金融機関等コンピュータシステムの安全対策基準・解説書 第 14 版 (2026年3月版)

Google Cloud と Google Workspace 解説書

本解説書は、2026年3月に金融情報システムセンターより示された、「金融機関等コンピュータシステムの安全対策基準・解説書 第 14 版 (2026年3月版)」(以下、本ガイドライン)に基づく情報提供の一環として、Google Cloud及びGoogle Workspaceが講じている安全管理措置の概要を示すものです。
本解説書で説明されている Google における管理は第三者監査のコンプライアンス・プログラムである ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 42001で認定済みです。
本解説書ではお客様が Google Cloud及びGoogle Workspaceのサービスや対応する ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 42001 コンプライアンスの管理の内容を活用し、本ガイドラインの各項目にどのように対処すべきかコメントしています。

基準番号は本ガイドラインの採番方法に準拠しています。お客様の責任範囲で実施いただく項目は「-」となっています。

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
統1	-	-
統1-1	-	-
統1-2	お客様を支援するため、Googleはお客様にて実施するサードパーティーに対するサイバーセキュリティリスクを含むリスク管理について、以下の参考情報を提供しています。 参考情報: ITアウトソーシングに伴うサイバーセキュリティリスクの管理をお客様にて実施する際の参考情報として、弊社のホワイトペーパー「Risk Governance of Digital Transformation in the Cloud」は、クラウドへのトランスフォーメーションがリスク、コンプライアンス、監査機能にどのような意味を持つのか、また、クラウドの世界で成功するためにこれらのプログラムを最適に配置する方法を理解するのに役立ちます。 Googleの「Board of Directors Handbook for Cloud Risk Governance」は、ビジネスのより広範なデジタルトランスフォーメーションの一環として、クラウドテクノロジーの新規導入、あるいは大幅な導入拡大に取り組む組織の取締役会に、実践的なガイダンスを提供します。特に、クラウドテクノロジーを導入し、そのメリットを最大限に活用するためにビジネスプラクティス、プロセス、運用モデルを調整することで、組織がオペレーショナルリスク管理を段階的に変革する機会がどのように得られるかを解説します。	-
統2	-	-
統3	-	-
統4	お客様を支援するため、Googleは外部委託業務/クラウドサービスの利用におけるセキュリティ管理体制をお客様にて整備する際の参考として以下の情報を提供しています。 参考情報: Googleの「Board of Directors Handbook for Cloud Risk Governance」は、ビジネスのより広範なデジタルトランスフォーメーションの一環として、クラウドテクノロジーの新規導入、あるいは大幅な導入拡大に取り組む組織の取締役会に、実践的なガイダンスを提供します。特に、クラウドテクノロジーを導入し、そのメリットを最大限に活用するためにビジネスプラクティス、プロセス、運用モデルを調整することで、組織がオペレーショナルリスク管理を段階的に変革する機会がどのように得られるかを解説します。	-
統4-1	-	-
統4-2	-	-
統5-1	Google は、お客様にてGoogleのサービス上にあるお客様の資産を管理する際に役立つツールを提供しています。例えば、次のようなツールです。 Google Cloud: ・Cloud Asset Inventory を使用すると、プロジェクトやサービス全体にわたる Google Cloud および Anthos のすべてのアセットを表示、監視、分析できます。いつでもインベントリ全体のスナップショットをエクスポートできるだけでなく、アセット構成の変更に関するリアルタイム通知を受け取ることもできます。 ・Cloud Data Loss Prevention は、クラウド内外のデータを分類し、適切なガバナンス、制御、コンプライアンスを確保するために必要な分析情報を提供します。 ・Resource Manager を使用すると、Google Cloud コンテナ リソース（組織やプロジェクトなど）をプログラムで管理して、他の Google Cloud リソースをグループ化し、階層的に整理することができます。 ・Mandiant Attack Surface Managementを使用すると、現代の動的かつ分散型の共有環境全体でインターネット アセットを検出、分析しながら、外部のエコシステムを継続的にモニタリングし、悪用される恐れがある脆弱性を検知できます。 Workspace: ・Admin Consoleを使用すると、ユーザーの追加、デバイスの管理、セキュリティと設定の構成が可能です。 ・Security Centerは、高度なセキュリティ情報と分析を提供し、ドメインに影響を与えるセキュリティ問題の可視性と制御性を高めます。 ・Endpointを使用すると、組織内で使用されるデバイスを管理し、個人所有デバイスと会社所有デバイス上の業務コンテンツを安全に保つことができます。	-
統5-2	お客様を支援するため、Googleは脅威情報及び脆弱性情報をお客様にて収集する際の参考として以下の情報を提供しています。 Google は、セキュリティ状況の最新動向を組織が常に把握できるよう、Threat Horizons インテリジェンス レポートを公開しています。 https://cloud.google.com/solutions/security/leaders?e=0&hl=en#latest-threat-intelligence-from-google-experts Google は、特定の Google Cloud サービスに関するセキュリティ アップデート、脆弱性、既知の問題を含む速報情報を https://cloud.google.com/support/bulletins で公開しています。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
統5-3	お客様を支援するため、サードパーティが保有するシステムの脆弱性対応の管理をお客様にて実施する際の参考として、Googleの脆弱性対応について以下の情報を提供しています。 Google の社内脆弱性管理プロセスでは、あらゆるテクノロジー スタックにわたってセキュリティ脅威を積極的にスキャンしています。このプロセスでは、商用ツール、オープンソース ツール、そして専用の社内ツールを組み合わせて使用し、品質保証プロセス、ソフトウェア セキュリティ レビュー、徹底的な自動および手動による侵入調査（大規模なレッドチーム演習を含む）、外部監査などを実施しています。 脆弱性管理組織とそのパートナーは、脆弱性の追跡とフォローアップを担当しています。セキュリティは問題が完全に解決されて初めて向上するため、自動化パイプラインは脆弱性の状態を継続的に再評価し、パッチを検証し、誤った解決策や部分的な解決策を報告します。 脆弱性管理組織は、検出能力を向上させるため、真の脅威を示すシグナルとノイズを区別する高品質な指標に重点を置いています。また、業界およびオープンソース コミュニティとの交流も促進しています。 詳細については、Google Cloudのセキュリティに関するホワイトペーパーと Google Workspaceのセキュリティに関するホワイトペーパーをご覧ください。 Googleは、お客様が当社のセキュリティ、プライバシー、コンプライアンス管理について独立した検証を期待していることを認識しています。この保証を提供するために、Googleは複数の独立した第三者機関による監査を定期的に受けています。Googleは、お客様との契約期間中、以下の主要な国際基準を遵守することをお約束します。 -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 Google の最新の認証と監査レポートはいつでもご確認いただけます。Compliance reports managerを使用すると、これらの重要なコンプライアンス リソースにオンデマンドで簡単にアクセスできます。	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2 (Security Measures) (Cloudデータ処理付録書) 認証及び監査レポート
統5-4	-	-
統5-5	Google の全社員は入社時研修の一環としてセキュリティとプライバシーに関するトレーニングを受けます。また、Google 在籍中は継続的にセキュリティとプライバシーに関するトレーニングを受けます。職務によっては、専門のセキュリティ研修が追加で実施される場合もあります。たとえば、情報セキュリティ チームが新しいエンジニアに安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導します。詳しくは、セキュリティに関するホワイトペーパーをご覧ください。	-
統6	-	-
統7	-	-
統8	-	-
統9	-	-
統10	-	-
統11	-	-
統12	-	-
統13	-	-
統14	-	-
統15	お客様を支援するため、Google はお客様及びその従業員に向けて、当社サービスの使用方法を説明したドキュメントをGoogle Cloud および Workspace についてご用意しています。またより詳しいガイド付きトレーニングをご希望のお客様には、様々な研修コースと認定資格もご用意しています。	-
統16	-	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
統17	-	-
統18	-	-
統19	-	-
統20	クラウドプロバイダを選定する際の適正評価は、お客様の責任となっています。 Google は、お客様が 我々のサービスをご利用いただく前に、デューデリジェンスとリスク評価を実施する必要があることを認識しています。お客様を支援するため、Googleは、お客様が適切に外部委託先としてGoogle Cloud や Google Workspace を評価するための以下を含むリソースを提供しています。 さらに、Google はサードパーティのリスク管理（TPRM）プロバイダと連携し、お客様のクラウドに対する評価をサポートしています。TPRM プロバイダは、Google Cloud のプラットフォームとサービスを定期的に評価し、NIST SP 800-53、NIST CSF、ISO 27001、PCI-DSS、HIPAA、CMMC、SOC2、CSA STAR などの業界標準と規制に準拠した、数百ものセキュリティ、プライバシー、事業継続性、運用の復元力に関する管理策を検査します。TPRM プロバイダは、その観察と評価に基づいて、お客様独自のリスク評価プロセスの拡張と迅速化に役立つ独立した監査レポートを作成します。詳細については、Google Cloud のリスク評価リソースのページをご覧ください。 ◯コンプライアンス Google Cloud コンプライアンス https://cloud.google.com/security/compliance 最新の認証の取得状況 https://cloud.google.com/security/compliance/offerings ◯Google Cloud サービス規約 Google Cloud Platform サービス概要 https://cloud.google.com/terms/services Google Cloud Platform サービスレベル契約 https://cloud.google.com/terms/sla/ Google Workspace サービス概要 https://workspace.google.co.jp/intl/ja/terms/user_features.html Google Workspace サービスレベル契約 https://workspace.google.com/terms/sla.html	-
統20 (続き)	Google Cloud サービス固有の規約 https://cloud.google.com/terms/service-terms Google Workspace サービス固有の利用規約 https://workspace.google.co.jp/intl/ja/terms/service-terms/index.html データ処理及びセキュリティ規約 https://cloud.google.com/terms/data-processing-terms#top_of_page Cloudデータ処理付録書 https://cloud.google.com/terms/data-processing-addendum#top_of_page Google Cloud の復処理者(サブプロセッサー) https://cloud.google.com/terms/subprocessors	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google Workspace and Cloud Identity Subprocessors https://workspace.google.com/terms/subprocessors.html 技術サポートガイドライン https://cloud.google.com/terms/tssg/ ◯Google Cloud セキュリティ Google のセキュリティに関するホワイトペーパー https://cloud.google.com/security/overview/whitepaper クラウドネイティブセキュリティに関するホワイトペーパー https://cloud.google.com/security/beyondprod Google Workspace セキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ インフラストラクチャのセキュリティ https://cloud.google.com/security/infrastructure/ インフラストラクチャのセキュリティ設計の概要 https://cloud.google.com/security/infrastructure/design/ Google の Secure by Design への取り組みの概要 https://publicpolicy.google/resources/google_commitment_secure_by_design_overview.pdf セキュリティのリソース https://cloud.google.com/security クラウドのセキュリティプロダクト https://cloud.google.com/products/security-and-identity Google Cloud セキュリティ ベスト プラクティス センター https://cloud.google.com/security/best-practices セキュリティユースケース https://cloud.google.com/security/showcase/	
統20 (続き)	◯Google Cloud ロケーション Google Cloud のロケーション https://cloud.google.com/about/locations/ データ所在地、運用透明性及びお客様のプライバシーに関する Google Cloud ホワイトペーパー https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf ◯Google Cloud の障害復旧やインシデント管理 障害復旧計画ガイド https://cloud.google.com/architecture/dr-scenarios-planning-guide Google Cloud Service Health Dashboard	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	https://status.cloud.google.com/ Personalized Service Health https://cloud.google.com/service-health Cloud Monitoring https://cloud.google.com/monitoring データインシデント対応に関するホワイトペーパー https://cloud.google.com/docs/security/incident-response ◯データ削除 Google Cloud Platform におけるデータ削除に関するホワイトペーパー https://cloud.google.com/security/deletion ◯サポート Google Cloud サポート https://cloud.google.com/support-hub 言語のサポート https://cloud.google.com/support/docs/language-working-hours ◯企業情報 Alphabetのインベスター・リレーションズ https://abc.xyz/investor/	
統21	Googleは、規制対象法人との間にGoogle Cloud金融サービス契約を締結可能です。	-
1	Google Cloud金融サービス契約は、フレームワークの各事項に言及しています。お客様を支援するため、お客様の検討を要する各領域に関する情報を以下に記載しています。 契約の変更 契約の変更に関する詳細については、1.(1), 6)を参照。サービスの変更に関する詳細については、1.(1), 7)を参照のこと。	-
1. (1) 基本的な事項	-	-
1.(1), 1)	当事者らの役割及び責任、用語の定義並びに準拠法は、Google Cloud金融サービス契約に定められます。 また、Google Cloud金融サービス契約は、損害賠償についても言及しています。具体的には、Googleによる本サービスのパフォーマンスがサービスレベル契約を満たさない場合、規制対象法人は、サービスクレジットを請求することができます。 Google Cloud Platformサービスレベル契約 https://cloud.google.com/terms/sla/ Google Workspaceサービスレベル契約 https://workspace.google.com/terms/sla/ 準拠法を日本法、管轄裁判所を東京地方裁判所に設定することができます。	-
1.(1), 2)	-	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
1.(1), 3)	品質 お客様は、本サービスの機能を使用して、Googleによる本サービス（SLAを含む）のパフォーマンスを継続的に監視することができます。 検証 Googleは、お客様が当社のセキュリティ、プライバシー、コンプライアンス管理について独立した検証を期待していることを認識しています。この保証を提供するために、Googleは複数の独立した第三者機関による監査を定期的に受けています。Googleは、お客様との契約期間中、以下の主要な国際基準を遵守することをお約束します。 ・ISO/IEC 27001 (Information Security Management Systems) ・ISO/IEC 27017 (Cloud Security) ・ISO/IEC 27018 (Cloud Privacy) ・PCI DSS ・SOC 1 ・SOC 2 ・SOC 3 Google の最新の認証と監査レポートはいつでもご確認いただけます。Compliance reports managerを使用すると、これらの重要なコンプライアンス リソースにオンデマンドで簡単にアクセスできます。	継続的パフォーマンスモニタリング 認証及び監査レポート
1.(1), 4)	作業時間 SLAには、本サービスの可用性に関するGoogleのコミットメントが記載されます。SLAは、Google Cloud Platformサービスレベル契約、Google Workspace サービスレベル契約に関するページにおいて入手することができます。 サポートサービスについては、技術サポートサービスガイドラインのページに記載されています。これには、営業時間、応答時間、サポート言語が含まれます。 立入場所 迅速性、信頼性、堅牢性及び回復性を有するサービスをお客様に提供するため、Googleは、自ら又は自らの復処理者が設備を維持する場所にお客様のデータを保管し、処理することができます。 ・Googleの設備の場所及び個別のGCPサービスの展開場所に関する情報は、当社のグローバルロケーションに関するページにおいて入手することができます。 ・Googleの復処理者の設備の場所に関する情報は、当社のGoogle Cloudの復処理者に関するページ、Google Workspace and Cloud Identity Subprocessorsにおいて入手することができます。 Googleは、お客様のデータ（当該データが所在する国／地域を問わない。）につき、同一の契約におけるコミットメント及び技術上・組織上の措置を提供します。具体的には、以下のとおりです。 ・国／地域を問わず、全てのGoogleの設備に同一の堅牢なセキュリティ対策が適用されます。 ・Googleは、国／地域を問わず、自らの全ての復処理者に関して同一のコミットメントを行います。 Googleは、お客様のデータの保管場所に関してお客様に選択肢を与えます。お客様によるデータ保管場所の選択により、Googleは、お客様が選択した地域外にデータを保管しません。 また、お客様は、データロケーションに関する要件を実行するため、Googleが提供するツールの使用を選択することもできます。詳細は、当社のデータ所在地、運用透明性及びお客様のプライバシーに関するGoogle Cloudホワイトペーパーを参照のこと。	本サービス 技術サポート データロケーション Google Cloud Platform サービス固有の規約 (Google Cloud Service Specific Terms) Google Workspace サービス固有の規約 (Google Workspace Service Specific Terms) Data Security; Subprocessors (Cloudデータ処理付録書)

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google Cloud Platformサービスレベル契約 https://cloud.google.com/terms/sla/ Google Workspace サービスレベル契約 https://workspace.google.com/terms/sla.html Google Cloud Services: 技術サポート サービス ガイドライン https://cloud.google.com/terms/tssg/ Google Workspace 技術サポート サービス ガイドライン https://workspace.google.com/terms/tssg/ グローバルロケーションに関するページ https://cloud.google.com/about/locations/ Google Cloudの復処理者に関するページ https://cloud.google.com/terms/subprocessors Google Workspace and Cloud Identity Subprocessors https://workspace.google.com/intl/en/terms/subprocessors.html データ所在地、運用透明性及びお客様のプライバシーに関するGoogle Cloudホワイトペーパー https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf	Data Transfers (Cloudデータ処理付録書)
1.(1), 5)	Google Cloud金融サービス契約を参照のこと。	使用制限
1.(1), 6)	サービスや技術に変更がある場合、Googleは、全てのお客様に適用される、URLに存在する一定の規約を更新することができます。あらゆる更新は、厳格な要件を満たさなければなりません。例えば、かかる更新により、サービスの全般的なセキュリティが著しく低下し、又は貴社の既存の権利に重大な悪影響が及ぶようなことがあってはなりません。制限を受けるこれら更新以外にも、あらゆる契約の変更は、両当事者の署名が付された書面で行われなければなりません。	規約の変更、修正
1.(1), 7)	お客様は、Google 担当者による操作なしに、サービスを独自に操作できます。どのサービスを使用するか、どのように使用するか、どのような目的で使用するかは、お客様が決定します。また、サービスの利用方法の変更も、お客様が管理します。 Googleは、お客様が最新技術を活用できるよう、継続的にサービスを更新します。当社のサービスが一対多数の性質を有することを踏まえ、更新は、全てのお客様に対して同時に適用されます。 Googleの変更管理へのアプローチは、お客様自身の変更管理プロセスにとって重要であると認識しています。Googleは、本サービスの機能性、パフォーマンス、可用性又はセキュリティを著しく減じるような更新を行いません。 Googleが、代替サービスを提供することなくサービスを停止する必要がある場合、お客様は、12ヶ月以上前に通知を受けます。Googleは、当該期間において、引き続きサポートを提供し、製品及びセキュリティを更新します。 Google Cloud の変更管理へのアプローチの詳細については、以下をご覧ください。 https://cloud.google.com/docs/cloud-approach-to-change	サービス変更
1. (2)	サービス仕様 Google Cloud サービスは、当社のサービスの概要に関するページに記載されます。 Google Workspace サービスは、当社のサービスの概要に関するページに記載されます。	定義

