戦略的ネットワークセキュリティ問題対策に関する考察(1)

熊本大学総合情報処理センター

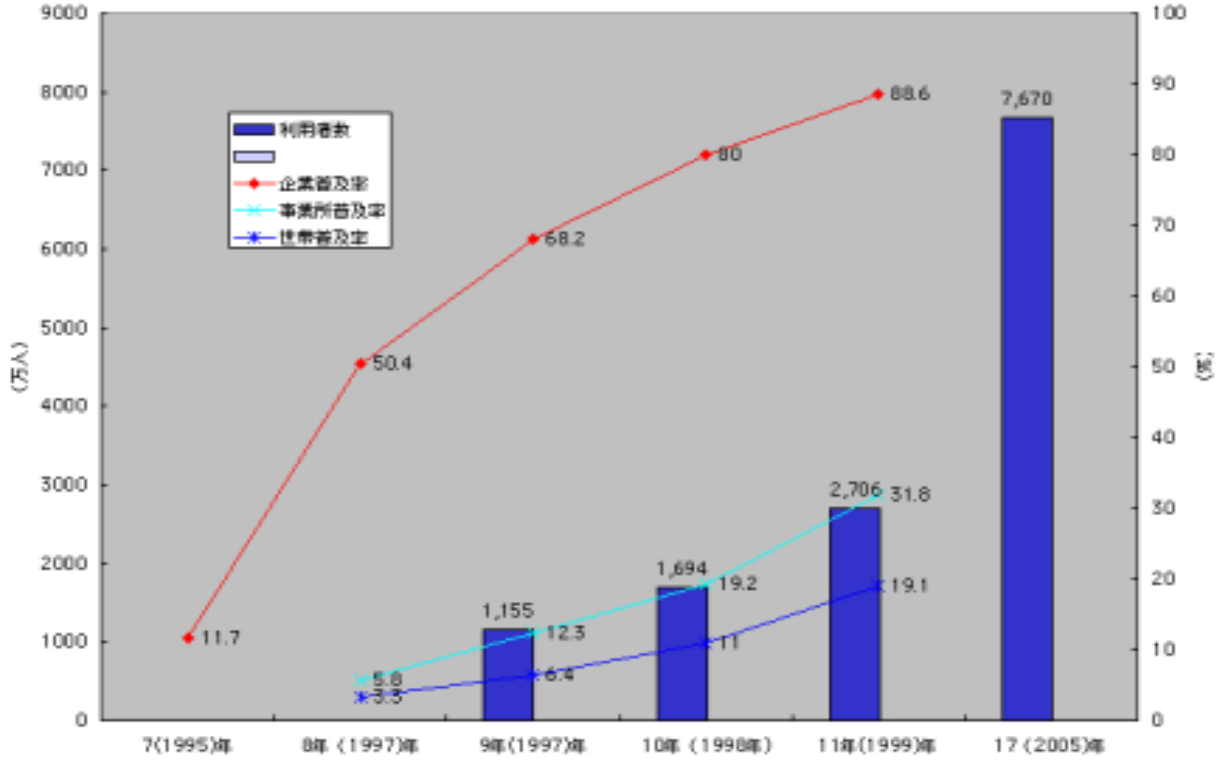
講師 武藏泰雄

今回お話しする内容は…

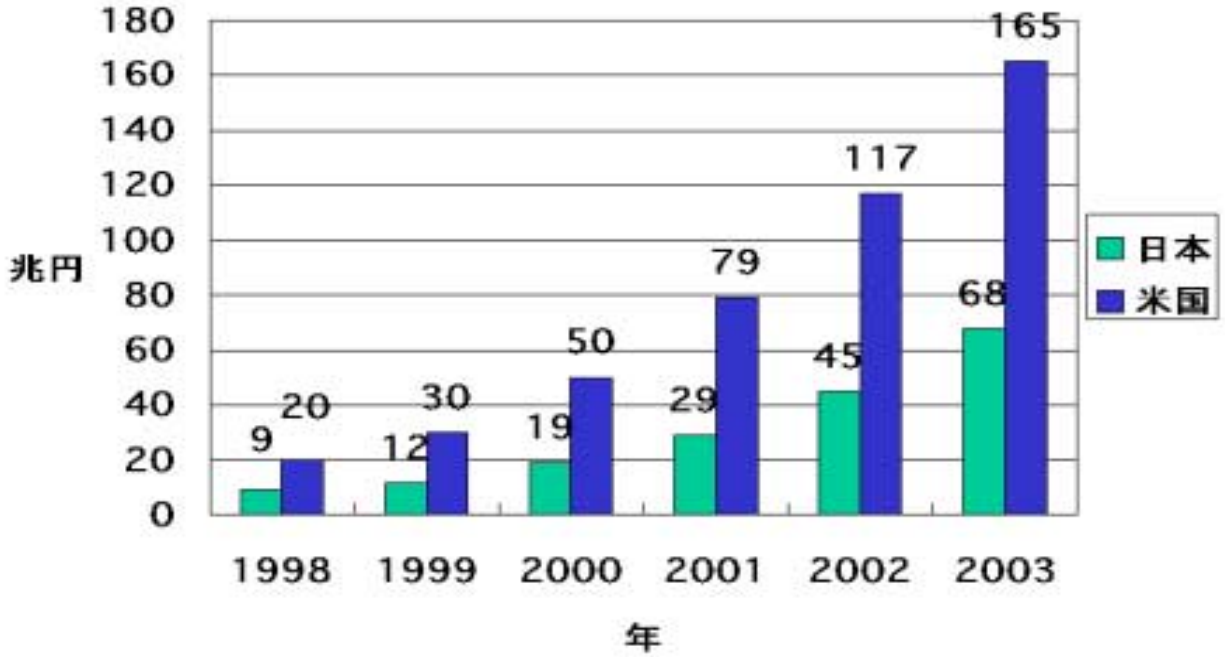
- □セキュリティに対する問題
- □セキュリティ対策の基本的な考え
- □セキュリティ対策の現状
- □これからのセキュリティ対策
- □大学におけるセキュリティの課題
- □DNSサーバにおけるIPフィルタの効果およびDNSサーバにおけるUDP(DNS)パケットのログの採集と解析の必要性
- □無線LANは安全だろうか

セキュリティに対する問題

国内におけるインターネットの普及の度合



国内電子商取引の規模


180
160
140
120
100
80
60
40
20
0
兆円
9
20
12
30
19
50
29
79
45
117
68
165
1998
1999
2000
2001
2002
2003
年
日本
米国

セキュリティ対策が重要となるのはなぜ?

