CompTIA Security+ 認定資格試験 出題範囲

試験番号：**SY0-501**

CompTIA

About the Exam

CompTIA Security+は、ベンダーニュートラルの認定資格です。Security+認定は、基本レベルのセキュリティスキルおよび知識を判断する、国際的に認められた認定試験で、世界中の企業およびセキュリティプロフェッショナルに活用されています。

CompTIA Security+認定資格試験に合格することで、アプリケーション、ネットワーク、デバイスのセキュリティを確保するために必要なシステムのインストールと設定、プラットフォームへの脅威を分析して適切な手法で緩和する対応、関連するポリシーや法規制を正しく認識した運用を行うために必要な知識とスキルを証明します。また、これらのタスクを、機密性、完全性、可用性の三大要件を維持し実行が可能なスキルを証明します。

CompTIA Security+認定資格試験は、以下の条件を満たすITセキュリティプロフェッショナルを対象としています。

・セキュリティに重点を置いたネットワーク管理における最低2年間の業務経験

・情報セキュリティのテクニカルな側面を日常的に扱う経験

・出題範囲に挙げられた項目を含む、セキュリティ上の問題や実装に関する幅広い知識

ここに掲載された例は出題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一覧ではありませんので、ご注意ください。

認定試験の認証

CompTIA Security+は、ISO 17024標準への準拠を米国国家規格協会（ANSI）より認定されており、定期的な出題範囲の見直しおよびアップデートを行っています。

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 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取得した認定資格を取り消され、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 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ます。個々の教材が不正教材（「ブレインダンプ」）扱いになるかどうかを確認するには、CompTIAの担当窓口（examsecurity@comptia.org）までお問い合わせください。

注意事項

箇条書きで例示された項目は、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ことがあります。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。必要な場合、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	CompTIA Security+ SY0-501
問題数	最大90問
出題形式	単一/複数選択、シミュレーション
試験時間	90分
推奨経験	セキュリティに重点を置いたIT管理における最低2年間の業務経験
合格ライン	750（100～900のスコア形式）

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 脅威、攻撃、脆弱性	21%
2.0 テクノロジーとツール	22%
3.0 アーキテクチャと設計	15%
4.0 アイデンティティとアクセス管理	16%
5.0 リスク管理	14%
6.0 暗号化とPKI	12%
合計	**100%**

1.0 脅威、攻撃、脆弱性

1.1 与えられたシナリオに基づいて、不正の痕跡を分析してマルウェアの種類を特定することができる。

- **ウイルス**
- **クリプトマルウェア**
- **ランサムウェア**
- **ワーム**
- **トロイの木馬**
- **ルートキット**
- **キーロガー**
- **アドウェア**
- **スパイウェア**
- **ボット**
- **リモートアクセスツール（RAT）**
- **ロジックボム**
- **バックドア**

1.2 さまざまな攻撃のタイプを比較対照することができる。

- **ソーシャルエンジニアリング**
  - フィッシング
  - スピアフィッシング
  - ホエーリング
  - ビッシング
  - テールゲート（共連れ）
  - 偽装
  - ゴミ箱あさり
  - ショルダーサーフィン
  - デマウイルス（Hoax）
  - 水飲み場型攻撃
  - 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（Familiality）
    - 信頼性（Trust）
    - 緊急性（Urgency）
- **アプリケーション/サービス攻撃**
  - DoS
  - DDoS
  - 中間者攻撃
  - バッファオーバーフロー
  - インジェクション
  - クロスサイトスクリプティング
  - クロスサイトリクエストフォージェリ
  - 特権エスカレーション
  - ARPポイズニング
  - アンプ攻撃
  - DNSポイズニング
  - ドメインハイジャッキング
  - MITB 攻撃（Man-in-the-Browser）
  - ゼロデイ攻撃
  - リプレイ攻撃
  - Pass-the-hash攻撃
  - ハイジャッキングおよび関連攻撃
    - クリックジャッキング
    - セッションハイジャッキング
    - URLハイジャッキング
    - タイポスクワッティング
  - ドライバ操作
    - シミング
    - リファクタリング
  - MACスプーフィング
  - IPスプーフィング
- **ワイヤレス攻撃**
  - リプレイ攻撃
  - IV攻撃
  - エビルツイン（Evil twin）
  - 不正なAP
  - ジャミング
  - WPS
  - ブルージャッキング
  - ブルースナーフィング
  - RFID
  - NFC
  - Disassociationフレーム
- **暗号攻撃**
  - 誕生日攻撃
  - 既知平文/暗号文攻撃
  - レインボーテーブル
  - 辞書攻撃
  - ブルートフォース攻撃
    - オンラインとオフラインの違い
  - 衝突攻撃
  - ダウングレード攻撃
  - リプレイ攻撃
  - 脆弱な設定への攻撃

