

コンピュータ不正アクセスの現状

IPA 情報処理振興事業協会
セキュリティセンター

内容

不正アクセス被害とその影響

不正アクセスの分類

不正アクセス被害の動向と対策

不正アクセス被害とその影響

不正アクセスとは何か

一般的な概念

システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと。

「コンピュータ不正アクセス対策基準」(平成8年8月8日付け通商産業省告示第362号)

<http://www.miti.go.jp/past/c60806a2.html>

法的な定義

参照：不正アクセス行為の禁止等に関する法律

<http://www.miti.go.jp/kohosys/topics/10000098/esecu02j.pdf>

http://www.mpt.go.jp/top/access_law/law.html

http://www.npa.go.jp/hightech/fusei_ac2/houann.htm

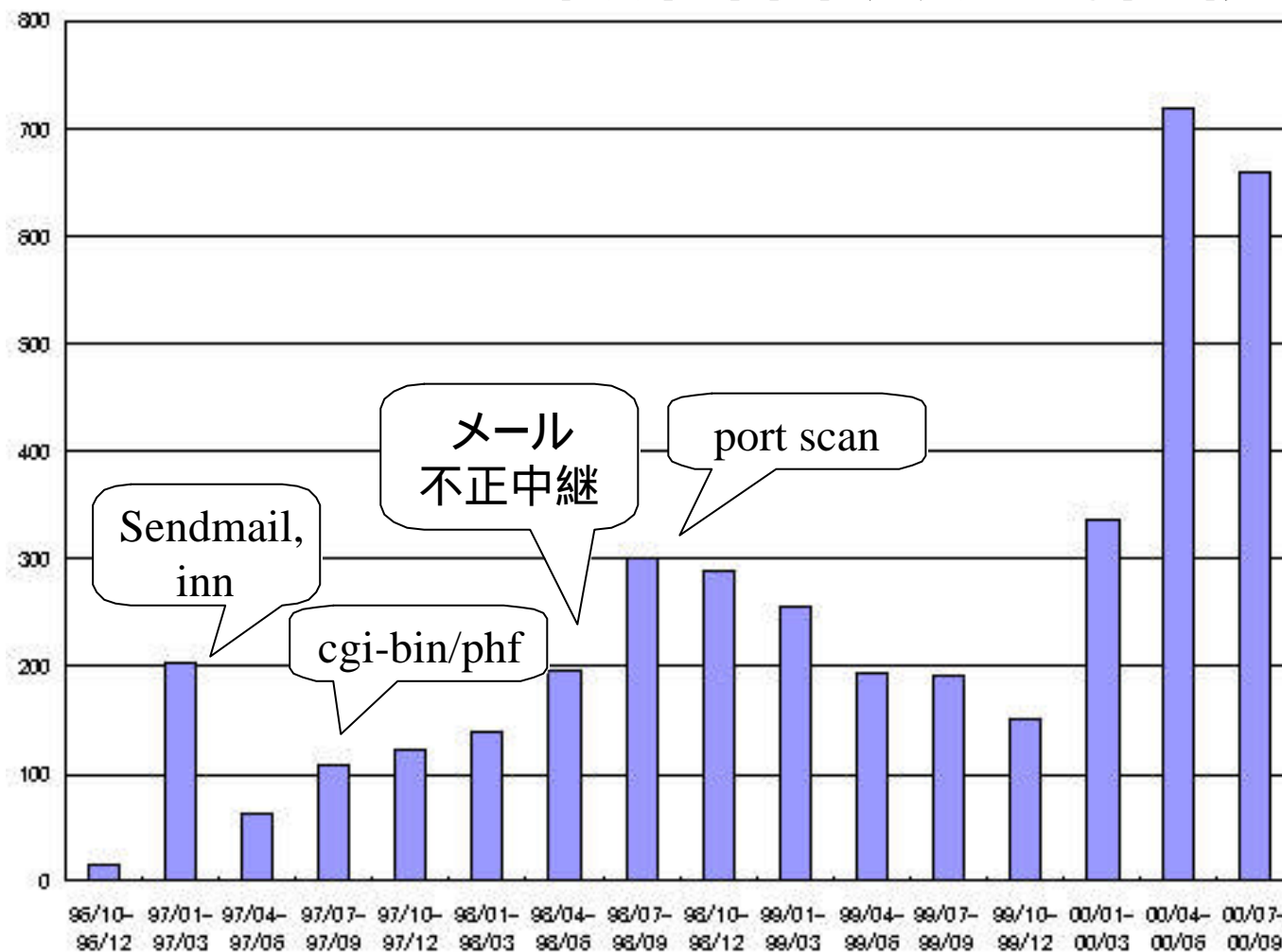
インシデントとは何か

(インターネットに接続された)システムの運用に際して、セキュリティ上の問題として捉えられる事象

「技術メモ - コンピュータセキュリティインシデントへの対応」(発行日：2000-08-25)

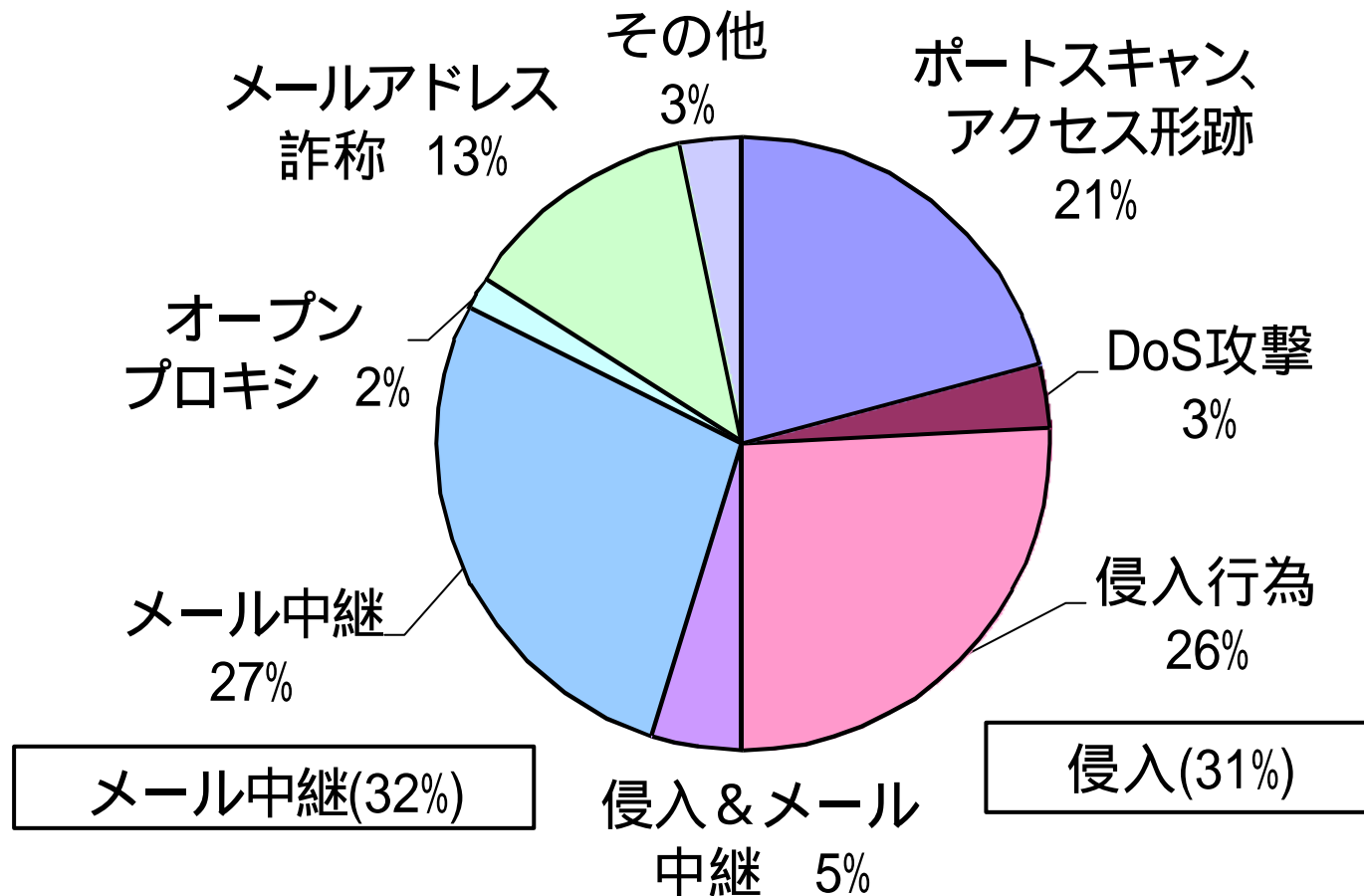
<http://www.jpccert.or.jp/ed/2000/ed000007.txt>

JPCERT/CCが受け付けた インシデント報告件数の推移



<http://www.jpcert.or.jp/stat/reports.html>

IPAが受け付けた被害内容の分類

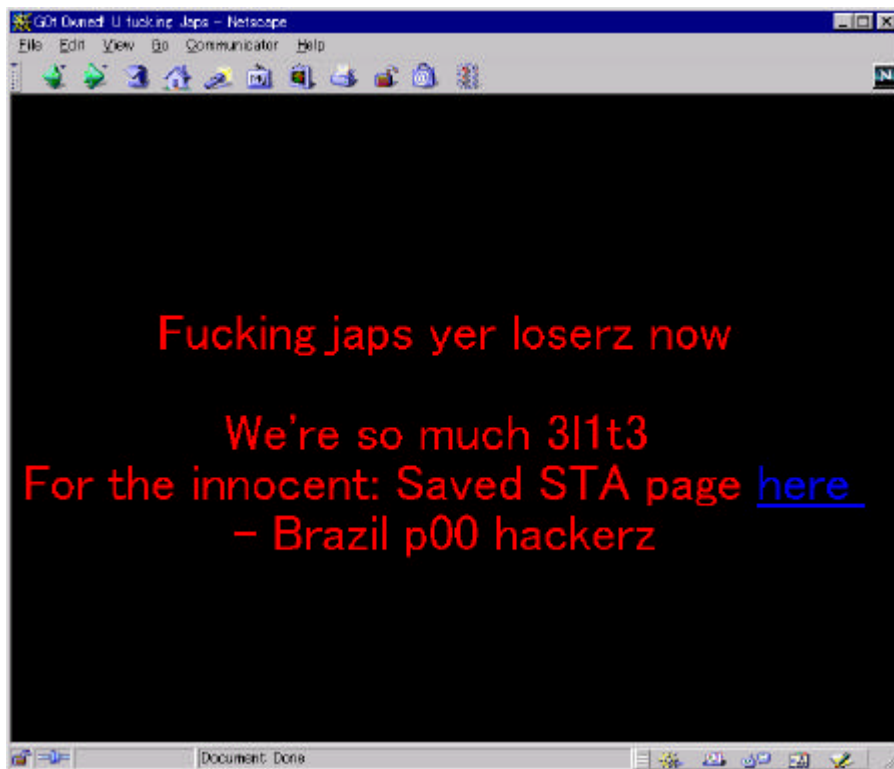


IPAへの不正アクセス被害届出件数(2000年上半期:1~6月)

