Google Cloud

総務省　電気通信事業部　御中

電気通信事業者でのクラウドの利用に関する意見交換資料

2026/04/30

渕野 大輔

グーグル・クラウド・ジャパン合同会社

執行役員 カスタマーエンジニアリング 統括技術本部長

総務省殿からのご質問

1. 電気通信事業者への提供状況、今後の方針

- 電気通信事業者に対する自社サービスの提供状況如何。
- 電気通信事業者へのサービス提供を今後積極的に進めていきたいなど社としての方向性はあるか。
- 電気通信事業者へサービス提供するにあたって、電気通信事業法上の技術基準への適合性担保に当たり、電気通信事業者に対してどのような協力を行っているか、また、それらの取組状況を整理したうえで電気通信事業者に提供することは可能か。例えば、予備機器等（事業用 電気通信設備規則第4条）や電源設備（同規則第 10 条）、停電対策（同規則第 11 条）については、電気通信事業者に対してどのような協力を行っているか。（我が国において電気通信事業者にサービスを提供していない場合には、諸外国における取組事例を御回答いただけますと幸いです（以下同じ。）。）
- 電気通信事業者に提供するサービスの品質保証及び情報保全（セキュリティ）について、技術面及び契約上それぞれにおいてどのように担保しているか。

総務省殿からのご質問

1. 電気通信事業者への提供状況、今後の方針

- **電気通信事業者に対する自社サービスの提供状況如何。**
- **電気通信事業者へのサービス提供を今後積極的に進めていきたいなど社としての方向性はあるか。**
- 電気通信事業者へサービス提供するにあたって、電気通信事業法上の技術基準への適合性担保に当たり、電気通信事業者に対してどのような協力を行っているか、また、それらの取組状況を整理したうえで電気通信事業者に提供することは可能か。例えば、予備機器等（事業用 電気通信設備規則第4条）や電源設備（同規則第 10 条）、停電対策（同規則第 11 条）については、電気通信事業者に対してどのような協力を行っているか。（我が国において電気通信事業者にサービスを提供していない場合には、諸外国における取組事例を御回答いただけますと幸いです（以下同じ。）。）
- 電気通信事業者に提供するサービスの品質保証及び情報保全（セキュリティ）について、技術面及び契約上それぞれにおいてどのように担保しているか。

電気通信事業者に対する自社サービスの提供状況

- 従来の「ベンダー・キャリア関係」から「クラウドネイティブ化の共創パートナー」への進化

【2. 現在の通信事業者との関係性（ 3つの柱）】

過去: Dedicated Device

Nokia/Ericsson等のNEPによる専用機器に垂直統合されたモデル。

課題
ハードウェア依存、高コスト、柔軟性の欠如。

過渡期: Virtualization/VNF

VMwareやOpenStack上での仮想化。

課題
まだオーバーヘッドが大きく、完全なクラウドのメリットを享受できていない。

現在: Cloud Native/CNF

Google Cloudの役割: GKE（Google Kubernetes Engine）ベースの共通基盤を提供。

NEPのアプリケーションもGoogle Cloud上で稼働する「Managed Hosted」へと進化し、SaaSモデルへシフト。

Google Cloud は通信事業者が目指す「コア機能のクラウドネイティブ化」と「周辺アプリのモダナイズ」を支える共通基盤として機能し、エコシステム全体で通信インフラの高度化（低遅延、高信頼性、コスト最適化）を支援しています。

電気通信事業者に対する自社サービスの提供状況

- 従来の「ベンダー・キャリア関係」から「クラウドネイティブ化の共創パートナー」への進化

【2. 現在の通信事業者との関係性（ 3つの柱）】

CNaaSの実現

KDDI 等の通信事業者がオーケストレーターとなり、Google Cloud の基盤上でコア機能をマネージドサービスとして利用する形態へ進化。

従来はNEPから「機器を買う」モデルだったが、現在はアプリのライセンス料込でクラウド上で「機能を利用する」モデルへ。

NEPとの協調 エコシステムの創造

Ericsson や Nokia といった Tier1 ベンダーと競合するのではなく、彼らの5Gアプリケーション（5G Core, IMS等）を動かすための最適化されたプラットフォームを提供

