コンピュータ概論B - ソフトウェアを中心に -

#11 セキュリティ

Yutaka Yasuda

情報セキュリティ

- 安全な情報サービスのために維持すべき性質
- 機密性： Confidentiality

  誰がその情報にアクセスして良いか
- 完全性： Integrity

  情報（やソフトウェア）が真正のものか
- 可用性： Availability

  必要な時に確実に情報にアクセスできるか

セキュリティ管理

- 他者との接触によっておびやかされる

  機会の増加：データのやりとり

  状況の変化：オープンなネットワークへの接続

- これら要素別にそのリスクを検討し、対策する

  事故・悪意のある処理によって破られない

  破られた場合の影響を許容範囲に収める

前提

- この場では余り重点的に扱わない事も多い

  物理セキュリティ

  社会工学 (social engineering)

  （内部者による）データ改ざんなどに伴う犯罪行為

  デジタルフォレンジック digital forensics

- 現実には安全管理は一般に総力戦であることを忘れず

  教育も行う（直接的なものだけでなく情報倫理も含め）

脅威

- 機密性・完全性の側面から

  データの改ざん、漏洩、なりすまし、Phishing

- 可用性の側面から

  サービスの妨害、資源の浪費

- 対策

  ウィルス検知ソフト、ファイアウォール、etc.