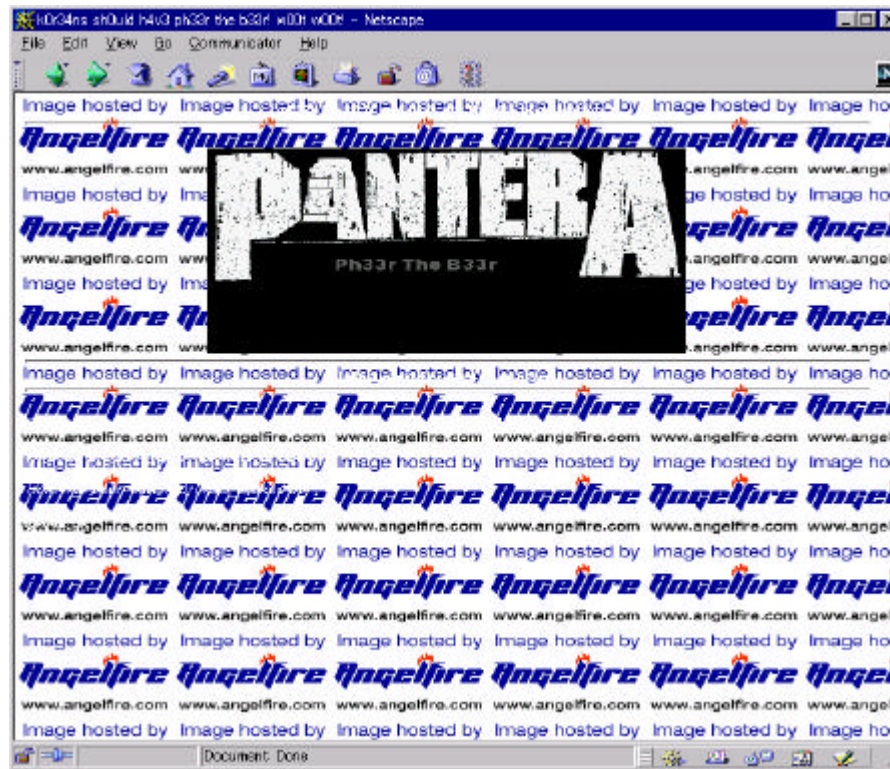
<http://www.ipa.go.jp/security/ciadr/txt/list.html>

Web改ざんの事例

2000年1月24日 官公庁において
改ざんされたWebページ



2000年3月22日 銀行において
改ざんされたWebページ



<http://www.attrition.org/mirror/attrition/>

ユーザID/パスワード流出の事例

大学LANへの侵入による
ユーザID/パスワードの流出

1999年1月28日 産経新聞

北海道教育大にハッカー侵入
学生らのID盗難
LAN停止

北海道教育大の学生らに、ハッカーが侵入し、学生らのIDやパスワードを盗み出した。盗み出したIDやパスワードは、インターネット上で公開された。盗み出したIDやパスワードは、インターネット上で公開された。盗み出したIDやパスワードは、インターネット上で公開された。

北海道教育大の学生らに、ハッカーが侵入し、学生らのIDやパスワードを盗み出した。盗み出したIDやパスワードは、インターネット上で公開された。盗み出したIDやパスワードは、インターネット上で公開された。

不正アクセス被害による影響

外部から
クラッカー、産業スパイ、元従業員など

内部から
従業員、クラッカーなど

不正アクセス被害

物理的な被害

経済的な損失

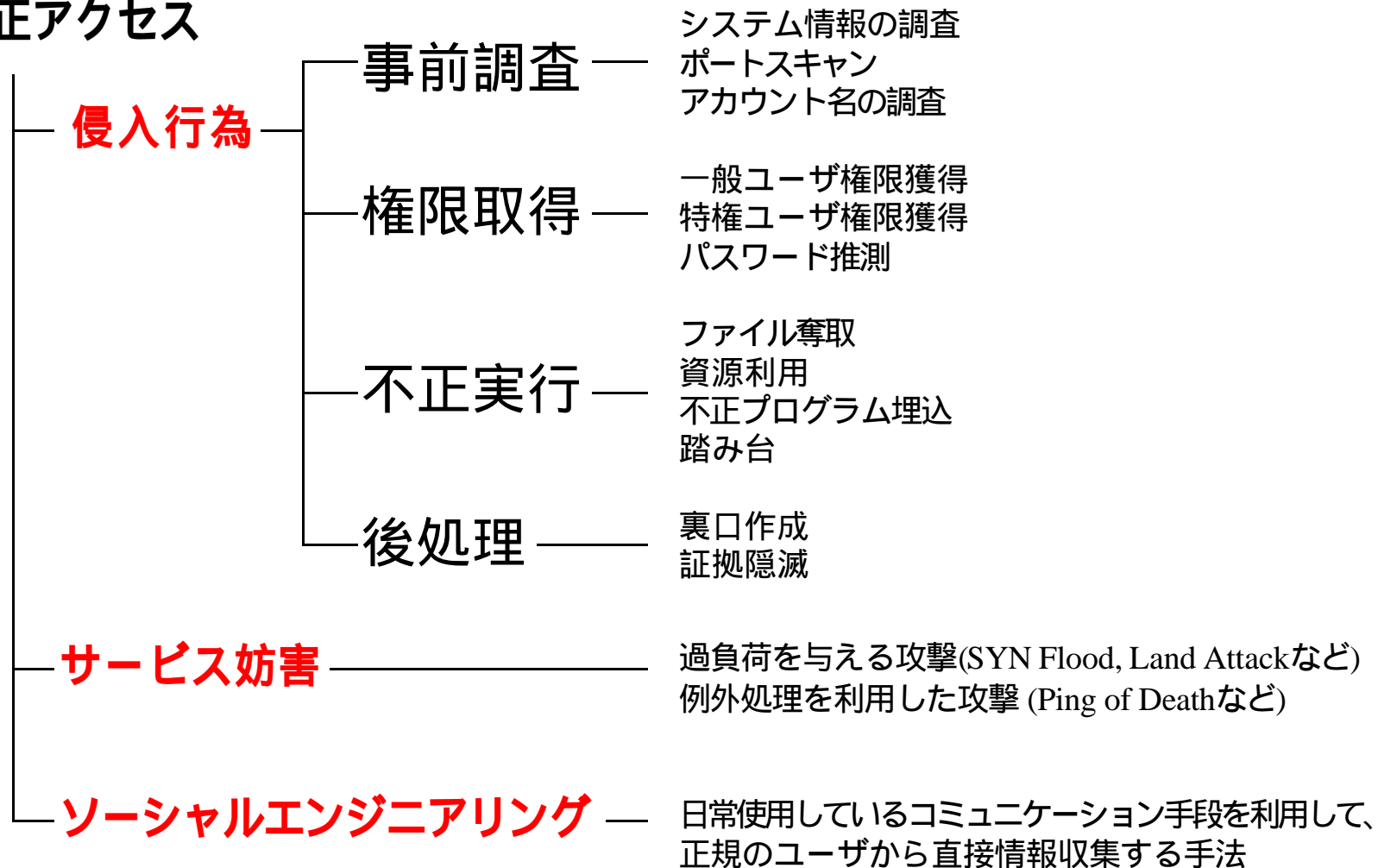
社会的な信頼の喪失

大きな代償

不正アクセスの分類

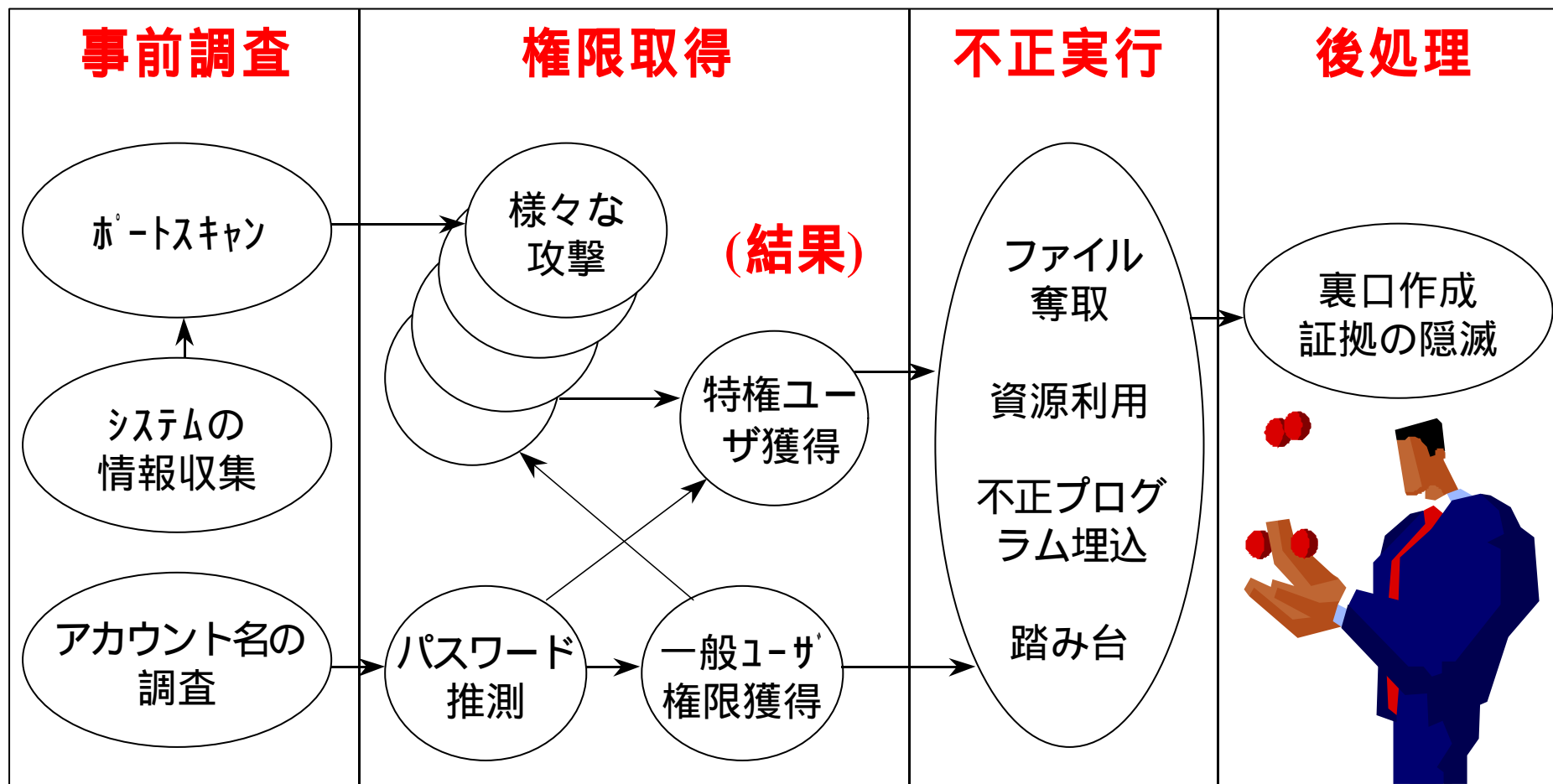
不正アクセスの分類

不正アクセス



侵入行為

一般的な侵入行為の流れ



サービス妨害攻撃

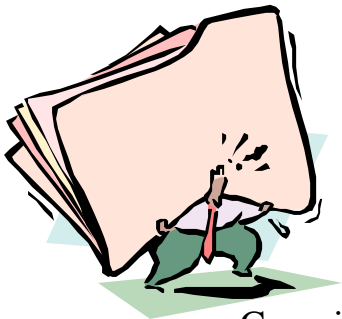
サービス妨害攻撃: DoS(Denial of Service)

過負荷を与える攻撃

標的マシンに対して過大の負荷を与え、パフォーマンスを低下させる。(SYN Flood Land Attackなど)

例外処理を利用した攻撃

標的マシンに対して実行不可能な例外処理を要求し、機能を停止または低下させる。(Ping-of-Deathなど)



ソーシャル・エンジニアリング

日常使用しているコミュニケーション手段を利用して、正規のユーザから直接情報収集する手法。

ほとんどは電話で行われる

- システム管理者になりすまし
「システムに異常があった。」「メンテナンス中である。」
- 初心者ユーザになりすまし
「ログインできない。」「パスワードを忘れた。」
- 他部署の上司になりすまし
「社長だが、」「急いでシステムにアクセスする必要がある。」

不正アクセス被害の動向と対策

不正アクセス増加の要因

- エンドユーザの増加
- 利用するシステム技術の急速な変化
- セキュリティ対策費の不足
- インターネットの利便性
- 攻撃手法の情報が容易に入手可能であること

