サーバの
セキュリティ対策に関して

特定非営利活動法人　学習開発研究所
副代表　三輪吉和

Institute for Learning Development

アジェンダ

- 自己紹介
- セキュリティとは
- セキュリティポリシー
- ネットワークのデザイン
- サーバの運用
- 最近の話題
- まとめ

Institute for Learning Development

自己紹介

- 特定非営利活動法人　学習開発研究所　副代表
  - 2004年4月　特定非営利活動法人として認可
  - ユビキタスラーニングの実現に貢献することを目的
- 主な実績
  - 教室内LANシステム開発
  - 全国の教育ネットワーク調査
    - http://www.cec.or.jp/es/E-square/h9seika2/index.htm
    - http://www.cec.or.jp/es/E-square/h10seika/html-II/II-Index.htm
    - http://www.cec.or.jp/es/E-square/books/chiiki/index.htm
  - 教育ネットワークの構築・運営
    - 京田辺市小中学校間ネットワーク
    - 京都府情報教育ネットワークヘルプデスクなど

Institute for Learning Development

「セキュリティ」とは

- 何から何を守るのか？
  - 何を守る
    - 個人情報？
      - 何が個人情報？
    - 機器の安定稼動
  - なぜ守るのか？
    - 不正利用（目的外使用）を防ぐ？
  - どのように守るのか？
    - 鍵をかける
    - 隠す

交通事故対策は

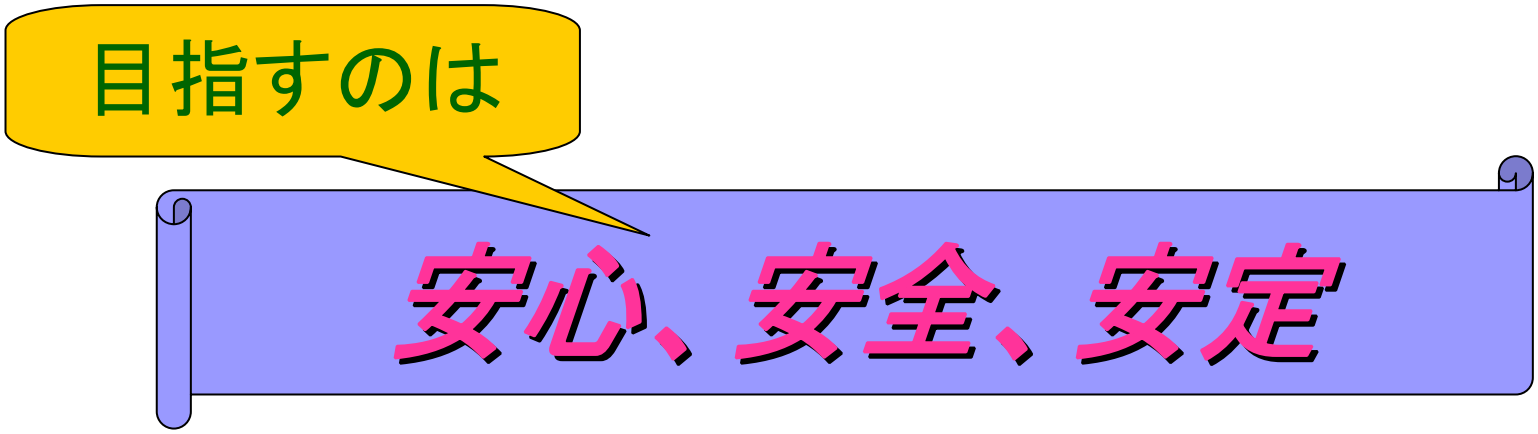
- 啓蒙
  - 交通安全教室
  - 長期休暇前にプリント配布
  - 自転車の乗り方
  - 集団登校
- 警察
  - 取り締まり
  - 規制や信号
- 行政
  - 道路の改良
  - ガードレール
- 保険
  - 自賠責保険、任意保険
  - 生命保険