インターネットへアクセスする場合は、

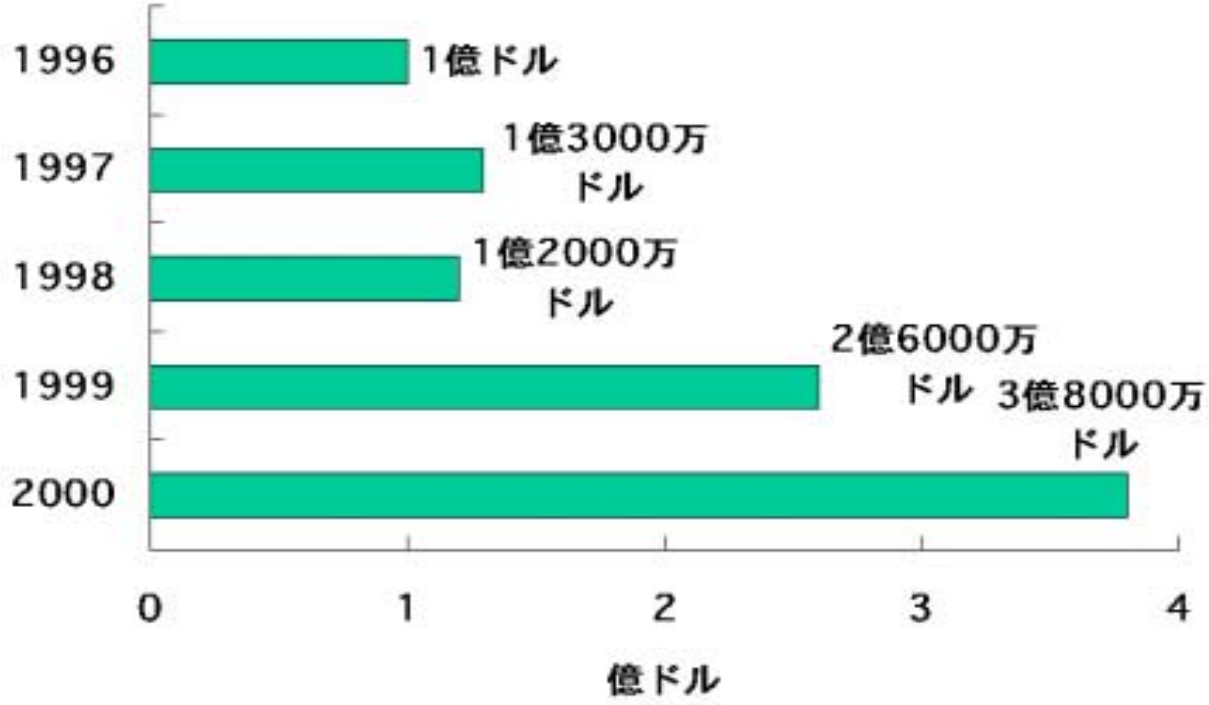
- □利用者の匿名性がある
- □監視されないところからのアクセスが可能

インターネットの急速な普及

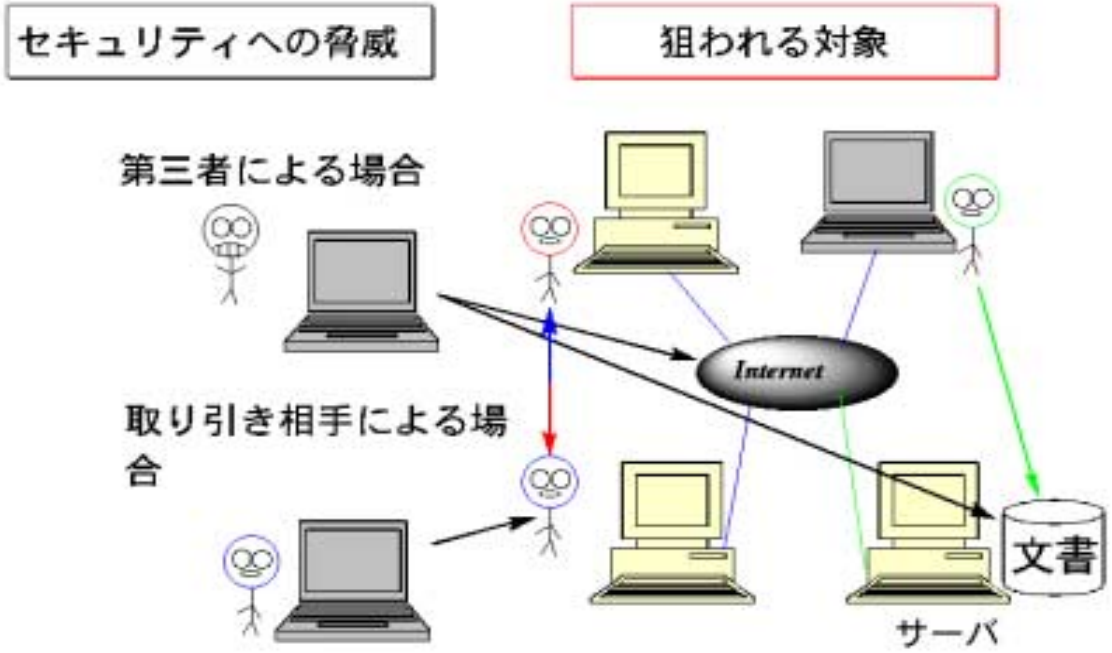
- □世界中の多様な利用者(数億人?)や運用主体の参加
- □企業の情報システムのインターネットへの依存
- □電子商取引等マネーを扱う業務の参入

セキュリティ対策はとても重要になっ

米国のネットワーク関連のセキュリティ被害総額



セキュリティへの脅威



具体的なセキュリティに対する脅威

第三者によるもの

(1) **機密性の喪失: 情報を不正に見られしまう**

(2) **完全性の喪失: 情報を不正改竄、消去、破壊される**

(3) **可用性の喪失: 不正利用によりデータやコンピュータ資源を使えなくする**

取り引き相手によるもの

(4) **証拠性の喪失: 取り引き事実や内容を不正に否認される**

(5) **原本性の喪失: 不正にコピーされる**

完全性喪失による事例

1. **医療データ改竄による殺人事件**:

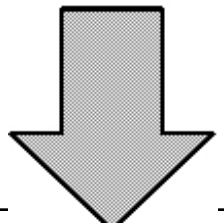
1995年オーストラリアにおいて、病院職員が勤務する病院のコンピュータに
アクセスし患者に投与すべき医薬に関するデータを改竄。看護婦が改竄された
データ通り薬をあたえたた患者が死亡した事件。

社会安全研究財団「情報セキュリティビジョン策定委員会報告書」

2. **預金額の改竄による不正送金**:

1995年ロシアのクラッカーにより米国の某銀行が、1000万ドルもの不正送金を
されてしまった事件。

山田英之「セキュリティの基礎」日経オープンシステム1998年4月号p. 258



攻撃者の種類とは?

1. **第三者(部外者)**
   (1) **クラッカー**
   (2) **スパイ**
   (3) **テロリスト**
   (4) **犯罪者(ネットワーク以外含めて)**

2. **身内(部内者)**
   (5) **職員・従業員**
   (6) **アルバイタ**

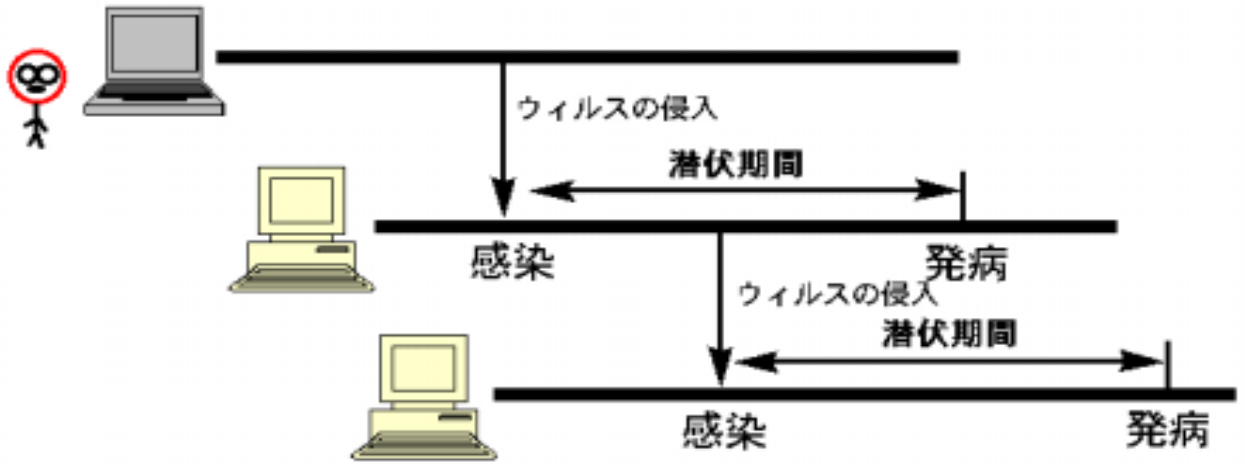
攻撃の種類は?

1. **直接的攻撃**
コンピュータを直接操作し不正アクセスを行ないネットワーク
上のファイルやデータを破壊

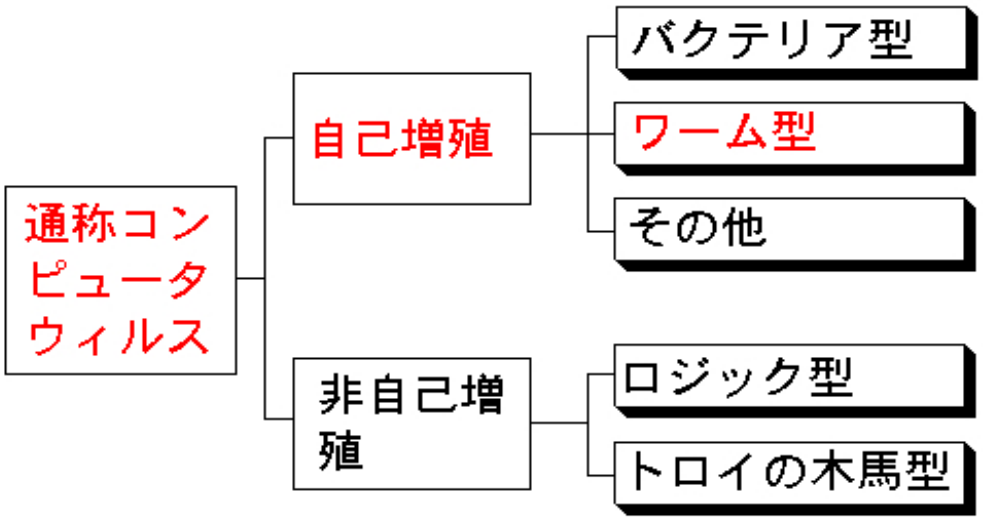
2. **間接的攻撃**
ウィルスなどのプログラムをコンピュータに送り込むことによる
ファイルなどを破壊

サイバーNGO**・軍の関与・犯罪組織やテロリスト集団による**

ウィルスの侵入と感染・発病



コンピュータウィルスの定義



PC利用者のためのウィルス対策７ヶ条

1. 最新のワクチンソフトを活用すること。
2. 万一のウィルス被害に備えるためデータのバックアップを行なうこと
3. ウィルスの兆候を見逃さず、ウィルス感染の可能性が考えられる場合はウィルス検査を行なうこと。
4. メールの添付ファイルはウィルス検査後開くこと。
5. ウィルス感染の可能性のあるファイルを扱うときは、マクロ機能の自動実行は行なわないこと。
6. 外部から持ち込まれたフロッピーディスク及びダウンロードしたファイルはウィルス検査後使用すること。
7. コンピュータの共同利用時の管理を徹底すること。

