

# 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、IJ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、IJが対応したインシデントについてまとめたものです。

このVol.2 では、Vol.1よりも1ヵ月長い 2008年9月から12月を対象とし、この間に発生したインシデントや観測状況を示しています。次号以降は対象期間を四半期(3ヵ月)とする予定です。

この4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、イスラエル軍によるガザ地区への侵攻等の国際情勢の動きがあり、これにともなうネットワーク上の攻撃が発生しています。また、スポーツイベントにともなう攻撃も発生しました。

脆弱性の分野では、TCPやIPv6、無線LAN等、通信プロトコルに関連する脆弱性の発見が相次ぎました。このような脆弱性では、実装ごとの脆弱性よりも影響範囲が大きくなることが多いため、IJではより迅速な対応を心がけています。

インターネット上のマルウェアの活動では、種類では従来の数を維持していますが、検体の取得総量は減少しています。またDDoS攻撃では、その攻撃件数は増えたものの、それぞれの攻撃は比較的小規模なものでした。Webサーバに対するSQLインジェクション攻撃に関する観測では、大規模な攻撃の試みを検知しています。

以上のように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

## 1.2 インシデントサマリ

ここでは、2008年9月から12月の期間にIJが取り扱ったインシデントについて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、分類の説明について表-1に示します。

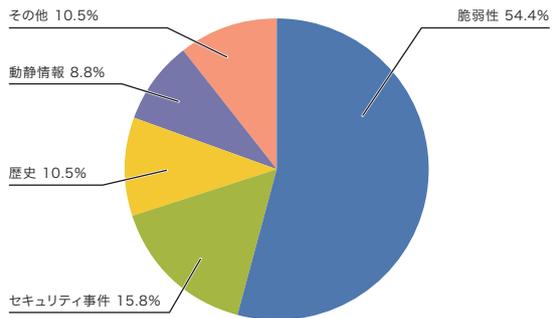


図-1 カテゴリ別比率(2008年9月~12月)

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、またはユーザー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。

## ■脆弱性

この期間には、通信プロトコルに関わる脆弱性が多く発見されました。まず、IPv6<sup>\*1</sup>に関する脆弱性が複数発見されています。続いて、TCP<sup>\*2</sup>、無線LANの暗号化プロトコルである WEP<sup>\*3</sup>やWPA/TKIP<sup>\*4</sup>、OpenSSH<sup>\*5</sup>について脆弱性が発見されました。また、マイクロソフトのOSで広く攻撃可能なMS08-067<sup>\*6</sup>や、Internet Explorerの脆弱性であるMS08-078<sup>\*7</sup>、更に、多くのブラウザで発現したクリックジャッキング<sup>\*8</sup>等、クライアントOSやクライアントで利用されているアプリケーションで悪用されるような問題が明らかになっています。その他としては、MD5で署名された証明書を偽装する手法<sup>\*9</sup>が大きな話題になりました。

## ■動静情報

この期間中にもスポーツの大会等の国際的なイベントや国際情勢の変化がありました。特に12月のフィギュアスケートの大会に関連した攻撃が報道等で大きく取り扱われています。また、イスラエル及び近隣諸国との情勢に応じた国際的な攻撃も発生しています。しかし、IJの設備及びIJのお客様のネットワークでは直接関連する攻撃は検出されませんでした。

## ■歴史

この期間には太平洋戦争終結日、満州事変、真珠湾攻撃等が含まれており、各種の動静情報に注意を払いましたが、関連するネットワーク上の攻撃は見られませんでした。

## ■セキュリティ事件

動静情報等に結び付かない突発的なインシデントとしては、IP電話に無言電話を引き起こすような攻撃、MS08-067を悪用したマルウェア、クリスマスや新年を祝うメールを装い、マルウェア感染に誘導する試み等が発生しています。また、12月の後半には、特定のWebサーバに対するSQLインジェクション攻撃の増加が観測されています。

## ■その他

IJでは、この期間のうち再起動が必要なマイクロソフトの修正リリースのタイミングで突発的な通信量の減少を観測しています(9月の定例、10月の定例、10月末のMS08-067緊急リリース等)。また、海外において、多くのボットネットのC&Cサーバを収容していた事業者がインターネットから切断されたこと<sup>\*10</sup>に起因した迷惑メールの減少を観測しました。

最近の脆弱性情報の取り扱いでは、研究者等がまず脆弱性の存在のみを発表し、対策を促した後、詳細を後日発表するという公開パターンが増えてきています。例えばKaminskyのDNSキャッシュポイズニング手法がそうでした。ここで示した中でも、TCPとOpenSSHの脆弱性については、その詳細は未だに発表されていません。IJでは、このような状況においても、適切に脅威評価や対応を行うため、公開情報に基づいた脆弱性の再現や、対策コミュニティへの参加、発見者に連絡を取って詳細情報を確認する等の活動をしています。