結局はリスク管理

発生数を減少させることはできる

- 事故の規模を小さくすることはできる
- しかし…

事故発生を0にすることは無理



セキュリティ管理

- 適切なコストで耐久性の高い「システム」の実現
- 見渡しの良い実施構造
  - 目標設定＝ セキュリティポリシー
  - 実現のための手段
    - 使えるものは全て使う
    - 技術、制度、慣行、契約、….
  - 状況変化への対応
    - 見直し
  - 平常時と緊急時の対応
    - 万が一のときに備える
    - 短時間で平常時へ復旧

セキュリティポリシー

- 事故発生を前提に
- 利用者も含めて全員が関係者
- 運用方針（どのように守るのか）
  - 不要な人には利用させない（保管）
    - アクセス管理
    - パスワード管理
  - 誰が使ったかを明確に（記録）
    - 記録をきちんと採取する
  - 事故発生時の対策（危機管理）
    - 誰が誰に報告し、迅速にどう対処するか

セキュリティの対象

- ネットワークセキュリティ
- サーバセキュリティ
- パソコンのセキュリティ
- ソーシャルセキュリティ

ネットワークのセキュリティデザイン

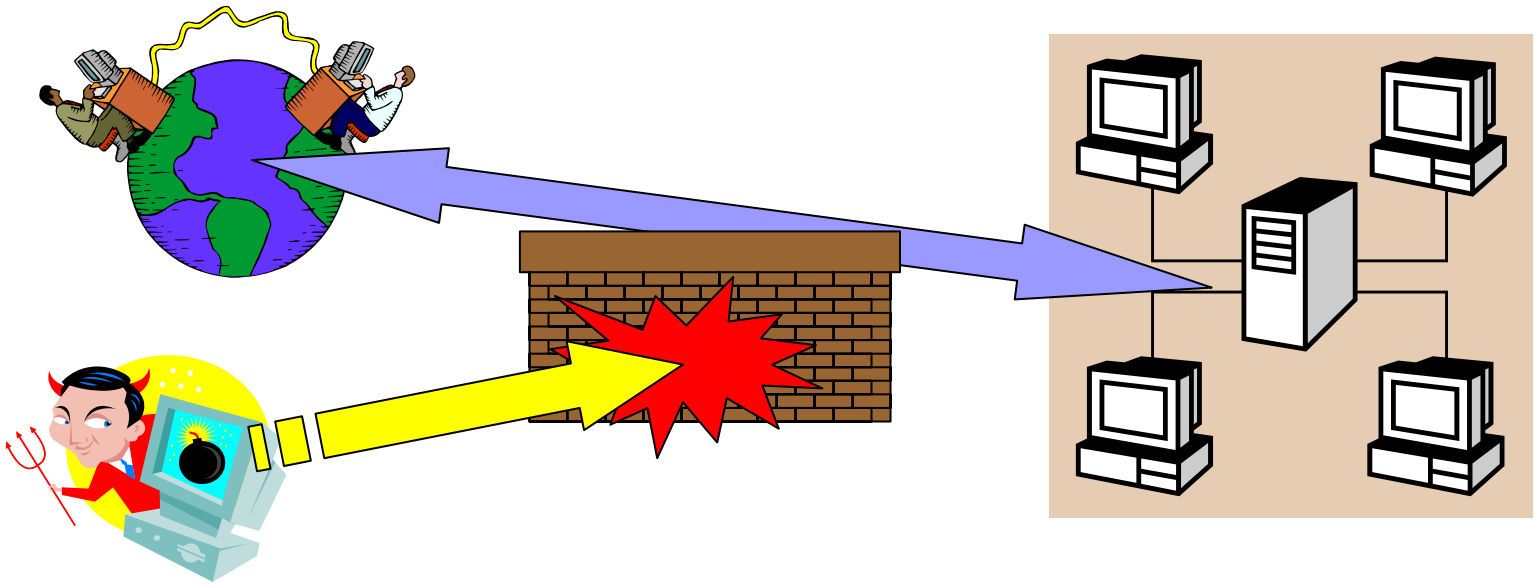
- 守りのために
  - ファイアーウォールとDMZ
  - 便利さと危険さと…無線LAN対策
  - 複数のセグメントに分割
    - 指導者用（事務職、管理職、教材研究、…）
    - 学習者用
    - 部外者用（PTA、学校開放などでの地域住民利用）

