

## 標的型攻撃とOperation Aurora

今回は、2010年1月から3月に発生したインシデントに関する報告とともに、昨年12月以降発生しているGumblar類似の事件と、米国の企業を対象にした標的型攻撃について解説し、IJのマルウェア対策活動MITFとその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IJ自身が取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、IJが対応したインシデントについてまとめたものです。今回のレポートで対象とする2010年1月から3月までの期間では、前回のレポートで取り上げた、IDとパスワードを盗み取るマルウェアGumblarとその類似のインシデントの発生が継続し、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、脆弱性に関しても、Webブラウザに関連するものやサーバに影響を与えるものが相次いで発見されています。このほかのインシデントとして、DNS情報を不正に操作したサービスの乗っ取りや、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。そして、米国の複数の大手企業を対象にした標的型攻撃が大きな話題となりました。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、2010年1月から3月までの期間にIJが取り扱ったインシデントと、その対応を示します。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。

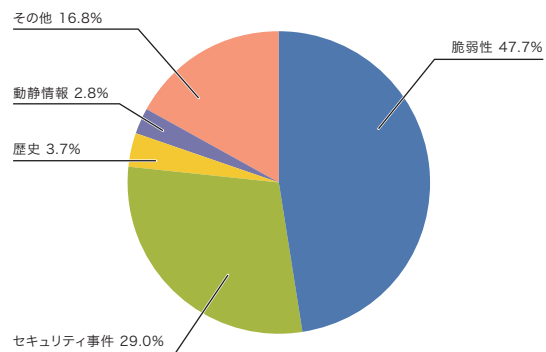


図-1 カテゴリ別比率 (2010年1月～3月)

\*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では、マイクロソフト社のInternet Explorer<sup>\*2\*3</sup>、アドビ社のAdobe ReaderとAcrobat<sup>\*4\*5</sup>、Flash Player<sup>\*6\*7</sup>、製品のアップデートに利用されているAdobe Download Manager<sup>\*8</sup>、リアルネットワークス社のReal Player<sup>\*9</sup>やオラクル社のJava Runtime Environment (JRE)<sup>\*10</sup>など、Webブラウザ自体とそのプラグインに関する脆弱性が数多く発見され、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、DNSサーバのBIND9<sup>\*11</sup>、プロキシサーバに利用されるSquid<sup>\*12</sup>、Oracle Database<sup>\*13</sup>等、広く利用されているサーバや、Linux Kernel<sup>\*14</sup>やMac OS<sup>\*15\*16</sup>等のOSに関する脆弱性、ジュニパーネットワークス社のJUNOS<sup>\*17</sup>やシスコシステムズ社のCisco IOS<sup>\*18</sup>等のルータ製品にも複数の脆弱性が修正されています。

## ■ 動静情報

IJ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、2月に開催

されたバンクーバーオリンピックなどに注目しましたが、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、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す。このため、各種の動静情報に注意を払いましたが、IJの設備やIJ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、中国の検索サイトである百度 (Baidu) 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<sup>\*19</sup>が発生しました。またハイチ地震やチリ地震などの自然災害の発生に付け込んで、検索エンジンなどの検索結果から詐欺的ソフトウェア (スケアウェア) に誘導する事件も発生しています<sup>\*20</sup>。さらに、P2Pファイル共有ネットワーク上の著作権法違反のコンテンツに対し、著作権団体を装ったり、マルウェアを悪用して金銭を請求する事件も報告されています<sup>\*21</sup>。

- \*2 マイクロソフト セキュリティ情報 MS10-002 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (978207) (<http://www.microsoft.com/japan/technet/security/Bulletin/MS10-002.msp>)。
- \*3 マイクロソフト セキュリティ情報 MS10-018 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (980182) (<http://www.microsoft.com/japan/technet/security/Bulletin/MS10-018.msp>)。
- \*4 Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB10-02 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-02.html>)。
- \*5 Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB10-07 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-07.html>)。
- \*6 Adobe Flash Player用セキュリティアップデート公開 APSB10-06 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-06.html>)。
- \*7 マイクロソフト セキュリティ アドバイザリ (979267) Windows XPで提供される Adobe Flash Player 6の脆弱性により、リモートでコードが実行される (<http://www.microsoft.com/japan/technet/security/advisory/979267.msp>)。
- \*8 Adobe Download Manager用セキュリティアップデート公開 APSB10-08 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-08.html>)。
- \*9 RealNetworks, Inc.、セキュリティ脆弱性に対応するアップデートをリリース ([http://service.real.com/realplayer/security/01192010\\_player/ja/](http://service.real.com/realplayer/security/01192010_player/ja/))。
- \*10 JavaTM SE 6 アップデートリリースノート (<http://java.sun.com/javase/ja/6/webnotes/6u19.html>)。
- \*11 JVN#360341 BIND 9のDNSSEC検証コードに脆弱性 (<http://jvn.jp/cert/JVN#360341/index.html>)。
- \*12 Squid Proxy Cache Security Update Advisory SQUID-2010:1 Denial of Service issue in DNS handling ([http://www.squid-cache.org/Advisories/SQUID-2010\\_1.txt](http://www.squid-cache.org/Advisories/SQUID-2010_1.txt))。
- \*13 Oracle Critical Patch Update Advisory - January 2010 (<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>)。
- \*14 JVN#571860 Linux カーネルの IPv6 jumbogram 処理に脆弱性 (<http://jvn.jp/cert/JVN#571860/index.html>)。
- \*15 セキュリティアップデート 2010-001 について ([http://support.apple.com/kb/HT4004?viewlocale=ja\\_JP](http://support.apple.com/kb/HT4004?viewlocale=ja_JP))。
- \*16 セキュリティアップデート 2010-002 / Mac OS X v10.6.3のセキュリティコンテンツについて ([http://support.apple.com/kb/HT4077?viewlocale=ja\\_JP](http://support.apple.com/kb/HT4077?viewlocale=ja_JP))。
- \*17 PSN-2010-01-623:JUNOS kernel cores when it receives an crafted TCP option. (<https://www.juniper.net/alerts/viewalert.jsp?actionBtn=Search&txtAlertNumber=PSN-2010-01-623&viewMode=view>) (参照にはユーザ登録が必要)。
- \*18 Cisco Systems, Inc. Summary of Cisco IOS Software Bundled Advisories, March 24, 2010 (<http://www.cisco.com/JP/support/public/ht/security/107/1076221/cisco-sa-20100324-bundle-j.shtml>)。
- \*19 この件に関しては次のトレンドマイクロ社のBlogに詳しい。Iranian "Cyber Army" Strikes at China's Search Engine Giant, Chinese Hackers Retaliate (<http://blog.trendmicro.com/iranian-cyber-army-strikes-at-china%e2%80%99s-search-engine-giant-chinese-hackers-retaliate/>)。
- \*20 ハイチ地震に関するSEOボイズニングについては次のエフセキュアブログに詳しい。ハイチ地震:新たなローグがニュースを悪用 (<http://blog.f-secure.jp/archives/50335541.html>)。
- \*21 この事件についてはエフセキュアブログに詳しい。ICPP著作権財団は偽物 (<http://blog.f-secure.jp/archives/50388533.html>)。

