インターネットセキュリティ概要 — 技術的な視点から

NII　情報セキュリティ基礎研修

稲葉宏幸 (京都工芸繊維大学)

情報セキュリティとは

- セキュリティ上の危険や脅威から情報資産を保護し、情報システムの信頼性を高める
- 情報セキュリティマネジメントの3つの観点
  - 機密性(confidentiality)
    権限のない人は情報にアクセスできない
  - 完全性(integrity)
    情報の正しさが保証されている
  - 可用性(availability)
    (権限のある人は)必要な時に情報が利用できる

情報セキュリティの対策方法

- 技術
  暗号、ハッシュ関数、実装、バイオメトリクス
- 管理･運営
  ISO/IEC 15408, 17799
- 法制度
  不正アクセス禁止法、電子署名法、個人情報保護法、等
- 倫理･教育

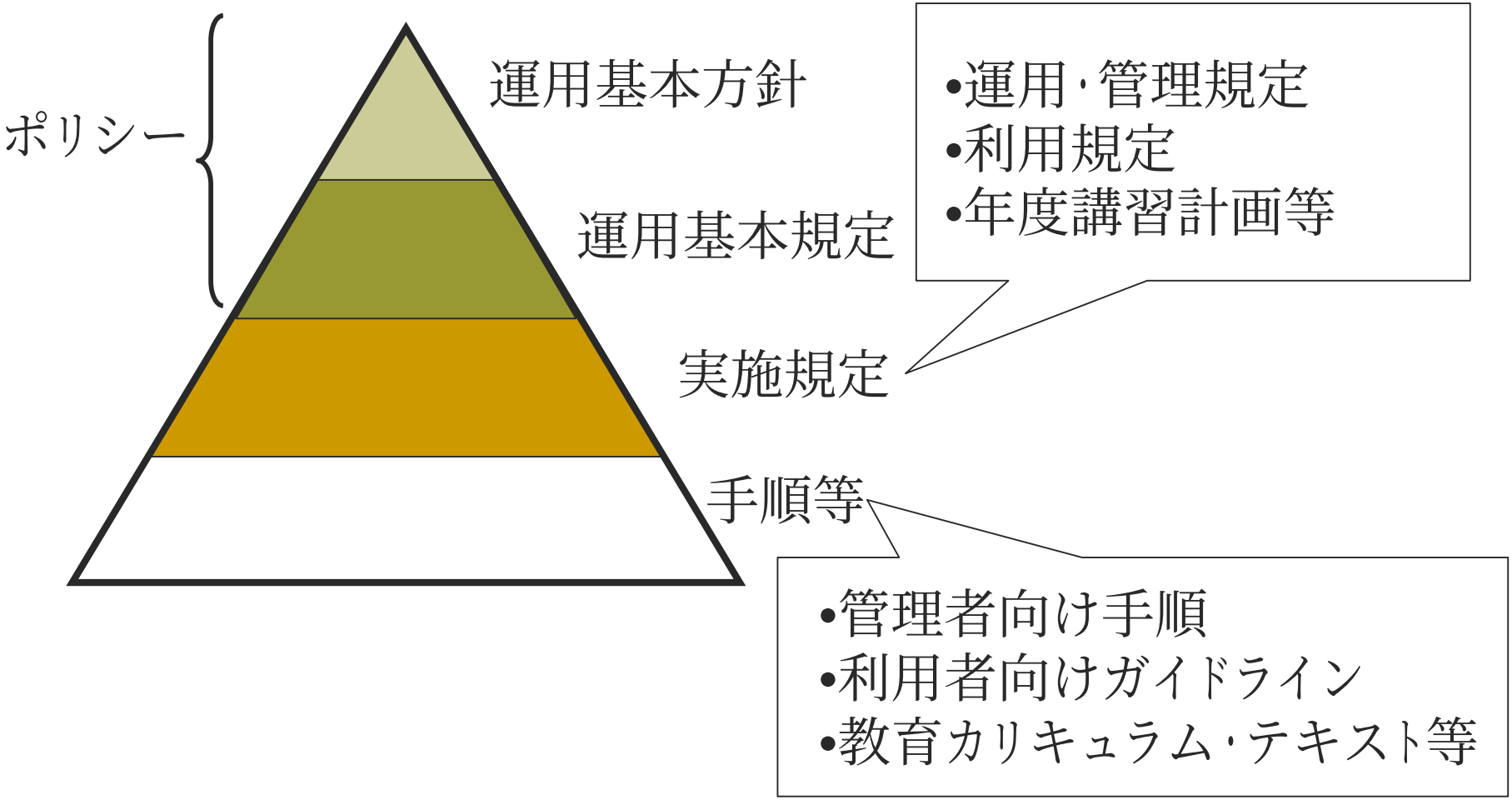
情報セキュリティの脅威に対処する段階

- 抑止
  不正者の意欲をそぐ
- 防止
  被害が発生しないように対策する
- 検出
  被害が発生してもすぐに検出できる
- 回復
  被害が発生した後すぐに正常に戻せる

高等教育機関の情報セキュリティ対策のためのサンプル規定集

- (2000/7)情報セキュリティポリシーに関するガイドライン（政府）
- (2002/5)大学における情報セキュリティポリシーの考え方（大学のセキュリティポリシーに関する研究会）
- (2003/4)高等教育研究機関におけるネットワーク運用ガイドライン（電子情報通信学会等）
- (2007/2)高等教育機関の情報セキュリティ対策のためのサンプル規定集（7大学＋NII、IEICE）
- (2007/10)高等教育機関の情報セキュリティ対策のためのサンプル規定集（２００７年度版）

