IT Specialist
Network Security　ネットワークセキュリティ

※出題範囲は以下の操作や機能を含みますが、これらに限定されるものではありません。

Objective domains	出題範囲（参考訳）
1. Defense in Depth	**1. 多層防御**
1.1 Identify core security principles	**1.1 セキュリティの基本原則の確認**
Confidentiality, integrity, availability, non-repudiation, threat, risk, vulnerability, principle of least privilege, attack surfaces including IoT	機密性、整合性/完全性、可用性、否認防止、脅威、リスク、脆弱性、最小権限の原則、IoTを含む攻撃対象領域
1.2 Define and enforce physical security	**1.2 物理的なセキュリティの定義と強化**
Site security, computer security, removable devices and drives, mantraps	場所に対するセキュリティ、コンピュータセキュリティ、リムーバブルデバイスとドライブ、マントラップ
1.3 Identify security policy types	**1.3 セキュリティポリシーの種類の識別**
Administrative controls, technical controls	管理者権限による制御、技術的な制御
1.4 Identify attack types	**1.4 攻撃の種類の識別**
Buffer overflow, viruses, polymorphic viruses, worms, Trojan horses, spyware, ransomware, adware, rootkits, backdoors, zero day attacks/ vulnerabilities, denial-of-service (DoS) attacks, common attack methods, types of vulnerability, cross-site scripting (XSS), SQL injection, brute force attack, man-in-the-middle (MITM) and man-in-the-browser (MITB), social engineering, keyloggers (software and hardware), logic bombs	バッファオーバーフロー、ウイルス、ポリモーフィック型ウイルス、ワーム、トロイの木馬、スパイウェア、ランサムウェア、アドウェア、ルートキット、バックドア、ゼロデイ攻撃／脆弱性、サービス拒否（DoS）攻撃、一般的な攻撃方法、脆弱性の種類、クロスサイトスクリプティング（XSS）、SQLインジェクション、ブルートフォース攻撃、中間者（MITM）およびマンインザブラウザ（MITB）攻撃、ソーシャルエンジニアリング、キーロガー（ソフトウェアおよびハードウェア）、論理爆弾
1.5 Identify backup and restore types	**1.5 バックアップと復元の種類の識別**
Full, incremental, differential	完全バックアップ、増分バックアップ、差分バックアップ
2. Operating System Security	**2. オペレーティングシステムのセキュリティ**
2.1 Identify client and server protection	**2.1 クライアントとサーバーの保護**
Separation of services, hardening, patch management, reducing the attack surface, group policy (gpupdate and gpresult), secure dynamic Domain Name System (DNS) updates, User Account Control (UAC), keeping client operating system and software updated, encrypting offline folders, software restriction policies	サービスの分離、ハードニング（強化）、パッチの管理、攻撃対象領域の削減、グループポリシー（gpupdateおよびgpresult）、安全な動的ドメインネームシステム（DNS）の更新、ユーザーアカウント制御（UAC）、クライアントのオペレーティングシステムおよびソフトウェアの更新、オフラインフォルダの暗号化、ソフトウェア制限ポリシー
2.2 Configure user authentication	**2.2 ユーザー認証の設定**
Multifactor authentication, enforcing password policies, remote access, using secondary sign-on to perform administrative tasks (Run As, sudo), domain and local user and group creation, Kerberos	多要素認証、パスワードポリシーの適用、リモートアクセス、管理者権限が必要なタスクを実行するためのセカンダリサインオンの使用（管理者として実行、sudo）、ドメインユーザー/グループおよびローカルユーザー/グループの作成、Kerberos認証
2.3 Manage permissions in Windows and Linux	**2.3 WindowsおよびLinuxでのアクセス許可の管理**
File and folder permissions, share permissions, inheritance, moving or copying files within the same disk or on another disk, multiple groups with different permissions, take ownership, delegation	ファイルとフォルダーのアクセス許可、共有許可、継承、同一ディスク内や別のディスク上でのファイルの移動またはコピー、異なるアクセス許可を持つ複数のグループ、所有権の取得、委譲
2.4 Facilitate non-repudiation using audit policies and log files	**2.4 監査ポリシーとログファイルによる否認防止の促進**
Types of auditing, what can be audited, enabling auditing, what to audit for specific purposes, where to save audit information, reviewing log files	監査の種類、監査可能な対象、監査の有効化、特定の目的のための監査対象、監査情報の保存場所、ログファイルの確認
2.5 Demonstrate knowledge of encryption	**2.5 暗号化についての知識の確認**
File and folder encryption, how encryption impacts moving/copying files and folders, drive encryption, TPM, secure communication processes (email, texting, chat, social media), virtual private network (VPN) encryption methods, public key/private key, certificate properties and services, Bitlocker	ファイルとフォルダの暗号化、暗号化がファイルやフォルダの移動/コピーに及ぼす影響、ドライブの暗号化、TPM、安全な通信方法（電子メール、テキスト、チャット、ソーシャルメディア）、仮想プライベートネットワーク（VPN）の暗号化方式、公開鍵/秘密鍵、証明書のプロパティとサービス、Bitlocker

