IT資格道場

GCP PSOE 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)

Google Cloud 公式 Professional Security Operations Engineer Exam Guide 2.0
(2026-11-15 取得)準拠
2026年11月版

SAMPLE

ご利用にあたって

- このテキストは「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。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの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。

SAMPLE

目次

3点セットの使い方

この教材の使い方

第1章 プラットフォーム運用 [1.1/1.2]

- テレメトリー ソースの優先順位 [1.1]
- 補い合うツールの使い分け [1.1]
- Content Hub の構築済みツール [1.1]
- 検出カバレッジの評価と穴の発見 [1.1]
- AI・自動化・クラウドのツールで強める [1.1]
- UDM 検索と stats 検索 [1.1]
- IOC と TTP の評価と統合 [1.1]
- 認証の構成（SCC・SecOps・MCP）[1.2]
- 機能アクセスの認可（機能 RBAC）[1.2]
- データアクセスの認可（データ RBAC）[1.2]
- 監査ログの構成と分析 [1.2]
- 自動化のための API アクセス [1.2]
- Workforce Identity 連携による ID のプロビジョニング [1.2]

サンプルはここまでです

SAMPLE

3点セットの使い方

種類	役割
① 学習用テキスト	これだけで問題が解けるようになる本編
② 頻出度別ノート	テキストを読んだら次はこれ。頻出順に絞った問題と解説で「解ける」に橋渡し。試験直前の最終チェックにも
③ 暗記用ノート	覚えるべき要点だけを一問一答に凝縮。空き時間の反復と用語の再確認用

使い方: ① 学習用を読む → ② 頻出度別で解き方を掴む → ③ 問題演習で腕試し → ④ 頻出度別に戻って再確認(試験直前もここ)。暗記用は空き時間や用語の再確認に。

このテキストの位置づけ: ①の学習用テキストです。まずはここを通読し、これだけで問題が解けるようになることを目標にしてください。

SAMPLE

この教材の使い方

このテキストは、Google Cloud が実施する **Professional Security Operations Engineer 認定** の合格を目的に作られています。

Professional 級の試験が問うのは、個々の製品の説明ではありません。**要件と制約を読み取り、複数の選択肢の中から最も適切な検出・調査・対応の判断を選べること**です。Exam guide の各セクションに沿って、「どの場面でどれを選ぶか・なぜ他は不適か」を本文に書き込んでいます。

試験の基本情報

項目	内容
試験名	Google Cloud Certified – Professional Security Operations Engineer
実施	Google Cloud（テストセンター、またはオンライン監督試験）
問題数	**50問**
試験時間	**120分**
出題形式	**択一（multiple choice）。複数を選ぶ問もある**
合格ライン	合否のみ通知
受験言語	英語・日本語

出題数・試験時間・試験ガイドは改定されることがあります。 お申し込みの前に、Google Cloud 公式サイトで最新の情報をご確認ください。

SAMPLE

章の並びは、Exam guide の並びとまったく同じです。節見出しの末尾にある `[1.1]` のような番号は、Exam guide のセクション番号です。Google Cloud はセクションごとの割合だけを公表しており、細目単位の出題数は公表していません。

サービス名・機能名は英語のまま覚えてください。本文では、製品名・機能名・用語を英語表記のまま書いています。本番の設問文と選択肢に出るのはこの表記であり、日本語訳だけを覚えても画面では出会いません。

出題範囲の全体像：6つのセクション

セクション	分野	採点対象に占める割合（公式）	対応する章
1	Platform operations	**13%**	第1章
2	Data management	**20%**	第2章
3	Threat hunting	**18%**	第3章
4	Detection engineering	**20%**	第4章
5	Incident response	**18%**	第5章
6	Observability	**11%**	第6章

SAMPLE

第1章 プラットフォーム運用 [1.1/1.2]

この章は、Google SecOps・Security Command Center（SCC）・Google Threat Intelligence（GTI）の3製品を、検出と対応の土台として動かす作業を扱います。前半の 1.1 は、何を取り込み、どの手段で検出し、どの脅威インテリジェンスで裏付けるかを決め、後半の 1.2 は、人と人以外の ID に、どの認証で、どの権限とデータ範囲を与えるかを決めます。

製品	役割	検出の材料
Google SecOps	SIEM（検索・検出ルール）と SOAR（プレイブック・ケース）	取り込んだログを UDM に正規化したイベント
SCC	脆弱性・設定ミス・脅威を finding として出す	Cloud Logging のログと資産のメタデータ
GTI	IOC・脅威アクター・TTP・スコアを出す	Google・Mandiant・VirusTotal の知見

テレメトリー ソースの優先順位 [1.1]

テレメトリー ソース（テレメトリ源）は、見つけたいものから逆算して入れる順を決めます。

見つけたいもの	先に入れる源	理由
不審な API 操作（権限昇格・漏えいした鍵の使用）	Cloud Audit Logs	Admin Activity 監査ログは常に書かれ、無効にできない
設定ミス・脆弱性・攻撃経路	SCC の finding	SCC が資産を評価して出す