サンプル規定集の構造


ポリシー
運用基本方針
運用基本規定
実施規定
手順等
•運用・管理規定
•利用規定
•年度講習計画等
•管理者向け手順
•利用者向けガイドライン
•教育カリキュラム・テキスト等

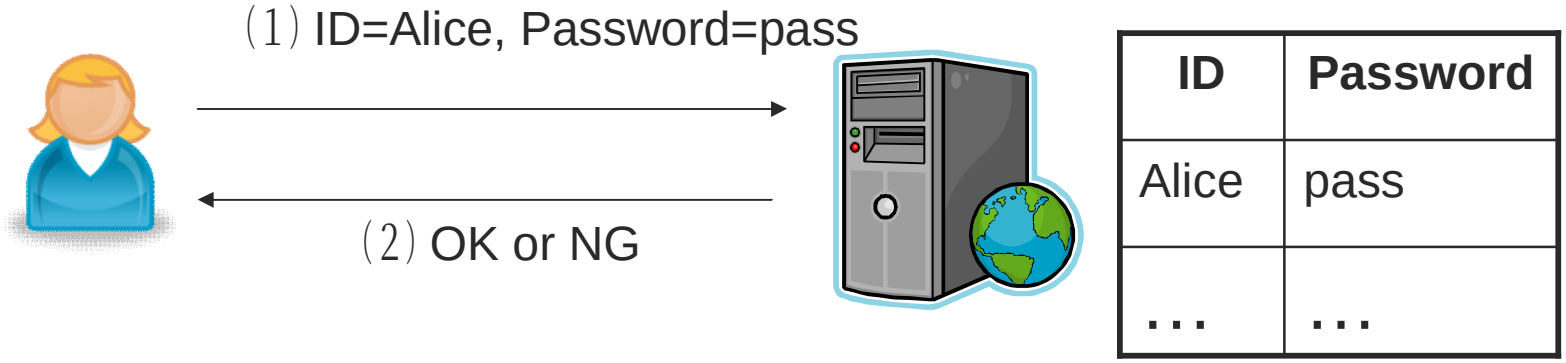
PC取扱ガイドライン

- 一般利用者向け（管理者権限なし）と特権利用者向け利用手順に分かれている
  - 学生への教育に配慮して（セキュリティと直接関係のない）倫理的な条項も含まれる
    Ex.飲食禁止、機器の破損、端末の占有等
  - アプリケーションのインストール時の注意（ウイルスチェック）
  - 重要なデータの管理（暗号化など）
  - パスワードの管理
  - セキュリティインシデントの報告

利用者パスワードガイドライン

- パスワードのつけ方
  6文字以上、
  英大小文字、数字、記号を含む、
  単語など容易に類推できるものはだめ
- パスワードの定期的な変更
  でも忘れてしまっては意味がない
- パスワードの管理
  メモしない、人に教えない
- パスワードを搾取されないように注意

パスワード認証方式 (基本)



☆パスワード認証方式に対する脅威、問題点

1. オンライン攻撃 (通信チャンネルの盗聴)

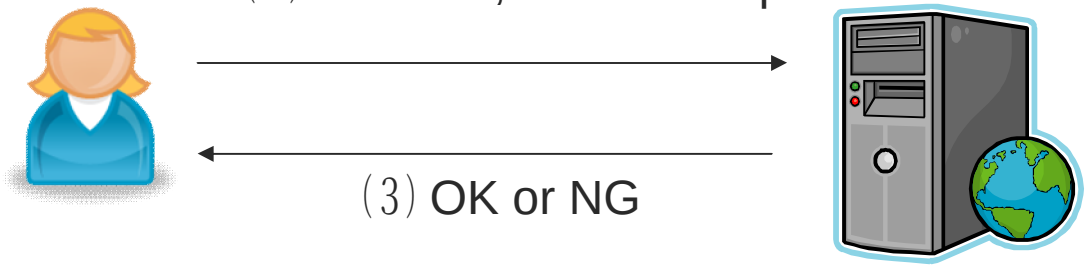
   キーボードの盗み見、スパイウェアによる監視も

2. オフライン攻撃 (サーバのデータベースの解析)

   パソコンの紛失、盗難も同じこと

3. スケーラビリティ (ユーザ数やサーバ数に対する拡張性)

