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IIJ自身が取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、IIJが対応したインシデントについてまとめたものです。今回のレポートで対象とする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係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IIJ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]。

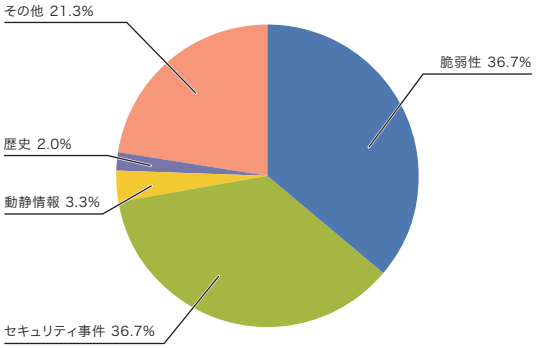


図-1　カテゴリ別比率(2011年4月～6月)

＊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.mspx)。
＊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.mspx)。
＊4 「マイクロソフト セキュリティ情報 MS11-020 - 緊急 SMB サーバーの脆弱性により、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.mspx)。
＊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.mspx)。
＊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.mspx)。
＊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.mspx)。
＊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で流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

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

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになっており、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IIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。ここでは、IIJ DDoS対策サービスの基準で攻撃と判定した通信異常の件数を示しています。IIJ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[*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IIJ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のパケットによって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

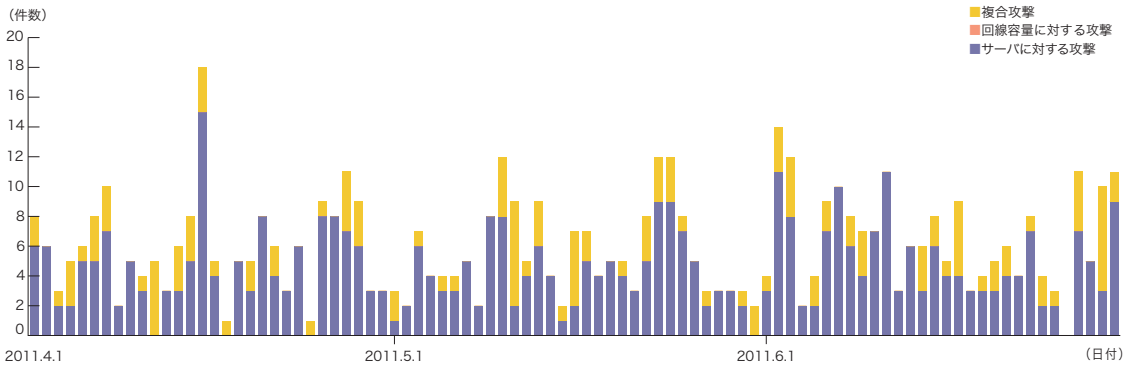


図-2　DDoS攻撃の発生件数

＊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利用させる。TCP connection flood攻撃は、実際に大量のTCP接続を確立させる。HTTP GET flood攻撃は、Webサーバに対しTCP接続を確立したのち、HTTPのプロトコルコマンドGETを大量に送付することで、同様に攻撃対象の処理能力やメモリを無駄に消費させる。

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、IIJでのマルウェア活動観測プロジェクトMITFのハニーポット[*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

