FISC 安全対策基準対応ガイド

設備	
FISC安全対策基準一覧	
項番	Google の回答
設1	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 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。
設2	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。 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 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。
設3	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設4	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設5	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 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。
設6	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 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。
設7	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。 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" 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。
設8	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。 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。
設9	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設10	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設11	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設12	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設13	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 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。
設14	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設15	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 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。
設16	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。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は、監視と記録の対象にしています。 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 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。
設17	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。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。 すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設18	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設で、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。 すべての施設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、水の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在する地域の建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。

設19	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は、監視と記録の対象になっています。 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。
設20	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在する地域の建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設21	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設22	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設23	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。 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。
設24	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 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。
設25	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。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。 すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設26	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。 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 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。
設27	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。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。 すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設28	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 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。
設29	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設で、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。 すべての施設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、水の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在する地域の建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設30	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。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。 すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設31	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在する地域の建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設32	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設で、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。 すべての施設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、水の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在する地域の建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設33	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。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。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設34	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設35	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。 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。
設36	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設37	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。

設38	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設39	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers
設40	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設41	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設42	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設43	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設で、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。 すべての施設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、水の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在する地域の建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設44	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。 Google では、データセンターが所在する地域に関連したリスクなど、リスクに基づいた管理体制をデータセンターに適用しています。該当する場合は、自然災害や環境災害の監視、管理を行い、現地の事象に対応できるよう人材のトレーニングも実施するなど適切な対策を講じています。 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。
設45	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は監視・記録され、アクセス権原を定期的に見直しています。 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。
設46	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設で、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。 すべての施設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、水の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設47	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。 Google では、データセンターが所在する地域に関連したリスクなど、リスクに基づいた管理体制をデータセンターに適用しています。該当する場合は、自然災害や環境災害の監視、管理を行い、現地の事象に対応できるよう人材のトレーニングも実施するなど適切な対策を講じています。 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。
設48	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設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」（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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。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。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設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」（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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設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」（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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設52	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。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。 すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設54	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。 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 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。
設55	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設で、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。 すべての施設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、水の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在する地域の建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。

設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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設で、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。 すべての施設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、水の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在する地域の建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設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）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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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ています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https //cloud.google.com/secur ty/whitepaper#state-of-the-art_data_centers 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。
設61	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設62	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設63	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設64	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設65	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。 Google では、データセンターが所在するリージョンに関連したリスクなど、リスクに基づいた管理体制をデータセンターに適用しています。該当する場合は、自然災害や環境災害の監視、管理を行い、現地の事象に対応できるよう人材のトレーニングも実施するなど適切な対策を講じています。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設66	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設67	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設68	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設69	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設70	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設71	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。
設72	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。 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。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。 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。
設73	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。 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。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。 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。
設74	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。 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。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。 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。
設75	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。 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、G Su te 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 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。
設76	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。 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。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。 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。
設77	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 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。
設78	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。 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。ディーゼル エンジンのバックアップ発電機により、各データセンターは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。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 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。

設79	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。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設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、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。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。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。 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。
設80	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 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。
設81	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 24 時間体制で稼働する高解像度の監視カメラを設置し、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 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。
設82	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 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。
設83	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 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。
設83-1	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 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。
設84	対象外
設85	対象外
設86	対象外
設87	対象外
設88	対象外
設89	対象外
設90	対象外
設91	対象外
設92	対象外
設93	対象外
設94	対象外
設95	対象外
設96	対象外
設97	対象外
設98	対象外
設99	対象外
設100	対象外
設101	対象外
設102	対象外
設103	対象外
設104	対象外
設105	対象外
設106	対象外
設107	対象外
設108	対象外
設109	対象外
設110	対象外
設111	対象外
設112	対象外
設113	対象外
設114	対象外
設115	対象外
設116	対象外
設117	対象外
設118	対象外
設119	対象外
設120	対象外
設121	対象外
設122	対象外
設123	対象外
設124	対象外
設125	対象外
設126	対象外
設127	対象外
設128	対象外
設129	対象外
設130	対象外
設131	対象外
設132	対象外
設133	対象外
設134	対象外
設135	対象外
設136	対象外
設137	対象外

