CompTIA Cybersecurity Analyst (CySA+) 認定資格試験

出題範囲

試験番号：CS0-002

CompTIA

試験について

CompTIA Cybersecurity Analyst（CySA+）認定資格は、組織のセキュリティに対して先を見越した継続的な対策と改善を実施できるスキルを評価するに認定資格です。
CompTIA CySA+を取得することで、以下の必要な知識とスキルを有していることを証明します。

- インテリジェンスと脅威検知技術の活用
- データの分析と解釈
- 脆弱性の特定と対処
- 予防措置の提案
- インシデントへの効果的な対応と復旧

CompTIA CySA+は、サイバーセキュリティのテクノロジー職種での4年の実務経験で得られる知識と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、試験のすべての出題内容を完全に網羅した一覧ではありません。

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、全員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。受験者はCompTIA受験者合意書を遵守することが求められます。個々の教材が不正教材（通称「ブレインダンプ」）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	CS0-002
問題数	最大で85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	165分
推奨経験	• サイバーセキュリティのテクノロジー職種で4年以上の実務経験 • CompTIA Security+とCompTIA Network+の取得、もしくは同等の知識とスキル
合格スコア	750

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 脅威および脆弱性マネジメント	22%
2.0 ソフトウェアおよびシステムセキュリティ	18%
3.0 セキュリティオペレーションおよびモニタリング	25%
4.0 インシデントレスポンス	22%
5.0 コンプライアンスおよびアセスメント	13%
計	**100%**

1.0 脅威および脆弱性マネジメント

1.1 脅威データとインテリジェンスの重要性を説明することができる。

- **インテリジェンスのソース**
  - オープンソース・インテリジェンス
  - 独自/クローズドソース・インテリジェンス
  - 適時性
  - 関連性
  - 正確性
- **信頼水準**
- **インジケーターマネジメント**
  - Structured Threat Information eXpression (STIX)
  - Trusted Automated eXchange of Indicator Information (TAXII)
  - OpenIoC
- **脅威の分類**
  - 既知の脅威と未知の脅威
  - ゼロデイ攻撃
  - APT攻撃
- **脅威アクター**
  - 国民・国家
  - ハクティビスト
  - 組織犯罪
  - インサイダー脅威
    - 意図的
    - 意図的でない
- **インテリジェンスサイクル**
  - 要件
  - 収集
  - 分析
  - 配布
  - フィードバック
- **コモディティマルウェア**
- **情報共有と分析コミュニティ**
  - ヘルスケア
  - 金融
  - 航空
  - 政府
  - 重要インフラストラクチャ

1.2 与えられたシナリオに基づいて、脅威インテリジェンスを使用して組織のセキュリティをサポートすることができる。

- **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
  - キルチェーン
- **脅威調査**
  - 評判
  - 行動
  - セキュリティ侵害インジケーター (IoC：Indicator of compromise)
  - 共通脆弱性スコアリングシステム (CVSS：Common vulnerability scoring system)
- **脅威モデリングの方法論**
  - 敵対者能力
  - 総合的な攻撃対象領域
  - 攻撃ベクトル
  - 影響
  - 可能性
- **サポート機能のある脅威インテリジェンスの共有**
  - インシデントレスポンス
  - 脆弱性マネジメント
  - リスクマネジメント
  - セキュリティエンジニアリング
  - 検出とモニタリング

1.3 与えられたシナリオに基づいて、脆弱性マネジメントアクティビティを実行することができる。

- **脆弱性の特定**
  - 資産の重要度
  - アクティブスキャンとパッシブスキャン
  - マッピング/列挙
- **検証**
  - トゥルー・ポジティブ
  - フォールス・ポジティブ
  - トゥルー・ネガティブ
  - フォールス・ネガティブ
- **改善/緩和**
  - 構成ベースライン
  - パッチ適用
  - ハードニング
  - 補正コントロール
  - リスク受容
  - 緩和の検証
- **スキャンパラメータと基準**
  - スキャン活動に関連するリスク
  - 脆弱性フィード
  - スコープ
  - クレデンシャルとノンクレデンシャル
  - サーバーベースとエージェントベース
  - 内部と外部
  - 特別な考慮事項
    - データの種類
    - 技術的制約
    - ワークフロー
    - 機密性レベル
    - 規制要件
    - セグメンテーション
    - 侵入防止システム (IPS)、侵入検知システム (IDS)、ファイアウォールの設定
- **改善の阻害要因**
  - 覚書 (MOU)
  - サービスレベルアグリーメント (SLA)
  - 組織のガバナンス
  - ビジネスプロセスの中断
  - 機能の低下
  - レガシーシステム
  - 独自のシステム

