3年次演習

第9回
セキュリティのおはなし(1)

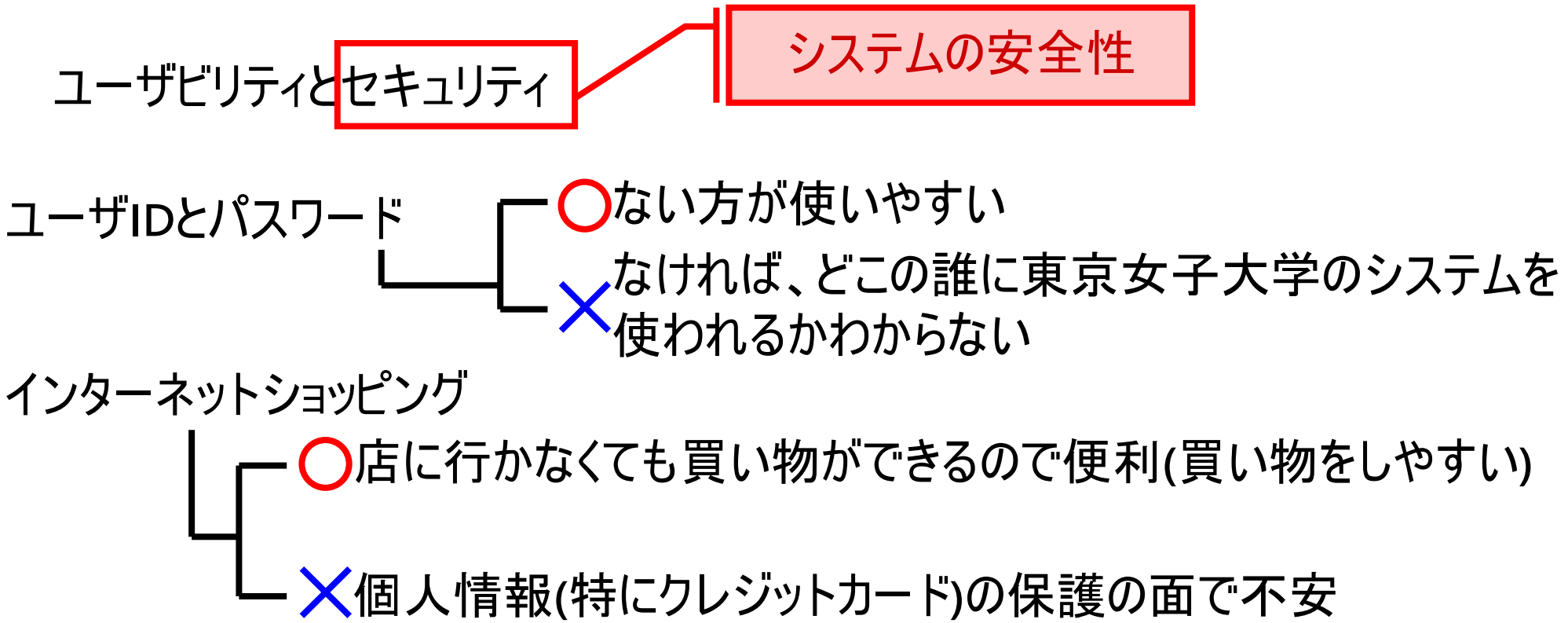
人間科学科コミュニケーション専攻
白銀 純子

今回の内容

- セキュリティ
  - 主に企業・組織の観点から

ユーザビリティとセキュリティのトレードオフ

- トレードオフ: 一方を取ればもう一方を取れないという関係



どこで折り合いをつけるかは非常に難しい問題

ただし、現在は多少利便性を犠牲にしてもセキュリティを上げておく必要

セキュリティ関係の事件簿

- 日本年金機構の個人情報流出(2015)
- ベネッセコーポレーションの個人情報流出(2014)
- DDos攻撃でPlaystation Networkがダウン (2014)
- LINEアカウントの乗っ取り(2014～)
- インターネットバンキングでの不正送金
- 企業・官公庁のWebサイト改ざん
- 無線LANの不正使用

事件一覧

- 個人情報漏洩事件・事故一覧: http://www.security-next.com/category/cat191/cat25
- サイバーセキュリティ事件簿: http://www.mbsd.jp/casebook_index.html

不正アクセス

不正アクセス

- 不正アクセス: 権限を持たない人が不正にコンピュータを利用すること
  - データが盗まれる
  - システムが破壊される
  - ウィルスなどを置いていかれる
  - etc.

