医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン

Google Cloud と Google Workspace 解説書

本解説書は、令和 2 年 8 月に経済産業省及び総務省より示された、「医療情報を取り扱う情報システム及びサービス提供者の安全管理ガイドライン」に基づく情報提供の一環として、Google Cloud及びGoogle Workspaceが講じている安全管理措置の概要を示すものです。本解説書で説明されている Google における管理は第三者監査のコンプライアンス・プログラムである ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 で認定済みです。
「医療情報を取り扱う情報システム及びサービス提供者の安全管理ガイドライン」で求められている「情報流」は、Google CloudやGoogle Workspaceの利用者毎に異なるため、各パターン別にその対応状況を示すことが難しいことから、Google では、「別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインとの対応表」の記載事項に関する「Google の対策」を公開しています。
＊行番号、Googleの対策、ISO基準詳細以外の各列は、「別紙2　旧ガイドラインの対策項目一覧と医療情報安全管理ガイドラインとの対応表」の列構成に準拠しています。

行番号	対策	大項目	小項目	No.	内容	Google の対策	ISO基準詳細
1	1. 人的・組織的対策	1.1. 規程・手順の策定	①アクセス管理規定の策定	①-1	医療情報システム等へのアクセス制限、記録、点検等を定めたアクセス管理規定を作成し、医療機関等の求めに応じて提出できる状態にしておく。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
2	1. 人的・組織的対策	1.1. 規程・手順の策定	①アクセス管理規定の策定	①-2	アクセス管理規定には以下の内容を含める。 ・アクセス権限、アカウント管理における登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセス ・認証及びアクセス等に対する記録の収集と保存 ・認証及びアクセス等に対する記録の定期的なレビュー ・アクセス管理の運用状況に関する定期的なレビューの実施	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）と「情報セキュリティのための組織」（ISO27001 2013、附属書 A.6）が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.5,6
3	1. 人的・組織的対策	1.1. 規程・手順の策定	②持ち出した機器の外部のネットワークに接続する	②-1	持ち出した機器を外部のネットワークに接続する場合の接続条件、安全管理措置等（格納された情報の漏洩や改竄が生じないようにするための具体的な措置（不正プログラム対策、暗号化、ファイアウォール導入等））を運用管理規程に含める。	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.1

			場合の対策の策定				
4	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-1	CD-R 等の廃棄手順について定める。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
5	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-2	ハードディスク等の廃棄手順について定める。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
6	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-3	破棄手順に、不可逆的な破壊･抹消等により元のデータを復元できなくする措置を含める。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7

						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されます。	
7	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-4	ハードディスク等を医療情報システム等内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認する。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
8	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-5	サーバ等の BIOS パスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去する。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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。Google は、NIST SP 800-88 Revision 1の「媒体のサニタイズに関するガイドライン」の Appendix A.において推奨される方法に従います。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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013、附属書 A.8.3.2, A.11.2.7
9	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-6	ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証する。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2

10	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-7	ハードディスクの廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等の求めに応じ、速やかに提出できるよう整備する。	ストレージメディアのセキュリティ管理をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はデータセンターにある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、バーコード及び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。構成要素がライフサイクル中の任意の時点で性能試験に合格しなかった場合は、インベントリから削除され、撤去されます。Google ハードドライブは、ハードディスク暗号化 (FDE) やドライブロックなどの技術を利用して、保存中のデータを保護します。Google の施設を離れたリムーバブルメディア上の個人識別情報(PII)は承認を経て、暗号化されます。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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。Google は、利用が定められた自動ワークフローツールを利用して、サニタイズ及び破壊プロセスを通じてディスクをレビュー、承認、追跡しています。	-
11	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-8	物理的な破壊措置については受託事業者自身で行うことが望ましいが、外部の事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し外部委託の了承を得ておく。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておく。 なお、ハードディスクの廃棄方法としては、一定以上の強度を持つ磁力線を照射する方法、溶融処理等の物理的破壊措置が確実であるが、ランダムデータ及び固定パターンの複数回の書き込みを行うソフトウェア実行によるデータ消去方式（NSA 推奨方式、米国防総省準拠方式、NATO 方式、グートマン方式等）も良く利用されている。保存されている情報の重要性に合わせて適切な方式を選択し、医療機関等側に選択の合理的な理由を説明、合意を得た上で実施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、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
12	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-9	電子媒体を廃棄する場合には、物理的な破壊措置（高温による融解、裁断等）を適用し、情報の読み出しが不可能であることを確認する。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7

						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されます。	
13	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-10	運用管理規程に以下の内容を定める。 ・管理する個人情報又はこれを格納する媒体等について、医療情報システム等提供上の要否の確認を定期的に行うこと。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体についての破棄手順。 ・医療情報システム等提供上不要とされた個人情報及びこれを格納する媒体の破棄に際して、医療機関等が不測の損害を被らないようにするための措置(事前に破棄の基準等を告知する等）。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
14	1. 人的・組織的対策	1.1. 規程・手順の策定	③情報の廃棄対応	③-11	情報の破棄手順について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
15	1. 人的・組織的対策	1.1. 規程・手順の策定	④情報や機器の組織外への持出に対する対策	④-1	受託する個人情報を運用や保守に用いる端末に原則保存しない旨、自社の運用管理規程等に定める。	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	・ISO 27001 2013, 附属書 A.11.2

16	1. 人的・組織的対策	1.1. 規程・手順の策定	④情報や機器の組織外への持出に対する対策	④-2	医療情報を格納する機器等を、保守（例えば機器の修理等）の目的で、医療機関等又は受託事業者等（再委託事業者含む）の組織外に持ち出す必要がある場合には、その手順を策定する。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
17	1. 人的・組織的対策	1.1. 規程・手順の策定	④情報や機器の組織外への持出に対する対策	④-3	④-2で定める手順及び情報の提供条件について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
18	1. 人的・組織的対策	1.1. 規程・手順の策定	④情報や機器の組織外への持出に対する対策	④-4	持ち出した機器を再度設置するための適切な検証手順を策定する。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5

19	1. 人的・組織的対策	1.1. 規程・手順の策定	④情報や機器の組織外への持出に対する対策	④-5	保守点検で障害不良等が発見された際の対応作業等を行う際には受託事業者の管理する領域にて行うこととし、外部に持ち出すことが無いようにする。必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去してから持ち出す。記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的な破壊を行ってからの廃棄を選択する。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
20	1. 人的・組織的対策	1.1. 規程・手順の策定	④情報や機器の組織外への持出に対する対策	④-6	持ち出し手順に含まれる事項には次のようなものが考えられる。 ・ 装置の持ち出し申請書のフォーマット（申請者情報、承認者情報、対象機器情報、持ち出し日時、返却予定日時、持ち出す場所の情報、持ち出す理由、機器に納められている情報の概要、持ち出しに伴うリスク評価の結果、機器が紛失・損傷した場合の対応策、等） ・ 申請承認プロセス ・ 返却確認プロセス、等。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5
21	1. 人的・組織的対策	1.1. 規程・手順の策定	④情報や機器の組織外への持出に対する対策	④-7	返却時の検証手順に含まれる事項には次のようなものが考えられる。 ・ 装置の動作確認 ・ 盗聴装置等、情報の安全性を脅かす装置の有無 ・ 悪意のあるプログラムの検出作業 ・ 収められている情報の検証作業（不正な改竄等）、等。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5

						Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	
22	1. 人的・組織的対策	1.1. 規程・手順の策定	⑤持ち出した機器や媒体の管理手順の策定	⑤-1	サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出しを含む）に関する方針及び規則等を、運用管理規程に定める。	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）、「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）と「暗号化」（ISO 27001 2013、附属書 A.10）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google または Google の代理者が管理していない物理的境界の外側を転送中のデータが移動する場合、Google は 1 つ以上のネットワークレイヤでそのデータを暗号化し、認証します。詳しくは https://cloud.google.com/security/encryption-in-transit/ をご覧ください。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7,10
23	1. 人的・組織的対策	1.1. 規程・手順の策定	⑤持ち出した機器や媒体の管理手順の策定	⑤-2	⑤-1における「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。	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）、「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）と「暗号化」（ISO 27001 2013、附属書 A.10）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google または Google の代理者が管理していない物理的境界の外側を転送中のデータが移動する場合、Google は 1 つ以上のネットワークレイヤでそのデータを暗号化し、認証します。詳しくは https://cloud.google.com/security/encryption-in-transit/ をご覧ください。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7,10
24	1. 人的・組織的対策	1.1. 規程・手順の策定	⑤持ち出した機器や媒体の管理手順の策定	⑤-3	⑤-1で定める内容について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおけるいかなる時点においても、性能試験に合格しな	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7

						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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	
25	1. 人的・組織的対策	1.1. 規程・手順の策定	⑤持ち出した機器や媒体の管理手順の策定	⑤-4	電子媒体について受託事業者施設外への不要な持ち出しを行わない。CD、DVD、MO 等の電子媒体については、追記のできない光学メディア（CD-R、DVD-R 等）を用い、情報交換作業終了後、電子媒体を確実に廃棄処分する。	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）、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.11.2, 8.3.2, 11.2.7
26	1. 人的・組織的対策	1.1. 規程・手順の策定	⑤持ち出した機器や媒体の管理手順の策定	⑤-5	情報交換目的やバックアップ目的で MT、DAT、半導体記憶装置、ハードディスク等の大容量の電子媒体を用いる場合には、その管理を厳重に行う。これらの電子媒体に複数回の情報記録を行う場合には、単に上書きするのではなく、確実な情報消去等の情報漏洩対策を行う。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
27	1. 人的・組織的対策	1.1. 規程・手順の策定	⑤持ち出した機器や媒体の管理手順の策定	⑤-6	全ての電子媒体には格納される情報の機密レベルを示すラベル付けを行う。	Google は ISO27001 認証を受けています。この基準では、「情報の分類」（ISO 27001 2013、附属書 A.8.2）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 お客様は、Google Cloud に保存されている情報に独自のデータラベリング標準を適用できます。	・ISO 27001 2013, 附属書 A.8.2

28	1. 人的・組織的対策	1.1. 規程・手順の策定	⑤持ち出した機器や媒体の管理手順の策定	⑤-7	記録媒体･記録機器に関し、以下の内容を運用管理規程に含める。 ・管理体制及び管理方法 ・記録媒体･記録機器の取扱い ・サービスに関する情報（受託情報、情報システムに関連する情報等）を格納する機器･媒体等の持ち出し（委託元からの持ち出し含む）に関する方針及び規則等（「持ち出し」には、物理的な持ち出しのほか、ネットワークを通じた外部への送信についても含む。） ・サービスに関する情報を持ち出した場合で、当該情報を格納する機器･媒体等の盗難･紛失（持ち出し時の機器･媒体等の物理的な盗難、紛失のほか、システム管理者が承認しない外部への送信等（第三者による悪意の送信、従業者等における誤送信等を含む。））が起きた場合の対応	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud のお客様は、運用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.1
29	1. 人的・組織的対策	1.1. 規程・手順の策定	⑤持ち出した機器や媒体の管理手順の策定	⑤-8	⑤-7の内容に関する教育を従業員等に対して行う。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 すべての Google 委託業者は、オリエンテーションプロセスの一環としてセキュリティ研修を受け、Google キャリアを通じて継続的なセキュリティ研修を受けます。新規の委託業者は、オリエンテーション中にお客様の情報を安全に保つことへのコミットメントを強調する当社の行動規範に同意します。役割に応じて、セキュリティの特定の側面に関する追加の研修が必要になる場合があります。たとえば、情報セキュリティチームは、安全なコーディング手法、製品設計、脆弱性テストツールなどのトピックについて、新しいエンジニアを指導します。また、技術者は、セキュリティ関連のトピックに関する技術プレゼンテーションに出席し、新しい脅威、攻撃パターン、軽減技法を網羅したセキュリティニュースレターを受け取ります。	・ISO 27001 2013, 附属書 A.7.2.2
30	1. 人的・組織的対策	1.1. 規程・手順の策定	⑤持ち出した機器や媒体の管理手順の策定	⑤-9	⑤-7の内容を含む運用管理規程については、再委託先に対しても遵守等を求める。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 すべての Google 委託業者は、オリエンテーションプロセスの一環としてセキュリティ研修を受け、Google キャリアを通じて継続的なセキュリティ研修を受けます。新規の委託業者は、オリエンテーション中にお客様の情報を安全に保つことへのコミットメントを強調する当社の行動規範に同意します。役割に応じて、セキュリティの特定の側面に関する追加の研修が必要になる場合があります。たとえば、情報セキュリティチームは、安全なコーディング手法、製品設計、脆弱性テストツールなどのトピックについて、新しいエンジニアを指導します。また、技術者は、セキュリティ関連のトピックに関する技術プレゼンテーションに出席し、新しい脅威、攻撃パターン、軽減技法を網羅したセキュリティニュースレターを受け取ります。	・ISO 27001 2013, 附属書 A.7.2.2
31	1. 人的・組織的対策	1.1. 規程・手順の策定	⑥機器・ソフトウェアの品質管理に係る手順の策定	⑥-1	情報処理装置及びソフトウェアの適切な変更手順を策定する。原則、保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受ける。	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）が規定されています。詳しくは、「Google インフラストラクチャのセキュリティ設計の概要」（https://cloud.google.com/security/security-design/）をご覧ください。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.12.1.2,14

32	1. 人的・組織的対策	1.1. 規程・手順の策定	⑥機器・ソフトウェアの品質管理に係る手順の策定	⑥-2	機器及びソフトウェアの品質管理に関する対応、手順等を運用管理規程等に含める。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5
33	1. 人的・組織的対策	1.1. 規程・手順の策定	⑥機器・ソフトウェアの品質管理に係る手順の策定	⑥-3	機器及びソフトウェアの品質管理に関する教育を従業員等に対して行う。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育及び訓練」(ISO 27001 2013、附属書 A.7.2.2) が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 すべての Google 委託業者は、オリエンテーションプロセスの一環としてセキュリティ研修を受け、Google キャリアを通じて継続的なセキュリティ研修を受けます。新規の委託業者は、オリエンテーション中にお客様の情報を安全に保つことへのコミットメントを強調する当社の行動規範に同意します。役割に応じて、セキュリティの特定の側面に関する追加の研修が必要になる場合があります。たとえば、情報セキュリティチームは、安全なコーディング手法、製品設計、脆弱性テストツールなどのトピックについて、新しいエンジニアを指導します。また、技術者は、セキュリティ関連のトピックに関する技術プレゼンテーションに出席し、新しい脅威、攻撃パターン、軽減技法を網羅したセキュリティニュースレターを受け取ります。	・ISO 27001 2013, 附属書 A.7.2.2
34	1. 人的・組織的対策	1.1. 規程・手順の策定	⑥機器・ソフトウェアの品質管理に係る手順の策定	⑥-4	医療情報システム等に係る委託先に対して、自社が本ガイドラインの要求事項に対応するために行う品質管理への対応等を求める。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 すべての Google 委託業者は、オリエンテーションプロセスの一環としてセキュリティ研修を受け、Google キャリアを通じて継続的なセキュリティ研修を受けます。新規の委託業者は、オリエンテーション中にお客様の情報を安全に保つことへのコミットメントを強調する当社の行動規範に同意します。役割に応じて、セキュリティの特定の側面に関する追加の研修が必要になる場合があります。たとえば、情報セキュリティチームは、安全なコーディング手法、製品設計、脆弱性テストツールなどのトピックについて、新しいエンジニアを指導します。また、技術者は、セキュリティ関連のトピックに関する技術プレゼンテーションに出席し、新しい脅威、攻撃パターン、軽減技法を網羅したセキュリティニュースレターを受け取ります。	・ISO 27001 2013, 附属書 A.7.2.2
35	1. 人的・組織的対策	1.1. 規程・手順の策定	⑥機器・ソフトウェアの品質管理に係る手順の策定	⑥-5	変更手順に含まれる事項には次のようなものが考えられる。 ・ 変更についての影響が及ぶ関係者への通知プロセス ・ 装置の変更申請書のフォーマット（申請者情報、承認者情報、対象機器情報、変更作業開始日時、変更作業期間、変更理由、機器に納められている情報の概	Google は ISO27001 認証を受けています。この基準では、「変更管理」（附属書 A.12.1.2）、「システムの取得、開発および保守」（ISO 27001 2013、附属書 A.14）が規定されています。 詳しくはGoogle インフラストラクチャのセキュリティ設計の概要をご覧ください。 https://cloud.google.com/security/security-design/ Google Cloud のお客様は、変更管理とシステム開発の手続きを含むお使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.2,14

					要、変更に伴うリスク評価の結果、機器が損傷した場合の対応策、等） ・ 申請承認プロセス ・ 変更試験プロセス ・ 変更作業に支障が発生した場合の復旧手順 ・ 変更終了確認プロセス ・ 変更に伴う影響を監視するプロセス、等。		
36	1. 人的・組織的対策	1.2. 個人情報を含まないテストデータの利用	①個人情報を含むデータの利用に対する対策	①-1	医療情報を開発及び試験用データとして直接利用しない。利用する場合には、個人を識別できる情報等の削除及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関等に示し、了解を得た上で利用する。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.4,14.2
37	1. 人的・組織的対策	1.3. 守秘義務に係る契約	①医療情報システム等提供に係る職員全てとの守秘義務に係る契約締結	①-1	医療情報を操作する可能性のある受託事業者の職員全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求める。派遣従業員については守秘義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求める。	Google は ISO27001 認証を受けています。この基準では、「雇用規約」（ISO 27001 2013、附属書 A.7.1.2）が規定されています。 セキュリティ意識の向上とトレーニングの管理を含む、雇用慣行管理は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、現地の法律で許可されている新規採用者の身元調査を行います。	・ISO 27001 2013, 附属書 A.7.1.2
38	1. 人的・組織的対策	1.3. 守秘義務に係る契約	①医療情報システム等提供に係る職員全てとの守秘義務に係る契約締結	①-2	医療情報を操作する可能性のある受託事業者の職員（派遣従業員含む）については、守秘義務に関する内容を就業規則等に含める。	Google Cloud と Google Workspace は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持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。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約をご覧ください。 利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	-
39	1. 人的・組織的対策	1.3. 守秘義務に係る契約	①医療情報システム等提供に係る職員全てとの守秘義務に係る契約締結	①-3	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておく。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求める。派遣従業員については、派遣契約解除時に同等の合意書への署名を求める。	Google は ISO27001 認証を受けています。この基準では、「雇用規約」（ISO 27001 2013、附属書 A.7.1.2）が規定されています。 セキュリティ意識の向上とトレーニングの管理を含む、雇用慣行管理は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、現地の法律で許可されている新規採用者の身元調査を行います。	・ISO 27001 2013, 附属書 A.7.1.2
40	1. 人的・組織的対策	1.3. 守秘義務に係る契約	①医療情報システム等提供に係る職員全てとの守秘義	①-4	医療情報を操作する受託事業者の職員（派遣従業員含む）が退職した場合の、就業中に取り扱った個人情報に関する守秘義務等について、雇用契約又は派遣契約に含めるか、就業規則等に含める。	Google は ISO27001 認証を受けています。この基準では、「雇用規約」（ISO 27001 2013、附属書 A.7.1.2）が規定されています。 セキュリティ意識の向上とトレーニングの管理を含む、雇用慣行管理は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、現地の法律で許可されている新規採用者の身元調査を行います。	・ISO 27001 2013, 附属書 A.7.1.2

			務に係る契約締結				
41	1. 人的・組織的対策	1.3. 守秘義務に係る契約	①医療情報システム等提供に係る職員全てとの守秘義務に係る契約締結	①-5	上記に違反した受託事業者（派遣従業員含む）の職員に対して、適切な懲戒手続きを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。定めた懲戒手続きについては各職員に周知し、理解したことの確認を行う。	Google は ISO27001 認証を受けています。この基準では、「雇用規約」（ISO 27001 2013、附属書 A.7.1.2）が規定されています。 セキュリティ意識の向上とトレーニングの管理を含む、雇用慣行管理は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、現地の法律で許可されている新規採用者の身元調査を行います。	・ISO 27001 2013, 附属書 A.7.1.2
42	1. 人的・組織的対策	1.3. 守秘義務に係る契約	①医療情報システム等提供に係る職員全てとの守秘義務に係る契約締結	①-6	医療情報を操作する受託事業者の職員（派遣従業員含む）に対する教育･訓練の実施状況や、守秘義務等への対応状況等に関する資料の提供について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「雇用規約」（ISO 27001 2013、附属書 A.7.1.2）が規定されています。 セキュリティ意識の向上とトレーニングの管理を含む、雇用慣行管理は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、現地の法律で許可されている新規採用者の身元調査を行います。	・ISO 27001 2013, 附属書 A.7.1.2
43	1. 人的・組織的対策	1.3. 守秘義務に係る契約	②医療機関等や再委託先との守秘義務を含めた契約の締結	②-1	医療情報システム等に係る情報及び受託した情報に関する守秘義務について、医療情報システム等提供に係る契約に含める。契約には、守秘義務に違反した受託事業者にはペナルティが課されること、及び委託した情報の取扱いに対する医療機関等による監督に関する内容を含める。	Google Cloud と Google Workspace は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持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。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約をご覧ください。 利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	-
44	1. 人的・組織的対策	1.3. 守秘義務に係る契約	②医療機関等や再委託先との守秘義務を含めた契約の締結	②-2	医療情報システム等の動作確認に際し、受託した個人情報を含むデータをやむを得ず使用する場合には、守秘義務が課された要員･委託先等により動作確認を行う旨を含めた手順を定める。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
45	1. 人的・組織的対策	1.3. 守秘義務に係る契約	②医療機関等や再委託先との守秘義務を含めた契約の締結	②-3	医療情報システム等の動作確認に際し、受託した個人情報をやむを得ず使用する場合について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
46	1. 人的・組織的対策	1.4. 教育訓練の実施	①医療情報システム等提供に係る教育訓練の実施	①-1	医療情報を操作する可能性のある受託事業者の職員の全てに個人情報保護及び情報セキュリティに関する教育を行い、一定水準の理解を得た職員だけを業務に従事させる。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 すべての Google 委託業者は、オリエンテーションプロセスの一環としてセキュリティ研修を受け、Google キャリアを通じて継続的なセキュリティ研修を受けます。新規の委託業者は、オリエンテー	・ISO 27001 2013, 附属書 A.7.2.2