1.3 脅威となる行為主体のタイプと属性について説明することができる。

- **行為主体のタイプ**
  - スクリプトキディ
  - ハクティビスト
  - 組織犯罪
  - 国家/APT
  - インサイダー
  - 競合相手
- **行為主体の属性**
  - 内部/外部
  - 巧妙さのレベル
  - リソース/資金
  - 意図/動機
- **オープンソースインテリジェンスの活用**

1.4 さまざまなペネトレーションテストのコンセプトについて説明することができる。

- **アクティブ偵察**
- **パッシブ偵察**
- **ピボット**
- **初期潜入**
- **持続性**
- **権限エスカレーション**
- **ブラックボックス**
- **ホワイトボックス**
- **グレーボックス**
- **ペネトレーションテストと脆弱性スキャンの違い**

1.5 脆弱性スキャンのコンセプトについて説明することができる。

- **セキュリティ管理のパッシブなテスト**
- **脆弱性の特定**
- **セキュリティ管理不備の特定**
- **一般的な設定ミスの特定**
- **侵入と非侵入の違い**
- **クレデンシャルとノンクレデンシャルの違い**
- **フォールス・ポジティブ**

1.6 脆弱性のタイプによる影響について説明することができる。

- **競合状態**
- **下記を原因とする脆弱性**
  - EOL（End of Life）システム
  - 組み込みシステム
  - ベンダーサポートの欠如
- **不適切なインプット処理**
- **不適切なエラー処理**
- **誤設定/弱い設定**
- **デフォルト設定**
- **リソースの枯渇**
- **ユーザートレーニングの欠如**
- **不適切なアカウント設定**
- **脆弱なビジネスプロセス**
- **弱い暗号スイートと実装**
- **メモリ/バッファの脆弱性**
  - メモリリーク
  - 整数オーバーフロー
  - バッファオーバーフロー
  - ポインタデリファレンス
  - DLLインジェクション
- **システムの無秩序な展開/文書化されていない資産**
- **アーキテクチャ/設計上の弱点**
- **新種の脅威/ゼロデイ攻撃**
- **証明書管理や鍵管理の不備**

2.0 テクノロジーとツール

2.1 組織のセキュリティを維持するために、ハードウェアおよびソフトウェアのネットワークコンポーネントをインストール・設定することができる。

- **ファイアウォール**
  - ACL
  - アプリケーションベースとネットワークベースの違い
  - ステートフルとステートレスの違い
  - 暗黙の拒否
- **VPNコンセントレーター**
  - リモートアクセスとサイトツーサイトの違い
  - IPSec
    - トンネルモード
    - トランスポートモード
    - AH
    - ESP
  - スプリットトンネルとフルトンネルの違い
  - TLS
  - 常時接続VPN
- **NIPS/NIDS**
  - 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
  - インバンドとアウトオブバンドの違い
  - ルール
  - アナリティクス
    - フォールス・ポジティブ
    - フォールス・ネガティブ
- **ルーター**
  - ACL
  - アンチスプーフィング
- **スイッチ**
  - ポートセキュリティ
  - レイヤー2とレイヤー3の違い
  - ループ防止
  - フラッドガード
- **プロキシ**
  - フォワードプロキシとリバースプロキシ
  - 透過性プロキシ
  - アプリケーション/多目的
- **ロードバランサー**
  - スケジューリング
    - アフィニティ
    - ラウンドロビン
  - アクティブ/パッシブ
  - アクティブ/アクティブ
  - 仮想IP
- **アクセスポイント**
  - SSID
  - MACフィルタリング
  - 信号強度
  - 帯域選択/幅
  - アンテナのタイプと配置
  - FatとThinの違い
  - コントローラーベースとスタンドアロンの違い
- **SIEM**
  - アグリゲーション
  - 相関分析
  - 自動アラートおよびトリガー
  - 時刻同期
  - イベントの重複排除
  - ログ/WORM（Write Once Read Many）
- **DLP**
  - USBブロッキング
  - クラウドベース
  - Eメール
- **NAC**
  - 一時利用と恒久利用の違い
  - ホストヘルスチェック
  - エージェント型とエージェントレス型の違い
- **メールゲートウェイ**
  - スパムフィルター
  - DLP
  - 暗号化
- **ブリッジ**
- **SSL/TLSアクセラレーター**
- **SSL復号装置**
- **メディアゲートウェイ**
- **ハードウェアセキュリティモジュール**

