

## CompTIA Security+ (2008 年版) 認定資格試験出題範囲

CompTIA Security+(2008 年版)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。

この試験で測られるスキル及び知識は、業界全体におけるジョブ タスク アナリシス (JTA)に基づき、2007 年第 4 四半期に行われたグローバルレベルの調査ではその検討および検証がされています。この調査の結果を基に、試験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。

CompTIA Security+ (2008 年版) 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

以下の表は試験分野および各分野の出題比率です。

CompTIA Security+ 認定試験分野	出題比率
第 1 章 システムセキュリティ	21%
第 2 章 ネットワークインフラストラクチャ	20%
第 3 章 アクセス制御	17%
第 4 章 アセスメントと監査	15%
第 5 章 暗号化技術	15%
第 6 章 組織面でのセキュリティ	12%

### <注記>

分野別に取り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。

## 第1章 システム セキュリティ (21%)

1.1 様々なシステムセキュリティ脅威を区別し、説明することができる。

- 権限の昇格
- ウイルス
- ワーム
- トロイ
- スパイウェア
- スпам
- アドウェア
- ルートキット
- ボットネット
- ロジックボム

1.2 システムハードウェアや周辺機器に関連したセキュリティリスクを説明することができる。

- BIOS
- USB デバイス
- 携帯電話
- リムーバブルストレージ
- ネットワーク接続ストレージ(NAS)

1.3 OSを強化する手段や方法を実行して、ワークステーションやサーバのセキュリティを確保する。

- ホットフィックス
- サービスパック
- パッチ
- パッチ管理
- グループポリシー
- セキュリティテンプレート
- 構成ベースライン

1.4 適切な手順を実行してアプリケーションのセキュリティを構築する。

- Active X
- Java
- スクリプト
- ブラウザ
- バッファオーバーフロー
- Cookie
- SMTP オープンリレー
- インスタントメッセージング

- P2P
- 入力検証
- クロスサイトスクリプティング (XSS)

1.5 セキュリティアプリケーションを実行する。

- HIDS
- パーソナルソフトウェアファイアーウォール
- ウイルス対策
- スпам対策
- ポップアップブロッカー

1.6 仮想化技術の目的と適用を説明することができる。

## 第2章 ネットワーク インフラストラクチャ(20%)

2.1 異なるポートとプロトコルのそれぞれにおける脅威やそれを減少させるテクニックの違いを区別し、説明することができる。

- 旧世代のプロトコル
- TCP/IP ハイジャック
- Null セッション
- スプーフィング(なりすまし)
- Man in the Middle(中間者)
- リプレイ
- DoS
- DDoS
- ドメインカイトイング(不正)
- DNS ポイズニング
- APR ポイズニング

2.2 ネットワークの設計要素と構成を区別する。

- DMZ
- VLAN
- NAT
- ネットワーク相互接続
- NAC
- サブネット
- テレフォニー

2.3 ネットワークセキュリティを強化するため、適切なネットワークセキュリティツールを判断し使用することができる。

- NIDS
- NIPS
- ファイアーウォール
- プロキシサーバ
- ハニーポット
- インターネットコンテンツフィルタ
- プロトコルアナライザー

2.4 ネットワークセキュリティを強化するため、適切なネットワークツールを使用することができる。

- NIDS
- ファイアーウォール
- プロキシサーバ

- インターネットコンテンツフィルタ
- プロトコルアナライザー

2.5 ネットワークデバイスに関連する脆弱性や軽減策について説明することができる。

- 権限の昇格
- 脆弱なパスワード
- バックドア
- デフォルトアカウント
- DoS

2.6 様々な伝送媒体に関連する脆弱性や軽減策について説明することができる。

- バンパイヤタック

2.7 ワイヤレスネットワークに関連する脆弱性を説明することができ、軽減策を実装することができる。

- データ流出
- ウォードライビング
- SSID ブロードキャスト
- ブルージャッキング
- ブルースナーフィング
- 不正アクセスポイント
- 脆弱な暗号化

## 第3章 アクセス制御（17%）

3.1 アクセス制御方法とされる業界のベストプラクティスを特定し適用することができる。

- 暗黙の拒否
- 最小特権
- 職務の分離
- ジョブローテーション

3.2 一般的なアクセス制御モデルとそれぞれの違いについて説明することができる。

- MAC
- DAC
- ロールベースアクセスコントロール
- ルールベースアクセスコントロール

3.3 ユーザーやコンピュータを、適切なセキュリティグループと役割に整理し、それぞれに適切な権限と特権を割り当てる。

3.4 ファイルやプリントリソースに対して、適切なセキュリティ制御を適用する。

3.5 論理アクセス制御方法を比較して実装する。

- ACL
- グループポリシー
- パスワードポリシー
- ドメインパスワードポリシー
- ユーザー名とパスワード
- 時間帯の制限
- アカウントの有効期限
- 論理トークン