運用

項番	Google の回答
運1	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 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）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、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。
運2	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 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）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、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。
運3	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 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）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、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。
運4	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 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）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、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。
運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ための方針群」（ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）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、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。
運6	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 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）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、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。
運7	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。
運8	Google は ISO27001 認証を受けています。この基準では、「人的資源のセキュリティ」（ISO27001 2013、附属書 A.7）が規定されています。人的資源の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。 全社員は Google の行動規範（https //abc.xyz/investor/other/google-code-of-conduct.html）に同意し、倫理とコンプライアンスに関する研修を受けています。 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。

運9	Google は ISO27001 認証を受けています。この基準では、「人的資源のセキュリティ」（ISO27001 2013、附属書 A.7）が規定されています。人的資源の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。 全社員は Google の行動規範（https //abc.xyz/investor/other/google-code-of-conduct.html）に同意し、倫理とコンプライアンスに関する研修を受けています。 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。
運10	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。
運10-1	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」（ISO27002 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。
運11	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"
運12	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"
運13	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"
運14	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。
運15	Google は ISO27001 認証を受けています。この基準では、「記録の保護」（附属書 A.12.1.1）と「事業継続マネジメントにおける情報セキュリティの側面」（附属書 A.17）が規定されています。 Google では、システム復旧を円滑に進めるための作業手順書を作成しています。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。
運16	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 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。
運17	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。
運18	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 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。
運19	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。 情報セキュリティの監督管理体制は、論理的なアクセス制御など、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。 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。
運20	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。
運21	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。
運22	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。
運23	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。
運24	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。情報セキュリティの監督管理体制は、ソフトウェアの開発管理など、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。 Google Cloud Platform のお客様は、入力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、管理するすべて権利と責任を保有します。
運25	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。情報セキュリティの監督管理体制は、ソフトウェアの開発管理など、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。 Google Cloud Platform のお客様は、入力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、管理するすべて権利と責任を保有します。
運26	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。情報セキュリティの監督管理体制は、ソフトウェアの開発管理など、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。 Google Cloud Platform のお客様は、入力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、管理するすべて権利と責任を保有します。
運27	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。
運28	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。情報セキュリティの監督管理体制は、ソフトウェアの開発管理など、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。 Google Cloud Platform のお客様は、プログラム 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。