SAMPLE

見つけたいもの	先に入れる源	理由
ブラウザー側の兆候（拡張機能・不審 URL・機密データの転送）	Chrome Enterprise のログ	ログタイプは CHROME_MANAGEMENT
既知の悪性 IP・ドメイン・ハッシュ	GTI	IOC と判定とスコアを照合に使う

SCC は3つの階層（ティア）で機能が変わります。

- Standard: 無料。基本の態勢管理だけ
- Premium: Standard に攻撃経路・脅威検出・コンプライアンス監視を足す。対象は Google Cloud だけで、プロジェクトか組織で有効にする
- Enterprise（非推奨）: 組織でしか有効にできない。2027-05-21 に終了し、Premium へ自動で移る

脅威検出の Event Threat Detection（ETD）は Premium の機能です。ETD は Cloud Logging のログの流れを読みます。組織で Premium を有効にすると、新しいプロジェクトのログも対象になります。Google Workspace のログも監視できます。[1]

ETD が finding を出すには、検出器ごとに決まったログが要ります。ETD のためにログを有効にするのは、次の3つがすべて当てはまる時だけです。

- その製品を使っている
- その製品を守る必要がある
- そのログが、Data Access 監査ログのように既定で無効のログである

同じ脅威を有効なログで見つけられるなら、別のログは足しません。ETD が一覧に載せていないログは、有効にしても読みません。組織レベルでしか使え

SAMPLE

ないログもあります。SCC をプロジェクトで有効にした場合、そのログは読まれず finding も出ません。

マルウェアのネットワーク検出は、Cloud DNS・Cloud NAT・Firewall Rules Logging・VPC Flow Logs のどれか1つで足ります。Cloud DNS のログがあれば、ドメイン解決だけでマルウェアを見つけられます。[2]

SecOps へ送る道は2つです。直接取り込みは、特別な Cloud Logging フィルタで、Cloud Audit Logs・Cloud DNS・Cloud NAT などをリアルタイムで送ります。SCC Premium の finding も同じ道です。フィルタを設定した時点からのログだけが対象で、VPC Flow や DNS のような量の多いログに向きます。名前空間とラベルは付けられません。

Cloud Storage 経由は、正規表現の除外フィルタで必要なログだけを通せます。取り込み量の課金を抑えたい場合に選びます。ただし Cloud Storage の費用が別にかかり、取り込みは定期の実行で即時ではありません。SCC の finding は、ingestion label でパーサーが決まります。GCP_SECURITYCENTER_THREAT、_MISCONFIGURATION、_VULNERABILITY、_OBSERVATION、_TOXIC_COMBINATION などです。[3]

Chrome のログは、Chrome Enterprise reporting connector が SecOps へ送ります。前提は Chrome 137 以降で、それより前は参照元 URL が完全ではありません。Chrome Enterprise Premium なら、拡張機能のインストール、機密データの転送、不審 URL などのログも転送できます。高度なログには Premium のライセンスが要ります。[4]

補い合うツールの使い分け [1.1]

検出手段は、検出カバレッジの要件に合わせて組み合わせます。

SAMPLE

手段	向く検出	向かない検出
Cloud Logging のログベース アラート	特定のログ1件が出たらすぐ通知（監査ログの特定メッセージなど）	件数の集計（ログベース指標を使う）。除外したログ
SCC の組み込み検出器（ETD など）	Google が管理する既知の脅威パターン。ルールを書かずに使う	自社固有の条件。足りない分は ETD のカスタム モジュールか、BigQuery へ出して SQL で探す
SecOps のルール（YARA-L）	複数のログ源をまたぐ相関と、期間をまたぐ集計	取り込んでいないログの検出

プロジェクトのシンクが、そのプロジェクトで生まれたログをログ バケットへ送る時は、そのプロジェクトのログベース アラートがそのログを走査します。シンクで運ばれるログは、ログベース アラートの対象の内側です。[5]

SecOps には、Google が管理する curated detection もあります。新しい rule set は既定で無効（Status が Disabled、Alerting が Off）で、有効にしない限り通知されません。例外は Applied Threat Intelligence の rule set で、Enterprise Plus では自動で有効になります。

既存の rule set に足された新ルールは、親の設定を引き継ぎます。更新されたルールは、自分の設定を保ちます。1つの rule set には、2種類のルールが入ることがあります。

- Precise: 確度の高い検出
- Broad: 不審な振る舞いまで広く拾う。誤検知も増える

有効化と通知は、この2種類ごとに別々に切り替えられます。[6]

SAMPLE

場面で選ぶ例です。Google Cloud の管理者が IAM ポリシーを変えた時に即座に知りたいなら、監査ログを条件にしたログベース アラートが最短です。既知の攻撃手法の兆候を、ルールを書かずに広く拾いたいなら ETD です。

Okta のサインインの失敗と Google Cloud の特権操作を、同じユーザーで結び付けたい場合は、どちらでも足りません。2つのログを SecOps へ取り込み、ルールで相関させます。ログベース アラートは、条件に合うログが現れた時に通知する仕組みで、別のログ源との突き合わせはできないためです。[7]

