Gumblarの再流行

今回は、2009年10月から12月に発生したインシデントに関する報告とともに、10月以降に再発しているGumblarに関する事件、暗号化通信に広く利用されているSSLおよびTLSのプロトコルの脆弱性の解説、P2Pファイル共有ネットワークとその調査技術について取り上げます。

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10月から12月までの期間では、IDとパスワードを盗み取るマルウェアGumblarが再発し、関連するWebサイトの改ざんが数多く報告されています。また、脆弱性に関しては、Webブラウザに関連するものが相次いで発見され、暗号化通信に広く利用されているSSLおよびTLSのプロトコルにも問題が見つかっています。このほか、DNS情報を不正に操作した乗っ取り事件や、天災に便乗したSEOポイズニング事件などが発生しています。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ー

ここでは、2009年10月から12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。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。

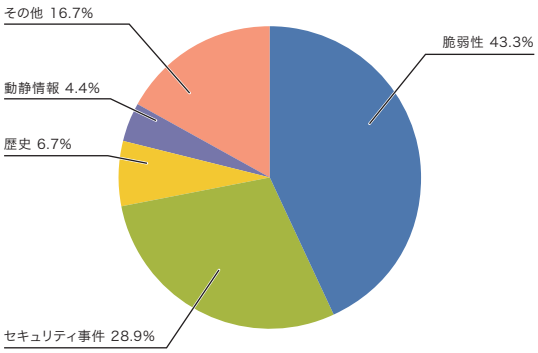


図-1　カテゴリ別比率（2009年10月～12月）

＊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を示す。

■ 脆弱性

今回対象とした期間では、マイクロソフト社のInternet Explorer[*2]、アドビシステムズ社のAdobe AcrobatとAdobe Reader[*3]、Adobe Flash PlayerとAdobe AIR[*4]、Adobe Shockwave Player[*5]、オラクル社のJava Runtime Environment（JRE）[*6]等、Webブラウザに関係する脆弱性が数多く発見され、対策されています。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されました[*7]。

また、時刻同期に利用されるNTPサーバ[*8]やDNSサーバのBIND9[*9]等、広く利用されているサーバにも脆弱性が発見され、対策されています。加えて、多くのサービスで暗号化通信のために利用されている、SSLおよびTLSプロトコルに脆弱性[*10]が発見されました。この脆弱性に関しては「1.4.2 SSLおよびTLSのrenegotiation機能の脆弱性を利用した中間者攻撃」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、11月のオバマ米国大統領や12月の習近平中国国家副主席といった外国要人の来日の動きに注目しましたが、関連する攻撃等は検出されませんでした。

■ 歴史

この期間には、過去に歴史的背景によるDDoS攻撃やホームページの改ざん事件が発生したことがありました。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、アップル社のiPhoneに感染するマルウェアが発見[*11]されました。また、SNS として広く利用されている twitterのDNS情報が不正に操作され、別のWebサイトに誘導される事件[*12]が発生しました。検索エンジンなどの検索結果で詐欺的ソフトウェア（スケアウェア）に誘導される事件も継続して起こっています[*13]。

加えて、10月初旬以降、4月に大規模な活動が認められたGumblar[*14]の活動再開が確認されました。この件に関する詳細は、「1.4.1 Gumblar の再流行」を参照してください。

＊2　マイクロソフト セキュリティ情報 MS09-072 - 緊急Internet Explorer用の累積的なセキュリティ更新プログラム（976325）（http://www.microsoft.com/japan/technet/security/bulletin/ms09-072.mspx）。
＊3　Security updates available for Adobe Reader and Acrobat APSB10-02（http://www.adobe.com/support/security/bulletins/apsb10-02.html）。
＊4　Adobe Flash Player用のセキュリティアップデート公開 APSB09-19（http://www.adobe.com/jp/support/security/bulletins/apsb09-19.html）。
＊5　Security updates available for Shockwave Player APSB09-16（http://www.adobe.com/support/security/bulletins/apsb09-16.html）。
＊6　Oracle Corporation、JavaTM SE 6アップデートリリースノート（http://java.sun.com/javase/ja/6/webnotes/6u17.html）。
＊7　脆弱性が修正される前に攻撃に悪用されることを0-day（ゼロデイ）攻撃という。例えば、この期間中Adobe ReaderおよびAcrobatの脆弱性について、Gumblarもしくはその類似の事件で修正が公開される前に悪用されていることをIIJでも確認している。この脆弱性は、修正が公開される前であっても、Adobe ReaderおよびAcrobatの設定でJavaScriptの利用を禁止することで一時的な対処とすることができた。
＊8　NTPにおけるサービス運用妨害（DoS）の脆弱性 JVNVU#568372（http://jvn.jp/cert/JVNVU568372/index.html）。特殊な要求パケットをNTPサーバに送ることで、応答と要求を無限に繰り返すループを作り出すことができる。
＊9　BIND 9のDNSSEC検証処理における脆弱性 JVNVU#418861（http://jvn.jp/cert/JVNVU418861/index.html）。DNSSEC利用時にキャッシュポイズニングの危険がある。
＊10 SSLおよびTLS プロトコルに脆弱性 JVNVU#120541（http://jvn.jp/cert/JVNVU120541/index.html）。
＊11 このワームの詳細についてはエフセキュア株式会社のblogに詳しい。初のiPhoneワームを発見（http://blog.f-secure.jp/archives/50301814.html）。
＊12 この攻撃の影響については次の公式blogに詳しい。Twitterブログ 昨日のDNS障害についての追加情報（http://blog.twitter.jp/2009/12/dns_19.html）。
＊13 検索エンジンの評価アルゴリズム等を利用し、特定の語句の検索結果として、悪意あるサイトへのリンクが上位に表示されるよう工夫することをSEOポイズニングと呼ぶ。例えば、次のトレンドマイクロ社のBlogでは、クリスマスシーズンに検索されると思われる単語について調査と解説を行っている。トレンドマイクロ社　SEOポイズニング：不正サイトもSEO対策？（http://blog.trendmicro.co.jp/archives/1255）。今回は 2009年9月30日に発生したサモア諸島付近の地震に関連する語句がSEOポイズニングの対象となった。
＊14 Gumblarについては本レポートのVol.4「1.4.2 ID・パスワード等を盗むマルウェアGumblar」でも解説を行っている（http://www.iij.ad.jp/development/iir/pdf/iir_vol04_infra.pdf）。

■ 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、10月に、利用者の多いインターネット掲示板が複数のISPに対して大規模なアクセス制限を行い、一般ユーザの利用に支障が生じる等の影響が発生しました。

