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

試験番号：CAS-003

CompTIA

試験について

The CompTIA Advanced Security Practitioner (CASP) CAS-003認定資格は、上級レベルのセキュリティプロフェッショナルに求められるスキルを評価するグローバルなベンダーニュートラルの認定資格です。

- **レジリエント企業を支援するため、複雑な環境全般にわたってのセキュアソリューションの概念化、設計、統合および実行**
- **提案するセキュリティ方針の広範な範囲にわたるクリティカルシンキング/判断の適用、組織的ストラテジーの計画をたてる継続的なセキュリティソリューションの実行とサポート、ビジネス要件または規制要件とセキュリティ要件とのバランス、リスクによる影響の分析、セキュリティインシデントへの対応**

CASP認定資格は、以下のITセキュリティのプロフェッショナルを目安に設計されています。

- **IT管理分野で、少なくとも10年の実務経験（少なくとも5年の技術的セキュリティ実務経験を含む）**
- **次に挙げるのは、推奨される資格要件です：CompTIA Network+、 Security+、 CySA+ 認定資格、または同等の知識**

認定資格試験の認証

CASP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。

試験の開発

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や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の担当窓口（examsecurity@comptia.org）ま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は、すべての試験内容を網羅するものではありません。本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。

**ベンダーの特定ツールおよび技術に関する基本的な知識はCASP認定資格試験に必要であるため、受験の際には、それらの知識を持っていなければなりません。CASP試験の準備用として、CompTIAは本文書の最後にサンプル用のハードウェアおよびソフトウェアのリストを掲載しています。このリストはトレーニング企業にも役立つと考えられます。

試験情報

試験	CAS-003
問題数	最大90問
出題形式	単一/複数選択、シミュレーション
試験時間	165分
推奨経験	IT管理分野での経験が10年あり、少なくとも 5年の実地での技術セキュリティ経験を含む
合格スコア	合格／不合格の記載のみ（得点表記はなし）

出題範囲（試験分野）

下記の表は、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 リスクマネジメント	19%
2.0 エンタープライズ・セキュリティ・アーキテクチャ	25%
3.0 エンタープライズ・セキュリティ・オペレーション	20%
4.0 エンタープライズ・セキュリティにおける技術統合	23%
5.0 調査、開発およびコラボレーション	13%
計	**100%**

1.0 リスクマネジメント

1.1 ビジネスおよび業界の影響やそれに関連するセキュリティリスクの概要を要約することができる。

- **新製品のリスクマネジメント、新技術およびユーザーの行動**
- **新規ビジネスまたは変化中のビジネスモデル／戦略**
  - パートナーシップ
  - アウトソーシング
  - クラウド
  - 買収／合併ー事業の売却／分割
    - データの所有権
    - データの再分類
- **統合におけるセキュリティの懸念点多様な業界**
  - ルール
  - ポリシー
  - 規制
    - 輸出管理
    - 法的要件
  - 地理
    - データの主権性
    - 管轄区域
- **内的および外的影響力**
  - 競合相手
  - 監査役／監査指摘事項
  - 監督機関
  - 内部および外部クライアントの要件
  - 最高レベルの管理
- **脱境界化 (de-perimeterization)の影響（例ネットワークの境界が絶えず変化していること）**
  - 在宅勤務
  - クラウド
  - モバイル
  - BYOD
  - アウトソーシング
  - 情報セキュリティに不可欠なレベルを有するサードパーティプロバイダの確保

1.2 組織の要件に基づくセキュリティ、プライバシーポリシー、手順を比較対照することができる。

- **ポリシーおよびプロセスのライフサイクルマネジメント**
  - 新規ビジネス
  - 新技術
  - 環境の変化
  - 規制要件
  - 発生リスク
- **人事、法務、管理および他の組織との協力による法的コンプライアンスおよび擁護の支援**
- **共通するビジネス文書を理解しセキュリティを支援**
  - リスクアセスメント (RA)
  - ビジネス影響度分析 (BIA)
  - 相互運用性協定 (Interoperability agreement:IA)
  - 相互接続セキュリティ協定 (ISA)
  - 覚書 (MOU)
  - サービスレベル合意書 (SLA)
  - 運用レベル合意書 (OLA)
  - 秘密保持契約書 (NDA)
  - ビジネスパートナー契約書 (BPA)
  - マスターサービス契約書（基本契約書、MSA）
- **契約書に関するセキュリティ要件の調査**
  - 提案依頼書 (RFP)
  - 見積依頼書 (RFQ)
  - 情報提供依頼書 (RFI)
- **機密情報に関する一般的なプライバシー原則の理解**
- **ポリシー開発の支援標準となるセキュリティ対策を含む**
  - 職務分離
  - ジョブローテーション
  - 強制的な休暇
  - 最小の権限
  - インシデント対応
  - フォレンジックな職務
  - 雇用及び契約終了手順
  - 継続的モニタリング
  - ユーザー向け研修及び意識の向上
  - 会計監査要件および実施頻度
  - 情報の分類

