経営監査の取り組み - 包括的なリスク評価（マクロアプローチとミクロアプローチ）

2019/07/03

新生銀行 グループ監査部GM　久保秀一

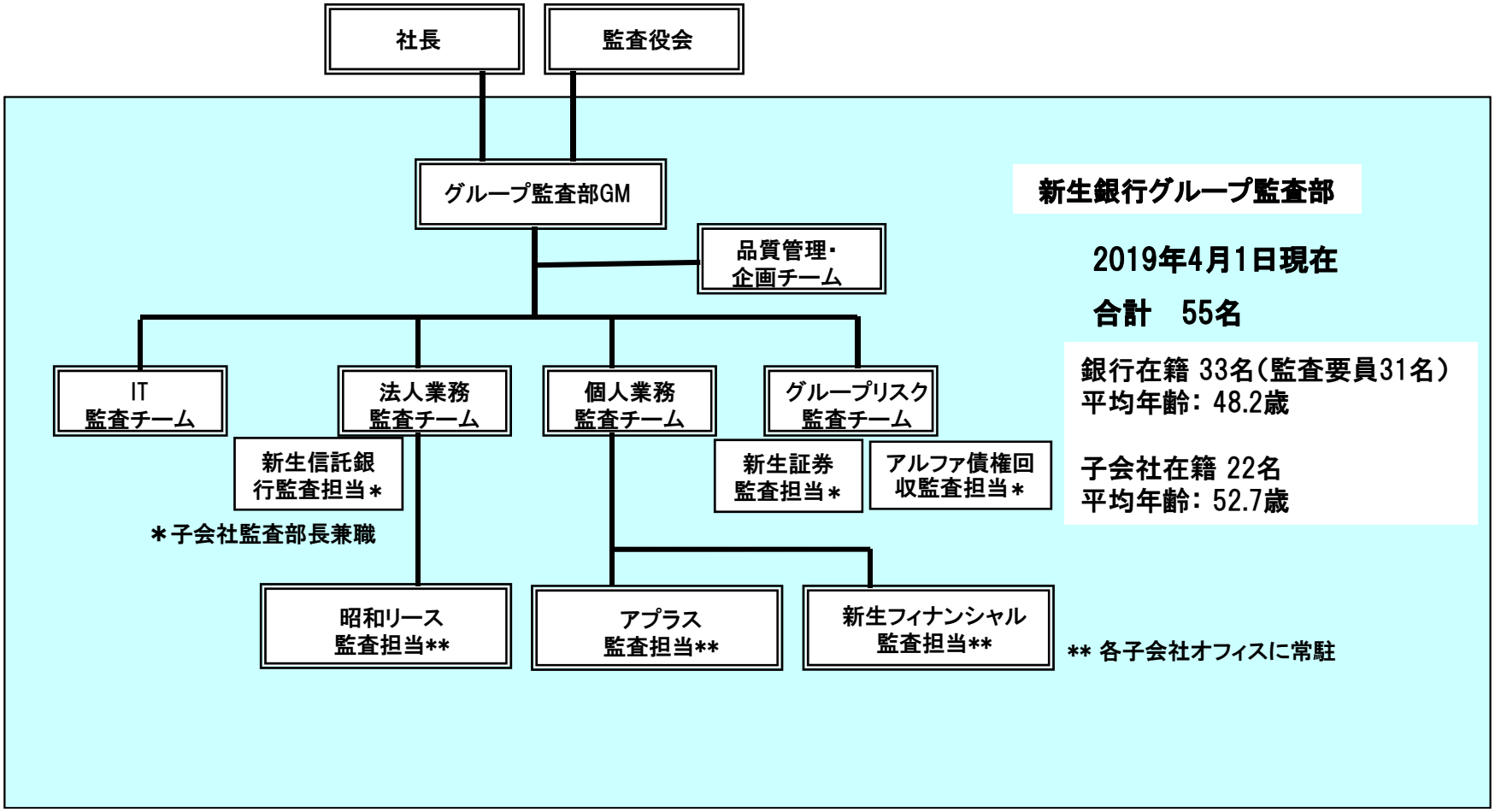
新生銀行グループ概要

- 従業員数： 単体2,248人、連結5,179人
- 本支店数: 26本支店、3出張所
- 総資産 9兆5,711億円 （連結ベース 2019年3月末）

- 法人向け及び金融市場ビジネスとして、コーポレートローン、シンジケートローン、買収ファイナンス、船舶ファイナンス、ヘルスケアファイナンス、ベンチャー企業向けファイナンス、プライベートエクイティ、リース業務、再生可能エネルギーファイナンス、クレジット・トレーディング、M&Aアドバイザリー、不動産ノンリコースファイナンス、プロジェクトファイナンス、再生ファイナンス、外国為替・デリバティブ、信託業務、証券業務など。
- 個人向けビジネスとして、リテールバンキング（総合口座、住宅ローン、投資信託）、コンシューマーファイナンス（無担保ローン、信販・クレジットカード、不動産担保ローン）など。

