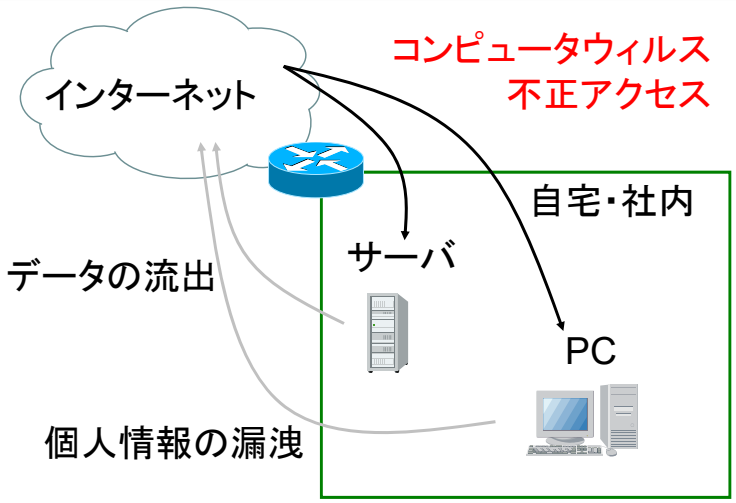
ネットワーク
工学

第14課　セキュリティ技術

14.1　セキュリティの必要性



14.2 ウィルスへの対応・対策

ウィルス対策ソフトウェアを用いる

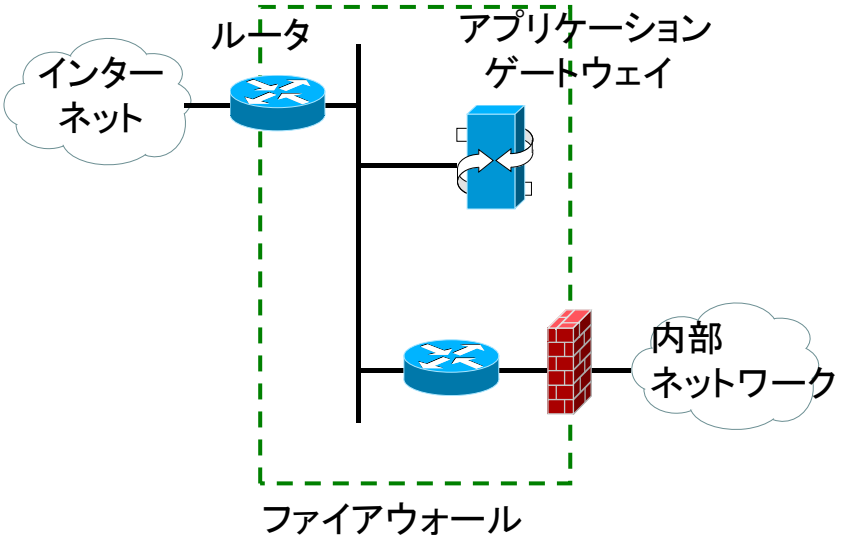
市販品: ノートンアンチウィルス
ウィルスバスター
マカフィー

フリーソフト: 多数

定義ファイルアップデートやスキャンの習慣

定期的なHDDのスキャン
ウィルス定義ファイルを常に最新に

14.3 ファイアウォール・アーキテクチャ



14.4 暗号化技術

アプリケーション	SSH（セキュア・シェル） SMIME（Secured MIME） PGP ・・・ アプリケーション単位
トランスポート	SSL（Secure Socket Layer）
ネットワーク	IPSec（IP Security Protocol） 拠点間で暗号化
データリンク 物理	

14.5 共通鍵暗号

通信相手と共通の鍵を作成
暗号化鍵と複合化鍵が同一
通信相手ごとに鍵を用意する必要あり
鍵が外部に漏れた際盗聴の危険性あり

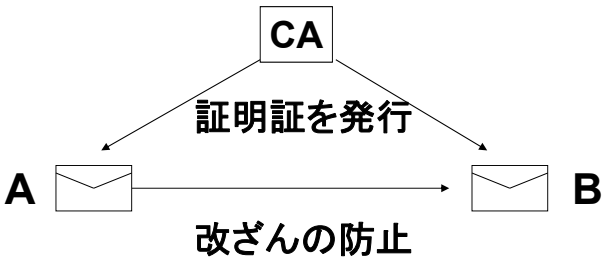
14.6 公開鍵暗号

暗号化に用いる鍵を公開する（復号はできない）
復号に用いる鍵はローカルに保持（公開しない）
鍵が外部に漏れる可能性が低い
複合化に時間がかかる（不可逆過程）

14.7 認証局（CA）

デジタル証明書を発行する信頼できる第三者
（例：マイクロソフトWindowsサーバの認証局機能）

目的：セキュリティ、否認防止



14.8 指紋センサー

- 指紋、虹彩情報などの生体認証機器
- ノートPCによく組み込まれている

14.9 セキュリティーを高めるには

- 指紋認証機器は追加コストが必要
- コストをかけずにセキュリティーを高める
  - パスワードを複雑に。大文字小文字数字混在。
  - 離席時にはPCをロック、スクリーンセイバーにもパスワードをかける

14.10 マルウェア

- マルウェア(Malware)とは、コンピューターやユーザーに何らかの被害をもたらす可能性のあるプログラム
- マルウェアによる被害を防ぐにはその対策が必要である

14.11 マルウェアの種類: 1

- **ウイルス**
  - -コンピューターに侵入して、ユーザーのなんらかの操作により増殖して感染範囲を広げてゆく悪意のあるプログラム
- **ワーム**
  - -コンピューターに侵入して、ユーザーの操作なしで自己増殖し感染範囲を広げてゆく悪意のあるプログラム
- **トロイの木馬**
  - -有用なプログラムに見せかけてコンピューターに侵入し、隠れて悪さをするプログラム。特にネットワーク経由で侵入口を作成するものをバックドアと呼ぶ。

14.12 マルウェアの種類: 2

- **キーロガー**
  - –キーボードの入力をすべて記録し、ネットワークを通じて外部へ送信。
  - –ID、パスワードの入力をすべて送信されるため、外部に機密情報が漏洩する危険性がある。
- **ボット**
  - –マルウェアの一種で、ボットに感染したコンピューターは外部から遠隔操作されて迷惑メールの送信や特定サイトへの攻撃などを行う。
  - –ボットに感染したコンピューターからなるネットワークはボットネットと呼ばれ、ボットネットのコンピューターは特定サイトの一斉攻撃（DDos攻撃）などに利用される。

14.13 マルウェアの種類: 3

- **スパイウェア**
  - – ユーザーの同意なしに勝手に個人情報を収集するプログラム
- **アドウェア**
  - – 広告を自動で表示したり、ダウンロードしたりするプログラム