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 9 版 (令和 2 年 3 月版)

Google Cloud と Google Workspace 解説書

本解説書は、令和 2 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 9 版 (令和 2 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 で認定済みです。本解説書ではお客様が Google Cloud のサービスや対応する ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 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2	-	-
統3	-	-
統4	-	-
統5	-	-
統6	-	-
統7	-	-
統8	-	-
統9	-	-
統10	-	-
統11	-	-
統12	-	-
統13	-	-
統14	-	-
統15	-	-
統16	-	-
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。 ◯コンプライアンス Google Cloud コンプライアンス https://cloud.google.com/security/compliance?hl=ja 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 サービス概要 https://cloud.google.com/terms/services Google Cloud サービスレベル契約 https://cloud.google.com/terms/sla/ サービス固有の規約 https://cloud.google.com/terms/service-terms 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 データ処理及びセキュリティ規約（データ移転) https://cloud.google.com/terms/data-processing-terms#10-data-transfers Google Cloud の復処理者(サブプロセッサー) https://cloud.google.com/terms/subprocessors 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?hl=ja 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 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/ 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	

	セキュリティのベストプラクティス https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#networking-and-security セキュリティユースケース https://cloud.google.com/security/showcase/ ◯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の構成要素 https://cloud.google.com/architecture/dr-scenarios-building-blocks 障害復旧計画ガイド https://cloud.google.com/architecture/dr-scenarios-planning-guide データの障害復旧シナリオ https://cloud.google.com/architecture/dr-scenarios-for-data インシデントとGoogle Cloud Status ダッシュボード https://cloud.google.com/support/docs/dashboard データインシデント対応に関するホワイトペーパー https://services.google.com/fh/files/misc/data_incident_response_2018.pdf Google Cloud Status Dashboard https://status.cloud.google.com/ ◯データ削除 Google Cloud 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?hl=ja 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Google Cloud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。 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)	該当なし	-
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、プライバシー及びコンプライアンス統制に関し、独立した検証が行われることを想定しているとの認識です。Googleは、これを確保するため、定期的に複数の独立した第三者による監査を受けています。Googleは、お客様との契約期間中において、以下の重要な国際基準を遵守することを確約します。 ISO/IEC 27001:2013（情報セキュリティ管理システム） ISO/IEC 27017:2015（クラウドセキュリティ） ISO/IEC 27018:2014（クラウドプライバシー） PCI DSS SOC 1 SOC 2 SOC 3	パフォーマンスの継続モニタリング 認証及び監査レポート

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 9 版 (令和 2 年 3 月版)

Google Cloud と Google Workspace 解説書

	お客様は、Googleの最新の認証及び監査レポートをいつでも参照することができます。	
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。 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Google Cloud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 データロケーション（サービス固有の規約） データセキュリティ、復処理者（データ処理及びセキュリティ規約） データ移転（データ処理及びセキュリティ規約）
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)	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。	サービス変更
1. (2)	サービス仕様	定義

	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。 データ保護 Googleがお客様のデータ保護に関するコミットメント（セキュリティ、使用、インシデント、アクセス及び保持に関するものを含む。）を行うデータ処理及びセキュリティ規約において言及されます。	 データセキュリティ、セキュリティ対策（データ処理及びセキュリティ規約）
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、お客様は、関連する行為について引き続き管理します。	-
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。	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。	データセキュリティ、Googleの職員によるセキュリティ遵守（データ処理及びセキュリティ規約）
1.(2), 6)	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。 (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。 ・当社のインフラストラクチャのセキュリティに関するページ ・当社のセキュリティに関するホワイトペーパー ・当社の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	データセキュリティ、Googleの職員によるセキュリティ遵守（データ処理及びセキュリティ規約）

