システム運用上の情報セキュリティポリシー

Information security policy in the system operation.

2003.10.23 Colloquium

京都大学東南アジア研究センター　資料部助手　木谷　公哉

(kitani@cseas.kyoto-u.ac.jp)

目次

- 情報セキュリティの必要性
  - 電子情報とは？、被害･損害
- 不正侵入

  種類、手法、手段、経路、実例
- セキュリティ対策
  - ユーザ、サーバ、ネットワーク、建物
- 不正侵入と対策のまとめ
- 情報システムとセキュリティ対策
  - 業務内容、導入、運用、拡充
- 情報セキュリティポリシーへの課題
  - 統合情報化センターを踏まえて

情報セキュリティの必要性

- 目に見える形ではない情報の危険性
  - 漏洩、破壊、書き換えをされても発見しづらい。
  - 見えない物を見えない者から守ることが困難。
- インターネットへの接続が必須の状況
  - 情報化社会においては情報を収集、伝達、発信が必須である。
- 高度成長しているITテクノロジーの利用
  - あらゆる人に恩恵をもたらすものは、悪意ある者にとっても都合がよく便利なものである。

情報セキュリティの被害

- 情報漏洩
  - 機密情報が外部に漏れる。
- 破壊
  - 公開データだけでなく、ユーザ個人PCのデータへの影響がある。
- サービス妨害
  - 無意味なデータを大量に送ることで、意味のあるデータを閲覧困難な状態にする。(DoS, SPAMなど)

自分の身は自分で守れ！

これらを行う上では、攻撃ルートの隠蔽が重要な要素である。

↓

被害者であるはずの一般ユーザを加害者にする

↓

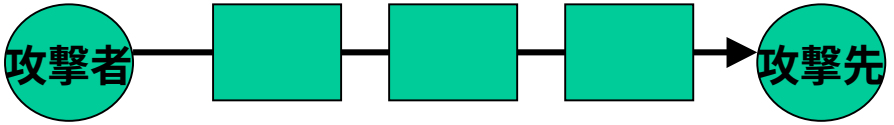
被害者の一人が加害者に仕立て上げられたユーザを訴える場合がある。

↓

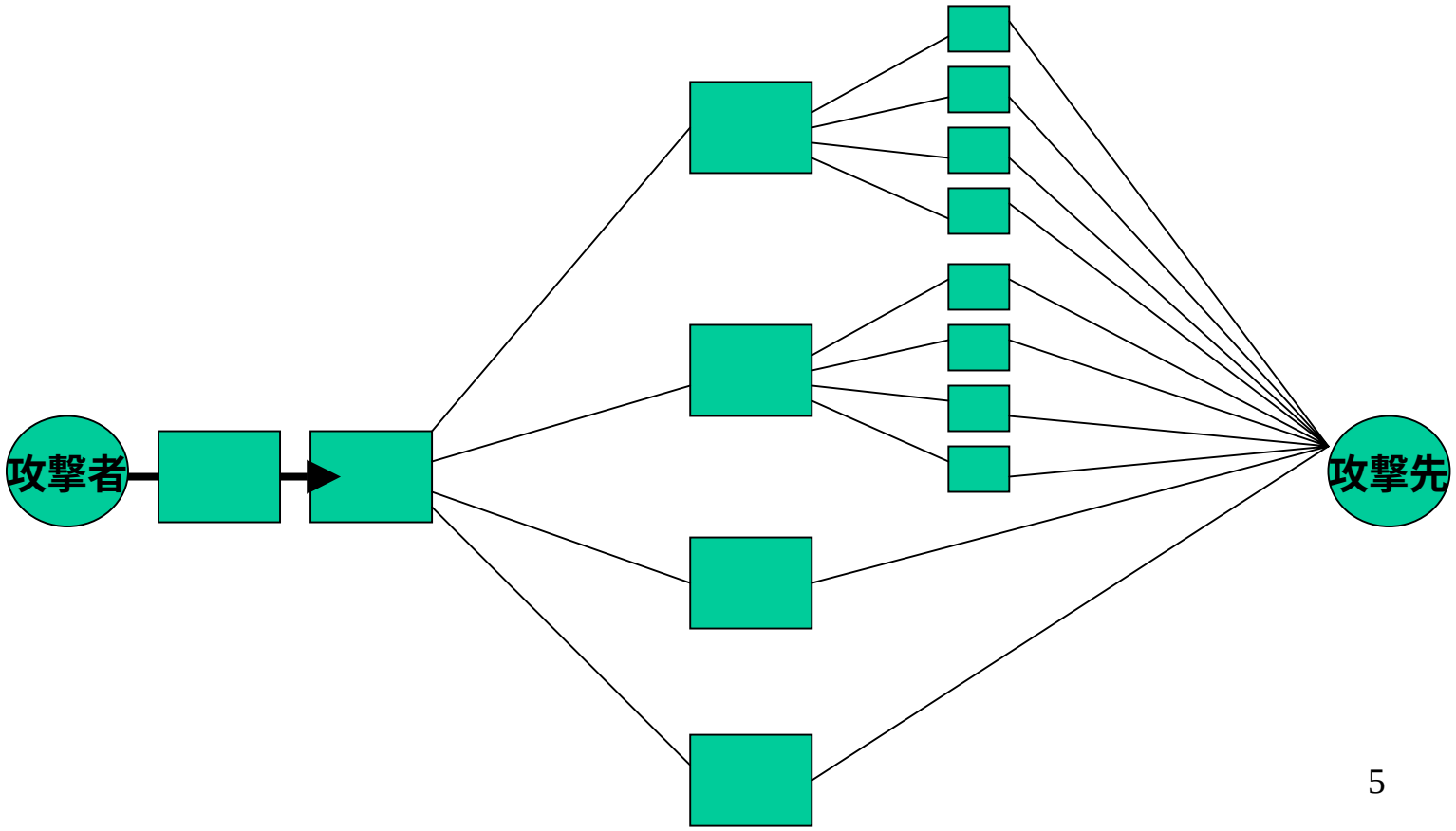
加害者に仕立て上げられたユーザは、自分が被害者であるということを立証できないケースがほとんど。

