厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.1-01	6	6.1	個人情報保護に関する方針を策定し、公開していること。	最低限	N/A
6.1-02			個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。その方針には、少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。	最低限	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。
6.2-01		6.2	情報システムで扱う情報をすべてリストアップしていること。	最低限	N/A
6.2-02			リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持していること。	最低限	N/A
6.2-03			このリストは情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理していること。	最低限	N/A
6.2-04			リストアップした情報に対してリスク分析を実施していること。	最低限	N/A
6.2-05			この分析により得られた脅威に対して、6.3 章～6.12 章に示す対策を行っていること。	最低限	N/A
6.2-06			上記の結果を文書化して管理していること。	推奨	N/A
6.3-01		6.3	情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。	最低限	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ ISO27002 2013、附属書 A.6）が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud 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。
6.3-02			個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。	最低限	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
6.3-03			情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた　Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査　記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート　サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。
6.3-04			個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.3-05			運用管理規程等において次の内容を定めること。 (a) 理念（基本方針と管理目的の表明）	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書　A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.3-06			(b) 医療機関等の体制	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書　A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.3-07			(c) 契約書・マニュアル等の文書の管理	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書　A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.3-08			(d) リスクに対する予防、発生時の対応の方法	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書　A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.3-09			(e) 機器を用いる場合は機器の管理	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書　A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.3-10			(f) 個人情報の記録媒体の管理（保管・授受等）の方法	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書　A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.3-11			(g) 患者等への説明と同意を得る方法	最低限	N/A

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.3-12			(h) 監査	最低限	Google はお客様の監査権に関する責務を負っています。 GCP のデータ処理とセキュリティ条項 (DPST) 7.5.2、および、G Suiteのデータ処理修正条項 (DPA) 7.5.2 をご覧ください。
6.3-13			(i) 苦情・質問の受付窓口	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書　A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.4-01		6.4	個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。	最低限	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
6.4-02			個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。 ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。	最低限	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"
6.4-03			個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・入退者の記録を定期的にチェックし、妥当性を確認する。	最低限	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"
6.4-04			個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。	最低限	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
6.4-05			覗き見防止の対策を実施すること。	最低限	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
6.4-06			防犯カメラ、自動侵入監視装置等を設置すること。	推奨	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"
6.5-01		6.5	情報システムへのアクセスにおける利用者の識別と認証を行うこと。	最低限	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。

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.5-02			本人の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。	最低限	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。
6.5-03			本人の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合には、IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。	最低限	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。 顧客データへのユーザーアクセスと内部アクセスの両方が、ユニークなユーザー　ID の使用によって制限されています。機密性の高いシステムやアプリケーションへのアクセスには、ユニークなユーザー　ID 、強力なパスワード、ワンタイムパスワード（OTP）、セキュリティキー、および /または証明書の形式での 2 要素認証が必要です。
6.5-04			入力者が端末から長時間、離席する際に、正当な入力者以外の者による入力の恐れがある場合には、クリアスクリーン等の防止策を講じること。	最低限	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
6.5-05			動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。	最低限	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。
6.5-06			医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行うよう、運用管理規程で定めていること。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことで担保する必要がある。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査　記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート　サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
6.5-07			アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した患者が特定できること。 情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容等）を必ず行うこと。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート　サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
6.5-08			アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート　サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
6.5-09			アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。	最低限	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 はすべての内部のシステムクロックを原子時計と　GPS に同期させ、独自の NTP サービスを実行しています。 Google は公共 NTPサービス https://developers.google.com/time を通してお客様が利用できるようにしています。
6.5-10			システム構築時、適切に管理されていないメディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行うこと。	最低限	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。

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.5-11			パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 (1) システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。また、利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者がパスワードを忘れたり、盗用されたりするおそれがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）し、本人以外が知り得ない方法で再登録を実施すること。 (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること（設定ファイルにパスワードが記載される等があってはならない）。 また、利用者は以下の事項に留意すること。 (1) パスワードは定期的に変更し（最長でも 2 ヶ月以内※D.5 に規定する 2 要素認証を採用している場合を除く。）、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。 (2) 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。	最低限	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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
6.5-12			無線LAN を利用する場合 システム管理者は以下の事項に留意すること。 (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策をとること。 (2) 不正アクセスの対策を施すこと。少なくとも SSID やMAC アドレスによるアクセス制限を行うこと。 (3) 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。 (4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。 (5) 無線LAN の適用に関しては、総務省発行の「安心して無線LAN を利用するために」を参考にすること。	最低限	N/A
6.5-13			13. IoT 機器を利用する場合 システム管理者は以下の事項に留意すること。 (1) IoT 機器により患者情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2) セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置の IoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。 (3) IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用すること。 (4) 使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を講じること。	最低限	N/A
6.5-14			情報の区分管理を実施し、区分単位でアクセス管理を実施すること。	推奨	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。 Google はまた、Google のデータ分類ガイドラインに従って情報のラベル付けと取り扱いの手順を確立するために、データセキュリティポリシー、データ分類ガイドライン、および Google の情報のセキュリティラベルを開発しました。方針および手順は必要に応じて見直され、更新されます。
6.5-15			離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等）。	推奨	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
6.5-16			外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクションやそれと同等の機能を含む）を設置し、ACL(アクセス制御リスト)等を適切に設定すること。	推奨	Google は ISO27001 認証を受けています。この基準では、「ネットワーク管理策」（ ISO 27001 2013、附属書 A.13.1.1）が規定されています。 論理的および物理的なアクセス制御に関連する一般的な基準は、 GoogleのSOC 2 Type IIレポートについて第三者の監査人によってレビューおよび検証されています。 Google は、外部からの攻撃対象を保護するために複数層のネットワークデバイスを使用しています。 Google は、潜在的な攻撃方法を検討し、その境界に適切な防衛策を取り入れています。 ネットワーク ACL は、必要に応じて、意図的にコメントを付けて構成ファイル内に文書化されています。
6.5-17			パスワードを利用者識別に使用する場合以下の基準を遵守すること。 （1）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不応時間を設定すること。 （2）パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。	推奨	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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
6.5-18			認証に用いられる手段としては、ID・パスワード＋バイオメトリクス又はIC カード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように 2 つの独立した要素を用いて行う方式（ 2 要素認証）等、より認証強度が高い方式を採用すること。ただし、情報システムを利用する端末に 2 要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め 2 要素以上（記憶・生体計測・物理媒体のいずれか 2 つ以上）の認証がなされていれば、2 要素認証と同等と考えてよい。	推奨	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。 顧客データへのユーザーアクセスと内部アクセスの両方が、ユニークなユーザー ID の使用によって制限されています。機密性の高いシステムやアプリケーションへのアクセスには、ユニークなユーザー ID 、強力なパスワード、ワンタイムパスワード（OTP）、セキュリティキー、および /または証明書の形式での 2 要素認証が必要です。
6.5-19			無線LAN のアクセスポイントを複数設置して運用する場合等は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば 802.1x や電子証明書を組み合わせたセキュリティ強化をすること。	推奨	N/A
6.5-20			IoT 機器を含むシステムの接続状況や異常発生を把握するため、IoT 機器・システムがそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。	推奨	N/A

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.6-01		6.6	（1）従業者に対する人的安全管理措置 医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。 1. 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。	最低限	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。
6.6-02			2. 定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。	最低限	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で　Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ　チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
6.6-03			3. 従業者の退職後の個人情報保護規程を定めること。	最低限	Google は ISO27001 認証を受けています。この基準では、「雇用の終了および変更」（ ISO 27001 2013、附属書 A.7.3）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。 本番マシン、サポートツール、ネットワークデバイス、および企業資産へのアクセスは、適切な　Googl 社員による終了要求の実行時にタイムリーに自動的に削除されます。
6.6-04			サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。	推奨	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"
6.6-05			医療機関等の事務、運用等を外部の事業者に委託する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。 ① 受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結すること	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.6-06			② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。　Google 社員に付与される既定のアクセス権限は、社員用メールや　Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。　Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
6.6-07			③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。	最低限	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"
6.6-08			④ 委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。	最低限	Google は ISO27001 認証を受けています。この基準では、「供給者関係」（ ISO 27001 2013、附属書 A.15）が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、 Google は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ　サプライヤーを利用するこ とがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。 Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
6.6-09			プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。	推奨	Google は ISO27001 認証を受けています。この基準では、「供給者関係」（ ISO 27001 2013、附属書 A.15）が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleは、コンプライアンスを確認するために、必要に応じて、 Googleのセキュリティポリシーおよびオンサイト検査を遵守するための契約上の要件を含むベンダー管理プロセスを採用しています。

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.7-01		6.7	「6.1 方針の制定と公表」で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者の特定、具体的な破棄の方法を含めること。	最低限	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
6.7-02			情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
6.7-03			外部保存を受託する機関に破棄を委託した場合は、「 6.6 人的安全対策（2）事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
6.7-04			運用管理規程において下記の内容を定めること。 (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成	最低限	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。
6.8-01		6.8	動作確認で個人情報を含むデータを使用するときは、明確な守秘義務の設定を行うとともに、終了後は確実にデータを消去する等の処理を行うことを求めること。	最低限	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。
6.8-02			メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。　Google 社員に付与される既定のアクセス権限は、社員用メールや　Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、　Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、　Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。　Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
6.8-03			そのアカウント情報は外部流出等による不正使用の防止の観点から適切に管理することを求めること。	最低限	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 は、必要性と職務に基づいてアクセスを制限しています。　Google は自動ログ収集および分析ツールを運用しています。 アカウントのロック、証明書の失効、および役割の割り当てを含む自動アクセス失効プロセスがあります。
6.8-04			保守要員の離職や担当変え等に対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付けまた、それに応じるアカウント管理体制を整えておくこと。	最低限	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 は、必要性と職務に基づいてアクセスを制限しています。　Google は自動ログ収集および分析ツールを運用しています。 アカウントのロック、証明書の失効、および役割の割り当てを含む自動アクセス失効プロセスがあります。
6.8-05			保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「供給者関係」（ ISO 27001 2013、附属書 A.15）が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Googleは、コンプライアンスを確認するために、必要に応じて、 Googleのセキュリティポリシーおよびオンサイト検査を遵守するための契約上の要件を含むベンダー管理プロセスを採用しています。
6.8-06			保守会社と守秘義務契約を締結し、これを遵守させること。	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.8-07			保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。	最低限	Googleは、データセンターへの物理的なアクセスを許可するための正式なアクセス手順を運用しています。 データセンターは、電子カードのキーアクセスを必要とする施設に収容されています。警報はオンサイトのセキュリティオペレーションにリンクされています。データセンターへ入場するすべての者は、自分自身を特定するだけでなく、オンサイトの警備員に身元証明を提示する必要があります。認定された従業員、請負業者、および訪問者のみがデータセンターへの入場を許可されています。許可された従業員および請負業者のみがこれらの施設への電子カードによるアクセスを要求することができます（その後に適切な承認プロセスが続きます）。 データセンターの電子カードのキーアクセス要求は電子メールで行う必要があり、要求者の管理者とデータセンターの管理者の承認が必要です。データセンターへの一時的なアクセスを必要とする他のすべての参加者は、(i) データセンターの管理者から、訪問を希望する特定のデータセンターおよび内部エリアについて事前に承認を得ます。(ii)オンサイト警備にて署名をし、(iii)承認済みデータセンターアクセスレコードを参照し個人を特定します。
6.8-08			リモートメンテナンスによるシステムの改造や保守が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに作業内容を医療機関等の責任者が確認すること。	最低限	Google は、さまざまなソースからログ情報を収集して関連付ける自動ログ収集および分析ツールを運用しています。
6.8-09			再委託が行われる場合は、再委託する事業者にも保守会社の責任で同等の義務を課すこと。	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.8-10			詳細なオペレーション記録を保守操作ログとして記録すること。	推奨	Google は、さまざまなソースからログ情報を収集して関連付ける自動ログ収集および分析ツールを運用しています。
6.8-11			保守作業時には医療機関等の関係者立会いのもとで行うこと。	推奨	Googleは強力なベンダー管理プログラムを運用しています。 Googleと提携しているベンダーは、関連するすべての情報セキュリティとプライバシーポリシーを遵守する必要があります。 コンプライアンスを判断するために、ベンダー監査プログラムが実施されています。
6.8-12			作業員各人と保守会社との守秘義務契約を求めること。	推奨	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.8-13			保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、詳細な作業記録を残すことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。	推奨	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」（ ISO 27001 2013、附属書 A.12.7）が規定されています。 情報セキュリティ 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、データセンターへの物理的なアクセスを許可するための正式なアクセス手順を運用しています。 データセンターは、電子カードのキーアクセスを必要とする施設に収容されています。警報はオンサイトのセキュリティオペレーションにリンクされています。データセンターへ入場するのすべての者は、自分自身を特定するだけでなく、オンサイトの警備員に身元証明を提示する必要があります。認定された従業員、請負業者、および訪問者のみがデータセンターへの入場を許可されています。許可された従業員および請負業者のみがこれらの施設への電子カードによるアクセスを要求することができます（その後に適切な承認プロセスが続きます）。データセンターの電子カードのキーアクセス要求は電子メールで行う必要があり、要求者の管理者とデータセンターの管理者の承認が必要です。データセンターへの一時的なアクセスを必要とする他のすべての参加者は、(i)データセンターの管理者から、訪問を希望する特定のデータセンターおよび内部エリアについて事前に承認を得ます。(ii)オンサイト警備にて署名をし、(iii)承認済みデータセンターアクセスレコードを参照し個人を特定します。
6.8-14			保守作業に関わるログの確認手段として、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者に何回のアクセスが行われたかが確認できる仕組みが備わっていること。	推奨	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
6.9-01		6.9	組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.9-02			運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.9-03			情報を格納した可搬媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程に定めること。	最低限	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書 A.12.1.1）が規定されています。 Google では内部ドキュメンテーションを盤石に維持し、 ISO27001 の要件に従って ISMS を運用しています。文書はすべて、複製とバックアップの対象になるシステムに保存されます。 Google Cloud 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。
6.9-04			運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。	最低限	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
6.9-05			医療機関等や情報の管理者は、情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握すること。	最低限	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。
6.9-06			情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けたり、定期的にパスワードを変更する等の措置を行うこと。	最低限	N/A
6.9-07			盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、容易に内容を読み取られないようにすること。	最低限	N/A
6.9-08			持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「 6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線LAN を利用できる場合があるが、公衆無線 LAN は6.5 章C-11 の基準を満たさないことがあるため、利用できない。ただし、公衆無線 LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は 6.11 章で述べている基準を満たした通信手段を選択すること。	最低限	N/A
6.9-09			持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除あるいは停止するか、業務に対して影響がないことを確認して用いること。	最低限	N/A
6.9-10			個人保有の情報機器（パソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、管理者は 1～5 の対策を行うとともに、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。	最低限	N/A

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.9-11			外部での情報機器の覗き見による情報の露見を避けるため、ディスプレイに覗き見防止フィルタ等を張ること。	推奨	N/A
6.9-12			情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。	推奨	N/A
6.9-13			情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。	推奨	N/A
6.9-14			スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。 ・BYODは原則として行わず、機器の設定の変更は管理者のみが可能とすること。 ・紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者情報にアクセスできる場合は、一定回数パスワード入力を誤った場合は端末を初期化する等の対策を行うこと。	推奨	N/A
6.10-01		6.10	医療サービスを提供し続けるための BCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。	最低限	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」（ ISO 27001 2013、附属書 A.17.1）が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内 DR プログラムを確立しています。 Google Cloud 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。
6.10-02			正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」（ ISO 27001 2013、附属書 A.17.1）が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内 DR プログラムを確立しています。 Google Cloud 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。
6.10-03			非常時の情報システムの運用 ・「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。 ・非常時機能が定常時に不適切に利用されることがないようにし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理及び監査をすること。 ・非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。 ・標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、関係先への連絡手段や紙での運用等の代替手段を準備すること。	最低限	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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
6.10-04			サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、 “非常時”と判断した上で所管官庁への連絡を行うこと。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。 連絡先 厚生労働省 医政局研究開発振興課医療技術情報推進室（03-3595-2430） ※独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、マルウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Web サイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先 情報処理推進機構 情報セキュリティ安心相談窓口（ 03-5978-7509）	最低限	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。
6.11-01		6.11	ネットワーク経路でのメッセージ挿入、ウイルス混入等の改ざんを防止する対策を行うこと。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を行うこと。 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策を行うこと。 上記を満たす対策として、例えば IPsec とIKE を利用することによりセキュアな通信路を確保することが挙げられる。 チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。	最低限	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。
6.11-02			データ送信元と送信先での、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、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。認証手段としては PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等の容易に解読されない方法を用いるのが望ましい。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
6.11-03			施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を行うこと。これに関しては、「 6.5技術的安全対策」で包括的に述べているので、それを参照すること。	最低限	N/A

