リスク管理とマテリアリティ・マネジメント

1. リスク管理の基本方針

当グループは、経営健全性の確保、経営戦略に基づくリスクテイクを通じた収益確保、持続的成長のため、グループ経営方針、内部統制基本方針に基づき、リスクの特定、評価、モニタリング、コントロールおよび削減、高度化検証・見直しなどの一連のリスク管理活動をとおして、リスクの状況を的確に把握し、リスクに対して必要な措置を講じることを基本方針としています。

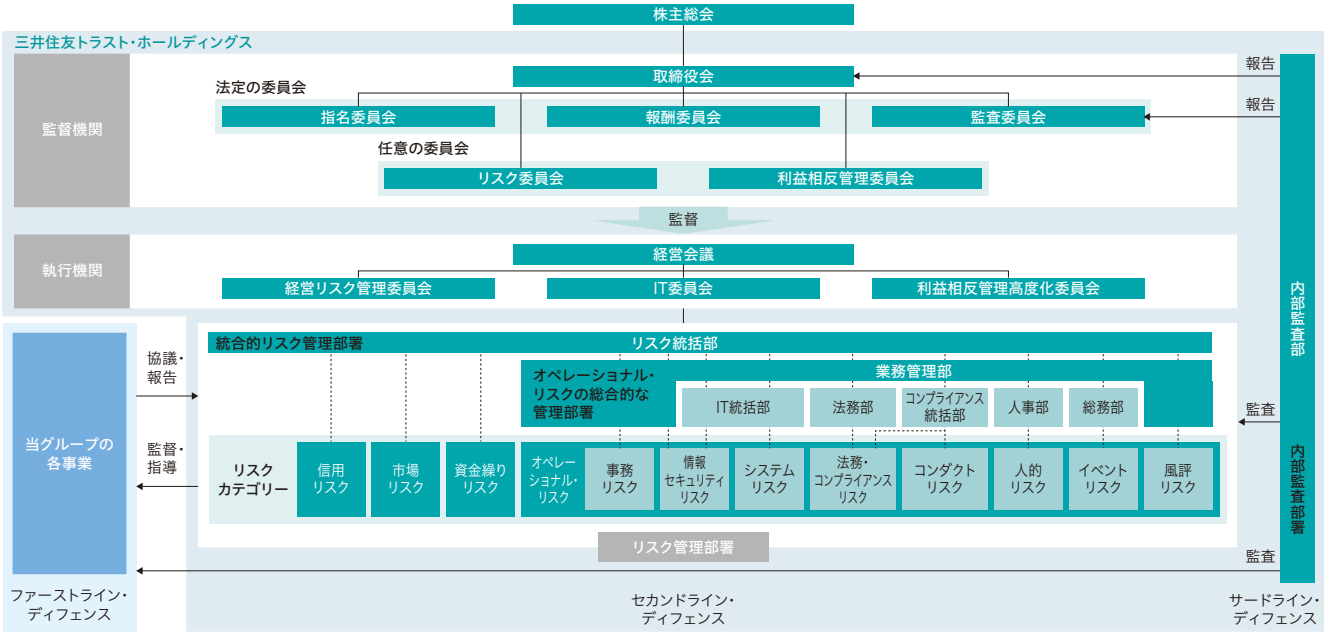
当グループのリスク管理のフレームワークは、リスクアペタイト・フレームワーク（RAF）※を取り込み、一体化してグループ内で有機的に機能しています。

※当グループの存在意義（パーパス）および経営理念に基づき策定した経営戦略の実現のため、リスクキャパシティの範囲内で、リスクアペタイト（経営計画達成のために進んで受け入れるべきリスクの種類と総量）を決定するプロセスおよびその適切性・十分性をモニタリングし担保する内部統制システムから構成される全社的な経営管理の枠組み

2. リスクガバナンス体制

当グループは、リスクアペタイト・フレームワークのもと、グループ全体のリスクガバナンス体制として、各事業によるリスク管理（ファーストライン・ディフェンス）、リスク統括部およびリスク管理各部によるリスク管理（セカンドライン・ディフェンス）、内部監査部による検証（サードライン・ディフェンス）の三線防御体制（スリーラインズ・オブ・ディフェンス）を構築しています。

リスクガバナンス体制



(1)ファーストライン・ディフェンス

グループ各事業は、業務商品知識を生かして自事業の推進におけるリスク特性の把握を行います。各事業は定められたリスクテイクの方針に基づき、リスクアペタイトの範囲内でリスクテイクを行うとともに、リスクを評価し、リスクが顕在化した際には現場レベルでのリスクコントロールを迅速に実行します。また、リスク管理の状況をセカンドラインに適時に報告します。