Content Hub の構築済みツール [1.1]

Content Hub は、Google SecOps の内容を探して入れて管理する場所です。コンテンツの種類は4つあります。Google は、Google が開発・保守・検証した物です。Partner と Community は、パートナーやコミュニティが保守し、自動の品質検査を通った物です。Custom は自分で作った物で、自分の Content Hub にだけ表示され、Google は検証しません。

Content Pack は、ログの取り込み、curated detection、ダッシュボードをまとめて入れる単位です。Google は、旧来のユースケースより Content Packs を勧めています。

入れた後の作業には順番があります。プレイブックを使う前に、Configure Integrations でインテグレーションのインスタンスを設定します。ルールの定義は Content Hub から変更できません。変えたい場合は、Rules ページで新しいルールを作ります。誤検知を減らす調整には、ルールの除外（rule exclusion）を使います。評価の対象から外す条件を決める機能です。[8]

SAMPLE

検出カバレッジの評価と穴の発見 [1.1]

既存ツールの有効性は、MITRE ATT&CK マトリクスで見ます。場所は Detection > Rules & Detections の MITRE ATT&CK Matrix タブで、列が tactic、カードが technique で、カードの色が検出カバレッジの状態と深さを示します。[9]

自作ルールを数えさせるには、メタデータに technique ID を書きます。たとえば `technique="T1548,T1134.001"` です。technique ID を書かないルールは、マトリクスの数に入りません。新しいルールは数分で出ます。[10]

穴の見つけ方は3つあります。

- ルール数が 0 で、ログタイプ数が出ているカード。データは既にあり、ルールだけが無いので、新しい検出の候補になる
- 新しい脅威情報で technique を絞り込んだ結果。たとえば T1486 の暗号化ランサムウェアが No Coverage なら、優先して塞ぐ穴
- ルールがあっても誤検知が多い technique。詳細のデータ ソース欄で、より精度の高い源（EDR など）に切り替えられないかを見る

AI・自動化・クラウドのツールで強める [1.1]

SecOps Chat は、Gemini の対話アシスタントです。自然言語から YARA-L の検索クエリを作り、結果を要約します。検出ルールも作れますが、単一イベントのルールに限ります。複数イベントのルールは作れません。脅威インテリジェンスの質問にも答えます。Agentic Chat を有効にすると、SecOps のツールを呼んで答えます。参照できるデータは、利用者の IAM ロールとデータのスコープで決まります。[11]

SAMPLE

Triage and Investigation Agent（TIN）は、alert が真か偽かを判定し、理由を要約します。1件の調査は平均 60 秒で、最長 20 分です。既定では alert の 5 分後に始まり、この待ち時間は最大 20 分まで延ばせます。対象は、SIEM に取り込んだデータの alert です。SOAR のコネクタが持ち込んだ alert は処理しません。調査には、動的な検索、GTI によるエンリッチメント、コマンドライン分析、プロセスツリーの再構成を使います。[12]

自動化は、SOAR のプレイブックと、通知の流れで作ります。SCC Premium を組織のレベルで有効にしていれば、SCC は finding を Cloud Logging のプロジェクトへ書け、そこから Pub/Sub で外へ出せます。Pub/Sub から Cloud Run functions へ渡せば、finding に応じた処理を自動で動かせます。[13]

UDM 検索と stats 検索 [1.1]

SIEM Search の検索の種類は7つで、種類ごとに期間の上限があります。上限は、テナントのログ保持期間にも制限されます。

種類	最大の期間
UDM・RAW・ECG	365 日
JOIN	内部結合 90 日。条件のない内部結合と外部結合は 14 日
STATS	90 日
CASE・CASE HISTORY	90 日

実行モードは2つあります。

- Basic（既定）: 高速なイベント取得と条件の試行錯誤に向く。仮説を広い期間でためす場面で使う

SAMPLE

- Advanced: タイムライン、ヒートマップ、prevalence、関連する検出を見たい時に使う

クエリの方言は、YL2（YARA-L・既定）と SQL（GoogleSQL）です。最大の期間は、YARA-L の検索が 365 日、SQL が 90 日です。1回のクエリで使える UDM フィールドは 100 までです。[14]

stats 検索は、YARA-L 2.0 と同じ構造で書きます。構造は、フィルタ、match（グループ化するフィールド）、outcome（出力）、dedup、order、limit の順です。order を指定しないと昇順になり、limit を超えた行は返しません。公式の例は、OKTA のログを IP ごとにまとめ、ユーザー数の多い順に 20 件を返します。

```
metadata.log_type = "OKTA"
match:
  principal.ip
outcome:
  $user_count_by_ip = count(principal.user.userid)
order:
  $user_count_by_ip desc
limit:
  20
```

集計関数は、array、array_distinct、avg、count、count_distinct、earliest、latest、max、min、stddev、sum の11個です。array 系が返す要素はランダムに切り詰められ、上限は、検索で 1,000 個、ダッシュボードとルールで 25 個です。[15]