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	データ保護 セキュリティを含むお客様のデータの保護に関するGoogleのコミットメントについては、Cloudデータ付録書で言及されます。 Google Cloud サービスの概要 https://cloud.google.com/terms/services Google Workspace サービスの概要 https://workspace.google.com/terms/user_features Cloudデータ処理付録書 https://cloud.google.com/terms/data-processing-addendum	秘密保持 Data Security; Google's Security Measures; (Cloudデータ処理付録書)
1.(2), 1)	手数料 Google Cloud金融サービス契約を参照のこと。 期間満了 Google Cloud金融サービス契約を参照のこと。	支払条件 契約期間及び解約
1.(2), 2)	Google Cloud サービスの内容に関しては、1. (2) を参照のこと。お客様は、使用するサービス並びにかかるサービスの使用方法及び用途を決定します。したがって、契約の範囲もお客様が決定します。 Google は、データセンターの物理的なセキュリティなど、お客様の組織が最終的に責任を負うリスクに対してクラウド プロバイダとして重大な責任を負っていることを認識しています。 規制対象法人にとって、クラウドにおける責任分担、特にお客様の組織とクラウド サービス プロバイダ間の責任の境界を明確に理解することが重要です。クラウドにおける責任分担は以下のとおりです。 クラウド サービス プロバイダは、ハードウェアやネットワークを含む、基盤となるクラウド インフラストラクチャのリスクとコントロールを管理する責任を負います。 お客様の組織は、データのセキュリティ保護やアプリケーションの管理など、クラウド内のお客様環境におけるリスクとコントロールを管理する責任を負います。 Google とお客様の責任分担についての更なる詳細については、Cloud Security Allianceのページにあるconsensus Assessment Initiative Questionnaire (CAIQ)への回答をご覧ください。	-
1.(2), 3)	Google Cloud サービスの内容に関しては1. (2) を、サービスの変更に関しては1.(1), 7)を参照のこと。	-
1.(2), 4)	Google Cloud金融サービス契約を参照のこと。 Googleは契約において、厳格な機密保持契約を締結しています。特に、お客様から提供された機密情報は契約に従ってのみ使用し、漏洩から保護します。	秘密保持
1.(2), 5)	Googleは、自らの従業員がGoogleのセキュリティ対策を遵守し、お客様データを処理する権限を与えられた全ての人員が秘密保持義務を負うことを確保します。 信頼できるインフラストラクチャ https://cloud.google.com/security/infrastructure	Data Security; Access and Compliance (Cloudデータ処理付録書)
1.(2), 6)	セキュリティを含むお客様のデータの保護に関するGoogleのコミットメントについては、Cloudデータ付録書で言及されます。 クラウドサービスのセキュリティは、2つの重要な要素から成ります。	秘密保持

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	(1) Googleのインフラストラクチャのセキュリティ Googleは、当社のインフラストラクチャのセキュリティを管理します。これは、本サービスをサポートするハードウェア、ソフトウェア、ネットワーキング及び設備のセキュリティを指します。 当社のサービスが一対多数の性質を有することを踏まえ、Googleは、全てのお客様に対して、同一の堅牢なセキュリティを提供します。 Googleは、セキュリティ実務に関してお客様に詳細な情報を提供することで、お客様がかかるセキュリティ実務を理解し、これをお客様自らのリスク分析の一環として検討できるようにします。 詳細は、以下より入手することができます。 ・インフラストラクチャのセキュリティ ・Googleのセキュリティに関するホワイトペーパー ・クラウドネイティブセキュリティに関するホワイトペーパー ・インフラストラクチャのセキュリティ設計の概要 ・セキュリティのリソース さらに、お客様は、GoogleのSOC 2レポートを参照することができます。 (2) クラウドにおけるお客様のデータのセキュリティ及び適用 お客様は、クラウドにおけるお客様のデータのセキュリティ及び適用を定義します。これは、お客様が本サービスを使用する際に実行および運用するために選択したセキュリティ対策を指します。 (a) デフォルトのセキュリティ 当社は、お客様のデータに関して可能な限り多くの選択肢を提供することを望んでいますが、お客様のデータのセキュリティはGoogleにとって最重要であるため、以下の予防措置を講じ、お客様を支援します。 保存データの暗号化: Googleは、お客様の追加行為を要することなく、保存されるお客様データをデフォルトで暗号化します。詳しくはGoogle Cloudの保存データの暗号化のページで確認できます。 転送データの暗号化: Googleは、当社によって又は当社のために管理されていない物理的境界の外に転送中のデータが移動する場合、一又は複数のネットワークレイヤでかかる全てのデータを暗号化し、認証します。詳しくはGoogle Cloudの転送データの暗号化のページで確認できます。 (b) セキュリティプロダクト Google以外にお客様が利用することのできるその他のツール及び方法に加え、お客様は、お客様のデータのセキュリティを強化し、監視するために、Googleが提供するツールの使用を選択することができます。Googleのセキュリティプロダクトに関する詳細は、Google Cloudのセキュリティプロダクトのページにおいて入手することができます。 (c) セキュリティリソース また、Googleは、以下のガイダンスを提供しています。 Google Cloud セキュリティ ベスト プラクティス センター	Data Security; Google's Security Measures; (Cloudデータ処理付録書)

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
1.(2), 7)	Google Cloudでは、お客様はバックアップの管理にGoogle Cloud バックアップと障害復旧（DR）サービス を活用することができます。データのバックアップに活用できるサービスについての詳細は、障害復旧の構成要素および データの障害復旧シナリオ をご参照ください。 Google Workspaceでは、お客様はデータ エクスポートを使用して組織全体のデータをエクスポートできます。Google は、API や BigQuery、パートナー ソリューションのAfi や SpinOne など、組織の Google Workspace データを操作および抽出するためのツールも多数提供しています。その他のサードパーティおよびパートナーのオプションについては、Google Cloud Partnerのディレクトリをご覧ください。	-
1. (3)	お客様は、本サービスの機能を使用して、Googleによる本サービス（SLAを含む）のパフォーマンスを継続的に監視することができます。 Googleによる本サービスのパフォーマンスがサービスレベル契約を満たさない場合、規制対象法人は、サービスクレジットを請求することができます。 Google Cloud Platformサービスレベル契約 https://cloud.google.com/terms/sla/ Google Workspaceサービスレベル契約 https://workspace.google.com/terms/sla/	パフォーマンスの継続モニタリング 本サービス
1. (4)	情報 Googleは、お客様が注文した本サービスを提供するためにのみお客様のデータにアクセスし、又は使用することを確約し、かかるデータをその他のGoogleの製品、サービス又は広告に使用しません。 監督当局への協力 Googleは、監督当局及び監督当局が任命する者に対し、監査、立入及び情報に係る権利を付与します。これには、文書及び情報へのアクセス並びに現場視察を実施する権利が含まれます。 Google は、監査、情報及び立入に係る権利を行使する監督当局、解決当局、およびその任命者に協力します。 報告、連絡及びインシデント対応 Google は、お客様による本サービスのご利用を効果的に管理するためには、本サービスに関する十分な情報を定期的に入手する必要があることを認識しています。Google は、お客様が本サービスを継続的に効果的に監視できるよう、さまざまな仕組みを提供しています。 Google は、お客様に提供される SLA に従って Google が本サービスを遂行する能力に重大な影響を与える事態の発生について、情報を提供します。 お客様は、本サービスの機能を使用して、Google による本サービスのパフォーマンス（SLA を含む）を継続的に監視できます。 例: Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。 さらに、Google はデータ インシデントが発生した場合、速やかに遅滞なくお客様に通知します。Google のデータ インシデント対応プロセスの詳細については、データ インシデント対応に関するホワイトペーパーをご覧ください。	カスタマーデータの保護 規制当局の情報、監査及び立入 カスタマーコンプライアンスの支援 重要な発生事項 Data Incidents (Cloudデータ処理付録書)
1.(4), 1)	お客様は、本サービスの機能を使用して、Googleによる本サービス（SLAを含む）のパフォーマンスを継続的に監視することができます。 例えば、以下の機能があります。 ・Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。	継続的パフォーマンスモニタリング

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	・Personalized Service Health は、プロジェクトに関連する中断を伴うイベントをフィルタリングし、影響の評価、ビジネス継続性の維持、更新の追跡に役立つ情報を提供します。Personalized Service Health は、Service Health ダッシュボード、構成可能なアラート、Cloud Logging によるエクスポート可能なログなど、あらゆるアラート、インシデント対応、モニタリング ワークフローに組み込むことができます。 ・Google Cloud のオブザーバビリティは、Google Cloud 上などで実行されているアプリケーションとシステム向けの統合モニタリング、ロギング、トレース マネージド サービスです。 ・Google Workspaceの管理コンソールのレポートは、潜在的なセキュリティリスクの調査、ユーザーのコラボレーションの測定、誰がいつサインインしたかの追跡、管理者のアクティビティの分析を含む様々な機能を提供します。 ・Google Cloudのアクセスの透明性およびGoogle Workspaceのアクセスの透明性は、お客様が自らのデータに関する、Googleの人員によるアクションのログを参照できる機能です。ログエントリには、影響を受けるリソース、アクション日時、アクション理由（サポート要請に関連するケース番号等）及びデータに対してアクションをした人に関するデータ（Googleの人員の所在地等）が含まれます。	
1.(4),2)	Googleは、お客様がデータへのアクセス、修正、処理の制限、ならびにデータの取得または削除を実施できる機能を提供しています。 お客様は、Google 担当者による操作なしに、サービスを独自に操作できます。どのサービスを使用するか、どのように使用するか、どのような目的で使用するかは、お客様が決定します。したがって、お客様は関連する作業について常に管理できます。 規制対象法人は、Googleに指示をすることができ、Googleは、それらの指示を遵守します。規制対象法人は、以下の機能を使用し、本サービスに関してGoogleに指示をすることができます。 ・Cloud Console：お客様が自らのGCPリソースを管理するために使用することができるウェブベースのグラフィカルユーザーインターフェース。 ・gcloud コマンドラインツール： GCPに主要なコマンドラインインターフェースを提供するツール。コマンドラインインターフェースは、コンピュータのオペレーティング・システムのユーザーインターフェースです。 ・Google APIs：GCPへのアクセスを提供するアプリケーションプログラミングインターフェース。	Access; Rectification; Restricted Processing; Portability (Cloudデータ処理付録書) Deletion by Customer (Cloudデータ処理付録書) Compliance with Customer's Instructions (Cloudデータ処理付録書)
1.(4),3)	Google Cloud金融サービス契約を参照のこと	準拠法
1.(4),4)	Google は、規制対象法人や監督当局にとってレジリエンスが重要な焦点であることを認識しています。Googleのホワイトペーパー「Strengthening operational resilience in financial services by migrating to Google Cloud」では、金融サービス分野におけるオペレーショナル・レジリエンスの継続した重要性、そして Google Cloud への適切な移行がオペレーショナル・の強化に果たす役割について説明しています。 Googleのホワイトペーパー「Google Cloud インフラストラクチャ信頼性ガイド」では、Google Cloud が設計から運用に至るまで、コアインフラストラクチャとサービスにレジリエンスと可用性をどのように組み込んでいるかを説明しています。また、Google とお客様の運命共同体モデルについても解説しています。これは、お客様が Google が提供するコアサービスを基盤として、ビジネスを運営し、規制およびコンプライアンス義務を満たすために必要なレベルの可用性とレジリエンスを実現する方法です。 さらに、アプリケーションで望ましい信頼性の結果を達成する方法については、「クラウド インフラストラクチャの停止に対する障害復旧の設計」のドキュメントを参照ください。 ビジネス継続性 / 障害復旧シナリオのテストについては、Googleにる自身の環境のテストに加え、規制対象法人が Google Cloud のデプロイメントを独自にテストできるツールおよびリソースも多数提供しています。 「データの障害復旧シナリオ」と「アプリケーションの障害復旧シナリオ」のドキュメントでは、それぞれデータのバックアップと復旧、およびアプリケーションのバックアップと復旧に関する一般的な災害シナリオに関する情報を提供しています。 お客様を支援するため、Google はお客様及びその従業員に向けて、当社サービスの使用方法を説明したドキュメントをGoogle Cloud および Workspace についてご用意しています。またより詳しいガイド付きトレーニングをご希望のお客様には、様々な研修コースと認定資格もご用意しています。	技術サポート
1.(4),5)	Google は、お客様が中断の発生を前提として影響許容度を設定することが期待されていることを認識しています。	事業継続性及び災害復旧

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google は、お客様が Google Cloud 上で望ましい信頼性を実現できるよう尽力しています。お客様を支援するため、クラウド プラットフォーム上で信頼性の高いサービスを設計および運用する方法を「Google Cloud Architecture Framework」のドキュメントで説明しています。また、「クラウド インフラストラクチャの停止に対する障害復旧の設計」のドキュメントでは、クラウド インフラストラクチャの障害に耐性のあるアプリケーションの設計方法に関する情報とリソースを提供しています。 影響許容度内にとどめるために、多くの場合、お客様は特定の復旧時間目標（RTO）と復旧ポイント目標（RPO）を達成できる必要があることを認識しています。当該ドキュメントでは、お客様がGoogle Cloud 上のアプリケーションで望ましい RTO と RPO を達成する方法について説明しています。	
1.(4),6)	Google はデータ インシデントが発生した場合、速やかに遅滞なくお客様に通知します。Google のデータ インシデント対応プロセスの詳細については、データ インシデント対応に関するホワイトペーパーをご覧ください。	Data Incidents (Cloudデータ処理付録書)
1.(4),7)	Google はデータ インシデントが発生した場合、速やかに遅滞なくお客様に通知します。Google のデータ インシデント対応プロセスの詳細については、データ インシデント対応に関するホワイトペーパーをご覧ください。 お客様自身のインシデント対応を支援するため、Google からのインシデント通知には以下の内容が記載されます。 ・データ インシデントの性質（影響を受けるお客様のリソースを含む） ・データ インシデントに対処し、潜在的なリスクを軽減するために Google が講じた、または講じる予定の対策 ・データ インシデントに対処するために Google がお客様に推奨する対策（該当する場合） ・詳細情報を入手できる連絡先の詳細 Google以外にお客様が利用することのできるその他のツール及び方法に加え、Google が提供するソリューションやツールを使用して、データのセキュリティを強化および監視することもできます。 ・エージェント SOC は、自律的なトリアージと調査、プロアクティブな脅威ハンティング、動的検出エンジニアリングなど、変化するセキュリティ環境にリアルタイムで適応するために、継続的なループで連携するAIエージェントの動的なシステムをオーケストレートします。 ・Google のセキュリティ プロダクトに関する情報は、こちらをご覧ください。Security Command Center は、Google Cloud の脆弱性と脅威に関する一元的なレポート サービスです。Security Command Center は、セキュリティとデータのアタックサーフェスの評価、資産のインベントリと検出機能の提供、構成ミスおよび脆弱性や脅威の特定、リスクの軽減と修復を支援することで、セキュリティ体制の強化を支援します。 ・Google Workspace では、Security center が高度なセキュリティ情報と分析の機能を提供し、ドメインに影響を与えるセキュリティ問題の可視性と制御性を高めます。Securiy center は、Google 管理コンソールの詳細設定を拡張し、セキュリティ データを表示します。 Googleは、当社サービスの全てのユーザーアクティビティに関して、誰がいつ、どこで、何をしたのかを可視化することがお客様にとって必要であることを認識しています。Google は、Cloud Console、暗号化、ログ記録とモニタリング、ID とアクセスの管理、セキュリティ スキャン、ファイアウォールなど、お客様がお客様のデータへのアクセスを保護および制御するために使用できるセキュリティ リソース、機能、コントロールを提供しています。 ・Identity and Access Management は、Google Cloud リソースへのアクセス権とロールを制御することで、不正アクセスを防止します。 ・Cloud Audit Logs は、お客様のセキュリティチームがGCPの監査証跡を維持し、管理アクティビティ、データアクセス及びシステムイベントに関する詳細を参照することを可能にします。 ・多要素認証（MFA）は 、ユーザー アカウントとデータを保護するための幅広い検証方法を提供します。 Googleのホワイトペーパー「Trusting your data with Google Cloud whitepaper」および「 Trusting your data with Google Workspace whitepaper 」のセクション「Safeguarding access to your data」では、Google のデータアクセス プロセスとポリシーについて説明しています。 さらに、以下のツールを使用して、Google 担当者がお客様のデータに対して実行する限定的なアクションを監視および制御することもできます。 ・アクセスの透明性は、Google 担当者がお客様のデータに対して行った操作のログを確認できる機能です。ログエントリには、影響を受けたリソース、操作の時刻、操作の理由（例：サポート リクエストに関連付けられたケース番号）、データに対して操作を行ったユーザーに関するデータ（例：Google 担当者の所在地）が含まれます。 ・Access Approvalは、Googleのサポート及びエンジニアリングチームにお客様のコンテンツへのアクセスを許可する前に、お客様による明示的な承認を義務付けることを可能とする機能です。Access Approvalは、アクセスの透明性が提供する透明性に加え、さらなる管理層を提供します。 またGoogle Workspaceについては、 ・Status Dashboard サービスのステータス情報を確認できます。 ・管理コンソールのレポート が潜在的なセキュリティリスクの調査、ユーザーのコラボレーションの測定、誰がいつサインインしたかの追跡、管理者のアクティビティの分析を含む様々な機能を提供します。	Data Security; Additional Security Controls (Cloudデータ処理付録書) Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloudデータ処理付録書)

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	・アクセスの透明性 で、お客様が自らのデータに関する、Googleの人員によるアクションのログを参照できます。ログエントリには、影響を受けるリソース、アクション日時、アクション理由（サポート要請に関連するケース番号等）及びデータに対してアクションをした人に関するデータ（Googleの人員の所在地等）が含まれます。	
1.(4),8)	Googleは、本サービスの事業継続計画を実施し、当該計画のレビュー及びテストを少なくとも年1回行い、業界基準に沿った最新の状態に保つよう確保します。規制対象法人は、当社の計画及びテスト結果を参照することができます。 Google のデータセンターは、独立した第三者監査機関による監査を受け、ISO 22301 準拠について認証を受けています。 さらに、お客様による事業コンティンジェンシープランの立案における当社の本サービスの使用方法に関する情報は、当社の障害復旧計画ガイドにおいて入手することができます。	事業継続性及び災害復旧
1. (5)	Googleは、本サービスの提供において適用される全ての法令を遵守します。 お客様は、Alphabetのインベスター・リレーションズに関するページに記載される当社の使命、理念及び文化に関する情報を参照することができます。また、当該ページには、当社の行動規範等の組織方針に関する情報についても記載があります。 Investor Updates - Alphabet Investor Relations https://abc.xyz/investor/	表明及び保証 反社会的勢力の排除
1. (6)	契約解除： 規制対象法人は、事前に通知することにより、自己都合（法律を遵守するのに必要な場合もしくは規制当局により指図された場合を含む）により当社の契約を解除することを選択できます。 さらに、規制対象法人は、Googleが是正期間後に重大な違反を犯し、支配権が変更され、又は支払不能に陥った場合、事前に通知することにより当社の契約を解除することができます。 データ消去： 契約関係を解除する際、Googleは、当社のシステムからお客様データを削除する旨のお客様の指示を遵守します。削除に関する詳細は、ホワイトペーパー「Google Cloud でのデータの削除」をご覧ください。 移行支援： Googleは、規制対象法人が当社サービスの利用をやめる（他のサービスプロバイダへのサービスの移行を含む。）場合、十分な時間が必要となることを認識します。規制対象法人がこれを達成できるよう、要請に応じて、Googleは、引き続き契約の満了又は解約後12ヶ月間サービスを提供します。 当社の本サービスは、お客様が自らのデータを自主的に移転することを可能とします。かかる移転には、Googleの許可は不要です。但し、規制対象法人がサポートを必要とする場合、要請に応じて、Googleは、ワークロードの移行又はその他本サービスの利用の移行を支援する助言サービス及び実施サービスを提供します。 Googleは、当社の契約の全期間中及び解除後の移行期間中、お客様が自らのデータにアクセスし、エクスポートすることを可能にします。お客様は、複数の業界基準フォーマットで、本サービスからお客様のデータをエクスポートすることができます。 例： ・Google Kubernetes Engineは、異なるクラウド間及びオンプレミス環境でのポータビリティを可能とする、準備の完了したマネージド環境です。 ・Migrate to Containersは、お客様がワークロードをGoogle Kubernetes Engineのコンテナに直接移動し、変換することを可能とします。 ・お客様は、全てのVMイメージをtarアーカイブ形式でエクスポート／インポートすることができます。OSイメージに関する詳細はこちら、ストレージのオプションに関する詳細はこちらのページをそれぞれご覧ください。 ・Google Workspaceについては、 Googleアカウントヘルプのページを参照ください。また、データ エクスポートは、当社のサービスからデータのコピーを安全に簡単にエクスポートおよびダウンロードできる機能です。 Google は、マルチクラウドとハイブリッドクラウドのアプローチをサポートするオープンクラウドを信条としています。オープンソースベースのテクノロジーを活用して実装することで、これらのアプローチは、堅牢な出口戦略に必要なレベルのポータビリティ、代替可能性、そして存続可能性をお客様に提供できます。詳しくは、Googleのホワイトペーパー「Strengthening operational resilience in financial services by migrating to Google Cloud」をご覧ください。	契約期間及び解除 解除に関する削除（データ処理及びセキュリティ規約） 移行

