金融セクターにおけるサードパーティのサイバーリスクマネジメント
に関するG7の基礎的要素（仮訳）

背景及び対象

金融セクターにおける民間及び公的金融機関（以下「金融機関」という。）は、業務運営を支えるためにサードパーティとの取引関係を拡大し続けている。近年、このようなサードパーティの利用急増には、情報通信技術(ICT)プロバイダの利用拡大が含まれる。ICT プロバイダは、金融機関に対して、オペレーショナル・レジリエンスの強化、レガシーIT システムへの依存度の低減並びに金融サービスの提供におけるイノベーション、多様化及び効率性に関するポテンシャルの向上といった便益を提供し得る。さらに、外部の ICT サービスを利用することで、金融機関は中核的な事業の運営に集中し、IT への支出を効率的に管理できる。

ICT プロバイダを含むサードパーティの利用は、金融機関が考慮、管理すべき追加的なサイバーリスクをもたらす可能性もある。近年、サイバーインシデントは、ICT サプライチェーンの特に重要な部分が個々の金融機関のみならず金融セクターに対するシステミックなサイバーリスクを含み得ることを示している。サードパーティの脆弱性に起因するサイバーインシデントによって、例えば、不正行為、金融機関の業務の中断、顧客若しくは企業の機微（センシティブ）情報への不適切なアクセスにつながり得る可能性、又は金融市場の安全性及び健全性に影響を及ぼす可能性がある。これらの関係の規模と複雑性が増すほど、サードパーティのサービスを利用する金融機関にとって、サイバーリスクの理解、測定及び軽減はますます困難になる。

本基礎的要素におけるサードパーティとの関係の定義は、その組織がグループ内企業であるか外部提供者であるかにかかわらず、金融機関と組織との間に結ばれる製品又はサービスを提供するための、あらゆる業務上の関係又は契約である。サードパーティとの関係の重要な形態の一つに業務委託がある。業務委託関係のもとでは、業務委託がなければ金融機関自身により提供されていたビジネス上の機能、サービス又はプロセスをサードパーティが提供する。

本基礎的要素における ICT サプライチェーンの定義は、金融機関が自身の業務を支えるために用いる ICT エコシステムを形成する、サードバーティ間の相互の

結び付きから成る。ICT サプライチェーンには、すべての製品、サービス及びインフラに加え、それらの提供者、供給者及び製造業者も含まれる。金融機関は、特に重要な業務を支援する ICT サプライチェーンについて、検知、回復、継続的なテスト及びインシデント対応のための適切なアプローチを維持することを検討し得る。

基礎的要素

サイバーリスクへの対応の一助として、「金融セクターのサイバーセキュリティに関する G7 の基礎的要素」（2016 年 10 月）及び「金融セクターのサイバーセキュリティの効果的な評価に関する G7 の基礎的要素」（2017 年 10 月）が公表された。金融セクターにおけるサードパーティのサイバーリスクマネジメントへの取組みをさらに支援するため、G7 は 2018 年に、「金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する G7 の基礎的要素」を公表した。

2018 年以降の業界の進展に対応するため、G7 は 2018 年の基礎的要素を改訂し、サードパーティとの関係の管理のみならず、ICT サプライチェーン管理にも焦点を当てている。アップデートされた基礎的要素は、脅威が絶えず変化する環境に対応するために、広範な情報共有と透明性の大切さを強調している。金融セクターにおけるサードパーティの役割がますます重要になっていることについて注意を喚起するために、新たな基礎的要素(要素 7)が追加された。

金融機関は基礎的要素を必要に応じて、自身に固有のリスクプロファイル、業務や脅威に関する環境、金融セクターにおける役割、法的及び規制上の枠組みに適応させることが好ましい。基礎的要素は拘束力を持たず、既存のフレームワークを無効化するものでも、これらのフレームワークの継続的な適応を妨げるものでもない。以下の基礎的要素は、個々の金融機関におけるサードパーティのリスクマネジメントに関するライフサイクル、金融セクターに対するサードパーティの役割及びシステム全体のサイバーリスクのモニタリングについて論じている。さらに本基礎的要素では、個々の金融機関の ICT サプライチェーン全体におけるサードパーティのサイバーリスクマネジメントについても論じている。

