コンピュータ・セキュリティ

～2004 年の傾向と今後の対策～

安 全 な イ ン タ ー ネ ッ ト の 利 用 を 目 指 し て

2005 年 3 月 31 日

コンピュータ・セキュリティ検討会

要約

2004 年も先年までと同様にソフトウェアのセキュリティ上の問題が数多く発見され、これらの問題が悪用されました。悪用される可能性があるソフトウェアのセキュリティ上の問題のことを「脆弱性(Vulnerability)」と呼びます。

脆弱性の悪用だけが被害の原因となるわけではありません。従来行われる攻撃は脆弱性自体を攻撃対象としたものが目立ちましたが、2004 年の傾向として、騙りや詐欺など、ソフトウェアを利用する人を対象とした攻撃がより増加しつつあります。特に、「ボット」「コンピュータウイルス」「フィッシング詐欺」などの、一般の利用者に対する直接的な攻撃が増加している傾向が見られました。

また、脆弱性の公表から脆弱性を悪用した攻撃までの時間差が短くなったため、対策方法が十分検討される前に攻撃手法が広まってしまい、一般の利用者が対策を行う前に被害を受けてしまうことが増えました。

2004 年の注目すべき主な脅威を説明します。

- 「ボット」
  ボットは、コンピュータに潜伏して組織的な攻撃を行うプログラムです。秘かに数多くのコンピュータの裏側で動き続けてボット同士のネットワークを作り、外部からの指令を待って一斉に組織化された攻撃を開始します。ボットの問題は、侵入されても悪用が開始されるまではなかなか気が付きにくいことと、組織的な攻撃を行うために大規模な被害を引き起こしやすいことです。
- 「コンピュータウイルス」
  流行したウイルスの大半を、数種類のウイルスとその亜種が占めました。亜種の出現する速度がはやく、次々と新しい機能を備えた亜種が出てきました。そのため、ワクチンソフトを利用している場合でも、ウイルス定義ファイルの配布が間に合わずに感染する危険性があります。
- 「フィッシング詐欺」
  偽のウェブサイトで人を騙し、情報を盗み取る事件が国内でも発見されました。メールで偽のサイトに誘導されて、大手ウェブサイトで利用するためのアカウント情報やパスワードを盗まれたり、クレジットカード番号を盗まれたりする危険性があります。
- 「個人情報の漏えい」
  ウェブサイトの脆弱性を狙った攻撃や情報媒体の紛失による、個人情報や企業情報の漏えいが数多くありました。2005 年 4 月からは個人情報保護法が全面施行されます。いかにして情報漏えいを起こさないか、情報漏えいを起こしてしまった場合にどのように対応するかが、個人情報を取り扱う組織として問われています。

■ 「複数製品にまたがる脆弱性の脅威」
多くの製品に影響する脆弱性がいくつも公開されました。中でもインターネットの通信に利用するプロトコルの脆弱性は、それを利用する全ての製品に影響する可能性がありました。また、画像形式等に関わる脆弱性は、多くの製品に類似の脆弱性が発見されました。

■ 「ウェブサイトの改ざん」
ウェブサイトが改ざんされると、セキュリティ管理が甘いと見なされ、運営主体の信用や責任問題となる危険性があります。改ざんされたウェブサイトの大部分は、脆弱性のあるソフトウェアを利用し続けていたことが原因で、改ざんされてしまいました。

これらの脅威への対策として、以下に最も基本的なことを示します。

■ 「ソフトウェアを安全に保つ」
バージョンアップやセキュリティパッチの適用などによりソフトウェアの脆弱性を修正することで、被害を受ける可能性を減らせます。ソフトウェアによっては、自動でセキュリティパッチの適用や、バージョンアップを行えるものがあります。

■ 「信頼できないソフトウェアやデータを使わない」
P2P ネットワークやウェブサイトから入手したソフトウェアやデータには、ウイルスやボットが付属していることがあります。ソフトウェアを導入したり、データを利用する際は、安全性を検討した上で利用してください。

■ 「対策ソフトウェアの導入」
ウイルスに対するワクチンソフトのような、特定の脅威に対する対策ソフトウェアを利用するという方法により、安全性を高められます。ワクチンソフトやパーソナルファイアウォール製品を利用することは、ウイルスやネットワークスキャンに対する効果的な対策となります。

■ 「利用者自身の対策」
利用者の行動自体が最大のセキュリティ対策となります。例えば、不審なメールを開かない、不審なウェブサイトを信用しないといった対策をすることで、ウイルスやフィッシング詐欺の被害にあう危険性を減らせます。

セキュリティは一つの対策、一時の対策だけで万全となるものではありません。物理的、ソフトウェア的、そして利用者自身の注意による対策を施してリスクを減らすことが重要となります。本資料を、今後のセキュリティ対策の参考としていただければ幸いです。

目次

1. はじめに

本資料は、「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、JPCERT コーディネーションセンター、電子情報技術産業協会、日本パーソナルコンピュータソフトウエア協会、情報サービス産業協会、日本ネットワークセキュリティ協会及び情報処理推進機構の関係者のほか、情報セキュリティ分野における研究者、実務担当者等で構成された「コンピュータ・セキュリティ検討会」における検討の成果として公表するものです。

「コンピュータ・セキュリティ検討会」では、一般利用者や管理者に今後のセキュリティ対策の参考にしていただくために、2004 年のセキュリティ状況を振りかえり、代表的なセキュリティ上の脅威や対策方法を検討いたしました。

2004 年も先年までと同様にソフトウェアのセキュリティ上の問題が数多く発見され、これらの問題が悪用されました。悪用される可能性があるソフトウェアのセキュリティ上の問題のことを「**脆弱性(Vulnerability)**」と呼びます。

脆弱性の悪用だけが被害の原因となるわけではありません。ほとんどの被害は、ソフトウェアを利用する人と、脆弱性の両方が攻撃対象とされた結果、引き起こされています。

本資料では、2004 年のセキュリティ上の代表的な脅威や対策方法を、一般の利用者向けと管理者向けに分けて説明します。一般の利用者向けとしてボットやコンピュータウイルス、フィッシング詐欺の問題を、管理者向けとして情報漏えいや複数の製品にわたる脆弱性、ウェブサイト改ざんの問題を取り上げています。2004 年のセキュリティ上の主な脅威を振り返り、今後の対策の参考にしていただければ幸いです。

2. 2004 年の傾向と対策 (利用者向け)