マルウェアの活動では、昨年より継続しているGumblarとそれに類似した事件<sup>\*22</sup>が活発になり、多くの企業のWebサイトで改ざんによる被害が確認されました。この事件に関しては「1.4.1 Gumblar型の攻撃スキームを持つru:8080」を参照してください。

また、Pushdoと呼ばれるボット型マルウェアによる目的不明なSSLの通信が、特定多数のWebサーバに対して行われていることも確認されています<sup>\*23</sup>。さらに、ボットネットmiraposaを運用していたグループがスペインで摘発されたり<sup>\*24</sup>、ボットネットWaledacに対しマイクロソフト社がサーバをテイクダウンする<sup>\*25</sup>など、ボットネットに対する取り組みが複数行われました。加えて、Internet Explorerの脆弱性を利用した標的型攻撃<sup>\*26</sup>により複数の米国企業で被害が発生しています。この標的型攻撃に関しては「1.4.2 標的型攻撃とOperation Aurora」を参照してください。

#### ■ その他

その他の事件としては、国内の利用者が多いインターネット掲示板が3月に大規模な攻撃を受け、利用に支障が生じる等の影響が発生しました。

その他のセキュリティに関係する情報としては、まず、スマートフォンに対する攻撃手法の研究が続けて発表されました<sup>\*27</sup>。また、昨年発見されたTLSのrenegotiation機能に関するプロトコルの脆弱性<sup>\*28</sup>に対して、この脆弱性を修正した通信プロトコルを規定するRFC5746が発行されました<sup>\*29</sup>。さらに、昨年度発生したセキュリティ事件をまとめた文書「2010年版10大脅威」がIPAから発表<sup>\*30</sup>されています。

## 1.3 インシデントサーベイ

IJでは、インターネット上で発生するインシデントのうち、インフラストラクチャ全体に影響を与える可能性があるインシデントに注目し、継続的な調査研究と対処を行っています。ここでは、そのうちDDoS攻撃、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きました。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、2010年1月から3月の期間にIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。

\*22 JPCERT/CC Alert 2010-01-07:Webサイト改ざん及びいわゆるGumblarウイルス感染拡大に関する注意喚起 (<https://www.jpccert.or.jp/at/2010/at100001.txt>)。

\*23 この攻撃に関する詳細は次の報告などが詳しい。Shadowserver Foundation:Pushdo DDoS'ing or Blending In? (<http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20100129>)。

\*24 この事件についての詳細は次のPanda Security社のブログに詳しい。Panda Security Japan ブログ:史上最大規模、Mariposaボットネットの摘発 (<http://pandajapanblogs.blogspot.com/2010/03/mariposa.html>)。

\*25 この件については次のマイクロソフト社のブログに詳しい。The Official Microsoft Blog:Cracking Down on Botnets ([http://blogs.technet.com/microsoft\\_blog/archive/2010/02/25/cracking-down-on-botnets.aspx](http://blogs.technet.com/microsoft_blog/archive/2010/02/25/cracking-down-on-botnets.aspx))。

\*26 米国ではこの脅威に対してUS-CERTが注意喚起を行うなど重大な脅威として取り扱っている Technical Cyber Security Alert TA10-055A:Malicious Activity Associated with "Aurora" Internet Explorer Exploit (<http://www.us-cert.gov/cas/techalerts/TA10-055A.html>)。

\*27 BlackBerryとiPhoneに関する独立した研究がそれぞれ別のカンファレンスで発表された。Tyler ShieldsによるBlackberry Mobile Spyware - The Monkey Steals the Berries (<http://www.shmoocon.org/presentations-all.html#monkeyberry>) およびNicolas SeriotによるiPhone Privacy (<http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html#Seriot>)。

\*28 この脆弱性については本レポートのVol.6 「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」にて解説を行っている。(http://www.ij.ad.jp/development/iir/pdf/iir\_vol06.pdf)。

\*29 IETF RFC5746 Transport Layer Security (TLS) Renegotiation Indication Extension (<http://www.rfc-editor.org/rfc/rfc5746.txt>)。

\*30 IPA (独立行政法人情報処理推進機構) による「2010年版 10大脅威」(<http://www.ipa.go.jp/security/vuln/10threats2010.html>)。

ここでは、IJ DDoS対策サービスの基準で攻撃と判定した通信異常の件数を示しています。IJでは、ここに示す以外のDDoS攻撃にも対処していますが、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<sup>\*31</sup>、サーバに対する攻撃<sup>\*32</sup>、複合攻撃(1つの攻撃対象に対して同時に数種類の攻撃を行うもの)の3種類に分類しています。

この3ヵ月間でIJは、227件のDDoS攻撃に対処しました。1日あたりの対処件数は2.52件で、平均発生件数は前回のレポート期間のものと同じく変わっていません。

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86%、複合攻撃が14%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に分類したもので、3万ppsの packets によって105Mbpsの通信量を発生させたものです。また、攻撃の継続時間は、全体の86%が攻撃開始から30分未満で終了し、14%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見られませんでした。

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<sup>\*33</sup>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<sup>\*34</sup>の利用によるものと考えられます。

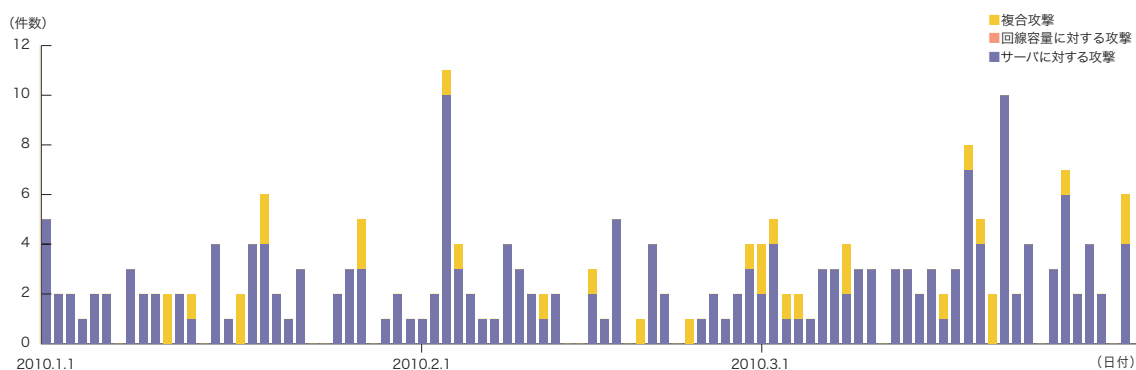


図-2 DDoS攻撃の発生件数

\*31 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。

\*32 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。

\*33 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。

\*34 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、IJが実施しているマルウェアの活動観測プロジェクトMITF\*35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\*36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

