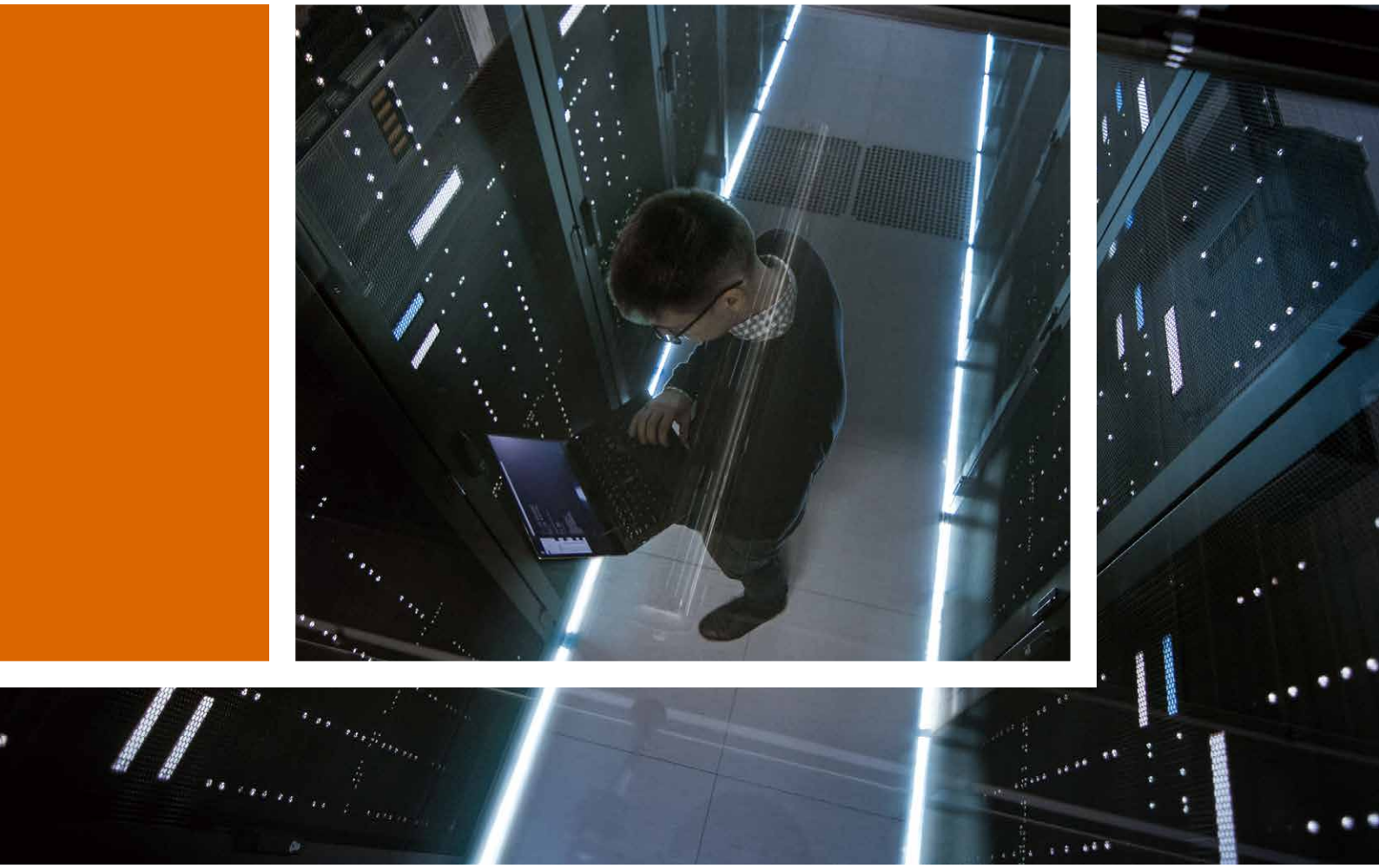
海外金融機関における
サプライチェーンサイバーリスク管理の
最新動向



pwc

www.pwc.com/jp

エグゼクティブサマリー

昨今、規制当局は金融機関に対してサプライチェーンのサイバーリスク管理を強化することを求めており、日本の金融機関も委託先のリスク管理策をアップデートする必要があります。サプライチェーンのサイバーリスク管理を怠ると、情報漏洩やシステム停止といった影響だけでなく、レピュテーションや顧客ロイヤリティなどへの中長期的なビジネス影響が発生する可能性があります。

