1 インフラストラクチャセキュリティ

1.1 はじめに

このレポートは、IIJ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、IIJ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.3では、2009年1月より3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の亜種の感染事例が多く報告されています。また、パスワード盗用によるコンテンツ書き換え事件が発生しました。

脆弱性の分野では、OpenSSLの脆弱性や、透過型プロキシサーバに関する問題等、影響範囲の広い問題が指摘されています。

IIJの観測では、インターネット上のマルウェアの検体の取得総量は減少しています。またDDoS攻撃においては、その攻撃件数は減少していますが、依然としてサーバに直接影響を与える規模の攻撃が発生しています。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1月から3月の期間にIIJ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。

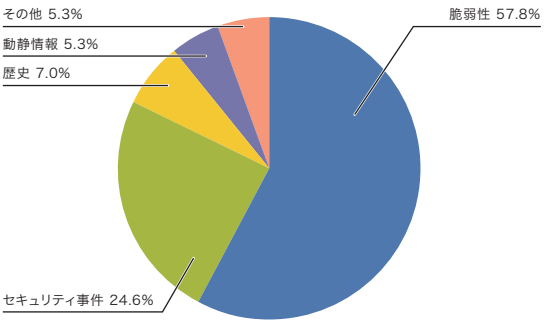


図-1　カテゴリ別比率（2009年1月～3月）

表-1　インシデントの分類

カテゴリ名	内容
脆弱性	インターネットで利用している、またはユーザの環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェア等の脆弱性への対応を示します。脆弱性そのものや、脆弱性に対する攻撃の情報、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

この期間においても、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に関連する脆弱性が多く発見されました。また、MD5の脆弱性を悪用したCAのなりすまし[*1]、OpenSSLの脆弱性[*2]、インテルTXTのセキュリティ構造に対する脆弱性の指摘[*3]、透過型プロキシサーバのHostヘッダ解釈の問題[*4]、Return Oriented Programming[*5]を利用したCisco IOSの攻撃方法[*6]等、特定の実装やバージョンに依存しない攻撃方法に関する発見や指摘が多く行われています。

■動静情報

この期間中には、野球のWorld Baseball Classic 2009等、複数の国際的なイベントが開催されていますが、IIJの設備及びIIJのお客様のネットワーク上では関連する攻撃は見られませんでした。また、日本国内の動きとして、この期間中の北方領土の日(2月7日)、竹島の日(2月22日)には各種の動静情報に注意を払いました。加えて、3月後半より北朝鮮によるミサイル発射関連の動きにも注目しましたが、同様にIIJの設備及び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。

■歴史

この期間には、過去に歴史的背景による日本国内複数のサイトに対するDDoS攻撃を検知した日が含まれていましたが、本年の同期間においてはIIJの設備及びIIJ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。

■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、マイクロソフトセキュリティ情報MS08-067を悪用したマルウェアConficker の亜種[*7]の感染拡大が観測されています。これらの亜種では、MS08-067の脆弱性を利用したネットワーク経由の感染だけではなく、USBメモリ等、他の媒体を経由した感染も行い、直接インターネットに接続していないPCでの被害が報告されています。これに関連して、Windowsの自動実行機能の無効化に関する議論[*8]が活発に行われました。

また、利用者のアカウント情報(ID・パスワード)の盗用によるコンテンツ書き換え[*9]が拡大しています。この件については、「1.4.2 ID・パスワード管理に関する注意喚起」を併せてご覧ください。

＊1　この手法を利用した攻撃により中間CA証明書を偽造できる。ただし、約8,000台のPCによる1 ～ 2日間の計算が必要とされている(http://www.win.tue.nl/hashclash/rogue-ca/)。

＊2　OpenSSLにおいて、一部の証明書の正当性検査に問題があり、偽の証明書を本物と判定する可能性がある(http://www.openssl.org/news/secadv_20090107.txt)。

＊3　インテルTXTのセキュリティ保護機能を迂回することのできる欠陥と、関連する実装エラーを発見したという発表(http://theinvisiblethings.blogspot.com/2009/02/attacking-intel-txt-paper-and-slides.html)。

＊4　WebブラウザとWebサーバの間に透過型プロキシが存在する場合、Webの動的コンテンツを悪用してHostヘッダに細工をすることにより、Java等の通信の宛先制限を迂回できる場合がある(http://www.kb.cert.org/vuls/id/435052)。

＊5　Return Oriented Programmingについての発表資料(http://www.blackhat.com/presentations/bh-usa-08/Shacham/BH_US_08_Shacham_Return_Oriented_Programming.pdf)。

＊6　この手法では、CiscoのROMMONのコードを利用した攻撃コードをReturn Oriented Programmingによって作成することで、汎用性の高い攻撃コードを生成できるとしている。リモートから攻撃可能な脆弱性が発見された場合に、この手法と組み合わせることで脅威となりうる(http://www.phenoelit-us.org/stuff/FX_Phenoelit_25c3_Cisco_IOS.pdf)。

＊7　ConfickerまたはDownadupと呼ばれるマルウェアの亜種に関しては、例えば次の情報がある。日本のセキュリティチームのブログ「Conficker(Downadup)ワームに関するまとめ」(http://blogs.technet.com/jpsecurity/archive/2009/01/24/3191000.aspx)。