- \*1 IPv6にかかわる脆弱性としては、例えば、FreeBSDのicmp6の脆弱性(<http://security.freebsd.org/advisories/FreeBSD-SA-08:09.icmp6.asc>)や、NetBSDのMLD queryパケットに関する脆弱性(<http://jvn.jp/cert/JVNVU817940/>)、IPv6実装におけるForward Information Baseのアップデートに関する問題(<http://jvn.jp/cert/JVNVU472363/index.html>)等。
- \*2 TCPの脆弱性の詳細はまだ公表されていない。フィンランドのCSIRT組織CERT-FIからのこの問題への対応状況を示す文章が発表されている(<https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>)。
- \*3 WEPの暗号化が現実的な時間で破られることは古くから知られていたが、コンピュータセキュリティシンポジウム2008 (<http://css2008.la.coocan.jp/>)において、非常に短い時間で破る方法が神戸大学の森井昌克教授らにより発表された。
- \*4 WPA/TKIPへの攻撃に関する発表(<http://dl.aircrack-ng.org/breakingwepandwpa.pdf>)。
- \*5 OpenSSHの脆弱性の詳細は現時点では公開されていない。英国CPNIによりこの問題への注意喚起が発表されている([http://www.cpni.gov.uk/Docs/Vulnerability\\_Advisory\\_SSH.txt](http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt))。
- \*6 MS08-067 (<http://www.microsoft.com/japan/technet/security/Bulletin/MS08-067.msp>)。
- \*7 MS08-078 (<http://www.microsoft.com/japan/technet/security/bulletin/ms08-078.msp>)。
- \*8 US-CERTによる Current Activity([http://www.us-cert.gov/current/archive/2008/10/01/archive.html#multiple\\_web\\_browsers\\_affected\\_by](http://www.us-cert.gov/current/archive/2008/10/01/archive.html#multiple_web_browsers_affected_by))。
- \*9 MD5の脆弱性(<http://www.kb.cert.org/vuls/id/836068>)や、MD5により署名された証明書に対する攻撃(<http://www.win.tue.nl/hashclash/rogue-ca/>)等。
- \*10 SANS ISCのHandler's Diary(<http://isc.sans.org/diary.html?storyid=5333>)等。

## 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、継続的に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

今日では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ることや、サーバの処理を過負荷にすることで、サービスを妨害するという目的を達成しようとしています。

ここで、2008年9月から12月の期間にIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を図-2に示します。この情報は、IJ DDoS対策サービスの基準で攻撃と判定された通信異常を件数で示したものです。IJでは、この他に接続サービスをご利用のお客様に対する攻撃等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。加えて、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<sup>\*11</sup>、サーバに対する攻撃<sup>\*12</sup>、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4ヵ月の期間中、IJでは479件のDDoS攻撃を扱っており、1日あたりでは4件程度となります。平均発生件数は、前回のレポートの期間よりもやや増加しました。全体の内訳は、回線容量に対する攻撃が1%、サーバに対する攻撃が95%、複合攻撃が4%です。

この期間は、サーバに対する攻撃が数多く発生していますが、例えば最大規模のSYN floodで20,000pps程度と、それぞれの規模は大きくありませんでした。この攻撃の対象はほとんどがWebサーバ(80/TCP及び443/TCP)であり、メールサーバ(25/TCP)への攻撃はごく少数のみを観測しました。回線容量に対する攻撃や複合攻撃においては、最大で100Mbps程度の攻撃が見られる状況でした。

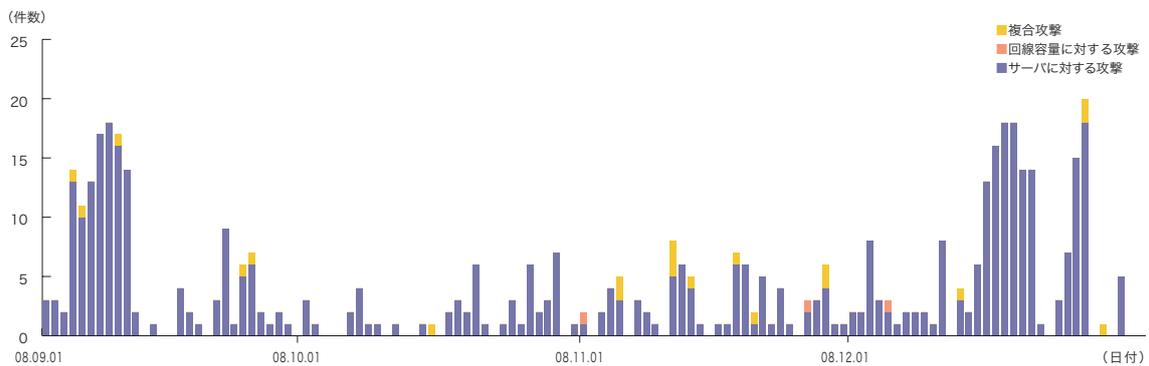


図-2 DDoS攻撃の発生件数

\*11 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。

\*12 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。

また、攻撃の継続時間については、全体の64%が攻撃開始から30分未満で終了し、35%が30分以上24時間未満の範囲で分布しています。ただし、数件ではあるものの、数日間にわたって継続する攻撃も発生しました。特に、年末において、特定のWebサーバへの長期にわたる継続的な攻撃を検出しましたが、その規模は大きくなく、動静情報との関係も見られませんでしたので、突発的な攻撃として対処を行っています。

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<sup>\*13</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>\*14</sup>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、IJJが実施しているマルウェアの活動観測プロジェクトMITF<sup>\*15</sup>による観測結果を示します。MITFでは、インターネットに一般利用者と同様に接続したハニーポット<sup>\*16</sup>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、攻撃先を探す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

まず、2008年9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アドレスの分布を国別に図-4に示します。

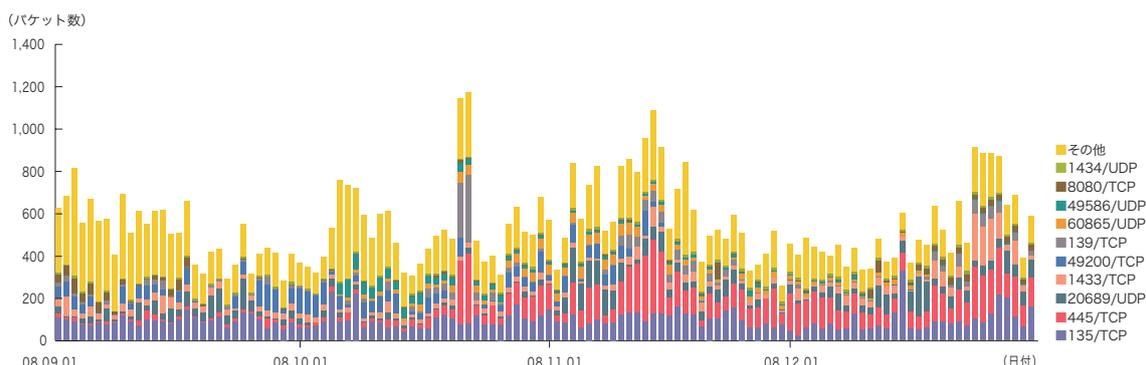


図-3 ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

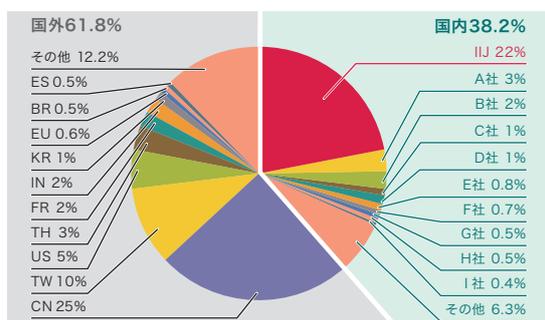


図-4 発信元の分布(全期間)

