Webを支える情報通信技術(11)
～ サーバ証明書 ～

佐藤周行、中山雅哉、西村健

先週の復習

- 暗号技術の残り
  - ハッシュ関数
- SSL/TLS
  (Secure Sockets Layer /
  Transport Layer Security)
  - HTTPなどに暗号化の機能を提供するもの
  - プロトコル階層の間に挟む

今週の内容

- サーバ証明書

SSLの弱点って？

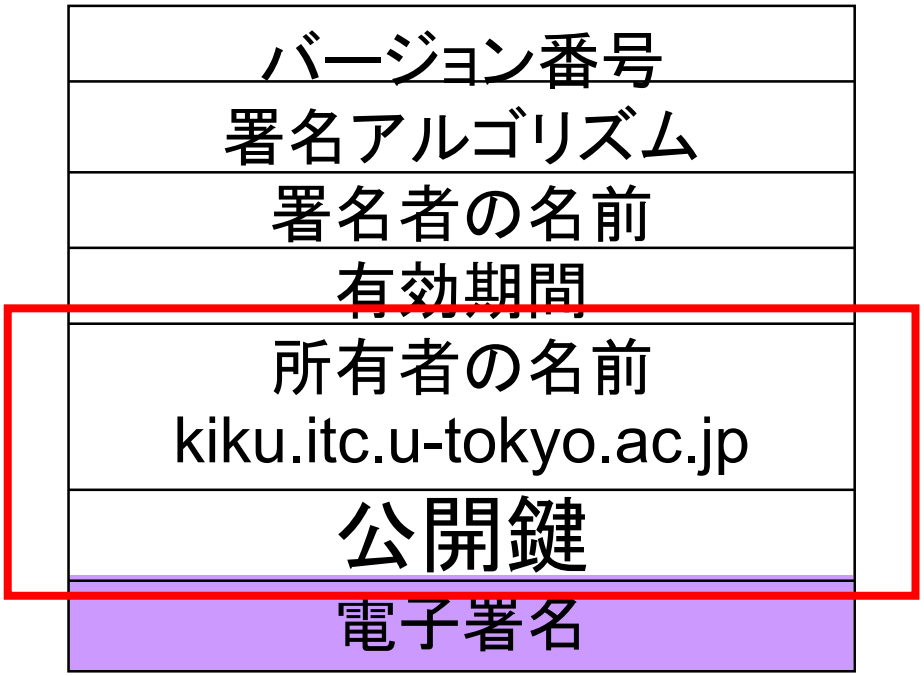
- 公開鍵（証明書）！

- （秘密鍵を厳重に管理しないといけない）

公開鍵は誰のもの？

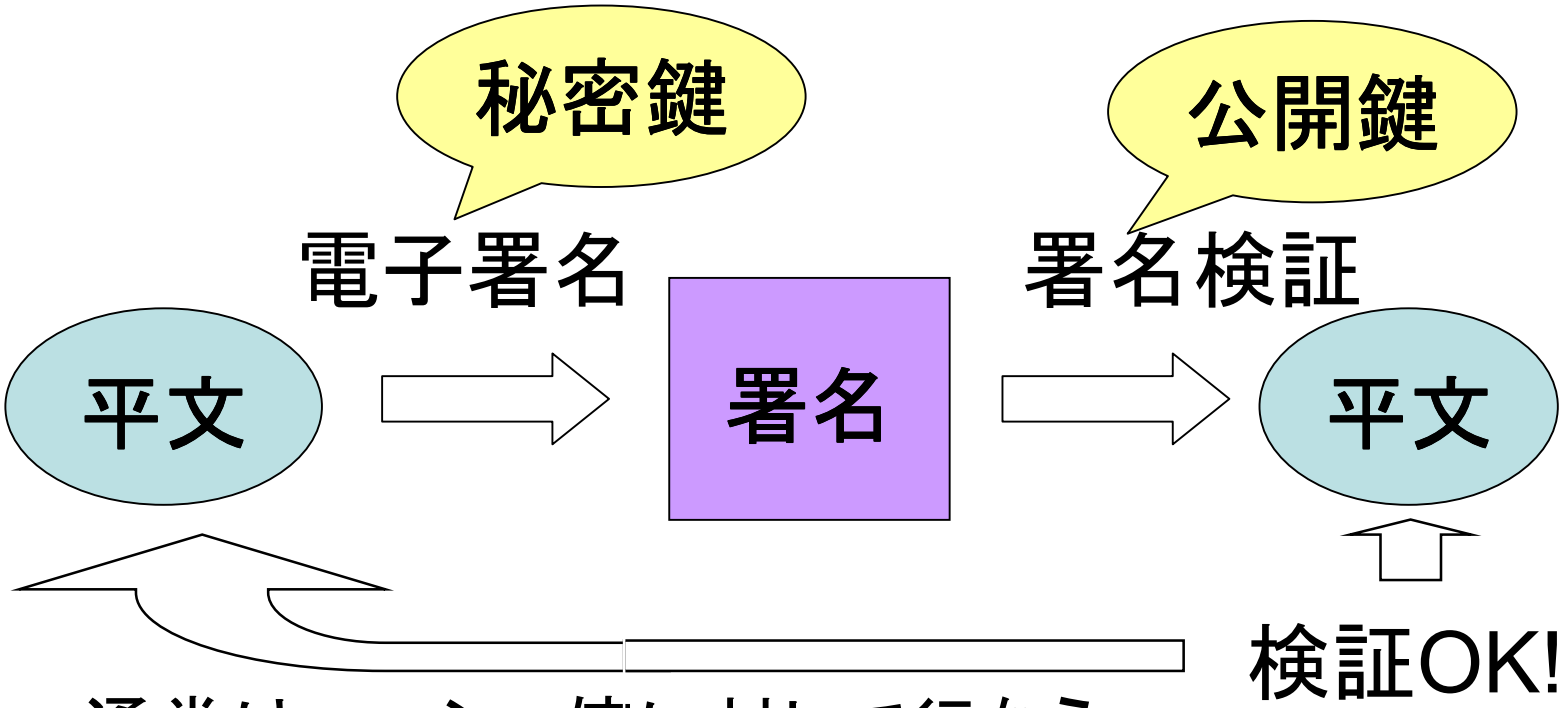
サーバ証明書

- 公開鍵証明書の一種
  - ISO/ITU X. 509, RFC 3280
- これでほんとに大丈夫？　ー　後述



電子署名

- 通信途中で改竄が行なわれていないことを確認するための方法。公開鍵暗号が使われる。



- 通常はハッシュ値に対して行なう

演習：サーバ証明書を作ってみよう

- 秘密鍵(testkey.key)が生成されていることが前提

```
$ openssl req –new –x509 –out testkey.cer
 –key testkey.key
…
Country Name (2 letter code) [AU]:JP
…
Common Name (eg, YOUR name) []:caXXXXX.ecc.u-tokyo.ac.jp
…
```

一行で書くこと

ホスト名を書く

演習：WebサーバをSSL対応に

- 作成した秘密鍵(testkey.key)、証明書(testkey.cer)をhttpdディレクトリの下に移動

以下、設定ファイル(httpd.conf)を編集

- ApacheのSSLモジュール(mod_ssl)の読み込み

```
#LoadModule ssl_module     /usr/libexec/httpd/libssl.so
