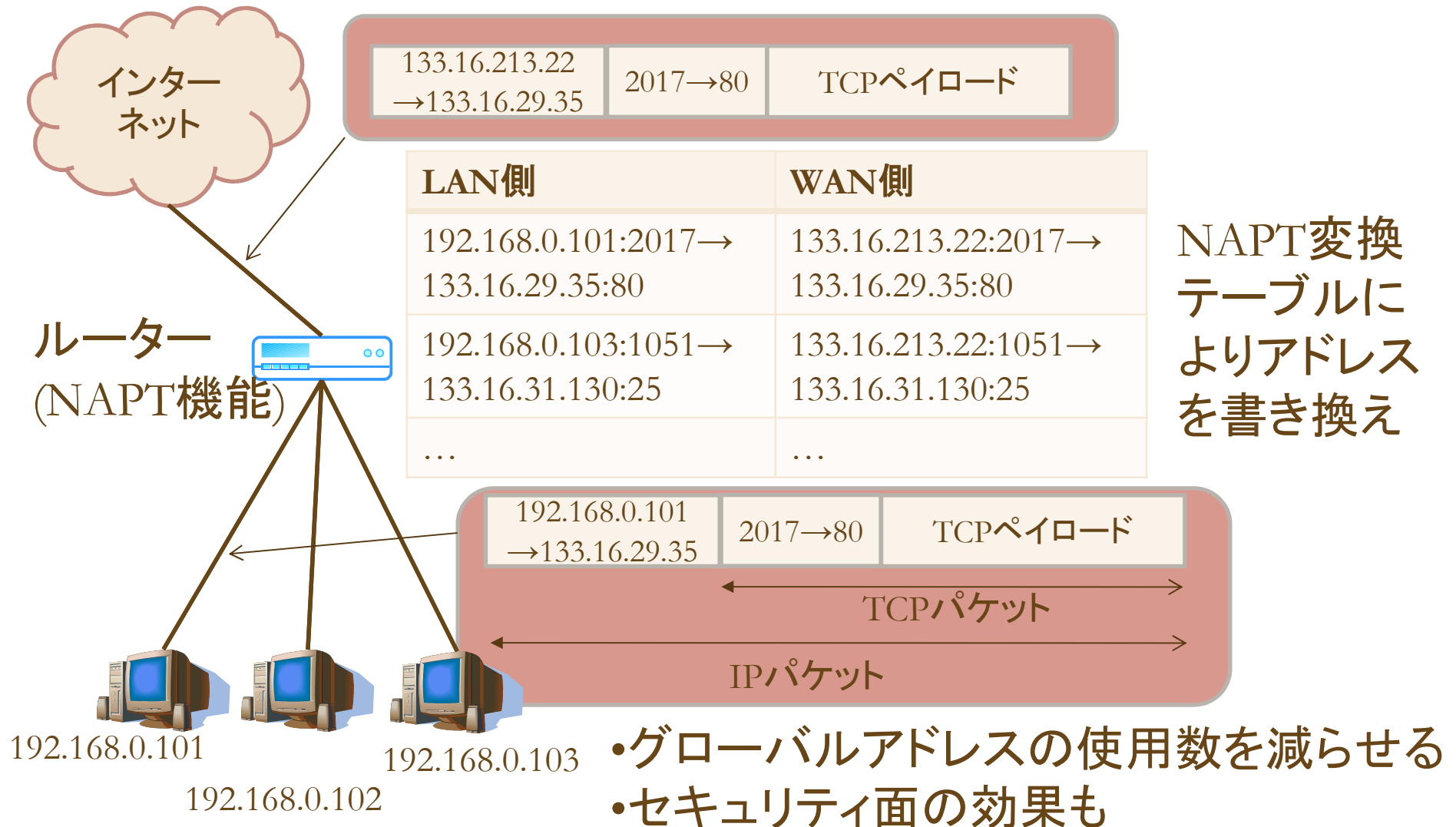
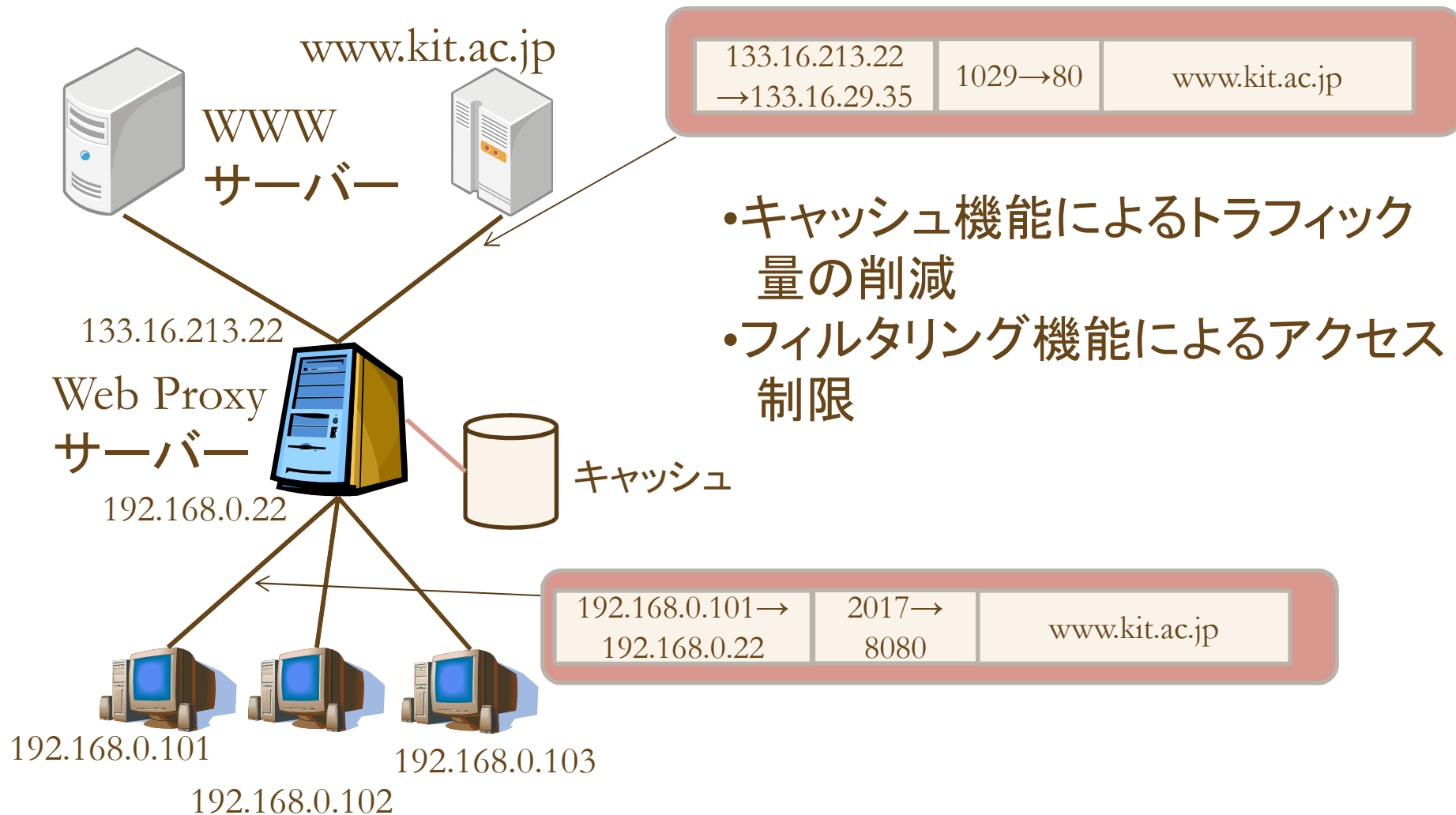