	・当社のインフラストラクチャのセキュリティ設計の概要に関するページ ・当社のセキュリティのリソースに関するページ さらに、お客様は、GoogleのSOC2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。 ・保管データの暗号化　Googleは、お客様の追加行為を要することなく、保管されるお客様データをデフォルトで暗号化します。詳細は、https://cloud.google.com/security/encryption-at-rest/default-encryptionにおいて入手することができます。 ・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。詳細は、https://cloud.google.com/security/encryption-in-transitにおいて入手することができます。 (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、当社のクラウドのセキュリティプロダクトに関する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、以下に関するガイダンスを公表します。 ・セキュリティのベストプラクティス ・セキュリティユースケース	
1.(2), 7)	規制対象法人は、定期的なバックアップの一環として、Cloud Storage を使用することができます。データバックアップサービスの使用方法に関する詳細は、当社の障害復旧の構成要素及びデータの障害復旧シナリオの記事を参照のこと。	顧客のセキュリティ責任
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Google Cloud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。	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に全面的に協力します。 報告、連絡及びインシデント対応 Googleは、SLAに従い本サービスを履行する自らの能力に悪影響を及ぼす開発に関する情報をお客様が入手できるようにする。詳細は、当社のインシデントとGoogle Cloudダッシュボードに関するページにおいて入手することができます。 さらに、Googleは、速やかに、また、不当に遅滞することなく、データインシデントを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に関する詳細は、当社のデータインシデント対応に関するホワイトペーパーにおいて入手することができます。	顧客データの保護 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 重要な開発 データインシデント（データ処理及びセキュリティ規約）
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 Status Dashboardは、本サービスに関するステータス情報を提供します。 ・Google Cloud Operations は、モニタリング、ロギング及び診断を行う総合的なホスト型ソリューションであり、お客様がGoogle Cloud上で動作する自らのアプリケーションの洞察を得ることを支援します。 ・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。	パフォーマンスの継続モニタリング
1.(4),2)	お客様は、自らのデータに関してGoogleに指示することができ、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に指示することができます。 ・Cloud Console：お客様が自らのGoogle Cloud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： Google Cloud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による指示の遵守（データ処理及びセキュリティ規約）

	・Google APIs：Google Cloud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。	
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)	当社の技術サポートサービスガイドラインに関するページに記載されるサポートサービスに加え、Googleは、規制対象法人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提供します。具体的に、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。 規制対象法人がさらなるトレーニングを希望する場合、Googleはさまざまなコース及び認定資格も提供しています。	技術サポート
1.(4),5)	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。具体的に、お客様が自らのアプリケーションに関して希望するRTO及びRPOの達成方法に関する情報については、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に関する記事を参照のこと。	事業継続性及び障害復旧
1.(4),6)	インシデントの報告に係るGoogleのプロセスに関する詳細については、1. (4)を参照のこと。	-
1.(4),7)	インシデントの報告に係るGoogleのプロセスに関する詳細については、1. (4)を参照のこと。 さらに、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。 ・Cloud Audit Logsは、お客様のセキュリティチームがGoogle Cloud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。 さらに、お客様は、以下のツールを使用して、Googleの人員がお客様のデータに関して行う制限されたアクションを監視し、管理することもできる。 ・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ある。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者に関するデータ（Googleの人員の所在地等）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。	-
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。 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。	事業継続性及び障害復旧
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。	表明及び保証

1. (6)	解除 規制対象法人は、事前に通知することにより、自己都合により（必要に応じて法律を遵守する場合を含む。）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。 削除 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、当社のGoogle Cloud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。 移行支援 他のサービスプロバイダへのサービスの移行又は規制対象法人への環境の戻し作業に関してGoogleが行う支援方法に関する詳細は、1.(6), 3)を参照のこと。	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） 該当なし
1.(6), 1)	規制対象法人が契約を解除する能力に関する詳細は、1. (6)を参照のこと。	-
1.(6), 2)	契約関係を解約する際、Googleは、当社のシステムからお客様データを削除する旨の規制対象法人の指示を遵守します。削除に関する詳細は、当社のGoogle Cloud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。	解除に関する削除（データ処理及びセキュリティ規約）
1.(6), 3)	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。 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、例えば以下の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。 ・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 for Anthos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。画像及びストレージのオプションに関する詳細は、当社のCompute Engineドキュメントに関するページに記載されています。 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。	移行期間 データのエクスポート（データ処理及びセキュリティ規約） 移行支援
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、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 顧客データの保護
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。	顧客データの保護、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)	お客様の考慮事項となります。	-
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に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再委託先
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再委託先
1. (11), 3)	Googleは、再委託された全ての義務の履行を監督し、当社の再委託先が当社及びお客様との間の契約（監査及び立入に係る権利並びにセキュリティ要件を含む。）を遵守することを確実にします。	Google再委託先
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再委託先
1. (12)	-	-
1. (12), 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、立入及び情報に係る権利を付与します。	規制当局の情報、監査及び立入、顧客の情報、監査及び立入