1.3 与えられたシナリオに基づいて、リスク緩和戦略とこれらを実行することができる。

- **CIAを基準とした影響レベルによるデータ種類の分類**
- **CIAの影響レベルの決定にステークホルダーからの情報を統合**
- **総スコアを基準とした最低限必要なセキュリティ管理のコントロール**
- **CIA要件および組織的ポリシーを基準としたコントロールの選択と実行**
- **極端な設定の想定/最悪ケースの設定**
- **システム特有のリスク分析の実行**
- **既知の測定項目を基準としたリスク判断の実行**
  - ALEおよびSLEを基準とした影響の大きさ
  - 身近に存在する脅威
    - モチベーション
    - ソース
  - ARO
  - 動向分析
  - 投資利益率 (ROI)
  - 所有にかかる総コスト
- **取引条件における技術的リスクの移転**
- **リスク選好に基づく適用すべき戦略の推薦**
  - 回避
  - 移転
  - 低減
  - 受容
- **リスクマネジメントの過程**
  - 適用の除外
  - 抑止
    - 固有性
    - 余剰分
- **継続的な向上／継続的なモニタリング**
- **事業継続計画**
  - RTO
  - RPO
  - MTTR
  - MTBF
- **ITガバナンス**
  - リスクに対するこだわりフレームワークの管理
- **企業のレジリエンス**

1.4 リスクの測定項目設定を分析し、企業のセキュリティ保護を実施することができる。

- **現行のセキュリティコントロールの影響度調査**
  - ギャップ分析
  - 教訓の管理
  - 対応報告
- **現行のソリューションを解析調査または脱構築する**
- **測定項目の作成、収集および分析**
  - KPI
  - KRI
- **複数のソリューションのひな型を作り、テストを行う**
- **ベンチマークの作成およびベースラインとの比較**
- **トレンドデータを分析・解明しサイバー保護のニーズを事前に予想する**
- **セキュリティソリューションにおける測定項目および計数値を分析し、ビジネスにおけるニーズにあっているかどうかを確認する**
  - パフォーマンス
  - 待ち時間
  - 拡張性
  - 将来性
  - 有用性
  - 保全性
  - 可用性
  - 修復性
  - ROI
  - TCO
- **大半のセキュアソリューションが利用できない場合、判断力を用いて問題を解決する**

2.0 エンタープライズ・セキュリティ・アーキテクチャ

2.1 設定を分析し、セキュリティ要件に合うようにネットワークやセキュリティ要素、コンセプトやアーキテクチャを導入することができる。

- **物理的および仮想的ネットワークおよびセキュリティ機器**
  - UTM
  - IDS/IPS
  - NIDS/NIPS
  - INE
  - NAC
  - SIEM
  - スイッチ
  - ファイアウォール
  - ワイヤレスコントローラ
  - ルータ
  - プロキシ
  - ロードバランサー
  - HSM
  - MicroSD HSM
- **アプリケーションおよびプロトコルアウェア技術**
  - WAF
  - ファイアウォール
  - パッシブ脆弱性検知ツール
  - DAM
- **上級ネットワーク設計（有線／無線）**
  - リモートアクセス
    - VPN
      - IPSec
      - SSL/TLS
    - SSH
    - RDP
    - VNC
    - VDI
    - リバースプロキシ
  - IPv4およびIPv6の移行技術
  - ネットワークの認証方法
  - 802.1x
  - メッシュネットワーク
  - 固定端末／モバイル端末の設置
  - ハードウェア及びアプリケーションの設置
- **データフロー向けの複雑なネットワークセキュリティソリューション**
  - DLP
  - ディープ・パケット・インスペクション
  - データフローの実施
  - ネットワークフロー（S/フロー）
  - データフロー図
- **ネットワークおよびセキュリティ要素のセキュリティ構成および基準位置の決定**
- **ソフトウェア定義ネットワーク**
- **ネットワーク管理 およびモニタリングツール**
  - 警告の定義およびルールの記載
  - 警告閾値の調整
  - 疲労の警告
- **ルータ、スイッチ、他のネットワーク機器の上級設定**
  - トランスポートセキュリティ
  - トランキングセキュリティ
  - ポートセキュリティ
  - ルートの保護
  - DDoSからの保護
  - ブラックホールの遠隔作動
- **セキュリティゾーン**
  - DMZ
  - 重要アセットの分離
  - ネットワーク・セグメンテーション
- **ネットワーク・アクセスコントロール**
  - 隔離／修復
  - 永続性／抑止または一時的なエージェント
  - エージェント型とエージェントレス型の違い
- **ネットワーク対応機器**
  - システム・オン・チップ (SoC)
  - 建物または家における自動システム
  - IPビデオ
  - HVACコントローラ
  - センサー
  - 制御システムへの物理的アクセス
  - A/Vシステム
  - 科学的／産業的装置
- **重要なインフラストラクチャ**
  - 監視制御およびデータ取得 (SCADA)
  - 産業用制御システム (ICS)

