CompTIA Advanced Security Practitioner (CASP+) 認定資格 試験出題範囲

試験番号：**CAS-004**

試験について

CompTIA Advanced Security Practitioner (CASP+/CAS-004)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：

- 複雑な環境全体にまたがる形でセキュアなソリューションの設計、構築、統合、および実装を行い、弾力性の高い事業をサポートすることができる
- モニタリング、検知、インシデント対応、および自動化を活用し、企業環境内で現在進行中のセキュリティオペレーションを事前にサポートすることができる
- クラウド、オンプレミス、エンドポイント、およびモバイルインフラストラクチャにセキュリティ慣行を適用しつつ、暗号化の技術と手法を検討することができる
- 企業全体におけるガバナンス、リスク、およびコンプライアンス上の要件を検討することができる

CASP+は、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年間の広範なセキュリティ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、試験の出題内容を完全に網羅したものではありません。

認定資格試験の認証

CompTIA CASP+（CAS-004）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、定期的な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試験は、エントリーレベルの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

CompTIACertifications、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	CAS-004
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	165 分
推奨する経験	• 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 • Network+、Security+、CySA+、Cloud+、および PenTest+、またはそれに相当する認定資格ないし知識
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（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 セキュリティアーキテクチャ	29%
2.0 セキュリティオペレーション	30%
3.0 セキュリティエンジニアリングと暗号化技術	26%
4.0 ガバナンス、リスク、コンプライアンス	15%
計	**100%**

1.0 セキュリティアーキテクチャ

1.1 与えられたシナリオに基づいて、セキュリティの要件と目標を分析し、新規または既存のネットワークに対して、適切かつセキュアなネットワークアーキテクチャを実現することができる。

- サービス
  - ロードバランサー
  - 侵入検知システム（IDS）/ ネットワーク侵入検知システム（NIDS）/ ワイヤレス侵入検知システム（WIDS）
  - 侵入防止システム（IPS）/ ネットワーク侵入防止システム（NIPS）/ ワイヤレス侵入防止システム（WIPS）
  - Web アプリケーションファイアウォール（WAF）
  - ネットワークアクセスコントロール（NAC）
  - 仮想プライベートネットワーク（VPN）
  - Domain Name System Security Extensions（DNSSEC）
  - ファイアウォール / 統合脅威管理（UTM）/ 次世代ファイアウォール（NGFW）
  - ネットワークアドレス変換（NAT）ゲートウェイ
  - インターネットゲートウェイ
  - フォワード / 透過型プロキシ
  - リバースプロキシ
  - 分散型サービス拒否（DDoS）保護
  - ルーター
  - メールセキュリティ
  - Application Programming Interface（API）ゲートウェイ / Extensible Markup Language（XML）ゲートウェイ
  - トラフィックミラーリング
    - Switched Port Analyzer（SPAN）ポート
    - ポートミラーリング
    - 仮想プライベートクラウド（VPC）
    - ネットワークタップ
  - センサー
    - セキュリティ情報とイベント管理（SIEM）
    - ファイル完全性モニタリング（FIM）
    - Simple Network Management Protocol（SNMP）トラップ
    - NetFlow
    - データ損失防止（DLP）
    - アンチウイルス
- セグメンテーション
  - マイクロセグメンテーション
  - ローカルエリアネットワーク（LAN）/ 仮想ローカルエリアネットワーク（VLAN）
  - ジャンプボックス
  - スクリーンされたサブネット
  - データゾーン
  - ステージング環境
  - ゲスト環境
  - VPC/ 仮想ネットワーク（VNET）
  - 可用性ゾーン
  - NAC リスト
  - ポリシー / セキュリティグループ
  - リージョン
  - アクセス制御リスト（ACL）
  - ピアツーピア
  - エアギャップ
- 脱境界化 / ゼロトラスト
  - クラウド
  - リモートワーク
  - モバイル
  - アウトソーシングと請負契約
  - ワイヤレス / 無線周波数（RF）ネットワーク
- 様々な組織のネットワークの統合
  - ピアリング
  - クラウドとオンプレミス
  - データの機密性レベル
  - 合併と買収
  - クロスドメイン
  - フェデレーション
  - ディレクトリサービス
- ソフトウェア定義ネットワーク（**SDN**）
  - オープン SDN
  - ハイブリッド SDN
  - SDN オーバーレイ

1.2 与えられたシナリオに基づいて、組織の要件を分析し、インフラストラクチャの正しいセキュリティ設計を決定することができる。

- 拡張性
  - 垂直
  - 水平
- レジリエンシー
  - 高可用性
  - 多様性 / 不均一性
  - 一連の行動のオーケストレーション
  - 分散配分
  - 冗長性
  - レプリケーション
  - クラスタリング
- 自動化
  - 自動スケーリング
  - Security Orchestration, Automation, and Response (SOAR)
  - ブートストラップ
- パフォーマンス
- コンテナ化
- 仮想化
- コンテンツ配信ネットワーク
- キャッシュ