新生銀行グループ　内部監査体制

2017年10月1日付でグループ監査部に統合



SHINSEI BANK GROUP

直面する現実への対応： リスクベースアプローチ

・ビジネス及び関連する外的・内的環境は変化する。
=>フォワードルッキング、すなわち一時点の状態（静態）のみならず、変化状況（動態）もとらえ、今後起こりうる事態・リスクを想定し、対応していくことが経営上の課題。

・このような変化に対応した内部統制の有効性を検証することが、内部監査に対して期待されている（普遍的な要請）。
=>内部監査もフォワードルッキングで、現在の内部統制が変化するビジネスに関するリスクの顕在化を十分予防しうるか、例え顕在化してもなお速やかに発見・是正し影響を最小化しうるかを検証する（既存の管理体制を疑う）。

・内部監査のリソースは無尽蔵ではなく、限られたリソースを有効に活用して、内部監査に対する期待に応える必要がある。
=>限られたリソースを、よりリスクが高い分野に優先的に投入する。

リスクベースの監査とは何か？

**フォワードルッキングでリスクを特定・評価し、
リスクの高い分野に監査資源を
優先的に投入すること。**

すなわち

機動的に「選択と集中」を行うこと。

リスク評価の二つのアプローチ

監査の方法は、リスクアプロー チを採用しており、当行グループが直面するリスクを全行的視点からとらえたマクロリスク評価と、各部店固有のリスクを個別にとらえたマイクロリスク評価との組み合わせにより、包括的なリスク評価を行っています。相対的にリスクが大きいと考えられる業務やプロセスに対しては、優先的に監査資源を投入しています。

（新生銀行 統合報告書より抜粋）

トップダウン： マクロリスク評価項目

主なマクロリスク評価項目は以下の通り。

- 全般的な経済情勢
- 決済インフラストラクチャーの更新及びその他情報技術革新
- 法令及び監督当局等の監督指針・自主規制ガイドライン等の変更及び法令等による内部監査の要請
- 監督当局等の新生銀行グループに対する検査指摘等
- 業界ADRの状況
- 新生銀行グループのビジネスプラン、新規事業・商品
- 上半期の業績、下半期及び来期の業績予想
- トレーディングポジション・ポートフォリオ・引当金・リスクリミットの増減・使用状況
- 主要な各種委員会及び経営陣との定期連絡会より示唆されるリスク
- グループ会社の異動・組織変更、人員増減
- システム・業務フローの変更
- 当行グループにおける事務事故、法令規則等違反・苦情等の発生状況
- 労務リスク、不正リスク
- システム障害の概況
- マネー・ローンダリング及びテロ資金供与対策の状況

マクロリスク評価方法と報告

- 各項目ごとに現状と動向の確認、リスク分析および結論付け（マクロリスクの観点からハイライトして実施すべき監査プロジェクト候補の有無の確認）を行う。
- 項目によって、全社的管理体制から一部署まで監査プロジェクト候補になりうる。
- 年次監査計画上の重要課題（重要監査プロジェクト）は、このマクロリスク評価結果から特定される。
- マクロリスク評価書（A4約100ページ）は、年次監査計画書の別添資料として、計画付議（承認依頼）時に社長・監査役会に提出する。

  2019年度計画分から、「マネー・ローンダリング及びテロ資金供与対策の状況」についての分析結果を、マクロリスク評価書の別冊（A4約40ページ）として取り纏め。ここで、環境、リスク評価書、海外送金と顧客・口座、疑わしい取引の届出などを分析し、監査対象を特定。

マクロリスク評価書(1)： 全体構成

マクロリスク評価書は、以下の項目で構成される。

- 総括
  - 重要課題
  - マクロリスクの観点から計画案に含める個別監査プロジェクト候補一覧
    ＊「重要課題」と同じ名前(タイトル)の監査プロジェクトを実施する

