金融分野におけるITレジリエンスに関する分析レポートの概要（2026年７月）

■ 金融庁では、2019年以降、金融機関において発生したシステム障害に関する分析レポートを継続的に公表してきたが、2025年６月には、「金融分野におけるITレジリエンスに関する分析レポート」として再構成して公表した。2025事務年度においても、近年の地政学リスク、サイバーリスク及びサードパーティリスク等の高まりに加え、金融機関の業務運営及び顧客サービスがIT・デジタル基盤に一層依存する状況を踏まえ、金融分野におけるITレジリエンスの強化に資する観点から、本レポートを取りまとめている。

■ 本レポートの構成：

（１）システム障害に関する分析（第２編）

（２）ITガバナンス高度化に係る実態把握（第３編）

（３）サイバーセキュリティ（第４編）

- モニタリング等で認められた課題と参考となる取組み
- AIによるサイバー脅威の変化への対応
- サードパーティ・サイバーセキュリティリスク管理強化に関する委託調査
- 顧客口座・アカウントの不正アクセス・不正取引への対策強化

（４）クラウド演習の進め方（第５編）

（補論１）システム障害事例集

（補論２）バーゼル銀行監督委員会による「健全なサードパーティリスク管理のための諸原則」

（コラム）耐量子計算機暗号への移行

■ 本レポートのメッセージ：

✓ 金融業界におけるITの複雑化、サードパーティへの依存の高まり、サイバー攻撃の高度化等を背景として、金融機関の経営ひいては金融システムの安定に影響を及ぼし得るリスクが一層高まっている

✓ 金融機関の経営陣は、ITリスク及びサイバーリスクを経営上のトップリスクとして認識し、自組織のガバナンス、管理態勢、投資、人材育成並びにサードパーティリスク管理について不断に見直し、その実効性を継続的に高めていく必要がある

✓ 対策を講じていたとしてもなお障害又はインシデントは発生し得るとの前提に立って、ITレジリエンスを強化する必要がある

✓ 当庁としては、金融機関の自助及び金融業界の共助を促進するとともに、検査・モニタリングに加え、意見交換、情報共有、ガイダンスの提供、演習等の機会の提供といった公助の取組みを推進していく

システム障害に関する分析（第２編）　概要

発生の端緒	障害傾向	課題・対応
(1)サイバー攻撃、不正アクセス等の意図的なもの	①　マルウェア感染（委託先含む） ②　ボイスフィッシング詐欺 ③　DDoS攻撃	• 委託業務の重要度見直し、統制の実効性確保（実地調査・第三者評価等によるチェック体制強化）、リモートアクセスを含む脆弱性管理の高度化、多要素認証や特権アカウント管理の強化 • 注意喚起や相談受付態勢整備、認証・取引時のモニタリング、リスクに応じた取引管理強化等 • DDoS対策ツール、アクセス制限、攻撃元ブロック等の防御対策の見直し、早期検知・復旧や業務継続に関する態勢整備、通信事業者との連携強化
(2)システム統合・更改や機能追加に伴い発生	①　障害発生時の影響見誤り、無影響確認テスト不足	• 障害発生時の影響を踏まえたプロジェクト体制構築、無影響確認テスト基準の明確化等による検証態勢強化
(3)日常の運用・保守等の過程の中で発生	①　サードパーティ（サービス）の障害による影響 ②　冗長構成が機能しない等の障害 ③　システム障害発生時の復旧不芳	• 障害箇所の早期特定と障害箇所の切り離し機能構築等の復旧対応整備 • 委託先管理の強化（委託先への監査・統制の厳格化）、セカンダリーデータセンターへの切替テストの実施等による冗長化設計の実効性確保 • 障害箇所の早期特定・影響範囲拡大抑止のための対応態勢整備、復旧手順の実効性確保
(4)プログラム更新、普段と異なる特殊作業等から発生	①　災害対策システム試験における影響範囲の評価誤り、障害対応態勢の整備不足	• 本番システムへの影響に関するリスク評価徹底、障害発生時における顧客対応を含む対応態勢整備、平時から研修・訓練を通じた実効性確保

