第九回
知的所有権とセキュリティ

2002年10月31日

連絡事項

- 次週 11月7日は 月曜日の振替

知的所有権

- 知的所有権
  - 工業所有権：産業経済の発展を目的とした制度
    - 特許権、実用新案権、意匠権、商標権など
  - 著作権：音楽、絵画、小説、映画、コンピュータ・プログラムなどの著作物の保護を目的とした制度
    - 著作者人格権、著作者財産権、著作隣接権

- 著作物とは

  思想または感情を創作的に表現したものであって、
  文芸、学術、美術、または音楽の範囲に属するものをいう。
  （著作権法）

- 著作物を創作した時に自動的に権利が発生
- 権利の取得にあたって登録などの必要はない

著作権と著作隣接権

- 著作権
  - 著作権者以外の人が著作物を利用しようとするときに、利用を認めたり(許諾)、禁止したりできる権利
  - 著作権法で認められている「私的使用のための複製」などのケースを除いて、著作物を利用する際には著作権者の許諾を得る必要がある（友人から借りたCDのコピーは×）
  - 財産権としての著作権:
    複製権 演奏権 公衆送信権 上映権 貸与権 頒布権 など
  - 著作権のうち「著作人格権」は他人に譲渡することができない
- 著作隣接権
  - 出版社、実演家、レコード製作者(レコード会社など)、放送事業者など、著作物を世の中へ伝達する役割を担う人の権利を保護

- 著作者が果たしている役割を尊重し、利用の際に著作者への正当な対価を支払うことが、新たな著作物の創作を産み、文化を発展させる
- プログラムの開発と配布においては従来の法律の枠組みでは解決できない課題がでてきている

Copyright と Copyleft

- Copyright: “copy” + “right” (複製する権利)
  - 権利を持つ人(作者)が自分のものであると主張し、利用者に対して利用を許可したり正当な対価を求めることができる権利 (著作権)
  - 国によってはソースコードを”public domain”(公の場)で公開すれば、Copyrightを放棄したとみなされ、自分のソースコードに対するその後の権利を失う（日本の著作権法では放棄できない）

- Copyleft:
  - 諸権利と共に複製物を得た人がさらにその複製物に諸権利を含めて再配布すれば、そのソースコードを使用、修正、再配布が可能となる。ソースコードと諸権利は法律的に切り離すことはできない。
  - 例： GPL (GNU Public License)
  - 著作権告知とGNU一般公有使用許諾書
  - プログラムを作成した人の権利を守りながらソースコードを公開して人類の知的活動の財産としてフリー・ソフトウェアを共有し、全体の種類を増やすことができる
  - 「思想」かつ「慣習」であり法律で確立しているわけではない

電子透かし

- デジタルデータはオリジナルと複製の区別ができない（全く同じものを幾つでも複製できる）
- 著作権者の権利を保護するための仕組みがいろいろと考案されてきた
- 画像や音楽データなどに、人間の目や耳では区別ができないほどのわずかな「ゆらぎ」として電子署名データを潜り込ませておくことができる
- 不正コピーをした人間が、電子署名を取り去りたいと考えても、「ゆらぎ」のどの部分に紛れ込んでいるのかを検出することは極めて困難
- 音楽ファイルの不正コピー対策などに用いられる
- Photoshop画像 → Digimarc など

パスワードによるログイン

- “UNIXパスワード”
- パスワードの文字列をシステムに入力
- 文字列を一方向のハッシュ関数で暗号化
- あらかじめ暗号化された文字列と比較
- 結果が一致すれば「正しいパスワード」と認識

cf. 米国の暗号技術輸出規制
(日本向けは2000年に緩和)

cf. 辞書攻撃 → 辞書に載っている単語(とその組み合せ)は簡単に破られる

暗号解読

- 暗号の形式が分かっていれば計算時間さえ十分長く取れば原理的には暗号解読ができる
- 暗号解読にかかる時間は暗号化関数の強度により異なる
- 暗号の鍵を時々変えてやらないといつかは解読される

ネットワーク経由のログイン

- telnet, ftp, pop3など
  - サーバー側でパスワードを暗号化して本人として認証
  - パスワードが平文でネットワーク上を流れる
  - パケットを傍受すればパスワードを簡単に入手できる
  - 傍受用のツールがネットワーク上で流通
- kerberos
  - サーバーとクライアントの身元を認証サーバーで確認
- ssh
  - 公開鍵方式による暗号化
- web上のオンラインショッピング
  - SSL, SecureHTTPなどによる通信の暗号化

