IT資格道場

CompTIA Security+ 学習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

CompTIA Security+ (SY0-701) Exam Objectives Version 5.0 準拠
2026年7月版

本書のご利用にあたって

- 本書は「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルであっても著作物です。本書の転載・改変しての再配布・二次販売を禁じます。
- 本書を AI モデルの学習データとして利用すること(学習目的の入力・データセット化を含む)を禁じます。
- 製品版(学習用テキスト・暗記用ノート・頻出度別ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

不正な配布を見つけた場合は info@shikaku-doujou.com までご連絡ください。

目次

はじめに ―― この教材の使い方

このテキストは、情報セキュリティの国際的な入門資格 **CompTIA Security+(試験コード SY0-701)** に、IT の予備知識が浅い状態から合格することを目的に作られています。

Security+ は、特定のクラウド事業者や製品に依存しない **ベンダー中立** の資格です。AWS や Azure のような「ある会社のサービス名」を覚える試験ではなく、**どの現場でも通用するセキュリティの共通言語と考え方**を問われます。用語の数は多いものの、一つひとつは「何のためのものか」を一言で言えれば戦えます。問われるのは大きく次の 3 つです。

1. **概念を正しく区別できるか**(例:「これは予防的統制か、抑止的統制か」)
2. **用語・技術と役割を結び付けられるか**(例:「送信元 IP を認可する仕組みは SPF・DKIM・DMARC のどれか」)
3. **場面に応じて適切な対応を選べるか**(例:「インシデント対応で封じ込めの次にやることは?」)

つまり「自分で高度に構築できる人」ではなく、「**正しく判断し、正しい言葉で言い当てられる人**」になれば合格ラインに届きます。本テキストは、そのために必要な内容だけを出題範囲(5 分野)に沿って説明します。

試験の基本情報

項目	内容
試験名	CompTIA Security+(試験コード SY0-701・第 7 版)
問題数	**最大 90 問**

項目	内容
出題形式	択一式(多肢選択)と**パフォーマンスベース問題(PBQ)**
試験時間	90 分
合格ライン	100〜900 のスケールスコアで **750**
受験前提	**必須の前提資格はなし**。CompTIA Network+ の取得とセキュリティ実務 2 年程度の経験が「推奨」されている(あくまで推奨であり、なくても受験できる)
受験方法	テストセンターまたは自宅からのオンライン監督試験
言語	**日本語で受験可**(英語・ポルトガル語・スペイン語・タイ語も提供)

パフォーマンスベース問題(PBQ) とは、択一ではなく「操作・並べ替え・設定の当てはめ」など、実際の作業に近い形で解かせる問題です。試験の前半に数問置かれることが多く、時間を取られやすいので、**難しければ後回しにして択一を先に片付ける**のが定石です(あとで戻れます)。

合格ラインの「750」は素点(正答数)ではなく、難易度で調整された**スケールスコア**です。全 900 点満点のうち 750 なので、ざっくり **8 割強の手応え**を目標にすると安全です。実施形式・受験料・提供言語は変わることがあるので、申し込み時に公式ページで最新情報を確認してください。

版(バージョン)について: 本教材が対象とするのは現行版の **SY0-701** です。CompTIA の試験はおおむね 3 年ごとに改訂され、次版(SY0-801 とされる)の提供開始も予定されていますが、**SY0-701 は本書作成時点で申し込める現行試験**です。いったん取得した Security+ 認定は、受験した版に関わらず**取**

得日から 3 年間有効です。受験直前には公式サイトで現行版を確認してください。

試験の設計図 —— 5 分野と配点

SY0-701 の出題範囲(Exam Objectives)は、分野ごとの配点比率を公式に明示しています。学習時間もこの比率に合わせて配分するのが合理的です。**本教材の頻出度 A/B/C の格付けも、この公式配点比率を土台にしています。**

分野	配点	本書の対応章
① 一般的なセキュリティの概念	**12%**	第 1〜2 章
② 脅威・脆弱性・緩和策	**22%**	第 3〜4 章
③ セキュリティアーキテクチャ	**18%**	第 5〜6 章
④ セキュリティの運用	**28%**	第 7〜8 章
⑤ セキュリティプログラムの管理と監督	**20%**	第 9〜10 章

注目すべきは、最大分野が**運用(28%)** で、次いで**脅威・脆弱性(22%)** と**管理・監督(20%)** だという点です。「暗号やアーキテクチャの知識試験」と身構えがちですが、実際は**日々セキュリティ業務を回す力**(監視・対応・IAM・ガバナンス)に配点が寄っています。ここが SY0-701 攻略の急所です。