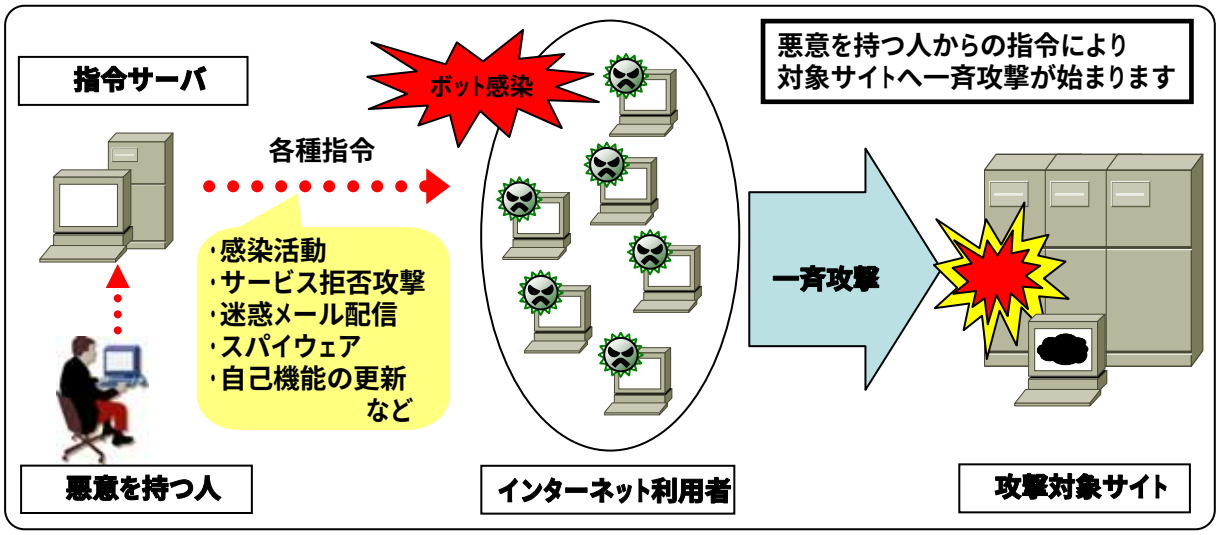
本章では、家庭や企業内部においてインターネットを利用する、一般的な利用者向けの情報を取り扱います。

2.1 2004 年の傾向

従来の攻撃は、ソフトウェア自体や利用者のコンピュータに蓄積されたデータを破壊するアプローチが目立ちましたが、徐々に利用者のコンピュータを第三者への攻撃の踏台として悪用したり、利用者のコンピュータに蓄積されたデータを盗み出すアプローチが目立つようになってきました。

特に、被害がなかなか顕在化しにくい「ボット」の脅威や、各種メディアを賑わせた「フィッシング詐欺」の脅威などは、2004 年になってから急激に目立ちはじめました。もちろん「コンピュータウイルス(ウイルス)」も先年までと同様に大きな脅威となっています。

2.1.1 ボットの脅威



ボット(bot)は、ネットワークを通じて感染し、外部からの指令に従って一斉に他者への攻撃を開始する、不正なプログラムの一種です。同じようにネットワークを通じて感染するウイルスとは違い、感染に成功してコンピュータへ侵入したボットは、ボットネット(botnet)と呼ばれる独自のネットワークに自動的に参加しようとします。

ボットネットには数多くのコンピュータが参加しており、中には数千、数万台にも及ぶものが発見されています。ボットネットに参加しているコンピュータの数は日々変化しています。国内でも実際に数多くのコンピュータがボットに感染し、ボットネットに参加していることが確認されています。

ボットは、侵入されてもなかなか気がつきにくいという性質があります。ボットの目的は侵入対象へ

害を与えることではなく、外部からの指令を受けるまでは極力発見されないように潜み、指令によって一斉に攻撃することだからです。

侵入されたコンピュータは、第三者への攻撃の踏台として利用されます。そのため、侵入されたコンピュータの持ち主は、直接攻撃の指令をしていなくても加害者となり、場合によっては被害者に訴訟を起こされる可能性もあります。

ボットの侵入する経路は様々です。ウイルスと同様に自ら他のコンピュータを攻撃して感染したり、ウェブサイトやP2Pネットワーク[1]等で配布されるソフトウェアに同梱されたり、他のウイルスにより頒布されたりするなど様々な手法が用いられます。

そのため、ボットの侵入を防ぐための直接的な対策手法はありません。しかし、後に述べるウイルス対策やセキュリティパッチの適用などの、基本的な対策を継続的に行うことで、ボットの侵入を防ぐことができます。

どんなボットが流行？

2004 年はボットの中でも、AGOBOT、SDBOT、RBOT といった自己増殖機能、感染機能を持ち合わせてたボットが多数の亜種とともに作成されました。ボットの中には、1000 以上の亜種が確認された種類も存在するそうです。

ボットには様々な種類があり、それぞれが複数の機能を備えています。その中から、多くのボットが備えている機能を以下に示します。

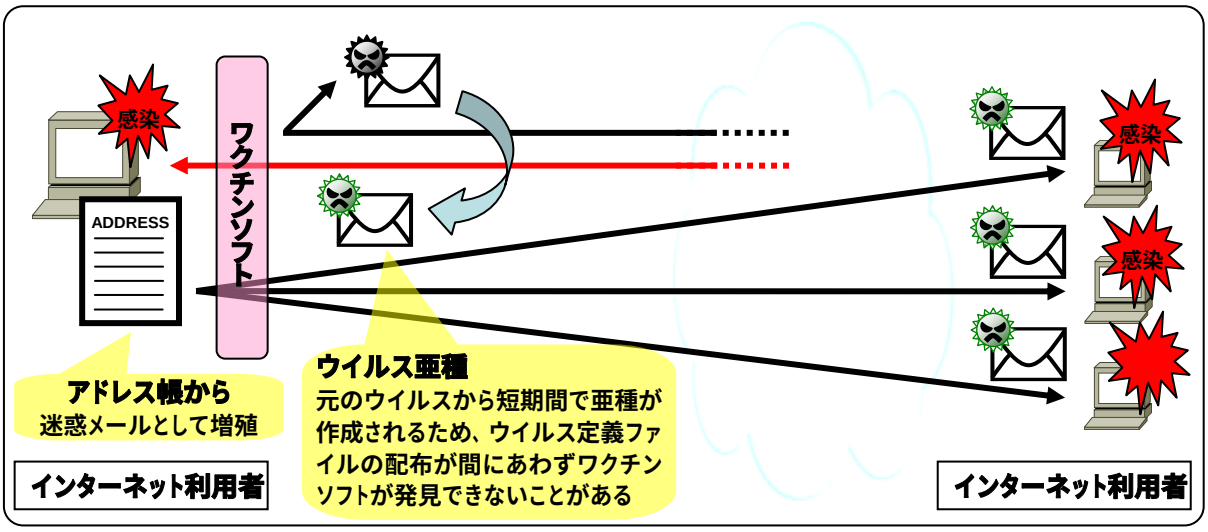
感染:	ソフトウェアの脆弱性を利用して他のコンピュータを攻撃、感染する
サービス拒否攻撃:	多量の通信を一箇所に集中して攻撃する
迷惑メール配信:	多量の宣伝メールを一斉に送信する
情報収集:	感染したコンピュータ内の情報を盗み、送信する
自己機能の更新:	ネットワークを通じて新機能を追加する
管理:	状態表示やプロキシサーバ[2]機能など攻撃者自身のための機能

ボットは侵入に成功しても利用者に発見されないように潜むため、なかなか実際の脅威や被害の事例が公開情報として現れません。警察庁によると、海外では、ボットに対し指令を行う者が、商用ウェブサイトに対してサービス拒否攻撃を行うという脅迫を行った例が報告されています[B1] 。

[1] サーバやクライアントといった役割を決めず、相互接続する不特定多数のコンピュータ同士が自律的に形成するネットワーク。ファイルの共有や、分散コンピューティングに利用されている。