(2)セカンドライン・ディフェンス

リスク統括部およびリスク管理各部は、各リスクカテゴリーの管理部署として、取締役会によって決定されたグループ全体のリスク管理方針に従い、ファーストラインから独立した立場で、ファーストラインのリスクテイクへの牽制機能を発揮し、リスクガバナンス体制の監督・指導を行います。

リスク統括部は、統合的リスク管理部署として、グループ全体を対象にリスクを特定・評価し、リスク管理プロセスを

構築し、リスク限度枠の設定を行うほか、リスクが顕在化した場合の全社リカバリー戦略をあらかじめ策定します。また、リスク管理各部と適切に情報共有を行い、リスクおよびリスク管理全体の状況を統合的にモニタリングし、その状況を経営会議、取締役会へ報告します。

(3)サードライン・ディフェンス

内部監査部は、グループのリスクガバナンス体制およびプロセスの有効性や適切性をファーストライン、セカンドラインから独立した立場で検証します。

(4)経営会議

経営会議は、代表執行役ならびに執行役社長が指定する執行役をもって構成され、リスク管理に関する事項の決定および取締役会決議・報告事項の予備討議を行います。

(5)取締役会

取締役会は、取締役全員をもって組織され、当グループの経営方針およびリスクテイクの戦略目標を決定し、リスクの所在と性質を十分認識した上で、戦略目標を踏まえたリスク管理方針などを策定し、適切なリスクガバナンス体制を整備し、実施状況を監督します。また、取締役会は当グループのビジネス戦略やリスクの特性を踏まえ、任意の諮問機関として「リスク委員会」および「利益相反管理委員会」を設置しています。

リスク委員会

リスク委員会は、当グループの経営を取り巻く環境認識に関する事項、リスク管理の実効性に関する事項などに関し、取締役会からの諮問を受けてその適切性などを検討し、答申を行います。

利益相反管理委員会

利益相反管理委員会は、信託の受託者精神に基づき当グループが目指す、お客さまの「ベストパートナー」の基盤となる、フィデューシャリー・デューティーおよび利益相反管理に関する事項に関し、取締役会から諮問を受けてその適切性などを検討し、答申を行います。

3. リスク管理のプロセス

当グループでは、リスク統括部およびリスク管理各部がセカンドラインとして、以下の手順でリスク管理を行います。また、このリスク管理プロセスについては、関連するシステムを含め、サードラインの内部監査部により定期的に監査されます。

(1)リスクの特定

当グループの業務範囲の網羅性も確保した上で、直面するリスクを網羅的に洗い出し、洗い出したリスクの規模・特性を踏まえ、管理対象とするリスクを特定します。この中で、特に重要なリスクを「重要リスク」として管理します。

(2)リスクの評価

管理対象として特定したリスクについて、事業の規模・特性およびリスクプロファイルに見合った適切なリスクの分析・評価・計測を行います。「重要リスク」については、定期的に、「発生頻度」「影響度」および「重要度」を評価し、トップリスク(1年以内に当グループの事業遂行能力や業績目標に重大な影響をもたらす可能性があると考えているリスク)やエマージングリスク(中長期に重大な影響をもたらす可能性があると考えているリスク)などに該当するかどうかの判断を行います。

(3)リスクのモニタリング

当グループの内部環境(リスクプロファイル、配分資本の使用状況など)や外部環境(経済、市場など)の状況に照らし、リスクの状況を適切な頻度で監視し、状況に応じ、グループ各事業に対して勧告・指導または助言を行います。モニタリングした内容は、定期的にまたは必要に応じて取締役会、経営会議などへ報告・提言します。

(4)リスクのコントロールおよび削減

リスク量がリスク限度枠を超過したとき、もしくは超過が懸念されるなど、経営の健全性に重大な影響を及ぼす事象が生じた場合には、取締役会、経営会議などに対して適切に報告を行い、リスクの重要度に応じ、必要な対応策を講じます。

4. 当グループのリスク特性

当グループは、信託銀行グループとして、信託の受託者精神に立脚し、高度な専門性と総合力を駆使して、銀行、資産運用・資産管理、不動産などを融合したトータルソリューション型ビジネスモデルで独自の価値を創出することを目指しています。