危ないのは機器よりも「ヒト」

- ソーシャルセキュリティ
  - 敵は内にあり
    - イントラネットの内側から攻撃があったら？
      - 雑誌の付録のソフトでちょっと実験した
    - 「代わりに〇〇するからパスワードを教えて」と言われたら？
    - 「警察ですが…」と電話があったら？
- セキュリティと便利さは相反する
  - 不便だから、ちょっとくらい設定を…
  - パスワードが覚えられないから…
- 日ごろからの心構え
  - わたしだけは大丈夫だから…しなくても

ファイアーウォール

- 対外防護壁のこと
- ルータの設定や専用機器で実現
- 利用できる通信がある＝これ以外の対策も必要



無線LAN
覚えておくべきキーワード

- 通信規格
  - 802.11b、802.11a、802.11g
- グループ化
  - ESS-ID
- 暗号化
  - WEPとWPAと802.11i
- 認証
  - 802.11x

	使用周波数	最大通信速度
802.11b	2.4GHz帯	11Mビット/秒
802.11a	5GHz帯	54Mビット/秒
802.11g	2.4GHz帯	54Mビット/秒

Institute for Learning Development

グループ化

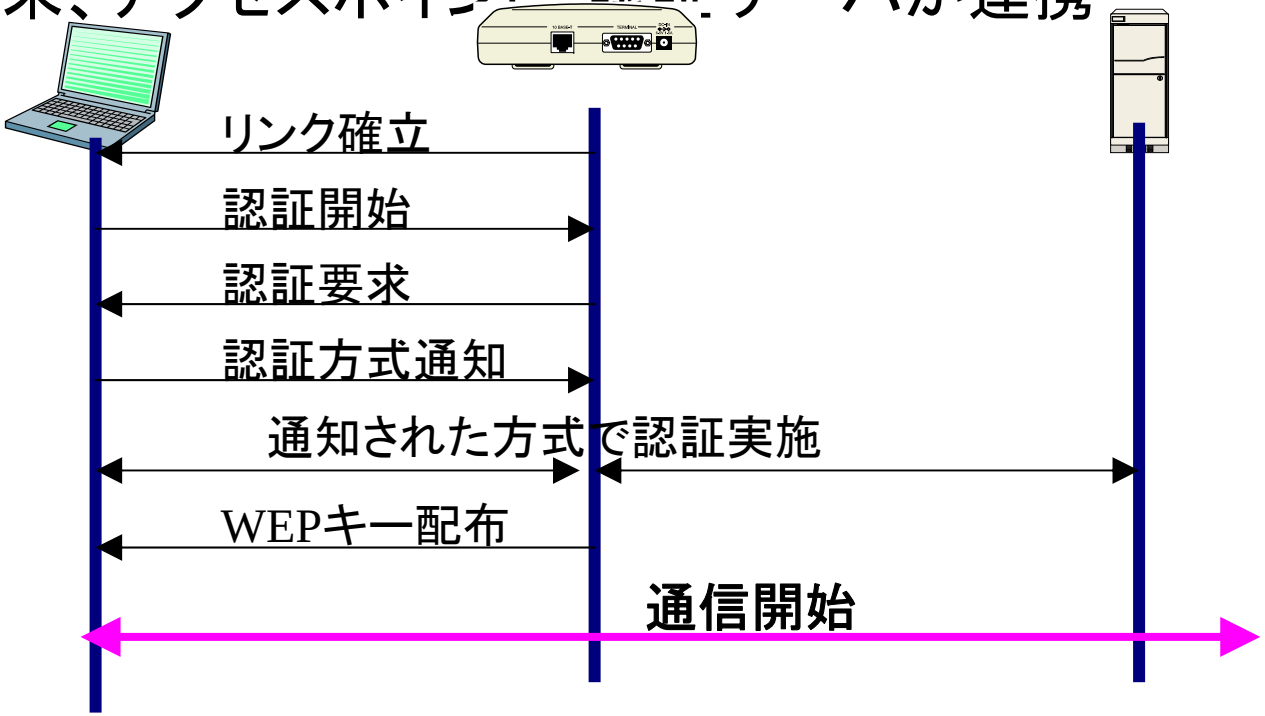
- ESS-ID(Extended Service Set Identifire)
  - アクセスポイントを識別するためのID
  - 「ANY」
    - だれでも参加できるID
    - セキュリティが無いに等しい
  - 推奨されるESS-ID
    - 利用者を推察しにくいもの
    - 無機質で機械的なもの
  - 悪い例
    - 会社名や組織名、個人名

