3-2　セキュリティ実装技術

問１

Check □□□

OSI 基本参照モデルのネットワーク層で動作し，“認証ヘッダ（AH）”と“暗号ペイロード（ESP）”の二つのプロトコルを含むものはどれか。

ア　IPsec　　イ　S/MIME　　ウ　SSH　　エ　XML 暗号

【2017年春期 SG 問28】

問２

Check □□□

HTTPS 通信において，暗号化とサーバ認証に使用されるものはどれか。

ア　Cookie　　イ　S/MIME
ウ　SSL/TLS　　エ　ダイジェスト認証

【2013年春期 AP 問36】

問３

Check □□□

SSH の説明はどれか。

ア　MIME を拡張した電子メールの暗号化とディジタル署名に関する標準
イ　オンラインショッピングで安全にクレジットカード決済を行うための仕様
ウ　共通鍵暗号技術と公開鍵暗号技術を併用した電子メールの暗号化，復号の機能をもつ電子メールソフト
エ　リモートログインやリモートファイルコピーのセキュリティを強化したプロトコル，及びそのプロトコルを実装したコマンド

【2018年秋期 SG 問29】

問４

Check □□□

HTTP over TLS（HTTPS）を用いて実現できるものはどれか。

ア　Web サーバ上のファイルの改ざん検知
イ　Web ブラウザが動作する PC 上のマルウェア検査
ウ　Web ブラウザが動作する PC に対する侵入検知
エ　ディジタル証明書によるサーバ認証

【2017年秋期 SG 問29】

前ページの解答 ＊ 問35 ウ　問36 エ

問5

Check □□□

次の電子メールの環境を用いて，秘密情報を含むファイルを電子メールに添付して社外の宛先の利用者に送信したい。その際のファイルの添付方法，及びその添付方法を使う理由として，適切なものはどれか。

〔電子メールの環境〕
- 電子メールは，Webブラウザから利用できる電子メールシステム（Webメール）を用いて送信する。
- WebブラウザとWebメールのサーバとの通信はHTTP over TLS（HTTPS）で行う。
- 社外の宛先ドメインのメールサーバはSMTPとPOP3を使用している。
- IP層以下は暗号化していない。

ア　WebブラウザからWebメールのサーバまでの通信が暗号化されているので，ファイルは平文のままでメールに添付する。
イ　WebブラウザからWebメールのサーバまでの通信は暗号化されるが，その後の通信が暗号化されないこともあるので，ファイルを暗号化してメールに添付する。
ウ　Webブラウザから宛先の利用者がメールを受信するPCまで，全ての通信は暗号化されるので，ファイルは平文のままでメールに添付する。
エ　Webメールのサーバから宛先ドメインのメールサーバまでの通信は暗号化されないが，サーバ間の通信はBase64形式でエンコードすれば盗聴できないので，ファイルはBase64形式でエンコードしてメールに添付する。

【2016年秋期 SG 問17】

問6

Check □□□

電子メールの本文を暗号化するために使用される方式はどれか。

ア　BASE64　　イ　GZIP　　ウ　PNG　　エ　S/MIME

【2018年春期 SG 問28】

問7

Check □□□

WPA3はどれか。

ア　HTTP通信の暗号化規格
イ　TCP/IP通信の暗号化規格
ウ　Webサーバで使用するディジタル証明書の規格
エ　無線LANのセキュリティ規格

【2019年秋期 SG 問18】

問８

Check □□□

SPF（Sender Policy Framework）の仕組みはどれか。

ア　電子メールを受信するサーバが，電子メールに付与されているディジタル署名を使って，送信元ドメインの詐称がないことを確認する。
イ　電子メールを受信するサーバが，電子メールの送信元のドメイン情報と，電子メールを送信したサーバの IP アドレスから，送信元ドメインの詐称がないことを確認する。
ウ　電子メールを送信するサーバが，電子メールの宛先のドメインや送信者のメールアドレスを問わず，全ての電子メールをアーカイブする。
エ　電子メールを送信するサーバが，電子メールの送信者の上司からの承認が得られるまで，一時的に電子メールの送信を保留する。

【2019年秋期 SG 問７】

問９

Check □□□

SPF（Sender Policy Framework）を利用する目的はどれか。

ア　HTTP 通信の経路上での中間者攻撃を検知する。
イ　LAN への PC の不正接続を検知する。
ウ　内部ネットワークへの侵入を検知する。
エ　メール送信者のドメインのなりすましを検知する。

【2019年春期 SG 問11】

問10

Check □□□

電子メールをドメインＡの送信者がドメインＢの宛先に送信するとき，送信者をドメインＡのメールサーバで認証するためのものはどれか。

ア　APOP　　イ　POP3S　　ウ　S/MIME　　エ　SMTP-AUTH

【2019年秋期 SG 問28】

問11

Check □□□

Web サーバの検査におけるポートスキャナの利用目的はどれか。

ア　Web サーバで稼働しているサービスを列挙して，不要なサービスが稼働していないことを確認する。
イ　Web サーバの利用者 ID の管理状況を運用者に確認して，情報セキュリティポリシからの逸脱がないことを調べる。
ウ　Web サーバへのアクセス履歴を解析して，不正利用を検出する。
エ　正規の利用者 ID でログインし，Web サーバのコンテンツを直接確認して，コンテンツの脆弱(ぜいじゃく)性を検出する。

【2019年秋期 SG 問30】

前ページの解答 ＊ 問1 ア　問2 ウ　問3 エ　問4 エ　問5 イ　問6 エ　問7 エ

問12

Check □□□

社内ネットワークとインターネットの接続点に，ステートフルインスペクション機能をもたない，静的なパケットフィルタリング型のファイアウォールを設置している。このネットワーク構成において，社内の PC からインターネット上の SMTP サーバに電子メールを送信できるようにするとき，ファイアウォールで通過を許可する TCP パケットのポート番号の組合せはどれか。ここで，SMTP 通信には，デフォルトのポート番号を使うものとする。

	送信元	宛先	送信元 ポート番号	宛先 ポート番号
ア	PC	SMTP サーバ	25	1024 以上
	SMTP サーバ	PC	1024 以上	25
イ	PC	SMTP サーバ	110	1024 以上
	SMTP サーバ	PC	1024 以上	110
ウ	PC	SMTP サーバ	1024 以上	25
	SMTP サーバ	PC	25	1024 以上
エ	PC	SMTP サーバ	1024 以上	110
	SMTP サーバ	PC	110	1024 以上

【2018年春期 SG 問18】

問13

Check □□□

PC への侵入に成功したマルウェアがインターネット上の指令サーバと通信を行う場合に，宛先ポートとして使用される TCP ポート番号80に関する記述のうち，適切なものはどれか。

ア　DNS のゾーン転送に使用されることから，通信がファイアウォールで許可されている可能性が高い。

イ　Web サイトの HTTPS 通信での閲覧に使用されることから，マルウェアと指令サーバとの間の通信が侵入検知システムで検知される可能性が低い。

ウ　Web サイトの閲覧に使用されることから，通信がファイアウォールで許可されている可能性が高い。

エ　ドメイン名の名前解決に使用されることから，マルウェアと指令サーバとの間の通信が侵入検知システムで検知される可能性が低い。

【2019年春期 SG 問19】