本資料について

- 本資料は下記著書を基にして作成されたものです。著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本を参照してください。

- 著者：白井雄一郎、白濱直哉、又江原恭彦、柳岡裕美
- 著書名：インターネットセキュリティ　不正アクセスの手法と防御
- 出版社：ソフトバンクパブリッシング株式会社
- 発行日：2001年7月26日

インターネットセキュリティ

不正アクセスの手法と防御

第1回輪講課題

発表用資料

渡邊研究室

11300J083 **竹尾大輔**

書籍情報

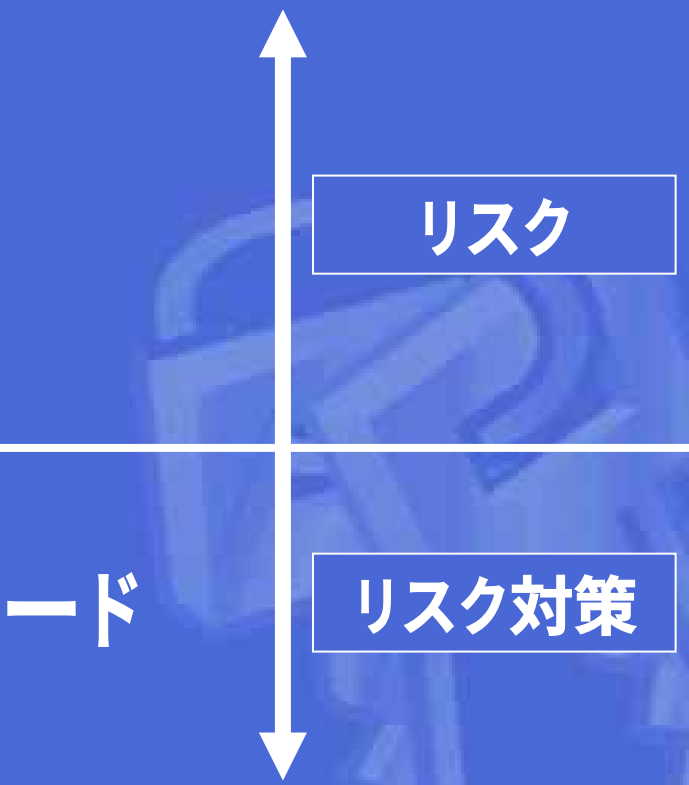
- 書籍名：
  インターネットセキュリティ
  不正アクセスの手法と防御
- 監修者：
  三輪信雄
- 著者：
  白井雄一郎、白濱直哉、又江原恭彦、柳岡裕美
- 発行：
  ソフトバンク　パブリッシング株式会社

はじめに

- 背景
  - インターネットに存在する恩恵とリスク
  - セキュリティに対する関心の高まり
  - なぜ攻撃ができてしまうのかを知ることが重要
  - 攻撃の原理・仕組みを知り、セキュリティを保つ

本書の構成

- 第1章　基本
- 第2章　調査
- 第3章　侵入
- 第4章　DoS攻撃
- 第5章　盗聴
- 第6章　検知・追跡
- 第7章　エクスプロイトコード
- 第8章　防御
- 第9章　情報収集



セキュリティ事情

- 多種多様の攻撃ツールが無料で公開されており、それらをスクリプトキディがゲーム感覚で使うことで、インターネットセキュリティレベルを悪化させている
- セキュリティ情報がＭＬやポータルサイトで議論･公開されているが、攻撃者に有利な情報を与えることにもなっている
- インターネットの匿名性により、不正行為が後を絶たない
- サイトのセキュリティ対策が不十分である

どこがどのように危ないのか

- Webサーバー
  - ホームページ改竄、CGIプログラムの問題
- メールサーバー
  - 不正中継、メール爆弾、本人以外のメール転送・覗き見
- DNSサーバー
  - ホスト情報の漏洩
- 構成・設定が不適切なルータやファイアウォール
  - 不正な経路情報更新、FW/OSのセキュリティホール
- RASからの侵入
  - 内部ネットワークへの侵入、メールの読み出し

調査

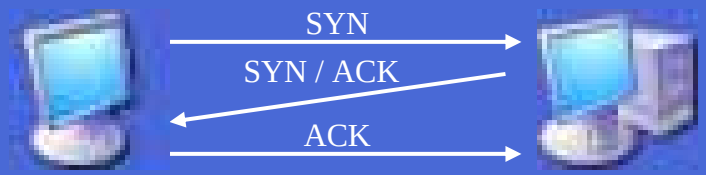
- 攻撃者は、いきなり侵入・攻撃を行うのではなく、事前にターゲットに関する様々な情報を調査している

<table>
<tr><th>ホストの役割</th><th>IPアドレス</th><th>アカウント情報</th><th>稼動サービス</th><th>アプリケーション/OSの種類</th></tr>
<tr><td>tracerouteコマンド</td><td>PINGスイープ</td><td rowspan="2">名刺、
HPのリンク、
容易に推測可能な名前</td><td rowspan="2">ポートスキャン</td><td rowspan="2">スタックフィンガープリンティング</td></tr>
<tr><td colspan="2">DNSからの情報取得</td></tr>
<tr><td colspan="3">whois</td><td colspan="2">バナー情報入手</td></tr>
</table>

