平成 24 年度　秋期　情報セキュリティスペシャリスト試験　採点講評

午後 I 試験

問 1

問 1 は，最近では広く利用されることが多くなってきた Ajax の基本概念について出題した。全体として正答率は低かった。

設問 1 の a については正答率が高かったが，b については，正答率が低かった。XMLHttpRequest という用語は知っていても，その制限までは知らない受験者が多いようだった。是非，最新のブラウザの仕組みを知っておいてほしい。

設問 2 は正答率が低かった。HTTPS 通信において，サーバ認証の場合，サーバだけの認証であるので，サーバ証明書だけを用意すればよいのに対して，クライアント認証の場合，相互認証であるので，利用者ごとにクライアント証明書の管理が必要となることに気がついてほしかった。

設問 4(1)は，正答率が低かった。この問題は，攻撃に対する一般的な対策方針に基づき安全なポイント表示サービスを設計する問題であった。攻撃を防ぐためには，トップページへのアクセスの際，正規に認証されていることを一般サイト側に知らせる仕組みが必要であることに気がついてほしかった。

問 2

設問 1 は，全体的に正答率が高かった。システムが採取しているログとモニタリングの要件を基に，機械処理可能なモニタリング条件を決定していく手順は，おおむね理解されているようであった。

設問 2 では，モニタリング条件の設定とその運用について出題した。条件を正確に記述している解答は少なかった。モニタリングを適切に実装・運用するためには，モニタリングの対象とするシステムの利用パターンを，モニタリング条件として正確に定義できる力が必要である。

設問 3 では，モニタリングの有効性と効率性を維持するための施策について出題した。モニタリング条件の見直しに利用部門が協力する点について言及している解答は少なかった。

モニタリングは，情報にアクセスする権限をもった利用者による権限の濫用を防ぐコントロールとして有効であるが，その条件設定が不適切であったり，また，システムが置かれている状況の変化に対応していなかったりすると，形骸化してしまう危険がある。モニタリングがもつそのような特性をよく理解しておいてほしい。

問 3

問 3 は最近話題として取り上げられることが多い標的型攻撃について出題した。全体として，正答率は低かった。

設問 1 ではメールヘッダから読み取れる内容について出題した。選択問題にもかかわらず，正答率は低かった。普段から電子メールが届く経路がメールヘッダにどのように記録されるかを理解しておいてほしい。

設問 2 では送信ドメイン認証技術の SPF（Sender Policy Framework）について出題した。(1)は正答率が高かったが，(2)は正答率が低かった。SPF のような標準的な技術については，何を基準にしているか，何をどのように確認しているか基本事項を理解しておいてほしい。

設問 3 では標的型攻撃について出題した。(1)の正答率は高かったが，(3)，(4)の正答率は低かった。(4)では，現在，一般的な製品になっている Web フィルタを利用する対策の記述を期待したが，正答率は低かった。

設問 3(1)，(3)は，問題文中に記述されている内容を落ち着いて読めば，正解を導けるはずである。設問 3(2)，(4)は，それぞれ問題文中に記述されている状況での対策を問うているので，問題文中の背景をしっかり理解して正解を導きだしてほしい。IPA が公開して“安全なウェブサイトの作り方”で扱っているように脆弱(ぜい)性を作りこまない根本的な対策を確実にすることだけではなく，攻撃による影響を軽減する保険的対策も有効なことを，区別して理解してほしい。

問４

問 4 では，インシデント発生時のログ調査から対策までの一連のプロセスについて出題した。全体として正答率は低かった。

設問 1 は，今回のようなインシデントでのログ調査では，LB のサービス稼働チェックログに加え，Web サーバ群のリソースグラフを確認することでログの調査範囲を絞り込むという手法は理解されているようであった。しかし，調査範囲を絞り込んだ後に判明した結果について述べられていた解答のように，設問の主旨を捉えていない解答も見られた。落ち着いて問題文を読んで解答してほしい。

設問 3(1)は，d の正答率が低かった。IDS 製品だけではなく，WAF 製品でも秘密鍵を利用して，HTTPS 通信を監視できるようになってきているので，一般的な知識として理解しておいてほしい。

設問 3(3)は，設定内容について正答率が低かった。プロキシサーバや LB などを利用するシステム構成では，X-Forwarded-For ヘッダフィールドは，送信元の IP アドレスを特定するために有効であることを，基本知識として理解しておいてほしい。