CompTIA Security+ 認定資格試験 出題範囲

試験番号：SY0-701

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。
- クラウド、モバイル、IoT などのハイブリッド環境を監視および保護する。
- ガバナンス、リスク、コンプライアンスの原則など、該当する規制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特定、分析、対応を実施する。

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、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」）とは提携関係になく、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（通称「ブレインダンプ」）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されていない場合でも、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

試験番号	SY0-701
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
推奨される経験	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、技術的情報セキュリティの実務経験、およびセキュリティコンセプトに関する幅広い知識

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	セキュリティコンセプトの概要	12%
2.0	脅威、脆弱性、軽減策	22%
3.0	セキュリティアーキテクチャ	18%
4.0	セキュリティオペレーション	28%
5.0	セキュリティプログラムの管理と監督	20%
計		**100%**

1.0 セキュリティコンセプトの概要

1.1 さまざまなタイプのセキュリティコントロールを比較対照することができる。

- **カテゴリ**
  - 技術的
  - 管理的
  - 運用的
  - 物理的
- **コントロールの種類**
  - 予防的
  - 抑止的
  - 検出的
  - 是正的
  - 補正的
  - 指揮的

1.2 基本的なセキュリティコンセプトを要約することができる。

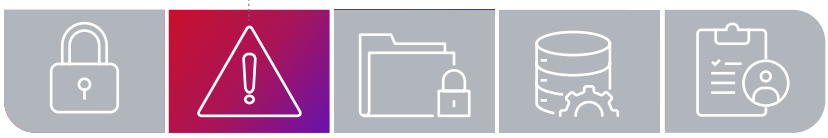
- **機密性、完全性、可用性（CIA）**
- **否認防止**
- **認証、認可、アカウンティング（AAA）**
  - 人の認証
  - システムの認証
  - 認証モデル
- **ギャップ分析**
- **ゼロトラスト**
  - コントロールプレーン
    - アダプティブ ID
    - 脅威スコープの縮小
    - ポリシー型のアクセスコントロール
    - ポリシー管理者
    - ポリシーエンジン
  - データプレーン
    - 暗黙のトラストゾーン
    - サブジェクト / システム
    - ポリシー施行点
- **物理的セキュリティ**
  - 侵入防止ゲート
  - アクセスコントロールが実施された玄関ホール
  - フェンス
  - ビデオによる監視
  - 保安要員
  - 入館証
  - 照明
  - センサー
    - 赤外線
    - 圧力
    - マイクロ波
    - 超音波
- **欺瞞と混乱のテクノロジー**
  - ハニーポット
  - ハニーネット
  - ハニーファイル
  - ハニートークン

1.3 変更管理プロセスの重要性とセキュリティへの影響を説明することができる。

- **セキュリティオペレーションに影響を及ぼすビジネスプロセス**
  - 承認プロセス
  - オーナーシップ
  - ステークホルダー
  - 影響分析
  - テスト結果
  - バックアウト計画
  - メンテナンス期間
  - 標準作業書
- **技術関連事項**
  - 許可リスト / 拒否リスト
  - 制限されているアクティビティ
  - ダウンタイム
  - サービスの再起動
  - アプリケーションの再起動
  - レガシーアプリケーション
  - 依存関係
- **文書化**
  - ダイアグラムの更新
  - ポリシー / 手順の更新
- **バージョン管理**