[2] 一般には、端末の代理で通信を中継し、外部にアクセスするサーバ。この場合は送信元を隠蔽する目的で利用される。

2.1.2 変化し続けるコンピュータウイルスの脅威



2004 年もまた、先年同様に新種のウイルスが続々と登場し、流行しました。先年と違うのは次々と大量の亜種が出現したことです。わずか 3 種類のウイルスの亜種が、ウイルスの流行のほとんどを占めた時期もありました[B2] 。

最近のウイルスの特徴としては、亜種の登場が素早く、脆弱性の発見からそれを利用した新種のウイルスの登場までの期間が短いという二点が挙げられます。ウイルスの素となるソースコードの流通やウイルス開発者同士の争いなどの原因により、一つのウイルスに新たな機能を付与した亜種が次々と出現するようになりました。そのため、従来の対策だけでは感染を防ぎにくく、ウイルス定義ファイルの配布が間にあわずに感染する危険性があります。

また、ウイルス感染の目的が変化しています。従来のウイルスはデータの破壊など派手な動きで愉快犯的な動機のものが多かったのに対し、現在は経済的な利益を得ることなどを目的としたものが増えています。例えば、格安商品を宣伝する迷惑メールを配布するためのウイルスがありました。

国内では、国産ソフトウェアの P2P ネットワークを利用して繁殖するウイルスが発見されました。亜種の中には利用者のデスクトップの画像やファイルを P2P ネットワークに公開してしまうものなども存在しました。

従来国内を主なターゲットにしたウイルスはほとんどありませんでしたが、このウイルスの流行により、今後は国内を主な対象とした国内発のウイルスが出現する可能性も考慮しなければならなくなりました。

ウイルス被害届出の増加

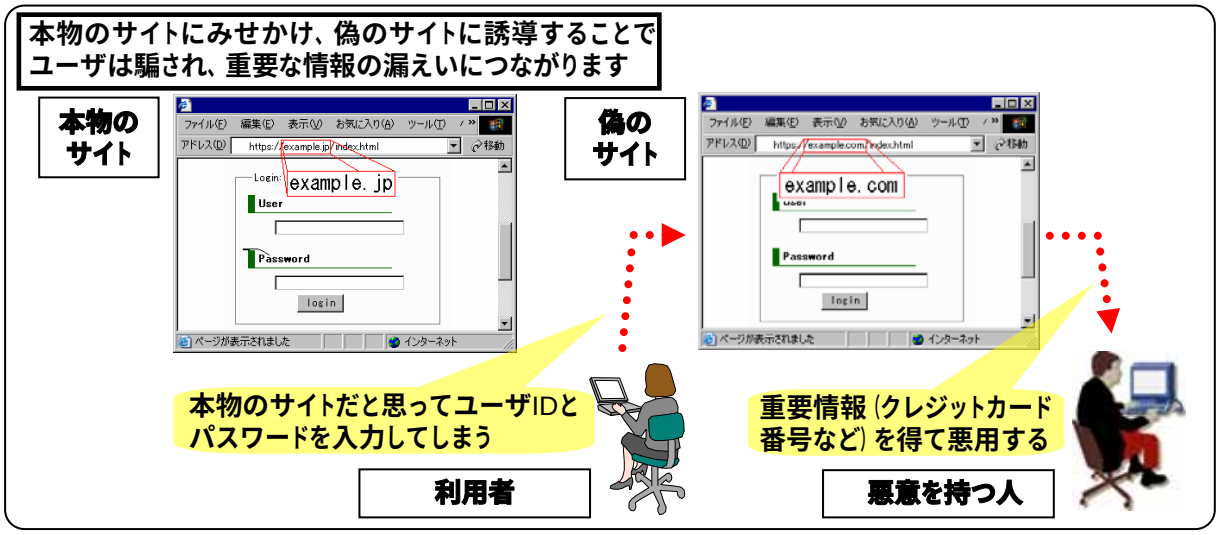
情報処理推進機構(IPA)に届けられたウイルスの届出件数は、先年に比べて約 3 倍と大きく増加しています[B2] 。

特に、W32/Netsky の亜種の被害が大きく、多数のユーザが感染していたようです。

大多数のウイルスは、従来のセキュリティ対策と日頃からの注意を心掛けることで十分防護できるため、感染する危険性自体は少なくなっています。しかし、次々と新種や亜種のウイルスが登場して

いることと、感染後の活動はより悪質なものが増えているため、感染後の活動による被害の危険性は高まっています。

2.1.3 フィッシング詐欺の脅威



フィッシング詐欺とは、クレジット会社やネット銀行などからのお知らせと偽ったメールを送信して、対象者を偽のウェブサイトに誘導し、個人情報やパスワード、カード情報といった重要情報を入力させて盗み取ろうとする手法の総称です。

単純な手法では送信元を偽ったメールを使い、本物のウェブサイトに似せたページに導いて騙そうとします。高度な手法になると、本物のウェブサイトにある脆弱性を利用してウェブページに偽情報を表示し、利用者を騙そうとするものもあります。

2004 年は、国内でフィッシング詐欺の流行が始まった年でした。フィッシング詐欺自体は海外で既に流行していましたが、国内向けのフィッシング詐欺が実際に発見されたのは 2004 年が初めてです。

国内で発見されたフィッシング詐欺の例として、アドレスバーやステータスバーの表示が上書きできるウェブブラウザの脆弱性を悪用して、アドレスバーを偽装するものがありました。また、本物のウェブサイトにある脆弱性を利用して本物のウェブサイトに偽情報を表示し、偽のウェブサイトへと誘導を行うものがありました。

利用者を騙す巧みな偽装

例えば、ウェブポータルサイト企業の有料サービスが利用されたフィッシング詐欺では、クレジットカード番号を入力させるために、いくつもの偽装が行われていました。

- 有料サービスの期限切れを装うメールを送信
- ブラウザの脆弱性を利用して URL を偽装
- 本物と酷似したログインフォームを用意
- 本物のサイトのログイン機能を利用して、正しいパスワードしか受け付けない
- 正しいログインで信用させた後で、クレジットカード情報を要求

注目すべき点として、日本でのフィッシング詐欺は先に挙げたウェブサイトやウェブブラウザの脆弱性を利用する手法のように、海外で時間をかけて培われた最新の手法が最初から用いられている

ということが挙げられます。単純な手法もよく用いられていますが、傾向としては最新の手法が利用され続けると考えられます。

2.2 対策

一般の利用者が行うセキュリティ対策で重要な事は、パッチの適用や対策ソフトウェアの導入といった、基本的な対策を継続的に行うことです。適切な対策を行い続ければ、大多数の攻撃の被害を受ける危険性を低くできます。

2.2.1 ソフトウェアを安全に保つ

ソフトウェアを、パッチの適用やバージョンアップなどで、可能な限り安全なものに保つようにしてください。バージョンアップの中には機能の追加だけではなく、脆弱性の修正が含まれることがあります。

一般に、ソフトウェアのバージョンが古いままだと、時間が経つにつれてセキュリティ上の危険度は高まっていきます。特に、有名なソフトウェアは利用者も多いために、攻撃者にとっても対象とする利点が多く、脆弱性が悪用されてしまう可能性が高くなります。

