

Internet Infrastructure Review

IIJ

Internet Initiative Japan

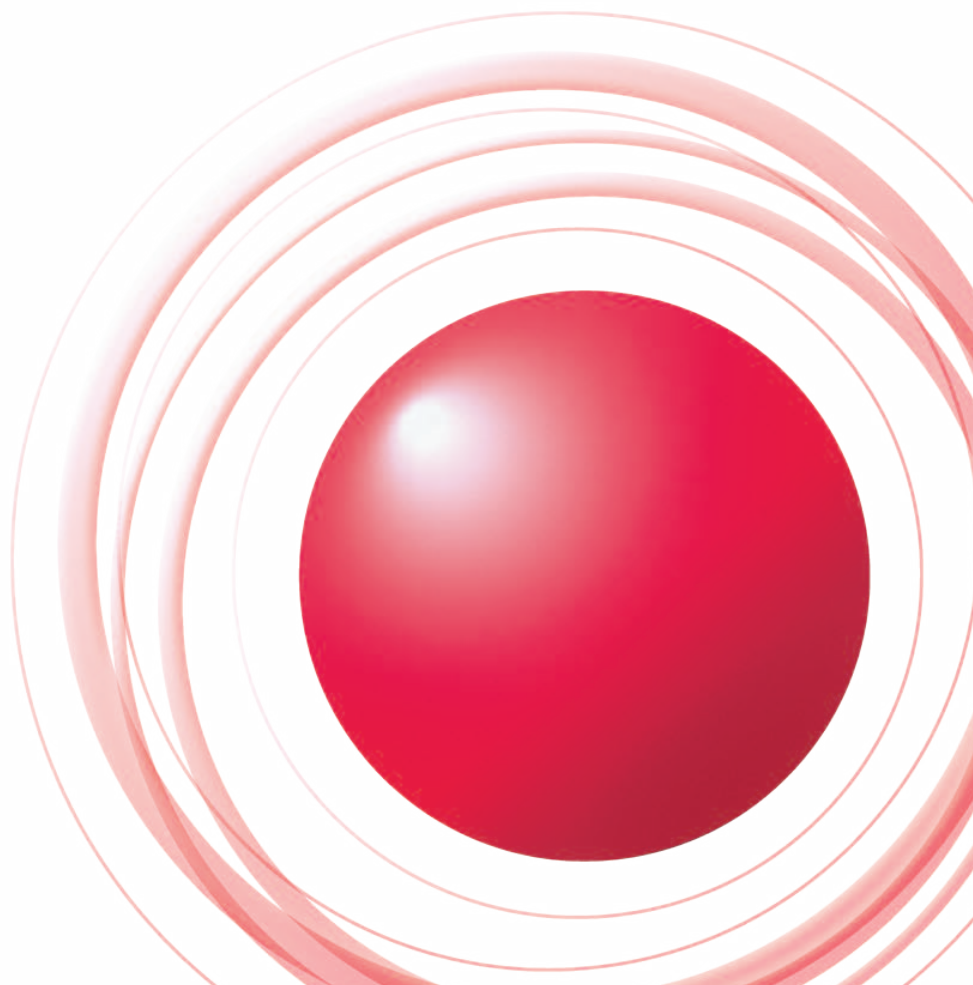
Vol.8

August
2010

インフラストラクチャセキュリティ
暗号アルゴリズムの2010年問題

メッセージングテクノロジー
欧州各国での迷惑メールの送信元割合が増加

ブロードバンドトラフィックレポート
P2Pファイル共有からWebサービスへ
シフト傾向にあるトラフィック



エグゼクティブサマリ	3
1. インフラストラクチャセキュリティ	4
1.1 はじめに	4
1.2 インシデントサマリー	4
1.3 インシデントサーベイ	6
1.3.1 DDoS攻撃	6
1.3.2 マルウェアの活動	8
1.3.3 SQLインジェクション攻撃	10
1.4 フォーカスリサーチ	11
1.4.1 暗号アルゴリズムの2010年問題の動向	11
1.4.2 DDoS攻撃によるbackscatterの観測	16
1.4.3 脆弱性情報の流通動向	19
1.5 おわりに	21
2. メッセージングテクノロジー	22
2.1 はじめに	22
2.2 迷惑メールの動向	22
2.2.1 迷惑メールの割合は微減したが、レベルは依然高いまま	22
2.2.2 迷惑メール送信元の1位は中国、欧州も増加傾向	23
2.3 メール技術動向	24
2.4 おわりに	24
3. ブロードバンドトラフィックレポート	25
3.1 はじめに	25
3.2 データについて	26
3.3 利用者の1日の使用量	26
3.4 ポート別使用量	28
3.5 おわりに	30
インターネットトピック:	
マネージドセキュリティサービス(MSS)選定ガイドラインの紹介	31

エグゼクティブサマリ

インターネットは、私たちの日常生活をさまざまな面で支える社会インフラです。今日ではたくさんの情報サービスがインターネットを利用しており、情報社会を生きる私たちにとって、インターネットはまさにライフラインとして無くてはならない存在になりました。そのようなネットワークであるがゆえに、社会的出来事が、インターネットの振舞いに大きな影響を与えるようになってきています。

例えば、2010年1月に日本のブロードバンドトラフィック量が2割近く減少しましたが、これほど大きく、かつ継続的にトラフィックが減少した事は、インターネットの商用化以来初めての事でした。原因は、同じく1月に施行された改正著作権法で、違法コンテンツのダウンロードが違法化されたためだと言われています。この仮説の元でトラフィックの動向を分析する事で、実際にネットワーク上で何が起こったのかを詳細に把握する事ができるのです。同様に、セキュリティ面でも、社会情勢や歴史的な出来事を踏まえてインシデントを想定して備えたり、起こった事象を解析したりする事が不可欠となっています。

このように、我々サービスプロバイダは、広く社会全般の出来事を付き合いながら、実際にネットワークで起こった事象を解析しないと、インターネットの安定運用や持続的発展をもちや担保できない時代になってきたといえるでしょう。

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

「インフラストラクチャセキュリティ」の章では、2010年4月から6月月末までの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、暗号アルゴリズムの2010年問題の動向、DDoS攻撃によるbackscatter観測、そして、脆弱性情報の流通動向についてご紹介いたします。

「メッセージングテクノロジー」の章では、2010年4月から6月までの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、送信ドメイン認証技術の導入状況についての報告を行います。

「ブロードバンドトラフィックレポート」の章では、上述のトラフィック変化を踏まえ、2010年5月24日から一週間のIIJのブロードバンド接続サービスのトラフィックの状況を、1年前の解析結果(IIR Vol4に掲載)と比較しながら解析し、1年間で何がどのように変化したのかを検証します。

「インターネットトピック」としては、日本セキュリティオペレーション事業者協議会 (ISOG-J) がまとめたマネージドセキュリティサービス(MSS)選定ガイドラインについてご紹介いたします。

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

執筆者:

浅羽 登志也(あさば としや)

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。

暗号アルゴリズムの2010年問題

今回は、2010年4月から6月に発生したインシデントに関する報告とともに、暗号アルゴリズムの2010年問題の動向、DDoS攻撃によるbackscatterの観測、脆弱性情報の流通に関する動向を取り上げます。

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IJ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、IJ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4月から6月までの期間では、以前のレポートでも取り上げたGumblar類似のインシデントが継続した一方で、ブログシステム等を直接攻撃してコンテンツを改ざんし、マルウェア感染に誘導する事件も発生しています。脆弱性に関しても、Webブラウザに関するものが相次いで発見されています。このほかのインシデントとしては、特定の国や特定の企業を対象とした標的型攻撃が行われました。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

1.2 インシデントサマリー

ここでは、2010年4月から6月までの期間にIJが取り扱ったインシデントと、その対応を示します。この期間に取り扱ったインシデントの分布を図-1に示します*1。

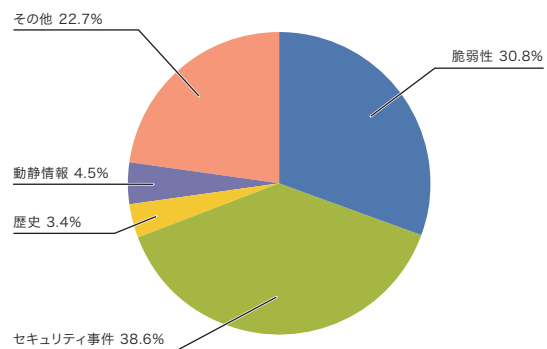


図-1 カテゴリ別比率(2010年4月～6月)

*1 このレポートでは取り扱ったインシデントを、脆弱性、動静情報、歴史、セキュリティ事件、その他の5種類に分類している。
 脆弱性: インターネットやユーザの環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェア等の脆弱性への対応を示す。
 動静情報: 要人による国際会議や、国際紛争に起因する攻撃等、国内外の情勢や国際的なイベントに関連するインシデントへの対応を示す。
 歴史: 歴史上の記念日等で、過去に史実に関連して攻撃が発生した日における注意・警戒、インシデントの検知、対策等の作業を示す。
 セキュリティ事件: ワーム等のマルウェアの活性化や、特定サイトへのDDoS攻撃等、突発的に発生したインシデントとその対応を示す。
 その他: イベントによるトラフィック集中等、直接セキュリティに関わるものではないインシデントや、セキュリティ関係情報を示す。

■ 脆弱性

今回対象とした期間では、マイクロソフト社のInternet Explorer^{*2}、アドビ社のAdobe ReaderとAcrobat^{*3*4}、Flash Player^{*5}、Shockwave Player^{*6}、製品のアップデートに利用されているAdobe Download Manager^{*7}、オラクル社のJava Deployment Toolkit^{*8}等、Webブラウザ自体と、そのプラグインに関する脆弱性が数多く発見され、修正されています。また、OSに関しても、Windows XPとWindows Server 2003の脆弱性^{*9}が修正され、Mac OS Xでも複数の脆弱性^{*10*11}が修正されています。アプリケーションでは、ジャストシステム社の一太郎の脆弱性^{*12}が修正されています。これらの脆弱性のうちいくつかは、対策が公開される前に悪用が確認されました。

■ 動静情報

IJ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、6月から開催されたサッカーワールドカップ等に注目しましたが、関連する攻撃は検出されませんでした。

■ 歴史

この期間には、過去に歴史的背景によるDDoS攻撃やホームページの改ざん事件が発生したことがあります。このため、各種の動静情報に注意を払いましたが、IJの設備やIJ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、ベトナムのユーザを対象とした標的型攻撃^{*13}で構築されたボットネットが発見されました^{*14}。また、インドの政府機関や企業等、複数の対象を監視しているとされるスパイ・ネットに関する報告^{*15}が発表されました。

マルウェアの活動では、昨年からのGumblarに類似した事件が継続して発生し、感染した端末に導入されるPushdoと呼ばれるボット型マルウェアによる目的不明なSSLの通信の増加が確認されています^{*16}。さらに、米国のホスティングサービス^{*17 *18}を利用しているブ

- *2 マイクロソフト セキュリティ情報MS10-035-緊急Internet Explorer用の累積的なセキュリティ更新プログラム(982381) (<http://www.microsoft.com/japan/technet/security/bulletin/ms10-035.mspx>)。
- *3 Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB10-09 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-09.html>)。
- *4 Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB10-15 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-15.html>)。
- *5 Adobe Flash Player用セキュリティアップデート公開 APSB10-14 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-14.html>)。
- *6 Shockwave Player用セキュリティアップデート公開 APSB10-12 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-12.html>)。
- *7 Security updates available for Adobe Reader and Acrobat APSB10-02 (<http://www.adobe.com/support/security/bulletins/apsb10-02.html>)。
- *8 Oracle Corporation, JavaTM SE 6 アップデートリリースノート (<http://java.sun.com/javase/ja/6/webnotes/6u20.html>)。
- *9 マイクロソフト セキュリティ アドバイザリ (2219475) Windowsのヘルプとサポート 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 (<http://www.microsoft.com/japan/technet/security/advisory/2219475.mspx>)。なお、本稿執筆時点では 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>)、にて修正されている。
- *10 セキュリティアップデート 2010-003のセキュリティコンテンツについて (http://support.apple.com/kb/HT4131?viewlocale=ja_JP)。
- *11 セキュリティアップデート2010-004 / Mac OS X v10.6.4 のセキュリティコンテンツについて (http://support.apple.com/kb/HT4188?viewlocale=ja_JP)。
- *12 JVN#98467259 一太郎シリーズにおける任意のコードが実行される脆弱性 (<http://jvn.jp/jp/JVN98467259/>)。
- *13 標的型攻撃に関しては、本レポートの Vol.7 「1.4.2 標的型攻撃とOperation Aurora」でも解説している (http://www.ij.ad.jp/development/iir/pdf/iir_vol07.pdf)。この種の攻撃には技術的な対応策がなく、ユーザ教育等の長期的な対策が必要となるため、Advanced Persistent Threat (APT) と呼ばれることもある。
- *14 詳細については次のトレンドマイクロ社のBlogに詳しい。ベトナムへの標的型攻撃か。正規ソフトウェアやドライバの更新を促す不正プログラム (<http://blog.trendmicro.co.jp/archives/3396>)。
- *15 詳細については次のShadowserver Foundationの発表を参照のこと (<http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20100406>)。日本語で参照できる情報としては、エフセキュアブログがある。Shadows in the Cloud (<http://blog.f-secure.jp/archives/50386788.html>)。
- *16 JPCERT/CC Alert 2010-04-28: いわゆるGumblarウイルスによってダウンロードされるDDoS攻撃を行うマルウェアに関する注意喚起 (<https://www.jpCERT.or.jp/at/2010/at100011.txt>)。また日本シーサート協議会では、このボットネットによる通信について観測とまとめを行っている (<http://www.nca.gr.jp/2010/pushdo-ssl-ddos/>)。
- *17 Network SolutionsのBlogでは、WordPressの脆弱性についてユーザに注意を呼び掛けている。Alert: WordPress Blog & Network Solutions (<http://blog.networksolutions.com/2010/alert-wordpress-blog-network-solutions/>)。
- *18 Go DaddyのBlogでは、コンテンツ改ざんについてユーザに注意を呼び掛けている。What's Up with Go Daddy, WordPress, PHP Exploits and Malware? (<http://community.godaddy.com/godaddy/whats-up-with-go-daddy-wordpress-php-exploits-and-malware/>)。

ログサイトでWordPress^{*19}等への攻撃が活発となり、多数のコンテンツが改ざんされて不正な別のWebサイトに誘導され、マルウェアに感染させられる事件が発生しました^{*20}。

また、日本国内で発生した巧妙な文面による標的型攻撃メールについて、JPCERT/CCから注意喚起^{*21}が行われました。標的型攻撃については、IPAからその特徴と対策方法をまとめた報告^{*22}が公開されています。