- 評価項目別結果
  - 評価項目01：全般的な経済情勢
    1. マクロ経済(世界及び日本)
    2. 業界動向(不動産、消費者金融、リースなど)
  - 評価項目02：決済インフラストラクチャーの更新及びその他情報技術革新
    1. 決済インフラストラクチャー(銀行・証券、カードなど)
    2. その他の情報技術革新(オープンAPI、AI・RPAなど)
  - 以下省略

マクロリスク評価書(2)： 評価項目別の内容

- 評価項目別の評価は、基本的に以下の内容で構成される。
  - 分析結果
  - 結論
  - 分析手法
  - 資料(出典)

- 分析の結果として、必ず、どういう監査を行うのか、あるいは監査をしないのかについて結論付ける。具体的には、結論は以下のいずれかになる。

1. グループ横断的・部署横断的な管理体制の検証を行う。
2. 特定の部署・業務・システム等の検証を行う。
3. 監査プログラム項目に追記し、あるいは検証サンプルに取り上げ、関連する部署等の監査でカバーする。
4. 既に近時監査実施済み。
5. 継続モニタリングを通じて今後の動向を注視する。
6. マクロリスクの観点からハイライトして実施すべき監査プロジェクト候補なし。

ボトムアップ： マイクロリスク評価の基礎

- まず、監査対象領域（オーディットユニバース）を特定する。

  組織図、子会社・関係会社リスト、業務委託先リスト、システムリスト等により監査対象・範囲を網羅的に把握する。

- 次に、監査対象単位（オーディットユニット）を決める。

  単一部署、複数部署（含む業務委託先）合同、特定ビジネス・業務（ex.部署を分割）、全行的管理体制、単一システム、複数アプリケーション合同など、業務の関連性・リスクの特性などに応じてリスク評価・監査実施の基本単位を決める。

（例）

✓ 複数支店をまとめて1つの監査単位に設定し、1度に複数店を監査し監査報告書も1つ。
✓ 市場取引のトレーディングデスクと市場取引関連の決済業務を行うバックオフィス部署とを合わせて1つの監査単位に設定し、まとめて1度に監査し、監査報告書も1つ。
✓ 個人向け預金口座に関連する複数のシステム・アプリケーションをまとめて1つの監査単位に設定。

マイクロリスク評価項目(1): デフォルト・リスク・スコア

ビジネス監査　定性評価
1.ガバナンス・組織体制上のリスク
2.市場リスク
3.信用リスク
4.流動性リスク
5.コンプライアンスリスク(顧客保護)
6.コンプライアンスリスク(AML/CFT)
7.コンプライアンスリスク(その他)
8.オペレーショナルリスク
9.税務リスク
10.その他

IT監査 定性評価
1.ガバナンス・組織体制上のリスク
2.データの機密性に関する影響度
3.データの完全性に関する影響度
4.データの可用性に関する影響度
5.サポートする業務の重要性・複雑性

- オーディットユニット毎に、各リスク項目に相対的リスクスコアをつける(10-100)。
- 上位3つのリスク項目のみ加重平均して、オーディットユニット毎のデフォルトリスクスコアを出す。
(1位:2位:3位＝5:3:2)

突出したリスク・プロファイル “スパイク” を捕らえる。

マイクロリスク評価項目(2): 加重ファクター

定量評価
1.取引量・残高(リスクエクスポージャー)・顧客規模
2.収益・費用の金額
3.要員数

前回監査
前回監査実施からの経過期間
前回監査の評価結果

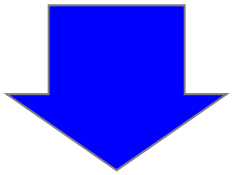
- 定量評価で、規模が相対的に大きいと評価したオーディットユニットのデフォルトリスクスコアに加重。(小さいと評価すればその逆)

- 前回監査実施時から一定期間(2年)経過前はデフォルトリスクスコアをディスカウント、一定期間経過後、加速度的にデフォルトリスクスコアに加重。
(基本加重係数1.5^(経過月数/24-1))

監査対象候補の序列と割合

- トップダウンアプローチであるマクロリスク評価をまず行い、ボトムアップアプローチであるマイクロリスク評価で補完する。（マクロリスク優先）

- すなわち、マクロリスク評価で監査プロジェクト候補を挙げ、それに対するリソースの割り当てをまず行い、次に残りのリソースをマイクロリスク評価上リスクが相対的に高いオーディットユニットに充てていく。

