Google Cloud

Google Cloud に移行して金融サービスのオペレーショナルレジリエンスを強化する

著者: Nick Godfrey、Dave Hannigan、David Knott、John Abel

目次

エグゼクティブ サマリー

オペレーショナル レジリエンスは、金融サービス機関にとって重視すべき分野であり、金融サービス業界の制度上のリスクに取り組む上で次の目標と考えられています。規制当局も、今まで以上にこのリスクに注目しはじめています。金融危機後、長年にわたって金融の復元力を高めることで金融の安定性を強化してはいるものの、経営面のショックも金融ショックと同程度に重大であることを認識したためです[1]。

オペレーショナル レジリエンスは、「あらゆる災害による混乱の中でも、業務（重要業務と中核事業を含む）を遂行する能力」と定義できます[2]。 この定義に基づくなら、オペレーショナル レジリエンスは、特異な活動ではなく「望ましい結果」として考える必要があります。それゆえ、その結果を達成するためのアプローチは、サイバーセキュリティ、サードパーティ、環境およびインフラストラクチャ、テクノロジーなど、さまざまな運用リスクに対処できるものでなければなりません。

こうした運用リスクは目まぐるしく変化する性質を持っています。また、金融サービス テクノロジーのニーズは複雑であり、商業上の考慮事項も存在します。そのため、金融機関が所有および運用するテクノロジーや、従来のテクノロジー アウトソーシング モデルでは、こうした課題に対処できなくなってきています。さらに、これらの活動に経営陣が注力しなければならなくなることで、高品質のサービスを相応の利幅で提供し、それらを迅速に進化させるという企業の中核的な使命が希釈されてしまいます。

Google Cloud に移行することで、金融サービス機関は潜在的な運用リスクの管理に本質的により適している機能やソリューションを活用して、顧客、株主、規制当局が求めるオペレーショナル レジリエンスを確保できます。

[1]「Resilience and continuity in an interconnected and changing world」、Lyndon Nelson、イングランド銀行副CEO

[2]「Sound Practices to Strengthen Operational Resilience」、FRB、OCC、FDIC

オペレーショナル レジリエンス

オペレーショナル レジリエンスの定義

金融サービスが複雑なシステム、自動化、テクノロジー、サードパーティへの依存度を高めている現状を反映して、金融サービス機関や規制当局は、オペレーショナル レジリエンスへの関心を高めています。

オペレーショナル レジリエンスについて、規制当局により複数の定義が示されています。

> 「運用の混乱に対する、企業、金融市場のインフラ、および金融セクター全体の予防、適応、対処、回復および学習能力」[3]

> 「あらゆる災害による混乱の中でも、業務（重要業務と中核事業を含む）を遂行する能力。混乱に備え、適応し、耐え、そこから回復するための十分な財務および業務上のリソースを確保したうえで効果的な運用リスク管理を行うことで、結果的に得られる能力である。」[4]

> 「金融機関が、自らが利用し、金融サービスの継続的な提供とその品質を支えるネットワークおよび情報システムのセキュリティの維持に必要な情報通信技術 (ICT) 関連の各種能力を、直接的に、またはICT サードパーティ プロバイダ サービスの利用を通して間接的に確保することにより、運用の完全性を技術的観点から確立、保証、確認する能力」[5]。

これらの定義に共通しているのは、重要業務の継続を妨げるおそれのあるリスクを効果的に管理することによって、オペレーショナル レジリエンスが達成されると考えるアプローチです。この目的を達成するためには、「オペレーショナル レジリエンスは実質的には事業継続計画を別の用語に言い換えたものだ」と解釈したり、視野の狭いアプローチを取ったりするのではなく、事業の継続を妨げるおそれのあるすべてのリスクを検討することが重要です。

もう 1 つの共通点は、クリティカルな（「重要な」と言うこともあります）ビジネス サービスを特定することに重点を置いていることです。ビジネス サービスは、企業の小売顧客または卸売顧客が、自分たちの利用するサービスを認識する方法と見なすことができます（リテール バンキングの例では、住宅ローンの組成など）。

企業に求められるオペレーショナル レジリエンスのレベルを定める手順として、重大ではあるものの現実的に起こりうる各種のシナリオを用いて、各ビジネス サービスについての「障害許容度」を決定することがよくあります。 地域によっては、この「障害許容度」は「リスク選好」とは定義が異なり、しきい値を特定する目的で設計されています。右はその一例です。

- 市場に影響: 金融サービスの広範なエコシステムに悪影響を引き起こす段階
- 顧客に影響: 金融サービス企業の顧客に甚大な損害が生じる段階

[3]「Operational resilience: Impact tolerances for important business Services」イングランド銀行、CP19/29
[4]「Sound Practices to Strengthen Operational Resilience」、FRB、OCC、FDIC
[5]「Draft Regulation on digital operational resilience for the financial sector」欧州委員会

こうした外部の基準点を用いた「障害許容度」の定義は、金融機関全体のオペレーショナル レジリエンスを強化しようとする規制当局の意図を反映したものです。別の言い方をすれば、企業の障害が市場や顧客に損害を与えるレベルが、リスク選好度によって示される、オペレーショナル レジリエンスに対する組織の努力目標のレベルとは異なっている可能性があります。

ではなぜ、障害許容度（またはリスク選好度）を定義したビジネス サービスを、オペレーショナル レジリエンスの管理のための出発点とすべきなのでしょうか？それは、こうした定義を設定することにより、組織の現在の技術、人材、施設、サードパーティ パートナーで達成可能な結果ではなく、顧客、組織、業界にとって適切な結果を得られるようになるからです。

以下のセクションで説明するように、オペレーショナル レジリエンスの概念はシンプルですが、必要なレベルのオペレーショナル レジリエンスを定義して達成し、それを継続的に証明することは困難です。しかし、達成しなければならない極めて重要なことでもあります[6]。

オペレーショナル レジリエンスとは、さまざまなリスクを効果的に管理する力

用リスクは結果であるため、管理が不十分であればオペレーショナル レジリエンスを損なうおそれのある用リスクの総体を特定することが重要です。考慮すべき主なリスクは、企業のビジネス サービスを支える依存関係（人、技術、施設、サードパーティなど）を破壊するおそれのあるものです。

サイバーセキュリティ:
外部の脅威や悪意のある内部関係者の活動を防止、検出してこれに対応するために、主要な管理権限、人、プロセス、技術を継続的に調整する

パンデミック:
同僚や顧客と対面で業務を行えない中で事業運用を維持する

環境およびインフラストラクチャ:
局地的な気象条件やインフラストラクチャに関連する事象の影響を軽減し、物理的な攻撃にも耐えられるような施設の設計と配置を行う

地政学:
組織内の依存関係とサードパーティとの依存関係の間の地理的および政治的境界に関連するリスクを理解して管理する

サードパーティ リスク:
サプライチェーンのリスク管理、特にベンダー ロックイン、存続性、ポータビリティへの対応による重要なアウトソース機能の管理を行う

テクノロジー リスク:
必要なレベルの可用性、容量、パフォーマンス、品質、機能を提供できるように、サードパーティ テクノロジー サービスを設計して運用する

以降のセクションでは、Google Cloud への移行によって、顧客がこうした運用リスクの各側面を大幅に改善する方法と、金融サービス機関と規制当局がオペレーショナル レジリエンスの目標を達成する仕組みについて検討します。

[6]「Resilience and continuity in an interconnected and changing world」、Lyndon Nelson、イングランド銀行副CEO

規制機関の見解のまとめ

世界中の規制当局は、金融復元力（信用リスク、市場リスク、流動性リスクの効果的な管理）と同様に、オペレーショナル レジリエンスが金融の安定性に甚大な影響を与える可能性があることを、これまで以上に深く認識するようになってきています。このセクションでは、規制当局によるこのリスクの認識と、企業にどのようなリスク管理を求めるかを概説します。付録では、世界各国で実施されている、または実施されつつある一部の規制の概要をさらに詳しく記載しています。

法域は数あれど、テーマは共通している

Google Cloud は、多数の法域でオペレーショナル レジリエンスや関連するテーマについて政策立案者と積極的に連携しており、各法域で現在取られているアプローチを支持しています。英国[7]、欧州連合[8]、米国[9]、および世界各国[10]の金融サービス規制当局は、いずれも過去 2 年間にオペレーショナル レジリエンスとそれに関連するテーマ（アウトソーシング、サードパーティ リスク、サイバーセキュリティ、情報通信技術、パンデミックなど）に関する包括的なガイダンスを発表しています。