通信事業者は、使い慣れたNEPの機能を、Google Cloud の拡張性・信頼性の上で利用可能。

AI による新たな価値創造

AI に対する期待値が一変

通信事業者は、単なる接続だけではなく、ネットワーク運用（AIOps）や顧客体験向上、収益化のためにGoogle のAIの機能を不可欠な要素として組み込んでいる。

電気通信事業者に対する自社サービスの提供状況

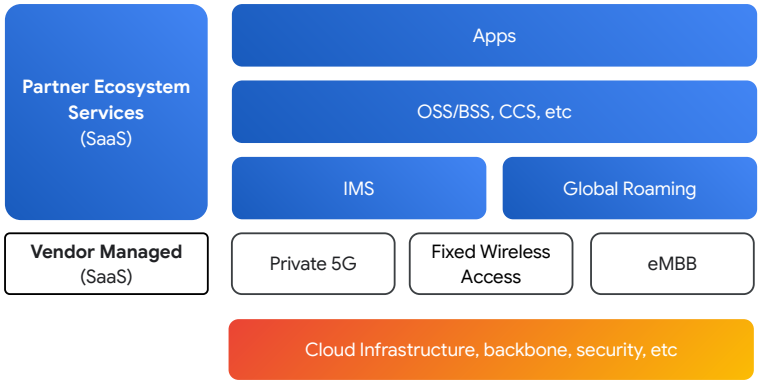
- 従来の「ベンダー・キャリア関係」から「クラウドネイティブ化の共創パートナー」への進化

Managed Hosted

ハイブリッド スタック - 5G コントロール プレーンとクラウド内のアプリ

Core Network as a Service

ベンダー管理の5GパケットコアはクラウドからSaaSとして提供される



Ex. Nokia PCF deployment for TEF Germany

Tier1/Tier2 事業者を対象とした DRサイト・バーストユースケース

NOKIA

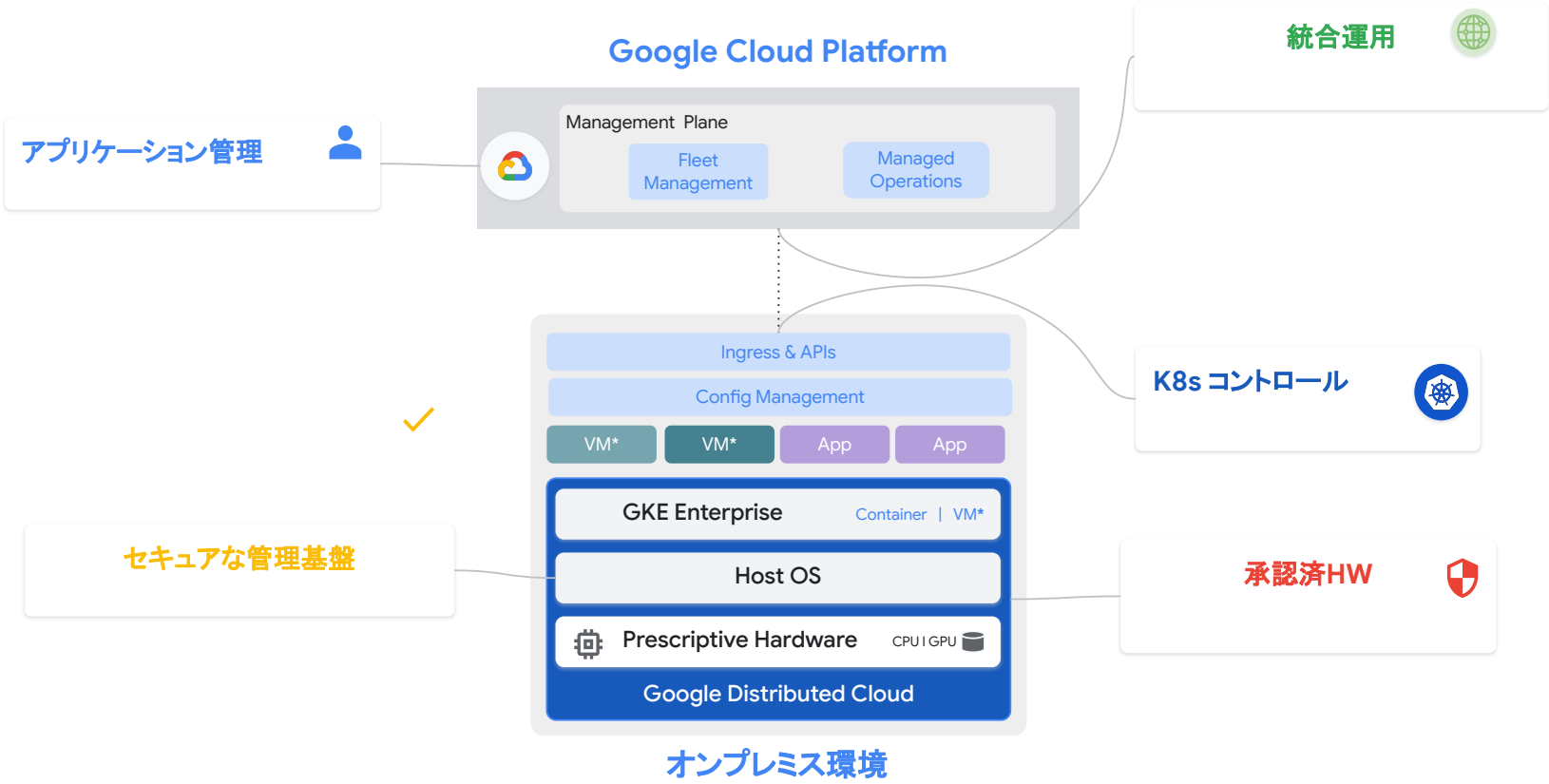
Ex. Ericsson on-demand SaaS service in GCP

