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 □□□

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 イ　問36 ウ

問 4

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 5

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決済を行うための仕様
ウ　対称暗号技術と非対称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ツール及びプロトコル

【2014年春期 AP 問44】

問 6

Check □□□

SMTP-AUTH（SMTP Service Extension for Authentication）における認証の動作を説明したものはどれか。

ア　SMTP サーバは，クライアントがアクセスしてきた場合に利用者認証を行い，認証が成功したとき電子メールを受け付ける。
イ　サーバは認証局のディジタル証明書をもち，クライアントから送信された認証局の署名付きクライアント証明書の妥当性を確認する。
ウ　電子メールを受信した際にパスワード認証が成功したクライアントの IP アドレスは，一定時間だけ SMTP サーバへの電子メールの送信が許可される。
エ　パスワードを秘匿するために，パスワードからハッシュ値を計算して，その値で利用者が電子メールを受信する際の利用者認証を行う。

【2014年秋期 AP 問37】

問 7

Check □□□

社内ネットワークとインターネットの接続点にパケットフィルタリング型ファイアウォールを設置して，社内ネットワーク上の PC からインターネット上の Web サーバの 80 番ポートにアクセスできるようにするとき，フィルタリングで許可するルールの適切な組合せはどれか。

ア

送信元	宛先	送信元ポート番号	宛先ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	80	1024 以上

イ

送信元	宛先	送信元ポート番号	宛先ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	1024 以上	80

ウ

送信元	宛先	送信元ポート番号	宛先ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	80	1024 以上

エ

送信元	宛先	送信元ポート番号	宛先ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	1024 以上	80

【2017年春期 FE 問42】

前ページの解答 ＊ 問1 ア　問2 ウ　問3 エ　問4 イ　問5 エ

問8

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TCPポート番号80が多く使用される理由はどれか。

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，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，侵入検知システムで検知される可能性が低い。

【2016年秋期 FE 問45】

問9

Check □□□

攻撃者がシステムに侵入するときにポートスキャンを行う目的はどれか。

ア　事前調査の段階で,攻撃できそうなサービスがあるかどうかを調査する。
イ　権限取得の段階で，権限を奪取できそうなアカウントがあるかどうかを調査する。
ウ　不正実行の段階で，攻撃者にとって有益な利用者情報があるかどうかを調査する。
エ　後処理の段階で，システムログに攻撃の痕跡が残っていないかどうかを調査する。

【2016年春期 SG 問29】

問10

Check □□□

社外からインターネット経由で PC を職場のネットワークに接続するときなどに利用する VPN（Virtual Private Network）に関する記述のうち，最も適切なものはどれか。

ア　インターネットとの接続回線を複数用意し，可用性を向上させる。
イ　送信タイミングを制御することによって，最大の遅延時間を保証する。
ウ　通信データを圧縮することによって，最小の通信帯域を保証する。
エ　認証と通信データの暗号化によって，セキュリティの高い通信を行う。

【2011年秋期 IP 問70】

問11

Check □□□

データベースのアカウントの種類とそれに付与する権限の組合せのうち，情報セキュリティ上，適切なものはどれか。

	アカウントの種類	レコードの更新権限	テーブルの作成・削除権限
ア	データ構造の定義用アカウント	有	無
イ	データ構造の定義用アカウント	無	有
ウ	データの入力・更新用アカウント	有	有
エ	データの入力・更新用アカウント	無	有

【2017年秋期 SG 問25】

問12

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)性を検出する。

【2017年春期 SG 問30】

問13

Check □□□

SQL インジェクション攻撃を防ぐ方法はどれか。

ア　入力中の文字がデータベースへの問合せや操作において，特別な意味をもつ文字として解釈されないようにする。
イ　入力に HTML タグが含まれていたら，HTML タグとして解釈されない他の文字列に置き換える。
ウ　入力に上位ディレクトリを指定する文字列（../）が含まれているときは受け付けない。
エ　入力の全体の長さが制限を超えているときは受け付けない。

【2015年秋期 FE 問42】

前ページの解答 ＊ 問6 ア　問7 ウ　問8 ウ　問9 ア　問10 エ

問14

Check
□□□

安全なWebアプリケーションの作り方について，攻撃と対策の適切な組合せはどれか。

	攻撃	対策
ア	SQLインジェクション	SQL文の組立てに静的プレースホルダを使用する。
イ	クロスサイトスクリプティング	任意の外部サイトのスタイルシートを取り込めるようにする。
ウ	クロスサイトリクエストフォージェリ	リクエストにGETメソッドを使用する。
エ	セッションハイジャック	利用者ごとに固定のセッションIDを使用する。

【2014年春期 AP 問40】