CSVガイドライン

医薬品・医薬部外品製造販売業者等におけるコンピュータ化システム適正管理ガイドライン（日本）

Google Cloud PlatformとG Suite解説書

本解説書は2010年 10 月 21 日 に厚生労働省により示された「医薬品・医薬部外品製造販売業者等 におけるコンピュータ化システム適正管理ガイドライン」（通称 CSV ガ イドライン）[リンク] に対する Google Cloud Platform の適合状況を示したものになります。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。

Google では、上述の CSV ガイドラインの内、6 章から 8 章 に着目して解説しています。そして、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。

＊項目番号は「章.節.項 (項目)」形で書いてあります。

行	項目番号	遵守事項	Googleの対策	ISO基準詳細
1	6.1 (1)	運用管理に関する文書の作成 運用に関する責任体制と役割 ① 組織 ② 運用責任者	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G Suite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 Platform 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。	ISO 27001の附属書 A.9 ISO 27017の 9 ISO 27018の 9
2	6.1 (2)	運用管理に関する文書の作成 コンピュータ化システムの操作	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.12.1.1 ISO 27017の12.1.1 ISO 27018の12.1.1
3	6.1 (3)	運用管理に関する文書の作成 保守点検管理	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。	ISO 27001の附属書 A.12.1.1 ISO 27017の12.1.1

		① 日常点検事項 ② 定期点検事項 ③ 保守点検を専門業者に委託する場合の取決め事項	Google Cloud Platform のお客様は、運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。	ISO 27018の12.1.1
4	6.1 (4)	運用管理に関する文書の作成 セキュリティ管理 ① データの入力、修正、削除等に関する担当者のアクセス権限の設定と不正アクセス防止 ② 識別構成要素の管理 ③ ハードウェア設置場所への立入制限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.12.1.1 ISO 27017の12.1.1 ISO 27018の12.1.1
5	6.1 (5)	運用管理に関する文書の作成 バックアップ及びリストア	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.12.1.1 ISO 27017の12.1.1 ISO 27018の12.1.1
6	6.1 (6)	運用管理に関する文書の作成 変更の管理 ① 変更の計画、承認の手順 ② 変更の影響評価 ③ その他、変更に必要な事項	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ための方針群」（ISO 27001 2013、附属書 A.5）、「情報セキュリティのための組織」（ISO27001 2013、附属書 A.6）、「運用の手順および責任」（ISO 27001 2013、附属書 A.12.1）が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、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 Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.5, 6,12.1 ISO 27017の5, 6, 12.1 ISO 27018の5, 6. 12.1
7	6.1 (7)	運用管理に関する文書の作成 逸脱（システムトラブル）の管理 ① 逸脱（システムトラブル）発生時の対応のための組織等 ② 逸脱（システムトラブル)の原因の究明及び影響評価 ③ 再発防止対策 ④ 回復措置 ⑤ システム停止後の再開手順及び再開時の確認事項	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ための方針群」（ISO 27001 2013、附属書 A.5）、「情報セキュリティのための組織」（ISO27001 2013、附属書 A.6）、「運用の手順および責任」（ISO 27001 2013、附属書 A.12.1）が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、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 Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.5, 6,12.1 ISO 27017の5, 6, 12.1 ISO 27018の5, 6. 12.1

		⑥ その他逸脱の管理に必要な事項		
8	6.1 (8)	運用管理に関する文書の作成 担当者の教育訓練	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。	ISO 27001の附属書 A.7.2.2 ISO 27017の7.2.2 ISO 27018の7.2.2
9	6.1 (9)	運用管理に関する文書の作成 自己点検	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」（ISO 27001 2013、附属書 A.12.7）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、社内監査の監督など、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。	ISO 27001の附属書 A.12.7 ISO 27017の12.7 ISO 27018の12.7
10	6.2 (1)	コンピュータ化システムの操作の手順に関する文書の作成 システムの担当者	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.12.1.1 ISO 27017の12.1.1 ISO 27018の12.1.1
11	6.2 (2)	コンピュータ化システムの操作の手順に関する文書の作成 コンピュータ化システムの操作	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.12.1.1 ISO 27017の12.1.1 ISO 27018の12.1.1
12	6.2 (3)	コンピュータ化システムの操作の手順に関する文書の作成 コンピュータ化システムの保守点検	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.12.1.1 ISO 27017の12.1.1 ISO 27018の12.1.1