SAMPLE

値のない UDM フィールドは NULL になりません。`""`、0、UNKNOWN_ACTION のゼロ値になります。そのため count_distinct は、空の値を1種類として数え、合計を1つ増やします。events 側に `$userid != ""` のような絞り込みを入れて除きます。繰り返しフィールドは `any` を付けて絞り込みます。[16]

stats の結果は、取り込みの処理が終わってから出ます。直近のイベントが数字に入らない遅れがあります。[17]

追加の権限が要る操作は、次の3つです。

操作	追加で要る権限
エンリッチ済みの拡張イベントの詳細	chronicle.events.fetchEnrichedEvent
検索の保存と検索ビューの編集	chronicle.savedSearches.update と chronicle.searchViews.update
ケース履歴の検索	chronicle.cases.get と chronicle.cases.list

データ RBAC が有効なら、見えるのは自分のスコープに合うデータだけです。UDM イベント、生ログ、alert、検出、ケースが対象です。[18]

IOC と TTP の評価と統合 [1.1]

SecOps は、取り込んだログを UDM に正規化した直後から、IOC のフィードと自動で照合します。照合は2通りで、新しいログをリアルタイムで当てる方法と、新しい IOC が入った時に過去を遡る方法です。遡りの範囲は、保持期間（ふつう 1 年）の過去データ全体です。[19]

自動の照合は、主にドメインと IP が対象で、ファイルのハッシュ（MD5、SHA-256、SHA-1）も照合します。結果は、Alerts & IOCs の IOC Matches に出ます。

SAMPLE

20

IOC は版を持ちます。Alerts & IOCs のページは、期限のない版は有効なまま残り、期間つきの版が入るとその期間だけ上書きすると書きます。上書きは開始の 5 日前から効き、期限が切れれば前の版に戻ります。脅威フィードの統合のページは、終了時刻の無い指標を自動の照合が評価しないと書くので、取り込む時は開始と終了の両方を埋めておきます。この版の話は IOC の有効期間の話で、entity graph の項目が取り込みの前後約 5 日だけ有効という期限と同じではありません。21

自作のルールで脅威インテリジェンスと突き合わせるなら、entity graph（Entity Context Graph）を使います。Google 提供のコンテキストは GLOBAL_CONTEXT、自分で取り込む IOC は ENTITY_CONTEXT です。

entity graph の項目は、既定で取り込み時刻の前後およそ 5 日だけ有効です。続けて照合するには、コンテキストを少なくとも 5 日ごとに取り込み直します。metadata.threat フィールドを持つ entity には、この期限がかかりません。過去の IOC 照合に向きます。データ RBAC が有効な環境では、見える IOC 一致は触れるアセットの分だけです。22

IOC の有効性は、GTI の判定で評価します。GTI は、verdict と severity の組から 0 から 100 の Threat Score を出します。

- verdict: Malicious、Suspicious、Undetected、Benign、Unknown の5つ
- severity: High、Medium、Low、None の4つ

判断の基準は Threat Score と verdict です。GTI Confidence Score は、機械学習の確からしさを示す補助の証拠です。23

SAMPLE

verdict と severity	Threat Score
Benign	0
Undetected	1
Suspicious（Low・Medium・High）	21・25・29
Malicious・Low	30 から 59
Malicious・Medium	60 から 79
Malicious・High	80 から 100

Suspicious の High が 29 で止まるのは、無力化されたり休眠したりした高い影響の脅威だからです。自動のブロックは起こさず、analyst の注意だけを残します。Confidence Score は、95 より大きいと Critical、80 から 95 が High の確度です。

GTI_IOC フィードに入る IOC は、次のうち1つ以上を満たす物だけです。

- GTI Confidence Score が 80 以上
- verdict が malicious
- 既知の脅威との関連がある

条件を満たす未レビューの IOC も取り込まれます。ただし metadata.threat.stable = false が付き、検証後に true になります。[24]

用途に合う GTI の統合は、ライセンスで分かれます。

SAMPLE

状況	使う統合
Enterprise Plus	Applied Threat Intelligence（ATI）。Google が管理するパイプラインで IOC を当て、Mandiant の知見で alert に優先度を付ける
Standard か Enterprise で GTI のライセンスがある	BYOL 統合。自分で Cloud Run functions、Cloud Scheduler、Secret Manager を配置する
検索や判定を手で深掘りする	GTI の画面と SOAR の GTI 統合

ATI の優先度モデルは4つです。

- Active breach: Mandiant が侵害の調査で観測した IOC。verdict が Malicious、severity が High
- High: 侵害の調査では見ていないが、脅威アクターやマルウェアに関連づけられた IOC
- Medium: Malicious で High の IOC のうち、Mandiant の調査で見ていない物。量が多いため、通知を切って運用するよう勧められる
- Inbound IP address authentication: 内部へ認証してきた外部 IP

ATI の curated detection には、複数の ATI alert を1つにまとめる composite ルールもあります。[25]

BYOL は、データを GCP_THREATINTEL のログタイプで UDM に正規化します。Third-party vendor alerts の Google Threat Intelligence (BYOL) rule set を有効にして使います。Enterprise Plus でも BYOL は使えます。ただし勧められるのは ATI です。[26]

