FS001	情報セキュリティの基礎	月　　日

第１回　情報セキュリティの基本用語

■情報セキュリティの概念

●情報セキュリティ(information security)
・情報の機密性、完全性、可用性を確保・維持し、さらに、真正性、責任追跡性を維持すること。
　→その結果、様々な脅威から情報システムや情報資産を保護する

●機密性（confidentiality）
・認可されていないものに、情報を公開せず、使用できないようにすること。

●完全性（integrity）
・情報資産の正確さや完全さを保護すること。

●可用性（availability）
・認可されたユーザから要求があったときに、情報システムにアクセスし利用できること。

●責任追跡性（accountability）
・情報システムに対するアクセスや操作が、いつ誰によって行われたのか、個人まで追跡できること。

●真正性（authenticity）
・間違いなく本物であること。改ざんなどが防止されていること。

●情報資産(information asset)
・組織にとって価値のある情報や媒体、情報を管理する仕組み。

例）取引情報、印刷された顧客情報、USB メモリ、情報管理のノウハウ

●情報セキュリティインシデント(information security　incident)
・情報セキュリティを脅かす好ましくない出来事。

■脅威と脆弱性

●リスク(risk)
・将来、損害や被害を与える可能性があるもの。

参考)「事象の発生確率と事象の結果との組合せ」(JISQ27002)

●脅威(threat)
・システムや組織に損害を与える可能性がある情報セキュリティインシデントの要因。

物理的脅威	自然災害、ハードウェア故障
技術的脅威	マルウェア（ウイルス、ワーム、ボット、スパイウェア） 不正アクセス、DoS 攻撃
人的脅威	設定ミス、誤操作、不正行為、盗難、情報漏えい、紛失 ソーシャルエンジニアリング

●脆弱性(vulnerability)
・脅威につけ込まれる情報システムや組織の弱点。

例）セキュリティホール、従業員の行動規範の不徹底、管理体制の不備

●セキュリティホール(security hole)
・情報セキュリティを脅かす可能性がある弱点のこと。
・特に OS やアプリケーションソフトウェアの欠陥(バグ)。

セキュリティパッチ	セキュリティホールをふさぐために配布される修正プログラム。
ゼロデイアタック	セキュリティホールのセキュリティパッチが配布される前に行われる攻撃。

平成 23 年秋期　IT パスポート

問80　情報セキュリティにおける“可用性”の説明として，適切なものはどれか。

ア　システムの動作と出力結果が意図したものであること
イ　情報が正確であり，改ざんされたり破壊されたりしていないこと
ウ　認められた利用者が，必要なときに情報にアクセスできること
エ　認められていないプロセスに対して，情報を非公開にすること

［解答］

平成 21 年秋期　IT パスポート

問66　セキュリティ事故の例のうち，原因が物理的脅威に分類されるものはどれか。

ア　大雨によってサーバ室に水が入り，機器が停止する。
イ　外部から公開サーバに大量のデータを送られて，公開サーバが停止する。
ウ　攻撃者がネットワークを介して社内のサーバに侵入し，ファイルを破壊する。
エ　社員がコンピュータを誤操作し，データが破壊される。

［解答］

平成 23 年春期　応用情報技術者

問41　JIS Q 27002 における情報資産に対する脅威の説明はどれか。

ア　情報資産に害をもたらすおそれのある事象の原因
イ　情報資産に内在して，リスクを顕在化させる弱点
ウ　リスク対策に費用をかけないでリスクを許容する選択
エ　リスク対策を適用しても解消しきれずに残存するリスク

［解答］