						ション中にお客様の情報を安全に保つことへのコミットメントを強調する当社の行動規範に同意します。役割に応じて、セキュリティの特定の側面に関する追加の研修が必要になる場合があります。たとえば、情報セキュリティチームは、安全なコーディング手法、製品設計、脆弱性テストツールなどのトピックについて、新しいエンジニアを指導します。また、技術者は、セキュリティ関連のトピックに関する技術プレゼンテーションに出席し、新しい脅威、攻撃パターン、軽減技法を網羅したセキュリティニュースレターを受け取ります。	
47	1. 人的・組織的対策	1.4. 教育訓練の実施	①医療情報システム等提供に係る教育訓練の実施	①-2	派遣従業員に関しては、派遣元に対し、個人情報保護及び情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行う。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 すべての Google 委託業者は、オリエンテーションプロセスの一環としてセキュリティ研修を受け、Google キャリアを通じて継続的なセキュリティ研修を受けます。新規の委託業者は、オリエンテーション中にお客様の情報を安全に保つことへのコミットメントを強調する当社の行動規範に同意します。役割に応じて、セキュリティの特定の側面に関する追加の研修が必要になる場合があります。たとえば、情報セキュリティチームは、安全なコーディング手法、製品設計、脆弱性テストツールなどのトピックについて、新しいエンジニアを指導します。また、技術者は、セキュリティ関連のトピックに関する技術プレゼンテーションに出席し、新しい脅威、攻撃パターン、軽減技法を網羅したセキュリティニュースレターを受け取ります。	・ISO 27001 2013, 附属書 A.7.2.2
48	1. 人的・組織的対策	1.4. 教育訓練の実施	①医療情報システム等提供に係る教育訓練の実施	①-3	この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行う。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 すべての Google 委託業者は、オリエンテーションプロセスの一環としてセキュリティ研修を受け、Google キャリアを通じて継続的なセキュリティ研修を受けます。新規の委託業者は、オリエンテーション中にお客様の情報を安全に保つことへのコミットメントを強調する当社の行動規範に同意します。役割に応じて、セキュリティの特定の側面に関する追加の研修が必要になる場合があります。たとえば、情報セキュリティチームは、安全なコーディング手法、製品設計、脆弱性テストツールなどのトピックについて、新しいエンジニアを指導します。また、技術者は、セキュリティ関連のトピックに関する技術プレゼンテーションに出席し、新しい脅威、攻撃パターン、軽減技法を網羅したセキュリティニュースレターを受け取ります。	・ISO 27001 2013, 附属書 A.7.2.2
49	1. 人的・組織的対策	1.4. 教育訓練の実施	①医療情報システム等提供に係る教育訓練の実施	①-4	医療情報を操作する受託事業者の職員（派遣従業員含む）の退職時又は契約終了時以降の守秘義務について、教育･訓練に含める。	Google は ISO27001 認証を受けています。この基準では、「雇用規約」（ISO 27001 2013、附属書 A.7.1.2）が規定されています。 セキュリティ意識の向上とトレーニングの管理を含む、雇用慣行管理は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、現地の法律で許可されている新規採用者の身元調査を行います。	・ISO 27001 2013, 附属書 A.7.1.2
50	1. 人的・組織的対策	1.5. 運用状況のモニタリング	①医療情報システム等提供に係る閲覧・操作内容のモニタリング	①-1	受託事業者の職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改竄又は破壊等の行為が行われていないことを検証する。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク管理策」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジ	・ISO 27001 2013, 附属書 A.9.1.2,13.1

						クスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。	
51	1. 人的・組織的対策	1.5. 運用状況のモニタリング	①医療情報システム等提供に係る閲覧・操作内容のモニタリング	①-2	医療情報システム等の保守業務を行う際には、原則として業務の事前及び事後に医療機関等の管理者に対して書面等による通知を行う。事前の了解を必要とする業務及びその業務について事前の了解を得ることができない場合の対応方法について、医療機関等と合意する。	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud - 利用規約: https://cloud.google.com/terms/ Google Workspace - 利用規約: https://workspace.google.com/terms/premier_terms.html セクション「1.4 変更 (a) 本サービスに対する変更」は、「Google は、本サービスに対して、商業上合理的な変更を随時行うことができます。Google が本サービスに対してお客様に大きな影響を与える重要な変更を加える場合、お客様がそのような変更の通知を受け取るよう Google に登録済みであれば、Google はお客様に通知を行うものとします」に言及しています。	-
52	1. 人的・組織的対策	1.5. 運用状況のモニタリング	①医療情報システム等提供に係る閲覧・操作内容のモニタリング	①-3	保守業務実施後には、医療機関等に対し報告等を行い、医療機関等の管理者の確認を得る。本手順の対応について、医療機関等と合意する。	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud - 利用規約: https://cloud.google.com/terms/ Google Workspace - 利用規約: https://workspace.google.com/terms/premier_terms.html セクション「1.4 変更 (a) 本サービスに対する変更」は、「Google は、本サービスに対して、商業上合理的な変更を随時行うことができます。Google が本サービスに対してお客様に大きな影響を与える重要な変更を加える場合、お客様がそのような変更の通知を受け取るよう Google に登録済みであれば、Google はお客様に通知を行うものとします」に言及しています。	-
53	1. 人的・組織的対策	1.5. 運用状況のモニタリング	①医療情報システム等提供に係る閲覧・操作内容のモニタリング	①-4	医療情報システム等の保守業務を医療機関等の施設内で行う際の対応について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
54	1. 人的・組織的対策	1.5. 運用状況のモニタリング	②機器や媒体の定期的な所在確認	②-1	電子媒体は台帳を作成して管理する。台帳と電子媒体を定期的に検証し、盗難、紛失の発生を検証する。台帳においては利用に関する記録を行い、電子媒体の廃棄後も一定期間にわたり記録を維持する。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5

						経て、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されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	
55	1. 人的・組織的対策	1.5. 運用状況のモニタリング	②機器や媒体の定期的な所在確認	②-2	情報を格納する機器･媒体等については、台帳管理等を行い、定期的に所在確認を行う。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5
56	1. 人的・組織的対策	1.5. 運用状況のモニタリング	②機器や媒体の定期的な所在確認	②-3	個人情報が保存されている機器や媒体は、サービスの提供及び運用上、必要最低限とし、定期的に所在確認や棚卸し等を行う。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5
57	1. 人的・組織的対策	1.5. 運用状況のモニタリング	③システム構成やソフトウェアの動作状況に関する	③-1	システム構成やソフトウェアの動作状況に関する内部監査の内容、手順等を運用管理規程等に含める。	Google は ISO27001 認証を受けています。この基準では、「変更管理」（附属書 A.12.1.2）、「システムの取得、開発および保守」（ISO 27001 2013、附属書 A.14）が規定されています。 詳しくはGoogle インフラストラクチャのセキュリティ設計の概要をご覧ください。 https://cloud.google.com/security/security-design/ Google Cloud のお客様は、変更管理とシステム開発の手続きを含むお使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.2,14

			内部監査の実施				
58	1. 人的・組織的対策	1.6. 物理的に情報を搬送する場合の対策	①組織外に持出する情報に対する暗号化等の対策	①-1	物理的に情報を搬送する際には以下の対策を実施する。 ・ 医療機関等が合意する基準にもとづいて信頼できる配送業者を選択する。 ・ 配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐ。 ・ 配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認する。 ・ 配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用する。 ・ 電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さない。 ・ 電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施す。	情報を保存する媒体は、Google のデータセンタからデータセンタ外に転送されません。Google Cloud のお客様が物理的に情報を搬送する場合は、お客様の責任において、本項目に対応ください。	-
59	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-1	受託した医療情報を保守･運用を行うために閲覧するのは必要最小限とする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
60	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三	①-2	①-1の閲覧が必要な場合には、緊急時を除き、システム管理者の事前･事後の承認により実施する。	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。 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。	・ISO 27001 2013, 附属書 A.9

			者提供の制限			データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
61	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-3	受託した医療情報を緊急時に閲覧した場合には、閲覧した受託情報の範囲及び緊急で閲覧が必要な理由等を示して、システム管理者の承認を得る。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
62	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-4	①-1～①-3における閲覧に係る範囲、手順等について、医療機関等と合意する。また①-2、①-3により医療情報を閲覧した場合に、速やかに医療機関等にその旨の報告を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も	・ISO 27001 2013, 附属書 A.9

						同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
63	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-5	受託した医療情報の解析･分析は、医療情報システム等提供に係る契約とは独立した契約に基づいて医療機関等からの委託を受けた場合を除いて行わない。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。お客様のデータは常に契約に基づいた方法で処理されます。 Googleのプライバシー保護の責任： https://cloud.google.com/security/privacy/?hl=ja	-
64	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-6	受託した医療情報を匿名加工した情報も、医療情報に準じて取り扱う。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。お客様のデータは常に契約に基づいた方法で処理されます。 Googleのプライバシー保護の責任： https://cloud.google.com/security/privacy/?hl=ja	-
65	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-7	受託した医療情報は、法令による場合又は医療機関等の指示に基づく場合を除き、患者本人を含め、第三者への提供は行わない。	Google Cloud と Google Workspace は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持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。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約をご覧ください。 利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	-
66	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-8	①-7の内容を、医療情報システム等提供に係る契約に含める。	Google Cloud と Google Workspace は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持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。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約とをご覧ください。 利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	-
67	1. 人的・組織的対策	1.7. 解析及び第三	①受託した医療情報の解析	①-9	医療機関等の指示に基づき、受託した医療情報の第三者提供（閲覧）を行う場合には、医療機関等が許諾した者以外が閲覧･取得できないように対応策を講じる。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。お客様のデータは常に契約に基づいた方法で処理されます。 Googleのプライバシー保護の責任：	-

		者提供の制限	及び第三者提供の制限			https://cloud.google.com/security/privacy/?hl=ja	
68	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-10	①-9により、第三者提供（閲覧）を行う場合には、閲覧･取得が可能な者のID及び利用権限について、医療機関等又はその委託を受けた者（医療情報連携ネットワーク等）の指示に基づき、速やかに変更･削除できる対応を行う。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。お客様のデータは常に契約に基づいた方法で処理されます。 Googleのプライバシー保護の責任： https://cloud.google.com/security/privacy/?hl=ja	-
69	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-11	医療機関等の指示に基づいて受託した医療情報の第三者提供を行った場合には、医療機関等に対してその内容（提供先（閲覧者）、閲覧情報、閲覧日時等）の報告を行う。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。お客様のデータは常に契約に基づいた方法で処理されます。 Googleのプライバシー保護の責任： https://cloud.google.com/security/privacy/?hl=ja	-
70	1. 人的・組織的対策	1.7. 解析及び第三者提供の制限	①受託した医療情報の解析及び第三者提供の制限	①-12	①-7～①-11により第三者提供及びその報告を行うための条件、範囲等について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。お客様のデータは常に契約に基づいた方法で処理されます。 Googleのプライバシー保護の責任： https://cloud.google.com/security/privacy/?hl=ja	-
71	1. 人的・組織的対策	1.8. 情報の破棄に係る記録の提出	①情報の破棄に係る実施記録の取得及び医療機関等への提出	①-1	情報の破棄を実施した場合に、医療機関等の求めに応じて、実施担当者及び情報の削除方法（電磁記録媒体の消磁･物理的破壊等）を含む実施内容を医療機関等に対して報告し、破棄記録等を提出する。	ストレージメディアのセキュリティ管理をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はデータセンターにある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、バーコード及び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。構成要素がライフサイクル中の任意の時点で性能試験に合格しなかった場合は、インベントリから削除され、撤去されます。Google ハードドライブは、ハードディスク暗号化 (FDE) やドライブロックなどの技術を利用して、保存中のデータを保護します。Google の施設を離れたリムーバブルメディア上の個人識別情報(PII)は承認を経て、暗号化されます。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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。Google は、利用が定められた自動ワークフローツールを利用して、サニタイズ及び破壊プロセスを通じてディスクをレビュー、承認、追跡しています。	-
72	1. 人的・組織的対策	1.8. 情報の破棄に係る記録の提出	①情報の破棄に係る実施記録の取得及び医療機関等への提出	①-2	物理的な電子媒体の破壊措置及び破壊した電子媒体の処分については受託事業者自身で行うことが望ましい。外部の専門事業者に依頼する場合には、事業者選択の根拠を医療機関等に示し十分な理解を得る。また、破壊措置により情報の読み出しが不可能となったことの証明書等を受け取り、保管しておく。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7

						には、所定の権限を持つ人が、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。	
73	1. 人的・組織的対策	1.8. 情報の破棄に係る記録の提出	①情報の破棄に係る実施記録の取得及び医療機関等への提出	①-3	①-1で講じる措置及び資料を提供するのに必要な条件等について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約とをご覧ください。 利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html	・ISO 27001 2013, 附属書 A.8.3.2,11.2.7
74	1. 人的・組織的対策	1.8. 情報の破棄に係る記録の提出	①情報の破棄に係る実施記録の取得及び医療機関等への提出	①-4	医療情報システム等提供の停止又は医療機関等における医療情報システム等利用停止が生じた場合は、速やかに、記録の削除、媒体の廃棄等を行う。記録の削除、媒体の廃棄等を行った場合には、これを証明する資料を医療機関等に対して提出する。	ストレージメディアのセキュリティ管理をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はデータセンターにある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、バーコード及び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。構成要素がライフサイクル中の任意の時点で性能試験に合格しなかった場合は、インベントリから削除され、撤去されます。Google ハードドライブは、ハードディスク暗号化 (FDE) やドライブロックなどの技術を利用して、保存中のデータを保護します。Google の施設を離れたリムーバブルメディア上の個人識別情報(PII)は承認を経て、暗号化されます。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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。Google は、利用が定められた自動ワークフローツールを利用して、サニタイズ及び破壊プロセスを通じてディスクをレビュー、承認、追跡しています。	-
75	1. 人的・組織的対策	1.8. 情報の破棄に	①情報の破棄に係る実施記	①-5	①-4に関して、医療機関等へのサポート（所管官庁への情報提供含む）等に関連して必要最低限の範囲で、記録を保持し続ける場合には、その目的、範囲、期	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。お客様のデータは常に契約に基づいた方法で処理されます。 Googleのプライバシー保護の責任：	-

		係る記録の提出	録の取得及び医療機関等への提出		間、記録の管理方法、安全管理措置、連絡先等について、医療機関等と合意する。	https://cloud.google.com/security/privacy/?hl=ja	
76	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-1	情報システム等に関する再委託を行う場合には、事前に医療機関等の管理者に対して説明を行い、合意を得る。また、当該再委託に係る契約において体制を明確にする。	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。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google のデータ処理およびセキュリティ条項は、お客様が復処理者の変更に反対するプロセスを記述しています(DPST 11.4 復処理者の変更に対する異議申し立ての機会)。 a.期間中、新しいサードパーティの復処理者が関与した場合、Google は、新規サードパーティ復処理者がお客様データの処理を開始する少なくとも30日前にお客様に通知します(関連する復処理者の名前と場所、およびそれが実行する活動を含む)。 b.お客様は、新しいサードパーティ復処理者の従事について通知を受けてから90日以内にGoogle に契約の解除を届け出ることで、異議を申し立てることができます。 この契約の解約権は、お客様が新しいサードパーティ復処理者に異議を唱える場合の唯一かつ排他的な救済策です。	・ISO 27001 2013, 附属書 A.15
77	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-2	再委託先には、自社と同等の個人情報保護指針等を遵守させる。	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。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はサービスを提供するために、事実上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。	・ISO 27001 2013, 附属書 A.15
78	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-3	再委託に係る契約に、委託業務に係る守秘義務を含める。	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。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はサービスを提供するために、事実上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。	・ISO 27001 2013, 附属書 A.15
79	1. 人的・組織的対策	1.9. 再委託を行う場合の再	①再委託を行う場合の医療機関等へ	①-4	再委託先に対して、委託先要員に自社と同等の守秘義務があることを確認する。	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。 セキュリティに対するベンダーの取り組みをはじめとする、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。	・ISO 27001 2013, 附属書 A.15

		委託先の管理	の情報提供と再委託先の適切な監督			Google はサービスを提供するために、事実上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。	
80	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-5	医療情報システム等の保守等の体制変更が生じた場合に、医療機関等に行う報告の範囲、内容等及びその情報の提供に関する条件について、医療機関等と合意する。	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud - 利用規約: https://cloud.google.com/terms/ Google Workspace - 利用規約: https://workspace.google.com/terms/premier_terms.html セクション「1.4 変更 (a) 本サービスに対する変更」は、「Google は、本サービスに対して、商業上合理的な変更を随時行うことができます。Google が本サービスに対してお客様に大きな影響を与える重要な変更を加える場合、お客様がそのような変更の通知を受け取るよう Google に登録済みであれば、Google はお客様に通知を行うものとします」に言及しています。	-
81	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-6	医療情報システム等の保守に関して、外部事業者にその一部又は全部を委託する場合には、自社において実施している運用管理規程及び安全管理措置等への対応を、当該外部事業者に対して求める。	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。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はサービスを提供するために、事実上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。	・ISO 27001 2013, 附属書 A.15
82	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-7	①-6の実施状況に関して、契約実施ごとに又は定期的に、外部事業者に対して報告を求め、確認する。	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。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はサービスを提供するために、事実上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。	・ISO 27001 2013, 附属書 A.15
83	1. 人的・組織的対策	1.9. 再委託を行う場合の再	①再委託を行う場合の医療	①-8	再委託先により提供される医療情報システム等の安全管理策及びサービスレベルが十分であることを確認する。	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。	・ISO 27001 2013, 附属書 A.15

		委託先の管理	機関等への情報提供と再委託先の適切な監督			セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はサービスを提供するために、事実上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。	
84	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-9	再委託先による医療情報システム等の実施、運用、維持について定期的に検証する。	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。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はサービスを提供するために、事実上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。	・ISO 27001 2013, 附属書 A.15
85	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-10	再委託先による医療情報システム等の実施、運用、維持について定期的サービス実施について事前、事後報告を義務づけ、報告内容を点検確認する。	サードパティリスク管理に対する取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は本プロダクトやサービスを支援している復処理者のパフォーマンスやセキュリティに対する姿勢を定期的にレビューしています。	-
86	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-11	再委託先による医療情報システム等を実施する人員は予め届け出を行い、サービス実施時に不正な人員を受入れない。	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。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はお客様のデータにアクセスのできる復処理者とSub-Data Processor Agreement（SDPA）を締結しています。SDPA は、Google がお客様のデータへのアクセスを与える前に、 Google のお客様のデータに関する義務を果たすために復処理者が満たさなければならないセキュリティやプライバシーの義務を定めています。これらの義務は身元調査のような担当者のセキュリティに関する要求事項も含んでいます。	・ISO 27001 2013, 附属書 A.15
87	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委	①-12	医療情報システム等の実施中に再委託先が管理区域に立ち入る場合は顔写真を券面に入れた身分証明を携帯する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物	・ISO 27001 2013, 附属書 A.11

			託先の適切な監督			理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	
88	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-13	再委託先による医療情報システム等の実施にともなう処理施設内への立ち入り手順に関しては、受託事業者の職員の入室、退室手順に準ずる。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	・ISO 27001 2013, 附属書 A.11
89	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-14	再委託先による医療情報システム等の変更時には、引き続き安全性が維持されていることについて適切な検証を行う。	サードパティリスク管理に対する取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は本プロダクトやサービスを支援している復処理者のパフォーマンスやセキュリティに対する姿勢を定期的にレビューしています。	-
90	1. 人的・組織的対策	1.9. 再委託を行う	①再委託を行う場	①-15	医療情報システム等の保守点検作業を外部事業者に委託する場合には、「医療情報システムの安全管理に関	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-

		場合の再委託先の管理	合の医療機関等への情報提供と再委託先の適切な監督		するガイドライン第 5 版」6.8 章 C 項の管理策を実施する。		
91	1. 人的・組織的対策	1.9. 再委託を行う場合の再委託先の管理	①再委託を行う場合の医療機関等への情報提供と再委託先の適切な監督	①-16	外部事業者が医療情報システム等を実施する際は、受託事業者又は外部事業者の正規職員が管理している状況で作業を行うことが望ましい。	Google は ISO27001 認証を受けています。この基準では、「供給者関係」（ISO 27001 2013、附属書 A.15）が規定されています。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はお客様のデータにアクセスのできる復処理者とSub-Data Processor Agreement（SDPA）を締結しています。SDPA は、Google がお客様のデータへのアクセスを与える前に、 Google のお客様のデータに関する義務を果たすために復処理者が満たさなければならないセキュリティやプライバシーの義務を定めています。これらの義務は身元調査のような担当者のセキュリティに関する要求事項も含んでいます。	・ISO 27001 2013, 附属書 A.15
92	1. 人的・組織的対策	1.10. 非常時に備えた対応	①医療情報システム等の提供に係る事業影響度分析の実施	①-1	医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理装置等について識別する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.17.2,12.3
93	1. 人的・組織的対策	1.10. 非常時に備えた対応	①医療情報システム等の提供に係る事業影響度分析の実施	①-2	業務プロセス間の相互関係を評価する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、	・ISO 27001 2013, 附属書 A.17.2,12.3

						地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
94	1. 人的・組織的対策	1.10. 非常時に備えた対応	①医療情報システム等の提供に係る事業影響度分析の実施	①-3	事業を継続するための業務プロセスの優先順位を明確にする。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.17.2,12.3
95	1. 人的・組織的対策	1.10. 非常時に備えた対応	①医療情報システム等の提供に係る事業影響度分析の実施	①-4	医療情報システム等に発生するハードウェア及びソフトウェアの障害が業務プロセスに与える影響について識別する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。	・ISO 27001 2013, 附属書 A.17.2,12.3

						冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
96	1. 人的・組織的対策	1.10. 非常時に備えた対応	①医療情報システム等の提供に係る事業影響度分析の実施	①-5	医療情報システム等に発生するハードウェア及びソフトウェアの障害が他のハードウェア、ソフトウェアに及ぼす影響、相互作用について認識し、影響度の大きなハードウェア及びソフトウェアを識別する。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」（ISO 27001 2013、附属書 A.17.1）が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.17.2,12.3
97	1. 人的・組織的対策	1.10. 非常時に備えた対応	②医療情報システム等の提供に係る事業継続のための計画策定と模擬試験等による検証	②-1	医療情報システム等の提供における業務プロセス及び医療情報システム等の優先順位にもとづいて、医療情報処理に関する事業継続計画を策定する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。	・ISO 27001 2013, 附属書 A.17.2,12.3

						Google Cloud 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。	
98	1. 人的・組織的対策	1.10. 非常時に備えた対応	②医療情報システム等の提供に係る事業継続のための計画策定と模擬試験等による検証	②-2	策定した事業継続計画について模擬試験を含めた適切な方法でレビューする。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.17.2,12.3
99	1. 人的・組織的対策	1.10. 非常時に備えた対応	②医療情報システム等の提供に係る事業継続のための計画策定と模擬試験等による検証	②-3	事業継続計画について定期的に見直しを行う。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.17.2,12.3

