CompTIA SecurityX 認定資格試験 出題範囲

試験番号：CAS-005

試験について

CompTIA SecurityX（旧称 CASP+）認定資格試験は、以下の必要な知識とスキルを証明します。

- 複雑な環境全体にわたり、セキュアなソリューションの設計、構築、統合、実装を行い、レジリエンスのある企業をサポートする。
- 自動化、モニタリング、検出、インシデント対応を使用して、企業の環境で継続的なセキュリティ運用をプロアクティブにサポートする。
- クラウド、オンプレミス環境、ハイブリッド環境でセキュリティ対策を適用する。
- 暗号技術や手法、（例：人工知能）新たなトレンドの影響が、情報セキュリティに与える影響を考慮する。
- 企業全体にわたり、適切なガバナンス、コンプライアンス、リスク管理、脅威モデリング戦略を活用する

認定資格試験の認定
CompTIA SecurityX 認定資格試験は、国際標準化機構（ISO）17024 標準への準拠を国家規格協会（ANSI）よりに認定されており、定期的に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 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作成されています。

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き、資格認定を取り消され、その後の受験資格を失います。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に、認定資格試験の受験者全員に CompTIA 認定資格試験実施ポリシーをご一読いただくようご案内しております。CompTIA の認定資格試験の受験に向けて学習を始める前に、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。個別の教材が無許可扱いになるかどうかを確認するには、CompTIA（examsecurity@comptia.org）までメールでお問い合わせください。

注意事項
箇条書きで挙げられた項目が、すべての試験内容を網羅しているとは限りません。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、あるいはタスクに関する問題が出題される場合もあります。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、継続的に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や教材等は、引き続き有効に利用できることにご留意ください。

試験の詳細

試験番号	CAS-005
問題数	最大 90 問
出題形式	複数選択、パフォーマンスベース
試験時間	165 分
推奨される経験	少なくとも 10 年間の一般的な IT の実務経験、そのうち少なくとも 5 年間の広範な IT セキュリティの実務経験
合格スコア	合格 / 不合格の記載のみ、得点表記はなし

試験の出題範囲（分野）

下の表は、この試験の試験分野（ドメイン）と出題比率の一覧です。

分野		出題比率
1.0	ガバナンス、リスク、コンプライアンス	20%
2.0	セキュリティアーキテクチャ	27%
3.0	セキュリティエンジニアリング	31%
4.0	セキュリティオペレーション	22%
計		**100%**

1.0 ガバナンス、リスク、コンプライアンス

1.1 組織のセキュリティ要件が与えられた場合に、適切なガバナンスコンポーネントを実装できる。

- **セキュリティプログラムの文書**
  - ポリシー
  - プロシージャー
  - 標準 / スタンダード
  - ガイドライン
- **セキュリティプログラム管理**
  - アウェアネスとトレーニング（意識向上トレーニング）
    - フィッシング
    - セキュリティ
    - ソーシャルエンジニアリング
    - プライバシー
    - 運用セキュリティ
    - 状況認識
  - コミュニケーション
  - 報告
  - 経営陣のコミットメント
  - RACI モデル /RACI マトリクス（Responsible, Accountable, Consulted, Informed）
- **ガバナンスフレームワーク**
  - Control Objectives for Information and Related Technologies（COBIT）
  - Information Technology Infrastructure Library（ITIL）
- **変更管理と構成管理**
  - 資産管理ライフサイクル
  - 構成管理データベース (CMDB)
  - インベントリ
- **ガバナンス、リスク、コンプライアンス（GRC）ツール**
  - マッピング
  - 自動化
  - コンプライアンス追跡
  - 文書化
  - 継続的モニタリング
- **ステージング環境におけるデータガバナンス**
  - 本番環境
  - 開発環境
  - テスト環境
  - 品質保証（QA）
  - データライフサイクル管理

1.2 組織のセキュリティ要件が与えられた場合に、リスク管理アクティビティを実行できる。

- **影響度分析**
  - 極端だが起こりうるシナリオ
- **リスクアセスメントと管理**
  - 定量的分析と定性的分析
  - リスクアセスメントフレームワーク
  - リスクアペタイト（選好度）とリスク許容度
  - リスクの優先順位付け
  - 重要度の影響
  - 修復
  - 検証
- **サードパーティのリスク管理**
  - サプライチェーンのリスク
  - ベンダーのリスク
  - サブプロセッサーのリスク
- 可用性リスクに関する考慮事項
  - 事業継続性とディザスタリカバリ
    - テスト
  - バックアップ
    - 接続済み
    - 接続解除済み
- **機密性リスクに関する考慮事項**
  - データ流出の対応
  - センシティブデータ / 機微データ・部外秘データの侵害
  - インシデントレスポンスのテスト
  - 報告
  - 暗号化
- **完全性リスクに関する考慮事項**
  - リモートジャーナリング
  - ハッシュ化
  - 干渉
  - 改ざん防止
- **プライバシーリスクに関する考慮事項**
  - データ主体の権利
  - データ主権
  - 生体認証
- **危機管理**
- **データ漏洩の対応**