SAMPLE

GTI 側の道具は2つです。IoC Stream は、購読したコレクションや脅威アクターに合致した IOC の通知で、30 日で自動削除されます。Threat Profile は、対象の業界や地域などを決めて、関連する脅威を推薦させる機能です。推薦の精度のため、期間は 90 日以上にします。[27]

TTP は、BYOL が取り込む MITRE ATT&CK の対応づけと、Threat Profile の TTP 分析で評価します。[28]

認証の構成（SCC・SecOps・MCP）[1.2]

SecOps の利用者の認証は、Cloud Identity、Google Workspace、Workforce Identity 連携のどれかを仲立ちにします。前提は、SecOps を Google Cloud のプロジェクトに結び付けることです。IAM のポリシーは、そのプロジェクトのレベルで定義するよう勧められます。[29]

外部の IdP は、SAML 2.0 か OIDC に対応していれば使えます（Okta、Microsoft Entra ID、AD FS など）。SecOps が扱うのは SP-initiated の SAML だけです。IdP の画面から始める IdP-initiated のログインは扱いません。[30]

SCC は、Google Cloud コンソールで IAM のロールを付けて使います。SCC Enterprise 階層の利用者が SecOps のコンソールで SCC の機能を見る場合は、少なくとも Security Center Admin Viewer（roles/securitycenter.adminViewer）が要ります。SCC のロールは組織で付けます。[31]

MCP は、AI アプリケーションが SecOps のツールを呼ぶ接続です。リモート MCP サーバーは、Google SecOps API（Chronicle API）を有効にすると使えます。認証は OAuth 2.0 と IAM で、スコープは `https://www.googleapis.com/auth/chronicle` です。[32]

SAMPLE

ツールを呼ぶ利用者には、MCP Tool User（roles/mcp.toolUser）と、Chronicle API のロール（roles/chronicle.admin など）が要ります。Gemini Enterprise と接続する場合は、Chronicle API Viewer、MCP Tool User、Service Usage Consumer のロールです。エンドポイントは、地域のドメインの末尾に /mcp を付けた `https://us-chronicle.googleapis.com/mcp` のような URL です。トランスポートは Streamable HTTP です。リダイレクト URI は独自の値を使えません。

SecOps のサインインに使う Workforce Identity 連携のプロバイダは、Google Cloud ホストの MCP の認証には使えません。MCP 用に別のプロバイダを作ります。外部 IdP の利用者は、先に連携した ID で gcloud CLI にサインインします。本番では自分の ID を使わず、権限を絞った別の agent か workload の ID を使います。[33]

機能アクセスの認可（機能 RBAC）[1.2]

機能 RBAC は、IAM のロールと権限で、使える機能を決めます。UDM の個々のレコードやフィールドへのアクセスは制御せず、それはデータ RBAC の役割です。権限名は SERVICE.FEATURE.ACTION の形で、chronicle.dashboards.edit なら、サービス名が chronicle、機能が dashboards、操作が edit です。事前定義ロールと違う権限の組み合わせが要る場合は、カスタム ロールを作ります。[34]

ロール	内容
roles/chronicle.admin	グローバル設定を含む全アクセス
roles/chronicle.editor	変更のアクセス
roles/chronicle.viewer	読み取りのみ
roles/chronicle.limitedViewer	読み取り。検出ルールと retrohunt を除く

SAMPLE

ロール	内容
roles/chronicle.soarAdmin	SOAR のアプリケーションと API サービスへの、グローバル設定を含む全アクセス

同じプロジェクトに SecOps 以外のサービスもある場合、Project IAM Admin の担当者を SecOps だけに絞るには、許可ポリシーに IAM 条件を足し、付与できるロールを limitedViewer、viewer、editor、admin の4つに限ります。

```
api.getAttribute(iam.googleapis.com/modifiedGrantsByRole,
[]).hasOnly([roles/chronicle.googleapis.com/limitedViewer,
roles/chronicle.googleapis.com/viewer,
roles/chronicle.googleapis.com/editor,
roles/chronicle.googleapis.com/admin])
```

この条件が付いた担当者は、4つ以外のロールを付与できません。[35]

データアクセスの認可（データ RBAC）[1.2]

データ RBAC は、利用者を scope に結び付けて、見えるデータを絞ります。scope は label で定義し、標準の label は名前空間（任意）、取り込みのメタデータ（任意）、ログタイプ（必須）です。自分で作る custom label も使えます。

custom label の名前は一意で 63 文字まで、使えるのは小文字・数字・ハイフンだけです。クエリの実行は 5 秒までで、データ テーブルやエンリッチメントのフィールドは使えません。scope と custom label は、それぞれ 200 種類までです。ラベルが付くのは新しく取り込むデータだけで、取り込み済みのデータには付きません。