1.4 与えられたシナリオに基づいて、一般的な脆弱性アセスメントツールからの出力を分析することができる。

- **Webアプリケーションスキャナー**
  - OWASP Zed Attack Proxy (ZAP)
  - Burp suite
  - Nikto
  - Arachni
- **インフラストラクチャ脆弱性スキャナー**
  - Nessus
  - OpenVAS
  - Qualys
- **ソフトウェア評価ツールとテクニック**
  - 静的解析
  - 動的解析
  - リバースエンジニアリング
  - ファジング
- **列挙**
  - Nmap
  - hping
  - アクティブとパッシブ
  - レスポンダー
- **ワイヤレスアセスメントツール**
  - Aircrack-ng
  - Reaver
  - oclHashcat
- **クラウドインフラストラクチャーアセスメントツール**
  - ScoutSuite
  - Prowler
  - Pacu

1.5 特定のテクノロジーに関連する脅威と脆弱性を説明することができる。

- **モバイル**
- **Internet of Things (IoT)**
- **組み込み**
- **リアルタイムオペレーティングシステム (RTOS：Real-time operating system)**
- **システム・オン・チップ (SoC：System-on-Chip)**
- **フィールド・プログラマブル・ゲート・アレイ (FPGA：Field programmable gate array)**
- **物理的アクセスコントロール**
- **ビルディングオートメーションシステム**
- **車両とドローン**
  - CAN bus
- **ワークフローとプロセスオートメーション・システム**
- **産業用制御システム**
- **監視制御システム (SCADA：Supervisory control and data acquisition)**
  - Modbus

1.6 クラウド運用に関連する脅威と脆弱性を説明することができる。

- **クラウドサービスモデル**
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- **クラウド展開モデル**
  - パブリック
  - プライベート
  - コミュニティー
  - ハイブリッド
- **Function as a Service (FaaS)/サーバーレスアーキテクチャ**
- **Infrastructure as code (IaC)**
- **セキュアではないアプリケーションプログラミングインタフェース (API)**
- **不適切なキーマネジメント**
- **保護されていないストレージ**
- **ロギングとモニタリング**
  - 不十分なロギングとモニタリング
  - アクセス不能

1.7 与えられたシナリオに基づいて、攻撃とソフトウェアの脆弱性を低減するためのコントロールを実装することができる。

- **攻撃の種類**
  - XML（Extensible markup language）攻撃
  - SQL（Structured query language）インジェクション
  - オーバーフロー攻撃
    - バッファ
    - 整数
    - ヒープ
  - リモートコード実行
  - ディレクトリトラバーサル
  - 特権エスカレーション
  - パスワードスプレー
  - クレデンシャルスタッフィング
  - なりすまし
  - 中間者（Man-in-the-middle）攻撃
  - セッションハイジャッキング
  - ルートキット
  - クロスサイトスクリプティング
    - リフレクション
    - APT攻撃
    - ドキュメントオブジェクトモデル (DOM)
- **脆弱性**
  - 不適切なエラー処理
  - デリファレンス
  - セキュアでないオブジェクトのリファレンス
  - 競合状態
  - 認証の失敗
  - 機密情報の露出
  - セキュアでないコンポーネント
  - 不十分なロギングとモニタリング
  - 弱い構成またはデフォルトの構成
  - セキュアでない機能の使用
    - strcpy

2.0 ソフトウェアおよびシステムセキュリティ

2.1 与えられたシナリオに基づいて、インフラストラクチャマネジメントのためのセキュリティソリューションを適用することができる。

- **クラウドとオンプレミス**
- **資産マネジメント**
  - 資産のタグ付け
- **セグメンテーション**
  - 物理的
  - 仮想
  - ジャンプボックス
  - システム分離
    - エアギャップ
- **ネットワークアーキテクチャ**
  - 物理的
  - ソフトウェア定義
  - 仮想プライベートクラウド（VPC）
  - 仮想プライベートネットワーク（VPN）
  - サーバーレス
- **変更管理**
- **仮想化**
  - 仮想デスクトップインフラストラクチャ（VDI）
- **コンテナ化**
- **アイデンティティ/アクセス管理**（IAM：Identity and access management）
  - 特権管理
  - 多要素認証（MFA）
  - シングルサインオン（SSO）
  - フェデレーション
  - ロールベース
  - 属性ベース
  - 強制
  - 手動レビュー
- **クラウドアクセスセキュリティブローカー（CASB）**
- **ハニーポット**
- **監視とロギング**
- **暗号化**
- **証明書マネジメント**
- **アクティブな防御**