1.3 コンプライアンスが情報セキュリティ戦略にどのように影響を及ぼすかを説明できる。

- **業界特有のコンプライアンスに関する認識**
  - ヘルスケア
  - 金融
  - 政府機関
  - ユーティリティ
- **業界標準**
  - Payment Card Industry Data Security Standard（PCI DSS）
  - 国際標準化機構 / 国際電気標準会議（ISO/IEC）27000 シリーズ
  - デジタル市場法（DMA：Digital Markets Act）
- **セキュリティおよび報告フレームワーク**
  - ベンチマーク
  - 基盤となるベストプラクティス
  - System and Organization Controls 2（SOC 2）
  - NIST サイバーセキュリティフレームワーク（NIST CSF）
  - Center for Internet Security（CIS）
  - Cloud Security Alliance（CSA）
- **監査、アセスメントと認証の違い**
  - 外部
  - 内部
- **プライバシー規制**
  - EU 一般データ保護規則（GDPR）
  - カリフォルニア州消費者プライバシー法（CCPA）
  - 一般データ保護規則（LGPD）
  - 児童オンラインプライバシー保護法（COPPA）
- **法規制間のコンプライアンス要件の認識**
  - e ディスカバリ
  - リーガルホールド
  - デューデリジェンス
  - デューケア
  - 輸出管理
  - 契約上の義務

1.4 与えられたシナリオに基づいて、脅威モデリングアクティビティを実行できる。

- **アクターの特性**
  - モチベーション
    - 金銭的
    - 地政学的
    - 現状改革主義
    - 悪名
    - スパイ行為
  - リソース
    - 時間
    - 金銭
  - 能力
    - サプライチェーンへのアクセス
    - 脆弱性の創出
    - 知識
    - エクスプロイトの開発
- **攻撃パターン**
- **フレームワーク**
  - MITRE Adversarial Tactics, Techniques, and Common Knowledge（ATT&CK）
  - Common Attack Pattern Enumeration and Classification（CAPEC）
  - サイバーキルチェーン
  - 侵入分析のダイヤモンドモデル
  - なりすまし、改ざん、否認、情報漏洩、サービス拒否、特権の昇格（STRIDE）
  - Open Web Application Security Project（OWASP）
- **攻撃対象領域の判断**
  - アーキテクチャレビュー
  - データフロー
  - 信頼境界線
  - コードレビュー
  - ユーザー要因
  - 組織変更
    - 合併
    - 買収
    - 売却
    - スタッフの変更
  - 列挙／検出
    - 社内資産と対外資産
    - サードパーティの接続
    - 未認可の資産 / アカウント
    - クラウドサービスの検出
    - 公開デジタルプレゼンス
- **手法**
  - 不正使用のケース
  - アンチパターン
  - アタックツリー / グラフ
- **組織または環境への脅威の適用可能性のモデル化**
  - 既存システムが配置されている状態
    - 適切なコントロールの選択
  - 既存システムが配置されていない状態

1.5 人工知能（AI）の導入に伴う情報セキュリティ上の課題の概要を説明できる。

- **法的およびプライバシーへの影響**
  - 誤用の可能性
  - 説明可能なモデルと説明不可能なモデル
  - AI の利用に関する組織の方針
  - 倫理的ガバナンス
- **モデルへの脅威**
  - プロンプトインジェクション
  - セキュアでない出力処理
  - トレーニングデータの汚染
  - モデルのサービス拒否攻撃（DoS）
  - サプライチェーンの脆弱性
  - モデルの盗難
  - モデル反転
- **AI を活用した攻撃**
  - セキュアでないプラグイン設計
  - ディープフェイク
    - デジタルメディア
    - 対話型
  - AI パイプラインインジェクション
  - ソーシャルエンジニアリング
  - エクスプロイトの自動生成
- **AI 使用上のリスク**
  - 過度の信頼
  - 機密情報の漏洩
    - モデルに対して
    - モデルから
  - AI の過剰な主体性
- **AI 対応アシスタント / デジタルワーカー**
  - アクセス / 許可
  - ガードレール
  - データ損失防止（DLP）
  - AI 使用の開示

2.0 セキュリティアーキテクチャ

2.1 与えられたシナリオに基づいて、システム要件を分析し、レジリエンスに優れたシステムを設計できる。

- **コンポーネントの配置と設定**
  - ファイアウォール
  - 侵入防止システム（IPS）
  - 侵入検出システム（IDS）
  - 脆弱性スキャンツール
  - 仮想プライベートネットワーク（VPN）
  - ネットワークアクセスコントロール（NAC）
  - ウェブアプリケーションファイアウォール（WAF）
  - プロキシ
  - リバースプロキシ
  - Application Programming Interface（API）ゲートウェイ
  - タップ
  - コレクター
  - コンテンツ配信ネットワーク（CDN）
- **可用性と完全性に関する設計上の考慮事項**
  - ロードバランシング
  - 復元可能性
  - 相互運用性
  - 地理的考慮事項
  - 垂直スケーリングと水平スケーリングの違い
  - 永続性と非永続性の違い