企業・組織に対するネットワークを通じた様々な攻撃の手段

- 侵入方法
  - 何らかの手段で入手した利用者のIDとパスワードを利用
  - セキュリティホールやソフトウェアの設定ミス、開いているポートを利用
  - 侵入するときに、侵入者は自分のIPアドレスを偽装することも

不正アクセスによってなされる悪事

- データの閲覧・改ざん・収集
  - 侵入したコンピュータに保存されているデータの閲覧・改ざん・収集
    - インターネットバンキングの不正送金では、勝手に別の口座にお金を送金される
  - 個人情報の流出のもと
- 他のコンピュータへの攻撃
  - 他のコンピュータと時期をあわせて一斉に官公庁や企業のコンピュータに攻撃
  - 官公庁や企業のコンピュータに不具合を起こさせたり、壊すことが目的
- ウィルス感染
  - 侵入したコンピュータにウィルスを置いていき、感染
  - 他のコンピュータへの一斉攻撃の足がかり

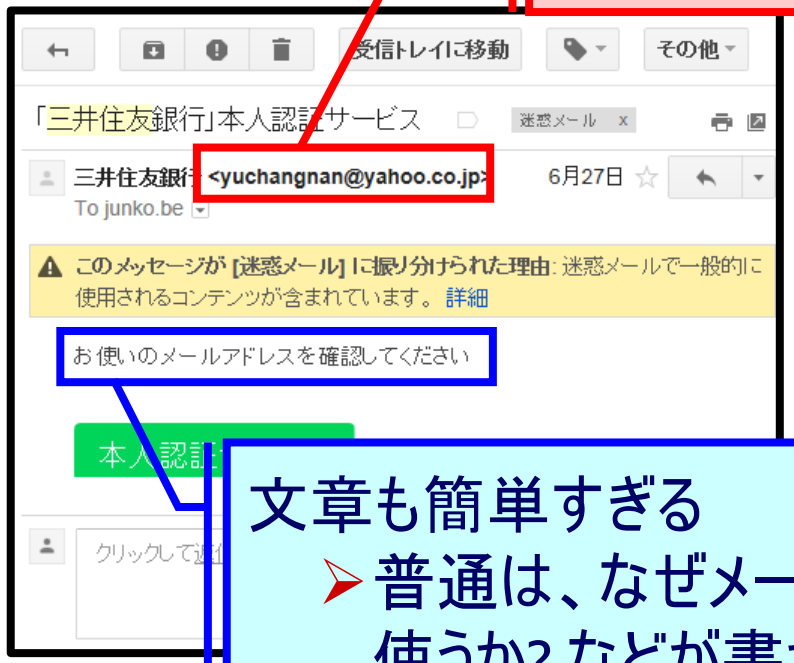
IDとパスワードの流出(1)

- フィッシング詐欺
  - アクセス先を書いたメールを送信し、アクセスさせる
    - アクセス先は、銀行やクレジットカードの会社などを装っている
  - 開いたページで個人情報を入力させる
    - 開いたページは、もっともらしく作ってある
    - ウィルスを使って本物のサイトにアクセスさせないケースもある
  - 入力された情報を盗み取る
    - IDとパスワードだけでなく、様々な個人情報を盗む

IDとパスワードの流出(2)

- 実際のフィッシング詐欺の例

ドメインから考えて、銀行のメールアドレスではない
- メールアドレスはYahoo!のフリーメールになっている
- まともな銀行が、フリーメールでメールを送ってくるはずがない



文章も簡単すぎる
- 普通は、なぜメールアドレスの確認が必要か? 何のためにこの情報を使うか? などが書かれてあるはず
- 問い合わせ窓口もあるはず

IDとパスワードの流出(3)

- パスワードクラック(パスワード攻撃)
  - IDを入手し、そのIDに対応するパスワードを調査
    - 手当たり次第にパスワードを入力して調査
    - 辞書(単語, 人名, 地名, etc.)を使ってパスワードを作り出して調査(辞書攻撃)

コンピュータを使って手当たりしだいに調査

- キーロガーを利用
  - キーロガー: キーボードのキー入力を記録するソフトウェア
  - インターネットカフェなど不特定多数の人が利用するPCに仕込んで入力された様々な情報(ID, パスワード, その他個人情報)を取得
- IDとパスワードの持ち主による漏洩

