かります。SNMPでは総量しか把握が出来ないので、異常や状況の変化の原因特定が難しいような場合でも、フロー情報を用いると詳細な解析が可能になります。

フロー情報を解析するに当たっての問題点は、そのデータ量が膨大であるということです。細かい通信内容を分析できる反面、必然的にデータ量が多くなってしまいます。一般的には、フロー情報を受信した直後に、ある程度の集計処理を行って、データ量を減らしてから格納することが多いようです。例えば、送信元アドレス単位で集計して、合計値のみを格納するというやり方です。しかし、集計した値では後で細かく解析することができなくなるため、IIJではフロー情報をほぼ全て保持し、必要になった段階で抽出や集計処理を行うようにしています。このようなやり方では、IIJのように多くのネットワーク機器を運用しているISPでは、極めて大きなデータを取り扱わなければなりません。

以前、IIJでは、フロー情報を一般的なリレーショナルデータベースに格納していました。しかし、フロー情報は、一つひとつのレコードは小さいものの、5分あたり数十万から数百万レコードに及ぶこともあり、従来のデータベースではごく短期間の情報しか保持できません。

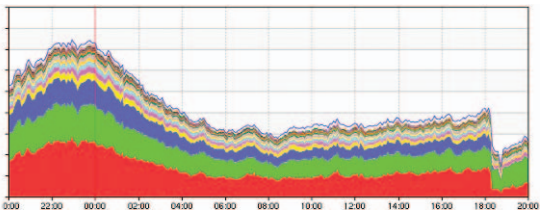


図-3　AS番号別に色分けしたトラフィックグラフ

そこで、長期間にわたる膨大なフロー情報を扱うため、IIJでは独自の分散システムを開発することとしました。それがdddです。数百億超の大量のフロー情報レコードを保持し、様々な条件で高速にデータを抽出したり、集計したりすることができます。

なお、dddは、フロー情報を扱うことを第一の目的として開発が始まりましたが、現在ではセキュリティサービスやアプリケーションサービスのログ解析、内外のセキュリティ情報の分析等、より広範なデータの処理に活用しています。

3.5 dddの概要

dddは、IIJ社内で使われている分散システムで、低コストなPCを利用しながら、高いスケーラビリティを実現した分散システムです。

dddには次のような特徴があります。

- pure P2Pによる、単一障害点を持たない構成
- データの自動冗長化機能を備え、動的に拡張可能な分散ストレージ
- MapReduceによる高速なデータ処理

dddの各ノードは以下のような3層構造になっています。全てのノードは同一の構造をしています。(図-4)

各項目について以下、順に説明していきます。

3.5.1 pure P2P

dddの各ノードは、中央管理ホストを持たないpure P2Pのネットワークを構成します。中央管理ホストが無いため単一障害点もありません。すべてのノードは対等で、それぞれが協調して動作します。後述のデータ冗長化機能と併せて、いつ、どのノードが故障してもシステム全体としては問題なく稼働します。

新規にノードを追加する場合は、既存のどれか1つのノードに接続して起動します。新規ノードは、接続した既存ノードから他のノードの情報(IPアドレスなど)を取得します。同時に、新規ノードの情報は他の既存のノードに広報されていきます。

dddは、起動している間ずっと他のノードと情報を数秒おきに交換しあっています。よって、各ノードは他のすべてのノードを情報を知っていることになります。このように相互に情報を共有しているノードの一群をクラスタと呼びます。

3.5.2 分散ストレージ

■キーバリューストア

dddのストレージ部分は、分散キーバリューストア(key-value store)と呼ばれるものに分類されます。キーバリューストアとは、データをキーとバリューの組み合わせで格納する、シンプルなデータベースの一種で、それを複数のノードで分担して管理するのが分散キーバリューストアです。

キーバリューストアは、従来のリレーショナルデータベース(RDB)に比べ機能が限られ、データの結合機能(JOIN)も、トランザクションによる一貫性の保持の機構もなく、基本的にはキーを指定して、対応する値を読み書きすることのみが可能です。