Tier 3/Tier 4 事業者を対象としたフルスタック製品

ERICSSON

- Google CloudとNokiaは、通信サービスプロバイダと企業顧客向けにクラウドネイティブ5Gコアソリューションを共同開発しています。 Google Cloud

ハイブリッド運用の方向性



Google Distributed Cloud - Connected Server

フルマネージドなローカルK8Sクラスタ

- **高可用性:** 堅牢な設計、2+1冗長構成、インターネット接続障害への高い耐性を実現
- **マネージド:** プラットフォームを通じたハードウェアの統合管理
- **省スペース:** 合計3RU、ハーフデプス（奥行き1/2）のコンパクト設計
- **スケーラブル:** ポリシーとアプリケーション構成を数万拠点に展開可能
- **拡張性:** VM、コンテナ、GPUを活用したAIアプリケーションに対応
- **柔軟性:** 複数のサイズ（96vCPUsから192vCPUs）を提供し、サーバーやコアの追加で段階的に拡張（Pay-as-you-grow）

Customer-managed ToR

GDC connected (Server)

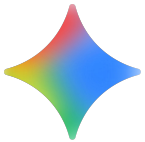
3-node Blade cluster

- Medium 32 vCPUs/64 GB/1.6 TB
- Large 64 vCPUs/128 GB/3.2 TB
- 3U total, full width, half depth

総務省殿からのご質問

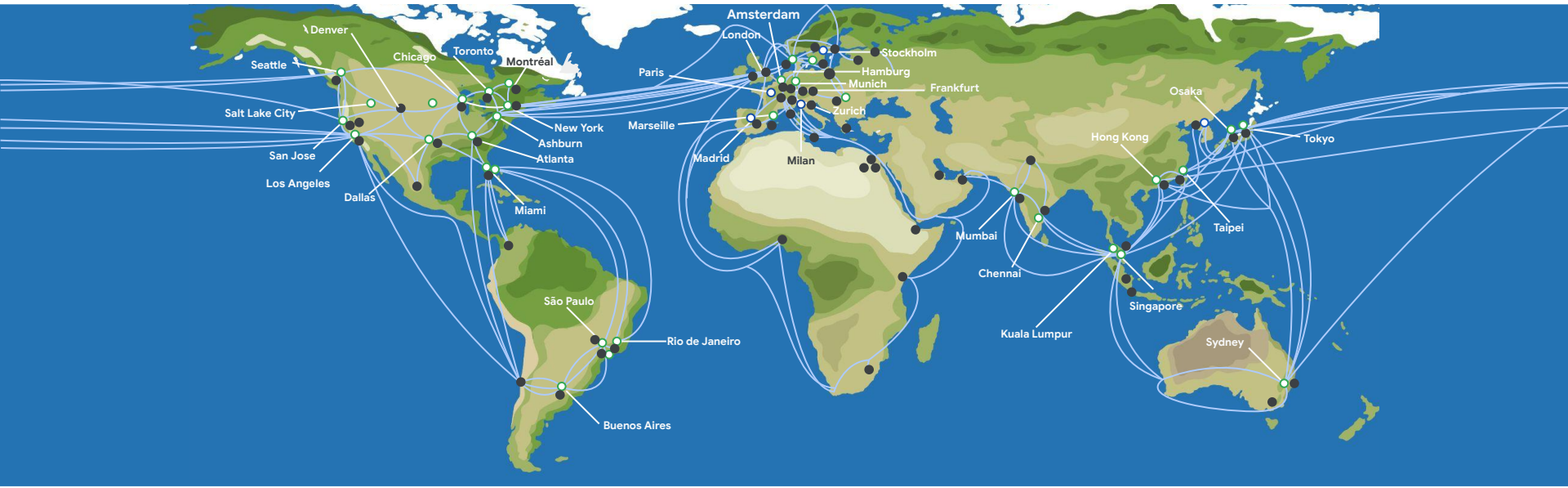
1. 電気通信事業者への提供状況、今後の方針

- 電気通信事業者に対する自社サービスの提供状況如何。
- 電気通信事業者へのサービス提供を今後積極的に進めていきたいなど社としての方向性はあるか。
- **電気通信事業者へサービス提供するにあたって、電気通信事業法上の技術基準への適合性担保に当たり、電気通信事業者に対してどのような協力を行っているか、また、それらの取組状況を整理したうえで電気通信事業者に提供することは可能か。例えば、予備機器等（事業用電気通信設備規則第4条）や電源設備（同規則第10条）、停電対策（同規則第11条）については、電気通信事業者に対してどのような協力を行っているか。（我が国において電気通信事業者にサービスを提供していない場合には、諸外国における取組事例を御回答いただけますと幸いです（以下同じ。）。）**
- **電気通信事業者に提供するサービスの品質保証及び情報保全（セキュリティ）について、技術面及び契約上それぞれにおいてどのように担保しているか。**



