情報セキュリティ

大阪工業大学
情報科学部

情報セキュリティ

1. 暗号とその適用
2. 電子認証とPKI
3. 共通鍵暗号とDES暗号
4. 整数論
5. 公開鍵暗号とRSA暗号
6. ディジタル署名とハッシュ
7. ネットワーク接続時の脅威
8. ネットワーク接続時の対処
9. 情報技術の利用者、開発者の責任

1. 暗号とその適用

ネットワークのオープン化

以前のネットワーク

クローズドネットワーク

例：電話網、銀行のネットワーク、みどりの窓口

セキュリティ上の脅威：利用上の不正（なりすまし等）

今日のネットワーク

オープンネットワーク

例：インターネット

セキュリティ上の脅威：ネットワークサービスの構成要素（情報、利用者、システム）すべてに亘る

ネットワークでの不正、脅威

不正の対象	不正の内容	対策例
情報	盗聴、漏洩	暗号化
	改ざん	メッセージ認証
	財産権の侵害（違法コピー）	電子透かし
利用者、行為	なりすまし	（個人）認証
	事実否認	電子公証
システム	不正使用	通過制御、侵入検知、認証、権限チェック
	サービス妨害	

5

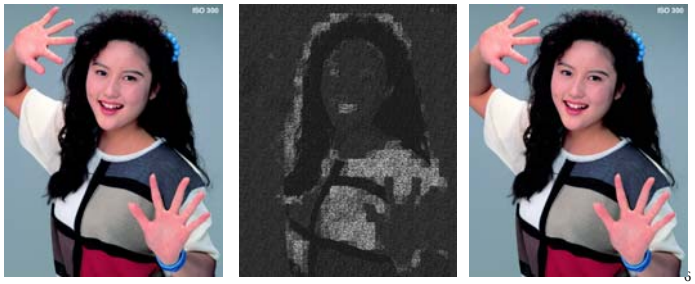
電子透かし

電子透かしの目的

コンテンツ利用者に気付かれない形で著作権表示を行い、コンテンツの違法使用を防止する

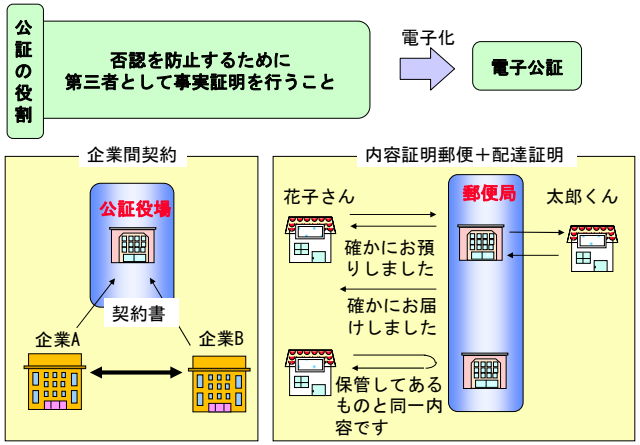
電子透かしの例

オリジナル画像　　差分データ　　透かし入り画像



6

電子公証



7

暗号、認証の利用

○ アプリケーションサービス

電子行政、電子政府（住民サービス*、電子入札、特許出願*）
電子商取引（受発注、電子決済、電子マネー）
企業内システム（電子決裁、ERP）
金融システム、証券システム
交通システム（鉄道、道路、航空）、物流システム
医療システム、保険システム