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google Cloud は、ポータビリティと相互運用性に対するお客様のニーズに応え、イノベーションを推進するためのオープン性を促進することに尽力しています。組織には、コンテンツを表示、削除、ダウンロード、転送するためのツールを提供しています。クラウドのお客様は、お客様のデータを完全に制御し、他のプラットフォームへの移行や、自社内でのデータの保存・処理を決定した場合に、Google Workspace および Google Cloud からデータを取り出すことができます。 サービス提供終了に伴う事前通知: 規制対象法人は、Googleとの直接契約を取り交わすことにより、Google によって特定されたサービスにおいてサービス提供終了に伴う事前通知を受けることができるようになります。	
1. (7)	Google Cloud金融サービス契約を参照のこと。	責任
1. (8)	お客様は、契約期間中および解除後においても、自らのデータ、当社サービス及び自らのアプリケーションの使用により自らのデータから得られたデータに含まれる全ての知的財産権を保持します。 Googleは、お客様が注文した本サービスを提供するためにのみお客様のデータにアクセスし、又は使用することを確約し、かかるデータをその他のGoogleの製品、サービス又は広告に使用しません。	知的財産 カスタマーデータの保護
1. (9)	-	-
1. (9), 1)	Googleは、お客様が注文した本サービスを提供するためにのみお客様のデータにアクセスし、又は使用することを確約し、そのデータをその他のGoogleの製品、サービス又は広告に使用しません。 Googleは契約において、厳格な機密保持契約を締結しています。特に、お客様から提供された機密情報は契約に従ってのみ使用し、漏洩から保護します。	カスタマーデータの保護 秘密保持
1. (9), 2)	Googleの報告、連絡及びインシデント対応に関する詳細は、1. (4)を参照のこと。	-
1. (10)	-	-
1. (10)	-	-
1. (11)	-	-
1. (11), 1)	Googleは、規制対象法人が、再委託に関連するリスクを検討する必要があることを認識します。また、当社は、提供し得る最も信頼性の高い、堅牢な、回復力の高いサービスを貴社および当社の全てのお客様に提供することも希望します。場合によっては、明確な利点（24時間/週7日体制でのサポートの提供等）により、信頼性の高い他の機関と協働する場合があります。 規制対象法人が再委託を管理し、使用するサービスに関して選択できるよう、Googleは以下を行います。 ・当社の再委託先に関する情報を提供します。 ・当社の再委託先に変更に関して事前に通知します。 ・新しい再委託先に関して懸念がある場合に、規制対象法人が解除することを可能とします。 Googleは、当社の再委託先が当社が行うのと同程度の高い基準を満たすことを義務付けます。具体的に、Googleは、当社の再委託先が当社及びお客様との間の契約を遵守することを義務付けます。 再委託先に業務を委託するにあたり、Googleは、再委託先及び再委託される機能関するリスクを検討する評価を実施し、当該再委託先が適任であることを確認します。	Google下請業者
1. (11), 2)	Googleは、再委託された全ての義務の履行に関し、お客様に対する説明責任を継続して負います。 Google は、再委託義務に関し、お客様に対する責任を継続して負います。	Google下請業者
1. (11), 3)	Googleは、当社の再委託先が当社が行うのと同程度の高い基準を満たすことを義務付けます。具体的に、Googleは、当社の再委託先が当社及びお客様との間の契約を遵守することを義務付けます。	Google下請業者
1. (11), 4)	規制対象法人は、サービスを提供する当事者らに関して選択肢を有するべきです。これを確保するため、規制対象法人は、再委託先の変更が自らのリスクを著しく増大させると判断する場合又は合意された通知を受領していない場合、当社の契約を解除する選択肢を有します。	Google下請業者
1. (12)	Googleは、規制対象法人、監督当局及びこれらが任命する者に対し、監査、立入及び情報提供に係る権利を付与します。	カスタマーコンプライアンスの支援 認証及び監査レポート

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Googleは、当社サービスの監査に関して規制対象法人をサポートすることを確約します。当該サポートは、公開される当社の通常のサービス手数料に含まれていないため、Googleは、監査に関連する追加手数料を課す場合があります。Googleは、活動の範囲を認識した時点で、かかる活動の前に手数料の詳細を通知します。 Google は、規制対象法人または監督当局に代わって実施される監査により、サービスの運用と管理において対処されていない逸脱が特定された場合、適切な是正措置または改善措置を講じるよう努めます。 Googleは、お客様が当社のセキュリティ、プライバシー、コンプライアンス管理について独立した検証を期待していることを認識しています。この保証を提供するために、Googleは複数の独立した第三者機関による監査を定期的に受けています。Googleは、お客様との契約期間中、以下の主要な国際基準を遵守することをお約束します。 ・ISO/IEC 27001 (Information Security Management Systems) ・ISO/IEC 27017 (Cloud Security) ・ISO/IEC 27018 (Cloud Privacy) ・PCI DSS ・SOC 1 ・SOC 2 ・SOC 3 Google の最新の認証と監査レポートはいつでもご確認いただけます。Compliance reports managerを使用すると、これらの重要なコンプライアンス リソースにオンデマンドで簡単にアクセスできます。	
1. (13)	Google は、規制対象事業体とその監督当局が 我々 のサービスを効果的に監査できる必要があることを認識しています。Googleは、規制対象法人、監督当局及びこれらが任命する者に対し、監査、立入及び情報提供に係る権利を付与します。 これには、立入監査を実施するために、本サービスを提供するために使用する Google の施設への立入も含まれます。 Google はデータ インシデントが発生した場合、速やかに遅滞なくお客様に通知します。Google のデータ インシデント対応プロセスの詳細については、データ インシデント対応に関するホワイトペーパーをご覧ください。 お客様自身のインシデント対応を支援するため、Google からのインシデント通知には以下の内容が記載されます。 ・データ インシデントの性質（影響を受けるお客様のリソースを含む） ・データ インシデントに対処し、潜在的なリスクを軽減するために Google が講じた、または講じる予定の対策 ・データ インシデントに対処するために Google がお客様に推奨する対策（該当する場合） ・詳細情報を入手できる連絡先の詳細 Google以外にお客様が利用することのできるその他のツール及び方法に加え、Google が提供するソリューションやツールを使用して、データのセキュリティを強化および監視することもできます。 ・エージェント SOC は、自律的なトリアージと調査、プロアクティブな脅威ハンティング、動的検出エンジニアリングなど、変化するセキュリティ環境にリアルタイムで適応するために、継続的なループで連携するAIエージェントの動的なシステムをオーケストレートします。 ・Google のセキュリティ プロダクトに関する情報は、こちらをご覧ください。Security Command Center は、Google Cloud の脆弱性と脅威に関する一元的なレポート サービスです。Security Command Center は、セキュリティとデータのアタックサーフェスの評価、資産のインベントリと検出機能の提供、構成ミスおよび脆弱性や脅威の特定、リスクの軽減と修復を支援することで、セキュリティ体制の強化を支援します。 ・Google Workspace では、Security center が高度なセキュリティ情報と分析の機能を提供し、ドメインに影響を与えるセキュリティ問題の可視性と制御性を高めます。Securiy center は、Google 管理コンソールの詳細設定を拡張し、セキュリティ データを表示します。 Googleは、当社サービスの全てのユーザーアクティビティに関して、誰がいつ、どこで、何をしたのかを可視化することがお客様にとって必要であることを認識しています。Google は、Cloud Console、暗号化、ログ記録とモニタリング、ID とアクセスの管理、セキュリティ スキャン、ファイアウォールなど、お客様がお客様のデータへのアクセスを保護および制御するために使用できるセキュリティ リソース、機能、コントロールを提供しています。 ・Identity and Access Management は、Google Cloud リソースへのアクセス権とロールを制御することで、不正アクセスを防止します。 ・Cloud Audit Logs は、お客様のセキュリティチームがGCPの監査証跡を維持し、管理アクティビティ、データアクセス及びシステムイベントに関する詳細を参照することを可能にします。 ・多要素認証（MFA）は 、ユーザー アカウントとデータを保護するための幅広い検証方法を提供します。	カスタマーコンプライアンスの支援 Data Incidents (Cloudデータ処理付録書) Data Security; Additional Security Controls (Cloudデータ処理付録書) Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloudデータ処理付録書)

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Googleのホワイトペーパー「Trusting your data with Google Cloud whitepaper」および「 Trusting your data with Google Workspace whitepaper 」のセクション「Safeguarding access to your data」では、Google のデータアクセス プロセスとポリシーについて説明しています。 さらに、以下のツールを使用して、Google 担当者がお客様のデータに対して実行する限定的なアクションを監視および制御することもできます。 ・アクセスの透明性は、Google 担当者がお客様のデータに対して行った操作のログを確認できる機能です。ログエントリには、影響を受けたリソース、操作の時刻、操作の理由（例：サポート リクエストに関連付けられたケース番号）、データに対して操作を行ったユーザーに関するデータ（例：Google 担当者の所在地）が含まれます。 ・Access Approvalは、Googleのサポート及びエンジニアリングチームにお客様のコンテンツへのアクセスを許可する前に、お客様による明示的な承認を義務付けることを可能とする機能です。Access Approvalは、アクセスの透明性が提供する透明性に加え、さらなる管理層を提供します。 またGoogle Workspaceについては、 ・Status Dashboard サービスのステータス情報を確認できます。 ・管理コンソールのレポート が潜在的なセキュリティリスクの調査、ユーザーのコラボレーションの測定、誰がいつサインインしたかの追跡、管理者のアクティビティの分析を含む様々な機能を提供します。 ・アクセスの透明性 で、お客様が自らのデータに関する、Googleの人員によるアクションのログを参照できます。ログエントリには、影響を受けるリソース、アクション日時、アクション理由（サポート要請に関連するケース番号等）及びデータに対してアクションをした人に関するデータ（Googleの人員の所在地等）が含まれます。	
1. (14)	データの削除（物理的な記録媒体がライフサイクルの終了に達した場合に安全に終了させることを含む）に関する詳細は、当社のGoogle Cloud Platformにおけるデータ削除に関するホワイトペーパーを参照のこと。 データ削除に関するホワイトペーパー https://cloud.google.com/docs/security/deletion Googleは、お客様が当社のセキュリティ、プライバシー、コンプライアンス管理について独立した検証を期待していることを認識しています。この保証を提供するために、Googleは複数の独立した第三者機関による監査を定期的に受けています。Googleは、お客様との契約期間中、以下の主要な国際基準を遵守することをお約束します。 ・ISO/IEC 27001 (Information Security Management Systems) ・ISO/IEC 27017 (Cloud Security) ・ISO/IEC 27018 (Cloud Privacy) ・PCI DSS ・SOC 1 ・SOC 2 ・SOC 3 Google の最新の認証と監査レポートはいつでもご確認いただけます。Compliance reports managerを使用すると、これらの重要なコンプライアンス リソースにオンデマンドで簡単にアクセスできます。	Decommissioned Disks and Disk Erase Policy (Cloudデータ処理付録書) 認証及び監査レポート
1. (15)	当社のサポートサービスは、日本語で利用することができます。当社の言語サポートに関する詳細は、言語サポートに関するページを参照のこと。 言語サポートと業務時間 https://cloud.google.com/support/docs/language-working-hours	技術サポート
1. (16)	Googleの報告、連絡及びデータインシデント対応に関する詳細は、1. (4)を参照のこと。 トレーサビリティに関する詳細は、1.(4),7)を参照のこと。	-
1. (17)	Google の社内脆弱性管理プロセスでは、あらゆるテクノロジー スタックにわたってセキュリティ脅威を積極的にスキャンしています。このプロセスでは、商用ツール、オープンソース ツール、そして専用の社内ツールを組み合わせて使用し、品質保証プロセス、ソフトウェア セキュリティ レビュー、徹底的な自動および手動による侵入調査（大規模なレッドチーム演習を含む）、外部監査などを実施しています。	Intrusion Detection / Incident Response, Data Center and Network Security, Appendix 2

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	脆弱性管理組織とそのパートナーは、脆弱性の追跡とフォローアップを担当しています。セキュリティは問題が完全に解決されて初めて向上するため、自動化パイプラインは脆弱性の状態を継続的に再評価し、パッチを検証し、誤った解決策や部分的な解決策を報告します。 脆弱性管理組織は、検出能力を向上させるため、真の脅威を示すシグナルとノイズを区別する高品質な指標に重点を置いています。また、業界およびオープンソース コミュニティとの交流も促進しています。 詳細については、Google Cloudのセキュリティ ホワイトペーパーと Google Workspaceのセキュリティ ホワイトペーパーをご覧ください。 Google のインシデントレスポンスチームは、高度な検出ツール、シグナル、アラートメカニズムを活用し、潜在的なインシデントを早期に検知します。 Google はデータ インシデントが発生した場合、速やかに遅滞なくお客様に通知します。Google のデータ インシデント対応プロセスの詳細については、データインシデント対応に関するホワイトペーパーをご覧ください。	(Security Measures) (Cloudデータ処理付録書) Data Incidents (Cloudデータ処理付録書)
2	SLA はサービスの測定可能なパフォーマンス基準を提供し、Google Cloud Platform および Google Workspace のサービスレベル契約ページでご確認いただけます。 技術サポートサービスガイドラインには、当社のサポート対応時間が記載されています。 Google Cloud Platformサービスレベル契約 https://cloud.google.com/terms/sla/ Google Workspace サービスレベル契約 https://workspace.google.com/terms/sla.html Google Cloud Services 技術サポートサービスガイドライン https://cloud.google.com/terms/tssg Google Workspace 技術サポートサービスガイドライン https://workspace.google.com/terms/tssg/	本サービス 技術サポート
3	お客様を支援するため、Googleはお客様にて対応策を検討する際の参考として以下の情報を提供しています。 お客様は、本サービスの機能を使用して、Googleによる本サービス（SLAを含む）のパフォーマンスを継続的に監視することができます。 例えば、以下の機能があります。 ・Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。 ・Personalized Service Health は、プロジェクトに関連する中断を伴うイベントをフィルタリングし、影響の評価、ビジネス継続性の維持、更新の追跡に役立つ情報を提供します。 Personalized Service Health は、Service Health ダッシュボード、構成可能なアラート、Cloud Logging によるエクスポート可能なログなど、あらゆるアラート、インシデント対応、モニタリング ワークフローに組み込むことができます。 ・Google Cloud のオブザーバビリティは、Google Cloud 上などで実行されているアプリケーションとシステム向けの統合モニタリング、ロギング、トレース マネージド サービスです。 Google は、規制対象法人や監督当局にとってレジリエンスが重要な焦点であることを認識しています。Googleのホワイトペーパー「Strengthening operational resilience in financial services by migrating to Google Cloud」では、金融サービス分野におけるオペレーショナル・レジリエンスの継続した重要性、そして Google Cloud への適切な移行がオペレーショナル・の強化に果たす役割について説明しています。 Googleのホワイトペーパー「Google Cloud インフラストラクチャ信頼性ガイド」では、Google Cloud が設計から運用に至るまで、コアインフラストラクチャとサービスにレジリエンスと可用性をどのように組み込んでいるかを説明しています。また、Google とお客様の運命共同体モデルについても解説しています。これは、お客様が Google が提供するコアサービスを基盤として、ビジネスを運営し、規制およびコンプライアンス義務を満たすために必要なレベルの可用性とレジリエンスを実現する方法です。	継続的パフォーマンスモニタリング

