

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.4では、2009年4月より6月までの3ヵ月間を対象としています。この期間において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、昨年より流行しているマルウェア Confickerの亜種の感染が、数多く報告されています。また、コンテンツ書き換えにより、Webを閲覧するだけで感染し、ID・パスワード等の情報を盗み出すマルウェアの流行がありました。

脆弱性の分野では、Adobe ReaderやApple QuickTimeなど、ブラウザのプラグインとして動作するソフトウェアの脆弱性が相次いで発見され、悪用事例も報告されています。

国際的には、中国で発生したDNSサーバに対する攻撃や、イランの大統領選挙に関連したDDoS攻撃など、多くの利用者に影響を与えるインシデントが発生しています。

IJの観測では、インターネット上のマルウェアの活動、DDoS攻撃、Webサーバに対するSQLインジェクション攻撃は、従来の規模で継続しています。

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、2009年4月から6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。

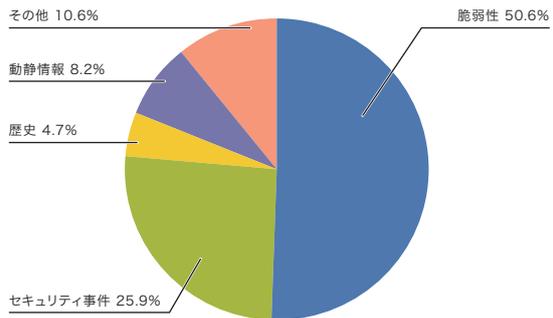


図-1 カテゴリ別比率(2009年4月～6月)

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、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

この期間では、ワードパッド及びOffice テキスト コンバーターの脆弱性*1、Microsoft Office PowerPointの脆弱性*2など、ユーザの利用するアプリケーションの脆弱性が発見されています。加えて、Adobe Acrobat及びAdobe Reader*3*4、Apple QuickTimeの複数の脆弱性*5等、Webブラウザから起動されるアプリケーションに関連する脆弱性が多く発見され、先に発見されていたFlash Playerの脆弱性*6などとともに悪用されました。また仮想化ソフトのVMwareにも複数の脆弱性*7が発見されています。

■動静情報

IJでは、国際情勢や時事に関連した各種動静情報に注意を払っています。この期間では、特に北朝鮮によるミサイル発射関連の動き、新型インフルエンザの世界的な発生、およびイランの大統領選挙等の、国際情勢や各種動静情報に注意を払いました。新型インフルエンザ関連では、国内での感染者発生に伴い、注意喚起を装ったマルウェアの添付されたメールが送られる事例*8が発生しました。

イランの大統領選挙に関しては、選挙結果における不

満からイラン国内に対してDDoS攻撃が発生したという情報がありました*9。また、5月及び6月の外国要人来日では警戒を行う等の対応を行いましたが、直接関連する攻撃は検出されませんでした。

■歴史

この時期には、過去に歴史的背景によるDDoS攻撃や、ホームページの改ざん事件などが発生していましたが、この期間においてはIJの設備及び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、まず、Confickerの亜種の感染拡大が観測されます。この件については「1.4.1 マルウェア Confickerの世界的流行」も併せてご参照ください。

また、改ざんされたWebコンテンツを参照することで感染し、ID・パスワード等を盗み出すマルウェア Gumblarについて、数多くの感染事例が報告されています。この件についても「1.4.2 ID・パスワード等を盗むマルウェア Gumblar」としてまとめていますので、併せてご参照ください。

*1 マイクロソフトセキュリティ情報MS09-010、ワードパッド及びOffice テキスト コンバーターの脆弱性 (<http://www.microsoft.com/japan/technet/security/bulletin/ms09-010.mspx>)。

*2 マイクロソフトセキュリティ情報MS09-017、Microsoft Office PowerPoint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/bulletin/ms09-017.mspx>)。

*3 2009年5月Adobeセキュリティ情報APSB09-06 (<http://www.adobe.com/jp/support/security/bulletins/apsb09-06.html>)。

*4 2009年6月Adobeセキュリティ情報APSB09-07 (<http://www.adobe.com/jp/support/security/bulletins/apsb09-07.html>)。

*5 QuickTime 7.6.2のセキュリティコンテンツについて (http://support.apple.com/kb/HT3591?viewlocale=ja_JP)。

*6 2009年2月Adobeセキュリティ情報APSB09-01 (<http://www.adobe.com/jp/support/security/bulletins/apsb09-01.html>)。

*7 ゲストOS上のユーザが、ホストOS上で任意のコードを実行する可能性がある等 (<http://www.vmware.com/security/advisories/VMSA-2009-0006.html>)。

*8 国立感染症研究所による注意喚起、「国立感染症研究所」を詐称したブタインフルエンザ関連メールにご注意ください (<http://www.nih.go.jp/niid/misc/warning090428.html>)。

*9 攻撃の様子については、例えば次のblog等に詳しい。Arbor network社のTHE ARBOR NETWORK SECURITY BLOG:iran DDoS Activity: Chatter, Tools and Traffic Rates (<http://asert.arbornetworks.com/2009/06/iran-ddos-activity-chatter-tools-and-traffic-rates/>)。

4月には、大きなサイズの応答を得るDNSクエリを大量に発生させることで、DNSキャッシュサーバに負荷を与える攻撃が複数観測されています*10。また、5月には、中国国内でDNSサーバに対するDDoS攻撃が発生し、数時間に渡って広範囲の障害を起こしています*11。加えて、いくつかのHTTPサーバに影響するDoS攻撃ツール*12が公開され、イランにおけるDDoS攻撃に悪用されたという情報がありました*13。

■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、Googleにかかわる経路情報の不具合により、世界的なトラフィック減があったことが注目されました*14。また、IP電話に無言電話が着信する可能性のあるSIPの通信を、断続的に観測しています。

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、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。

*10 このDNSキャッシュサーバへの攻撃については、例えば以下から始まるDNS OARCでの議論を参照のこと (<https://lists.dns-oarc.net/pipermail/dns-operations/2009-April/003779.html>)。

