

コンピュータ不正アクセスの現状 (45分)

2001/11/22

情報処理振興事業協会 セキュリティセンター

不正アクセス被害とその影響

不正アクセスの分類

不正アクセス被害の動向と対策



不正アクセス被害とその影響

不正アクセスとは何か

一般的な概念

システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと。

「コンピュータ不正アクセス対策基準」(平成8年8月8日付け通商産業省告示第362号)
<http://www.meti.go.jp/press/past/c60806a2.html>

法的な定義

参照：不正アクセス行為の禁止等に関する法律

<http://www.meti.go.jp/kohosys/topics/10000098/esecu02j.pdf>
http://www.joho.soumu.go.jp/top/access_law/law.html
http://www.npa.go.jp/hightech/fusei_ac2/houann.htm

インシデントとは何か

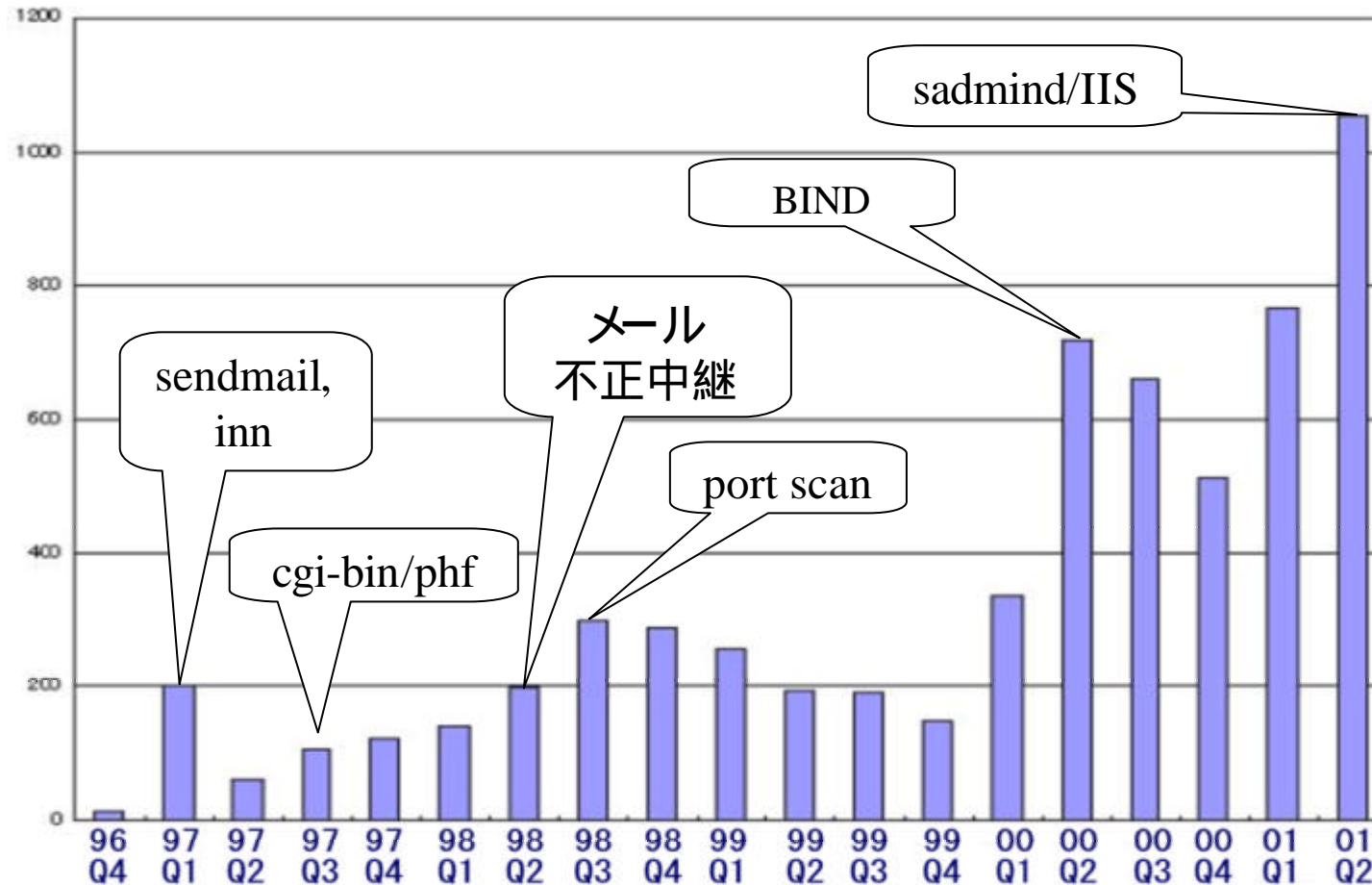
(インターネットに接続された)システムの運用に際して、セキュリティ上の問題として捉えられる事象

技術メモ - コンピュータセキュリティインシデントへの対応」(発行日 2000-08-25)
<http://www.jpccert.or.jp/ed/2000/ed000007.txt>

情報セキュリティ分野においては (security incident) 情報セキュリティリスクが発現した事象をいう

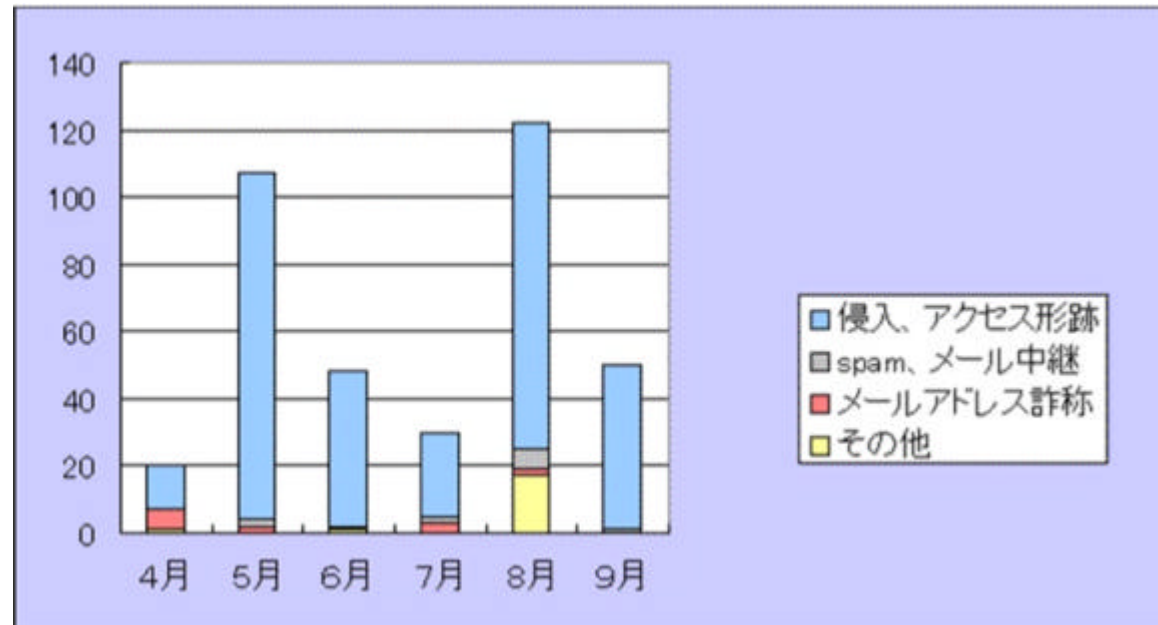
ネットワークセキュリティ関連用語集
<http://www.ipa.go.jp/security/ciadr/crword.html>

