

Internet Infrastructure Review

IIJ

Internet Initiative Japan

Vol.12

August
2011

インフラストラクチャセキュリティ

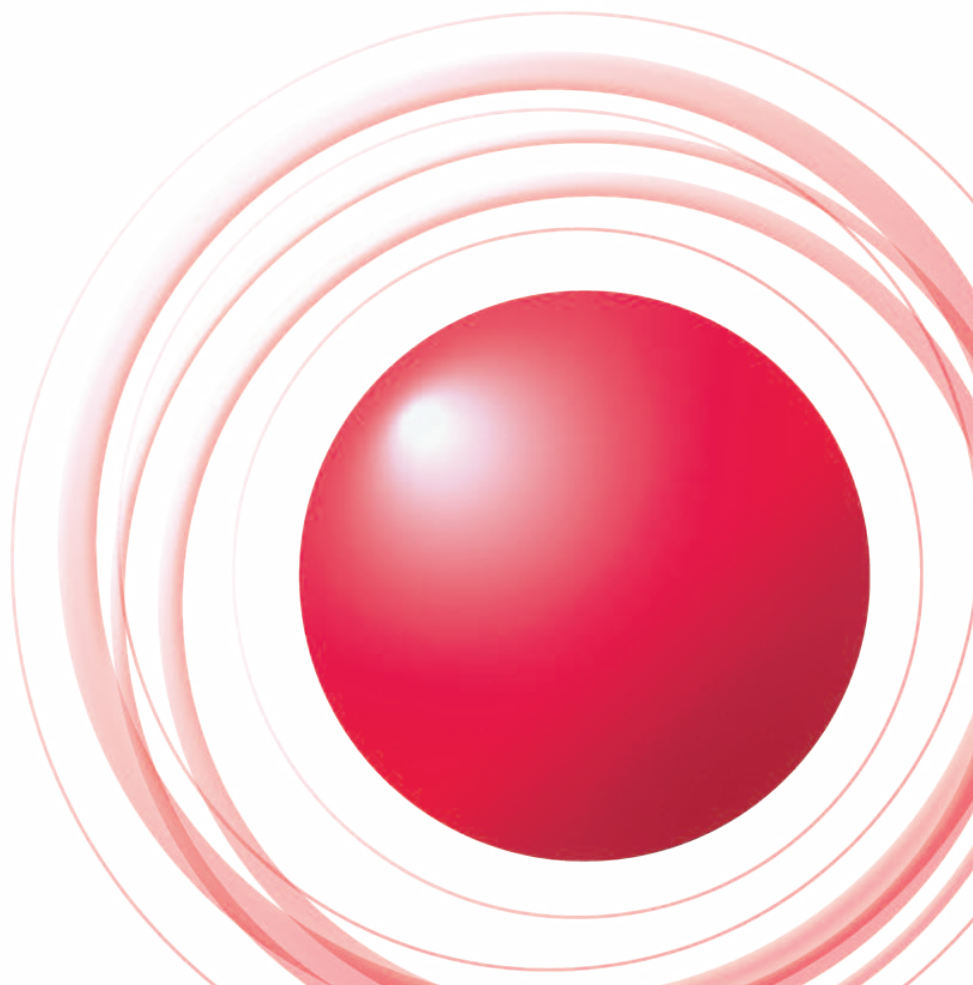
連続する企業や政府関係組織への攻撃

メッセージングテクノロジー

迷惑メール送信元地域の割合と実数が中国で急増

ブロードバンドトラフィックレポート

マクロレベルな視点で見た、震災によるトラフィックへの影響



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	4
1.3 インシデントサーベイ	7
1.3.1 DDoS攻撃	7
1.3.2 マルウェアの活動	9
1.3.3 SQLインジェクション攻撃	11
1.4 フォーカスリサーチ	13
1.4.1 連続する企業や政府関係組織への攻撃	13
1.4.2 電気通信事業者における大量通信等への対処と通信の秘密に関する ガイドライン(第2版)	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引き続き減少	22
2.2.2 日本が迷惑メール送信元の第2位に	23
2.2.3 主要迷惑メール送信元地域の推移	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 震災の影響について	25
3.3 データについて	27
3.4 利用者の1日の使用量	27
3.5 ポート別使用量	28
3.6 おわりに	30
インターネットトピック: 国内ISPによる児童ポルノブロッキングについて	31

エグゼクティブサマリ

世界のインターネットユーザ数は、2010年末時点で20億人に達しました。世界人口がおよそ70億人ですから普及率でいうと約30%、およそ3人に1人がインターネットを使っていることになります。一方携帯電話の契約数は50億あるそうですので、インターネットを使うユーザの数も、今後さらに増加すると考えても間違いではなさそうです。

そんな状況下で、本年4月には日本でもIPv4アドレスの在庫枯渇が起きました。マクロ的に見ると、単純計算では43億個利用可能なIPv4アドレスでは、実効上は20億のユーザを収容するのが限界であり、今後のユーザ数増大に備えるためにも、いよいよIPv6という次のフェーズのインフラ技術へのステップアップが必要になったということです。

また、インフラの上でのサービスを見ても、例えばfacebookのようなソーシャルメディアサービスは、1事業者で7億人のユーザを抱えています。同様に億単位のユーザを抱えるメディアサービス事業者は世界に何社もあります。このようなメディア事業者や、また、そこへのアクセスを提供するISPでは、ユーザの個人情報の管理や、流れるコンテンツの扱いについて、これまでとは規模や質が異なるレベルでの対応が求められるようになってきています。技術面でのステップアップのみならず、情報モラルや社会的規範の面でも、インターネットは次のステップにあがる必要があるでしょう。

本レポートは、このような状況の中で、IIJがインターネットというインフラを持続的に整備・発展させ、お客様に安心・安全に利用し続けていただくため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、2011年4月から6月末までの3ヵ月間を対象として、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、昨年末から継続的に発生している企業や政府機関を狙った攻撃の分析、及び、インターネットの安定的運用に関する協議会(第2期)が作成した「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン(第2版)」についての解説を行います。

「メッセージングテクノロジー」の章では、2011年4月から7月初頭までの13週間の迷惑メールの割合の推移と送信元地域の分布、主要迷惑メール送信元地域の推移を示します。またSPFとDKIMによる認証結果の割合について考察し、送信ドメイン認証技術の普及状況について論じます。

「ブロードバンドトラフィックレポート」の章では、東日本大震災が日本のブロードバンドトラフィックに与えた影響に関して、マクロレベルでの分析を行います。また、2011年5月30日からの1週間のトラフィック量やポート使用量を、昨年同時期のデータと比較することで、2010年からのトラフィックの傾向の変化について考察します。

「インターネットトピック」としては、2011年4月より複数の国内ISP等により順次開始されている、児童ポルノプロッキングについて、その背景やこれまでの検討経緯、及び、実施方法と今後の課題について解説します。

IIJでは、このような活動を通じて、インターネットの安定性を維持しながらも、日々改善し発展させて行く努力を続けております。今後も、お客様の企業活動のインフラとして最大限に活用していただくべく、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。

連続する企業や政府関係組織への攻撃

今回は、昨年末より頻発している政府関係組織や企業への連続的な攻撃の詳細を紹介するとともに、電気通信事業者におけるDDoS攻撃等への対応ガイドラインについて解説します。

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2011年4月から6月までの期間では、前回に引き続きWebブラウザとそのプラグインに関する脆弱性が悪用されました。また、スマートフォンの不正アプリケーションとして流布するマルウェアが増加し、韓国では金融システムに大規模なシステム障害が発生しました。さらに、世界各国の複数の企業や政府関係組織に対する攻撃が継続的に発生しています。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

1.2 インシデントサマリ

ここでは、2011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。まず、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。

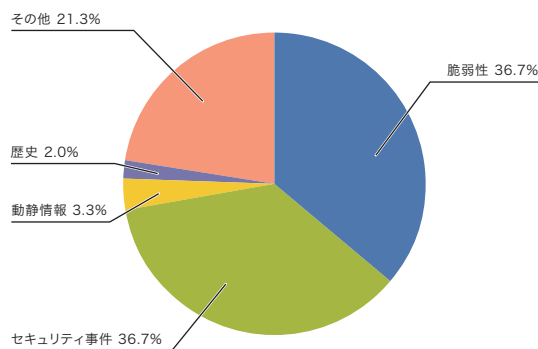


図-1 カテゴリ別比率(2011年4月～6月)

*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には、Microsoft社のInternet Explorer^{*2*3}、Windows^{*4*5*6}、Adobe社のAdobe ReaderとAcrobat^{*7*8}、Flash Player^{*9*10*11*12}、Shockwave Player^{*13}、Oracle社のJRE^{*14}、Webブラウザで3D表示するための標準仕様WebGL^{*15}等、Webブラウザやアプリケーションに数多く脆弱性が発見され、対策されています。Apple社のMac OS X^{*16*17}でも、複数の脆弱性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。

また、Microsoft社のIIS(Internet Information Service)^{*18}、Flashの配信に使われるFlash Media Server^{*19}、データベースサーバとして利用されているOracle社のOracle Database^{*20}、DNSサーバのISC BIND^{*21}、WebサーバのApache HTTP Server^{*22}、CMSとして利用されているWordPress^{*23}等、サーバアプリケーションでも多くの脆弱性が修正されました。さらに、携帯電話等のプラットフォームとして利用されているApple社のiOS^{*24}でも脆弱性が発見され、修正されています。

■ 動静情報

IIJは、国際情勢や時事に関連する各種動静情報にも注意を払っています。今回対象とした期間では、パキスタンにおけるビンラディン殺害、日中韓サミット、G8サミット等の動きに注目しましたが、IIJの設備やIIJのお客様のネットワーク上では直接関係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もありました。このため、各種の動静情報に注意を払いましたが、IIJの設備やIIJのお客様のネットワーク上では直接関係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、独自の主張を持つ複数の集団によって、政府や企業に対するDDoS攻撃やサーバからの情報漏えいが多数発生しました。この事件に関しては「1.4.1 連続する企

- *2 「マイクロソフト セキュリティ情報 MS11-018 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(2497640)」(<http://www.microsoft.com/japan/technet/security/bulletin/ms11-018.msp>)。
- *3 「マイクロソフト セキュリティ情報 MS11-050 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(2530548)」(<http://www.microsoft.com/japan/technet/security/bulletin/ms11-050.msp>)。
- *4 「マイクロソフト セキュリティ情報 MS11-020 - 緊急 SMB サーバの脆弱性により、リモートでコードが実行される(2508429)」(<http://www.microsoft.com/japan/technet/security/bulletin/ms11-020.msp>)。
- *5 「マイクロソフト セキュリティ情報 MS11-026 - 重要 MHTML の脆弱性により、情報漏えいが起こる(2503658)」(<http://www.microsoft.com/japan/technet/security/bulletin/ms11-026.msp>)。
- *6 「マイクロソフト セキュリティ情報 MS11-043 - 緊急 SMB クライアントの脆弱性により、リモートでコードが実行される(2536276)」(<http://www.microsoft.com/japan/technet/security/bulletin/ms11-043.msp>)。
- *7 APSB11-08:「Adobe ReaderおよびAcrobat用セキュリティアップデート公開(<http://www.adobe.com/jp/support/security/bulletins/apsb11-08.html>)。
- *8 APSB11-16:「Adobe ReaderおよびAcrobat用セキュリティアップデート公開(<http://www.adobe.com/jp/support/security/bulletins/apsb11-16.html>)。
- *9 APSB11-07:「Adobe Flash Player用セキュリティアップデート公開(<http://www.adobe.com/jp/support/security/bulletins/apsb11-07.html>)。
- *10 APSB11-12:「Adobe Flash Player用セキュリティアップデート公開(<http://www.adobe.com/jp/support/security/bulletins/apsb11-12.html>)。
- *11 APSB11-13:「Flash Player 用セキュリティアップデート公開(http://kb2.adobe.com/jp/cps/906/cpsid_90656.html)。
- *12 APSB11-18:「Flash Player 用セキュリティアップデート公開(http://kb2.adobe.com/jp/cps/907/cpsid_90799.html)。
- *13 APSB11-17:「Adobe Shockwave Player用セキュリティアップデート公開(<http://www.adobe.com/jp/support/security/bulletins/apsb11-17.html>)。
- *14 "Oracle Java SE Critical Patch Update Advisory - June 2011" (http://www.oracle.com/technetwork/topics/security/javacpujune2011-313339.html#PatchTable_JAVA)。
- *15 この脆弱性に関しては、発表者である次のContext Information Security社のBlogに詳しい「WebGL - A New Dimension for Browser Exploitation」(<http://www.contextis.com/resources/blog/webgl/>)。
- *16 「セキュリティアップデート 2011-003 について」(http://support.apple.com/kb/HT4657?viewlocale=ja_JP)。
- *17 「Mac OS X v10.6.8 のセキュリティコンテンツおよびセキュリティアップデート 2011-004 について」(http://support.apple.com/kb/HT4723?viewlocale=ja_JP)。
- *18 「マイクロソフト セキュリティ情報 MS11-035 - 緊急 WINS の脆弱性により、リモートでコードが実行される(2524426)」(<http://www.microsoft.com/japan/technet/security/bulletin/MS11-035.msp>)。
- *19 APSB11-11:「Adobe Flash Media Server用セキュリティアップデート公開」(<http://www.adobe.com/jp/support/security/bulletins/apsb11-11.html>)。
- *20 "Oracle Critical Patch Update Advisory - April 2011" (<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>)。
- *21 "Large RRSIG RRsets and Negative Caching can crash named" (<http://www.isc.org/software/bind/advisories/cve-2011-1910>)。
- *22 "Apache HTTP Server 2.2.19 Released" (<http://www.apache.org/dist/httpd/Announcement2.2.html>)。
- *23 「WordPress 3.1.4 (および 3.2 リリース候補 3)」(<http://ja.wordpress.org/2011/06/30/wordpress-3-1-4-and-3-2-release-candidate-3/>)。
- *24 「iOS 4.3.2 ソフトウェア・アップデートのセキュリティコンテンツについて」(http://support.apple.com/kb/HT4606?viewlocale=ja_JP)。

業や政府関係組織への攻撃」を参照してください。また、SQLインジェクション攻撃によりWebサイト改ざんを行うLizaMoonの活動が再確認されたり^{*25}、SNS^{*26}やGoogle Image検索^{*27}等を悪用する試みが継続して発生しています。さらに、これらの事件でダウンロードされるスケアウェアで、Mac OS Xを対象とするものが複数確認^{*28}されました。

これらの事件に加えて、スマートフォンのプラットフォームであるAndroid OSを対象とし、正規のアプリケーションマーケットで流通しているアプリケーションに、複数のマルウェアがあることが確認されました^{*29}。また、韓国では金融機関の業務システムに攻撃が原因とみられる大規模なシステム障害が発生し、数日間にわたりシ