ウィルス検出ソフト

- PC が自身の処理内容を監視

  ネットワーク、ファイルのアクセス等

  Malware を検出・検疫・削除

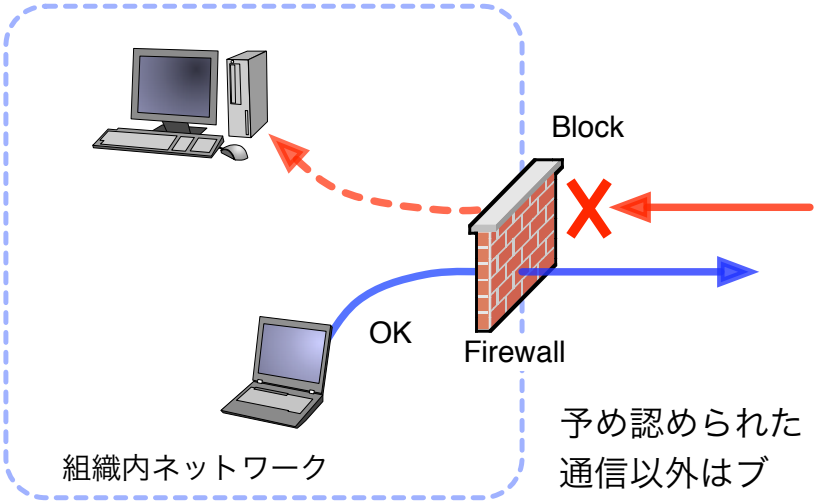
- 問題

  アップデート vs 亜種

  ゼロディ攻撃

  システム負荷（パフォーマンスへの影響）

ファイアウォール

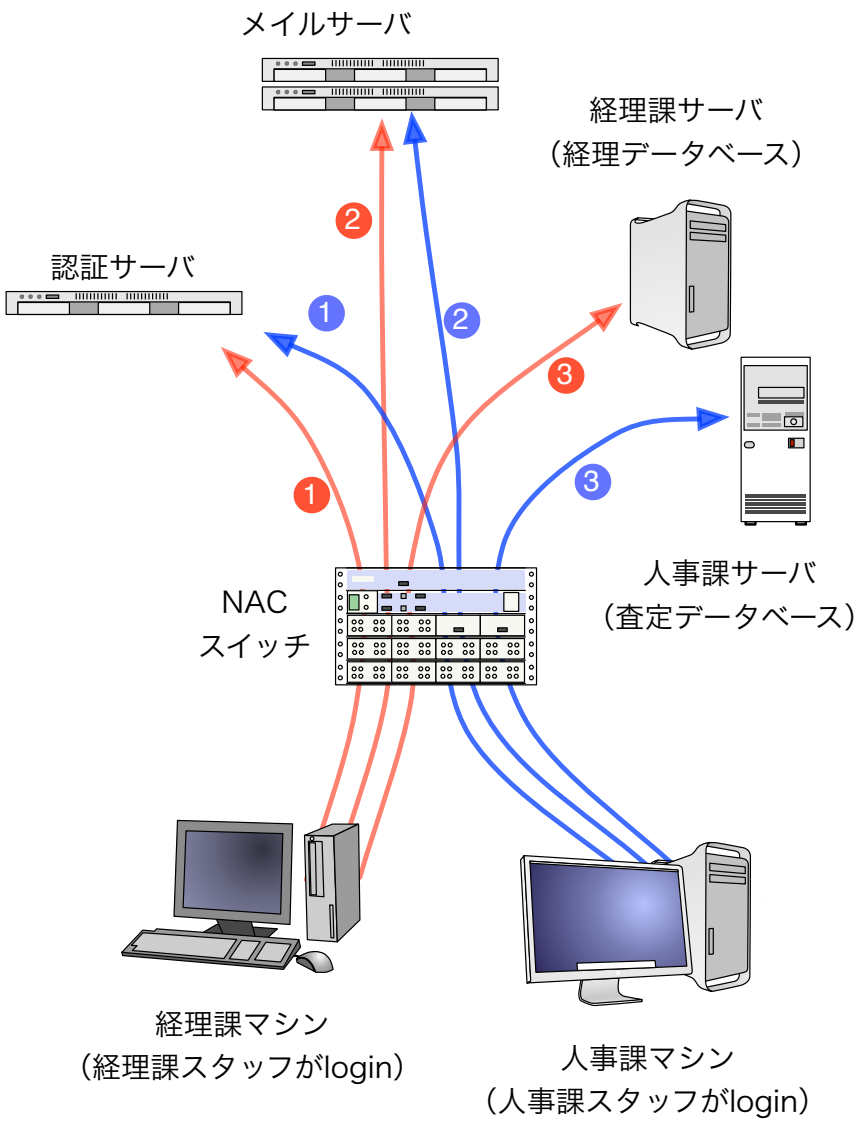


- ネットワーク越しの侵入を防ぐ
  - セキュリティ・ホールを狙った攻撃
  - 漏洩した・推測されたパスワードによるアクセス
  - 予め認められた通信以外をブロックする etc.
- インターネット接続点に設置
  - いまどきは各マシンごとに設定
  - default で on に（Windows なら XP SP2 以降）
- 内と外の区別が無くなった
  - ウィルス感染した内部のPCが攻撃する

参考：NAC

- Network Access Control or Network Admission Control
- 異常の検出
  - 機器の監視（登録）
  - 経路の監視
  - ユーザ認証との組み合わせ
- アクセス制限
  - ユーザ情報に従ってアクセス可能な資源を限定

まずユーザ認証してからサービスにアクセス
部署ごとにアクセスできるサービスなどが限定される
Internet へのアクセス可否なども設定可能



実際の製品例：Cisco NAC アプライアンス (Clean Access) 概要
http://www.cisco.com/web/JP/product/hs/security/cca/prodlit/pdf/nacapp_atg.pdf

侵入口

- セキュリティホール（exploit：脆弱性）

  不正パスワード取得にしてもその後の権限昇格が問題

- 本来はソフトウェアの欠陥（バグ）

  従来から存在する問題だが近年脅威が増しつつある

  インターネット接続＋再攻撃可能なOSの普及

- 実際に多い（報告されているだけでも）
- 基本的にはアップデートで対応

  ゼロディ問題（再び）

誤：感染する機会が無ければ良いのではないか？

- IPA 2010/12/6 【今月の呼びかけ】

  ウェブサイトを閲覧しただけでウイルスに感染させられる “ドライブ・バイ・ダウンロード” 攻撃に注意しましょう!

