CompTIA Cybersecurity Analyst+（CySA+） 試験出題範囲

試験番号: CS0-001

CompTIA Cybersecurity Analyst（CySA+）認定資格は、中級レベルのセキュリティのスキルと知識を評価するワールドワイドで提供されているベンダーニュートラルの認定資格です。CompTIA CySA+認定資格試験を受験する際には、必須ではありませんが CompTIA Security +の取得、または同等のセキュリティスキルを前提としています。その上で、CompTIA CySA+は、IT セキュリティ分析に必須となる「実践的なテクニカルスキル」に焦点を当てています。

CompTIA CySA+は、IT セキュリティアナリスト、脆弱性アナリスト、脅威インテリジェンスアナリストといった職種の方、またはこれらの職種を目指される方を対象に設計されています。CompTIA CySA+認定資格試験では、脅威検出ツールの構成や使用、データ分析の実施、分析結果から組織内のアプリケーションやシステムをセキュリティ維持と保護といった目的を達成するための脆弱性、脅威、リスクを特定するために必要となるスキルや知識が網羅されています。

CompTIA CySA+認定資格試験は、以下の条件を満たす IT プロフェッショナルを対象としています。
ー情報セキュリティに関連する 3～4 年の実務経験
ーCompTIA Network+、CompTIA Security+の取得、もしくは同等の知識

この出題範囲には、出題分野、出題比率、出題例が含まれています。出題例は出題項目を明確にするためであり、試験の出題内容そのものを反映している訳ではありませんので、ご注意ください。

以下は試験分野および各分野の出題比率表です。

試験分野	出題比率
第1章　脅威の管理	27%
第2章　脆弱性の管理	26%
第3章　サイバーインシデントの対応	23%
第4章　セキュリティ設計とツールの設定	24%
合計	100%

CompTIA Authorized Materials Use Policy

CompTIA では、パートナー契約を締結していない、もしくは承認、推奨、許可されていないサードパーティーのトレーニングサイトで提供されるコンテンツは容認、許可をしていません。CompTIA 認定資格試験の受験のためこれらの教材を利用することは、CompTIA Candidate Agreement の取り決めにより、将来的に受験ができなくなる可能性があります。認定を受けていない教材を利用することに対する CompTIA 認定資格試験の方針をより明確にするため、CompTIA では全ての受験者に対して CompTIA Certification Exam policy を下記の Web サイトにて公開しています。

http://certification.comptia.org/Training/testingcenters/policies.aspx

CompTIA 認定資格試験への学習を始める前に、CompTIA のポリシーをご確認ください。また、全ての受験者は、全ての試験に対して CompTIA Candidate Agreement を遵守する必要があります。

http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx

受験者の方が、教材を利用する前に、これらの教材が不正な教材かどうかを判断していただく際に、必要に応じて examsecurity@comptia.org までメールにてご連絡をいただくことも可能です。

※ 分野別に取扱例があげられていますが、これらがすべての出題傾向を網羅しているわけではありません。また、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、あるいはタスクについて、試験に含まれる可能性があります。

CompTIA は、配信されている試験内容を継続的にセキュリティ上問題がなく、最新の状態であることを監視しています。そのため、試験問題/本出題範囲は、必要に応じて、予告なく変更される場合がございます。予めご了承ください。

また、変更がされた場合においても、全ての学習教材は、問題なくご活用いただけます。

（出題範囲内で使われている略語については、本文書の最後の略語一覧をご参照ください。）

第1章　脅威の管理（27%）

1.1 与えられたシナリオに基づいて、適切なツールとプロセスを用いて、環境の現状調査を実施することができる。

- 手順/一般的なタスク
  - トポロジーディスカバリー
  - OS フィンガープリント
  - サービスディスカバリー
  - パケットキャプチャ
  - ログのレビュー
  - ルータ/ファイアウォールの ACL レビュー
  - メールハーベスティング
  - ソーシャルメディアプロファイリング
  - ソーシャルエンジニアリング
  - DNS ハーベスティング
  - フィッシング
- 環境の変化
  - 無線と有線の違い
  - 仮想環境と物理環境の違い
  - インターナルとエクスターナルの違い
  - オンプレミスシステムとクラウドシステムの違い
- ツール
  - NMAP
  - ホストスキャン
  - ネットワークマッピング
  - NETSTAT
  - パケットアナライザ
  - IDS / IPS
  - HIDS / NIDS
  - ファイアウォールのルールベースとログ
  - Syslog
  - 脆弱性スキャナ
  -