ステムが停止したために、利用者に大きな影響を与えました^{*30}。さらに、世界中で200万台以上が感染しているといわれるCorefloodボットネットの活動を停止させるため、米国の法執行機関によってC&Cサーバの停止とドメインの差押えを含む対応が行われました^{*31}。

■ その他

その他の直接インシデントに関係しない動向としては、IPv6によるサービス提供を世界規模で確認するWorld IPv6 Day^{*32}が6月に実施されました。また、日本国内のISPによる児童ポルノサイトのブロッキングが開始されました^{*33}。さらに、コンピュータウイルスの作成等を処罰する「情報処理の高度化等に対処するための刑法等の一部を改正する法律案」が国会で可決されました^{*34}。

*25 Lizamoonの活動に関しては、例えば次のIBM社の東京SOCによる報告に詳しい。「新しいタイプのWebサイト改ざんSQLインジェクション攻撃(続報)」(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/sqlinjection_20110516)。

*26 SNSを利用した攻撃には、次のエフセキュアブログに紹介されているような例がある。「WindowsとMac双方のマルウェアを拡散するFacebook攻撃」(<http://blog.f-secure.jp/archives/50606705.html>)。

*27 この件に関しては、例えば次のエフセキュアブログに詳しい。「Google Webサーチを使用して改ざんされたGoogle画像を見つける」(<http://blog.f-secure.jp/archives/50604330.html>)。

*28 MacOSで動作するスケアウェアについては、例えば次のトレンドマイクロ社のセキュリティブログで紹介されている。「Macユーザを狙う不正プログラム、次々と確認される」(<http://blog.trendmicro.co.jp/archives/4225>)。

*29 Android Marketで配布するマルウェアについては、例えばSOPHOS社のブログであるnakedsecurityで紹介されている。「Android market affected by SMS Trojans」(<http://nakedsecurity.sophos.com/2011/05/13/android-market-affected-by-sms-trojans/>)

*30 この件に関しては、例えば次のNetwork Worldの報道に詳しい。「South Korea probes possible cyberattack on large bank」(<http://www.networkworld.com/news/2011/041911-south-korea-probes-possible-cyberattack.html>)。

*31 このボットネットのテイクダウンに関しては、次の米国司法省とFBIの共同発表に詳しい。「More Than 2 Million Computers Infected with Keylogging Software as Part of Massive Fraud Scheme」(<http://www.justice.gov/opa/pr/2011/April/11-crm-466.html>)。

*32 World IPv6 Dayに関しては、例えば次のIPv4アドレス枯渇対応タスクフォースより文章が公開されている。「World IPv6 Dayのご案内」(<http://www.kokatsu.jp/blog/ipv4/event/W6D.pdf>)。公式には次のInternet Societyの特設ページがある。「World IPv6 Day」(<http://www.worldipv6day.org/>)。

*33 一般社団法人インターネットコンテンツセーフティ協会「児童ポルノ画像が掲載されたサイトのブロッキングなどの流通防止の取り組みを開始」(<http://www.netsafety.or.jp/news/press/press-003.html>)。この活動については「インターネットトピック: 国内ISPによる児童ポルノブロッキングについて」も合わせて参照のこと。

*34 次の法務省のホームページでは法案やFAQ等の資料が掲載されている。「情報処理の高度化等に対処するための刑法等の一部を改正する法律案」(http://www.moj.go.jp/keiji1/keiji12_00025.html)。また法務省による解説「いわゆるコンピュータ・ウイルスに関する罪について」(<http://www.moj.go.jp/content/000076666.pdf>)も参照のこと。

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

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになっており、その内容は、状況により多岐にわたります。しかし、一般には、脆弱性等の高度な知識を利用した攻撃ではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にしたりすることでサービスの妨害を狙ったものになっています。

■ 直接観測による状況

図-2に、2011年4月から6月の期間中に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。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、攻撃の実態を

正確に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、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^{*35}、サーバに対する攻撃^{*36}、複合攻撃(1つの攻撃対象に対して同時に数種類の攻撃を行うもの)の3種類に分類しています。

この3ヵ月間でIJは、549件のDDoS攻撃に対処しました。1日あたりの平均対処件数は6.0件で、前回のレポート期間と比べて減少しています。DDoS攻撃全体に占める各種攻撃の割合は、回線容量に対する攻撃が0%、サーバに対する攻撃が75%、複合攻撃が25%でした。

今回の対象期間中に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されるもので、最大3万ppsの packets によって131Mbpsの通信量を発生させるものでした。また、攻撃の継続時間は、全体の89%が攻撃開始から30分未満で終了し、11%が30分以上24時間未満の範囲に分布しています。24時間以上継続した攻撃はありませんでした。なお、今回最も長く継続した攻撃は、サーバに対する攻撃に分類されるもので16時間にわたりました。攻撃元の分布としては、国内、国

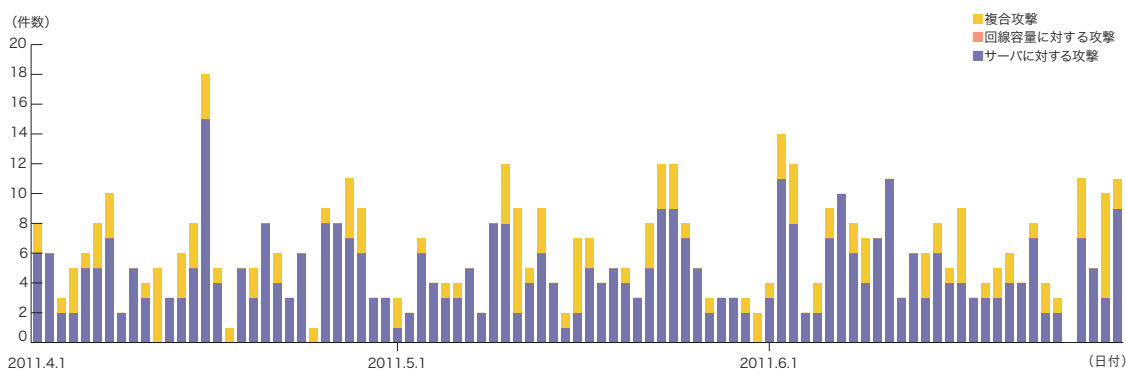


図-2 DDoS攻撃の発生件数

*35 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。

*36 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。

外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング*³⁷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*³⁸の利用によるものと考えられます。

■ backscatterによる観測

次に、IJJでのマルウェア活動観測プロジェクトMITFのハニーポット*³⁹によるDDoS攻撃のbackscatter観測結果を示します*⁴⁰。backscatterを観測することで、外部のネットワークで発生したDDoS攻撃の一部を、それに介在することなく第三者として検知できます。2011年4月から6月の期間中に観測したbackscatterについて、ポート別のパケット数推移を図-3に、発信元IPアドレスの国別分類を図-4にそれぞれ示します。

観測されたDDoS攻撃の対象ポートのうち最も多かったものは、Webサービスで利用される80/TCPで、対象期間における全パケット数の44.5%を占めています。また、リモートデスクトップで利用される3389/TCPや、DNSで利用される53/TCPへの攻撃も観測されています。図-4で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、アルゼンチン31.6%、米国25.1%、中国18.5%、日本10.6%が比較的大きな割合を占めており、以下その他の国々が続いています。

前回のレポート期間に引き続いて、アルゼンチンの複数のIPアドレスに対して、ポートスキャンに似た複数ポートへの攻撃が5月16日まで観測されました。対象

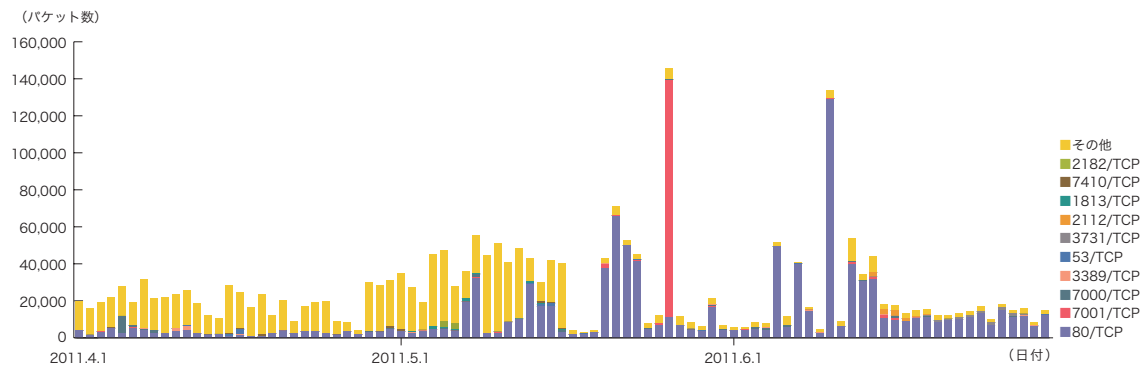


図-3 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

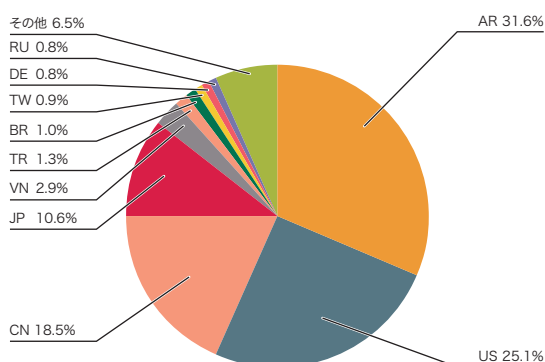


図-4 backscatter観測によるDDoS攻撃対象の分布(国別分類、全期間)

*37 発信元IPアドレスの詐称。他人からの攻撃に見せかけたり、多人数からの攻撃に見せかけたりするために、攻撃パケットの送出時に、攻撃者が実際に利用しているIPアドレス以外のアドレスを付与した攻撃パケットを作成、送出すること。

*38 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。

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

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

ポート80/TCPに対しては5月以降にDDoS攻撃の大きな増加が数回見られました。このうち5月における3回の増加では、主に日本国内のホスティング事業者が持つIPアドレスが攻撃対象になっています。5月26日には7001/TCPを対象とする攻撃が特に多く観測されていますが、すべて中国国内の2つのIPアドレスが攻撃対象となっています。

また、今回の対象期間中には、Anonymous等による複数のDDoS攻撃が話題になりました^{*41}。IJJでの観測でも、それらのうちSony社関連サイトへの攻撃、米国General Electric社サイトへの攻撃、ブラジル政府系サイトへの攻撃によるものと考えられるbackscatterをそれぞれ検知しています。

1.3.2 マルウェアの活動

ここでは、IJJが実施しているマルウェアの活動観測プロジェクトMITF^{*42}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^{*43}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

2011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-5に、その発信元IPアドレスの国別分類を図-6にそれぞれ示します。MITFでは、数多くのハニーポットを用いて観測

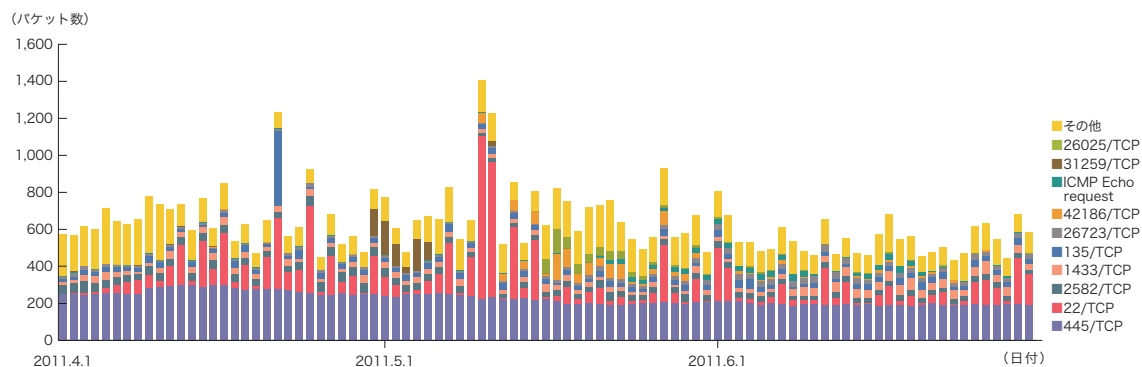


図-5 ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

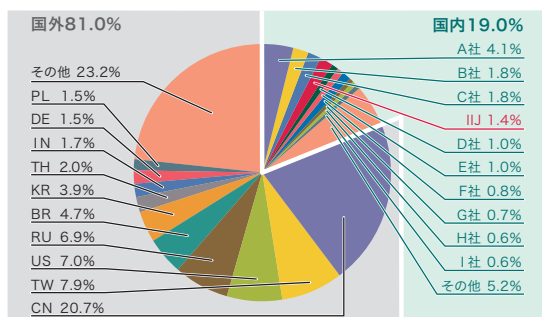


図-6 発信元の分布(国別分類、全期間)

*41 AnonymousやLulzSec等による一連の事件については、「1.4.1 連続する企業や政府関係組織への攻撃」に解説している。

*42 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。

*43 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て、攻撃者の行為やマルウェアの活動目的を記録する装置。

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。また、この観測では、MSRPCへの攻撃のような特定のポートに複数回の接続を伴う攻撃は、複数のTCP接続を1回の攻撃と数えるように補正しています。

ハニーポットに到着した通信の多くは、Microsoft社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQL Serverで利用される1433/TCPや、SSHで利用される22/TCPに対する探索行為も観測されています。これらに加えて、2582/TCP、25723/TCP、31259/TCP等、一般的なアプリケーションでは利用されない目的不明な通信も観測され

ました。図-6で発信元の国別分類を見ると、中国の20.7%、日本国内の19.0%が比較的大きな割合を占めています。

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの取得検体数の推移を図-7に、そのうちのユニーク検体数の推移を図-8に、マルウェアの検体取得元の分布を図-9にそれぞれ示します。このうち図-7と図-8では、1日あたりに取得した検体^{*44}の総数を総取得検体数、検体の種類をハッシュ値^{*45}で分類したものをユニーク検体数としています。また、検体をアンチウイルスソフトウェアで判別し、上位10種類の内訳をマルウェア名称別に色分けして示しています。