\*13 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。  
 \*14 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。  
 \*15 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。  
 \*16 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。

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。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)について全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わかります。一方で、20689/UDPや49200/TCP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ました。また、10月21日から445/TCP及び139/TCPへの攻撃が増加していますが、これはMS08-067の脆弱性を狙った攻撃の増加を示しています。発信元の分布を国別に見ると、日本国内の38%、中国の25%が比較的多くなっています。

■ ネットワーク上でのマルウェアの活動

次に、MITFで観測したマルウェアの活動について示します。同じ期間中における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に示します。取得検体数の推移では、総取得検体数は1日あたりに取得できた検体<sup>\*17</sup>の総数を示し、ユニーク検体数は検体の種類をハッシュ値<sup>\*18</sup>で分類したものです。

期間中の一日平均としては、総取得検体数で2,235検体を、種類で55種類程度のマルウェアを取得しています。前回のレポートの期間では、一日平均の総取得検体数で8,000ほど、種類では60種類でしたので、この期間

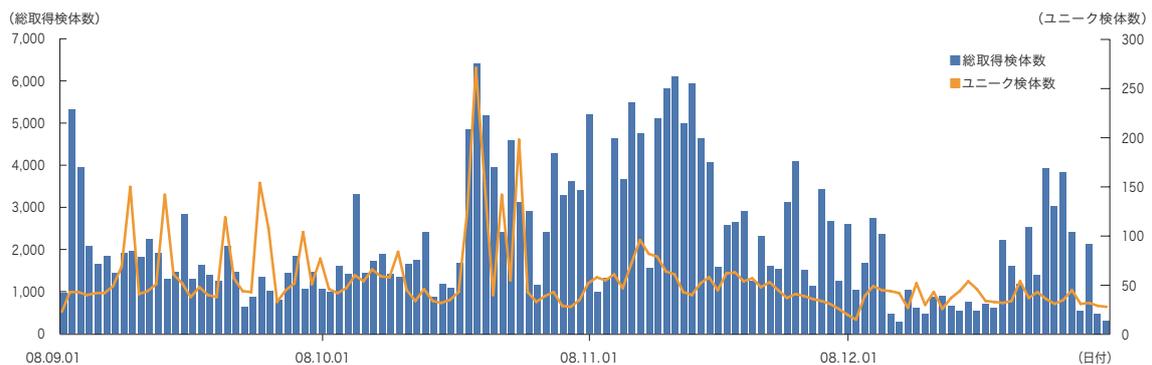


図-5 取得検体数の推移(総数、ユニーク検体数)

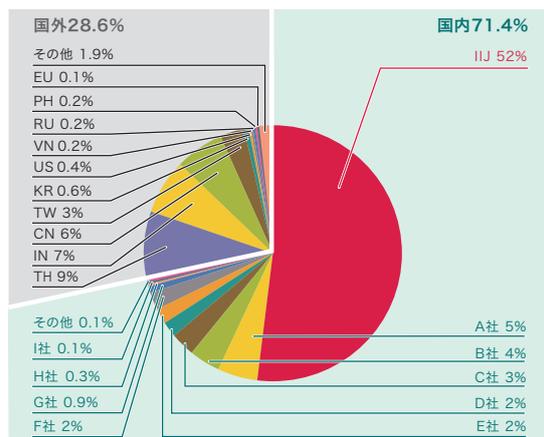


図-6 検体取得元の分布(全期間)

\*17 ここでは、ハニーポット等で取得したマルウェアを指す。

\*18 様々な入力に対して一定長の出力をする一方性関数(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。

中では、総取得検体数が大幅に減少傾向にありました。これは、この期間中に広範囲のIPアドレスで感染活動を行うマルウェアの流行が見られなかったため、特に、国外からのマルウェア感染活動が著しく減少しています。このため、検体取得元の分布では、日本国内が71.4%、IJのユーザ同士のマルウェア感染活動が52%と、その比率が増加しました。しかし、日本国内においても取得検体数の総数は減少しており、全体として沈静化傾向が見られます。Vol.1の期間と今回の期間の総取得検体数の比較を図-7に示します。

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11%、ボット型58%、ダウンロード型31%となりました。また、この解析により、73個のボットネットC&Cサーバ<sup>\*19</sup>と415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

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<sup>\*20</sup>について継続的に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。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たりします。また、最近流行している攻撃では、コンテンツ改ざんの結果として、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。

まず、2008年9月から12月の期間中に検知したWebサーバに対するSQLインジェクション攻撃の推移を

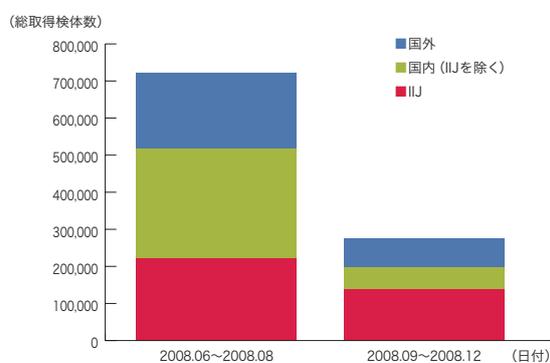


図-7 総検体取得数の比較 (Vol.1とVol.2)