機能が限られるかわりに、キーの値によって担当するノードを振り分けて分散化するのに適しており、スケー

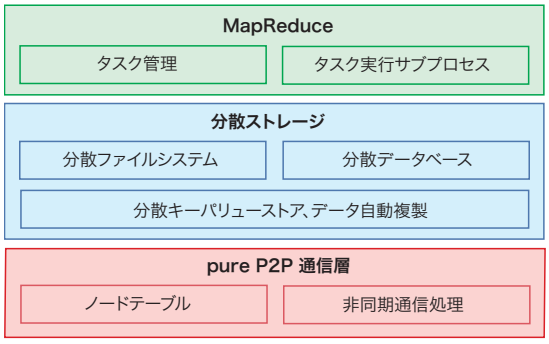


図-4　ddd内部構造概略

ラビリティを高めることができるため、クラウド時代のデータストアと言われることもあります。

キーに応じて担当ノードを振り分けるために、dddではコンシステントハッシュ法と呼ばれるアルゴリズムを採用しています。

コンシステントハッシュ法では、各ノードもキーも論理的にリング上のハッシュ空間に配置されているものとして考えます（この配置はノードの物理的なネットワークトポロジとは無関係です）。ノードには、IPアドレスをハッシュした値がノードIDとしてつけられます。また、格納したいキーも同様にハッシュ空間に写像し、そこから反時計回りにまわって最初に遭遇するノードが、そのキーの格納ノードとして処理を担当することとなります。（なお、ハッシュ関数にはSHA1を使っているため、ハッシュ空間は2の160乗の大きさがあります）。この方法では、格納されているキーの数やデータの量とは無関係に、キーの値からハッシュ値を計算するだけで格納ノードを割り出すことが可能です。（図-5）

コンシステントハッシュ法の最大のメリットは、ノードが増減した場合に、影響を受けるキーの範囲が限定されることです。例えば、図の中でノードBが故障でなくなった場合、薄い緑色で示される範囲のキーのみが影響を受け、それ以外のキーは影響を受けません。（図-6）

分散システム環境では、日常的なノードの増減を前提として考える必要があります。コンシステントハッシュ法は、その増減に強いという利点のため、分散キーバリューストアではよく使われるアルゴリズムです。

■データの自動的な冗長化

dddでは、冗長化のために、全てのデータは必ず異なる3つのノードに複製されるようになっています。先ほど、コンシステントハッシュ法で、キーのハッシュ値から反時計回りに最初にあたったノードに格納することを解説しましたが、さらに２番目と３番目のノードにも同じデータをコピーします。つまり、同時に３台のノードが壊れない限り、データはいずれかのノードに保持されるため、データ保全の信頼性は高いといえるでしょう。

ノードが壊れると、一時的にはデータの複製数が３つではなく２つや１つになります（ここではゼロになってしまうことは考えません）。この状態が長く続かないよう、dddでは残ったデータをコピーして常に複製数を３つに保つようになっています。そのために、dddは図-7のようなihave/sendmeと呼ばれる仕組みがあります。

まず、各ノードは自分の持っているキーをリストアップします。キーの値から、コンシステントハッシュ法により、そのキーを担当しているべきノードを割り出せるの

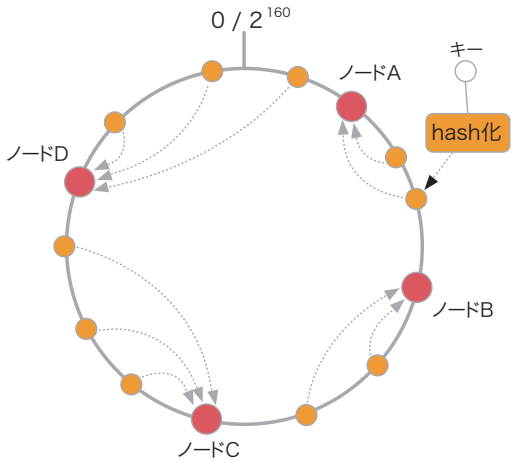


図-5　コンシステントハッシュ法：キーとノードの論理的配置図

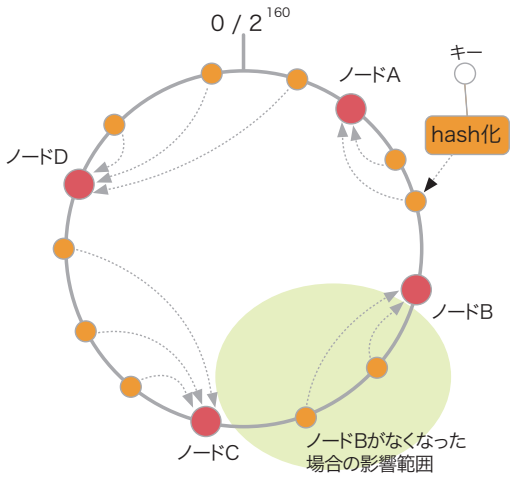


図-6　コンシステントハッシュ法：ノード故障時の影響範囲

で、そのノードに向かって、キーのリストを送ります。これを、ihaveメッセージといいます。ihaveメッセージを受け取った側は、リストに含まれているキーと自分の持っているキーを比べて、持っていないキーがあればそのデータの送信要求を返します。これをsendmeメッセージといいます。sendmeを受け取ったノードは、要求元にデータを送信します。実際には、キーの数は大量にあるため、一度に全てのキー情報を交換するのではなく、少しずつ分割してやりとりします。また、ノードの数が増減した場合は、その影響を受ける範囲のキーについてのみ、コンシステントハッシュ法で割り出されるihave送信先が変化し、新たに担当となったノードにデータが転送されます。図-6で、ノードBが無くなったケースにおいて、薄い緑色で示される範囲のキーの担当は「ノードB、A、D」から、「ノードA、D、C」に変化し、新たに担当となったCにA、Dのいずれかからデータが転送されます。dddは延々とこれを繰り返し、結果として、若干のリードタイムでデータの複製数を３つ保持します。