不正侵入 (種類)

1. **直接攻撃型**



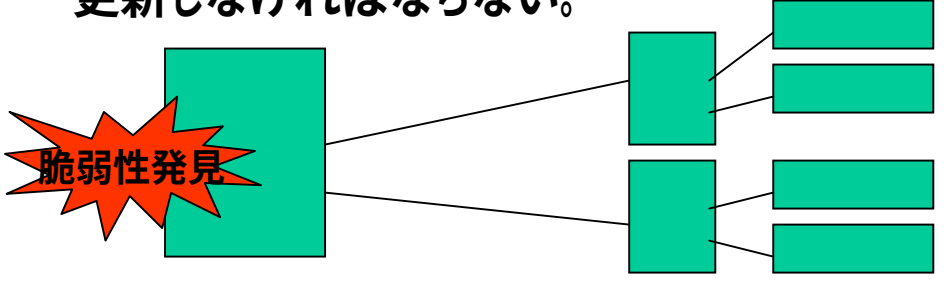
2. **分散攻撃型**



不正侵入 (脆弱性)

1. **ポートスキャン**
   - ネットワーク上に存在するコンピュータリストを調査する行為。専用のツールが簡単に入手できる。リストに載ったコンピュータはその後、攻撃対象とされる場合がほとんど。
   - FTP, TELNET, SMTP,HTTPは脆弱性が存在する場合が多いため、脆弱性までをボタン一つで発見するツールが出回っている。

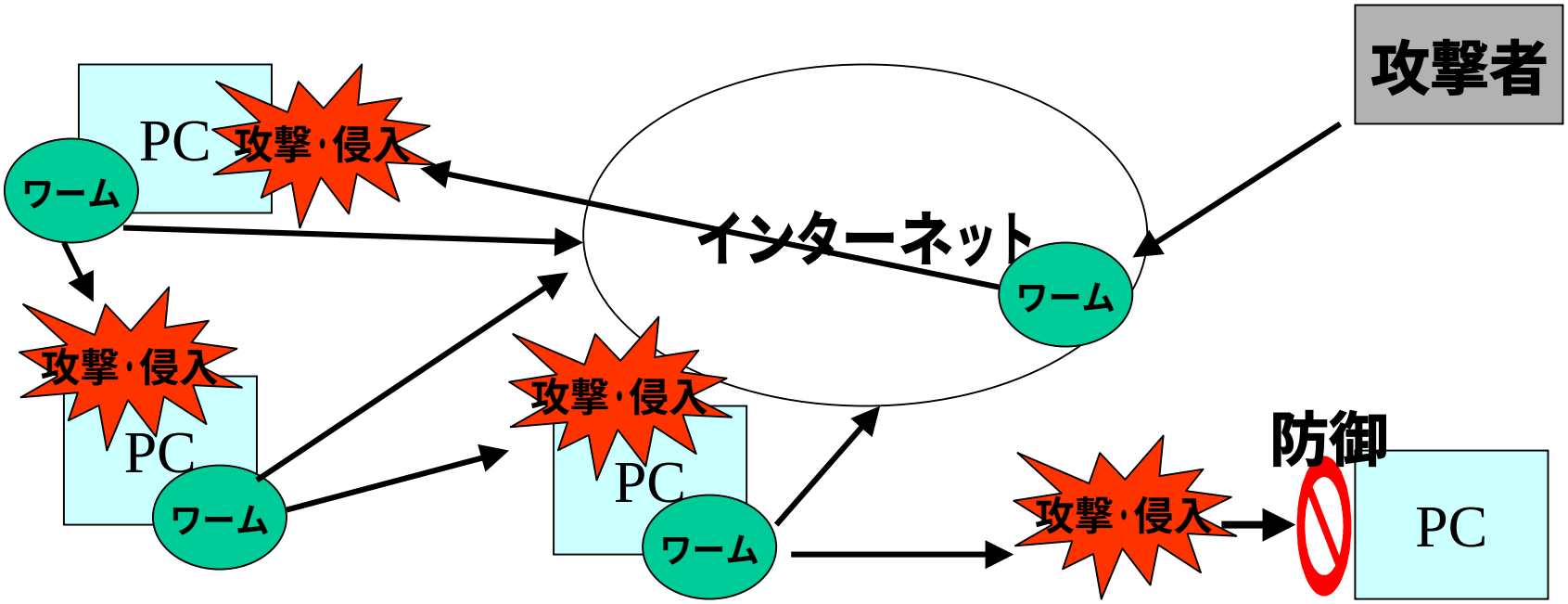
2. **バッファオーバーフロー**
   - システムが予期しない大量のデータを送りつけることで、システムを麻痺させ、それに乗じてそのシステムを動作させている権限 (大抵は管理者権限) を奪取するもの。
   - システム自身、もしくはシステムが利用したシステムの脆弱性によって引き起こされる。
   - この脆弱性が発見された場合、関連するあらゆるシステムをすべて更新しなければならない。