また、この期間においては、ユーザが利用するアプリケーション、特にWebブラウザのプラグインの脆弱性を利用した攻撃が数多く発生していたため、アプリケーションやプラグインのバージョンを確認するためのツールがリリースされています（IPA MyJVNバージョンチェッカ[*15]やFirefox PluginChecker[*16]等）。さらに、マイクロソフト社の新しいオペレーティングシステム Windows7が発売され、セキュリティ機能の向上の観点からも注目されました。

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10月から12月の期間に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。

＊15 MyJVN バージョンチェッカでは、利用しているPCにインストールされている対象ソフトウェアのバージョンが確認できる（http://jvndb.jvn.jp/apis/myjvn/）。

＊16 Mozilla Firefox にて次のURLを参照のこと（https://www-trunk.stage.mozilla.com/en-US/plugincheck/）。また、機能としては「ツール（T）」「アドオン（A）」から更新有無の確認を行うこともできる。本機能はFirefoxの機能であり、他のブラウザ、例えばMicrosoft Internet Explorerのプラグインに関しては別の手法での確認が必要となる。

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*17、サーバに対する攻撃*18、複合攻撃（1つの攻撃対象に対し、同時に数種類の攻撃を行うもの）の3種類に分類しています。

この3ヵ月間でIIJは、185件のDDoS攻撃に対処しました。1日あたりの対処件数は2.01件で、平均発生件数は前回のレポート期間のものと大きく変わりはありません。

DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0.5%、サーバに対する攻撃が87.6%、複合攻撃が11.9%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、サーバに対する攻撃で、65万ppsのパケットによって245Mbpsの通信量を発生させています。また、攻撃の継続時間は、全体の77%が攻撃開始から30分未満で終了し、23%が30分以上24時間未満の範囲に分布しています。今回の期間中で最も長い攻撃は、約12時間継続していました。

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*19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*20の利用によるものと考えられます。

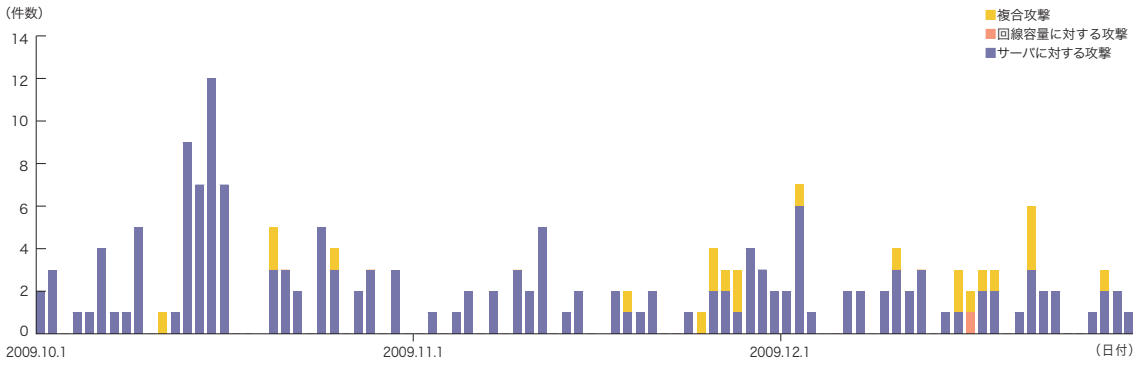


図-2　DDoS攻撃の発生件数

＊17 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。

＊18 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。

＊19 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。

＊20 ボットとは、感染後に外部のC&Cサーバからの命令を受けて攻撃を実行するマルウェアの一種。ボットが多数集まって構成されたネットワークをボットネットと呼ぶ。

1.3.2 マルウェアの活動

ここでは、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[*21]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[*22]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

2009年10月から12月の期間中に、ハニーポットに到着した通信の総量（到着パケット数）の推移を図-3に、その発信元IPアドレスの国別分類を図-4にそれぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、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ポートに対する探索行為でした。また、前回の期間と同様に、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、2582/TCP、31138/TCP等、一般的なアプリケーションで利用されていない目的不明の通信も観測されました。発信元の国別分類を見ると、日本国内の22.6%、中国の20.0%が比較的大きな割合を占めています。

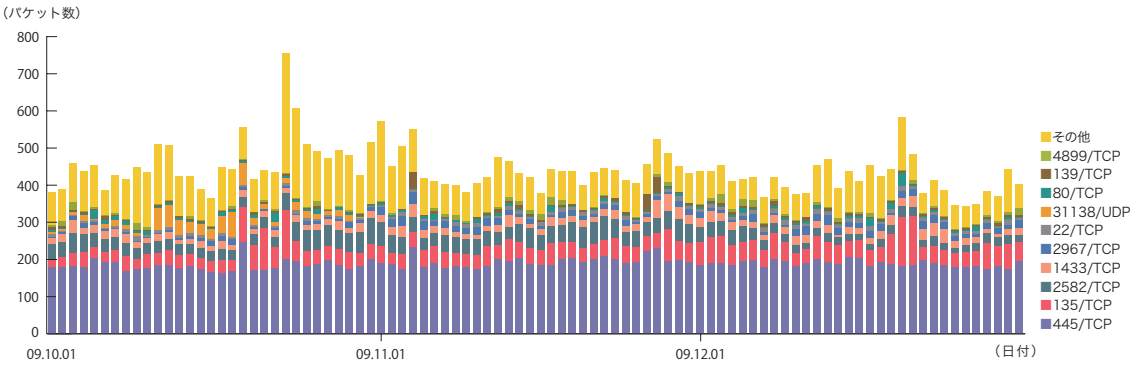


図-3　ハニーポットに到着した通信の推移（日別・宛先ポート別・一台あたり）

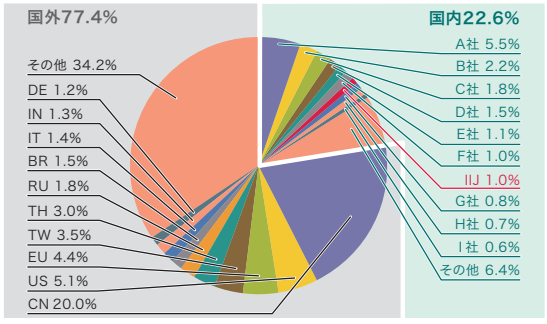


図-4　発信元の分布（国別分類、全期間）

＊21 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、流行状況や技術情報を把握し、対策につなげる試み。

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

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの取得検体数の推移を図-5に、マルウェアの検体取得元の分布を図-6にそれぞれ示します。図-5では、1日あたりに取得した検体[*23]の総数を総取得検体数、検体の種類をハッシュ値[*24]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623、ユニーク検体数が44です。前回の集計期間での平均値が総取得検体数で592、ユニーク検体数で46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前回と同程度の値でした。