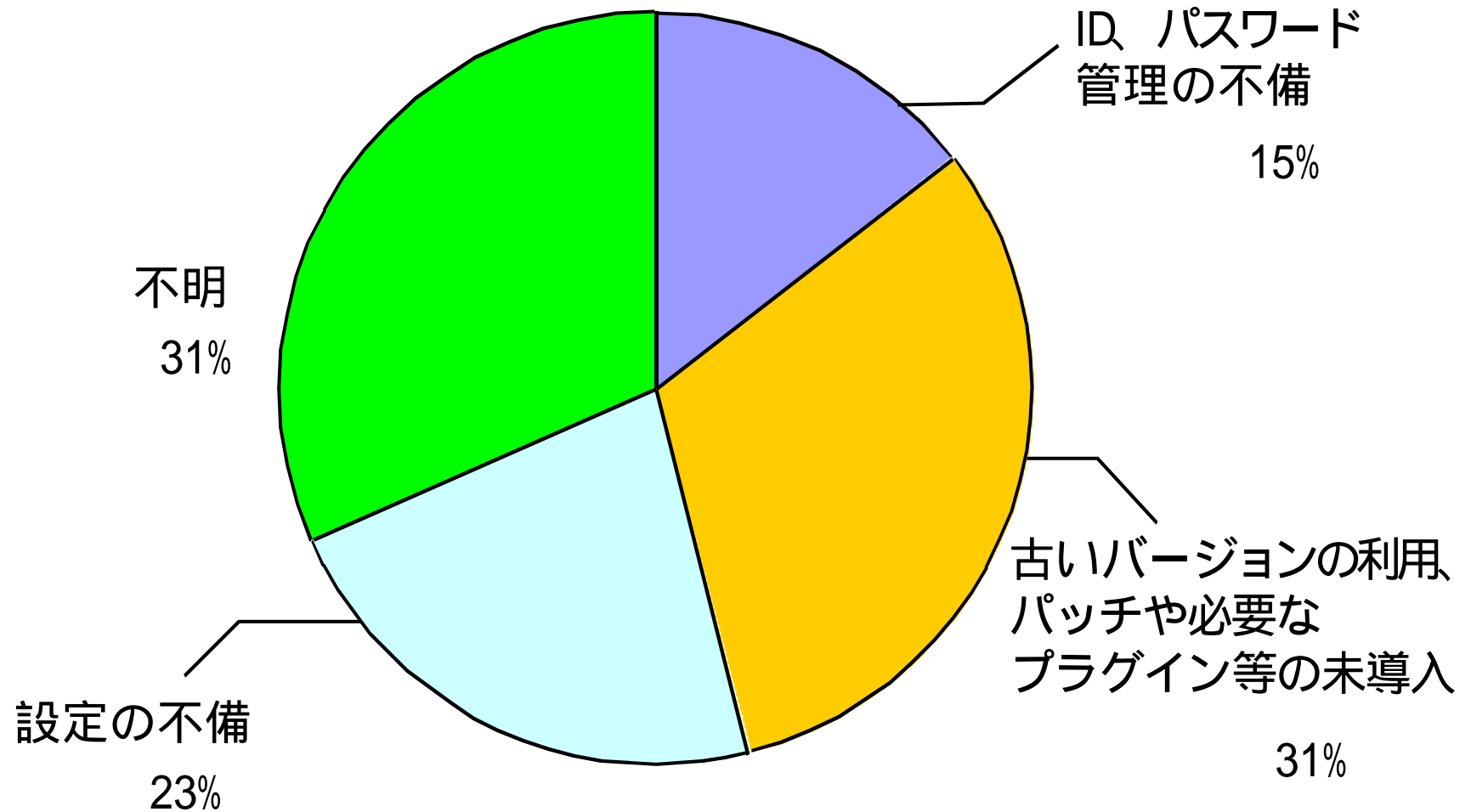
狙われるネットワークサービス

- BINDの弱点
- CGIプログラムの脆弱性
- Remote Procedure Call(RPC)の弱点
- IISにおけるRemote Data Service(RDS)のセキュリティホール
- Sendmailにおけるバッファオーバーフローの弱点
- saminとmountdによるリモートアクセスの問題
- NetBIOSとWindowsNTのポート135 ~ 139(Windows2000では445)によるファイルまたは情報の共有の問題
- ユーザーIDの問題(特にパスワード設定無しまたは安易なパスワードの管理者ID)
- IMAPとPOPにおけるバッファオーバーフローの脆弱性と設定ミス
- SNMPのデフォルト設定

SANS, The Ten Most Critical Internet Security Threats

<http://www.sans.org/topten.htm>

IPAが受け付けた被害原因の分類

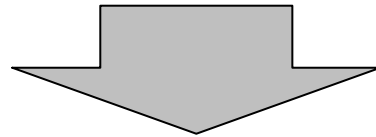


IPAへの不正アクセス被害届出件数(1999年)

http://www.ipa.go.jp/security/crack_report/20000203/99all.htm

現状についてのまとめ

- 不正アクセスは増加している
- 狙われるのは既知の脆弱性である
- 被害原因は初歩的な不備が多い



既に分かっている不正アクセス対策によって多くの被害を未然に防ぐことができる。

コンピュータシステムの 実践的不正アクセス対策

IPA 情報処理振興事業協会
セキュリティセンター

内容

技術的な対策

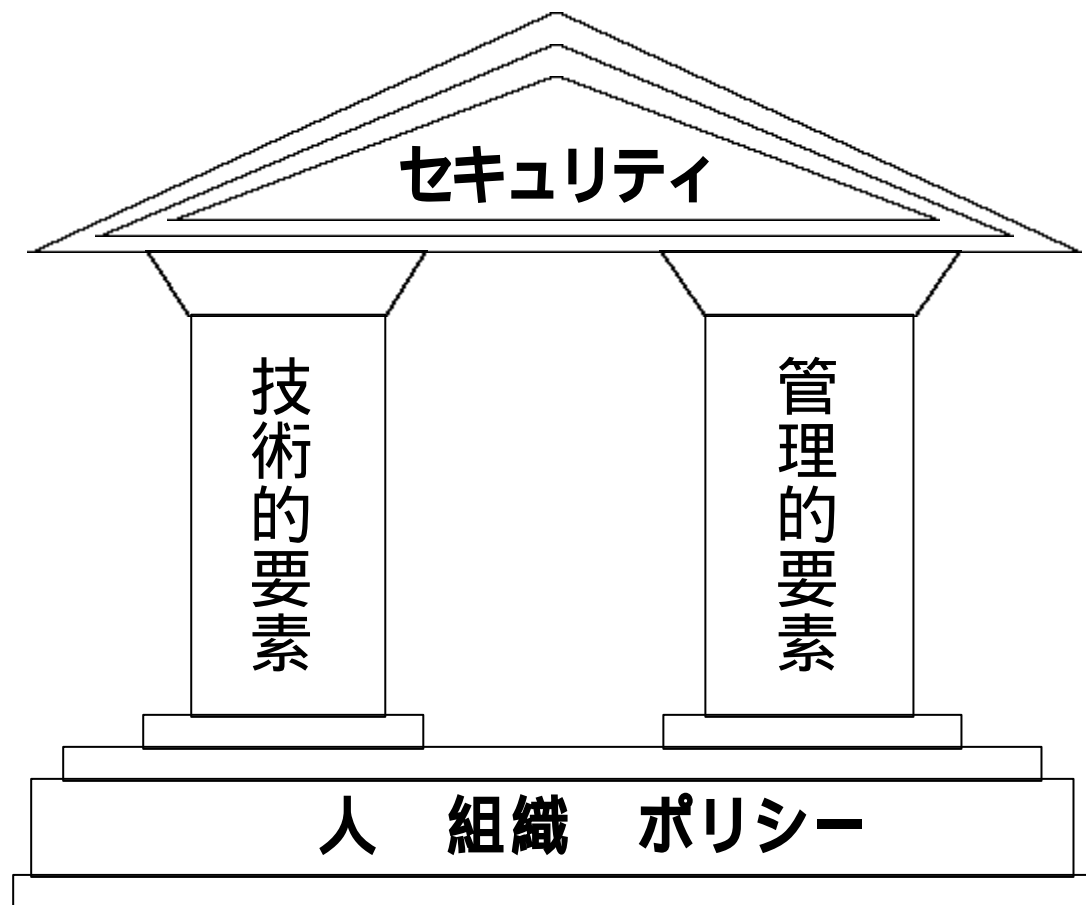
- サーバの要塞化
- 本人認証
- ルータ、ファイアウォールによる防御
- 通信の暗号化
- 侵入検知システム(IDS)による監視
- ログの管理

管理的な対策

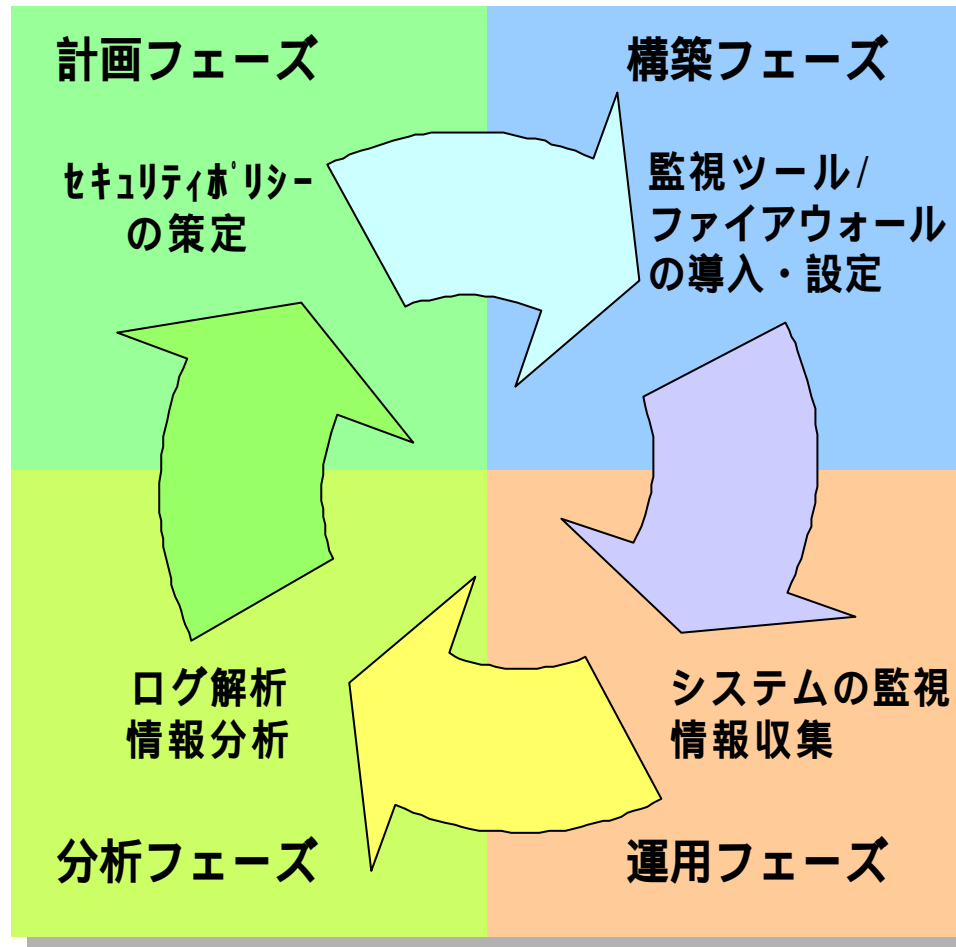
- セキュリティポリシーの適用
- システム構成の管理
- ユーザID/パスワードの管理
- エンドユーザの教育
- セキュリティ監査
- インシデント対応