1. (12), 2)	Googleは、当社サービスの監査又は試験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、監査又は試験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。	顧客コンプライアンスの支援、手数料
1. (12), 3)	Googleは、当社サービスの監査又は試験に関して規制対象法人をサポートすることを確約し、監査、情報及び立入に係る権利を行使する規制対象法人に全面的に協力します。	顧客コンプライアンスの支援
1. (13)	-	-
1. (13), 1)	Googleは、規制対象法人及び規制対象法人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。	顧客の情報、監査及び立入
1. (13), 2)	範囲に関して事前に協議することにより、Googleが効果的に監査を行うことが可能となります。例えば、当社は、関連するGoogleの専門家を手配し、お客様の時間を最大限有効活用するようにすることができます。また、通知により、お客様又はその他のGoogleのお客様の環境に不当なリスクが発生しないよう、Googleが監査を計画することも可能となります。	手配
1. (13), 3)	規制対象法人は、サービスに係る自らのデータにいつでもアクセスし、自らの監督当局にアクセス権を付与することができます。現場視察及び事前協議に関する詳細は、1. (13), 2)を参照のこと。	-
1. (14)	-	-
1. (14)	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（データ処理及びセキュリティ規約）
1. (15)	-	-
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。	技術サポート
1. (16)	-	-
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。	-
2.	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。 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。	本サービス 技術サポート
3.	顧客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。	-
3. (1)	データの抽出及びGoogleによるデータ移行作業への協力に関する詳細は、1.(6), 3)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。 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。	-
3. (2)	セキュリティに関する詳細は、1.(2), 6)を参照のこと。	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、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）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 の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ チームに配属されたエンジニアは、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を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。	
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」(ISO 27001 2013、附属書 A.15) 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/security/overview/whitepaper?hl=ja) ・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機能を提供しています。 ・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-terms (Google Cloud) https://workspace.google.com/terms/dpa_terms.html (Google Workspace) 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 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確認する。(https://cloud.google.com/security/overview/whitepaper?hl=ja) ・これまでのクラウド事業における実績について、以下の金融サービス向けソリューション公式サイトにおいて金融業界での実績を確認できます。(https://cloud.google.com/solutions/financial-services?hl=ja) ・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。GoogleCloud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。 ・Google Cloudは、お客様の要件に合わせた複数の保守サポートメニューをご用意しています。詳しくは公式サイトを御覧ください(https://cloud.google.com/support-hub?hl=ja) ・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。(https://cloud.google.com/security/compliance?hl=ja) 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。 Data Processing and Security Terms https://cloud.google.com/terms/data-processing-terms (Google Cloud) https://workspace.google.com/terms/dpa_terms.html (Google Workspace) Data Incident Response Whitepaper https://cloud.google.com/security/incident-response	-

統25	-	-
統26	-	-
実1	-	-
実2	-	-
実3	-	-
実4	-	-
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、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 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。 Data Processing and Security Terms https://cloud.google.com/terms/data-processing-terms (Google Cloud) https://workspace.google.com/terms/dpa_terms.html (Google Workspace) Data Incident Response Whitepaper https://cloud.google.com/security/incident-response	-

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。	-
実16	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 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。 Data Processing and Security Terms https://cloud.google.com/terms/data-processing-terms (Google Cloud) https://workspace.google.com/terms/dpa_terms.html (Google Workspace) Data Incident Response Whitepaper https://cloud.google.com/security/incident-response	-
実17		-
実18		-
実19	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク管理策」（ISO 27001 2013、附属書 A.13.1）が規定されています。 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。 Data Processing and Security Terms https://cloud.google.com/terms/data-processing-terms (Google Cloud)	-

	https://workspace.google.com/terms/dpa_terms.html (Google Workspace) Data Incident Response Whitepaper https://cloud.google.com/security/incident-response	
実20	-	-
実21	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書 A.12.2) 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はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ 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、「マルウェアからの保護」(附属書 A.12.2) 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はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	-
実23	-	-
実24	-	-
実25	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9) 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。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 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。	-
実26	-	-
実27	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9) 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 では、アクセスの妥当性を確認するために、全システムへの論理的アクセスの審査を定期的に実施しています。さらに、Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 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。	
実28	-	-
実29	-	-
実30	-	-
実31	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、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)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 の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ チームに配属されたエンジニアは、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を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。	-
実32	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書 A.12.2)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 はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェアセキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。 Google Cloud のお客様は、適切なウィルス対策の設定など、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33	-	-
実34	-	-
実35	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)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 社員のアクセス権限とそのレベルは、職務と役割に基づいて決定されています。その際に、「最小権限」と「必知事項」のコンセプトに基づき、アクセス権限と所定の職務を一致させています。システムのオペレーションは、身元が複数の方法で確認された、承認済みの管理者のみが行います。Google 社員によるアクセスは、専用のセキュリティ、プライバシー、および内部監査チームによりモニタリングおよび監査されます。また、Google は、Google Cloud のアクセスの透明性(https://cloud.google.com/access-transparency?hl=ja)を通じて監査ログを提供しています。	-
実36	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)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 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に	-