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.11-04			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し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。	最低限	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」（ISO 27001 2013、附属書 A.9.1.2）「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には、ネットワークの監視、維持、管理、保護を担当する専門チームがいます。　企業のワイヤレスネットワークへの接続は暗号化されています。
6.11-05			送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。たとえば、 SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。	最低限	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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。 鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
6.11-06			医療機関等の間の情報通信には、医療機関等だけでなく、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。 そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。 ・診療情報等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通または著しい遅延の場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・伝送情報の暗号化に不具合があった場合の対処 ・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・障害が起こった場合に障害部位を切り分ける責任 ・送信元の医療機関等または送信先の医療機関等が情報交換を中止する場合の対処 また、医療機関内においても次の事項において契約や運用管理規程等で定めておくこと。 ・通信機器、暗号化装置、認証装置等の管理責任の明確化。外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結。 ・患者等に対する説明責任の明確化。 ・事故発生時における復旧作業・他施設やベンダとの連絡に当たる専任の管理者の設置。 ・交換した医療情報等に対する管理責任及び事後責任の明確化。 個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項。	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
6.11-07			リモートメンテナンスを実施する場合は、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を行って不必要なログインを防止すること。 また、メンテナンス自体は「 6.8 情報システムの改造と保守」を参照すること。	最低限	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」（ISO 27001 2013、附属書 A.9.1.2）「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には、ネットワークの監視、維持、管理、保護を担当する専門チームがいます。　企業のワイヤレスネットワークへの接続は暗号化されています。
6.11-08			回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認すること。 また上記 1 及び 4 を満たしていることを確認すること。	最低限	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。
6.11-09			患者に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、システムやアプリケーションを切り分けし、ファイアウォール、アクセス監視、通信の TLS暗号化、PKI 個人認証等の技術を用いた対策を実施すること。 また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、IT に係る以外の法的根拠等も含めた幅広い対策を立て、それぞれの責任を明確にすること。	最低限	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」（ISO 27001 2013、附属書 A.9.1.2）「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、転送中、および保管中に暗号化されます。
6.11-10			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、IPsec を用いた VPN 接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLS のプロトコルバージョンを TLS1.2 のみに限定した上で、クライアント証明書を利用した TLS クライアント認証を実施すること。その際、 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水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。また、ソフトウェア型の IPsec 若しくは 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）等による攻撃からの防護について、適切な対策を実施すること。	最低限	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。
6.11-11			やむを得ず、従業者による外部からのアクセスを許可する場合は、PC の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに運用等の要件を設定すること。	推奨	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」（ISO 27001 2013、附属書 A.9.1.2）「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 は本番環境と企業環境を適切なネットワーク境界管理で分離しています。
6.12-01		6.12	（1）厚生労働省の定める準拠性監査基準を満たす健医療福祉分野PKI 認証局若しくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと 1. 保健医療福祉分野 PKI 認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。従ってこの保健医療福祉分野 PKI 認証局の発行する電子署名を活用することが推奨される。ただし、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできることが必要である。	最低限	N/A
6.12-02			2. 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくてもAの要件を満たすことは可能であるが、同等の厳密さで本人確認を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。	最低限	N/A
6.12-03			3.「電子署名に係る地方公共団体の認証業務に関する法律」（平成 14 年法律第 153号）に基づき、平成 16 年 1 月 29 日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者がすべて公的個人認証サービスを用いた電子署名を検証できることが必要である。	最低限	N/A
6.12-04			（2）電子署名を含む文書全体にタイムスタンプを付与すること。 1. タイムスタンプは、「タイムビジネスに係る指針ーネットワークの安心な利用と電子データの安全な長期保存のためにー」（総務省、平成 16 年 11 月）等で示されている時刻認証業務の基準に準拠し、財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能であること。	最低限	N/A
6.12-05			2. 法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。	最低限	N/A
6.12-06			3. タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を講じる必要がある。	最低限	N/A

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
6.12-07			（3）上記タイムスタンプを付与する時点で有効な電子証明書を用いること。 1. 当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。 本来法的な保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば、電子署名を含めて改変の事実がないことが証明されるために、タイムスタンプ付与時点で、電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。	最低限	N/A
7.1-01	7	7.1	【医療機関等に保存する場合】 （1）入力者及び確定者の識別及び認証 a. 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合 1. 入力者及び確定者を正しく識別し、認証を行うこと。	最低限	Cloud Identity & Access Management (Cloud IAM) を使用すると、管理者は特定のリソースに対してアクションを実行できるユーザーを承認し、クラウドリソースを一元管理するための完全な制御と可視性を得ることができます。複雑な組織構造、数百のワークグループ、そしてさらに多くのプロジェクトを抱える確立された企業のために、Cloud IAM は、コンプライアンスプロセスを容易にするためのビルトイン監査により、組織全体のセキュリティポリシーへの統一ビューを提供します。 IAM アクセスポリシーは、ユーザーおよびグループのきめ細かい制御を使用して、または ACL を使用してプロジェクトレベルで定義されます。
7.1-02			2. システムへの全ての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定めること。また、権限のある入力者以外による作成、追記、変更を防止すること。	最低限	Cloud Identity & Access Management (Cloud IAM) を使用すると、管理者は特定のリソースに対してアクションを実行できるユーザーを承認し、クラウドリソースを一元管理するための完全な制御と可視性を得ることができます。複雑な組織構造、数百のワークグループ、そしてさらに多くのプロジェクトを抱える確立された企業のために、Cloud IAM は、コンプライアンスプロセスを容易にするためのビルトイン監査により、組織全体のセキュリティポリシーへの統一ビューを提供します。 IAM アクセスポリシーは、ユーザーおよびグループのきめ細かい制御を使用して、または ACL を使用してプロジェクトレベルで定義されます。
7.1-03			3. 業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること。	最低限	Cloud Identity & Access Management (Cloud IAM) を使用すると、管理者は特定のリソースに対してアクションを実行できるユーザーを承認し、クラウドリソースを一元管理するための完全な制御と可視性を得ることができます。複雑な組織構造、数百のワークグループ、そしてさらに多くのプロジェクトを抱える確立された企業のために、Cloud IAM は、コンプライアンスプロセスを容易にするためのビルトイン監査により、組織全体のセキュリティポリシーへの統一ビューを提供します。 IAM アクセスポリシーは、ユーザーおよびグループのきめ細かい制御を使用して、または ACL を使用してプロジェクトレベルで定義されます。
7.1-04			b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合 1. 装置の管理責任者や操作者が運用管理規程で明確にされ、装置の管理責任者、操作者以外による機器の操作が運用上防止されていること。	最低限	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
7.1-05			2. 当該装置による記録は、いつ・誰が行ったかがシステム機能と運用の組み合わせにより明確になっていること。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
7.1-06			（2）記録の確定手順の確立と、作成責任者の識別情報の記録 a. 電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合 1. 診療録等の作成・保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。その際、作成責任者の氏名等の識別情報、信頼できる時刻源を用いた作成日時が含まれること。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
7.1-07			2.「記録の確定」を行うにあたり、作成責任者による内容の十分な確認が実施できるようにすること。	最低限	N/A
7.1-08			3.「記録の確定」は、確定を実施できる権限を持った確定者が実施すること。	最低限	N/A
7.1-09			4. 確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。	最低限	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
7.1-10			5. 一定時間後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを策定し運用管理規程に明記すること。	最低限	N/A
7.1-11			6. 確定者が何らかの理由で確定操作ができない場合、例えば医療機関等の管理責任者が記録の確定を実施する等のルールを運用管理規程で定め、記録の確定の責任の所在を明確にすること。	最低限	N/A

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
7.1-12			b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合 1. 運用管理規程等に当該装置により作成された記録の確定ルールが定義されていること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時が記録に含まれること。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
7.1-13			2. 確定された記録が、故意による虚偽入力、書き換え、消去及び混同されることの防止対策を講じておくこと及び原状回復のための手順を検討しておくこと。	最低限	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
7.1-14			（3）更新履歴の保存 1. 一旦確定した診療録等を更新した場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合せることができること。	最低限	Google は、さまざまなソースからログ情報を収集して関連付ける自動ログ収集および分析ツールを運用しています。
7.1-15			2. 同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること。	最低限	不正なアカウントが使用される可能性を最小限に抑えるために、 Google はアクセスリストを慎重に監視しています。 Google は定期的にアクセスリストを確認し、不要になったアクセスを削除します。すべてのアカウントアクションが記録されています。
7.1-16			（4）代行入力の承認機能 1. 代行入力を実施する場合、具体的にどの業務等に適用するか、また誰が誰を代行してよいかを運用管理規程で定めること。	最低限	N/A
7.1-17			2. 代行入力が行われた場合には、誰の代行が誰によっていつ行われたかの管理情報が、その代行入力の都度記録されること。	最低限	Cloud Identity & Access Management (Cloud IAM) を使用すると、管理者は特定のリソースに対してアクションを実行できるユーザーを承認し、クラウドリソースを一元管理するための完全な制御と可視性を得ることができます。複雑な組織構造、数百のワークグループ、そしてさらに多くのプロジェクトを抱える確立された企業のために、Cloud IAM は、コンプライアンスプロセスを容易にするためのビルトイン監査により、組織全体のセキュリティポリシーへの統一ビューを提供します。 IAM アクセスポリシーは、ユーザーおよびグループのきめ細かい制御を使用して、または ACL を使用してプロジェクトレベルで定義されます。
7.1-18			3. 代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認）」が行われること。この際、内容の確認を行わずに確定操作を行ってはならない。	最低限	N/A
7.1-19			（5）機器・ソフトウェアの品質管理 1. システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかが明らかにされており、システムの仕様が明確に定義されていること。	最低限	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。
7.1-20			2. 機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスが規定されていること。	最低限	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。
7.1-21			3. 機器、ソフトウェアの品質管理に関する作業内容を運用管理規程に盛り込み、従業者等への教育を実施すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で　Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ　チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
7.1-22			4. 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を定期的に実施すること。	最低限	Google は業界のベストプラクティスと規制要件に準拠した内部監査プログラムを運用しています。　Google の社内監査チームは、機能横断的な評価監査など、 Google のさまざまな分野と運用面をカバーしています。
7.1-23			【ネットワークを通じて医療機関等の外部に保存する場合】 医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。 （1）通信の相手先が正当であることを認識するための相互認証を行うこと診療録等のオンライン外部保存を受託する機関と委託する医療機関等が、お互いに通信目的とする正当な相手かどうかを認識するための相互認証機能が必要である。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
7.1-24			(2) ネットワーク上で「改ざん」されていないことを保証すること ネットワークの転送途中で診療録等が改ざんされていないことを保証できること。 なお、可逆的な情報の圧縮・解凍並びにセキュリティ確保のためのタグ付けや暗号化・平文化等は改ざんにはあたらない。	最低限	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。
7.1-25			(3) リモートログイン機能を制限すること 保守目的等のどうしても必要な場合を除き行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。 なお、これらの具体的要件については、「 6.11 外部と診療情報等を含む医療情報を交換する場合の安全管理」を参照すること。	最低限	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」（ISO 27001 2013、附属書 A.9.1.2）「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。 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。
7.2-01		7.2	(1) 情報の所在管理 紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者毎の情報の全ての所在が日常的に管理されていること。	最低限	N/A
7.2-02			(2) 見読化手段の管理 電子媒体に保存された全ての情報とそれらの見読化手段は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。	最低限	N/A
7.2-03			(3) 見読目的に応じた応答時間 目的に応じて速やかに検索表示もしくは書面に表示できること。	最低限	N/A
7.2-04			(4) システム障害対策としての冗長性の確保 システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするために、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」（ ISO 27001 2013、附属書 A.17.1）が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内 DR プログラムを確立しています。 Google Cloud 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。
7.2-05			【医療機関等に保存する場合】 (1) バックアップサーバ システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。	推奨	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
7.2-06			(2) 見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力することができること。	推奨	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
7.2-07			(3) 遠隔地のデータバックアップを使用した見読機能 大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップし、そのバックアップデータと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読することができること。	推奨	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。
7.2-08			【ネットワークを通じて外部に保存する場合】 医療機関等に保存する場合の推奨されるガイドラインに加え、次の事項が必要となる。 (1) 緊急に必要になることが予測される診療録等の見読性の確保 緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。	推奨	N/A

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
7.2-09			（2）緊急に必要になるとまではいえない診療録等の見読性の確保 緊急に必要になるとまではいえない情報についても、ネットワークや外部保存を受託する機関の障害等に対応できるような措置を行っておくこと。	推奨	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
7.3-01		7.3	【医療機関等に保存する場合】 （1）ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止 1. いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行うこと。	最低限	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。
7.3-02			（2）不適切な保管・取扱いによる情報の滅失、破壊の防止 1. 記録媒体及び記録機器の保管及び取扱いについては運用管理規程を作成し、適切な保管及び取扱いを行うように関係者に教育を行い、周知徹底すること。また、保管及び取扱いに関する作業履歴を残すこと。	最低限	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。
7.3-03			2. システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能用量（サイズ、期間）、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明示すること。これらを運用管理規程としてまとめて、その運用を関係者全員に周知徹底すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
7.3-04			3. 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を施すこと。	最低限	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"
7.3-05			4. 電子的に保存された診療録等の情報に対するアクセス履歴を残し、管理すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
7.3-06			5. 各保存場所における情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわれた範囲が容易に分かるようにしておくこと。	最低限	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
7.3-07			（3）記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止 1. 記録媒体が劣化する以前に情報を新たな記録媒体又は記録機器に複写すること。記録する媒体及び機器ごとに劣化が起こらずに正常に保存が行える期間を明確にして、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体又は記録機器については、その データを新しい記録媒体又は記録機器に複写すること。これらの一連の運用の流れを運用管理規程にまとめて記載し、関係者に周知徹底すること。	最低限	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
7.3-08			（4）媒体・機器・ソフトウェアの不整合による情報の復元不能の防止 1. システム更新の際の移行を迅速に行えるように、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること。	最低限	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。
7.3-09			2. マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えていること。	最低限	Google は ISO27001 認証を受けています。この基準では、「ロギングとモニタリング」（ ISO 27001 2013、附属書 A.12.4）が規定されています。 システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。
7.3-10			【ネットワークを通じて医療機関等の外部に保存する場合】 医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。 （1）データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと 保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する機関は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持しなくてはならない。	最低限	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。
7.3-11			（2）ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。	最低限	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
7.3-12			【医療機関等に保存する場合】 （1）不適切な保管・取扱いによる情報の滅失、破壊の防止 1. 記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。	推奨	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"
7.3-13			2. サーバ室には、許可された者以外が入室できないように、鍵等の物理的な対策を施すこと。	推奨	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"
7.3-14			3. 診療録等のデータのバックアップを定期的に取得し、その内容に対して改ざん等による情報の破壊が行われていないことを検査する機能を備えること。	推奨	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。

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
7.3-15			(2) 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止 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は、RAID-1 若しくは RAID-6 相当以上のディスク障害に対する対策を行うこと。	推奨	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、Google Cloud や G Suite のお客様の業務が中断されることはありません。冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
7.3-16			【ネットワークを通じて医療機関等の外部に保存する場合】 (1) ネットワークや外部保存を受託する機関の設備の互換性を確保すること 1. 回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、記録された情報を読み出すことに支障が生じるおそれがある。従って、外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し、安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。	推奨	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。
8.1-01	8	8.1	① 病院、診療所、医療法人等が適切に管理する場所に保存する場合 (ア) 病院や診療所の内部で診療録等を保存すること。	最低限	N/A
8.1-02			(イ) 保存を受託した診療録等を委託した病院、診療所や患者の許可なく分析等を目的として取り扱わないこと。	最低限	N/A
8.1-03			(ウ) 病院、診療所等であっても、保存を受託した診療録等について分析等を行う場合は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を目的としない場合に限ること。	最低限	N/A
8.1-04			(エ) 匿名化された情報を取り扱う場合においても、匿名化の妥当性の検証を検証組織で検討することや、取り扱いをしている事実を患者等に掲示等を使って知らせる等、個人情報の保護に配慮した上で実施すること。	最低限	N/A
8.1-05			(オ) 情報を保存している機関に患者がアクセスし、自らの記録を閲覧するような仕組みを提供する場合は、情報の保存を受託した病院、診療所は適切なアクセス権を規定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。	最低限	N/A
8.1-06			(カ) 情報の提供は、原則、患者が受診している医療機関等と患者間の同意で実施されること。	最低限	N/A
8.1-07			② 行政機関等が開設したデータセンター等に保存する場合 (ア) 法律や条例により、保存業務に従事する個人もしくは従事していた個人に対して、個人情報の内容に係る守秘義務や不当使用等の禁止が規定され、当該規定違反により罰則が適用されること。	最低限	N/A
8.1-08			(イ) 適切な外部保存に必要な技術及び運用管理能力を有することを、システム監査技術者及び Certified Information Systems Auditor（ISACA 認定）等の適切な能力を持つ監査人の外部監査を受ける等、定期的に確認されていること。	最低限	N/A
8.1-09			(ウ) 医療機関等は保存された情報を、外部保存を受託する事業者が分析、解析等を実施しないことを確認し、実施させないことを明記した契約書等を取り交わすこと。	最低限	N/A
8.1-10			(エ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等が起こらないようにさせること。	最低限	N/A
8.1-11			③ 医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合 (ア) 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取り扱いに対して監督を行えること。	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-12			(イ) 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線の安全性に関しては「 6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること。	最低限	N/A
8.1-13			(ウ) 受託事業者が民間事業者等に課せられた経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省の「 ASP・SaaS における情報セキュリティ対策ガイドライン」及び「 ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」等を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。	最低限	Google は ISO27001 認証を受けています。この基準では、「供給者関係」（ ISO 27001 2013、附属書 A.15）が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、 Google は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ サプライヤーを利用するこ とがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。 Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
8.1-14			(エ) 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「 6.8 情報システムの改造と保守」を遵守すること。	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-15			(オ) 外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-16			(カ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等が起こらないようにさせること。	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

