医療情報とセキュリティ

医学部医療情報学講座
平野章二

講義の概要

- 医療分野における個人情報
  - 取り扱いの歴史と背景
  - 医療情報の種類と特性
- 医療情報の電子化と情報セキュリティ
  - 医療機関の情報化，医療情報の電子化
  - 情報セキュリティ，ネットワークセキュリティ

医療分野における個人情報

欧米諸国における個人情報保護の歴史

- 「ヒポクラテスの誓い」(B.C. 300頃)
  - 「医神アポロン，アスクレピオス，ヒギエイア，パナケイアおよび全ての男神と女神に誓う。私の能力と判断に従ってこの近いと約束を守ることを。 …医に関すると否とにかかわらず，他人の生活について秘密を守る。… 」(野崎貞彦編「新簡明衛生公衆衛生」)
- 「ナイチンゲール誓詞」(1893年，米国)
  - 「われは取り扱える人々の私事のすべて，知り得たる一家の内事のすべて，われは人に漏らさざるべし。」
- 世界医師会ジュネーブ宣言
- 日本医師会「医師の倫理」

⇒ 業務上知り得た秘密の守秘を規定

欧米諸国における個人情報保護の歴史

- 米国プライバシー法 (Privacy Act; 1974)
  - 「自己情報コントロール権」を規定
  - 自己の情報を知り，自身でコントロール
  - 医療；患者に自己の健康状態やとりうる治療方法について十分に説明し情報を与える，その上で患者自身がその情報の扱いを決める

⇒ 「守秘」の概念が大きく変化

- OECD 個人情報保護に関するガイドライン (1980)
- EU 個人情報保護に関する指令 (1995)

日本の現状

- 医療情報保護に関する法は未整備
  - 2000年12月，病歴情報を薬局に売却しようとした業者が書類送検される： 名誉毀損罪 (朝日新聞)
  - 26%の医療機関が患者の同意無く外部へカルテ情報を提供 (2002年厚労省研究班調査発表)

⇒ カルテ情報の取り扱いに関する法の未整備

- 個人情報として捉えた場合
  - 憲法，刑法，民法，医療に関する各業法

日本の現状

- 刑法　第134条
  - ①　医師，薬剤師，医薬品販売業者，助産師，弁護士，弁護人，公証人またはこれらの職にあった者が，正当な理由がないのに，その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは，6月以下の懲役または10万円以下の罰金に処する。
- 医療関連の各業法における機密保持規定
  - 保健師助産師看護師法　第42条
  - 放射線技師法　第29条
  - 臨床検査技師，衛生検査技師等に関する法律　第19条
  - 理学療法士及び作業療法士法　第46条
  - 児童虐待の防止等に関する法律　第6条，第7条
  - 社会保険診療報酬支払基金法　第14条の5

日本の現状

- 刑法，各業法
  - 人的限定を付与
  - 医療情報の漏洩の全てを直接に対象とするものではない
  - 新業種への対応，業種の相違による罰則の相違
  - 機密情報の漏洩という行為自体に対する網が必要
  - 「だれが」ではなく，「誰であれ，患者の医療情報を扱うことになった場合は，それを漏らしてはならない」

⇒ (自己) 情報のコントロール権という概念
医療従事者の責務から患者の権利へ

⇒ 個人情報保護法の制定

個人情報保護法と医療情報

- 患者主体；同意に基づく個人情報の利用
  - 利用目的の特定 (第15条)
  - 利用外目的の制限 (第16条)
  - 取得に際しての利用目的の通知 (第18条)

⇒ 患者の同意が重要に

- 個人情報の適切な取得と管理
  - 適正な取得 (第17条)
  - 正確性の確保 (第19条)
  - 安全性の確保 (第20条)

医療における個人情報

- 診療に関連して発生する個人情報＝診療情報
  - 患者基本情報
    - 氏名，年齢，生年月日，住所，電話番号などの個人識別情報，勤務先，配偶者，職業など
  - 健康保険・福祉情報
    - 健康保険，公費医療，障害者手帳，療育手帳に関する情報など
  - 診療管理用情報
    - 受診診療科，適用保険，受診日，入退院日など
  - 生活背景情報
    - 喫煙歴，飲酒歴，生活歴など
  - 医学的背景情報
    - 出産時体重，妊娠分娩歴，予防接種歴，既往歴，輸血歴，アレルギー，家族歴など

医療における個人情報

- 診察記録情報
  - 問診記録，現病歴，身体所見，経過記録，診断，治療計画など
- 指示実施記録情報
  - 検査実施及び結果，処方実施記録，手術実施記録，処置実施記録，各種指導記録など
- 診療情報交換記録
  - 診療情報提供書など
- 診療説明・同意情報
- 要約情報
  - 診療要約，退院時要約など
- 死亡記録情報
  - 死亡診断書，剖検記録など