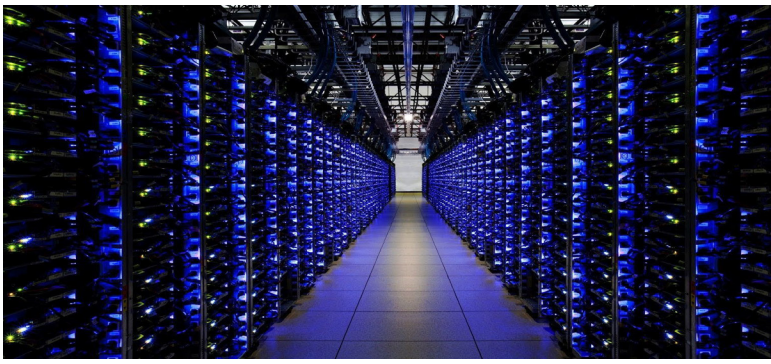
前のセクションで触れたとおり、オペレーショナル レジリエンスの定義と、その背後にある規制当局の意図には大きな共通点があります。すなわち、企業には、市場における自社の地位に照らし合わせてオペレーショナル レジリエンスの要件を定量化すること、および大きな混乱に直面した場合でも、定量化したレベルのオペレーショナル レジリエンスを達成することが期待されています。どのような混乱の中でも運用が維持されることを主な目標としていること、また、運用に対するリスクを特定する責任は企業にあることを強調しつつも、ほとんどの規制当局は、考慮すべき主要な運用リスクに関するガイダンスを提供しています。以下がその例です。

> 「企業は近年、**テクノロジーベースの障害**、**サイバー インシデント**、**パンデミックの発生**、**自然災害**など、さまざまな破壊的事象がもたらした重大な問題をいくつも経験しています。技術の進歩により、さまざまな種類の混乱を特定し、混乱から回復する能力を向上させています。しかしながら、サイバー脅威がますます高度化しており、サードパーティへの依存度も高まっているため、企業は今後もさまざまな運用リスクにさらされることになります。こうした運用リスクにより、どのような規模の企業であっても、オペレーショナル レジリエンスを強化することが重要であることが明らかになっています。」[11]

> 「**パンデミック**、**サイバーインシデント**、**テクノロジー障害**、**自然災害**など、運用リスクに関連する事象の影響を緩和する銀行の能力を強化するべきです。こうした事象は、運用上の大きな障害や金融市場の大規模な混乱を引き起こすおそれがあります。」[12]

[7] イングランド銀行、健全性規制機構、金融行為監督機構
[8] 欧州銀行監督局、欧州保険企業年金監督局、欧州証券市場監督局
[9] 連邦準備制度理事会、通貨監督庁、連邦預金保険公社
[10] バーゼル銀行監督委員会、証券監督者国際機構
[11]「Sound Practices to Strengthen Operational Resilience」、FRB、OCC、FDIC
[12]「Principles for operational resilience」、バーゼル銀行監督委員会

クラウド テクノロジーにより オペレーショナル レジリエンスを 高めることができる



近年では、「クラウド テクノロジーへの移行を今後数年間のうちにつつがなく行うことで、他の方法では達成できないやり方で金融サービスのオペレーショナル レジリエンスを強化でき、不要なリスクが新たに生み出されることもまずない」という認識が高まっています。以下がその例です。

「クラウド サービス プロバイダは、製品化までの時間を短縮できる既製のソリューションを提供しています。また、拡張性のメリットを活用して最先端のアナリティクスを提供するため、企業はビジネスモデルをほぼリアルタイムで学習して調整できるようになり、復元力も向上します」[13]

「企業がクラウドへの機能の移行を進めることは、必ずしも悪いことではありません。[中略] クラウド プロバイダのサイバー復元力が、特定の企業よりも高い場合があります」[14]

「アウトソーシングの潜在的な利点の一例は、クラウドベースのサービスやインフラストラクチャの使用にはっきりと見られます。[中略]クラウド コンピューティングの専門家やクラウドベース インフラストラクチャの提唱者とのやり取りによれば、次のようないくつかの利点があります。」

アクセシビリティ向上:
さまざまなデバイスや、クラウドへのネットワーク アクセスが可能な場所からサービスにアクセスできるようになります。

コスト効率:
クラウド プロバイダのリソースはプールされ、複数のクライアントに提供されます。これにより、スケール メリットが生まれ、データストレージのコストが削減されます。

需要に応じた拡張性:
クラウドは、クライアントのニーズに合わせて拡張および縮小できる柔軟なプラットフォームを提供します。

常時稼働による高可用性:
クラウド インフラストラクチャで実行しているアプリケーションがオフラインになることはほとんどなく、インターネット接続がある限りいつでもアクセスできます。

セキュリティの向上:
クラウドのセキュリティの慎重な監視は、クラウド プロバイダの主要な関心事の 1 つとなっています。これは、従来の社内システムの監視セキュリティよりも効率的です。[15]

[13]「New economy, new finance, new Bank」、イングランド銀行
[14] 金融サービス業界における IT の失敗、英国下院財務特別委員会
[15]「Principles on Outsourcing」、証券監督者国際機構

「CS（クラウド サービス）は、スケール メリット、コスト削減、高品質システム管理へのアクセス、統一されたセキュリティ基準とベスト プラクティスに準拠した運用など、さまざまなメリットをもたらす可能性があります。CS はまた、多大なハードウェアやソフトウェアの支出やリードタイムを伴わず、使用要件の変化に応じて迅速にコンピューティング リソースを拡大および縮小できる柔軟性と俊敏性を提供するためにも使用できます。また、CS の分散型の性質により、特定の地域での災害や障害時のシステムの復元力が向上する可能性があります」[16]

「技術的な観点から、大規模なパブリック　クラウド プロバイダは、少なくとも個々の金融機関が自社施設で構築できるのと同じくらい堅牢な IT 環境を提供することも珍しくありません。スケール メリットにより、クラウド プロバイダは、高い冗長性、地理的多様性、高度なセキュリティとエンジニアリングを低コストで達成できます」[17]

Google Cloud は、グローバルな金融システムの安定性を維持する上で、このリスクの重要性と、それを管理するための適切な規制の枠組みの必要性を理解しており、お客様によるオペレーショナル レジリエンスの目標を達成の支援と、政策立案者と連携した関連基準の策定に取り組んでいます。Google のグローバル プラットフォーム、およびお客様がアクセスできるサービスとソリューションは、独自の差別化された機能セットを提供し、オペレーショナル レジリエンスの達成に必要な重大な運用リスクの管理を可能にします。

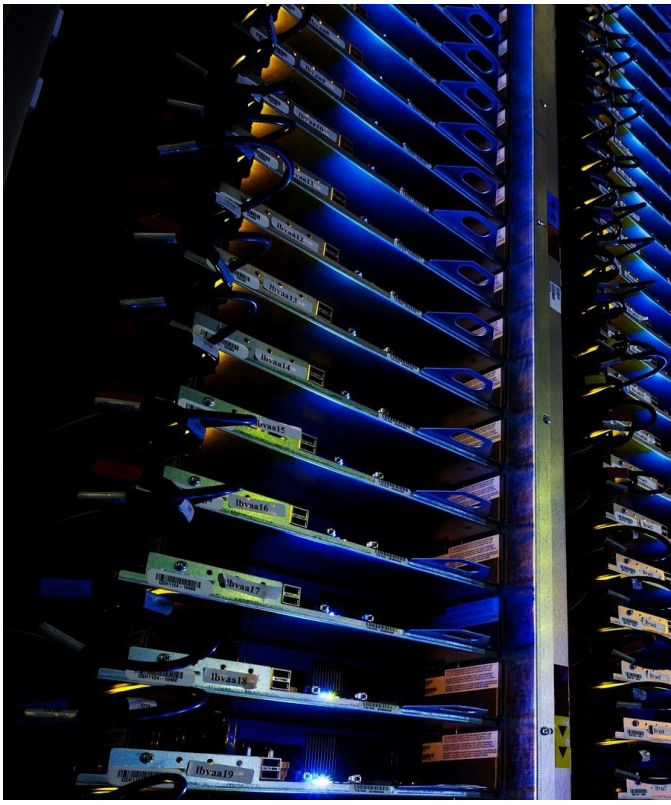
[16]「Guidelines on Outsourcing」、シンガポール金融管理局
[17]「Third-party dependencies in cloud services」、金融安定理事会

Google Cloud に移行してオペレーショナル レジリエンスを強化する

Google は、オペレーショナル レジリエンスの達成は困難を伴うものであり、管理すべき多次元的なリスクが存在すること、またそうしたリスクは金融サービスに影響を与えるリスクの中でも特に変化の激しいものであることを理解しています。Google Cloud を導入することで、金融サービス機関はオペレーショナル レジリエンスを強化し、主に次の 2 つの理由からこれらのリスクに新たな方法で対処できるようになります。

- Google Cloud のインフラストラクチャや運用モデルには、金融サービス機関には商業的、技術的にほぼ実現不可能なスケーラビリティと堅牢性が備わっています。[18] そのため、お客様が自社のアプリケーションやビジネスを構築する基盤は、すでに大いに復元力のあるものとなっています。
- こうした差別化されたソリューションは、Google Cloud がお客様に提供する機能です。お客様はアプリケーションやビジネスを構築し、従来達成可能だったレベルよりも高いレベルのオペレーショナル レジリエンスを達成できるようになります。

最初の項目についてさらに詳しく説明すると、Google Cloud は、過去 20 年間にわたり技術的な復元力に多額の投資を行ってきました。これは、Google 検索などの Google サービスを動かすテクノロジーと同じです。このモデルの基礎には以下が含まれます。