1.4 適切な暗号化ソリューションを用いる重要性を説明することができる。

- **公開鍵インフラストラクチャー（PKI）**
  - 公開鍵
  - 秘密鍵
  - キーエスクロー
- **暗号化**
  - レベル
    - フルディスク
    - パーティション
    - ファイル
    - ボリューム
    - データベース
    - レコード
  - トランスポート / コミュニケーション
  - 非対称
  - 対称
  - 鍵交換
  - アルゴリズム
  - 鍵の長さ
- **ツール**
  - Trusted Platform Module（TPM）
  - Hardware Security Module（HSM）
  - 鍵管理システム
  - セキュアなエンクレーブ
- **難読化**
  - o ステガノグラフィ
  - o トークン化
  - o データマスキング
- **ハッシュ化**
- **ソルトの使用**
- **デジタル署名**
- **鍵ストレッチング**
- **ブロックチェーン**
- **公開台帳**
- **証明書**
  - 認証局
  - 証明書失効リスト（CRL）
  - Online Certificate Status Protocol（OCSP）
  - 自己署名
  - サードパーティー
  - Root of Trust
  - 証明書署名要求（CSR）生成
  - ワイルドカード



2.0 脅威、脆弱性、軽減策

2.1 一般的な脅威アクターと誘因を説明することができる。

- **脅威アクター**
  - 国民・国家（Nation-state）
  - 未熟な攻撃者
  - ハクティビスト
  - 内部脅威
  - 組織的犯罪
  - シャドー IT
- **行為主体の属性**
  - 内部 / 外部
  - リソース / 資金
  - 巧妙さ / 能力のレベル
- **誘因**
  - データ流出
  - スパイ行為
  - サービス妨害
  - 脅迫
  - 経済的利益
  - 思想 / 政治的信念
  - 倫理
  - 復讐
  - 混乱 / カオス
  - 戦争

2.2 一般的な脅威ベクターと攻撃対象領域を説明することができる。

- **メッセージベース**
  - o E メール
  - o ショートメッセージサービス（SMS）
  - o インスタントメッセージ（IM）
- **画像ベース**
- **ファイルベース**
- **音声通話**
- **取り外し可能デバイス**
- **脆弱なソフトウェア**
  - o クライアントベースとエージェントレス
- **サポートされていないシステムとアプリケーション**
- **セキュアでないネットワーク**
  - ワイヤレス
  - 有線
  - Bluetooth
- **オープンサービスポート**
- **デフォルト認証情報**
- **サプライチェーン**
  - マネージドサービスプロバイダー（MSP）
  - ベンダー
  - サプライヤー
- **ヒューマンハッキング / ソーシャルエンジニアリング**
  - フィッシング
  - ビッシング
  - スミッシング
  - ミスインフォメーション / ディスインフォメーション
  - なりすまし
  - ビジネスメール詐欺（BEC）
  - プリテキスティング /Pretexting
  - 水飲み場
  - ブランド偽装
  - タイポスクワッティング

2.3 様々な種類の脆弱性を説明することができる。

- **アプリケーション**
  - メモリインジェクション
  - バッファオーバーフロー
  - 競合状態
    - Time-of-Check（TOC）
    - Time-of-Use（TOU）
  - 悪意ある更新
- **オペレーティングシステム（OS）ベース**
- **Web ベース**
  - SQL インジェクション（SQLi）
  - クロスサイトスクリプティング（XSS）
- **ハードウェア**
  - ファームウェア
  - End of Life
  - レガシー
- **仮想化**
  - 仮想マシン（VM）エスケープ
  - リソースの再利用
- **クラウド固有**
- **サプライチェーン**
  - サービスプロバイダー
  - ハードウェアプロバイダー
  - ソフトウェアプロバイダー
- **暗号化**
- **設定ミス**
- **モバイルデバイス**
  - サイドローディング
  - ジェイルブレイク
- **ゼロデイ**

