

情報セキュリティ白書 2009 第Ⅱ部

10 大脅威

攻撃手法の『多様化』が進む



IPA[®]

独立行政法人 情報処理推進機構
セキュリティセンター

2009年3月

目次

第Ⅱ部 10大脅威

攻撃手法の『多様化』が進む

■ 組織への脅威.....	2
【1位】 DNS キャッシュポイズニングの脅威 [総合:1位].....	2
【2位】 巧妙化する標的型攻撃 [総合:3位].....	4
【3位】 恒常化する情報漏えい [総合:5位].....	6
■ 利用者への脅威.....	8
【1位】 多様化するウイルスやボットの感染経路 [総合:4位].....	8
【2位】 脆弱な無線 LAN 暗号方式における脅威 [総合:6位].....	10
【3位】 減らないスパムメール [総合:8位].....	12
【4位】 ユーザ ID とパスワードの使いまわしによる危険性 [総合:10位].....	14
■ システム管理者・開発者への脅威	16
【1位】 正規のウェブサイトを経由した攻撃の猛威 [総合:2位].....	16
【2位】 誘導型攻撃の顕在化 [総合:7位].....	18
【3位】 組込み製品に潜む脆弱性 [総合:9位].....	20
【付録 1】 10大脅威関係表	22
【付録 2】 10大脅威相関図.....	23
【付録 3】 参考資料	24
第Ⅱ部 執筆協力者	25

本書は、次の URL からダウンロードできます。

情報セキュリティ白書 2009 第Ⅱ部

10大脅威 攻撃手法の『多様化』が進む

<http://www.ipa.go.jp/security/vuln/10threats2009.html>

第Ⅱ部 10 大脅威

攻撃手法の『多様化』が進む

「情報セキュリティ早期警戒パートナーシップ」に参画する関係者のほか、情報セキュリティ分野における研究者、実務担当者など 111 名から構成される「情報セキュリティ検討会(P.25 参照)」でまとめたものである。

安全なインターネットの利用における脅威を、2008 年に「印象が強かったもの」「社会的影響が大きいもの」などの観点からランキング投票を行い、10 大脅威を選んだ。また、今年は新たに、「組織」「利用者」「システム管理者・開発者」の 3 つのカテゴリに分け、それぞれの脅威を主に関連するカテゴリで分類し、問題の概要、問題の経緯、被害状況・対策状況、対策方法などをまとめた。

近年、特定の組織を狙った DNS キャッシュポイズニングや巧妙化する標的型攻撃、また、不特定多数を狙って多様化するウイルスやボット、正規のウェブサイトを改ざんして閲覧者を狙う攻撃など、攻撃手法の多様化が進んでいる。

■組織への脅威

- 【1 位】 DNS キャッシュポイズニングの脅威
- 【2 位】 巧妙化する標的型攻撃
- 【3 位】 恒常化する情報漏えい

■利用者への脅威

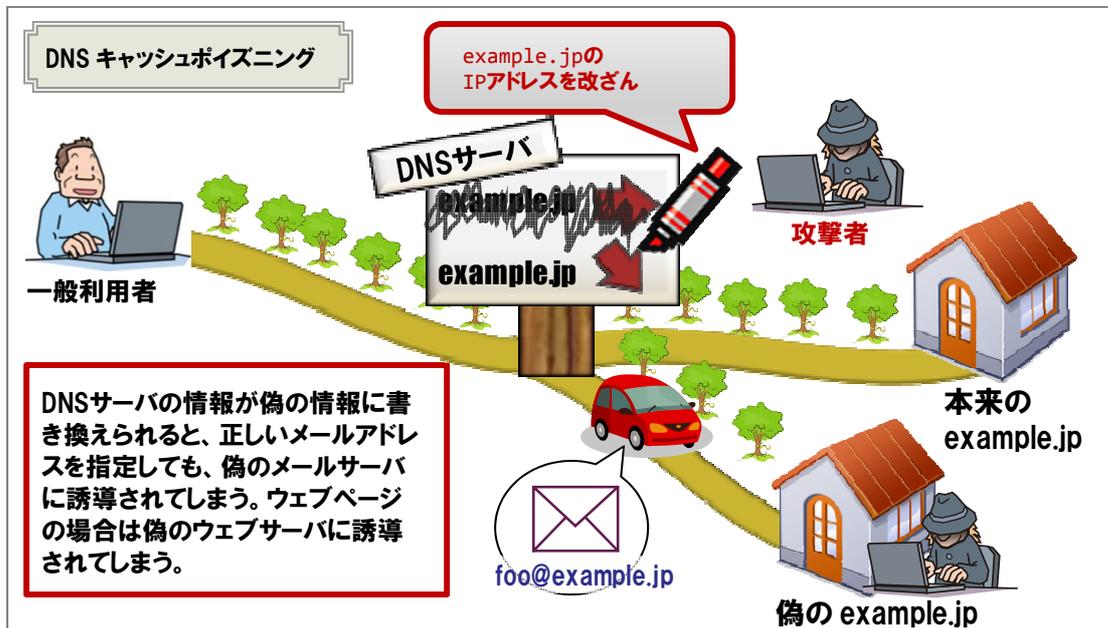
- 【1 位】 多様化するウイルスやボットの感染経路
- 【2 位】 脆弱な無線 LAN 暗号方式における脅威
- 【3 位】 減らないスパムメール
- 【4 位】 ユーザ ID とパスワードの使いまわしによる危険性

■システム管理者・開発者への脅威

- 【1 位】 正規のウェブサイトを経由した攻撃の猛威
- 【2 位】 誘導型攻撃の顕在化
- 【3 位】 組込み製品に潜む脆弱性

■ 組織への脅威

【1位】DNS キャッシュポイズニングの脅威 [総合:1位]



2008年の7月に、各ベンダより一斉にDNS関連ソフトウェアのバージョンアップやパッチがリリースされた。これはDan Kaminsky氏により発見された新しいDNSキャッシュポイズニングの脆弱性に暫定的な対策をするためのものだった。

<問題の概要>

DNS(Domain Name System)は、ホスト名(例:www.ipa.go.jp)とIPアドレス(例:202.229.63.242)とを結び付ける情報を提供する仕組みである。インターネット上の多くのネットワークサービスはDNSの存在を前提としていることから、DNSはインターネットの基盤サービスとも言える。

DNSキャッシュポイズニングの脆弱性は攻撃に悪用されると、DNSサービスを提供しているサーバ(DNSサーバ)の本来あるべき情報を偽の情報に書き換えられてしまう。偽の情報に書き換えられると、被害を受けたDNSサーバの利用者は正しいURLやメールアドレスを入力しているにも関わらず、攻撃者が用意した偽のウェブサイトやメールサーバなどに誘導されてしまい、フィッシング詐欺やメールの情報漏えいなどの被害を受ける可能性がある。

従来からDNSキャッシュポイズニングの脆弱性があることが知られていたが、この脆弱性をつく攻撃の場合、1度攻撃(偽の応答の送信)を行ってから次の攻撃を行うまでに待ち時間が生じるため、攻撃の効率が非常に悪いと考えられていた。Dan Kaminsky氏は、この待ち時間を無くす攻撃方法を発見し、多くのDNSサーバが極めて脆弱な状態にあることを示した。

各ベンダから公表されているこのDNSキャッシュポイズニングの脆弱性への対策はあくまで暫

定的な対策である。この問題に対する完全な対策はDNSのセキュリティを向上させるための拡張仕様であるDNSSEC(DNS Security Extension)を利用するなどの手段がある。しかし、この技術はまだ一般的ではない。現在この脅威をどのようにすれば根本的に対策できるかが、インターネット関連技術の標準化を進めるIETF(Internet Engineering Task Force)などで議論されている。

<問題の経緯>

2008年にKaminsky氏が発表したDNSキャッシュポイズニングの脆弱性は、当初、修正パッチが公表された後に詳細を公表する予定であったが、7月に各ベンダが対策を公表したのとほぼ同時に攻撃の手法が推測により公表され、攻撃として悪用されてしまい問題が深刻化した。

<被害状況・対策状況>

この問題により、米国のインターネットサービスプロバイダ(ISP)が運営するDNSキャッシュサーバを攻撃され本来辿りつくべきウェブサイトとは異なるウェブサイトに誘導される被害があったと報道されている。

なお、2008年12月末までに早期警戒パートナーシップに基づいてIPAへ届出られたDNSキャッシュポイズニングの脆弱性に関する届出は792件あった。このうち、1月末までに修正が完了する等で取り扱い終了となった件数は108件で、まだ684件が修正されていない状況である。

<対策方法>

システム管理者は本問題の被害を軽減するために、DNS関連ソフトウェアを対策版へバージョンアップした上で、次のような対策をする必要がある。

- ・ コンテンツサーバの再帰問合せ動作が無効になっていることを確認する。
- ・ キャッシュサーバはファイアウォールなどのパケットフィルタリング機能を用いて、必要な箇所からの再帰問合せのみを許可するよう制限する。
- ・ キャッシュサーバ兼コンテンツサーバで運用している場合には、再帰問合せ動作は、組織内ネットワークからのアクセスのみを許可したり、それが難しい場合、キャッシュサーバとコンテンツサーバを物理的に分離したりして運用する必要がある。