2.2 与えられたシナリオに基づいて、組織のセキュリティ対策に最適なソフトウェアツールを活用することができる。

- **プロトコルアナライザー**
- **ネットワークスキャナー**
  - 無許可（ローグ）システム検出
  - ネットワークマッピング
- **ワイヤレススキャナー/クラッカー**
- **パスワードクラッカー**
- **脆弱性スキャナー**
- **構成コンプライアンススキャナー**
- **エクスプロイトフレームワーク**
- **データサニテーションツール**
- **ステガノグラフィツール**
- **ハニーポット**
- **バックアップユーティリティ**
- **バナーグラビング**
- **パッシブとアクティブの違い**
- **コマンドラインツール**
  - ping
  - netstat
  - tracert
  - nslookup/dig
  - arp
  - ipconfig/ip/ifconfig
  - tcpdump
  - nmap
  - netcat

2.3 与えられたシナリオに基づいて、一般的なセキュリティ問題のトラブルシューティングを実施することができる。

- **暗号化されていないクレデンシャル/平文**
- **ログおよびイベントのアノマリー**
- **承認の問題**
- **アクセス違反**
- **証明書の問題**
- **データ流出**
- **デバイスの誤設定**
  - ファイアウォール
  - コンテンツフィルター
  - アクセスポイント
- **弱いセキュリティ設定**
- **人員の問題**
  - ポリシー違反
  - インサイダーの脅威
  - ソーシャルエンジニアリング
  - ソーシャルメディア
  - 個人的なEメール
- **承認外のソフトウェア**
- **ベースライン違反**
- **ライセンスのコンプライアンス違反（許諾範囲以外の使用/改変）**
- **資産管理**
- **認証の問題**

2.4 与えられたシナリオに基づいて、セキュリティテクノロジーのアウトプットを分析・解釈することができる。

- **HIDS/HIPS**
- **アンチウイルス**
- **ファイル完全性チェック**
- **ホストベースのファイアウォール**
- **アプリケーションホワイトリスト**
- **リムーバブルメディア管理**
- **高度なマルウェアツール**
- **パッチ管理ツール**
- **UTM**
- **DLP**
- **データ実行防止**
- **Webアプリケーションファイアウォール**

2.5 与えられたシナリオに基づいて、モバイルデバイスを安全に導入することができる。

- **接続方法**
  - 携帯電話
  - Wi-Fi
  - SATCOM
  - Bluetooth
  - NFC
  - ANT
  - 赤外線
  - USB
- **モバイルデバイス管理のコンセプト**
  - 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
  - プッシュ通知サービス
  - パスワード/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
- **規制と監視**
  - サードパーティのアプリストア
  - root化/Jailbreaking
  - 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
  - ファームウェアのOTA更新
  - カメラの使用
  - SMS/MMS
  - 外付けメディア
  - 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
  - 決済方法
- **導入モデル**
  - BYOD
  - COPE
  - CYOD
  - 会社所有
  - VDI

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

- **プロトコル**
  - DNSSEC
  - SSH
  - S/MIME
  - SRTP
  - LDAPS
  - FTPS
  - SFTP
  - SNMPv3
  - SSL/TLS
  - HTTPS
  - Secure POP/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

3.0 アーキテクチャと設計

3.1 フレームワーク、ベストプラクティス、セキュア構成ガイドの適用例と目的について説明することができる。

- **業界標準フレームワークとリファレンスアーキテクチャ**
  - 規制
  - 規制外
  - 国内と国際的規制の違い
  - 業種固有のフレームワーク
- **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
    - オペレーティングシステム
    - アプリケーションサーバー
    - ネットワークインフラ機器
  - 汎用ガイド
- **多層防御/レイヤードセキュリティ**
  - ベンダーの多様化
  - 管理の多様化
    - 管理的側面
    - 技術的側面
  - ユーザートレーニング