Google Cloudは、電気通信事業者向けの技術基準への適合支援、ならびにサービスの品質保証および情報保全について、責任共有モデルに基づく強力なクラウドインフラを提供しています。これらの要件は、利用規約（ ToS）、サービスレベル契約（ SLA）、およびCloud のデータ処理に関する追加条項（ CDPA）などの契約上のコミットメントによって明確に担保されています。

Googleインフラのレジリエンスと拡張性



43 regions live (many more announced)

130 availability zones

36 subsea cable investments announced

200+ countries and territories served

Googleインフラのレジリエンスと拡張性

データセンターの堅牢性

- **継続稼働：**冗長化された電源、フル稼働可能な予備発電、最適な冷却システムにより24時間365日の稼働を維持。
- **ハードウェア保護：**高度な火災・熱・煙検知システムと集中警報による徹底した保護体制。

システムアーキテクチャと信頼性

- **冗長性と複製:** データとサービスを各種コンポーネントや施設間で分散配置し、単一障害点を排除。
- **自動フェイルオーバー:** 障害を即座に検知し、ワークロードを正常なインフラへシームレスに移行。
- **障害の分離:** インフラを独立した「ゾーン」に分割し、システム全体への障害波及を防止。

Google Cloud サービスは、SLAで定義された高い可用性を維持しています$LA で定義されたサービス稼働率 GCP、Workspace)

「責任共有モデル」

利用サービスにより責任範囲は変わりますが、**お客様は常にデータの安全性を自らコントロールし、**Googleは常にインフラの安全を保障します。

責任の範囲を超えて、Googleはリスク管理において**「Shared Fate（運命の共有）」モデル**を採用しています。お客様が安全にデプロイし、運用できるよう、プロダクト、ベストプラクティス、パートナーへのアクセスを提供し、積極的に連携します。

サービスの品質保証（ SLA）に関する契約上の担保

品質保証については、サービスレベル合意書（　SLA）が契約の核となります。

- **可用性のコミットメント ：**
  - 個々のサービス（Compute Engine, Cloud Storage等）ごとに、月間稼働率（例：99.9% ～ 99.99%以上）を明文化しています。これを下回った場合、利用料金の一部を返金（補填）する「サービスクレジット」の仕組みが契約に組み込まれています。
- **透明性の確保：**
  - Google Cloud Service Health などを通じ、稼働状況をリアルタイムで公開することを約束しており、不透明なダウンタイムを排除しています。
- **保守・運用の免責事項の明確化 ：**
  - 計画メンテナンスの通知義務や、障害発生時のサポート窓口（技術サポート契約）の提供を契約で定めています。

