米国および韓国における大規模DDoS攻撃

今回は、2009年7月～9月の期間にIIJが対応したインシデントに関する報告とともに、米国と韓国で複数のWebサーバを対象に発生した大規模なDDoS攻撃の詳細、CERT-FIで発表されたTCPの脆弱性の内容、SIPによる無言電話発生の仕組みを取り上げます。

1.1 はじめに

このレポートは、インターネットの安定運用のためにIIJ自身が取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、IIJが対応したインシデントについてまとめたものです。今回のレポートで対象とする2009年7月から9月までの期間では、米国および韓国の複数のWebサーバに対する大規模なDDoS攻撃が発生しました。また、脆弱性に関しては、Webブラウザ関連の脆弱性が相次いで発見され、DNSサーバ等インターネット上での利用度が高いサーバの脆弱性も報告されました。加えて、多くの実装に影響するTCPの脆弱性が発表されています。このほか、偽のセキュリティソフトウェアやDDoS攻撃を伴った恐喝事件等、直接金銭被害を与える事件が継続しています。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ー

ここでは、2009年7月から9月までの期間にIIJが扱ったインシデントと、その対応を示します。この期間に扱ったインシデントの分布を図-1に示します*1。

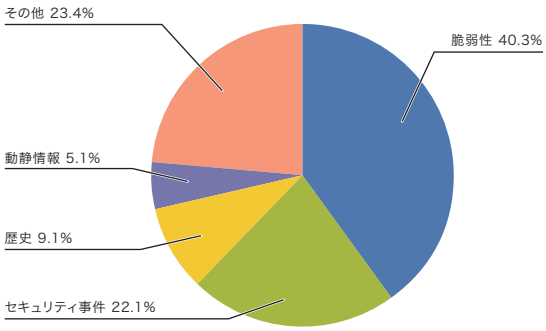


図-1　カテゴリ別比率（2009年7月～9月）

＊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、対策等の作業が該当する。
セキュリティ事件：ワーム等のマルウェアの活性化や、特定サイトへのDDoS攻撃等、突発的に発生したインシデントとその対応を示す。
その他：イベント等によるトラフィック集中等、直接セキュリティに関わるものではないインシデントを示す。

■ 脆弱性

今回対象とした期間では、マイクロソフト社のInternet Explorerの脆弱性[*2]、SMB2.0の脆弱性[*3]、Visual StudioのActive Template Libraryの脆弱性[*4]等、ユーザが利用するアプリケーションに関する脆弱性への対策が発表されました。また、ActiveXのkillbitに関する脆弱性[*5]、Jscriptに関する脆弱性[*6]、Adobe Flash PlayerやAdobe Acrobat Readerの脆弱性[*7]、Apple QuickTimeに関する脆弱性[*8]等、Webブラウザに関係する脆弱性にも多数対策が実施されています。

これらに加えて、BIND9[*9]、Squid[*10]等、サーバとしてよく利用されるソフトウェアにも、安定動作に影響するような脆弱性が発見されています。また、Cisco社製ルータのBGPに関する脆弱性[*11]や、IOSの定例アップデートがあり、複数の脆弱性[*12]が修正されています。さらに、TCPにかかわる脆弱性が公開され、多くの実装に影響するとされています。TCPの脆弱性に関する詳細は、「1.4.2 TCPの脆弱性(Sockstress)」を参照してください。

■ 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、第45回衆議院議員総選挙や消費者庁の発足等、日本国内の動きに注目しましたが、関連する攻撃は検出されませんでした。

■ 歴史

この期間には、日本における終戦記念日や太平洋戦争終結日等が含まれます。この時期には、過去に歴史的背景によるDDoS攻撃やホームページの改ざん事件等が発生しており、各種の動静情報に注意を払いました。しかしながら、IIJの設備やIIJのお客様のネットワーク上では直接関連する攻撃は検出されませんでした。

■ セキュリティ事件

動静情報に結びつかない突発的なインシデントとしては、7月初旬に米国および韓国の複数のWebサーバに対する大規模なDDoS攻撃が発生しました。この件に関する詳細は、「1.4.1 米国および韓国におけるDDoS攻撃」を参照してください。また、クラウド環境からP2P

＊2　マイクロソフト セキュリティ情報 MS09-034 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(972260)（http://www.microsoft.com/japan/technet/security/bulletin/ms09-034.mspx)。
＊3　マイクロソフト セキュリティ情報 MS09-050 - 緊急 SMBv2 の脆弱性により、リモートでコードが実行される(975517)（http://www.microsoft.com/japan/technet/security/Bulletin/MS09-050.mspx)。
＊4　マイクロソフト セキュリティ情報 MS09-035 - 警告 Visual Studio の Active Template Library の脆弱性により、リモートでコードが実行される(969706)（http://www.microsoft.com/japan/technet/security/bulletin/ms09-035.mspx)。および、Adobe Flash Playerに関するセキュリティ情報APSA09-04（http://www.adobe.com/jp/support/security/advisories/apsa09-04.html)等。
＊5　マイクロソフト セキュリティ情報 MS09-032 - 緊急ActiveX の Kill Bit の累積的なセキュリティ更新プログラム(973346)（http://www.microsoft.com/japan/technet/security/bulletin/MS09-032.mspx)。
＊6　マイクロソフト セキュリティ情報 MS09-045 - 緊急JScript スクリプト エンジンの脆弱性により、リモートでコードが実行される(971961)（http://www.microsoft.com/japan/technet/security/bulletin/ms09-045.mspx)。
＊7　Adobe Reader、AcrobatおよびFlash Playerに関するセキュリティ情報 APSA09-03（http://www.adobe.com/jp/support/security/advisories/apsa09-03.html)。Adobe Flash Player、Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB09-10（http://www.adobe.com/jp/support/security/bulletins/apsb09-10.html)。
＊8　QuickTime 7.6.4 のセキュリティコンテンツについて(http://support.apple.com/kb/HT3859?viewlocale=ja_JP)。
＊9　BIND Dynamic Update DoS (https://www.isc.org/node/474)。この脆弱性はプライマリサーバとしてゾーン情報を持つBINDサーバが対象となる。キャッシュ機能のみを提供するサーバでもlocalhostなどのゾーン情報を持つことが多いので注意が必要。
＊10　Squid Proxy Cache Security Update Advisory SQUID-2009:2（http://www.squid-cache.org/Advisories/SQUID-2009_2.txt)。
＊11　Cisco Security Advisory: Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities (http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml)
＊12　Cisco Security Advisory: Summary of Cisco IOS Software Bundled Advisories, September 23, 2009（http://www.cisco.com/warp/public/707/cisco-sa-20090923-bundle.shtml)。

ファイル共有ネットワークへの攻撃*13、Twitterに対するDDoS攻撃*14等が発生しました。さらに、8月にはDDoS攻撃を行った上で対策費用と称して金銭を要求する事件*15の発生も確認しています。

■ その他

直接セキュリティに関係しないインシデントとしては、台湾における台風の影響によって複数の国際海底ケーブルが損傷し、通信に影響を与えたことが注目されました*16。また、複数のアンチウイルスソフトウェアで2010年度版がリリースされ、それらにそっくりな偽のソフトウェアが登場して話題になりました*17。同様に、マイクロソフト社の無償アンチウイルスツールMicrosoft Security Essentials*18のリリースに伴い、検索エンジンの検索結果から詐欺的ソフトウェア(スケアウェア)に誘導される事件も起こっています*19。