当グループの各事業はそのビジネス特性に応じ、信用リスク、市場リスク、資金繰りリスクおよびオペレーショナル・リスクといったさまざまなリスクにさらされています。

こうしたなか、信託業務関連のリスクについては、留意すべき基本的事項を取りまとめたグループベースの「信託業務指針」を管理高度化の礎として制定しているほか、三井住友信託銀行では、信託受託者としての善管注意義務・忠実義務・分別管理義務などの観点も加え、信託業務関連のリスクについて主にオペレーショナル・リスクのカテゴリーで管理しています。また、コンダクトリスクについても、三井住友信託銀行において、主要なリスクの状況を定期的に把握し、社内研修等を通じて役員・社員の意識の浸透・醸成に努めることにより、リスクの削減・管理、リスク顕在化の未然防止に取り組んでいます。

当グループでは、フォワードルッキングな視点で、経営者が定期的にトップリスクやエマージングリスクを選定の上、リスクの状況をモニタリング、コントロールしながら、対応策を講じ、取締役会等への報告を行っています。当グループのESGにかかわる主なトップリスク・エマージングリスクとその対応策は以下の通りです。

新型コロナウイルス感染症の世界的流行に関するリスク

〈リスクの内容〉

新型コロナウイルス感染症の世界的流行が長期化することにより、世界経済に悪影響をもたらす可能性があります。当グループにおいては、事業戦略への悪影響や、与信先の事業等への悪影響を通じて、信用ポートフォリオの質が悪化し、与信関係費用が増加する可能性があります。また、当グループの社員、関係者への感染が増加すれば、業務継続が困難となる可能性があります。これらにより、当グループの業務運営や業績等に悪影響が及ぶ可能性があります。

〈当グループにおける対応策〉

- 当グループは、信用ポートフォリオについて、定期的にマクロ経済シナリオをベースにしたストレステストを実施しており、ストレス時のアクションプランを策定しています。経済環境や内部格付の変動状況等を踏まえ、新型コロナウイルス感染症の拡大による業績への影響度合いや収束後の回復の見通しの程度に応じて、業種ごとに将来の信用リスクの悪化の程度に関する仮定を置き、当該業種に属する一部の与信について将来発生すると予想される信用損失の再見積りを行い、追加的な貸倒引当金を計上しています。
- 業務継続に関するリスクに対しては、緊急対策本部を設置し、「社員および家族の健康と安全確保」「社会インフラとしての業務継続維持」「社会への感染拡大防止（感染拡大しにくい社会形成への活動を含む）」を基本スタンスと定め、国内外の感染状況、政府要請、顧客動向等を踏まえた機動的な対応を行ってきており、BCPに定める各種業務継続策の実施、テレワーク勤務の積極的活用などにより、サービス維持と安全面の両立を図っています。

サイバー攻撃に関するリスク

（詳細は43-45頁参照）

法務・コンプライアンスリスク

〈リスクの内容〉

当グループは、銀行法、金融商品取引法、金融機関の信託業務の兼営等に関する法律等の各種法令諸規則等の遵守を徹底していますが、役員および社員が遵守を怠った場合、当グループに対する罰則・行政処分や市場での評価の失墜を招く可能性があります。また、当グループが提供する商品・サービスがお客さまの期待に合致せず、業務遂行の過程で発生するさまざまなトラブルやクレームに起因して損害賠償請求訴訟を提起される可能性があります。これらにより、当グループの業務運営や、業績および財務状況に悪影響が及ぶ可能性があります。

〈当グループにおける対応策〉

- 当グループは、グループ各社の業務特性に応じた適切なコンプライアンス態勢を整備するため、コンプライアンス・プログラムを策定し、進捗・達成状況を管理しています。
- 当グループは、グループ全体としてコンプライアンス意識の浸透を促進するため、コンプライアンス研修を強化しています。具体的には、グループ全体にまたがるテーマにつ

いて、eラーニング研修やディスカッション型勉強会などの研修資料をグループ各社に提供しています。グループ各社は、業務・商品の特性やお客さまの属性に応じた研修、勉強会および個別テーマに関するeラーニング研修を実施しています。

- 当グループは、議決権行使集計業務にとどまらず、全ての事業において業務品質の改善、向上のプロセスが真に定着しているか確認を進めていきます。

データ管理に関するリスク

〈リスクの内容〉

当グループは、お客さまへのさまざまなサービスの提供や対外的な報告等のため、多くのシステム等を使用しており、その中には、個人情報を含むさまざまな情報が含まれています。当該経営情報等の管理について、バーゼル銀行監督委員会の「実効的なリスクデータ集計とリスク報告に関する諸原則（BCBS239）」に沿って確立したデータガバナンス体制を適用する業務範囲の拡大と高度化が必要となります。これらの経営情報等のデータ管理プロセスに不備があることにより、経営の意思決定等を誤り、当グループの企業価値の低下や信頼を失う可能性があります。これにより、当グループの業務運営や業績等に悪影響が及ぶ可能性があります。

