ネットワークセキュリティ

第3回：情報セキュリティへの脅威

2017年10月18日

情報アーキテクチャ学科
稲村　浩

本日の講義　　教科書　第2章

（２．１　情報セキュリティとは）

２．２　攻撃手法

２．３　セキュリティ対策の分類

情報セキュリティに対する攻撃

1. 不正アクセス（侵入者）
2. 盗聴
3. サービスの妨害
4. コンピュータウィルス

コンピュータへの不正侵入

- コンピュータ内の目的とする情報の取得や改竄

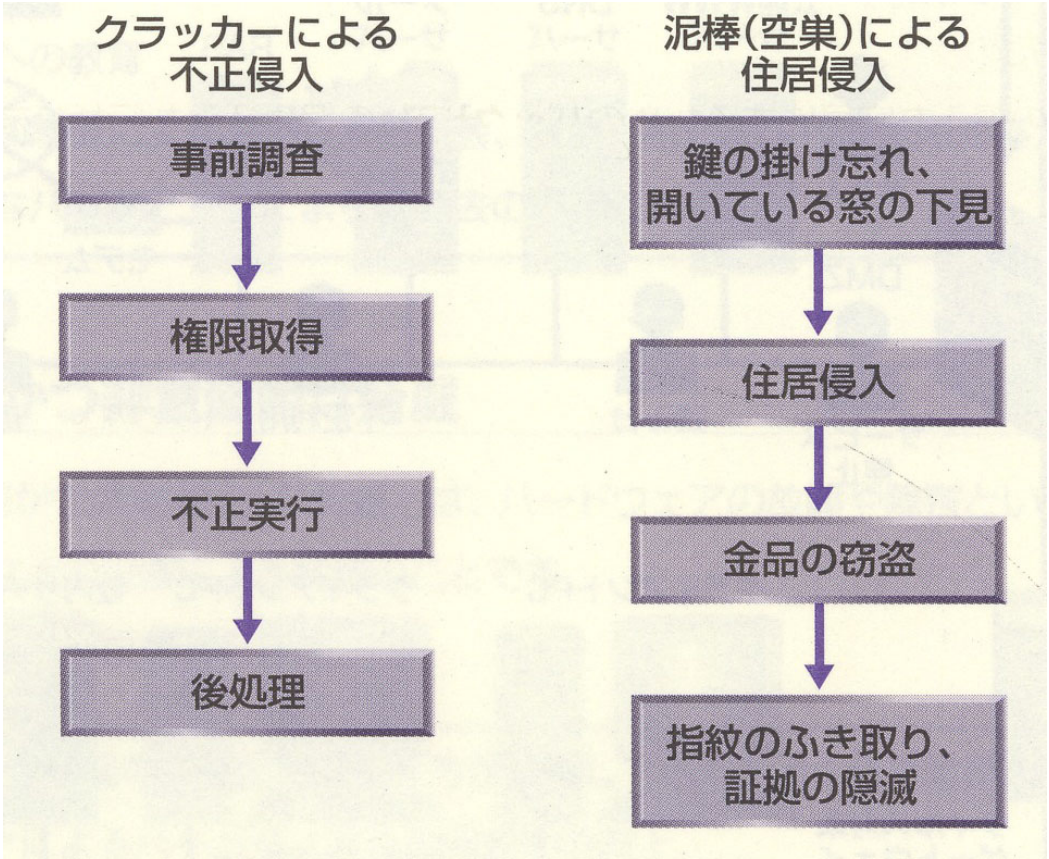
- 例）

  - 個人情報の漏洩，口座情報や取引内容の不正な変更

  - 侵入口（バックドア）の組込み，トロイの木馬によるアカウント情報やパスワード等の取得

侵入の手順

- 「事前調査」,「権限取得」,「不正実行」,「後処理」の段階からなる



事前調査

- スキャン
- ドメイン名やIPアドレスを最初の手がかりに，ファイアウォールやOSの種類，サーバソフトウェアの種類とバージョン，ネットワーク構成等を調べ，脆弱性を探る

スキャン

- **アドレススキャン**

  ドメイン名，whoisデータベースで得られるIPアドレスを最初の手がかりにして，周辺のアドレスにpingコマンドを実行し，接続可能なホストのIPアドレス一覧を作成