＊8　自動実行機能を無効化することでUSBメモリ経由のマルウェア感染を防ごうとする試みについて。Technical Cyber SecurityAlert TA09-020A(http://www.us-cert.gov/cas/techalerts/TA09-020A.html)、マイクロソフト(http://support.microsoft.com/kb/967715)。

＊9　例えば、「SQLとかRFIを使わないWeb改竄(http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=SQL%A4%C8%A4%ABRFI%A4%F2%BB%C8%A4%EF%A4%CA%A4%A4Web%B2%FE%E3%E2)」等。

加えて、利用者の意図しない動作を誘発する手法として、昨年話題になったクリックジャッキングについて、注意喚起*10が行われました。その他、新年やバレンタインデー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ました。

■その他

直接セキュリティと関係しないインシデントとしては、Seagate社のHDDに関する不具合*11が、可用性の観点から注目されました。また、ネットワーク運用上では、BGPによる経路交換において、非常に長いAS Path属性値を持つ経路情報の流通*12により、いくつかのBGP実装が影響を受けました。これらのBGP実装を利用していたネットワークで、通信断や通信が不安定になる等の事象が発生しましたが、IIJの直接運用するネットワークにおいては影響ありませんでした。

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、日常的に発生しています。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ます。

＊10 JPCERT/CCによる技術メモ「クリックジャッキング対策(http://www.jpcert.or.jp/ed/2009/ed090001.pdf)」。
＊11 この件についてはSeagate社の発表を参照のこと(http://seagate.custkb.com/seagate/crm/selfservice/search.jsp?DocId=207931)。
＊12 例えば、NANOGにおける議論(http://www.merit.edu/mail.archives/nanog/msg15468.html)を参照のこと。

ここで、2009年1月から3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*13、サーバに対する攻撃*14、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ヵ月の期間中、IIJでは197件のDDoS攻撃に対処しました。1日あたりでは2件程度となり、平均発生件数は前回のレポートの期間(2008年9月〜12月)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0%、サーバに対する攻撃が94%、複合攻撃が6%です。サーバに対する攻撃は、例えば最大規模のSYN floodで90,000pps程度であり、攻撃対象に深刻な影響を与える規模になりますが、複合攻撃等の回線への攻撃の最大規模は108Mbps程度でした。回線に対する攻撃の頻度や規模が小さくなっている理由として、この種の攻撃では攻撃者側の回線にも、同時に負荷が掛かることが考えられます。

また、攻撃の継続時間については、全体の74%が攻撃開始から30分未満で終了し、26%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、ほとんどのケースで、国内、国外を問わず、非常に多くのIPアドレスが観測されています。これは、IPスプーフィング*15の利用や、DDoS攻撃を行うための手法としてのボットネット*16の利用によるものと考えられます。

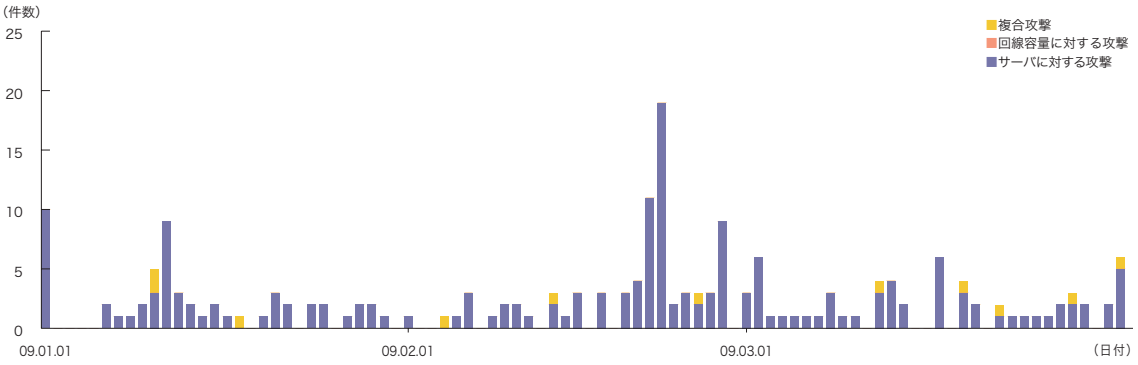


図-2　DDoS攻撃の発生件数

＊13 攻撃対象に対し、本来必要のない大きなサイズの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。

＊14 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消費させる。TCP Connection flood攻撃は、実際に大量のTCP接続を確立させる。HTTP GET flood攻撃は、Webサーバに対しTCP接続を確立したのち、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浪費させる。

＊15 発信元IPアドレスの詐称。他人からの攻撃に見せかけたり、多人数からの攻撃に見せかけたりするために、攻撃パケットの送出時に、攻撃者が実際に利用しているIPアドレス以外のアドレスを付与した攻撃パケットを作成、発信すること。

＊16 ボットとは、感染後に外部の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*17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*18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試みであると考えられます。

■無作為通信の状況

まず、2009年1月から3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。

MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均をとり、到着したパケットの種類(上位10種類)について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した。また、この期間においては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に対する探索行為も観測されています。

一方で、11075/UDPや20689/UDP等、一般的なアプリケーションで利用されない目的不明の通信も観測されました。また、445/TCP等MS08-067の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、日本国内の36.1%、中国の23%が比較的多くなっています。

