

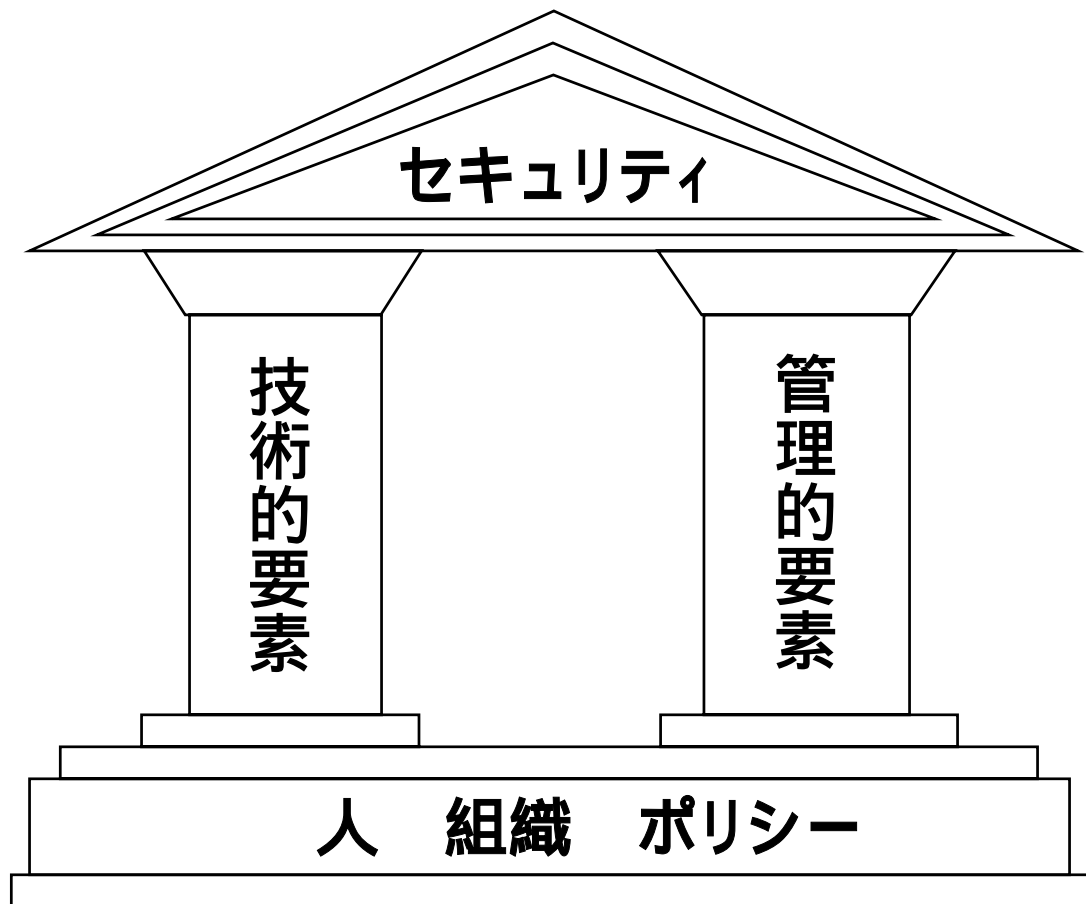
コンピュータシステムの 実践的不正アクセス対策 (50分)

