Session Report

クラウド特有のセキュリティ リスクに対応する
Google Cloud の基本的機能

Google Cloud の セキュリティ機能、基本のキ Security Command Center で 実現するリスク管理

Google Cloud　カスタマー エンジニアリング　セキュリティ スペシャリスト
髙橋 悟史

Google Cloud

Google Cloud

セッション レポート概要

Google Cloud が提供するセキュリティ機能の中でも、「基本のキ」に位置付けられるのが Security Command Center です。今回は、生成 AI を組み込むなど、進化を遂げた同ソリューションの最新機能とともに、リスク管理のためのアプローチを紹介します。最近話題のアタック サーフェス管理との違いや使い分けについても解説します。

プレゼンター紹介

Google Cloud
カスタマー エンジニアリング　セキュリティ スペシャリスト
髙橋 悟史

グーグル・クラウド・ジャパンにてお客様のセキュリティ課題解決のためにセキュリティ専門のカスタマー エンジニアとして勤務。グーグル・クラウド・ジャパンに入社する前は、複数のクラウド ベンダー、セキュリティ ベンダー、IT ベンダーにてセキュリティ領域の担当経験がある。

目次

クラウド環境特有のリスクとその対策の必要性

Google Cyber Security Action チームが定期的に発行している、クラウド環境の脅威と対策を解説した「Threat Horizon Report」の 2023 年 8 月版によると、Google Cloud 環境のセキュリティ侵害の主な要因として「クラウド環境の侵害の原因の大部分が認証情報の悪用によるもの」が指摘されています。

認証情報と聞くと、ID とパスワードを思い浮かべるかもしれませんが、ここでの認証情報とは、VM に SSH ログインする際のキー、Google Cloud サービスのアカウントキーなどのことです。端的な例としては、サービス アカウント情報を含めたソースコードを GitHub の公開リポジトリに上げてしまって、すぐ乗っ取られたという話をよく聞きます。

つまりクラウド環境のリスクにはクラウド特有のものがあり、その対策も特有のものが必要になるということです。

オンプレミス用の対策ツールは、アプライアンスや OS のエージェントなどがあり、今も引き続き利用されています。一方で、一般的にクラウド環境は、アーキテクチャとして最初からセキュアになるようにデフォルトの構成が設定されているものの、サービス アカウント キーや SSH などの認証情報を適切に管理していなければ、それがリスクとなります。

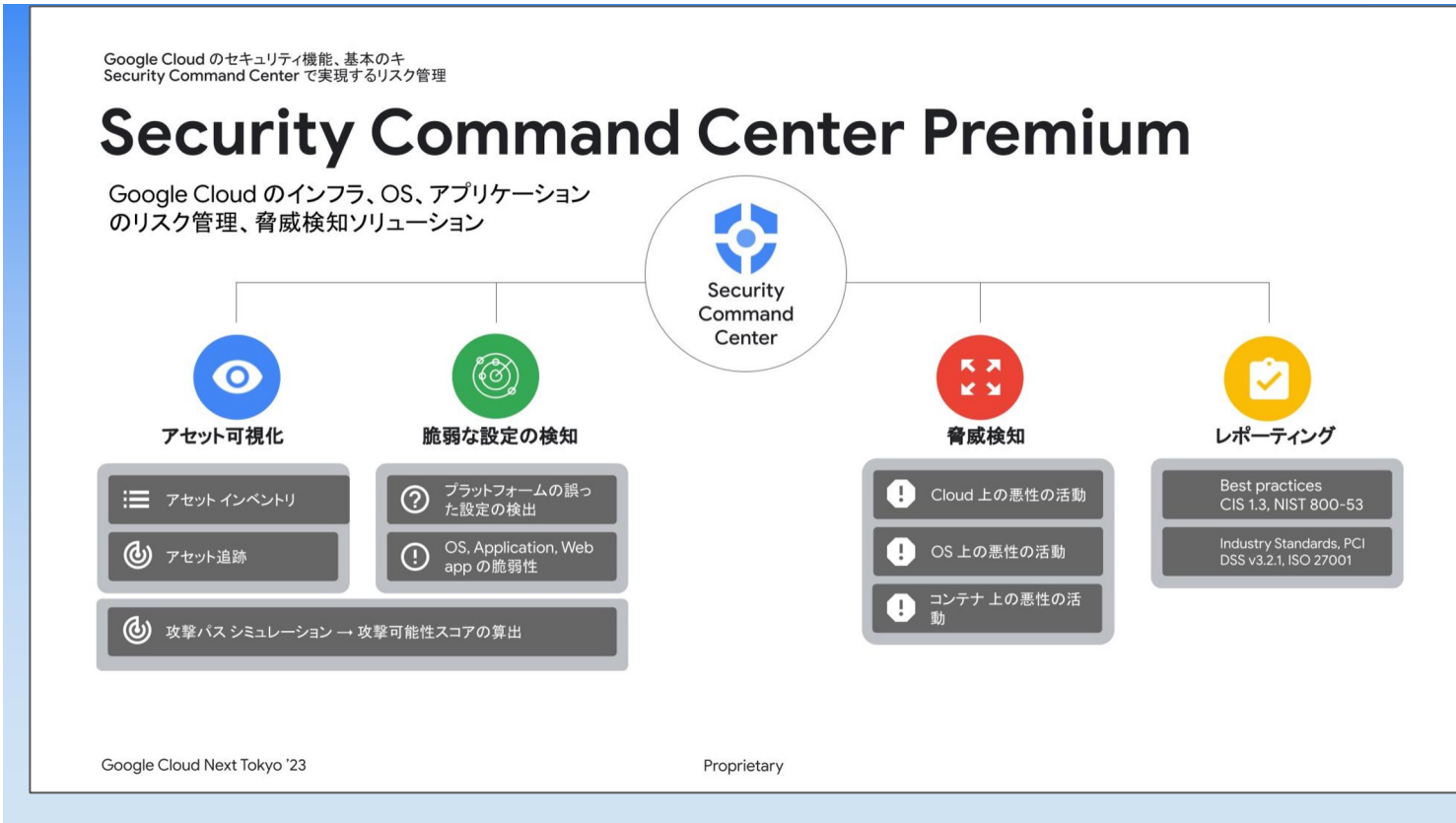
そこで追加対応するには、オンプレミスで利用していたセキュリティ製品では不十分です。例えば、オンプレミスのサーバーに API のキーを使ったアプリケーションを構築することは一般的ではなく、対応機能を備えていないでしょう。