○ ネットワークサービス

Web（SSL）、電子メール、シリアル接続（PAP, CHAP）、VPN、IPセキュリティ、リモートアクセス（SSH）、携帯電話、無線LAN

○ ネットワーク不正アクセス対策

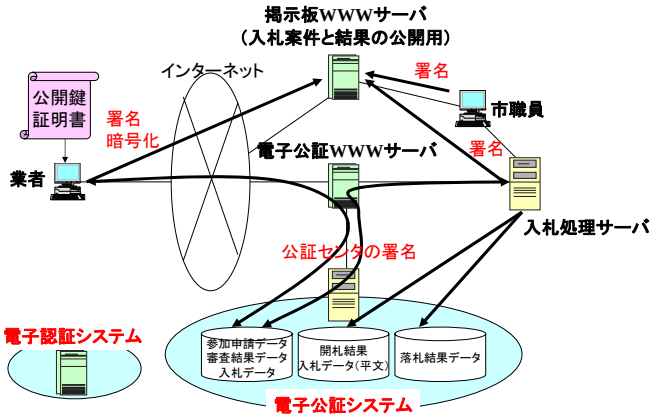
ファイアウォール、アクセス制御、経路制御

○ 放送

ディジタル放送、衛星放送

8

電子入札



★ ［注］電子公証システムの利用者は電子認証システム（CA）が発行する公開鍵証明書が必要

9

ICカードの定期券・乗車券

暗号技術を利用して、以下を実現
- ○ 定期券・乗車券の正しさ
- ○ やり取りする情報の保護

事業者	呼称
JR東日本	Suica（スイカ）
JR西日本	ICOCA（イコカ）
スルッとKANSAI協議会	PiTaPa（ピタパ）

定期券・乗車券と
改札口の間で情報
を安全にやり取り

10

電子マネー

暗号技術を利用して、以下を実現
- ○ ICカードの正しさ
- ○ やり取りする情報の保護

事業者	呼称
ビットワレット	Edy
JCB	QUICPay（クイックペイ）
VISA	VISAキャッシュ
Mondex	モンデックス

電子マネーのカード入手

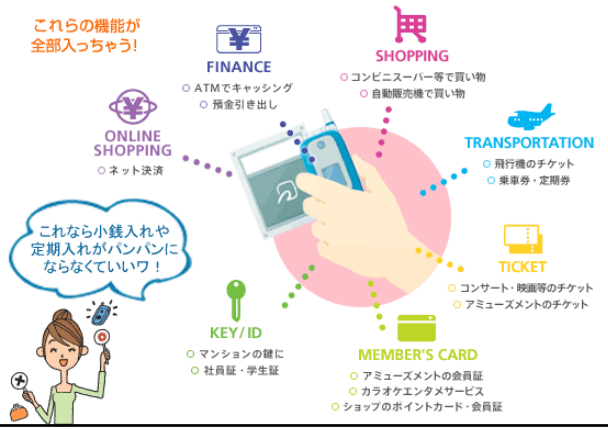
電子マネーのチャージ

電子マネーによる購入

11

携帯電話の高機能化

DoCoMoのおサイフケータイも暗号技術を利用してサービスを実現



12

Webアクセス

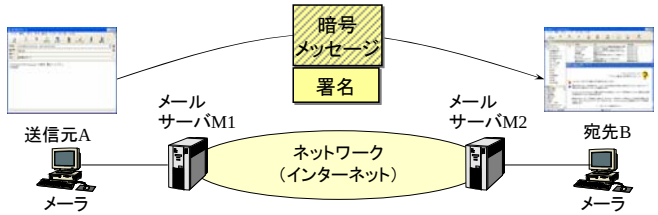
ネットショッピングなどの電子商取引にも暗号技術が必要（情報保護とサーバ認証）

13

電子メール

安全な電子メールの送受信にも暗号技術が必要

- ネットワークを流れる情報は容易に盗聴可能 ⇨ 暗号化
- 電子メールアドレスは容易に偽造可能 ⇨ 署名

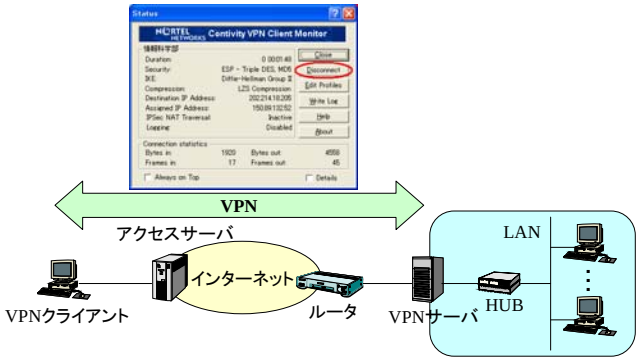


14

VPN

VPN(Virtual Private Network)