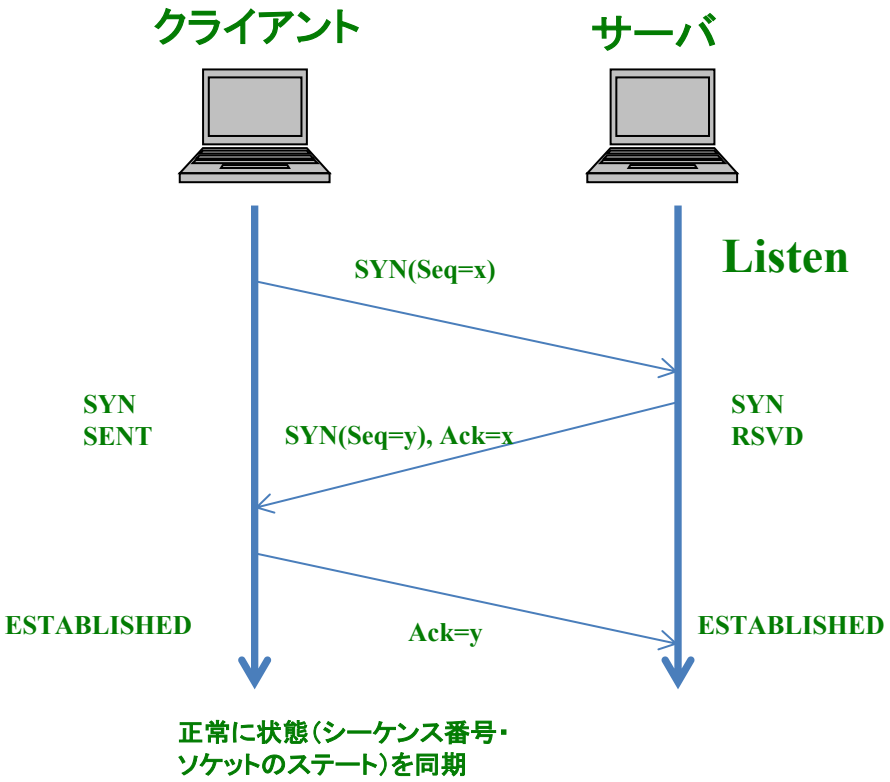
- **ポートスキャン**

  ターゲットとするサーバのポートに対してTCP/IPを利用して，サービス/アプリケーション，OSの種類を調査

スキャン行為自体は，不正アクセス行為には含まれず違法ではない

Port scanの原理

- あるポート番号に対応するサーバの有無の確認
- 確認方法



- ポートに対してListen状態のソケットの有無は普通にconnectしてみればわかる
- TCPのシーケンスの途中までやってみる．SYNを送るとACK+SYNが返ってくることでわかる
- いい加減なフラグを立てたパケットを送るとRSTパケットが返ってくる – OSの種類がわかる
- Etc.

権限取得

- パスワードを不正に入手，認証を回避する不正プログラムによりサーバ等の利用権限を不正に入手

- パスワードクラック，バッファオーバフロー，セキュリティフォール，など

パスワードクラック

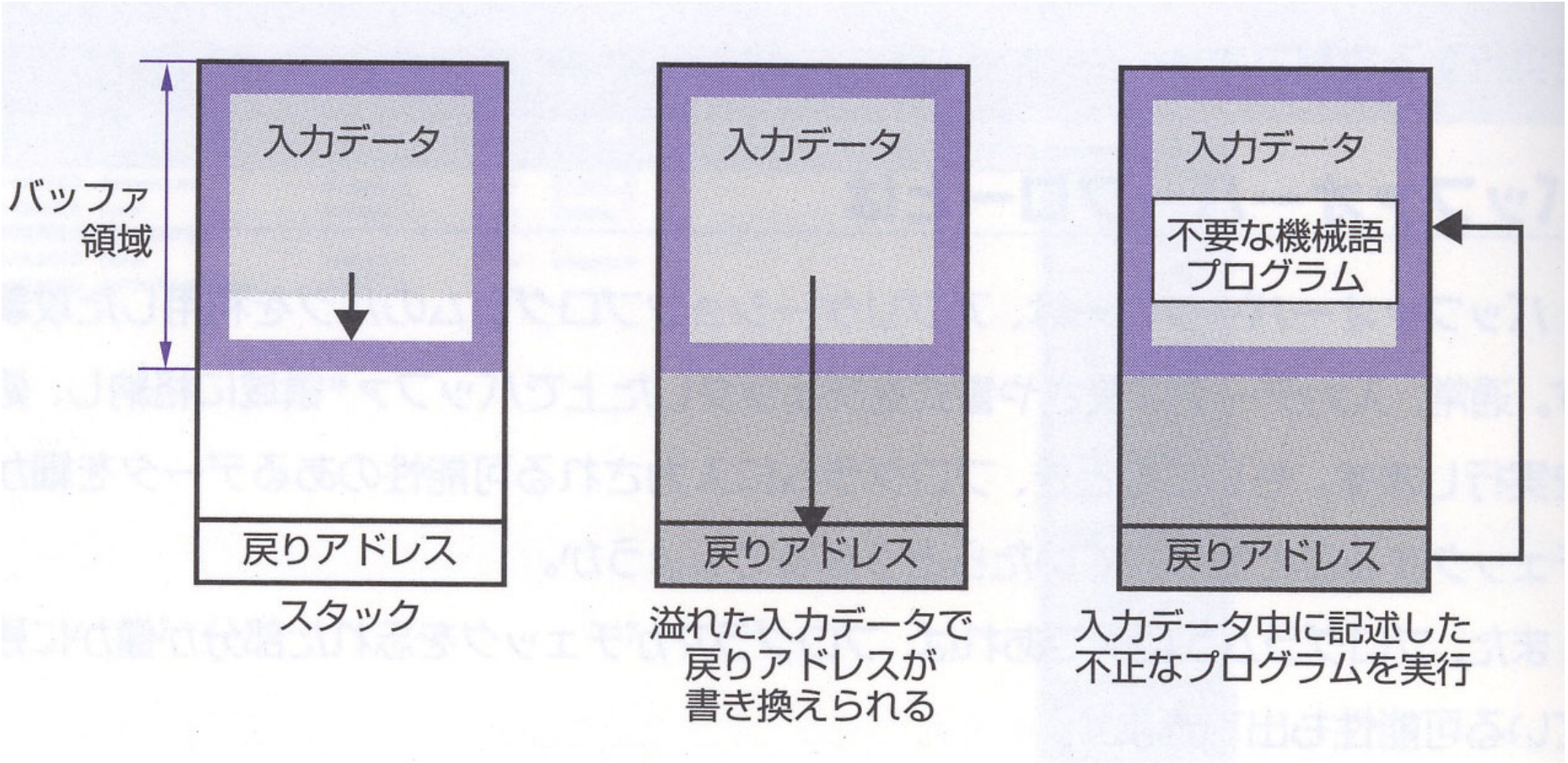
- **総当たり攻撃（ブルートフォースアタック）**
  時間さえあれば確実に取得可能
  例）アルファベット大，小文字と数字８文字の場合
  62^8=218,340,105,584,896通り
- **辞書攻撃**
  単語，固有名詞，よく使われるユーザ名などを利用
- **盗聴（後述）**