100	1. 人的・組織的対策	1.10. 非常時に備えた対応	②医療情報システム等の提供に係る事業継続のための計画策定と模擬試験等による検証	②-4	策定される事業継続計画には次のような事項を含むことが望ましい。 ・ 事前準備計画 ・ 「非常時」判断手順 ・ 関係者の召集、対応本部の設置 ・ 機器及び作業員の縮退措置及び代替施設の手配措置 ・バックアップ施設等、代替施設への切替え措置 ・ 代替施設運用中の考慮事項（非常時アカウントの運用手順、復帰後に医療情報を正常システムに同期するための配慮等） ・障害の拡大範囲に関する判断手順、基準 ・正常復帰の判断手順、基準 ・正常復帰後の医療情報システム等の点検手順（不正侵入、情報改竄、情報破損等の検出等） ・ 所管官庁への連絡体制、等	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.17.2,12.3
101	1. 人的・組織的対策	1.10. 非常時に備えた対応	②医療情報システム等の提供に係る事業継続のための計画策定と模擬試験等による検証	②-5	策定した事業継続計画に基づくサービス内容について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.17.2,12.3
102	1. 人的・組織的対策	1.10. 非常時に備えた対応	③医療情報システム等復旧後におけ	③-1	非常時に行ったデータ処理の結果が、サービス回復後に齟齬が生じないよう、データの整合性を確保するための対応策（規約の策定･検証方法の規定等）を講じる。	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。	・ISO 27001 2013, 附属書 A.17.1

			る整合性確保			Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
103	1. 人的・組織的対策	1.10. 非常時に備えた対応	④非常時用の利用者アカウントや機能の管理手順の策定	④-1	非常時に用いる利用者アカウント及び非常時用の機能の有効化のための措置について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）、「バックアップ」（ISO27001 2013、附属書 A.12.3）と「操作手順書」（ISO27001 2013、附属書 A.12.1.1.）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.17.2,12.3,12.1.1
104	1. 人的・組織的対策	1.10. 非常時に備えた対応	④非常時用の利用者アカウントや機能の管理手順の策定	④-2	非常時に用いる利用者アカウントの利用状況については定期的にレビューを行う。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）、「バックアップ」（ISO27001 2013、附属書 A.12.3）と「操作手順書」（ISO27001 2013、附属書 A.12.1.1.）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計	・ISO 27001 2013, 附属書 A.17.2,12.3,12.1.1

						全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	
105	1. 人的・組織的対策	1.10. 非常時に備えた対応	④非常時用の利用者アカウントや機能の管理手順の策定	④-3	非常時に用いる利用者アカウントが利用された場合、システム管理者及び運用者がこれを速やかに確認できるための措置を講じる。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）、「バックアップ」（ISO27001 2013、附属書 A.12.3）と「操作手順書」（ISO27001 2013、附属書 A.12.1.1.）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3,12.1.1
106	1. 人的・組織的対策	1.10. 非常時に備えた対応	④非常時用の利用者アカウントや機能の管理手順の策定	④-4	非常時に有効化した利用者アカウント及び非常時用の機能については、正常復帰後、速やかに無効化を図る。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）、「バックアップ」（ISO27001 2013、附属書 A.12.3）と「操作手順書」（ISO27001 2013、附属書 A.12.1.1.）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生して	・ISO 27001 2013, 附属書 A.17.2,12.3,12.1.1

						も、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	
107	1. 人的・組織的対策	1.11. サイバー攻撃等による障害発生時の対応	①サイバー攻撃等による障害発生時の医療機関等への速やかな状況報告	①-1	サイバー攻撃等により、サービスの提供に支障が生じた場合において、サービスに生じている障害の状況及び復旧に関する見通し等について、医療機関等に速やかに報告を行う。	Google は ISO27001 認証を受けています。この基準では、「ネットワーク及びネットワークサービスへのアクセス」（ISO27001 2013、附属書 A.9.1.2）と「ネットワーク管理策」（ISO27001 2013、附属書 A.13.1.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、最も高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、犯罪科学や証拠取り扱いの訓練を受けています。お客様の機密情報が保存されるシステムなどの重要な分野では、インシデント対応計画のテストが実施されます。これらのテストでは、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。インシデントで顧客データが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、不正アクセスを適切に検知し、レビューすることを含むお使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9.1.2, 13.1.1
108	1. 人的・組織的対策	1.11. サイバー攻撃等による障害発生時の対応	①サイバー攻撃等による障害発生時の医療機関等への速やかな状況報告	①-2	サイバー攻撃等により、サービスの提供に支障が生じた場合において、医療機関等が行う必要のある所管官庁への連絡･報告のために提供する資料の範囲、条件等について、医療機関と合意する。	Google は ISO27001 認証を受けています。この基準では、「ネットワーク及びネットワークサービスへのアクセス」（ISO27001 2013、附属書 A.9.1.2）と「ネットワーク管理策」（ISO27001 2013、附属書 A.13.1.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、最も高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、犯罪科学や証拠取り扱いの訓練を受けています。お客様の機密情報が保存されるシステムなどの重要な分野では、インシデント対応計画のテストが実施されます。これらのテストでは、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。インシデントで顧客データが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、不正アクセスを適切に検知し、レビューすることを含むお使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9.1.2, 13.1.1

109	1. 人的・組織的対策	1.11. サイバー攻撃等による障害発生時の対応	①サイバー攻撃等による障害発生時の医療機関等への速やかな状況報告	①-3	医療機関等が所管官庁に対して法令に基づき提出する資料を円滑に提出できるよう、サービスの提供に用いるアプリケーション、プラットフォーム、サーバ･ストレージ等は国内法の執行が及ぶ場所に設置する。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はクラウドを利用するお客様に、データ処理と保存のロケーション選択権利を提供しています。ローケーション別のプロダクト提供状況の一覧は、Google のウェブサイト上で公開しています（https://cloud.google.com/about/locations）。 Google Workspace のお客様は、対象となる特定のデータをどこに保存するか（米国、ヨーロッパ全体、又はグローバルに分散するか）を選択できます。データエクスポートツールはGoogle Workspace コアサービスと Google Workspace のお客様にデータを書き出す機能を提供し、書き出したデータはお客様の場所に保存できます。 データエクスポートツールは通常、ユーザーが Google Takeout で利用できるデータと同じデータに加えて、管理者のみが利用できるデータを書き出します。 データエクスポートツールを使用して書き出したデータに含まれる情報は、Google のウェブサイト上で公開しています（https://support.google.com/a/answer/100458?hl=en）。	・ISO 27002 2013、附属書 A.5, A.6
110	1. 人的・組織的対策	1.11. サイバー攻撃等による障害発生時の対応	②サイバー攻撃等による原因調査のためのログ等の記録の保全	②-1	サイバー攻撃等により、サービスの提供に支障が生じた場合に、その原因探査に必要なログ等の記録を保全するための措置を講じる。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ISO27002 2013、附属書 A.6）が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は規程や Google のデータ保持の要求事項に沿って方針や手続を定めています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.5, 6
111	1. 人的・組織的対策	1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-1	ネットワーク経路におけるウイルスや不正なメッセージの混入等の改竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
112	1. 人的・組織的対策	1.12. ネットワーク上の責任範	①外部と医療情報を交換する際の責任範囲・	①-2	ネットワーク経路におけるウイルスや不正なメッセージの混入等の改竄に対する防護措置に関する受託事業者の役割の範囲について、医療機関等と合意する。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試	・ISO 27001 2013, 附属書 A.12.2

		囲・役割の合意	役割の合意			行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	
113	1. 人的・組織的対策	1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-3	ネットワークで用いられる医療機関等の施設内のルータについて、これを経由して施設間を結ぶVPNの間で送受信ができないように経路設定すること等に関する受託事業者の役割分担について、医療機関等と合意する。	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。 データおよびデータを保存または処理するシステムを含む情報リソースへのアクセスは、最小特権の原則に基づいて承認されています。 ネットワークデバイスへのアクセスは、ユーザーID、パスワード、セキュリティキー、および/または証明書によって認証されます。 アクセスが許可される前に、外部システムのユーザーが Google アカウント認証システムを介して識別および認証されます。	・ISO 27001 2013, 附属書 A.9
114	1. 人的・組織的対策	1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-4	回線の管理、品質等に対する受託事業者の責任の範囲、役割等について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」（ISO 27001 2013、附属書 A.13）と「公衆ネットワーク上のアプリケーション サービスのセキュリティの考慮」（ISO27002 2013、附属書 A.14.1.2）が規定されています。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.13,14.1.2
115	1. 人的・組織的対策	1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-5	通常運用時及び非常時の医療機関等と受託事業者との起点から終点までの通信手順、その他厚生労働省ガイドライン第5版6.11 C項の6で定めるネットワーク経路及びこれに関連する機器等に係る責任の所在を明確にし、受託事業者の負う責任の範囲、役割等について、医療機関等と合意する。	Google Cloud と Google Workspace は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持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。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	-
116	1. 人的・組織的対策	1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-6	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。	Google Cloud と Google Workspace は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持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。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	-
117	1. 人的・組織的対策	1.12. ネットワーク上の責任範	①外部と医療情報を交換する際の責	①-7	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う責任の範囲、役割等について、医療機関等と合意する。	Google Cloud と Google Workspace は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持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。 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。	-

		囲・役割の合意	任範囲・役割の合意			利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	
118	1. 人的・組織的対策	1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-8	サービスにより管理する医療情報を患者等の閲覧に供する場合に、受託事業者において対応すべきセキュリティ上の措置の条件、内容等について、医療機関等と合意する。	Google Cloud と Google Workspace は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持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。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	-
119	1. 人的・組織的対策	1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-9	交換する情報の機密レベルについて、受領側で機密レベルが低くならないよう、医療機関等と合意する。	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。 インターネットを介した認証と管理者アクセスを保護するために暗号化を使用しています。Google が管理するマシンにリモートアクセスする場合は、Google が発行したデジタル証明書と2要素認証を必要とします。 Google は、Google Cloud プロダクトと Google Workspace プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://cloud.google.com/security/encryption-in-transit/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Google Cloud 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。	・ISO 27001 2013, 附属書 A.10
120	1. 人的・組織的対策	1.12. ネットワーク上の責任範囲・役割の合意	①外部と医療情報を交換する際の責任範囲・役割の合意	①-10	医療機関等の管理者の患者等に対する説明責任、管理責任等に関し、受託事業者が負う責任の範囲、役割等について、医療機関等と合意する。	Google Cloud と Google Workspace は、クラウド プロバイダのための ISO27017 認証を受けています。機密保持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。 詳しくは、契約上の義務や契約内容をまとめた Google の利用規約と SLA をご覧ください。 利用規約 https://cloud.google.com/terms/ https://workspace.google.com/terms/dpa_terms.html SLA: https://workspace.google.com/terms/sla.html https://cloud.google.com/terms/sla/	-
121	1. 人的・組織的対策	1.13. 機器・ソフトウェア	①医療情報システム等に関する構成	①-1	医療情報システム等における機器及びソフトウェアの構成図を作成する。	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。	・ISO 27001 2013, 附属書 A.8.1, 8.3.2, 11.2.7, 12.5

		の品質管理	図や仕様に係るドキュメント作成			Google Cloud と Google Workspace のプロダクトについてはSOC 2、Type II の「A.オペレーション概要」に記載されており、第三者機関によるレビューと検証を受けています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	
122	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	①医療情報システム等に関する構成図や仕様に係るドキュメント作成	①-2	医療情報システム等のネットワーク構成図を作成する。	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）、「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）、「操作手順書」（附属書 A.12.1.1）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google は、ネットワーク上に新しいサーバー、ルーター、スイッチを構成及びインストールする際の手順とチェックリストを文書化しています。 ネットワークは、Google の本番ネットワークの性質と適用可能な要件を説明するネットワーク図と構成文書に記載されています。 この文書は、社内ネットワーク上のアクセスが制限された部分にあります。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,11.2.7,12.1.1, 12.5
123	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	①医療情報システム等に関する構成図や仕様に係るドキュメント作成	①-3	①-1、①-2で作成する各構成図に含まれる機器等について、システム要件等の説明を付した資料を作成する。	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）、「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）、「操作手順書」（附属書 A.12.1.1）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google は、ネットワーク上に新しいサーバー、ルーター、スイッチを構成及びインストールする際の手順とチェックリストを文書化しています。 ネットワークは、Google の本番ネットワークの性質と適用可能な要件を説明するネットワーク図と構成文書に記載されています。 この文書は、社内ネットワーク上のアクセスが制限された部分にあります。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,11.2.7,12.1.1, 12.5
124	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	①医療情報システム等に関する構成図や仕様に係るドキュメント作成	①-4	医療情報システム等を構成する機器及びソフトウェア等の更新の仕様等に関する資料並びにその更新履歴を作成する。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google Cloud と Google Workspace のプロダクトについては SOC 2、Type II の「A.オペレーション概要」に記載されており、第三者機関によるレビューと検証を受けています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5
125	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	①医療情報システム等に関する構成図や仕様に係るドキュメント作成	①-5	①-1～①-4で策定した資料等を医療機関等の求めに応じて提出することについて、開示内容、範囲、条件等を医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google Cloud と Google Workspace のプロダクトについては SOC 2、Type II の「A.オペレーション概要」に記載されており、第三者機関によるレビューと検証を受けています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5
126	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	②機器・ソフトウェアの導入や変更における事前検証の実施	②-1	保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行う。	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）、「変更管理」（附属書 A.12.1.2）、「システムの取得、開発、保守」（附属書 A.14）が規定されています。 詳細は Google インフラストラクチャのセキュリティ設計の概要をご覧ください。 https://cloud.google.com/security/security-design/ Google Cloud のお客様は、変更管理を含んだ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。	・ISO 27001 2013, 附属書 A.11.2.4, 12.1.2, 14

127	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	②機器・ソフトウェアの導入や変更における事前検証の実施	②-2	変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を講じる。	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）が規定されています。詳しくは、「Google インフラストラクチャのセキュリティ設計の概要」（https://cloud.google.com/security/security-design/）をご覧ください。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.12.1.2,14
128	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	②機器・ソフトウェアの導入や変更における事前検証の実施	②-3	情報処理に供するアプリケーションについては、受託事業者自身で開発したアプリケーションを用いる。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いる。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」（ISO 27001 2013、附属書 A.14）が規定されています。詳しくは、「Google インフラストラクチャのセキュリティ設計の概要」（https://cloud.google.com/security/security-design/）をご覧ください。 Google Cloud のお客様は、システム開発の手順など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.14
129	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	②機器・ソフトウェアの導入や変更における事前検証の実施	②-4	ソフトウェアに不正プログラムが混入することが無いよう、バイナリコードレベル、ソースコードレベルの双方で検証プロセスを実施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、「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。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.14
130	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	②機器・ソフトウェアの導入や変更における事前検証の実施	②-5	業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入する。	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。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.14
131	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	③本番環境と開発環境の分離	③-1	ソフトウェア開発を行う際には、運用されているソフトウェアに影響を与えない環境で行う。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.4,14.2
132	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	③本番環境と開発環境の分離	③-2	開発施設では不正プログラムが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には不正プログラムへの対策を行う。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.4,14.2
133	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	③本番環境と開発環境の分離	③-3	運用施設に保存されている医療情報を開発施設及び試験施設にコピーしない。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.4,14.2

134	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	③本番環境と開発環境の分離	③-4	運用システムの混乱を避けるため、開発用コード又はコンパイラ等の開発ツール類を運用システム上に置かない。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.4,14.2
135	1. 人的・組織的対策	1.13. 機器・ソフトウェアの品質管理	③本番環境と開発環境の分離	③-5	情報処理に不必要なファイル等を運用システム上におかない。	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）が規定されています。ソフトウェアの開発管理をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.14
136	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	①医療情報システム等に用いる機器やソフトウェアのサポート	①-1	医療情報を格納する機器、媒体等の見読性が確保されていることを定期的に確認する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.17.2,12.3
137	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	①医療情報システム等に用いる機器やソフトウェアのサポート	①-2	受託する医療情報を格納する機器･媒体等の見読性確保が困難となる可能性がある場合（媒体の劣化、読取装置等のサポート切れ等）、速やかに代替的な措置を講じ、見読性確保のための対応を行う。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。	・ISO 27001 2013, 附属書 A.17.2,12.3

						冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
138	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	①医療情報システム等に用いる機器やソフトウェアのサポート	①-3	それぞれの装置は製造元又は供給元が指定する間隔及び仕様に従って保守点検を行い、必要であれば交換を行う。	Google は ISO27001 認証を受けています。この基準では、「装置の保守」（ISO 27001 2013、附属書 A.11.2.4）「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）が規定されています。 Google はデータセンターにある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、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクル内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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.11.2.4, 8.1, 8.3.2, 11.2.7
139	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	①医療情報システム等に用いる機器やソフトウェアのサポート	①-4	情報システムに関する機器については、定期的に劣化状況に関する検査を行い、必要な措置を講じる。	Google は ISO27001 認証を受けています。この基準では、「装置の保守」（ISO 27001 2013、附属書 A.11.2.4）、「変更管理」（附属書 A.12.1.2）、「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。 Google は本番機器やネットワーク装置を支えるインフラストラクチャ—ハードウェアに予防的なメンテナンスと通常のメンテナンスの双方を実施しています。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。	・ISO 27001 2013, 附属書 A.11.2.4,12.1.2,14
140	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	①医療情報システム等に用いる機器やソフトウェアのサポート	①-5	医療情報システム等について、機器やソフトウェア等の提供事業者におけるサポート終了等が生じた場合は、サービスへの影響範囲について分析を行い、必要な措置を講じる。	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud 利用規約: https://cloud.google.com/terms/ セクション1.4(d)サービスの中止:「Google は、サービス(または関連する重要な機能)を中止する少なくとも12ヶ月前にお客様に通知します。ただし、Google が、このような中止されたサービスまたは機能を実質的に類似したサービスまたは機能に置き換える場合を除きます。 さらに、Google は、後方互換性のない方法で顧客向けGoogle APIを大幅に変更する前に、少なくとも12ヶ月前にお客様に通知します。 このセクション1.4(d) (サービスの中止)には、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりする Google の能力を制限するものはありません。 このセクション1.4(d) (サービスの中止)は、一般より前に利用可能なサービス、オファリング、または機能には適用されません。 Google Workspace 利用規約: https://workspace.google.com/terms/premier_terms.html	-

						セクション1.4(e)コアサービスの中止:「Google は、コアサービス(または関連する重要な機能)を中止する少なくとも12ヶ月前に、お客様に通知します。ただし、Google が、中止されたコアサービスまたは機能を実質的に類似したコアサービスまたは機能に置き換える場合を除きます。 このセクション1.4(e) (コアサービス の中止） では、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(e)(コアサービスの中止)は、その他のサービスや、一般より前に利用可能なサービス、オファリング、または機能には適用されません。	
141	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	①医療情報システム等に用いる機器やソフトウェアのサポート	①-6	医療情報システム等について、機器の劣化や提供事業者における機器やソフトウェア等のサポート終了等により、サービスの一部又は全部の提供が困難となる場合やサービスに変更が生じる場合には、利用している医療機関等への影響を最小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud 利用規約: https://cloud.google.com/terms/ セクション1.4(d)サービスの中止:「Google は、サービス(または関連する重要な機能)を中止する少なくとも12ヶ月前にお客様に通知します。ただし、Google が、このような中止されたサービスまたは機能を実質的に類似したサービスまたは機能に置き換える場合を除きます。 さらに、Google は、後方互換性のない方法で顧客向けGoogle APIを大幅に変更する前に、少なくとも12ヶ月前にお客様に通知します。 このセクション1.4(d) (サービスの中止)には、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(d) (サービスの中止)は、一般より前に利用可能なサービス、オファリング、または機能には適用されません。 Google Workspace 利用規約: https://workspace.google.com/terms/premier_terms.html セクション1.4(e)コアサービスの中止:「Google は、コアサービス(または関連する重要な機能)を中止する少なくとも12ヶ月前に、お客様に通知します。ただし、Google が、中止されたコアサービスまたは機能を実質的に類似したコアサービスまたは機能に置き換える場合を除きます。 このセクション1.4(e) (コアサービス の中止） では、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(e)(コアサービスの中止)は、その他のサービスや、一般より前に利用可能なサービス、オファリング、または機能には適用されません。	-
142	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	①医療情報システム等に用いる機器やソフトウェアのサポート	①-7	①-6においてサービスの一部又は全部の停止、変更等が生じる場合の医療機関等への対応の内容、条件等について、医療機関等と合意する。	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud 利用規約: https://cloud.google.com/terms/ セクション1.4(d)サービスの中止:「Google は、サービス(または関連する重要な機能)を中止する少なくとも12ヶ月前にお客様に通知します。ただし、Google が、このような中止されたサービスまたは機能を実質的に類似したサービスまたは機能に置き換える場合を除きます。 さらに、Google は、後方互換性のない方法で顧客向けGoogle APIを大幅に変更する前に、少なくとも12ヶ月前にお客様に通知します。 このセクション1.4(d) (サービスの中止)には、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(d) (サービスの中止)は、一般より前に利用可能なサービス、オファリング、または機能には適用されません。 Google Workspace 利用規約: https://workspace.google.com/terms/premier_terms.html	-

						セクション1.4(e)コアサービスの中止:「Google は、コアサービス(または関連する重要な機能)を中止する少なくとも12ヶ月前に、お客様に通知します。ただし、Google が、中止されたコアサービスまたは機能を実質的に類似したコアサービスまたは機能に置き換える場合を除きます。 このセクション1.4(e) (コアサービス の中止） では、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(e)(コアサービスの中止)は、その他のサービスや、一般より前に利用可能なサービス、オファリング、または機能には適用されません。	
143	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	②保守作業に伴う医療情報システム等停止時間の最小化	②-1	情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画をたてて実施する。	Google は ISO27001 認証を受けています。この基準では、「装置の保守」（ISO 27001 2013、附属書 A.11.2.4）が規定されています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.11.2.4
144	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	②保守作業に伴う医療情報システム等停止時間の最小化	②-2	保守業務における事前の通知には、保守業務の影響が及ぶ範囲を明示し、保守業務が完遂しなかった場合を想定して原状回復に必要な時間の予測を含める。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、目標復旧時点（RPO）の目標も、目標復旧時間（RTO）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。	・ISO 27001 2013, 附属書 A.17.2
145	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	②保守作業に伴う医療情報システム等停止時間の最小化	②-3	保守業務の実施にあたっては、医療機関等がサービスを利用できない状況に陥らないよう十分な対応策を講じ、その手順を運用管理規程に含める。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。	・ISO 27001 2013, 附属書 A.17.2

						冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、目標復旧時点（RPO）の目標も、目標復旧時間（RTO）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。	
146	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	②保守作業に伴う医療情報システム等停止時間の最小化	②-4	②-3に定めた手順を医療機関等に示し、医療機関等と合意する。なお、本手順に基づき保守を行う際に必要となる事項等について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、目標復旧時点（RPO）の目標も、目標復旧時間（RTO）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。	・ISO 27001 2013, 附属書 A.17.2
147	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	②保守作業に伴う医療情報システム等停止時間の最小化	②-5	②-3で示された手順について、医療機関等が対応すべき事項がある場合、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、目標復旧時点（RPO）の目標も、目標復旧時間（RTO）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。	・ISO 27001 2013, 附属書 A.17.2
148	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影	③医療情報システム等の停止や仕様	③-1	サービスの一部又は全部の停止やサービス変更の場合（軽微なバージョンアップは含まない）には、医療情報システム等を利用している医療機関等への影響を最	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud 利用規約: https://cloud.google.com/terms/	-

		響の最小化	変更時の対応		小とするための措置を講じるほか、医療機関等が対応するために十分な期間をもって告知を行う。	セクション1.4(d)サービスの中止:「Google は、サービス(または関連する重要な機能)を中止する少なくとも12ヶ月前にお客様に通知します。ただし、Google が、このような中止されたサービスまたは機能を実質的に類似したサービスまたは機能に置き換える場合を除きます。 さらに、Google は、後方互換性のない方法で顧客向けGoogle APIを大幅に変更する前に、少なくとも12ヶ月前にお客様に通知します。 このセクション1.4(d) (サービスの中止)には、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(d) (サービスの中止)は、一般より前に利用可能なサービス、オファリング、または機能には適用されません。 Google Workspace 利用規約: https://workspace.google.com/terms/premier_terms.html セクション1.4(e)コアサービスの中止:「Google は、コアサービス(または関連する重要な機能)を中止する少なくとも12ヶ月前に、お客様に通知します。ただし、Google が、中止されたコアサービスまたは機能を実質的に類似したコアサービスまたは機能に置き換える場合を除きます。 このセクション1.4(e) (コアサービス の中止） では、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(e)(コアサービスの中止)は、その他のサービスや、一般より前に利用可能なサービス、オファリング、または機能には適用されません。	
149	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	③医療情報システム等の停止や仕様変更時の対応	③-2	③-1の場合、受託した医療情報を、医療機関等に返却する。返却するデータの範囲（データ種類、期間等）、データ形式(データ項目、項目の詳細、ファイル形式）、返却方法、条件については、医療機関等と合意する。また医療機関等のサービス利用開始後に、医療機関等と合意した内容を変更する場合には、③-1に準じた対応策を講じる。	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud 利用規約: https://cloud.google.com/terms/ セクション1.4(d)サービスの中止:「Google は、サービス(または関連する重要な機能)を中止する少なくとも12ヶ月前にお客様に通知します。ただし、Google が、このような中止されたサービスまたは機能を実質的に類似したサービスまたは機能に置き換える場合を除きます。 さらに、Google は、後方互換性のない方法で顧客向けGoogle APIを大幅に変更する前に、少なくとも12ヶ月前にお客様に通知します。 このセクション1.4(d) (サービスの中止)には、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(d) (サービスの中止)は、一般より前に利用可能なサービス、オファリング、または機能には適用されません。 Google Workspace 利用規約: https://workspace.google.com/terms/premier_terms.html セクション1.4(e)コアサービスの中止:「Google は、コアサービス(または関連する重要な機能)を中止する少なくとも12ヶ月前に、お客様に通知します。ただし、Google が、中止されたコアサービスまたは機能を実質的に類似したコアサービスまたは機能に置き換える場合を除きます。 このセクション1.4(e) (コアサービス の中止） では、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(e)(コアサービスの中止)は、その他のサービスや、一般より前に利用可能なサービス、オファリング、または機能には適用されません。	-
150	1. 人的・組織的対策	1.14. 変化に伴う医療機関	③医療情報システム等の停	③-3	③-2におけるデータの返却については、厚生労働省ガイドライン第5版「5情報の相互運用性と標準化について」に従って行うこととし、その内容について医療機	Google は、お客様の元のデータ形式を変更する可能性のある機能を提供しており、お客様はGoogle が提供する例えば以下のような仕様を理解する責任があります。	-

		等への影響の最小化	止や仕様変更時の対応		関等と合意する。なお、返却するデータに、受託事業者において実施した不可逆的な圧縮（画像データ等）や変換（パスワード等）によるデータが含まれる場合があるので、その旨も合わせて、医療機関等と合意する。	https://cloud.google.com/terms/data-processing-terms https://workspace.google.com/terms/dpa_terms.html https://support.google.com/a/answer/100458 https://support.google.com/accounts/answer/3024190. https://cloud.google.com/bigquery/docs/exporting-data https://cloud.google.com/sql/docs/mysql/import-export/exporting https://cloud.google.com/spanner/docs/import-export-csv https://cloud.google.com/datastore/docs/export-import-entities	
151	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	③医療情報システム等の停止や仕様変更時の対応	③-4	③-1においてサービスの変更を含む医療情報システム等の一部又は全部の停止（軽微なバージョンアップは含まない）が生じる場合の医療機関等への対応の内容（移行支援等で、③-2の対応は除く）、条件等について、医療機関等と合意する。	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud 利用規約: https://cloud.google.com/terms/ セクション1.4(d)サービスの中止:「Google は、サービス(または関連する重要な機能)を中止する少なくとも12ヶ月前にお客様に通知します。ただし、Google が、このような中止されたサービスまたは機能を実質的に類似したサービスまたは機能に置き換える場合を除きます。 さらに、Google は、後方互換性のない方法で顧客向けGoogle APIを大幅に変更する前に、少なくとも12ヶ月前にお客様に通知します。 このセクション1.4(d) (サービスの中止)には、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(d) (サービスの中止)は、一般より前に利用可能なサービス、オファリング、または機能には適用されません。 Google Workspace 利用規約: https://workspace.google.com/terms/premier_terms.html セクション1.4(e)コアサービスの中止:「Google は、コアサービス(または関連する重要な機能)を中止する少なくとも12ヶ月前に、お客様に通知します。ただし、Google が、中止されたコアサービスまたは機能を実質的に類似したコアサービスまたは機能に置き換える場合を除きます。 このセクション1.4(e) (コアサービス の中止） では、適用可能な法律に準拠するのに必要な変更をしたり、重要なセキュリティリスクに対処したり、実質的な経済的または重要な技術的負担を回避したりするGoogle の能力を制限するものはありません。 このセクション1.4(e)(コアサービスの中止)は、その他のサービスや、一般より前に利用可能なサービス、オファリング、または機能には適用されません。	-
152	1. 人的・組織的対策	1.14. 変化に伴う医療機関等への影響の最小化	③医療情報システム等の停止や仕様変更時の対応	③-5	医療機関等の都合により医療機関等の医療情報システム等利用が終了する場合も、③-2、③-3に示す対応策を講じる。	契約上の義務や契約内容をまとめた Google の利用規約をご参照ください。 Google Cloud - 利用規約: https://cloud.google.com/terms/; データ処理およびセキュリティ規約（お客様): https://cloud.google.com/terms/data-processing-terms Google Workspace - 利用規約: https://workspace.google.com/terms/premier_terms.html;データ処理の修正条項 https://workspace.google.com/terms/dpa_terms.html セクション9.1 アクセス;修正;制限付き処理;ポータビリティ:「本契約期間中、Google は、お客様が本サービスの機能と一貫性のある方法（セクション6.1(お客様による削除)に記載されているGoogle が提供する削除機能を含む）でお客様のデータへのアクセス、修正、処理の制限や、お客様のデータをエクスポートすることを可能にする。」	-
153	1. 人的・組織的対策	1.14. 変化に伴う医療機関	③医療情報システム等の停	③-6	③-1～③-5についての手順等を、運用管理規程等に含める。	Google は契約上の義務や契約内容をまとめた Google の利用規約を公開しています。 Google Cloud - 利用規約: https://cloud.google.com/terms/; データ処理およびセキュリティ規約（お客様): https://cloud.google.com/terms/data-processing-terms	-

		等への影響の最小化	止や仕様変更時の対応			Google Workspace - 利用規約: https://workspace.google.com/terms/premier_terms.html;データ処理の修正条項 https://workspace.google.com/terms/dpa_terms.html	
154	2.物理的対策	2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-1	機器や媒体の設置場所等のセキュリティ境界への入退管理については、個人認証システム等による制御に基づいて行い、入退者の特定ができるようにする。これによることが難しい場合には、例えば、入退に必要な暗証番号等の変更を週単位で行う等、入退者を特定しうる方策を講じる。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11
155	2.物理的対策	2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-2	機器や媒体の設置場所については、許可された者のみが入退できるように制限する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11

156	2.物理的対策	2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-3	医療情報システム等を設置、医療情報を保管する部屋の出入りを制限するため、有人の受付、機械式の認証装置のいずれか、あるいは双方を設置して、入退館及び入退室者の確実な認証を行う。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。立ち入りが許可されているのは特定の役割を持つ承認された社員のみです。こうしたエリアへのアクセスは監視・記録され、アクセス権原を定期的に見直しています。 Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。	・ISO 27001 2013, 附属書 A.11
157	2.物理的対策	2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-4	有人受付を置かずに機械式の認証装置により入退室者を管理する場合には、生体認証を一つ以上含む複数要素を利用した認証装置を利用する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	・ISO 27001 2013, 附属書 A.11
158	2.物理的対策	2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-5	有人受付、機械式入退管理のいずれの場合も認証履歴を取得し、定期的に履歴を検証して、不審な活動が無いことを確認する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。	・ISO 27001 2013, 附属書 A.11

						Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	
159	2.物理的対策	2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-6	受託事業者の職員の業務に応じて執務室内に滞在できる時間を指定する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。立ち入りが許可されているのは特定の役割を持つ承認された社員のみです。こうしたエリアへのアクセス管理をモニタリングとロギングの対象にし、その妥当性を定期的に検証しています。アクセス権を持つ社員は、セキュリティ エリアへの立ち入りに関する方針と手続きに従う義務があります。	・ISO 27001 2013, 附属書 A.11
160	2.物理的対策	2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-7	機械式の認証装置で利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN ）、パスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わ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。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	・ISO 27001 2013, 附属書 A.11
161	2.物理的対策	2.1. 入退管理	①機器や媒体の設置場所への認証や入退管理	①-8	機器や媒体の設置場所への入退状況の管理（入退記録のレビュー含む）は定期的に行う。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。	・ISO 27001 2013, 附属書 A.11

						セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	
162	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-1	受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認する。 ・ 医療情報が保存されるサーバ機器等への不正アクセスを防止するため、サーバラックの施錠管理、鍵管理を行う。	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11.2
163	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-2	機器、媒体等の設置場所等のセキュリティ境界について、施錠管理を行う。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11

164	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-3	サーバ等を格納するラック等について、施錠管理を行う。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11
165	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-4	媒体等を格納するキャビネット等について、施錠管理を行う。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11
166	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの	①-5	電子媒体を保存するキャビネット等には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮する。	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。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5

			施錠管理・鍵管理			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、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	
167	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-6	データセンターを運営する外部事業者が、自社専有の建物と同等な安全管理策を実施する等、受託事業者の管理外にある者の物理的な不正操作に対する十分な安全性が確保されていることを確認する。	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11.2
168	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-7	医療情報システム等の設置されるサーバラックには施錠を行い、定められた受託事業者の職員以外が鍵を扱わないよう、確実な鍵管理を行う。	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11.2
169	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビ	①-8	受託事業者が医療情報システム等の設置されるサーバラックを解錠して行う作業については、作業者、作業	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。	・ISO 27001 2013, 附属書 A.11.2

			ネットの施錠管理・鍵管理		開始時刻、作業終了時刻、作業内容等について記録する。	セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	
170	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-9	データセンターを運営する外部事業者がサーバラックを解錠して作業を行う場合には、事前連絡を原則とし、医療情報システム等、医療情報に影響を与えないことを確認する。	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11.2
171	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-10	医療情報システム等であることが、同じデータセンター内に立ち入る他事業者にわからないよう、扱う情報の種類、システムの機能等が識別できるような情報を外部から見える状態にしない。	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。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11.2
172	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビ	①-11	医療情報システム等の設置されるサーバラックの施錠装置については、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）、パスワード	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。	・ISO 27001 2013, 附属書 A.11

			ネットの施錠管理・鍵管理		等の記憶要素、生体情報（バイオメトリクス）等を組み合わせることが望ましい。	セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	
173	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-12	受託事業者の管理外にある者の不正なアクセスに対する十分な安全性が確保されていることを確認する。	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。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はサービスを提供するために、事実上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。	・ISO 27001 2013, 附属書 A.15
174	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-13	機器や媒体の保存場所（ラック、保管庫含む）の外部から、取り扱う情報の種類、システムの機能等が識別できるような情報が見えないようにする。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。	・ISO 27001 2013, 附属書 A.11

						Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	
175	2.物理的対策	2.2. 施錠管理・鍵管理	①サーバラックやキャビネットの施錠管理・鍵管理	①-14	①-1~①-13につき、運用管理規程等に規定する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11
176	2.物理的対策	2.3. 不正な侵入の監視	①防犯カメラ等による医療情報を処理する施設内への侵入監視	①-1	受託事業者の専有する領域に医療情報システム等を設置する場合には、以下に示す物理的安全管理策を施す。外部事業者が運用するデータセンター及びサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合においても、同等の措置がとられていることを確認する。 ・ 傍受、盗撮等の不正な行為を防止するため、部屋を区切る壁面、天井、床部分においては十分な厚みを持たせ、監視カメラでの常時監視及び画像記録の保存、不正に取り付けられた装置の定期的な検出等の対策を施す。 ・ 建物、部屋に対する不正な物理的な侵入を抑止するため、監視カメラ等の侵入検知装置を導入する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセスは、監視と記録の対象になっています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。	・ISO 27001 2013, 附属書 A.11
177	2.物理的対策	2.3. 不正な侵入の監視	①防犯カメラ等による医療情報を処	①-2	防犯カメラ等の監視映像は記録し、期間を定めて管理を行い、必要に応じて事後参照できる措置を講じる。	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。	・ISO 27001 2013, 附属書 A.11

			理する施設内への侵入監視			セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	
178	2.物理的対策	2.3. 不正な侵入の監視	①防犯カメラ等による医療情報を処理する施設内への侵入監視	①-3	機器、媒体等が物理的に保存されている場所に、監視カメラ等を設置し、その記録を保存し、状況を確認することで、不正な入退者がないことを確認する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11
179	2.物理的対策	2.3. 不正な侵入の監視	①防犯カメラ等による医療情報を処理する施設内への侵入監視	①-4	サービスの運用･保守端末等を設置している区域は監視カメラ等により適切に監視を行う。	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置	・ISO 27001 2013, 附属書 A.11.2

						し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	
180	2.物理的対策	2.3. 不正な侵入の監視	②受託事業者の職員に対する職員証等の着用の義務付け	②-1	受託事業者の専有する領域での職務中においては、職員の顔写真を券面に記録した受託事業者の職員証を外部から目視で確認できる状態で携帯することを義務付け、受託事業者の職員で無い者が領域内に立ち入っていた場合に識別できるようにしておく。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	・ISO 27001 2013, 附属書 A.11
181	2.物理的対策	2.3. 不正な侵入の監視	②受託事業者の職員に対する職員証等の着用の義務付け	②-2	受託事業者の職員は、受託事業者の専有する領域にて、受託事業者の職員で無い者を識別した際には声掛け等を行い、身分を確認する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。	・ISO 27001 2013, 附属書 A.11

						Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	
182	2.物理的対策	2.3. 不正な侵入の監視	②受託事業者の職員に対する職員証等の着用の義務付け	②-3	職員証を紛失あるいは不正利用された疑いを持った際には、ただちに管理者に連絡する、受託事業者の職員の退職時には確実に職員証を回収・廃棄する等、職員証の厳密な発行及び失効管理を行う。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	・ISO 27001 2013, 附属書 A.11
183	2.物理的対策	2.4. バックアップ施設における対策	①バックアップ施設に対する物理的安全対策の実施	①-1	医療機関等に提供する医療情報システム等の継続に必要であれば、受託する医療情報のバックアップ施設等、医療情報システム等を継続するための代替情報処理施設を設置し、それらの施設に対しても物理的安全対策を施す。	システムの可用性と完全性に関する統制については、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、世界中に、高度に冗長で地理的に分散したセキュアなデータセンターのネットワークを構築しました。Google は、重要な要素として、データセンター間の地理的な分離を含むサイト選択プロセスに基づいてデータセンターを選択します。これにより、同じ環境またはインフラストラクチャの、気象事象、地災、大規模な停電のような脅威や危険に対するデータセンターの影響を軽減できます。世界中のGoogle ハードウェア、ソフトウェア、データセンターは、一貫性のある信頼できるセキュリティを提供し、メンテナンスを容易にし、透過性のあるソリューションをお客様に提供します。 Google の処理サイトは、プライマリまたは代替としてラベル付けされていません。すべての処理サイトは、一部のプロセスのプライマリとしてや他のプロセスの代替として機能する場合があります。したがって、一次処理サイトの保護と代替の処理サイトとの区別はありません。すべての処理サイトは、セキュアな体制に必要な基本的なセキュリティとアクセス制限を満たしています。	-
184	2.物理的対策	2.5. 個人所有物の持ち込み制限	①医療情報を処理する施設内への個人所有物	①-1	医療情報処理施設内への業務遂行に関係のない個人的所有物の持ち込みを制限する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物	・ISO 27001 2013, 附属書 A.11

			の持ち込み制限			理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0	
185	2.物理的対策	2.5. 個人所有物の持ち込み制限	①医療情報を処理する施設内への個人所有物の持ち込み制限	①-2	機器や媒体の設置場所には、業務遂行に関係のない個人的所有物の持ち込みを制限する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0"	・ISO 27001 2013, 附属書 A.11
186	2.物理的対策	2.6. 機器の盗難への対策	①重要な機器への盗難防止用チェーン等の取付	①-1	個人情報が存在するPC 等の重要な機器には、盗難防止用チェーン等を取り付ける。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータ	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5

						を消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	
187	2.物理的対策	2.7. 覗き見への対策	①覗き見防止対策	①-1	医療情報等が表示される端末画面等がアクセス権限の無いものが視野に入らないような対応（室内の機器レイアウト等）を行う。	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	・ISO 27001 2013, 附属書 A.11.2
188	2.物理的対策	2.7. 覗き見への対策	①覗き見防止対策	①-2	個人情報の表示中の覗き見を予防するために、端末に覗き見対策のシートを貼る等の対策を行う。	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	・ISO 27001 2013, 附属書 A.11.2
189	2.物理的対策	2.8. 災害等への対策	①地震、水害、落雷、火災等、及び、それに伴う停電等への対策	①-1	機器や媒体を物理的に保存するための施設は、災害（地震、水害、落雷、火災等、及び、それに伴う停電等）に耐えうる機能･構造を備え、災害による障害（結露等）について対策が講じられている建築物に設置する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設には堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。火災検知器や消火設備を設置し、ハードウェアの損傷を防ぎます。熱、火、煙の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在するリージョンの建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。 https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。	・ISO 27001 2013, 附属書 A.11

190	2.物理的対策	2.8. 災害等への対策	①地震、水害、落雷、火災等、及び、それに伴う停電等への対策	①-2	①-1の施設を設置する建築物について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設には堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。火災検知器や消火設備を設置し、ハードウェアの損傷を防ぎます。熱、火、煙の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在するリージョンの建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。 https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。	・ISO 27001 2013, 附属書 A.11
191	2.物理的対策	2.8. 災害等への対策	①地震、水害、落雷、火災等、及び、それに伴う停電等への対策	①-3	火災発生時の消火設備が機器に損傷を与えないよう配慮する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設には堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。火災検知器や消火設備を設置し、ハードウェアの損傷を防ぎます。熱、火、煙の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在するリージョンの建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。 https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers	・ISO 27001 2013, 附属書 A.11
192	2.物理的対策	2.8. 災害等への対策	①地震、水害、落雷、火災等、及び、それに伴う停電等への対策	①-4	医療情報システム等を配置する室内での喫煙、飲食を禁止する。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 すべての Google 委託業者は、オリエンテーションプロセスの一環としてセキュリティ研修を受け、Google キャリアを通じて継続的なセキュリティ研修を受けます。新規の委託業者は、オリエンテーション中にお客様の情報を安全に保つことへのコミットメントを強調する当社の行動規範に同意します。役割に応じて、セキュリティの特定の側面に関する追加の研修が必要になる場合があります。たとえば、情報セキュリティチームは、安全なコーディング手法、製品設計、脆弱性テストツールなどのトピックについて、新しいエンジニアを指導します。また、技術者は、セキュリティ関連のトピックに関する技術プレゼンテーションに出席し、新しい脅威、攻撃パターン、軽減技法を網羅したセキュリティニュースレターを受け取ります。	・ISO 27001 2013, 附属書 A.7.2.2
193	2.物理的対策	2.8. 災害等への対策	①地震、水害、落雷、火災等、及び、それに伴う停電等への対策	①-5	医療情報システム等を配置する室内に可燃物及び液体を置く場合には、装置との間に十分な距離を保ち、専用の収納設備を設ける等、装置に悪影響を及ぼさないよう配慮する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設で、熱、火、煙、水の検知を含め、環境面に関する十分な対策を施しています。 すべての施設には堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。火災検知器や消火設備を設置し、ハードウェアの損傷を防ぎます。熱、火、煙、水の探知機は、異常が発生しているゾーン、セ キュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。Google は、データセンターが所在する地域の建築要件をすべて遵守しています。	・ISO 27001 2013, 附属書 A.11

						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 Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。	
194	2.物理的対策	2.8. 災害等への対策	①地震、水害、落雷、火災等、及び、それに伴う停電等への対策	①-6	医療情報システム等を設置するサーバラックについては以下の安全管理策を実施する。 ・ 震災時に転倒することが無いよう確実に設置する。 ・ 熱による障害を防ぐため十分な空調設備を保有し、サーバラック内が十分に換気されている。 ・ 扉には十分な安全強度を持つ物理的施錠装置を設け、鍵管理について十分に配慮する。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google のデータセンターは、24 時間体制で稼働しサービスを中断しないようにするため、冗長電源システムと環境管理を導入しています。同じ電力供給量を持つ主電源と代替電源が、すべての重要なコンポーネントに設置されています。 ディーゼル エンジンのバックアップ発電機により、各データセンターは緊急時でも最大限の性能を発揮できる電力を得ます。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減され ます。火災検知器や消火設備を設置し、ハードウェアの損傷を防ぎます。熱、火、煙の探知機は、異常が発生しているゾーン、セキュリティ操作コンソール、リモート モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて遵守し、自然災害による損害を最小限に抑えるベスト プラクティスに従って設備を運用しています。	・ISO 27001 2013, 附属書 A.11
195	3.技術的対策	3.1. 利用者認証の実装	①利用者を一意に識別する方式の採用	①-1	医療情報システム等にて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
196	3.技術的対策	3.1. 利用者認証の実装	①利用者を一意に識別する方式の採用	①-2	医療情報システム等の利用者を特定し識別できるように、アカウントの発行を行う（複数の利用者によるIDの共同利用は行わない。ただし当該医療情報システム等が他の医療情報システム等を利用するためのID（non interactive ID）は除く）。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシー	・ISO 27001 2013, 附属書 A.9