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

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになっています。DDoS攻撃の内容は、状況により多岐にわたりますが、一般には、脆弱性等の高度な知識を利用した攻撃ではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にしたりすることで、サービスの妨害を狙ったものになっています。図-2に、2009年7月から9月までの期間にIIJ DDoS対策サービスで扱ったDDoS攻撃の状況を示します。

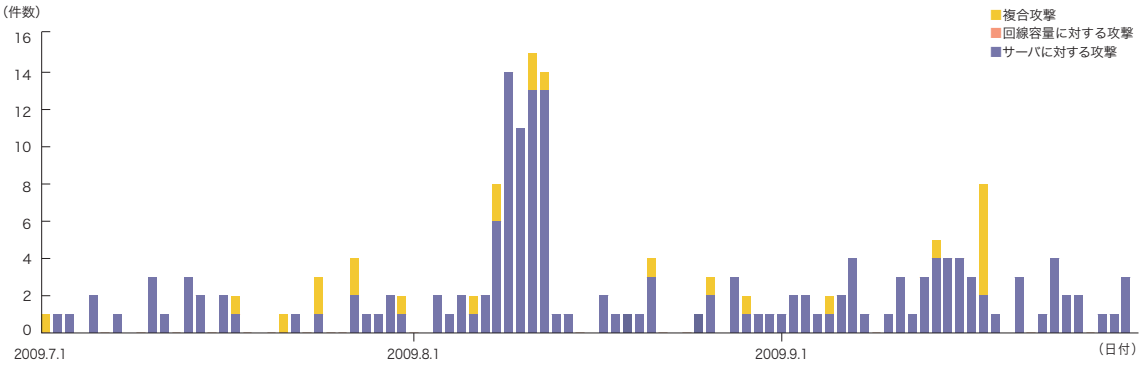


図-2　DDoS攻撃の発生件数

＊13 cNotes による「Amazon Web Serviceを利用したShareネットワークへの攻撃」(http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=Amazon+Web+Service%A4%F2%CD%F8%CD%D1%A4%B7%A4%BFShare%A5%CD%A5%C3%A5%C8%A5%EF%A1%BC%A5%AF%A4%D8%A4%CE%B9%B6%B7%E2)。

＊14 次は攻撃の様子を示すtwitterによるツイート(http://status.twitter.com/post/157191978/ongoing-denial-of-service-attack)。通信量の減少については次のArbor Networks社のblogに詳しい「Where Did All the Tweets Go?」(http://asert.arbornetworks.com/2009/08/where-did-all-the-tweets-go/)。

＊15 同様の事件については、例えばトレンドマイクロ社による次の記事を参照のこと「日本国内にも広がるボットネットによる恐喝事件(DDoS攻撃)」(http://blog.trendmicro.co.jp/archives/1385)。

＊16 本件については、例えば次の報道がある。NetworkWorld社による "Asian undersea cable disruption slows Internet access" (http://www.networkworld.com/news/2009/081209-asian-undersea-cable-disruption-slows.html)。

＊17 Symantec社の製品にそっくりな偽ソフトウェアに関するblog Symantec Security Blogs:Nort “what” AV? (http://www.symantec.com/connect/blogs/nort-what-av)。

＊18 Microsoft Security Essentials(http://www.microsoft.com/security_essentials/)。

＊19 IIJでは、検索エンジンを英語環境で利用したときに偽のソフトウェアに誘導するリンクが上位に現われることを確認している。

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、正確な攻撃の実態を把握することが困難なため、この集計からは除外しています。

DDoS攻撃には多くの攻撃手法が存在します。また、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*20]、サーバに対する攻撃[*21]、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か月間でIIJは、192件のDDoS攻撃に対処しました。1日あたりの対処件数は2.08件程度で、平均発生件数は前回のレポート期間よりも増加しています。ただし、8月9日から8月12日までの複数の攻撃は特定のサイトに対して断続的に発生したものであり、全体の動向は前回のレポート期間での発生状況と大きく変わりません。

DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0%、サーバに対する攻撃が87%、複合攻撃が13%でした。今回の対象期間で観測されたもっとも大規模な攻撃は、複合攻撃に分類した、14万ppsのパケットによって566Mbpsの帯域を埋める攻撃でした。また、攻撃の継続時間は、全体の80%が攻撃開始から30分未満で終了し、19%が30分以上24時間未満の範囲に分布しています。今回の期間中では、24時間以上継続する攻撃は1件で、94時間30分(約4日間)にわたって継続していました。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されています。これは、IPスプーフィング[*22]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[*23]の利用によるものと考えられます。

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[*24]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[*25]を利用して、インターネットから到着する通信を観測しています。そのほとんどがマルウェアによる無作為に宛先を選んだ通信か、攻撃先を探索するための探索の試みであると考えられます。

＊20 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。

＊21 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。

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

＊23 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。

＊24 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。

＊25 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。

■ 無作為通信の状況

2009年7月から9月までの期間中に、ハニーポットに到着した通信の総量(到着パケット数)の推移を図-3に、その発信元IPアドレスの国別分類を図-4にそれぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均をとり、到着したパケットの種類(上位10種類)ごとに推移を示しています。

ハニーポットに到着した通信の多くはマイクロソフト社のOSで利用されているTCPポートに対するもので、クライアントへの探索行為でした。また、今回の期間においても、前回と同様にシマンテックのクライアントソフトウエアが利用する2967/TCP、PCリモート管理ツールが利用する4899/TCPに対する探索行為が観測されています。一方で、53248/TCPや20689/TCP等一般的なアプリケーションで利用されていない目的不明な通信も観測されました。また、マイクロソフト社の脆弱性を狙った445/TCPへの攻撃は、昨年10月以来継続して観測されています。発信元の国別分類を見ると、日本国内の26.6%、中国の24.4%が比較的大きな割合を占めています。

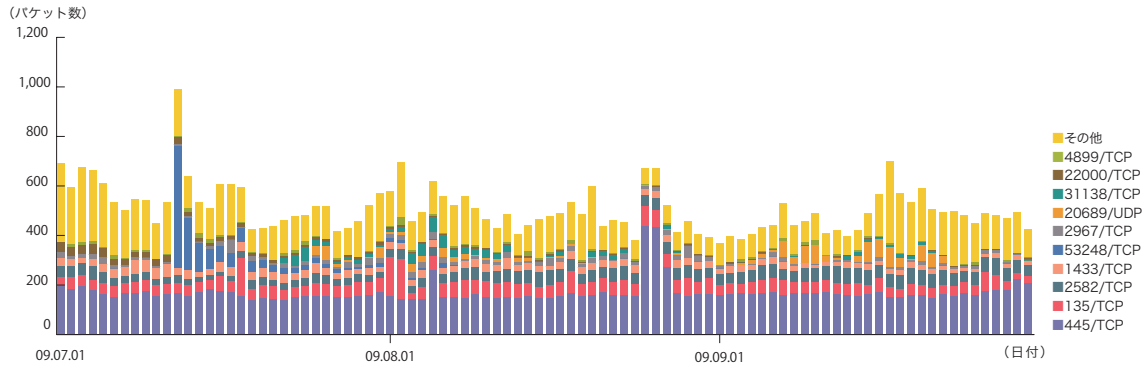


図-3　ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

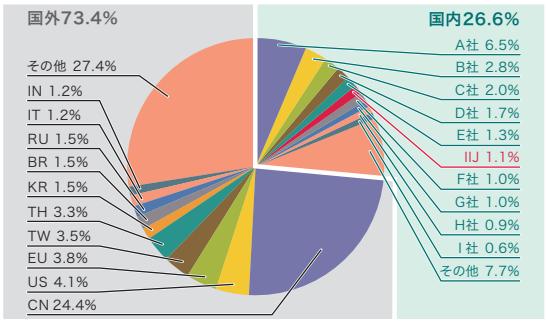


図-4　発信元の分布(全期間)