SAMPLE

1つの scope には、許可の label と、任意で拒否の label を入れます。同じ種類の許可（ログタイプ同士）は OR、違う種類（ログタイプと名前空間）は AND で結びます。拒否は常に許可に勝ち、複数の拒否は OR で、どれか1つに合えば拒否です。エンリッチされたイベントは、元のイベントが scope に入らないか、エンリッチの label が拒否に当たる場合は見えません。[36]

scope を管理するには、Role Viewer（roles/iam.roleViewer）が要ります。

利用者の種類は2つです。

- scoped user: Chronicle API Restricted Data Access（roles/chronicle.restrictedDataAccess）と、事前定義かカスタムのロールを付けた人
- global user: このロールを付けない人。全データが見える

同じ人にグローバルとスコープの両方を付けると、グローバルが勝ちます。カスタムでグローバルに触らせるには、カスタム ロールに chronicle.globalDataAccessScopes.permit を足します。scope 用のカスタム ロールには、chronicle.dataAccessScopes.list を含めます。chronicle.DataAccessScopes.permit と chronicle.globalDataAccessScopes.permit は含めません。Editor や Admin を土台にすると、混ざりやすい権限です。[37]

scope を人に割り当てるのは、IAM 条件です。restrictedDataAccess の付与に条件を足し、リソース名（scope 名）が ENDS_WITH、STARTS_WITH、EQUALS_TO に合うかで決めます。完全に一致させるには、ENDS_WITH の値の前に / を付けます。付けないと、testscopename のような別の名前にも合います。[38]

SAMPLE

1つの付与に足せる条件は 12 個までで、超える場合は付与を分けます。条件つきの付与は、同じロールの条件なしの付与を上書きできません。空のグループに割り当てた scope は、誰にも効きません。

有効化には2通りあります。データ RBAC を有効にしてから scope を割り当てる場合、scoped user は最初は何も見えません。scope を先に割り当ててから有効にする場合は、有効にした瞬間からデータが見えます。有効にする前は、scope を持つ人も含めて全員がグローバルで、全データが見えます。

有効化は、Settings > Access Management > Data Access の Assignments タブで Enforce data access を押します。ダッシュボードは、roles/chroniclesiem.restrictedViewer を付けた人なら、表示が scope で絞られます。[39]

監査ログの構成と分析 [1.2]

Cloud Audit Logs は4種類です。

種類	既定	止められるか
Admin Activity	常に書かれる	構成・除外・無効化できない
Data Access	BigQuery を除き無効	有効化して使う
System Event	常に書かれる	構成・除外・無効化できない
Policy Denied	既定で有効	無効にできないが、除外フィルタで保存を止められる

Admin Activity と System Event は _Required バケットに入ります。Data Access と Policy Denied は _Default バケットに入ります。ログ名は `projects/PROJECT_ID/logs/cloudaudit.googleapis.com%2Factivity` のように、/logs/ の後ろを URL エンコードし、/ は %2F と書きます。[40]

SAMPLE

読む権限にも違いがあります。Logs Viewer（roles/logging.viewer）では、_Default バケットの Data Access ログを読めません。Private Logs Viewer（roles/logging.privateLogViewer）が要ります。Editor ロールにも、その権限は入っていません。

Data Access を有効にするには、IAM ポリシーの auditConfigs を編集します。設定できるのは組織・フォルダ・プロジェクトで、請求先アカウントは gcloud CLI で設定します。権限の種類は ADMIN_READ、DATA_READ、DATA_WRITE で、特定の principal を記録の対象外にもできます。有効にすると、ログの量と課金が増えます。[41]

設定は階層ごとの和集合になります。同じ階層で、サービス全体（allServices）の設定と特定のサービスの設定が両方ある時も、そのサービスの設定は 2 つの和集合です。上位の組織やフォルダで有効にしたログは、下位で無効にできません。上位に入れた除外の principal も、下位で外せません。MCP サーバーの呼び出しは、mcp.googleapis.com の Data Access ログで記録します。[42]

SecOps 自身の監査ログは、サービス名が 3 つあります。chronicle.googleapis.com、chronicleservicemanager.googleapis.com、malachitefrontend-pa.googleapis.com です。リソースタイプは audited_resource です。

SecOps の Admin Activity は、常に有効で無効にできません。Data Access は既定で有効です。Google Cloud の他のサービスとは、既定が逆です。利用者が実行した検索のクエリ（UDM 検索と生ログ検索）を残すには、設定が1つ要ります。IAM & Admin の Audit Logs で、Chronicle API と Chronicle Service Manager API の権限の種類（Admin Read、Data Read、Data Write）を全部選びます。[43]

SAMPLE

分析で読むフィールドは4つです。

- protoPayload.authenticationInfo.principalSubject: 実行した人
- protoPayload.methodName: 呼ばれた API
- protoPayload.status: 結果。空が成功、コード 7 が権限の拒否
- protoPayload.authorizationInfo: 確認された権限名と、許可か拒否か

Logs Explorer では、Admin Activity は log name の activity、Data Access は data_access を選びます。[44]

自動化のための API アクセス [1.2]

Chronicle API は OAuth 2.0 で認証します。クライアント ライブラリは Application Default Credentials（ADC）を使い、REST は gcloud の認証情報か ADC を使います。ローカルでは、gcloud auth application-default login で ADC を作ります。[45]