ITガバナンス高度化に係る実態把握（第３編）概要

- 一部の地域銀行を対象にITガバナンスの実態把握を行い、金融機関のITガバナンスの高度化に資する論点や参考事例を整理している。
- 各金融機関が自らの規模や経営戦略等を踏まえて、創意工夫を進めていく際の参考として活用することを想定している。

IT戦略

- 経営戦略とIT戦略の連携は相応に進展し、生成AIやデータ利活用等のDX施策の推進が確認された。
- 一方で、IT戦略の策定に当たっては、各部門の要望を積み上げるだけではなく、目指すべきビジネスの姿やそれを支えるデータ・システム基盤等を整理した上で、中長期的な方向性と重点施策を明確化していくことが有用と考えられる。
- また、重点施策の実効性を確保する観点からは、進捗確認にとどまらず、追加投資や計画修正等の経営判断に資するKPIを設定し、継続的に活用することが有用と考えられる。

ITコスト

- ITコストについては、基幹系以外の周辺システムを中心とした保守・維持費用の割合が高く、その割合も増加傾向にある一方、戦略的な新規開発（前向き投資）の割合は相対的に低水準にとどまっている。
- ITコスト分析については、新規開発など使用目的別の割合やその推移に加え、ITコスト総額の増減、保守・維持費用等の継続的に発生する費用の割合、主要案件の内容及びIT投資額の状況を合わせて確認し、戦略領域への資源配分の実態を把握することが有用と考えられる。

IT人材

- IT人材については、採用等に一定の進展が見られる一方、高度専門人材の確保・育成等の課題は依然残っている。
- こうした状況を踏まえると、経営陣が積極的に関与する形で、自組織で保有すべき能力と外部連携により補完すべき能力を整理した「人材ポートフォリオ」の視点で捉えることが期待される。その上で、中長期的な人材像やスキルを明確化し、育成・評価・キャリアパスの整備を進めていく必要がある。
- その際、競争領域か否かや、顧客影響、専門性等を踏まえ、自組織と外部活用の領域を見極めることが重要である。

IT戦略・ITコスト・IT人材は相互に関連する経営課題。経営陣がリーダーシップを発揮し、方向性や優先順位、資源配分を明確にした上で取組みを主導することが重要と考えられる。

共同センターの利用実態

- 地域銀行では、共同センターの利用により、ITコストの削減やリソースの最適化が進む一方、障害影響の拡大や開発・運用スキルの低下、開発自由度の低下等のリスクも認識されている。
- 共同センターの利用に当たっては、こうしたリスクの性質を踏まえ、自行が利用するシステム・サービスの内容やリスク特性について必要な理解を維持し、障害時や更改時等に適切に確認・判断できる態勢を確保していくことが重要である。

共同センター運営におけるガバナンス

- リーダー行の設置や会議体を通じて、加盟行の意見を集約し意思決定を行う枠組みが一定程度機能している一方、一部では、要件調整等に課題認識を持ち、ベンダー主導で意思決定が行われている状況も見られる。
- 運営に当たっては、投資の方向性、サービス水準、コスト構造、リスク対応方針等について、加盟行が主体的に関与し、判断できる状態を維持することが重要である。このため、ベンダーが主導する領域と、銀行が責任を持って判断すべき領域を整理し、加盟行側の関与と説明責任を確保することが、ガバナンス確保の観点から有用と考えられる。

共同化範囲の拡大

- 地域銀行では、人件費やシステムコストの上昇等を背景に、共同化を進めることで負担軽減につながる可能性がある。
- こうした中で、共同化範囲の拡大は単なるコスト削減策にとどまらず、非戦略領域の標準化・効率化を通じて、限られたIT投資やIT人材を戦略領域へ再配分するためのITガバナンス上の取組みとして位置付けることが重要である。
- 一方で、共同利用先等への依存関係が複層化し、障害時の影響波及や集中リスクが高まる可能性もあることから、効率性とレジリエンスの両面を踏まえた検討が求められる。

