本資料ついて

- 本資料は下記文献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障できないため、正確な知識を求める方は原文を参照してください。

- 著者：Jeff Crume
- 文献名：Inside Internet Security:
  What Hackers Don’t What You To Know
- 出版社：株式会社ピアソンエデュケーション
- 発行日：2002年8月9日

ハッカーの秘密

渡邊研究室
平田　祐二

インターネットは脆弱

- インターネットを構成するコンポーネントの中で重要な二つ（DNSとルーティングシステム）が脆弱

- DNS：集中化されているために脆弱
- ルーティングシステム：
  - 分散化されすぎているために脆弱
  - 通信相手に頼っているために脆弱

インターネットは安全か

- コンピュータシステムを安全かどうか定義する場合

実用的な面からの定義

「我々がコンピュータを頼りにでき、ソフトウェアが期待通りに動作するならコンピュータシステムは安全」

- 現実では「このコンピュータが安全である」ことを説明できない　→相対的に考えなければならない

例)「システムAはシステムBより安全か」

「このシステムは以前のシステムより安全か」

ハッカーの定義

- ハッキングを行う人
- 特定の活動について未経験であるか又は未熟な人
- コンピュータのプログラミングや問題解決の専門家
- コンピュータに不法に侵入したり、みだりに情報を書き換えたりする人

リスク分析

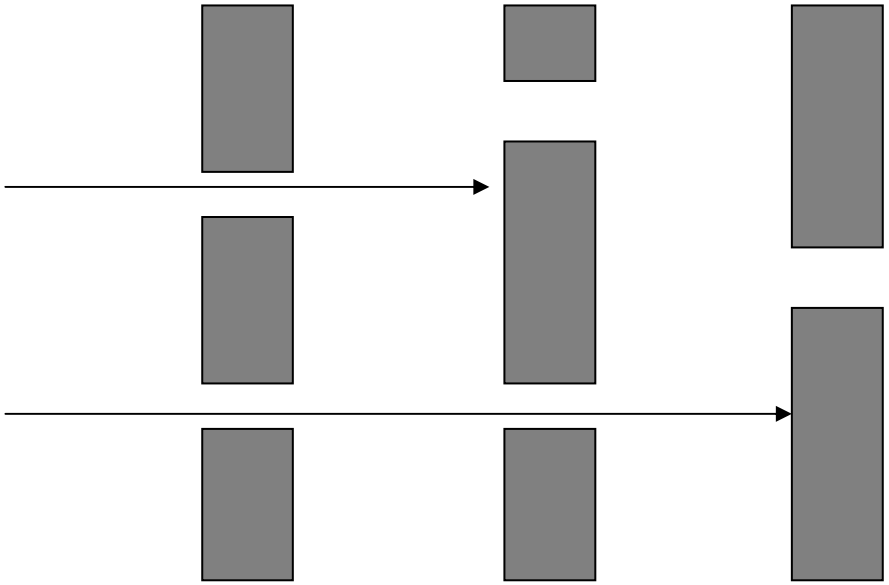
リスク分析をする際の確認事項

- どんな資源を保護する必要があるのか
- 何から、あるいは誰から保護する必要があるのか
- 攻撃を受けた場合にどんな被害を被るか
- 防御にはどんな費用がかかるか

多重防御

- 一つのツールや方針や手順でネットワークの安全を保障できない

  →多重防御が必要となる



危険度の大きさ

装置	信頼性(%)	危険度の累積確立(%)	危険な時間（時間／年）	危険な時間（日／年）
1	99.9	0.1	8.8	0.4
2	99.8	0.2	17.5	0.7
3	99.7	0.3	26.3	1.1
4	99.6	0.4	35.0	1.5
5	99.5	0.5	43.7	1.8
6	99.4	0.6	52.4	2.2
7	99.3	0.7	61.1	2.5
8	99.2	0.8	69.8	2.9
9	99.1	0.9	78.5	3.3
10	99.0	1.0	87.2	3.6