1997年8月8日 情報処理進行事業協会

メールの添付ファイルの取り扱い4つの心得

1. 見知らぬ相手先から届いた添付ファイル付きのメールは厳重注意する。テキストファイル(readme.txt)や画像ファイル(samp01.jpg)等のウィルに感染することがないファイルに見せかけた添付ファイルを送りつけるウィルスが多くなっている。ファイルの見た目に惑わされない。
2. 知り合いから届いたどことなく変な添付ファイル付きのメールは疑ってかかる。Sircam Win32などはMy Document 等のファイル名を使うので最悪な場合もある。
3. メールの本文でまかなえるようなものをテキスト形式等のファイルで添付しない。
4. 各メールソフト特有の添付ファイルの取り扱いに注意する。特に最近ではMicrosoft Outlook/Outlook ExpressとInternet Explorerの組み合わせによる問題などは有名である。

2000年6月27日 情報処理進行事業協会
セキュリティセンター・その

セキュリティ対策の基本的な考え

不正侵入・攻撃に対する主な対策

技術対策

(1) **被害発生防止**

(a) **アクセス管理制御(ネットワーク防火壁の設置で自由に入れなくする)**

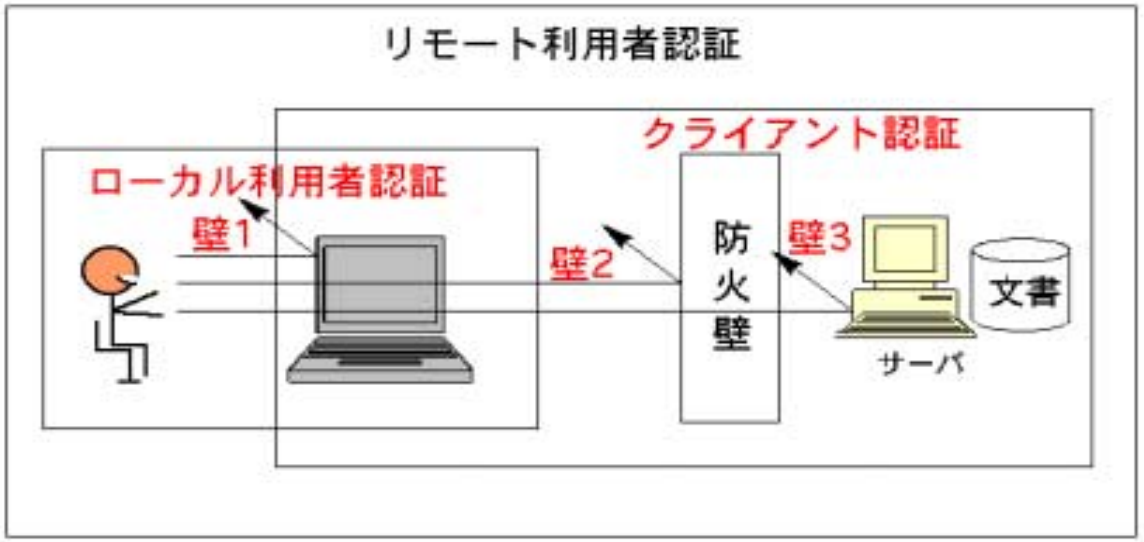
(b) **暗号化(データの不可視化)**

(2) **予防・検知・回復・セキュリティ監視等(ログの採取)**

管理対策

(3) **セキュリティポリシーの構築、運用、教育そして監査**

アクセス管理技術の概念



利用者認証の技術

本人確認(クライアント側)

- □本人の知識を利用するもの
  - ○暗証番号、パスワード、パスフレーズ等
- □本人の持ち物を利用するもの
  - ○磁気カード、ICカード、スマートカード等
- □本人の身体的特徴を利用するもの
  - ○指紋、声紋、虹彩、顔面等

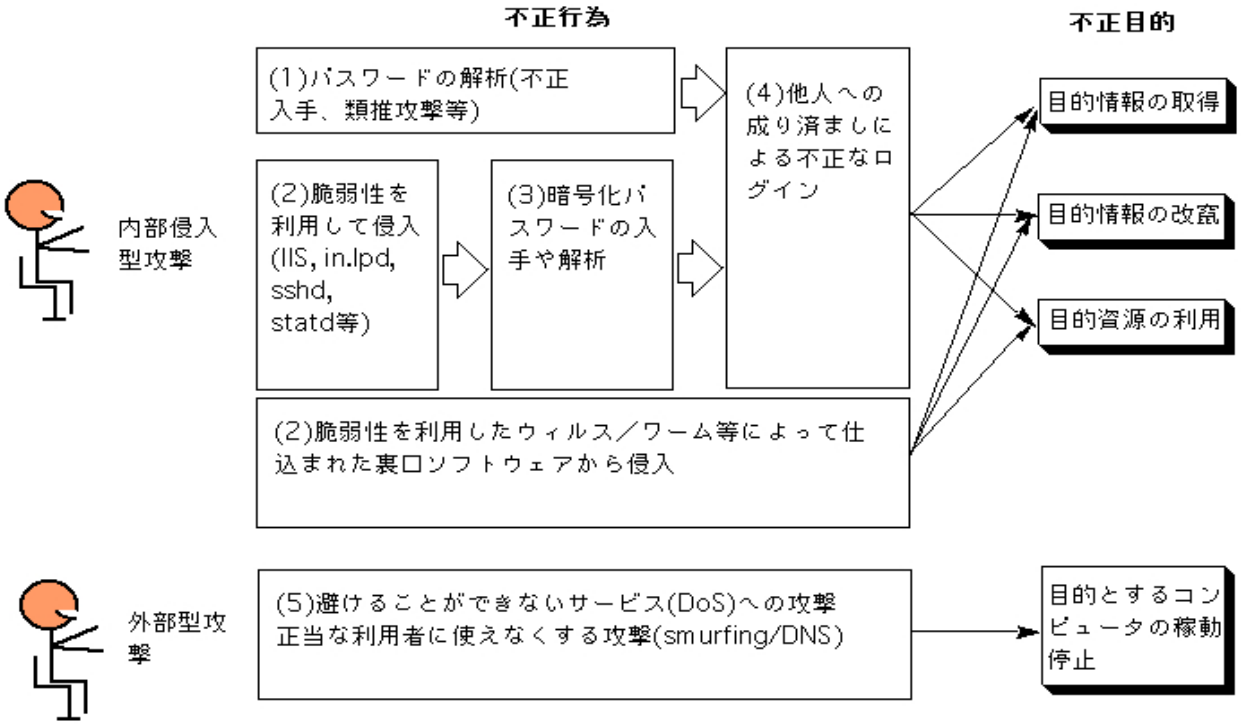
リモート利用者認証 -- 上記に第3者による認証を加える

(1) クライアントの認証結果を利用するもの

(2) 認証局を利用するもの

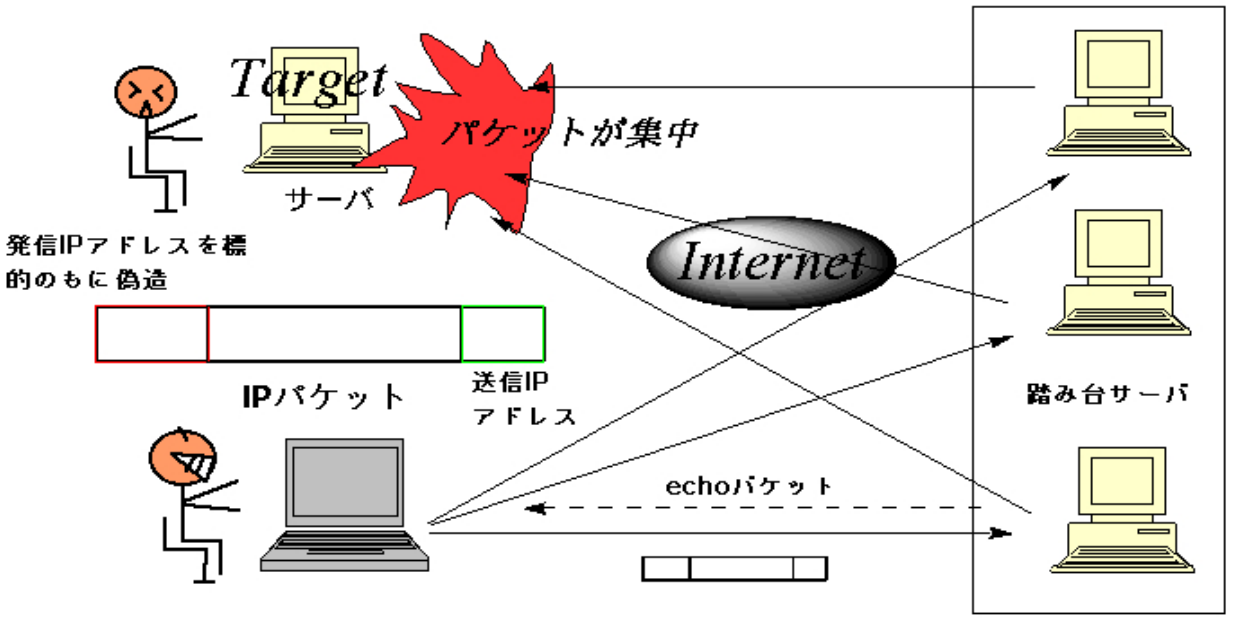
認証サーバを利用する

不正侵入の分類


不正行為
不正目的
(1)パスワードの解析(不正入手、類推攻撃等)
(2)脆弱性を利用して侵入(IIS, in.lpd, sshd, statd等)
(3)暗号化パスワードの入手や解析
(4)他人への成り済ましによる不正なログイン
(2)脆弱性を利用したウィルス／ワーム等によって仕込まれた裏口ソフトウェアから侵入
内部侵入型攻撃
外部型攻撃
(5)避けることができないサービス(DoS)への攻撃 正当な利用者に使えなくする攻撃(smurfing/DNS)
目的情報の取得
目的情報の改竄
目的資源の利用
目的とするコンピュータの稼動停止