関連資料

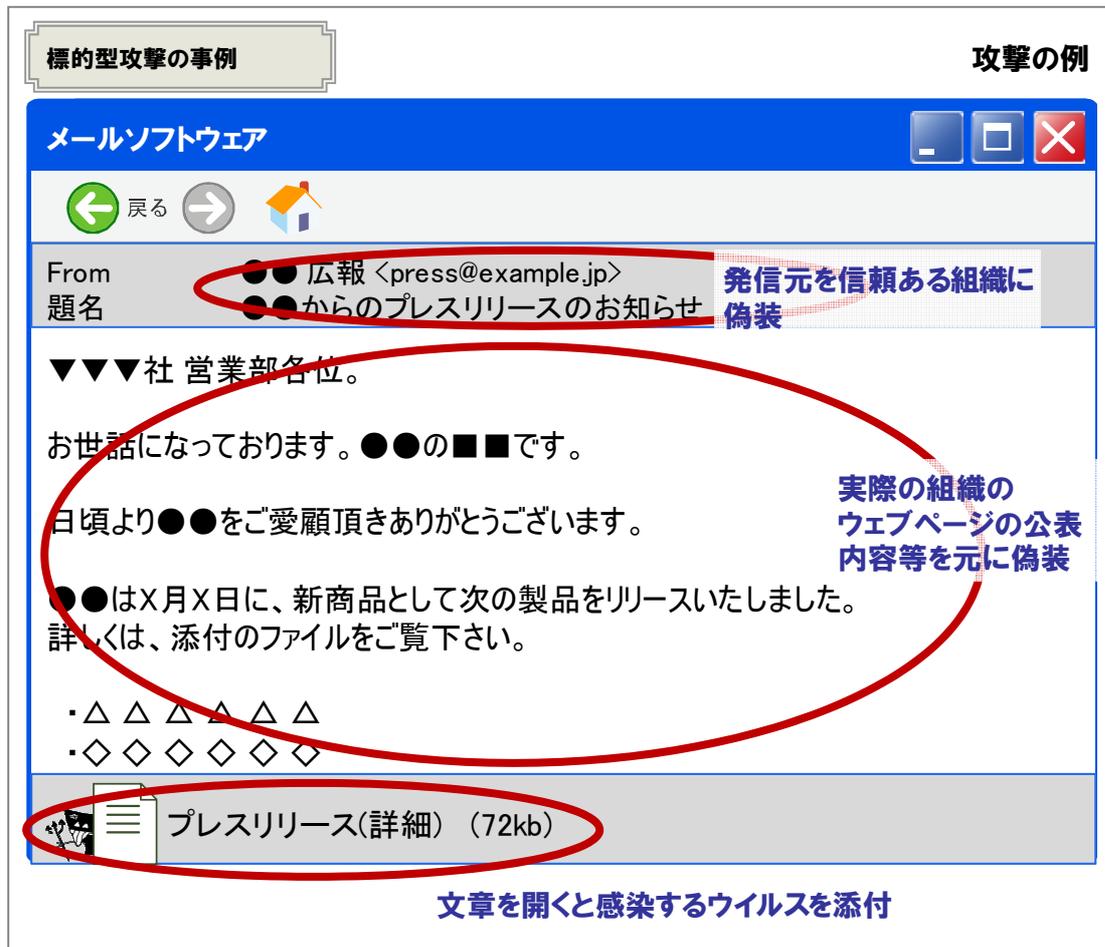
JPCERT/CC: 複数のDNSサーバ製品におけるキャッシュポイズニングの脆弱性

<http://www.jpccert.or.jp/at/2008/at080013.txt>

IPA: DNSキャッシュポイズニング対策

http://www.ipa.go.jp/security/vuln/DNS_security.html

【2位】巧妙化する標的型攻撃 [総合:3位]



標的型攻撃は、攻撃対象を特定の組織や人に限定した攻撃である。2008 年は、人間の心理・行動の隙を突くことで情報を不正に取得する「ソーシャル・エンジニアリング」の手口を利用し、ソフトウェアの脆弱性を利用したウイルスなどを配布など、攻撃手法が巧妙化した(※ウイルスの詳細は、■利用者への脅威 - 【1位】多様化するウイルスやボットの感染経路を参照)。

<問題の概要>

標的型攻撃は、ソーシャル・エンジニアリングの手口により、攻撃であることに気づきにくいことが最大の脅威である。例えば信頼ある取引先や人物からのメールとして差出人を偽装され、内容も信ぴょう性の高い情報が記載されているため、つい信用してしまう危険性がある。また、このようなメールに添付されている文書ファイルや圧縮ファイルには、脆弱性を悪用するウイルスが仕込まれていることがあり、通常のファイルと同じように見えてしまうため、つい開けてしまう危険性がある。添付されたウイルスファイルを開いてしまうと、あたかも通常の文書ファイルが表示されているだけのように見えるが、実際には利用者に見えない方法で、他のウイルスに感染させられたり、重要な情

報を盗まれたりすることがある。

＜問題の経緯＞

標的型攻撃は、2005年に米国のUS-CERTなどが発表した資料から問題視されるようになった。それを受けて、日本ではJPCERT/CCから標的型攻撃に関する注意喚起「トロイの木馬に関する注意喚起」が発表された。2006年には、警察庁に対して標的型攻撃が行われたことについての報道や、防衛庁(現防衛省)を騙ったメールに関する注意喚起が話題となった。

完全な対策が困難であることに大きな変化はないが、2008年にはJPCERT/CCが「標的型攻撃対策手法に関する調査報告書」を発表したり、IPAから「近年の標的型攻撃に関する調査研究」を発表したりと、標的型攻撃に対抗するべく実態の調査が行われた。

＜被害状況＞

2008年春にはIPAや情報処理学会のコンピュータセキュリティシンポジウム(CSS)2008を騙った標的型攻撃があった。IPAを騙った標的型攻撃では、IPAがウェブサイトで公開している情報セキュリティに関わる注意喚起や調査報告書の文面および添付ファイルが悪用されていた。この添付ファイルを開くことによって、複数の脆弱性によってウイルスに感染させられる可能性があった。また、2008年は、米国で経営者に対して標的型攻撃があったことが報道された。

＜対策方法＞

標的型攻撃においても、ウイルス感染を防ぐには、一般的なウイルス対策が有効である。OSやアプリケーション、ActiveXなどのプラグイン、ウイルス対策ソフトウェアの定義ファイルを随時最新の状態にするなどの対策が挙げられる。

またIPAを騙った標的型攻撃の例では、ユーザのコンピュータに感染したウイルスは攻撃者からの指令を受けるために外部との通信を試みている。この場合、システム管理者がファイアウォールで不要な通信を遮断したり、HTTP/HTTPSアクセスを認証付プロキシサーバ経由に限定したりすることで、被害の拡大を防ぐ効果が得られる。

関連資料

PC Online:国内企業を狙った「標的型攻撃」を確認、手口を変えて毎週攻撃

<http://pc.nikkeibp.co.jp/article/news/20081218/1010634/>

TECHWORLD:企業の経営層を標的にした巧妙な詐欺メールがまん延

<http://www.techworld.jp/channels/security/101778/>

【3位】 恒常化する情報漏えい [総合:5位]



毎日のように個人情報や技術情報などの機密情報といった、各種情報漏えいに関する事件・事故が話題になっている。2008 年も情報漏えいの事件・事故は多発した。情報漏えいは情報セキュリティ白書においても毎年取り上げている重要度の高い問題である。

<問題の概要>

情報漏えいの事件・事故は、その要因として様々なものが挙げられる。

- ・ 記憶媒体や紙媒体の紛失・盗難によって漏えいするケース
- ・ ウイルス感染によって漏えいするケース
- ・ メール等の誤送信によって漏えいするケース
- ・ 組織内部での不正行為によるケース
- ・ ファイル交換ソフトを介して漏えいするケース
- ・ ウェブサーバの設定ミスなど、不適切な運用により漏えいするケース
- ・ ウェブアプリケーションに存在するSQLインジェクションなどの脆弱性により漏えいするケース(※詳細は■システム管理者・開発者への脅威【1位】 - 正規のウェブサイトを経由した攻撃の猛威を参照。)

情報漏えいの事件・事故の全てを防ぐことは難しいが、技術的な対策の実施や組織としてのルール作成し、運用することによって、情報漏えいの予防や、従業員に対する意識の向上などの効果が期待できる。

<問題の経緯>

2003年に成立し、2005年に完全施行された個人情報保護法をきっかけに、情報漏えいの事件が目立つようになり、同法に対応すべく各企業において組織体制が整備されるようになった。情報漏えい事故の対策として、持ち出せるコンピュータを制限するルールを適用したり、USBなどの外部接続メディアの使用を禁止したりするなど、情報機器の利便性を低下させるルールを採用する組織もある。一方で、仮に持ち出したコンピュータを紛失、盗難の被害にあった場合でも情報漏えいの被害にあわないよう、コンピュータのHDDに暗号機能を標準搭載するなど、利便性を犠牲にすることなく安全に使用できるよう技術の面での取り組みも進んできている。

<被害状況>

個人情報の漏えいを例にすると、JNSA(NPO 日本ネットワークセキュリティ協会)のセキュリティ被害調査ワーキンググループが発表した「2008年上半期 情報漏えいインシデント報告書(速報版)」によると、漏えいした個人情報の延べ人数は前年までと比較して大幅に減少した。しかし、漏えい件数は2008年上半期のみで683件ののぼり、過去最も多かった2005年(1,032件)を上回る可能性があるとされている。また漏えいの原因は、誤操作、紛失などのヒューマンエラーによるものが半数以上を占めている。

<対策方法>

経営者はIPAが公表している「情報セキュリティマネジメントとPDCAサイクル」などを参考に組織の情報セキュリティに対する考え方を整理し、組織内に徹底する必要がある。組織にどのような危険があり、どのような対策を行うべきか、どのような効果があるかを検討する必要がある。その検討から、ルールを作成したり、体制を整備したり、ルールを運用したりする必要がある。

システム管理者は経営者が作成した基準に基づいてどのように運用していくか、具体的に守るべき手法についての手順を作成する必要がある。手順は一度作成して終わりではなく、手順自体の見直しも必要である。例えば手順の修正が必要な箇所の洗い出しや新しい脅威が出た場合の対応方法についても考慮しておく必要がある。

関連資料

JNSA:【速報版】2008年上半期 情報セキュリティインシデントに関する調査報告書(Ver. 1.0)