ポートスキャン

- １番ポートから順番に接続を行うことで、ターゲットサーバーで稼動しているサービスを調べることができる

TCPコネクションスキャン



コネクションが確立される

TCPコネクションの確立を試みることで、ポートが開いているかを調べる

TCPハーフスキャン

コネクションは確立されない

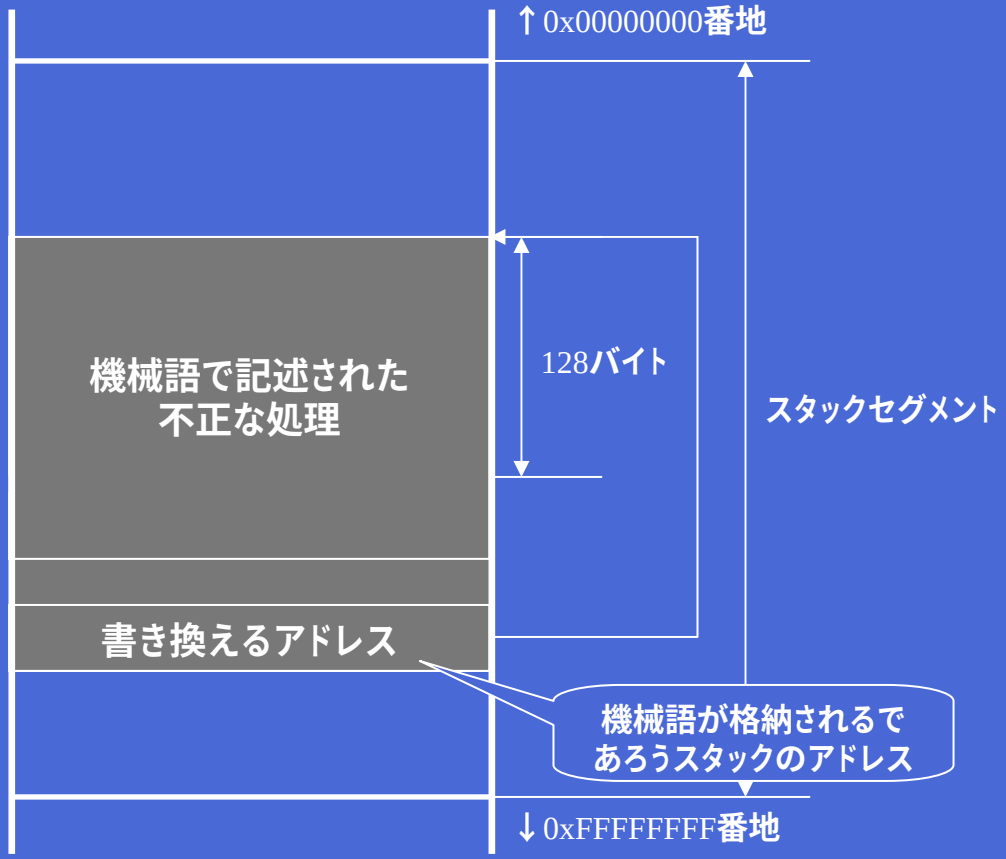
ログに残らない

TCPコネクションを確立することなく、ポートが開いているかを調べる

侵入(1)

- アカウントのなりすましによる侵入
  - ブルートフォース攻撃
  - 辞書攻撃
  - オンライン（オフライン）パスワードクラッキング
- ホストのなりすましによる侵入
  - 踏み台
  - FTPバウンスアタック
  - TCPシーケンス番号推測によるIPスプーフィング
  - IPソースルーティングを利用したIPスプーフィング
- ソフトウェアのバグを悪用した侵入
  - CGIのバグを悪用する攻撃
  - *リモート*（ローカル）*バッファオーバーフロー攻撃*
  - フォーマットストリングバグ攻撃

リモートバッファオーバーフロー攻撃



スタックの状態

```
 1  main()
 2  {
 3        :
 4      sub() ;
 5        :
 6      sub() ;
 7        :
 8  }
 9
10  sub()
11  {
12      int a ;
13      char buf[128] ;
14        :
15      strcpy(buf, DATA) ;
16        :
17      return ;
18  }
```

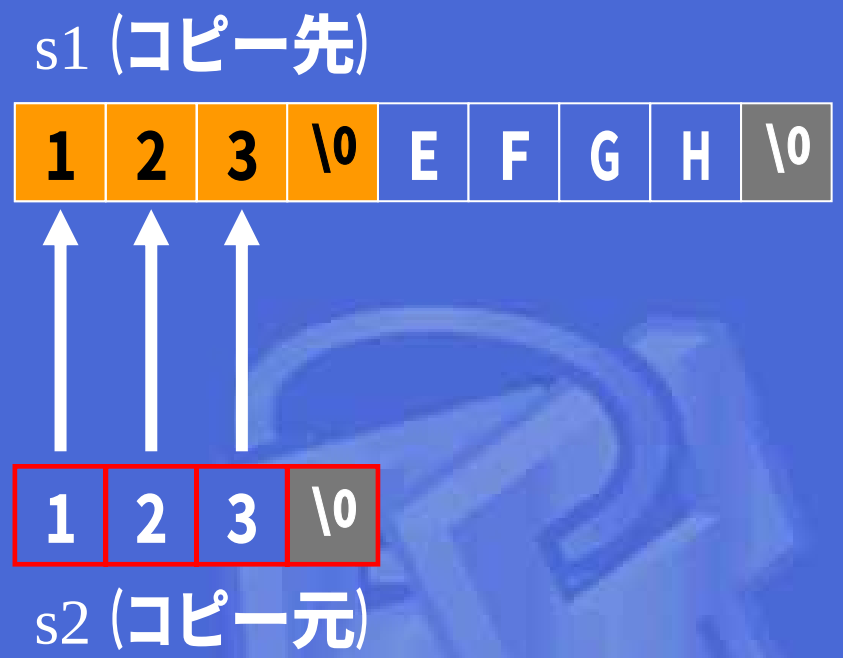
C言語で記述された
プログラム

strcpy()の定義・動作例

```
char *strcpy(char *s1, const char *s2)
{
  char *p = s1 ; /* s1の位置保存のため */

  while(*s2) /* '\0'になるまで */
  {
    *p = *s2 ; /* 代入 */
    p ++ ; /* p を進める */
    s2++ ; /* s2を進める */
  }
  *p = '\0' ; /* 空文字代入 */

  return *s1 ;
}
```

