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 | 基準大項目 | 基準中項目 | 基準小項目 | 適用にあたっての考え方 | Google の回答 |
| 設1 | IV 設備基準<br>I. コンピュータセンター | 建物(環境) | 設1 各種災害、障害が発生しやすい地域を避けること。 | コンピュータセンターへの災害の影響を少なくするため、各種災害及び障害が発生しやすい地域の立地を避けることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設2 | IV 設備基準<br>I. コンピュータセンター | 建物(周囲) | 設2 立地環境の変化に伴う災害および障害の発生の可能性を調査し、防止対策を講ずること。 | コンピュータセンターへの災害の影響を少なくするため、コンピュータセンターの自然環境、地域環境等の変化に伴う災害および障害の発生の可能性を調査し、防止対策を講ずることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設3 | IV 設備基準<br>I. コンピュータセンター | 建物(周囲) | 設3 敷地には通路を確保すること。 | 敷地には火災時の安全かつ適切な消火活動、避難を容易にするため、建築基準法に定められた幅員の通路を確保すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設4 | IV 設備基準<br>I. コンピュータセンター | 建物(周囲) | 設4 隣接物との間隔を十分に取ること。 | 延焼の防止および消火活動を容易にするため、隣接する建物との間隔を十分取ることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設5 | IV 設備基準<br>I. コンピュータセンター | 建物(周囲) | 設5 塀または柵および侵入防止装置を設けること。 | 敷地内への不法侵入、建物等の破壊行為を防止するため、敷地境界において入退管理を行う場合は塀または柵を設けることが望ましく、必要に応じて侵入防止装置を設けることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設6 | IV 設備基準<br>I. コンピュータセンター | 建物(周囲) | 設6 看板等を外部に出さないこと。 | 外部からの侵入、破壊行為等の人為的災害を未然に防止するため、コンピュータセンター等の所在を示した表示板、看板等は外部に出さないことが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設7 | IV 設備基準<br>I. コンピュータセンター | 建物(周囲) | 設7 建物には避雷設備を設置すること。 | 落雷による障害、事故を防止するため、周囲に高い建物がない場合または落雷多発地域においては、建物には避雷設備を設置することが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0"<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |

| | | | | | |
|---|---|---|---|---|---|
| 設8 | IV 設備基準<br>I. コンピュータセンター | 建物(周囲) | 設8 建物はコンピュータシステム関連業務専用、または建物内においてコンピュータシステム関連業務専用の独立区画とすること。 | 安全管理の徹底のため、建物はコンピュータシステム関連業務専用、または建物内においてコンピュータシステム関連業務専用の独立区画とすることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設9 | IV 設備基準<br>I. コンピュータセンター | 建物(周囲) | 設9 敷地内の通信回線・電力線は、切断・延焼の防止措置を講ずること。 | コンピュータシステムのサービス中断を防止するため、敷地内の通信回線・電力線は、工事や外部からの侵入等による切断・延焼の防止措置を講ずることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設10 | IV 設備基準<br>I. コンピュータセンター | 建物(構造) | 設10 耐火建築物であること。 | 防火対策のため、コンピュータセンターの建物は、建築基準法に規定する耐火建築物とすること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設11 | IV 設備基準<br>I. コンピュータセンター | 建物(構造) | 設11 構造の安全性を有すること。 | コンピュータシステムに障害を及ぼさないため、建築基準法に規定する構造の安全性を有すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設12 | IV 設備基準<br>I. コンピュータセンター | 建物(構造) | 設12 外壁、屋根等は十分な防水性能を有すること。 | コンピュータシステムに障害を及ぼさないため、外壁、屋根等は漏水の防止措置を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設13 | IV 設備基準<br>I. コンピュータセンター | 建物(構造) | 設13 外壁等に強度を持たせること。 | コンピュータ関連設備を破壊行為等から防御するため、公道等外部に面する外壁等は、強度を持たせることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設14 | IV 設備基準<br>I. コンピュータセンター | 建物(開口部) | 設14 窓には防火措置を講ずること。 | 延焼を防止するため、延焼のおそれのある窓には防火措置を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設15 | IV 設備基準<br>I. コンピュータセンター | 建物(開口部) | 設15 防犯措置を講ずること。 | コンピュータセンター建物内への不法な侵入等を防止するため、外部から容易に接近、侵入できる1階等の窓には、防犯措置を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設16 | IV 設備基準<br>I. コンピュータセンター | 建物(開口部) | 設16 常時利用する出入口は1カ所とし、出入管理設備、防犯設備を設置すること。 | 入退館管理を確実に行うことによる不法侵入の防止、不審物品の搬出入防止のため、常時利用する出入口は1カ所とし、出入管理設備、防犯設備を設置することが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |

| | | | | | |
|---|---|---|---|---|---|
| 設17 | IV 設備基準<br>I. コンピュータセンター | 建物(開口部) | 設17 非常口を設けること。 | 災害時の安全な避難と非常時持出しの円滑化のため、適切な位置に非常口を設けること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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、緊急時に全社員が安全に非難できるよう、必要な標識を掲示したり、訓練を実施したりしています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設18 | IV 設備基準<br>I. コンピュータセンター | 建物(開口部) | 設18 防水措置を講ずること。 | 浸水および漏水によるコンピュータ機器等への障害を防止するため、出入口、窓、機器の搬出入口等の開口部は、防水措置を講ずることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設19 | IV 設備基準<br>I. コンピュータセンター | 建物(開口部) | 設19 出入口の扉は、十分な強度を持たせるとともに、錠を付けること。 | 防犯・防災のため、出入口には十分な強度を有する扉を設置し、錠を付けること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設20 | IV 設備基準<br>I. コンピュータセンター | 建物(内装等) | 設20 不燃材料および防炎性能を有するものを使用すること。 | 要員およびコンピュータシステムを守るため、内装等には、建築基準法に規定する不燃材料および消防法に規定する防炎性能を有するものを使用すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設21 | IV 設備基準<br>I. コンピュータセンター | 建物(内装等) | 設21 地震による内装等の落下・損壊の防止措置を講ずること。 | 要員およびコンピュータシステムに被害を及ぼさないようにするため、地震による内装等の落下・損壊の防止措置を講ずることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>Google は、データセンターが所在する地域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 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室(位置) | 設22 災害を受けるおそれの少ない位置に設置すること。 | コンピュータシステムへの影響を防止するため、地震、火災、浸水等の災害を受けるおそれの少ない位置に設置すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域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 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室(位置) | 設23 外部から容易に入れない位置に設置すること。 | 侵入、破壊、機密漏洩等を防止するため、出入口付近およびエレベータまたは階段で直接入れる位置を避けて設置すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設24 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室(位置) | 設24 室名等の表示は付さないこと。 | 侵入、破壊、機密漏洩等を防止するため、コンピュータ室・データ保管室の室名等の表示は付さないこと。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 設25 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(位置) | 設25 必要空間を確保すること。 | 保守、避難のため、必要空間を確保すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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、緊急時に全社員が安全に非難できるよう、必要な標識を掲示したり、訓練を実施したりしています。<br><br>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。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設26 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(位置) | 設26 専用の独立した室とすること。 | 安全管理の徹底のため、専用の独立した室とすること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設27 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(開口部) | 設27 常時利用する出入口は1カ所とし、前室を設けること。 | 入退室管理を確実に行うため、常時利用する出入口は1カ所とすることが望ましい。また、安全性を保ち、外部からの熱、湿気、塵埃の侵入を防止するため、常時利用する出入口には、前室を設けることが望ましい。 | | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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、緊急時に全社員が安全に非難できるよう、必要な標識を掲示したり、訓練を実施したりしています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設28 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(開口部) | 設28 出入口の扉は、十分な強度を持たせるとともに、錠を付けること。 | 防犯・防災のため、出入口には十分な強度を有する扉を設置し、錠を付けること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設29 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(開口部) | 設29 窓に防火、防水、破損防止措置を講じ、外部から室内の機器等が見えない措置を講ずること。 | 防犯・防災のため、窓を設ける場合は防火・防水措置および窓ガラスの破損防止措置を講じ、さらに外部から室内の機器等が見えない措置を講ずること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設30 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(開口部) | 設30 非常口、避難器具、誘導灯等を設置すること。 | 災害時の避難と非常持出しの円滑化のため、コンピュータ室には適切な位置に非常口および避難器具を設置すること。また、非常口への誘導灯および誘導標識を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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、緊急時に全社員が安全に非難できるよう、必要な標識を掲示したり、訓練を実施したりしています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設31 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(構造・内装等) | 設31 独立した防火区画とすること。 | 建物内他区画からの火災の延焼防止のため、コンピュータ室・データ保管室は、建築基準法に規定する独立した防火区画とすること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 設32 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(構造・内装等) | 設32 漏水防止対策を講ずること。 | 建物、設備等の損傷およびコンピュータ機器等に対する障害を未然に防止するため、天井、壁、床面からの漏水防止対策を講ずること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設33 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(構造・内装等) | 設33 静電気の防止措置を講ずること。 | コンピュータシステムへの悪影響を防止するため、コンピュータ室の床表面材料は、静電気の発生、帯電等による影響を防止する措置を講ずること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設34 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(構造・内装等) | 設34 内装等には不燃材料および防炎性能を有するものを使用すること。 | 要員およびコンピュータシステムを火災による被害から守るため、内装等には、建築基準法に規定する不燃材料および消防法に規定する防炎性能を有するものを使用すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設35 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(構造・内装等) | 設35 地震による内装等の落下・損壊の防止措置を講ずること。 | 要員およびコンピュータシステムへ被害を及ぼさないようにするため、間仕切壁、天井、照明器具等、地震の際に落下・損壊の危険のあるものは、落下・損壊防止措置を講ずること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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、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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設36 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(構造・内装等) | 設36 フリーアクセス床は地震時に損壊しない構造とすること。 | 地震時に損壊することのないよう、フリーアクセス床は耐震措置を講ずること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域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 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設37 自動火災報知設備を設置すること。 | 火災が発生した場合、早期に発見、通報して、初期消火や避難等ができるように、適切な自動火災報知設備を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設38 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設38 非常時の連絡装置を設置すること。 | 火災等の異常事態の発生を知らせ、初期消火、避難等について適切な指示を与えるため、非常時の連絡装置を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設39 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設39 消火設備を設置すること。 | 火災時に備えて、適切な消火設備を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers |