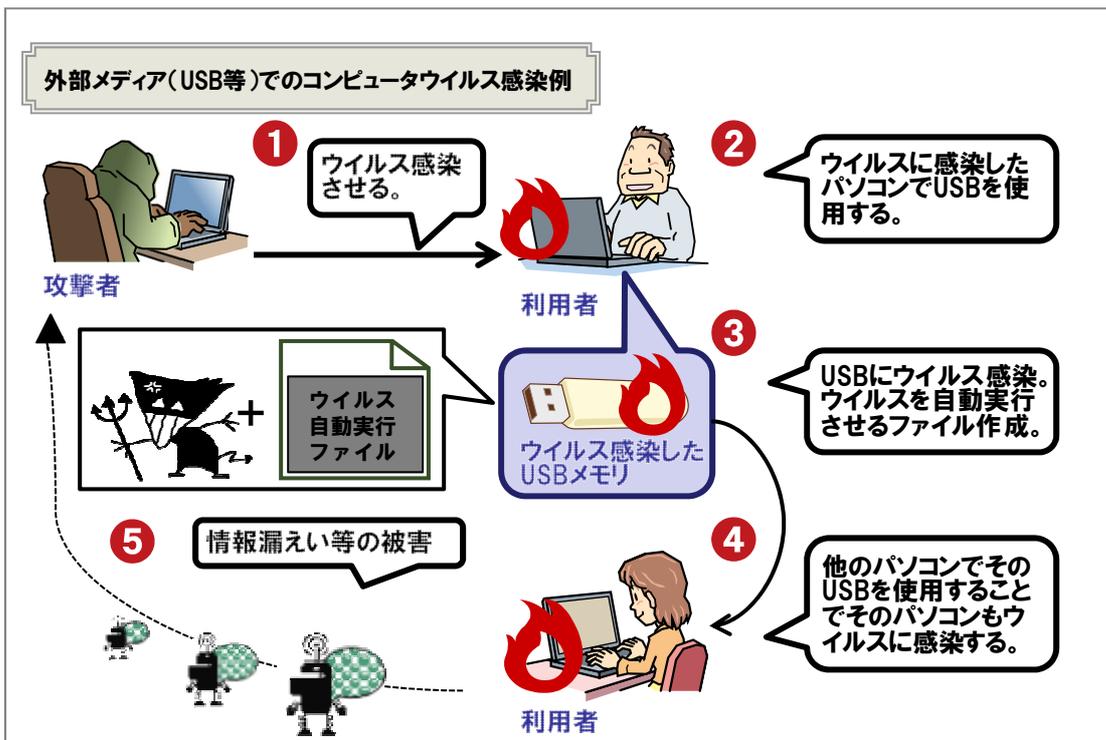
<http://www.jnsa.org/result/2008/pol/incident/>

IPA: 情報漏えいインシデント対応方策に関する調査

<http://www.ipa.go.jp/security/awareness/johorouei/index2.html>

■ 利用者への脅威

【1位】多様化するウイルスやボットの感染経路 [総合:4位]



2008年のウイルスは、感染の手口が更に巧妙になり、多様化した。

<問題の概要>

2008年のウイルス感染の事例では、主に下記のようなものがあった。

- ・ ソフトウェアの脆弱性を利用した、電子文書のファイルフォーマットである PDF (Portable Document Format) ファイルや Microsoft Office Word ファイルなどによる感染
- ・ USBメモリなどの外部メディアを介する感染

従来は、主にネットワークに接続されたコンピュータに対してウイルス感染するものだったが、2008年は外部メディアをコンピュータに接続した際に自動的にメディアの内容が実行される機能を悪用して感染するものも出てきたことが特徴と言える。もし、感染した外部メディアをその他のコンピュータで使用すれば、そのコンピュータがネットワークに接続していなかったとしても感染する可能性がある。また、感染したコンピュータが、インターネットに接続できない隔離されたネットワーク上の端末だった場合は、隔離されたネットワーク内で感染が拡大する危険性もある。

また、ボットも猛威を振るった。ボットはウイルスの一種で、コンピュータに感染し、外部からネットワークを通じて操ることを目的として作成されたプログラムである。ボットに感染すると、ボットを利用する指令サーバからの攻撃の命令によって、利用者のコンピュータがスパムメールの大量送信

元や、特定サイトへの DDoS 攻撃元として悪用され、加害者になってしまうなどの脅威がある。

米国の情報セキュリティ専門の民間団体である SANS は、ボット感染コンピュータの台数が、2008 年 6 月から同年 8 月末までの 3 カ月で 4 倍以上になったことの原因について、SQL インジェクション攻撃によって「ボット感染のわな」を仕込まれたウェブサイト経由の感染が増えているためと推測している(※詳細は「■システム管理者・開発者への脅威 - 【1 位】正規のウェブサイトを経由した攻撃の猛威」を参照)。総務省・経済産業省連携プロジェクトのサイバークリーンセンター(CCC)の活動実績によると、ハニーポット(おとりマシン)で収集されたボットウィルスの検体数は 1 ヶ月およそ 30~65 万程度で推移している。

<問題の経緯>

ウイルスは、2000 年頃まで、フロッピーディスクによる感染や、電子メールの添付ファイルによる感染の事例が目立った。2001 年頃よりサーバの脆弱性を悪用して感染を広げるワームというウイルスの一種による脅威が増え始めた。2002 年から 2003 年頃にボットが出現し、2004 年後期より日本国内で問題視されるようになった。その後、ボットは挙動の観測をしにくしたり、指令サーバを冗長化させたりと、年々攻撃が巧妙になり対策が難しくなっている。また、ウイルス作成者の目的も愉快犯的なものから、ウイルスやボットを使用することによって、相手に気づかれずに金銭を狙うことに変化してきている。

<対策方法>

本脅威には従来からの対策である、OS やアプリケーション、ActiveX などのプラグイン、ウイルス対策ソフトウェアの定義ファイルを随時最新の状態にするなどの対策が挙げられる。また、サイバークリーンセンターが配布するボット駆除ツール(CCC クリーナー)は、ボットに感染しているかを確認および感染していた場合の駆除に役立つ。他にも、出所不明の外部メディアをコンピュータに接続しない、外部メディアの自動実行をさせないようにする必要がある。

関連資料

トレンドマイクロ: USBメモリで広まるウイルスへの対策

<http://jp.trendmicro.com/jp/threat/solutions/usb/>

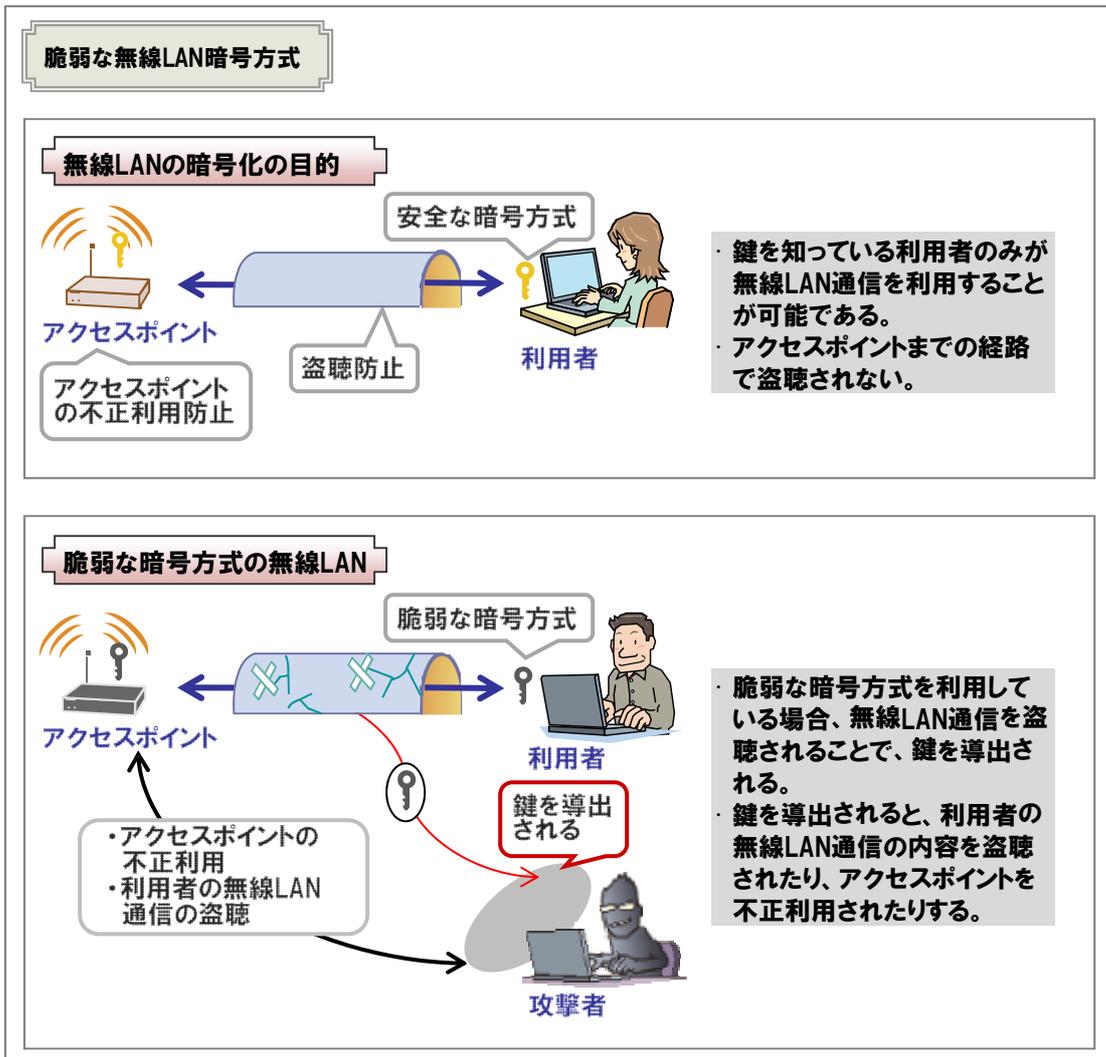
サイバークリーンセンター(CCC): ボットの駆除対策手順

<https://www.ccc.go.jp/flow/index.html>

IPA: コンピュータウイルス・不正アクセスの届出状況[12月分および2008年年間]について

<http://www.ipa.go.jp/security/txt/2009/01outline.html>

【2 位】 脆弱な無線 LAN 暗号方式における脅威 [総合:6 位]



2008 年 10 月、情報処理学会のコンピュータセキュリティシンポジウム(CSS)2008 において、無線 LAN の暗号方式の規格の一つである WEP(Wired Equivalent Privacy)が一般的な環境下において極めて短い期間に解読可能であるという論文が発表された。

<問題の概要>

無線 LAN は、電波を使って無線 LAN アクセスポイントと無線 LAN 機能を持つパソコンなどとの機器間で通信を行うネットワーク環境のことである。無線通信の電波の届く範囲なら壁などの障害物を超えてどこでも通信が可能という利便性を備えている。

しかし、その便利さの一方、物理的な線で通信する有線 LAN に比べて、オフィスや家に侵入せずに無線通信を傍受できるため、通信内容を盗聴する場合、有線 LAN に比べて、悪意ある者から不正アクセスの手段として狙われ易い環境とも言える。