クラウドの設定や状況を把握して、自動的に対策を講じるためには、クラウド環境に特化したセキュリティ対策製品が必要です。Google Cloud では、インフラ、OS、アプリケーションのリスク管理および脅威検知ソリューション「Security Command Center」を提供しています。

Security Command Center（SCC）Premium が解決する課題

有償版の「Security Command Center Premium」は、アセット可視化、脆弱な設定の検知、脅威検知、レポーティングと大きく 4 つの機能を備えています。

脆弱な設定の検知では、クラウドそのものやクラウドの上で動いている Web アプリケーションの設定などから、悪用される可能性が含まれている状態のものを発見します。脅威検知では、今起きている不信な動きを見つけます。

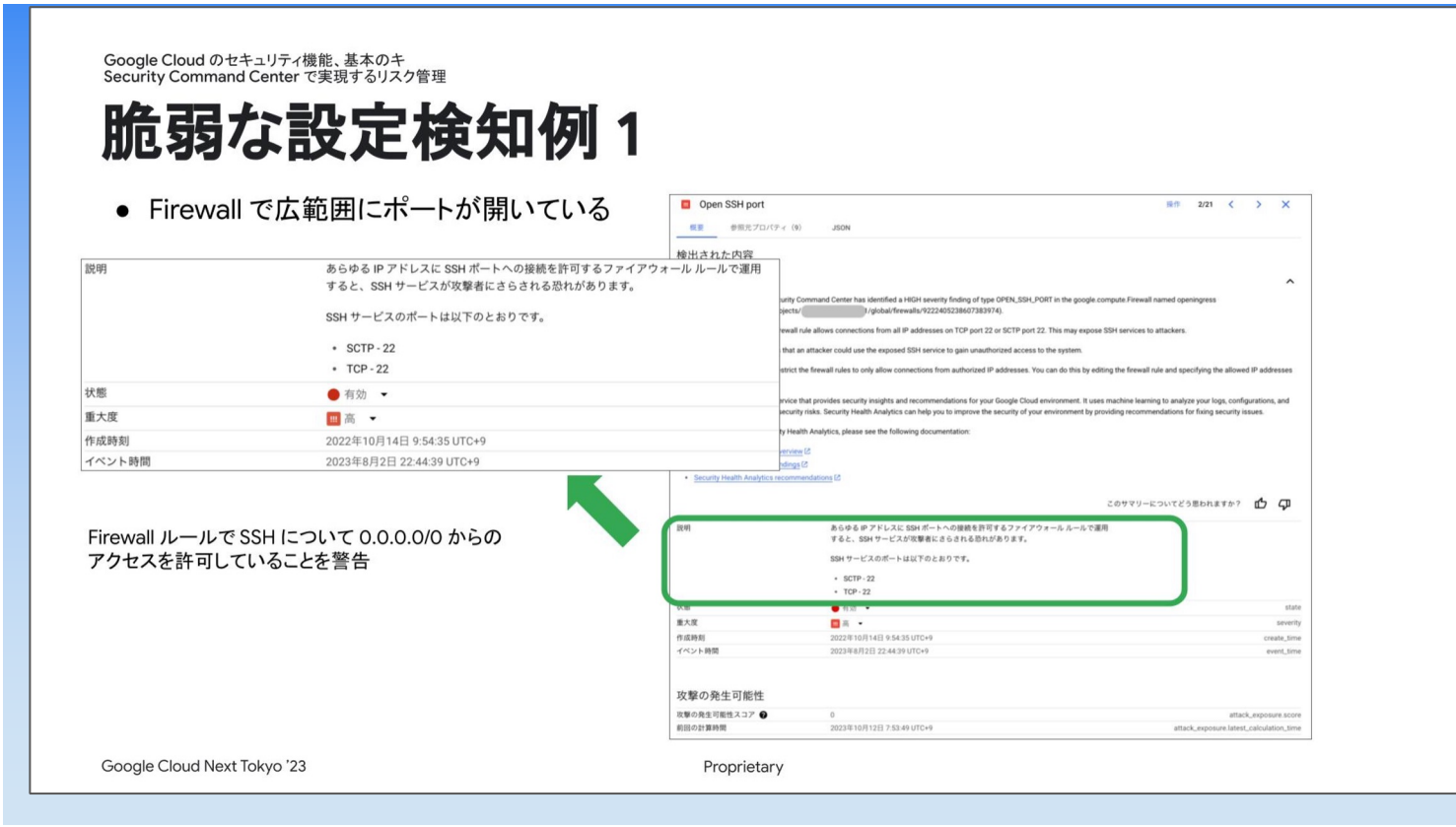


Security Command Center Premium が持つ機能の全体像

どのような検知が行えるのか、代表的なユースケースで紹介します。

脆弱な設定 検知例 1「ファイアウォールで広範囲にポートが開いている」

クラウド側で、VPC の ファイアウォール の設定を検知します。プリミティブな例では、SSH で使われる 22 番ポートが、インターネットのどこからでもアクセス可能な 0.0.0.0/0 となっている状態を警告します。



ファイアウォールで広範囲にポートが開いている場合の警告画面イメージ

脆弱な設定 検知例 2「Compute Engine 上の OS の脆弱性」

「Compute Engine」上で動いている OS が持つパッケージのリストの中から、脆弱性が報告されているバージョンが使われていることを検知します。

従来、検知時の説明内容は固定されていましたが、生成 AI によって利用環境に合わせた説明が可能になり、問題が起きている箇所やリスク、修正方法を知ることができます。なお、Google の生成 AI モデルである PaLM 2 を、セキュリティにチューニングした Sec-PaLM 2 が使われています。

脅威検知 例 1「サービス アカウントの悪用の可能性」

最近増加している認証情報の悪用を検知できます。サービス アカウントが持っている権限をダンプする IM の API が実行されると検知します。

通常、正規の行為としてサービス アカウントの権限を確認することはまずありません。一方で、サービス アカウントの情報が何らかの形で漏れてしまった場合、攻撃者はまず権限を確認するため、危険な兆候として反応すべきです。