バッファオーバフロー

- アプリケーションプログラムのバグを利用して，メモリ領域に確保されたバッファを超えてデータを書き込むことで不正なプログラムを実行する

- バッファ領域にあるスタックには，関数やサブルーティンが終了した後の「戻り（再開地点）アドレス」を，オーバフローさせて不正に書き換えることによりシステムを乗っ取る

バッファオーバフローの原理



セキュリティホール/脆弱性

- OS，Webブラウザ，メールソフトなどの欠陥を利用して，外部から不正なプログラムを実行

- 例

  1)Webサーバが不正な文字列を含んだURLを受取ると，公開していないファイルのアクセス　が可能となる

  2)メールサーバが悪意を持って作成されたメールアドレスを含むメールを受取ると管理者権限を取得可能

脆弱性

- 情報セキュリティ(機密性,完全性,可用性)に関わる 情報システムあるいはそれを扱う人間や組織の弱点
- 対応する脅威の発生によってインシデントを 引き起こすもの.

- ■脆弱性の分類
  - (1)技術的脆弱性
  - (2)人間や組織(企業)の脆弱性

脆弱性届出制度

- 技術的脆弱性を社会で管理する仕組み
- 2004年7月：ソフトウェア等脆弱性関連情報取扱基準（経産省）で情報処理推進機構（IPA）が受付機関，JPCERT/CCが製品開発者との調整機関として指定
- 製品の脆弱性対応状況を公開JVN （http://jvn.jp/）

JVN Japan Vulnerability Notes

最終更新日：2016/10/11
English

共通脆弱性評価システム CVSS v3 による評価採用のお知らせ

過去のお知らせ

新着リスト

RSS

JVN#39619137:	FlashAir におけるアクセス制限不備の脆弱性 [2016/10/11 17:00]（更新）
JVNVU#91754464:	iOS 版「U by BB&T」に SSL サーバ証明書の検証不備の脆弱性 [2016/10/11 11:10]
JVN#32504719:	Usermin におけるクロスサイトスクリプティングの脆弱性 [2016/10/07 12:00]
JVN#80157683:	SetucoCMS における複数の脆弱性 [2016/10/07 12:00]
JVN#20786316:	Cryptography API: Next Generation (CNG) におけるサービス運用妨害 (DoS) の脆弱性 [2016/10/07 12:00]
JVN#85336306:	複数製品で使用されている International Components for Unicode (ICU) に解放済みメモリ使用 (use-after-free) の脆弱性 [2016/10/06 10:00]
JVN#70739377:	複数製品で使用されている International Components for Unicode (ICU) にサービス運用妨害 (DoS) の脆弱性 [2016/10/06 10:00]
JVNVU#95089754:	Animas OneTouch Ping に複数の脆弱性 [2016/10/05 18:30]
JVN#11288252:	サイボウズ Office における意図しないファイルをダウンロードさせられる脆弱性 [2016/10/03 12:00]
JVN#10092452:	サイボウズ Office におけるサービス運用妨害 (DoS) の脆弱性 [2016/10/03 12:00]
JVN#09736331:	サイボウズ Office における情報漏えいの脆弱性 [2016/10/03 12:00]
JVN#08736331:	サイボウズ Office におけるメールヘッダインジェクションの脆弱性 [2016/10/03 12:00]
JVN#07148816:	サイボウズ Office における複数のアクセス制限不備の脆弱性 [2016/10/03 12:00]
JVN#06726266:	サイボウズ Office における複数のクロスサイトスクリプティングの脆弱性 [2016/10/03 12:00]
JVN#46351856:	L-04D におけるクロスサイトリクエストフォージェリの脆弱性 [2016/10/03 12:00]

脆弱性レポート一覧

Status Tracking Notes

JVNTR-2011-05:	Apache HTTPD サーバにサービス運用妨害 (DoS) の脆弱性 (CVE-2011-3192, JVNVU#405811) [2011/09/01] (New)
JVNTR-2010-23:	Microsoft Windows における DLL 読み込みに関する脆弱性 (TA10-238A) [2011/03/14]
JVNTR-2011-02:	Java Double.parseDouble にサービス運用妨害 (DoS) の脆弱性 (通称、"2.2250738585072011e-308" の問題) (CVE-2010-4476) [2011/03/13]
JVNTR-2011-01:	マイクロソフト Graphics Rendering Engine の脆弱性 (CVE-2010-3970, JVNVU#106516) [2011/01/23]
JVNTR-2010-26:	Apple Quicktime における複数の脆弱性に対するアップデート (CVE-2010-1818, JVNVU#997815) [2010/09/23]

JVN
HOME
JVNとは
脆弱性レポートの読み方
脆弱性レポート一覧
VN-JP
VN-JP (連絡不能)
VN-VU
TA
TRnotes
JVN iPedia 脆弱性対策情報データベース
MyJVN
JVNJS/RSS
ベンダ情報一覧
連絡不能開発者一覧
脆弱性情報の届出
お問合せ先
サイト運営組織
JPCERT/CC JPCERTコーディネーションセンター
IPA/ISEC 情報処理推進機構セキュリティセンター
早期警戒パートナー
JEITA 社団法人電子情報技術産業協会
JISA 社団法人情報サービス産業協会
CSAJ 社団法人コンピュータソフトウェア協会
JNSA NPO日本ネットワークセキュリティ協会
関連組織
CERT/CC
CPNI