分散データセンター

Google には世界 24 の地域と 73 のゾーンがあり、200 か国以上のお客様にサービスを提供しています。そして今なお成長を続けています。

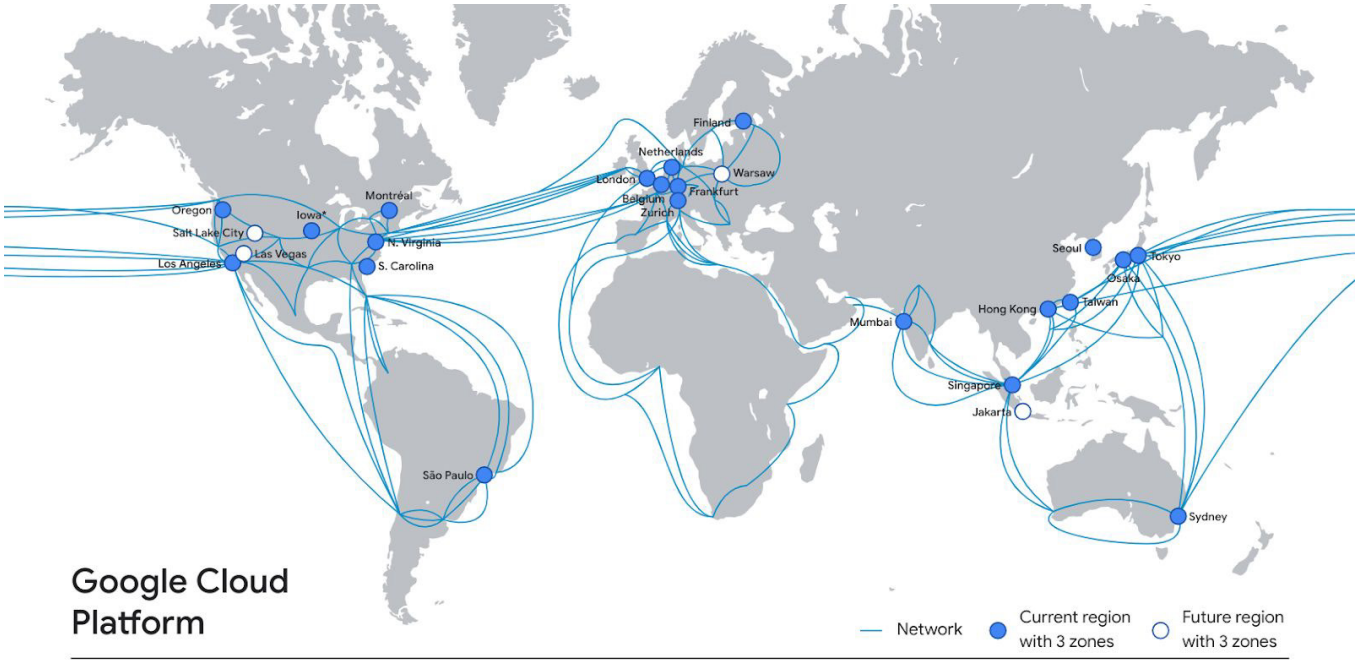
グローバル ネットワーク

Google は、130 以上の拠点を持つ世界最大級のバックボーン ネットワークを運営しており、低レイテンシとセキュリティの強化を実現しています。

高可用性サービス

コンピューティング、データベース、ネットワーク、ストレージ、その他のサービスを、公開された SLA に基づく極めて高いレベルの可用性で提供しています[19]。

[18]「Third-party dependencies in cloud services」、金融安定理事会
[19] https://cloud.google.com/terms/sla



Our global infrastructure

2 つ目の項目について: Google Cloud プロダクトは、Google Cloud でアプリケーションやビジネスを構築する際、その本来の性能により、個々の企業が達成可能なレベルよりもはるかに高いレベルのオペレーショナル レジリエンスをお客様に提供します。この 2 つ目の項目の解説として、以下のセクションでは、前述したようにオペレーショナル レジリエンスに関連する主なリスクを説明し、お客様が高レベルのオペレーショナル レジリエンスを達成する過程で使用できる Google Cloud の差別化要因の一部に焦点を当てます。

サイバーセキュリティ

Google のグローバル規模の技術インフラストラクチャは、情報処理ライフサイクル全体でセキュリティを確保できるように設計されています。このインフラストラクチャにより、サービスの安全なデプロイ、エンドユーザーのプライバシー保護を備えたデータの安全な格納、サービス間での安全な通信、インターネット経由の顧客との安全な非公開通信、管理者による安全な操作が可能になります。

インフラストラクチャのセキュリティは、データセンターの物理的セキュリティに始まり、インフラストラクチャの基盤となるハードウェアとソフトウェアのセキュリティに至る、段階的なレイヤで設計されています。その上に運用上のセキュリティ対策として、技術的制約とプロセスがあります。後述するように、Google には、ほとんどの金融サービス機関の技術的、商業的手段を超えたセキュリティへのアプローチに投資できるスケール メリット[20]があります。そのため、Google Cloud に移行することで、サイバーセキュリティのリスクを即座に軽減できます。

[20]「Third-party dependencies in cloud services」、金融安定理事会

安全なインフラストラクチャ

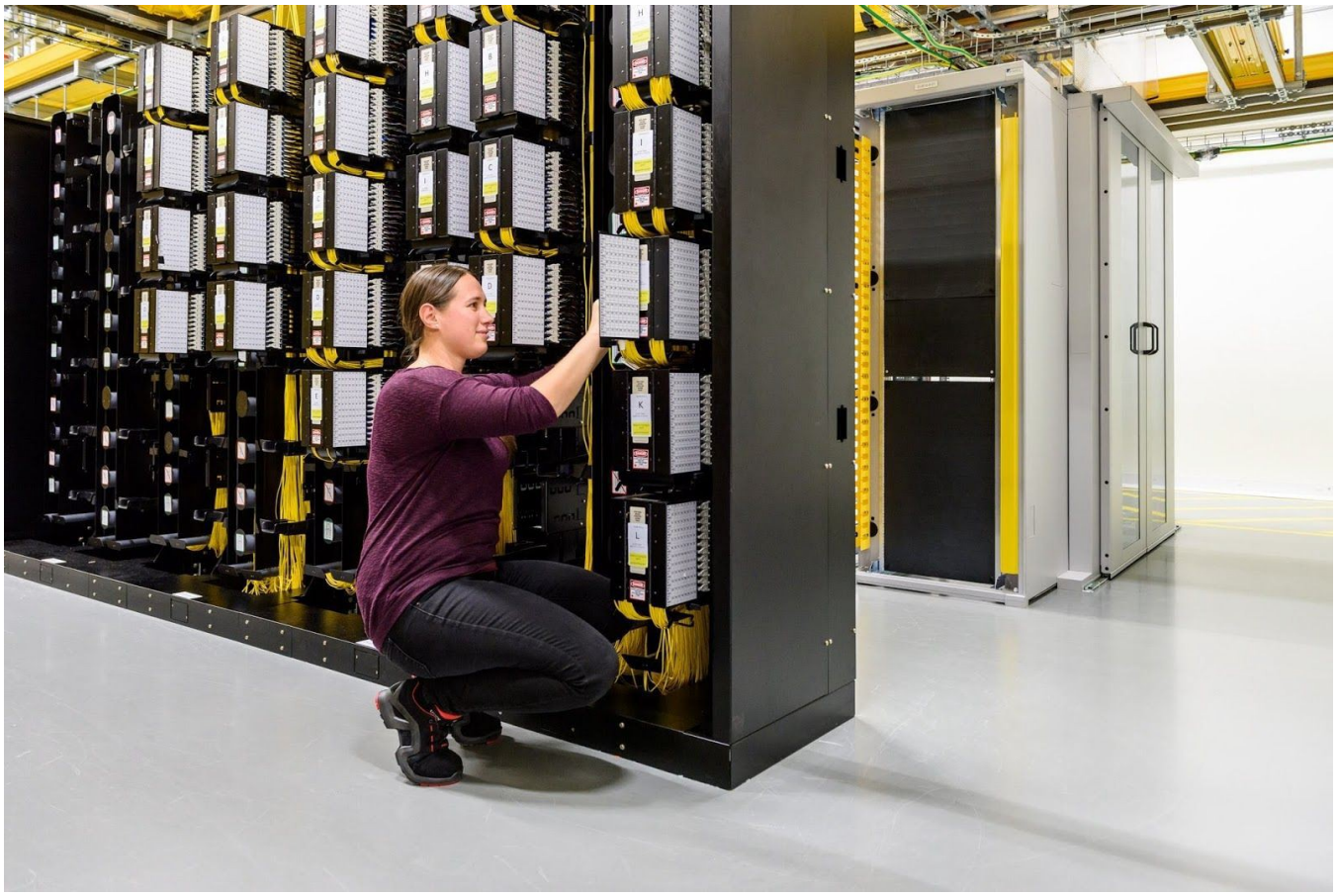
Google のサーバーとそのオペレーティング システムは、Google 向けに設計され、カスタム設計されています。さらに、Google は、Titan などのセキュリティ専用のハードウェアを設計して組み込んでいます。Titan はカスタム セキュリティ チップで、Google のサーバーと周辺機器でハートウェアのルート オブ トラストを確立するために使用されています。