JPCERT/CCが受け付けた インシデント報告件数の推移



JPCERT/CC (コンピュータ緊急対応センター) インシデント報告件数の推移 (2001-07-26) <http://www.jpcert.or.jp/stat/reports.html>

IPAが受け付けた被害内容の分類



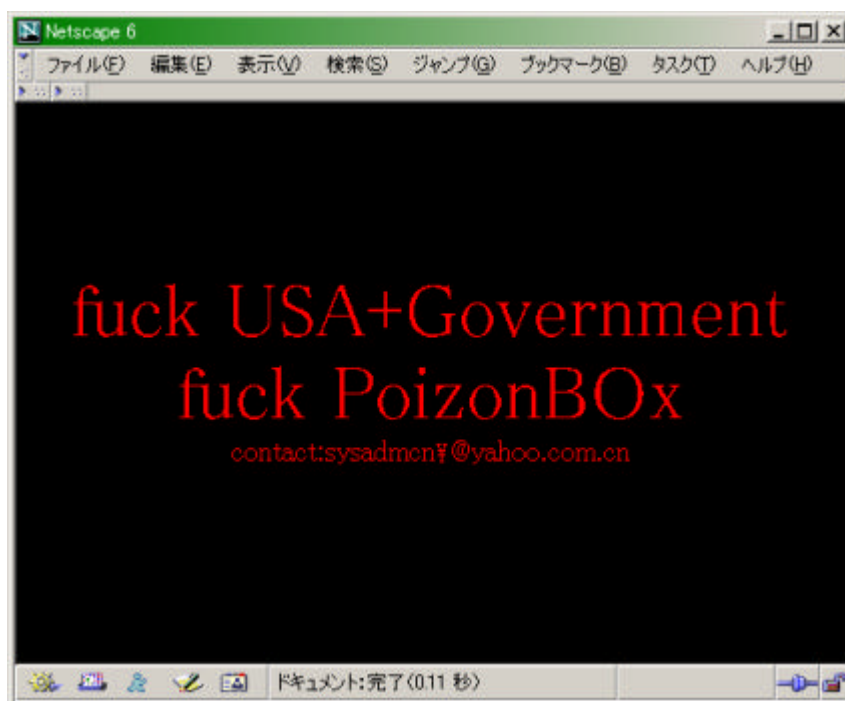
	4月	5月	6月	7月	8月	9月	合計
侵入、アクセス形跡	13	103	46	25	97	49	333
spam、メール中継	0	2	0	2	6	1	11
メールアドレス詐称	6	2	1	3	2	0	14
その他	1	0	1	0	17	0	19
合計(件)	20	107	48	30	122	50	377

不正アクセスの届出状況概要について (2001年9月)

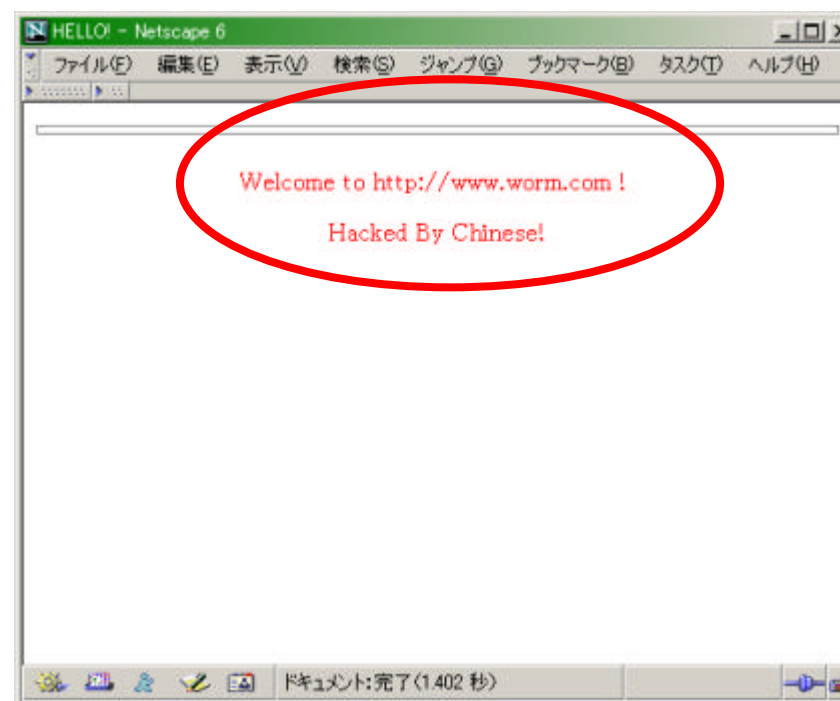
http://www.ipa.go.jp/security/crack_report/20011005/0109.html