dddでは、ノードのハードウェアコストを低く抑えるために、RAID等のディスク冗長化技術は採用していません。そのかわり、より上位のレベルでデータを冗長化して、いつノードが故障して脱退しても支障のない仕組みを実現しています。

一方で、分散ストレージでは、同じデータを複数ノードで分散保持するために、データの一貫性を保つことが常にできるとは限りません。複数のノードをネットワークで接続する分散システムでは、一部のノードが故障したり、ネットワーク的に分断される可能性があり、それでもシステムの可用性を高めるためには、必然的にトレードオフとして一貫性を保証できなくなります。多くの場合、不整合が発生するタイミングはごく短く、時間経過により一貫性が保たれるような機構になっていますが、アプリケーション側で不整合に対処することも必要です。

IIJでは、前述のフロー情報や、各種サーバのログなどを、機器IDと時刻をキーにしてdddの分散ストレージに格納しています。フロー情報もログ情報も、内容は不変であり、一度書き込んだ情報を更新する必要はありません。そのため、上記の一貫性が保証されない特性は、ほとんど問題になりません。ただし、ノードの増減に伴うデータの複製が発生している瞬間は、あるはずのノードにデータがないということが起こりえます。その場合、dddを使うアプリケーション側で、2番目・3番目の候補のノードにリトライしてデータを取得するようにしています。

3.5.3 MapReduce

MapReduceは、Googleで考案された大規模データ処理のためのプログラミングモデルです。名前の通り、データをmapとreduceの２段階に分けて処理するモデルで、うまく使うと多数のノードで効率よく分散並列処理ができます。(図-8)

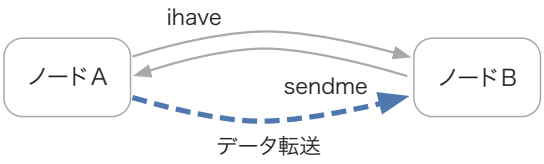


図-7　ihave/sendmeの仕組み

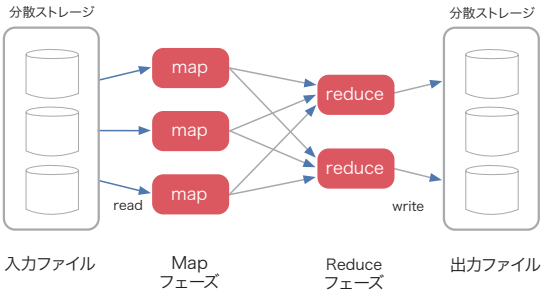


図-8　MapReduce概念図

GoogleのMapReduceのソースコードは公開されていませんが、Googleにより仕組みに関する論文が発表されています。今では、それを元に類似の機能を持った実装がいくつか出てきており、検索エンジンのインデックスの作成や、ログファイルの解析等に使われたりしているようです。dddも、分散ストレージのデータを処理するためにMapReduceの機能を搭載しています。

mapとreduceは、わかりやすく言い換えると「抽出」と「集約」と言えます。map（抽出）のフェーズではデータの中から必要な情報を抽出し、必要に応じて後の処理がしやすい形に変換します。reduce（集約）のフェーズでは、mapされた情報を集約します。処理内容それぞれに依存関係がないならば、その処理は複数のノードに分担して並列実行できます。

MapReduceの、もっとも単純で分かりやすい応用分野は、分散grepでしょう。grepはUnix系のOSに付属しているコマンドで、ファイルの中で指定したパターンにマッチする行を検索して出力するものです。grepは事前に検索のためのインデックスを作らず、その都度総当たりで調べるため、ファイルが巨大であったり、大量にある場合は時間がかかることがあります。MapReduceを使えば、対象ファイルのgrep処理を複数ノードで分担できるため、全体の処理時間を短縮することが期待できます。

IIJでは、前述のとおりフロー情報やサーバが出力するログを分散ストレージに格納しており、MapReduceを使ってデータの抽出や加工をしています。これらのデータの解析可能なパラメータの組合わせは多岐にわたっており、解析するポイントに応じて、様々なパラメータで解析できるようなシステムを構築しています。