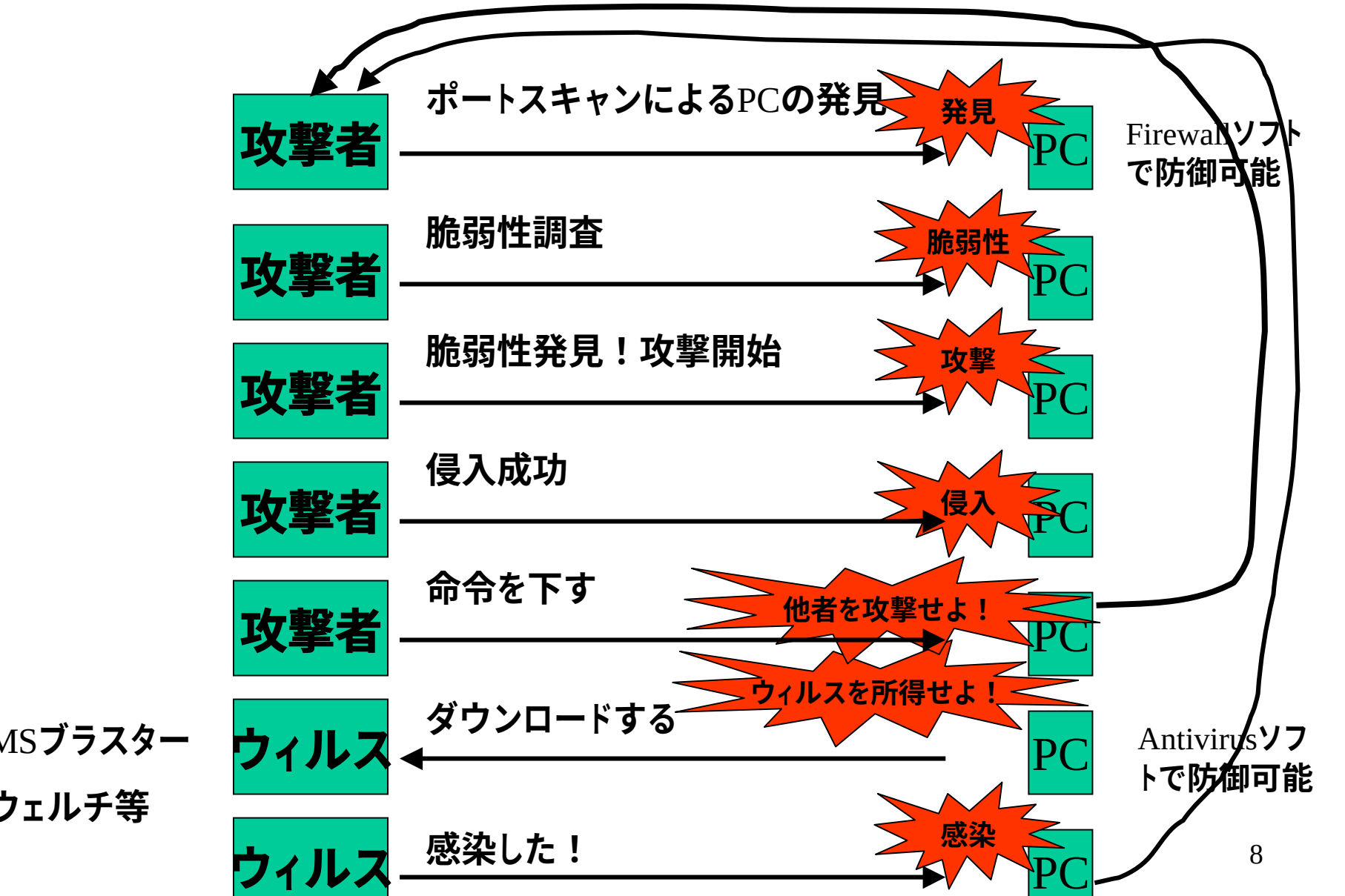
線で結ばれているすべての機能が脆弱性を含むことになる。

不正侵入（分散攻撃型の手法）

- 攻撃者はワーム（他者の力を借りずに増殖できる機能を持つ）をインターネットに流す。
- ワームは侵入先に自身を複製し、侵入先を新たな攻撃者として、ワームを流布させる。
- ワームが流布してしまうと、感染した全員が攻撃者となるため、誰が犯人か特定できなくなる。

