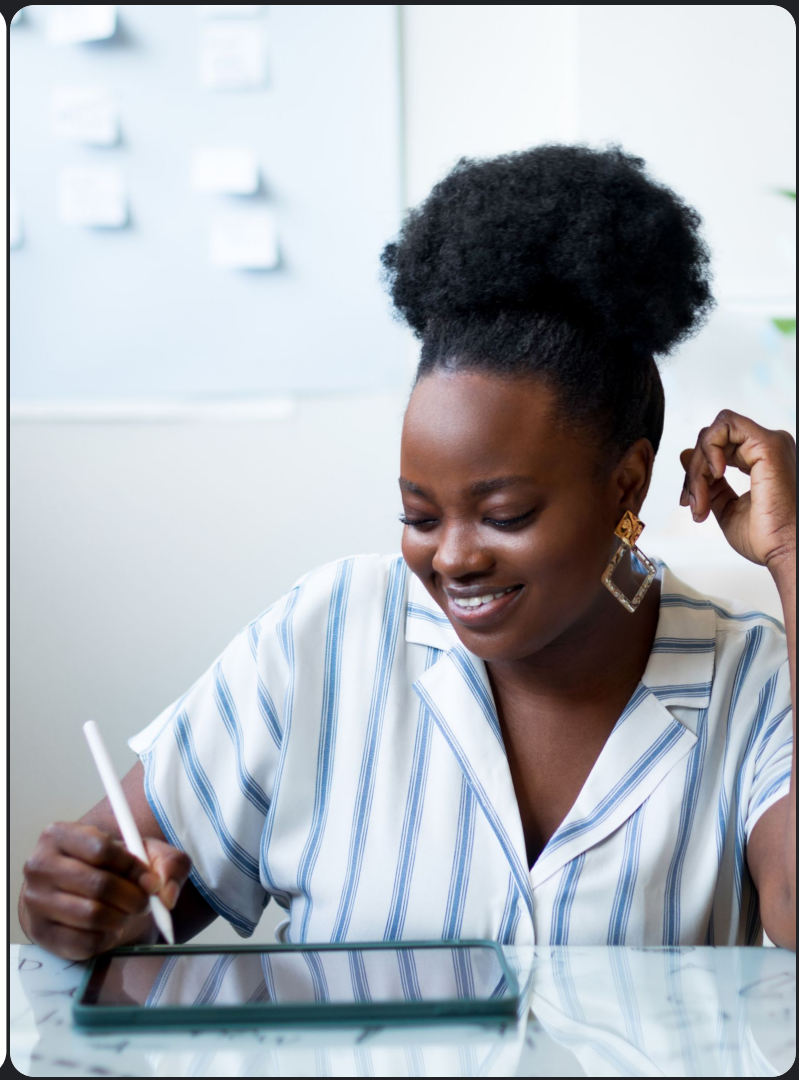
Google Cloud

Google Cloud で安全なデータ プラットフォームを構築する



Google Cloud

はじめに



データ志向が求められる中、組織は膨大な量のデータと向き合わなくてはなりません。機密性の高いビジネスデータや顧客データから、行動分析やマーケティング分析のためのデータまで、アクセス、管理、分析しなければならないデータの種類も量も増え続ける一方です。組織全体でデータを利活用してよりアジャイルに向かい、イノベーションを推進するためにクラウド サービスを導入している企業は増えましたが、クラウドデータを保護する最適解にはまだ遠く、デジタル トランスフォーメーションを実現するために乗り越えなければならない課題として残っています。

オンプレミスのデータセンターから移行するデータやアプリケーションが増えるにつれ、それらは従来のセキュリティ メカニズムやインフラストラクチャから離れてしまうため、新しい防御手段が必要になります。オンプレミス データ セキュリティの基礎的な要素の多くを維持しつつ、それらをクラウドに適応させる必要があります。

しかも、脅威の進化がさらなる課題をもたらします。Mandiant は 2024 年の M-Trends レポート で、攻撃者はクラウド移行の傾向を追いかけて、標的をクラウドでホストされているデータにすり変え、クラウド コンピューティング リソースを攻撃に使用するようになったと指摘しています。たとえば、2024 年前半に注目を集めたサイバー攻撃は、データ窃盗と恐喝を目的として、マルチクラウド データ ウェアハウジング SaaS プラットフォームを標的としていました。攻撃者は、盗んだ認証情報を利用して顧客インスタンスを組織的に不正利用し、サイバー犯罪フォーラムで被害者のデータを販売する広告を掲載し、多くの被害者を恐喝しようとしました。

Google Cloud では、運命共有モデルを採用し、Google Cloud のお客様の積極的なパートナーとして、プラットフォームでワークロードを安全にデプロイできるよう緊密なサポートを提供します。セキュア バイ デフォルトの構成、ブループリント、ポリシー階層、高度なセキュリティ機能を提供してベスト プラクティスの実践をお手伝いし、データ プラットフォームやツールをまたいで一貫したセキュリティを確立できるよう支援いたします。

この電子書籍は、データとセキュリティの責任者様を対象に、Google Cloud のデータ セキュリティ機能を包括的に紹介しています。クラウド内の機密性の高いデータアセットを保護し、データ主導のイノベーション戦略を自信を持って推進するために、Google Cloud がどのような支援を提供できるかについて詳しく説明しています。



Google Cloud

目次

BigQuery プラットフォーム レベルのセキュリティ	07
アクセスとガードレール	13
境界保護	18
データ保護	24
モニタリングとコンプライアンス	30
詳細	35

あらゆるレベルで データ保護を強化

データの完全性と機密性は、デジタル時代と呼ばれる昨今の最重要事項です。内外の脅威から重要なデータアセットを保護できるように、Google Cloud では多層型のデータ セキュリティが設計されています。

Google Cloud の強力なデータ ウェアハウス ソリューションである BigQuery はきめ細かい制御が可能で、アクセスと共有の管理を精密に行うことができます。アクセスとガードレールのメカニズムにより、認証プロトコルがさらに強化され、承認された個人とデータのみが特定のリソースとやり取りできるようにしています。保存時、使用時、転送中の機密情報は暗号化によって保護され、そのライフサイクルを通じて機密性が確保されます。

境界保護が堅牢な外側の防御レイヤを構築し、意図しない、または悪意のあるデータ侵害を未然に防止します。能動的なモニタリング機能により、プラットフォームの潜在的な脆弱性を絶えず探して可視化し、コンプライアンスとセキュリティの要件が遵守されていることを確保します。



「見えないところで活躍するセキュリティソリューションのおかげで、Commerzbank は時間とリソースを大幅に節約しながらセキュリティを強化しただけでなく、クラウドにおけるセキュリティの定義を考え直すことができました。Google Cloud の協力を得て打ち立てた新たな基準は、当社だけでなく、すべての人々がクラウド セキュリティに対する理解を深めるために役立つと思います。」