パスワード認証方式（ハッシュ）

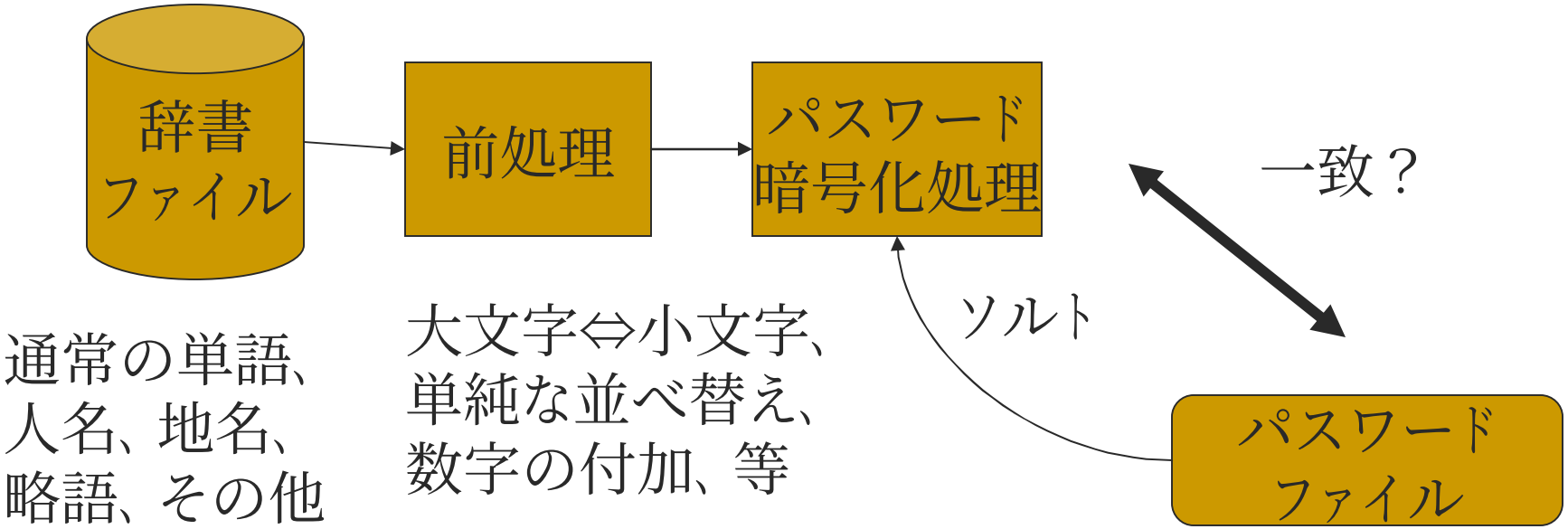


ID	Hash
Alice	#$3aBk
…	…

(2) H(“pass”)を計算、照合

- オフライン攻撃に強くなる（ソルトを使用することもある）
- オンライン攻撃には無力

パスワードクラック



- (注) 英単語 (60万語程度<20bit) 全て対象としても計算機には楽勝

ビットサイズと全数探索

事項	個数	文字数 (6bit/1文字)	ビット数	探索時間 (10^{-13}秒/1件)
地球の人口	60億	6	32	60msec
DES	7京(7×10^{16})	9	56	1.9時間
水(180cc)分子の数	6×10^{24}	14	82	19000年
AES-128	3.4×10^{38}	21	128	100万　兆年
AES-256	1.2×10^{77}	43	256	
宇宙の基本粒子数	10^{80}	44	265	

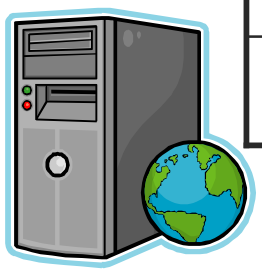
リプレイ攻撃

脆弱性を持つ例

鍵 K

(1) ID=Alice, E(K, pass)