DoS(サービス拒否)攻撃の手法

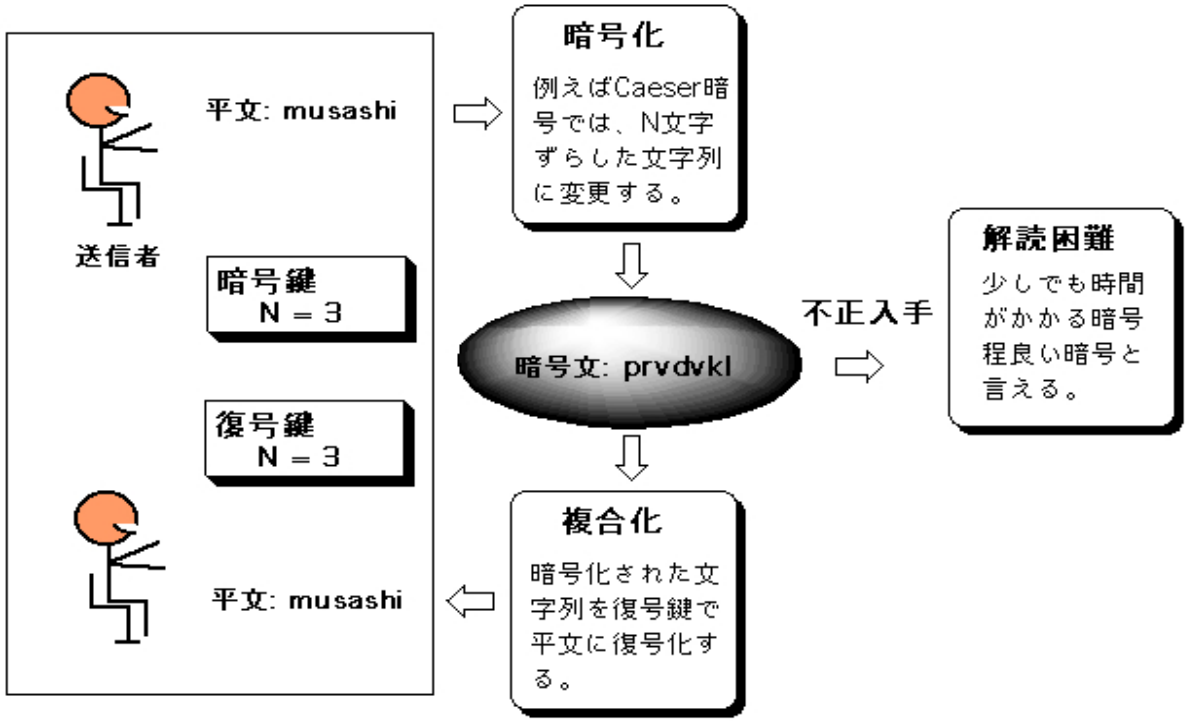
Smurf攻撃: 送信元を偽造したecho要求パケットを踏み台となった第三者のホストに送りつけ、そのecho応答パケットが標的に向かうようにする攻撃。



これらの攻撃や障害発生を防止対策

- □セキュリティホール対策のサーバプログラムへバージョンアップする。
- □利用しない/されないサーバプログラムは停止する/させる。
- □ファイアウォールの設置により、サーバへのアクセス可能な送信元ホストやプロトコルを制限する。
- □侵入検知システム(IDS)やiplogなどを用いてセキュリティ監視を行ない不正なアクセスの兆候を掴み、予防したり、誰が攻撃者かを特定する。
- □暗号化技術を用いてデータを保護する。

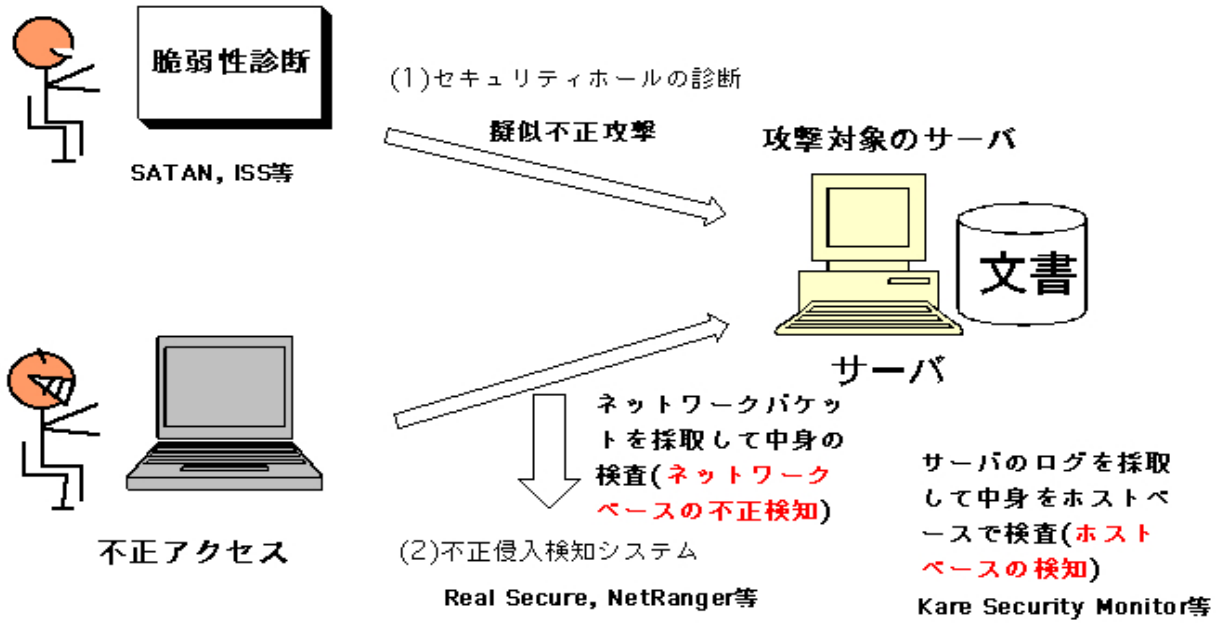
通信路暗号化


平文: musashi
送信者
暗号鍵
N = 3
復号鍵
N = 3
平文: musashi
暗号化
例えばCaeser暗号では、N文字ずらした文字列に変更する。
暗号文: prvdvkl
不正入手
解読困難
少しでも時間がかかる暗号程良い暗号と言える。
複合化
暗号化された文字列を復号鍵で平文に復号化する。

共通鍵暗号と公開鍵暗号

	共通暗号鍵型	公開暗号鍵型
方式	米国: DES 日本: EAL,MULTI	米国: RAS
暗号鍵の関係	暗号鍵 ＝ 復号鍵	暗号鍵 ≠ 復号鍵
秘密鍵の配送	必要 	不要 
安全な認証 (電子捺印・署名)	困難 	容易 
暗号化速度	高速 	低速 
用途	データの暗号化	電子捺印・署名 鍵の配布