3 ステップ学習法

購入者限定テキストは 3 冊で 1 セットです。次の順番で使うと最短です。

- **STEP 1(理解する)**: 本書「学習用テキスト」を通読する。ここで全体の地図を頭に入れる
- **STEP 2(覚える)**: 「暗記用ノート」の一問一答を、即答できるまで繰り返す
- **STEP 3(仕上げる)**: 「頻出度別ノート」で頻出度 A の論点から総点検し、仕上げに本サイトの問題演習を回す

用語量が多いので、フル通読が難しければ、先に「頻出度別ノート」で頻出度 A の論点を確認し、それを含む章から読み始めても構いません。

第1章 セキュリティの基本概念(分野① 前半)

最初の分野は、以降すべての土台になる**共通概念**です。ここでの用語(CIA・AAA・統制の分類・ゼロトラスト)は、他の 4 分野の設問の中にも顔を出します。配点は 12% と小さめですが、**取りこぼすと全分野に響く**ので、定義を正確に押さえてください。

1-1 情報セキュリティの三本柱 —— CIA

セキュリティが「守るもの」は、頭文字を取って **CIA** と呼ばれる 3 つに集約されます。

- **機密性(Confidentiality)**: 許可された人・システムだけが情報を見られる状態。破る攻撃=盗み見・漏えい。守る手段=暗号化・アクセス制御
- **完全性(Integrity)**: 情報が改ざんされず、正確なまま保たれている状態。守る手段=ハッシュ・デジタル署名
- **可用性(Availability)**: 必要なときに使える状態。破る攻撃=DDoS(第 4 章)。守る手段=冗長化・バックアップ

これに **否認防止(Non-repudiation)** を加えて覚えます。否認防止とは、「**やっていない、と後から言い逃れできないようにする**」仕組みで、デジタル署名や監査ログで実現します。「電子署名が提供するのは?」→ 完全性・認証・**否認防止**、が定番です。

1-2 AAA —— 認証・認可・アカウンティング

アクセス管理の背骨が **AAA** です。3 つを順番に区別してください。

- **認証(Authentication)**:「あなたは誰か」を確かめる(本人確認)
- **認可(Authorization)**:「あなたに何を許すか」を決める(権限付与)
- **アカウンティング(Accounting)**:「あなたが何をしたか」を記録する(追跡・監査)

認証には「人の認証」と「システムの認証」があり、証拠として使えるのは次の**3 要素**です。

認証要素	一言で	例
知識(something you know)	知っていること	パスワード、PIN
所持(something you have)	持っているもの	スマホのトークン、セキュリティキー
生体(something you are)	その人自身の特徴	指紋、顔、虹彩

種類の違う要素を 2 つ以上組み合わせるのが **多要素認証(MFA)** です(第 7 章)。「パスワード+秘密の質問」は**どちらも知識**なので MFA にならない、というひっかけが出ます。位置情報(**somewhere you are**)も補助的な要素として登場します。

1-3 セキュリティ統制の分類 —— 2 つの軸

守るための施策(**統制/コントロール**)は、2 つの軸で分類されます。この分類の判別は最頻出です。

軸① カテゴリ(何によって実装するか)

カテゴリ	一言で	例
技術的(Technical)	システムで実装	ファイアウォール、暗号化、ウイルス対策
管理的(Managerial)	方針・計画で実装	リスク評価、セキュリティポリシー
運用的(Operational)	人が日常運用で実施	意識向上訓練、警備員の巡回
物理的(Physical)	物で実装	フェンス、施錠、監視カメラ

軸② タイプ(いつ・どう効くか)

タイプ	一言で	例
予防的(Preventive)	起きる前に防ぐ	アクセス制御リスト、施錠
抑止的(Deterrent)	思いとどまらせる(心理的)	警告看板、「監視中」の掲示
検知的(Detective)	起きたことを見つける	ログ、侵入検知、監視カメラの録画
是正的(Corrective)	起きた後に元へ戻す	バックアップからの復旧、パッチ適用
補償的(Compensating)	本来の統制の代わりの代替策	直せない旧システムを隔離網に置く
指示的(Directive)	こうしなさいと導く	手順書、利用規定

急所は **抑止と予防の違い**です。抑止は「やる気をなくさせる(看板・カメラの存在・**夜間の照明**で人影が見える状態を保つこと)」、予防は「物理的・技術的に実際にできなくする(施錠・ACL)」。なお**入退室ログの突き合わせや侵入時の自動通報は「発見的」**で、起きたことを見つける側にあたります。また、**1 つの統制が複数に当てはまる**点も重要です。たとえばフェンスは「物理的」かつ「予

防的」かつ「抑止的」です。設問は「**最も適切なのはどれか**」を問うので、場面の力点(実際に阻止したいのか、思いとどまらせたいのか)で選びます。

1-4 ゼロトラスト ―― 「決して信頼せず、常に検証する」

ゼロトラストは、「社内ネットワークの中だから安全」という前提を捨て、**すべてのアクセスをそのつど検証する**考え方です。SY0-701 では構成要素の名前と役割が問われます。2 つの面(プレーン)に分かれます。