2001/11/02

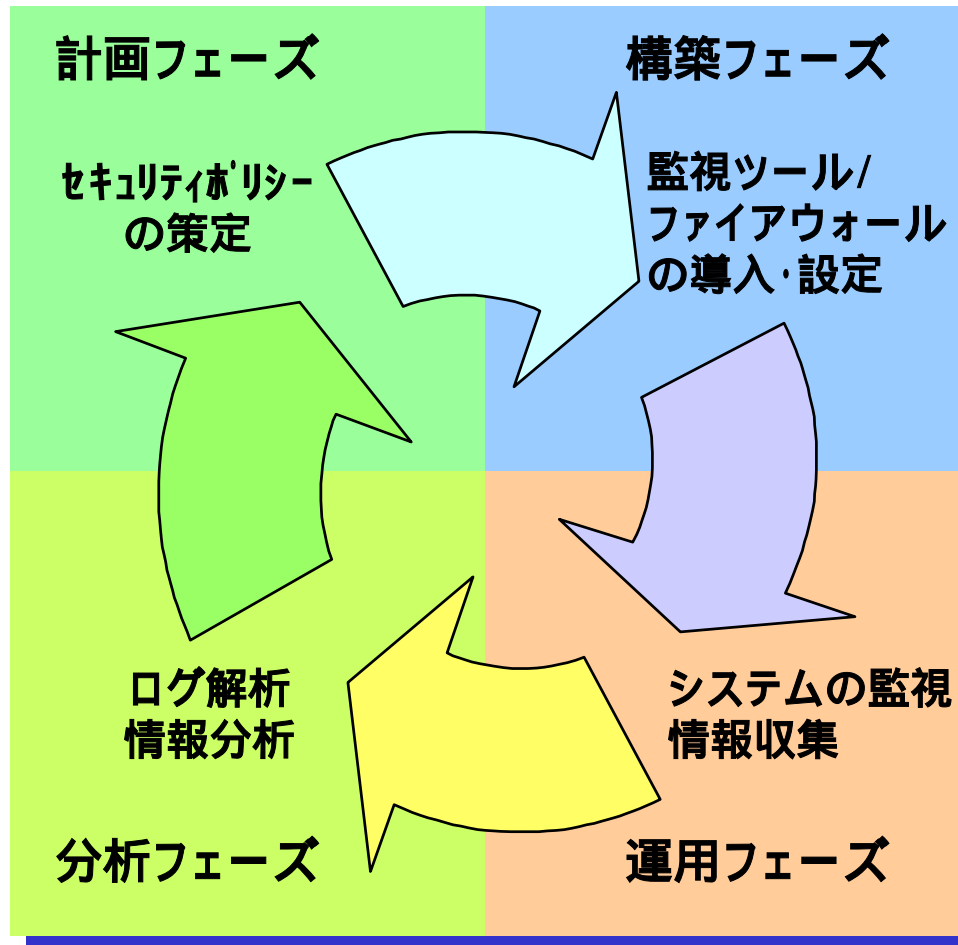
情報処理振興事業協会 セキュリティセンター

セキュリティ対策の基本的考え方

技術的な対策と管理的な対策の両方が必要

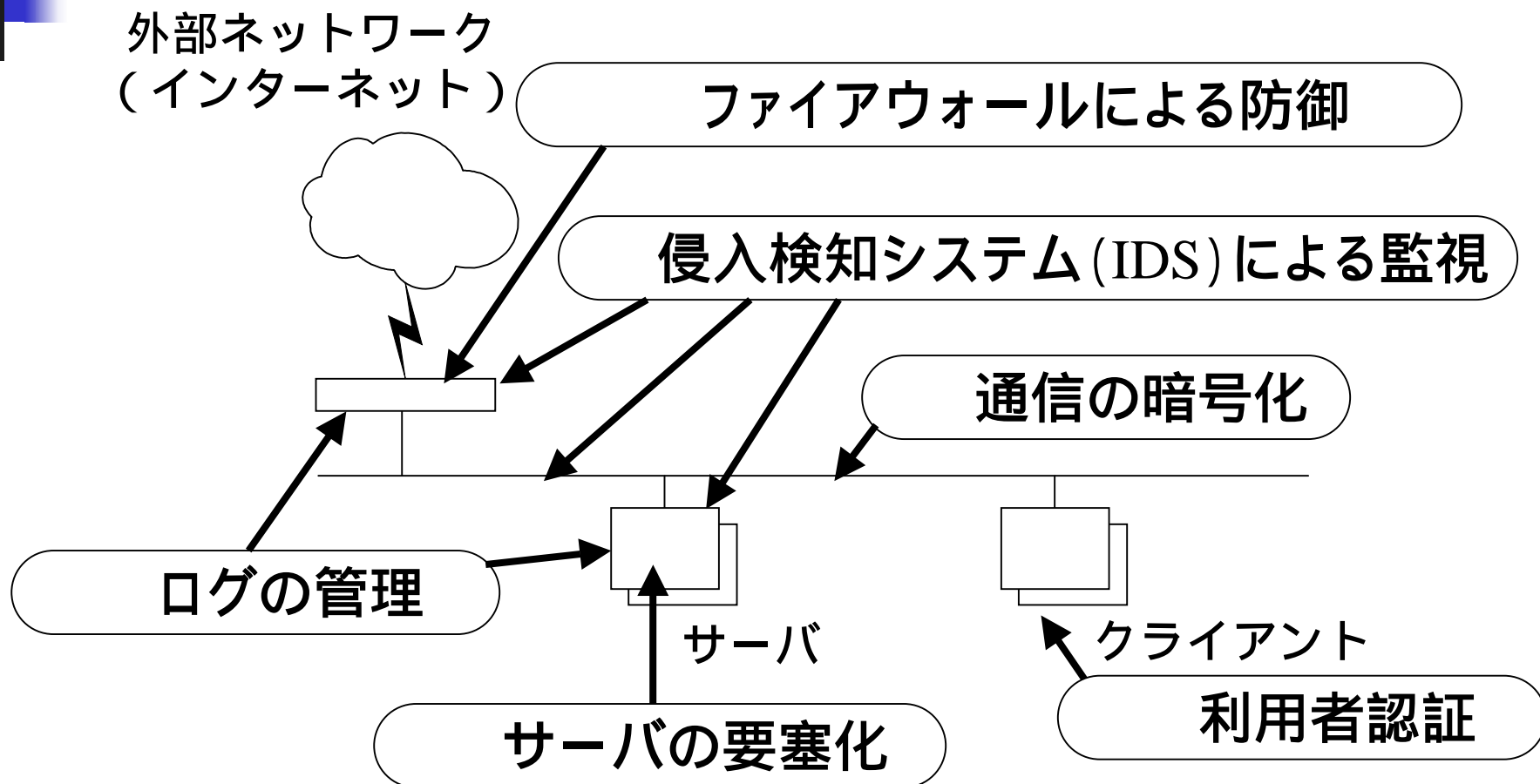


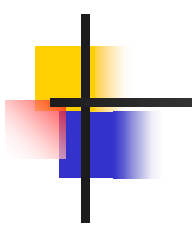
セキュリティ管理サイクル



継続的な改善 = セキュリティの維持

技術的な対策

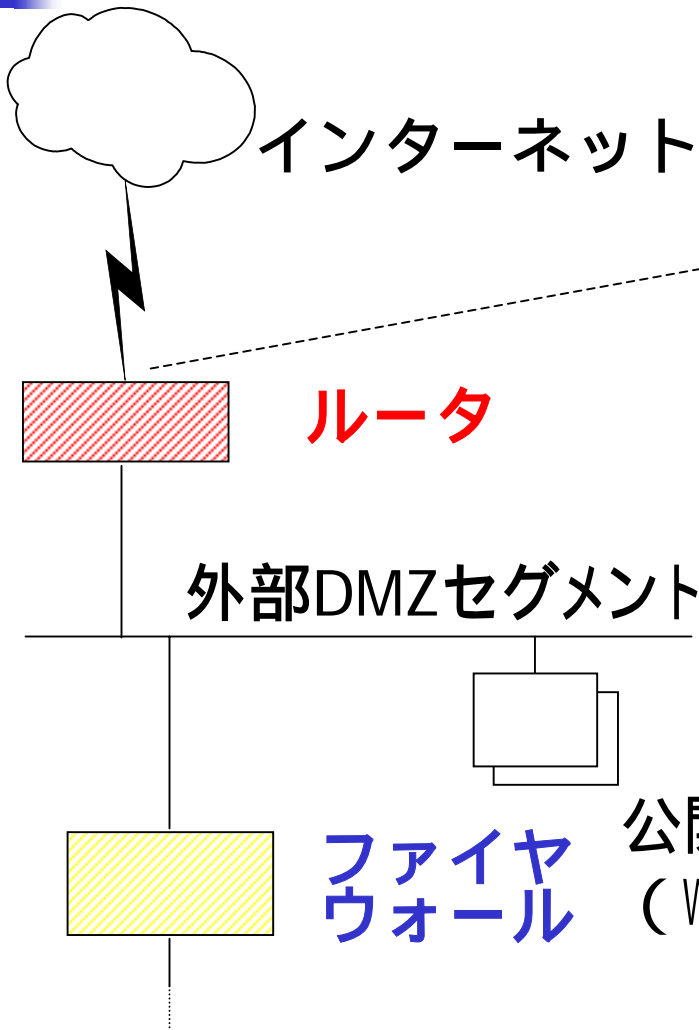




技術的な対策 ファイアウォール による防御

