1. インフラストラクチャセキュリティ

1.1 はじめに

このレポートは、IIJが対応したインシデントとその対応の実態をまとめたものです。IIJ自身がインターネットの安定運用のために取得している一般情報や、インシデントの観測環境の情報、サービスに関連する情報、協力関係にある企業や団体から得た情報をもとにしています。その情報の内容は、単純な通信量から社会情勢に至るまで、多様なものとなっています。
一部の予備的な調査を除き、ここでは2008年6月から8月の3ヵ月間に発生したインシデントや観測状況を示しています。この3ヵ月の間にも様々なインシデントが発生していますが、ここではその中から代表的なものを紹介します。

この期間には、洞爺湖サミットや北京オリンピック等の国際的なイベントがありました。これらのイベントについてはインターネット上では関連するインシデントの発生は見られず、イベント自体も無事に終了しています。一方で、グルジアにおける武力衝突にともない、国際的なDDoS攻撃が発生しました。日本から遠く離れた国の出来事ですが、ボット等のマルウェアに感染することで、その攻撃に荷担させられたクライアントが日本国内にも存在していました。

脆弱性の分野では、DNSキャッシュポイズニングの問題が大きく取り扱われました。IIJにおいてもこの問題への対応は可能な限り迅速に実施しました。また、この期間に2Gbpsを超える規模の攻撃が発生し、対策を行いました。これは今までにIIJが取り扱ったDDoS攻撃の中でも最大級のものです。
インターネットの上では、ネットワークを経由して感染活動を行うマルウェアの活動も依然として活発であり、セキュリティ対策を行っていないクライアントをインターネットに接続すると、短時間で何らかのマルウェアに感染してしまうような状況が継続しています。また、本年影響の大きかったインシデントの調査を実施した結果、SQLインジェクション攻撃、マルウェア感染に誘導する迷惑メール等のインシデントが継続して発生していることが明らかになりました。

インターネット全体の安定性を脅かすようなインシデントの発生は避けられましたが、個人の利用者やネットワークの管理者一人一人が適切にセキュリティ対策を実施しなければ、安心してインターネットを利用できない状況が続いています。

1.2 インシデントサマリ

ここでは、2008年6月から8月の期間にIIJが取り扱ったインシデントの代表的なものを抽出し、その対応の実態を解説します。この期間に取り扱ったインシデント全体の件数の分布を図-1 に、分類の説明について表-1 に示します。

■脆弱性

この期間中において、複数の実装に脆弱性が発見されており、それぞれに対策を実施していますが、ここでは大きく話題となった2つの問題への対応を示します。

■ DNS キャッシュポイズニングの問題への対応

DNS キャッシュポイズニング*1 の問題は古くから繰り返し指摘され、対策されてきたものですが、今回は今日一般的に利用されている DNS の実装においても、非常に短い時間で攻撃を成立させる手法が発見されました。7月8日、複数のセキュリティ団体による注意喚起*2 や実装の修正リリースがあり、可能な限り速やかに対応しました。また、詳細情報から検証コードを作

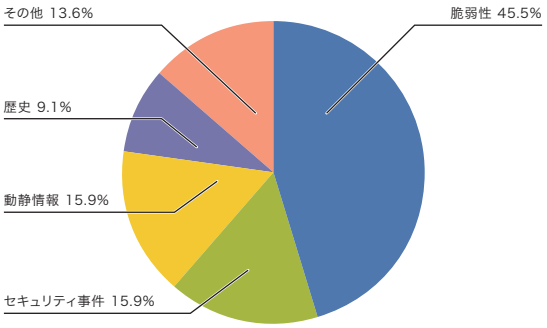

図-1 カテゴリ別比率（2008年6月〜8月）

表-1 インシデントの分類

カテゴリ名	内容
脆弱性	インターネットで利用している、またはユーザの環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェア等の脆弱性への対応を示します。脆弱性そのものや、脆弱性に対する攻撃の情報、攻撃の検証作業、ベンダによる脆弱性への対応情報、対応作業等が該当します。
動静情報	国内外の情勢や国際的なイベントに関連するインシデントへの対応を示します。要人による国際会議や、国際紛争に起因する攻撃等への対応で、注意・警戒、インシデントの検知、対策といった作業が該当します。
歴史	歴史上の記念日等で、過去に史実に関連して攻撃が発生した日における、注意・警戒、インシデントの検知、対策等の作業が該当します。
セキュリティ事件	突発的に発生したインシデントとその対応を示します。ネットワークワーム等のマルウェアの活性化や、特定サイトへの DDoS 攻撃等で、原因のはっきりしないインシデントへの対応が含まれます。
その他	上記のいずれにも該当しないインシデントを示します。イベント等によるトラフィック集中等、直接セキュリティに関わるものではないインシデント等も含まれています。

＊1　今回の攻撃手法の発見者による発表資料（http://www.doxpara.com/DMK_BO2K8.ppt）
＊2　JPCERT/CC による「複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性」等（http://www.jpcert.or.jp/at/2008/at080013.txt）

成し、問題があると指摘された実装に対し、実際に攻撃が可能であることを確認しています。加えて、8月の発表の場[*3]にスタッフを参加させ、発見者自身による発表で攻撃手法について確認しています。