(財) 医療情報システム開発センター
「電子保存された診療録情報の
交換のためのデータセット項目」

診療情報の特徴

- 多様かつ膨大な情報
  - 恒常的情報＋時系列情報
- 大部分の情報は間接的，また，理解に知識が必要
  - 血液学的検査の結果，心電図の波形など
  - 診断などは医療従事者の技能や視点により変化し得るが，原則として主観で左右されるものではない
- 取得方法が多岐
  - 基本情報：　受診申込時に直接患者から
  - 既往歴，身体所見など：　診察時に直接患者から
  - 検査結果：　検査部や外注検査業者などから

⇒ 自己に関する情報の種類，性質，内容，収集過程を患者が把握することは困難

診療情報の特徴

- 利用目的が多彩
  - 診療； TPO (Treatment, Payment, and Health Care Operations)
  - 教育，研究
    - 臨床試験
    - 疫学研究，データマイニングなど
  - 医療行政
    - 行政による医療機関の監督，検査など
    - 精神保健法，身体障害者福祉法，児童福祉法等に基づく診療情報提供など
  - 司法
    - 訴訟上の証拠としての診療情報提供，事件性の有無の判断材料
  - その他各機関からの照会

診療情報の特徴

- 医療特有の個人情報保護上の問題
  - 死者のプライバシー保護
    - 生前に蓄積した情報の死後における取り扱い
    - 同意取得の可否，遺族の代理可否（病理解剖，脳死臓器移植）
    - 対立する遺族間での開示請求に対する姿勢の違い
  - 家族
    - 家族歴の取得；家族の健康状態を本人の同意なしに収集可能か
  - 遺伝子解析情報
    - 含有情報の重要性から特段の配慮が必要

医療情報の電子化と情報セキュリティ

医療機関の情報化

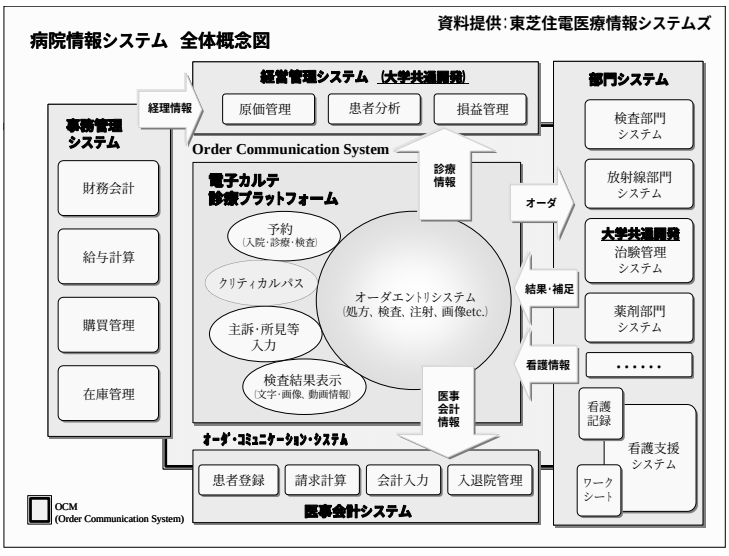
- 様々な診療情報を電子化して計算機で処理することで，省力化と情報の利用性の向上を目指す
  - 医事会計システム
    - 診療報酬請求を効率的に行うシステム
    - 患者基本情報，健康保険情報，公費負担情報，診療報酬算定可能な医療行為に関する情報などを処理
  - 部門システム
    - 血液検査，生理検査，放射線検査などを効率的に行うシステム。検査機器の制御，出力結果の処理，予約管理，医事会計情報の伝送など
    - 患者基本情報，検査指示情報，検査結果情報などを処理

整備の順序 ↓

医療機関の情報化

- オーダーエントリシステム
  - 外来検査室，病棟看護ステーション，検査室，薬局，事務受付など，病院の全ての部署に計算機端末を設置し，各現場で発生する指示，処方などをその場で入力・参照させることで，医療機関内での情報伝達を迅速化，合理化するシステム
  - 医事会計システム，部門システムの同様の情報を処理
- 電子カルテ
  - 診療現場で発生する情報の大部分が電子化された状態
  - 事務作業の合理化のみにとどまらず，積極的にグループ診療をサポートする機能を取り入れる
  - オーダーエントリーの扱う情報の他，外来など診療部門で発生する患者の主訴，所見，治療計画などの情報も処理

資料提供：東芝住電医療情報システムズ



医療情報の情報化

- 医療情報電子化の影響（保護の観点から）
  - 情報の分類と階層化
    - 匿名化，無名化作業が容易に
    - 情報管理ポリシーの細分化が可能に
  - 利用性，可動性の向上→不正利用のリスク増大
    - 大量の情報を取得可能で複製も容易
      → 漏洩により生じる被害の範囲が大幅に拡大
    - 計算機ネットワークを通じたアクセスが可能
      → カルテ庫の物理的侵入への対策のみならず，計算機ネットワークを通じた不正アクセスへの対策が不可欠
  - 安全基準，安全対策の標準化とそれらへの準拠が必要
    - JIS Q 15001など