- パケットフィルタ
不要・不正なパケットをまず遮断する
- ファイアウォール
セグメントに分離しアクセス制御をする
- プロキシサーバー
通信の間に入ってクライアントを守る

パケットフィルタ



内向き通過を禁止すべきパケット

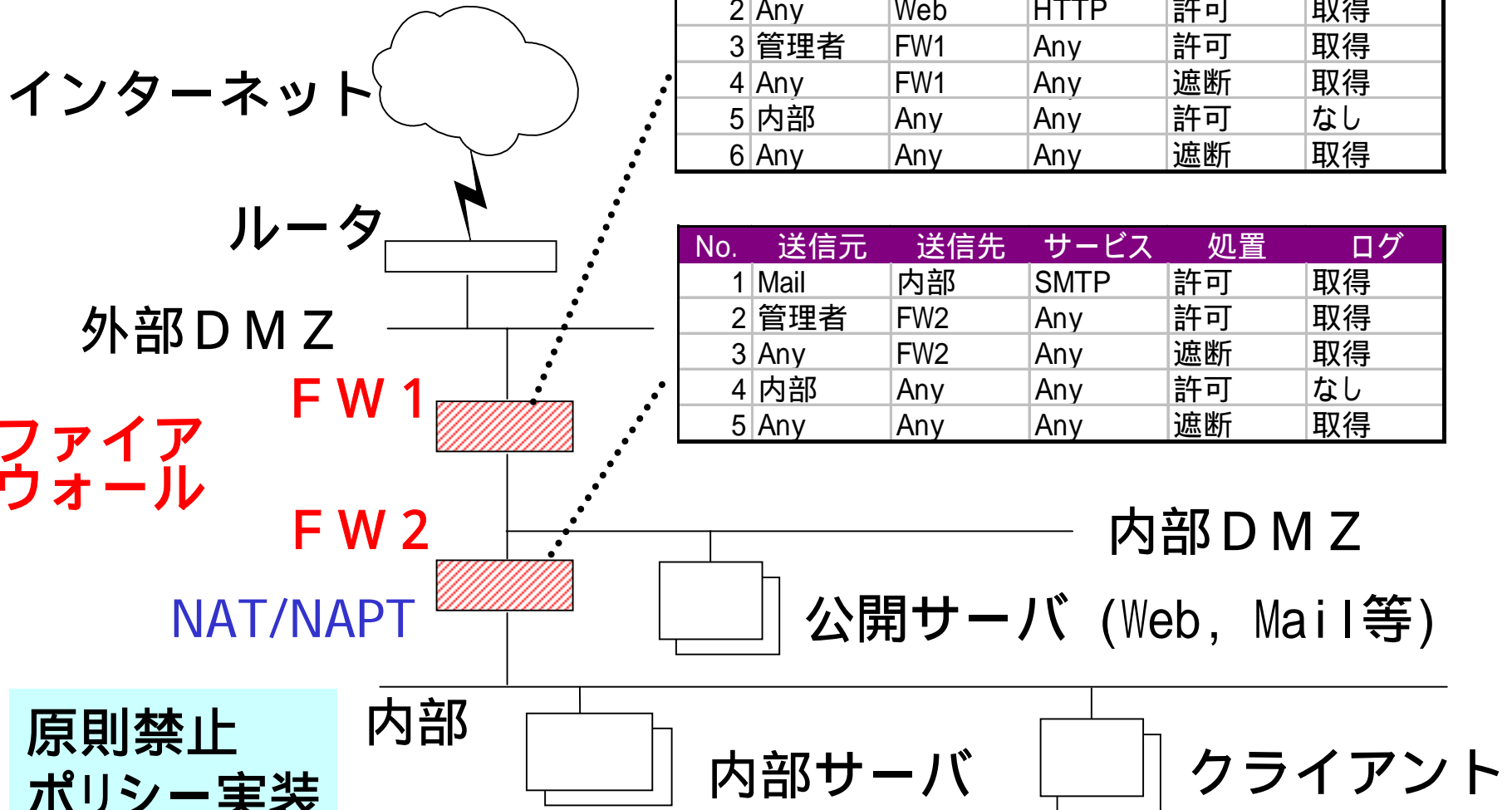
送信元IP	送信元Port	送信先IP	送信先Port
Any	Any	ルータ自身	Any
DMZ	Any	Any	Any
RFC1918	Any	Any	Any
127.0.0.1	Any	Any	Any
0.0.0.0	Any	Any	Any
Any	Any	Any	ICMP
Any	Any	Any	SNMP