厚生労働省「医療情報システムの安全管理に関するガイドライン　第 5 版（平成 29 年 5 月）」					Google の回答
項目番号	章	節	ガイドライン	分類	
8.1-17			(キ) 医療機関等において(ア)から(カ)を満たした上で、外部保存を受託する事業者の選定基準を定めること。少なくとも以下の 4 点について確認すること。 (a) 医療情報等の安全管理に係る基本方針・取扱規程等の整備 (b) 医療情報等の安全管理に係る実施体制の整備 (c) 実績等に基づく個人データ安全管理に関する信用度 (d) 財務諸表等に基づく経営の健全性	最低限	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-18			(ア)「①病院、診療所、医療法人等が適切に管理する場所に保存する場合」のうち、医療法人等が適切に管理する場所に保管する場合、保存を受託した機関全体としてのより一層の自助努力を患者・国民に示す手段として、それぞれ個人情報保護及び情報セキュリティマネジメントの認定制度である、プライバシーマークやISMS 認定等の第三者による認定を取得すること。	推奨	N/A
8.1-19			(イ)「②行政機関等が開設したデータセンター等に保存する場合」においては、制度上の監視や評価等を受けることになるが、更なる評価の一環として、(ア)で述べた第三者による認定を受けること。	推奨	N/A
8.1-20			(ウ)「②行政機関等が開設したデータセンター等に保存する場合」及び「③医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合」では、技術的な方法としては、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保すること。	推奨	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
8.1-21			(エ) 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を併せ持つこと。	推奨	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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。 鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
8.2-01		8.2	(1)診療録等の外部保存委託先の事業者内における個人情報保護 ① 適切な委託先の監督を行うこと 診療録等の外部保存を受託する事業者内の個人情報保護については本ガイドライン 6 章を参照し、適切な管理を行う必要がある。	最低限	N/A
8.2-02			(2) 外部保存実施に関する患者への説明 診療録等の外部保存を委託する施設は、あらかじめ患者に対して、必要に応じて患者の個人情報が特定の外部の施設に送られ、保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。 ① 診療開始前の説明 患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始すること。	最低限	N/A
8.2-03			② 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合 意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明を行い、理解を得る必要がある。	最低限	N/A
8.2-04			③ 患者本人に説明することが困難であるが、診療上の緊急性が特にない場合 乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。 ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。	最低限	N/A
8.3-01		8.3			N/A
8.4-01		8.4	診療録等が機微な個人情報であるという観点から、外部保存を終了する場合には、医療機関等及び受託する事業者双方で一定の配慮をしなくてはならない。 診療録等の外部保存を委託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、外部保存を終了しなければならない診療録等は速やかに処理した上で、当該処理が厳正に執り行われたかを監査しなくてはならない。また、外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要がある。 これらの廃棄に関わる規定は、外部保存を開始する前に委託契約書等にも明記をしておく必要がある。また、実際の廃棄に備えて、事前に廃棄プログラム等の手順を明確化した規定を作成しておくべきである。 これらの厳正な取扱い事項を双方に求めるのは、同意した期間を超えて個人情報を保持すること自体が、個人情報の保護上問題になり得るためであり、そのことに十分に留意しなければならない。 ネットワークを通じて外部保存する場合は、外部保存システム自体も一種のデータベースであり、インデックスファイル等も含めて慎重に廃棄しなければならない。また電子媒体の場合は、バックアップファイルについても同様の配慮が必要である。 また、ネットワークを通じて外部保存している場合は、自ずと保存形式が電子媒体となるため、情報漏えい時の被害は、その情報量の点からも甚大な被害が予想される。従って、個人情報保護に十分な配慮を行い、確実に情報が廃棄されたことを、外部保存を委託する医療機関等と受託する事業者とが確実に確認できるようにしておかなくてはならない。 （厚労省ガイドラインでは「 B.考え方」の枠に記載されている内容だが、総務省ガイドラインでは要求事項として扱われているためここに記載）		Google は ISO27001 認証を受けています。この基準では、「媒体の処分」(ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する 際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」(情報処理 GL)				Google の回答
項目番号		区分 (推奨/最低限/その他)	ガイドライン	
7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定		推奨	(1) 認証取得あるいは更新の際に ISMS の安全管理策として、本ガイドライン「 7 医療情報を受託管理する情報処理事業者における安全管理上の要求事項」にて提示する安全管理策を盛り込むことが望ましい。	Google は ISO27001 認証を受けています。この基準では、「法的要件および契約要件の遵守」(ISO 27001 2013、附属書 A.18.1)が規定されています。 Googleは、セキュリティインフラストラクチャと運用モデルを詳しく説明した包括的な外部ドキュメントとホワイトペーパーを提供しています。Google は内部 ISMS も運用しており、その有効性の証拠は ISO 27001 認証を通じて提供されています。
		推奨	(2) 受託管理する医療情報の入り口から出口まで包括的にISMS の適用範囲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、「法的要件および契約要件の遵守」(ISO 27001 2013、附属書 A.18.1)が規定されています。 Googleは、セキュリティインフラストラクチャと運用モデルを詳しく説明した包括的な外部ドキュメントとホワイトペーパーを提供しています。Google は内部 ISMS も運用しており、その有効性の証拠は ISO 27001 認証を通じて提供されています。
		推奨	(3) 安全管理措置が適切に適用されていることを、医療機関等が委託先事業者を選定する際に確認できるよう、医療機関等の要請に応じて適用宣言書の閲覧を即座に行うことができるよう準備を行っておくことが望ましい(適用宣言書には医療情報を取り扱うために特別に配慮している管理策を明確にすること)。	Google は ISO27001 認証を受けています。この基準では、「法的要件および契約要件の遵守」(ISO 27001 2013、附属書 A.18.1)が規定されています。 Googleは、セキュリティインフラストラクチャと運用モデルを詳しく説明した包括的な外部ドキュメントとホワイトペーパーを提供しています。Google は内部 ISMS も運用しており、その有効性の証拠は ISO 27001 認証を通じて提供されています。
7.2 情報資産管理	7.2.1 資産台帳	推奨	(1) 資産台帳等を紙文書として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について検出・記録できるような仕組みを実装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。 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"
		推奨	(2) 資産台帳等に記録する情報には次のようなものが考えられる。 ・整理番号 ・資産の名称(医療情報の名称) ・資産の医療情報としての種別 ・データ形式及び見読化手段 ・資産の所在地と複製の可否及び複製の所在地 ・資産を保存する情報処理装置、電子媒体の識別番号等 ・資産を扱う医療機関等業務の概要 ・情報処理事業者における管理責任者 ・設定されたアクセス権限とアクセス権限者 ・資産の発生日時、保有する期限、廃棄予定日 ・資産に対する処理の履歴(保存、配送、複製、廃棄等)	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。
		推奨	(1) 情報の処理について履歴を取得し、資産台帳等に記録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、「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。
7.3 組織的安全管理策(体制、運用管理規程)				N/A
7.4 医療情報の伝達経路におけるリスク評価				N/A
7.5 物理的安全対策	7.5.1 医療情報処理施設の建物に関する要求事項			N/A
	7.5.2 医療情報処理施設への入退館、入退室等に関する要求事項	(1) 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域(自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等)を利用する場合		N/A
		推奨	(1) 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(PIN40)、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
		(2) 外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合		N/A
		推奨	(1) 医療情報システム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。	N/A
		(3) 外部事業者の運営するサーバ環境(専有サーバ、仮想プライベートサーバ等)を利用する場合		N/A
				N/A