2.4 与えられたシナリオに基づいて、悪意あるアクティビティの指標を分析することができる。

- **マルウェア攻撃**
  - ランサムウェア
  - トロイの木馬
  - ワーム
  - スパイウェア
  - ブロートウェア
  - ウイルス
  - キーロガー
  - ロジックボム
  - ルートキット
- **物理攻撃**
  - ブルートフォース攻撃
  - 無線 IC タグ（RFID）クローニング
  - 環境的
- **ネットワーク攻撃**
  - 分散型サービス拒否（DDoS）攻撃
    - アンプ / 増幅
    - リフレクション / 反射
  - ドメイン名システム（DNS）攻撃
  - ワイヤレス
  - オンパス
  - 認証情報リプレイ
  - 悪意あるコード
- **アプリケーション攻撃**
  - インジェクション
  - バッファオーバーフロー
  - リプレイ攻撃
  - 特権エスカレーション
  - フォージェリ攻撃
  - ディレクトリトラバーサル
- **暗号攻撃**
  - ダウングレード攻撃
  - 衝突攻撃
  - 誕生日攻撃
- **パスワード攻撃**
  - スプレー攻撃
  - ブルートフォース攻撃
- **指標**
  - アカウントのロックアウト
  - セッションの同時使用
  - コンテンツのブロック
  - あり得ない移動
  - リソース消費
  - リソースへのアクセス不可
  - サイクルから外れたログ記録
  - 公開 / 文書化
  - 行方不明のログ

2.5 企業の保護に用いられる軽減手法の目的を説明することができる。

- **セグメンテーション**
- **アクセスコントロール**
  - アクセスコントロールリスト（ACL）
  - 許可
- **アプリケーション許可リスト**
- **隔離**
- **パッチ適用**
- **暗号化**
- **モニタリング**
- **最小権限**
- **構成の実施**
- **廃止**
- **ハードニング手法**
  - 暗号化
  - エンドポイント保護の設置
  - ホスト型ファイアウォール
  - ホスト型侵入防止システム（HIPS）
  - ポート / プロトコルの無効化
  - デフォルトパスワードの変更
  - 不要なソフトウェアのアンインストール

3.0 セキュリティアーキテクチャ

3.1 様々なアーキテクチャモデルのセキュリティ関連事項を比較対照することができる。

- **アーキテクチャとインフラストラクチャのコンセプト**
  - クラウド
    - 責任マトリックス
    - ハイブリッドな考慮事項
    - サードパーティーベンター
  - Infrastructure as code（IaC）
  - サーバーレス
  - マイクロサービス
  - ネットワークインフラストラクチャ
    - 物理的隔離
      - エアギャップ
    - 論理セグメンテーション
    - ソフトウェア定義ネットワーク（SDN）
  - オンプレミス
  - 一元化と非一元化
  - コンテナ化
  - 仮想化
  - IoT
  - 産業用制御システム（ICS）/ Supervisory Control And Data Acquisition（SCADA）
  - リアルタイムオペレーティングシステム（RTOS）
  - 組み込みシステム
  - 高可用性
- **検討事項**
  - 可用性
  - レジリエンス
  - 費用
  - 応答性
  - スケーラビリティ
  - 展開の容易さ
  - リスク移転
  - 復旧の容易さ
  - 利用可能なパッチの適用
  - パッチ適用不可
  - 電源
  - コンピュート

3.2 与えられたシナリオに基づいて、セキュリティ原則を適用し、企業インフラストラクチャを保護することができる。

- **インフラストラクチャの検討事項**
  - デバイスの配置
  - セキュリティゾーン
  - 攻撃可能領域
  - 接続性
  - 故障モード
    - フェイルオープン
    - フェイルクローズ
  - デバイス属性
    - アクティブとパッシブ
    - インラインとタップ / モニター
  - ネットワークアプライアンス
    - ジャンプサーバー
    - プロキシサーバー
    - 侵入防止システム（IPS）/ 侵入検知システム（IDS）
    - ロードバランサー
    - センサー
  - ポートセキュリティ
    - 802.1X
    - 拡張認証プロトコル（EAP）
  - ファイアウォールのタイプ
    - Web アプリケーションファイアウォール（WAF）
    - 統合脅威管理（UTM）
    - 次世代ファイアウォール（NGFW）
    - レイヤー 4/ レイヤー 7
- **セキュアなコミュニケーション / アクセス**
  - 仮想プライベートネットワーク（VPN）
  - リモートアクセス
  - トンネリング
    - トランスポートレイヤーセキュリティ（TLS）
    - インターネットプロトコルセキュリティ（IPSec）
  - ソフトウェア定義ワイドエリアネットワーク（SD-WAN）
  - Secure Access Secure Edge（SASE）
- **効果的なコントロールの選択**