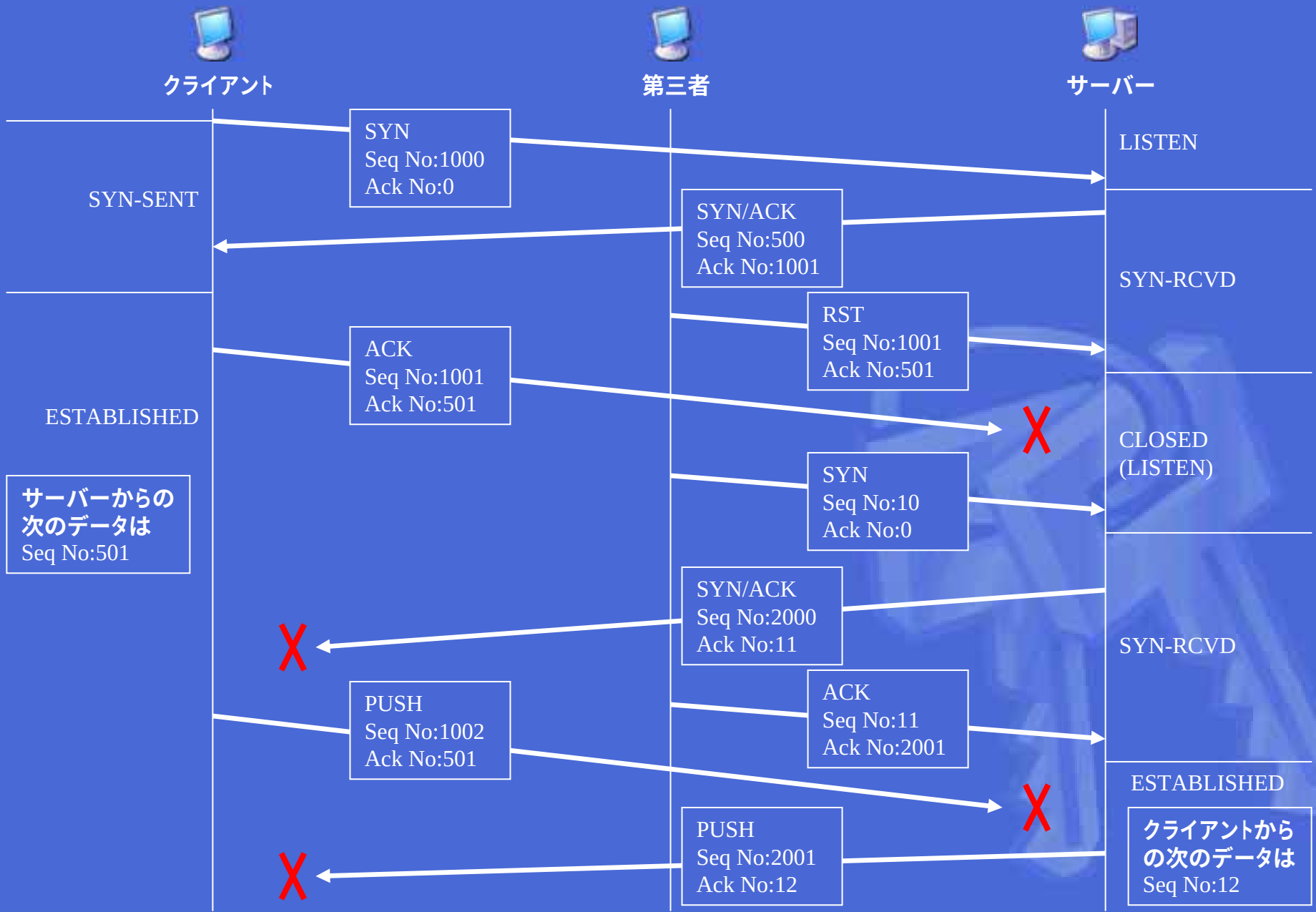


バッファオーバーフローする例

侵入(2)

- セッションハイジャック
  - *TCPシーケンス番号の不整合を利用したハイジャック*
  - 偽造ARPを利用したハイジャック
- バックドアからの侵入
  - inetdを利用したバックドア
  - バックドア専用ツール
  - その他のバックドア（r系サービスの利用、バックドア用アカウント、ベンダー専用バックドア、SetUID rootシェル）