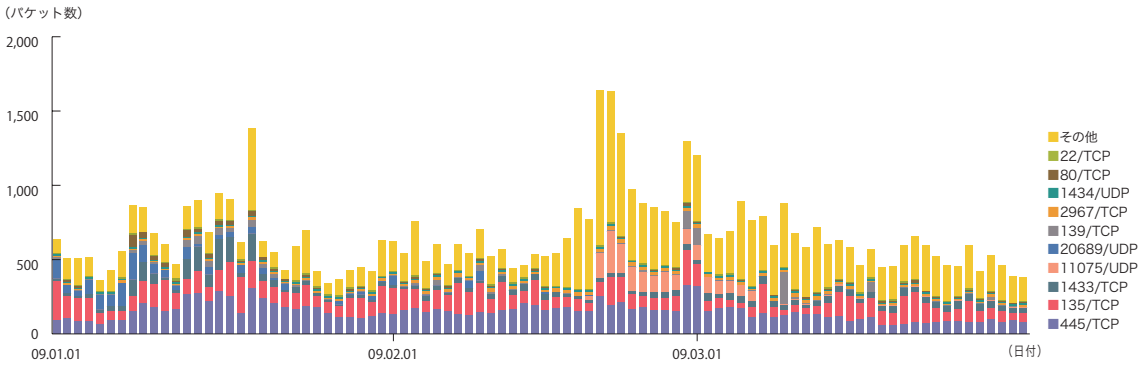


図-3　ハニーポットに到着した通信の推移(日別・宛先ポート別・一台あたり)

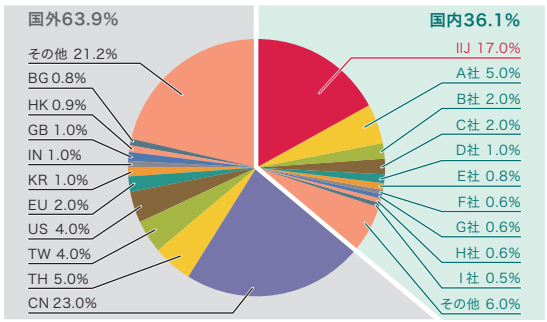


図-4　発信元の分布(全期間)

＊17 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。

＊18 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

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[*19]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[*20]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899検体、種類では44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2,235検体、種類では55種類でしたので、この期間中では、総取得検体数は大幅な減少傾向にありますが、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、日本国内が70.1％、国外が29.9%であり、全体のうちIIJのユーザ同士のマルウェア感染活動が33.0%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14%、ボット型45%、ダウンローダ型41%となりました。また、この解析により、86個のボットネットC&Cサーバ[*21]と540個のマルウェア配布サイトの存在を確認しています。

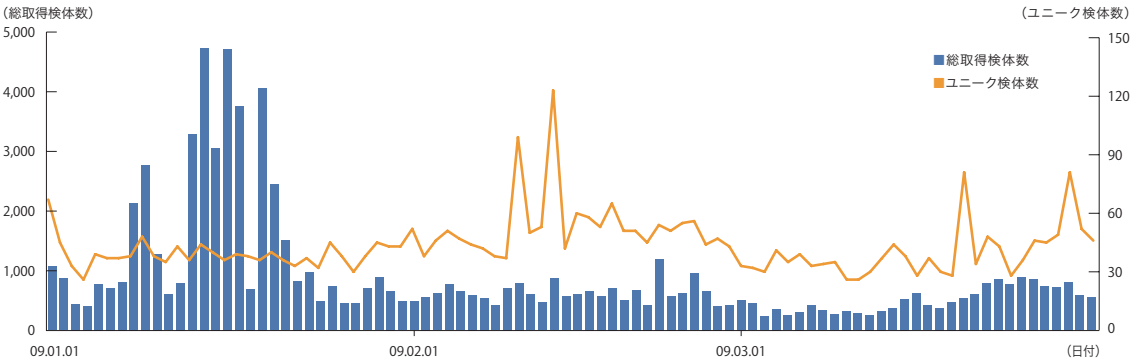


図-5　取得検体数の推移（総数、ユニーク検体数）

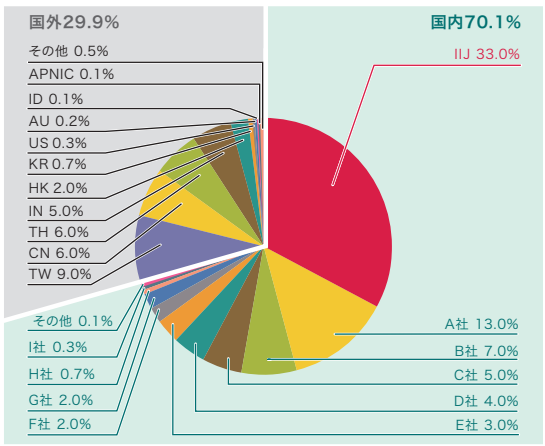


図-6　検体取得元の分布（全期間）

＊19 ここでは、ハニーポット等で取得したマルウェアを指す。

＊20 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。

＊21 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*22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。この攻撃は、データを盗むための試み、コンテンツの削除や書き換えへの試み、サーバへの侵入の試みの3つがあることが分かっています。

まず、2009年1月から3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、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についてまとめたものです。ただし、昨年末より継続している大規模攻撃については除外しています。発信元の分布では、日本38.5%、韓国20.3%、米国8.3%で、以下その他の国が続いています。また、前回のレポートでも示したように、12月末より少数特定のWebサーバに対する大規模なSQLインジェクション攻撃が発生しましたが、この攻撃は2009年に入ってから急激に減少し、1月の最初の1週間でほぼ沈静化しました。