ポートを使った攻撃(1)

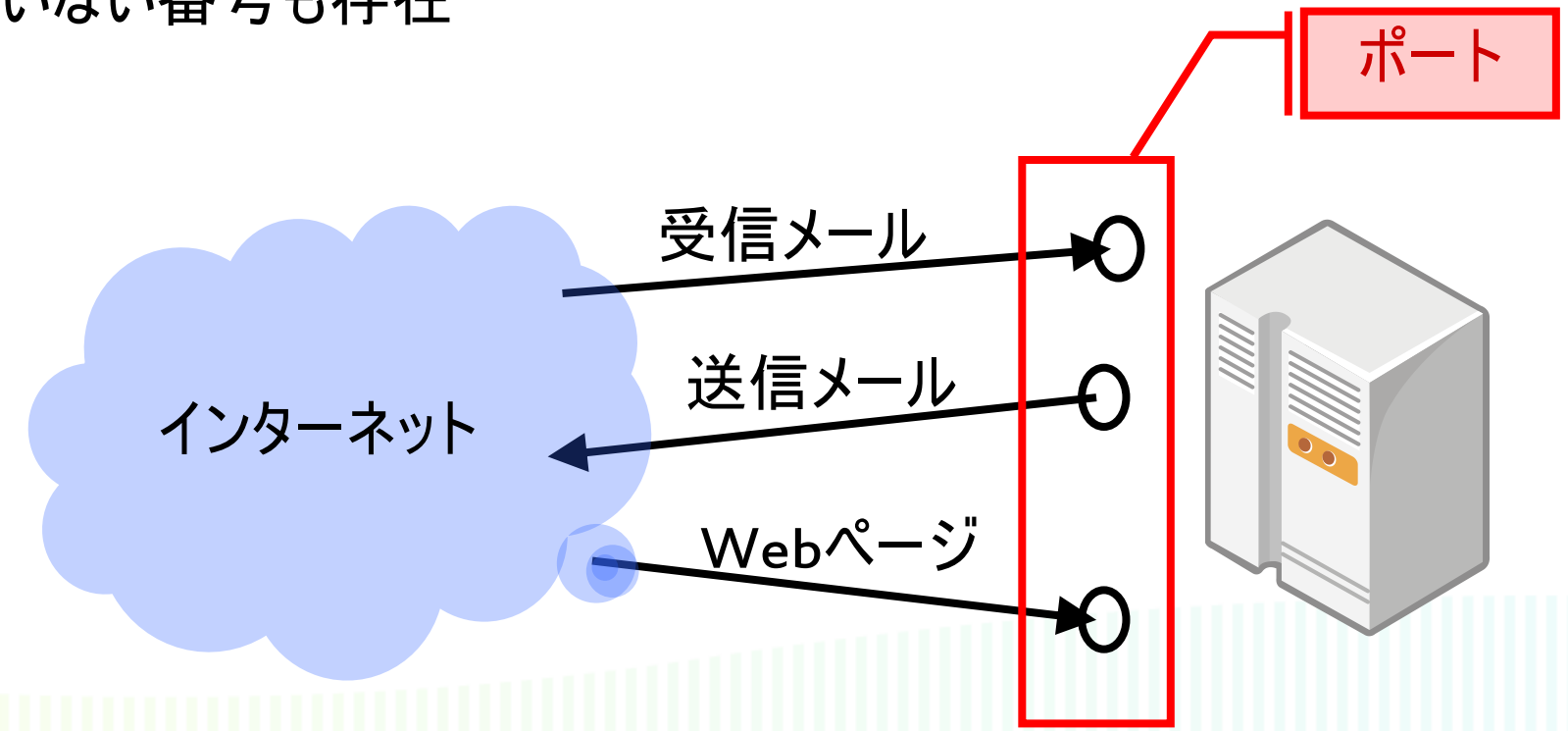
- ネットワークでのコンピュータは、アパート or マンションのようなもの
  - IPアドレス(ネットワークでのコンピュータの住所)は、アパート or マンションの住所のイメージ
- ネットワークでやりとりされるデータは、アパート or マンションの各部屋からやりとりされるもの

データに関して、どこに送るか・どこから送られるかの部屋番号が必要

部屋番号 = ポート

ポートを使った攻撃(2)