*11 本件については、例えば次の報道がある (<http://www.networkworld.com/news/2009/052109-dns-attack-downs-internet-in.html>)。

*12 この手法では、HTTPリクエストの一部分のみをサーバに送付し、リクエストを完成させないまま接続を保持することでWebサーバの負荷を上げる。技術詳細は作者自身による解説が最も詳しい (<http://ha.ckers.org/slowloris/>)。この問題の影響を受けるかどうかと、その対策方法は実装により異なるため、利用中のWebサーバの対策情報を参照のこと。

*13 例えば SANS ISC のHandler's Diary: Slowloris and Iranian DDoS attacks (<http://isc.sans.org/diary.html?storyid=6622>)。

*14 この事故による通信への影響については Arbor network社のTHE ARBOR NETWORK SECURITY BLOG: The Great GoogleLapse (<http://asert.arbornetworks.com/2009/05/the-great-googlelapse/>) に詳しい。Google向けのトラフィックがアジア(日本)に向かったとする情報もあるが、詳細は不明。IJではこの時間帯に経路情報やトラフィックの異常は観測していない。

ここで、2009年4月から6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、図-2に示します。

この情報は、IIJ 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。IIJでは、この他の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。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^{*15}、サーバに対する攻撃^{*16}、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カ月の期間中、IIJでは114件のDDoS攻撃に対

処しました。1日あたりでは1.25件程度となり、平均発生件数は前回のレポートの期間よりも減少しています。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86%、複合攻撃が13%です。最大規模のSYN floodで67,000pps程度であり、回線への攻撃の最大規模は125Mbps程度でした。この期間中、150,000pps以上のパケット数によるICMP floodが観測されていますが、個々のパケットが小さかったため、回線容量への影響は77Mbps程度となっています。また、攻撃の継続時間については、全体の83%が攻撃開始から30分未満で終了し、17%が30分以上24時間未満の範囲で分布しています。この期間中では、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^{*17}や、ポットネット^{*18}の利用によるものと考えられます。

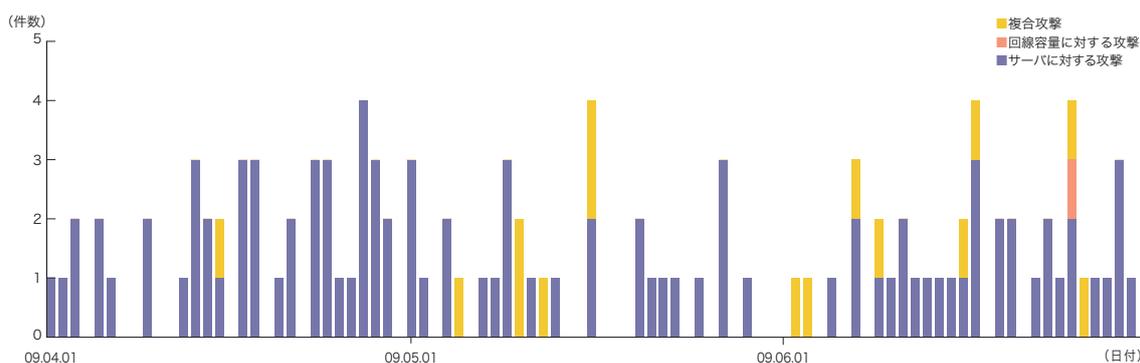


図-2 DDoS攻撃の発生件数

*15 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。

*16 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。

*17 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。

*18 ポットとは、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。ポットが多数集まって構成されたネットワークをポットネットと呼ぶ。

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*19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*20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、2009年4月から6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。ここではハニーポット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。

この期間では、マイクロソフトのOSで利用されている通信や、P2Pファイル共有ソフトウェアの6881/UDP、PCリモート管理ツール*21の4899/TCP、シマンテックのクライアントソフトウェアの2967/TCP等、クライアントに対する探索行為が数多く観測されています。一方で、10044/UDPのように、目的不明の通信も観測されています。また、445/TCPなどMS08-067*22で示される脆弱性を狙った攻撃が、昨年10月以来継続しています。

全体の発信元の分布を国別に見ると、中国の29.2%、日本国内の20.3%、が比較的多くなっています。

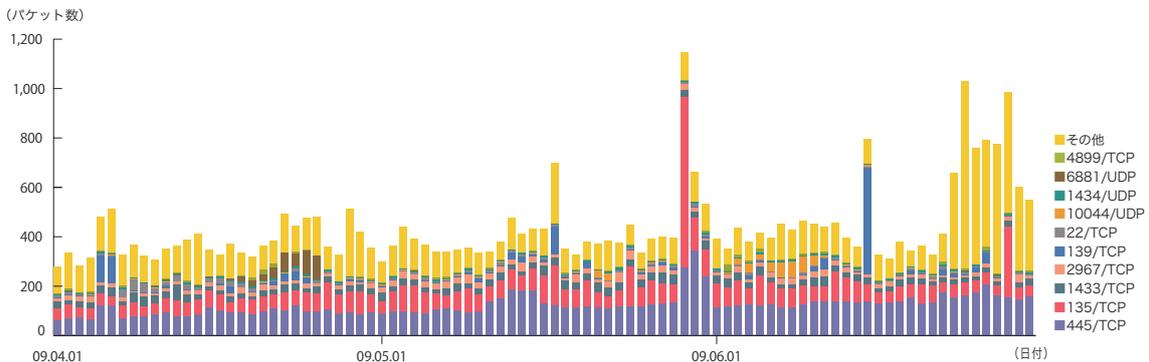


図-3 ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

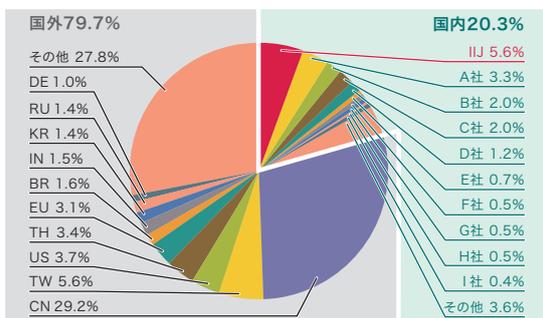


図-4 発信元の分布(全期間)