金融機関及びサードパーティは、自身のサイバーリスクマネジメントのツールキットの一部として、本基礎的要素を活用し得る。その際、金融機関は、サード

パーティとの関係の規模、特性、対象、複雑性及び潜在的な金融システムにとっての重要性を考慮した相応のアプローチをとるべきである。

一法域の当局及び法域横断的な当局は、サードパーティサイバーリスクに対応するための自らの政策や規制・監督上の取組みを形成するため、本基礎的要素を活用し得る。

サードパーティのリスクマネジメントのライフサイクル

要素１：ガバナンス

金融機関のガバナンス組織は、サードパーティのサイバーリスクマネジメントの効果的な監視及び実行に関する責任を有すること。

取締役会や役員会など、金融機関のガバナンスに関する組織は、サードパーティとの関係の管理を含む、金融機関のサイバーリスクマネジメントの監視及び実行に関する最終的な責任を有する。この監視及び実行には以下が含まれる：サードパーティ依存への対処に関する文書化された戦略、サードパーティ及びサイバーリスクに関する方針、サードパーティとの関係に対するリスク許容度の設定、並びに企業のリスク管理機能に統合され、かつ、所与の活動のリスクと重要性のレベルに応じて管理された、サードパーティのサイバーリスクマネジメントに関する役割、責任及び説明責任の明確化。このほか、金融機関内部のあらゆるレベル並びに金融機関、サードパーティ及び関連当局との間における、通常業務としての適切なコミュニケーション及びエスカレーションのプロセスも含まれる。

要素２：サードパーティのサイバーリスクに対するリスクマネジメントプロセス

金融機関は、サードパーティのリスクマネジメントのライフサイクル全体を通じ、サードパーティのサイバーリスクを管理する有効なプロセスを有すること。

金融機関は、サードパーティに関連するサイバーリスクを特定、評価、監視し、適切なレベルの管理者に報告し、リスクベースアプローチを用いてサードパーティのサイバーリスクを管理すべきである。金融機関は、伝播するサードパーティのサイバーリスクから身を守るために、ポリシーや統制手段を導入すべきである。金融機関は、再委託の利用に関するリスクマネジメントのプラクティスを含め、

特に重要なサードパーティのサイバーリスクマネジメントのプラクティスを把握すべきである。

サードパーティと重要性の特定

金融機関は、サードパーティの一覧及び当該サードパーティが金融機関の業務にとってどの程度重要かの理解を維持すること。

一覧には、全てのサードパーティのリスト、提供するサービス及び機能、金融機関のシステムに対し有するアクセスレベル、保持又は処理するデータの種類や機密性及び場所を含むべきである。

金融機関は、サードパーティの業務上の重要性を識別できるようにすべきである。重要性を決定する要素には、サードパーティがどの程度まで、特に重要な機能及び中核的な業務分野に対して、サポートし、アクセスするかが含まれ得る。金融機関はリスクベースアプローチを用いて、サードパーティと関連する ICT サプライチェーンを更に評価することが推奨される。例えば、ソフトウェア供給者から、関連するサードパーティと厳密には関連していない（例：オープンソース）、ソフトウェアを構成するソフトウェアライブラリのリストのような、ソフトウェア部品表を入手することも重要なステップになり得る。

サイバーリスクの評価とデューディリジェンス

金融機関は、サードパーティと新たな取引関係に入る前、及び関係が継続する間、自らのサイバー戦略と整合的かどうかを検討するために、サードパーティのサイバーリスク評価及びデューディリジェンスを実施すること。

金融機関は、サードパーティの製品やサービスの提供能力に関するリスクだけでなく、サードパーティ及び ICT サプライチェーンが業務環境にもたらす潜在的なサイバーリスクや脆弱性を評価、管理すべきである。金融機関は、サポート対象の業務運営の重要性、サードパーティによる（物理的及び論理的の両面による）アクセスのレベル、アクセスまたはホストするデータ又はシステムの機密性並びに接続方法などのリスク要素を評価することができる。

金融機関が実施するデューディリジェンスの一部として収集する情報には、サードパーティの現在のサイバーリスク戦略及びサイバーレジリエンス（サイバー攻撃への耐性やダメージからの回復力）に関する過去のパフォーマンスを含めることができる。金融機関は、サードパーティのリスクマネジメントプログラムが金融機関の統制環境（法的・規制上の義務を含む）に従って実施されていることについて比例的で最新の確認を行うために、サイバーリスクに係るデューディリジェンスを、契約前と契約期間中の両方で、リスクベースアプローチに基づいて実施すべきである。金融機関は、上述のリスク評価やデューディリジェンスを効率的に実施するため、共同でサードパーティを評価することを検討することができる。

