コース名：	情報セキュリティ対策実践シリーズ 基礎から学ぶセキュア環境構築･運用入門編

問題 1

正解：3　［配点：10 点］

解説

情報セキュリティガバナンスは、情報セキュリティを取り巻く環境の変化に継続的に対応するために、情報セキュリティ上の観点から内部統制の仕組みを構築し運用することです。
【参考】テキスト 20 ページ

問題 2

正解：1　［配点：10 点］

解説

情報セキュリティの定義は、『情報の機密性、完全性、及び可用性を維持すること。』（出典：「JIS Q 27000:2019」）とされています。このため、機密性、完全性、可用性が情報資産に対する情報セキュリティ上の品質と考え、対策によってそれらを確保し続けることが必要です。
【参考】テキスト 26 ページ

問題 3

正解：4　［配点：10 点］

解説

ファイアーウォールのアクセス制御は、ネットワーク間でやり取りされるパケットの許可や遮断による制御を行い、社内ネットワークシステムの機密性を維持します。この制御を実現する主要な技術として、パケットフィルタリングやステートフルパケットインスペクションがあります。
【参考】テキスト 51 ページ

問題 4

正解：2　　［配点：10 点］

解説

ネットワーク間でのアクセスルートの制御においては、直接と間接的な制御方法があり、間接的に通信を制御した方がよりセキュリティが高くなります。内外ネットワークの場合、境界ネットワークとして DMZ（DeMilitarized Zone：非武装地帯）を作成します。その DMZ には、公開サーバや中継サーバを配置し、間接的に通信が行われるようアクセスルートを制御します。
【参考】テキスト 58 ページ

問題 5

正解：1　　［配点：10 点］

解説

EDR（Endpoint Detection & Response）は、エンドポイントにおける脅威検知と対処のための対策です。万が一のウイルス感染に備え、不正な挙動を特定し、迅速にネットワークからの遮断、封じ込めを行い、影響把握を可能にします。
【参考】テキスト 68,71 ページ

問題 6

正解：3　　［配点：10 点］

解説

公開鍵暗号方式では、秘密鍵と公開鍵の 2 種類の鍵を用います。共通鍵は、共通鍵暗号方式の暗号化と復号で用いられています。
【参考】テキスト 73 ページ

問題 7

正解：2　　［配点：10 点］

解説

IPsec(Security Architecture for Internet Protocol)および SSL-VPN において、拠点間でやり取りされる業務データ通信は共通鍵暗号方式が用いられています。共通鍵暗号方式で使用する共通鍵の交換は、公開鍵暗号方式が用いられています。
【参考】テキスト 84 ページ

問題 8

正解：3　　［配点：10 点］

解説

モバイル端末の紛失や盗難発生時の対策技術には、遠隔消去やロック、BIOS パスワード認証、HDD の暗号化、シンクライアントがあります。
【参考】テキスト 105 ページ

問題 9

正解：1　　［配点：10 点］

解説

SIEM（Security Information and Event Management：セキュリティ情報イベント管理）は、正常な状態の逸脱をログ相関分析によって検知し、早期に異常を警告する技術です。
【参考】テキスト 106 ページ

問題 10

正解：3　　［配点：10 点］

解説

CSIRT（Computer Security Incident Response Team）は、インシデントの発生を速やかに検知・対応するための専門的な機関や役割・体制の総称です。主な役割は、世界中のインシデント関連情報やぜい弱性情報（JVN）、攻撃予兆情報の収集・分析、脅威への対応方針の策定、防御策の戦略策定、インシデント発生時の対応方法の策定などを行います。
【参考】テキスト 121 ページ