医療情報の電子化とセキュリティ

- 医療情報の電子化
  - 利用性の向上，業務の効率化，収納空間の有効活用
  - 紙媒体→電子媒体へ

    電子情報としての特性を考慮した保護対策
    ＝情報セキュリティの必要性

情報セキュリティ

- 情報セキュリティの担保すべき3要素： CIA
  - 機密性 （Confidentiality）
    - 権限を持つ者だけが情報にアクセスできること
    - 脅威： 情報漏洩，不正アクセスなど
  - 完全性 （Integrity）
    - 情報および処理方法が正確であることおよび完全であること
    - 脅威： 意図的改ざん，予期しない誤修正など
  - 可用性 （Availability）
    - 許可された利用者が適切な方法により必ず情報を利用できること
    - 脅威： サービス不能攻撃，ウイルスなど

- （参考）診療録等の電子媒体による保存：必要3要件
  - 真正性の確保
    - 故意または過失による虚偽入力、書換え、消去及び混同を防止すること
    - 作成の責任の所在を明確にすること
  - 見読性の確保
    - 情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること
    - 情報の内容を必要に応じて直ちに書面に表示できること
  - 保存性の確保
    - 法令に定める保存期間内、復元可能な状態で保存すること

  平成11年厚生省3局長通知：「診療録等の電子媒体による保存について」より

情報システムのセキュリティ

- 物理的セキュリティ
  - 侵入者による破壊，盗難や自然災害による破損など，コンピュータシステムや記憶媒体に対する物理的脅威への対策
- 論理的セキュリティ　ネットワークセキュリティと密接に関係
  - 不正アクセスや改ざん，盗聴など，情報の内容そのものに対する脅威への対策
- 人的セキュリティ
  - 過失，機密漏洩など，人的な脅威への対策

医療機関における ネットワークセキュリティ

- 安全性の追求
  → 医療機関内で完全に閉じた（対外接続の無い）ネットワークを運用

⇕

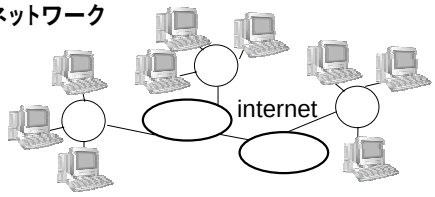
- 利便性の追求
  → インターネット等外部ネットワークとの相互接続

- 携帯型PC等を介した双方向的中継接続路の形成
- 完全な分離は困難； インターネットと同等のセキュリティ対策が必要

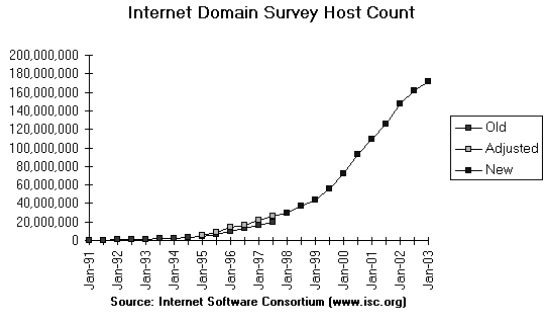
ネットワーク･セキュリティ
ーインターネットを中心にー

インターネットとは

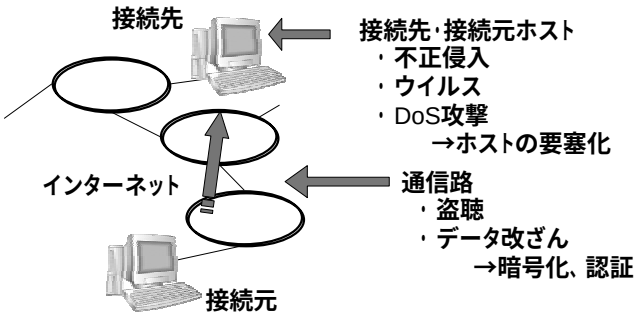
- internet: 複数のコンピュータネットワークを相互に接続した「ネットワークのネットワーク」
  - the Internet: TCP/IPによる世界規模のinternet
- 1969年のARPAnetが起源
  - ARPAnet：米国防総省高等研究計画局が開発した軍事用ネットワーク



インターネット接続台数の推移



インターネット上の脅威と対策



ホストへの攻撃に対する防御

ホストへの攻撃：不正侵入

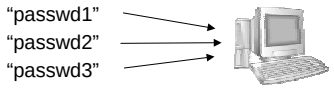
侵入の手口

- アカウントのなりすまし
  - パスワードの自動解析･推測ツール
  - 緊急時の管理者を装ってパスワードを聞き出す
- ホストのなりすまし
- セキュリティーホール
  - OS、アプリケーションに存在する脆弱性を利用
- 設定ミス、バックドア