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの取得検体数の推移を図-5に、マルウェアの検体取得元の分布を図-6にそれぞれ示します。図-5では、1日あたりに取得した検体[*26]の総数を総取得検体数、検体の種類をハッシュ値[*27]で分類したものをユニーク検体数として示しています。

期間中での1日あたりの平均値は、総取得検体数が592、ユニーク検体数が46です。前回の集計期間での平均値が総取得検体数で708、ユニーク検体数で60でした。今回は、総取得検体数においても、検体の種類を表すユニーク検体数においても減少傾向にありました。

検体取得元の分布では、日本国外が35.6%、国内が64.4%でした。このうちIIJのユーザ同士のマルウェア感染活動は1.5%です。前回の観測期間では、IIJのユーザ同士の感染が16.8%でしたので、急激に減少しています。マルウェアの種類に注目した分析によると、これは、6月まで活発であったVirut[*28]とその亜種を感染させるための活動や、Sdbot[*29]とその亜種の活動が、IIJの網内で急激に見られなくなったことに起因しています。

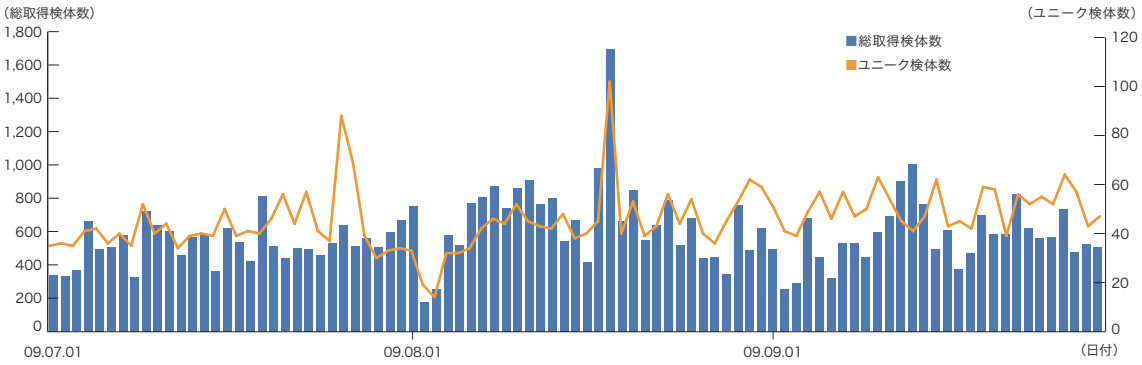


図-5　取得検体数の推移(総数、ユニーク検体数)

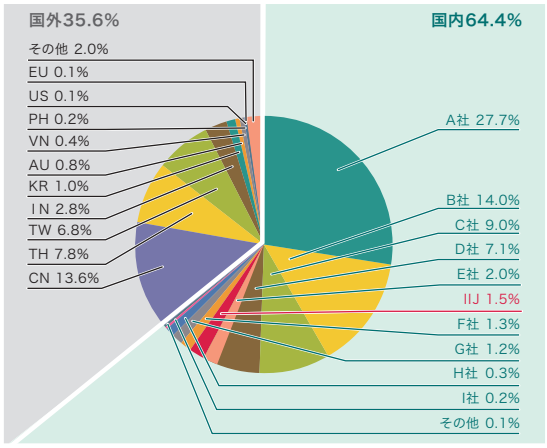


図-6　検体取得元の分布(全期間)

＊26 ここでは、ハニーポット等で取得したマルウェアを指す。

＊27 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。

＊28 Virutはファイル感染型のウイルスで、一般にはネットワークを介した感染は行わないが、脆弱性を利用した攻撃の結果としてこのウイルスを送り込む試みが流行していた。次はトレンドマイクロ社によるVirutの説明(http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=PE_VIRUT.GEN)。次はIPA (独立行政法人 情報処理推進機構)による、Webコンテンツ経由でのVirut感染に対する注意喚起(http://www.ipa.go.jp/security/txt/2009/03outline.html)。サイバークリーンセンターにおいても同様のマルウェアを感染させる試みを検出しており、他のマルウェアの感染活動とも関連するとしている(https://www.ccc.go.jp/report/200907/0907monthly.html)。

＊29 Sdbotはボットの一種で、C&Cサーバと IRCで通信を行う。次はトレンドマイクロ社によるSdbotの説明(http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_SDBOT.GEN)。

MITFでは、マルウェアの解析環境を用意し、取得した検体について独自の解析を行っています。この結果、この期間に取得した検体は、ワーム型4.5%、ボット型89.6%、ダウンローダ型5.9%となりました。また、この解析により、44個のボットネットC&Cサーバ*30と548個のマルウェア配布サイトの存在を確認しています。

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*31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。

2009年7月から9月までに検知した、Webサーバに対するSQLインジェクション攻撃の推移を図-7に、攻撃の発信元の分布を図-8にそれぞれ示します。これらは、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67.3%、中国11.6%、米国4.9%となり、以下その他の国々が続いています。

Webサーバに対するSQLインジェクション攻撃の発生状況は、前回の観測結果に比べて減少が見られました。このため、SQLインジェクション攻撃の総数は減少しましたが、国外を発信元とする攻撃の減少が顕著であったため、日本国内を発信元とする攻撃の割合が大きくなっています。

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

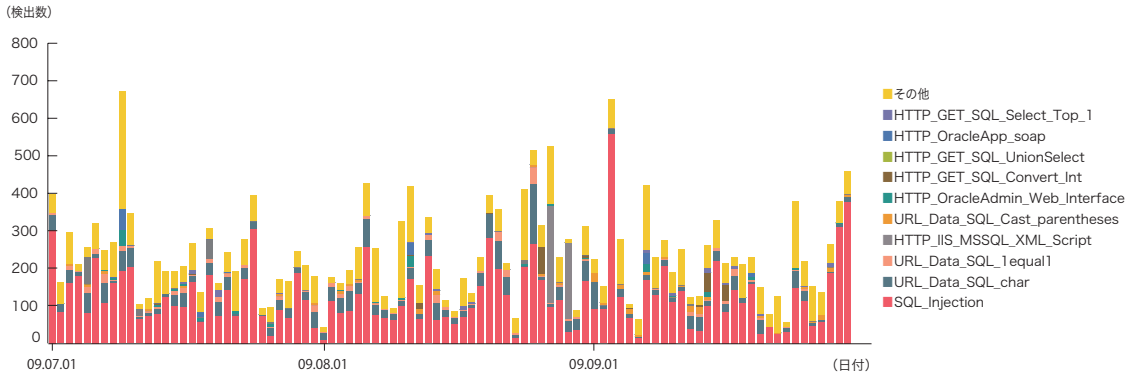


図-7　SQLインジェクション攻撃の推移(日別、攻撃種類別)