ハードウェアの設計と供給元

サーバーボードとネットワーク機器はいずれも Google がカスタム設計したものです。そのため、ビデオカードや周辺機器の相互接続など、脆弱性の原因になりかねない不要なコンポーネントは含まれていません。私たちは、コンポーネント ベンダーを調査してコンポーネントを慎重に選定し、コンポーネントが提供するセキュリティ プロパティの監査と検証をベンダーと連携して行っています。

サービスへのアクセス管理

サービスの所有者は、インフラストラクチャが提供するアクセス管理機能を使用して、通信可能な他のサービスを正確に指定することができます。たとえばサービスによっては、他のサービスの特定の「許可リスト」にのみ API を提供します。このサービスは、これらのサービス アカウント ID で設定でき、アクセス制限が自動的に適用されます。



安全なサービス

Google Cloud インフラストラクチャは、基本的にマルチテナントになるように設計されており、インフラストラクチャ上で実行されるサービス間の信頼を前提としていません。内部リソースの保護を、外部のネットワーク境界に依存していた従来のデータセンターでのアプローチとは大きく異なります。さらに、サービスのセキュリティは次のように保護されます。

サービス ID
インフラストラクチャ上で実行される各サービスには、関連付けられたサービス アカウント ID があります。サービスには、その ID を証明する際に使用できる暗号化された認証情報が提供されます。これらの ID は、クライアントが正しいサーバーと通信していることを確認するため、およびサーバーが特定のクライアントへのメソッドとデータへのアクセスを制限する目的で使用されます。

サービス間アクセスの管理
サービスの所有者は、インフラストラクチャが提供するアクセス管理機能を使用して、通信可能な他のサービスを正確に指定することができます。たとえばサービスによっては、他のサービスの特定の「許可リスト」にのみ API を提供します。このサービスは、これらのサービス アカウント ID で設定でき、アクセス制限が自動的に適用されます。

Application Layer Transport Security（ALTS）
Google では、アプリケーション層で実行される相互認証およびトランスポート暗号化システムである ALTS を使用して、RPC 通信を保護しています。アプリケーション レベルのセキュリティを使用すると、各アプリケーションが認証されたリモートピア ID を持つことができ、それを利用してきめ細かな認可ポリシーを実装することが可能になります。

Binary Authorization for Borg（BAB）
とは、デプロイ時に内部で行われる強制適用チェックのことで、Google にデプロイされた本番のソフトウェアと構成が（特にそのコードがユーザーデータにアクセスできる場合に）適切に確認および承認されるようにすることで、インサイダー リスクを最小限に抑えます。これにより Google では、コードと構成のデプロイが特定の基準を満たしていることを確認し、本番環境でのソフトウェアの供給元を制限できます。

安全なデータ

Google Cloud では、サードパーティの検証済みの暗号技術に基づき、保存中および転送中のデータがデフォルトで暗号化されます。この暗号化に必要なお客様の処理はありません。Google は、顧客や規制当局が、特定のタイプのデータを処理する際など特殊な状況で、より高レベルの制御や自律性を求める場合があることを認識しています。そのため Google Cloud は、さまざまな鍵管理ソリューションを提供し、データの処理中にデータを暗号化する機能を備えています。

顧客管理の暗号鍵

Google Cloud を使用すると、お客様は Google Key Management System（KMS）内、または Google が所有および運営する専用 HSM 内で、独自の鍵を管理できるようになります。

顧客所有の鍵

より高度な制御を行うため、お客様は Google KMS を操作するための独自の鍵を支給できます。また、Google データセンターに隣接するコロケーションの HSM 内の特定の状況でも鍵を支給できます。

External Key Manager

最高レベルの制御が必要な場合、Google は External Key Manager（EKM）を提供します。EKM では、お客様のファシリティで鍵を保管し、必要な場合以外はアクセスできません。また、Key Access Justification（以下を参照）を追加することで、お客様は鍵へのアクセスの最終決定者となります。

Confidential Computing

Google Cloud をご利用のお客様は、最新の CPU（第 2 世代 AMD EPYC™ CPU でサポートされる Secure Encrypted Virtualization 拡張機能など）に搭載されたセキュリティ テクノロジーと、機密コンピューティング クラウド サービスを活用して、使用中のデータを暗号化できます。お客様はデータの処理中も、データの機密性を保持し、暗号化された状態を確実に維持できます。

安全なインターネット通信

前述したように、Google のインフラストラクチャはネットワーク上で相互に接続された多数のマシンで構成されており、サービス間通信のセキュリティはネットワークのセキュリティに依存していません。しかし、インフラストラクチャをインターネットからプライベート IP 空間に分離しているので、マシンのサブセットのみを外部のインターネット トラフィックに直接公開することで、サービス拒否（DoS）攻撃に対する防御など追加の保護をより簡単に実装できるようになっています。

Google Front End サービス

インターネット上でサービスを利用可能にする必要がある場合、Google Front End（GFE）と呼ばれるインフラストラクチャ サービスにそのサービスを登録できます。GFE では、すべての TLS 接続が正しい証明書を使用し、完全な前方秘匿性のサポートなどのベスト プラクティスに従って終端されることが保証されています。

サービス拒否攻撃（DoS）の軽減

インフラストラクチャの規模が大きいために、Google では多くの DoS 攻撃を単純に吸収することができますが、GFE の背後で動作しているサービスに対する DoS 攻撃のリスクを大幅に低減する、マルチティアでマルチレイヤの DoS 防御も施されています。Google のバックボーンがデータセンターの 1 つに外部接続を提供した後、ハードウェアとソフトウェアのロードバランサの複数の層を通過します。これらのロードバランサは、インフラストラクチャ上で実行している中央の DoS サービスに、着信トラフィックに関する情報を報告します。中央の DoS サービスが DoS 攻撃の発生を検出すると、攻撃に関連するトラフィックをドロップまたは抑制するようにロードバランサを設定できます。

安全な運営

Google は、Google Cloud でセキュリティを管理する上で必要な制御と自律性をもたらすツールとソリューションを提供しています。

Google 内の脅威の管理

Google Cloud のアクセスの透明性は、Google 社員によるお客様の環境へのアクセスに、他に例を見ない透明性を提供しています。また、External Key Manager と Key Access Justification のデプロイにより、暗号鍵へのアクセスを制御できる独自のサービスも提供されます。

外部の脅威の管理

Google Cloud のインフラストラクチャのスケールとデータ分析機能を活用し、Chronicle と Backstory を使用してペタバイト規模のセキュリティ データの保存と分析を行います。

クラウドのセキュリティ

Google は、Google Cloud のお客様のセキュリティを運命の共有と捉えており、ブループリント、ランディング ゾーン、Security Command Center の提供により重要な制御機能の管理を支援しています。

パンデミック

2020 年に見られたように、パンデミックが発生すると、特定の物理的な場所や施設から従業員や顧客を切り離さざるを得なくなります。これにより、リモートでの業務や連携の必要性など、運用上さまざまな課題が発生し、適切なソリューションを使用して適切な管理を行わないと、運用リスクが増大し、オペレーショナル レジリエンスが低下する結果となります。Google Cloud は、こうした分断された世界にとって最適な機能を備えた多数のソリューションを提供しています。

- **BeyondCorp によるリモートワーク**
  BeyondCorp リモート アクセスは、Google 社内でほぼ 10 年にわたり使用されているゼロトラスト アプローチに基づくクラウド ソリューションです。従業員や外部の人材は、従来のリモート アクセス VPN ゲートウェイを使用することなくほぼすべてのデバイスを使ってどこからでも社内のウェブアプリにアクセスできます。

- **Google Workspace**
  クラス最高水準のコラボレーション機能により、リモートで分散して働く従業員がオフィスにいるときと同様の生産性を維持できるようにします。

- **Rapid Response Virtual Agent**
  カスタマイズされた Contact Center AI 仮想エージェントをすばやく構築、実装することにより、パンデミックなどに関するお客様からの質問にチャット、音声、ソーシャル チャネルで対応できるようにします。

- **即座に処理能力をスケールアップ**
  Burst Capacity ソリューションは、特に大きなコンピューティング能力を必要とするワークロードを処理するための追加のコンピューティング能力と分析機能を提供します。お客様がトラフィックの急増や大きな処理能力を必要とするワークロードに安全、効率的かつ大規模に対応できるようにすることを目指しています。

環境およびインフラストラクチャ

Google は、複数の物理的セキュリティ保護レイヤからなるデータセンターを独自に設計して建設しています。このようなデータセンターへのアクセスは、ごく少数の Google 社員に制限されています。Google は、生体認証システム、金属探知、カメラ、車両障害物、レーザーを使用した侵入検知システムなどの技術を使用して複数の物理的なセキュリティ レイヤを設けることで、データセンターのフロアを保護しています[21]。また、一部のサーバーをサードパーティのデータセンターでホストしています。ここでも、データセンターの運営業者が提供するセキュリティ レイヤに加え、Google が管理する物理セキュリティ対策が設置されています。たとえばこのようなサイトでは、独立した生体認証システム、カメラ、金属探知器を使用する場合があります。同じく重要なのは、Google が業界で最もクリーンなクラウドを提供していることです。お客様はコンピューティングとデータ ストレージの炭素排出量をゼロに削減できます[22]。