NAPTによるIPアドレス/ポート番号の変換



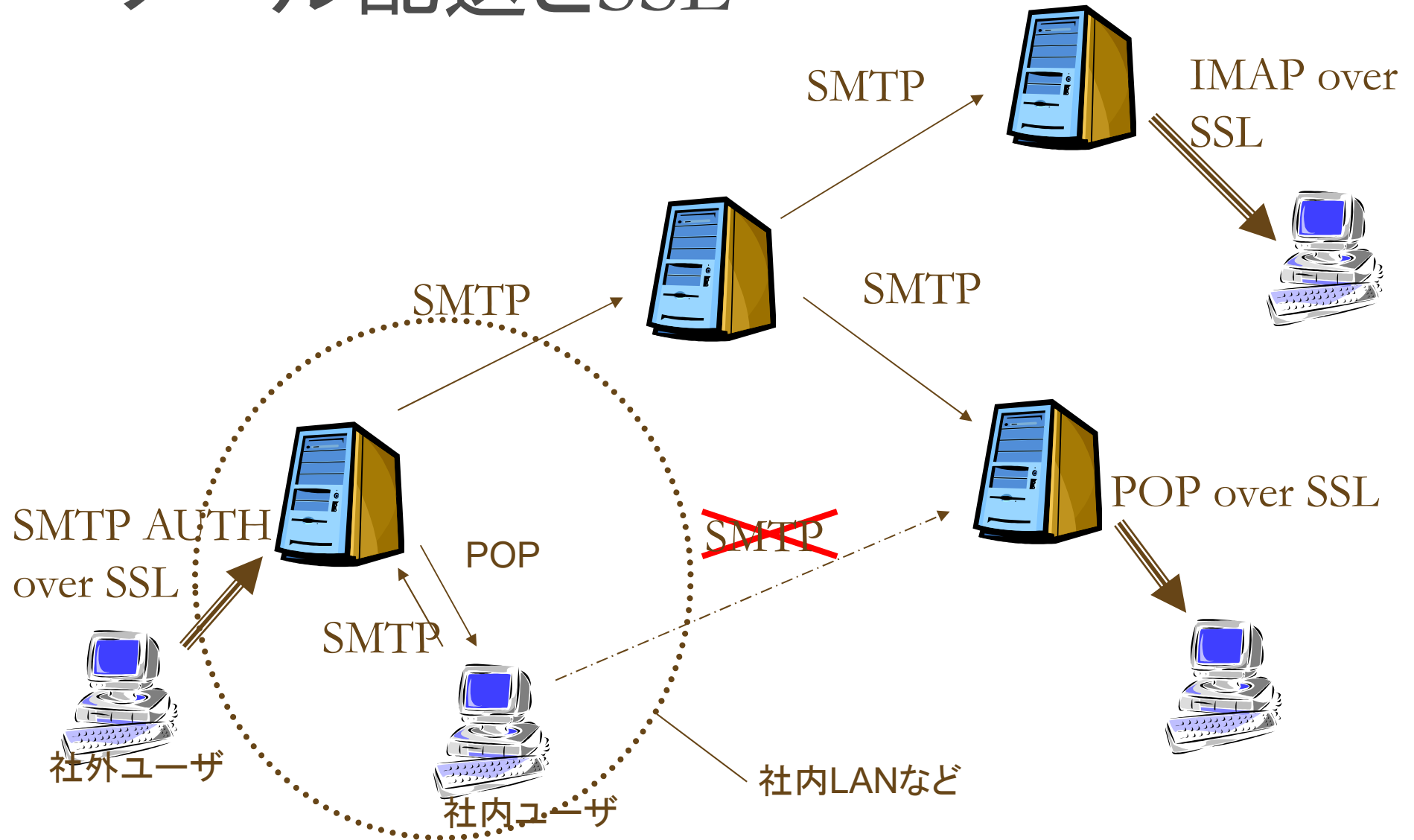
Proxyによる中継



IPSECとSSL/TLSの比較

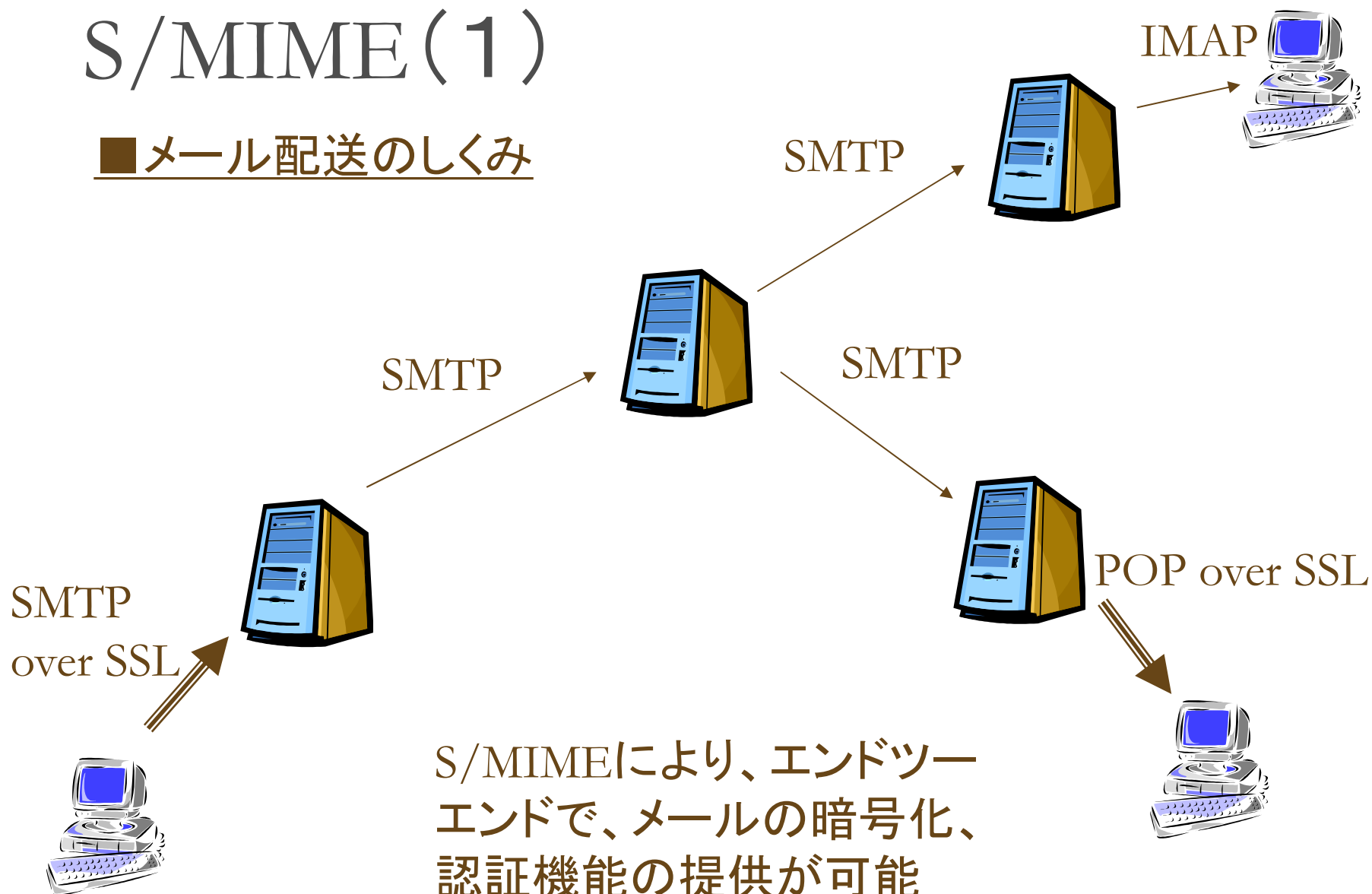
IPSEC	SSL/TLS
IPヘッダも保護可能	ペイロードのみ
TCP/UDPともに適用可	TCPのみ
アプリケーションの変更不要	アプリケーションの変更必要
OSの変更(対応)必要	OSの変更(対応)不要
プロキシが使えない	プロキシが使える
NAT(NAPT)が使えない	NAT(NAPT)が使える

メール配送とSSL



S/MIME (1)

■メール配送のしくみ



S/MIME (2)

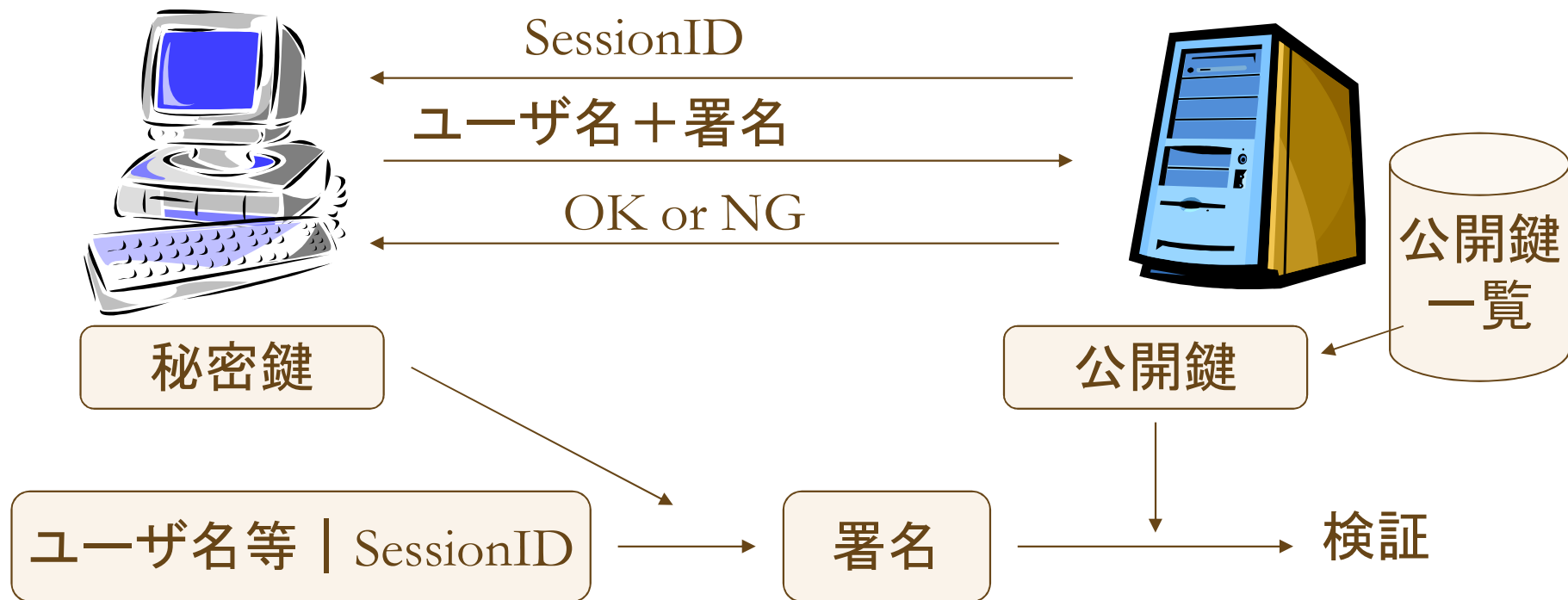
- S/MIMEの基本機能

- 親展機能: 決まった相手しか電子メールが読めないように暗号化する
- 署名機能: 送信者が正しいこと、メール内容が改ざんされていないことを保証する

- 普及のための課題

- 利用者毎にデジタル証明書(X.509)が必要
→ 費用面、操作面の問題
- メールソフトの対応
→ 主なアプリケーションは対応。操作面の問題。

SSH(ユーザ認証)



