Google Cloud

Professional Cloud Security Engineer

認定試験ガイド

Cloud Security Engineer は、組織が Google Cloud で安全なワークロードとインフラストラクチャを設計して実装できるように支援します。セキュリティに関するベスト プラクティスと業界の要件についての知識を活かしながら、Google のセキュリティ技術を利用して安全なソリューションを設計、開発、管理します。Cloud Security Engineer は、Identity and Access Management、組織のセキュリティ構造とポリシーの定義、Google Cloud テクノロジーを使用したデータ保護の提供、ネットワークセキュリティの防御の構成、脅威に対応するための環境のモニタリング、セキュリティの自動化、AI セキュリティ、安全なソフトウェア サプライ チェーン、規制管理の適用に習熟しています。

セクション **1:** アクセスの構成（試験内容の約 **25%**）

1.1 Cloud Identity を管理する。以下のような点を考察します。

- Google Cloud Directory Sync とサードパーティ コネクタの構成
- 特権管理者アカウントの管理
- ユーザー ライフサイクル管理プロセスの自動化
- プログラムを使用したユーザー アカウントとグループの管理
- Workforce Identity 連携の構成

1.2 サービス アカウントを管理する。以下のような点を考察します。

- サービス アカウント（デフォルトのサービス アカウントを含む）のセキュリティ確保と保護
- サービス アカウントが必要なシナリオの特定
- サービス アカウントの作成、無効化、承認
- サービス アカウント キーの保護、監査、使用の制限
- 有効期間の短い認証情報の管理と作成
- Workload Identity 連携の構成
- サービス アカウントの権限借用の管理

1.3 認証を管理する。以下のような点を考察します。

- ユーザー アカウントのパスワードおよびセッション管理ポリシーの作成
- Security Assertion Markup Language（SAML）と OAuth の設定
- 2 段階認証プロセスの構成と適用。

1.4 認可制御を管理、実装する。以下のような点を考察します。

- Identity and Access Management（IAM）のロールと権限による特権ロールと職掌分散の管理

- IAM とアクセス制御リスト（ACL）の権限の管理
- IAM 条件や IAM 拒否ポリシーを使用した、さまざまな種類の ID への権限の付与
- 組織、フォルダ、プロジェクト、リソースレベルでの ID ロールの設計
- Access Context Manager の構成
- ポリシー インテリジェンス を適用した権限管理の改善
- グループを通じた権限の管理

1.5 リソース階層を定義する。以下のような点を考察します。

- 大規模な組織の作成と管理
- 組織のフォルダ、プロジェクト、リソースの組織のポリシーの管理
- リソース階層を使用したアクセス制御と権限の継承

セクション **2:** 通信の保護と境界保護の確立（試験内容の約 **20%**）

2.1 境界セキュリティを設計して構成する。以下のような点を考察します。

- ネットワークの境界制御の構成（ファイアウォール ルール、階層型ファイアウォール ポリシー、Identity-Aware Proxy（IAP）、ロードバランサ、Certificate Authority Service）
- プライベート IP アドレスとパブリック IP アドレスの区別
- ウェブ アプリケーション ファイアウォールの構成（Google Cloud Armor）
- Secure Web Proxy のデプロイ
- Cloud DNS セキュリティ設定の構成
- 構成された API の継続的なモニタリングと制限

2.2 境界セグメントを構成する。以下のような点を考察します。

- VPC ネットワーク、VPC ピアリング、共有 VPC、ファイアウォール ルールのセキュリティ プロパティの構成
- N 層アプリケーション用のネットワーク分離とデータのカプセル化の構成
- VPC Service Controls の構成

2.3 プライベート接続を確立する。以下のような点を考察します。

- VPC ネットワークと Google Cloud プロジェクトの間のプライベート接続の設計と構成（共有 VPC、VPC ピアリング、オンプレミス ホスト用のプライベート Google アクセス）
- データセンターと VPC ネットワークの間のプライベート接続の設計と構成（HA-VPN、IPsec、MACsec、Cloud Interconnect）
- VPC と Google API の間のプライベート接続の確立（プライベート Google アクセス、オンプレミス ホスト用のプライベート Google アクセス、制限付き Google アクセス、Private Service Connect）
- Cloud NAT を使用した送信トラフィックの有効化

セクション **3:** 確実なデータ保護（試験内容の約 **23%**）

3.1 センシティブ データを保護し、データ損失を防止する。以下のような点を考察します。

- 個人情報（PII）の検査と秘匿化
- センシティブ データ（構造化データと非構造化データ）の継続的な検出の確立
- 仮名化の構成
- フォーマット保持暗号化の構成
- BigQuery、Cloud Storage、Cloud SQL のデータストアへのアクセスの制限
- Secret Manager でのシークレットの保護
- コンピューティング インスタンス メタデータの保護と管理

3.2 保存データ、転送中のデータ、使用中のデータの暗号化を管理する。以下のような点を考察します。

- Google のデフォルトの暗号化、顧客管理の暗号鍵（CMEK）、Cloud External Key Manager（EKM）、Cloud HSM のユースケースの特定
- CMEK と EKM の暗号鍵の作成と管理
- ユースケースへの Google の暗号化アプローチの適用
- Cloud Storage のオブジェクト ライフサイクル ポリシーの構成
- Confidential Computing の有効化

3.3 AI におけるセキュリティとプライバシーを計画する。以下のような点を考察します。

- AI / ML システムのセキュリティ管理の実装による、データやモデルの意図しない不正使用の防止
- IaaS および PaaS でホストされたトレーニング モデルのセキュリティ要件の決定

セクション **4:** オペレーションの管理（試験内容の約 **20 %**）

4.1 インフラストラクチャとアプリケーションのセキュリティを自動化する。以下のような点を考察します。

- 継続的インテグレーションと継続的デリバリー（CI / CD）のパイプラインによる、共通脆弱性識別子（CVE）に対するセキュリティ スキャンの自動化
- GKE クラスタまたは Cloud Run を保護するための Binary Authorization の構成
- 仮想マシンイメージの作成、強化、メンテナンス、パッチ管理の自動化
- コンテナ イメージの作成、検証、強化、メンテナンス、パッチ管理の自動化
- ポリシーとドリフト検出の大規模な管理（Security Health Analytics のカスタム組織のポリシーとカスタム モジュール）

4.2 ロギング、モニタリング、検出を構成する。以下のような点を考察します。

- ネットワーク ログの構成と分析（ファイアウォール ルール ロギング、VPC フローログ、Packet Mirroring、Cloud Intrusion Detection System（Cloud IDS）、ログ分析）
- 効果的なロギング戦略の設計
- セキュリティ インシデントのロギング、モニタリング、対応、修正
- ログへの安全なアクセスの設計
- 外部セキュリティ システムへのログのエクスポート
- Google Cloud Audit Logs とデータアクセス ログの構成と分析
- ログのエクスポートの構成（ログシンクと集約シンク）
- Security Command Center の構成とモニタリング

セクション **5:** コンプライアンス要件のサポート（試験内容の約 **12%**）

5.1 クラウドの規制要件を決定する。以下のような点を考察します。

- コンピューティング、データ、ネットワーク、ストレージに関する懸念事項の特定
- 責任共有モデルの評価
- コンプライアンス要件をサポートするためのクラウド環境内のセキュリティ管理の構成（データとサービスのリージョン化）
- 規制遵守のためのコンピューティングとデータの制限（Assured Workloads、組織のポリシー、アクセスの透明性、アクセス承認）
- 規制遵守のための Google Cloud 環境の決定