Web改ざんの事例

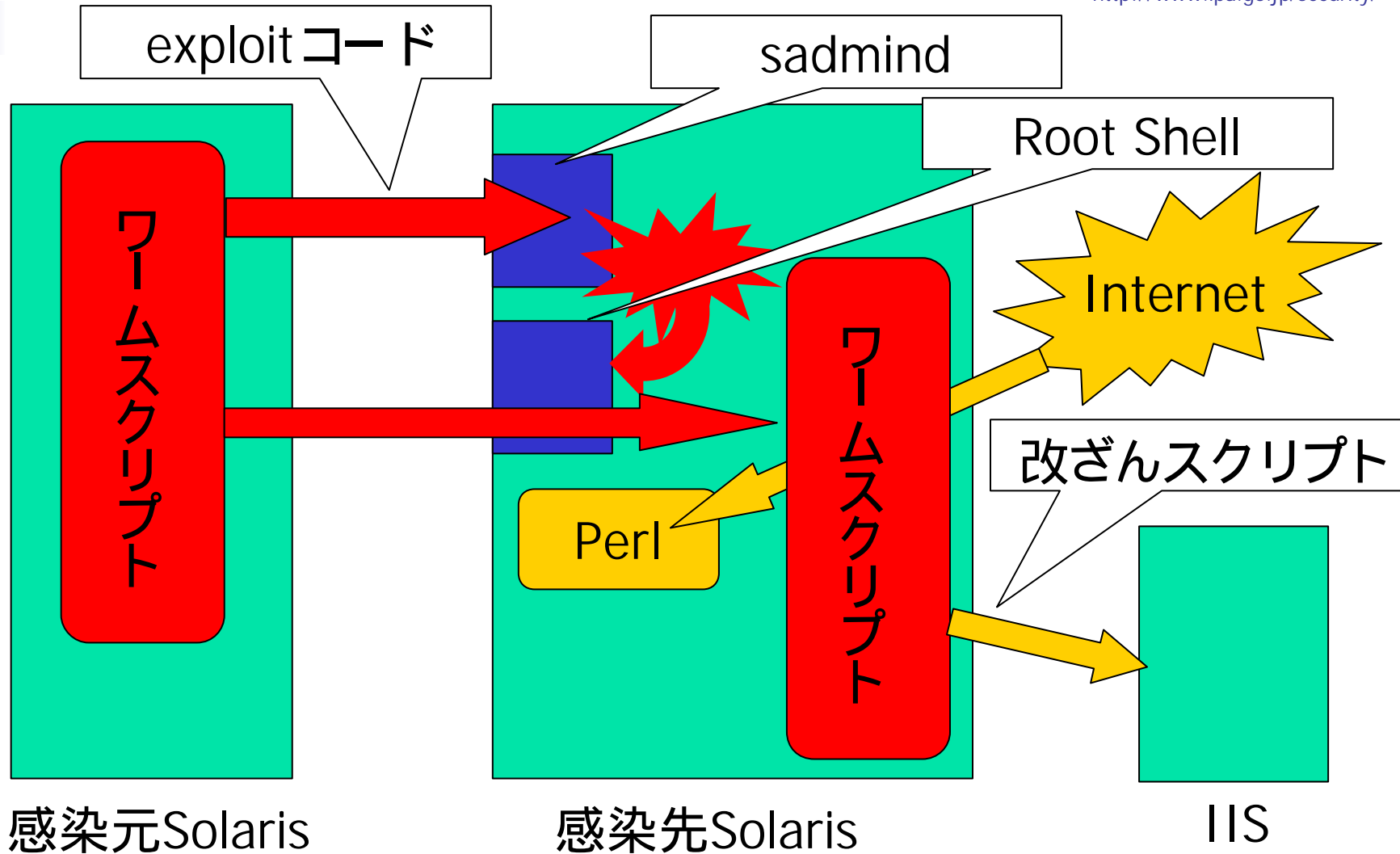
2001年5月 sadmind/IISで
改ざんされたWebページ



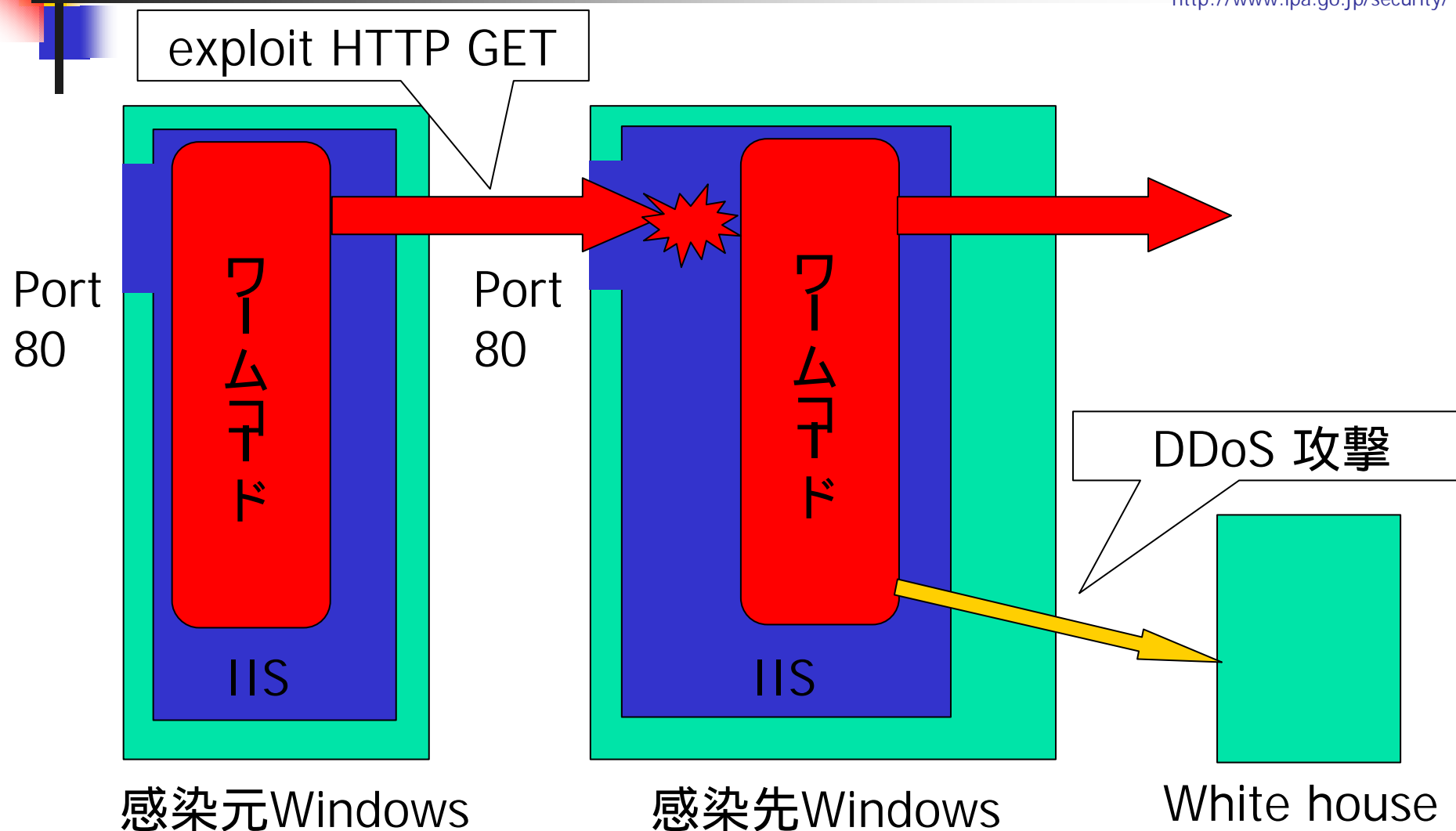
2001年7月 にCodeRed で
改ざんされたWebページ



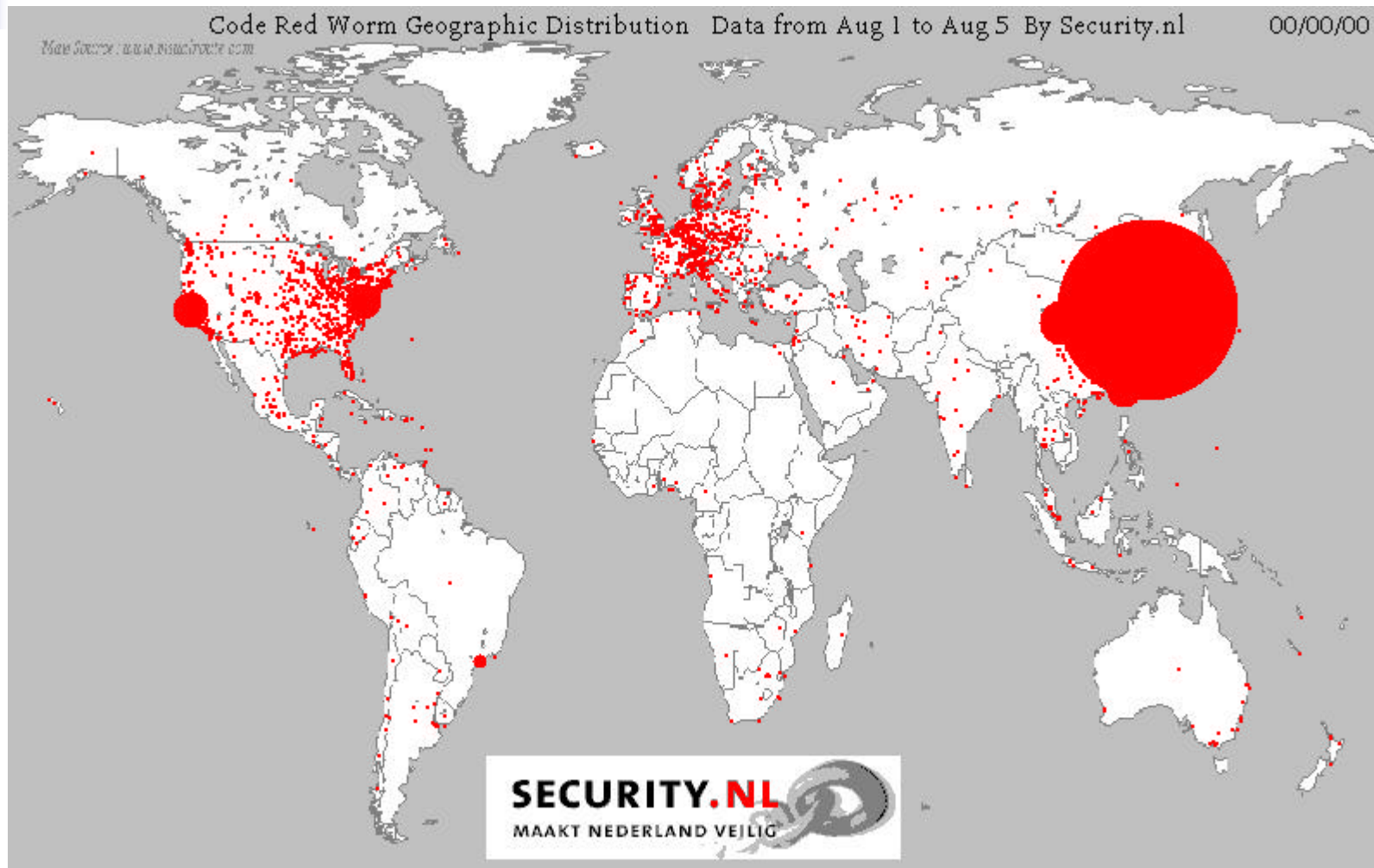