	割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定 の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 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。	
実37	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)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 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定 の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 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。	-
実38	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9)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 社員によるオペレーション操作は、記録され、オペレーション結果の検証が行われます。アクセスは、専用のセキュリティ、プライバシー、および内部監査チームによりモニタリングおよび監査されます。また、Google は、Google Cloud のアクセスの透明性(https://cloud.google.com/access-transparency?hl=ja)を通じて監査ログを提供しています。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。Google社員によるお客様が管理する範囲のシステムのオペレーションは、行うことができません。	-
実39	-	-
実40	-	-
実41	-	-
実42	-	-
実43	-	-
実44	Googleでは、国際標準化機構(ISO)によって確立されたベストプラクティスガイドラインを満たす、品質管理システムを確立しています。 品質管理システムは、Google Cloud と Google Workspace の開発と運用をサポートするアセットを含む製品の運用に適用されます。Googleの品質管理システムは、手順、プロセス、リソースなど、Google Cloud と Google Workspace の品質管理を実装するために必要な要素を自動化し、適切な情報管理を行います。	-
実45	Googleでは、国際標準化機構(ISO)によって確立されたベストプラクティスガイドラインを満たす、品質管理システムを確立しています。 品質管理システムは、Google Cloud と Google Workspace の開発と運用をサポートするアセットを含む製品の運用に適用されます。Googleの品質管理システムは、手順、プロセス、リソースなど、Google Cloud と Google Workspace の品質管理を実装するために必要な要素を自動化し、適切な情報管理を行います。	-

実46	-	-
実47	-	-
実48	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）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、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、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。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。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。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 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 https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	-
実50	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、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。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。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。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 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 https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	-
実51	Google は ISO27001 認証を受けています。この基準では、「装置の保守」（ISO 27001 2013、附属書 A.11.2.4）が規定されています。	-
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」（ISO 27001 2013、附属書 A.11.2.4）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」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、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。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、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。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡し	-

	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。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 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 https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	
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」(ISO 27001 2013、附属書 A.11.2.4) 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」(ISO 27001 2013、附属書 A.12.1.3) 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」(ISO27001 2013、附属書 A.11) が規定されています。システムの可用性に関する物理的な統制についても、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。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、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。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。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。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア (データ サーバー フロアなど) 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。セキュリティ エリアへの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です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 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 https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	-
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」(ISO27001 2013、附属書 A.11) が規定されています。システムの可用性に関する物理的な統制についても、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。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、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。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。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。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア (データ サーバー フロアなど) 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。セキュリティ エリアへの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です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 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 https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	-