フロー情報を解析する場合を例に、MapReduceの実際の動きを説明すると以下のようになります。

- 解析対象ルータ、対象期間と、抽出条件やグルーピングしたい軸等のパラメータを含む、MapReduceジョブリクエストを準備
- クライアントは、dddのノードのどれかに対しMapReduceジョブリクエストを送信する
- リクエストを受けたノードは、対象期間を一定時間間隔で分割する形で、MapReduceジョブを複数のmapタスクとreduceタスクに分解する
- mapタスクを各ノードに割り振り、各ノードはパラメータに従い、抽出やグルーピングの処理をする
- 各ノードでのmapタスクの実行が終わったら、reduceタスクを起動して結果を集約する
- 集約された結果は分散ストレージに書き出される。またはクライアントに返すことも可能

このようなシステムでは、ごく短期間のデータしか保持できなかったり、解析に長い時間がかかったりするものが多いですが、IIJでは多数のノードからなる分散システムを用いることで、長期間のデータから実用的な応答速度での解析を実現しています。

3.6 おわりに

IIJで開発した、dddという分散システムについて説明しました。dddを用いることで、膨大なデータを保持し処理することができます。今後、プロバイダのインフラで扱うデータはますます増加していくと考えられます。IIJでは継続してdddを開発し、社会基盤として信頼性の高いサービスを提供していきます。

執筆者：
前橋 孝広（まえばし たかひろ）
IIJ 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
dddの実装を始めとした、IIJのバックボーンネットワーク運用に関わるプログラムの開発を手がける。

4 メッセージングテクノロジー

本レポートはこれまで「メールテクニカルレポート」として発行していたものです。今号より名称を「メッセージングテクノロジー」と変更いたします。

4.1 はじめに

メッセージングテクノロジーでは、迷惑メールの最新動向や迷惑メール対策に関連する技術等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られる各種情報を元に様々な分析を行い、結果を公表しています。メールの流量は平日と休日の違いなど、曜日ごとの変動があるため、より傾向を把握しやすいように1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年の第14週(2009/03/30〜2009/04/05)から第26週(2009/06/22〜2009/06/28)までの13週、91日間を対象にしました。

メールの技術動向としては、送信ドメイン認証技術の受信側の導入状況とDKIMの利用方法の例を解説しています。

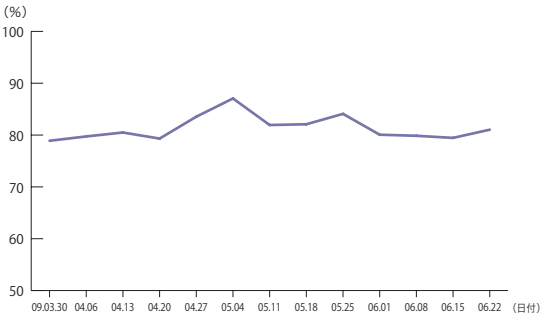


図-1　迷惑メールの割合

4.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IIJが提供する迷惑メールフィルタ機能によって検知され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。

4.2.1 迷惑メールの割合

2009年第14週から第26週までの91日間について週ごとの迷惑メールの割合の推移を図-1に示します。この期間の受信メール全体に対する迷惑メールの割合は、平均して81.6%でした。平均値としては前回(81.5%)とほぼ同水準でしたが、この期間の割合の推移には幾つか特徴的な変動がみられました。最も割合が高かったのは、第19週(2009/05/04〜2009/05/10)の87.1%でした。

これまでの傾向と同様に、この期間は5月の連休を含んでいたため、業務としての一般的なメール量が少なくなり、これにより相対的に迷惑メールの割合が高くなりました。しかし、この時期から迷惑メールの受信量そのものも急激に増加しています。特に、第18週(2009/04/27週)から第22週(2009/05/25週)にかけて迷惑メール量が増え、割合としても80%を超える高いレベルで推移しました。

その後、第23週(2009/06/01週)から迷惑メール量が若干減少傾向になりました。この時期の2009年6月4日に米連邦取引委員会(FTC)から発表された内容によれば[*1]、スパイウェアやフィッシング、児童ポルノなどの温床になっていると言われている、ISPのPricewert社のネットワークを遮断したと報告されています。Pricewert社は、3FNやAPS Telecomといった名義でのISP事業も行っており、昨年11月に遮断されたMcColo社[*2]と同様に、ボットネットの管理サーバ(Command & Control サーバ)も置かれていたと言われています。Pricewert社のネットワークが遮断されたことにより、ボットネットの活動が弱まり、迷惑メール量も減少したものと考えられます。しかし、今回はMcColo社のケースのような劇的な減少[*3]は見られな