ホストへの攻撃：不正侵入

アカウントのなりすまし

- パスワードの解析・推測（オンラインクラッキング）
  - システムに何度も接続し、生成したパスワードを ひとつひとつしらみつぶしに調べる
  - 時間がかかり、大量のログが残る。攻撃者には高リスク



防御法：

- ログインに失敗するごとに、次回ログインするのに必要な待ち時間を倍増
- 規定回数以上の連続失敗に対しアカウントをロック

ホストへの攻撃：不正侵入

アカウントのなりすまし

- パスワードの解析・推測（オフラインクラッキング）
  - 暗号化されたパスワードファイルを取得し、手元の計算機資源で解析

パスワードファイルの例（UNIX）

```
root: qG13XGpfHqAww:0:0:Super-User:/:/bin/tcsh
hirano: DqsGjJ9SuABPY:1:100:Shoji Hirano:/home/hirano:/bin/tcsh
```

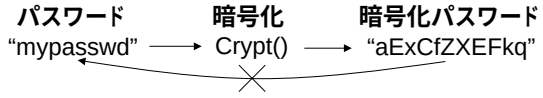
暗号化されたパスワード
（正確には、パスワードをキーとして ある文字列を暗号化したもの）

  - 最小限のログしか残らない
  - 相当規模の計算機資源と時間があれば確実に解析可能

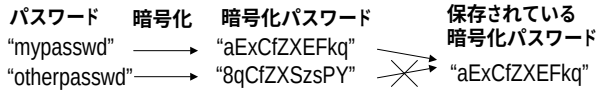
ホストへの攻撃：不正侵入

アカウントのなりすまし

- パスワードの仕組み



  - 暗号化アルゴリズム：DES、MD5
  - 一方向性のハッシュ関数を用いる。 逆関数の計算は現実的にはほぼ不可能
- パスワードの照合



ホストへの攻撃：不正侵入

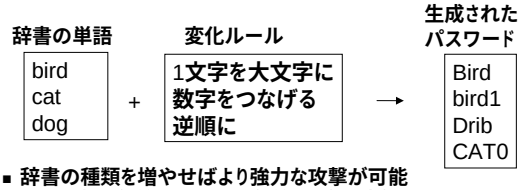
アカウントのなりすまし

- ブルートフォース攻撃（総当り攻撃）
  - パスワードで使用するすべての文字組を生成して総当り
  - 計算時間は（文字種類数）の（桁数）乗に比例
  - 4桁、アルファベット大文字のみなら26^4=46万通り
    - AAAA, AAAB, AAAC, … ZZZY, ZZZZ
  - 6桁、アルファベット大文字＋数字なら36^6=21億通り
  - 8桁、アルファベット大文字、小文字＋数字なら62^8=200兆通り
- 防御策
  - パスワードに大文字、小文字、数字を混ぜ、桁数を多くし、計算時間を非現実的にする
  - ワンタイムパスワード

ホストへの攻撃：不正侵入

アカウントのなりすまし

- 辞書攻撃
  - 辞書にある単語と変化ルールを組み合わせてパスワードを生成



  - 辞書の種類を増やせばより強力な攻撃が可能 車の名前、タレントの名前、人名、地名．．．。
- 防御策： 辞書に載っている単語をそのまま使わない

ホストへの攻撃：不正侵入

アカウントのなりすまし

- キーロガー
  - あらかじめソフトを仕込み，キー入力をすべて記録
  - パスワード，クレジットの暗証番号等を識別して利用
  - インターネットカフェなど，共有型ＰＣで被害例
  - ネットバンキングを悪用して他人の口座から預金を引き出す
  - 不用意なソフトの導入を防ぐ適切な権限設定が必要
- スパイウェア

ホストへの攻撃：不正侵入

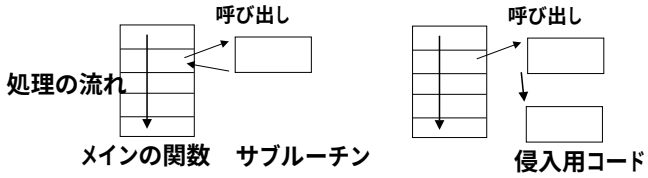
ホストのなりすまし

- アクセスを許可されているホストになりすます
  - FTPバウンスアタック
  - TCPシーケンス番号によるIPスプーフィング
  - DNSの詐称
- 踏み台
  - あるサイトに侵入し、そこからさらに別サイトを攻撃
  - 多段の踏み台を経ることで追跡を困難に

ホストへの攻撃：不正侵入

セキュリティーホール

- システムのセキュリティ上の欠陥（プログラムの誤り等）を突いた攻撃
- バッファオーバーフロー攻撃
  - オーバーフローを利用して関数の戻りアドレスを書き換え、任意のプログラムを実行