■ その他

その他のセキュリティに関する動向としては、日本でも準備が進められているDNSSECの導入^{*23}に向けて、DNSの最上位階層であるルートゾーンに署名を導入するためのTCRの選定^{*24}が行われました(署名は2010年7月に実施)。また、クラウド・コンピューティングに関するセキュリティを検討する団体、CLOUD SECURITY ALLIANCE (CSA) JAPAN CHAPTER (日本クラウドセキュリティアライアンス^{*25})の設立に向けたシンポジウムが開催されました。

1.3 インシデントサーベイ

IJでは、インターネット上で発生するインシデントのうち、インフラストラクチャ全体に影響を与える可能性があるインシデントに注目し、継続的な調査研究と対処を行っています。ここでは、そのうちDDoS攻撃、ネットワーク上のマルウェアの感染活動、Webサーバに対するSQLインジェクション攻撃の実態について、その調査と分析の結果を示します。

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになってきました。DDoS攻撃の内容は、状況により多岐にわたりますが、一般には、脆弱性等の高度な知識を利用した攻撃ではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にしたりすることで、サービスの妨害を狙ったものになっています。図-2に、2010年4月から6月の期間にIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。

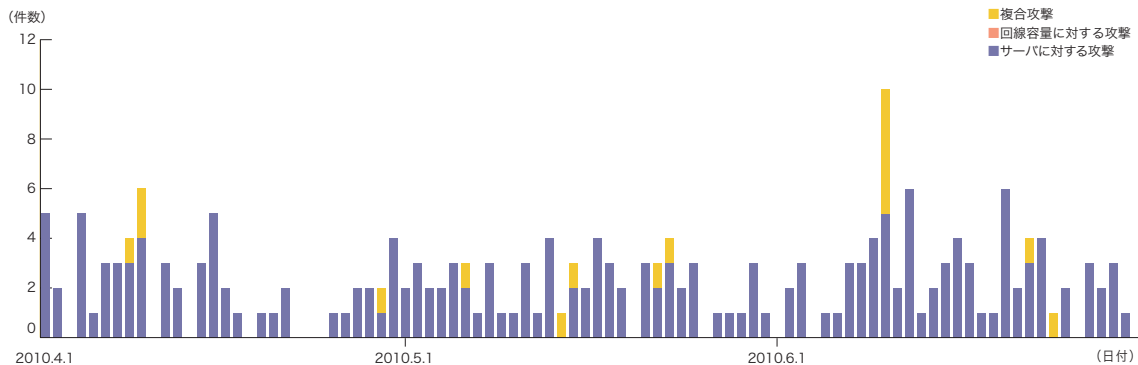


図-2 DDoS攻撃の発生件数

*19 WordPressはオープンソースのブログソフトウェア(<http://wordpress.org/>)。
 *20 詳細については、例えば次のトレンドマイクロ社のBlogに詳しい。WordPress Blogs Suffer from a Mass Compromise (<http://blog.trendmicro.com/wordpress-blogs-suffer-mass-compromise/>)。
 *21 JPCERT/CC (一般社団法人JPCERTコーディネーションセンター)による、JPCERT/CC Alert 2010-06-01社内PCのマルウェア感染調査を騙るマルウェア添付メールに関する注意喚起 (<http://www.jpcert.or.jp/at/2010/at100013.txt>)
 *22 IPA (独立行政法人情報処理推進機構)による、実例から分かる標的型攻撃メールの「違和感に気付くポイント」と「違和感に気付いた後の対策ポイント」～「脆弱性を狙った脅威の分析と対策について Vol.3」の公開～ (<http://www.ipa.go.jp/about/press/20100602.html>)。
 *23 DNSSECに関する日本国内での動向については、次のJPRSによるDNSSEC関連情報 (<http://jprs.jp/dnssec/>)に詳しい。
 *24 TCR (Trusted Community Representatives)はルートDNSサーバに使用する鍵を生成・更新権限を持つ人。2010年7月に実施されるルートゾーンへの署名導入に伴い、2010年6月に選任された (<http://www.root-dnssec.org/tcr/selection-2010/>)。
 *25 CLOUD SECURITY ALLIANCE JAPAN CHAPTER (<http://www.cloudsecurityalliance.jp/>)。

ここでは、IJ 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。IJでは、ここに示す以外のDDoS攻撃にも対処していますが、正確な攻撃の実態を把握することが困難なため、この集計からは除外しています。

DDoS攻撃には多くの攻撃手法が存在します。また、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃^{*26}、サーバに対する攻撃^{*27}、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IJは、205件のDDoS攻撃に対処しました。1日あたりの対処件数は2.25件で、平均発生件数は前回のレポート期間のものと同じく変わっていません。DDoS

攻撃全体に占める割合は、回線容量に対する攻撃が0%、サーバに対する攻撃が92%、複合攻撃が8%でした。

今回の対象期間で観測された最も大規模な攻撃はサーバに対する攻撃に分類したもので、約4万ppsのパケットによって160Mbpsの通信量を発生させたものでした。また、攻撃の継続時間は、全体の92%が攻撃開始から30分未満で終了し、8%が30分以上24時間未満の範囲に分布しています。今回の期間中では24時間以上継続する攻撃は見られませんでした。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されています。これは、IPスプーフィング^{*28}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^{*29}の利用によるものと考えられます。

*26 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。

*27 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消費させる。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。

*28 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。

*29 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、IJが実施しているマルウェアの活動観測プロジェクトMITF*30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*31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アドレスの国別分類を図-4にそれぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っています。ここでは1台あたりの平均をとり、

到着したパケットの種類(上位10種類)ごとに推移を示しています。

ハニーポットに到着した通信の多くは、マイクロソフト社のOSで利用されているTCPポートに対する探索行為でした。また、前回の集計期間と同様に、シマンテックのクライアントソフトウェアが利用する2967/TCP、SSHで利用する22/TCPに対する探索行為が観測されています。一方で、25162/TCP、10263/TCP、15636/TCP等、一般的なアプリケーションで利用されていない目的不明の通信も観測されました。

発信元の国別分類を見ると、中国の21.1%、日本国内の19.4%、台湾の7.0%が比較的大きな割合を占めています。

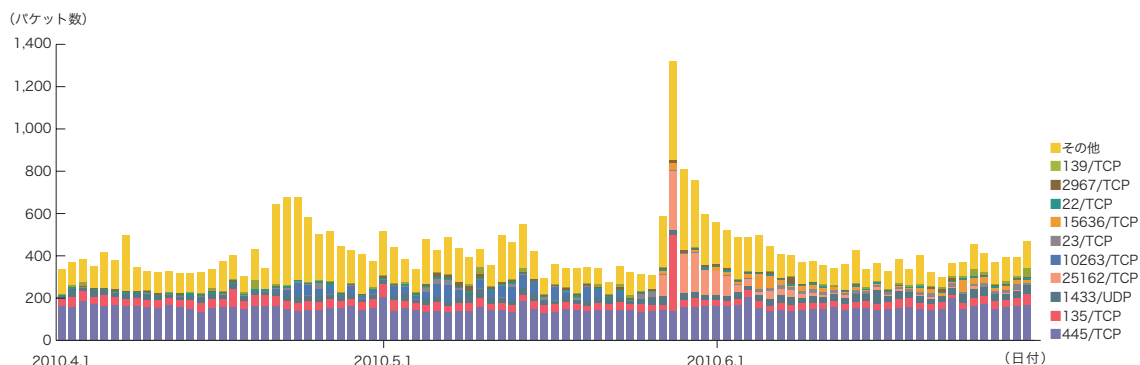


図-3 ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

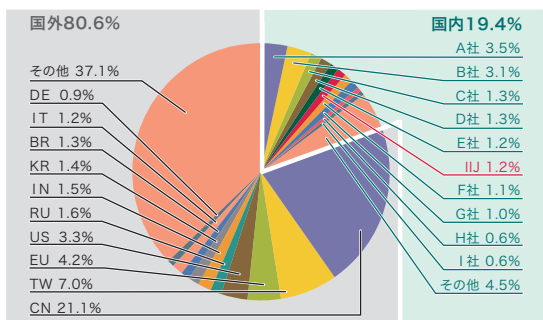


図-4 発信元の分布(国別分類、全期間)

*30 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。より詳しくは、本レポートの Vol.7 「1.4.3 マルウェア対策活動MITF」を参照のこと (http://www.ij.ad.jp/development/iir/pdf/iir_vol07.pdf)。

*31 脆弱性のエミュレーション等の手法で、攻撃を受けつけて被害に遭ったふりをし、攻撃者の行為やマルウェアの活動目的を記録する装置。

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの取得検体数の推移を図-5に、マルウェアの検体取得元の分布を図-6にそれぞれ示します。図-5では、1日あたりに取得した検体^{*32}の総数を総取得検体数、検体の種類をハッシュ値^{*33}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378、ユニーク検体数が32です。前回の集計期間での平均値が総取得検体数で479、ユニーク検体数で37でした。今回は、総取得検体数、ユニーク検体数ともに、前回より減少傾向が見られました。

検体取得元の分布では、日本国内が49.6%、国外が50.4%でした。このうちIJのユーザ同士のマルウェア感染活動は0.1%で、前回の観測期間に続いて低い値

を示しています。なお、台湾が28.9%と前回に引き続き多くの割合を占めていますが、これは台湾においてSdbotとその亜種の活動が活発になっているためと考えられます。

MITFでは、マルウェアの解析環境を用意し、取得した検体について独自の解析を行っています。この結果、この期間に取得した検体は、ワーム型16.8%、ボット型73.3%、ダウンロード型9.9%となりました。また、この解析により、27個のボットネットC&Cサーバ^{*34}と4個のマルウェア配布サイトの存在を確認しています。マルウェア配布サイトの検出数の減少は、取得した検体にダウンロード型の検体が減少したこと、従来見られていた複数の配布サイトにアクセスする検体が減少したことによります。

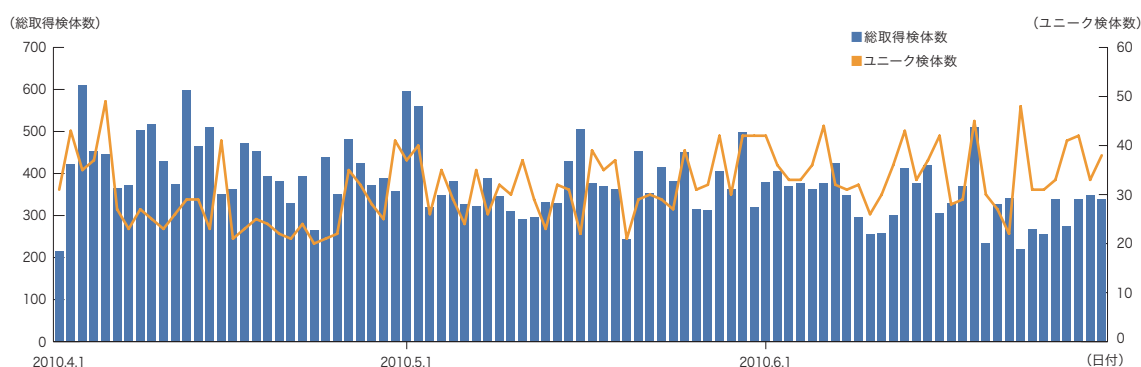


図-5 取得検体数の推移(総数、ユニーク検体数)

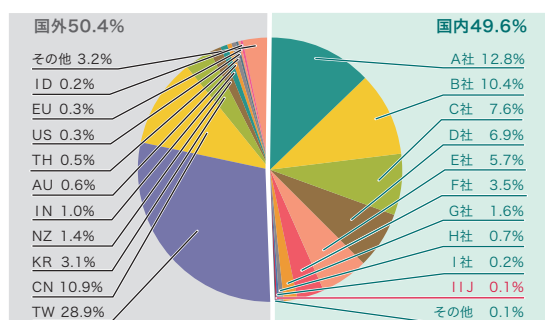


図-6 検体取得元の分布(国別分類、全期間)

*32 ここでは、ハニーボット等で取得したマルウェアを指す。

*33 様々な入力に対して一定長の出力をする一方性関数(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。

*34 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

IJ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^{*35}について継続して調査を行っています。SQLインジェクション攻撃は、過去にもたびたび流行し話題となった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

2010年4月から6月までに検知した、Webサーバに対するSQLインジェクション攻撃の推移を図-7に、攻撃の発信元の分布を図-8にそれぞれ示します。これらは、IJ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31.3%、中国24.7%、米国11.8%となり、以下その他の国々が続いています。

今回、Webサーバに対するSQLインジェクション攻撃の発生状況に大幅な増加が見られました。これは、主に中国や米国等の海外から、特定少数のWebサーバに対する攻撃が増加したためです。国内からの攻撃に関しては前回と同様の状況でした。

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

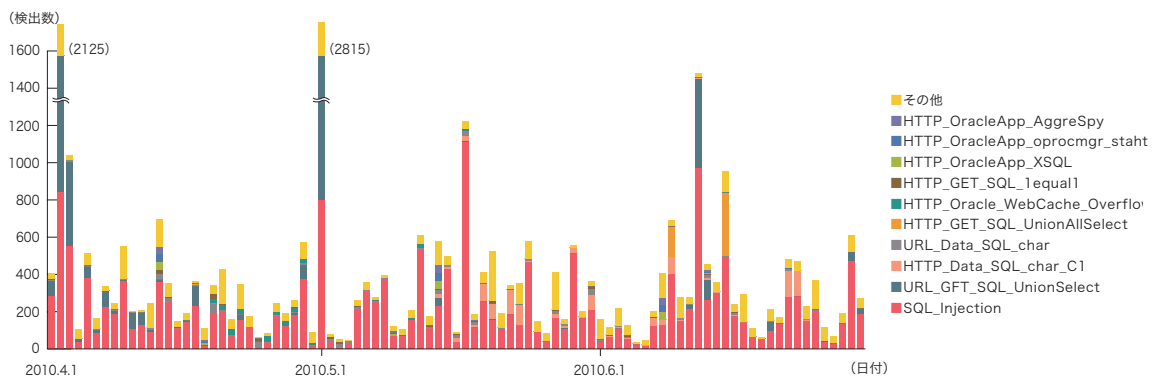


図-7 SQLインジェクション攻撃の推移(日別、攻撃種類別)

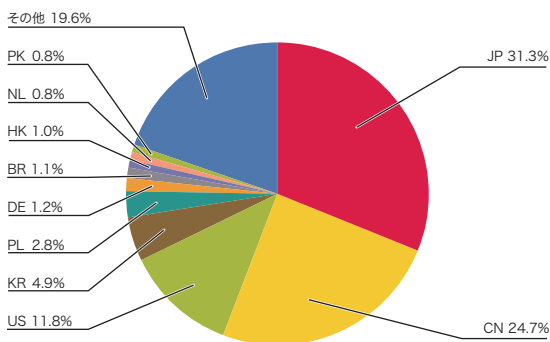


図-8 SQLインジェクション攻撃の発信元の分布(国別分類、全期間)

