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）

背景および対象

金融セクターにおける民間・公的金融機関（以下、「金融機関」）では、様々な業務上の理由により、サードパーティを活用している。サードパーティを活用することにより、それを活用する金融機関に追加的なサイバーリスクマネジメント上の課題が生じる。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り、不正行為や業務の中断、顧客または企業の機微（センシティブ）情報へのアクセスに至る可能性がある。サードパーティの規模、複雑性、相互依存関係が高まり、またその利用が継続的に増加することに伴い、サイバーリスクの可視性を維持することは、個々の金融機関や金融システム全体にとって大きな課題となってきている。

金融機関は、自らが依存するサードパーティに対して、しっかりとしたリスクマネジメント手法を未だに確立できていない可能性があり、このことがサイバーリスクマネジメントの複雑性を増している。

サードパーティとは、モノやサービスを提供するために金融機関と業務上の関係や契約を有する組織である。サードパーティとの関係の重要な形態の一つとして、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業務機能、サービス、またはプロセスをサードパーティが提供する。

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）および「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。

G7 では、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、「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」を策定した。これは、金融機関が、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、法律や規制のフレームワークに対応できるように設計された基礎的要素である。各基礎的要素はノンバインディングであり、既存のフレームワ

ークを無効化したり、そうしたフレームワークの継続的な適応を妨げるものではない。

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、およ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。金融機関およびサードパーティは、本「基礎的要素」を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活用することができる。その際、金融機関は、サイバーリスクの規模、特性、対象、複雑性、潜在的にシステミックな重要性を考慮した相応のアプローチをとるべきである。一国の、または国を跨る当局も、サードパーティリスクに対応するための自らの政策や規制・監督上の取組みを伝えるため、本「基礎的要素」を活用することができる。

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およ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組織は、サードパーティの管理を含む、金融機関のサイバーリスクマネジメントの監視および実行に関する最終的な責任を有する。監視および実行には、サードパーティとの関係について文書化された戦略やリスク許容度、および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と責任の明確化が含まれる。このほか、金融機関内部のあらゆるレベル、およびサードパーティ、関連当局との間での通常業務としての適切なコミュニケーションやエスカレーションを実施することも含まれる。

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、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。サードパーティから金融機関への（サイバーリスクの）伝播を防ぐためのポリシーや管理措置を、金融機関は導入すべきである。金融機関は、再

委託の利用など、サードパーティ自身が別のサードパーティに依存することを含め、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を保有するとともに、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を理解しておくこと。

一覧には、全てのサードパーティのリスト、提供するサービスや機能、保持または処理するデータの種類や機密性、金融機関の業務にとっての重要性が含まれるべきである。

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に、自らの戦略と整合的かどうかを検討するために、サイバーリスク評価およ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、サードパーティによる（物理的および論理的の両面による）アクセスのレベル、アクセスするデータやシステムの機密性、接続方法などのリスク要素を検討することができる。

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、サードパーティに自らのサードパーティリスクのライフサイクルに沿って、デューディリジェンス実施することを要求すべきである。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の契約の中に、サイバーリスクマネジメントを支援するための条項を含むこと。

金融機関は、サードパーティとの取引開始に先立ち、法的義務や関連当局の要求、およ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。この中には、機密データの保持、移転および廃棄に関する条件を含めることができる。

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、アクセスや監査に関する権限、報告に関する定め、再委託に関する定め、契約終了のオプション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、金融機関や関連当局に対し、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報告に関する期待要件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、リスクの重要性に応じ、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、サードパーティの重大なサイバー脆弱性やリスクの変化、その業務環境、サイバーの脅威やインシデントの影響を含めることができる。金融機関はサードパーティのパフォーマンスが期待どおりか判定するために、契約を確認すべきである。金融機関は、モニタリングを裏付けるため、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。

サードパーティが重要な機能を提供していたり、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、より厳格かつ高い頻度で、適切な監視を伴ってモニタリングすることが検討されるべきである。金融機関は、サードパーティに関連するサイバーリスクの進化に対応するための学習や能力開発を継続すべきである。

要素３：インシデント対応

金融機関は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には、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、サードパーティおよび適切な当局との連絡手段が含まれるべきである。また、役割と責任、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まれるべきである。

定期的な演習は、弱点の特定、サイバー攻撃に対する頑健性のテスト、対応や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は、金融機関、サードパーティその他の関係者と共同で演習が実施されるべきである。インシデント対応計画は、組織変更や教訓を考慮し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

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もしくは金融機関が許容できるリスクを超えてサイバーリスクを発生させた場合に備えて、適切なコンティンジェンシープランを用意しておくこと。

金融機関は、サードパーティに関連するサイバーインシデントが発生した後も重要な機能を継続するための能力を支援するため、コンティンジェンシープランを評価・利用すべきである。コンティンジェンシープランのオプションとして、金融機関は、サードパーティによる重要な機能の提供に代わる適切かつ実行可能な代替手段を特定すべきである。代替手段には迅速なアクセスが必要となる可能性がある。このため、サードパーティの業務機能やサービスを金融機関側に切り戻すことや、並行的に一つ以上の代替用サードパーティと契約することの検討が必要になる可能性がある。可能な場合には、金融機関は、サードパーティとの契約の中に契約解除条項を設けておくべきである。また、金融機関は、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確認・評価し、これらがどの程度有効なものかを把握すべきである。

<u>システム全体のサイバーリスクとセクターを跨ぐ協調のマネジメント</u>

要素５：潜在的なシステミックリスクのモニタリング

金融セクターを取り巻くサードパーティとの取引がモニタリングされ、潜在的にシステミックなインプリケーション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、個別金融機関の域を超えて発生することがある。サードパーティがシステム上重要な金融機関に重要な機能を提供している場合や、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、潜在的にシステミックなインプリケーションを有する可能性がある。こうしたリスクが管理できるよう、特定のうえ評価されるべきである。

サードパーティがシステム上重要な金融機関に重要な機能を提供していない場合であっても、同じサードパーティが複数の金融機関と取引している場合、集中リスクが生じる可能性がある。同様に、一つのサードパーティが複数の機能を提供している場合、リスクの集積や複合を引き起こすことがある。

こうしたリスクの管理や情報共有の改善方法には、金融機関を跨いでサードパーティに関する情報を積み上げることや、単一障害点、集中リスク、またはリスクの伝播チャネルが生じ得る場所を特定することが含まれる。サードパーティの代替可能性は、これらのリスクに対応するための検討事項かもしれない。そうした方策を有効なものとするため、金融機関および関連当局は、金融セクターを取り巻くサードパーティとの取引関係に関する情報共有の改善に努めるべきである。

要素６：セクターを跨る協調

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ベ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、セクターを跨る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モニタリング・管理できるように、サイバーリスクに関するセクター間の情報共有を改善する努力が奨励されるべきである。

金融セクターは、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のため、他のセクターや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求め続けるべきである。