＊1　http://www.ftc.gov/opa/2009/06/3fn.shtm
＊2　IIR vol.2（http://www.iij.ad.jp/development/iir/pdf/iir_vol02_mail.pdf）で解説
＊3　2008年第47週(11/17〜23)に迷惑メールの割合が68.0%まで減少

かったことから、対象となるボットネットの規模が小さかったか、送信者が事前に状況を察知してすでにネットワーク遮断に対する何らかの対策を講じた可能性が考えられます。

4.2.2 迷惑メールの送信元

この期間の迷惑メール送付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1位は、前回と同様にブラジル（BR）で、全体の11.8%を占めていました。前回（vol.3）が11.3%でしたので、微増したことになります。2位は米国（US）の11.4%で、前回（vol.3、10.9%）、前々回（vol.2、14.4%）と同じ順位でした。

今回の調査結果では、上位2カ国と3位以降に若干の開きがありました。3位は中国（CN、6.9%）で、4位は韓国（KR、5.6%）、5位はトルコ（TR、5.4%）、6位はインド（IN、5.3%）となりました。前回の調査結果と比べると、それぞれ若干の順位の入れ替えはありましたが、いずれも6位以内にすべて残ったままという結果になりました。日本（JP、2.6%）は前回と同様に11位でした。

これら6カ国に日本を加えた7カ国について、週単位での割合の推移を図-3に示します。ブラジルはいずれの週も高い割合で推移していますが、米国は5月中旬以降に割合を下げていることがわかります。中国は前々回（vol.2）で1位になって以降、割合が若干下がっていましたが、6月以降から高いレベルに戻りつつあり、再度注意が必要です。

日本に送られてくる迷惑メールの大部分が海外から送信されていることから、引き続き迷惑メール対策の国際連携が重要であると考えています。

4.2.3 迷惑メール対策の国際的な動向

これまで示してきたデータからもわかるように、迷惑メールの送信量は依然として高いレベルで推移しています。これは日本だけではなく世界的にも同様の傾向となっています。その送信元の多くは、一般ユーザのPCをマルウェアに感染させ、ネットワークの外部から操作する、ボットであると言われています。

日本では、一般ユーザが利用する動的IPアドレスから、外部ネットワークへの直接のメール送信を制限するOP25B[*4]を普及させたことにより、こういったボットを利用した、迷惑メール送信ができない環境を構築してきました。元々 OP25Bは、日本が最初に導入した技術ではなく、大手を含む米国のISP数社が導入していた技術です。国際的な迷惑メールの対策団体であるMAAWG[*5]が発足後に、迷惑メール送信側の対策として、有効な技術の一つと注目されました。日本の

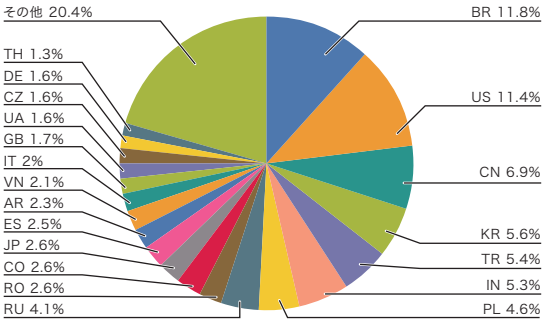


図-2　迷惑メールの送信元

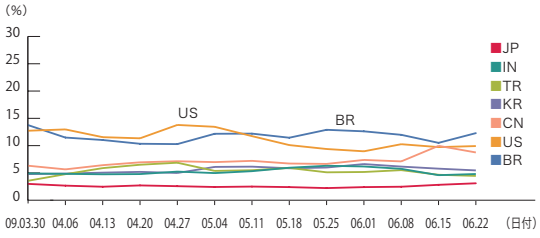


図-3　迷惑メール送信元の推移

＊4　Outbound Port 25 Blocking
＊5　MAAWG（Messaging Anti-Abuse Working Group）についてはインターネットトピックスを参照

JEAG[*6]で議論を重ねた結果、リコメンデーション（提言書）を発表[*7]し、これにより日本国内で急速に浸透しました。

OP25Bをより広範囲な地域に広めることによって、日本が受信する海外からの迷惑メールを減らすことができるはずです。そのため、IIJではMAAWGなどの国際会議の場や、政府と協調した活動を通して他国に対して、その有効性と技術概要を説き、導入を促す努力を継続してきました。その結果、一部の地域では導入が進みましたが、多くの地域では幾つかの理由により、導入がなかなか進んでいません。その詳細については、別の機会に解説したいと考えていますが、引き続きOP25Bの導入を促していきたいと考えています。