無線 LAN 通信の盗聴を困難にするために、通信を暗号化する技術の一つに、WEP(Wired Equivalent Privacy)という暗号化方式がある。この WEP が一般的な利用環境下において短時間に、例えば 20MB の通信では 10 秒で解析可能であるという論文が発表された。これにより、従来は条件つきであるが、短時間で解読可能であった WEP が、特に条件を必要とせずに解読できることが明らかになった。利用者は暗号化を施しているから無線通信を傍受されても内容が知られないと考えるが、WEP を利用している場合、暗号化した通信内容が漏えいしたり、無線 LAN アクセスポイントを悪用されたりする可能性がある。また、WEP の後継である WPA(Wi-Fi Protected Access)が採用している TKIP(Temporal Key Integrity Protocol)という暗号の規格についても、限定的に一部情報の解読が可能であることが発表された。そのため、将来的観点から、無線 LAN を利用する際、WPA2(Wi-Fi Protected Access 2)を AES(Advanced Encryption Standard)という暗号規格で利用することが推奨されている。

<問題の経緯>

1999 年に無線 LAN の暗号方式の規格として WEP が制定されて以来、研究者による解読が試みられてきた。年々進む暗号解読技術の進化により、WEP では十分な安全性が保てないことが明確となり、2003 年には後継となる WPA が、2004 年には WPA2 が制定された。WEP は問題があるため利用するべきではないとされていたが、2008 年にはそれが更に確定的になった。

<対策方法>

無線 LAN を利用する場合、脆弱な暗号方式 (WEP, WPA-TKIP)の利用を避け、WPA2 の AES の暗号方式を利用する。自宅や組織内などで無線 LAN アクセスポイントを設置する場合、可能であれば電波出力の制限などアクセスできる範囲を制限することで被害を緩和できる。

現在既に WEP を実装されている製品を販売している場合、製品の開発者は、WEP を利用するべきでないことを明確に利用者に示す必要がある。また、WEP に代わる暗号化方式を利用できない製品については、WPA2 などの暗号化方式を利用できるようにソフトウェアを改善することが望まれる。

関連資料

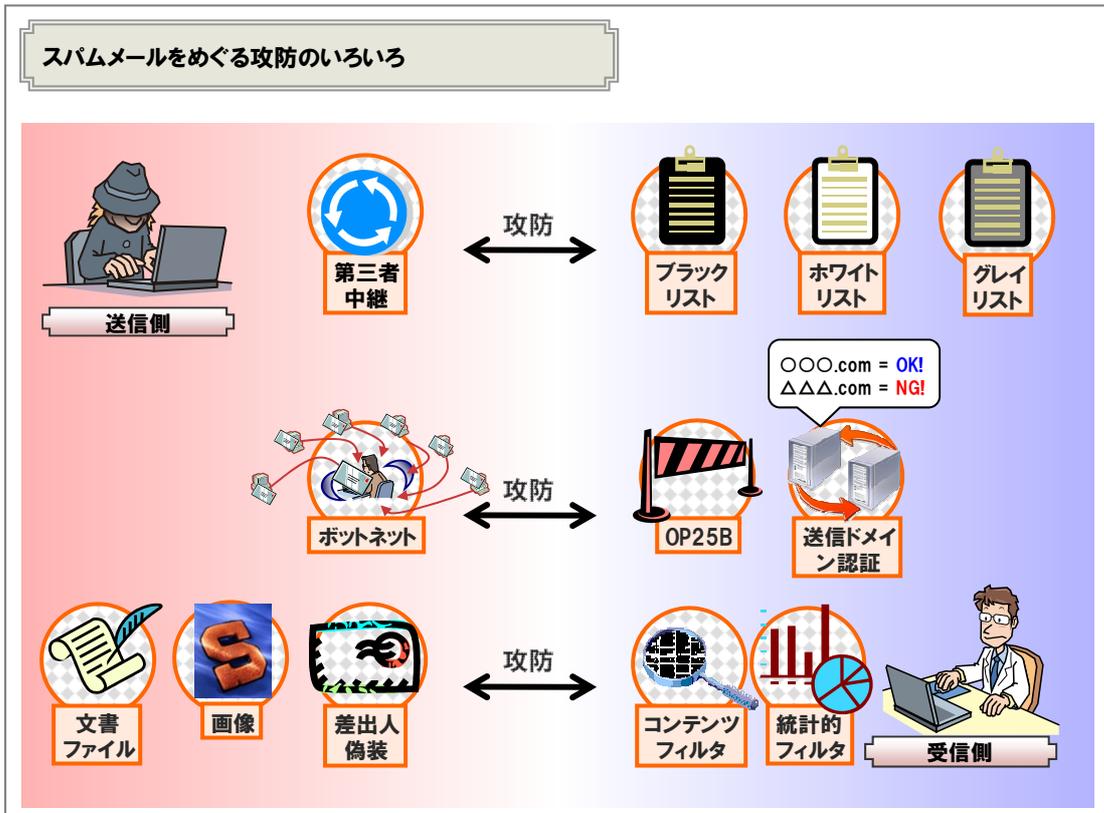
ITmedia:「WEPを一瞬で解読する方法」を研究者グループ発表 プログラムも公開予定

<http://www.itmedia.co.jp/news/articles/0810/14/news020.html>

Impress: WPA-TKIPの暗号を部分的に解読、ドイツの研究者が報告

<http://internet.watch.impress.co.jp/cda/news/2008/11/10/21464.html>

【3位】減らないスパムメール [総合:8位]



スパムメールは迷惑メールとも呼ばれるメールで、広告やフィッシング詐欺、ウイルス感染などの目的で無差別かつ大量に送信され、受信者本来のメールの利用を妨げる。

<問題の概要>

スパムメールによって、本来受け取るべきメールが大量に受信したスパムメールの中に埋もれてしまったり、スパムメール対策の副作用として本来受け取るべきメールが受け取れなかったりするなどの問題がある。また、スパムメールにはウイルスが添付されていることがあり、ウイルスに感染してしまう危険性もある。

スパムメールに対してメール本文の内容を解析してスパムメール判定を行う対策技術が登場しているが、攻撃者はメールに画像や PDF ファイルを添付するなどの手口を使って、スパムメール判定をかいくぐろうとしている。インターネットサービスプロバイダ(ISP)やスパムメール対策ソフトウェアなどでも対策が行われているが、攻撃者はかいくぐるための手法を用意し、いたちごっこになっている。

<問題の経緯>

スパムメールは古くから問題視されている。古いタイプのスパムメールはメールサーバの脆弱性

を悪用して大量に送付したり、メールに添付したウイルスを受信者に実行させることで、スパムメールを送付したりするものがあった。

日本では 2001 年頃より携帯電話のメールに対するスパムメールが特に問題視されるようになった。この背景には、受信者が望んでいないにもかかわらず、受信したメールの通信料を払わなければならない点などが問題になったことが挙げられる。これに対応すべく、2003 年に各携帯電話会社からスパムメール対策の強化が発表され、携帯電話へのスパムメールは激減した。

しかし、パソコン向けメールに対するスパムメールは減ることはなく、2004 年頃より激増した。この原因は、ボットを悪用してスパムメールを送付することが多くなったためと考えられる。2008 年には海外でスパムメールを大量に送付していた業者の通信を ISP で止めることでスパムメールの数が激減したという報道もあった。しかしながらそれ以降、また増加したという報道もあり、完全な対策には至っていないのが現状である。

<被害状況>

海外セキュリティベンダの統計によると、インターネット上に流れている電子メールの 90%以上がスパムメールであるとされている。

<対策方法・注意の啓発>

利用者は、スパムメールに対して返信しない、スパムメール中の URL をクリックしないなど、スパムメールに反応しないことが大切である。スパムメールに反応するとスパムメールの送信業者にスパムメールの効果があると判断され、より多くのスパムメールを送付される場合がある。また、ISP で提供されているスパムメール防止のためのサービスを利用したり、スパムメールフィルタを導入したりすることでスパムメールに触れる機会を減少させることが可能である。

システム管理者は、送信ドメイン認証の技術である SPF(Sender Policy Framework)や SenderID、DomainKeys、メールの暗号化と電子署名に関する規格である S/MIME などの導入を検討したい。これらの技術はスパムメールを直接減らすための技術ではないが、送信元の信頼性向上に寄与するため、長期的にスパムメールを減少させていくことに期待できる。

関連資料

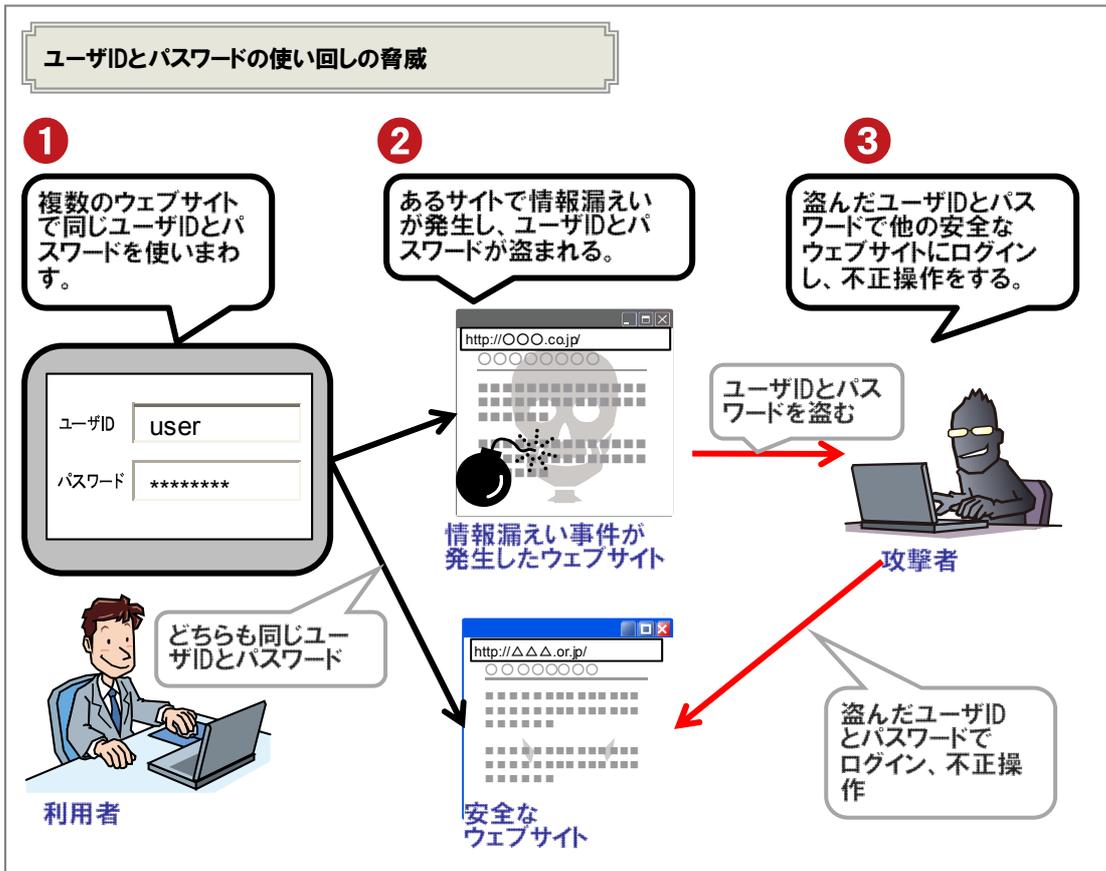
ITmedia: 企業に届く正規メールは1割以下に

<http://www.itmedia.co.jp/enterprise/articles/0901/30/news032.html>

nikkei BP net: 2008年のスパム・メール、悪質業者の摘発にもかかわらず前年比25%増

<http://www.nikkeibp.co.jp/it/article/NEWS/20090127/323513/>

【4位】 ユーザ ID とパスワードの使いまわしによる危険性 [総合:10位]