3.2 与えられたシナリオに基づいて、セキュアネットワークアーキテクチャのコンセプトを導入することができる。

- **ゾーン/トポロジー**
  - DMZ
  - エクストラネット
  - イントラネット
  - ワイヤレス
  - ゲスト
  - ハニーネット
  - NAT
  - アドホック
- **セグリゲーション/セグメンテーション/アイソレーション**
  - 物理的
  - 論理的（VLAN）
  - 仮想化
  - エアギャップ
- **トンネリング/VPN**
  - サイトツーサイト
  - リモートアクセス
- **セキュリティデバイス/テクノロジーの配置**
  - センサー
  - コレクター
  - 相関分析エンジン
  - フィルター
  - プロキシ
  - ファイアウォール
  - VPNコンセントレーター
  - SSLアクセラレーター
  - ロードバランサー
  - DDoSミティゲーター
  - アグリゲーションスイッチ
  - TAPおよびポートミラー
- **SDN**

3.3 与えられたシナリオに基づいて、セキュアなシステムデザインを導入することができる。

- **ハードウェア/ファームウェアのセキュリティ**
  - FDE/SED
  - TPM
  - HSM
  - UEFI/BIOS
  - セキュアブートと検証
  - サプライチェーン
  - 信頼の基点（root of trust）となるハードウェア
  - EMI/EMP
- **オペレーティングシステム**
  - タイプ
  - ネットワーク
  - サーバー
  - ワークステーション
  - アプライアンス
  - Kiosk
  - モバイルOS
  - パッチ管理
  - 不要なポートやサービスの無効化
  - 最少機能
  - セキュアコンフィギュレーション
  - トラステッドオペレーティングシステム
  - アプリケーションホワイトリスト/ブラックリスト
  - デフォルトのアカウント/パスワードの無効化
- **周辺装置**
  - ワイヤレスキーボード
  - ワイヤレスマウス
  - ディスプレイ
  - WiFi機能つきmicroSDカード
  - プリンター/MFD
  - 外付けストレージデバイス
  - デジタルカメラ

3.4 セキュアなステージングデプロイメントのコンセプトの重要性を説明することができる。

- **サンドボックス**
- **環境**
  - 開発
  - テスト
  - ステージング
  - プロダクション
- **セキュアベースライン**
- **完全性測定**

3.5 組み込み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。

- **SCADA/ICS**
- **スマートデバイス/IoT**
  - ウェアラブルテクノロジー
  - ホームオートメーション
- **HVAC**
- **SoC**
- **RTOS**
- **プリンター/MFD**
- **カメラシステム**
- **特殊な用途**
  - 医療用デバイス
  - 車両
  - 航空機/無人機

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

- **開発ライフサイクルモデル**
  - ウォーターフォール型とアジャイル型の違い
- **セキュアなDevOps**
  - セキュリティオートメーション
  - 継続的インテグレーション
  - ベースライン
  - イミュータブルシステム
  - Infrastructure as code
- **バージョン管理、変更管理**
- **プロビジョニング、デプロビジョニング**
- **セキュアコーディングテクニック**
  - 適切なエラー処理
  - 適切な入力検証
  - 正規化
  - ストアードプロシージャ
  - コード署名
  - 暗号化
  - 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SDKの利用
  - データ露出
- **コードの品質とテスト**
  - スタティックコードアナライザー
  - 動的分析（例：ファジング）
  - 負荷テスト
  - サンドボックス
  - モデル検証
- **コンパイルドコードとランタイムコードの違い**

3.7 クラウドと仮想化に関するコンセプトを要約することができる

- **ハイパーバイザー**
  - Type I
  - Type II
  - アプリケーションセル/アプリケーションコンテナ
- **VMスプロールの防止**
- **VMエスケープへの対策**
- **クラウドストレージ**
- **クラウド開発モデル**
  - SaaS
  - PaaS
  - IaaS
  - プライベート
  - パブリック
  - ハイブリッド
  - コミュニティ
- **オンプレミス、ホステッド、クラウドの違い**
- **VDI/VDE**
- **クラウドアクセスセキュリティブローカー（CASB）**
- **Security as a Service**