検体取得元の分布では、日本国内が60.2%、国外が39.8%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3.0%で、前回の観測期間に続いて低い値を示しています。

MITFでは、マルウェアの解析環境を用意し、取得した検体について独自の解析を行っています。この結果、この期間に取得した検体は、ワーム型4.3%、ボット型93.1%、ダウンローダ型2.6%となりました。また、この解析により、42個のボットネットC&Cサーバ[*25]と519個のマルウェア配布サイトの存在を確認しています。

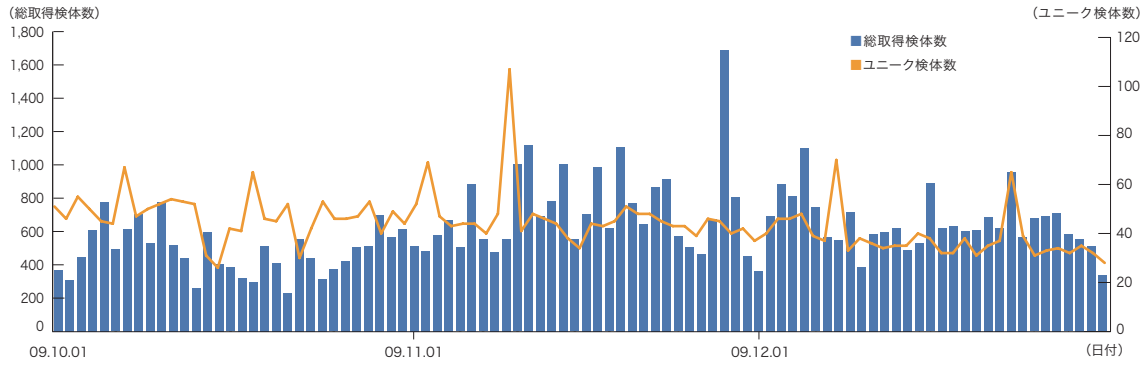


図-5　取得検体数の推移(総数、ユニーク検体数)

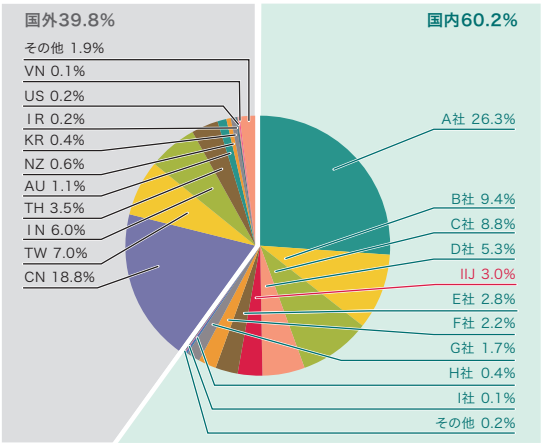


図-6　検体取得元の分布 (国別分類、全期間)

＊23 ここでは、ハニーポット等で取得したマルウェアを指す。

＊24 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。

＊25 Command & Controlサーバの略。多数のボットで構成されたボットネットに指令を与えるサーバ。

1.3.3 SQLインジェクション攻撃

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*26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10月から12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61.7%、中国6.7%、米国5.3%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、前回と同様の発生数となっています。散発的にみられる攻撃の増加は、特定の攻撃元から複数の宛先への攻撃を検知したものです。

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、攻撃の試みは継続しているため、引き続き注意が必要な状況です。

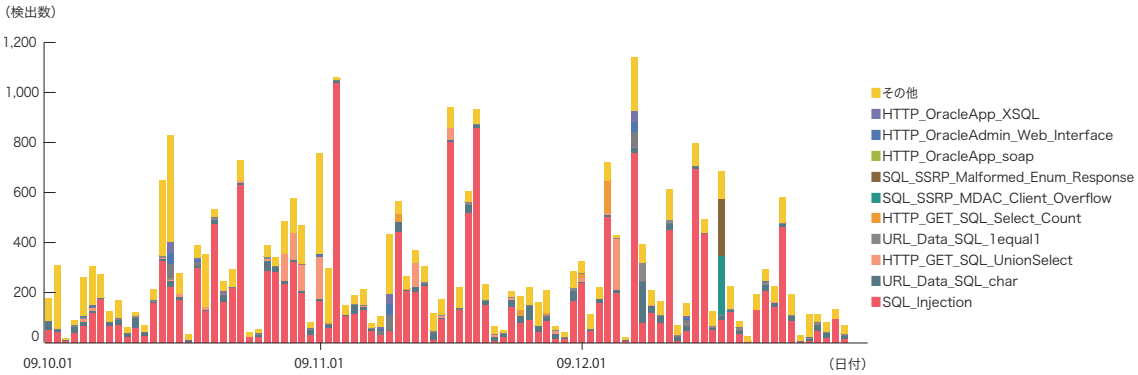


図-7　SQLインジェクション攻撃の推移（日別、攻撃種類別）

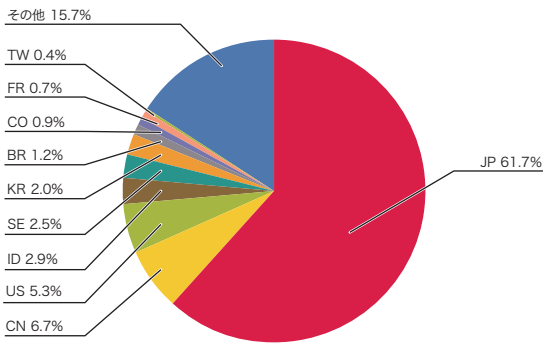


図-8　SQLインジェクション攻撃の発信元の分布（国別分類、全期間）

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

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、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うことで対策につなげています。ここでは、この期間に実施した調査のうち、Gumblarの再流行、SSLおよびTLSのrenegotiation機能の脆弱性を利用した中間者攻撃、P2Pファイル共有ネットワークの調査技術について、その詳細を示します。

1.4.1 Gumblar の再流行

2009年4月以降に流行したマルウェアGumblarが2009年10月から12月にかけて再流行し、被害が拡大しました。ここでは、最近の事件について、前回のGumblarとの違いに着目して解説します*27。

■ 新しいGumblar

Gumblarは、事前に盗み取ったFTPアカウントを悪用したWebコンテンツ改ざんに始まる、マルウェア感染事件です。感染したマルウェアによってIDとパスワードが盗まれ、それが次の改ざんに悪用されることで被害が拡大します。この事件は、複数のWebサイトと複数のマルウェアが関係する複雑な事件です*28。今回の流行は、10月12日頃に複数のWebサイトが改ざんされたことで明らかになり*29、本稿執筆時点でも断続的に発生し続けています。