権限を試す時は、サービス アカウントの偽装（impersonation）を使います。偽装には、iam.serviceAccounts.getAccessToken を含む Service Account Token Creator（roles/iam.serviceAccountTokenCreator）が要ります。Google Cloud 上で動く処理には、実行するリソースにサービス アカウントを付けるのが望ましい方法です。API キーは、呼び出しを課金とクォータのためにプロジェクトへ結び付けるだけです。呼び出した人の ID は決めません。Chronicle API で API キーが使えるメソッドは、projects.locations.instances.feeds.importPushLogs だけです。[46]

旧 API には終了の日付があります。Backstory API と Ingestion API は、2027-07-20 に止まります。移行先は Chronicle API で、認証は API トークン

SAMPLE

とサービス アカウントの認証情報から OAuth 2.0 に変わります。サービス アカウントと IAM は自分で管理できます。

Backstory API は、Google が管理するプロジェクトのサービス アカウントでしか動きません。自分のプロジェクトのサービス アカウントを使うと、API が有効でないというエラーになります。SOAR の旧 API と AppKey の認証は、2027-03-31 に止まります。[47]

SCC の finding を SOAR へ送るには、サービス アカウントを2つ使います。利用者側のサービス アカウント（user service account）には、プロジェクトで Pub/Sub Editor を付けます。組織では、次の4つのロールを付けます。

- Security Center Admin Viewer
- Security Center Notification Configurations Editor
- Organization Viewer
- Cloud Asset Viewer

SOAR 側のサービス アカウントには、利用者側のサービス アカウントに対する Service Account Token Creator を付け、偽装させます。SOAR をオンプレミスで動かす場合だけ、利用者側のサービス アカウントのキー（JSON）を作って渡します。finding の送信は、SCC API を有効にし、Pub/Sub のトピックを作り、そのトピックを使う NotificationConfig を作って設定します。NotificationConfig には、送りたい finding の絞り込み条件を入れます。[48]

GTI の API キーには、個人のキーと、グループの管理者が作るサービス アカウントのキーがあります。連携にはサービス アカウントのキーが向きます。特定の個人に結び付かず、メールアドレスも要らないためです。[49]

個人のキーの更新（rotate）は、24 時間に1回までです。更新すると、古いキーの要求はすぐ拒否されます。旧 Mandiant の連携は、api_key（API Key ID）を

SAMPLE

文字列 gti-user に置き換えます。api_secret（API Secret）は、GTI のサービスアカウントの API キーに置き換えます。[50]

Workforce Identity 連携による ID のプロビジョニング [1.2]

Workforce Identity 連携は、外部の IdP の利用者を Google Cloud の ID として扱う仕組みです。ユーザー アカウントは Google Cloud に保存しません。IdP からの同期の道具（Google Cloud Directory Sync など）は要りません。これを sync-less と呼びます。対象は人の利用者で、自動化の処理には Workload Identity 連携を使います。トークンの交換には、組織ごとに毎分 1,000 リクエストの既定のクォータがあり、すべての pool、provider、利用者、自動化の処理が共有します。[51]

pool は組織のレベルで作り、pool の ID は Google Cloud の全 pool で一意でなければなりません。SecOps 用の pool は SecOps 専用で、他の用途と共有できません。pool の ID は 4 から 61 文字、provider の ID は 4 から 32 文字で、使えるのは小文字・数字・ハイフンです。IAM のポリシーは、provider でなく pool に付けます。provider は、1つの IdP との関係を表します。

OIDC の流れは2つです。

- authorization code flow: 安全。大きなトークンも取得でき、UserInfo のクレームも使える
- implicit flow: ID トークンのクレームだけ（only-id-token-claims）が使える

属性は CEL で対応づけます。google.subject は必須で、最大 127 バイトです。変わる値にすると、IdP で値が変わった利用者がアクセスを失います。google.groups は任意です。1人が 400 を超えるグループに入っていると、サインインできません。

SAMPLE

マッピング全体は 16 KB までで、超えるとサインインできません。独自の属性は 50 個まで、1つ 2,048 文字までです。attribute condition は、受け入れる ID を絞る CEL の式です。GitHub のように複数の組織が同じ issuer URL を共有する IdP は、attribute condition で正しいテナントに限らなければなりません。[52]

IAM のポリシーで使う principal の書き方は4つです。

対象	書き方
単一の ID	`principal://iam.googleapis.com/locations/global/workforcePools/POOL_ID/subject/値`
グループ	`principalSet://iam.googleapis.com/locations/global/workforcePools/POOL_ID/group/GROUP_ID`
属性	`principalSet://iam.googleapis.com/locations/global/workforcePools/POOL_ID/attribute.NAME/VALUE`
pool 内の全員	`principalSet://iam.googleapis.com/locations/global/workforcePools/POOL_ID/*`

SCIM によるグループの管理は、Gemini Enterprise にだけ適用されます。詳細な監査ログ（detailed audit logging）は、IdP から受け取った属性を Cloud Audit Logs に残します。provider の作成時に有効にして、属性のマッピング エラーの調査に使います。[53]