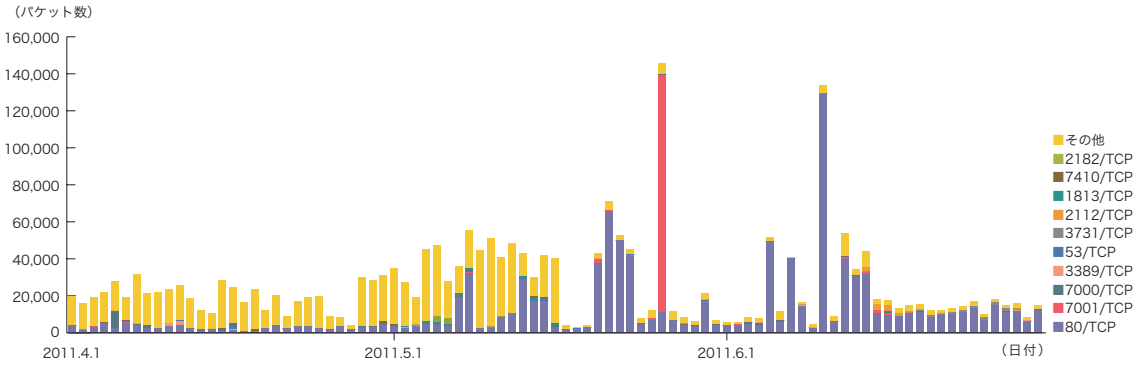


図-3　DDoS攻撃によるbackscatter観測（観測パケット数、ポート別推移）

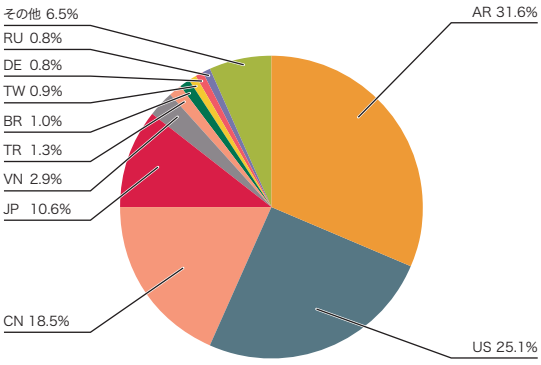


図-4　backscatter観測によるDDoS攻撃対象の分布（国別分類、全期間）

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

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

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]。IIJ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、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*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

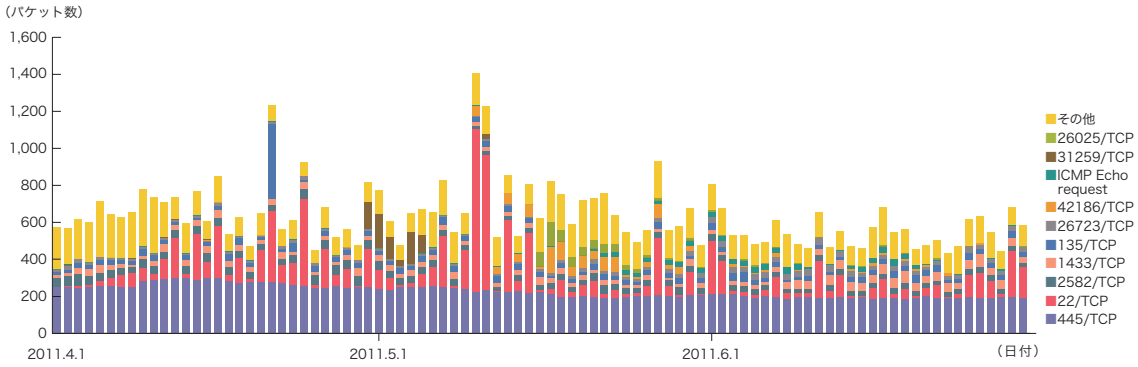


図-5　ハニーポットに到着した通信の推移（日別・宛先ポート別・一台あたり）

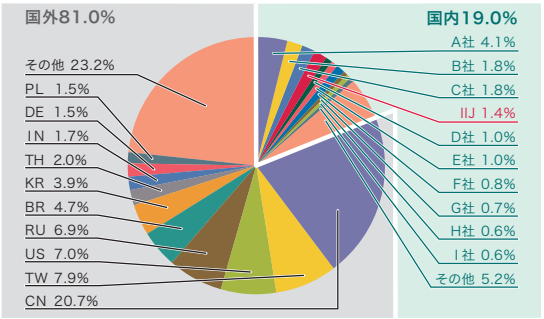


図-6　発信元の分布（国別分類、全期間）

＊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、攻撃者の行為やマルウェアの活動目的を記録する装置。

を行っていますが、ここでは1台あたりの平均をとり、到着したパケットの種類（上位10種類）ごとに推移を示しています。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。