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



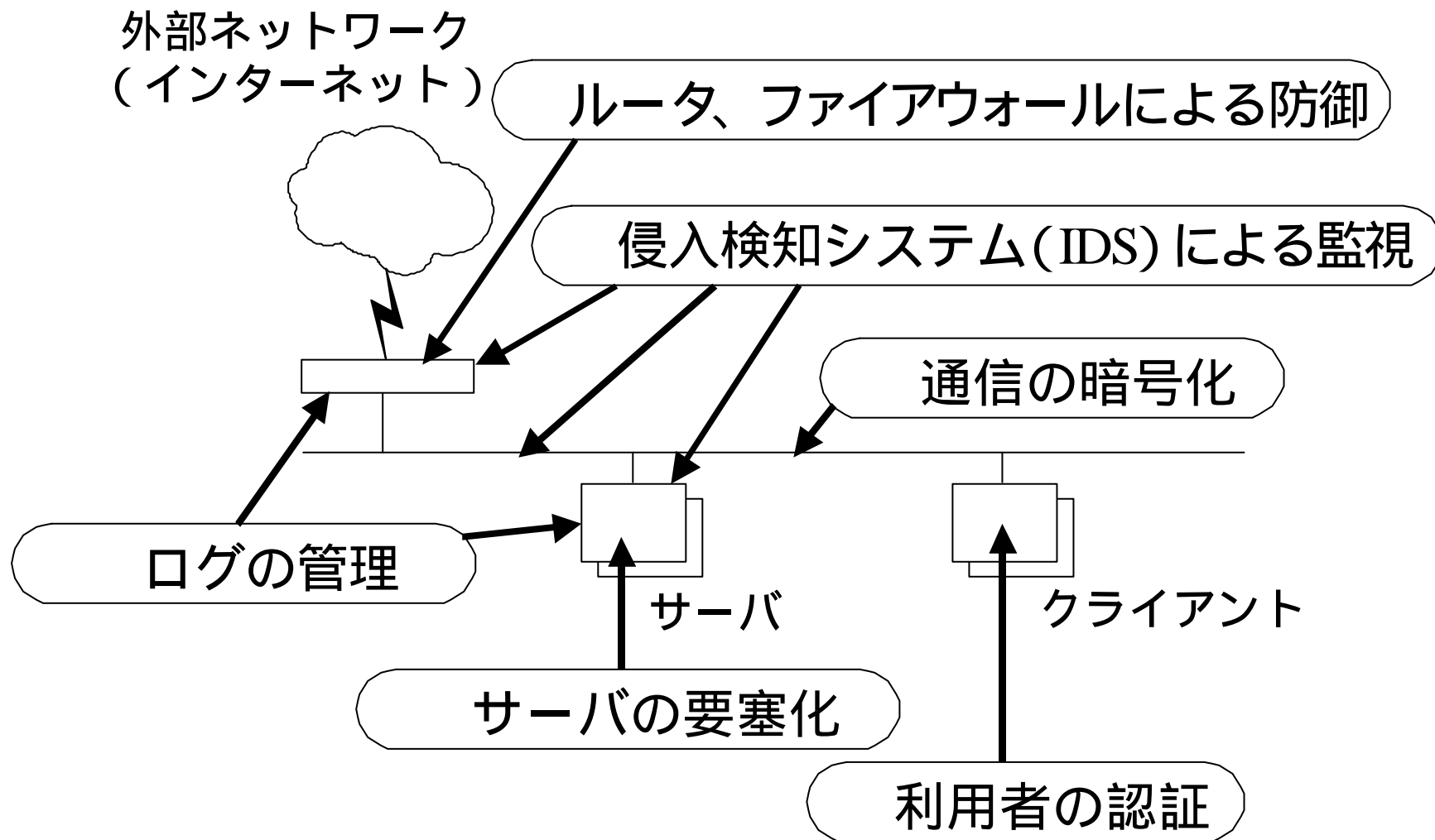
セキュリティ管理サイクル



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



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

- 不要なサービスの停止によって侵害の可能性を軽減する
- TCP/IPのアクセス制御によって他の機器からの不正なアクセスを回避する
- 最新版へのアップグレード、セキュリティパッチの適用によって脆弱性を排除する

不要なサービスの停止

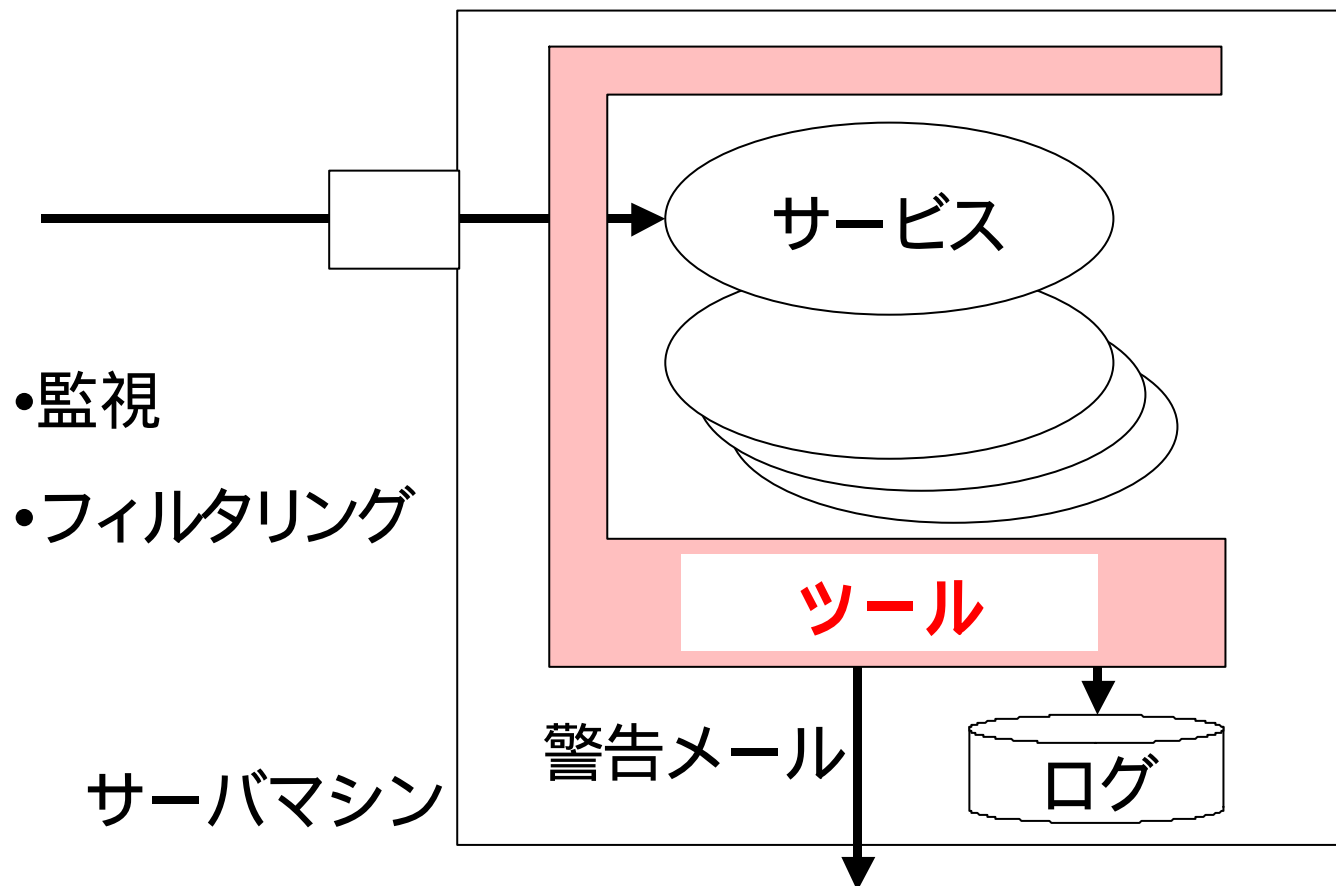
- 不要なサービスがあれば狙われる

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

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



最新版へのアップグレード セキュリティパッチの適用

- セキュリティホールへの対応: パッチ導入
- 設定の拡張性: 最新版への移行
 - セキュリティレベルの向上
 - 設定内容の多様化

脆弱性・対応パッチ等の情報

- **Cert Advisory**
 - <http://www.cert.org/advisories/>
- **JPCERT/CC**
 - <http://www.jpccert.or.jp/>
- **IPA**
 - <http://www.ipa.go.jp/security/>
- **製品提供元のサポートサービス**
 - Web、定期的なメールを利用した公開情報
- **脆弱性・攻撃に係わる情報源**
 - セキュリティ対策関連のメールサービス

技術的な対策 利用者の認証

利用者の認証のための手法

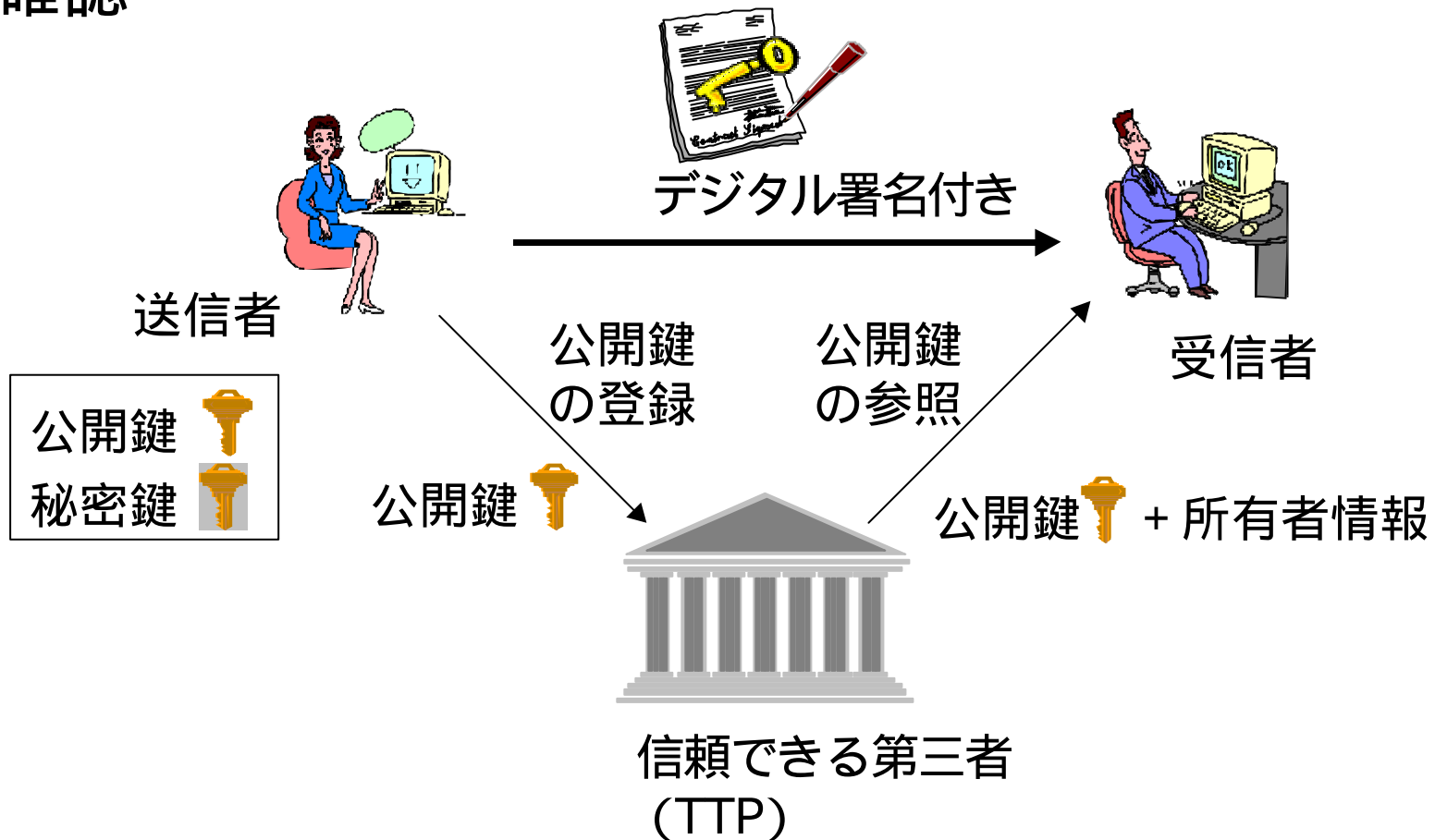
- パスワードシステムを改善するシステム技術を導入する
- PKIを利用して本人認証するシステムを構築する