●これらの事例等は、地域銀行全体の傾向や優劣を示すものではなく、監督上の一律の基準やチェックリストを示すことを意図するものでもない点に留意が必要である。

サイバーセキュリティ（第４編）　概要

フロンティアAI等の発展やサードパーティへの攻撃等、サイバーセキュリティの脅威は高まっている

１．フロンティアAI等の発展

- **脆弱性が短期間に大量に発見**される可能性
- **脆弱性の発見から攻撃開始までの時間が大幅に短縮**し、従来のパッチマネジメント手法が通用しない恐れ
- **高度なサイバー攻撃が増加**する懸念

⇒ 金融庁・日本銀行から金融業界に対し、短期的な対応に関する**要請文を発出**

２．ランサムウェアの猛威

- **ランサムウェア被害は依然として高水準で推移。**金融業界以外において、ビジネスや顧客に甚大な影響を及ぼすような事例も複数発生

⇒「金融分野におけるサイバーセキュリティに関するガイドライン」に基づく検査・モニタリング等により、**金融業界全体のサイバーセキュリティ態勢の底上げ**

３．サードパーティへの攻撃

- **サードパーティに由来するサイバーインシデントで金融機関の業務や顧客が影響を受ける事例が発生**

⇒諸外国の金融機関におけるサードパーティ・サイバーセキュリティリスク管理に関する委託調査を実施

⇒上記委託調査やモニタリング等を通して、**実効性のあるサードパーティリスクの管理強化を推進**

４．不正アクセス・取引等の被害

- フィッシングサイト等で窃取した顧客情報（ログインID・パスワード等）による証券口座不正アクセス・取引被害が発生
- 2025年の不正送金被害額は約104億円（前年比約1.2倍）。そのうち約９割がフィッシング

⇒ **フィッシング耐性のある強固な多要素認証（パスキー等）による認証強化等を推進**（要請文及び監督指針等の改正並びに広報活動）

経営主導での迅速な態勢強化が求められる

- サイバー攻撃の脅威の変化を的確に捉え、経営トップのリーダーシップにより、必要なリソース配分を含めた意思決定を行う必要
- 従来の対策の延長にとどまらず、サイバーハイジーン、多層防御及びレジリエンスのより一層の強化を図る必要

サイバーセキュリティ（第４編）　概要

モニタリング等で認められた課題と参考となる取組み　1/2

ガイドライン項番	主なポイント	課題・参考取組み
サイバーセキュリティ管理態勢の構築（2.1.）	● **経営陣の主体的な関与**の下、リソースを適切に配分することが重要。インシデントが起きてから態勢を見直すという受け身の対応ではなく、**平時から能動的に態勢を見直す必要**。 ● サイバーセキュリティに関する知見を有する人材が、ガバナンス、リスク管理、コンプライアンスを担う各機能において不足。 技術が急速に進展する中でも、**持続可能な人事政策や教育・研修制度が必要**。	**＜課題＞** 経営陣の主体的関与や、残存リスクの把握が不足 **＜参考事例＞** 親会社主導のグループ統制や、他社比較による自組織リスクの把握
サイバーセキュリティリスクの特定（2.2.）	● 脆弱性管理については、その前提として、**情報資産（HW/SWを含めたIT資産）及びネットワーク構成・データフロー（どのようなデータがどの経路を通過するか）の可視化を行い、最新の状態に維持することが重要**。 ● 脆弱性診断、ペネトレーションテスト、TLPTなどを活用し**優先順位をつけて脆弱性を診断する手法、範囲、時期を定め計画的に実施することが必要**。 AIの発展を踏まえると、特定されたリスクに対する迅速な対応が求められる。	**＜課題＞** リスク評価への反映の遅れや、ＩＴ資産管理台帳の網羅性・記載項目の不足 **＜参考事例＞** 技術的リスクの経営情報への変換や、リスク評価の高度化
サイバー攻撃の防御（2.3.）	● AIの発展を踏まえると、ゼロデイ攻撃や、脆弱性の公表後時間を置かず攻撃が開始される可能性があり、**ソース自体が公開されているOSSの利用に関するサプライチェーンリスクの再評価が必要**であるとともに、**従来のパッチマネジメント手法では不十分となるおそれ**がある。 ● **多要素認証などの認証強化や最小権限・職務分離の原則に基づくアクセス管理の強化などを更に加速させる必要**。また、ゼロトラストの考え方に基づく対策として**マイクロセグメンテーション等を検討し、多層防御を講じることが重要**。	**＜課題＞** バックアップ対策の検討不足、境界型防御への過信、情報資産の更新計画の整備不足 **＜参考事例＞** 厳格なアクセス制御やマイクロセグメンテーション、防御対策の可視化