2010年1月から3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ポートに対する探索行為でした。また、前回のレポート期間と同様に、シマンテックのクライアントソフトウェアが利用する2967/TCP、SSHで利用する22/TCPに対する探索行為が観測されています。一方で、2582/TCP、11999/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。発信元の国別分類を見ると、中国の17.9%、日本国内の15.9%、ベトナムの9.9%が比較的大きな割合を占めています。

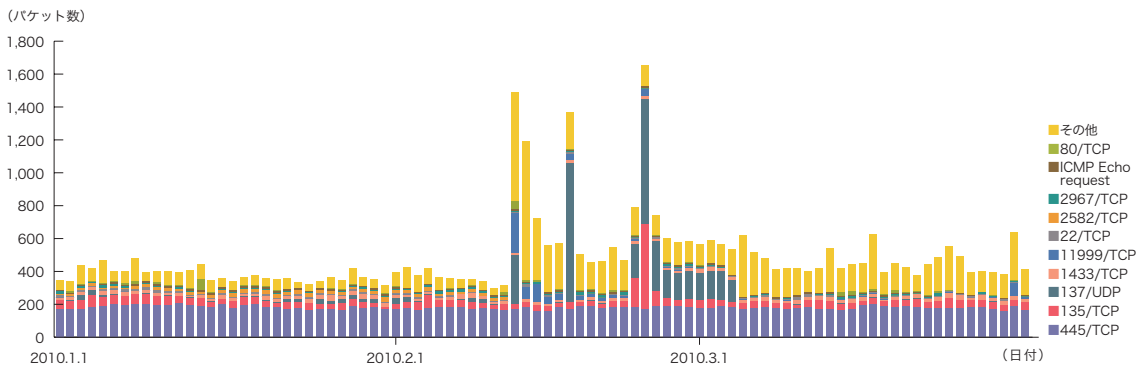


図-3 ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

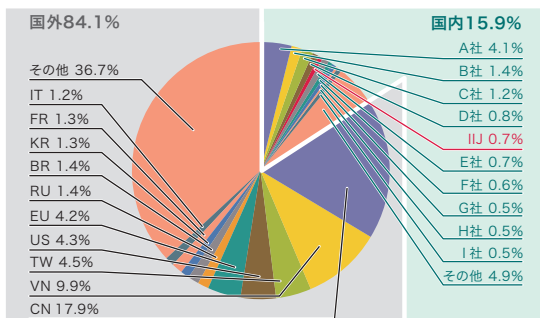


図-4 発信元の分布(国別分類、全期間)

\*35 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。

\*36 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<sup>\*37</sup>の総数を総取得検体数、検体の種類をハッシュ値<sup>\*38</sup>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479、ユニーク検体数が37です。前回の集計期間での平均値が総取得検体数で623、ユニーク検体数で44でした。今回は、総取得検体数、検体の種類を表すユニーク検体数ともに、前回より減少傾向が見られました。

検体取得元の分布では、日本国内が61.3%、国外が38.7%でした。このうちIJのユーザ同士のマルウェア感染活動は0.1%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、ワーム型が14.3%、ボット型が84.6%、ダウンロード型が1.1%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<sup>\*39</sup>と96個のマルウェア配布サイトの存在を確認しています。

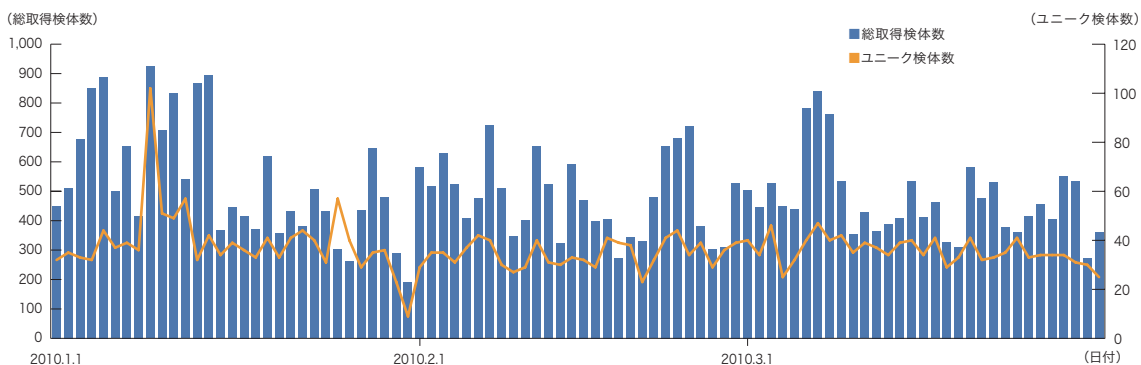


図-5 取得検体数の推移(総数、ユニーク検体数)

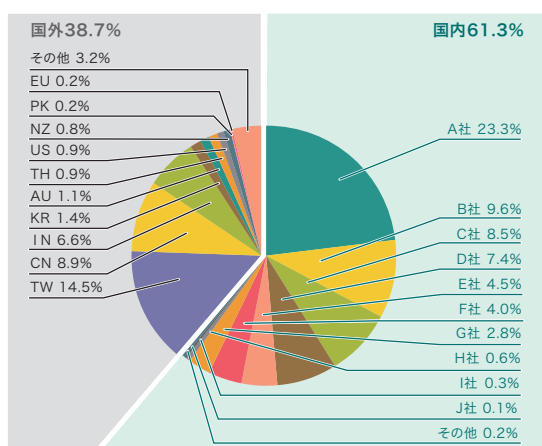


図-6 検体取得元の分布(国別分類、全期間)

\*37 ここでは、ハニーボット等で取得したマルウェアを指す。

\*38 様々な入力に対して一定長の出力をする一方関数(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。

\*39 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

IJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃\*40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になった攻撃です。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。

