ＥＳ：０４_ ネットワークとセキュリティ

ネットワークアーキテクチャ

ＡＰ：０６．ネットワーク

セキュリティ技術

暗号化方式

共通鍵暗号化方式

- DES（56ビット）⇐非推奨
- Triple−DES（168ビット）
- AES（128、192、256ビット）
- ・・・

公開鍵暗号方式

- RSA（1024、2048ビット）
- 楕円曲線暗号方式
- ElGamal方式
- ・・・

ハイブリッド方式　例：TLS（Transport Layer Security）

- 送信側は受信側から受け取ったサーバ証明書の正当性を、認証局の公開鍵を使って検証する
- 送信側は受信側から受信者の公開鍵をうけとる
- 送信側は共通鍵の元となる文字列を生成する
- 送信側は共通鍵を受信側の公開鍵を暗号化して、受信者側に送信する
- 受信者側は自身の秘密鍵で暗号化された共通鍵で復号する
- 共通鍵を用いて暗号化通信を開始する

ステガノグラフィ：steganography

メッセージの存在自体を隠す、画像データや音声データのように冗長性の高いデータにはメッセージを埋め込みやすい

ディジタル署名

ハッシュ関数などを用いて作成したメッセージダイジェストに公開鍵暗号方式を適用することによって、メッセージ認証とエンティティ認証を同時に行う技術である

- メッセージ認証：受信された電子文書が、送信者が送信した時点のものから改ざんされていないことを証明する技術
- エンティティ認証：電子文書が確かに当該送信者によって発信されたものであることを証明する技術

時刻認証（タイムスタンプ）

電子文書の内容と作成された時刻を同時に証明する技術

利用者はまず電子文書のメッセージダイジェストをタイムスタンプ機関に送る。タイムスタンプ機関では、受け取ったメッセージダイジェストと時刻情報などを組み合わせて新たなメッセージダイジェストを作成し、これを自身の暗号鍵で暗号化する

セキュリティ対策技術

ＡＰ：０７．セキュリティ

ファイアウォール

パケットフィルタリング方式

パケットの中身については問わず、ヘッダ部分を確認するだけでアクセスの許可・不許可を決定する

アプリケーションゲートウェイ方式

ファイアウォールがプロキシサーバとして動作することでパケットの内容にまで踏み込んだ解析を行い、アプリケーションごとに必要な変換を加えて転送を行う。

アプリケーションのプロトコルごとにゲートウェイ機能の設定が必要である。そのため、プロキシ型ファイアウォールとも呼ばれる

IDS：Intrusion Detection System

ネットワーク型IDS

ネット上を流れるすべてのパケットを監視する方式である。暗号化されたパケットについての不正検出はできない

ホスト型IDS

サーバに常駐し、不正パケットの検出を行う方式である。暗号化されたパケットにも検出可能

手法

- ログのモニタリング
- ファイルの改竄をチェック
- 不正なパケット検出とアクセスの遮断

IPS：Intrusion Prevention System

セキュリティマネジメント

ＡＰ：０７．セキュリティ

情報セキュリティマネジメントシステム

情報処理システムの運用に際してセキュリティを管理するための認証規格である

- ISO / IEC 9000シリーズ（品質管理）
- ISO / IEC 14000シリーズ（環境管理）
- ISO / IEC 15408（JIS X5070）：IT製品及びシステムのセキュリティ特性の評価のための基準についてきさいされている
- ISO / IEC 27000シリーズ：2005年に制定された情報セキュリティ管理に関する国際認証規格。（元：英国のBS7799、日本になたらISMSが設定）

ISO / IEC規格とJIS規格の対応

	内容	対応するJIS規格	元の英国規格
ISO／IEC 27000	原則及び用語集	JIS Q 27000	
ISO／IEC 27001	要求事項	JIS Q 27001	BS7799−2
ISO／IEC 27002	実施のための規範	JIS Q 27002 / JIS X 5080	BS 7799−1
ISO／IEC 27003	実施のガイドライン		
ISO／IEC 27004	効果測定		
ISO／IEC 27005	リスクマネジメント		

情報セキュリティの特性に関する概念

ISMSからの変更

	ISMSでの定義（変更前）	JIS Q 27001での定義（変更後）	リスク	対応策の例
機密性	アクセスを認可されたものだけが情報にアクセスできることを確実にすること	認可されていない個人、エンティティまたはプロセスに対して、情報を使用不可または非公開にする特性	なりすましによるデータの盗難	パスワードの定期的な変更（社会工程の研究では、これはマイナスになる可能、簡単が傾向になる）、不要ユーザIDの削除
安全性	情報及び処理方法が、正確であることおよび完全であることを保護する	資産の正確さ及び安全さを保護する特性	故意の改竄	パスワードにより悪意あるもの者のアクセスを排除する
			操作ミスによる誤入力	入力データチェックなどによるソフト対策
可用性	認可された利用者が、必要な時に、情報及び関連する資産にアクセスできることを確実にすること	認可されたエンティティが要求した時に、アクセス及び使用が可能である特性	装置故障により利用不可の時間が発生する	装置の多重化を行いシステムの信頼性を高める

リスクと事業継続計画

運用

組織全体で共通となる「情報セキュリティ基本方針文書」については、経営陣によって承認され、全従業員に公表する。また、情報資産リストやリスクと対応策については、定期的な見直しを行い、必要に応じて改訂が行われるよう、組織としての仕組みを作っておかなければならない

プライバシーマーク

事業者が個人情報の取扱を適切に行うための体制などを整備していることを認証する制度である

付与機構：一般財団法人日本情報経済社会推進協会（JIP−DEC）では、左記の条件を満たすことが規定されている

1．JIS Q 15001：2006「個人情報保護マネジメントシステム−要求事項」に準拠した個人情報保護マネジメントシステム−要求事項（以下PMS）を定めていること

2．PMSに基づき実施可能な体制が整備されており、且つ、個人情報の適切な取扱が実施されている