サイバーセキュリティ（第４編）　概要

モニタリング等で認められた課題と参考となる取組み　2/2

ガイドライン項番	主なポイント	課題・参考取組み
サイバー攻撃の検知(2.4.)	● EDR 、IPS 、SOAR等、様々なセキュリティ機器を利用し**不正アクセスの試行を的確に検知して即時に対応できる態勢の整備が重要**。 ● 検知態勢の巧拙は、金融機関における**サイバーセキュリティ確保の水準を大きく左右。**	**＜課題＞** アラート検知時に必要な対応及び報告の不備 **＜参考事例＞** EDRの計画的導入や、複数ログの関連分析
サイバーインシデント対応及び復旧 (2.5.)	● **経営陣は**、迅速かつ的確に現状を把握し、**様々なリスクを勘案の上、システムの停止・再開等の経営判断を実施することが肝要**。 ● **有事の場合にBCPが機能するようにIT部門だけでなく経営陣や関係部門等を含め、練度を高めておくことが重要**。	**＜課題＞** コンティンジェンシープラン等の対象範囲の不十分さ及び更新漏れ **＜参考事例＞** 潜伏期間を考慮したバックアップや、脅威シナリオによる研修・訓練の実施
サードパーティリスク管理 (2.6.)	● 金融機関は**リスクベースで**第三者保証による報告書や外部評価の枠組み、契約書等を活用し、**サードパーティへのモニタリングの実効性を高める**とともに、必要に応じてヒアリングを実施し、ASMツール等を活用して外部に晒されている脆弱性を把握するなど、**複数の手段を組み合わせたり、確認の頻度を変更する等の工夫が必要**。 ● サードパーティを含むコンティンジェンシープラン等の整備状況をあらかじめ検証し実効性を高めておくなど、**サードパーティにおけるインシデント発生を前提とした態勢整備をしておくことが重要**。	**＜課題＞** チェックリストの形骸化や、委託先任せのリスク管理 **＜参考事例＞** サプライチェーン全体のリスクの可視化や、代替ソリューションの特定

サイバーセキュリティ（第４編）　概要

AIによるサイバー脅威の変化への対応

- AI技術が急速に進展する中、サイバー攻撃の速度・規模が劇的に加速・拡大するなど、サイバーセキュリティを巡る脅威が急速に高まっている。
- 金融庁では、「AI脅威に対する金融分野のサイバーセキュリティ対策強化に関する官民連携会議」等を通じて金融業界とIT業界、政府・日本銀行等の連携強化を図るとともに、金融機関等における短期的な対応の強化に向け、要請文を発出し、更なる対応を促している。
- AI脅威に対しても、「金融分野におけるサイバーセキュリティに関するガイドライン」に基づく対策を着実に実行していくことが引き続き重要。

○要請文の概要

① フロンティアAIへの対応を経営課題として扱う

- 経営トップは、フロンティアAIへの対応を**IT部門にとどまらない全社的な経営課題**として扱い、**関係部門が横断的に連携**して対応できるようにする。
- **経営トップのリーダーシップの下、CIO、CISOをはじめとする経営層が直接関与**する。