*19 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。

*20 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。

*21 同様の探索行為については、同時期に他の組織においても観測されている。例えば SANS ISC のHandler's Diary: TCP scanning increase for 4899 (<http://isc.sans.org/diary.html?storyid=6637>)。

*22 マイクロソフト セキュリティ情報 MS08-067、緊急:Server サービスの脆弱性により、リモートでコードが実行される (<http://www.microsoft.com/japan/technet/security/bulletin/ms08-067.msp>)。

■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^{*23}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^{*24}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708検体を、種類で60種類程度のマルウェアを取得しています。前回の集計期間では、一日平均の総取得検体数で899検体、種類では44種類でしたので、この期間中では、総取得検体数が減少傾向にあります。種類においては

その水準を維持しています。

検体取得元の分布では、日本国外が43.2%、国内が56.8%であり、全体のうちIJJのユーザ同士のマルウェア感染活動が16.8%となっています。これは、依然として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5%、ポット型59%、ダウンロード型36%となりました。また、この解析により、81個のポットネットC&Cサーバ^{*25}と、528個のマルウェア配布サイトの存在を確認しています。

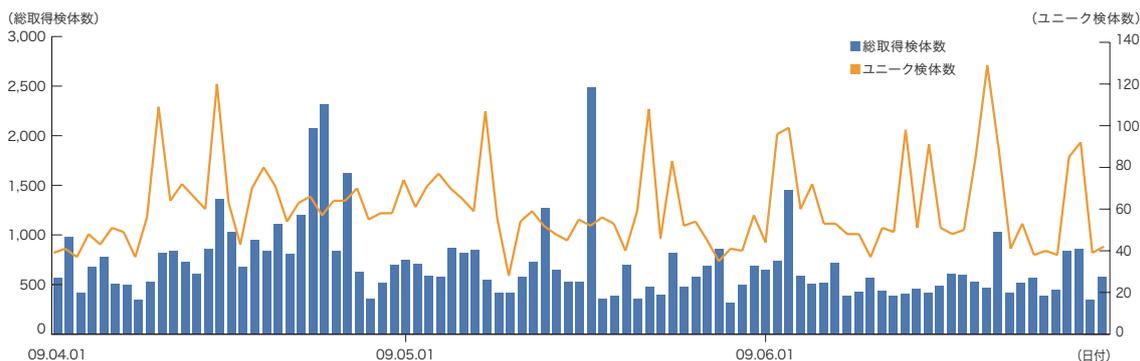


図-5 取得検体数の推移(総数・ユニーク検体数)

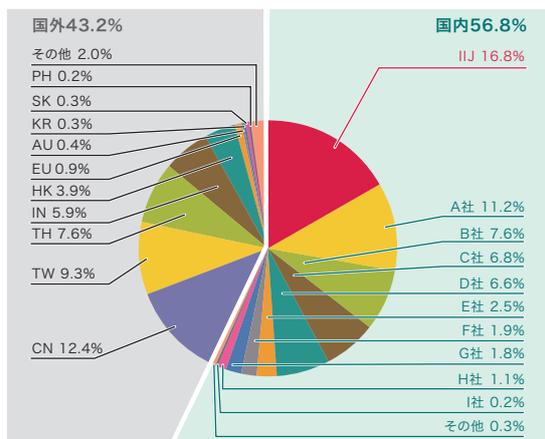


図-6 検体取得元の分布(全期間)

*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。多数のポットで構成されたポ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*26について継続的な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。

まず、2009年4月から6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に、攻撃の発信元の分布を図-8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。Webサーバに

対するSQLインジェクション攻撃の発生状況は、前回のレポートの水準を維持しています。4月3日に発生している大量の検出は、特定のWebサーバに対するもので、南米の多数のIPアドレスを送信元とした攻撃が、それぞれの送信元から同じ数だけ観測されており、ボットネットを利用した攻撃であることが窺えます。6月7日に発生した大量攻撃は、中国の特定のアドレスから特定のWebサーバに対するものでした。発信元の分布では、日本39.4%、中国34.4%、米国4.9%となり、以下その他の国が続いています。

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。

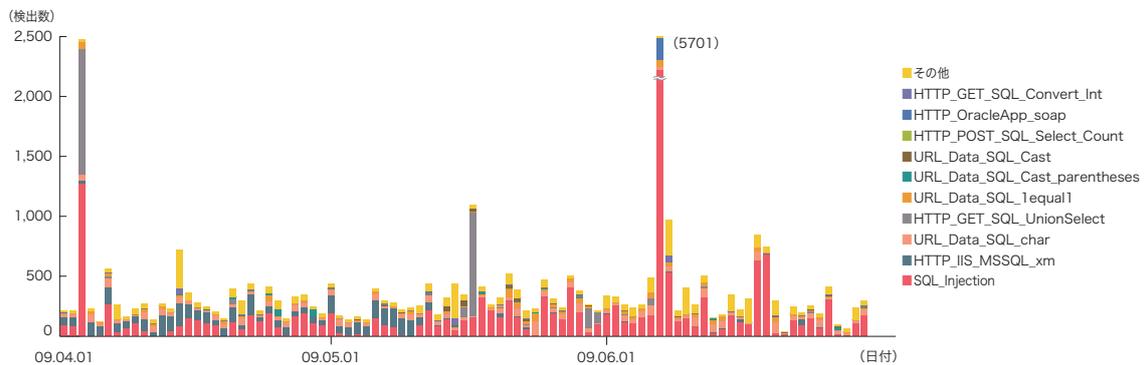


図-7 SQLインジェクション攻撃の推移(日別・攻撃種別)