契約の構成

金融機関とサードパーティとの契約は、再委託から生じるものを含んだ、サイバーリスクマネジメントに資する条項を含むこと。

金融機関は、サードパーティとの取引開始に先立って、法的義務並びに関連当局の要件及び金融機関の期待要件が契約に含まれていることを確認すべきである。

金融機関は、サイバーセキュリティに関する契約の条項の中に、取引の対象、パフォーマンス基準、金融機関及びその関連当局のアクセス、情報及び監査に関する権限、報告規定、サイバーレジリエンステストの種類（例：侵入テスト、TLPT）及び頻度に関する要求、データの所在、保管、保持、移転及び廃棄に関する取決め、再委託、さらには可能な範囲において ICT サプライチェーンに関する規定並びに契約終了の条件を含めることができる。法律で別段の定めがない場合には、契約上の合意により、契約されたサービスの納品にかかる重大な変更を含め、サードパーティとの取引により生じるサイバーリスクの評価に必要な情報が金融機関や関連当局に対し、確実に提供されるようにすべきである。

さらに、サイバーインシデントを含め、サードパーティのサイバーリスクプロファイルに悪影響を及ぼし得る、ICT サプライチェーン内での事象が金融機関に報告されることに関する期待が、契約中に明示されるべきである。

継続的なモニタリング

金融機関は、自らのサイバーリスクを管理するため、継続的にサードパーティの重要性やリスクの変化をモニタリングし、契約履行状況を確認すること。

モニタリングは、リスクの重大性に応じたものであるべき、またサードパーティとの関係の特性の変化を考慮に入れて実施すべきである。継続的なモニタリングの対象には、サードパーティに係る重大なサイバー脆弱性及びリスクの変化、その業務環境及びサイバー脅威又はインシデントの影響を含めることができる。金融機関は、契約上の期待に達しているかどうかを判断するため、サードパーティのパフォーマンスを定期的に監視すべきである。金融機関は、モニタリングに資するため、サイバーリスクの定量的指標やリスク評価指標を収集・分析することができる。

サードパーティが特に重要な機能を提供している場合や、より重大なリスクを金融機関にもたらしている場合には、適切な監視を伴った、より厳格かつ高頻度のモニタリングの実施が検討されるべきである。

金融機関は、サードパーティ及び ICT サプライチェーンに関連するサイバーリスクの進化に対応するため継続的に学習し、能力開発すべきである。

要素３：インシデント対応

金融機関は特に重要なサードパーティを含むインシデント対応計画を策定し、演習を実施すること。

金融機関のインシデント対応計画は、サードパーティに関係するサイバーインシデントの検知・情報収集の方法や、サードパーティ及び適切な当局との連絡手段を含むべきである。また、役割及び責任並びに国の CIRT（サイバーインシデント対応のためのチーム）を含む関連当局への報告基準も含めるべきである。

定期的な演習は、弱点の特定、サイバーレジリエンスのテスト並びに対応及び復旧の適切性の評価に役立てることができる。可能な場合には、インシデント対応計画について、金融機関、サードパーティ及びその他関係者と共同で演習を実

施するべきである。インシデント対応計画は、組織変更や教訓を踏まえて見直されるべきである。

要素４：コンティンジェンシープランと出口戦略

金融機関は、サードパーティがサイバー関連のパフォーマンスの期待要件を満たさない場合又は金融機関の許容範囲を超えるサイバーリスクをもたらす場合に備えて、適切なコンティンジェンシープランと出口戦略を有しておくこと。

金融機関は、特に重要な機能を提供する能力を確保するため、実行可能なコンティンジェンシープラン及び出口戦略を策定し、維持すべきである。金融機関のサイバーリスクに影響を及ぼすシナリオには、以下が含まれ得る：サードパーティの業務運営における重要事象、サードパーティの運営能力の変化並びにサードパーティの商業上又はビジネス上の戦略及び/若しくはパフォーマンスの変化。検討すべき事項には、サービスを金融機関に戻す又は別のサードパーティに移管することが含まれ得る。金融機関は、自らの業務に最も適し、かつ、金融システムの安全性と健全性を促進し、消費者被害を抑制するために最適な選択肢を評価すべきである。