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（情報処理 GL）				Google の回答
項目番号		区分 （推奨/最低限/その他）	ガイドライン	
	7.5.3 情報処理装置のセキュリティ	推奨	（1）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。
	7.5.4 情報処理装置の廃棄及び再利用に関する要求事項	推奨	（1）物理的な破壊措置については情報処理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こと。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、保管しておくこと。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用 」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
	7.5.5.情報処理装置の外部への持ち出しに関する要求事項	推奨	（1）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） ・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。
		推奨	（2）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（不正な改ざん等）、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。
7.6.技術的安全対策	7.6.1.情報処理装置及びソフトウェアの保守	推奨	（1）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。	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。
	7.6.2.開発施設、試験施設と運用施設の分離	推奨	（1）ソフトウェアに悪意のあるコード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。
	7.6.3.悪意のあるコードに対する管理策			N/A
	7.6.4.ウェブブラウザを使用する際の要求事項	推奨	（1）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 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。
	7.6.5.第三者が提供するサービスの管理	推奨	（1）外部事業者がサービスを実施する際は、情報処理事業者もしく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。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、 Google は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ　サプライヤーを利用するこ とがあります。サードパーティ　サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。　Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
	7.6.6.ネットワークセキュリティ管理	推奨	（1）医療情報システムから、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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（情報処理 GL）				Google の回答
項目番号		区分 （推奨/最低限/その他）	ガイドライン	
	7.6.6.ネットワークセキュリティ管理	推奨	（2）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。	N/A
	7.6.7.電子媒体の取扱	推奨	（1）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情報処理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こと。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、保管しておくこと。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
	7.6.7.電子媒体の取扱	推奨	（2）医療情報システム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ことが望ましい。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 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。
	7.6.7.電子媒体の取扱	推奨	（3）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 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。
	7.6.8.情報交換に関するセキュリティ	N/A		N/A
	7.6.9.医療情報システムに対するセキュリティ要求事項	N/A		N/A
	7.6.10.アプリケーションに対するセキュリティ要求事項	推奨	（1）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。
	7.6.11.暗号による管理策	推奨	（1）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。	N/A
		推奨	（2）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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-in-transit/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.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。
		推奨	（3）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 Platformプロダクトと G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
		推奨	（4）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ことが望ましい。	N/A
	7.6.12.ログの取得及び監査	推奨	（1）医療情報システム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/
		推奨	（2）監査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。 ・作業者情報（作業者 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（作業者 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（作業者 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（作業者 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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。　Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（情報処理 GL）				Google の回答
項目番号		区分 （推奨/最低限/その他）	ガイドライン	
		推奨	（3）監査ログを検証するため、作業者がアクセスした医療情報等を迅速に確認できるよう、作業者 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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
	7.6.13.アクセス制御方針	推奨	（1）作業者に与えられた権限外の情報や権限外の操作画面を表示しないよう権限管理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、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた　Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。Google 社員に付与される既定のアクセス権限は、社員用メールや　Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査　記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		推奨	（2）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。
	7.6.14.作業者アクセス及び作業者IDの管理	推奨	（1）アクセスを許可された作業者 ID の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。
		推奨	（1）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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		推奨	（2）システム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ざん、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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		推奨	（1）作業者が医療情報システムへのログオン用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、作業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検討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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」(情報処理 GL)				Google の回答
項目番号		区分 (推奨/最低限/その他)	ガイドライン	
		推奨	(2) パスワードの品質基準としては、パスワードを十分に長くすること(８文字以上等)、アルファベット及び数字並びに記号を一つ以上含むこと、等が考えられる。	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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
		推奨	(1) 不正なアカウントの利用又は試みが行われたことを作業者自身で検出するため、作業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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
		推奨	(2) 不正なアカウントの利用を防ぐため、作業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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		推奨	(3) 認可されていない作業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」と表示すると作業者 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。
		推奨	(4) 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。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		推奨	(5) 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)、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、「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。
	7.6.15.作業者の責任及び周知			N/A
7.7.人的安全対策		推奨	(1) 医療情報を操作する情報処理事業者職員については、規定の安全管理策に違反する行為を行った場合の懲戒手続きについて予め定めておくことが望ましい。これは服務規程等に含めることもできる。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こと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2)が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
7.8.情報の破棄				N/A
7.9.医療情報システムの改造と保守		推奨	(1) 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、外形的なぜい弱性検査を行う。	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。
7.10.医療情報処理に関する事業継続計画	7.10.1.要求事項の識別			N/A
7.10.医療情報処理に関する事業継続計画	7.10.2.事業継続計画の立案及びレビュー	推奨	(1) 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の点検手順(不正侵入、情報改ざん、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、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内 DR プログラムを確立しています。 Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
2.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定		医療情報に係る情報処理事業を受託する機関においては、医療情報の安全確保を目的として、合理的・客観的な基準による公正な第三者認証を取得すること。	Google は、セキュリティ、プライバシー、コンプライアンス管理の独立した検証が定期的に見直されるプログラムの維持に取り組んでいます。 Google は下記のようにデータの安全性、プライバシー、およびセキュリティをテストするために、いくつかの独立した第三者による監査を受けています。 SOC 1 / 2 / 3 (SSAE 18 - formerly SSAE 16 / SAS 70) ISO 27001 ISO 27017 / 27018 PCI - DSS HIPAA 証明書とコンプライアンス資料の全リストについては、以下を参照してください。 https://cloud.google.com/security/compliance
2.2 情報資産管理	2.2.1 資産台帳	(1) 医療機関等から預かる情報を管理するための管理台帳の整備について文書化して管理すること。	Google は ISO27001 認証を受けています。この基準では、「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。
		(2) 預託された情報の全てを資産台帳に記録すること。	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書　A.12.1.1）が規定されています。 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。
		(3) 必要に応じて資産台帳の閲覧が速やかに行うことができる状態で管理しておくこと。	Google は ISO27001 認証を受けています。この基準では、「操作手順書」（附属書　A.12.1.1）が規定されています。 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。
		(4) 資産台帳等へのアクセスについては、閲覧・編集が必要な作業者に制限すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		(5) 資産台帳等を電磁的記録として管理する場合には、資産台帳等へのアクセス制限を侵害する行為について記録すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
	2.2.2 情報の分類	(1) 情報を分類するための指針を決定し、情報の所有者、管理責任者が指針に従って適切な分類を行うことができるようにしておくこと。	Google は ISO27001 認証を受けています。この基準では、「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。
		(2) 情報の所有者、管理責任者は情報の分類が正しく行われていることを定期的に確認すること。	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。
		(3) 預託される情報に対して分類にもとづいたリスク分析を実施すること。	Google は ISO27001 認証を受けています。この基準では、「情報の分類」（ 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。
		(4) リスク分析の結果に応じて、リスク低減に必要な管理策を実施すること。	Google は ISO27001 認証を受けています。この基準では、「情報の分類」（ 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。
		(5) 分類がわかるように情報にラベルをつけること（電磁的な記録にラベルをつける方式には様々なものが考えられるので、実装する方式の詳細及び安全性について、医療機関等側の確認、承認を得ること）。	Google は ISO27001 認証を受けています。この基準では、「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。
		(6) 各ラベルに応じた処理方式（保存、配送、閲覧、廃棄等）を定めること。	Google は ISO27001 認証を受けています。この基準では、「情報の分類」（ 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。
2.3 組織的安全管理策（体制、運用管理規程）		(1) 医療情報の安全管理に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ ISO27002 2013、附属書 A.6）が規定されています。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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(2) 個人情報保護に関する方針を策定し、医療機関等の求めに応じて提出できる状態にしておくこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ ISO27002 2013、附属書 A.6）が規定されています。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。
		(3) 個人情報保護に関しては、医療機関等の監督の下に行うこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ ISO27002 2013、附属書 A.6）が規定されています。情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud 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。
		(4) 情報処理の安全管理に関わる手順書、運用管理規程を整備すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ ISO 27001 2013、附属書 A.5）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。
		(5) 運用管理規程には、情報セキュリティに対する組織的取組方針、情報処理事業者内の体制及び施設、医療機関及び清掃事業者等の外部事業者との契約書の管理、情報処理に関わるハードウェア・ソフトウェアの管理方法、リスクに対する予防、リスク発現時の対応、医療情報を格納する媒体の管理（保管・授受等）、第三者による情報セキュリティ監査、医療機関等の管理者からの問い合わせ窓口の設置、対応等について記載しておくこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのための方針群」（ ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ ISO27002 2013、附属書 A.6）が規定されています。情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud 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。
2.4 .医療情報の伝達経路におけるリスク評価		医療情報の取扱いに際しては高い機密性が求められていることに配慮しなければならない。機密性を確保するためには、医療情報の移動する範囲を限定することが必要である。情報の入り口から保管場所、電子媒体であれば適切な保護機能と一定の強度を備えた保管庫、電磁的記録であれば適切なアクセス管理を施されたデータベース、ファイルサーバ等に保存されるまでの経路、及び医療機関等に医療情報を提供する経路、最終的に情報を廃棄する経路を認識し、その経路上に存在する脅威を列挙してリスク評価を行うこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティのレビュー」（ ISO 27001 2013、附属書 A.18.2）が規定されています。 システムの可用性と完全性に関連する統制は、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。 定性的および定量的方法を使用して、識別されたすべてのリスクの可能性と影響を判断するために、正式なリスク評価が少なくとも年 1回行われます。各リスクに関連する可能性と影響は、各リスクカテゴリを考慮して、個別に決定されます。
2.5 物理的安全対策	2.5.1 医療情報処理施設の建物に関する要求事項	(1) 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、鍵管理が行われていること。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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
		(2) 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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティ 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。
		(3) 建物、部屋に対する不正な物理的な侵入を抑止するため、侵入検知装置を導入すること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 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。
		(4) 自然災害、人的災害による損傷を避けるため、建物自体の防災対策を適切に実施すること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方　　法、ネットワークやインターネットの接続性、さらにソフトウェア サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって　1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、　Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に　2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google は、データセンターが所在するリージョンの建築要件と設備要件をすべて満たしています。
	2.5.2 .医療情報処理施設への入退館、入退室等に関する要求事項	(1) 情報処理事業者の管理外にある者の立ち入りを抑制することのできる、情報処理事業者が専有する建造物あるいは領域（自社専有のデータセンター、外部データセンター事業者のコロケーション領域のうち独立した領域等）を利用する場合	N/A
		・医療情報システムを設置、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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティ 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		・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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、 Google の設計基準の根幹をなしています。 Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ　ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ　モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。 データセンターには棟の内外に高解像度の監視カメラを設置し、 24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ　バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー　https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画　https://www.youtube.com/watch?v=XZmGGAbHqa0
		・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こと（履歴の保全については「 2.6.12.ログの取得及び監査」を参照）。	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
		・情報処理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情報処理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、情報処理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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、 Google の設計基準の根幹をなしています。 Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ　ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ　モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。 データセンターには棟の内外に高解像度の監視カメラを設置し、 24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ　バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー　https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画　https://www.youtube.com/watch?v=XZmGGAbHqa0
		・情報処理事業者の職員は、情報処理事業者の専有する領域にて、情報処理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、身分を確認すること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、 Google の設計基準の根幹をなしています。 Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ　ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ　モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。 データセンターには棟の内外に高解像度の監視カメラを設置し、 24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ　バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー　https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画　https://www.youtube.com/watch?v=XZmGGAbHqa0
		・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、情報処理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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、 Google の設計基準の根幹をなしています。 Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ　ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ　モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。 データセンターには棟の内外に高解像度の監視カメラを設置し、 24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ　バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー　https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画　https://www.youtube.com/watch?v=XZmGGAbHqa0
		・情報処理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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティ 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		・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認めないこと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 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
		（2）外部事業者の運営するデータセンター内にサーバラック等の設置場所を借りて利用する場合	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
		・データセンターを運営する外部事業者が、（1）と同等な安全管理策を実施する等、情報処理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こと。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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
		・医療情報システムの設置されるサーバラックには施錠を行い、定められた情報処理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こと。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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
		・情報処理事業者が医療情報システム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、作業開始時刻、作業終了時刻、作業内容等について記録すること。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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、医療情報に影響を与えないことを確認すること。	Google は ISO27001 認証を受けています。この基準では、「装置」（ 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
		・医療情報システムであることが、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こと。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(3) 外部事業者の運営するサーバ環境（専有サーバ、仮想プライベートサーバ等）を利用する場合	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
		Øサーバ環境を運営する外部事業者が、(1)及び(2)と同等な安全管理策を実施する等、情報処理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こと。	Google は ISO27001 認証を受けています。この基準では、「供給者関係」（ ISO 27001 2013、附属書 A.15）が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、 Google は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ　サプライヤーを利用するこ とがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
	2.5.3 情報処理装置のセキュリティ	(1) 不正な装置を識別するため、医療情報システム内で利用する情報処理装置を登録したリストを作成・維持すること。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書　A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書　A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 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。
		(2) 医療情報システムに用いる装置には、必要のないアプリケーション等をインストールしないこと。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書　A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書　A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 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。
		(3) 医療情報等が表示される端末画面等をアクセス権限の無いものが閲覧することが無い様に室内の機器レイアウトを行うこと。このようなレイアウトが難しい場合には、端末画面に覗き見防止用フィルターを設置する等の対策を行うこと。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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
		(4) 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こと。	Google は ISO27001 認証を受けています。この基準では、「暗号」（ ISO 27001 2013、附属書 A.10）が規定されています。 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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
		(5) 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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 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
		(6) 医療情報システムを配置する室内での喫煙、飲食を禁止すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で　Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ　チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(7) 医療情報システム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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 環境の健全性と安全性の統制は、Google の全データセンターにおいて徹底されています。すべての施設で、熱、火、煙、水の検知を含め、環境面に関する十分な対策を施しています。 すべての施設には堅牢な防火設備が導入されており、火災の防止と検知においても万全な対策を施しています。火災検知器や消火設備を設置し、ハードウェアの損傷を防ぎます。熱、火、煙、水の探知機は、異常が発生しているゾーン、セ　キュリティ操作コンソール、リモート　モニタリング デスクにおいて、一斉に音声と視覚効果による警報を発する仕組みになっています。 Google は、データセンターが所在する地域の建築要件をすべて遵守しています。 詳しくは、Google セキュリティ ホワイトペーパーをご覧ください。https://cloud.google.com/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。
		(8) 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こと。	Google は ISO27001 認証を受けています。この基準では、「装置の保守」（ ISO 27001 2013、附属書 A.11.2.4）が規定されています。
		(9) 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情報処理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こと。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こと。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廃棄を選択すること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。 なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
		(10) 医療情報システム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こと。 震災時に転倒することが無いよう確実に設置すること。　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こと。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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 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。
		(11) 起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「 2.6.14.作業者アクセス及び作業者IDの管理」に従うこと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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。
		(12) 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こと。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に　2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
		(13) 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こと。	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。
	2.5.4 情報処理装置の廃棄及び再利用に関する要求事項	(1) ハードディスク等を医療情報システム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こと。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。 なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(2) 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、それらを消去すること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
		(3) 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こと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書　A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、　SOC 2、Type II の報告書を取得しています。 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。
		(4) 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こと。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
	2.5.5.情報処理装置の外部への持ち出しに関する要求事項	(1) 情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。	Google は ISO27001 認証を受けています。この基準では、「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。
		(2) 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こと。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書　A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書　A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 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。
2.6.技術的安全対策	2.6.1.情報処理装置及びソフトウェアの保守	(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こと。	Google は ISO27001 認証を受けています。この基準では、「装置の保守」（ ISO 27001 2013、附属書 A.11.2.4）が規定されています。
		(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検討すること。	Google は ISO27001 認証を受けています。この基準では、「変更管理」（ ISO 27001 2013、附属書 A.12.1.2）と「システムの取得、開発および保守」（ ISO 27001 2013、附属書 A.14）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。
		(3) 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こと。	Google は ISO27001 認証を受けています。この基準では、「運用の手順および責任」（ ISO 27001 2013、附属書 A.12.1）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。
		(4) 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立てて実施すること。	Google は ISO27001 認証を受けています。この基準では、「装置の保守」（ ISO 27001 2013、附属書 A.11.2.4）が規定されています。
		(5) 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こと。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こと。	Google は ISO27001 認証を受けています。この基準では、「変更管理」（ ISO 27001 2013、附属書 A.12.1.2）と「システムの取得、開発および保守」（ ISO 27001 2013、附属書 A.14）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。
		(6) 不正な改ざん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（改ざん検知）を実施すること。	Google は ISO27001 認証を受けています。この基準では、「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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(7) 医療情報システム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こと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書　A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、　SOC 2、Type II の報告書を取得しています。 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。
		(8) 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）を決定すること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書　A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、　SOC 2、Type II の報告書を取得しています。 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。
		(9) 修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。	Google は ISO27001 認証を受けています。この基準では、「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。
		(10) 保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し、「 2.6.5.第三者が提供するサービスの管理」の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。	Google は ISO27001 認証を受けています。この基準では、「供給者関係」（ ISO 27001 2013、附属書 A.15）が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、　Google は顧客サポートやテクニカル　サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ　サプライヤーを利用するこ とがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
	2.6.2.開発施設、試験施設と運用施設の分離	(1) 情報処理に供するアプリケーションについては、情報処理事業者自身で開発したアプリケーションを用いること。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こと。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」（ ISO 27001 2013、附属書 A.14）が規定されています。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。
		(2) ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設（以下、「開発施設」という。）を用いて行うこと。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud 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。
		(3) 開発施設では、悪意のあるコード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「2.6.3.悪意のあるコードに対する管理策」に従うこと。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud 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。
		(4) 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ざん防止、検知策を実施すること。	Google は ISO27001 認証を受けています。この基準では、「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。
		(5) 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こと。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud 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。
		(6) 医療情報を開発及び試験用データとして直接、利用しないこと。利用する場合には、個人情報の消去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に示し、了解を得た上で利用すること。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud 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。
	2.6.3.悪意のあるコードに対する管理策	(1) 最新の脅威についての情報収集に努め、導入している悪意のあるコード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こと。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。
		(2) 悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。 ・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。
		(3) 一定期間、悪意のあるコード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といった対策が行われていること	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書　A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、　SOC 2、Type II の報告書を取得しています。 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
	2.6.4.ウェブブラウザを使用する際の要求事項	(1) 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こと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書　A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、　SOC 2、Type II の報告書を取得しています。 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。
		(2) 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になっていること（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。
		(3) 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「 2.6.3.悪意のあるコードに対する管理策」に即して検査されること。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書　A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、　SOC 2、Type II の報告書を取得しています。 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。
	2.6.5.第三者が提供するサービスの管理	(1) 第三者により提供されるサービス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こと。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
		(2) サービスの実施、運用、維持について定期的に検証すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員および全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で　Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
		(3) 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こと。	Google は ISO27001 認証を受けています。この基準では、「供給者関係」（ ISO 27001 2013、附属書 A.15）が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、 Google は顧客サポートやテクニカル　サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ　サプライヤーを利用するこ とがあります。サードパーティ　サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
		(4) サービス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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、 Google の設計基準の根幹をなしています。 Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ　ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ　モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。 データセンターには棟の内外に高解像度の監視カメラを設置し、 24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ　バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー　https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画　https://www.youtube.com/watch?v=XZmGGAbHqa0
		(5) サービス実施中に第三者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こと。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 セキュリティとデータ保護を重視する方針は、 Google の設計基準の根幹をなしています。 Google のデータセンターは、カスタム設計された電子アクセスカード、警報、車両セキュリティ　ゲート、外周フェンス、金属探知機、生体認証などの安全保護対策を施した、多層セキュリティ　モデルによって物理的なセキュリティを確保しています。また、データセンターのフロアには、レーザー光線による侵入検知システムが導入されています。 データセンターには棟の内外に高解像度の監視カメラを設置し、 24 時間体制で侵入者を検知、追跡しています。インシデントが発生した際は、アクセスログ、アクティビティ記録、カメラ映像による確認ができます。また、厳格な身元調査とトレーニングを受けた経験豊富な警備員が定期的にパトロールしています。 セキュリティ エリア（データ サーバー フロアなど）に入るには、セキュリティ通路を通らなければなりません。このセキュリティ通路では、セキュリティ　バッジと生体認証を利用した多元的なアクセス管理を実施しています。セキュリティ エリアへの立ち入りが許可されているのは特定の役割を持つ承認された社員です。こうしたエリアへのアクセス管理は、モニタリングとロギングの対象になっています。 Google のデータセンター プロセスについて詳しくは、Google セキュリティ ホワイトペーパーとデータセンターを紹介する動画をご覧ください。 Google セキュリティ ホワイトペーパー　https://cloud.google.com/security/whitepaper#state-of-the-art_data_centers データセンターを紹介する動画　https://www.youtube.com/watch?v=XZmGGAbHqa0