公開鍵方式とは

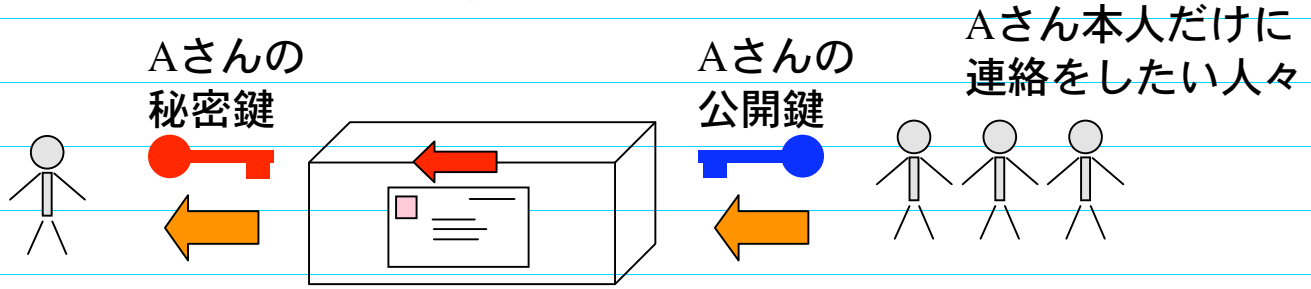
- 暗号化に用いる鍵と復号化に用いる鍵がペアになっている（秘密鍵と公開鍵）
- 秘密鍵で暗号化した暗号文は公開鍵でしか解読できない

- 公開鍵で暗号化した暗号文は秘密鍵でしか解読できない

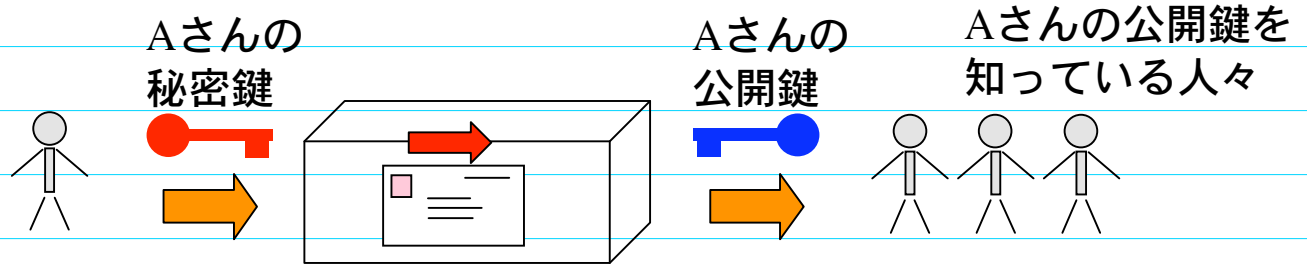
自分の公開鍵は誰に渡してもよい
自分の秘密鍵は盗まれてはいけない

公開鍵方式の応用

- 公開鍵方式は二つの鍵を持つ私書箱 (ただし解読は一方通行)
- 本人だけが解読できる**暗号化通信**



- 本人が作った文書であることの証明(**電子署名**)



- Aさんの公開鍵が「本当にAさんのもの」であることを
  誰が証明する?
  PKI : Public Key Infrastructure → 認証局

VeriSign社など

信用の輪：友達の友達は友達

セキュリティとは

- 計算機、ネットワークの不正侵入、不正利用から守る
- 機密データ、プライバシーなどの流出を防止する
- サービス妨害などの攻撃から守る

- それぞれの組織における「セキュリティポリシー」を定める
  - 守るべき「情報・サービス」はなにか？
  - 誰から守るのか？（外部の人間、他の部署の人間、など）
  - 他に迷惑をかけないか？（踏み台にされないか？）
  - 誰がなにに責任を持つのか？

cf. 破られたシステムを元の状態に復旧するための作業時間も「守られるべきコスト」

セキュリティ向上の現実

- 攻撃と防御「矛と盾」→「絶対安全」はあり得ない
- 攻撃側の手口と計算能力は日進月歩
- 安全なサイト構築には最新の攻撃手口を熟知することが不可欠
- 自分のサイトへの攻撃をハッカーに依頼して、防御策をより堅固にする場合もある
- 攻撃と防御を純粋な研究対象とするハッカー
  →「ホワイト・ハット(善意の人)」
- 自分の技量を反社会的行為に用いるハッカー
  →「ブラック・ハット(悪意の人)」

