問題番号：Ａ１３（Ｐ５０～Ｐ５１）

２００３年5月１６日　日比担当分

問題のテーマ：セキュリティ技術

概論

◇セキュリティ技術の必要性

インターネットは世界中のコンピュータとつながっている

→個人情報の漏洩、盗聴、なりすましなどのネットワーク犯罪が起こっている

→防ぐためのセキュリティ技術が必要

問題について

◇暗号化

内容を暗号化することによって、情報を盗み見られても内容が分からないようにする

○暗号化の方式

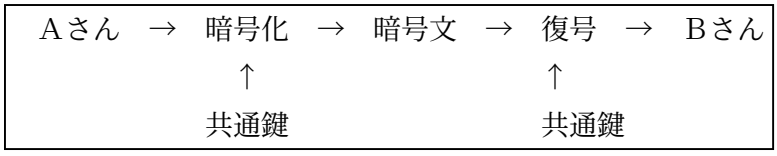
①秘密鍵方式（共通鍵方式）

・暗号化と復号を共通の鍵で行う。そのため、送り手と受け手が鍵を共有する

→鍵の所持者しか、暗号化も復号もできない

・通信前に相手に安全な方法で秘密鍵を渡さなければならない

・送受信者ごとに異なる鍵が必要となる。



②公開鍵方式

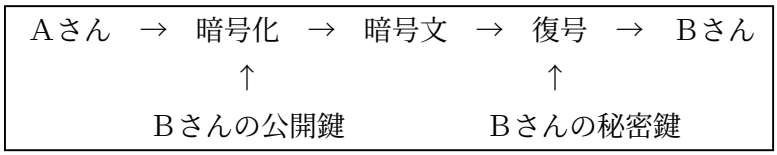
・暗号化と復号を別の鍵で行う

・復号鍵は秘密（秘密鍵）にし、暗号化鍵は公開（公開鍵）する

→暗号化は誰でもできるが、復号できるのは秘密鍵の所持者だけ

・鍵を安全に渡すことができる

・受信者ごとに鍵を作る必要がない



◇ディジタル証明書

信頼できる第三者機関（認証局）が発行する暗号文書

○特徴

・公開鍵暗号方式を利用している

・暗号化鍵を秘密（秘密鍵）にし、復号鍵を公開（公開鍵）する

→公開鍵で復号できるのは、秘密鍵で暗号化したデータだけ

→秘密鍵の所持者が送ったデータだと保証される

・送信者を特定できるため、なりすましを防ぐことができる

・ユーザの公開鍵の正当性を保証できる

・送信者が信頼できるかどうかは保証されない

○手順

１．送信者（Ａさん）がディジタル証明書の発行を認証局に申請する

２．認証局が身元の確認後、送信者（Ａさん）にディジタル証明書を発行する
同時に送信者の秘密鍵と公開鍵を作成する

３．送信者（Ａさん）が秘密鍵で暗号化したデータに
ディジタル証明書を添付して送信する

４．受信者（Ｂさん）はディジタル証明書に記載された認証局にアクセスし、
認証局の公開鍵を入手する

５．受信者（Ｂさん）は認証局の公開鍵でディジタル証明書を復号し、
送信者（Ａさん）の公開鍵を取り出す

６．受信者（Ｂさん）は取り出した公開鍵を使ってデータを復号する

（注）一連の作業はメーラが自動的に行ってくれる

◇ＳＳＬ

ＷｅｂサーバーとＷｅｂブラウザ間でデータを暗号化して送受信するために
開発されたセキュリティ通信のための通信プロトコル。
基本的に上で説明したディジタル証明書と同じしくみ。

参考資料

・『図解　ネットワークセキュリティのしくみ』、ディー・アート（２００１）

ディジタル証明書の仕組み