Christian Gorke 氏

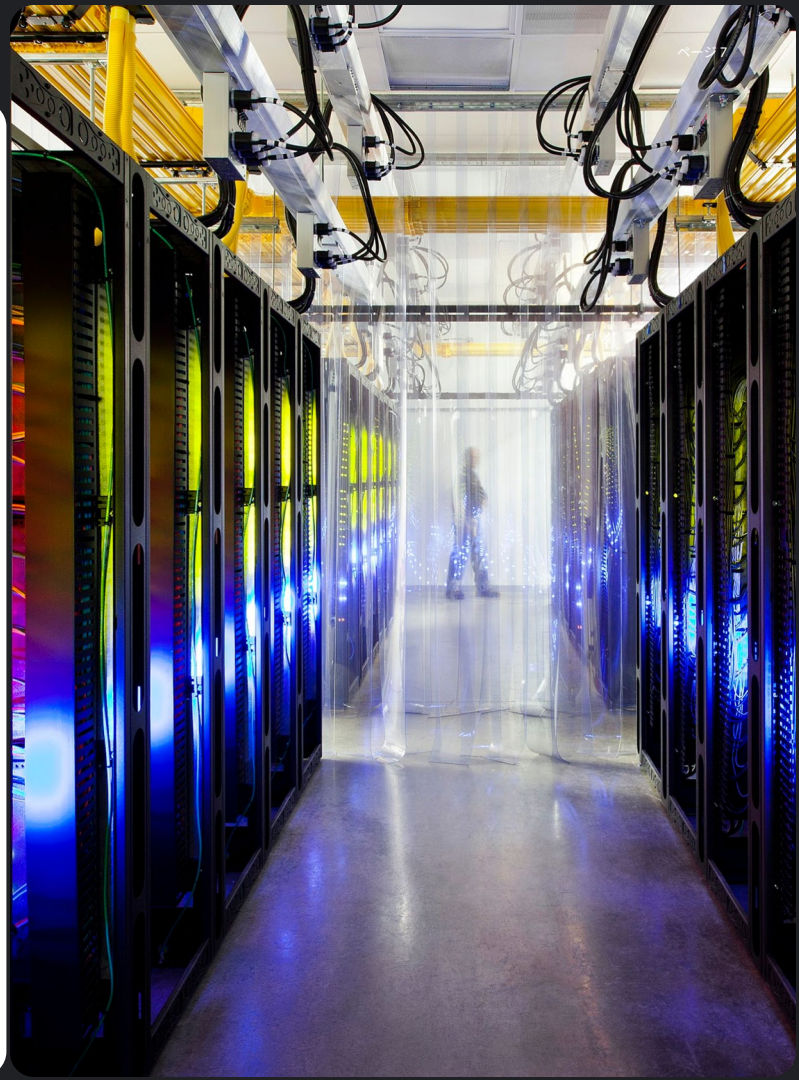
Commerzbank、バイス プレジデント兼
サイバー センター オブ エクセレンス責任者



COMMERZBANK

出典: https://cloud.google.com/customers/commerzbankag

BigQuery プラットフォーム レベルの セキュリティ



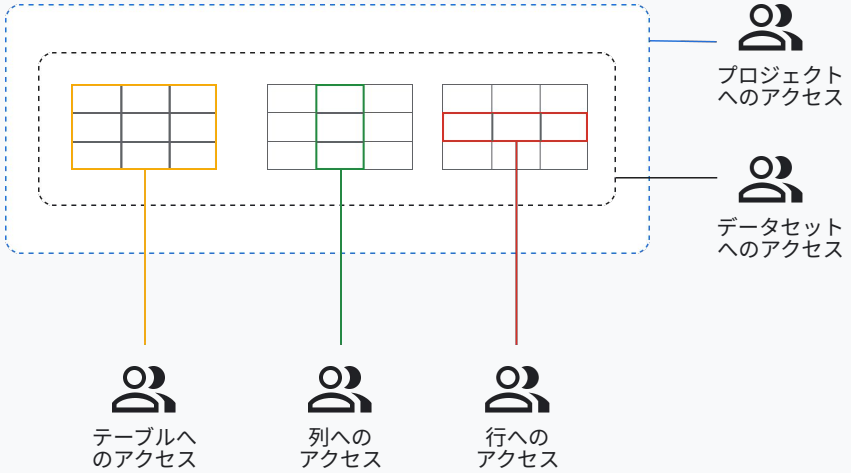
セクション 01

BigQuery のデータ セキュリティの概要

BigQuery には、データ暗号化、マスキング、きめ細かいレベルのアクセス制御などの堅牢なセキュリティ機能がデータ プラットフォーム レベルで組み込まれており、データリソースを保護し、安全なデータ共有やガバナンス ポリシー管理を支援しています。

BigQuery は Cloud Identity and Access Management（IAM）と緊密に連携し、データへのアクセス制御とあらゆるクラウド リソースの一元管理を実現しています。きめ細かいアクセス制御を使用すると、プロジェクト、データセット、テーブル、行、列など、リソースポリシーをより詳細に定義できます。

BigQuery の細分化されたアクセス制御を利用すると、
きめ細かいレベルでリソース ポリシーを定義できる



BigQuery の IAM のロールと権限の割り当ての詳細

暗号化とマスキングで機密データを保護

BigQuery は、データがディスクに書き込まれる前に、そのすべてを自動的に暗号化します。暗号化されたデータは、承認済みのユーザーが読み取りを行う際に自動的に復号されます。Cloud Key Management System を使用すると、暗号鍵の管理と保管の柔軟性がさらに高まります。

データ暗号化の詳細 →

BigQuery は、列レベルでのデータ マスキングもサポートしています。データ マスキングを使用すると、ユーザー グループの権限に基づいて列データを難読化しながら列へのアクセスを許可できます。Sensitive Data Protection を使用すると、データを自動的にスキャン、検出、分類して、IAM でアクセス ポリシーを設定できます。

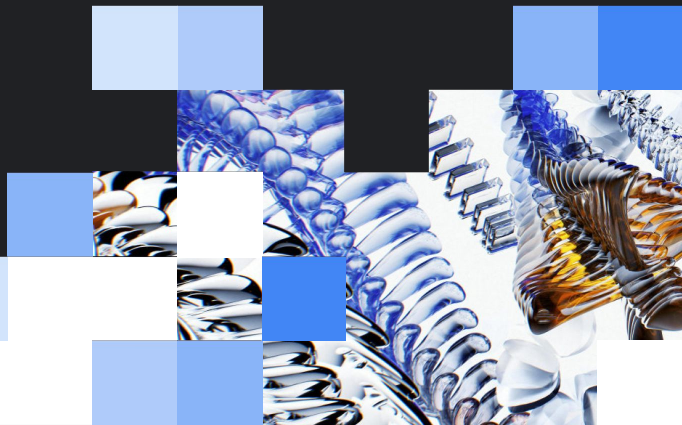
データ マスキングの詳細 →

BigQuery のデータ マスキング



「動的なフィールド レベルの暗号化を可能にすることは、高い安全性を保ち、FedRAMP、PCI、GDPR、CCPA など、複数の規則を遵守した厳格なセキュリティ ポリシーによって規制されたアセットを管理する当社のデータ ファブリック プラットフォームにとって最も重要なことです。BigQuery の列レベルの暗号化機能により、外部で暗号化されたデータを BigQuery で安全に復号できるようになり、800 人以上のアナリストが行う分析ユースケースの制限を取り除きました。」

Kumar Menon 氏
Equifax、CTO



EQUIFAX

出典: https://cloud.google.com/blog/ja/products/identity-security/announcing-new-bigquery-capabilities-to-help-secure-sensitive-data?e=48754805