複数のウェブサイトなどのオンラインサービスに同一のユーザIDやパスワードを設定する、いわゆる使い回しの行為をすると、一つのウェブサイトで情報漏えい事件があった場合、他のウェブサイトのオンラインサービスなどに不正ログインされるなど、漏えいした情報を不正利用される危険性がある。

<問題の概要>

SQLインジェクションなどで漏えいしたユーザID・パスワードが、他ウェブサイトで不正ログインに使われるという事例が報告されている。この問題の背景の一つとして、利用者が本人確認用のユーザIDやパスワードを複数のサイトで使いまわしていることが考えられる。

様々なウェブサイトでユーザIDとパスワードが、本人認証の手段として利用されている。利用者はそのたびにユーザIDとパスワードを設定しなければならない。しかし、利用者はウェブサイトごとにユーザIDとパスワードを管理することが難しいため、複数のウェブサイトで同じパスワードを使いがちになる。サービスを提供する側も、ウェブサイトでユーザIDとパスワードを管理している場合、利用者のユーザIDとパスワードが他のウェブサイトでも同じものが利用されているかは分からない

ため、本問題に対する技術的な対策は困難である。

<問題の経緯>

2008 年以前より同じユーザ ID とパスワードの使い回しをしないようにという注意の呼びかけがあった。しかしながら、実際に使い回しによる被害が発生することによって、利用者がユーザ ID やパスワードの管理することの難しさが表面化したのが 2008 年と言える。2008 年には、複数のオンラインサービスで、ユーザ ID とパスワードを使いまわすことに関する注意喚起が行われた年であった。

<対策方法>

利用者は、パスワード管理ソフトウェアなど適切にパスワードを管理できる仕組みを利用して、ウェブサイト間で同じユーザ ID とパスワードを設定しないように対策をすることが大切である。また、同じユーザ ID とパスワードを設定しない以外にも、安易なパスワードは設定せずに推測されにくいパスワードを設定することも大切である。

システム管理者は利用者がユーザ ID やパスワードの利用方法に注意を呼び掛けるなど、利用者に本問題の注意を呼び掛けることで、セキュリティ意識を啓発することが大切である。同じユーザ ID・パスワードの使い回し以外にも、パスワードの強固さも重要であるため、ウェブサイトのプログラムなどにおいては、ユーザのパスワードを平文のまま保存せず、ハッシュ値のみを保存するという対策が可能だ。こうすることで、データが漏洩しても元のパスワードは漏洩せず、被害を最小限に留めることができる。

本人認証の簡易な管理については、2008 年に大手ウェブサイトが参加を表明しはじめた OpenID の利用なども考えられる。しかしながら、利用者の利便性の一方で OpenID の認証サーバの信頼性などまだまだ課題があるのが現状である。

また、経営者はウェブサイトの脆弱性などにより実際にユーザ ID・パスワードが漏えいしてしまった場合、利用者に漏えいしたことの説明とともに本問題に対する危険性についても説明する必要がある。それによって防げる二次被害もある。

関連資料

日経ネットプラス: ネット利用、パスワード「使い回し」8割超す

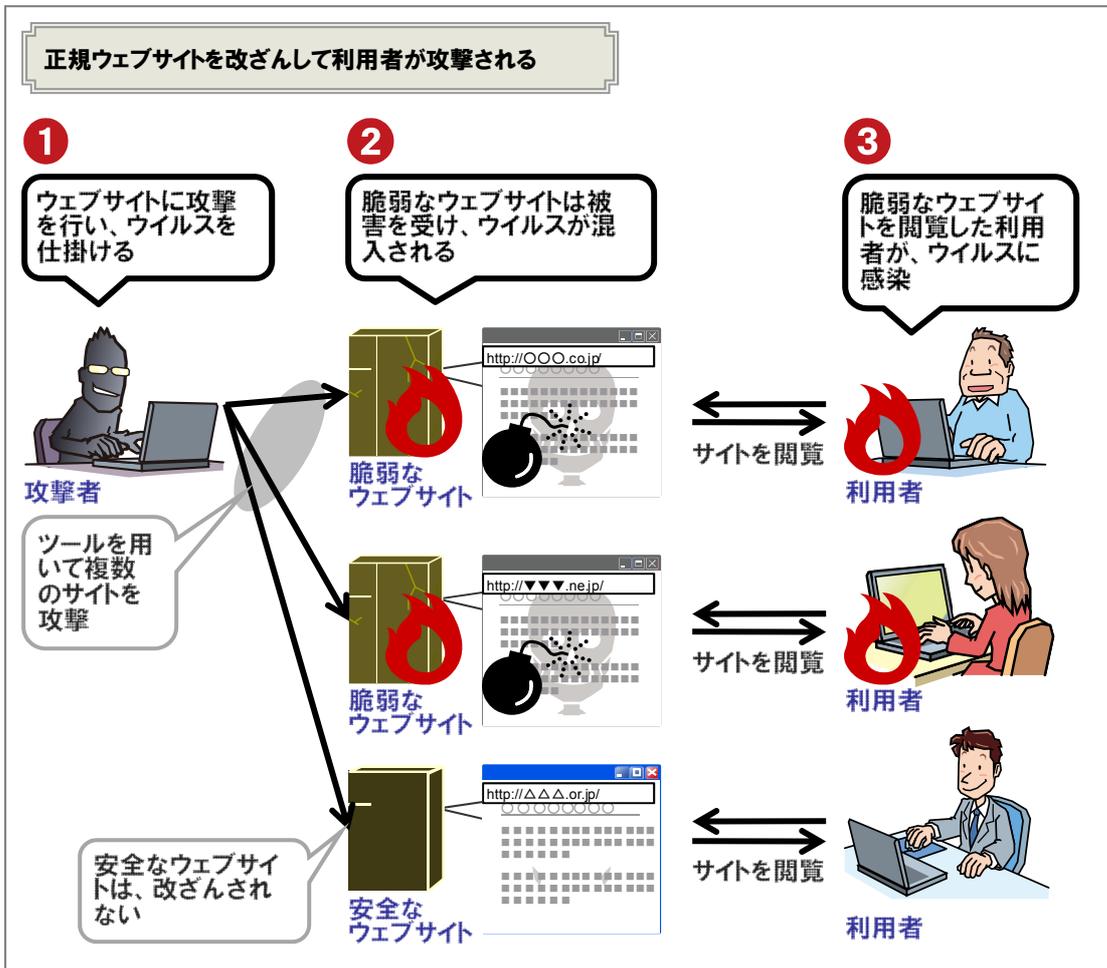
<http://netplus.nikkei.co.jp/netnavi/tozai/toz081021.html>

Yahoo! Japan セキュリティセンター: サイトごとに違うパスワードを!

<http://security.yahoo.co.jp/attention/password/>

■ システム管理者・開発者への脅威

【1位】 正規のウェブサイトを経由した攻撃の猛威 [総合:2位]



2008 年も正規のウェブサイトが改ざんされ、その結果、改ざんされたウェブサイトを開覧した利用者も被害を受ける攻撃が猛威を振るっている。

<問題の概要>

正規のウェブサイトの利用者を狙った攻撃では、攻撃者はまずウェブサイトの改ざんを試みる。ウェブサイトの改ざんには様々な攻撃手法が使われるが、2008 年のウェブサイトの被害傾向として、ウェブアプリケーションにある SQL インジェクションの脆弱性を狙った攻撃(SQL インジェクション攻撃)が多くみられた。SQL インジェクション攻撃はウェブサイトで利用するデータベースを狙う攻撃手法である。ウェブサイトで稼働しているデータベース内部の情報を盗まれたり、改ざんされたり、消去されたりする。その中でも特に、改ざんした後に次の攻撃の起点としてウェブサイトを悪用されてしまうようになった。また、攻撃者はこれらの攻撃を自動的に行うツールを利用していると言われている。

<問題の経緯>

日本では、SQL インジェクション攻撃は 2005 年の SQL インジェクションによる情報漏えいの事件によりニュースなどでも取り上げられるようになった。当初 SQL インジェクションによる被害は、攻撃者によってウェブサイトの持つデータベース上の情報を盗まれるものが主流であった。その攻撃が 2007 年頃より変化し、今日では SQL インジェクション攻撃で正規のウェブサイトの一部にウイルスを仕込むように改ざんされ、そのウェブサイトを閲覧したユーザをウイルスに感染させる攻撃手法が主流となり、被害が拡大している(※詳細は「■利用者への脅威 - 【1 位】多様化するウイルスやボットの感染経路」を参照)。

2007 年は前年と比べて SQL インジェクション攻撃の件数が増加傾向にあったが、2008 年は攻撃件数が加速度的に増加していることが、国内のセキュリティベンダの観測などで確認された。更に利用者が同じユーザ ID やパスワードを複数で使いまわしていたため、他のウェブサービスを不正利用された事例が表面化した(※詳細は、■利用者への脅威 - 【4 位】ユーザ ID とパスワードの使いまわしによる危険性を参照)。

<対策方法>

SQL インジェクション攻撃が増加している背景の一つとして、データベースと連携したウェブサイトが一般的となっている一方、SQL インジェクション対策が不十分であるウェブサイトが依然として減っていないことが挙げられる。

