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
3. 暗号技術と認証
4. 公開鍵インフラストラクチャ（PKI）
5. 共通鍵暗号
6. 整数論
7. 公開鍵暗号
8. メッセージ認証とハッシュ
9. ネットワーク接続時の脅威
10. ネットワーク接続時の対処
11. 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	盗難、漏洩	暗号化
	改ざん	ディジタル署名、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

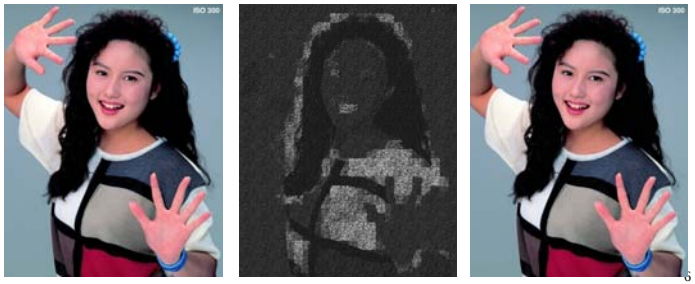
電子透かし

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

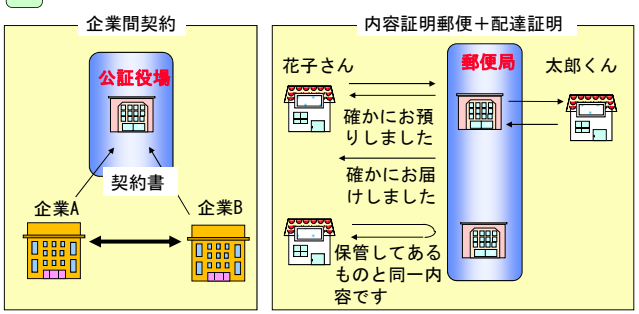


6

電子公証

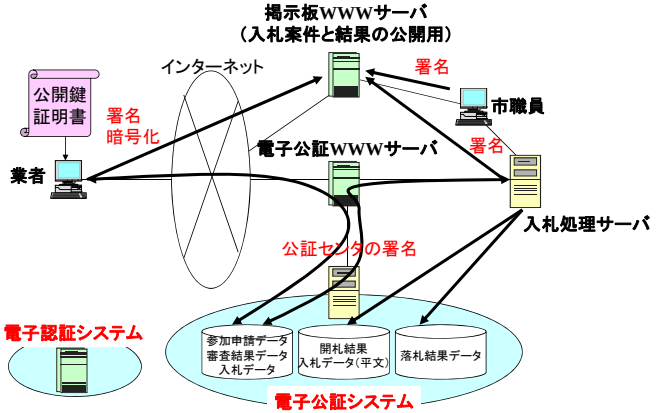
公証の役割：否認を防止するために第三者として事実証明を行うこと

電子化 → 電子公証



7

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

8

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）
パスモ	PASMO（パスモ）

定期券・乗車券と改札機の間で情報を安全にやり取り

9

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（エディ）
アイワイカードサービス	Nanaco（ナナコ）
イオン	WAON（ワオン）
JCB	QUICPay（クイックペイ）
NTTドコモiD	iD（アイディ）