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」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、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。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、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。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。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。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア(データ サーバー フロアなど)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。セキュリティ エリアへの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です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 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 https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	-
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」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、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。 セキュリティ エリア(データ サーバー フロアなど)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管理をモニタリングとロギングの対象にし、その妥当性を定期的に検証しています。アクセス権を持つ社員は、セキュリティ エリアへの立ち入りに関する方針と手続きに従う義務があります。	-
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」(ISO27001 2013、附属書 A.11)と「装置の保守」(ISO 27001 2013、附属書 A.11.2.4)が規定されています。システムの可用性に関する物理的な統制についても、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。 セキュリティ エリア(データ サーバー フロアなど)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管理をモニタリングとロギングの対象にし、その妥当性を定期的に検証しています。アクセス権を持つ社員は、セキュリティ エリアへの立ち入りに関する方針と手続きに従う義務があります。	-
実61	-	-
実62	-	-
実63	-	-
実64	-	-
実65	-	-
実66	-	-
実67	-	-
実68	-	-
実69	-	-
実70	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2)、「バックアップ」(ISO27001 2013、附属書 A.12.3)と「操作手順書」(ISO27001 2013、附属書 A.12.1.1.)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 プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。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、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 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 Cloud Status Dashboard はGoogle Cloudのサービスのステータス情報を提供します。ステータスにはサービス障害、停止、一時的な問題に関する情報が含まれます。Google Workspace Status Dashboard は、Gmail, Calendar, Google Meet といった Google Workspaceのコアのサービスにおける現在の状態に関する情報を提供します。 ダッシュボードは各サービスの現在の状態や障害や停止に関する情報を提供します。通知アイコンをクリックすることで該当の問題の詳細情報を確認できます。その情報には解決時期の見込みも含まれます。グローバルの Customer Care チームは、様々な異なるタイプのシグナルを活用してサービスの状態を監視し、広範囲の問題に関するイベント情報をダッシュボードに更新します。必要に応じて、彼らはインシデント解決後、詳細を示したインシデント分析レポートを更新します。 https://cloud.google.com/support/docs/dashboard https://cloud.google.com/security/incident-response	
実71	-	-
実72	Googleは、SLAに従い本サービスを履行する自らの能力に悪影響を及ぼす開発に関する情報をお客様が入手できるようにします。詳細は、当社のインシデントとGoogle Cloudダッシュボードに関するページにおいて入手することができます。 インシデントとGoogle Cloudダッシュボード https://cloud.google.com/support/docs/dashboard さらに、Googleは、速やかに、また、不当に遅滞することなく、データインシデントを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に関する詳細は、当社のデータインシデント対応に関するホワイトペーパーにおいて入手することができます。 データインシデント対応に関するホワイトペーパー https://services.google.com/fh/files/misc/data_incident_response_2018.pdf Googleがどのように根本原因を調査しているかは以下を参照してください。 https://cloud.google.com/security/incident-response	-
実73	-	-

実74	-	-
実75	-	-
実76	-	-
実77	-	-
実78	-	-
実79	-	-
実80	-	-
実81	-	-
実82	-	-
実83	-	-
実84	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2) 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 プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。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、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト (Google Workspace、Google Cloud) では、RPO (目標復旧時点) の目標も、RTO (目標復旧時間) の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 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、「冗長性」(ISO27001 2013、附属書 A.17.2) 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 プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。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、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト (Google Workspace、Google Cloud) では、RPO (目標復旧時点) の目標も、RTO (目標復旧時間) の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 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86	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2) 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 プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。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、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 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、「冗長性」（ISO27001 2013、附属書 A.17.2）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 プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。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、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 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、「冗長性」（ISO27001 2013、附属書 A.17.2）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 プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。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、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 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	-	-
実90	-	-

実91	-	-
実92	-	-
実93	-	-
実94	-	-
実95	-	-
実96	-	-
実97	-	-
実98	-	-
実99	-	-
実100	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14)が規定されています。詳しくは、「Google 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/security-design/)をご覧ください。 Google Cloud のお客様は、システム開発の手順など、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、「ログ取得及び監視」(ISO 27001 2013、附属書 A.12.4)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 のセキュリティ モニタリング プログラムは、内部ネットワーク トラフィックから収集されている情報、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焦点を当てています。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。この分析では、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、トラフィックのキャプチャと解析を行っています。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。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティ エンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データ レポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリング リスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知して Google セキュリティ スタッフに通知します。ネットワーク解析 に加え、システムログの自動解析も行われています。	-
実103	Google は ISO27001 認証を受けています。この基準では、「ログ取得及び監視」(ISO 27001 2013、附属書 A.12.4)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 のセキュリティ モニタリング プログラムは、内部ネットワーク トラフィックから収集されている情報、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焦点を当てています。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。この分析では、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、トラフィックのキャプチャと解析を行っています。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。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティ エンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データ レポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリング リスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知して Google セキュリティ スタッフに通知します。ネットワーク解析 に加え、システムログの自動解析も行われています。	-
実104	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2)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 プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。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、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。	
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127	-	-
実128	-	-
実129	-	-
実130	-	-
実131	-	-
実132	-	-
実133	-	-
実134	-	-
実135	-	-
実136	-	-
実137	-	-
実138	-	-
実139	-	-
実140	-	-
実141	-	-
実142	-	-
実143	-	-
実144	-	-
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の入る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	設3に同じ。	-
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適切な避雷設備が設置されており、アース接続されています。建築基準法や他の法に基づいた避雷設備が設置されています。避雷設備は日本工業規格に準拠しています。	-
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	設3に同じ。	-
設11	設3に同じ。	-
設12	設3に同じ。	-
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	設4にあるように、Googleのデータセンターは隣接建物と十分に離れている為延焼の恐れはありません。	-
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、人の出入口は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。 注意）この記述は日本（東京、大阪）のデータセンターに適用されます。	-
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のデータセンターは、熱、火、煙、水の検知を含め、環境面に関する十分な対策を施しています。開口部のまわりには適切な防水措置を施しています。	-
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	設3に同じ。	-
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部屋となっています。	-
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で前室が設けられ、テールゲートを防ぐ設備があります。Googleサイトはテールゲートを禁止するポリシーを保有しています。長時間ドアが開いたドアまたは適切に閉じていないドアは、アラームを発します。	-
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床は耐震措置対策済です。 注意)この記述は日本(東京、大阪)のデータセンターに適用されます。	-
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のケーブルは延焼防止措置済みです。	-
設41	設3に同じ。	-
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建物内の震度を測定するために、地震感知器がサーバースペースの外の管理エリアに設置されています。	-
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)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は	-