						の適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、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。	
197	3.技術的対策	3.1. 利用者認証の実装	①利用者を一意に識別する方式の採用	①-3	利用者のなりすまし等を防止するための認証を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
198	3.技術的対策	3.1. 利用者認証の実装	①利用者を一意に識別する方式の採用	①-4	医療情報システム等の運用若しくは開発に従事する者又は管理者権限を有する者に対するIDの発行は必要最小限とし、定期的な棚卸しを行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
199	3.技術的対策	3.1. 利用者認証の実装	②一時的な認証手段の用意	②-1	利用者の認証に際して、何らかの物理的な媒体･身体情報等を必要とする場合に、例外的にそれらの媒体等がなくても一時的に認証するための代替的手段･手順を事前に定める。	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。 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。	・ISO 27001 2013, 附属書 A.9

						Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud 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。	
200	3.技術的対策	3.1. 利用者認証の実装	②一時的な認証手段の用意	②-2	代替的手段･手順を用いるケースにおいては、本来の利用者の認証方法による場合とのリスクの差が最小となるようにする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
201	3.技術的対策	3.1. 利用者認証の実装	②一時的な認証手段の用意	②-3	代替的手段･手順により、医療情報システム等利用を行った場合でも、事後の追跡を可能とする記録を行い、これを管理する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
202	3.技術的対策	3.1. 利用者認証の実装	②一時的な認証手段の用意	②-4	その他、一時的な利用者の認証方法について医療機関等と合意する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
203	3.技術的対策	3.1. 利用者認証の実装	③長時間離席時の対策	③-1	離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐ。	Google は ISO27001 認証を受けています。この基準では、「無人状態にある利用者装置」（ISO 27001 2013、附属書 A.11.2.8）が規定されています。 組織は、無人状態の際、ユーザにコンピュータやモバイル機器をロックすることを求めるセキュリティガイダンスを保持しています。	・ISO 27001 2013, 附属書 A.11.2.8
204	3.技術的対策	3.1. 利用者認証の実装	③長時間離席時の対策	③-2	サービスの運用･保守端末等に、クリアスクリーン等の防止策を講じることを運用管理規程等に定める。	Google は ISO27001 認証を受けています。この基準では、「無人状態にある利用者装置」（ISO 27001 2013、附属書 A.11.2.8）が規定されています。 組織は、無人状態の際、ユーザにコンピュータやモバイル機器をロックすることを求めるセキュリティガイダンスを保持しています。	・ISO 27001 2013, 附属書 A.11.2.8
205	3.技術的対策	3.1. 利用者認証の実装	③長時間離席時の対策	③-3	医療機関等に設置されている医療情報の参照等が可能な利用者端末等に対するクリアスクリーン等の情報漏洩防止策について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「クリアデスク・クリアスクリーン方針」（ISO 27001 2013、附属書 A.11.2.9）が規定されています。 組織にはセキュリティガイダンスがあり、ユーザーはデバイスを放置又は席を外す場合には、コンピュータとモバイルデバイスをロックする必要があります。	・ISO 27001 2013, 附属書 A.11.2.9

206	3.技術的対策	3.1. 利用者認証の実装	③長時間離席時の対策	③-4	端末又はセッションの乗っ取りのリスクを低減するため、利用者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行う。	Google は ISO27001 認証を受けています。この基準では、「利用者領域にある無人運転の装置」（ISO 27001 2013、附属書 A.11.2.8）が規定されています。 Google は、エンドユーザーコンピューターのセッションロック機能を有効化しています。これは、ユーザーがコンピューターを15 分間操作しないと、パスワードで保護されたスクリーンセーバーが起動する形式をとっています。スクリーンセーバーは、ユーザーがコンピューターにサインバックするまでロックされたままになります。また、Google は、本番環境への接続に対して暗号化セッションを強制することで、中間者攻撃やセッションハイジャックを防ぎます。	・ISO 27001 2013, 附属書 A.11.2.8
207	3.技術的対策	3.1. 利用者認証の実装	③長時間離席時の対策	③-5	離席の場合のクローズ処理の具体的な適用について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「利用者領域にある無人運転の装置」（ISO 27001 2013、附属書 A.11.2.8）が規定されています。 Google は、エンドユーザーコンピューターのセッションロック機能を有効化しています。これは、ユーザーがコンピューターを15 分間操作しないと、パスワードで保護されたスクリーンセーバーが起動する形式をとっています。スクリーンセーバーは、ユーザーがコンピューターにサインバックするまでロックされたままになります。また、Google は、本番環境への接続に対して暗号化セッションを強制することで、中間者攻撃やセッションハイジャックを防ぎます。	・ISO 27001 2013, 附属書 A.11.2.8
208	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-1	パスワードについては、第三者から容易に推定されにくい内容を含む品質基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
209	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-2	パスワードポリシーについて、医療機関等と合意する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
210	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-3	パスワードには有効期限の設定を行い、定期的な変更を強制する。ただし、利用者が患者等である場合には、他のサービスで利用しているパスワードを使わないよう特に促すだけでなく、サービス提供側から患者等に対して定期的なパスワードの変更を要求しないようにする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はNIST ガイダンス(SP 800-63c) に従い、パスワード履歴とローテーションの要求事項を強制していません。しかし、Google は外部のお客様がSAML経由でSSOを統合するためのメカニズムを提供しています。このことを前提とすると、Google は、当社のパスワードポリシーが3省2ガイドライン基準要件よりも「同等か、それ以上のセキュリティ」を提供していると考えています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud 本番環境、内部サポートツール及びお客様データへのアクセスを制限するために、強力な認証とアクセス制御が実装されています。マシンレベルのアクセス制限は、トランスポート・レ	・ISO 27001 2013, 附属書 A.9

						イヤー・セキュリティ (TLS) 認証に基づくGoogle が開発した分散認証サービスに依拠しており、リソースアクセスの要求を確実に把握することが可能です。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
211	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-4	パスワードの世代管理を行い、パスワード変更に際して、安全性を確保するために必要な範囲で、過去に設定したパスワードを設定できないような運用を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
212	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-5	パスワード発行時には、乱数から生成した仮の医療情報システム等へのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
213	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-6	パスワードをシステムに記憶させる自動ログオン機能を利用しないよう利用者に徹底する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
214	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-7	利用者がパスワードを登録及び変更する際には、予め定めた品質を満たしていることを保証する仕組み、乱数によりパスワードを生成するプログラム等の導入、利用者が設定しようとする品質の低いパスワードを認めないシステムの導入等を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google の担当者は、パスワードをリセットする前に、有効なクレデンシャル情報を用いた認証が必要です。パスワードはパスワード構築、保護、および管理のガイドラインに従って管理および設定され、以下が適用されます。 • 最小文字数 • 複雑性 • 履歴 • アイドル時のロックアウト	・ISO 27001 2013, 附属書 A.9

						パスワード設定要件は、内部システムによって強制適用されます。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、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。	
215	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-8	本人の識別･認証に用いる情報は、本人しか知り得ない状態に保つよう対策を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud 本番環境、内部サポートツール及びお客様データへのアクセスを制限するために、強力な認証とアクセス制御が実装されています。マシンレベルのアクセス制限は、トランスポート・レイヤー・セキュリティ (TLS) 認証に基づくGoogle が開発した分散認証サービスに依拠しており、リソースアクセスの要求を確実に把握することが可能です。このサービスは、転送中のデータを暗号化するためにトランスポートの暗号化も実施しています。Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
216	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-9	利用者に対して初期パスワードを発行した場合、最初の利用時にそのパスワードを変更しないと医療情報システム等にアクセスできないにようにする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
217	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-10	初期パスワード以外のパスワードは、利用者本人に設定させるとともに、利用者本人しか知りえない内容を設定するよう求める。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。	・ISO 27001 2013, 附属書 A.9

						Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
218	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-11	パスワードの設定に際しては、複数の文字種（英数字・大文字・小文字・記号等）を用い、また、8文字以上等、十分に安全な長さの文字列等から構成されるルールとする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google の担当者は、パスワードをリセットする前に、有効なクレデンシャル情報を用いた認証が必要です。 パスワードはパスワード構築、保護、および管理のガイドラインに従って管理および設定され、以下が適用されます。 • 最小文字数 • 安全なパスワードを要求する • 過去に利用したパスワードを再利用させない • 未使用時間によるロックアウト設定 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
219	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-12	利用者がIDやパスワードを失念した場合には、予め策定した手順（本人確認を含む）に則り、本人への通知又は再発行を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
220	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-13	パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とする。	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。 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。 ユーザーは、パスワードをリセットする前に有効なクレデンシャル情報を使用して認証する必要があります。	・ISO 27001 2013, 附属書 A.9

						パスワードはパスワード構築、保護、および管理のガイドラインに従って管理および設定され、以下が適用されます。 a) 最小文字数 b) 安全なパスワードを要求する c) 過去に利用したパスワードを再利用させない d) 未使用時間によるロックアウト設定 パスワードのセキュリティ要件はセキュリティのガイドラインで規定されており、Google のパスワード標準が確実に適用されるようにするための制御（パスワードの複雑さ、有効期限など）がシステムに組み込まれています。	
221	3.技術的対策	3.1. 利用者認証の実装	④安全なパスワード要件の定義	④-14	パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定する。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とする。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入する。	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。 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。 ユーザーは、パスワードをリセットする前に有効なクレデンシャル情報を使用して認証する必要があります。 パスワードはパスワード構築、保護、および管理のガイドラインに従って管理および設定され、以下が適用されます。 a) 最小文字数 b) 安全なパスワードを要求する c) 過去に利用したパスワードを再利用させない d) 未使用時間によるロックアウト設定 パスワードのセキュリティ要件はセキュリティのガイドラインで規定されており、Google のパスワード標準が確実に適用されるようにするための制御（パスワードの複雑さ、有効期限など）がシステムに組み込まれています。	・ISO 27001 2013, 附属書 A.9
222	3.技術的対策	3.1. 利用者認証の実装	⑤多要素認証方式の採用	⑤-1	ログオン時に利用する認証要素としては、ハードウェアトークン又は IC カード等の認証デバイス、暗証番号（PIN）又はパスワード等の記憶要素、生体情報（バイオメトリクス）等を組み合わせた多要素認証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、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
223	3.技術的対策	3.1. 利用者認証の実装	⑤多要素認証方式の採用	⑤-2	医療情報システム等の運用若しくは開発に従事する者又は管理者権限を有する者の情報システム利用に係る認証は、多要素認証とする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
224	3.技術的対策	3.1. 利用者認証の実装	⑤多要素認証方式の採用	⑤-3	利用者の認証で採用する認証方式について、医療機関等と合意する。	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。	・ISO 27001 2013, 附属書 A.9

						論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud 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。	
225	3.技術的対策	3.1. 利用者認証の実装	⑤多要素認証方式の採用	⑤-4	利用者の認証において、ID･パスワードによる認証方式を採用している場合には、ID･パスワードのみに頼らない認証方式の採用に対応しうる機能を備えるよう努める。なお、厚生労働省ガイドラインにおいては、厚生労働省ガイドライン 第5版の公表（平成29年5月）から約10年後を目途に2要素認証について厚生労働省ガイドライン6.5章「C.最低限のガイドライン」とすることを想定する旨が記載されていることから、これに随時対応できるようにする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
226	3.技術的対策	3.2. アクセス権限の管理	①必要最小限となるようなアクセス権限の管理	①-1	医療情報システム等の操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、閲覧、編集、削除等を防止する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
227	3.技術的対策	3.2. アクセス権限の管理	①必要最小限となるようなアクセス権限の管理	①-2	医療機関等の利用者の職種等に応じたアクセス制御の設定について医療機関等に示し、医療機関等と必要な協議を行い、実際に設定する作業に関する役割分担も含めて合意する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許	・ISO 27001 2013, 附属書 A.9

						可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
228	3.技術的対策	3.2. アクセス権限の管理	①必要最小限となるようなアクセス権限の管理	①-3	医療情報システム等の構成要素（情報処理装置、ソフトウェア）それぞれのアクセス管理に係るセキュリティ要求事項を整理する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
229	3.技術的対策	3.2. アクセス権限の管理	①必要最小限となるようなアクセス権限の管理	①-4	それぞれの情報にアクセスする権限を持つ利用者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9

230	3.技術的対策	3.2. アクセス権限の管理	①必要最小限となるようなアクセス権限の管理	①-5	業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
231	344	3.2. アクセス権限の管理	①必要最小限となるようなアクセス権限の管理	①-6	定められたアクセス制御方針がファイル、ディレクトリパーミッション、データベースアクセス等のアクセス制御機構として適切に反映されていることを定期的に検証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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、アクセスの妥当性を確認するために、全システムへの論理的アクセスの審査を定期的に実施しています。さらに、Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
232	3.技術的対策	3.2. アクセス権限の管理	①必要最小限となるようなアクセス権限の管理	①-7	予定された保守･運用等を行う際に受託した医療情報を許可なく閲覧できないようにするために、権限設定等の対策を講じる。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、アクセスの適切性を保証するために、すべてのシステムへの論理的なアクセスを定期的にレビューします。 また、Googlerのアクセスは、当社のセキュリティ、プライバシー、内部監査チームによって監視および監査されています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
233	3.技術的対策	3.2. アクセス権限の管理	①必要最小限となるようなアクセス	①-8	システム管理者、運用担当者、保守担当者等が、意図しない閲覧を行わないことを担保するための措置（データベースの暗号化等）を講じる。	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。 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。	・ISO 27001 2013, 附属書 A.9

			権限の管理			Google は、アクセスの適切性を保証するために、すべてのシステムへの論理的なアクセスを定期的にレビューします。 また、Googlerのアクセスは、当社のセキュリティ、プライバシー、内部監査チームによって監視および監査されています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
234	3.技術的対策	3.2. アクセス権限の管理	②医療情報に対するアクセス制御	②-1	医療情報とそれ以外の情報を区分できる措置を講じる。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ ISO 27001 2013, 附属書 A.9
235	3.技術的対策	3.2. アクセス権限の管理	②医療情報に対するアクセス制御	②-2	医療情報については、情報区分に従ってアクセス制御を行えるようにする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセス	・ISO 27001 2013, 附属書 A.9

						は、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
236	3.技術的対策	3.2. アクセス権限の管理	②医療情報に対するアクセス制御	②-3	仮想化技術を用いた資源をサービスに供する場合には、論理的に区分管理を行えることを保証できる措置を講じる。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
237	3.技術的対策	3.2. アクセス権限の管理	②医療情報に対するアクセス制御	②-4	医療機関等による情報資産の区分の設定や、これに対するアクセス制御の設定の対応について、医療機関等と合意する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。	・ISO 27001 2013, 附属書 A.9

						Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
238	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-1	利用者は医療情報システム等上においてユニークな利用者ごとのID により識別する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
239	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-2	利用者のID を発行する際に、既存の ID との重複を排除する仕組みを導入する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
240	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの	①-3	複数利用者で共用するためのグループ ID の利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、利用者ごとのID でログ	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。	・ISO 27001 2013, 附属書 A.9

			管理・運用		オンしてからグループ ID に変更する仕組みを利用する。	Google では、アクセスの妥当性を確認するために、全システムへの論理的アクセスの審査を定期的に実施しています。さらに、Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
241	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-4	利用者のID の発行は医療情報システム等の管理に必要な最小限の人数に留める。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
242	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-5	監視ログの監査時に利用者を確実に特定するため、利用者の ID は過去に使われたものを再利用しない。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は定期的にすべてのシステムへの論理的なアクセスを確認してアクセスの適切性を確認します。さらに、Google 社員のアクセスは、Google 専任のセキュリティ、プライバシー、および内部監査チームによって監視および監査されています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
243	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-6	アクセスを許可された利用者 のID によるアクセス可能範囲が許可された通りとなっていること（不正に変更されていないこと）を定期的に確認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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、アクセスの妥当性を確認するために、全システムへの論理的アクセスの審査を定期的に実施しています。さらに、Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9

244	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-7	不正なアカウントの利用又は試みが行われたことを利用者自身で検出するため、利用者のログオン後に前回のログオンが成功していれば成功日時を表示し、前回のログオンが失敗していれば、第三者による不正なログオンの試みが行われた可能性があるという内容の警告メッセージとともに失敗日時を表示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。 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。 ユーザーは、パスワードをリセットする前に有効な資格情報を使用して認証する必要があります。 パスワードはパスワード構築、保護、および管理のガイドラインに従って管理および設定され、以下が適用されます。 a) 最小文字数 b) 安全なパスワードを要求する c) 過去に利用したパスワードを再利用させない d) 未使用時間によるロックアウト設定 パスワードのセキュリティ要件はセキュリティのガイドラインで規定されており、Google のパスワード標準が確実に適用されるようにするための制御（パスワードの複雑さ、有効期限など）がシステムに組み込まれています。	・ISO 27001 2013, 附属書 A.9
245	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-8	不正なアカウントの利用を防ぐため、利用者のログオンを許可する曜日、時間帯は作業に必要な曜日、時間帯に制限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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
246	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-9	認可されていない利用者あるいは第三者がログオンを試みた際に「パスワードが異なります」と表示すると当該ID が存在していることを知る手がかりとなるため、「認証に失敗しました」、あるいは単にログオンプロンプトを再表示するといった特段の情報を与えないようなメッセージのみの表現に留めることが望ましい。	Google は ISO27001 認証を受けています。この基準では、「ユーザーアクセス管理」（ISO 27001 2013、附属書 A.9.2）が規定されています。 Google ネイティブ認証には、最低 8 文字の複雑なパスワードが必要です。テナントは最大値を設定することも、最小値を増やすこともできます。組み込みパスワードモニタは、パスワード作成時にエンドユーザーと、後で弱いパスワードを持つことが検出されたユーザーにパスワード変更を強制することを決定できるテナントのシステム管理者に表示されます。 Google のネイティブ認証には、ブルートフォース攻撃を検出してユーザーに Captcha の解決を要求し、疑わしい行為が検出された場合は自動的にアカウントをロックする保護機能があります。テナントのシステム管理者はそのアカウントをエンドユーザー用にリセットできます。	・ISO 27001 2013, 附属書 A.9.2
247	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-10	緊急時の作業のため、規定時間外にログオンを行う必要が発生した場合の妥当な承認プロセスを策定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。 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。	・ISO 27001 2013, 附属書 A.9

						Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、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。	
248	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-11	医療情報システム等に許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知する。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク管理策」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9.1.2,13.1
249	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの管理・運用	①-12	利用者が変更あるいは退職した際には、ただちに当該作業者 ID を利用停止とする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、本番環境へアクセスする、組織のユーザー（または組織のユーザーに代わって動作するプロセス）を一意に識別および認証します。 Google でのアカウント作成は、Google の従業員の場合、まずHRによって自動化されたプロセスが開始されます。そして、オンボーディングシステムが新しい従業員（ベンダー、請負業者、派遣従業員を含む）に一意のユーザーIDを割り当てます。 このユーザーIDは一意であり、他の個人に再利用されることはありません。 従業員がGoogle を離れた場合、ユーザーIDは削除されず、関連付けられたアカウントが無効になり、同じ従業員がGoogle に戻った場合にのみユーザーIDを再利用できます。	・ISO 27001 2013, 附属書 A.9
250	3.技術的対策	3.3. ID・パスワードの管理	①利用者アクセス及びIDの	①-13	不要な利用者の ID が残っていないことを定期的に確認する。	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。 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。	・ISO 27001 2013, 附属書 A.9

			管理・運用			Google では、アクセスの妥当性を確認するために、全システムへの論理的アクセスの審査を定期的に実施しています。さらに、Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
251	3.技術的対策	3.3. ID・パスワードの管理	②特権IDの最小限の利用及び作業実施内容の記録	②-1	特権 ID の発行は必要な最小限のものに留める。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
252	3.技術的対策	3.3. ID・パスワードの管理	②特権IDの最小限の利用及び作業実施内容の記録	②-2	特権使用者に昇格可能な利用者の ID を制限する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセス	・ISO 27001 2013, 附属書 A.9

						は、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
253	3.技術的対策	3.3. ID・パスワードの管理	②特権IDの最小限の利用及び作業実施内容の記録	②-3	特権の使用時には作業実施内容を記録する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	・ISO 27001 2013, 附属書 A.9
254	3.技術的対策	3.3. ID・パスワードの管理	②特権IDの最小限の利用及び作業実施内容の記録	②-4	管理端末以外からの特権 ID による直接ログオンを禁止する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1
255	3.技術的対策	3.3. ID・パスワードの管理	②特権IDの最小限の利用及び作業実施内容の記録	②-5	特権の種類に応じてアカウントを分離し、ファイルやディレクトリに対するアクセスを制限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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9

256	3.技術的対策	3.3. ID・パスワードの管理	②特権IDの最小限の利用及び作業実施内容の記録	②-6	医療情報システム等の機能として可能であれば、特権 ID で使用可能なコマンド及びユーティリティについて業務上必要な最低限の範囲に制限し、重要なコマンド、ユーティリティ及びログについて改竄、削除など不正な行為を防止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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。 社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
257	3.技術的対策	3.3. ID・パスワードの管理	③パスワードの管理・運用	③-1	各利用者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
258	3.技術的対策	3.3. ID・パスワードの管理	③パスワードの管理・運用	③-2	医療情報システム等及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等の棚卸を行い、必要のないアカウントについては削除あるいはパスワード変更を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、アクセスの妥当性を確認するために、全システムへの論理的アクセスの審査を定期的に実施しています。さらに、Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
259	3.技術的対策	3.3. ID・パスワードの管理	③パスワードの管理・運用	③-3	パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管する。	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）、「暗号」（ISO 27001 2013、附属書 A.10）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 内部パスワードは、不正な開示や変更のリスクを軽減するために、暗号化ハッシュ処理の対象となります。	・ISO 27001 2013, 附属書 A.9, 10