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	さらに、アプリケーションで望ましい信頼性の結果を達成する方法については、「クラウド インフラストラクチャの停止に対する障害復旧の設計」のドキュメントを参照ください。	
4	データの抽出及びGoogleによる移行作業への協力に関する詳細は、1.(6)を参照のこと。 移行費用は透明であり、当社が公表するサービス手数料に基づきます。 さらに、Google Cloudのお客様がGoogle Cloud の利用を中止し、データを別のクラウド プロバイダやオンプレミスに移行したい場合、無料のデータ転送サービスを利用して Google Cloud からデータを移行できます。詳しくは、ブログをご覧ください。 当社サービスは、貴社が自らのデータを自主的に移転することを可能とします。但し、規制対象法人がサポートを必要とする場合、要請に応じて、Googleは、合意する追加手数料に基づき、ワークロードの移行又はその他本サービスの利用の移行を支援する助言サービス及び実施サービスを提供します。	移行支援
統22	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育及び訓練」(ISO 27001:2022、附属書 A 6.3) が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員は入社時研修の一環としてセキュリティとプライバシーに関するトレーニングを受けます。また、Google 在籍中は継続的にセキュリティとプライバシーに関するトレーニングを受けます。職務によっては、専門のセキュリティ研修が追加で実施される場合もあります。たとえば、情報セキュリティ チームが新しいエンジニアに安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導します。詳しくは、セキュリティに関するホワイトペーパーをご覧ください。	-
統23	Google は ISO27001 認証を受けています。この基準では、供給者関係に関する管理策（ISO 27001:2022、附属書 A 5.19～5.22）が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者の監査法人によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloudを外部委託先として評価する場合、次の様な公開済みの情報を提供します。 ・「Google のセキュリティに関するホワイトペーパー」にて各種サービスの可用性・データの安全性（機密性保護）・完全性の確保のための体制などを総合的に説明しています。 https://cloud.google.com/docs/security/overview/whitepaper ・Google Cloudは外部独立監査組織によるSOC監査レポートのご提供が可能です。 ・Google Cloudは、お客様の指示によりGoogle Cloudがお客様データにアクセスする際のログが取得出来るアクセスの透明性ログ機能を提供しています。 https://cloud.google.com/access-transparency ・お客様はGoogle Cloudの復処理者について以下のリソースを参考にできます。 https://cloud.google.com/terms/subprocessors https://cloud.google.com/terms/data-processing-addendum (section 11. Subprocessors)	-
統24	Google Cloudを外部委託先として評価する場合、以下の情報および契約を通じて安全対策を講じることができます。 ・「Google セキュリティ ホワイトペーパー」にて Google Cloud がその責任範囲において実施する各種安全対策（伝送データのセキュリティ、データのセキュリティ、オペレーション セキュリティなど）を総合的に確認できます。 Google セキュリティ ホワイトペーパー https://cloud.google.com/docs/security?hl=ja Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	・Google Cloudは、独立監査組織によるSOC監査報告書等のご提供が可能です。 ・個人データを含むお客様のデータに対する統制権はお客様にあります。Google Cloudはお客様のデータ保全を実現するためのセキュリティサービスを提供します。 ・準拠法及び取り扱い裁判所を個別契約条件により日本とすることが可能です。 ・規制遵守状況は、次の公式サイトを御覧ください。 コンプライアンスリソースセンター https://cloud.google.com/security/compliance ・Google のお客様情報の取り扱いとデータインシデントの対応プロセスについては、以下の資料で確認できます。 Cloudデータ処理付録書 https://cloud.google.com/terms/data-processing-addendum データ インシデント対応 ホワイトペーパー https://cloud.google.com/docs/security/incident-response	
統25	-	-
統26	-	-
統27	-	-
統28	Google Cloud では、信頼は透明性から生まれると考えており、お客様と緊密に連携して、デュー デリジェンス、リスク管理、規制遵守の要件を満たせるようサポートしています。 Google は、お客様が 我々のサービスをご利用いただく前に、デューデリジェンスとリスク評価を実施する必要があることを認識しています。お客様を支援するため、Googleは、お客様が適切に外部委託先としてGoogle Cloud や Google Workspace を評価するためのリソースを提供しています。詳細については統20に記載のGoogleの対策の内容をご参照ください。 Google Cloud は、Google Cloud の運用を保護するだけでなく、Google Cloud のお客様とパートナーの信頼を維持する、堅牢なサードパーティ リスク管理プログラムの整備に尽力しています。 Google Cloud は、Google Cloud サービスに関連する特定の活動を実施するために、サードパーティ（下請け業者）を利用することがあります。これらのサードパーティは、Google Cloud のサードパーティ リスク管理（TPRM）プログラムを通じてモニタリングおよび管理されます。このプログラムは、サードパーティとの契約において Google Cloud のセキュリティ、コンプライアンス、運用効率の高い基準が維持されるように設計されています。詳しくはクラウド サードパーティ リスク管理リソース センターをご参照ください。	-
実1	-	-
実2	-	-
実3	-	-
実4	Google Cloudとお客様は、責任共有／運命共有モデルに基づき、耐量子計算機暗号（PQC）の導入において責任を共有します。 Googleはインフラストラクチャのセキュリティ確保に注力し、お客様は上位レイヤーのセキュリティ確保に責任を負います。クラウドネイティブなPQCソリューションの必要性を認識し、Google Cloudの製品チームは、データ、認証、鍵交換のセキュリティを確保するために、関連製品にPQCを導入しています。Googleが管理責任を持つインフラストラクチャおよびマネージドサービスについては、お客様によるハードウェアの交換やシステムアーキテクチャの変更は不要です。鍵と暗号化構成をご自身で管理するお客様向けには、Google Cloudが移行を円滑に進めるためのガイダンスとツールを開発しています（「運命共有」）。 Google Cloudがお客様のクラウドにおけるPQC導入をどのように支援しているかについては、こちらをご覧ください：量子耐性のある未来への準備を支援するGoogle Cloudの取り組み Google Cloudは、PQCへの移行を以下の方法で支援します。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	・他の組織の参考となるよう、PQC導入の進捗状況を定期的に公開 (PQCナレッジハブ). ・PQCへの移行を開始する組織に対し、CISOオフィスチームを通じて専門的なアドバイスを提供 (Office of the CISO). ・セキュリティ変革を支援し、PQC準備における適切な暗号化技術の使用に関する疑問に対応するため、Mandiant and Google Cloud コンサルティングを含むコンサルティングサービスを提供。	
実5	-	-
実6	-	-
実7	-	-
実8	-	-
実9	-	-
実10	-	-
実11	-	-
実12	-	-
実13	-	-
実14	Google は ISO27001 認証を受けています。この基準では、情報セキュリティインシデントに関する管理策（ISO 27001:2022、附属書 A 5.24～5.28）、「監視活動」（ISO 27001:2022、附属書 A 8.16）、「ネットワークセキュリティ」（ISO 27001:2022、附属書 A 8.20）、「ネットワークサービスのセキュリティ」ISO 27001:2022、附属書 A 8.21）が規定されています。 Google では、高度なデータ処理パイプラインを使用して、個々のデバイスでのホストベースの信号、インフラストラクチャ内のさまざまなモニタリング ポイントからのネットワーク ベースの信号、インフラストラクチャ サービスからの信号を統合しています。これらのパイプライン上に構築されたルールとマシン インテリジェンスにより、セキュリティ エンジニアは潜在的なインシデントの警告を確認できます。Google の調査およびインシデント対応チームは、これらの潜在的なインシデントを年中無休で選別、調査、対応しています。Google では、検出メカニズムと対応メカニズムの有効性を評価して改善するための Red Team 訓練を実施しています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。 Google のお客様情報の取り扱いとデータインシデントの対応プロセスについては、以下の資料で確認できます。 Cloudデータ処理付録書 https://cloud.google.com/terms/data-processing-addendum データ インシデント対応 ホワイトペーパー https://cloud.google.com/security/incident-response Google のインフラストラクチャのセキュリティ設計については、以下の資料で確認できます。 https://cloud.google.com/docs/security/infrastructure/design	-
実14-1	Google のセキュリティ モニタリング プログラムが対象としているのは、内部ネットワーク トラフィック、社員によるシステム上の操作、外部に知られている脆弱性によって集められた情報です。Google の基本原則は、セキュリティ テレメトリー データを集約して 1 か所に保存し、統一されたセキュリティ分析を行うことです。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google のグローバル ネットワークのさまざまな箇所で、内部トラフィックに疑わしい動作（たとえば、トラフィックにボットネットに接続している可能性が見られるなど）がないか検査しています。Google では、オープンソースのツールと商用ツールを組み合わせて使用し、トラフィックをキャプチャして解析することで、この分析を実行できるようにしています。Google の技術を基に構築された独自の相関システムもこの解析をサポートしています。Google では、ネットワーク解析を補足してシステムログを調べることで、顧客データへのアクセスの試行などの異常な行動を特定します。 Google のセキュリティ エンジニアは、受信したセキュリティ レポートを確認し、公開のメーリング リスト、ブログ投稿、Wiki をモニタリングします。未知の脅威が発生した可能性がある場合、自動化されたネットワーク解析とシステムログの自動解析により判別できます。自動化されたプロセスが問題を検出した場合、Google のセキュリティ スタッフにエスカレーションされます。 お客様にてGoogle Cloud でワークロードをモニタリングする方法のご参考として、以下をご覧ください。 Cloud Monitoring Security Command Center Monitoring integrity on Shielded VMs 詳細については、Googleのセキュリティに関するホワイトペーパーをご参照ください。 Google はデータ インシデントが発生した場合、速やかに遅滞なくお客様に通知します。Google のデータ インシデント対応プロセスの詳細については、データ インシデント対応に関するホワイトペーパーをご覧ください。 Google以外にお客様が利用することのできるその他のツール及び方法に加え、Google が提供するソリューションやツールを使用して、データのセキュリティを強化および監視することもできます。 ・エージェント SOC は、自律的なトリアージと調査、プロアクティブな脅威ハンティング、動的検出エンジニアリングなど、変化するセキュリティ環境にリアルタイムで適応するために、継続的なループで連携するAIエージェントの動的なシステムをオーケストレートします。 ・Google のセキュリティ プロダクトに関する情報は、こちらをご覧ください。Security Command Center は、Google Cloud の脆弱性と脅威に関する一元的なレポート サービスです。Security Command Center は、セキュリティとデータのアタックサーフェスの評価、資産のインベントリと検出機能の提供、構成ミスおよび脆弱性や脅威の特定、リスクの軽減と修復を支援することで、セキュリティ体制の強化を支援します。 ・Google Workspace では、Security center が高度なセキュリティ情報と分析の機能を提供し、ドメインに影響を与えるセキュリティ問題の可視性と制御性を高めます。Securiy center は、Google 管理コンソールの詳細設定を拡張し、セキュリティ データを表示します。	
実14-2	お客様を支援するため、サードパーティが保有するシステムの脆弱性対応の管理をお客様にて実施する際の参考として、Googleの脆弱性対応について以下の情報を提供しています。 Google の社内脆弱性管理プロセスでは、あらゆるテクノロジー スタックにわたってセキュリティ脅威を積極的にスキャンしています。このプロセスでは、商用ツール、オープンソース ツール、そして専用の社内ツールを組み合わせて使用し、品質保証プロセス、ソフトウェア セキュリティ レビュー、徹底的な自動および手動による侵入調査（大規模なレッドチーム演習を含む）、外部監査などを実施しています。 脆弱性管理組織とそのパートナーは、脆弱性の追跡とフォローアップを担当しています。セキュリティは問題が完全に解決されて初めて向上するため、自動化パイプラインは脆弱性の状態を継続的に再評価し、パッチを検証し、誤った解決策や部分的な解決策を報告します。 脆弱性管理組織は、検出能力を向上させるため、真の脅威を示すシグナルとノイズを区別する高品質な指標に重点を置いています。また、業界およびオープンソース コミュニティとの交流も促進しています。 詳細については、Google Cloudのセキュリティ ホワイトペーパーと Google Workspaceのセキュリティ ホワイトペーパーをご覧ください。 お客様は、Google の事前の承認を得ることなく、いつでも本サービスのペネトレーションテストを実施できます。 また、Google は、本サービスのペネトレーションテストを実施するために、資格を有する独立した第三者機関と契約しています。詳細はこちらをご覧ください。	-
実15	Google Cloud では、外部ネットワークからのアクセス可能な限られたアクセスポイントを提供しています。また、不要な通信ポートや通信機能は停止あるいは制限されています。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
実16	Google は ISO27001 認証を受けています。この基準では、情報セキュリティインシデントに関する管理策（ISO 27001:2022、附属書 A 5.24～5.28） 、「監視活動」（ISO 27001:2022、附属書 A 8.16）、「ネットワークセキュリティ」（ISO 27001:2022、附属書 A 8.20）、「ネットワークサービスのセキュリティ」ISO 27001:2022、附属書 A 8.21）が規定されています。 Google では、高度なデータ処理パイプラインを使用して、個々のデバイスでのホストベースの信号、インフラストラクチャ内のさまざまなモニタリング ポイントからのネットワーク ベースの信号、インフラストラクチャ サービスからの信号を統合しています。これらのパイプライン上に構築されたルールとマシン インテリジェンスにより、セキュリティ エンジニアは潜在的なインシデントの警告を確認できます。Google の調査およびインシデント対応チームは、これらの潜在的なインシデントを年中無休で選別、調査、対応しています。Google では、検出メカニズムと対応メカニズムの有効性を評価して改善するための Red Team 訓練を実施しています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。 Google のお客様情報の取り扱いとデータインシデントの対応プロセスについては、以下の資料で確認できます。 Cloudデータ処理付録書 https://cloud.google.com/terms/data-processing-addendum データ インシデント対応 ホワイトペーパー https://cloud.google.com/security/incident-response Google のインフラストラクチャのセキュリティ設計については、以下の資料で確認できます。 https://cloud.google.com/docs/security/infrastructure/design	-
実17	-	-
実18	-	-
実19	Google は ISO27001 認証を受けています。この基準では、情報セキュリティインシデントに関する管理策（ISO 27001:2022、附属書 A 5.24～5.28） 、「監視活動」（ISO 27001:2022、附属書 A 8.16）、「ネットワークセキュリティ」（ISO 27001:2022、附属書 A 8.20）、「ネットワークサービスのセキュリティ」ISO 27001:2022、附属書 A 8.21）が規定されています。 Google では、高度なデータ処理パイプラインを使用して、個々のデバイスでのホストベースの信号、インフラストラクチャ内のさまざまなモニタリング ポイントからのネットワーク ベースの信号、インフラストラクチャ サービスからの信号を統合しています。これらのパイプライン上に構築されたルールとマシン インテリジェンスにより、セキュリティ エンジニアは潜在的なインシデントの警告を確認できます。Google の調査およびインシデント対応チームは、これらの潜在的なインシデントを年中無休で選別、調査、対応しています。Google では、検出メカニズムと対応メカニズムの有効性を評価して改善するための Red Team 訓練を実施しています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。 Google のお客様情報の取り扱いとデータインシデントの対応プロセスについては、以下の資料で確認できます。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Cloudデータ処理付録書 https://cloud.google.com/terms/data-processing-addendum データ インシデント対応 ホワイトペーパー https://cloud.google.com/security/incident-response Google のインフラストラクチャのセキュリティ設計については、以下の資料で確認できます。 https://cloud.google.com/docs/security/infrastructure/design	
実20	Google は ISO27001 認証を受けています。この基準では、「マルウェアに対する保護」（附属書 A 8.7）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、さまざまなマルウェア検出手法を駆使して、コアプロダクト（Gmail、Google ドライブ、Google Chrome、YouTube、Google 広告、Google 検索など）のマルウェア対策を維持しています。マルウェアが潜むファイルを事前に検出するために、ウェブクロール、ファイル デトネーション、カスタム静的検出、動的検出、機械学習検出を使用しています。また、複数のウイルス対策エンジンも使用しています。 従業員を保護するため、Chrome Enterprise Premium の高度なセキュリティ機能と Google Chrome のセーフ ブラウジング保護強化機能を使用しています。これらの機能により、社員がウェブを閲覧する際に、フィッシング サイトやマルウェア サイトを事前に検出できます。また、Gmail セキュリティ サンドボックスなど、Google Workspace で利用可能な最も厳格なセキュリティ設定により、不審な添付ファイルを事前にスキャンします。これらの機能からのログは、次のセクションで説明するように、Google のセキュリティ モニタリング システムにフィードされます。 Google Cloud 環境では、Google Security Operations（SecOps）、Security Command Center、VirusTotal を使用して、さまざまな種類のマルウェアをモニタリングし、対応することができます。 ・Google SecOps のクラウドネイティブなセキュリティ運用プラットフォームは、セキュリティ チームがサイバーセキュリティの脅威をより適切に検出、調査、対応できるようにします。 ・Security Command Center は、セキュリティの担当者によるセキュリティに関する問題の防止、検出、対応を支援するクラウドベースのリスク管理ソリューションです。 ・VirusTotal は、ファイルと URL を分析して、ウイルス対策エンジンと Web サイト スキャナーによって検出されたウイルス、ワーム、トロイの木馬、その他の悪意のあるコンテンツを識別するオンライン サービスです。 Google の社内脆弱性管理プロセスでは、あらゆるテクノロジー スタックにわたってセキュリティ脅威を積極的にスキャンしています。このプロセスでは、商用ツール、オープンソース ツール、そして専用の社内ツールを組み合わせて使用し、品質保証プロセス、ソフトウェア セキュリティ レビュー、徹底的な自動および手動による侵入調査（大規模なレッドチーム演習を含む）、外部監査などを実施しています。 脆弱性管理組織とそのパートナーは、脆弱性の追跡とフォローアップを担当しています。セキュリティは問題が完全に解決されて初めて向上するため、自動化パイプラインは脆弱性の状態を継続的に再評価し、パッチを検証し、誤った解決策や部分的な解決策を報告します。 脆弱性管理組織は、検出能力を向上させるため、真の脅威を示すシグナルとノイズを区別する高品質な指標に重点を置いています。また、業界およびオープンソース コミュニティとの交流も促進しています。 詳細については、Google Cloudのセキュリティに関するホワイトペーパーと Google Workspaceのセキュリティに関するホワイトペーパーをご覧ください。	-
実21	Google は ISO27001 認証を受けています。この基準では、「マルウェアに対する保護」（附属書 A 8.7）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、さまざまなマルウェア検出手法を駆使して、コアプロダクト（Gmail、Google ドライブ、Google Chrome、YouTube、Google 広告、Google 検索など）のマルウェア対策を維持しています。マルウェアが潜むファイルを事前に検出するために、ウェブクロール、ファイル デトネーション、カスタム静的検出、動的検出、機械学習検出を使用しています。また、複数のウイルス対策エンジンも使用しています。 従業員を保護するため、Chrome Enterprise Premium の高度なセキュリティ機能と Google Chrome のセーフ ブラウジング保護強化機能を使用しています。これらの機能により、社員がウェブを閲覧する際に、フィッシング サイトやマルウェア サイトを事前に検出できます。また、Gmail セキュリティ サンドボックスなど、Google Workspace で利用可能な最も厳格なセキュリティ設定により、不審な添付ファイルを事前にスキャンします。これらの機能からのログは、次のセクションで説明するように、Google のセキュリティ モニタリング システムにフィードされます。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google Cloud 環境では、Google Security Operations（SecOps）、Security Command Center、VirusTotal を使用して、さまざまな種類のマルウェアをモニタリングし、対応することができます。 ・Google SecOps のクラウドネイティブなセキュリティ運用プラットフォームは、セキュリティ チームがサイバーセキュリティの脅威をより適切に検出、調査、対応できるようにします。 ・Security Command Center は、セキュリティの担当者によるセキュリティに関する問題の防止、検出、対応を支援するクラウドベースのリスク管理ソリューションです。 ・VirusTotal は、ファイルと URL を分析して、ウイルス対策エンジンと Web サイト スキャナーによって検出されたウイルス、ワーム、トロイの木馬、その他の悪意のあるコンテンツを識別するオンライン サービスです。 Google の社内脆弱性管理プロセスでは、あらゆるテクノロジー スタックにわたってセキュリティ脅威を積極的にスキャンしています。このプロセスでは、商用ツール、オープンソース ツール、そして専用の社内ツールを組み合わせて使用し、品質保証プロセス、ソフトウェア セキュリティ レビュー、徹底的な自動および手動による侵入調査（大規模なレッドチーム演習を含む）、外部監査などを実施しています。 脆弱性管理組織とそのパートナーは、脆弱性の追跡とフォローアップを担当しています。セキュリティは問題が完全に解決されて初めて向上するため、自動化パイプラインは脆弱性の状態を継続的に再評価し、パッチを検証し、誤った解決策や部分的な解決策を報告します。 脆弱性管理組織は、検出能力を向上させるため、真の脅威を示すシグナルとノイズを区別する高品質な指標に重点を置いています。また、業界およびオープンソース コミュニティとの交流も促進しています。 詳細については、Google Cloudのセキュリティに関するホワイトペーパーと Google Workspaceのセキュリティに関するホワイトペーパーをご覧ください。	