安全なデータ共有を実現

BigQuery Analytics Hub は、組織間でデータアセットを効率的かつ安全に交換できるプラットフォームです。境界を越えてアセットの共有を簡単に、スケーラブルに管理できます。より厳格な規制要件やプライバシー要件の対象となり得るデータを共有する場合は、BigQuery のデータ クリーンルームが追加の保護レイヤとして機能し、プライバシーを重視した方法でデータの共有、分析、コラボレーションができるようにします。

安全なデータ共有の詳細 →

大規模なデータ ガバナンスを支援

BigQuery には、データレイク、ウェアハウス、データベースデータ上に分散されたデータや AI アーティファクトを管理、統制するための Dataplex が監視レイヤとしてプリロードされています。データ ライフサイクルの全フェーズをモニタリングしながら、データ プロファイルの確立、データ品質の評価、リネージの特定、ドメインへの分類と整理ができるようユーザーを支援します。さらに、リージョン全体が停止した場合に備えて、BigQuery は障害復旧シナリオにも対応しています。

データ ガバナンスの詳細 →

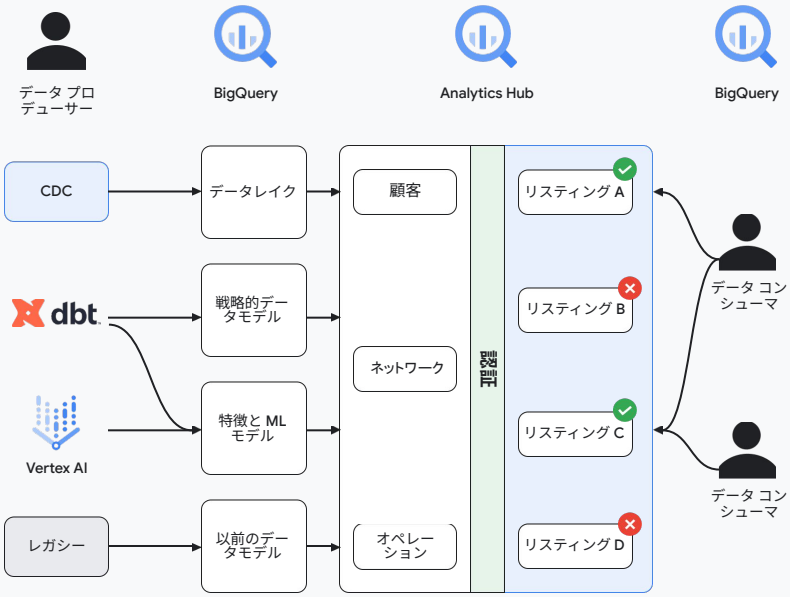


Virgin Media O2、Analytics Hub でデータ共有を簡素化

メディア・通信会社の Virgin Media O2 は、業務の最適化、戦略の推進、意思決定者への支援を実現するために、組織全体でクラウドデータ共有を活用しています。

同社のデータ プラットフォーム チームは、Analytics Hub が提供するスケーラビリティ、セルフサービス機能、データタグや品質ガバナンスのシンプル化されたモデルを確認した後、Analytics Hub の試験運用を行うことを決定しました。

Analytics Hub を約 25 のチームにロールアウトした結果、トレーニング、サポート、デプロイ時のパイプライン問題、コミュニケーションのオーバーヘッドに費やす時間が、以前のソリューションと比較して週最大 30 時間削減されました。ダッシュボードを構築してサブスクライバーとその広範なチームにデータアクセスを許可し、アクセスの民主化を実現しました。



プラットフォーム エンジニアリング - ガバナンス、プライバシー、トレーニング、オブザーバビリティ

Virgin Media の事例の詳細 →

アクセスとガードレール



セクション 02

ID とアクセスの管理

データを保護し、コラボレーションを促進

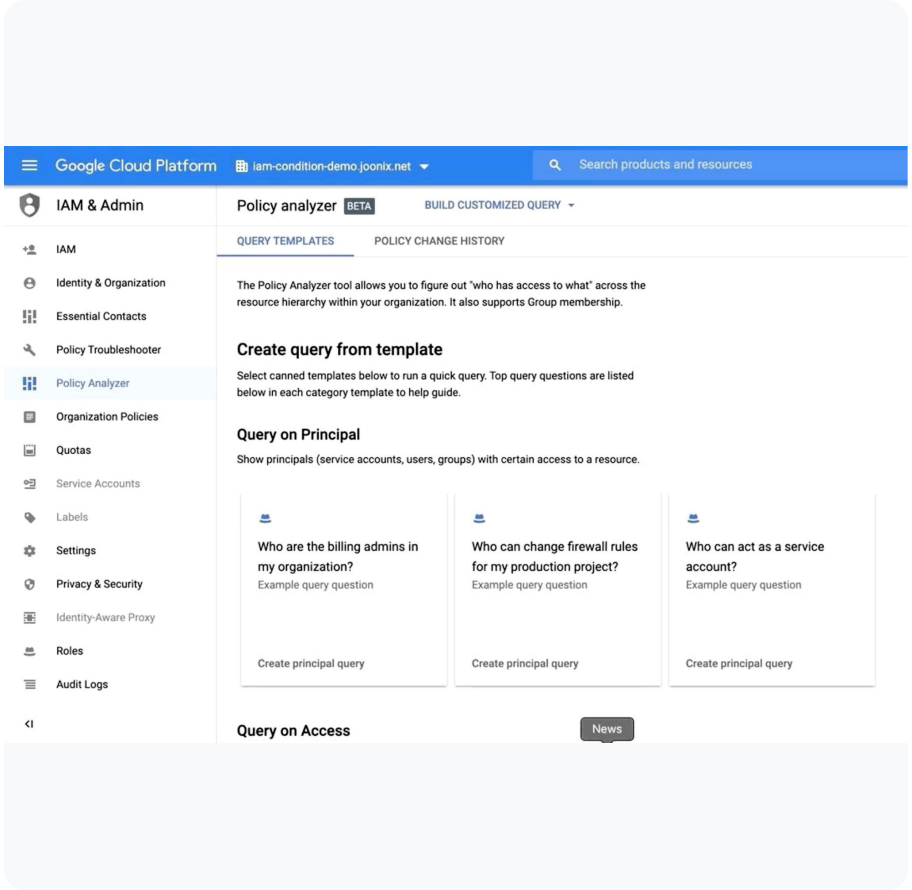
Google Cloud の Identity and Access Management（IAM）ソリューションは、データにアクセスできるユーザーをきめ細かく制御します。

Cloud IAM を使用すると、重要な BigQuery データだけでなく、Cloud Run、Cloud Functions、GKE リソースなどの他の主要サービスのデータも直接管理でき、適切なユーザーに適切なアクセス権を付与して、リスクを最小限に抑えることができます。

不正ログインが心配ですか？
多要素認証は、Google 認証システムやフィッシングに強い Titan セキュリティ キーなど、複数の認証方法を提供して追加の防御レイヤを構成し、侵害を防止してデータを安全に保ちます。

外部とのデータ共有や連携が必要ですか？
Workforce Identity 連携により、サードパーティの ID プロバイダとシームレスに統合できるため、パートナーや請負業者と連携する場合でも、安全かつ管理されたアクセスを確保できます。

IAM の詳細 →



アクセス ポリシーと組織のポリシー

クラウド セキュリティをきめ細かく制御

Google Cloud の Identity and Access Management（IAM）では、アクセス ポリシーと組織のポリシーの 2 つのタイプのポリシーにより、クラウド リソースを誰が操作し、どのようなアクションを実行できるかを管理するための堅牢なフレームワークを提供します。