2.2 与えられたシナリオに基づいて、システムのライフサイクルの初期段階とその後の段階を通じてセキュリティを実装することができる。

- **セキュリティ要件の定義**
  - 機能要件
  - 非機能要件
  - セキュリティとユーザビリティのトレードオフ
- **ソフトウェア保証**
  - 静的アプリケーションセキュリティテスト（SAST）
  - 動的アプリケーションセキュリティテスト（DAST）
  - インタラクティブなアプリケーションセキュリティテスト（IAST）
  - ランタイムアプリケーション自己保護（RASP）
  - 脆弱性分析
  - ソフトウェア構成分析（SCA）
  - ソフトウェア部品表（SBOM）
  - 形式手法
- **継続的インテグレーションと継続的デプロイ（CI/CD）**
  - コーディングスタンダードとリンティング
  - ブランチの保護
  - 継続的改善
  - テストアクティビティ
    - カナリア
    - リグレッション
    - 統合
    - 自動テストと再テスト
    - 単体
- **サプライチェーンリスク管理**
  - ソフトウェア
  - ハードウェア
- **ハードウェア保証**
  - 認証と検証プロセス
- End-of-life（EOL）に関する考慮事項

2.3 与えられたシナリオに基づいて、セキュアなアーキテクチャの設計において適切な管理を統合できる。

- **攻撃対象領域の管理と低減**
  - 脆弱性の管理
  - ハードニング
  - 多層防御
  - アーキテクチャ内のレガシーコンポーネント
- **検出および脅威ハンティングの実現要因**
  - ログ記録の一元化
  - 継続的モニタリング
  - アラート
  - センサーの配置
- **情報およびデータのセキュリティ設計**
  - 分類モデル
  - データのラベル付け
  - タグ戦略
- DLP
  - 保存中
  - 転送中
  - データ検出
- **ハイブリッドインフラストラクチャ**
- **サードパーティ統合**
- **コントロール効率**
  - アセスメント
  - スキャン
  - メトリクス

2.4 与えられたシナリオに基づいて、アクセス、認証、認可システムの設計にセキュリティの概念を適用できる。

- プロビジョニング / デプロビジョニング
  - 資格情報の発行
  - セルフプロビジョニング
- フェデレーション
- シングルサインオン（SSO）
- 条件付きアクセス
- ID プロバイダー
- サービスプロバイダー
- 証明書
- ポリシーの決定と執行ポイント
- アクセスコントロールモデル
  - ロールベースのアクセスコントロール
  - ルールベースのアクセスコントロール
  - 属性ベースのアクセスコントロール（ABAC）
  - 強制アクセスコントロール（MAC）
  - 任意アクセスコントロール（DAC）
- ログ記録と監査
- 公開鍵基盤（PKI）アーキテクチャ
  - 証明書の延長
  - 証明書の種類
  - Online Certificate Status Protocol（OCSP）
  - 認証局 / 登録局（CA/RA）
  - テンプレート
  - デプロイおよび統合のアプローチ
- アクセスコントロールリスト
  - 物理的
  - 論理的

2.5 与えられたシナリオに基づいて、企業環境にクラウドの機能をセキュアに実装できる。

- Cloud Access Security Broker（CASB）
  - API ベース
  - プロキシベース
- シャドー IT 検出
- 責任共有モデル
- CI/CD パイプライン
- Terraform
- Ansible
- パッケージモニタリング
- コンテナのセキュリティ
- コンテナオーケストレーション
- サーバーレス
  - ワークロード
  - 関数
  - リソース
- API のセキュリティ
  - 認可
  - ログ記録
  - レート制限
- クラウドと顧客管理の比較
  - 暗号キー
  - ライセンス
- クラウドデータのセキュリティに関する考慮事項
  - データ露出
  - データ流出
  - 残存データ
  - セキュアでないストレージのリソース
- クラウドコントロール戦略
  - 予防的
  - 検出的
  - 防止的
- 顧客環境とクラウド間の接続（Customer-to-cloud）
- クラウドサービスの統合
- クラウドサービスの導入

2.6 与えられたシナリオに基づいて、ゼロトラストの概念をシステムアーキテクチャ設計に統合できる。

- 継続的な認可
- コンテキストベースの再承認
- ネットワークアーキテクチャ
  - セグメンテーション
  - マイクロセグメンテーション
  - VPN
  - Always-on VPN
- API の統合と検証
- 資産の識別、管理、証明
- セキュリティ境界線
  - データ境界
  - セキュアゾーン
  - システムコンポーネント
- 境界の消失
  - Secure Access Secure Edge（SASE）
  - Software-defined Wide Area Network（SD-WAN）
  - ソフトウェア定義ネットワーク
- 主体と対象関係の定義