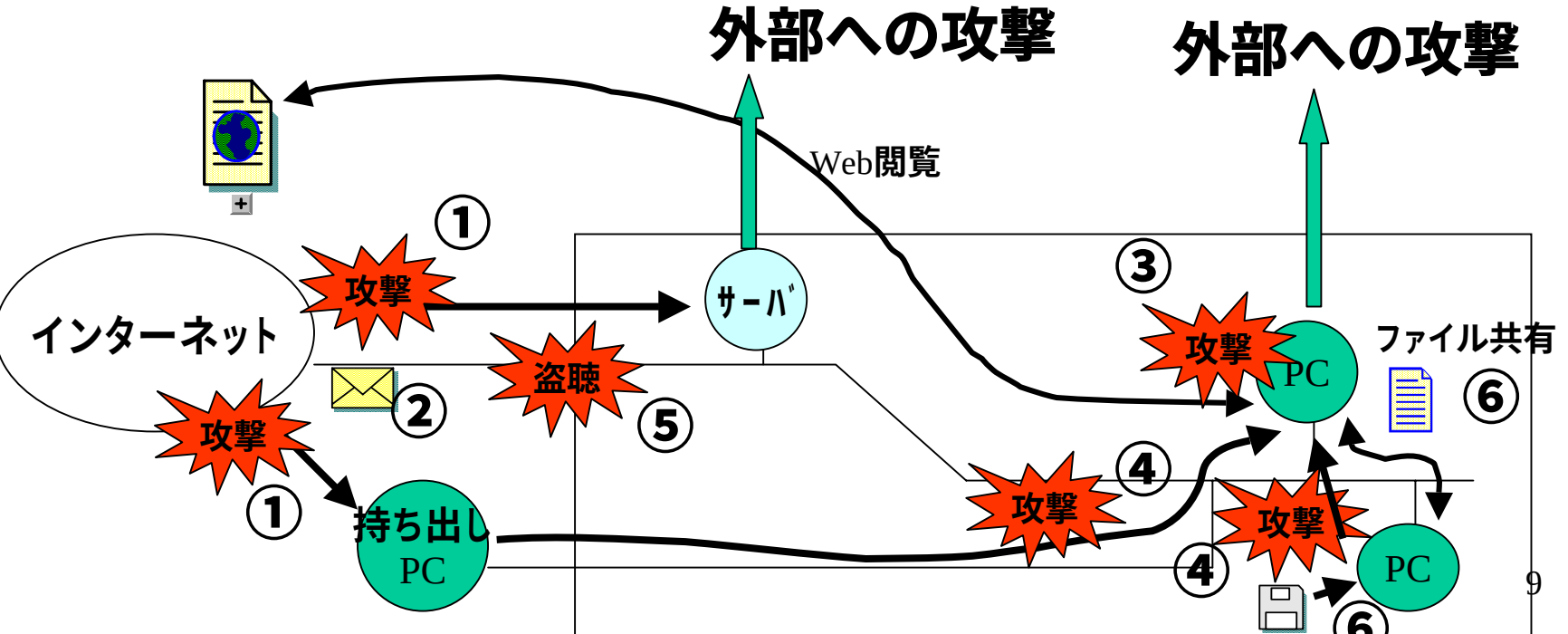


不正侵入（分散攻撃型の手法詳細）

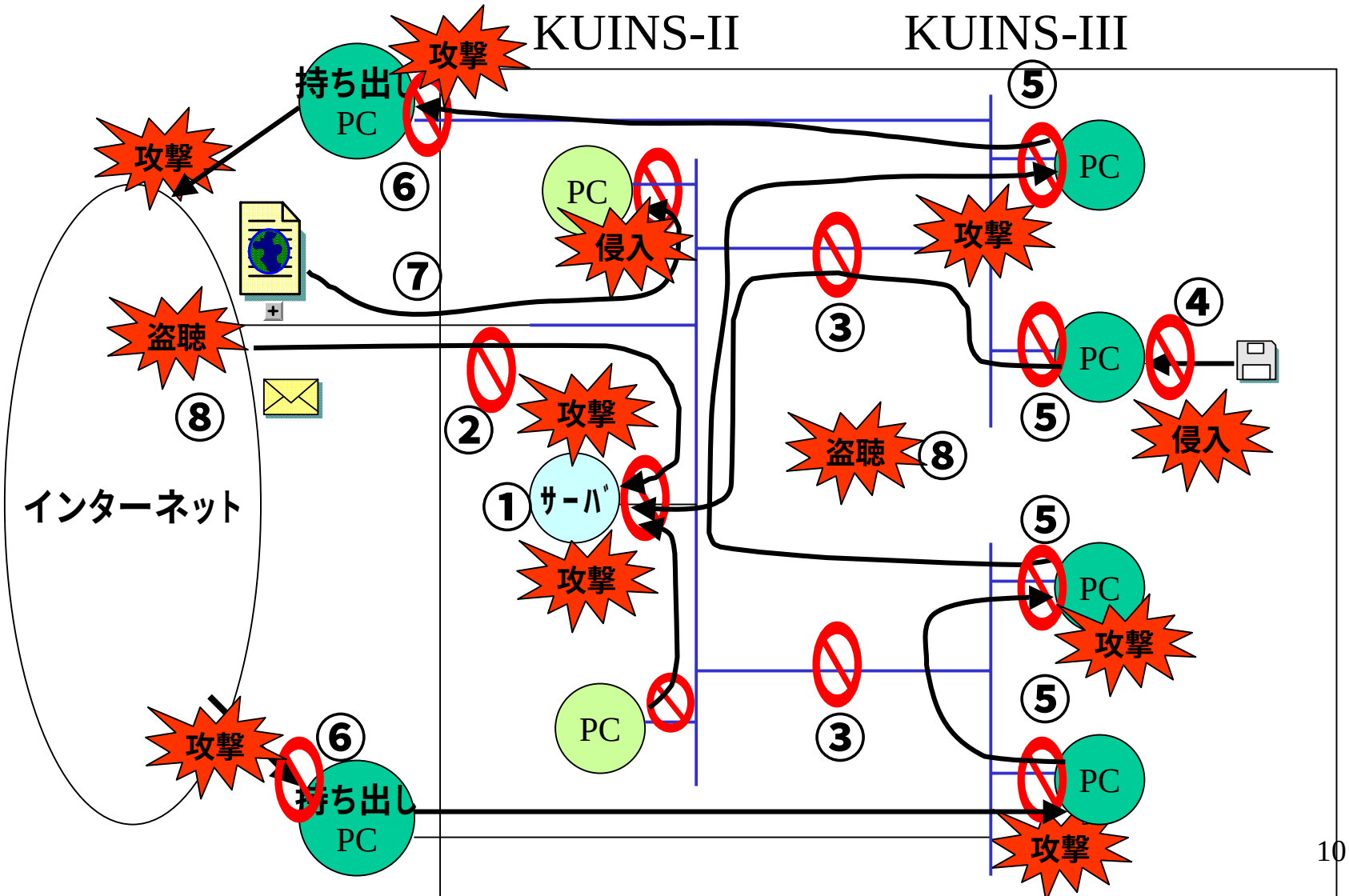


不正侵入 (経路図)

1. 外部からの直接攻撃
2. 電子メールによるワーム転送
3. Webブラウザ脆弱性によるワーム転送
4. 内部攻撃
5. 盗聴によるシステムへの侵入
6. 外部メディア･ファイル共有からの侵入



不正侵入とその対策 (図示)