---
LoadModule ssl_module      /usr/libexec/httpd/libssl.so
```

```
#AddModule mod_ssl.c
---
AddModule mod_ssl.c
```

- ポート番号の変更

```
Port 8080
---
Port 10443
Listen 10443
```

- サーバ名の設定

```
#ServerName new.host.name
---
ServerName caXXXXX.ecc.u-tokyo.ac.jp
```

- SSL関連の設定（元ファイルにはないのでファイル末尾に追加）

```
SSLPassPhraseDialog builtin
SSLSessionCache dbm:ssl_scache
SSLSessionCacheTimeout 300
SSLMutex file:ssl_mutex
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
SSLLog ssl_engine_log
SSLLogLevel info
SSLCertificateFile testkey.cer
SSLCertificateKeyFile testkey.key
SSLEngine on
```

- Webサーバの停止と起動

```
$ httpd/apachectl stop
…
$ httpd/apachectl start
…
```

- openssslコマンドでアクセスしてみる

```
$ openssl s_client –connect caXXXXX.ecc.u-tokyo.ac
.jp:10443 –state
…
GET / HTTP/1.0
…
```

- Firefoxでアクセスしてみる

```
https://caXXXXX.ecc.u-tokyo.ac.jp:10443/
```

- Safariでアクセスしてもうまくいかない