3.0 セキュリティエンジニアリング

3.1 与えられたシナリオに基づいて、企業環境における ID 管理とアクセス管理（IAM）コンポーネントに関するよくある問題のトラブルシューティングができる。

- 主体アクセスコントロール
  - ユーザー
  - プロセス
  - デバイス
  - サービス
- 生体認証
- シークレット管理
  - トークン
  - 証明書
  - パスワード
  - キー
  - ローテーション
  - 削除
- 条件付きアクセス
  - ユーザーとデバイスのバインディング
  - 地理的位置
  - 時間ベース
  - 設定
- 証明
- クラウド IAM アクセスおよび信頼ポリシー
- ログ記録とモニタリング
- 特権 ID 管理
- 認証と認可
  - Security Assertions Markup Language（SAML）
  - OpenID
  - 多要素認証（MFA）
  - SSO
  - Kerberos
  - Simultaneous Authentication of Equals (SAE)
  - 特権アクセス管理（PAM）
  - オープン認証（OAuth）
  - 拡張認証プロトコル（EAP）
  - ID 検証
  - Institute for Electrical and Electronics Engineers（IEEE）802.1X
  - フェデレーション

3.2 与えられたシナリオに基づいて、システム要件を分析し、エンドポイントとサーバーのセキュリティを強化できる。

- アプリケーションコントロール
- Endpoint Detection Response（EDR）
- イベントのログ記録とモニタリング
- エンドポイント特権管理
- 攻撃対象領域のモニタリングと低減
- ホストベース侵入防御システム / ホストベース侵入検知システム（HIPS/HIDS）
- マルウェア対策
- SELinux
- ホストベースのファイアウォール
- ブラウザ分離
- 構成管理
- モバイルデバイス管理（MDM）技術
- 脅威アクターの戦術、手法、手順（TTP）
  - インジェクション
  - 特権の昇格
  - 認証情報のダンプ（クレデンシャルダンプ）
  - 不正な実行
  - ラテラルムーブメント
  - 防御的回避

3.3 与えられたシナリオに基づいて、複雑なネットワークインフラストラクチャのセキュリティの問題をトラブルシューティングできる。

- **ネットワークの設定ミス**
  - 設定ドリフト
  - ルーティングエラー
  - スイッチエラー
  - セキュアでないルーティング
  - VPN またはトンネル接続エラー
- **IPS/IDS の問題**
  - ルールの設定ミス
  - ルールの欠如
  - フォールスポジティブ / フォールスネガティブ
  - 配置
- **観測可能性**
- **Domain Name System（DNS）のセキュリティ**
  - Domain Name System Security Extensions（DNSSEC）
  - DNS ポイゾニング /DNS 汚染
  - シンクホーリング
  - ゾーン転送
- **メールのセキュリティ**
  - Domain Keys Identified Mail（DKIM）
  - Sender Policy Framework（SPF）
  - Domain-based Message Authentication Reporting & Conformance（DMARC）
  - Secure/Multipurpose Internet Mail Extension（S/MIME）
- **Transport Layer Security（TLS）エラー**
- **暗号の不一致**
- **PKI の問題**
- **暗号技術に関する問題**
- **実装**
- **DoS/ 分散型サービス拒否攻撃（DDoS）**
- **リソース枯渇攻撃**
- **ネットワークアクセスコントロールリスト（ACL）に関する問題**

3.4 与えられたシナリオに沿って、ハードウェアのセキュリティ技術および手法を実装できる。

- **Root of Trust**
  - トラステッドプラットフォームモジュール（TPM）
  - ハードウェアセキュリティモジュール（HSM）
  - 仮想トラステッドプラットフォームモジュール（vTPM）
- **セキュリティコプロセッサ**
  - Central Processing Unit（CPU）セキュリティ拡張機能
  - セキュアエンクレーブ
- **仮想ハードウェア**
- **ホストベースの暗号化**
- **自己暗号化ドライブ（SED）**
- **セキュアブート**
- **メジャードブート**
- **自己修復ハードウェア**
- **改ざん検出とエラー検知と対策**
- **脅威アクターの TTP**
  - ファームウェアの改ざん
  - シミング
  - Universal Serial Bus（USB）ベースの攻撃
  - Basic Input/Output System、Unified Extensible Firmware Interface（BIOS/UEFI）
  - メモリ
  - 電磁妨害（EMI）
  - 電磁パルス（EMP）

3.5 与えられたシナリオに基づいて、専用システムやレガシーシステムを脅威から保護できる。

- **運用技術 (OT)**
  - Supervisory Control and Data Acquisition（SCADA）
  - 産業用制御システム（ICS）
  - 空調システム（HVAC）/ 環境
- **Internet of Things（IoT）**
- **システムオンチップ（SoC）**
- **組み込みシステム**
- **ワイヤレス技術 / 無線周波数（RF）**
- **セキュリティおよびプライバシーに関する考慮事項**
  - セグメンテーション
  - モニタリング
  - 集約
  - ハードニング
  - データ分析
  - 環境
  - 規制
  - 安全性
- **業種固有の課題**
  - ユーティリティ
  - 運輸
  - ヘルスケア
  - 製造
  - 金融
  - 政府 / 防衛
- **専用システムやレガシーシステムの特徴**
  - 保護不可
  - 旧型
  - サポート対象外
  - 制約が多い