システム管理者・ウェブアプリケーション開発者は、ウェブサイトでデータベースを利用する場合、ウェブアプリケーションを設計・構築する際に SQL インジェクション対策を行わなければならない。IPA が公開している「安全なウェブサイトの作り方」などの資料を参考にウェブサイトの安全性向上に取り組む必要がある。また、ウェブサイトにおける脆弱性検査・システムの改修計画も検討する必要がある。

関連資料

ラック:改ざんされたWebサイト閲覧による組織内へのボット潜入被害について

<http://www.lac.co.jp/news/press20081222.html>

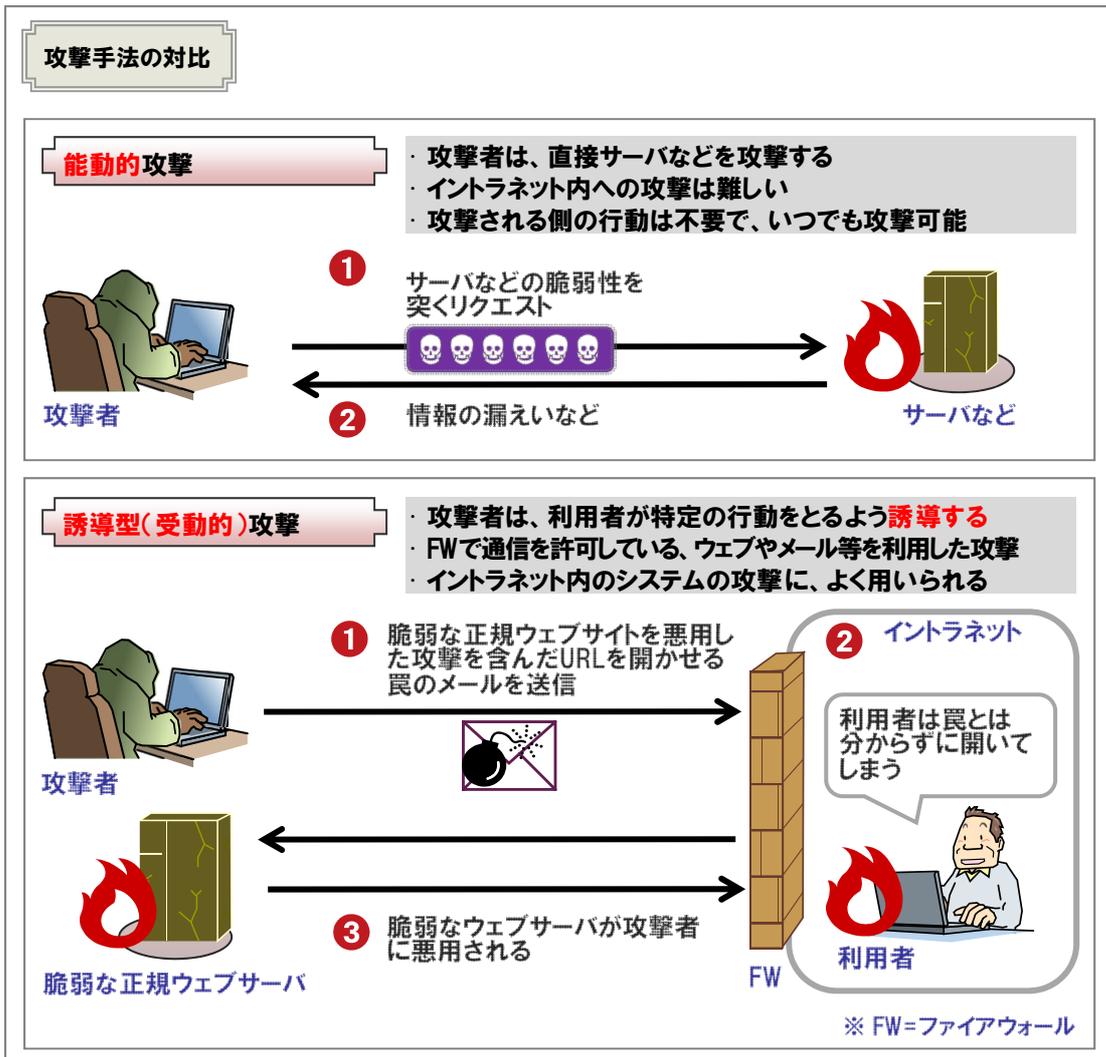
NRI Secure Technologies: セキュリティ診断結果の傾向分析レポート2008年版を公開

<http://www.nri-secure.co.jp/news/2008/0728.html>

IPA: 「安全なウェブサイトの作り方 改訂第3版」を公開

<http://www.ipa.go.jp/security/vuln/websecurity.html>

【2位】誘導型攻撃の顕在化 [総合:7位]



脆弱な正規ウェブサーバが狙われて正規ウェブサイト上に偽りのページが表示され、そのページに利用者が誘導される形(誘導型攻撃¹)の被害が増加している。また、脆弱なソフトウェア製品を狙った誘導型攻撃も増加している。

<問題の概要>

誘導型攻撃は、利用者を脆弱なウェブサイトや罠のメールを閲覧させることで成立する種類の攻撃のことである。誘導型攻撃の代表例としては、クロスサイト・スクリプティングの脆弱性やブラウザの脆弱性を利用した攻撃、標的型攻撃などが挙げられる(※詳細は、■組織への脅威 - 【2位】巧妙化する標的型攻撃を参照)。

クロスサイト・スクリプティングは、ウェブアプリケーションの脆弱性を悪用して、ウェブサイトの利用者を狙う攻撃手法の一つである。ウェブサイトを閲覧した利用者のブラウザ内で悪意あるスクリ

¹ このような攻撃は、受動的攻撃(Passive Attack)とも呼ばれている。

プトが実行され、フィッシング詐欺や、情報の漏えいなどの被害が引き起こされる。クロスサイト・スクリプティングの対策が行き届いていないウェブサイトは多く、IPA に多数の脆弱なウェブサイトについての情報が届出られている。

ブラウザの脆弱性を利用する誘導型攻撃では、悪意あるウェブサイトにアクセスするだけで利用者のコンピュータがウイルスに感染するなどの危険性があるものである。

誘導型攻撃の特徴は、企業内において一般的に利用可能なネットワークを悪用する点にある。背景には攻撃者が直接攻撃できる対象が限られてきていることが挙げられる。近年は企業でファイアウォールの導入が当たり前に行われるようになった。また、能動的に攻撃される危険性のあるソフトウェアでは、悪用される脆弱性の種類が少なくなった。このような背景から誘導型攻撃が増加していると考えられる。

<問題の経緯>

誘導型攻撃の脅威については古くから存在していた。クロスサイト・スクリプティングの脆弱性は2000年2月にCERT/CCとMicrosoft社の情報によって広く知られるものとなった。また、ブラウザの脆弱性についても数多く発見され、悪用されているものもある。しかし、当時は能動的攻撃の問題が重要視されており、誘導型攻撃はほとんど理解されていなかった。しかし、標的型攻撃が現れたり、ブラウザの脆弱性を利用した攻撃も行われたり、徐々に誘導型攻撃に関する脅威が認識されるようになり、近年では深刻な問題の一つとして認識されている。

<対策状況>

2008年12月末までに早期警戒パートナーシップに基づいてIPAへ届出られたクロスサイト・スクリプティングの脆弱性に関する届出は1,024件ある。このうち、1月末までに修正完了などで取り扱い終了となった件数は314件で、まだ710件が取り扱い中の状況である。

<対策方法>

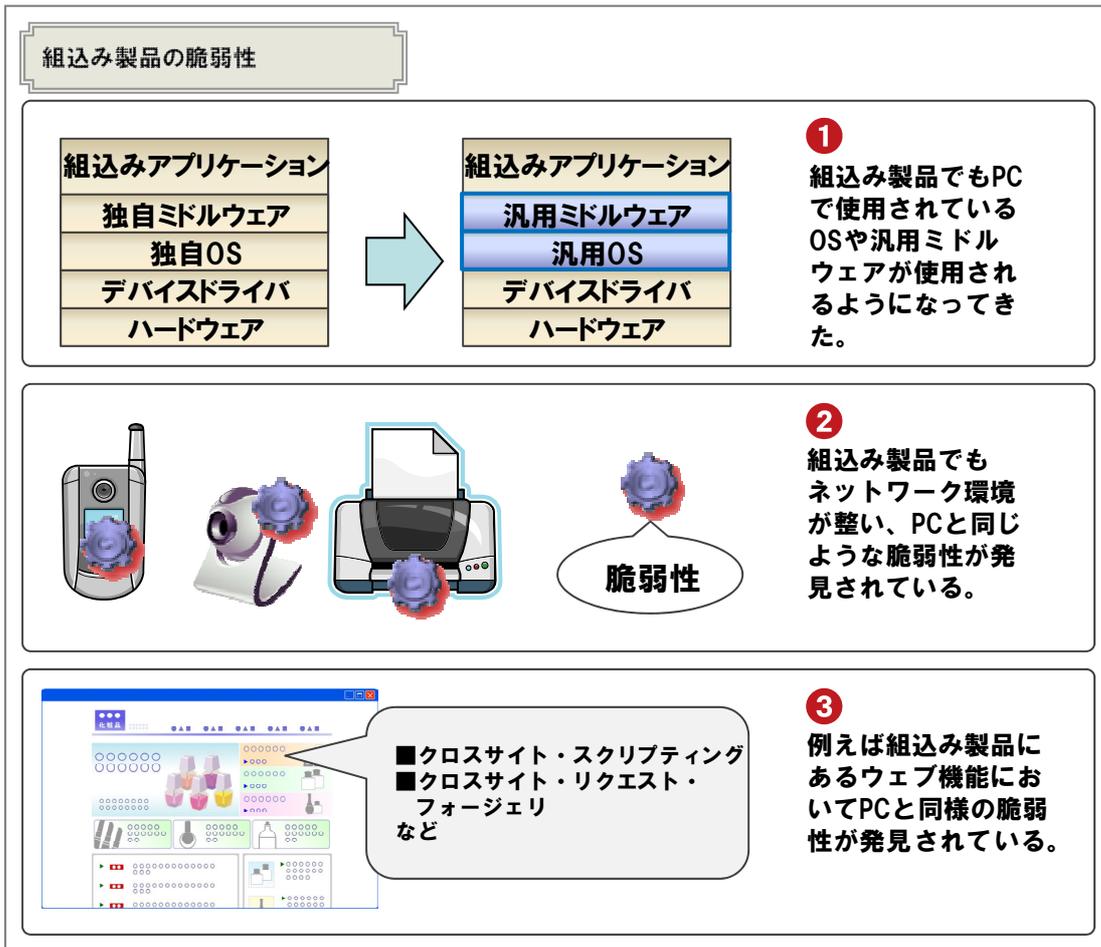
システム管理者・ウェブアプリケーション開発者は、誘導型攻撃の原因となるクロスサイト・スクリプティング等の脆弱性に留意する必要がある。利用者では根本的な対策ができない問題であるため、開発者が対策を行うべき問題である。設計の段階から対策を検討して、漏れが無いようにすべきである。IPAが公開している「安全なウェブサイトの作り方」などの資料を参考に対策する必要がある。