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
 - ソフトウェアによる実装 (S/Key)
 - ハードウェアによる実装 (SecureID)
- 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

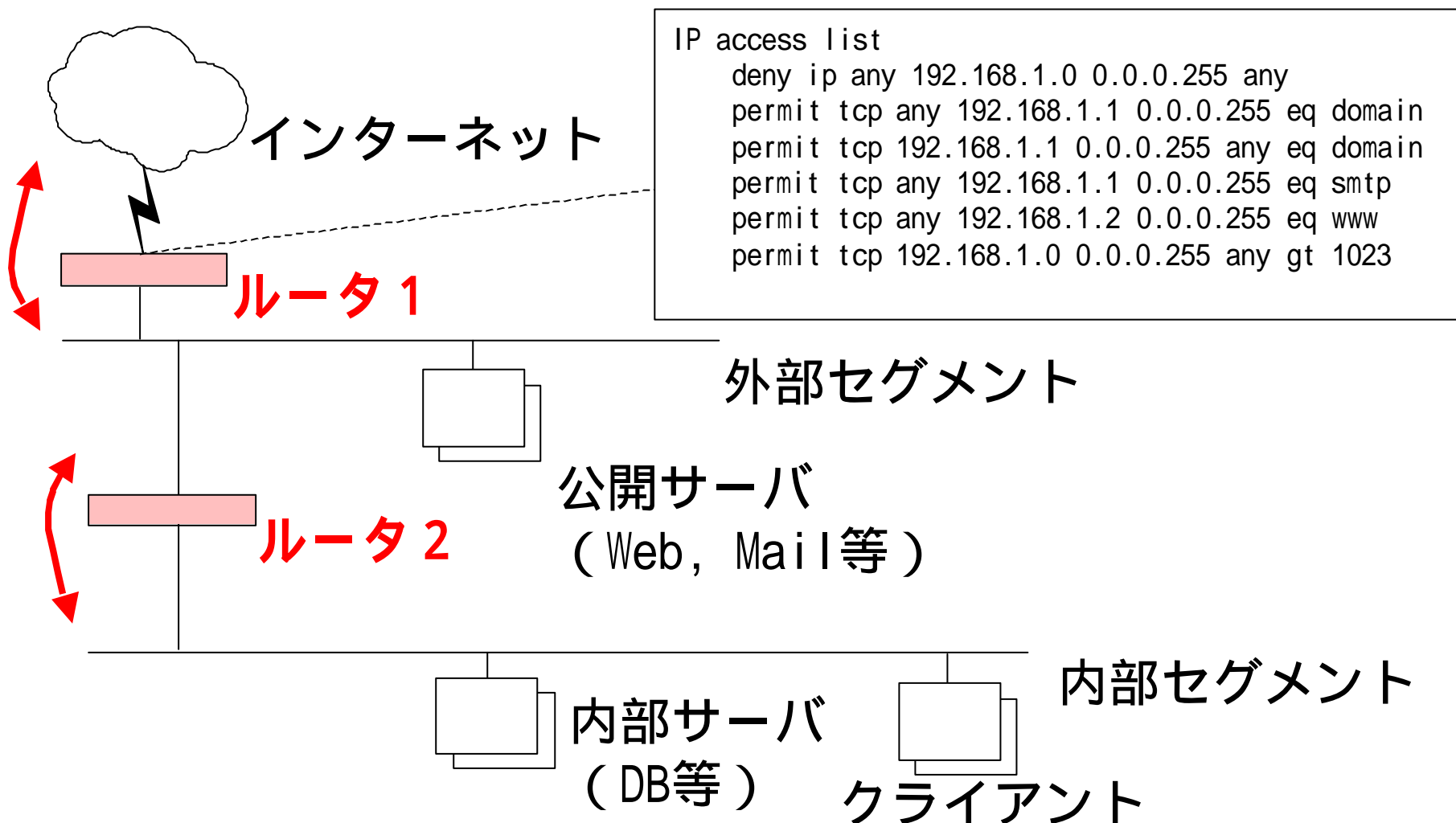
PKIを利用した本人認証

公開鍵証明書とデジタル署名による利用者の正当性の確認



技術的な対策
ルータ、ファイアウォール
による防御

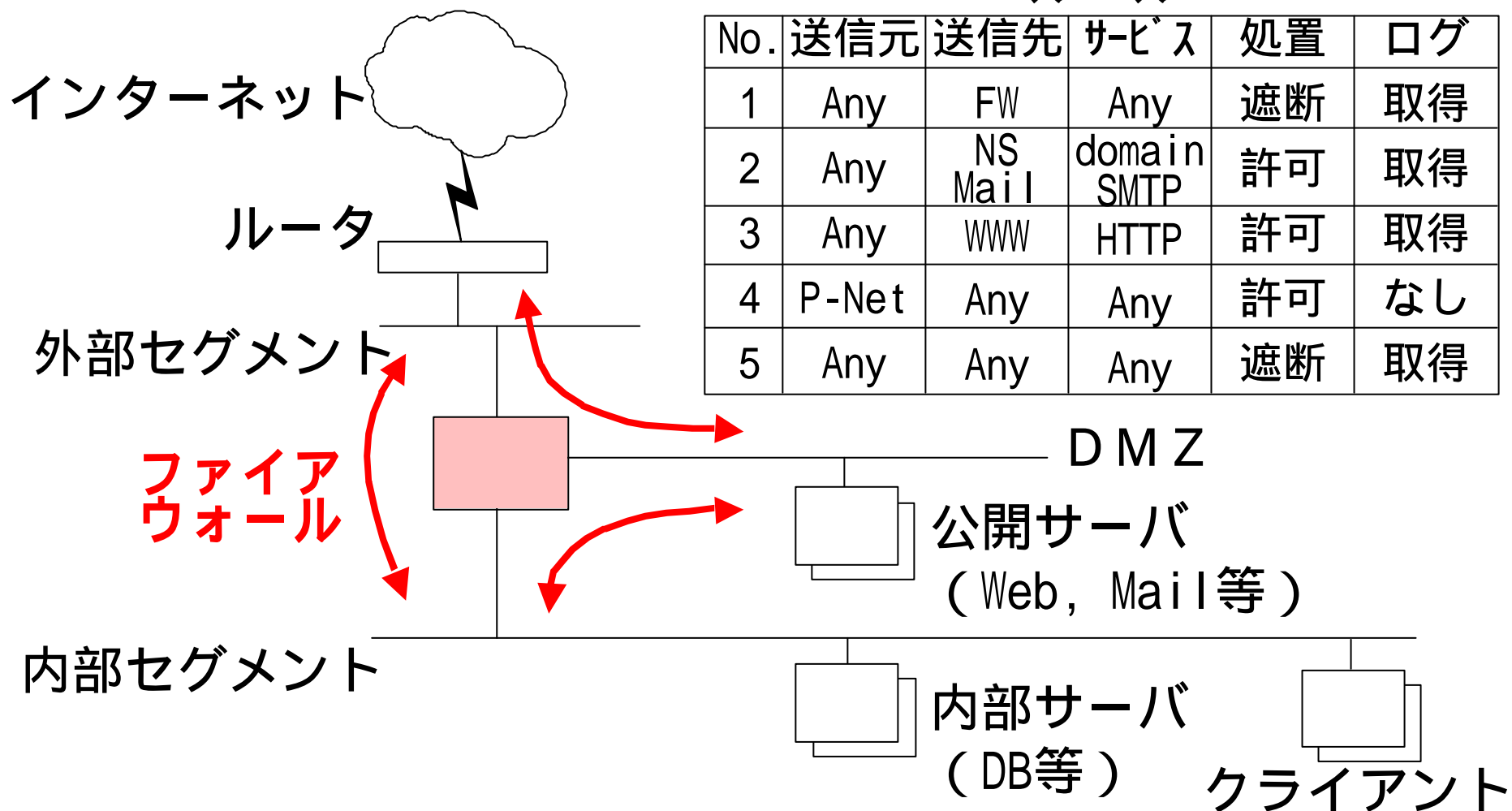
ルータの導入事例



ファイアウォールの導入事例

ルール

No.	送信元	送信先	サービス	処置	ログ
1	Any	FW	Any	遮断	取得
2	Any	NS Mail	domain SMTP	許可	取得
3	Any	WWW	HTTP	許可	取得
4	P-Net	Any	Any	許可	なし
5	Any	Any	Any	遮断	取得



ルータ、ファイアウォール による防御のまとめ

- 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
- 外部からのアクセスを制限し、安全な接続を提供する
- 内部と外部とを透過的に接続する
- アクセス状況のログを収集する

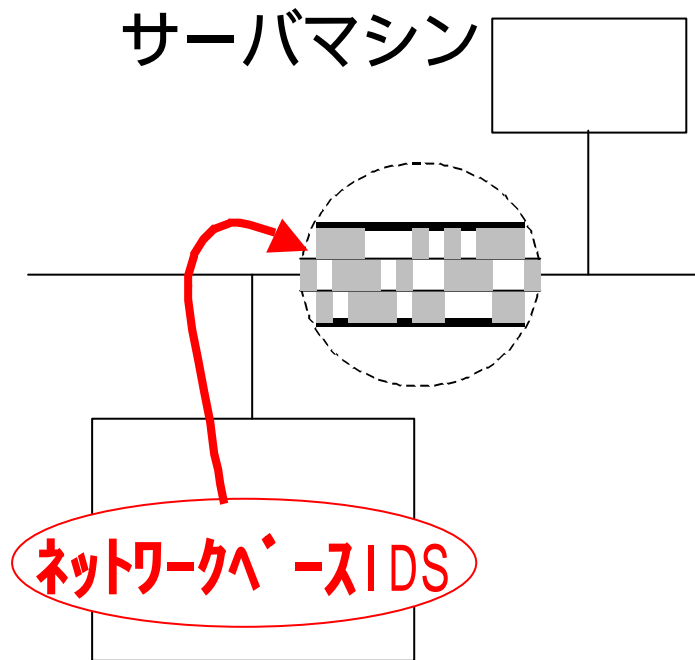
技術的な対策 通信の暗号化

通信の暗号化

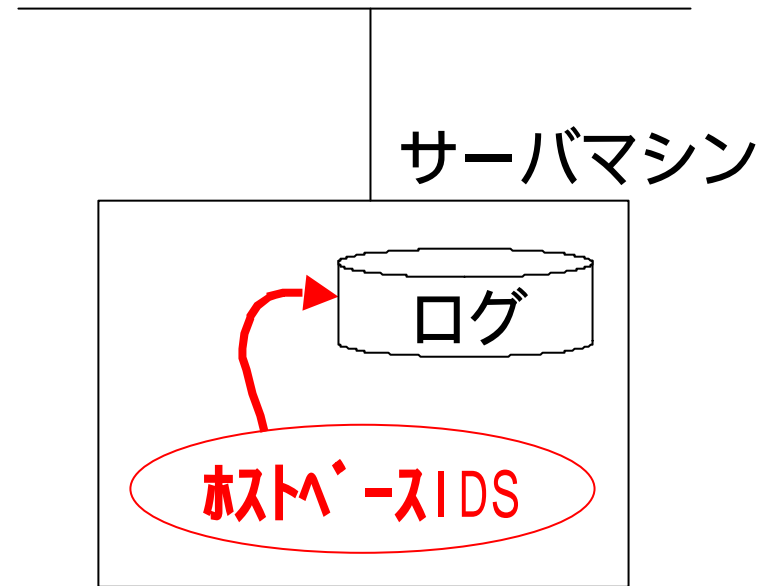
- SSH (SecureShell)
 - コマンドに対しセキュリティを強化するプロトコル
 - 特定のアプリケーションでの暗号化
- VPN (Virtual Private Network)
 - 仮想的な専用線としてのネットワーク
 - アプリケーションの変更が不必要