3.6 様々な認証モデルを認識し、それぞれの構成について特定する。

- 1、2、または3要素認証
- シングルサインオン(SSO)

3.7 様々な認証モデルを配備し、それぞれの構成について認識する。

- バイオメトリックス(生体)リーダー
- RADIUS
- RAS
- LDAP
- リモートアクセスポリシー

- リモート認証
- VPN
- Kerberos
- CHAP
- PAP
- Mutual
- 802.1x
- TACACS

3.8 識別 (Identification) と認証 (Authentication) の違いについて説明することができる。

3.9 物理アクセスセキュリティ方法を説明し、適用する。

- 物理アクセスのログ／リスト
- ハードウェアのロック
- 物理アクセス制御 — ID バッチ
- 入退室管理システム (ドアアクセスシステム)
- マントラップ
- 物理トークン
- ビデオ監視 — カメラの種類と配置

## 第4章 アセスメントと監査 (15%)

4.1 リスクアセスメントの実施とリスク緩和を実行する。

4.2 一般的ツールを使用し、脆弱性アセスメントを実施する。

- ポートスキャナー
- 脆弱性スキャナー
- プロトコルアナライザー
- OVAL
- パスワードクラッカー
- ネットワークマッパー

4.3 脆弱性アセスメント領域において、侵入テストや脆弱性スキャナーの適切な使用について説明することができる。

4.4 システムやネットワークに監視ツールを使用し、セキュリティ関連の異常項目を検出する。

- パフォーマンスの監視
- システムの監視
- パフォーマンスベースライン
- プロトコルアナライザー

4.5 様々な種類の監視方法について比較・対照することができる。

- ビヘイビアベース(振る舞いベース)
- シグネチャベース(署名ベース)
- アノマリベース(異常ベース)

4.6 適切なログ管理手順を実行し、結果を評価する。

- セキュリティアプリケーション
- DNS
- システム
- パフォーマンス
- アクセス
- ファイアーウォール
- アンチウイルス

4.7 システムのセキュリティ設定について定期監査を実施する。

- ユーザーのアクセスと権限の確認
- ストレージと保存に関するポリシー
- グループポリシー

## 第5章 暗号化技術（15%）

5.1 一般的な暗号化作成の概念について説明することができる。

- 鍵の管理
- ステガノグラフィー
- 対称鍵
- 非対称暗号化鍵
- 機密性 (Confidentiality)
- 完全性 (integrity)
- 可用性 (availability)
- 否認防止
- アルゴリズムの比較強度
- デジタル署名
- ディスク全体の暗号化
- トラステッドプラットフォームモジュール (TPM)
- シングルとデュアル認証
- 実証済み (評価済み) 暗号化技術の使用

5.2 基本的なハッシングの概念を説明し、適切なアプリケーションへ様々な暗号化アルゴリズムを適用することができる。

- SHA
- MD5
- LANMAN
- NTLM

5.3 基本的暗号化技術の概念を説明し、適切なアプリケーションへ様々な暗号化アルゴリズムを適用することができる。

- DES
- 3DES
- RSA
- PGP
- 楕円曲線
- AES
- AES256
- ワンタイムパッド
- 通信暗号化技術 (WEP TKIP など)

5.4 プロトコルについて説明し、実装することができる。

- SSL/TLS

- S/MIME
- PPTP
- HTTP、HTTPS、SHTTP
- L2TP
- IPSEC
- SSH

5.5 公開鍵暗号化の基本概念について説明することができる。

- 公開鍵基盤 (PKI)
- リカバリーエージェント
- 公開鍵
- 秘密鍵
- 認証機関 (CA)
- レジストレーション
- キーエスクロー(鍵供託)
- 証明書失効リスト(CRL)
- 信頼モデル

5.6 PKIと認証管理を実装する。

- 公開鍵基盤 (PKI)
- リカバリーエージェント
- 公開鍵
- 秘密鍵
- 認証機関 (CA)
- レジストレーション
- キーエスクロー (鍵供託)
- 証明書失効リスト (CRL)