なお、発信元 IP アドレスや SDK の種類などが表示されるため、正規の行為かどうかを判断可能です。

脅威 検知例 2「仮想通貨マイニングの実行」

サービス アカウントを入手した攻撃者は、VM インスタンスを作る権限を持つことが判明すると、恐らく仮想通貨マイニングを実行するでしょう。料金が急に増えたことに気が付いて停止できますが、24 時間程度でも攻撃者としては十分マネタイズできるので、この攻撃は止まない状況になっています。

SCC では、ハイパーバイザーからメモリーを監視して検知します。OS にエージェントは不要であるため、お客様の環境に負荷が一切かかりません。この機能はクラウド プロバイダーでなければ実現できず、現在提供しているのは Google Cloud だけです。

脅威検知 例 3「GKE クラスタ上の不正な活動」

既にデプロイして実行済みの「Google Kubernetes Engine（GKE）」のクラスタ上で、モジュールやライブラリの追加、あるいは Reverse Shell（コンテナの内側から外部に通信チャネルを確立する行為）を検知します。IP アドレス、ポート番号、プロセス名などが表示されるため、どのような通信チャネルが確立されたのかが分かります。

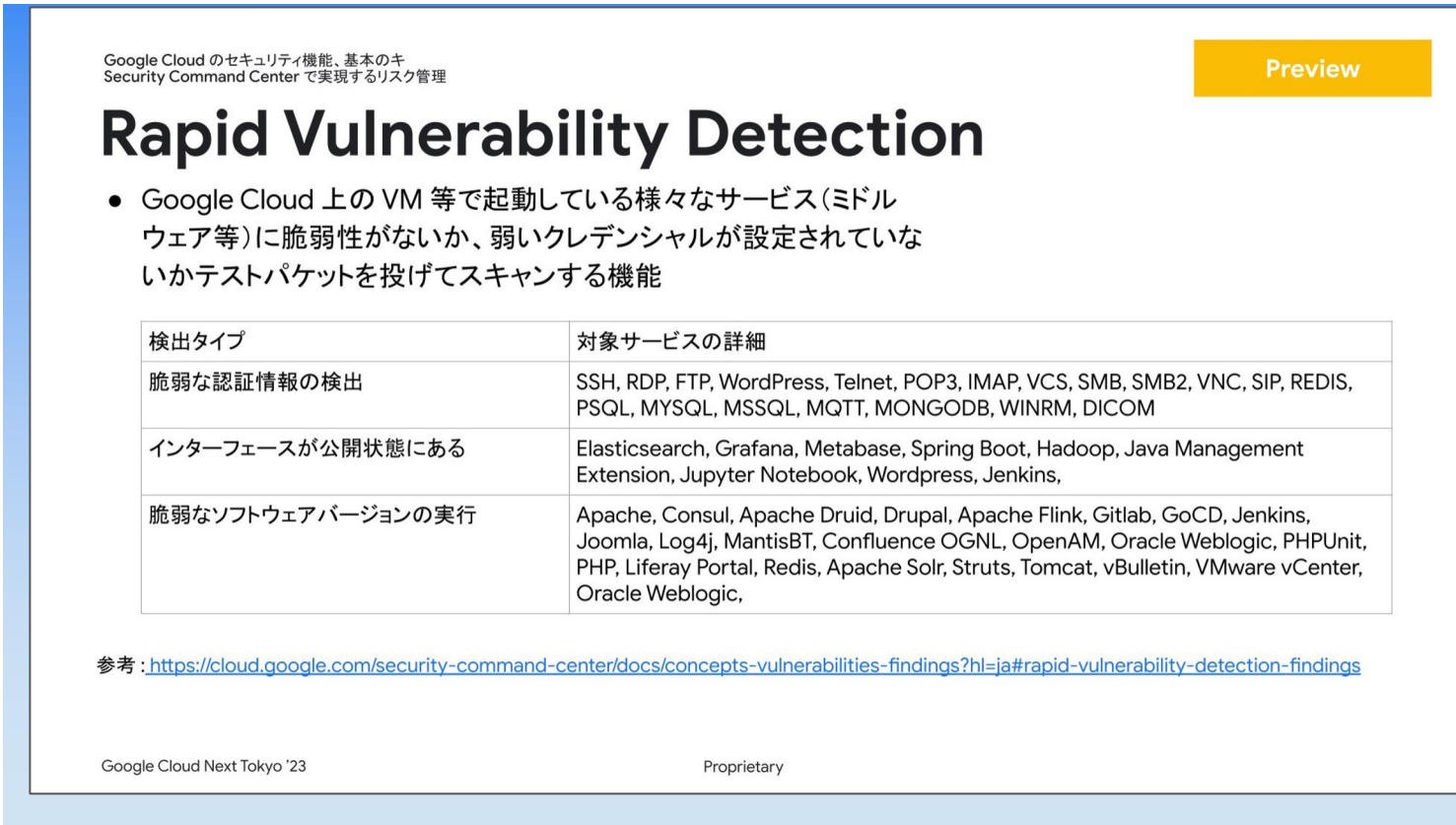
GKE が使う COS イメージ（Google Cloud が提供するコンテナに特化した OS イメージ）には、最初からエージェントが入っているため、お客様側でエージェントの導入や管理は不要です。

SCC の最新機能

SCC は頻繁にアップデートされており、最新脅威への対応や利便性向上に努めています。ここでは、この 1 年ほどで追加された最新機能のうち 3 つを紹介します。

• **VM Threat Detection**
既に説明した、ハイパーバイザー上から実行メモリーを監視する機能です。エージェント不要で、「OS ルートキット」と呼ばれる OS の深いところに侵入するマルウェアや、仮想通貨マイニングなどの活動を検知することが可能です。

• **Rapid Vulnerability Detection**
Web だけでなく、さまざまなサービスの脆弱性を検知できます。代表的な例では、MySQL などの DB 系サービスで管理系ポートが開いているような場合、スキャン パケットを投げて、ID とパスワードの組み合わせが辞書に載っているような弱いものではないかをチェックします。