260	3.技術的対策	3.3. ID・パスワードの管理	③パスワードの管理・運用	③-4	パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用する。また、一般の作業者による閲覧を制限する。	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）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。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。 データの完全性を確保するために、アプリケーションおよびファイルシステムレベルで完全性チェックが実施されています。アプリケーションレベルでは、アップロードの破損から保護するために、チェックサム比較が実施されます。ファイルシステムの完全性チェックでは、完全性を検証するユーザーレベルプログラムを使用して、ストレージレイヤーにも展開されます。	・ISO 27001 2013、附属書 A.12.1
261	3.技術的対策	3.3. ID・パスワードの管理	③パスワードの管理・運用	③-5	パスワード等の情報の漏洩が生じた場合（不正な第三者からの攻撃による場合を含む）には、直ちに当該IDを無効化し、予め策定した手順に基づき、新規のログイン情報の再発行を行い、利用者に速やかに通知する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
262	3.技術的対策	3.3. ID・パスワードの管理	③パスワードの管理・運用	③-6	パスワード等の情報の漏洩のおそれがある場合、利用者本人にその事実を通知した上で、当該パスワードを無効化し、変更できるような対応を講じる。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
263	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-1	利用者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録したログを作成し、一定期間保存する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、アプリケーションの脆弱性を検出して報告するための監視ツールを実装しています。また、Google は、特権アクセスとユーザーデータへのアクセスのログを保持しています。監査ログへの論理アクセスは、認められた担当者に制限されます。監査ログは、Google 独自のセキュリティ情報およびイベント管理システムを使用して継続的に監視され、侵入の試みやその他のセキュリティ関連イベントを検出します。Google は、Google のデータの保存・削除方針に基づき、機密情報を廃棄する手続きを整備しています。また、Google は、ユーザーデータの返却、移転、処分に関する方針を保持し、これらの方針をお客様に適用します。	・ISO 27001 2013, 附属書 A.9
264	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-2	ログを定期的に検証して不正な行為、システムの異常等を検出する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、データへのアクセスを管理するデータセキュリティポリシーと、不正アクセスを防止および検出するためのメカニズムを管理しています。	・ISO 27001 2013, 附属書 A.9

265	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-3	ログに記録する事項としては次のようなものが考えられる。 ・ 利用者情報（利用者の ID、ログオンの可否、利用時刻及び時間、実行作業内容、ネットワークアクセスの場合はアクセス元 IP アドレス） ・ ファイル及びデータへのアクセス、変更、削除記録（利用者の ID、アクセスの可否、利用時刻及び時間、作業内容、対象ファイル又はデータ種類） ・ データベース操作記録（利用者のID、接続及び作業の可否、利用時刻及び時間、実施作業内容、アクセス元 IP アドレス、設定変更時にはその内容）修正パッチの適用作業（利用者の ID、変更されたファイル） ・ 特権操作（特権取得者 ID、特権取得の可否、利用時刻及び時間、実行作業内容） ・ システム起動、停止イベント ・ ログ取得機能の開始、終了イベント外部デバイスの取り外し ・ IDS・IPS 等のセキュリティ装置のイベントログ ・ サービス及びアプリケーションの動作により生成されたログ（時刻同期に関するログを含む）	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
266	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-4	ログを集中させ問題の検出を一箇所で確実に行うことを目的として、システムとして可能な場合は専用のログサーバにログデータを集約して分析管理する。	Google は ISO27001 認証を受けています。この基準では、「イベントログ取得」（ISO 27001 2013、附属書 A.12.4.1）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、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 監査ログは、Google 独自のセキュリティ情報およびイベント管理システムを使用して継続的に監視され、侵入の試みやその他のセキュリティ関連イベントを検出します。 セキュリティアラートは、事前定義されたしきい値に基づいて追加調査するために生成されます。 これらの監視ツールは、セキュリティ要員に自動アラートを出します。	・ISO 27001 2013, 附属書 A.12.4.1
267	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-5	運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	・ISO 27001 2013, 附属書 A.9
268	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-6	システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こ	・ISO 27001 2013, 附属書 A.9

						うしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、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。	
269	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-7	医療情報システム等の運用若しくは開発に従事する者又は管理者権限を有する者によるアクセスの記録については、定期的なレビューを行い、不正なアクセス等がないことを確認する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	・ISO 27001 2013, 附属書 A.9
270	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-8	①-7に関する情報の医療機関等への提供について、医療機関等と合意する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	・ISO 27001 2013, 附属書 A.9
271	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-9	ログの取得機能を有しない場合には、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「イベントログ取得」（ISO 27001 2013、附属書 A.12.4.1）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、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 監査ログは、Google 独自のセキュリティ情報およびイベント管理システムを使用して継続的に監視され、侵入の試みやその他のセキュリティ関連イベントを検出します。 セキュリティアラートは、事前定義されたしきい値に基づいて追加調査するために生成されます。 これらの監視ツールは、セキュリティ要員に自動アラートを出します。	・ISO 27001 2013, 附属書 A.12.4.1
272	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-10	医療情報システム等の保守に従事する者及び管理者権限を有する者が、その業務の目的で当該医療情報システム等にアクセスする場合には、当該要員ごとに発行されたアカウントにより、アクセスを行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。	・ISO 27001 2013, 附属書 A.9

						Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、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。	
273	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-11	①-10で定めるアカウントで行った作業等は、アクセスした個人情報が特定できる形で、ログ等により記録し、保存する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	・ISO 27001 2013, 附属書 A.9
274	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-12	医療情報システム等の保守において実施した操作結果について、操作ログ等により記録し、管理する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	・ISO 27001 2013, 附属書 A.9
275	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-13	取得した操作ログ等により、アクセスされた医療情報についての状況をレビューする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	・ISO 27001 2013, 附属書 A.9
276	3.技術的対策	3.4. ログの取得と検証	①ログの取得と検証	①-14	ログを検証するため、利用者がアクセスした医療情報等を迅速に確認できるよう、利用者の ID と、情報の識別子（資産台帳記載の番号等）、生成時系列、アクセス時系列等、多様な指標での並び替え、情報の種別、アクセス時間等での絞り込み等が行うことができるようなシステムを整備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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9
277	3.技術的対策	3.4. ログの取得と検証	②ログの改竄や削除を防止	②-1	ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用する。	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。	・ISO 27001 2013, 附属書 A.9

			するためのアクセス制限や外部保存		・ ログデータにアクセスする利用者及び操作を制限する。 ・ 容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとる。 ・ ログデータに対する不正な改竄及び削除行為に対する検出・防止策を施す。	論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、データへのアクセスを管理するデータセキュリティポリシーと、不正アクセスを防止および検出するためのメカニズムを管理しています。	
278	3.技術的対策	3.4. ログの取得と検証	③時刻の標準時刻への同期	③-1	ログを利用して正確に事故原因等を検証するため、医療情報システム等のすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておく。	Google は ISO27001 認証を受けています。この基準では、「時刻同期」（ISO 27001 2013、附属書 A.12.4.4）が規定されています。 Google は時刻同期プロトコルを使用して、すべてのシステムが共通の時間を参照できるようにしています。また、Google は NTP プロトコルを公開し、お客様が使用できるようにしています。 https://developers.google.com/time/	・ISO 27001 2013, 附属書 A.12.4.4
279	3.技術的対策	3.4. ログの取得と検証	③時刻の標準時刻への同期	③-2	医療情報システム等のすべてのサーバ機器等の時刻が時刻サーバ等の提供する標準時刻に同期していることを定期的に検証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、「時刻同期」（ISO 27001 2013、附属書 A.12.4.4）が規定されています。 Google は時刻同期プロトコルを使用して、すべてのシステムが共通の時間を参照できるようにしています。また、Google は NTP プロトコルを公開し、お客様が使用できるようにしています。 https://developers.google.com/time/	・ISO 27001 2013, 附属書 A.12.4.4
280	3.技術的対策	3.4. ログの取得と検証	③時刻の標準時刻への同期	③-3	ログの時刻の信頼性を確保するために、医療情報システム等の時刻と、信頼できる機関が提供する標準時刻あるいは同等の時刻情報との同期を日次又はそれよりも多い頻度で行う。	Google は ISO27001 認証を受けています。この基準では、「時刻同期」（ISO 27001 2013、附属書 A.12.4.4）が規定されています。 Google は時刻同期プロトコルを使用して、すべてのシステムが共通の時間を参照できるようにしています。また、Google は NTP プロトコルを公開し、お客様が使用できるようにしています。 https://developers.google.com/time/	・ISO 27001 2013, 附属書 A.12.4.4
281	3.技術的対策	3.4. ログの取得と検証	④リモートメンテナンスにおける不正な侵入防止とログの取得・検証	④-1	リモートメンテナンスにより保守業務を行う場合の手順を策定するとともに、医療情報システム等への不正な侵入が生じないよう安全管理措置を講じる。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	・ISO 27001 2013, 附属書 A.9
282	3.技術的対策	3.4. ログの取得と検証	④リモートメンテナンスにおける不正な侵入防止とログの取得・検証	④-2	リモートメンテナンスによる保守業務の記録を、アクセスログ等により取得し、システム管理者はその内容を速やかに確認する。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	・ISO 27001 2013, 附属書 A.9
283	3.技術的対策	3.4. ログの取得と検証	④リモートメンテナンスにおける不	④-3	サービス提供に必要な医療情報システム等の保守をリモートメンテナンスで行う場合、医療機関等と合意する。	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。 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。	・ISO 27001 2013, 附属書 A.9

			正な侵入防止とログの取得・検証			Google はアプリケーションの脆弱性を検出して報告するための監視ツールを実装しました。 また、Google は、特権アクセスおよびユーザーデータへのアクセスのためにユーザーアクセスログを管理しています。監査ログへの論理アクセスは、許可された担当者に制限されています。	
284	3.技術的対策	3.4. ログの取得と検証	⑤取り扱う医療情報の法定保存年限に基づくログの保存期間の設定	⑤-1	取り扱う医療情報に法定保存年限が設けられている場合、診療録等に関するログ又はこれに代わる記録について、当該法定年限以上の保存期間を設ける。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
285	3.技術的対策	3.4. ログの取得と検証	⑤取り扱う医療情報の法定保存年限に基づくログの保存期間の設定	⑤-2	法定保存年限が経過した医療情報及び法定保存年限が設けられていない医療情報の保存期間について、医療機関等と合意する。なお、本項におけるログの管理方法について保存期間を設けた場合には、原則として法定保存年限がある医療情報に準じて取り扱う。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
286	3.技術的対策	3.5. 不正プログラムへの対策	①不正プログラム対策ソフトウェアの導入と管理	①-1	最新の脅威についての情報収集に努め、導入している不正プログラム対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認する。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
287	3.技術的対策	3.5. 不正プログラムへの対策	①不正プログラム対策ソフトウェアの導入と管理	①-2	不正プログラム対策ソフトウェアにおいて次の設定を行う。 ・ リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信）リスク評価の結果として必要であれば定期的にスキャンを実施 ・ 電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン ・ 定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新 ・ 管理者以外による設定変更やアンインストールの禁止	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2

288	3.技術的対策	3.5. 不正プログラムへの対策	①不正プログラム対策ソフトウェアの導入と管理	①-3	一定期間、不正プログラムのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止又は隔離措置をとる。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
289	3.技術的対策	3.5. 不正プログラムへの対策	①不正プログラム対策ソフトウェアの導入と管理	①-4	医療情報システム等の構築に際しては、不正プログラム等の混入が生じないようにするための手順を策定し、これに則って構築する。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
290	3.技術的対策	3.5. 不正プログラムへの対策	①不正プログラム対策ソフトウェアの導入と管理	①-5	不正プログラム対策ソフトウェアのパターン定義ファイルを常に最新のものに更新する。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
291	3.技術的対策	3.5. 不正プログラムへの対策	①不正プログラム対策ソフトウェアの導入と管理	①-6	医療情報システム等の構築に際して、外部からプログラムを媒体で持ち込んだりダウンロードしたりする必要がある場合には、必ず事前に最新の不正プログラム対策ソフトウェア等の導入を行う。また情報システムへの影響度を勘案して、最新のセキュリティパッチの適用を行う。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソー	・ISO 27001 2013, 附属書 A.12.2

						ス ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	
292	3.技術的対策	3.5. 不正プログラムへの対策	①不正プログラム対策ソフトウェアの導入と管理	①-7	医療情報システム等利用環境がウイルス等による攻撃を受けた場合に、医療情報システム等提供に係る影響について、速やかに医療機関等に周知し、必要な対応等を求める。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
293	3.技術的対策	3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-1	医療情報はサーバ機器のみに保存し、表示のための一時的な保存等を除き、端末上に保存されることがないようにする。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google の利用規約は、お客様のデータへのアクセス手順を規定しています（5.2お客様のデータの保護）。Google はお客様にサービス及びテクニカルサポートサービス（TSS）を提供するため、又はお客様からの指示があった場合のみ、お客様のデータにアクセスし、ほかのGoogle 製品、サービス、又は広告には使用しません。また、Google のデータ処理およびセキュリティ条項で定められているように、Google はお客様のデータを保護するための管理、物理的、及び技術的な保護手段を実装し、維持します。 Google 独自のイベント管理ツールは、サイト間のトラフィックを監視し、疑わしい動作が検知されたときにアラートを送信するために、セキュリティチームによって利用されます。Google は、ソースコードなど特定の重要なデータの直接監視も実施しています。企業ネットワークと本番ネットワークの間で大量のデータが転送されることは日常的であり、それ自体がアラートの原因ではないことに注意してください。ただし、外部ストレージクラウドなどの外部の場所への大規模な転送、または想定していないIPアドレスからのソースコードへのアクセスは検出され、アラートが生成される可能性が高いです。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	
294	3.技術的対策	3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-2	ウェブブラウザの接続するサーバを業務上必要なサーバに限定する。	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」（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。	・ISO 27001 2013, 附属書 A.12.2

						Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。 Google は、ユーザー端末とGoogle の内部ネットワーク間のプロキシサーバーとして機能する独自の境界デバイスを介して、入出力トラフィックをルーティングします。 これらの境界デバイスを使用すると、Google の内部ネットワークと外部ネットワーク間の直接接続が防止され、内部ネットワーク識別子と構成の難読化、負荷分散、トラフィックフィルタリング、およびユーザーリクエストの効率的なルーティングが可能になります。	
295	3.技術的対策	3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-3	ウェブブラウザの設定で、認可していないサイトから、ActiveX、Java アプレット、Flash 等のプログラムコードをダウンロード及び実行することができない設定とする（管理ソフトウェアが実行されるサーバのみを認可する）。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。 Google は、情報システムを受容できないリスクにさらすソフトウェアやサービスの使用を制限するポリシーや手順を定めたガイダンスを作成しています。Google セキュリティチームは、Google を危険から保護するために、Google のシステム内の有害な脆弱性を検出してブロックしています。 Google は、アプリケーション(Adobe Flash Player、Javaブラウザプラグインなど)固有のセキュリティ上の欠陥によってブロックされたアプリケーションをリスト化し管理しています。	・ISO 27001 2013, 附属書 A.12.2
296	3.技術的対策	3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-4	認可したサイトからダウンロードされるコードについても不正プログラム対策ソフトウェアにより検査する。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
297	3.技術的対策	3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-5	ウェブブラウザからメールクライアント等の業務処理において想定しない外部アプリケーションが明示的な	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。	・ISO 27001 2013, 附属書 A.12.2

					確認なしに起動されないよう設定を行うことが望ましい。	Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	
298	3.技術的対策	3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-6	医療情報システム等のサーバ機器等への同時ログオンユーザ数（OS アカウント等）に適切な上限を設ける。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9.1.2,13.1
299	3.技術的対策	3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-7	医療情報システム等に用いる装置には、必要のないアプリケーション等をインストールしない。	Google は ISO27001 認証を受けています。この基準では、「ソフトウェアインストールの制限」（附属書 A.12.6）が規定されています。 Google は、承認されたマシンディストリビューションおよびソフトウェアバイナリリストに従ってプログラムの実行を防止します。Google は、非標準の分配をマシンで実行させない仕組みを導入しています。独自の構成管理ツールの設定は、バージョン管理システムの基準および承認された構成を使用して、すべての本番マシンのルートパーティション上のシステムファイルを同期します。ツールは、マシンに逸脱がないかどうかをチェックし、これらの差異を1日を通して正規化します。本番環境で実行される自動検証ソフトウェアは、承認されたチャネルを介してリリースされていないソフトウェアバイナリを検出します。	・ISO 27001 2013, 附属書 A.12.6
300	3.技術的対策	3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-8	医療情報システム等に関する情報を格納する機器を持ち出す場合には、当該持ち出しの目的に必要な最小限のアプリケーションをインストールする。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
301	3.技術的対策	3.6. 端末やサーバの堅牢化	①端末やサーバの堅牢化	①-9	医療情報システム等に関する情報を格納する機器を持ち出す際のアプリケーションのインストールに関する手順を定める。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
302	3.技術的対策	3.7. 機器・ソフトウェア	①安全性が確認できるネットワーク	①-1	ルータ等のネットワーク機器は、安全性が確認できる機器を利用する。	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。	・ISO 27001 2013, 附属書 A.11.2

		の脆弱性への対応	機器の利用			Google は、自社のマシンとネットワークデバイスのセキュリティ設定を管理しています。この構成情報は維持され、本番インスタンスと比較するためのマスターコピーとして機能します。設定のずれは識別され修正されます。	
303	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	①安全性が確認できるネットワーク機器の利用	①-2	ルータ等のネットワーク機器は、ISO/IEC 15408で規定されるセキュリティターゲット又はそれに類する文書が、本ガイドラインに適合しているものを選定する。	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。 Google は、すべてのハードウェアおよびネットワークデバイスを購入前に評価しています。Google におけるすべての重要なコンポーネントは、市販されていない独自の基準および高度にカスタマイズされた機能に従ってGoogle によって開発されます。そのため、標準規格を用いた評価はGoogle のハードウェアとソフトウェアには適用できません。その代わり、内部セキュリティレビューに依拠することで、Google は取得システムとサービスのテストを実施しています。	・ISO 27001 2013, 附属書 A.12.1.1
304	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	②パッチ適用等の実施	②-1	医療情報システム等に関連する技術的脆弱性については台帳等を利用して管理する。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
305	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	②パッチ適用等の実施	②-2	潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定する。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
306	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	②パッチ適用等の実施	②-3	修正パッチの適用前にパッチが改竄されていないこと及び有効性を検証する。	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）が規定されています。詳しくは、「Google インフラストラクチャのセキュリティ設計の概要」（https://cloud.google.com/security/security-design/）をご覧ください。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.12.1.2,14

307	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	②パッチ適用等の実施	②-4	オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システム等に対する影響を評価し、試験結果を確認してから実施する。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.4,14.2
308	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	③医療情報システム等への脆弱性診断の実施	③-1	提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行う。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入する。	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。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、 Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームは Google のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。	・ISO 27001 2013, 附属書 A.12.2
309	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	③医療情報システム等への脆弱性診断の実施	③-2	アプリケーションの安全性診断は提供しているサービスに対して直接実施するのではなく、別途、試験環境を用意して行うことが望ましい。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.12.1.4,14.2
310	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	③医療情報システム等への脆弱性診断の実施	③-3	開発されたソフトウェアの脆弱性検出をソースコードレベルで行うことが望ましい。 パッケージソフトウェア等、ソースコードの提供を要求できない場合には、ソースコードレベルではなく、アプリケーションを動作させて、外形的な脆弱性検査を行う。	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。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.14
311	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	④最新の脆弱性に関する情報の収集	④-1	アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとる。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、	・ISO 27001 2013, 附属書 A.12.2

						Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	
312	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	④最新の脆弱性に関する情報の収集	④-2	医療情報システム等の脆弱性に関する情報は、JPCERTコーディネーションセンター（JPCERT/CC）、内閣サイバーセキュリティセンター（NISC）、独立行政法人情報処理推進機構（IPA）等の情報源から、定期的及び必要なタイミングで取得し、確認する。	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」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。	・ISO 27001 2013, 附属書 A.12.2
313	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	⑤IoT機器に関する情報収集及び脆弱性への対応	⑤-1	IoT機器の利用を含むサービスを提供する場合、医療機関等との役割分担について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
314	3.技術的対策	3.7. 機器・ソフトウェアの脆弱性への対応	⑤IoT機器に関する情報収集及び脆弱性への対応	⑤-2	IoT機器の利用を含むサービスを提供する場合、利用が想定されるIoT機器に対する脆弱性に関する情報を定期的に収集し、必要な対策を講じる。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
315	3.技術的対策	3.8. ネットワーク上のアクセス制御	①ネットワークのアクセス制御	①-1	セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ等）を設置して、接続先の限定、接続時間の限定等、確立されたポリシーに基づいて各ネットワークインタフェースのアクセス制御を行う。ホスティング利用時等、ネットワーク境界にセキュリティゲートウェイを設置できない場合は、個々の情報処理装置（サーバ）にて、同様のアクセス制御を行う。	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。 Google は、自社のマシンとネットワークデバイスのセキュリティ設定を管理しています。この構成情報は維持され、本番インスタンスと比較するためのマスターコピーとして機能します。設定のずれは識別され修正されます。	・ISO 27001 2013, 附属書 A.11.2
316	3.技術的対策	3.8. ネットワーク上のアクセス制御	①ネットワークのアクセス制御	①-2	セキュリティゲートウェイでは、不正な IP アドレスを持つトラフィックが通過できないように設定する（接続機器類の IP アドレスをプライベートアドレスとして設定して、ファイアウォール、VPN 装置等のセキュリティゲートウェイを通過しようとするトラフィックを IP アドレスベースで制御する等）。	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」（ISO 27001 2013、附属書 A.13）と「公衆ネットワーク上のアプリケーション サービスのセキュリティの考慮」（ISO27002 2013、附属書 A.14.1.2）が規定されています。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.13,14.1.2
317	3.技術的対策	3.8. ネットワーク上のアクセス制御	①ネットワークのアクセス制御	①-3	医療情報システム等において、インターネット等のオープンネットワーク上のサービスとの接続について、以下にあげるサービスとの接続に限定する。他に	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。	・ISO 27001 2013, 附属書 A.13,14.1.2

					必要なサービスがある場合には、医療機関等の合意を得てから利用する。 ・ 外部からの医療情報システム等の稼動監視・遠隔保守 ・ セキュリティ対策ソフトウェアの最新パターンファイル等のダウンロード ・ オペレーティングシステム及び利用アプリケーションのセキュリティパッチファイル等のダウンロード ・ 電子署名時の時刻認証局へのアクセス、電子署名検証における失効リスト等認証局へのアクセス ・ ファイアウォール、IDS・IPS などのセキュリティ機器に対する不正アクセス監視 ・ 時刻同期のための時刻配信サーバへのアクセス ・ これらのサービスを利用するために必要なインターネットサービス（ドメインネームサーバへのアクセス等） ・ その他の医療情報システム等の稼動に必要なサービス（外部認証サーバ、外部医療情報データベース等）	Google Cloud 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。	
318	3.技術的対策	3.8. ネットワーク上のアクセス制御	②なりすましの防止	②-1	次の情報交換方法について予め合意しておく。 ・ 情報を電子媒体に記録して交換する際の手順 ・ 情報をネットワーク経由で文書ファイル形式にて交換する際の手順 ・ 情報をネットワーク経由でアプリケーション入力にて交換する際の手順 ・ 情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
319	3.技術的対策	3.8. ネットワーク上のアクセス制御	②なりすましの防止	②-2	情報交換手順では搬送の形態によらず次の事項を確実にする。 ・ 発送者、受領者を識別し記録する。 ・ 発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止対策を行う。 ・ 交換する情報の機密レベルに関して合意する（受領側で機密レベルが低くならないようにする）。 ・ 交換された情報に悪意のあるコードが含まれていないことを確実とする。	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。 インターネットを介した認証と管理者アクセスを保護するために暗号化を使用しています。Google が管理するマシンにリモートアクセスする場合は、Google が発行したデジタル証明書と2要素認証を必要とします。 Google は、Google Cloud プロダクトと Google Workspace プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://cloud.google.com/security/encryption-in-transit/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Google Cloud 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。	・ISO 27001 2013, 附属書 A.10
320	3.技術的対策	3.8. ネットワーク上のアクセス制御	②なりすましの防止	②-3	電子的に情報を転送する際には以下の対策を実施する。 ・ 送信者、受信者は相互に電子的に認証を行って相手の正当性を検証する。認証方式は接続形態、転送に利	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。 インターネットを介した認証と管理者アクセスを保護するために暗号化を使用しています。Google が管理するマシンにリモートアクセスする場合は、Google が発行したデジタル証明書と2要素認証を必要とします。	・ISO 27001 2013, 附属書 A.10