SAMPLE

サンプルはここまでです

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

Footnotes

1. https://cloud.google.com/security-command-center/docs/service-tiers ↩
2. https://cloud.google.com/security-command-center/docs/concepts-event-threat-detection-overview ↩
3. https://cloud.google.com/chronicle/docs/ingestion/default-parsers/ingest-gcp-logs ↩
4. https://cloud.google.com/chronicle/docs/ingestion/default-parsers/chrome-management ↩
5. https://cloud.google.com/logging/docs/alerting/log-based-alerts ↩
6. https://cloud.google.com/chronicle/docs/detection/curated-detections ↩
7. https://cloud.google.com/logging/docs/alerting/log-based-alerts ↩
8. https://cloud.google.com/chronicle/docs/secops/content_hub ↩

SAMPLE

9. https://cloud.google.com/chronicle/docs/detection/mitre-dashboard ↩
10. https://cloud.google.com/chronicle/docs/detection/mitre-dashboard ↩
11. https://cloud.google.com/chronicle/docs/secops/gemini-docs ↩
12. https://cloud.google.com/chronicle/docs/secops/triage-investigation-agent ↩
13. https://cloud.google.com/security-command-center/docs/concepts-event-threat-detection-overview ↩
14. https://cloud.google.com/chronicle/docs/investigation/udm-search ↩
15. https://cloud.google.com/chronicle/docs/investigation/statistics-aggregations-in-udm-search ↩
16. https://cloud.google.com/chronicle/docs/investigation/statistics-aggregations-in-udm-search ↩
17. https://cloud.google.com/chronicle/docs/investigation/statistics-aggregations-in-udm-search ↩
18. https://cloud.google.com/chronicle/docs/investigation/udm-search ↩
19. https://cloud.google.com/chronicle/docs/investigation/alerts-iocs ↩

SAMPLE

20. https://cloud.google.com/chronicle/docs/investigation/alerts-iocs ↩
21. https://cloud.google.com/chronicle/docs/investigation/alerts-iocs ↩
22. https://cloud.google.com/chronicle/docs/investigation/alerts-iocs ↩
23. https://gtidocs.readme.io/docs/google-threat-intelligence-indicator-score.md ↩
24. https://cloud.google.com/chronicle/docs/detection/ati-fusion-feed ↩
25. https://cloud.google.com/chronicle/docs/detection/ati-prioritization ↩
26. https://cloud.google.com/chronicle/docs/detection/gti-byol ↩
27. https://gtidocs.readme.io/docs/ioc-stream-guide.md ↩
28. https://gtidocs.readme.io/docs/manage-threat-profiles.md ↩
29. https://cloud.google.com/chronicle/docs/onboard/configure-authentication ↩
30. https://cloud.google.com/chronicle/docs/onboard/configure-authentication ↩
31. https://cloud.google.com/security-command-center/docs/configure-secops-users ↩

SAMPLE

32. https://cloud.google.com/chronicle/docs/secops/use-google-secops-mcp ↩

33. https://cloud.google.com/chronicle/docs/secops/use-google-secops-mcp ↩

34. https://cloud.google.com/chronicle/docs/onboard/configure-feature-access ↩

35. https://cloud.google.com/chronicle/docs/onboard/configure-feature-access ↩

36. https://cloud.google.com/chronicle/docs/administration/datarbac-overview ↩

37. https://cloud.google.com/chronicle/docs/administration/datarbac-overview ↩

38. https://cloud.google.com/chronicle/docs/administration/configure-datarbac-users ↩

39. https://cloud.google.com/chronicle/docs/administration/configure-datarbac-users ↩

40. https://cloud.google.com/logging/docs/audit ↩

41. https://cloud.google.com/logging/docs/audit/configure-data-access ↩

42. https://cloud.google.com/logging/docs/audit/configure-data-access ↩

SAMPLE

43. https://cloud.google.com/chronicle/docs/administration/audit-logging ↩

44. https://cloud.google.com/chronicle/docs/administration/audit-logging ↩

45. https://cloud.google.com/chronicle/docs/reference/authentication ↩

46. https://cloud.google.com/chronicle/docs/reference/authentication ↩

47. https://cloud.google.com/chronicle/docs/administration/migrate-from-legacy-api-to-chronicle-api ↩

48. https://cloud.google.com/security-command-center/docs/how-to-configure-secops-soar ↩

49. https://gtidocs.readme.io/docs/how-get-gti-api-keys.md ↩

50. https://gtidocs.readme.io/docs/rotate-api-key.md ↩

51. https://cloud.google.com/iam/docs/workforce-identity-federation ↩

52. https://cloud.google.com/iam/docs/workforce-identity-federation ↩

53. https://cloud.google.com/iam/docs/workforce-identity-federation ↩

SAMPLE

GCP PSOE 学習用テキスト(無料サンプル)

版

2026年11月版(Google Cloud 公式 Professional Security Operations Engineer Exam Guide 2.0（2026-11-15 取得）準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

Google Cloud および関連の製品名・サービス名は、Google LLC の商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材は公式シラバスの内容を基に作成したもので、Google LLC との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点は info@shikaku-doujou.com までご連絡ください。

SAMPLE