情報保全（セキュリティ）の技術面の担保

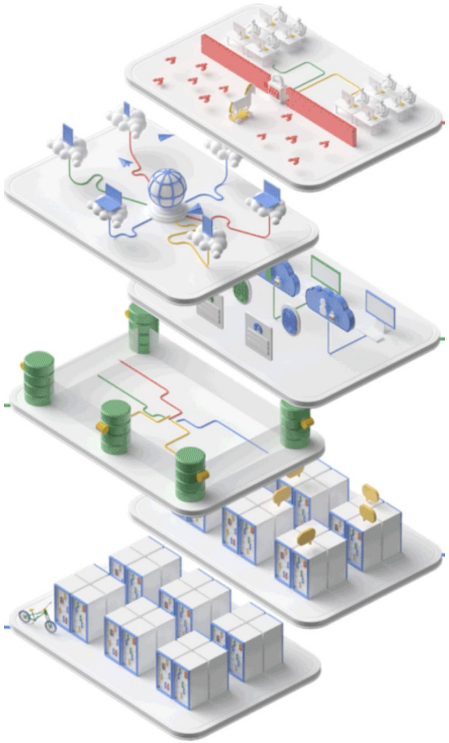
Defence in depth & at scale（大規模な多層防御）

Google Cloud プラットフォームのセキュリティ設計思想

インターネット通信
デフォルトでの通信の暗号化

ストレージサービス
デフォルトの保存データの暗号化

ハードウェア インフラストラクチャ
カスタマイズされたハードウェア、Titan



運用上およびデバイスのセキュリティ
ゼロ トラスト – BeyondCorp
リスクとコンテキストに基づくアクセス制御

ID
強固な認証

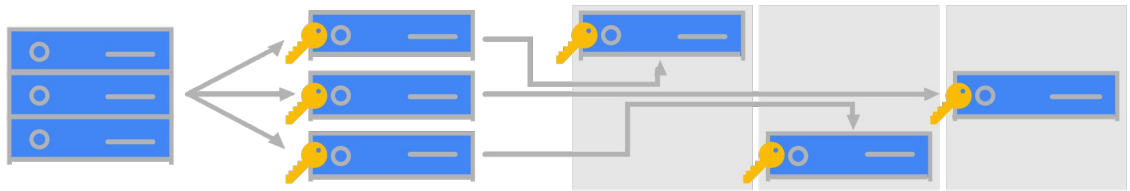
サービスのデプロイ
ゼロ トラスト – BeyondProd

詳細は Google インフラストラクチャのセキュリティ設計の概要をご参照ください。

蓄積データの格納方法と暗号化 （デフォルトでの暗号化 ）

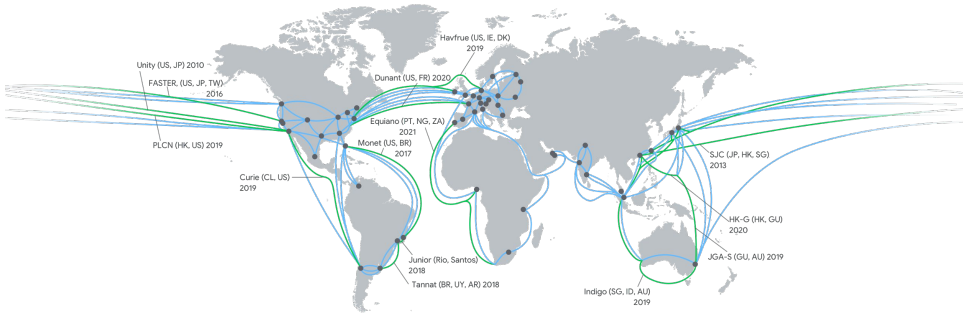
- 「Google Cloud セキュリティ ホワイトペーパー」に、お客さまが Google Cloudに格納されたデータのデフォルトでの保管方法を記載しております。
  - https://services.google.com/fh/files/misc/security_whitepapers_4_booklet_jp.pdf?hl=ja
  - https://cloud.google.com/security/encryption-at-rest/default-encryption?hl=ja

- データは保存にあたりサブファイル チャンクに分割されます。各チャンクは、個別の暗号鍵を使ってストレージ レベルで暗号化されます。2 つのチャンクの暗号鍵が同じになることはありません。たとえそれら 2 つのチャンクが、同じお客様が所有する同じ Google Cloud Storage オブジェクトに属していても、あるいは同じマシンに保存されていても、異なる暗号鍵が使われます 1。データのチャンクが更新されると、元の鍵を再利用せず、新しい鍵を使用してこのチャンクを暗号化します。このように分割されたデータのそれぞれが異なる鍵を使用するため、データ暗号鍵が漏えいしたとしても、被害範囲はそのデータチャンクだけにとどまります。
- 各チャンクは複数の Google のストレージ システムに分散され、バックアップと障害復旧のために暗号化形式で複製されます。悪意のあるユーザーが顧客データに仮にアクセスしようとする場合、(1)目的のデータに該当するすべてのストレージ チャンクと、(2)それらのチャンクに対応する暗号鍵をすべて把握し、さらにそれらのアクセス権を得る必要があります。



転送データの暗号化

- Google のネットワーク インフラストラクチャ
  - https://cloud.google.com/security/encryption-in-transit?hl=ja#physical_boundaries_of_googles_network
- Google は、Google または Google 代行者が管理している物理境界内から外側へとデータが転送されるとき、転送されるデータにさまざまな保護を適用しています。
  - 物理境界 (Google または Google 代行者が管理している物理空間) 内では Google が厳格な保護対策を実施できます。これらの場所への立ち入りは制限され、厳重に監視されています。物理境界の内側でやり取りされるデータは、通例、認証されていますが、デフォルトでは必ずしも暗号化されません。
  - 一方、グローバルなインターネットでは、規模の関係上、物理境界内と同じ物理セキュリティ統制を導入することは不可能です。このため、物理的な信頼境界の外側では、追加的な保護対策を自動的に適用します。
    これらの保護対策の一貫として、転送されるデータの暗号化を行います。



蓄積データの格納方法と暗号化（お客様管理の暗号鍵）

- **Customer Supplied Encryption Keys (Googleに鍵を保存しない方法（1))**

  お客様指定の暗号鍵を使うことが可能です。お客様指定の暗号鍵を指定した場合、その鍵を **Google のサーバーに永続的に保存することはなく、またユーザーの鍵を管理することもありません。代わりに、 Cloud Storage の各オペレーションについてお客様が独自の鍵を指定し、そのオペレーションが完了した後で鍵は Google のサーバーから削除されます。** Cloud Storage は、鍵の暗号学的ハッシュ関数のみを保存し、今後発生するリクエストをそのハッシュ関数に対して検証できるようにします。このハッシュ関数から鍵を復元することはできません。このハッシュ関数でデータを復号することもできません。