					用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。 ・ 送受信する経路は適切な方法で傍受のリスクから保護されている。 ・ 受信した情報について経路途中での損傷、改竄が無いことを検証する対策を講じる。 ・ 送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施する。	Google は、Google Cloud プロダクトと Google Workspace プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://cloud.google.com/security/encryption-in-transit/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Google Cloud 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。	
321	3.技術的対策	3.8. ネットワーク上のアクセス制御	②なりすましの防止	②-4	医療機関等から受託事業者までのネットワークにおいて、医療機関等の送受信の拠点の出入り口･使用機器･使用機器上の機能単位･利用者等の必要な単位で経路の確認を行う。	Google のセキュリティチームは強力な境界保護に尽力しており、専任のスタッフが Google のネットワークインフラの安全性とセキュリティに責任を負っています。 Google は、さまざまな種類のペネトレーションテストを通じて、ネットワーク境界の厳密なテストを内部で継続的に実施しています。さらに、Google は選定および認定された侵入テスターを使用して外部の第三者侵入テストを調整します。	-
322	3.技術的対策	3.8. ネットワーク上のアクセス制御	②なりすましの防止	②-5	②-4において、医療機関等が外部接続するサーバ等と受託事業者のサーバとの間の相互認証を行う。	Google のセキュリティチームは強力な境界保護に尽力しており、専任のスタッフが Google のネットワークインフラの安全性とセキュリティに責任を負っています。 Google は、さまざまな種類のペネトレーションテストを通じて、ネットワーク境界の厳密なテストを内部で継続的に実施しています。さらに、Google は選定および認定された侵入テスターを使用して外部の第三者侵入テストを調整します。	-
323	3.技術的対策	3.8. ネットワーク上のアクセス制御	②なりすましの防止	②-6	②-4について、受託事業者が保守業務を再委託している場合には、受託事業者と再委託先との接続では、別途なりすましを防止する策を講じる。	Google のセキュリティチームは強力な境界保護に尽力しており、専任のスタッフが Google のネットワークインフラの安全性とセキュリティに責任を負っています。 Google は、さまざまな種類のペネトレーションテストを通じて、ネットワーク境界の厳密なテストを内部で継続的に実施しています。さらに、Google は選定および認定された侵入テスターを使用して外部の第三者侵入テストを調整します。	-
324	3.技術的対策	3.8. ネットワーク上のアクセス制御	②なりすましの防止	②-7	厚生労働省ガイドライン第5版6.11 C項の2に基づいて医療機関等が採用する通信方式認証手段が妥当なものであることの確認について、医療機関等と合意する。	Google のセキュリティチームは強力な境界保護に尽力しており、専任のスタッフが Google のネットワークインフラの安全性とセキュリティに責任を負っています。 Google は、さまざまな種類のペネトレーションテストを通じて、ネットワーク境界の厳密なテストを内部で継続的に実施しています。さらに、Google は選定および認定された侵入テスターを使用して外部の第三者侵入テストを調整します。	-
325	3.技術的対策	3.8. ネットワーク上のアクセス制御	③ネットワークポートへの不正な装置の接続制限	③-1	ネットワーク機器及びサーバ、端末の利用していないネットワークポートへの物理的な接続を制限する。	Google は ISO27001 認証を受けています。この基準では、「装置」（ISO 27001 2013、附属書 A.11.2）が規定されています。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。	・ISO 27001 2013, 附属書 A.11.2

						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	
326	3.技術的対策	3.8. ネットワーク上のアクセス制御	③ネットワークポートへの不正な装置の接続制限	③-2	不正な装置を識別するため、医療情報システム等内で利用する情報処理装置を登録したリストを作成・維持する。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5
327	3.技術的対策	3.8. ネットワーク上のアクセス制御	③ネットワークポートへの不正な装置の接続制限	③-3	不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用する。	Google は ISO27001 認証を受けています。この基準では、「ログ取得及び監視」（ISO 27001 2013、附属書 A.12.4）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google のセキュリティ モニタリング プログラムは、内部ネットワーク トラフィックから収集されている情報、社員によるシステム上の操作、外部に知られている脆弱性に焦点を当てています。Google のグローバル ネットワークのさまざまな箇所で、内部トラフィックに疑わしい動作（たとえば、トラフィックにボットネットに接続している可能性が見られるなど）がないか検査しています。この分析では、オープンソースのツールと商用ツールを組み合わせて使用し、トラフィックのキャプチャと解析を行っています。Google の技術を基に構築された独自の相関システムもこの解析をサポートしています。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティ エンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データ レポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリング リスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知して Google セキュリティ スタッフに通知します。ネットワーク解析 に加え、システムログの自動解析も行われています。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.12.4
328	3.技術的対策	3.8. ネットワーク上のアクセス制御	④無線LAN利用時の対策	④-1	医療情報を取り扱うサービスの利用に際して、医療機関等が無線LANを利用する場合に必要なセキュリティ対策について、医療情報システム等事業者の役割分担等について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
329	3.技術的対策	3.8. ネットワーク上のアクセス制御	④無線LAN利用時の対策	④-2	業務上、医療情報システム等に関する情報を格納するモバイル端末を持ち出す場合には、公衆無線LANへの接続は行わない。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-

330	3.技術的対策	3.9. 不正な通信の検知や遮断	①ネットワーク上の不正な通信の検知や遮断	①-1	医療機関等との接続ネットワーク境界には侵入検知システム（IDS）、侵入防止システム（IPS）等を導入してネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行う。ホスティング利用時等、ネットワーク境界に装置を設置できない場合は、個々の情報処理装置にて、同様の制御を行う。	Google は、潜在的なセキュリティ問題を検出して対処するためのネットワークおよびホストベースのツールを実装しています。 Google は調査をサポートするために自動化されたログ収集および分析ツールを維持しています。	-
331	3.技術的対策	3.9. 不正な通信の検知や遮断	①ネットワーク上の不正な通信の検知や遮断	①-2	侵入検知システム等が、常に最新の攻撃・不正アクセスに対応可能なように、シグネチャ・検知ルール等の更新、ソフトウェアのセキュリティパッチの適用等を行う。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9.1.2,13.1
332	3.技術的対策	3.9. 不正な通信の検知や遮断	①ネットワーク上の不正な通信の検知や遮断	①-3	侵入検知システム等が、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定とする。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9.1.2,13.1
333	3.技術的対策	3.9. 不正な通信の検知や遮断	①ネットワーク上の不正な通信の検知や遮断	①-4	侵入検知の記録には不正アクセス等の事後処理に必要な項目が含める。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク管理策」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直	・ISO 27001 2013, 附属書 A.9.1.2,13.1

						接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。	
334	3.技術的対策	3.9. 不正な通信の検知や遮断	①ネットワーク上の不正な通信の検知や遮断	①-5	医療情報システム等から、不正・不審なトラフィックが内部ネットワークから外部ネットワークへと流れていないことをネットワーク境界において監視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、「ログ取得及び監視」（ISO 27001 2013、附属書 A.12.4）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google のセキュリティ モニタリング プログラムは、内部ネットワーク トラフィックから収集されている情報、社員によるシステム上の操作、外部に知られている脆弱性に焦点を当てています。Google のグローバル ネットワークのさまざまな箇所で、内部トラフィックに疑わしい動作（たとえば、トラフィックにボットネットに接続している可能性が見られるなど）がないか検査しています。この分析では、オープンソースのツールと商用ツールを組み合わせて使用し、トラフィックのキャプチャと解析を行っています。Google の技術を基に構築された独自の相関システムもこの解析をサポートしています。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティ エンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データ レポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリング リスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知して Google セキュリティ スタッフに通知します。ネットワーク解析 に加え、システムログの自動解析も行われています。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.12.4
335	3.技術的対策	3.9. 不正な通信の検知や遮断	①ネットワーク上の不正な通信の検知や遮断	①-6	侵入検知システム自身が攻撃・不正アクセスの対象とならないように、その存在を外部から隠す設定（ステルスモード）や、侵入検知システムへのアクセスの適切な制御を実施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、「ネットワークおよびネットワーク サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ISO 27001 2013、附属書 A.13.1）が規定されています。 Google では厳格なインシデント管理プロセスにより、システムやデータの機密性、完全性、または可用性に影響を与える可能性があるセキュリティ イベントに対応しています。インシデントが発生した場合、セキュリティ チームはインシデントを 記録して、重大度に応じて優先順位を設定します。直接お客様に影響を与えるイベントには、特に高い優先順位が設定されます。このプロセスでは、行動方針や、通知、エスカレーション、対処、および文書化のための手順が指定されています。中心となるスタッフは、イベント発生に備えて、サードパーティ ツールや独自ツールの使用など、フォレンジクスや証拠取り扱いの訓練を受けています。お客様の機密情報を保存するシステムなどの重要な領域では、インシデント対応計画のテストを実施しています。こうしたテストでは、内部関係者による脅威やソフトウェアの脆弱性など、さまざまなシナリオが考慮されています。セキュリティ上のインシデントを早期解決するため、Google のセキュリティ チームは、24 時間体制で全社員からの問い合わせに対応しています。インシデントでお客様のデータが影響を受ける場合、Google またはそのパートナーはお客様にその旨を通知し、Google のサポートチームを通じて調査活動に協力します。 Google Cloud のお客様は、お使いの環境を設定、管理するほか、不正アクセスを検知、レビューするすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.9.1.2,13.1

336	3.技術的対策	3.9. 不正な通信の検知や遮断	①ネットワーク上の不正な通信の検知や遮断	①-7	IoT機器の利用を含むサービスを提供する場合、IoT機器による医療情報システム等へのアクセス状況を記録し、不正なアクセスがないことを定期的に監視する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
337	3.技術的対策	3.10. 外部へ持ち出す機器や情報の管理	①持ち出しを行う機器の認証	①-1	機器等については、起動パスワードの設定を行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。Google の利用規約は、お客様のデータへのアクセス手順を規定しています（5.2お客様のデータの保護）。Google はお客様にサービス及びテクニカルサポートサービス（TSS）を提供するため、又はお客様からの指示があった場合のみ、お客様のデータにアクセスし、ほかのGoogle 製品、サービス、又は広告には使用しません。また、Google のデータ処理およびセキュリティ条項で定められているように、Google はお客様のデータを保護するための管理、物理的、及び技術的な保護手段を実装し、維持します。 Google セキュリティチームは、モバイルデバイスの使用制限、接続要件、構成要件及び実装ガイダンスを確立します。Google はモバイルデバイスの複数のトラスト層を特定しました。高権限アクセスとして分類されたデバイスのみが、本番環境へのアクセスを許可されます。Google はマシン証明書を発行し、これは本番環境へ接続する全てのデバイスにインストールすることが求められます。Google のネットワークインフラストラクチャは、マシン証明書を検証し、有効な証明書のないアクセスを拒否します。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud のお客様は、運用手順書の利用ガイドの作成など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013、附属書 A.9
338	3.技術的対策	3.10. 外部へ持ち出す機器や情報の管理	①持ち出しを行う機器の認証	①-2	起動パスワードは、推定しにくいものを設定する、機器の特性に応じて定期的に変更を行う等、第三者による不正な機器の起動がなされないよう対策を講じる。	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。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへの	・ISO 27001 2013、附属書 A.9

						アクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。Google の利用規約は、お客様のデータへのアクセス手順を規定しています（5.2お客様のデータの保護）。Google はお客様にサービス及びテクニカルサポートサービス（TSS）を提供するため、又はお客様からの指示があった場合のみ、お客様のデータにアクセスし、ほかのGoogle 製品、サービス、又は広告には使用しません。また、Google のデータ処理およびセキュリティ条項で定められているように、Google はお客様のデータを保護するための管理、物理的、及び技術的な保護手段を実装し、維持します。 Google セキュリティチームは、モバイルデバイスの使用制限、接続要件、構成要件及び実装ガイダンスを確立します。Google はモバイルデバイスの複数のトラスト層を特定しました。高権限アクセスとして分類されたデバイスのみが、本番環境へのアクセスを許可されます。Google はマシン証明書を発行し、これは本番環境へ接続する全てのデバイスにインストールすることが求められます。Google のネットワークインフラストラクチャは、マシン証明書を検証し、有効な証明書のないアクセスを拒否します。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud 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。	
339	3.技術的対策	3.10. 外部へ持ち出す機器や情報の管理	①持ち出しを行う機器の認証	①-3	医療情報システム等に関する情報を格納する情報機器へのログイン及びアクセスについては、複数の認証要素を組み合わせて行う。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。社員の承認設定は、Google Cloud や Google Workspace に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。Google の利用規約は、お客様のデータへのアクセス手順を規定しています（5.2お客様のデータの保護）。Google はお客様にサービス及びテクニカルサポートサービス（TSS）を提供するため、又はお客様からの指示があった場合のみ、お客様のデータにアクセスし、ほかのGoogle 製品、サービス、又は広告には使用しません。また、Google のデータ処理およびセキュリティ条項で定められているように、Google はお客様のデータを保護するための管理、物理的、及び技術的な保護手段を実装し、維持します。 Google セキュリティチームは、モバイルデバイスの使用制限、接続要件、構成要件及び実装ガイダンスを確立します。Google はモバイルデバイスの複数のトラスト層を特定しました。高権限アクセスとして分類されたデバイスのみが、本番環境へのアクセスを許可されます。Google はマシン証明書を発行し、これは本番環境へ接続する全てのデバイスにインストールすることが求められます。Google のネットワークインフラストラクチャは、マシン証明書を検証し、有効な証明書のないアクセスを拒否します。	・ISO 27001 2013、附属書 A.9

						Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud 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。	
340	3.技術的対策	3.10. 外部へ持ち出す機器や情報の管理	②搬送する情報に対する対策	②-1	情報を格納する機器･媒体等を持ち出す場合の手順には、機器･媒体自体に暗号化措置を施す、格納されている情報に暗号化措置を講じる、パスワードを設定する等の事項を含める。	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。 アップロード、作成されたお客様のデータを暗号化しています。Google では複数の暗号化レイヤーを使用してデータを保護しています。複数の暗号化レイヤーを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと Google Workspace プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Google Cloud 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。	・ISO 27001 2013, 附属書 A10
341	3.技術的対策	3.11. 仮想デスクトップやMDM・MAMによる情報漏洩への対策	①個人所有の機器の管理	①-1	利用者が個人所有する機器による医療情報システム等利用に関する対応策について、医療機関等と合意する。 なお具体的には以下の内容を参考にする。 ・利用者が所有する機器からの情報漏洩等を防止する観点から、例えば、仮想デスクトップを用いてOS レベルで業務利用領域と個人利用領域を分け、業務利用領域を医療機関等が管理できるようにするほか、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し管理する端末と同等のセキュリティ対策の徹底を図ることなどが考えられる。	従業員には、業務用のGoogle のマシンおよびモバイルデバイスが与えられています。さらに Google は、Google が管理し、従業員が所有しているデバイスを業務利用することも許可しています。このような従業員所有のデバイスも完全にGoogle によって管理されています。	-
342	3.技術的対策	3.11. 仮想デスクトップやMDM・MAMによる情報漏洩への対策	①個人所有の機器の管理	①-2	サービスの提供に係る目的（開発、保守、運用含む）で従業員等の個人所有の機器を利用することは原則禁止とする。	従業員には、業務用のGoogle のマシンおよびモバイルデバイスが与えられています。さらに Google は、Google が管理し、従業員が所有しているデバイスを業務利用することも許可しています。このような従業員所有のデバイスも完全にGoogle によって管理されています。	-
343	3.技術的対策	3.11. 仮想デスクトップやMDM・MAMによる情報	②端末側に情報を残さない技術の導入	②-1	医療機関等の利用者が、医療機関等の外部からサービスを利用する場合に、医療機関等の利用者が用いるPCの作業環境に仮想デスクトップ等の技術を導入するための受託事業者の役割分担等につき、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-

		漏洩への対策					
344	3.技術的対策	3.12. 未登録の電子媒体の接続制限	①サーバ等への未登録の電子媒体の接続制限	①-1	医療情報システム等においてはサーバ等に接続できる電子媒体の種別を限定するため、不要なデバイスドライバを削除する。加えて、認められていない種類の装置の接続を防止する為に、管理者以外がデバイスドライバのインストールやアンインストールが出来ない設定とすることが望ましい。	Google は ISO27001 と ISO27017の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）、「変更管理」（ISO 27001 2013、附属書 A.12.1.2）、「仮想マシン（ハードニング）」（ISO 27017 2015、附属書 A.CLD.9.4.2）が規定されています。 論理的なアクセス制御や変更管理はじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、不要な機能やポートなどを排除するために、高度にカスタマイズされたデバイス又は初期設定から変更されたオペレーティングシステムや設定を使用します。Google のシステムエンジニアは、セキュリティを向上させ、デバイスの攻撃ベクトルを大幅に削減するカスタム設定を作成します。また、ツールを使用して、本番マシンが事前定義されたオペレーティングシステム(OS) 設定から逸脱した場合には検知し、自動で修正されます。これにより、一貫性のある方法でシステムファイルの更新を簡単にロールアウトできるため、マシンも自動的にアップデートがなされます。	・ISO 27001:2013, 附属書 A.9,12.1.2 ・ISO 27017:2015, 附属書 A.CLD.9.4.2
345	3.技術的対策	3.12. 未登録の電子媒体の接続制限	①サーバ等への未登録の電子媒体の接続制限	①-2	不要なデバイスドライバが追加されていないことを定期的に検証することが望ましい。	Google は ISO27001 と ISO27017の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）、「変更管理」（ISO 27001 2013、附属書 A.12.1.2）、「仮想マシン（ハードニング）」（ISO 27017 2015、附属書 A.CLD.9.4.2）が規定されています。 論理的なアクセス制御や変更管理はじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、不要な機能やポートなどを排除するために、高度にカスタマイズされたデバイス又は初期設定から変更されたオペレーティングシステムや設定を使用します。Google のシステムエンジニアは、セキュリティを向上させ、デバイスの攻撃ベクトルを大幅に削減するカスタム設定を作成します。また、ツールを使用して、本番マシンが事前定義されたオペレーティングシステム(OS) 設定から逸脱した場合には検知し、自動で修正されます。これにより、一貫性のある方法でシステムファイルの更新を簡単にロールアウトできるため、マシンも自動的にアップデートがなされます。	・ISO 27001:2013, 附属書 A.12.1.2
346	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-1	ネットワークにおいて、情報の盗聴、改竄、誤った経路での通信、破壊等から保護するために必要な措置（情報交換の実施基準･手順等の整備、通信の暗号化等）を行う。	Google は ISO27001 と ISO27017の認証を受けています。この基準では、「暗号化制御」（ISO 27001 2013、附属書 A.10.1）、「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。 ネットワーク構成や管理はじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google または Google の代理者が管理していない物理的境界の外側を転送中のデータが移動する場合、Google は 1 つ以上のネットワークレイヤーでそのデータを暗号化し、認証します。詳しくは https://cloud.google.com/security/encryption-in-transit/ をご覧ください。	・ISO 27001 2013, 附属書 A.10.1,13.1
347	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-2	アクセス先のなりすまし（セッション乗っ取り、フィッシング等）等を防ぐのに必要な措置(サーバ証明書の導入等）を行う。	Google は ISO27001 と ISO27017の認証を受けています。この基準では、「暗号化制御」（ISO 27001 2013、附属書 A.10.1）、「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。 ネットワーク構成や管理はじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google または Google の代理者が管理していない物理的境界の外側を転送中のデータが移動する場合、Google は 1 つ以上のネットワークレイヤーでそのデータを暗号化し、認証します。詳しくは https://cloud.google.com/security/encryption-in-transit/ をご覧ください。	・ISO 27001 2013, 附属書 A.10.1,13.1
348	3.技術的対策	3.13. 暗号化・電	①安全性が確認された暗号	①-3	経路の安全性確保のため、IPsec + IKEへの対応や閉域ネットワークへの対応等及びその条件等について、医療機関等と合意する。	Google は ISO27001 と ISO27017の認証を受けています。この基準では、「暗号化制御」（ISO 27001 2013、附属書 A.10.1）、「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。	・ISO 27001 2013, 附属書 A.10.1,13.1

		子署名の利用	化・電子署名の利用			ネットワーク構成や管理はじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google または Google の代理者が管理していない物理的境界の外側を転送中のデータが移動する場合、Google は 1 つ以上のネットワークレイヤーでそのデータを暗号化し、認証します。詳しくは https://cloud.google.com/security/encryption-in-transit/ をご覧ください。	
349	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-4	情報伝送に用いるケーブル類については直接の傍受リスクについて配慮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。 セキュリティとデータ保護を重視する方針は、Google の設計基準の根幹をなしています。Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。データセンターには棟の内外に高解像度の監視カメラを設置し、24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画 https://www.youtube.com/watch?v=XZmGGAbHqa0 Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。	・ISO 27001 2013, 附属書 A.11
350	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-5	暗号アルゴリズムは十分な安全性を有するものを使用する。選択基準としては電子政府推奨暗号リスト 等を用いる。	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。 アップロード、作成されたお客様のデータを暗号化しています。Google では複数の暗号化レイヤを使用してデータを保護しています。複数の暗号化レイヤーを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと Google Workspace プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Google Cloud 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。	・ISO 27001 2013, 附属書 A.10
351	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-6	送信元と送信先の間で、暗号化等の情報そのものに対するセキュリティ対策を実施する。	Google または Google の代理者が管理していない物理的境界の外側を転送中のデータが移動する場合、Google は 1 つ以上のネットワークレイヤでそのデータを暗号化し、認証します。詳しくは https://cloud.google.com/security/encryption-in-transit/ をご覧ください。	・ISO 27001 2013, 附属書 A.10
352	3.技術的対策	3.13. 暗号化・電	①安全性が確認さ	①-7	サービスの提供においてSSL/TLSを用いる際には、TLS1.2に対応した措置を講じる。	Google は、オープンな暗号化手法の使用をサポートしています。 Google は、すべての認証トラフィックに対してTLS を強制します。	-