送信側の迷惑メール対策の動向としては、2008年11月のMcColo社、2009年6月のPricewert社のネットワーク遮断と続いたように、米国ではボットネットの管理元と思われるネットワークを遮断する動きが続いています。確かに、個別のボットにそれぞれ対処していくよりは、ボットに対して指令を送っている、管理元からの通信を遮断する手法の方が、一時的には大きな効果が得られます。しかしながら、今回のPricewert社の効果が限定的であったように、迷惑メールの送信側であるボットネットの管理者は、対応策を施し、既に新たな技術を導入している可能性があります。実際に、特定の管理元を持たずに、Peer-To-Peer技術を使って指令を伝播させていく、新たなボットネットの存在については以前から報告されていました[*8]。迷惑メール送信が、ビジネスとして成り立っている間は、こういった送信手法の高度化は続いていくものと考えられます。

送信側の対策として、最近ではWalled Garden[*9]という手法を導入する通信事業者も出てきています。Walled Gardenは、迷惑メール送信などを行っていると考えられるユーザの通信を、直接インターネットへ流さずに、特定の場所に囲い込む手法です。これにより、ボットの挙動を解析したり、マルウェア感染等により、意図せず不正な通信を行っている一般ユーザへ、注意喚起を行うことによって、セキュリティ対策を実施してもらうことができます。例えば、全てのウェブアクセス（HTTP/HTTPS）を特定のページに誘導させ、そのページでウィンドウズアップデートの実施を促したり、アンチウイルスソフトェアの実行を可能にして、PCがクリーンになるまでインターネットへ接続できないようにします。しかしWalled Gardenの手法には、怪しい挙動をしている通信元の特定や、Walled Gardenに誘導した利用者からの、問い合わせに対応する体制の整備等、課題も多くあります。

OP25Bは、迷惑メール送信については抑制できますが、例えば、ボットを利用したDDoS攻撃には対応できません。最近、米国や韓国の政府系ウェブサイトが閲覧できなくなるという事象が発生しましたが、この攻撃元にボットネットが使われているとの報道もあります。そのため、OP25Bの導入で安心することなく、Walled Gardenの手法も組み合わせることにより、クリーンなネットワーク環境を維持する努力も必要と考えています。

＊6　JEAG（Japan Email Anti-Abuse Group）は、2005年3月に主要ISPや携帯電話事業者を中心に創設された、迷惑メール対策のためのワーキンググループ（http://www.iij.ad.jp/news/pressrelease/2005/0315.html）
＊7　迷惑メール対策グループJEAGにおけるリコメンデーションの策定について（http://www.iij.ad.jp/news/pressrelease/2006/0223.html）
＊8　HotBots'07（http://www.usenix.org/events/hotbots07/tech/）
＊9　MAAWGではWalled Gardenに関するベストプラクティスを発表しています（http://www.maawg.org/about/whitepapers/MAAWG_Walled_Garden_BP_2007-09.pdf）

4.3 メールの技術動向

4.3.1 送信ドメイン認証技術の動向

日本のドメイン("jp"ドメイン)での送信ドメイン認証技術の、送信側での導入状況については、これまでも何度か引用してきたWIDEプロジェクトの調査結果[*10]があります。これにより、送信側の導入率、特にSPFレコードの宣言率の高さ(2009年5月時点で34.77%)を確認することができます。一方、メール受信側での、送信ドメイン認証技術の導入状況はどの程度進んでいるのでしょうか。

財団法人日本データ通信協会では、ISPや携帯電話事業者等、メールサービスを広く一般ユーザに提供している事業者を対象に、送信ドメイン認証技術の導入状況について調査を行い、結果を公表しています[*11]。調査結果によれば、2009年7月2日時点で、調査対象41社のうち、SPF(Sender Policy Framework)あるいはSenderIDの、受信側の認証を行っている事業者は13社となりました。割合としては約31.7%になりますが、対象をISPに限定すると約22.6%で、より低い普及率となります。DKIMの受信側の導入状況は、さらに低く約14.6%となっています。

今回の調査対象となっていない事業者は数多くあり、それぞれ調査対象でもメールの流量やアカウント数等の状況も異なるため、単純に受信側の送信ドメイン認証技術の普及率を示すことにはなりません。しかし、調査対象が通信事業者であることを考えると、「意外に少ない」というのが率直な感想です。受信側の認証を行うためには、新たな機能追加が必要になりますので、単純に比較はできませんが、送信側の普及率の高さと比較すると明らかに見劣りします。受信側の導入を促進させるためには、導入による効果や利点をより明確に示す必要があると考えています。

なお、今回の調査では個人系のメールサービスを対象としており、IIJではIIJ4U、IIJmioが対象のサービスとなります。そのため、DKIMの受信側の認証が未対応という結果になっていますが、IIJではSecureMXサービスで標準機能として DKIMの受信側認証を提供しており、これまで長い間、運用実績を持っています。現在この機能を個人系のサービスにも提供する準備を進めていることを補足しておきます。