② 優先的に対応すべきサービス／ITシステムを特定する

- **優先的に対応すべきサービス／ITシステムを特定**し、リソースを重点的に配分する等、リスクベースで対応する。(例：インターネットバンキング)
- 当該システムが共同運営形態で提供される場合、**利用側・提供側双方での十分な認識共有、責任分担の明確化が必要**である。

③ 特定した資産の技術負債を解消しておく

- 脆弱性発見時に**パッチ適用対象を即時に特定できる状態**を確保する。
- 特権ID削除や未対応パッチの適用等により**技術負債を極力解消**することで、迅速なパッチ適用が可能な状態を確保する。特にサポートが終了している製品は、**サポート対象のバージョンへ更新**する。

④ パッチ適用に係る人的リソースを追加する

- 金融機関等やベンダーにおいてパッチ適用に係る**人的リソース追加を検討**する。
- 脆弱性の優先度判断に係る評価体制についても、上記同様に人的リソースを確保する。

⑤ ベンダーとの維持保守契約の内容を確認する

- ①**パッチ適用作業が現行の維持保守契約に含まれていること**及び**役割分担が明確であること**、②緊急にパッチ適用作業が必要な場合に、**夜間・休日等も含めて適時に対応可能な契約内容となっていること**を確認する。
- ベンダー側で必要なリソース確保状況を確認しつつ、リソースがひっ迫すること等も想定し、パッチ適用の遅延に係るリスク受容等のプロセスを整備する。

⑥ パッチ適用プロセスをリスクベースにする

- 発見された脆弱性が自組織のサービス／ITシステムに及ぼし得る**影響と攻撃が成立する蓋然性も踏まえた評価**に基づき、**よりリスクの高い脆弱性から対応**する。
- パッチ適用作業に係る事前のテストについて、想定されるリスクを総合的に勘案し、テスト実施内容の合理的な縮小等の対応も検討する。

⑦ パッチ適用以外の対策も強化する

- パッチ適用そのものが困難である場合等は、仮想パッチの適用やボット対策の導入等により、**多層防御の強化**を図る。
- ネットワーク分離の実施、特権IDへの多要素認証の導入等による**防御能力の強化や内部侵入後の横展開への対策**等を講じる。
- **パッチが適用できないことによる残存リスクを評価した上で**、パッチ適用に要する期間を踏まえた**適切なリスク受容手続**を講じる。

⑧ 優先サービス／ITシステムの停止に備える

- **サイバー攻撃によりITシステムが停止する場合を想定**する。**システムを能動的に停止させざるを得ない場合もあらかじめ選択肢として検討**する。
- **BCPの有効性や顧客等への対応手順、緊急時の連絡体制等を点検**する。
- **能動的なサービス／ITシステム停止の判断基準及び手順を明確**にしておく。
- サードパーティが提供するソフトウェアやサービスの停止に備える。

⑨ 外部との連携を維持・強化する

- 金融ISACや各業界団体・コミュニティ、当局等からの情報に積極的にアクセスし、必要な情報収集をする。
- 自組織での取組を金融ISAC等の共助コミュニティで積極的に共有し、金融分野全体の強靭性の向上に努める。

サイバーセキュリティ（第４編）　概要
サードパーティ・サイバーセキュリティリスク管理強化に関する委託調査

- 金融機関において、サードパーティが多様化・複層化するとともに、システムを構成する機器・ソフトウェアの構成や調達関係が複雑化している。また、金融機関のサードパーティへのサイバー攻撃により、金融機関の顧客情報が漏洩又は漏洩の恐れのある事案が発生している。
- こうした状況を踏まえ、サードパーティのサイバーセキュリティリスク管理（以下、TPCRM）について、以下の調査を行い、得られた知見を当庁のHPにて公表・還元することで、本邦金融機関におけるTPCRMの強化を図る。
  - ✓ 金融分野のTPCRM向上に資する国際的なガイダンスや諸外国（米国、EU、英国等）の制度・基準・ガイダンス等を対象とした文献調査
  - ✓ 米国・EU・英国の銀行、保険会社へのヒアリング