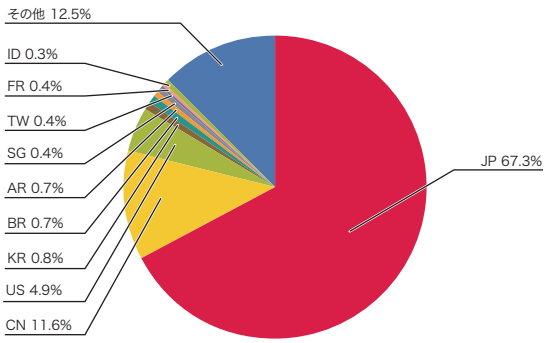


図-8　SQLインジェクション攻撃の発信元の分布

＊30 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。
＊31 Webサーバに対するアクセスを通じて、SQLコマンドを発行し、その背後にいるデータベースを操作する攻撃。データベースの内容を権限なく閲覧、改ざんすることにより、機密情報の入手やWebコンテンツの書き換えを行う。

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。IIJでは、流行したインシデントについて独自の調査や解析を行い対策につなげています。ここでは、2009年7月から9月までに実施した調査のうち、米国および韓国におけるDDoS攻撃、TCPの脆弱性(Sockstress)、無作為に到着するSIPパケットについて、その詳細を示します。

1.4.1 米国および韓国におけるDDoS攻撃

2009年7月初旬、米国および韓国の複数のWebサイトに対して、同時多発のDDoS攻撃が発生しました*32。ここではIIJが入手した情報を元に、その攻撃の状況を示します。

■ DDoS攻撃の経緯

今回のDDoS攻撃では、昨今DDoS攻撃に広く利用されているボットネットは利用されず、今回の攻撃専用のマルウェアが利用されました。この攻撃専用のマルウェアは、韓国国内でファイル共有を行うWebサイトに置かれたファイルを介して感染したとされています*33。このため、攻撃元のIPアドレスの多くは、韓国国内のものであったとされています*34。また、韓国国外の同様のWebサービスにも同種のマルウェア感染用ファイルが置かれ、韓国以外の国にも感染被害がありました*35。この感染活動がどの程度の期間にわたって行われていたかは不明ですが、アンチウイルスベンダによる発見や対処を避けるために、DDoS攻撃の発生直前に一気に感染活動が行われたものと見られています*36。また、このマルウェアに感染したPCの総数は不明ですが、後日の韓国側からの発表では、韓国国内において約7万8千台の規模の感染があったとしています*37。

DDoS攻撃はまず、韓国時間の7月5日*38および7月6日に、政府官公庁関係を主とした米国の複数のWebサーバに対して発生しました。この後7月7日以降、攻撃は韓国国内の複数のサイトに推移しました。韓国に対する攻撃では、政府官公庁関係に加えて、オンラインバンクやWebメール等、生活に密着したサイトも対象となりました。攻撃の通信面では、マルウェアに感染し攻撃に利用された個々のPCからの通信の量は多くなく、大量の通信によって回線を埋める攻撃よりもサーバに直接負荷を与えるような攻撃が主であったと伝えられています*39。

今回のDDoS攻撃は、7月10日を境に下火となり終息しています*40。これは、約7万8千台の感染PCの95%を4日間で駆除することに成功するなど、韓国国内におけるISPやセキュリティ関係組織や、メディア等の努力によるところが大きいと考えられます*41。このような対策活動の結果、7月10日を経た時点でDDoS攻撃は収束し、マルウェア感染の副作用として発生するHDD破壊も数百台程度であったと伝えられています。

＊32 本DDoS攻撃にて米国のサイトのいくつかがアクセスできなくなっていることをエフセキュア株式会社がブログで報じている(http://blog.f-secure.jp/archives/50255293.html)。また、韓国国内へのDDoS攻撃によっていくつかのサイトがアクセスできなくなっていることは、韓国国内の報道機関によって伝えられていた。

＊33 Web上でのファイル共有サービス(いわゆるアップローダー)は、韓国国内においては、企業や教育機関等で広く日常的に利用されており、マルウェアを感染させるファイルが共有ファイルとして置かれたため、多くの利用者が感染したと伝えられている。

＊34 次の報告では、攻撃に加担したPCは10万台以上で、そのうち韓国からの攻撃は全体の90～95%であったとしている(http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20090710)。

＊35 次は日本国内からの攻撃があったことを示すJPCERT/CCによる注意喚起「韓国、米国で発生している DDoS 攻撃に関する注意喚起」(http://www.jpcert.or.jp/at/2009/at090012.txt)。

＊36 一つの状況証拠として、IIJで入手した検体を調査した結果では、ファイルの作成日は2004年に偽装されているものの、PEヘッダ内のタイムスタンプは例えばperfvwr.dllが2009年7月4日0:38等、いずれのヘッダも攻撃が開始される直前の日付が記録されていた。

＊37 韓国国内の感染台数に関する情報はKRNIC of KISA (Korean Internet & Security Agency)によるAPNIC28での発表に詳しい(http://meetings.apnic.net/__data/assets/pdf_file/0019/14077/lee-ddos-attack.pdf)。

＊38 韓国と日本の間に時差はない。最初の攻撃は韓国時間で7月5日午前2時に開始されたが、米国時間(EDT)では7月4日(独立記念日)の午後13時にあたる。

＊39 例えば、次のKrCERTによる注意喚起にはこのマルウェアによるDDoS攻撃の通信の状況が示されている(http://www.krcert.or.kr/noticeView.do?num=340)。(韓国語の情報)

＊40 トラフィックが正常に戻ったことを受け、7月12日には韓国NCSC(National Cyber Security Center)は警報を"注意"から"関心"に推移させた。

＊41 APNIC28におけるKrNICの発表内容による(http://meetings.apnic.net/28/program/apops/transcript#ji-young-lee)。その他の活動としては、例えば、韓国国内に対するDDoS攻撃が発生した後、攻撃に利用されたマルウェアの情報や、その駆除ツールが複数のアンチウイルスベンダから早期に提供されていた。また、テレビのニュース番組や、多くのユーザが利用するWebサービスのTOPページでの告知等で、この問題に関する注意と対策の情報を広めようとする努力がなされた。さらに、マルウェアの少なくとも1つの亜種によって7月10日にHDDが破壊されるということが判明し、PCの時計を戻す等の一時的な対策手法に関する情報も伝えられていた。

■ 攻撃に利用されたマルウェア

IIJでは、今回の攻撃の発生時から、一般のマルウェア関係の情報源や、関係組織を介して、最初にDDoS攻撃用マルウェア感染を誘導するマルウェア、実際にDDoS攻撃の機能を持つマルウェア、攻撃先を更新するマルウェア等、複数の検体を入手しました。

