CompTIA Security+ 認定資格試験出題範囲

試験番号：**SY0-601**

試験について

CompTIA Security+認定資格試験は、以下の必要な知識とスキルを持っていることを証明します：

- エンタープライズ環境のセキュリティ態勢を評価し、適切なセキュリティソリューションを推奨および実装する
- ククラウド、モバイル、IoTなどハイブリッド環境のセキュリティを確保しモニタリングする
- ガバナンス、リスク、コンプライアンスの原則を含む適切な法律やポリシーを認識したうえで運用する
- セキュリティイベントやインシデントの識別分析、対応を実施する

CompTIA Security+は、セキュリティ/システム管理者として2年間の実務経験に相当するスキルを目安に設計されています。

出題範囲に掲載された項目は、認定資格試験の目的を明確にするためのものであり、試験の出題内容を完全に網羅したものではありません。

試験開発

CompTIAの認定資格試験は、ITプロフェッショナルに必要とされるスキルと知識に関して検討する、専門分野のエキスパートによるワークショップ、および業界全体へのアンケートの調査結果に基づいて策定されています。

CompTIA認定教材の使用に関するポリシー

CompTIA Certifications, LLCは、無許可の第三者トレーニングサイト（通称「ブレインダンプ」）とは提携関係がなく、これらが提供するいかなるコンテンツも公認・推薦・容認しません。CompTIAの認定資格試験の受験準備にこのような教材を使用した個人は、CompTIA受験者同意書の規定に基づいて資格認定を取り消され、その後の受験資格を停止されます。CompTIAでは、無許可教材の使用に関する試験実施ポリシーをよりよく理解していただくための取り組みを進めています。認定資格試験を受験される方は、CompTIA認定資格試験実施ポリシーをご一読ください。CompTIAの認定資格試験を受験するための学習を始める前には、必ずCompTIAが定めるすべてのポリシーをご確認ください。受験者には、CompTIA受験者同意書の規定を遵守することが求められています。個々の教材が無許可扱いになるかどうかを確認するには、CompTIA (examsecurity@comptia.org) までメールにてご確認ください。

注意事項

箇条書きで挙げられた項目は、すべての試験内容を網羅するものではありません。この出題範囲に掲載がない場合でも、各分野に関連する技術、プロセス、あるいはタスクを含む問題が出題される可能性があります。CompTIAでは、提供している認定資格試験の内容に現在必要とされているスキルを反映するため、また試験問題の信頼性維持のため、継続的な試験内容の検討と問題の改訂を行っています。必要に応じて、現在の出題範囲を基に試験を改訂する場合があります。この場合、現在の試験に関連する資料・教材等は、継続的にご利用いただくことが可能です。

試験情報

試験番号	SY0-601
問題数	最大90問
出題形式	単一/複数選択、パフォーマンスベーステスト
試験時間	90分
推奨経験	• セキュリティに重点を置いたITシステム管理における最低2年間の業務経験 • 技術的情報セキュリティの実務経験 • セキュリティコンセプトに関する幅広い知識
合格ライン	750 (100〜900のスコア形式)

試験の出題範囲 (試験分野)

下表は、この試験における試験分野 (ドメイン) と出題比率の一覧です:

試験分野	出題比率
1.0 攻撃、脅威、脆弱性	24%
2.0 アーキテクチャと設計	21%
3.0 実装	25%
4.0 運用とインシデントレスポンス	16%
5.0 ガバナンス、リスク、コンプライアンス	14%
計	**100%**

1.0 脅威、攻撃、脆弱性

1.1 異なるタイプのソーシャルエンジニアリング手法を比較対照することができる。

- フィッシング
- スミッシング
- ビッシング
- スパム
- インスタントメッセージに対するスパム **(SPIM)**
- スピアフィッシング
- ダンプスターダイビング
- ショルダーサーフィン
- ファーミング
- テールゲート (共連れ)
- 情報抽出
- ホエーリング
- プリペンディング
- 身分詐称
- 請求書詐欺
- クレデンシャルハーベスティング
- 偵察
- デマウイルス **(Hoax)**
- なりすまし
- 水飲み場型攻撃
- タイポスクワッティング
- プリテキスティング
- インフルエンスキャンペーン
  - ハイブリッド戦争
  - ソーシャルメディア
- 原則 (有効性の理由)
  - 権威 (Authority)
  - 脅迫 (Intimidation)
  - 多数意見 (Consensus)
  - 希少性 (Scarcity)
  - 親しみ (Familiarity)
  - 信頼性 (Trust)
  - 緊急性 (Urgency)

1.2 与えられたシナリオに基づいて、可能性のあるインジケーターを分析して攻撃の種類を特定することができる。

- マルウェア
  - ランサムウェア
  - トロイの木馬
  - ワーム
  - 望ましくない可能性のあるプログラム (PUP)
  - ファイルレスウイルス
  - コマンド＆コントロール
  - ボット
  - クリプトマルウェア
  - ロジックボム
  - スパイウェア
  - キーロガー
  - リモートアクセス型トロイの木馬 (RAT)
  - ルートキット
  - バックドア
- パスワード攻撃
  - スプレー攻撃
  - 辞書攻撃
  - ブルートフォース攻撃
    - オフライン
    - オンライン
  - レインボーテーブル
  - プレーンテキスト/非暗号化
- 物理攻撃
  - 悪意のあるユニバーサルシリアルバス (USB) ケーブル
  - 悪意のあるフラッシュドライブ
  - カードクローニング
  - スキミング
- 敵対的人工知能 **(AI)**
  - 機械学習 (ML) 用汚染データ
  - 機械学習アルゴリズムのセキュリティ
- サプライチェーン攻撃
- クラウドベース攻撃とオンプレミス攻撃
- 暗号攻撃
  - 誕生日攻撃
  - 衝突攻撃
  - ダウングレード攻撃