(4) OK or NG



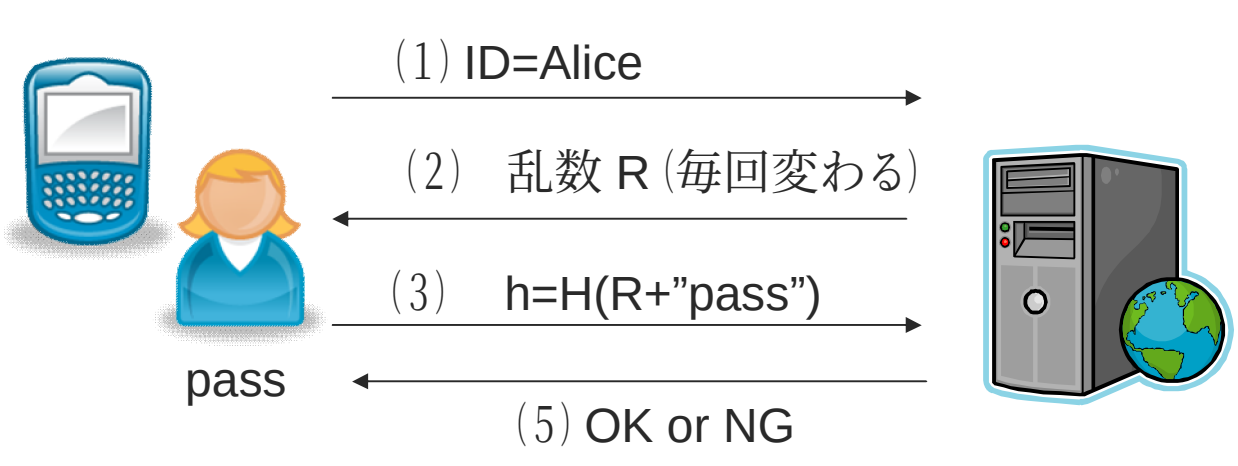
ID	Key	Hash
Alice	K	#$3aBk
…	…	…

(2) E(K,pass)を復号
(3) h(“pass”)を計算、照合

E(K, data)： 鍵Kによるdataの暗号化

- オンライン攻撃に強くなる？
- リプレイ攻撃に対して無力

チャレンジレスポンス方式

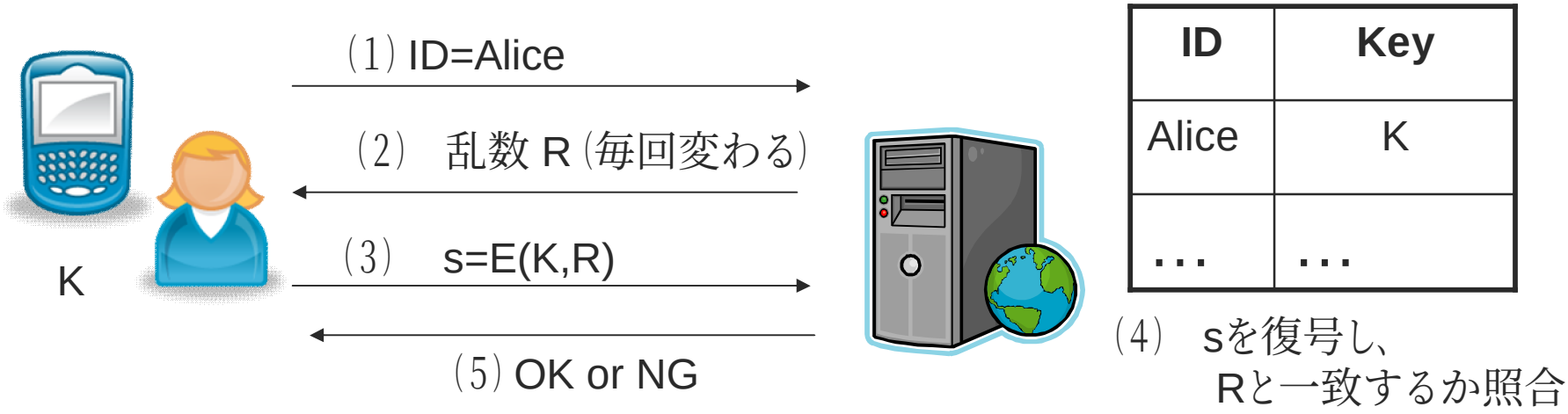


ID	Password
Alice	pass
…	…

(4) H(R+"pass")を計算、h と一致するか照合

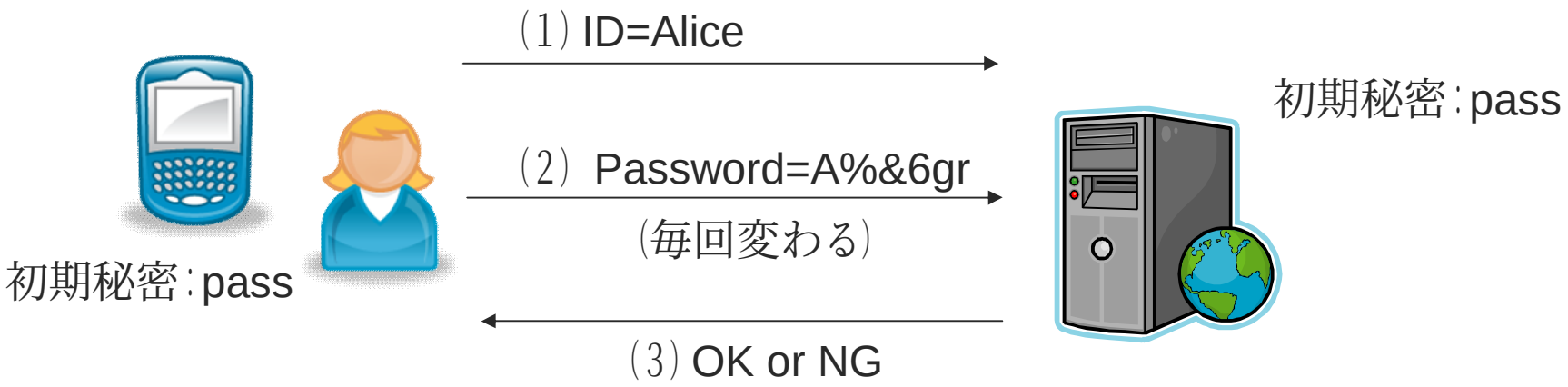
- オンライン攻撃 (リプレイ攻撃) 不可
- オフライン攻撃は可能

チャレンジレスポンス方式(2)



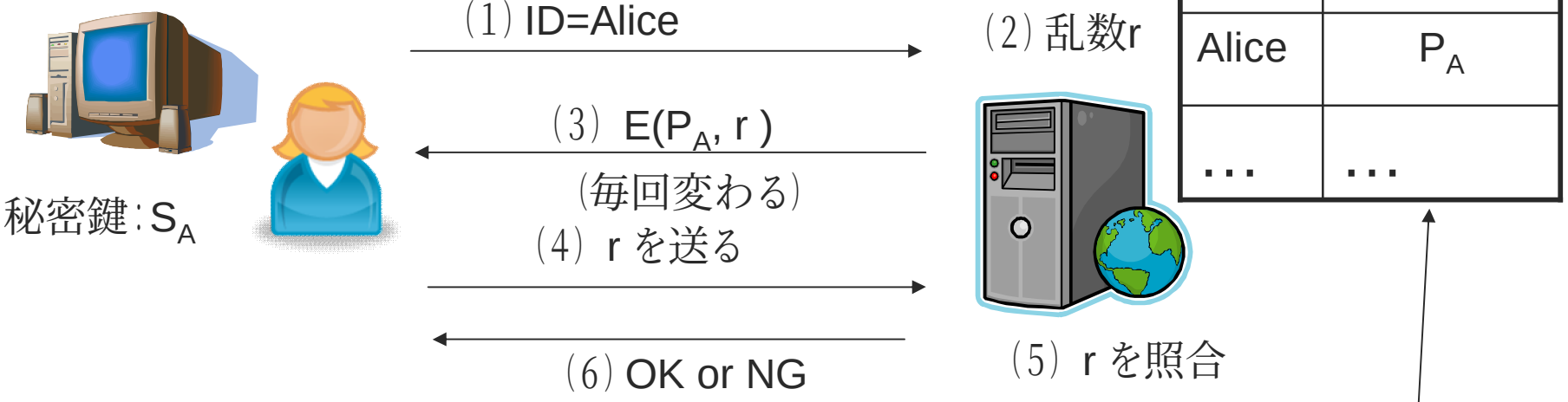
- オンライン攻撃 (リプレイ攻撃) 不可
- オフライン攻撃は可能
- 鍵情報が漏洩した場合の影響大