CVE COMPATIBLE

ソフトウェア等の脆弱性関連情報に関する届け出状況（2016年第2四半期現在, IPA）

表1-1. 届出件数

分類	今期件数	累計件数
ソフトウェア製品	690 件	3,162 件
ウェブサイト	63 件	9,263 件
合計	753 件	12,425 件

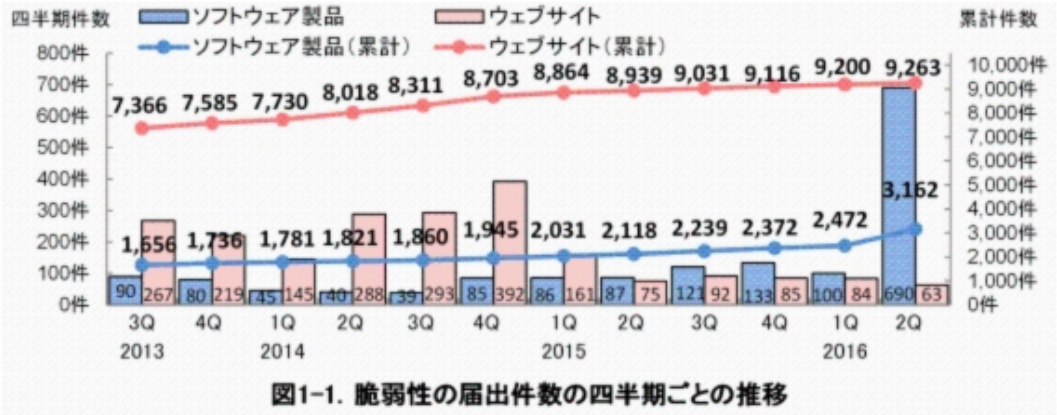


図1-1. 脆弱性の届出件数の四半期ごとの推移

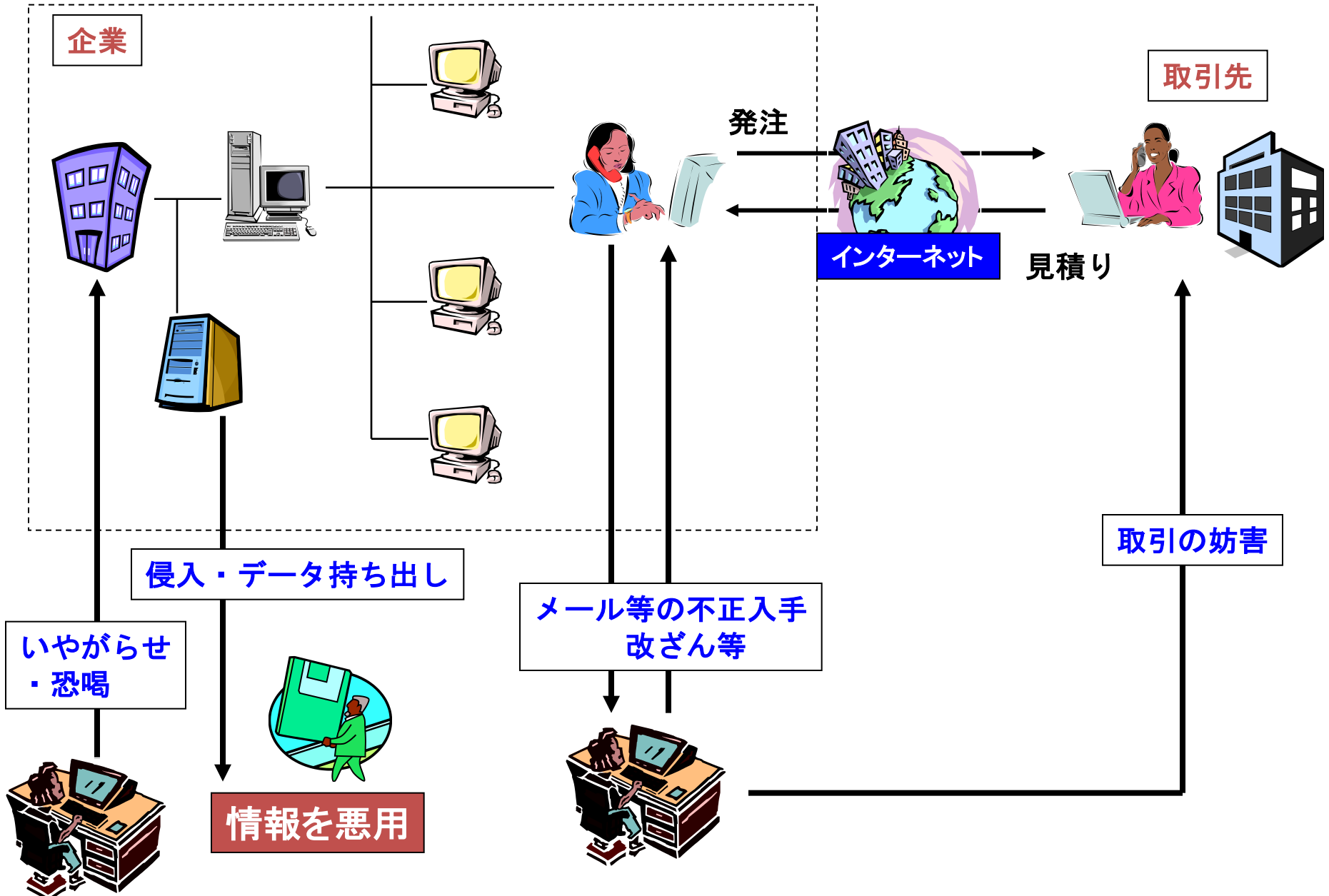
表1-2. 届出件数（過去3年間）

	2013		2014				2015				2016	
	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q
累計届出件数[件]	9,022	9,321	9,511	9,839	10,171	10,648	10,895	11,057	11,270	11,488	11,672	12,425
1就業日あたり[件/日]	4.00	4.03	4.01	4.04	4.07	4.16	4.16	4.13	4.11	4.11	4.17	4.26

