CompTIA Security+認定資格試験出題範囲

試験番号：SY0-401

はじめに

CompTIA Security+は、ベンダーニュートラルの認定資格です。Security+認定は、基本レベルのセキュリティスキルおよび知識を判断する、国際的に認められた認定試験で、世界中の企業およびセキュリティプロフェッショナルに活用されています。

CompTIA Security+ 認定資格試験は、試験対象者がリスクの確認、リスク軽減の実践、インフラの整備、アプリケーション、運用、情報セキュリティ、機密情報保持のためのセキュリティコントロールの適用、整合性、有効性、適切な技術と製品の確認、適切なセキュリティポリシーの確認と運用、法律、各種の規制に関する、必要な知識とスキルを評価する認定資格試験です。

CompTIA Security+認定資格試験は、以下の条件を満たすITセキュリティプロフェッショナルを対象としています。
－セキュリティ関連のネットワーク管理における最低2年間の業務経験
－日常的な技術情報セキュリティにおける経験
－下記の試験分野に挙げられた項目を含む、セキュリティ上の問題や実装に関する幅広い知識

CompTIA Security+は、ISO 17024より認定（Personnel Certification Accreditation）を受けており、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。
CompTIA Security+認定資格試験で評価されるスキルおよび知識は、サブジェクト・マター・エキスパートのワークショップおよび2年程度の経験のある情報セキュリティエンジニアに求められる知識とスキルに関する業界の調査結果の内容を反映しています。
この調査の結果を基に、出題分野の内容および全体に対する出題比率を検討し、内容の相対的な重要性の裏付けをしています。

この出題範囲には、試験分野、出題比率、出題例が含まれています。出題例は出題範囲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　ネットワークセキュリティ	20%
第2章　コンプライアンスと運用セキュリティ	18%
第3章　脅威と脆弱性	20%
第4章　アプリケーション、データ、ホスティングセキュリティ	15%
第5章　アクセスコントロール、認証マネジメント	15%
第6章　暗号化	12%
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。
https://certification.comptia.org/testing/test-policies/unauthorized-training-materials

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ために、Cert Guard を利用して検索をしていただくことができます。
http://www.certguard.com/search.asp

もしくは、下記のリストを参照していただくことも可能です。
http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx

※ 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。

第1章　ネットワークセキュリティ（20%）

1.1 ネットワーク機器と技術におけるセキュリティ設定について実装することができる。

- ファイアウォール
- ルーター
- スイッチ
- ロードバランサー
- プロキシー
- Web セキュリティゲートウェイ
- VPN コンセントレーター
- NIDS / NIPS
  - ビヘイビアベース（振る舞いベース）
  - シグネチャベース
  - アノーマリベース
  - ヒューリスティックベース
- プロトコルアナライザー
- スパムフィルター
- オールイン型セキュリティアプライアンス
  - URL フィルター
  - コンテンツ分析
  - マルウェア分析
- Web アプリケーションファイアウォールとネットワークファイアウォールの違い
- アプリケーション・アウェアデバイス
  - ファイアウォール
  - IPS
  - IDS
  - プロキシー

1.2 与えられたシナリオに基づいて、セキュアなネットワーク管理ポリシーを適用することができる。

- ルールベースマネジメント
- ファイアウォールルール
- VLAN マネジメント
- セキュアなルーター設定
- アクセスコントロールリスト（ACL）
- ポートセキュリティ
- 802.1x
- Flood Guards(DoS/DDos, SYN floods, ping floods 等)
- ループプロテクション
- 暗黙の拒否
- ネットワークの隔離
- ログ解析
- UTM（統合脅威管理：Unified Threat Management）

1.3 ネットワーク設計の要素とコンポーネントを説明することができる。

- DMZ
- サブネット化
- VLAN
- NAT
- リモートアクセス
- テレフォニー
- NAC

- 仮想化
- クラウドコンピューティング
  - Platform as a Service（PaaS）
  - Software as a Service（SaaS）
  - Infrastructure as a Service（IaaS）
  - プライベート
  - パブリック
  - ハイブリッド
  - コミュニティ
- 階層セキュリティ/多層防御（Defense in depth）