事例: sadmind/IIS



事例: Code Red



Code Red の感染の広がり

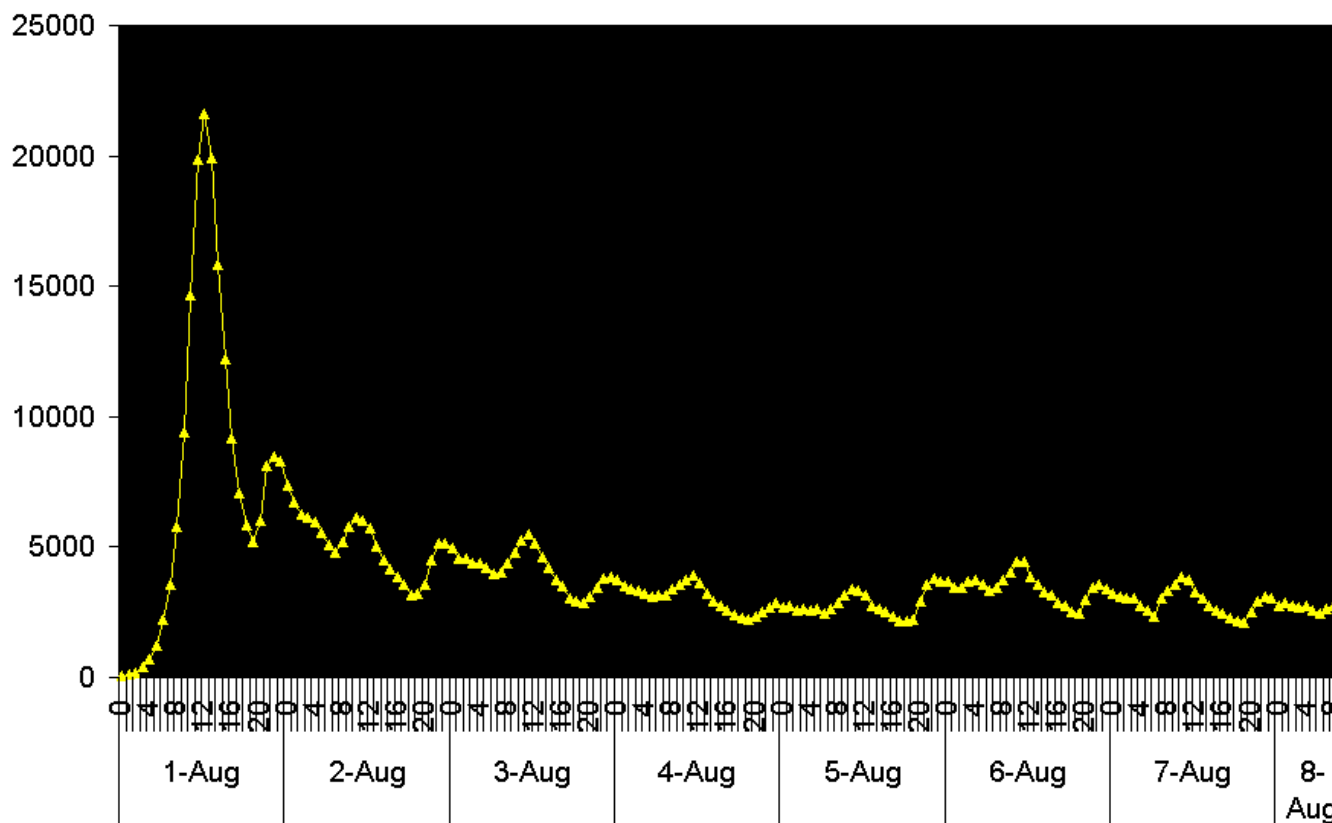


SECURITY.NL "Code Red worm stats"

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