1.3 与えられたシナリオに基づいて、ソフトウェアアプリケーションを、セキュアな形で企業のアーキテクチャに統合することができる。

- ベースラインとテンプレート
  - セキュアな設計パターン /Web テクノロジーの各タイプ
    - ストレージの設計パターン
  - コンテナ API
  - セキュアコーディング標準
  - アプリケーション審査プロセス
  - API 管理
  - ミドルウェア
- ソフトウェア保証
  - サンドボックス / 開発環境
  - サードパーティーライブラリの検証
  - 定義済みの DevOps パイプライン
  - コード署名
  - Interactive Application Security Testing（IAST）、Dynamic Application Security Testing（DAST）、およびStatic Application Security Testing（SAST）
- エンタープライズアプリケーションの統合に関する検討事項
  - 顧客管理（CRM）
  - 企業資源計画（ERP）
  - 構成管理データベース（CMDB）
  - コンテンツマネジメントシステム（CMS）
  - 統合イネーブラ
    - ディレクトリサービス
    - ドメインネームシステム（DNS）
    - サービス指向アーキテクチャ（SOA）
    - エンタープライズサービスバス（ESB）
- 開発ライフサイクルへのセキュリティの統合
  - 公式な手法
  - 要件
  - 保守
  - 挿入と改善
  - 廃棄と再利用
  - テスト
    - 回帰
    - ユニットテスト
    - 結合テスト
  - 開発アプローチ
    - SecDevOps
    - アジャイル
    - ウォーターフォール
    - スパイラル
    - バージョン管理
    - 継続的インテグレーション / 継続的デリバリー（CI/CD）パイプライン
  - ベストプラクティス
    - Open Web Application Security Project（OWASP）
    - 適切な Hypertext Transfer Protocol（HTTP）ヘッダー

1.4 与えられたシナリオに基づいて、データセキュリティの手法を実施し、企業のアーキテクチャを保護することができる。

- データ損失防止
  - 外部メディアの使用禁止
  - 印刷の禁止
  - リモートデスクトッププロトコル（RDP）の禁止
  - クリップボードプライバシー制御
  - 制限された仮想デスクトップインフラストラクチャ（VDI）の実装
  - データ分類による阻止
- データ損失検知
  - 電子透かし
  - デジタル著作権管理（DRM）
  - ネットワークトラフィックの復号 / ディープパケットインスペクション
  - ネットワークトラフィック解析
- データの分類、ラベリング、およびタギング
  - メタデータ / 属性
- 難読化
  - トークン化
  - スクラビング
  - マスキング
- 匿名化
- 暗号化と非暗号化の違い
- データのライフサイクル
  - 作成
  - 使用
  - 共有
  - 保存
  - アーカイブ
  - 破壊
- データのインベントリとマッピング
- データ完全性管理
- データの保存、バックアップ、および復旧
  - RAID

1.5 与えられたシナリオに基づいて、セキュリティの要件と目標を分析し、認証と認可を適切に制御することができる。

- クレデンシャル管理
  - パスワードリポジトリアプリケーション
    - エンドユーザーパスワードストレージ
    - オンプレミスリポジトリとクラウドリポジトリ
  - ハードウェア鍵マネージャー
  - 特権アクセス管理
- パスワードポリシー
  - 複雑さ
  - 長さ
  - 文字の種類
  - 履歴
  - 最大 / 最小有効期間
  - 監査
  - 可逆的暗号化
- フェデレーション
  - 推移する信頼関係
  - OpenID
  - Security Assertion Markup Language（SAML）
  - Shibboleth
- アクセス制御
  - 強制アクセス制御（MAC）
  - 任意アクセス制御（DAC）
  - ロールベースアクセス制御
  - ルールベースアクセス制御
  - 属性ベースアクセス制御
- プロトコル
  - Remote Authentication Dial-in User Server（RADIUS）
  - Terminal Access Controller Access Control System（TACACS）
  - Diameter
  - Lightweight Directory Access Protocol（LDAP）
  - Kerberos
  - OAuth
  - 802.1X
  - Extensible Authentication Protocol（EAP）
- 多要素認証（**MFA**）
  - 2要素認証（2FA）
  - 2段階認証
  - インバンド
  - アウトオブバンド
- ワンタイムパスワード（**OTP**）
  - HMAC-based One-Time Password（HOTP）
  - Time-based One-Time Password（TOTP）
- ハードウェアの **Root of Trust**
- シングルサインオン（**SSO**）
- **JSON Web** トークン（**JWT**）
- 証明とアイデンティティフルーフィング

1.6 一連の要件に基づいて、クラウドと仮想化のセキュアなソリューションを実装することができる。

- 仮想化戦略
  - タイプ1ハイパーバイザーとタイプ2ハイパーバイザーとの違い
  - コンテナ
  - エミュレーション
  - アプリケーションの仮想化
  - VDI
- プロビジョニングとデプロビジョニング
- ミドルウェア
- メタデータとタグ
- デプロイモデルと検討事項
  - ビジネスディレクティブ
    - コスト
    - 拡張性
    - リソース
    - ロケーション
    - データ保護
  - クラウドデプロイモデル
    - プライベート
    - パブリック
    - ハイブリッド
    - コミュニティ
- ホスティングモデル
  - マルチテナント
  - シングルテナント
- サービスモデル
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- クラウドプロバイダーの制約
  - IPアドレス体系
  - VPCピアリング
- 適切なオンプレミス制御の拡張
- ストレージモデル
  - オブジェクトストレージ/ファイルベースストレージ
  - データベースストレージ
  - ブロックストレージ
  - Blob ストレージ
  - キーバリュー型ペア