*35 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、IJ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、暗号アルゴリズムの2010年問題の動向、DDoS攻撃によるbackscatterの観測、脆弱性情報の流通動向を取り上げます。

1.4.1 暗号アルゴリズムの2010年問題の動向

米国国立標準技術研究所 (NIST)^{*36}による次世代暗号アルゴリズムへの移行宣言^{*37}を皮切りに、さまざまな場面において暗号アルゴリズムの2010年問題が無視できない状況になっています。発端は、CRYPTO2004でのJouxやWangらによる複数の暗号学的ハッシュ関数への攻撃^{*38}に関する発表でした。この発表を受け、NISTから2010年までに米国政府におけるSHA-1の利用を中止するとのコメントが出されたことで、この期限が暗号アルゴリズムの2010年問題として広く知られるようになりました^{*39}。その後、SHA-1以外の暗号アルゴリズムの移行スケジュールについても詳細化され、今後いくつかのアルゴリズムが使えなくなることが示されています (NIST's Policy on Hash Functions^{*40}、およびSP800-57^{*41})。ここでは、NISTがなぜ暗号アルゴリズムを移行する判断を下したのか、またこの移行が及ぼす影響について解説します。

■ 暗号アルゴリズムの危殆化

暗号アルゴリズムについて、設計当初想定したよりも低いコストで「セキュリティ上の性質」が危うくなる状況を「危殆化(きたいか)」と呼びます^{*42}。ここでのセキュリティ上の性質とは、共通鍵暗号と公開鍵暗号におい

ては、秘密鍵を持つ場合のみ平文を復号できる性質であり、平文と暗号文のペアや公開鍵から、秘密鍵の推定が困難である性質を指します。ハッシュ関数においては、一方方向性(ハッシュ後のデータから元データを見つけることが困難である性質)と衝突困難性(ハッシュ後のデータが同じになるような2つの異なる元データを見つけることが困難である性質)がこれにあたります。

危殆化の要因の1つとしては、CPU処理能力の増大に伴う解析能力の向上が考えられます。処理能力の増大は、攻撃者側の立場で考えると、それまでと同じコストで解読に利用できる計算能力が向上することを意味します。実際に、最近では高性能なハードウェアが安価に入手できるようになっています。例えば、中間者CA証明書偽造問題でのMD5コリジョン探索には、クラスタ化したブレイステーション3が用いられました^{*43}。また、ハードウェアを準備せずに計算能力を時間単位で購入できるクラウドサービスも簡単に利用できるようになる等、ほとんど初期コストをかけずに膨大な計算能力を容易に手に入れられる環境が整いつつあります。

一方で、暗号解読研究の進展が危殆化を招くケースもあります。このような場合の厄介な点は、利用中の暗号アルゴリズムについて、ある日突然、急激に危殆化が進行することです。このための対策として、数学的バックグラウンドの異なる複数のアルゴリズムの利用が考えられます。実際に、SSL/TLSが搭載されたWebブラウザには、複数のアルゴリズムが搭載され、利用者が選択できるような実装もあります^{*44}。

■ 安全性低下の表現

暗号アルゴリズムの危殆化がどの程度進行しているかを把握するための指標として、「nビット安全性」という

*36 国立標準技術研究所 National Institute of Standards and Technology (<http://www.nist.gov/>)。アメリカ合衆国商務省配下の組織で暗号政策の中心的機関である。

*37 NIST Brief Comments on Recent Cryptanalytic Attacks on Secure Hashing Functions and the Continued Security Provided by SHA-1、2004年8月25日 (http://csrc.nist.gov/groups/ST/toolkit/documents/shs/hash_standards_comments.pdf)。

*38 CRYPTREC Report 2004の2.1.3.3節に詳しい。(http://www2.nict.go.jp/y/y213/cryptrec_publicity/c04_wat_final.pdf)。

*39 宇根、神田、暗号アルゴリズムにおける2010年問題について、日本銀行金融研究所ディスカッション・ペーパー 2005-J-22 (<http://www.imes.boj.or.jp/japanese/jdps/2005/05-J-22.pdf>)。

*40 NIST's Policy on Hash Functions、2006年3月15日 (<http://csrc.nist.gov/groups/ST/hash/policy.html>)。

*41 NIST Special Publication 800-57 Recommendation for Key Management - Part 1: General (http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf)。

*42 IPA、暗号の危殆化に関する調査報告書 (http://www.ipa.go.jp/security/fy16/reports/crypt_compromise/documents/crypt_compromise.pdf)。

*43 MD5 considered harmful today (<http://www.win.tue.nl/hashclash/rogue-ca/>)。

*44 WebブラウザOpera (<http://jp.opera.com/>)では、[詳細設定]-[セキュリティ]-[セキュリティプロトコル]-[詳細]からセキュア通信に利用するアルゴリズムを一覧・選択することができる。

概念を利用します。暗号アルゴリズムの攻撃^{*45}に 2^n (2 の n 乗)の計算量が必要なとき、当該アルゴリズムの強度を「 n ビット安全性」を持つと表記します。つまり、特定の暗号アルゴリズムについて、そのアルゴリズムの「セキュリティ上の性質」を危うくするために必要となる実際の計算量で、危殆化の状況を表現します。共通鍵暗号においては、全数探索する際の鍵空間の大きさが 2^n (n は共通鍵ビット長)、ハッシュ関数の例としては、一方向性で 2^n 、衝突困難性で $2^{(n/2)}$ (n は出力ビット長)が攻撃に必要な計算量の理論値となります。

危殆化の要因として2番目に示した暗号解読研究の進展により、本来持つはずの安全性が低下した暗号アルゴリズムとしては、例えばTriple DESがあります。2-key Triple DES、3-key Triple DESはそれぞれ鍵長が112ビットと168ビットです。このため、 n ビット安全性の理論値は112ビットと168ビットになります。しかし、暗号解読研究の結果、現時点ではそれぞれ80ビットと112ビットまで危殆化が進んでいます(先述のSP800-57等)。またハッシュ関数の例としては、出力長が128ビットのMD5は一方向性として123.4ビット安全性(理論値: 128ビット安全性)^{*46}、出力長が160ビットのSHA-1は衝突困難性として63ビット安全性

(理論値: 80ビット安全性)^{*47}まで低下しています。

また、公開鍵暗号についても n ビット安全性で表現する方法が試みられ、鍵長に応じた対応付けがなされています。例えば、RSA暗号については、1999年にはLenstraらによる評価^{*48}が、翌2000年にRSAラボラトリによる評価^{*49}が発表されました。この2つの評価には差異がありましたが、2004年のLenstraらによる再評価^{*50}、2007年のNISTによる評価(前述のSP800-57)と、最新版が2010年に発行されたECRYPT2^{*51}による評価^{*52}等では、中間的で妥当であると考えられる数値が示されました。例えば、共通鍵暗号の80ビット安全性に対応するRSA暗号の鍵長は、1329 (Lenstra)、1024 (NIST)、1248 (ECRYPT2)となっています(表-1)。逆の見方をすると、RSA-1024は、NISTの評価では80ビット安全性と等価ですが、ECRYPT2では73ビット安全性しか持たないと評価されています。

一方で楕円曲線暗号については、NISTとECRYPT2の両報告ともに、鍵長 n ビットの場合に $n/2$ ビット安全性を持つと評価され、差異はありませんでした。しかし、2010年1月の富士通による評価^{*53}では、表-2に示すようにNISTらに比べ少し強いと評価されています。

表-1 RSA暗号における等価安全性の評価比較

nビット 安全性	Lenstra (1999)	RSA Lab (2000)	Lenstra (2004)	NIST (2007)	ECRYPT2 (2010)	FUJITSU (2010)
56		430			640	
64	682		640		816	850
80	1513	760	1329	1024	1248	1219
112	4509		3154	2048	2432	2206
128	6669	1620	4440	3072	3248	2832
192				7680	7936	6281
256				15360	15424	11393

表-2 楕円曲線暗号における等価安全性の評価比較

nビット安全性	NIST, ECRYPT2	FUJITSU
64	128	122
80	160	152
112	224	214
128	256	245
192	384	371
256	512	497

*45 共通鍵暗号方式における一般的な攻撃には、候補となる共通鍵をひとつひとつ試して鍵を同定する全数探索攻撃がある。一方で、ある暗号アルゴリズムに特有の構造に欠陥が見つかった場合には、全数探索攻撃よりも計算量の少なく済む効率的な攻撃が用いられる。公開鍵暗号においては安全性の根拠となる数学的困難性に依存する。例えばRSAの場合、合成数の素因数分解ができれば秘密鍵が求められるため、効率のよい素因数分解方法が攻撃として用いられる。

*46 Yu Sasaki, Kazumaro Aoki, Finding Preimages in Full MD5 Faster Than Exhaustive Search, EUROCRYPT2009 (<http://www.springerlink.com/content/d7pm142n58853467/>)。

*47 RSA Laboratories, SHA1 Collisions can be Found in 2^{63} Operations (<http://www.rsa.com/rsalabs/node.asp?id=2927>)。

*48 Arjen K. Lenstra, Eric R. Verheul, Selecting Cryptographic Key Sizes (<http://www.win.tue.nl/~klenstra/key.pdf>)。

*49 A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, RSA Laboratories' Bulletin #13 (<http://www.rsa.com/rsalabs/node.asp?id=2088>)。

*50 Arjen K. Lenstra, Key Lengths (Contribution to The Handbook of Information Security) (<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.90.213>)。

*51 European Network of Excellence in Cryptology II。暗号に関する2008年8月から2012年7月までのリサーチプロジェクトであり、EU欧州委員会におけるFP7 (Seventh Framework Programme) と呼ばれる計画のうち情報通信技術 (ICT) にカテゴライズされたプロジェクトのひとつである (<http://cordis.europa.eu/fp7/ict/>)。

*52 ECRYPT II yearly report on algorithms and key sizes (2009-2010), EU FP7, ICT-2007-216676 (<http://www.ecrypt.eu.org/documents/D.SPA.13.pdf>)。

*53 富士通研究所、楕円曲線暗号とRSA暗号の安全性比較 (<http://jp.fujitsu.com/group/labs/techinfo/technote/crypto/cryptanalysis.html>)。

この危険化の指標では、 n を大きくすることが安全性を向上させることとなります。つまり、共通鍵暗号や公開鍵暗号では鍵長を長くすることで、ハッシュ関数では出力ビット長を長くすることで、大きな n を確保できます。ただし、一般的には、鍵長や出力ビット長を長くすることは暗号処理にかかる時間が大きくなる傾向となるため、計算処理の負荷や利用者の利便性を考慮した上で、利用するアルゴリズムと鍵長を選択する必要があります。

■ アルゴリズム移行の考え方

前項で解説した評価結果を用いることで、アルゴリズムと鍵長等の条件を決めれば、 n ビット安全性を知ることができます。では、 n ビット安全性の「 n 」としてどの程度の値を持つべきなのでしょう。ここでは、各国の考え方と移行スケジュールを紹介します。

まず、米国政府の移行スケジュールを紹介します。先に紹介したNISTによるSP800-57のTable 4では、推奨されるアルゴリズムと鍵長の組み合わせがいくつか示されています。2007年に公開されたこの表によると、2010年末までに80ビット安全性を持つアルゴリズムから、112ビット安全性を持つアルゴリズムに移行することが分かります。具体的にはRSA-1024やSHA-1の利用を中止し、2011年からはRSA-2048やSHA-2ファミリー^{*54}へ全面移行するスケジュールが示されました。さらに、2030年末までには、最低128ビット安全性を確保することが推奨されていて、Triple DESの利用を中止し、AESへ完全移行する予定です。

2010年前半まではこのスケジュールに基づいて準備が進められてきましたが、2010年6月にNISTは新しいSP800-131のドラフトを発行しました^{*55}。このドラフトでは2007年に策定されたSP800-57 に比べ、移行に

関するスケジュールがより明確になっています。2010年末に完全移行するのではなく、3年(2-key Triple DESのみ5年)の猶予期間が設けられ、2013年までは“Deprecated”という状態での利用が可能になる見込みです。この状態は利用者がリスクを許容する時のみ使用可能であることを示しています。

次に、欧州各国での動きを紹介します。2003年にNESSIE^{*56}プロジェクトによって、推奨暗号アルゴリズムリスト^{*57}が制定されています。ここでは、鍵長における注意が楕円曲線暗号のみ言及されていますが、時間的な制約等については触れられていません。

ドイツのBSI (Bundesamt für Sicherheit in der Informationstechnik、Federal Office for Information Security)による移行方針^{*58}では、ハッシュ関数の移行は次のようなものになっています。理論値として80ビット安全性を持つSHA-1及びRIPEMD-160は2010年で利用を推奨されなくなり、2015年までの(証明書検証のためだけの利用に制限する)猶予期間を設けた後、2016年からは理論値として128ビット安全性を持つSHA-256以降のSHA-2ファミリの推奨に切り替わります。また、RSAについては、2010年までは1728ビット、2011年以降は1976ビット以上の鍵長が推奨されます。

フランスのFNISA (French Network and Information Security Agency)による移行方針^{*59}では、2010年から2020年までは共通鍵暗号、ハッシュ関数は100ビット安全性を持つアルゴリズム、またRSA-2048が利用可能であり、2020年以降は128ビット安全性を持つアルゴリズム及びRSA-4096へ移行することが推奨されています。

*54 SHA-224/256/384/512をまとめてSHA-2ファミリーと呼ぶ。アルゴリズム名に付随の数値はそれぞれダイジェストの出力ビット長を意味している。現在、さらに次世代のハッシュ関数であるSHA-3のコンペティションをNISTが開催している。NIST、Cryptographic Hash Algorithm Competition (<http://csrc.nist.gov/groups/ST/hash/sha-3/>)。現在Round2のフェーズに14種類のアルゴリズムが候補として残っており、2012年2Qを目処に決定される見込みである。

*55 Second Draft Special Publication 800-131, Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths (http://csrc.nist.gov/publications/drafts/800-131/draft-sp800-131_spd-june2010.pdf)。本稿の執筆時点では、2回目のパブリックコメントが終了したところであり、このドラフトに記載されているスケジュールどおりに移行しない可能性もある点に注意。

*56 New European Schemes for Signatures, Integrity and Encryption。EU (<http://cordis.europa.eu/ist/>)のファンドで2000年から2003年まで行われていた暗号アルゴリズムの評価プロジェクト。

*57 NESSIE, Portfolio of recommended cryptographic primitives(<https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf>)。

*58 Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen Veröffentlicht am 04. Februar 2010 im Bundesanzeiger Nr. 19, Seite 426 (<http://www.bundesnetzagentur.de/cae/servlet/contentblob/148572/publicationFile/3994/2010AlgoKatpdf.pdf>)。