不正侵入とその対策（図の説明）

① 導入ソフト、OSのセキュリティ設定をしっかりする

② Firewallゲートウェイを設置（KUINS-II）

③ 細分化したネットワーク同士のFirewallゲートウェイを設置（VLAN）

④ 閲覧することで侵入を許すタイプは、導入ソフト、OS設定をしっかりするとともに、Antivirusソフトの導入をする。

⑤ 直接攻撃はFirewallソフトの導入で対処する。

⑥ 特に外部ネットワークに持ち出すPCはFirewall, Antivirus、を導入するとともに、導入ソフト、OS設定をしっかりする。

⑦ Webを閲覧するだけで侵入を許すタイプは、Firewallソフトウェアの導入か、Webブラウザソフトウェアの設定を強化する。

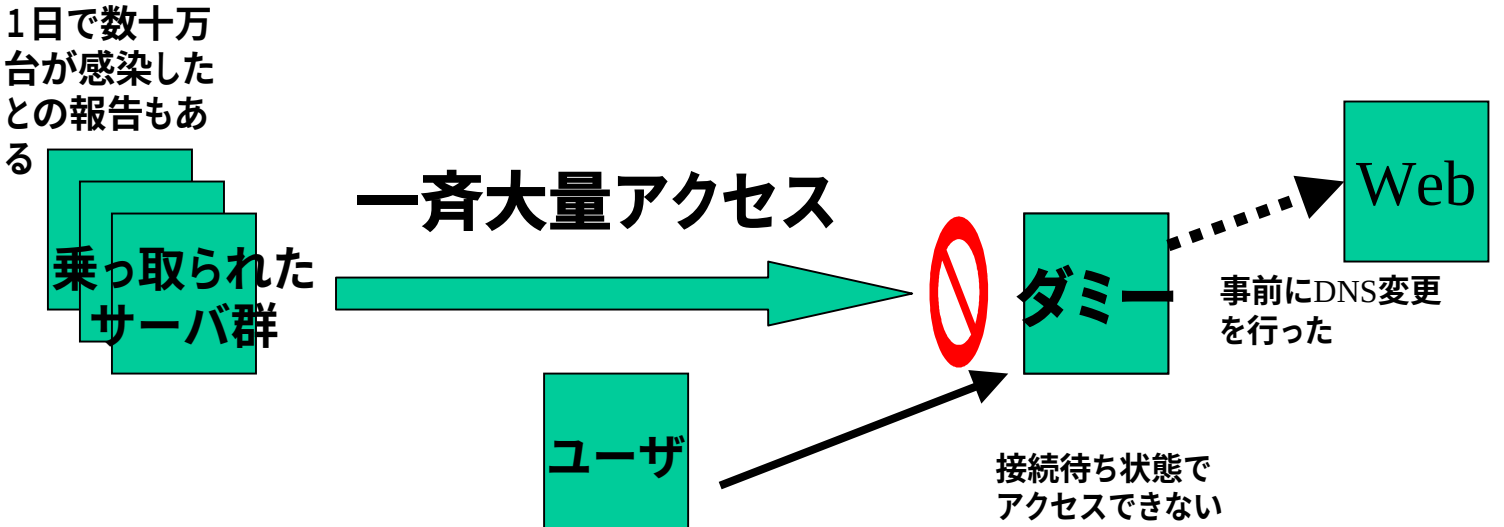
⑧ 盗聴を防止するための措置が必要

機器レベルでは防止できないので、通信を暗号化することで対処せざるを得ない。そしてネットワーク内に不審なデータや不審者がいるかどうかを監視する体制が必要（監査装置による記録や怪しげな人が建物に入れないようにする等）

不正侵入（実例と対策1）

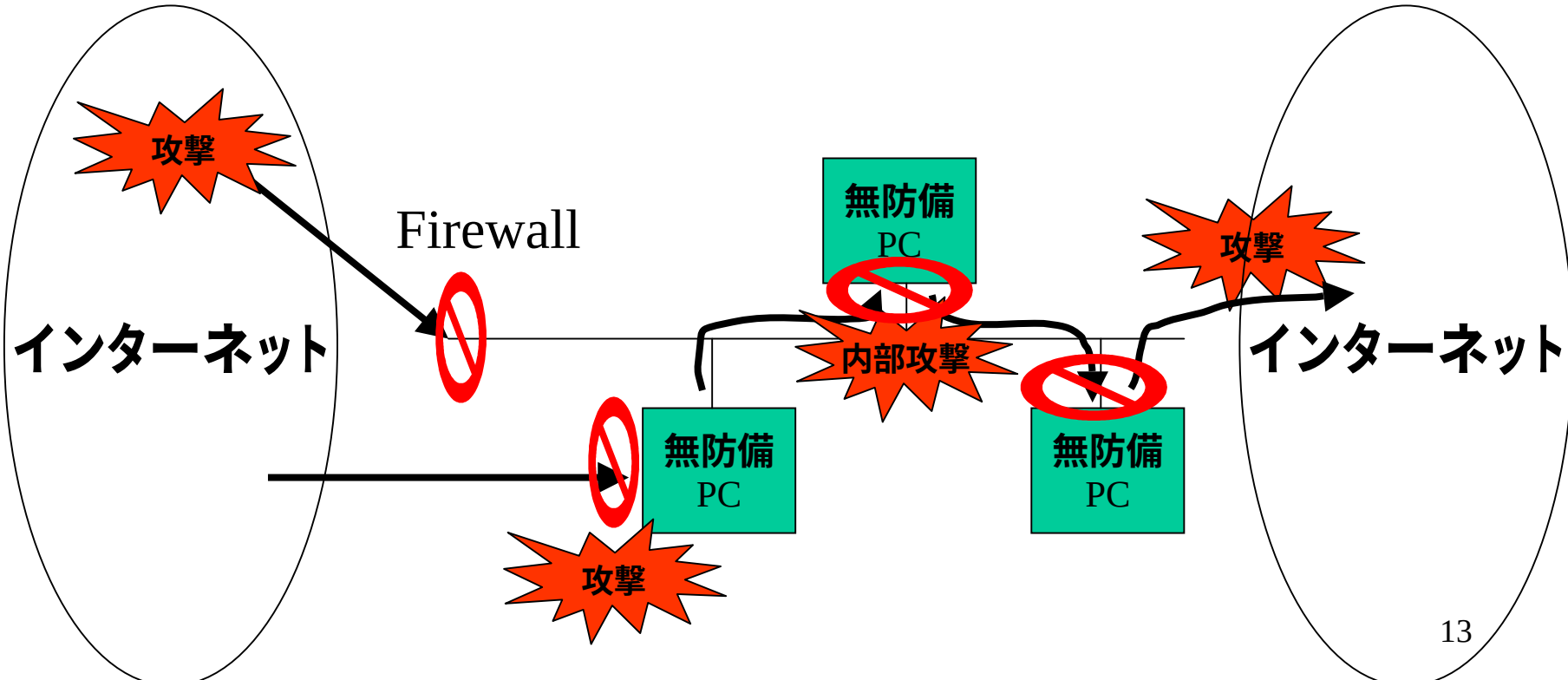
- **サービス拒否攻撃**（DoS: Denial of Service）
  - **ホワイトハウスへ攻撃**（2001.7.19 AM8:00 →）
    - Cord Redというコンピュータウィルスを用いて乗っ取ったサーバを利用し、それらのサーバから一斉にホワイトハウスのWebサーバへ攻撃。
    - これに対しホワイトハウスは、この攻撃前に自らのWebサーバのIPアドレスを変更することで攻撃を回避。

