

情報セキュリティ特論

第6回

第6回：情報リテラシー

今回の目標

- ・ セキュリティに関する情報リテラシー
- ・ デジタルフォレンジック



1. セキュリティに関する情報リテラシー

インターネットにおけるセキュリティ

そのURLは安全か？

Hogehoge大学の公式サイト

www.hogehoge.ac.jp

これが正しいhogehoge大の公式サイトであることの証明と管理

1. セキュリティに関する情報リテラシー

URLの安全を保障する仕組み

- PKI (Public Key Infrastructure): 公開鍵基盤

サーバ（サイト）の存在証明

- DNS (Domain Name Server): ネームサーバ

サーバの名称、ドメイン名の管理



PKI: 公開鍵基盤

サーバ（サイト）の存在証明

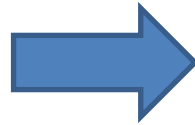
hogehoge大学の公式サイト

www.hogehoge.ac.jp

ブラウザで見るとURLの欄が

<https://www.hogehoge.ac.jp>

となっている。

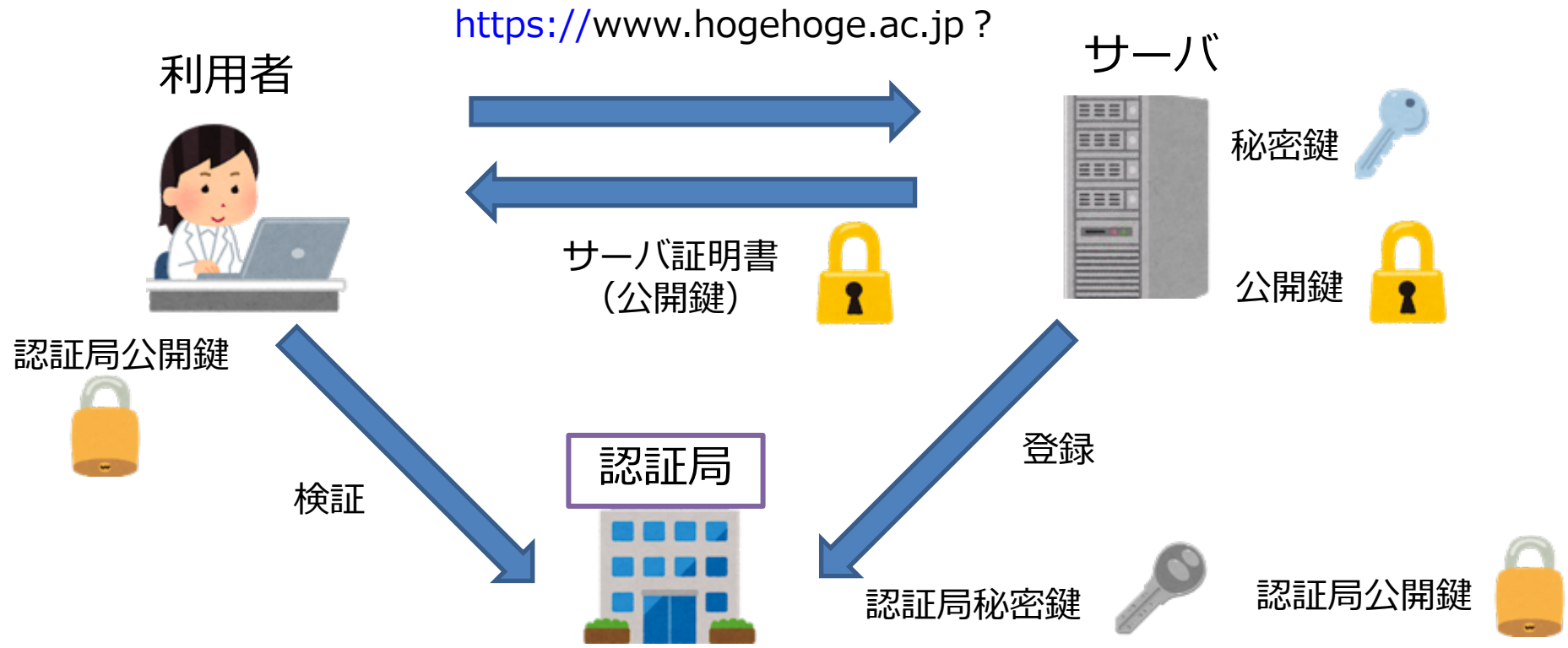


「実在性」がこれによって担保されている

PKI: 公開鍵基盤

<https://www.hogehoge.ac.jp>

サーバ証明書

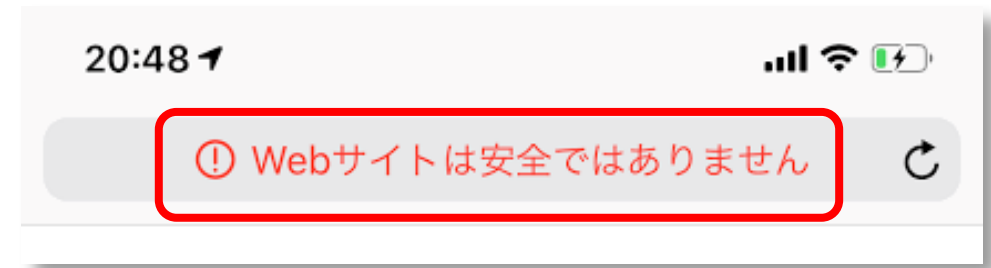


PKI: 公開鍵基盤

<http://www.hogehoge.ac.jp>

これにはその仕組みが入らない

ブラウザが「これは安全ではありません」と警告を出すのはそのため。



現在はほぼ全ての公式サイトがサーバ証明書を使用。

DNS: ネームサーバ

名前の管理

hogehoge大のドメイン

(インターネット上の住所のようなもの)

hogehoge.ac.jp

下位  上位

勝手に同じ名前を名乗らないように、上位ドメインがその下位ドメインの名前を管理する。

hogehoge大はhogehoge.ac.jp以下を管理

例) 公式サイト: www.hogehoge.ac.jp

学生用メール: st-mail.hogehoge.ac.jp

シングルサインオン: sso.hogehoge.ac.jp

電子メールのセキュリティ

- ・メールアドレスの信憑性

なりすましメール（送信者偽装）



- ・メール送受信時の暗号化

通信経路の暗号化（とくに無線LAN）