- ポート: コンピュータへデータが出入りする部屋番号
  - 1つのコンピュータに多くのポートが存在
  - 原則として、通信の種類によってどの番号を使うかは決定済み
    - メール受信・メール送信・Webページアクセスなど
    - 使われていない番号も存在



ポートを使った攻撃(3)

- ポートを使うには、ポートを開いておく(部屋のドアを開いておく)必要
  - ポートは、アパート or マンションの玄関のドアのようなイメージ
- ポートを開いておくことで、攻撃のターゲットに
  - 攻撃対象のコンピュータの、開いているポートの有無を調査(ポートスキャン)
  - 開いているポートが見つかったら、そこを突破口にして対象のコンピュータに攻撃

ポートを使った攻撃を防止するには?(1)

- ポートは全て閉じておきたい!

  でも…
- メールやWebなどは、ポートを開いておかないと利用できない

  なので…
- 必要なポートのみ開いておき、不要なポートを閉じておく
  - どのポートが必要で、どのポートが不要かの判断が難しい

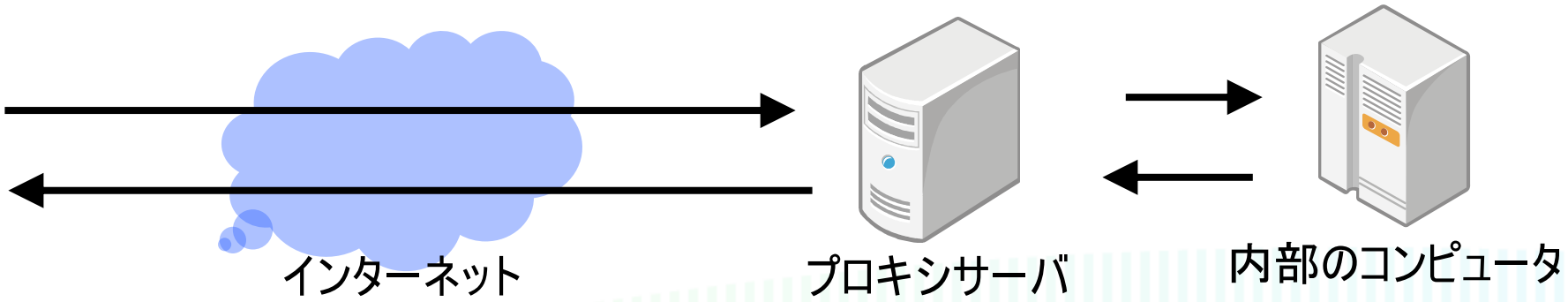
ポートを使った攻撃を防止するには?(2)

- 不要なポートを閉じる: ファイアウォールを導入する
  - ファイアウォール: コンピュータに出入りするデータを監視して、許可されているデータのみ通す(フィルタリング)ためのソフトウェアや機器
    - 許可されていないものは廃棄
  - ちなみに...個人のPC用のファイアウォールソフト(パーソナルファイアウォール)もたくさんあり、簡単に導入可能
    - Windows XP Service Pack 2以降に付属
    - ウィルスソフトを開発・提供している会社で、ウィルスソフトと一緒にして提供しているものも
    - etc.