- **コントロールプレーン(制御面)** = 通すかどうかを**決める頭脳**
  - **ポリシーエンジン**: 許可/拒否を**判断**する
  - **ポリシー管理者(Policy Administrator)**: 判断に従って接続を**確立・切断**する
  - **適応型 ID / 脅威範囲の縮小 / ポリシー駆動アクセス制御**: 判断の材料と方針
- **データプレーン(データ面)** = 実際に通信が**流れる場所**
  - **ポリシー実施点(PEP)**: 決定を**現場で実行**する門番
  - **暗黙の信頼ゾーン / 主体(Subject)・システム**: 検証の対象

「判断するのはポリシーエンジン、実行するのは PEP」という**頭脳と手足の分業**が覚えどころです。

1-5 物理セキュリティと欺瞞技術

物理セキュリティの道具も名前で問われます。**車止め(Bollards)**、**入退室用の二重扉(Access control vestibule/マントラップ)**、フェンス、監視カメラ、警備員、入館バッジ、照明、各種**センサー**(赤外線・感圧・マイクロ波・超音波)。二重扉は「共連れ(1 人の認証で複数人が入る)」を防ぐ仕組みとして頻出で

す。入館バッジの多くは **RFID(近距離無線)** で本人確認しますが、正規カードの信号を読み取って複製する**RFID クローニング**という物理攻撃があり、バッジ運用だけでは防ぎきれない弱点として問われます。

欺瞞・かく乱技術(Deception) は、攻撃者をわざとおびき寄せて観察・検知する仕掛けです。規模で区別します。

- **ハニーポット**: おとりの**システム 1 台**
- **ハニーネット**: おとりの**ネットワーク**(複数のハニーポット)
- **ハニーファイル**: おとりの**ファイル**(開かれたら通知)
- **ハニートークン**: おとりの**データや認証情報**(使われたら不正の証拠)

1-6 変更管理とギャップ分析

変更管理(Change Management) は、システムへの変更を無秩序に行わず、承認・記録・切り戻しの手順に沿って進める仕組みです。設定変更が新たな穴を生むのを防ぐ、セキュリティ上も重要なプロセスです。試験に効く要素は次のとおりです。

- **承認プロセス / オーナーシップ / 利害関係者**: 誰が判断し、誰に影響するか。承認を担う会議体が **CAB(変更諮問委員会 / Change Advisory Board)** で、**承認を得る前に変更を実施しないこと**が変更管理の要点。緊急時は簡略化した経路(緊急変更)を使うが、その場合も**事後に必ず起票して記録を残す**
- **影響分析 / テスト結果**: 変更が及ぼす範囲を事前に評価
- **技術的影響(Technical impact)**: 変更が引き起こしうる具体的な副作用。**ダウンタイム・サービス/アプリケーションの再起動・他システムとの依存関係・レガシーアプリとの互換性**などを事前に洗い出す

- **切り戻し計画(Backout plan)**: **失敗したら元に戻す**手順(必須)
- **メンテナンス期間(Maintenance window)**: 影響の小さい時間帯に実施
- **標準作業手順(SOP)** と **バージョン管理**: 手順の標準化と履歴管理

ギャップ分析は、「あるべき姿」と「現状」の差を洗い出し、埋めるべき課題を特定する作業です。

第1章の試験ポイント

- CIA=機密性(暗号化で守る)・完全性(ハッシュで守る)・可用性(冗長化で守る)+否認防止(署名・ログ)
- AAA=認証(誰)・認可(何を許す)・アカウンティング(記録)。認証 3 要素は知識・所持・生体。異種を 2 つ以上で MFA
- 統制の 2 軸=カテゴリ(技術/管理/運用/物理)×タイプ(予防・抑止・検知・是正・補償・指示)。抑止=心理的、予防=実際に阻止
- ゼロトラスト=判断はポリシーエンジン、実行は PEP(ポリシー実施点)
- ハニーポット(システム)/ハニーネット(網)/ハニーファイル/ハニートークンを規模で区別
- 変更管理の要=切り戻し計画・メンテナンス期間・承認プロセス(**CAB=変更諮問委員会**)。手順の順序は**起票 → 影響とリスクと切り戻しの評価 → 承認 → 周知 → 実施と確認 → 記録と構成情報の更新**

サンプルはここまでです

続き(第2章〜巻末)は、Security+ 問題集のご購入で、暗記用ノート・頻出度別ノートと合わせて3点すべてダウンロードできます。

CompTIA Security+ 学習用テキスト(無料サンプル)

版

2026年7月版(CompTIA Security+ (SY0-701) Exam Objectives Version 5.0 準拠)

発行

IT資格道場(https://www.shikaku-doujou.com)

お問い合わせ

info@shikaku-doujou.com