1.4 与えられたシナリオに基づいて、コマンドとサービスを利用することができる。

- プロトコル
  - IPSec
  - SNMP
  - SSH
  - DNS
  - TLS
  - SSL
  - TCP/IP
  - FTPS
  - HTTPS
  - SCP
  - ICMP
  - IPv4
  - IPv6
  - iSCSI
  - ファイバーチャネル
  - FCoE
  - FTP
  - SFTP
  - TFTP
  - テルネット
  - HTTP
  - NetBIOS
- ポート
  - 21
  - 22
  - 25
  - 53
  - 80
  - 110
  - 139
  - 143
  - 443
  - 3389
- OSI 参照モデル

1.5 与えられたシナリオに基づいて、ワイヤレスネットワークのセキュリティ脅威に関するトラブルシューティングを実施することができる。

- WPA
- WPA2
- WEP
- EAP
- PEAP
- LEAP
- MAC フィルター
- SSID ブロードキャストの無効化
- TKIP
- CCMP
- アンテナの設置
- パワーレベル（受信レベル）コントロール
- Captive Portal
- アンテナタイプ
- Site Survey（サイト調査）
- VPN（オープンワイヤレスネットワークからの利用）

第 2 章　コンプライアンスと運用セキュリティ（18%）

2.1　リスクに関連する概念の重要性を説明することができる。

- コントロール・タイプ
  - 技術面
  - マネジメント
  - 運用面
- フォールスポジティブ
- フォールスネガティブ
- リスク軽減ポリシーの重要性
  - プライバシーポリシー
  - 許容される利用
  - セキュリティポリシー
  - 強制休暇
  - ジョブローテーション
  - 職務の分離
  - 最小特権
- リスクの算出
  - 可能性
  - ALE（年間損失予算）
  - 影響度
  - SLE（単一損失予測）
  - ARO（年間発生頻度）
  - MTTR（平均復旧時間）
  - MTTF（平均修理時間）
  - MTBF（平均故障間隔）
- 定量的/定性的
- 脆弱性
- Threat Vector（脅威ベクター）
- セキュリティ評価/脅威の軽減
- リスクの回避、移転、受容、軽減、阻止
- クラウドコンピューティングと仮想化に関連するリスク
- RTO（復旧時間目標：Recovery time objective）と RPO（復旧時点目標：Recovery point objective）

2.2　システム統合や第三者とのデータ統合に関連するセキュリティを実施することができる。

- オンボーディング/オフボーディングのビジネスパートナー
- ソーシャルメディアネットワークのアプリケーション
- 相互運用の同意書
  - SLA
  - BPA
  - MOU
  - ISA
- プライバシーの検討
- リスクの認知
- 承認されていないデータの共有
- データの所有権
- データバックアップ
- セキュリティポリシーと手順の確認
- 標準的なコンプライアンスとパフォーマンスを同意書が満たしているか確認する

2.3 与えられたシナリオに基づいて、適切なリスク軽減対策を実装することができる。

- 変更管理
- インシデント管理
- ユーザー権限とアクセス権の確認
- パフォーマンスの定期的な監査
- データの損失や盗難を防止するためのポリシーと手続きを実施する
- テクノロジーコントロールを実装する
  - DLP（Data Loss Prevention）

2.4 与えられたシナリオに基づいて、基本的なフォレンジック分析を実施することができる。

- 揮発性の順序（Order of Volatility）
- システムイメージのキャプチャー
- ネットワークのトラフィックとログ
- ビデオの撮影
- 時系列の記録
- ハッシュの取得
- スクリーンショット
- 証拠
- 工数と費用の確認
- 証拠保管の継続性（Chain of custody）
- ビッグデータの分析

2.5 一般的なインシデント対応の手順を実施することができる。

- 準備
- インシデントの識別
- エスカレーションと通知
- 緩和手順
- 教訓
- 報告
- 復旧/再構成手順
- 初動対応者
- インシデントの分離
  - 検疫
  - デバイスの削除
- データ漏洩/侵害
- 被害と損失の制御

2.6 セキュリティの意識づけとトレーニングの重要性を説明することができる。

- セキュリティポリシーのトレーニングと手順
- ロールベーストレーニング
- 個人情報（PII：Personally Identifiable Information）
- 情報機密区分
  - 高
  - 中
  - 低
  - 機密事項
  - プライベート
  - パブリック
- データのラベル付け、取り扱い、廃棄
- 法律を配慮したコンプライアンス/ベストプラクティス/業界標準
- ユーザーの習慣

