Google Cloud Whitepaper

October 2024

3省2ガイドライン (日本)

Google Cloud

はじめに

個人を特定できる医療に関連する情報（医療情報）を含むシステムの利用者又は、提供者は、以下の2つのガイドラインの何れかに準拠する必要があります。

1. 医療情報システムの安全管理に関するガイドライン [1]

2. 医療情報を取り扱う情報システム及びサービス提供者のための安全管理ガイドライン[2]

厚生労働省、経済産業省、総務省の3省が発行するこれらのガイドラインは「3省2ガイドライン」と総称されます。Googleは、システムを構築するための安全な基盤、システムのセキュリティを支援するツール、それらのツールを活用するための教育を提供することで、お客様が3省2ガイドラインの義務を果たすことを支援しています。本稿では、Googleがどのようにその義務を果たしているか、また、お客様が3省2ガイドラインの義務を果たすためにGoogleのサービスをどのように利用できるかについて説明します。このホワイトペーパーは、情報提供のみを目的としています。本ホワイトペーパーのいかなる内容も、お客様に法的アドバイスを提供することを意図したものではなく、また法的アドバイスの代替となるものではありません。

要求事項

対象範囲

「医療情報システムの安全管理に関するガイドライン」は、病院、診療所、産院、薬局、訪問看護ステーション、介護事業者、医療情報ネットワークなど、個人を特定できる医療に関連する情報（医療情報）を扱うシステムの**利用者**が遵守すべき事項を定めたものです。 なお、第6.0版（2023年5月）の改訂により、本文が概説編、経営管理編、企画管理編及びシステム運用編に分けられ、各編で想定する読者ごとに求められる遵守事項及びその考え方がより明確に示されるようになりました。

「医療情報を取り扱う情報システム及びサービス提供者のための安全管理ガイドライン」は、デジタル化された医療情報を含むシステムの**提供者**が遵守すべき事項を定めたものです。これには、そのようなシステムの構築に使用される*Google Cloud*サービスも含まれます。

これらのガイドラインでは、さらに以下の規則に準拠する必要があります。

- 個人情報保護法第20条に基づく安全管理措置 （医療情報システムの安全管理基準を満たすために、個人を特定できる医療に関連する情報（医療情報）を取り扱う際は安全管理措置を施す）

[1]第6.0版 2023年5月発行（厚生労働省）
[2]第1.1版 2023年7月発行（経済産業省と総務省の共同発行）

- e-文書法に基づく、電子記録の三原則（真正性、見読性、保存性）（医療情報システムの安全管理に関するガイドライン（第7章、第9章）の電子保存する情報の基準を満たすため）
- 厚生労働省の「外部保存に関する通知」に基づく医療情報を外部に保存する際の要件
- サービスを提供するためのアプリケーション、サーバー、ストレージなどは、国内の行政機関による法の執行が可能な範囲に設置し、行政機関への書類提出がスムーズに行えるようにする

Googleは、お客様に対して直接的に医療情報を含むシステムを提供しているわけではありません。しかしながら、お客様がGoogleのサービスを利用して医療情報を含むシステムを開発し、利用するケースが想定されることから、Googleは間接的に医療情報を含むシステムを提供している、という考え方もできます。よって、Googleは「医療情報を取り扱う情報システム及びサービス提供者の安全管理ガイドライン」に基づく、情報提供を行っています。

「医療情報を取り扱う情報システム及びサービス提供者の安全管理ガイドライン」では、サービス提供者に対してリスクマネジメントとリスクコミュニケーションの両面からの対応が求められています。

リスク管理では、データの流れを明確にし、リスクを特定、評価した上で、合理的なリスク管理策を講じることを求めています。

リスクコミュニケーションの面において、サービス提供者は、医療機関に対して自らのリスク管理策を開示する必要があります。これには、医療機関がサービスを利用する際に、リスク管理のためにどのような行動をとることができるかを明確にすることが含まれています。

リスク管理対策

これらの要求を満たすために必要なリスク管理対策は、以下の4つに分けられます。

(1) 組織的安全管理措置

組織的安全管理措置は、セキュリティを管理するための組織体制を構築、運用し、文書化することを指します。

(2) 人的安全管理措置

人的安全管理措置は、従業員の秘密保持及び、セキュリティ研修を受けることを確実にする対策のことを指します。

(3) 物理的安全管理措置

物理的安全管理措置は、施設へのアクセス者を制限するための区画管理、施錠および関連する対策などの物理的なアクセス制御のことを指します。

(4) 技術的安全管理措置

技術的安全管理措置は、認証、承認、アクセス制御などのデジタルアクセス制御、およびログ管理、暗号化、データ漏洩防止、脆弱性管理、脅威検知などのセキュリティ対策を指します。

責任共有モデル

Google Cloud はクラウドのセキュリティに対して責任を負います。お客様にはお客様自身のクラウド環境に対するセキュリティの責任を負っていただくことになります。これらの前提となる考え方として、Google では 責任共有モデル をフレームワークとして提供しています。

Google Cloud とそのお客様との間には関係性がありますが、お客様のエンドユーザーとの関係はありません。 Google Cloud は、お客様が GCP または Google Workspace に保存した個人情報に関知せず、その個人情報の取扱事業者となることもありません。お客様が選択したサービスを実行する目的でのみ、Google Cloud は自社システム内の顧客データを処理します。お客様は、クラウドサービスに置くデータを保護するために、適切な措置を講じていただかなければなりません。

以下の表は、各カテゴリの要件と安全管理のコンセプトの対応関係を示したものです。以降のセクションでは、セキュリティの責任共有モデルの安全な基盤を実現するうえで Google Cloud が果たす役割について説明していきます。そして、お客様が責任共有モデルにおけるお客様側の責任を遵守できるように、それぞれのセキュリティ対策を支援するGoogle Cloudのプロダクトやサービスを紹介します。

組織的安全管理措置

要件	安全管理のコンセプト
医療情報の取り扱いに関与する人物の役割と責任を 明確にする	ID データガバナンス
医療情報に関するインシデントを検出して報告するメカニズム を構築する	脅威の検出
アクセスや変更をはじめとする、医療情報の取り扱い 記録を保持する	ロギング データガバナンス