3.8 レジリエンスと自動化によってリスクを低減する戦略について説明することができる。

- **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
  - 設定の検証
- **テンプレート**
- **マスターイメージ**
- **非持続性（ノンパーシスタンス）**
  - スナップショット
  - 既知の状態に復帰
  - 既知の設定にロールバック
  - Live bootメディア
- **エラスティシティ（弾性）**
- **スケーラビリティ**
- **分散配分**
- **リダンダンシー**
- **フォールトトレラレンス**
- **高可用性**
- **RAID**

3.9 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。

- **照明**
- **表示**
- **フェンス/ゲート/ケージ**
- **保安要員**
- **アラーム**
- **金庫**
- **セキュアキャビネット/エンクロージャ**
- **保護された配電装置/保護されたケーブル**
- **エアギャップ**
- **マントラップ**
- **ファラデーケージ**
- **ロックの種類**
- **生体認証**
- **バリケード/ボラード**
- **トークン/カード**
- **環境管理**
  - HVAC
  - ホットアイル、コールドアイル
  - 消火
- **ワイヤーロック**
- **画面フィルター**
- **カメラ**
- **モーション検知**
- **ログ**
- **赤外線検知**
- **鍵管理**

4.0 アイデンティティとアクセス管理

4.1 アイデンティティとアクセス管理のさまざまなコンセプトを比較対照することができる。

- **識別、認証・認可・アカウンティング（AAA）**
- **多要素認証**
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- **フェデレーション**
- **シングルサインオン**
- **推移する信頼関係**

4.2 与えられたシナリオに基づいて、アイデンティティ管理サービスのインストールと設定ができる。

- **LDAP**
- **Kerberos**
- **TACACS+**
- **CHAP**
- **PAP**
- **MSCHAP**
- **RADIUS**
- **SAML**
- **OpenID Connect**
- **OAUTH**
- **Shibboleth**
- **Secure Token**
- **NTLM**

4.3 与えられたシナリオに基づいて、認証管理とアクセス管理のコントロールを実装することができる。

- **アクセス制御モデル**
  - **MAC**
  - **DAC**
  - **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
- **物理的アクセス制御**
  - 近接型（非接触）カード
  - **ICカード**
- **バイオメトリクス対応**
  - 指紋スキャナー
  - 網膜スキャナー
  - 虹彩スキャナー
  - 音声認識
  - 顔認識
  - 他人受入率
  - 本人拒否率
  - クロスオーバーエラー率
- **トークン**
  - ハードウェア
  - ソフトウェア
  - **HOTP/TOTP**
- **コンテキストベース認証**
  - **PIV/CAC/ICカード**
  - **IEEE 802.1x**
- **ファイルシステムのセキュリティ**
- **データベースのセキュリティ**

4.4 与えられたシナリオに基づいて、一般的なアカウント管理手法の差異を明らかにすることができる。

- **アカウントの種類**
  - ユーザーアカウント
  - 共有/包括的なアカウント/資格情報
  - ゲストアカウント
  - サービスアカウント
  - 特権アカウント
- **一般的なコンセプト**
  - 最小権限
  - オンボーディング/オフボーディング
  - 承認状況の監査および評価
  - 利用状況の監査および評価
  - 時間帯制限
  - 再認証
  - 標準命名規則
  - アカウントメンテナンス
  - グループベースアクセス制御
  - ロケーションベースのポリシー
- **アカウントポリシーの執行**
  - クレデンシャルマネジメント
  - グループポリシー
  - パスワードの複雑さ
  - 有効期限
  - 復旧
  - 無効化
  - ロックアウト
  - パスワード履歴
  - パスワード再利用
  - パスワード文字数

5.0 リスク管理

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

- **標準業務手順書**
- **合意書のタイプ**
  - BPA
  - SLA
  - ISA
  - MOU/MOA
- **人事管理**
  - 強制的な休暇
  - ジョブローテーション
  - 職務分離
  - クリーンデスク
  - バックグラウンドチェック
  - 退職者面接
  - ロールベースの意識向上トレーニング
    - データオーナー
    - システム管理者
    - システムオーナー
    - ユーザー
    - 特権ユーザー
    - エグゼクティブユーザー
  - NDA
  - オンボーディング
  - 継続教育
  - アクセプタブルユースポリシー/行動ルール
  - 有害な行動
- **一般セキュリティポリシー**
  - ソーシャルメディアネットワーク/アプリケーション
  - 個人的なEメール