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。

SQLインジェクション攻撃については「1.4.1 SQLインジェクション攻撃とその影響」も併せてご覧ください。

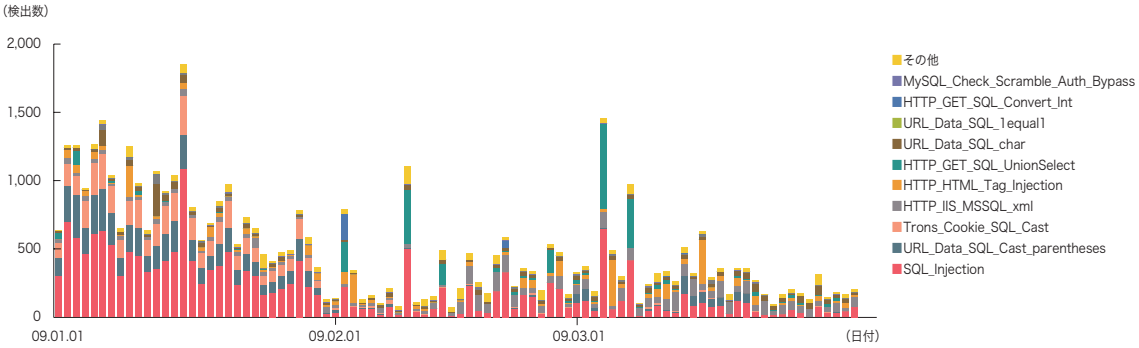


図-7　SQLインジェクション攻撃の推移(日別，攻撃種類別，大規模攻撃を除く)

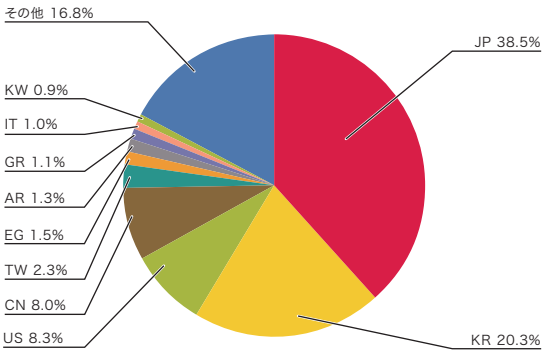


図-8　SQLインジェクション攻撃の発信元の分布

*22 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、その背後に接続された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、改ざんしたり、システム命令を発行することにより，機密情報の入手やWebコンテンツの書き換え、侵入等を行う。

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、SQLインジェクション攻撃とその影響、ID・パスワード管理に関する注意喚起、スケアウェアについて示します。

1.4.1 SQLインジェクション攻撃とその影響

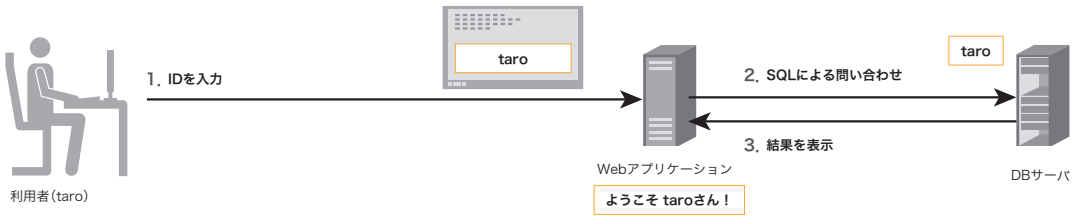
Webサイトに対する攻撃手法のひとつとして、SQL[*23]インジェクション攻撃と呼ばれる手法が知られています。これは、外部からの要求により、Webを構築するためのソフトウェア(Webアプリケーション)が利用しているデータベース(DB)を不正に操作するものです。

「1.3.3 SQLインジェクション攻撃」でも示したように、この攻撃は継続的に発生しています。この攻撃の結果、DBに保存された顧客情報等を盗み取るだけではなく、Webのコンテンツを改ざんして不正なプログラムを埋め込んだり、悪質なサイトへ誘導する内容に書き換えたりすることで、利用者に直接被害を与えることになります。

■SQLインジェクション攻撃の仕組み

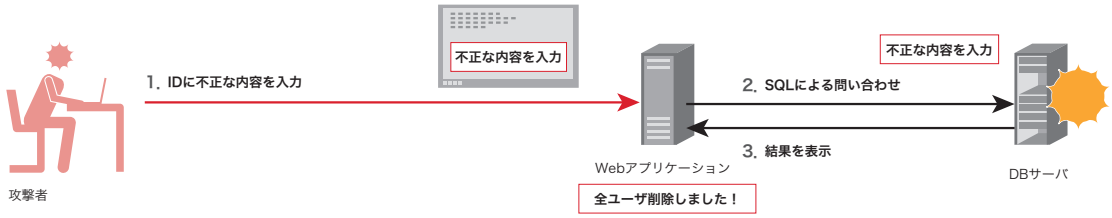
Webアプリケーションが利用者の要求に応じてDBへ問い合わせる際、利用者からの入力値を元にSQL文を構成する処理を行います。入力値に特別な文字が含まれていない場合は、テンプレートとなる元のSQL文に入力値をそのまま展開することで、意図したとおりの問い合わせが行われます(図-9)。しかし、悪意のある攻撃者が、引用符等の特殊な文字を含み、SQL構文の一部を構成するような文字列を入力した場合、入力値の形式チェックや引用符のエスケープ等を行っていないと、展開後のSQL文が意図したものと異なる命令になることがあります(図-10)。