個人情報の性質、目的、同意、アクセス権を持つ人物など、管理下にある医療情報管理に関する記録を保持する	データガバナンス アクセス制御
漏洩の可能性を調査し、関係当局に事実を報告できるようにする	ロギング 脅威の検出
医療情報の取り扱い業務を監査できるようにする	ロギング データガバナンス
委託先事業者において医療情報の適切な取扱いがなされていることを管理する	サードパーティー サプライヤーの管理

人的安全管理措置

要件	安全管理のコンセプト
医療情報を取り扱う人物を監督する	ロギング 契約に基づくセキュリティ セキュリティ認証・評価制度への適合
医療情報の取り扱いに関するトレーニングを実施する	トレーニングとコンサルティング
従業員が機密情報を漏らさないようにする	トレーニングとコンサルティング

物理的安全管理措置

要件	安全管理のコンセプト
医療情報を取り扱うエリアを管理して制限を設ける	インフラストラクチャのセキュリティ ID データガバナンス データの変換
許可されていない人物によるアクセスや閲覧ができないように、医療情報を取り扱うエリアに障壁を設ける	インフラストラクチャのセキュリティ データの変換

保存中および転送中の医療情報の物理的な盗難を確実に防止する	インフラストラクチャのセキュリティ データの変換
不可逆的な医療情報データ削除方法を実装する	データの削除

技術的安全管理措置

要件	安全管理のコンセプト
アクセスが必要な人物しか医療情報にアクセスできないようにする	ID アクセス制御 データガバナンス データの変換
各役割に必要な医療情報にしかアクセスできないよう制限をかける	アクセス制御
医療情報の取り扱い担当者全員が識別され、認証されるようにする	ID
ネットワーク アクセス制御を実装して、潜在的なアクセスを制限する	アクセス制御
セキュリティ テクノロジーを利用して、不正アクセスからシステムを保護する	エンドポイント セキュアな CI / CD パイプライン パートナーソリューション
自動更新によって、システムを最新の安全な状態 に維持する	セキュアな CI / CD パイプライン マネージドサービス
ログを分析し、ログ内の脅威を検出する	脅威の検出
システムの脆弱性を継続的に評価する	リスクの検出
保存中および転送中の医療情報を保護する	データの変換
医療情報やシステムのバックアップを確保する	バックアップとレジリエンス

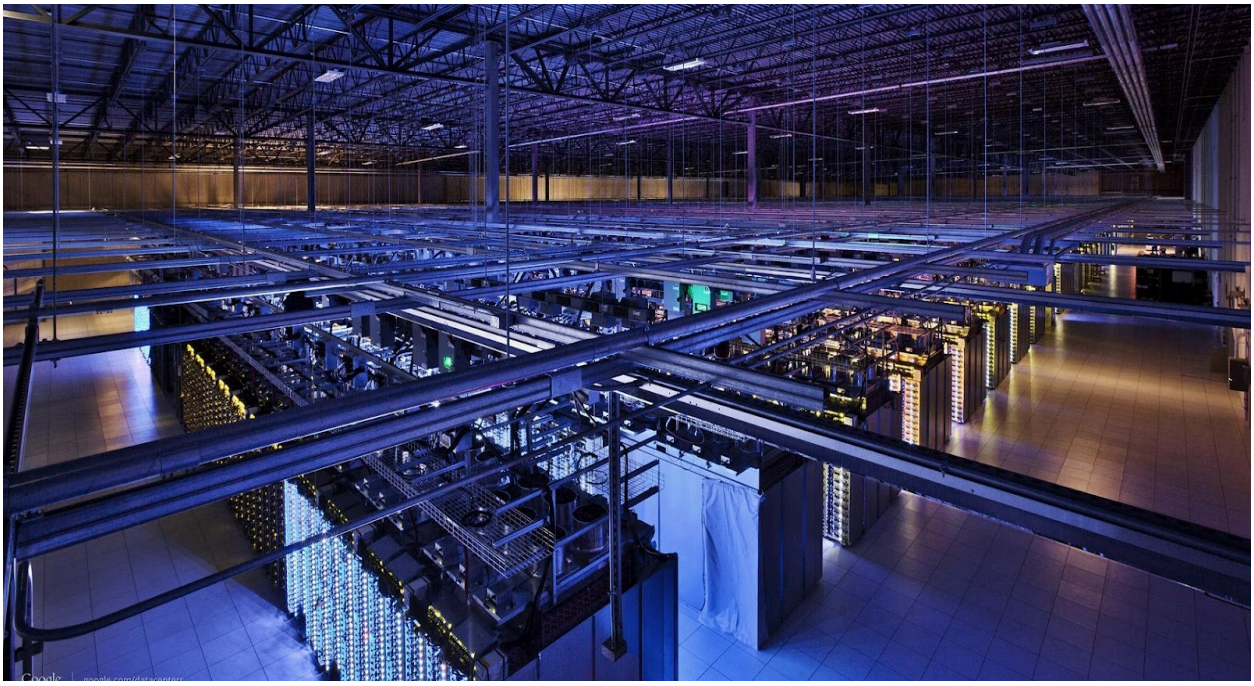
Google Cloudのセキュリティとサービス

以下のセクションでは、前セクションで「安全管理のコンセプト」として紹介したサービス、サポートおよび技術的対策の詳細を説明しています。

インフラストラクチャのセキュリティ

Google では、情報処理ライフサイクルを通じて最先端のセキュリティを提供するように設計されたグローバル インフラストラクチャを運用しています。

このインフラストラクチャは、サービスの安全なデプロイ、エンドユーザーのプライバシー保護を備えたデータの安全な格納、サービス間での安全な通信、インターネット経由の顧客との安全な非公開通信、管理者による安全な操作を実現できるよう構築されています。また、データセンターの物理的なセキュリティ、ハードウェアとソフトウェアのセキュリティ保護、運用セキュリティのサポートに使用するプロセスが相互に補完しあう階層型のインフラストラクチャ セキュリティが構築されています。インフラストラクチャ セキュリティの詳細については、Google インフラストラクチャのセキュリティ設計ホワイトペーパーをご覧ください。