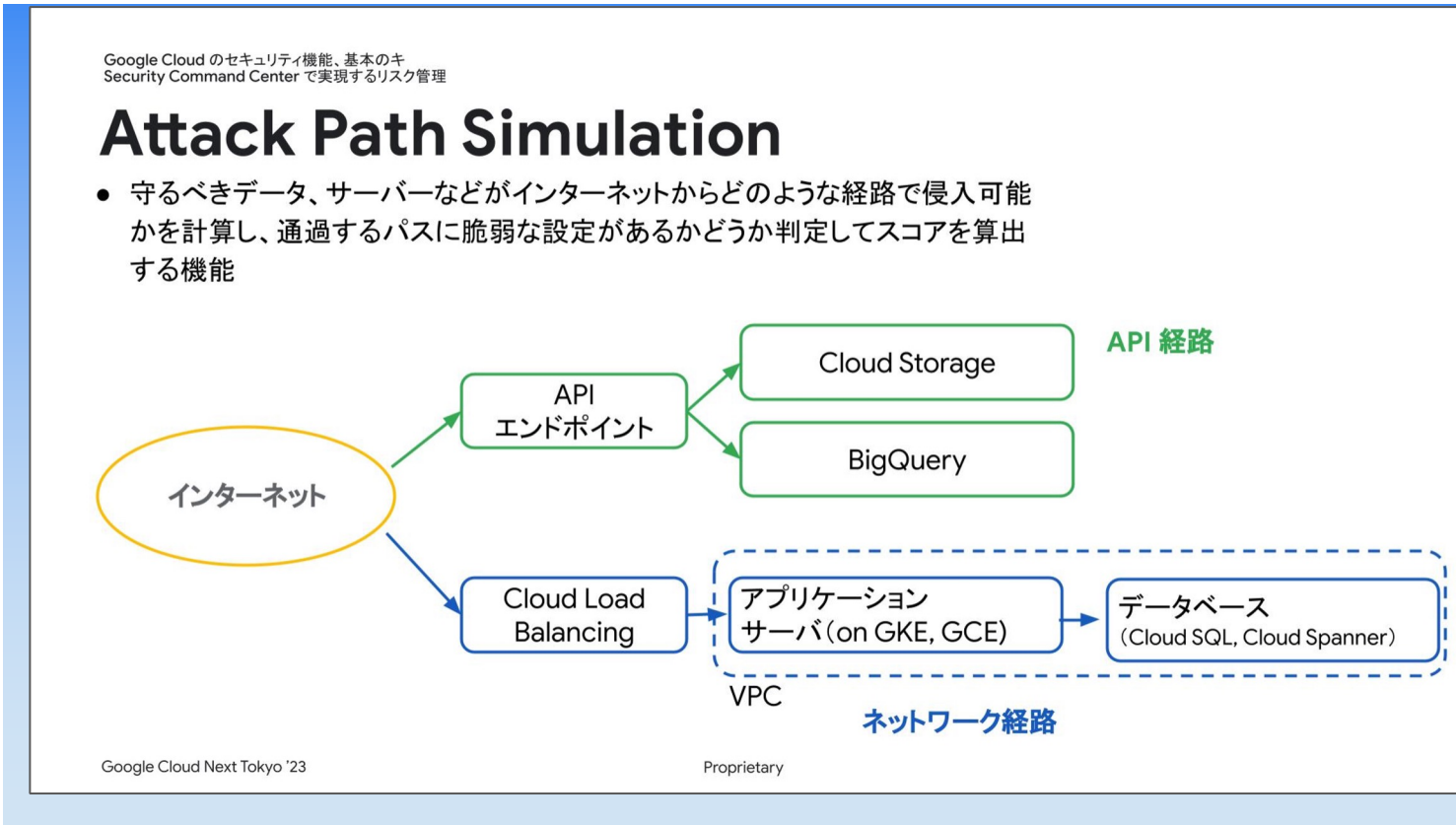


Rapid Vulnerability Detection のスキャン対象サービスと検出タイプ

SCC の Web Security Scanner および Rapid Vulnerability Detection の大きな強みは、ユーザーによる設定が不要で、IP アドレスやサーバーを指定しなくても、SCC がオンになっていれば自動的に開いているポートを見つけてスキャンし、リスクを発見してくれる点です。

• **Attack Path Simulation**
インターネットから侵入されたとき、最も守りたいのはデータではないでしょうか。この機能は、インターネットからデータにたどり着くまでの経路を自動計算して、その間に通過するコンポーネント（ロード バランサー、アプリケーション サーバー、DB サーバー、BigQuery など）の脆弱性を見つけます。

VM ベースであれば一般的には VPC を通るイメージもありますが、クラウドでは API エンドポイントを使って VPC 外のCloud Storageや BigQuery にアクセスする経路もあります。API エンドポイントで必要なサービス アカウント キーが漏れた場合には、侵入のリスクが高まります。



Attack Path Simulation が対象とする経路の全体像

セキュリティ対策ソリューションにポート設定の不備を指摘されても、本当に対処しなければならないのか判断に悩むことがありますが、このシミュレーション結果があれば、実際にインターネットから入ってくる可能性を加味したリスクがスコアで明らかになるため、判断を助けます。例えば、一見リスクがありそうな VM 関連のポートが開いていたとしても、後ろに VM がない構成であればスコアは常にゼロになります。

Attack Path Simulation の解析結果例

SCC 運用のポイント

SCC によって脅威を検知できますが、一日中コンソールを眺めているわけにはいきません。また、検出結果があまりに多い場合に、どこから手を付ければよいのか分からなくなってしまいます。こうした問題には、次のようなポイントを抑えた運用が効果的です。

・外部ツールへの通知

Slack やケース管理ツール、GitHub などに検出結果を転送してイシュー管理しているお客様もいます。SCC Premium は Google Cloud の「Pub/Sub」にリアルタイムにエクスポートする機能がありますので、Pub/Sub 経由で「Cloud Functions」を起動し、Webhook などを使って外部のツールに連携できます。