1.2 与えられたシナリオに基づいて、ネットワークの現状調査結果を分析することができる。

- 手順/一般的なタスク
  - トポロジーディスカバリー
- ポイントインタイムデータ分析
  - パケット分析
  - プロトコル分析
  - トラフィック分析
  - ネットフロー分析
  - ワイヤレス分析
- データの相関関係と分析
  - 異常分析
  - トレンド分析
  - 可用性分析
  - ヒューリスティック分析
  - ビヘイビア分析
- アウトプットデータ
  - ファイアウォールログ

- パケットキャプチャ
- NMAP スキャン結果
- イベントログ
- Syslogs
- IDS レポート

- ツール
  - SIEM
  - パケットアナライザ
  - IDS
  - リソース監視ツール
  - ネットフローアナライザ

1.3 想定されたネットワークベースの脅威に対して、適切な対応と対策を実施、または推奨することができる。

- ネットワークセグメンテーション
  - システム分離
  - ジャンプボックス
- ハニーポット
- エンドポイントセキュリティ
- グループポリシー
- ACL
  - シンクホール
- ハードニング
  - 強制アクセス制御（MAC）
  - コントロールの補正
  - 未使用のポート/サービスのブロック
  - パッチの適用
- ネットワークアクセス制御（NAC）
  - 時間ベース
  - ルールベース
  - ロールベース
  - ロケーションベース

1.4 企業のセキュリティを維持するための手法の目的を説明することができる。

- ペネトレーションテスト（侵入テスト）
  - 実施規約
    - －タイミング
    - －スコープ
    - －承認
    - －エクスプロイテーション
    - －コミュニケーション
    - －レポート
- リバースエンジニアリング
  - 分離/サンドボックス
  - ハードウェア
    - －ハードウェアのソースの信頼性
    - －信頼できる製造工場
    - －OEM ドキュメント
- ソフトウェア/マルウェア
  - フィンガープリント/ハッシュ値
  - 分解
- トレーニングと実践演習

- レッドチーム
- ブルーチーム
- ホワイトチーム

- リスク評価
  - 技術管理レビュー
  - 運用管理レビュー
  - 技術的な影響と可能性
    - ー高程度
    - ー中程度
    - ー低程度

第2章　脆弱性の管理（26%）

2.1 与えられたシナリオに基づいて、情報セキュリティの脆弱性の管理を実施することができる。

- 要件の特定
  - 法規制
  - 企業方針
  - データの分類
  - 資産インベントリ情報
    - ークリティカル
    - ーノンクリティカル
- スキャン頻度の確定
  - リスクアペタイト
  - 規制要件
  - 技術的制約
  - ワークフロー
- 要件に応じてスキャンを実行するツールを構成する
  - スキャン条件を決定する
    - ー感度レベル
    - ー脆弱性情報
    - ースコープ
    - ー信用証明書と非信用証明書の違い
    - ーデータの種類
    - ーサーバーベースとエージェントベースの違い
  - ツールの更新/プラグイン
    - ーSCAP
  - パーミッションとアクセス
- スキャンを実行する
- レポートを生成する
  - 自動配布と手動配布の違い
- 修復
  - 優先順位付け
    - ークリティカル
    - ー実装の難易度
  - コミュニケーション/変更管理
  - サンドボックス/テスト
  - 修正に対する阻害要因
    - ーMOU
    - ーSLA
    - ー組織のガバナンス
    - ービジネスプロセスの中断
    - ーデグレード
- 進行中のスキャンと継続的な監視

2.2 与えられたシナリオに基づいて、脆弱性スキャンの出力結果を分析することができる。

- 脆弱性スキャンのレポートを分析する
  - スキャン結果の確認と解釈
    - ーフォールス・ポジティブを特定する
    - ー例外を特定する
    - ーレスポンスアクションの優先順位付け
- 結果の検証と他のデータポイントとの相関関係

- ベストプラクティス、コンプライアンスとの比較
- 結果を調整する
- 関連するログやその他のデータソースを確認する
- トレンドを決定する

2.3 組織内の様々なターゲットに共通する脆弱性を比較対照することができる。

- サーバー
- エンドポイント
- ネットワークインフラストラクチャ
- ネットワークアプライアンス
- 仮想インフラストラクチャ
  - 仮想ホスト
  - 仮想ネットワーク
  - 管理インターフェース
- モバイルデバイス
- 相互接続されたネットワーク
- 仮想プライベートネットワーク（VPN）
- 産業用制御システム（ICS）
- SCADA デバイス