Google Cloud の基盤を構成するサーバー ハードウェアやネットワーク機器においても、侵入や脆弱性からの保護がなされるよう設計および調達されています。

Google のデータセンターには専用のサーバーとネットワーク機器があり、その一部はGoogle によって独自に設計されています。Google のサーバーは、パフォーマンス、冷却、電力効率を最大化するようカスタマイズされており、さらに物理的な侵入からも保護できるように設計されています。一般に販売されているハードウェアとは異なり、Google のサーバーにはビデオカード、チップセット、周辺機器コネクタなどの不要なコンポーネントはありません。これらのコンポーネントが脆弱性を引き起こす可能性があるためです。Google は、コンポーネントベンダーを調査し、慎重にコンポーネントを選択しています。加えて、ベンダーと協力して、コンポーネントが提供するセキュリティ特性を監査および検証しています。Titan などのカスタムチップの提供や、デバイスの起動に使用するコードの実装などの手段を通して、正規の Google デバイスをハードウェア レベルで安全に識別して認証できるようにしています。

契約に基づくセキュリティ

Google Cloud のデータ処理規約には、セキュリティとプライバシーに関するお客様へのコミットメントが明確に記載されています。Google では、お客様や規制当局からのフィードバックに基づいて、長年にわたってこれらの規約を進化させてきました。お客様が Google のシステムに入力したデータは、お客様の指示に従ってのみ処理されるという考えがこの規約の柱となっています。

Google Cloud では、システムの機密性、整合性、可用性を確保するためのセキュリティ対策も実施しています。これらは、セキュリティ対策に将来的に加えられる変更によってセキュリティが低下することはないというコミットメントとともに、契約に詳しく記載されています。お客様向けのセキュリティを継続的に改善することがこのような記載の目的です。

下表にGoogle Cloud およびGoogle Workspace における一部のサービスのSLAを示します。すべてのサービスのSLAはGoogle Cloud のサービスレベル契約で公開しており、Google Cloud の各サービスがお客様の求めるサービス要件を満たすか確認することができます。下表は 2024 年10 月作成時点の状況を表しています。最新の情報は各サービスのリンクから確認することができます。

Google Cloud サービス	対象サービス	SLAで保証される月間稼働率
Compute Engine	複数のゾーンのインスタンス	99.99%
	メモリ最適化ファミリーの単一インスタンス	99.95%

	他の全てのファミリーの単一インスタンス	99.9%
Cloud Storage	Cloud Storage のマルチリージョンまたはデュアルリージョンの標準ストレージクラス	99.95%
	Cloud Storage のリージョナルロケーションにおける標準ストレージ、マルチリージョンまたはデュアルリージョンの Nearline 、Coldline 、Archive ストレージ	99.9%
	Cloud Storage のリージョナルロケーションにおける Nearline 、Coldline 、Archive ストレージ、任意の場所にある耐久性の高い可用性の低いストレージクラス	99.0%
Cloud SQL	高可用性(HA)を備えた Cloud SQL Enterprise Plus エディション	99.99%
	高可用性(HA)を備えた Cloud SQL Enterprise エディション	99.95%
Cloud Functions	-	99.95%
Google Kubernetes Engine	ゾーンクラスタ(コントロールプレーン)	99.5%
	リージョナルクラスタ(コントロールプレーン)	99.95%
	Autopilot クラスタ(コントロールプレーン)	99.95%
	複数のゾーンでの Autopilot Pod	99.9%
	複数のリージョンでの GKE Enterprise Autopilot Pod	99.99%

表 2 : Google Cloud における一部のサービスのSLA

Google Workspace サービス	対象サービス	SLAで保証される月間稼働率
Google Workspace	AppSheet 対象サービス(※1)	99.99%
	Google Workspace 対象サービス(※2)	99.99%

表 3 : Google Workspace におけるサービスのSLA

※1： AppSheet 対象サービス
AppSheet Enterprise Standard (2024/06/17 以前に購入) 、AppSheet Enterprise Plus
※2 : Google Workspace 対象サービス
Gmail 、Google カレンダー 、Google Cloud Search 、 Google ドキュメント 、 Google スプレッドシート 、Google スライド 、 Google フォーム 、Google ドライブ、ビジネス向け Google グループ、Google Chat、Google Meet、Google Keep、Google サイト、Google Jamboard、Google ToDo リスト、Google Vault、Google Voice

セキュリティ認証・評価制度への適合

Google Cloud と Google Workspace では、複数の第三者監査機関によるデータ安全性、プライバシー、セキュリティに関する監査を受けています。Google の第三者監査アプローチは、機密性、整合性、可用性に関する情報セキュリティレベルの保証を提供するために、包括的なものになるように設計されています。お客様は第三者機関によるこうした監査を利用することで、Google が提供しているプロダクトが自社のコンプライアンスとデータ処理のニーズをどのように満たしているかを確認できます。

Google は政府機関等にクラウドサービスを提供する事業者として、「政府情報システムのためのセキュリティ評価制度」（ISMAP）に対応しています。Google Cloud と Google Workspace を含むGoogle のクラウドサービスは、ISMAP の認定を受けたクラウドサービスとして登録されています。ISMAP に登録されているGoogle のサービスおよびプロダクトの詳細はISMAP クラウドサービスリストからご確認ください。

Googleが取得および対応しているその他のサードパーティ認証は以下のとおりです。詳細については、Google Cloud のコンプライアンス リソース センターをご覧ください。

ISO/IEC 27001
ISO/IEC 27001 は、情報セキュリティ管理システムの要件を概説および規定するセキュリティ標準です。Google がセキュリティ管理の包括的で継続的な改善モデルを構築できるようにするための、安全管理のフレームワークとチェックリストが規定されています。Google Cloud と Google Workspace は、ISO 27001 遵守の認証を受けています。

ISO/IEC 27018
ISO/IEC 27018 は、パブリック クラウド サービスにおける個人情報の保護に関するプラクティスの国際標準です。Google Cloud と Google Workspace は、ISO/IEC 27018遵守の認証を受けています。

ISMAP
政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: ISMAP）は、政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録するための政府主導プログラムです。ISMAPは、ISO27001、ISO27002、ISO270017、政府統一基準、NIST SP 800-53を基礎として作成されています。Google Cloud と Google Workspaceは ISMAP コンプライアンスに関する評価を完了し、ISMAP の認定を受けたクラウド サービス プロバイダとして登録されています。Google Cloud のサービスにおける登録内容に関しては、情報処理推進機構（IPA）のウェブサイトにて確認することができます。