2.2 設定の分析、セキュリティ要件に合うようにホストデバイスにセキュリティ管理策を導入することができる。

- **トラステッドOS（Trusted OS、例：どのように、いつそれを使用するか）**
  - SELinux
  - SEAndroid
  - TrustedSolaris
  - 最少機能
- **エンドポイントのセキュリティソフトウェア**
  - アンチマルウェア
  - アンチウイルス
  - アンチスパイウェア
  - スパムフィルタ
  - パッチ管理
  - HIPS/HIDS
  - データ損失の防止
  - ホストベースのファイアウォール
  - ログのモニタリング
  - エンドポイントの検出応答(EDR)
- **ホストの強化**
  - 標準の動作環境／基準値設定
    - アプリケーションのホワイトリスト化およびブラックリスト化
  - セキュリティ／グループポリシーの実装
  - コマンドシェルの制限
  - パッチ管理
    - マニュアル
    - 自動化
      - スクリプトの記述とレプリケーション
  - 専用インタフェースの設定
    - アウトオブバンド管理
    - ACL
    - 管理インタフェース
    - データインタフェース
  - 外部I/Oの制限
    - USB
    - 無線
      - Bluetooth
      - NFC
      - IrDA
      - RF
      - 802.11
      - RFID
    - ドライブのマウント
    - ドライブのマッピング
    - ウェブカメラ
    - 録音用マイク
    - オーディオ出力
    - SD用ポート
    - HDMI用ポート
  - ファイルおよびディスクの暗号化
  - ファームウェアの更新
- **ブートローダの保護**
  - セキュアブート
  - 計測済みのローンチ
  - 完全性計測アーキテクチャ(IMA)
  - BIOS/UEFI
  - 認証サービス
  - TPM
- **ハードウェアに関連する脆弱性**
- **ターミナルサービス／アプリケーション デリバリーサービス**

2.3 設定の分析、セキュリティ要件に合うモバイル・デバイスやスモール・フォームファクタ・デバイス向けセキュリティ管理策を導入することができる。

- **エンタープライズモビリティ・マネジメント**
  - コンテナ化
  - プロファイルおよびペイロードの構成
  - 個人所有、会社での利用可能
  - アプリケーション・ラッピング
  - リモートアシスタンスのアクセス
    - VNC
    - スクリーンミラーリング
  - アプリケーション、コンテンツおよびデータ管理
  - 無線アップデート（ソフトウェア／ファームウェア）
  - リモートワイピング（遠隔消去）
  - SCEP
  - BYOD
  - COPE
  - VPN
  - アプリケーションの許可
  - サイドローディング
  - 署名なしアプリ／システムアプリ
  - コンテキストを意識したマネジメント
    - ジオロケーション／ジオフェンシング
    - ユーザ行動
    - セキュリティ制限
    - 時間基準の制限
- **セキュリティ実装／プライバシーの懸念事項**
  - データストレージ
    - 移動不可のストレージ
    - 移動可能なストレージ
    - クラウドストレージ
    - 制御不可能なストレージへのデータの移動／データのバックアップ
    - USB OTG
  - 機器の損失／盗難
  - ハードウェアのアンチタンパー
    - eFuse
  - TPM
  - rooting化／ジェイルブレイク
  - プッシュ通知サービス
  - ジオタギング
  - 暗号化済インスタントメッセージアプリ
  - トークナイゼーション
  - OEM/キャリアのAndroidフラグメンテーション
  - モバイル端末での支払い
    - NFCの利用が可能
    - インダクタンスの利用が可能
    - モバイルウォレット
    - 周辺装置で利用可能な支払い方法（クレジットカード読み取り機）
  - テザリング
    - USB
    - スペクトラムマネジメント
    - Bluetooth 3.0と4.1の違い
  - 認証
    - スワイプパターン
    - ジェスチャー
    - PINコード
    - バイオメトリック
      - 顔認証
      - 指紋
      - 虹彩認証
  - マルウェア
  - 不正なドメインブリッジング
  - ベースバンド無線／SOC
  - 拡張現実
  - SMS/MMS/メッセージング
- **ウェアラブル技術**
  - 機器
    - カメラ
    - 時計
    - フィットネス機器
    - メガネ
    - 医療用センサ／機器
    - ヘッドセット
  - セキュリティ関連事項
    - 不正なリモートアクティベーション／機器または機能の非アクティベーション
    - 暗号化および未暗号化通信の懸念
    - 物理的調査
    - 個人情報の盗難
    - 健康に関するプライバシー
    - 収集データのデジタル・フォレンジック