ソフトウェアによっては、自動的なバージョンアップの手段を備えているものがあります。例えばマイクロソフト社の製品ならば「Windows Update」、アップル社の製品ならば「ソフトウェアアップデート」を利用することで、バージョンアップにかかる手間を軽減できます。

ベンダ毎の修正ポリシーの違い

ベンダ(製品開発者)によっては、ウェブサイトで脆弱性情報と修正のための情報を提供しています。

また、ベンダによっては、次の製品の出荷時にあわせて修正をするものもあります。

しかし、必ずしも全てのベンダがパッチやバージョンアップによる脆弱性の修正を行うわけではありません。

あらかじめ、利用するソフトウェアの、セキュリティに関するベンダの対応方針を確認しておくことを勧めします。

2.2.2 信頼できないソフトウェアやデータを使わない

P2P ネットワークやウェブサイトから入手したソフトウェアやデータには、ウイルスやボットが付属していることがあります。ソフトウェアを導入したり、データを利用する際は、以下に挙げるような情報から、安全性を検討した上で、利用してください。

- 製品開発者が公開している情報以外の、第三者が公開している情報
- 身近で利用している人から得られる情報
- 別途、対策ソフトウェアを利用して、ソフトウェアを調査した情報

また、ソフトウェアによっては、個人情報などを収集するスパイウェアと呼ばれるプログラムを共にイ

ンストールするものがあります。スパイウェアは、ソフトウェアのライセンスで導入が必須と定められている場合があります。2004 年には無料をうたう製品がスパイウェアを含んでいたことが問題となりました。ソフトウェアの導入の際は、あらかじめライセンスを確認し、必要以上の情報を収集するような項目が無いことを確認した上で導入するようにしてください。

2.2.3 対策ソフトウェアの導入

ウイルスに対するワクチンソフトといったような、対策のためのソフトウェアを導入することで被害を軽減できる脅威もあります。

ワクチンソフトを利用することで、既存のウイルスに対して感染前にウイルスを発見したり、ウイルスの感染時の活動を防いだりすることが可能です。古いウイルス定義ファイルではウイルスを検知できないため、ワクチンソフトを利用されている場合は、ウイルス定義ファイルを常に最新に保つことをおすすめします。

対策ソフトウェア以外の対策

情報処理推進機構はウェブサイトで、ウイルス対策として初心者向けの説明や対策チェックシートなどを提供しています[B3] 。

また、セキュリティ対策についても、対象にあわせた情報を提供しています[B4] 。

また、ネットワーク外部からの攻撃を防ぐために、パーソナルファイアウォール製品を導入する方法もあります。

2.2.4 利用者自身の対策

フィッシング詐欺など利用者の心理を対象とした脅威の増加に伴い、利用者自身の注意がますます必要となっています。例えば、フィッシング詐欺を防ぐ方策として、個人情報や重要情報の入力を促すメールは信用しないということや、ウイルスを防ぐ方策として、不審なメールを開かないということがあります。

マイクロソフト社はウェブサイトで、フィッシング詐欺の防ぎ方として具体的な 5 つのステップを示しています[B5] 。

公共ネットワークの信頼性

不特定多数が利用可能なインターネット喫茶のコンピュータに、キーボードの入力を記録する「キーロガー」というソフトウェアを仕掛け、ネット銀行の口座から預金を引き出される事件がありました。

誰もが利用可能な環境にあるコンピュータは、悪意ある人も利用しています。信頼できないネットワークの場合、重要な情報を取り扱わないなど、自衛をした上で利用してください。

警察庁では「フィッシング 110 番」を設けて、フィッシング詐欺の被害の相談窓口の紹介や情報の受付を行っています[B6] 。

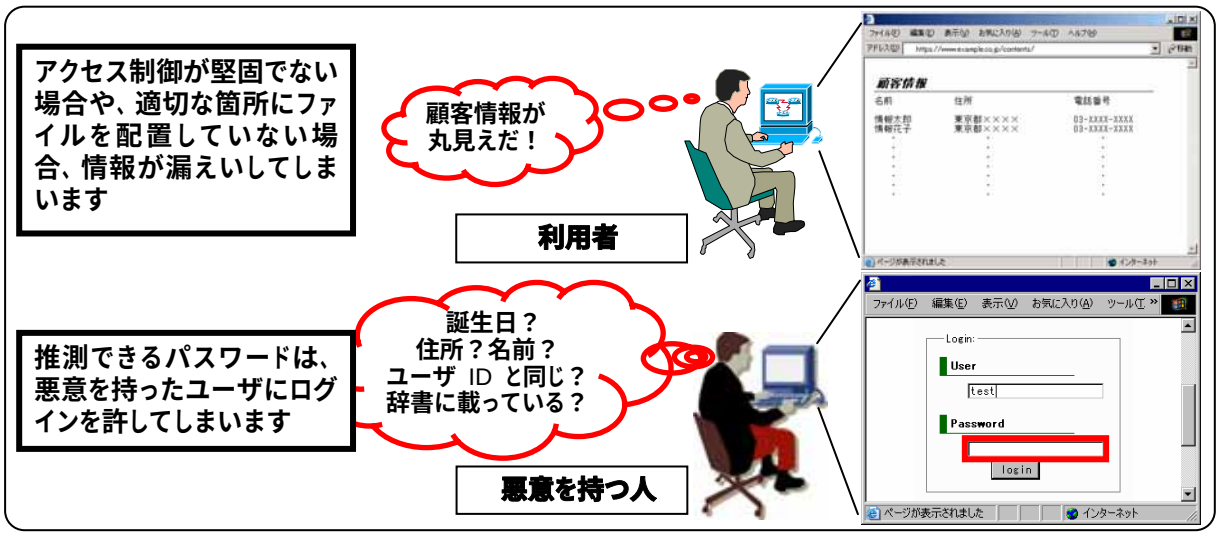
3. 2004 年の傾向と対策 (管理者向け)

この章では、組織のシステム管理者およびネットワーク管理者、個人でサーバを立ててサービスを提供している人など、管理者向けの情報を取り扱います。

3.1 2004 年の脅威の特徴

2004 年も様々な脆弱性が公表されましたが、昨年までと同様に、公表時期の新旧の区別無く、外部から任意のコードが実行できるといったような攻撃に有用な脆弱性であれば利用されています。

3.1.1 個人情報保護への関心の高まりと漏えい事件の多発



2005 年 4 月 1 日の「個人情報の保護に関する法律」施行を控え、個人情報の保護が官民を問わず重要視されています。

しかし、依然として個人情報漏えいに関する事件も多く、特にウェブサーバからの漏えいはネットワーク越しの個人情報漏えいとして先年に引き続き話題となりました。

ウェブサーバからの個人情報漏えいの類例としては、公開すべきではない情報を誤って公開している場合があります。通常はアクセス制御を行うか、ウェブサーバとは切り離して保管しておくべき情報を、ウェブサーバの公開ディレクトリに置いてしまい、結果として情報が漏えいしてしまう例がありました。