Windowsのものよりも高機能なので、こちらを導入することがおすすめ

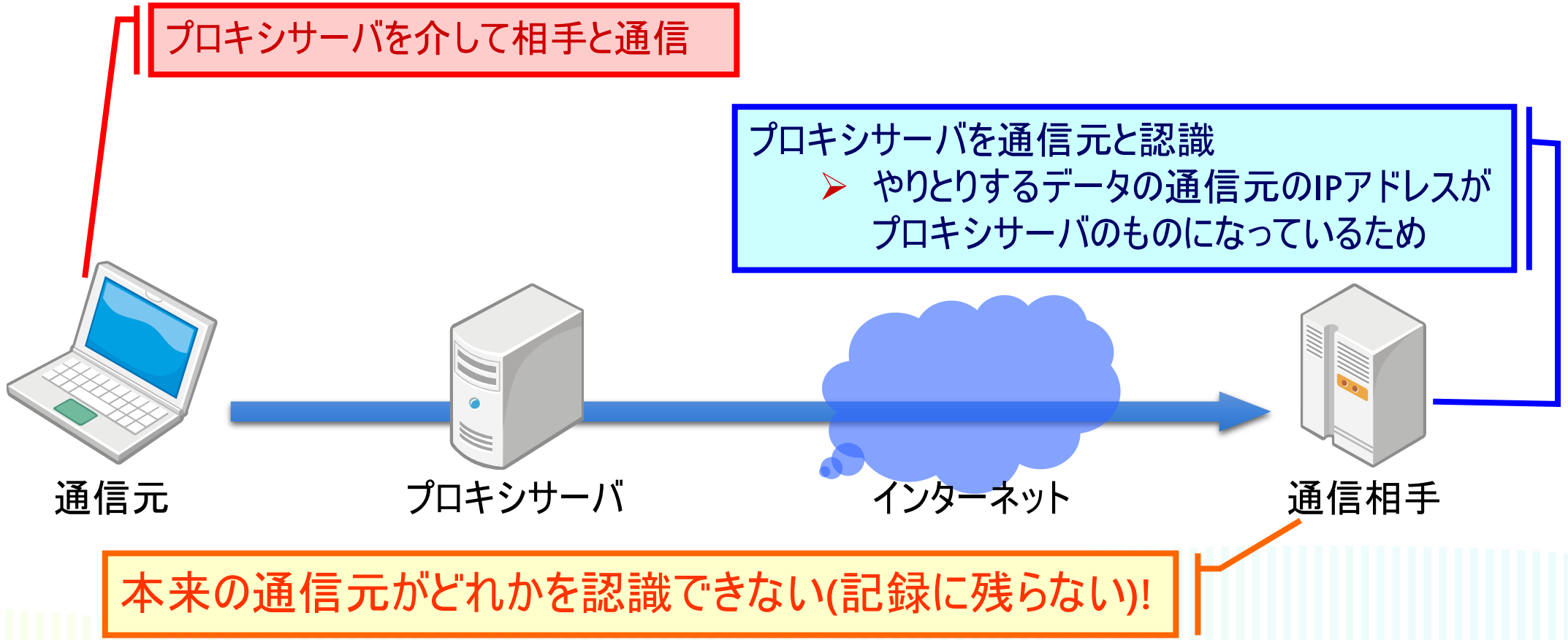
IPアドレスの偽装(1)

- プロキシサーバ: 不正アクセスから内部のコンピュータを守るための仕組み
  - 外部から直接アクセスできるコンピュータを少数に限定する
    - このコンピュータを「プロキシサーバ」と呼ぶ
  - 外部からのアクセスは、必ずプロキシサーバを通して行う
  - 不正アクセスで攻撃されるのは、プロキシサーバだけになる
  - 内部の重要なコンピュータは壊されない



IPアドレスの偽装(2)

- 本来はプロキシサーバは不正アクセスを防止するためのものだけど…
  - プロキシサーバを使った通信は、相手先から本来の通信相手を隠す
    - 相手先で通信相手として記録されるIPアドレスが、プロキシサーバのIPアドレスになる



IPアドレスの偽装(2)

- 不正アクセスの攻撃者はプロキシサーバで自分のIPアドレスを偽装(プロキシサーバを「踏み台」にする、と呼ぶ)
  - 被害にあったコンピュータの通信の履歴(アクセスログ)にはプロキシサーバのIPアドレスが記録
  - 攻撃者本人のコンピュータのIPアドレスは記録なし

攻撃されると、攻撃者を特定して対処する必要

- IPアドレスをもとに攻撃者を特定
- IPアドレスが偽装されていると、偽装されたプロキシサーバからさらにたどる必要
  - ✓ 複数のプロキシサーバを踏み台にしている場合も