4.3.2 DKIMの利用について

前回は、DKIMの認証の仕組みと送信側、受信側それぞれでの処理の概要について説明しました。今回は、DKIMの利点やその応用面について解説します。

DKIMは、秘密鍵を持っている送信者でなければ、作り出すことができない電子署名をメールに添付することにより、メールの送り手を認証します。電子署名は、メールの本文及びヘッダから作成されますので、これらの元になる情報が変更されない限り、署名を検証する公開鍵が入手可能ならば、いつでも検証することができます。そのため、ネットワークベースのSPF/SenderIDと違い、メールが転送されることによって認証が失敗する、ということがありません。この点はDKIMの大きな長所となっています。

逆にDKIMの認証が失敗するケースとして、メーリングリストなどで"Subject" ヘッダに、メーリングリスト名や番号などを付加する場合があります。こういった文字列の追加は、メールの改変にあたるため電子署名が一致しないことになり、認証が失敗します。このことは、しばしばDKIMの短所として取り上げられるポイントになっています。

しかし現在のメーリングリストの多くは、こういった"Subject"ヘッダへの情報の追加や、送信者情報の変更を既に行っており、もはや単なるメールの転送処理では無く、メーリングリストメンバへの再配送を行っているシステムといえます。つまり、メーリングリストのシステムが、配送されるメールの送信元にとなってお

＊10 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)
＊11 送信ドメイン認証実装状況(http://www.dekyo.or.jp/soudan/auth/)

り、DKIMの観点でみれば、本来はメーリングリストシステム側の署名を添付すべきと考えています。よって、DKIMのメーリングリストによる認証の失敗という問題については、配送時に電子署名を作成することによる回避を推奨しています。

メールの本文だけでDKIMの電子署名を認証できる利点は他にもあります。例えば、メールマガジンの購読を中止したり、改善を申し立てたりする際、そういった苦情を受ける送信側の立場では、申告者が本当に、送ったメールの受信者であるかどうかを確認したいはずです。ここで、メールの送信側が予め配信時にDKIMの電子署名を添付しておき、苦情を申告する側が、元々送られてきたメールを添付すれば、その添付されたメールを再認証することで、本当に送信されたメールか否かを確認することができます。また、こういった申告に利用可能な形式としても利用できるARF（Abuse Reporting Format）がIETFのInternet Draftとして公開され、標準化の議論が行われています。（図-4）

2.4 おわりに

今回のメッセージングテクノロジーでは、送信側の迷惑メール対策の最近の動きとして、ボットネットの管理元の対策の動きや、OP25B以外の送信側の対策手法として広がりつつある、Walled Gardenの手法を紹介しました。迷惑メールの送信は、送信している側はビジネスとして行っているために、日々技術革新を行い、迷惑メールが届くための工夫をしています。今後もネットワークの管理の在り方や、メールの送信側、受信側それぞれで総合的な対策が必要になってきます。本レポートでは、今後もこういった対策技術の紹介を継続していきます。

SPFレコードを一度記述して公開すれば良いSPF/Sender IDに比べて、DKIMの導入はなかなか進んでいないという現実があります。この背景には、費用対効果の関係もあると考えられますので、DKIMの長所や利用方法を紹介していくことにより、今後も普及を促進していきたいと考えています。