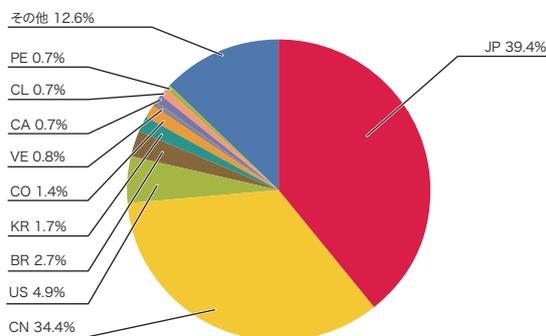


図-8 SQLインジェクション攻撃の発信元の分布

*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、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、マルウェア Confickerの世界的流行、ID・パスワード等を盗むマルウェア Gumblar、クラウドコンピューティングとセキュリティについて示します。

1.4.1 マルウェアConfickerの世界的流行

■Confickerとは

Confickerは2008年11月から流行しているマルウェアです。数々の亜種の登場により、現在でもその感染規模は拡大しており、5月に米国大統領談話^{*27}で言及されるなど、大きく注目されています。ここでは、このConfickerとその感染拡大についてまとめます。

■Confickerの亜種とその動作

本稿執筆時点で存在が確認されているConfickerの亜種と、その特徴について表-2に示します^{*28}。以下ではそれぞれの機能について紹介します。

■感染活動

Confickerはまず、MS08-067で示された脆弱性を利用して、ネットワーク経由の感染活動を行います。また、USBメモリ等で利用される自動実行の仕組みを悪用し、ファイアウォール等の、境界防御を設定したネットワークの内部に対する感染活動を行います。さらに、Windowsファイル共有で設定されている管理共有ADMIN\$の認証情報に対して辞書攻撃^{*29}を行い、成功した場合はファイル共有を通じて組織内ネットワーク上に伝播します。

■制御とアップデート

ConfickerはHTTPを利用してアップデートを行います。アップデートに利用されるWebサーバのURLのドメイン部は、時刻をもとにしてあるアルゴリズムで生成された、複数の文字列によって決定されます(1日あたり250から50,000種類)。感染PCを操ろうとする者は、このアルゴリズムによって、ある特定の日に感染PCがアクセスを試みるURLを事前に知ることができ、そのドメインを取得することで、制御を行います。

表-2 Confickerの亜種

名称	発見日	特徴
Conficker.A	2008/11/21	●MS08-067で示される脆弱性を利用して感染活動を行う。 ●1日あたり250 URLを生成してアクセスし、アップデートを試みる。
Conficker.B	2008/12/29	同上 ●USBメモリなどの自動実行機能を悪用して感染する。 ●Windowsのファイル共有を経由した感染を試みる。
Conficker.C(B++)	2009/2/20	同上 ●P2P通信を実装し、それを通じてアップデートを試みる。
Conficker.D(C)	2009/3/4	●同上だが、1日あたり50,000 URLを生成し、そのうち500 URLにアクセスを試みる。 ●また、P2P通信に変更が加えられた。
Conficker.E	2009/4/8	●同上だがネットワーク経由等の感染機能は持たない。 ●Conficker.CもしくはDから、P2P通信を利用してアップデートされた。 ●別のマルウェア(例えばWaledac やスケアウェア)をダウンロードする。 ●5月3日に自己削除を行う(5月3日に削除されていないという情報もある)。

*27 全文は次で参照できる。REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE (http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/)。

*28 この表は極力直接得た情報をもとに作成しているが、IJではすべての亜種の検体を取得しているわけではなく、不足している情報については(<http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline>)などの公開情報をもとにしている。ConfickerはDownadupと呼ばれることもあり、その亜種の呼び方についても、ウイルス対策ソフトベンダや、時期によって異なる場合がある。また、脆弱性とConficker.AについてはIIR Vol2「1.4.2 MS08-067を悪用するマルウェア」も合わせて参照のこと(http://www.ij.ad.jp/development/iir/pdf/iir_vol02.pdf)。

*29 辞書攻撃とは、あらかじめ用意した辞書(一般名詞や機械的に生成した文字列などで構成される辞書)の内容を、一つずつ試すことで、正当なパスワードを見つけ出す試み。

また、いくつかの亜種ではP2P通信によるアップデートの機能が搭載されています。この機能を持つConfickerが利用するP2P通信は、初期状態や中央サーバ等を必要としない純粋なP2P通信で、通信の一極集中が発生しないため、発見が困難となっています。実際に、Conficker.EはこのP2P通信により伝播したとされています。

■他のマルウェアの導入

Conficker.Eでは、感染したPCをWaledac^{*30}等のボットに感染させようと試みます。この試みが成功すれば、ボットネットの一部として悪用されてしまう可能性があります。

■流行の様子

Confickerは以上の機能を利用して感染を拡大しています。特に国内においては、USBメモリ経由の感染や、ファイル共有を悪用した手法で、企業等の組織内ネットワークにおいて大規模に感染活動を行いました。また、Conficker.Dが4月1日に大きく挙動を変えることが発

見され、広く注目^{*31}されましたが、IJでは当日、通信上の異常を確認できませんでした。図-9では、MITFにおけるConficker.Dの感染活動の観測回数の総数を示しています^{*32}。この図で示されるように、日本国内においてはほとんど感染活動は見られませんが、中国、ブラジル、ヨーロッパ、ロシア、米国の順で感染活動が多いことが分かります。Conficker Working Group^{*33}によると、本稿執筆時点で、すべての亜種の合計感染台数は500万台を越える^{*34}としています。

以上にまとめたように、Confickerは現在でも全世界で多数の感染が確認されており、数多くのPCが悪用される状態にあることを示しています。これは、インターネット全体にとって非常に大きな脅威であるといえるでしょう。このため、多くのセキュリティベンダや研究者たちによる、協調対策活動が行われています^{*35}。制御の仕組みの問題や対策活動の成果として、現時点では500万台ものPCが、一斉に操られるような事態にはいたっていませんが、予断を許さない状況が継続しています。