しかし、金融機関が資本関係のない委託先に対して、どこまでリスク管理を求めるべきか、どこまでなら下請法（下請代金支払遅延等防止法）に抵触しない範囲か、といった課題を持つセキュリティ責任者の懸念が多々生じています。そこでPwCコンサルティング合同会社では、国内金融機関のセキュリティ責任者への示唆を得るために、海外金融機関の有識者に先進事例に関するインタビューを実施しました。

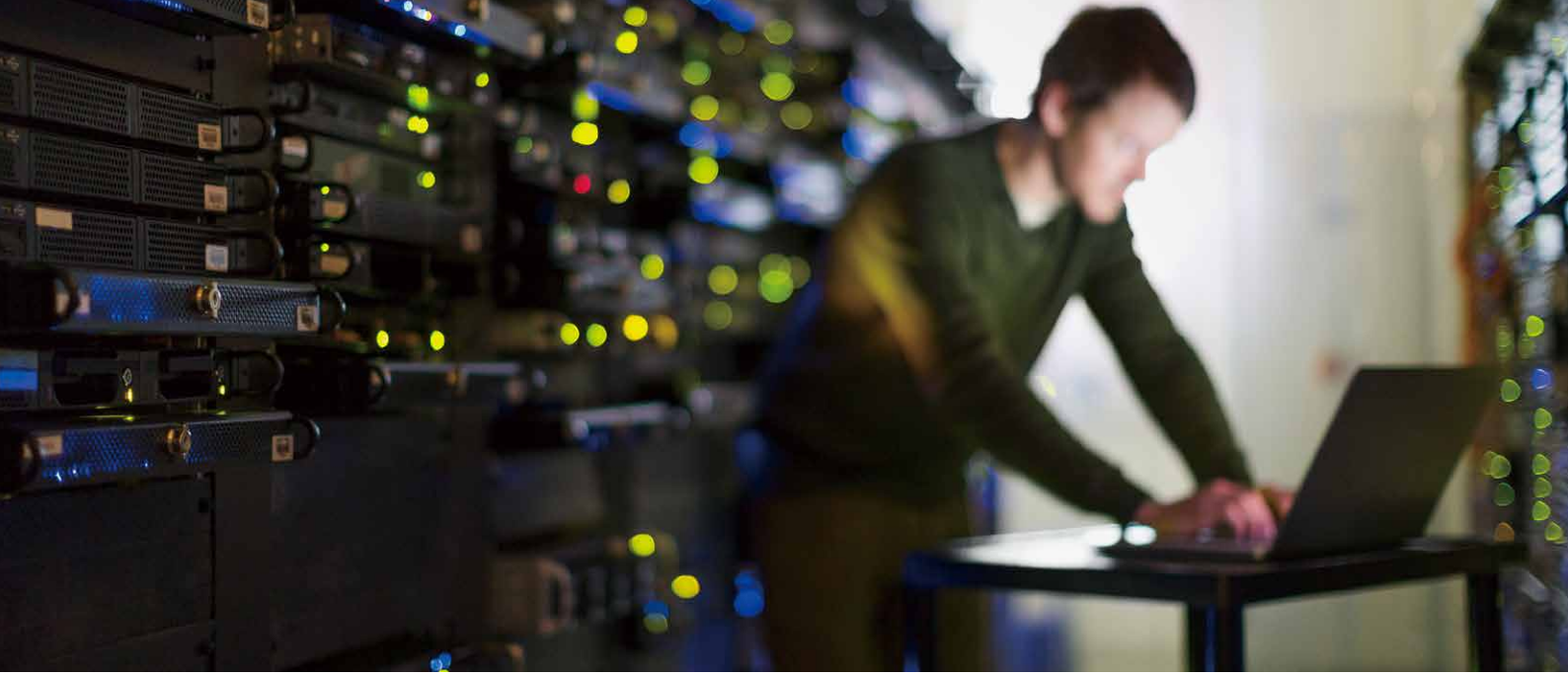
本レポートは、国内金融機関のサイバーセキュリティ責任者に対し、サプライチェーンのサイバーリスク管理に関する海外の先進的な取り組み事例を整理し、日本の金融機関が今後実施すべきアクションを提言としてまとめたものです。