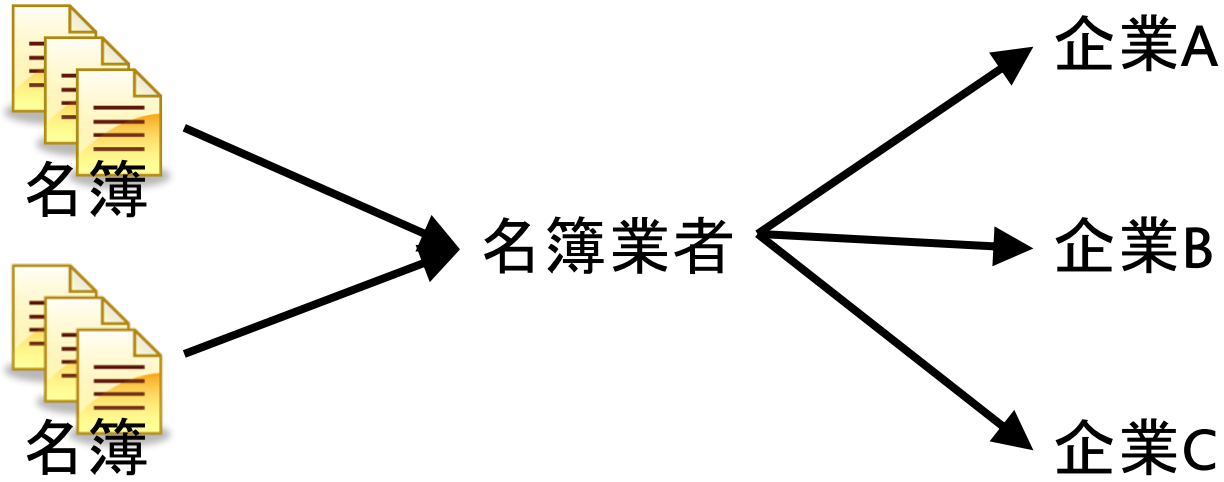
↓

攻撃者の特定がしにくくなる

個人情報の流出

なぜ流出事件が多いか??

- 個人情報はお金になるから!
  - まともな企業でも個人情報は欲しい
    - ダイレクトメールや勧誘などの営業のために...



- 興味本位や個人的欲求
  - 仕事で会う人の個人情報を見てみたかった!
  - 気になる人の家に訪ねたい!
  - etc.

どうやって流出するか??(1)

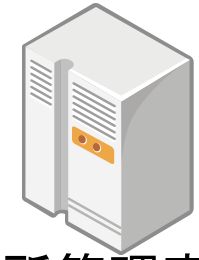
- 個人情報を扱っているコンピュータへの不正アクセス
  - IDとパスワードの利用
    - 簡単なパスワードを設定していたためにパスワードを解析された
    - 他人にパスワードを教えてしまった
    - etc.
  - コンピュータ利用上のミス
    - 世界中に公開している場所に個人情報を置いてしまった
    - セキュリティホールを埋めるパッチを適用していなかった
      - セキュリティホール: ウィルスや不正アクセスをされやすい、ソフトウェアの不具合
      - パッチ: セキュリティホールやその他不具合を修正するための差分ソフトウェア
    - etc.
  - ウィルスを介した乗っ取りやセキュリティホールをついた攻撃
  - etc.

どうやって流出するか??(2)

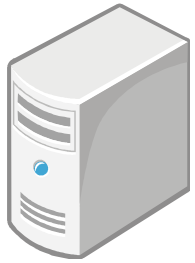
- 個人情報へのアクセスが許可された人が持ち出し
  - 故意に持ち出し
    - 売ってお金儲けが目的、など
  - 管理不行き届き
    - 個人情報の入ったノートPCを電車内などに置き忘れた、など
- 古いPCや携帯電話、スマホなどの機器類の処分
  - 保存されていたデータの消し忘れ
  - データを消していても、データ復元ソフトで読み取り
    - データをゴミ箱に入れ、ゴミ箱から消去しても、データ復元ソフトで復元できるものも多い

日本年金機構での個人情報流出～前提知識～

- 個人情報の取り扱い: 個人情報は断片にされて別々のコンピュータで管理
  - 住所や氏名、電話番号、年金番号など、バラバラにして管理
  - 1つ1つのデータを見ただけでは、個人の特定は不可
- ファイルにパスワードをかければ、各情報を集めて保存してもOKというルール
  - 個人と連絡を取りたいときなど



住所管理専門



氏名管理専門

日本年金機構での個人情報流出～経緯～(1)

- 職員が各情報を集めてファイルに保存した作業をした
  - 大半のファイルにパスワードかかけられていなかった
- ファイルを保存したコンピュータをネットワークに接続したまま、メールを読んだ
  - 件名はまともそうなメール
  - 添付ファイルも開封
    →ウィルスつきの添付ファイルで、職員のPCがウィルスに感染
    - 数人の職員が同様にメールの添付ファイルを開封してPCがウィルスに感染
    - ウィルスはいくつかの違う種類のものだったが、ほとんどが新しいもの

日本年金機構での個人情報流出～経緯～(2)

- ネットワークを通じて他のPCにもウィルスが広まった
  - ネットワークは接続したまま
  - ウィルス対策ソフトは更新
- ウィルスを介してファイルを保存したコンピュータにアクセスされた

DoS攻撃

DoS(Denial of Sevice)攻撃って?