- **Cloud EKM (External Key Manager) (Googleに鍵を保存しない方法（2))**

  Cloud EKM では、**外部鍵管理パートナー** 内で管理する鍵を使用して、Google Cloud 内のデータを保護できます。BigQuery または Compute Engine の永続ストレージ内に保存するか、Cloud Key Management Service API を直接呼び出して、データを保護できます。外部で管理する鍵は、Google Cloud にキャッシュされることや、保存されることはありません。代わりに、 Cloud EKM はリクエストごとに外部の鍵管理パートナーと直接通信します。

AI による脅威検知の担保

Googleのグローバルな脅威インテリジェンスと LLM / Agent を活用し、24時間365日の高度なセキュリティ監視を実現しています。
具体的には、Agent がシステムログの相関分析をリアルタイムで行い、従来の技術では困難だった未知の攻撃や複雑な振る舞いの異常（アノマリ）を即座に特定します。これにより、大規模な通信インフラにおけるサイバー攻撃の早期検知と、インシデント対応の迅速化・自動化を両立しています。

例：セキュリティ運用の効率化と迅速なレスポンス

AI（生成AIを含む）を活用し、検知した後の初動を早めます。

- 複雑なセキュリティアラートを AIが自然言語で要約し、管理者に推奨される対策を提示します。
  これにより、電気通信事業者のような大規模インフラにおいて、インシデント発生から封じ込めまでの時間を大幅に短縮（MTTRの削減）します。

情報保全（セキュリティ）の契約上の担保

情報保全（セキュリティ）に関する契約上の担保

セキュリティ面では、Googleが預かるデータの「取り扱いルール」を法的に定義しています。

データ処理の法的合意（CDPA）

Google Cloud の契約には、**Cloud Data Processing Addendum (CDPA)** というデータ処理補足条項が含まれます。ここでは以下が保証されます。

- **データの所有権：**「お客様のデータはお客様のものであり、Googleが広告のためにスキャンしたり、二次利用したりすることはない」ことを明記しています。
- **利用目的の制限：**Googleは、サービスの提供および契約上の義務を果たすためにのみデータを使用し、それ以外の目的での利用を禁止しています。

第三者認証の継承

契約上、Googleが独立した第三者監査機関による評価を継続的に受けていることを保証しています。 （次ページ参照）

- **主要な認証：**ISO/IEC 27001（情報セキュリティ管理）、27017（クラウドセキュリティ）、27018（個人情報保護）や、SOC 2/3 レポートの提 供。
- **政府・業界基準への準拠 ：**日本のISMAP（政府情報システムのためのセキュリティ評価制度）への登録状況を、契約上の信頼の根拠として提示できます。

第三者認証の取得（ISO, SOC, PCI DSS等）

- お客様の信頼を得るために、独立した機関によるセキュリティ、プライバシー、コンプライアンス統制の監査を定期的に実施し、世界的な基準の各種認証を取得しています。
  以下は、取得済みの認証の例 (一部) です。
  - ISO/IEC 27001
  - ISO/IEC 27017
  - ISO/IEC 20718
  - ISO/IEC 27701
  - SOC1, SOC2, SOC3
  - PCI DSS, PCI 3DS
  - HIPAA
  - FedRAMP
  - Cloud Security Alliance (CSA) STAR
  - EU モデル契約条項
  - FIPS 140-2
  - NIST 800-53
  - NIST 800-34 - Contingency Planning
  - NIST 800-171
  - ISAE 3000 Type 2 Report
  - SEC Rule 17a-4(f)、CFTC Rule 1.31(c)-(d)、FINRA Rule 4511(c)
  - DoD Impact Level 2 provisional authority to operate
  - **ISMAP**

- FISC安全対策基準には認証取得という概念はありませんが、Google としての準拠状況についてのガイドをご提供しています。
  https://cloud.google.com/security/compliance/fisc?hl=ja

Google社員によるアクセスに対する統制

通信の秘密への配慮

- 障害対応等、お客様の要請に基づいてGoogleにて貴社データへのアクセスを行う場面で、Google社員の誰が、どのデータへのアクセスを、どのような理由で行ったのかを明示することができます。
  (アクセスの透明性ログ:
  <Google Cloud> https://cloud.google.com/logging/docs/audit/access-transparency-overview?hl=ja
  <Workspace> https://support.google.com/a/answer/9230979?hl=ja)