- インターネットなどに設置した仮想的な専用線
- アクセス元の認証、通信路の暗号化により実現

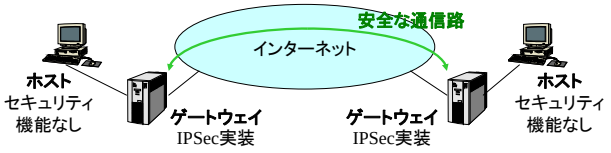


15

IPセキュリティ

ネットワーク層でのセキュリティ機能（IPSec）

- 送受信間の相互認証
- 通信路の暗号化
- IPv4とIPv6の両方での利用が可能

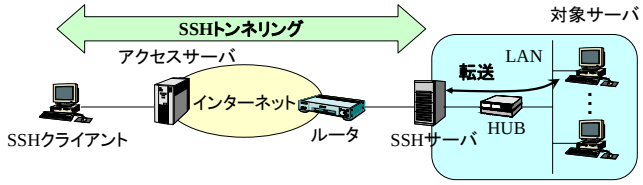


16

SSH

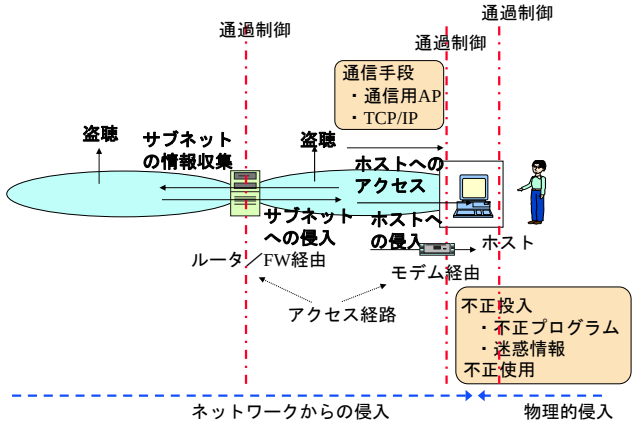
SSH(Secure Shell)

- ・クライアント、サーバの相互認証
- ・通信路の暗号化
- ・対象サーバへの転送



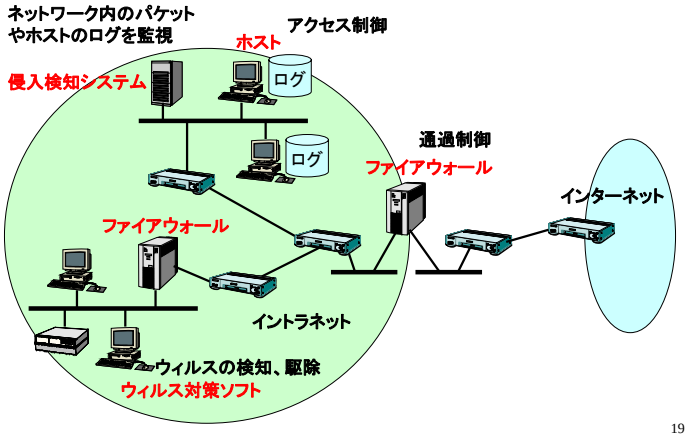
17

ネットワークへの不正行為／攻撃



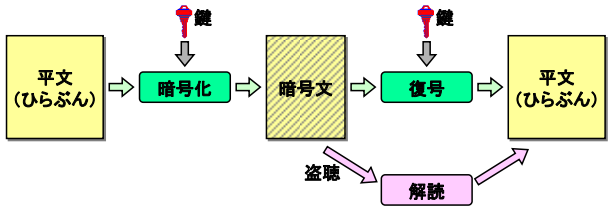
18

不正アクセスの防御



19

暗号とは



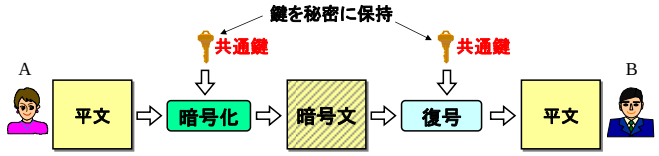
平文(ひらぶん):通常の文
暗号文:そのままでは理解不能な文(暗号化された文)
暗号化:平文を暗号文に変換すること
復号:鍵を使って暗号文を平文に変換すること
解読:暗号文を不正な方法で(通常は鍵を使わず)平文に変換すること

設問:鍵は何故必要か?