13	6.2 (4)	コンピュータ化システムの操作の手順に関する文書の作成 コンピュータ化システムのセキュリティ管理	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.12.1.1 ISO 27017の12.1.1 ISO 27018の12.1.1
14	6.2 (5)	コンピュータ化システムの操作の手順に関する文書の作成 その他、コンピュータ化システムの特性に応じた運用管理	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.12.1.1 ISO 27017の12.1.1 ISO 27018の12.1.1
15	6.3 (1)	保守点検事項の実施 担当者に保守点検を実施させ、その結果を記録し、保管すること。	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。	ISO 27001の附属書 A.11.2.4 ISO 27017の11.2.4 ISO 27018の11.2.4
16	6.3 (2)	保守点検事項の実施 保守点検の記録により保守点検管理が適切に行われていることを確認すること。	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。	ISO 27001の附属書 A.11.2.4 ISO 27017の11.2.4 ISO 27018の11.2.4
17	6.4 (1)	セキュリティ管理の実施 データの入力、修正、削除等に関する担当者のアクセス権限の設定と、不正アクセスの防止措置 を講じること。	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	ISO 27001の附属書 A.9 ISO 27017の9 ISO 27018の9

			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 G Suite 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 Platform 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。	
18	6.4 (2)	セキュリティ管理の実施 識別構成要素等の取扱いについて、機密保護を図ること。	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 は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud Platform 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。	ISO 27001の附属書 A.9 ISO 27017の9 ISO 27018の9
19	6.4 (3)	セキュリティ管理の実施 必要に応じてハードウェア設置場所への立入制限を行うこと。	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	ISO 27001の附属書 A.11 ISO 27017の11 ISO 27018の11

			データセンターを紹介する動画 https://www.youtube.com/watch?v=7pkNt3szF1A	
20	6.4 (4)	セキュリティ管理の実施 セキュリティ管理に関する記録を作成するとともに、これを保管すること。	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」（ISO27001 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 の全社員は、入社時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。新入社員は入社時研修で 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。 Google Cloud Platform のお客様は、運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。	ISO 27001の附属書 A.7.2.2 ISO 27017の7.2.2 ISO 27018の7.2.2
21	6.5 (1)	バックアップ及びリストア ソフトウェア及びデータのバックアップを行うこと。	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）と「バックアップ」（ISO27001 2013、附属書 A.12.3）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 G Suite 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（G Suite、Google Cloud Platform）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 Platform のお客様は、データファイル管理をサポートするプロセスの開発など、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。	ISO 27001の附属書 A.12.3, 17.2 ISO 27017の12.3, 17.2 ISO 27018の12.3, 17
22	6.5 (2)	バックアップ及びリストア	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）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関	ISO 27001の附属書 A.12.3 17.2

		障害発生からの回復のためにソフトウェア及びデータのリストアを行うこと。	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 G Suite 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（G Suite、Google Cloud Platform）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 Platform 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。	ISO 27017の12.3, 17.2 ISO 27018の12.3, 17
23	6.5 (3)	バックアップ及びリストア バックアップ及びリストアに関する記録を作成するとともに、これを保管すること。	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）と「バックアップ」（ISO27001 2013、附属書 A.12.3）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 G Suite 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（G Suite、Google Cloud Platform）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 Platform 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。	ISO 27001の附属書 A.12.3, 17.2 ISO 27017の12.3, 17.2 ISO 27018の12.3, 17