- ユーザ認証以前に、ホスト同士で鍵交換(DH法)をして通信を暗号化(3DES等)
- パスワード認証モードもある
- ポートフォワーディングにより他のプロトコル(Xなど)の暗号化も

SSHのアクセスログの例

```
Oct 27 12:33:50 hoge sshd[18252]: Invalid user staff from *.*.207.20
Oct 27 12:33:52 hoge sshd[18255]: Invalid user sales from *.*.207.20
Oct 29 21:09:06 hoge sshd[18802]: Invalid user xwang from *.*.29.7
Oct 29 21:09:09 hoge sshd[18805]: Invalid user www from *.*.29.7
Oct 29 21:09:14 hoge sshd[18808]: Invalid user www from *.*.29.7
Nov 12 07:06:09 hoge sshd[4470]: Invalid user oracle from *.*.2.183
Nov 12 07:06:10 hoge sshd[4473]: Invalid user oracle from *.*.2.183
Nov 12 07:06:11 hoge sshd[4476]: Invalid user oracle from *.*.2.183
Nov 15 12:15:24 hoge sshd[12501]: Invalid user yo from *.*.202.101
Nov 15 12:15:27 hoge sshd[12504]: Invalid user yo from *.*.202.101
Nov 18 07:52:21 hoge sshd[13298]: Invalid user oracle from *.*.229.220
Nov 18 07:52:23 hoge sshd[13301]: Invalid user oracle from *.*.229.220
Nov 19 00:10:07 hoge sshd[13352]: Invalid user oracle from *.*.194.70
```

→頻繁にBrute-Force Attackがあるので脆弱なパスワードだと危険。

コンピュータウイルス

● コンピュータウイルスの機能

- 自己伝染機能
- 潜伏機能
- 発病機能

● マルウェア (malware) とは

- ウイルス (実行形式、マクロ)
- ワーム
- ボット
- スパイウェア
- ランサムウェア

コンピュータウイルス等の感染

● 感染経路

- ネットワーク(メール、メッセージャー、Webなど)
- メディア(CD, DVD, USBメモリなど)

● 感染方法

- 電子メールの添付ファイルをユーザに実行させる
- 電子メールの添付ファイルをOS,アプリのバグを利用して自動実行させる
- メッセージャーやファイル共有機能等を利用してネットワークから侵入
- ウェブ閲覧時にプログラムをダウンロード、実行させる

コンピュータウイルス等への対策

● 事前対策

- ウイルス対策ソフト(ウイルス定義ファイルの更新)
- OS、アプリのパッチ(修正プログラム)の適用
- ファイルのバックアップ、シグネチャ登録
- ソフトウェアの設定に留意する
- パソコンの管理

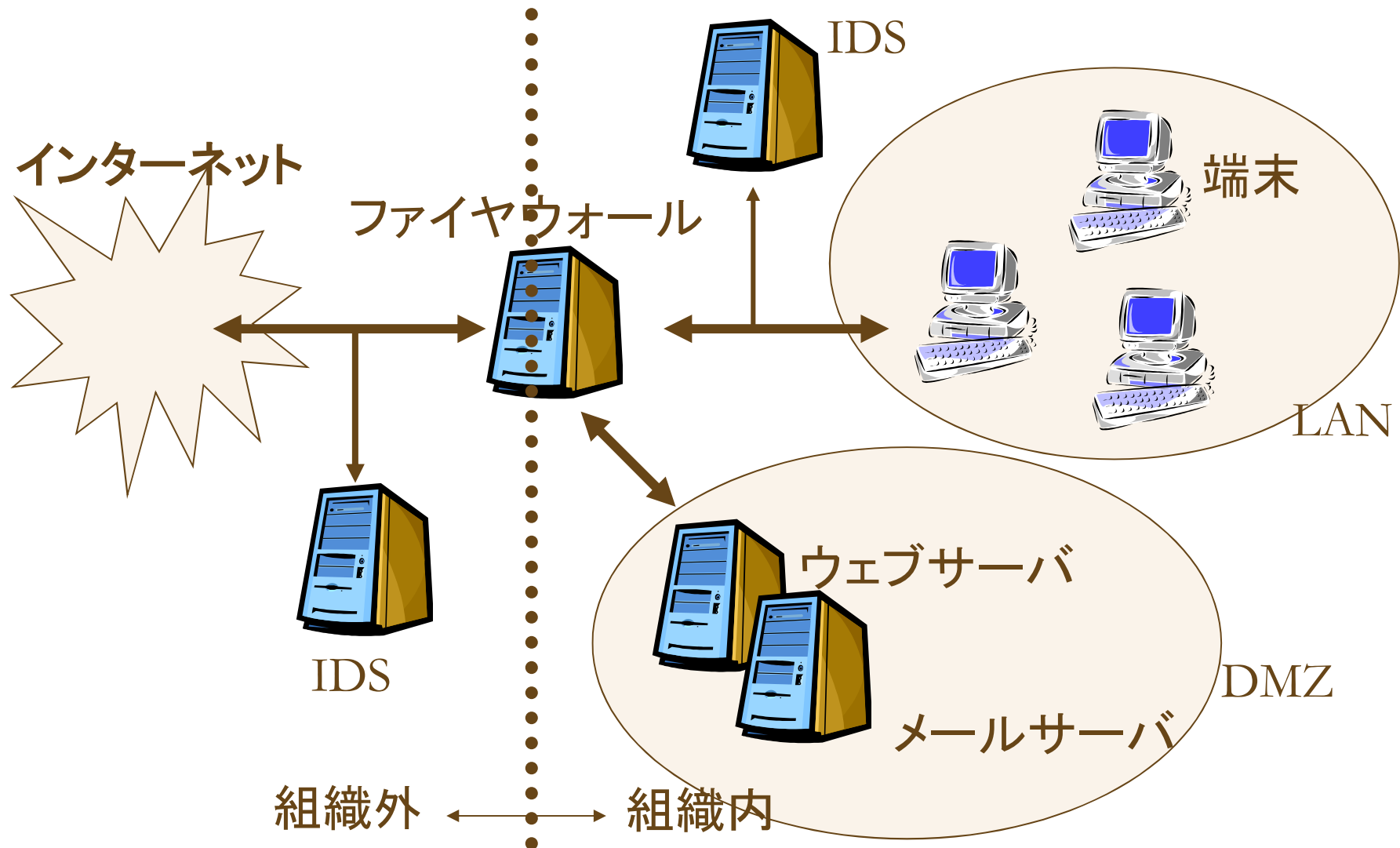
● 事後対策

- ウイルス検出、ファイル改ざん検出
- データの回復
- 届出(所属機関、IPA(情報処理推進機構)、警察など)

ソフトウェアのライフサイクル

- ソフトウェアにも寿命がある
 1. 初版(またはβ版)リリース
 2. セキュリティパッチ、アップデート
 3. バージョンアップ
 4. 開発停止(セキュリティメンテナンスのみ)
 5. 開発終了(セキュリティメンテナンスもなし)
- 段階5のソフトウェアは原則使用できない
(例: Windows 7 :
2020年1月14日にサポート終了)