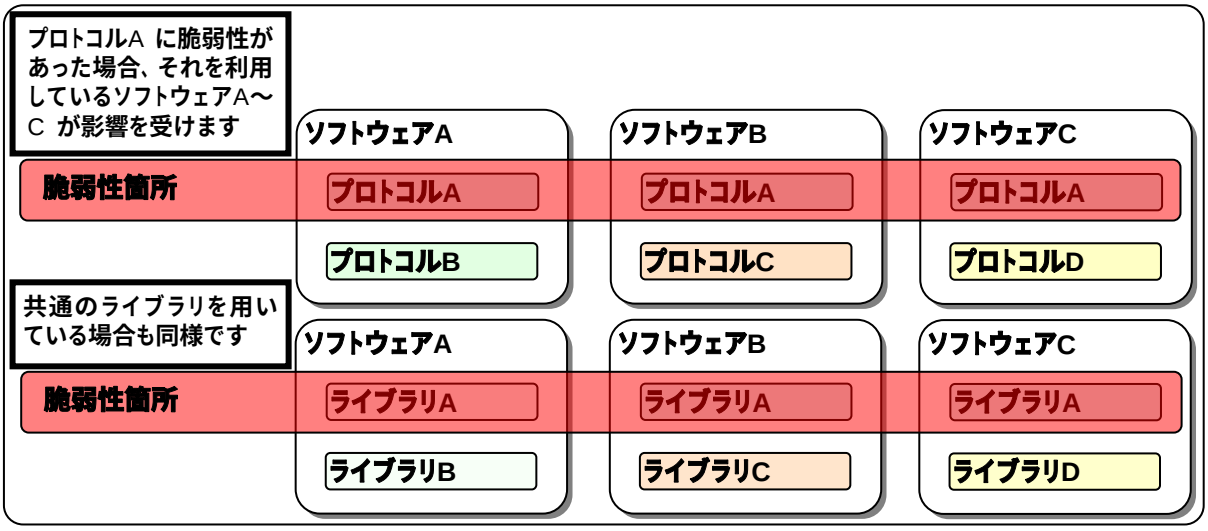
俳優の公式サイトから情報漏えい

俳優の公式ページにおいて、第三者に氏名、住所、電話番号、メールアドレス、パスワード、性別、生年月日などの個人情報が漏えいしてしまう事件がありました。

この件では、ウェブサイトで利用している認証情報が推測可能であったために、認証を回避してアクセスできてしまい、第三者がユーザを騙ってアクセス可能でした。

他にも、ウェブアプリケーションの脆弱性を攻撃された結果、情報が漏えいする場合があります。国内でも実際に、悪用が容易な脆弱性を攻撃され、個人情報が漏えいした例がありました。

3.1.2 複数製品にまたがる脅威の増加



2004 年に発見された脆弱性の中には、インターネットの通信に利用するプロトコルの設計上の脆弱性や実装上の脆弱性、画像フォーマットの解釈の問題などといった、複数のベンダの複数の製品にまたがる影響範囲の広い脆弱性がいくつもありました。

特に、インターネットの基礎となっている TCP/IP プロトコルの脆弱性(参考情報:A.5.1)は、仕様自体の弱点をついているために修正が難しく、各所で論議を呼びました。

2004 年は、「仕様」が「脆弱性」という観点からも注目されるきっかけとなった年でした。

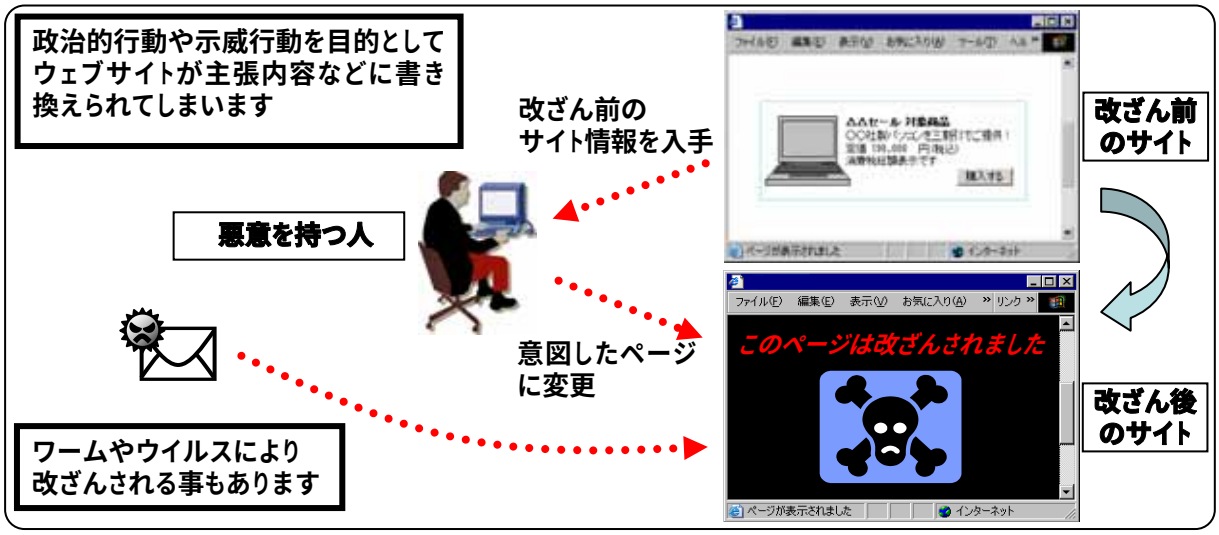
国内においては、このような複数のベンダにまたがる脆弱性情報をいち早く必要な関係者に伝達し、対策を検討するために、情報処理推進機構を受付機関、JPCERT/CC を調整機関とした、「情報セキュリティ早期警戒パートナーシップ」を運用しています[B7] 。

連続する脆弱性の発見

いくつかの製品の BMP 形式の画像ファイルのヘッダの解釈に問題がありました。これらの脆弱性は、以下のように次々と連続して発見されました。

- 2004 年 7 月
  Microsoft Windows の脆弱性
  (参考情報:A.5.4)
- 2004 年 8 月
  QT Library の脆弱性
  (参考情報:A.5.5)
- 2004 年 9 月
  Mozilla の脆弱性
  (参考情報:A.5.6)

3.1.3 ウェブサイトの改ざんの脅威



ウェブサイトの改ざんは日々数多く繰り返されています。国内においても例外ではありません。

被害数が減らない理由としては、二つあります。一つ目は、悪質なワームやウイルスによる自動的な攻撃により、攻撃対象を意識的に選択しない無差別的な活動が増えたことです。二つ目は、結果が見た目にわかりやすい攻撃であるため、政治的行動や示威行動の手段として公的機関のウェブサイトなどを狙う者がいるということです。

改ざんが行われるということは、何らかの脆弱性がそのウェブサイトにあったということを示しています。ウェブサイトの改ざんが行われると、セキュリティ管理が甘いと見なされ、ウェブサイトの運営者にとって社会的な信用問題となります。被害が改ざんだけに見えても、実際には個人情報の漏えいがあったり、第三者への攻撃の踏台として利用されたり、悪意のあるプログラムが潜伏している可能性があります。

また、年末には新たな手法のウェブサイトを改ざんするウイルスが発見されました。従来と違う点は、無差別に対象を選択して攻撃するのではなく、特定バージョンのウェブアプリケーションを利用しているウェブサイトを検索サイトで調べて攻撃しており、対象を選んでいる点です。今後もウイルスの手法として利用される可能性が高い、注目すべき手法といえます。