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(6) サービス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、情報処理事業者の職員の入室、退室手順に準ずること。	Google は ISO27001 認証を受けています。この基準では、「物理的および環境的セキュリティ」（ ISO27001 2013、附属書 A.11）が規定されています。システムの可用性に関する物理的な統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 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
		(7) サービスの変更時には、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こと。	Google は ISO27001 認証を受けています。この基準では、「供給者関係」（ ISO 27001 2013、附属書 A.15）が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、 Google は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ　サプライヤーを利用するこ とがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
		(8) 医療情報システム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するガイドライン第4．1版（厚生労働省、平成 22年2月）」6．8章C項の管理策を実施すること。	N/A
	2.6.6.ネットワークセキュリティ管理	(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こと。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こと。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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。
		(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こと（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。
		(3) 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こと。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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。
		(4) 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こと。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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
		(5) 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（以下、「IDS」という。）及び侵入防止システム（以下、「IPS」という。）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こと。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、同様の制御を行うこと。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク　サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ ISO 27001 2013、附属書 A. 13.1）が規定されています。 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。
		(6) 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こと。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク　サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ ISO 27001 2013、附属書 A. 13.1）が規定されています。 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(7) 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にしていること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク　サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ ISO 27001 2013、附属書 A.13.1）が規定されています。 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。
		(8) 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まれていること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク　サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク管理策」（ ISO 27001 2013、附属書 A.13.1）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。
		(9) 医療情報システムにおいて、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こと。他に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こと。 ・外部からの医療情報システムの稼働監視・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 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。
		(10) 医療情報システム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こと。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク　サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ ISO 27001 2013、附属書 A.13.1）が規定されています。 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。
		(11) ネットワーク接続のログ（認証ログ及び接続ログ）を記録すること。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク　サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク セキュリティ管理」（ ISO 27001 2013、附属書 A.13.1）が規定されています。 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。
		(12) ネットワーク接続ログを定期的に検証し不審な活動が行われていないことを検証すること。	Google は ISO27001 認証を受けています。この基準では、「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。
		(13) 医療情報を保存する医療情報システムにおいて無線ネットワーク（Bluetooth 等の近距離無線通信を含む）LAN を利用しないこと。	N/A
		(14) VPN接続を行う場合には以下の事項に従うこと。　I接続時にVPN装置間で相互に認証を行うこと。　I傍受、リプレイ等のリスクを最小限に抑えるために、「2.6.11.暗号による管理策」に従い、適切な暗号技術を利用すること。　I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こと。　I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こと。	Google は ISO27001 認証を受けています。この基準では、「通信のセキュリティ」（ ISO 27001 2013、附属書 A.13）と「公衆ネットワーク上のアプリケーション　サービスのセキュリティの考慮」（ ISO27002 2013、附属書 A.14.1.2）が規定されています。 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
	2.6.7.電子媒体の取扱	(1) 電子媒体について情報処理事業者施設外への不要な持ち出しを行わないこと。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、DVDR等）を用い、情報交換作業終了後、電子媒体を(9)に示す方式にて確実に廃棄処分すること。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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
		(2) 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と。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こと。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
		(3) 電子媒体は台帳を作成して管理すること。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こと。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こと。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書　A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書　A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 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。
		(4) 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こと。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書　A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書　A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 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。
		(5) 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媒体の製造者により指定される保管環境にて保管すること。	Google は ISO27001 認証を受けています。この基準では、「資産に対する責任」（附属書　A.8.1）、「媒体の処分」（附属書 A.8.3.2）、「装置のセキュリティを保った処分または再利用」（附属書　A.11.2.7）、「運用ソフトウェアの管理」（附属書 A. 12.5）が規定されています。 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。
		(6) 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、他媒体に複写すること。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）と「バックアップ」（ISO27001 2013、附属書 A.12.3）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
		(7) 情報を保管するためにハードディスク装置を用いる場合には、RAID－1もしくはRAID－6相当以上のディスク障害に対する対策を取ること。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(8) 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こと。	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。
		(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こと。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A.8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
	2.6.8.情報交換に関するセキュリティ	(1) 医療機関等と情報処理事業者間の情報交換に関して、次の事項を予め合意しておくこと。 l情報を電子媒体に記録して交換する際の手順 l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 l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	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」（ ISO 27001 2013、附属書 A.14）が規定されています。情報セキュリティの監督管理体制は、ソフトウェアの開発管理など、第三者機関によるレビューと検証を受け、 SOC 2、Type II の報告書を取得しています。 Google Cloud のお客様は、入力管理をサポートするプロセスの開発など、お使いの環境を設定、管理するすべて権利と責任を保有します。
		(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こと。 ・発送者、受領者を識別し記録すること。 ・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、否認防止策を行うこと。 ・交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと。）。 ・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こと。	Google は ISO27001 認証を受けています。この基準では、「暗号」（ ISO 27001 2013、附属書 A.10）が規定されています。 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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
		(3) 物理的に情報を搬送する際には以下の対策を実施すること。 ・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こと。 ・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こと。 ・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こと。 ・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こと。 ・電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。 ・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こと。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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
		(4) 電子的に情報を転送する際には以下の対策を実施すること。 ・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こと。認証方式は接続形態、転送に利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こと。 ・受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。 ・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こと	Google は ISO27001 認証を受けています。この基準では、「暗号」（ ISO 27001 2013、附属書 A.10）が規定されています。 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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
	2.6.9.医療情報システムに対するセキュリティ要求事項	(1) 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こと。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud 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。
		(2) 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こと。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」（ ISO 27001 2013、附属書 A.14）が規定されています。情報セキュリティの監督管理体制は、ソフトウェアの開発管理など、第三者機関によるレビューと検証を受け、 SOC 2、Type II の報告書を取得しています。 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。
		(3) 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こと。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」（ ISO 27001 2013、附属書 A.14）が規定されています。 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。
		(4) 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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は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。
		(5) 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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。　Google 社員に付与される既定のアクセス権限は、社員用メールや　Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、　Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、　Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
	2.6.10.アプリケーションに対するセキュリティ要求事項	(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こと。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こと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（ 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。
		(2) 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こと。	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」（附属書 A.12.2）が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、 SOC 2、Type II の報告書を取得しています。 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。
		(3) アプリケーションにて情報の登録、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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		(4) アプリケーションにて医療事業者側の作業者を認証する情報（ID／パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
		(5) アプリケーションによる情報操作については、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、編集、削除等を防止すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
	2.6.11.暗号による管理策	(1) 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こと。選択基準としては電子政府推奨暗号リスト等を用いること。	Google は ISO27001 認証を受けています。この基準では、「暗号」（ ISO 27001 2013、附属書 A.10）が規定されています。 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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(2) 暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。	Google は ISO27001 認証を受けています。この基準では、「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。
		(3) 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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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。
		(4) 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こと。	Google は ISO27001 認証を受けています。この基準では、「暗号」（ ISO 27001 2013、附属書 A.10）が規定されています。 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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
		(5) 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、真正性を検証すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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。
	2.6.12.ログの取得及び監査	(1) 作業者の活動、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監査ログを作成し管理すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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。
		(2) 監査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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、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。
		(3) 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こと。	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/
		(4) 標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。	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 はすべての内部のシステムクロックを原子時計と GPS に同期させ、独自の NTP サービスを実行しています。 Google は公共 NTPサービス https://developers.google.com/time を通してお客様が利用できるようにしています。
		(5) 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こと。 ・ログデータにアクセスする作業者及び操作を制限すること。 ・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こと。・ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。	Google is certified to the ISO27001 Standard, which regulates "Access Control" (ISO 27001:2013, Annex A.9). Information security oversight and management controls, including logical access controls are reviewed and verified by a third party auditor for Google's SOC 2, Type II report. Google maintains a Data Security Policy that governs access to data and mechanisms to prevent and detect unauthorized access.
	2.6.13.アクセス制御方針	(1) 情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」（ ISO 27001 2013、附属書 A.14）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。
		(2) 情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること。	Google は ISO27001 認証を受けています。この基準では、「システムの取得、開発および保守」（ ISO 27001 2013、附属書 A.14）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。
		(3) アクセス権限の登録申請、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を規定すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(4) それぞれの情報にアクセスする権限を持つ作業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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		(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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
	2.6.14.作業者アクセス及び作業者IDの管理	(1) 作業者は情報処理装置上においてユニークな作業者IDにより識別されること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		(2) 作業者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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		(3) 複数作業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、作業者IDでログオンしてからグループIDに変更する仕組みを利用すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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。
		(4) 作業者IDの発行は医療情報システムの管理に必要な最小限の人数に留めること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(5) 作業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を利用停止とすること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 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。
		(6) 監視ログの監査時に作業者を確実に特定するため、作業者IDは過去に使われたものを再利用しないこと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は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。
		(7) 不要な作業者IDが残っていないことを定期的に確認すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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。
		(8) 特権IDの発行は必要な最小限のものに留めること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		(9) 特権使用者に昇格可能な作業者IDを制限すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		(10) 特権の使用時には作業実施内容を記録すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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。
		(11) 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こと。	Google は ISO27001 認証を受けています。この基準では、「運用の手順および責任」（ ISO 27001 2013、附属書 A.12.1）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。
		(12) 情報処理装置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、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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 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。
		(13) 医療情報システムへのログオン用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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(14) 医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
		(15) 医療情報システムへのログオン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
		(16) 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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
		(17) 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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。 サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		(18) パスワードの満たすべき品質の基準を策定し、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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud 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。
		(19) 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作業者に徹底すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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。
		(20) 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こと。また、一般の作業者による閲覧を制限すること。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
		(21) 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、作業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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 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。
		(22) 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こと。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と。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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
	2.6.15.作業者の責任及び周知	(1) 各作業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こと。	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」（ ISO 27001 2013、附属書 A.9）が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、多元的なログイン方法を採用しています。ユーザーは、セキュリティ　トレーニングの一環として、パスワードの正しい作成方法や管理方法について指導を受けます。さらに、パスワード管理システムを導入し、社内ポリシーの徹底した遵守に努めています。 Google Cloud 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。
		(2) システム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こと。	Google は ISO27001 認証を受けています。この基準では、「ネットワークおよびネットワーク　サービスへのアクセス」（ISO 27001 2013、附属書 A.9.1.2）と「ネットワーク管理策」（ ISO 27001 2013、附属書 A.13.1）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。
		(3) 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こと。	Google は ISO27001 認証を受けています。この基準では、「装置」（ ISO 27001 2013、附属書 A.11.2）が規定されています。 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
2.7.人的安全対策		(1) 医療情報を操作する可能性のある情報処理事業者職員の全てについて、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こと。派遣従業員については秘密保持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こと。	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。
		(2) 医療情報を操作する可能性のある情報処理事業者職員の全てに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ものだけを選定すること。派遣従業員に関しては、派遣元に対し、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こと。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こと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」（ISO 27001 2013、附属書 A.7.2.2）が規定されています。 セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で　Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ　チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
		(3) 情報処理事業者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、改ざん又は破壊等の行為が行われていないことを検証すること。	Google は ISO27001 認証を受けています。この基準では、「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。
		(4) 医療情報を操作する情報処理事業者職員が退職する際には、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こと。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こと。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こと。	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。
		(5) 医療機関等との委託契約において、情報処理事業者職員との秘密保持契約を結ぶこと、情報セキュリティ教育を受けさせること、及び、規定に反して預託情報を不正に扱った際の懲罰規定等、預託情報の機密管理に関する条項を設けること。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
2.8.情報の破棄		(1) CD－R等の廃棄については「 2.6.7.電子媒体の取扱」を参照すること。	N/A
		(2) ハードディスク等の廃棄については「 2.5.4.情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。	N/A
		(3) 情報処理事業者は「医療情報システムの安全管理に関するガイドライン」に従って情報の破棄を行った記録を提出すること。	Google は ISO27001 認証を受けています。この基準では、「媒体の処分」（ ISO 27001 2013、附属書 A. 8.3.2）と「装置のセキュリティを保った処分または再利用　」（ISO 27001 2013、附属書 A.11.2.7）が規定されています。 Google はデータセンターにあるすべての機器のロケーションと状態を、購入、設置から廃棄、破壊にいたるまで、バーコードやアセットタグを使用して細心の注意を払いながら追跡しています。データセンターのフロアから承認なしで機器が持ちだされることがないように、金属探知機や映像監視システムを導入しています。ライフサイクル中のいかなる時点においても、性能試験に合格しなかったコンポーネントは、インベントリから除外され、廃棄されます。ハードドライブを破棄する　際には、所定の権限を持つ人が、ディスクのデータをゼロ書き込みで消去してから、複数段階の検証ステップにより、ドライブのデータが消去されていることを確認します。なんらかの理由でドライブのデータを消去することができない場合、物理的に破壊できる状況になるまで、厳重に保管されます。ディスクの物理的な破壊は複数の段階で行われます。最初に、破砕機でドライブを変形させ、次にシュレッダーでドライブを細かく砕きます。その破片は安全な施設でリサイクルされます。各データセンターでは、処分に関する厳格な方針を遵守しており、なんらかの違反があった場合にはすぐに対処します。
2.9.医療情報システムの改造と保守		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こと。	Google は ISO27001 認証を受けています。この基準では、「開発環境、試験環境および運用環境の分離」（ISO 27001 2013、附属書 A.12.1.4）と「開発およびサポート プロセスにおけるセキュリティ」（ ISO 27001 2013、附属書 A.14.2）が規定されています。 Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」(安全管理 GL)			Google の回答
章	項目番号	ガイドライン	
2.10.医療情報処理に関する事業継続計画	2.10.1.要求事項の識別	(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)、情報処理設備等について識別すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。
		(2) 業務プロセス間の相互関係を評価すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。
		(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こと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。
		(4) 医療情報システム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こと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。
		(5) 医療情報システム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こと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。

経済産業省「医療情報を受託管理する情報処理事業者向けガイドライン　第2版」（安全管理 GL）			Google の回答
章	項目番号	ガイドライン	
		(6) 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検討すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」（ ISO 27001 2013、附属書 A.17.1）が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。
		(7) 医療機関等に提供する情報処理サービス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、情報処理サービス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本ガイドラインで提示する物理的安全対策を施すこと。	Google は ISO27001 認証を受けています。この基準では、「冗長性」（ ISO27001 2013、附属書 A.17.2）が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。
	2.10.2.事業継続計画の立案及びレビュー	(1) 医療情報システムのサービス提供における業務プロセス及び医療情報システム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として策定すること。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」（ ISO 27001 2013、附属書 A.17.1）が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。
		(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こと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」（ ISO 27001 2013、附属書 A.17.1）が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。
		(3) 事業継続計画について定期的に見直しを行うこと。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」（ ISO 27001 2013、附属書 A.17.1）が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.1	(ア)	①サービスの提供についての管理責任を有する責任者を設置する。 ②情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者(システム管理者)を設置する。 ③サービスの提供に係る情報システムの運用に関する事務を統括する責任者を設置する。 ④①から③に掲げた責任者の任命･解任等のルールを策定する。	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 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。
3.2.1	(イ)1	①　サービス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、サービス提供に係る契約に含める。契約には、守秘義務に違反したクラウドサービス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 G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.1	(イ)2	①サービス提供に係る契約において、次項(ウ) 1.に定める運用管理規程等の内容、その他最新の関連法令等を遵守し、安全管理措置を実施する旨を明らかにする。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.1	(イ)3	①　サービス提供に係る契約において、本ガイドラインのほか、厚生労働省ガイドライン及び経済産業省ガイドラインを遵守する旨を含める。 ②　①に示す各ガイドラインの遵守状況を医療機関等に提示する際は、可能な限り具体的に行う(例えば、総務省が定める「 ASP･SaaS(医療情報取扱いサービス)の安全･信頼性に係る情報開示指針」（平成29年3月31日)に定める事項に準じた情報の提供を行う等)	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.1	(ウ)1	①経営者は、自社における個人情報保護指針、プライバシーポリシー等について明確にする。 ②①の指針等には個人情報保護法及び個人情報保護委員会のガイドラインに定める安全管理措置等を実施する旨を含める。 ③①の指針等には、個人情報保護法の対象外の情報(死者に関する情報等)であっても、医療情報の特殊性から個人情報保護法における運用に準じて取り扱う旨を含める。 ④情報セキュリティに係るポリシー等を含む関する基本方針、運用管理規程等の情報セキュリティポリシーを策定する。 ⑤情報セキュリティポリシーの遵守を担保する組織体制の構築とその文書化を行う。 ⑥情報セキュリティに関する組織的取組における基本方針セキュリティポリシーについては、サービス仕様適合開示書に基づき、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、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud 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。
3.2.1	(ウ)2	①サービスの提供に係る体制を、緊急時の対応も含めて明確にする。 ②サービスの提供に係る体制等に関する情報(再委託による体制に関する情報を含む)の開示等について、サービス仕様適合開示書に基づき、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、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud 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。
3.2.1	(ウ)3	①情報セキュリティに関する基本方針や運用管理規程等、重要な文書の作成や管理に関する規程を策定し、これに基づき文書の管理を行う。 ②サービスの運用や資源管理に関して、適切に文書化を行い、セキュリティ情報として管理する。 ③サービスの運用等に係るマニュアル等の文書管理に関して、開示可能範囲、開示に必要な条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④医療情報の管理状況に関係する資料の提供について、サービス仕様適合開示書に基づき、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、「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。
3.2.1	(ウ)4	①サービスに係るリスクの分析を行い、必要な対応措置等を講じる旨を定める。 ②サービスに係るリスク分析の結果、対応措置及び事故等の発生時の対応等について、サービス仕様適合開示書に基づき、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、「情報セキュリティのレビュー」(ISO 27001 2013、附属書 A.18.2)が規定されています。 システムの可用性と整合性に関する管理は、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。 定性的および定量的方法を使用して、識別されたすべてのリスクの可能性と影響を判断するために、正式なリスク評価が少なくとも年 1回行われます。各リスクに関連する可能性と影響は、各リスクカテゴリを考慮して、個別に決定されます。
3.2.1	(ウ)5	①　機器等の管理方法について、文書化を行う。 ②　機器等について、台帳管理等により所在確認等を行う旨を定める。 ③　機器等の管理等に関する自社の運用規程について、サービス仕様適合開示書に基づき、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 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。
3.2.1	(ウ)6	①　個人情報を記録した媒体の管理等に関する運用規程を策定する。 ②　個人情報を記録した媒体の管理等に関する運用規程について、サービス仕様適合開示書に基づき、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、「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
3.2.1	(ウ)7	①　医療機関等で患者等への説明及び同意を得る際のクラウドサービス事業者の情報提供に関して、その提供範囲やクラウドサービス事業者が担う役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.1	(ウ)8	①　サービスを提供する情報システム、組織体制、運用等に関する監査の方針、内容等について明文化を行う。 ②　第三者が提供するクラウドサービスを利用する場合については、これに対する監査又は代替する対応についての方針、内容を明確にする。 ③　監査実施について記録し、当該記録の保存・管理方法を明確にする。 ④　自社において実施する情報システム監査等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤　医療機関等に開示する監査記録等の範囲・条件等について、サービス仕様適合開示書に基づき、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、「情報システム監査の考慮事項」(ISO 27001 2013、附属書 A.12.7)が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google は、Goole の ID 管理、ソースコード管理及びインフラストラクチャー管理に対する管理者のコンプライアンスを評価する責任を負う内部監査機能を確立している。
3.2.1	(ウ)9	① 医療機関等の管理者からの問合せ窓口を設ける。また受付の時間帯等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 自社で契約した第三者が提供するクラウドサービスを利用してサービスを提供する場合でも、医療機関等からの問合せ窓口を一元化する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.1	(エ)1	①クラウドサービス事業者における情報システムへのアクセス権限、アカウント管理、認証及びアクセス等に対する記録の収集と保存、並びに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等を内容とするアクセス管理規程を策定する。 ②サービスの提供に係るアクセス記録(外部からのアクセス、利用者によるアクセス等を含む)の保存、記録の定期的なレビューと改善を実施する旨を内容とするアクセス管理規程を策定する。	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 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。
3.2.1	(エ)2	①医療情報の取扱いに関する委託契約に、以下の内容を含める。 ・個人情報に関して、他の情報と区別して適切に管理を行う。 ・医療情報は、死者に関する情報についても個人情報に準じて取り扱う旨を明確にする。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.2	(ア)1	①　サービスに供する機器、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。 ②　サービスに供するサーバ等を格納するラック等について、施錠管理を行う。 ③　サービスに供する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"
3.2.2	(ア)2	①　サービスに供する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。 ②　サービスに供する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。 ③　サービスに供する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。 ④　サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付ける。 ⑤　サービスに供する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。 ⑥　サービスに供する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。 ⑦　①～⑥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"
3.2.2	(ア)3	①　サービスに供する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、火災等並びにそれに伴う停電等)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。 ②　①の施設を設置する建築物は、サービス仕様適合開示書に基づき、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。
3.2.2	(ア)4	①　サービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置する。 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。 ③　サービスに供する機器、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"