2.2 ソフトウェアアシュアランスのベストプラクティスを説明することができる。

- **プラットフォーム**
  - モバイル
  - ウェブアプリケーション
  - クライアント/サーバー
  - 組み込み
  - システム・オン・チップ（SoC：System-on-Chip）
  - ファームウェア
- **ソフトウェア開発ライフサイクル（SDLC）の統合**
- **DevSecOps**
- **ソフトウェア評価方法**
  - ユーザー受け入れテスト（UAT：User acceptance testing）
  - アプリケーションの負荷テスト
  - セキュリティ回帰テスト
  - コードレビュー
- **セキュアなコーディングのベストプラクティス**
  - 入力検証
  - 出力エンコーディング
  - セッションマネジメント
  - 認証
  - データ保護
  - パラメータ化されたクエリ
- **静的解析ツール**
- **動的解析ツール**
- **重要なソフトウェアを検証する正式な方法**
- **サービス指向アーキテクチャ（SOA）**
  - Security Assertions Markup Language (SAML)
  - Simple Object Access Protocol (SOAP)
  - Representational State Transfer (REST)
  - マイクロサービス

2.3 ハードウェア保証のベストプラクティスを説明することができる。

- **ハードウェアの**Root of Trust
  - Trusted platform module (TPM)
  - Hardware security module (HSM)
- **eFuse**
- **Unified Extensible Firmware Interface (UEFI)**
- **信頼できる工場**
- **セキュアな処理**
  - 信頼できる実行
  - セキュアなエンクレーブ
  - プロセッサのセキュリティ拡張
  - アトミック実行
- **アンチタンパー**
- **自己暗号化ドライブ（SED）**
- **信頼できるファームウェアのアップデート**
- **Measured bootとアテステーション**
- **Bus暗号化**

3.0 セキュリティオペレーションおよびモニタリング

3.1 与えられたシナリオに基づいて、セキュリティモニタリングアクティビティの一環としてデータを分析することができる。

- **ヒューリスティクス**
- **トレンド分析**
- **エンドポイント**
  - マルウェア
    - リバースエンジニアリング
  - メモリ
  - システムとアプリケーションのビヘイビア
    - 既知の正常なビヘイビア
    - 異常なビヘイビア
    - エクスプロイトテクニック
  - ファイルシステム
  - User and entity behavior analytics (UEBA)
- **ネットワーク**
  - URL (Uniform Resource Locator) とDNS (domain name system) 分析
    - ドメイン生成アルゴリズム
  - フロー分析
  - パケットとプロトコルの分析
    - マルウェア
- **ログのレビュー**
  - イベントログ
  - Syslog
  - ファイアウォールのログ
  - Webアプリケーションファイアウォール（WAF）
  - プロキシ
  - 侵入検知システム（IDS)/侵入防止システム（IPS）
- **影響分析**
  - 組織の影響と局所的影響
  - 即時と全体
- **セキュリティ情報イベントマネジメント（SIEM: Security information and event management）のレビュー**
  - ルールの記述
  - 既知の不適切なインターネットプロトコル（IP）
  - ダッシュボード
- **クエリの記述**
  - 文字列検索
  - スクリプト
  - パイプ
- **メール分析**
  - 悪意のあるペイロード
  - Domain Keys Identified Mail (DKIM)
  - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
  - Sender Policy Framework (SPF)
  - フィッシング
  - フォワーディング
  - デジタル署名
  - メール署名ブロック
  - 組み込みリンク
  - なりすまし
  - ヘッダー

3.2 与えられたシナリオに基づいて、セキュリティを向上させるために既存のコントロールへ構成変更を実装することができる。

- **権限**
- **ホワイトリストへの登録**
- **ブラックリストへの登録**
- **ファイアウォール**
- **侵入防止システム（IPS）のルール**
- **データ損失防止（DLP）**
- **EDR：Endpoint detection and response**
- **ネットワークアクセスコントロール（NAC）**
- **シンクホール**
- **マルウェアの署名**
  - 開発/ルールの記述
- **サンドボックス**
- **ポートセキュリティ**

3.3 プロアクティブな脅威ハンティングの重要性を説明することができる。

- **仮説を立てる**
- **脅威アクター—とアクティビティをプロファイルする**
- **脅威ハンティングの戦略**
  - 実行可能なプロセス分析
- **攻撃対象領域の削減**
- **重要な資産をまとめる**
- **攻撃ベクトル**
- **統合インテリジェンス**
- **検知機能の改善**