これら複数の検体を解析し、実証実験を行ったところ、今回の攻撃に利用されたマルウェアは図-9に示すような動作を行うことが分かりました*42。

まず、発端となるマルウェア(msiexec*.exe等)は、2種類のマルウェア(perfvwr.dll (もしくはwmiconf.dll)と、wmcfg.exe)をドロップ(生成)します(1)。マルウェアperfvwr.dll (もしくはwmiconf.dll)はまず、攻撃に先立って感染したPCのパーソナルファイアウォールを停止します。また、3か所のサーバに接続し、攻撃のための設定ファイル(uregvs.nls)を生成します(2)。マルウェアのうちperfvwr.dllとwmiconf.dllは、設定ファイルに従ってDDoS攻撃を行います(3)。設定ファイルには、DDoS攻撃の期間、対象とするサーバ、攻撃の種類、回数が記述されています。このマルウェアによる攻撃は、この設定ファイルに従って図-9の(4)のように行われます。IIJにおける実証実験の結果、1台あたりの攻撃の通信量は、TCP syn floodで110pps、TCP ACK floodが110pps、UDP FloodおよびICMP floodで216Kbps程度、HTTP GET floodもしくはHTTP POST floodで107cps(command per sec)となりしました。また、プログラム上の一時停止命令によって、これらの通信が断続的に増減しながら発生する様子が観測されています。

一方でwmcfg.exeは、さらにmstimer.dllとwversion.exeをドロップします(5)。mstimer.dllは、複数のWebサーバからflash.gifという名前のファイルをダウンロード(6)し、そのファイル内からwversion.exeを抽出してアップデート(7)すると同時に、複数の宛先に迷惑メールを送信します(8)。一方でwversion.exeは、mstimer.dllと自分自身を削除する等、痕跡を消去する活動を行います(9)。ただし、アップデートされた後は、ハードディスク内部の特定の拡張子を持つファイルを検索して破壊したり(10)、ハードディスクのMBR*44周辺に特定の文字列を書き込み、PCを起動不能にする機能が追加されます(11)。

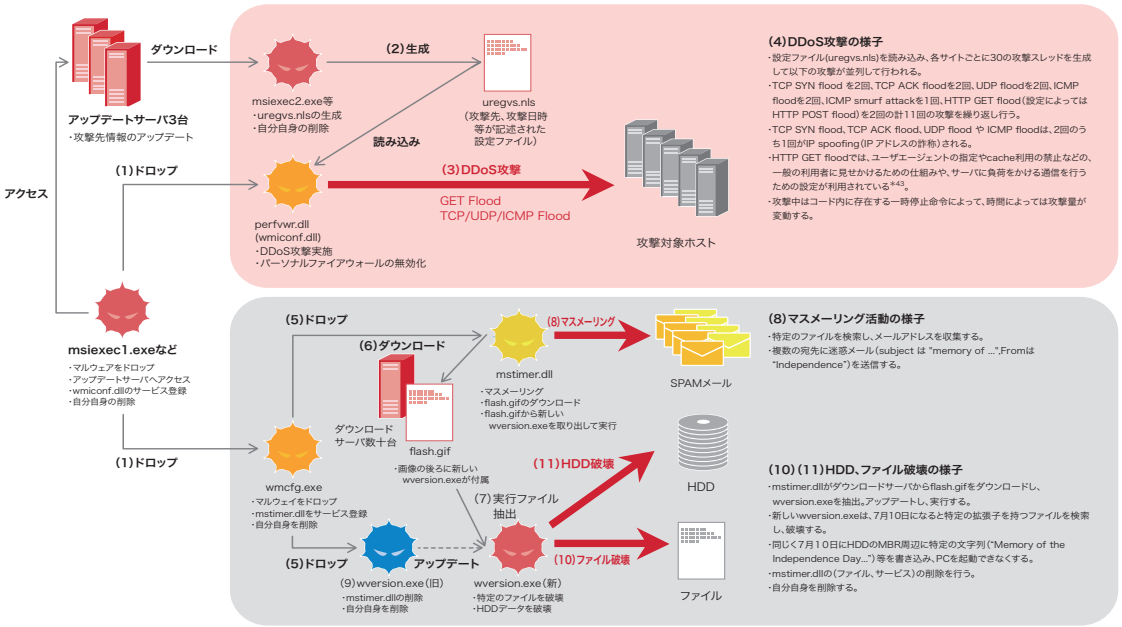


図-9　DDoS攻撃に利用されたマルウェアの動作

＊42 この動作の様子は、極力直接得た情報をもとに取りまとめているが、DDoS攻撃発生当時のインターネット上の各種サーバ等の役割や状況については、IIJで直接確認していない情報も含んでいる。

＊43 User-AgentヘッダにはfirefoxやIE7.0、IE8.0に見せかける文字列が存在し、様々なパターンがある。Accept-Languageヘッダにはko (韓国語)が指定される。またCache-Controlヘッダにはno-store, must-revalidateが指定されるが、すべてのリクエストに必ず付加されるわけではない。

＊44 MBR:Master Boot Recordの略。ハードディスクの先頭にある領域で、通常はこの領域にOSの起動用のプログラムが格納される。

■ 攻撃の全体像

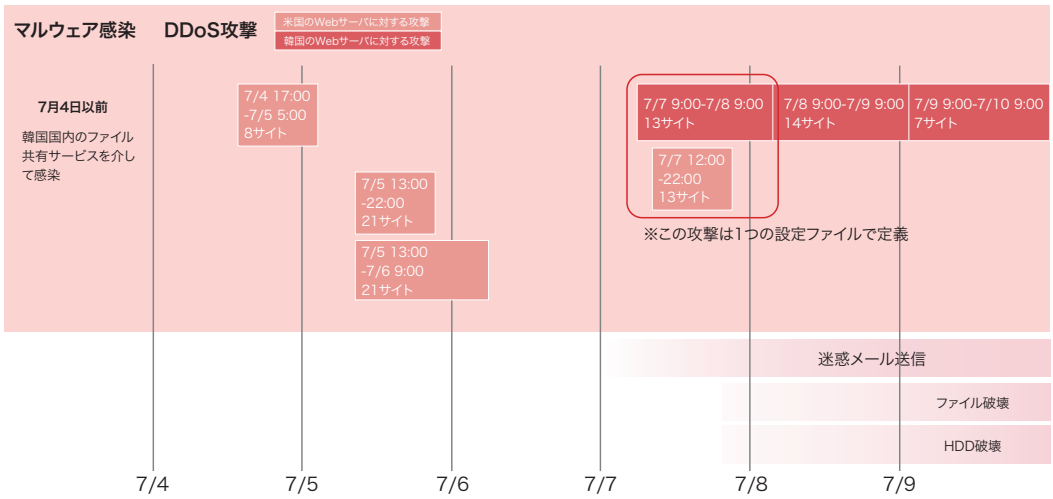
今回発生した事件における、攻撃対象の推移や関連する事象を時系列順でまとめ、図-10に示します。

