

情報セキュリティ A 期末試験 サンプル問題 (2011-07-27 版)

(持込みは、自筆ノート A4 判 1 枚だけ)

この用紙に解答を記入し、提出する。自筆ノートにも、右下に学年、番号、氏名を記入して提出すること。[] 内の配点は目安である。

1. 次の文章のうち正しいものには ○ を、誤っているものには × を、解答欄に記入しなさい。[15 点, 各 3 点] 解答欄
- (1) 氏名と電話番号の組は、個人情報保護法の定める個人情報に該当しない。 (1) []
- (2) 可用性とは、許可されている人だけが情報にアクセスできる性質をいう。 (2) []
- (3) 電子メールのヘッダにある発信者名は、偽造することができる。 (3) []
- (4) 一定の条件下であらかじめ同意を得ずに個人情報が利用できるしくみを、オプトインという。 (4) []
- (5) 脆弱性を利用してリスクを実現する手段のことを脅威という。 (5) []
2. 次の各問いに対する答えを、それぞれの選択肢から選び、その記号を解答欄に記しなさい。[52 点, 平均各 4 点]
- (1) 三井住友銀行から電子署名付き電子メールを受信したとき、確認しなくてもよいことはどれか。 (1) []
- a. 送信者のアドレスが xxxxx@xxx.smbc.co.jp であること
e. 電子証明書の発行元が VeriSign Class 3 Organizational CA となっていること
n. 電子署名付き電子メールを受信した際にセキュリティ警告が出ていないこと
t. 本文の文字コードが ISO-2022-JP であること
- (2) 個人情報保護法が対象としている個人情報はどれか。 (2) []
- a. 行政機関に登録されている個人に関する情報に限られる。 e. 個人が秘密にしているプライバシーに関する情報に限られる。
n. 生存している個人に関する情報に限られる。 t. 日本国籍の個人に関する情報に限られる。
- (3) 情報セキュリティで維持すべき三つの事項のうち二つは完全性と可用性である。残りの一つはどれか。 (3) []
- a. 安全性 e. 機密性 n. 効率性 t. 信頼性
- (4) スパイウェアによって引き起こされた情報の漏えいに該当するものはどれか。 (4) []
- a. 暗号化せずに電子メールを送信したところ、ネットワーク上で内容が読み取られてしまった。
e. インターネットに接続したところ、パソコン内の利用者情報が知らないうちに送信されてしまった。
n. パスワードを忘れてしまったという電話に対して、システム管理者が教えたのでパスワードが他人に知られてしまった。
t. パソコンをそのまま破棄したところ、磁気媒体上に残存していたデータが読み取られてしまった。
- (5) ISMS の PDCA サイクルにおいて、Plan で実施するものはどれか。 (5) []
- a. 運用状況の管理 e. 改善策の実施 n. 実施状況に対するレビュー t. 情報資産のリスク分析
- (6) JIS Q 27001 (ISO/IEC 27001) “情報セキュリティマネジメントシステム — 要求事項” に規定されているものはどれか。 (6) []
- a. ISMS が適切に運用されているかどうかを評価するために、定期的に外部監査を受けなければならない。
e. 経営者の責任が重要であり、コミットメント、経営資源の提供、マネジメントレビューなどに関与しなければならない。
n. 附属書の管理策は、すべて適用しなければならない。
t. リスクアセスメントで明らかになったすべてのリスクに対して、リスク管理策を適用しなければならない。
- (7) IT ガバナンスを説明したものはどれか。 **情報セキュリティには直接関係しないので出題しない。** (7) []
- a. IT サービスの管理・運用規則に関するベストプラクティスを、包括的にまとめたもの
e. 企業が競争優位性を構築するために、IT 戦略の策定・実行をガイドし、あるべき方向に導く組織能力
n. 企業が情報システムや IT サービスなどを調達する際、発注元となる IT ベンダに具体的なシステム提案を要求したもの
t. サービスを提供するプロバイダが、品質を保証するため、提供するサービスの水準を明確に定義したもの
- (8) 給与システムにおいて、情報セキュリティの要素の一つである Integrity の確保に該当するものはどれか。 (8) []
- a. 運用担当者が、給与システムの処理時間を短縮するためにシステム構成を変更する。
e. 給与明細表が支給日までに、確実に印刷される。
n. 権限のない従業員が、給与データを書き換えることはできない。
t. 権限のない従業員が、給与データを読むことはできない。
- (9) リスク調査、リスク分析、セキュリティ対策の策定と実施のプロセスにおいて、リスク分析で得られる結果はどれか。 (9) []
- a. 脆弱性の発見 e. セキュリティ対策の組込み n. セキュリティ仕様 t. 損失の大きさと発生頻度
- (10) 情報システムのリスク分析における作業 ①～⑤ の、適切な順序はどれか。 (10) []
- ① 損失の分類と影響度の評価 ② 対策の検討・評価と優先順位の決定 ③ 事故の関連分析と損失額予測
④ 脆弱性の発見と識別 ⑤ 分析対象の理解と分析計画
- a. ⑤→④→②→①→③ e. ⑤→④→②→③→① n. ⑤→④→③→②→① t. ⑤→④→③→①→②