ファイアウォールとIDS



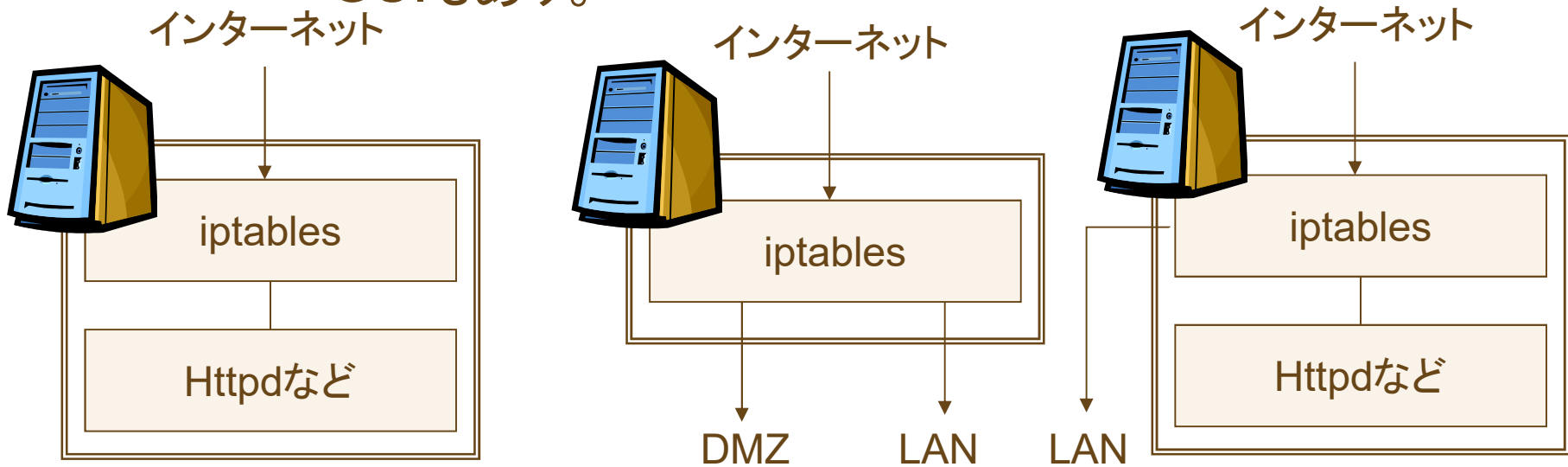
ファイアウォール

- 未対策のWindowsPCを直接ネット接続すると約4分でウイルス感染するとの調査も→修正パッチを適用するまでに感染？！
- アクセス制御するネットワーク階層による分類
 - ネットワーク層型:IP層で制御を行う。ルータの機能として実装されていることも多い。高速処理が可能。
 - トランスポート層型:TCP/UDP層で制御を行う。IPアドレスを変換することもある。比較的高速。
 - アプリケーション層型:アプリケーションゲートウェイとも呼ばれる。アプリケーション毎に依存した処理が可能。高速処理は困難。
- 運用管理:適切な運用管理が不可欠
 - 適切な設定
 - ログ情報の管理
 - FW自体のアップデート

アプリケーション層
プレゼンテーション層
セッション層
トランスポート層
ネットワーク層
データリンク層
物理層

ファイアウォールの例 (iptables)

iptables : Linux (カーネル2.4以降) に組み込まれている
ファイアウォール。設定は原則コマンドベースだが
GUIもあり。



サーバー内蔵型:

- 専用のホスト不要
- サーバのサービスに特化できる
- 他のサーバは保護できない

独立型:

- 専用のホスト (複数のネットワークデバイス)
- ネットワーク内の全てのホストを保護できる

複合型

IDS

(Intrusion Detection System)

- 設置形式による分類
 - ホスト型: 各ホストへの侵入、スキャン行為などを検知する
 - ネットワーク型: ネットワーク単位で侵入、スキャン行為などを検知する
- 検知方法による分類
 - シグネチャ型: あらかじめ不正侵入のパターン(シグネチャ)を登録しておく
 - プロファイル型: 通常のふるまいを登録しておき、それから外れたら不正侵入とみなす
- 運用上の注意点
 - 誤検知(False Positive, False Negative)は避けられない。適切なチューニングが重要。
 - 侵入を防止するものではない。ログの管理、運用が大事。

IDSの例 (Snort)

Snort: オープンソースとして開発、配布されているシグネチャ型IDS

ネットワーク
インタフェース

パケット
キャプチャ

ネットワークに流れるパケットをインタフェース毎
キャプチャ(取り込む)

プリプロセッサ

- パケットの再構築
- 一部プロトコルの解析
- アノマリ型機能の実現

ルール
ファイル

ルール
マッチング

パケット毎にルール(シグネチャ)にマッチするか
どうか調べられる。
シグネチャは、種別毎に幾つかのファイルに
まとめられている。
シグネチャの自動更新(Oinkmaster)機能も

データ
ベース等

アウトプット
プラグイン

検知結果をテキストログや、各種RDB
(MySQL, PostgreSQL等)へ出力

無線LANの通信規格

- IEEE802委員会、WG11により規格化
 - IEEE802.11b : 2.4GHz帯、DS(直接拡散)方式、11Mbps
 - IEEE802.11a : 5GHz帯、OFDM方式、54Mbps
 - IEEE802.11g : 2.4GHz帯、OFDM方式、54Mbps
 - IEEE802.11n: 2.4GHz/5GHz帯、OFDM/MIMO方式、600Mbps(実効150～300Mbps)
 - IEEE802.11ac: 5GHz帯、OFDM/MU-MIMO方式、6.9Gbps

無線LANのセキュリティ(0)

- SSID（セキュリティとは直接関係ないが）
 - アクセスポイントを区別するための識別子
 - SSIDのアナウンスをやめてany接続を禁止すれば少しはまし(気休め程度)
 - MACアドレス制限
 - あらかじめ登録したMACアドレス機器からしか接続できない
 - MACアドレスを任意に設定することは可能なのでセキュリティ対策としては不十分
(誤接続を防止する効果はある)
- いずれも盗聴を防止する効果はない
(電波を受信できれば丸見え)

無線LANのセキュリティ規格

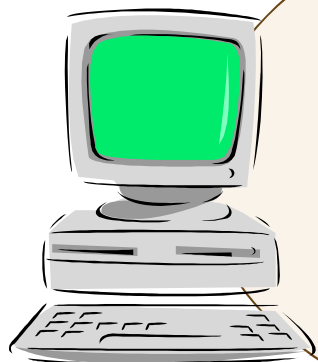
- WEP(Wired Equivalent Privacy)
 - 暗号化アルゴリズムRC4
(暗号化鍵5byteまたは13byte)
 - 脆弱性が指摘されており数十秒で解読可能
- WPA(Wi-Fi Protected Access)
 - 業界団体(Wi-Fi Alliance)制定
 - 暗号化アルゴリズムTKIP(RC4) 安全性△？
 - 認証方式の規格(IEEE802.1X, PSK)も含む
- WPA2(IEEE802.11i)
 - 暗号化アルゴリズムCCMP(AESベース)
- WPA3
 - WPA2の脆弱性を修正
 - SAE(認証時の鍵確立プロトコル)の強化など

- アクセスポイントの先は暗号化されない
- HTTPS 等と併用するのが望ましい

IPスプーフィング

通常の流れ

ホストA



アドレスA

SYN(アドレスA)

SYN/ACK(S)

ACK(S)



サーバ(攻撃対象)
(ホストAを信頼している)

S: 初期
シーケンス番号

攻撃時の流れ

初期シーケンス
番号が予想できる
ことが必要

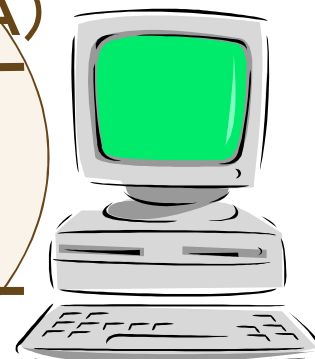
(2) SYN/ACK(S)



サーバ(攻撃対象)