3.6 与えられたシナリオに基づいて、企業の保護に自動化を使用できる。

- スクリプティング
  - PowerShell
  - Bash
  - Python
- Cron タスクまたはスケジュール済みタスク
- イベントベースのトリガー
- Infrastructure as code（IaC）
- 設定ファイル
  - Yet Another Markup Language (YAML)
  - Extensible Markup Language (XML)
  - JavaScript Object Notation (JSON)
  - Tom's Obvious, Minimal Language (TOML)
- クラウド API/ ソフトウェア開発キット（SDK）
  - ウェブフック
- 生成 AI
  - コードアシスト
  - 文書化
- コンテナ化
- 自動パッチ適用
- 自動封じ込め
- Security Orchestration, Automation, and Response（SOAR）
  - ランブック
  - プレイブック
- 脆弱性スキャンと報告
- Security Content Automation Protocol（SCAP）
  - Open Vulnerability Assessment Language（OVAL）
  - Extensible Configuration Checklist Description Format（XCCDF）
  - 共通プラットフォーム一覧（CPE）
  - 共通脆弱性識別子（CVE）
  - 共通脆弱性評価システム（CVSS）
- ワークフロー自動化

3.7 高度な暗号技術の概念の重要性を説明できる。

- ポスト量子暗号（PQC）
  - ポスト量子暗号 vs. Diffie-Hellman と楕円曲線暗号（ECC）
  - 量子コンピュータ暗号解読攻撃への耐性
  - 新興技術の実装
- キーストレッチング
- キーの分割
- 準同型暗号（Homomorphic encryption）
- 前方秘匿性（forward secrecy）
- ハードウェアアクセラレーション
- エンベロープ暗号化
- パフォーマンスとセキュリティの関係
- セキュアマルチパーティコンピューティング（秘匿マルチパーティ計算）
- 認証付き暗号（AEAD：Authenticated encryption with associated data）
- 相互認証

3.8 与えられたシナリオに基づいて、適切な暗号技術のユースケースおよび / または手法を適用できる。

- ユースケース
  - 保存中のデータ
  - 転送中のデータ
    - 暗号化されたトンネル
  - 使用中のデータや処理中のデータ
  - セキュアなメール
  - イミュータブルデータベースやブロックチェーン
  - 否認防止
  - プライバシーアプリケーション
  - 法的または法令に関する考慮事項
  - リソースに関する考慮事項
  - データのサニタイズ
  - データの匿名化
  - 証明書ベースの認証
  - パスワードレス認証
  - ソフトウェアの起源
  - ソフトウェアやコードの整合性
  - キーの一元管理と分散管理の違い
- 手法
  - トークン化
  - コード署名
  - 暗号化消去 / 難読化
  - デジタル署名
  - 難読化
  - シリアライズ
  - ハッシュ化
  - ワンタイムパッド
  - 対称暗号化
  - 非対称暗号化
  - 軽量暗号化

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、データを分析してモニタリングおよび対応アクティビティを実行できる。

- **セキュリティ情報イベント管理（SIEM）**
  - イベントの解析
  - イベントの重複排除
  - 非報告デバイス
  - 保持期間
  - イベントのフォールスポジティブとフォールスネガティブ
- **集約データ分析**
  - 相関分析
  - 監査ログの低減
  - 優先順位付け
  - 傾向
- 振る舞いのベースラインと分析
  - ネットワーク
  - システム
  - ユーザー
  - アプリケーション / サービス
- **多様なデータソースの組み込み**
  - 第三者レポートとログ
  - 脅威インテリジェンスフィード
  - 脆弱性スキャン
  - CVE の詳細
  - 報奨金制度
  - DLP データ
  - エンドポイントログ
  - インフラストラクチャデバイスログ
  - アプリケーションログ
  - Cloud security posture management（CSPM）データ
- **アラート**
  - フォールスポジティブ / フォールスネガティブ
  - 障害アラート
  - 優先順位付け要因
    - 重要度
    - 影響
    - 資産の種類
    - 残留リスク
    - データ分類
  - マルウェア
  - 脆弱性
- **報告とメトリクス**
  - 可視化
  - ダッシュボード