第 3 章　サイバーインシデントの対応（23%）

3.1 与えられたシナリオに基づいて、脅威となるデータや振る舞いを識別し、インシデントの影響を判断することができる。

- 脅威の分類
  - 既知の脅威と未知の脅威の違い
  - ゼロデイ攻撃
  - APT 攻撃（Advanced persistent threat ）
- インシデントの重大度と優先順位付けに寄与する要因
  - 影響のスコープ
    - ーダウンタイム
    - ー復旧時間
    - ーデータの完全性
    - ー経済的影響
    - ーシステムプロセスの致命度
  - データの種類
    - ー個人情報（PII：Personally Identifiable Information）
    - ー健康情報（PHI：Personal Health Information）
    - ーカード情報
    - ー知的財産
    - ー企業秘密
      - 経理データ
      - 合併および買収情報

3.2 与えられた情報に基づいて、ツールキットを準備し、適切なフォレンジックツールを利用して調査を実施することができる。

- フォレンジックキット
  - デジタルフォレンジックワークステーション
  - ライトブロッカー
  - ケーブル
  - ドライブアダプタ
  - ワイプされたリムーバブルメディア
  - カメラ
  - 立ち入り禁止テープ
  - 開封防止シール
  - ドキュメント/フォーム
    - ー証拠の連鎖（Chain of custody）の文書化
    - ーインシデント対応計画
    - ーインシデントフォーム
    - ー通話リスト/エスカレーションリスト
- フォレンジック調査スイート
  - イメージングユーティリティ
  - 分析ユーティリティ
  - 証拠の連鎖（Chain of custody form）
  - ハッシュ値
  - OS とプロセス分析
  - モバイルデバイスフォレンジック
  - パスワードクラッカー
  - 暗号化ツール
  - ログビューアー

3.3 インシデント対応プロセスにおけるコミュニケーションの重要性を説明することができる。

- ステークホルダー
  - 人事
  - 法務
  - マーケティング
  - 経営層
- 通信プロセスの目的
  - 信頼できる関係者のみに通信を制限する
  - 法規制に基づく情報の開示
  - 誤って情報が漏洩しないようにする
  - 安全な通信手段
- 役割に基づく責任
  - 技術的
  - 経営層
  - 法執行機関
  - インシデント対応プロバイダを雇う

3.4 与えられたシナリオに基づき、一般的な兆候を分析し、インシデント対応の最良の行動方針を選択することができる。

- 一般的なネットワークに関連する兆候
  - 帯域幅の消費
  - ビーコニング
  - 不定期なピアツーピア通信
  - ネットワーク上の不正なデバイス
  - スキャンスウィープ
  - 異常なトラフィックスパイク
- 一般的なホストに関連する兆候
  - プロセッサ消費
  - メモリ消費
  - 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
  - データの流出
- 一般的なアプリケーションに関連する兆候
  - 異常なアクティビティ
  - 新しいアカウントの導入
  - 予期しない出力
  - 予期しないアウトバウンド通信
  - サービスの中断
  - メモリオーバーフロー

3.5 インシデントリカバリと事後対応プロセスを要約することができる。

- 封じ込め（コンテインメント）テクニック
  - セグメンテーション
  - アイソレーション
  - リムーバル
  - リバースエンジニアリング
- 根絶テクニック
  - サニタイゼーション

- 再構築/再イメージ化
- 安全な廃棄

- 検証
  - パッチの適用
  - 権限
  - スキャン
  - セキュリティ監視へのログ/通信の確認
- 是正措置
  - 教訓の文書化
  - コントロールプロセスを変更する
  - インシデント対応計画を更新する
- インシデントサマリーを文書化する

