2017年1月

米国におけるシステムリスク管理の動向 ～2線強化の観点から～

金融機関のリスク管理領域においては、Three lines of Defenseという考え方が一般的である。Three lines of Defenseとは、金融機関のリスク管理を3つのレイヤー（層）で実施する考え方で、システムリスク管理の領域のみならず、コンプライアンスリスクや市場リスク等にも適用される。以下1線、2線、3線の主な役割・責任について整理する。

1線（Business Owner/System Owner）

各部門における戦略策定やオペレーションを遂行し、一定のリスクの範囲内で期待される収益を上げること、戦略に沿った効果的なITの導入などの役割を担う。

日本の金融機関のシステムリスク領域ではCIO（最高情報責任者）、システム担当役員が責任を負うケースが多い。

2線（Standard Settler）

リスク管理の枠組み策定や1線に対するモニタリングを実施し、組織として許容されるリスクの範囲でビジネスを遂行しているかについて1線を牽制・監督する役割を担う。

日本の金融機関のシステムリスク領域ではIT部門内にリスク管理担当を設置しCIOが実質的な責任を負うケースが多いが、一部の金融機関ではCRO（最高リスク責任者）が責任を負うケースも存在する。

3線（Assurance Provider）

1線および2線とは独立した評価を実施し、経営者が円滑にビジネスを遂行するにあたっての一定のアシュアランス（保証）を与える役割を担う。

監査担当役員が責任を負うケースがほとんどで、小規模な金融機関では社長が兼務しているケースも稀に見られる。

本稿では、米国の規制当局の動向を踏まえ、1線に対する2線の独立性の観点からシステムリスク管理の動向について、欧米大手金融機関の事例を交えて解説する。

1. 米国規制の動向

（1）OCCガイドライン

2008年の金融危機以降、金融機関に対するリスク管理に係る当局の要請は高まる傾向にあり、2014年に米国OCC（Office of the Comptroller of the Currency：米国通貨監督庁）が、外国銀行の支店を含む大手金融機関に関するリスク・ガバナンス・フレームワーク（Risk Governance Framework）の高度化ガイドラインの最終規則を公表した。

本ガイドラインはOCCガイドラインと呼ばれており、本稿で解説するシステムリスク管理強化の根拠規則と位置づけられ、英文で100ページ以上の内容であるが、そのなかに「Independent risk management」に関し以下の記載がある。

Independent risk management

Independent risk management should oversee the covered bank's risk-taking activities and assess risks and issues independent of the front line units by

i. identifying and communicating to the CEO and board of directors or board's risk committee material risks and significant instances where independent risk management's assessment of risk differs from that of a front line unit, and significant instances where a front line unit is not adhering to the risk governance framework;
ii. developing, attracting, and retaining talent and maintaining staffing levels required to carry out the unit's role and responsibilities effectively while establishing and adhering to talent management processes and compensation and performance management programs.

出典：米国通貨監督庁ガイドラインより抜粋（下線筆者※）
https://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-117a.pdf#search='OCC+independent+risk+management'
※下線は本稿において筆者が特に強調したい箇所に引いたもの

この「Independent risk management」が冒頭で説明したThree lines of Defenseの2線活動そのものと解釈できる。

重要なポイントは、まず第1に1線が実施するリスクアセスメントと異なる独立したアセスメント結果について、2線がCEOおよび取締役会（リスク管理委員会等）への報告を要求している点である。1線と2線で異なる報告ラインを保有することを要求しているため、1線の報告ラインの責任者と2線の報告ラインの責任者が同一人物だと対外説明が難しく、1線と2線で別々の責任配下での報告ラインを持つことを要求されていると解釈できる。

第2に、システムリスク管理に期待される役割・責任を果たすために、2線における有能な人材の育成・確保、報酬制度等の整備を要求している点である。米国においても日本と同様、システムリスクに精通した人材を2線に確保することは決して容易ではなく、具体的な事例については後述するが、各社さまざまな組織形態、1線2線の役割分担を模索している状況である。

（2）FFIEC Information Technology Examination Handbook

米国には業界、州や連邦等でさまざまな規制当局が存在し、そのメンバーにより米国連邦金融機関検査協議会（FFIEC：Federal Financial Institutions Examination Council）が構成されている。金融機関に対する検査目線をそろえるために、システムリスクの管理領域について金融機関が遵守すべき共通の基準としてシステム開発、システム運用、情報セキュリティ、外部委託、事業継続等の単位で作成されたガイドラインがFFIEC Information Technology Examination Handbook（以下、「FFIECハンドブック」という）である。