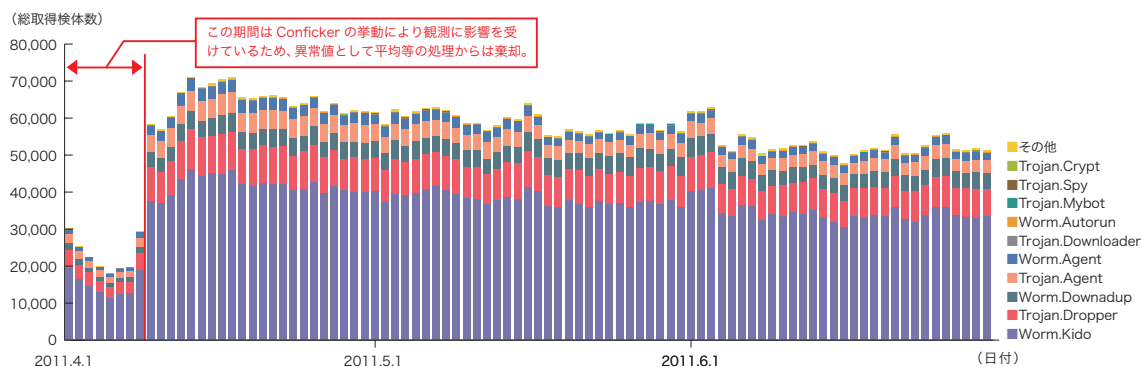


図-7 総取得検体数の推移

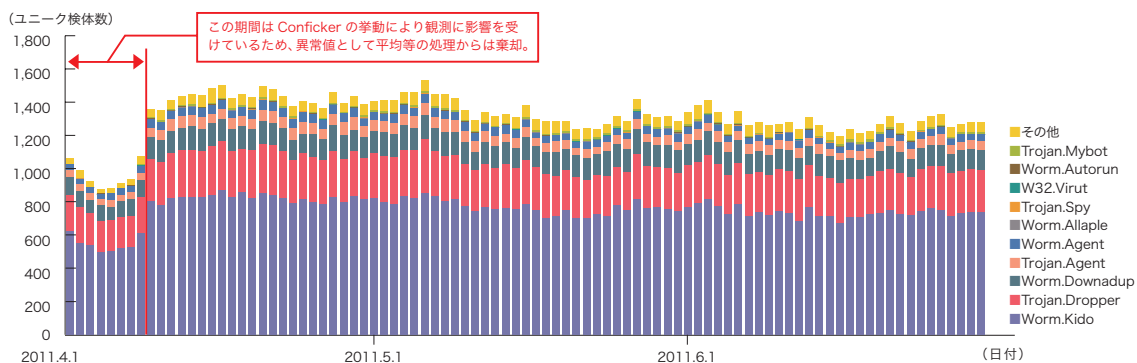


図-8 ユニーク検体数の推移

*44 ここでは、ハニーポット等で取得したマルウェアを指す。

*45 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。

今回からdionaea^{*46}を中心とした新システムを用いて観測を行っています。4月1日から4月8日までは、それ以降の期間より検体取得数が少なくなっています。これは、Confickerの亜種の一部がハニーポットに対して繰り返し攻撃を行い、観測システムに負荷を与えていたためです。IJでは、dionaeaの実装、MSRPCプロトコル、Confickerの解析等で原因追求を行いました。その結果、Confickerの挙動を変えないかぎりこの現象は収まらないことが分かりました。このため、一度検体を取得した攻撃元に関しては、その後一定時間アクセスを拒否するように観測システムを修正しました。この修正によって、1台の感染PCから同一の検体を多数取得してしまう問題が排除でき、負荷の低減によって他の検体の取得数が増加することを確認しています。また、この問題の影響下にあった期間の観測情報は、観測上の異常値として平均等の計算からは除外しました。

期間中での1日あたりの平均値は、総取得検体数が58,368、ユニーク検体数が1,343でした。マルウェアの種類としては、Conficker(図-7や図-8でのWorm.Kido及びWorm.Downadup)が中心的な勢力を持ち、総検体取得数で72.4%、ユニーク検体数で67.2%を占

めています。図-9に示す検体取得元の分布では、日本国内が2.7%、国外が97.3%でした。国別分布では、ロシア16.0%、台湾11.7%、ブラジル9.9%、米国9.2%の順でした。これは、主にConfickerが国外において大規模に活動しているためです。

MITFでは、マルウェアの解析環境を用意し、取得した検体に関する独自の解析も行っています。今回の調査期間中に取得した検体は、ワーム型75.1%、ポット型2.3%、ダウンロード型22.6%でした。また、解析により、23個のポットネットC&Cサーバ^{*47}と17個のマルウェア配布サイトの存在を確認しました。

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^{*48}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。

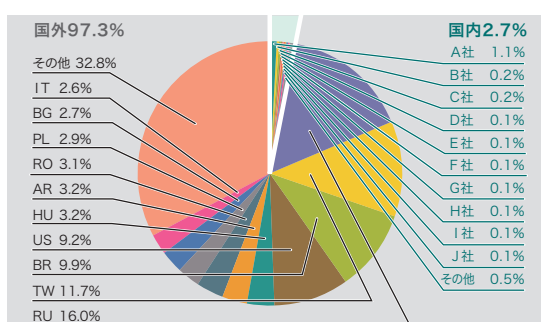


図-9 検体取得元の分布(国別分類、全期間)

*46 dionaea (<http://dionaea.carnivore.it/>) とその機能についてはIIR Vol.11 (http://www.ij.ad.jp/development/iir/pdf/iir_vol11_infra.pdf) の「1.4.1 dionaeaハニーポット」でも解説している。

*47 Command & Controlサーバの略。多数のポットで構成されたポットネットに指令を与えるサーバ。

*48 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。

2011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-10に、攻撃の発信元の分布を図-11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53.0%、中国11.6%、米国11.1%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生件数には、前回からあまり変化していません。日本と中国からの攻撃の割合が増加していますが、これは前回

多かった米国からの攻撃が減少したためで、攻撃件数の傾向はあまり変わっていません。また、前回のレポート期間で話題となったSQLインジェクションによりWebサイト改ざんを行うLizaMoonの活動が、再活動しているとの報告がありましたが、お客様のネットワークでは攻撃を確認できませんでした。

ここまで示したとおり、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。

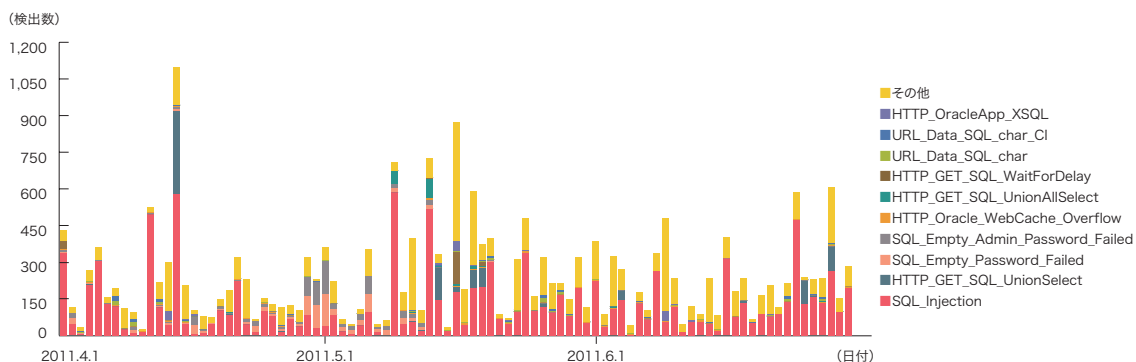


図-10 SQLインジェクション攻撃の推移(日別、攻撃種別)

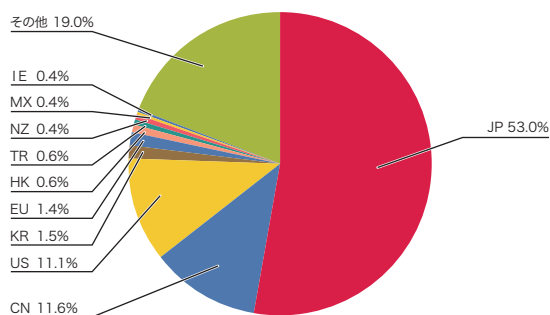


図-11 検体取得元の分布(国別分類、全期間)

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続けることで対策につなげています。ここでは、これまでに実施した調査のうち、昨年末より継続的に発生している企業や政府機関を狙った攻撃と、電気通信事業者におけるDDoS攻撃等への対応ガイドラインについて解説します。

1.4.1 連続する企業や政府関係組織への攻撃

この3ヵ月間(2011年4～6月)は、企業等への攻撃や情報漏洩事件が世界中で数多く発生しました^{*49}。また、それまでは主にDDoS攻撃による政治的主張を繰り返してきたAnonymousが、その活動範囲を拡大し、より活発な動きを見せた期間でもありました^{*50*51}。ここでは、これらの事件を振り返りつつ、攻撃内容の変化等を分析し、今後どのように対応すべきかについて考察します。

表-1 企業や政府関係組織への攻撃、情報漏洩事件一覧(2011年4月～6月)

※太字はSony社関連企業への攻撃、グレーの地色はAnonymous関連の攻撃、赤い地色はLulzSec及びAntiSec関連の攻撃の事例を示す。

日付	概要	種別	攻撃の主体
04.01	マーケティングサービス会社Epsilonが外部から侵入され、多数の顧客企業の個人情報(メールアドレス)が流出。数百万人分のぼると見られる。	情報漏洩	
04.03	AnonymousがSonyに対するDDoS攻撃を行う。(#OpSony)	DoS	Anonymous
04.08	韓国の大手金融会社である現代キャピタルから40万人以上の顧客情報が流出。	情報漏洩	
04.11	米国テキサス州当局から約350万人分の個人情報が漏洩。	情報漏洩	
04.12	セキュリティベンダーのBarracuda Networksが自社製品のWAF(Web Application Firewall)のメンテナンス中にSQLインジェクション攻撃を受け、内部情報が流出。	情報漏洩	
04.13	韓国の農協銀行システムで不正なプログラムの実行により障害。ATM、ネット、窓口等が数日間すべて停止。	DoS	
04.13	ブログサービス大手のWordpress.comが外部から侵入され、管理者権限を奪われる。	情報漏洩	
04.17	米国エネルギー省傘下のオークリッジ国立研究所がメールによる標的型攻撃を受ける。	標的型	
04.20	Anonymousがイタリアの大手電力会社ENELとフランスの大手電力会社EDFに対してDDoS攻撃を行う。(#OperationGreenRights)	DoS	Anonymous
04.26	Anonymousがニュージーランド政府に対するDDoS攻撃を開始。(#OpNZBlackOut)	DoS	Anonymous
04.26	PlayStation Network (PSN)から約7,700万人分の個人情報が漏洩。	情報漏洩	
05.01	Anonymousがイラン政府に対するDDoS攻撃を開始。(#OpIran)	DoS	Anonymous
05.02	Sony Online Entertainment (SOE)で約2,640万人分の個人情報が漏洩。	情報漏洩	
05.05	パスワード管理サービス大手のLastPassが外部から侵入され、ユーザのパスワード情報が漏洩した可能性がある。	情報漏洩	
05.05	ギリシャのSony Music Greeceのサイトの一部が改ざんされる。個人情報も流出。	情報漏洩、改ざん	
05.06	米国のSony Electronicsの個人情報一部流出。	情報漏洩	
05.07	LulzSecが米国のオーディション番組X Factorの応募者情報を公開する。	情報漏洩	LulzSec
05.10	LulzSecが米国の大手テレビネットワークFOXに侵入し内部情報を公開する。	情報漏洩	LulzSec
05.11	インドネシアのSony Music Indonesiaでサイトの一部が改ざんされる。	改ざん	
05.14	スクウェア・エニックスの欧州子会社から個人情報が漏洩。	情報漏洩	Anonymous
05.15	AnonymousがENELに対して再びDDoS攻撃を行う。(#OperationGreenRights)	DoS	Anonymous
05.16	インターネットサービスプロバイダーのSo-netで、第三者が他人のアカウントを不正に利用しポイントの不正交換を行う。	アカウント盗用	
05.19	ゲーム専用ポイントサービスのgamer-point.netから約5,200人分の個人情報が漏洩。	情報漏洩	
05.20	タイのSony Thailandのサイトの一部が改ざんされフィッシングサイトに悪用される。	改ざん	
05.22	AnonymousがENELに対して再びDDoS攻撃を行う。(#OperationGreenRights)	DoS	Anonymous
05.23	セキュリティサービス会社のComodo BrazilがSQLインジェクションで攻撃され、内部情報が流出。	情報漏洩	
05.24	Anonymousが米商工会議所のサイトuschamber.comにDDoS攻撃を行う。(#Operation Payback)	DoS	Anonymous
05.24	カナダのSony Ericsson Canadaのサイトがレバノン人ハッカーIdahcによってSQLインジェクション攻撃を受け、約2,000人分の個人情報が流出。	情報漏洩	Idahc
05.24	イタリアのSony Pictures ItaliaのサイトでSQLインジェクション脆弱性が見つかる。	情報漏洩	
05.24	日本のソニーミュージックのサイトでSQL Injection脆弱性が見つかる。	情報漏洩	LulzSec
05.27	米国の航空宇宙/防衛企業大手Lockheed Martin社で外部からの不正侵入が発生。対応が早かったため情報流出は特にない。3月にRSAから流出したSecurIDの情報が悪用された。	標的型	
05.27	カナダのHonda Canadaで28.3万人分の顧客情報が今年の2月に流出していたことが判明。	情報漏洩	
05.28	インターネット販売のunicoオンラインショップで不正アクセス。約17,000人分の個人情報が流出。	情報漏洩	
05.30	米国の公共放送ネットワークであるPublic Broadcasting Service (PBS) がLulzSecに侵入され、ニュースサイトに偽の記事が投稿されるとともに、メールアドレスやパスワード等を含む多数の内部の個人情報が流出。	情報漏洩、改ざん	LulzSec

*49 例えば、世界中の情報漏洩事件を記録しているDataLossDB (<http://datalossdb.org/>) では、6月に90件のインシデントを記録している。これは2008年12月の95件に次いで過去2番目に多い。

*50 Anonymousは2006年頃、米国の匿名掲示板サイトを起源として生まれたと言われる活動。この活動には誰でも参加することができ、Anonymousという名が活動への参加者個人を指すこともある。2008年に宗教団体への抗議活動を行ったことで世間に知られるようになった。Anonymousの中で大きな勢力を占めているAnonOpsは、ネットの自由等を理由に、これまで多数のサイトに対するDDoS攻撃を行っている。昨年末にはPayPal、Visa、MasterCard等WikiLeaksへの寄付受付を停止した企業に対するDDoS攻撃を行った。また今年に入ってからは、チュニジアやエジプトにおける民主化運動の際に、それぞれの政府関連Webサイトに対するDDoS攻撃を行っている。

*51 このようにDDoS攻撃等によってインターネット上で政治的な主張をする行為を"hacktivism"と呼ぶ。"hack"と"activism"とを組合せて作られた造語。