このように、元のSQL文に別のSQL文を注入(inject)し、予定と異なる動作をさせる攻撃手法を、SQLインジェ



通常のアクセスでは、利用者の入力内容がWebアプリケーションによりDBに渡され、コンテンツが生成される。

図-9　通常の処理



SQLインジェクション攻撃では、不正な入力内容がWebアプリケーションによりDBに渡され、意図しない動作が発生する。

図-10 SQLインジェクション攻撃

*23 SQLとは、アプリケーションプログラムがデータの操作(検索、作成、変更、削除等)をデータベースに指示する際に使用する問い合わせ言語。

クション攻撃と呼びます。SQL文を注入するための手段には、Webアプリケーションのテキスト入力フォームのほか、WebアプリケーションやDBの実装に依存して、Cookie等のHTTPヘッダや、GET、POST等のパラメータへの注入等、様々な手段があります。これらの手段は検知をすり抜けるために悪用されています。

また、SQLインジェクション攻撃が成立した場合でも、WebアプリケーションやDBには、エラーメッセージなどの痕跡が残らないことが多く、通常の監視では検出が困難です。この性質から、特にコンテンツが改ざんされた場合は、第三者からの通報で初めて事件が発覚するケースが多くなっています。

■SQLインジェクション攻撃の影響

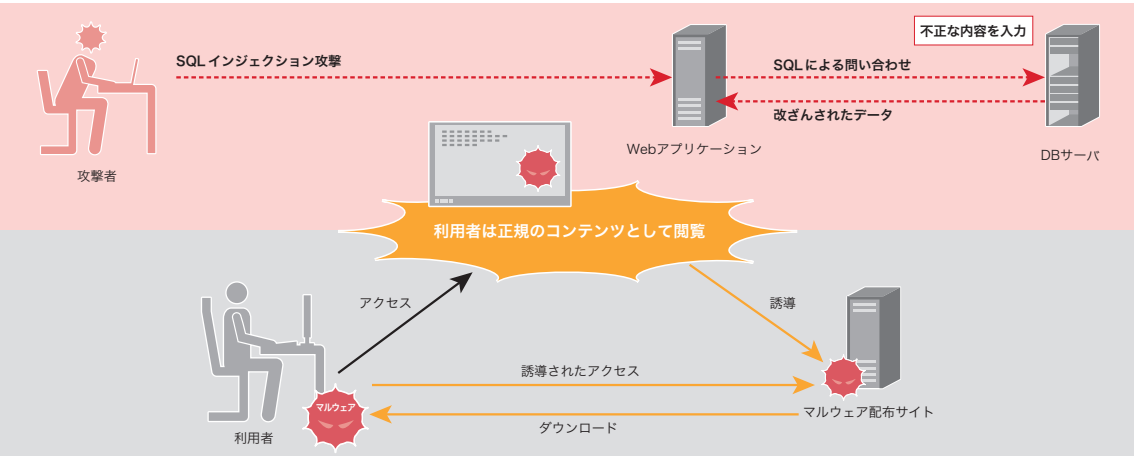
SQLインジェクション攻撃が成功した場合、その結果としていくつかの被害が考えられます。

まず、DBに格納された機密情報や、利用者の個人情報の漏えいが想定されます。次に、データの消去破壊が考えられます。Webコンテンツやユーザ情報等を消去された場合、Webを通じたサービス提供が不可能となります。更に、コンテンツの書き換えが挙げられます。Webのコンテンツを書き換えられると、意図しない内容の情報を発信することになり、マルウェアに感染させる悪質なサイトへと誘導する等、利用者に直接的な被害を与えることもあります。他には、SQLインジェクション攻撃をきっかけにして、システムに侵入される事件も発生しています。バックドアを設置する等の手法で、システムを制御されると、そのシステムを踏み台にして他のシステムに攻撃が行われることになります。

SQLインジェクション攻撃が成功した場合には、以上のような影響を受けますが、その影響に気が付かず、放置していると、第三者や他のシステムに被害が拡大する可能性が高くなります。

■コンテンツの改ざんによる利用者への攻撃

SQLインジェクション攻撃の最近の傾向として、Webサイトのコンテンツを改ざんして攻撃スクリプト等を設置することで、Webサーバにアクセスしてきた利用者を、マルウェアのダウンロードサイトへ誘導する攻撃が増えています*24 (図-11)。Webサーバ自体は正当なものであるため、利用者は改ざんされた悪意のあるコン



SQLインジェクション攻撃によるコンテンツ改ざんでは、Webサーバのコンテンツが改ざんされるだけではなく、改ざんされたコンテンツにアクセスした利用者が、被害を受ける可能性がある。

図-11 コンテンツの改ざんによる利用者への攻撃

＊24 例えば、情報処理推進機構による「10大脅威 攻撃手法の『多様化』が進む（http://www.ipa.go.jp/security/vuln/10threats2009.html）」に掲載されている「システム管理者・開発者への脅威　第1位 正規のウェブサイトを経由した攻撃の猛威」等。