1.7 暗号化技術と公開鍵インフラストラクチャ (PKI) が、セキュリティの目標と要件をいかにサポートするかを説明することができる。

- プライバシーと機密性の要件
- 完全性の要件
- 否認防止
- コンプライアンスとポリシーの要件
- 一般的な暗号手法の使用例
  - 保存データ
  - 転送データ
  - 処理中のデータ / 使用中のデータ
  - Webサービスの保護
  - 組み込みシステム
  - キーエスクロー/管理
  - モバイルセキュリティ
  - セキュア認証
  - スマードカード
- 一般的な **PKI** の使用例
  - Webサービス
  - Eメール
  - コード署名
  - フェデレーション
  - 信頼モデル
  - VPN
  - 事業とセキュリティの自動化 / オーケストレーション

1.8 新興テクノロジーが企業のセキュリティとプライバシーに与える影響を説明することができる。

- 人工知能
- 機械学習
- 量子コンピューティング
- ブロックチェーン
- 準同型暗号
  - プライベート情報の検索
  - 安全機能評価
  - プライベート機能評価
- 複数の当事者によるコンピューターの安全な使用
- 分散型合意
- ビッグデータ
- 仮想 / 拡張現実
- **3D** プリンタ
- パスワードレス認証
- ナノテクノロジー
- ディープラーニング
  - 自然言語の処理
  - ディープフェイク
- 生体的なりすまし

2.0 セキュリティオペレーション

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

- インテリジェンスの種類
  - 戦術的
    - コモディティマルウェア
  - 戦略的
    - 標的型攻撃
  - 運用
    - 脅威ハンティング
    - 脅威エミュレーション
- アクターの種類
  - Advanced Persistent Threat (APT)/ 国民・国家
  - インサイダー脅威
  - 競合相手
  - ハクティビスト
  - スクリプトキディ
  - 組織犯罪
- 脅威アクターの特性
  - リソース
    - 時間
    - 金銭
  - サプライチェーンアクセス
  - 脆弱性の作成
  - 能力/洗練度
  - 手法の特定
- インテリジェンス収集手段
  - インテリジェンスフィード
  - ディープWeb
  - 専有
  - オープンソースインテリジェンス (OSINT)
  - ヒューマンインテリジェンス (HUMINT)
- フレームワーク
  - MITRE Adversarial Tactics, Techniques, & Common knowledge (ATT&CK)
    - 産業用制御システム (ICS) 向けATT&CK
  - 侵入分析のダイヤモンドモデル
  - サイバーキルチェーン

2.2 与えられたシナリオに基づいて、侵害の痕跡を分析し、適切な対応策を立案することができる。

- セキュリティ侵害インジケーター (**IoC**)
  - パケットキャプチャ (PCAP)
  - ログ
    - ネットワークログ
    - 脆弱性ログ
    - オペレーティングシステムログ
    - アクセスログ
    - NetFlow ログ
  - 通知
    - FIM アラート
    - SIEM アラート
    - DLP アラート
    - IDS/IPS アラート
    - アンチウイルスアラート
  - 通知の深刻度 / 優先順位
  - 異常なプロセスアクティビティ
- 対応
  - ファイアウォールのルール
  - IPS/IDS ルール
  - ACLルール
  - シグネチャルール
  - ビヘイビアルール
  - DLPルール
  - スクリプト / 正規表現

2.3 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。

- 脆弱性スキャン
  - クレデンシャルとノンクレデンシャル
  - エージェントベース/サーバーベース
  - 重大度のランク付け
  - アクティブとパッシブ
- セキュリティ設定共通化手順（**SCAP**）
  - セキュリティ設定チェックリスト記述形式（XCCDF）
  - セキュリティ検査言語（OVAL）
  - 共通プラットフォーム一覧（CPE）
  - 共通脆弱性識別子（CVE）
  - 共通脆弱性スコアリングシステム（CVSS）
  - 共通セキュリティ設定一覧（CCE）
  - 評価結果形式（ARF）
- セルフアセスメントとサードパーティーベンダーによるアセスメント
- パッチ管理
- 情報源
  - 勧告
  - 公報
  - ベンダー Web サイト
  - ISAC
  - ニュース報道