日付	概要	種別	攻撃の主体
06.02	Gmailでメールアドレスのなりすましが行われていたことをGoogleが公表。米政府関係者や中国の活動家等数百人が被害にあった。フィッシングでユーザ名とパスワードをとられ、メールをすべて外部にフォワードする設定に変更された。	標的型	
06.03	Anonymousがイラン外務省における機密文書(ビザ発給に関するメール等)を公開。(#Opran)	情報漏洩	Anonymous
06.03	AnonymousがEDFに対して再びDDoS攻撃を行う。(#OperationGreenRights)	DoS	Anonymous
06.03	Gmailだけでなく、HotmailやYahoo! Mailでも同様の攻撃が行われていたことを、セキュリティ企業のTrendMicroが報告。	標的型	
06.03	米国のSony Pictures、ベルギーのSony BMG Belgium、オランダのSony BMG NetherlandsでLulzSecによる情報流出。Sony Picturesは後日、約37,500人分の顧客情報が流出したことを認めた。	情報漏洩	LulzSec
06.04	LulzSecがInfragardアトランタ支部のサイトに侵入し、約180人分の個人情報情報を公開。またInfragard協力企業(Unveillance)のメール約1,000通もあわせて公開。InfragardはFBIとアメリカの民間企業が協力して運営する非営利団体で、情報の共有や分析等を行っている。	情報漏洩	LulzSec
06.04	米国のNintendo.comでサーバ設定ファイルの一部がLulzSecによって公開される。任天堂は数週間前に不正侵入を受けたが、個人情報が含まれていなかったため、発表していなかったとコメント。	情報漏洩	LulzSec
06.04	台湾の大手PCメーカーであるAcerの欧州のサイトがPCA (Pakistan Cyber Army)によって侵入され、40,000人以上の個人情報流出。	情報漏洩	PCA
06.04	欧州のSony Europeがレバノン人ハッカー Idahcによって侵入され、120人分の個人情報流出。	情報漏洩	Idahc
06.05	ロシアのSony Pictures RussiaのサイトでSQLインジェクション脆弱性が公開される。個人情報の流出はなし。	情報漏洩	
06.05	ブラジルのSony Music Brazilのサイトが昨年11月から改ざんされていたことが発覚。	改ざん	
06.06	Sony Computer EntertainmentのDeveloper Network (scedev.net)のソースコードと、Sony BMGの内部ネットワーク情報がLulzSecによって公開される。	情報漏洩	LulzSec
06.08	ゲーミングショップで4月に不正アクセスが行われ、顧客情報が流出していたことを公表。	情報漏洩	
06.08	ソニーポイントで、第三者によるアカウントの不正利用。95件のメールアドレスが利用され、27,800ポイント(約28万円相当)が不正に交換された。	アカウント盗用	
06.09	米Citigroupで不正侵入による情報流出。シティカードをもつ顧客のうち約36万人分のクレジットカード情報が漏洩し、約270万ドルの被害が発生した。	情報漏洩	
06.09	ポルトガルのSony Music Portugal(sonymusic.pt)がIdahcによって侵入され、約350人分のメールアドレスが公開される。	情報漏洩	Idahc
06.10	Anonymousが米国の大手バイオ化学メーカー Monsantoに対してDDoS攻撃を行う。(#OperationGreenRights)	DoS	Anonymous
06.10	英国のゲーム開発会社 Codemasterが不正侵入を受け、顧客情報が流出。	情報漏洩	
06.10	中越間で南シナ海の領有権をめぐる対立が激化。サイバー攻撃も活発になり、ベトナムの1,500以上のサイトが改ざんの被害にあう。	改ざん	
06.12	国際通貨基金(IMF)に対して大規模な攻撃が行われていたとの報道。	標的型	
06.12	Sony関連の3つのサイトでLulzSecによってSQLインジェクション脆弱性が公開される。個人情報の流出等はなし。	情報漏洩	LulzSec
06.13	ゲーム開発会社Epic Gamesが不正アクセスを受け、ユーザのパスワードをリセット。	情報漏洩	
06.14	LulzSecがゲーム会社のBethesdaと米上院のサイト Senate.govに不正侵入し、入手した情報を公開。	情報漏洩	LulzSec
06.15	LulzSecが複数のゲーム関係サイトにDDoS攻撃を行う。	DoS	LulzSec
06.16	Anonymousがマレーシアの政府関係サイトにDDoS攻撃。少なくとも41のサイトで被害。	DoS	Anonymous
06.16	LulzSecが複数のサイトにDDoS攻撃を行う。電話リクエストに応じてランダムにターゲットを選択。最後にCIAを攻撃し、サイトが一時ダウン。	DoS	LulzSec
06.17	Anonymousがスペイン、シリア、トルコの政府関係サイトにDDoS攻撃。	DoS	Anonymous
06.17	ゲーム開発会社BioWareで不正侵入。18,000人分の個人情報流出。	情報漏洩	
06.18	セガの欧州子会社の運営するサービス「SEGAPASS」で不正侵入。約130万人分の個人情報流出。	情報漏洩	
06.19	Anonymousが米国企業のGE (www.ge.com)に対してDDoS攻撃を行う。(#OperationGreenRights)	DoS	Anonymous
06.20	仮想通貨Bitcoinの交換所サイトMt.Goxでアカウント情報が漏洩。さらにそのアカウント情報を利用した不正取引により交換レートが一時暴落。	アカウント盗用 情報漏洩	
06.20	フランスのSony Pictures Franceで Idahc等によってSQLインジェクション脆弱性が発見され、一部の情報が公開される。	情報漏洩	Idahc
06.20	ドメイン登録業者のNetwork Solutionsが6/20と6/21に2度にわたりDDoS攻撃を受ける。	DoS	
06.21	認証局サービスのStartComが6/15に不正侵入されていたことが判明。証明書発行には特に影響なし。	情報漏洩	
06.23	米国の移動通信事業者であるVirgin Mobileの顧客情報が流出。	情報漏洩	AntiSec
06.24	LulzSecが米国アリゾナ州当局の内部情報を公開する。	情報漏洩	AntiSec
06.24	Anonymousがドイツの製薬企業大手BAYERに対してDDoS攻撃を行う。(#OperationGreenRights)	DoS	Anonymous
06.25	Anonymousがブラジル政府系サイトにDDoS攻撃を行う。(OpBrazil)	DoS	Anonymous
06.25	ハッカーチームのTeaMp0isoNが英国の首相トニー・ブレア氏の個人情報(Webメールのアドレス帳)を公開する。	情報漏洩	TeaMp0isoN
06.27	Anonymousがチュニジア政府系サイトを攻撃、改ざん。	改ざん	Anonymous
06.29	LulzSecが米国アリゾナ州当局の内部情報を公開する。(2回目)	情報漏洩	AntiSec
06.29	米国のメディアグループ企業Viacomと大手レコード会社Universal Musicの内部情報が流出。	情報漏洩	AntiSec
06.29	Anonymousが米国フロリダ州オーランド市当局のサイトにDDoS攻撃を行う。(OpOrlando)	DoS	Anonymous
06.29	米国の掲示板サイト4chan.orgへのDDoS攻撃が発生。	DoS	
06.29	MasterCardへのDDoS攻撃が発生。しかしMasterCardはISPの問題だったと攻撃を否定。	DoS	
06.29	MySpaceとPayPalの一部ユーザの認証情報が流出。	情報漏洩	
06.30	Grouponのインド子会社(SoSasta)で約30万人分の個人情報流出。データベースの内容がまるごとGoogleで検索可能な状態になっていた。	情報漏洩	

(注1) Operation Anti-Security (AntiSec) はLulzSecとAnonymousが共同で6月20日から開始した作戦で、参加者も攻撃の主体も様々であるが、ここでは呼びかけを行ったLulzSecの活動として色分けを行った。

(注2) この表で取り上げた事件はすべて、ニュースサイト等で一般に公開されている情報に基づいている。

■ 主要なトピック

この期間に発生した主なセキュリティ事件を表-1に示します。マーケティングサービスを行うEpsilon社から数百万人分のメールアドレスが流出した事件を皮切りに、大規模な情報漏洩事件が相次いで起こりました。特に、PSN (PlayStation Network) 及びSOE (Sony Online Entertainment) 社で起きた、合わせて約1億件にも上る個人情報漏洩は過去最大規模のものでした。

もう1つの大きな話題は、5月に突如活動を開始したLulzSecによる多数の情報流出です。LulzSecは、Anonymousを母体として生まれたグループで、今年2月に起きたセキュリティ企業HBGary社への侵入事件を主導したメンバによって構成されていると言われていいます。彼らは、FoxやPBS等のメディア企業、Sony社関連企業、ゲーム開発会社、米上院やFBI関連のサイト等、多数のサーバに不正に侵入し、そこから取得した内部情報を一般に公開するという行為を繰り返しました。特にSony社に対する執着が強く、4度にわたって関連企業サイトへの攻撃を行いました。また、これに便乗する形で世界中の関連企業が狙われ、主なものだけでも20件以上の攻撃が行われました^{*52}。

Anonymousも、Sony社を始めとしてイタリアとフランスの電力会社やニュージーランド、イラン、アメリカ、マレーシア、シリア、スペイン、トルコ、ブラジル等の政府系サイトへのDDoS攻撃を行いました。特に6月下旬にLulzSecがAnonymousとの共同作戦「Operation Anti-Security (AntiSec)」を宣言してからは、世界中で攻撃活動がさらに活発になりました^{*53}。なお、LulzSecは、その後活動開始50日目に突然に活動の終了を宣言しました^{*54}。しかし、AnonymousによるAntiSecの攻撃は衰えることがなく、参加者を増やしながら継続しています。

これらに加えて注目すべき事件として、米国の国防に関わる組織等に対して相次いで行われた標的型攻撃^{*55}

があります。まず、オークリッジ国立研究所等の米エネルギー省傘下の複数の組織が攻撃され、復旧のために外部とのネットワーク接続を一時切断しなければならない事態になりました。また、Lockheed Martin社は、今年3月にRSA (EMC社) から流出した情報を悪用して攻撃されました^{*56}。同じ時期には、L-3 Communications社やNorthrop Grumman社等の国防関連企業も攻撃されました。これらは軍事機密情報を狙った一連の活動の可能性があります、詳細は分かっていません。

■ 分析

この期間中で特に目立った活動は、Anonymous、LulzSec及びAntiSecに関連する事件です。ここでは、これらの攻撃内容をより詳細に分析していきます。

■ 攻撃活動の進行

メディア等では、Anonymousは「ハッカー集団」と呼ばれることもあります。しかし、Anonymousは、特定のメンバで構成されるグループではなく、共通の理念への賛同者による非常に緩やかな集合体です。特定のリーダーや中心となる組織は存在しません。では、どのようにして攻撃目標を選定して攻撃活動を進めていくのでしょうか。注目すべき点は、各地域における活動と情報発信です。Anonymousの活動は世界中に広がっています。しかし、全体として統制されているわけではなく、各地域に分散した活動がそれぞれ独自に同時に並行して動いています。例えば、ある地域でインターネット検閲に関する問題が持ち上がると、その地域の人々が反対活動を開始し、インターネット上に情報を発信します。その動きに合わせてその地域のAnonymousが攻撃目標の選定、攻撃方法、攻撃日時等の内容を決め、賛同者への支援を求めます^{*57}。この呼び掛けに世界中のAnonymousが呼応してDDoS攻撃に参加するといった流れになります。一方、LulzSecは、少数のメンバーから構成されるチームであり、Anonymousとは活動方法がまったく異なっています^{*58}。

*52 Sony関連企業へのこれまでの攻撃状況をまとめたサイトがある。Absolute Sownage (http://attribution.org/security/rants/sony_aka_sownage.html)。

*53 LulzSecによる#AntiSecに関する発表 (<http://pastebin.com/9KyA0E5v>)。

*54 "50 Days of Lulz"に関する発表 (<http://pastebin.com/1znEGmHa>)。

*55 標的型攻撃については、IIR Vol.7 「1.4.2 標的型攻撃とOperation Aurora」にて説明している (http://www.ij.ad.jp/development/iir/pdf/iir_vol07.pdf)。

*56 EMC社は6月6日付け顧客向けレターにおいて、Lockheed Martin社への攻撃について言及している (<http://japan.rsa.com/node.aspx?id=3874>)。

*57 Anonymousの攻撃活動をいくつか観測したところでは、攻撃内容は話し合いで決めたり、投票を行って決めていくというわけではなく、突然途中で方針を変更することもある。

*58 LulzSec自身がTwitter等で発表した内容によると、6人のコアメンバーから構成されている。

■ 攻撃目標の選定

攻撃目標の選び方には2つの特徴が見られます。1番目の特徴は無差別攻撃です。特別な理由がないか、後から理由をこじつけて、いきなり攻撃を開始します。例えば、Google等の検索エンジンを利用して脆弱性のあるサイトを見つけて攻撃し、内部情報を不正に取得すると、それを公開する行為が行われます。LulzSecが活動期間の終盤に実施した、電話リクエストで攻撃先を募集するDDoS攻撃等も、無差別攻撃の典型例と言えます。LulzSecは、Anonymousと同じように政治的な目的等に関わる攻撃を行う一方で、単に楽しいから(“for the lulz”と表現しています)というだけの理由でも攻撃を行いました。防御側からすれば、こうした攻撃は非常に予測しづらく、不意を突かれるものになります。

2番目の特徴は、特定の攻撃目標に固執した攻撃です。先ほど示したように、世界中のSony社関連企業に対して20件以上の攻撃が発生していますが、これらは、全体として統制された活動ではありません^{*59}。また、それと同時に、同じゲーム業界にも攻撃が派生し、複数のゲーム関連会社が情報漏洩等の被害に遭いました。これらの攻撃は、AnonymousによるSonyに対するDDoS攻撃に端を発し、便乗した人々により複数の企業に波及した一連の攻撃と考えることができます。これらは日本やアメリカの掲示板サイト等に見られる「祭り」の行動によく似ています。このような攻撃の矛先はどの組織にも向けられるものと考えられます。

■ 攻撃の動機

攻撃の動機が分かりにくいことも注目すべき点です。米国の金融機関Citigroupから36万人分のクレジットカード情報が漏洩した事件では、漏洩したカード情報の一部が実際に悪用され、約270万ドルが不正利用されています^{*60}。このような攻撃は、金銭を目的としたサイバー犯罪であることが明らかです。また、インドとパキスタン、中国とベトナム等、領土問題に関する火種を抱える2国間で、互いに相手国の多数のWebサイトを攻撃し、改ざんするといったものも多く発生してい

ます。過去には日本でも周辺諸国との間で同じようなトラブルが発生したことがあります。これは、国家間の争いをそのままインターネット上に持ち込んだもので、攻撃の動機としては分かりやすいと言えます。

Anonymous等による今回の一連の攻撃は、これらの事件と比較すると明らかに様相の異なるケースが多数見られました。具体的には、ある組織の内部情報を不正に取得しているが、それを悪用することが目的ではないケースです。実際、入手した情報を直接悪用せず、単に「取得した」という事実とその内容をインターネット上に公開するという行為が複数行われました。例えばLulzSecは不正に取得した多数の情報を公開しましたが、彼ら自身はほとんどその情報を悪用していないとされています。また、その後のAntiSecの攻撃においても、不正に取得された内部情報がmediafire等のファイル共有サイトやBitTorrent^{*61}、Pastebin^{*62}等を利用して公開されましたが、攻撃者自身がこれらの情報を悪用したケースはほとんど見られません。