1.3 与えられたシナリオに基づいて、アプリケーション攻撃に関連する可能性のあるインジケーターを分析することができる。

- 特権エスカレーション
- クロスサイトスクリプティング
- インジェクション
  - SQLインジェクション
  - DLLインジェクション
  - LDAPインジェクション
  - XMLインジェクション
- ポインタ/オブジェクトデリファレンス
- ディレクトリトラバーサル
- バッファオーバーフロー
- 競合状態
  - TOC/TOU
- エラーハンドリング
- 不適切な入力処理
- リプレイ攻撃
  - セッションリプレイ
- 整数オーバーフロー
- リクエストフォージェリ
  - サーバーサイド
  - クロスサイト
- アプリケーションプログラミングインタフェース **(API)** 攻撃
- リソースの枯渇
- メモリリーク
- **Secure Sockets Layer (SSL)** ストリップ
- ドライバ操作
  - シミング
  - リファクタリング
- **Pass-the-hash**攻撃

1.4 与えられたシナリオに基づいて、ネットワーク攻撃に関連する可能性のあるインジケーターを分析することができる。

- 無線
  - エビルツイン (Evil twin)
  - 不正なアクセスポイント
  - ブルースナーフィング
  - ブルージャッキング
  - ディスアソシエーション
  - ジャミング
  - Radio Frequency Identification (RFID)
  - 近距離無線通信 (NFC)
  - 初期化ベクトル (IV)
- **On-Path**攻撃 (以前の中間者攻撃/マン・イン・ザ・ブラウザ攻撃)
- レイヤ**2**攻撃
  - アドレス解決プロトコル (ARP) ポイズニング
  - メディアアクセスコントロール (MAC) フラッディング
  - MACクローニング
- ドメインネームシステム **(DNS)**
  - ドメインハイジャッキング
  - DNSポイズニング
  - Uniform Resource Locator (URL) リダイレクション
  - ドメインの評価
- 分散型サービス拒否 **(DDoS)**
  - ネットワーク
  - アプリケーション
  - オペレーショナルテクノロジー (OT)
- 悪意あるコードまたはスクリプトの実行
  - PowerShell
  - Python
  - Bash
  - マクロ
  - Visual Basic for Applications (VBA)

1.5 様々な脅威アクター、ベクター、インテリジェンスソースを説明することができる。

- アクターと脅威
  - 高度標的型攻撃 (APT)
  - インサイダー脅威
  - 国家アクター
  - ハクティビスト
  - スクリプトキディ
  - 犯罪シンジケート
  - ハッカー
    - 承認されている (Authorized)
    - 承認されていない (Unauthorized)
    - 部分的に承認されている (Semi-authorized)
  - シャドーIT
  - 競合相手
- 行為主体の属性
  - 内部/外部
  - 巧妙さ/能力のレベル
  - リソース/資金
  - 意図/動機
- ベクトル
  - 直接アクセス
  - 無線
  - Eメール
  - サプライチェーン
  - ソーシャルメディア
  - リムーバブルメディア
  - クラウド
- 脅威インテリジェンスソース
  - オープンソースインテリジェンス (OSINT)
  - クローズド/専用
  - 脆弱性データベース
  - パブリック/プライベート情報共有センター
  - ダークウェブ
  - セキュリティ侵害インジケーター (IoC)
  - Automated Indicator Sharing (AIS)
    - 脅威情報構造化記述形式 (STIX)/検知インジケーター情報自動交換手順 (TAXII)
  - 予測分析
  - 脅威マップ
  - ファイル/コードリポジトリ
- リサーチソース
  - ベンダーウェブサイト
  - 脆弱性フィード
  - カンファレンス
  - 学術誌
  - Request for Comments (RFC)
  - 特定の業界グループ
  - ソーシャルメディア
  - 脅威フィード
  - 攻撃者の戦術、技術、手順 (TTP)

1.6 様々な脆弱性のタイプによるセキュリティの懸念について説明することができる。

- クラウドベースの脆弱性とオンプレミスの脆弱性
- ゼロデイ攻撃
- 脆い設定
  - 開放された権限
  - セキュアでないルートアカウント
  - エラー
  - 弱い暗号化
  - セキュアでないプロトコル
  - デフォルトの設定
  - オープンポートとサービス
- サードパーティのリスク
  - ベンダー管理
    - システム統合
    - ベンダーサポートの欠如
  - サプライチェーン
  - コード開発のアウトソース
  - データストレージ
- 不適切または脆いパッチ管理
  - ファームウェア
  - オペレーティングシステム (OS)
  - アプリケーション
- レガシープラットフォーム
- インパクト
  - データ損失
  - 情報侵害
  - データ流出
  - 身元詐称
  - 財務
  - 評判
  - 可用性損失

1.7 セキュリティ評価で使用する手法を要約することができる。

- 脅威ハンティング
  - インテリジェンスの融合
  - 脅威フィード
  - アドバイザリーと報告
  - 策略
- 脆弱性スキャン
  - フォールスポジティブ
  - フォールスネガティブ
  - ログのレビュー
  - クレデンシャルとノンクレデンシャル
  - 侵入型と非侵入型
  - アプリケーション
  - ウェブアプリケーション
  - ネットワーク
  - 共通脆弱性識別子 (CVE)/共通脆弱性評価システム (CVSS)
  - 構成レビュー
- **Syslog**/セキュリティ情報イベントマネジメント **(SIEM)**
  - レビューレポート
  - パケットキャプチャ
  - データ入力
  - ユーザー行動分析
  - センチメント分析
  - セキュリティ監視
  - ログ集約
  - ログコレクター
- **Security Orchestration, Automation, and Response (SOAR)**

1.8 ペネトレーションテストで使用する手法を説明することができる。

- ペネトレーションテスト
  - 既知の環境
  - 未知の環境
  - 部分的に既知の環境
  - 実施条件 (Rules of engagement)
  - ラテラルムーブメント
  - 特権エスカレーション
  - 永続性
  - クリーンアップ
  - バグバウンティ
  - ピボッティング
- パッシブ偵察とアクティブ偵察
  - ドローン
  - ウォーフライング
  - ウォードライビング
  - フットプリンティング
  - OSINT
- 演習タイプ
  - レッドチーム
  - ブルーチーム
  - ホワイトチーム
  - パープルチーム