\*19 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。

\*20 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。

図-8に、攻撃の発信元の分布を図-9に示します。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についてまとめたものです。ただし、後述の大規模攻撃については除外しています。発信元と攻撃先、及び攻撃手法の組み合わせについて解析したところ、SQLインジェクション攻撃については、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。発信元の分布では、日本36.7%、米国22.9%、中国11.0%となり、以下その他の国が続いています。

また、他のセキュリティベンダによるレポート<sup>\*21</sup>にもあるように、12月には大規模なSQLインジェクション攻撃が発生しており、IJにおいても突発的な攻撃増加

を観測しています。ただし、この増加は全般的な傾向ではなく、特定少数のWebサーバにおいてのみ観測されました。突発的なSQLインジェクションの増加を検出したWebサーバにおける攻撃の推移を図-10に、その攻撃の発信元の分布を図-11に示します。このように、これらのWebサーバに対しては、他のWebサーバと比べ1,000倍以上の攻撃が発生していました。この攻撃の発信元としては、韓国52.7%と日本41.1%が大半を占めています。これら少数のWebサーバが特に狙われた理由は不明です。

以上の攻撃について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おり、引き続き注意が必要な状況です。

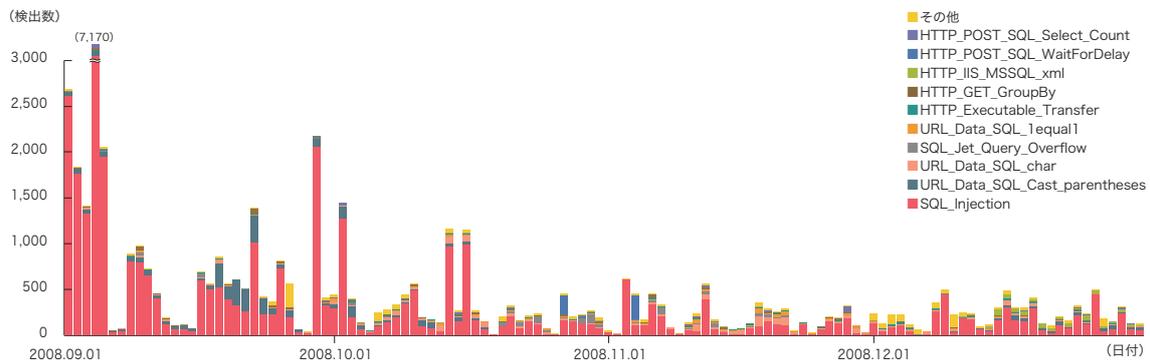


図-8 SQLインジェクション攻撃の推移（日別、攻撃種別）

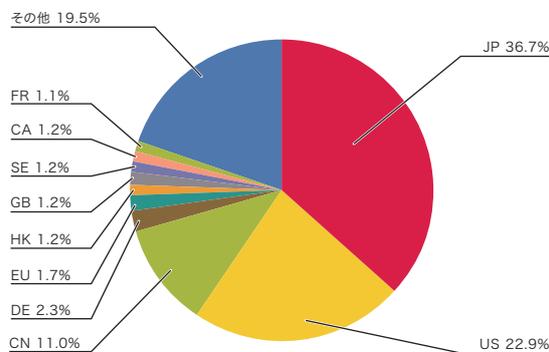


図-9 SQLインジェクション攻撃の発信元の分布(全期間)

\*21 例えば、株式会社ラックによる注意喚起(<http://www.lac.co.jp/news/press20081222.html>)等。

## 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、IJ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、DNSキャッシュポイズニング、MS08-067を悪用するマルウェア、無線LANのセキュリティへの攻撃について示します。

### 1.4.1 DNSキャッシュポイズニング

DNSキャッシュポイズニングの問題は、その攻撃の容易さや、効果の深刻さ、そして対策の難しさ等の理由で、2008年に非常に大きな話題となりました。

### ■DNSとその動作

DNS(Domain Name System)とは、問い合わせに対して対応するリソースを応答するシステムです。インターネットでは、主に名前解決に利用されており、ホスト名(Fully Qualified Domain Name: FQDN)を、IPアドレスに変換するために利用されています。私たち人間は通常 www.example.co.jp 等のFQDNを覚えておいて通信先を指定しますが、インターネットに接続された機器は、すべてIPアドレスで通信先を指定します。つまり、DNSはインターネットで通信を成立させるために必要な、重要な仕組みの一つです。

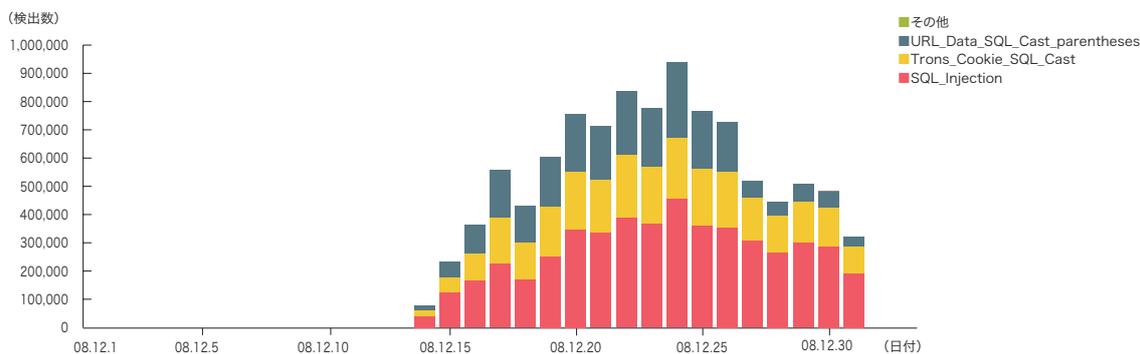


図-10 12月に発生した大規模なSQLインジェクション攻撃の推移 (日別、攻撃種類別)