*59 Mécanismes cryptographiques. Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques (http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf)。

日本では、2003年2月にCRYPTREC*60による電子政府推奨暗号リスト*61が発表されました。このリストの付随情報として、共通鍵暗号やハッシュ関数としては128ビット安全性を持つアルゴリズムが推奨されています。公開鍵暗号の推奨鍵長については、2つのガイドブック*62*63に記載されていますが、移行スケジュールについては記載されていません。

また、現在日本国内では、内閣官房情報セキュリティセンター（NISC）が政府機関の情報システムで使用する暗号アルゴリズムに関する各省庁間の取りまとめを行っています。SHA-1（積極的に推奨してはしないものの2002年度版電子政府推奨暗号リストに掲載されている）とRSA1024の移行に関する指針*64が、情報セキュリティ政策会議第17回会合（2008年4月22日）で承認され、同第20回会合（2009年2月3日）で検討状況が公表されました*65。政府機関の情報システムで使用する暗号アルゴリズムとして、2014年度にSHA-256及びRSA-2048の利用が始まり、3年間の猶予期間を経て2017年度にSHA-1及びRSA-1024の利用が中止される見込みです。3年の猶予期間は、公開鍵証明書の有効期限に依

存するため、5年になるとも考えられます。

米国やフランスでは2段階（100から112ビット安全性を確保する中期的計画と128ビット安全性と確保する長期的計画）の移行が行われていますが、現在日本で立案されている計画は、前者の範囲であり、128ビット安全性確保等、より高度な安全性確保に向けた計画は今後立案されるものと考えられます。

ここで、過去の代表的な暗号アルゴリズムの危殆化状況と、以上の各国の動きをまとめて図-9に示します。

■ 暗号アルゴリズムの2010年問題の影響と対策

NISTの方針に端を発した暗号アルゴリズムの2010年問題では、当初2010年末までに完全移行されようと考えられていました。しかし、現状ではNISTのSP800-131のドラフトで示されるように、2010年末までに突発的な移行問題が発生しないことが明らかになってきています。一方で、公開鍵認証基盤をビジネスとする認証機関を中心に早めの対策が進められ、今年に入ってから各PKIベンダから2010年問題に対処するとのアナウン

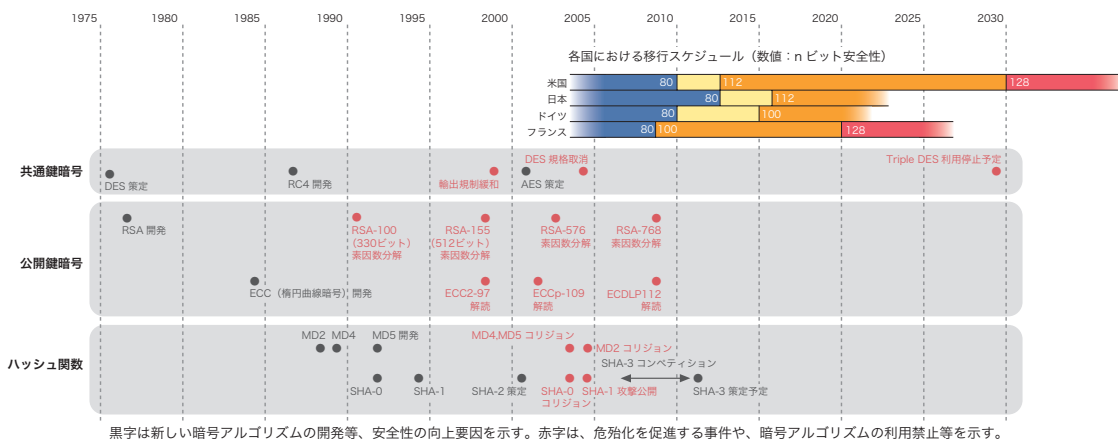


図-9 暗号アルゴリズム移行スケジュール

*60 CRYPTREC: Cryptography Research and Evaluation Committees (<http://www.cryptrec.go.jp/>)。電子政府推奨暗号の安全性を評価・監視し暗号モジュール評価基準等の策定を検討するプロジェクト。総務省及び経済産業省が共同で運営を行っている。
 *61 電子政府推奨暗号リスト (<http://www.cryptrec.go.jp/list.html>)。
 *62 CRYPTREC、電子政府推奨暗号の利用方法に関するガイドブック (http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf)。
 *63 CRYPTREC、2008年度版リストガイド(電子署名) (http://www.cryptrec.go.jp/report/c08_listguide2008_signature_v7.pdf)。
 *64 政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針 (http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf)。
 *65 「政府機関の情報システムにおいて使用している暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」に基づく検討状況について (<http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0502.pdf>)。

スが行われています*66*67。特にEV証明書*68は、危殆化を考慮した発行ガイドラインがCA/Browser Forum*69によって策定され、有効期限が2011年以降になる公開鍵証明書ではRSA-1024が利用できず、RSA-2048に制限されます。また、ハッシュ関数は、SHA-256以降のアルゴリズムが推奨され、SHA-2ファミリがほとんどのWebブラウザに搭載されるまでの期間のみSHA-1の利用が認められています(正確な期間は明確化されていません)。

暗号アルゴリズムの2010年問題の影響は、PKIや公開鍵証明書以外にも及んでいます。SSL/TLS、S/MIME、DNSSEC等のプロトコルに関しては、NISTによって詳細な設定情報の推奨値が示されています*70。また、タイムスタンプや長期保存署名といったタイムビジネスにおいても、SHA-2及びRSA-2048への移行を目指した検討が行われています*71。

暗号アルゴリズムの2010年問題への対応を考えてみましょう。暗号アルゴリズムはそれぞれで互換性がないため、アルゴリズム自体を交換することで移行を実施する必要があります。移行は、次の2つのフェーズに分けることができます。1つ目は、Webブラウザやソフトウェア等をアップデートすることで新しい暗号アルゴリズムを搭載する段階です。しかし、Internet Explorerバージョン6の利用中止の取り組み*72等が示すように、一般的にエンドユーザに対して更新を強要することは困難です。特にPCよりも携帯電話やゲーム機器での移行が難しいとの指摘もあります*73。

2つ目のフェーズは、危殆化したアルゴリズムを捨てるという段階です。NISTの“Deprecated”という考え方に見られるように、利用者が安全性の低い暗号アルゴリズムを使用するときには、そのリスクを理解した上で利用する必要があるでしょう。このリスクの例として、バージョンの古いWebブラウザで、利用者の設定によって危殆化したアルゴリズムを使った接続が行われるケースがあることが報告されています*74。また、携帯端末等においては、RSA-2048が利用できない端末もあり、コスト負担や機会損失を恐れてサーバ側で安全性の低い証明書の排除が躊躇されることも考えられます。

■ まとめ

これまで示してきたように、暗号アルゴリズムは時間の経過とともに危殆化し、その安全性が低下していきます。これは今回紹介した2010年問題に限らず、過去にも(例えば56bitDES等で)起こってきたことであり、また今後も継続的に発生するものです。したがって、暗号アルゴリズムとその実装を利用するときには、利用する時点で安全性が十分に確保されているものであることを見極めて利用する必要があります。

日本国内においては、現在CRYPTRECにより、電子政府推奨暗号リストの改訂が検討されています*75。これは、現行の2002年度版リスト*76の改訂であり、政府調達等に影響します。次の2013年度版リストに、鍵長に関する制約が記載されるのか、次に発表されるであろうNISCの移行指針との整合性があるか等、今後の動向に注意を払っていく必要があります。

*66 ベリサイン サーバIDおよびコードサイニング証明書製品における公開鍵長などの仕様変更について(統報) (<https://www.verisign.co.jp/ssl/about/20100128b.html>)。

*67 セコムトラストシステムズ、暗号アルゴリズムの2010年問題に伴うセコムパスポートforWeb SR2.0(RSA鍵長)に関する重要なお知らせ (<http://www.secomtrust.net/service/ninsyo/algorithm2010.html>)。

*68 EV SSL証明書:Extended Validation SSL Certificate。ブラウザでSSL/TLSサイトを閲覧した際にURL入力欄がグリーンになるような仕掛けがなされており、これまでのSSLサーバ証明書の発行基準よりも厳しい審査が行われるためより安全なサイトとしてユーザに認識されることが想定されている。

*69 CA/Browser Forum(<http://www.cabforum.org/>)、Guidelines For The Issuance And Management Of Extended Validation Certificates (http://www.cabforum.org/Guidelines_v1_2.pdf)。Appendix A "Minimum Cryptographic Algorithm and Key Sizes"に2010年を境にした推奨アルゴリズム、鍵長が記載されている。

*70 NIST Special Publication 800-57 Recommendation for Key Management - Part 3: Application-Specific Key Management Guidance(http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf)

*71 タイムビジネス認定センター、デジタル署名を利用するTSA及びTA業務に対する暗号アルゴリズム移行への検討開始のお知らせ (<http://www.dekyo.or.jp/tb/data/100708.pdf>)。

*72 内閣官房情報セキュリティセンター、旧型ブラウザから新型ブラウザへの移行に係る取組について (http://www.nisc.go.jp/press/pdf/browser_transition_press.pdf)。

*73 松本、宇根、SSL証明書における暗号アルゴリズム移行の現状と今後の対応、日本銀行金融研究所ディスカッション・ペーパー 2010-J-11 (<http://www.imes.boj.or.jp/japanese/jdps/2010/10-J-11.pdf>)。

*74 神田、TLS/SSLの暗号利用に関する現状と課題、Internet Week 2009 (<http://www.nic.ad.jp/ja/materials/iw/2009/proceedings/h9/iw2009-h9-04.pdf>)。

*75 電子政府推奨暗号リスト改訂のための暗号技術公募(2009年度)の書類受付開始 (http://www.cryptrec.go.jp/topics/cryptrec_20091001_application_open.html)。

*76 各府省の情報システム調達における暗号の利用方針、平成15年2月28日 (http://cryptrec.go.jp/images/cryptrec_02.pdf)。

1.4.2 DDoS攻撃によるbackscatterの観測

インターネットに接続しているホストには、本来到着するはずのない不要なパケットが到着することがあります。これらのうち通信開始を試みるパケットは、マルウェアや攻撃ツール等が適当な攻撃先を探すために送信してきたパケットだと考えられ、その現状はこれまでも本レポートの「1.3.2 マルウェアの活動」に無作為通信の状況として示してきました。しかし、観測される不要パケットには、通信開始を試みるものだけでなく、プロトコル仕様上は応答に分類されるべきパケットが突発的に到着することもしばしば見られます。こうした唐突に到着する応答パケットは、インターネット上のどこかのホストがDDoS攻撃を受けて副次的に発生した「backscatterパケット」の可能性があり、ここでは、backscatterパケット発生の仕組みと、DDoS攻撃観測への応用について解説します。

■ backscatter発生の仕組み

「1.3.1 DDoS攻撃」でも示しているように、一般的なDDoS攻撃では対象のホストに向けて多量のパケットが送りつけられます。攻撃対象となったホストは、

TCP/IPの仕様に基づいて、受信したパケットに応じた応答パケットを送り返します(表-3)。このとき、元となる攻撃パケットが発信元IPアドレスをランダムに詐称(IPスプーフィング)していると、応答パケットは本来の発信元ではなく、詐称されたIPアドレスに向けて送り返されることとなります。これがDDoS攻撃に伴って発生する、backscatterと呼ばれる現象です。backscatterパケット発生の様子を図-10に示します。

このbackscatter発生の現象を利用して、インターネット上でのDDoS攻撃を間接的に推定する、「backscatter解析」と呼ばれる技術があります^{*77}。観測ホストをインターネットに接続し、到着したbackscatterパケットを得た時、その発信元IPアドレスはDDoS攻撃を受けていると推測されるサーバのIPアドレスになります。この手法による観測報告は、これまでも数多く公開されています^{*78}。また、いくつかの仮定の元で確率論的計算を行うことで、backscatterパケットの到着頻度から元の攻撃トラフィックの規模(単位時間あたりのパケット数等)を見積もる試みも行われています。

表-3 主要な受信パケットとTCP/IPの仕様で定められた応答

受信パケット	応答パケット
TCP SYN	TCP SYN/ACK (サービスしているポートの場合)
TCP SYN	TCP RST (サービスしていないポートの場合)
TCP DATA	TCP RST
TCP RST	応答なし
ICMP Echo Request	ICMP Echo Reply
UDP	上位プロトコルに依存 (サービスしているポートの場合)
UDP	ICMP Port Unreachable (サービスしていないポートの場合)

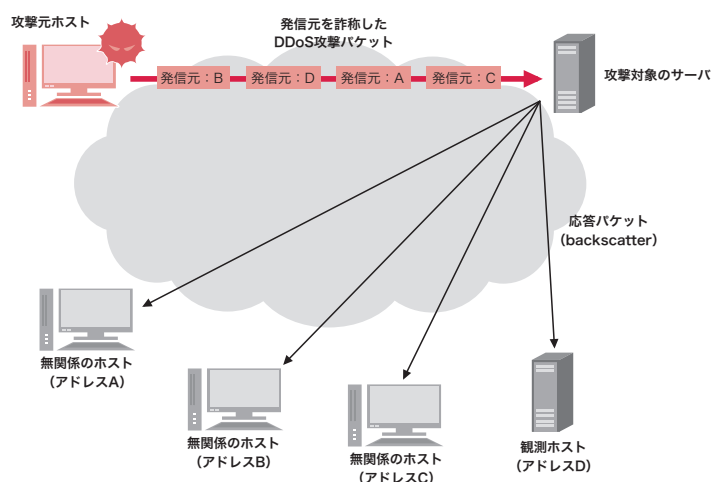


図-10 DDoS backscatterの発生

*77 古くは2001年開催のUSENIX Security Symposiumで発表された次の研究がある。David Moore, Geoffrey M. Voelker, Stefan Savage, "Inferring Internet Denial-of-Service Activity" (<http://www.usenix.org/events/sec01/moore.html>)。

*78 例えば、警察庁が公開している情報技術解析の年報にはbackscatter解析による分析報告がある。情報技術解析平成21年報(http://www.npa.go.jp/cyberpolice/detect/pdf/H21_nempo.pdf)、および別冊資料(http://www.npa.go.jp/cyberpolice/detect/pdf/H21_betsu.pdf)。

■ MITFでのbackscatter観測

IJが実施しているMITFのハニーポットでも、backscatterと考えられるパケットが観測されています。ここでは2010年7月の観測結果を紹介します。

この1ヶ月間に観測されたbackscatterのパケット数について、発信元アドレスの国別分類による推移を図-11に、全期間での国別分布を図-12に、発信元ポートで分類した場合の推移を図-13に、全期間でのポート別分布を図-14にそれぞれ示します。全期間を通じた1日あたりの平均では4,611パケットが検出されました。