3.3 データ保護のコンセプトと戦略を比較対照することができる。

- **データの種類**
  - 規制対象
  - 企業秘密
  - 知的財産
  - 法務情報
  - 財務情報
  - 可読 / 不可読
- **データ分類**
  - 機微
  - 機密
  - パブリック
  - 部外秘
  - プライベート
  - 重要
- **データに関する一般的な検討事項**
  - データの状態
    - 保存中のデータ
    - 転送中のデータ
    - 使用中のデータ
  - データ主権
  - ジオロケーション
- **データ保護の方法**
  - 地理的制限
  - 暗号化
  - ハッシュ化
  - マスキング
  - トークナイゼーション
  - 難読化
  - セグメンテーション
  - 許可の制限

3.4 セキュリティアーキテクチャにおけるレジリエンスと復旧の重要性を説明することができる。

- **高可用性**
  - ロードバランシングとクラスタリング
- **サイトに関する検討事項**
  - ホット
  - コールド
  - ウォーム
  - 地理的分散
- **プラットフォームの多様化**
- **マルチクラウドシステム**
- **オペレーションの継続**
- **キャパシティプランニング**
  - 人
  - テクノロジー
  - インフラストラクチャ
- **テスト**
  - 机上演習
  - フェイルオーバー
  - シミュレーション
  - 並列処理
- **バックアップ**
  - オンサイト/オフサイト
  - 頻度
  - 暗号化
  - スナップショット
  - 復旧
  - レプリケーション
  - ジャーナリング
- **電源**
  - ジェネレータ
  - 無停電電源装置（UPS）

4.0 セキュリティオペレーション

4.1 与えられたシナリオに基づいて、一般的なセキュリティ手法をコンピューティングリソースに適用することができる。

- **セキュアベースライン**
  - 確立
  - 展開
  - 維持
- **ハードニングのターゲット**
  - モバイルデバイス
  - ワークステーション
  - スイッチ
  - ルーター
  - クラウドインフラストラクチャ
  - サーバー
  - ICS/SCADA
  - 組み込みシステム
  - RTOS
  - IoT デバイス
- **ワイヤレスデバイス**
  - インストールに関する検討事項
    - サイトサーベイ
    - ヒートマップ
- **モバイルソリューション**
  - モバイルデバイス管理（MDM）
  - 展開モデル
    - デバイス持ち込み（BYOD）
    - 企業所有、個人使用（COPE）
    - デバイス選択（CYOD）
  - 接続方法
    - セルラー通信（LTE）
    - Wi-Fi
    - Bluetooth
- **ワイヤレスセキュリティ設定**
  - Wi-Fi Protected Access 3（WPA3）
  - AAA/Remote Authentication Dial-in User Service（RADIUS）
  - 暗号化プロトコル
  - 認証プロトコル
- **アプリケーションセキュリティ**
  - 入力検証
  - セキュア属性（Secure Cookies）
  - 静的コード分析
  - コード署名
- **サンドボックス化**
- **モニタリング**

4.2 適切なハードウェア、ソフトウェア、およびデータアセット管理のセキュリティ関連事項を説明することができる。

- **取得 / 調達プロセス**
- **割り当て / アカウンティング**
  - オーナーシップ
  - 分類
- **モニタリング / アセット追跡**
  - インベントリ
  - 列挙
- **廃棄 / 廃止**
  - サニタイゼーション
  - 破壊
  - 第三者認証
  - データ保持