NIST SP 800-171
NIST SP 800-171は、非連邦情報システムおよび組織における管理対象非機密情報（CUI）の機密保持のためのセキュリティ標準です。NIST SP 800-171 のセキュリティ統制は、NIST SP 800-53 に関連付けることができ、 Google Cloud サービスはすでに独立した第三者評価を受け、FedRAMP の適用範囲に含まれる NIST SP 800-53 統制と、NIST SP 800-171 に記載のすべての統制要件に準拠していることが確認されています。NIST SP 800-171 の第三者評価の対象となるサービスは、Google Cloudのウェブサイトにて確認することができます。

エンドポイント

情報を安全に取り扱うためには、安全なエンドポイントを使用して情報にアクセスする必要があります。Google では、Chrome プロダクトファミリの一部としてブラウザとOS テクノロジーを開発しました。これらのプロダクトでは、エンドポイントに一般的な脅威が進入するのを防ぐために、攻撃対象領域が非常に小さくなっています。Chrome ブラウザ、Chrome OS、Chromebook をChrome Enterprise で一元管理することで、お客様にこれらのソリューションを提供しています。

Chrome ブラウザは自動的に更新されるコンパクトなブラウザです。Chrome ではセーフ ブラウジングを使用して、既知の不正な URL を登録したデータベースと現在アクセスしている URL を照合し、リスクが高いと見なされるサイトをブロックしたり、警告を表示したりできます。Chrome ではタブだけでなくタブ内のI-フレームまでもがサンドボックス化されています。Chrome 自体は OS 上で隔離されており、他のプロセスにはアクセスできません。

Chromebook にはChrome OS が搭載されています。Chrome OS は読み取り専用の OS であるため、マルウェアがシステム ファイルに感染したり、システム ファイルを変更したりすること

はできません。 Chromebook には、作業コピーとスタンバイ コピーという Chrome OS の 2つのコピーが保持されています。作業コピーの起動に失敗すると、スタンバイ コピーで起動が行われます。これは、アップグレードにスタンバイ コピーを使用し、再起動時にそのスタンバイ コピーを作業コピーにする場合に便利です。そのため、セキュリティが強化されるだけでなく、アップグレードのダウンタイムも発生しません。Chromebook には、ファームウェア、OS、ブラウザコードを検証するTitan C チップが搭載されています。変更が検出された場合、そのバージョンの OS は起動しません。

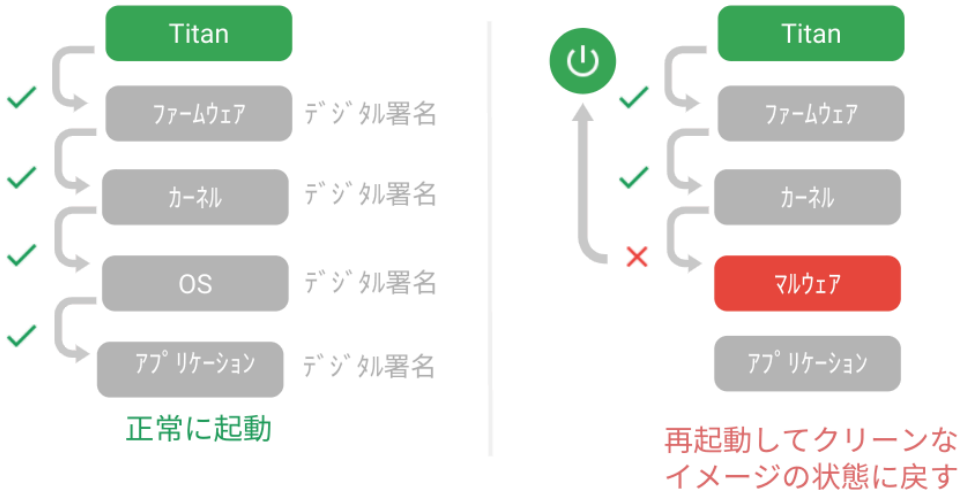


図 3 : Titan C チップによる検証

Chromebook 内では保存データが暗号化されますが、Google Workspace およびGoogle Cloud サービスに大半のデータが保存されるため、Chrome ユーザーがChromebook 上に保存するデータ量はごく少量です。そのため、ランサムウェアのリスクを最小限に減らすことができます。

Chrome Enterprise Upgrade は、Chrome OS 環境で一貫した管理を行うためのクラウドベースの管理システムです。すべてのデバイスに対して1つのコンソールからソフトウェアのデプロイ、アップグレード、Chrome の設定を構成できます。

ID

IDはアクセス制御の要です。 Google Cloud では、複数のIDプロバイダと自らが提供する Cloud Identity をサポートしています。Cloud Identity では機械学習を使用して不正アクセスを検出し

ます。さらに、正しいパスワードを使用した不正侵入者を検出してブロックすることもできます。

また、FIDO準拠のセキュリティ キーなど、複数の2段階認証オプションを含む、強力な形のアカウント保護もサポートしています。Google社員はGoogleアカウントにログインする際に、セキュリティ キーを使用することで、より強力なIDの保護を実現し、フィッシング攻撃を防止しています。お客様側でも同じ対策を実施することをおすすめします。

アクセス制御

情報を安全に取り扱うためには、情報にアクセスする権限を必要最小限の範囲で適切に設定することが重要です。Google Cloud では、すべてのサービスで使用に認証が必要です。認証は主に Identity and Access Management（以下「IAM」） で管理されます。IAM を使用すると、ユーザーやグループなどのメンバーにロールを付与できます。これらのロールはきめ細かい権限で構成されています。厳選されたロールがあらかじめ用意されており、必要に応じてカスタムのロールを作成することもできます。

条件 (IAM Conditions)をロールに適用することもできます。たとえば、午前9時から午後5時まで業務を行う契約社員の場合、アクセスを午前9時から午後5時までに制限する条件を契約社員のロールに追加できます。

Google Cloud には、フォルダツリーを設定してプロジェクトを整理できるResource Managerが用意されています。アクセス制御は階層のどのレイヤでも管理でき、下の階層に継承されるため、適切なガバナンスに威力を発揮します。特定の情報専用のフォルダを作成し、そこにアクセス制御を適用することで、 そのフォルダ内のすべてのプロジェクト間で一貫性を保つことができます。