ホストへの攻撃：不正侵入

セキュリティーホール

- CGI のバグを利用した攻撃
  - CGI (Common Gateway Interface) :
    Webサーバにおいて、ユーザからの要求に応じて動的に変化するコンテンツを提供するための仕組み
    - 例：カウンタ、検索エンジンなど

  - バグがあると任意のコードを実行され得る
    例：phfのバグを突きパスワードファイルを表示させる

http://www.some.site/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

ホストへの攻撃：

コンピュータウイルス／ワーム

- コンピューターウイルス (Computer Virus)
  - 「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの」（IPAより）

(1)自己伝染機能
自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

(2)潜伏機能
発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

(3)発病機能
プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

ホストへの攻撃：

コンピュータウイルス／ワーム

- ワーム (Worm)
  - ネットワークにまたがり自律的に増殖するプログラム
  - 最近のウイルスは「ウイルス型ワーム」
- ウイルス、ワームはOSやアプリケーションのセキュリティホールをついて伝染
  - Microsoft Outlook Express（「I love you」他多数）
  - Microsoft Internet Explorer（「Nimda」他多数）
  - Microsoft IIS server (「CodeRed」他多数）
  - Sun sysadmind（「Sircam」他）
  - Linux + BIND（「Lion」他）

ホストへの攻撃：ウイルス / ワーム

ウイルス／ワームの動作例

- 感染したコンピュータにあるファイルを消去
  (ExploreZip.worm等)
- 大量の電子メール送付 (Melissa等多数)
  - 計算機／ネットワーク資源の浪費
- 個人情報の頒布 (Antinny等)，ファイル転送 (Sircam等)
  - 機密情報の漏洩
- 特定サイトへのDoS（サービス不能）攻撃 (Codered等)
  - サービス提供の妨害機能停止

ホストへの攻撃：ウイルス / ワーム

最近のワーム例： Nimda

- 強力な感染力
  - 感染経路の多様化
    - メール： 感染ファイルのプレビュー、閲覧
    - Webブラウズ： 感染サイトのページ閲覧
    - IISサーバへのファイル転送
    - 共有ドライブへのコピー
  - 感染後の動作の多様化
    - 感染の継続： メール、IISサーバ、共有ドライブ
    - Webページ改ざん： Javaスクリプト埋め込み
    - バックドア作成
    - システム改変：常にウイルスを起動状態に

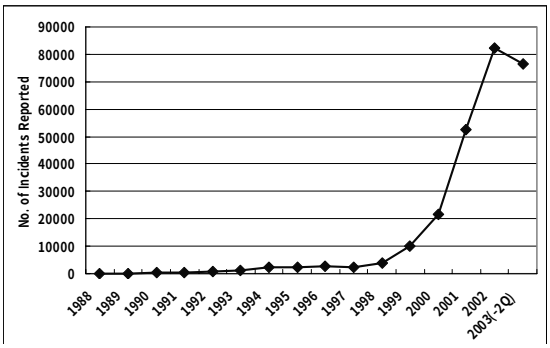
ホストへの攻撃：ウイルス / ワーム

最近のワーム例： Antinny

- P2Pファイル共有ソフトwinnyを経由して感染
  - 個人情報の流布
    - ログイン名／登録名，組織名，メールアドレス
    - 画面のスクリーンショット
    - 個人情報をwinny共有ネットワークへ自動的に頒布；<u>回収は現実的に不可能</u>
- 実際に機密度の高い情報が流出
  (いずれも詳細な原因は調査中)
  - 捜査書類： 複数の警察組織
  - 防衛関連書類： 自衛隊

ホストへの攻撃：ウイルス / ワーム

感染件数の推移

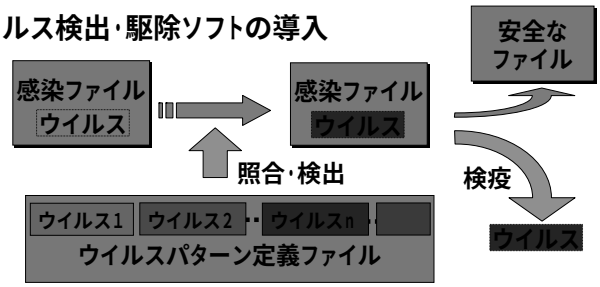


※2003年7月現在、CERT報告分

ホストへの攻撃：ウイルス / ワーム

感染を防ぐには

- ウイルス検出・駆除ソフトの導入



- <u>ウイルス定義ファイルを常に最新の状態に保つことが肝心！</u>

ホストへの攻撃：ウイルス / ワーム

感染を防ぐには

- OS/アプリケーションに対するセキュリティパッチ適用
  - 既知のセキュリティーホールを塞ぐ
- 不審なメール/ファイルは開かない
  - 完全なウイルスチェックは困難
  - 定義ファイルに無い新種のウイルスは検出できない
    - 医学部での感染例
      - Frethem (2002年7月)
        - 日本で発生した亜種
        - 対応済定義ファイルの配布以前に侵入、数人のユーザが実行して感染・メールの大量送信等の活動を発動
        - 対策のためメールサーバを1日間停止
      - MSBlast (2003年8月)、Netsky (2004年3月)