4.3 脆弱性管理に関連する様々なアクティビティを説明することができる。

- **特定方法**
  - 脆弱性スキャン
  - アプリケーションセキュリティ
    - 静的解析
    - 動的解析
    - パッケージモニタリング
  - 脅威フィード
    - オープンソースインテリジェンス（OSINT）
    - 専有 / サードパーティー
    - 情報共有組織
    - ダークウェブ
  - ペネトレーションテスト
  - 責任ある公開プログラム
    - バグバウンティプログラム
  - システム / プロセスの監査
- **分析**
  - 確認
    - フォールスポジティブ
    - フォールスネガティブ
  - 優先順位
  - 共通脆弱性スコアリングシステム（CVSS）
  - 共通脆弱性タイプ一覧（CVE）
  - 脆弱性分類
  - 露出係数
  - 環境変数
  - 業界 / 組織的影響
  - リスク許容度
- **脆弱性への対応と是正**
  - パッチ適用
  - 保険
  - セグメンテーション
  - 補正的コントロール
  - 例外と除外
- **是正の検証**
  - 再スキャン
  - 監査
  - 検証
- **レポート**

4.4 セキュリティアラートとモニタリングのコンセプトとツールを説明することができる。

- **コンピューティングリソースのモニタリング**
  - システム
  - アプリケーション
  - インフラストラクチャ
- **アクティビティ**
  - ログ集約
  - アラート
  - スキャン
  - レポート
  - アーカイブ
  - アラートへの対応と是正 / 検証
    - 隔離
    - アラートの調整
- **ツール**
  - セキュリティ設定共通化手順（SCAP）
  - ベンチマーク
  - エージェント / エージェントレス
  - Security Information and Event Management（SIEM）
  - アンチウイルス
  - データ損失防止（DLP）
  - Simple Network Management Protocol（SNMP）トラップ
  - NetFlow
  - 脆弱性スキャナー

4.5 与えられたシナリオに基づいて、エンタープライズ機能を修正してセキュリティを強化することができる。

- **ファイアウォール**
  - ルール
  - アクセスリスト
  - ポート / プロトコル
  - スクリーンサブネット
- **IDS/IPS**
  - 傾向
  - 署名
- **Web フィルター**
  - エージェントベース
  - 一元的プロキシ
  - Universal Resource Locator（URL）スキャン
  - コンテンツのカテゴリー化
  - ブロックルール
  - 評判
- **オペレーティングシステムのセキュリティ**
  - グループポリシー
  - SELinux
- **セキュアなプロトコルの実装**
  - プロトコルの選択
  - ポートの選択
  - トランスポートの方法
- **DNS フィルタリング**
- **電子メールのセキュリティ**
  - Domain-based Message Authentication Reporting and Conformance（DMARC）
  - DomainKeys Identified Mail（DKIM）
  - Sender Policy Framework（SPF）
  - ゲートウェイ
- **ファイル完全性モニタリング**
- **DLP**
- **ネットワークアクセスコントロール（NAC）**
- **エンドポイントでの検出と対応（EDR）/ 拡張検出と対応（XDR）**
- **ユーザー行動分析**

4.6 与えられたシナリオに基づいて、ID とアクセスの管理を実施および維持することができる。

- **ユーザーアカウントのプロビジョニング / デプロビジョニング**
- **許可の割り当てと関連事項**
- **アイデンティティプルーフィング**
- **フェデレーション**
- **シングルサインオン（SSO）**
  - Lightweight Directory Access Protocol（LDAP）
  - オープン認証（OAuth）
  - Security Assertions Markup Language（SAML）
- **相互運用性**
- **アテステーション**
- **アクセスコントロール**
  - 強制
  - 任意
  - ロールベース
  - ルールベース
  - 属性ベース
  - Time of day/ 時間帯制限
  - 最小権限
- **多要素認証**
  - 実装
    - 生体認証
    - ハード / ソフト認証トークン
    - セキュリティキー
  - 要素
    - Something you know
    - Something you have
    - Something you are
    - Somewhere you are
- **パスワードのコンセプト**
  - パスワードのベストプラクティス
    - 長さ
    - 複雑さ
    - 再利用
    - 有効期限
    - 経過期間
  - パスワードマネージャー
  - パスワードレス
- **特権アクセス管理ツール**
  - ジャストインタイム許可
  - パスワードボールト
  - 一時的な認証情報