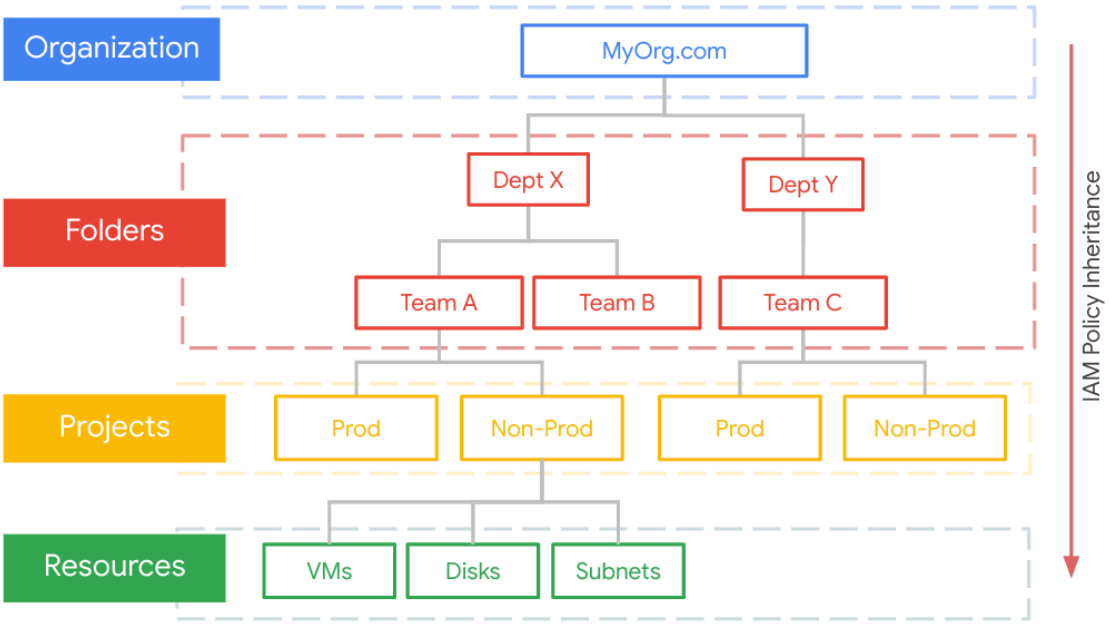


図 4 : フォルダツリーとIAM Policy の継承の関係

企業のお客様にとっての最大の課題の一つはアクセス権の付与ではなく、アクセス権が不要、あるいは過剰な場合にアクセス権を無効にすることです。IAM Recommender では、機械学習を使用して、使用されている権限と使用されていない権限を把握し、過剰なアクセス権を削除するように推奨します。Policy Analyzer では、どの情報に誰がアクセスできるかを把握できるため、監査の場面で役立ちます。

一部の Google Cloud サービスには、IAM に用意されている以上のサービス固有のアクセス制御機能があります。たとえば、BigQuery では、データテーブルのビューに制限をかけたり、特定の条件を満たす行や列をフィルタしたりできます。情報データアナリストが閲覧できる情報を最小限にする場合や、完全に表示しない場合にこの機能が非常に役に立ちます。

Google Workspace では、ユーザーの ID とデバイスのコンテキストに基づいてサービスにアクセス制御を適用できます。各ファイルまたはフォルダの読み取り、コメント入力、編集を行えるユーザーをファイルレベルで定義できます。

ネットワークアクセスの制御

大半のクラウド プロバイダでも使用されている従来のネットワークでは、ネットワーク アクセスを制御するファイアウォール ルールを特定の箇所でしか適用できません。Google Cloud には、はるかに柔軟性が高いファイアウォール ルールが用意されています。単一の VM、タグ付きアセット、同じサービス アカウントを共有するアセット、または複数の要素の組み合わせに適用できます。

すべてのプロジェクトに同じルールを適用する代わりに、階層型ファイアウォール ポリシーを使用して、フォルダレベルまたは組織レベルのプロジェクトに共通のルールを適用できます。

アセットに影響するルールは、コマンドラインと Network Intelligence Center の両方から分析できます。

サービス API へのアクセスを制御することも重要です。Google Cloud では、有効または無効にする API をお客様が決定します。さらに、VPC Service Controls ではプロジェクトで使用する API の周囲に境界を配置できます。また、データ送信をブロックし、データ受信に条件を設定することもできます。

なりすまし攻撃やキャッシュ汚染攻撃からドメインを保護するため、DNSの適切な管理も重要です。DNSSECは、ドメイン名のルックアップに対するレスポンスを認証するドメイン ネーム システム（DNS）の機能です。Cloud DNS は DNSSEC をサポートしており、これらのルックアップに対するプライバシー保護は行いませんが、DNS リクエストに対するレスポンスの改ざんや汚染を防ぎます。

アプリケーションのアクセス制御

Google Cloud には、お客様が独自のアプリケーションを構築できるインフラストラクチャが用意されています。こうしたアプリケーション内のアクセス制御は、お客様が用意するアプリケーション ロジックの一部です。一方で、Chrome Enterprise Premium という Google Cloud のコンテキスト アウェア アクセス システムを活用してこうしたアプリケーションへのアクセスを制御することもできます。

Chrome Enterprise Premium は、一元化された脅威からのデータ保護によるアプリケーションとクラウド リソースへのセキュアなアクセスを実現する、Google のグローバル ネットワークを介して提供されるゼロトラスト ソリューションです。ゼロトラストは、人やデバイスがデフォルトで組織のネットワーク内にあっても信頼されないという考え方に基づいて、組織を保護するために使用されるセキュリティ モデルです。ゼロトラスト アプローチは、信頼できる境

界だけでなく、ネットワーク全体で厳格な ID 認証と認可を行うことにより、暗黙の信頼を排除することを目的としています。

Chrome Enterprise Premium では、どのユーザーがどのような条件でどのアプリケーションにアクセスできるかを定義できます。これらの条件は、状況（時間など）、デバイス（企業で管理しているものなど）、ユーザー の ID と認証（2段階認証など）に関連付けることができます。これにより、情報を扱うシステムの IDをシンプルにするより強力なコントロールを追加することができます。

Chrome Enterprise Premium には、Chromeでデータのアップロード／ダウンロードを調べ、特定のデータが含まれているかどうかを判断する機能もあります。特定のデータの移動をブロックするなど、あらかじめ定義したアクションを取ることができます。