- **世界と地域における復元性** Google Cloud は世界中で複数のゾーンを持つデータセンターを運用しており、局地的か地域全体かを問わず、環境およびインフラストラクチャに関する事象に対する復元力を備えています。
- **世界中で利用可能な Google のサポート** Google Cloud は世界各地にサポート部署を配備しており、大部分のエンジニアがリモートでの作業に対応可能なため、厳しい状況にあるお客様もサポートできます。
- **費用対効果の高い IT 復元力** 容量をオンデマンドで増減できるため、障害復旧機能を維持するための費用のかたちが大きく変わります（アイドル状態のインフラストラクチャに対する支払いは必要になったときにのみ発生します）。

地政学

現在、Google Cloud のベースラインの制御とセキュリティ機能は優れた保護を達成し、現行の厳しいセキュリティ要件を満たしています。さらにほとんどの場合、お客様のニーズに完全に対応しています。Google には、世界中のお客様にとって最も重要な機能を長年サポートしてきました。これには、データ所在地制御、保存データのデフォルト暗号化、組織ポリシー制約、VPC Service Controls などの重要な機能が含まれます。

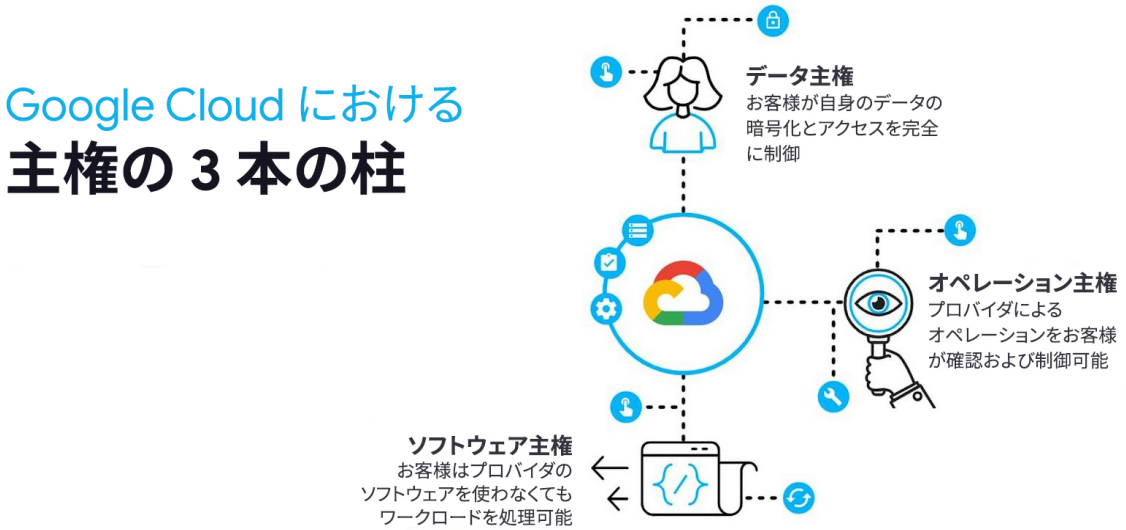
一方で Google は、特にヨーロッパのお客様や政策立案者が、セキュリティと自律性の向上に努めていることを理解しています。Google Cloud では、デジタル主権という用語でしばしば議論されるこれらの問題を真剣に受け止めています。Google は、データ主権、運用主権、ソフトウェア主権の 3 つの分野で、クラウド コンピューティングにおけるデジタル主権の実現に向けて、真摯に取り組んでいます。

[21] https://www.youtube.com/watch?v=kd33UVZhnAA
[22] https://cloud.google.com/sustainability

デジタル主権に基づく戦略的自律性

Google は、お客様が主権について次のような要望を持っているものと理解しています。まず、どのような担当者がどのリージョンからアクセスできるかを含む、プロバイダによるデータへのあらゆるアクセスの制御。次に、プロバイダが制御を回避したり、データをリージョン外に移動したりできないように、データへのアクセスやセキュリティに影響を与えるクラウド インフラストラクチャやサービスの変更を検査できること。そして、プロバイダからソフトウェアのアップデートを受け取れなくなった場合でも、ワークロードを長期間にわたって存続できることが求められています。

これらの要件は、データ主権、運用主権、ソフトウェア主権という 3 つの異なる主権の柱を反映したものです。



データ主権は、お客様のデータにプロバイダがアクセスできないようにするメカニズムを提供し、お客様が必要と考える特定のプロバイダの行動に対してのみアクセスを承認します。Google Cloud が提供する顧客管理の例としては、クラウド外での暗号鍵の保存と管理、詳細なアクセスの正当性に基づいてこのみれらのキーへのアクセスのみを許可する権限の付与、使用中のデータの保護などがあります。これらの機能によりお客様は、データへのアクセスに最終決定を下すことができます。

運用主権は、クラウド プロバイダの従業員がお客様のワークロードを侵害できないという保証を顧客に提供します。これらの機能により、お客様は、従来のオンプレミス環境と同様の制御を維持しつつ、マルチテナント環境の規模からメリットを得ることができます。たこうした制御の例としては、新しいリソースのデプロイを特定のプロバイダのリージョンに限定する、事前に定義された属性に基づいてサポート要員のアクセスを制限したりする、といったことが挙げられます。

ソフトウェア主権は、単一のクラウド プロバイダへの依存やロックインを伴わずにワークロードの可用性を制御し、これを必要な場所で実行できるという保証をお客様に提供します。これには、ワークロードの展開場所や外部接続の許可レベルを迅速に変更する必要がある事象を切り抜ける能力も含まれます。これは、ワークロード管理を簡素化し、集中リスクを軽減する 2 つの要件が満たされている場合にのみ可能です。1 つ目は、オープン API とサービスを採用したプラットフォームにお客様がアクセスできることです。2 つ目は、オーケストレーション ツールを使用して、マルチクラウド、ハイブリッド、オンプレミスなど、さまざまな構成での複数のプラットフォームにまたがったアプリケーションのデプロイをサポートするテクノロジーにアクセスできることです。これらの制御には、 お客様が複数のプロバイダをまたいでワークロードを管理できるプラットフォーム、および独自のクラウドベースやオープンソースの代替ソリューションなど、さまざまなプロバイダで実行されるアプリケーションを基盤とする単一の API を作成できるオーケストレーション ツールなどがあります。

サードパーティ リスク

Google は、企業の全体的なオペレーショナル レジリエンスにおける重要な要素の 1 つにサードパーティ リスクがあることを認識しています。 それを踏まえ、金融サービスのお客様は、主要なサードパーティも同等かそれ以上のオペレーショナル レジリエンスを備えていることを望んでいます。私たちは、オンサイト監査やコンプライアンス認定[23]など、必要な保証を構築できるさまざまなメカニズムを通じて、お客様に透明性を提供しています。

一方で、金融サービス機関の観点からは、望ましいオペレーショナル レジリエンスの達成には、サードパーティが何らかの理由で契約サービスを提供できない状況の解決が含まれる場合があることも認識しています。Google Cloud では、マルチクラウドとハイブリッドクラウドのアプローチをサポートするオープン クラウド[24]を採用しています。オープンソース ベースのテクノロジーを使用して実装した場合、オペレーショナル レジリエンスのリスク選好度への対応に必要なポータビリティ、代替性、存続性がお客様に提供されます。

マルチクラウド戦略によって軽減されるリスク

クラウドのハイパースケーラーは、十分に堅牢なサービスを提供します。このサービスは設計および設定が適切に行われている場合、企業のデータセンターで達成できるレベルかそれ以上の復元力を発揮します[25]。
マルチクラウド戦略は、次のような点で重要です。

1. ビジネスに最大限の価値と柔軟性を提供するサービスを選択できる
2. あらゆる特定のプロバイダからの出口戦略を設定することが可能になり、切り替えやポータビリティの確保ができるという安心感を持てる
3. 単一のサービス プロバイダへのリスクの集中を排除または軽減し、ベンダーへの依存を低減できる
4. 従来のワークロードとの整合性が保証され、単一のサービス プロバイダよりも低い投資レベルでより多くの価値を得られる

オペレーショナル レジリエンスの観点では、クラウドを使用することでサードパーティとの関係への依存が生まれ、その関係が崩れる、サードパーティの事業が失敗する、地政学的なリスクの結果、サービスの提供が途絶えるなるなどのリスクが生じます。ほとんどの企業では、これらのリスクを軽減するための出口戦略を策定しています。多くの法域では、これは重要なアウトソーシングにおける規制要件となっています。マルチクラウドは、企業のデータセンター内にクラウドに似た機能を構築する、複数のクラウドプロバイダと関係を確立し証明する、またはその両方を行うことにより、このような出口戦略を策定する手段となります。

[23] https://cloud.google.com/security/compliance/financial-services
[24] https://cloud.google.com/blog/products/gcp/why-google-believes-in-open-cloud
[25]「Third-party dependencies in cloud services」、金融安定理事会

ポータビリティとクラウド ネイティブ サービスの比較

クラウド プラットフォームの主な利点として、完全に管理されたサービスへのアクセスと、オンプレミス ソリューションでは利用できない機能へのアクセスが可能な点があります。ただしこのようなサービスは、多くの場合、個々のクラウド プロバイダが独占的に所有しているので、クラウド プロバイダ間でサービスを移動する機能が阻害され、マルチクラウド戦略の価値を低下させるおそれがあります。

