金融情報システムセンター -（FISC: The Center for Financial Industry Information Systems）は、日本の金融情報システムに関連する諸問題(技術、利活用、管理態勢、脅威と防衛策等)の国内外における現状、課題、将来への発展性とそのための方策等についての調査研究を行う、日本の公益財団法人です。

FISCは、金融機関等の情報システムに対する安全対策を解説した「金融機関等コンピュータシステムの安全対策基準・解説書」（以下「FISC安全対策基準」）を公開しています。「金融機関等コンピュータシステムの安全対策基準・解説書」は、金融機関等のビジネスモデルや情報通信技術の最新動向など諸環境の変化を踏まえて適時に改訂されており、金融機関等がクラウドの利用・導入にあたって適切な安全管理対策を実施する上でのデファクトスタンダードとして広く活用されています。

この安全対策基準は「統制基準」「実務基準」「設備基準」「監査基準」の4編で構成されています。Google は、これら安全対策基準に対して次のような対応を行っています。

「統制基準」には、方針の策定、体制整備、人材育成、外部委託管理等の対策が含まれています。Google は専任のセキュリティチームやプライバシーチームを有しており、また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。

「実務基準」には、情報セキュリティ、システム運用、システム利用、システム開発等の対策が含まれています。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 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

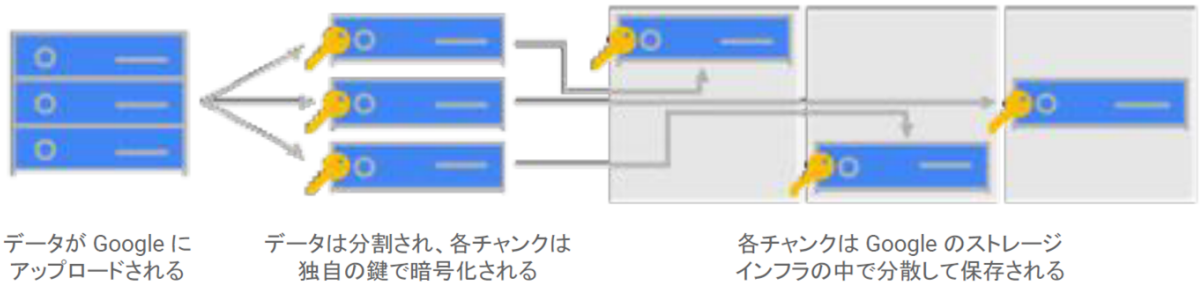
ています。このインフラストラクチャによって、サービスのデプロイ、データストレージやお客様のプライバシー保護、サービス間通信、インターネット経由の通信のセキュリティを確保するとともに、管理者オペレーションの安全性を提供しています。

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 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



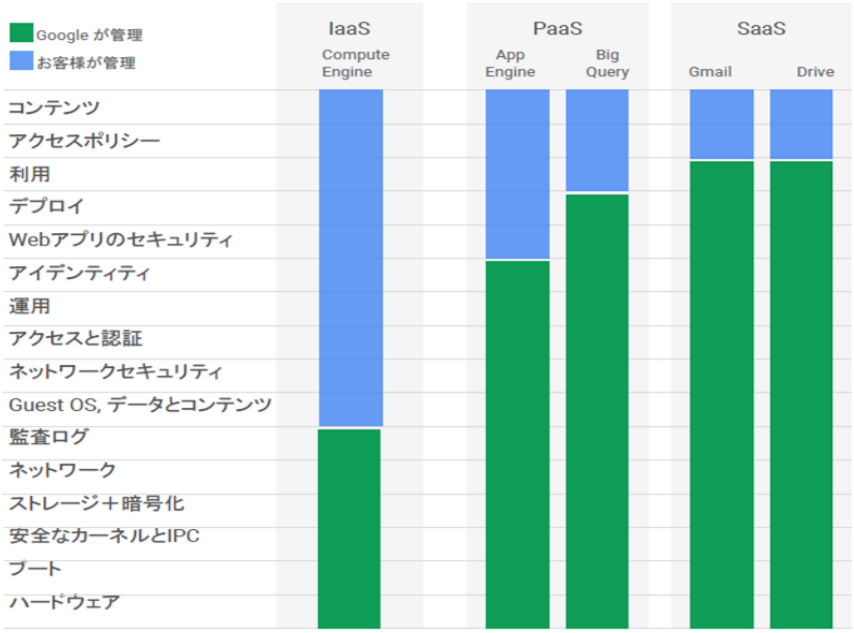
データが Google にアップロードされる

データは分割され、各チャンクは独自の鍵で暗号化される

各チャンクは Google のストレージインフラの中で分散して保存される

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）の一つである Google App Engine を利用する場合、お客様がアプリを構築後、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



「設備基準」は、設備ごとの要件に関する対策等が含まれています。
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。

「監査基準」は、監査体制の整備や手順等の対策が含まれています。Google はセキュリティ関連法令のコンプライアンスを確認する専用の内部監査チームを有しています。Google では第三者による監査を定期的に実施しており、データセンターやインフラストラクチャ、運用における管理状況を厳格に検査しています。

Google では、Google 専任の内部監査チームにより、世界中のセキュリティに関する法規制への準拠について審査しています。さらに、定期的に独立した第三者機関による監査を受け、データセンター、インフラ、オペレーションについての調査を行っています。定期的な監査では、ISO 27001、ISO 27017、ISO 27018、SOC 2、SOC 3 の監査規格へのコンプライアンスがチェックされます。また、Google ではネットワークトラフィックの記録や分析を行うための機能や、監査ログの精査を容易にするための機能が提供されており、お客様によるGCP の管理や問題解決、コンプライアンスの実証をサポートしています。

Google Cloud

Google における管理環境の FISC 安全対策基準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。FISC 安全対策基準に対する 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