○調査結果概要

①サードパーティの分類と管理方針

サードパーティを**「外部委託先」だけに限定せず**、金融機関と取引のあるすべての組織を管理対象としている。その上で、サービスの重要度や固有リスクに基づき分類を行い、全体のうち**1～10%程度**に該当する「重要なサードパーティ」へ管理を集中させている。

② 集中リスク

集中リスクは、**オペレーショナル・レジリエンス確保の観点**から重視されている。単一サードパーティ、重要なNthパーティ、特定地域への依存といった形で可視化し、集中度が高い場合には**代替可能性**まで含めて評価している。

③ 選定時（デューデリジェンス）

金融機関・サードパーティの双方に負担が発生することから、**業界共通の質問票**などを重要度に応じてリスクベースで活用している。また、契約書等に**最低限実施すべきサイバーセキュリティの条項**を設けることで、これを充足できない場合は契約を見送る対応が取られている。

④ 期中モニタリングと監査権

サードパーティ管理は**契約締結後も継続的に行われ**、脅威インテリジェンス等を活用してリスク変化を把握している。問題が是正されない場合には契約解除も検討している。また、契約時に**監査権を明記**し、重要なサードパーティには必要に応じて**現地調査を実施**している。

⑤ 出口戦略・出口計画

重要なサードパーティについては、サービス停止時を想定した出口戦略・出口計画を事前に整備している。**対応方針を定め、切替手順を具体化**することで、実効性を確保している。また、定期的な見直しや**机上テスト**などを行い形骸化を防いでいる。

⑥ インシデント対応

サードパーティでのインシデント発生を前提に、**報告フローや遮断・再接続手順を明確化**している。対応時には、契約部署とサイバー部門を含めた関係部署が連携する体制が確立されている。また、重要なサードパーティとは、平時から**共同演習を行い**対応力を高めている。

サイバーセキュリティ（第４編）　概要
顧客口座・アカウントの不正アクセス・不正取引への対策強化関連

- 証券会社の実在するウェブサイトを装った偽のウェブサイト（フィッシングサイト）等で窃取した顧客情報（IDやパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引の被害が2025年春頃から急増。

- こうした不正アクセス・不正取引による被害は、**証券業界に限らず**、**金融業界の信頼を揺るがしかねないもの**であり、真のお客様保護のため、早急に**認証強化などのセキュリティ対策**を進めることが必要。

- このため、金融庁は今般の事案を受け、フィッシングに耐性のある多要素認証の導入等の要請文の発出をするとともに、**監督指針の改正を実施**。

  ✓ 全所管金融機関に対して要請文を発出(2025年7月)

  ✓ 「金融商品取引業者等向けの総合的な監督指針」を改正(2025年10月15日)

  （参考）https://www.fsa.go.jp/news/r7/shouken/20251015/20251015.html

  ✓ 「預金取扱等金融機関」および「暗号資産関連業者」に関する監督指針・事務ガイドラインを改正(2026年2月27日)

  （参考）https://www.fsa.go.jp/news/r7/sonota/20260227/20260227.html

  ✓ 「保険会社」および「資金移動業者」等に関する監督指針・事務ガイドラインを改正（2026年７月17日）

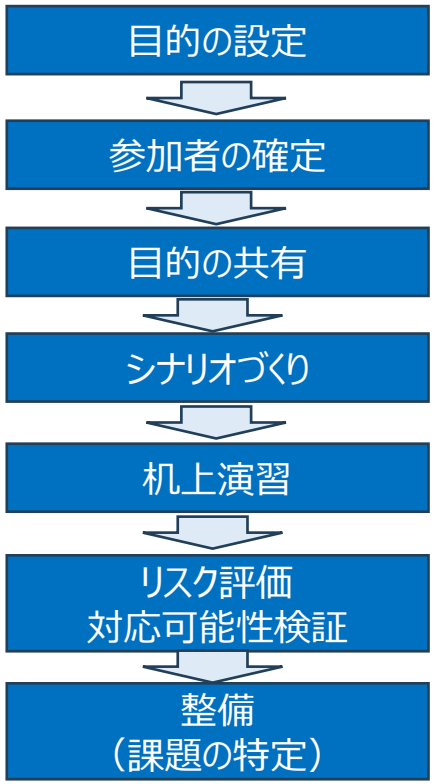
  （参考）https://www.fsa.go.jp/news/r8/sonota/20260717-2/20260717.html