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 とホストベースIDS



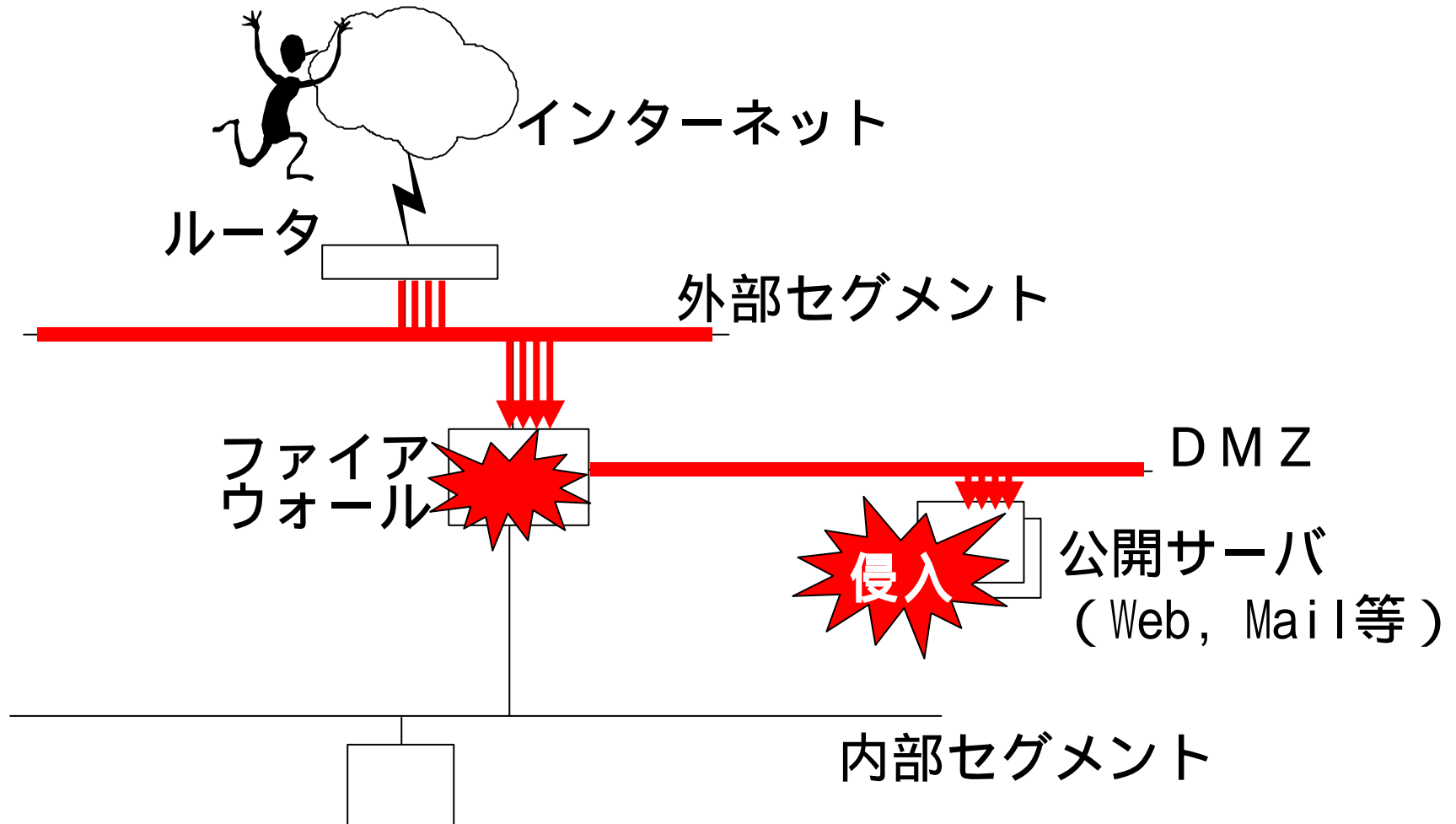
ネットワーク上の
パケットを監視



ログ等ホスト内の
ファイルを監視

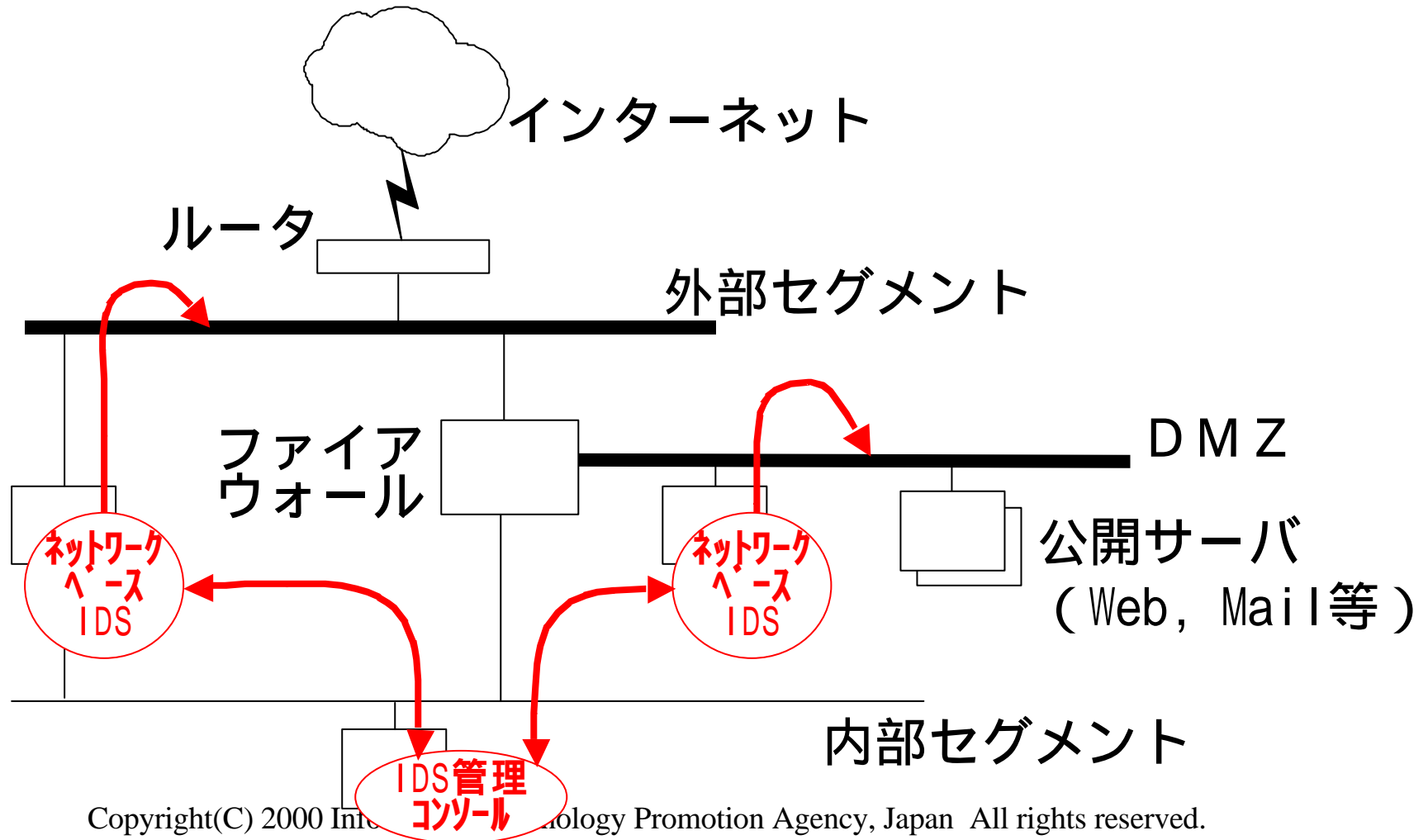
IDSの導入事例1

- ネットワークベースIDS



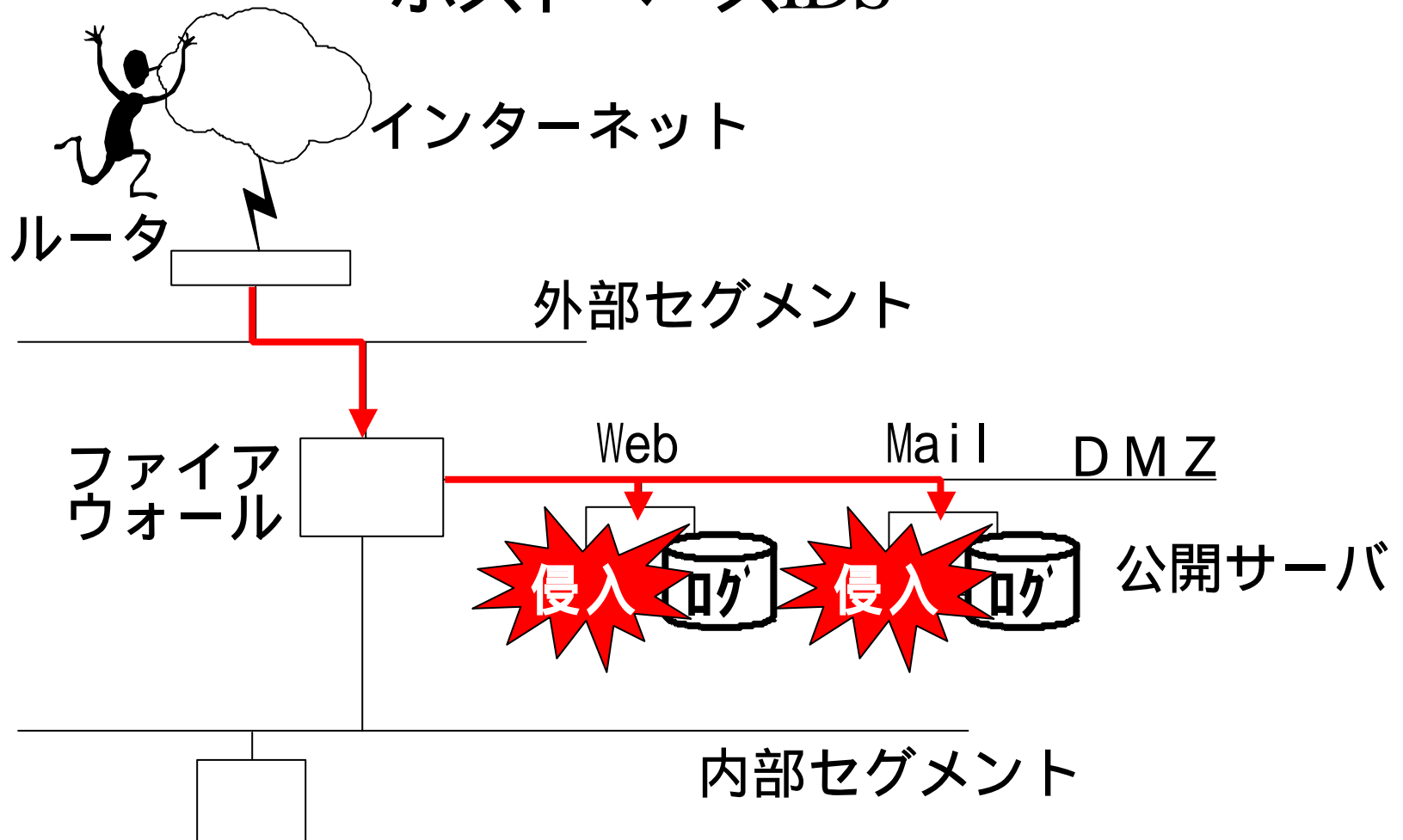
IDSの導入事例1

- ネットワークベースIDS



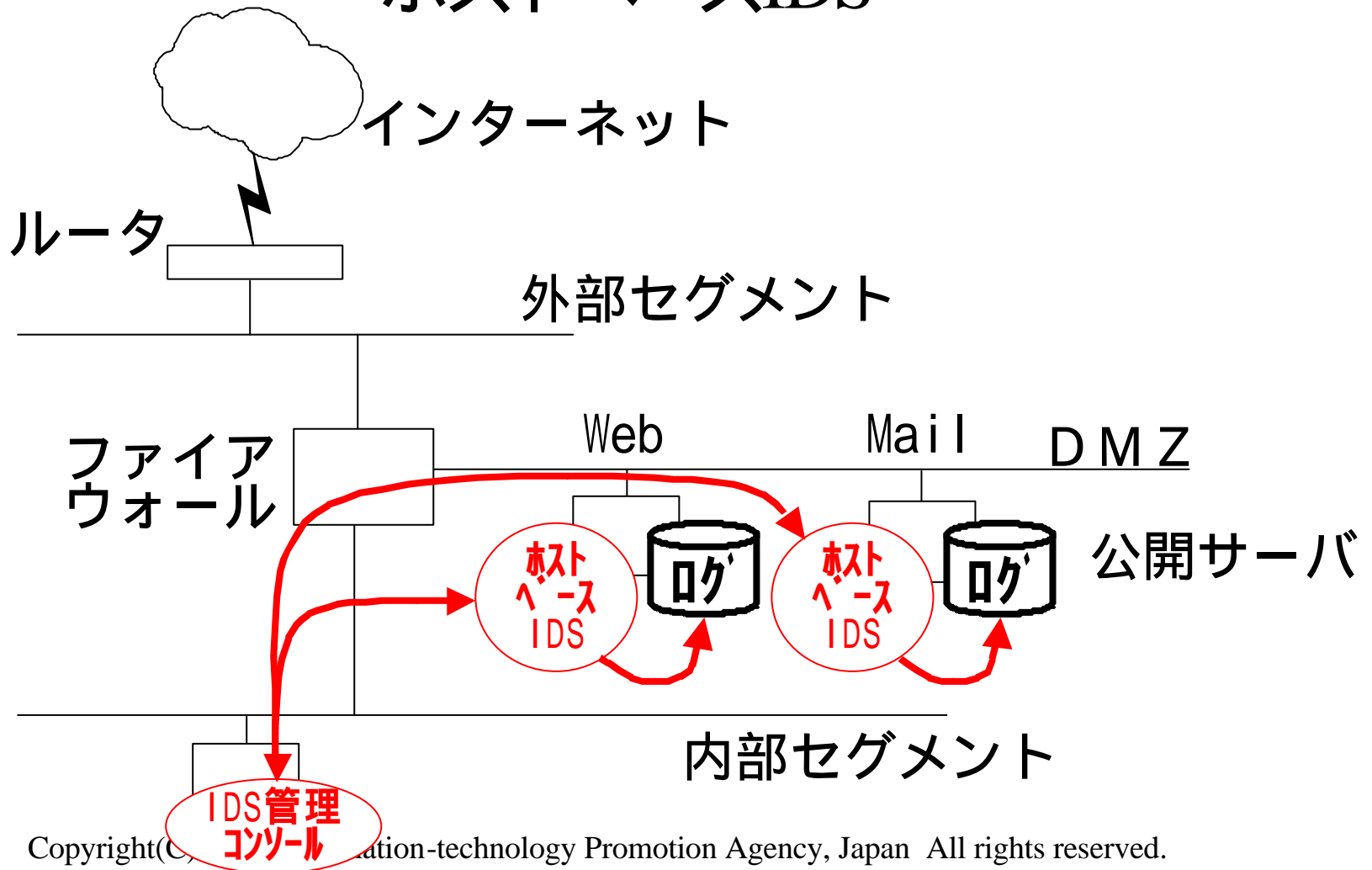
IDSの導入事例2

- ホストベースIDS



IDSの導入事例2

- ホストベースIDS



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を利用する
- 誤報を排除する

技術的な対策 ログの管理

ログの特徴 1

- UNIX環境

ログファイル `su log` の格納内容

日付、時刻、`su`コマンド実行結果、端末名称、ユーザ-ID、新ユーザ ID

出力例

```
SU 06/24 11:37 + pts/7 User-A-root
SU 06/30 12:17 - pts/8 User-B-root
SU 06/30 12:18 - pts/8 User-C-root
```

ログ出力設定を変更した出力例

```
Jun 30 12:17:15 Host-A su: 'su User-A' failed for User-B on /dev/pts/8
Jun 30 12:17:28 Host-A su: 'su root' failed for User-B on /dev/pts/8
Jun 30 12:18:00 Host-A su: 'su root' failed for User-C on /dev/pts/8
```

ログの特徴2

- Windows環境

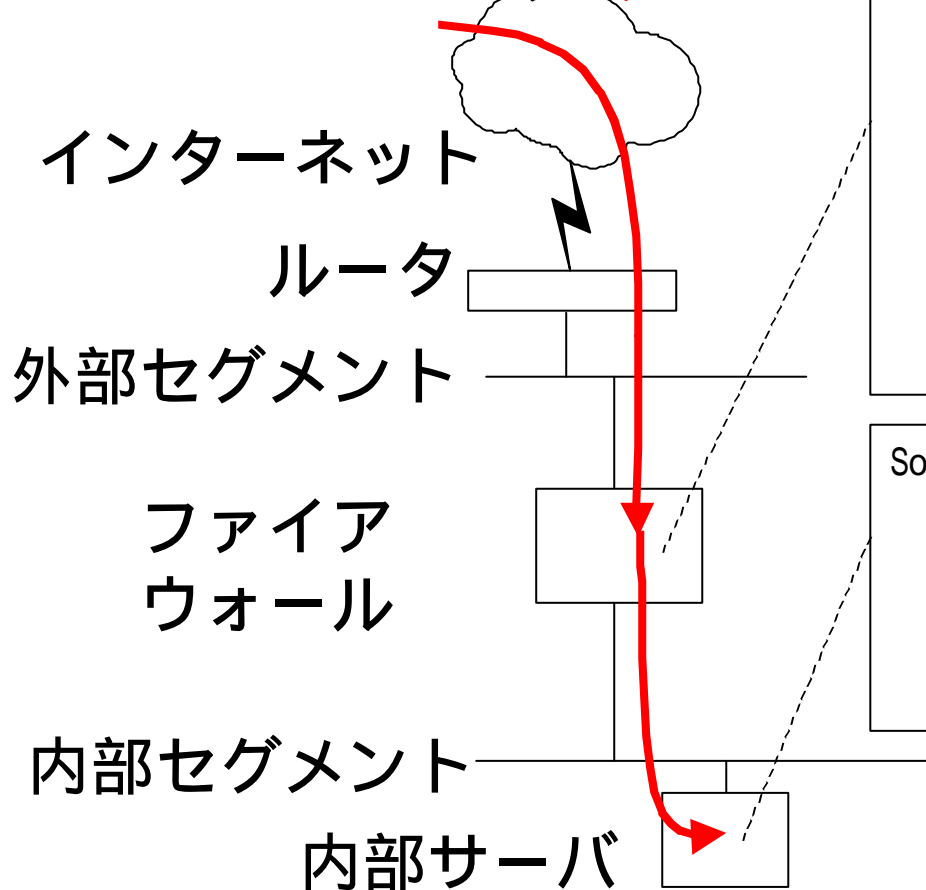