〈当グループにおける対応策〉

- 当グループは、個人情報、経営情報の管理に関する規程類を整備し、継続的なデータ管理の強化およびBCBS239に沿ったデータガバナンスの高度化に努めています。
- 情報管理に関するポリシーや事務手続き等を策定しており、社員に対する教育・研修等により情報管理の重要性について周知徹底しています。

気候変動に関するリスク

〈リスクの内容〉

中長期的気候変動により、自然環境や社会インフラ、お客さまの資産等に物理的被害が及ぶリスク（物理的リスク）が増加したり、政策変更や、気候変動に対する金融市場の選好や社会通念の変化、技術革新等による低炭素社会への急速な移行（移行リスク）が起こることにより、当グループの業績や財務状況に悪影響が及ぶ可能性があります。

具体的には、自然災害により与信先の信用状況や担保資産の価値が悪化し、当グループの信用ポートフォリオに悪影響をもたらすリスク（物理的リスク）や、低炭素社会への急速な移行により、二酸化炭素を多く排出する企業が発行する有価証券や当該企業向け貸出金等、当グループの保有資産の価格が下落するリスク等（移行リスク）があります。

〈当グループにおける対応策〉

- 当グループは、2021年10月にカーボンニュートラル宣言を行い、本宣言を着実に推進するため、Net-Zero Banking Alliance（NZBA）へ加盟しました。
- 当グループは、金融安定理事会（FSB）の気候変動関連財務情報開示タスクフォース（TCFD）の最終提言（2017年6月）に基づき、気候変動関連リスクを全社的リスク管理の枠組みの中で管理していきます。
- 信用リスク管理において、セクターポリシーを策定し、温暖化ガスの排出量が多い石炭火力発電所向けの新規融資は原則禁止することとしており、関連指標を定期的にモニタリングしています。
- 中長期的な視点で、移行リスク、物理的リスクが当グループに与えるインパクトを計測するシミュレーションを実施しています。

イノベーションに関するリスク

〈リスクの内容〉

フィンテック等、金融ビジネスに関わるテクノロジーの高度化は、業界の垣根を越えて進歩し、お客さまの行動にも変化が生じています。当グループがこのような変化に適応できない場合、競争力の低下や事業規模の縮小等につながる可能性があり、これにより、当グループの業績や財務状況に悪影響が及ぶ可能性があります。

〈当グループにおける対応策〉

- デジタル技術を活用した既存業務のオペレーションの効率化や、信託銀行固有の領域における新たなプラットフォームの構築等に取り組んでいきます。

日本の少子高齢化の進展に関するリスク

〈リスクの内容〉

我が国の人口動態の変化により、当グループのお客さま

の年齢構成等も中長期的に変化していきます。当グループの個人向けコンサルティング業務、住宅ローン業務のお客さまが中長期的に減少する可能性があり、これにより、当グループの業績や財務状況に悪影響が及ぶ可能性があります。

〈当グループにおける対応策〉

- 「人生100年時代」を迎え、老後資金準備への不安により資産形成機運が高まっており、信託銀行の多彩な機能を活用した当グループならではのビジネスモデルへの進化・高度化に努めています。

5. 統合的リスク管理

(1)統合的リスク管理体制

当グループでは直面するリスクに関して、それぞれのリスクカテゴリーごとに評価したリスクを総合的に捉え、経営体力と比較・対照することによって、リスク管理を行っています(統合的リスク管理)。

当グループでは、年に1回、リスク管理やリスクコントロールの実効性を評価し、環境変化などにより必要が生じたと判断した場合は、リスクカテゴリーの体系、リスク管理体制などの見直しを検討することとしています。

また、当グループでは統合的リスク管理における管理対象リスクのうち、VaR※などの統一的尺度で計量可能なリスク値を合算して、経営体力(自己資本)と対比することにより管理しています(統合リスク管理)。