暗号化

- WEP（Wired Equivalent Privacy)
  - 無線データを暗号化する
    - 64ビットキー方式：キーデータは40ビット（5文字）
    - 128ビットキー方式：キーデータは104ビット（13文字）
  - クラックツールもあり、安全な暗号ではない
- WEPの弱点を克服した802.11i
  - しかし、規格化が遅れた
  - 暫定規格としてWPAが利用可能に

認証

- 802.11x
  - 端末、アクセスポイント、認証サーバが連携



Institute for Learning Development

無線LANの注意点（1）

802.11b/g

- 使用できる通信能力
  - 有線LANのハブなら100Mbps全2重のスイッチ
  - 無線LANは10Mbps半2重ダムハブ以下
- チャンネルを複数使っても限界がある
  - 802.11b/gでは14チャンネル（aは4チャンネル）
  - 機器によっては11チャンネルまで
  - 4チャンネル空けないと電波が干渉
  - b/g混在環境では速度低下もある

無線LANの注意点（2）

- セキュリティ対策（1）

  第3者の不正使用を防止

  - MACアドレス制限
    - MACアドレス：LAN機器固有の番号
    - 許可していないMACアドレスの機器を接続しない
  - DHCPを使用しない
    - DHCP：IPアドレスなどを自動的に配布する機能
    - 不正利用者にIPアドレスなどを渡さない

無線LANの注意点（3）

- セキュリティ対策（2）

無線LAN装置によっては以下の設定が可能

- ESS-ID遮蔽
  - ESS-IDを放送しない機能
- ANYアクセス拒否
  - ESS-IDがANYの機器からの通信を無視

無線LANで実際におこったこと

注意しないとホットスポットになる

- ある百貨店でPOSデータが丸見え
- ホテルの窓際がホットスポット
  - ホテルの近所の家庭に接続？
- 隣家の無線LANに接続
  - 自宅よりも隣家の電波が強い

サーバとパソコンのセキュリティ

- 設定での注意
- コンピュータウィルスに対する注意
  - MicrosoftのProtect your PC
    - ファイアーウォールを利用
    - Windows Updateの使用
    - 最新のウィルス対策ソフトを使う
- 利用に当たっての注意

設定について(1)

- サーバ、クライアントともに基本なんですけど…
  - GUESTアカウントを無効にする
  - Administratorグループに所属するユーザは限定
  - Administratorグループ所属のユーザアカウントにパスワードを設定
  - ドライブのファイルシステムはNTFS
  - WindowsTimeサービスで時刻合わせ
    - インターネットのNTPが利用可能
  - WindowsUpdateなどでセキュリティパッチは確実に適用

設定について（2）

- ソフトの導入
  - ウィルス対策ソフト
    - ウイルスデータベースの更新をお忘れなく
  - パーソナルファイアーウォール
- サーバでは
  - セキュリティパッチ（WindowsUpdate)はちょっと注意
    - 動作しなくなるソフトがあるかも
    - SQLserverはWindowsUpdateで更新できない
    - OfficeはOfficeUpdateで適用
  - サーバでは作業をしない（ネットサーフィンは×）

設定について(3)

- サーバでは(続き)
  - 不要なサービスは停止＆無効
    - 何が不要なサービスなのかわからない
    1. NMAPなどのポートスキャナでサーバをスキャン
    2. 不審なポート番号を確認
    3. fport.exe(Foundstone社)でポート番号とそれを使用しているプログラムの対応を確認

日経ネットワークセキュリティ
プロが薦める！最強ツール　42～51ページ

Win2000で最低限必要なサービス
DNS Client
Event Log
Logical Disk Manager
Plug and Play
Protected Storage
Remote Procedure Call (RPC)
Removable Storage
RunAs Service
Security Accounts Manager
Server
Windows Management Instumentation Driver Extensions