■ BGPプレフィックス・ハイジャッキングの問題への対応

8月のセキュリティカンファレンス[*4]において、特定のネットワークの経路を誘導することで、通信の遮断や通信内容の取得を行う手法（BGPプレフィックス・ハイジャッキング[*5]）の発表と実演が行われました[*6]。今年2月に発生したYouTubeのハイジャック事件[*7]のように、ISPの設定ミスが全世界に影響をおよぼす事態に発展してしまうことも事実です。IIJではこの問題を以前から把握しており、適切なプレフィックス・フィルタの運用強化等、IIJとして可能な対策を実施するだけではなく、この現象の発見システムの開発・運用プロジェクト[*8]等に参画し、他のISPと協調することで、この問題を悪用したインシデントの早期の発見と収束に努めています。

■動静情報

国内外で発生した事件や事故、ニュースや動静情報に応じて、インターネット上でもインシデントが発生することが多くなっています。

■国際的なイベントへの対応（洞爺湖サミット、北京オリンピック）

洞爺湖サミット開催期間及び関連会合の期間中、IIJは、加盟するセキュリティ関連団体「Telecom-ISAC Japan[*9]」からの依頼に応じ、他のISPと共同でインターネット上での攻撃発生について警戒を行いました。また、北京オリンピックについても、中国のセキュリティ関連組織からの要請に応じて警戒を行うと共に、当該組織との間に直接の連絡窓口を開設し、インシデント発生時に相互に緊急連絡を行う体制を構築しました。結果として、両イベント共に関連するサイト等への攻撃は見られませんでした。

■グルジアに対するDDoS攻撃への対応

グルジアにおける争乱と同時に、インターネット上でもDDoS攻撃[*10]が発生していました。関連する国際団体等[*11]から、この攻撃に荷担している疑いのある日本のIPアドレスの情報を入手しましたが、調査の結果、IIJに関わるIPアドレスは存在しませんでした。

■歴史

過去に攻撃が発生したことのある日、特に、歴史上の記念日については、攻撃が再発する可能性があるため、要注意日として取り扱っています。この期間には日本における終戦記念日が含まれていたため、各種の動静情報に注意を払いましたが、IIJの設備及びIIJのユーザのネットワークに対する攻撃は見られませんでした。

■セキュリティ事件

脆弱性や動静情報等に結び付かず、原因のはっきりしない突発的なインシデントをセキュリティ事件として

＊3　Black Hat USA 2008（http://www.blackhat.com/html/bh-usa-08/bh-us-08-main.html）
＊4　DEFCON16（http://www.defcon.org/）
＊5　BGPプロトコルによる経路情報の交換において、本来権限のないIPアドレス空間に対する経路を広告することで、他人のネットワークに向かった通信を指定した宛先に引き込む行為。設定ミス等でも発生する。
＊6　DEFCON16における発表者による資料（https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf）
＊7　YouTubeに対するハイジャック事件については、RIPEによる報告が詳しい。（http://www.ripe.net/news/study-youtube-hijacking.html）
＊8　国内ではTelecom-ISAC Japanの「経路奉行」プロジェクトへの参画等（http://www.janog.gr.jp/meeting/janog19/files/irr.pdf）
＊9　財団法人日本データ通信協会 テレコム・アイザック・ジャパン（https://www.telecom-isac.jp/）
＊10　Distributed Denial of Service攻撃の略。非常に多くの攻撃元から1つの攻撃先に対して実施される攻撃で、その目的は攻撃先のサービスや事業を停止させることにある。
＊11　IIJの加盟する国際団体は複数あるが、そのうちのFIRST等。（http://www.first.org/）

分類しています。この期間においても、OSのアップデートを阻害するウイルスの流行や、偽のセキュリティソフトウェア等、様々なインシデントが発生しました。IIJでは、ニュースサイトを騙る迷惑メールに注目し、迷惑メールからマルウェア*12の感染に誘導される過程について調査を実施しました（「1.4.2 マルウェア感染に誘導する迷惑メール」をご覧ください）。

■その他

直接セキュリティに関係しない現象が、インターネットの安定的な運用に影響を与えるような通信量の変動や、アクセス集中等を引き起こす場合があります。IIJでは、この期間の７月初旬に、突発的な通信量の減少を観測しました。これは、7月のマイクロソフトのOSアップデートで再起動を必要としたため、常時通信を行うP2P型ファイル共有アプリケーション等を利用している端末において、通信が停止したためではないかと判断しています。

1.3 インシデントサーベイ

IIJではインターネット上で発生するインシデントのうち、インフラストラクチャ全体に影響を与える可能性があるインシデントに注目し、継続的に調査を行っています。ここでは、そのうちDDoS攻撃及びネットワーク上のマルウェアの感染活動について、その調査と分析の結果を示します。

1.3.1 DDoS 攻撃

DDoS攻撃は、日本国内においては2003年頃から観測されていました。2004年のサッカーの試合に関連して発生したDDoS攻撃を皮切りに、その対象や攻撃規模は徐々に大きくなり、今日では一般の企業のサーバが対象となった攻撃が、日常的に発生するようになっています。

DDoS攻撃では、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、大量の通信を発生させて通信回線を埋めることや、サーバを過負荷にすることで、サービスを妨害しようとします。ここで、2008年6月から8月の期間にIIJが取り扱ったDDoS攻撃の実態を図-2に、また期間中最大のDDoS攻撃における最大