20

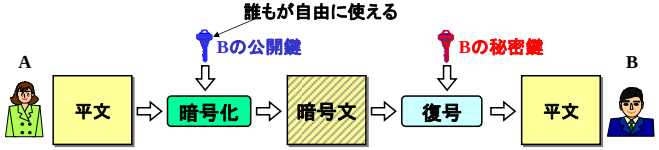
共通鍵暗号と公開鍵暗号

●共通鍵暗号方式（同じ鍵を使用）



AとBの間で、同じ鍵を誰にも知られずに共有する必要がある

●公開鍵暗号方式（対になった鍵を使用）

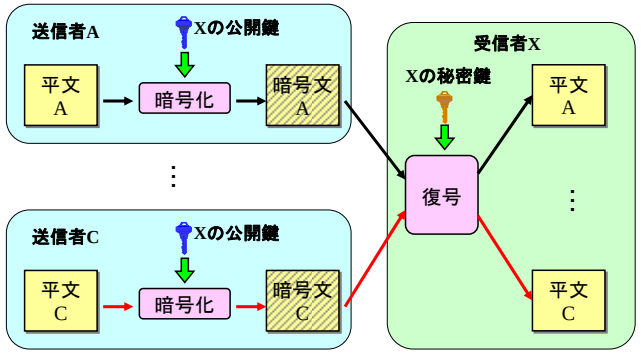


秘密鍵は誰にも渡す必要がない（共通鍵は相手に渡す必要がある）

21

公開鍵暗号による暗号化

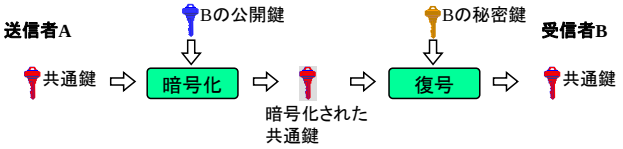
○公開鍵は誰でも使えるので、誰でも暗号文を作れる
○復号できるのは、秘密鍵の所有者のみ



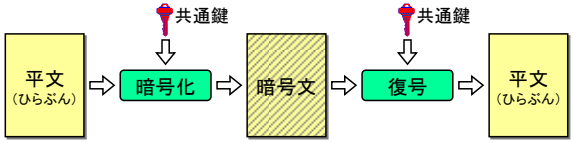
22

公開鍵暗号と共通鍵暗号の利用法

① 公開鍵暗号を使用し、共通鍵を安全に送信（鍵共有）



② 共通鍵暗号を使用し、情報を安全に送信



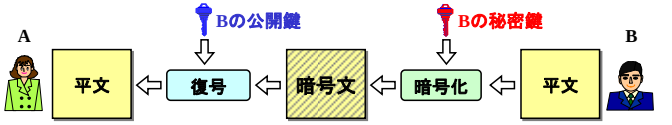
この共通鍵を**セッション鍵**とも呼ぶ

23

公開鍵暗号は双方向

一方の鍵で暗号化し、他方の鍵で復号
- 公開鍵：誰もが自由に使用できる鍵
- 秘密鍵：本人だけが使用できる鍵（鍵を秘密に保持）

暗号文は秘密鍵所有者しか、復号できないので、安全

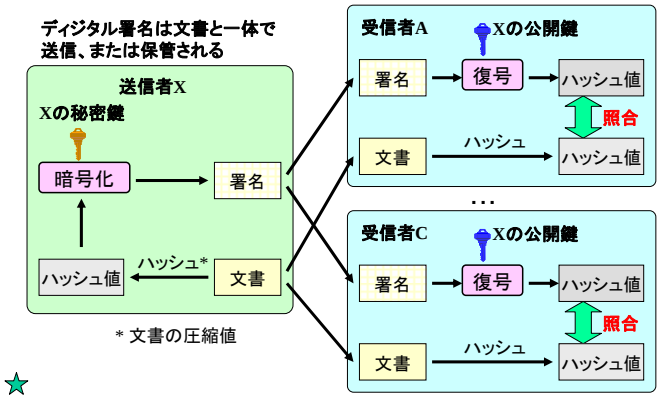


誰でも復号できるので、暗号化の意味がない

24

ディジタル署名

○秘密鍵を持っている所有者しか暗号化（署名）ができない
○公開鍵は誰でも使えるので、誰でも復号（署名検証）できる

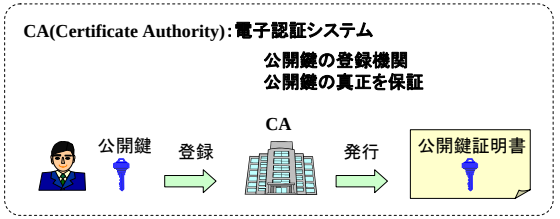


25

電子認証システム

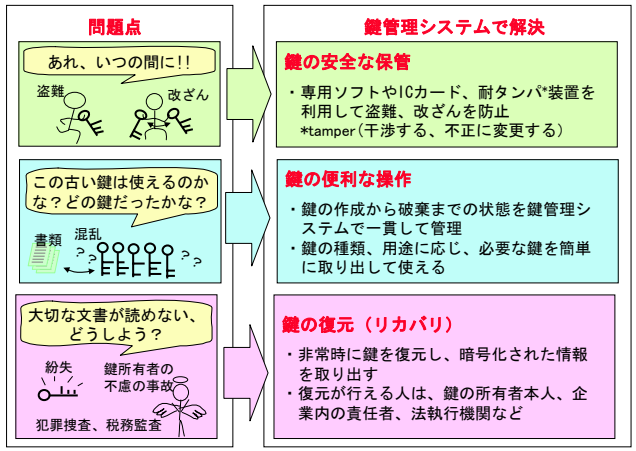
印鑑（実印）の登録

公開鍵の登録



26

付. 鍵管理と鍵リカバリ



27