ハッカー(Hacker)とは
巨大なコードを
ハッキング(hacking)
すなわち切り刻む人
転じて「プログラミング
能力の優れた人間」

厳密な区別があるわけではない。
年齢や社会的立場から「ブラック・
ハット」から「ホワイト・ハット」
に転向する例もあればその逆もある。

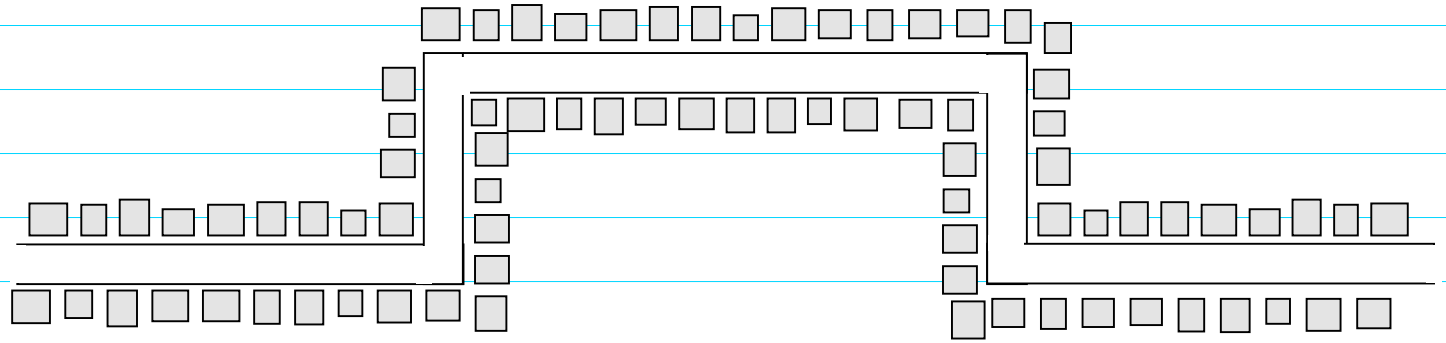
cf. DEFCON

年に一度の「ハッカー達」の大集会
ジーンズ、長髪のハッカーや
FBI, CIAなどのセキュリティ担当者
が入り乱れて、攻撃と防御の最新の
手口を語り合う

攻撃と防御

- 遠見遮断(とおみしゃだん)