実22	Google は ISO27001 認証を受けています。この基準では、「マルウェアに対する保護」（附属書 A 8.7）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、さまざまなマルウェア検出手法を駆使して、コアプロダクト（Gmail、Google ドライブ、Google Chrome、YouTube、Google 広告、Google 検索など）のマルウェア対策を維持しています。マルウェアが潜むファイルを事前に検出するために、ウェブクロール、ファイル デトネーション、カスタム静的検出、動的検出、機械学習検出を使用しています。また、複数のウイルス対策エンジンも使用しています。 従業員を保護するため、Chrome Enterprise Premium の高度なセキュリティ機能と Google Chrome のセーフ ブラウジング保護強化機能を使用しています。これらの機能により、社員がウェブを閲覧する際に、フィッシング サイトやマルウェア サイトを事前に検出できます。また、Gmail セキュリティ サンドボックスなど、Google Workspace で利用可能な最も厳格なセキュリティ設定により、不審な添付ファイルを事前にスキャンします。これらの機能からのログは、次のセクションで説明するように、Google のセキュリティ モニタリング システムにフィードされます。 Google Cloud 環境では、Google Security Operations（SecOps）、Security Command Center、VirusTotal を使用して、さまざまな種類のマルウェアをモニタリングし、対応することができます。 ・Google SecOps のクラウドネイティブなセキュリティ運用プラットフォームは、セキュリティ チームがサイバーセキュリティの脅威をより適切に検出、調査、対応できるようにします。 ・Security Command Center は、セキュリティの担当者によるセキュリティに関する問題の防止、検出、対応を支援するクラウドベースのリスク管理ソリューションです。 ・VirusTotal は、ファイルと URL を分析して、ウイルス対策エンジンと Web サイト スキャナーによって検出されたウイルス、ワーム、トロイの木馬、その他の悪意のあるコンテンツを識別するオンライン サービスです。 Google の社内脆弱性管理プロセスでは、あらゆるテクノロジー スタックにわたってセキュリティ脅威を積極的にスキャンしています。このプロセスでは、商用ツール、オープンソース ツール、そして専用の社内ツールを組み合わせて使用し、品質保証プロセス、ソフトウェア セキュリティ レビュー、徹底的な自動および手動による侵入調査（大規模なレッドチーム演習を含む）、外部監査などを実施しています。 脆弱性管理組織とそのパートナーは、脆弱性の追跡とフォローアップを担当しています。セキュリティは問題が完全に解決されて初めて向上するため、自動化パイプラインは脆弱性の状態を継続的に再評価し、パッチを検証し、誤った解決策や部分的な解決策を報告します。 脆弱性管理組織は、検出能力を向上させるため、真の脅威を示すシグナルとノイズを区別する高品質な指標に重点を置いています。また、業界およびオープンソース コミュニティとの交流も促進しています。 詳細については、Google Cloudのセキュリティに関するホワイトペーパーと Google Workspaceのセキュリティに関するホワイトペーパーをご覧ください。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
実23	お客様を支援するため、Google はお客様及びその従業員に向けて、当社サービスの使用方法を説明したドキュメントをGoogle Cloud および Workspace についてご用意しています。 またより詳しいガイド付きトレーニングをご希望のお客様には、様々な研修コースと認定資格もご用意しています。	-
実24	-	-
実25	Google は ISO27001 認証を受けています。この基準では、論理的なアクセス制御に関する管理策（ISO 27001:2022、附属書A 5.15～5.18、8.2～8.5）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google のインフラストラクチャは、お客様のデータを他のお客様やユーザーのデータから論理的に分離するように設計されています。同じ物理サーバーに保存されている場合も同様です。顧客データへのアクセスが許可されているのは、ごく少数の Google 社員のグループのみです。アクセス権とアクセスレベルは、社員の職務と役割に基づいて付与されており、責務に対して必要なアクセス権が、最小権限および need to know（知る必要がある人にのみ知らせる）原則に則して与えられています。Google の社員には社内のリソース（社員用メールや Google 社内の社員用ポータルなど）に対する限られたデフォルトの権限しか許可されていません。追加のアクセス権を得るには、Google のセキュリティ ポリシーに従い、データまたはシステムのオーナー、マネージャー、他のエグゼクティブなどへのリクエストとその承認による正式なプロセスに従う必要があります。 承認は、すべての変更の監査記録を維持するワークフロー ツールによって管理されています。これらのツールによって、承認設定の変更と承認プロセスの両方が管理されます。これにより、承認ポリシーが一貫して適用されるようになります。社員の承認設定は、Google Cloud サービスのデータやシステムなど、リソースへのアクセスを制御するために使用されます。サポート サービスは、承認済みの顧客管理者に対してのみ提供しています。専門のセキュリティ チーム、プライバシー チーム、内部監査チームが従業員のアクセスをモニタリングして監査します。Google は、Google Cloudのアクセスの透明性を通じて監査ログを提供します。また、アクセス承認を有効にすると、Google のサポート担当者とエンジニアが、お客様のデータにアクセスするために明示的な承認を要求します。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。 お客様を支援するため、Googleはクラウドの設定誤りや不正なセキュリティ設定変更の早期発見について以下を含むソリューションを提供しています。 ・Security Command Center は、セキュリティの担当者によるセキュリティに関する問題の防止、検出、対応を支援するクラウドベースのリスク管理ソリューションです。Security Health Analytics は Security Command Center のマネージド サービスで、クラウド環境をスキャンして、攻撃を受ける可能性のある一般的な構成ミスを検出します。 ・リスク・コンプライアンス管理のコード化（RCaC）は、インフラストラクチャとポリシーを体系化し、定期的なコンプライアンス チェックを自動化します。	-
実26	-	-
実27	Google は ISO27001 認証を受けています。この基準では、論理的なアクセス制御に関する管理策（ISO 27001:2022、附属書A 5.15～5.18、8.2～8.5）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleは、当社サービスの全てのユーザーアクティビティに関して、誰がいつ、どこで、何をしたのかを可視化することがお客様にとって必要であることを認識しています。Google は、Cloud Console、暗号化、ログ記録とモニタリング、ID とアクセスの管理、セキュリティ スキャン、ファイアウォールなど、お客様がお客様のデータへのアクセスを保護および制御するために使用できるセキュリティ リソース、機能、コントロールを提供しています。 ・Identity and Access Management は、Google Cloud リソースへのアクセス権とロールを制御することで、不正アクセスを防止します。 ・Cloud Audit Logs は、お客様のセキュリティチームがGCPの監査証跡を維持し、管理アクティビティ、データアクセス及びシステムイベントに関する詳細を参照することを可能にします。 ・多要素認証（MFA）は 、ユーザー アカウントとデータを保護するための幅広い検証方法を提供します。 Googleのホワイトペーパー「Trusting your data with Google Cloud whitepaper」および「 Trusting your data with Google Workspace whitepaper 」のセクション「Safeguarding access to your data」では、Google のデータアクセス プロセスとポリシーについて説明しています。 さらに、以下のツールを使用して、Google 担当者がお客様のデータに対して実行する限定的なアクションを監視および制御することもできます。 ・アクセスの透明性は、Google 担当者がお客様のデータに対して行った操作のログを確認できる機能です。ログエントリには、影響を受けたリソース、操作の時刻、操作の理由（例：サポート リクエストに関連付けられたケース番号）、データに対して操作を行ったユーザーに関するデータ（例：Google 担当者の所在地）が含まれます。 ・Access Approvalは、Googleのサポート及びエンジニアリングチームにお客様のコンテンツへのアクセスを許可する前に、お客様による明示的な承認を義務付けることを可能とする機能です。Access Approvalは、アクセスの透明性が提供する透明性に加え、さらなる管理層を提供します。 またGoogle Workspaceについては、 ・Status Dashboard サービスのステータス情報を確認できます。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	・管理コンソールのレポート が潜在的なセキュリティリスクの調査、ユーザーのコラボレーションの測定、誰がいつサインインしたかの追跡、管理者のアクティビティの分析を含む様々な機能を提供します。 ・アクセスの透明性 で、お客様が自らのデータに関する、Googleの人員によるアクションのログを参照できます。ログエントリには、影響を受けるリソース、アクション日時、アクション理由（サポート要請に関連するケース番号等）及びデータに対してアクションをした人に関するデータ（Googleの人員の所在地等）が含まれます。	
実28	-	-
実29	-	-
実30	-	-
実31	Google はお客様及びその従業員に向けて、当社サービスの使用方法を説明したドキュメントをGoogle Cloud および Workspace についてご用意しています。 またより詳しいガイド付きトレーニングをご希望のお客様には、様々な研修コースと認定資格もご用意しています。	-
実32	実20および実21を参照のこと。	-
実33	-	-
実34	Google の社内脆弱性管理プロセスでは、あらゆるテクノロジー スタックにわたってセキュリティ脅威を積極的にスキャンしています。このプロセスでは、商用ツール、オープンソース ツール、そして専用の社内ツールを組み合わせて使用し、品質保証プロセス、ソフトウェア セキュリティ レビュー、徹底的な自動および手動による侵入調査（大規模なレッドチーム演習を含む）、外部監査などを実施しています。 脆弱性管理組織とそのパートナーは、脆弱性の追跡とフォローアップを担当しています。セキュリティは問題が完全に解決されて初めて向上するため、自動化パイプラインは脆弱性の状態を継続的に再評価し、パッチを検証し、誤った解決策や部分的な解決策を報告します。 脆弱性管理組織は、検出能力を向上させるため、真の脅威を示すシグナルとノイズを区別する高品質な指標に重点を置いています。また、業界およびオープンソース コミュニティとの交流も促進しています。 詳細については、Google Cloudのセキュリティ ホワイトペーパーと Google Workspaceのセキュリティ ホワイトペーパーをご覧ください。 Google のインシデントレスポンスチームは、高度な検出ツール、シグナル、アラートメカニズムを活用し、潜在的なインシデントを早期に検知します。 Google はデータ インシデントが発生した場合、速やかに遅滞なくお客様に通知します。Google のデータ インシデント対応プロセスの詳細については、データインシデント対応に関するホワイトペーパーをご覧ください。	-
実35	Google は ISO27001 認証を受けています。この基準では、論理的なアクセス制御に関する管理策（ISO 27001:2022、附属書A 5.15～5.18、8.2～8.5）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleは、当社サービスの全てのユーザーアクティビティに関して、誰がいつ、どこで、何をしたのかを可視化することがお客様にとって必要であることを認識しています。Google は、Cloud Console、暗号化、ログ記録とモニタリング、ID とアクセスの管理、セキュリティ スキャン、ファイアウォールなど、お客様がお客様のデータへのアクセスを保護および制御するために使用できるセキュリティ リソース、機能、コントロールを提供しています。 ・Identity and Access Management は、Google Cloud リソースへのアクセス権とロールを制御することで、不正アクセスを防止します。 ・Cloud Audit Logs は、お客様のセキュリティチームがGCPの監査証跡を維持し、管理アクティビティ、データアクセス及びシステムイベントに関する詳細を参照することを可能にします。 ・多要素認証（MFA）は 、ユーザー アカウントとデータを保護するための幅広い検証方法を提供します。 Googleのホワイトペーパー「Trusting your data with Google Cloud whitepaper」および「 Trusting your data with Google Workspace whitepaper 」のセクション「Safeguarding access to your data」では、Google のデータアクセス プロセスとポリシーについて説明しています。 さらに、以下のツールを使用して、Google 担当者がお客様のデータに対して実行する限定的なアクションを監視および制御することもできます。 ・アクセスの透明性は、Google 担当者がお客様のデータに対して行った操作のログを確認できる機能です。ログエントリには、影響を受けたリソース、操作の時刻、操作の理由（例：サポート リクエストに関連付けられたケース番号）、データに対して操作を行ったユーザーに関するデータ（例：Google 担当者の所在地）が含まれます。 ・Access Approvalは、Googleのサポート及びエンジニアリングチームにお客様のコンテンツへのアクセスを許可する前に、お客様による明示的な承認を義務付けることを可能とする機能です。Access Approvalは、アクセスの透明性が提供する透明性に加え、さらなる管理層を提供します。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	またGoogle Workspaceについては、 ・Status Dashboard サービスのステータス情報を確認できます。 ・管理コンソールのレポート が潜在的なセキュリティリスクの調査、ユーザーのコラボレーションの測定、誰がいつサインインしたかの追跡、管理者のアクティビティの分析を含む様々な機能を提供します。 ・アクセスの透明性 で、お客様が自らのデータに関する、Googleの人員によるアクションのログを参照できます。ログエントリには、影響を受けるリソース、アクション日時、アクション理由（サポート要請に関連するケース番号等）及びデータに対してアクションをした人に関するデータ（Googleの人員の所在地等）が含まれます。	
実36	Google は ISO27001 認証を受けています。この基準では、論理的なアクセス制御に関する管理策（ISO 27001:2022、附属書A 5.15～5.18、8.2～8.5）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleは、当社サービスの全てのユーザーアクティビティに関して、誰がいつ、どこで、何をしたのかを可視化することがお客様にとって必要であることを認識しています。Google は、Cloud Console、暗号化、ログ記録とモニタリング、ID とアクセスの管理、セキュリティ スキャン、ファイアウォールなど、お客様がお客様のデータへのアクセスを保護および制御するために使用できるセキュリティ リソース、機能、コントロールを提供しています。 ・Identity and Access Management は、Google Cloud リソースへのアクセス権とロールを制御することで、不正アクセスを防止します。 ・Cloud Audit Logs は、お客様のセキュリティチームがGCPの監査証跡を維持し、管理アクティビティ、データアクセス及びシステムイベントに関する詳細を参照することを可能にします。 ・多要素認証（MFA）は 、ユーザー アカウントとデータを保護するための幅広い検証方法を提供します。 Googleのホワイトペーパー「Trusting your data with Google Cloud whitepaper」および「 Trusting your data with Google Workspace whitepaper 」のセクション「Safeguarding access to your data」では、Google のデータアクセス プロセスとポリシーについて説明しています。 さらに、以下のツールを使用して、Google 担当者がお客様のデータに対して実行する限定的なアクションを監視および制御することもできます。 ・アクセスの透明性は、Google 担当者がお客様のデータに対して行った操作のログを確認できる機能です。ログエントリには、影響を受けたリソース、操作の時刻、操作の理由（例：サポート リクエストに関連付けられたケース番号）、データに対して操作を行ったユーザーに関するデータ（例：Google 担当者の所在地）が含まれます。 ・Access Approvalは、Googleのサポート及びエンジニアリングチームにお客様のコンテンツへのアクセスを許可する前に、お客様による明示的な承認を義務付けることを可能とする機能です。Access Approvalは、アクセスの透明性が提供する透明性に加え、さらなる管理層を提供します。 またGoogle Workspaceについては、 ・Status Dashboard サービスのステータス情報を確認できます。 ・管理コンソールのレポート が潜在的なセキュリティリスクの調査、ユーザーのコラボレーションの測定、誰がいつサインインしたかの追跡、管理者のアクティビティの分析を含む様々な機能を提供します。 ・アクセスの透明性 で、お客様が自らのデータに関する、Googleの人員によるアクションのログを参照できます。ログエントリには、影響を受けるリソース、アクション日時、アクション理由（サポート要請に関連するケース番号等）及びデータに対してアクションをした人に関するデータ（Googleの人員の所在地等）が含まれます。	-
実37	Google は ISO27001 認証を受けています。この基準では、論理的なアクセス制御に関する管理策（ISO 27001:2022、附属書A 5.15～5.18、8.2～8.5）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleは、当社サービスの全てのユーザーアクティビティに関して、誰がいつ、どこで、何をしたのかを可視化することがお客様にとって必要であることを認識しています。Google は、Cloud Console、暗号化、ログ記録とモニタリング、ID とアクセスの管理、セキュリティ スキャン、ファイアウォールなど、お客様がお客様のデータへのアクセスを保護および制御するために使用できるセキュリティ リソース、機能、コントロールを提供しています。 ・Identity and Access Management は、Google Cloud リソースへのアクセス権とロールを制御することで、不正アクセスを防止します。 ・Cloud Audit Logs は、お客様のセキュリティチームがGCPの監査証跡を維持し、管理アクティビティ、データアクセス及びシステムイベントに関する詳細を参照することを可能にします。 ・多要素認証（MFA）は 、ユーザー アカウントとデータを保護するための幅広い検証方法を提供します。 Googleのホワイトペーパー「Trusting your data with Google Cloud whitepaper」および「 Trusting your data with Google Workspace whitepaper 」のセクション「Safeguarding access to your data」では、Google のデータアクセス プロセスとポリシーについて説明しています。 さらに、以下のツールを使用して、Google 担当者がお客様のデータに対して実行する限定的なアクションを監視および制御することもできます。 ・アクセスの透明性は、Google 担当者がお客様のデータに対して行った操作のログを確認できる機能です。ログエントリには、影響を受けたリソース、操作の時刻、操作の理由（例：サポート リクエストに関連付けられたケース番号）、データに対して操作を行ったユーザーに関するデータ（例：Google 担当者の所在地）が含まれます。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	・Access Approvalは、Googleのサポート及びエンジニアリングチームにお客様のコンテンツへのアクセスを許可する前に、お客様による明示的な承認を義務付けることを可能とする機能です。Access Approvalは、アクセスの透明性が提供する透明性に加え、さらなる管理層を提供します。 またGoogle Workspaceについては、 ・Status Dashboard サービスのステータス情報を確認できます。 ・管理コンソールのレポート が潜在的なセキュリティリスクの調査、ユーザーのコラボレーションの測定、誰がいつサインインしたかの追跡、管理者のアクティビティの分析を含む様々な機能を提供します。 ・アクセスの透明性 で、お客様が自らのデータに関する、Googleの人員によるアクションのログを参照できます。ログエントリには、影響を受けるリソース、アクション日時、アクション理由（サポート要請に関連するケース番号等）及びデータに対してアクションをした人に関するデータ（Googleの人員の所在地等）が含まれます。	
実38	Google は ISO27001 認証を受けています。この基準では、論理的なアクセス制御に関する管理策（ISO 27001:2022、附属書A 5.15～5.18、8.2～8.5）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleは、当社サービスの全てのユーザーアクティビティに関して、誰がいつ、どこで、何をしたのかを可視化することがお客様にとって必要であることを認識しています。Google は、Cloud Console、暗号化、ログ記録とモニタリング、ID とアクセスの管理、セキュリティ スキャン、ファイアウォールなど、お客様がお客様のデータへのアクセスを保護および制御するために使用できるセキュリティ リソース、機能、コントロールを提供しています。 ・Identity and Access Management は、Google Cloud リソースへのアクセス権とロールを制御することで、不正アクセスを防止します。 ・Cloud Audit Logs は、お客様のセキュリティチームがGCPの監査証跡を維持し、管理アクティビティ、データアクセス及びシステムイベントに関する詳細を参照することを可能にします。 ・多要素認証（MFA）は 、ユーザー アカウントとデータを保護するための幅広い検証方法を提供します。 Googleのホワイトペーパー「Trusting your data with Google Cloud whitepaper」および「 Trusting your data with Google Workspace whitepaper 」のセクション「Safeguarding access to your data」では、Google のデータアクセス プロセスとポリシーについて説明しています。 さらに、以下のツールを使用して、Google 担当者がお客様のデータに対して実行する限定的なアクションを監視および制御することもできます。 ・アクセスの透明性は、Google 担当者がお客様のデータに対して行った操作のログを確認できる機能です。ログエントリには、影響を受けたリソース、操作の時刻、操作の理由（例：サポート リクエストに関連付けられたケース番号）、データに対して操作を行ったユーザーに関するデータ（例：Google 担当者の所在地）が含まれます。 ・Access Approvalは、Googleのサポート及びエンジニアリングチームにお客様のコンテンツへのアクセスを許可する前に、お客様による明示的な承認を義務付けることを可能とする機能です。Access Approvalは、アクセスの透明性が提供する透明性に加え、さらなる管理層を提供します。 またGoogle Workspaceについては、 ・Status Dashboard サービスのステータス情報を確認できます。 ・管理コンソールのレポート が潜在的なセキュリティリスクの調査、ユーザーのコラボレーションの測定、誰がいつサインインしたかの追跡、管理者のアクティビティの分析を含む様々な機能を提供します。 ・アクセスの透明性 で、お客様が自らのデータに関する、Googleの人員によるアクションのログを参照できます。ログエントリには、影響を受けるリソース、アクション日時、アクション理由（サポート要請に関連するケース番号等）及びデータに対してアクションをした人に関するデータ（Googleの人員の所在地等）が含まれます。	-
実39	Google Cloudでは、お客様はバックアップの管理にGoogle Cloud バックアップと障害復旧（DR）サービス を活用することができます。データのバックアップに活用できるサービスについての詳細は、障害復旧の構成要素および データの障害復旧シナリオ をご参照ください。 Google Workspaceでは、お客様はデータ エクスポートを使用して組織全体のデータをエクスポートできます。Google は、API や BigQuery、パートナー ソリューションのAfi や SpinOne など、組織の Google Workspace データを操作および抽出するためのツールも多数提供しています。その他のサードパーティおよびパートナーのオプションについては、Google Cloud Partnerのディレクトリをご覧ください。	-
実40	-	-
実41	-	-
実42	Google は ISO27001 認証を受けています。この基準では、論理的なアクセス制御に関する管理策（ISO 27001:2022、附属書A 5.15～5.18、8.2～8.5）および「ネットワークセキュリティ」（ISO 27001:2022、附属書 A 8.20）が規定されています。 ネットワーク構成や管理はじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。	Internal Data Access Processes and Policies – Access Policy, Appendix 2 (Security Measures) (Cloudデータ処理付録書)

