本資料について

本資料は下記書籍を基にして作成されたものです。
文書の内容の正確さは保証できないため、正確な知識を求める方は原文を参照してください。

書籍名：　ハッカーの秘密
　　インターネットセキュリティ入門
著者：ジェフ・クルーム (Jeff Crume)
訳者：林　秀幸
発行日：2002年8月20日
出版社：株式会社ピアソン・エデュケーション

ハッカーの秘密

渡辺研究室
0404271177　細尾幸宏

背景

- インターネットの急速な普及
- インターネット上でのビジネスの普及
- 情報の価値の増加
- ハッキング被害や悪事に利用される危険性の増加

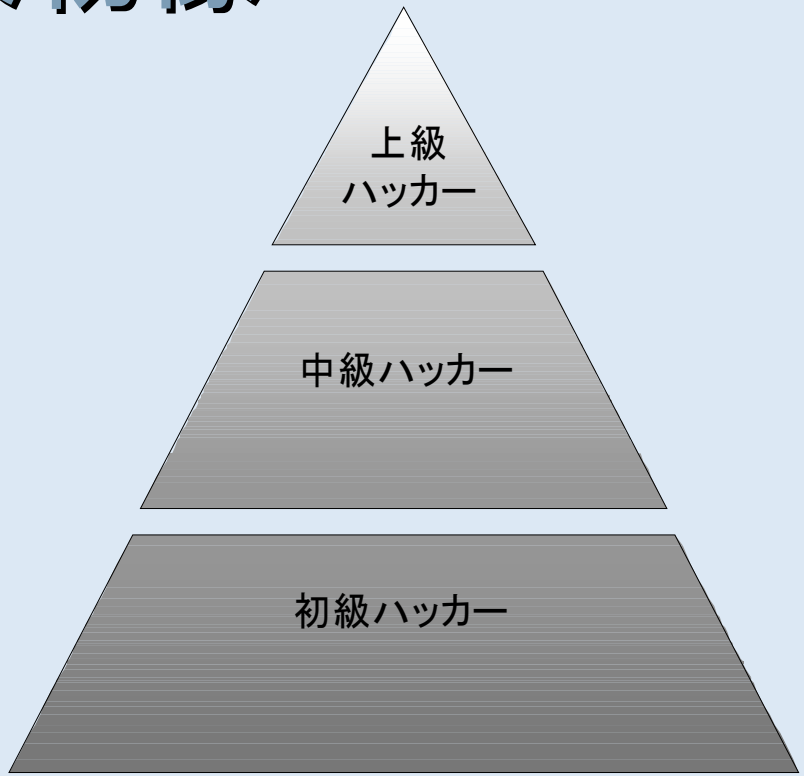
インターネットは安全ではない

- TCP/IPはセキュリティではなく、接続性のために設計されている
- TCP/IPが設計された時代はインターネットのような公衆回線を経由した伝送は想定されておらず、専用回線だけを経由して伝送することを想定していた。
- データにアクセスできる端末は銃を持った警備兵が監視

ハッカーの人物像

ハッカーの種類

- 初級ハッカー
  - 入手したツールを理解せずに使用
- 中級ハッカー
  - ツールの意味を理解した上で使用
- 上級ハッカー
  - 多くのシステムを理解し、新しい攻撃手段を考え出すことができる