セキュリティ監視方法

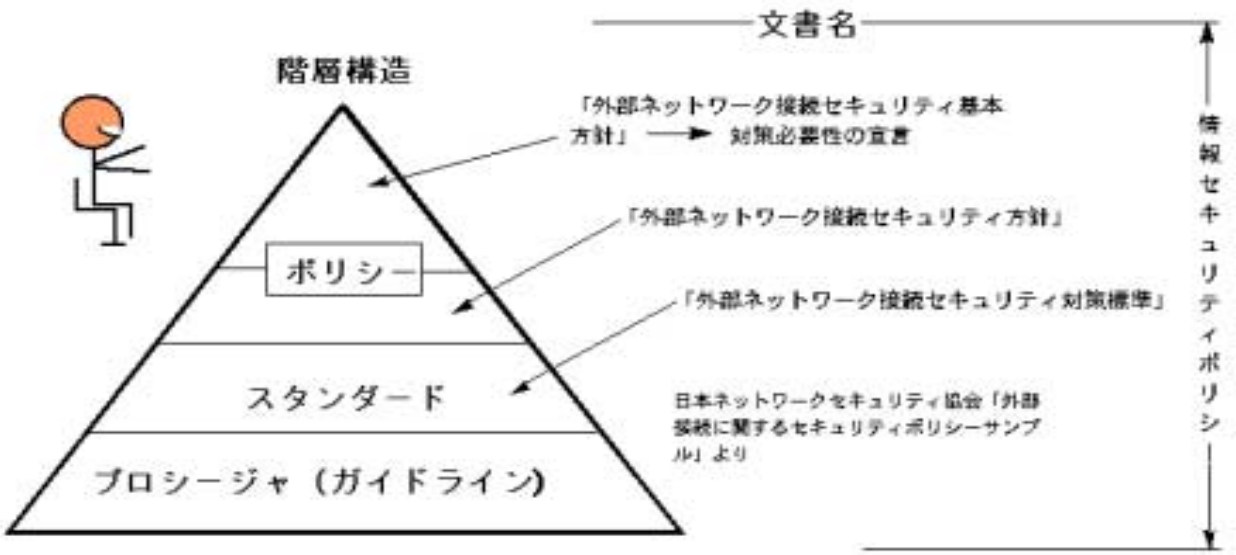

脆弱性診断
SATAN, ISS等
(1)セキュリティホールの診断
擬似不正攻撃
攻撃対象のサーバ
文書
サーバ
不正アクセス
ネットワークパケットを採取して中身の検査(ネットワークベースの不正検知)
(2)不正侵入検知システム
Real Secure, NetRanger等
サーバのログを採取して中身をホストベースで検査(ホストベースの検知)
Kare Security Monitor等

セキュリティポリシーが必要となる

□セキュリティポリシーとは?; 「組織の情報セキュリティに対するルールのことであり要件を文章化した規則集」のことである。

- ○企業の経営方針・就業規則と同様従業員に対して強制力がある。
- ○具体的に実施される情報セキュリティ対策の理由づけを提供する。
- ○各組織で独自でことなる(同業者あっても)。
- ○具体的には:
  - ▹ユーザパスワードは8文字以上の英数字、記号文字から構成する。
  - ▹重要データを格納する場合、ファイル単位で暗号化する。
  - ▹セキュリティ監査証明や証跡を文書を作成する。
  - ▹従業員は毎年情報セキュリティ合意書に署名する。

セキュリティポリシーの階層構造と文章構成



セキュリティ対策の現状は…

セキュリティ対策の現状に関する調査(警察庁)

調査主体: **警察庁**

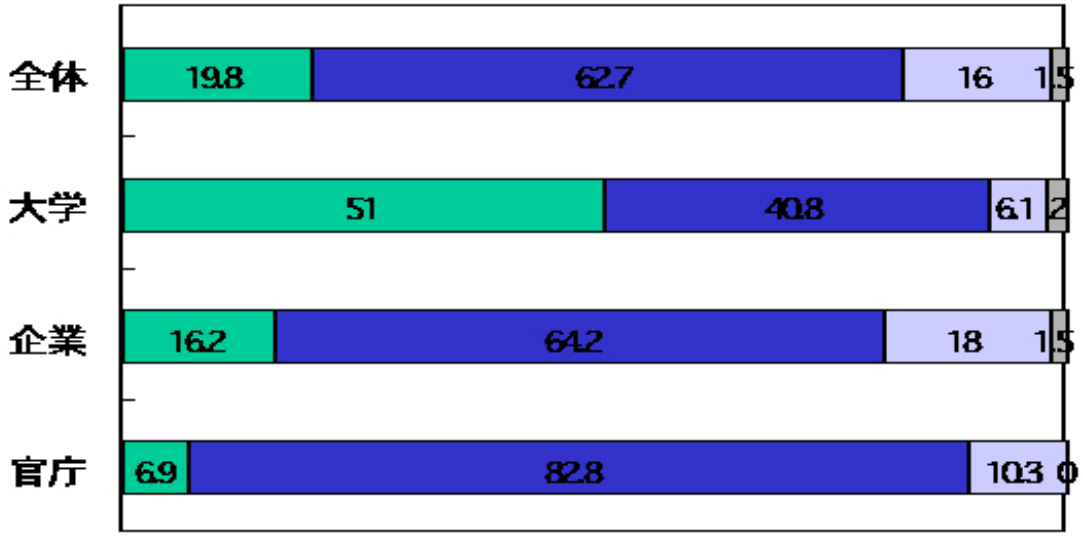
報告書: **不正アクセス対策に関するアンケート報告書**(2001年6月14日)
http://www.npa.go.jp/hightech/fusei_ac4/index.html

調査期間: 2000年10月～12月実施

調査対称および回収状況

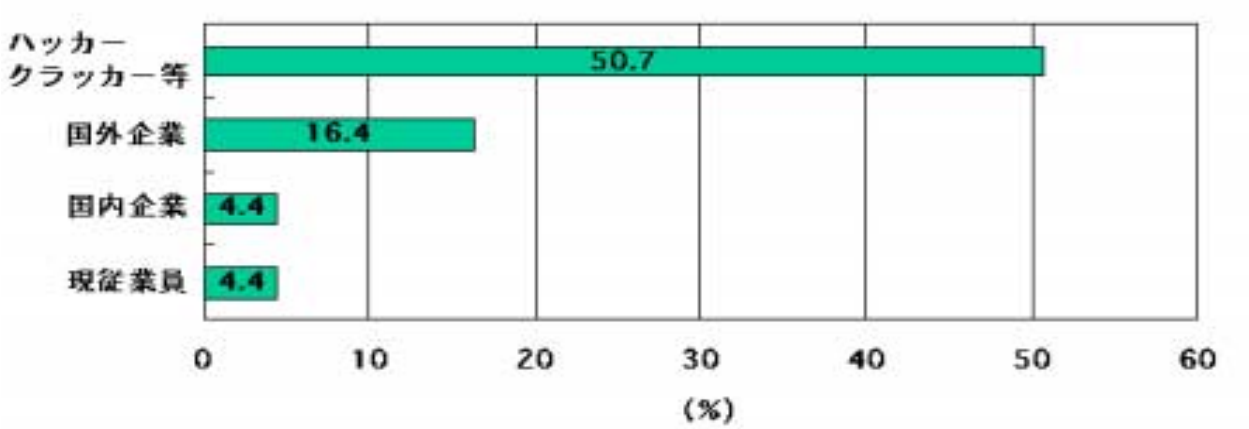
	発送件数	有効回収件数	回収率(%)
全体	1006	405	40.3
大学	100	49	49.0
企業	826	327	39.6
役所	80	29	36.3

不正アクセス被害状況



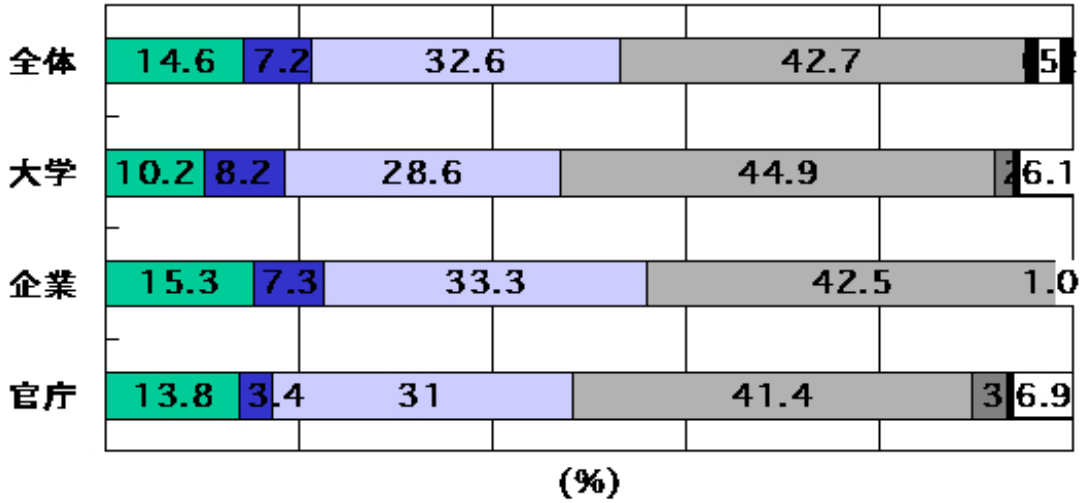
被害に遭ったものの中、ウィルスによるものが55%、
SPAM**メール不正中継が**45%**であった。**

不正アクセス行ったのは…



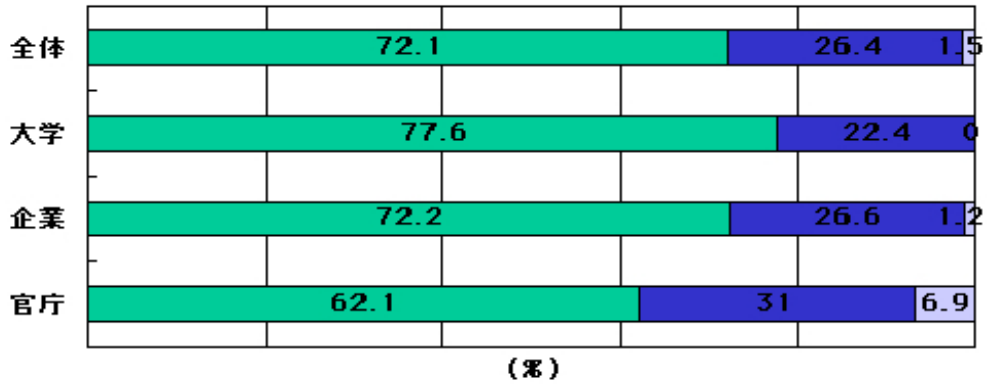
組織外からの場合が約70%であり、組織内は極端に少ない。
米国では組織内が50%と回答している場合と大きく異なる。

セキュリティポリシーの設定はしてますか?