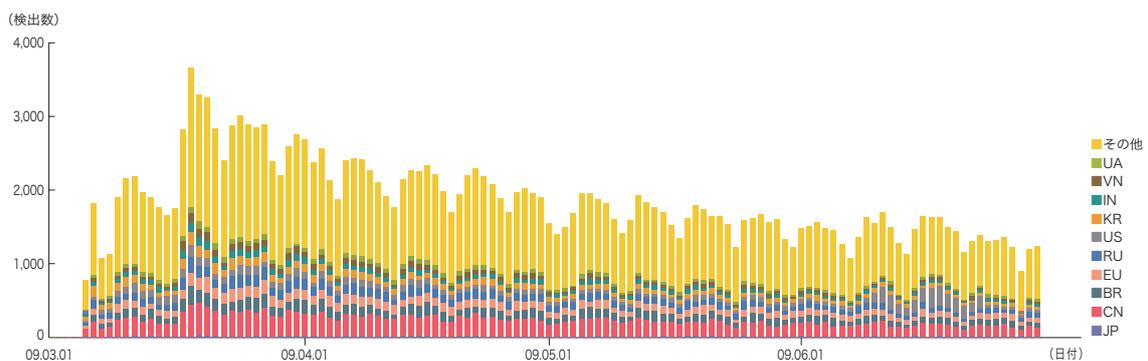


図-9 Conficker.DのP2Pポートへのアクセス(国別)

*30 Waledacはボットの種類であり、スパムメールを大量に送信することで知られている。ConfickerとWaledacの関係については、たとえば次の情報を参照のこと (<http://blog.trendmicro.com/downloadconficker-watch-new-variant-in-the-mix/>)。

*31 Confickerに関する、US-CERTのTechnical Advisory (<http://www.us-cert.gov/cas/techalerts/TA09-088A.html>)。

*32 Conficker.Dは攻撃先のIPアドレスと時刻をもとに算出されるポート(TCPもしくはUDP)でP2P通信を待ち受ける。この集計は、このP2Pポートへのアクセスがあった送信元を集計することで作成している (<http://nmap.org/nseodoc/scripts/p2p-conficker.html>)。この図の作成には、IJで実験的に運用するハニーボットでの観測情報も採用しているため、他の集計、例えば図-3とは母集団が異なり、単純に比較できないことに注意。また、日本の様子を見やすくするために、図中の一番下に表示しているが、実際の順位は第26位であった。

*33 Conficker Working Group とは、Confickerを撲滅するための活動で、セキュリティベンダを含む多くのITベンダや研究機関等が参加している。メンバー構成や活動の詳細については以下のURLを参照のこと (<http://www.confickerworkinggroup.org/wiki/>)。

*34 Conficker Working Groupによる感染端末の推移 (<http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking>)。

*35 たとえば、Confickerがアップデートに使うURLは、日付をもとにしてあるアルゴリズムで生成されるため、対策を実施する側でも特定の日にConfickerがアクセスを試みるURLを知ることができる。このような知識を利用して、Confickerの動作に先行した監視や対応を行っている。

1.4.2 ID・パスワード等を盗むマルウェア Gumblar

4月から5月にかけて、あらかじめ盗まれたFTPアカウントを悪用した、Webサイトのコンテンツ改ざん事件が相次ぎました。この改ざんされたコンテンツは、第三者がアクセスしただけでマルウェア感染を引き起こします。さらに、感染したマルウェアによって、個人情報やID・パスワード等の情報が盗まれるという事態に発展しています^{*36}。

■ 今回の事件の流れ

はじめに、今回の事件の流れを図-10に示します。以下、本説明中の数字は図-10内の数字に相当します。

■ コンテンツ改ざんからマルウェア感染まで

まず、攻撃者はあらかじめ盗んだFTPアカウントを悪用し、Webコンテンツを改ざんします(1)。第三者が改ざんされたWebコンテンツにアクセスした場合(2)、

改ざんによって挿入されたJavaScript等により、自動的に悪意のあるWebサイトへ誘導されます(3)。このスクリプトにより、Adobe ReaderやFlash Playerの脆弱性を悪用する、攻撃用のファイルがダウンロードされます。利用者のPCにこれらの脆弱性が存在する場合、ファイル内の攻撃コードが実行され、マルウェアAがダウンロードされます(4)。

■ マルウェアの動作

マルウェアAは実行されると、マルウェアBを生成(Drop)し、レジストリに登録した上で、自分自身を削除します(5)。マルウェアBは実行されると、いくつかのAPIをフックし、HTTPやFTP等の通信を盗聴します。また、感染を発見されにくくするために、cmd.exeやregedit.exeを起動できなくします。さらに、別のマルウェア配布サイトにアクセスし、新しいマルウェアをダウンロードして実行する場合があります(6)。

1. 事前に盗み出したID・パスワードを用い、FTPでコンテンツを改ざんする(スクリプトの挿入)。
2. あるユーザが改ざんされたサイトにアクセスすることで、Webブラウザ上でスクリプトが動作する。
3. ユーザの操作なしに、自動的にマルウェア配布サイトAに誘導される。
4. Adobe Reader や Flash Playerの脆弱性を悪用してマルウェアAをダウンロードし、実行する。
5. マルウェアAはマルウェアBをドロップし、レジストリに登録後、マルウェアA自身を削除する。
6. マルウェアBは新たなマルウェアをダウンロード、実行したり、FTP通信等を盗聴し、アカウント情報等を特定のサーバにアップロードして盗み出す。
7. マルウェアBはさらに、他のマルウェアのダウンロード、活動痕跡の削除、PC内のファイル消去等の破壊を行う場合もある。
8. 盗まれたFTPアカウントは再びコンテンツ改ざんに利用される。
9. 盗まれた情報は、商品購入やオークションの詐欺行為などで悪用される場合もある。