しかし、攻撃者自身が悪用していないとは言え、情報が公開されてしまうと、当然それを悪用する二次的な動きが起こります。仮に悪用されなかったとしても、攻撃を受けた側は、情報が漏洩したことに対するユーザーへの説明や、パスワードリセット等の対応が必要になります。また、情報が漏洩したという事実だけでも、組織のブランドイメージや株価への悪影響は避けられません。今回の一連の攻撃の動機が他の事件と異なっていると云っても、現実の被害を受けるという点では変わりはありません。

これまでAnonymousは、検閲等といったインターネット上の自由な活動を阻害する行為に対して強く反発し、DDoS攻撃を行ってきました。しかし、LulzSecやAntiSecの活動においては、このような目的からやや逸脱し、DDoSや不正侵入等の手段自体が目的化している傾向が見られます。この傾向が一時的なものなのか、今後の活動範囲を拡大する動きなのかは不明です。

*59 20件以上の攻撃の内、Idahcというレバノン人ハッカーとLulzSecがそれぞれ4件ずつに関わったことを表明しているが、他の攻撃については行為者が誰か分かっていない事件が多く、AnonymousやLulzSecとの関連性も不明である。

*60 "Updated Information on Recent Compromise to Citi Account Online For Our Customers" (<http://www.citigroup.com/citi/press/2011/110610c.htm>)。

*61 P2Pネットワークによりファイルの転送(共有)を行うプロトコル及びそのソフトウェア。

*62 匿名でWebページを作成できるサイト (<http://pastebin.com/>)。他にPastie (<http://pastie.org/>)やPastHTML (<http://pastehtml.com/>) 等類似サイトが多数ある。

■ 攻撃活動の公開

AnonymousやLulzSecの活動において非常に特徴的な点は、彼らが攻撃活動の大半を公開していることです。Anonymousの攻撃活動は、IRCのチャンネル単位で行われています。しかも、これらはほとんどオープンであり、誰でも参加することができます*63。また、TwitterやFacebook等のSNS、Blogを通じた情報発信にも積極的です。LulzSecは、IRCを通じて外部とのコミュニケーションを図ったり、メディア向けのチャンネルを特別に用意したりもしていました。こうした公開活動を通じて世間の注目を集めることは、活動への賛同者を得やすくするだけでなく、自分達の行動に何らやましい点がないことをアピールするための根拠にもなっています。

■ 攻撃ツール

Anonymousの攻撃手法は、他の攻撃者と比較しても特別な独自性はありません。中には高度な攻撃技術を持つ者もいますが、大半の参加者はそうではありません。このため、彼らはDDoS攻撃を行う専用ツールとしてLOIC (Low Orbit Ion Cannon) を開発し配布しています*64。TCP、UDP、HTTPの3つのプロトコルから1つを選択し、攻撃目標の情報を入力することで、大量の packets や接続が攻撃先に送信されます。技術力のない参加者でも簡単に使えるツールです。また、手動で攻撃するモードに加えて、IRCモードと呼ばれる機能も用意されています。このモードでは、IRCサーバとチャンネル名を入力して接続するだけで、その後はIRCサーバから送られてくるコマンドに従って遠隔操作で攻撃が行われます。これは、BotnetがC&Cサーバからの指令で操作されるときと似ています。LOICのIRCモードでは、参加者が自主的にBotnetに加わることになります。

しかし、LOICには、送信元アドレスを詐称する機能はありません。これは、AnonymousがDDoS攻撃を正当な抗議行動の手段であると主張している点に関係しています。しかし、彼らがいくらそのように主張しても、いくつかの国では、大量の packets を送信したり接続を発生させたりしてサービスを妨害することは違法行為になります。このため、DDoS攻撃の参加者の中から

しばしば逮捕者が出ており、未成年者が逮捕されるケースも多く見られます*65。

実際のAnonymousによるDDoS攻撃では、LOICだけが使われているわけではなく、他のBotnetも攻撃に利用されています。5月にイギリスで逮捕されたAnonymousへのインタビュー記事では、Sony社に対するDDoS攻撃において、逮捕者自らが制御するBotnetを使用したと答えています*66。また、IJJのマルウェア活動観測プロジェクトMITFの観測データでは、Sony社やブラジル政府系サイト等への複数のDDoS攻撃におけるbackscatterデータが観測されています。backscatterは送信元アドレスを詐称した攻撃が行われた際に観測されるものです。したがって、これらの攻撃においては、LOICだけでなくアドレス詐称機能を持つ別の攻撃ツールが使用されたこととなります。

■ 対応

では、防御する側の立場にいる者は、今後どのような対策を行えばよいのでしょうか。ここまでの分析を元に、攻撃を受ける可能性を次の3段階に分けて対応を考えてみます。

1. 攻撃目標とはなっていないが無差別に攻撃を受ける可能性がある状態
2. 特定の攻撃活動において攻撃目標の範囲に入っている状態
3. すでに攻撃の目標となっている、もしくは攻撃を受けている状態

まず、1番目の可能性についてですが、インターネットに接続しているかぎり、無差別な攻撃の被害に遭う可能性は常にあります。したがって、いつ攻撃を受けても対応できるようセキュリティ対策を進め、攻撃に備えておくようにします。これは、外部公開しているサーバやWebアプリケーションの脆弱性対策を行ったたり、ファイアウォールやIPS等の装置で境界を設定したり、アンチウイルスソフトウェアでマルウェア対策を実施するなど、従来のセキュリティ対策を実施するこ

*63 Anonymousが運営しているIRCサーバは複数ある。例えばirc.anonops.li等。

*64 LOICは一般に公開されており、誰でも入手できる。

*65 6月にはスペインで3人の逮捕者がでていた。スペイン警察当局による発表 (http://www.policia.es/prensa/20110610_2.html)。

*66 "The fighting continues as AnonOps stages a comeback" (<http://www.thetechherald.com/article.php/201119/7163/The-fighting-continues-as-AnonOps-stages-a-comeback>)。

とで実現します。また、Anonymousのように攻撃活動を公開している攻撃者はむしろ稀であり、大半の攻撃活動は予告もなく行われます。このような場合に攻撃活動を事前に予測することは難しいため、無差別攻撃と同様に備えるしかありません。攻撃が発生した事実を早期に把握し、攻撃内容と被害の状況に応じて適切な対応をとれる準備を行う必要があります。

2番目の状態での対応は非常に重要です。自組織にも攻撃が及ぶことを事前に把握して適切に対応すれば、被害を軽減したり、未然に防いだりできる可能性があるためです。特定の組織が攻撃活動の目標となる理由は様々です。自組織の活動そのものが問題となる場合や、同じ業種の別の企業への攻撃が波及してくる場合、日系企業である等の組織の属性が問題となる場合があります。このため、ニュースやSNS等の一般に公開されている情報から、同業他社への攻撃情報や、自社の業務に関わる評判の情報等に注意することが有効です。また、本稿で紹介した攻撃事例を見ると、Anonymousが攻撃手段としてDDoS攻撃を多用する一方、LulzSecやその後のAntiSecの活動では、SQLインジェクション攻撃等の不正侵入によって情報漏洩が発生する例の多いことがわかります。このように、過去及び現在進行中の攻撃事例を分析することで、攻撃者とその攻撃手段の傾向を把握でき、次の攻撃を予測し、対策につなげることができます。自組織がこれらの攻撃の目標となる可能性をできるだけ早く把握し、サーバの設定の見直しやソフトウェアのバージョン確認等を行うことで、攻撃を受けたときに実際の被害を生まない可能性を高めることができます*67。

以上に加えて、自組織への攻撃が予測される状況では、攻撃の発生を素早く検知して即応できるようにするための体制を、より強化することが必要になります。

最後に3番目の状態である、既に攻撃の目標となることが分かっている、もしくはすでに攻撃を受けている状態です。攻撃の目標となることが分かった場合には、攻撃者についての情報、特にその背景や攻撃の意図、過去に引き起こした攻撃の種類を知ることが必要となります。攻撃の原因となる背景は、組織の活動その

ものを問題視する場合や、組織の経営層による不用意な発言等多岐にわたりますが、原因がはっきりしているのであればその点を修正することで、攻撃を発生させなくすることができる場合があります。

また、攻撃者の意図を理解することで、攻撃が単発の攻撃で終るのか、目的を達成するまでしつこく継続するか、攻撃の種類や内容、将来攻撃に変化が起こるか等のある程度予測することができます。例えば、本稿で紹介した一連のSQLインジェクションによる攻撃では、特に最近では情報漏洩に至らず、SQLインジェクションの脆弱性を確認し、その事実を公開することにとどまっている場合があります。これは攻撃者が、情報を奪うために攻撃を行うのではなく、脆弱性の存在を公開し組織の評判を落とすことを目的としているためと考えられます。

すでに攻撃を受けている場合には、まず攻撃の影響を正確に把握することが重要です。サービス停止により被害をこうむった顧客がいるのか、情報漏洩が発生したかどうか、漏洩した情報はどのような内容でどの程度の規模なのか等を把握し、発生した被害の影響評価に基づく対応を行うことが必要です。攻撃が継続している状態であれば、攻撃を阻止する対応を行います。例えばDDoS攻撃では数時間から数日間にわたって攻撃が継続する例もあります。自組織だけで防ぐことが難しい場合には通信事業者等の外部組織との連携が必要になりますが、そのためには日頃から協力関係を構築しておくことが不可欠となります。

また事後対応としては、被害の復旧、再発防止策の検討等に加えて、適切な情報開示が欠かせません。特に顧客等の他者が影響を受ける場合には、起きた事象について正確かつ迅速な情報開示が求められ、事件に対する企業や組織としての姿勢を示す活動が必要となります。

最近の攻撃傾向から、企業や政府等への攻撃が頻繁に発生する状況が今後もしばらく続くと考えられます。ここで示したように、自らが攻撃目標となる可能性を常に想定し、攻撃者に関する情報を的確に把握して備えておくことが、防御する側にとってより重要なこととなります。

*67 例えばSony社への攻撃の事例では、攻撃がSony社のグループ企業やゲーム業界に波及する可能性が事前に予測できた。

1.4.2 電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン(第2版)

本稿の前節で示したように、昨今では企業や国の関係組織に対する攻撃が増加しています。攻撃への対処は、その攻撃内容によって様々ですが、特に大量の通信をとまなうDDoS攻撃においては、被害者となった組織だけでは対策できず、IJのようなISPを含む電気通信事業者が何らかの形で介入することで、適切な対処となる場合も考えられます。一方で、通信事業者による通信の遮断等の対処は、ともすれば通信主体の様々な権利を侵害することにもなりかねません。そこで、電気通信事業者がどのような状況で攻撃の通信に対してどのような対策を実施できるかについて、電気通信事業法等に定められる通信の秘密の保護との関係で整理し、事例を提示したガイドライン^{*68}が2011年3月25日に公開されました。

このガイドラインでは、攻撃により発生すると考えられる複数の種類の通信への対処について議論していますが、特にDDoS攻撃対応に関しては現時点で国内唯一のガイドラインとなっています。ここでは、このガイドラインの内容について、ISPにおけるDDoS攻撃への対策を中心に解説します。

■ ガイドライン策定の経緯

このガイドラインは、様々な場におけるISPにおける攻撃への対処の検討の結果を反映したものです。これは、2005年に日本国内の複数のWebサーバに対して発生した同時多発的なDDoS攻撃への対処の経験から、当時問題となっていた大量通信をとまなう様々な攻撃に対する対処について、Telecom-ISAC Japan^{*69}等のメンバである複数の国内ISPで重ねた検討を基にしています。当初は事例集として公開することを目的に整理していましたが、2006年より通信関連団体を中心としてガイドライン化作業を開始しました。その結果、現在の形態である、設問とその解釈、事例の順に表記したガイドラインとして2007年5月30日第一版^{*70}が策定されました。その後、大規模化するインターネット上の

攻撃や、いくつかの新しい攻撃事例に対応するために、2010年4月に改訂作業^{*71}を行い、本年3月に一般公開に至りました。

■ ガイドラインの概要と位置づけ

以上の経緯を経て策定されたこのガイドラインは、DoS攻撃、DDoS等のサイバー攻撃、マルウェアの感染拡大、迷惑メールの大量送信及び壊れたパケット等を対象としており、これらの大量通信への電気通信事業者による対処について、それぞれ通信の秘密の侵害にあたるかどうかを検討したものです。様々な大量通信の状況について、特に対処の違法性が阻却される状況の考え方と事例を示しています。このため、例えば有害情報への対策やフィッシング対策等、明白な大量通信をとまなない攻撃への対処や、いわゆる利用の公平性、個人情報保護、契約解除等のその他法的問題についてはこのガイドラインの対象ではなく、別途検討を行う必要があるとしています。

また、このガイドラインは民間の事業者団体が自主的に策定したガイドライン(自主基準)であるため、このガイドラインに従った対処を実施したことによりまったく責任が発生しなくなる、といった性質のものではありません。さらに、大量通信かどうかの判断は、事業者の回線規模や状況、攻撃手法等により異なり、汎用の定量的な判断基準をもうけることが困難なため、実際の攻撃事例への対処においては、このガイドラインの適用事例となるかどうかを個別に判断した上で対処を実施すべきである、とされています(以上第2条総論)。同時に、インターネットの状況やその上の攻撃は、時々刻々と変化することから、このガイドライン自体も永続的に利用できるものではなく、状況を踏まえて適宜見直しをされるべきものと記載されています(第5条)。

■ 攻撃による通信への対処と通信の秘密の整理

利用者がDDoS攻撃にさらされていることが自明な時に、その攻撃内容を調査し、攻撃の通信を遮断し、攻撃

*68 ガイドライン第2版の全文は次より入手することができる。「インターネットの安定的な運用に関する協議会」(<http://www.jaipa.or.jp/other/mfcs/index.html>)。次は、協議会メンバーである社団法人日本インターネットプロバイダー協会(JAIPA)によるガイドライン公開に関するプレスリリース「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドラインの改定について」(http://www.jaipa.or.jp/other/mfcs/info_110325.html)。

*69 財団法人データ通信協会 テレコム・アイザック推進会議(<https://www.telecom-isac.jp/>)。Telecom-ISAC Japan は通称。

*70 次はJAIPAによる第1版策定に関するプレスリリース(http://www.jaipa.or.jp/info/2007/info_070530.html)。この第1版は、文章の位置づけと総論を示す序文のみ一般公開し、内容については電気通信事業者のみ(参加4団体の会員企業内での)公開ということになった。