関連資料

IPA: 脆弱性関連情報に関する届出状況（プレスリリース）

<http://www.ipa.go.jp/security/vuln/report/press.html>

【3 位】 組み込み製品に潜む脆弱性 [総合:9 位]



組み込み製品でもネットワーク環境が整いつつあり、また OS やミドルウェアなどソフトウェアの汎用化が進んでいる。そのため、組み込み製品に脆弱性があった場合、攻撃に悪用され易くなってきていると言える。

<問題の概要>

家電、携帯電話、自動車、プリンタなどの組み込み製品が普及している。また、情報通信技術の発展により通信機能の搭載が容易になっており、いつでもどこでもネットワークを利用できる環境になりつつある。

このような組み込み製品に脆弱性があり、それを悪用されてしまった場合、従来のインターネットに接続して使用するコンピュータソフトウェアと同様に情報を盗まれたり、組み込み製品そのものを不正に操作されたりする被害が想定される。特に近年は組み込み製品の OS やミドルウェアが汎用化され、インターネットを利用できる製品が増えてきている。そのため、従来のインターネットに接続して使用するコンピュータソフトウェアと同様の問題に直面しつつある。

2008年には、日本で普及している携帯電話に脆弱性が発見されたり、IP電話に無言電話がかかってきたりする攻撃に関する注意喚起があった。JVN(Japan Vulnerability Notes)でも日本で普及している携帯電話・携帯音楽プレイヤー、小型端末における脆弱性を公表した。また、インターネットに接続できる組込み製品にはウェブインターフェースの機能が用意されていることがある。これらの機能ではウェブアプリケーションの脆弱性が存在する可能性がある。2008年にJVNで公表された組込み機器に関連する脆弱性8件の内、4件がウェブインターフェースの機能における脆弱性であった。組込み機器のウェブインターフェースにおいてもウェブアプリケーションと同様に対策を進める必要がある。

<問題の経緯>

数年前までは、組込み製品はインターネットに接続する機能が少なかったため、アップデート機能が存在していないものが多かった。しかし、最近の組込み製品の内、特にインターネットに接続するものにはアップデート機能を搭載している製品も多くなってきており、仮に脆弱性が見つかった場合でも利用者がアップデートを行うことが可能になっている。

<対策方法>

開発者はネットワークに接続する組込み製品に関しては脆弱性を作りこまないように、設計の段階から注意を払う必要がある。万が一脆弱性が見つかった場合でも、利用者が分かりやすく安全にアップデートできるための仕組みを用意することが望ましい。組込み製品においてもセキュリティを意識した開発を行うべきである。IPAが公開している「安全なウェブサイトの作り方」などの資料を参考にウェブアプリケーションの安全性向上に取り組む必要がある。

関連資料

IPA: 複数の組込み機器の組み合わせに関するセキュリティ調査報告書

<http://www.ipa.go.jp/security/fy19/reports/embedded/>

IPA: 複数のアイ・オー・データ製無線 LAN ルータにおけるセキュリティ上の弱点(脆弱性)の注意喚起

http://www.ipa.go.jp/security/vuln/documents/2008/200803_iodata.html

IPA: 複数のヤマハルーター製品におけるセキュリティ上の弱点(脆弱性)の注意喚起

http://www.ipa.go.jp/security/vuln/documents/2008/200801_Yamaha.html

【付録 1】 10 大脅威関係表

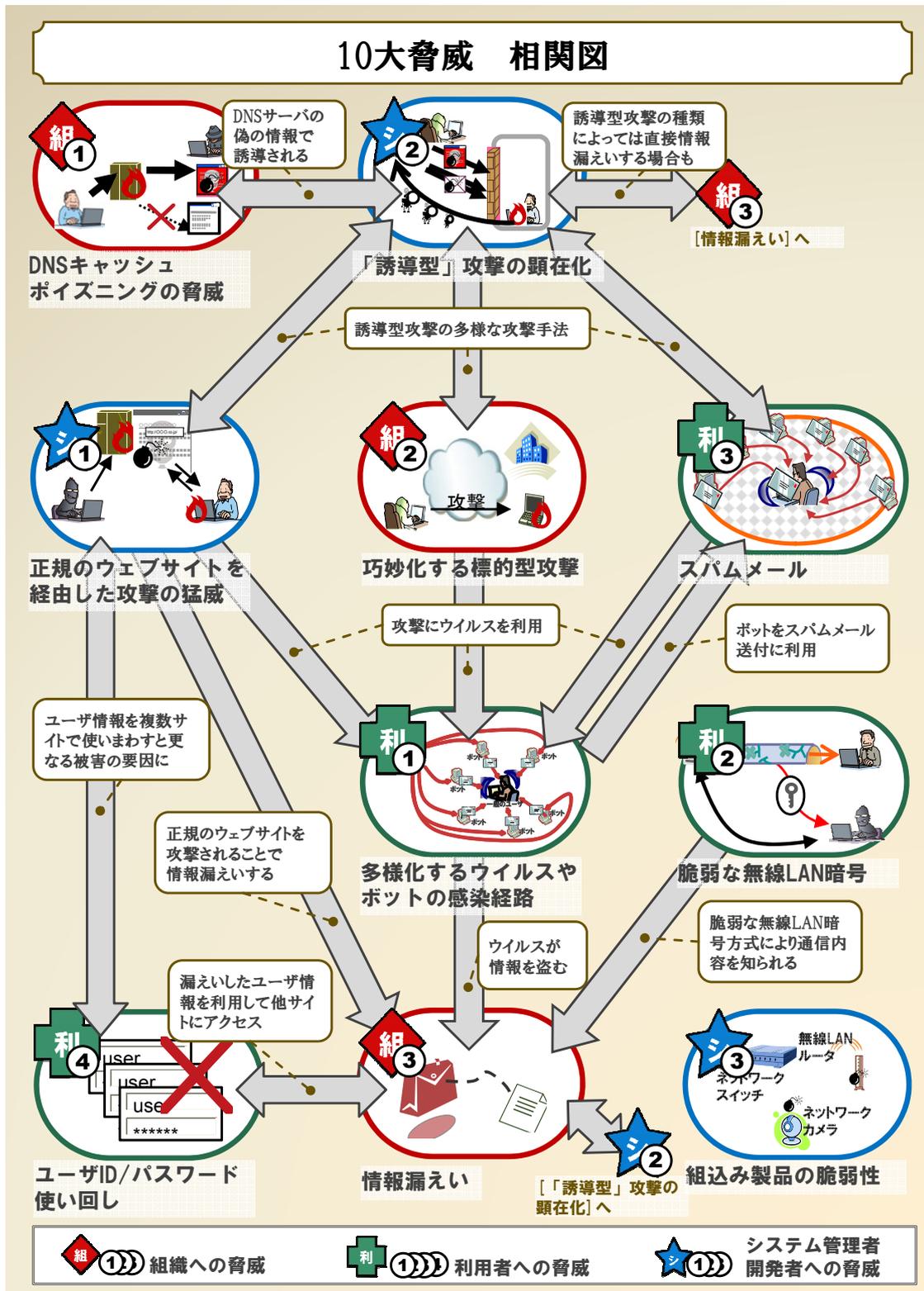
付表 1. 10 大脅威 対策が必要な対象者と総合順位

10 大脅威		対策が必要な主な対象者				総合 順位 [白書 2009]	前回 順位 [白書 2008]
		経営者	利用者	システム 管理者	開発者		
■組織への脅威							
1 位	DNS キャッシュポイズニングの脅威			◎		1 位 ↑	—
2 位	巧妙化する標的型攻撃	○		◎		3 位 ↑	4 位
3 位	恒常化する情報漏えい	◎		○		5 位	3 位
■利用者への脅威							
1 位	多様化するウイルスやボットの感染経路		◎	○		4 位 ↑	6 位
2 位	脆弱な無線 LAN 暗号方式における脅威		◎	○	○	6 位 ↑	—
3 位	減らないスパムメール		◎	○		8 位 ↑	9 位
4 位	ユーザ ID とパスワードの使いまわしによる危険性	○	◎	○		10 位 ↑	—
■システム管理者・開発者への脅威							
1 位	正規のウェブサイトを経由した攻撃の猛威	○		◎	○	2 位	2 位
2 位	誘導型攻撃の顕在化			○	◎	7 位	1 位
3 位	組込み製品に潜む脆弱性				◎	9 位 ↑	10 位

◎:特に対策が必要な対象者 ○:対策を考慮する必要がある対象者 ↑:昨年より順位が上がったもの

付表 1 で、10 大脅威における対策が必要な主な対象者と総合順位を表す。今年、新規に取り上げられた脅威としては、「DNS キャッシュポイズニングの脅威」や「脆弱な無線 LAN 暗号方式における脅威」などがある。また、総合順位では昨年の 10 大脅威より順位が上がったものとして、「多様化するウイルスやボットの感染経路」や「巧妙化する標的型攻撃」などがある。

【付録2】 10大脅威 相関図



付図 1. 10大脅威の主要な関係

【付録 3】 参考資料

[組織向け]

- (参考資料 1) ソーシャル・エンジニアリングを巧みに利用した攻撃の分析と対策、2009 年 2 月
<http://www.ipa.go.jp/security/vuln/report/newthreat200902.html>
- (参考資料 2) 近年の標的型攻撃に関する調査研究－調査報告書－、2008 年 3 月
<http://www.ipa.go.jp/security/fy19/reports/sequential/>
- (参考資料 3) 知っていますか？脆弱性(ぜいじゃくせい)、2007 年 7 月
http://www.ipa.go.jp/security/vuln/vuln_contents/
- (参考資料 4) 情報漏えい発生時の対応ポイント集、2007 年 9 月
<http://www.ipa.go.jp/security/awareness/johorouei/>