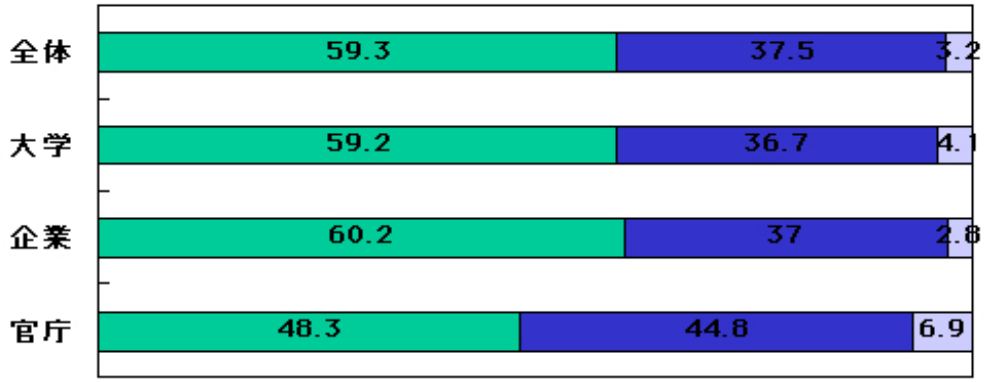
企業が多い。

ネットワークのアクセス制御対策は?



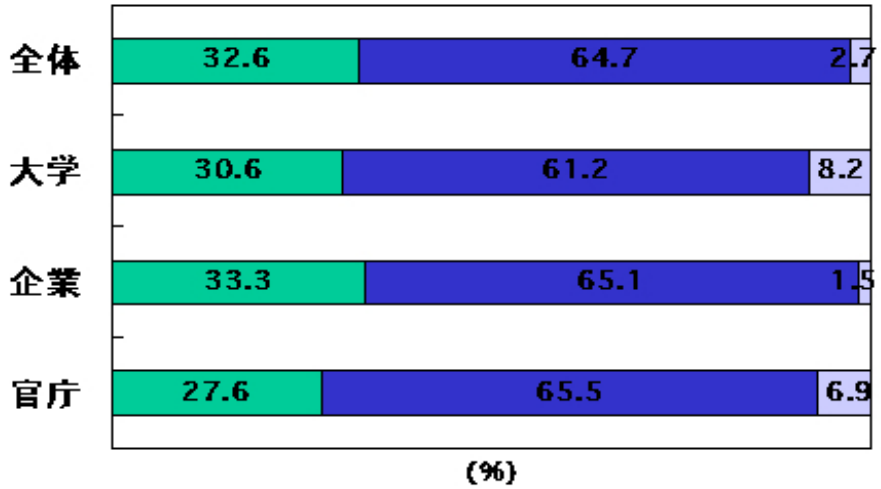
約6-7割がファイアウォールとルータによるものである。
他にプロキシサーバやコールバックによるものがある。

ファイアウォール導入の割合



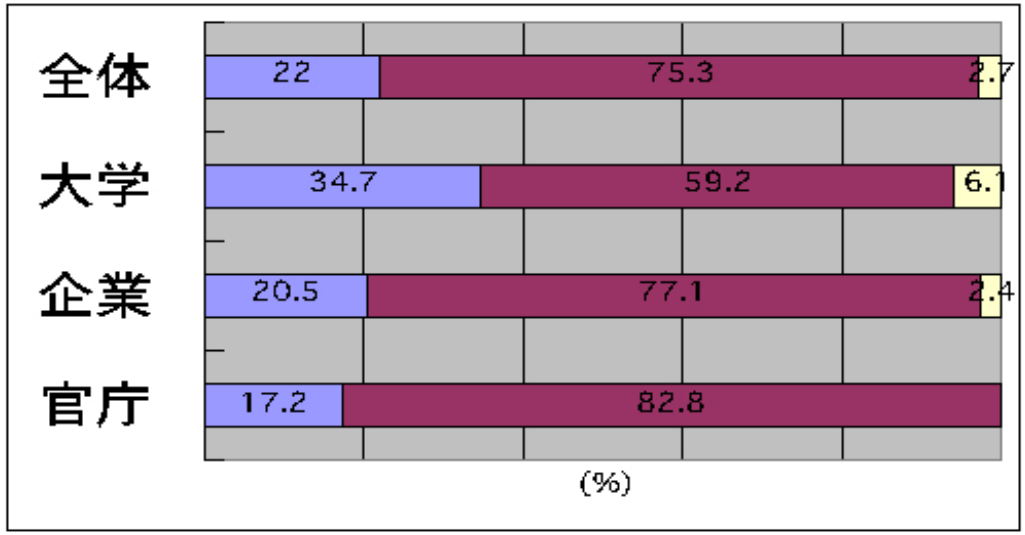
全体の6割が導入している。

不正アクセス監視・検知対策



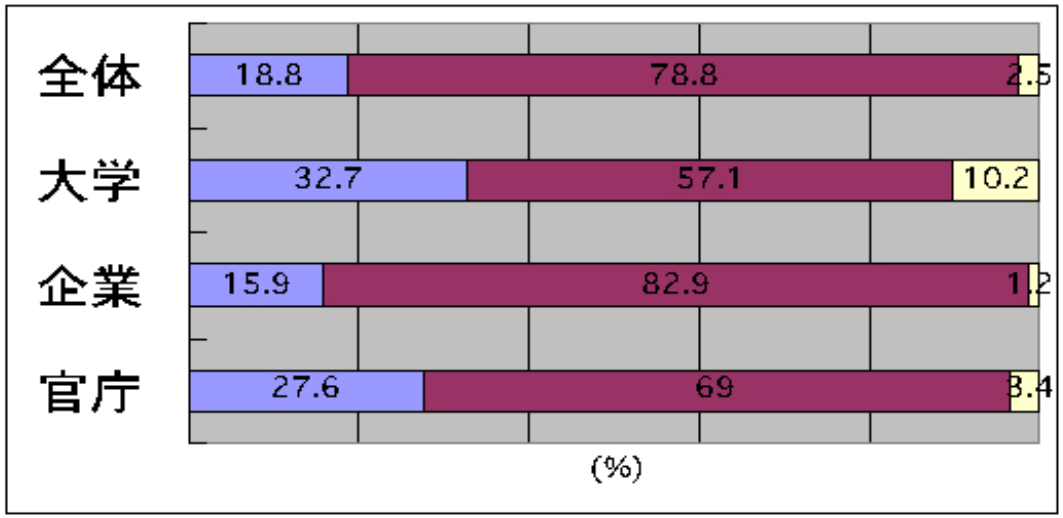
導入したものの使いこなせない、高価だ。
ちょっとしたことでもなんでも反応するのでうるさい。

暗号化対策の導入?



大学が意外と多い。メールの暗号化が多い。

セキュリティ教育の状況



大学が多い。

これからのセキュリティ技術

これからのインターネット

セキュリティ技術が支える未来

インターネット: Webなどの情報発信・メール・ニュース

イントラネット: 情報共有・グループウェア

エクストラネット: 企業間EC・広域制御

ソーシャルネット: 遠隔医療・電子投票・電子図書館・電子政府(国家)・
電子オークション・消費者EC・新しい公共社会インフラ

電子捺印・デジタル署名・透かし技術が重要。

電子捺印・デジタル署名

紙の場合:

- □契約書に捺印・目視で確認可能
- □インクで書き、いじったり消せば即座に判明

電子の場合:

- □公開鍵暗号を利用し、対応する鍵を利用していることで確認

大規模な組織におけるセキュリティの課題

セキュリティ対策における大学の特徴

不正アクセス被害に遭遇した比率は高い(一説には6割以上)
企業では、約16%(2001年6月NPA報告書)

(1) **情報システム部門にシステムを統括的に管理する権限がない場合がある。**
(2) **管理のための技術者のマンパワーが不足しがちである。**
(3) **セキュリティ対策費用が不十分である場合が少ない。**

学生は被害者になる可能性があるばかりでなく、意識しないで加害者になったり犯罪者になる可能性が強い。

これは情報倫理教育の重要性を示すものである。

不正対象と不正者の分類

不正対象:

- □学内では、センター管理、研究室管理のコンピュータやネットワーク
- □学外では、学外のコンピュータやネットワーク

不正者:

- □学内では、学生、教職員、その他
- □学外では、侵入者、クラッカー、スパイ、その他(卒業生)

学外からの侵入

大学内部部からの侵入と攻撃

(1) **データの盗み出し**

(2) **データの破壊・改竄**

(3) **ネットワークやコンピュータの無断利用**

踏み台となる(被害者ながらも加害者である)

(4) DoS**攻撃**(Land, Smurf, SPAM**メール**)

(5) **成りすまし**

発生＝損害賠償請求の可能性大

学内からの不正

内部から外部へ

(1) **不正侵入(データの盗む、データ破戒・改竄)**

(2) **他人の資源の不正利用**

(3) **プライバシー侵害**

(4) **著作権侵害**

(5) **ギャンブル・猥褻画像公開や反社会的行為・言動**

内部から内部へ….