- パスワードの特徴
- データの取り扱い
- クリアデスクポリシー
- テールゲート（セキュリティゲート）による防止
- 個人所有の機器

- 新しい脅威やセキュリティトレンド/アラート
  - 新種のウイルス
  - フィッシング攻撃
  - ゼロディ攻撃
- ソーシャル・ネットワーキング（SNS）と P2P の利用
- コンプライアンスやセキュリティに対する意識づけを確認するためトレーニングメトリックを実施し、フォローする

2.7 物理セキュリティと環境管理を実施し、比較対照することができる。

- 環境管理
  - HVAC
  - 消火設備
  - EMI シールディング
  - 高温列・低温列配置
  - 環境モニタリング
  - 温度湿度管理
- 物理セキュリティ
  - ハードウェアのロック
  - マントラップ
  - ビデオ監視
  - フェンシング
  - 非接触カードリーダー
  - アクセスリスト
  - 適切な照明
  - サイン
  - ガード
  - バリケード
  - バイオメトリクス
  - 保護されたケーブル敷設
  - アラーム
  - モーション検知
- 管理タイプ
  - 抑止
  - 予防
  - 検知
  - 補正
  - 技術
  - 管理

2.8 リスクマネジメントのベストプラクティスを理解し、説明することができる。

- 事業継続の概念
  - 事業影響度分析（BIA）
  - クリティカルなシステムとコンポーネントの特定
  - 単一障害点の排除
  - 事業継続計画とテスト
  - リスクアセスメント

- 運用の継続
- 災害復旧（Disaster Recovery）
- IT コンテンジェンシープラン
- 権限の移譲計画
- 高可用性
- 冗長性
- 机上演習

- フォールトトレランス
  - ハードウェア
  - RAID
  - クラスタリング
  - 負荷分散
  - サーバ
- 災害復旧の概念
  - バックアッププラン/ポリシー
  - バックアップの実行/頻度
  - コールドサイト
  - ホットサイト
  - ワームサイト

2.9 与えられたシナリオに基づいて、セキュリティの目標を達成するための適切な管理方法を選択することができる。

- 機密性（Confidentiality）
  - 暗号化
  - アクセス制御
  - ステガノグラフィ
- 完全性（Integrity）
  - ハッシュ
  - デジタル署名
  - 証明書
  - 否認防止
- 可用性（Availability）
  - 冗長性
  - フォールトトレランス
  - パッチ適用
- 安全性（Safety）
  - フェンシング
  - 照明
  - ロック
  - CCTV
  - 避難計画
  - 訓練
  - 避難ルート
  - テストコントロール

第 3 章　脅威と脆弱性（20%）

3.1　マルウェアの各種タイプを解析、分類することができる。

- アドウェア
- ウイルス
- スパイウェア
- トロイの木馬（Trojan）
- ルートキット
- バックドア
- ロジックボム
- ボットネット
- ランサムウェア
- ポリモルフィックマルウェア
- Armored virus

3.2　攻撃の各種タイプを理解し、説明することができる。

- 中間者攻撃（Man-in-the-middle）
- DDoS
- DoS
- リプレイ
- スマーフ攻撃
- なりすまし（スプーフィング）
- スパム（spam）
- フィッシング（phishing）
- スピム（spim）
- ビッシング（vishing）
- スピアフィッシング（スピア型攻撃）
- クリスマスアタック
- ファーミング（pharming）
- 権限昇格
- 内部犯行の脅威
- DNS ポイズニング/ ARP ポイズイング
- Transitive access
- クライアントサイド攻撃
- パスワード攻撃
  - ブルートフォースアタック
  - 辞書攻撃
  - ハイブリッドアタック
  - 誕生日攻撃
  - レインボーテーブル
- タイポスクワッティング/セッションハイジャック
- ウォーターホール攻撃

3.3　ソーシャル・エンジニアリング攻撃と各種攻撃に関連する有効な対策の概要を理解し、説明することができる

- ショルダーサーフィン
- ダンプスターダイビング（ゴミ箱あさり）
- テールゲート（セキュリティゲート/共連れ）
- なりすまし
- 偽証
- ホエーリング攻撃
- ビッシング（Vishing）
- 原則（有効性の理由）

- 認証機関
- 脅迫
- コンセンサス/ソーシャルプルーフ（社会的証明）
- 希少性
- 緊急度
- 親しみやすい/好み
- 信頼性

3.4 無線上の攻撃の各種タイプを理解し、説明することができる。

- 不正アクセスポイント（AP）
- ジャミング/干渉
- エビルツイン（ワイフィッシング）
- ウォードライビング
- ブルージャッキング攻撃
- ブルースナーフィング攻撃
- ウォーチョーキング
- IV（Initialization Vector）攻撃
- パケットスニッフィング
- 近距離無線通信
- リプレイ攻撃
- WEP/ WPA 攻撃
- WPS 攻撃