[運営者向け]

- (参考資料 5) 安全なウェブサイト運営入門、2008 年 6 月
<http://www.ipa.go.jp/security/vuln/7incidents/>
- (参考資料 6) ウェブサイト運営者のための脆弱性対応ガイド、2008 年 2 月
http://www.ipa.go.jp/security/fy19/reports/vuln_handling/
- (参考資料 7) 脆弱性対策情報ポータルサイト JVN、<http://jvn.jp/>
- (参考資料 8) 脆弱性対策情報データベース JVN iPedia、<http://jvndb.jvn.jp/>
- (参考資料 9) 脆弱性対策情報収集ツール MyJVN、<http://jvndb.jvn.jp/apis/myjvn/>
- (参考資料 10) SQL インジェクション検出ツール iLogScanner、2008 年 4 月
<http://www.ipa.go.jp/security/vuln/iLogScanner/index.html>
- (参考資料 11) DNS キャッシュポイズニング対策、2009 年 1 月
http://www.ipa.go.jp/security/vuln/DNS_security.html

[開発者向け]

- (参考資料 12) セキュアプログラミング講座
<http://www.ipa.go.jp/security/awareness/vendor/programmingv2/>
- (参考資料 13) 安全なウェブサイトの作り方 改訂第 3 版、2008 年 3 月
<http://www.ipa.go.jp/security/vuln/websecurity.html>
- (参考資料 14) TCP/IP に係る既知の脆弱性に関する調査報告書・検証ツール、2009 年 1 月
http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html
http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html
- (参考資料 15) SIP に係る既知の脆弱性に関する調査報告書・検証ツール、2009 年 4 月
http://www.ipa.go.jp/security/vuln/vuln_SIP.html
http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html
- (参考資料 16) ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル、2007 年 5 月
http://www.ipa.go.jp/security/fy18/reports/vuln_handling/
- (参考資料 17) 自動車と情報家電の組込みシステムのセキュリティに関する調査報告書、2009 年 3 月
<http://www.ipa.go.jp/security/fy20/reports/embedded/index.html>

第Ⅱ部 執筆協力者

情報セキュリティ検討会 構成メンバー

氏名	所属	氏名	所属
渡部 章	(株)アークン	星澤 裕二	(株)セキュアブレイン
石田 淳一	(株)アールジェイ	山村 元昭	(株)セキュアブレイン
加藤 雅彦	(株)アイアイジェイ テクノロジー	正木 健介	セコムトラストシステムズ(株)
根岸 征史	(株)アイアイジェイ テクノロジー	澤永 敏郎	ソースネクスト(株)
高橋 康敏	(株)アイアイジェイ テクノロジー	青谷 征夫	ソースネクスト(株)
齋藤 衛	(株)インターネットイニシアティブ	百瀬 昌幸	(財)地方自治情報センター (LASDEC)
徳丸 浩	HASH コンサルティング(株)	小橋 一夫	(社)電子情報技術産業協会 (JEITA)
三輪 信雄	S&J コンサルティング(株)	渡辺 淳	(株)デンソーウェーブ
小林 克巳	NRI セキュアテクノロジーズ(株)	吉松 健三	(株)東芝
佐藤 利幸	NTT コミュニケーションズ(株)	小島 健司	東芝ソリューション(株)
西尾 秀一	(株)NTT データ	小屋 晋吾	トレンドマイクロ(株)
池田 和生	(株)NTT データ	須川 賢洋	新潟大学
入宮 貞一	(株)NTT データ	徳田 敏文	日本アイ・ビー・エム(株)
井上 克至	NTTデータ・セキュリティ(株)	井上 博文	日本アイ・ビー・エム(株)
岸本 博之	(財)金融情報システムセンター (FISC)	木村 道弘	日本電気(株)
井土 和志	経済産業省	谷川 哲司	日本電気(株)
清水 友晴	経済産業省	秋山 卓司	(中)日本電子認証協議会 (JCAF)
秋貞 幸雄	経済産業省	長島 雅夫	日本電信電話(株)
西村 高志	(社)コンピュータソフトウェア協会 (CSAJ)	杉浦 芳樹	日本電信電話(株)
鈴木 啓紹	(社)コンピュータソフトウェア協会 (CSAJ)	安部 哲哉	日本電信電話(株)
高木 浩光	(独)産業技術総合研究所	渡瀬 順平	日本電信電話(株)
大岩 寛	(独)産業技術総合研究所	雨宮 俊一	日本電信電話(株)
宮地 利雄	(中)JPCERT コーディネーション センター(JPCERT/CC)	やすだ なお	特定非営利活動法人日本ネット ワークセキュリティ協会(JNSA)
伊藤 友里恵	(中)JPCERT コーディネーション センター(JPCERT/CC)	榎本 司	日本ヒューレット・パッカー(株)
宮崎 清隆	(中)JPCERT コーディネーション センター(JPCERT/CC)	西垣 直美	日本ヒューレット・パッカー(株)
古田 洋久	(中)JPCERT コーディネーション センター(JPCERT/CC)	佐藤 直之	日本ベリサイン(株)
井上 信吾	(中)JPCERT コーディネーション センター(JPCERT/CC)	杉岡 弘毅	(株)ネクストジェン
林 薫	(株)シマンテック	山田 陽介	ネットエージェント(株)
福森 大喜	(株)セキュアスカイ・テクノロ ジー	大野 雅子	ネットエージェント(株)
		水越 一郎	東日本電信電話(株)

第Ⅱ部 10 大脅威 攻撃手法の『多様化』が進む

氏名	所属	氏名	所属
太田 良典	(株)ビジネス・アーキテクツ	志田 智	(株)ユビテック
吉野 友人	(株)ビジネス・アーキテクツ	矢野 ミチル	(株)ユビテック
本川 祐治	(株)日立情報システムズ	遠山 真	(株)ユビテック
田山 晴康	(株)日立製作所	福本 佳成	楽天(株)
寺田 真敏	(株)日立製作所	岩井 博樹	(株)ラック
梅木 久志	(株)日立製作所	山崎 圭吾	(株)ラック
藤原 将志	(株)日立製作所	柳澤 伸幸	(株)ラック
鵜飼 裕司	(株)フォティーンフォティ技術 研究所	川口 洋	(株)ラック
金居 良治	(株)フォティーンフォティ技術 研究所	伊藤 耕介	(株)ラック
森 玄理	富士通(株)	中田 邦彦	(株)ルネサス テクノロジ
富士原 裕文	富士通(株)	山田 安秀	
木村 秀年	富士通(株)	小森 聡	
草間 正	富士通(株)	小松 文子	
望月 大光	(株)富士通ソフトウェアテクノ ロジーズ	杉浦 昌	
佐藤 友治	(株)ブロードバンドセキュリティ	小門 寿明	
高橋 正和	マイクロソフト(株)	木邑 実	
加藤 義宏	マカフィー(株)	加賀谷 伸一郎	
国分 裕	三井物産セキュアディレクショ ン(株)	花村 憲一	
後藤 久	三井物産セキュアディレクショ ン(株)	宮本 一弘	
青木 歩	三井物産セキュアディレクショ ン(株)	小林 偉昭	
村瀬 一郎	(株)三菱総合研究所	中野 学	
川口 修司	(株)三菱総合研究所	渡辺 貴仁	
村野 正泰	(株)三菱総合研究所	山岸 正	
藤井 誠司	三菱電機(株)	園田 道夫	
		若居 和直	
		永安 佑希允	
		相馬 基邦	
		大谷 槇吾	

※独立行政法人情報処理推進機構の職員(執筆当時)については所属組織名を省略しました。

情報セキュリティ白書 2009 第Ⅱ部

10 大脅威 攻撃手法の『多様化』が進む

2009年 3月 24日 第1刷発行

2009年 5月 25日 第2刷発行

[編集] 情報セキュリティ検討会

[事務局・発行] 独立行政法人情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコートセンターオフィス 16 階

<http://www.ipa.go.jp/>

情報セキュリティに関する届出について

IPA セキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出を受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。

URL: <http://www.ipa.go.jp/security/todoke/>

コンピュータウイルス情報

コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合に届け出てください。

不正アクセス情報

ネットワーク(インターネット、LAN、WAN、パソコン通信など)に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

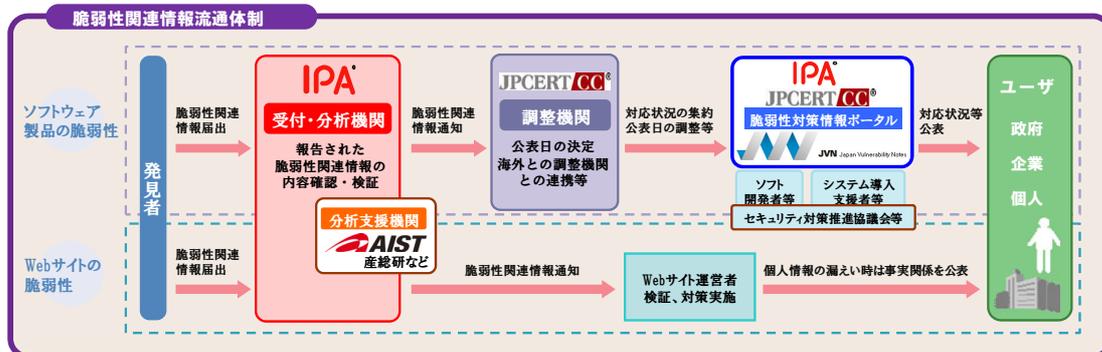
ソフトウェア製品脆弱性関連情報

OSやブラウザ等のクライアント上のソフトウェア、ウェブサーバ等のサーバ上のソフトウェア、プリンタやICカード等のソフトウェアを組み込んだハードウェア等に対する脆弱性を見つけた場合に届け出てください。

ウェブアプリケーション脆弱性関連情報

インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムに対する脆弱性を見つけた場合に届け出てください。

脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※IPA: 独立行政法人 情報処理推進機構、JPCERT/CC: 有限責任中間法人 JPCERT コーディネーションセンター、産総研: 独立行政法人 産業技術総合研究所

IPA[®]

独立行政法人 情報処理推進機構

〒113-6591

東京都文京区本駒込二丁目28番8号

文京グリーンコートセンターオフィス16階

<http://www.ipa.go.jp>

セキュリティセンター

TEL: 03-5978-7527 FAX: 03-5978-7518

<http://www.ipa.go.jp/security/>