4.2 与えられたシナリオに基づいて、脆弱性と攻撃を分析し、攻撃対象領域を低減する推奨ソリューションを提示できる。

- **脆弱性と攻撃**
  - インジェクション
  - クロスサイトスクリプティング（XSS）
  - セキュアでないメモリ使用率
  - レースコンディション
  - クロスサイトリクエストフォージェリ
  - サーバーサイドリクエストフォージェリ
  - セキュアでない設定
  - 組み込みシークレット
  - 古いかパッチ未適用のソフトウェアやライブラリ
  - サポートが終了したソフトウェア
  - 汚染
  - ディレクトリサービスの設定ミス
  - オーバーフロー
  - 非推奨機能
  - 脆弱なサードパーティ
  - Time of check, time of use（TOCTOU）
  - デシリアライゼーション
  - 脆弱な暗号
  - Confused deputy（混乱する代理問題）
  - インプラント
- **緩和策**
  - 入力の検証
  - 出力のエンコーディング
  - セキュアな機能
    - 不可分操作
    - メモリ安全性機能
    - スレッドセーフ機能
  - セキュリティ設計パターン
  - アップデートやパッチの適用
    - オペレーティングシステム（OS）
    - ソフトウェア
    - ハイパーバイザー
    - ファームウェア
    - システムイメージ
  - 最小権限
  - フェイルセーフ
  - シークレット管理
    - キーローテーション
  - 最少機能
  - 多層防御
  - 依存関係管理
  - コード署名
  - 暗号化
  - インデックス作成
  - 許可リスト

4.3 与えられたシナリオに基づいて、脅威ハンティングと脅威インテリジェンスの概念を適用できる。

- **内部情報ソース**
  - 敵対的エミュレーションの取り組み
  - 内部偵察
  - 仮説に基づく検索
  - ハニーポット
  - ハニーネット
  - ユーザー行動分析（UBA）
- **外部情報ソース**
  - オープンソースインテリジェンス（OSINT）
  - ダークウェブモニタリング
  - Information sharing and analysis center（ISAC）
  - 信頼性要因
- **カウンターインテリジェンスとオペレーションのセキュリティ**
- **脅威インテリジェンスプラットフォーム（TIP）**
  - サードパーティーベンター
- **侵害指標（IoC）の共有**
  - Structured Threat Information eXchange（STIX）
  - Trusted automated exchange of indicator information（TAXII）
- **ルールベースの言語**
  - Sigma
  - Yet Another Recursive Acronym（YARA）
  - Rita
  - Snort
- 攻撃指標
  - TTP

4.4 与えられたシナリオに基づいて、インシデント対応アクティビティにおいてデータとアーティファクトを分析できる。

- **マルウェア分析**
  - デトネーション
  - IoC 抽出
  - サンドボックス
  - コードスタイル測定
    - バリアントマッチング
    - コード類似性
    - マルウェアの属性
- **リバースエンジニアリング**
  - 逆アセンブリと逆コンパイル
  - バイナリ
  - バイトコード
- **揮発性ストレージ分析 / 不揮発性ストレージ分析**
- **ネットワーク分析**
- **ホスト解析**
- **メタデータ分析**
  - メールヘッダー
  - 画像
  - 音声や動画
  - ファイルやファイルシステム
- ハードウェア分析
  - Joint Test Action Group（JTAG）
- **データの復旧と抽出**
- **脅威への対応**
- **準備状況の演習**
- **タイムラインの再構築**
- **根本原因分析**
- Cloud Workload Protection Platform（CWPP）
- **インサイダー脅威**

CompTIA SecurityX 略語一覧

CompTIA SecurityX CAS-005 の認定資格試験で使用される略語一覧は、以下の通りです。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	の定義
ABAC	Attribute-based Access Control（属性ベースのアクセスコントロール）
ACL	Access Control List（アクセスコントロールリスト）
ACME	Automated Certificate Management Environment（自動証明書管理環境）
AEAD	Authenticated Encryption with Associated Data（関連データによる認証暗号化）
AI	Artificial Intelligence（人工知能）
API	Application Programming Interface
APT	Advanced Persistent Threat
AQL	Ariel Query Language
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BEAST	Browser Exploit against SSL/TLS（SSL/TLS に対するブラウザエクスプロイト）
BIOS	Basic Input/Output System
BYOD	Bring Your Own Device
C2	Command and Control（コマンドアンドコントロール攻撃）
CA	Certificate Authority（認証局）
CAPEC	Common Attack Pattern Enumeration and Classification
CA/RA	Certificate Authority/Registration Authority（認証局 / 登録局）
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining（暗号ブロック連鎖）
CCPA	California Consumer Privacy Act（カリフォルニア州消費者プライバシー法）
CDN	Content Delivery Network（コンテンツ配信ネットワーク）
CI/CD	Continuous Integration/Continuous Deployment（継続的インテグレーションと継続的デプロイ）
CIS	Center for Internet Security
CMDB	Configuration Database Management（構成データベース管理）
CNAME	Canonical Name
COBIT	Control Objectives for Information and Related Technologies
COPPA	Children's Online Privacy Act（児童オンラインプライバシー保護法）
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPE	Common Platform Enumeration（共通プラットフォーム一覧）
CPU	Central Processing Unit
CRL	Certificate Revocation List（証明書失効リスト）
CRM	Customer Relationship Management（顧客関係管理）
CSA	Cloud Security Alliance
CSPM	Cloud Security Posture Management（クラウドセキュリティ体制管理）
CSR	Certificate Signing Request（証明書署名要求）
CSRF	Cross-site Request Forgery（クロスサイトリクエストフォージェリ）
CVE	Common Vulnerabilities and Exposures（共通脆弱性識別子）
CVSS	Common Vulnerability Scoring System（共通脆弱性評価システム）
CWPP	Cloud Workload Protection Platform（クラウドワークロード保護プラットフォーム）
D3FEND	Detection, Denial, and Disruption Framework Empowering Network Defense
DAC	Discretionary Access Control（任意アクセスコントロール）
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol

略語	の定義
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMA	Digital Markets Act（デジタル市場法）
DMARC	Domain-based Message Authentication Reporting and Conformance
DNS	Domain Name System（ドメインネームシステム）
DNSSEC	Domain Name System Security Extensions
DORA	Digital Operational Resilience Act（デジタル業務レジリエンス法）
DoS	Denial of Service
EAP	Extensible Authentication Protocol（拡張認証プロトコル）
ECC	Elliptic Curve Cryptography（楕円曲線暗号）
EDR	Endpoint Detection Response
EMI	Electromagnetic Interference（電磁妨害）
EMP	Electromagnetic Pulse（電磁パルス）
EOL	End-of-Life
FAST	Flexible Authentication via Secure Tunneling
FDE	Full Disk Encryption（フルディスク暗号化）
FIDO	Fast Identity Online
GDPR	General Data Protection Regulation（EU 一般データ保護規則）
GPO	Group Policy Objects（グループポリシーオブジェクト）
GRC	Governance, Risk and Compliance（ガバナンス、リスク、コンプライアンス）
HIPS/HIDS	Host-based Intrusion Protection System/Host-based Detection System（ホストベース侵入防御システム / ホストベース不正侵入検知システム）
HKLM	Hkey_Local_Machine
HSM	Hardware Security Module（ハードウェアセキュリティモジュール）
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating Ventilation and Air Conditioning（空調システム）
IaC	Infrastructure as Code
IAM	Identity and Access Management（ID 管理とアクセス管理）
IAST	Interactive Application Security Testing
ICS	Industrial Control System（産業用制御システム）
IDS	Intrusion Detection System（不正侵入検出システム）
IDE	Integrated Development Environment（統合開発環境）
IEEE	Institute for Electrical and Electronics Engineers
IIS	Internet Information Services
IKE	Internet Key Exchange
IoC	Indicator of Compromise（侵害指標）
IoT	Internet of Things
IPS	Intrusion Prevention System（侵入防止システム）
ISAC	Information Sharing and Analysis Centers
ISO	International Organization for Standardization（国際標準化機構）
ISP	Internet Service Provider（インターネットサービスプロバイダー）
ITIL	Information Technology Infrastructure Library
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LGPD	General Data Protection Law（一般データ保護法）
LLM	Large Language Model（大規模言語モデル）
MAC	Mandatory Access Control（強制アクセスコントロール）
MDM	Mobile Device Management（モバイルデバイス管理）
MFA	Multifactor Authentication（多要素認証）

略語	の定義
MIME	Multipurpose Internet Mail Extensions
MX	Mail Exchange
NAC	Network Access Control（ネットワークアクセスコントロール）
NFS	Network File System（ネットワークファイルシステム）
NIDS	Network-based Intrusion Detection System（ネットワークベースの不正侵入検出システム）
NIPS	Network-based Intrusion Prevention System（ネットワークベースの侵入防止システム）
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework（国立標準技術研究所サイバーセキュリティフレームワーク）
NTLM	New Technology LAN Manager
OAUTH	Open Authorization
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OS	Operating System（オペレーティングシステム）
OSINT	Open-source Intelligence（オープンソースインテリジェンス）
OT	Operational Technology（運用技術）
OTP	One-Time Password（ワンタイムパスワード）
OVAL	Open Vulnerability Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management（特権アクセス管理）
PCI DSS	Payment Card Industry Data Security Standard
PEAP	Protected Extensible Authentication Protocol
PII	Personally Identifiable Information（個人を特定できる情報）
PKI	Public Key Infrastructure（公開鍵基盤）
PQC	Post-quantum Cryptography（ポスト量子暗号）
PTR	Pointer Record
QA	Quality Assurance（品質保証）
RACI	Responsible, Accountable, Consulted, Informed（実行責任者、説明責任者、協業先、報告先）
RADIUS	Remote Authentication Dial-in User Service
RASP	Runtime Application Self-Protection
RAT	Remote Access Trojan（遠隔操作ウイルス）
RCE	Remote Code Execution（リモートコード実行）
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RF	Radio Frequency（無線周波数）
RPO	Recovery Point Objective（目標復旧時点）
RSA	Rivest-Shamir-Aldeman Encryption Algorithm（Rivest, Shamir, Aldeman 暗号化アルゴリズム）
RTO	Recovery Time Objective（目標復旧時間）
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertions Markup Language
SAN	Storage Area Network
SASE	Secure Access Service Edge
SAST	Static Application Security Testing（静的アプリケーションセキュリティテスト）
SBoM	Software Bill of Materials（ソフトウェア部品表）
SCA	Software Composition Analysis（ソフトウェア構成分析）
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCCM	System Center Configuration Management
SCEP	Simple Certificate Enrollment Protocol
SCHANNEL	Secure Channel
SDK	Software Development Kit（ソフトウェア開発キット）
SDLC	ソフトウェア開発ライフサイクル
SDN	Software Defined Network