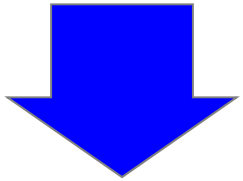


計画プロジェクト数の割合実績は、マクロリスク評価結果：マイクロリスク評価結果が、7：3から6：4程度。

（あくまで結果論で、この割合をターゲットにしている訳ではない。）

監査を実施する計画としない計画

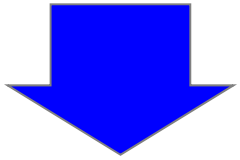
- Hは毎年、Mは2年に1回、Lは3年に1回といったように監査頻度を定型化しない。
- リスクが高いものから現状のリソース（要員数）で出来るところまでやる、という監査計画を作成すると、前回監査日から相当程度の期間が経過していてもリスクスコアが上がらないプロジェクトや、相応に高いリスクスコアのプロジェクトでも他にもっと高いリスクスコアのプロジェクトがある場合は、それらが年次監査計画から除外されることがありえる。



年次監査計画書には、監査を実施する計画とともに実施しない計画、すなわち前回監査日から相当程度の期間が経過しているプロジェクトや高いリスクスコアのプロジェクトで翌年の実施計画に含めないものがあれば、その理由の説明とともに記述し、合わせて、社長・監査役会の承認を得る。

継続モニタリングと年次監査計画の見直し

- 経営陣とのミーティング、重要会議等への陪席、監督当局からの発表、ニュース報道などを通じて、継続的に内外の環境変化をモニタリングしていくと、新しいリスクやリスクの変化が出てくる。



- 期中を通じて、今年度の監査計画の修正（監査プロジェクトの追加や既存の監査プロジェクトでのカバー範囲の拡大など）を実施するか、来年度以降の監査計画で対応するかを判断する。
- 必要に応じて随時、年度監査計画を修正する。

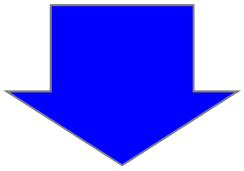
速やかに監査を実施すべきリスクの高い事象が認識されたが、追加の監査を実施するリソースがない場合は、相対的にリスクの低い監査プロジェクトを年度計画から落とす。
割り切って「選択と集中」を行う。

そのために、最初から「Lは3年に1回」といった定型的な監査頻度は定めない。

グループベースでのリスク評価・監査計画の統合

- 2018年度監査計画からリスク評価及び計画書をグループベースで統合。

- マクロリスク評価で銀行グループ全体をカバー。
- マイクロリスク評価でグループ全体の業務・システムを監査単位に分類し、相対的リスク評価を実施。



グループ監査部でグループ全体及び子会社用の年次監査計画書を作成。

マクロリスク評価結果として、グループベースでの重要課題と子会社レベルでの重要課題を特定。

マイクロリスク評価のため、子会社の監査単位を再編。（複数部署を一つの監査単位化）
グループ全体で横串を刺しながらリスクスコアを付与。

近年、マクロリスク評価結果から重要課題とした項目例

- マネー・ローンダリング及びテロ資金供与対策
- 海外送金事業
- 信用リスク管理及び資産査定管理体制
- グループ無担保カードローン事業（含む信用保証業務）
- オープンAPIに関する管理体制
- RPA（ Robotic Process Automation ）導入管理体制
- 次期コアバンキングシステムプロジェクト
- サイバー攻撃への対応
- 改正犯収法及び共通報告基準（CRS）対応

まとめ

1. リスクアプローチは直面する現実への対応として不可避。
   監査の実施において「選択と集中」を行う。
2. リスク評価をトップダウンとボトムアップの2つのアプローチ（マクロリスク評価とマイクロリスク評価）で行う。
3. マクロリスク評価では、外的要因と内的要因を評価した上で監査プロジェクト候補を挙げるとともに、年次監査計画上の「重要課題」を特定する。
4. マイクロリスク評価では、監査対象領域の網羅性を確認し、監査対象単位ごとに、突出したリスクプロファイル（“スパイク”）に着目したリスクスコアリングを行う。
   リスクスコアは、監査対象単位の規模、前回監査の状況に応じて加重する。
5. 監査プロジェクト候補は、マクロリスク評価優先で決める。マイクロリスク評価からの監査プロジェクト候補の選出はそのあと。
6. 年次監査計画書には、監査を実施する計画にしない計画も含めて承認を得る。
7. 継続モニタリングを踏まえ、必要に応じて年度監査計画を修正する。
8. これらをグループ全体で統合して実施する。