有識者ヒアリングから得られた推奨事項

サプライチェーンのサイバーセキュリティに対して先進的な取り組みを行う海外組織の有識者へのヒアリング結果から、国内企業で採用可能な各フェーズにおける主な推奨事項が以下のように明らかになりました。

フェーズ	推奨事項
委託先、サービスなどの選定時のセキュリティリスク評価	・公開情報の収集・分析により企業、サービスなどのセキュリティリスクを評価する。外部の評価サービスを利用することで、評価プロセスを効率化できる場合がある。
契約時のセキュリティ評価	・委託先や外部のサービスを評価するチームには技術的なセキュリティに明るいメンバーも参画させ、トレンドの脅威シナリオに応じて関連する評価を取り入れる。 ・インシデント発生時やその疑いがある場合を想定し、委託先の責任範囲や報告時限をSLA（Service Level Agreement：サービスレベル合意書）に定める。
委託先のリスク管理	・高リスクなシステムを取り扱う委託先に対しては、委託先の拠点をオンサイト訪問して確認を行う。 ・再委託を行う場合、再委託先のセキュリティ管理は委託先が実施するよう要求する。それ以降の再委託がある場合も同様に、各委託元が自社への要求と同レベルのセキュリティ管理を実施するよう依頼する。
ソフトウェア管理	・ソフトウェア構成管理は製品などを導入して徹底し、脆弱性管理につなげる。SBOM（Software Bill of Materials：ソフトウェア部品表）の利用も検討する。 ・オープンソースソフトウェア（OSS）の管理にはツールを活用し、選定時の判断や依存関係の洗い出しなどを効率化する。
ハードウェア管理	・資産管理を徹底し、ファームウェアの迅速なアップデートが可能な体制を整備する。 ・脅威シナリオベースのセキュリティテストを行う。
経営層への報告	・セキュリティコストについて、技術用語を多用せず、収益、顧客満足度、評判、顧客ロイヤリティへの影響などを踏まえたビジネス用語で整理し、報告する。 ・サイバーセキュリティリスクを経営層へ報告する経路は組織により最適解が異なるため、リスクベース、金額ベース、ITベースなど、各組織に適した経路を検討する。その際、CIO（Chief Information Officer）とCISO（Chief Information Security Officer）の利益相反が生じない工夫をする。