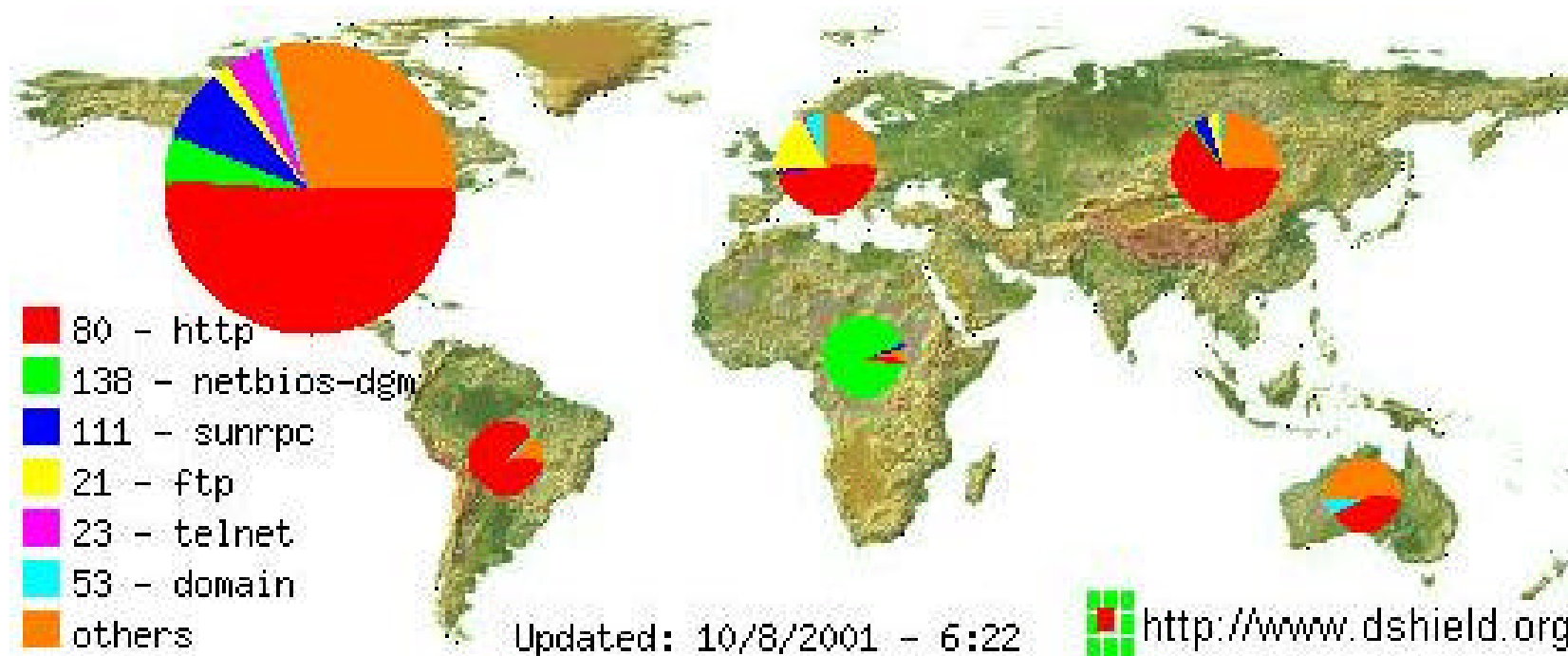
Code Red の感染速度

New IPS Infected Each Hour (1時間当たりの新規感染 IP アドレス数)



Digital Island - SANS Internet Storm Center "Code Red Status" <http://www.digitalisland.net/codered/>