2.0 アーキテクチャと設計

2.1 エンタープライズ環境におけるセキュリティコンセプトの重要性を説明することができる。

- 構成管理
  - ダイアグラム
  - ベースライン構成
  - 標準命名規則
  - インターネットプロトコル (IP) スキーム
- データ主権
- データ保護
  - データ損失防止 (DLP)
  - マスキング
  - 暗号化
  - 休眠中
  - 転送/動作中
  - 処理中
  - トークナイゼーション
  - 権利管理
- 地理的考慮事項
- 対応制御と復旧制御
- セキュアソケットレイヤー **(SSL)**/トランスポートレイヤーセキュリティ **(TLS)** の検査
- ハッシング
- **API**の考慮事項
- サイトのレジリエンス
  - ホットサイト
  - コールドサイト
  - ウォームサイト
- 欺瞞と混乱
  - ハニーポット
  - ハニーファイル
  - ハニーネット
  - フェイクテレメトリー
  - DNSシンクホール

2.2 仮想化コンセプトとクラウドコンピューティングのコンセプトを要約することができる。

- クラウドモデル
  - Infrastructure as a Service (IaaS)
  - Platform as a Service (PaaS)
  - Software as a Service (SaaS)
  - Anything as a service (XaaS)
  - パブリック
  - コミュニティ
  - プライベート
  - ハイブリッド
- クラウドサービスプロバイダー
- マネージドサービスプロバイダー **(MSP)**/マネージドセキュリティサービスプロバイダー **(MSSP)**
- オンプレミスとオフプレミス
- フォグコンピューティング
- エッジコンピューティング
- シンクライアント
- コンテナ
- マイクロサービス/**API**
- **Infrastructure as Code**
  - ソフトウェア定義ネットワーク (SDN)
  - ソフトウェア定義ビジビリティ (SDV)
- サーバーレスアーキテクチャ
- サービス統合
- リソースポリシー
- トランジットゲートウェイ
- 仮想化
  - 仮想マシン (VM)
  - スプロール回避
  - VMエスケープへの対策

2.3 セキュアなアプリケーションの開発、デプロイ、自動化に関するコンセプトを要約することができる。

- 環境
  - 開発
  - テスト
  - ステージング
  - プロダクション
  - 品質保証
- プロビジョニング、デプロビジョニング
- 完全性測定
- セキュアコーディングテクニック
  - 正規化
  - ストアドプロシージャ
  - 難読化/カモフラージュ
  - コード再利用/デッドコード
  - サーバー側とクライアント側での実行と検証の違い
  - メモリ管理
  - サードパーティのライブラリやソフトウェア開発キット (SDK) の利用
  - データ露出
- **Open Web Application Security Project (OWASP)**
- ソフトウェアダイバーシティ
  - コンパイラ
  - バイナリ
- 自動化/スクリプティング
  - 一連の行動の自動化
  - 継続的モニタリング
  - 継続的バリデーション
  - 継続的インテグレーション
  - 継続的デリバリー
  - 継続的デプロイメント
- エラスティシティ (弾性)
- 拡張性
- バージョン管理

2.4 認証と認可の設計コンセプトを要約することができる。

- 認証方法
  - ディレクトリサービス
  - フェデレーション
  - アテステーション
  - テクノロジー
    - タイムベースドワンタイムパスワード (TOTP)
    - HMACベースドワンタイムパスワード (HOTP)
    - ショートメッセージサービス (SMS)
    - トークンキー
    - 静的コード
    - 認証アプリケーション
    - プッシュ通知
    - 通話
  - スマートカード認証
- 生体認証
  - 指紋認証
  - 網膜認証
  - 虹彩認証
  - 顔認証
  - 音声認証
  - 静脈認証
  - 歩行分析
  - 有効率
  - 他人受入
  - 本人拒否
  - クロスオーバーエラー率
- 多要素認証 **(MFA)** の要素と属性
  - 要素
    - Something you know
    - Something you have
    - Something you are
  - 属性
    - Somewhere you are
    - Something you can do
    - Something you exhibit
    - Someone you know
- 認証、認可、アカウンティング **(AAA)**
- クラウドとオンプレミスの要件の違い

2.5 与えられたシナリオに基づいて、サイバーセキュリティのレジリエンスを実装することができる。

- 冗長性
  - 地理的分散
  - ディスク
    - RAID レベル
    - マルチパス
  - ネットワーク
    - ロードバランサー
    - ネットワークインターフェースカード (NIC) チーミング
  - 電源
    - 無停電電源 (UPS)
    - ジェネレータ
    - デュアル電源
    - マネージド電力分配ユニット (PDU)
- レプリケーション
  - ストレージエリアネットワーク
  - VM
- オンプレミスとクラウドの違い
- バックアップの種類
  - フル
  - 増分
  - スナップショット
  - 差分
  - テープ
  - ディスク
  - コピー
  - ネットワークアタッチトストレージ (NAS)
  - ストレージエリアネットワーク
  - クラウド
  - イメージ
  - オンラインとオフラインの違い
  - オフサイトストレージ
    - 距離の考慮事項
- 非永続性 (ノンパーシスタンス)
  - 既知の状態に復帰
  - 最後に確認された正しい設定
  - Live Bootメディア
- 高可用性
  - 拡張性
- 回復順序
- ダイバーシティ
  - テクノロジー
  - ベンダー
  - 暗号化
  - コントロール

2.6 組み込みシステムおよび特殊システムがもたらすセキュリティ上の影響について説明することができる。

- 組み込みシステム
  - Raspberry Pi
  - フィールドプログラマブルゲートアレイ (FPGA)
  - Arduino
- 監視制御とデータ収集 **(SCADA)**/産業用制御システム **(ICS)**
  - 設備
  - 産業
  - 製造部門
  - エネルギー
  - ロジスティクス
- **Internet of Things (IoT)**
  - センサー
  - スマートデバイス
  - ウェアラブル
  - ファシリティの自動化
  - 脆いデフォルト
- 専門
  - 医療システム
  - 車両
  - 航空機
  - スマートメーター
- ボイスオーバーインターネットプロトコル **(VoIP)**
- 暖房、換気、および空調 **(HVAC)**
- ドローン
- 複合機 **(MFP)**
- リアルタイムオペレーティングシステム **(RTOS)**
- 監視システム
- システム・オン・チップ **(SoC)**
- 通信の考慮事項
  - 5G
  - ナローバンド
  - ベースバンド無線
  - 加入者識別モジュール (SIM) カード
  - Zigbee
- 制約
  - 電源
  - コンピュート
  - ネットワーク
  - 暗号化
  - パッチ不可
  - 認証
  - 範囲
  - 費用
  - 暗黙的信頼