| | | | | | | |
|---|---|---|---|---|---|---|
| 設40 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設40 ケーブルの難燃化、延焼防止措置を講ずること。 | ケーブルの燃焼・延焼を防止するため、ケーブルの難燃化措置を講ずることが望ましい。また、防火壁、床等のケーブル貫通部分は延焼防止措置を講ずること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設41 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設41 排煙設備を設置すること。 | 火災時に備えて、必要な排煙設備を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設42 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設42 非常用照明設備、携帯用照明器具を設置すること。 | 火災等の異常事態発生時に室内要員が安全に避難できるように、コンピュータ室には、非常用照明設備および携帯用照明器具を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設43 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設43 水使用設備を設置しないこと。 | 漏水によるコンピュータシステムへの影響を防止するため、コンピュータ室・データ保管室に水使用設備を設置しないこと。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設44 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設44 地震感知器を設置すること。 | コンピュータシステムの運転継続を判断し、データ破壊や電気火災等の二次災害発生を防止するため、コンピュータ室には地震感知器を設置することが望ましい。 | | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設45 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設45 出入口には出入管理設備、防犯設備を設置すること。 | 不法侵入を防止するため、コンピュータ室・データ保管室の出入口には入退室者を識別、記録する出入管理設備を設置すること。さらに、防犯設備を設置することが望ましい。 | | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設46 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設46 温湿度自動記録装置または温湿度警報装置を設置すること。 | コンピュータシステムの予防保全、障害時の原因分析のため、温湿度自動記録装置または温湿度警報装置を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設47 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(設備) | 設47 ネズミの害を防止する措置を講ずること。 | ネズミによってケーブルが害を受けることを防止するため、適切な措置を講ずることが望ましい。 | | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設48 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室<br>(コンピュータ機器、什器・備品) | 設48 什器・備品は不燃性とすること。 | 引火と火災拡大を防止するため、什器・備品はスチール製品等の不燃性とすること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |

| | | | | | |
|---|---|---|---|---|---|
| 設49 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室(コンピュータ機器、什器・備品) | 設49 静電気防止措置を講ずること。 | コンピュータシステムへの悪影響を防止するため、コンピュータ機器、什器・備品は、静電気防止措置を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設50 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室(コンピュータ機器、什器・備品) | 設50 耐震措置を講ずること。 | 地震の際に要員やコンピュータ機器に影響を与えないよう、コンピュータ機器および什器等の耐震措置を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域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 | IV 設備基準<br>I. コンピュータセンター | コンピュータ室・データ保管室(コンピュータ機器、什器・備品) | 設51 運搬車等に固定装置を取り付けること。 | 地震の際に要員やコンピュータ機器に損傷を与えないよう、磁気テープ、磁気ディスク等の運搬車等は、制動または固定する装置を取り付けること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域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 | IV 設備基準<br>I. コンピュータセンター | 電源室・空調機械室 | 設52 災害を受けるおそれの少ない場所に設置すること。 | コンピュータシステムへの影響を防止するため、地震、火災、浸水等の災害を受けるおそれの少ない場所に設置すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域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 | IV 設備基準<br>I. コンピュータセンター | 電源室・空調機械室 | 設53 保守点検に必要な空間を確保すること。 | 機器、装置等の保守点検および災害時の避難のため、必要な広さ、高さの空間を確保すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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、緊急時に全社員が安全に非難できるよう、必要な標識を掲示したり、訓練を実施したりしています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設54 | IV 設備基準<br>I. コンピュータセンター | 電源室・空調機械室 | 設54 専用の独立した室とすること。 | 保守管理および障害の拡大防止のため、他の室とは独立した専用の室とすることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設55 | IV 設備基準<br>I. コンピュータセンター | 電源室・空調機械室 | 設55 無窓とし、錠を付けた扉を設置すること。 | 外部からの侵入防止、防火、防水のため、無窓とすることが望ましく、錠を付けた扉を設置すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設56 | IV 設備基準<br>I. コンピュータセンター | 電源室・空調機械室 | 設56 耐火構造とすること。 | 火災による延焼防止のため、耐火構造とすること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設57 | IV 設備基準<br>I. コンピュータセンター | 電源室・空調機械室 | 設57 自動火災報知設備を設置すること。 | 早期に火災を発見するため、自動火災報知設備を設置すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 設58 | IV 設備基準<br>I. コンピュータセンター | 電源室・空調機械室 | 設58 ガス系消火設備を設置すること。 | 火災時に備えて、全域放出型のガス系消火設備を設置することが望ましい。 | | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設59 | IV 設備基準<br>I. コンピュータセンター | 電源室・空調機械室 | 設59 空調設備の漏水防止措置を講ずること。 | 漏水による障害を回避するため、冷却水の水漏れ、結露等による漏水の防止措置を講ずること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設60 | IV 設備基準<br>I. コンピュータセンター | 電源室・空調機械室 | 設60 ケーブル、ダクトからの延焼防止措置を講ずること。 | 延焼を防止するため、ケーブル、ダクトからの延焼防止措置を講ずること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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/security/whitepaper#state-of-the-art_data_centers<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設61 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設61 電源設備の容量には余裕を持たせること。 | コンピュータシステムに必要な電力を安定的に供給するため、電源設備の容量には余裕を持たせること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設62 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設62 電源は複数回線で引き込むこと。 | 受電設備の障害時に備え、電源は複数回線で引き込むことが望ましい。 | | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設63 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設63 良質な電力を供給する設備を設置すること。 | コンピュータシステムを安定稼働させるため、良質な電力を供給する設備を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設64 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設64 自家発電設備、蓄電池設備を設置すること。 | 停電時でもコンピュータシステムを継続して稼働させるため、自家発電設備及び蓄電池設備を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設65 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設65 電源設備には避雷設備を設置すること。 | 落雷による被害を防止するため、電源設備には避雷設備を設置すること。 | | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |

| | | | | | |
|---|---|---|---|---|---|
| 設66 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設66 電源設備には耐震措置を講ずること。 | 地震による移動、損傷等を防止するため、電源設備には耐震措置を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域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 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設67 分電盤からコンピュータ機器への電源の引込みは専用とすること。 | コンピュータシステムへの影響を最小限にするため、コンピュータ機器への電源の引込みは専用分電盤から専用回路にて配線すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設68 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設68 負荷変動の激しい機器との共用を避けること。 | コンピュータシステムに安定して電力を供給するため、コンピュータシステムと負荷変動の激しい機器との電源系統は分けること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設69 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設69 コンピュータシステムのアースは適切に施工すること。 | 電源設備や電気機器等からの影響を防止するため、コンピュータシステムのアースは適切に施工すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設70 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設70 過電流、漏電により各機器に障害を及ぼさないよう措置を講ずること。 | 各機器に障害を及ぼさないように、過電流や漏電への措置を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設71 | IV 設備基準<br>I. コンピュータセンター | 電源設備 | 設71 防災、防犯設備用の予備電源を設置すること。 | 停電した場合でも防災、防犯設備が作動するように、予備電源を設置すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設72 | IV 設備基準<br>I. コンピュータセンター | 空調設備 | 設72 空調設備の能力には余裕を持たせること。 | コンピュータ室の温湿度を適切に調整するため、空調設備の能力には余裕を持たせること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設73 | IV 設備基準<br>I. コンピュータセンター | 空調設備 | 設73 空調設備は安定的に空気調和できる措置を講ずること。 | コンピュータシステムの継続した運用を確保するため、空調設備には安定的に空気調和ができる措置を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設74 | IV 設備基準<br>I. コンピュータセンター | 空調設備 | 設74 空調設備はコンピュータ室専用とすること。 | コンピュータ室の温湿度制御を的確に行うため、空調設備は他の室との共用を避けコンピュータ室専用とすること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設75 | IV 設備基準<br>I. コンピュータセンター | 空調設備 | 設75 空調設備の予備を設置すること。 | 障害の発生に備えて、主要な空調設備機器については予備を設置することが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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 Suite のお客様の業務が中断されることはありません。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設76 | IV 設備基準<br>I. コンピュータセンター | 空調設備 | 設76 空調設備には自動制御装置、異常警報装置を設置すること。 | 空調設備を安定的に稼働させるため、各種の自動制御装置のほか、機器の異常を迅速に検知する異常警報装置を設置すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |

| | | | | | |
|---|---|---|---|---|---|
| 設77 | IV 設備基準<br>I. コンピュータセンター | 空調設備 | 設77 空調設備には侵入、破壊防止対策を講ずること。 | コンピュータシステムの運用に支障を来さないようにするため、空調設備には侵入、破壊に対する防止対策を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設78 | IV 設備基準<br>I. コンピュータセンター | 空調設備 | 設78 空調設備には耐震措置を講ずること。 | 地震による移動、損傷等を防止するため、空調設備には耐震措置を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google は、データセンターが所在する地域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 | IV 設備基準<br>I. コンピュータセンター | 空調設備 | 設79 空調設備の断熱材料、給排気口は不燃材料とすること。 | 火災時の空調設備の損傷を防止するため、空調設備のダクト等の断熱材料および給排気口は不燃材料とすること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設80 | IV 設備基準<br>I. コンピュータセンター | 監視制御設備 | 設80 監視制御設備を設置すること。 | 障害発生等を早期に発見するため、電源設備、空調設備、防災設備、防犯設備等の監視制御設備を設置すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設81 | IV 設備基準<br>I. コンピュータセンター | 監視制御設備 | 設81 中央管理室を設置すること。 | 電源設備、空調設備、防災設備、防犯設備等の運営管理を円滑にし、かつ有効活用を図るため、これらの設備を集中管理する中央管理室を設置することが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設82 | IV 設備基準<br>I. コンピュータセンター | 回線関連設備 | 設82 回線関連設備には錠をつけること。 | 不正アクセス、破壊等の不法行為を防止するため、コンピュータ室外に設置される回線関連設備の機器収容架等には錠を付けること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設83 | IV 設備基準<br>I. コンピュータセンター | 回線関連設備 | 設83 回線関連設備の設置場所の表示は付さないこと。 | 部外者に回線関連設備の設置場所を知らせないため、設置場所の表示は付さないこと。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 設83-1 | IV 設備基準<br>I. コンピュータセンター | 回線関連設備 | 設83-1 回線は、専用の配線スペースに設けること。 | 回線を障害および犯罪から防護し、また、他の電源ケーブル等からのノイズの混入を防止するため、専用の配線スペースに設けることが望ましい。 | | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0<br><br>Google は、データセンターが所在する地域の建築要件と設備要件をすべて遵守しています。 |