- 当庁としては、改正後の監督指針等に基づき、**国民が安心して金融取引を行うことができる環境を確保する観点から**、モニタリングを行っていく。

クラウド演習の進め方（第５編）　概要

- 当庁は、金融機関、パブリッククラウドサービス事業者とともに、障害情報の取扱いに関する机上演習を実施。得られた知見を、「クラウド演習の進め方」として還元する。
- 重要なシステムでパブリッククラウドサービスの利用を検討している金融機関は、これを参考に、関係者と机上演習に取り組むことを通じて、パブリッククラウドサービス利用時のリスクをあらかじめ確認するとともに、その結果を、レジリエンス確保のために活用することが望ましい。

取組みプロセスの全体像（第１章）



演習シナリオ（第４章）

想定以上に深刻なものだが、起こり得るシナリオ

「初動」 リージョンの全てのサービスが突然停止（オフライン）する。ソーシャル・ネットワーキング・サービス（SNS）等を通じて障害情報が拡散する。
「業務継続確保」 SNS等を通じて、障害情報が更に拡散する。クラウドサービス事業者が障害原因の特定に至らない中で、金融機関は業務継続確保に向けた意思決定を行う。
「復旧」 クラウドサービス事業者は障害原因を特定し復旧を進め、サービスが徐々に再開する。金融機関は、停止していたクラウドサービスへの再接続（オンライン化）の意思決定を行う。
「真因分析・再発防止」 金融機関は、クラウドサービス事業者とともに、障害の真因分析と再発防止策を検討、その結果を監督当局に報告する。

着眼点（第６章）

パブリッククラウドサービスの特性を踏まえたものとして例示

・パブリッククラウドサービス事業者が公表する障害情報を、速やかに収集分析しているか
・影響を受けうるシステムを速やかに特定しているか
・パブリッククラウドサービスを利用する他事業者の特定および他事業者から受ける影響の分析に努めているか
・顧客からの問い合わせ・苦情に加え、SNS等を通じたパブリッククラウドサービス事業者や金融機関の風評拡大状況といった情報収集分析に努めているか
・パブリッククラウドサービス事業者からの情報提供を契約で担保しているか　等

目的の設定（第２章）セッション（第３章）本番セッションの進行（第５章）留意点（第７章）

バーゼル委による「健全なサードパーティリスク管理のための諸原則」（補論２）概要

- 2025年12月、バーゼル銀行監督委員会は、「健全なサードパーティリスク管理のための諸原則」（以下、「諸原則」。）を最終化・公表。
- 諸原則を踏まえ、一部の国際統一基準金融機関と、サードパーティリスク管理に関する意見交換を実施。
- 金融庁では、従前より、モニタリング等を通じて金融機関のサードパーティリスク管理のあり方に係る実態把握を実施。今後もモニタリングや対話を通じて把握した先進的な取組事例や共通課題について、業界と共有するほか、サードパーティとなり得る事業者との相互理解を深め、実務の実態を踏まえた建設的な関与を進める。