運29	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、プログラム 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。
運30	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、www.google.com/intl/en/corporate/security.html をご覧ください。 Google Cloud Platform 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。
運31	Google は ISO27001 認証を受けています。この基準では、「運用の手順および責任」(ISO 27001 2013、附属書 A.12.1)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 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。 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。
運32	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。
運33	Google は ISO27001 認証を受けています。この基準では、「記録の保護」(ISO 27001 2013、附属書 A.12.1.1)が規定されています。 Google Cloud Platform のお客様は、ストレージ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。
運34	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、フォーム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。
運35	フォーム管理をサポートするプロセスの開発は、お客様側で対応していただく必要があります。
運36	フォーム管理をサポートするプロセスの開発は、お客様側で対応していただく必要があります。
運37	出力情報をサポートするプロセスの開発は、お客様側で対応していただく必要があります。
運38	トランザクション管理はお客様側で対応していただく必要があります。
運39	トランザクション管理はお客様側で対応していただく必要があります。
運40	トランザクション管理はお客様側で対応していただく必要があります。
運41	トランザクション管理はお客様側で対応していただく必要があります。
運42	トランザクション管理はお客様側で対応していただく必要があります。
運43	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https //cloud.google.com/security/encryption-at-rest/ https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、暗号鍵管理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。
運44	ID 確認はお客様側で対応していただく必要があります。
運44-1	CD や ATM での現金取引の確認はお客様側で対応していただく必要があります。
運45	CD や ATM、無人の支店については、お客様側で対応していただく必要があります。
運46	CD や ATM、無人の支店については、お客様側で対応していただく必要があります。
運47	CD や ATM、無人の支店については、お客様側で対応していただく必要があります。
運48	CD や ATM、無人の支店については、お客様側で対応していただく必要があります。
運49	CD や ATM、無人の支店については、お客様側で対応していただく必要があります。
運50	携帯端末については、お客様側で対応していただく必要があります。
運51	CD や ATM、無人の支店については、お客様側で対応していただく必要があります。
運51-1	CD や ATM、無人の支店については、お客様側で対応していただく必要があります。
運52	CD や ATM、無人の支店については、お客様側で対応していただく必要があります。
運53	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。また、自社のデータを保護し、保護対策におけるすべての責任を負います。
運53-1	お客様は、ユーザーの生体認証データを使用する場合、そのデータを安全に保護する必要があります。
運54	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 Cloud Platform のお客様は、リソース管理など、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。
運55	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」(ISO 27001 2013、附属書 A.13)と「公衆ネットワーク上のアプリケーション サービスのセキュリティの考慮」(ISO27002 2013、附属書 A.14.1.2)が規定されています。 Google Cloud Platform のお客様は、外部接続の管理など、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。
運56	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」(ISO 27001 2013、附属書 A.13)と「公衆ネットワーク上のアプリケーション サービスのセキュリティの考慮」(ISO27002 2013、附属書 A.14.1.2)が規定されています。 Google Cloud Platform のお客様は、外部接続の管理など、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。
運57	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
運58	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
運59	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.11.2.4)が規定されています。
運60	Google は ISO27001 認証を受けています。この基準では、「ロギングおよびモニタリング」(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。 Google Cloud Platform のお客様は、お使いの環境を設定、管理、モニタリングするすべての権利と責任を保有します。
運61	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。
運62	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。
運63	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。
運64	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。

運65	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 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。 また、不測の事態への対応など、しっかりとした社内 DR プログラムを確立しています。 Google Cloud Platform のお客様は、危機管理計画の作成など、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。
運66	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 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。
運67	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。
運68	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。
運69	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。
運70	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。
運71	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、ストレージ管理の手順など、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。
運72	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.14.2)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 Platform 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。
運73	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.14.2)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 Platform 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。
運74	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。
運75	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。
運76	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
運77	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
運78	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。
運79	Google は ISO27001 認証を受けています。この基準では、「ロギングおよびモニタリング」(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。
運80	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。
運81	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。
運82	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。
運83	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 チームは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。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。
運84	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。
運85	Google は ISO27001 認証を受けています。この基準では、「人的資源のセキュリティ」(ISO27001 2013、附属書 A.7)が規定されています。人的資源の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 Cloud Platform のお客様は、人的資源の管理など、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。
運86	Google は ISO27001 認証を受けています。この基準では、「人的資源のセキュリティ」(ISO27001 2013、附属書 A.7)が規定されています。人的資源の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 Cloud Platform のお客様は、人的資源の管理など、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。
運87	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、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、Google は顧客サポートやテクニカル サポートなどのサービスを提供するためにサードパーティ サプライヤーを利用することがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。 https //cloud.google.com/terms/subprocessors https //gsuite.google.com/terms/subprocessors.html
運87-1	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、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、Google は顧客サポートやテクニカル サポートなどのサービスを提供するためにサードパーティ サプライヤーを利用することがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。 https //cloud.google.com/terms/subprocessors https //gsuite.google.com/terms/subprocessors.html
運88	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、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、Google は顧客サポートやテクニカル サポートなどのサービスを提供するためにサードパーティ サプライヤーを利用することがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。 https //cloud.google.com/terms/subprocessors https //gsuite.google.com/terms/subprocessors.html
運89	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。
運90	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、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、Google は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ サプライヤーを利用することがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
運90-1	Google は、お客様に代わって金融取引ソフトウェアを運用しません。CD や ATM のネットワーク保守はお客様側で対応していただく必要があります。
運91	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。
運92	インストア ブランチについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運93	コンビニの ATM については、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運94	コンビニの ATM については、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。