2.4 与えられたシナリオに基づいて、脆弱性アセスメントとペネトレーションテストに関する、適切な手法とツールを使用することができる。

- 方式
  - 静的解析
  - 動的解析
  - サイドチャネル解析
  - リバースエンジニアリング
    - ソフトウェア
    - ハードウェア
  - ワイヤレス脆弱性スキャン
  - ソフトウェアコンポジション解析
  - ファジングテスト
  - ピボッティング
  - 侵入後の活動
  - 永続性
- ツール
  - SCAPスキャナ
  - ネットワークトラフィックアナライザー
  - 脆弱性スキャナ
  - プロトコルアナライザー
  - ポートスキャナー
  - HTTP インターセプタ
  - エクスプロイトフレームワーク
  - パスワードクラッカー
- 依存関係の管理
- 要件
  - 作業範囲（SOW）
  - 交戦規定
  - 侵略的と非侵略的
  - 資産インベントリ
  - 許可とアクセス
  - 企業ポリシーの検討事項
  - 施設の検討事項
  - 物理的セキュリティの検討事項
  - 修正 / 変更のための再スキャン

2.5 与えられたシナリオに基づいて、脆弱性を分析し、リスク低減策を推奨することができる。

- 脆弱性
  - 競合状態
  - オーバーフロー
    - バッファ
    - 整数
  - 認証の失敗
  - セキュアでない参照
  - 不十分な例外処理
  - セキュリティの構成ミス
  - 不適切なヘッダー
  - 情報漏洩
  - 証明書エラー
  - 脆弱な暗号の実装
  - 脆弱な暗号
  - 脆弱な暗号スイートの実装
  - ソフトウェアコンポジション解析
  - 脆弱なフレームワークとソフトウェアモジュールの使用
  - セキュアでない機能の使用
  - サードパーティーのライブラリ
    - 依存性
    - コードインジェクション / 悪意ある変更
    - サポートの終了/寿命
    - 回帰問題
- 本質的に脆弱なシステム / アプリケーション
    - クライアントサイドの処理とサーバーサイドの処理
    - JSON/Representational State Transfer (REST)
    - ブラウザの拡張
      - Flash
      - ActiveX
    - Hypertext Markup Language 5 (HTML5)
    - Asynchronous JavaScript and XML (AJAX)
    - Simple Object Access Protocol (SOAP)
  - 悪意あるコードとバイトコード、もしくはインタープリタ方式とエミュレート方式
- 攻撃
  - ディレクトリトラバーサル
  - クロスサイトスクリプティング (XSS)
  - クロスサイトリクエストフォージェリ (CSRF)
  - インジェクション
    - XML
    - LDAP
    - SQL
    - コマンド
    - プロセス
  - サンドボックスエスケープ
  - 仮想マシン (VM) のホッピング
  - VMエスケープ
  - BGP/ルートハイジャッキング
  - 傍受攻撃
  - サービス拒否 (DoS)/DDoS
  - 認証のバイパス
  - ソーシャルエンジニアリング
  - VLANホッピング

2.6 与えられたシナリオに基づいて、プロセスを用いてリスクを低減することができる。

- 事前予防と検知
  - 追跡
  - 管理策の開発
  - 欺瞞テクノロジー
    - ハニーネット
    - ハニーポット
    - 囮ファイル
    - シミュレーター
    - 動的ネットワーク構成
- セキュリティデータの分析
  - パイプラインの処理
    - データ
    - ストリーム
  - インデックス化と検索
  - ログの収集とキュレーション
  - データベースアクティビティモニター
- 予防
  - アンチウイルス
  - イミュータブルシステム
  - ハードニング
  - サンドボックスのデトネーション
- アプリケーション制御
  - ライセンス技術
  - 許可リストとブロックリスト
  - TOCとTOU
  - アトミック実行
- セキュリティオートメーション
  - クーロン/スケジューリングされたタスク
  - Bash
  - PowerShell
  - Python
- 物理的セキュリティ
  - 照明の見直し
  - ビジターログの見直し
  - カメラの見直し
  - オープンスペースと密閉空間

2.7 与えられたインシデントに基づいて、適切な対応策を実施することができる。

- イベントの分類
  - フォールス・ポジティブ
  - フォールス・ネガティブ
  - トゥルー・ポジティブ
  - トゥルー・ネガティブ
- イベントの優先順位付け
- 事前エスカレーションタスク
- インシデント対応プロセス
  - 準備
  - 検知
  - 分析
  - 封じ込め
  - 復旧
  - 教訓の管理
- 特定の対応に関する手順書 / プロセス
  - シナリオ
    - ランサムウェア
    - データ流出
    - ソーシャルエンジニアリング
  - 自動化されてない対応手法
  - 自動化された対応手法
    - ランブック
    - SOAR
- コミュニケーション計画
- ステークホルダー管理

2.8 フォレンジックコンセプトの重要性について説明することができる。

- 法的な目的と組織的な目的
- フォレンジックプロセス
  - 識別
  - 証拠収集
    - 証拠の連鎖
    - データの揮発性
      - メモリのスナップショット
      - イメージ
    - クローニング
  - 証拠保全
    - セキュアなストレージ
    - バックアップ
  - 分析
    - フォレンジックツール
  - 検証
  - プレゼンテーション
- 完全性の維持
  - ハッシュ化
- 暗号解析
- ステガノグラフィー解析