- Google社員のアクセス前に、お客様の承認を得るプロセスにも対応できます。
  (デバイスからのアクセスに対して管理者の承認を必須にする
  <Google Cloud> https://cloud.google.com/access-approval/docs/overview?hl=ja
  <Workspace> https://support.google.com/a/answer/7508418?hl=ja)

総務省殿からのご質問

2. 障害発生時の対応について

- 障害発生時において、電気通信事業者との責任分界は契約上どのようになるか。どこまでが自社の問題で、どこからが通信事業者の問題かを判断する手順などはあるか。
- 電気通信事業者に対して、①通信事故発生前及び②発生後それぞれについて、どのように情報提供しているか。具体的な情報提供範囲及び情報提供のスピード感について御教示願いたい。
- 障害の規模が電気通信事業法上の「重大事故」に該当する場合には、電気通信事業者は、電気通信事業法第 28 条第第1項第2号ハに基づき、総務大臣に対する報告を行わなければならないこととされている。その際、電気通信事業者は、事故発生時の原因、影響、復旧状況、再発防止策等の報告を求められることとなり、自らが利用する他者設備の提供事業者に対してこれらの情報提供を求めることが想定される。このような背景を踏まえ、電気通信事業者に対して、通常の利用者よりも詳細な情報提供をすることは可能か（契約上担保できるか）。また、そのような情報提供に際して、電気通信事業者には提供困難な情報であっても、国であれば情報提供しやすいといったように、情報提供先の違いに起因する対応の容易度の違いはあるか。

総務省殿からのご質問

2. 障害発生時の対応について

- **障害発生時において、電気通信事業者との責任分界は契約上どのようになるか。どこまでが自社の問題で、どこからが通信事業者の問題かを判断する手順などはあるか。**
- **電気通信事業者に対して、①通信事故発生前及び②発生後それぞれについて、どのように情報提供しているか。具体的な情報提供範囲及び情報提供のスピード感について御教示願いたい。**
- 障害の規模が電気通信事業法上の「重大事故」に該当する場合には、電気通信事業者は、電気通信事業法第 28 条第第1項第2号ハに基づき、総務大臣に対する報告を行わなけれ ばならないこととされている。その際、電気通信事業者は、事故発生時の原因、影響、復旧状 況、再発防止策等の報告を求められることとなり、自らが利用する他者設備の提供事業者に対してこれらの情報提供を求めることが想定される。このような背景を踏まえ、電気通信事業者 に対して、通常の利用者よりも詳細な情報提供をすることは可能か（契約上担保できるか）。また、そのような情報提供に際して、電気通信事業者には提供困難な情報であっても、国であ れば情報提供しやすいといったように、情報提供先の違いに起因する対応の容易度の違いはあるか。

ケースの初回応答時間目標時間（ SLO）

24 x 365
日本語対応

優先度	影響	説明	スタンダード	エンハンスト	プレミアム
P1	重大	**サービス停止または使用不可** ● サービスを利用できない ● エンドユーザー ベース全体がサービスを利用できない	（選択不可）	1 時間	15 分
P2	高	**サービスに重大な障害がある** ● サービスのパフォーマンスが低下している ● サービスは利用できるがエラー メッセージが表示される	4 時間	4 時間	2 時間
P3	中	**サービスが一部機能しない** ● エラー メッセージが表示される。エンドユーザーへの影響はない ● ユーザー向けリリースで使用されている機能に関する質問	8 時間	8 時間	4 時間
P4	低	**サービスは使用できる** ● 機能や開発に関する質問またはリクエスト ● ドキュメントまたはメッセージに修正が必要	8 時間	8 時間	8 時間

👉 言語サポートと業務時間（TAM サービスのご提供時間もこれに準じます）

24 時間 365 日対応

営業時間内（9 時 - 17 時 JST、土日祝を除く）

総務省殿からのご質問

2. 障害発生時の対応について

- 障害発生時において、電気通信事業者との責任分界は契約上どのようになるか。どこまでが自社の問題で、どこからが通信事業者の問題かを判断する手順などはあるか。
- 電気通信事業者に対して、①通信事故発生前及び②発生後それぞれについて、どのように情報提供しているか。具体的な情報提供範囲及び情報提供のスピード感について御教示願いたい。
- **障害の規模が電気通信事業法上の「重大事故」に該当する場合には、電気通信事業者は、電気通信事業法第 28 条第第1項第2号ハに基づき、総務大臣に対する報告を行わなけれ ばならないこととされている。その際、電気通信事業者は、事故発生時の原因、影響、復旧状況、再発防止策等の報告を求められることとなり、自らが利用する他者設備の提供事業者に 対してこれらの情報提供を求めることが想定される。このような背景を踏まえ、電気通信事業者 に対して、通常の利用者よりも詳細な情報提供をすることは可能か（契約上担保できるか）。また、そのような情報提供に際して、電気通信事業者には提供困難な情報であっても、国であれば情報提供しやすいといったように、情報提供先の違いに起因する対応の容易度の違いはあるか。**