2.4 与えられたソフトウェア脆弱性に関するシナリオに基づき、適切なセキュリティ管理策を選択することができる。

- **アプリケーションセキュリティの設計検討**
  - セキュリティ保護：設計、規定値、配置による安全性
- **特定のアプリケーションに関する問題**
  - 安全でない直接オブジェクト参照
  - XSS
  - クロスサイトリクエストフォージェリ (CSRF)
  - クリックジャック攻撃
  - セッション管理
  - 入力の確認
  - SQLインジェクション
  - 不正なエラーおよび例外ハンドリング
  - 特権エスカレーション
  - 機微データの不正ストレージ
  - ファジング／フォールトインジェクション
  - 安全なcookieのストレージおよび送信
  - バッファオーバーフロー
  - メモリーリーク
  - 整数オーバーフロー
  - 競合状態
    - チェックの時間
    - 使用時間
  - リソース枯渇
  - ジオタギング
  - データの残り
  - サードパーティのライブラリの使用
  - コードの再利用
- **アプリケーションのサンドボックス**
- **暗号化済エンクレーブのセキュリティ保護**
- **データベースの動作モニタ**
- **ウェブ用アプリケーションのファイアウォール**
- **クライアント側処理とサーバ側処理**
  - JSON/REST
  - ブラウザの拡張
    - ActiveX
    - Javaアプレット
  - HTML5
  - AJAX
  - SOAP
  - 状態管理
  - Javaスクリプト
- **OSの脆弱性**
- **ファームウェアの脆弱性**

3.0 エンタープライズ・セキュリティ・アーキテクチャ

3.1 与えられたシナリオに基づき、適切な方法を使用したセキュリティ状態の評価を実施することができる。

- **方式**
  - マルウェア用サンドボックス
  - メモリダンピング、ランタイムデバッグ
  - 偵察
  - フィンガープリンティング
  - コードの参照
  - ソーシャルエンジニアリング
  - ピボッティング
  - オープン・ソース・インテリジェンス
    - ソーシャルメディア
    - Whois
    - ルーティングテーブル
    - DNSの記録
    - サーチエンジン
- **種類**
  - ペネトレーションテスト
    - ブラックボックス
    - ホワイトボックス
    - グレーボックス
  - 脆弱性アセスメント
    - セルフアセスメント
      - 机上演習
  - 社内監査および社外監査
  - カラーチーム訓練
    - レッド・チーム
    - ブルー・チーム
    - ホワイト・チーム

3.2 設定や調査結果に基づき、セキュリティアセスメントのために適切な手段を選択することができる。

- **ネットワークツールの種類**
  - ポートスキャナ
  - 脆弱性検査ツール
  - プロトコルアナライザ
    - 有線
    - 無線
  - SCAPスキャナ
  - ネットワークの定数
  - ファザー
  - HTTPインターセプタ
  - エクスプロイテーションツール／フレームワーク
  - 可視化ツール
  - ログの減少および分析ツール
- **ホスト用ツールの種類**
  - パスワードクラッカー
  - 脆弱性検査ツール
  - コマンドラインツール
  - ローカルのエクスプロイテーションツール／フレームワーク
  - SCAPツール
  - ファイル完全性のモニタリング
  - ログ分析ツール
  - アンチウイルス
  - リバースエンジニアリング用ツール
- **物理的セキュリティツール**
  - ピッキング行為
  - RFIDツール
  - IRカメラ

3.3 与えられたシナリオに基づいて、インシデント対応および復帰手順を実行することができる。

- **E-ディスカバリ**
  - 電気的な在庫管理およびアセットのコントロール
  - データ保持ポリシー
  - データリカバリおよびストレージ
  - データの所有権
  - データハンドリング
  - 訴訟ホールド
- **情報漏洩**
  - 検出と収集
    - データアナリティクス
  - 低減
    - 最小化
    - 隔離
  - リカバリ／復元
  - 対応
  - 開示
- **インシデント検出および対応の促進**
  - チーミングの検索
  - ヒューリスティック分析／ビヘイビア分析
  - システム、監査、およびセキュリティログの構築および確認
- **インシデントおよび緊急事態への対応**
  - 証拠の連鎖
  - セキュリティを侵害されたシステムのフォレンジック分析
  - オペレーションの継続
  - ディザスタリカバリ
  - インシデント対応チーム
  - データ移動順序
- **インシデント対応サポートツール**
  - dd
  - tcpdump
  - nbtstat
  - netstat
  - nc (Netcat)
  - memdump
  - tshark
  - foremost
- **インシデントまたは漏洩の重大度**
  - 範囲
  - インパクト
  - 費用
  - ダウンタイム
  - 法律上の問題
- **インシデント対応後**
  - 根本起因解析
  - 教訓の管理
  - 対応報告後