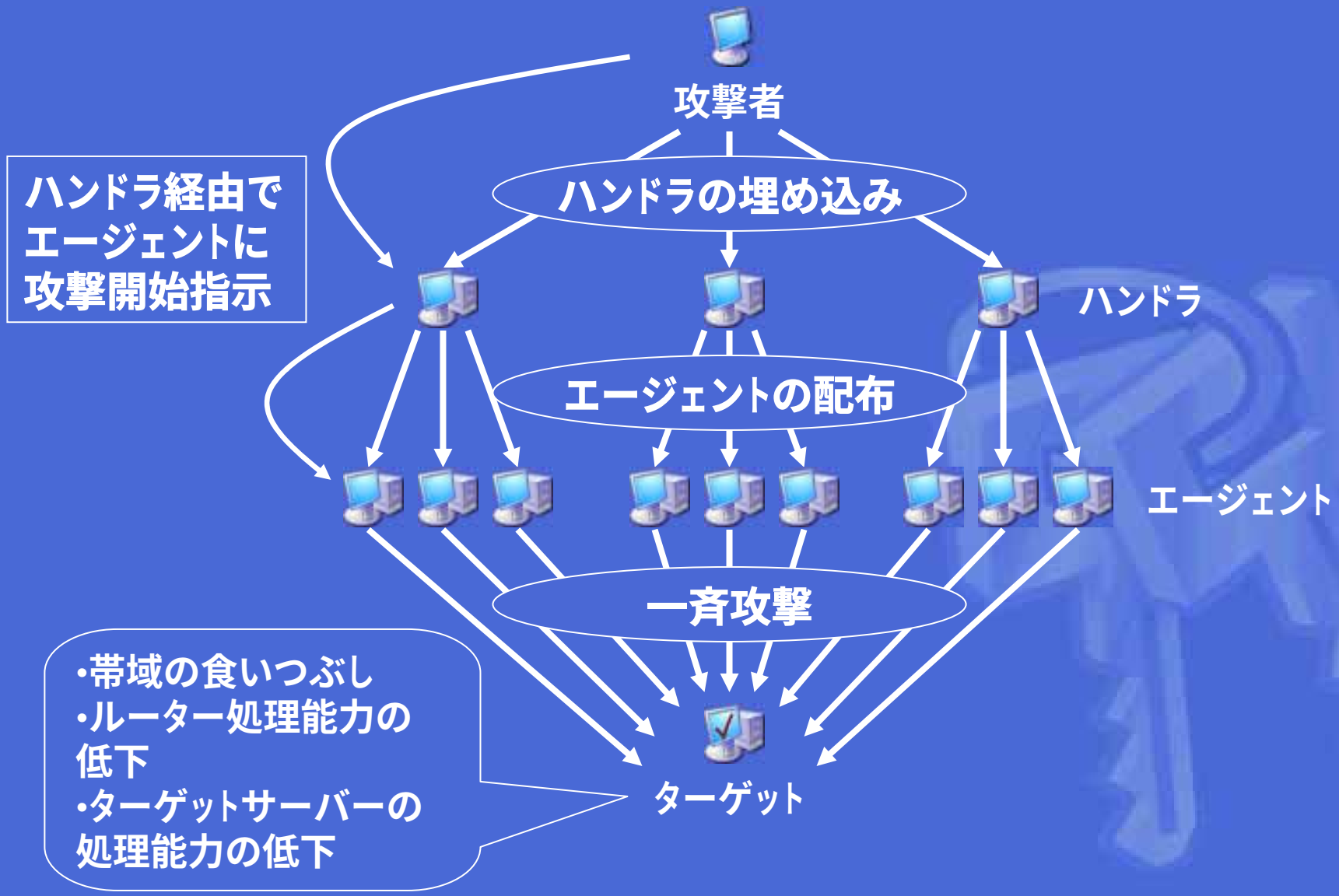
TCPシーケンス番号の不整合を利用したハイジャック



DoS (Denial of Service) 攻撃

- Flood系DoS攻撃
  - SYN Flood攻撃
  - UDP Data Flood攻撃
  - Syslog Flood攻撃
- 奇形パケットを悪用した攻撃
  - Ping of Death
  - Land
- トラフィックを過負荷状態にする攻撃
  - Echo/Chargenループ
  - Smurf
  - DDoS攻撃 (Distributed DoS：分散DoS)

DDoS攻撃

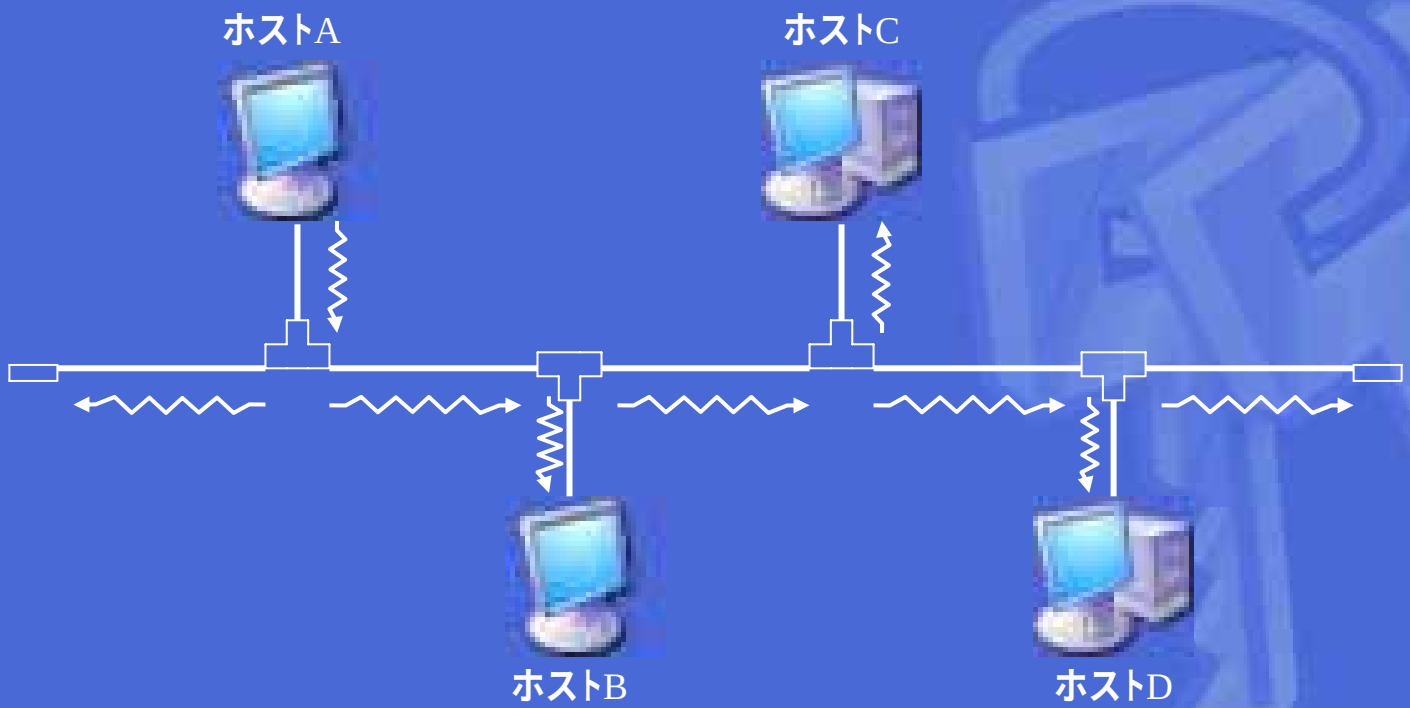

攻撃者
ハンドラの埋め込み
ハンドラ経由で
エージェントに
攻撃開始指示
ハンドラ
エージェントの配布
エージェント
一斉攻撃
ターゲット
•帯域の食いつぶし
•ルーター処理能力の
低下
•ターゲットサーバーの
処理能力の低下

盗聴

- ***パケットキャプチャリング***
- **偽サーバー･偽プロキシ**
- **ルーティング情報書き換え**
- UNIX**固有の問題**
  - **キーボードタッチのキャプチャリング**
  - **トロイの木馬**
- Windows**固有の問題**
  - ***チャレンジレスポンスの盗聴***
  - SMB**パケットの盗聴**
  - **トロイの木馬**