Objective domains	出題範囲（参考訳）
3. Network Device Security	**3. ネットワークデバイスのセキュリティ**
3.1 Implement wireless security	**3.1 ワイヤレスセキュリティの実装**
Wireless security types (strength of encryption), service set identifiers (SSIDs), MAC filtering, default configuration (OOBE)	ワイヤレスセキュリティの種類（暗号化の強度）、サービスセット識別子（SSID）、MACフィルタリング、初期設定（OOBE）
3.2 Identify the role of network protection devices	**3.2 ネットワーク保護デバイスの役割の確認**
Purpose of firewalls, hardware vs. software firewalls, network vs. host firewalls, stateful vs. stateless firewall inspection, security baselines, intrusion detection system (IDS), intrusion prevention system (IPS), security information and event manager (SIEM), content filtering, blacklisting/whitelisting	ファイアウォールの目的、ハードウェアファイアウォールとソフトウェアファイアウォール、ネットワーク型ファイアウォールとホスト型ファイアウォール、ステートフル インスペクションとステートレス インスペクションのファイアウォール、セキュリティベースライン、不正侵入検知システム（IDS）、不正侵入防止システム（IPS）、セキュリティ情報イベント管理（SIEM）、コンテンツフィルタリング、ブラックリスト方式／ホワイトリスト方式
3.3 Identify network isolation methods	**3.3 ネットワークの分離方法の確認**
Routing, honeynet, perimeter networks (DMZ), NAT/PAT, VPN, IPsec, air gap network, DirectAccess, virtual LAN (VLAN)	ルーティング、ハニーネット、境界ネットワーク（DMZ）、NAT/PAT、VPN、IPsec、エアギャップネットワーク、 DirectAccess、仮想 LAN (VLAN)
3.4 Identify protocol security concepts	**3.4 プロトコルのセキュリティ概念の確認**
Tunneling, DNSSEC, network sniffing, well-known ports (FTP, HTTP, HTTPS, DNS, RDP, Telnet, SSH, LDAP, LDAPS, SNMP, SMTP, IMAP, SFTP)	トンネリング、DNSSEC、ネットワークスニッフィング、ウェルノウン ポート（FTP、HTTP、HTTPS、DNS、RDP、Telnet、SSH、LDAP、LDAPS、SNMP、SMTP、IMAP、SFTP）
4. Secure Computing	**4. 安全なコンピューター利用**
4.1 Implement email protection	**4.1 電子メール保護の実施**
Antispam, spoofing, phishing, and pharming, client protection, user training	スパム対策、スプーフィング（なりすまし）、フィッシング、ファーミング、クライアントの保護、ユーザー教育
4.2 Manage browser security	**4.2 ブラウザーのセキュリティ管理**
Browser settings, cache management, private browsing	ブラウザーの設定、キャッシュの管理、プライベートブラウジング
4.3 Install and configure anti-malware and antivirus software	**4.3 マルウェア対策ソフトやウイルス対策ソフトのインストールと設定**
Installing, uninstalling, reinstalling, and updating; remediation, scheduling scans, investigating alerts	インストール、アンインストール、再インストール、アップデート、修復、スキャンのスケジュール設定、アラートの調査