

## ゴールドマン・サックスのオペレーショナル・レジリエンス、業務継続および災害復旧について

ゴールドマン・サックス・グループ（以下、当グループ）のオペレーショナル・レジリエンスフレームワークはお客様や市場、当グループに影響を与える重大な業務上の障害に対して、未然防止・対応・復旧・適応のために設計されています。

オペレーショナル・レジリエンスは、当グループの優先事項の一つであり、お客様に対するサービスを継続して提供し、またお客様の資産と、当グループの従業員および資産を、継続的に保護できる態勢を適切に確保することを目標としています。当グループのオペレーショナル・レジリエンスの状況は定期的に取り締役に報告され、グループ全体のオペレーショナル・レジリエンスプログラムの検証と監督が確実に行われるようにしています。

オペレーショナル・レジリエンスフレームワークを実践するうえでの基礎となるのは、当グループの業務継続、災害復旧および危機管理プログラムです。またこれら 3 つのプログラムのベースにあるのは、包括的なテクノロジー障害復旧、サイバー・レジリエンス、サードパーティ・ベンダー・レジリエンス、施設のレジリエンスや従業員のウェルネスを含む、アセットベース・レジリエンスプログラムとなります。

### レジリエンス・プランニング

当グループは重要なビジネスサービス (IBS) の管理、業務継続計画、およびアセットベース・レジリエンスプログラムを通して、レジリエンス計画を実施しています。

- **重要なビジネスサービス** (または、現地での規制で求められる同等のもの) は、当グループが提供するサービスの中で、中断した場合に顧客、市場、または当グループに容認できない損害をもたらす可能性のある重要なサービスとして特定されます。インパクト・トランス (重大な影響が発生する前の、IBS への最大許容中断レベル) および IBS の提供に不可欠な資源 (ディペンデント・アセット) は計画段階で特定され、これにより業務継続に必要なレジリエンス・コントロールを確立することができます。当グループの IBS へのアプローチは、グループ全体の業務継続計画プログラムを活用しています。
- **業務継続計画 (BCP)** においては、グローバルかつ体系化されたプログラムを採用し、当グループの体制とコンティンジェンシープランを定めています。BCP は当グループの各ビジネス・ユニット単位で策定され、各業務の重要性や目標復旧時間 (RTO - インシデント発生後に BCP が利用できない最大許容時間) などの詳細が含まれています。ディペンデント・アセット、業務要件、シナリオに依存しない業務復旧戦略 (代替策を含む) も文書化されています。BCP は定期的に見直し、更新しています。
- **アセットベース・レジリエンスプログラム** は、当グループにおけるディペンデント・アセットのレジリエンス能力を確保することに重点を置いています。具体的には、

  - **テクノロジー障害復旧プログラム** : 障害復旧計画は、ネットワークやアプリケーション、マーケットデータやその他の共有システムを含む、中核となるテクノロジーインフラストラクチャーの復旧を図るための計画とそのテストに注力しています。アプリケーションはそれぞれ適切な RTO と目標復旧時点 (RPO: 予期せぬデータ損失インシデント発生時に許容される、時間で表される最大のデータ損失量) を定めるとともに、これらの指標以内でのデータとアプリケーションの復旧に要する手順を策定しています。
  - **サイバー・レジリエンス** : 当グループは、外部からの脅威および内部の悪意ある活動の両方に対する防御として、情報セキュリティ、特にサイバーセキュリティを重視しています。当グループの情報セキュリティおよびサイバーセキュリティプログラムは、情報およびテクノロジー環境の機密性、完全性、可用性を維持します。このプログラムのフレームワークと取り組みは、[クライアント・セキュリティ・ステートメント](#) に要約されています。

- **サードパーティ・ベンダー・レジリエンスプログラム**:ベンダー・レジリエンスプログラムは、サードパーティにおける業務障害発生時からの復旧能力の適切性と有効性を評価するものです。当グループの重要なサードパーティについて、サービスが受けられなくなった場合の出口戦略および代替戦略についても文書化しています。代替手段がすぐに用意できない場合、リスクエクスポージャーを把握するためにさらなる分析を行い、リスク低減のためのコントロールやその他のレジリエンス強化など、適切な是正措置を実施します。
- **施設のレジリエンス**:当グループの施設のレジリエンスは、各拠点における業務やシステムの重要性の分析によって決まります。ビジネスのレジリエンス要件を満たすため、無停電電源装置(UPS)による保護、ユーティリティサービス・通信の多様化、バックアップ発電機の設置などのレジリエンス機能を、必要に応じて導入しています。
- **ピープル・ウェルネスプログラム**:当グループは、幅広いレジリエンス・リソースプログラムを通じて、従業員やその家族を支援しています。例えば、世界保健機関と疾病管理センターの潜在的なパンデミックに関する情報を積極的にモニタリングしており、必要に応じて実施する手順を文書化しています。