セキュリティ分析

- 危険度は相乗効果
- ビジネスでは顧客がアクセスできるようにしなければならない
- セキュリティはビジネスを抑制するものでなく、促進するものでなければならない

→両者のバランスを保つことが課題

相対価値の高い対策

- ビジネスの現状に合わせてどの対応策が理にかなっているかを判断

相対価値＝損害費用＊損害確率／防御費用

相対価値：システムの安全性
損害費用：攻撃を受けた際に被る費用
損害確率：攻撃を受ける確率
防御費用：セキュリティを構築する際の費用

セキュリティ方針のまとめ

- セキュリティの効果を高める三つの要素

1. 人 ― 知識を持っているか
2. 対策 ― リスク分析を行っているか
3. ツール ― うまく適用できているか

ファイアウォールとは

- 信頼できるネットワークと信頼できないネットワークの間でバッファとしての役割を果たす装置

基本機能

1. パケットフィルタ
2. パケットの状態検査（SPI）
3. アプリケーションレベルのプロキシ

パケットフィルタ

- 受け取ったパケットのヘッダを調べて、そのパケットを次に進めるか遮断するかを判断

規則の作成

- パケットがどこから送られてきたか
- パケットがどこに向かっているか
- 使用するネットワークプロトコルは何か
- 通信データの種類を示すポート番号として何番を使っているか

パケットフィルタの特徴

- 実装が最も単純で、値段も安め
- パケットの先頭部分だけ調べるので処理が速い
- パケットの内部を詳しく調べることはできない

→特定のアプリケーションを標的にした攻撃を検出することはできない

パケットの適性検査（SPI）

- SPIファイアウォールはパケットのヘッダ情報に基づいてアクセスの許可または禁止を判断

- SPIファイアウォールは現在の接続と最近の状態とを表にして管理

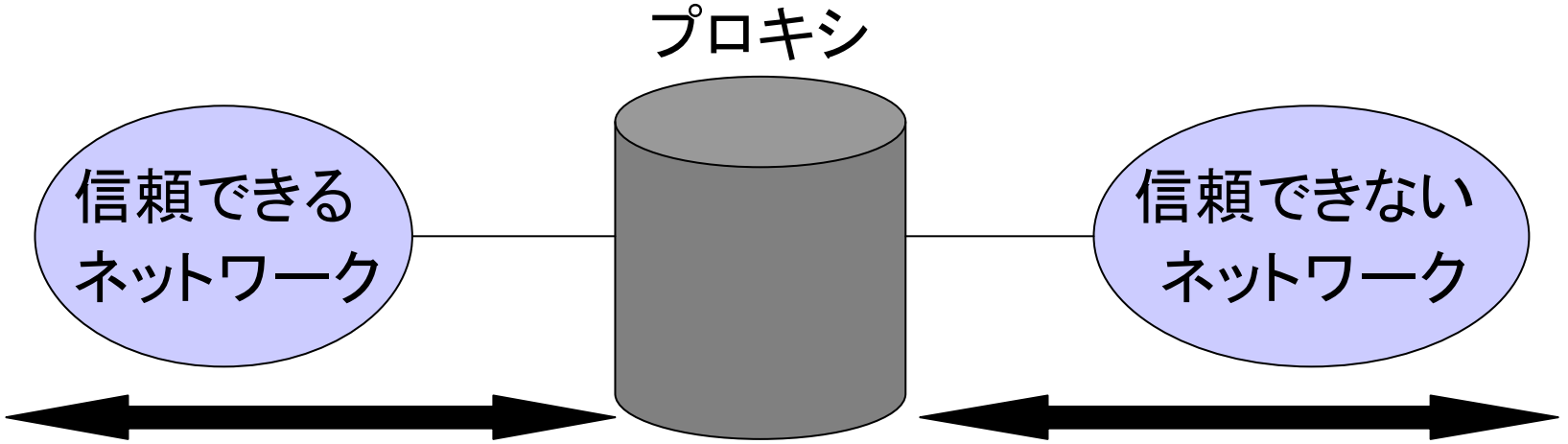
  →脅威となりうる異常なデータの発見

- パケット中に含まれるアプリケーションデータを考慮

  →ネットワーク層を越えた範囲まで検査可能

アプリケーションレベルのプロキシ

- プロキシを使用してアプリケーションレベルでパケットを調べ、受け入れるかどうか判断
- プロキシの仕組みがオーバーヘッドを増し、パフォーマンスの低下
- 保護対象のアプリケーションごとにプロキシを書かなければならない