運95	コンビニの ATM については、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運96	コンビニの ATM については、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運97	コンビニの ATM については、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運98	コンビニの ATM については、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運99	デビットカードについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運100	デビットカードについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運101	デビットカードについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運102	デビットカードについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運103	オープン ネットワークを利用した金融サービスについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運104	オープン ネットワークを利用した金融サービスについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運105	オープン ネットワークを利用した金融サービスについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運105-1	オープン ネットワークを利用した金融サービスについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運106	オープン ネットワークを利用した金融サービスについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運107	オープン ネットワークを利用した金融サービスについては、お客様側で対応していただく必要があります。これは、Google プラットフォームの範囲外です。
運108	クラウド プロバイダを選定する際の適正評価は、エンドユーザーの責任となっています。Google は、見込み顧客が特定のプロダクトを評価できるよう、公開済みの情報を提供します。
運109	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約と SLA をご覧ください。 利用規約 https //cloud.google.com/terms/ https //gsuite.google.com/terms/2013/1/premier_terms.html SLA https //gsuite.google.com/terms/sla.html https //cloud.google.com/terms/sla/
運110	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https //cloud.google.com/security/encryption-at-rest/ https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、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。
運111	Cloud Platform のお客様のデータは、Google ではなくお客様が所有しています。お客様が Google のシステムに入力したデータはお客様のものであり、Google が広告のためにスキャンしたり、サードパーティに売却したりすることはありません。Google ではお客様にデータ処理の詳細な修正条項を提示しています。この条項は、お客様のデータの保護に対する Google の取り組みを示すものです。この条項では、Google が契約上の義務を履行する場合以外では、いかなる目的でもデータを処理しないことが明記されています。さらに、お客様がデータを削除した場合、Google は 180 日以内にそのデータをシステムから削除します。Google は、お客様が Google のサービスの使用を中止することにした場合にデータを簡単に取得するためのツールを提供しています。このとき、Google が罰金や追加料金を課すことはありません。 Google Cloud Platform のお客様は、適切な暗号化対策の開発など、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。
運112	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独立したレビュー」(ISO 27001 2013、附属書 A.18.2.1)が規定されています。 さらに、Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。 Google では、各種監査を実施して Google の統制環境について第三者機関による検証を受けており、必要に応じて、お客様に監査証明書を提供しています。 第三者機関によるコンプライアンス監査をまとめた最新リストは、以下のページで確認できます。 https //cloud.google.com/security/compliance https //gsuite.google.com/learn-more/compliance-google-apps.html
運113	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」(ISO 27001 2013、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、www.google.com/intl/en/corporate/security.html をご覧ください。

技術	
項番	Google の回答
技1	Google は ISO27001 認証を受けています。この基準では、「装置の保守」(附属書 A.11.2.4)が規定されています。 Google のインフラストラクチャはコンテナ テクノロジーを採用し、機器の障害を柔軟かつシームレスに処理します。機器の不具合を継続的にモニタリングし、問題が見つかった場合は、データを他の機器に転送してサービスの停止を回避します。
技2	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 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。
技3	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 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。
技4	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 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。
技5	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 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。
技6	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 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。
技7	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.14.2)が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、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。
技8	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.14.2)が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、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。
技9	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.14.2)が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、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。
技10	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.14.2)が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、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。
技11	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.14.2)が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、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。
技12	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.14.2)が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、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。
技13	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.14.2)が規定されています。 Google Cloud Platform のお客様は、システム開発プロセスの管理など、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。
技14	Google は ISO27001 認証を受けています。この基準では、「変更管理」(ISO 27001 2013、附属書 A.12.1.2)と「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14.2)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 Platform のお客様は、変更管理手順やシステム開発手順など、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。
技15	Google は ISO27001 認証を受けています。この基準では、「変更管理」(ISO 27001 2013、附属書 A.12.1.2)と「システムの取得、開発および保守」(ISO 27001 2013、附属書 A.14.2)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 Platform のお客様は、変更管理手順やシステム開発手順など、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。
技16	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.14.2)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 Platform 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。
技17	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.14.2)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 Platform 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。
技18	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.14.2)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 Platform 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。
技19	CD や ATM の遠隔制御機能の確認はお客様側で対応していただく必要があります。
技20	Google は ISO27001 認証を受けています。この基準では、「ロギングおよびモニタリング」(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。
技21	Google は ISO27001 認証を受けています。この基準では、「ロギングおよびモニタリング」(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。
技22	Google は ISO27001 認証を受けています。この基準では、「ロギングおよびモニタリング」(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。
技23	アカウント レベルでエラーを最小限に抑える対策は、お客様側で対応していただく必要があります。