ロギング

Google Cloudには、サービス用の豊富な監査ログの機能が用意されています。ネットワーク ログでは、詳細なネットワーク サービス テレメトリーでネットワークとセキュリティ両方の運用を把握できます。VPC フローログは、ネットワークのモニタリング、フォレンジック、リアルタイムのセキュリティ分析に使用できます。Packet Mirroring でパケットレベルのキャプチャを行えば、コンテンツを分析したり、データをネットワーク侵入検知システムに提供したりできます。ファイアウォール ルール ロギングでは、ファイアウォール ルールの効果を監査、検証、分析できます。NAT ログとDNS ログを脅威分析に使用することもできます。

Google Cloud の Cloud Audit Logsでは、誰が何をいつどこで実行したかなどの API アクティビティが記録されます。データアクセス ログはデータレベルの詳細情報を提供し、データ管理サービスで特に便利です。Google Cloud でお客様のデータを処理することはあ

り ません。ただし、トラブル シューティングのサポートの一環としてデータへ のアクセスをお客様から明確に指示された場合は、そのアクセスもログに記録され、お客様はアクセスの透明性によりこれらのログを確認できます。

Cloud Operations には、OS レベルのエージェント、Fluentd、REST API、クライアントライブラリ、またはサードパーティアプリケーションから送信されたカスタムログなど、さまざまなソースからログを取得できるロギング集中管理ツールが用意されています。ログはログ ビューアを使用することで、リアルタイムで調査・分析を行うことができます。また、ログを可視化して、ログベースの指標と Cloud Monitoring を使用してログに対するアラートを出すこともできます。

Google Cloud には、セキュリティとコンプライアンス両方の要件を満たすためのさまざまなログストレージと保持オプションが用意されています。システムログとデータ アクセス ログはデフォルトで30日間保持され、必要に応じて最大10年まで保持期間を延長できます。管理ログはロックがかかったストレージに400日間保持されます。ログデータは変更が不可能で、保存時に暗号化され、アクセスの透明性によってモニタリングされます。

Google Workspaceには、管理からユーザー、サービス、デバイスに至るまで、あらゆるものに対応する豊富なロギング機能が用意されています。これらのログを Google Cloud のCloud Operations に送信して、統合分析を行うことができます。

脅威の検出

Google Cloud の Security Command Center（SCC）では、Google Cloud のお客様が包括的なリスク管理を行うことができます。 SCC のコンポーネントの 1つに脅威検出があります。SCC は、ログを既知のセキュリティ侵害の痕跡だけでなく、疑わしい動作とも比較してアラートを出します。これらのアラートには、Cloud Functions をトリガーすることで自動的に対処できます。そのため、たとえば、侵害が検出された VM のイメージ化とネットワーク上での隔離をすべて自動的に行うことができます。ログを Google Cloud から Google Security Operations SIEM や Splunk などのサードパーティ SIEM にエクスポートして、脅威をさらに分析したり、クラウド以外のログと関連付けたりして、企業の脅威の全体像を把握することもできます。Google Security Operations SIEM は、すべてのログをセキュリティ侵害インジケーター（IOC）の膨大なデータ ベースと継続的に比較し、一致するものがあればそれを表示します。Google Security Operations SIEM では、ペタバイト単位のログをわずか 1秒で検索できます。

Google Security Operations SOARは、組織がセキュリティの脅威をリアルタイムで検出、調査、対応できるように設計されたプラットフォームです。Google Security Operations SOARは Google の機械学習機能を活用してセキュリティ ワークフローを自動化および合理化します。

これにより、セキュリティ アナリストは、高度なコーディング知識を必要とせずに、インシデントの調査、ワークフローの作成、対応アクションの自動化を行うことができます。

マネージドサービス

システムのメンテナンスは、ほとんどのお客様にとって複雑でコストがかかり、面倒な作業です。そのため、Google がメンテナンスしているマネージド サービスを使用することをおすすめします。下の図にあるように、Google に任せるサービス管理の度合いが増えるほど、よりデータに集中して、基盤となるインフラストラクチャの責任の多くを Google に担わせることができます（責任共有モデル）。

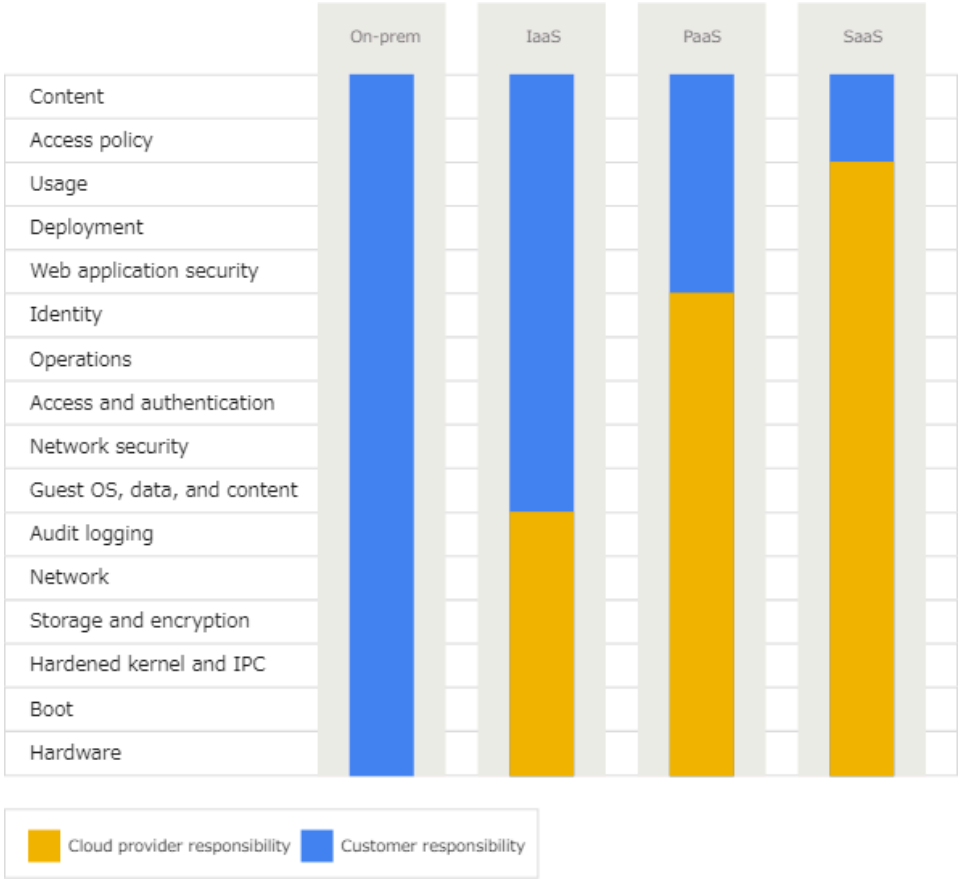


図 5 : Googleとお客様のGoogle Cloudでの責任範囲

コンピューティング サービスが必要な場合でも、自社管理が不要なサービスを利用することをおすすめします。たとえば、Cloud Functions では、管理の手間を増やすことなくシンプルな関数を実行できます。GKE ではノードの自動アップグレードを使用してコンテナを管理できるため、メンテナンスの負担が軽減されます。