第 4 章　セキュリティ設計とツールの設定（24%）

4.1 フレームワーク、共通ポリシー、コントロール、手順の関係を説明することができる。

- 法規制への準拠
- フレームワーク
  - NIST
  - ISO
  - COBIT
  - SABSA
  - TOGAF
  - ITIL
- ポリシー
  - パスワードポリシー
  - 許容される使用ポリシー
  - データ所有ポリシー
  - データ保持ポリシー
  - アカウント管理ポリシー
  - データ分類ポリシー
- コントロール
  - クライテリアに基づいた選択のコントロール
  - 組織的に定義されたパラメータ
  - 物理的制御
  - 論理的制御
  - 管理的制御
- 手順
  - 継続的な監視
  - 証拠の開示
  - パッチの適用
  - 補完コントロールの実装
  - コントロールテスト手順
  - 例外を管理する
  - 修復計画
- 検証と品質管理
  - 監査
  - 査定
  - 評価
  - 成熟度モデル
  - 認証

4.2 与えられたシナリオに基づいて、データに基づいて個人の特定とアクセス管理に関連するセキュリティ問題の修復を推奨することができる。

- コンテキストベース認証に関連するセキュリティ問題
  - 時間
  - ロケーション
  - 頻度
  - 振る舞い
- 個人と関連付けられているセキュリティ問題
  - 社員
  - エンドポイント
  - サーバー

- サービス
- 役割
- アプリケーション

- ID リポジトリに関連するセキュリティ問題
  - ディレクトリサービス
  - TACACS +
  - RADIUS
- フェデレーション/シングルサインオンに関連するセキュリティ問題
  - 手動プロビジョニング/プロビジョニング解除と自動プロビジョニング/プロビジョニング解除の違い
  - セルフサービスのパスワードリセット
- エクスプロイト
  - 偽装
  - 中間者攻撃
  - セッションハイジャック
  - クロスサイトスクリプティング
  - 特権エスカレーション
  - ルートキット

4.3 与えられたシナリオに基づいて、セキュリティ設計を検討し、補完コントロールの実装するための推奨事項を提示することができる。

- セキュリティデータ分析
  - データ集約と相関関係
  - トレンド分析
  - ヒストリカル分析
- 手動レビュー
  - ファイアウォールログ
  - Syslogs
  - 認証ログ
  - イベントログ
- 多層防御（Defense in depth）
  - 人材
    - ートレーニング
    - ーデュアルコントロール
    - ー職務分離
    - ー第三者/コンサルタント
    - ークロストレーニング
    - ー強制的な休暇
    - ー後継者育成計画
  - プロセス
    - ー継続的な改善
    - ースケジュールされたレビュー
    - ープロセスの回収
  - テクノロジー
    - ーレポートの自動化
    - ーセキュリティアプライアンス
    - ーセキュリティスイート
    - ーアウトソーシング
      - SECaaS（Security as a Service）
    - ー暗号化
  - その他のセキュリティコンセプト
    - ーネットワーク設計

－ネットワークセグメンテーション

4.4 与えられたシナリオに基づいて、ソフトウェア開発ライフサイクル（SDLC）を考慮しながら、アプリケーションセキュリティのベストプラクティスを適用することができる。

- ソフトウェア開発のベストプラクティス
  - セキュリティに関する要件定義
  - セキュリティテストのフェーズ
    －静的コード分析
    －Web アプリケーションの脆弱性のスキャン
    －ファジー化
  - －アプリケーションをクロールするためにインターセプションプロキシを使用する
  - マニュアルの査読
  - ユーザー受け入れテスト
  - 負荷テストアプリケーション
  - セキュリティ回帰テスト
  - 入力の検証
- 安全なコーディングのベストプラクティス
  - OWASP
  - SANS
  - 米国インターネットセキュリティセンター（Center for Internet Security）
    －システム設計時の推奨事項
    －ベンチマーク

4.5 様々なサイバーセキュリティツールとテクノロジーを使用する一般的な目的と理由を比較対照することができる。（この出題項目の目的は、特定のベンダーの製品や機能を評価することではありません。）**

- 予防的観点
  - IPS
    －Sourcefire
    －Snort
    －Bro
  - HIPS
  - ファイアウォール
    －Cisco
    －Palo Alto
    －Check Point
  - ウイルス対策
  - マルウェア対策
  - EMET
  - Web プロキシ
  - Web アプリケーションファイアウォール（WAF）
    －ModSecurity
    －NAXSI
    －Imperva
- 収集的観点
  - SIEM
    －ArcSight
    －QRadar
    －Splunk
    －AlienVault
    －OSSIM
    －Kiwi Syslog