ウイルスによる改ざん

2004 年末に、phpBB の脆弱性(参考情報:A.6.1)を悪用したウイルスが、検索サイトを用いた手法で話題となりました。このウイルスは以下のような特徴を持っていました。

- 検索サイトを利用して phpBB の特定バージョンを使用しているサイトを検索
- 検索したサイトを攻撃
- 感染の世代が 3 代目以降ならば、ウェブサイトを改ざん

最終的に、検索サイトで対策が行われ、ウイルスの被害は収束しました。

ウェブサイトの改ざんに利用される脆弱性は、必ずしも新しいものばかりとは限りません。セキュリティ企業の報告によると、実際の攻撃で一番利用されたのは、2002 年に発見された OpenSSL の問題(参考資料:A.6.2)でした。数年前に発見された脆弱性の対策を行っていないウェブサイトがいまだ

に多いことがわかります。

3.2 対策

管理者の管理下にあるネットワークにおいて事故が発生した場合、個人の場合と比べて社会に対する影響が大きくなります。一過性のセキュリティ対策ではなく、セキュリティマネジメントとして PDCA（計画・実施・点検・処置）の各サイクルに沿い、継続的にセキュリティ対策および運用をする事が重要です。

3.2.1 セキュリティを意識した設計

セキュリティを保つためには、設計段階から、サーバやソフトウェアのセキュリティを考慮する必要があります。例えば OS で不要なサービスを停止させ脆弱性へのリスクを軽減したり、参照を意図していない URL を外部から指定されてもサーバ内のファイルが読まれないようにしたりするなどです。

情報処理推進機構への脆弱性関連情報の届出によると、ウェブサイトの検索フォームや、ショッピングカート、問合せフォームなどの要素に対して、クロスサイト・スクリプティングの脆弱性などの様々な脆弱性が報告されています[B8] 。

ウェブサイト等で利用するウェブアプリケーションを開発する際は、セキュリティに気を配った安全なプログラミングのために、情報処理推進機構や産業技術総合研究所が公開している資料[B4] [B9] などを参考にし、脆弱性を作りこまないように注意してください。

個人情報の保護

個人情報を保存する際には、必ずアクセス制御を行い、必要な人間やプログラムだけがアクセスできるようにしてください。可能ならばウェブサーバとは他の場所に保存し、確実に外部からアクセスできないように設定することを強く推奨します。

3.2.2 システム検査を実施する

構築されたシステムやウェブアプリケーションに対し、脆弱性が存在するかどうか確認を行うためのセキュリティ検査を行い、脆弱性が発見された個所に対して対処を行うことをお勧めします。

堅固なシステムを構築したつもりでも、最新の脆弱性を見落としていたり、逆に古い脆弱性の対策が抜けていたりするかもしれません。検査を専門家に依頼する方法もあります。

3.2.3 総合的なセキュリティレベルを保つ

管理者の管理下にあるコンピュータやネットワークのセキュリティレベルを保つには、個々のクライアントやネットワークインフラストラクチャの構成要素のセキュリティを保つ以外にも、セキュリティポリシーを定め、クライアントの管理方法やパッチの適用手法、トラブルが発生した場合の対処法などを定める方法があります。

組織の場合は攻撃による被害を受けないための対策と同様に、いざ被害を受けた際の対応をセキュリティポリシーであらかじめ規定しておくことが重要です。被害を受けた際に適切な対応を取ることで、組織としての信用が保たれる可能性が高くなります。

また、検査で良い結果が出たとしても、時間の経過とともに脆弱性が発見される可能性が高くなります。セキュリティマネジメントの一環として、定期的なセキュリティレベルの確認を実施する事をお勧めします。

セキュリティ管理規格

2004 年は組織全体のセキュリティとして、ISMS が注目を浴びました。ISMS は、組織で執り行う情報セキュリティ管理に関する世界的なスタンダード規格です。

国内では、日本情報処理開発協会（JIPDEC）を中心として認定が行われています[B10]。

4. まとめ

2004 年は、発見された脆弱性の数、種類に大きな変化は見られませんでしたが、その悪用方法が大きく変化した年でした。特にその傾向は、コンピュータを利用する人間を狙うフィッシング詐欺や、発見されないようにひそかに事を進めようとするボットなどに特徴的に現われていました。

発見される脆弱性も、類似の脆弱性が多くの製品に発見されたり、情報漏えいやウェブサイトの改ざんが行われたりするなど、脆弱性の内容そのものよりもむしろその脆弱性によって被る社会的な影響が目立つようになってきています。

セキュリティは一つの対策、一時の対策だけで万全となるものではありません。物理的、ソフトウェア的、そして利用者自身の注意による対策を施してリスクを減らすことと、被害を受けてしまった場合の対応をあらかじめ決めておくことが重要となります。

本資料を、今後のセキュリティ対策に役立てていただければ幸いです。

5．検討会構成メンバー

検討会構成メンバー（順不同･敬称略）

斉藤 純平	株式会社アークン
渡部 章	株式会社アークン
佐藤 友治	株式会社 IRI コミュニケーションズ
齋藤 衛	株式会社インターネットイニシアティブ
高橋 正和	インターネットセキュリティ システムズ株式会社
守屋 英一	インターネットセキュリティ システムズ株式会社
徳田 敏文	インターネットセキュリティ システムズ株式会社
関取 嘉浩	NRI セキュアテクノロジーズ株式会社
菅谷 光啓	NRI セキュアテクノロジーズ株式会社
竹内 健治	NRI セキュアテクノロジーズ株式会社
佐藤 利幸	NTT コミュニケーションズ株式会社
西尾 秀一	株式会社 NTT データ
池田 和生	株式会社 NTT データ
勝見 勉	グローバルセキュリティエキスパート株式会社
石飛 節	経済産業省
川口 修司	経済産業省
南 英生	経済産業省
高木 浩光	独立行政法人 産業技術総合研究所
伊藤 友里恵	JPCERT コーディネーションセンター（JPCERT/CC）
笹木 一義	ソフトバンク BB 株式会社
日名子 聡志	ソフトバンク BB 株式会社
平原 伸昭	トレンドマイクロ株式会社
門林 雄基	奈良先端科学技術大学院大学
宮地 利雄	日本電気株式会社
西村 高志	日本パーソナルコンピュータソフトウェア協会(JPSA)
田山 晴康	株式会社日立製作所
大力 洋介	富士通株式会社
富田 英夫	富士通株式会社
岡谷 貢	防衛庁
加藤 義宏	マカフィー株式会社
佐山 享史	三井物産セキュアディレクション株式会社
井上 信吾	株式会社三菱総合研究所
村瀬 一郎	株式会社三菱総合研究所
牧野 京子	株式会社三菱総合研究所

岩井 博樹　　株式会社ラック
山崎 圭吾　　株式会社ラック
新井 悠　　株式会社ラック
柳澤 伸幸　　株式会社ラック
早貸 淳子　　独立行政法人 情報処理推進機構
福澤 淳二　　独立行政法人 情報処理推進機構
花村 憲一　　独立行政法人 情報処理推進機構
田原 美緒　　独立行政法人 情報処理推進機構
石山 和行　　独立行政法人 情報処理推進機構
若居 和直　　独立行政法人 情報処理推進機構