    ※ 乗っ取られるのはWindowsサーバのWebサーバシステム（IIS）のみ。



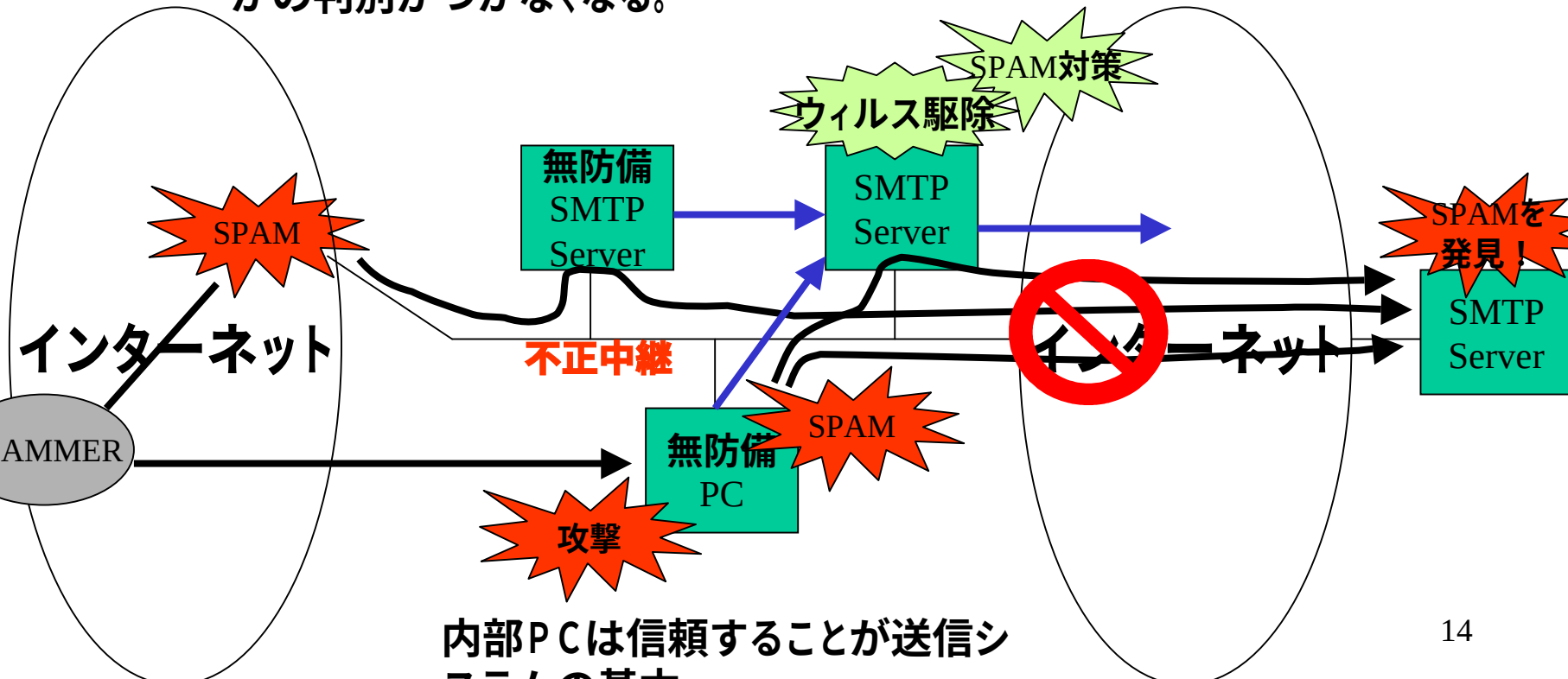
不正侵入（実例と対策2）

- **複合分散型攻撃**（MSブラスター: 2003.08 →）
  - WindowsNT,2000,XPのリモート制御機能の脆弱性を利用し侵入。
  - Webを閲覧した、メールを開いたなどの人為的操作を必要としない。
  - コンピュータウィルス対策ソフトでは完全に防御できない。
  - Firewallソフトウェアを個々のPCに導入しなければならない。



不正侵入（実例と対策3）

- **無差別迷惑行為（ＳＰＡＭ）**
  - 不正中継可能なメールサーバを利用
  - From, Toに記載されているアドレスは信用できない。
  - メール送信システムであるＳＭＴＰは、利用者が善意ある人たちであることが前提で設計されているものである、差出人、宛先ともに詐称され、かつメールサーバを変更されながら送信されると、誰がいったい悪さを行っているかの判別がつかなくなる。