ワンタイムパスワード方式



- オンライン攻撃(リプレイ攻撃)不可
- パスワード計算デバイスが必要
- 定期的に更新が必要な場合も

公開鍵による方式



- オンライン攻撃(リプレイ攻撃)不可
- オフライン攻撃不可
- 秘密漏洩時の影響が小さい
- 計算量が多い

ウェブブラウザ利用ガイドライン

- 全般的な注意事項
  - 目的外利用の禁止
  - プラグインの導入、利用
  - 不適切な書き込み（個人情報、著作権、etc.）
- 閲覧時における注意
  - 偽情報、クロスサイトスクリプティング、フィッシング
  - SSL/TLS通信における注意
- フォーム送信、ファイルのアップロード時の注意
- ファイルのダウンロード時の注意
  ウイルスチェックを行う

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(認証情報など)を、悪意のあるサイトに盗み取られる

ユーザ

example.com
PASS1234

ログインパスワード

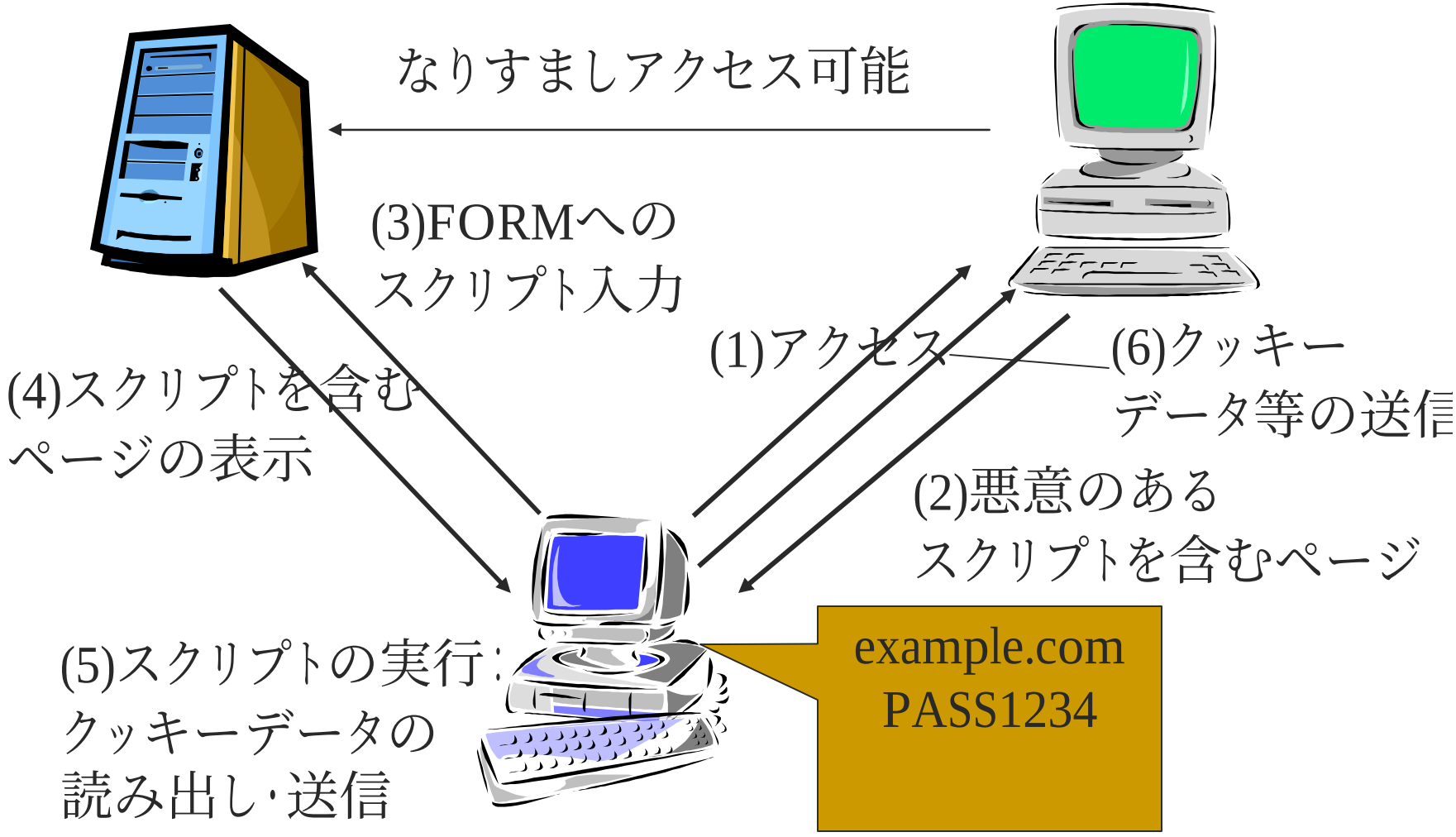
クッキー

サーバ
(example.com)

HTTPにはセッション管理がないので、クッキーを使うことが多い。

サーバ(example.com)から送られたクッキーは、そのサイトから送られたスクリプトでないと呼び出せない

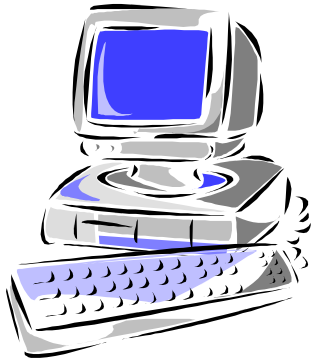
クロスサイトスクリプティング(2)



