平成 30 年度　秋期　情報セキュリティマネジメント試験　採点講評

午後試験

問 1

問 1 では，ビジネスメール詐欺の被害に遭遇した会社を題材として，偽メールの手口，振込手続き上のリスクと対策などについて幅広く出題した。

設問 4 は，(1)の正答率が低かった。クロスサイトスクリプティングを選んだ解答が多く見受けられたが，クロスサイトスクリプティングは，送受信データを書き換える手法でも，マルウェアでもない。代表的な攻撃手法について概要を理解してほしい。

設問 5(2)は，おおむね理解されていた。会社のメールクライアントソフトからドメインを詐称したメールを送信するという選択肢を選んだ解答も見受けられたが，実在しないドメインでは犯人はメールを受信できないことを理解してほしい。(4)は，正答率が低かった。電話確認のために差出人のメールに電話番号を記載してもらうという選択肢を選んだ解答が見受けられたが，偽メールの場合，記載された電話番号も偽装されているリスクがあるので，対策として適切とはいえない。注意してほしい。

本問の事例では，相互けん制の省略が脆弱性となり，ビジネスメール詐欺による金銭的被害につながった。情報セキュリティリーダは，組織に潜む様々な脆弱性がもたらす情報セキュリティリスクに注意し，必要な対策を講じることを期待したい。

問 2

問 2 は，情報セキュリティ点検で報告された指摘事項に基づく，リスク対応策の検討について出題した。

設問 1(2)は，正答率が低かった。本問では，退職時誓約書に退職後の秘密保持に関する条項が記載されているという状況設定にしている。入社時に締結する秘密保持契約書にも同様の条項を追加するべきであるという助言の主旨を理解できなかったようである。情報セキュリティリーダには，指摘事項を事実に基づいて理解し，対応方針と正しく関連付ける能力を期待したい。

設問 1(7)も，正答率が低かった。加盟店におけるクレジットカード情報の非保持化は，情報セキュリティ確保が必要な情報を限定することによってリスクを大幅に低減し，対応費用を削減する手段として有効である。ISMS クラウド認証を取得している組織のクラウドサービスを利用したとしても，それだけでは PCI DSS に準拠しているとはいえない。情報セキュリティ要件への対応には，更に，機能の実装及び運用時の対策が必要であることを理解しておいてほしい。

情報セキュリティリーダは，組織の業務を良く理解し，様々な対応方針の中から組織の状況に最も適したものを選択する能力を養ってほしい。

問 3

問 3 では，標的型メール攻撃への対応訓練を題材として，情報セキュリティリーダに必要となる，訓練計画を立案する能力及び訓練で明らかになった課題に対する解決策を検討する能力について出題した。

設問 3 は，標的型攻撃訓練で使用する訓練メールが転送されてきたときの X 社外部メールサーバの動作を本文から読み取っていない解答が多く見受けられた。本文に書かれた機能をしっかり読んだ上で解答してほしい。

設問 4(1)は，おおむね解答できていた。本物の標的型メールを転送した場合に想定される情報セキュリティリスクを正確に理解しておいてほしい。(2)の正答率は低かった。マルウェア検査サイトを使用した場合に予想される被害を本文から読み取ってほしい。(3)は，標的型攻撃訓練の学習効果を高める方策及びマルウェア検査サイトへの添付ファイルのアップロードによるリスクへの対策が良く理解されていた。

標的型メール攻撃による被害は，今後ますます増えていくと予想される。対応訓練は標的型メール攻撃への有効な対策の一つである。情報セキュリティリーダには，巧妙化する他の攻撃手法に対しても効果的な対応訓練を実施し，組織の情報セキュリティ対策をリードしていくことを期待したい。