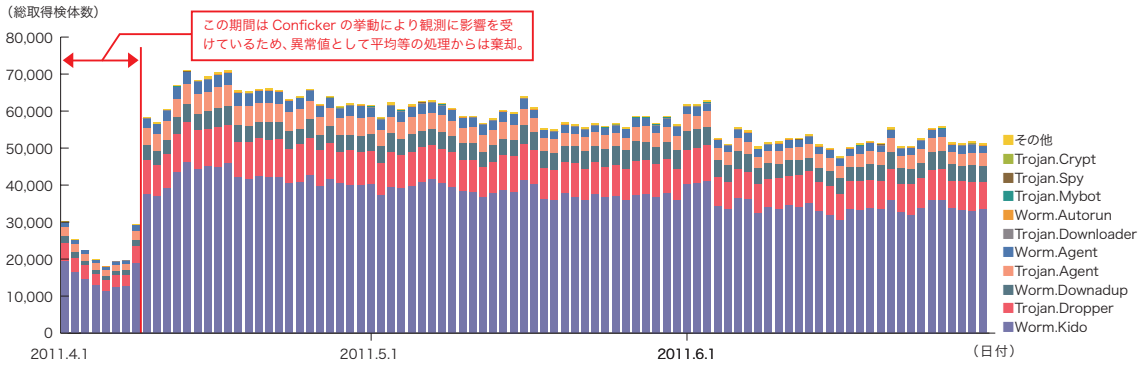


図-7　総取得検体数の推移

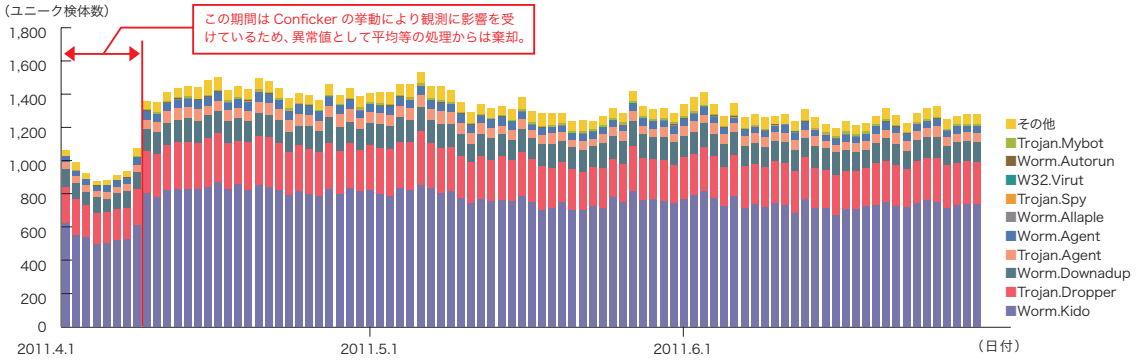


図-8　ユニーク検体数の推移

＊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。IIJ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 の挙動を変更し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%、ボット型2.3%、ダウンローダ型22.6%でした。また、解析により、23個のボットネット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

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃[*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。

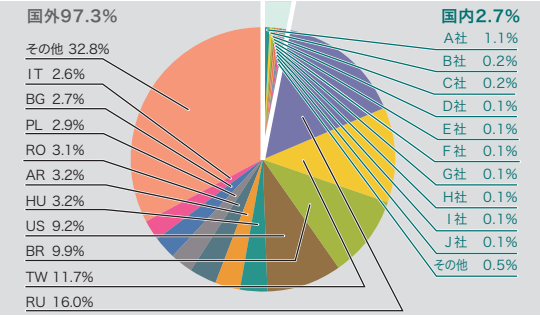


図-9　検体取得元の分布（国別分類、全期間）

＊46 dionaea（http://dionaea.carnivore.it/）とその機能についてはIIR Vol.11（http://www.iij.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。
＊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、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、日本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。

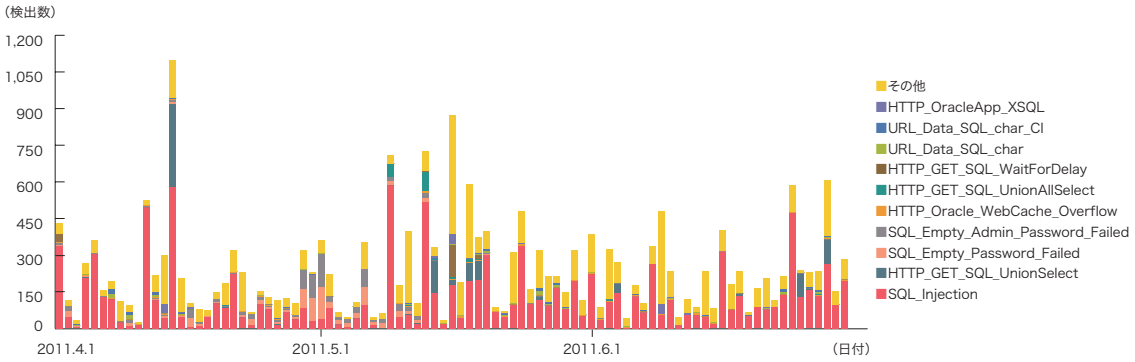


図-10 SQLインジェクション攻撃の推移(日別、攻撃種別)