5.2 ビジネスインパクト分析に関するコンセプトを要約することができる。

- **RTO/RPO**
- **MTBF**
- **MTTR**
- **ミッションエッセンシャル機能**
- **クリティカルなシステムの特定**
- **単一障害点**
- **インパクト**
  - 人命
  - 資産
  - 安全
  - 財務
  - 評判
- **プライバシー影響評価**
- **プライバシー閾値評価**

5.3 リスク管理のプロセスとコンセプトについて説明することができる。

- **脅威アセスメント**
  - 環境的なもの
  - 人為的なもの
  - 内部と外部の違い
- **リスクアセスメント**
  - SLE
  - ALE
  - ARO
  - 資産価値
  - リスク登録簿
  - 発生可能性
  - サプライチェーンアセスメント
  - インパクト
  - 定量的
  - 定性的
  - テスト
    - ペネトレーションテスト承認
    - 脆弱性テスト承認
  - リスク対応の手法
    - 受容
    - 移転
    - 回避
    - 低減
- **変更管理**

5.4 与えられたシナリオに基づいて、インシデント対応の手順を実行することができる。

- **インシデント対応計画**
  - 文書化されたインシデントの種類/カテゴリーの定義
  - 役割と責任
  - 報告義務/エスカレーション
  - サイバーインシデント対応チーム
  - 演習
- **インシデント対応プロセス**
  - 準備
  - 識別
  - 封じ込め
  - 根絶
  - 復旧
  - 教訓の管理

5.5 フォレンジックの基本的なコンセプトを要約することができる。

- **揮発性の順序（Order of volatility）**
- **証拠の連鎖（Chain of custody）**
- **訴訟ホールド**
- **データ取得**
  - システムイメージのキャプチャ
  - ネットワークトラフィックおよびログ
  - 動画のキャプチャ
  - タイムオフセットの記録
  - ハッシュの取得
  - スクリーンショット
  - 証人への聴取
- **保全**
- **復旧**
- **インテリジェンス/カウンターインテリジェンスの戦略的収集**
  - アクティブログ
- **工数の記録**

5.6 災害復旧と事業継続のコンセプトについて説明することができる。

- **リカバリサイト**
  - ホットサイト
  - ウォームサイト
  - コールドサイト
- **復旧の順序**
- **バックアップのコンセプト**
  - 差分
  - 増分
  - スナップショット
  - フル
- **地理的な検討項目**
  - オフサイトバックアップ
  - 距離
  - ロケーション選定
  - 法的な影響
  - データの主権性
- **事業継続計画の策定**
  - 演習/机上演習
  - 対応報告
  - フェールオーバー
  - 代替処理サイト
  - 代替業務手順

5.7 さまざまな管理タイプを比較対照することができる。

- **抑止**
- **予防**
- **検知**
- **補正**
- **補完**
- **技術**
- **運用管理**
- **物理**

5.8 与えられたシナリオに基づいて、データのセキュリティとプライバシーを守る手順を実行することができる。

- **データの破壊とメディアの消去**
  - 焼却
  - シュレッディング
  - 溶解
  - 粉砕
  - 消磁
  - パージング
  - ワイプ
- **データの機密度表示と取り扱い**
  - コンフィデンシャル
  - プライベート
  - パブリック
  - プロプライエタリ
  - 個人情報（PII）
  - 医療情報（PHI）
- **データに関する役割**
  - オーナー
  - Steward
  - プライバシーオフィサー
- **データ保全**
- **法規とコンプライアンス**