テンツであることに気付かず、マルウェアに感染する可能性が高くなります。この場合、利用者が偽の情報を見分けることは困難であり、サイト運営者による対策が重要です。

■対策

最後に、SQLインジェクション攻撃を防ぐための対策手法についてまとめます。

■Webアプリケーション作成時の注意

Webアプリケーションを作成する場合には、SQLインジェクションに対して耐性を持つように十分注意する必要があります。前述のように、SQLインジェクションは、不正な入力文字列の取り扱いが不完全であるために発生するものです。まず、DBへの問い合わせを行う際にバインド機構*25と呼ばれる仕組みを利用することができます。

その他の対策としては、入力文字列の形式チェックや、攻撃者へ攻撃のヒントを与えないようにエラーメッセージに含める情報を必要最小限にする、また、DBへのアクセス権限を適切な範囲に限定する等が考えられます。加えて、Webアプリケーションの動作テストには、Webアプリケーションの脆弱性を検証するためのソフトウェアの利用や、第三者による監査を受けることが望まれます。詳しくは、IPAの「安全なウェブサイトの作り方」*26やOWASP (Open Web Application Security Project)の「SQL Injection」*27等をご覧ください。

■運用上の対策

今日では、Webサイトは複数のソフトウェアで構築されているので、利用中の実装の脆弱性情報に十分に注意しましょう。静的なコンテンツのみを提供する場合においても同様です。また、攻撃を受けた際の正確な状況把握のために、通信ログ(POSTデータ、Cookie、SQLクエリ文等)を確実に記録・保存できる環境を構築する必要があります。

異常を早期に検知し、攻撃の状況を把握するためには、DBへの問い合わせで発生したエラーをアラートとして通知し、アラート発生に応じて状況を確認するような運用を行うことが必要です。このために、IDSやIPS、WAF*28等の導入や、専門事業者によるセキュリティオペレーションサービスの利用を検討することもできます。

1.4.2 ID・パスワード管理に関する注意喚起

■頻発するID不正利用事件

2008年9月、国内オークションサイトでIDとパスワードの盗難による「なりすまし事件」が発生し、身に覚えのない出品料を請求される被害が発生しました。この事件では「他サイトと同一のパスワードを設定していたこと」が原因のひとつであるとされ、他サイトとパスワードを共有しないよう注意喚起がなされています。また、2008年末ごろから、ID不正利用によってホームページが書き換えられ、マルウェア感染に誘導される悪質なコンテンツを埋め込まれる事件が増加しており、IIJのお客様においても被害が確認されています。

＊25 バインド機構とは、SQL文中で、特別な文字を含んだ文字列を安全に扱うための機能で、SQL文の構造そのものと入力値から生成した文字列を明確に分けて扱うことで、不正なSQL文の注入を防ぐ。バインドメカニズムとも呼ばれる。
＊26 情報処理推進機構による「安全なウェブサイトの作り方(http://www.ipa.go.jp/security/vuln/websecurity.html)」。
＊27 OWASPによるSQL Injection対策(http://www.owasp.org/index.php/SQL_Injection)。
＊28 Webアプリケーションファイアウォール(Web Application Firewall)。Webの通信を監視し、受信した入力や送信するコンテンツの内容を検査することで脆弱性への攻撃や不正侵入等を防御するファイアウォールの一種。

■パスワードの強さ

古くから「強いパスワード」の選択方法や、正しくパスワードを管理する手法が存在しています。IPAによる注意喚起[*29]では、定期的な変更やログイン履歴の確認等について、基本的な管理方法が紹介されています。またSANSパスワードポリシー[*30]等、強いパスワードの付け方に関するベストプラクティスも共有されるようになり、ある規則を満たした強いパスワードを自動生成するオープンソースソフトウェア[*31]も利用できるようになりました。これらの手法を利用することで、ある特定のIDに対するパスワードは、その基本的な機能を十分に発揮することができます。

■IDとパスワード管理の難しさ

一方で、一般的にインターネットを利用するユーザは、ネットショッピングやSNS、ブログ等様々なサービスを利用するようになってきました。それに伴い、多くのサービスでIDとしてメールアドレスを利用しています。また、異なるサービスごとに適切なパスワードを設定し、適切に管理を行う必要が出てきました。つまり、一般のユーザが、複数の異なる「強いパスワード」を定期的に変更しながら利用する必要に迫られています。このため、複数の異なるパスワードを覚えきれなくなり「パスワードの使い回し」も行われています。

この状況から、ひとつのサービスのIDとパスワードを知られると、他の複数のサービスも不正利用される可能性がある等、IDとパスワードが他人に知られたときのリスクが高くなっています。

■利用者としての確認

多くのユーザは、Webブラウザやメールソフトウェアに IDとパスワードを記憶させています。いくつかのWebブラウザでは、Webブラウザ自身の機能やアドオンの利用により、自分がどのようなIDとパスワードを利用しているのかを知ることができます。複数の異なるサイトで同じIDとパスワードを利用している場合は、それぞれ新しいパスワードに変更することをお勧めします。IDとパスワードが漏えいした場合に、どのような影響があるかを検討し、直接金銭にかかわるサービス等、特に重要度の高い対象については、他のサービスと同じIDとパスワードを利用しないようにしましょう。

次に、複数のパスワードを記憶する方法の利用を検討してください。例えば、ひとつのマスタパスワードだけを覚えておくことで管理できる、集中型パスワード管理ツール(Password Safe[*32]やPassword Wallet[*33]等)が挙げられます。