中世の町並みなどに見られる変則的な形状の道路



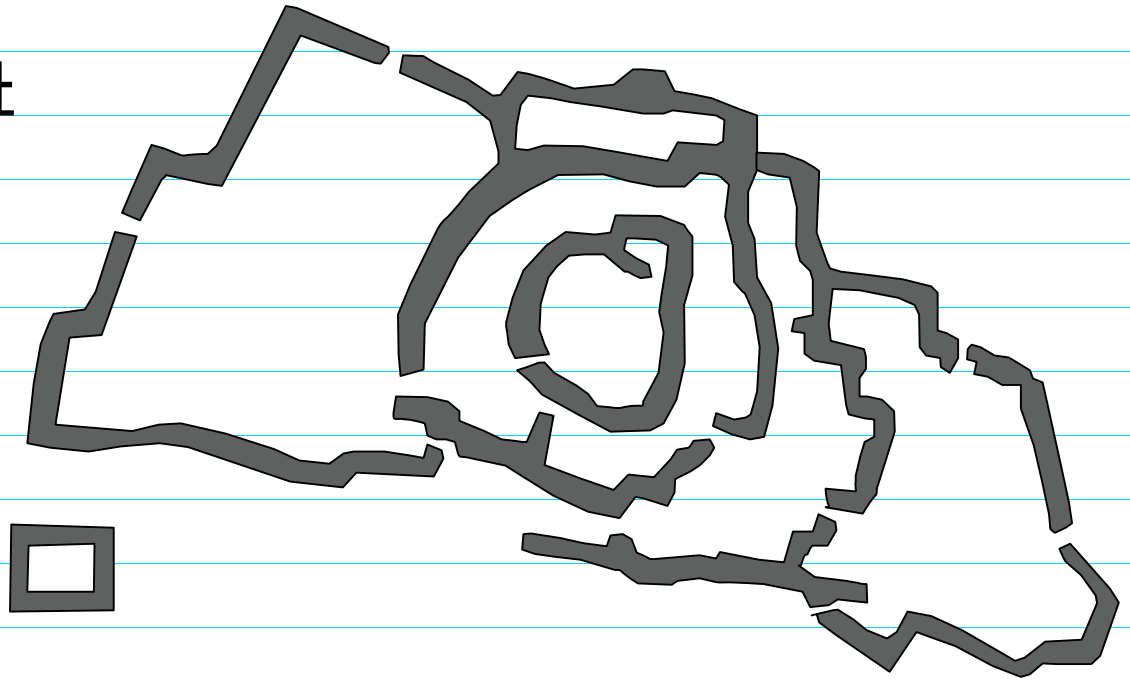
街道筋をクランク状に曲げるなどして外敵の侵入を妨げる

攻撃側は敵の配置を把握しずらい
防御側は敵の動きが見えやすい

つくば市 旧谷田部町, 吉沼
石下町　下妻市 など

サイト構築の原則

旧真壁城趾



外部からは内部の構造がつかみづらいこと
内部からは侵入の動きがつかみやすいこと
出入り口(ポート)を限定して、重点的に守る

cf. 防衛庁ネットワークデータ流出問題

参考URL: http://www.intio.or.jp/makabeht/newmakabejou.files/mokuji.htm

セキュリティホール

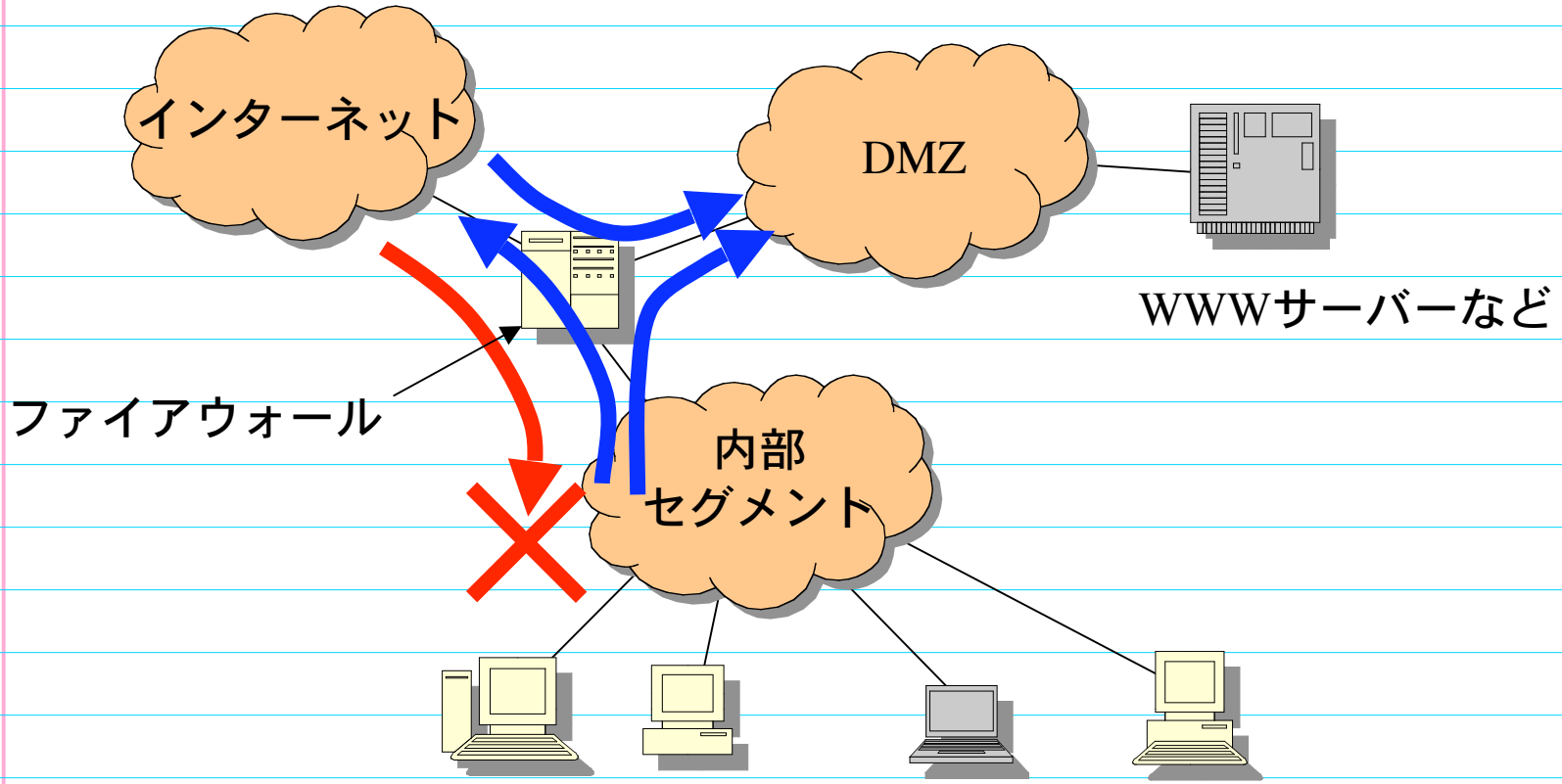
- 想定された利用法以外の方法により、不正利用を許してしまうプログラム上のバグ
- それまで安全だったネットワーク機器が、セキュリティホールが見つかった時点から最も弱い侵入ポイントとなる
- 例：バッファーオーバーフローなど
- 防御側は「動的かつ迅速な」システム修正が不可欠