SSL（Secure Socket Layer）/TLS

- 元々Netscape社が提案したプロトコル
- httpの暗号化に主に用いられるが他のプロトコルもOK

https://……



クライアント

暗号アルゴリズム等のネゴシエーション

暗号化されたマスター鍵

ハンドシェイクメッセージの確認

公開鍵証明書のチェック

データの送受信

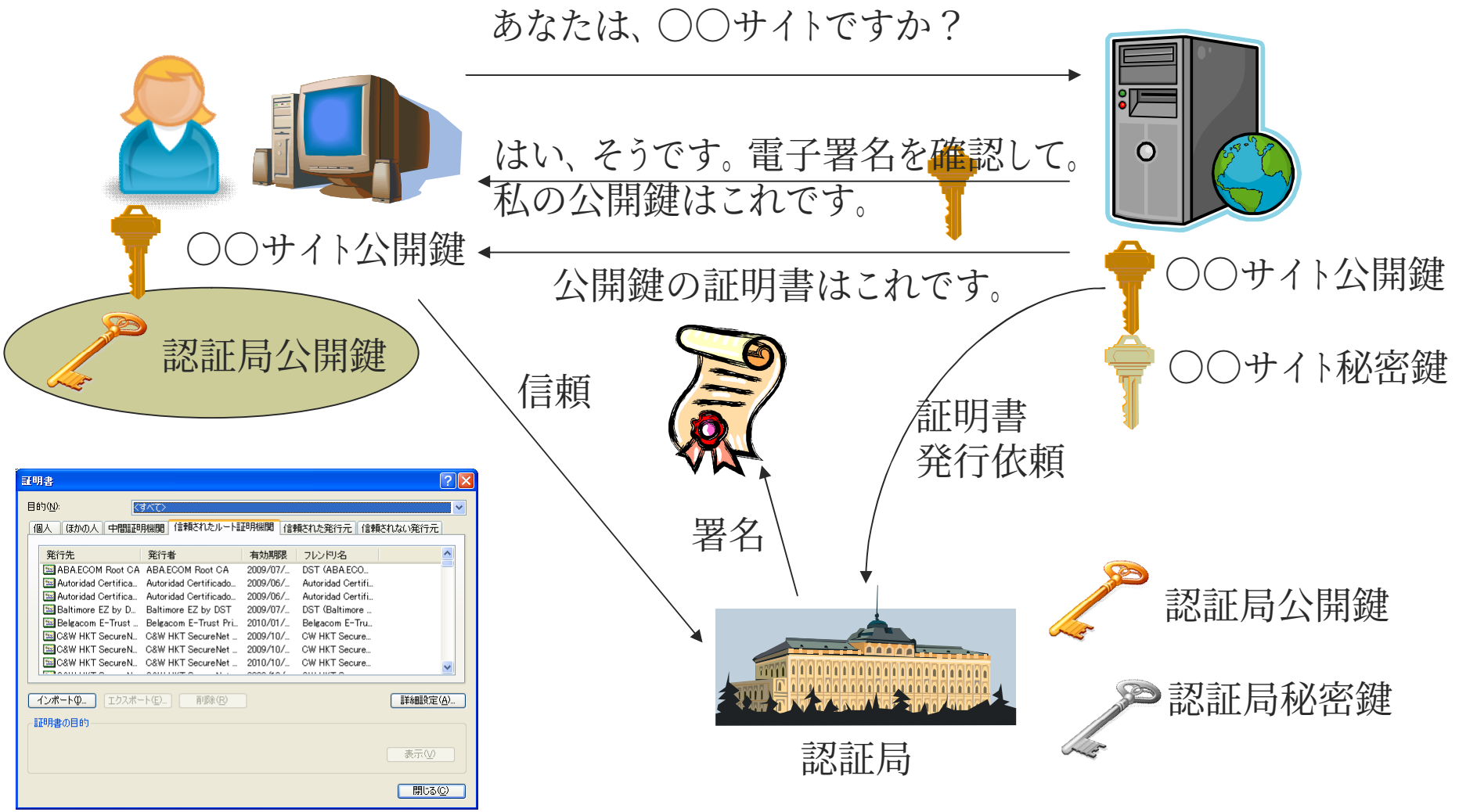
終了

終了確認

サーバ

公開鍵証明書

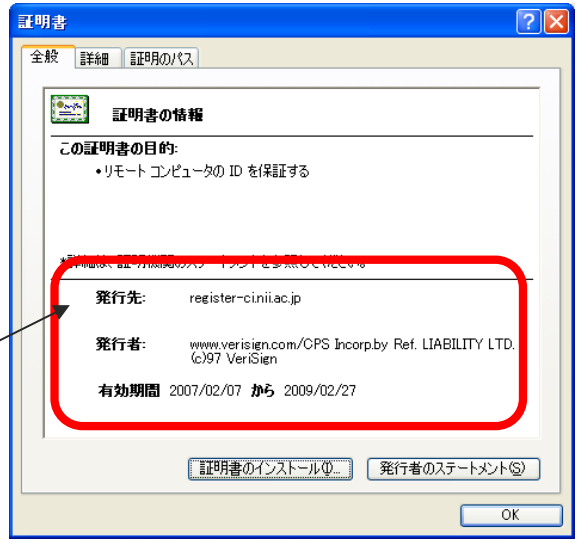
PKIとは


あなたは、○○サイトですか？
はい、そうです。電子署名を確認して。
私の公開鍵はこれです。
○○サイト公開鍵
公開鍵の証明書はこれです。
認証局公開鍵
信頼
署名
証明書
発行依頼
○○サイト公開鍵
○○サイト秘密鍵
認証局公開鍵
認証局秘密鍵
認証局