K8s の ID、認可、およびセキュリティ ポリシー コードの大部分を設計、作成したチームが GKE のセキュリティ管理も担当しています。このチームは、K8s の開発当初からすべての重大な脆弱性の調査、トリアージ、パッチ適用、通知を主導または担当しています。

セキュアなCI/CDパイプライン

脅威アクターはアプリケーションに読み込まれるコードを変更することで、システムや情報を悪用する場合もあります。だからこそ、継続的インテグレーションと継続的デリバリー（CI / CD）パイプラインの一環として、セキュリティ対策を実施することが非常に重要です。

Google では健全なコード レビュープロセスを設けることを推奨しており、このプロセスに関するプラクティスと考えを紹介したガイドを一般公開しています。

Google Cloud にはノード用の COS（Container Optimized OS）が用意されています。Container-Optimized OS はフットプリントが小さく、セキュリティの脅威にさらされる可能性が最小限でありながら、読み取り専用の最小ルートファイルシステム、ファイルシステムの整合性チェック、遮断されたファイアウォール、監査ログといった重要なセキュリティ機能が組み込まれています。自動更新によって適切なタイミングでセキュリティの脆弱性が自動的にふさがれることで、侵害のリスクがさらに軽減されます。シールドされた GKE ノード は、Titan チップを搭載したハードウェア上に構築されており、ホストブートローダーからゲスト COS カーネルにいたる出所検証シーケンスを開始して、エンドツーエンドのサプライチェーンセキュリティを実現します。

脆弱なコンテナを検出して対処することが重要になります。Google Cloud では、Artifact Registryに追加されたコンテナをスキャンして、不具合を検出できます。

コンテナ ポリシーは Anthos Container の Policy Controller を使って設定できます。Policy Controller は ガバナンスに最適で、会社のポリシーで許可されている権限を超えてプロジェクトチームがコンテナをデプロイしないようにするために使用できます。

Binary Authorization を使用することで、CI / CD パイプラインのさまざまなステップを通過するための署名を定義できます。これらの署名はデプロイの条件としてチェックできます。これ

により、すべてのステップが確実に通過されるようになるだけでなく、不正なコードが本番環境にデプロイされるのを防ぐことができます。

リスクの検出

OWASP がターゲットとする一般的な構成ミスや脆弱性を探す Web Security Scanner を実行することで、アプリケーション コードをチェックすることができます。Google Cloud のプレミアム サービスでは、Google Cloud をスキャンしてウェブ アプリケーションを検索し、認可なしで密かに構築されたアプリケーションをあぶり出すこともできます。

Security Command Center (SCC) は、Google Cloud を利用している組織全体で構成ミスや脆弱性をチェックし、それらをクラウド アセットのリストにマッピングします。実際に SCC は、アセットだけでなく、 ISO 27001、PCI DSS、Google Cloud の CIS ベスト プラクティスなど、さまざまなコンプライアンス フレーム ワークにもリスクと脅威をマッピングします。これにより、Google Cloud に配置した情報に影響を与えるインシデントを防止、検出するという義務を果たすことができます。さらに、Google Cloud セキュリティ ベスト プラクティス センターでは、Google Cloud にワークロードをデプロイする際の、セキュリティとコンプライアンスの目標を達成するためのベスト プラクティス を提供しており、お客様は設定の誤りを防止する対策を施すことができます。

Google Workspace では、セキュリティ センターと呼ばれる 1 つの包括的なダッシュボードで、セキュリティ イベント、およびセキュリティ対策の有効性を示す指標を把握できます。このダッシュボードでは、組織全体にわたって悪意のあるメールを削除したり、情報ファイルの共有を調査して潜在的なデータ流出を特定、阻止したりするなど、セキュリティとプライバシーの問題を特定し、優先順位を付け、対処することができます。

データガバナンス

企業内のさまざまなシステムや部署で情報の異なるコピーを作成するため、情報の追跡は組織にとって課題となる場合があります。データ ガバナンスこそが鍵であり、それを支援できるのが Google Cloud です。Google Cloud ではデータ ガバナンスを次のように定義しています。

1. 情報の検出
2. 情報へのラベル付け
3. 情報へのルールの適用

Google Cloud

Data Catalog では、DLP API を使用して場所に関係なくメタデータ ラベルを検索して情報に適用できます。これらのラベルを使用してルールを適用することで、処理中のジョブまたはデータ分析システムで特定のデータの表示・非表示を制御できます。

お客様は、日本にある2つのリージョンを含め、ワークロードを実行するリージョンを選択することができます。

Google Workspace には DLP 機能もあります。管理者は DLP 機能を使用して、ファイル内の情報を検出し、アラートなどの操作を行ったり、外部との共有を制限するなどの設定を行ったりできます。

データの変換

複数の変換手法を使用して、情報を取り扱うさまざまな場面で情報を非表示にしたり削除したりできます。DLP API では、情報をマスキングまたは秘匿化することで情報を削除できます。

ID	Job Title	Phone	Comments
359740	Senior Engineer	307-964-0673	Please email them at jane@imadethisup.com
981587	VP, Engineer	713-910-6787	none
394091	Lawyer	692-398-4146	Updated phone to: 692-398-4146
986941	Senior Ops Manager	294-967-5508	none
490456	Junior Ops Manager	791-954-3281	Tried to verify account with their SSN 222-44-5555

→

ID (FPE)	Job Title	Phone	Comments
438422	Engineer	307-###-####	Please email them at [Found Email]
530375	Engineer	713-###-####	none
496534	Lawyer	692-###-####	Updated phone to: 692-###-####
242348	Ops	294-###-####	none
593887	Ops	791-###-####	Tried to verify account with their SSN [Found SSN]