前回と同様に、今回再発した事件においても、複数のWebサイトを経由してマルウェア感染に誘導する流れは変わっていません。前回はマルウェア配布サイトが専用に用意された少数のサーバでしたが、今回は改ざんされた多数のWebサイトが悪用されています。このため、今回の流行では、マルウェア配布サイトへのアクセスを禁止したり、そのサイトを停止（テイクダウン）したりすることで被害拡大を食い止めることが困難となりました（図-9）。

今回改ざんされたWebサイトや、盗み取られたIDやパスワードの総数は不明ですが、その活動の規模を示す情報が、いくつか公開されています。例えば、マルウェア感染に誘導するように改ざんされたWebサイト数が約8万（日本国内に3千以上）、マルウェア配布サイト数としては2千以上（日本国内に約80）が存在したという報告があります*30。

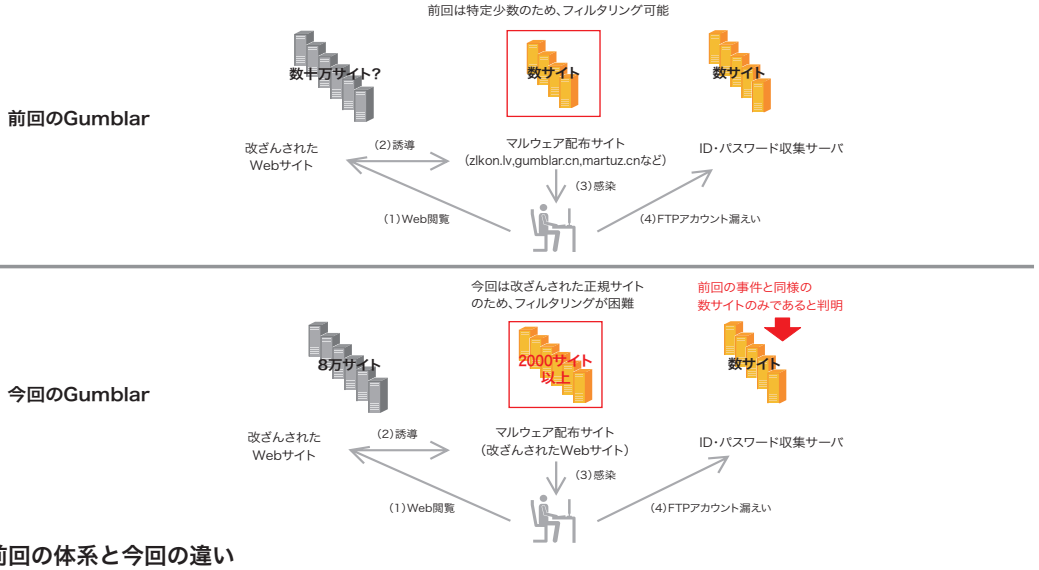


図-9　前回の体系と今回の違い

＊27 Gumblarとは2009年4月～5月当時マルウェア配布Webサイトのドメイン名（gumblar.cn）の一部。本稿では関係するWebサイトやマルウェアなど、全体を示す名前としてGumblarを使う。一般には、今回の流行を前回と区別するために、Gumblar.Xと呼ぶこともある。

＊28 Gumblarにかかわる Webサイトの役割やマルウェアの動作解析結果等、4月に流行した事件の詳細については、IIR Vol.4「1.4.2 ID・パスワード等を盗むマルウェア Gumblar」を参照のこと（http://www.iij.ad.jp/development/iir/pdf/iir_vol04_infra.pdf）。

＊29 cNotesでは、10/12にこの攻撃が観測され始めていることを伝えている。「zlkon、gumblar、martuz 再臨（http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=zlkon%A1%A2gumblar%A1%A2martuz+%BA%C6%CE%D7）。

＊30 本文中のサイト数は次のKaspersky Labs社のblogによるAnalyst's Diary,"Gumblar infection count"（http://www.viruslist.com/en/weblog?weblogid=208187923）。

■ 今回利用されたマルウェアと対策

IIJでは、今回利用されたマルウェアの複数の検体を解析しました。その結果、前回のマルウェアに複数の機能が追加されたものが悪用されていることを確認しています[*31]。また、盗んだIDとパスワードをサーバに送る通信も、前回と同様に行われています。この通信では、通常のHTTPリクエストには出現しない、RFCに違反した特徴的なヘッダが使用されています。このため、これらをProxyサーバやIDSなどで監視することで、感染者を発見したり、IDやパスワードの漏えいを防止したりすることが可能になります(図-10)。盗み取ったIDやパスワードをアップロードするサーバが前回と同様に少数であることが判明したため、これらのサーバについて停止[*32]を行うことで対策を試みました。しかし、すぐに別のサーバを利用して活動が再開したことが確認されています。

■ より新しい事件

この事件と並行し、12月初旬からまったく異なる改ざん内容や感染手段と、新しいマルウェアおよび異なる通信手段を利用した事件が発生しています[*33]。マルウェアを感染させる手段が高度になり、Java実行環境の脆弱性[*34]や、Adobe Reader(Acrobatを含む)の新たな脆弱性[*35]等が悪用されています。また、感染させられるマルウェアは、FTPクライアントの設定等からもIDとパスワードを盗んだり、ボットのような動きをすることも確認されています。この事件では、2009年末から2010年初めにかけて多数のWebサイトが改ざん被害に遭っています。

以上のように、Gumblarは現在も継続中の事件であり、引き続き、クライアントのOSやソフトウェアのバージョン管理、パスワード管理、Webコンテンツ改ざんに注意が必要な状況です。