3.5 アプリケーション攻撃の各種タイプを理解し、説明することができる。

- クロスサイトスクリプティング
- SQL インジェクション
- LDAP インジェクション
- XML インジェクション
- ディレクトリトラバーサル/コマンドインジェクション
- バッファーオーバーフロー攻撃
- 整数オーバーフロー攻撃
- ゼロディ攻撃
- Cookie と添付ファイル
- LSO（Locally Shared Objects）
- Flash クッキー
- 悪意あるアドオン
- セッションハイジャッキング
- ヘッダー偽装
- 任意のコードの実行/リモートでのコードの実行

3.6 状況を分析し、リスク軽減と抑止技術の適切な方法を選択することができる。

- システムログの監視
  - イベントログ
  - 監査ログ
  - セキュリティログ
  - アクセスログ
- セキュリティの強化
  - 不要サービスの停止
  - 管理インターフェースとアプリケーションの保護
  - パスワード保護
  - 不要アカウントの無効化

- ネットワークセキュリティ
  - MAC アドレス制限とフィルタリング
  - 802.1x
  - 使用していないインターフェースおよび、アプリケーションサービスポートの無効化
  - 不正マシンの検出
- セキュリティに関する心構え
  - ベースラインの設定
  - 継続的なセキュリティ監視
  - 改善
- レポート
  - アラーム
  - アラート
  - トレンド
- 検出コントロールと予防コントロール
  - IDS/IPS
  - カメラ/ガード

3.7 与えられたシナリオに基づいて、適切な技術とツールを利用して、セキュリティの脅威と脆弱性を発見することができる。

- セキュリティアセスメントツールの結果の解釈
- ツール
  - プロトコルアナライザー
  - 脆弱性スキャナー
  - ハニーポット
  - ハニーネット
  - ポートスキャナー
  - パッシブツール/アクティブツール
  - バナーグラビング
- リスクの算出
  - 脅威/可能性
- 評価タイプ
  - リスク
  - 脅威
  - 脆弱性
- 評価技術
  - ベースライン・レポート
  - コードレビュー
  - 攻撃手法の特定
  - アーキテクチャの確認
  - 設計の確認

3.8 脆弱性の評価に対する、侵入テスト（ペネトレーションテスト）の適切な利用について説明することができる。

- 侵入テスト（ペネトレーションテスト）
  - 存在する脅威の確認
  - セキュリティコントロールのバイパス
  - セキュリティコントロールの機能テスト
  - 脆弱性の悪用
- 脆弱性スキャン
  - セキュリティコントロールのテスト
  - 脆弱性の特定
  - セキュリティコントロール欠如の特定

- 一般的な誤設定の確認
- Intrusive/non-intrusive
- 証明書あり/証明書なし
- フォールスポジティブ

- ブラックボックス
- ホワイトボックス
- グレーボックス

第 4 章　アプリケーション、データ、ホスティングセキュリティ（15%）

4.1　アプリケーションセキュリティの重要性を説明することができる。

- ファジング
- ソースコード・コーディング・コンセプト
  - エラーと例外処理
  - 入力検証
- クロスサイトスクリプティング
- クロスサイトリクエストフォージェリー（XSRF）
- アプリケーション設定ベースライン（適切設定）
- アプリケーション強化
- アプリケーション・パッチ管理
- SQL 以外のデータベースと SQL データベースの比較
- サーバ側とクライアント側での検証

4.2　モバイルセキュリティの概念と技術を説明することができる。

- デバイスセキュリティ
  - デバイスのフル暗号化
  - リモートワイプ
  - ロックアウト
  - スクリーンロック
  - GPS
  - アプリケーションコントロール
  - ストレージのセグメント
  - アセットトラッキング
  - インベントリーコントロール
  - モバイルデバイス管理
  - デバイスのアクセスコントロール
  - リモートストレージ
  - 使用していない機能の無効化
- アプリケーションセキュリティ
  - キーマネジメント
  - クレデンシャルマネジメント
  - 認証
  - ジオタギング
  - 暗号化
  - アプリケーションのホワイトリスト
  - トランシブトラスト/認証
- BYOD の懸念事項
  - データの所有者
  - サポート対象
  - パッチ管理
  - アンチウイルスソフトの管理
  - フォレンジック
  - プライバシー
  - オンボード/オフボード
  - 企業ポリシーの遵守
  - ユーザー側の許容
  - アーキテクチャ/インフラストラクチャへの考慮事項
  - 法規制への懸念
  - 利用ポリシーの許容