日付	時刻	ソース	分類	イベント ID	イベント ユーザー	コンピュータ
99/06/15	午前 9:59:42	Security	システム イベント	514	SYSTEM	
99/06/15	午前 9:59:42	Security	システム イベント	512	SYSTEM	
99/06/12	午後 4:00:27	Security	ログオン/ログオフ	538	Administr	
99/06/12	午後 4:00:27	Security	ログオン/ログオフ	528	Administr	
99/06/12	午後 1:38:24	Security	ログオン/ログオフ	529	SYSTEM	
99/06/12	午後 1:38:21	Security	ログオン/ログオフ	529	SYSTEM	
99/06/12	午前 11:43:26	Security	ログオン/ログオフ	528	Administr	
99/06/12	午前 11:43:18	Security	ログオン/ログオフ	528	ANONYMO	
99/06/12	午前 11:43:17	Security	システム イベント	515	SYSTEM	

[管理ツール]-[イベントビューア]-[セキュリティログ]
による状況確認

ログの特徴3

- FirewallとUNIX

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



FireWall-1

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

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

Solaris: message

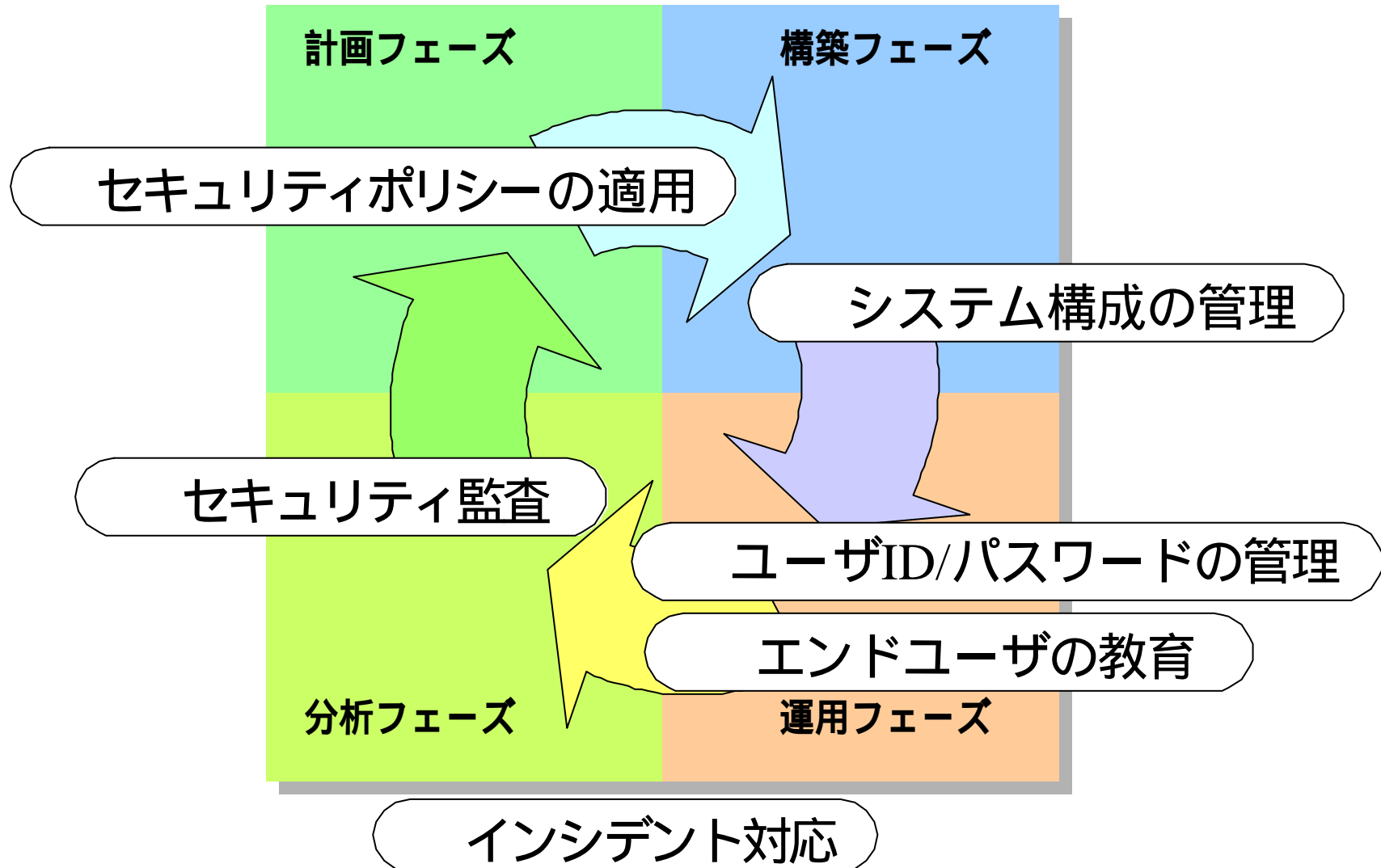
```
Jun 29 10:54:02 ultra7 statd[122]: statd:
pathname too long: /var/statmon/sm/<^1
FF>OGuG~OGuG~OGuFPV6;P.ahm.rg,bsntbg.slo.sdrs-
SWS
```