4.7 セキュアなオペレーションに関連する自動化とオーケストレーションの重要性を説明することができる。

- **自動化とスクリプティングのユースケース**
  - ユーザーのプロビジョニング
  - リソースのプロビジョニング
  - ガードレール
  - セキュリティグループ
  - チケット作成
  - エスカレーション
  - サービスとアクセスの有効化 / 無効化
  - 継続的インテグレーションとテスト
  - 統合と Application Programming Interface（API）
- **メリット**
  - 効率性 / 時間節約
  - ベースラインの実施
  - 標準的なインフラストラクチャ構成
  - セキュアな規模拡張
  - 従業員の定着
  - 応答時間
  - 労働力の倍増
- **その他の検討事項**
  - 複雑性
  - 費用
  - 単一障害点（SPOF）
  - 技術的負債
  - 継続的なサポートの可能性

4.8 適切なインシデントレスポンスアクティビティを説明することができる。

- **プロセス**
  - 準備
  - 検知
  - 分析
  - 封じ込め
  - 根絶
  - 復旧
  - 教訓
- **トレーニング**
- **テスト**
  - 机上演習
  - シミュレーション
- **根本原因分析**
- **脅威ハンティング**
- **デジタルフォレンジック**
  - 訴訟ホールド
  - 証拠の連鎖
  - 調達
  - レポート
  - 保全
  - E- ディスカバリ

4.9 与えられたシナリオに基づいて、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。

- **ログデータ**
  - ファイアウォールログ
  - アプリケーションログ
  - エンドポイントログ
  - OS 固有のセキュリティログ
  - IDS/IPS ログ
  - ネットワークログ
  - メタデータ
- **データソース**
  - 脆弱性スキャン
  - 自動化されたレポート
  - ダッシュボード
  - パケットキャプチャ

CompTIA

5.0 セキュリティプログラムの管理と監督

5.1 効果的なセキュリティガバナンスの要素を説明することができる。

- ガイドライン
- ポリシー
  - 利用規約（AUP）
  - 情報セキュリティポリシー
  - 事業継続
  - 災害復旧
  - インシデントレスポンス
  - ソフトウェア開発ライフサイクル（SDLC）
  - 変更管理
- 標準
  - パスワード
  - アクセスコントロール
  - 物理的セキュリティ
  - 暗号化
- 手順
  - 変更管理
  - オンボーディング / オフボーディング
  - プレイブック
- 外部の検討事項
  - 規制
  - 法務
  - 業界
  - 現地 / 地域規模
  - 国家規模
  - 世界規模
- モニタリングと改訂
- ガバナンス構造のタイプ
  - 取締役会
  - 委員会
  - 政府機関
  - 一元的 / 非一元的
- システムとデータに関するロールと責任
  - オーナー
  - コントローラー
  - プロセッサー
  - カストディアン / スチュワード

5.2 リスク管理プロセスの要素を説明することができる。

- リスク特定
- リスクアセスメント
  - アドホック
  - 定期的
  - ワンタイム
  - 継続的
- リスク分析
  - 定性的
  - 定量的
  - 単一損失予測（SLE）
  - 年間損失予測（ALE）
  - 年間発生率（ARO）
  - 確率
  - 可能性
  - 露出係数
  - 影響
- リスク登録簿
  - 重要なリスク指標
  - リスクオーナー
  - リスクしきい値
- リスク受容
- リスクアペタイト
  - 拡大的
  - 保守的
  - 中立
- リスク管理戦略
  - 移転
  - 受容
    - 除外
    - 例外
  - 回避
  - 低減
- リスク報告
- 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）