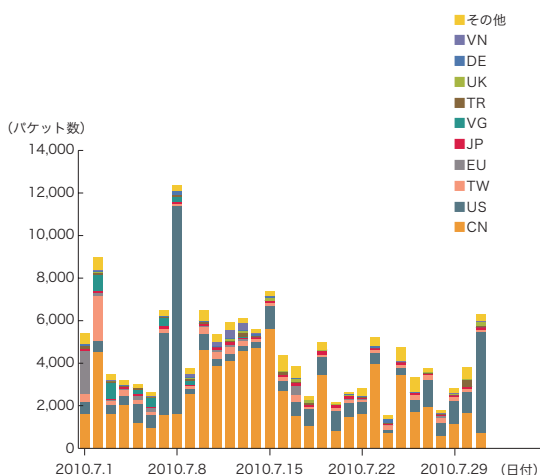


図-11 発信元の国別分類によるbackscatterパケット数の推移

国別分類では中国の51.8%、米国の24.9%が大きな割合を占めており、これらの国々のホストがIJのIPアドレスを詐称した攻撃を多く受けていることがわかります。ただし、攻撃パケットのIPアドレス詐称が完全にランダムなものではない可能性もあり、このデータだけからでは単純に攻撃量の大小は比較できないことに注意してください。また、ポート別分類ではWebサービスで利用される80/TCPが57.6%を占め、数多く観測されました。80/TCP以外には、FTPが利用する21/TCPのように良く知られたポートも散見されますが、オンラインゲームで利用されるポートや、用途不明のポートも検出されています。これらのポートからのbackscatterパケットは、そのほとんどが中国を発信元としています。

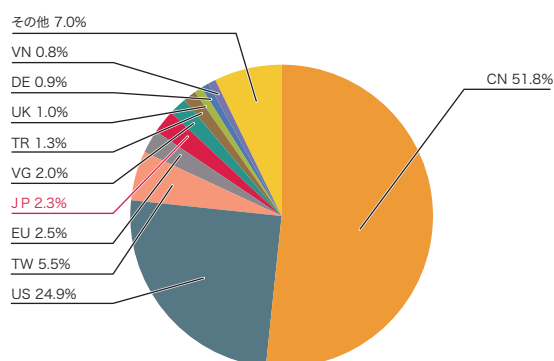


図-12 全期間での国別分布

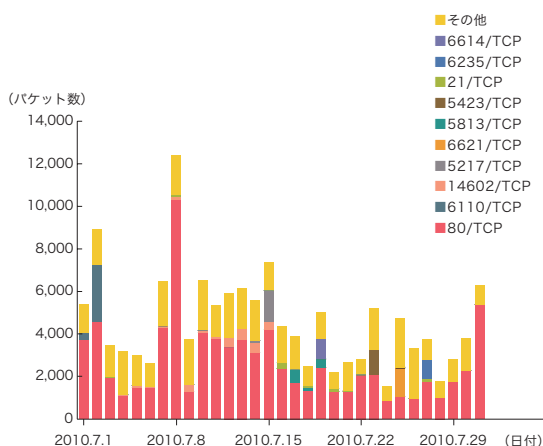


図-13 発信元ポート別分類によるbackscatterパケット数の推移

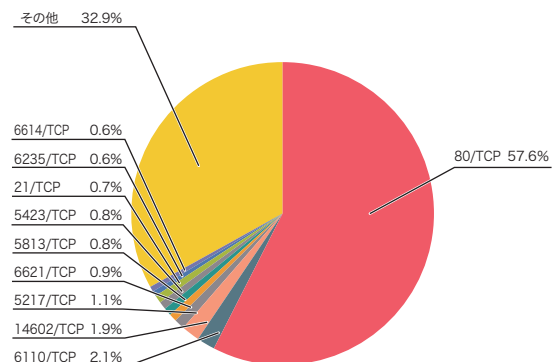


図-14 全期間でのポート別分布

次に、Webサービスの80/TCPを発信元ポートに持つbackscatterパケットを抽出し、件数の多い発信元アドレスについて分析した図を示します(図-15)。特に多数のbackscatterパケットが観測された事例としては、7日から8日にかけて、米国のWebホスティング事業者のIPアドレスから合計12,901パケットが観測されました。このIPアドレスでは複数のWebサイトがホスティングされていますが、いずれも中国語のコンテンツを配信するサイトであることが確認されています。つまり、IPアドレスは米国であっても、中国企業が攻撃対象になっていたものと考えられます。10日から16日にかけては、中国のIPアドレスから合計13,408パケットが観測されました。

この他にも、7月1日にはカナダ企業のIPアドレスから、翌2日には台湾のIPアドレスから、また2日から6日にかけて英領バージン諸島のIPアドレスからbackscatterパケットが観測されています。16日から23日にかけては先述とは別の米国Webホスティング事業者のIPアドレスからのbackscatterパケットが観測されました。このアドレスも複数企業のWebサイトをホスティングしており、そのほとんどがトルコ語のコンテンツを持つサイトでした。

このようにWebサービスに関しては、様々な国々の、主に企業のサイトが攻撃対象になっていることが観測されています。

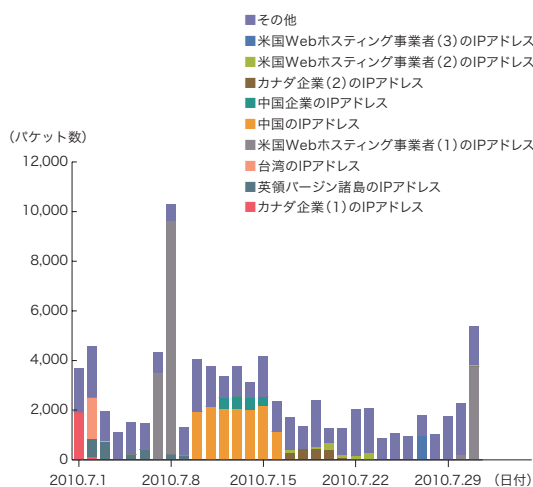


図-15 ポート80/TCPからのbackscatterパケット

■ backscatter観測の限界と位置づけ

以上に示したようにbackscatter解析は、DDoS攻撃の観測に応用できます。しかし、この手法で検知できるものは、DDoS攻撃の中でも一部の種類に限られます(図-16)。例えば、HTTP GET FloodのようなIPアドレスを詐称しない(しにくい)攻撃ではbackscatterは発生しません。また、TCP RST等の応答が必要ないパケットを使った攻撃でもbackscatterは発生しません。攻撃対象となっているサーバが高負荷な状態であったり、設定によって応答パケットをほとんど返さなかったりすることも考えられます。

また、backscatterパケットを観測しても、攻撃の対策に必要な詳細情報を得ることはできません。例えば、backscatterはIPアドレスが詐称された結果として発生するため、本来の攻撃元を知ることはできません。さらに、ごく限られたケースを除いて、攻撃の通信量(総帯域等)を推測することもできません。

backscatterから間接的にDDoS攻撃を観測する手法にはこうした限界があり、直接観測を代替するものではありません。しかし、外部のネットワークで発生したDDoS攻撃を、それに介在することなく、第三者として検知したり観測したりできるメリットがあり、直接観測等の情報を補完することができます。このように、DDoS攻撃に関する情報を多く集めることで、日本国内で発生するDDoS攻撃の検出や対策に役立てることができると考えています。

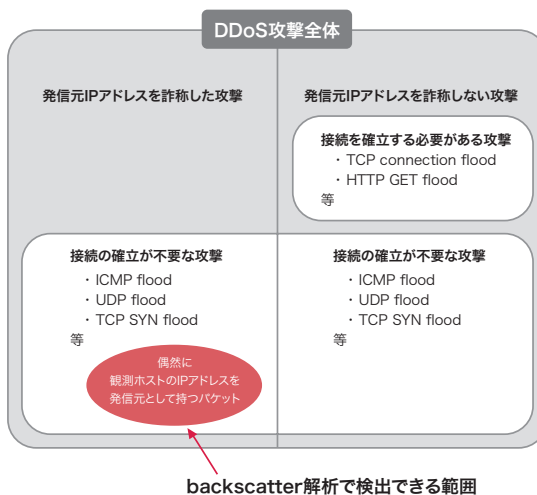


図-16 backscatter解析で検出できるDDoS攻撃の範囲

1.4.3 脆弱性情報の流通動向

インターネットに接続する、すべてのソフトウェアやハードウェアには、何らかの形で脆弱性が存在しています。悪用されるとセキュリティ上の脅威となる脆弱性には、プログラムのバグ等の実装上の問題だけでなく、インターネットの利用方法の変化に伴って発生する処理能力の限界等、外的要因の状況によって発現するものも考えられます。システムを運用する立場では、脆弱性を早期に把握し適切に対処することが、システムのセキュリティを維持する上で重要な作業になります。しかし、脆弱性に関する情報は、広く周知する^{*79}必要がある反面、その情報自体が悪用される可能性を持つため、取り扱いには十分に注意する必要もあります。ここでは、脆弱性の発見からベンダへの通知、対策の作成、公開までの流れを円滑に実現するための活動と、利用者が脆弱性情報の重要度を評価するための基準について紹介します。

■ JVNと情報セキュリティ早期警戒パートナーシップ

脆弱性対策を行う立場から参考になる情報として、脆弱性に関する情報を集約し開示する試みである Vulnerability Notes Database (US-CERT VN)^{*80} や、脆弱性を示す固有の番号で辞書的に利用できる Common Vulnerabilities and Exposures (CVE)^{*81} 等があります。ただし、これらは、すべて英語による情報であり、また、日本国内の製品に関する情報が少ないという問題がありました。

日本語ワードプロセッサやパーソナルルータ等、日本国内で利用される製品に関する脆弱性とその修正情報を集約し、より多くの国内の利用者に参照してもらう

ためには日本語で情報発信を行う必要があります。このために、2003年2月にJPCERT/CCのプロジェクト Japan Vulnerability Notes (JVN)^{*82}が公開されました。

続いて、2004年4月のIPAにおける研究会^{*83}での検討結果等を受け、2004年7月には経済産業省告示二百三十五号^{*84}に基づき、製品開発者に対する脆弱性情報の流通体制である、情報セキュリティ早期警戒パートナーシップ^{*85}が構築されました。

このパートナーシップでは、経済産業省告示二百三十六号によりIPAを脆弱性情報の受付機関、JPCERT/CCを製品開発者との間の調整機関に指定しています。この2つの組織が連携し、脆弱性情報に対して、報告者の保護や製品開発者間での公開日の調整等を行いながら、最終的に製品ごとに対策情報を取りまとめて公開するまでの処理が実施されます。現在JVNは、このパートナーシップにおいて、製品開発者が公開する情報を集約する場としての役割を担い、JPCERT/CCとIPAによって共同運用されています。また、2007年4月には、このパートナーシップで取り扱う脆弱性情報に加えて、一般の脆弱性情報や脆弱性に対する脅威評価、対策の情報をまとめたJVN iPedia^{*86}も公開されました。

これらの活動は、日本国内における製品の脆弱性情報の流通を実現させたことだけではなく、国や公的機関が主導的な役割を發揮した脆弱性対策の先進的な事例であることや、日本固有の情報を英語に翻訳して発信し、日本の状況を広く世界に伝えている点が国際的に高く評価されています。

*79 公開の場で脆弱性情報の共有や議論を行う場としては、例えばbugtraq (<http://www.securityfocus.com/archive/1>) や、full-disclosure (<http://lists.grok.org.uk/full-disclosure-charter.html>) 等がある。

*80 CERT/CCのVulnerability Notes Database。後にUS-CERT Vulnerability Notes Database (<http://www.kb.cert.org/vuls/>) となった。IJJもルータ製品SEIL (<http://www.seil.jp/>) に関する情報提供を行っている。

*81 Common Vulnerabilities and Exposures (CVE (<http://cve.mitre.org/>))。特定の脆弱性に対し脆弱性の一意性を示すCVE-IDを付与することで、類似の脆弱性との違いを示す。CVEは米国MITRE社が運営しているが、CVE番号の採番組織CNA(CVE Numbering Authority)は複数あり、日本では2010年6月にJPCERT/CCがCNAとして認定された (http://www.jpCERT.or.jp/press/2010/PR20100624_cna.pdf)。

*82 Japan Vulnerability Notes (<http://jvn.jp/>)。当初はJPCERT/CCのプロジェクトとして公開されたが、現在はJPCERT/CCとIPAの共同運営となっている。

*83 IPA「情報システム等の脆弱性情報の取り扱いに関する研究会」報告書 (<http://www.ipa.go.jp/about/press/20040406.html>)。

*84 ソフトウェア等脆弱性関連情報取り扱い基準 (平成16年経済産業省告示第235号) (http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm)。

*85 経済産業省、「情報セキュリティ早期警戒パートナーシップ」の運用開始について (http://www.meti.go.jp/policy/it_policy/press/0005399/) (<http://www.ipa.go.jp/security/vuln/report/>) (<http://www.jpCERT.or.jp/vh/>)。IJJは、このパートナーシップの運用開始時より、製品開発者として参加している。

*86 JVN iPedia (<http://jvn.db.jvn.jp/>)。

今日利用できるその他の脆弱性情報には、米国標準技術研究所 (NIST) による米国政府向けの標準脆弱性データベースNVD^{*87}、非営利団体であるOpen Security Foundation を中心としたセキュリティコミュニティによって維持されているOSVDB^{*88}や、セキュリティ専門企業によるデータベース^{*89}等があります。

■ 脆弱性情報の評価

現在では、ソフトウェアや製品のベンダにより、脆弱性対策パッチやファームウェアを自動的に配布する試みを実施されています。しかし、このようなパッチやファームウェアには、脆弱性の修正だけではなく、機能の追加等と同梱されていることもあり、脆弱性だけを修正するつもりで適用しても、設定インターフェースや従来の機能に変更が加えられたりすることがあります。また、日本の多くの企業で見られるような独自の作り込みが行われたアプリケーションを利用しているときには、動作検証を行う作業と、そのための時間が必要になります。さらに、パッチの適用時に再起動を要する場合には、継続運用が要求されるシステムにおいては修正のタイミングを調整する必要もあります。

そこで、脆弱性情報を受け取る立場でも脆弱性に関する情報の詳細を検討し、脆弱性の対策となるパッチを導入するかどうかや、そのタイミングを決定する必要があります。このためには、脆弱性の攻撃の容易さや、脆弱性の影響の深刻さ、システムへ影響の度合い等を考慮した脅威評価を行う必要があります。ベンダから脆弱性の脅威の情報を提供し、利用者の環境に合わせた判断を補助するための指標として利用できるのがCVSS (Common Vulnerability Scoring System)^{*90}です。