## 第6章 組織面でのセキュリティ (12%)

6.1 冗長化計画とその構成について説明することができる。

- ホットサイト
- コールドサイト
- ウォームサイト
- バックアップジェネレーター
- 単一障害ポイント
- RAID
- スペアパーツ
- 冗長サーバ
- 冗長 ISP
- UPS
- 冗長接続

6.2 災害復旧(ディザスタリカバリ)手順を実行する。

- プランニング
- 災害復旧の実行
- バックアップのテクニックと実行—ストレージ
- スキーム
- 復旧

6.3 インシデントの対応手順を認識し、適切な対応手順を実施することができる。

- フォレンジック分析
- 証拠の連鎖
- 第一対応者
- 被害と損失の制御
- 報告—情報の公開

6.4 該当する法規制と企業ポリシーを認識し説明することができる。

- コンピュータの安全な廃棄処分
- 利用規定
- パスワードの複雑性
- 変更管理
- 情報のレベル分け
- 強制休暇
- 個人情報 (PII)
- 妥当な注意
- 妥当な注意義務

- 適正手続き
- SLA
- セキュリティに関連した人事ポリシー
- ユーザー教育と意識トレーニング

6.5 環境管理の重要性について説明することができる。

- 火災の鎮静化
- HVAC
- シールド化

6.6 ソーシャルエンジニアリングの概念とそのリスク軽減方法について説明することができる。

- フィッシング
- デマ情報
- ショルダーサーフィング(肩ごしの盗み見)
- ダンプスターダイビング(ごみ箱あさり)
- ユーザー教育と意識トレーニング

### CompTIA Security+ 略語一覧

3DES	— Triple Digital Encryption Standard
ACL	— Access Control List
AES	— Advanced Encryption Standard
AES256	— Advanced Encryption Standards 256bit
AH	— Authentication Header
ALE	— Annualized Loss Expectancy
ARO	— Annualized Rate of Occurrence
ARP	— Address Resolution Protocol
AUP	— Acceptable Use Policy
BIOS	— Basic Input / Output System
BOTS	— Network Robots
CA	— Certificate Authority
CAN	— Controller Area Network
CCTV	— Closed-circuit television
CHAP	— Challenge Handshake Authentication Protocol
CRL	— Certification Revocation List
DAC	— Discretionary Access Control
DDoS	— Distributed Denial of Service
DES	— Digital Encryption Standard
DHCP	— Dynamic Host Configuration Protocol
DLL	— Dynamic Link Library
DMZ	— Demilitarized Zone
DNS	— Domain Name Service (Server)
DoS	— Denial of Service
EAP	— Extensible Authentication Protocol
ECC	— Elliptic Curve Cryptography
FTP	— File Transfer Protocol
GRE	— Generic Routing Encapsulation
HIDS	— Host Based Intrusion Detection System
HIPS	— Host Based Intrusion Prevention System
HTTP	— Hypertext Transfer Protocol
HTTPS	— Hypertext Transfer Protocol over SSL
HVAC	— Heating, Ventilation Air Conditioning
ICMP	— Internet Control Message Protocol
ID	— Identification
IM	— Instant messaging
IMAP4	— Internet Message Access Protocol v4

IP	—	Internet Protocol
IPSEC	—	Internet Protocol Security
IRC	—	Internet Relay Chat
ISP	—	Internet Service Provider
KDC	—	Key Distribution Center
L2TP	—	Layer 2 Tunneling Protocol
LANMAN	—	Local Area Network Manager
LDAP	—	Lightweight Directory Access Protocol
MAC	—	Mandatory Access Control / Media Access Control
MAC	—	Message Authentication Code
MAN -	—	Metropolitan Area Network
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
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
PGP	—	Pretty Good Privacy
PII	—	Personally Identifiable Information
PKI	—	Public Key Infrastructure
PPP	—	Point-to-point Protocol
PPTP	—	Point to Point Tunneling Protocol
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

S/MIME	—	Secure / Multipurpose internet Mail Extensions
SCSI	—	Small Computer System Interface
SHA	—	Secure Hashing Algorithm
SHTTP	—	Secure Hypertext Transfer Protocol
SLA	—	Service Level Agreement
SLE	—	Single Loss Expectancy
SMTP	—	Simple Mail Transfer Protocol
SNMP	—	Simple Network Management Protocol
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
TKIP	—	Temporal Key Interchange Protocol
TLS	—	Transport Layer Security
TPM	—	Trusted Platform Module
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
WEP	—	Wired Equivalent Privacy
WPA	—	Wi-Fi Protected Access