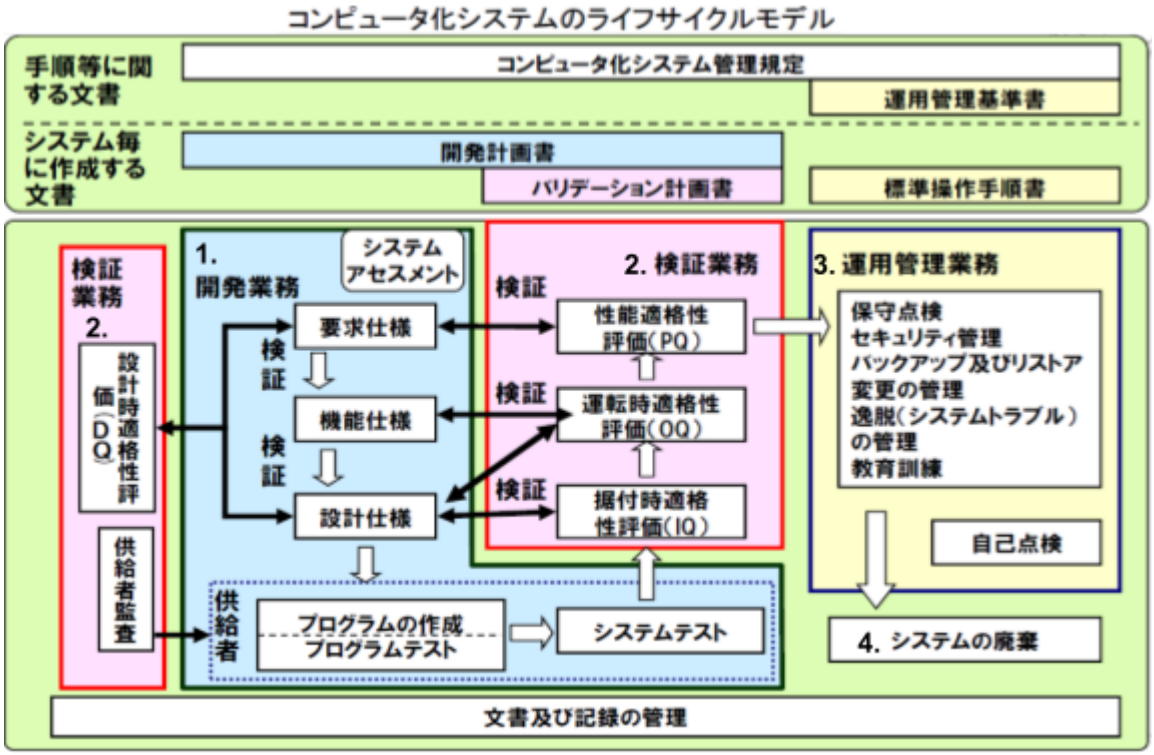
近年、製品の信頼性・安全性がより求められる製薬・医療機器業界においては、各種業務に使用されるコンピュータ化システムの品質や信頼性確保のための検証が必要不可欠なものとなっております。

医薬品やヘルスケア製品の製造に関する専門家等で構成された国際的な非営利団体であるISPE（国際製薬技術協会）では、コンピュータ化システムのバリデーション（CSV）を効率的に行うための実用的なガイダンスとして、GAMP（The Good Automated Manufacturing Practice）を発行、各国のGxP 規制におけるCSV 実施の参考文書として言及されるなど、CSV の実質的な国際的なガイドライン的な役割を担っております。

日本では、医薬品等の品質基準について定められた「医薬品、医薬部外品、化粧品及び再生医療等製品の品質管理の基準に関する省令」（厚生労働省令第136号　GQP 省令）及び「医薬品及び医薬部外品の製造管理及び品質管理の基準に関する省令」（厚生労働省令第179号　GMP 省令）において、製造・品質管理における信頼性の確保のため、バリデーションの実施が求められております。また、これらの省令に基づく業務を行うコンピュータ化システムのバリデーションの実施に関するガイドラインとして、2010年10月に厚生労働省により「医薬品・医薬部外品製造販売業者等におけるコンピュータ化システム適正管理ガイドライン」（新適正管理ガイドライン）が示され、2012年4月より適用開始となりました。

新適正管理ガイドラインでは、システムの開発・検証・運用・廃棄の各業務からなるコンピュータ化システムのライフサイクルモデルをベースに、システムの利用者である医薬品・医薬部外品の製造販売業者が実施すべき内容が定められております。Google は、Google Cloud Platform (GCP) 上のセキュリティ対策を行い、高可用性や冗長性を備えた仮想化環境を提供していますが、当ガイドラインの基本的な方針としては、コンピュータ化システムの利用者自らがシステム開発や検証に係る定義・文書化、ならびにコンピュータ化システムの開発・運用を実施するものとなります。



出典：医薬品・医薬部外品製造販売業者等におけるコンピュータ化システム適正管理ガイドライン

コンピュータ化システムのライフサイクルにおける各業務（1. 開発業務、2. 検証業務、3. 運用管理業務、4. システムの廃棄）のシステム利用者への要求事項、および Google の対応状況は以下の内容になります。

1 開発業務において、製造販売業者等は、コンピュータ化システムの開発計画や仕様の定義、テストの実施等の各開発業務の文書化が求められています。
GCP は、検証テストを実施するための仮想環境を有しており、検証テストの完了後にそのまま本番環境に移行させることができるなど、柔軟かつ効率的なシステム検証および拡張が可能です。

2 検証業務において、製造販売業者等は、バリデーション方針や体制等を含む全体計画を策定後、設計時・据付時・運転時の各段階、ならびに性能に関する適正評価の実施や結果の文書化が求められています。