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.2	(イ)1	① 個人情報の表示中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る等の対策を行う。 ② 運用中の画面が、運用者以外の者の視野に入らないような対応等を行う。	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
3.2.2	(ウ)1	① 個人情報が物理的に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。 ② 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を取り付ける。 ③ 受託する個人情報を運用や保守に用いる端末に保存しない旨、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、「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。
3.2.3	(ア)1	① 情報システム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。ただし当該情報システムが他の情報システムを利用するための ID(non interactive ID)は除く)。 ② 利用者のなりすまし等を防止するための認証を行う。 ③ 利用者には、医療機関等においてサービスを利用する者のほか、情報システム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も含める。 ④ 情報システム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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
3.2.3	(ア)2	① 本人の識別・認証に、ユーザ IDとパスワードを組み合わせて用いる場合には、それらを、本人しか知り得ない状態に保つよう対策を行う。具体的には以下のような対策を行う。 ・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情報システムにアクセスできないようにする。 ・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。 ・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。 ② パスワード認証に係る以下のルールを実現する措置を講じる。 ・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。 ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない仕組みとする。 ③ パスワードには十分な安全性を満たす有効期間を設定する。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。 ④ 認証に際して ID及びパスワードによらない場合でも、上記と同等以上の安全性を確保する。	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。
3.2.3	(ア)3	① 利用者のパスワード情報は、ハッシュ値での保存を行う等、暗号化手法により、管理する。 ② サービスに供する製品等の導入に際しては、初期パスワードを変更するだけでなく、必要なアカウントの棚卸しを行い、不要なものについては削除を行う。 ③ 利用者が ID、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。 ④ パスワード等の情報の漏洩が生じた場合又は不正な第三者からの攻撃により漏洩した場合には、直ちに当該 IDを無効化し、あらかじ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。 ⑤ 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。 ⑥ 利用者が設定する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、これに基づく運用を行う。 ⑦ 利用者のパスワードの世代管理を行い、パスワード変更に際して、安全性を確保するのに必要な範囲で、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。 ⑧ 自社において定めたパスワードポリシーについて、サービス仕様適合開示書に基づき、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。
3.2.3	(ア)4	① 情報システム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、2要素認証以上の認証強度のある方法による。 ② 利用者の認証で採用する認証方式について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 利用者の認証において、固定式の ID・パスワードによる認証方式を採用している場合には、固定式の 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。 ④ 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。 ⑤ 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。 ⑥ 代替的手段・手順により、情報システム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。 ⑦ その他、一時的な利用者の認証方法について、サービス仕様適合開示書に基づき、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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.3	(イ)1	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。 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。 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。 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、サービス仕様適合開示書に基づき、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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
3.2.3	(イ)2	① サービスには、医療従事者、関係職種ごとにアクセス権限・範囲等のアクセス制御が可能な機能を含める。 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。なお、アクセス制御に係る情報の提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 運用管理規程に従い、アクセス管理に関する運用を行い、医療機関等の求めに応じて資料を提出できるようにする。資料の提供に係る条件等については、サービス仕様適合開示書に基づき、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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
3.2.3	(イ)3	① サービスには、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。	N/A
3.2.3	(ウ)(a)1	① e-文書法の対象となる医療情報を含む文書等の作成に PC等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・医療機関等の職務権限等に応じたアクセス制御の可否を含め、入力者及び確定者の識別及び認証に関する仕様	N/A
3.2.3	(ウ)(a)2	① e-文書法の対象となる医療情報を含む文書等の作成に臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムを利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・サービスとの連携におけるインタフェースの構築に関する役割分担	N/A
3.2.3	(ウ)(b)1	① e-文書法の対象となる医療情報を含む文書等の作成に PC等の汎用入力端末を利用する場合、以下の事項について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ・確定された登録情報（入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時）に関する仕様 ・入力された内容についての記録確定前における確認の可否等についての仕様 ・記録の確定権限に関する仕様 ・確定した記録の追記・削除の機能等に関する仕様 ・確定した記録の原状回復の機能等に関する仕様 ・記録の自動確定機能等に関する仕様 ・代替的な確定権限の機能等に関する仕様	N/A
3.2.3	(ウ)(c)1	① 真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新前と更新後のデータが保存される、又は更新履歴等が保存される等、更新前後の内容を照らし合せることができる機能を含める。	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。
3.2.3	(ウ)(c)2	① 真正性が求められる医療情報を取り扱うサービスには、一旦確定した診療録等を更新する時に更新履歴が保存され、更新の順序性が識別できる機能を含める。	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。
3.2.3	(ウ)(d)	① 真正性が求められる医療情報を取り扱うサービスにおける代行入力を実施するアカウント及び権限設定に関する機能や運用方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 真正性が求められる医療情報を取り扱うサービスには、代行入力の内容（代行者及び被代行者、代行対象となった記録、代行の日時等）を記録する機能を含める。 ③ 真正性が求められる医療情報を取り扱うサービスには、代行入力後の確定操作(承認)に関する機能を含める。	N/A
3.2.3	(エ)1	① 情報システムへのアクセスを記録し、一定期間保存する。 ② アクセス記録には、アクセスした ID、アクセス時刻、アクセス時間、アクセス対象（情報主体単位）等を含める。 ③ アクセス記録の機能を有しない場合には、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④ 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、診療録等に関するアクセス記録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。 ⑤ ④で定める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、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、本項におけるアクセス記録の管理方法については、サービス仕様適合開示書で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。 ⑥ 情報システム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。 ⑦ ⑥に関する情報の医療機関等への提供について、サービス仕様適合開示書に基づき、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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.3	（エ）2	① アクセス記録が保存されている資源に対して、アクセス制限を行い、不正なアクセスを防止する。 ② アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る。 ③ アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる。	Google は ISO27001 認証を受けています。この基準では、「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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
3.2.3	（エ）3	① アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、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 はすべての内部のシステムクロックを原子時計と GPS に同期させ、独自の NTP サービスを実行しています。 Google は公共 NTPサービス https://developers.google.com/time を通してお客様が利用できるようにしています。
3.2.3	（オ）1	① 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。 ② 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。 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、サービス仕様適合開示書に基づき、医療機関等と合意する。 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する、あるいは強制ログオフを行うことができるようにする。 ⑤ 医療機関等における利用者端末への④の措置の具体的な適用について、サービス仕様適合開示書に基づき、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、「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
3.2.3	（カ）1	① 情報システムの構築に際しては、ウイルスやマルウェア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。 ② ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新する。 ③ 情報システムの構築に際して、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、必ず事前に最新のウイルス対策ソフト等の導入を行う。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。 ④ サービス利用環境がウイルス等による攻撃を受けた場合に、サービス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。 ⑤ 情報システム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。
3.2.3	（カ）2	① 外部のネットワークと医療情報を格納する機器との接続に際しては、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。 ② 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を検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる。 ③ 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。 ④ ホスティングの利用時等、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。
3.2.3	（キ）	① 医療機関等がサービスを利用する際の、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、サービス仕様適合開示書に基づき、医療機関等と合意する。	N/A
3.2.3	（ク）1	① 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。 ② 医療機関等がサービスを利用する際に、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、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 情報システム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。 ④ ③において、他の事業者が提供するクラウドサービス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。仮想化技術によるクラウドサービスを利用する場合には、クラウドサービス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。 ⑤ ③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。 ⑥ サービスに係る委託先に対しても、③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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
3.2.3	（ク）2	① 3. 2. 1（2）（ウ）4. ①において実施するリスク分析結果に基づき情報システム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。 ② ①に従い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、記録内容の改ざん･破壊等がないことを確認する。 ③ 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／ディスクの別、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。 ④ ③の対象となるバックアップの記録媒体につき、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。 ⑤ ①～④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。 ⑥ バックアップに係る情報の提供について、サービス仕様適合開示書に基づき、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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.3	(ク)3	① 情報システム、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。 ② 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。 ③ ①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、サービス仕様適合開示書に基づき、医療機関等と合意する。 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、サービス仕様適合開示書に基づき、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、「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、自然災害や人為的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内 DR プログラムを確立しています。 Google Cloud 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。
3.2.3	(ク)4	① 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。 ② ①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。 ③ ②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、サービス仕様適合開示書に基づき、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、自然災害や人為的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
3.2.3	(ク)5	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。 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、「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、自然災害や人為的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内 DR プログラムを確立しています。 Google Cloud 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。
3.2.3	(ケ)1	① 情報システムにおける機器及びソフトウェアの構成図を作成する。 ② 情報システムのネットワーク構成図を作成する。 ③ 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。 ④ 情報システム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。 ⑤ 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、サービス仕様適合開示書に基づき、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 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。
3.2.3	(ケ)2	① サービスに供する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。 ② サービスに供する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。 ③ サービス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。 ④ 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、「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。
3.2.3	(コ)1	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、クラウドサービス事業者の役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	N/A
3.2.3	(コ)2	① IoT機器の利用を含むサービスを提供する場合、医療機関等との責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 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。 ③ 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。	N/A
3.2.4	(ア)1	① サービスの提供に従事する要員(被用者、派遣従業者等)については、守秘義務に関する内容を、雇用契約又は派遣契約に含めるか、就業規則等に含める。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.4	（ア）2	① サービスの提供に従事する要員に対して、個人情報保護ポリシー及び個人情報の安全管理に関する教育・訓練を行う。 ② この教育・訓練は就業開始時及び就業後定期的に行う。	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。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で　Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ　チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
3.2.4	（ア）3	① サービスの提供に従事する要員が退職した場合の、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。 ② サービスの提供に従事する要員が業務上管理していた個人情報については、離職時（内部の異動含む）に返却を求め、システム管理者が返却されたことを確認する。 ③ サービスの提供に従事する要員の退職時又は契約終了時以降の守秘義務について、上記2.における教育・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。
3.2.4	（ア）4	① 上記1.～3.に違反した被用者、派遣事業者等に対して、適切なペナルティを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。	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。
3.2.4	（ア）5	① サービスの提供に従事する要員に対する教育・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、サービス仕様適合開示書に基づき、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。
3.2.4	（イ）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、当該再委託に係る契約において体制を明確にする。 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。 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。 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。 ⑤ 再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.5	（ア）1	① サービスに供する情報を格納する機器、媒体等を破棄する手順に、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。 ② 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。 ③ ①で講じる措置及び②の資料を提供するのに必要な条件等について、サービス仕様適合開示書に基づき、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。
3.2.5	（ア）2	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、当該再委託に係る契約において体制を明確にする。 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。 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。 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。 ⑤ 再委託先が、本ガイドラインに規定する安全管理対策を行っ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。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、 Google は顧客サポートやテクニカル　サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ サプライヤーを利用するこ とがあります。サードパーティ　サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
3.2.6	（ア）1	① 情報システムの保守に従事する者及び管理者権限を有する者が、その業務の目的で該当情報システムにアクセスする場合には、当該要因ごとに発行されたアカウントにより、アクセスを行う。 ② ①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。
3.2.6	（ア）2	① 情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが漏洩しないよう厳重に管理する。	N/A
3.2.6	（イ）1	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、情報システムへの不正な侵入が生じないよう安全管理措置を講じる。 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。 ③ サービス提供に必要な情報システムの保守をリモートメンテナンスで行う場合、サービス仕様適合開示書に基づき、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。
3.2.6	（イ）2	① 情報システム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。 ② 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。
3.2.6	（イ）3	① 情報システム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、サービス仕様適合開示書に基づき、医療機関等と合意する。	N/A
3.2.6	（イ）4	① 情報システム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、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② ①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。 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。 ④ ③に定めた手順を医療機関等に示し、サービス仕様適合開示書に基づき、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、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤ ④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、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑥ 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、サービス仕様適合開示書に基づき、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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.6	(ウ)1	①情報システムの動作確認に際しては、原則として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。 ②情報システムの動作確認に際し、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、3.2.4で示す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。 ③情報システムの動作確認に際し、受託した個人情報をやむを得ず使用する場合について、サービス仕様適合開示書に基づき、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。
3.2.6	(ウ)2	①　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、医療機関等又はクラウドサービス事業者等（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。 ②　①で定める手順及び情報の提供条件について、サービス仕様適合開示書に基づき、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。
3.2.6	(エ)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。 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、サービス仕様適合開示書に基づき、医療機関等と合意する。	N/A
3.2.6	(エ)2	①　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情報システムに備える。 ②　①に示す機能等を備えることが困難な場合の情報システム更新・移行の手順について、サービス仕様適合開示書に基づき、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。
3.2.6	(エ)3	①　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。 ②　①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。 ③　②は、他の情報システム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、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④　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、3．4に示す対策を講じる。	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。
3.2.6	(エ)4	①　サービスに供する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。 ②　サービスに供する情報システムについて、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。 ③　サービスに供する情報システムについて、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。 ④　③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、サービス仕様適合開示書に基づき、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。
3.2.6	(エ)5	①　医療情報を取り扱うサービスに供する情報システム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。 ②　他のクラウドサービス事業者が提供するクラウドサービスを用いて、サービスを提供する場合には、他のクラウドサービス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、他のクラウドサービス事業者のクラウドサービスの停止・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、「４．サービスに供する機器の劣化対策」②～④に示す対応策を講じる。 ③　医療情報を取り扱うサービスに供する情報システムに係る機器若しくはソフトウェア等の更新を行う場合、又は利用する他のクラウドサービス事業者のクラウドサービスの変更を行う場合には、①、②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、「供給者関係」(ISO 27001 2013、附属書 A.15)が規定されています。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、　Google は顧客サポートやテクニカル　サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ サプライヤーを利用するこ とがあります。サードパーティ　サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
3.2.6	(オ)1	①　情報システム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、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.6	(オ)2	①　情報システムの保守に関して、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。 ②　①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 Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.7	(ア)1	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。 ②　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。 ③　①で定める内容について、サービス仕様適合開示書に基づき、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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.7	(ア)2	① サービスに供する記録媒体・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 ・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ざんが生じないようにするための具体的な措置(マルウェア対策、暗号化、ファイアウォール導入等))	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。
3.2.7	(ア)3	①「2.サービスに供する記録媒体・記録機器に関する対応」に示した内容に関する教育を従業員等に対して行う。 ② 上記の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。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で　Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ　チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
3.2.7	(ア)4	①「2.サービスに供する記録媒体・記録機器に関する対応」、「 3.従業員等及び委託先に対する対応」に示す情報の持ち出しに関する運用管理規程等における対応について、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.7	(イ)	① サービスに関する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。
3.2.7	(ウ)1	① サービスに供する機器等については、起動パスワードの設定を行う。 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。 ③ サービス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。 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。
3.2.7	(ウ)2	① サービスに関する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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
3.2.7	(ウ)3	① サービス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。 ② サービス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。	N/A
3.2.7	(ウ)4	① 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禁止する。 ② 利用者が個人所有する機器によるサービス利用に関する対応策については、サービス仕様適合開示書に基づき、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えい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。	Google のデバイスポリシーは、アプリケーションのインストールを含む、モバイルデバイス上のユーザーとデバイスの動作を制限します。高度な用途では、制限付きアプリストアを含むワークプロファイルが必要です。
3.2.7	(ウ)5	① 業務上、サービス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。	N/A

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.8	(ア)1	① 障害等が生じた場合の責任分界を明確にした上で、稼動を保証するサービスの範囲について、サービス仕様適合開示書に基づき、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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
3.2.8	(ア)2	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、サービス仕様適合開示書に基づき、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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
3.2.8	(ア)3	① 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、サービス仕様適合開示書に基づき、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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
3.2.8	(ア)4	① 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、サービス仕様適合開示書に基づき、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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。
3.2.8	(ア)5	① 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 ）をサービスに含めること及びこれに必要なセキュリティ等の情報提供について、サービス仕様適合開示書に基づき、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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.8	(イ)1	①　サービスに係るBCP及びコンテンジェンシープランの策定を行う。 ②　①で策定するBCP及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める。 ③　①で策定したBCP及びコンテンジェンシープランに基づくサービス内容について、サービス仕様適合開示書に基づき、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、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内 DR プログラムを確立しています。 Google Cloud 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。
3.2.8	(イ)2	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、サービス仕様適合開示書に基づき、医療機関等と合意する。 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。 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。 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も、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
3.2.8	(イ)3	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。 ②　①の場合において、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。 ③　①の場合において、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、サービス仕様適合開示書に基づき、医療機関と合意する。 ④　③で定める、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 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。
3.2.8	(イ)4	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、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内 DR プログラムを確立しています。 Google Cloud 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。
3.2.9	(ア)1	①　ネットワークにおいて、情報の盗聴、改ざん、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。 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。 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、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④　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ざんに対する防護措置に関するクラウドサービス事業者の役割の範囲について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤　医療機関等がチャネル・セキュリティの確保を閉域ネットワークの採用に期待する場合、サービスの閉域性の範囲に関する情報について、サービス仕様適合開示書に基づき、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。
3.2.9	(ア)2	①　医療機関等からクラウドサービス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。 ②　①において、医療機関等が外部接続するサーバ等とクラウドサービス事業者のサーバとの間の相互認証を行う。 ③　①について、事業者が保守業務を再委託している場合には、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。 ④　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、サービス仕様適合開示書に基づき、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。
3.2.9	(ア)3	①　ルータ等のネットワーク機器は、ISO15408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。 ②　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クラウドサービス事業者の役割分担について、サービス仕様適合開示書に基づき、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。
3.2.9	(ア)4	①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。 ②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。 ③②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、サービス仕様適合開示書に基づき、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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。