(6) **プライバシー侵害**

(7) **著作権侵害**

(8) **目的外使用(商売に利用)**

(9) **賭博・猥褻画像公開や反社会的行為・言動**

DNSサーバにおけるパケットログとその解析の必要性

DNSサーバとは…

DNSサーバ(Domain Name Server)

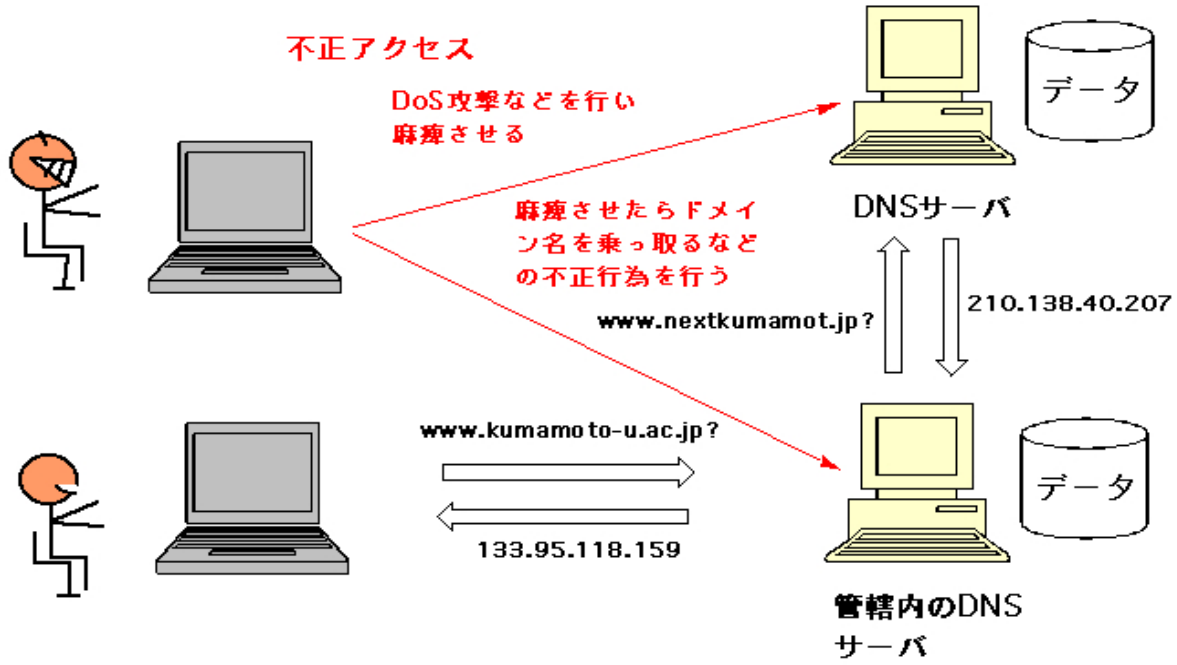
(1) ホストドメイン名とIPアドレスの対応付け行なうサーバである。
(2) 自分のホストドメイン名と管轄IPに関するテキストベースのデータベースを持っている。
(3) 管轄外のデータはすべて上流のDNSサーバへ訊ねる(クライアントとして動作。

DNSサーバのセキュリティ

(1) Webアプリなどのネットワークアプリケーションはは DNSサーバに強く依存している。
(2) Webアプリなどのプログラムはは IPアドレスで通信を確立するが、人間は、ホスト・ドメイン名で入力するので DNSサービスは必須。

DNSサーバのセキュリティ対策は重要!!

DNSサーバに対するセキュリティ攻撃



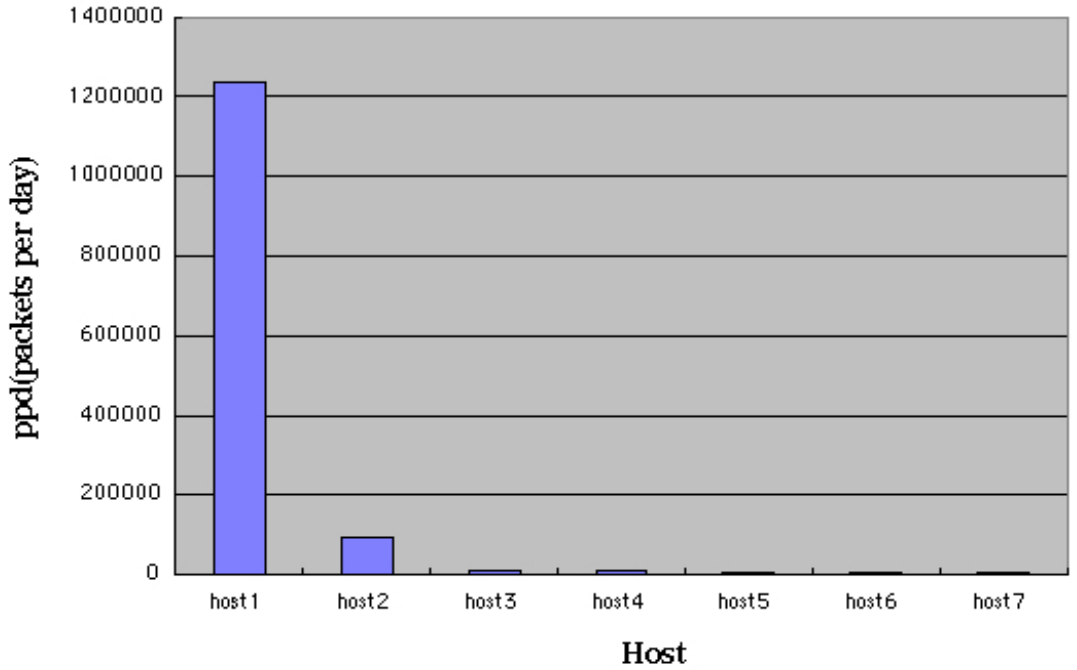
DNSサーバへどんなアクセスがあるのか?

→ パケットログの採集

対DNS-DoS攻撃の事例1

於DNSサーバ(Intel Pentium III 600E), iplogger**によるログ採集**

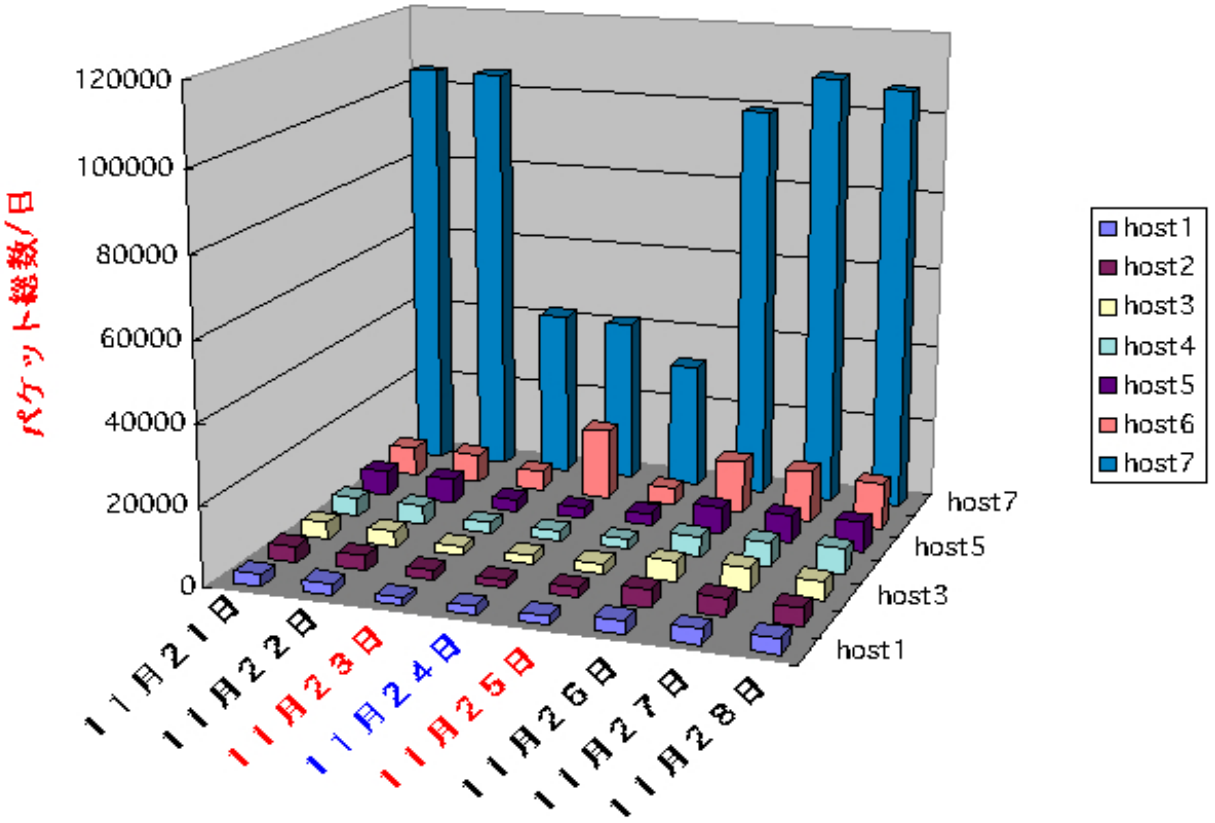
2001年9月20日～21日



攻撃が始まって二日後に気づきiptables**でIPフィルタによって防衛**
その後当該管理者へ連絡で解決、原因は不明。
その頃はNimda**がはやりはじめた頃だった。**