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google の社内データアクセスプロセスおよびポリシーは、顧客データの処理に使用されるシステムへの不正なアクセスを防止するために設計されています。Google は、(i) 許可された人物のみがアクセスを許可されたデータにアクセスできるようにし、(ii) 処理中、使用中、および記録後に顧客データが不正に読み取り、コピー、変更、または削除されないようシステムを設計しています。これらのシステムは、不適切なアクセスを検出するように設計されています。Google は、本番環境サーバーへの担当者のアクセスを制御するために集中アクセス管理システムを導入し、限られた数の承認された担当者のみにアクセスを許可しています。Google の認証および認可システムは、SSH 証明書とセキュリティキーを利用し、Google に安全で柔軟なアクセスメカニズムを提供するように設計されています。これらのメカニズムは、サイトホスト、ログ、データ、および設定情報への承認されたアクセス権のみを付与するように設計されています。Google は、アカウントの不正使用の可能性を最小限に抑えるため、固有のユーザー ID、強力なパスワード、二要素認証、および厳密に監視されたアクセスリストの使用を義務付けています。アクセス権の付与または変更は、承認された担当者の職務責任、承認されたタスクを実行するために必要な職務要件、および必要に応じた情報提供に基づいて行われます。アクセス権の付与または変更は、Google の社内データアクセスポリシーとトレーニングに準拠する必要があります。承認は、すべての変更の監査記録を保持するワークフローツールによって管理されます。システムへのアクセスはログに記録され、アカウンタビリティのための監査証跡が作成されます。認証にパスワードを使用する場合（ワークステーションへのログインなど）、少なくとも業界標準の慣行に準拠したパスワードポリシーが実装されます。これらの標準には、パスワードの再利用の制限と十分なパスワード強度が含まれます。	
実43	-	-
実44	-	-
実45	-	-
実46	-	-
実47	-	-
実48	Google は ISO27001 認証を受けています。この基準では、「情報及びその他の関連資産の目録」（附属書 A 5.9）、「情報及びその他の関連資産の許容される利用」（附属書 A 5.10）、「資産の返却」（附属書 A 5.11）、「装置の設置及び保護」（ISO 27001:2022、附属書 A 7.8）、「構外にある資産のセキュリティ」（ISO 27001:2022、附属書 A 7.9）、「記憶媒体」（ISO 27001:2022、附属書 A 7.10）、「装置の保守 」（ISO 27001:2022、附属書 A 7.13）、「装置のセキュリティを保った処分または再利用 」（ISO 27001:2022、附属書 A 7.14）、および「運用システムへのソフトウェアの導入 」（ISO 27001:2022、附属書 A 8.19）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	-
実49	Google は ISO27001 認証を受けています。この基準では、物理的および環境的セキュリティに関する管理策（ISO27001:2022、附属書 A 7.1～7.14）が規定されています。 Google の主な設計基準の一つとして、セキュリティとデータ保護の重視があります。Google データセンターの物理的セキュリティは、階層化されたセキュリティ モデルです。物理的な安全対策として、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を実施しています。また、侵入者の検知と追跡のために、レーザー光線侵入検知や高解像度の terior 内外監視カメラによる 24 時間 365 日のモニタリングなどのセキュリティ対策を採用しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。厳格な身元調査に合格し、訓練を受けた経験豊かな警備員が、データセンターを定期的に巡回しています。 データセンターのフロアに近くなるほど、セキュリティ対策も厳重になります。データセンターのフロアに入るには、セキュリティ通路を通らなければなりません。この通路では、セキュリティバッジや生体認証による多元的出入管理が行われています。特定の役割を持つ承認された社員しか立ち入りは許可されていません。Google のデータセンターにアクセスできる Google 社員はごく少数です。 Google のデータセンター内では、物理論理空間でセキュリティ管理を採用しています。これは、「ラック内のマシンからマシンのランタイム環境までの一定の距離」として定義されます。これらの制御には、ハードウェアの強化、タスクベースのアクセス制御、異常イベントの検出、システムの自己防衛が含まれます。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー：最先端のデータセンター https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google セキュリティ ホワイトペーパー：Google がデータセンターの物理論理空間を保護する仕組み	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	https://cloud.google.com/docs/security/physical-to-logical-space Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	
実50	Google は ISO27001 認証を受けています。この基準では、物理的および環境的セキュリティに関する管理策（ISO27001:2022、附属書 A 7.1～7.14）が規定されています。 Google の主な設計基準の一つとして、セキュリティとデータ保護の重視があります。Google データセンターの物理的セキュリティは、階層化されたセキュリティ モデルです。物理的な安全対策として、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を実施しています。また、侵入者の検知と追跡のために、レーザー光線侵入検知や高解像度の terior 内外監視カメラによる 24 時間 365 日のモニタリングなどのセキュリティ対策を採用しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。厳格な身元調査に合格し、訓練を受けた経験豊かな警備員が、データセンターを定期的に巡回しています。データセンターのフロアに近くなるほど、セキュリティ対策も厳重になります。データセンターのフロアに入るには、セキュリティ通路を通らなければなりません。この通路では、セキュリティバッジや生体認証による多元的出入管理が行われています。特定の役割を持つ承認された社員しか立ち入りは許可されていません。Google のデータセンターにアクセスできる Google 社員はごく少数です。 Google のデータセンター内では、物理論理空間でセキュリティ管理を採用しています。これは、「ラック内のマシンからマシンのランタイム環境までの一定の距離」として定義されます。これらの制御には、ハードウェアの強化、タスクベースのアクセス制御、異常イベントの検出、システムの自己防衛が含まれます。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー：最先端のデータセンター https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google セキュリティ ホワイトペーパー：Google がデータセンターの物理論理空間を保護する仕組み https://cloud.google.com/docs/security/physical-to-logical-space Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
実51	Google は ISO27001 認証を受けています。この基準では、物理的および環境的セキュリティに関する管理策（ISO27001:2022、附属書 A 7.1～7.14）が規定されています。 Google の主な設計基準の一つとして、セキュリティとデータ保護の重視があります。Google データセンターの物理的セキュリティは、階層化されたセキュリティ モデルです。物理的な安全対策として、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を実施しています。また、侵入者の検知と追跡のために、レーザー光線侵入検知や高解像度の terior 内外監視カメラによる 24 時間 365 日のモニタリングなどのセキュリティ対策を採用しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。厳格な身元調査に合格し、訓練を受けた経験豊かな警備員が、データセンターを定期的に巡回しています。データセンターのフロアに近くなるほど、セキュリティ対策も厳重になります。データセンターのフロアに入るには、セキュリティ通路を通らなければなりません。この通路では、セキュリティバッジや生体認証による多元的出入管理が行われています。特定の役割を持つ承認された社員しか立ち入りは許可されていません。Google のデータセンターにアクセスできる Google 社員はごく少数です。 Google のデータセンター内では、物理論理空間でセキュリティ管理を採用しています。これは、「ラック内のマシンからマシンのランタイム環境までの一定の距離」として定義されます。これらの制御には、ハードウェアの強化、タスクベースのアクセス制御、異常イベントの検出、システムの自己防衛が含まれます。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー：最先端のデータセンター https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google セキュリティ ホワイトペーパー：Google がデータセンターの物理論理空間を保護する仕組み https://cloud.google.com/docs/security/physical-to-logical-space Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	
実52	Google は ISO27001 認証を受けています。この基準では、「装置の保守」（ISO27001:2022、附属書 A 7.13）が規定されています。	-
実53	Google は ISO27001 認証を受けています。この基準では、物理的および環境的セキュリティに関する管理策（ISO27001:2022、附属書 A 7.1～7.14）が規定されています。 Google の主な設計基準の一つとして、セキュリティとデータ保護の重視があります。Google データセンターの物理的セキュリティは、階層化されたセキュリティ モデルです。物理的な安全対策として、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を実施しています。また、侵入者の検知と追跡のために、レーザー光線侵入検知や高解像度の terior 内外監視カメラによる 24 時間 365 日のモニタリングなどのセキュリティ対策を採用しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。厳格な身元調査に合格し、訓練を受けた経験豊かな警備員が、データセンターを定期的に巡回しています。データセンターのフロアに近くなるほど、セキュリティ対策も厳重になります。データセンターのフロアに入るには、セキュリティ通路を通らなければなりません。この通路では、セキュリティバッジや生体認証による多元的出入管理が行われています。特定の役割を持つ承認された社員しか立ち入りは許可されていません。Google のデータセンターにアクセスできる Google 社員はごく少数です。 Google のデータセンター内では、物理論理空間でセキュリティ管理を採用しています。これは、「ラック内のマシンからマシンのランタイム環境までの一定の距離」として定義されます。これらの制御には、ハードウェアの強化、タスクベースのアクセス制御、異常イベントの検出、システムの自己防衛が含まれます。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー：最先端のデータセンター https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google セキュリティ ホワイトペーパー：Google がデータセンターの物理論理空間を保護する仕組み https://cloud.google.com/docs/security/physical-to-logical-space Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
実54	Google は ISO27001 認証を受けています。この基準では、「装置の保守」（ISO27001:2022、附属書 A 7.13）が規定されています。システムの管理方法について、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。	-
実55	Google は ISO27001 認証を受けています。この基準では、「容量・能力の管理」（ISO27001:2022、附属書 A 8.6）が規定されています。Google は、世界中で容量をモニタリングし、必要に応じて調整する強固なネットワークを確立しています。	-
実56	Google は ISO27001 認証を受けています。この基準では、物理的および環境的セキュリティに関する管理策（ISO27001:2022、附属書 A 7.1～7.14）が規定されています。 Google の主な設計基準の一つとして、セキュリティとデータ保護の重視があります。Google データセンターの物理的セキュリティは、階層化されたセキュリティ モデルです。物理的な安全対策として、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を実施しています。また、侵入者の検知と追跡のために、レーザー光線侵入検知や高解像度の terior 内外監視カメラによる 24 時間 365 日のモニタリングなどのセキュリティ対策を採用しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。厳格な身元調査に合格し、訓練を受けた経験豊かな警備員が、データセンターを定期的に巡回しています。データセンターのフロアに近くなるほど、セキュリティ対策も厳重になります。データセンターのフロアに入るには、セキュリティ通路を通らなければなりません。この通路では、セキュリティ	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	バッジや生体認証による多元的出入管理が行われています。特定の役割を持つ承認された社員しか立ち入りは許可されていません。Google のデータセンターにアクセスできる Google 社員はごく少数です。 Google のデータセンター内では、物理論理空間でセキュリティ管理を採用しています。これは、「ラック内のマシンからマシンのランタイム環境までの一定の距離」として定義されます。これらの制御には、ハードウェアの強化、タスクベースのアクセス制御、異常イベントの検出、システムの自己防衛が含まれます。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー：最先端のデータセンター https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google セキュリティ ホワイトペーパー：Google がデータセンターの物理論理空間を保護する仕組み https://cloud.google.com/docs/security/physical-to-logical-space Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	
実57	Google は ISO27001 認証を受けています。この基準では、物理的および環境的セキュリティに関する管理策（ISO27001:2022、附属書 A 7.1～7.14）が規定されています。 Google の主な設計基準の一つとして、セキュリティとデータ保護の重視があります。Google データセンターの物理的セキュリティは、階層化されたセキュリティ モデルです。物理的な安全対策として、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を実施しています。また、侵入者の検知と追跡のために、レーザー光線侵入検知や高解像度の terior 内外監視カメラによる 24 時間 365 日のモニタリングなどのセキュリティ対策を採用しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。厳格な身元調査に合格し、訓練を受けた経験豊かな警備員が、データセンターを定期的に巡回しています。データセンターのフロアに近くなるほど、セキュリティ対策も厳重になります。データセンターのフロアに入るには、セキュリティ通路を通らなければなりません。この通路では、セキュリティバッジや生体認証による多元的出入管理が行われています。特定の役割を持つ承認された社員しか立ち入りは許可されていません。Google のデータセンターにアクセスできる Google 社員はごく少数です。 Google のデータセンター内では、物理論理空間でセキュリティ管理を採用しています。これは、「ラック内のマシンからマシンのランタイム環境までの一定の距離」として定義されます。これらの制御には、ハードウェアの強化、タスクベースのアクセス制御、異常イベントの検出、システムの自己防衛が含まれます。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー：最先端のデータセンター https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google セキュリティ ホワイトペーパー：Google がデータセンターの物理論理空間を保護する仕組み https://cloud.google.com/docs/security/physical-to-logical-space Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
実58	Google は ISO27001 認証を受けています。この基準では、物理的および環境的セキュリティに関する管理策（ISO27001:2022、附属書 A 7.1～7.14）が規定されています。 Google の主な設計基準の一つとして、セキュリティとデータ保護の重視があります。Google データセンターの物理的セキュリティは、階層化されたセキュリティ モデルです。物理的な安全対策として、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を実施しています。また、侵入者の検知と追跡のために、レーザー光線侵入検知や高解像度の terior 内外監視カメラによる 24 時間 365 日のモニタリングなどのセキュリティ対策を採用しています。インシデントが発生した	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。厳格な身元調査に合格し、訓練を受けた経験豊かな警備員が、データセンターを定期的に巡回しています。 データセンターのフロアに近くなるほど、セキュリティ対策も厳重になります。データセンターのフロアに入るには、セキュリティ通路を通らなければなりません。この通路では、セキュリティバッジや生体認証による多元的出入管理が行われています。特定の役割を持つ承認された社員しか立ち入りは許可されていません。Google のデータセンターにアクセスできる Google 社員はごく少数です。 Google のデータセンター内では、物理論理空間でセキュリティ管理を採用しています。これは、「ラック内のマシンからマシンのランタイム環境までの一定の距離」として定義されます。これらの制御には、ハードウェアの強化、タスクベースのアクセス制御、異常イベントの検出、システムの自己防衛が含まれます。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー：最先端のデータセンター https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google セキュリティ ホワイトペーパー：Google がデータセンターの物理論理空間を保護する仕組み https://cloud.google.com/docs/security/physical-to-logical-space Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	
実59	Google は ISO27001 認証を受けています。この基準では、物理的および環境的セキュリティに関する管理策（ISO27001:2022、附属書 A 7.1～7.14）が規定されています。 Google の主な設計基準の一つとして、セキュリティとデータ保護の重視があります。Google データセンターの物理的セキュリティは、階層化されたセキュリティ モデルです。物理的な安全対策として、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を実施しています。また、侵入者の検知と追跡のために、レーザー光線侵入検知や高解像度の terior 内外監視カメラによる 24 時間 365 日のモニタリングなどのセキュリティ対策を採用しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。厳格な身元調査に合格し、訓練を受けた経験豊かな警備員が、データセンターを定期的に巡回しています。 データセンターのフロアに近くなるほど、セキュリティ対策も厳重になります。データセンターのフロアに入るには、セキュリティ通路を通らなければなりません。この通路では、セキュリティバッジや生体認証による多元的出入管理が行われています。特定の役割を持つ承認された社員しか立ち入りは許可されていません。Google のデータセンターにアクセスできる Google 社員はごく少数です。 Google のデータセンター内では、物理論理空間でセキュリティ管理を採用しています。これは、「ラック内のマシンからマシンのランタイム環境までの一定の距離」として定義されます。これらの制御には、ハードウェアの強化、タスクベースのアクセス制御、異常イベントの検出、システムの自己防衛が含まれます。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー：最先端のデータセンター https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google セキュリティ ホワイトペーパー：Google がデータセンターの物理論理空間を保護する仕組み https://cloud.google.com/docs/security/physical-to-logical-space Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	-
実60	Google は ISO27001 認証を受けています。この基準では、物理的および環境的セキュリティに関する管理策（ISO27001:2022、附属書 A 7.1～7.14）が規定されています。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google の主な設計基準の一つとして、セキュリティとデータ保護の重視があります。Google データセンターの物理的セキュリティは、階層化されたセキュリティ モデルです。物理的な安全対策として、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を実施しています。また、侵入者の検知と追跡のために、レーザー光線侵入検知や高解像度の terior 内外監視カメラによる 24 時間 365 日のモニタリングなどのセキュリティ対策を採用しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。厳格な身元調査に合格し、訓練を受けた経験豊かな警備員が、データセンターを定期的に巡回しています。 データセンターのフロアに近くなるほど、セキュリティ対策も厳重になります。データセンターのフロアに入るには、セキュリティ通路を通らなければなりません。この通路では、セキュリティバッジや生体認証による多元的出入管理が行われています。特定の役割を持つ承認された社員しか立ち入りは許可されていません。Google のデータセンターにアクセスできる Google 社員はごく少数です。 Google のデータセンター内では、物理論理空間でセキュリティ管理を採用しています。これは、「ラック内のマシンからマシンのランタイム環境までの一定の距離」として定義されます。これらの制御には、ハードウェアの強化、タスクベースのアクセス制御、異常イベントの検出、システムの自己防衛が含まれます。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー：最先端のデータセンター https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google セキュリティ ホワイトペーパー：Google がデータセンターの物理論理空間を保護する仕組み https://cloud.google.com/docs/security/physical-to-logical-space Google Workspaceセキュリティホワイトペーパー https://workspace.google.com/learn-more/security/security-whitepaper/page-1/ Google Data Center Security: 6 Layers Deep https://www.youtube.com/watch?v=kd33UVZhnAA	
実61	-	-
実62	-	-
実63	-	-
実64	-	-
実65	-	-
実66	-	-
実67	-	-
実68	-	-
実69	お客様情報の保護に関するサービスは、以下の資料で確認できます。 機密データの保護 (Sensitive Data Protection, 旧 Cloud Data Loss Prevention) https://cloud.google.com/dlp/docs	-
実70	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。 Google は、お客様による本サービスのご利用を効果的に管理するためには、本サービスに関する十分な情報を定期的に入手する必要があることを認識しています。Google は、お客様が本サービスを継続的に効果的に監視できるよう、さまざまな仕組みを提供しています。 Google は、お客様に提供される SLA に従って Google が本サービスを遂行する能力に重大な影響を与える事態の発生について、情報を提供します。 お客様は、本サービスの機能を使用して、Google による本サービスのパフォーマンス（SLA を含む）を継続的に監視できます。 例: Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。 インシデントが検出されると、Google Cloud Service Health チームがインシデントについて迅速に通知し、インシデントが継続している間、定期的に更新情報を提供します。インシデントを完全に把握し、信頼性の改善へ向けて Google がすべきことを明らかにするため、すべてのインシデントが社内で事後分析されます。事後分析によって特定された改善策が追跡および実装されます。広範囲にわたり深刻な影響を与えるインシデントの場合、Google は、その症状、影響、根本原因、是正措置、今後のインシデント防止策をまとめたインシデント報告書をリリースします。事後検証と同様、問題から学び、信頼性を改善するために講じる措置に特に注意を払っています。Google が事後検証報告書を作成して公開する目的は、透明性を確保し、お客様に安定したプロダクトを提供するという Google の取り組みを示すことにあります。 インシデントのコミュニケーションと対応の詳細については、以下のホワイトペーパーをご参照下さい。 Google Cloud インシデントのコミュニケーション https://docs.cloud.google.com/service-health/docs/incident-communication インシデントのライフサイクル https://docs.cloud.google.com/service-health/docs/incident-lifecycle	
実71	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。 Google は、お客様による本サービスのご利用を効果的に管理するためには、本サービスに関する十分な情報を定期的に入手する必要があることを認識しています。Google は、お客様が本サービスを継続的に効果的に監視できるよう、さまざまな仕組みを提供しています。 Google は、お客様に提供される SLA に従って Google が本サービスを遂行する能力に重大な影響を与える事態の発生について、情報を提供します。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	お客様は、本サービスの機能を使用して、Google による本サービスのパフォーマンス（SLA を含む）を継続的に監視できます。 例: Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。 インシデントが検出されると、Google Cloud Service Health チームがインシデントについて迅速に通知し、インシデントが継続している間、定期的に更新情報を提供します。インシデントを完全に把握し、信頼性の改善へ向けて Google がすべきことを明らかにするため、すべてのインシデントが社内で事後分析されます。事後分析によって特定された改善策が追跡および実装されます。広範囲にわたり深刻な影響を与えるインシデントの場合、Google は、その症状、影響、根本原因、是正措置、今後のインシデント防止策をまとめたインシデント報告書をリリースします。事後検証と同様、問題から学び、信頼性を改善するために講じる措置に特に注意を払っています。Google が事後検証報告書を作成して公開する目的は、透明性を確保し、お客様に安定したプロダクトを提供するという Google の取り組みを示すことにあります。 インシデントのコミュニケーションと対応の詳細については、以下のホワイトペーパーをご参照下さい。 Google Cloud インシデントのコミュニケーション https://docs.cloud.google.com/service-health/docs/incident-communication インシデントのライフサイクル https://docs.cloud.google.com/service-health/docs/incident-lifecycle	
実72	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。 Google は、お客様による本サービスのご利用を効果的に管理するためには、本サービスに関する十分な情報を定期的に入手する必要があることを認識しています。Google は、お客様が本サービスを継続的に効果的に監視できるよう、さまざまな仕組みを提供しています。 Google は、お客様に提供される SLA に従って Google が本サービスを遂行する能力に重大な影響を与える事態の発生について、情報を提供します。 お客様は、本サービスの機能を使用して、Google による本サービスのパフォーマンス（SLA を含む）を継続的に監視できます。 例: Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。 インシデントが検出されると、Google Cloud Service Health チームがインシデントについて迅速に通知し、インシデントが継続している間、定期的に更新情報を提供します。インシデントを完全に把握し、信頼性の改善へ向けて Google がすべきことを明らかにするため、すべてのインシデントが社内で事後分析されます。事後分析によって特定された改善策が追跡および実装されます。広範囲にわたり深刻な影響を与えるインシデントの場合、Google は、その症状、影響、根本原因、是正措置、今後のインシデント防止策をまとめたインシデント報告書をリリースします。事後検証と同様、問題から学び、信頼性を改善するために講じる措置に特に注意を払っています。Google が事後検証報告書を作成して公開する目的は、透明性を確保し、お客様に安定したプロダクトを提供するという Google の取り組みを示すことにあります。 インシデントのコミュニケーションと対応の詳細については、以下のホワイトペーパーをご参照下さい。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google Cloud インシデントのコミュニケーション https://docs.cloud.google.com/service-health/docs/incident-communication インシデントのライフサイクル https://docs.cloud.google.com/service-health/docs/incident-lifecycle	
実73	Google は、お客様による本サービスのご利用を効果的に管理するためには、本サービスに関する十分な情報を定期的に入手する必要があることを認識しています。Google は、お客様が本サービスを継続的に効果的に監視できるよう、さまざまな仕組みを提供しています。 Google は、お客様に提供される SLA に従って Google が本サービスを遂行する能力に重大な影響を与える事態の発生について、情報を提供します。 お客様は、本サービスの機能を使用して、Google による本サービスのパフォーマンス（SLA を含む）を継続的に監視できます。 例: Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。 さらに、Google はデータ インシデントが発生した場合、速やかに遅滞なくお客様に通知します。Google のデータ インシデント対応プロセスの詳細については、データ インシデント対応に関するホワイトペーパーをご覧ください。	-
実73-1	Google は、お客様による本サービスのご利用を効果的に管理するためには、本サービスに関する十分な情報を定期的に入手する必要があることを認識しています。Google は、お客様が本サービスを継続的に効果的に監視できるよう、さまざまな仕組みを提供しています。 Google は、お客様に提供される SLA に従って Google が本サービスを遂行する能力に重大な影響を与える事態の発生について、情報を提供します。 お客様は、本サービスの機能を使用して、Google による本サービスのパフォーマンス（SLA を含む）を継続的に監視できます。 例: Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。 さらに、Google はデータ インシデントが発生した場合、速やかに遅滞なくお客様に通知します。Google のデータ インシデント対応プロセスの詳細については、データ インシデント対応に関するホワイトペーパーをご覧ください。	-
実74	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	-
実75	Google は、お客様を支援するために、セキュリティ・バイ・デザインおよびセキュリティ・バイ・デフォルトのインフラストラクチャ プラットフォームを提供しています。詳細は、以下のホワイトペーパーをご覧ください。 Google セキュリティの概要:	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	https://cloud.google.com/docs/security/overview/whitepaper An Overview of Google's Commitment to Secure by Design: https://publicpolicy.google/resources/google_commitment_secure_by_design_overview.pdf	
実76	-	-
実77	-	-
実78	-	-
実79	-	-
実80	-	-
実81	-	-
実82	Googleは、お客様がデータへのアクセス、修正、処理の制限、ならびにデータの取得または削除を実施できる機能を提供しています。 契約関係を解除する際、Googleは、当社のシステムからお客様データを削除する旨のお客様の指示を遵守します。削除に関する詳細は、ホワイトペーパー「Google Cloud でのデータの削除」をご覧ください。	-
実83	-	-
実84	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	-
実85	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
実86	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	-
実87	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	-
実88	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	-
実89	Google は、お客様を支援するために、セキュリティ・バイ・デザインのインフラストラクチャ プラットフォームを提供しています。詳細は、以下のホワイトペーパーをご覧ください。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Google セキュリティの概要: https://cloud.google.com/docs/security/overview/whitepaper An Overview of Google's Commitment to Secure by Design: https://publicpolicy.google/resources/google_commitment_secure_by_design_overview.pdf	