2.7 物理的セキュリティコントロールの重要性について説明することができる。

- ボラード/バリケード
- アクセスコントロールが実施されている玄関
- バッジ
- アラーム
- 標識
- カメラ
  - 動作認識
  - 物体検出
- 閉鎖回路テレビ **(CCTV)**
- 産業施設カモフラージュ
- 人的
  - 警備員
  - ロボット警備
  - 受付
  - 2人ルールの適用 (TPI)/コントロール
- 施錠
  - 生体認証
  - 電子的施錠
  - 物理的施錠
  - ワイヤーロック
- **USB**データブロッカー
- 照明
- 柵
- 消火
- センサー
  - 人感センサー
  - ノイズ検出
  - 非接触カードリーダー
  - 湿気検出
  - カード
  - 温度
- ドローン
- ビジターログ
- ファラデーケージ
- エアギャップ
- スクリーンサブネット (以前の「非武装地帯」)
- ケーブル配線の保護
- セキュア領域
  - エアギャップ
  - 保管室
  - 金庫
  - ホットアイル
  - コールドアイル
- セキュアなデータ破棄
  - 焼却
  - シュレッディング
  - 溶解
  - 粉砕
  - 消磁
  - サードパーティのソリューション

2.8 暗号化コンセプトの基本を要約することができる。

- デジタル署名
- 鍵の長さ
- 鍵ストレッチング
- ソルトの使用
- ハッシング
- 鍵交換
- 楕円曲線暗号
- 完全前方秘匿性 **(PFS)**
- 量子暗号
  - 通信
  - コンピューティング
- ポスト量子暗号
- 一時的
- 利用モード
  - 認証済み
  - 未認証
  - カウンター
- ブロックチェーン
  - 公開台帳
- 暗号スイート
  - ストリーム
  - ブロック
- 対称と非対称
- 軽量暗号
- ステガノグラフィ
  - オーディオ
  - ビデオ
  - イメージ
- 準同型暗号
- 一般的な適用例
  - 低電力デバイス
  - 低レイテンシー
  - 高レジリエンス
  - 機密性への対応
  - 完全性への対応
  - 難読化への対応
  - 認証への対応
  - 否認防止への対応
- 制限
  - 速度
  - サイズ
  - 弱い鍵
  - 時間
  - 有効期限
  - 予測可能性
  - 再利用
  - エントロピー
  - 演算オーバーヘッド
  - リソース上の制約とセキュリティ上の制約

3.0 実装

3.1 与えられたシナリオに基づいて、セキュアなプロトコルの実装を行うことができる。

- プロトコル
  - Domain Name System Security Extensions (DNSSEC)
  - SSH
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Secure Real-time Transport Protocol (SRTP)
  - Lightweight Directory Access Protocol Over SSL (LDAPS)
  - File Transfer Protocol over SSL/TLS (FTPS)
  - SSH File Transfer Protocol (SFTP)
  - Simple Network Management Protocol Version3 (SNMPv3)
  - Hypertext Transfer Protocol Secure (HTTPS)
  - IPSec
    - Authentication Header (AH)/ Encapsulated Security Payload (ESP)
    - トンネル/トランスポート
  - ポストオフィスプロトコル (POP)/ インターネットメッセージアクセスプロトコル (IMAP)
- 用途
  - 音声および動画
  - 時刻同期
  - EメールおよびWeb
  - ファイル転送
  - ディレクトリサービス
  - リモートアクセス
  - ドメイン名解決
  - ルーティングおよびスイッチング
  - ネットワークアドレスの割り当て
  - サブスクリプションサービス

3.2 与えられたシナリオに基づいて、ホストまたはアプリケーションのセキュリティソリューションを実装することができる。

- エンドポイントプロテクション
  - アンチウイルス
  - アンチマルウェア
  - エンドポイントにおける検知と対応 (EDR)
  - DLP
  - 次世代ファイアウォール (NGFW)
  - ホスト型侵入防止システム (HIPS)
  - ホスト型侵入検知システム (HIDS)
  - ホスト型ファイアウォール
- ブート時の完全性
  - ブートセキュリティ/Unified Extensible Firmware Interface (UEFI)
  - メジャーブート
  - ブートアテステーション
- データベース
  - トークナイゼーション
  - ソルトの使用
  - ハッシング
- アプリケーションセキュリティ
  - 入力確認
  - セキュア属性 (Secure Cookies)
  - Hypertext Transfer Protocol (HTTP) ヘッダー
  - コード署名
  - 許可リスト
  - ブロックリスト/拒否リスト
  - セキュアコーディングプラクティス
  - 静的コード分析
    - 手動コードレビュー
  - 動的コード分析
  - ファジング
- 要塞化
  - オープンポートとサービス
  - レジストリ
  - ディスク暗号化
  - OS
  - パッチ管理
    - サードパーティの更新
    - 自動更新
- 自己暗号化ドライブ **(SED)**/フルディスク暗号化 **(FDE)**
  - Opal仕様
- ハードウェアの信頼の起点
- **Trusted Platform Module (TPM)**
- サンドボックス化