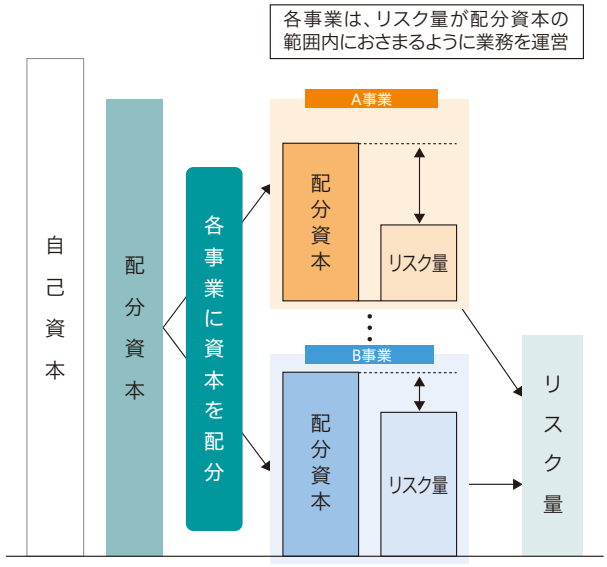
※バリュー・アット・リスク(Value at Risk)

(2)資本配分運営

当グループでは、外部環境、リスク・リターンの状況、シナリオ分析および自己資本充実度評価の結果を踏まえ、各リスクカテゴリー(信用リスク、市場リスク、オペレーショナル・リスク)を対象に、グループ各社を含めた各事業へ資本を配分する運営を行っています。資本配分の計画は、取締役会で決議しています。配分する資本の水準は、当グループのリスクアペタイトに基づいて決定されます。

各事業は、リスク量が配分された資本の範囲内、かつリスクアペタイトの範囲内となるように業務を運営します。また、リスク統括部は、月次でリスク量を計測し、配分された資本およびリスクアペタイトに対するリスクの状況を、定期的に取締役会などに報告しています。

資本配分の仕組み



(3)ストレステストと自己資本充実度評価

リスク統括部は、資本配分の計画の策定および見直しの都度、預金者保護の視点による自己資本充実度の確保のため、仮想シナリオ、ヒストリカルシナリオおよび発生確率検証の3種類のストレステストを実施し、その結果に基づき自己資本充実度を評価の上、取締役会などに報告しています。

仮想シナリオによるストレステスト

十分に強く、かつ現実的に発生可能性のあるストレスシナリオを策定し、ストレス時の自己資本比率等を推計することによって、自己資本充実度を評価します。

ヒストリカルシナリオによるストレステスト

過去に発生したストレス期におけるパラメータ等を用い、ストレス時の自己資本比率等を推計することによって、自己資本充実度を評価します。

発生確率検証

信頼区間99.9%のリスク量を算出し、その値を自己資本比率規制上の総自己資本と比較することによって、自己資本充実度を評価します。

ストレステストの枠組み

①シナリオ案策定	将来の「仮想シナリオ」、過去イベントの「ヒストリカルシナリオ」等の複数案を策定
②シナリオ協議・選定	役員が出席する委員会等において、シナリオを協議・選定
③影響額評価	選定シナリオ発生時の影響額を算定し、自己資本充実度の評価等を実施
④取締役会等への報告	評価結果の報告を受け、経営計画策定に活用

6. リスク文化の醸成と浸透

当グループでは、リスク文化を「信託の受託者精神に基づく高い自己規律のもと、リスクの適切な評価を踏まえたリスクテイク、リスク管理、リスクコントロールを機動的に実行する当グループの組織および役員・社員の規範・態度・行動を規定する基本的な考え方」と定義しています。

当グループでは、リスク文化の醸成・浸透のため、経営計画策定時にビジネスごとのリスクテイク方針を明確化するとともに、役員・社員全員が適切なリスクテイクを行うことを通じて、当グループが持続可能なビジネスモデルを構築し、企業価値向上およびステークホルダーの価値向上に貢献することを目指しています。また、リスクアペタイト・フレームワークを明文化したリスクアペタイト・ステートメント（RAS）を策定し、当グループの共通言語として、グループ内のリスクアペタイトに関する活発な議論に活用しています。

7. 災害時における危機管理・業務継続（BCP）

（1）当グループの取り組み

当社と三井住友信託銀行では、自然災害やシステム障害、新種感染症の流行などの危機発生時において、緊急時対応を迅速に実行するため、コンティンジェンシープランを整備しています。

さらに、資金決済などの重要な業務については、BCP（業務継続計画）やバックアップオフィスなど、業務継続体制を整備し、その実効性を確保するため、定期的な訓練、BCP見直しの実施など、業務継続のための体制を整備しています。

発生した危機が重大で影響が広範囲に及ぶなど、三井住友信託銀行や当グループの正常な業務活動に重大な支障を及ぼし、その対応に緊急に総合的かつ高度な経営判断を要する場合には、全社的対応組織として緊急対策本部を設置して、緊急時対応を迅速に実行していきます。

特に、全国に店舗を持つ三井住友信託銀行では、大規模な地震が発生した場合に備え、お客さま、社員の安全や業務の継続などに配慮した対応を行うとともに、その実効性を確保するため、定期的に訓練を実施しています。