5.3 サードパーティーのリスク評価とリスク管理に関連するプロセスを説明することができる。

- **ベンダーアセスメント**
  - ペネトレーションテスト
  - 監査権条項
  - 内部監査の証拠
  - 独立評価
  - サプライチェーン分析
- **ベンダーの選択**
  - デューディリジェンス
  - 利益相反
- **合意書のタイプ**
  - サービスレベル合意書（SLA）
  - 合意覚書（MOA）
  - 了解覚書（MOU）
  - マスターサービス契約書（MSA）
  - 作業指示（WO）/ 作業明細書（SOW）
  - 秘密保持契約書（NDA）
  - ビジネスパートナー契約書（BPA）
- **ベンダーの監視**
- **アンケート**
- **行動規定**（ROE）

5.4 効果的なセキュリティコンプライアンスの要素を説明することができる。

- **コンプライアンスレポート**
  - 内部
  - 外部
- **コンプライアンス違反の結果**
  - 罰金
  - 制裁措置
  - 風評被害
  - ライセンスの喪失
  - 契約への影響
- **コンプライアンス監視**
  - デューディリジェンス / ケア
  - 証明と同意
  - 内部と外部
  - 自動化
- **プライバシー**
  - 法的な影響
    - 現地 / 地域規模
    - 国家規模
    - 世界規模
  - データ主体
  - コントローラーとプロセッサー
  - オーナーシップ
  - データのインベントリと保持
  - 忘れられる権利

5.5 監査および評価のタイプと目的を説明することができる。

- **アテステーション**
- **内部**
  - コンプライアンス
  - 監査委員会
  - セルフアセスメント
- **外部**
  - 規制
  - 調査
  - 評価
  - 独立した第三者による監査
- **ペネトレーションテスト**
  - 物理的
  - オフェンシブ
  - ディフェンシブ
  - 統合型
  - 既知の環境
  - 部分的に既知の環境
  - 未知の環境
  - 偵察
    - パッシブ
    - アクティブ

5.6 与えられたシナリオに基づいて、セキュリティ意識向上のプラクティスを実施することができる。

- **フィッシング**
  - キャンペーン
  - フィッシングの試みの認識
  - 報告された疑わしいメッセージへの対応
- **異常なビヘイビアの認識**
  - リスキー
  - 予期しない
  - 意図的でない
- **ユーザーのガイドとトレーニング**
  - ポリシー / ハンドブック
  - 状況認識
  - インサイダーの脅威
  - パスワード管理
  - リムーバブルメディアとデバイス
  - ソーシャルエンジニアリング
  - 業務上のセキュリティ
  - ハイブリッド / リモート勤務環境
- **報告と監視**
  - 初期
  - 定期的
- **開発**
- **実行**

CompTIA Security+ SY0-701 略語リスト

下記は CompTIA Security+ SY0-701 試験で使用される略語の一覧です。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	詳細説明
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AES-256	Advanced Encryption Standards 256-bit
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
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 Partners Agreement
BPDU	Bridge Protocol Data Unit
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
CCMP	Counter Mode/CBC-MAC Protocol
CCTV	Closed-circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback

略語	詳細説明
CHAP	Challenge Handshake Authentication Protocol
CIA	Confidentiality, Integrity, Availability
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CMS	Content Management System
COOP	Continuity of Operation Planning
COPE	Corporate Owned, Personally Enabled
CP	Contingency Planning
CRC	Cyclical Redundancy Check
CRL	Certificate Revocation List
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 Vulnerability Enumeration
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
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman Ephemeral
DKIM	DomainKeys Identified Mail
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DMARC	Domain Message Authentication Reporting and Conformance
DNAT	Destination Network Address Translation
DNS	Domain Name System
DoS	Denial of Service
DPO	Data Privacy Officer