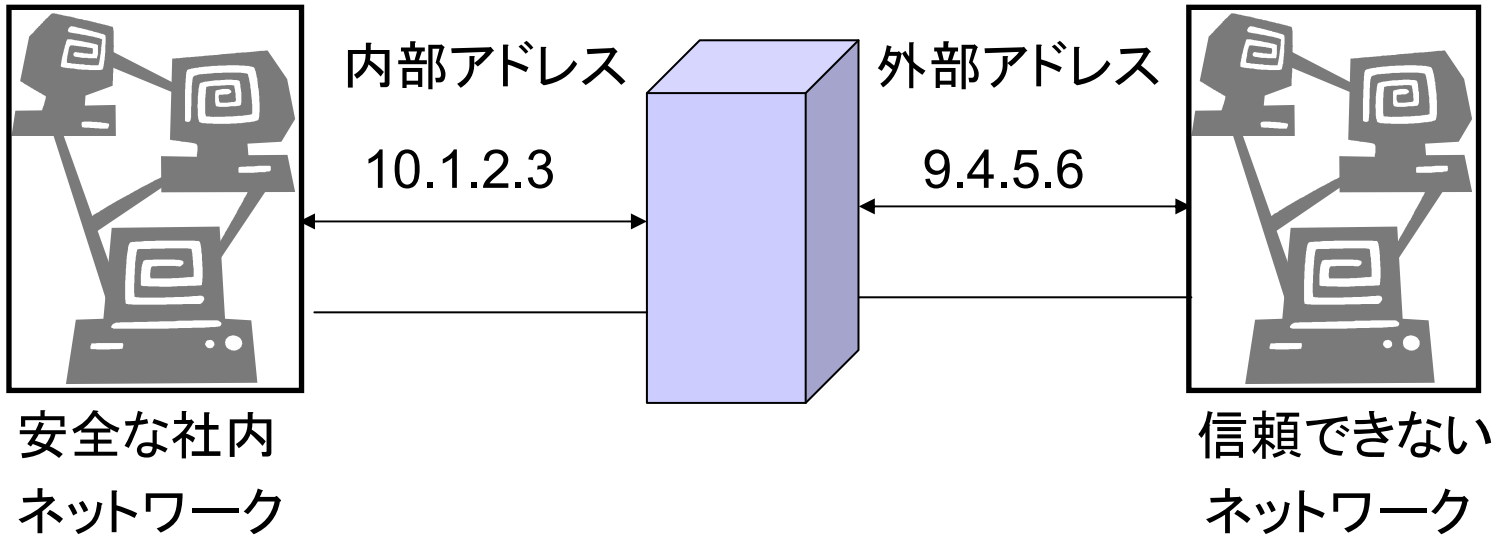


ファイアフォールの可能領域

1. 信頼できないネットワークを隔離
2. 社内のイントラネットの一部を隔離
3. ある種の攻撃に対するリスクを減少
4. ネットワークの一箇所からセキュリティポリシーを実践
5. 一箇所で作業の記録と監視

ファイアウォールの不可能領域

1. プラットフォームを共有してはいけない
2. ファイアフォールの情報を開示してはならない
3. 社内ネットワークの情報を開示してはならない



ファイアウォールの位置づけ

- ファイアウォールの多様性をうまく利用して適切な場所で使用することが大切

- ファイアウォールは全体の一部

- セキュリティを高めるために実践すべきことは多く存在する

（例）脆弱性検査ツール

侵入検地システム