証明書
目的(N):
<すべて>
個人
ほかの人
中間証明機関
信頼されたルート証明機関
信頼された発行元
信頼されない発行元
発行先
発行者
有効期限
フレンドリ名
インポート(I)...
エクスポート(E)...
削除(R)
詳細設定(A)...
証明書の目的
表示(V)
閉じる(C)

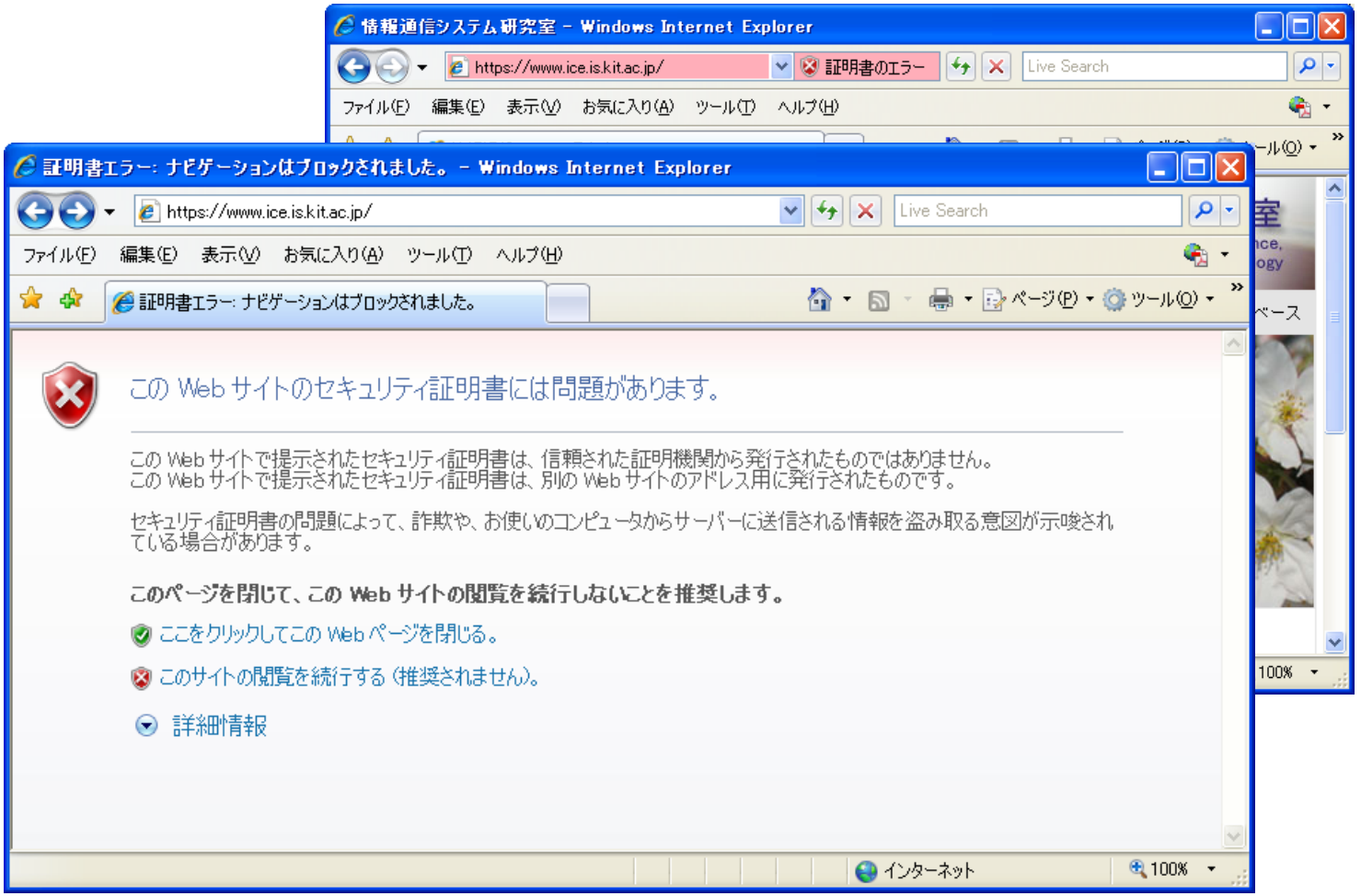
Web証明書の例

同じになる



- 発行先
- 発行者
- 有効期間

Web証明書のエラーの例



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
  - ポッド
  - スパイウェア

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、メッセンジャー、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
  - メッセン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（感染の兆候を見逃さない）
- 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