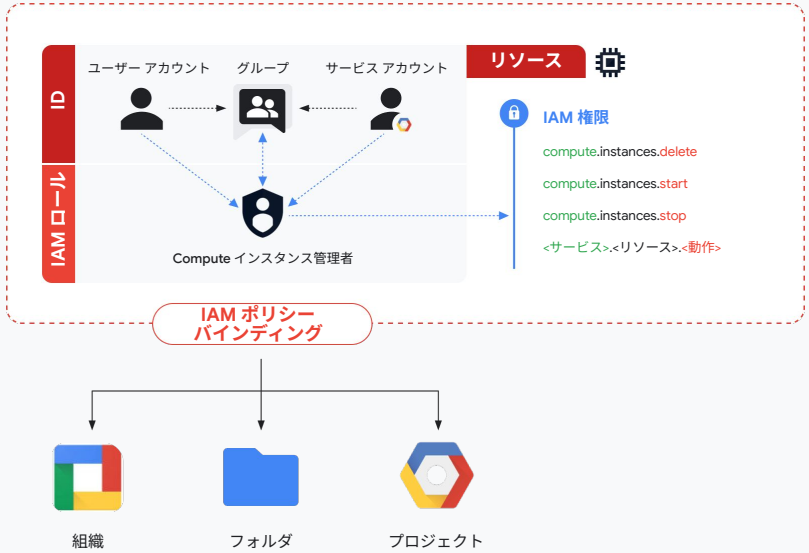
組織のポリシーは、Google Cloud プロジェクト全体のリソースの使用状況や構成を管理するために作成するもので、プリンシパル（ユーザー、グループ、またはサービス アカウント）を特定のロールに関連付けるバインディングで構成されます。それぞれのロールによって、特定のリソースに対して各プリンシパルに付与される権限が決まります。

これをさらに一歩進めてきめ細かな制御を可能にしたのが、IAM アクセス ポリシーです。IAM 許可ポリシーと IAM 拒否ポリシーの両方を定義できるため、特定のリソースへのアクセスやアクションを明示的に許可または禁止できます。最小権限の原則を実践し、ユーザーがタスクを実行するために必要な最小限の権限のみ持つようにするには、このレベルの粒度が不可欠です。

これらの機能を組み合わせることで、安全かつ適切に管理されたクラウド環境を構築し、アクセスを厳格に管理しながら機密データと重要なオペレーションを保護することができます。

組織のポリシーの詳細 →

IAM ポリシーは ID、ロール、リソースをバインドする



組織内アクセス制限

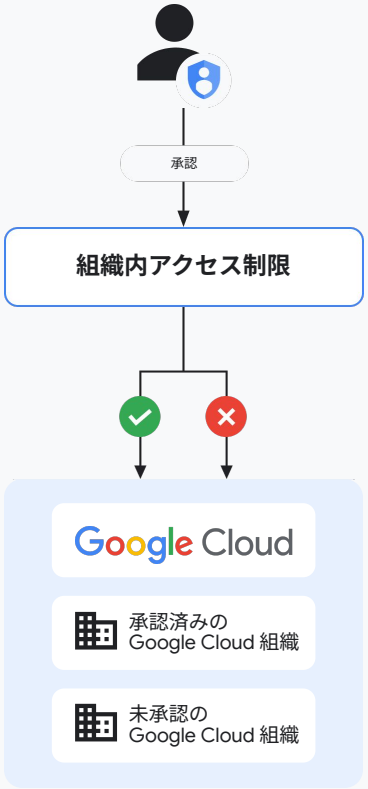
データの引き出しに対する保護の強化

Google Cloud の組織内アクセス制限も防御レイヤのひとつです。承認された Google Cloud 組織のみにアクセスを制限することでデータ漏洩に対する防御力を強化し、貴重なデータを盗み出そうとするフィッシングやインサイダー攻撃などの脅威を阻止します。

組織内アクセス制限は、Cloud IAM（Identity and Access Management）と組み合わせることでさらに強力になります。IAM が組織内の特定のリソースへのアクセスを制御するのに対し、組織内アクセス制限は組織自体へのアクセスを制御します。この二重の保護レイヤにより、信頼できるエンティティのみがデータを操作できるようにします。

Google Cloud は、組織内アクセス制限ヘッダーに基づいてリクエストを検査し、組織のポリシーを厳格に適用します。このプロアクティブなアプローチにより、不正アクセスに対する保護を強化しています。

つまり、組織内アクセス制限を構成して Google Cloud 環境の周囲に安全な境界を構築することで、データへのアクセスを信頼できるネットワークだけに限定できます。



「Identity and Access Management はクラウド セキュリティに不可欠であり、当行のような業界では最小権限と組み合わせて使うことが多いです。特定の ID を持つプリンシパルが特定リソースへのジャストインタイム アクセスを必要とする場合、時間制限付きで承認ベースのアクセス権昇格機能が絶対に必要です。Google Cloud の Privileged Access Manager により、承認プロセスや監査ロギングなど、当行が 求めていた機能を提供してくれる効率的なサービスを利用できるようになりました。セキュリティ シナリオが簡素化されただけでなく、アドホックなデータ分析情報、インフラストラクチャ知識の共有、ペネトレーション テストのサポートなどのセキュリティ向上の機会が生まれました。」

Christian Gorke 氏

Commerzbank、バイス プレジデント兼
サイバー センター オブ エクセレンス責任者



COMMERZBANK

出典: https://cloud.google.com/blog/ja/products/identity-security/move-from-always-on-privileges-to-on-demand-access-with-privileged-access-manager?e=48754805

境界保護

セクション 03



VPC Service Controls

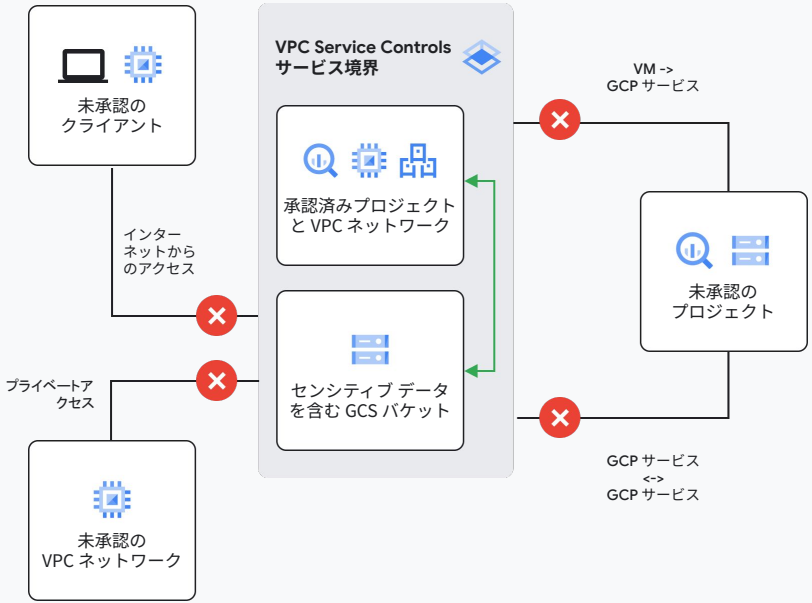
クラウドデータを守る仮想の堀

VPC Service Controls は、意図しない漏洩を防ぎ、標的型攻撃を阻止するのに役立ちます。この Google Cloud プロダクトは、貴重なデータの周囲に保護境界を設定し、データアクセスと移動をきめ細かく制御できるようにします。