CVSSでは、脆弱性の脅威評価基準を、基本評価基準、現状評価基準、環境評価基準の3つに分類しています。

基本評価基準では、その脆弱性の悪用のしやすさに関する情報と、悪用されたときのセキュリティのCIA (Confidentiality, Integrity, Availability) への影響を評価します。現状評価基準では、現時点でその脆弱性の悪用されやすさの基準として、攻撃コードの存在の有無、パッチなどの対策の有無、脆弱性情報の信憑性について表現します。最後の環境評価基準では、利用環境のなかで、この脆弱性を攻撃されたときに二次被害が発生する可能性があるかどうか、その脆弱性を持つシステムがどの程度の数存在するかどうか、対象システムのCIAに対するセキュリティ要求度合いについて評価します。

多くの場合、基本評価基準と現状評価基準は、製品ベンダやセキュリティベンダから提供されますが、環境評価基準には利用者が自分の環境にあわせて設定する項目があります。それぞれの評価項目について評価した段階で、最終的にある計算式で脅威評価を行います^{*91}。この評価は、対策パッチのリリースや、脆弱性を悪用するコードの出現等の状況の変化に応じて、何度でも再計算することができ、利用者が現時点での脅威を適切に知ることができるようになっています。

利用者が脅威評価の参考にしてできる基準としては、CVSSの他にも、JVNに掲載された情報に対するJPCERT/CCによる独自評価^{*92}等があります。また、マイクロソフト社のマイクロソフト悪用可能性指標 (Microsoft Exploitability Index)^{*93}は、悪用事例やそ

*87 National Vulnerability Database (<http://nvd.nist.gov/>)。

*88 The Open Source Vulnerability Database (<http://osvdb.org/>)。

*89 例えば米国のIBM ISSのThreat List (<http://www.iss.net/threats/ThreatList.php>) や、デンマークのSecunia (<http://secunia.com/>) 等。フランスのVUPEN security (<http://www.vupen.com/english/>) のように非公開脆弱性情報を顧客に提供するサービスもある。

*90 CVSSはFIRSTのCVSS-SIG (<http://www.first.org/cvss/>) で策定され運用が行われている。現在利用されているCVSS2.0の各評価項目に設定される値については次の資料を参照のこと。A Complete Guide to the Common Vulnerability Scoring System Version 2.0 (<http://www.first.org/cvss/cvss-guide.html>)。日本語での情報はIPAの次の文章に詳しい。共通脆弱性評価システムCVSS (<http://www.ipa.go.jp/security/vuln/CVSS.html>)。ただし、この文章では各項目の設定値も日本語にしているので、実際にCVSSの評価を行うときにはFIRSTのガイドとともに参考にした方がよい。

*91 CVSSの計算を自動化する仕組みとしては、例えばIPAによるCVSS 計算機 (<http://jvndb.jvn.jp/cvss/ja.html>)がある。

*92 JPCERT/CCでは、脆弱性情報の脅威をその悪用の状況に応じて、攻撃経路、認証レベル、攻撃成立に必要なユーザの関与、攻撃の難易度にかけて独自の評価を与えている (<http://jvn.jp/nav/jvnhelp.html>)。

*93 マイクロソフト悪用可能性指標では、対象とする脆弱性の悪用について、実証コードや悪用コードの有無実際の悪用事例等をもとにした、3段階の評価を提供している (安定した悪用コードの可能性、不安定な悪用コードの可能性、機能する見込みのない悪用コード)。悪用可能性指標の詳細については次の説明を参照のこと (<http://www.microsoft.com/japan/technet/security/bulletin/cc998259.mspx>)。

の流行状況等を加味した値となっています。さらに、SANS ISC のISC rating^{*94}のように、パッチの内訳や利用の方法に基づいた情報も提供されるようになってきました。

■ まとめ

ここでは、脆弱性情報を円滑に流通させるための日本の活動と、利用者がその情報を評価するために有用な基準について紹介しました。

脆弱性情報の取り扱いについては、脆弱性情報に対価を払って購入しようとする動き^{*95}や、脆弱性対策情報の流通や、対策そのものの自動化を推進するSCAP^{*96}導入の動き等があり、利用者の立場での脆弱性情報の取り扱いに、今後大きく影響する可能性があります。これらの関連する動きについては、また次の機会にご紹介したいと思います。

1.5 おわりに

このレポートは、IJJ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。今回は特定の事件に関するものではなく、インシデント対応に必要な準備として、暗号アルゴリズムの2010年問題に対する各国の状況、DDoS攻撃の観測手法としてのbackscatter解析と、最後に脆弱性情報の流通動向についてまとめました。

IJJ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続けてまいります。

執筆者:

齋藤 衛(さいとう まもる)

IJJ 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後、2001年よりIJJグループの緊急対応チームIJJ-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。IJJ-SECTの活動は、国内外の関係組織との連携活動を評価され、平成21年度情報化月間記念式典にて、「経済産業省商務情報政策局長表彰(情報セキュリティ促進部門)」を受賞した。

土屋 博英 (1.2 インシデントサマリ)

土屋 博英 鈴木 博志 (1.3 インシデントサーベイ)

須賀 祐治 (1.4.1 暗号アルゴリズムの2010年問題)

永尾 禎啓 (1.4.2 DDoS攻撃による backscatterの観測)

齋藤 衛 (1.4.3 脆弱性情報の流通動向)

IJJ サービス本部 セキュリティ情報統括室

協力:

加藤 雅彦 吉川 弘晃 鈴木 博志 IJJ サービス本部 セキュリティ情報統括室

*94 ISC ratingでは、マイクロソフト社のパッチに対して、特定のパッチに含まれる修正の一覧や、対応するKBやexploitの有無、悪用可能性指標を整理するとともに、利用形態がクライアントかサーバによって攻撃の可能性を評価し、Less Urgent, Important, Critical, PATCH NOW の4段階の独自の評価を提供している。例えば、2010年6月の定例パッチについては(<http://isc.sans.edu/diary.html?storyid=8929>)、2010年7月の定例パッチについては(<http://isc.sans.edu/diary.html?storyid=9166>)を参照のこと。

*95 GoogleのOpenSource Project The Chromium Projectでは、脆弱性情報の提供者に \$500を支払うとしている(<http://blog.chromium.org/2010/01/encouraging-more-chromium-security.html>)。またHP TippingPoint社の主催する Zero Day Initiative では、脆弱性情報提供者に報償を与えるとしている(<http://www.zerodayinitiative.com/about/benefits/>)。

*96 Security Content Automation Protocol。米国国立標準技術研究所(NIST)によって定められた、米国政府内関係組織でセキュリティ対策の標準化と自動化を行うための情報交換フォーマットとプロトコル群。本稿で紹介したCVEやCVSSはその構成要素となっている。また、IPAの提供するJVN iPediaでは、SCAPの構成要素を利用し、日本国内におけるSCAPの先進的実装となっている。

欧州各国での迷惑メールの送信元割合が増加

今回は、2010年第13～25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として中国が1位でした。

また、ドイツやイギリスといった欧州各国が送信元としての割合を増しています。

2.1 はじめに

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

今回のレポートでは、2010年第13週(2010年3月29日～4月4日)から第25週(2010年6月21日～6月27日)までの13週間分のデータを対象としています。メールの流通量や迷惑メールの割合は、長期休暇などの時期的な要因で変化します。ただし、迷惑メールの割合の推移を前年同期と合わせて示すことで、時期的な要因を勘案した比較が可能になります。

今回は、迷惑メールの動向として、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、メールの技術動向では、送信ドメイン認証技術の導入状況について報告します。

2.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IJJ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。

2.2.1 迷惑メールの割合は微減したが、レベルは依然高いまま

2010年第13週から第25週までの91日間に検出した迷惑メールの割合は、平均81.3%でした。前回(2010年第1～12週)の平均が82.1%、2009年同期(第14～26週)が81.6%でしたので、いずれに対しても微減という結果になります。今回の調査期間を含めた2009年第14週からの迷惑メールの割合の推移を図-1に示します。

今回の調査期間中には5月に大型連休があり、それを含む2010年第18週(2010年5月3日～5月9日)での迷惑

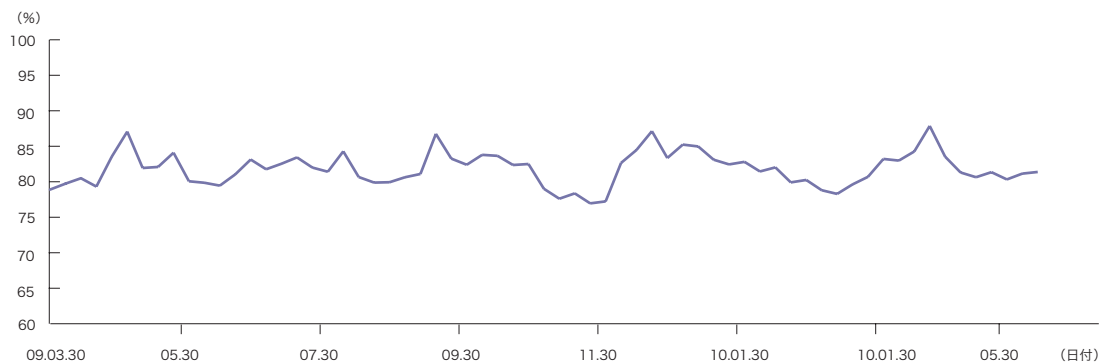


図-1 迷惑メール割合の推移

メールの割合が最も高く、87.9%という結果になりました。この87.9%という割合は、図-1の調査期間で最も高いものでした。一方、最も低い割合を示した週は、2010年第13週(2010年3月29日～4月4日)の79.6%でした。今回の調査期間での迷惑メールの割合は、平均すると微減でした。しかし、受信メール全体に占める迷惑メールの割合は、いまだに高いレベルにあります

2.2.2 迷惑メール送信元の1位は中国、欧州も増加傾向

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位は中国(CN)で、迷惑メール全体の11.1%を占めていました。前は7.6%で2位でしたので、その割合を大幅に増やし、IIR Vol.2(2008年第36週～52週)以来の1位になりました。2位は米国(US)の7.8%、3位は前回と同じくインド(IN)の6.8%でし

た。4位はドイツ(DE)で4.7%、前回の6位から順位と割合がともに上がっています。5位はブラジル(BR)で4.6%でした。こちらは、前回に引き続き割合が低下しています。6位にはイギリス(GB)で4.0%でした。

今回の調査結果の特徴として、ドイツやイギリスといった欧州の先進国が迷惑メールの送信元となる割合が高くなっています。他社の分析データ*1でも同様の結果が得られていますので、欧州各国の割合が増えてきているのは全体的な傾向と言えます。これらの地域は、以前から人口が多くインターネット接続環境も整備されている地域です。これまで上位の地域となっていなかったのは、日本と同様にいくつかの対策が実施されてきたことによるものと考えられます。それが今回の調査で上位になったのは、対策が不十分になってきたためと考えられます。また、新たな送信手法が使われ始めているのかもしれない。このため、今後も注目する必要があると必要と考えています。なお、日本の順位は、前回と同様の7位で、割合も前回と同じく3.9%でした。

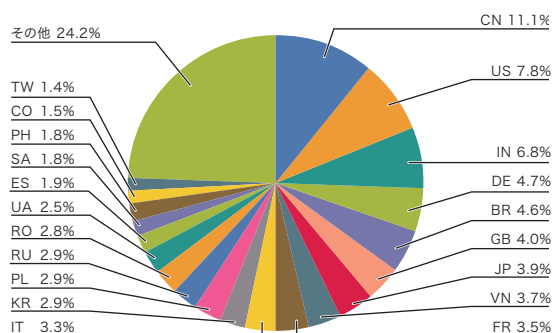


図-2 迷惑メール送信元地域の割合

図-3に、これまでの迷惑メールの主要送信元である5地域(CN, US, IN, BR, KR)の割合の推移を示します。中国(CN)は、3月以降はほぼ最も割合の高い地域となっています。ブラジル(BR)や韓国(KR)は比較的落ち着いていますが、インド(IN)がやや増加傾向にあることがわかります。

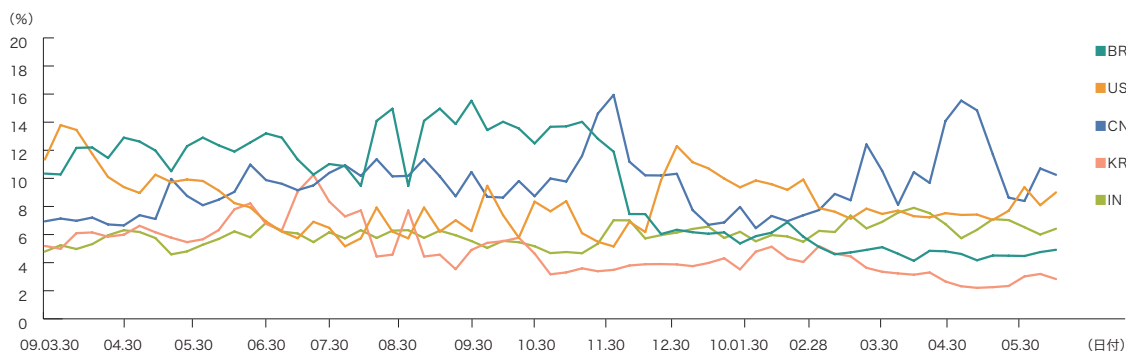


図-3 主要迷惑メール送信地域の推移

*1 The top twelve spam relaying countries for April - June 2010 (<http://www.sophos.com/pressoffice/news/articles/2010/07/dirty-dozen.html>)

2.3 メールの技術動向

ここでは、ネットワークベースの送信ドメイン認証技術のひとつであるSPF (Sender Policy Framework) の導入状況の調査結果を報告します。IJが提供する特定メールサービスにおいて、今回の調査期間 (2010年4月～6月) での認証結果の割合を図-4に示します。この期間に受信したメールの認証結果は、全体の54.9%が“none”でした。これは、受信メールの約45.1%のドメインでSPFレコードが宣言されていたことを表します。この結果は、前回の調査に比べて0.7%の微増となります。

また、JPドメインについても、同様に認証結果の割合を図-5に示します。全体の41.7%が“none”でしたので、受信メールの約58.2%のJPドメインでSPFレコードが宣言されていたこととなります。

WIDEプロジェクトがJPRS (Japan Registry Service Co.,Ltd.: (株)日本レジストリサービス) との共同研究契約で行っているJPドメインのSPFレコード宣言率の調査^{*2}によれば、2010年5月時点での普及率は38.8%でした。JPドメインの属性別でのSPFレコードの宣言率についても、企業などが利用するco.jpドメインは45.4%と最も高い割合となっています。これらの結果から、日本のJPドメインでのSPFレコードの宣言率は、