コンティンジェンシープラン及び出口戦略は、実行可能な範囲で適切にテストされるべきである。また、金融機関は、コンティンジェンシープラン及び出口戦略に対応するガバナンスに関する方針や基準に加え、特に重要なサードパーティのコンティンジェンシープランを理解し、検証すべきである。

<u>システム全体のサイバーリスクのモニタリングとセクター横断的な調整管理</u>

要素５：潜在的なシステミックリスクのモニタリング

金融セクター全体にわたるサードパーティとの取引がモニタリングされるとともに、潜在的にシステミックな影響を及ぼす可能性を有するサードパーティのサイバーリスクの要因が評価されていること。

サードパーティのサイバーリスク評価は、個別金融機関という単位を超えるものである。サードパーティがシステム上重要な金融機関に特に重要な機能を提供している場合又は複数の金融機関が共通のサードパーティを利用している場合

（集中リスク）、サードパーティのサイバーリスクは、システミックな影響を及ぼす可能性がある。こうした潜在的なシステミックリスクは特定及び評価され、管理でき得るべきである。

サードパーティがシステム上重要な金融機関に特に重要な機能を提供していない場合であっても、同一のサードパーティが複数の金融機関にサービスを提供している場合、集中リスクが生じる可能性がある。同様に、同一のサードパーティが複数の機能を提供している場合、リスクの集積又は複合を引き起こすことがある。金融機関は、サードパーティの利用に関して、自らの観点から集中リスクを特定、評価、監視し、関連当局と関連情報を共有すべきである。

関連当局は、必要に応じて、金融機関レベルとセクターレベルの両方で、集中リスク及び潜在的なシステミックリスクを特定、評価、監視するよう努めるべきである。これらのリスクのアプローチについて、関連当局は、これらのリスクを管理し、情報共有を改善するために適切な措置を実施するよう検討すべきである。手法の例としては、複数の金融機関に跨ったサードパーティ関連情報の統合並びに単一障害点、サードパーティの集中リスク又はリスクの伝播チャネルが生じ得る場所の特定が挙げられる。金融機関は、当該リスクを軽減するためにサードパーティの代替先を検討し得る。そのような措置を効果的なものとするため、金融機関、サードパーティ及び関連当局には、金融セクター内におけるサードパーティとの関係に関する情報共有を改善することが推奨される。

要素６：セクター横断的な調整

セクターを跨るサードパーティへの依存に関連したサイバーリスクは、それらのセクター間で特定のうえ、管理されていること。

金融セクターは、他のセクターのサードパーティに依存している。こうしたセクターの一つを混乱させるサイバーインシデントが発生した場合には、金融機関の中核的な業務機能の提供に影響を与える可能性がある。こうしたサイバーリスクを特定、管理するため、セクター間を跨いだ協調を促進するための適切なステップがとられるべきである。

金融機関が他のセクターのサードパーティから生じるサイバーリスクを監視、管理できるように、サイバーリスクに関するセクター横断的な情報共有の改善に努めることが奨励されるべきである。

金融機関及び関連当局は、健全なサイバーリスクマネジメントの促進、サイバーレジリエンスの向上、有効なプラクティスの共有支援及び可能な場合には協調的対応に資するため、他のセクター及び重要インフラに関するフォーラムとの協働の機会を継続的に模索すべきである。

要素７：金融セクターのサードパーティ

金融機関と契約するサードパーティは、金融機関のリスク管理要件が、サービス・物品の提供に影響を及ぼす可能性を認識すべきである。

金融機関は、サードパーティの提供するサービスの安全かつ健全な運営を確保する責任を免れない。しかし、サードパーティは、金融機関がサイバーリスクを特定、評価、監視、軽減し、関連するリスク管理要件を遵守することを支援すべきである。これは特に、ICT 及びサイバーセキュリティサービスをサポートするサードパーティに当てはまる。この限りにおいて、サードパーティは、金融機関によるサイバーリスクの効果的な管理を促進するために、サードパーティに関するサイバーリスクを含め、必要な情報を利用できるようにすべきである。これには、重大インシデントに関連する情報、サービス又はサービスや製品のサポートを終了する意図並びに ICT サプライチェーンの他の当事者と特に重要なサードパーティとの関係を開始する意図のような、金融機関や顧客に影響を及ぼす可能性のある情報が含まれる。

該当する場合、サードパーティは、ICT サプライチェーンにおける自身のサードパーティから生じるサードパーティリスクに対処するために、本基礎的要素を用いることが奨励される。