Institute for Learning Development

Windowsのライフサイクルに注意

- Windows95/NT3.5/NT4はすでにサポート打ち切り
- Windows98/ME
  - 「セキュリティ」サポートのみ2006年6月30日まで延長
- Windows 2000 professional、Windows 2000 Server
  - セキュリティサポートは2007年3月31日まで
- Windows XP Home Edition
  - セキュリティサポートは2006年12月31日まで
- Windows XP Professional
  - セキュリティサポートは2008年12月31日まで

http://www.microsoft.com/japan/windows/lifecycle.asp
http://www.microsoft.com/japan/windows2000/support/lifecycle/

管理者としての勘所

- 情報収集に努める
  - 新聞の情報はぜんぜんだめ
  - 雑誌にはちょうちん記事があると思え
  - ネットの情報にはガセも多い
  - 信頼できるネットワーク（人脈）
- 上司と信頼関係を
  - 緊急時にどう対処するか
- 自分のカンを信じる
  - このパッチは今適用すべきか、待つべきか
    - Microsoftのアップデートプログラムがトラブルの元になることも

Institute for Learning Development

日々のマメさが重要

- ファイアーウォールがあっても
  - 装置自体のセキュリティホールやバグ対策
  - ネットワークの裏口があったら
    - ダイアルアップ装置や、VPNソフト（SoftEther）の無断利用、無線LANが窓際にあった
- ウィルス対策ソフトがあっても
  - ウィルスデータの更新が必要
  - MSBlastみたいにウィルス対策ソフトで対策できないもののある
- ファイアーウォールの内側にいるから
  - Webブラウザでネットサーフィンするだけで情報漏えいも
- ネットワークにつながないから
  - ウィルスはフロッピーからでも感染する

Institute for Learning Development

情報の収集

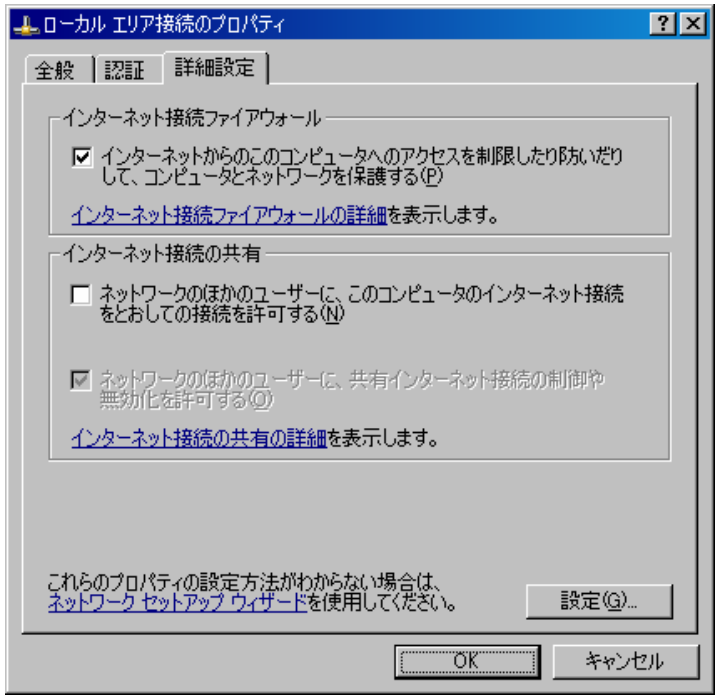
- ホームページ
  - セキュリティホール memo
    http://www.st.ryukoku.ac.jp/%7Ekjm/security/memo/
  - ITPro
    http://itpro.nikkeibp.co.jp/
  - Microsoft TechNet
    http://www.microsoft.com/japan/technet/default.mspx
  - Net Security
    https://www.netsecurity.ne.jp/
- ツール
  - Microsoft Baseline Security Analyzer(MBSA）1.2
    - 現在はHFNetChkの最新版としてCUIで使用
  - WindowsUpdate
    - XP SP2：proxycfgコマンドで設定しないとProxy環境では機能せず