4.0 エンタープライズ・セキュリティにおける技術統合

4.1 与えられたシナリオに基づいて、ホスト、ストレージ、ネットワークやアプリケーションをエンタープライズアーキテクチャにセキュアに統合することができる。

- **データフロー・セキュリティを変化するビジネスのニーズに合わせるために適用**
- **標準**
  - オープン標準
  - 標準の順守
  - 競合する標準
  - 標準の欠如
  - デファクトスタンダード
- **相互運用性の問題点**
  - レガシーシステムおよびソフトウェア／現在のシステム
  - アプリケーション要件
  - ソフトウェアの種類
    - 自社開発
    - コマーシャル
    - 特製コマーシャル
    - オープンソース
  - 標準データのフォーマット
  - プロトコルおよびAPI
- **レジリエンスの問題点**
  - 異機種環境のコンポーネントの使用
  - 行動指針オートメーション／オーケストレーション
  - 重要アセットの分配
  - データの永続性および非永続性
  - 冗長性／高可用性
  - 想定される攻撃の可能性
- **データセキュリティの考慮**
  - データの残り
  - データ集約
  - データの分離
  - データの所有権
  - データの主権性
  - データ量
- **リソースプロビジョニングおよびデプロビジョニング**
  - ユーザー
  - サーバー
  - バーチャル機器
  - アプリケーション
  - データの残り
- **合併、買収、会社分割／売却中の設計の検討**
- **ネットワークの安全なセグメンテーションと委託**
- **該当端末全ての論理的配置図および対応する物理的配置図**
- **ストレージ統合のセキュリティおよびプライバシーの考慮**
- **統合エンタープライズ・アプリケーションのセキュリティ関連事項**
  - CRM
  - ERP
  - CMDB
  - CMS
  - 統合イネーブラ
    - ディレクトリサービス
    - DNS
    - SOA
    - ESB

4.2 与えられたシナリオに基づいて、クラウドや仮想化技術をエンタープライズアーキテクチャにセキュアに統合することができる。

- **技術的デプロイメントモデル（アウトソーシング／インソーシング マネージドサービス／パートナーシップ）**
  - クラウドおよび仮想化の検討およびホスティングのオプション
    - パブリック
    - プライベート
    - ハイブリッド
    - コミュニティ
    - マルチテナント
    - シングルテナント
  - オンプレミスとホステッドとの違い
  - クラウドサービスのモデル
    - SaaS
    - IaaS
    - PaaS
- **仮想化におけるセキュリティ上の長所および短所**
  - 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
  - 基準とするコンテナ
  - vTPM
  - ハイパーコンバージドインフラストラクチャ
  - 仮想デスクトップインフラストラクチャ
  - セキュリティエンクレーブおよび量
- **クラウド拡張型セキュリティサービス**
  - アンチマルウェア
  - 脆弱性検査
  - サンドボックス
  - コンテンツのフィルタリング
  - クラウドセキュリティブローカー
  - Security as a service（サービスとしてのセキュリティ）
  - マネージドセキュリティサービスのプロバイダ
- **異なるセキュリティ要件に基づくホストの混合に関連する脆弱性**
  - VMエスケープ
  - 特権の昇格
  - ライブVMマイグレーション
  - データの残り
- **データセキュリティの考慮**
  - 複数のデータの種類をホスティングする単独サーバに関連する脆弱性
  - 複数の仮想マシン上で複数のデータの種類／所有者をホスティングする単独プラットフォームに関連する脆弱性
- **リソースプロビジョニングおよびデプロビジョニング**
  - バーチャル機器
  - データの残り

4.3 与えられたシナリオに基づいて、エンタープライズセキュリティの目的に沿うように高度な認証認可のテクノロジーを導入、トラブルシューティングすることができる。

- **認証**
  - 証明書ベースの認証
  - シングルサインオン
  - 802.1x
  - コンテキストアウェア認証
  - プッシュ型認証
- **認可**
  - OAuth
  - XACML
  - SPML
- **証明**
- **アイデンティティ・プルーフィング**
- **アイデンティティ・プロパゲーション**
- **フェデレーション**
  - SAML
  - OpenID
  - Shibboleth
  - WAYF
- **信頼モデル**
  - RADIUS設定
  - LDAP
  - AD