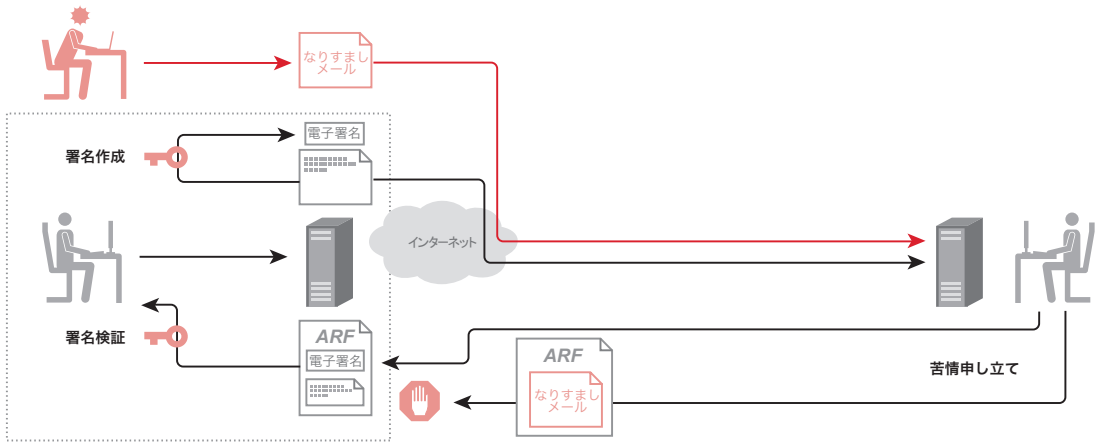


図-4　DKIMのARFでの利用例

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。

インターネットトピック: Messaging Anti-Abuse Working Group

■MAAWGとは

世界的な迷惑メールの増加を背景に、IIJを含む国際的な電気通信事業者やISP等19社は、2004年1月19日にMAAWG (Messaging Anti-Abuse Working Group) *1を設立しました*2。IIJはMAAWGの創設メンバとして、これまで5年間継続してMAAWGの活動に参加しています。今回は、MAAWGの活動内容や2009年6月に開催された16th General Meetingの様子を紹介します。

MAAWGのメンバは、主要ISPやESP(Email Service Providers)、メール配信業者やベンダ等、メールに関わる様々な企業によって構成されています。その数は、2008年末で161社まで増えています。MAAWGの活動は、主に迷惑メール(スパム)やウイルス等、メールの不正利用の対策が主体ですが、近年はそれらの送信元となっているボットネットの対策や、その原因となるマルウェア(不正プログラム)等多くの問題が議題になります。活動の成果として、MAAWG提言書(Recommendation)やベストプラクティス、ホワイトペーパー等、様々な文書を発表しています。これらはメンバ以外にも公開されており、MAAWGのウェブサイトから入手できます。

このように、現在のMAAWGメンバは、メールに関わる様々な側面をもった企業が参加しています。技術的な事柄を議論するTechnical Committee、運用的な問題を議論するCollaboration Committee、法執行関係者や国際機関との連携等の活動を行うPublic Policy Committee等、メンバがそれぞれの分野で議論を行っています。また特徴的なのが、送信事業者が集まるSenders SIGや、逆にISPに参加が限定されたISP Closed Colloquiumが開催される等テーマや参加者の役割に応じた、様々な議論が行われています

MAAWGメンバは、1年に3回開催されるGeneral Meetingで顔を会わせますが、それ以外にも普段からメーリングリストで、情報交換や各種文書の意見交換を行っています。また、メンバ間で直接連絡が取り合えるように、Abuse Contact Databaseが作られ、ISP間でメールの疎通がうまくいっていない場合に、状況確認に活用される等、国際的なメール環境の向上にも貢献しています。

■16th MAAWG General Meeting

MAAWGメンバが直接顔を会わせることができるGeneral Meetingは、MAAWGにとって貴重な機会となっています。近年は2月頃と10月頃に北米で、6月に欧州での開催が定着してきています。今回は、6月8日から6月11日にオランダのアムステルダムで開催された16th General Meetingの様子を紹介します。

MAAWGの設立当初は、誰でも参加できるオープンなセッションもありましたが、現在はMAAWGメンバと招待されたゲストだけが参加できる会合になっています。会合の内容をメンバ外に公開することも禁止されているため、セッションの内容について触れることはできませんが、概要について紹介します。

欧州での開催は、ITUやOECD等の国際機関の本部があることもあり、行政府関連の参加者が多くなる傾向があります。今回も欧州評議会や欧州刑事警察機構(ユーロポール)、米国FTCやオランダOPTA(独立郵便・電気通信庁)等、多くの組織が参加し、それぞれの取り組みなどについて発表しました。今回は、これまでの欧州開催で最も多い、19カ国、270名以上の参加となり、関心の高さ、逆にいえばこの分野の問題の深刻さを表しています。

General Meetingは、通常3日間開催され、朝の8時半から夕方の6時頃まで様々な議題のセッションが続きます。ほとんどがメールに関係した内容であり、複数のセッションが平行して開催されるため、この期間はほとんど会場のホテルに缶詰状態になります。メンバ間の親交を深めるためのSocial Eventも開催され、外に集まって日頃抱えている問題の解決や、各企業間の協調等の機会にもなっています。

日本で迷惑メール対策の活動を行っているJEAG*3 (Japan Email Anti-Abuse Group)は、このMAAWGの設立を背景に創設されました。MAAWGとの連携も行っており、JEAGのメンバがMAAWGのGeneral Meetingにゲストとして参加したり、JEAGの活動や日本での取り組みの紹介等を行っています。IIJは双方の設立メンバとして、日本と国際組織の橋渡し役としても、精力的に活動していきます。

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

＊1　http://www.maawg.org/
＊2　http://www.iij.ad.jp/news/pressrelease/2004/0119.html
＊3　http://www.jeag.jp/

Ongoing
Innovation

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-MKTG021AA-0908KO-08000PR