不正実行

- 破壊，消去，改竄，データの不正入手，盗聴
- サービス停止攻撃，盗聴，リソース不正利用，SQLインジェクション，クロスサイトスクリプティング，など

不正侵入によるデータ漏洩・改ざん



なりすましによるパソコンの不正使用

利用者本人

①会議・出張等
による離席

誰にでも利用
できる状態

③混乱

この決済は何？

あれ？受注日が今ごろ変更？

混乱

業務に関係ないサービスの
利用が多いな。

権限のない利用者

②なりすまし

ID/パスワードの不正入手

盗聴

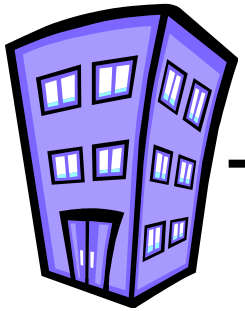
- ネットワーク上を流れる自分宛以外のデータを傍受

  - パケットモニタリングツール等を利用

- パソコンの盗難，等

パソコンの盗難による被害

従業員や搬送業者の
ふりをして持ち出し



社外での
置き忘れ、盗難

データを解読

機密情報の売買

顧客データ／取引
データ／商談情報
の漏洩による不利益

設備・資産の損失

恐喝

持ち出されないための施錠や,
データを解読させない策が必要

サービスの妨害：DoS攻撃

- DoS（Denial of Service)攻撃

  サービスを一時的に利用不能とする

  - SYN Flood攻撃：TCPコネクションの確立用パケット(SYNパケット）を大量に送りつける

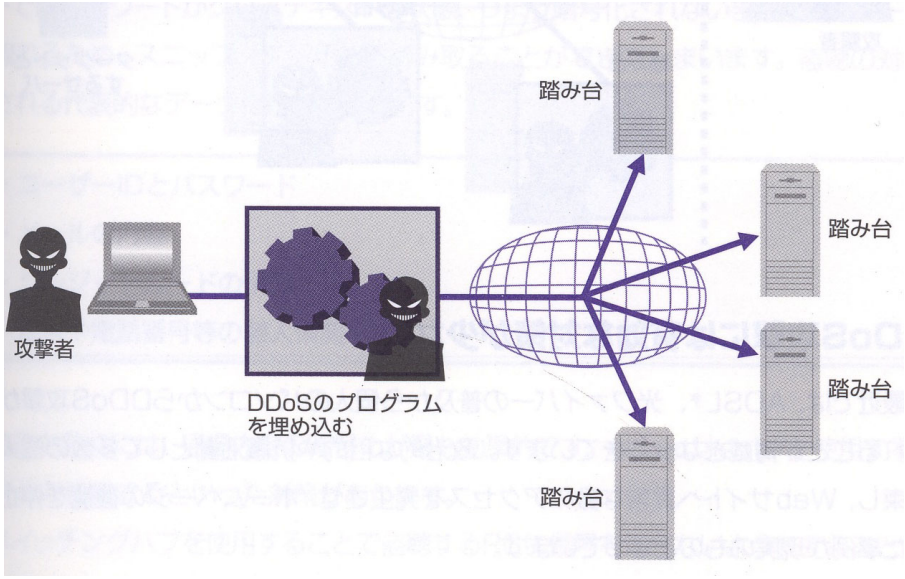
  - メール爆弾：巨大なメールや大量のメールを送りつける

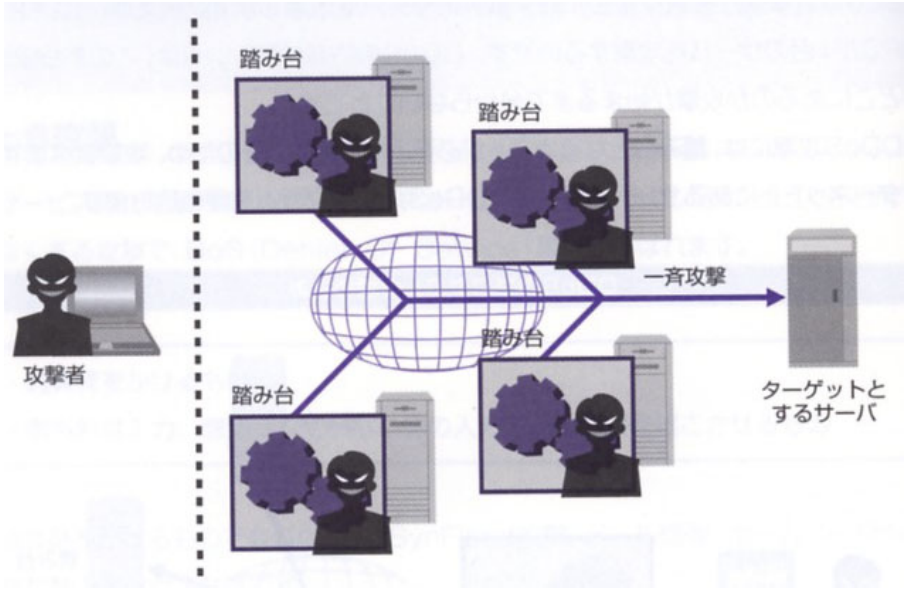
  - ホームページへの異常な数のアクセス

サービスの妨害：DDoS攻撃

DDoS（Distributed DoS)攻撃

攻撃用ソフトウェアをあらかじめ他のコンピュータ（踏み台）に組み込み，指示により一斉に攻撃





マルウェア

- コンピュータウィルス，ワーム，スパイウェアなどの「悪意のこもった」ソフトウェアを総称してマルウェアと呼ぶ

コンピュータウィルス

『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1つ以上有するもの』

（経済産業省告示「コンピュータウィルス対策基準」より）

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，条件が満たされるまで症状を出さない機能

3）**発病機能**：　プログラムやデータ等のファイルの破壊を行ったり，コンピュータに異常な動作をさせる等の機能

コンピュータウィルスの種類

- 人手を介して他のコンピュータに感染

1) プログラム感染型ウィルス
   - 実行形式プログラムに感染
   - 他の実行形式プログラムを探しウィルスをコピー
2) ブート感染型ウィルス
   - ブートプログラムに感染
   - USBメモリ，DVD-ROM経由で感染
3) マクロウィルス
   - 文書ファイルに付加されたマクロで感染