3.3 与えられたシナリオに基づいて、セキュアなネットワークデザインを実装することができる。

- ロードバランシング
  - アクティブ/アクティブ
  - アクティブ/パッシブ
  - スケジューリング
  - 仮想IP
  - 永続性
- ネットワークセグメンテーション
  - バーチャルローカルエリアネットワーク (VLAN)
  - スクリーンサブネット (以前の「非武装地帯」)
  - East-Westトラフィック
  - エクストラネット
  - イントラネット
  - ゼロトラスト
- 仮想プライベートネットワーク **(VPN)**
  - 常時オン
  - スプリットトンネルとフルトンネルの違い
  - リモートアクセスとサイトツーサイトの違い
  - IPSec
  - SSL/TLS
  - HTML5
  - Layer 2 Tunneling Protocol (L2TP)
- **DNS**
- ネットワークアクセスコントロール **(NAC)**
  - エージェント型とエージェントレス型
- アウトオブバンド管理
- ポートセキュリティ
  - ブロードキャストストーム防止
  - Bridge Protocol Data Unit (BPDU) ガード
  - ループ防止
  - Dynamic Host Configuration Protocol (DHCP) スヌーピング
  - メディアアクセスコントロール (MAC) フィルタリング
- ネットワークアプライアンス
  - 踏み台サーバー
  - プロキシサーバー
    - フォワーディング
    - リバース
  - ネットワーク型侵入検知システム (NIDS)/ネットワーク型侵入防止システム (NIPS)
    - シグネチャベース
    - ヒューリスティック/ビヘイビア
    - アノマリ
    - インラインとパッシブの違い
  - HSM
  - センサー
  - コレクター
  - アグリゲーター
  - ファイアウォール
    - Webアプリケーションファイアウォール (WAF)
    - NGFW
    - ステートフル
    - ステートレス
    - Unified threat management (UTM)
    - ネットワークアドレス変換 (NAT) ゲートウェイ
    - コンテンツ/URLフィルター
    - オープンソースとプロプライエタリの違い
    - ハードウェアとソフトウェアの違い
    - アプライアンスとホストベースと仮想の違い
- アクセスコントロールリスト **(ACL)**
- 経路セキュリティ
- サービス品質 (QoS)
- **IPv6**の影響
- ポートスパニング/ポートミラーリング
  - ポートタップ
- モニタリングサービス
- ファイル完全性モニタリング

3.4 与えられたシナリオに基づいて、ワイヤレスセキュリティ設定をインストール、構成することができる。

- 暗号化プロトコル
  - WiFi Protected Access 2 (WPA2)
  - WiFi Protected Access 3 (WPA3)
  - Counter-mode/CBC-MAC Protocol (CCMP)
  - 同等性同時認証 (SAE)
- 認証プロトコル
  - Extensible Authentication Protocol (EAP)
  - Protected Extensible Authentication Protocol (PEAP)
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1X
  - Remote Authentication Dial-in User Service (RADIUS) フェデレーション
- 方式
  - 事前共有キー (PSK) とエンタープライズとオープンの違い
  - WiFi Protected Setup (WPS)
  - キャプティブポータル
- インストールの考慮事項
  - 現地調査
  - ヒートマップ
  - WiFiアナライザー
  - チャネルのオーバーラップ
  - ワイヤレスアクセスポイント (WAP) の配置
  - コントローラーとアクセスポイントのセキュリティ

3.5 与えられたシナリオに基づいて、セキュアなモバイルソリューションを実装することができる。

- 接続の方法とレシーバー
  - 携帯電話
  - Wi-Fi
  - Bluetooth
  - NFC
  - 赤外線
  - USB
  - ポイントツーポイント
  - ポイントツーマルチポイント
  - Global Positioning System (GPS)
  - RFID
- モバイルデバイス管理 **(MDM)**
  - アプリケーション管理
  - コンテンツ管理
  - リモートワイプ
  - ジオフェンシング
  - ジオロケーション
  - 画面ロック
  - プッシュ通知
  - パスワードとPIN
  - 生体認証
  - コンテキストアウェア認証
  - コンテナ化
  - ストレージセグメンテーション
  - フルデバイス暗号化
- モバイルデバイス
  - MicroSDハードウェアセキュリティモジュール (HSM)
  - MDM/統合エンドポイント管理 (UEM)
  - モバイルアプリケーション管理 (MAM)
  - SEAndroid
- 強制と監視
  - サードパーティのアプリケーションストア
  - root化/ジェイルブレイク
  - サイドローディング
  - カスタムファームウェア
  - キャリア端末のロック解除
  - Firmware over-the-air (OTA) の更新
  - カメラの使用
  - SMS/マルチメディアメッセージングサービス (MMS)/リッチコミュニケーションサービス (RCS)
  - 外付けメディア
  - USB On-The-Go (USB OTG)
  - 録音マイク
  - GPSタグの付与
  - Wi-Fi Direct/アドホック
  - テザリング
  - ホットスポット
  - 決済方法
- 導入モデル
  - Bring your own device (BYOD)
  - Corporate-owned personally enabled (COPE)
  - Choose your own device (CYOD)
  - 会社所有
  - 仮想デスクトップインフラストラクチャ (VDI)

3.6 与えられたシナリオに基づいて、クラウドにサイバーセキュリティソリューションを適用することができる。

- クラウドセキュリティコントロール
  - ゾーン全体の高可用性
  - リソースポリシー
  - シークレット管理
  - 統合と監査
  - ストレージ
    - 権限
    - 暗号化
    - レプリケーション
    - 高可用性
  - ネットワーク
    - 仮想ネットワーク
    - パブリックサブネットとプライベートサブネット
    - セグメンテーション
    - API検査と統合
  - コンピュート
    - セキュリティグループ
    - 動的リソース割り当て
    - インスタンス認識
    - 仮想プライベートクラウド (VPC) エンドポイント
    - コンテナのセキュリティ
- ソリューション
  - CASB
  - アプリケーションセキュリティ
  - 次世代セキュアウェブゲートウェイ (SWG)
  - クラウド環境におけるファイアウォールの考慮事項
    - 費用
    - セグメンテーションの必要性
    - Open Systems Interconnection (OSI) レイヤー
- クラウドネイティブコントロールとサードパーティソリューションの違い

3.7 与えられたシナリオに基づいて、認証管理とアカウント管理の制御を実装することができる。

- アイデンティティ
  - アイデンティティプロバイダ (IdP)
  - 属性
  - 証明書
  - トークン
  - SSHキー
  - スマートカード
- アカウントの種類
  - ユーザーアカウント
  - 共有アカウントと一般アカウント/資格情報
  - ゲストアカウント
  - サービスアカウント
- アカウントポリシー
  - パスワードの複雑さ
  - パスワード履歴
  - パスワード再利用
  - ネットワークロケーション
  - ジオフェンシング
  - ジオタギング
  - ジオロケーション
  - 時間ベースのログイン
  - アクセスポリシー
  - アカウント権限
  - アカウント監査
  - 不可能な移動時間/危険なログイン
  - ロックアウト
  - 無効化