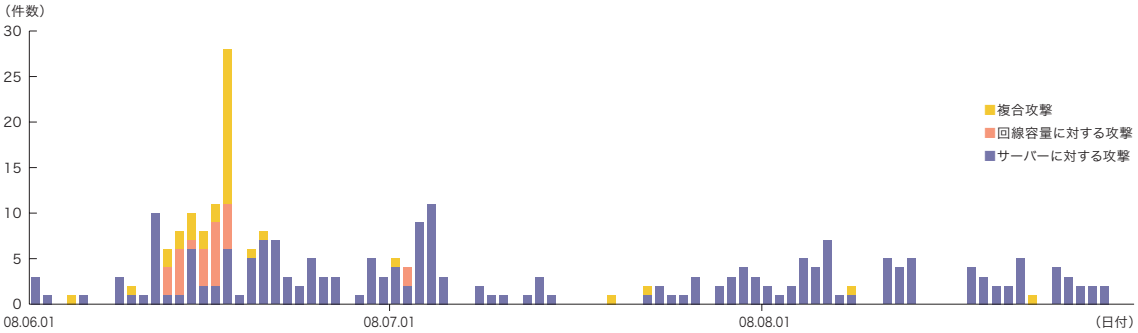

図-2 DDoS攻撃の対処件数

*12 パソコン上のデータの破壊や不正コピー、DDoS攻撃や迷惑メール送信の実施等、パソコン内部やインターネットに対して利用者の意図しない悪性活動を行うソフトウェア。その動作によってウイルスやワーム、ボット等に分類される。

通信量の推移を図-3に示します。対処件数の情報は、攻撃と判定された異常を件数で示したものです。IIJでは、様々なサービスをご利用のお客様に対する攻撃等に対処していますが、正確な攻撃の様子を把握することが困難な場合については、今回の集計からは除外しています。この期間の1日の平均は3件程度、合計272件の攻撃に対処しました。

DDoS攻撃には多くの手法が存在します。また、攻撃対象となった環境の規模（回線容量やサーバの処理能力）によって影響が異なります。図-2の集計では、DDoS攻撃全体を、「回線容量に対する攻撃」と「サーバに対する攻撃」及び「複合攻撃」に分類しています。ここで、「回線容量に対する攻撃」[*13]は、大きなサイズのIPパケットを大量に送付することで攻撃対象の接続回線容量を圧迫するような攻撃です。「サーバに対する攻撃」[*14]は、TCPの呼に相当するSYNパケットを大量に送付することや、実際に同時に大量のTCP接続を行うことで、対象サーバを過負荷に陥れることを狙った攻撃です。「複合攻撃」は、1つの攻撃対象に対し、同時に複数種類の攻撃を観測した状況を指しています。

この期間のDDoS攻撃の発生件数では、回線容量に対する攻撃が10%、サーバに対する攻撃が77%、複合攻撃が13%となりました。サーバに対する攻撃が数多く発生していますが、それぞれは大規模なものではありませんでした。一方で、回線容量に対する攻撃や複合攻撃では、特に通信量に関して増加傾向にあります。これは、サーバに対する攻撃が非常に小さいパケットで構成され、攻撃者側のネットワーク装置等に過負荷を与えるため、攻撃者が攻撃を継続しにくいためではないかと予測しています。

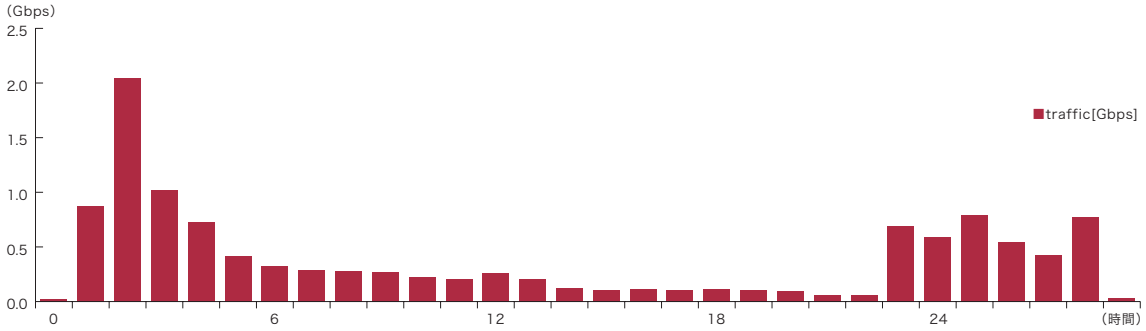

図-3 期間中最大のDDoS攻撃の様子

＊13 攻撃対象に対し、本来不必要な、大きなサイズのパケットや、その断片を大量に送りつけることで、回線を圧迫する攻撃。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。

＊14 TCP SYN flood攻撃は、TCPで接続開始の呼を示す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接続を確立した後、HTTPのプロトコルコマンドGETを大量に送付することで、やはり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。

また、攻撃の継続時間については、全体の72%が攻撃開始から30分未満で終了し、残りの28%が30分～24時間の範囲で分布しています。ごく少数ではあるものの、数日間にわたって継続する攻撃にも対応しています。攻撃の規模と攻撃期間との間に有意な関係は見られませんでした。
攻撃元の分布については、多くの場合、国内、国外を問わず、非常に多くのIPアドレスが観測されています。これは、IPスプーフィング[*15]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[*16]の利用によるものと考えられます。