各国政府機関からのデータ要請への対応

https://cloud.google.com/security/transparency/govt-requests?hl=ja
https://policies.google.com/terms/information-requests

米国法務省のポリシーでは、検察官は犯罪の疑いのある当事者（例: GCP利用企業の顧客）に令状を直接発行する必要があります。できない場合（例: GCP利用企業の顧客が米国にいない）、GCP利用企業に発行します。Google への要請は、そのようなGCP利用企業の顧客及びGCP利用企業の両方にアプローチできないという稀なケースのみ発生します。

Google が顧客アカウントに関するデータ要請を政府から受けた場合、各要請は以下のガイドラインに従って確認されます。

Google に保存されているユーザーデータのプライバシーとセキュリティの尊重

法的要請を受けた場合、Google のチームはその要請が法的要件と Google のポリシーを満たしているかどうかを確認します。一般的に、Google がデータを提示するには、要請が書面で作成されていること、要請機関の正式な担当者が署名していること、適正な法律に基づいて要請が出されていることが必要です。要請の対象範囲が過度に広いと判断した場合は、範囲を限定することを要求しています。Google にはこうした取り組みに特化した専門チームがあります。

お客様への通知

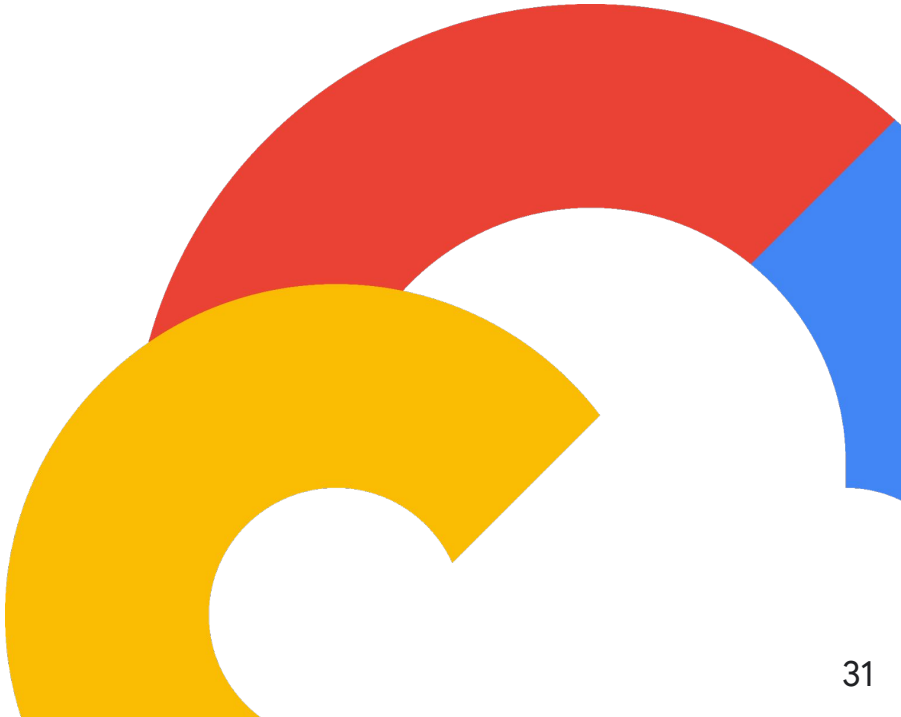
Google は、法律および要請の規約によって許される範囲で、情報を開示する前にお客様に通知することをポリシーとしています。ただし、このような通知が法令で禁止されている場合を除きます。Google は、法定または裁判所命令による開示禁止期間が終了したときなど、法的禁止が解除されてからユーザーに通知をお送りします。この通知は通常、Google Cloud のお客様の連絡窓口に届きます。

お客様からの異議の検討

Google は、法律および要請の規約によって許される範囲で、お客様が所轄裁判所に開示の異議を申し立てたり、その異議の写しを Google に提示したりするなどして要請と対立するお客様の妥当な要求に従います。米国政府の法的要請については、Google が法的要請をお客様に通知した後、お客様が裁判所に開示の異議申し立てを行い、その異議の写しを Google に提示すると、お客様の主張どおりに異議が解決した場合、Google は法的要請に応じてデータを提供することはしません。他の司法管轄区では手順が異なる場合があり、適宜処理されます。

政府機関からのエンタープライズデータ開示要請に関する透明性の提供に関する最新のレポートを発行いたしましたので、
あわせてご参照頂ければ幸いです。
https://cloud.google.com/blog/ja/products/identity-security/google-clouds-semi-annual-transparency-report-now-available
https://transparencyreport.google.com/user-data/overview?hl=jp

Thank you



Google Cloud