4.4 与えられたシナリオに基づいて、暗号化テクノロジーを実装することができる。

- **技術**
  - 鍵ストレッチング
  - ハッシュ化
  - デジタル署名
  - メッセージ認証
  - コード署名
  - 疑似乱数の生成
  - 完全前方秘匿性 (PFS)
  - データ通信中の暗号化
  - インメモリデータ／データ処理
  - 保存データの暗号化
    - ディスク
    - ブロック
    - ファイル
    - 記録
  - ステガノグラフィー
- **実装**
  - 暗号モジュール
  - 暗号プロセッサ
  - 暗号サービスプロバイダ
  - DRM
  - 電子透かし
  - GPG
  - SSL/TLS
  - SSH
  - S/MIME
  - 暗号アプリケーションおよび適切／不適切な実装
    - 強度
    - パフォーマンス
    - 実装の実現可能性
    - 相互運用性
  - ストリームとブロック
  - PKI
    - ワイルドカード
    - OCSPとCRL
    - エンティティの発行
    - キーエスクロー
    - 証明書
    - トークン
    - ステープリング
    - ピンニング
  - 暗号通貨／ブロックチェイン
  - モバイル機器の暗号化 検討
  - 楕円曲線暗号
    - P-256とP-384とP521

4.5 与えられたシナリオに基づいて、セキュアなコミュニケーションやコラボレーションソリューションを導入するための適切な保護策を選択することができる。

- **リモートアクセス**
  - リソースおよびサービス
  - デスクトップおよびアプリケーションの共有
  - リモートアシスタンス
- **一体型コラボレーションツール**
  - カンファレンス
    - ウェブ
    - ビデオ
    - オーディオ
  - ストレージおよび文書コラボレーションツール
  - 一体型コミュニケーション
  - インスタントメッセージ
  - プレゼンス
  - Eメール
  - テレフォニーおよびVoIPの統合
  - コラボレーションサイト
    - ソーシャルメディア
    - クラウドベース

5.0 調査、開発およびコラボレーション

5.1 与えられたシナリオに基づいて、業界のトレンドや企業へのインパクトを実施し、適切な調査手法を用いることができる。

- **進行中調査の実施**
  - ベストプラクティス
  - 新技術、セキュリティシステムおよびサービス
  - テクノロジーの進歩（例、RFC、ISO）
- **脅威インテリジェンス**
  - 最新の攻撃
  - 現在の脆弱性および脅威の知識
  - ゼロデイ脆弱性に対するミティゲーション制御および改善
  - 脅威モデル
- **ビジネスツールから発生するセキュリティ関連事項を調査**
  - ソーシャルメディアプラットフォームの進歩
  - ビジネス内での統合
  - ビッグデータ
  - AI／機械学習
- **世界規模でのIA業界／コミュニティ**
  - コンピュータ緊急時対応チーム（CERT）
  - コンベンション／カンファレンス
  - リサーチコンサルタント／ベンダー
  - アクターによるアクティビティの脅威
  - 脅威源の発生

5.2 与えられたシナリオに基づいて、技術的なライフサイクル全体にわたる、セキュリティ保護活動を実行することができる。

- **システムの開発ライフサイクル**
  - 要件
  - 取得
  - テストおよび評価
  - コミッショニング／デコミッショニング
  - 動作上のアクティビティ
    - モニタリング
    - メインテナンス
    - 設定および管理の変更
  - アセット・ディスポーザル
  - アセット／オブジェクトの再利用
- **ソフトウェアの開発ライフサイクル**
  - アプリケーションのセキュリティフレームワーク
  - ソフトウェア・アシュアランス
    - 標準ライブラリ
    - 業界で受容されているアプローチ
    - ウェブサービスのセキュリティ（WSセキュリティ）
    - 禁止されたコーディング技術
    - NX/XNビットの使用
    - ASLRの使用
    - コードの質
    - コードアナライザー
      - ファザー
      - 静的
      - 動的
  - 開発アプローチ
    - DevOps
    - セキュリティ関連事項アジャイル型、ウォーターフォール型およびスパイラル型ソフトウェア開発方法論
    - 継続的インテグレーション
    - バージョニング
  - セキュアコーディング標準
  - ドキュメンテーション
    - セキュリティ要件トレーサビリティ・マトリクス（SRTM）
    - 要件の定義
    - システム設計文書
    - テスト計画
  - バリデーションおよび受け入れテスト
    - レグレッション
    - ユーザー受け入れテスト
    - ユニットのテスト
    - 結合テスト
    - ピアレビュー
- **対処するソリューションを適応：**
  - 脅威の発生
  - 破壊的技術
  - セキュリティのトレンド
- **アセットマネジメント（在庫管理のコントロール）**