ハッキングの目的

- ハッキングを試みること自体が目的
- 金銭目的でなく、自分の楽しみのため

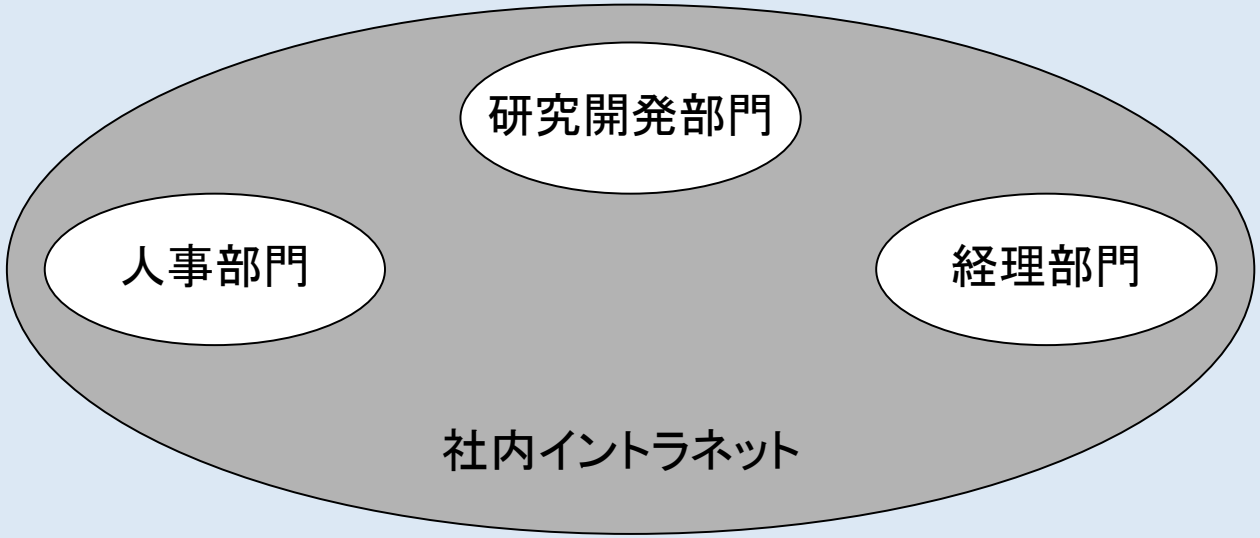
- 企業や組織にとっては重要でもハッカーにとって重要とは限らない
- 画面の向こうにいる「人間」を意識していない

サイバーテロ

- 1996年　スウェーデンのグループがCIAのウェブサイトを書き換え
- 1999年3月　英国軍の通信衛星に侵入し、軍事通信、監視衛星および通話を制御する回線に関する設定を変更
- カナダ、ノルウェー、タイを経由して米国防総省を集団攻撃

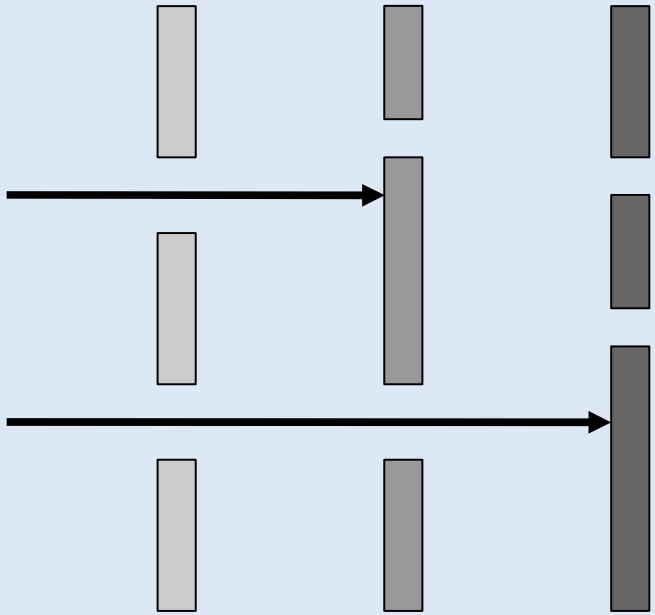
ハッカーは内部にもいる

- 1999年のFBIとCSIによる調査では内部の人間によるハッキングは全体の半数
- イントラネット内にファイアウォールを設置してセキュリティゾーンを確立して内部からも隔離
- 外部からの侵入者にとってもう1つの障害になる