*71 第2版の検討のためのインターネットの安定的な運用に関する協議会には、第1版の協議会メンバーに加え、財団法人データ通信協会 テレコム・アイザック推進会議が参加している。

元を収容するISPに対策を依頼した場合、これらの行為をISPが自主的に実施した場合は、すべて通信の秘密の侵害行為(知得、窃用、漏洩のいずれか)に該当し、違法行為となります。しかし、現実にはこれらの行為もしくはその一部を実施しないと、攻撃の影響を減らすことはできません。では、どのような条件であれば、違法行為とならないように対処を実施することができるのでしょうか。本ガイドラインでは第2条から第4条において、その考え方を整理して示しています。

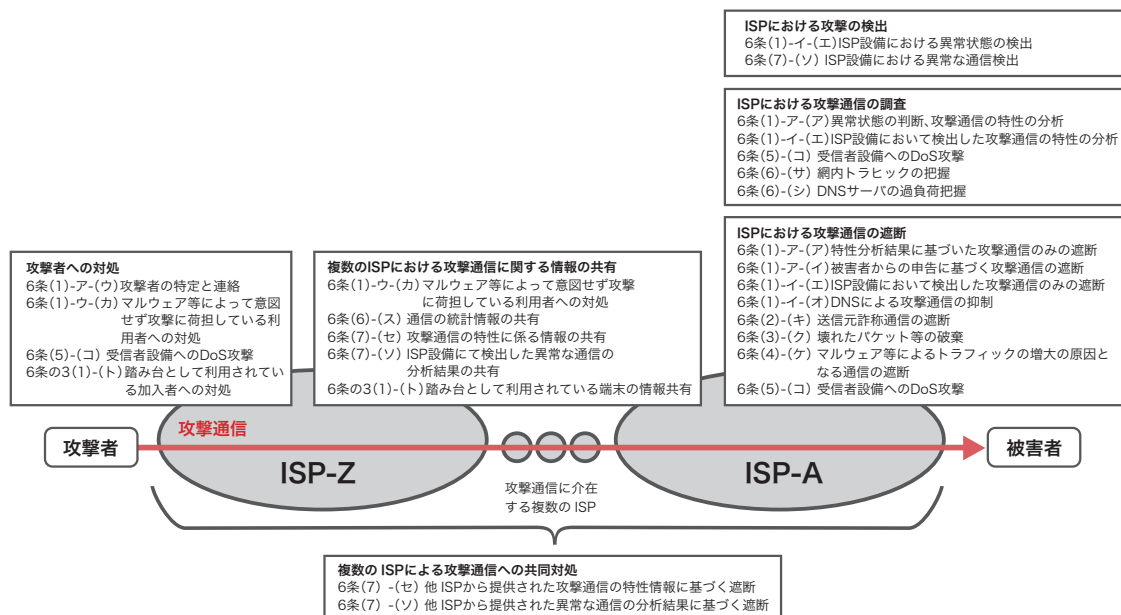
まず、通信に関する操作(知得も含む)がすべて通信の秘密の侵害であるとした上で、その違法性が阻却される場合として、通信当事者の同意がある場合、ISP自身が通信当事者である場合、法令行為、正当業務行為、正当防衛、緊急避難^{*72}に相当する場合があるとしています。

ここでは、正当業務行為に相当する場合について説明します。電気通信事業者の正当業務行為とは、電気通信事業の維持・継続に必要な行為とされています。攻撃への対処として通信に対する操作が、目的が正当であるかどうか、行為が必要であるかどうか、その手段が相当かどうか、この3つの要件を満たすときのみ、正当業務行為として違法性が阻却されるというものです。例えば、

インターネットを構成するルータは、IPパケットのヘッダを参照し、経路情報と付き合わせてパケットの転送先を決定する装置ですが、ヘッダを参照する行為は通信の秘密を侵害しています。しかし、この行為は、通信を成立させる目的で、この行為を行わないと通信が成立せず、IPパケットの転送先を見つけるためにはヘッダの参照以外の方法がないということから、電気通信事業における正当業務行為と判断することができます。また、ネットワークの安定的運用のために必要な措置の例として、大量通信等によるネットワークに対する攻撃への対処や、いわゆるOP25B・IP25Bによる迷惑メール対策、帯域制御等もこれにあたるとしています。

■ガイドラインに記載された事例

第2章各論において、個別の状況下での、対処と通信の秘密に関する議論を行っています。実際には様々な攻撃について検討を行っていますが、ここでは、DDoS攻撃への対策を例にとりガイドライン上の記載事項を紹介いたします。まず、ガイドライン中のDDoS攻撃対策への言及を、攻撃の検出、攻撃の調査、攻撃の遮断、情報共有、攻撃者への対処、共同対処といったDDoS対策の各段階別にまとめたものを図-12に示します。ガイドラインでは、特定の攻撃と対策について、その条件等を順序だて



※この図はガイドライン内において、DDoS攻撃への対応の各段階に関する言及部分を列記したものの、項番に対応する文章は言及内容をまとめたもので、実際の文章での表現とは異なる場合があります。ここに記載された行為は無条件に許容されるものではなく、ガイドライン本文の条件や文脈、例を参考に発生した事案の状況と照らしあわせて可否を個別に判断すべきものである。

図-12 DDoS攻撃対策におけるガイドライン上の対応項目

*72 正当防衛(刑法36条)、緊急避難(刑法37条)。

て検討していますので、実際に適用可能かどうかはガイドライン本文を参照する必要があります。

例えば、6条(1)-ア「被害者からの申告があった場合」の(イ)では、「攻撃に係る通信の特性を把握した上、当該特性を有する通信のみを機械的に遮断することは、通信の秘密の侵害に当たりうる」としながらも、受信者もしくは加入者から個別の同意を得るか、「不正な攻撃通信により全加入者の端末に生じる侵害を防止するために必要な範囲で相当な方法により行われる場合」には違法性が阻却されるとの考え方を示しています。その上で、前者の事例として、利用者から依頼に基づいて、特定のWebサーバのIPアドレスに向かったポート80番の通信遮断を実施する事例を、後者については通信設備に影響を与える恐れのあるIPオプションの付与されたIPパケットの遮断事例を紹介しています。また、「6条(2)-(キ)送信元詐称通信の遮断」では、IPアドレスを詐称された通信の遮断について、「送信元IPアドレスに関する情報を、送信元詐称通信を自動遮断するために利用することは、別途通信の秘密の窃用に当たりうる」としながらも、事業者の設備や利用者の設備に影響が出る場合には、正当防衛又は緊急避難に当たるとの考え方を示しています。事例としてはuRPF^{*73}のloose modeとstrict modeに相当する行為の説明を行っています。

このガイドラインを利用する時には、ここで紹介したような個別の設問の状況だけでなく、例えば、1つのISPの自社網の中に攻撃者と被害者が存在している時等、複数の場合を組み合わせる判断すべき場合もあります。

■ まとめと課題

このガイドラインによって、攻撃の発生状況においてISP等の電気通信事業者が実施して良いことの基準が示されましたが、すべての状況において各事業者がこのガイドラインに記載された対処を実施するものではありません。対処を実施するかどうかは、攻撃の規模や内容、対応のコスト等を加味した上で事業者の判断で決められるものです。個々に記載された項目についても、迅速に、間違いを犯さないように実現するためには、特に被害者からの申告の在り方^{*74}やISP間の連携の在り方について、今後実施方法を検討し詳細な方法について規定する必要があります。これらの課題については、今後Telecom-ISAC Japan等の業界団体での活動を通じて検討していきます。

1.5 おわりに

このレポートは、IJ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、昨年末より連続している複数の企業や各国の政府関係組織に対する攻撃と、そのような攻撃に通信事業者が対処するためのガイドラインについて解説しました。IJでは、このレポートのようにインシデントとその対応について明らかにして公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を続けてまいります。

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 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IJグループの緊急対応チームIJ-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)

土屋 博英 鈴木 博志 永尾 禎啓(1.3 インシデントサーベイ)

根岸 征史(1.4.1 連続する企業や政府関係組織への攻撃)

齋藤 衛(1.4.2 電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン(第2版))

IJサービス本部セキュリティ情報統括室

協力:

加藤 雅彦 須賀 祐治 吉川 弘晃 齋藤 聖悟 鈴木 博志 小林 直 IJサービス本部セキュリティ情報統括室

*73 Unicast Reverse Path Forwarding (uRPF)。RFC3704に定義される、経路上に存在しないIPアドレスからの通信を抑制する手法。

*74 DDoS攻撃を受けた場合のISP等の組織との連携の取り方については、IIR vol.9 (http://www.ij.ad.jp/development/iir/pdf/iir_vol09.pdf)の「1.4.1 小規模システムでのDDoS攻撃への備え」にて、検討している。

迷惑メール送信元地域の割合と実数が中国で急増

今回は、2011年第14～26週での迷惑メールの推移を報告します。

迷惑メール送信元地域の第1位は、前回のレポートと同様に中国でした。

中国が占める割合は、2011年2月以降、急激に増えています。

2.1 はじめに

このレポートでは、迷惑メールの最新動向やメールに関連する技術解説、IJが関わる様々な活動についてまとめています。今回は、日本の多くの企業の第1四半期にあたる2011年第14週(2011年4月4日～4月10日)から第26週(2011年6月27日～7月3日)までの13週間分のデータを調査対象にしています。また、送信ドメイン認証技術の普及状況を把握するために、SPF (Sender Policy Framework) と DKIM (DomainKeys Identified Mail) の認証結果の割合についても報告します。

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、IJ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。前回のレポートでは、迷惑メールの割合が減少傾向にあると報告しましたが、今回の調査結果からも減少傾向が続いていることが分かりました。その要因についても、迷惑メールの送信元の割合から考察します。

2.2.1 迷惑メールの割合は引き続き減少

今回の調査期間と前年の同時期を含む1年3ヵ月分(65週)の迷惑メールの割合の推移を図-1に示します。今回の調査期間での迷惑メールの割合の平均は50.2%でした。前回のレポートから15.2%減少しており、前年の同時期に比べると32.1%と大幅な減少となっています。昨年後半からの迷惑メールの割合の減少が、そのまま続いていることが分かります。この低下は、前回のレポートでも報告したとおり、迷惑メール送信の主要な手段であるボットネットが各国の執行機関やセキュリティ専門家などの努力によって摘発され、その活動を低下させられてきたことが理由です。

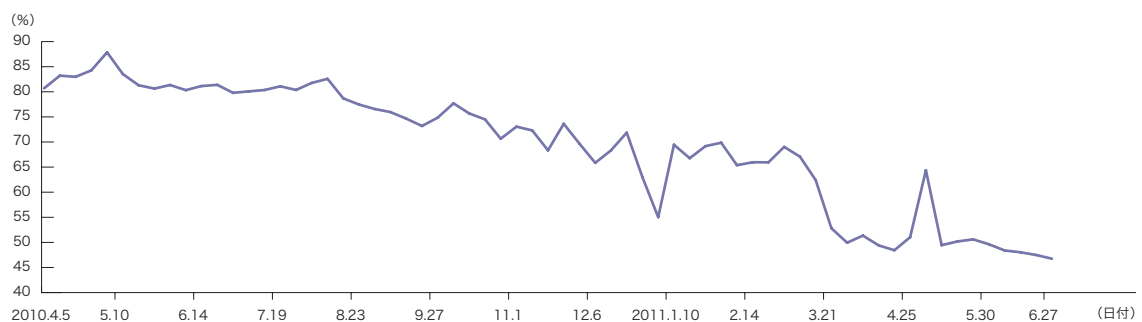


図-1 迷惑メール割合の推移

では、このまま迷惑メールは減少していくのでしょうか。これまで効果を上げてきた対策では、ボットネットの制御元（指令を送信するホストやその管理者）を抑えることによって、迷惑メール送信等の活動を止めるようにしてきました。最近では、セキュリティベンダ Kaspersky Labが新しいタイプのマルウェア（不正プログラム）に関する分析結果を報告しています*1。このTDSSマルウェアとその亜種、特にTDL-4では、制御元からの指令が暗号化されていることに加えて、その伝達手段としてPeer-to-Peerネットワークを利用するなど、多くの改良が行われているようです。このように、PCとインターネットを使って不正行為をする側は絶えず進化しているため、これらの対策がいつまで有効であるかは分かりません。

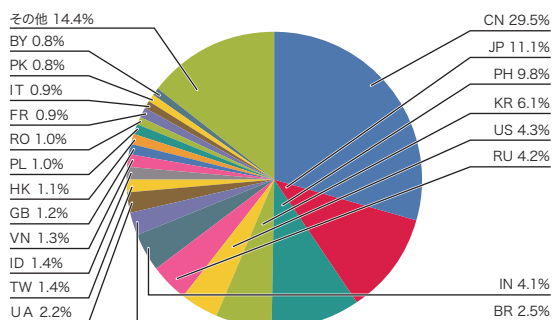


図-2 迷惑メール送信元地域の割合

2.2.2 日本が迷惑メール送信元の第2位に

今回の調査期間での迷惑メール送信元地域の分析結果を図-2に示します。今回の調査では、迷惑メールの送信元地域の1位は前回に引き続き中国（CN）で、迷惑メール全体の29.5%を占めており、実数でも前回の報告より増えています。2位は日本（JP）で11.1%でした。実数は、前回のレポートのものともあまり変化がありませんでしたが、迷惑メールの量自体が減少しているために割合として増えました。3位はフィリピン（PH、9.8%）で、前回の4位から割合も順位も上がっています。4位は韓国（KR、6.1%）、5位は米国（US、4.3%）、6位はロシア（RU、4.2%）という結果でした。

日本の迷惑メールの送信元を詳しく調べてみると、その多くはメールマガジン等のメール配信事業を行っていると思われる送信元が送信していました。契約者の素性を確認したり、届かなかったメールアドレスをきちんと管理して迷惑なメールを送信しないようにしているメール配信事業者がいる一方で、配送しているメールの内容や届け先のメールアドレスにあまり注意を払わないメール配信事業者もいます。こういった事業者の存在が、メール配信事業者全体が悪い印象を持たれてしまうことにもなりかねません。

2.2.3 主要迷惑メール送信元地域の推移

迷惑メール全体の減少とともに、日本が受信する迷惑メール送信元地域の傾向も変わってきているようです。今回の調査で、迷惑メールの送信元の上位6地域について、2011年の推移を図-3に示します。