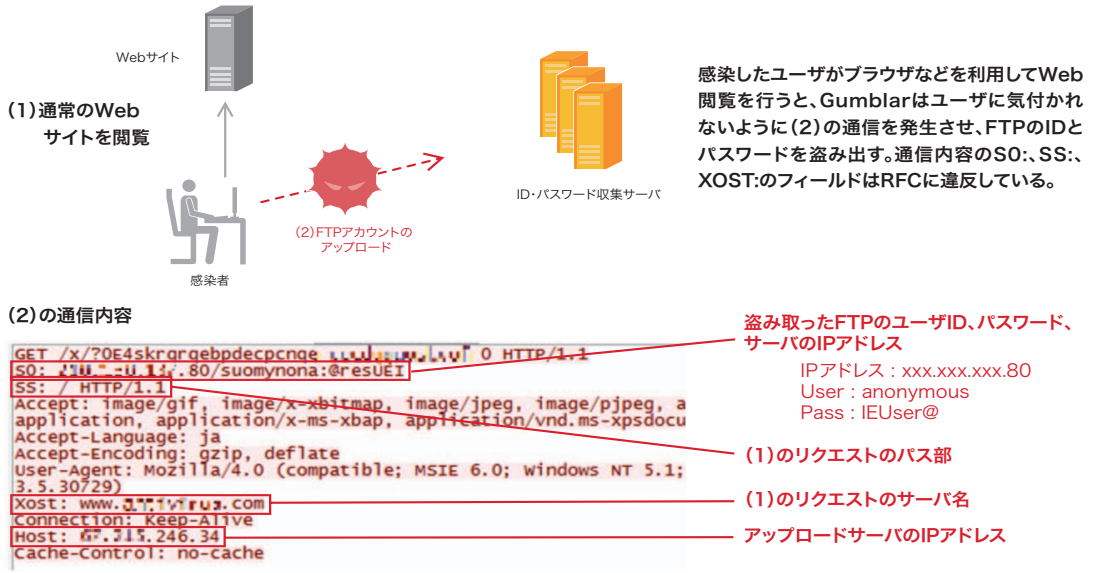


図-10 GumblarによるFTPアカウントを盗む通信

＊31 レジストリの隠ぺいや特定Webサイトへの通信妨害、rootkit検査ツールの起動の妨害など。rootkitとは、元々UNIX上のroot権限を奪取するために使われるツールのこと。この行為を隠ぺいするツールも同時に利用されることが多く、権限奪取と隠ぺいのツールを総称してrootkitと呼ぶようになった。GumblarはID・パスワードを盗むためにAPIのフックや特定レジストリの存在の隠ぺいなど、rootkit的な動作をするため、rootkit検査ツールによる発見を阻害しようと試みている。

＊32 IIJが確認したサーバについては、JPCERT/CCに停止依頼を行った。このような悪性活動を行うサーバの停止依頼等は、JPCERT/CCの「インシデント報告の届出」から行うことができる(http://www.jpcert.or.jp/form/)。

＊33 マルウェア感染に誘導する改ざんの様子と、利用されているマルウェアが異なるため、この事件をGumblarと呼ばないこともある。改ざんの様子からGNU GPL(CODE1, LGPL)、ru:8080、8080等様々な呼ばれ方をしている。

＊34 Java RuntimeEnvironment (JRE)の脆弱性が使われていることがIBM ISSのTokyo SOC Reportで伝えられている(http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1333966?cntxt=a1010214)。

＊35 Adobe AcrobatとAdobe Readerの脆弱性が利用されていることは、同じく、IBM ISSのTokyo SOC Reportで続報として伝えられている(http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1333971?cntxt=a1010214)。この脆弱性は、悪用された時点で、修正の公開されていない問題で、0-day攻撃となっていた。本稿執筆時点では、"Security updates available for Adobe Reader and Acrobat"(http://www.adobe.com/support/security/bulletins/apsb10-02.html)として修正されている。

1.4.2 SSLおよびTLSのrenegotiation機能の脆弱性を利用した中間者攻撃

■ 背景

2009年11月、SSLおよびTLSプロトコル*36*37に中間者攻撃*38を成立させる可能性のある脆弱性がMarsh Ray、Steve Dispensa、Martin Rex によって公表されました*39。SSLとTLSは、IP層とアプリケーション層の間に位置し、アプリケーションデータの暗号化とデータの完全性を保証し、通信相手をX.509公開鍵証明書によって認証する機能を提供します。HTTP、SMTP、POPなどのアプリケーション層の通信プロトコルと合わせて用いられるため、本脆弱性は多くのアプリケーションやシステムに影響を及ぼします。

特にHTTPS（HTTP over SSL）プロトコル*40は、多くのWebブラウザとWebサーバに実装されていますし、Marsh Rayらの報告でもHTTPSを用いた攻撃方法が例として紹介されています。さらに、これをTwitter APIに適用して攻撃者のTwitterアカウントにパスワード情報を投稿させる方法*41が公開されるなど、実際に悪用可能であることが示されました。HTTP以外のプロトコルへの適用可能性については、Thierry Zollerによって検討されています*42。FTPS、SMTPSは脆弱であり、EAP-TLSは影響を受けないことが示されていますが、POPやLDAPなど影響を受けるかどうかが明らかになっていないアプリケーションプロトコルも残っています。

本脆弱性は、SSLとTLSのプロトコル仕様そのものの問題に起因します。OpenSSL*43やApache*44などで修正が公開されていますが、その多くが問題となるrenegotiation機能を単に無効にするという修正です*45。根本的な対処のためには、現仕様を更新し、新仕様にあわせた実装に移行する必要があります。IETF*46もこの認識にあり、現在、対策を策定したRFC化を目指してインターネットドラフト*47が異例の速さで検討されています。本脆弱性は、TLSのすべてのバージョンのプロトコルに加えてSSLバージョン3.0にも影響します。SSLの仕様はIETFで策定されていませんが、新仕様ではTLSと同様に適用可能と記されています（当該ドラフト4.5節）。

■ renegotiation 機能を悪用した中間者攻撃

SSLとTLSは、アプリケーションデータを安全に送受信する前に、ハンドシェイクプロトコルにて暗号アルゴリズムや鍵情報などを共有します。renegotiation機能は、クライアントとサーバの間で合意されたアルゴリズムや鍵情報などを更新するために利用されます。今回の報告では、renegotiation機能の仕様上の問題を利用すると、中間者攻撃により、SSLやTLSの通信に割り込むことが可能であることが示されました。具体的なケースとして、セッション途中でクライアント認証（公開鍵証明書を用いたクライアント認証）に切り替えるケースが指摘されています。

＊36 Alan O. Freier, Philip Karlton, Paul C. Kocher, "The SSL Protocol Version 3.0", Internet Draft (http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00)。

＊37 Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246 (http://www.ietf.org/rfc/rfc5246.txt)。

＊38 中間者攻撃（Man in the middle attack）とは、通信に対する攻撃手法で、通信を行う2者の間に攻撃者が存在することで成立する攻撃のこと。その結果として、通信の傍受と改ざん（通信を行う2者それぞれに対する成りすましを含む）などが発生する。この攻撃手法が成立するかどうかを検討したり、対策を検討したりするうえで、あらかじめ中間に存在する攻撃者を仮定して検討する。実際に中間者攻撃を成立させるためには、その攻撃手法だけではなく、通信の間に割り込むための別の手法（例えばインターネットでは経路ハイジャック等）を併用しなければならない。

＊39 Marsh Ray, Steve Dispensa, "Renegotiating TLS" (http://extendedsubset.com/Renegotiating_TLS.pdf). 本脆弱性はCVE-2009-3555 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555)およびJVNVU#120541 SSL および TLS プロトコルに脆弱性(http://jvn.jp/cert/JVNVU120541/index.html)として管理されている。