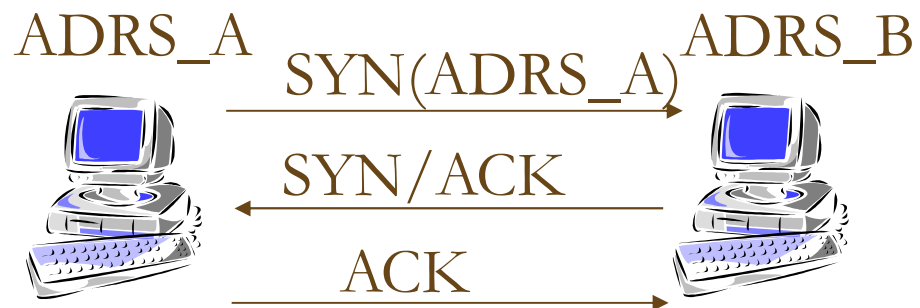
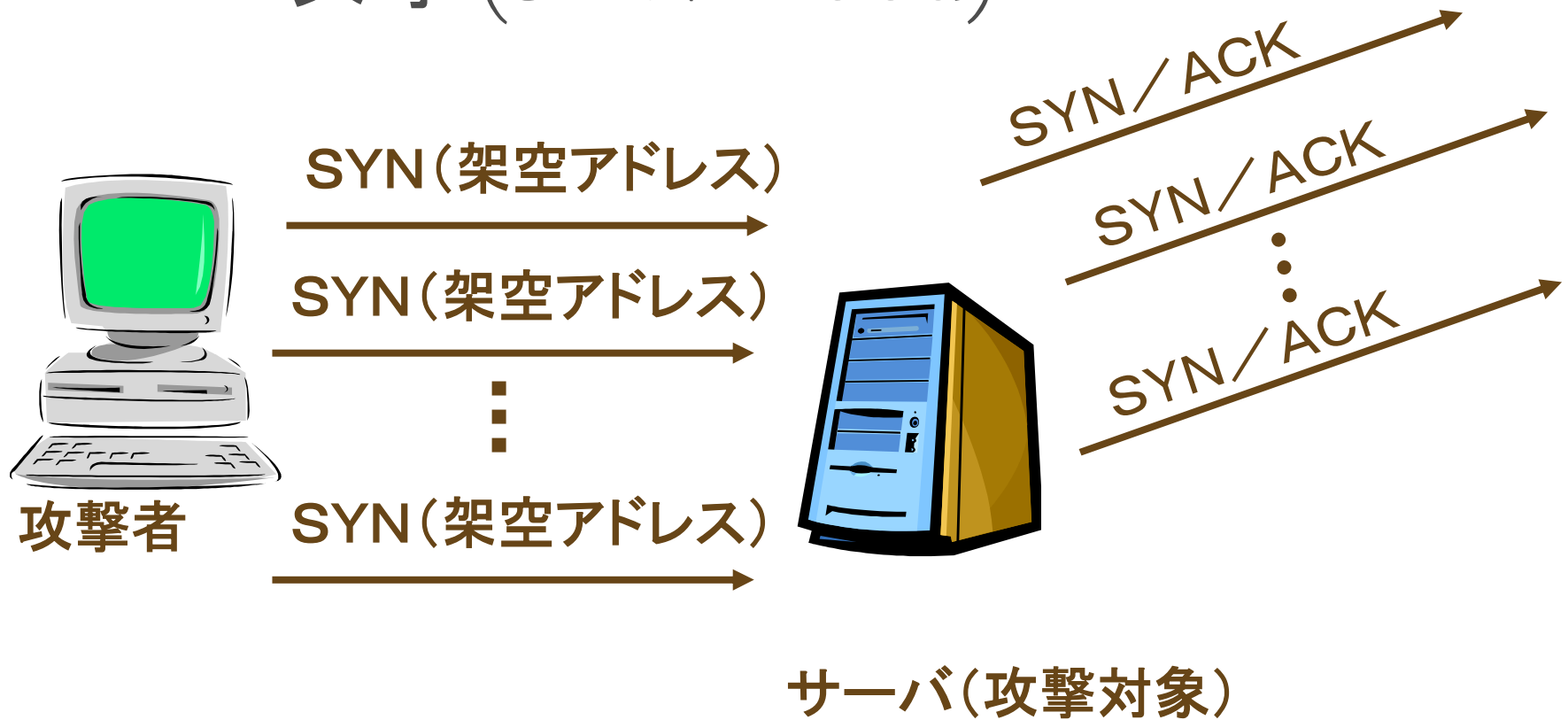
(1) SYN(アドレスA)

(3) ACK(S)

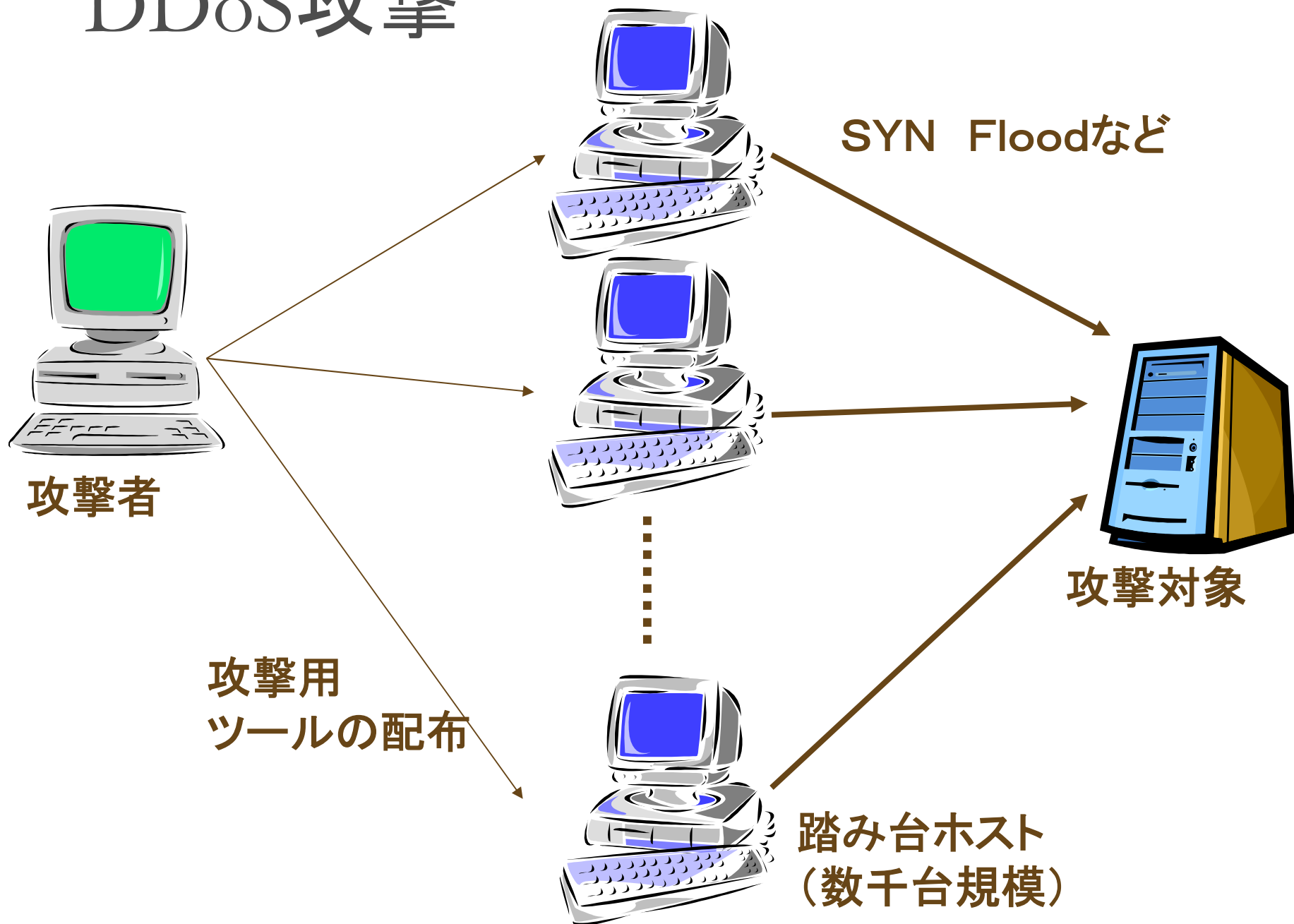


攻撃者

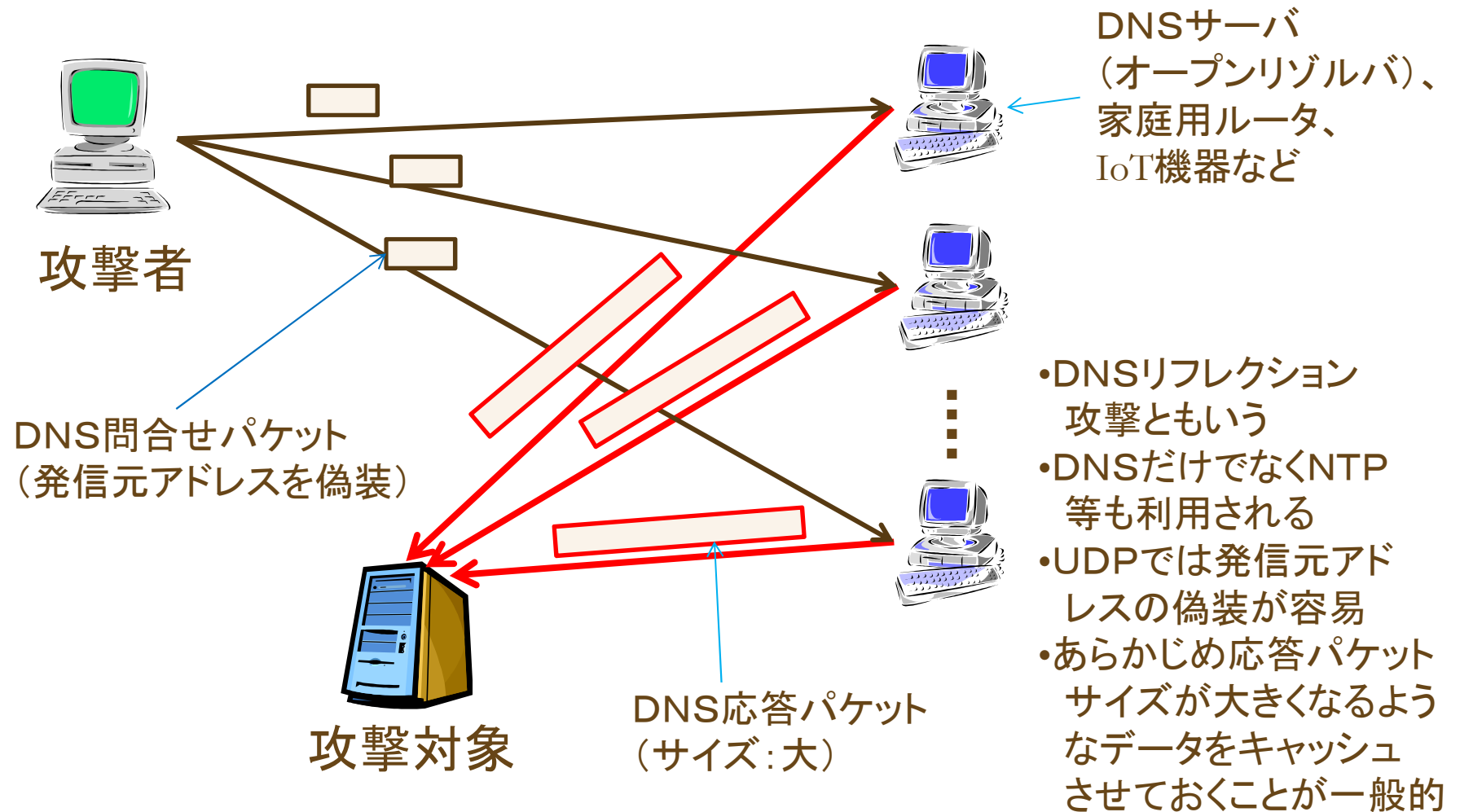
DoS攻撃(SYN Flood)