- ・ソースルートパケット
- ・ディレクテッドブロードキャストパケット

**原則禁止
必要なものだけ許可**

公開サーバ
(Web, Mail等)

ファイアウォール

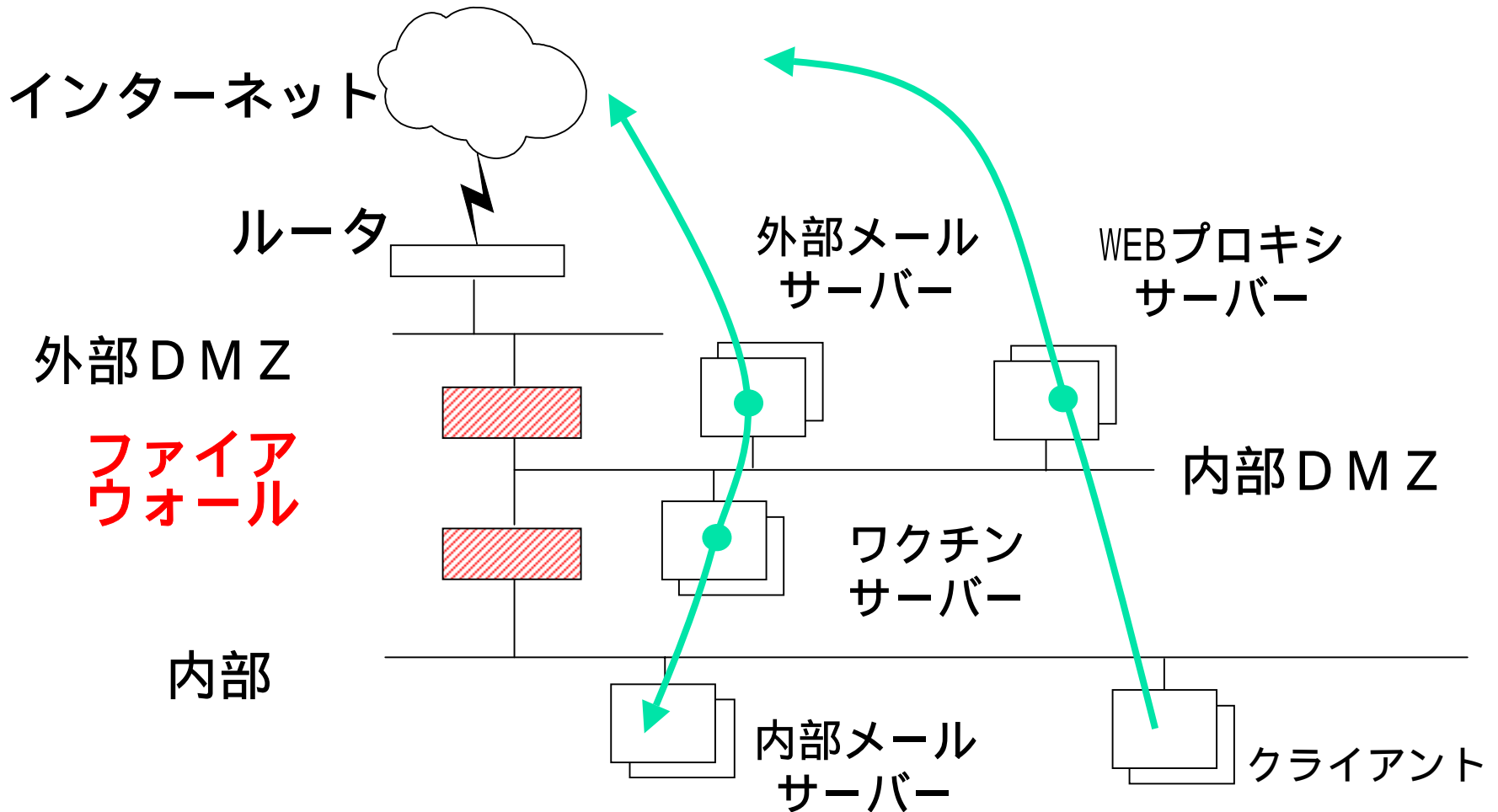


No.	送信元	送信先	サービス	処置	ログ
1	Any	Mail	SMTP	許可	取得
2	Any	Web	HTTP	許可	取得
3	管理者	FW1	Any	許可	取得
4	Any	FW1	Any	遮断	取得
5	内部	Any	Any	許可	なし
6	Any	Any	Any	遮断	取得

No.	送信元	送信先	サービス	処置	ログ