MBSA1.2.1（SP2対応）

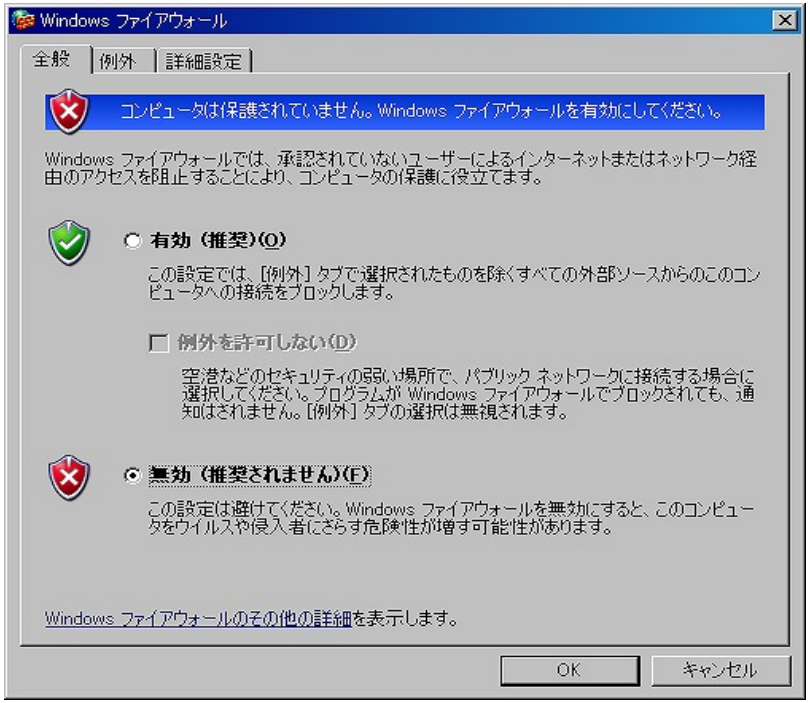
パーソナルファイアーウォール

- Windowsファイアーウォール（XP標準機能）
  - XP附属版の機能は市販の製品に及ばない
  - 出て行くデータは素通しする

Windows XP SP1

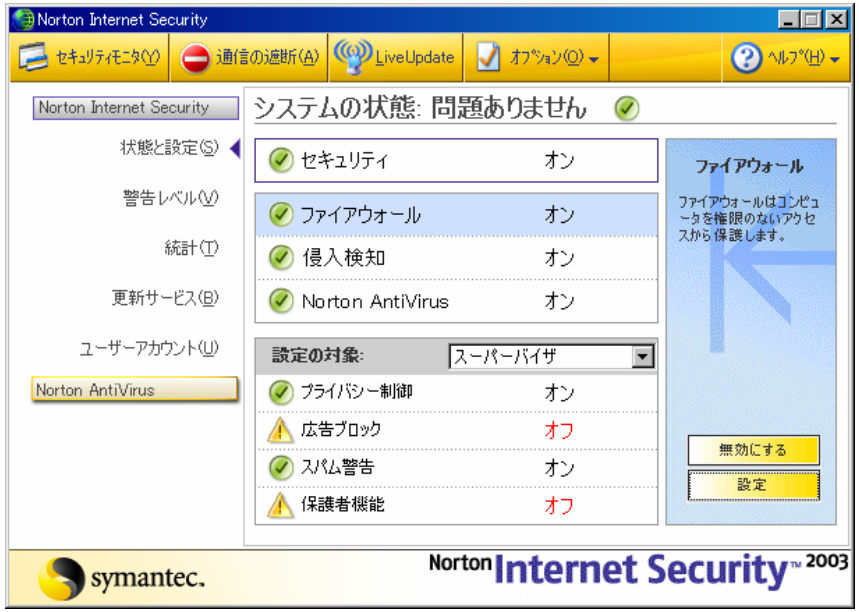


Windows XP SP2



パーソナルファイアーウォール（続）

- Norton Internet Security
  - このほかにもZoneAlerm,ウィルスバスターの標準機能などいろいろ
  - pingすら不許可にするので注意が必要
    - 通信テストができないことも