DDoS攻撃



DNS amp による DDos攻撃



DNSキャッシュポイズニング

www.kit.ac.jp (本物)
133.16.29.35



権威DNSサーバ



www.kit.ac.jp (偽物)
1.2.3.4



www1.kit.ac.jp ?

www1.kit.ac.jp ?

?

www.kit.ac.jp?

1.2.3.4



キャッシュDNSサーバ



DNSキャッシュサーバに大量の
偽応答パケットを送り、偽の情報を
キャッシュさせる

DNS応答(UDP)は、リクエスト発行時に
DNSサーバが利用したポート番号(16bit)と
トランザクションID(16bit)が一致すれば
受け入れられる。

偽応答

www1.kit.ac.jp→1.2.3.4

*.kit.ac.jp→1.2.3.4

DNSSEC (DNSサーバの応答情報に
電子署名を付ける拡張方式)への対応が
順次進められている

中間者攻撃

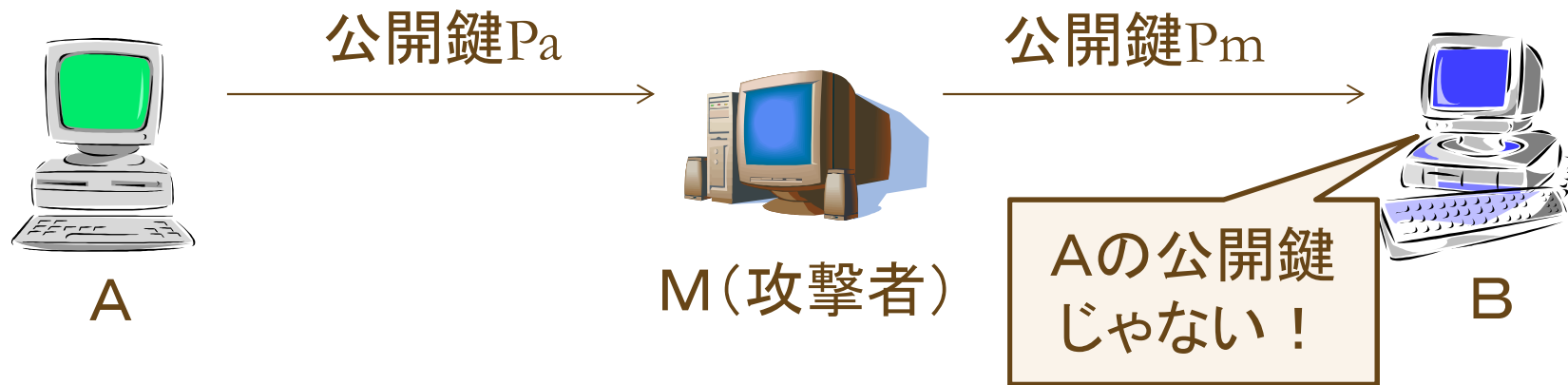
(Man In The Middle attack)

攻撃者が通信経路の途中に割り込んで通信内容を盗聴したり改ざんしたりする攻撃



中間者攻撃への対策

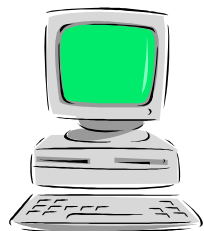
•PKIを利用する



•インターロックプロトコル

P_b で暗号化

1 2



A

1

2

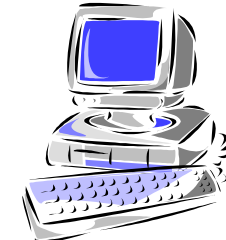
1と2が揃わないと
復号できない

1

2

P_a で暗号化

1 2



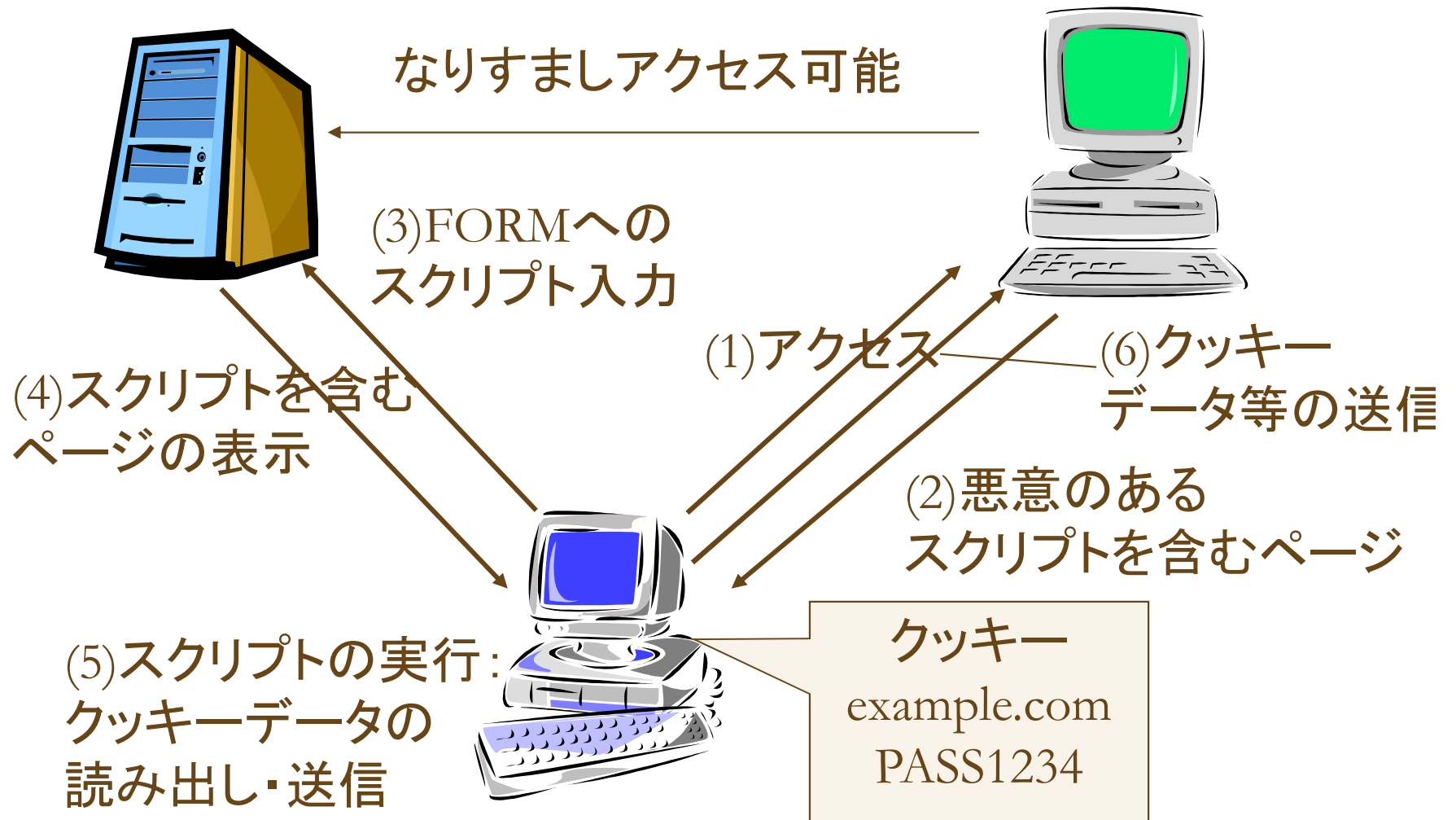
B

クロスサイトスクリプティング(1)