＊40 E. Rescorla, "HTTP Over TLS" (http://www.ietf.org/rfc/rfc2818.txt)。

＊41 Twitter APIの問題を指摘するAnil Kurmusのblog "TLS renegotiation vulnerability (CVE-2009-3555)" (http://www.securegoose.org/2009/11/tls-renegotiation-vulnerability-cve.html)。ここで指摘された問題はTwitterによってすぐに修正された。

＊42 Thierry Zoller, TLS & SSLv3 renegotiation vulnerability (http://www.g-sec.lu/practicaltls.pdf)。

＊43 OpenSSL Security Advisory(http://www.openssl.org/news/secadv_20091111.txt)。

＊44 http://www.apache.org/dist/httpd/patches/apply_to_2.2.14/CVE-2009-3555-2.2.patch

＊45 renegotiation が無効になっているかどうかは次のTLS Renegotiation Testで確認することができる。TLS Renegotiation Test (http://netsekure.org/2009/11/tls-renegotiation-test/)。

＊46 Internet Engineering Task Force。インターネットに関する通信プロトコルやデータフォーマットなどの技術の標準化を行う組織。標準化仕様を規定する文書Request for Comments(RFC)の発行を行う。

＊47 RFCの草稿段階の文書をインターネットドラフトと呼ぶ。本稿執筆時点では、この問題への対策に関するインターネットドラフトは次のものであった(http://tools.ietf.org/html/draft-ietf-tls-renegotiation-03)。この文章は、後の2010年2月13日にRFC5746（http://www.ietf.org/rfc/rfc5746.txt）として発行された。本稿はインターネットドラフトをもとに執筆したもので、状態名等をRFCの内容に合わせてある。

HTTPSにおける攻撃の例を図-11に示します。この攻撃により、中間者である攻撃者は、クライアントとサーバ間での暗号化された通信に割り込むことができます。この結果、攻撃者のHTTPリクエストと正当なユーザによるリクエストを結合し、サーバに送信することが可能になります。このとき、正当なユーザのアプリケーションデータは暗号化されたままであり、攻撃者による改ざんやデータ搾取が行われない点に注意してください。攻撃者のリクエストと正当なユーザの既存のリクエストがHTTP Cookie等で結び付けられる場合、サーバは一連のリクエストが同一ユーザによるものであると解釈し、攻撃者のリクエストを受領して処理する可能性があります。

■ 仕様の改変点

次に、RFC化が予定されているインターネットドラフトでの改変点を紹介します。このドラフトでは、TLSの拡張タイプの値としての“renegotiation_info”と、本来ならば暗号アルゴリズムを表現するCipher Suiteの状態として"TLS_EMPTY_RENEGOTIATION_INFO_SCSV"が導入されています。renegotiation_info拡張を用いてrenegotiationを安全に行う実装であることを通信相手に宣言できます。具体的には、クライアントとサーバがともにハンドシェイクプロトコルで安全に共有した情報を保存しておきます。renegotiationを行う際にrenegotiation_info拡張を用いて、お互いしか知りえない情報を交換することで、それまで接続していた通信相手であることを確認します。また、renegotiation_info拡張を処理不能なTLS拡張と認識し、通信を中断する実装が存在するため、"TLS_EMPTY_RENEGOTIATION_INFO_SCSV"を用いる方法も準備されています。

■ 対策と後方互換性の問題

このインターネットドラフトがRFC化され、新たに対策された実装が普及し今回の問題が解消されることが望まれますが、移行には時間がかかると考えられます。後方互換性の観点から現バージョンとの互換性を確保すべきですが、旧実装からrenegotiationが行われた場合、正しい相手からのリクエストであるかどうかを安全に確認する手段はありません。このため新実装では、旧実装からのrenegotiation要求を拒否することが推奨されています。これは、現在の一時的な対策に相当するもので、renegotiation機能を利用することはできません。つまり、安全にrenegotiationを行う必要がある利用形態では、新しい仕様がRFC化された後、クライアントとサーバで、ともに新仕様に対応した新しい実装を導入する必要があります。