Institute for Learning Development

発想を変えることも重要

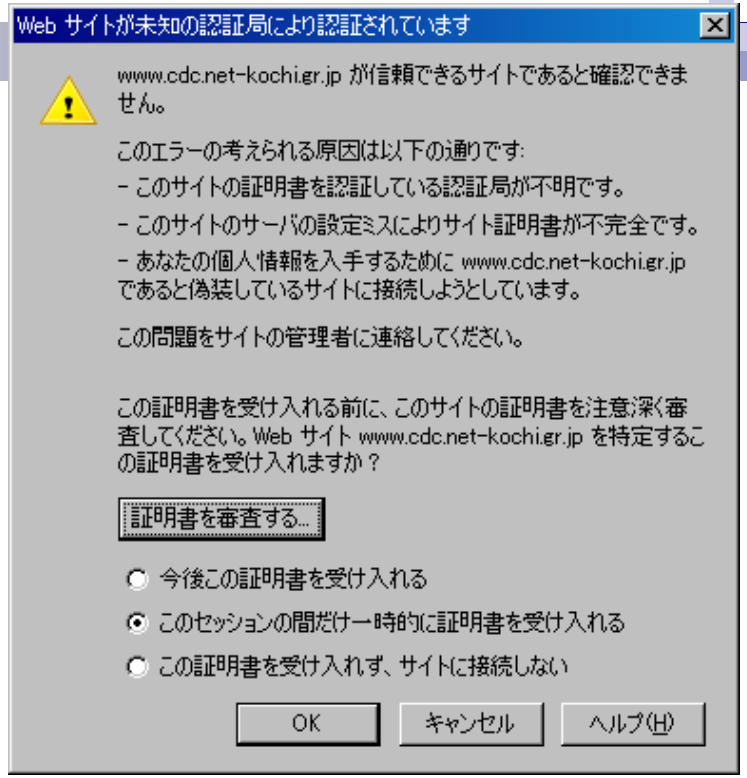
- おまけのソフトの利用をやめる
  - InternetExplorerにはセキュリティ上の問題がよく見つかる
  - OutlookExpressはウィルスに感染しやすい
- Windowsをやめる
  - セキュリティ対策やウィルス対策を軽減
    - ブラウズするだけなら、LindowsCDやKNOPPIX
      http://www.alpha.co.jp/knoppix/index.html
    - サーバはUnix
    - OfficeソフトはStarSuit
- HDDの利用制限
  - 感染してもすぐ回復（障害対策も兼ねる）
    - HDDガードソフトで、ユーザはインストール不可に
    - ディスクレスのシステムを採用

Institute for Learning Development

最近の話題

- オレオレ証明書
  - 正しく検証できず、受け入れるかどうかを状況でのみ判断しなければならないサーバ証明書
- フィッシング詐欺
  - OSのhostsファイルを書き換えてしまう新手法
    「**pharming（ファーミング）**」と細分する人もいるがしなくても…
- 802.11a用の周波数変更・新規開放
  - 2005年5月に802.11a用周波数が変更の予定
    - 新製品と既存製品で通信できなくなる可能性がある
  - 新規利用可能周波数4チャンネル分が追加予定

オレオレ証明書（1）



- 信頼するところとして
  選択していない認証機関が
  発行しているサーバ証明書
  - 例）「高知県　電子申請・届出システム」の場合、
    「登録画面」で…
    - http://www.pref.kochi.jp/~jyouhou/denshishinsei/
  - 参考
    - 高木浩光＠自宅の日記
      - http://takagi-hiromitsu.jp/diary/200501.html
      - http://takagi-hiromitsu.jp/diary/20050114.html

オレオレ証明書（2）

- **SSL入門**
  - **http://www005.upp.so-net.ne.jp/nakagami/Memo/SSL/**
- Webサーバと暗号通信（https)するには
  - 公開鍵で暗号化する
  - サーバ証明書で公開鍵の真贋を確かめる
  - CA（認証局）の署名でサーバ証明書の真贋を確かめる
  - CAの署名の真贋は他のCAの署名で確かめる
  - 他のCAの署名の真贋は「ルート認証局」で確かめる
  - 「ルート認証局」の証明書はブラウザに組み込まれている
- オレオレ証明書はこの仕組みでは認証できない

オレオレ証明書の何が問題なのか

- 真贋を確かめきれないのに「信用しろ」と教育？！
  - 例）埼玉県　わくわく子どもページ
    - http://www.pref.saitama.jp/kodomo/top.htm
      - クイズの問題文と答えの入力の画面をたどると…