2.9 与えられたシナリオに基づいて、フォレンジック分析ツールを使用することができる。

- ファイルカービングツール
  - foremost
  - ストリング
- バイナリ解析ツール
  - Hex dump
  - Binwalk
  - Ghidra
  - GDB
  - OllyDbg
  - readelf
  - objdump
  - strace
  - ldd
  - file
- 解析ツール
  - ExifTool
  - Nmap
  - Aircrack-ng
  - Volatility
  - The Sleuth Kit
  - 動的リンクと静的リンク
- イメージングツール
  - Forensic Toolkit (FTK) Imager
  - dd
- ハッシュ化ユーティリティ
  - sha256sum
  - ssdeep
- ライブ収集ツールと事後分析ツール
  - netstat
  - ps
  - vmstat
  - ldd
  - lsof
  - netcat
  - tcpdump
  - conntrack
  - Wireshark

3.0 セキュリティエンジニアリングと暗号化技術

3.1 与えられたシナリオに基づいて、企業のモビリティにセキュアな構成を適用することができる。

- 構成管理
  - アプリケーション制御
  - パスワード
  - MFAの要件
  - トークンベースアクセス
  - パッチリポジトリ
  - Firmware Over-the-Air
  - リモートワイプ
  - WiFi
    - WPA2/WPA3
    - デバイス証明書
  - プロファイル
  - ブルートゥース
  - 近距離無線通信（NFC）
  - 周辺装置
  - ジオフェンシング
  - VPN設定
  - ジオタギング
  - 証明書管理
  - フルデバイス暗号化
  - テザリング
  - 機内モード
  - 位置情報サービス
  - DNS over HTTPS（DoH）
  - カスタムDNS
- デプロイシナリオ
  - Bring Your Own Device（BYOD）
  - Corporate Owned
  - Corporate Owned, Personally Enabled（COPE）
  - Choose Your Own Device（CYOD）
- セキュリティの検討事項
  - 不正なリモートアクティベーション / デバイスまたは機能の非アクティベーション
  - 暗号化通信と非暗号化通信に関する懸念事項
  - 物理的調査
  - 個人情報の盗難
  - 健康に関するプライバシー
  - ウェアラブルデバイスが持つ意味
  - 収集データのデジタルフォレンジック
  - 未承認のアプリケーションストア
  - 脱獄 / root化
  - サイドローディング
  - コンテナ化
  - OEMとキャリアの違い
  - サプライチェーン問題
  - eFuse

3.2 与えられたシナリオに基づいて、エンドポイントセキュリティ管理を構成および実装することができる。

- ハードニング手法
  - 不要なサービスの削除
  - 使用されていないアカウントの無効化
  - イメージ / テンプレート
  - 寿命を迎えたデバイスの処分
  - サポートが終了したデバイスの処分
  - ローカルドライブ暗号化
  - Enable no execute（NX）/ execute never（XN）ビット
  - 中央処理装置（CPU）仮想化サポートの無効化
  - 安全に暗号化されたエンクレーブ / メモリ暗号化
  - Shell の制限
  - Address Space Layout Randomization（ASLR）
- プロセス
  - パッチ適用
    - ファームウェア
    - アプリケーション
  - ロギング
  - モニタリング
- 強制アクセス制御
  - SELinux/SEAndroid
  - カーネルとミドルウェア
- 信頼できるコンピューティング
  - TPM
  - セキュアブート
  - UEFI/BIOS保護
  - 認証サービス
  - Hardware security module（HSM）
  - メジャーブート
  - 自己暗号化ドライブ（SED）
- 補正コントロール
  - アンチウイルス
  - アプリケーション制御
  - ホスト侵入検知システム（HIDS）/ ホスト侵入防止システム（HIPS）
  - ホスト型ファイアウォール
  - エンドポイントでの検知と対応（EDR）
  - 冗長性を有するハードウェア
  - 自己回復ハードウェア
  - ユーザーとエンティティの行動分析（UEBA）

3.3 特定のセクターやオペレーション技術に影響を及ぼすセキュリティ上の検討事項を説明することができる。

- 組み込み
  - Internet of Things（IoT）
  - システムオンチップ（SoC）
  - ASIC
  - FPGA
- **ICS/SCADA**
  - PLC
  - ヒストリアン
  - ラダーロジック
  - 安全計装システム
  - 暖房、換気、および空調（HVAC）
- プロトコル
  - Controller Area Network（CAN）バス
  - Modbus
  - Distributed Network Protocol 3（DNP3）
  - Zigbee
  - Common Industrial Protocol（CIP）
  - データ配信サービス
- セクター
  - エネルギー
  - 製造業
  - ヘルスケア
  - 公共事業
  - 民間サービス
  - 施設サービス