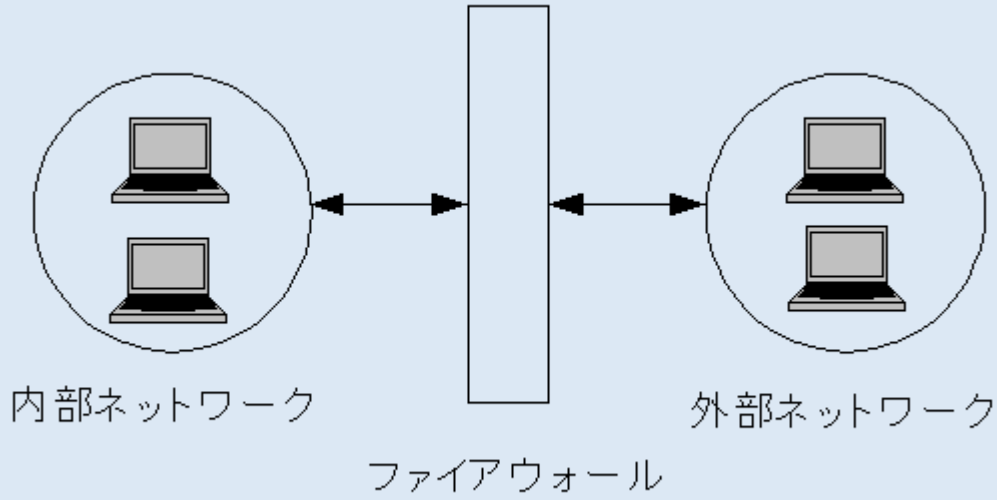
セキュリティ対策

- 単一のセキュリティ対策では脆弱性が必ず存在する
- ツール、方針、手順などを何層にも組み合わせて多重防御
- ハッカーの攻撃が失敗する可能性を高める



ファイアウォール

- 内部ネットワークと信頼できない外部ネットワークの間に設置する防壁



- 主な技術
- パケットフィルタ
- パケットの状態検査
- プロキシ

ファイアウォールの技術

- パケットフィルタ
  - パケットのヘッダ部分を調べて処理を行うか判断
    - 送信元、宛先IPアドレス、プロトコル、ポート番号
- パケットの状態検査
  - パケットのヘッダ情報からアクセスの可否を判断
    - 特定の通信の状況や状態を監視し、異常なデータを発見
    - ネットワーク層を越えた範囲まで検索可能

ファイアウォールの技術

- アプリケーションレベルのプロキシ
  - パケット取り込んでアプリケーションで実行
    - リモートサーバのセッションとクライアントのセッションを別個に用意して内部ネットワークアドレスを隠蔽
    - オーバヘッドの増加によりパフォーマンスが低下
    - 保護するアプリケーションごとにプロキシを書く必要

ファイアウォールの技術

- サーキットレベルのプロキシ（例：SOCKS）
  - トランスポート層で動作しデータ送受信を代理
    - リモートサーバのセッションとクライアントのセッションを別個に用意して内部ネットワークアドレスを隠蔽
    - プロキシだけが2つのセッションの関係を知っているので内部のホストは特定の種類のネットワークベース攻撃から隔離される

システムの中で最も弱いのは人間

- スパイ組織CIAの元長官のような立場の人なら機密情報をセキュリティの弱いコンピュータに置いておくことが危険な行為だと認識しているはず
- しかし、実際にはこれと同様な危険な行為を行っていたことをCIAは認めている

パスワードは安全ではない

- ユーザIDとパスワードによる認証システム
- パスワードの問題点・・・パスワードを知っていれば本人に間違いないと仮定する
- しかし、パスワードのような「知識」は複数人で共有できてしまう