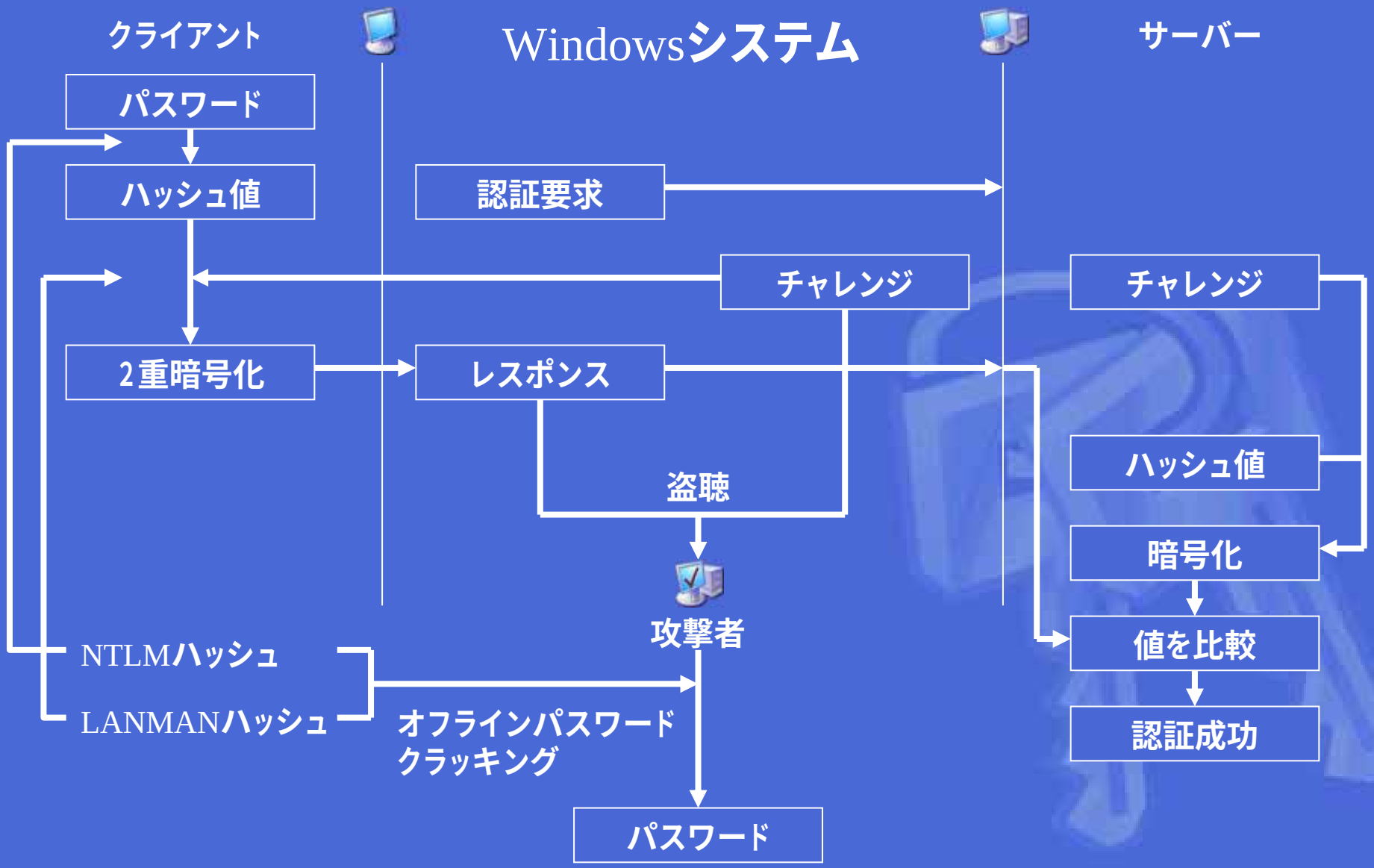
パケットキャプチャリング

- Ethernetを使用したネットワークで通信をする場合、電気信号（パケット）はすべてのノードへと流れている



10BASE-2で構成したネットワーク

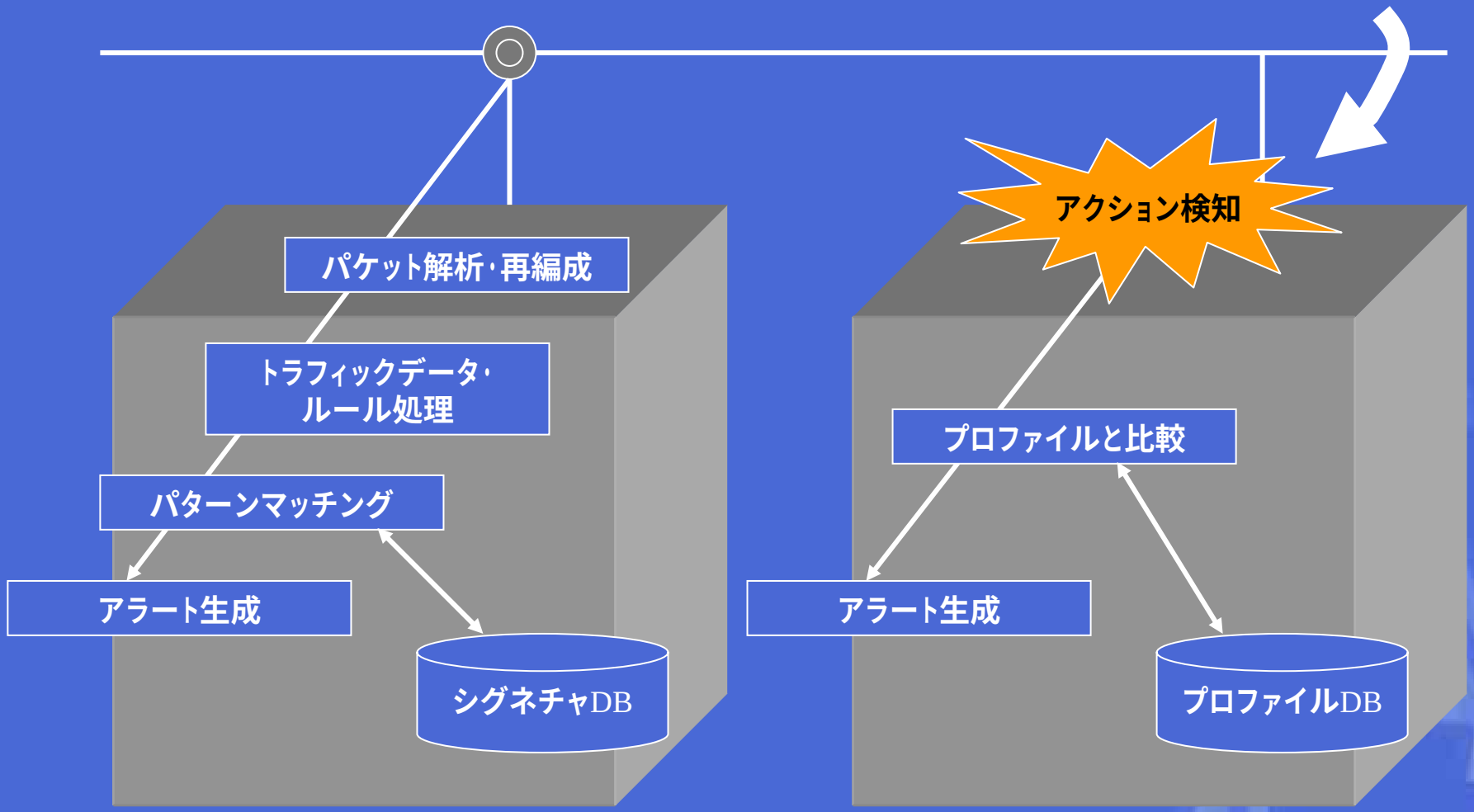
チャレンジレスポンスの盗聴



検知・追跡

- IDS（侵入検知システム）
  - 不正アクセスの監視・検知
  - *ネットワークIDSとホストIDS*
- ハニーポット
  - 偽りの情報を侵入者に与えて、容易に侵入できそうなサーバーのように見せる「おとりサーバー」
- 調査・解析・追跡
  - *ログ*

NIDSとHIDSの概念図



ログ

- 機能
  - 障害や侵入の原因を特定できる調査資料、攻撃者への心理的抑止、攻撃の兆候を発見
- 種類
  - システムログ、アプリケーションログ、サードベンダーアプリケーションログ
- 管理
  - 日付による管理、別ファイルシステムに保存、定期的に圧縮
- 解析