これは暗号化通信を行う際の、証明書についての警告メッセージです。
上記画面のように「**この証明書には問題がある**」という文章が表示されますが、
（中略）、
ブラウザでは安全性が判断できず利用者の方の意思を確認するものです。

「はい」をクリックすることで、このセキュリティ証明書を信頼するという**意思表示**となり、
暗号化通信が開始されます。

「JPドメイン名」だとフィッシングされるかも（似たドメイン名を誰でも取得可能）

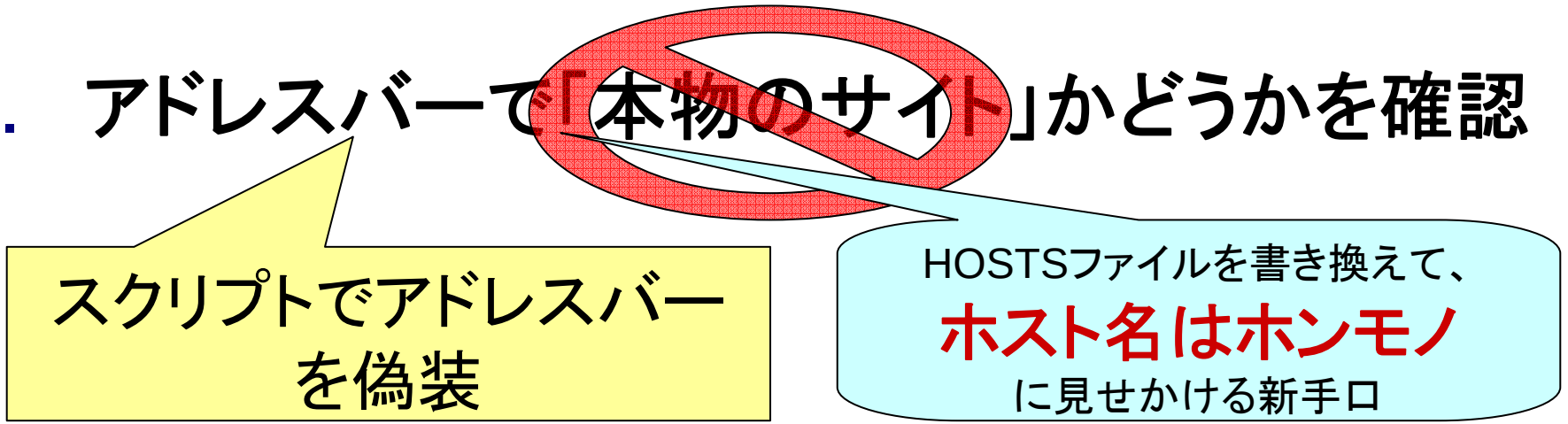
フィッシング詐欺とは

- 「Phishing」
  - 「釣り」（fishing）ではありません。

- クレジットカード番号や暗証番号を入手する詐欺
  - 実在の金融機関などを装ったメールを送付
  - メールのリンクでホンモノそっくりの
    「罠のサイト」に呼び込む
  - クレジットカード番号やパスワードなどを入力させる

フィッシング詐欺対策は

1. メールを信用しない、リンクをクリックしない
2. “こちらから”本物のサイトにアクセス
3. アドレスバーで「本物のサイト」かどうかを確認



Institute for Learning Development

まとめ

- セキュリティ対策
  - 守るものを明確に
  - 守り方
    - コストとのバランス
    - 便利さとのバランス
  - 万が一のときの準備
    - 休日でも夜間でもすぐに対処できるか
  - 機器に頼らない
    - 問題を起こすのも、対処するのもヒト

Institute for Learning Development

おまけ

- 事象(事故とかトラブルとは呼ばない）発生時
  - できるだけ正確な報告書を早急に作成する
    - 中途半端な報告は解決を遠ざける
    - 迅速な手当てが被害を小さくする
  - 自分のミスがあっても決して隠さない
    - ゴマカシがあればどんどんぬかるみにはまる
    - ミスがミスを呼ぶ
  - 報告する相手を選ぶ
    - 邪推される相手に中途半端な情報が渡ると風評被害もありえる
- セキュリティの自習資料
  - 「情報セキュリティ読本- IT時代の危機管理入門 -」(IPA)
    http://www.ipa.go.jp/security/publications/dokuhon/ppt.html