- コンピュータに大量の負荷をかけて、コンピュータを動作不能にする攻撃
  - スパムメールを一斉に大量に送りつける(メール爆弾, メールボム)
    - DoS攻撃ではないが、あけおめメールとか災害時の一斉安否確認なども同様の結果に
  - Webページへの一斉の大量アクセス
  - etc.

コンピュータの処理能力の限界を超えさせる攻撃

- 複数のコンピュータから一斉に攻撃することをDDos攻撃
  - DDos: Distributed Deinal of Service

DoS攻撃の理由と影響

- なぜDoS攻撃をするのか?
  - 愉快犯
    - おもしろそうなソフトがあったから使ってみた、とか...
  - 自分の技術力の自慢
  - 攻撃先に対するうらみ, etc.
- DoS攻撃されるとどうなるか?
  - 提供していたサービスをユーザが利用できなくなる
    - ゲームであれば遊べなくなる
    - メールのやり取りができなくなる, etc.

ものによっては深刻な影響も...

- 銀行や株式のシステムが攻撃されると、経済に影響
- 電車や飛行機のシステムが攻撃されると、人命に影響

Webページの改ざん

Webページの改ざんって??

- Webページが、本来の内容とは違うものに変更されてしまうこと
  - 不正アクセスの一種
  - 見た目に変わりなくても、何か仕込まれていることも…

- 改ざんの目的
  - 愉快犯
  - 自己主張: 自分の主義主張を世に知らせたい
  - 攻撃先へのうらみ: 改ざんすることによって信頼のできない官公庁や企業であることを知らせたい
  - ウィルスのばらまき: アクセスしてきたコンピュータをウィルスに感染させたい
    - DDoS攻撃に参加させるためとか

どうやって改ざんする?

- Webページの管理用IDとパスワードの入手
- 設定ミスがないかを調査
- セキュリティホールの利用
- ウィルスを送りつけ

セキュリティ関連の事件を防ぐには?

結局のところ…

- セキュリティ関係の事件の主な原因
  - IDやパスワードの流出
  - 設定・利用上のミス
  - ソフトウェア(OS, ウィルス対策ソフト, その他ソフトウェア)のアップデートの怠り
  - ユーザの故意・過失
  - セキュリティホール
  - ウィルス

利用者(人間)側の問題

(アップデートの怠りなどがなければ)コンピュータ側の原因

コンピュータでの対策は当然ながら、人間側の意識改善が一番必要!

- 企業・組織でのセキュリティのあり方(セキュリティポリシー)を策定する
- ユーザに対する教育をきちんと行って意識を向上させる

日本年金機構での個人情報流出での分類(1)

- 職員が各情報を集めてファイルに保存した作業をした
  - 大半のファイルにパスワードかかけられていなかった
- ファイルを保存したコンピュータをネットワークに接続したまま、メールを読んだ
  - 件名はまともそうなメール
  - 添付ファイルも開封

→ウィルスつきの添付ファイルで、職員のPCがウィルスに感染

- 数人の職員が同様にメールの添付ファイルを開封してPCがウィルスに感染
- ウィルスはいくつかの違う種類のものだったが、ほとんどが新しいもの

コンピュータ側の問題
- ウィルス対策ソフトは使っていたようなので

個人の問題
- ファイルにパスワードをかけなかったのはルール違反
- 添付ファイルをむやみに開かないのはセキュリティの基本
  - ✓ ただし、組織の教育体制の不備である可能性も

日本年金機構での個人情報流出での分類(2)

- ネットワークを通じて他のPCにもウィルスが広まった
  - ネットワークは接続したまま
  - ウィルス対策ソフトは更新
- ウィルスを介してファイルを保存したコンピュータにアクセスされた

(おそらく)組織の考え方(体質)の問題
- 接続したままで良いという判断は組織の上部や全体でしているはず

やってみよう!

- ニュースに出てきた企業や組織のセキュリティ関連の事件をいくつか探して、原因を分類してみよう
  1. 企業・組織の考え方(体質・セキュリティポリシー)の問題?
  2. 働いている個人の問題(教育の問題)?
  3. コンピュータ側の問題(1. と2. はきちんと行っていたのでどうしようもなかった)?
- さらに、対処によってユーザビリティの問題が起こりそうかも考えてみよう

※自分はどう分類できると思ったか? でOK