  - ツールを利用した定型的な解析、生のログを専門家が解析

エクスプロイトコード

(バッファオーバーフロー攻撃を例とする)

- エクスプロイトコードとは
  - プログラムで見つかったセキュリティホールに対して実際に攻撃されたときに、どのようなことが行えるかを実証するツール
- セキュリティホールの発見
  - 長い文字列を送り込む、ソースコード解析、リバースエンジニアリング
- エクスプロイトコードの構成
  - ターゲットのアーキテクチャに合わせたコード
  - シェルコードを含んだ、送り込む文字列の生成処理
  - 書き換えるリターンアドレスの埋め込み
  - ターゲットへの文字列の投入 (攻撃部分)

防御

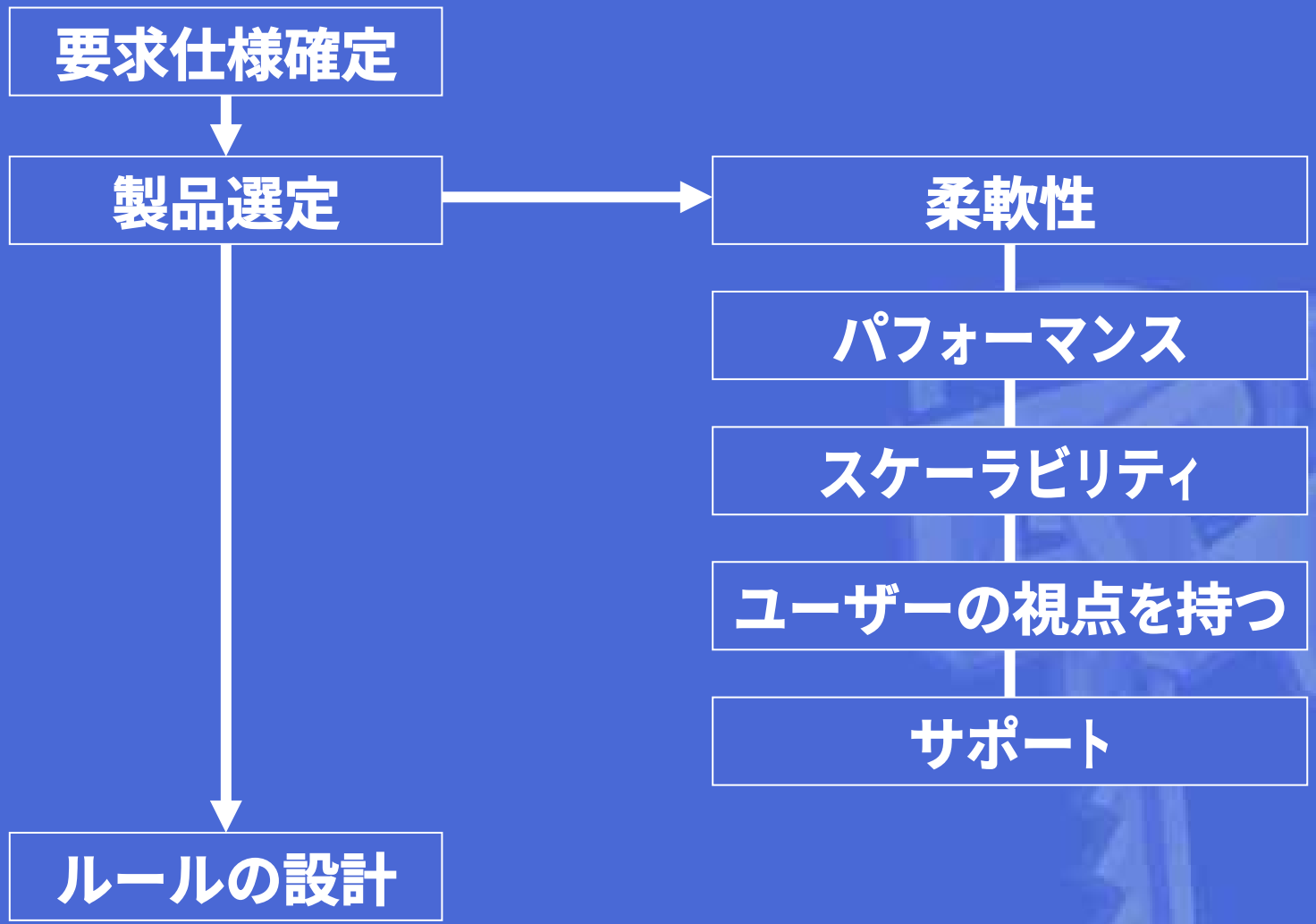
- システム防御の基本設計
  - 防御のためにどのようなインフラを設計・構築すべきか
- ***ファイアウォール***
- ホストの要塞化
  - ファイアウォールの限界、ホスト要塞化の必要性
- ***運用***
  - システムが安全かつ有効に管理され、セキュリティレベルを下げないようにする