■管理者としての確認

組織内ネットワークの管理者の立場では、組織内で適切なIDとパスワード利用を徹底するために、最低限、業務に利用しているIDとパスワードを個人的に利用しないということを、ユーザに周知徹底する必要があります。個人的に利用しているサイトで業務と同じIDとパスワードを利用しているケースを発見し、指摘することは容易ではありませんが、組織内ポリシーで明文化し、使い回しの危険性を周知することで、ユーザの意識を向上させることができます。

＊29 情報処理推進機構による「今一度、パスワードを点検しましょう！（http://www.ipa.go.jp/security/txt/2008/10outline.html)」。
＊30 The SANS Instituteによる「SANS Password Policy(http://www.sans.org/resources/policies/Password_Policy.pdf)」。
＊31 例えば、pwgen(http://sourceforge.net/projects/pwgen/)等。
＊32 Password Safe(http://www.schneier.com/passsafe.html http://passwordsafe.sourceforge.net/)。
＊33 Password Wallet(http://www.apple.com/jp/downloads/macosx/utilities/passwordwallet.html)。

また、自組織内のサーバにおいては、パスワードが容易に推測できるものかどうかを、チェックするシステムの利用が望まれます。一般的には辞書を用いてチェックする方法[*34]があります。

■まとめ

本稿では、IDとパスワードの管理方法について利用者及び管理者が確認すべき点について指摘しました。業務で利用するサーバとSNSやブログ等プライバシ情報を取り扱うサービス、更に懸賞応募等の一時的にしか利用しないWebサイト等で、安易に同じIDとパスワードを利用していないでしょうか。今一度ご確認されることをお勧めします。

1.4.3 スケアウェア

ここでは、最近脅威が高まっている偽セキュリティソフト「スケアウェア(Scareware)」の実態について紹介します。スケアウェアとは、Scare＝恐怖を与える、Software＝ソフトウェアが語源となったマルウェアの一種です。

スケアウェアは詐欺行為の手助けをするソフトウェアです。ユーザがWebを閲覧中に、「PCがマルウェアに感染している」等と脅し、偽の製品に誘導し、実際には不必要なソフトウェアを購入させることでユーザから金銭を詐取します。

ここでは、偽ウイルス対策ソフトを例にとり、スケアウェアによる詐欺行為の典型的な流れを示します。

1. ユーザがWebページを閲覧していると、突然「あなたのコンピュータはウイルスに感染している可能性があります。今すぐ検査をしますか？」というメッセージのポップアップが出現します(図-12)。

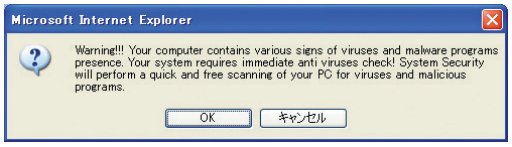


図-12 スケアウェアによるポップアップの例

2. そのポップアップをクリックすると、オンラインウイルススキャンを偽った検査画面が表示されます(図-13)。

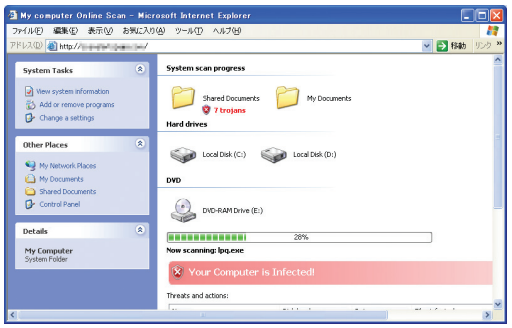


図-13 偽のスキャン画面

3. 偽スキャンが終了すると、「あなたのコンピュータは脅威にさらされています。今すぐウイルス対策ソフトをダウンロードしてインストールしてください」と促すポップアップが出現します(図-14)。

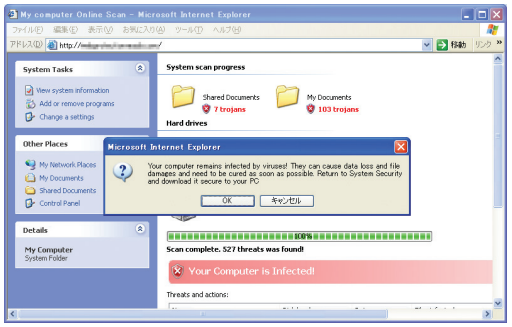


図-14 偽のスキャン結果

＊34 例えば、LinuxではPAM (Pluggable Authentication Modules)としてpam_cracklibが提供されており、辞書を用いたパスワードチェックを行うことができる(http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/sag-pam_cracklib.html)。

4. そのポップアップをクリックすると、偽ウイルス対策ベンダのWebページ(図-15)に誘導されたり、直接スケアウェアのダウンロードが始まったりするという精巧な作りになっています。