3.4 クラウドテクノロジーの採用が組織のセキュリティにどう影響するかを説明することができる。

- 自動化とオーケストレーション
- 暗号化設定
- ログ
  - 可用性
  - 収集
  - モニタリング
  - 構成
  - 警告
- モニタリング設定
- 鍵の所有権と所在
- 鍵のライフサイクル管理
- バックアップと復旧の手法
  - 事業継続性と災害復旧（BCDR）としてのクラウド
  - プライマリプロバイダーの BCDR
  - 代替プロバイダーの BCDR
- インフラストラクチャとサーバーレスコンピューティング
- アプリケーションの仮想化
- ソフトウェア定義ネットワーク
- 設定ミス
- コラボレーションツール
- ストレージ設定
  - ビット分割
  - データ分散
- クラウドアクセスセキュリティブローカー（**CASB**）

3.5 与えられたビジネス要件に基づいて、適切な PKI ソリューションを実装することができる。

- **PKI** 階層
  - 認証局（CA）
  - 従属 / 中間CA
  - 登録認定機関（RA）
- 証明書の種類
  - ワイルドカード証明書
  - EV証明書
  - マルチドメイン
  - 汎用
- 証明書の使用 / プロファイル / テンプレート
  - クライアント認証
  - サーバー認証
  - デジタル署名
  - コード署名
- 拡張領域
  - コモンネーム（CN）
  - サブジェクト代替名（SAN）
- 信頼できるプロバイダー
- 信頼モデル
- 相互認証
- プロファイルの構成
- ライフサイクル管理
- 公開鍵と秘密鍵
- デジタル署名
- 証明書のピンニング
- 証明書のステープリング
- 証明書署名要求（**CSR**）
- **Online Certificate Status Protocol**（**OCSP**）と証明書失効リスト（**CRL**）
- **HTTP Strict Transport Security**（**HSTS**）

3.6 与えられたビジネス要件に基づいて、暗号化の適切なプロトコルとアルゴリズムを実装することができる。

- ハッシュ化
  - Secure Hashing Algorithm (SHA)
  - Hash-based Message Authentication Code (HMAC)
  - メッセージダイジェスト (MD)
  - RACE Integrity Primitives Evaluation Message Digest (RIPEMD)
  - Poly1305
- 対称アルゴリズム
  - 動作モード
    - Galois/Counter Mode (GCM)
    - Electronic Codebook (ECB)
    - Cipher Block Chaining (CBC)
    - Counter (CTR)
    - Output Feedback (OFB)
  - ストリームとブロック
    - Advanced Encryption Standard (AES)
    - Triple Digital Encryption Standard (3DES)
    - ChaCha
    - Salsa20
- 非対称アルゴリズム
  - 鍵共有
    - ディフィー・ヘルマン
    - 楕円曲線ディフィー・ヘルマン (ECDH)
  - 署名
    - Digital Signature Algorithm (DSA)
    - Rivest, Shamir, and Adleman (RSA)
    - Elliptic-Curve Digital Signature Algorithm (ECDSA)
- プロトコル
  - Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
  - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - Internet Protocol Security (IPSec)
  - Secure Shell (SSH)
  - EAP
- 楕円曲線暗号
  - P256
  - P384
- 前方秘匿性
- 認証付き暗号
- 鍵ストレッチング
  - Password-Based Key Derivation Function 2 (PBKDF2)
  - Bcrypt

3.7 与えられたシナリオに基づいて、暗号化技術の実装に関する問題をトラブルシューティングすることができる。

- 実装と設定の問題
  - 使用期限
  - 間違った証明書の種類
  - 失効した証明書
  - 正しくない名前
  - チェーンの問題
    - 無効な root CA と中間CA
    - 自己署名
  - 脆弱な署名アルゴリズム
  - 脆弱な暗号スイート
  - 正しくない権限
  - 暗号の不一致
  - ダウングレード攻撃
- 鍵
  - 不一致
  - 不適切な鍵の処理
  - 埋め込まれた鍵
  - 鍵の再生成
  - 秘密鍵の漏洩
  - 暗号シュレッディング
  - 暗号学的難読化
  - キーローテーション
  - 侵害された鍵

4.0 ガバナンス、リスク、コンプライアンス

4.1 一連の要件に基づいて、適切なリスク戦略を適用することができる。

- リスクアセスメント
  - 可能性
  - 影響
  - 質と量
  - 露出係数
  - 資産価値
  - 所有にかかる総コスト（TCO）
  - 投資利益率（ROI）
  - 平均復旧時間（MTTR）
  - 平均故障間隔（MTBF）
  - 年間損失予測（ALE）
  - 年間発生率（ARO）
  - 単一損失予測（SLE）
  - ギャップ分析
- リスク処理の手法
  - 移転
  - 受容
  - 回避
  - 低減
- リスクの種類
  - 固有
  - 残余
  - 例外
- リスク管理のライフサイクル
  - 識別
  - 評価
  - コントロール
    - 人物
    - プロセス
    - テクノロジー
    - 保護
    - 検知
    - 対応
    - 復旧
  - レビュー
  - フレームワーク
- リスクの追跡
  - リスク登録簿
  - 重要なパフォーマンス指標
    - 拡張性
    - 信頼性
    - 可用性
  - 重要なリスク指標
- リスクアペタイトとリスク許容度
  - トレードオフ分析
  - 利便性とセキュリティ要件
- ポリシーとセキュリティ慣行
  - 職務分離
  - ジョブローテーション
  - 強制的な休暇
  - 最小権限
  - 雇用および契約終了プロシージャ
  - ユーザー向け研修と意識の向上
  - 監査の要件と頻度