全社的な対応においては、緊急対策本部機能の実効性を高めるため、定期的な訓練のほか、情報収集・情報連携の体制強化とともに、東京地区での発災を想定して大阪地区の体制強化も推進しています。

また、支店においては、定期的な訓練を通じ対応力の強化を図るとともに、立地条件や主要設備の状況等、店舗固有事情を踏まえた災害対策への取り組みを推進し、また、支店間での支援体制も整備しています。

（2）サイバー攻撃の脅威への対応

国内外で被害が拡大しているサイバー攻撃の脅威からお客さまの大事な財産を守るため、当社では各種の対応を実施しています（詳細は43-45頁参照）。

役員・社員の行動基準

1.役員・社員は危機管理の重要性を十分に認識・理解し、緊急事態の発生に備えるとともに、緊急事態が発生した場合には、迅速かつ的確に対応できるよう、平素より知識の涵養等に努めなければならない。

2.緊急事態が発生した場合には、役員・社員の判断・行動にあたっては、以下の原則に基づき対応しなければならない。

(1)生命の安全確保
緊急事態が発生した場合は、お客さま、役員・社員とその家族の安全を最優先で確保する。また、各種緊急時対応においては、常に人道面での配慮を優先させる。

(2)三井住友信託銀行の企業資産の保全
緊急事態が発生する場合に備え予防と減災措置をとり、緊急事態が発生した場合には三井住友信託銀行の企業資産を保全する。また、業務活動に支障となる悪影響に対して、可能な限りリスク軽減措置を講じる。

(3)業務継続と早期復旧
緊急事態が発生した場合、優先する業務の早期復旧と継続を図る。

(4)地域社会との連携
緊急事態が発生した場合、地域における救命活動等、地域との連携を図る。

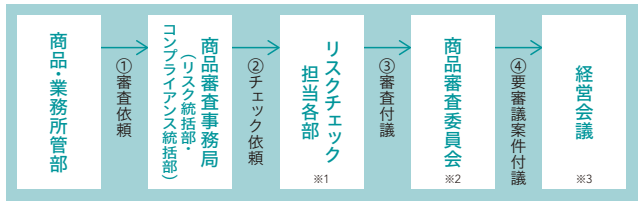
8. 新商品・サービスの導入時審査体制と導入後管理体制

新商品・サービスを導入する際には、あらかじめ内在するリスクの有無、種類の特定・評価・管理、お客さまへの説明資料・手法など、商品や業務を継続するためにさまざまな体制整備を行う必要があります。このため、当グループでは新商品・サービスの導入時に審査を実施する体制としています。

この審査プロセスにおいては、お客さまから信頼していただける商品・サービスの導入を重視し、複数の部署がさまざまな角度から検証を行います。

新商品・サービスの導入後は、商品審査委員会で審査された案件については、リスク管理の観点も含め、導入後の取り組み状況を定期的にモニタリングしています。また、商品審査委員会での審議の有無にかかわらず、環境変化などによりお客さまへの説明内容が変わることが想定される商品・サービスに対しても、適切な説明を行う観点から、定期的にモニタリングを行っています。これらの検証結果を商品審査委員会へ報告するとともに、審査時の前提条件と異なる事態が発生した場合には対応方法を協議し、その内容をリスク統括部およびコンプライアンス統括部の統括役員へ報告します。

商品審査のプロセス(三井住友信託銀行)



※1 リスク統括部、コンプライアンス統括部、法務部、業務部、FD・CS企画推進部、財務企画部、業務管理部など
※2 商品性を勘案し、利益相反の観点で審査が必要な場合は「利益相反管理高度化委員会」と合同開催します。
※3 三井住友信託銀行の経営会議付議案件のうち当グループの経営に重大な影響を与える可能性のある新商品などについては、当社宛協議することとしており、経営会議への付議・取締役会への報告を行う枠組みとしています。

9. 情報セキュリティリスクとサイバーセキュリティ対策

情報セキュリティリスク管理態勢

当グループは、情報資産は最も重要な経営資源の一つという認識のもと、個人情報・顧客データ保護を経営基盤マテリアリティの一つに設定するほか、情報セキュリティリスクを「情報の漏えい、情報が正確でないこと、情報システムが利用できないこと、情報の不正使用等、情報資産が適切に維持・管理されないことにより、当グループが損失を被るリスク」と定め、オペレーショナル・リスク内のリスクサブカテゴリーの一つに位置付けて、統括役員および管理部署を設置し、顧客情報の適切な管理やサイバーセキュリティ対策を行っています。