| 設84 | IV 設備基準<br>II. 本部・営業店等 | 建物(周囲) | 設84 敷地内の通信回線・電力線の切断・延焼の防止措置を講ずること。 | コンピュータシステムのサービス中断を防止するため、敷地内の通信回線・電力線は、切断・延焼の防止措置を講ずることが望ましい。 | | 対象外 |
| 設85 | IV 設備基準<br>II. 本部・営業店等 | 建物(構造) | 設85 耐火建築物であること。 | 防火対策のため、建物は建築基準法に規定する耐火建築物であることが望ましい。 | | 対象外 |
| 設86 | IV 設備基準<br>II. 本部・営業店等 | 建物(構造) | 設86 構造の安全性を有すること。 | 構造の安全性を確保するため、建物は建築基準法の規定に従うこと。 | | 対象外 |
| 設87 | IV 設備基準<br>II. 本部・営業店等 | 建物(構造) | 設87 外壁、屋根等は十分な防水性能を有すること。 | 漏水を防止するため、十分な防水性能を有するように措置を講ずること。 | | 対象外 |
| 設88 | IV 設備基準<br>II. 本部・営業店等 | 建物(構造) | 設88 外壁等の強度を確保すること。 | 破壊侵入等を防御するため、公道等外部に面する外壁は強度を持たせることが望ましい。 | | 対象外 |
| 設89 | IV 設備基準<br>II. 本部・営業店等 | 建物(開口部) | 設89 窓には防火措置を講ずること。 | 延焼を防止するため、延焼のおそれのある窓には防火措置を講ずること。 | | 対象外 |
| 設90 | IV 設備基準<br>II. 本部・営業店等 | 建物(開口部) | 設90 窓・扉には防犯措置を講ずること。 | 不法な侵入等を防止するため、外部から容易に接近、侵入できる窓・扉には、防犯措置を講ずること。 | | 対象外 |
| 設91 | IV 設備基準<br>II. 本部・営業店等 | 建物(開口部) | 設91 出入口の扉は十分な強度を持たせるとともに、錠を付けること。 | 防犯、防災のため、出入口には十分な強度を有する扉を設置し、錠を付けること。 | | 対象外 |
| 設92 | IV 設備基準<br>II. 本部・営業店等 | 建物(開口部) | 設92 通用口には、入室者の識別設備を設置すること。 | 不法侵入を防止するため、営業時間外に利用する通用口には、インターホン等室内から相手確認ができる識別装置を設置すること。 | | 対象外 |
| 設93 | IV 設備基準<br>II. 本部・営業店等 | 建物(開口部) | 設93 出入口には防水措置を講ずること。 | 雨水等の浸水を防止するため、出入口には防水措置を講ずることが望ましい。 | | 対象外 |
| 設94 | IV 設備基準<br>II. 本部・営業店等 | 建物(内装等) | 設94 天井および壁は、遮熱、吸音機能を持たせること。 | 端末機器等を正常に機能させるため、天井および壁は遮熱機能および吸音機能を持たせることが望ましい。 | | 対象外 |
| 設95 | IV 設備基準<br>II. 本部・営業店等 | 建物(内装等) | 設95 地震による内装等の落下・損壊の防止措置を講ずること。 | 人身および端末機器等へ被害を及ぼさないようにするため、天井、壁、照明器具等、地震の際に落下・損壊の危険のあるものは、落下・損壊防止措置を講ずること。 | | 対象外 |
| 設96 | IV 設備基準<br>II. 本部・営業店等 | 建物(内装等) | 設96 床表面は、塵埃や静電気が発生しにくい材質のものとすること。 | 端末機器等への悪影響を防止するため、床表面は塵埃や静電気が発生しにくい材質のものが望ましい。 | | 対象外 |
| 設97 | IV 設備基準<br>II. 本部・営業店等 | 建物(内装等) | 設97 端末機器への回線等は、切断のおそれのない措置を講ずること。 | 通行時に切断することのないよう、端末機器への回線、電源ケーブル等は適切な位置に布設すること。 | | 対象外 |
| 設98 | IV 設備基準<br>II. 本部・営業店等 | 建物(内装等) | 設98 端末機器に接続している回線、電源ケーブル等への漏水防止対策を講ずること。 | 事故による漏水等でシステムが停止しないよう、端末機器に接続している回線、電源ケーブル等は漏水防止対策を講ずることが望ましい。 | | 対象外 |
| 設99 | IV 設備基準<br>II. 本部・営業店等 | 建物(設備) | 設99 自動火災報知設備および消火器を設置すること。 | 火災が発生した場合、早期に発見、通報して、初期消火や避難ができるように、煙感知器等を用いた自動火災報知設備および消火器を設置すること。 | | 対象外 |
| 設100 | IV 設備基準<br>II. 本部・営業店等 | 建物(設備) | 設100 設備等の耐震措置を講ずること。 | 端末機器等に影響を与えないよう、什器、備品等は耐震措置を講ずることが望ましい。 | | 対象外 |
| 設101 | IV 設備基準<br>II. 本部・営業店等 | 建物(設備) | 設101 耐火金庫を設置すること。 | 火災等の災害に起因するシステム障害の影響を最小限にするため、耐火金庫、耐火キャビネット等のデータ保管庫を設置し、復旧に必要な媒体、資料等のデータを保管すること。 | | 対象外 |
| 設102 | IV 設備基準<br>II. 本部・営業店等 | 建物(設備) | 設102 避雷設備を設置すること。 | 落雷によるコンピュータシステムの障害、室内にいる人の感電死傷、火災等の事故を防止するため、周囲に高い建物がない場合は避雷設備を設置することが望ましい。 | | 対象外 |
| 設103 | IV 設備基準<br>II. 本部・営業店等 | 建物(設備) | 設103 防犯措置を講ずること。 | 犯罪の未然防止と発生時の対応のため、防犯カメラ、非常通報装置等の防犯措置を講ずること。 | | 対象外 |
| 設104 | IV 設備基準<br>II. 本部・営業店等 | 建物(回線関連設備) | 設104 回線関連設備の設置場所の表示は付さないこと。 | 部外者に回線関連設備の設置場所を知らせないため、回線関連設備の設置場所の表示は付さないこと。 | | 対象外 |
| 設105 | IV 設備基準<br>II. 本部・営業店等 | 建物(回線関連設備) | 設105 回線関連設備には錠を付けること。 | 不正アクセス、破壊等の不法行為を防止するため、関係者以外に触れやすい場合には錠を付けること。 | | 対象外 |
| 設106 | IV 設備基準<br>II. 本部・営業店等 | 建物(回線関連設備) | 設106 回線関連設備から各端末機器までの配線を二重化すること。 | 回線障害時に迅速に対応するため、回線関連設備から各端末機器までの配線を二重化することが望ましい。 | | 対象外 |
| 設107 | IV 設備基準<br>II. 本部・営業店等 | 建物(電源設備) | 設107 電源ケーブルは、端末機器等に支障を来さないよう布設すること。 | 端末機器等に支障を来さないようにするため、電源ケーブルは分電盤から直接布設するか、他の機器の影響を受けないように布設すること。 | | 対象外 |
| 設108 | IV 設備基準<br>II. 本部・営業店等 | 建物(電源設備) | 設108 防災、防犯設備用の予備電源を設置すること。 | 停電に備えて、防災、防犯設備および非常用照明設備が作動するように予備電源を設置すること。 | | 対象外 |
| 設109 | IV 設備基準<br>II. 本部・営業店等 | 建物(電源設備) | 設109 自家発電設備等を設置すること。 | 停電に備えて、自家発電設備等を設置することが望ましい。 | | 対象外 |
| 設110 | IV 設備基準<br>II. 本部・営業店等 | 建物(空調設備) | 設110 空調設備を設置すること。 | 端末機器等の異常動作を防止するため、端末機器台数に応じた空調設備を設置すること。 | | 対象外 |
| 設111 | IV 設備基準<br>II. 本部・営業店等 | 建物(自動機器室) | 設111 通話装置を設置すること。 | 自動機器室の機器の障害に対し迅速に対応するため、電話、インターホン等の通話装置により、障害時に営業室等との通話ができること。 | | 対象外 |
| 設112 | IV 設備基準<br>II. 本部・営業店等 | 建物(自動機器室) | 設112 非常通報装置を設置すること。 | 自動機器室で発生した非常事態に対し迅速に対応するため、非常時に営業室等への通報ができる非常通報装置を設置すること。 | | 対象外 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 設113 | IV 設備基準<br>II. 本部・営業店等 | 建物(自動機器室) | 設113 防犯措置を講ずること。 | 自動機器室の安全を確保するため、設置形態と周辺の環境に応じて、自動機器室の防犯設備と自動機器本体の防犯措置等とを適切に組み合わせた防犯対策を講ずること。 | | 対象外 |
| 設114 | IV 設備基準<br>II. 本部・営業店等 | 建物(自動機器室) | 設114 照明設備および非常用照明設備を設置すること。 | 自動機器室における各種犯罪を未然に防止するため、室内の状況が外部から確認できるように、十分な照度の照明設備を設置すること。 | | 対象外 |
| 設115 | IV 設備基準<br>II. 本部・営業店等 | 建物(自動機器室) | 設115 扉は、一部を素通しにすること。 | 各種犯罪を未然に防止するため、扉は外部から内部が見えるように、一部を素通しにすること。 | | 対象外 |
| 設116 | IV 設備基準<br>II. 本部・営業店等 | 建物(自動機器室) | 設116 自動機器の現金の装填と保守のための必要な空間を確保すること。 | 現金の安全な装填と保守のために、必要な空間を自動機器後面に確保することが望ましい。 | | 対象外 |
| 設117 | IV 設備基準<br>II. 本部・営業店等 | 建物(自動機器室) | 設117 自動運行設備を設置すること。 | 無人運用を適切に行うため、必要な自動運行設備を設置することが望ましい。 | | 対象外 |
| 設118 | IV 設備基準<br>II. 本部・営業店等 | 建物(端末機器) | 設118 端末機器には耐震措置を講ずること。 | 端末機器の移動、転倒による故障や破損を防止するとともに要員を保護するために、移動や転倒を防止する措置を講ずることが望ましい。 | | 対象外 |
| 設119 | IV 設備基準<br>II. 本部・営業店等 | 建物(端末機器) | 設119 機器のアースを確実に取ること。 | 機器の保護のために、アースの必要な機器は必ずアースを分電盤から取ること。 | | 対象外 |
| 設120 | IV 設備基準<br>II. 本部・営業店等 | 建物(端末機器) | 設120 漏水および塵埃等に対する保護措置をとること。 | 水滴や塵埃等から機器を防護するために、防水カバー等の必要な措置をとることが望ましい。 | | 対象外 |
| 設121 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(位置) | 設121 災害を受けるおそれの少ない位置とすること。 | コンピュータシステムへの影響を防止するため、地震、火災、浸水等の災害を受けるおそれの少ない位置とすることが望ましい。 | | 対象外 |
| 設122 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(位置) | 設122 外部から容易に入れない位置とすること。 | 侵入、破壊、機密漏洩等を防止するため、出入口付近およびエレベータまたは階段で直接入れる位置を避けて設置することが望ましい。 | | 対象外 |
| 設123 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(位置) | 設123 室名等の表示は付さないこと。 | 侵入、破壊、機密漏洩等を防止するため、室名等の表示は付さないことが望ましい。 | | 対象外 |
| 設124 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(位置) | 設124 専用の区画とすること。 | 安全管理の徹底のため、専用の区画とすることが望ましい。 | | 対象外 |
| 設125 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(構造・内装等) | 設125 防火区画に設置すること。 | 建物内他区画の火災による延焼防止のため、建築基準法に規定する防火区画内に位置することが望ましい。 | | 対象外 |
| 設126 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(構造・内装等) | 設126 漏水防止対策を講ずること。 | 漏水によるサーバー等の被害を未然に防止するため、天井、壁、床面からの漏水防止対策を講ずることが望ましい。 | | 対象外 |
| 設127 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(構造・内装等) | 設127 フリーアクセス床は地震に備えて耐震措置を講ずること。 | フリーアクセス床は地震時に損壊することのないよう耐震措置を講ずることが望ましい。 | | 対象外 |
| 設128 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(設備) | 設128 消防設備を有すること。 | 火災によるサーバー等の被害を防止するため、必要な消防設備を設置することが望ましい。 | | 対象外 |
| 設129 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(設備) | 設129 地震感知器を設置すること。 | 運転継続の判断のため、サーバー設置場所に地震感知器を設置することが望ましい。 | | 対象外 |
| 設130 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(設備) | 設130 サーバーを設置した室の出入口には出入管理設備、防犯設備を設置すること。 | 不法侵入を防止するため、サーバーを設置した室の出入口には出入管理設備、防犯設備を設置することが望ましい。 | | 対象外 |
| 設131 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(設備) | 設131 温湿度自動記録装置または温湿度警報装置を設置すること。 | コンピュータシステムの予防保全、障害時の原因分析のため、温湿度自動記録装置または温湿度警報装置を設置することが望ましい。 | | 対象外 |
| 設132 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(設備) | 設132 空調設備を設置すること。 | 適切な温湿度条件を確保するため、専用空調を設置することが望ましい。 | | 対象外 |
| 設133 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(設備) | 設133 ネズミの害を防止する措置を講ずること。 | ネズミによってケーブルが害を受けることを防止するため、適切な措置を講ずることが望ましい。 | | 対象外 |
| 設134 | IV 設備基準<br>II. 本部・営業店等 | サーバー設置場所(設備) | 設134 電源コンセントの抜け防止対策を講ずること。 | 電源プラグが簡単にはずれることのないようにするため、電源コンセントの抜け防止対策を講ずること。 | | 対象外 |
| 設135 | IV 設備基準<br>II. 本部・営業店等 | インストアブランチ | 設135 他の区画からの侵入防止措置を講ずること。 | 破壊侵入等を防御するため、インストアブランチの区画はストアの他の区画から独立した防犯区画とすること。 | | 対象外 |
| 設136 | IV 設備基準<br>II. 本部・営業店等 | インストアブランチ | 設136 使用するストアの設備状況に応じて、適切な補強策を講ずること。 | 破壊侵入等を防御するため、ストアの既設施設が金融機関等が求める基準と相違する場合には、設備の補強や運用面での対策を実施すること。 | | 対象外 |
| 設137 | IV 設備基準<br>III. 流通・小売店舗との提携チャネル | コンビニATM | 設137 防犯措置を講ずること。 | コンビニATMの安全を確保するため、設置形態と周辺の環境に応じて、防犯設備とATM本体の防犯措置等とを適切に組み合わせた防犯対策を講ずること。 | | 対象外 |

**運用**

| 項番 | 基準大項目 | 基準中項目 | 基準小項目 | 適用にあたっての考え方 | | Google の回答 |
|---|---|---|---|---|---|---|