ログの管理におけるまとめ

- 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
- サーバの時間などをもとに分散化したログを分析する
- ログを安全に保管する

管理的な対策

管理的な対策



管理的な対策
セキュリティポリシーの適用

セキュリティポリシー策定の留意点

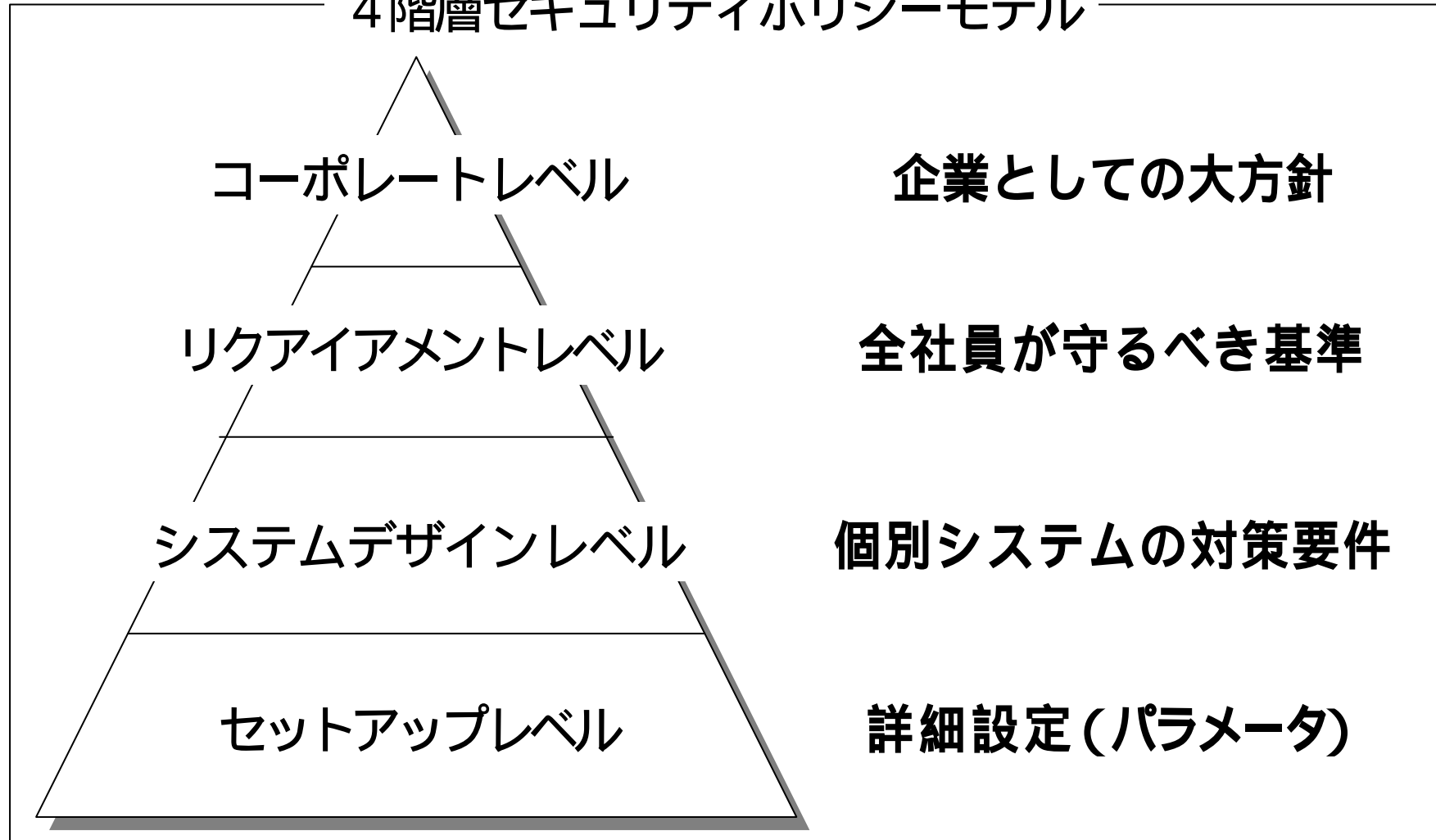
- 策定チームの体制
 - 経営層代表者
 - 機能的な各部門の担当者
 - 作成者
- 文書の構成
 - 方針、基準、実施手順
- 現状の種々の状況との擦りあわせ
 - 既存の管理規約、就業規則
 - 物理的な状況(組織の地理的な配置等)
- バランス
 - 使いやすさとセキュリティ

セキュリティポリシー運用 の留意点

- 運用の体制
 - ユーザへの周知徹底
 - 実施状況について情報収集
- 定期的な見直し
 - 実施状況や監査結果により検討
 - 適用範囲の対象はどこまでか

セキュリティポリシーのモデル

4階層セキュリティポリシーモデル



セキュリティポリシー文書構成例

セキュリティポリシー規定文書の例

階層	規定文書
コーポレートレベル	情報セキュリティ基本方針書
リクアイアメントレベル	情報システム利用倫理規準書 ネットワーク利用倫理規準書 電子化機密情報取扱規準書 アクセス管理規準書 ネットワーク構築・運用規準書 ウイルス対策規準書 物理的セキュリティ規準書 要員管理規準書 著作権規準書 個人情報保護規準書 緊急時対応計画に係る規準書 セキュリティ監査規準書
システムデザインレベル	セキュリティ対策技術ガイドライン 利用者セキュリティガイドライン セキュリティ運用ガイドライン
セットアップレベル	ファイアウォール設定 データベースアクセス設定 ID・パスワード利用マニュアル

「情報セキュリティ基本方針書」 項目例

- 総則
 - 目的、定義、関連規約、経営者の声明(方針)
- 情報資産の管理
 - 情報資産の分類及び管理、情報資産へのアクセス
- 組織内情報システム
 - 基本方針の遵守、外部委託
- 運用管理体制
 - 担当役員、担当部署、部門担当者
- 社員等の義務、違反に対する処分

セキュリティポリシー運用体制例



管理的な対策
システム構成の管理

システム構成管理に関する留意点

- 許可されていないハードウェアを導入させないようにする
- 不正なプログラム埋め込みから保護するための検出ツールを導入する
- リモート管理を実施する場合、管理対象の各コンピュータにおいて管理者以外のリモートアクセスを制御する

管理的な対策
ユーザID/パスワードの管理

ユーザID/パスワードの管理

- 休眠アカウントの停止
 - 強制的な処理
- 不適切なパスワードの排除
 - パスワード設定における制限
 - 定期的な検査
- 適切なパスワードの利用
 - ユーザへの徹底
- パスワードの盗難防止

パスフレーズによる パスワードの設計

パスフレーズ

「HARUHA AKEBONO」

母音を抜き記号や数字を挿入

パスワード

「HR \$ HK % BN」



管理的な対策
エンドユーザの教育

ユーザ利用における留意点

- セキュリティポリシーを遵守させる
- ブラウザやメーラを安全に設定させる
- ダウンロードまたは送受信したファイルの安全性を検証させる
- 適切なパスワード管理を実施させる
- インシデント対応の手順を認識させる

管理的な対策
セキュリティ監査

セキュリティ監査手法と項目

手法:

- セキュリティ監査ツール
- 監査の経験とノウハウを用いた手作業

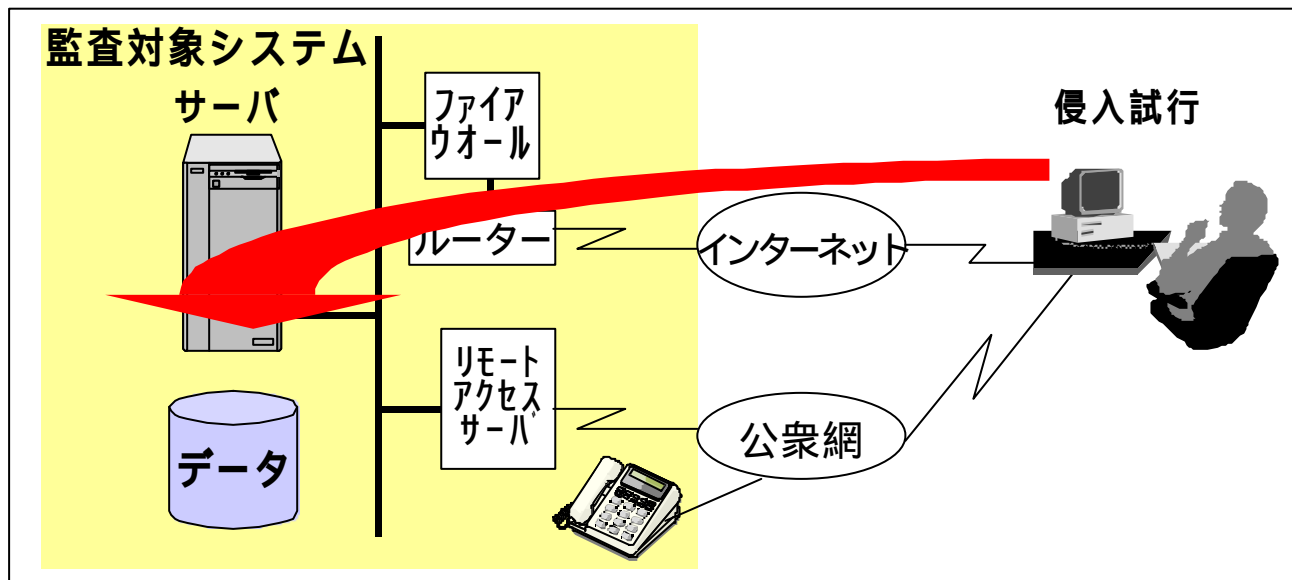
項目:

- 安全なパスワードの使用
- 安全なバージョンのソフトウェアを使用
- サービス使用状況の確認 (不要サービス、ポートの排除)
- サーバ、ルータの設定状況の確認
- セキュリティ・ホールの排除
- 不適切なプログラムの排除 (CGIプログラム)
- 不審なサービス、プログラムの確認 (トロイの木馬、バックドア)
- ネットワーク構成全体に対する脆弱性チェック (不要モデム)
- アタックに対するネットワークの安全性評価 (組織として)

セキュリティ監査サービスの事例

タイガーチームサービス

- ハッキング手法、アタックノウハウを用いてシステムへの侵入を試みる。
- 潜在するセキュリティ・ホール、脆弱性を検証する。



管理的な対策 インシデント対応

インシデント対応の作業手順

- 1 . 手順の確認
- 2 . 作業記録の確認
- 3 . 責任者、担当者への連絡
- 4 . 事実の確認
- 5 . スナップショットの保存
- 6 . ネットワーク接続やシステムの遮断もしくは停止
- 7 . 影響範囲の特定
- 8 . 渉外、関係サイトへの連絡
- 9 . 要因の特定
- 10 . システムの復旧
- 11 . 再発防止策の実施
- 12 . 監視体制の強化
- 13 . 作業結果の報告
- 14 . 作業の評価、ポリシー・運用体制・運用手順の見直し

技術メモ - コンピュータセキュリティインシデントへの対応

<http://www.jpccert.or.jp/ed/2000/ed000007.txt>

Copyright(C) 2000 Information-technology Promotion Agency, Japan All rights reserved.

被害の報告等

被害の届出(事後)

情報処理振興事業協会(IPA)

セキュリティセンター

不正アクセス対策室

E-mail: crack@ipa.go.jp

FAX: 03-5978-7518

相談専用電話: 03-5978-7509

インシデントの
相談・報告

JPCERT/CC

(コンピュータ緊急対応センター)

E-mail: info@jpcert.or.jp

FAX: 03-5575-7764

TEL: 03-5575-7762

まとめ

- 既存の不正アクセス対策を実施
- 技術的な対策と運用的な対策の両方を実施
- 継続的な改善によりセキュリティを維持
- セキュリティの向上には、管理者による推進が不可欠

情報処理振興事業協会 (IPA)
セキュリティセンター
不正アクセス対策室
E-mail: crack@ipa.go.jp