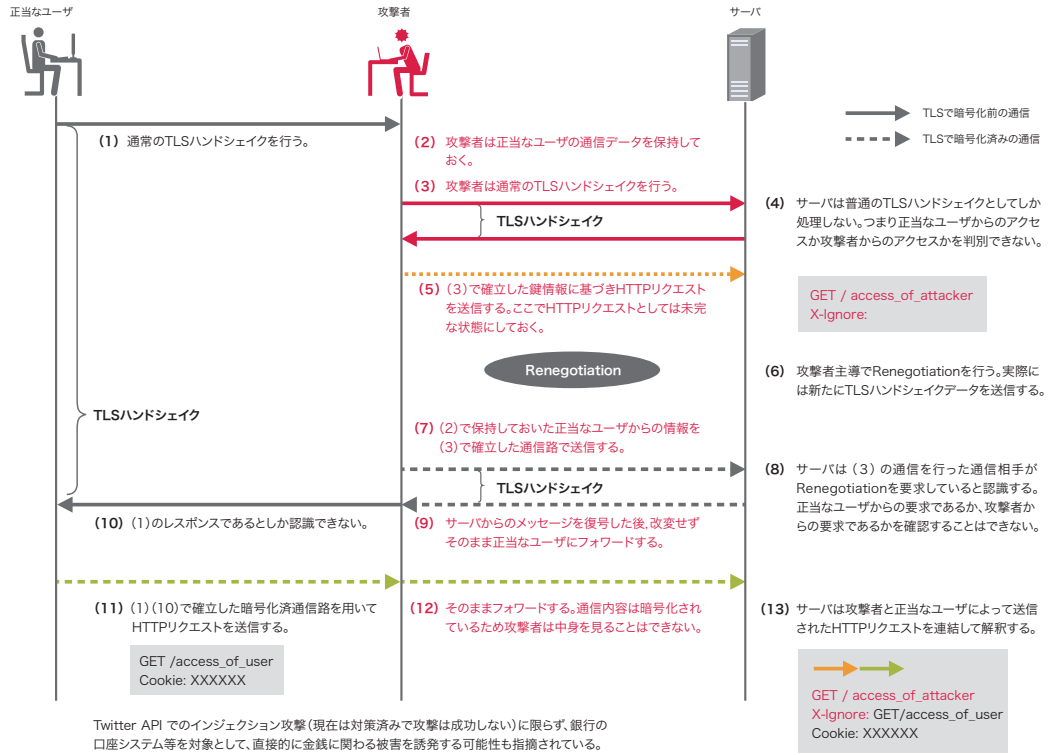


図-11 攻撃シナリオ

1.4.3 P2Pファイル共有ネットワークの調査技術

■ はじめに

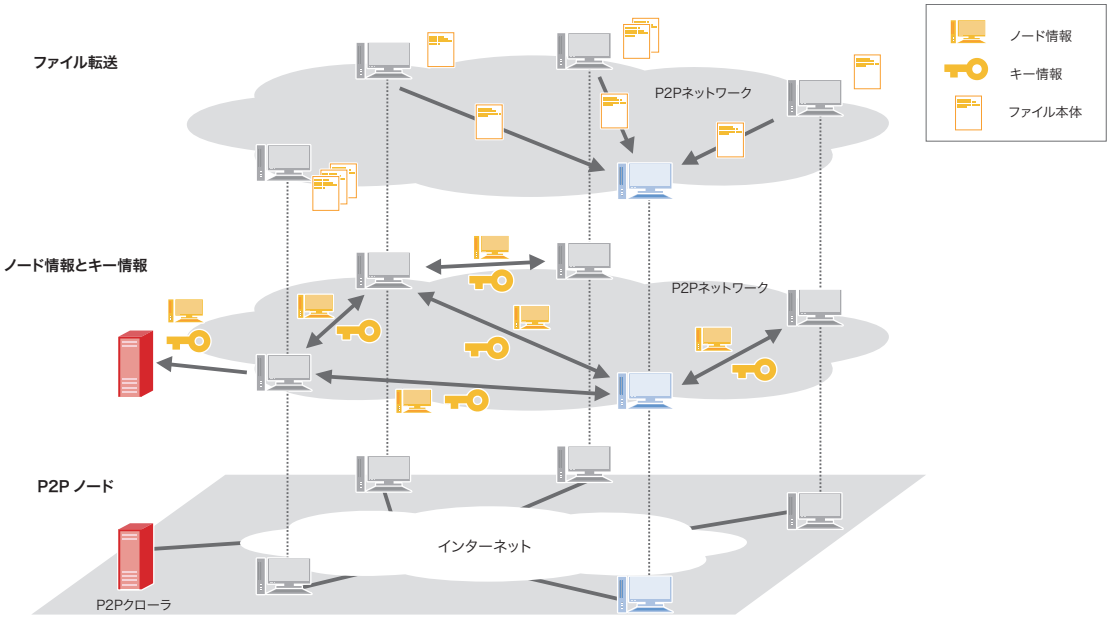
IIJでは、情報漏洩への対策の検討と通信の特性調査の2つの観点から、WinnyやShareといったP2Pファイル共有ソフトウェアが構成するP2Pネットワークの調査技術に注目し、2006年頃から関連する研究会等[*48]に積極的に参加しています。

また、2010年1月1日に施行される改正著作権法[*49]では、いわゆる「ダウンロード違法化」の規定が盛り込まれるため、著作権侵害行為との関連からP2Pファイル共有ネットワークが再び注目されています。ここでは、これを機会に、WinnyやShareといったP2Pファイル共有ソフトウェアの仕組みと、そのネットワークの調査技術についてまとめます。

■ P2Pファイル共有ネットワークの仕組み

P2Pファイル共有ネットワークには、ファイルを共有するためにファイルを公開する機能、ファイルを検索する機能、ファイルをダウンロードする機能が備わっています。P2Pノードは、希望するファイルを効率よく検索するために、どのノードがどういったファイルを持っているかを示す「キー情報」を頻繁に交換します。このキー情報交換の仕組みは、自分が公開しているファイルを他のノードに通知するためにも利用されます。

また、P2Pファイル共有ネットワーク全体でのダウンロード効率を上げるための工夫として、ダウンロードが完了したファイルを「キャッシュ」として残し、他のノードに対して自動的に公開します。ユーザ自らがダウンロードしなくても、ファイル転送の中継などによって自動的にキャッシュが作られ、公開される仕組みも備えています。この仕組みによって、「人気のある」ファイルは自動的に多くのノードで公開されるのです。そして、ピュアP2P方式で不特定多数のノードが自由に参加したり離脱したりできるようにするために、どのノードも他ノードの情報を交換し蓄積してP2Pファイル共有ネットワークを維持しています。以上の説明をまとめたものを図-12に示します。実際のP2Pファイル共有ソフトウェアは、ユーザの指定するキーワード等をもとにして、自動的にファイルを収集します。このため、P2Pファイル共有ネットワーク上でキー情報の収集とファイル転送を行う通信が常時発生し、通信量を増加させることがあります。



インターネットに接続したP2Pノード（下段）は、ノード間で接続してP2Pネットワークを構成し、ノード情報やキー情報を交換、蓄積する（中段）。ファイルをダウンロードしたいノード（図中の青いノード）は、蓄積されたキー情報からファイルを検索してファイル（もしくはその一部）を持つノードを特定し、そのノードに直接接続してファイルを転送してもらう（上段）。一方で、P2Pクローラは、ノードへの接続と、ノード情報とキー情報の収集までを行い（下〜中段）、ファイル転送は行わない。

図-12 P2Pファイル共有ネットワークの仕組み

＊48 例えば、安心・安全インターネット推進協議会 P2P研究会（http://www.scat.or.jp/stnf/）等。
＊49 著作権法の条文は、法令データ提供システム（http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi）から閲覧できる。

■ P2Pファイル共有ネットワーク調査技術

P2Pネットワークでは、全体の一元管理を行うサーバは存在しません。このため、その全体像を調べるときに、クローリング手法が用いられます[*50]。クローリングによる調査では、クローラが実際にP2Pノードに接続してP2Pファイル共有ネットワークのプロトコルで通信し、他ノードの情報を取得します。そして、そこで知り得たノードに接続し、さらに他ノード情報を取得する作業を繰り返し、P2Pファイル共有ネットワーク上のノードを網羅的に調査します（図-13）。

クローリングによる調査で、ノード情報と同時に収集されるキー情報を分析することで、どのノードでどのようなファイルが公開されているかも知ることができます。このようなクローリング手法による調査では、ファイルの拡散などの副作用を起こすことなく、P2Pファイル共有ネットワークの全体像を把握できるメリットがあります。

■P2Pネットワークの実態

P2Pファイル共有ネットワークの実態調査の例[*51]として、IIJが外部の組織と協力して実施している調査から、その結果の一部を紹介します。この調査で、IIJのネットワーク内にはWinnyのノード全体の約2%、Shareのノード全体の約3%が存在していることがわかっています。また、これらのノードがIIJのネットワークの外にあるノードとの通信で発生させている通信量を把握することで、ネットワーク全体に対する影響を評価しています。この調査の結果明らかになったWinnyとShareのノード数の推移[*52]を図-14に、IIJのネットワーク内のノードがIIJのネットワークの外にあるノードとの通信で発生させている通信量を調査した結果を図-15に示します。