この期間の最大の攻撃は回線容量に対する攻撃で、2Gbps[*17]を超えるものでした。これは、IIJが対処した中で最大級の攻撃です。この攻撃の内容は時間と共に変化し、回線に対する攻撃（UDP floodとICMP flood）の組み合わせで始まり、途中でサーバに対する攻撃を試みた後、再び回線に対する攻撃に戻っています。攻撃元アドレスのばらつきはあまり大きくないため、ボットネットによる攻撃ではなく、専用ツールを使った攻撃であると判断しています。

1.3.2 マルウェアの活動

ここでは、IIJが昨年から実施しているマルウェアの活動観測プロジェクトMITF[*18]による観測結果を示します。MITFは2007年4月から開始した活動で、ハニーポット[*19]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、技術情報を集め、対策につなげる試みです。これらのハニーポットは、インターネットに一般利用者と同様に接続していますが、ハニーポットから通信を発生させることはありません。つまり、このハニーポットで受信した通信は、すべて本来到着するはずのない不要な通信です。そのほとんどが、マルウェアによる無作為に宛先を選んだ通信か、攻撃先を探すための探索の試みであると考えられます。

＊15 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。
＊16 ボットとは、感染後に外部の指令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。
＊17 Bit Per Secのことで、1秒あたりの通信量を示す。
＊18 Malware Investigation Task Forceの略。マルウェアの活動状況を把握することを目的としたIIJのタスクフォース。
＊19 脆弱性のエミュレーション等の手法で、攻撃を受け付けて被害にあったふりをすることで、攻撃者の行為や、マルウェアの活動目的を記録する装置。

■無作為通信の様子

まず、この期間に、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-4に、その発信元IPアドレスの分布を国別に図-5に示します。

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）についてこの期間の推移を示しています。多くはマイクロソフトのOSで利用されているTCPポートであり、クライアントに対する探索行為であることが分かります。一方で、2582/tcpや22133/udp等、一般的なアプリケーションで利用されない目的不明の通信も観測されています。また、発信元の分布を国別にみると、日本国内合計の43%、中国の27%が比較的多いものの、その他は世界中の国々からさほど変わらない量の通信が到着しています。図中では発信元となった国内ISPの分布も示していますが、特に大きな傾向は見られません。

以上のように、ネットワーク上では、攻撃相手を探索する行為が継続しています。しかし、今日では多くのクライアント用のセキュリティ製品が登場し、また、最新のOSではファイアウォール機能が利用できるようになっていますので、これらの機能の利用により防御は可能です。

■ネットワーク上でのマルウェアの活動

次に、MITFの観測環境において取得した、マルウェアの活動について示します。この期間におけるマルウェア

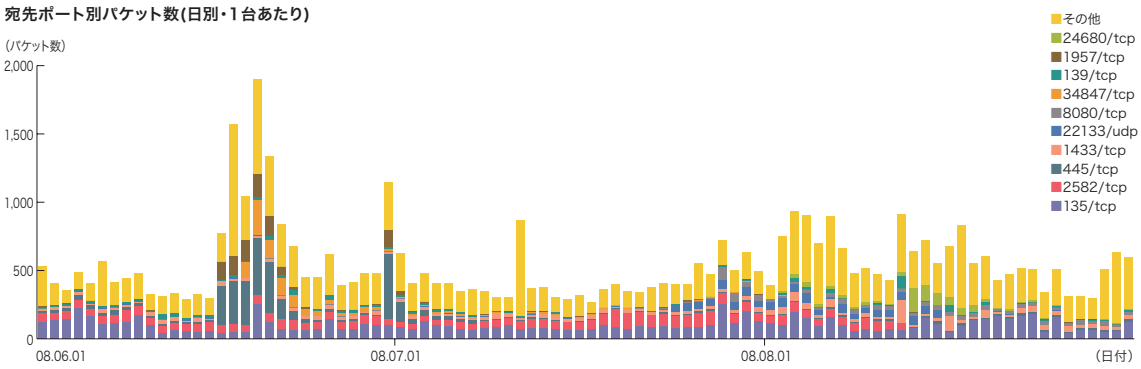

図-4 ハニーポットに到着した通信の推移（日別・宛先ポート別・一台あたり）

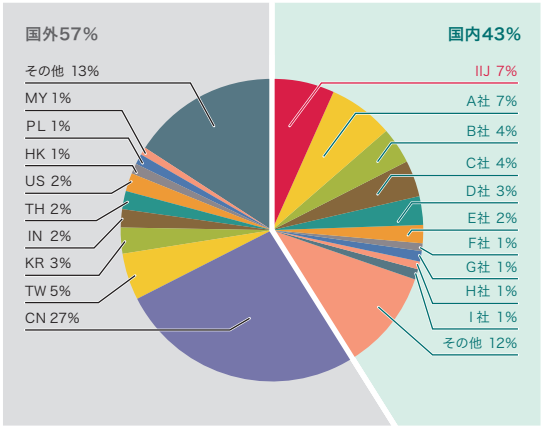

図-5 発信元の分布（全期間）

の検体[*20]取得数の推移を図-6に、マルウェアの検体取得元のIPアドレスの分布を図-7に示します。

検体取得数の推移では、総取得検体数は1日あたりに取得できた検体の数を示し、ユニーク検体数はハッシュ値[*21]で検体の種類を調べたものです。総取得検体数では一日平均で8,000ほどの検体を取得しています。また、ユニーク検体数は、毎日定常的に60種類程度のマルウェアを取得しています。これらの数字は、MITF開始以後大きく変化していません。この結果と、国内の他の試み[*22]の結果と比較すると、IIJの観測では、より数少ない種類のマルウェアの活発な活動が観測されています。これは、現在のマルウェアの感染活動が、非常に局所的であることを示していると考えられます。