2010年1月から3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、IJ

マネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。発信元の分布では、日本が60.4%、中国が10.0%、米国が9.5%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。

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

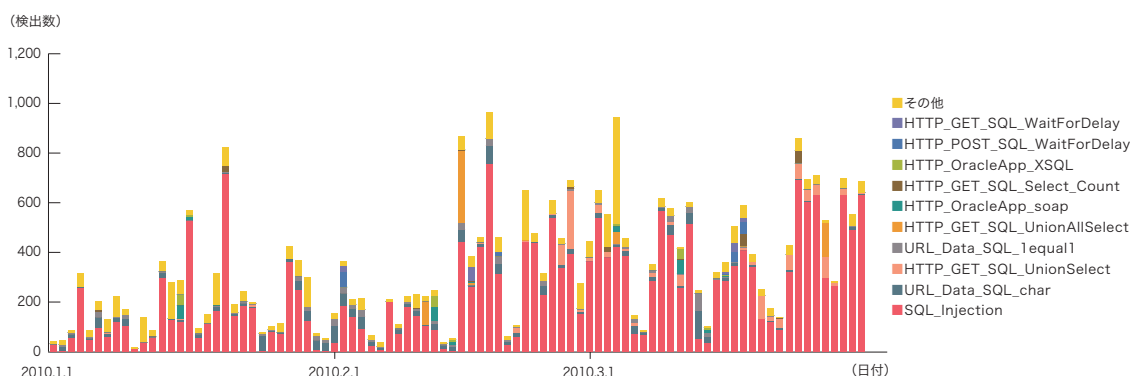


図-7 SQLインジェクション攻撃の推移(日別、攻撃種類別)

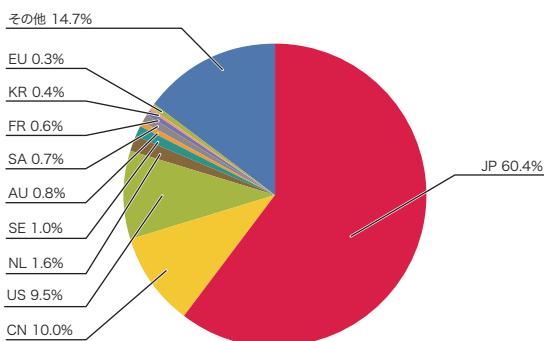


図-8 SQLインジェクション攻撃の発信元の分布(国別分類、全期間)

\*40 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。



その他にもポットをインストールして迷惑メールを送信したり、スケアウェア<sup>\*45</sup>をインストールしてユーザを騙して金銭を直接詐取しようとするなど、その悪性活動は多岐に渡ります。また、感染手法もGumblarに比べて強化されています(表1)。特に、Adobe Readerの脆弱性への攻撃は、悪用時には対策が存在しない0-day攻撃であったため、被害がより大きくなったと考えられます<sup>\*46</sup>。

### ■ マルウェアの動作

ru:8080で使われているマルウェアは、ダウンローダ型<sup>\*47</sup>のマルウェアであり、感染後にサーバから2～5種類のマルウェアをダウンロードします<sup>\*48</sup>。これらマル

ソフトウェア	バージョン	脆弱性	Gumblar	ru:8080
Internet Explorer	== 7	MS09-002	●※	
Microsoft Video ActiveX Control	<= XP SP3	MS09-032		●※
Microsoft Office	<= 2003 SP3	MS09-043	●	
MDAC	<= 2.8 SP2	MS06-014	●	●
	<= 2.8 SP2	MS07-009	●	
Microsoft Access Snapshot Viewer	-	MS08-041		●
Adobe Flash	< 9.0.124	CVE-2007-0071	●	
	<10.0.23	CVE-2009-1862	●	
Adobe Reader / Acrobat	< 8.1.1	CVE-2007-5659		●
	< 8.1.2	CVE-2008-0655	●	
	< 8.1.3	CVE-2009-0927	●	
	< 8.1.3	CVE-2008-2992	●	●
	< 9.2.1	CVE-2009-4324		●
Java (JRE)	< 1.6.11	CVE-2008-5353	●	●
AOL Radio AmpX ActiveX	<= 2.4.0.6	BID:35028		●

赤字は 事件発生時点で0-day 攻撃であった脆弱性 ※IJJでは未確認

表-1 Exploitに利用される脆弱性の比較

ウェアのいくつかは、ファイルとして保存されない<sup>\*49</sup>ため、発見が困難です。また、ダウンロードされるマルウェアの数や種類も時間の経過とともに変化していきます。2010年1月初旬にru:8080のマルウェアがダウンロードしたマルウェア群の一覧を図-10に示します。この時点では、IDとパスワードを盗み出すマルウェアとともに、ポット(Waledacや後にPushdo等)、スケアウェア(Security tool)、rootkitなどをインストールしています。

### ■ 対策にむけて

ru:8080とサーバ間の通信内容はエンコードされ、番号キーはRFCに違反したHTTPヘッダとして追加されています<sup>\*50</sup>。この通信をWAFやIPSなどで検知して防御することで、マルウェアの動作を実質的に無力化できます<sup>\*51</sup>。IJJでは、取得したマルウェアを解析してえられたこれらの特徴を、サービスでのアクセス制御に反映しています。また、さまざまな団体の活動<sup>\*52</sup>に積極的に参加し、複数の事業者間でより効果的な対策を実施するための情報交換や対策手法も検討しています。

Gumblarやru:8080に限らず、今後も同種の事件は発生し続けると考えられます。このため、状況の変化に応じて、継続的に予防や対策の活動を行っていくことが必要です。特に、ru:8080では、アプリケーションに保存したパスワードが盗まれるという点が大きな脅威となっています。アプリケーションごとに保存された情報の安全性を個別に評価し、対策を実施することは困難であることから、パスワード管理ツール等の利用で包括的に防御することが考えられます。

\*45 金銭を詐取る詐欺行為を手助けするソフトウェア。スケアウェアについてはIIR Vol.3の「1.4.3 スケアウェア」において解説している([http://www.ijj.ad.jp/development/iir/pdf/iir\\_vol03.pdf](http://www.ijj.ad.jp/development/iir/pdf/iir_vol03.pdf))。

\*46 この脆弱性は2010年1月12日に修正がリリースされている。Adobe ReaderおよびAcrobat用セキュリティアップデート公開 APSB10-02 (<http://www.adobe.com/jp/support/security/bulletins/apsb10-02.html>)。