上り（内向き）ポリシーを使用して、保護されたゾーン内のデータにアクセスできるユーザーまたはサービスを厳密に定義できます。下り（外向き）ポリシーを使用してデータの送信先を制限すると、追加の防御レイヤとして機能します。

細分性を備えた Cloud IAM ポリシーと組織内アクセス制限を VPC Service Controls によって強力に補完し、データ漏洩に対する多層防御を構成できます。機密情報が安全に保護されていると確信して、データ侵害以外のイノベーション的な作業に集中できる時間を増やすことができます。

VPC Service Controls の詳細



Cloud NGFW

高度なネットワーク保護を簡素化



Cloud Next-Generation Firewall（NGFW）は、高度なセキュリティ機能を提供するクラウドネイティブのソリューションです。防御力を損なわずにネットワーク セキュリティを簡素化し、貴重なデータを保護します。

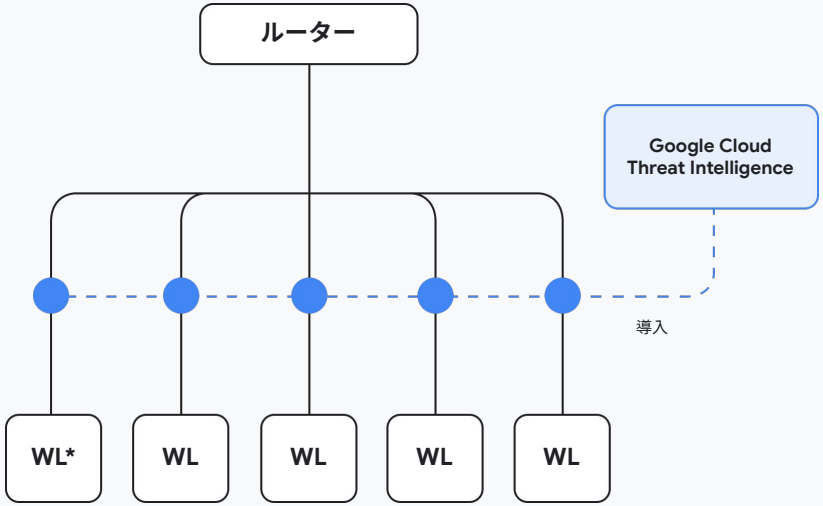
クラウド向けに設計されており、迅速かつ簡単にデプロイでき、マネージド型ネットワーク脅威防止機能により安全な環境を維持します。

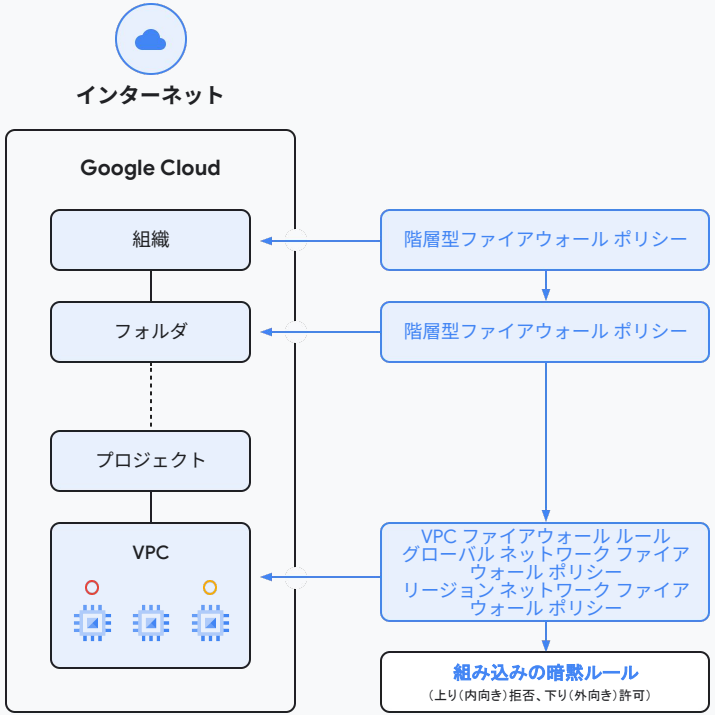
Cloud NGFW は、ニーズに合わせてスケーリングしやすく、トラフィックや需要が増加しても高いパフォーマンスと可用性を確保できます。Enterprise ティアには、Palo Alto Networks とのパートナーシップにより開発された業界トップクラスの脅威検出機能が含まれており、さらなる保護を提供できます。

Cloud NGFW を使用すると、セキュリティ ポスチャーを完全に可視化できます。ファイアウォール違反が検出された場合、ユーザー フレンドリーなインターフェース、API、Cloud Logging、Google Security Operations など複数のチャネルを通じて通知を受け取ることができます。サードパーティの SIEM/SOAR ツールをご利用いただくことも可能です。

次世代ファイアウォールの詳細 →

Cloud NGFW


ルーター
Google Cloud
Threat Intelligence
導入
WL*
WL
WL
WL
WL
* WL = ワークロード


インターネット
Google Cloud
組織
フォルダ
プロジェクト
VPC
階層型ファイアウォール ポリシー
階層型ファイアウォール ポリシー
VPC ファイアウォール ルール
グローバル ネットワーク ファイア
ウォール ポリシー
リージョン ネットワーク ファイア
ウォール ポリシー
組み込みの暗黙ルール
（上り（内向き）拒否、下り（外向き）許可）

Cloud Armor

ウェブ アプリケーションをサイバー脅威から保護

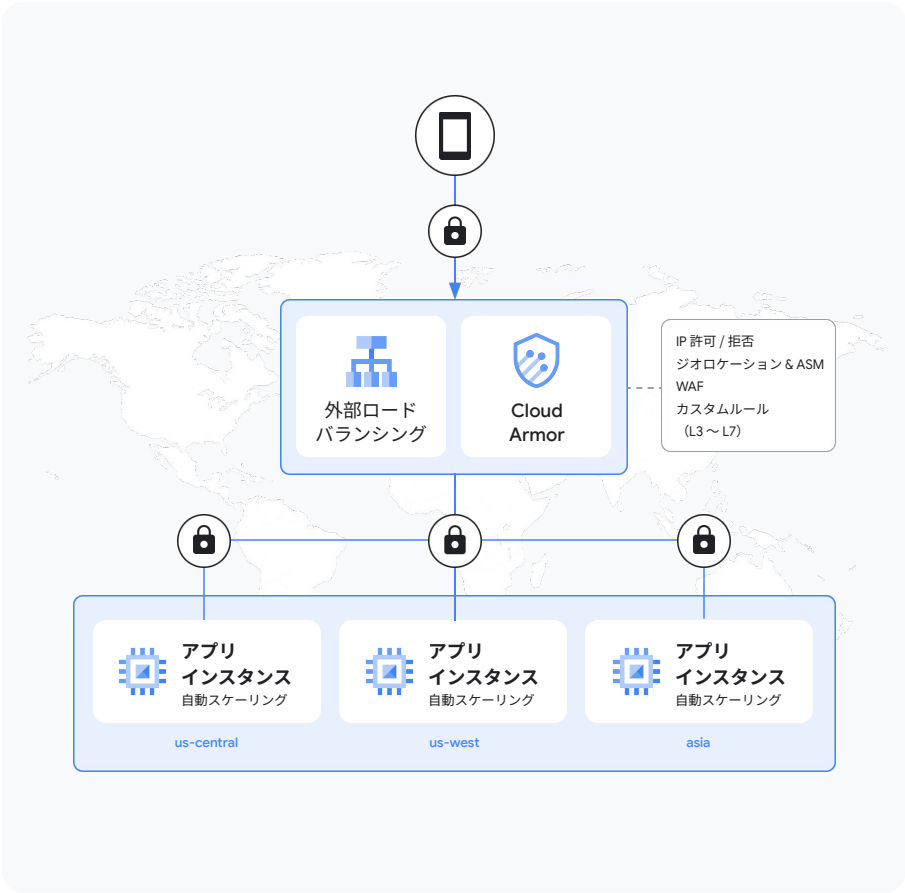
Cloud Armor は、ウェブ アプリケーションやサービスを標的としたさまざまな脅威に対抗する強力な多層防御を提供します。