また、BigQuery へエクスポートもできるため、分析や可視化を行うダッシュボード上に検出結果を表示するような運用も可能です。

・トライアルや PoC 実施結果を踏まえた棚卸し

「検出結果が多すぎてどこから手を付ければよいのか分からない」。これはプロジェクトの数が 100 を超えるような大規模環境で、トライアルや PoC を実施したときに聞かれるコメントです。

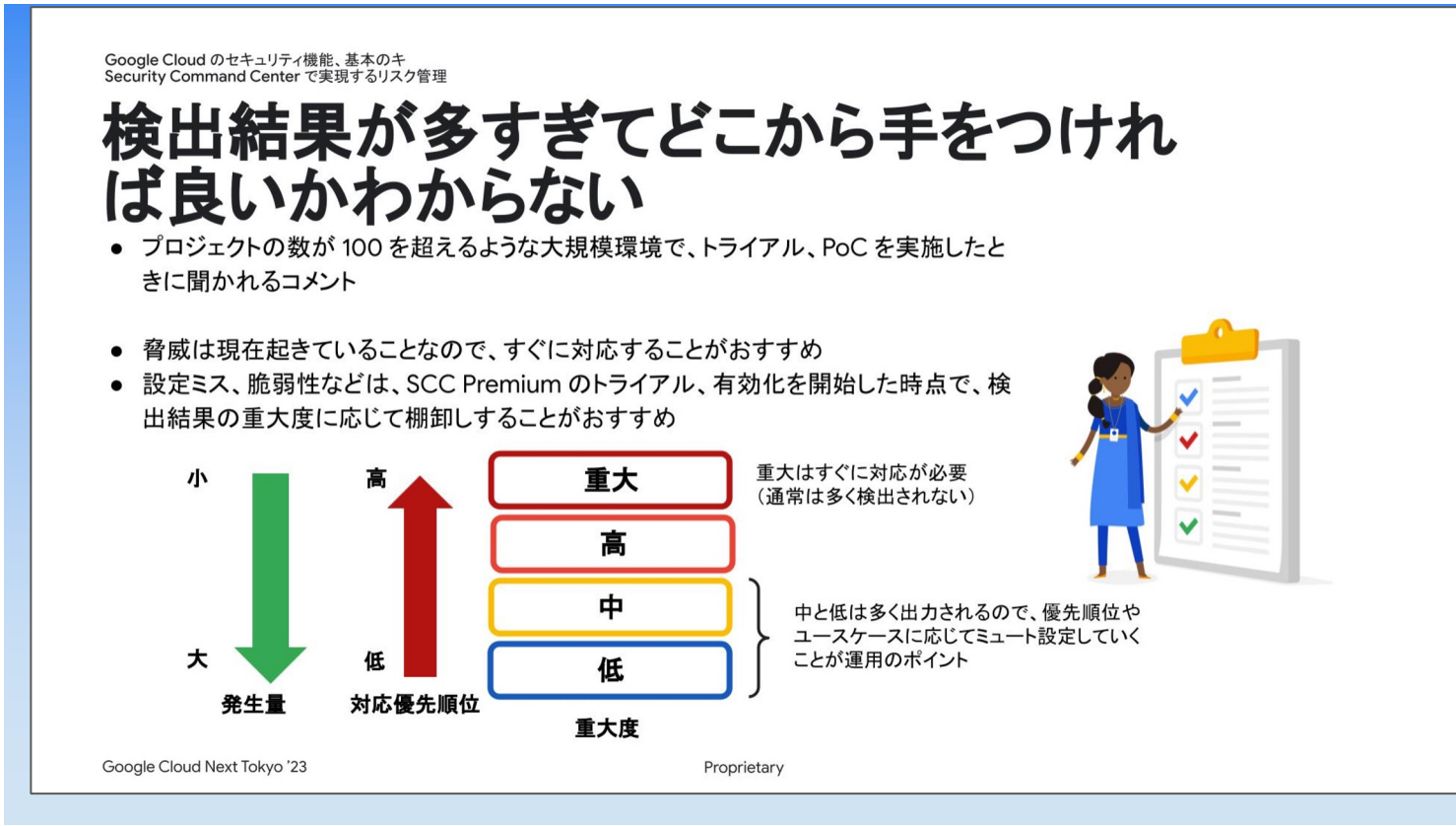
規模が大きいと 1 つの環境に導入した途端に、脅威や脆弱性が大量に見つかることが珍しくありません。100 プロジェクトで各 100 個が見つかれば 1 万個で、どう対処すればよいのかと驚くお客様もいます。

優先順位を付けて対応していきますが、このとき意識したいのが「脅威」と「設定ミス」「脆弱性」の違いです。

自動的に付けられた重大度のラベルが「低」だとしても、「脅威」はすぐに内容を確認することをお勧めします。例えば、サービス アカウントの自己権限確認は、重大度が低めの脅威として検出しますが、通常の運用ではあまりないことのため心配です。もっとも、実運用環境において「脅威」の数は多くないため、あまり心配することはないでしょう。

「設定ミス」「脆弱性」は、環境によっては大量に検出されます。例えば、Google Cloud の組織ポリシー機能で、ガードレールで制約を付けていない環境の場合です。

そこでお勧めしているのは、トライアルや PoC によって環境の弱みを認識し、重要度に応じた棚卸しを実施することです。これを踏まえて、後ほど紹介するミュート設定などに反映させます。