インターネット上のスキャン分布



Geographic Distribution of attack sources. Last 5 days

DShield "Distributed Intrusion Detection System" <http://www.dshield.org/>

不正アクセス被害による影響

外部から
クラッカー、産業スパイ、元従業員など

内部から
従業員、クラッカーなど

不正アクセス被害

物理的な被害

経済的な損失

社会的な信頼の喪失

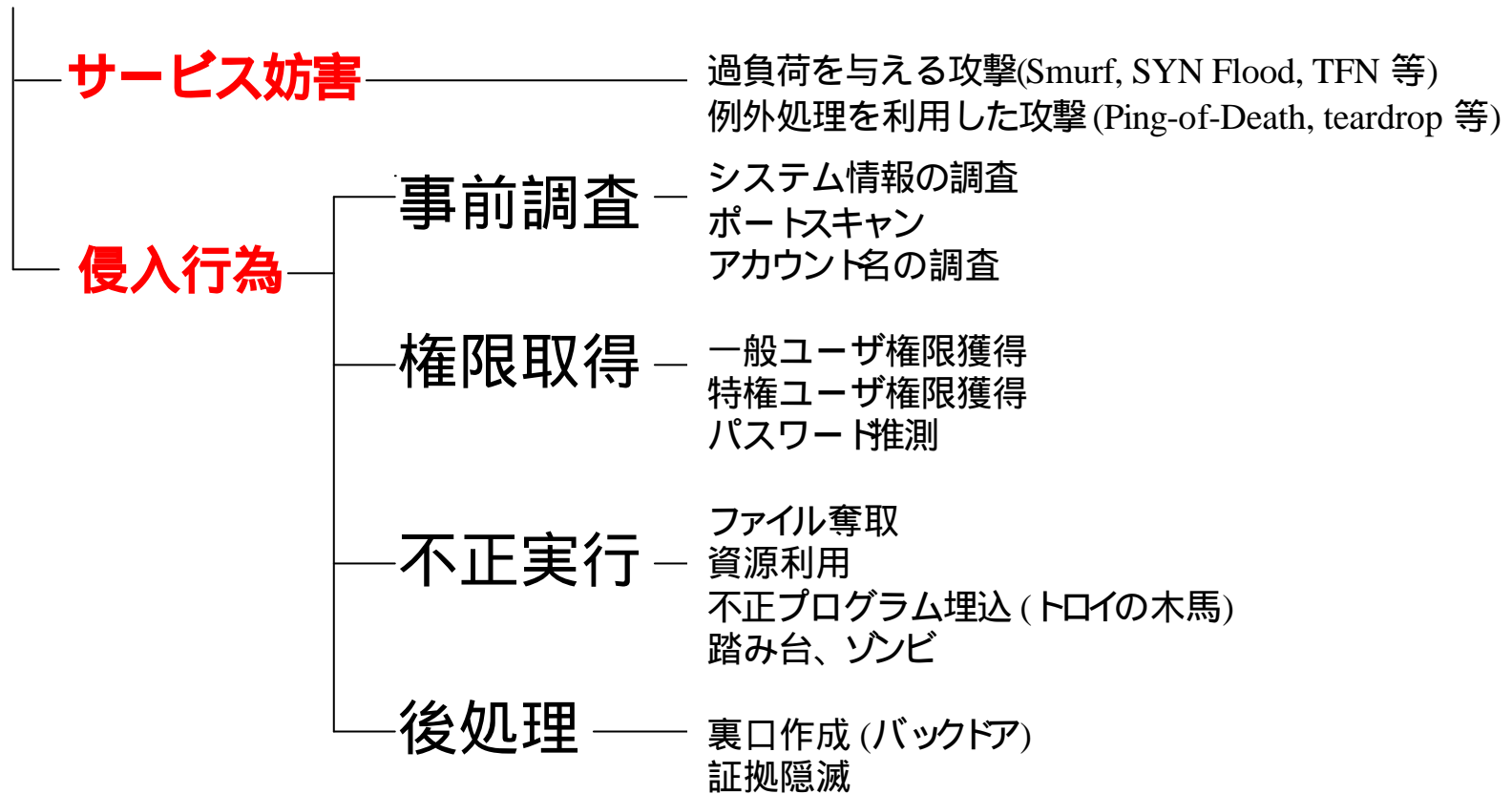
大きな代償



不正アクセスの分類

不正アクセスの分類

不正アクセス



サービス妨害攻撃 :DoS (Denial of Service)

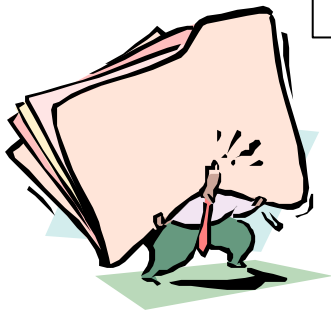
過負荷を与える攻撃

標的マシンに対して過大の負荷を与え、パフォーマンスを低下させる。(Smurf、SYN Flood など)

DDoS: 複数のマシンを使った DoS攻撃。(TFN, Code Red など)

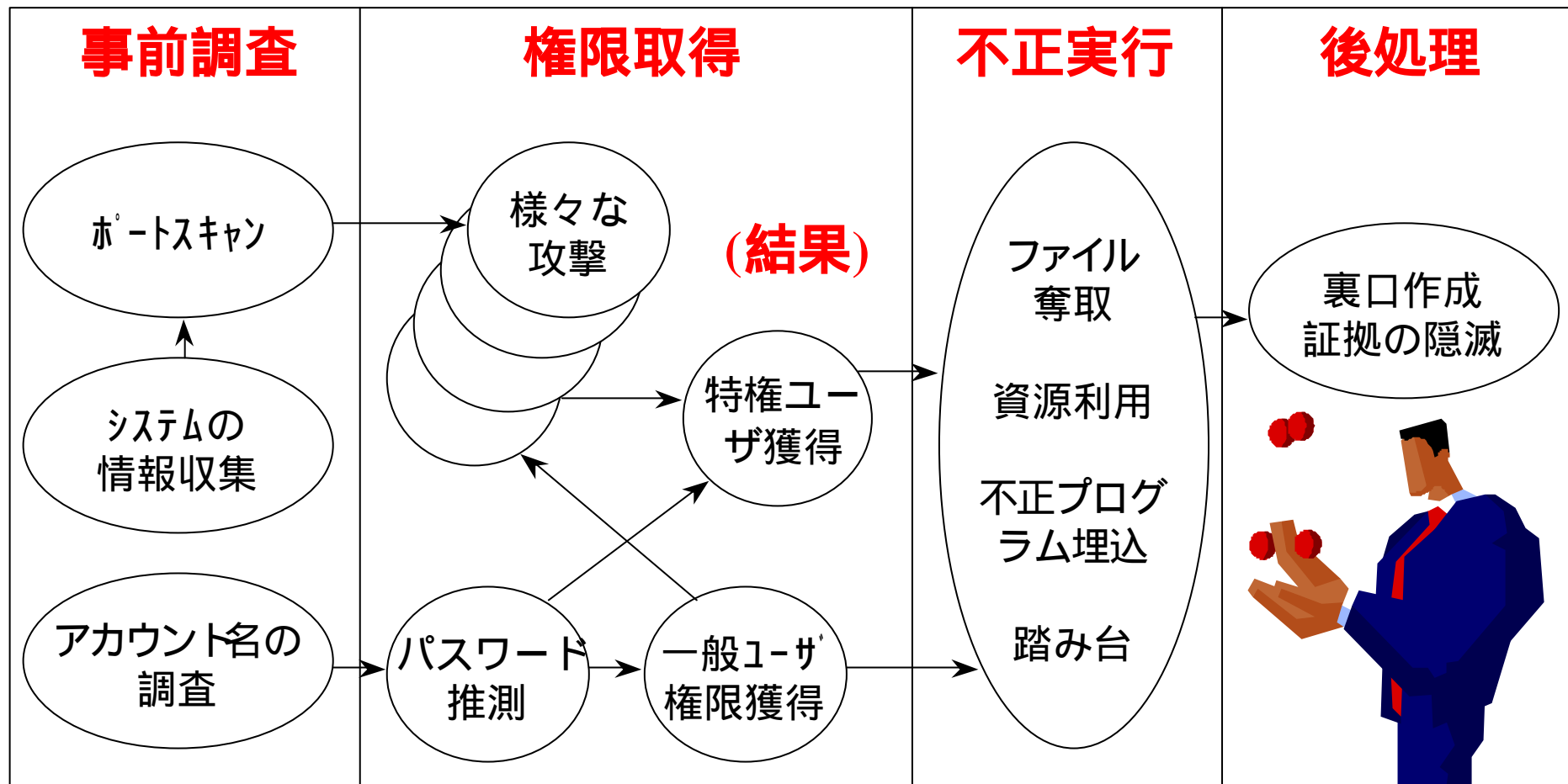
例外処理を利用した攻撃

標的マシンに対して実行不可能な例外処理を要求し、機能を停止または低下させる。(teardrop, Ping-of-Death など)