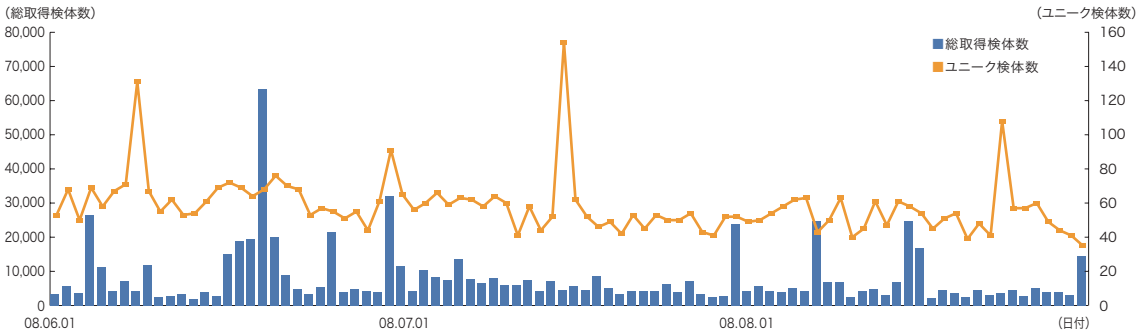

図-6 取得件対数の推移（総数、ユニーク検体数）

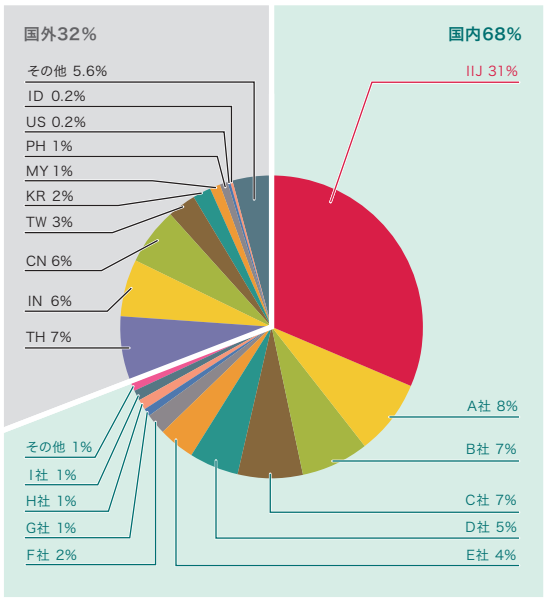

図-7 検体取得元の分布（全期間）

＊20 ここでは、ハニーポット等で取得できたマルウェアを指す。
＊21 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。
＊22 例えば、官民連携プロジェクトであるサイバークリーンセンターの活動実績等。（http://www.ccc.go.jp/）

次に、検体取得元の分布では、68%が日本国内であり、全体の31%がIIJとなっています。MITFによる観測開始以後、日本国内比率は大きく変化していませんが、IIJのユーザを発信元としたマルウェア感染活動は40%程度から30%程度に減少しています。
MITFでは、マルウェアの解析環境を用意し、取得できた検体について独自の解析を行っています。この結果、この期間に取得できた検体の内訳は、ワーム型4.2%、ボット型68.8%、ダウンローダ型27.0%となりました。また、この解析により、84個のボットネットC&Cサーバ[*23]と531個のマルウェア配布サイトの存在が明らかになりました。

この観測状況を受け、IIJでは、大規模なマルウェア感染活動を発見した場合、そのユーザに連絡をし、マルウェアの駆除をお願いする形での対策を行っています。また、この観測結果を、複数のアンチウイルスソフトウェアベンダや、一部の協力企業の研究所等に提供することで、アンチウイルス製品での対策や、対策手法の検討等を推進しています。

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を行い、対策につなげています。ここでは、この期間で影響の大きかったインシデントに対する様々な調査のうち、WebサーバへのSQLインジェクション攻撃、マルウェア感染に誘導する迷惑メール、P2Pネットワークに起因する不要な通信、の3つのテーマについて、その調査結果を示します。

1.4.1 WebサーバへのSQLインジェクション攻撃

Webサーバに対する攻撃のうち、本年流行が見られるSQLインジェクション攻撃[*24]について調査を行いました。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。この攻撃が成立すると、Webサーバの背後にあるデータベースの内容が漏えいしたり、Webのコンテンツが改ざんされる等の被害につながります。また、本年流行した攻撃では、コンテンツが改ざんされた結果、マルウェアの配布サイトに誘導する仕組みが埋め込まれていました。このような攻撃では、改ざんされたコンテンツにアクセスしたクライアントにマルウェアを感染させることで、クライアントPCの制御を奪うことや、クライアント内部の情報（ID、パスワード等）を盗み出すことが最終的な目的となっています。

＊23 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ためのサーバ。
＊24 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、その背後の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、情報の入手やWebコンテンツの書き換えを試みる。

まず、この期間に検知したWebサーバに対する攻撃の推移を図-8に示します。
これは、IPSのシグネチャによる攻撃の検出結果について、Webサーバに対する攻撃で、かつSQLに関連するものをまとめたものです。
これらの図から、まず、SQLインジェクション攻撃が依然として継続していることが分かります。また、全体として、攻撃の大半は日本国内からのものでした。攻撃元と攻撃先、及び攻撃手法の組み合わせについて解析したところ、今回観測したSQLインジェクション攻撃については、次の3種類の傾向があることが分かりました。