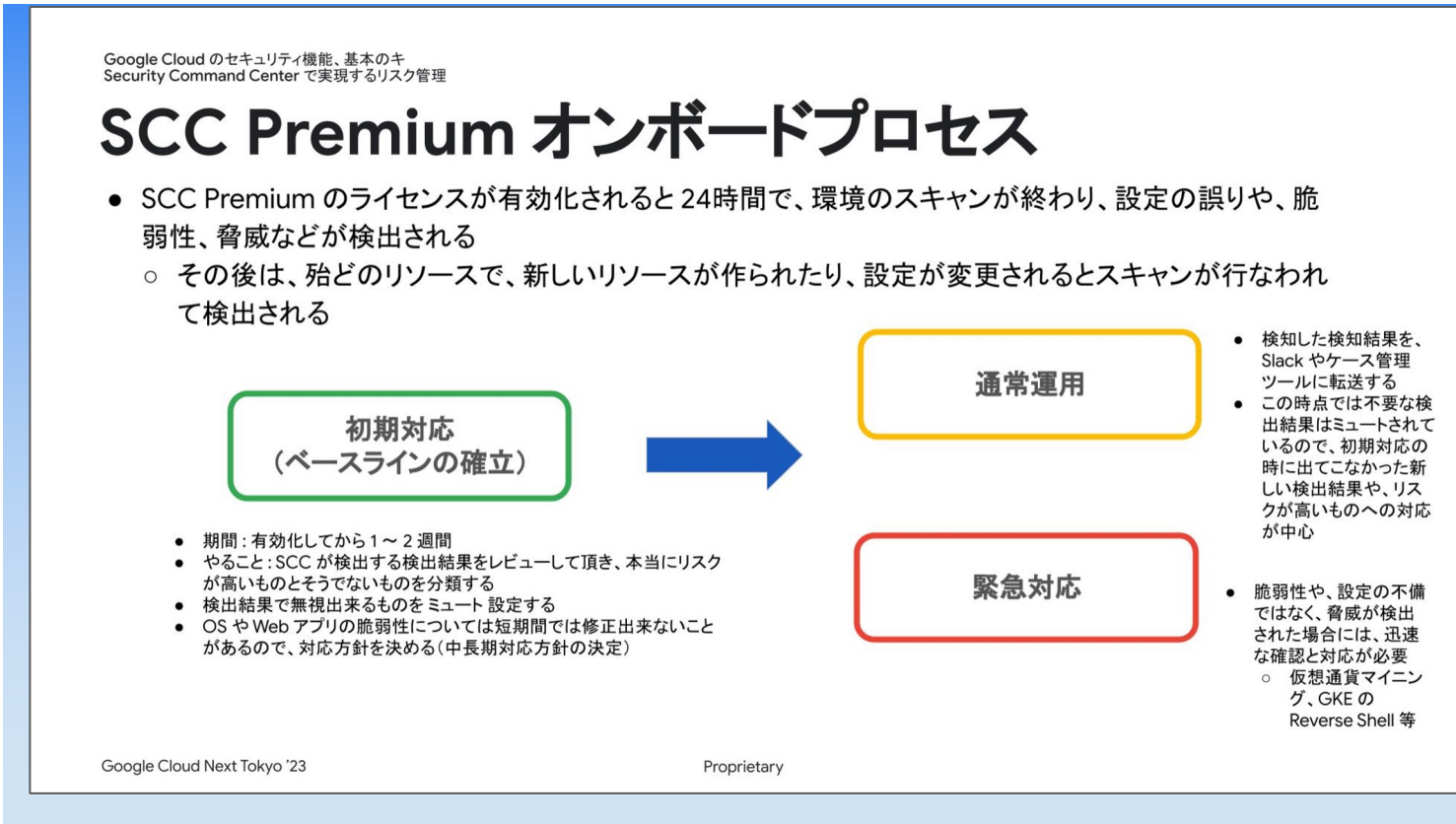


重大度と棚卸しの考え方の一例

・オンボード プロセスの進め方

SCC Premium を有効化して検出された脅威や脆弱性などに対して、まずベースラインを確立することをお勧めしています。SCC の指摘に対して、自組織がそれを問題視し対応するのか、対応しないでよいと判断するのかを決めます。新機能の Attack Path Simulation も役立てられるでしょう。対応しないと決めたものはミュート設定にするなどして、通常運用に入ります。

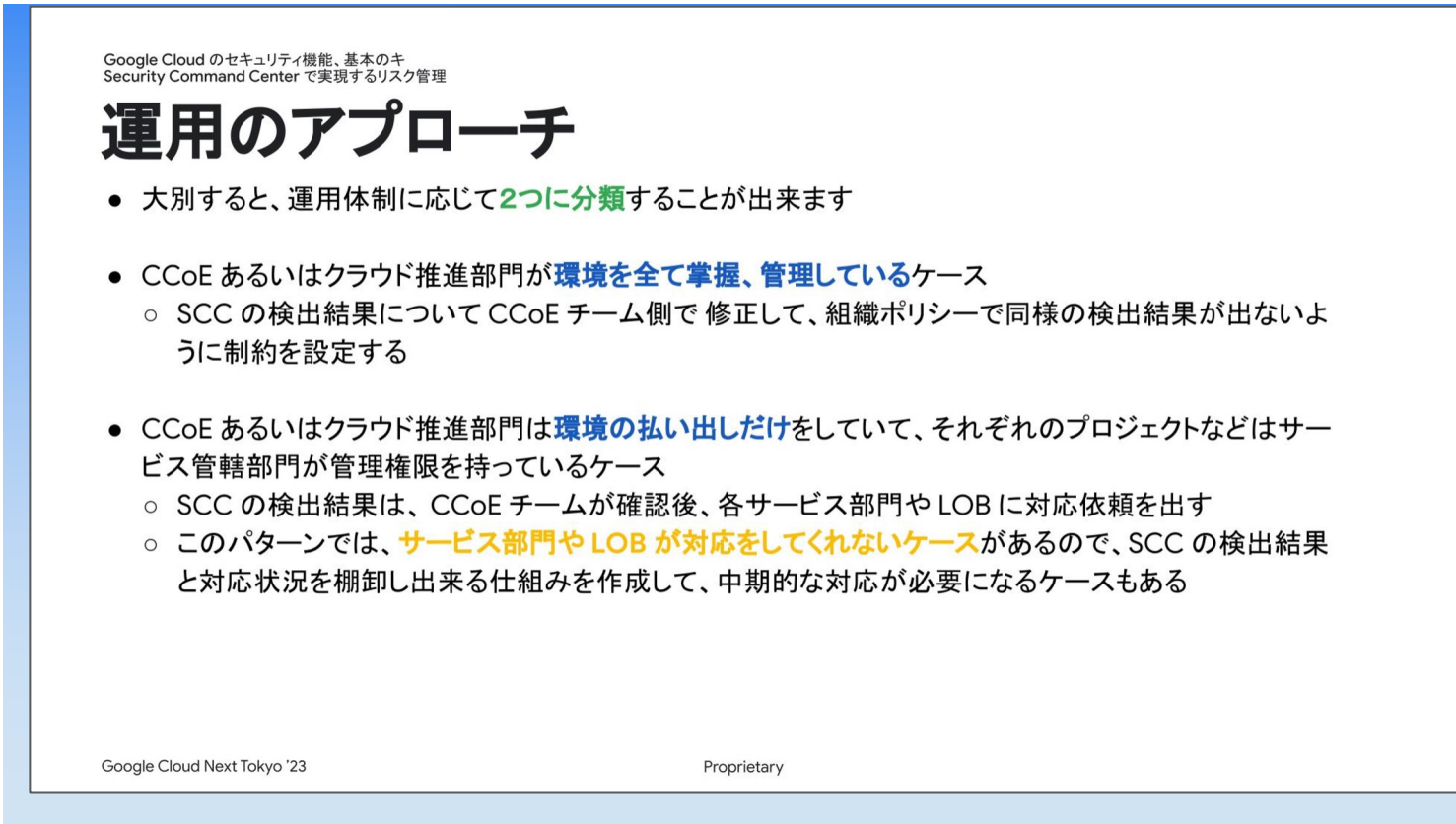
一方で、上位層で動いているアプリケーションの脆弱性が突かれた場合などに「脅威」が検出されると、緊急対応する必要があります。例えば、仮想通貨マイニングや GKE の Reverse Shell といった、非常に重大度が高い問題が発生した場合に備えて、緊急対応するためのプロセスを作っておくことが重要です。