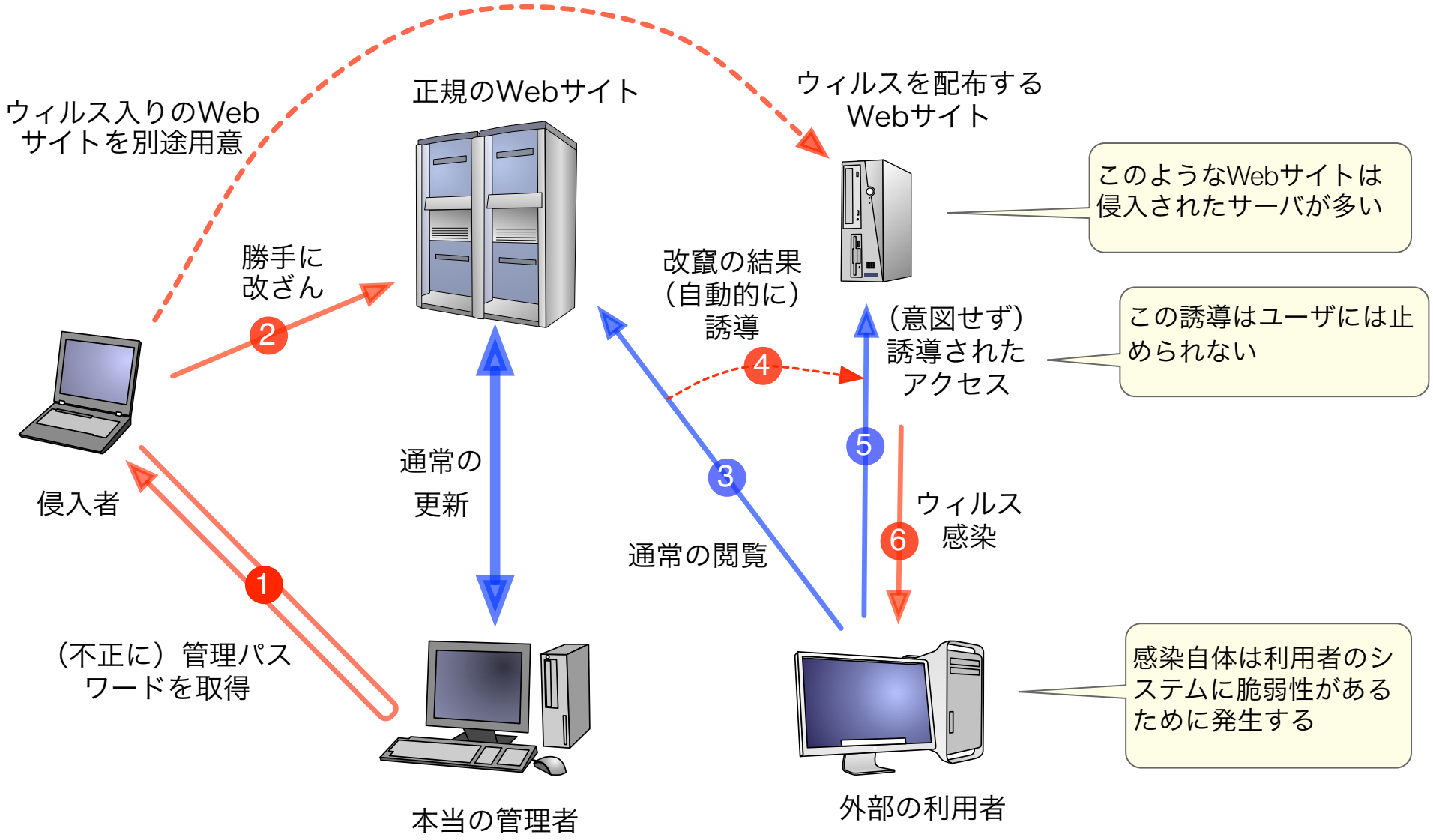
- ドライブ・バイ・ダウンロード

  悪意のあるWebサイトを閲覧しただけで感染させられる手法（セキュリティ・ホールを衝く）

- 誤：怪しいサイトを意図して閲覧しなければ良い

  正当なWebサーバの改竄もあり得る（ガンブラー）

事例：ガンブラー（手法）


ウィルス入りのWeb
サイトを別途用意
正規のWebサイト
ウィルスを配布する
Webサイト
このようなWebサイトは
侵入されたサーバが多い
勝手に
改ざん
2
改竄の結果
（自動的に）
誘導
4
（意図せず）
誘導された
アクセス
この誘導はユーザには止
められない
侵入者
通常の
更新
3
5
ウィルス
感染
6
通常の閲覧
1
（不正に）管理パス
ワードを取得
本当の管理者
外部の利用者
感染自体は利用者のシ
ステムに脆弱性がある
ために発生する

Botnet

- ボット(Bot)

  悪意を持った誰かによってネットワーク越しにコントロールされているマシン

  持ち主が知らない間に遠隔操作用のプログラムを仕込まれてしまう

  そのうちに他のマシンの攻撃に加担

  そのような状態にあっても持ち主は気づかない

  ネット上に大量に存在し、組織的に利用 → **Botnet**

- 愉快犯ではなく犯罪目的

サイバークリーンセンターによる2008年6月の国内ボット感染者数調査（推定）
「ブロードバンドユーザ約3000万人のうち約30万人（感染率約1％）」
https://www.ccc.go.jp/bot/index.html

不正・犯罪行為への加担

- SPAM 送信
- DoS 攻撃（Denial of Service）
- さらなる感染
- ついで(?)にキースキャンなど

行動管理

- オンラインゲーム設定

  パソコン購入直後のセキュリティ設定

  インターネット利用時のセキュリティ設定

  メイル利用時のセキュリティ設定

- ウィルス感染を防ぐ
- 侵入対策
- 情報漏洩防止
- スパイウェア対策
- Phishing 詐欺対策
- ワンクリック詐欺防止
- 無線LAN設定
- etc. etc.