Google Cloud

Google は、上記 1 において記載した通り、開発業務における検証環境の提供を通じて、柔軟かつ効率的な検証の実施をサポートしております。

3 運用管理業務において、製造販売業者等は、運用管理に関する体制や方針、実施内容について定めた基本文書を作成するとともに、当文書に基づき保守点検・変更管理・障害対応等のシステム運用管理、およびアクセス権限の設定や不正アクセス防止措置を含むセキュリティ管理を実施し、記録を作成することが求められています。
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。

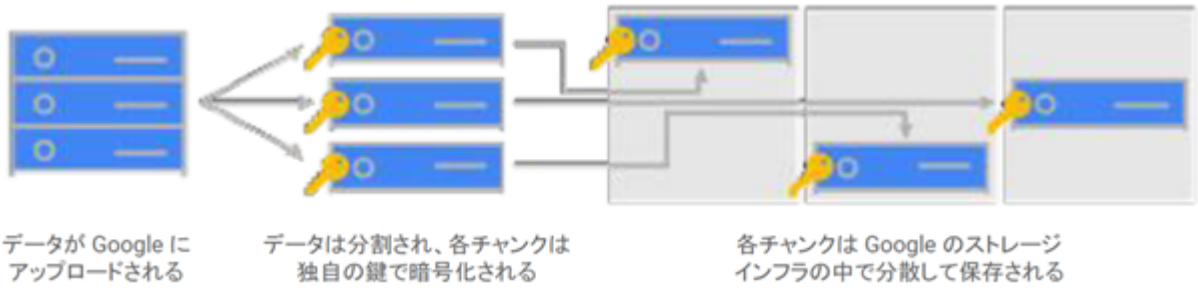
Googleの多段セキュリティモデル

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 のサービス間の通信の際には、GCP

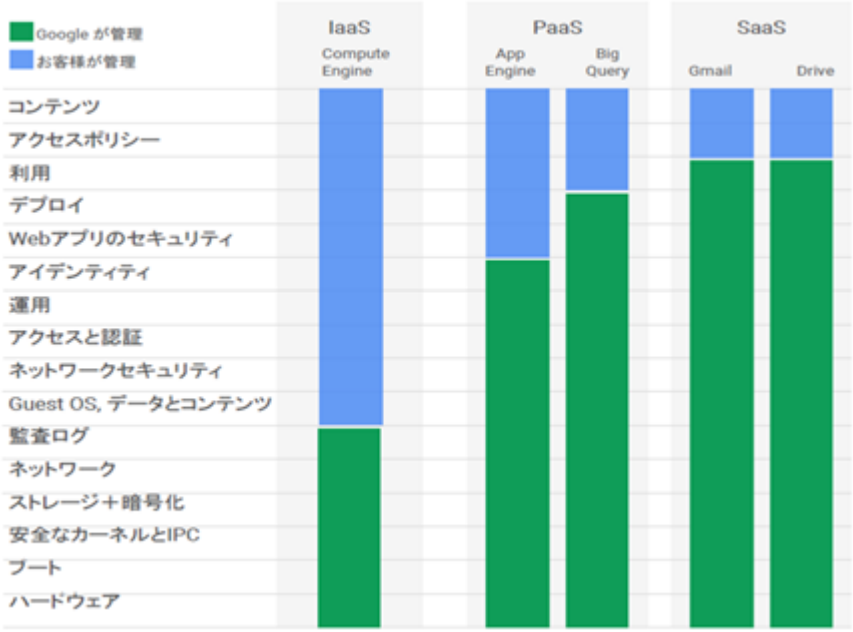
サービスに最適化された独自の通信プロトコルを利用し、自動的にデータの暗号化が行われています。

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。
GCP のサービス利用に関しては、セキュリティに係る責任をお客様と Google で共有する「責任共有モデル」が採用されています。例えば、GCP のプラットフォームサービス（PaaS）の1つである Google App Engine を利用する場合、お客様がアプリケーションを展開後、Google が大部分のリソースを管理します。また、インフラストラクチャサービス（IaaS）である Google Compute Engine を利用する場合には、Guest OS を含むシステムを設定・管理、監視するのはお客様の責任であり、Google はリソースの提供のみ行います。

Googleの責任共有モデル



Google の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。

Google のデータセンターでの電力供給については、24 時間体制で稼働しサービスが中断されないようにするため、冗長電源システムと環境管理が導入されています。すべての重要箇所に主電源と代替電源があり、どちらも電力は同じです。ディーゼル エンジンのバックアップ発電機により、各データセンターは緊急時でも最大限の性能を発揮できる電力を得られます。冷却システムによりサーバーなどのハードウェアの動作温度が一定に保たれ、サービス停止のリスクが軽減されます。火災検知および抑制装置は、ハードウェアの損傷を防ぐのに役立ちます。熱、火、煙検出検知器により、異常発生箇所、セキュリティ操作コンソール、リモート監視デスクで音声および視覚効果によるアラームが発生します。

4 システムの廃棄において、製造販売業者等は、データ移行やセキュリティ対策が考慮された、コンピュータシステムの廃棄に関する計画書を作成するとともに、廃棄結果の記録を作成し、保管することが求められています。
Google では、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バーコードやアセットタグを使用して追跡するとともに、未承認の機器がデータセンターから持ち出されることを防ぐため、金属探知機や映像監視システムを導入しています。ハードドライブを破棄する際には、適切な担当者によりデータを消去後、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。ディスクの物理的な破壊は複数の段階で行われ、破砕機でドライブを変形させた後、シュレッダーでドライブを細かく砕きます。

Google における管理環境の新適正管理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。新適正管理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

Google Cloud