問題のある電子商取引サイト等から送られるクッキー情報
(パスワードなど)を、悪意のあるサイトに盗み取られる

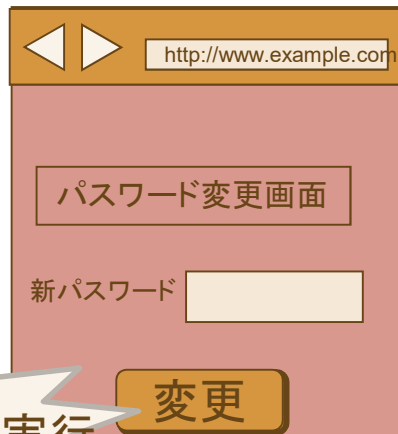


クロスサイトスクリプティング(2)



クロスサイトリクエスト フォージェリ (XSRF)

www.example.com



http://www.example.com

パスワード変更画面

新パスワード

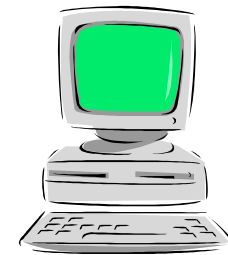
変更

(3) スクリプト実行

(0) クッキー保存
example.com
PASS1234



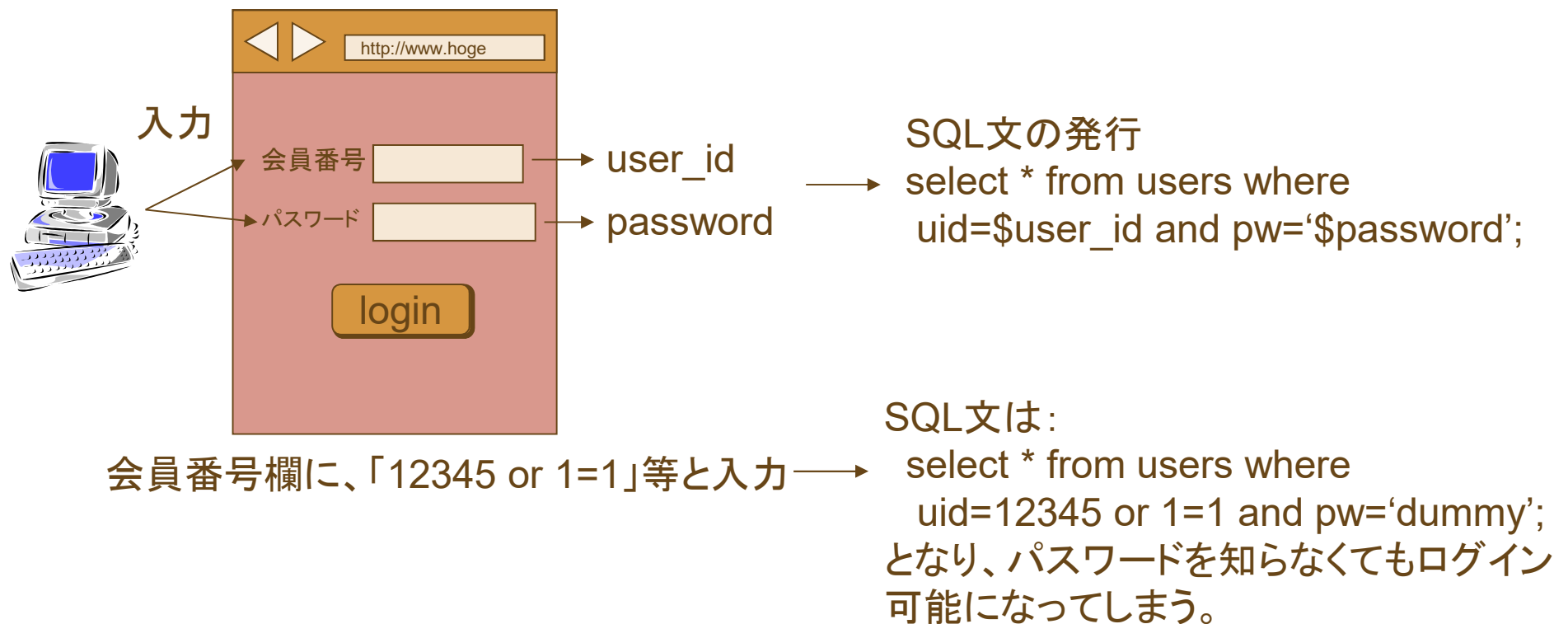
(2) 悪意のあるスクリプト
(パスワード変更操作など)



(1) 罯サイトへのアクセス
(HTMLメール等でもよい)

- 罯サイトを踏まない
(HTMLメールへの対策も)
- 重要サービスにログインしたままに
しない(クッキーを削除)
- 根本的にはサーバー側の対策が
重要

SQLインジェクション



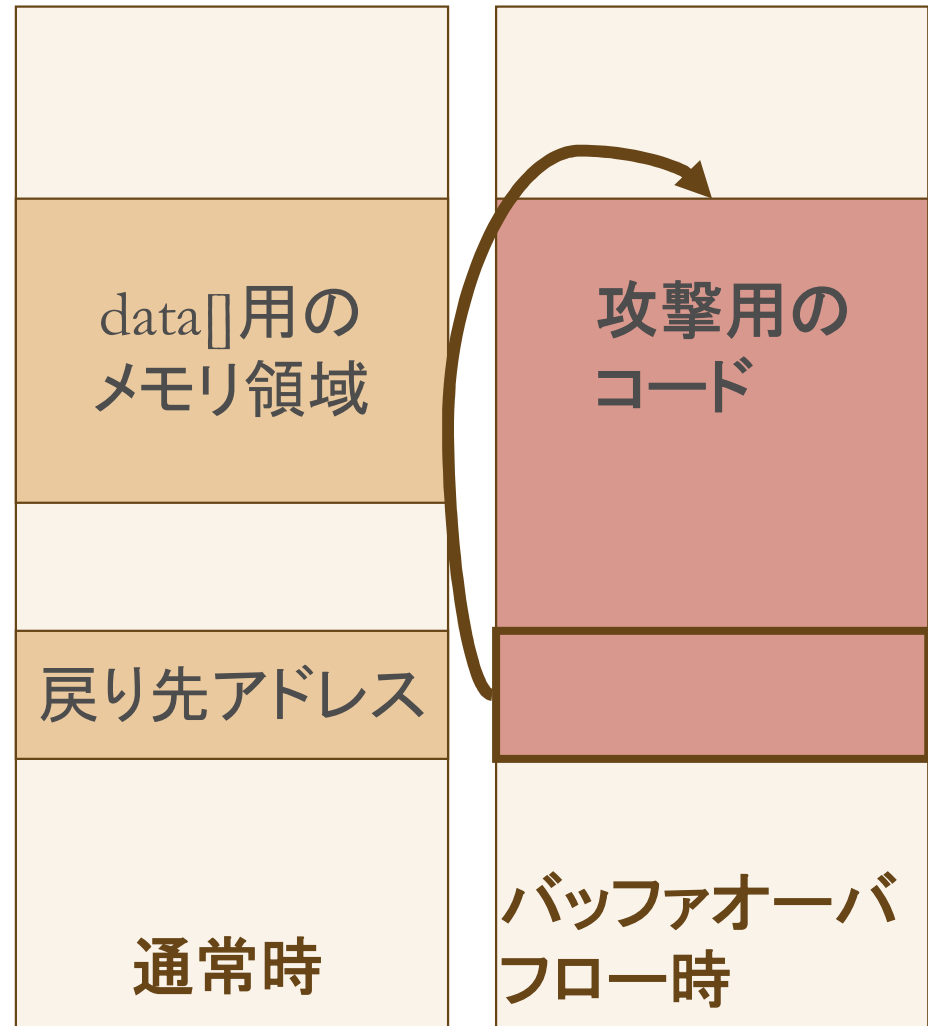
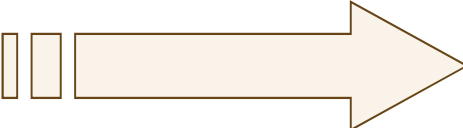
データベースを利用するウェブアプリケーションでは
フォーム入力値に対して厳密なチェックが不可欠

バッファオーバーフロー

→サービスの停止や、最悪の場合、管理者権限の奪取も

```
foo()
{
    char data[64];
    /*
     配列dataにデータを読み込む
    */
    return;
}
```