## 危機管理

当グループの危機管理プログラムは、業務障害時の対応と復旧において、会社全体で連携したアプローチを採用しています。障害に対して効率的・効果的に対応するため、多岐にわたり迅速に対応する態勢を確立・維持しており、そのなかには次のようなものがあります。

- 当グループの世界各地域に設置された危機管理センター(CMCs)。CMCsは危機の状況を把握し、既定の危機管理手順を実行し、緊急対策を指揮します
- 業務障害発生時にその状況分析、報告、意思決定を支援するように指名・訓練された危機対応チーム
- 現地の規制当局との情報共有や対応を円滑に行い、また当グループにおける業務障害により影響を受けうる、外部のステークホルダーや当グループの従業員へのコミュニケーション
- 業務障害発生時およびその全期間を通じて、主要なステークホルダーと初動対応者に迅速に通知するために、定期的にテストされたプロセスとコミュニケーションツール
- 重要なサードパーティでの業務障害時における、当グループへの連絡手順等を含む適切な取り決め

## オペレーショナル・レジリエンスおよび危機対応訓練

当グループは、グループ全体のオペレーショナル・レジリエンスプログラム(業務継続を含む)の実施と管理に関わる従業員にトレーニングを提供しています。さらに、危機対応に関わる従業員に対しては、業務障害時における各自の責任を認識させるためのトレーニングが提供されています。ゴールドマン・サックスの従業員や施設に影響を及ぼす可能性のある事象を報告するためのリソースも用意されています。

## レジリエンス・テストおよび危機管理テスト

当グループは、危機対応、復旧、および業務継続能力を評価するために、設定された頻度で数種類のテストを実施しています。

- **BCPリカバリー・ストラテジー・テスト**: (人、施設、システム、外部業務委託先などの)アセットを1つ以上喪失した場合、業務やプロセスの引き継ぎ、在宅勤務、代替施設、およびアセットの代替策などの代替的な手段で業務を遂行します。これらの代替ソリューションは、当グループの規定に従って、毎年テストを実施しています。
- **重要なビジネスサービス(IBS)の統合テスト**: 極端だが起こり得る重大なシナリオに基づいて、当グループの重要なプロセスの復旧能力を評価するために、IBS統合テストと呼ばれる一連の対応・復旧のシミュレーションテストを少なくとも年に一度実施しています。
- **テクノロジー障害復旧テスト**: 業務障害後の復旧能力を実証するために、その重要度に応じて、さまざまな

頻度でアプリケーションの障害復旧テストを実施します。

- **サードパーティ・ベンダー・レジリエンス・テスト:** サードパーティ・ベンダーのレジリエンスは、当グループのサードパーティ・オペレーショナル・レジリエンス・アシュアランス(TORA)およびベンダー業務継続計画(VBCP)プログラムを通じて評価されます。これらのプログラムの一環として、当グループは重要なサードパーティ・ベンダーの評価を実施し、業務継続計画の適切性と有効性、およびビジネスにおいて求められる期間内に復旧する能力を評価します。
- **危機対応テスト:** 当グループは、危機対応時に期待される行動を強化し、プログラムやプロセスを継続的に改善する機会とすべく、机上演習や実地訓練を通して、定期的に危機管理対応策のテストを行っています。また当グループのフレームワークは、演習や訓練の企画・実施において、自然災害、地政学的事象、およびその他の環境や健康への危害など、特定の場所や地域のリスク特性を加味しています。

上記の通り、当グループは前年度において、ポリシー要件に従いこれらのレジリエンス・テストを完了しております。また、テスト要件の遵守状況を把握し、必要に応じて適切な委員会等に報告しております。テストの結果として生じる対応策は、適切に把握・管理しています。

### **お客様へ：連絡とご質問**

本書面は、当グループのオペレーショナル・レジリエンスプログラムの概要を提供するものです。さらにご質問がございましたら、当グループの各担当者にご連絡をいただきますようお願い申し上げます。なお、当グループのセキュリティ上支障の出かねないプログラムに関する具体的なご質問にはお答えしかねることがございます。

本概要に関連する最新情報については、こちらのウェブサイト(<http://www.goldmansachs.com/japan/business-continuity-plan>))にてご覧いただけます。

### **最終更新: 2025 年 6 月 10 日**

本文は英語の原文を翻訳したものです。本文と原文に相違がある場合には、英語の原文(<https://www.goldmansachs.com/disclosures/business-resilience.pdf>) が優先します。