ファイアウォールのタイプ

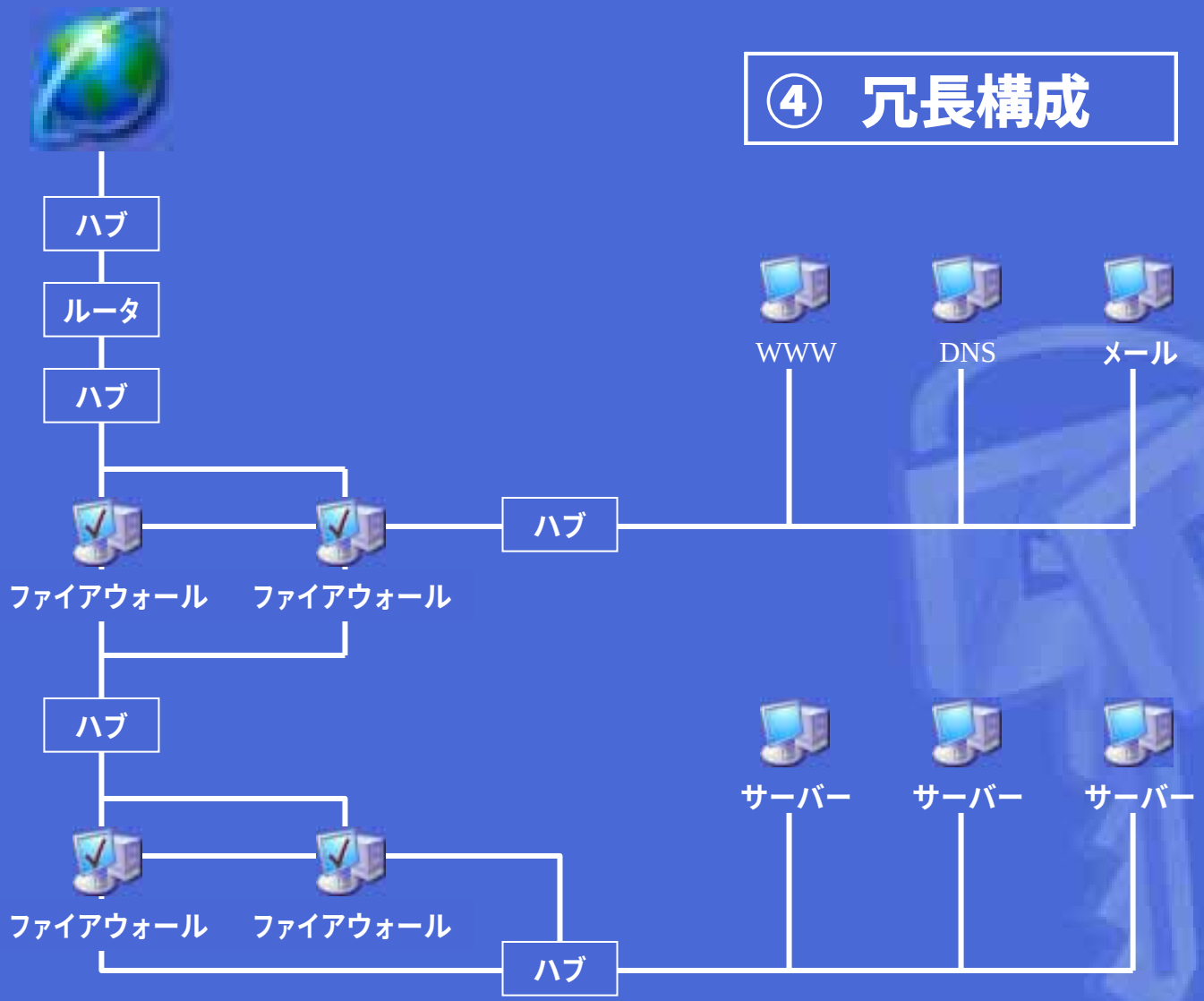
- パケットフィルタリング型
  - パケットの転送元、宛先、転送に用いられるセッション及びプロトコルで転送を判断
- アプリケーション型とハイブリッド型
  - アプリケーション層のプロトコルを理解し、認証システムとの連携が可能

タイプ	参照範囲				
	宛先IP	送信元IP	プロトコルの種類	TCPヘッダー	アプリケーションデータ
パケットフィルタリング型	→	→	→		
アプリケーション型	→	→	→	→	→
ハイブリッド型・オリジナル型	→	→	→		→