侵入行為

一般的な侵入行為の流れ





不正アクセス被害の動向と対策

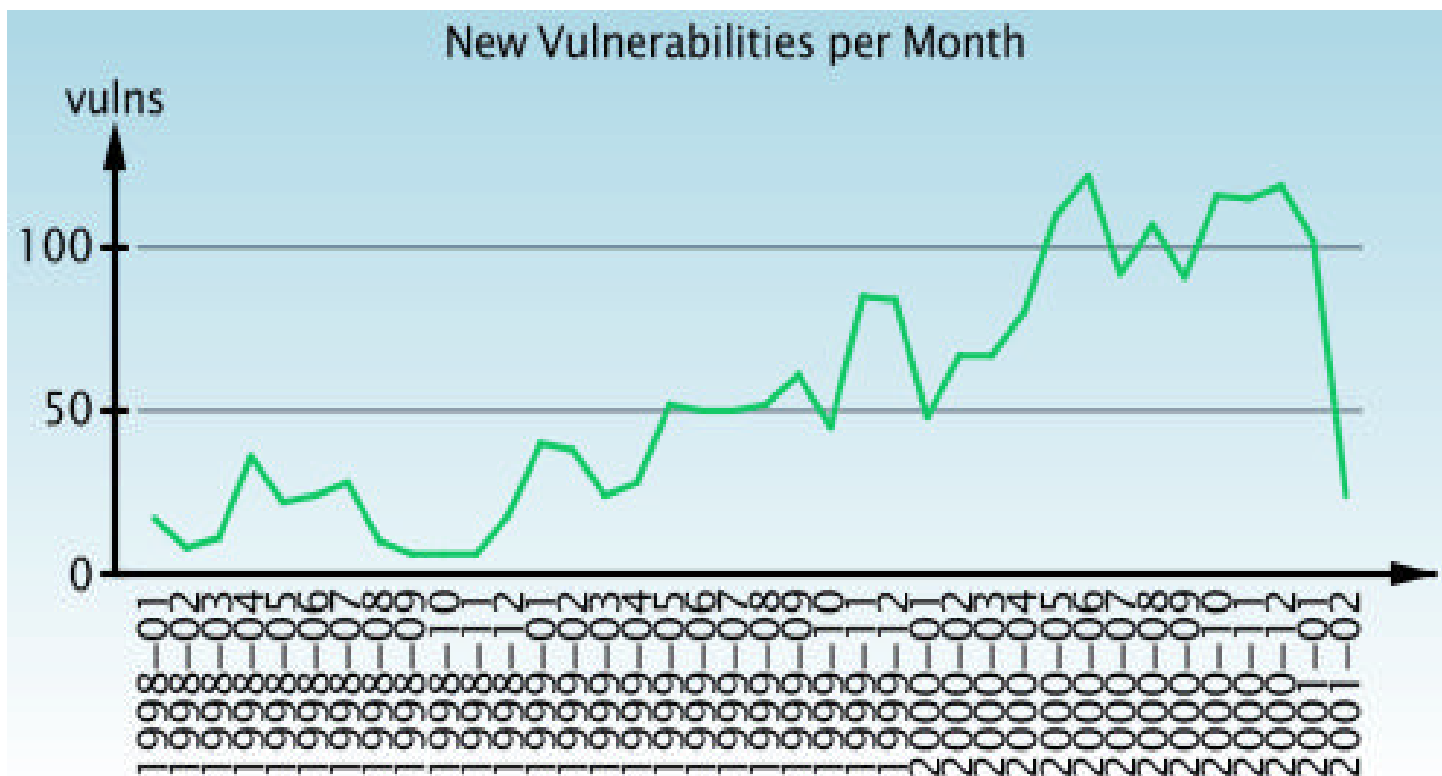
不正アクセス届出増加の要因

- 被害対象となるサイト数自体の増加
- 不正アクセスを行う攻撃者数の増加
(exploit コード, root キット)
- 管理者・組織のセキュリティに関する認識の変化 (→届出増)