A. 2004 年の脆弱性トップ 19

本文で紹介した 2004 年の注目すべき主な脅威のそれぞれについて、脅威に関連する代表的な脆弱性情報を解説します。これらの脆弱性の多くは、実際に 2004 年に起きた被害の原因となったものです。それぞれの脆弱性について、どのような問題で、どのような危険性があるのかを説明し、参考となる URL を添えました。今後の対策の参考にしていただければ幸いです。

A.1 ボット(botnet)の脅威

A.1.1 Microsoft Windows の LSASS の脆弱性

Microsoft Windows では、LSA(Local Security Authority)サービスというセキュリティのためのサービスが動作しています。LSASS DCE/RPC 経由で利用できる Microsoft Active Directory サービスの、デバッグ出力を行う関数には、バッファオーバーフローが可能な問題がありました。

この問題を悪用されると、リモートから RPC 接続経由でバッファオーバーフローが発生し、サービスの権限で任意のコードを実行される危険性があります。

参考:

- US-CERT Vulnerability Note VU#753212
  http://www.kb.cert.org/vuls/id/753212
- Microsoft Windows **のセキュリティ修正プログラム**
  http://www.microsoft.com/japan/technet/security/bulletin /ms04-011.mspx

A.1.2 Microsoft Windows の RPC の脆弱性

Microsoft Windows の RPC サービスは、外部から特定の機能を実行するリモートプロシージャ機能を提供します。DCOM インタフェースは RPC サービスを利用し、ネットワーク経由でサービスを提供します。DCOM インタフェースには、入力を適切に取り扱わないためにオーバーフローが可能な問題がありました。

この問題を悪用されると、サービスの動作権限で任意のコードを実行される危険性があります。

参考:

- RPC **インタフェースのバッファ オーバーランによりコードが実行される**
  http://www.microsoft.com/japan/technet/security/bulletin/MS03-026.mspx

A.2 変化し続けるコンピュータウイルスの脅威

A.2.1 Microsoft Internet Explorer の IFRAME 要素の脆弱性

Microsoft Internet Explorer には、複数のウェブページを表示する frame 要素や、ページの中に別のウェブページを埋めこむ iframe 要素の複数の属性において、ヒープメモリ領域のオーバーフローが可能な問題がありました。

この問題を悪用されると、frame 要素あるいは iframe 要素を利用したウェブサイトや電子メールを閲覧した利用者は、利用者の権限で任意のコードを実行される危険性があります。

参考:

- US-CERT Vulnerability Note VU#842160
  http://www.kb.cert.org/vuls/id/842160
- Internet Explorer **用の累積的なセキュリティ更新プログラム**
  http://www.microsoft.com/japan/technet/security/bulletin/ms04-040.mspx

A.2.2 OpenSSH サーバプログラムの脆弱性

OpenSSH は安全なシェル通信を行う SSH(Secure SHell)の実装の一つです。チャレンジ･レスポンス認証など複数の認証方法をサポートしています。

OpenSSH のサーバには、チャレンジ･レスポンス認証を利用する際にオーバーフローが可能な問題がありました。

この問題を悪用されると、リモートから OpenSSH のサーバが動作している権限で、任意のコードを実行される危険性があります。

参考:

- OpenSSH **サーバプログラムの脆弱性に関する注意喚起**
  http://www.jpcert.or.jp/at/2002/at020004.txt
- CERT Advisory CA-2002-18 OpenSSH Vulnerabilities in Challenge Response Handling
  http://www.cert.org/advisories/CA-2002-18.html

A.2.3 Microsoft Windows のドメインコントローラの脆弱性

Microsoft Windows の Locator Service は、オブジェクトと名前をマップするネームサービスで、RPC などに利用されています。Locator Service には、パラメータを適切に検証しないためにバッファオーバーフローが発生する問題がありました。

この問題を悪用されると、サービスの動作権限で、任意のコードを実行される危険性があります。

参考:

- Locator Service **の未チェックのバッファにより、コードが実行される**
  http://www.microsoft.com/japan/technet/security/bulletin/MS03-001.mspx

A.3 フィッシング詐欺の脅威

A.3.1 Microsoft Internet Explorer でコンテンツ枠外の座標への描画が可能な脆弱性

Microsoft Internet Explorer の Windows XP Service Pack 2 以前のバージョンには、window.open()や window.createPopup()メソッドで位置を示す座標の指定に負の値が利用可能であったため、Internet Explorer の通常ウェブサイトを表示するコンテンツ部分に座標が限定されず、範囲外の領域にも自由に新しいウィンドウやポップアップを表示する事が可能な問題がありました。

この問題を悪用されると、アドレスバーの上やステータスバーの上に偽の表示をされ、利用者が想定したものとは他のウェブサイトに誘導されてしまう危険性があります。

参考:

- Windows XP Service Pack 2 **への対応に向けた** Web **サイトの最適化**
  http://www.microsoft.com/japan/msdn/windows/windowsxp/xpsp2web.asp

A.3.2 Microsoft Internet Explorer でステータスバーに表示する URL が偽造可能な脆弱性

いくつかのウェブブラウザや HTML を解釈するメールクライアントにおいて、table 要素を利用したアンカーにより、実際にリンクをクリックした際に有効な URL と、ステータスバーに表示される URL を異なる表示に偽造可能な問題がありました。

この問題を悪用されると、利用者が想定したものとは他のウェブサイトに誘導されてしまう危険性があります。

参考:

- **成りすました** Web **サイトおよび悪質なハイパーリンクを見分けるための手順**
  http://support.microsoft.com/?id=833786
- US-CERT Vulnerability Note VU#925430
  http://www.kb.cert.org/vuls/id/925430

A.4 サーバからの情報漏えいの脅威

A.4.1 ディレクトリトラバーサルの脆弱性

ウェブサイトで利用される CGI の中には、"../" などのファイルパスを遡るための文字列を適切に取り扱わないものが存在します。サーバの内部のファイルを指定する識別子がウェブサイトの入力より操作可能である場合、入力に "../" など上位のディレクトリを含む内容を送信することで、実際にはアクセスできないディレクトリに存在するファイルにアクセスできる可能性があります。

この問題を悪用されると、パスワードファイルなど、サーバ内の任意のファイルを取得される危険性があります。

参考

■**ファイルオープン時のパスにご用心**
http://www.ipa.go.jp/security/awareness/vendor/programming/a04_01.html

A.5 複数製品にまたがる脅威の増加

A.5.1 TCP プロトコルの脆弱性

TCP/IP プロトコルには、長時間 TCP コネクションを切断せずに通信をしている場合、第三者から、コネクションの切断が可能な問題がありました。
この問題を悪用されると、多数の通信切断によるサービス妨害攻撃を受ける危険性があります。

参考:

■TCP **にサービス運用妨害を伴う脆弱性**
http://jvn.jp/cert/JVNTA04-111A/index.html
■TCP **プロトコルに潜在する信頼性の問題**
http://www.jpcert.or.jp/at/2004/at040003.txt

A.5.2 H.323 プロトコルの脆弱性

H.323 は、ITU-T の規格で定められた音声通信や動画通信のためのプロトコルです。複数製品の H.323 機能には、入力の内容を適切に検証しないためにオーバーフローが可能な問題がありました。

この問題を悪用されると、製品によっては任意のコードを実行される危険性があります。

参考:

■Cisco Security Advisory:Vulnerabilities in H.323 Message Processing
http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml
■Microsoft Internet Security and Acceleration Server 2000 H.323 **フィルタの脆弱性により、リモートでコードが実行される**
http://www.microsoft.com/japan/technet/security/Bulletin/MS04-001.mspx

A.5.3 JPEG 処理 (GDI+) のバッファオーバーランにより、コードが実行される

Microsoft 製品が利用する GDIPLUS.DLL には、JPEG 形式のファイルのヘッダ情報を適切に検証しないために、オーバーフローが可能な問題がありました。
この問題を悪用されると、利用者が JPEG ファイルを閲覧することで、任意のコードを実行される危険性があります。

参考:

- JPEG **処理** (GDI+) **のバッファ オーバーランにより、コードが実行される**
  http://www.microsoft.com/japan/technet/security/bulletin/MS04-028.mspx

A.5.4 Microsot Internet Explorer の BMP ファイル処理における脆弱性

Microsoft Internet Explorer には、BMP 形式のファイルのヘッダ情報を適切に検証しないために、オーバーフローが可能な問題がありました。

この問題を悪用されると、利用者が BMP ファイルを閲覧することで、任意のコードを実行される危険性があります。

参考:

- Internet Explorer **用の累積的なセキュリティ更新プログラム**
  http://www.microsoft.com/japan/technet/security/bulletin/ms04-025.mspx

A.5.5 QT ライブラリの BMP ファイル処理における脆弱性

QT ライブラリは KDE(K Desktop Environment)などで利用されているライブラリです。QT ライブラリには、BMP 形式のファイルのヘッダ情報を適切に検証しないために、オーバーフローが可能な問題がありました。

この問題を悪用されると、利用者が BMP ファイルを閲覧することで、任意のコードを実行される危険性があります。

参考:

- ISS X-Force Database:qt-bmp-bo(17040): Qt BMP image buffer overflow
  http://xforce.iss.net/xforce/xfdb/17040

A.5.6 Mozilla 製品の BMP ファイル処理における脆弱性

Mozilla Project の複数の製品には、BMP 形式のファイルのヘッダ情報を適切に検証しないために、オーバーフローが可能な問題がありました。

この問題を悪用されると、利用者が BMP ファイルを閲覧することで、任意のコードを実行される危険性があります。

参考:

- US-CERT Vulnerability Note VU#847200
  http://www.kb.cert.org/vuls/id/847200

A.6 ウェブサイトの改ざんの脅威

A.6.1 phpBB の脆弱性

phpBB はプログラミング言語 PHP を利用した掲示板システムです。phpBB で利用するページの一つである viewtopic.php には、highlight パラメータの入力を適切に処理していない問題がありました。

この問題を悪用されると、任意のコマンドを実行されたり、phpBB が動作しているサーバの管理者権限を奪取されたりする危険性があります。

参考:

- US-CERT Vulnerability Note VU#497400
  http://www.kb.cert.org/vuls/id/497400

A.6.2 OpenSSL の複数の脆弱性

OpenSSL は、様々なソフトウェアで利用されている暗号化ライブラリです。OpenSSL には、サービス停止やオーバーフローが可能な複数の脆弱性がありました。

これらの問題を利用されると、OpenSSL を利用しているソフトウェアの権限で、任意のコードを実行される危険性があります。

参考:

- CERT Advisory CA-2002-23 Multiple Vulnerabilities In OpenSSL
  http://www.cert.org/advisories/CA-2002-23.html

A.6.3 Microsoft IIS の WebDAV の脆弱性

Microsoft IIS は Microsoft Windows で動作するウェブサーバです。IIS は HTTP を介してファイルの操作を行う WebDAV プロトコルに対応しています。Microsoft IIS の WebDAV サービスには、入力を適切に検証しないためにオーバーフローが可能な問題がありました。

この問題を悪用されると、任意のコードを実行される危険性があります。

参考:

- Windows **コンポーネントの未チェックのバッファにより サーバが侵害される**
  http://www.microsoft.com/japan/technet/security/bulletin/MS03-007.mspx

A.6.4 クロスサイト・スクリプティングの脆弱性

ウェブサイトの中には、form 要素を利用したり、URL のパスやクエリを指定することで、利用者の入力に合わせて動的にページを生成したりするものがあります。動的なページを持つウェブサイトの中には、利用者からの入力をそのまま動的なページの一部として表示してしまったり、パラメータとして埋めこんでしまったりするものがあります。そのようなページに対してスクリプトを含んだ入力を送信された場合、動的なページを訪れた利用者のブラウザ上で、入力に含まれるスクリプトの実行が可能な問題があります。

この問題を悪用されると、ウェブページ自体の改ざんや、フィッシング詐欺ページへの誘導、クッキー(Cookie)の盗難、他の脆弱性との連携などが行われてしまう危険性があります。

参考:

■IPA **セキュア** Web **プログラミング** 1-2. **クロスサイトスクリプティング**
http://www.ipa.go.jp/security/awareness/vendor/programming/a01_02_main.html

A.6.5 Web アプリケーションのセッション管理方式の脆弱性

HTTP はステートレスなプロトコルです。そのため、ユーザのログイン状態を管理する必要があるウェブサイトでは、クッキーを用いた「セッション管理」が行われることがあります。そのとき、ウェブサイトはクッキーの値によってどのユーザからのアクセスかを識別します。

クッキーの値が公開された情報（たとえばユーザ名や会員番号、メールアドレスなど）であったり、推測可能な情報（桁数の短いセッション ID や、規則性のあるセッション ID）となっている場合、パスワード入力なしにログインできてしまったり、ログイン中の他のユーザのセッションをハイジャックできてしまう危険性があります。セッション管理用のクッキーの値は、十分に長いランダムな値としなくてはなりません。

参考:

■**秘密情報を含まない** COOKIE **に頼ったアクセス制御方式の脆弱性**
http://securit.gtrc.aist.go.jp/SecurIT/advisory/rawcookie/

B. 参考資料

[B1] @police「ボットネット(botnet)に注意
http://www.cyberpolice.go.jp/detect/pdf/H170127_botnet.pdf

[B2] IPA セキュリティセンター「コンピュータウイルス・不正アクセスの届出状況について」
http://www.ipa.go.jp/security/txt/2005/01outline.html

[B3] IPA セキュリティセンター 対策情報 ウイルス対策
http://www.ipa.go.jp/security/isg/virus.html

[B4] IPA セキュリティセンター 読者層別: 情報セキュリティ対策 実践情報
http://www.ipa.go.jp/security/awareness/awareness.html

[B5] Microsoft 「フィッシング詐欺を防ぐ」
http://www.microsoft.com/japan/athome/security/spam/phishing.mspx

[B6] 警察庁 「フィッシング 110 番」
http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

[B7] 経済産業省 「情報セキュリティ早期警戒パートナーシップ」の運用開始について
http://www.meti.go.jp/policy/it_policy/press/0005399/

[B8] ソフトウェア等の脆弱性関連情報に関する届出状況 2004 年第 4 四半期
http://www.ipa.go.jp/security/vuln/report/vuln2004q4.html

[B9] SecurIT
http://securit.gtrc.aist.go.jp

[B10] 情報セキュリティマネジメントシステム(ISMS)適合性評価制度
http://www.isms.jipdec.jp/