6.0 暗号化とPKI

6.1 暗号化の基本的なコンセプトを比較対照することができる。

- **対称アルゴリズム**
- **利用モード**
- **非対称アルゴリズム**
- **ハッシュ化**
- **ソルト、IV、ノンス**
- **楕円曲線**
- **弱い/非推奨のアルゴリズム**
- **鍵交換**
- **デジタル署名**
- **拡散**
- **撹乱**
- **衝突**
- **ステガノグラフィ**
- **難読化**
- **ストリームとブロックの違い**
- **鍵強度**
- **セッション鍵**
- **一時的な鍵**
- **秘密アルゴリズム**
- **データ伝送時（Data-in-transit）**
- **データ格納時（Data-at-rest）**
- **データ使用時（Data-in-use）**
- **乱数/擬似乱数の生成**
- **鍵ストレッチング**
- **実装とアルゴリズム選択**
  - 暗号サービスプロバイダー
  - 暗号モジュール
- **PFS（Perfect forward secrecy）**
- **隠蔽によるセキュリティ（Security through obscurity）**
- **一般的な適用例**
  - ローパワーデバイス
  - 低レイテンシー
  - 高レジリエンス
  - 機密保持への対応
  - 完全性保護への対応
  - 難読化への対応
  - 認証への対応
  - 否認防止への対応
  - リソース上の制約とセキュリティ上の制約

6.2 各種の暗号アルゴリズムとそれぞれの基本的な特徴について説明することができる。

- **対称アルゴリズム**
  - AES
  - DES
  - 3DES
  - RC4
  - Blowfish/Twofish
- **暗号利用モード**
  - CBC
  - GCM
  - ECB
  - CTR
  - ストリームとブロック
- **非対称アルゴリズム**
  - RSA
  - DSA
  - ディフィー・ヘルマン
    - グループ
    - DHE
    - ECDHE
  - 楕円曲線
  - PGP/GPG
- **ハッシングアルゴリズム**
  - MD5
  - SHA
  - HMAC
  - RIPEMD
- **鍵ストレッチングアルゴリズム**
  - BCRYPT
  - PBKDF2
- **難読化**
  - XOR
  - ROT13
  - 換字式暗号

6.3 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、実装することができる。

- **暗号化プロトコル**
  - WPA
  - WPA2
  - CCMP
  - TKIP
- **認証プロトコル**
  - EAP
  - PEAP
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1x
  - RADIUS Federation
- **方式**
  - PSK、エンタープライズ、オープンの違い
  - WPS
  - キャプティブポータル

6.4 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。

- **コンポーネント**
  - CA
  - 中間CA
  - CRL
  - OCSP
  - CSR
  - 証明書
  - 公開鍵
  - 秘密鍵
  - オブジェクト識別子（OID）
- **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
- **証明書の種類**
  - ワイルドカード
  - SAN
  - 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（Extended validation）証明書
- **証明書の形式**
  - DER
  - PEM
  - PFX
  - CER
  - P12
  - P7B

CompTIA Security+ 略語一覧

下記はCompTIA Security+認定資格試験で使用される略語の一覧です。受験者には、試験準備の一環として、これら用語を復習し、理解することをお勧めします。

略語	展開形
3DES	Triple Digital Encryption Standard
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-based Access Control
ACL	Access Control List
AES	Advanced Encryption Standard
AES256	Advanced Encryption Standards 256bit
AH	Authentication Header
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	Application Service Provider
AUP	Acceptable Use Policy
AV	Antivirus
AV	Asset Value
BAC	Business Availability Center
BCP	Business Continuity Planning
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partners Agreement
BPDU	Bridge Protocol Data Unit
BYOD	Bring Your Own Device
CA	Certificate Authority
CAC	Common Access Card
CAN	Controller Area Network
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAR	Corrective Action Report
CBC	Cipher Block Chaining
CCMP	Counter-Mode/CBC-Mac Protocol
CCTV	Closed-circuit Television
CER	Certificate

略語	展開形
CER	Cross-over Error Rate
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge Handshake Authentication Protocol
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CMS	Content Management System
COOP	Continuity of Operations Plan
COPE	Corporate Owned, Personally Enabled
CP	Contingency Planning
CRC	Cyclical Redundancy Check
CRL	Certificate Revocation List
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
CTR	Counter
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DBA	Database Administrator
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DER	Distinguished Encoding Rules
DES	Digital Encryption Standard
DFIR	Digital Forensics and Investigation Response
DHCP	Dynamic Host Configuration Protocol
DHE	Data-Handling Electronics
DHE	Diffie-Hellman Ephemeral
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DMZ	Demilitarized Zone