表 4 : DLP API によるマスキング

情報を秘匿しながらも、その情報を使わなければならない場合もあります。これは 2つの方法で実現できます。データテーブルのフィールドとして使用する場合、DLP API を使用して情報を一意のトークンで置き換えることができます（トークン化）。保存中または転送中のデータのみを秘匿する必要があるものの、後で秘匿を解除する場合は暗号化の方が適しています。

Google Cloud には多くの暗号化オプションが用意されています。Cloud Key Management Service（Cloud KMS） では、API を介してアクセスするマネージド サービスとして暗号操作を行うことができます。また、お客様管理の暗号鍵（CMEK）を、Cloud KMS にて管理し、Google Cloud の保存データを保護する鍵の所有権を持ち、制御することもできます。

Cloud HSM では、バックエンドが FIPS-2 レベル 3 認定の HSM を利用して、同じ Cloud KMS のサービス、APIアクセスを使用することができます。セキュリティの要件に応じて、お客様ご自身で用意した暗号鍵を用いることもできます。オンプレミスなど、Google Cloudのデータセンターの外部にあるHSMを利用したい場合には、External Key Manager を使ってフロントエンドで Cloud KMS を使用することもできます。

データの削除

Google Cloud のお客様データの所有権はお客様にあり、いつでも削除できます。当該データを削除すると、そのデータは直ちに使用できなくなり、関連するさまざまなサービス コンポーネントにまで対象が及ぶデータ消去プロセスが開始されます。データ消去プロセスが完了するのに最大で180日かかる場合があります。プロセスが完了すると、データを元に戻すことができなくなります。詳細については、Google Cloud と Google Workspace に関するホワイトペーパーをご覧ください。

バックアップとレジリエンス

非常時における組織の業務継続のために、システム復旧計画の策定やバックアップが必要です。Google Cloud におけるバックアップや障害復旧のソリューションを利用することにより、様々なデータ損失につながる脅威や障害に備えることができます。

Google Cloud のプロダクトおよびサービスでは、Backup for GKE、 Persistent Disk のスナップショット、 Cloud SQL のバックアップ、 Filestore のバックアップ、 地理的に冗長な Cloud Storage などの幅広いデータ保護機能を提供しています。また、Google Cloud のリソースを複数のリージョンとゾーンで作成してデプロイすることで、復元性に優れた高可用性システムを構築することもできます。

バックアップと DR サービスでは、さまざまなワークロードを保護し、一元化されたダッシュボードからバックアップと復元を管理できます。データ破損からの回復、データ損失、ランサムウェアからの回復、テスト / 開発のためのデータベースのクローン作成などの重要なユースケースに対応します。

また、クラウドサービス事業者であるGoogle の管理する基盤側でデータ損失等が発生しないよう、Google のプラットフォームの構成要素は冗長性に優れた設計になっています。Google のデータセンターは地理的に分散されているため、ある地域の自然災害や局地的な停電などでグローバルなプロダクトが使用不可能となった場合においても、その影響は最小限に抑えられます。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、プラットフォーム サービスとコントロール プレーンは自動的かつ迅速に別の施設に切り替わり、プラットフォーム サービスが中断されずに継続されます。

Google のシステムは、プラットフォームをアップグレードする必要がある場合のダウンタイムやメンテナンスの時間枠を最小限に抑えるように設計されています。Google Cloud が設計からオペレーションまで復元力と可用性をコア インフラストラクチャとサービスに組み込む方法については、Google Cloud インフラストラクチャ信頼性ガイドをご覧ください。

また、Google Cloud Service Healthダッシュボード（CSH）には、Google Cloud に含まれるプロダクトのステータス情報が表示されます。ステータスには、プロダクトの中断、停止、一時的な問題に関する情報メッセージなどが含まれています。これにより、お客様は、現在発生しているインシデントの情報を把握し、Google Cloudに構築したシステムの障害原因を確認することや復旧目途を整理することができます。

サードパーティー サプライヤーの管理

医療機関等が選定・利用するクラウドサービスの提供者がその役務内容を再委託している場合、当該サービス提供者がサプライヤーの管理を適切に行っているかについても注意を払う必要があります。

Google Cloudでは、ほとんどのデータ処理アクティビティで、Google 独自のインフラストラクチャでサービスを提供しています。ただし、カスタマー サポートやテクニカル サポートなど、Google Cloud に関連するサービスを提供するためにサードパーティのサプライヤーを利用する場合があります。

Google は、サプライヤーに業務委託する前に、当該サプライヤーのセキュリティとプライバシー対策の実施状況を評価しています。この評価では、サプライヤーが、データへのアクセスや、担当するサービスの範囲に適したレベルのセキュリティとプライバシーを提供しているか確認します。 サプライヤーのリスクを評価した後、Google と当該サプライヤーは、所定のセキュリティ、機密保持、プライバシーの各契約を締結します。

詳細については、サプライヤー行動規範をご覧ください。

Google Cloud

トレーニングとコンサルティング

Google Cloud には、お客様のために、次のような幅広いトレーニングとコンサルティングのサポートが用意されています。

- Google Cloud サービスのデモと適切なサービスの選択のサポートを行うプリセールス スタッフ
- お客様のチームにトレーニングを行うトレーニング スタッフと教育スタッフ
- Cloud OnAir と YouTube 動画
- 都合に合わせてトレーニングが受けられるオンライン トレーニング パートナー
- 必要なスキルを身に付けられる認定資格プログラム
- 複数の言語に対応したオンライン ドキュメント
- 実際に Google Cloud のサービスを使いながら学習できるGoogle Cloud Skills Boost
- 販売後のコンサルティング サービス
- 大規模なソリューションの構築と管理を実現するシステム インテグレーター パートナーシップ
- アイデアを共有してインスピレーションを与える、ブログ、ナレッジ、動画、チャットルームで 構成された活発なオンライン コミュニティ

パートナーソリューション

Google Cloud はさまざまなセキュリティ ソリューション企業と提携して、Google Cloud Marketplaceや その他のパートナーシップ契約を通じてお客様がパートナー企業のソリューションを利用できるようにしています。また、Google Cloud パートナー以外の企業のものも含めた大半のセキュリティソリューションをサポートできる、基本的なコンピューティング サービスも提供しています。

Google Cloud のセールスチームでは、お客様のセキュリティ要件をお聞きしたうえで、ユースケース に最適なパートナー ソリューションに関する助言を提供しています。