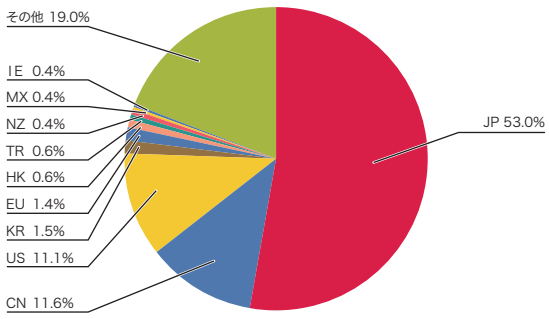


図-11 検体取得元の分布(国別分類、全期間)

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、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、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。数百万人分にのぼると見られる。	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の個人情報が一部流出。**	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	インテリア販売の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でメールアカウント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。(#OpIran)	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	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ので、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人以上の個人情報が流出。	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人分の個人情報が流出。**	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	ゲオE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人分の個人情報が流出。	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が流出。	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が英国の前首相トニー・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が流出。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が、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の活動は世界中に拡がっています。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://attrition.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.iij.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る。ただし、これらが決まった方法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言っても、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、大量のパケット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、大量のパケット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、IIJ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になります。

■ 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る。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ってい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。攻撃の目標となってい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を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っています。

＊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もなう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、IIJのようなISPを含む電気通信事業者が何らかの形で介在することで、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も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もなわ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/mtcs/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/mtcs/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。

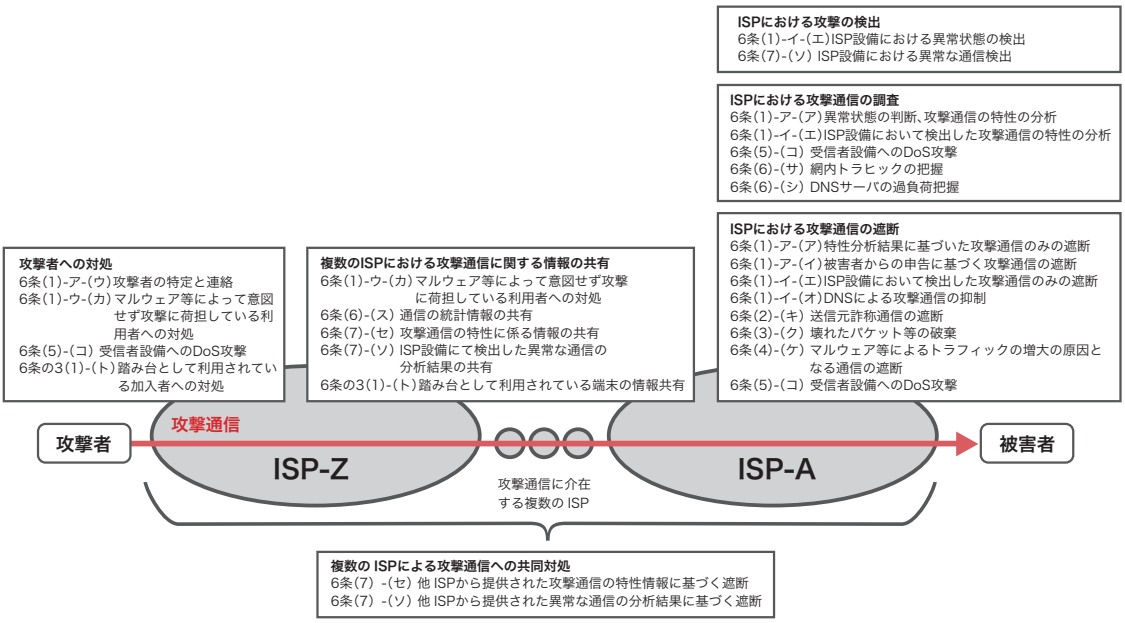
元を収容するISPに対策を依頼した場合、これらの行為をISPが自主的に実施した場合は、すべて通信の秘密の侵害行為（知得、窃用、漏洩のいずれか）に該当し、違法行為となります。しかし、現実にはこれらの行為もしくはその一部を実施しないと、攻撃の影響を減らすことはできません。では、どのような条件であれば、違法行為とならないように対処を実施することができるのでしょうか。本ガイドラインでは第2条から第4条において、その考え方を整理して示しています。

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

執筆者:
齋藤 衛(さいとう まもる)
IIJ サービス本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発等に従事の後、2001年よりIIJグループの緊急対応チームIIJ-SECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会等、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))
IIJ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　IIJ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.iij.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。