		子署名の利用	れた暗号化・電子署名の利用			お客様のデータは、Google の内部ネットワーク上や転送中、保存中に暗号化されます。	
353	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-8	①-7のほか、医療機関等がメールの暗号化（S/MIME等）やファイルの暗号化への対応を求める場合には、その対応に必要な措置及び条件等について、医療機関等と合意する。	Google または Google の代理者が管理していない物理的境界の外側を転送中のデータが移動する場合、Google は 1 つ以上のネットワークレイヤでそのデータを暗号化し、認証します。詳しくは https://cloud.google.com/security/encryption-in-transit/ をご覧ください。	・ISO 27001 2013, 附属書 A.10
354	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-9	VPN 接続を行う場合には以下の事項に従う。 ・ 接続時に VPN 装置間で相互に認証を行う。 ・ 傍受、リプレイ等のリスクを最小限に抑えるために、適切な暗号技術を利用する。 ・ インターネット上のトラフィックが VPN チャンネルに混入しないように、プライベートネットワークインタフェースとインターネットインタフェースの間に直接の経路を設定しない。 ・ 複数の医療機関等から情報処理業務を受託している場合には、医療機関等の間で情報が混同するリスクを避けるためVPN チャンネルを医療機関等別に構築する等の対策を実施する。	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」（ISO 27001 2013、附属書 A.13）と「公衆ネットワーク上のアプリケーション サービスのセキュリティの考慮」（ISO27002 2013、附属書 A.14.1.2）が規定されています。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.13,14.1.2
355	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-10	オープンなネットワークを介してHTTPS を利用した接続を行う際は、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性の高い「高セキュリティ型」に準じた適切な設定を行う。	Google は、オープンな暗号化技術の使用をサポートしています。 Google はすべての認証トラフィックに対して TLS を強制します。顧客データは、Google の社内ネットワーク上、伝送中、および保管中に暗号化されます。	-
356	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-11	SSL-VPNは、原則として使用しない。	Google は、オープンな暗号化技術の使用をサポートしています。 Google はすべての認証トラフィックに対して TLS を強制します。顧客データは、Google の社内ネットワーク上、伝送中、および保管中に暗号化されます。	-
357	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子署名の利用	①-12	サービス提供に際して、ソフトウェア型のIPsec 又はTLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃について、適切な対策を実施する。	Google は、オープンな暗号化技術の使用をサポートしています。 Google はすべての認証トラフィックに対して TLS を強制します。顧客データは、Google の社内ネットワーク上、伝送中、および保管中に暗号化されます。	-
358	3.技術的対策	3.13. 暗号化・電子署名の利用	①安全性が確認された暗号化・電子	①-13	医療機関等における利用者がソフトウェア型のIPsec 又はTLS1.2 により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃についての、適切な対策	Google は、オープンな暗号化技術の使用をサポートしています。 Google はすべての認証トラフィックに対して TLS を強制します。顧客データは、Google の社内ネットワーク上、伝送中、および保管中に暗号化されます。	-

			署名の利用		に関する情報提供を行う。情報提供の範囲、条件等について、医療機関等と合意する。		
359	3.技術的対策	3.13. 暗号化・電子署名の利用	②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理	②-1	暗号鍵が漏洩した場合に備えた対応策を策定しておく。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（ISO 27001 2013、附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェア セキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかると、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告 されている問題を追跡しています。セキュリティ問題の報告について詳しくは、https://www.google.com/about/appsecurity/ をご覧ください。 Google では、情報セキュリティチームのメンバーがすべてのネットワーク、システム、サービスのセキュリティ計画を確認しています。このチームは Google のプロダクト チームやエンジニアリング チームにプロジェクトごとのコンサルティング サービスを行っています。このチームは、Google のネットワーク上の不審な動作を監視し、情報セキュリティ上の脅威に対処し、セキュリティ評価および監査を日常的に実施し、外部の専門家による定期的なセキュリティ評価を実施します。Google では「プロジェクト ゼロ」という専門チームを作りました。このチームは指定の攻撃を防ぐことを目的とし、バグをソフトウェア ベンダーに報告して外部データベースに記録しています。	・ISO 27001 2013, 附属書 A.12.2
360	3.技術的対策	3.13. 暗号化・電子署名の利用	②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理	②-2	電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとする。	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。 Google は認証の整合性を達成するために証明書と ACL を使用します。	・ISO 27001 2013, 附属書 A.9
361	3.技術的対策	3.13. 暗号化・電子署名の利用	②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理	②-3	暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮する。	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。 アップロード、作成されたお客様のデータを暗号化しています。Google では複数の暗号化レイヤーを使用してデータを保護しています。複数の暗号化レイヤーを使用することにより、冗長データ保護機能が追加され、アプリケーションの要件に基づいて最適な手法を選択できるようになります。 Google は、Google Cloud プロダクトと Google Workspace プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Google Cloud 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。	・ISO 27001 2013, 附属書 A.10

362	3.技術的対策	3.13. 暗号化・電子署名の利用	②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理	②-4	医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
363	3.技術的対策	3.13. 暗号化・電子署名の利用	②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理	②-5	暗号モジュールが外部のソースコードやライブラリを利用する場合には、その真正性を、製造元による電子署名等による完全性の検証を行った上で利用することが望ましい。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
364	3.技術的対策	3.13. 暗号化・電子署名の利用	②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理	②-6	暗号鍵の生成は耐タンパー性 を有する IC カード、USB トークンデバイスといった安全な環境で実施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、「暗号」（ISO 27001 2013、附属書 A.10 ）が規定されています。 Google は、Google Cloud プロダクトと Google Workspace プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-in-transit/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Google Cloud 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。	・ISO 27001 2013, 附属書 A.10
365	3.技術的対策	3.13. 暗号化・電子署名の利用	②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理	②-7	暗号鍵の喪失に備えて鍵預託を行う場合は、暗号鍵のリポジトリに正当な管理者及び正当なプロセスのみがアクセスできるようアクセス制御を行うことが望ましい。	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。 Google は、Google Cloud プロダクトと Google Workspace プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://services.google.com/fh/files/misc/google-workspace-encryption-wp.pdf Google Cloud 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。	・ISO 27001 2013, 附属書 A.10
366	3.技術的対策	3.13. 暗号化・電子署名の利用	②暗号アルゴリズムの危殆化や暗号鍵の漏洩に備えた暗号鍵及び電子署名の管理	②-8	電子署名法にもとづき、医療従事者が文書に施した電子署名を検証する環境においては、暗号アルゴリズムの脆弱化に影響されずに署名検証を継続できるようにすることが望ましい。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-

367	3.技術的対策	3.14. リモートメンテナンスのアクセス管理	①リモートメンテナンスの不必要なログインを防止するためのアクセス管理	①-1	リモートメンテナンスにより保守を行う場合、必要に応じて適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等の安全管理措置を講じる。	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。 セキュリティに対するベンダーの取り組みをはじめとする、情報セキュリティの監督管理体制は、、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はサービスを提供するために、事実上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。	・ISO 27001 2013, 附属書 A.15
368	3.技術的対策	3.15. 電子署名を利用する場合の管理	①信頼できる第三者機関が発行した電子証明書の利用	①-1	医療情報システム等において電子署名を利用する場合、保健医療福祉分野PKI 認証局の発行する署名用電子証明書等の信頼できる第三者機関が発行した電子証明書を利用する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
369	3.技術的対策	3.15. 電子署名を利用する場合の管理	②電子署名を施す場合のタイムスタンプの付与	②-1	電子署名を施す情報に対しては、タイムスタンプを付与する。この場合には、タイムスタンプの内容･検証方法について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
370	3.技術的対策	3.15. 電子署名を利用する場合の管理	②電子署名を施す場合のタイムスタンプの付与	②-2	タイムスタンプを付与した情報を取り扱う場合に、法定保存年限内における当該タイムスタンプの有効性を検証する方法、対応方法等について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
371	3.技術的対策	3.15. 電子署名を利用する場合の管理	②電子署名を施す場合のタイムスタンプの付与	②-3	タイムスタンプを付与した情報を取り扱う場合に、当該情報を長期保存する場合に講じる対策等について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
372	3.技術的対策	3.15. 電子署名を利用する場合の管理	③タイムスタンプを付与する時点で有効な電子証明書の使用	③-1	タイムスタンプを付与した情報を取り扱う場合に、電子証明書の失効前の電子署名の有効性を担保するためのタイムスタンプの付与方法等について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-

373	3.技術的対策	3.16. 改竄防止・検知策の実装	①ソフトウェアの改竄防止・検知策の実装	①-1	不正な改竄を受けていないことを検証するため、定期的にソフトウェアの整合性検査（改竄検知）を実施する。	Google は ISO27001 認証を受けています。この基準では、「ログ取得及び監視」（ISO 27001 2013、附属書 A.12.4）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google のセキュリティ モニタリング プログラムは、内部ネットワーク トラフィックから収集されている情報、社員によるシステム上の操作、外部に知られている脆弱性に焦点を当てています。Google のグローバル ネットワークのさまざまな箇所で、内部トラフィックに疑わしい動作（たとえば、トラフィックにボットネットに接続している可能性が見られるなど）がないか検査しています。この分析では、オープンソースのツールと商用ツールを組み合わせて使用し、トラフィックのキャプチャと解析を行っています。Google の技術を基に構築された独自の相関システムもこの解析をサポートしています。こうしたネットワーク解析に加え、顧客データへのアクセスの試行などの異常な動向を特定するために、システムログを精査しています。Google のセキュリティ エンジニアは、Google のインフラストラクチャに影響する可能性があるセキュリティ上のインシデントを検知する永続的な検索アラートを一般公開データ レポジトリに設定しています。また、受信したセキュリティレポートの確認や、公開のメーリング リスト、ブログ、Wiki のモニタリングを積極的に行っています。自動ネットワーク解析は、未知の脅威が発生した可能性がある状態を検知して Google セキュリティ スタッフに通知します。ネットワーク解析 に加え、システムログの自動解析も行われています。 Google Cloud 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。	・ISO 27001 2013, 附属書 A.12.4
374	3.技術的対策	3.16. 改竄防止・検知策の実装	①ソフトウェアの改竄防止・検知策の実装	①-2	不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改竄防止、検知策を実施する。	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）が規定されています。詳しくは、「Google インフラストラクチャのセキュリティ設計の概要」（https://cloud.google.com/security/security-design/）をご覧ください。 Google Cloud のお客様は、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。	・ISO 27001 2013, 附属書 A.12.1.2,14
375	3.技術的対策	3.17. 患者ごとの情報の管理	①患者ごとに情報を管理する機能の実装	①-1	医療情報システム等には、受託する医療情報を患者等ごとに管理できる機能を含める。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
376	3.技術的対策	3.18. 利用目的に応じた応答時間の確保	①医療情報システム等の利用目的に応じた応答時間の確保	①-1	医療機関等が医療情報システム等を利用する際の、応答時間（一般的な表示速度、検索結果の表示時間等）について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
377	3.技術的対策	3.19. 冗長化による障害対策	①医療情報システム等の停止に備えた冗長化	①-1	情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。	・ISO 27001 2013, 附属書 A.17.2

						Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	
378	3.技術的対策	3.19. 冗長化による障害対策	①医療情報システム等の停止に備えた冗長化	①-2	医療情報システム等、ネットワーク等に関し、通常の診療等に影響が生じないようサービスの継続に必要な冗長化対策を講じる。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
379	3.技術的対策	3.19. 冗長化による障害対策	①医療情報システム等の停止に備えた冗長化	①-3	①-2を踏まえて、障害等が生じた場合のサービスの継続性を保証する水準について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。	・ISO 27001 2013, 附属書 A.17.2,12.3

						冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	
380	3.技術的対策	3.19. 冗長化による障害対策	①医療情報システム等の停止に備えた冗長化	①-4	障害時等でも診療等が継続できるようにするための医療機関等の側の代替措置等について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
381	3.技術的対策	3.19. 冗長化による障害対策	②ディスク障害対策	②-1	診療録等の情報をハードディスク等の記録機器に保存する場合、RAID-1又はRAID-6相当以上のディスク障害対策を講じる。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内	・ISO 27001 2013, 附属書 A.17.2,12.3

						でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	
382	3.技術的対策	3.20. システム障害時の措置	①医療情報システム等障害時における機能の実装	①-1	医療情報を医療機関等に保存する場合に、障害時における見読性確保のために医療機関等側で講じうる方策に関する情報提供について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）、「バックアップ」（ISO27001 2013、附属書 A.12.3）と「操作手順書」（ISO27001 2013、附属書 A.12.1.1.）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3,12.1.1.
383	3.技術的対策	3.20. システム障害時の措置	①医療情報システム等障害時における機能の実装	①-2	ハードウェア及びソフトウェアの持つ影響度の大きさを評価し、影響度が大きすぎる部分については、該当システム部分の冗長化や、システムに障害が発生して情報の閲覧が不可能となった際に備え、汎用のブラウザ等で閲覧が可能となるよう、見読性が確保される形式（PDF、JPEG 及び PNG 等のフォーマット）で外部ファイルに出力可能とすることなどの方策を講じる。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3

384	3.技術的対策	3.20. システム障害時の措置	①医療情報システム等障害時における機能の実装	①-3	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために必要な外部ファイル等の出力に関する機能の提供の有無、内容について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）、「バックアップ」（ISO27001 2013、附属書 A.12.3）と「操作手順書」（ISO27001 2013、附属書 A.12.1.1.）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3,12.1.1.
385	3.技術的対策	3.20. システム障害時の措置	①医療情報システム等障害時における機能の実装	①-4	医療情報を医療機関等に保存する場合に、障害時の見読性を確保するために遠隔地に保存するバックアップデータの利用のための機能、利用に必要な情報の提供、条件等について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。	・ISO 27001 2013, 附属書 A.17.2
386	3.技術的対策	3.20. システム障害時の措置	①医療情報システム等障害時における機能の実装	①-5	緊急時に備えた医療機関等における診療録等の見読性の確保を支援する機能（例えば画面の印刷機能、ファイルダウンロードの機能等)をサービスに含め、これに必要なセキュリティ等の情報提供について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）、「バックアップ」（ISO27001 2013、附属書 A.12.3）と「操作手順書」（ISO27001 2013、附属書 A.12.1.1.）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計	・ISO 27001 2013, 附属書 A.17.2,12.3,12.1.1.

						全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、該当するリージョンやゾーンを設定して障害や災害を防止するなど、お使いの環境を設定、管理するすべての権利と責任を保有します。	
387	3.技術的対策	3.20. システム障害時の措置	①医療情報システム等障害時における機能の実装	①-6	障害等が生じた場合の役割分担を明確にした上で、稼動を保証するサービスの範囲について、医療機関等と合意する。	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。 Google Cloud - 利用規約: https://cloud.google.com/terms Google Workspace - 利用規約: https://workspace.google.com/terms/premier_terms.html SLA https://cloud.google.com/terms/sla/ https://workspace.google.com/terms/sla.html	-
388	3.技術的対策	3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-1	電子媒体の損傷等による情報喪失のリスクを最小限にするため電子媒体の製造者により指定される保管環境にて保管する。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書 A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書 A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコード及び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、金属探知機やビデオ監視機器を導入しています。ライフサイクルにおける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、ディスクに対してゼロ書き込みを実施後、複数段階の検証ステップを経て、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されます。 Google Cloud のお客様は、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.8.1,8.3.2,11.2.7,12.5
389	3.技術的対策	3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-2	各医療機関等が利用可能な、保存可能資源の残量については、随時提供できる措置を講じる。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデー	・ISO 27001 2013, 附属書 A.17.2,12.3

						タセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
390	3.技術的対策	3.21.バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-3	医療機関等が医療情報システム等を利用する際に、利用可能な資源に係る情報（保存可能容量、利用可能期間、リスク、バックアップ頻度、バックアップ方法等）について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
391	3.技術的対策	3.21.バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-4	医療情報システム等が情報を保存する場所（内部、可搬媒体）、その場所ごとの保存可能容量、保存可能期間、リスク等を運用管理規程等に含める。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。	・ISO 27001 2013, 附属書 A.17.2,12.3

						冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
392	3.技術的対策	3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-5	①-4において、他の事業者が提供する医療情報システム等を利用する場合においても、同様の情報を収集して、対応する。仮想化技術による医療情報システム等を利用する場合には、受託事業者が他の事業者との契約上利用可能な資源に関する情報を確認する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
393	3.技術的対策	3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-6	①-4により運用管理規程に定める管理方法に関する教育を従業員等に対して行う。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内	・ISO 27001 2013, 附属書 A.17.2,12.3

						でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
394	3.技術的対策	3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-7	医療情報システム等に係る委託先に対しても、①-4の運用管理規程に定める管理方法への対応等を求める。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
395	3.技術的対策	3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-8	情報が毀損した場合、速やかに回復するための措置を講じ、その内容･手順等について、運用管理規程等に含める。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3

396	3.技術的対策	3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-9	①-8に示す措置によっても毀損された情報の回復が困難となる場合を想定した対応について、運用管理規程等に含める。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
397	3.技術的対策	3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-10	①-9で示す場合の、毀損した情報に関する責任の範囲、免責条件等について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
398	3.技術的対策	3.21. バックアップ及	①バックアップやリストア	①-11	リスク分析結果に基づき医療情報システム等のバックアップを取得する。バックアップの取得対象、取得頻度、保存方法･媒体、管理方法等を定め、その内容を運用管理規程等に含める。	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。	・ISO 27001 2013, 附属書 A.17.2,12.3

		びリストアの管理	等の情報の管理			Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
399	3.技術的対策	3.21. バックアップ及びリストアの管理	①バックアップやリストア等の情報の管理	①-12	取得するバックアップについて、その記録媒体の管理方法に応じて必要な定期的な検査等をおこない、記録内容の改竄･破壊等がないことを確認する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
400	3.技術的対策	3.21. バックアップ及びリストアの管理	②バックアップに用いる記録媒体の管理	②-1	記録媒体に格納するバックアップについては、その媒体の特性（テープ／ディスクの容量等）を踏まえたバックアップ内容、使用開始日、使用終了日を明らかにして管理する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセン	・ISO 27001 2013, 附属書 A.17.2,12.3

						ター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
401	3.技術的対策	3.21.バックアップ及びリストアの管理	②バックアップに用いる記録媒体の管理	②-2	バックアップの記録媒体の使用終了日が近づいた場合には、終了日以前に、別の媒体等にその内容を複写する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
402	3.技術的対策	3.21.バックアップ及びリストアの管理	②バックアップに用いる記録媒体の管理	②-3	製造者の定める有効利用限度期間を超過することがないよう、電子媒体の有効利用限度期間が近づいた場合は、別の媒体等に複写する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的に	・ISO 27001 2013, 附属書 A.17.2,12.3

						データが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
403	3.技術的対策	3.21. バックアップ及びリストアの管理	②バックアップに用いる記録媒体の管理	②-4	②-1～②-3の手順を運用管理規程等に含め、従業員等及び再委託業者に対して必要な教育を行う。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、データファイル管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべての権利と責任を保有します。	・ISO 27001 2013, 附属書 A.17.2,12.3
404	3.技術的対策	3.21. バックアップ及びリストアの管理	②バックアップに用いる記録媒体の管理	②-5	バックアップに係る情報の提供について、医療機関等と合意する。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や Google Workspace のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。Google Cloud プロダクト（Google Workspace、Google Cloud ）では、RPO（目標復旧時点）の目標も、RTO（目	・ISO 27001 2013, 附属書 A.17.2,12.3

						標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブレプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud のお客様は、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。	
405	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-1	診療録等のデータ項目で、厚生労働省における保健医療情報分野の標準規格（以下、「厚生労働省標準規格」という。）が定められているものについては、それを採用する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
406	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-2	厚生労働省標準規格が定められていないデータ項目については、変換が容易なデータ形式とし、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
407	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-3	医療情報に係るマスターテーブルの変更に際して、レコードの管理方法やとるべき措置等について、診療録等の情報に変更が生じない機能及び検証方法を医療情報システム等に備える。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
408	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-4	①-3に示す機能等を備えることが困難な場合の医療情報システム等更新･移行の手順について、医療機関等と合意する。	本項目は、Google Cloud のお客様の責任範囲で実施いただくものであり、対象外です。	-
409	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-5	医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートする。	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）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。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。	・ISO 27001 2013, 附属書 A.12.1
410	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-6	データ形式や転送プロトコルをバージョンアップ又は変更しようとする場合には、サービスの利用に与える影響を確認する。	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）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。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。	・ISO 27001 2013, 附属書 A.12.1
411	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-7	①-6の結果、サービスの利用に影響があると認められる場合には、医療機関等が対応を図るために十分な期間を想定してバージョンアップ又は変更に係る告知を行うほか、対応に必要な措置に関する具体的な情報提供を行う。	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）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。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。	・ISO 27001 2013, 附属書 A.12.1

412	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-8	①-7は、他の医療情報システム等とのデータ連携等を考慮して行う。医療機関等に対する互換性確保に係る情報提供について、医療機関等と合意する。	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）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。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。	・ISO 27001 2013, 附属書 A.12.1
413	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-9	データ形式･転送プロトコルの変更等の結果、医療機関等がサービスの利用を終了する場合には、見読性確保の対策を講じる。	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）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。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。	・ISO 27001 2013, 附属書 A.12.1
414	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-10	医療情報システム等に関する機器及びソフトウェアについては、将来的な互換性確保を視野に入れて決定するとともに、サービス提供後に標準仕様等の変更が生じた場合のリスクについても検討を行う。	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。 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。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。	・ISO 27001 2013, 附属書 A.9.1.2,13.1
415	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-11	他の事業者が提供する医療情報システム等を用いて、サービスを提供する場合には、他の事業者がサービスを停止した際にも、自社のサービス提供に支障が生じないようにするための対応策を検討し、対策を講じる。なお、他の事業者のサービスの停止･変更に伴い、自社が提供するサービスの一部又は全部の停止、変更（軽微なバージョンアップは含まない）等が生じる場合には、機器の劣化対策を講じる。	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。 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。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。	・ISO 27001 2013, 附属書 A.9.1.2,13.1
416	3.技術的対策	3.22. システム更改に備えた互換性確保	①データ形式・プロトコルの互換性の確保	①-12	医療情報システム等に係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他の事業者のサービスの変更を行う場合には、①-10、①-11を考慮して行う。	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。 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。 セキュリティ、可用性、処理の整合性、または機密性に影響を与える可能性のあるシステムの変更は、影響を受ける管理者およびユーザーに伝達されます。	・ISO 27001 2013, 附属書 A.9.1.2,13.1