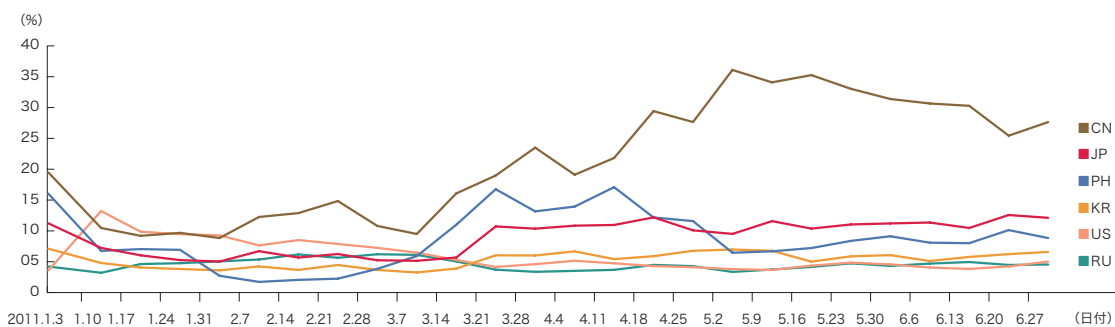


図-3 主要迷惑メール送信元地域の割合の推移

*1 http://www.securelist.com/en/analysis/204792180/TDL4_Top_Bot

この図を見ると、中国 (CN) が今年 (2011年) の2月あたりから急激に割合を増やしていることが分かります。特に5月前半には、全体の3分の1を超える大量の迷惑メールを送信していました。また、日本は5月以降2位が続いていることも分かります。

2.3 メールの技術動向

ここでは、メールに関わる様々な技術的な動向について解説します。今回も送信ドメイン認証技術の受信側での認証結果を分析して報告します。

今回の調査期間 (2011年4～6月) に受信したメールのSPFによる認証結果の割合を図-4に示します。送信側のドメインがSPFレコードを宣言していないことを示す認証結果「none」の割合は46.5%で、前回から3.7%減少しました。これは、メールの流量ベースで、導入割合が3.7%増加したことを意味しています。認証結果「pass」の割合も35.4%と前回から6.8%増えましたので、SPFを宣言している正規のメール送信者からのメー

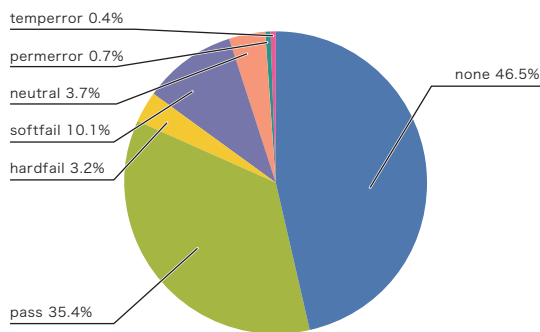


図-4 SPFによる認証結果の割合

ルが増えてきていることを示しています。

同様に、もう1つの主要な送信ドメイン認証技術であるDKIMの認証結果の割合を図-5に示します。DKIMを導入していないことを示す認証結果「none」の割合が95.9%でしたので、残念ながらDKIMの送信側への導入はまだまだ進んでいないようです。

2.4 おわりに

IJが2004年の創設時から関わっているMAAWG (Messaging Anti-Abuse Working Group) の22回目のGeneral Meetingに、6月に出席しました。MAAWGは、迷惑メール対策に関連した様々な内容をグローバルの関係者間で議論する集まりです。しかし、会場の開催場所の関係もあり、残念ながら日本からの参加者はあまり多くありません。また、日本だけでなくアジア地域からの参加者も少なく、どうしても議論が欧米主体となってしまうがちです。そのため筆者は、なるべく日本とアジアの状況について、関係者と意見交換を行うよう努めています。次回は、10月にフランスのパリで23回目の会合が行われる予定です。

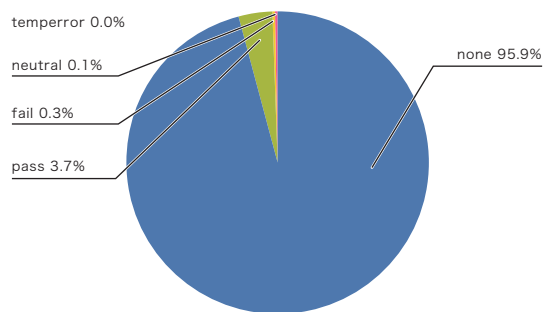


図-5 DKIMによる認証結果の割合

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。総務省 迷惑メールへの対応の在り方に関する検討WG 構成員。

3. ブロードバンドトラフィックレポート

マクロレベルな視点で見た、震災によるトラフィックへの影響

2011年3月に発生した東日本大震災では通信インフラも大きな被害を受けました。しかし、マクロレベルな視点で見ると、震災によるトラフィックへの影響は限定的なものでしかありませんでした。ここでは、東日本大震災によるトラフィックへの影響を報告した後、2011年5月30日から1週間のトラフィック量やポート使用量を用いて2010年からのトラフィックの変化を探っていきます。

3.1 はじめに

本レポートでは、IJJ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て、その結果を報告します。昨年、IIR Vol.8で、以前からあったP2Pファイル共有からWebサービスへの移行の流れが改正著作権法、いわゆるダウンロード違法化を契機にヘビーユーザにも浸透してきたと報告しました。本レポートでは、まず、ブロードバンドトラフィックへの東日本大震災の影響について報告します。その後、これまでと同様に利用者の1日のトラフィック量やポート別使用量等を元に、この1年間のトラフィックの変化を報告します。

3.2 震災の影響について

2011年3月11日に発生した東日本大震災では、回線の切断、設備と機器の損壊等、通信インフラも大きな被害を受けました。しかし、国内インターネット全体への影響は限定的なものでした。震災直後に固定電話や携帯電話が繋がらなくなったため、インターネットが情報交換に大きな役割を果たしました。

今回のレポートでは、まず、震災によるブロードバンドトラフィックへの影響を見ていきます。図-1に、IJJが

運用するブロードバンド接続サービスでの宮城県と全国における2011年3月1ヵ月間のトラフィックを示します。ここでは、Y軸のトラフィック量が絶対値で開示できないため、ピーク値を1として正規化しています。

東北地方でのIJJの拠点である仙台データセンターの設備に被害はありませんでしたが、東京と仙台の間を結ぶ冗長構成のバックボーン回線がともに切断されました。しかし、翌日3月12日午前中にはバックボーン回線は復旧しました。この時点では、宮城県内のほとんどの地域が停電中で、仙台データセンターは自家発電で運用を行っていましたが、トラフィックはほとんどありませんでした。その後の電気と回線の復旧に伴い徐々にトラフィックが回復していき、震災発生後10日ほどで以前の85%くらいまで回復し、その後は横ばい状態になりました。東北電力からの送電、NTT東日本の通信サービスも、震災発生後10日ほどで90%近くまで急速に回復し、一部を除いた地域は、4月末くらいまでに回復しています。

全国レベルのトラフィックを見ると、震災発生直後に20%くらい減少しています。夜間には少し戻りますが、震災当日は停電に加えて首都圏で多くの人々が帰宅難民となり、トラフィックもその影響を受けました。しかし、翌日の土曜日は、前週の土曜日の85%くらいま

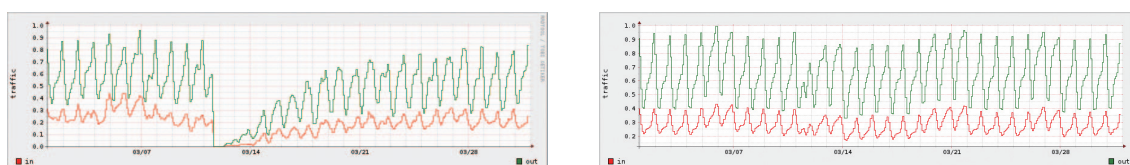


図-1 2011年3月でのブロードバンドトラフィック (左側:宮城県、右側:全国)

で回復しています。その後の1週間ほどは計画停電の影響もあって数%減となりますが、以降はほぼ元のトラフィック量に回復しています。このような状況は、IIJのブロードバンド接続サービスに限ったものではなく、他ISPも同様の状況であったと聞いています。

図-2に、過去4年間でブロードバンド全体の月平均トラフィックを示します。ここからも、震災の影響が限定的なものであったことがわかります。昨年報告した^{*1}、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ときに比べて、その影響が小さかったと言えます。また、2010年1月以降、OUT(ダウンロード)が増える一方でIN(アップロード)は横ばいであり、ファイル共有の利用が減っていることがうかがえます。ただし、トラフィックに対する影響がどの程度あるのかは不明ですが、障害に強いP2Pの特性を利用して震災情報を共有するユーザが増えたという話もあります。

トラフィックへの影響が限定的であった理由はいくつか考えられます。まず、地震と津波によって壊滅的な被害を受けた地域に主要設備がなかったため、基幹サービスへの影響が小さくて済んだことです。これは、あくまでマクロレベルな視点で見たときの影響です。震災発生から4ヵ月経つ本稿執筆時点でも、まだサービスを復旧ができていない被災地が数多く存在しています。また、3月11日以降も、度重なる余震によって回線断が多発しましたが、現場の迅速な復旧作業のおかげで、

大きな障害には至りませんでした。今回の震災の影響がこの程度でおさまっているのは、復旧に尽力された多くの方々のおかげです。

また、震災後の電力不足と節電によるトラフィックへの影響もあまり見られません。当初、電力不足が問題になると考えられた地域は、東北電力及び東京電力管内に限られていました。とはいえ、これらの地域におけるブロードバンドトラフィック量の合計は全体の半分以上を占めています。しかし、実際には、節電によって利用が減った分を、情報収集等のためにインターネット利用が増えた分で相殺しているように見えます。そもそも、節電の為にインターネットの利用を控えた利用者は少ないと思われる。企業等では、社内のサーバやPCをできるかぎり停止する等の措置が取られました。しかし、そのような場合にも、社内トラフィックは大きく減ったとしても、我々通信事業者から見える組織間トラフィックは相手先との調整が必要なため削減が難しいと考えられます。さらに、震災と計画停電の実施により、社内や家庭内のサーバをクラウドに移行したり、遠隔地へバックアップしたりする傾向が加速し、それがトラフィックの押し上げ要因となっている可能性もあります。

このようにマクロレベルな視点で見ると、震災によってトラフィックが大きく変わったようには見えません。次節以降では、2010年5月末からのデータを使い、より詳細なトラフィック傾向の変化を分析します。

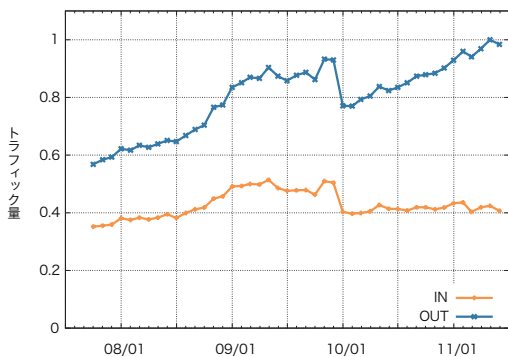


図-2 過去4年間のブロードバンドトラフィック量の推移 (2011年5月のOUT値を1として正規化)

*1 「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」(長健二郎著、Internet Infrastructure Review Vol.8 25 ~ 30ページ) http://www.iiij.ad.jp/development/iir/pdf/iir_vol08_report.pdf

3.3 データについて

今回のレポートも、前回までと同様に個人及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の利用者を収容しているルータから、Sampled NetFlowによって収集したデータを利用しています。ブロードバンドトラフィックは平日と休日でその傾向が異なるため、1週間分のデータを解析の対象にしています。今回は、2011年5月30日から6月5日までの1週間分のデータを、前回解析した2010年5月24日から30日の1週間分のデータと比較します。

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を考慮して1/8192に設定しました。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することで、使用量の少ない利用者のデータには誤差が生じる恐れがありますが、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が得られます。

なお、ここ数年、DSLからファイバーへの移行が進み、2011年に観測したユーザ数の88%がファイバー利用者であり、トラフィック量全体の93%を占めるまでになっています。また、本レポート内でのトラフィックのIN/OUTは、ISP側から見た方向を表しています。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。

3.4 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-3に、利用者の1日の平均使用量の分布(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、図-3の左側では2010年と2011年を、右側では2005年と2011年をそれぞれ比較しています。X軸は対数表示で、その範囲は 10^4 (10KB) から 10^{11} (100GB) です。最も使用量が多い利用者のトラフィックは1.2TB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} (100G) までの範囲に分布しています。なお、グラフ左側に現れている突起は、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、線形グラフにおいて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1桁ほど大きくなっています。

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がきます。実際にはOUT(ダウンロード)の分布にも、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

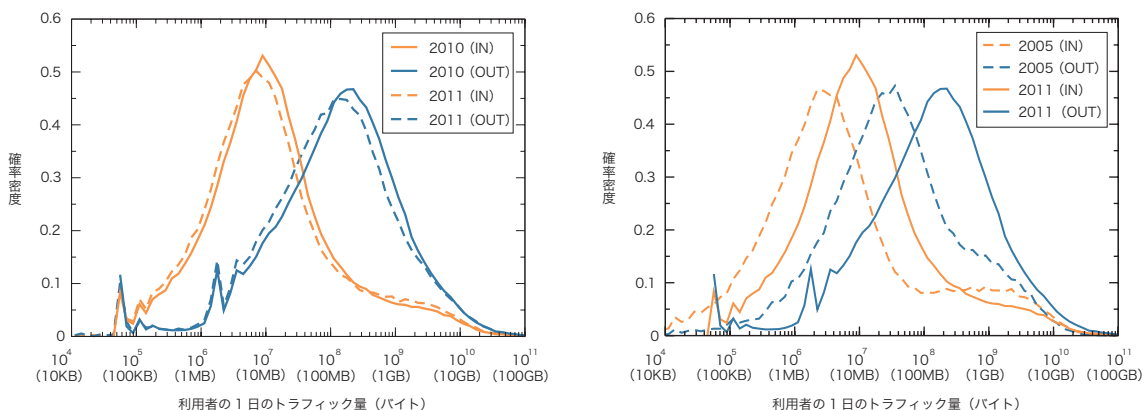


図-3 利用者の1日のトラフィック量分布(左側: 2010年と2011年の比較、右側: 2005年と2011年の比較)

の分布は、INとOUTでほぼ同じ位置にあり、IN/OUTのトラフィック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。

表-1に、トラフィック量の平均値と、分布の頂点である最頻出値の推移を示します。平均値はグラフ右側に存在するヘビーユーザの使用量の影響を受けるので、2011年の平均値はIN(アップロード)が432MB、OUT(ダウンロード)が1,001MBでした。2010年では、それぞれ469MBと910MBでしたので、INが減少しOUTが増えています。

クライアント型利用者での分布の最頻出値を2010年と2011年で比較すると、IN(アップロード)で7MBから8.5MB、OUT(ダウンロード)で145MBから223MBにそれぞれ増え、特にダウンロード量が増えていることが分かります。

2005年と2011年を比較している図-3の右側に注目すると、一般利用者の使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使用量が横ばいであり、その割合が減ってきていることが分かります。

図-4では、ランダムに抽出した利用者5,000人のIN/OUT使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)を採り、両対数グラフで表しています。IN/OUTのトラフィック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。