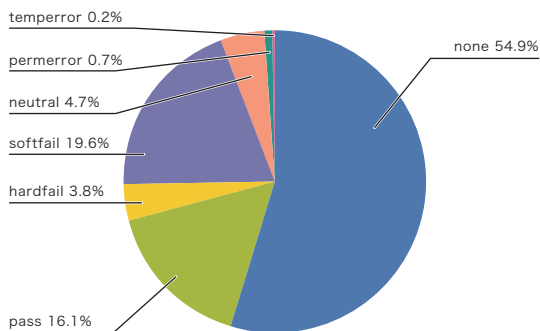


図-4 受信メールに対する SPF 認証結果の割合

かなり高いレベルにあると言えます。今後は、メール受信側での認証機能の導入が進むことにより、迷惑メールに多い詐称された送信者情報を受信側で判断できるようになることが期待できます。

2.4 おわりに

6月の下旬に、その創設時からIJも参加しているMAAWG (Messaging Anti-Abuse Working Group) の19回目の会合 (General Meeting) に出席してまいりました。今回の調査結果にも見られるとおり、世界的にも迷惑メールの割合は高いレベルで推移しており、ISPは多くの課題に直面しています。迷惑メールの送信手法が日々変化しているため、対策側であるISPが後追いつる状況が続いています。最近では、固定回線に加えて、無線LANやモバイルデータ通信などのインターネットへの新たな接続経路が利用できるようになってきています。利用する側の立場としては、インターネットによるさまざまなサービスがどこでも使える環境になり便利になりましたが、迷惑メールを送信する側にとっても、利便性が高まっていることを忘れてはいけません。IJは、これからも国内およびグローバルにさまざまな組織と連携し、迷惑メール対策を推進するために協力していく予定です。

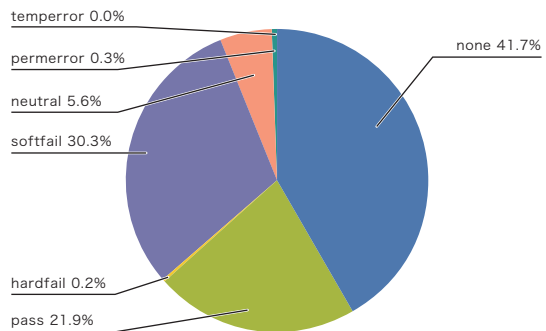


図-5 JPドメインでの認証結果の割合

執筆者:

櫻庭 秀次 (さくらば しゅうじ)

IJ 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。

*2 ドメイン認証の普及率に対する測定結果 (<http://member.wide.ad.jp/wg/antispam/stats/index.html>)

P2Pファイル共有からWebサービスへ シフト傾向にあるトラフィック

これまで年率30%程度で比較的安定して伸びてきたインターネットのトラフィック量が2010年1月初めに20%近く急減しました。その原因は、改正著作権法、いわゆるダウンロード違法化にあると言われています。ここでは、2010年5月24日から一週間のトラフィック量やポート使用量を用い、2009年のデータと比較することで、トラフィック量が減少した原因を探っていきます。

3.1 はじめに

本レポートは、IIR Vol.4でのレポート[1]の続報であり、IIJが運用するブロードバンド接続サービスでのトラフィックを分析して、その結果をまとめたものです。前回のレポートでは、過去5年間で国内外のインターネットのトラフィック量が年率30%程度の伸びを示し、比較的安定していると報告しました。ただし、トラフィック量には、一部のヘビーユーザの挙動が大きく影響したり、技術以外の社会的要因等でユーザの利用の仕方が変わったりするため、過去のデータを元に将来を予測することが難しいことも述べました。

実際2010年1月には、トラフィック量の伸びがマイナスになるという状況が生まれました。図-1に示すように、ブロードバンドトラフィック量が1月初めに2割近く減りました。これまでもトラフィック量の変動はありましたが、このような大きな減少が半年も続いたことはありませんでした。今回の減少は、2010年1月に施行された改正著作権法、いわゆるダウンロード違法化の影響だろうと言われています。しかし、罰則規定のないダウンロード違法化の施行が、ここまで影響したことは予想外でした。

本レポートでは、前回と同様に、利用者の1日のトラフィック量やポート別使用量などを元に、1年前と比べて実際に何が変わったのかを検証していきます。

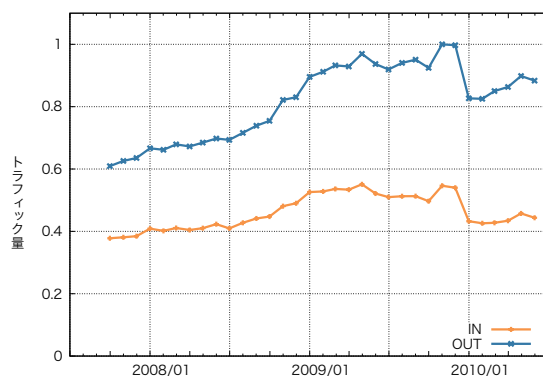


図-1 過去3年間のブロードバンドトラフィック量の推移 (2009年11月のOUT値を1として正規化)

3.2 データについて

今回利用した調査データは、前回と同様に、個人および法人向けのブロードバンド接続サービスでファイバーとDSLのブロードバンド顧客を収容しているルータから、Sampled NetFlowによって収集しました。ブロードバンドトラフィックは平日と休日での傾向が異なるため、一週間分のトラフィック量を解析の対象にしています。今回は、2010年5月24日から30日の一週間のデータを使用しました。また、比較のために、前回解析した2009年5月25日から31日の一週間のデータも用いています。

各利用者の使用量は、利用者に割り当てられているIPアドレスと、観測したIPアドレスを照合して求めました。また、Sampled NetFlowで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のいずれかを設定しています。観測し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。このようなサンプリング方法を採用したため、使用量が少ない利用者のデータには誤差が生じています。しかし、使用量がある程度以上である利用者のデータでは、統計的に意味のある数字を得ることができます。

なお、ファイバーとDSLで観測する利用者数は、2005年頃にはほぼ同数でしたが、その後ファイバーへの移行が進み、2010年に観測したユーザ数の85%がファイバー利用者で、全トラフィック量の92%を占めるまでになっていました。また、本レポート内でのトラフィックのIN/OUTは、ISP側から見た方向で表しています。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になります。

3.3 利用者の1日の使用量

まず、ブロードバンド利用者の1日の使用量をいくつかの視点から見ていきます。ここでの1日の使用量は、各利用者の1週間分のデータを7で割った1日平均です。

図-2に、利用者の1日のトラフィック量を相補累積度分布で示します。これは、1日の使用量がX軸の値より大きい利用者の割合を両対数グラフで示したもので、全体に対するヘビーユーザの分布を見るときに有効です。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わかります。また、ヘビーユーザは全体に分布していて、決して一部の特殊な利用者ではないとも言えます。

IIR Vol.4で示した2009年での相補累積分布と比較してみると、ヘビーユーザの割合がIN（アップロード）で若干減少しています。例えば、1日に 10^8 (100MB)以上をアップロードしているユーザの割合は、2009年に全体の8.2%でしたが、2010年に6.5%に減っています。これは、全体に対して1.7ポイントの減少に過ぎませんが、ヘビーユーザの数で見ると約20%も減少したことになります。一方、グラフ右端の部分では、2009年での分布よりも2010年のほうが伸びていて、極端なヘビーユーザは逆に増えていることもわかります。

図-3に、利用者間のトラフィック使用量の偏りを示します。このグラフは、使用量が上位X%である利用者によって全トラフィック量のY%が占められている事を表しています。使用量には大きな偏りがあり、結果として全体が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（ダウンロード）

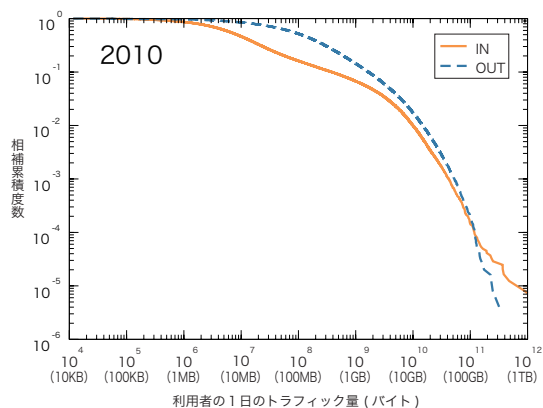


図-2 利用者の1日のトラフィック量の相補累積度分布

ド)の78%、IN(アップロード)の96%を占めています。また、上位1%の利用者がOUT(ダウンロード)の33%、IN(アップロード)の51%を占めています。

IIR Vol.4で示した2009年での使用量の偏りと比較すると、IN(アップロード)での偏りが大きくなっています。これは、ヘビーユーザの総数は減ったが、極端なヘビーユーザが増えた結果です。OUT(ダウンロード)では、ほとんど変化がありませんが、上位3%以上で若干偏りが小さくなっています。

しかし、このような偏りの傾向は、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したものです。例えば、使用量が上位である利用者を除いて再度偏りの分布を見ても、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に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量の偏りは、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が、使用量の分布がベキ乗則に従っているため、実際には多様なユーザが幅広く存在しています。

図-4に、利用者の一日の平均利用量の分布(確率密度関数)を示します。ここでは、IN(アップロード)とOUT(ダウンロード)に分け、X軸に利用者のトラフィック量、Y軸にその出現確率をそれぞれ示しています。また、X軸は対数表示で、その範囲は 10^4 (10KB)から 10^{11} (100GB)です。今回の調査では、最も使用量が多い利用者のトラフィック量は2TBにも及び、一部の

利用者がグラフの範囲外になりますが、おおむね 10^{11} (100GB)までの範囲に分布しています。なお、グラフ左側に突起が現れていますが、これはサンプリングレートの影響によるノイズです。

IN(アップロード)とOUT(ダウンロード)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、線形グラフで見ると、左端近くにピークがあり右方向になだらかに減少する、いわゆるロングテールな分布になります。OUTの分布がINの分布より右にあり、ダウンロード量がアップロード量よりも一桁ほど大きくなっています。平均値は、グラフ右側にあるヘビーユーザの利用量の影響を受け、IN(アップロード)で469MB、OUT(ダウンロード)で910MBです。2009年では、それぞれ556MBと971MBでしたので、利用量は減少しています。

IN(アップロード)の分布の右端に注目してみると、もう1つの小さな分布の山があることに気づきます。実際には、OUT(ダウンロード)にも、メインの分布に重なっていますが、同様の分布の山があります。これらの分布は、IN(アップロード)とOUT(ダウンロード)でほぼ同じ位置にあり、IN/OUTのトラフィック量が対称であるヘビーユーザの存在を示しています。そこで、ここでは便宜上、大多数を占めIN/OUTのトラフィック量が非対称な分布を「クライアント型利用者」、右側にある少数でIN/OUTのトラフィック量が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での最頻出値を2009年と2010年で比較すると、IN(アップロード)で6MBから7MBに、OUT(ダウンロード)で114MBから145MBにそ

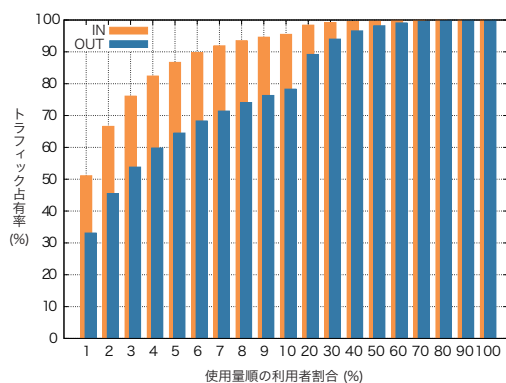


図-3 利用者間のトラフィック使用量の偏り

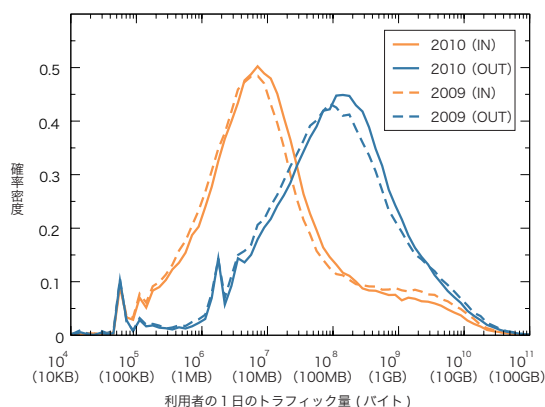


図-4 利用者の1日のトラフィック量分布

それぞれ増え、各利用者のトラフィック量が特にダウンロード側で増えていることが分かります。これに対して、ピア型利用者の出現確率は、わずかですが低下しています。つまり、一般利用者の利用量が着実に増えているのに対して、量的に大勢を占めるヘビーユーザの利用量が減ったため、それがトラフィック総量の減少に繋がったと言えます。

図-5では、ランダムに抽出した利用者5,000人のIN/OUT利用量をプロットしています。X軸にOUT(ダウンロード)、Y軸にIN(アップロード)をそれぞれ採り、両対数グラフで表しています。IN/OUTのトラフィック量が同量である利用者は、グラフの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。対角線の下側にあり、対角線に沿って広がるクラスタは、ダウンロード量がアップロード量より桁多いクライアント型利用者です。もう1つのクラスタは、右上の対角線あたりを中心に広がるピア型利用者です。しかし、この2つのクラスタの境界はあいまいです。これは、実際には、クライアント型利用者である一般ユーザもSkypeなどのピア型アプリケーションを利用しますし、ピア型利用者であるヘビーユーザもウェブ等のダウンロード型アプリケーションを利用しているためです。つまり、多くの利用者が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ます。また、各利用者の利用量やIN/OUT比率のバラツキも大きく、多様な利用形態が存在することがうかがえます。この傾向は、2009年と比較しても、ほとんど違いがありませんでした。

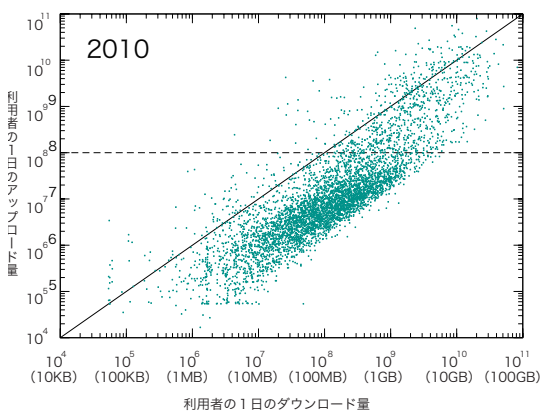


図-5 利用者ごとのIN/OUT使用量

3.4 ポート別使用量

次に、トラフィックの内訳をポートごと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は、双方で動的ポートを使うものが多く、また、クライアント・サーバー型アプリケーションの多くは、ファイアウォールを回避するために、HTTPで使われる80番ポートを利用しています。大雑把に分けると、双方が1024番以上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・サーバー型アプリケーションの可能性が高いと言えます。そこで、ここでは、TCPとUDPでソースとデスティネーションのうちポート番号の小さいほうを採り、ポート番号ごとの使用量を見ることにします。

