※出題範囲は以下の内容を含みますが、これらに限定されるものではありません。

出題範囲（参考訳）
セキュリティの基本原則
セキュリティの基本原則の定義
脆弱性、脅威、エクスプロイト、リスク。 攻撃ベクトル。堅牢化。多層防御。機密性・完全性・可用性（セキュリティの三原則、CIA）。攻撃者の種類。攻撃の理由。倫理規定。
一般的な脅威や脆弱性についての説明
マルウェア、ランサムウェア、サービス拒否（DoS)、ボットネット、ソーシャルエンジニアリング攻撃（テールゲーティング、スピアフィッシング、フィッシング、ヴィッシング、スミッシング等）、物理攻撃、中間者攻撃、IoT の脆弱性、インサイダー脅威、高度標的型（APT）攻撃
アクセス管理の原則についての説明
認証、認可、アカウンティング（AAA）。RADIUS。多要素認証（MFA）。パスワードポリシー
暗号化の手法とアプリケーションについての説明
暗号化の種類、ハッシュ化、証明書、公開鍵基盤（PKI）。強度の高い/低い暗号化アルゴリズム。データの状態に応じた適切な暗号化（送信中データ、保存データ、使用中データ）。暗号化を使用するプロトコル
ネットワークセキュリティの基本概念
TCP/IP プロトコルの脆弱性についての説明
TCP、UDP、HTTP、ARP、ICMP、DHCP、DNS
ネットワークアドレスがネットワークセキュリティに与える影響の説明
IPv4 / IPv6 アドレス、MAC アドレス、ネットワーク セグメンテーション、CIDR 表記、NAT、パブリックネットワークとプライベートネットワークの比較
ネットワークインフラストラクチャと技術についての説明
ネットワークセキュリティ アーキテクチャ、DMZ、仮想化、クラウド、ハニーポット、プロキシサーバー、IDS、IPS
安全な SoHo ワイヤレスネットワークの構築
MAC アドレスフィルタリング、暗号化標準とプロトコル、SSID
安全なアクセス技術の実装
ACL、ファイアウォール、VPN、NAC
エンドポイントセキュリティの概念
オペレーティングシステムのセキュリティの概念
Windows、macOS、Linux。Windows Defender、ホスト型ファイアウォールを含むセキュリティ機能。CLI と PowerShell。ファイルとディレクトリのアクセス権限。権限昇格
セキュリティ評価情報を収集する適切なエンドポイントツールの知識
netstat、nslookup、tcpdump
エンドポイントシステムがセキュリティポリシーや標準の要件を満たすことの確認
ハードウェア在庫（資産管理）、ソフトウェア在庫、プログラムの展開、データバックアップ、企業コンプライアンス（PCI DSS、HIPAA、GDPR）、BYOD（デバイス管理、データ暗号化、アプリ配布、構成管理）

出題範囲（参考訳）
ソフトウェアとハードウェアのアップデートの実行
Windows アップデート、アプリケーションのアップデート、デバイスドライバー、ファームウェア、パッチ
システムログの解釈
イベントビューア、監査ログ、システムログとアプリケーションログ、syslog、異常の特定
マルウェアの除去に関する知識
走査システム、スキャンログの確認、マルウェアの駆除
脆弱性の評価とリスクマネジメント
脆弱性管理についての説明
脆弱性の特定、管理、改善。能動的/受動的調査。検証（ポートスキャン、自動化）
脅威インテリジェンスの技術を使用したネットワークの潜在的脆弱性の特定
脆弱性データベースの利用と限界。脆弱性評価および提言・ポリシー・レポート作成に使用される業界標準ツール。共通脆弱性識別子（CVEs）。サイバーセキュリティ レポート、サイバーセキュリティ ニュース、サブスクリプションサービス、集合知（集団的知性）。アドホックおよび自動化された脅威インテリジェンス。サイバーセキュリティインシデントの前後最中に文書情報や他の形態のコミュニケーションを積極的に更新することの重要性。文書情報を保管・共有・更新する方法。
リスクマネジメントについての説明
脆弱性とリスクの比較、リスクの格付け、リスクマネジメントの方法、リスク緩和のための戦略、リスクレベル（低、中、高、非常に高）、特定のデータの種類や分類に伴うリスク、ITシステムのセキュリティ評価（情報セキュリティ、チェンジマネジメント、コンピューター操作、情報保証）
ディザスタリカバリ（災害復旧）と事業継続計画の重要性についての説明
自然災害と人災、ディザスタリカバリ計画（DRP）と事業継続計画（BCP）の特徴、バックアップ、ディザスタリカバリ制御対策（発見、予防、修正）
インシデント ハンドリング
セキュリティイベントの監視と、エスカレーションが必要なタイミングの把握
SIEM と SOAR の役割、ネットワークデータの監視とセキュリティインシデントの特定（パケットキャプチャ、各種ログファイルのエントリ等）、疑わしいイベントを発生時に特定
デジタル フォレンジックと攻撃内容特定プロセス
サイバーキルチェーン、MITRE ATT&CK マトリクス、ダイヤモンドモデル。TTP（戦術、技術、手順）。証拠資料（アーティファクト）。証拠の取り扱い（デジタルエビデンスの保存、証拠保全）
インシデント ハンドリングにコンプライアンスの枠組みが与える影響の説明
コンプライアンスの枠組み（GDPR、HIPAA、PCI-DSS、FERPA、FISMA)、報告および通知の要件
サイバーセキュリティ インシデントレスポンスの要素の説明
ポリシー、計画および手順の要素。インシデントレスポンスの各段階（NIST Special Publication 800-61 sections 2.3, 3.1-3.4)