- 搭載されているカメラ/ビデオの使用

4.3 与えられたシナリオに基づいて、ホストのセキュリティを確立するための適切なソリューションを実行することができる。

- オペレーティングシステムのセキュリティと設定
- OS の要塞化
- アンチマルウェア
  - アンチウィルス
  - アンチスパム
  - アンチスパイウェア
  - ポップアップブロック
- パッチ管理
- ホワイトリストとブラックリストのアプリケーション
- トラステッド OS
- ホストベースファイアウォール
- ホストベースの侵入検知
- ハードウェアセキュリティ
  - ケーブルロック
  - 安全性
  - 鍵のかかったキャビネット
- ホストソフトウェアのベースライン
- 仮想化
  - スナップショット
  - パッチの互換性
  - ホストの可用性/柔軟性
  - セキュリティ管理のテスト
  - サンドボックス

4.4 データのセキュリティを確保するために適切な管理を実施することができる。

- クラウドストレージ
- SAN
- ビッグデータの扱い
- データの暗号化
  - フルディスク
  - データベース
  - 個々のファイル
  - リムーバブルメディア
  - モバイルデバイス
- ハードウェアベースの暗号化
  - TPM
  - HSM
  - USB の暗号化
  - ハードディスク
- データの送信中、データの格納中、データの使用中
- パーミッション/ ACL
- データポリシー
  - ワイプ
  - 廃棄
  - リテンション
  - ストレージ

4.5 静的環境においてセキュリティリスクを軽減するための代替え方法を検討し、実装することができる。

- 環境
  - SCADA
  - 組み込み（プリンタ、スマートテレビ、HVAC 制御）
  - Android
  - iOS
  - メインフレーム
  - ゲームコンソール
  - 車載コンピュータシステム
- 方法
  - ネットワークのセグメント化
  - セキュリティ層
  - アプリケーションファイアウォール
  - マニュアルのアップデート
  - ファームウェアのバージョン管理
  - Wrapper
  - 冗長性と多様性を管理する

第 5 章　アクセスコントロール、認証マネジメント（15%）

5.1　認証サービスの目的と機能を比較し、実装することができる。

- RADIUS
- TACACS+
- Kerberos
- LDAP
- XTACACS
- SAML
- セキュア LDAP

5.2　与えられたシナリオに基づいて、適切な認証、承認、アクセスコントロールを選択することができる。

- 識別（Identification）と認証（Authentication）と承認（Authorization）の違い
- 承認
  - 最小特権
  - 職務の分離
  - ACL
  - 強制アクセス
  - 任意アクセス
  - ルールベースのアクセス制御（Rule-based access control）
  - ロールベースのアクセス制御（Role-based access control）
  - 時間帯の制限
- 認証
  - トークン
  - コモンアクセスカード
  - スマートカード
  - 多要素認証
  - TOTP（Time-Based One-Time Password)
  - HOTP（HMAC-Based One-time Password）
  - CHAP（Challenge Handshake Authentication Protocol）
  - PAP（Password Authentication Protocol）
  - シングルサインオン
  - アクセス制御
  - 暗黙の拒否
  - トラステッド OS
- 認証要素
  - 誰か
  - 何を持っているか
  - 何を知っているか
  - どこにいたか
  - 何をしたか
- 識別
  - バイオメトリクス
  - PIV（個人識別情報の検証カード）
  - ユーザー名
- フェデレーション
- 継続的な信頼/認証

5.3 ベストプラクティスに基づいてアカウント管理を行う際のセキュリティ管理を実装、設定することができる。

- 複数のアカウントやロールを持ちアカウントを共有しているユーザーに起因する問題の軽減
- アカウントポリシーの実施
  - クレデンシャルの管理
  - グループポリシー
  - パスワードの複雑化
  - 有効期限
  - リカバリー
  - 失効
  - ロックアウト
  - パスワードの履歴
  - パスワードの再利用
  - パスワードの長さ
  - 一般的なアカウントの禁止事項
- グループ単位の権限
- ユーザー単位の権限
- ユーザーアクセスの確認
- 継続的なモニタリング