コンピュータウィルスの基本動作

- 宿主となるプログラムの一部を書き換えて感染，感染した宿主のプログラムが実行されたときに不正動作が機能
- 単独では動作出来ないため，感染したプログラムが起動されない限り不正動作は機能しない

ワーム

- 感染する媒体を持たず単独で動作し感染を広げる（増殖能力が高い）

  - メールの添付ファイル

  - 感染したコンピュータ内のメールアドレスを収集し，それらを宛先として自分をコピーして大量には移送する，など

  - Blaster，LoveLetter, Sircam, Code Red, Nimda，等

トロイの木馬

トロイの木馬（Torojan　Horse）：

・　見た目には、あるいは実際に便利な機能を持ちながら、それに加えて（隠れた）機能を持っており、不正に正規の権限を取得して安全性を損なうプロセスを実行するプログラム

・　前述のメールワームはネットワーク経由で感染活動を行い，その正体を無害な添付ファイルと偽るので一種のトロイの木馬

その他のマルウェア

- エクスプロイト
  - コンピュータのソフトウェアやハードウェアの脆弱性を利用した悪意ある行為のために書かれたスクリプトまたはプログラム
  - 単体では自己増殖機能を持たない亜種:山田オルタナティブ
    感染するとPCのHDDに保存されたすべてのデータがインターネット上に流出

- bot型ウィルス
  - 外部からコンピュータをリモートコントロール（ゾンビPCとC&Cサーバ）（DDoS攻撃，スパムメール，ワーム，情報漏洩，等
    http://www.active.go.jp/security/malware/

- スパイウェア
  - コンピュータ内の情報を外部に不正に持ち出す機能をもつ．正規のソフトをインストールするときに利用許諾を求めOKするとインストールされることがある．（アドウェア，キーロガー，rootkit）

その他の脅威（1/3）

- ソーシャルエンジニアリング
  - 実社会に於ける不正アクセスを目的とした行為（正規に利用者になりすまし，管理者から　パスワード等を聞き出す，ピギーバック，ショルダーハッキング，データサルベージ，等）

- フィッシング（Phishing)詐欺
  - 実社会の振り込め詐欺と類似
  - 銀行やクレジット会社のサイトを偽装し，メール等で偽のサイトへアクセスするよう誘導

その他の脅威(2/3)

- **P2Pファイル共有ソフトの悪用**

　P2Pファイル共有ソフトがインストールされているコンピュータがコンピュータウィルスに感染し，保存していた情報がP2Pファイル共有ソフトを介してインターネットに公開される（情報漏洩）

- **クロスサイトスクリプティング**

　Webサイトで実行されるアプリのセキュリティ上の不備を利用して，サイト間を横断して悪意のあるスクリプトをユーザ端末に注入

その他の脅威(3/3)

- **Drive-by-download**

　マルウェアなどをユーザに気づかせることなくダウンロードさせる不正行為.

　Webサイトを閲覧しただけで，ユーザの意図に関わらずマルウェアがダウンロードされて実行される.