この堅牢なソリューションは、システムダウンを狙った大規模な分散型サービス拒否（DDoS）攻撃を阻止するだけでなく、機密データを侵害する可能性のあるクロスサイト スクリプティング（XSS）や SQL インジェクション（SQLi）などの悪質な脅威からもアプリケーションやサービスを守ります。

Google Cloud Load Balancer とシームレスに統合された Cloud Armor が脅威を探して軽減し、トラフィックを包括的に制御できるようにします。地理的位置、既知の脅威インテリジェンス、特定の IP アドレスなどのさまざまな要素に基づいて保護ルールを定義できます。

さらに、Cloud Armor には静的なルールだけでなく、適応型保護もあります。これは ML を使用してトラフィック パターンを分析して異常を検出する機能で、新たな攻撃ベクトルに対抗するためのウェブ アプリケーション ファイアウォール（WAF）ルールを提案することもできます。

Cloud Armor の詳細 →



「Cloud Armor のおかげで、Symantec のネットワーク セキュリティ インフラストラクチャのセキュリティ ポスチャーが強化され、最先端のエンタープライズ向けソリューションをお客様に提供できるようになりました。運用オーバーヘッドの削減というおまけまで付いてきて、Broadcom 社内のリソースが解放されたので、サイバーセキュリティ分野の大きな課題の解決に向けて最先端のソフトウェア ソリューションの開発に専念できるようになりました。」

Ben-Haroche 氏

Broadcom、プラットフォーム グループ マネージャー



BROADCOM

出典: https://cloud.google.com/blog/ja/products/identity-security/how-google-cloud-armor-helps-broadcom-block-ddos-attacks?e=48754805

データ保護



セクション 04

Sensitive Data Protection

貴重な情報を安全に保護

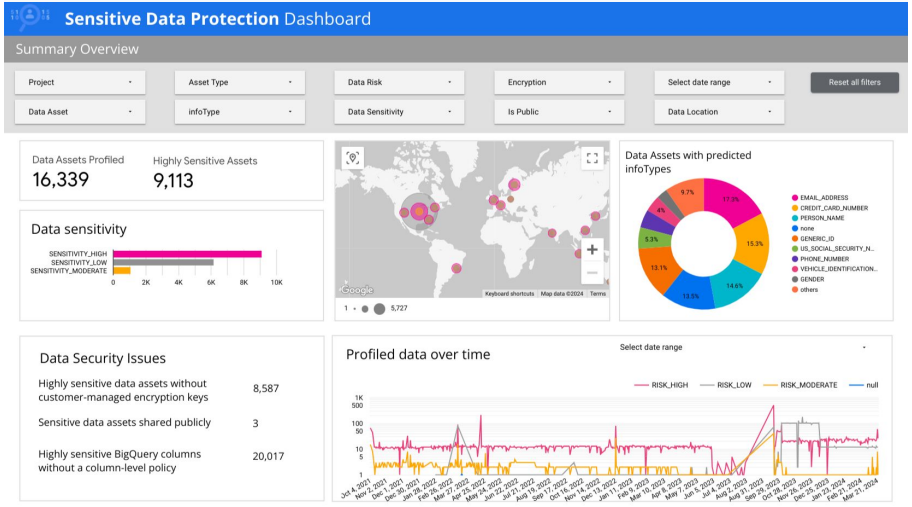
Google Cloud の Sensitive Data Protection は、機密データを発見するだけでなく、脅威から積極的に保護し、BigQuery 環境内のリスクを軽減してコンプライアンスを維持するのに役立つツールの総合的なスイートを提供します。

まず、継続的な検出を有効にして、データをスキャンして分類し、その構成を把握して関連リスクを特定します。次に、この情報を保護するための予防措置を講じます。難読化と匿名化によりセンシティブな要素をマスクし、削除、マスキング、トークン化、変換によって、構造化データと画像を含む非構造化データの両方にセキュリティ レイヤを追加します。

150 を超える事前定義済みの検出項目のライブラリと、カスタム検出項目の作成オプションを組み合わせることで、特定のビジネス要件にも Sensitive Data Protection で対応できます。データの固有の性質や潜在的な脅威にも対処できる柔軟性を備えています。

さらに詳細な分析情報を提供するために、Sensitive Data Protection の検出結果を Security Command Center（SCC）と統合できます。これらの検出結果と仮想レッドチーム テクノロジーにより、潜在的な攻撃パターンを分析し、標的となる可能性のあるデータの種類に関する貴重なコンテキストを得ることができます。