■データを盗む試み
Webサーバの背後にあるデータベースに蓄積された情報を閲覧しようとする試みです。少数特定のWebサーバが標的となっています。期間中に数回見られる検出数のピークは、短い時間に集中して行われたこの攻撃によるものです。また、攻撃元は、日本国内の少数のIPアドレスのみでした。

■データベースサーバに対して過負荷を与える試み
情報を検索する命令等を送付してデータベースサーバに負荷を与えたり、その処理を停止させたりすることで、データベースやWebサーバに対するDoS攻撃[*25]を成立させようとする試みです。データを盗む試みと同様に、少数特定のWebサーバが標的となっていますが、

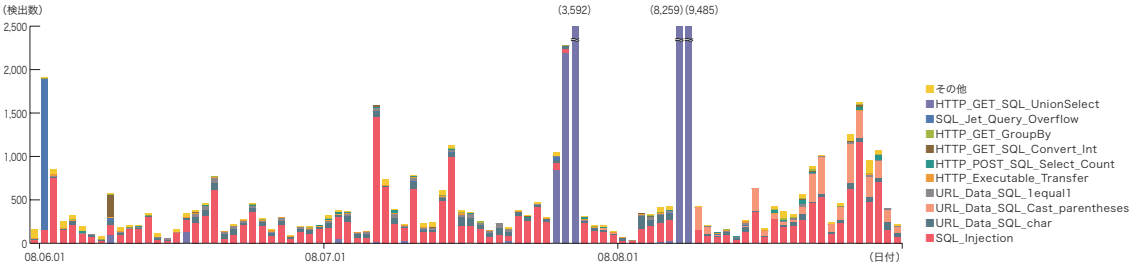

図-8 SQLインジェクション攻撃の推移(日別、攻撃種類別)

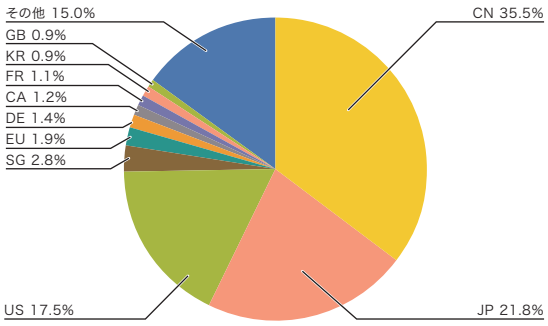

図-9 SQLインジェクション攻撃の発信元の分布(全期間)

*25 Denial of Service攻撃。サービス妨害攻撃。DDoS攻撃とは異なり、脆弱性等を悪用している場合があり、1つのパケットで攻撃対象を停止させることもある。

今回の調査では、この攻撃については比較的長い時間継続する傾向にありました。攻撃元は国内外の複数のIPアドレスとなっていますが、その分布の規模は大きくなく、Open Proxy[*26]等を利用しているものと判断しています。

■コンテンツ改ざんの試み

本年流行したWebのコンテンツを改ざんするような試みです。複数のWebサーバに対する特定の発信元からの攻撃が検出されていることから、コンテンツの改ざんが可能なWebサーバを探して、無作為に攻撃を行っている様子がうかがえます。

データを盗む試みと過負荷を与える試みを除外した情報を元に、攻撃の発信元アドレスの国別分布を作成し、図-9として示します。攻撃元の傾向は、多い順に中国35.5%、日本21.8%、米国17.5%となり、以下その他の国が続いています。

これらの攻撃についてはそれぞれ適切に検出され、対応が実施されています。しかし、攻撃の試みが継続していることから、インターネット上には依然としてSQLインジェクション攻撃に対して脆弱なWebサーバが存在していると考えられます。また、今回の調査は、SQLインジェクション攻撃の状況を把握するためのものでした。今後は、改ざんされた結果、特にマルウェア感染に誘導する様子を把握するための調査を行う予定です。

1.4.2 マルウェア感染に誘導する迷惑メール

この調査では、迷惑メールからマルウェア感染に誘導する仕組みの実態と量について調査を行いました。あるメールアドレスに8月の間に到着した迷惑メールをサンプルとし、これらのメールの本文からWebサーバに誘導するURLを抽出します。Webクライアントの機能を有するクローラ[*27]を利用して、抽出したURLに実際にアクセスすることで、マルウェアをダウンロードさせたか否かを判定しています。メールからURLの抽出を行うプログラムとWebクローラは、この調査のために新規に開発しました。

調査の結果、1ヵ月間に到着した2,683通の迷惑メールの本文に、3,348個のURLが存在し、そのURLをクロールすることで、158個のマルウェアの検体を取得することができました。今回の問題についての説明を図-10に、調査対象と迷惑メールとマルウェアの関係を図-11に、取得できたマルウェアの種類の分布を図-12に示します。