ホストへの攻撃：

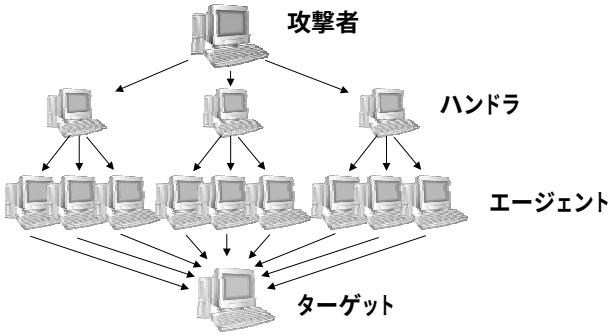
DoS攻撃

- DoS: Denial of Service; サービス不能
- サーバのフリーズ、サービスの停止が目的
  - Flood系DoS攻撃
    - サーバに大量のデータ（パケット）を送りつけて洪水状態にさせ、サービスを停止させる
  - 奇形パケットの悪用ーPing of Death
    - 規定外のパケットを送り処理エラーを起こさせる
  - トラフィックの高過負荷化
    - ネットワーク帯域を占有し、サービス継続を不可能に

ホストへの攻撃：

Distributed DoS (DDoS)攻撃

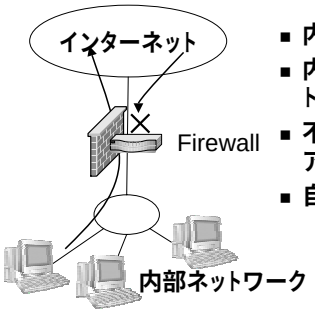
- 分散した多数のホストからの同時DoS攻撃



ホストでの防御：

ファイアウォールによる防御

- Firewall: 防火壁
  - 攻撃による被害から内部ネットワークを守る「壁」

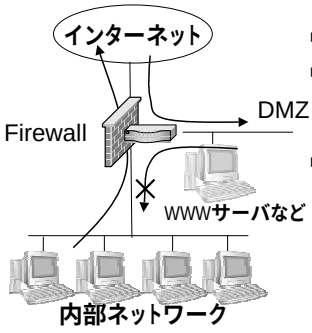


- 内部ネットと外部ネットの境界に設置
- 内部／外部をまたぐのすべての トラフィックを監視し、アクセスを制御
- 不正なアクセスは遮断、適切な アクセスのみを通過
- 自身への攻撃に備え要塞化

ホストでの防御：

ファイアウォールによる防御

- DMZ: De-Militarized Zone；非武装地帯

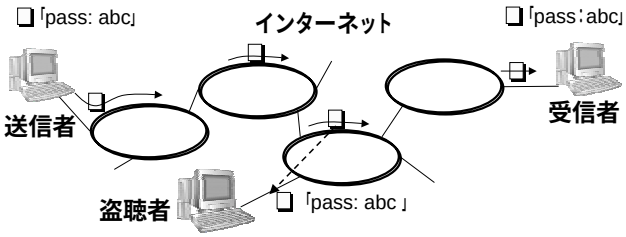


- 内部と外部の中間地帯
- 不正アクセスが予想される危険な 公開サーバ（WWWサーバ、DNS サーバ等）を内部から分離
- DMZから内部へのアクセスを禁止

  → 万一、サーバに侵入された 場合でも、内部ネットの被害を 最小限に限定

通信路への攻撃と防御

通信路への攻撃：盗聴



- 盗聴用ホストを（侵入あるいは物理的に）設置
- ネットワークを流れるすべてのパケットを観察
- 平文で流れるユーザID、パスワードなどを取得

通信路への攻撃：

ネットワーク盗聴の種類

- パケットキャプチャリング
  - ネットワークを流れるすべてのパケットを受信して解析
- 偽サーバ・偽プロキシ
  - DNSキャッシュを書き換えて本物のサーバになりすます
- 経路情報の書き換え

通信路への攻撃：

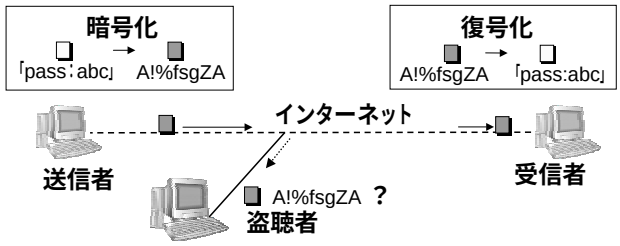
ネットワーク盗聴の危険性

- 電話の盗聴に比べ、不特定多数に対して容易に、かつ地理的要因に束縛されずに実施可能
- 盗聴により信用情報など重要なデータが流出
  - 電子商取引： クレジット番号、暗証番号
  - 各種サービス利用： アカウント、パスワード
  - 電子メール： 内部情報、パスワード、文書ファイル