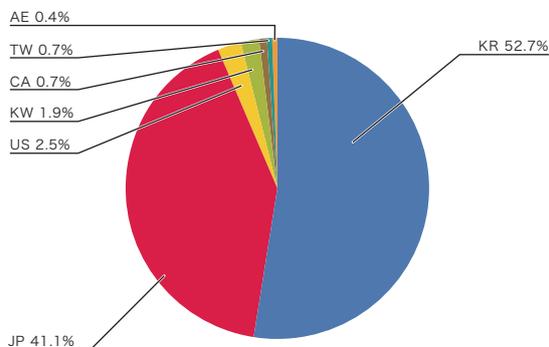


図-11 12月に発生した大規模なSQLインジェクション攻撃の発信元の分布

DNSによる名前解決は、通常、図-12(1)のように動作します。クライアントは実際の通信を行う前に名前解決の要求(クエリ)を、参照するDNSキャッシュサーバに送ります。DNSキャッシュサーバは、解決するドメインを管理するDNSコンテンツサーバに問い合わせます。DNSキャッシュサーバはその結果を受け取り、クライアントに回答するとともに、その解決結果を指定された期間保存します。DNSキャッシュサーバは、ISPが運用していたり、組織内ネットワークで独自に運用されていたりするもので、インターネットへの接続時にDHCP等を通じて自動的に指定されます。このため、通常はユーザが自分の参照するDNSキャッシュサーバを意識することはありません。

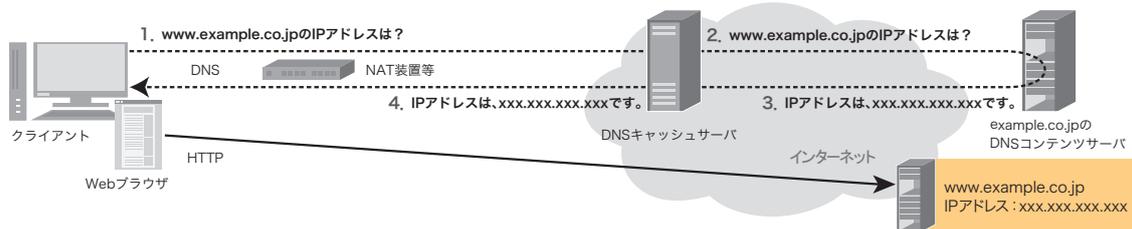
■DNSキャッシュポイズニングとは

DNSキャッシュポイズニングとは、何らかの方法でのDNSキャッシュサーバに偽の応答を送り込み、偽の名前解決の情報を保存させることを意味しています。偽の情報を保存させられたDNSキャッシュサーバを参照しているクライアントは、フィッシングサイト等の偽のサーバに誘導される危険にさらされることになります。また、利用者側で偽の応答を受け取ったことを判別できないことも、DNSキャッシュポイズニングの大きな特徴といえるでしょう。

DNSキャッシュポイズニングの攻撃は、今回初めて明らかになったわけではなく、過去にも数回その危険性が

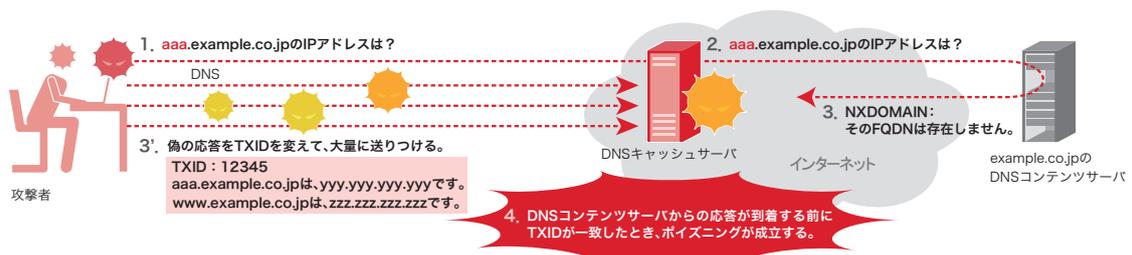
(1) 正常な名前解決の動作

正常なDNSの名前解決は、DNSキャッシュサーバを介してDNSコンテンツサーバに問い合わせを行う。



(2) Kaminskyの手法によるキャッシュポイズニング攻撃

Kaminskyの手法では、DNSキャッシュサーバに対して存在しないFQDNに関する名前解決要求を行い、同時に偽造した応答を大量に送付する。DNSコンテンツサーバからの応答が到着する前にTXIDが一致すれば、攻撃が成立する。



(3) キャッシュポイズニングの影響

ポイズニングされたDNSキャッシュサーバを参照すると、偽のサーバに誘導されてしまう。また、NAT装置等によって攻撃が成立しやすい環境が作り出されることもある(P14参照)。



図-12 DNSによる名前解決とキャッシュポイズニング

指摘され、対策が施されています<sup>\*22</sup>。今回話題となったKaminskyによる手法<sup>\*23</sup>は、過去の対策を実施していてもなお、現実的な時間でキャッシュポイズニングが成立する手法ということで大きな脅威となりました。

#### ■Dan Kaminskyの手法

今回 Kaminskyが明らかにした手法の概要を図-12(2)と(3)に示します。この手法は、DNS名前解決の応答をIPスプーフィングとTXIDを一致させることで詐称し、その偽の応答に余分な名前解決情報を付与することで成立します。

この図では、攻撃者はwww.example.co.jpについて、偽のIPアドレスに誘導する場合の攻撃の流れについて示しています。この試みは、正当なDNSコンテンツサーバからNXDOMAINが到着した時点で失敗に終わりますが、攻撃者は他の存在しないFQDN(例えば、bbb.example.co.jp等)を利用して何度でもリトライすることができ、全体として成立の可能性が高くなっています。

#### ■Kaminskyの手法への対策

では、このKaminskyの発見した手法に対してはどのような対策が考えられるのでしょうか。DNSのプロトコルを変更するには時間が必要であるため、以下の事項が推奨されました。