またマルウェアへ誘導する際、以下のような手法が使

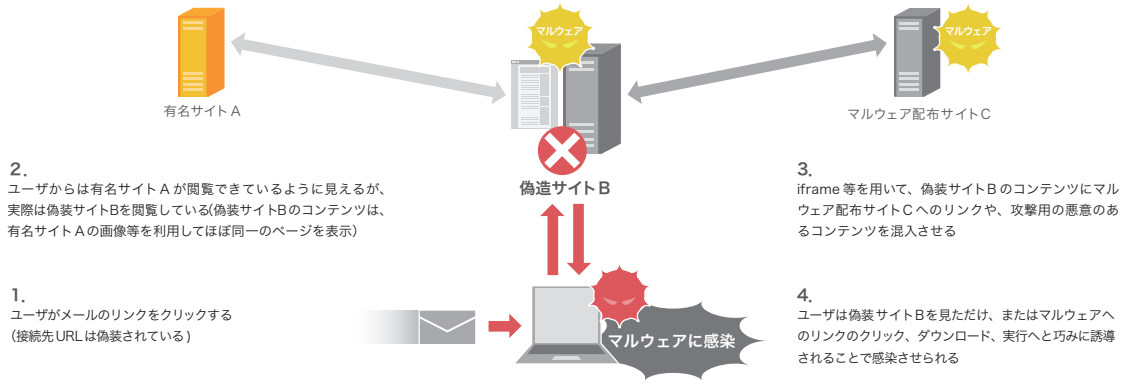

図-10 迷惑メールからマルウェア感染に誘導する様子

＊26 設定ミスや故意により、インターネットに対し広く解放され、誰からでも利用できるようになっているProxyサーバ。攻撃の踏み台として利用されることもある。
＊27 与えられたURLに自動的にアクセスし、そのコンテンツを収集するプログラム。

用されていることが分かりました。

■迷惑メールでURLを隠ぺいする試み
検索エンジンのリダイレクト機能を利用して、一見すると検索エンジンへのリンクに見える、またはHTMLメールにおいて実際のリンクを隠ぺいする等の手法が用いられていました。

■偽装Webサイトの試み
有名サイトの偽装サイトを作成する際、元のサイトのコンテンツをコピーしたり、リンクにより元のサイトのコンテンツをそのまま利用したりすることで、よりユーザが気付きにくくする工夫が施されていました。

■マルウェアをダウンロードさせるための試み
JavaScript[*28]によってブラウザやプラグインの脆弱性をついて自動的にファイルをインストールさせたり、自動的にダウンロードを開始させたりする機能が利用されていました。また、このようなJavaScriptには難読化が施されており、そのソースからは処理内容が把握しにくくなっていました。この他にも動画を見るために必要なファイルを偽って、マルウェアをインストールさせるといった手口も用いられていました。

今回取得できたマルウェアの種類は限られたものでしたが、調査の結果マルウェアに誘導されたURLを1つ以上含むメールの数は、全体数の2.8%となりました。迷惑メール全体の数を考慮すると、これは非常に大きな数であると判断しています。

今回の調査は特定のメールアドレスに到着した迷惑メールを元にしており、そのメールの分布がユーザに到着する迷惑メールの分布とは異なる可能性があります。このため、よりユーザに近い環境を用意し、そこに到着した迷惑メールに関する調査を開始しています。

1.4.3 P2Pネットワークに起因する不要な通信

「1.3.2 マルウェアの活動」に示したように、今日では、インターネットに接続しただけである程度の不要な通信が到着しますが、突然、多くの発信元から特定のTCPポートに対して接続要求を受けることがあります。この場合、ファイアウォール等の警告が数多く発生しますが、多数の発信元から特定のポートへの警告であるため、何か、特別に狙われているのではないかと、不安に駆られるユーザもいるようです。ここでは、このような通信がP2Pソフトウェア[*29]の影響によるものであると確認した実験の様子を示します。

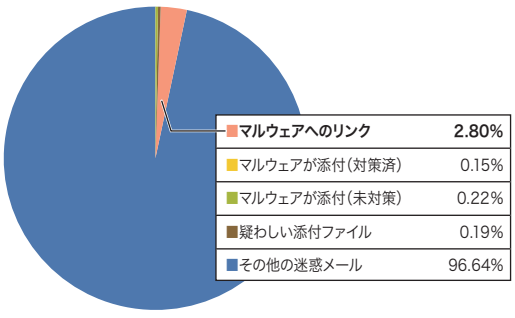

図-11 迷惑メールとマルウェアの関係

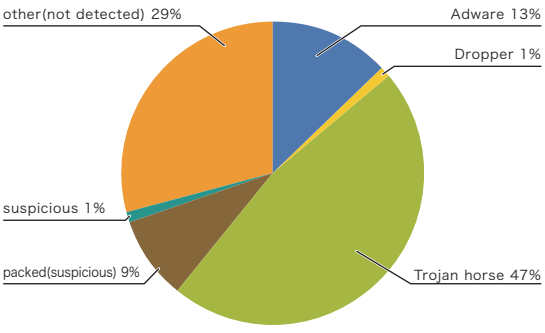

図-12 取得したマルウェアの種類の分布

*28 Webブラウザ上で動作するスクリプト。
*29 構成要素が相互に通信することでネットワークを形成するようなソフトウェア。

P2P ネットワークでは各ノード*30 が相互に通信を行っており、一般に、新たな参加者は既存のノードリスト等の手がかりを元に P2P ネットワークに参加します。逆に、時間に応じて P2P ネットワークから消えていくノードも存在します。こうしたノードの状態の変動は他のノードも伝えられ、P2P ネットワークを動的に維持しています。

一方、ブロードバンド接続の多くでは、接続の度に動的に IP アドレスが割り振られます。ある時割り振られた IP アドレスについて、そのアドレスの前のユーザが P2P ソフトウェアを利用していた場合に、そのIP アドレスが P2P ノードでなくなったことを知らない他の P2P ノードから、現在のユーザに対して接続要求が届く可能性が考えられます(図 -13)。P2P ネットワークにおいて、ノード管理が適切に行われていればこのようなことは発生しませんが、現実には、P2P ソフトウェアの実装は様々です。そこで、実際にこの事象が発生するかどうかを検証するために、専用の環境を構築しました。