これらの結果が示すようにWinny、Shareともにノード数は減少傾向にありますが、現時点でも常時約6Gbpsの帯域を占有する通信量を発生させていることがわかります。

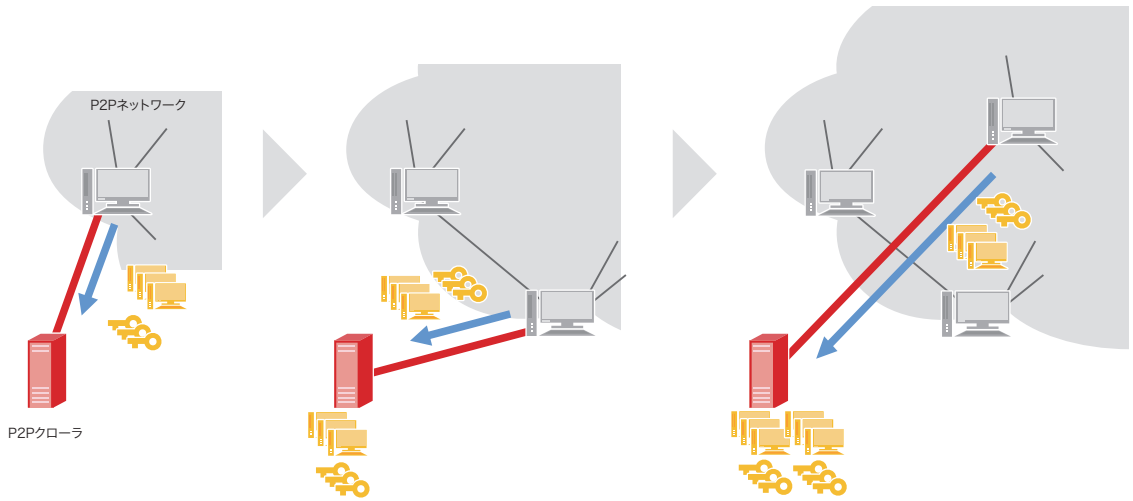


図-13 クローリング手法の概要

＊50 クローリング調査については、例えば、次の論文にも報告がある。寺田ら: クローリング手法を用いたP2P ネットワークの観測, 情報処理学会 コンピュータセキュリティ 研究報告 Vol.2007 No.48, pp.51-56（2007）（http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/CSEC07037009.pdf）。実際にこのような調査を行う製品としては、株式会社フォティーンフォティ技術研究所（http://www.fourteenforty.jp/）のWinny RadarおよびShare Radarがある。

＊51 P2Pファイル共有ネットワークの実態調査には、例えば株式会社クロスワープによる P2Pの現状 ~Winny、Shareネットワーク状況調査報告~ (http://www.scat.or.jp/stnf/contents/p2p/p2p080910_2.pdf)等がある。安心・安全インターネット推進協議会の主催による2008年9月の情報セキュリティセミナーでは、こうした実態調査が他にも複数報告され、現在はWebページから発表資料を入手できる(http://www.scat.or.jp/stnf/contents/p2p080910.html)。また、次回のセミナーは2010年3月2日に開催が予定されている(http://www.scat.or.jp/stnf/contents/p2p100302/P2P.htm)。

＊52 2010年1月1日の改正著作権法の施行日の前後では、Winny、Shareともにノード数が2割前後減少している様子が観測されている。この図が示すノード数は減少後の数値であることに注意が必要。

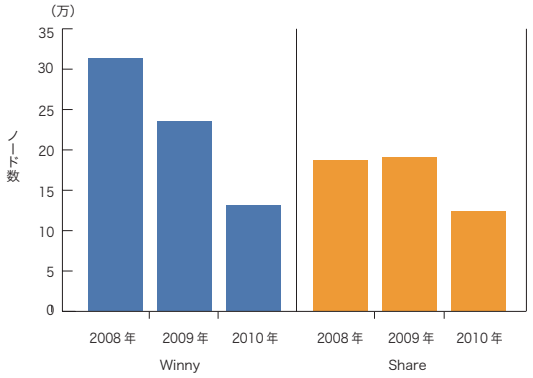
ここでは、継続的に調査を行っているWinnyとShareについて、その状況を紹介しました。P2Pファイル共有ネットワークには、まだ他にも実装があり、利用状況の変化に伴って、今後も通信特性が大きく変わる可能性があります。IIJでは、安定したネットワーク基盤を提供しつづけるために、今後もこのような調査を継続していきます。

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。

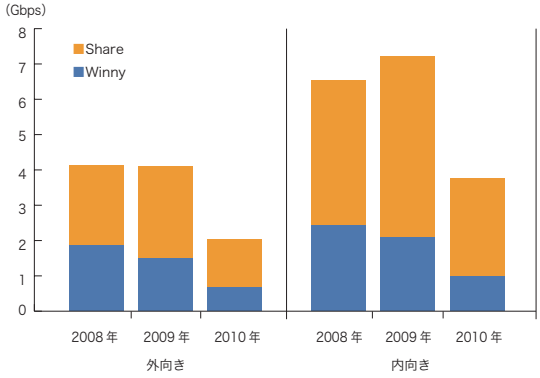
今回は現在でも継続中の事件であるGumblarの続報と、通信プロトコルであるSSLおよびTLSの脆弱性、P2Pファイル共有ネットワークの調査技術についてまとめています。特に、P2Pファイル共有ネットワークについては今日話題となったことではなく、発生させる通信量、匿名性、情報漏洩、著作権侵害等、様々な議論が重ねられているテーマであり、IIJでも長期にわたり調査を行っています。今回は調査手法と通信量への影響という形でその一部を示しましたが、今後も調査は継続しますし、別の切り口についても機会があれば紹介していきたいと思います。

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。



各年1月のある1週間を対象に調査した。24時間ごとに重複を除きノードを数えて1日のノード数とし、7日間の平均をとってその年のノード数とした。

図-14 WinnyとShareの1日平均ノード数の比較



各年1月のある1週間（図-14と同一）の平均通信量を算出した。
外向きはIIJのネットワークの内から外部へ出ていく通信を、
内向きはIIJのネットワークの外から内部へ入ってくる通信を示す。

図-15 WinnyとShareの通信量（1週間の時間平均）

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 Gumblarの再流行）
須賀 祐治（1.4.2 SSLおよびTLS renegotiation機能の脆弱性を利用した中間者攻撃）
齋藤 衛 永尾 禎啓　（1.4.3 P2Pファイル共有ネットワークの調査技術）
IIJ サービス事業統括本部 セキュリティ情報統括部

協力:
加藤 雅彦　IIJ サービス事業統括本部 セキュリティ情報統括部