略語	詳細説明
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
ERP	Enterprise Resource Planning
ESN	Electronic Serial Number
ESP	Encapsulated Security Payload
FACL	File System Access Control List
FDE	Full Disk Encryption
FIM	File Integrity Management
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	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 Secure
HVAC	Heating, Ventilation Air Conditioning
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
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

略語	詳細説明
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol
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
ISO	International Standards Organization
ISP	Internet Service Provider
ISSO	Information Systems Security Officer
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	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
ML	Machine Learning
MMS	Multimedia Message Service
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multi-protocol Label Switching
MSA	Master Service Agreement
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSP	Managed Service Provider
MSSP	Managed Security Service Provider
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure

略語	詳細説明
MTTR	Mean Time To Recover
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near Field Communication
NGFW	Next-generation Firewall
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
OSINT	Open-source Intelligence
OSPF	Open Shortest Path First
OT	Operational Technology
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	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
PCI DSS	Payment Card Industry Data Security Standard
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PEM	Privacy Enhanced Mail
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards

略語	詳細説明
PKI	Public Key Infrastructure
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-shared Key
PTZ	Pan-tilt-zoom
PUP	Potentially Unwanted Program
RA	Recovery Agent
RA	Registration Authority
RACE	Research and Development in Advanced Communications Technologies in Europe
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service
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
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
SAN	Storage Area Network
SAN	Subject Alternative Name
SASE	Secure Access Service Edge
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SD-WAN	Software-defined Wide Area Network
SDK	Software Development Kit
SDLC	Software Development Lifecycle
SDLM	Software Development Lifecycle Methodology

略語	詳細説明
SDN	Software-defined Networking
SE Linux	Security-enhanced Linux
SED	Self-encrypting Drives
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
SLE	Single Loss Expectancy
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
SOW	Statement of Work
SPF	Sender Policy Framework
SPIM	Spam over Internet Messaging
SQL	Structured Query Language
SQLi	SQL Injection
SRTP	Secure Real-Time Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXchange
SWG	Secure Web Gateway
TACACS+	Terminal Access Controller Access Control System
TAXII	Trusted Automated eXchange of Indicator Information
TCP/IP	Transmission Control Protocol/ Internet Protocol
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOC	Time-of-check
TOTP	Time-based One-time Password
TOU	Time-of-use
TPM	Trusted Platform Module
TTP	Tactics, Techniques, and Procedures
TSIG	Transaction Signature
UAT	User Acceptance Testing
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
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
VBA	Visual Basic
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
WO	Work Order
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
WTLS	Wireless TLS
XDR	Extended Detection and Response
XML	Extensible Markup Language
XOR	Exclusive Or
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting

CompTIA Security+ SY0-701 ハードウェアとソフトウェアの一覧

本リストは Security+ SY0-701 認定試験の受験準備として役立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
- タブレット
- ノートパソコン
- Web サーバー
- ファイアウォール
- ルーター
- スイッチ
- IDS
- IPS
- ワイヤレスアクセスポイント
- 仮想マシン
- メールシステム
- インターネットアクセス
- DNS サーバー
- IoT デバイス
- ハードウェアトークン
- スマートフォン

予備のハードウェア
- NIC
- 電源
- GBIC
- SFP
- マネージドスイッチ
- ワイヤレスアクセスポイント
- UPS

ツール
- Wi-Fi アナライザ
- Nmap
- NetFlow アナライザー

ソフトウェア
- Windows OS
- Linux OS
- Kali Linux
- パケットキャプチャソフトウェア
- ペンテストソフトウェア
- 静的解析と動的解析のツール
- 脆弱性スキャナー
- ネットワークエミュレーター
- サンプルコード
- コードエディタ
- SIEM
- キーロガー
- MDM ソフトウェア
- VPN
- DHCP サービス
- DNS サービス

その他
- クラウド環境へのアクセス
- ネットワーク文書と図表のサンプル
- サンプルログ

CompTIA