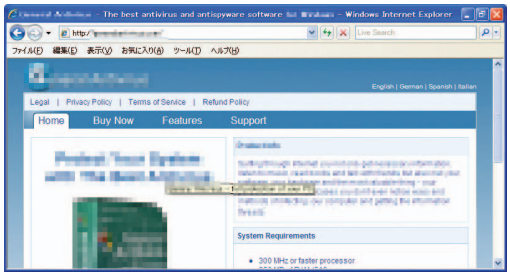


図-15 偽ウイルス対策ベンダのWebページの例

5. ユーザはそこから偽のウイルス対策ソフトをダウンロードし、インストールしてしまいます。

6. 偽のウイルス対策ソフトによる自動スキャンが行われ、ここでも多数のマルウェアに感染していると、偽の結果が表示されます(図-16)。

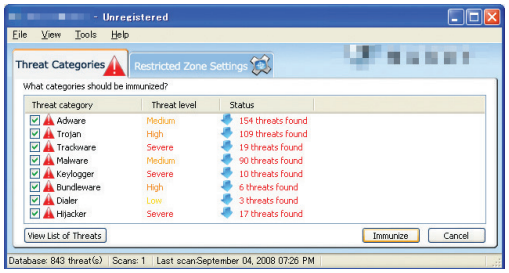


図-16 偽ウイルス対策ソフトによる偽のスキャン結果

7. 見つかったマルウェアを駆除しようと駆除ボタンを押すと、有料版を購入するよう指示が表示されます。マルウェアの感染を信じ込まされたユーザは役に立たないソフトウェアを購入することになります(図-17)。

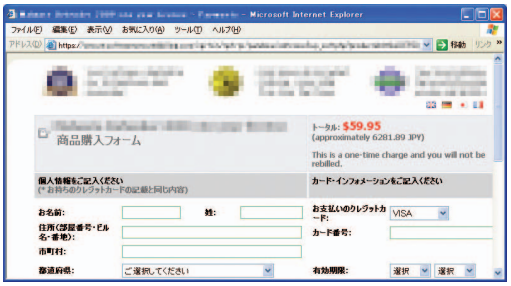


図-17 偽ウイルス対策ソフトの購入画面の例

またスケアウェアをインストールすると、スケアウェア自身がアップデートと称して別のマルウェアをダウンロードしてインストールをする場合もあります。以上の流れを図-18に示します。

偽ウイルス対策ソフトの画面(図-16)や偽ウイルス対策ベンダのWebページ(図-15)のように、スケアウェアは実際のウイルス対策ソフトのGUIやWebコンテンツとよく似た作りになっているため、被害が拡大していると考えられます。また日本語でスケアウェアに誘導される場合もあります。

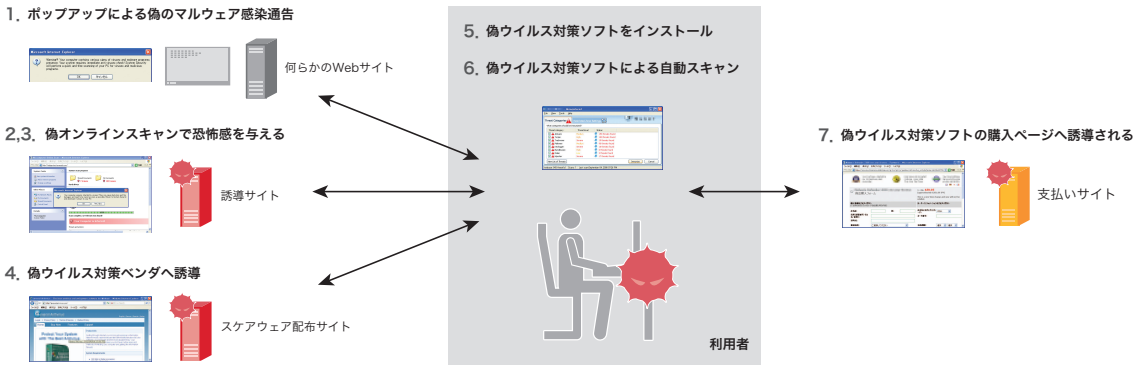


図-18 スケアウェア問題の流れ

今回例として紹介した偽のウイルス対策ソフトの他にも、偽のファイアウォールや、偽のスパイウェア対策ソフト等の存在も確認されています。この手口に惑わされないためには、まず信頼できる正規のセキュリティ対策ソフトを普段から利用しておくことが重要です。例えば、ウイルス対策ソフトでは、信頼できる情報源から紹介*35された対策ソフトを選ぶことや、ウイルス対策の業界団体*36の加盟企業を確認することで、信頼できるウイルス対策ソフトを見分けることができます。

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。

このVol.3では、通常の状況報告に加え、パスワード管理やスケアウェア等、現在流行中で、調査と対策を行っており、未だに決着を見ていないインシデントについて紹介しました。

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、安全かつ安心して利用できるよう、今後も努力を継続してまいります。

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。

大原 重樹　土屋 博英（1.4.1 SQLインジェクション攻撃とその影響）
永尾 禎啓　須賀 祐治（1.4.2 ID･パスワード管理に関する注意喚起）
鈴木 博志　梅澤 威志（1.4.3 スケアウェア）
IIJ サービス事業統括本部 セキュリティ情報統括部

桃井 康成（1.4.1 SQLインジェクション攻撃とその影響）
IIJ 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

協力:
松崎 吉伸
IIJ ネットワークサービス本部 ネットワークサービス部 技術推進課

堂前 清隆
IIJ 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

＊35 利用するISP等が紹介する製品はもちろんのこと、例えば、マイクロソフト社のWebページに記載されている対策ベンダー一覧等も参考にすることができる(http://support.microsoft.com/kb/49500/ja)。
＊36 ウイルス対策業界団体の例。例えば、VIA(Virus Information Alliance)（http://technet.microsoft.com/ja-jp/security/cc165596.aspx)、AMTSO（Anti-Malware Testing Standards Organization）(http://www.amtso.org/members.html)、ASC（Anti-Spyware Coalition）(http://www.antispywarecoalition.org/about/index.htm)等。