厚生労働省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.2.9	（ア）5	① 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。 ② SSL-VPNは、原則として使用しない。 ③ 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。 ④ 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、サービス仕様適合開示書に基づき、医療機関等と合意する。	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。
3.2.9	（ア）6	① 回線の管理、品質等に対するクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、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。
3.2.9	（ア）7	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クラウドサービス事業者の役割分担等につき、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google は、Google のセキュリティおよびプライバシーポリシーの遵守についてプロバイダと契約上合意しており、コンプライアンスを決定するためのベンダー監査プログラムを持っています。
3.2.9	（イ）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。 情報セキュリティの監督管理体制は、セキュリティに対するベンダーの取り組みなど、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google では、サービス実施のためのほぼすべてのデータ処理を直接行っています。ただし、 Google は顧客サポートやテクニカル サポートなど、Cloud Platform に関連するサービスを提供するためサードパーティ サプライヤーを利用するこ とがあります。サードパーティ サプライヤーと提携する前に、Google はサードパーティ サプライヤーのセキュリティおよびプライバシー対策について評価を行います。これにより、データへのアクセスや、担当するサービスの範囲に適した水準のセキュリティやプライバシーが確保されていることを確認します。Google はサードパーティ サプライヤーに付随するリスクを評価した上で、所定のセキュリティ、機密保持、プライバシーの各契約を締結することをサプライヤーに義務付けています。
3.2.9	（ウ）1	① 通常運用時及び非常時の医療機関等と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、事業者の負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 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、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 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、事業者が負う責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.9	（ウ）2	① 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、クラウドサービス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、サービス仕様適合開示書に基づき、医療機関等と合意する。 ② 医療情報を患者等の閲覧に供する場合に、医療機関等及び患者等の閲覧環境において対応すべきセキュリティ上の対応に係る情報の提供条件、内容等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 患者等が情報を閲覧する情報システムのセキュリティに関する説明責任等におけるクラウドサービス事業者の責任の範囲、役割等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.2.10	（ア）	① 法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合に、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へ対応することの可否を、医療機関等に対して明らかにする。 ② 保健医療福祉分野 PKI 認証局の発行する電子証明書以外の、電子署名法における認定認証事業者が発行する電子証明書を用いて、法令で定められた記名・押印を電子署名で行うサービスを提供する場合には、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。なお、電子署名法の規定に基づく認定認証事業者の発行する電子証明書を用いなくても「電子署名及び認証業務に関する法律（平成 12 年法律第102 号）」第2 条1 項の要件を満たすことは可能であることから、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能であることを担保して、認定認証事業者以外が発行する電子証書書を利用する場合には、上記要件を担保できることを示して、当該サービスにおける本人確認方法及び検証方法について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③ 公的個人認証サービスにおける署名用電子証明書を利用して、法令で定められた記名・押印を電子署名で行うサービスを提供する場合には、当該サービスにおける公的個人認証サービスに係る電子証明書の検証方法等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	N/A
3.2.10	（イ）	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、サービス仕様適合開示書に基づき、医療機関等と合意する。 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、サービス仕様適合開示書に基づき、医療機関等と合意する。 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、サービス仕様適合開示書に基づき、医療機関等と合意する。	N/A
3.2.10	（ウ）	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、サービス仕様適合開示書に基づき、医療機関等と合意する。	N/A
3.3.1		厚生労働省ガイドライン第 5版では、医療情報の外部保存を行うための指針等を「 8 診療録及び診療諸記録を外部に保存する際の基準」に示しており、クラウドサービス事業者が医療情報を取り扱う際もこれを満たすことが求められる。 またクラウドサービスによる外部保存は、電子保存であり、この場合には厚生労働省ガイドライン第 5版「7電子保存の要求事項について」に示される真正性、見読性、保存性を満たすことが求められる。	N/A
3.3.2		外部保存の要求事項が求められる文書は、厚生労働省ガイドライン第 5版の3.2章に示されているとおり、外部保存改正通知で定められた表 1に示す文書が対象となる。 また、表1に示す文書等がその法定保存年限が経過した等の事由によって、施行通知26や外部保存改正通知の対象外となった場合にも、外部保存を実施（継続）する場合には、第 7章～第9章に準じて取り扱うことが求められる（厚生労働省ガイドライン第5版3.4章）。	N/A
3.3.3	【医療機関等に保存する場合】	（1）入力者及び確定者の識別及び認証	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。
		（2）記録の確定手順の確立と、識別情報の記録	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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
		(3) 更新履歴の保存	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。
		(4) 代行入力の承認機能	N/A
		(5) 機器・ソフトウェアの品質管理	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。
	【ネットワークを通じて医療機関等の外部に保存する場合】	(1) 通信の相手先が正当であることを認識するための相互認証をおこなうこと	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書　A.12.2) が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、　SOC 2、Type II の報告書を取得しています。 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。
		(2) ネットワーク上で「改ざん」されていないことを保証すること	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書　A.12.2) が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、　SOC 2、Type II の報告書を取得しています。 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。
		(3) リモートログイン機能を制限すること	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9) が規定されています。 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。 監視ツールは、事前定義された基準に基づいて運用担当者に自動アラートを送信します。インシデントはポリシーごとにエスカレートされます。
3.3.4	【保存する場所について共通する内容】	(1) 情報の所在管理	Google は ISO27001 認証を受けています。この基準では、「アクセス制御」(ISO 27001 2013、附属書 A.9) が規定されています。 論理的なアクセス制御をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。 お客様のデータにアクセスできるのは、ごく限られた　Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査　記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート　サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。　Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
		(2) 見読化手段の管理	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2) と「バックアップ」(ISO27001 2013、附属書 A.12.3) が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって　1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、　Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト (G Suite、Google Cloud Platform) では、RPO (目標復旧時点) の目標も、RTO (目標復旧時間) の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に　2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
		(3) 見読目的に応じた応答時間	Google は、お客様に稼働時間グラフと業界標準の監査レポートおよび認証を提供します。
		(4) システム障害対策としての冗長性の確保	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2) と「バックアップ」(ISO27001 2013、附属書 A.12.3) が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって　1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、　Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト (G Suite、Google Cloud Platform) では、RPO (目標復旧時点) の目標も、RTO (目標復旧時間) の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に　2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
	【医療機関等に保存する場合】	(1)バックアップサーバ	Google は ISO27001 認証を受けています。この基準では、「冗長性」(ISO27001 2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12.3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
		(2)見読性確保のための外部出力	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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
		(3)遠隔地のデータバックアップを使用した見読機能	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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
	【ネットワークを通じて外部に保存する場合】	(1)緊急に必要になることが予測される診療録等の見読性の確保	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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
		(2)緊急に必要になるとまではいえない診療録等の見読性の確保	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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.3.5	【医療機関等に保存する場合】	(1) ウイルスや不適切なソフトウェア等による情報の破壊及び混同等の防止	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。
		(2) 不適切な保管・取扱いによる情報の滅失、破壊の防止	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"
		(3) 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止	Google は ISO27001 認証を受けています。この基準では、「冗長性」(　ISO27001 2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12.3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
		(4) 媒体・機器・ソフトウェアの整合性不備による復元不能の防止	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。 データの整合性を保証するために、整合性チェックがアプリケーションレベルとファイルシステムレベルで実行されています。
		(1) 不適切な保管・取扱いによる情報の滅失、破壊の防止	Google は ISO27001 認証を受けています。この基準では、「冗長性」(　ISO27001 2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12.3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
		(2) 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止	Google は ISO27001 認証を受けています。この基準では、「冗長性」(　ISO27001 2013、附属書 A.17.2)と「バックアップ」(ISO27001 2013、附属書 A.12.3)が規定されています。システムの可用性と完全性に関する統制についても、第三者機関による審査と検証を受け、 SOC 2、Type II の報告書を取得しています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されています。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
	【ネットワークを通じて医療機関等の外部に保存する場合】	(1)データ形式及び転送プロトコルのバージョン管理と継続性の確保をおこなうこと	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。 データの整合性を保証するために、整合性チェックがアプリケーションレベルとファイルシステムレベルで実行されています。
		(1)ネットワークや外部保存を受託する機関の設備の劣化対策をおこなうこと	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。 データの整合性を保証するために、整合性チェックがアプリケーションレベルとファイルシステムレベルで実行されています。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
		(1)ネットワークや外部保存を受託する機関の設備の互換性を確保すること	Google は ISO27001 認証を受けています。この基準では、「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。 データの整合性を保証するために、整合性チェックがアプリケーションレベルとファイルシステムレベルで実行されています。
3.3.6	(ア)	①　サービスの提供に係る契約に際して、医療機関等の求めに応じて、以下の情報の提供を行う。 ・医療情報等の安全管理に係る基本方針・取り扱い規程等の整備状況 ・医療情報等の安全管理に係る実施体制の整備状況 ・実績等に基づく個人データ安全管理に関する信用度 ・財務諸表等に基づく経営の健全性	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.3.6	(イ)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。 ②　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。 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。 ④　①～③における閲覧に係る範囲、手順等について、サービス仕様適合開示書に基づき、医療機関等と合意する。また②、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同様です。お客様のデータにアクセスできるのは、ごく限られた Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー ツールによって管理され、すべての変更の監査 記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。 Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
3.3.6	(イ)2	①　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。 ②　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 Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.3.6	(ウ)1	①　受託した医療情報の解析･分析は、サービス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。 ②　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。	N/A
3.3.6	(ウ)2	①　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。 ②　①の内容を、サービス提供に係る契約に含める。 ③　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、3．2．3及び3．2．9に示す対応策を講じる。 ④　③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。 ⑤　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。 ⑥　①～⑤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、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.3.7	(ア)	①　個人情報保護対応策を、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.3.7	(イ)	①　医療機関等が患者等に対して行う個人情報等の外部保存に関する説明に必要な資料の提供とその範囲、役割分担等について、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.4.1		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、サービスを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。 ②　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、サービス仕様適合開示書に基づき、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、サービス仕様適合開示書の内容を変更する場合には、①に準じた対応策を講じる。 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関等と合意する。なお、返却するデータに、クラウドサービス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、サービス仕様適合開示書に基づき、医療機関等と合意する。 ④　①においてサービスの変更を含むサービス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、②の対応は除く）、条件等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑤　医療機関等の都合により医療機関等のサービス利用が終了する場合も、②、③に示す対応策を講じる。 ⑥　サービス提供の停止又は医療機関等におけるサービス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。 ⑦　⑥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、期間、記録の管理方法、安全管理措置、連絡先等について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ⑧　①～⑦についての手順等を、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、「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。
3.5.2		①　オンライン診療システムにおいて、医療情報システムとの接続がある場合には、本ガイドラインの「3.2」～「3.4」の要求事項を、オンライン診療システムを提供するクラウドサービス事業者にも適用する。 ②　患者側端末で利用するオンライン診療システムの機能には、オンライン診療の実施中に医療情報システムと接続する機能等を含まないこと、及びこれに関する情報提供について、サービス仕様適合開示書に基づき、医療機関等と合意する。 ③　医師が利用するオンライン診療システムを提供するクラウドサービス事業者と患者との間の責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。	Google Cloud と G Suite は、クラウド プロバイダのための　ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.1		①PHRサービス事業者については、3．2．1～3．2．9、3．3．6～3．3．7に示す要求事項を以下のとおり読み替えるものとする。 ・「医療情報」→「PHRで利用する医療情報 31」 ・「医療機関等」→「患者等」 ・「クラウドサービス事業者」→「PHRサービス事業者」 ②PHRサービス事業者については、3．2．9（2）（イ）2.の①の要求事項における「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水準の高い「高セキュリティ型」に準じた適切な設定を行う」とある部分を、「TLS の設定は 1.2に限定し、信頼性の高い機関によって発行されたサーバ証明書を用いるとともに、本人性の確認を確実に実施する」と読み替えるものとする。 ③PHRサービス事業者については、3．2．3（2）（ア）4.の③の要求事項における「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「 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。」とある部分を削除するものとする。 ④PHRサービス事業者については、3．3．6（2）（ウ）2．の①の要求事項における「患者本人を含め」とある部分を削除するものとする。 ⑤PHRサービス事業者については、3．2．1～3．2．9、3．3．6～3．3．7に示す要求事項のうち、3．6．3に掲げる要求事項を適用対象外とする。 ⑥PHRサービスの提供に際しては、以下の内容を含む手順を策定し、その手順に基づいて実施したことを確認する。 ・登録時の ID申請者である患者等の本人確認（実在性の確認） ・利用時の患者等の認証（利用者の本人確認） ・新たに受領した医療情報の患者等の IDへの紐づけ（患者本人の情報であることの確認） ⑦PHRサービス事業者については、3．2．1～3．2．9、3．3．6～3．3．7に示す要求事項のうち、上記①による読み替え後に「サービス仕様適合開示書に基づき、患者等と合意する」となる要求事項は適用対象外とし、それらの要求事項に代えて以下の対応を行うこととする。 ・PHRサービスで取り扱う個人情報に関して、患者等からの同意の取得方法について運用管理規程を策定する。その運用管理規程には、本ガイドラインを遵守して個人情報を取り扱う旨を含める。 ・PHRサービスの提供終了時又は契約終了時における患者等に関する医療情報の返却の範囲、方法、条件について、患者等とあらかじめ合意する。 ・患者等の指示により、医療機関等が（自ら管理する）医療情報を患者等が契約するPHRサービス事業者へ送付する場合において、 PHRサービス事業者と医療機関等との責任分界について、あらかじめ患者等に示す。 ・PHRサービスの提供に関する患者等との合意においては、この情報が個人情報保護法上の要配慮個人情報であることや消費者保護法等の適用を受ける可能性があることを勘案して、免責事項等の内容を定める。	N/A
3.6.2	（1）（ア）	サービスの提供についての管理責任を有する責任者を設置する。 ② 情報システムについての管理責任を負い、これについて十分な技術的能力及び経験を有する責任者（システム管理者）を設置する。 ③ サービスの提供に係る情報システムの運用に関する事務を統括する責任者を設置する。 ④ ①から③に掲げた責任者の任命・解任等のルールを策定する。	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 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。
3.6.2	（1）（イ）1	① サービス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、サービス提供に係る契約に含める。契約には、守秘義務に違反した　PHRサービス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患者等による監督に関する内容を含める。	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レビュー」（　ISO 27001 2013、附属書 A.18.2）が規定されています。 システムの可用性と完全性に関連する統制は、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、ISMSをサポートするために必要に応じてリスクアセスメントを実行します。
3.6.2	（1）（イ）2	① サービス提供に係る契約において、次項（ウ） 1.に定める運用管理規程等の内容、その他最新の関連法令等を遵守し、安全管理措置を実施する旨を明らかにする。	Google Cloud と G Suite は、クラウド プロバイダのための　ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.2	（1）（ウ）1	① 経営者は、自社における個人情報保護指針、プライバシーポリシー等について明確にする。 ② ①の指針等には個人情報保護法及び個人情報保護委員会のガイドラインに定める安全管理措置等を実施する旨を含める。 ③ ①の指針等には、個人情報保護法の対象外の情報（死者に関する情報等）であっても、PHRで利用する医療情報の特殊性から個人情報保護法における運用に準じて取り扱う旨を含める。 ④ 情報セキュリティに関する基本方針、運用管理規程等の情報セキュリティポリシーを策定する。 ⑤ 情報セキュリティポリシーの遵守を担保する組織体制の構築とその文書化を行う。	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ための方針群」（　ISO 27002 2013、附属書 A.5）と「情報セキュリティのための組織」（ ISO27002 2013、附属書 A.6）が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud 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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.6.2	(1)(ウ)2	① サービスの提供に係る体制を、緊急時の対応も含めて明確にする。	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 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。
3.6.2	(1)(ウ)4	① サービスに係るリスクの分析を行い、必要な対応措置等を講じる旨を定める。	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。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
3.6.2	(1)(ウ)5	① 機器等の管理方法について、文書化を行う。 ② 機器等について、台帳管理等により所在確認等を行う旨を定める。	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。
3.6.2	(1)(ウ)6	① 個人情報を記録した媒体の管理等に関する運用規程を策定する。	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。
3.6.2	(1)(ウ)8	① サービスを提供する情報システム、組織体制、運用等に関する監査の方針、内容等について明文化を行う。 ② 第三者が提供するクラウドサービスを利用する場合については、これに対する監査又は代替する対応についての方針、内容を明確にする。 ③ 監査実施について記録し、当該記録の保存･管理方法を明確にする。	Google は ISO27001 認証を受けています。この基準では、「情報システムの監査に対する考慮事項」(ISO 27001 2013、附属書 A.12.7)が規定されています。 情報セキュリティの監督管理体制は、社内監査の監督など、第三者機関によるレビューと検証を受け、　SOC 2、Type II の報告書を取得しています。
3.6.2	(1)(ウ)9	② 自社で契約した第三者が提供するクラウドサービスを利用してサービスを提供する場合でも、患者等からの問合せ窓口を一元化する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.2	(1)(エ)1	① PHRサービス事業者における情報システムへのアクセス権限、アカウント管理、認証及びアクセス等に対する記録の収集と保存、並びに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等を内容とするアクセス管理規程を策定する。 ② サービスの提供に係るアクセス記録(外部からのアクセス、利用者によるアクセス等を含む)の保存、記録の定期的なレビューと改善を実施する旨を内容とするアクセス管理規程を策定する。	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。 Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
3.6.2	(1)(エ)2	① PHRで利用する医療情報の取扱いに関する委託契約に、以下の内容を含める。 ・個人情報に関して、他の情報と区別して適切に管理を行う。 ・PHRで利用する医療情報は、死者に関する情報についても個人情報に準じて取り扱う旨を明確にする。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.2	(2)(ア)1	① サービスに供する機器、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。 ② サービスに供するサーバ等を格納するラック等について、施錠管理を行う。 ③ サービスに供する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"