SCC Premium で運用する場合のオンボード プロセス

・運用体制に応じたアプローチ

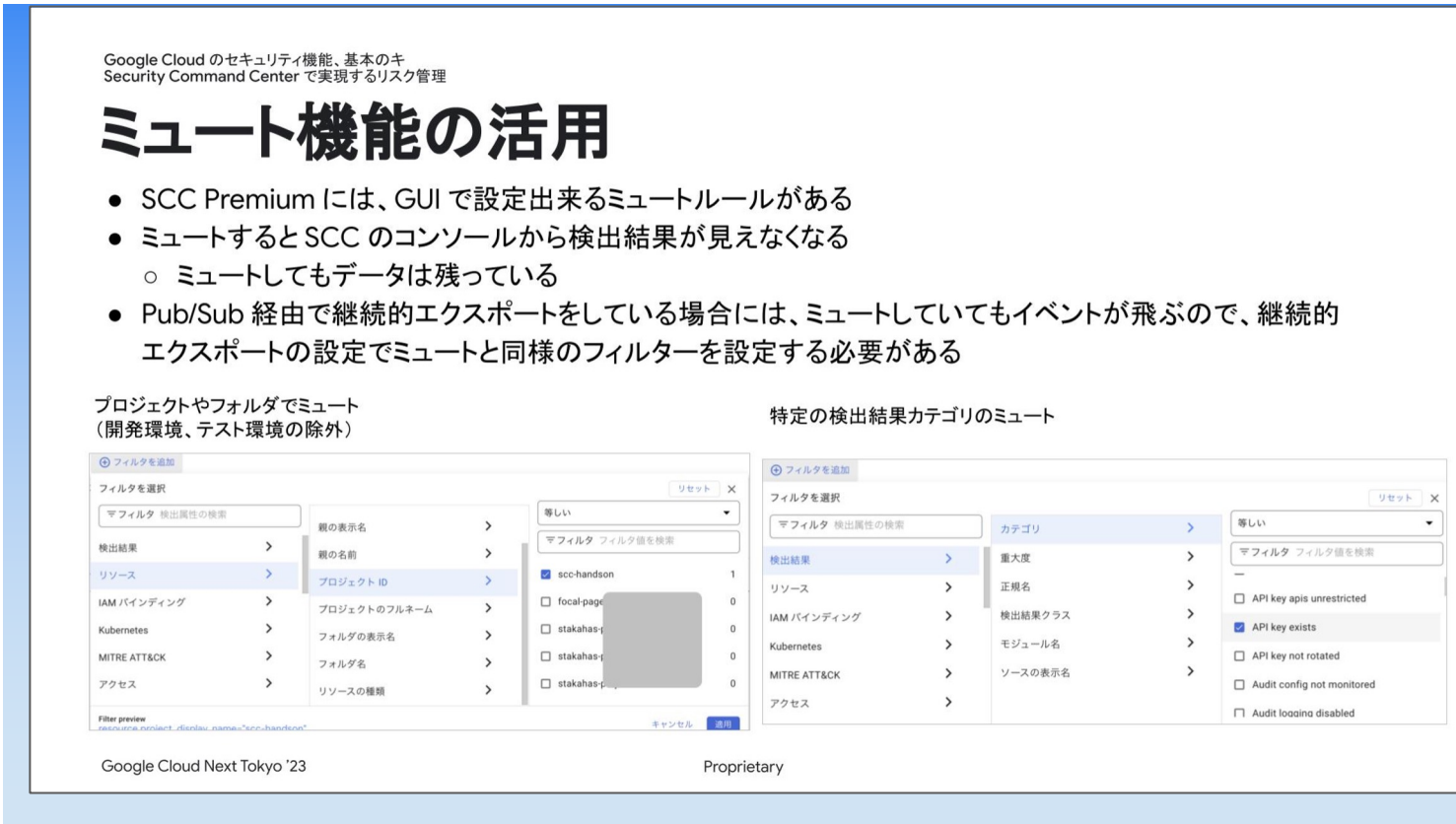
体制の違いによって、運用のアプローチも異なることに留意しておくべきです。CCoE またはクラウド推進部門が環境を全て掌握・管理しているケースと、それらの部門が環境の払い出しだけをして、それぞれのプロジェクトなどはサービス管轄部門が管理権限を持っているケースが考えられます。



運用体制に応じた 2 つのアプローチ

・ミュート機能の活用

検出結果が大量に出る場合には、ミュート機能を活用します。GUI でカテゴリを選ぶと、それに合致するものはミュート可能です。カテゴリ以外にも、プロジェクト（もう見ない開発環境やテスト環境など）や、フォルダにも設定できます。