また、トラフィックの全量がピア型利用者であるヘビーユーザのトラフィックに支配されていることから、クライアント型利用者である一般利用者の動向を知るために、少々乱暴なやり方ですが、1日のアップロード量が100MB未満のユーザを抜き出し、それらをクライアント型利用者としてしました。これは、図-4でIN(アップロード)の2つの分布の中間あたり、図-5でIN = 100MBにある水平線の下側の利用者になります。

図-6は、ポートの使用状況を、全体とクライアント型利用者に分けて2009年と2010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。

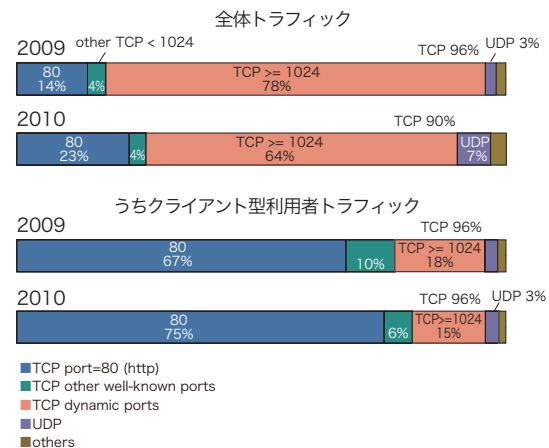


図-6 ポート別使用量概要

2010年のトラフィック量の90%がTCPです。全体のトラフィック量では、2009年に総量の78%だった1024番以上のTCPの動的ポートの割合が2010年には64%にまで減少しています。動的ポートでの個別のポート番号の割合はわずかで、最大でも総量の1%にしか過ぎません。一方、80番ポートの割合は、2009年の14%から23%に増加しています。つまり、2010年のトラフィック減少分を考慮すると、動的ポート同士の通信が約25%減少し、そのうちの1/3程が80番ポートに移行したと考えることができます。

また、クライアント型利用者に注目してみると、2009年に67%を占めていた80番ポートの利用割合は、2010年に75%まで増加しています。一方、動的ポートの割合は、18%から15%に減少しています。

これらのことから、依然として、TCP80番ポートのトラフィック量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ェアアップデートなども含まれるためコンテンツタイプは特定できませんが、クライアント・サーバ型の通信量が増えていると言えます。

protocol port	2009		2010	
	total (%)	client type	total (%)	client type
TCP *	95.80	95.73	90.09	95.82
(<1024)	18.23	77.31	26.46	80.87
80 (http)	14.46	67.30	23.00	75.12
554 (rtsp)	1.48	6.89	1.15	2.45
443 (https)	0.64	1.91	0.98	2.28
20 (ftp-data)	0.19	0.17	0.18	0.07
(>=1024)	77.57	18.42	63.63	14.95
1935 (rtmp)	0.36	1.51	1.04	2.91
6346 (gnutella)	1.10	0.60	0.86	0.33
6699 (winmx)	0.70	0.24	0.65	0.17
8084	0.00	0.00	0.61	0.00
UDP	2.24	2.60	6.79	2.76
ESP	1.87	1.55	2.91	1.30
GRE	0.07	0.08	0.14	0.06
IP-IP	0.01	0.00	0.04	0.01
ICMP	0.02	0.05	0.02	0.04

表-1 ポート別使用量詳細

図-7は、全トラフィックによるTCPポート利用状況の週間推移を2009年と2010年のそれぞれで示したものです。ここでは、TCPでのポート利用を、80番ポート、その他のウェルノウンポート、動的ポートの3つに分けています。また、トラフィックの絶対量が公開できないため、ピーク時の総トラフィック量を1として正規化しています。全トラフィックでは、動的ポートが支配的であり、そのピークが23:00～1:00にあります。また、土日には昼間のトラフィック量も増加していて、家庭での利用時間が反映されています。2009年のデータと比較してみると、80番ポートの割合が増えていることがわかります。

図-8は、図-7と同様にクライアント型利用者によるTCPポート利用状況の週間推移を示したものです。ここでも、2010年には80番ポートの割合が増加しています。また、ピーク時間は21:00～23:00で、全トラフィックの利用状況を示す図-7に比べて2時間ほど早くなっています。さらに、土日は朝から利用が増えています。

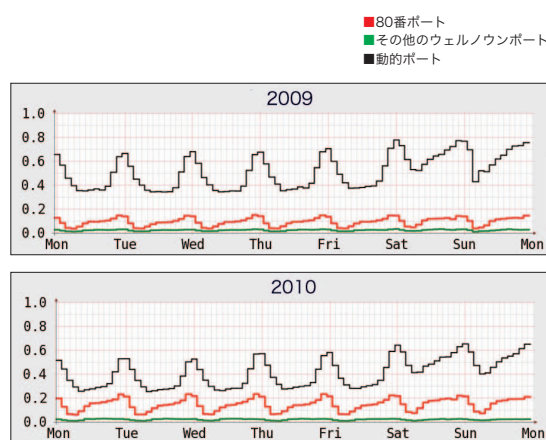


図-7 TCPポート利用の週間推移

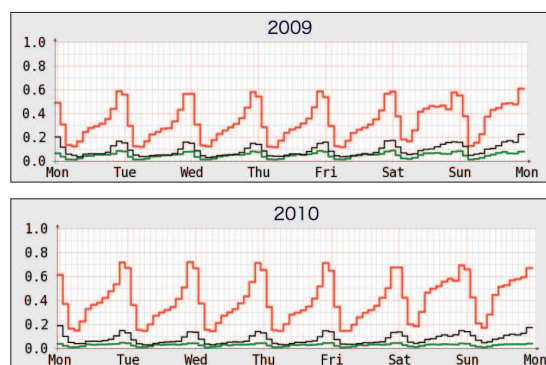


図-8 クライアント型利用者のTCPポート利用の週間推移

3.5 おわりに

前回のレポートでは、P2Pファイル共有に代表されるピア型トラフィックが、依然として量的に支配的であるものの、2005年からあまり増加していないことを示しました。また、利用者がP2Pファイル共有から、より使いやすく魅力的なビデオ共有サイト等のWebサービスへ移行している傾向を伝えました。その一方で、一般利用者の利用量が、ビデオコンテンツや他のWeb 2.0系のリッチコンテンツによって着実に増加していることも示しました。

今回の調査でも、これらの傾向に変化はありませんが、ヘビーユーザ部分の変動がこれまでよりも大きかったと言えます。ただし、ヘビーユーザや動的ポート同士の通信が単純に減ったわけではありません。ヘビーユーザ数は20%程減少しましたが、一方で極端なヘビーユーザのトラフィック量は増えています。また、ポートごとの通信量では、動的ポート同士の通信量が25%程減少しましたが、そのうちの約1/3は80番ポートに移行しています。これらのことから、前回のレポートで一般利用者に顕著だったP2Pファイル共有からWebサービスへの移行がヘビーユーザにも広がっていると言えます。

したがって、トラフィック量の減少と改正著作権法の影響に関しては、「改正著作権法でP2Pファイル共有が減った」というよりは、むしろ「以前からあったP2Pファイル共有からWebサービスへの移行という流れ

が、改正著作権法を契機に進んだ」と考えるべきだと思います。例えるならば、地震で地滑りが起こったのは、地盤が緩んでいたことが本当の原因であり、地震はあくまでトリガーに過ぎない、ということです。

世界的にも、トラフィックは、P2Pファイル共有からWebサービスへシフトしてきています[2、3、4]。また、今回取り上げた改正著作権法と同様に、他の国でも著作権に関する規制や法整備、あるいは違反者の検挙などで、トラフィックが減少したという事例が報告されています。しかし、ここまで示してきたように、個別の事例の背景には、著作権侵害のリスクに対する社会的認識の変化や、P2Pファイル共有の代替技術の成熟に伴う全体的な利用形態の変化が関係していることがあります。

今回取り上げた2010年初頭からのトラフィックの減少は日本だけの現象です。日本では、ファイバーアクセスが普及して帯域に余裕があるため、他の国に比べてヘビーユーザのトラフィック利用量の比率が高く、P2Pファイル共有でのトラフィックの割合も大きくなっています。その分、今回示したように、ヘビーユーザの挙動変化が全体に及ぼす影響が大きくなります。

IJでは、インターネットの利用形態の変化に迅速に対応できるよう、継続的にトラフィックの観測を行っています。今後も、定期的にレポートを提供していく予定です。

参考文献

- [1] 長 健二郎. 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. Internet Infrastructure Review. vol.4. pp18-23. August 2009.
- [2] G.-Maier, A.Feldmann, V.Paxson, and M.Allman. On Dominant Characteristics of Residential Broadband Internet Traffic. *IMC2009*. Chicago, IL, Nov. 2009.
- [3] C.Labovitz, D.McPherson, and S.Iekel-Johnson. 2009 Internet Observatory Report. *NANOG47*. Dearborn, MI. October, 2009.
- [4] Cisco. Visual Networking Index — Forecast and Methodology, 2009-2014. June 2010.

執筆者:

長 健二郎 (ちょう けんじろう)

株式会社IJイノベーションインスティテュート 技術研究所

インターネットトピック: マネージドセキュリティサービス(MSS)選定ガイドラインの紹介

ここでは、日本セキュリティオペレーション事業者協会(ISOG-J)*1と、この団体で作成し先日発行された『マネージドセキュリティサービス(MSS)選定ガイドライン』*2の概要を紹介します。

■日本セキュリティオペレーション事業者協会とは

ISOG-Jは、セキュリティサービスを提供する事業者の団体です。企業におけるセキュリティ確保を担う事業者が集まり、セキュリティオペレーションに関する情報共有や、共通課題を解決するための場として2008年6月に設立されました。その会員構成はセキュリティ専門会社、セキュリティ製品ベンダ、メーカ、SIベンダ、アンチウイルス製品ベンダ、ISPと多岐にわたっています。

ISOG-Jが設立された目的の1つに、セキュリティオペレーションに関する共通認識の醸成があります。現在、さまざまな事業者が自社のサービスに関してそれぞれ独自の表現を使っているため、利用者が自身の要求事項を満足する適切なサービスを選定しにくいという状況があります。また、セキュリティオペレーションはサービス提供者側の一方的な作業だけで完了するものではなく、利用者と事業者間の協力によってセキュリティを向上させるものです。利用者間と事業者間の認識の違いがあると、それに起因するトラブルを引き起こすことがあります。これら状況を改善し、トラブルの発生を少なくするための手段として、ガイドラインの策定を行うことになりました。

■サービスマップ

『マネージドセキュリティサービス(MSS)選定ガイドライン』は、2年間に及ぶISOG-Jのワーキンググループの活動成果です*3。活動の1年目には、各社が提供するセキュリティサービスの一覧作成とその分類を行い、結果をサービスマップ*4としてまとめました。これは、ISOG-Jに集まった事業者間で、サービスやセキュリティに関する考え方、サービスの特徴が異なり、ガイドラインで対象とするサービスの空間を定義する必要があったためです。

サービスマップでは、保護対象であるITシステムのライフサイクル(計画、導入、定常運用、異常運用)におけるセキュリティオペレーションの寄与に注目して、サービスを分類しました*5。

■マネージドセキュリティサービス(MSS)選定ガイドライン

サービスマップの整備により、対象とするサービスの範囲と、セキュリティオペレーションに関する認識がISOG-Jの会員間で共有できました。この認識をもとに、セキュリティサービスの利用方法をまとめたものが『マネージドセキュリティサービス(MSS)選定ガイドライン』です。

このガイドラインは、3部で構成されています。第1章において、用語や概念の定義と説明を行っています。また、第2章において、サービスマップの分類にも利用したITシステムのライフサイクルに応じて、「導入計画」「設計・構築」「定常運用」「異常運用」の各段階に分けて解説しています。「導入計画」では、導入の目的や保護対象の整理、要求事項のまとめ方、サービスや事業者の選定のポイントを示しています。「設計・構築」では、事業者とともに要求事項を具現化するための手順や注意点について紹介しています。「定常運用」では、定期報告や設定変更等、日常的に発生する利用者や事業者の相互関係について示しています。「異常運用」では、セキュリティインシデントの発生時に、利用者、事業者双方で行う確認事項や判断、対策実施について記載しています。そして、最後にAppendixにおいて、セキュリティサービス利用時のケーススタディとして、いくつかのセキュリティインシデントを例にとり、利用者と事業者の相互のやりとりを説明しています。これにより、実際にサービス利用したときに得られるものを具体的に示しています。

以上のように、このガイドラインでは、セキュリティサービスを選定する場合の、利用者側の準備について整理しています。このガイドラインを活用することによって、複数の事業者のサービスを公正に比較することができたり、利用者や事業者のお互いの思い込みで発生するトラブルを避けたりすることが可能となります。現在マネージドセキュリティサービスの導入を検討されている方だけではなく、すでにサービスに加盟している利用者にもご利用いただければと思います。

■今後の活動

ISOG-Jでは、今回紹介した活動以外にも、マネージドセキュリティサービスに関わる法制度の検討、技術情報の共有、オペレータ育成、オペレータ間のコミュニティ形成等、さまざまな活動を行っています。IJは、今後もISOG-Jの活動に積極的に参加し、セキュリティサービスの向上や、利用者の皆様のセキュリティ向上に役立てていきます。



執筆者:
齋藤 衛(さいとう まもる)
IJサービス本部 セキュリティ情報統括室

- *1 英語表記は、Information Security Operation providers Group Japan. 略称のISOG-Jは「いそぐじえい」と読む。ロゴの中央に位置するフクロウは、「知恵」や「賢明」のシンボルであるとともに、利用者のセキュリティを確保するために、日々夜更かして見張りを続けるオペレータを表している(<http://www.jnsa.org/isog-j/index.html>)。
- *2 マネージドセキュリティサービス(MSS)選定ガイドライン(<http://www.jnsa.org/isog-j/activities/result.html>)。セキュリティに関する運用を提供するサービスは、Managed Security Service(MSS)と英語表記されることが多いため、ガイドライン中でもMSSと表記している。
- *3 ガイドライン策定の経緯や内容については、次の発表に詳しく書かれている(http://www.jnsa.org/seminar/2010/0611/data/1-A_2.pdf)。
- *4 MASP事業者サービスマップ(<http://www.jnsa.org/isog-j/activities/result.html>)。
- *5 このマップでは、迷惑メール対策、安全なファイル交換手段、ICカード等による物理的なセキュリティ確保といった、特徴ある多くのサービスや機能が「その他」に分類されている。これは、マップの作成方針に因るものであり、これらのセキュリティ上の役割が小さいというわけではないことに注意が必要。

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@ij.ad.jp URL: <http://www.ij.ad.jp/>

本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。当社は、本書の内容につき細心の注意を払っていますが、本書に記載されている情報の正確性、有用性につき保証するものではありません。

©2008-2010 Internet Initiative Japan Inc. All rights reserved.

IJJ-MKTG019HA-1008KO-08000PR