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.6.2	(2)(ア)2	① サービスに供する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。 ② サービスに供する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。 ③ サービスに供する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。 ④ サービスに供する機器や媒体の設置場所への不明者の入退を発見するために、入退者に名札等の着用を義務付ける。 ⑤ サービスに供する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。 ⑥サービスに供する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。 ⑦①～⑥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"
3.6.2	(2)(ア)3	① サービスに供する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、火災等並びにそれに伴う停電等）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。
3.6.2	(2)(ア)4	①サービスに供する機器等が保存されている建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等を設置する。 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。 ③サービスに供する機器、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"
3.6.2	(2)(イ)1	① 個人情報の表示中の覗き見を予防するために、運用端末に覗き見対策のシートを貼る等の対策を行う。 ② 運用中の画面が、運用者以外の者の視野に入らないような対応等を行う。	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
3.6.2	(2)(ウ)1	① 個人情報が物理的に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。 ② 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を取り付ける。 ③ 受託する個人情報を運用や保守に用いる端末に保存しない旨、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、「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。
3.6.2	(3)(ア)1	① 情報システム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。ただし当該情報システムが他の情報システムを利用するための ID（non interactive ID）は除く）。 ② 利用者のなりすまし等を防止するための認証を行う。 ③ 利用者には、患者等においてサービスを利用する者のほか、情報システム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も含める。 ④ 情報システム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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。　サポート サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.6.2	(3)(ア)2	① 本人の識別・認証に、ユーザ IDとパスワードを組み合わて用いる場合には、それらを、本人しか知り得ない状態に保つよう対策を行う。具体的には以下のような対策を行う。 ・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情報システムにアクセスできないようにする。 ・初期パスワード以外のパスワードは、利用者本人が設定し、本人しか知りえない内容に限定する。 ・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。 ② パスワード認証に係る以下のルールを実現する措置を講じる。 ・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。 ・パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない仕組みとする。 ③ パスワードには十分な安全性を満たす有効期間を設定する。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。 ④ 認証に際してID及びパスワードによらない場合でも、上記と同等以上の安全性を確保する。	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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
3.6.2	(3)(ア)3	①利用者のパスワードは、ハッシュ値での保存を行う等、暗号化して管理する。 ②サービスを提供する製品等の導入に際しては、初期パスワードを変更するだけでなく、アカウントの棚卸しを行い、不要なものについては削除を行う。 ③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。 ④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。 ⑤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。 ⑥利用者が設定する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、これに基づく運用を行う。 ⑦利用者の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。
3.6.2	(3)(ア)4	①情報システム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、2要素認証以上の認証強度のある方法による。 ③利用者の認証において、固定式の ID・パスワードによる認証方式を採用している場合には、固定式の 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。 ④ 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。 ⑤ 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。 ⑥ 代替的手段・手順により、情報システム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。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
3.6.2	(3)(イ)1	① PHRで利用する医療情報とそれ以外の情報を区分できる措置を講じる。 ② PHRで利用する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。 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。	N/A
3.6.2	(3)(イ)3	① サービスには、受託する PHRで利用する医療情報を患者等ごとに管理できる機能を含める。	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 G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート　サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。　Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
3.6.2	(3)(エ)1	⑥ 情報システム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。 監視ツールは、事前定義された基準に基づいて運用担当者に自動アラートを送信します。インシデントはポリシーごとにエスカレートされます。
3.6.2	(3)(エ)2	① アクセス記録が保存されている資源に対して、アクセス制限を行い、不正なアクセスを防止する。 ② アクセス記録の保存に必要な容量を十分確保し、可用性、完全性の確保を図る。 ③ アクセス記録を暗号化する、あるいは定期的に追記不能な媒体への記録を行う等、改ざん防止の措置を講じる。	Google は ISO27001 認証を受けています。この基準では、「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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
3.6.2	(3)(エ)3	① アクセス記録の時刻の信頼性を確保するために、情報システムの時刻と、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 はすべての内部のシステムクロックを原子時計と　GPS に同期させ、独自の NTP サービスを実行しています。 Google は公共 NTPサービス https://developers.google.com/time を通してお客様が利用できるようにしています。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.6.2	(3)(オ)1	① 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。 ② 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。 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する、あるいは強制ログオフを行うことができるようにする。	Google は ISO27001 認証を受けています。この基準では、「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
3.6.2	(3)(カ)1	① 情報システムの構築に際しては、ウイルスやマルウェア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。 ② ウイルス対策ソフトのパターン定義ファイルを常に最新のものに更新する。 ③ 情報システムの構築に際して、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、必ず事前に最新のウイルス対策ソフト等の導入を行う。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。 ④ サービス利用環境がウイルス等による攻撃を受けた場合に、サービス提供に係る影響について、速やかに患者等に周知し、必要な対応等を求める。 ⑤ 情報システム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。
3.6.2	(3)(カ)2	① 外部のネットワークとPHRで利用する医療情報を格納する機器との接続に際しては、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。 ② 患者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を検出する、あるいは不正なトラフィックの遮断を行う等の措置を講じる。 ③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。 ④ ホスティングの利用時等、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。
3.6.2	(3)(ク)2	① 3. 2. 1(2)(ウ)4. ①において実施するリスク分析結果に基づき情報システム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。 ② ①に従い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、記録内容の改ざん･破壊等がないことを確認する。 ③ 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／ディスクの別、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。 ④ ③の対象となるバックアップの記録媒体につき、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。 ⑤ ①～④の手順を運用管理規程等に含め、従業者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 G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト（G Suite、Google Cloud Platform）では、RPO（目標復旧時点）の目標も、RTO（目標復旧時間）の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 Google Cloud 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。
3.6.2	(3)(ケ)1	① 情報システムにおける機器及びソフトウェアの構成図を作成する。 ② 情報システムのネットワーク構成図を作成する。 ③ 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。 ④ 情報システム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 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。
3.6.2	(1)(ウ)3	① 情報セキュリティに関する基本方針や運用管理規程等、重要な文書の作成や管理に関する規程を策定し、これに基づき文書の管理を行う。 ② サービスの運用や資源管理に関して、適切に文書化を行い、セキュリティ情報として管理する。	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。
3.6.2	(3)(ケ)2	① サービスに供する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。 ② サービスに供する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。 ③ サービス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。 ④ 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、「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。
3.6.2	(4)(ア)1	① サービスの提供に従事する要員（被用者、派遣従業者等）については、守秘義務に関する内容を、雇用契約又は派遣契約に含めるか、就業規則等に含める。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.6.2	(4)(ア)2	① サービスの提供に従事する要員に対して、個人情報保護ポリシー及び個人情報の安全管理に関する教育・訓練を行う。 ② この教育・訓練は就業開始時及び就業後定期的に行う。	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。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で　Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ　チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
3.6.2	(4)(ア)3	① サービスの提供に従事する要員が退職した場合の、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。 ② サービスの提供に従事する要員が業務上管理していた個人情報については、離職時(内部の異動含む)に返却を求め、システム管理者が返却されたことを確認する。 ③ サービスの提供に従事する要員の退職時又は契約終了時以降の守秘義務について、上記2.における教育・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。
3.6.2	(4)(ア)4	① 上記1.～3.に違反した被用者、派遣事業者等に対して、適切なペナルティを課すことを、雇用契約又は派遣契約に含めるか、就業規則等に含める。	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。
3.6.2	(4)(イ)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。 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。 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。 ⑤ 再委託先が、本ガイドラインに規定する安全管理対策を行っていることを確認する。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/
3.6.2	(5)(ア)2	① 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、サービス提供上の要否の確認を定期的に行うこと。 ・サービス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。 ・サービス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、患者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。
3.6.2	(6)(ア)1	① 情報システム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情報システム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。 ② ①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。 監視ツールは、事前定義された基準に基づいて運用担当者に自動アラートを送信します。インシデントはポリシーごとにエスカレートされます。
3.6.2	(6)(ア)2	① 情報システムの保守に従事する者及び管理者権限を有する者は、業務上用いるアカウントが漏洩しないよう厳重に管理する。	Google の社員は、機密保持契約を締結する必要があり、 Google の機密保持およびプライバシーポリシーを受領し、それに準拠していることを確認する必要があります。
3.6.2	(6)(イ)1	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、情報システムへの不正な侵入が生じないよう安全管理措置を講じる。 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。 監視ツールは、事前定義された基準に基づいて運用担当者に自動アラートを送信します。インシデントはポリシーごとにエスカレートされます。
3.6.2	(6)(イ)2	① 情報システム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。 ② 取得した操作ログ等により、アクセスされた PHRで利用する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。 監視ツールは、事前定義された基準に基づいて運用担当者に自動アラートを送信します。インシデントはポリシーごとにエスカレートされます。
3.6.2	(6)(ウ)1	① 情報システムの動作確認に際しては、原則として受託した個人情報を含むデータを使用せず、テスト用のデータを使用する。 ② 情報システムの動作確認に際し、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、3．2．4で示す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。	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。 監視ツールは、事前定義された基準に基づいて運用担当者に自動アラートを送信します。インシデントはポリシーごとにエスカレートされます。
3.6.2	(6)(ウ)2	①PHRで利用する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、患者等又は PHRサービス事業者等（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。
3.6.2	(7)(ア)1	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。 ② 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、「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。
3.6.2	(7)(ア)2	① サービスに供する記録媒体・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 ・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ざんが生じないようにするための具体的な措置（マルウェア対策、暗号化、ファイアウォール導入等））	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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.6.2	(7)(ア)3	①「2.サービスに供する記録媒体・記録機器に関する対応」に示した内容に関する教育を従業員等に対して行う。 ② 上記の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。 Google の全委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の委託業者は初期研修で　Google の行動規範に同意します。この行動規範では、Google が顧客情報を安全に保護する責務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ　チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。
3.6.2	(7)(イ)	① サービスに関する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。
3.6.2	(7)(ウ)1	① サービスに供する機器等については、起動パスワードの設定を行う。 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。 ③ サービス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。 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、一連のパスワードの作成、保護、および管理ガイドラインに従って管理されており、以下を強制します。 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。
3.6.2	(7)(ウ)2	① サービスに関する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 G Suite プロダクトの暗号化と鍵管理に関する詳細を公開しています。鍵管理と暗号化について詳しくは、次を参照してください https://cloud.google.com/security/encryption-at-rest/ https://storage.googleapis.com/gfw-touched-accounts-pdfs/google-encryption-whitepaper-gsuite.pdf Google Cloud 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。
3.6.2	(7)(ウ)3	① サービス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。 ② サービス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。	N/A
3.6.2	(7)(ウ)5	①業務上、サービス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。	N/A
3.6.2	(8)(イ)1	① サービスに係るBCP及びコンテンジェンシープランの策定を行う。 ② ①で策定するBCP及びコンテンジェンシープランには、非常時における体制及びサービス回復手順等の内容を含める。	Google は ISO27001 認証を受けています。この基準では、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。
3.6.2	(8)(イ)3	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。 ② ①の場合において、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、患者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、「情報セキュリティのための方針群」(ISO 27002 2013、附属書 A.5)と「情報セキュリティのための組織」(ISO27002 2013、附属書 A.6)が規定されています。 情報セキュリティ ポリシーの文書化をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google Cloud 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。
3.6.2	(8)(イ)4	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、「情報セキュリティ継続」(ISO 27001 2013、附属書 A.17.1)が規定されています。 Google プラットフォームのコンポーネントは、高度な冗長性を確保した設計になっています。この冗長性は、Google のサーバー設計、データ保存方法、ネットワークやインターネットの接続性、さらにソフトウェア　サービスにも適用されていま す。この「すべてに冗長性」の方針は、エラー処理を設計全体に組み込むという考え方にも生きており、これによって 1 台のサーバー、1 か所のデータセンター、1 件のネットワーク接続だけに依存しないソリューションが構築されています。 Google のデータセンターは、自然災害や局地的な停電といった地域的な障害の影響を最小限に抑えるために、地理的に分散しています。ハードウェア、ソフトウェア、ネットワークの障害が発生しても、自動的にデータが別の施設に切り替えられるため、 Google Cloud や G Suite のお客様の業務が中断されることはありません。 冗長性が高い Google のインフラストラクチャは、お客様をデータ損失から守ります。 Google Cloud プロダクト(G Suite、Google Cloud Platform)では、RPO(目標復旧時点)の目標も、RTO(目標復旧時間)の設計目標もゼロに設定しています。Google は、こうした目標をライブ レプリケーションまたは同期レプリケーションによって達成することを目指しています。 Google Cloud プロダクト内でお客様が行った操作は同時に 2 か所のデータセンターに複製されるため、一方のデータセンターに障害が発生しても、他方のデータセンターに転送されます。 また、不測の事態への対応など、しっかりとした社内　DR プログラムを確立しています。 Google Cloud 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。

総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版」			Google の回答
項目番号		ガイドライン	
3.6.2	(9)(ア)1	① ネットワークにおいて、情報の盗聴、改ざん、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。 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 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。
3.6.2	(9)(ア)3	① ルータ等のネットワーク機器は、ISO15408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。
3.6.2	(9)(ア)4	① 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。 ② 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。	データが、 Google によって管理されていない物理的な境界の外側または Googleに代わって移動する場合、Google は1つ以上のネットワークレイヤで転送中のすべてのデータを暗号化して認証します。以下を参照してください。 https://cloud.google.com/security/encryption-in-transit/ for more informaiton.
3.6.2	(9)(ア)5	① 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1.2に限定し、信頼性の高い機関によって発行されたサーバ証明書を用いるとともに、本人性の確認を確実に実施する。 ② SSL-VPNは、原則として使用しない。 ③ 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。	データが、 Google によって管理されていない物理的な境界の外側または Googleに代わって移動する場合、Google は1つ以上のネットワークレイヤで転送中のすべてのデータを暗号化して認証します。以下を参照してください。 https://cloud.google.com/security/encryption-in-transit/ for more informaiton.
3.6.2	(9)(イ)	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、「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。 Google Cloud Platform を使用しているお客様は、入力される情報の管理をサポートするためのプロセスの開発を含め、環境を構成および管理するためのすべての権利と責任を保持します。
3.6.2	(10)(イ)1	① 受託したPHRで利用する医療情報を保守・運用を行うために閲覧するのは必要最小限とする。 ② 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。 ③ 受託したPHRで利用する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。	N/A
3.6.2	(10)(イ)2	① 予定された保守・運用等を行う際に受託した PHRで利用する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。 ② 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。 データのプライバシーとセキュリティを確保するため、 Google はそれぞれのお客様のデータを他のお客様やユーザーから論理的に分離しています。実際には同じ物理サーバーに保存されている場合も同様です。お客様のデータにアクセスできるのは、ごく限られた　Google 社員のみです。Google 社員のアクセス権とアクセスレベルは職務上の役割を基準にしており、必要最小限の権限と情報のみを許可するという方針に基づいて、アクセス権を定義済みの職務に割り当てています。 Google 社員に付与される既定のアクセス権限は、社員用メールや Google 社員用の社内ポータルといった会社のリソースのみに、アクセスが制限されています。既定以上のアクセス権を要求する場合は、 Google のセキュリティ ポリシーの規定に従い、データまたはシステムのオーナー、マネージャー、またはその他の上級管理職者に要請して承認を得るといった公式の手順を経る必要があります。この承認はワークフロー　ツールによって管理され、すべての変更の監査　記録が維持されます。こうしたツールで認可設定の変更と承認プロセスの両方を管理することで、一貫性のある承認ポリシーの適用が保証されます。社員の承認設定は、 Google Cloud や G Suite に関連したデータやシステムを含む、すべてのリソースへのアクセス制御に使用されます。サポート　サービスは、複数の方法による本人確認を経た上で、正式に承認されたお客様の管理者に対してのみ提供されます。　Google 社員によるアクセスは、セキュリティ、プライバシー、内部監査を担当する社内の専任チームによってモニタリング、監査されます。 Google Cloud 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。
3.6.2	(10)(ウ)2	① 受託したPHRで利用する医療情報は、法令による場合又は患者等の指示に基づく場合を除き、第三者への提供は行わない。 ② ①の内容を、サービス提供に係る契約に含める。 ③ 患者等の指示に基づき、受託した PHRで利用する医療情報の第三者提供(閲覧)を行う場合には、患者等が許諾した者以外が閲覧・取得できないように、3．2．3及び3．2．9に示す対応策を講じる。 ④ ③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、患者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。 ⑤ 患者等の指示に基づいて受託した PHRで利用する医療情報の第三者提供を行った場合には、患者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。	Google Cloud と G Suite は、クラウド プロバイダのための ISO27017 認証を受けています。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://gsuite.google.com/intl/ja_ALL/terms/2014/1/premier_terms_apac.html SLA https://gsuite.google.com/terms/sla.html https://cloud.google.com/terms/sla/