Google は、ほとんどの金融サービス機関はマルチクラウド戦略を採用するため、重要なワークロードをクラウドに移行する際は、出口戦略を策定する必要がある考えています。Google では、オープン スタンダードのサポート、オープンソース プロジェクトへの貢献、およびマルチクラウド サービスとしての Anthos の開発を通じて、高いレベルのポータビリティを提供しています。Google は、このようなオープン性とマルチクラウドのサポートは、クラウド業界では先進的なものであると考えています。ただし、これらの機能を使用する場合でも、ポータビリティは、最終的な目的ではなく手段として捉える必要があります。ポータビリティはクラウド サービスの必須機能ではなく、出口戦略をサポートするツールにすぎません。ポータビリティをクラウド サービスの必須機能と考えると、使用できるサービスが制限され、クラウドの利点も制限されてしまいます。

- **クラウド ネイティブ サービス** 出口戦略を必要とするサービスで、実行可能な戦略の作成の妨げになる場合を除き、できる限りネイティブ サービスを使用します。
- **オープンソースをベースとした出口戦略** Google Cloud の共通標準とオープン標準の取り組みを活用して、必要なときに実行可能な出口戦略を作成します。
- **Anthos によるマルチクラウドの簡素化** オンプレミスとクラウド プラットフォーム全体に対応した共通の Kubernetes や他のサービスのデプロイを実現します。

テクノロジー リスク

金融サービスのテクノロジーを扱う企業は現在転換期にあります。銀行がメインフレームを導入してからおよそ 50 年間、業界はオンプレミスの自己管理型テクノロジーに数兆ドルを投資してきました。 その間、独自のデータセンターやグローバル ネットワークの構築、数十万台のサーバーと PC の管理、独自のアプリケーションの作成などを行ってきました。さらに、こうしたテクノロジーのほとんどは、データが 1 日あたり決まった回数だけコンピュータで処理され、仕事は支店の営業時間の間だけ、小切手や通知を配達する郵便の速度で進むという、デジタル以前の時代のビジネスを想定して構築されました。

しかし現代の顧客は、さまざまなデジタル チャネルを通じて、金融製品やサービスにいつでもアクセスできることが当たり前と考えています。このように、既存のテクノロジーの上にこれを達成するのは至難の業であり、技術上および運用上の障害が発生する可能性があります。このような障害は、金融の安定性と顧客の被害防止を目指す規制当局にとって、ますます重要な監視対象となっています[26]。

そこで、金融サービス テクノロジーの戦略的見直しについて、いやがうえにも議論が必要になります。一方、

[26] 金融サービス業界における IT の失敗、英国下院財務特別委員会

従来の IT 提供方法（オンプレミスや従来のアウトソーシングモデル）で既存のテクノロジーのリファクタリングを行うには、コストと時間がかかるため、ほとんどの企業にとって達成可能な戦略ではないと考えられています。その理由の 1 つは、これまで述べてきたように、従来のモデルではデータセンターから先をすべて金融サービス機関が管理しているためです。

Google Cloud に移行することで、金融サービス機関は、テクノロジー企業が基盤のテクノロジーではなく、高品質のサービスとエクスペリエンスの提供を重視していることを確認し、その結果、テクノロジー リスクを大幅に軽減できます。以下がその例です。

- **インフラストラクチャを気にせず運用** Google Cloud に移行すると、お客様はデプロイされた Google Cloud プロダクトを自身で制御でき、かつデータセンター、物理サーバー、ネットワーク機器を管理するためのリソースの確保や、パッチ適用やコア オペレーティング システムの保守について心配する必要がなくなります。
- **コンテナを活用して負債を削減** アプリケーションを完全にモダナイズできなくても（近い将来に廃止される可能性がある場合など）、コンテナ イメージに移行して Google Kubernetes Engine（GKE）を使用して管理することで、そのアプリケーションに関連する技術的負債（サポートされないハードウェアやオペレーティング システムなど）を軽減できます。
- **メインフレームのモダナイゼーション** Google Cloud のツールは、自動プロセスの使用を通して COBOL、PL/1、アセンブリ言語を使用したプログラムをサービスに変換し、クラウド ネイティブ（コンテナ化されたマネージド環境など）にします。

まとめ

金融の安定性を維持するには、オペレーショナル レジリエンスがきわめて重要です。金融サービス機関やその顧客、取引先、および政策立案者がいずれもオペレーショナル レジリエンスの強化を重視しているのは理にかなっています。

Google Cloud は、現在取られているアプローチを支持しており、今後も政策立案者やお客様との連携を継続して、お客様が期待どおりの成果を達成できるように支援します。Google は、金融サービスのテクノロジーが複雑さに満ちていることを知っています。また、オペレーショナル レジリエンスの要件に対応しつつ、顧客が必要とする商品やサービスを提供する過程で、業界が困難な道のりを歩まなければならないことを理解しています。

Google は、金融サービス業界がオペレーショナル レジリエンスのあらゆる要件に最高レベルで適合できるよう、金融サービス向けの Google Cloud ソリューションの設計に取り組んでいます。さらに Google は、この問題が Google Cloud の復元力だけにとどまらず、金融業界が必要とする自律性、主権、存続性にも関わるものであることも認識しています。

付録

オペレーショナル レジリエンスに関する規制当局の見解

世界中の規制当局は、オペレーショナル レジリエンスの重要性を認識しています。また、オペレーショナル レジリエンスが財務の復元力（信用リスク、市場リスク、流動性リスク）と同様に金融の安定性に甚大な影響を与える可能性があることや、オペレーショナル レジリエンスの強化には複数の経営リスクの効果的な管理が必要であることも認識しています。

近年では、「クラウド テクノロジーへの移行を今後数年間のうちにつつがなく行うことで、他の方法では達成できないやり方で金融サービスのオペレーショナル レジリエンスを強化でき、不要なリスクが新たに生み出されることもまずない」という認識が高まっています。

Google Cloud は、グローバルな金融システムの安定性を維持する上で、このリスクの重要性と、それを管理するための適切な規制の枠組みの必要性を理解しており、顧客によるオペレーショナル レジリエンスの目標を達成の支援と、政策立案者と連携した基準の策定に取り組んでいます。

英国

2018 年、イングランド銀行、健全性規制機構（PRA）、金融行為監督機構（FCA）は、上記のセクションで説明したいくつかの新しい概念を記述した共同ディスカッション ペーパー[27] を発表しました。金融機関は、「業務の中断に対する復元力を確保するための幾多の課題に直面しており、このような課題は近年、進化する技術や敵対的なサイバー環境の中で、より複雑で難しいものになっている」ことから、より広範なアプローチを採用する必要性が確認されています。これらの課題のいくつかは、共同ディスカッション ペーパーから引用した以下の図で示されます。

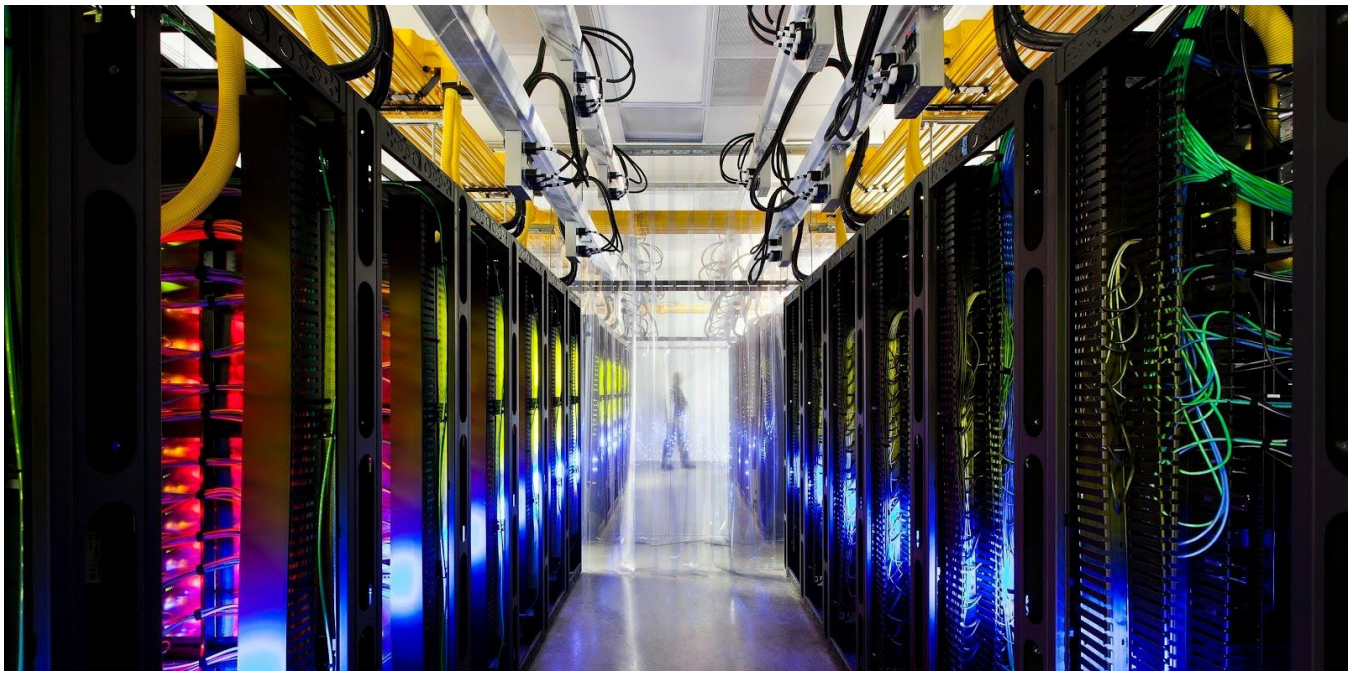
[27]「Building the UK financial sector's operational resilience」、イングランド銀行、PRA、FCA