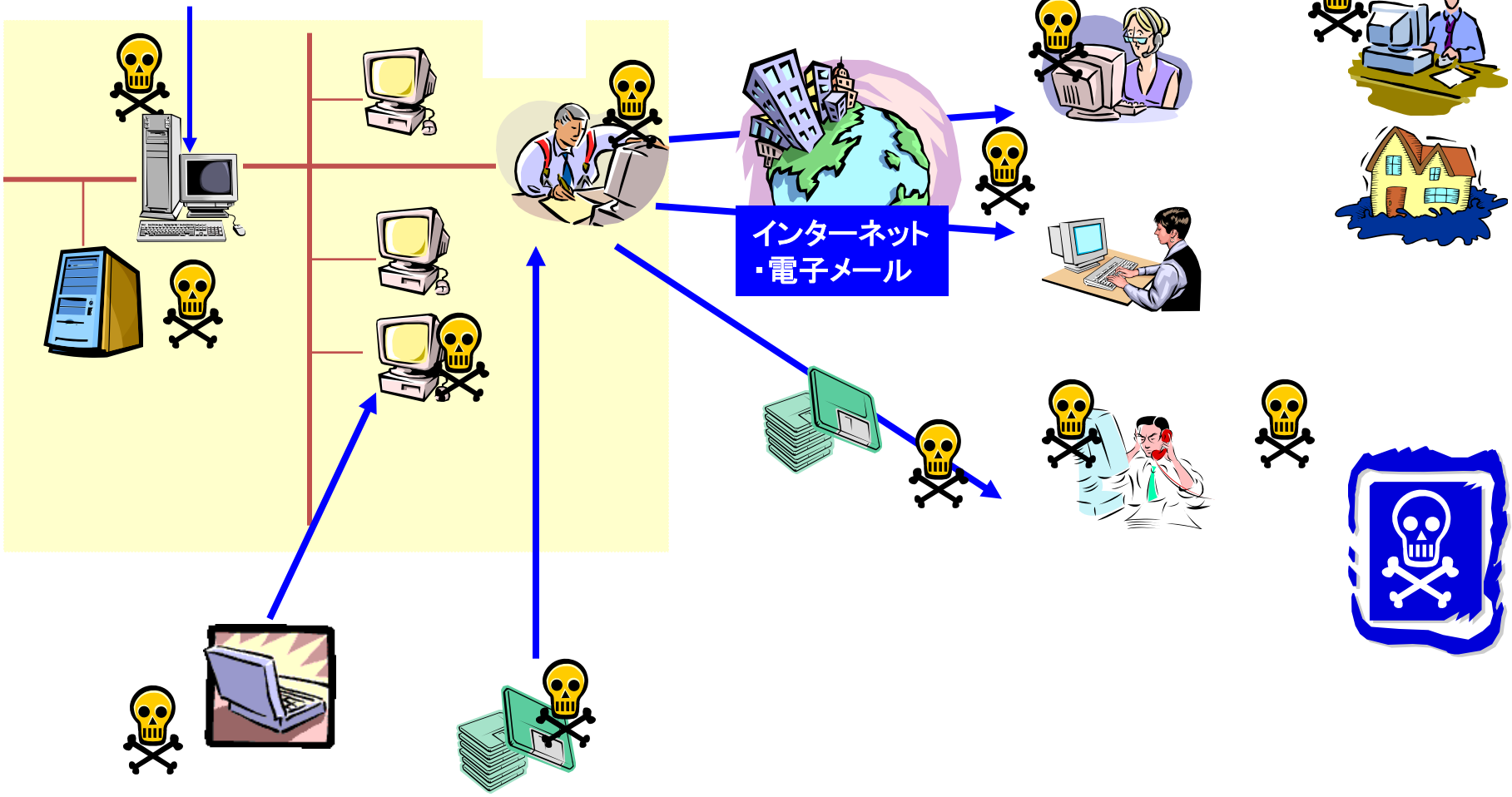
- **サイバー攻撃**

　インターネットの接続容易性を悪用して，コンピュータ上の情報搾取やハッキングを行う犯罪．金銭・経済的な狙いで被害規模が年々増大(3億7800万人(国内400万人)が被害，2013年)

ウイルスによる被害

・顧客データの削除
・機密データ書き換え
・ディスクの破壊　など

取引先　　一般消費者



ウィルスの約80%は電子メールから．最初にいかに食い止めるかが対策の鍵．

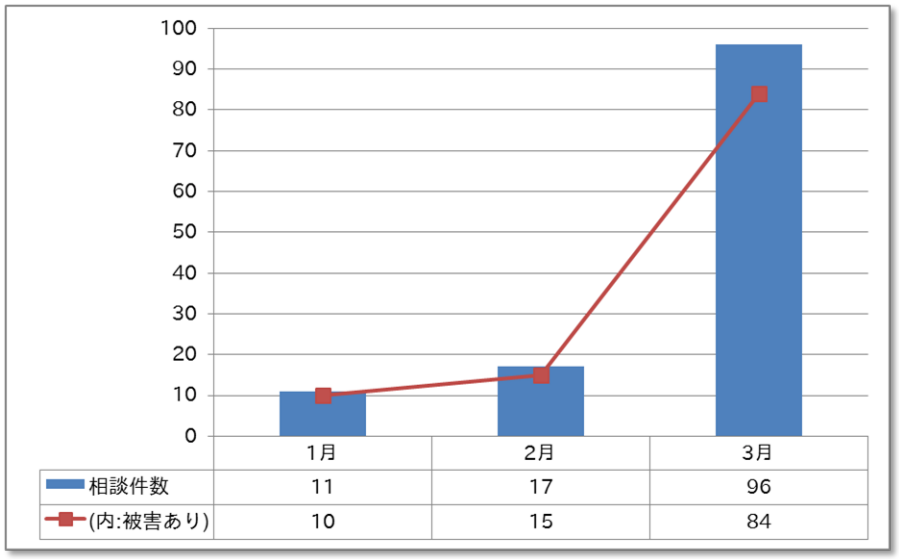
被害の例（総務省）

- http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/index.html

- 事例1：資料請求の情報が漏洩した
- 事例2：私の名前で誰かがメールを
- 事例3：ホームページを見ただけで・・・
- 事例4：猛威！デマウイルス
- 事例5：メールが他人に読まれている？，etc.

最近の事例

- ランサムウェア(Ransomware)
  - 感染したPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラム
  - 身代金要求型不正プログラムとも呼ばれる
  - メイルウィルスによる侵入が見つかっている



	1月	2月	3月
相談件数	11	17	96
(内:被害あり)	10	15	84

2016/4/13のIPAによる注意喚起のリリース中の統計

https://www.ipa.go.jp/security/topics/alert280413.html

一般的なセキュリティ対策

- セキュリティホールをなくす
  （OS、アプリケーションをアップデート）
- ファイアウォールを設定
- セキュリティソフトの導入

セキュリティ対策(1)

- 技術的な対策

  - セキュリティ防御：不正行為の発生を直接的に防御する
    - 認証(Authentication)
    - アクセス制御
    - 暗号
    - 電子署名

  - セキュリティ監視：不正行為の発生を予防・検出する
    - 不正侵入監視
    - ウィルス監視
    - コンテンツ監視

認証　Authentication　とは

認証：本人であることを確認すること　Person Authentication

「認証」を実現したり、保証したりする技術：

知らない特定個人との取引、サービスなどが存在する場合

実世界（日常生活）で使われる認証方式

－所有物による認証　---　印鑑

－知識による認証　---　インターネットでは唯一の手段

➡ 相手しか持っていないものを確認することが前提

アクセス制御

- 認証により確認したユーザ（装置）に，コンピュータ資源に対するアクセスを権限の応じて許可

暗号

- 機密性を実現
- 共通鍵暗号方式：暗号化と復号で同じ暗号鍵を使用
- 公開鍵暗号方式：暗号化と復号で異なる暗号鍵を使用

電子署名

- 電子商取引において取引内容を穏当に行ったことの証明するための対策（捺印，署名）

  - 第三者および電子署名を受け取った受取人によって偽造できない
  - 電子署名を行った本人が後でそれを否認できない

不正侵入監視（侵入の検知）

(IDS: Intrusion Detection System)