まず、データセンタに観測用のサーバと P2P ソフトウェアを稼働させるホストを用意し、過去に P2P ソフトウェアを利用していないことが分かっている IP アドレスを利用しました。実装の調査は Skype (3.6.0.248)、Winny (2b71)、Share (ex2)の 3 つを対象としています。これらを 24 時間稼働させて終了させ、その後、送られて来るパケットを記録しました(観測結果の例として、図 -14 をご覧ください)。

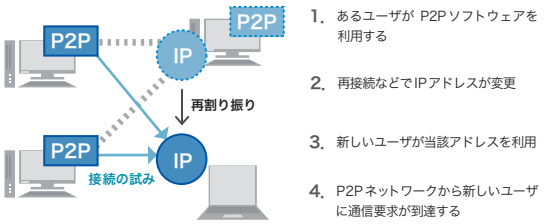

図 -13 P2P ネットワークにより不要な通信が発生する様子

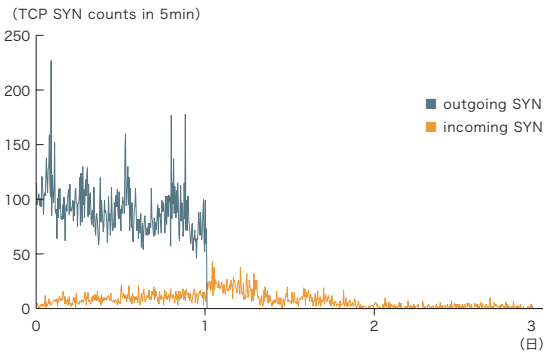

図 -14 P2P ネットワークの通信の様子(Share・3 日間)

■ Skype の観測結果

Skype では終了後、12 時間程度の間 TCP SYN*31 の到着を観測しましたが、5 分あたり 4 個程度の頻度であり、P2P を利用しないでも到着する不要な通信とほぼ同程度の数となりました。5 日後にあるホストからの接続を受信したものの、その後は 6ヵ月以上に渡り、新しい TCP SYN を観測していません。

■ Winny の観測結果

Winny では終了後、9 時間程度は 5 分あたり 20 個と多くの TCP SYN を観測しました。その後も 2 週間程度は断続的に 5 分あたり 3 個程度の TCP SYN を観測しました。25 日後に最後の TCP SYN を受信した後、5ヵ月以上に渡って新しい TCP SYN を観測していません。

*30 P2P ネットワークの構成要素。特定のノードは、クライアントとして動作するだけではなく、同時に他のノードに対してサーバとしても動作する。
*31 TCP 接続の呼をあらわす、通信要求のパケット。

■ Shareの観測結果

Shareでは終了後、24時間程度は5分あたり10～30個と多くのTCP SYNを観測しました。その後徐々に頻度は減っているものの、長期に渡って5分あたり2～6個程度のTCP SYNを断続的に受信しています。利用終了から6ヵ月経った現在でも、月に2個程度ではあるもののTCP SYNを観測しています。

今回の条件では、Skypeは比較的早く収束しましたが、WinnyやShareでは終了後も長期に渡って接続要求を受信しました。これにはP2Pノードのノードリストの管理方法の違いが関連しています。WinnyやShareでは、再起動時には前回の終了時に保存された他のノードの情報を手がかりにP2Pネットワークへの参加を試みるため、長期にわたって接続要求が観測されたと考えられます。つまり、すべてのノードの保存情報からノード情報が削除されるまでは、継続的に接続要求を受信する可能性があるのです。

今回の調査ではP2Pソフトの利用終了後も接続要求を受信することが分かりました。特にP2Pソフトの実装や利用方法の違いによって、利用終了直後に接続要求が活発に到着する期間があることや、少量ではあるものの、長期に渡って到着する様子が明らかになっています。このような現象が、インターネットに接続した際に身に覚えのないパケットを受信する原因の一つとなっていると言えるでしょう。

1.5 おわりに

このレポートでは、IIJが対応を行ったインシデントについてまとめました。ここに記載したインシデントがすべてではありませんが、これらの情報だけでも、ISPがIPパケットの転送だけを行っていた時代は終わり、自らが提供しているネットワークの中で発生するインシデントについての知識を持たなければ、インターネットを安定的に提供することができない時代になっていることを示していると考えています。

このために、IIJでは、従来運用のために取得、利用していたネットワークの情報に加え、個別のインシデントに関する観測の仕組みを整備してきました。このような観測の結果を利用して、個々のインシデントに対する経験に基づいた早期の対応を実現し、また、対応策をサービスとして提供していきます。

また、このレポートのように、インシデントとその対応について明らかにし、公開していくことで、インターネット利用の危険な側面についてご理解いただき、必要な対応策を講じた上で安全に、安心して利用できるように、努力を継続して参ります。

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の開発等に従事の後、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。

荒田 恵子　永尾 禎啓　桃井 康成　大原 重樹　梅澤 威志　鈴木 博志　石川 哲

IIJ サービス事業統括本部 セキュリティ情報統括部

松崎 吉伸

IIJ ネットワークサービス本部 ネットワークサービス部 技術推進課