DoSのパケットのトップ7

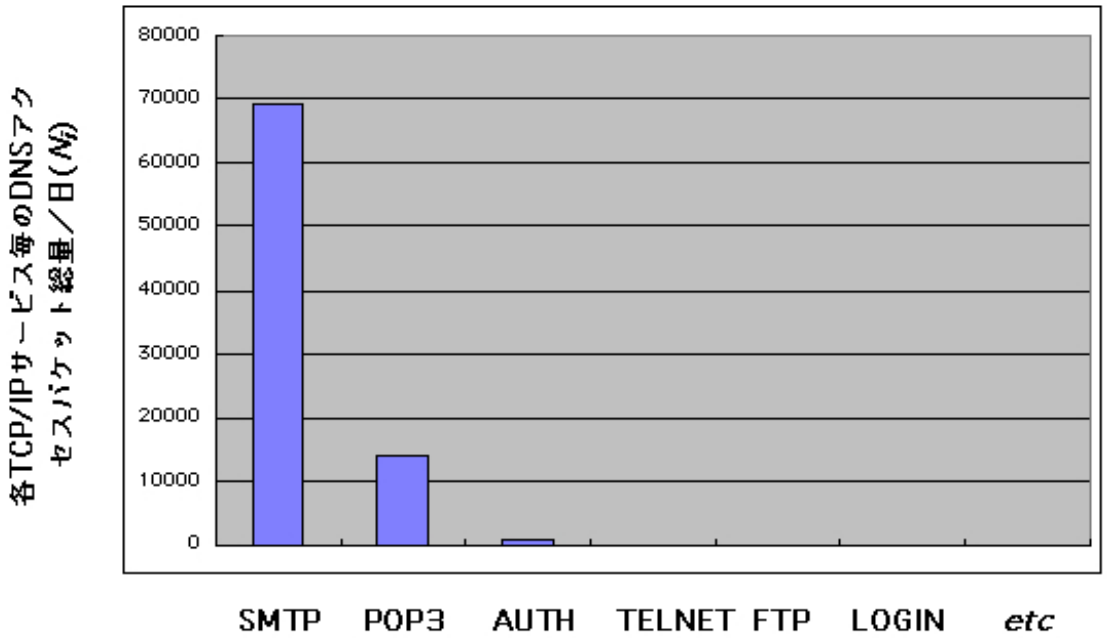
於DNSサーバ(AMD Athlon 1.4GHz), iploggerによるログ採集
2001年11月21日～28日



11月21日～23日は正常、祝日・土日はアクセス全体が減少
11月24日に第2位が約40%を占めた(学外からDoS攻撃発生)
11月25日は正常
11月26日～28日まで第2位が0.5割～1割を占めた(Win32 Aliz?)

トップのホスト1のDNSアクセスの内訳

ホスト1はメールサーバである。
下記は2001年10月24日～11月7日まで平均総量の内訳でSMTP以外のプロトコルによるものはiplogで、またSMTPは平均総量からSMTP以外のプロトコル差し引くことで求めた。



圧倒的にSMTPとPOP3によるものが多い

DNSアクセス総量と各プロトコルとの関係式

$$D_{\mathrm{q}} = \sum r_i = r_{\mathrm{SMTP}} + r_{\mathrm{POP3}} + r_{\mathrm{AUTH}} + \cdots \quad (1)$$

$$r_i = m_i N_i \quad (2)$$

r_i ：SMTPやPOP3によるDNSアクセスの総数／日

N_i ：SMTPやPOP3等のネットワークアプリケーションの総数／日

m_i：ネットワークアプリケーションあたりのDNSアクセス数／日

ところで次式(3)が成り立つと思われるので、

$$r_{\mathrm{SMTP}} + r_{\mathrm{POP3}} >> r_{\mathrm{AUTH}} + \cdots \quad (3)$$

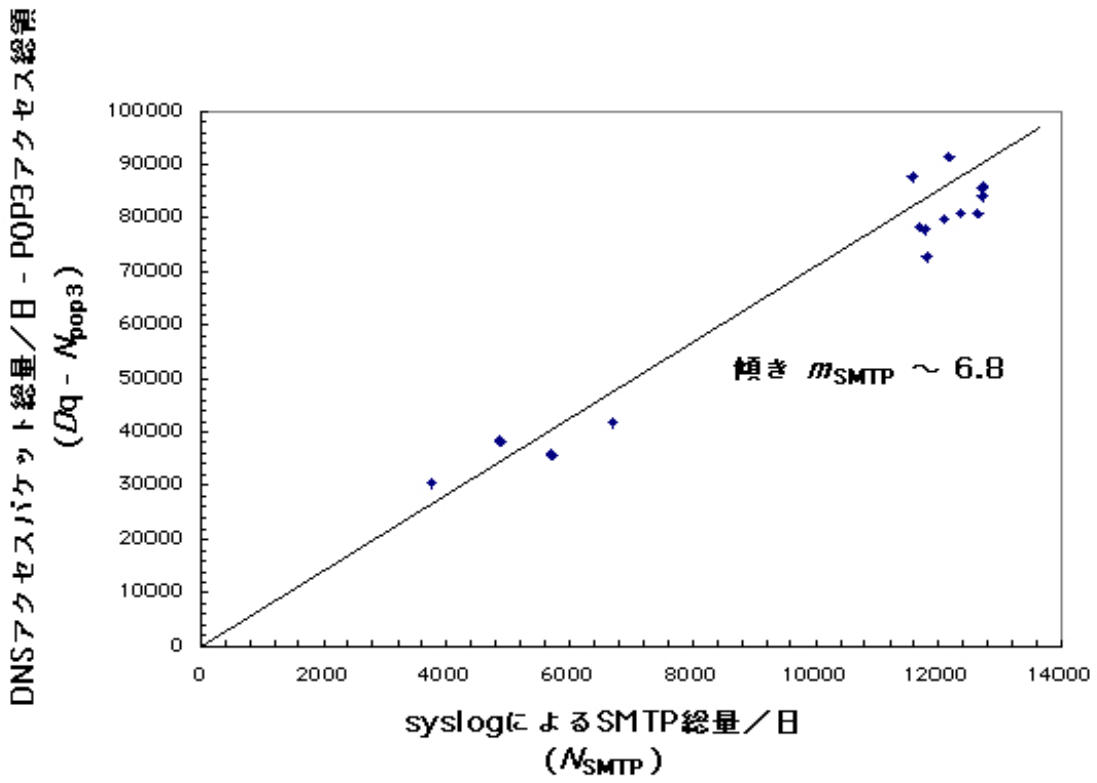
$$D_{\mathrm{q}} \sim r_{\mathrm{SMTP}} + r_{\mathrm{POP3}} \sim m_{\mathrm{SMTP}} N_{\mathrm{SMTP}} + m_{\mathrm{POP3}} N_{\mathrm{POP3}}$$

調査すると、m_{SMTP} = 3.0～4.0およびm_{POP3} = 1.0なので、

$$D_{\mathrm{q}} \sim m_{\mathrm{SMTP}} N_{\mathrm{SMTP}} + N_{\mathrm{POP3}} \quad (4)$$

$$D_{\mathrm{q}} - N_{\mathrm{POP3}} \sim m_{\mathrm{SMTP}} N_{\mathrm{SMTP}} \quad (5)$$

DNSアクセス総量とSMTP総量の関係



DNSアクセス総量とsyslogから得られたSMTP総量の間に相関がある

DNSサーバのログ解析の結論

今回の解析でわかったこと

(1) **ウィルスやワームが動作すると**DNS**アクセスが激しくなる傾向がある。**

(2) DNS**アクセス総量と**syslog**から得られた**SMTP**総量の間に相関がある**

上記の結果を用いて展開される新たな課題

(3) **各部署のネットワークサーバは**DNS, SMTP/POP3, HTTPD**などいろいろ動作しているが、**(2)**の結果からそのサーバがメールサーバとして動いているかどうかがわかるだろう。更に言い換えるなら、メールサーバが正常に動いているかどうか判定できる。**