メール本体の暗号化（PGP, S-MIME）



- ・ウィルス対策

ウィルス除去サーバ

エンドポイントセキュリティ（アンチウィルスソフト）



メールアドレスの信憑性

インターネット上でメールを送受信するにはSMTPと言われるプロトコルを用いる。

(SMTP: Simple Mail Transfer Protocol)

これはインターネット黎明期からある仕組みで
「なりすまし防止」や「暗号化」等の直接の実装が無い。

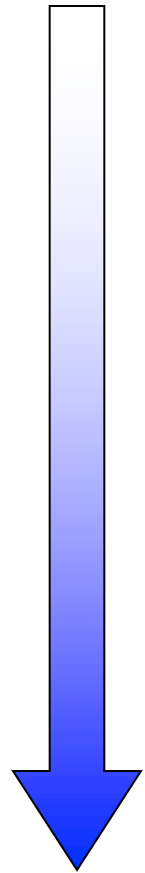
(「古き良き時代」の名残りを使い続けている状態)

なりすまし防止にはメール配送時にDNSで送信メールサーバが
実在するかを確認する仕組み (SPF等) を用いる。

しかし、実在するメールサーバからSPAMメールを送りつけられる
ような場合に対しては無力である。



無線LANの暗号化



WEP

- 最もポピュラーな暗号化
- 暗号鍵が固定⇒簡単に解読されてしまう

TKIP

- 鍵を定期的に変更

AES

- 鍵を定期的に変更
- 複雑な暗号化

認証: WPA, WPA2, WPA3

セキュリティが高い

メール送受信時の暗号化

- ・通信経路の暗号化

無線LANの暗号化

WPA2, WPA3

Passkey(SSIDのパスワード) が漏れると傍受されてしまう



サーバ通信の暗号化

<https://www.hogehoge.ac.jp> (hogehoge大の公式サイト)

実在性のみならず、暗号化 (SSL通信) も行う

SSL: Secure Sockets Layer



メール送受信時の暗号化

- ・メール本体の暗号化

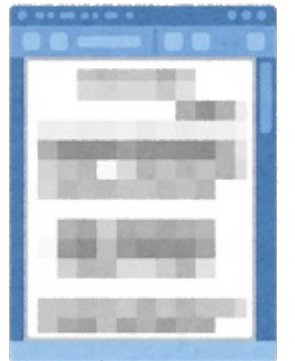
メール送信時に送信者がメールを暗号化しておき、受信時に受信者が復号する。

PGP (Pretty Good Privacy)

S-MIME (Secure Multipurpose Internet Mail Extension)

問題点

- 送信先ごとに違う公開鍵が必要
- Webメールには使えない



2. デジタルフォレンジック

「フォレンジック」とは

直訳的には「法科学」となるが、意味合いとしては「法的問題解決における科学技術」である。

サイバー犯罪あるいは犯罪に情報機器が用いられた場合に
証拠物件・捜査対象としてデジタルフォレンジックを適用する。

PCやサーバ、携帯端末内の記憶装置（HDD、SSD、フラッシュメモリ等）
から必要なデータを抜き出す。