3.4 自動化の概念とテクノロジーを比較対照することができる。

- **ワークフローオーケストレーション**
  - Security Orchestration,Automation, and Response (SOAR)
- **スクリプティング**
- **アプリケーションプログラミングインタフェース (API) の統合**
- **マルウェア署名の自動作成**
- **データの強化**
- **脅威フィードの組み合わせ**
- **機械学習**
- **自動化プロトコルと基準の使用**
  - Security Content Automation Protocol (SCAP)
- **継続的インテグレーション**
- **継続的な展開/デリバリー**

4.0 インシデントレスポンス

4.1 インシデントレスポンスプロセスの重要性を説明することができる。

- **コミュニケーション計画**
  - コミュニケーションを信頼できる当事者に制限する
  - 規制/法的要件に基づいて開示する
  - 情報の不注意な公開を防止する
  - セキュアな通信方法を使用する
  - 報告要件
- **関係機関との対応調整**
  - 法務部
  - 人事部
  - 広報部
  - 内部と外部
  - 法執行機関
  - シニアリーダー層
  - 規制機関
- **データの重要性に寄与する要因**
  - Personally identifiable information (PII)
  - Personal health information (PHI)
  - Sensitive personal information (SPI)
  - 高価値資産
  - 財務情報
  - 知的財産
  - 会社情報

4.2 与えられたシナリオに基づいて、適切なインシデント対応プロセスを適用することができる。

- **準備**
  - トレーニング
  - テスト
  - 手順の文書化
- **検知と分析**
  - 重大度レベル分類に寄与する特性
  - ダウンタイム
  - 復旧時間
  - データの整合性
  - 経済的
  - システムプロセスの重要度
  - リバースエンジニアリング
  - データ解析
- **封じ込め**
  - セグメンテーション
  - 分離
- **根絶と復旧**
  - 脆弱性の軽減
  - サニタイゼーション
  - 再構成/再イメージング
  - セキュアな廃棄
  - パッチ適用
  - 権限の回復
  - リソースの再構成
  - 機能とサービスの回復
  - ロギングの検証とセキュ

リティモニタリングの通信

- **インシデント後のアクティビティ**
  - 証拠保持
  - 教訓レポート
  - 変更管理プロセス
  - インシデントレスポンス計画のアップデート
  - インシデントサマリーレポート
  - IoCの生成
  - モニタリング

4.3 想定されたインシデントに基づき、潜在的なセキュリティ侵害インジケーター（IoC）を分析することができる。

- **ネットワーク関連**
  - 帯域幅の消費
  - ビーコン
  - 不規則なピアツーピア通信
  - ネットワーク上の不正デバイス
  - スキャン/スイープ
  - 異常なトラフィックの急増
  - 非標準ポート上の共通プロトコル
- **ホスト関連**
  - プロセッサの消費
  - メモリの消費
  - ドライブ容量の消費
  - 許可されていないソフトウェア
  - 悪意のあるプロセス
  - 許可されていない変更
  - 許可されていない特権
  - データ流出
  - OSプロセスの異常なビヘイビア
  - ファイルシステムの変更または異常
  - レジストリの変更または異常
  - 許可されていないスケジュールされたタスク
- **アプリケーション関連**
  - 異常なアクティビティ
  - 新規アカウントの導入
  - 想定されていない出力
  - 想定されていないアウトバウンド通信
  - サービスの中断
  - アプリケーションログ

4.4 与えられたシナリオに基づいて、基本的なデジタルフォレンジックテクニックを使用することができる。

- **ネットワーク**
  - Wireshark
  - tcpdump
- **エンドポイント**
  - ディスク
  - メモリ
- **モバイル**
- **クラウド**
- **仮想化**
- **訴訟ホールド**
- **手順**
- **ハッシュ化**
  - バイナリへの変更
- **カービング**
- **データ収集**

5.0 コンプライアンスおよびアセスメント

5.1 データのプライバシーと保護の重要性を理解する。

- **プライバシーとセキュリティ**
- **非技術的制御**
  - 分類
  - オーナーシップ
  - 保持
  - データの種類
  - 保持基準
  - 機密性
  - 法的要件
  - データの主権
  - データの最小化
  - 目的の制限
  - 秘密保持契約 (NDA)
- **技術的制御**
  - 暗号化
  - データ損失防止 (DLP)
  - データマスキング
  - 匿名化
  - トークン化
  - デジタル著作権管理（DRM）
    - 電子透かし
  - 地理的アクセス要件
  - アクセスコントロール

