A20　情報保護の技術

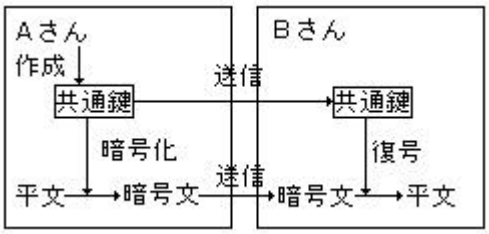
2002.5.8 資料

7091－1072　萩原 尚史

1、PKI（Public Key Infrastructure）による暗号化

1-1 共通鍵暗号方式

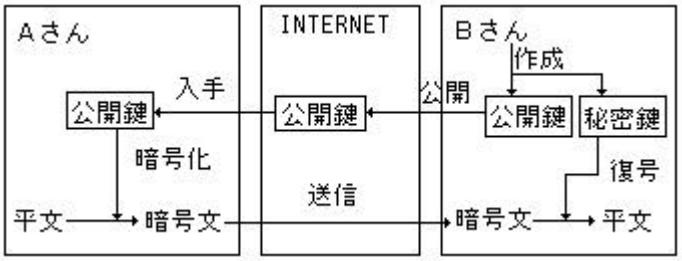
・メッセージの送信者・受信者が共通の鍵を使って暗号化と復号を行う方式。



・前提として、送信者は受信者に共通鍵を送信しなければならず、オンライン上では安全性に欠ける。

1-2 公開鍵暗号方式

・暗号化のための公開鍵と、復号のための秘密鍵の二種類の鍵（鍵ペア）を用いる方式。



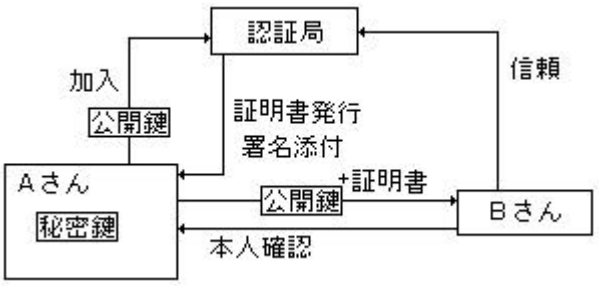
・複雑な処理を行う為、暗号化、復号に時間がかかるという欠点がある。そのため、公開鍵方式で共通鍵を送信、以降は共通鍵方式でメッセージのやりとりを行う場合もある。

1-3 デジタル署名

・秘密鍵で署名を生成、受信者は公開鍵で署名を検証することでメッセージの改竄を検出できる。

2、認証局

・公開鍵の所有者を確認・保証し、証明書を発行する機関。CA（Certification Authority）という。
加入者の公開鍵に認証局の署名を付与し、受信者は認証局の情報と照合することで本人確認が可能。



・デジタル証明書（電子証明書）

一般に、公開鍵証明書のことを指す。X509 という ISO／IEC の国際標準規格で定められている。

3、SSL（Secure Socket Layer）

・web ブラウザと web サーバ間でやりとりされるデータを保護するプロトコル。保護されているページはアドレスが「https」で表示される。

・特徴として…（1）セキュリティ・パイプを構築することで、ブラウザとサーバ間の情報を暗号化。

（2）サーバ情報が認証されているため、ユーザは閲覧しているページの正当性を確認できる。

4、web ページにおけるパスワードの認証

・上記の SSL や、チェック機能をもつサーバ（NCSA httpd や Apache）であればパスワードは暗号化されるが、ＣＧＩを利用した簡単なパスワード認証もあり、全てが暗号化されるわけではない。

5、クッキーの設定

・web サイト閲覧の際にユーザのハードディスク内に保存される情報のことで、その内容に応じて表示内容を変化させることができる。

注）**1-3** 電子署名とデジタル署名は異なる意味を持つ。

電子署名は国により様々に定義され、デジタル署名を包括する署名として位置付けられている。

【参考資料】

IPA セキュリティセンター＞PKI関連技術解説

：http://www.ipa.go.jp/security/index.html

COMPUTER WORLD.jp＞キーワード解説 SSL

：http://www.computerworld.jp/resource/keyword/back/20001026.html

とほほのwww入門

：http://tohoho.wakusei.ne.jp/

KENT WEB

：http://www.kent-web.com/