3.8 与えられたシナリオに基づいて、認証と認可のソリューションを導入することができる。

- 認証管理
  - パスワードキー
  - パスワードボールト
  - TPM
  - HSM
  - 知識ベースの認証
- 認証/認可
  - EAP
  - Challenge-Handshake Authentication Protocol (CHAP)
  - Password Authentication Protocol (PAP)
  - 802.1X
  - RADIUS
  - シングルサインオン (SSO)
  - Security Assertions Markup Language (SAML)
  - Terminal Access Controller Access Control System Plus (TACACS+)
  - OAuth
  - OpenID
  - ケルベロス
- アクセスコントロールスキーム
  - Attribute-based access control (ABAC)
  - ロールベースアクセス制御
  - ルールベースアクセス制御
  - 強制アクセス制御 (MAC)
  - 任意アクセス制御 (DAC)
  - 条件付アクセス
  - 特権アクセス管理
  - ファイルシステム権限

3.9 与えられたシナリオに基づいて、公開鍵インフラストラクチャを実装することができる。

- 公開鍵インフラストラクチャ **(PKI)**
  - 鍵管理
  - 認証局 (CA)
  - 中間CA
  - 登録認定機関 (RA)
  - 証明書失効リスト (CRL)
  - 証明書属性
  - Online Certificate Status Protocol (OCSP)
  - 証明書署名要求 (CSR)
  - コモンネーム (CN)
  - サブジェクト代替名
  - 有効期限
- 証明書の種類
  - ワイルドカード
  - サブジェクト代替名
  - コード署名
  - 自己署名
  - マシン/コンピューター
  - Eメール
  - ユーザー
  - ルート
  - ドメイン認証
  - EV証明書
- 証明書の形式
  - 識別符号化規則 (DER)
  - プライバシー強化電子メール (PEM)
  - 個人情報交換 (PFX)
  - .cer
  - P12
  - P7B
- コンセプト
  - オンラインCAとオフラインCAの違い
  - ステープリング
  - ピンニング
  - 信頼モデル
  - キーエスクロー
  - 証明書チェーン

4.0 運用とインシデントレスポンス

4.1 与えられたシナリオに基づいて、適切なツールを利用して組織のセキュリティにアクセスすることができる。

- ネットワークの偵察と発見
  - tracert/traceroute
  - nslookup/dig
  - ipconfig/ifconfig
  - nmap
  - ping/pathping
  - hping
  - netstat
  - netcat
  - IPスキャナー
  - arp
  - route
  - curl
  - theHarvester
  - sn1per
  - scanless
  - dnsenum
  - Nessus
  - Cuckoo
- ファイル操作
  - head
  - tail
  - cat
  - grep
  - chmod
  - logger
- シェル環境とスクリプト環境
  - SSH
  - PowerShell
  - Python
  - OpenSSL
- パケットキャプチャとリプレイ
  - Tcpreplay
  - Tcpdump
  - Wireshark
- フォレンジック
  - dd
  - Memdump
  - WinHex
  - FTK imager
  - Autopsy
- エクスプロイトフレームワーク
- パスワードクラッカー
- データのサニタイズ

4.2 インシデントレスポンスのポリシー、プロセス、手順の重要性を要約することができる。

- インシデントレスポンス計画
- インシデントレスポンスプロセス
  - 準備
  - 識別
  - 封じ込め
  - 根絶
  - 復旧
  - 教訓の管理
- 演習
  - 机上演習
  - ウォークスルー
  - シミュレーション
- 攻撃フレームワーク
  - MITRE ATT&CK
  - 侵入分析のダイヤモンドモデル
  - サイバーキルチェーン
- ステークホルダー管理
- コミュニケーション計画
- 災害復旧計画
- 事業継続計画
- 業務計画の継続性 **(COOP)**
- インシデントレスポンスチーム
- 保持ポリシー

4.3 想定されたインシデントに基づき、適切なデータソースを使用して調査をサポートすることができる。

- 脆弱性スキャンの出力
- **SIEM**ダッシュボード
  - センサー
  - 機密度
  - 傾向
  - 警告
  - 相関分析
- ログファイル
  - ネットワーク
  - システム
  - アプリケーション
  - セキュリティ
  - ウェブ
  - DNS
  - 認証
  - ダンプファイル
  - VoIPとコールマネージャー
  - セッション開始プロトコル (SIP) トラフィック
- **syslog/rsyslog/syslog-ng**
- **journalctl**
- **NXLog**
- 帯域幅モニター
- メタデータ
  - Eメール
  - モバイル
  - ウェブ
  - ファイル
- **Netflow/sFlow**
  - Netflow
  - sFlow
  - IPFIX
- プロトコルアナライザーの出力

4.4 想定されたインシデントに基づき、低減技術や制御を適用して環境を保護することができる。

- エンドポイントのセキュリティソリューションの再設定
  - アプリケーション認定リスト
  - アプリケーションブロック/拒否リスト
  - 検疫
- 構成変更
  - ファイアウォールのルール
  - MDM
  - DLP
  - コンテンツフィルター/URLフィルター
  - 証明書の更新または失効
- 分離
- 封じ込め
- セグメンテーション
- **SOAR**
  - ランブック
  - プレイブック

4.5 デジタルフォレンジックの重要な側面について説明することができる。

- 文書化/証拠
  - 訴訟ホールド
  - ビデオ
  - 容認可能性
  - 証拠の連鎖
  - 一連のイベントのタイムライン
    - タイムスタンプ
    - タイムオフセット
  - タグ
  - レポート
  - イベントログ
  - インタビュー
- 取得
  - データの揮発性
  - ディスク
  - ランダムアクセスメモリー (RAM)
  - スワップ/ページファイル
  - OS
  - 機器
  - ファームウェア
  - スナップショット
  - キャッシュ
  - ネットワーク
  - アーティファクト
- オンプレミスとクラウドの違い
  - 監査権
  - 規制/管轄権
  - データ侵害の通知に関する法
- 完全性
  - ハッシング
  - チェックサム
  - 出所
- 保全
- eディスカバリー
- データのリカバリ
- 否認防止
- 戦略的なインテリジェンス/カウンターインテリジェンス