通常、DDoS攻撃は、特定のサイトに対する嫌がらせ等、明確な狙いを持って行われることが多く、インターネット上で発生するインシデントの中では、比較的その意図がわかりやすいものの１つです。しかし、今回のDDoS攻撃は、主に韓国国内で攻撃用マルウェアが広まったこと、攻撃先が米国から韓国に推移した*45こと、介在したマルウェアが2つの独立したマルウェアに分かれること等、複雑で意図が読み取りにくい攻撃となっています。

■ 今回のようなDDoS攻撃への対策

ここでは今回のDDoS攻撃の被害を受けたときの対策について、通常のDDoS攻撃への対策との差異に注目して検討します。今回の攻撃は、多くのマルウェア感染PCの一斉動作によるもので、攻撃の通信を発生させているPCのIPアドレスについて個別にアクセス制御や帯域制御を行うことは困難です。しかし、攻撃の通信の多くは、一つの国の国内から発生しており、ネットワーク単位でアクセス制御や帯域制御を行うことは、一時的な対策として有効であったと考えられます。また、今回は個々のマルウェア感染PCからの攻撃の通信量が小さく、特に攻撃にかかわるWebのリクエストはマルウェアにより利用者の挙動を真似るように偽装されているため、正常な通信と攻撃による通信の判別が比較的難しくなっていることが特徴でした。DDoS 対策装置等を利用できる場合でも、異常検知のしきい値や動作モードの設定等に工夫が必要になる状況が考えられます。

最後に、IIJとしては、今回の事件のような仕組みで日本国内からDDoS攻撃が発生した状況を想定し、対処方法を検討しておく必要があると考えています。攻撃に利用されたマルウェアは事前に配布される設定にしたがって攻撃を実施することから、一元的に管理されるボットネット等への対策とは異なり、攻撃が開始された後はマルウェアに感染したPCから個々にマルウェアを駆除するより他に攻撃を止める方法はありません。韓国で実際に行われたように、多くのPCから早期にマルウェアを駆除するためには、多くの組織による連携した活動が必要です。このためには、関係組織での間で日常から有事に備え、いざというときの対策において相乗効果を発揮できることが重要となります*46。



攻撃対象の数は報道等の情報にIIJで確認した攻撃先を加えたもの

図-10 米国および韓国に対するDDoS攻撃: 時系列で整理(UTC)

＊45 取得した検体から、米国13サイトへの攻撃(2009年7月7日18:00から7月8日18:00)と韓国13サイトへの攻撃(2009年7月7日 21:00から7月8日7:00)が同一設定ファイル内で行われ、これを境に攻撃全体が韓国国内への攻撃に推移したことが分かっている。

＊46 日本では、総務省による「電気通信事業分野におけるサイバー攻撃対応演習」(http://www.soumu.go.jp/menu_news/s-news/2006/061201_4.html)や日本データ通信協会Telecom-ISAC Japan (https://www.telecom-isac.jp/)等で、サイバー攻撃に対する演習が行われており、また国際的にはAPCERTによる演習(http://www.apcert.org/documents/pdf/APCERT-drill-2008.pdf)等がある。IIJはこのような場に積極的に参加している。

1.4.2 TCPの脆弱性(Sockstress)

2009年9月、フィンランドのCSIRT組織であるCERT-FIにより、TCPに関する脆弱性への対応状況が発表され、報道等でも大きく取り上げられました*47。ここでは、このTCPの脆弱性とその対応について説明します。

■ 経緯

今回発表された脆弱性そのものは、発表の1年以上前である2008年9月に、スウェーデンに本拠地を置くセキュリティベンダOutpost24社の2名の研究者によって、その存在が指摘されたものです。この研究者たちは、ネットワーク上の監査を高速化するツールUnicornscan*48を開発し、その利用中にTCPの不審な挙動に気づき、その動作を狙って通信を行うツールSockstress*49を作成しました(このツール自体は非公開になっています)。

この脆弱性の存在を示す情報を受け、CERT-FIを中心に製品開発者間に対策を促進するためのコミュニティが組織されました。日本では、情報セキュリティ早期警戒パートナーシップ*50で取り扱われています。

■ 脆弱性として指摘された問題

脆弱性を攻撃するためのツールSockstress自体は非公開であり、今回指摘された脆弱性の全容は公開されていません。ここでは、もっとも大きく取り上げられたゼロウィンドウサイズの問題について解説します。

ゼロウィンドウサイズの指定による攻撃は、次の順序で発生します。

1. クライアントからサーバに対してTCP接続を確立する。
2. 通信の途上にクライアント側で受信ウィンドウサイズ0の指定を行い、「受信バッファに空きがなく、これ以上はデータを受け取れない」と宣言する。この状態で、サーバ側は当該TCP接続によるデータ転送を一時停止する。サーバ側は、クライアント側に現在の受信ウィンドウサイズをある間隔で問い合わせ、応答がある限り接続を保持し続ける。
3. クライアント側からサーバに対して上記の1と2を多量に繰り返す。
4. サーバ側の資源が埋め尽くされ新しいTCP接続を受け入れられない状態になる。

実際には、サーバ側の実装や資源の量等によって、攻撃が成立するまでの時間は変化します。また、高負荷にはなるものの、攻撃が成立しないことも考えられます。

ゼロウィンドウサイズの状態で接続が保持されること自体は、TCPの規格RFC793*51やRFC1122*52に記載されている正常な動作です。TCPによる通信を利用する通常のクライアントでも、正常な通信制御としてゼロウィンドウサイズの指定を行うことがあります。今回の指摘では、ゼロウインドウサイズの指定が、システム資

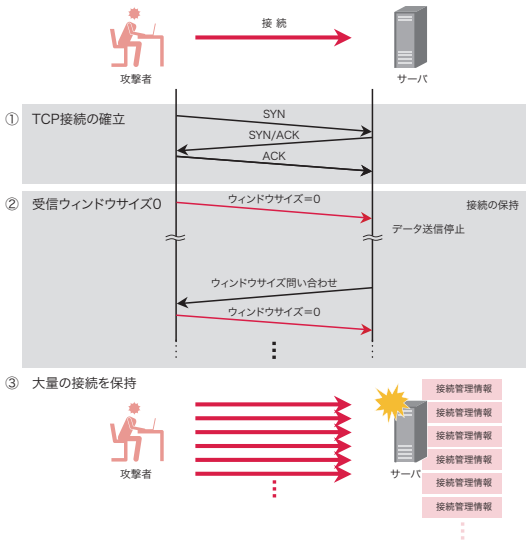


図-11 ゼロウィンドウサイズの指定によるサーバ側のスタック

*47 TCPに関する脆弱性への対応状況(https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html)、(http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4609)、(http://www.microsoft.com/japan/technet/security/bulletin/ms09-048.mspx)など。
*48 Unicornscan(http://www.unicornscan.org/)。
*49 Sockstress自体は非公開とされているが、関連情報は次にまとまっている(http://sockstress.com/)。
*50 情報セキュリティ早期警戒パートナーシップは経済産業省告示に基づく製品開発者への脆弱性情報流通の仕組み。このパートナーシップでは、IPA(http://www.ipa.go.jp/security/vuln/report/)が脆弱性情報の受付機関として、JPCERTコーディネーションセンター(http://www.jpcert.or.jp/vh/)が製品開発者との調整機関として活動している。 取り扱われた脆弱性に関する情報はJVNにて公開される(http://jvn.jp/)。IIJはルータ等の自社製品の製品開発者としてこのパートナーシップに参加している。
*51 RFC793 Transmission Control Protocol(http://www.ietf.org/rfc/rfc793.txt)。
*52 RFC1122 Requirements for Internet Hosts - Communication Layers(http://www.ietf.org/rfc/rfc1122.txt)。