また、お客さまや株主の皆さまの個人情報などの保護に万全を期するための取組方針を「個人情報保護宣言」として定め、公表し、これを遵守することを宣言しています。

管理態勢や情報の取り扱い等について、個人情報保護法、関連法令および金融庁が定める「金融分野における個

人情報保護に関するガイドライン」等に則り、社内規程類を整備するとともに、年2回定期的に全社員向け研修を実施する等を通じて、日常業務における各種情報の取り扱いに関する留意事項の周知に加え、情報セキュリティに関するプリンシプルベースでの理解浸透を図っています。

情報セキュリティリスク管理に関連する規程類

規程	個人情報保護宣言、リスク管理規程
規則	リスク管理規則、オペレーショナル・リスク管理規則、情報セキュリティリスク管理規則、システムリスク管理規則
要領	情報セキュリティリスク管理要領、システムリスク管理要領、個人情報取扱要領、個人データ管理事務取扱要領、CSIRT運営要領、社内OA管理取扱要領、顧客情報の社外持出に係る事務取扱要領、等

組織体制等

情報セキュリティリスクに関する事項は、オペレーショナル・リスク内のリスクサブカテゴリーとして、三井住友トラスト・ホールディングスでは経営リスク管理委員会において、三井住友信託銀行ではオペレーショナル・リスク管理委員会において、管理態勢の整備、計画の策定およびリスクの特定・評価・モニタリング・コントロールといった一連のプロセス等を総合的に審議しています。また、方針や計画については経営会議での審議を経て取締役会が決定しています。一連のプロセスについては権限規程等に基づき情報セキュリティリスクの管理部署である業務管理部およびIT統括部をはじめとする各部署等において実行しています。これら管理態勢全般について、業務管理部統括役員およびIT統括部統括役員が情報セキュリティリスク管理全般の統括役員として統括する態勢としています。

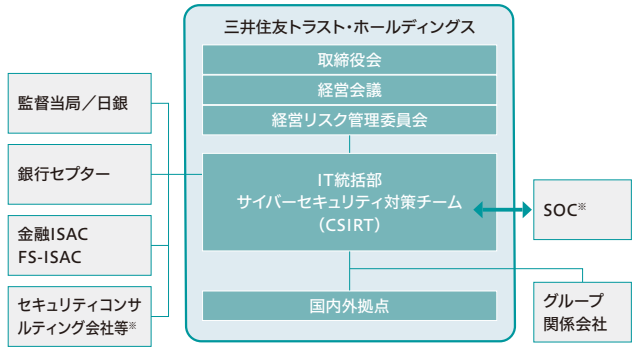
組織体制	取締役会、経営会議 経営リスク管理委員会 （三井住友トラスト・ホールディングス） オペレーショナル・リスク管理委員会 （三井住友信託銀行）
統括役員	業務管理部統括役員およびIT統括部統括役員
管理部署	業務管理部およびIT統括部

サイバーセキュリティ管理態勢

当グループは、サイバー攻撃をガバナンス・経営基盤マテリアリティの一つに設定するほかトップリスクに選定しており、「サイバーセキュリティ経営宣言」を策定の上、経営主導によるサイバーセキュリティ対策の企画・推進を行っています。

- サイバーセキュリティ対策の専門組織としてSuMiTRUST-CSIRT※1を設置し、グループ内外から脅威情報や脆弱性情報を収集・分析、セキュリティ対策を企画・導入し、経営へ報告する管理態勢を構築しています。またセキュリティ対策の検討会やIT委員会を通じて、外部知見も活用の上高度化を進めています。
- 米国のセキュリティ基準に基づく社内規程類を制定し、サイバー攻撃に対する平時、有事の対応プロセスを整備しています。
- 関係会社を含む当グループにおいて、サイバーセキュリティリスクアセスメントやシステム脆弱性診断を定期的に実施するほか、サイバーセキュリティ関連規程類の共通化を進め、グループ全体のサイバーセキュリティ態勢の高度化・標準化を推進しています。

サイバーセキュリティ管理体制



※SOC：Security Operation Centerの略称。ネットワークを監視し、サイバー攻撃の検出や分析を行う。

監視体制

当グループはインターネット通信のグループ共通基盤を構築しており、共通基盤ネットワークにおいてSOC（Security Operation Center）による24時間365日監視や各種データの相関分析による脅威検知を行っています。これらはSuMiTRUST-CSIRTに情報集約しており、CSIRTを中心とした監視体制を構築しています。