\*47 主にサーバから追加機能をダウンロードするためのマルウェア。機能をダウンロードと実行のみに限定して小型化することで、ウイルス対策製品等による検知を迂回する狙いがある。従来のGumblarはドロップタイプであり、情報の盗難を行うマルウェアを内部に格納しているため、Gumblarが実行されると即座に情報が盗み出される可能性があった。ru:8080ではこのような機能を別途マルウェアをダウンロードして実行するため、ダウンロードに利用されるHTTP等の通信を阻害することで情報盗難の被害を比較的容易に防ぐことができる。

\*48 ru:8080が接続するダウンロードサイトは数週間ごとに変更されていた。IJJが確認した限りでは、例えば2009年12月28日から2010年1月12日はforhomessale.ru、2010年1月7日から2月10日はyourarray.ru、2月5日から2月27日はexitguide.ru、2月26日から3月18日はstelane.ruなど。

\*49 エンコードしたマルウェアをダウンロードし、ファイルとして保存しないでメモリ上の処理だけでデコードした後、直接ほかのプロセスにインジェクションして実行する。このため通信上でもファイルとしてもウイルス対策製品で検出されにくい。

\*50 HTTPレスポンスにMagic-Number: や Entity-Info: など、RFCに違反したヘッダが追加される。これらのヘッダに付随する情報は、エンコードされたマルウェアを復元するために使われる。

\*51 一般には、HTTPリクエストを".ru:8080"でフィルタすることで効果があるとされていたが、本稿執筆時点では.info等、他のTLDの利用も見られるようになってきている。これには4月1日より.ruドメイン取得手続きが厳格化されたことが影響していると考えられる。Coordination Center for ccTLD .RUによるアナウンス([http://www.cctld.ru/en/news/news\\_detail.php?ID=682](http://www.cctld.ru/en/news/news_detail.php?ID=682))。

\*52 例えばWeb感染型マルウェア対策コミュニティ([http://www.fourteenforty.jp/news/WebMalwareCommunity\\_PR.pdf](http://www.fourteenforty.jp/news/WebMalwareCommunity_PR.pdf))やTelecomSAC Japan(<https://www.telecom-isac.jp/>)、日本シーサート協議会(<http://www.nca.gr.jp/>)の各種活動等。

### 1.4.2 標的型攻撃とOperation Aurora

近年、標的型攻撃による被害が問題視されています。2010年1月にグーグル社は、中国における事業の方針転換を表明した公式ブログ記事<sup>\*53</sup>の中で、2009年12月から標的型攻撃を受けていたことを明らかにしました。この攻撃は、Operation Auroraと名付けられ、大きく取り上げられました。

#### ■ 特定の対象を狙う標的型攻撃

標的型攻撃は、特定の組織や人々を対象とした攻撃です。ネットワークワーム感染のように、不特定多数が対象となる無差別の攻撃とは異なり、攻撃の範囲を限定した上で、標的とする組織や人に合わせた話題を用いる等の手法が使われます。典型的な手口は、なりすましメールによる攻撃です。攻撃対象にとって実際に関係する組織や人を発信者にかたったメールを悪用し、表題、本文、添付ファイルに至るまで、いかにも受信者の業務に関連した内容のように思わせ、添付ファイルを開くように誘います。添付ファイルにはアプリケーションの脆弱性を悪用する攻撃コードが含まれていて、添付ファイルを開くとマルウェアに感染させられます。

このマルウェアには、他のマルウェアをダウンロードする等の手法によって、検知や解析を難しくする仕組みを備えたものが多いようです。これらのマルウェアに感染すると、表面上は何ら症状が見られずにマルウェアに潜伏され、気付かないうちに機密情報が盗み取られていく可能性があります(図-11上段)。

#### ■ 標的型攻撃の事例

標的型攻撃は、2005年頃から広く知られるようになりました<sup>\*54</sup>。当初の攻撃対象は、主に政府機関で、日本でも官公庁を狙ったなりすましメールによる攻撃が報じられました<sup>\*55</sup>。その後、企業の経営層を狙った標的型攻撃も報告され始め<sup>\*56</sup>、民間企業等も攻撃対象になることが広く意識されるようになりました。

2008年6月には、コンピュータセキュリティに関するシンポジウムの論文募集アナウンスをかたる標的型攻撃が発生しました<sup>\*57</sup>。メールの本文は正規の文章を切り貼りして作られ、正規のPDFファイルにマルウェアを埋め込んで作られた添付ファイルとともに送付されました。このときの攻撃対象はセキュリティ専門の研究者

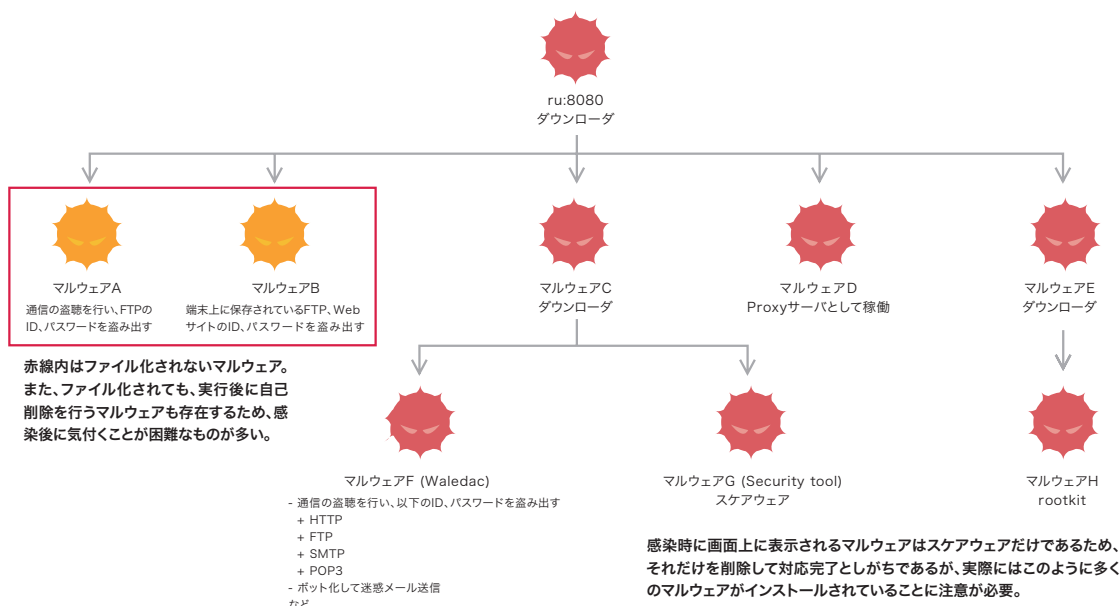


図-10 ru:8080がインストールするマルウェアの一例

\*53 Official Google Blog: A new approach to China (<http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>).