- ネットワークスキャン
  - NMAP
- 脆弱性スキャン
  - Qualys
  - Nessus
  - OpenVAS
  - Nexpose
  - Nikto
  - Microsoft Baseline Security Analyzer
- パケットキャプチャ
  - Wireshark
  - tcpdump
  - Network General
  - Aircrack-ng
- コマンドライン/ IP ユーティリティ
  - netstat
  - ping
  - tracert / traceroute
  - ipconfig / ifconfig
  - nslookup / dig
  - Sysinternals
  - OpenSSL
- IDS / HIDS
  - Bro

- 分析的観点
  - 脆弱性スキャン
    - Qualys
    - Nessus
    - OpenVAS
    - Nexpose
    - Nikto
    - Microsoft Baseline Security Analyzer
  - 監視ツール
    - MRTG
    - Nagios
    - SolarWinds
    - Cacti
    - NetFlow Analyzer
  - インターセプションプロキシ
    - Burp Suite
    - Zap
    - Vega
- エクスプロイト
  - インターセプションプロキシ
    - Burp Suite
    - Zap
    - Vega
  - エクスプロイトフレームワーク
    - Metasploit
    - Nexpose
  - ファジィー化

- －Untidy
- －Peach Fuzzer
- －Microsoft SDL File/Regex Fuzzer

- フォレンジック
  - フォレンジックスイート
    - －EnCase
    - －FTK
    - －Helix
    - －Sysinternals
    - －Cellebrite
  - ハッシング
    - －MD5sum
    - －SHAsum
  - パスワードクラッキング
    - －John the Ripper
    - －Cain & Abel
  - イメージング
    - －DD

CompTIA 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。

ACL	—	Access Control List
CIS	—	Center for Internet Security
CoBiT	—	Control Objectives for Information and Related Technology
DNS	—	Domain Name Service
EMET	—	Enhanced Mitigation Experience Toolkit
FTK	—	Forensic Tool Kit
HIDS	—	Host Intrusion Detection System
HIPS	—	Host Intrusion Prevention System
HR	—	Human Resources
ICS	—	Industrial Control Systems
IDS	—	Intrusion Detection System
IPS	—	Intrusion Prevention System
ISO	—	International Organization for Standardization
ITIL	—	Information Technology Infrastructure Library
MAC	—	Mandatory Access Control
MD5	—	Message Digest 5
MOA	—	Memorandum Of Agreement
MOU	—	Memorandum Of Understanding
MRTG	—	Multi Router Traffic Grapher
NAC	—	Network Access Control
NAXSI	—	Nginx Anti XSS & SQL Injection
NIDS	—	Network Intrusion Detection System
NIST	—	National Institute of Standards & Technology
OEM	—	Original Equipment Manufacturer
OSSIM	—	Open Source Security Information Management
OWASP	—	Open Web Application Security Project
PCI	—	Payment Card Industry
PHI	—	Protected Health Information
PII	—	Personally Identifiable Information
RADIUS	—	Remote Authentication Dial-In User Service
SABSA	—	Sherwood Applied Business Security Architecture
SANS	—	System Administration, Networking, and Security Institute
SCADA	—	Supervisory Control and Data Acquisition
SCAP	—	Security Content Automation Protocol
SDLC	—	Software Development Life Cycle
SHA	—	Secure Hash Algorithm
SIEM	—	Security Incident and Event Manager
SLA	—	Service Level Agreement
SSL	—	Secure Sockets Layer
TACACS+	—	Terminal Access Controller Access Control System Plus
TLS	—	Transport Layer Security
TOGAF	—	The Open Group Architecture Framework
VAS	—	Vulnerability Assessment System
VPN	—	Virtual Private Network
WAF	—	Web Application Firewall

CompTIA CySA+ 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験コンポーネントを作成したい場合に役立ちます。各トピックで記載されている内容は、一例であり、出題範囲を全て網羅しているわけではありません。

ITハードウェア

- ルーター
- スイッチ
- ファイアーウォール
- ワークステーション/ラップトップ（ノートPC）
- IDS/IPS
- サーバー
- Write blocker
- ペリカンケース
- ワイヤレスアクセスポイント
- ドライブアダプター
- VoIPフォン
- モバイルフォン

ツール

- ドライバー
- PCサービスツールキット

消耗品

- CAT5/6ケーブル
- 予備ドライブ/予備フラッシュドライブ

ソフトウェア

- 仮想化プラットフォーム
- Kali Linux/BackTrack
- 仮想の攻撃対象
    - Webサーバー
    - データベースサーバー
    - タイムサーバー
    - DNSサーバー
    - PCワークステーション