内部ＰＣは信頼することが送信シ

検討すべき対策事項

- ユーザレベル
  - パスワード設定･保護の重要性認識
  - 第三者への踏み台にされるかもしれない危機意識
  - 見かけに騙さないようにする（偽造メールに注意）
- サーバーレベル
  - システム構成ポリシーを制定（不必要な機能を削る）
  - 特にパスワード盗聴防止のための暗号化体制
  - アプリケーションへの迅速なセキュリティ修正を行える体制
- ネットワークレベル
  - 特に内部攻撃をチェックする監視体制
  - 盗聴発見のための監視体制
- 建物レベル
  - 不審者の発見が可能かどうか。

ユーザレベルでの対策

- 利用するパソコンに強力なパスワードを設定する。
- OSレベルでのセキュリティ修正パッチの導入
  - Windows　(2003.10.16付けのニュース)
    - ひと月に一度（毎月第 2 火曜日）以降にWindowsUpdateを実施する。
  - MacOSX
    - 自動更新機能をONにしておけば、ポップアップによりお知らせをしてくれる。
  - UNIX系
    - 導入したソフトウェアのうち、ネットワーク接続が必要なものに関しては更新する（ただしソフトウェアが利用するライブラリへの注意も必要）
- Firewall、アンチウィルスソフトを導入し、ネットワークからの不正侵入、内部侵入を防ぐ。
  - Norton Internet Security、ウィルスバスター等の導入

サーバレベルでの対策

- ユーザパスワードに安直なものを使用しない
- 必要のないシステムは停止する
  - 必要のないソフトウェアは削除するか使用しない構成に変更
- 動作させるソフトウェアは徹底管理する
  - 動作に必要なライブラリも含めて、常にセキュリティ情報収集を行い、迅速なセキュリティ修正を行う。
  - 利用する範囲が限定的なものは、限定構成を組む。
- 機密情報は暗号化する
  - サーバへのファイル転送、ログインの暗号化
  - SSLによるWebデータ暗号化
  - メール閲覧のためのパスワード
- サーバを設計する段階から、セキュリティへの配慮を行う
  - 設置場所、必要なシステムを確立し、可能ならばテスト環境を構築し、実際に動作させた上での調査を行う。

ネットワークレベルでの対策

- 一般PCと外部公開するサーバは、ネットワーク的に分離すべき（VLANやDMZなどを利用）
- Firewallを導入することで、組織レベルでの防衛対策は必須である。
- その他Web閲覧やファイル転送、メールに関して可能な限り、コンピュータウィルス対策を施す必要がある。
- 暗号化されていない通信は盗聴されるため、特にパスワードに関してはネットワークに流れる通信を暗号化するよう心がける。

不正侵入対策のまとめ

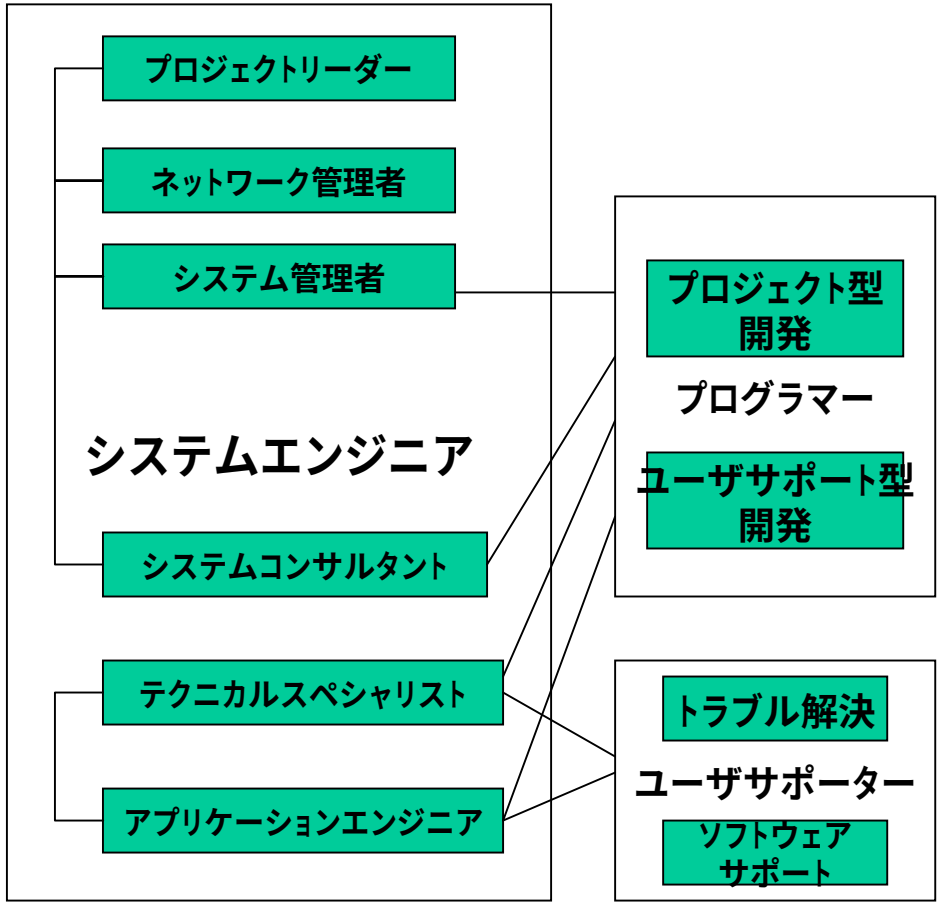
もっとも恐ろしい敵は、内部にあり。

不正侵入対策のまとめ (対策)

- 個々のPCレベルで不正侵入対策を推進
  - Antivirusソフトウェアの導入
  - Firewallソフトウェアの導入
- 組織レベルでの不正侵入対策は必須
  - Firewall for Gateway
  - Antivirus for Mail Gateway
  - VLANによるサーバ、クライアント分離
    - ただしVLAN構成を正しくしないと意味がない
  - DMZによるサーバ、クライアント分離
  - Antivirus for Web Gateway