5.0 ガバナンス、リスク、コンプライアンス

5.1 様々な制御タイプを比較対照することができる。

- カテゴリ
  - 管理的
  - 運用的
  - 技術的
- 制御のタイプ
  - 予防的
  - 検知的
  - 是正的
  - 抑止的
  - 補正的
  - 物理的

5.2 組織のセキュリティ態勢に影響を及ぼす適用される規制、標準、フレームワークの重要性について説明できる。

- 規制、標準、法律
  - 一般データ保護規則 (GDPR)
  - 国内法、領土法、または州法
  - クレジットカード業界データセキュリティスタンダード (PCI DSS)
- 主要なフレームワーク
  - インターネットセキュリティセンター (CIS)
  - 米国国立標準技術研究所 (NIST) リスク管理フレームワーク (RMF)/ サイバーセキュリティフレームワーク (CSF)
  - 国際標準化機構 (ISO) 27001/27002/27701/31000
  - SSAE SOC 2 Type I/II
  - クラウドセキュリティアライアンス
  - クラウドコントロールマトリックス
  - リファレンスアーキテクチャ
- ベンチマーク/セキュア構成ガイド
  - プラットフォームまたはベンダー固有のガイド
    - Webサーバー
    - OS
    - アプリケーションサーバー
    - ネットワークインフラ機器

5.3 組織のセキュリティに関連するポリシーの重要性について説明することができる。

- 人的
  - 利用規約
  - ジョブローテーション
  - 強制的な休暇
  - 職務分離
  - 最小の権限
  - デスクスペースの清掃
  - バックグラウンドチェック
  - 秘密保持契約書 (NDA)
  - SNS分析
  - オンボーディング
  - オフボーディング
  - ユーザートレーニング
    - ゲーミフィケーション
    - キャプチャーザフラッグ
    - フィッシングキャンペーン
      - フィッシングのシミュレーション
    - コンピューターベーストレーニング (CBT)
    - 役割に基づくトレーニング
- トレーニング技術の多様化
- サードパーティのリスク管理
  - ベンダー
  - サプライチェーン
  - ビジネスパートナー
  - サービスレベル合意書 (SLA)
  - 覚書 (MOU)
  - 測定システム分析 (MSA)
  - ビジネスパートナー契約書 (BPA)
  - エンドオブライフ (EOL)
  - エンドオブサービスライフ (EOSL)
  - NDA
- データ
  - 分類
  - ガバナンス
  - 保持
- 資格情報に関するポリシー
  - 従業員
  - サードパーティ
  - 機器
  - サービスアカウント
  - 管理者/ルートアカウント
- 組織のポリシー
  - 変更管理
  - 変更制御
  - 資産マネジメント

5.4 リスク管理のプロセスとコンセプトについて要約することができる。

- リスクタイプ
  - 外部
  - 内部
  - レガシーシステム
  - マルチパーティ
  - 知的財産窃盗
  - ソフトウェアコンプライアンス/ライセンシング
- リスクマネジメント戦略
  - 受容
  - 回避
  - 移転
    - サイバーセキュリティ保険
  - 低減
- リスク分析
  - リスク登録簿
  - リスクマトリックス/ヒートマップ
  - リスク管理評価
  - リスク管理自己評価
  - リスク認識
  - 固有リスク
  - 残留リスク
  - 統制上リスク
  - リスクアペタイト
  - リスク態勢に影響する規則
  - リスク評価の種類
    - 定性的
    - 定量的
  - 発生可能性
  - 影響
  - 資産価値
  - 単一損失予測 (SLE)
  - 年間損失予測 (ALE)
  - 年間発生率 (ARO)
- 災害
  - 環境的なもの
  - 人的なもの
  - 内部と外部の違い
- ビジネス影響度分析
  - 目標復旧時間 (RTO)
  - 目標復旧時点 (RPO)
  - 平均修復時間 (MTTR)
  - 平均故障間隔 (MTBF)
  - 機能復旧計画
  - 単一障害点
  - 災害復旧計画 (DRP)
  - 業務上必要不可欠な機能
  - クリティカルなシステムの識別
  - サイトリスク評価

5.5 セキュリティに関連するプライバシーおよび機密データの概念を説明することができる。

- プライバシーおよびデータ侵害の組織的結果
  - 風評被害
  - 身元詐称
  - 罰金
  - 知的財産窃盗
- 侵害の通知
  - エスカレーション
  - 公告と開示
- データの種類
  - 分類
    - パブリック
    - プライベート
    - 機密度
    - 機密
    - 重要
    - 専有
  - 個人を識別可能な情報 (PII)
  - 健康情報
  - 財務情報
  - 政府関連データ
  - 顧客データ
- プライバシー強化技術
  - データの最小化
  - データマスキング
  - トークナイゼーション
  - 匿名化
  - 疑似匿名化
- 役割と責任
  - データオーナー
  - データコントローラー
  - データプロセッサー
  - データカストディアン/スチュワード
  - データ保護責任者 (DPO)
- 情報のライフサイクル
- 影響評価
- 合意条件
- プライバシー通知

Security+ (SY0-601) 略語リスト

下記はCompTIA Security+認定資格試験で使用される略語一覧です。包括的な試験準備プログラムの一環として、リストを復習し、知識の習得に努めてください。

略語	定義
3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-based Access Control
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
AES256	Advanced Encryption Standards 256bit
AH	Authentication Header
AI	Artificial Intelligence
AIS	Automated Indicator Sharing
ALE	Annualized Loss Expectancy
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
ASP	Active Server Pages
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AUP	Acceptable Use Policy
AV	Antivirus
BASH	Bourne Again Shell
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partnership Agreement
BPDU	Bridge Protocol Data Unit
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAR	Corrective Action Report
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CBT	Computer-based Training
CCMP	Counter-Mode/CBC-MAC Protocol
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge-Handshake Authentication Protocol
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CIS	Center for Internet Security
CMS	Content Management System
CN	Common Name
COOP	Continuity of Operations Planning
COPE	Corporate-owned Personally Enabled
CP	Contingency Planning
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSA	Cloud Security Alliance
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
CSP	Cloud Service Provider
CSR	Certificate Signing Request
CSRF	Cross-Site Request Forgery
CSU	Channel Service Unit
CTM	Counter-Mode
CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DBA	Database Administrator
DDoS	Distributed Denial-of-Service
DEP	Data Execution Prevention