実90	-	-
実91	-	-
実92	-	-
実93	-	-
実94	-	-
実95	-	-
実96	-	-
実97	-	-
実98	-	-
実99	-	-
実100	-	-
実101	-	-
実102	Google は ISO27001 認証を受けています。この基準では、「ログ取得」（ISO 27001:2022、附属書 A 8.15）、「監視活動」（ISO 27001:2022、附属書 A 8.16）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud は、内部モニタリングと合成モニタリングを使用してインシデントを検出します。詳しくは、Google の書籍『Site Reliability Engineering』の第 6 章をご覧ください。 お客様は、本サービスの機能を使用して、Googleによる本サービス（SLAを含む）のパフォーマンスを継続的に監視することができます。 例えば、以下の機能があります。 ・Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。 ・Personalized Service Health は、プロジェクトに関連する中断を伴うイベントをフィルタリングし、影響の評価、ビジネス継続性の維持、更新の追跡に役立つ情報を提供します。 Personalized Service Health は、Service Health ダッシュボード、構成可能なアラート、Cloud Logging によるエクスポート可能なログなど、あらゆるアラート、インシデント対応、モニタリング ワークフローに組み込むことができます。 ・Google Cloud のオブザーバビリティは、Google Cloud 上などで実行されているアプリケーションとシステム向けの統合モニタリング、ロギング、トレース マネージド サービスです。	-
実103	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。 Google は、お客様による本サービスのご利用を効果的に管理するためには、本サービスに関する十分な情報を定期的に入手する必要があることを認識しています。Google は、お客様が本サービスを継続的に効果的に監視できるよう、さまざまな仕組みを提供しています。 Google は、お客様に提供される SLA に従って Google が本サービスを遂行する能力に重大な影響を与える事態の発生について、情報を提供します。 お客様は、本サービスの機能を使用して、Google による本サービスのパフォーマンス（SLA を含む）を継続的に監視できます。 例: Google Cloud Service Healthダッシュボードと Google Workspace ステータス ダッシュボードは、本サービスのステータス情報を提供します。 インシデントが検出されると、Google Cloud Service Health チームがインシデントについて迅速に通知し、インシデントが継続している間、定期的に更新情報を提供します。インシデントを完全に把握し、信頼性の改善へ向けて Google がすべきことを明らかにするため、すべてのインシデントが社内で事後分析されます。事後分析によって特定された改善策が追跡および実装されます。広範囲にわたり深刻な影響を与えるインシデントの場合、Google は、その症状、影響、根本原因、是正措置、今後のインシデント防止策をまとめたインシデント報告書をリリースします。事後検証と同様、問題から学び、信頼性を改善するために講じる措置に特に注意を払っています。Google が事後検証報告書を作成して公開する目的は、透明性を確保し、お客様に安定したプロダクトを提供するという Google の取り組みを示すことにあります。 インシデントのコミュニケーションと対応の詳細については、以下のホワイトペーパーをご参照下さい。 Google Cloud インシデントのコミュニケーション https://docs.cloud.google.com/service-health/docs/incident-communication インシデントのライフサイクル https://docs.cloud.google.com/service-health/docs/incident-lifecycle	
実103-1	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	-
実104	Google は ISO27001 認証を受けています。この基準では、「情報のバックアップ」（ISO27001:2022、附属書 A 8.13）と「情報処理施設・設備の冗長性」（ISO27001:2022、附属書 A 8.14）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	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。この冗長性は、Google のサーバーの設計、データの保存方法、ネットワークとインターネットの接続、さらにソフトウェア サービス自体に適用されます。この「すべての冗長性」には、例外処理が含まれ、単一のサーバー、データセンター、ネットワーク接続に依存しないソリューションが作成されます。 Google のデータセンターは地理的に分散されているため、ある地域で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できなくなっても、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。 冗長性の高いインフラストラクチャにより、データ損失を防ぐことができます。 Google Cloud リソースを複数の地域とゾーンで作成してデプロイし、復元性に優れた高可用性システムを構築できます。Google のシステムは、プラットフォームのサービス メンテナンスやアップグレードを行う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。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	
実105	-	-
実106	-	-
実107	-	-
実108	-	-
実109	-	-
実110	-	-
実111	-	-
実112	-	-
実113	-	-
実114	-	-
実115	-	-
実116	-	-
実117	-	-
実118	-	-
実119	-	-
実120	-	-
実121	-	-
実122	-	-
実123	-	-
実124	-	-
実125	-	-
実126	-	-
実132	-	-
実133	-	-
実134	-	-
実135	-	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
実136	-	-
実137	-	-
実138	-	-
実139	-	-
実140	-	-
実141	-	-
実142	-	-
実143	-	-
実144	-	-
実145	-	-
実146	-	-
実147	-	-
実148	-	-
実149	-	-
実150	Google の AI 開発および活用におけるアプローチは、その創業時のミッションに根ざしており、2019年より毎年公開されている「AI 原則」に沿って推進されています。この原則は、明確なユースケースの適用境界を定義し、安全性、公平性、プライバシー、および説明責任（アカウンタビリティ）を最優先事項として掲げています。 厳格なコンプライアンスを実証するため、Google Cloud Platform、Google Workspace、および Gemini は、人工知能マネジメントシステム（AIMS）の国際標準規格である「ISO/IEC 42001:2023」の認証を取得しています。 Google の AI 準備態勢（レディネス）およびプロセスは、独立した第三者評価機関である Coalfire 社によって、NIST の「AI リスクマネジメントフレームワーク（AI RMF）」および「ISO/IEC 42001」に照らして検証されており、企業のエンタープライズ・リスクガバナンスに対応可能な「成熟（Mature）」した態勢であることが確認されています。 社内において Google は、Google DeepMind の「モデル提供開始前レビュー（Model Launch Review）」、一元化された専門家によるリスクレビュー、および「AGI フォーラム」を含む専門のフォーラムを通じて、多層的な監視・統制（オーバーサイト）を徹底しています。 お客様向けには、Google Cloud は「Secure AI Framework（SAIF）」を提供しています。これは、従来の主要なセキュリティ手法（多層防御、セキュアバイデザインなど）を AI ワークロードに適応させたもので、インタラクティブなリスク自己アセスメントやエージェントリスクマップを提供します。また、Google は業界のパートナー企業とともに「Coalition for Secure AI（CoSAI）」を共同設立し、エコシステム全体におけるセキュリティ対策の標準化に取り組んでいます。 詳細については、以下のドキュメントをご参照ください。 AI Principles - Google AI: https://ai.google/principles/ Google Cloud - Delivering trusted and secure AI: https://services.google.com/fh/files/misc/ociso-ai-trust-paper-v2.pdf ISO/IEC 42001 - Compliance | Google Cloud: https://cloud.google.com/security/compliance/iso-42001 Coalfire evaluates Google Cloud AI: ‘Mature,’ ready for governance, compliance: https://cloud.google.com/blog/products/identity-security/coalfire-evaluates-google-cloud-ai-mature-ready-for-governance-compliance?e=48754805 Responsible AI Progress Report (Published in February 2026): https://ai.google/static/documents/ai-responsibility-update-2026.pdf SAIF Risk Self-Assessment: https://saif.google/risk-self-assessment	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
実151	Google Cloud は、AI システムの事実としての正確性、監査可能性、および運用の透明性を確保するための包括的な機能とツールを提供しています。 ・事実の正確性を担保するグラウンディング（Grounding for Factual Accuracy）：Google Cloud は、「Google 検索によるグラウンディング（Grounding with Google Search）」、「Web Grounding for Enterprise（エンタープライズ向けウェブ グラウンディング）」、および「Grounding with Google Maps（Google マップによるグラウンディング）」を含む高度なグラウンディング機能を提供しています。これらは、プロンプトを検証済みの企業データやリアルタイムのウェブインデックスと相互参照させることで、ハルシネーション（事実に基づかない回答の生成）を最小限に抑え、モデルの回答の信頼性を向上させます。 ・Vertex AI のガバナンスとモニタリング（Vertex AI Governance & Monitoring）：Google は、「Vertex Explainable AI」（予測結果の解釈）、「モデル評価（Model Evaluation）」（BLEU などの定量的評価指標や公平性・バイアス測定指標）、「モデルモニタリング（Model Monitoring）」（本番環境におけるドリフトやパフォーマンスの乖離の検出）、「モデルレジストリ（Model Registry）」などのネイティブツールを統合しています。 ・Model Armor：LLM のプロンプトとレスポンスをリアルタイムでスクリーニングし、プロンプトインジェクション、ジェイルブレイク（脱獄）、悪意のある URL、機密データの漏洩、および不適切なコンテンツからシステムを防御するフルマネージドサービスです。 ・敵対的テスト（Adversarial Testing）：Google は、専任の「AI レッドチーム（倫理的ハッカー）」を擁し、提供開始前および提供開始後に広範なテストを実施することでシステムへの負荷テスト（ストレステスト）を行い、脆弱性をプロアクティブに軽減しています。 ・ウォーターマーキングと透明性（Watermarking & Transparency）：Google は、自社の AI ツールによって生成された合成メディアに能動的にウォーターマーク（電子透かし）を埋め込むほか、モデル開発の経緯、機能の限界、安全性テストのプロトコルを詳しく説明したモデルカードや技術レポートを公開しています。 詳細については、以下のドキュメントをご参照ください。 Service Specific Terms | Google Cloud: https://cloud.google.com/terms/service-terms Google Cloud - Delivering trusted and secure AI: https://services.google.com/fh/files/misc/ociso-ai-trust-paper-v2.pdf Generative AI Risk Management in Financial Institutions: https://services.google.com/fh/files/misc/wp_generative_ai_risk_management_in_fs.pdf Google Cloud Services Summary: https://cloud.google.com/terms/services Generative AI, Privacy, and Google Cloud: https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf	-
実152	Google Cloud は、責任共有モデルのもと、エンタープライズグレードの安全性、セキュリティ、およびプライバシーに関するコミットメントを厳格に履行しています。 ・データプライバシーとトレーニングの制限：Google は、「お客様のデータはお客様のもの」および「お客様のデータが Google のモデルの学習に使用されることはない」ことを保証しています。事前合意なく、お客様のプロンプトや生成された出力が Google の基盤モデルのトレーニングに使用されることはありません。ファインチューニングを行う際、トレーニングデータはお客様の安全なインスタンス内に留まり、学習されたパラメータ（アダプターの重みなど）は、そのお客様のみがアクセスできる論理的に分離されたレイヤーに保存されます。 ・サプライチェーンセキュリティ：Google は、SLSA（ソフトウェア アーティファクトのためのサプライ チェーン レベル）フレームワークと Sigstore を使用してファーストパーティモデルを保護し、モデルの来歴（Provenance）に暗号署名を施すことで、モデルのウェイト(Weights)の改ざんを防止しています。 ・データ保護とインフラストラクチャ：データは、保存時（AES-256）および転送時のいずれにおいてもデフォルトで暗号化され、Cloud KMS を介した顧客管理暗号化鍵（CMEK）のオプションも提供されています。お客様は、VPC Service Controls を使用してバックエンドの AI インフラストラクチャを保護できるほか、データセットを取り込む前に、Sensitive Data Protection（旧 DLP）を使用して個人識別情報（PII）のスキャン、マスク、またはトークン化を行うことができます。 ・生成 AI に関する知的財産権（IP）の免責保証：「運命共同体（Shared Fate）」のアプローチのもと、Google は、Google が使用するトレーニングデータと、基盤モデルから生成された出力の双方をカバーする二面的な知的財産権の免責保証を提供しており、適切な方法で使用されている限り、著作権に関する異議申し立てに対して法的責任を負います。 詳細については、以下のドキュメントをご参照ください。 Best Practices for Security Deploying AI on Google Cloud: https://services.google.com/fh/files/misc/best-practices-for-securely-deploying-ai-on-google-cloud.pdf	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
	Service Specific Terms | Google Cloud: https://cloud.google.com/terms/service-terms Generative AI, Privacy, and Google Cloud: https://services.google.com/fh/files/misc/genai_privacy_google_cloud_202308.pdf Google Cloud - Delivering trusted and secure AI: https://services.google.com/fh/files/misc/ociso-ai-trust-paper-v2.pdf	
実153	Google Cloud は、多様なプログラムを通じて、お客様のイネーブルメント（活用支援）、AI リテラシーの向上、およびエコシステム全体のセキュリティ強化を積極的にサポートしています。 ・技術トレーニングと認定資格：Google は、豊富なトレーニングリソース、ドキュメント、および特定の学習プラン（「Machine Learning Engineer パス」など）を提供し、お客様の担当者が AI 技術の仕組み、モデルの限界、およびコンプライアンス上の責任を的確に理解できるよう支援します。 ・責任ある生成 AI ツールキット：Google は、オープンソース開発者やユーザーに対し、独自の安全性分類システム()の構築、適切なコンテンツモデレーションの設定、およびカスタムのセーフティフィルターしきい値の確立を支援するためのツールキットやフレームワークを提供しています。 ・ホワイトペーパーによる情報発信：Google Cloudでは、技術的リサーチに基づくセキュリティガイダンスや、金融サービス向けの特定リスク管理フレームワーク、さらには既存の「モデルリスク管理（MRM：Model Risk Management）」フレームワークを生成 AI にいかに適応させるかを解説したホワイトペーパーなどを積極的に公開しています。 ・エコシステムへの貢献：Google は、自動で AI 構成要素を把握・管理する GKE（Google Kubernetes Engine）の「k8s-aibom」（AI のソフトウェア部品構成表：AI Bill of Materials）をはじめとするオープンソースセキュリティツールの普及に貢献しています。また、国際的な規制機関や標準化団体（NIST、ISO など）と緊密に連携し、相互運用可能で安全な AI プラクティスの確立を推進しています。 詳細については、以下のドキュメントをご参照ください。 Compliance resource center | Google Cloud: https://cloud.google.com/compliance Google Cloud - Delivering trusted and secure AI: https://services.google.com/fh/files/misc/ociso-ai-trust-paper-v2.pdf Google Cloud - Delivering trusted and secure AI: https://services.google.com/fh/files/misc/ociso-ai-trust-paper-v2.pdf 7 key questions CISOs need to answer to drive secure, effective AI: https://cloud.google.com/blog/transform/7-key-questions-cisos-need-to-answer-to-drive-secure-effective-AI Applying model risk management guidance to artificial intelligence/machine learning based risk models https://services.google.com/fh/files/misc/wp_applying_existing_ai_ml_model_risk_management_guidance.pdf Generative AI Risk Management in Financial Institutions: https://services.google.com/fh/files/misc/wp_generative_ai_risk_management_in_fs.pdf Google's Secure AI Framework: https://saif.google/	-
設1	Googleは、各種災害の影響が少ない地域をデータセンターの場所として選択しています。	-
設2	Googleのデータセンターでは、定期的に環境に関する検査を行い、災害に関する適切な対策を行っています。	-
設3	Google は、データセンターが所在するリージョンの法的な建築要件と設備要件をすべて満たしています。	-
設4	Google は、データセンターが所在するリージョンの法的な建築要件と設備要件をすべて満たしています。	-
設5	Google のデータセンターは、警報、車両セキュリティ ゲート、外周フェンスなどの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。	-
設6	Google のデータセンターでは、所在を表した看板はありません。	-
設7	Googleのデータセンターでは建築基準法や他の法に基づいた適切な避雷設備が設置されています。	-
設8	Googleのデータセンターは独立区画となっており、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施しており、立ち入りが許可されているのは特定の役割を持つ承認された社員のみです。	-
設9	Googleのデータセンターではケーブルの地下埋設、難燃性素材の利用などにより、切断・延焼への防止措置を講じています。	-
設10	Google は、データセンターが所在するリージョンの法的な建築要件と設備要件をすべて満たしています。	-
設11	Google は、データセンターが所在するリージョンの法的な建築要件と設備要件をすべて満たしています。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
設12	Googleのデータセンターでは、当該地域の環境的リスクの評価に基づき、適切な浸水対策を講じています。	-
設13	Googleのデータセンターは外壁等に十分な強度を持たせております。	-
設14	Google のデータセンターは、各国及び地域の消防・防火基準に応じた延焼防止対策を講じています。	-
設15	Googleのデータセンターにはアラームつきセキュリティシステムが設置されています。	-
設16	Googleのデータセンターでは、常時利用する出入口は1箇所であり、警備員による受付、非接触カードによる入館、監視カメラの設置などの防犯措置を施しています。	-
設17	Googleのデータセンターは非常口を設置しており、社員の安全を特に重視しており、緊急時に全スタッフが安全に避難できるよう、必要な標識を掲示したり、訓練を実施したりしています。	-
設18	Googleのデータセンターでは、当該地域の環境的リスクの評価に基づき、適切な浸水対策を講じています。	-
設19	Googleのデータセンターでは出入口の扉に十分な強度を施しており、施錠可能です。	-
設20	Google は、データセンターが所在するリージョンの法的な建築要件と設備要件をすべて満たしています。	-
設21	Googleのデータセンターでは地震による落下、損壊の防止措置を施しています。	-
設22	Google は、データセンターが所在するリージョンの建築要件と設備要件を遵守し、自然災害による損害を最小限に抑えるベストプラクティスに従って設備を運用しています。サーバースペースは、建物の免震層より上の階にあり、JQAに準拠しています。	-
設23	セキュリティ エリア（サーバースペースなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。立ち入りが許可されているのは特定の役割を持つ承認された社員のみです。こうしたエリアへのアクセスを監視・記録しており、アクセス権限を定期的に見直しています。	-
設24	コロケーションプロバイダーからリースするスペースの外側にGoogleの室名表示はありません。コロケーションプロバイダーは、消防用の見取図をメンテナンスし、部外者の目に触れない場所に保管しています。	-
設25	Googleのデータセンターにおけるサーバースペースには、機器の操作・メンテナンスのため十分なスペースを保有しており、避難経路も確保してあります。また機器を移動せずとも扉の開閉が可能なスペースがあります。	-
設26	Googleのデータセンターにおけるサーバースペースは専用の独立した区画となっています。	-
設27	Googleのデータセンターにおけるサーバースペースでは、常時利用する出入口は一か所に限定されており、出入口扉が長時間開放された場合は警報が発動し、監視センターに通報されます。更に、テールゲート（共連れ）を禁止するポリシーを運用すると共に、出入口は24時間遠隔監視を実施しています。	-
設28	Googleのデータセンターにおけるサーバースペースでは、出入口の扉は十分な強度を持ち、施錠可能です。	-
設29	Googleのデータセンターにおけるサーバースペースでは全て無窓化されております。	-
設30	Googleのデータセンターにおけるサーバースペースでは二方向避難の非常口を設置しており、社員の安全を特に重視しており、緊急時に全スタッフが安全に避難できるよう、必要な標識を掲示したり、訓練を実施したりしています。	-
設31	Googleのデータセンターにおけるサーバースペースは、建築基準法に規定された独立した防火区画としています。	-
設32	Googleのデータセンターにおけるサーバースペースは、漏水検知器を設置しており、異常が発生しているゾーン、データセンターオペレーション操作室において、一斉に警報を発する仕組みになっています。	-
設33	Googleのデータセンターは ESD の防止を含めた ESD プログラムに継続的に取り組んでいます。 （ESD：静電気放電）	-
設34	Googleのデータセンターにおけるサーバースペースでは、内装等に不燃材料及び防火性能を有するものを使用しています。	-
設35	Google は、データセンターが所在するリージョンの建築要件をすべて遵守し、自然災害による損害を最小限に抑えるベスト プラクティスに従って設備を運用しています。地震による内装等の落下、損壊の防止措置を施しています。	-
設36	Googleのデータセンターにおけるサーバースペースのフリーアクセスフロアは、各国・地域における地震リスク及び耐震基準に合致したものを導入しています。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
設37	Googleのデータセンターでは、施設に堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。火災検知器や消火設備を設置し、ハードウェアの損傷を防ぎます。熱、火、煙の探知機は、異常が発生しているゾーン、データセンターオペレーション操作室において、一斉に警報を発する仕組みになっています。	-
設38	Googleのデータセンターにおける熱、火、煙の探知機は、異常が発生しているゾーン、データセンターオペレーション操作室にこにおいて、一斉に警報を発する仕組みになっています。	-
設39	Googleのデータセンターでは施設に堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。火災検知器や消火設備を設置し、ハードウェアの損傷を防ぎます。Googleのデータセンターにおける熱、火、煙の探知機は、異常が発生しているゾーン、データセンターオペレーション操作室において、一斉に警報を発する仕組みになっています。	-
設40	Googleのデータセンターにおけるサーバースペースには、他区画から延焼を防止する措置が導入されています。	-
設41	Google は、データセンターが所在するリージョンの法的な建築要件と設備要件をすべて満たしています。	-
設42	Googleのデータセンターにおけるサーバースペースは非常用照明設備、携帯用照明器具を設置しています。	-
設43	Googleのデータセンターにおけるサーバースペース内には水関連施設は設置されていません。	-
設44	Googleのデータセンターでは、各地域における災害発生予測に基づいた適切な対策を設置・導入しています。例えば、地震発生時の対応基準の一環として、建物内の震度を測定するための地震感知器を設置しています。	-
設45	Googleのデータセンターにおけるセキュリティ エリア（サーバースペースなど）内への立ち入りには、セキュリティバッジや生体認証を利用した多元的なアクセス管理を実施しています。また、立ち入りが許可されているのは、特定の役割を持ち、事前にアクセス権限が承認された人員のみで、その権限は定期的に見直されています。併せて、セキュリティエリアへのアクセスは監視・記録され、異常が発生した場合には即時に警報が発動し、対応する仕組みになっています。	-
設46	環境の健全性と安全性の統制は、Google のデータセンターにおいて徹底されており、環境面に関する十分な対策を施しています。温湿度の計測・警報装置は、適切な場所に設置され、常時監視されています。	-
設47	Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。建物物衛生法に規定される建築物環境衛生管理基準に準拠し、維持管理、巡回等の適切な予防措置を実施しており、また厨房・飲食店等は建物内にありません。	-
設48	Googleのデータセンターにおけるサーバースペースでは、什器や備品は不燃性のものを使用しています。	-
設49	環境の健全性と安全性の統制は、Google のデータセンターにおいて徹底されており、施設で環境面に関する十分な対策を施しています。適用基準に関するトレーニングだけでなく、データセンター全体での ESD の防止を含めた ESD プログラムに継続的に取り組んでいます。 （ESD：静電気放電）	-
設50	Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて遵守し、自然災害による損害を最小限に抑えるベスト プラクティスに従って設備を運用しています。機器について、地震に対する予防策が講じられています。	-
設51	Googleのデータセンターにおけるサーバースペース内での運搬車（台車等）の利用は搬入出時に限定し、サーバースペース内に放置することはありません。運搬車には固定装置の取り付けを徹底しております。	-
設52	Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて遵守し、自然災害による損害を最小限に抑えるベスト プラクティスに従って設計し、構築されています。	-
設53	Googleのデータセンターにおける電源室・空調機械室には、機器の操作・メンテナンスのため十分なスペースを保有しており、避難経路も確保してあります。また機器を移動せずとも扉の開閉が可能なスペースがあります。	-
設54	Googelのデータセンターでは、電源室・空調機械室は専用のスペースです。 電源室・空調機械室へのアクセスは必要に応じて提供され、スペース内で必要な作業に従事する担当者にのみ与えられます。	-
設55	Googleの電源室・空調機械室には窓がなく、扉は施錠可能な「特定防火設備」であり、十分な強度があります。 また、電源室・空調機械室の出入口は1カ所です。	-
設56	環境の健全性と安全性の統制は、Google のデータセンターにおいて徹底されており、施設で環境面に関する十分な対策を施しています。電源室・空調機械室には堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。	-
設57	環境の健全性と安全性の統制は、Google のデータセンターにおいて徹底されており、施設で環境面に関する十分な対策を施しています。電源室・空調機械室には堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。火災検知器や消火設備を設置し、ハードウェアの損傷を防ぎます。熱、火、煙の探知機は、異常が発生しているゾーン、データセンターオペレーション操作室において、一斉に警報を発する仕組みになっています。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
設58	環境の健全性と安全性の統制は、Google のデータセンターにおいて徹底されており、環境面に関する十分な対策を施しています。電源室・空調機械室には堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。Googleのデータセンターの電源室・空調機械室にはガス系消火設備を設置しています。また、消火器は、各地域の消防法に基づき適切な位置に配置しています。	-
設59	Google は、データセンターが所在するリージョンの法的な建築要件と設備要件をすべて満たしています。	-
設61	Googleのデータセンターの電源設備では十分な余裕をもった設計で構築されています。	-
設62	Google のデータセンターは、24 時間体制で稼働しサービスを中断しないようにするため、冗長電源システムと環境管理を導入しています。同じ電力供給量を持つ主電源と代替電源が、すべての重要なコンポーネントに設置されています。	-
設63	Googleのデータセンターではコンピュータシステムを安定稼働させるため、UPSシステムが設置されています。また、バックアップ発電機により、緊急時でも最大限の性能を発揮できる電力を得られます。	-
設64	Googleのデータセンターではコンピュータシステムを安定稼働させるため、UPSシステムが設置されています。また、バックアップ発電機により、緊急時でも最大限の性能を発揮できる電力を得られます。	-
設65	Googleのデータセンターでは、接地電極からのサージ伝搬を防止する避雷器とSPDが誘導雷に対して設置されています。	-
設66	Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて遵守し、自然災害による損害を最小限に抑えるベスト プラクティスに従って設備を運用しています。 機器について、地震に対する予防策が講じられています。	-
設67	Googleのサーバースペースでは専用の回路を導入しています。また、サーバースペースへの電源は複数系統を確保し、適切に施設内を経由して引き込みを行っています。	-
設68	Googleサーバースペース内では、大きな負荷変動を引き起こす可能性のある機器と電源を共有していません。	-
設69	Googleのデータセンターでは、コンピュータシステム専用のアースを設置しています。	-
設70	Googleのデータセンターでは、過電流から各機器を保護するため、電源配線はブレーカからの配線とし、漏電警報器を設置済みです。	-
設71	Googleのデータセンターの防災・防犯設備には、UPS系電源を使用しています。また、バックアップ発電機により、緊急時でも最大限の性能を発揮できる電力を得られます。	-
設72	Googleのデータセンターの空調設備では十分な余裕をもった設計で構築されています。サーバーなどのハードウェアの動作温度を一定に保つことで、サービス停止のリスクを軽減します。	-
設73	Google は、業界が推奨する運用手順に従って、冷却システムを導入し維持しています。 自動制御装置、異常警報装置を設置しており、コンピュータ室の温湿度を適切に調整するよう監視・制御しています。	-
設74	Googleのデータセンターの空調設備は、コンピュータ室専用となります。	-
設75	Google のデータセンターは、24 時間体制で稼働しサービスを中断しないようにするため、十分な余裕をもった冗長システムと自動制御装置、異常警報装置を導入しています。Google は、業界が推奨する運用手順に従って、冷却システムを導入し維持しています。	-
設76	Google のデータセンターは、24 時間体制で稼働しサービスを中断しないようにするため、十分な余裕をもった冗長システムと自動制御装置、異常警報装置を導入しています。Google は、業界が推奨する運用手順に従って、冷却システムを導入し維持しています。	-
設77	Googelのデータセンターでは、電源室・空調機械室は専用のスペースです。 電源室・空調機械室へのアクセスは必要に応じて提供され、スペース内で必要な作業に従事する担当者にのみ与えられます。	-
設78	Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて遵守し、自然災害による損害を最小限に抑えるベスト プラクティスに従って設備を運用しています。 機器について、地震に対する予防策が講じられています。	-
設79	Googleのデータセンターでは、火災時の損傷防止の為、空調設備の断熱材料および給排気口には不燃材料を使用しています。	-
設80	Googleのデータセンターでは、中央監視装置や防犯監視装置等を設置しています。障害や異常が発生した際には、即時に警報を発動し、対応する仕組みになっています。	-
設81	Googleのデータセンターでは、中央監視装置や防犯監視装置等を設置しています。障害や異常が発生した際には、即時に警報を発動し、対応する仕組みになっています。	-
設82	Googelのデータセンターでは、回線関連設備は厳重に施錠され、アクセスは必要に応じて提供され、スペース内で必要な作業に従事する担当者にのみ与えられます。部屋が回線関連設備であることを示す案内板等はドアに設置されていません。	-