#### ■DNSキャッシュサーバの利用者を適切な範囲に限定すること

DNSキャッシュサーバがインターネット側から参照可能な場合、攻撃の可能性が増大します。設定ミス等によりインターネット側から参照可能なDNSキャッシュサーバがある程度存在していることは事実であるため、まずは今運用しているDNSサーバの設定を見直すこと

が推奨されました。

#### ■DNSクエリごとにUDPの発信元ポートを変更すること

DNSの名前解決1つ1つについて、問い合わせに利用するトランスポート(多くの場合UDP)のポートを動的に変更することで、偽の応答を受け取りにくくします。多くのDNSサーバの実装がKaminskyの手法への対策としてこの機能を採用しています。

また、一部のDNSキャッシュサーバの実装では、TXIDの詐称された応答が大量に発生したときに警告を発することで、DNSキャッシュサーバの管理者に攻撃発生の可能性を注意喚起するという機能を追加しています。

#### ■抜本対策のためには

これらの対策は、現状のインターネットにおいて、Kaminskyの手法に対して有効ですが、ワークアラウンドでしかありません。今後のインターネットをめぐる技術や環境の変化に応じて、従来の手法で再び攻撃が成立する状況になる可能性があります。例えば、すでにロシアの技術者によって、非常に理想的なネットワーク環境において、今回の対策済みのDNSキャッシュサーバに対して、10時間でポイズニングを成立させることができたという報告<sup>\*24</sup>がなされています。

このため、近い将来のうちにDNSSEC<sup>\*25</sup>等、より安全なプロトコルの利用に切り替えることが議論されています<sup>\*26</sup>。しかし、実際には、すべてのDNSキャッシュポイズニング攻撃をなくすためには、すべてのDNSサーバにおいてDNSSECに対応しなければなりませんし、DNSキャッシュサーバにおける処理の負荷増大の問題等で導入には多くのコストが必要と見込まれてい

\*22 例えば(<http://www.kb.cert.org/vuls/id/457875>)等。

\*23 Dan Kaminskyによるプレゼンテーション([http://www.doxpara.com/DMK\\_BO2K8.ppt](http://www.doxpara.com/DMK_BO2K8.ppt))。

\*24 Evgeniy Polyakovのブログ([http://tsservice.net.ru/~s0mbre/blog/devel/networking/dns/2008\\_08\\_08.html](http://tsservice.net.ru/~s0mbre/blog/devel/networking/dns/2008_08_08.html))。

\*25 DNSSEC (Domain Name System Security Extensions)では、DNSコンテンツサーバからの応答に電子署名を行う。DNSキャッシュサーバでは、この署名を検証することで、正当な応答であることを確認できる。

\*26 例えば、米国政府では、政府官公庁を示す.govドメインすべてに対し、2009年12月までにDNSSECに対応するように指示している(<http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf>)。

ます。更に、スウェーデン等、すでにDNSSECの導入を試みた国々では、ブロードバンドルータ等でのトラブル<sup>\*27</sup>が報告されています。このように、DNSSECの導入には、DNSサーバだけでなくユーザの環境まで含めた総合的な検証が必要であり、広く利用されるようになるには、まだまだ時間が必要です。

#### ■DNS参照環境の再確認を

繰り返しになりますが、DNSはインターネットを正常に利用するために必要なシステムです。今回の問題については、IJの運用するDNSキャッシュサーバではすでに対策を施しています。また、国内の他の大手通信事業者においても、すでに対応は終わっています。

一方で、このDNSキャッシュポイズニングは、ISPだけが対応すれば良いものではなく、利用者側でも対策が必要な場合があります。例えば、組織内部の攻撃者を想定すれば、企業ネットワークの内部のDNSキャッシュサーバにおいても対策が必要となります。また、DNSキャッシュサーバでUDPポートを動かす対策を行っていたとしても、NAT機能のある装置によってランダムであったUDPポートが昇順につけ変えられてしまうといった事例も報告されています。組織内部のDNSキャッシュサーバを利用している場合、DNSキャッシュポイズニングが成立したときには、気付かないうちに偽サーバに誘導されるといった被害を受ける場合があります。

これを機に、自分がどのような装置やサーバを経由してDNS名前解決を行っているかを調査し、次の点についてそれぞれが安全であることを確認してみることを

お勧めします<sup>\*28</sup>。

- 利用しているPCが参照しているDNSキャッシュサーバはどこにあるか調査する。特に、DNSキャッシュサーバが組織内ネットワークに構築されたものであるか、ISPのものであるかを調査する。
- 組織内ネットワークに構築されたDNSキャッシュサーバを利用している場合には、そのキャッシュサーバでクエリごとにUDPポートを動かすような対策がなされているかどうかを確認する。
- ISPのDNSキャッシュサーバを利用している場合には、そのISPのサーバが対策済であることを確認する。
- 組織内のネットワークとインターネットとの間にNAT機能をもった装置があるかどうかを確認する。NAT装置がある場合、そのNAT装置がDNSクエリのUDPポートを適切に扱えることを確認する。

#### 1.4.2 MS08-067を悪用するマルウェア

2008年10月24日、マイクロソフトから緊急パッチMS08-067<sup>\*29</sup>がリリースされました。マイクロソフトが10月より採用している悪用可能性指標<sup>\*30</sup>で「1-安定した悪用コードの可能性」<sup>\*31</sup>と評価されているところを見ても、その緊急性が高いことがうかがえます。

実際、「1.3.2 マルウェアの活動」図-3の無作為通信の状況に示したように、IJでの観測でも、10月21日からこの脆弱性を狙ったと判断できる通信が数倍から10倍程度に増加しています。加えて複数のお客様の組織内ネットワークにおいて、この脆弱性を悪用したマルウェアによるものと考えられる感染活動が観測されています。