１．諸原則の概要

対象	原則	項目	概要
銀行	1	取締役会等の責任	取締役会は、銀行のサードパーティリスクの監督に対して最終的な責任を負い、明確な戦略を承認し、銀行のリスクアペタイトとサービス中断（disruption）に対する許容度を定義すべき。
	2	リスク管理枠組みの実施	取締役会は、上級管理職が、銀行のサードパーティ戦略に沿ったサードパーティリスク管理枠組みに基づく方針及びプロセスを実施することを確実にすべき。これらの方針及びプロセスには、TPSPの実績・TPSPとの取決めに関連するリスク・低減措置について、取締役会へ報告することが含まれる。
	3	リスク評価	銀行は、TPSPとの取決めを締結する前及びライフサイクル全体を通じて、特定されたリスク及び潜在的なリスクを評価し管理するために、サードパーティリスク管理の枠組みの下で包括的なリスク評価を行うべき。
	4	デューデリジェンス	銀行は、TPSPとの取決めを締結する前に適切なデューデリジェンスを行うべき。
	5	契約締結	TPSPとの取決めは、すべての当事者の権利・義務、責任及び期待を明確に記述した法的拘束力のある書面による契約によって管理されるべき。
	6	オンボーディング	銀行は、デュー・デリジェンスや契約条項の解釈の過程で特定されたあらゆる問題解決への対応を含め、新たなTPSPのオンボーディングを円滑に進めるための十分な資源を投入すべき。
	7	継続的なモニタリング	銀行は、TPSPとの取決めのパフォーマンス、リスク及び重要性の変化を継続的に評価・モニタリングし、その結果を取締役会や上級管理職に報告し、必要に応じて問題に対応すべき。
	8	業務継続管理	銀行は、サードパーティのサービスが中断した場合に業務を継続する能力を確保するために、堅固な業務継続管理を維持すべき。
	9	契約終了	銀行は、サードパーティとの取決めの計画的な終了のための出口計画及び計画外の（予期せぬ）終了のための出口戦略を維持すべき。
監督当局	10	監督当局の役割	監督当局は、銀行に対する継続的な評価の不可欠な要素として、サードパーティリスク管理を評価すべき。
	11		監督当局は、銀行セクターにサービスを提供する一つ又は複数のTPSPの集中によってもたらされるものを含め、潜在的なシステミック・リスクを特定するため、入手可能な情報を分析すべき。
	12		監督当局は、銀行にサービスを提供する重要なTPSPによってもたらされるシステミック・リスクを監視するため、分野横断的かつ国境を越えた連携および対話を促進すべき。

２．金融機関における現状（意見交換の結果）

- 一部の国際統一基準金融機関では、既存の法令・監督指針や諸原則等を踏まえ、従来の外部委託先管理の枠組みをサードパーティリスク管理の枠組みに置換する取組みが進行。
- 管理対象を、外部委託先だけではなく、購買・調達先やデータ・サービス連携先等へと拡大するとともに、これらのサードーパーティサービス提供者（TPSP）の類型や金融機関グループを横断する形で、ライフサイクルを通じたリスクベースの対応を進めることを志向。
- 他方、諸原則の内容にも照らすと、以下の点については、引き続き既存の枠組み、実務を高度化する余地が見受けられる。
  - 取締役会や経営会議等による基本方針策定への関与、モニタリング、ロードマップの明確化
  - グループ横断的、TPSPの類型横断的な台帳・システム、統一的なリスク管理戦略・方針の策定
  - サードパーティリスク管理にあたる人材・リソースの強化、自動化・標準化・システム化を通じた台帳整備、リスク評価実務の効率化や、評価方法の統一性・明確性確保
  - 契約、業務継続計画及び出口戦略に関する契約条項の見直しや調整

３．今後の対応

- サードパーティリスク管理について、各金融機関においてまずは経営層が関与するもとで明確な全社的ロードマップを策定し、リスクベースで優先度の高い課題から着実に管理の高度化を進めていくことが肝要。
- 金融庁では、サードパーティリスク管理に関する監督の考え方の整理や明確化に向け、必要に応じて検討を進める方針。
- 個別金融機関では対応に難しさを伴う論点も多いことから、金融機関横断での協調的な対応が重要な役割を果たし得る。金融ISAC等、共助の取組みを通じた各金融機関のリスク管理の底上げに期待。金融庁としても、業界における共助の取組みを後押しする。
- モニタリングや対話で聴取した先進的な取組事例や共通課題について、今後も様々な機会を通じて業界と共有を行う。