\*54 US-CERTによる2005年7月の注意喚起: US-CERT Technical Cyber Security Alert TA05-189A -- Targeted Trojan Email Attacks (<http://www.us-cert.gov/cas/techalerts/TA05-189A.html>).

\*55 例えば、外務省による次の注意喚起がある。外務省: 外務省を発信元と詐称するウィルスメールにご注意ください ([http://www.mofa.go.jp/mofaj/press/oshirase/18/osrs\\_0120.html](http://www.mofa.go.jp/mofaj/press/oshirase/18/osrs_0120.html)).

\*56 例えば SANS ISCのHandler's Diary: Better Business Bureau targeted malware spam (<http://isc.sans.org/diary.html?storyid=2853>).

\*57 情報処理学会コンピュータセキュリティ研究会による次の報告には、状況推移や対応の記録をはじめ、添付されたマルウェアの解析結果など、詳細な情報がまとまっている。CSS2008のCFPを騙ったウィルスメールに関する情報 (<http://www.iwsec.org/csec/css2008-cfp-secinfo.html>).

でした。また、2009年に新型インフルエンザの感染が拡大しつつあった時期に、医療研究機関からの注意喚起を装ったメールが、企業等の組織の新型インフルエンザ対策を担当する人々に送られました\*58。

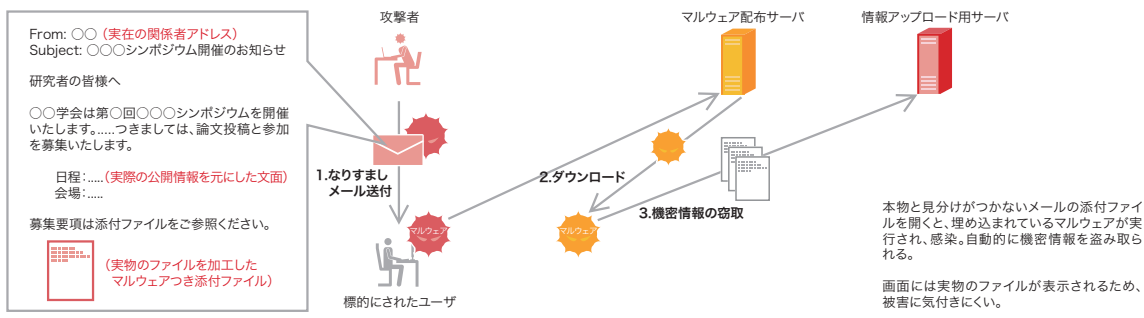
### ■ Operation Aurora

2010年1月に公表されたOperation Auroraも、民間企業を狙った標的型攻撃と考えることができます。攻撃対象は、グーグル社だけではなく、数十社の米国企業に及んでいます\*59。

この事件では、メールやインスタントメッセージを通して悪意のあるWebサイトへのリンクが送られたと

言われています。リンクをクリックすると、JavaScriptによりInternet Explorerの未知の脆弱性\*60を悪用した0-day攻撃\*61が実行され、マルウェアに感染させられました\*62。このマルウェアはC&Cサーバに接続し、攻撃者からの命令を受け、ファイルや設定を盗んだり書き込んだりする機能や、新たなマルウェアをダウンロードして実行する等の機能を持っています\*63。また、デスクトップ共有の機能もっており、攻撃者が感染PCの画面を監視でき、自由に操作できる状態になっていました。この様な感染PCを踏み台に、企業内ネットワークにある他のホストの情報にもアクセスされ、ソースコード等の企業秘密が盗まれたとされています(図-11下段)。

#### ▶ マルウェアを添付したなりすましメールによる攻撃の一般例



#### ▶ Operation Auroraにおける攻撃

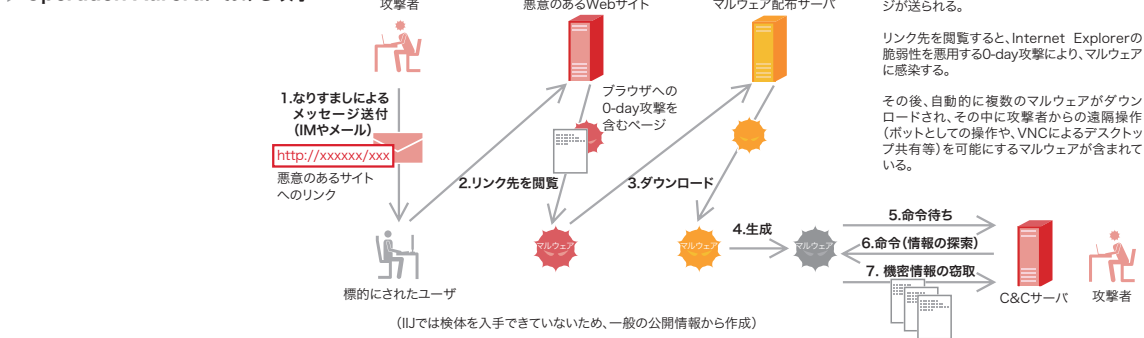


図-11 なりすましメールによる標的型攻撃

\*58 この事例については、本レポートの Vol.4 「1.2 インシデントサマリ」で触れている ([http://www.ij.ad.jp/development/ir/pdf/ir\\_vol04.pdf](http://www.ij.ad.jp/development/ir/pdf/ir_vol04.pdf))。  
 \*59 Operation Auroraについては、US-CERTからも注意喚起のアドバイザリが発行されている (<http://www.us-cert.gov/cas/techalerts/TA10-055A.html>)。このアドバイザリでは感染ホストの検出に役立つ技術情報も提供されている。  
 \*60 この脆弱性は、Googleによるブログ記事の公表後、すぐに修正された。マイクロソフト セキュリティ情報MS10-002 - 緊急 :Internet Explorer用の累積的なセキュリティ更新プログラム(978207) (<http://www.microsoft.com/japan/technet/security/bulletin/MS10-002.msp>)。  
 \*61 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。  
 \*62 この攻撃コードやマルウェアの解析結果は、例えば次のレポートに詳しい。HBGary Threat Report: Operation Aurora (<http://www.hbgary.com/press/hbgary-threat-report-operation-aurora/>)。  
 \*63 本件のマルウェアHydraqの解析報告は、例えば次の記事がある。ThreatExpert Blog: Trojan.Hydraq Exposed (<http://blog.threatexpert.com/2010/01/trojanhydraq-exposed.html>)。