\*27 DNSSECの署名等によってサイズが大きくなった名前解決の応答パケットを適切に処理できないブロードバンドルータによるトラブルが報告されている。次はスウェーデンの .SE (The Internet Infrastructure Foundation) によるルータの対応に関する調査(<http://iis.se/about/press?id=135> ※英語版は下の方のリンクにある)。英国のNominet U.K.による同様の調査では、調査対象の装置のうち、38%でDNSSECが利用できないとしている(<http://download.nominet.org.uk/dnssec-cpe/DNSSEC-CPE-Report.pdf>)。

\*28 確認作業に役立つ資料としては、独立行政法人情報処理推進機構(IPA)による「DNS (Domain Name System) の役割と関連ツールの使い方」([http://www.ipa.go.jp/security/vuln/DNS\\_security.html](http://www.ipa.go.jp/security/vuln/DNS_security.html))等。

\*29 この更新により修正される脆弱性の影響についてはSVRDのブログに詳しい(<http://blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx>)。また、この脆弱性を悪用した攻撃コードの存在も知られている(<http://www.microsoft.com/japan/technet/security/advisory/958963.mspx>)。

\*30 Microsoft Exploitability Index(悪用可能性指標)に関する説明(<http://www.microsoft.com/japan/technet/security/bulletin/cc998259.mspx>)。

\*31 MS08-067の悪用可能性指標については、10月のセキュリティ情報に掲載されている(<http://www.microsoft.com/japan/technet/security/bulletin/ms08-oct.mspx>)。

#### ■MS08-067

マイクロソフトの更新プログラムMS08-067は、NETAPI32.DLLの「NetprPathCanonicalize」APIに存在するスタックベースのバッファオーバーフローを修正するものです。この修正を行わないと、Windows Serverサービスがリモートから攻撃を受ける可能性があります。より具体的には、パスに「.¥ (1つ上のディレクトリを指定)」が含まれていた場合の処理に問題があります。また、この脆弱性の修正箇所は過去の修正であるMS06-040と類似しており、Windows 2000やXP、2003等、多くのWindows OSに共通して存在しています。

#### ■マルウェアConficker.A

11月に入り、この脆弱性を悪用するマルウェアが発見されました<sup>\*32</sup>。このマルウェアに感染すると、ネットワーク上では次の活動を行うことがわかっています。

- ランダムな宛先にMS08-067を悪用した攻撃を行い、自分自身を感染させようとする。
- 感染したPCにおいて、ランダムなポートでWebサーバを起動し、他のPCからの接続を受け付け、マルウェアを配布しようとする。
- 外部のWebサーバに接続し、新しいマルウェアをインストールしようとする。

このマルウェアが組織内のネットワークに入り込むと、活発な感染活動を行います。このマルウェアが企業内に設置されたファイアウォール等のセキュリティ境界をどのように越えたのかはわかりませんが、Webからのダウンロードや、USBメモリ等を介して感染する可能性があります。また、IJでは、Windows XP Embeddedをベースにしたシステムにおける感染事例も確認しています。

毎年数多くの脆弱性が発見され、対策がリリースされていますが、脆弱性にはマルウェアで悪用されやすい

ものとそうでないものが存在します。特定のアプリケーションや言語等環境に依存する脆弱性は、あまり広く利用されません。一方で、数年前の脆弱性が、いまだに最新のマルウェアで悪用されているような場合も見受けられます。

今回の脆弱性は多くのマイクロソフトのOSに共通で存在し、悪用されやすい脆弱性の一つだと言えます。今後も他のマルウェアで悪用される可能性が高いと考えられます。このような状況から、まだMS08-067の適用を実施していない場合には、早期の対策を行うことをお勧めします。特にWindows Embeddedを利用したシステムでは、修正がOEMベンダ経由での提供となるようですので、注意が必要です。

#### 1.4.3 無線LANのセキュリティへの攻撃

この9月から12月の期間において、無線LANのセキュリティ確保プロトコルである、WEPに対する攻撃とWPA/TKIPに対する攻撃が続いて発表されました。ここでは、無線LANのセキュリティプロトコルに対する攻撃とはどのようなもので、どの程度の危険があるのかについてまとめます。

#### ■無線LANとそのセキュリティプロトコル

無線LANにおいては、光ファイバ等の有線接続とは異なり、電波が届く範囲にいて無線を送受信する能力がある装置を持つ人は誰でも、無線LANを介した通信を受信(傍受)したり、その無線LANを勝手に使ったりして、他の利用者に成りすますことが可能です。

このため、無線LANを安全に利用するために、通信の暗号化や、通信相手や内容の正当性を検証することのできるセキュリティプロトコルが定義され、利用されています。しかし、このようなプロトコルは、無線LANの悪用を試みる人に通信を届かなくするものではありません。例えば、暗号化を利用したとしても、暗号化後

\*32 このマルウェアに関する説明は、「日本のセキュリティチームのblog」で和訳されている(<http://blogs.technet.com/jpsecurity/archive/2008/11/28/3160741.aspx>)。

の通信内容を傍受した上で、その内容に対して暗号理論的な解析を行い、復号を試みることができます。また、無線LANで通信を行っている人は、その通信が傍受されているとしても気付けないことにも留意しなければなりません。(図-13参照)

#### ■WEPに対する攻撃

WEPはもっとも早くから利用されている無線LANのセキュリティプロトコルですが、暗号化に利用するIV (Initial Vector)の採用方法に問題があり、この問題を利用してWEPの暗号化鍵を取得する手法は2001年から知られています\*33。また、2008年10月、神戸大の森井教授らは、既存の鍵攻撃手法を組み合わせで改良し、30,000IPパケットを観測することで0.5の確率で、50,000IPパケットを観測することで0.95の確率で、WEPの暗号化に用いる104ビットの秘密鍵を解読できると発表しています\*34。加えて、通常のPCを用いて実際に10秒程度で秘密鍵の取得に成功した例のビデオが公開されました。