パスワードを覚える人間の問題

- 楽なほうを選択する傾向
  覚えやすいパスワードを設定する
  複数のパスワードを同じものに設定する

- 人間には複雑なパスワードを覚えるのは困難
  頻繁に変更されるパスワードを覚えるのは困難
  解析されにくいパスワードを覚えるのは困難

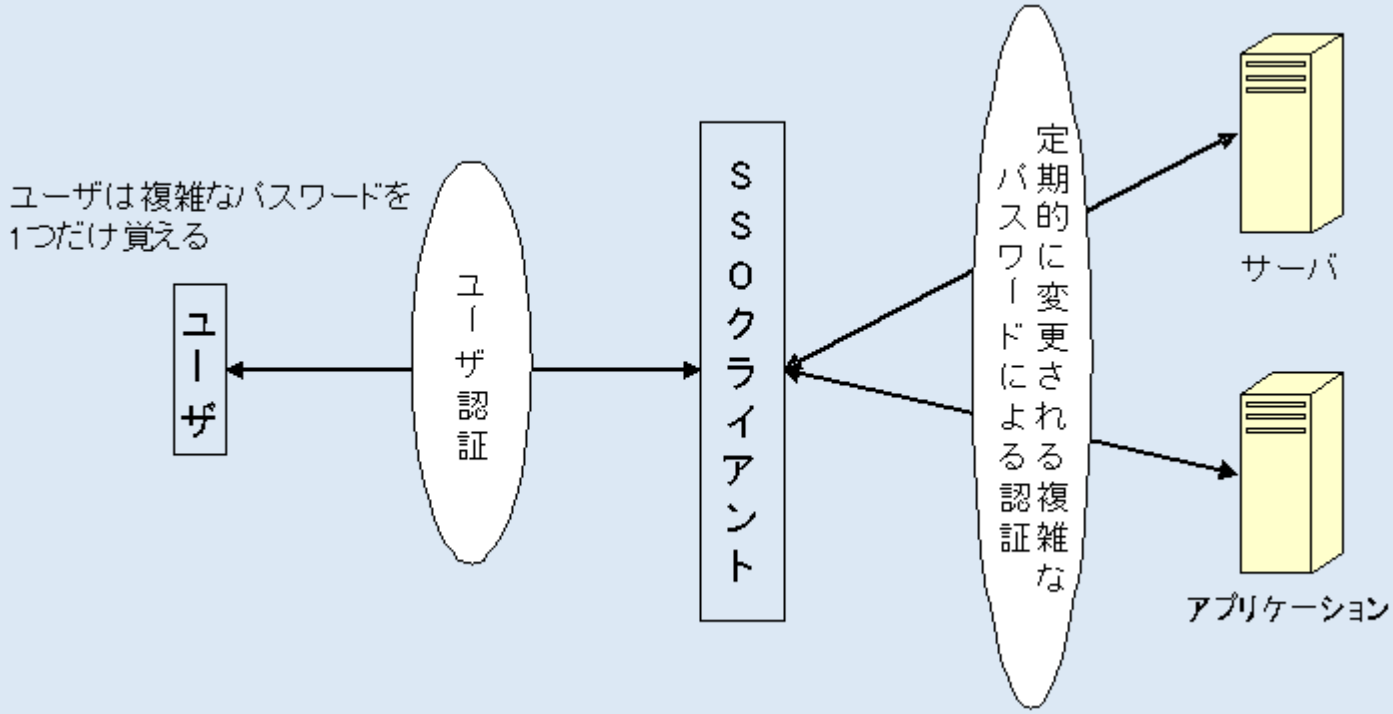
パスワードを破る

- パスワードを推測
- パスワードを盗み見る
- 辞書攻撃と合成攻撃
- 総当り攻撃

- ハッカーはしばらく待っているだけでいい

シングルサインオン（SSO）

- セキュリティと使いやすさを両立した方法

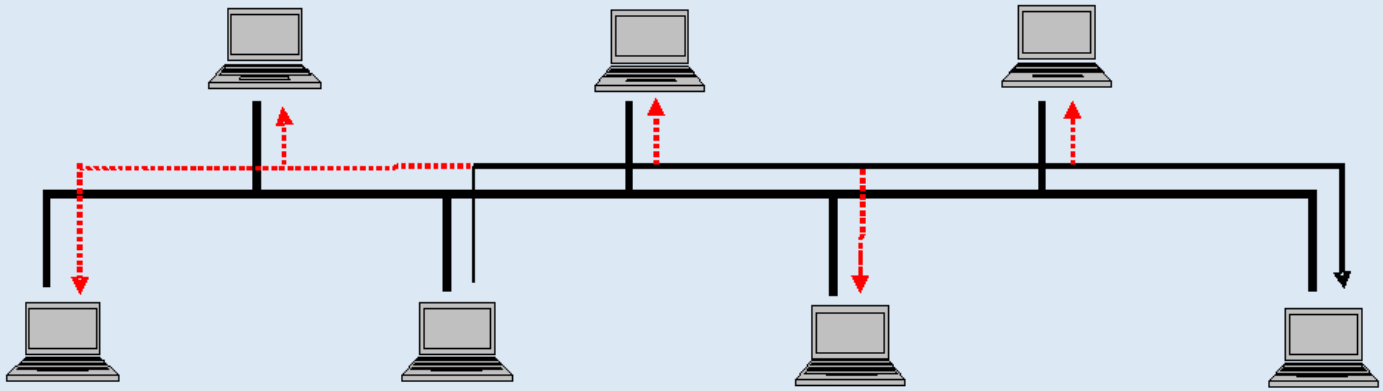


- 単一のパスワードで複数のシステムにアクセスできる問題の解決にはならない

ネットワークの盗聴

イーサネット**(Ethernet)**の基本動作

- パケットを作成してネットワークにブロードキャスト
- パケットは接続しているすべての端末に到達する
- 端末は自分宛のパケット以外はすぐに破棄する



LANアダプタのプロミスキャスモード

- プロミスキャスモードは自分宛かどうかに関係なく、全てのパケットのデータをコピーする
- 宛て先以外のノードがデータをコピーしたことは通知されないし、防ぐこともできない
- ネットワーク管理のための利用とハッカーによる悪用