IPA 情報セキュリティ「個人の方」http://www.ipa.go.jp/security/personal/

Phishing 詐欺（手法）

- 例：
  1. 銀行を装ってオンライン口座にアクセスさせるようなメイルを送る（「住所の確認をしています」etc.）
  2. 書かれていたURLをクリックすると全然違うサイトへ
  3. しかし見た目はいつもの login 画面そっくり
  4. いつものユーザ名とパスワードを入力（これを取得）
  5. あたかもパスワードを打ち間違えたかのようなメッセージを出して、本物の銀行の login 画面に移動させる
- 予備知識

  メイルの送信者欄は全く信用できない（擬装可能）

IPA 情報セキュリティ「個人の方」フィッシング対策 http://www.ipa.go.jp/security/personal/protect/phishing.html

Phishing 詐欺（対策）

- アクセス先の確認

  そもそもパスワードを入力させるような作業がメイルで来ることはない

- メイルの URL を信用しない

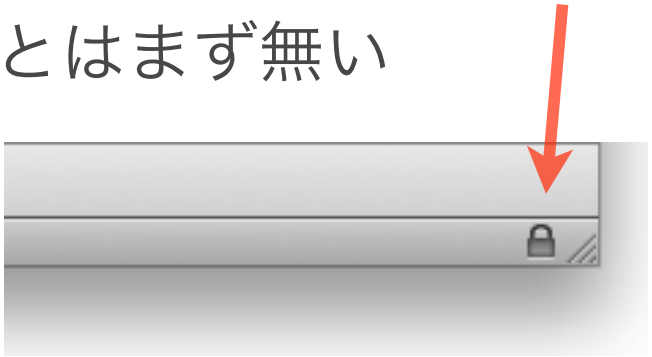
  ブックマークなり信頼できるリンクからアクセス

  URL のドメイン名を確認

- HTTPS によるアクセス

  パスワードを暗号化無しで入れることはまず無い

  https://... なら電子証明書を確認



IPA 情報セキュリティ「個人の方」フィッシング対策 http://www.ipa.go.jp/security/personal/protect/phishing.html

信頼できる証明書？？


一般
詳細
この証明書は以下の用途に使用する証明書であると検証されました:
SSL サーバ証明書
発行対象
一般名称 (CN) mail.google.com
組織 (O) Google Inc
部門 (OU) <証明書に記載されていません>
シリアル番号 1F:19:F6:DE:35:DD:63:A1:42:91:8A:D5:2C:C0:AB:12
発行者
一般名称 (CN) Thawte SGC CA
組織 (O) Thawte Consulting (Pty) Ltd.
部門 (OU) <証明書に記載されていません>
証明書の有効期間
発行日 09/12/18
有効期限 11/12/19
証明書のフィンガープリント
SHA1 フィンガープリント 68:AC:69:DF:BE:72:B3:0D:08:0E:54:10:84:FD:78:91:FC:BD:6D:9B
MD5 フィンガープリント 52:12:A2:B1:27:E3:BB:CC:E5:F5:AA:BD:A1:A1:E6:F8

多機能化への要求：UTM

- Unified Threat Management （統合型セキュリティ管理）

  Anti Virus, Anti SPAM （メッセージ処理）

  コンテンツフィルタ（Web アクセス）

  トラフィック抑制・遮断（P2P等）

  侵入検知 (IDS) 、侵入防止 (IPS)

  VPN 接続（正規利用者の内部ネットワークへの接続）

まとめ

- ネットワーク越しの攻撃
  - 侵入（データの取得やコントロール目的）
  - DoS （サービス妨害）
  - ボット
- 対策
  - システムアップデート、ウィルス検出ソフト、ファイアウォール、etc.
  - 個別対応の積み重ねしかない
  - 技術・教育・社会制度（法）も含めて前進
- 加害者とならないよう

参考：Google Chrome

- セキュリティ・ホールによる影響を軽減する
  - ドライブ・バイ・ダウンロード, ゼロディなどに対応
  - 突破されても被害を最小限に
- サンドボックス
  - マルチプログラミングの性質を利用
  - ブラウザのタブごとに別のプロセスとして実行
  - 攻撃の影響を最小化（閉じれば影響は消える（かも））
- Chrome 8 - PDF Viewerを内蔵、サンドボックス内で実行
- Adobe Reader もサンドボックス実行モデルをとる