| 運1 | V. 運用基準 | 管理体制の確立(セキュリティ管理と責任の明確化) | 運1 セキュリティ管理方法を具体的に定めた文書を整備すること。 | セキュリティ管理を適切に行うため、セキュリティ管理の具体的手順、責任等を明確にした文書を整備すること。 | | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 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。<br><br>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。<br><br>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 | V. 運用基準 | 管理体制の確立(セキュリティ管理と責任の明確化) | 運2 セキュリティ管理方法を具体的に定めた文書の評価と改訂を行うこと。 | セキュリティ管理の方法を最適なものとするため、作成された文書については、業務の実態にあっているかを定期的に評価し、必要に応じて改訂すること。 | | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 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。<br><br>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。<br><br>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 | V. 運用基準 | 管理体制の確立(セキュリティ管理と責任の明確化) | 運3 セキュリティ管理体制を整備すること。 | セキュリティ管理を適切に行うため、セキュリティ管理の責任者等を定め、その職務範囲と権限及び責任について定めること。 | | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 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。<br><br>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。<br><br>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 | V．運用基準 | 管理体制の確立(セキュリティ管理と責任の明確化) | 運4　システム管理体制を整備すること。 | システムの安全かつ円滑な運用と不正防止のため、システムの管理手順を定め、管理体制を整備すること。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 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。<br><br>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。<br><br>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 | V．運用基準 | 管理体制の確立(セキュリティ管理と責任の明確化) | 運5　データ管理体制を整備すること。 | データの安全かつ円滑な運用と不正防止のため、データ管理手順を定め、管理体制を整備すること。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 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。<br><br>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。<br><br>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 | V．運用基準 | 管理体制の確立(セキュリティ管理と責任の明確化) | 運6　ネットワーク管理体制を整備すること。 | コンピュータネットワークの適切かつ効率的な運用と不正アクセス等の防止のため、ネットワークの管理手順を定め、管理体制を整備すること。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 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。<br><br>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。<br><br>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 | V．運用基準 | 管理体制の確立(組織の整備) | 運7　防災組織を整備すること。 | 災害の予防および被害軽減のため、防災組織を整備し、責任者を明確にすること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2）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。<br><br>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。<br><br>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。<br><br>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 | V．運用基準 | 管理体制の確立(組織の整備) | 運8　防犯組織を整備すること。 | 犯罪を防止するため、防犯組織を整備し、責任者を明確にすること。 | 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。<br><br>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。<br><br>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 | V．運用基準 | 管理体制の確立(組織の整備) | 運9　業務組織を整備すること。 | コンピュータシステムに係わる業務を円滑かつ適正に運営するとともに、不正を防止するため、業務範囲および責任と権限を明確にし、相互牽制体制を整備すること。 | 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。<br><br>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。<br><br>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 | V．運用基準 | 管理体制の確立(各種規定の整備) | 運10　各種規定を整備すること。 | コンピュータシステムを円滑かつ適正に運用、管理するため、防災、防犯、業務の各組織における責任と権限を明確にした規定を整備すること。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001:2013、附属書 A 5）、「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6）、「運用の手順および責任」(ISO 27001:2013、附属書 A.12.1）が規定されています。<br><br>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。<br><br>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 | V．運用基準 | 管理体制の確立(セキュリティ遵守状況の確認) | 運10-1　セキュリティ遵守状況を確認すること。 | セキュリティ関連文書に定められた事項の遵守状況を確認し、全役職員(外部要員を含む)のセキュリティポリシーに対する意識やセキュリティレベルの向上を図ること。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO27002:2013、附属書 A.7 2 2）が規定されています。<br><br>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。<br><br>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。<br><br>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 | V．運用基準 | 入退管理(入退館(室)管理) | 運11　資格付与および鍵の管理を行うこと。 | コンピュータセンターへの入館者、およびコンピュータ室、データ保管室等重要な室への入室者を特定するため、資格付与と鍵の管理を行うこと。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0" |

| | | | | | |
|---|---|---|---|---|---|
| 運12 | V．運用基準 | 入退管理(入退館(室)管理) | 運12　入退館管理を行うこと。 | 不法侵入、危険物持込み、不法持出し等を防止するため、入退館者の資格確認により、コンピュータセンターの入退館管理を行うこと。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0" |
| 運13 | V．運用基準 | 入退管理(入退館(室)管理) | 運13　入退室管理を行うこと。 | 不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室及びデータ保管室等重要な室については、資格確認により入退室管理を行うこと。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0" |
| 運14 | V．運用基準 | 運用管理(マニュアルの整備) | 運14　通常時マニュアルを整備すること。 | コンピュータシステムを正確かつ安全に運用するとともに、本部・営業店等設置の端末機器の誤操作を予防し、事務処理を円滑に行うため、通常時における各種手順(含む操作手順)を定めたマニュアルを整備すること。 | 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。<br><br>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。<br><br>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 | V．運用基準 | 運用管理(マニュアルの整備) | 運15　障害時・災害時マニュアルを整備すること。 | 障害・災害によるコンピュータシステムへの影響の極小化と早期復旧ならびに本部・営業店等における業務継続のため、障害時・災害時における代替措置、復旧手順及び対応方法等について定めたマニュアルを整備すること。 | 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。<br><br>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。<br><br>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 | V．運用基準 | 運用管理(アクセス権限の管理) | 運16　各種資源、システムへのアクセス権限を明確にすること。 | 無資格者によるアクセスを防止するため、コンピュータシステムと、システムの運用上及び業務上重要なファイルは、アクセス権限所有者を特定すること。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A 9）が規定されています。<br><br>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。<br><br>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。<br><br>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 | V．運用基準 | 運用管理(アクセス権限の管理) | 運17　パスワードが他人に知られないための措置を講じておくこと。 | パスワード等の漏洩防止のため、他人に知られないための注意喚起等の措置を講じておくこと。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A 9）が規定されています。<br><br>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。<br><br>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。<br><br>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 | V．運用基準 | 運用管理(アクセス権限の管理) | 運18　各種資源、システムへのアクセス権限の付与、見直し手続きを明確化すること。 | 各種資源、システムへのアクセスを管理するため、アクセス権限を与えるにあたってその手続きを明確に定めることが必要である。さらに、アクセス権限を適切に保つため、見直しの手続きを明確化することが必要である。 | 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。<br><br>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。<br><br>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。<br><br>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 | V．運用基準 | 運用管理(オペレーション管理) | 運19　オペレータの資格確認を行うこと。 | コンピュータシステムの不正使用を防止するため、オペレータの資格確認を行うこと。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A 9）が規定されています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(オペレーション管理) | 運20 オペレーションの依頼・承認手続きを明確にすること。 | コンピュータシステムの不正使用を防止するため、オペレーションの依頼・承認手続きを明確にすること。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A 9)が規定されています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(オペレーション管理) | 運21 オペレーション実行体制を明確にすること。 | コンピュータシステムの誤操作および不正使用を防止するため、オペレーション実行体制を明確にすること。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A 9)が規定されています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(オペレーション管理) | 運22 オペレーションの記録、確認を行うこと。 | オペレーションの正当性を検証するため、オペレーションの記録、確認を行うこと。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A 9)が規定されています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(オペレーション管理) | 運23 クライアントサーバー・システムにおける作業の管理を行うこと。 | クライアントサーバー・システムにおける不正使用等を防止するため、依頼、承認等の手続きを明確にし、実行、記録、結果確認等を適切に管理することが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A 9)が規定されています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(入力管理) | 運24 データの入力管理を行うこと。 | データの正確な処理と不正防止のため、入力手順を定めること。 | 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。<br><br>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 | V. 運用基準 | 運用管理(データファイル管理) | 運25 授受・管理方法を定めること。 | データファイルの不正使用、改ざん、紛失等を防止するため、データファイルの授受、保管は定められた方法によって行うこと。 | 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。<br><br>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 | V. 運用基準 | 運用管理(データファイル管理) | 運26 修正管理方法を明確にすること。 | 不正使用・改ざんを防止するため、データファイルに不整合が生じた場合のデータファイルの修正および管理は、定められた方法で行うこと。 | 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。<br><br>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 | V. 運用基準 | 運用管理(データファイル管理) | 運27 バックアップを確保すること。 | 重要なデータファイルの障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12 3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(プログラムファイル管理) | 運28 管理方法を明確にすること。 | プログラムの改ざん、破壊等を防止するため、プログラムファイルの管理は、定められた方法によって行うこと。 | 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。<br><br>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 | V. 運用基準 | 運用管理(プログラムファイル管理) | 運29 バックアップを確保すること。 | プログラムの障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12 3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(コンピュータウイルス対策) | 運30 コンピュータウイルス対策を講ずること。 | コンピュータウイルス等の侵入および感染に備えて、防御、検知、復旧の手順を明確にしておくこと。 | 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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(ネットワーク設定情報管理) | 運31 設定情報の管理を行うこと。 | ネットワーク機器の設定情報が不正に変更されないように管理を行うこと。 | 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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(ネットワーク設定情報管理) | 運32 設定情報のバックアップを確保すること。 | ネットワーク設定情報の不正な変更、障害や災害等への対応のため、バックアップを取得し、管理方法を明確にすること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12 3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(ドキュメント管理) | 運33 保管管理方法を明確にすること。 | 不正使用、改ざん、紛失等を防止するため、ドキュメントは定められた方法によって管理すること。 | 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。<br><br>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 | V. 運用基準 | 運用管理(ドキュメント管理) | 運34 バックアップを確保すること。 | 災害時の復旧対応のため、復旧に必要なドキュメントはバックアップを取得し、管理方法を明確にすること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12 3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(帳票管理) | 運35 未使用重要帳票の管理方法を明確にすること。 | 不正使用を防止するため、未使用重要帳票の在庫管理および廃棄は定められた方法によって行うこと。 | 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 | V. 運用基準 | 運用管理(帳票管理) | 運36 重要な印字済帳票の取扱方法を明確にすること。 | 不正使用を防止するため、重要な印字済帳票の受渡しおよび廃棄は定められた方法によって行うこと。 | 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 | V. 運用基準 | 運用管理(出力管理) | 運37 出力情報の作成、取扱いについて、不正防止および機密保護対策を講ずること。 | 出力情報の改ざん、盗難、漏洩等を防止するため、作成、取扱い等にあたっては不正防止および機密保護対策を講ずること。 | 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 | V. 運用基準 | 運用管理(取引の管理) | 運38 各取引の操作権限を明確にすること。 | 端末機操作による不正、不当取引を防止するため、取引内容ごとに端末機操作者等が操作できる権限の範囲を明確にすること。 | 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 | V. 運用基準 | 運用管理(取引の管理) | 運39 オペレータカードの管理を行うこと。 | 端末機操作による不正取引を防止するため、オペレータカードは管理者を定め管理すること。 | 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 | V. 運用基準 | 運用管理(取引の管理) | 運40 取引の操作内容を記録・検証すること。 | 端末機操作による不正取引を防止するため、取引明細表、端末機操作記録等により、取引内容が検証できる体制を整備すること。 | 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 | V. 運用基準 | 運用管理(取引の管理) | 運41 顧客からの届出の受付体制を整備し、事故口座の管理を行うこと。 | 事故による不正使用を防止するため、口座とリンクして顧客資産の移動を可能とする機器および媒体の盗難等の届けを受け付けられる体制を整備すること。また、事故届のあった口座の管理は定められた方法により行うこと。 | 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 | V. 運用基準 | 運用管理(取引の管理) | 運42 機器および媒体の盗難、破損等に伴い、利用者が被る可能性がある損失および責任を明示すること。 | 利用者に責任と注意を喚起するため、電子的価値を蓄積する媒体および通信等に使用する機器の盗難、破損等に伴い、利用者が被る可能性がある損失および利用者側の責任についてもわかり易く明示すること。 | 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 | V. 運用基準 | 運用管理(暗号鍵の管理) | 運43 暗号鍵の利用において運用管理方法を明確にすること。 | 不正行為を防止するため、暗号鍵の利用において暗号鍵の生成、配布、使用および保管等に係わる手続きを定めておくこと。また、その管理書類等は役席者が厳重に管理すること。 | 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。<br><br>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:<br><br>https //cloud google.com/security/encryption-at-rest/<br>https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf<br><br>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 | V. 運用基準 | 運用管理(厳正な本人確認の実施) | 運44 本人確認を行うこと。 | 口座開設等を行う場合は適切な方法により本人確認を行うこと。 | 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 | V. 運用基準 | 運用管理(厳正な本人確認の実施) | 運44-1 CD・ATM等の機械式預貯金取引における正当な権限者の取引を確保すること。 | 不正払戻し防止のための措置を講ずることにより機械式預貯金払戻し等が正当な権限を有する者に対して適切に行われることを確保すること。 | 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 | V. 運用基準 | 運用管理(CD・ATM等および無人店舗の管理) | 運45 運用管理方法を明確にし、かつ不正払戻防止の措置を講ずること。 | CD・ATMおよび無人店舗の安全性を確保し、円滑に稼働させるため、運用管理方法を明確に定めること。 | 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 | V. 運用基準 | 運用管理(CD・ATM等および無人店舗の管理) | 運46 監視体制を明確にすること。 | 無人店舗における異常状態を発見するため、監視体制を明確にすること。 | 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 | V. 運用基準 | 運用管理(CD・ATM等および無人店舗の管理) | 運47 防犯体制を明確にすること。 | 無人店舗における犯罪を防止するため、防犯方法および犯罪発生時の対応方法を明確にすること。 | 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 | V. 運用基準 | 運用管理(CD・ATM等および無人店舗の管理) | 運48 障害時・災害時の対応方法を明確にすること。 | 無人店舗の円滑な運営のため、障害時・災害時の対応方法を明確にすること。 | 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 | V．運用基準 | 運用管理(CD・ATM等および無人店舗の管理) | 運49　関係マニュアルの整備を行うこと。 | 無人店舗の円滑な運営、安全確保のため、各種対応を想定した関係マニュアルを整備しておくこと。 | 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 | V．運用基準 | 運用管理(渉外端末の管理) | 運50　運用管理方法を明確にすること。 | 渉外端末の不正使用を防止するため、運用管理方法を明確にすること。 | 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 | V．運用基準 | 運用管理(カード管理) | 運51　カードの管理方法を明確にすること。 | 安全性の確保及び処理の円滑化のため、カードの発行、保管、交付、回収及び廃棄は定められた方法によって行うこと。 | 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 | V．運用基準 | 運用管理(カード管理) | 運51-1　顧客に対して犯罪に関する注意喚起を行うこと。 | 顧客並びに取引の安全性を確保するため、犯罪に関する注意喚起を行うこと。 | 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 | V．運用基準 | 運用管理(カード管理) | 運52　指定された口座のカード取引監視方法を明確にすること。 | 不正使用を防止するため、指定された口座のカード取引を監視できる方法を明確にすること。 | 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 | V．運用基準 | 運用管理(顧客データ保護) | 運53　顧客データの保護策を講ずること。 | 顧客データを保護し、適正に利用するため、管理・取扱い方法を定めること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12 3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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 | V．運用基準 | 運用管理(顧客データ保護) | 運53-1　生体認証における生体認証情報の安全管理措置を講ずること。 | 顧客を認証する手段として、生体認証を用いる場合に、生体認証情報を安全に管理するための手順を定めること。 | 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 | V．運用基準 | 運用管理(資源管理) | 運54　能力及び使用状況の確認を行うこと。 | コンピュータシステムの障害及び処理能力の低下を回避するため、各種資源の能力及び使用状況の確認を行い、適切な措置を講ずること。 | 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。<br><br>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 | V．運用基準 | 運用管理(外部接続管理) | 運55　接続契約内容を明確にすること。 | 外部との接続を安全かつ正確に行うため、回線接続によるデータ授受に係わる契約締結にあたっては、接続の方法、データフォーマット、データ内容等を明確にすること。 | 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。<br><br>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 | V．運用基準 | 運用管理(外部接続管理) | 運56　外部接続における運用管理方法を明確にすること。 | データ漏洩、不正アクセス等を防止するため、外部接続時には運用管理方法を明確にし、相手先確認、接続条件(パスワード等)の登録・変更管理などを適切に行うこと。 | 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。<br><br>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 | V．運用基準 | 運用管理(機器の管理) | 運57　管理方法を明確にすること。 | コンピュータシステムを構成する各機器の不正使用、破壊、盗難等を防止するため、定められた方法によって管理すること。 | 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。<br><br>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。<br><br>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。<br><br>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 | V．運用基準 | 運用管理(機器の管理) | 運58　ネットワーク関連機器の保護措置を講ずること。 | 不正使用、破壊、盗難等を防止するため、重要なデータを扱うシステムを構成するネットワーク機器等は、適切な保護措置が講じられていることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「装置」(ISO 27001:2013、附属書 A.11.2)が規定されています。<br><br>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。<br><br>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。<br><br>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 | V．運用基準 | 運用管理(機器の管理) | 運59　保守方法を明確にすること。 | コンピュータシステムを構成する各機器の障害を防止するため、保守点検を実施し、点検内容および結果を把握すること。 | 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 | V．運用基準 | 運用管理(運行監視) | 運60　監視体制を整備すること。 | 異常状態早期発見のため、監視対象、監視内容及び監視方法を定めること。 | 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。<br><br>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。<br><br>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 | V．運用基準 | 運用管理(コンピュータ室・データ保管室の管理) | 運61　入室後の作業を管理すること。 | 不法侵入、危険物持込み、不法持出し等を防止するため、コンピュータ室およびデータ保管室等重要な室における入室者の作業を管理すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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 | V．運用基準 | 運用管理(障害時・災害時対応策) | 運62　関係者への連絡手順を明確にすること。 | 障害時・災害時に関係者へ迅速かつ確実に連絡を行うため、連絡手順を定めておくこと。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12 3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(障害時・災害時対応策) | 運63 障害時・災害時復旧手順を明確にすること。 | 障害または災害等によりコンピュータシステムが正常に稼働しなくなった場合の復旧手順を明確にすること。なお、当該手順については、コンティンジェンシープランと整合性のとれた内容にすること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12 3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(障害時・災害時対応策) | 運64 障害の原因を調査・分析すること。 | すばやく復旧するため、障害の原因を調査する手法を講じておくこと。また、障害の発生原因を記録し、傾向分析等を通じて再発防止に役立てること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12 3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | 運用管理(コンティンジェンシープランの策定) | 運65 コンティンジェンシープランを策定すること。 | 不慮の災害や事故、あるいは障害等により重大な損害を被り、業務の遂行が困難になった場合の損害の範囲と業務への影響を極小化し、早期復旧をはかるために、あらかじめコンティンジェンシープラン(緊急時対応計画)を策定しておくこと。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」(ISO 27001:2013、附属書 A.17.1)が規定されています。<br><br>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。<br><br>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。<br><br>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。<br><br>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 | V. 運用基準 | システム開発・変更(ハードウェア・ソフトウェア管理) | 運66 ハードウェア、ソフトウェアの管理を行うこと。 | システムの導入、変更、廃棄を確実に行うため、ハードウェア、ソフトウェアの構成管理、版数管理などを行うこと。 | 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。<br><br>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。<br><br>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 | V. 運用基準 | システム開発・変更(システム開発・変更管理) | 運67 開発・変更手順を明確にすること。 | システム開発・変更における内容の正当性を確保するため、開発・変更手順を明確にすること。 | Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」(ISO 27001 2013、附属書 A.12.1.4)と「開発およびサポート プロセスにおけるセキュリティ」(ISO 27001:2013、附属書 A.14.2)が規定されています。<br><br>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 | V. 運用基準 | システム開発・変更(システム開発・変更管理) | 運68 テスト環境を整備すること。 | 本番システムの安全性を確保するため、本番環境へ影響を与えないようなテスト環境を整備すること。 | Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」(ISO 27001 2013、附属書 A.12.1.4)と「開発およびサポート プロセスにおけるセキュリティ」(ISO 27001:2013、附属書 A.14.2)が規定されています。<br><br>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 | V. 運用基準 | システム開発・変更(システム開発・変更管理) | 運69 本番への移行手順を明確にすること。 | 本番システムの安全性を確保するため、本番への移行に際しては、各システムの特性を考慮し、移行手順を明確にするとともに、関連する各部門の手順の整合性を確認すること。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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 | V. 運用基準 | システム開発・変更(ドキュメント管理) | 運70 作成手順を定めること。 | システムドキュメントを適切に作成するため、作成対象とするものを決め、それらについての作成手順を定めること。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001:2013、附属書 A 5)、「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)、「運用の手順および責任」(ISO 27001:2013、附属書 A.12.1)が規定されています。<br><br>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。<br><br>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 | V. 運用基準 | システム開発・変更(ドキュメント管理) | 運71 保管管理方法を明確にすること。 | 円滑な利用および改ざん、不正使用等の防止のため、システムドキュメントの保管管理を適正に行うこと。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」(ISO 27001:2013、附属書 A 5)、「情報セキュリティのための組織」(ISO27001 2013、附属書 A.6)、「運用の手順および責任」(ISO 27001:2013、附属書 A.12.1)が規定されています。<br><br>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。<br><br>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 | V. 運用基準 | システム開発・変更(パッケージの導入) | 運72 評価体制を整備すること。 | パッケージを導入する場合のシステム開発・変更を円滑に行うため、パッケージの有効性、信頼性、生産性等を評価する体制を整備すること。 | 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。<br><br>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 | V. 運用基準 | システム開発・変更(パッケージの導入) | 運73 運用・管理体制を明確にすること。 | パッケージの導入後のトラブル対応、機能拡張等を円滑に行うため、パッケージの運用・管理体制を明確にすること。 | 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。<br><br>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 | V. 運用基準 | システム開発・変更(システムの廃棄) | 運74 廃棄計画、手順を策定すること。 | システムの廃棄を円滑、確実かつ安全に実施するため、運用およびユーザー責任者の承認を得て不正防止、機密保護対策を含めた計画、手順を策定すること。 | Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A 8 3.2)と「装置のセキュリティを保った処分または再利用 」(ISO 27001:2013、附属書 A.11 2.7)が規定されています。<br><br>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 | V. 運用基準 | システム開発・変更(システムの廃棄) | 運75 情報漏洩防止対策を講ずること。 | 機密保護や不正防止等のため、システムの廃棄にあたっては機器等から情報漏洩が生じないように防止策を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A 8 3.2)と「装置のセキュリティを保った処分または再利用 」(ISO 27001:2013、附属書 A.11 2.7)が規定されています。<br><br>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 | V. 運用基準 | 各種設備管理(保守管理) | 運76 管理方法を明確にすること。 | コンピュータシステムを円滑に運用するため、設備の管理責任者および管理方法を明確にし、定められた方法によって管理すること。また、障害時・災害時の対応方法を明確にすること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google のデータセンター ブ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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0 |
| 運77 | V. 運用基準 | 各種設備管理(保守管理) | 運77 保守方法を明確にすること。 | コンピュータシステムを円滑に運用するため、保守点検を実施し、点検内容および結果を把握すること。 | Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」(ISO27001 2013、附属書 A.11)が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。<br><br>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。<br><br>Google のデータセンター ブ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。<br><br>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<br><br>データセンターを紹介する動画: https //www.youtube com/watch?v=XZmGGAbHqa0 |
| 運78 | V. 運用基準 | 各種設備管理(資源管理) | 運78 能力および使用状況の確認を行うこと。 | 異常状態早期発見のため、各種設備の容量および性能の限界を把握し、使用状況の確認を行うこと。 | 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 | V. 運用基準 | 各種設備管理(監視) | 運79 監視体制を整備すること。 | 異常状態早期発見のため、監視対象、監視内容および監視方法を定めること。 | 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。<br><br>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 | V. 運用基準 | 教育・訓練(教育・訓練) | 運80 セキュリティ教育を行うこと。 | セキュリティ意識の向上を図るため、全役職員(外部要員を含む)に対するセキュリティポリシーの周知徹底と、具体的なセキュリティ対策実施に関するセキュリティ教育を、担当する業務内容等を勘案のうえで行うこと。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。<br><br>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。<br><br>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 | V. 運用基準 | 教育・訓練(教育・訓練) | 運81 要員に対するスキルアップ教育を行うこと。 | システムとその開発対象となる適用業務に関する知識および技能の向上を図るための教育を、担当する業務内容等を勘案のうえで行うこと。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。<br><br>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。<br><br>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 | V. 運用基準 | 教育・訓練(教育・訓練) | 運82 オペレーション習熟のための教育および訓練を行うこと。 | コンピュータシステムに係わる通常時運用の円滑化および営業店事務処理に係わる端末機器の操作習熟のため、オペレーションの教育および訓練を行うこと。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。<br><br>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。<br><br>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 | V. 運用基準 | 教育・訓練(教育・訓練) | 運83 障害時・災害時に備えた教育・訓練を行うこと。 | 障害時・災害時に備えるため、コンピュータシステムの運用に係わるオペレーション等の教育・訓練を行うこと。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。<br><br>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。<br><br>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 | V. 運用基準 | 教育・訓練(教育・訓練) | 運84 防災・防犯訓練を行うこと。 | 非常時に備えて防災・防犯訓練を行うこと。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。<br><br>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。<br><br>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 | V．運用基準 | 要員管理(要員管理) | 運85　要員の人事管理を適切に行うこと。 | システムの円滑な運用のため、要員の配置、交替等人事管理を適切に行うこと。 | | 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。<br><br>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 | V．運用基準 | 要員管理(要員管理) | 運86　要員の健康管理を行うこと。 | 作業環境の整備や定期的に健康診断を実施するなど要員の健康管理を適切に行うこと。 | | 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。<br><br>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 | V．運用基準 | 外部委託管理(外部委託に関する計画) | 運87　システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲を明確にすること。 | システムの開発や運用等で外部委託を行う場合は、事前に目的や範囲等を明確にすることが必要である。 | | 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。<br><br>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。<br><br>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。<br><br>https //cloud google.com/terms/subprocessors<br>https //gsuite.google com/terms/subprocessors.html |
| 運87-1 | V．運用基準 | 外部委託管理(外部委託に関する計画) | 運87-1　外部委託先の選定手続きを明確にすること。 | 外部委託先の選定に際しては手続きを明確にし、委託業者を客観的に評価すること。委託業者の決定にあたっては、責任者の承認を得ること。 | | 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。<br><br>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。<br><br>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。<br><br>https //cloud google.com/terms/subprocessors<br>https //gsuite.google com/terms/subprocessors.html |
| 運88 | V．運用基準 | 外部委託管理(外部委託に関する計画) | 運88　安全対策に関する項目を盛り込んだ委託契約を締結すること。 | 安全性確保のため、機密保護、安全運行等に関する項目を盛り込んだ委託契約を締結すること。 | | 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。<br><br>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。<br><br>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。<br><br>https //cloud google.com/terms/subprocessors<br>https //gsuite.google com/terms/subprocessors.html |
| 運89 | V．運用基準 | 外部委託管理(外部委託業務管理) | 運89　外部委託先の要員にルールを遵守させ、その遵守状況を管理、検証すること。 | 外部委託先の要員のセキュリティ管理を適切に行うため、外部委託業務の内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種ルールの遵守を義務づけ、教育、監査を行うこと。 | | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。<br><br>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。<br><br>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 | V．運用基準 | 外部委託管理(外部委託業務管理) | 運90　外部委託における業務組織の整備と業務の管理、検証を行うこと。 | 外部に委託した業務内容を確認するため、業務組織の整備を行うとともに、委託契約に基づき管理、検証を行うこと。 | | 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。<br><br>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。<br><br>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 | V．運用基準 | 外部委託管理(外部委託業務管理) | 運90-1　金融機関相互のシステム・ネットワークのサービス利用にあたっては、適切なリスク管理を行うこと。 | 金融機関相互のシステム・ネットワークは、金融機関相互の金融取引の決済やCD/ATMオンライン提携などを行う上で、基幹インフラとしての機能を担っている。仮にシステム・ネットワークにおいて、障害が発生した場合は、その影響は決済システム全体および顧客サービス全般に及びかねないことから、適切なリスク管理を行うこと。 | | 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 | V．運用基準 | システム監査(システム監査) | 運91　システム監査体制を整備すること。 | コンピュータシステムおよびその管理について、有効性、効率性、信頼性、遵守性、および安全性の面から把握、評価するため、システム監査体制を整備すること。 | | Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」（ISO 27001:2013、附属書 A.12.7）が規定されています。<br><br>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 | V．運用基準 | インストアブランチ | 運92　出店先の選定基準を明確にすること。 | インストアブランチの安全性を確保するため、出店先地域やストアの選定基準を明確にすること。 | | 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 | V．運用基準 | コンビニATM | 運93　出店先の選定基準を明確にすること。 | コンビニATMおよび利用者の安全性を確保するため、出店先地域やコンビニエンスストアの選定基準を明確にすること。 | | 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 | V．運用基準 | コンビニATM | 運94　現金装填等メンテナンス時の防犯対策を講じること。 | コンビニATMのメンテナンス時の安全性を確保するため、防犯体制および防犯方法を明確にすること。 | | 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 | V．運用基準 | コンビニATM | 運95　障害時・災害時対応手順を明確にすること。 | コンビニATMの障害時・災害時に迅速な対応を行うため、その対応手順を明確にすること。 | | 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 | V．運用基準 | コンビニATM | 運96　ネットワーク関連機器、伝送データの安全対策を講ずること。 | 伝送データの安全性、信頼性を確保し、また不正使用、破壊、改ざん等を防止するため、ネットワーク関連機器の適切な保護措置および伝送データの安全対策を講ずること。 | | 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 | V．運用基準 | コンビニATM | 運97　所轄の警察および警備会社等関係者との連絡体制を確立すること。 | 犯罪発生時に関係者へ迅速に連絡を行うため、所轄の警察および警備会社等関係者との連絡体制の確立および訓練を行うこと。 | | 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 | V．運用基準 | コンビニATM | 運98　顧客に対して犯罪に関する注意喚起を行うこと。 | 顧客ならびに取引の安全性を確保するため、犯罪に関する注意喚起を行うこと。 | | 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 | V．運用基準 | デビットカード(デビットカード・サービスの安全性確保) | 運99　デビットカード・サービスにおける安全対策を講ずること。 | デビットカード・サービスの安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センターや加盟店等と共に安全対策を講ずること。 | | 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 | V．運用基準 | デビットカード(デビットカード・サービスの安全性確保) | 運100　口座番号、暗証番号等の安全性を確保すること。 | 口座番号、暗証番号等の安全性を確保するため、金融機関等はサービスの提供形態に応じて、情報処理センターや加盟店等と共に安全対策を講ずること。 | | 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 | V．運用基準 | デビットカード(顧客保護) | 運101　デビットカード利用時の顧客保護の措置を講ずること。 | デビットカード利用時の安全性を確保するため、適切な顧客保護の措置を講ずること。 | | 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 | V．運用基準 | デビットカード(顧客への注意喚起) | 運102　デビットカード利用上の留意事項を顧客に注意喚起すること。 | 顧客に注意を喚起するため、デビットカード利用上の留意事項を顧客に明示すること。 | | 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 | V. 運用基準 | オープンネットワークを利用した金融サービス(インターネット、モバイル) | 運103 不正使用を防止すること。 | オープンネットワークを利用した金融サービスの安全性を確保するため、接続相手先が本人であることを確認する予防策やアクセス制限、検知策等の不正使用防止機能を設けること。 | 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 | V. 運用基準 | オープンネットワークを利用した金融サービス(インターネット、モバイル) | 運104 不正使用を早期発見すること。 | 利用者を不正使用から守るため、利用者自身が使用状態を確認する機能を設けること。 | 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 | V. 運用基準 | オープンネットワークを利用した金融サービス(インターネット、モバイル) | 運105 安全対策に関する情報開示をすること。 | 利用者が適切に取引機関や金融サービスの選択を行うため、安全対策に関する情報を開示することが望ましい。 | 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 | V. 運用基準 | オープンネットワークを利用した金融サービス(インターネット、モバイル) | 運105-1 顧客対応方法を明確にすること。 | インターネット、モバイル等を用いた金融サービスにおいて、注意喚起や受付対応等の顧客対応方法を明確にすること。 | 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 | V. 運用基準 | オープンネットワークを利用した金融サービス(インターネット、モバイル) | 運106 インターネットやモバイル等を用いた金融サービスの運用管理方法を明確化すること。 | インターネットやモバイル等を用いた金融サービスにおいて、利用者を保護し、安全性を確保し円滑に稼働させるため、運用管理方法を明確化すること。 | 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 | V. 運用基準 | オープンネットワークを利用した金融サービス(電子メール) | 運107 電子メールの運用方針を明確にすること。 | 電子メールの運用にあたっては、信頼性、安全性を確保するため、その運用方針を明確にすること。 | 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 | V. 運用基準 | クラウドサービスの利用 | 運108 クラウドサービスの利用を行う場合は、事前に利用目的や範囲等を明確にするとともに、事業者選定の手続きを明確にすること。 | クラウドサービスの利用を行う場合は、事前に目的や範囲等を明確にするとともに、クラウド事業者の選定に際しては手続きを明確にし、事業者を客観的に評価すること。<br>また、事業者の決定にあたっては、責任者の承認を得ること。 | 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 | V. 運用基準 | クラウドサービスの利用 | 運109 クラウド事業者と安全対策に関する項目を盛り込んだ契約を締結すること。 | 安全性確保のため、機密保護、安定的なシステム運用等に関する項目を盛り込んだ委託契約を締結すること。 | 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。<br><br>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。<br><br>利用規約:<br><br>https //cloud google.com/terms/<br>https //gsuite.google com/terms/2013/1/premier_terms html<br><br>SLA:<br><br>https //gsuite.google com/terms/sla html<br>https //cloud google.com/terms/sla/ |
| 運110 | V. 運用基準 | クラウドサービスの利用 | 運110 クラウドサービス利用にあたって、データ漏洩防止策を講ずること。 | ファイルのコピーや盗難等による漏洩を防止するため、重要なデータについては暗号化等の対策を講ずること。 | 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。<br><br>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:<br><br>https //cloud google.com/security/encryption-at-rest/<br>https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf<br><br>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 | V. 運用基準 | クラウドサービスの利用 | 運111 クラウド契約終了時のデータ漏洩防止策を講ずること。 | 機密保護や不正防止等のため、クラウド契約の終了にあたっては当該システム・機器等からデータの漏洩が生じないように防止策を講ずること。 | 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。<br><br>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 | V. 運用基準 | クラウドサービスの利用 | 運112 クラウド事業者に対する立入監査・モニタリング態勢を整備すること。 | 直接の内部統制の及びにくいクラウド事業者について、リスク管理態勢等の有効性を検証すること。 | Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの独立したレビュー」(ISO 27001:2013、附属書 A.18.2.1)が規定されています。<br><br>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。<br><br>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。<br>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。<br><br>https //cloud google.com/security/compliance<br>https //gsuite.google com/learn-more/compliance-google-apps.html |
| 運113 | V. 運用基準 | サイバー攻撃対応態勢の整備 | 運113 サイバー攻撃対応態勢を整備すること。 | サイバー攻撃の手口は高度化かつ巧妙化しているため、サイバー攻撃対応態勢の整備にあたっては、手口の高度化や巧妙化にあわせて見直すことが必要である。 | 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。<br><br>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 | 基準大項目 | 基準中項目 | 基準小項目 | 適用にあたっての考え方 | Google の回答 |
| 技1 | VI. 技術基準<br>I.システム信頼性向上対策 | ハードウェアの信頼性向上対策(ハードウェアの障害予防策) | 技1 予防保守を実施すること。 | ハードウェアの障害を予防するため、装置の特性や重要度に応じ、予防保守を定期的にまたは随時実施すること。 | Google は ISO27001 認証を受けています。この基準では、「装置の保守」(附属書 A.11.2.4)が規定されています。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ハードウェアの信頼性向上対策(ハードウェアの予備) | 技2 本体装置の予備を設けること。 | 本体装置の障害時に迅速に対応するため、重要な本体装置には予備を設けること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)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。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ハードウェアの信頼性向上対策(ハードウェアの予備) | 技3　周辺装置の予備を設けること。 | 周辺装置の障害時に迅速な対応を行うため、重要な周辺装置は予備または代替機能を設けること。 | | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2）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。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ハードウェアの信頼性向上対策(ハードウェアの予備) | 技4　通信系装置の予備を設けること。 | 通信系装置の障害時の迅速な対応のために、重要な通信系装置は予備を設けること。 | | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2）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。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ハードウェアの信頼性向上対策(ハードウェアの予備) | 技5　回線の予備を設けること。 | 回線障害時の迅速な対応のために、重要な回線は予備を設けることが望ましい。 | | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ハードウェアの信頼性向上対策(ハードウェアの予備) | 技6　端末系装置の予備を設けること。 | 端末系装置の障害時の迅速な対応のため、端末系装置は予備または代替機能を設けること。 | | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2）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。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ソフトウェアの信頼性向上対策(開発時の品質向上対策) | 技7　システム開発計画は中長期計画との整合性を確認するとともに、承認を得ること。 | コンピュータシステム全体の信頼性向上のため、システム開発計画は、中長期のシステム化計画と整合性が取れており、かつ内外の技術調査を実施していること、また開発責任者(システムを企画、開発する部門の長)の承認を得ていること。 | | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ソフトウェアの信頼性向上対策(開発時の品質向上対策) | 技8　必要となるセキュリティ機能を取り込むこと。 | セキュリティ対策を確実に実施するため、システム計画段階において必要となるセキュリティ機能が取り込まれていることを明確にすること。 | | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ソフトウェアの信頼性向上対策(開発時の品質向上対策) | 技9　設計段階でのソフトウェアの品質を確保すること。 | 設計段階でのソフトウェアの信頼性向上のため、開発の前提となる要件を明確にするとともに、信頼度設計の考慮や設計作業の標準化等を行い、ソフトウェアの品質を確保すること。 | | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ソフトウェアの信頼性向上対策(開発時の品質向上対策) | 技10　プログラム作成段階での品質を確保すること。 | プログラム作成段階での、ソフトウェアの信頼性向上のため、プログラム仕様書に基づいたプログラミングを行うとともにプログラム作成作業の標準化・自動化等を行い、ソフトウェアの品質を確保すること。 | | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ソフトウェアの信頼性向上対策(開発時の品質向上対策) | 技11　テスト段階でのソフトウェアの品質を確保すること。 | テスト段階でのソフトウェアの信頼性向上のために、テスト計画の策定、テスト環境・体制の整備、テストサポート機能の活用、テスト実施段階での各種管理等を行い、ソフトウェアの品質を確保すること。 | | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ソフトウェアの信頼性向上対策(開発時の品質向上対策) | 技12　プログラムの配布を考慮したソフトウェアの信頼性を確保すること。 | 配布時のソフトウェアの信頼性を確保するため、配布先の稼働環境との整合性確認やウイルスチェックを行うこと。 | | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ソフトウェアの信頼性向上対策(開発時の品質向上対策) | 技13　パッケージ導入にあたり、ソフトウェアの品質を確保すること。 | パッケージソフトウェアの品質を確保するために、機能および自社システムとの整合性を十分確認すること。 | | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ソフトウェアの信頼性向上対策(メンテナンス時の品質向上対策) | 技14　定型的変更作業時の正確性を確保すること。 | 営業店新設、機器増設等の定型的変更作業時における正確性を確保するため、変更作業の合理化等の必要な対策を講ずること。 | | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | ソフトウェアの信頼性向上対策(メンテナンス時の品質向上対策) | 技15　機能の変更、追加作業時の品質を確保すること。 | 機能の変更、追加作業時におけるソフトウェアの品質を確保するため、開発時の品質向上対策を準用すること。 | | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | 運用時の信頼性向上対策(運用時の信頼性向上対策) | 技16　オペレーションの自動化、簡略化を図ること。 | オペレーションの信頼性を向上させるため、オペレーションの自動化、簡略化を図ることが望ましい。 | | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | 運用時の信頼性向上対策(運用時の信頼性向上対策) | 技17　オペレーションのチェック機能を充実すること。 | オペレーションミスを防止するため、チェック機能を充実すること。 | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | 運用時の信頼性向上対策(運用時の信頼性向上対策) | 技18　負荷状態の監視制御機能を充実すること。 | コンピュータシステムの安定稼働のために、各種資源の能力や容量の限界を超えないように負荷状態を監視し、必要に応じて制御する機能を充実すること。 | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | 運用時の信頼性向上対策(運用時の信頼性向上対策) | 技19　CD・ATM等の遠隔制御機能を設けること。 | 無人店舗におけるCD・ATM等の安定運用のために、運用状況を集中監視し、必要に応じて遠隔制御を行う機能を設けること。 | 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 | VI. 技術基準<br>I. システム信頼性向上対策 | 障害の早期発見・早期回復(障害の早期発見) | 技20　システム運用状況の監視機能を設けること。 | 障害の早期発見・回復のために、コンピュータシステムの運用状況(稼働状態、停止状態、エラー状態)を監視する機能を設けること。 | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | 障害の早期発見・早期回復(障害の早期発見) | 技21　障害の検出および障害箇所の切り分け機能を設けること。 | 迅速な障害回復に役立てるため、コンピュータシステムに発生する各種障害を的確に検出し、障害箇所を切り分ける機能を設けること。 | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | 障害の早期発見・早期回復(障害の早期回復) | 技22　障害時の縮退・再構成機能を設けること。 | 障害時に、一部の処理を中断しても、システム全体を停止させることなく運転を続行させるため、機能を縮小し、システムを再構成する機能を設けること。 | 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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | 障害の早期発見・早期回復(障害の早期回復) | 技23　取引制限機能を設けること。 | ファイル障害やプログラムミス等による影響を極小化するため、ファイル単位、科目単位等による取引制限機能を設けること。 | 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 | VI. 技術基準<br>I. システム信頼性向上対策 | 障害の早期発見・早期回復(障害の早期回復) | 技24　リカバリ機能を設けること。 | 障害が発生した場合は、速やかにシステムを回復させ業務を支障なく続行させるために必要なリカバリ機能を設けること。 | Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001:2013、附属書 A.17.2)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。<br><br>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。<br><br>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 | VI. 技術基準<br>I. システム信頼性向上対策 | 災害時対策(バックアップサイト) | 技25　バックアップサイトを保有すること。 | コンピュータセンター等が災害等により機能しなくなった場合に備えて、業務の優先度を考慮してバックアップサイトを保有することが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | データ保護(漏洩防止) | 技26　暗証番号・パスワード等は他人に知られないための対策を講ずること。 | 暗証番号・パスワード等の漏洩防止のため、非表示、非印字等の必要な対策を講ずること。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A 9)が規定されています。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | データ保護(漏洩防止) | 技27　相手端末確認機能を設けること。 | 公衆通信網を通じて自動着信端末に出力する場合には、誤接続を防止するため、確認可能なものについては相手端末を確認する機能を設けることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A 9)が規定されています。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | データ保護(漏洩防止) | 技28　蓄積データの漏洩防止策を講ずること。 | ファイルのコピーや盗難等による漏洩を防止するため、重要なデータについては暗号化等の対策を講ずることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001:2013、附属書 A.10) が規定されています。<br><br>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:<br><br>https //cloud google.com/security/encryption-at-rest/<br>https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | データ保護(漏洩防止) | 技29　伝送データの漏洩防止策を講ずること。 | データ伝送時の盗聴等による漏洩を防止するため、重要なデータについては暗号化の対策を講ずることが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「暗号」(ISO 27001:2013、附属書 A.10) が規定されています。<br><br>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:<br><br>https //cloud google.com/security/encryption-at-rest/<br>https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | データ保護(破壊・改ざん防止) | 技30　ファイルに対する排他制御機能を設けること。 | ファイル内容の矛盾発生防止のため、ファイルに対する排他制御機能を設けること。 | 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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | データ保護(破壊・改ざん防止) | 技31　ファイルに対するアクセス制御機能を設けること。 | 不正アクセス等からデータを保護するため、プログラムとファイル間のアクセス権限チェック機能等を設けること。 | 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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | データ保護(破壊・改ざん防止) | 技32　不良データ検出機能を充実すること。 | システムへの不良データの混入を防止するため、不良データの検出・除外機能を充実すること。 | 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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | データ保護(検知策) | 技33　伝送データの改ざん検知策を講ずること。 | 重要なデータの伝送においては、改ざん検知のための対策を講じておくことが望ましい。 | Google は ISO27001 認証を受けています。この基準では、「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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | データ保護(検知策) | 技34　ファイル突合機能を設けること。 | 故意または過失により起きたファイル間の不整合を早期に発見するため、元帳、精査表、ジャーナル等のファイル間の突合機能を設けること。 | 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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(アクセス権限確認)) | 技35　本人確認機能を設けること。 | 不正使用防止のため、業務内容や接続方法に応じ、接続相手先が本人もしくは正当な端末であることを確認すること。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A 9) が規定されています。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(アクセス権限確認)) | 技35-1　生体認証の特性を考慮し、必要な安全対策を検討すること。 | 生体認証の導入と運用にあたっては、技術の最新動向等に留意し、その特性を十分考慮し、必要な安全対策を検討すること。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A 9) が規定されています。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(アクセス権限確認)) | 技36　IDの不正使用防止機能を設けること。 | 不正アクセス防止のため、システムやデータ等へのアクセスに用いるIDの不正使用防止機能を設けること。 | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A 9) が規定されています。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(アクセス権限確認)) | 技37　アクセス履歴を管理すること。 | アクセス状況を管理するため、システムやデータへのアクセス履歴を取得し、監査証跡として必要期間保管するとともに定期的にチェックすること。 | | Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A 9）が規定されています。<br><br>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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(利用範囲の制限)) | 技38　取引制限機能を設けること。 | 不正アクセスを防止するため、端末等取引に使用する機器・媒体の種類、設置場所、用途等により、取引内容の制限機能を設けること。 | | 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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(利用範囲の制限)) | 技39　事故時の取引禁止機能を設けること。 | カード、通帳、印鑑等の盗難・紛失等の事故に対処するため、その口座に対する当該媒体による取引を禁止する機能を設けること。また、渉外端末の盗難・紛失等の事故に対処するため、端末ごとの取引禁止機能を設けること。 | | 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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(不正・偽造防止対策)) | 技40　カードの偽造防止対策のための技術的措置を講ずること。 | 不正使用防止のため、カードの偽造防止のための技術的措置を講ずることが望ましい。 | | 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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(不正・偽造防止対策)) | 技41　電子的価値の保護機能、または不正検知の仕組みを設けること。 | 電子的価値のコピー、二重使用等の不正行為に対処するため、データの保護機能を具備するか、あるいはその発生を検知できる仕組みを構築しておくことが望ましい。 | | 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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(不正・偽造防止対策)) | 技42　電子化された暗号鍵を蓄積する機器、媒体、またはそこに含まれるソフトウェアには、暗号鍵の保護機能を設けること。 | 暗号鍵が他人に知られることによる不正行為を防止するため、暗号鍵の保護機能を機器、媒体またはソフトウェアに具備すること。 | | 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。<br><br>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:<br><br>https //cloud google.com/security/encryption-at-rest/<br>https //storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(予防策(不正・偽造防止対策)) | 技42-1　電子メール送受信、ホームページ閲覧等の不正使用防止機能を設けること。 | 業務目的以外の電子メールの送受信やホームページの閲覧等に対処するため、不正使用防止対策を講ずることが望ましい。 | | 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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(外部ネットワークからのアクセス制限) | 技43　外部ネットワークからの不正侵入防止機能を設けること。 | 不正侵入を防止するため、重要なデータやプログラムを扱うシステムについては、外部ネットワーク(オープンネットワーク、リモートアクセス等)との接続部分に適切な不正侵入防止策を講ずること。 | | 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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(外部ネットワークからのアクセス制限) | 技44　外部ネットワークからアクセス可能な接続機器は必要最小限にすること。 | 不正アクセスによるコンピュータシステムへの侵入を防ぐため、外部からアクセス可能な通信経路、通信関連機器等は最小限とし、不必要な機器は接続しないこと。 | | 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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(検知策) | 技45　不正アクセスの監視機能を設けること。 | 不正アクセスを早期に発見するため、アクセスの失敗や不正アクセスを監視する機能を設けること。 | | 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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(検知策) | 技46　異常な取引状況を把握するための機能を設けること。 | 不正取引による被害発生の防止等のため、異常な取引状況を早期に把握するための機能を検討し実施すること。 | | 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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(検知策) | 技47　異例取引の監視機能を設けること。 | 不正アクセスを早期に発見するため、異例取引の監視機能を設けること。 | | 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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正使用防止(対応策) | 技48　不正アクセスの発生に備えて対応策、復旧策を講じておくこと。 | 不正アクセスを検知した場合に備えて、不正アクセスの拡大防止のための対応策、復旧手順を明確にしておくことが望ましい。不正アクセスを検知した場合、その被害の有無にかかわらず、不正アクセスの拡大防止策、復旧策を講ずること。また、不正アクセスの原因を分析後、再発防止策を講ずること。 | | 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。<br><br>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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正プログラム防止(防御策) | 技49 コンピュータウイルス等不正プログラムへの防御対策を講ずること。 | 開発、保守、運用時におけるコンピュータウイルス等不正プログラムによる被害を防ぐため、防御対策を講ずること。 | | 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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正プログラム防止(検知策) | 技50 コンピュータウイルス等不正プログラムの検知対策を講ずること。 | システムの信頼性を確保・維持するため、コンピュータウイルス等の不正プログラムの侵入や組込みの有無を検証する検知対策を講ずること。 | | 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。<br><br>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 | VI. 技術基準<br>II. 安全性侵害対策 | 不正プログラム防止(復旧策) | 技51 コンピュータウイルス等不正プログラムによる被害時対策を講ずること。 | コンピュータウイルス等の不正プログラムによる被害を最小限にするため、発見時からシステム復旧までの対策を講ずること。 | | 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。<br><br>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。 |