DNAT	Destination Network Address Transaction
DNS	Domain Name Service (Server)
DoS	Denial of Service
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
DSU	Data Service Unit
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EFS	Encrypted File System
EMI	Electromagnetic Interference
EMP	Electro Magnetic Pulse
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulated Security Payload
EF	Exposure Factor
FACL	File System Access Control List
FAR	False Acceptance Rate
FDE	Full Disk Encryption
FRR	False Rejection Rate
FTP	File Transfer Protocol
FTPS	Secured File Transfer Protocol
GCM	Galois Counter Mode
GPG	Gnu Privacy Guard
GPO	Group Policy Object
GPS	Global Positioning System
GPU	Graphic 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	Hashed Message Authentication Code
HOTP	HMAC-based One-Time Password
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL/TLS
HVAC	Heating, Ventilation and Air Conditioning
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
ID	Identification
IDEA	International Data Encryption Algorithm
IDF	Intermediate Distribution Frame
IdP	Identity Provider
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IIS	Internet Information System
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP4	Internet Message Access Protocol v4
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Incident Response
IR	Infrared
IRC	Internet Relay Chat
IRP	Incident Response Plan
ISA	Interconnection Security Agreement
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	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDF	Main Distribution Frame
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MFD	Multi-function Device
MITM	Man-in-the-Middle
MMS	Multimedia Message Service
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multi-protocol Label Switching
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSP	Managed Service Provider

略語	展開形
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Recover or Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near Field Communication
NGAC	Next Generation Access Control
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OAUTH	Open Authorization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OTA	Over The Air
OVAL	Open Vulnerability Assessment Language
P12	PKCS #12
P2P	Peer to Peer
PaaS	Platform as a Service
PAC	Proxy Auto Configuration
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
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PEM	Privacy-enhanced Electronic Mail
PFS	Perfect Forward Secrecy
PFX	Personal Exchange Format
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POODLE	Padding Oracle on Downgrade Legacy Encryption
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol

略語	展開形
PSK	Pre-shared Key
PTZ	Pan-Tilt-Zoom
RA	Recovery Agent
RA	Registration Authority
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RAT	Remote Access Trojan
RBAC	Role-based Access Control
RBAC	Rule-based Access Control
RC4	Rivest Cipher version 4
RDP	Remote Desktop Protocol
RFID	Radio Frequency Identifier
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RMF	Risk Management Framework
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
SAML	Security Assertions Markup Language
SAN	Storage Area Network
SAN	Subject Alternative Name
SCADA	System Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy
SCSI	Small Computer System Interface
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDLM	Software Development Life Cycle Methodology
SDN	Software Defined Network
SED	Self-encrypting Drive
SEH	Structured Exception Handler
SFTP	Secured File Transfer Protocol
SHA	Secure Hashing Algorithm
SHTTP	Secure Hypertext Transfer Protocol
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SLA	Service Level Agreement

略語	展開形
SLE	Single Loss Expectancy
SMB	Server Message Block
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
SoC	System on Chip
SPF	Sender Policy Framework
SPIM	Spam over Internet Messaging
SPoF	Single Point of Failure
SQL	Structured Query Language
SRTP	Secure Real-Time Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STP	Shielded Twisted Pair
TACACS+	Terminal Access Controller Access Control System Plus
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
UAT	User Acceptance Testing
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UPS	Uninterruptable 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
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
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	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup
WTLS	Wireless TLS
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。

機材
- ルーター
- ファイアウォール
- アクセスポイント
- スイッチ
- IDS/IPS
- サーバー
- コンテンツフィルター
- クライアント
- モバイルデバイス
- VPNコンセントレーター
- UTM
- エンタープライズセキュリティマネージャー/SIEMスイート
- ロードバランサー
- プロキシ
- DLPアプライアンス
- ICSまたは類似のシステム
- ネットワークアクセスコントロールサーバー
- DDoS対策ハードウェア

予備のパーツ/ハードウェア
- キーボード
- マウス
- ネットワークケーブル
- モニター
- ワイヤレスドングル、Bluetoothドングル

ハードウェアツール
- WiFiアナライザー
- ハードウェアのデバッグ機能

ソフトウェアツール
- 脆弱性診断用ディストリビューション（例：Kali Linux）
- プロキシサーバー
- 仮想化ソフトウェア
- 仮想化アプライアンス
- Wireshark
- tcpdump
- NMAP
- OpenVAS
- Metasploit/Metasploitable2
- Back Orifice
- Cain & Abel
- John the Ripper
- pfSense
- Security Onion
- Roo
- 任意のUTM

その他
- SourceForge