参考: 不正アクセス手法と技術的対策に関する調査 - 「不正アクセス動向調査報告書」

http://www.ipa.go.jp/security/fy12/contents/crack/mri/report_trend.pdf

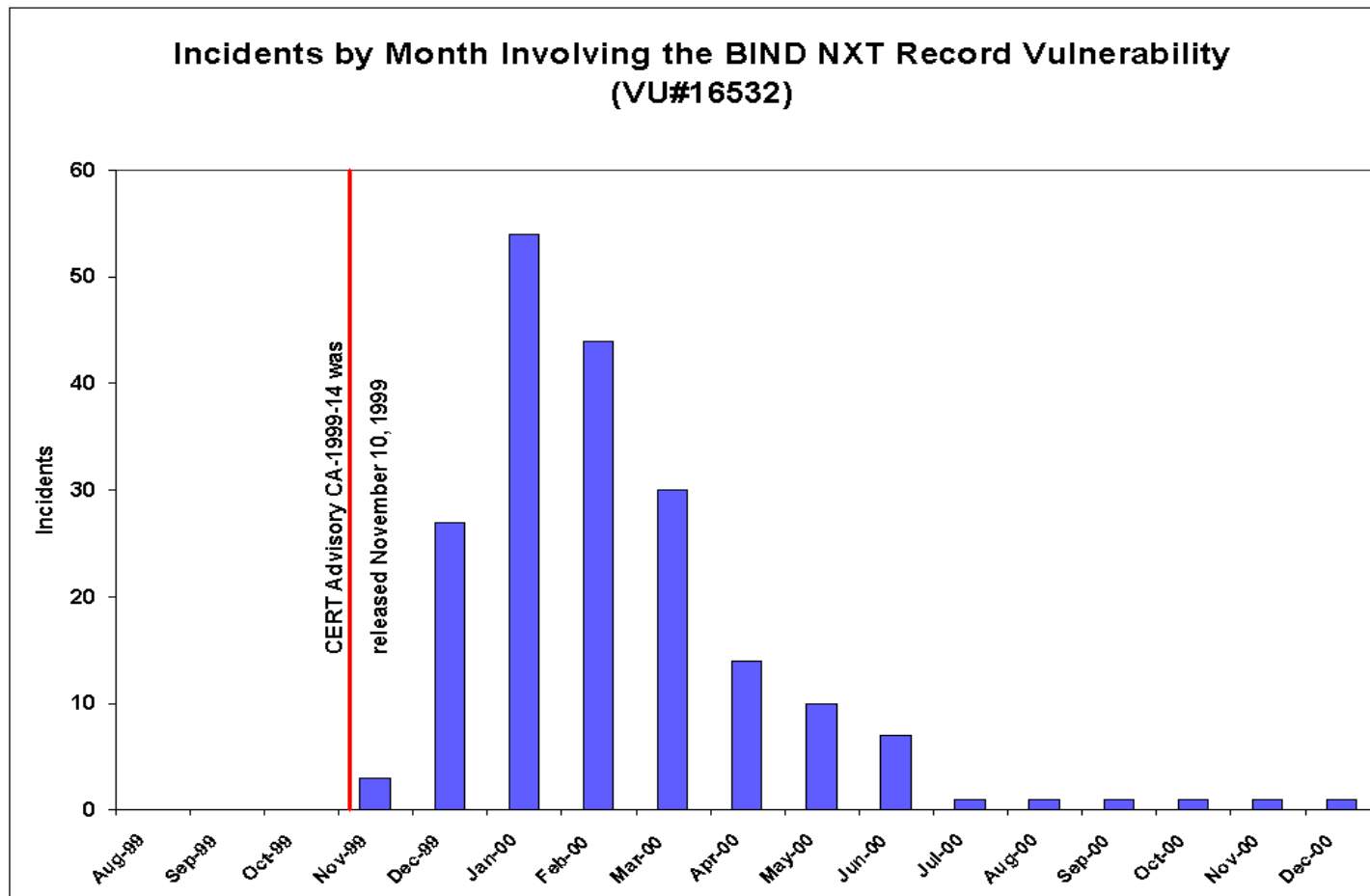
脆弱性の発見件数の推移



Securityfocus “New Vulnerabilities per Month”

<http://www.securityfocus.com/images/vdb/vperm.gif>

不正アクセス手法の流布



CERT/CC

<http://www.cert.org/advisories/CA-2001-02/nxt-history.png>

狙われる脆弱性 Top 20

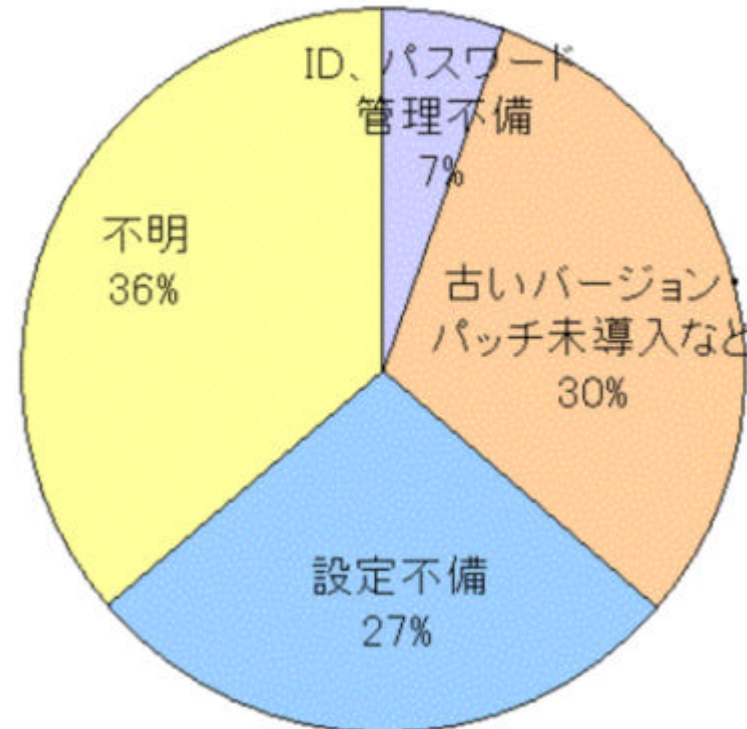
- OS, アプリケーションのデフォルトインストール
- 弱いパスワードまたはパスワード未設定
- バックアップをしていない、または不完全
- 多くのポートが開けっ放し
- パケットフィルタリングをしていない
- ログをとっていない、または不完全
- 脆弱性を持つ CGI プログラム

- Windows 関係の脆弱性 6つ
- Unix系 OS 関係の脆弱性 7つ

SANS, The Twenty Most Critical Internet Security Threats
<http://www.sans.org/top20.htm>

IPAが受け付けた被害原因の分類

2000年被害原因別分類

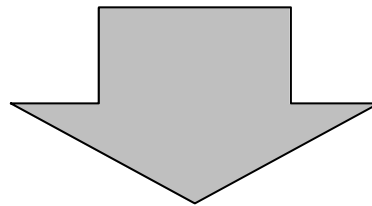


2000年一年間の不正アクセス被害届出状況 - 2.原因別分類

http://www.ipa.go.jp/security/crack_report/20010222/00all.html

現状についてのまとめ

- 不正アクセスは増加している
- ワームによる自動攻撃が多くなっている
- 狙われるのは既知の脆弱性である
- 被害原因は初歩的な不備が多い



基本的な不正アクセス対策を確実に実行し
最新のセキュリティ情報による対策を行えば
多くの被害を未然に防ぐことができる。

セキュリティ情報源

- IPA/ISEC (<http://www.ipa.go.jp/security/>)
- JPCERT/CC (<http://www.jpccert.or.jp/>)
- CERT/CC (<http://www.cert.org/>)
- SANS Institute (<http://www.sans.org/>)
- SecurityFocus (<http://www.securityfocus.com/>)
- 製品提供元のサポートサービス
 - Web、定期的なメールを利用した公開情報
- 脆弱性・攻撃に係わる情報源
 - セキュリティ対策関連のメールサービス

情報処理振興事業協会 セキュリティセンター (IPA/ISEC)

〒113-6591

東京都文京区本駒込 2 - 28 - 8

文京グリーンコートセンターオフィス 16階

TEL03 (5978)7508 FAX03 (5978)7518

ウイルス/不正アクセス相談 110番 TEL03 (5978)7509

電子メール virus@ipa.go.jp crack@ipa.go.jp

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