5.3 セキュリティ目標を達成する多種多様なビジネスユニットとの相互作用の重要性に関する説明をすることができる。

- **他の方針由来のステークホルダーとの通信を行うためのセキュリティ要件および目標の解釈**
  - セールス・スタッフ
  - プログラマー
  - データベース管理者
  - ネットワーク管理者
  - マネジメント／経営管理
  - 財務
  - 人事
  - 緊急時対応チーム
  - ファシリティ・マネージャ
  - フィジカルセキュリティ・マネージャ
  - 法律顧問
- **セキュリティプロセスおよびコントロールに関するスタッフおよび経営陣への公平な推奨および客観的なガイダンスの提供**
- **チーム内でのセキュアソリューションの実行を行う効果的なコラボレーションの構築**
- **ガバナンス、リスクおよびコンプライアンス委員会**

CASP略語一覧

下記は、CASP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こに挙げた略語全てを復習し、理解することをお勧めします。

略語	詳細説明
2FA	Two-Factor Authentication
3DES	Triple Digital Encryption Standard
AAA	Authentication, Authorization and Accounting
AAR	After Action Report
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
AH	Authentication Header
AJAX	Asynchronous JavaScript and XML
ALE	Annualized Loss Expectancy
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
AUP	Acceptable Use Policy
AV	Antivirus
B2B	Business-to-Business
BCP	Business Continuity Planning
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partnership Agreement
BPM	Business Process Management
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CASB	Cloud Access Security Broker
CBC	Cipher Block Chaining
CCMP	Counter-Mode/CBC-Mac Protocol
CCTV	Closed-Circuit Television
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
CHAP	Challenge Handshake Authentication Protocol

略語	詳細説明
CIA	Confidentiality, Integrity and Availability
CIFS	Common Internet File System
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CLI	Command Line Interface
CMDB	Configuration Management Database
CMS	Content Management System
COOP	Continuity of Operations
COPE	Corporate Owned, Personally Enabled
COTS	Commercial Off-the-Shelf
CRC	Cyclical Redundancy Check
CredSSP	Credential Security Support Provider
CRL	Certification Revocation List
CRM	Customer Resource Management
CSP	Cloud Service Provider
CSP	Cryptographic Service Provider
CSRF	Cross-Site Request Forgery
CTR	Counter Mode
CVE	Collaborative Virtual Environment
CYOD	Choose Your Own Device
DAC	Discretionary Access Control
DAM	Database Activity Monitoring
DAR	Data at Rest
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DKIM	Domain Keys Identified Mail
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOM	Document Object Model
DoS	Denial of Service
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm

略語	詳細説明
EAP	Extensible Authentication Protocol
ECB	Event Control Block
ECC	Elliptic Curve Cryptography
EDR	Endpoint Detection Response
EFS	Encrypted File System
EMI	Electromagnetic Interference
ERP	Enterprise Resource Planning
ESA	Enterprise Security Architecture
ESB	Enterprise Service Bus
ESP	Encapsulated Security Payload
EV	Extended Validation (Certificate)
FDE	Full Disk Encryption
FIM	File Integrity Monitoring
FTP	File Transfer Protocol
GPG	GNU Privacy Guard
GPO	Group Policy Object
GPU	Graphic Processing Unit
GRC	Governance, Risk and Compliance
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HDD	Hard Disk Drive
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMAC	Hashed Message Authentication Code
HOTP	HMAC-based One-Time Password
HSM	Hardware Security Module
HSTS	HTTP Strict Transport Security
HVAC	Heating, Ventilation and Air Conditioning
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDE	Integrated Development Environment
IdM	Identity Management
IdP	Identity Provider
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IM	Instant Messaging
IMAP	Internet Message Access Protocol
INE	Inline Network Encryptor
IOC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPMI	Internet Protocol Multicast Initiative
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security

略語	詳細説明
IR	Incident Response
IRC	Internet Relay Chat
IS-IS	Intermediate System to Intermediate System
ISA	Interconnection Security Agreement
ISAC	Information Sharing Analysis Center
ISMS	Information Security Management System
ISP	Internet Service Provider
IV	Initialization Vector
JSON	JavaScript Object Notation
KDC	Key Distribution Center
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
LTE	Long-Term Evolution
LUN	Logical Unit Number
MAC	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MD5	Message Digest 5
MDM	Mobile Device Management
MEAP	Mobile Enterprise Application Platform
MFA	Multifactor Authentication
MFD	Multifunction Device
MITM	Man in the Middle
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MSA	Master Service Agreement
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSS	Managed Security Service
MSSP	Managed Security Service Provider
MTA	Message Transfer Agent
MTBF	Mean Time Between Failure
MTD	Maximum Tolerable Downtime
MTP	Media Transfer Protocol
MTTR	Mean Time to Recovery
MTU	Maximum Transmission Unit
NAC	Network Access Control