Sensitive Data Protection の詳細 →



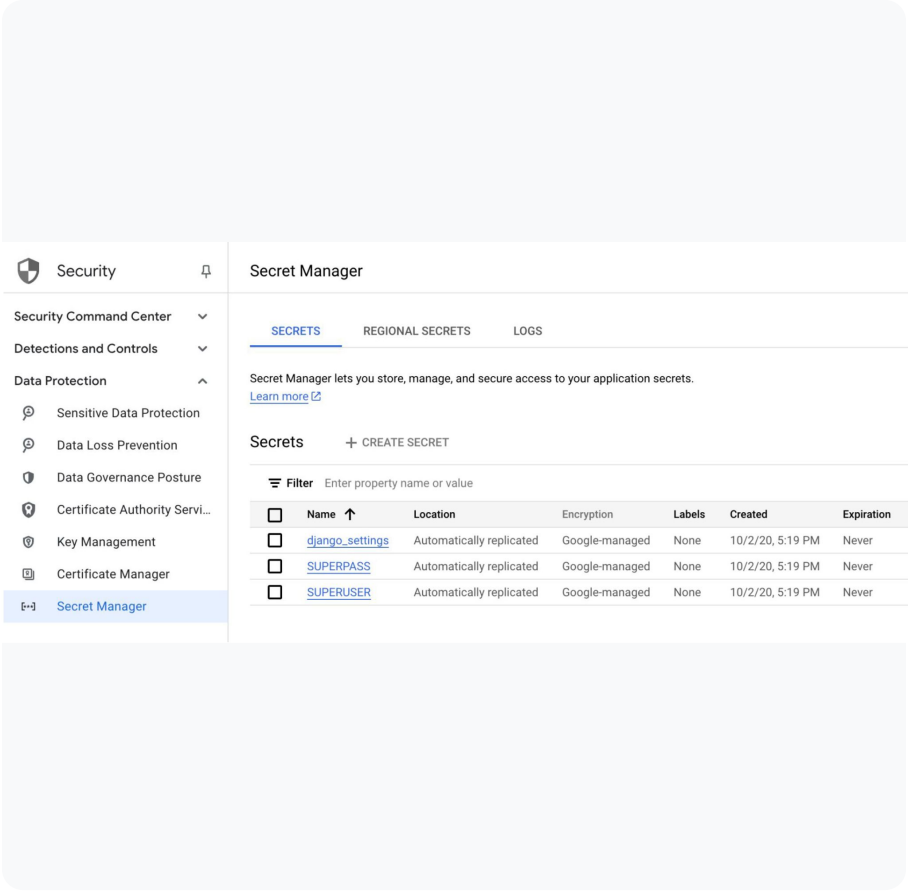
Secret Manager

シークレットを保護

クラウド コンピューティングの世界では、機密データのセキュリティを確保することが最重要事項です。Google Cloud の Secret Manager は、API キー、パスワード、証明書、その他の認証情報などの機密データを保護するための堅牢なソリューションを提供します。

Secret Manager は安全なストレージを提供するだけでなく、厳格なアクセス制御ポリシーを適用し、承認されたユーザーとサービスのみが、機密データを格納するリソース（シークレット）にアクセスできるようにします。自動バージョン管理と包括的な監査ロギングによりシークレットを管理することで、セキュリティとコンプライアンスがさらに強化されます。

BigQuery とのシームレスな統合によりワークフローを合理化してワンクリックでユーザーをデータにアクセスさせることもできます。機密性の高いパスワードが公開されないため、意図しないデータ漏洩や不正使用のリスクを最小限に抑えることができます。



Secret Manager の詳細

Cloud KMS と HSM

Google Cloud で データ暗号化を管理

Google Cloud はデータ セキュリティを最優先事項としています。BigQuery では、保存データはデフォルトで暗号化されますが、暗号鍵をより高度なセキュリティ レベルで管理したい場合は、Cloud KMS と HSM で柔軟に対応できます。

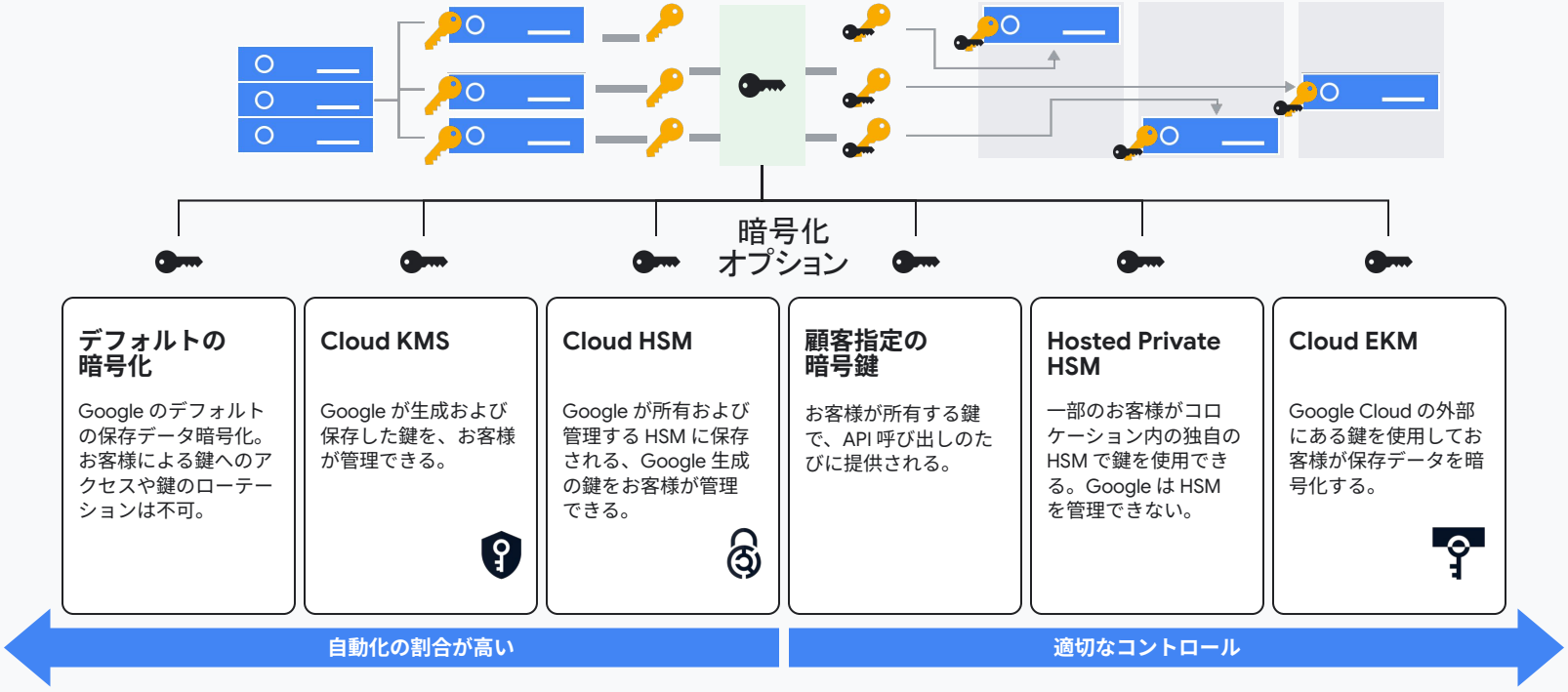
BigQuery の顧客管理の暗号鍵（CMEK）を使用すると、Google Cloud ではなく、お客様がデータを保護する暗号鍵の所有者になることができます。つまり、Cloud KMS 内で鍵の作成、ローテーション、追跡、削除を制御できるため、暗号化の実装方法をお客様の組織のセキュリティ要件やコンプライアンス要件に完全に合わせることができます。

Cloud KMS は鍵管理を簡素化し、Cloud HSM は FIPS 140-2 レベル 3 認定のハードウェア上で鍵を管理してセキュリティを強化します。使い慣れた Cloud KMS API フロントエンドにより、HSM を既存のワークフローに簡単に統合できます。

鍵管理の詳細 →



Cloud KMS と HSM



「Google Cloud Sensitive Data Protection（SDP）を導入したことで、BigQuery データ全体をスキャンして、ビジネス固有のルールやエッジケースを適用し、データ プロファイリングのパフォーマンスをチューニングできるようになりました。 これにより、データ ウェアハウス内だけでなく、ビジネス全体における個人情報（PII）のデジタル フットプリントをより詳細に把握できるようになりました。」

Anthony Tsoi 氏

Charlotte Tilbury Beauty、DataOps リード エンジニア



CharlotteTilbury

出典: https://cloud.google.com/blog/ja/topics/customers/how-charlotte-tilbury-beauty-responds-to-customer-data-requests?e=48754805