#### ■WPA/TKIPに対する攻撃

WPAは、WEPと同じRC4暗号を利用する等、既存

のWEP対応機器のファームウェアを書き換えるだけで対応できる、WEPの延命を目的にした規格です。その鍵更新プロトコルとしてTKIP (Temporal Key Integrity Protocol)が利用されていますが、2008年11月に、このTKIPに対する攻撃\*35が発表されています。TKIPにおいて正当性検証のために付与されるメッセージ検証データ(MIC: Message Integrity Check)の生成アルゴリズム(MICHAEL)の不備を悪用し、一方向の(アクセスポイントからクライアント方向の)RC4から出力される乱数列の一部を取得した上で、MIC鍵の情報を得られるというものです。発見者らによると、攻撃者は無線LANアクセスポイントに成りすまして、最大7パケットを無線LANクライアントに送れるとしています。更に、この7パケットを悪用した攻撃の可能性についても検討を行っています。この手法によるMIC鍵の取得には12分から15分程度の間、通信の傍受が必要であり、鍵更新の頻度を非常に短く(例えば120秒程度)に設定することで、この攻撃を回避できるとされています\*36。この攻撃手法については、現時点で現実的な脅威といえないかもしれませんが、念のために鍵交換間隔を短くする対処を行ったほうが良いでしょう。



図-13 無線LANの傍受

\*33 FMS攻撃。例えば、Adam Stubblefield, John Ioannidis, Aviel D. Rubin, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP (<http://www.isoc.org/isoc/conferences/ndss/02/papers/stubbl.pdf>)等。

\*34 森井昌克 神戸大学大学院教授らによる発表資料は次より入手することができる(<http://srv.prof-morii.net/~morii/#CSS20081009>)。

\*35 Martin Beck, Erik Tews, Practical attacks against WEP and WPA (<http://eprint.iacr.org/2008/472>)。また、この攻撃手法は無線LANの攻撃ツール Aircrack-ngにも実装されている。

\*36 Cisco Security Response: Cisco Response to TKIP Encryption Weakness (<http://www.cisco.com/warp/public/707/cisco-sr-20081121-wpa.shtml>) ([http://www.cisco.com/en/US/products/products\\_security\\_response09186a0080a30036.html](http://www.cisco.com/en/US/products/products_security_response09186a0080a30036.html)) や、Aruba networks, TKIP Vulnerabilities (<https://edge.arubanetworks.com/article/tkip-vulnerabilities>)等。

## ■CCMPへの移行

WPAでの暗号化・メッセージ検証方式として、RC4の代わりに、より強力な暗号化アルゴリズムAESを採用したCCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) が規格化<sup>\*37</sup>され、WPA2<sup>\*38</sup>で利用可能となりました。現時点ではCCMPに対する攻撃は明らかになっていませんので、重要な通信を行うような無線LAN環境においては、CCMPの利用をお勧めします。

以上のように、今日では、WEPではもはやセキュリティを確保することはできず、組織内ネットワーク等重要な通信を行う場所での利用には、大きな危険がともなう状況になりました。一方で、家電等ではWEPのみにしか対応していない無線LAN対応機器がまだ多く利用されていますし、ファストフード店等の公衆無線LANアクセスポイント等は、今日でもWEPのみの対応で提供されています。このようなアクセスポイントを利用する場合には、事実上暗号化されていない裸の無線LANに接続するつもりで利用し、重要な通信を行う必要がある場合には、SSHやIPSecといった、より高度な暗号化に対応した通信プロトコルを併用する等、十分な配慮のもとに利用する必要があります。

今回ご紹介したように、無線LANのセキュリティプロトコルに対する攻撃手法は次々と明らかになっていきますし、暗号化アルゴリズムの危殆化<sup>\*39</sup>等も伴って、

状況が時々刻々と変化しています。無線LANのセキュリティについては、一旦設定したセキュリティ対策がいつまでも有効であるとはいえません。関連情報に注意し、攻撃手法の進化等に応じて見直しをかけながら利用していく必要があります。

## 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。このVol.2では、対象期間が通常よりも1ヵ月長いと、紙面の都合上もう少し詳しくお伝えしたい事柄について、項目だけの紹介にとどめている部分もあります。これらの事柄については、また別の機会に詳しくご紹介したいと思います。

また、2008年10月に実施されたマルウェア対策研究人材育成ワークショップ2008 (MWS2008)については、2009年1月に発行の広報誌 IIJ.news Vol.90<sup>\*40</sup>にて、対談の中で概要をお伝えしていますので、このレポートには記載しませんでした。併せて、IIJ.newsもご参照いただければ幸いです。

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、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、努力を続けてまいります。

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の開発等に従事後、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。

鈴木 博志 (1.4.2 MS08-067を悪用するマルウェア) 須賀 祐治 (1.4.3 無線LANのセキュリティへの攻撃)

荒田 恵子 永尾 禎啓 桃井 康成 大原 重樹 梅澤 威志

IIJ サービス事業統括本部 セキュリティ情報統括部

\*37 CCMPは、IEEE802.11iで規格化されている。また、CCMPで利用されるCCM (Counter with CBC-MAC)は、RFC3610に定義されている(<http://www.ietf.org/rfc/rfc3610.txt>)。

\*38 一般にWPA2として知られるWifi-Allianceによって定められた規格ではCCMPが採用されている。しかし、一部の無線LAN製品で「WPA2でTKIPの利用」や、「WPAでAESによる暗号化」という組み合わせが利用可能であるため、本稿では「WPA2は安全」や「AESなら安全」といった表現を使っていない。このように無線LAN機器の設定にはさまざまな表現が用いられており、設定インタフェース等での表現が、実際にどの暗号化手法と正当性検査の仕組みを表しているのかを、十分に確認してから利用したほうがよい。

\*39 アルゴリズム自身の問題の発見や、PCの性能向上等により、十分な暗号強度を確保できなくなる状況を指す。

\*40 IIJ.news(<http://www.iiij.ad.jp/news/iiijnews/2009/vol90.html>)。