目次



1 はじめに

1.1 サプライチェーンにおけるサイバーリスクとは

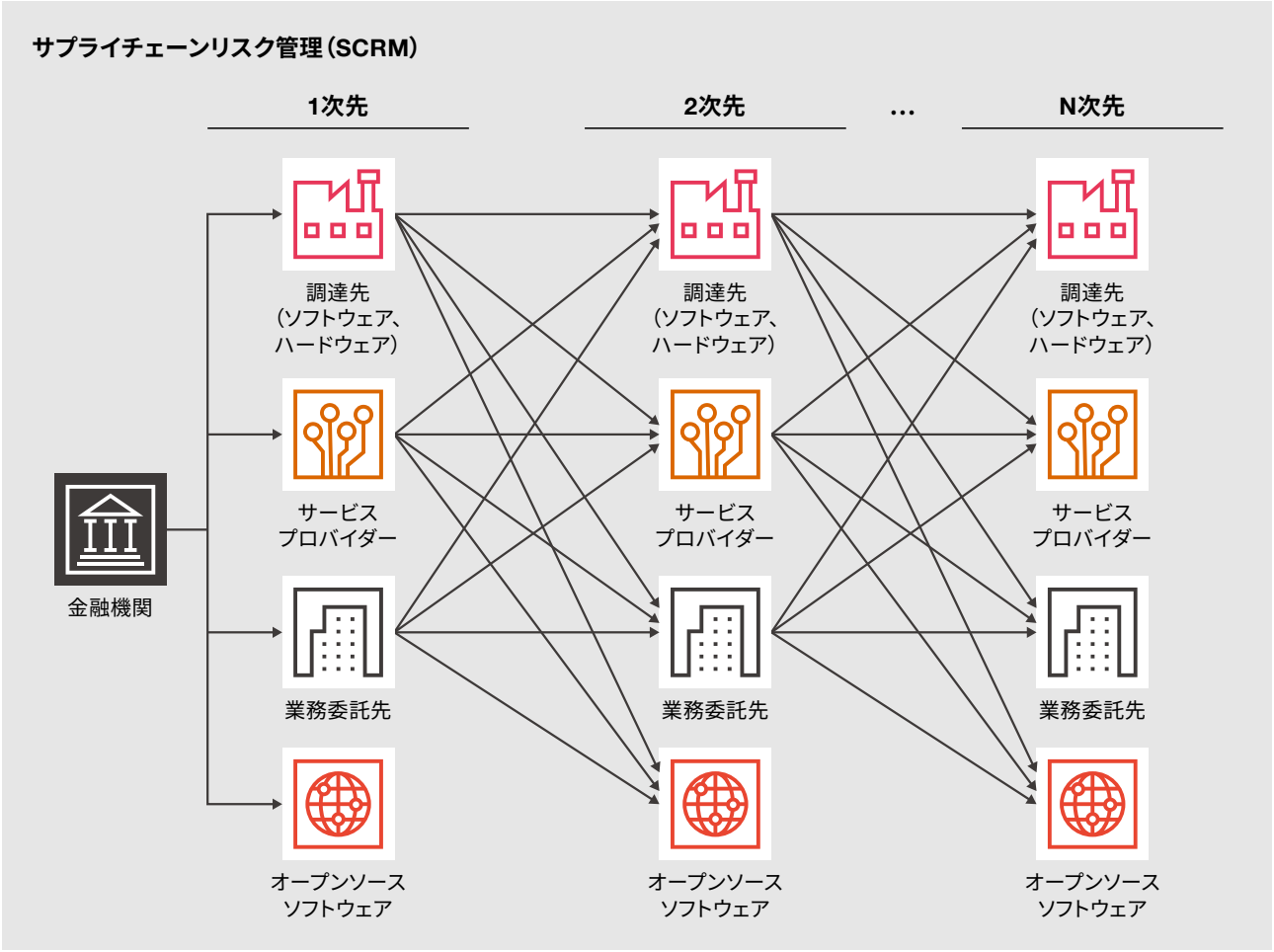
サプライチェーンを悪用したサイバー攻撃の被害は近年頻繁に確認され、懸念が高まっています。具体的には、標的とする組織を直接狙わずに、セキュリティ対策が比較的手薄な関係組織を踏み台とする攻撃や、幅広く使用されるソフトウェアやハードウェア、サービスのサプライヤーを侵害し、そのユーザー企業に被害をもたらす攻撃などが該当します。IPA（Information technology Promotion Agency：独立行政法人情報処理推進機構）の「情報セキュリティ10大脅威[1]」の「組織」向け脅威においても、「サプライチェーンの弱点を悪用した攻撃」は、2022年は3位、2023年は2位と高位での選出が続いています。組織の関連先ごとに想定されるサイバーリスクには、以下のようなものが考えられます。