24	6.6 (1)	変更の管理 変更がコンピュータ化システムに与える影響を評価し、評価の結果に基づき適切な措置を実施す ること。なお評価の結果、バリデーションが必要と判断された場合は、リスクの程度に応じて「4. 開発業務」及び「5. 検証業務」に戻ってバリデーションを実施すること。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud Platform 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。	ISO 27001の附属書 A.12.1.4, 14.2 ISO 27017の12.1.4, 14.2 ISO 27018の12.1.4, 14
26	6.6 (2)	変更の管理 変更に伴い発生する手順に関する文書の変更箇所を特定し、必要な改定を実施すること。	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ための方針群」（ISO 27001 2013、附属書 A.5）、「情報セキュリティのための組織」（ISO27001 2013、附属書 A.6）、「運用の手順および責任」（ISO 27001 2013、附属書 A.12.1）が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、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 Cloud Platform のお客様は、システム文書の管理など、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。	ISO 27001の附属書 A.5, 6, 12.1 ISO 27017の5, 6, 12.1 ISO 27018の5, 6, 12.1
27	6.6 (3)	変更の管理 変更内容の関係者への周知の方法を決定し、必要に応じて教育訓練を実施すること。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud Platform 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。	ISO 27001の附属書 A.5, 6, 14.2 ISO 27017の5, 6, 14.2 ISO 27018の5, 6, 14
28	6.6 (4)	変更の管理 変更の管理の記録を作成し、運用責任者の確認を得るとともに、運用責任者及び変更の管理に関する責任者等の承認を得てこれを保管すること。	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ための方針群」（ISO 27001 2013、附属書 A.5）、「情報セキュリティのための組織」（ISO27001 2013、附属書 A.6）、「運用の手順および責任」（ISO 27001 2013、附属書 A.12.1）が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、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 Cloud Platform のお客様は、システム文書の管理など、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。	ISO 27001の附属書 A.5, 6, 12.1 ISO 27017の5, 6, 12.1 ISO 27018の5, 6, 12.1
29	6.7 (1)	逸脱(システムトラブル)の管理 発生した逸脱（システムトラブル）が製品の品質に及ぼす影響を評価し、速やかに適切な対応措置を講じるとともに、その原因を究明し、必要な再発防止措置を実施すること。	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）と「バックアップ」（ISO27001 2013、附属書 A.12.3）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。	ISO 27001の附属書 A.12.3, 17.2 ISO 27017の12.3, 17.2 ISO 27018の12.3, 17

			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 G Suite 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（G Suite、Google Cloud Platform）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 Platform 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。	
30	6.7 (2)	逸脱(システムトラブル)の管理 逸脱（システムトラブル）発生後にコンピュータ化システムの運用を再開する場合には、復帰稼働が適切に行われていることを確認すること。	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）と「バックアップ」（ISO27001 2013、附属書 A.12.3）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 G Suite 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（G Suite、Google Cloud Platform）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 Platform 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。	ISO 27001の附属書 A.12.3, 17.2 ISO 27017の12.3, 17.2 ISO 27018の12.3, 17
31	6.7 (3)	逸脱(システムトラブル)の管理 逸脱（システムトラブル）の管理の記録を作成し、運用責任者の確認を得るとともに、運用管	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）と「バックアップ」（ISO27001 2013、附属書 A.12.3）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	ISO 27001の附属書 A.12.3, 17.2 ISO 27017の12.3, 17.2 ISO 27018の12.3, 17

		理責任者及び逸脱の管理に関する責任者等の承認を得てこれを保管すること。	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 G Suite 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（G Suite、Google Cloud Platform）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 Platform 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。	
32	6.8.1	教育訓練 運用責任者は、運用管理基準書に基づき、あらかじめ指定した者に、コンピュータ化システムを使用した業務に従事する者に対する教育訓練計画を作成させること。なお、教育訓練についてはＧＱＰ省令、ＧＭＰ省令における手順に従って運用することが望ましい。	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。	ISO 27001の附属書 A.7.2.2 ISO 27017の7.2.2 ISO 27018の7.2.2
33	6.8.2	教育訓練 教育訓練の実施 運用責任者は、教育訓練計画に基づき、あらかじめ指定した者に次に掲げる業務を行わせること	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	ISO 27001の附属書 A.7.2.2 ISO 27017の7.2.2 ISO 27018の7.2.2

			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。	
34	6.8 (1)	教育訓練 コンピュータを使用した業務に従事する者に対して、コンピュータ化システムを使用した業務に関する教育訓練を計画的に実施し、その記録を作成すること。	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。	ISO 27001の附属書 A.7.2.2 ISO 27017の7.2.2 ISO 27018の7.2.2
35	6.8 (2)	教育訓練 教育訓練の実施状況について運用責任者の確認を得るとともに、品質保証責任者又は製造管理者若しくは責任技術者に対して文書により報告すること。	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。	ISO 27001の附属書 A.7.2.2 ISO 27017の7.2.2 ISO 27018の7.2.2
36	6.8.3	教育訓練 教育訓練の記録の保管 運用責任者は教育訓練の実施の記録を保管すること。	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	ISO 27001の附属書 A.7.2.2 ISO 27017の7.2.2 ISO 27018の7.2.2