第 6 章　暗号化（12%）

6.1　与えられたシナリオに基づき、一般的暗号化のコンセプトを理解し、確認することができる。

- 対称（Symmetric）と非対称（Asymmetric）の違い
- セッション鍵
- インバンドとアウトオブバンド伝送の違い
- 暗号化手法と基本的な違い
  - ブロックとストリームの違い
- 通信の暗号化
- 否認防止
- ハッシュ化
- キーエスクロー
- 電子透かし技術
- デジタル署名
- 実績ある技術の利用
- 楕円曲線暗号と量子暗号
- Ephemeral key（短期鍵）
- Perfect forward secrecy（前方秘匿性）

6.2　与えられたシナリオに基づき、適切な暗号化ツールと製品を使用することができる。

- WEP と WPA/WPA2 の違いと事前共有鍵
- MD5
- SHA
- RIPEMD
- AES
- DES
- 3DES
- HMAC
- RSA
- ディフィー・ヘルマン鍵共有
- RC4
- ワンタイムパッド
- NTLM
- NTLMv2
- Blowfish
- PGP/GPG
- TwoFish
- DHE
- ECDHE
- CHAP
- PAR
- アルゴリズムの強度比較
- 通信暗号化のアルゴリズムの使用
  - SSL
  - TLS
  - IPSec
  - SSH
  - HTTPS
- Cipher suite
  - 強力な暗号/弱い暗号

- パスワードの強度
  - PBKDF2
  - Bcrypt

6.3 与えられたシナリオに基づき、適切な PKI、認証マネジメント、これらに関連するコンポーネントを使用することができる。

- 公開鍵証明書認証局と電子証明書
  - CA
  - CRL
  - OCSP
  - CSR
- PKI
- リカバリーエージェント
- 公開鍵
- 秘密鍵
- 登録
- キーエスクロー
- 信頼モデル

CompTIA Security+ 略語一覧

下記はCompTIA Security+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。

3DES	―	Triple Digital Encryption Standard
AAA	―	Authentication, Authorization, and Accounting
ACL	―	Access Control List
AES	―	Advanced Encryption Standard
AES256	―	Advanced Encryption Standards 256bit
AH	―	Authentication Header
ALE	―	Annualized Loss Expectancy
AP	―	Access Point
ARO	―	Annualized Rate of Occurrence
ARP	―	Address Resolution Protocol
AUP	―	Acceptable Use Policy
BCP	―	Business Continuity Planning
BIOS	―	Basic Input / Output System
BOTS	―	Network Robots
CA	―	Certificate Authority
CAC	―	Common Access Card
CAN	―	Controller Area Network
CCMP	―	Counter-Mode/CBC-Mac Protocol
CCTV	―	Closed-circuit television
CERT	―	Computer Emergency Response Team
CHAP	―	Challenge Handshake Authentication Protocol
CIRT	―	Computer Incident Response Team
CRC	―	Cyclical Redundancy Check
CRL	―	Certification Revocation List
DAC	―	Discretionary Access Control
DDOS	―	Distributed Denial of Service
DEP	―	Data Execution Prevention
DES	―	Digital Encryption Standard
DHCP	―	Dynamic Host Configuration Protocol
DLL	―	Dynamic Link Library
DLP	―	Data Loss Prevention
DMZ	―	Demilitarized Zone
DNS	―	Domain Name Service (Server)
DOS	―	Denial of Service
DRP	―	Disaster Recovery Plan
DSA	―	Digital Signature Algorithm
EAP	―	Extensible Authentication Protocol
ECC	―	Elliptic Curve Cryptography
EFS	―	Encrypted File System
EMI	―	Electromagnetic Interference
ESP	―	Encapsulated Security Payload
FTP	―	File Transfer Protocol
GPU	―	Graphic Processing Unit
GRE	―	Generic Routing Encapsulation
HDD	―	Hard Disk Drive