- **統計的な異常検知**

  閾値に基づく検出：ユーザの区分に関係なく、様々な事象の起こる頻度の閾値を定義

  行動記録に基づく検出：各ユーザの活動の記録を行い、それを用いて個々のアカウント

- **ルールに基づく検出**

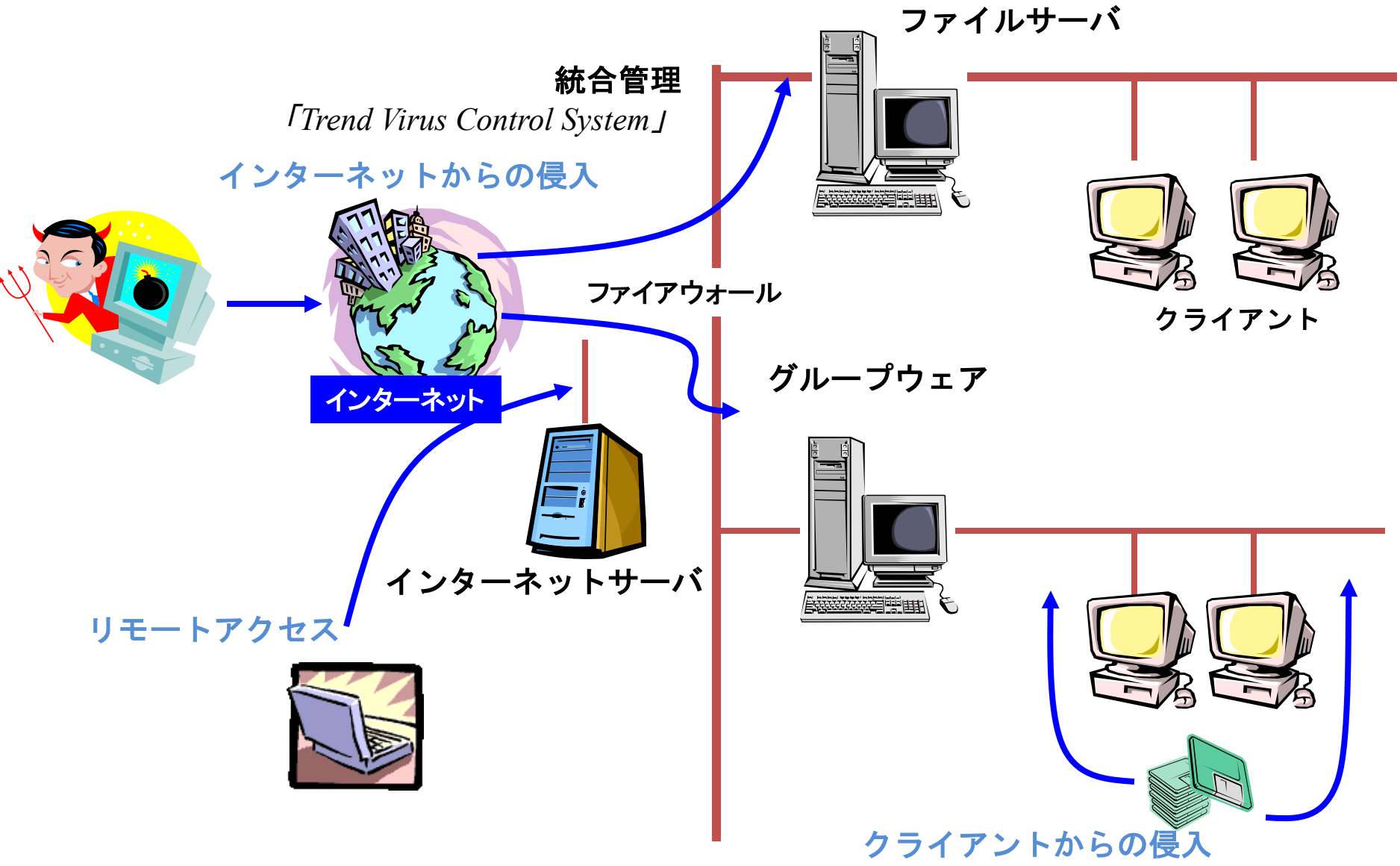
  異常検出：通常の行動パターンから逸脱するものを検出する規則を作成

  侵入の識別：疑わしい行動を探し出すための一種のエキスパートシステム

ウィルス監視

- ウィルスの検出，駆除
- ウィルス定義ファイルに基づき検出
- ファイアウォールやメールサーバと連携して，ネットワーク入り口で検出，駆除

ウィルス監視例


ファイルサーバ
統合管理
「Trend Virus Control System」
インターネットからの侵入
ファイアウォール
クライアント
グループウェア
インターネット
インターネットサーバ
リモートアクセス
クライアントからの侵入

コンテンツ監視

- Webの内容やメールの内容をチェック

  - Webフィルタリング
  - メールフィルタリング

セキュリティ対策(2)

- 運用・管理面での対策
  - セキュリティ対策方針の明確化：セキュリティポリシー
  - 人間や組織の脆弱性への対処

脅威分析によるリスクの明確化
保護対象の明確化
利用許可/許可内容の整理
セキュリティ実装方式，等

課題

- コンピュータウィルスの実例を1つ調べ，その特性（基本動作），被害状況と対策方法について述べよ.

締め切り 10/24(火) 15:00