盗聴

- 盗聴は受動的に動作し、発見が難しい
- トロイの木馬(RAT:Remote Access Trojan)
  - 無害なプログラムを装って盗聴ツールをインストール
- 盗聴ツールはインターネット経由で外部に情報を伝える

盗聴者を発見する(1)

Anti Sniff

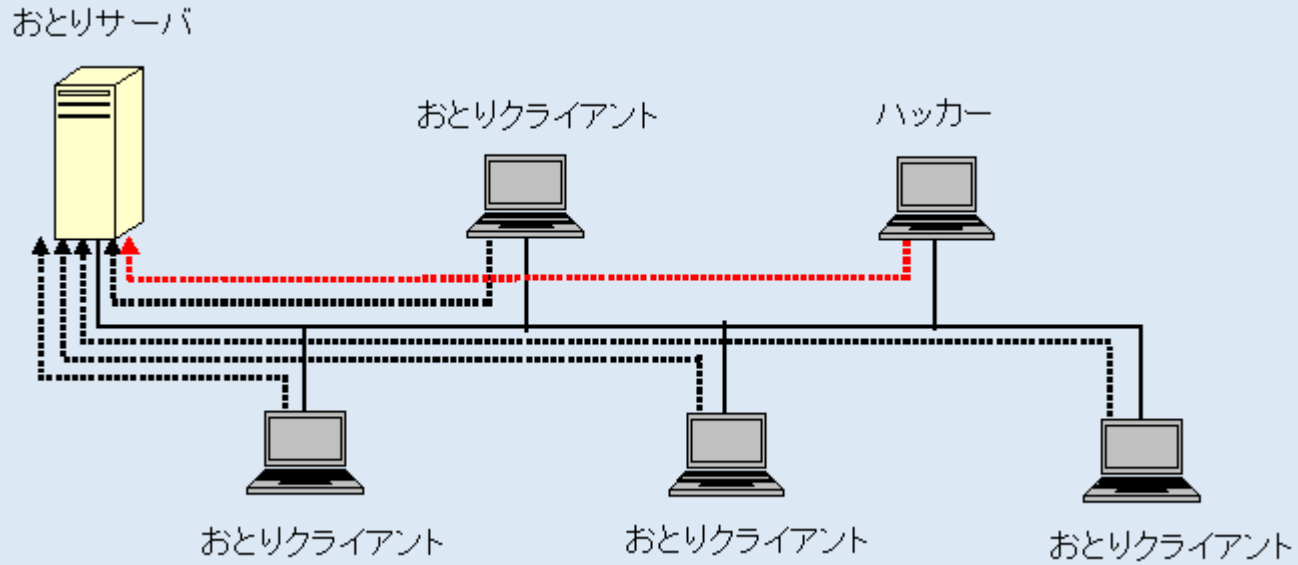
- ネットワーク内に存在しないIPアドレスからの通信データを作成し、調査対象のノードに送信する。ホスト名調べる逆DNS探索を監視

- ネットワーク内に偽物の通信データを大量に発生させた場合に応答に遅延が発生するかどうかを監視

盗聴者を発見する(2)

Sniffer Detector

- いくつかのおとりクライアントがおとりのサーバにログオンし、いくつかの作業を行ってログオフする。
- おとりサーバにおとりクライアント以外のIPアドレスからログオンを試みられたらそれが盗聴者である可能性が高い



攻撃が簡単になってきた

- ハッキングツールの入手が容易になっている
- ツールを使う無知なハッカーによる安易な攻撃の脅威
- ツールを用いた自動攻撃
  サービス不能攻撃（DoS攻撃）
  SYN洪水攻撃（SYN flood）
  Smurf攻撃
  分散型サービス不能攻撃（DDoS攻撃）

ハッカーの未来

- ITへの依存度が増すほど脅威も増していく
- 無線LANネットワークの危険性
- 暗号による解決への期待
- 防御する側の未来も明るい

終わり