年	IN (MB/day)		OUT (MB/day)	
	平均値	最頻出値	平均値	最頻出値
2005	430	3.5	447	32
2007	433	4	712	66
2008	483	5	797	94
2009	556	6	971	114
2010	469	7	910	145
2011	432	8.5	1,001	223

表-1 利用者の1日のトラフィック量の平均値と最頻出値の推移

ここでは、2つのクラスタが見られます。対角線の下側にあり、対角線に沿って広がるクラスタは、OUT(ダウンロード)量がIN(アップロード)量よりも1桁多いクライアント型利用者です。一方、右上の対角線上あたりを中心に薄く広がるクラスタは、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もSkype等のピア型アプリケーションを利用し、ピア型利用者もWeb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ます。また、各利用者の使用量やIN/OUT比率のばらつきも大きく、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、2010年と比較しても、ほとんど違いがありません。

3.5 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が困難です。P2P系アプリケーションでは、双方で動的ポートを使うものが多い一方で、クライアント・サーバ型アプリケーションの多くでは、ファイアウォールを回避するためにHTTPで使われる80番ポートが利用されています。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。

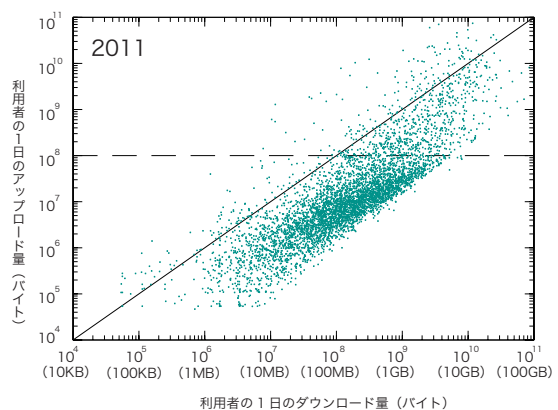


図-4 利用者ごとのIN/OUT使用量

また、トラフィックの全量では、利用量の多いピア型利用者のトラフィックの影響が大きくなります。このため、クライアント型利用者の動向を見るために、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-3でIN(アップロード)の2つの分布の中間にあたり、図-4でIN=10⁸(100MB)である水平線の下側の利用者になります。

図-5は、ポート別使用状況を、全体とクライアント型利用者に分け、2010年と2011年で比較したものです。また、表-2に、その詳細を数値で示します。

2011年では、トラフィック量の86%がTCPです。しかし、全体のトラフィックでは、2010年に総量の64%だった1024番以上のTCPの動的ポートの割合が、2011年は50%まで減少しています。動的ポートでの各ポート番号が占める個々の割合はわずかで、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、2010年の23%から32%に増加しています。

クライアント型利用者に注目してみると、2010年に75%を占めていた80番ポートの割合が、2011年は67%に減少しています。2番目に大きな割合を占める554番ポートは、2009年以前に7%程度ありましたが、2010年に2%まで減った後7%に回復しています。このポートは、RTSP(Real-Time Streaming Protocol)で使われ、ビデオコンテンツの増加に関連しています。また、動的ポートの割合は15%から11%に減少しています。

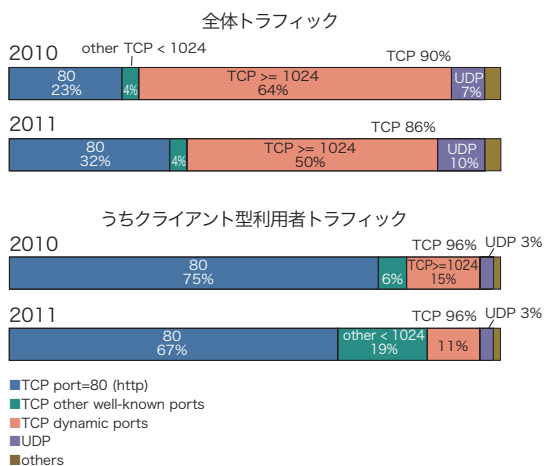


図-5 ポート別使用状況

これらのことから、昨年報告したTCP80番ポートのトラフィックの増加が一般利用者に加えてヘビーユーザにも広がっているという傾向が、いまだに続いていることが確認できます。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等も含まれるため、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ことは確かです。

図-6は、全トラフィックでのTCPポート利用状況の週間推移を示しています。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、トラフィック量は、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。全トラフィックでは、依然として動的ポートの割合が大きく、そのピークが23:00~1:00にあります。土日には昼間のトラフィックも増加し、家庭での利用時間が反映されています。しかし、2010年と2011年のデータを比較してみると、2011年では80番ポートの割合が増え、動的ポートの割合に肩を並べるほどになっています。

protocol	port	2010		2011	
		total (%)	client type	total (%)	client type
TCP	*	90.09	95.82	85.95	96.28
	(<1024)	26.46	80.87	36.24	85.69
	80 (http)	23.00	75.12	32.10	67.30
	443 (https)	0.98	2.28	1.33	1.91
	554 (rtsp)	1.15	2.45	1.33	6.89
	22 (ssh)	0.14	0.10	0.27	0.17
	(>=1024)	63.63	14.95	49.71	10.59
	1935 (rtmp)	1.04	2.91	1.58	1.51
	6346 (gnutella)	0.86	0.33	0.68	0.60
	6699 (winmx)	0.65	0.17	0.40	0.24
	7144 (peerlist)	0.34	0.04	0.38	0.00
UDP		6.79	2.76	10.01	2.61
ESP		2.91	1.30	3.56	1.02
GRE		0.14	0.06	0.15	0.05
L2TP		0.00	0.00	0.13	0.00
ICMP		0.02	0.04	0.10	0.04

表-2 ポート別使用量詳細

図-7は、図-6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。2011年では、80番ポートの割合が2010年よりも増えています。また、ピーク時間は21:00～23:00で図-6に比べて少し早くなっていますし、土日は朝から利用が増えています。

3.6 おわりに

前回のレポートでは、それま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きたことを報告しました。また、一般利用者の使用量が、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き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なく、Webサービスへの移行が一層進んだことが確認できます。

また、今回は、東日本大震災の影響について、マクロレベルの視点で見たときには限定的であったことも報告しました。社会が大きく影響を受けた災害でも、インターネットのトラフィックがあまり影響を受けなかったことは、インターネットが生活に欠かせないインフラになっていることを示しています。

ところで、私自身は、今回の震災でもっとトラフィックが減ると予想していました。計画停電や節電のために、P2Pファイル共有等に使われている自宅サーバーを停止する利用者がもっといると思ったからです。

2010年1月の改正著作権法施行の時に比べて、トラフィックへの影響が少なかった理由にはふたつの見方があります。ひとつは、一部のヘビーユーザの行動はダウンロード違法化のような強制措置を取らないと変わらないというものです。別な見方は、前回の報告で述べたように、ダウンロード違法化はすでにあった流れを加速するトリガーになったに過ぎないという視点から、最初のトリガーで移行が進んだので、2回目のトリガーの効果が少なかったというものです。もし、法改正と震災が逆順で起こっていたら、やはり最初のトリガーで移行が進んだ可能性もあります。

もし近い将来に別の強制措置がP2Pファイル共有の利用に関して取られるようなことがあれば、その時にトラフィックが減れば前者の見方が、減らなければ後者の見方が有力だと考えることができそうです。

IJでは、今回の震災のような大きな出来事や、ユーザの利用形態の変化にも素早く対応できるよう、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。

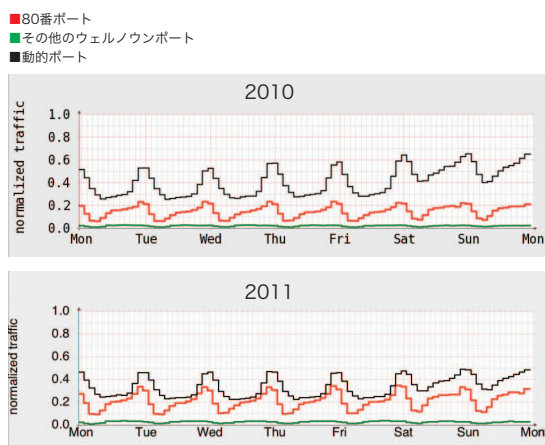


図-6 TCPポート利用の週間推移

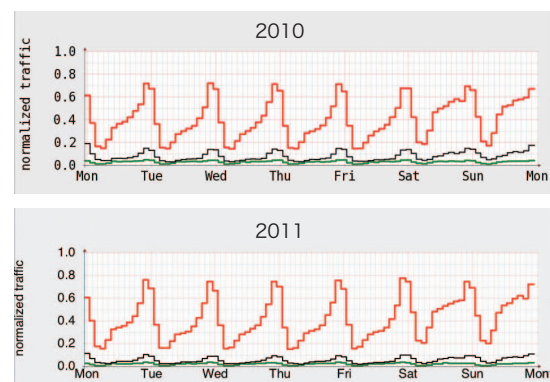


図-7 クライアント型利用者のTCPポート利用の週間推移

執筆者：
長 健二朗(ちよう 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 所長

インターネットトピック: 国内ISPによる児童ポルノブロッキングについて

ISP等による児童ポルノコンテンツのブロッキングは、違法な児童ポルノコンテンツを配信するサーバへのアクセスを阻止することにより、コンテンツの流通そのものを機能させないようにするためのものです。我が国においては、2011年4月より国内の複数ISP等により順次開始されています。ここでは、この活動の経緯と現時点での実現方法、及びその課題について紹介します。

■経緯

インターネットは、日常的に利用される便利な道具ですが、一方でその黎明期より違法なコンテンツの流通に悪用されてきていることも事実です。実際、いくつかの国では、インターネット関連の法整備が児童ポルノ対策を機に実施されています。2001年11月に採択された国際条約「サイバー犯罪条約」*1においても、不正アクセス等の直接コンピュータに関連する行為と同等のものとして、児童ポルノ関連犯罪への対応がうたわれています。

国内においても、インターネットの利用方法の変化や児童が巻き込まれる事件等を受け、2008年度の総合セキュリティ対策会議*2において、ISPやコンテンツ配信事業者、検索エンジン事業者、フィルタリング事業者により、一般の利用者が児童ポルノコンテンツにアクセスできないようにする行為（ブロッキング）の実現について、諸外国の事例等を参考に検討が行われました。また、その報告書*3の中で、ISP等による児童ポルノコンテンツブロッキングの技術的方式を紹介するとともに、実施に当たった際の検討項目と、児童ポルノ流通防止対策推進協議会（仮称）*4と児童ポルノ掲載アドレスリスト作成管理団体（仮称）の設置が提言されました。

■実施の検討

この提言を受け、通信事業者の間では、安心ネットづくり促進協議会*5の児童ポルノ対策作業部会*6にて、インターネット上での児童ポルノの流通を防止するブロッキングの法的検討、ブロッキング技術の検討、アドレスリスト管理団体と、そのリストの在り方等に関する整理が行われました。法的な側面からは、特に副作用で通常の通信を阻害してしまうオーバブロッキングの問題とその対策を中心に議論されました。また、技術的な側面からは、DNSブロッキング方式について、既存のDNSの運用やDNSSEC等の関連技術との適合性を中心に、通常のDNS運用に対する副作用等の問題が検討されました。

執筆者:

齋藤 衛 (さいとう まもる)

IIJ サービス本部 セキュリティ情報統括室 室長

監修・協力:

三膳 孝通 IIJ 常務取締役

山本 功司 IIJ サービス本部 アプリケーションサービス部 副部长

■ブロッキングの実現と課題

このような検討を経て、児童ポルノ掲載アドレスリスト作成管理団体であるICSA (Internet Content Safety Association: インターネットコンテンツセーフティ協会)*7が2011年3月に設立され、この団体が提供するアドレスリストを基に日本国内における児童ポルノコンテンツのブロッキングの仕組みが構築されました。ただし、このコンテンツのブロッキングは、それをもって抜本対策とするのではなく、法執行機関による対策活動を円滑に行うための一時的な措置として位置づけられています*8。実際には、作成されたアドレスリストに基づいたブロッキングが、本年4月以降に参加ISP等より順次実施されています。IIJにおいても複数のサービスにおいて4月よりブロッキングを実施しています。

現時点では、多くの事業者が導入コストの安いDNSブロッキングを採用しています。しかし、この手法には更新処理によるDNSサービスの提供そのものへの影響が想定されたり、DNSのクエリに対する回答を詐称できなくなるための技術である、DNSSECとの不整合が指摘されています。加えて、DNSによるブロッキング方式では、アドレスリストの一部のブロッキングしか実現できず、問題となる画像単位のブロッキングへの展開に向けた検討が必要とされています*9。このため、より精度が高く、実効性を向上させたブロッキング手法への移行について、コスト、設備構成、運用等を総合的に考慮した検討を今後も継続的に行っていく必要があります。

■まとめ

児童ポルノコンテンツへの対策は、被害児童の人権保護の観点から必要な対策です。IIJでは、本活動への参加を通じて、違法なコンテンツの流通がないインターネットを実現するための努力を継続していきます。

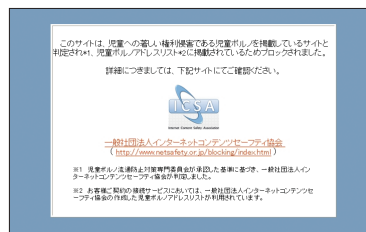


図-1 ICSAのアドレスリストによるブロッキングの結果表示

*1 サイバー犯罪に関する条約 (http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html)。

*2 警察庁主導の会議。過去にインターネット上の違法・有害情報への対策や、ファイル共有ソフトを用いた著作権侵害問題等を検討している (<http://www.npa.go.jp/cyber/csmeeting/index.html>)。

*3 平成20年度総合セキュリティ対策会議報告書「インターネット上での児童ポルノの流通に関する問題とその対策について」 (<http://www.npa.go.jp/cyber/csmeeting/h20/pdf/pdf20.pdf>)。

*4 児童ポルノ流通防止対策推進協議会（仮称）は、後に児童ポルノ流通防止対策専門委員会として組織された (<http://www.netsafety.or.jp/blocking/007.html>)。

*5 安心ネットづくり促進協議会 (<http://good-net.jp/about.html>)。

*6 「児童ポルノ対策作業部会最終報告書について」 (http://good-net.jp/press_jipo_20110428.html)。

*7 一般社団法人インターネットコンテンツセーフティ協会 (<http://www.netsafety.or.jp/about/index.html>)。

*8 このスキームについてのICSAの説明を参照のこと。「アドレスリスト作成業務について」 (<http://www.netsafety.or.jp/blocking/index.html>)。

*9 「DNSブロッキングによる児童ポルノ対策ガイドライン」 (<http://good-net.jp/usr/imgbox/pdf/20110427091336.pdf>)。

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。

©2008-2011 Internet Initiative Japan Inc. All rights reserved.

IIJ-MKTG019LA-1108KO-08000PR