4.2 ベンダーリスクの管理と低減の重要性を説明することができる。

- 共同責任モデル（役割 / 職務）
  - クラウドサービスプロバイダー（CSP）
    - 地理的位置
    - インフラストラクチャ
    - コンピュート
    - ストレージ
    - ネットワーク
    - サービス
  - クライアント
    - 暗号化
    - オペレーティングシステム
    - アプリケーション
    - データ
- ベンダーロックインとベンダーロックアウト
- ベンダーの生存能力
  - 財務リスク
  - 吸収合併リスク
- 顧客要件を満たす
  - 法務
  - 変更管理
  - 離職
  - デバイスと技術的構成
- サポートの可用性
- 地理的考慮事項
- サプライチェーンの可視性
- インシデントの報告要件
- ソースコードエスクロー
- 現在利用中のベンダーに対するアセスメントツール
- サードパーティーへの依存
  - コード
  - ハードウェア
  - モジュール
- 技術的な検討事項
  - 技術的テスト
  - ネットワークセグメンテーション
  - 送信制御
  - 認証情報の共有

4.3 コンプライアンスのフレームワークと法的検討事項とそれらが組織に与える影響を説明することができる。

- 多様な業界の統合にまつわるセキュリティ上の懸念
- データの検討事項
  - データの主権
  - データの所有権
  - データ分類
  - データ保持
  - データの種類
    - 健全性
    - 金融
    - 知的財産
    - 個人を特定可能な情報（PII）
  - データの消去、破壊、およびサニタイズ
- 地理的な検討事項
  - データの所在地
  - データ主体の所在地
  - クラウドプロバイダーの所在地
- サードパーティーによるコンプライアンス認証
- 規制、認定、および標準
  - PCI DSS
  - 一般データ保護規則（GDPR）
  - 国際標準化機構（ISO）
  - 能力成熟度モデル統合（CMMI）
  - 国立標準技術研究所（NIST）
  - 児童オンラインプライバシー保護法（COPPA）
  - コモンクライテリア
  - Cloud Security Alliance（CSA）Security Trust Assurance and Risk（STAR）
- 法的検討事項
  - デューディリジェンス
  - デューケア
  - 輸出管理
  - 訴訟ホールド
  - Eーディスカバリ
- 契約書と合意書の種類
  - サービスレベル合意書（SLA）
  - マスターサービス契約書（MSA）
  - 秘密保持契約（NDA）
  - 覚書（MOU）
  - 相互接続セキュリティ協定（ISA）
  - 運用レベル合意書
  - プライバシーレベル合意書

4.4 事業継続性と災害復旧のコンセプトの重要性を説明することができる。

- ビジネス影響度分析
  - 目標復旧時点
  - 目標復旧時間
  - 復旧サービスレベル
  - 業務上不可欠な機能
- プライバシー影響評価
- 災害復旧計画（**DRP**）/事業継続計画（**BCP**）
  - コールドサイト
  - ウォームサイト
  - ホットサイト
  - モバイルサイト
- インシデント対応計画
  - 役割 / 職務
  - 対応報告
- テスト計画
  - チェックリスト
  - ウォークスルー
  - 机上演習
  - フルインタラプションテスト
  - パラレルテスト / シミュレーションテスト

CASP+(CAS-004) 略語リスト

下記は CompTIA CASP+ 認定資格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
2FA	Two-Factor Authentication
3DES	Triple Digital Encryption Standard
ACL	Access Control List
AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
ALE	Annualized Loss Expectancy
API	Application Programming Interface
APT	Advanced Persistent Threat
ARF	Asset Reporting Format
ARO	Annualized Rate of Occurrence
ASIC	Application Specific Integrated Circuit
ASLR	Address Space Layout Randomization
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
BCDR	Business Continuity and Disaster Recovery
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BIOS	Basic Input/Output System
BYOD	Bring Your Own Device
CA	Certificate Authority
CAN	Controller Area Network
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CCE	Common Configuration Enumeration
CI/CD	Continuous Integration/Continuous Delivery
CIP	Common Industrial Protocol
CMDB	Configuration Database Management
CMMI	Capability Maturity Model Integration
CN	Common Name
COPE	Corporate Owned, Personally Enabled
COPPA	Children's Online Privacy Protection Act
CPE	Common Platform Enumeration
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CSP	Cloud Service Provider

略語	詳細説明
CSR	Certificate Signing Request
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DLP	Data Loss Prevention
DNP3	Distributed Network Protocol 3
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
DoS	Denial of Service
DRM	Digital Rights Management
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
ECB	Electronic Codebook
ECDH	Elliptic-Curve Diffie-Hellman
ECDSA	Elliptic-Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
FIM	File Integrity Monitoring
FPGA	Field-Programmable Gate Array
FTK	Forensic Toolkit
GCM	Galois/Counter Mode
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hash-based Message Authentication Code
HOTP	HMAC-based One-Time Password
HSM	Hardware Security Module
HSTS	HTTP Strict Transport Security
HTML	Hypertext Markup Language

