



CompTIA Cybersecurity Analyst (CySA+)

認定資格試験出題範囲

試験番号：CS0-003



試験について

CompTIA Cybersecurity Analyst (CySA+) 認定資格試験は、合格者が以下を行うために必要な知識とスキルを有することを証明するものです。

- 悪意あるアクティビティの指標を検出し、分析する
- 脅威ハンティングと脅威インテリジェンスの概念を理解する
- 攻撃と脆弱性の管理、優先順位付け、対応に適切なツールおよび方法を使用する
- インシデントレスポンスプロセスを実行する
- 脆弱性管理およびインシデントレスポンスアクティビティに関連する報告とコミュニケーションの概念を理解する

試験開発

CompTIAの認定資格試験は、上級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（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	CS0-003
問題数	最大 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	インシデントレスポンスアナリストまたはセキュリティオペレーションセンター（SOC）アナリストとして 4 年間の実務経験

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	セキュリティオペレーション	33%
2.0	脆弱性管理	30%
3.0	インシデントレスポンス・管理	20%
4.0	報告とコミュニケーション	17%
計		100%



1.0 セキュリティオペレーション

1.1 セキュリティオペレーションにおけるシステムとネットワークアーキテクチャの概念の重要性を説明できる。

- ログインジェスト
 - 時刻同期
 - ログingleレベル
- オペレーティングシステム (OS) の概念
 - Windows レジストリ
 - システムのハードニング
 - ファイル構造
 - 構成ファイルの場所
 - システムプロセス
 - ハードウェアのアーキテクチャ
- インフラストラクチャの概念
 - サーバーレス
 - 仮想化
 - コンテナ化
- ネットワークアーキテクチャ
 - オンプレミス
 - クラウド
 - ハイブリッド
 - ネットワークセグメンテーション
 - ゼロトラスト
 - Secure Access Secure Edge (SASE)
 - ソフトウェア定義ネットワーク (SDN)
- ID・アクセス管理
 - 多要素認証 (MFA)
 - シングルサインオン (SSO)
 - フェデレーション
- Privileged Access Management (PAM)
- パスワードレス
- Cloud Access Security Broker (CASB)
- 暗号化
 - 公開鍵インフラストラクチャ (PKI)
 - SSL インспекション
- 機密データ保護
 - データ損失防止 (DLP)
 - 個人を特定できる情報 (PII)
 - カード会員のデータ (CHD: Cardholder Data)

1.2 与えられたシナリオに基づいて、潜在的な悪意あるアクティビティの指標を分析できる。

- 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 / スニープ
 - 異常なトラフィックの急増
 - 想定外のポートでのアクティビティ
- 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
 - 未承認のソフトウェア
- 悪意のあるプロセス
- 未承認の変更
- 未承認の特権
- 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
- その他
 - ソーシャルエンジニアリング攻撃
 - 難読化リンク



1.3

与えられたシナリオに基づいて、適切なツールまたはテクニックを使用して悪意のあるアクティビティを判断できる。

- ツール
 - パケットキャプチャ
 - Wireshark
 - tcpdump
 - ログ分析 / 相関分析
 - セキュリティ情報とイベント管理 (SIEM)
 - Security Orchestration, Automation, and Response (SOAR)
 - エンドポイントセキュリティ
 - エンドポイントでの検知と対応 (EDR)
 - ドメインネームサービス (DNS) とインターネットプロトコル (IP) レビュー
 - WHOIS
 - AbuseIPDB
- ファイル分析
 - Strings/ 文字列
 - VirusTotal
- サンドボックス
 - Joe Sandbox
 - Cuckoo Sandbox
- 一般的な技術
 - パターン照合
 - コマンド&コントロール
 - 疑わしいコマンドの検証
 - 電子メール分析
 - ヘッダー
 - 偽装
 - DomainKeys Identified Mail (DKIM)
 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- Sender Policy Framework (SPF)
- 組み込みリンク
- ファイル分析
 - ハッシュ化
- ユーザー行動分析
 - 異常なアカウントアクティビティ
 - あり得ない移動
- プログラミング言語 / スクリプティング
 - JavaScript Object Notation (JSON)
 - Extensible Markup Language (XML)
 - Python
 - PowerShell
 - シェルスクリプト
 - 正規表現