また、この事件と同一の脆弱性を悪用するWebサイトの発見や、そうしたサイトへのリンクを仕込んだ標的型攻撃のメールも報告され、Operation Auroraに限らず、標的型攻撃の被害拡大が懸念されました。さらに、この事件に便乗して、Aurora関連の情報と称したメールを送付する標的型攻撃まで発生したとの情報もあります\*64。

#### ■ 標的型攻撃の対応の難しさ

これらの事例が示すように、個々の標的型攻撃はその対象が限定されています。しかし、その対象は多岐にわたり、現在では誰もが狙われる可能性がある身近な脅威となっています。また、その手口は巧妙で、顕在化しにくいことから、標的型攻撃への対応は難しいとされています。このため、標的型攻撃への備えとしては、まず、なりすましメールにだまされないための対策を行うことが考えられます。教育や演習\*65などを通じてユーザの意識を高く保つこと、そして、電子署名や送信ドメイン認証のような発信者の確認に役立つ仕組みを利用することが挙げられます。また、標的型攻撃では、未知の脆弱性や、ウイルス対策製品が対応していないマルウェアが悪用されることがあります。この場合、攻撃に気付いた後の対策として、情報の共有が重要になります。事前にウイルス対策製品ベンダやセキュリティ専門家と相談できる関係を築いておくことや、事後にセキュリティの専門組織に相談\*66することが有効です。

#### 1.4.3 マルウェア対策活動MITF

ここでは、IJが実施しているMITF (Malware Investigation Task Force) について説明します。MITFは、2007年5月から続けているマルウェア対策のための活

動です。いくつかの調査において\*67、発生するインシデントがネットワークごとに異なる状況にあることが判明し、IJが運用するネットワークの状況を独自に把握するためにMITFを開始しました。MITFでは、専用の装置でマルウェアの活動を検知し、マルウェアを収集して解析を行い、対策に必要な情報を抽出しています\*68。

#### ■ マルウェアを取得するための仕組み

インターネット上のマルウェアの感染活動には、ウイルスなどのファイルを経由した感染だけでなく、ネットワーク上での直接感染、Webコンテンツ経由の感染、メール経由の感染などが考えられます。ここでは、これらの感染活動を観測する仕組みとして、ハニーポットとWebクローラを説明します。

ハニーポットでは、脆弱性のエミュレーション機能を持つホストをインターネットに接続し、外部から無作為に到着する通信を観測します。マルウェアの感染活動がネットワーク経由でこのハニーポットに到着し、脆弱性が適合すると、攻撃元の情報やマルウェアの検体が取得できます\*69。MITFでは、IJが運用する日本全国の網にこのハニーポットを設置し、マルウェアの活動を観測しています。その密度は、IPアドレス空間/23ごとに1台 (IPアドレス512個につき1台) としています。

Webクローラは、通常のWebブラウザと同様に、検査対象のURLの一覧に順次アクセスし、脆弱性などを利用した攻撃を含むコンテンツを受け入れます。この結果、実際にマルウェアに感染して、検体を入手します\*70。MITFの開始当初、Webクローラは試験的に構築し運用

\*64 エフセキュアブログ:「Operation Aurora」をエサにした標的型攻撃 (<http://blog.f-secure.jp/archives/50339288.html>)。

\*65 例えばJPCERT/CCは擬似攻撃メールを用いた実地調査を行い、その結果を報告している (<http://www.jpccert.or.jp/research/#inoculation>)。

\*66 標的型攻撃の相談窓口としては、IPAの不審メール110番 (<http://www.ipa.go.jp/security/virus/fushin110.html>) や、JPCERT/CCへのインシデント報告の届出 (<http://www.jpccert.or.jp/form/>) 等がある。

\*67 例えばJPCERT/CCの調査研究 (<http://www.jpccert.or.jp/research/#botnet>) 等。

\*68 日本国内においてはサイバークリーンセンター (<http://www.ccc.go.jp/>) が先に同様の活動を開始しており、この活動にはIJも参加しているが、日本の全体像を把握する試みに加え、IJの網内をより詳細に調査する必要があると判断した。実際に両者の観測結果には差異があり、その差異についてはMWS2009 (<http://www.iwsec.org/mws/2009/presentation/A2-2.pdf>) やIJ.news ([http://www.ij.ad.jp/news/ijnews/2009/\\_icsFiles/afiefieldfile/2009/01/07/vol90.pdf](http://www.ij.ad.jp/news/ijnews/2009/_icsFiles/afiefieldfile/2009/01/07/vol90.pdf)) 等で公開している。

\*69 ハニーポットの実装としては、例えば、dionaea (<http://dionaea.carnivore.it/>) 等。製品としてはSPECTER (<http://www.specter.com/>) 等がある。このハニーポットとして実際に脆弱性を持つOSのPCを利用する事もあるが、IJでは、悪用される可能性を極力排除するために、脆弱性をエミュレーションする実装を選択している。

\*70 Webクローラの実装には、例えばHoneySpider (<http://www.honeyspider.net/>) がある。製品としてはフォティオンフォティ技術研究所のOrigma+ (<http://www.fourteenforty.jp/products/origma/>) 等。

していました。しかし、Gumblar に代表されるWebコンテンツで感染するマルウェアの流行に伴い、現在ではマルウェア取得のための重要な構成要素となっています。

MITFでは、これらの他にも迷惑メールからマルウェア感染に誘導される様子を観測するための仕組みや、P2Pファイル共有ネットワーク等で交換されるファイルを観測するための仕組みも利用しています。

#### ■ マルウェアを解析するための仕組み

MITFでは、取得したマルウェアの検体から、対策の検討に必要な情報を抽出する仕組みも用意しています。ただし、ここでの解析の目的は、マルウェアの検知や駆除ではなく、その活動による通信特性(宛先やプロトコル、通信量等)に注目した情報の収集です。

解析手法の1つである動的解析では、外部に接続していない閉じたネットワーク環境で、仮想のインターネットを再現し、そこで実際にマルウェアを動作させることで、動作に伴って発生する通信の様子を観測します\*71。このため、動的解析環境には、マルウェアからの要求に応答するDNSサーバ、HTTPサーバ、IRCサーバなどの機能が用意されています。また動的解析では、通信の様子とともに、マルウェアによるファイル生成やプロセス生成の様子も観測します\*72。この解析により、ダウンロードサーバ、アップデートサーバ、ボットネットのC&CサーバのIPアドレスやURLを特定することができます。この手法では、ウイルス対策製品等で判別できない未知のマルウェアに関しても、その活動を阻害するための有益な情報を取得することが可能です。