5.2 与えられたシナリオに基づいて、組織のリスク軽減をサポートするセキュリティコンセプトを適用することができる。

- **ビジネス影響度分析**
- **リスク特定プロセス**
- **リスク計算**
  - 確率
  - マグニチュード
- **リスク要因の伝達**
- **リスクの優先順位付け**
  - セキュリティ管理
  - エンジニアリングのトレードオフ
- **システム評価**
- **文書化された補正コントロール**
- **トレーニングと演習**
  - レッドチーム
  - ブルーチーム
  - ホワイトチーム
  - 机上演習
- **サプライチェーンアセスメント**
  - ベンダーのデューデリジェンス
  - ハードウェアソースの信頼性

5.3 フレームワーク、ポリシー、プロシージャー、およびコントロールの重要性を説明することができる。

- **フレームワーク**
  - リスクベース
  - 規範的
- **ポリシーとプロシージャー**
  - 行動規範/倫理
  - 利用規約 (AUP)
  - パスワードポリシー
  - データの所有権
  - データ保持
  - アカウントマネジメント
  - 継続的なモニタリング
  - 作業成果物の保持
- **コントロールのタイプ**
  - 経営
  - 運用
  - テクニカル
  - 予防
  - 検知
  - 対応
  - 是正
- **監査と評価**
  - 規制
  - コンプライアンス

CompTIA Cybersecurity Analyst (CySA+) 略語一覧

下記はCompTIA CySA+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、これらの用語を復習し、理解することをお勧めします。

略語	詳細説明
3DES	Triple Data Encryption Algorithm
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AUP	Acceptable Use Policy
BEC	Business Email Compromise
BYOD	Bring Your Own Device
CA	Certificate Authority
CAN	Controller Area Network
CASB	Cloud Access Security Broker
CI/CD	Continuous Integration/Continuous Delivery
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technology
CPU	Central Processing Unit
CRM	Customer Relations Management
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DGA	Domain Generation Algorithm
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOM	Document Object Model
DRM	Digital Rights Management
EDR	Endpoint Detection and Response

略語	詳細説明
ELK	Elasticsearch, Logstash, Kibana
ERP	Enterprise Resource Planning
FaaS	Function as a Service
FPGA	Field-programmable Gate Array
FTK	Forensic Toolkit
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
IoC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MaaS	Monitoring as a Service
MAC	Mandatory Access Control
MD5	Message Digest 5
MDM	Mobile Device Management
MFA	Multifactor Authentication
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MRTG	Multi Router Traffic Grapher
NAC	Network Access Control
NAS	Network-attached Storage

略語	詳細説明
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NIC	Network Interface Card
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OSSIM	Open Source Security Information Management
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Pluggable Authentication Modules
PCAP	Packet Capture
PCI	Payment Card Industry
PHI	Personal Health Information
PID	Process Identification Number
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-in User Service
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RTOS	Real-time Operating System
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDLC	Software Development Life Cycle
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMB	Server Message Block
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SoC	System on Chip
SPF	Sender Policy Framework
SPI	Sensitive Personal Information
SQL	Structured Query Language
SSH	Secure Shell
SSHD	Solid-state Hybrid Drive
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXpression
TACACS+	Terminal Access Controller Access Control System Plus
TAXII	Trusted Automated eXchange of Intelligence Information
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
XML	Extensible Markup Language
XSS	Cross-site Scripting
ZAP	Zed Attack Proxy

CompTIA CySA+推奨ハードウェアとソフトウェアの一覧

本リストは、CompTIA CySA+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。
各トピックの下の箇条書きリストは例であり、すべてを網羅するものでは
ありません。

ITハードウェア

- VMが実行可能なワークステーション（またはノートパソコン）
- マネージドスイッチ
- ファイアウォール
- 携帯電話
- VoIP電話
- WAP
- IDS/IPS
- IoTデバイス
- サーバー

ソフトウェア

- 攻撃対象のVMイメージ
- Windowsサーバー
- Windowsクライアント
  - Commando VM
- Linux
  - Kali
  - ParrotOS
  - Security Onion
- Chrome OS
- UTMアプライアンス
- pfSense
- Metasploitable
- クラウドインスタンスへのアクセス
  - Azure
  - AWS
  - GCP
- SIEM
  - Graylog
  - ELK
  - Splunk
- 脆弱性スキャナー
  - OpenVAS
  - Nessus