技24	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 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。
技25	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 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。
技26	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、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。
技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 社員のアクセス権とアクセスレベルは職務上の役割に基づいており、権限を最小限にし、知る必要がある人物にだけ知らせるという考え方に基づいて、アクセス権を定義済みの職務に対応付けています。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、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。
技28	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https //cloud.google.com/security/encryption-at-rest/ https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、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。
技29	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https //cloud.google.com/security/encryption-at-rest/ https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、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。
技30	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.14.2)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 Platform 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。
技31	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.14.2)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 Platform 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。
技32	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.14.2)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 Platform 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。
技33	Google は ISO27001 認証を受けています。この基準では、「ロギングおよびモニタリング」(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。 Google Cloud Platform のお客様は、不正データや未確認データを検出するためのモニタリング設定など、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。
技34	Google は ISO27001 認証を受けています。この基準では、「ロギングおよびモニタリング」(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。 Google Cloud Platform のお客様は、不正データや未確認データを検出するためのモニタリング設定など、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。
技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、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。
技35-1	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、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。
技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 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、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。
技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 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、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。
技38	不正使用の防止については、お客様側で対応していただく必要があります。
技39	不正使用の防止については、お客様側で対応していただく必要があります。
技40	お客様は、偽造カードの使用について適切な予防策を講じる必要があります。
技41	お客様は、偽造カードの使用について適切な予防策を講じる必要があります。
技42	Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001 2013、附属書 A.10)が規定されています。 Google は、Google Cloud プロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https //cloud.google.com/security/encryption-at-rest/ https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud Platform のお客様は、適切な暗号化対策の開発など、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。
技42-1	お客様は、不正な閲覧について適切な予防策を講じる必要があります。
技43	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。Google のセキュリティ インシデント管理プログラムは、インシデントの処理に関する NIST ガイダンス(NIST SP 800-61)に基づいています。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、法科学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 Platform 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。
技44	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。Google のセキュリティ インシデント管理プログラムは、インシデントの処理に関する NIST ガイダンス(NIST SP 800-61)に基づいています。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、法科学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 Platform 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。
技45	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.13.1.1)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。Google のセキュリティ インシデント管理プログラムは、インシデントの処理に関する NIST ガイダンス(NIST SP 800-61)に基づいています。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、法科学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 Platform 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。
技46	お客様は、疑わしいトランザクションを識別するためのパラメータを設定する必要があります。
技47	お客様は、疑わしいトランザクションを識別するためのパラメータを設定する必要があります。
技48	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.13.1.1)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。Google のセキュリティ インシデント管理プログラムは、インシデントの処理に関する NIST ガイダンス(NIST SP 800-61)に基づいています。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、法科学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 Platform 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。
技49	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、www.google.com/intl/en/corporate/security.html をご覧ください。

技50		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、www.google.com/intl/en/corporate/security.html をご覧ください。
技51		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、www.google.com/intl/en/corporate/security.html をご覧ください。