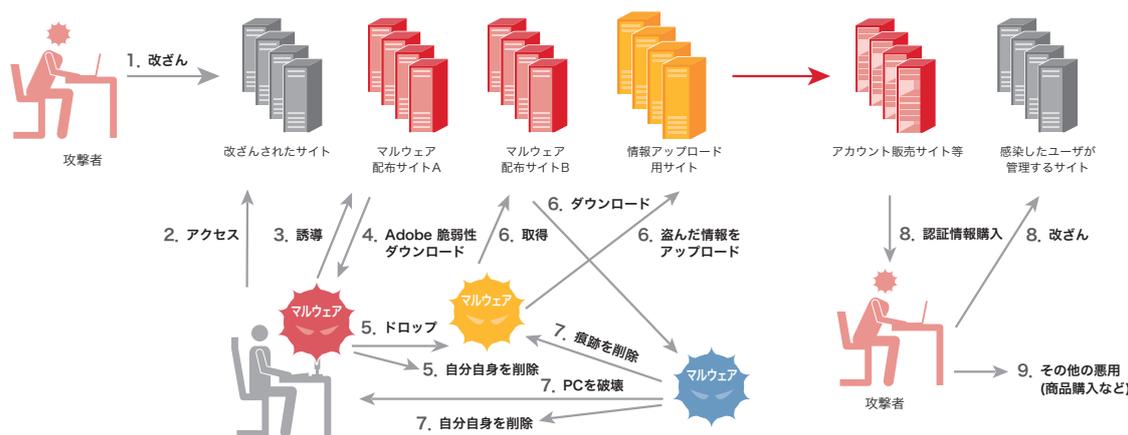


図-10 攻撃の全体像

^{*36} US-CERT Current Activity:Gumblar Malware Exploit Circulating (http://www.us-cert.gov/current/archive/2009/05/18/archive.html#gumblar_malware_attack_circulating).

Gumblarとはマルウェア配布Webサイトのドメイン名の一部で、実際には gumblar.cnにアクセスすると感染が発生していた。同様なWebサイトに zikon.lv, martuz.cnなどがあった。この事件は複雑で全体を示す適切な名前がなく、本稿では関係するWebサイトやマルウェア等、全体を示す名前としてGumblarと呼んでいる。

■情報のアップロードから悪用まで

マルウェアB、もしくは更新された新しいマルウェアは、通信の盗聴や設定ファイル等から盗み出した情報を、外部のサーバにアップロードします(6)。この情報には、個人情報や実際の通信に利用したID・パスワード等の情報が含まれます。また、活動の痕跡となるファイルを削除したり、PC上のOSやデータを破壊したりします(7)。このようにして盗み出された情報は、再びコンテンツ改ざんに悪用され、新たにマルウェア感染に誘導するWebサイトが増えていきます(8)。そして、情報を盗むこととその悪用を、循環的に繰り返すことで拡大し、最終的に多くの利用者が被害を受けていると考えられています。加えて、盗み出した情報は、他人に成りすますために悪用されたり、商品購入等で直接の金銭被害を引き起こしたりしています(9)^{*37}。

■Gumblarの特徴

まずGumblarでは、個人のブログ等、比較的参照する人の少ない小規模なサイトに対して改ざん行為が行われていたため、発見が遅れていました。今回の件が大きな事件として取り上げられるようになったのは、ある企業のオンラインショップのコンテンツが改ざんされ、多くの被害が出たことによります。

また、Gumblarには複数のWebサイトや脆弱性、マルウェアが関係していることも特徴として挙げられます。特に悪用されたマルウェアが、シーケンシャルマルウェア^{*38}であったことで、発見や解析、対策が困難となっていました。

加えて、マルウェアにより盗み出された情報が、ある程度時間が経過してから悪用されていることも挙げられます。このため、ユーザが改ざんに気づいた時点でウイ

ルス対策ソフトによる検査を行っても、マルウェア自身や痕跡が削除されており、PC上からは異常が発見されにくいケースが目立ちました。

Gumblarについては、現時点で関係した複数のマルウェア配布サイトが停止され、関係するマルウェアもウイルス対策ソフトで検出可能となっているため、すでに過去の事件として考えられています。しかし、一旦感染したユーザの情報は盗まれたままであることを忘れてはいけません。新たなマルウェア配布サーバを用意するだけで、今回と同様の循環を構築することができ、実際に現在でも他のWebサイトやマルウェアを利用した、同様の事件が継続的に起こり続けています^{*39}。

■利用者における注意点

この問題に対して、利用者として注意すべき事項は、利用しているPCにインストールされているソフトウェアの脆弱性情報に注意し、常に最新版を利用するように心がけることです。自動更新機能を持っていないソフトウェアや、特にブラウザのプラグインとして提供されているソフトウェア(今回の事例で悪用されたようなAdobe ReaderやFlash Player)は、今後も悪用の対象となる可能性があるため、注意が必要です。もし自分が感染したことに気付いた場合には、その端末上で入力したことのあるすべてのIDとパスワードを変更する必要があります。また、日ごろからIDとパスワードの管理を適切に行うことも重要となってきます^{*40}。

1.4.3 クラウドコンピューティングとセキュリティ

ここでは、最近話題となっているクラウドコンピューティング(以下クラウド)の紹介とともに、その利用の観点から、セキュリティに関する考察を示します。

*37 以上のマルウェアの動作は、IJで入手した検体を解析したうえで再現したもので、マルウェアAやマルウェアBとして、他の多くのマルウェアが介在することを示す情報もあり、必ずしも毎回この通りであるとは限らない。

*38 シーケンシャルマルウェアとは、マルウェアを機能ごとに分割し、必要時に個別にダウンロードし、実行していく仕組み。ウイルス対策ソフトをすり抜けるための手段として使われる。本事件では、リダイレクタ(javascriptマルウェア)、ダウンロード(PDFマルウェア、マルウェアB)、ドロップ(マルウェアA)、アカウント盗用マルウェア(マルウェアB)などが利用されており、全体で1つのシーケンシャルマルウェアを構成していると考えられる。

*39 たとえばNine-Ball等。以下は改ざんの様子を示すcNotes(<http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=molo.tw>)。

*40 パスワード管理手法の関連資料については本レポートのvol.3において紹介している(http://www.ijj.ad.jp/development/iir/pdf/iir_vol03.pdf)。その他の立場での対策については、独立行政法人情報処理推進機構による今月の呼びかけ「あなたのウェブサイト、改ざんされていませんか?」(<http://www.ipa.go.jp/security/txt/2009/07outline.html>)等も参考になる。