1.4

脅威インテリジェンスと脅威ハンティングの概念を比較対照できる。

- 脅威アクター
 - 高度標的型攻撃 (APT)
 - ハクティビスト
 - 組織犯罪
 - 国民・国家
 - スクリプトキディ
 - インサイダーの脅威
 - 意図的
 - 意図的ではない
 - サプライチェーン
- 戦術、技術、手順 (TTP)
- 信頼水準
 - 適時性
 - 関連性
 - 正確性
- 収集手段と情報源
 - オープンソース
 - ソーシャルメディア
 - ブログ / フォーラム
 - 政府広報
 - Computer Emergency Response Team (CERT)
 - Cybersecurity Incident Response Team (CSIRT : サイバーセキュリティインシデントレスポンスチーム)
 - ディープ / ダークウェブ
 - クローズドソース
 - 有料フィード
 - Information Sharing Organizations
 - 内部ソース
- 脅威インテリジェンス共有
 - インシデントレスポンス
 - 脆弱性管理
 - リスク管理
 - セキュリティエンジニアリング
 - 検出とモニタリング
- 脅威ハンティング
 - Indicators of Compromise (IoC)
 - 収集
 - 分析
 - 適用
 - 重点分野
 - 構成 / 構成ミス
 - 隔離されたネットワーク
 - ビジネスクリティカルなアセットとプロセス
 - アクティブな防御
 - ハニーポット



1.5 セキュリティオペレーションにおける効率化とプロセス改善の重要性を説明できる。

- 標準化プロセス
 - 自動化に適したタスクの特定
 - 反復可能/人手を必要としない
 - 自動化を管理・促進するためのチーム連携
- オペレーションの効率化
 - 自動化とオーケストレーション
 - Security Orchestration, Automation, and Response (SOAR)
 - 脅威インテリジェンスデータのオーケストレーション
 - データエンリッチメント
 - 脅威フィードの組み合わせ
 - 人的関与の最小化
- 技術とツールの統合
 - アプリケーションプログラミングインターフェース (API)
 - Webhooks
 - プラグイン
- Single Pane of Glass (SPOG/単一の画面)



2.0 脆弱性管理

2.1 与えられたシナリオに基づいて、脆弱性スキャンの方法と概念を実装できる。

- アセットディスカバリー
 - マップスキャン
 - デバイスフィンガープリンティング
- 特別な考慮事項
 - スケジュール
 - オペレーション
 - パフォーマンス
 - 機密性レベル
 - セグメンテーション
 - 規制要件
- 内部スキャンと外部スキャン
- エージェント型とエージェントレス型
- クレデンシャルとノンクレデンシャル
- パッシブとアクティブ
- 静的と動的
 - リバースエンジニアリング
 - ファジング
- 重要なインフラストラクチャ
 - オペレーショナルテク
 - ノロジー (OT)
 - 産業用制御システム (ICS)
 - Supervisory Control and Data Acquisition (SCADA)
- セキュリティベースラインスキャン
- 業界のフレームワーク
 - Payment Card Industry Data Security Standard (PCI DSS)
 - CIS (Center for Internet Security) benchmarks
 - Open Web Application Security Project (OWASP)
 - 国際標準化機構 (ISO) 27000 シリーズ

2.2 与えられたシナリオに基づいて、脆弱性評価ツールからの出力を分析できる。

- ツール
 - ネットワークスキャンとマッピング
 - Angry IP Scanner
 - Maltego
 - Webアプリケーションスキャナー
 - Burp Suite
 - Zed Attack Proxy (ZAP)
 - Arachni
 - Nikto
 - 脆弱性スキャナー
 - Nessus
 - OpenVAS
 - デバッグ
 - Immunity debugger
 - GNUデバッガ (GDB)
 - 多目的ツール
 - Nmap
 - Metasploit Framework (MSF)
 - Recon-ng
 - クラウドインフラストラクチャセメントツール
 - Scout Suite
 - Prowler
 - Pacu



2.3 与えられたシナリオに基づいて、データを分析して脆弱性の優先順位付けができる。

- 共通脆弱性スコアリングシステム (CVSS) の解釈
 - 攻撃ベクトル
 - 攻撃の複雑さ
 - 権限が必要
 - ユーザーの操作
 - 範囲
- 影響
 - 機密性
 - 完全性
 - 可用性
- 検証
 - True/False Positives
 - True/False Negatives
- コンテキストアウェアネス
 - 内部
 - 外部
 - 隔離
- 悪用可能性 / 武器化
- 資産価値
- ゼロデイ

2.4 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推奨することができる。

- クロスサイトスクリプティング
 - 反射型
 - 永続的
- オーバーフロー脆弱性
 - バッファ
 - 整数
 - ヒープ
 - スタック
- データポイズニング
- アクセス制御の不備
- 暗号化の失敗
- インジェクションフロー
- クロスサイトリクエストフォージェリ
- ディレクトリトラバーサル
- セキュアでない設計
- セキュリティの構成ミス
- エンドオブライフまたは古いコンポーネント
- 識別と認証の失敗
- サーバーサイドリクエストフォージェリ
- リモートコード実行
- 特権エスカレーション
- ローカルファイルインクルード (LFI) / リモートファイルインクルード (RFI)