HIDS	–	Host Based Intrusion Detection System
HIPS	–	Host Based Intrusion Prevention System
HMAC	–	Hashed Message Authentication Code
HSM	–	Hardware Security Module
HTTP	–	Hypertext Transfer Protocol
HTTPS	–	Hypertext Transfer Protocol over SSL
HVAC	–	Heating, Ventilation Air Conditioning
IaaS	–	Infrastructure as a Service
ICMP	–	Internet Control Message Protocol
ID	–	Identification
IKE	–	Internet Key Exchange
IM	–	Instant messaging
IMAP4	–	Internet Message Access Protocol v4
IP	–	Internet Protocol
IPSEC	–	Internet Protocol Security
IRC	–	Internet Relay Chat
ISP	–	Internet Service Provider
IV	–	Initialization Vector
KDC	–	Key Distribution Center
L2TP	–	Layer 2 Tunneling Protocol
LANMAN	–	Local Area Network Manager
LDAP	–	Lightweight Directory Access Protocol
LEAP	–	Lightweight Extensible Authentication Protocol
MAC	–	Mandatory Access Control / Media Access Control
MAC	–	Message Authentication Code
MAN	–	Metropolitan Area Network
MBR	–	Master Boot Record
MD5	–	Message Digest 5
MSCHAP	–	Microsoft Challenge Handshake Authentication Protocol
MTU	–	Maximum Transmission Unit
NAC	–	Network Access Control
NAT	–	Network Address Translation
NIDS	–	Network Based Intrusion Detection System
NIPS	–	Network Based Intrusion Prevention System
NIST	–	National Institute of Standards & Technology
NOS	–	Network Operating System
NTFS	–	New Technology File System
NTLM	–	New Technology LANMAN
NTP	–	Network Time Protocol
OS	–	Operating System
OVAL	–	Open Vulnerability Assessment Language
PAP	–	Password Authentication Protocol
PAT	–	Port Address Translation
PBX	–	Private Branch Exchange
PEAP	–	Protected Extensible Authentication Protocol
PED	–	Personal Electronic Device
PGP	–	Pretty Good Privacy
PII	–	Personally Identifiable Information
PKI	–	Public Key Infrastructure
POTS	–	Plain Old Telephone Service

PPP	–	Point-to-point Protocol
PPTP	–	Point to Point Tunneling Protocol
PSK	–	Pre-Shared Key
PTZ	–	Pan-Tilt-Zoom
RA	–	Recovery Agent
RAD	–	Rapid application development
RADIUS	–	Remote Authentication Dial-in User Server
RAID	–	Redundant Array of Inexpensive Disks
RAS	–	Remote Access Server
RBAC	–	Role Based Access Control
RBAC	–	Rule Based Access Control
RSA	–	Rivest, Shamir, & Adleman
RTO	–	Recovery Time Objective
RTP	–	Real-Time Transport Protocol
S/MIME	–	Secure / Multipurpose internet Mail Extensions
SaaS	–	Software as a Service
SCAP	–	Security Content Automation Protocol
SCSI	–	Small Computer System Interface
SDLC	–	Software Development Life Cycle
SDLM	–	Software Development Life Cycle Methodology
SHA	–	Secure Hashing Algorithm
SHTTP	–	Secure Hypertext Transfer Protocol
SIM	–	Subscriber Identity Module
SLA	–	Service Level Agreement
SLE	–	Single Loss Expectancy
SMS	–	Short Message Service
SMTP	–	Simple Mail Transfer Protocol
SNMP	–	Simple Network Management Protocol
SONET	–	Synchronous Optical Network Technologies
SPIM	–	Spam over Internet Messaging
SSH	–	Secure Shell
SSL	–	Secure Sockets Layer
SSO	–	Single Sign On
STP	–	Shielded Twisted Pair
TACACS	–	Terminal Access Controller Access Control System
TCP/IP	–	Transmission Control Protocol / Internet Protocol
TKIP	–	Temporal Key Integrity Protocol
TLS	–	Transport Layer Security
TPM	–	Trusted Platform Module
UAT	–	User Acceptance Testing
UPS	–	Uninterruptable Power Supply
URL	–	Universal Resource Locator
USB	–	Universal Serial Bus
UTP	–	Unshielded Twisted Pair
VLAN	–	Virtual Local Area Network
VoIP	–	Voice over IP
VPN	–	Virtual Private Network
VTC	–	Video Teleconferencing
WAF	–	Web-Application Firewall
WAP	–	Wireless Access Point

WEP	–	Wired Equivalent Privacy
WIDS	–	Wireless Intrusion Detection System
WIPS	–	Wireless Intrusion Prevention System
WPA	–	Wireless Protected Access
XSRF	–	Cross-Site Request Forgery
XSRF	–	Cross-Site Request Forgery
XSS	–	Cross-Site Scripting