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」は、医療情報システムの安全管理や e-文書法への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したものです。
また、医療情報システムの外部委託、またはインターネットを経由したクラウド型サービスを利用している医療機関などは、上記の厚生労働省のガイドラインのみでなく、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」、および経済産業省「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ガイドライン」が求める管理要件も考慮した上で、組織としての管理対策を検討しなければなりません。厚生労働省、総務省、経済産業省の 3 省が発行する上記 3 つのガイドラインは、「 3 省 3 ガイドライン」と総称されています。

以下は各ガイドラインの概要および関係性と Google が各ガイドラインに対して行っている対応についての説明です。

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）」
本ガイドラインは、医療機関（病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等）における電子的な医療情報の取扱いに係る責任者を対象とし、医療情報を扱うシステムの安全管理や e - 文書法への適切な対応を行うために必要な対策を示しています。

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」
本ガイドラインは、厚生労働省ガイドラインにおける医療機関側への要求事項を踏まえ、医療機関から委託を受けて医療情報を取り扱うクラウドサービス事業者（想定するクラウドサービスとして ASP ・ SaaS のほか、 PaaS 、 IaaS 等を含む）を対象とし、クラウドサービス事業者が医療情報を取り扱う際に求められる責任、安全管理対策、医療機関との合意形成の考え方を示しています。加えて医療・介護環境の変化に伴う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が対応すべき要求事項（オンラ

イン診療システムが医療情報システムと接続する場合）、および PHR サービス(Personal Health Record ：個人の医療情報を自身の健康管理等に活用するサービス) を提供するクラウド事業者への要求事項等についても整理し、必要な対策を示しています。

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」
本ガイドラインは、厚生労働省ガイドラインにおける医療機関側への要求事項を踏まえ、医療情報を受託管理する情報処理事業者を対象とし、情報処理事業者が実施すべき対策を規定しています。医療情報処理施設や装置の物理的安全対策、装置やソフトウエア、ネットワークの技術的安全対策、人的安全対策等が示されています。

各ガイドラインにおける主な安全管理策を①組織的安全管理策、②物理的安全対策、③技術的安全対策、④人的安全対策、⑤災害、サイバー攻撃等の非常時の対応、⑥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 6 つの要求事項に分類し、各要求事項への Google の対応状況を以下で説明します。

1. 「組織的安全管理策」では、組織・体制の整備、運用管理規定、運用管理規定に基づく各種文書類の整備等が求められています。Google では組織体制とポリシーが整備され、社員に公開されています。また、 Google は、データセンター運用、セキュリティ管理、システム及びハードウェアの変更管理、雇用、教育、人事評価、インシデントのエスカレーションなど、運用に関する正式な方針、手順、および職務説明を作成し、文書化しています。これらの方針や手順は、職務分掌に基づいて業務を実施するように設計されています。

2. 「物理的安全対策」では、機器の施錠管理や入退室管理等の物理的なアクセス制御等が求められています。Google Cloud Platform (GCP) のインフラストラクチャはセキュリティを中核に据えて設計されており、データセンターでは、物理的なセキュリティを確保するため多層セキュリティ モデルを採用しています。たとえ

ば、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が実施されています。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 24 時間 365 日稼働する高解像度の棟内外監視カメラが設置されており、侵入者の検知と追跡に対応します。

3. 「技術的安全対策」では、医療情報の情報区分に応じたアクセス制御、なりすまし対策、不正ソフトウェア対策、アクセス記録の取得・保存管理、データの暗号化等が求められています。Google は脆弱性管理、マルウェア防止、セキュリティ モニタリング、インシデント管理等の運用セキュリティを運用の中核をなす要素としています。Google Cloud Platform (GCP) は、安全運用を前提として設計および構築されたテクノロジー プラットフォームです。Google では、複数の暗号化レイヤを使用して、 Google Cloud 内のお客様の保存データを保護しています。

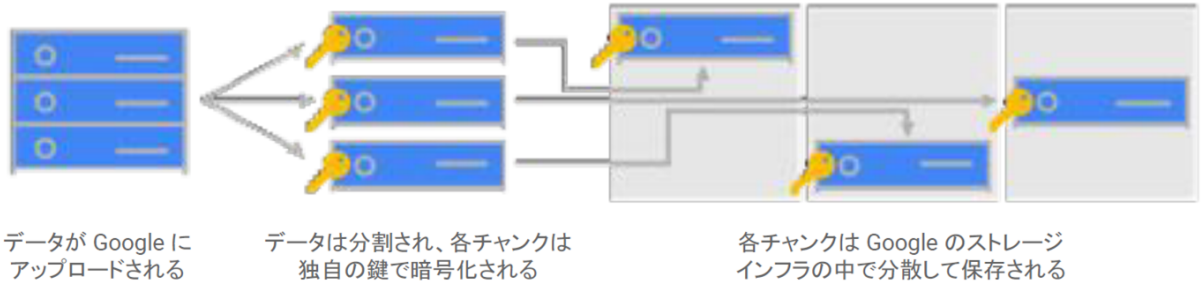
Google はセキュリティを最重視しており、情報処理ライフサイクル全域を通してセキュリティが確保できるよう、インフラストラクチャを設計しています。このインフラストラクチャによって、サービスのデプロイ、データストレージ、お客様のプライバシー保護、サービス間通信、インターネット経由の通信のセキュリティを確保するとともに、管理者オペレーションの安全性を提供しています。