1	Mail	内部	SMTP	許可	取得
2	管理者	FW2	Any	許可	取得
3	Any	FW2	Any	遮断	取得
4	内部	Any	Any	許可	なし
5	Any	Any	Any	遮断	取得


原則禁止
ポリシー実装

プロキシサーバー



ファイアウォール による防御のまとめ

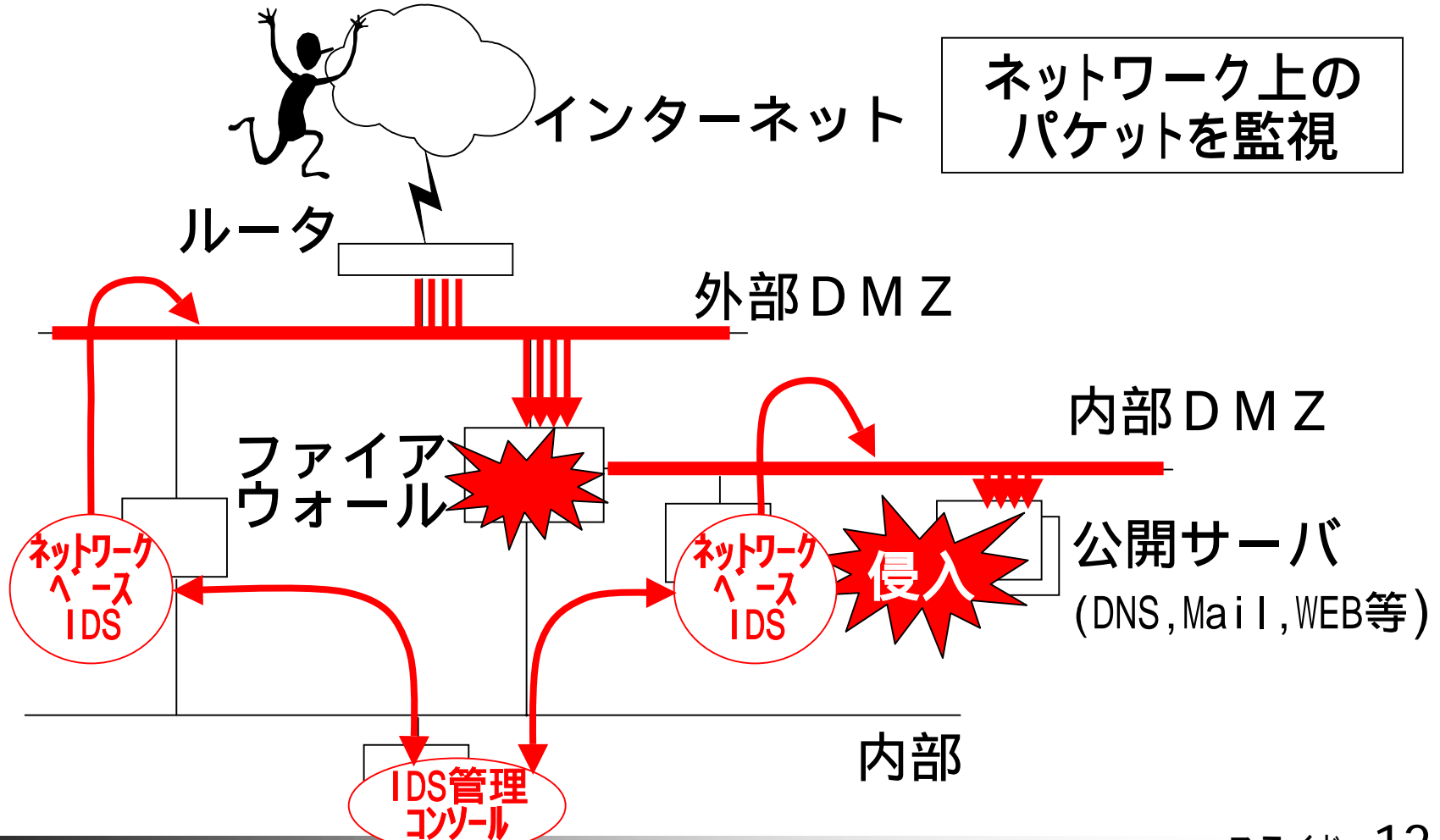
- 不必要なパケットは先に遮断する
- 各ネットワークセグメントの目的に応じてアクセス制御を実現する
- 各ネットワークセグメントの目的に応じてアクセス制御を実現する
- アクセス状況のログを収集する