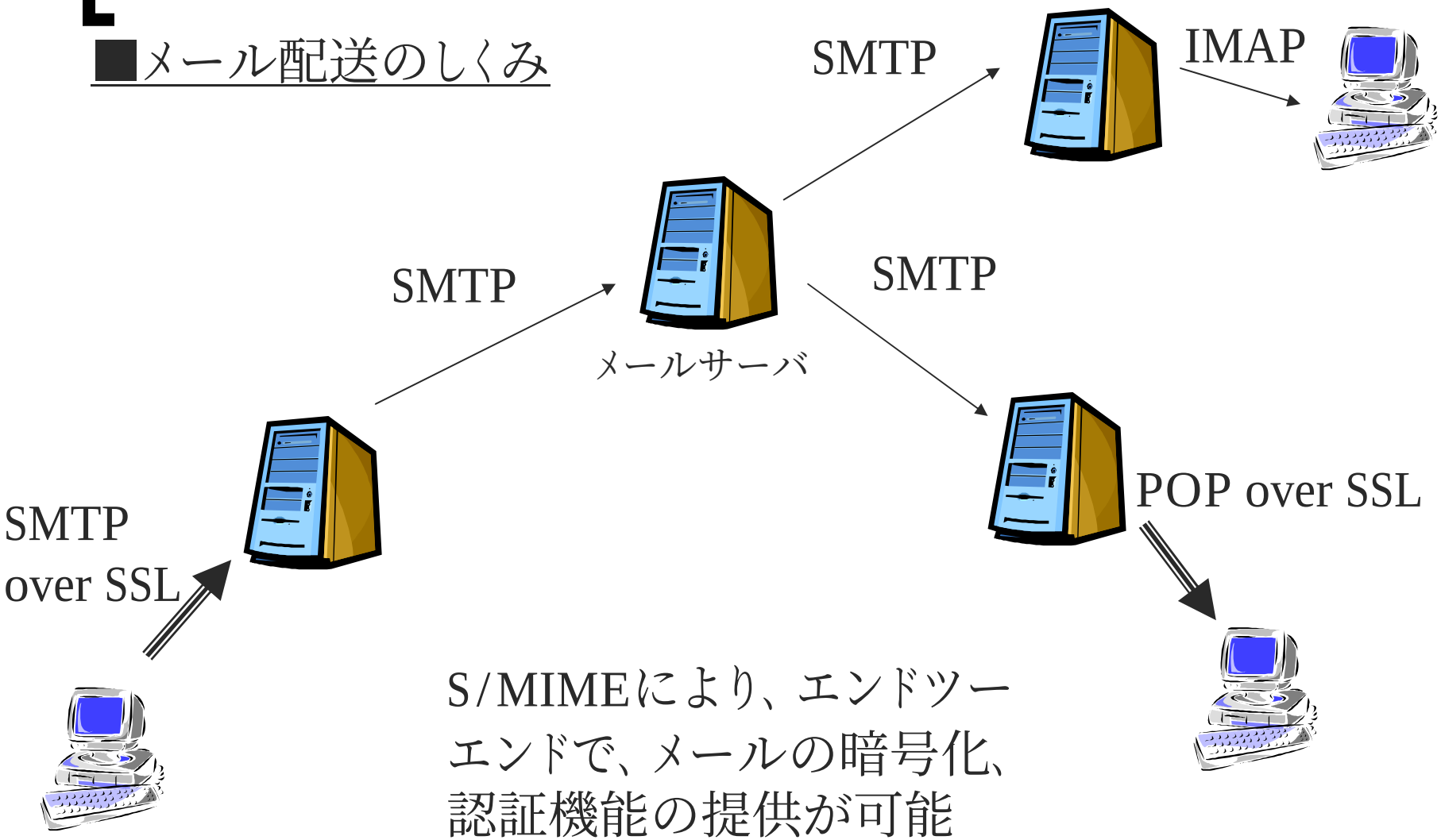
- ソフトウェアにも寿命がある
  1. 初版（またはβ版）リリース
  2. セキュリティパッチ、アップデート
  3. バージョンアップ
  4. 開発停止（メンテナンスのみ）
  5. 開発終了（メンテナンスもなし）
- 段階5のソフトウェアは原則使用できない（例：Winny）

電子メール利用ガイドライン

- 誹謗中傷の禁止、著作権への配慮、マナー的なこと
- 自動転送の禁止
- 電子メールアカウントの管理
- 添付ファイルのウイルスチェック
- HTML形式メールの原則禁止
- 暗号化メール（S/MIMEなど）の利用
- 添付ファイルの暗号化
- 不審メール、迷惑メールへの対策

S/MIME（1）

■メール配送のしくみ



S/MIMEにより、エンドツーエンドで、メールの暗号化、認証機能の提供が可能

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
  - 利用者毎にディジタル証明書(X.509)が必要
    →費用面、手続き面の問題
  - 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。

ファイルの暗号化

- OS（ファイルシステム）の機能を用いる
  - Windows EFSが有名。暗号化アルゴリズムは、DES,DESX,3DES,AES
  - ユーザは暗号化を意識せずに使える
  - コピー、外部送信時は自動的に復号される
- アプリケーションの機能を用いる
  - オフィス(Word, Excel等)、Acrobat等。暗号化アルゴリズムはRC4が多い。
  - 暗号とは呼べない場合もあるので注意
  - ファイル毎に個別にパスワード設定が必要
- 暗号化専用ツールを用いる

迷惑メール対策

- 迷惑メールの全メールに対する割合：80%以上
- 迷惑メールに返送してはいけない
  - 配送拒否はこちら、と書いてあっても
  - エラーメールを装っている場合も
- メールアドレスを晒してはいけない
  Web,掲示板,ブログ,SNS,懸賞応募等
- メールアドレスの使い分け
- 迷惑メールフィルターの利用
  分類エラーもあるので注意
- アドレスの定期的な変更

まとめ

- 情報セキュリティ対策に終わりはない
- 攻撃側も防御側も日々進歩、更新がある
  - 日々のメンテナンス：ウイルス情報更新、OS セキュリティパッチ、データバックアップ、等
  - OS、アプリケーション、機器の更新
  - セキュリティトレンド？の収集
- 最も大切なのは、人（組織）の意識

ご清聴ありがとうございました。