			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。	
37	7.1 (1)	自己点検 コンピュータ化システムがこのガイドラインに基つき管理されていることを確認するために定期的に自己点検を実施すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」（ISO 27001 2013、附属書 A.12.7）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、社内監査の監督など、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。	ISO 27001の附属書 A.12.7 ISO 27017の12.7 ISO 27018の12.7
38	7.1 (2)	自己点検 自己点検の結果について品質保証責任者又は製造管理者若しくは責任技術者に対して文書により報告すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」（ISO 27001 2013、附属書 A.12.7）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、社内監査の監督など、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。	ISO 27001の附属書 A.12.7 ISO 27017の12.7 ISO 27018の12.7
39	7.1 (3)	自己点検 自己点検の結果の記録を作成し、これを保管すること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」（ISO 27001 2013、附属書 A.12.7）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、社内監査の監督など、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。	ISO 27001の附属書 A.12.7 ISO 27017の12.7 ISO 27018の12.7
40	7.2	改善措置の実施 製造販売業者等は、自己点検の結果に基つ□き、改善か□必要な場合には所要の措置を講し□、その記録を作成しこれを保管させること。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」（ISO 27001 2013、附属書 A.12.7）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、社内監査の監督など、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。	ISO 27001の附属書 A.12.7 ISO 27017の12.7 ISO 27018の12.7
41	8.1 (1)	コンピュータシステムの廃棄の計画に関する文書の作成 廃棄に関する責任体制と役割 ① 組織 ② コンピュータシステムの廃棄の責任者	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）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	ISO 27001の附属書 A.11.2.7, 8.3.2 ISO 27017の11.2.7, 8.3.2 ISO 27018の11.2.7, 8

			があった場合にはすぐに対処します。	
42	8.1 (2)	コンピュータシステムの廃棄の計画に関する文書の作成 廃棄対象とするコンピュータシステム	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）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。	ISO 27001の附属書 A.11.2.7, 8.3.2 ISO 27017の11.2.7, 8.3.2 ISO 27018の11.2.7, 8
43	8.1 (3)	コンピュータシステムの廃棄の計画に関する文書の作成 データの移行に関する事項	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）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。	ISO 27001の附属書 A.11.2.7, 8.3.2 ISO 27017の11.2.7, 8.3.2 ISO 27018の11.2.7, 8
44	8.1 (4)	コンピュータシステムの廃棄の計画に関する文書の作成 セキュリティに関する事項	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）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	ISO 27001の附属書 A.11.2.7, 8.3.2 ISO 27017の11.2.7, 8.3.2 ISO 27018の11.2.7, 8

			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。	
45	8.1 (5)	コンピュータシステムの廃棄の計画に関する文書の作成 コンピュータシステムの廃棄方法 コンピュータシステムの種類や規模、用途等に応じて以下を参考にして適切に定めること ① リスクアセスメント ② 前提条件 ③ スケジュール ④ 具体的な廃棄の方法 ・ハードウェア ・ソフトウェア ・データ ・文書類（手順書、記録、契約書等）	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）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。	ISO 27001の附属書 A.11.2.7, 8.3.2 ISO 27017の11.2.7, 8.3.2 ISO 27018の11.2.7, 8
46	8.1 (6)	コンピュータシステムの廃棄の計画に関する文書の作成 廃棄完了の判断基準	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）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。	ISO 27001の附属書 A.11.2.7, 8.3.2 ISO 27017の11.2.7, 8.3.2 ISO 27018の11.2.7, 8

47	8.2	コンピュータシステムの廃棄記録の作成 コンピュータシステムの廃棄の責任者は、廃棄計画書に基づきコンピュータシステムを廃棄するとともに、廃棄の記録を作成し、これを保管すること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）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。	ISO 27001の附属書 A.11.2.7, 8.3.2 ISO 27017の11.2.7, 8.3.2 ISO 27018の11.2.7, 8