技術的な対策
侵入検知システム (IDS)
による監視

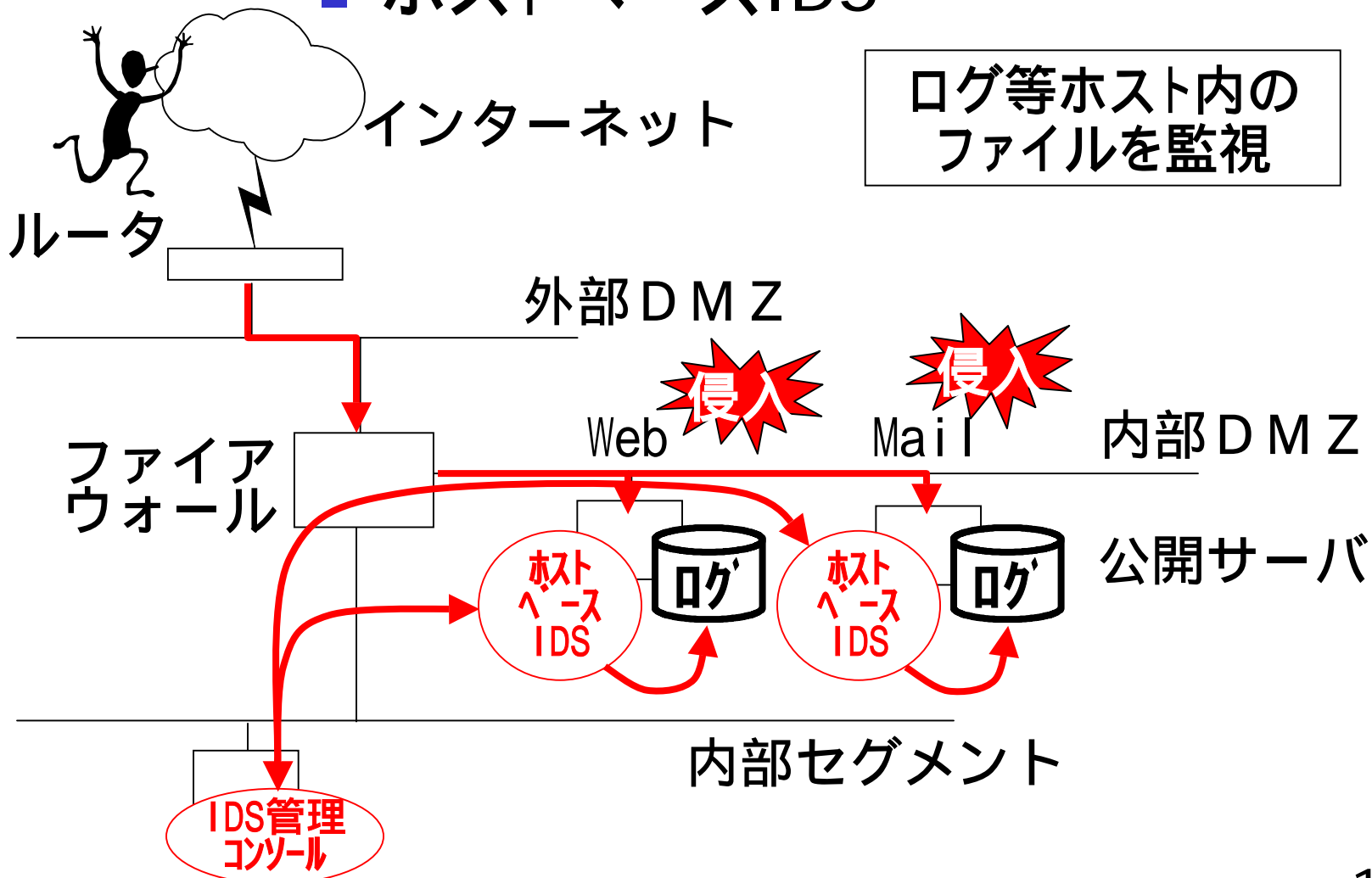
ネットワークベースIDS

■ ネットワークベースIDS



ホストベースIDS

■ ホストベースIDS



■ Misuse Detection (signature-based)

定義済みのパターン(signature)に一致するか否かで検出

利点: 検出効率が良い。誤報が少ない。

欠点: 未知の攻撃を検出できない

■ Anomaly Detection

普通でない異常なイベントを検出

閾値で検出 (例: 1秒間に10回もログインに失敗した)

統計的に異常なイベントを検出

利点: 既知の攻撃パターンなしで検出可能

欠点: 誤報が多い

侵入検知システム (IDS) による監視のまとめ

- 監視したい対象からデータを収集する
- 検出したい情報を求めて収集データを分析する
- 検出内容による応答の選択
- 誤報を排除するなどのチューニング
- 常に最新のシグネチャーに更新