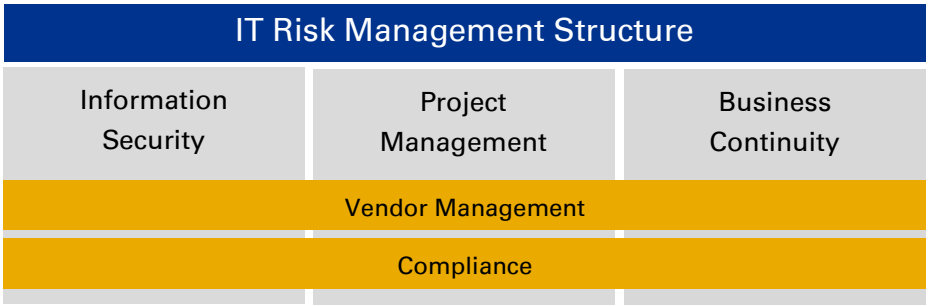
FFIECハンドブックはシステムリスクに特化した内容となっているが、そのなかに「Management」の領域があり、2014年に改定されている。OCCガイドラインに基づく2線強化の流れと関連していると考えられるため、その一部を紹介したい。

FFIECハンドブックでは、日本の金融庁が定義するシステムリスク管理をITRM（IT Risk Management）と呼んでおり、概念的に以下の領域に整理されている。

- Information Security
- Project Management
- Business Continuity
- Vendor Management
- Compliance

大きな分類としてはInformation Security（情報セキュリティ）、Project Management（プロジェクト管理）、Business Continuity（事業継続）の3領域で、それぞれの領域に対しVendor Management（外部委託先管理）とCompliance（コンプライアンス）が横断的にカバーする構造である。

【図表1】FFIECにおけるITリスクマネジメントの構造



FFIECハンドブックでは、Information Security、Project Management、Business Continuityの各領域の管理に関して、またCIO/CTO（最高情報責任者／最高技術責任者）、CISO（情報セキュリティ責任者）の役割・責任についての記載があり、それぞれ以下に抜粋して紹介する。

① Information Security

1.B.2 Information Security

The institution should separate information security program management and monitoring from the daily security duties of IT operations. The IT department should have personnel with daily responsibility for implementing the institution's security policy.

出典：FFIECハンドブックより抜粋（下線筆者※）
http://ithandbook.ffiec.gov/it-booklets/management.aspx
※下線は本稿において筆者が特に強調したい箇所に引いたもの

情報セキュリティ領域では、日常的にITオペレーションを担当する部署と、セキュリティマネジメントおよびモニタリングを担当する部署を分けることを要求しており、ITオペレーションを担当する1線と、リスク管理を行う2線の明確な分離を強く求めていることが読み取れる。

② Project Management

1.B.3 Project Management

Based on an institution's size and complexity, an institution pursuing a more-than-moderate growth path should consider establishing a project management office to promote sound management practices and principles.

出典：FFIECハンドブックより抜粋（下線筆者※）
http://ithandbook.ffiec.gov/it-booklets/management.aspx
※下線は本稿において筆者が特に強調したい箇所に引いたもの

プロジェクト管理領域では、2線の独立的モニタリングに係る具体的な記載はなく、情報セキュリティ領域のような独立的なリスク評価は要求されていない。一方で、健全なプロジェクト推進を行うため、組織の大きさ・複雑さに応じてPMO（Project Management Office）設置の検討を要求しており、PMOを開発プロジェクト推進の立場から一定の距離を置いたチーム・組織と位置づけ、プロジェクトを客観的にモニタリングすることを推奨していると解釈できる。

③ Business Continuity

1.B.4 Business Continuity

Business continuity planners should assess the ability for all lines of business to remain resilient or recover from disruptions or degradations.The business continuity function often resides in the risk management organizational structure. A specific member of management should be assigned responsibility for the oversight of the business continuity function, and both business and technology departments should assign personnel to develop and maintain the individual business unit plans.

出典：FFIECハンドブックより抜粋（下線筆者※）
http://ithandbook.ffiec.gov/it-booklets/management.aspx
※下線は本稿において筆者が特に強調したい箇所に引いたもの

事業継続管理領域では、経営者による事業継続の監督機能に係る記載があり、システム技術／ビジネス両面から横断的な関与を要求しており、IT部門および事業部門を横断した事業継続に責任を有する役員が監督を行う前提と推察される。

④　CIO/CTO（最高情報責任者／最高技術責任者）の役割・責任

The CIO or chief technology officer（CTO）is responsible and should be held accountable for the development and implementation of the IT strategy to support the institution's business strategy in line with its risk appetite.