略語	詳細説明
HTTP	Hypertext Transfer Protocol
HUMINT	Human Intelligence
HVAC	Heating, Ventilation, and Air Conditioning
IaaS	Infrastructure as a Service
IAST	Interactive Application Security Testing
ICS	Industrial Control System
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISA	Interconnection Security Agreement
ISAC	Information Sharing Analysis Center
ISO	International Organization for Standardization
ISP	Internet Service Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
KVM	Keyboard, Video, and Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MD	Message Digest
MFA	Multifactor Authentication
MOU	Memorandum of Understanding
MSA	Master Service Agreement
MTBF	Mean Time Between Failure
MTTR	Mean Time to Recovery
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NFC	Near Field Communication
NGFW	Next Generation Firewall
NIC	Network Interface Controller
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
NX	No Execute
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OFB	Output Feedback
OS	Operating System
OSINT	Open-Source Intelligence
OTP	One-Time Password
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PBKDF2	Password-Based Key Derivation Function 2
PBX	Private Branch Exchange
PCAP	Packet Capture
PCI DSS	Payment Card Industry Data Security Standard
PGP	Pretty Good Privacy
PII	Personal Identifiable Information

略語	詳細説明
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSK	Pre-Shared Key
QoS	Quality of Service
RA	Registration Authority
RACE	Research and Development in Advanced Communications Technologies in Europe
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Inexpensive Disks
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RF	Radio Frequency
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RPO	Recovery Point Objective
RSA	Rivest, Shamir, and Adleman
RTO	Recovery Time Objective
RTU	Remote Terminal Unit
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAE	Simultaneous Authentication of Equals
SAML	Security Assertion Markup Language
SAN	Subject Alternate Name
SASE	Secure Access Service Edge
SAST	Static Application Security Testing
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SD-WAN	Software-Defined Wide Area Network
SEAndroid	Security Enhanced Android
SED	Self-Encrypting Drive
SELinux	Security Enhanced Linux
SFTP	SSH File Transfer Protocol
SHA	Secure Hashing Algorithm
SIEM	Security Information Event Management
SLA	Service-Level Agreement
SLE	Single Loss Expectancy
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, and Response
SoC	System-on-Chip
SPAN	Switched Port Analyzer
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
STAR	Security Trust Assurance and Risk
TACACS	Terminal Access Controller Access Control System

略語	詳細説明
TAP	Test Access Points
TCO	Total Cost of Ownership
TLS	Transport Layer Security
TOTP	Time-Based One-Time Password
TPM	Trusted Platform Module
UEBA	User and Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
UTM	Unified Threat Management
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNET	Virtual Network
VNET	Virtual Network
VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WPA	WiFi Protected Access
WS	Web Services
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language
XN	Execute Never
XSS	Cross-Site Scripting

CASP+ ハードウェアとソフトウェア一覧

本リストは、CASP+ 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

- ラップトップ
- 基本的なサーバーハードウェア（メールサーバー/アクティブディレクトリサーバー、信頼できる OS）
- トークン
- モバイル端末（Android および iOS）
- スイッチ（マネージドスイッチ）—IPv6 対応
- ゲートウェイ / ルーター—IPv6 対応（有線 / ワイヤレス）
- ファイアウォール
- VoIP
- プロキシサーバー
- ロードバランサー
- NIPS
- HSM
- アクセスポイント
- クリプトカード
- スマートカード
- スマートカードリーダー
- バイオメトリック機器
- アルデュイーノ（Arduino）/ラズベリーパイ（Raspberry Pi）
- SCADA システム：RTUとPLC

予備のハードウェア

- キーボード
- ケーブル
- NIC
- 電源
- リムーバブルメディア
- 高性能グラフィックスカード

ツール

- スペクトラムアナライザー
- アンテナ
- RF ハッキングハードウェア / SDR
- RSA トークン
- KVM スイッチ

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、RSA 認証、アスタリスクPBX）
- Windows
- Linux ディストリビューション
- VMware Player/VirtualBox
- 脆弱性アセスメントツール
- SSH および Telnet ユーティリティ
- 脅威モデリングツール
- IPS/IDS、HIPS
- WIPS
- フォレンジックツール
- 認証局
- Kali、すべての Kali ツールセット
- 改善用ソフトウェア
- GNS および関連ファームウェア
- ログ分析ツール
- API
- ELK Stack
- Graylog
- Python 3+
- Security Onionツール
- Metasploitable 2

その他

- サンプルログ
- ネットワークトラフィック（パケットキャプチャ）のサンプル
- 組織構造のサンプル
- ネットワーク文書のサンプル
- ブロードバンドインターネット接続
- 4G/5G、および/またはホットスポット
- コンピュータおよびモバイル周辺機器
- クラウドサービス
- Visio/Excel
- Open Office

CompTIA