サイバーセキュリティ対策高度化

サイバー攻撃への技術的な対策として、境界型防御策（入口対策、出口対策、内部対策の多層防御）を構築しており、DDoS攻撃対策やフィッシングサイトの検知・遮断等の各種対策によりリスク低減を図っています。

また、サイバーセキュリティヒートマップを用いたリスク状況の自己分析、FFIEC-CAT※2など国際的なサイバーセキュリティアセスメントツールを用いた第三者評価を定期的に実施するほか、金融ISAC※3や内閣サイバーセキュリティセンターが主催するサイバー演習に参加するなど、サイバーレジリエンス強化に向けPDCAサイクルによる対策高度化を進めています。さらに、サイバー保険による万が一への備えも行っています。

技術的な主な対策	
入口対策 出口対策	• 悪意のある通信の検知、遮断（含むDDoS攻撃対策） • ウイルスやマルウェア（不審なアプリ）の侵入を阻止 • 振舞検知による不審な通信の規制 • 脆弱性診断によるインターネット経路の脆弱性の評価・改善
内部対策	• エンドポイント（社内OA端末やサーバー）に侵入したマルウェアの挙動を検知
統合監視	• ファイアーウォールやプロキシサーバーなどから取得する複数の通信ログを統合的に分析し検知精度を向上 • 暗号化通信（HTTPS等）を複合化の上分析し検知範囲を拡大

ニューノーマルへの対応

新型コロナウイルス感染症への対応として、当グループにおいても在宅勤務・テレワーク環境が急拡大しています。テレワークに関わるサイバーセキュリティリスクに対しては、リモート端末等のセキュリティ対策・情報管理を徹底し、リスクアセスメント、侵入テストにより安全性を確認しています。

セキュリティ人材の育成

サイバーセキュリティの高度な専門知識を有する人材を育成するため、CSIRTでは社内検討会における社外専門家との協業、金融ISAC、FS-ISAC※4等の社外コミュニティへの参加、社外研修や資格取得支援、大学院への社員派遣などを行っています。

また、全社員を対象とした情報セキュリティ研修やフィッシングメール訓練、外部機関と連携したサイバー演習を通じて、社員教育にも継続的に取り組んでいます。

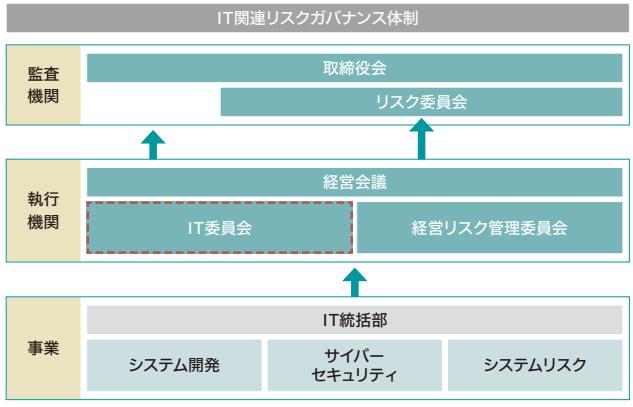
システムリスク管理態勢

大規模障害や災害による情報システムへの影響極小化、早期復旧ならびに業務継続へ備えるため、グループの連絡・対応体制を明確化し、代替措置・復旧手順などを整備するとともにオペレーションの教育・訓練などを行い、レジリエンス強化に努めています。

また、一定規模のシステム開発に起因する遅延・費用増加等に関わるリスクに対しては、大型システム開発案件の進捗管理・品質管理面のモニタリングを行い、IT委員会へ報告・協議する体制となっており、システム開発の適正運営に努めています。

IT委員会

IT委員会は、IT統括部統括役員を含む経営管理各部の統括役員、部長、および外部委員をもって構成され、重要なシステム投資、システム技術に係る事項に関し多面的な視野からの検討・協議を行っています。リスク管理面においては、システム開発に起因するリスク、サイバーセキュリティおよびシステムリスクなどについて本委員会にて共有・協議しており、諮問機関として社外の専門家である外部委員の知見を積極的に活用し、議論の充実化、管理高度化に取り組んでいます。



※1 CSIRT：Computer Security Incident Response Team：攻撃予兆情報の収集・分析・対応策を進める社内組織
※2 FFIEC-CAT：FFIEC（米連邦金融機関検査協議会）が金融機関向けに公表したリスク評価ツール（Cyber Assessment Tool）
※3 金融ISAC：Information Sharing and Analysis Center：国内金融機関の情報共有組織
※4 FS-ISAC：Financial Services Information Sharing and Analysis Center：米国を中心とする金融機関の情報共有組織