	監視・記録され、アクセス権限を定期的に見直しています。	
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、施設で環境面に関する十分な対策を施しています。温湿度記録装置はおよび温湿度警報装置は、データホールの適切な場所に設置されています。	-
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。	-

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、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。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。消化器は出入り口付近の扱いやすい場所に配置してあります。	-
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60	Googleのデータセンターの電源室・空調機械室のケーブル・ダクトは難燃性素材の利用などを行い、延焼への防止措置を講じています。	-
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	設63に同じ。	-
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には専用の回路がサーバースペースに導入されています。サーバースペースへの電源は2系統あり、さまざまな経路でケーブルが施設を適切に経由しています。	-
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	設75に同じ	-
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、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、警報を発する仕組みになっています。	-
設81	設80に同じ	-
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。	-
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、回線には専用のスペースを設けています。	-
設84	-	-
設85	-	-
設86	-	-
設87	-	-
設88	-	-
設89	-	-
設90	-	-
設91	-	-
設92	-	-
設93	-	-
設94	-	-
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	-	-
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135	-	-
設136	-	-
設137	-	-
監1	-	-
監1-1	Googleには、Googleの ID 管理、ソースコード管理、インフラストラクチャ管理に対する経営陣のコンプライアンスを評価する内部監査機能が確立されています。 組織には内部監査機能があり、情報セキュリティを管理するための組織のアプローチの有効性について独立したレビューを実施するために定期的に第三者機関と連携しています。 組織は、内部およびお客様への影響を減らすために、そのような活動を実施する前に、関連する利害関係者とのシステムセキュリティ関連の監査を計画および調整します。	-
監1-2	-	-
監1-3	Googleには、Googleの ID 管理、ソースコード管理、インフラストラクチャ管理に対する経営陣のコンプライアンスを評価する内部監査機能が確立されています。 組織には内部監査機能があり、情報セキュリティを管理するための組織のアプローチの有効性について独立したレビューを実施するために定期的に第三者機関と連携しています。 組織は、内部およびお客様への影響を減らすために、そのような活動を実施する前に、関連する利害関係者とのシステムセキュリティ関連の監査を計画および調整します。	-
監1-4	Googleには、Googleの ID 管理、ソースコード管理、インフラストラクチャ管理に対する経営陣のコンプライアンスを評価する内部監査機能が確立されています。	-

	組織には内部監査機能があり、情報セキュリティを管理するための組織のアプローチの有効性について独立したレビューを実施するために定期的に第三者機関と連携しています。 組織は、内部およびお客様への影響を減らすために、そのような活動を実施する前に、関連する利害関係者とのシステムセキュリティ関連の監査を計画および調整します。	
監1-5	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、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)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。 すべての Google 委託業者は、オリエンテーションプロセスの一環としてセキュリティ研修を受け、Google キャリアを通じて継続的なセキュリティ研修を受けます。新規の委託業者は、オリエンテーション中にお客様の情報を安全に保つことへのコミットメントを強調する当社の行動規範に同意します。役割に応じて、セキュリティの特定の側面に関する追加の研修が必要になる場合があります。たとえば、情報セキュリティチームは、安全なコーディング手法、製品設計、脆弱性テストツールなどのトピックについて、新しいエンジニアを指導します。また、技術者は、セキュリティ関連のトピックに関する技術プレゼンテーションに出席し、新しい脅威、攻撃パターン、軽減技法を網羅したセキュリティニュースレターを受け取ります。 また、Googleは契約を締結している金融機関によるGoogleのデータセンターやオフィスの監査を受け入れる可能性があります。詳しくは Google Cloud の営業担当者にお問い合わせください。	-