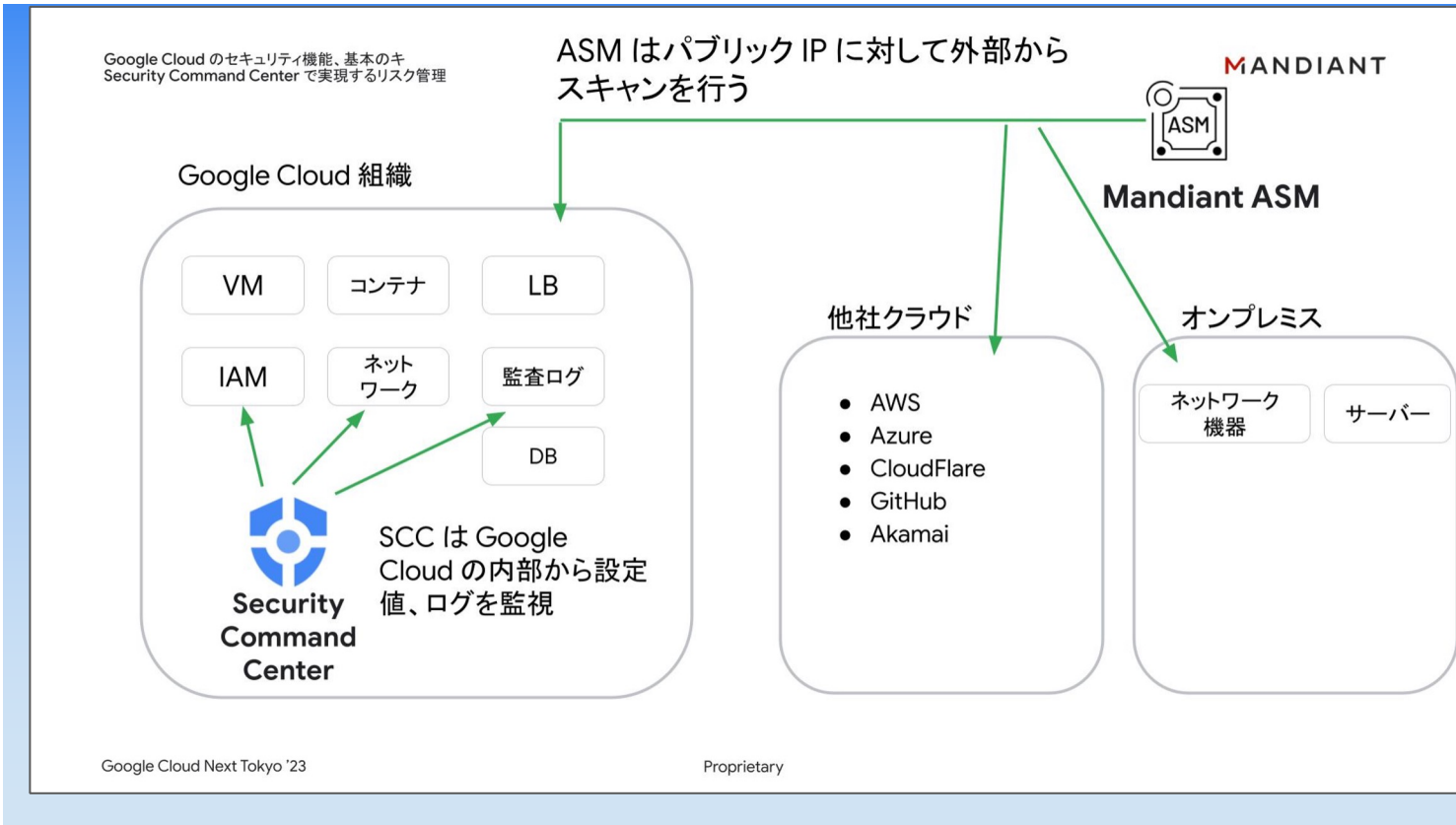
ミュート機能の概要

Mandiant ソリューションとのすみわけと活用

Google Cloud 傘下の Mandiant も、SCC 同様にクラウド環境の可視化やモニタリング、リスク分析を行うソリューション「Attack Surface Management（ASM）」を提供しています。

動作イメージは、ユーザーが持つドメイン名や IP アドレスなどを入力すると、ASM が自動処理で IT 資産をスキャンして、そこにセキュリティの問題がないかを調べてくれるというものです。基本的にインターネットから到達可能であればどのような環境でもスキャンが可能で、Google Cloud だけでなく他社のクラウド、オンプレミスにも対応しています。

注目ポイントは、ASM が行うのは外部からのスキャンであって、内部からのスキャンではないということです。内部からの監視と外部からの監視では、目的が異なるため、どちらかを選ぶのではなく両方のよいところを使う運用をお勧めします。実際に、SCC と併せて Mandiant でのスキャンも実施しているお客様がいますし、追加する価値はあります。



SCC と Mandiant ASM のカバーする対象の違い

ASM では、SCC の紹介で挙げた、VM 上での仮想通貨マイニングを発見するような使い方はできません。一方で、Google Cloud 以外もスキャンできるため、企業全体の IT 資産を包括的に守れます。

特徴的なのは、スキャン結果の評価方法です。CVE などの公開されている脆弱性情報に加えて、Mandiant のコンサルタントが分析した最前線の攻撃者が使う手法と照らし合わせることで、本当にリスクがある脆弱性の対処に注力できます。

一般的にクラウドは、設計段階からセキュリティ対策を組み込んだ「セキュリティ・バイ・デザイン」になっていますが、それでもクラウド特有のセキュリティ リスクに対応しなければならず、クラウド特有の対策ツールが必要です。Google Cloud の運用では、まずは SCC や Mandiant ASM の活用をご検討ください。

参照リンク

1. Security Command Center 製品紹介ページ
2. Google Cloud のセキュリティ機能、基本のキ｜Security Command Center で実現するリスク管理 アーカイブ視聴ページ

製品、サービスに関するお問い合わせ

goo.gl/CCZL78

Google Cloud の詳細については、上記 URL もしくは QR コードからアクセスしていただくか、同ページ「お問い合わせ」よりお問い合わせください。

Google Cloud