2019 年にイングランド銀行は、このディスカッション ペーパーを加筆修正したほぼ同様の文書をコンサルテーション ペーパー[28] として発表し、また「英国金融界の先行き」に関する委託調査の報告書を発表しました[29]。この報告書とイングランド銀行の回答[30] には、企業経営の復元力強化にはクラウド テクノロジーの導入が重要であることが指摘されています。

> 「もう 1 つの優先事項は、金融サービスがクラウド テクノロジーを採用することです。クラウド テクノロジーは、規制当局や金融機関の高い期待に応えられる段階まで成熟しています。社内のデータ ストレージと処理からクラウド環境に移行することで、イノベーションが加速し、最適な分析ツールの使用が可能になり、競争力が高まり、復元力が構築されます」

> 「クラウド サービス プロバイダは、製品化までの時間を短縮できる既製のソリューションを提供しています。また、その規模のメリットを活用して最先端のアナリティクスを提供するため、企業はビジネスモデルをほぼリアルタイムで学習して調整できるようになり、また、復元力も向上します」

2019 年 12 月、PRA はアウトソーシングに関するコンサルテーションを発表し、その一部として「クラウドなどの新しいテクノロジーの復元力の向上と導入の促進」が議論されています。一方で、企業は契約から抜け出す能力に焦点を当てることで、集中リスクとベンダーロックインの課題に対処する必要があることを指摘しています（このリスクについてお客様による管理を可能にする Google Cloud の本質的な機能については、**サードパーティ** リスクを参照してください）。規制当局は、2021 年初頭に最終的なガイダンスを発行する予定です。



[28]「Operational resilience: Impact tolerances for important business services」、イングランド銀行、PRA、FCA
[29]「Review on the outlook for UK Financial Services: What it means for the Bank of England」、van Steenis
[30]「New economy, new finance, new Bank」、イングランド銀行

欧州連合

2019 年から 2020 年にかけて、EU の金融サービス規制当局は、情報通信技術（ICT）[31] やアウトソーシングなど、オペレーショナル レジリエンスの主要事項に関するガイドラインを発表しました。欧州銀行企業監督局（EBA）、欧州保険年金監督局（EIOPA）、欧州証券市場監督局（ESMA）が起草中のアウトソーシング ガイドラインはいずれも、オペレーショナル レジリエンスと、明確に定義され管理されたアウトソーシングへのアプローチとの間の相互依存関係を織り込んでおり、金融機関に次のような運用リスクへの対応を求めています。

サードパーティ リスク: サプライチェーンのリスク管理、特にベンダーロックイン、存続性、ポータビリティへの対応による重要なアウトソース機能の管理を行う

> 「必要不可欠または重要な機能のアウトソーシングに関しては、適切な期間内に、少なくとも次のいずれかの措置を講じることができます。
> i. 機能を別のサービスプロバイダに委託する
> ii. 機能を再統合する
> iii. 機能に依存する業務を取りやめる」[32]

サイバーセキュリティ: 外部の脅威や悪意のある内部関係者の活動を防止、検出してこれに対応するために、主要な制御、人、プロセス、技術を継続的に調整する

> 「転送中のデータ、メモリ内のデータ、保存されているデータについて具体的な対策を必要に応じて検討してください。たとえば、暗号化技術と適切な鍵管理を組み合わせて使用する方法などが挙げられます」[33]

地政学: 組織内の依存関係とサードパーティとの依存関係の間の地理的および政治的境界に関連するリスクを理解して管理する

> 「問題となっている法域の政治的な安定性と安全性について検討してください。たとえば、次のような状況です。
> i. データ保護に関する法律などの施行中の法律
> ii. 施行中の法執行規定
> iii.サービス プロバイダの経営破綻を受けて適用される破産法の規定や、特に金融機関や支払元のデータの緊急回復に関連して生じる制約」[34]

[31]「Guidelines on ICT and security risk management」、欧州銀行監督局
[32]「Guidelines on Outsourcing Arrangements」、欧州銀行監督局
[33]「Guidelines on Outsourcing to Cloud Service Providers」、欧州保険企業年金監督局
[34]「Guidelines on Outsourcing Arrangements」、欧州銀行監督局

2020 年、欧州の政策立案者は、新しい規制案「金融部門のデジタルオペレーショナル レジリエンス（DORA）」[35] を通じて、金融サービスにおけるオペレーショナル レジリエンスのニーズに、より直接的に対応するための一歩を踏み出しました。

DORA は、情報通信技術（ICT）サービスを利用する金融機関にとって重要なテーマを数多く扱っており、インシデントの報告、オペレーショナル レジリエンスのテスト、サードパーティ リスクの管理など、欧州の金融システムのデジタル復元力の強化を目的としています。前述したように、復元力とセキュリティは Google Cloud の運用の中核となっています。私たちは、パブリック クラウドへの移行が、金融機関のオペレーショナル レジリエンスとセキュリティ体制の向上に役立つと確信しています。同時に、DORA に基づく主要なサードパーティ プロバイダの監視フレームワークは、ICT サービス プロバイダ、金融機関、金融規制当局間の理解、透明性、信頼性を高め、最終的に欧州の金融業界のイノベーションを促進する真の機会を生み出す可能性があります。

米国

2020 年末、通貨監督庁、連邦預金保険公社、米連邦預金保険公社（以下、総称して当局）は、金融サービスにおけるオペレーショナル レジリエンスを強化する目的で策定された省庁間文書[36] を発表しました。 この文書には以下のような記載があります。

> 「企業は近年、テクノロジーベースの障害、サイバー インシデント、パンデミックの発生、自然災害など、さまざまな破壊的事象がもたらした重大な問題をいくつも経験しています。技術の進歩により、企業は混乱の種類を特定し、混乱から回復する能力を向上させています。しかしながら、サイバー脅威がますます高度化しており、サードパーティへの依存度も高まっているため、企業は今後もさまざまな運用リスクにさらされることになります。こうした運用リスクにより、どのような規模の企業であっても、オペレーショナル レジリエンスを強化することが重要であることが明らかになっています。」

この文書では、経営面での復元力を高めるには、複数の経営リスクを管理することの重要性が強調されています。以下がその例です。

環境およびインフラストラクチャ: 局地的な気象条件やインフラストラクチャに関する事象の影響を軽減し、物理的な攻撃にも耐えられるような施設の設計と配置を行う

> 「企業は障害が発生した際に、企業の重大な運用と中核的な事業を遂行するための十分なリソース（人員を含む）、テクノロジー、能力、機能を備えた代替サイトを備えています。代替サイトは、主要サイトから地理的に十分離れた距離にあり、明確なリスク プロファイルを備えています。

[35]「Draft Regulation on digital operational resilience for the financial sector」、欧州委員会
[36]「Sound Practices to Strengthen Operational Resilience」、FRB、OCC、FDIC

パンデミック: 同僚や顧客と対面で業務を行えない中で事業運用を維持する

> 「企業の事業継続性管理には、不測の事態に備えてリモート アクセスを含んでいます。これにより従業員は、障害発生時にも、企業の重要業務と中核事業を継続できます。不測の事態の管理では、重要業務と中核事業を優先しており、従業員に適切な接続性、通信、コラボレーション ツール、必要なテクノロジー リソース、ネットワーク システムへのアクセスを提供します」

サードパーティ リスク: サプライチェーンのリスク管理、特にベンダーロックイン、存続性、ポータビリティへの対応による重要なアウトソース機能の管理を行う

> 「企業は、サードパーティがサービスの提供を継続できなくなった場合に、支援を望める他の第三者を特定しています。さらに、企業の重大な運用と中核的な事業をサポートするサードパーティのサービスの代替可能性を評価します。これには、サービスを社内に戻す可能性も含みます」

サイバーセキュリティ: 外部の脅威や悪意のある内部関係者の活動を防止、検出してこれに対応するために、主要な制御、人、プロセス、技術を継続的に調整する

> 「企業の重要業務と中核事業用の情報システム アーキテクチャには企業のサイバー復元力の要件を組み込んだセキュリティ重視の設計となっています。また、相互依存性、相互接続性、規模、複雑性のリスクについても考慮しています」

テクノロジー リスク: 必要なレベルの可用性、容量、パフォーマンス、品質、機能を提供できるように、サードパーティ サービスやテクノロジー サービスを設計して運用する

> 「企業は、プロセスのライフサイクル全体にわたって自社の復元力要件を組み込み、テクノロジーの入手、開発、テスト、統合について定義済みのプロセスを実施しています」