情報システムの業務

全てにおいてセキュリティ意識をもっていなければならない。



プロジェクトを行うためのシステム設計･構成を統括管理する

ネットワークの運用、管理、ユーザにとって不便なく利用できる

導入した様々なシステムの維持管理を行う。

システムの設計、構築、運用をサポート

様々な技術サポートを行う

ユーザサービスなどを目的としたシステム開発を行う

情報システム運用におけるセキュリティ対策

- 導入時にセキュリティを考慮にいれた構築をすることでその後の維持管理を容易にする。
  - ＰＣセットアップ：1台1日～2日：センターでは２００台程度
    - 主に扱うソフトウェアの脆弱性の修正をチェック。
  - サーバセットアップ：1台1ヶ月～2ヶ月：センターでは7台
    - 動作させるシステムに必要な機能を調査
    - 必要な機能を実現するための構成を検討
    - 必要なソフトウェア・ハードウェアを導入（ソフトは数百程度導入することとなる）
    - セキュリティチェックを行い、またすべてのシステム記録を保持させるようにする。
    - 万が一のことを想定し、データのバックアップシステムを構築。
  - ネットワーク構築：新規だと1年～3年：KUINS-I --> II --> III
    - サーバとクライアントを不用意に同一ネットワークに置かない。
    - 内部攻撃を受けた場合には、遮断措置を行える体制にする。
    - 防御措置を施しつつ、ユーザにとって使いやすい環境を整備する。
- サーバやその上で動作させるシステムが増大すると、セキュリティレベルは低下する（人的問題を解消できない限り）
- 一つでもほころびが生じると、システム全体が機能低下もしくは停止してしまうおそれあり。（内部攻撃）

セキュリティポリシーの現状

- 統合管理型
  - メリット：情報の統合・共有化が容易。セキュリティレベルが高い
  - デメリット：負担が集中してしまう。
- 分散管理型
  - 各講座等で管理が別（統合管理者が存在しない）
    - メリット：一人にかかる負担が少ない。
    - デメリット：情報の統合・共有化が難しい。セキュリティレベルが低い

セキュリティポリシーへ向けて

セキュリティ対策専門の室を設け、それ専属のスタッフを常駐させることが一般的

↓

現実には1名ないし、2名程度の兼任がほとんど

↓

システムを拡充すればするほど、時間的な問題で、迅速な対応が困難ほとんど

↓

セキュリティレベルが低下していく

セキュリティポリシーへの課題

- ユーザサポートとシステム設計･構築は分離すべき
  - ユーザサポート
    - ルーチンワーク化
    - 時間制
  - ユーザサービス系開発
    - システム開発系とは別にすべき。
  - システム維持管理（サーバ系）
    - 数人の開発者を常に保持し、開発者にシステム維持管理業務の一端を担ってもらう
  - システム設計･構築
    - 少なくてもハードウェアに関しては保守体制を確立し、故障時の負担を減らす。（破損、停電、バックアップ、場所を考慮に入れる）
- 複数の部署が混在する場合には、機能面のみの統合する
  - ネットワークは物理的に分かれている場合、それぞれのポリシーで運営する。
  - ユーザサポートはサービスの質が異なる場合が多いため、無理に統合しない方がよい。統合する場合には、ユーザサポート専属の要員が必ず必要になってくる）
  - プロジェクトなど共同作業が必要なものに関して、その性質を見極めた上で、どのネットワークに置くかを判断し、統一管理していく。

参考資料

不正侵入防止ソフトウェア紹介
情報セキュリティ関連ＵＲＩ

セキュリティ関連ソフトウェア製品

- Antivirus Software
  - Norton Antivirus
  - Symantec Antivirus Corporate Edition for EDU
    - **ライセンス購入しておけば、英語版、日本語版問わず購入したライセンス数だけ利用できる。**EDU**は**Education**版であり、学術機関向けにかなり安価で提供されている。**
- Firewall Software
  - Norton Personal Firewall
- **統合型防御**（Antivirus + Firewall + **情報漏洩防御+スパイウェア防御**）Software
  - Norton Internet Security
  - Symantec Client Security for EDU
    - **ライセンス版**

セキュリティ関連ソフトウェア製品

- Antivirus Software
  - GriSoft (http://www.grisoft.com)
    - **機能限定版をフリーソフトウェアとして提供。ただし新種のウィルスへの対応が市販のものと比べ、遅い。**
- Firewall
  - Zone Alarm (http://www.zonealarm.com)
    - **機能限定版をフリーソフトウェアとして提供。フリー版は細かな設定ができないので単独で利用するクライアントPCで使う場合にのみ、機能面は十分といえるでしょう。ただしフリー版は無保証であるため、組織的に利用することは難しいでしょう。**
- **統合型防御**（Antivirus + Firewall + **情報漏洩防御+スパイウェア防御**） Software
  - **ウィルスバスター** (http://www.trendmicro.com/)
  - McAfee （http://www.nai.com/japan/)

情報セキュリティ関連ＵＲＩ

- オンラインウィルス・セキュリティチェック(Symantec)

  自分のPCのセキュリティに不安がある場合、もしくはセキュリティ対策をしていなければ一度はチェックしたほうがいいでしょう。 http://www.symantec.co.jp/region/jp/securitycheck/index.html

- 京都大学学術情報メディアセンター提供のセキュリティ情報

  http://webdb.kuins.kyoto-u.ac.jp/security_info/

- 文部科学省大臣官房政策課情報化推進室提供のセキュリティ情報

  http://shinko-www.mext.go.jp/security/index.htm

- Symantec Security Response (solarisでデフォルト起動のsadminサービス脆弱性に注意)

  http://www.symantec.co.jp/region/jp/sarcj/index.html

- IPA情報処理進行事業協会

  http://www.ipa.go.jp/