cf. 「Apacheのバージョン x.xx.xxにはyyyというセキュリティホールがある」

- JPCERTやOSメーカーなどのセキュリティ情報に気を配る
- 終わることのない“もぐらたたき”

ファイアウォール

- Fire Wall：「防火壁」
- あるサイトのLANを「DMZ(外部公開用セグメント)」と「内部セグメント」に分けて、通信が可能な範囲をきめ細かく制御する



コンピュータ・ウィルス

- 他のプログラムに寄生して、プログラムの実行を乗っ取ることで自分自身を増殖させていくプログラム断片のこと
- 増殖させていくだけで他には何もしないウィルスから、ある特定の日時に「発病」して、システムやユーザーのファイルをすべて破壊するものまで、種類と手口は千差万別
- 最近は感染先のアドレス帳を開いて登録ユーザーに自分の名前を騙って、知人に電子メールを勝手に送りつけるウィルスが多い
- 他のプログラムに寄生せずに自分自身を実行し複製するものを「ワーム」と呼ぶ
- 自分が使用するプログラムのセキュリティホールを潰しておくのが感染予防の大前提

セキュリティ向上の条件

- よいセキュリティを実現するためのバランス “式”

$$\text{セキュリティ} = \frac{(\text{コスト})\times(\text{ノウハウ})\times(\text{運用})}{(\text{ヒューマンエラー})}$$

参考文献: すずきひろのぶ著「実践Linuxセキュリティ」

今週のレポート

問1:米国のレコード会社と映画会社の業界団体であるRIAAがこれまでに「著作権侵害である」として起こした訴訟について、検索してわかったことを説明せよ。

問2: 音楽家坂本龍一氏が著作権について語っているページを検索して、そのページのURLと感想を述べよ。

問3: GNUプロジェクトについて検索して説明せよ。

問4: オンラインショッピングなどのwebサーバーはどうやって自分が本物であることを顧客に保証しているか。インターネットなどで検索してその原理を説明せよ。

問5: 「バッファーオーバーフロー」とはなにか。インターネットなどで検索してその原理を説明せよ。

問6: コンピュータ・ウィルスの作者がなぜウィルスを作成したのか、その動機について検索して、わかったことを説明せよ。またその作者に対する感想を述べよ。

参考文献

- すずきひろのぶ 著「実践Linuxセキュリティ」インプレス
  ISBN4-8443-1404-1

- 武田圭史, 磯崎宏 共著「ネットワーク侵入検知」ソフトバンク
  ISBN4-7973-1253-X

- 小舘香椎子, 上川井良太郎, 中村克彦 共著
  「教養のコンピュータサイエンス情報科学入門 第2版」 丸善
  ISBN4-621-04871-6

- 菊沢正裕, 山川修, 田中武之共著「情報リテラシー：メディアを手中におさめる基礎能力」森北出版
  ISBN4-621-04871-6