技術的な対策 サーバの要塞化

サーバの要塞化のための手法

運用管理上の対策

セキュアなサービス構成

不要なサービスの停止

TCP/IP のアクセス制御

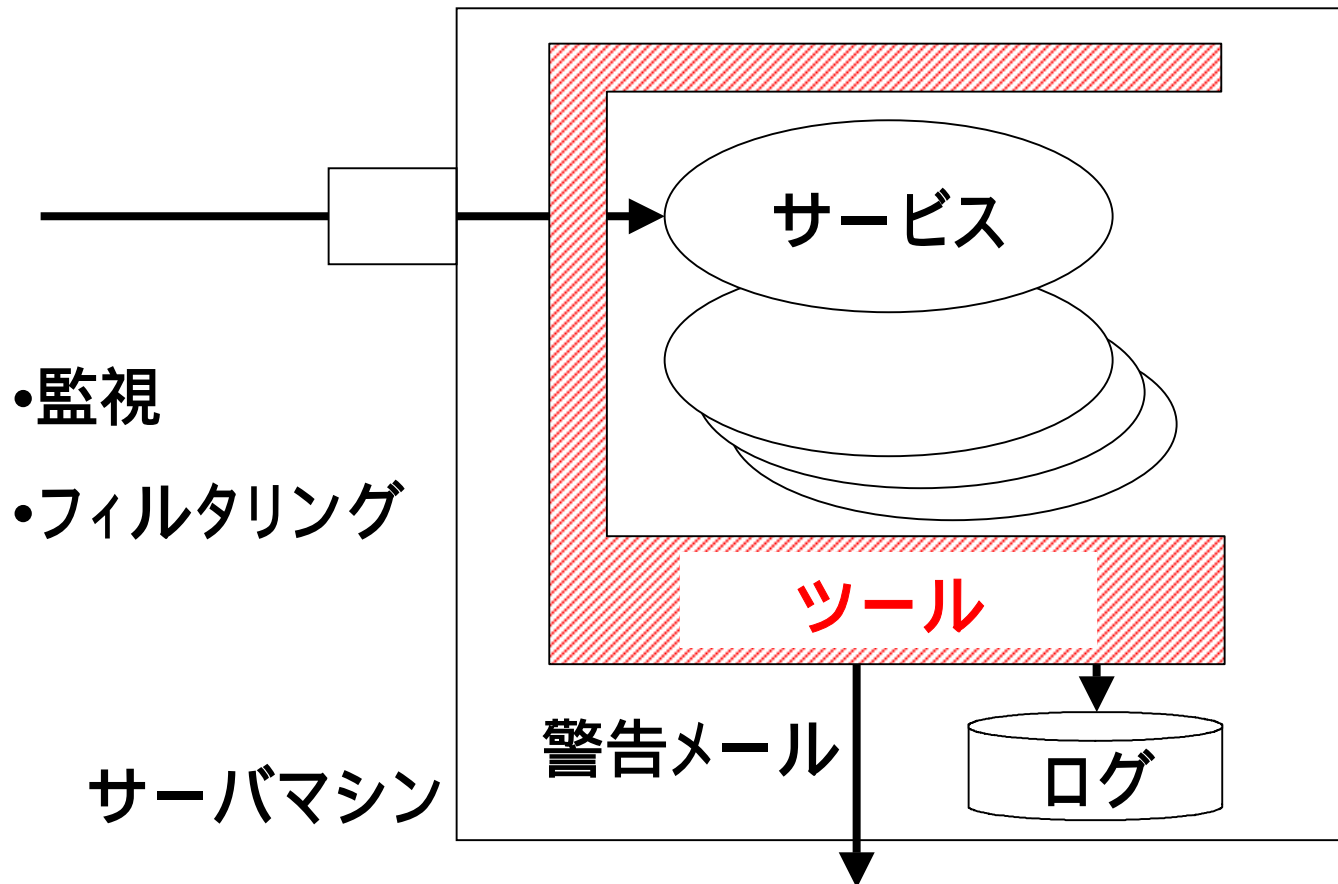
パケットフィルタリング

パケットフィルタリング

- OSレベルでネットワーク接続を制限
- 不正なパケットをフィルター
- フィンガープリントを最小にする

TCP/IP のアクセス制御

外部からのアクセスに対して、相手のIPアドレスによって、アクセスを制御する



不要なサービスの停止

■ 不要なサービスがあれば狙われる

デフォルト設定の見直し

- 提供しているサービスの状況把握

システム管理者が把握しておくべき情報

- 各サイトのセキュリティポリシーの実装

導入時設定では最大限利用可能な状態

- 潜在的脆弱性の脅威の低減

セキュアなサービスの構成

■ 共通

- 一般ユーザーで実行
- chroot で実行

■ DNS

- ゾーン転送の制限

■ Mail

- メール転送の制限
- qmail, Postfix などの検討

■ WWW

- 不要なモジュール/CGI/ISAPI 拡張 の削除

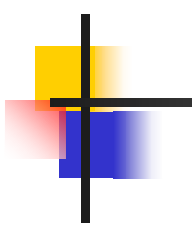
運用管理上の対策

- 完全性保護対策
- バックアップ
- ログインの制限
- 最新版/パッチの適用
- 脆弱性情報などのセキュリティ情報の収集



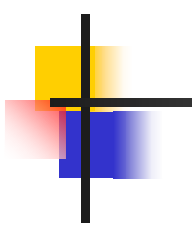
技術的な対策 通信の暗号化

- SSH (SecureShell)
 - コマンドに対しセキュリティを強化するプロトコル
 - 特定のアプリケーションでの暗号化
- VPN (Virtual Private Network)
 - 仮想的な専用線としてのネットワーク
 - アプリケーションの変更が不必要
 - IPsec で相互接続

A decorative graphic in the top-left corner consisting of a vertical black line and a horizontal grey line, with overlapping yellow, red, and blue squares.