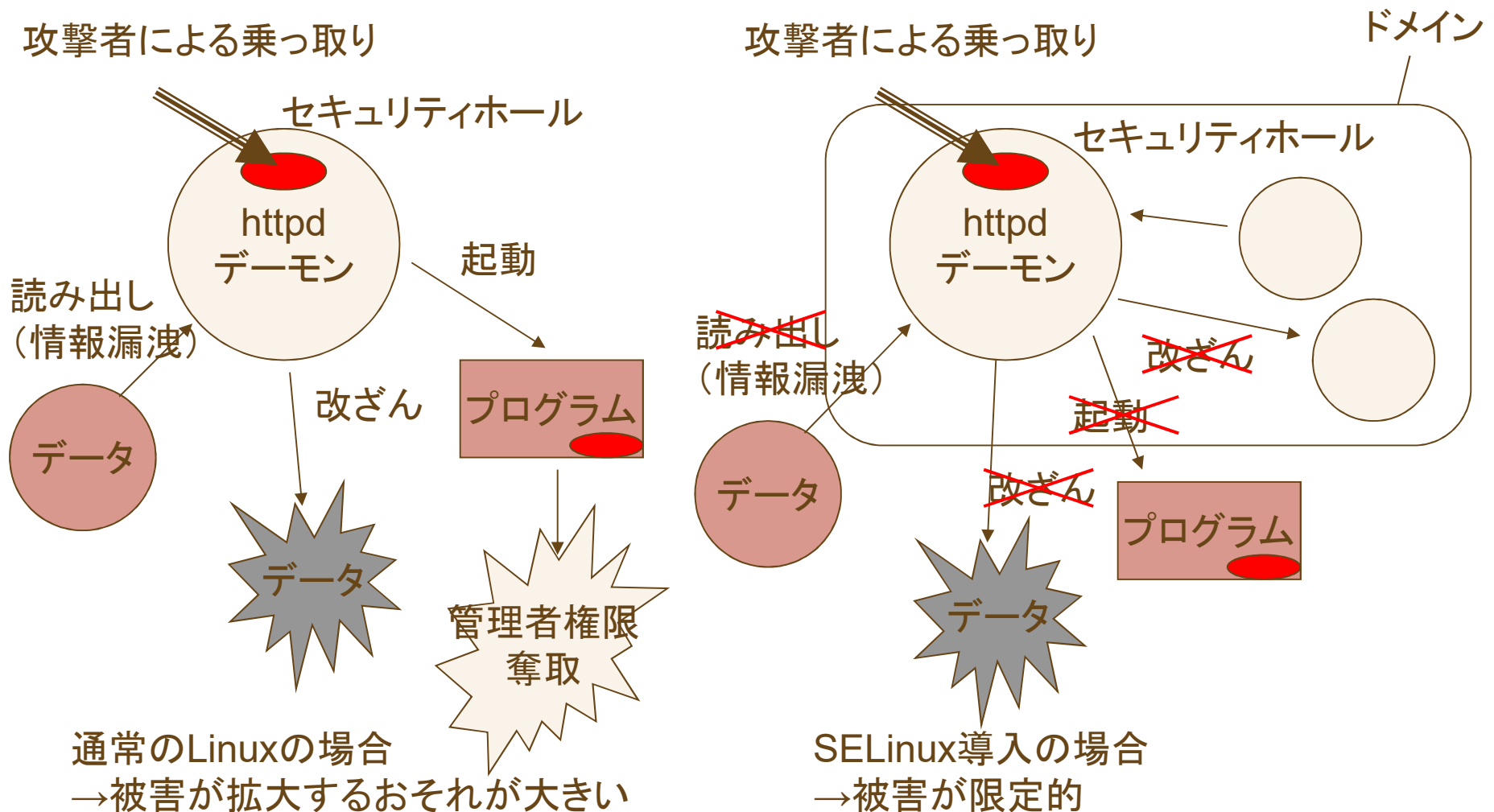
メモリイメージ



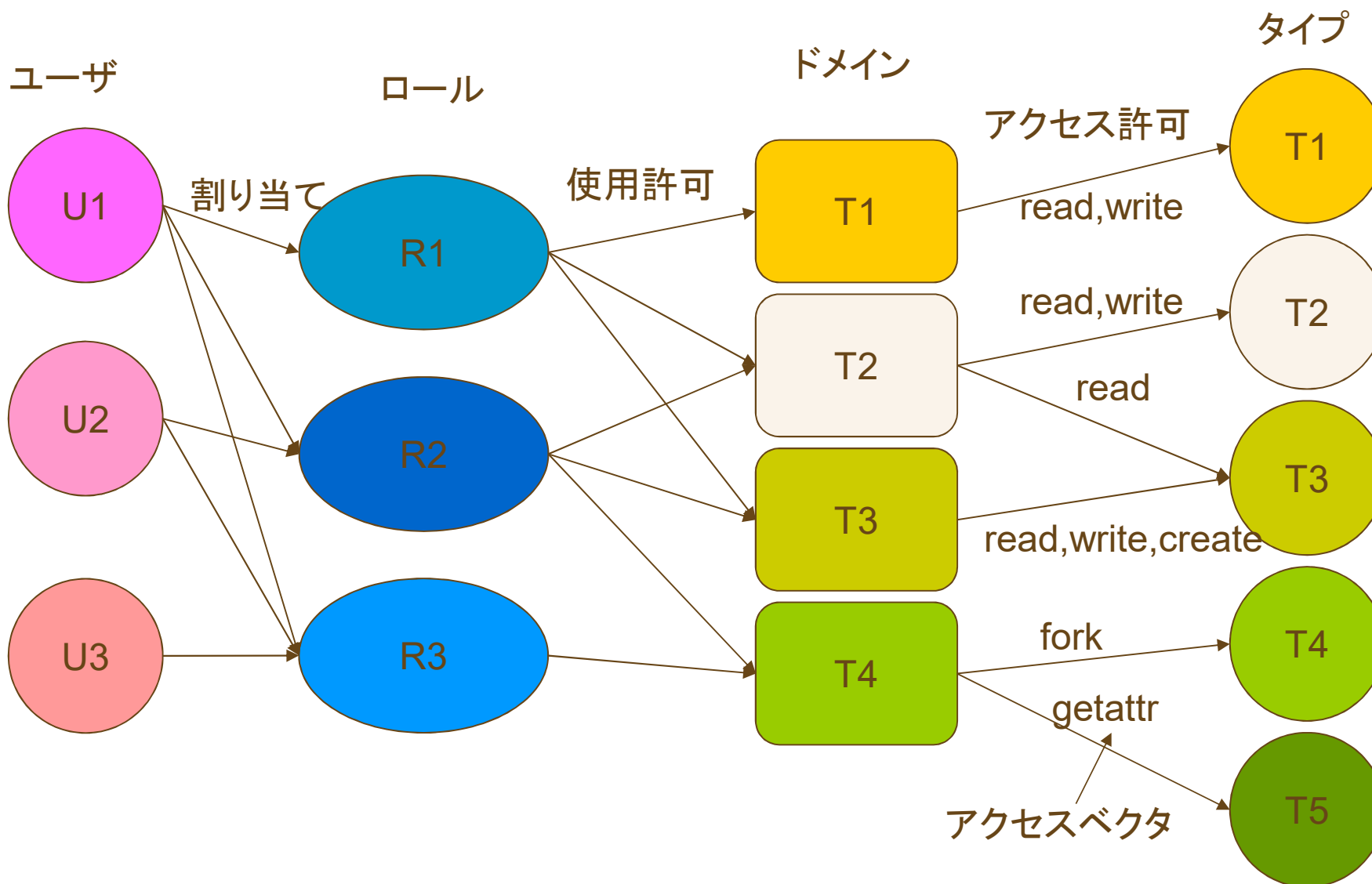
データアクセス制御の方式

- 任意アクセス制御 (DAC)
オブジェクトの所有者が利用者の属性ごとに権限を設定する
- 強制アクセス制御 (MAC)
システムが強制的にアクセス権限を決める
- ロールベースアクセス制御 (RBAC)
オブジェクトへのアクセス権限が利用者が属するロール(役割)に基づいて決まる

SELinuxによるセキュリティ強化



SELinuxの概要



ハードウェアの管理など

- サーバ、サーバールームの施錠
- BIOSパスワードの設定
- CDROM等、外部メディアからの起動禁止
- Web設定画面にログインしたままにしない
(クロスサイトリクエストフォージェリ対策)
- バックアップメディアの管理
- ハードディスクの廃棄
 - 物理的な破壊(業者による破壊サービスも)
 - ソフトウェアによる消去(通常のフォーマット処理では不十分)

セキュリティと法律

→知りませんでした、では済まない。業務では損失にも

- 不正アクセス禁止法(1999年)
 - 不正アクセス行為の禁止
 - 不正アクセス行為を助長する行為の禁止
- 電子計算機損壊等業務妨害(刑法234条)
- 電子計算機使用詐欺(刑法246条)
- 電磁的記録不正作出及び供用(刑法161条)
- 電子署名法(2001年)
- プロバイダ責任制限法(2001年)
- 特定電子メールの送信の適正化等に関する法律(2008年)
- その他、所属組織の関連規則(セキュリティポリシー、セキュリティガイドラインなど)

情報収集

- 日々、新たなセキュリティホール、Exploitコードが出現している→情報収集が重要
- セキュリティポータル
Security Focus, SANS, CERT/CC, NIST CSRC, CIRC, 警察庁@police, IPA, JPCERT
- ベンダー
Microsoft, Adobe, Symantec, F-secure, TrendMicro, McAfee
- その他
IT系各ニュースサイト,
セキュリティホールmemo