略語	詳細説明
NAS	Network Attached Storage
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NFC	Near Field Communication
NFS	Network File System
NGFW	Next Generation Firewall
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
NLA	Network-Level Authentication
NOS	Network Operating System
NSP	Network Service Provider
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OLA	Operating-Level Agreement
OOB	Out-of-Band
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTP	One-Time Password
OVAL	Open Vulnerability Assessment Language
OWASP	Open Web Application Security Project
P2P	Peer-to-Peer
PaaS	Platform as a Service
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBKDF2	Password-Based Key Derivation Function 2
PBX	Private Branch Exchange
PCI-DSS	Payment Card Industry Data Security Standard
PDP	Policy Distribution Point
PEAP	Protected Extensible Authentication Protocol
PEP	Policy Enforcement Point
PFS	Perfect Forward Secrecy
PGP	Pretty Good Privacy
PII	Personal Identifiable Information
PIP	Policy Information Point
PIR	Post Incident Report
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
POC	Proof of Concept
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-Shared Key
QA	Quality Assurance

略語	詳細説明
QoS	Quality of Service
R&D	Research and Development
RA	Recovery Agent
RA	Registration Authority
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Inexpensive/Independent Disks
RAS	Remote Access Server
RBAC	Role-Based Access Control
RBAC	Rule-Based Access Control
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFC	Request for Comments
RFI	Request for Information
RFID	Radio Frequency Identification
RFP	Request for Proposal
RFQ	Request for Quote
ROI	Return on Investment
RPO	Recovery Point Objective
RSA	Rivest, Shamir and Adleman
RTBH	Remotely Triggered Black Hole
RTO	Recovery Time Objective
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SAN	Subject Alternative Name
SAN	Storage Area Network
SAS	Statement on Auditing Standards
SATCOM	Satellite Communications
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy
SCSI	Small Computer System Interface
SDL	Security Development Life Cycle
SDLC	Software Development Life Cycle
SED	Self-Encrypting Drive
SELinux	Security Enhanced Linux
SFTP	Secure File Transfer Protocol
SHA	Secure Hashing Algorithm
SIEM	Security Information Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service-Level Agreement
SLE	Single Loss Expectancy
SMB	Server Message Block
SMS	Short Message Service

略語	詳細説明
SMTP	Simple Mail Transfer Protocol
SNAT	Source Network Address Translation
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOA	Start of Authority
SOA	Statement of Applicability
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
SOC	Service Organization Controls
SOE	Standard Operating Environment
SOP	Standard Operating Procedure
SOW	Statement of Work
SOX	Sarbanes-Oxley Act of 2002
SP	Service Provider
SPIM	Spam over Internet Messaging
SPML	Service Provisioning Markup Language
SRTM	Security Requirements Traceability Matrix
SRTP	Secure Real-Time Protocol
SRV	Service Records
SSD	Solid State Drive
SSDLC	Security System Development Life Cycle
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
SSP	Storage Service Provider
TACACS	Terminal Access Controller Access Control System
TCO	Total Cost of Ownership
TCP/IP	Transmission Control Protocol/Internet Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOC/TOU	Time of Check/Time of Use
TOS	Type of Service
TOTP	Time-based One-Time Password
TPM	Trusted Platform Module
TSIG	Transaction Signature Interoperability Group
TTR	Time to Restore
UAC	User Access Control
UAT	User Acceptance Testing
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UPS	Uninterruptable Power Supply
URL	Universal Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMFS	VMware File System
VNC	Virtual Network Connection
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
vSAN	Virtual Storage Area Network
VTC	Video Teleconferencing
vTPM	Virtual Trusted Platform Module
WAF	Web Application Firewall
WAP	Wireless Access Point
WAYF	Where Are You From
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WMI	Windows Management Interface
WPA	Wireless Protected Access
WRT	Work Recovery Time
WSDL	Web Services Description Language
XACML	eXtensible Access Control Markup Language
XHR	XMLHttpRequest
XMPP	eXtensible Messaging and Presence Protocol
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デモ、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も役立ちます。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
- ノート型パソコン
- 基本的なサーバのハードウェア（Eメール用サーバ／アクティブディレクトリサーバ、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）ーIPv6利用可能
- ルーターIPv6利用可能（有線／ワイヤレス）
- ゲートウェイ
- 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端末

予備のハードウェア
- キーボード
- ケーブル
- NIC
- 電源
- 外部USBフラッシュドライブ

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

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／仮想ボックス
- 脆弱性アセスメントツール
- SSHおよびTelnetユーティリティ
- モデリングツールの脅威
- ホストIPS
- Helixソフトウェア
- KaliおよびKaliのすべてのツールセット
- 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

その他
- サンプルログ
- サンプルネットワーク・トラフィック（パケットキャプチャ）
- 組織構造のサンプル
- サンプルネットワーク文書
- ブロードバンドインターネット接続
- 3G／4G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

CompTIA