もう1つの解析手法である静的解析では、まず、取得したマルウェアの検体を複数のウイルス対策製品で検査

します。マルウェアの名前や機能に関して参照可能な外部情報があるときには、それらを参考にします。また、閉環境や仮想マシン環境を検知する仕組みを持つマルウェアもあり、動的解析だけでは情報を抽出できないことがあります。この場合には、解析ツールを利用して手作業で解析を行います。さらに、マルウェアの検体は、協力関係にある研究機関やウイルス対策製品ベンダ\*73にも提供しています。

#### ■ MITFの全体像と今後の予定

図-12に、MITFの全体像を示します。ここに示すように、取得したマルウェアとその解析情報は、セキュリティサービスの設定として還元するなど、お客様のネットワークの保護やIJのネットワークの安全な運用のために役立てています。

今回説明したMITFの環境では、これまでこのレポートで示してきたものよりも多くの情報が取得されています。たとえば、探索行為を行っている行為者に関する情報や、活動しているマルウェアの種類、IPアドレスを詐称された通信の戻りパケット(backscatter)によるDDoS攻撃の検知等です。今後は、このような情報も提供していく予定です。

また、MITFの開始当初に比べて、ネットワーク上で直接感染するマルウェアの活動は下火になりつつあり、Webコンテンツから感染するマルウェアに推移しています。今後、IPv6の利用推進やクラウド利用の一般化などネットワークの利用方法が変化することで、発生するインシデントの傾向も変わっていくと考えられます。MITFでは、このような変化に適切に対応できるように準備を行っています。

\*71 この閉じた仮想的なインターネットは、IJで独自に実装したものです。

\*72 このような機能を実現する実装には、例えばProcess Monitor (<http://technet.microsoft.com/ja-jp/sysinternals/bb896645.aspx>) がある。

\*73 2010年4月の段階では、複数のウイルス対策製品ベンダや、セキュリティ団体、研究機関に対して検体を提供している。IJでは、IJの網内で流行しているマルウェアについて、ユーザの利用する可能性のあるウイルス対策製品で適切に対処されることを望んでいる。ご協力いただけるウイルス対策製品ベンダはIJグループセキュリティコーディネーションチーム(IJ-SECT) <[sect@ij.ad.jp](mailto:sect@ij.ad.jp)>にコンタクトをお願いします。

## 1.5 おわりに

このレポートは、IJが対応を行ったインシデントについてまとめたものです。今回は、現在でも継続中であるGumblar類似の事件と標的型攻撃、そしてIJのマルウェア対策活動であるMITFについて説明しました。

IJでは、このレポートのようにインシデントとその対応について明らかにし公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を続けてまいります。

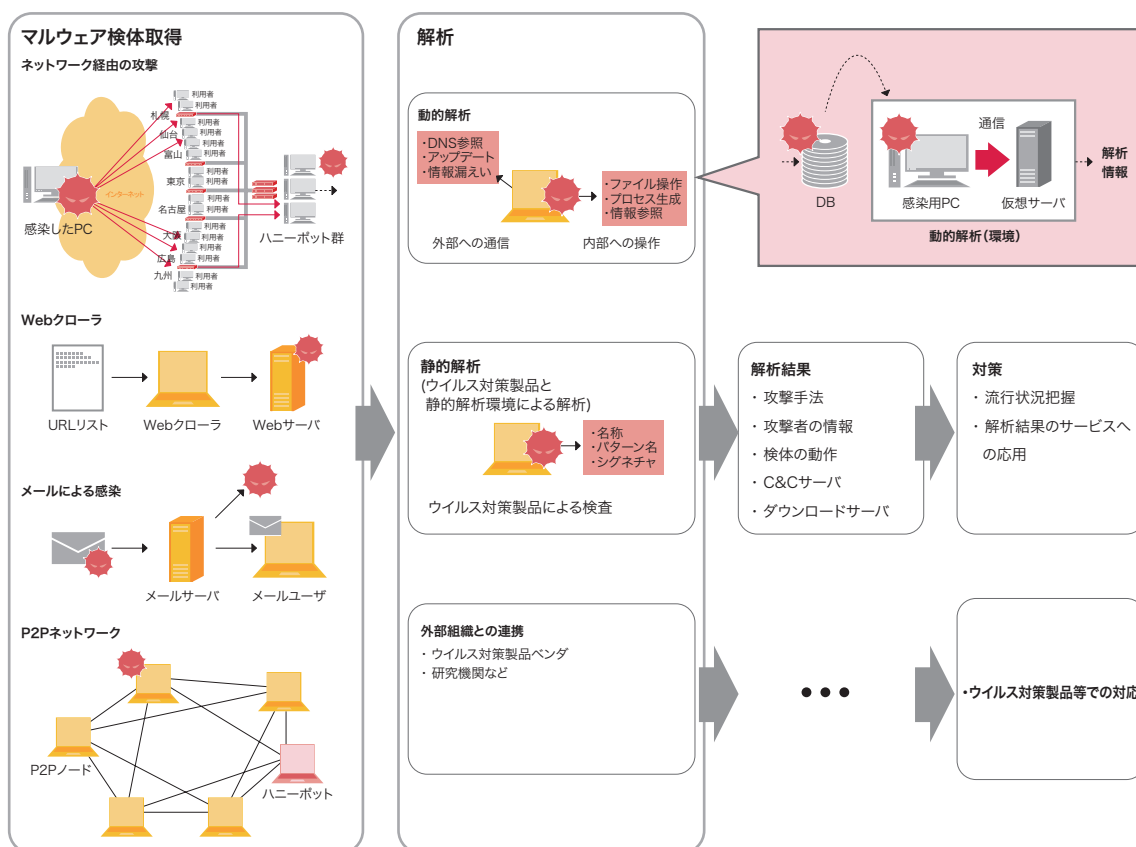


図-12 MITFのフレームワーク

執筆者:

齋藤 衛(さいとう まもる)

IJ サービス本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発等に従事後、2001年よりIJグループの緊急対応チームIJ-SECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会、Web感染型マルウェア対策コミュニティ等、複数の団体の運営委員を務める。IJ-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型の攻撃スキームを持つ ru:8080)

永尾 禎啓 (1.4.2 標的型攻撃とOperation Aurora)

齋藤 衛 (1.4.3 マルウェア対策活動MITF)

IJ サービス本部 セキュリティ情報統括室

協力:

加藤 雅彦 須賀 祐治 吉川 弘晃 IJ サービス本部 セキュリティ情報統括室