モニタリングとコンプライアンス



セクション 05

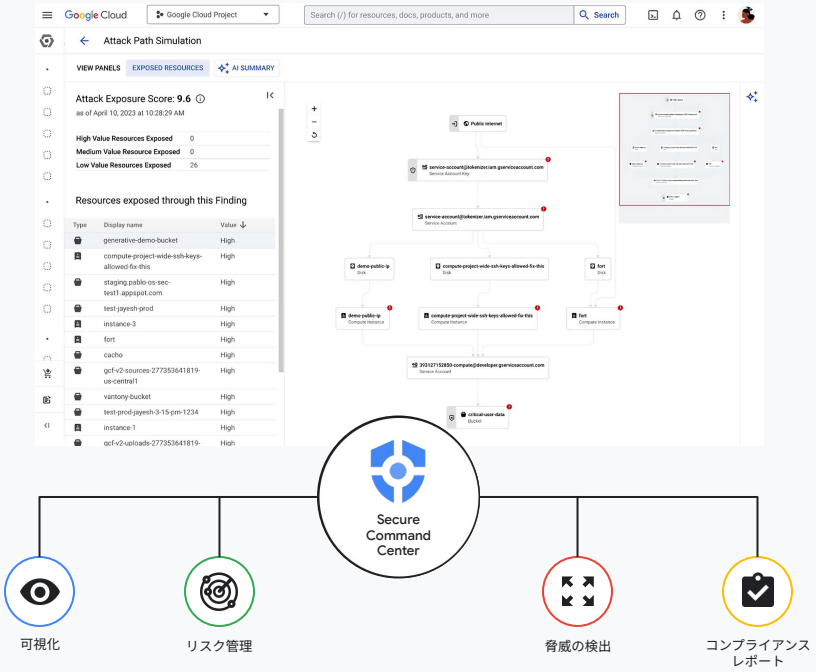
Security Command Center

Security Command Center は、セキュリティ ポスチャーの強化、クラウド リスクの積極的な管理を支援し、貴重なアセットである組織データが常に保護され、コンプライアンスに準拠していることをモニタリングします。

BigQuery とのシームレスな統合により、Security Command Center はデータセットを直接可視化し、データ ウェアハウス内の潜在的な脆弱性や構成ミスを発見して対処できるようにします。

Security Command Center が BigQuery を監視することで、損害が出る前に不正アクセスやデータの引き出しを未遂に防ぐことができます。

コンプライアンス レポートの自動化により、データ責任者はデータ保護規制の遵守を容易に維持できます。Gemini AI を活用した先を見越した提案と組み合わせることで、BigQuery のセキュリティ戦略を継続的に改良し、絶えず変化する脅威の動向に合わせて進化させることができます。



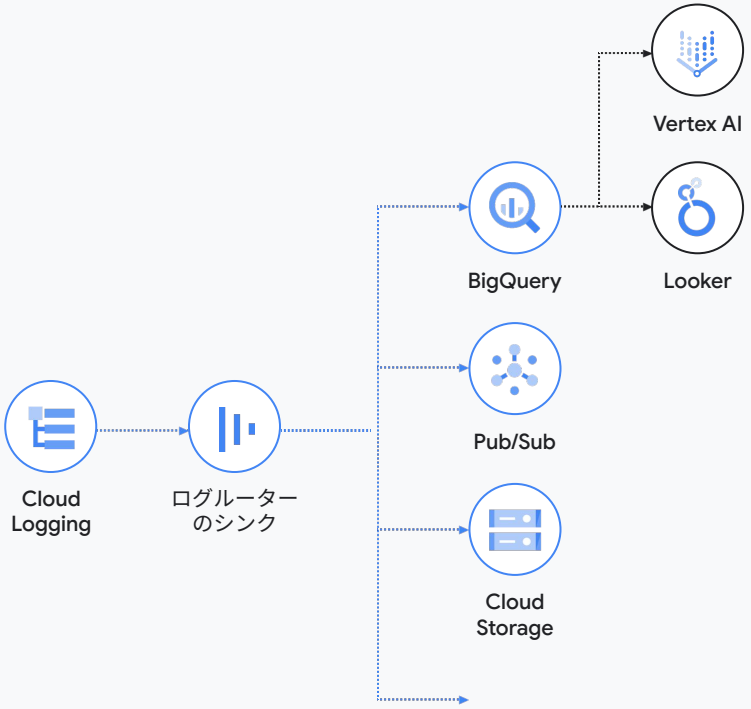
Security Command Center の詳細

Cloud Logging

Google Cloud Logging は、包括的なログ収集、保存、分析機能を提供し、データ セキュリティ ポスチャーを強化します。

BigQuery、App Engine、Cloud Run、GKE、Compute Engine VM などの重要な Google Cloud サービス全体でロギングを行うことで、システム アクティビティとデータアクセス パターンを完全に可視化できます。リアルタイムの分析情報により、異常の検出、潜在的な脅威の調査、セキュリティ インシデントへの迅速な対応が可能になります。

Cloud Logging のストレージ オプションは、デフォルトの保持期間から長期のアーカイブまで柔軟に対応でき、コンプライアンス監査やフォレンジック調査が必要な場合は過去のログデータにアクセスできます。さらに、ログは BigQuery にエクスポートできるため、詳細な分析や他のデータソースとの相関関係の把握が可能になり、隠れたパターンや潜在的な脆弱性を発見できます。



Google Cloud Logging の詳細

Assured Workloads

クラウドのコンプライアンスとセキュリティを簡素化

クラウドで機密データとワークロードを管理することは複雑な作業で、特にコンプライアンスとセキュリティ要件の両立が求められる場合は一筋縄ではいかないものです。Assured Workloads は、必要な制御を合理化するソリューションを提供します。

Assured Workloads を使用すると、組織の特定のニーズに合わせて機密性の高いリソースを確実に保護して構成できます。経験や勘を頼りにクラウド セキュリティを構成する必要はありません。データのロケーション、アクセス制御、暗号化レベルなど、必要なセキュリティ設定を選択するだけで、Google Cloud が必要な制御を実装します。

このアプローチにより、重要な資産を保護しながら規制遵守を維持できます。Assured Workloads によって複雑な作業から解放されることで、安心してクラウドの可能性を最大限に活用することに集中できます。

Assured Workloads の詳細 →

コンプライアンス

- データのロケーション
- 担当者のアクセス
- 継承された統制

Assured Workloads

1. 規制対象のアクセスのニーズを選択
2. 保存データのロケーションを設定
3. 鍵管理を構成
4. 規制対象の境界を作成

信頼性の高いコンプライアンス

再現可能なデプロイ
機密性の高いワークロードを保護しながら、コンプライアンスのニーズに合わせて構成できます。

コンプライアンスをシンプルに

再現可能な適用
選択した任意のリージョンに、リソース、要員、データ ロケーションの制限を適用できます。

「Google Cloud Assured Workloads を使用してデプロイすることを選んだのは、必要なセキュリティ管理が提供され、幅広いコンプライアンス要件への対応に役立つからです。世界中の要件を満たすことができれば、複数の国の入り組んだコンプライアンス プロセスのオーバーヘッドと複雑さを軽減しながら、自らのビジネスを成長させることができます。」

David Williams 氏

Iron Mountain、クラウド マネージャー



IRON MOUNTAIN®

出典: https://cloud.google.com/blog/ja/products/identity-security/how-iron-mountain-uses-assured-workloads-to-serve-customer-compliance-needs

Google Cloud

詳細やトライアルは こちらから:

BigQuery & クラウド セキュリティ