出典：FFIECハンドブックより抜粋（下線筆者※）
http://ithandbook.ffiec.gov/it-booklets/management.aspx
※下線は本稿において筆者が特に強調したい箇所に引いたもの

CIO/CTOは、事業上のリスク選好に応じたシステム導入に関し責任があるものの、システムリスク管理に係る役割、責任は明記されていない。なお、日本の大手金融機関では、CIO/CTO配下にシステムリスク管理機能を設置しているケースが多数である。

⑤　CISO（情報セキュリティ責任者）の役割・責任

- The chief information security officer（CISO）is responsible for overseeing and reporting on the management and mitigation of information security risks across the institution and should be held accountable for the results of this oversight and reporting. The CISO should be an enterprise-wide risk manager rather than a production resource devoted to IT operations.

- To ensure independence, the CISO should report directly to the board, a board committee, or senior management and not IT operations management.

出典：FFIECハンドブックより抜粋（下線筆者※）
http://ithandbook.ffiec.gov/it-booklets/management.aspx
※下線は本稿において筆者が特に強調したい箇所に引いたもの

CISOは独立性を確保するため、ITオペレーション機能と独立すること、および直接、取締役会やリスク管理部門等に報告することが要求されている。ITオペレーション機能を管轄しているのは一般的にCIOであるため、CIOとCISOは別担当であることが暗黙的に求められていると解釈できる。

日本の金融機関では、情報セキュリティ全体をコンプライアンス部門、IT技術領域をIT部門が管轄していることが多く、さらにサイバーセキュリティ領域を別部署が所管しているケースや事業部門との責任分担があいまいなケース等、CISOを特定できないケースもある。

2. 欧米大手金融機関の事例

米国における規制強化の流れを受け、システムリスク管理の組織設計および1線2線の役割責任について、KPMGが欧米G-SIFIs4社を対象に2016年8月に調査を実施した[1]。

本調査における1線はCIOに報告する責任のある部署、2線はCROに報告する責任のある部署と定義している。

なお、調査結果の要約は図表2のとおりである。

【図表2】調査結果概要

	欧米金融機関のシステムリスク管理における1線2線の役割分担	1線のリスク管理機能の有無	2線のCROへの報告実施者
A社	1線にリスク管理機能がなく、2線に集中的なITリスク管理機能を設置。独立的な監督に加え、1線の実態を把握するために1線の活動の一部を2線が支援。管理モデルレビュー中。	×	2線スタッフ
B社	1線にリスクマネジャーを設置しているが、独立的監督機能を発揮するため、オペレーションリスクの枠組みのなかで2線にITリスク管理部署を新設。	○	2線スタッフ
C社	1線にリスク管理機能を有するOperations and Technology Risk and Control（OTRC）を設置。2線にTechnology Risk Management groupを設置し、CRO経由でCEOに報告。さらにOTRCや開発技術チーム等の1線メンバーを含むWorking groupを2線に設置し、より透明性のあるITリスク管理を支援。	○	1線および2線スタッフの混成
D社	1線にITリスク管理に責任を有するマネジメントコミッティを設置。2線に地域／部署の代表者で構成される独立評価チームを設置し、ORM（Operation Risk Management）長に報告、また、グローバルのITリスクコミッティも担当（Functional Reporting）。	○	1線スタッフ

1 Technology Risk Management – 1st and 2nd Lines of Defense at Large FS（KPMG）

3. まとめ

- CIOとCROへそれぞれレポートを上げる点は、欧米大手金融機関4社で共通しているものの、組織設計は4社各様であり、2線としてのあるべき姿を各社模索している状況である。
- 米国当局がCIOから独立した2線によるシステムリスク管理モデルを承認するか否かは、2線の組織形態ではなく、システムリスク管理に係る人材の配置および独立した報告ライン機能が実質かつ有効的に機能しているかが判断基準であると想定される。
- 本規制は現時点で日本の金融機関に適用されるものではないが、金融規制のグローバル化の大きな流れを受け将来的に日本においても適用される可能性はゼロではない。特にCIOの配下にシステムリスク管理部門が設置されている場合に、システムリスク管理部門による1線の活動に対する実効的な評価が行われているか、無難な落としどころを想定した予定調和型のシステムリスク管理になっていないかについて、日本の金融機関は今一度自社の管理態勢を見直す良い機会と考える。

KPMGコンサルティング株式会社
ディレクター　原田　克樹

KPMGコンサルティング株式会社

東京本社
〒100-0004
東京都千代田区大手町1丁目9番5号
大手町フィナンシャルシティ　ノースタワー
TEL ： 03-3548-5111
FAX： 03-3548-5114

大阪事務所
〒541-0048
大阪市中央区瓦町3丁目6番5号　銀泉備後町ビル
TEL ： 06-7731-2200

名古屋事務所
〒450-6426
名古屋市中村区名駅3丁目28番12号　大名古屋ビルヂング
TEL ： 052-571-5485

kpmg.com/jp/kc