基準番号	**Google** の対策	**Google Cloud**金融サービス契約の対応箇所
設83	Googelのデータセンターでは、回線関連設備は厳重に施錠され、アクセスは必要に応じて提供され、スペース内で必要な作業に従事する担当者にのみ与えられます。部屋が回線関連設備であることを示す案内板等はドアに設置されていません。	-
設83-1	Googleのデータセンターでは専用の回路にて回線の引き込みを行い、障害及び回線への不正なアクセスを防いでいます。	-
設84	-	-
設85	-	-
設86	-	-
設87	-	-
設88	-	-
設89	-	-
設90	-	-
設91	-	-
設92	-	-
設93	-	-
設95	-	-
設96	-	-
設97	-	-
設98	-	-
設99	-	-
設100	-	-
設101	-	-
設102	-	-
設103	-	-
設104	-	-
設105	-	-
設106	-	-
設107	-	-
設108	-	-
設109	-	-
設110	-	-
設111	-	-
設112	-	-
設113	-	-
設114	-	-
設115	-	-
設116	-	-

基準番号	Google の対策	Google Cloud金融サービス契約の対応箇所
設117	-	-
設118	-	-
設119	-	-
設120	-	-
設121	-	-
設122	-	-
設123	-	-
設124	-	-
設125	-	-
設126	-	-
設127	-	-
設128	-	-
設129	-	-
設130	-	-
設131	-	-
設132	-	-
設133	-	-
設134	-	-
設138	-	-
監1	Googleは、規制対象法人、監督当局及びこれらが任命する者に対し、監査、立入及び情報提供に係る権利を付与します。 Googleは、当社サービスの監査に関して規制対象法人をサポートすることを確約します。当該サポートは、公開される当社の通常のサービス手数料に含まれていないため、Googleは、監査に関連する追加手数料を課す場合があります。Googleは、活動の範囲を認識した時点で、かかる活動の前に手数料の詳細を通知します。 Google は、規制対象法人または監督当局に代わって実施される監査により、サービスの運用と管理において対処されていない逸脱が特定された場合、適切な是正措置または改善措置を講じるよう努めます。 Googleは、お客様が当社のセキュリティ、プライバシー、コンプライアンス管理について独立した検証を期待していることを認識しています。この保証を提供するために、Googleは複数の独立した第三者機関による監査を定期的に受けています。Googleは、お客様との契約期間中、以下の主要な国際基準を遵守することをお約束します。 -ISO/IEC 27001 (Information Security Management Systems) -ISO/IEC 27017 (Cloud Security) -ISO/IEC 27018 (Cloud Privacy) -PCI DSS -SOC 1 -SOC 2 -SOC 3 Google の最新の認証と監査レポートはいつでもご確認いただけます。Compliance reports managerを使用すると、これらの重要なコンプライアンス リソースにオンデマンドで簡単にアクセスできます。	カスタマーコンプライアンスの支援 認証及び監査レポート
監1-1	-	-