源を超える量のTCP接続を保持させるための手法として、攻撃に悪用可能であることが示されました。ただし、このゼロウィンドウサイズによる攻撃は、新しい手法ではなく、例えばIETF*53のTCPMワーキンググループ*54でSockstress登場前の2006年7月頃から話題に上っています*55。

■ プロトコルの問題か実装の問題か

すでに示したようにゼロウィンドウサイズの指定は、プロトコル規格上は正常な状態ですが、これを大量に引き起こすことが問題視されています。この問題を解決するために、TCPプロトコルそのものに変更を加えるか、タイムアウト値の設定や調整等実装上の回避策を行うかという議論がありました。

先に述べた過去のIETF TCPMワーキンググループでの議論では、この種の攻撃はOSやサーバ実装の資源管理上の問題であり、プロトコル規格ではなく実装時に個別の事情に応じた解決をすべきというのが大方のコンセンサスでした。こうした状況もあり、今回の件は実装上の対応を行う方向で対処されました。

■ 対策の有効性

今回のゼロウィンドウサイズの問題に関して、マイクロソフト社の対策を例にとり、対策を施す前の実装と、対策後の実装で実証実験を行いました。この実験の結果を図-12に示します*56。

この実験結果が示すように、対策後の実装では、対策前の実装よりも今回の攻撃に対する耐性が強化されています。ただし、この対策では、新しいTCP接続を受け入れるために、既存のTCP接続を強制的に終了することで資源を解放しており、重要な接続を切断してしまう可能性を否定できません。また、この攻撃を完全に防ぎきるものではありません。マイクロソフト社に限らず、「対策済み」としている多くの実装においても同じように有限の資源の利用法を調整することで対策としている状況にあります。

ここまで紹介したように、今回の問題は実装の脆弱性として取り扱われましたが、TCPの規格から見て攻撃の接続と正常な接続を区別できない以上、本質的には、大量の接続を受けるシステムの資源管理の問題であると言え

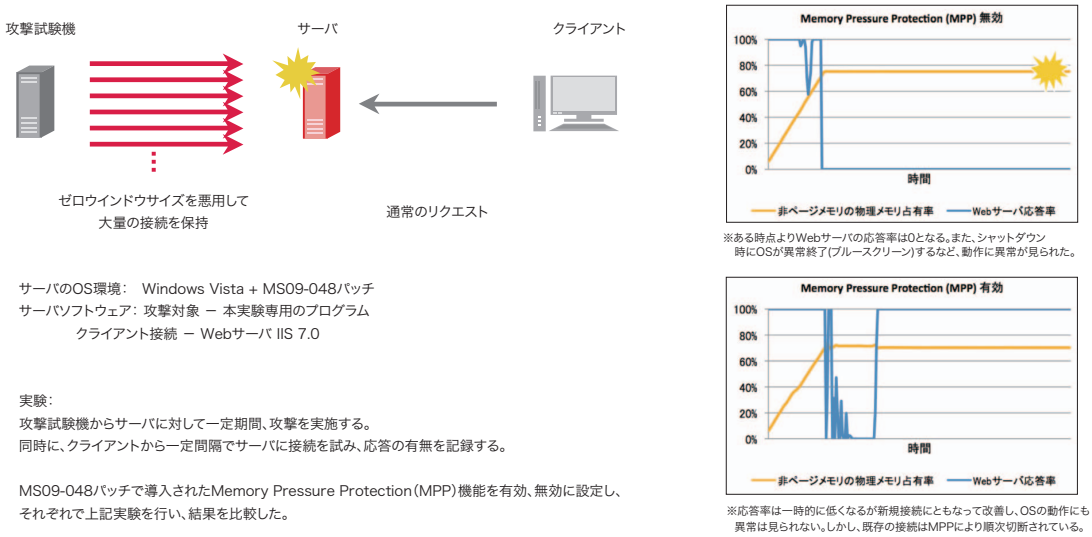


図-12 実証実験とその結果

＊53 IETF Internet Engineering Task Force の略。インターネット技術の標準化を推進する組織（http://www.ietf.org/）。
＊54 TCPMワーキンググループ TCP Maintenance and Minor Extensions Working Group（http://www.ietf.org/dyn/wg/charter/tcpm-charter.html）。
＊55 TCPM WGメーリングリストでの（http://www.ietf.org/mail-archive/web/tcpm/current/msg02189.html）に始まる議論や、その後提出されたInternet Draft、「Clarification of sender behaviour in persist condition」（https://datatracker.ietf.org/drafts/draft-ananth-tcpm-persist/）等。
＊56 実際にはマイクロソフト社のWebサーバ、インターネット インフォメーション サービス（IIS）には、OSの負荷状況によりWebの応答を調整する機構が備わっており、Webサービスに対して今回の攻撃を行うだけでは、OSの動作異常までは至らなかった。このため、今回の実験ではWebサービス以外のサービスに対して攻撃を行って負荷をかけている。

ます。このように、実装の修正による根本的な対策ができない問題は他にも存在し[*57]、今後も新たに発見される可能性があります。したがって、インターネット上に公開しているサーバについては、引き続きその負荷等に注意して運用していく必要があるのです。

1.4.3 無作為に到着するSIPパケット

■ 不正なSIPの通信

IIJでは、昨年よりハニーポットに到達するSIP（Session Initiation Protocol: セッション確立プロトコル）[*58]のパケットを断続的に観測しています。これらのSIPパケットは、インターネット上の不特定多数に対して送信されていて、SIPを解釈することのできる端末への接続が試みられています。一部のVoIPルータやIP電話端末では、設定によってSIPのパケットが到着しただけで着信音を鳴らす等の反応を起こすことがあります。このような理由による無言電話の事例が多く報告[*59]されています。

■ SIPによるVoIP通信の仕組み

SIPは、その名前が示すとおり、セッションの制御に使われるプロトコルの1つで、HTTPと同様にリクエストとレスポンスを基本としています。SIPは、IP電話サービス等VoIP通信で利用されています。ただし、HTTPがデータの配送まで規定しているのに対して、SIPはVoIP機器間でのセッションの開始、変更、終了の3つの制御をするだけで、音声等はRTP（Real-time Transport Protocol[*60]）等の別のプロトコルで配信されます。図-13に、IP電話でのSIPの通信例を示します。