> 「企業は開発者、ベンダー、メーカーから技術サポートが受けられなくなる前に、情報システムのコンポーネントをアップグレードまたは交換しています」

シンガポール

シンガポール金融管理局は、「アウトソーシングに関するガイドライン」[37]において、アウトソーシングが金融機関のリスク プロファイルに与える影響を認識し、以下の点を考慮するよう求めています。

> 「アウトソーシング契約が金融機関の全体的なリスク プロファイルに与える影響を分析し、特定されたリスクを軽減するための正しい専門知識と適切なリソースが社内にあることを確認すること」

テクノロジー リスク管理[38]や事業継続管理[39] といった他のガイドラインには、クラウドの導入によって組織が簡素化される可能性がある、テクノロジー リスク、サイバーセキュリティ 、**サードパーティ** リスクに関するさまざまな要件が盛り込まれています。

また、「クラウド サービス（CS）」への移行をうまく管理すれば、オペレーショナル レジリエンスが向上する可能性があることも指摘されています。

> 「CS は、スケール メリット、コスト削減、品質システム管理へのアクセス、統一されたセキュリティ基準とベスト プラクティスに準拠した運用など、さまざまなメリットをもたらす可能性があります。CS は、多大なハードウェアやソフトウェアの支出やリードタイムを伴うことなく、使用要件の変化に応じてコンピューティング リソースを速やかに拡大および縮小できる柔軟性と俊敏性を提供するためにも使用できます。また、CS の分散型の性質により、ロケーション固有の災害や障害時のシステムの復元力が向上する可能性があります」

[37]「Guidelines on Outsourcing」、シンガポール金融管理局
[38]「Guidelines on Technology Risk Management」、シンガポール金融管理局
[39]「Guidelines on Business Continuity Management」、シンガポール金融管理局

香港

香港金融管理局の運用リスク[40]に関する監督ポリシー マニュアルのモジュールでは、会社の運用リスクプロファイルは、テクノロジー リスク、アウトソーシング 、事業継続性を含むいくつかの要因によって大きく左右されるとしており、これらはすべて、監督ポリシー マニュアルでそれぞれ別のモジュール[41]として取り上げられています。

オーストラリア

オーストラリア健全性規制庁（APRA）は、クラウド アウトソーシング[42]、情報セキュリティ[43]、事業継続[44]など、オペレーショナル レジリエンスに関する数多くの文書や基準を管理しています。APRA は、次のような見解を示しています。

> オペレーショナル レジリエンスの中核は、規制対象の企業が以下のような潜在的障害に直面しても事業サービスを提供し続ける能力である:

物理的およびサイバー攻撃、IT システムの停止、サードパーティのサプライヤの障害などの人工的な障害、

火災、洪水、悪天候、パンデミックなどの自然災害、

規制の強化、より効率的な事業モデルを持つ新たな競合他社、気候変動に伴うリスク、革新的な技術ソリューションなど、より戦略的な対応を必要とする状況や事象の出現[45]

[40] 「Supervisory Policy Manual: OR-1 Operational Risk Management」、香港管理局（HKMA）
[41] 「SA-2 Outsourcing」、「TM-G-1」、「General Principles for Technology Risk」、TM-G-2「Business Continuity Planning」、HKMA
[42] 「Outsourcing involving cloud computing services」、オーストラリア健全性規制庁
[43] 「Prudential Standard CPS 234 Information Security」、オーストラリア健全性規制庁
[44] 「Prudential Standard CPS 232 Business Continuity Management」、オーストラリア健全性規制庁
[45] https://www.apra.gov.au/covid-19-a-real-world-test-of-operational-resilience

世界各国

2020 年半ば、バーゼル銀行監督委員会は、オペレーショナル レジリエンスに関する諮問文書を発表し[46]、「資本と流動性の水準が大幅に向上したことで、銀行の金融ショック緩和能力は改善された」としながらも、以下の点についてさらなる取り組みが必要であるとしています。

> 「パンデミック、サイバー インシデント、テクノロジー障害、自然災害など、運用リスクに関連する事象の影響を緩和する銀行の能力を強化するべきです。こうした事象は、運用上の大きな障害や金融市場の大規模な混乱を引き起こすおそれがあります。」

この文書では、オペレーショナル レジリエンスの本質的な要素として、運用リスクの効果的な管理を挙げており、特に、事業継続性（人、プロセス、テクノロジー、施設、サードパーティへの依存、および**パンデミック**、**環境およびインフラストラクチャ関連の事象**などの運用リスクを含む）、サードパーティへの依存の管理、**サイバーセキュリティ**を含む ICT のリスクが重要であるとされています。

さらに、証券監督者国際機構（IOSCO）[47] は、アウトソーシングとサードパーティ管理に関するコンサルテーション ペーパーを発行しています。他の規制文書と同様に、この文書では、クラウドベースのサービスを活用することで得られる潜在的メリットと、それに伴うリスクを管理する必要性の両面を指摘しています。

> アウトソーシングの潜在的な利点の例は、クラウドベースのサービスやインフラストラクチャの使用に見られます。[中略]クラウド コンピューティングの専門家やクラウドベース インフラストラクチャの提唱者とのやり取りによれば、次のようないくつかの利点があります。

アクセシビリティ向上:
さまざまなデバイスや、クラウドへのネットワーク アクセスが可能な場所からサービスにアクセスできるようになります。

コスト効率:
クラウド プロバイダのリソースはプールされ、複数のクライアントに提供されます。これにより、スケール メリットが生まれ、 データ ストレージのコストが削減されます。

需要に応じた拡張性:
クラウドは、クライアントのニーズに合わせて拡張および縮小できる柔軟なプラットフォームを提供します。

常時稼働による高可用性:
クラウド インフラストラクチャで実行しているアプリケーションがオフラインになることはほとんどなく、インターネット接続がある限りいつでもアクセスできます。

セキュリティの向上:
クラウドのセキュリティの慎重な監視は、クラウド プロバイダの主要な関心事の 1 つとなっています。これは、従来の社内システムの監視セキュリティよりも効率的です。

[46]「Principles for operational resilience」、バーゼル銀行監督委員会
[47]「Principles on Outsourcing」、証券監督者国際機構

最後に、金融安定理事会（Financial Stability Board）は、このテーマに関連する 2 つの文書を発表しており、いずれも、クラウドの利用によって金融サービスのオペレーショナル レジリエンスが向上する可能性を指摘しています。

> 「クラウド サービスは、オンプレミスのデータセンターのような従来のテクノロジーに比べ、多くの利点があります。地理的に分散したインフラストラクチャを構築し、セキュリティに多大な投資を行うことで、クラウド サービス プロバイダは個々の機関の復元力を大幅に強化できる可能性があります」[48]。

また、クラウド サービスの重要性が増すにつれ、関連するリスクを管理し、クラウドを採用する企業を規制するためのアプローチが進化し続けていることを指摘しています。

> 「金融機関のサードパーティとの関係が進化していることから、いくつかの監督官庁は、アウトソーシング、サードパーティ リスク管理、事業継続計画、サイバーセキュリティとそれに関連するデータ保護、オペレーショナル レジリエンス、リスク管理などの分野における規制、監督の枠組みの更新やその検討を行っています」[49]。

[48]「Third-party dependencies in cloud services」、金融安定理事会
[49]「Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships」、金融安定理事会

参考資料

[Resilience and continuity in an interconnected and changing world](#)
Lyndon Nelson のスピーチ、イングランド銀行

[Sound Practices to Strengthen Operational Resilience](#)
FRB、OCC、FDIC

[Operational resilience: Impact tolerances for important business services](#)
イングランド銀行、PRA、FCA

[Draft Regulation on digital operational resilience for the financial sector](#)
欧州委員会

[Building the UK financial sector's operational resilience](#)
イングランド銀行、PRA、FCA

[Review on the outlook for UK Financial Services: What it means for the Bank of England](#)
報告者: Huw van Steenis

[New economy, new finance, new Bank](#)
イングランド銀行

[Guidelines on ICT and security risk management](#)
欧州銀行監督局グランド銀行

[Guidelines on Outsourcing Arrangements](#)
欧州銀行監督局

[Guidelines on Outsourcing to Cloud Service Providers](#)
欧州保険企業年金監督局

[Draft Guidelines on Outsourcing to Cloud Service Providers](#)
欧州証券市場監督局

[Principles for operational resilience](#)
バーゼル銀行監督委員会

[Principles on Outsourcing](#)
証券監督者国際機構

[IT failures in the Financial Services Sector](#)
英国下院財務特別委員会

[Guidelines on Outsourcing](#)
シンガポール金融管理局

[Guidelines on Technology Risk Management](#)
シンガポール金融管理局

[Guidelines on Business Continuity Management](#)
シンガポール金融管理局

[Supervisory Policy Manual](#)
香港金融管理局

[Third-party dependencies in cloud services](#)
金融安定理事会

[Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships](#)
金融安定理事会

[Outsourcing involving cloud computing services](#)
オーストラリア健全性規制庁

[Prudential Standard CPS 234 Information Security](#)
オーストラリア健全性規制庁

[Prudential Standard CPS 232 Business Continuity Management](#)
オーストラリア健全性規制庁