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

10

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

http://www.nttdocomo.co.jp/service/osaifu_shopping/osaifu/about/index.html

11

Webアクセス

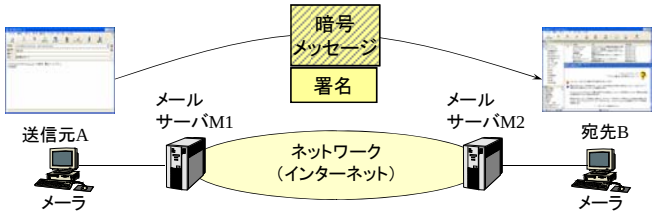
ネットショッピングなどの電子商取引にも暗号技術が必要（情報保護とサーバ認証）

12

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**

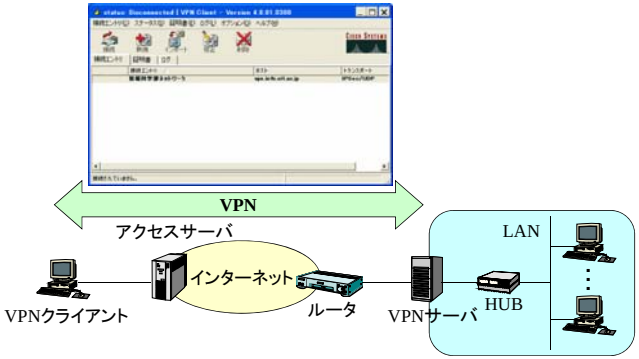


13

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**

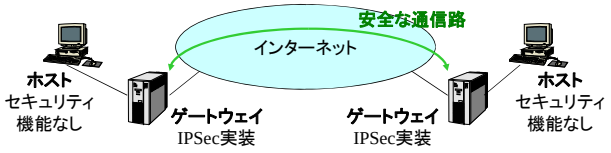


14

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**

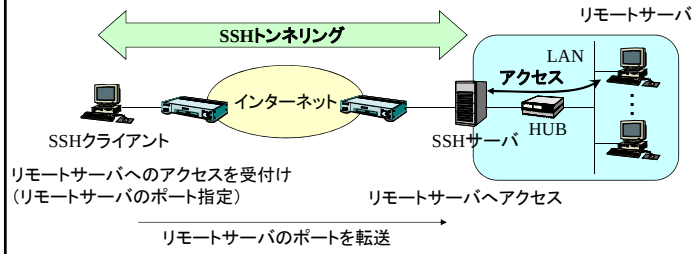


15

SSH

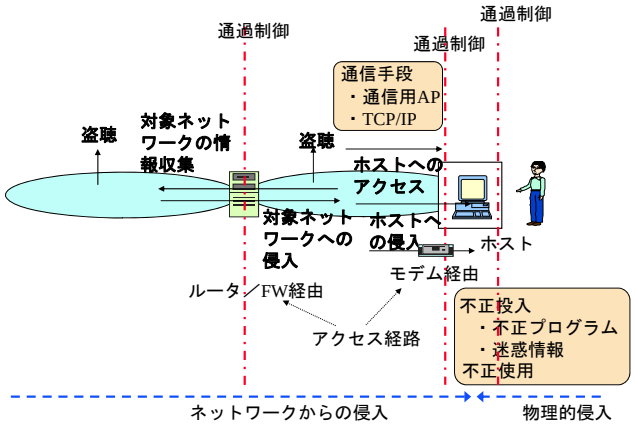
SSH(Secure Shell)

- **クライアント、サーバの相互認証**
- **通信路の暗号化**
- **ポート転送（リモートサーバへのアクセスを仲介）**



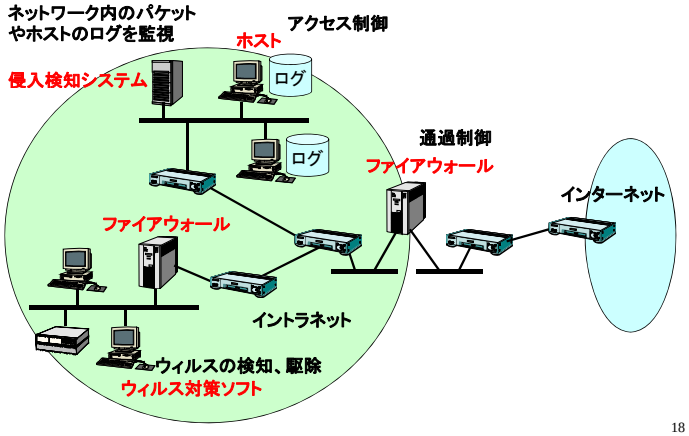
16

ネットワークへの不正行為／攻撃



17

不正アクセスの防御



18

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

19