■クラウドコンピューティングとは

現時点で多くの団体^{*41}がクラウドの定義や標準化の議論を行っていますが、例えば、Open Cloud Manifestoでは、クラウドの主な特徴として「必要に応じた処理能力を低コストで確保でき、その能力を手軽に利用できること」としています^{*42}。具体的にはAmazon、Google、Microsoftといった例が挙げられます。Amazonは計算環境を提供するEC2^{*43}や、ストレージサービスのS3^{*44}といった、利用者が自由に組み合わせて、構築、運用できる仕組みを提供しています^{*45}。また、GoogleはGmailに代表されるアプリケーションサービスを主に提供しています^{*46}。マイクロソフトはWindows Live Mail (Hotmail)や、Windows Update等のサービスを、クラウドの技術を基に提供しています。また、Windows Azureというクラウドプラットフォームサービスを提供することを発表しました^{*47}。このように、同じクラウドと呼ばれるサービスでも、コンピュータ資源の提供、プラットフォームの提供、アプリケーションの提供といった違いがあります。この違いをXaaS (X as a Service) と表記します。Googleのように、ソフトウェア (Software) をサービスとして提供する場合は、SaaS (Software as a Service) と呼び、ハードウェア (Hardware)、インフラストラクチャ (Infrastructure)、プラットフォーム (Platform) を提供するサービスは、それぞれ、HaaS、IaaS、PaaSと表記します。XaaS間の相互の関係を図-11に示します。

また、クラウドはパブリッククラウドと、プライベートクラウドに分類されます。パブリッククラウドとは、主にインターネット上で提供されている環境で、不特定多数の利用者が資源を共有します。一方、プライベートクラウドは、クラウド技術を使い、不特定多数向けではない限定的な用途に利用するクラウドです。

以上のように、クラウドは資源やサービスの提供形態を示しています。一方で、このクラウドと呼ばれる環境を実現するためには、ユーティリティコンピューティング、SOA、Web2.0、仮想化、そして従来よりも低価格で手に入る潤沢な資源^{*48}、といった要素の積み重ねが必要であり、これをクラウドの技術的要素と考えることができます。クラウドは表面的には利用方法の変化に見えますが、膨大な資源をまとめることによる複雑さの増加や、管理に用いる情報量の爆発的な増加といった、技術的に考慮すべき側面を含んでいるのです。

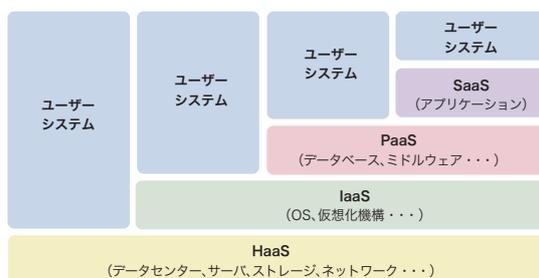


図-11 XaaSの関連図

*41 クラウドに関する標準化などを推進している代表的な団体は以下の通り。Open Cloud Manifesto (<http://www.opencloudmanifesto.org/>)、Open Cloud Consortium (<http://www.opencloudconsortium.org/>)、Cloud Security Alliance (<http://www.cloudsecurityalliance.org/>)、Open Cloud Standards Incubator (<http://www.dmtf.org/about/cloud-incubator>)。

*42 原文はopen cloud manifesto (<http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf>)。ただし、この文章はクラウドの定義ではなく、定義などの議論を行うための整理であるとしている。

*43 Amazon EC2はElastic Compute Cloudの略で、インターネット上でCPU資源を提供するサービス (<http://aws.amazon.com/ec2/>)。

*44 Amazon S3はSimple Storage Serviceの略で、EC2で利用するディスクを提供するサービス (<http://aws.amazon.com/s3/>)。

*45 導入事例としてはNASDAQのMarket ReplayやThe New York TimesのTimesMachine等がある。Market Replayは過去の市場動向分析が可能なアプリケーションで、データの保存にS3を利用している (<http://aws.amazon.com/about-aws/media-coverage/2008/07/18/nasdaq-use-of-amazon-s3>)。The New York Timesでは過去の新聞のアーカイブ化にEC2を利用し非常に短期間で紙面のPDF化作業を終えた (<http://open.blogs.nytimes.com/2007/11/01/self-service-prorated-super-computing-fun/>)。

*46 メールサービスで有名なGmailをはじめ、スケジュール管理を行うGoogleカレンダー、OfficeツールのGoogleドキュメント等が用意されている (<http://www.google.com/apps/intl/ja/business/index.html>)。

*47 Windows Azureでは、計算環境やストレージ環境、またはWindows Live等のサービスを自由に組み合わせてシステムを構築する事ができる (<http://www.microsoft.com/azure/whatisazure.msp>)。

*48 CPUのメニーコア化、通信路の帯域、メモリ、ディスク等の記憶装置の容量等。

■クラウド上のセキュリティ問題

ここで、クラウドで利用される、従来とは異なる技術要素を検討した上で、配慮すべき点をいくつか紹介します。

■境界に関する問題

仮想化技術そのものの脆弱性によって、論理的に分離されている資源の境界を越えて、データへの不正なアクセスが発生する等、脆弱性による影響が従来環境よりも拡大する可能性があります。また、クラウド自体にどのような境界を設定するかが、新たな検討課題となります。パブリッククラウドとプライベートクラウドは、安易に相互接続してはいけません。パブリック側からの不正アクセスを想定するだけでなく、クラウドへの侵入に成功したとき入手できる膨大な資源を、踏み台として悪用されないようにする必要があります。

■APIにかかわる問題

クラウドの制御には、基本的にAPIを利用しますので、そのAPIに脆弱性が発見された場合の影響について、検討が必要です。その影響は、クラウド上の個別のサービスの不正利用だけでなく、クラウド自体への不正な操作(停止も含む)等、従来環境よりも多岐にわたります。APIにアクセスを行うための認証情報を奪われた場合や、クラウド管理用端末に侵入された場合等への対策は、従来のセキュリティ対策課題と同様ですが、クラウドにおいては、その影響が増大すると考えられます。