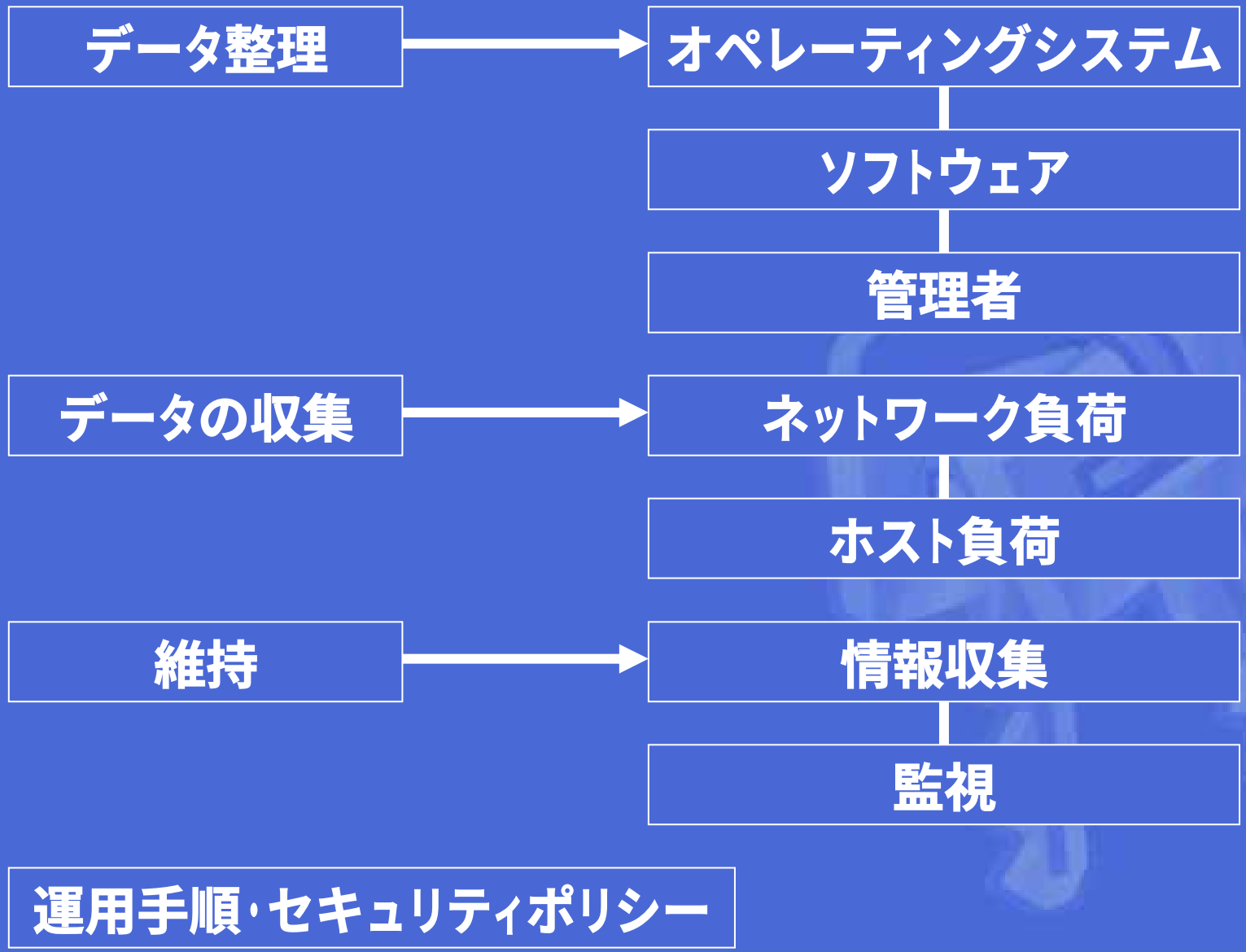
ファイアウォールの設計



ファイアウォールの構成例



運用


データ整理
オペレーティングシステム
ソフトウェア
管理者
データの収集
ネットワーク負荷
ホスト負荷
維持
情報収集
監視
運用手順・セキュリティポリシー

情報収集

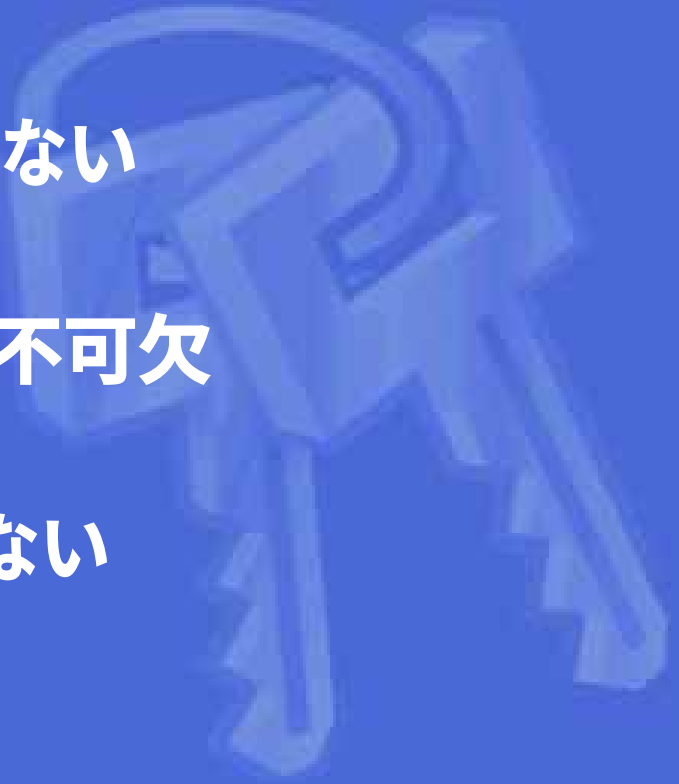
- メーリングリスト
  - Bugtraq（SecurityFocusサイト参照）
- セキュリティポータルサイト
  - SecurityFocus、CERT/CC
- ベンダーが提供するセキュリティ情報
  - 修正パッチのインストール
- セキュリティコンサルティング企業
  - SAIC（http://www.saic.com/）
- ***情報ソースとなるWebサイト***

情報ソースとなるWebサイト

セキュリティ全般情報サイト	
SecurityFocus	http://www.securityfocus.com/
CERT/CC	http://www.cert.org/
各種OS、アプリケーションセキュリティ情報サイト	
Red Hat Linux	http://www.redhat.com/support/errata/ http://www.jp.redhat.com/support/errata/
Microsoft	http://www.microsoft.com/technet/security/current.asp http://www.microsoft.com/japan/technet/security/current.asp
その他セキュリティ関連サイト	
Georgi Guninski Security Reseach	http://www.guninski.com/
Port139	http://www.port139.co.jp/

最後に

- まとめ
  - パフォーマンスやアベイラビリティだけでなく、セキュリティも
  - 導入しただけでは万全と言えない
  - セキュリティ設定や要塞化が不可欠
  - 適切な運用を怠れば意味がない



End