通信路での防御：

暗号化

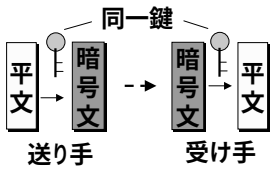
- 盗聴への対策：暗号化
  - 通信内容を暗号化し、盗聴されても判読できない形に
  - 送り手で暗号化、受け手が復号化



通信路での防御：

通信内容の暗号化

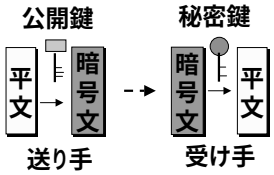
- 暗号化、復号化の方式
  - 共有鍵暗号方式（秘密鍵暗号方式）
  - 公開鍵暗号方式
- 共有鍵暗号方式
  - 送り手、受け手が同じ鍵を共有
  - 処理が高速
  - 鍵交換時の安全性が問題
    - メールで送れば鍵自体が盗聴の危険にさらされる
  - 相手ごとに異なる鍵が必要



通信路での防御：

通信内容の暗号化

- 公開鍵暗号方式
  - 2種類の異なる鍵を使用
    - 受け手の鍵： 秘密鍵
    - 送り手の鍵： 公開鍵
  - 受け手は秘密鍵から公開鍵を作成し、送り手に渡す
  - 公開鍵で暗号化した文は、秘密鍵でのみ復号化可能
  - 公開鍵では復号化できないため、鍵交換が容易
  - 鍵の改ざんのみに気をつければよい
  - 処理に時間がかかる



通信路での防御：

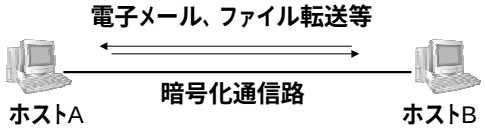
通信内容の暗号化

- 暗号化方式の比較
- これらの複合形も用いられる
  - 例：電子メールの暗号化
    - メッセージ本文：共有鍵暗号方式
    - 共有鍵： 公開鍵暗号方式

通信路での防御：

通信路の暗号化

- 通信路そのものを暗号化し、その上を流れるすべての通信を盗聴から保護する



通信路での防御:

通信路の暗号化

- VPN (Virtual Private Network)
  - インターネットなどの公衆網を専用線のように利用するサービスの総称
  - IPSecなどの暗号化技術を用いて通信路を暗号化
  - 専用線に比べ安価に安全なネットワークを構築可能
  - 信頼性は利用するインターネット環境に依存

通信路での防御:

通信路の暗号化

- VPN のいろいろ
  - IPSec
  - SSL (Secure Socket Layer)
  - SSH (Secure Shell)

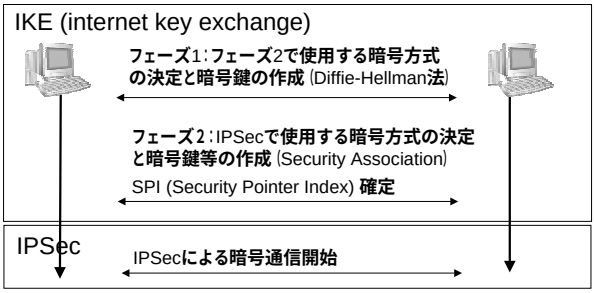
  暗号化を行う層が異なる
- OSI参照モデル
  - 通信プロトコルを機能別に7つの層に分け、それぞれの役割を定義したもの

アプリケーション層	SSH
プレゼンテーション層	
セッション層	SSL
トランスポート層	
ネットワーク層	IPSec
データリンク層	
物理層	

通信路での防御:

通信路の暗号化

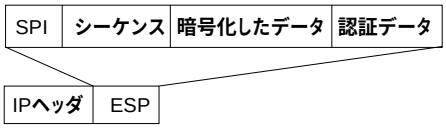
- IPSec (IP Security Protocol)
  - ネットワーク層における暗号化／認証プロトコル
  - 共有鍵暗号方式 (高速、双方向通信)



通信路での防御:

通信路の暗号化

- IPSec (続き)
  - ESP (Encapsulating Security Payload)
    - IKEで作り出したSPI、暗号化されたデータ、認証データ、シーケンス番号を入れる入れ物
    - 通常のIPヘッダのあとにつなげ、カプセル化したデータを送る



  - SPI, 暗号化、シーケンス、認証データの組により、データの完全性、機密性の確保と認証を実現

通信路での防御:

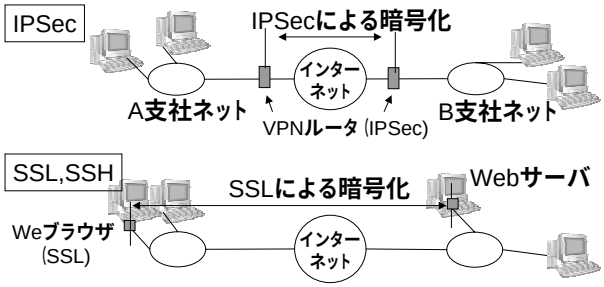
通信路の暗号化

- SSL (Secure Socket Layer)
  - セッション層における暗号化／認証プロトコル
  - 認証は公開鍵暗号方式、通信の暗号化は共有鍵暗号方式
  - HTTP、FTPなどの上位プロトコルによる通信を暗号化
  - Webブラウザなど、アプリケーションごとに実装
- SSH (Secure Shell)
  - アプリケーション層における暗号化／認証プロトコル
  - システムへの遠隔ログイン、ファイル転送などを行うアプリケーション間の通信を暗号化

通信路での防御:

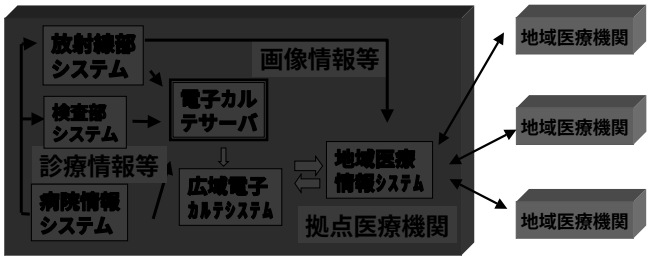
通信路の暗号化

- IPSecは包括的な暗号化、SSL、SSHはアプリケーション、ホストなどの対象を限定した暗号化向き



遠隔地医療支援システム

- 診療機関間で診療情報を共有
- 大規模病院の存在しない遠隔地においても
  質の高い医療、保健、福祉を提供

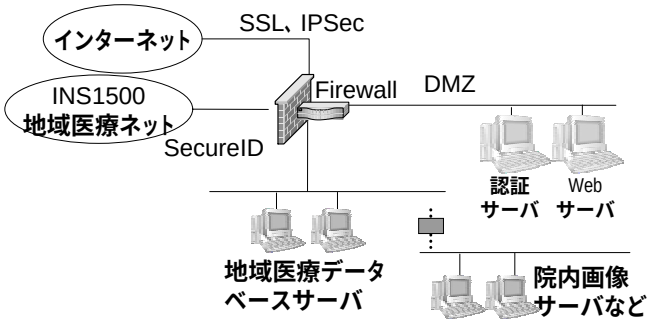


遠隔地医療支援システム

- 想定される脅威
  - 医療情報サーバへの侵入、あるいはネットワーク盗聴
    による個人情報の不正取得
  - 部外者の不正利用
  - DoSアタック等による機能停止
- 要求されるセキュリティ技術
  - 侵入対策： ファイアウォール
  - 盗聴、改ざん対策： 通信路暗号化
  - 不正利用： 認証

遠隔地医療支援システム

- 実際のシステム（島根地域医療情報ネットワークの例）



まとめ（1）

- 個人情報の取扱を巡る概念の変化
  - 職務上の守秘→個人による自己情報のコントロール
- 個人情報保護法
  - 医療情報との深い関わり； 多彩な要秘匿情報
  - 患者の同意の重要性が増加
  - 実際に医療に適用した場合，具体にどのようになるか，
    まだ未確定
    - 個別法の策定（個人情報保護法案に対する付帯決議）
    - ガイドラインの策定

まとめ（2）

- 診療情報の電子化
  →電子情報としてのセキュリティ対策が必要に
- 情報セキュリティの3要素
  - 機密性，完全性，可用性
- セキュリティの分類
  - 物理的セキュリティ
  - 論理的セキュリティ → ネットワークセキュリティと関連
  - 人的セキュリティ

まとめ（3）

- 中心的な防御技術
  - 暗号化、認証、アクセス制御
  - コンピュータウイルスチェック
  - 最新のセキュリティパッチ適応
- インターネットを利用した遠隔地医療では
  個人情報の秘匿が最重要用件
- 技術的な対応には限界がある；
  人的脅威の排除が現実的な重要課題
  - 内部漏洩の防止，パスワードなどの管理徹底

参考文献／情報

- 不正アクセス、セキュリティ
  - 白井雄一郎他：不正アクセスの手法と防御、ソフトバンクパブリッシング、2001.
  - CERT: Computer Emergency Response Team http://www.cert/org
  - D. Brent Chapman他：Building Internet Firewalls, O' Reilly, 1995.
- 医療情報システム
  - MEDIS http://www.medis.or.jp/
  - UMIN http://plaza.umin.ac.jp/~jami/

参考文献／情報

- 個人情報保護
  - 開原成允，樋口範雄 編 「医療の個人情報保護とセキュリティ 個人情報とHIPAA法」有斐閣，2003