Google の多段セキュリティモデル

利用	監査ログ	セーフブラウジングAPI	BeyondCorp	セキュリティキーの配布		
運用	コンプライアンスと第三者認証	ライブマイグレーションで、インフラメンテナンスやパッチ適用	インテリジェントな脅威分析	Open Source フォレンジックツール	異常検知 (インフラ)	インシデントレスポンス (インフラ)
デプロイ	TLS暗号化と perfect forward secrecy	Certificate Authority	無料かつ自動的な証明更新	DDoS 防御 (PaaS & SaaS)		
アプリ	ピアコードレビューと静的コード解析 (Infrastructure SLDC)	Source code provenance (Infrastructure)	バイナリ検証 (Infrastructure code)	WAF (PaaS と SaaS)	IDS/ IPS (PaaS & SaaS)	Web Application スキャナー (Google Services)
ネットワーク	データセンター間通信の RPC暗号化	DNS	Global プライベートネットワーク	Andromeda SDN コントローラ	Jupiter データセンターネットワーク	B4 SDN ネットワーク
ストレージ	データ保存時の暗号化	ロギング	Identity and Access Management	Global な鍵管理サービス		
OS と IPC	安全な KVM ハイパーバイザ	ホストやジョブ間の認証	キュレーションされたホストイメージ	サービス間通信の暗号化		
ブート	信頼できるブート	Cryptographic Credentials				
ハードウェア	独自設計のチップ	独自設計のサーバ	独自設計のストレージ	独自設計のネットワーク	独自設計のデータセンター	

また、 Google では顧客データの保護がコアビジネスの一部であり、最重要視するテーマです。Google のストレージ サービスにデータを保存する際には、中央の鍵管理サービスから取得した鍵を使用し、書き込み前のすべてのデータを暗号化することができます。また、 GCP サービス間の通信の際には、 GCP に最適化された独自の通信プロトコルを利用し、自動的に暗号化が行われています。

マネージド・サービスストレージ暗号化



Google では、お客様がデータの利用と共有を制御します。Google Cloud Trust Principles に基づき、お客様とお客様の顧客のデータのプライバシー保護に取り組んでいます。お客様のビジネス上のデータはお客様の指示によって処理され、 Google は G Suite および GCP のデータ処理規約を通じて契約責任に合意しています。

データの削除義務や委託先による復処理の透明性に関するコミットメントも提供しています。

4. 「人的安全対策」では、従業員に関する守秘義務規定、安全管理教育・訓練、入退室管理・アクセス記録の保存等が求められています。Google では、全社員を対象としたセキュリティ研修やセキュリティとプライバシーに関する研修を通じて強固で包括的なセキュリティ文化を築いています。

5. 「災害、サイバー攻撃等の非常時の対応」では、BCPの策定等が求められています。GCP の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、GCP 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。

6. 「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」では、セキュリティ水準の高いネットワークによる通信、不正トラフィックの遮断等が求められています。GCP では転送中のデータの信頼性、整合性、プライバシーを保証するため、複数のセキュリティ対策を採用しています。すべての転送データは、Google が管理している物理的境界または Google のために管理されている物理的境界の外へ出るときに、1 つ以上のネットワーク レイヤで暗号化され認証されます。

Google における管理環境の 3 省 3 ガイドラインに対する適合状況をお客様にご理解いただくため、Google は解説書を作成しました。この解説書で説明されている Google の管理のほとんどは、ISO 27001、ISO 27017 および ISO 27018 認証を含む、第三者監査コンプライアンス プ

ログラムで認定済みです。3 省 3 ガイドラインに対する Google の対応状況の詳細については、解説書をご覧ください。

Google のセキュリティやコンプライアンスへの対応状況の詳細に関しましては、以下をご参照ください。

・Google Cloud のセキュリティとコンプライアンスに関するホワイトペーパー
・Google インフラストラクチャのセキュリティ 設計の概要
・Google のセキュリティに関するホワイトペーパー