2.5 脆弱性への対応、取り扱い、管理に関連する概念を説明できる。

- 補正コントロール
- コントロールのタイプ
 - 管理的
 - オペレーション的
 - 技術的
 - 予防的
 - 検知的
 - 応答的
 - 修正的
- パッチと構成の管理
 - テスト
 - 実装
 - ロールバック
 - 検証
- ウインドウ
- 例外
- リスク管理の原則
 - 受容
 - 移転
 - 回避
 - 低減
- ポリシー、ガバナンス、サービスレベル目標 (SLO)
- 優先順位とエスカレーション
- 攻撃対象領域管理
 - エッジディスカバリー
 - パッシブディスカバリー
 - セキュリティコントロールテスト
 - ペネトレーションテストと敵対的エミュレーション
 - バグバウンティ
 - 攻撃対象領域削減
- セキュア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
 - セッション管理
 - 認証
 - データ保護
 - パラメータ化クエリ
- セキュアソフトウェア開発ライフサイクル (SDLC)
- 脅威のモデリング



3.0 インシデントレスポンス・管理

3.1 攻撃手法のフレームワークに関連する概念を説明できる。

- サイバーキルチェーン
- 侵入分析のダイヤモンドモデル
- MITRE ATT&CK
- Open Source Security Testing Methodology Manual (OSS TMM)
- OWASP テスティングガイド

3.2 与えられたシナリオに基づいて、インシデントレスポンスアクティビティを実行できる。

- | | |
|----------------------------|-----------------|
| • 検知と分析 | • 封じ込め、根絶、および復旧 |
| - IoC | - 範囲 |
| - 証拠の取得 | - 影響 |
| ▫ 証拠の連鎖 (Chain of Custody) | - 隔離 |
| ▫ データの完全性検証 | - 改善 |
| ▫ 保全 | - イメージの再取得 |
| ▫ 訴訟ホールド | - 補正コントロール |
| - データとログ解析 | |

3.3 インシデント管理ライフサイクルの準備段階とインシデント後のアクティビティ段階を説明できる。

- | | | |
|------------------|--------------------------|-------------------|
| • 準備 | - 机上演習 | • インシデント後のアクティビティ |
| - インシデントレスポンスプラン | - トレーニング | - フォレンジック分析 |
| - ツール | - 事業継続性 (BC) / 災害復旧 (DR) | - 根本原因分析 |
| - プレイブック | | - 教訓 |



4.0 報告とコミュニケーション

4.1 脆弱性管理の報告とコミュニケーションの重要性を説明できる。

- 脆弱性管理の報告
 - 脆弱性
 - 影響を受けたホスト
 - リスクスコア
 - 低減
 - 再発
 - 優先順位
- コンプライアンスレポート
- アクションプラン
 - 構成管理
 - パッチ適用
- 補正コントロール
 - 意識向上、教育、トレーニング
 - ビジネス要件の変化
- 改善の阻害要因
 - 覚書 (MOU)
 - サービスレベル合意書 (SLA)
 - 組織的ガバナンス
 - ビジネスプロセスの中断
 - 機能の低下
 - レガシーシステム
 - プロプライエタリシステム
- 測定基準と重要業績評価指標 (KPI)
 - 傾向
 - トップ 10
 - 重大な脆弱性とゼロデイ
 - SLO
- ステークホルダーの識別とコミュニケーション

4.2 インシデントレスポンスの報告とコミュニケーションの重要性を説明できる。

- ステークホルダーの識別とコミュニケーション
- インシデントの宣言とエスカレーション
- インシデントレスポンス報告
 - エグゼクティブサマリー
 - 誰が、何を、いつ、どこで、なぜ
 - 推奨
 - タイムライン
 - 影響
- 範囲
- 証拠
- コミュニケーション
 - 法務
 - 広報
 - 顧客コミュニケーション
 - メディア
 - 規制報告
 - 法執行機関
- 根本原因分析
- 教訓
- 測定基準と KPI
 - 平均検出時間
 - 平均応答時間
 - 平均修正時間
 - アラートボリューム