技術的な対策 利用者の認証

- パスワードシステムの改善
 - ワンタイムパスワード
 - 一度しか有効ではない、使い捨て形式のパスワードによる利用者の正当性の確認(S/Key, SecureID等)
 - バイオメトリックス
 - 指紋、虹彩など生体計測技術による利用者の正当性の確認
- PKIを利用しての本人認証
 - ICカード

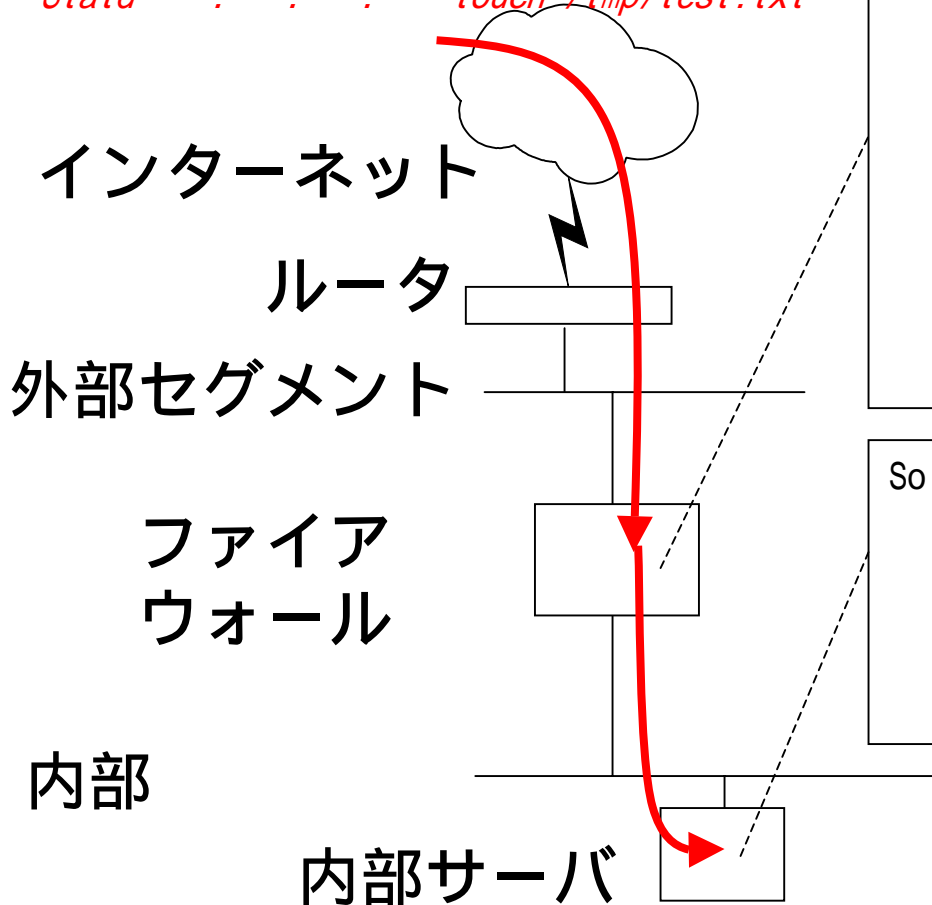
A decorative graphic in the top-left corner consisting of a vertical black line and a horizontal grey line, with overlapping yellow, red, and blue squares.

技術的な対策 ログの管理

- 必要な情報を収集することができるようにログ出力を設定する
- ツールを利用して分析する
- ログを安全に保管する
- 詳細な監査ログ
- 時計の同期 (照合のため)
- DoS 対策 (log 攻撃)

■ FirewallとUNIX

*Statd ***.***.***.*** touch /tmp/test.txt*



FireWall-1

```
10:57:11 accept firewall-1 >SMCPWR111 proto
udp src 192.168.10.1 dst ultra7.xxx.co.jp
service sunrpc s_port 772 len 84 rule 1
```

```
10:57:11 accept firewall-1 >SMCPWR111 proto
udp src 192.168.10.1 dst ultra7.xxx.co.jp
service 32808 s_port 773 len 1140 rule 1
```

Solaris: message

```
Jun 29 10:57:11 ultra7 statd[122]: statd:
pathname too long: /var/statmon/sm/<^1
FF>OGuG~OGuG~OGuFPV6;P.ahm.rg,bsntbg.slo.sdrs-
SWS
```

- 既知の不正アクセス対策を確実に実施
- ポリシーに基づいてセキュリティ機能を実装
- 継続的な改善によりセキュリティを維持
- 多段階での防御をする
- 防御、検知、リアクション

情報処理振興事業協会 セキュリティセンター (IPA/ISEC)

〒113-6591

東京都文京区本駒込2 - 28 - 8

文京グリーンコートセンターオフィス16階

TEL 03(5978)7508 FAX 03(5978)7518

ウイルス/不正アクセス相談110番 TEL 03(5978)7509

電子メール virus@ipa.go.jp crack@ipa.go.jp

URL <http://www.ipa.go.jp/security/>