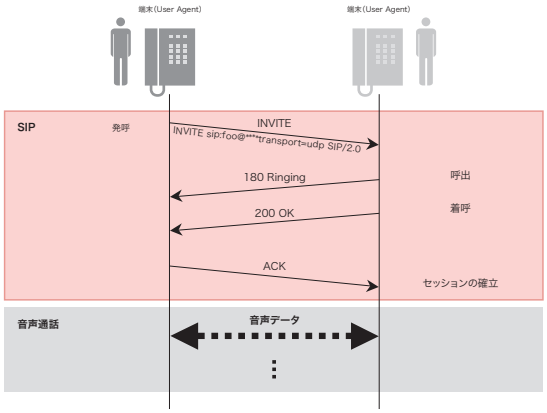


図-13 SIPによる音声通話確立の様子

① IP電話で電話をかけるときには、まず、発信元の端末（UA: User Agent）が通話先に対してINVITEメッセージを送信する。
② 着信側の端末は、INVITEメッセージを受け取ると、着信ベルを鳴らして人に知らせる。同時に、呼出中であることを意味する（180Ringing）をINVITEメッセージの発信元に返答する。
③ 通話先で人が受話器を取ると、着信側端末は200 OKを発信元に送信する。
④ これを受け取った発信元は、着信側にACK応答を返しセッションを確立する。

これは基本的な動作で、一般的には、接続する際に直接端末同士で通信せず、SIPサーバ[*61]等を利用します。

■ IP-PBXを狙った攻撃

最近では、企業等においても、導入コストや維持費等を抑えるため、従来のPBX[*62]による回線交換網の利用をやめ、IP-PBX[*63]を利用したIP電話システムを導入する事例が増えてきています。安価なIP-PBXアプライアンス製品も登場しているため、今後このような導入がますます増えると考えられています。

IP-PBXは、コスト抑制等の導入メリットが大きい半面、これまでの電話網と異なり、インターネットや閉域IP網等、他の通信が行われていたり、VoIP機器以外の機器が接続されているネットワークに接続します。この

＊57 例えば、英国CPNIによるTCPの頑健性に関する調査報告書（https://www.cpni.gov.uk/Docs/tn-03-09-security-assessment-TCP.pdf）やIPAによるTCP/IPの既知の脆弱性をまとめた調査報告書（http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html）では、こうした問題を複数示して、開発者向けにTCP/IPプロトコルスタックを実装する上での注意点を解説している。また、後者の報告書には運用者向けのガイドも記述されている。
＊58 無作為なSIPのパケットについては本レポートのVol.4においても紹介している（http://www.iij.ad.jp/development/iir/pdf/iij_vol04.pdf）。
＊59 例えばcNoteによる「INVITE Flood?不正なSIP着信」（http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=INVITE+Flood%3F++%C9%D4%C0%B5%A4%CASIP%C3%E5%BF%AE）。
＊60 Real-time Transport Protocolはデータストリームをリアルタイムに配送するためのデータ転送プロトコル。音声や動画の転送などに利用され、VoIP機器の多くはRTPをサポートしている。
＊61 SIPサーバには中継（プロキシ）・転送（リダイレクト）・登録（レジスター）等の機能があり、通常はSIPサーバを経由することで相手との通信を行う。
＊62 PBX（Private Branch eXchange）は主に企業等に導入されている構内交換機のこと。内線と外線（公衆電話回線網）とを接続し、その発着信の制御を確立する。
＊63 VoIP機能に対応したPBXのこと。例えばAsterisk（http://www.asterisk.org/）等が知られている。

ため、従来のPBXに比べると、外部や内部からの攻撃を受けやすい点を考慮する必要があります。また、現在のVoIP製品の多くがUDP上でSIPを利用しているため、IPアドレスや発信元の電話番号等を詐称したSIPパケットを容易に作成できる状況にあります。実際に、海外では脆弱性を悪用してIP-PBXを不正に操作し、IP電話サービスの契約情報を取得して悪用する試み[*64]や、番号を詐称して着信履歴を残すことで折り返し有料電話サービスに電話をかけさせて料金をだまし取ろうとした事例[*65]が発生しています。IIJで観測した無作為のSIPパケットに関しても、無言電話を引き起こすことが目的ではなく、悪用可能な脆弱性を持つIP-PBXを探査する狙いがあったと考えられます。

■ VoIPのセキュリティ対策

このような被害を受けないためには、どのような脅威があるかを正しく理解し[*66]、利用しているVoIP機器のベンダで推奨している設定や製品に関する情報を定期的に確認したり、利用しているISP等によるサービス利用上の注意事項を確認する等、常に機器を適切に運用することが大切です。また、利用できるようであれば、VoIP機器の暗号化機能を設定したり、特定のSIPサーバからのみSIPパケットを受け取るように設定する等、不特定多数からのSIPメッセージを受け取らないよう、機能や設定で適切なアクセス制御を行います。さらに、VoIPに対応したファイアウォール、IDS、IPSを導入したり、セッションボーダーコントローラ[*67]を導入することも有効です。

個人向けIP電話や企業でのIP-PBX等、VoIPは今後ますます普及すると考えられます。見ず知らずな電話番号からの着信は不用意に折り返さないなど、従来の電話での脅威に対する対応と同様に、これら新たな脅威に対しても適切な対応を行うことが必要です。

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、IIJが直接関与していないインシデントですが、米国と韓国におけるDDoS攻撃について大きく取り上げました。このように他国で発生した事件についても、情報を収集し解析を行うことで、将来日本において同様のインシデントが発生したときに迅速に対処できるように備えておくことも、我々の使命だと考えています。

IIJでは、このレポートのようにインシデントとその対応について明らかにし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 サービス事業統括本部 セキュリティ情報統括部 部長。法人向けセキュリティサービス開発等に従事の後、2001年よりIIJグループの緊急対応チームIIJ-SECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会等、複数の団体の運営委員を務める。IIJ-SECTの活動は、国内外の関係組織との連携活動を評価され、平成21年度情報化月間記念式典にて、「経済産業省商務情報政策局長表彰(情報セキュリティ促進部門)」を受賞した。

土屋 博英(1.2 インシデントサマリ)
土屋 博英 鈴木 博志(1.3 インシデントサーベイ)
鈴木 博志(1.4.1米国および韓国におけるDDoS攻撃)
永尾 禎啓 須賀 祐治(1.4.2 TCPの脆弱性(Sockstress))
土屋 博英(1.4.3無作為に到着するSIPパケット)
IIJ サービス事業統括本部 セキュリティ情報統括部

協力:
大原 重樹 サービス事業統括本部システム基盤統括部システム開発課
加藤 雅彦、根岸 征史 IIJ サービス事業統括本部 セキュリティ情報統括部

＊64 例えば、米国の法執行機関(連邦捜査局等)と連携してサイバー犯罪に取り組んでいるIC3(Internet Crime Complaint Center)から注意喚起が出ている(http://www.ic3.gov/media/2008/081205-2.aspx)。
＊65 例えば エフセキュア株式会社のブログ「ワン切り詐欺にご用心」(http://blog.f-secure.jp/archives/50260210.html)。
＊66 既知の脆弱性とその脅威に関しては、例えば以下の報告書等を参照のこと。IPAによる「SIPに係る既知の脆弱性に関する調査報告書 改訂第2版」(http://www.ipa.go.jp/security/vuln/vuln_SIP.html)。
＊67 VoIPネットワークの境界等に設置され、SIPパケットの内容に応じて必要なポートの制御を行ったり、NAT環境下でも正常にVoIPの通信が行えるように制御を行う装置。