略語	の定義
SDR	Software-defined Radio
SD-WAN	Software-defined Wide Area Network
SED	Self-encrypting Drive（自己暗号化ドライブ）
SIEM	Security Information Event Management（セキュリティ情報イベント管理）
SLA	Service-level Agreement（サービスレベルアグリーメント）
S/MIME	Secure/Multipurpose Internet Mail Extensions
SOA	Service-Oriented Architecture（サービス指向アーキテクチャ）
SOAR	Security Orchestration, Automation, and Response
SoC	System-on-Chip（システムオンチップ）
SOC	Security Operations Center（セキュリティオペレーションセンター）
SOC 2	System and Organization Controls 2
SPF	Sender Policy Framework
SSD	Solid-State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-on（シングルサインオン）
STIX	Structured Threat Information eXchange
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege（なりすまし、改ざん、否認、情報漏洩、サービス拒否、特権の昇格）
TAXII	Trusted Automated Exchange of Indicator Information
TIP	Threat Intelligence Platforms（脅威インテリジェンスプラットフォーム）
TLS	Transport Layer Security
TOCTOU	Time of Check, Time of Use
TOML	Tom's Obvious, Minimal Language
TPM	Trusted Platform Module（トラステッドプラットフォームモジュール）
TTP	Tactics, Techniques, and Procedures（戦術、手法、手順）
UBA	User Behavior Analytics（ユーザー行動分析）
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics（ユーザーおよびエンティティの行動分析）
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VDI	Virtual Desktop Environment（仮想デスクトップ基盤）
VPN	Virtual Private Network（仮想プライベートネットワーク）
vTPM	Virtual Trusted Platform Module（仮想トラステッドプラットフォームモジュール）
VLAN	Virtual Local Area Network
VPN	Virtual Private Network（仮想プライベートネットワーク）
WAF	Web Application Firewall（ウェブアプリケーションファイアウォール）
WIPS	Wireless Intrusion Prevention System（ワイアレス侵入防止システム）
WLAN	Wireless Local Area Newtork
XCCDF	Extensible Configuration Checklist Description Format
XDR	Extended Detection and Response
XML	Extensible Markup Language
XSS	Cross-site Scripting
YAML	Yet Another Markup Language
YARA	Yet Another Recursive Acronym

CompTIA SecurityXが提案するハードウェアとソフトウェアの一覧

SecurityX CAS-005認定試験の受験準備として役立てるためにCompTIAが提案するハードウェアとソフトウェアの一覧は以下のとおりです。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する場合に役立ちます。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。

機器

- TPM 搭載コンピューター
- 基本的なサーバーハードウェア（メールサーバー /Active Directory サーバー、トラステッド OS）
- トークン
- モバイルデバイス（Android や iOS）
- スイッチ（マネージドスイッチ）
- ゲートウェイまたはルーター（有線 / ワイヤレス）
- ファイアウォール
- プロキシサーバー
- ロードバランサー
- アクセスポイント
- 生体認証デバイス
- Arduino または Raspberry Pi
- Software-defined radio（SDR）

その他

- サンプルログ
- ネットワークトラフィックのサンプル（パケットキャプチャ）
- 組織構造のサンプル
- ネットワーク文書のサンプル
- インターネット接続
- クラウドサービス
- オンライン生産性向上スイート
- ダイアグラム作成ソフトウェアのコネクタ

ソフトウェア

- 仮想アプライアンス（ファイアウォール、IPS、SIEM ソリューション）
- Windows
- Linux ディストリビューション
- VMware Workstation Player
- 脆弱性アセスメントツール
- Secure Shell（SSH）と Telnet ユーティリティ
- 脅威モデリングツール
- IPS/IDS
- HIPS
- ワイヤレス侵入防止システム（WIPS）
- フォレンジックツール
- 認証局
- Kali および Kali のすべてのツールセット
- GNS および関連ファームウェア
- ログ分析ツール
- API SDK
- Python 3+
- Security Onion ツール
- Metasploitable
- 大規模言語モデルプラットフォーム
- IDE
- 暗号技術ライブラリ
- コードのバージョン管理、統合、デプロイ用プラットフォーム

CompTIA