■デジタルフォレンジック

デジタルフォレンジック*49をどのように行うのかも、大きな問題となります。クラウドでは物理的な実体と、論理的な実体が乖離する機会が多いため、通信の監視

やハードディスクのイメージ調査、ログの調査等が非常に困難となります。また、クラウドの構成要素の状態を示す、より多くの管理情報の取得と記録が必要となります。

■クラウドを安全に利用するために

クラウドを利用するという事は、様々なデータの管理や処理をクラウドに任せることであり、例えば、クラウドにあるデータのCIA(機密性、完全性、可用性)を、利用者の立場で適切に制御できるかが懸念されます。これは、従来型のアウトソースを利用しても発生する懸念であり、局面によって適切にクラウドを使い分け、契約や運用上のルールで対応することで、従来と同様の対策を考えることができます(図-12)。

但し、先に技術的要素として紹介したように、従来型のアウトソースとクラウドには、仮想化技術によるシステムの複雑さの増加と、資源の管理情報の大容量化の点で違いがあります。逆に言えば、この2点に対処することができれば、クラウドを利用する際に、従来と同程度のセキュリティを求めることができます。前者の課題に対しては、例えば筆者らは、図-13のようなモデルを使って、クラウド上で構成されるシステムのOSや、アプリケーションの依存性、システムの分離分割方法や、アクセス制御構造の把握を行うための研究を行っ

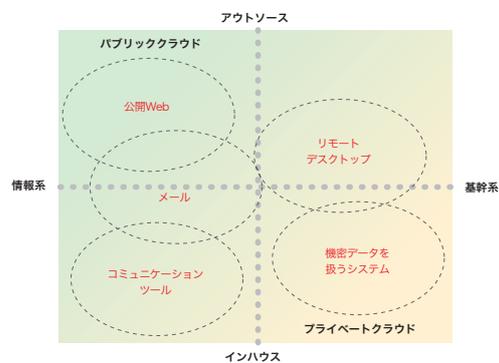


図-12 システムの利用用途によるサービスの使い分け

*49 特定非営利活動法人デジタル・フォレンジック研究会による定義では「インシデント・レスポンスや法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術をいう」としている(<http://www.digitalforensic.jp/wdfitm/wdf.html>)。

1.5 おわりに

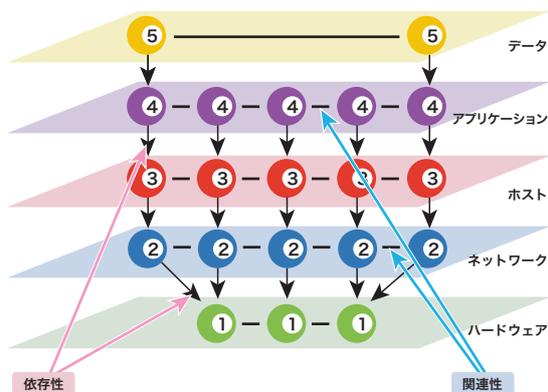
ています*50。後者の課題に対しては、システムをデータモデル化し、コンピュータによる自動管理を推進することが重要です。膨大で複雑な構造をもったクラウド環境をモデル化することで、異常時の影響範囲を自動的に把握し*51、制御するといったことも可能となります。

本稿では、クラウドのセキュリティに関する様々な懸念を述べてきました。情報システムの集約化、効率化の流れから、今後必然的にクラウドを利用する機会は増えていきます。ここで示したように、クラウドの仕組みや構造を理解した上で、従来の環境とクラウドの使い分けの検討を行えば、安全性を確保しながらクラウドならではの利点を享受することが可能となります。

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。このVol.4では、今現実には発生している大きな脅威2つについて解説するとともに、クラウドコンピューティングにおけるセキュリティ対策について考察しました。

実際に被害が発生している今日のインシデントに対応していくだけではなく、時々刻々と変化する技術動向を適切に把握し、将来におけるインシデントの予測とその対策を検討することにより、備えを行うことが重要です。

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、安全かつ安心して利用できるように、努力を継続してまいります。



番号付きの球は管理対象となる資源を示す。それぞれの資源は属性(装置、OS、アプリケーション名等)を持つ。各レイヤで資源を繋いでいる線は、そのレイヤ内での資源の関連性(アプリケーション間の通信など)を示す。レイヤ間の線は、資源の依存関係を表す。クラウド内の管理対象をこのようにモデル表現することで、たとえばハードウェアの一部が故障したときの影響範囲を把握することができる。

図-13 クラウド上のシステムの論理表現モデル例

執筆者:

齋藤 衛(さいとう まもる)

IJ 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等、複数の団体の運営委員を務める。

土屋 博英(1.2 インシデントサマリ) 永尾 禎啓、須賀 祐治、大原 重樹、鈴木 博志(1.3 インシデントサーベイ)

鈴木 博志、梅澤 威志(1.4.1 マルウェアConfickerの世界的流行) 鈴木 博志(1.4.2 ID・パスワード等を盗むマルウェア Gumblar)

加藤 雅彦(1.4.3 クラウドコンピューティングとセキュリティ)

IJ サービス事業統括本部 セキュリティ情報統括部

協力:

桃井 康成 IJ ネットワークサービス本部 セキュリティサービス部 サービス推進課

大津 繁樹、牧野 泰光 IJ サービス事業統括本部 システム基盤統括部

堂前 清隆 IJ サービス事業統括本部 データセンター事業統括部 事業企画課

*50 金岡晃、藤堂伸勝、加藤雅彦、岡本栄司:「ネットワークシステムの安全性定量化に向けた新たな表現モデルとアクセス制御解析」 暗号と情報セキュリティシンポジウム2008(SCIS2008)、(2008)

*51 加藤雅彦、金岡晃、藤堂伸勝、岡本栄司:「ネットワークシステムにおける脆弱性影響度の定量化と可視化」 コンピュータセキュリティシンポジウム2008(CSS2008) 論文集、pp.551-556、(2008)