CompTIA CySA+ CS0-003 略語リスト

下記は CompTIA CySA+ CS0-003 試験で使用する略語の一覧です。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	略語	詳細説明
ACL	Access Control List	HTTPS	Hypertext Transfer Protocol Secure
API	Application Programming Interface	IaaS	Infrastructure as a Service
APT	Advanced Persistent Threat	ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol	ICS	Industrial Control Systems
AV	Antivirus	IDS	Intrusion Detection System
BC	Business Continuity	IoC	Indicators of Compromise
BCP	Business Continuity Plan	IP	Internet Protocol
BGP	Border Gateway Protocol	IPS	Intrusion Prevention System
BIA	Business Impact Analysis	IR	Incident Response
C2	Command and Control	ISO	International Organization for Standardization
CA	Certificate Authority	IT	Information Technology
CASB	Cloud Access Security Broker	ITIL	Information Technology Infrastructure Library
CDN	Content Delivery Network	JSON	JavaScript Object Notation
CERT	Computer Emergency Response Team	KPI	Key Performance Indicator
CHD	Cardholder Data	LAN	Local Area Network
CI/CD	Continuous Integration and Continuous Delivery	LDAPS	Lightweight Directory Access Protocol
CIS	Center for Internet Security	LFI	Local File Inclusion
COBIT	Control Objectives for Information and Related Technologies	LOI	Letter of Intent
CSIRT	Cybersecurity Incident Response Team	MAC	Media Access Control
CSRF	Cross-site Request Forgery	MFA	Multifactor Authentication
CVE	Common Vulnerabilities and Exposures	MOU	Memorandum of Understanding
CVSS	Common Vulnerability Scoring System	MSF	Metasploit Framework
DDoS	Distributed Denial of Service	MSP	Managed Service Provider
DKIM	Domain Keys Identified Mail	MSSP	Managed Security Service Provider
DLP	Data Loss Prevention	MTTD	Mean Time to Detect
DMARC	Domain-based Message Authentication, Reporting, and Conformance	MTTR	Mean Time to Repair
DNS	Domain Name Service	NAC	Network Access Control
DoS	Denial of Service	NDA	Non-disclosure Agreement
DR	Disaster Recovery	NGFW	Next-generation Firewall
EDR	Endpoint Detection and Response	NIDS	Network-based Intrusion Detection System
FIM	File Integrity Monitoring	NTP	Network Time Protocol
FTP	File Transfer Protocol	OpenVAS	Open Vulnerability Assessment Scanner
GDB	GNU Debugger	OS	Operating System
GPO	Group Policy Objects	OSSTMM	Open Source Security Testing Methodology Manual
HIDS	Host-based Intrusion Detection System	OT	Operational Technology
HIPS	Host-based Intrusion Prevention System	OWASP	Open Web Application Security Project
HTTP	Hypertext Transfer Protocol	PAM	Privileged Access Management

略語	詳細説明	略語	詳細説明
PCI DSS	Payment Card Industry Data Security Standard	SOC	Security Operations Center
PHP	Hypertext Preprocessor	SPF	Sender Policy Framework
PID	Process Identifier	SQL	Structured Query Language
PII	Personally Identifiable Information	SSL	Secure Sockets Layer
PKI	Public Key Infrastructure	SSO	Single Sign-on
PLC	Programmable Logic Controller	SSRF	Server-side Request Forgery
POC	Proof of Concept	STIX	Structured Threat Information Expression
RCE	Remote Code Execution	SWG	Secure Web Gateway
RDP	Remote Desktop Protocol	TCP	Transmission Control Protocol
REST	Representational State Transfer	TFTP	Trivial File Transfer Protocol
RFI	Remote File Inclusion	TLS	Transport Layer Security
RXSS	Reflected Cross-site Scripting	TRACE	Trade Reporting and Compliance Engine
SaaS	Software as a Service	TTP	Tactics, Techniques, and Procedures
SAML	Security Assertion Markup Language	UEBA	User and Entity Behavior Analytics
SASE	Secure Access Secure Edge	URI	Uniform Resource Identifier
SCADA	Supervisory Control and Data Acquisition	URL	Uniform Resource Locator
SDLC	Software Development Life Cycle	USB	Universal Serial Bus
SDN	Software-defined Networking	VLAN	Virtual LAN
SFTP	Secure File Transfer Protocol	VM	Virtual Machine
SIEM	Security Information and Event Management	VPN	Virtual Private Network
SLA	Service-level Agreement	WAF	Web Application Firewall
SLO	Service-level Objective	WAN	Wide Area Network
SMB	Server Message Block	XDR	Extended Detection Response
SMTP	Simple Mail Transfer Protocol	XML	Extensible Markup Language
SNMP	Simple Network Management Protocol	XSS	Cross-site Scripting
SOAR	Security Orchestration, Automation, and Response	XXE	XML External Entity
		ZAP	Zed Attack Proxy
		ZTNA	Zero Trust Network Access

CompTIA CySA+ CS0-003ハードウェアとソフトウェアのリスト

本リストは、CySA+ CS0-003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

- 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）
- ファイアウォール
- IDS/IPS
- サーバー

ソフトウェア

- Windowsオペレーティングシステム
 - Commando VM
- Linuxオペレーティングシステム
 - Kali
- オープンソースUTMアプライアンス
- Metasploitable
- SIEM
 - Greylog
 - ELK
 - Splunk
- TCPDump
- Wireshark
- 脆弱性スキャナー（OpenVASなど）
- Nessus
- クラウドインスタンスへのアクセス
 - Azure
 - AWS
 - GCP