略語	定義
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman Ephemeral
DKIM	Domain Keys Identified Mail
DLL	Dynamic-link Library
DLP	Data Loss Prevention
DMARC	Domain Message Authentication Reporting and Conformance
DNAT	Destination Network Address Transaction
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial-of-Service
DPO	Data Protection Officer
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECC	Elliptic-curve Cryptography
ECDHE	Elliptic-curve Diffie-Hellman Ephemeral
ECDSA	Elliptic-curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
EFS	Encrypted File System
EIP	Extended Instruction Pointer
EOL	End of Life
EOS	End of Service
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulating Security Payload
ESSID	Extended Service Set Identifier
FACL	File System Access Control List
FDE	Full Disk Encryption
FIM	File Integrity Monitoring
FPGA	Field Programmable Gate Array
FRR	False Rejection Rate
FTP	File Transfer Protocol
FTPS	Secured File Transfer Protocol
GCM	Galois/Counter Mode
GDPR	General Data Protection Regulation
GPG	GNU Privacy Guard
GPO	Group Policy Object
GPS	Global Positioning System
GPU	Graphics Processing Unit
GRE	Generic Routing Encapsulation
HA	High Availability
HDD	Hard Disk Drive
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hash-based Message Authentication Code
HOTP	HMAC-based One-time Password

略語	定義
HSM	Hardware Security Module
HSMaaS	Hardware Security Module as a Service
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, Air Conditioning
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDEA	International Data Encryption Algorithm
IDF	Intermediate Distribution Frame
IdP	Identity Provider
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP4	Internet Message Access Protocol v4
IoC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IR	Incident Response
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
ISFW	Internal Segmentation Firewall
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
ITCP	IT Contingency Plan
IV	Initialization Vector
KDC	Key Distribution Center
KEK	Key Encryption Key
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
MaaS	Monitoring as a Service
MAC	Media Access Control
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDF	Main Distribution Frame
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
ML	Machine Learning

略語	定義
MMS	Multimedia Message Service
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MSA	Measurement Systems Analysis
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAS	Network-attached Storage
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near-field Communication
NFV	Network Function Virtualization
NGFW	Next-generation Firewall
NG-SWG	Next-generation Secure Web Gateway
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NOC	Network Operations Center
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OSI	Open Systems Interconnection
OSINT	Open-source Intelligence
OSPF	Open Shortest Path First
OT	Operational Technology
OTA	Over-The-Air
OTG	On-The-Go
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
P12	PKCS #12
P2P	Peer-to-Peer
PaaS	Platform as a Service
PAC	Proxy Auto Configuration
PAM	Privileged Access Management
PAM	Pluggable Authentication Modules
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBKDF2	Password-based Key Derivation Function 2
PBX	Private Branch Exchange
PCAP	Packet Capture

略語	定義
PCI DSS	Payment Card Industry Data Security Standard
PDU	Power Distribution Unit
PE	Portable Executable
PEAP	Protected Extensible Authentication Protocol
PED	Portable Electronic Device
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PoC	Proof of Concept
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Preshared Key
PTZ	Pan-Tilt-Zoom
PUP	Potentially Unwanted Program
QA	Quality Assurance
QoS	Quality of Service
PUP	Potentially Unwanted Program
RA	Registration Authority
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RAS	Remote Access Server
RAT	Remote Access Trojan
RC4	Rivest Cipher version 4
RCS	Rich Communication Services
RFC	Request for Comments
RFID	Radio Frequency Identification
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RPO	Recovery Point Objective
RSA	Rivest, Shamir, & Adleman
RTBH	Remotely Triggered Black Hole
RTO	Recovery Time Objective
RTOS	Real-time Operating System
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertions Markup Language
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol

略語	定義
SCEP	Simple Certificate Enrollment Protocol
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDLM	Software Development Life-cycle Methodology
SDN	Software-defined Networking
SDP	Service Delivery Platform
SDV	Software-defined Visibility
SED	Self-Encrypting Drives
SEH	Structured Exception Handling
SFTP	SSH File Transfer Protocol
SHA	Secure Hashing Algorithm
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service-level Agreement
SLE	Single Loss Expectancy
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, Response
SoC	System on Chip
SOC	Security Operations Center
SPF	Sender Policy Framework
SPIM	Spam over Instant Messaging
SQL	Structured Query Language
SQLi	SQL Injection
SRTP	Secure Real-time Transport Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXpression
STP	Shielded Twisted Pair
SWG	Secure Web Gateway
TACACS+	Terminal Access Controller Access Control System
TAXII	Trusted Automated eXchange of Intelligence Information
TCP/IP	Transmission Control Protocol/Internet Protocol
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOTP	Time-based One Time Password
TPM	Trusted Platform Module
TSIG	Transaction Signature
TTP	Tactics, Techniques, and Procedures
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USB	Universal Serial Bus
USB OTG	USB On-The-Go
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VBA	Visual Basic for Applications
VDE	Virtual Desktop Environment
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VLSM	Variable-length Subnet Masking
VM	Virtual Machine
VoIP	Voice over IP
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAF	Web Application Firewall
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WORM	Write Once Read Many
WPA	WiFi Protected Access
WPS	WiFi Protected Setup
XaaS	Anything as a Service
XML	Extensible Markup Language
XOR	Exclusive OR
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting

CompTIA Security+ ハードウェアとソフトウェアの一覧

本リストは、CompTIA Security+の受験準備として役立てていただくためのハードウェアとソフトウェアのリストです。トレーニングを実施している企業でも、トレーニングの提供に必要な実習室コンポーネントを作成したい場合に役立ちます。各トピックに箇条書きで挙げられた項目は例であり、すべてを網羅するものではありません。

ハードウェア

- インターネットにアクセスできるラップトップ
- 別個のワイヤレスNIC
- WAP
- ファイアウォール
- UTM
- モバイルデバイス
- サーバー/クラウドサーバー
- IoTデバイス

ソフトウェア

- 仮想化ソフトウェア
- ペネトレーションテストOS/ディストリビューション (Kali Linux, Parrot OSなど)
- SIEM
- Wireshark
- Metasploit
- tcpdump

その他

- CSPへのアクセス