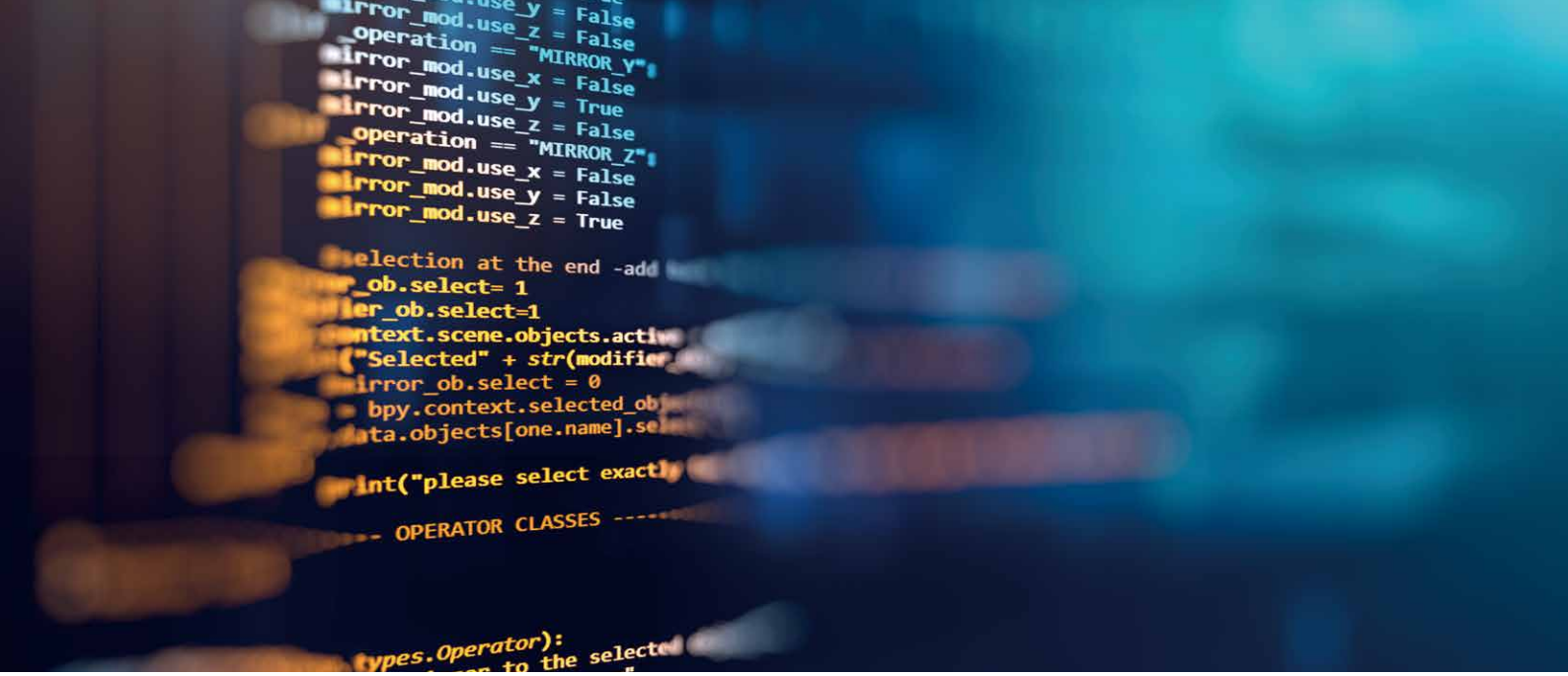
関係先	想定されるサイバーリスク例
業務委託先	・委託先従業員の故意・過失による情報漏洩 ・オンラインサービスの不適切なアクセス制御によるソースコードや知財の窃取、漏洩 ・業務委託先で発生したサイバーインシデントの波及 ・業務委託先を経由した不正アクセス
調達先（ハードウェア、ソフトウェア）	・納品前の段階で組み込まれたバックドアからの不正アクセス ・ソフトウェアアップデートが悪用されマルウェア感染 ・脆弱性を悪用した不正アクセス
サービスプロバイダー	・ソフトウェアアップデートが悪用されマルウェア感染 ・脆弱性を悪用した不正アクセス
オープンソースソフトウェア	・脆弱性を悪用した不正アクセス ・開発時点での不正なコードの埋め込み

1：https://www.ipa.go.jp/security/10threats/index.html

1.2 本調査のスコープ

本調査では、以下のようなサプライチェーンを想定し、金融機関にかかわる有識者を対象にサードパーティなどの1次先、またフォースパーティ以降の関係先のサイバーセキュリティリスクへの取り組みに関する調査を実施しました。





2 海外の金融機関における サプライチェーンリスク管理の 規制・ガイドの動向

金融機関においてもサプライチェーンのサイバーリスクは懸念されており、G7サイバー・エキスパート・グループ（CEG：Cyber Expert Group[2]）は2022年10月、「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[3]」の改定版を公表しました。各国でも金融機関におけるサプライチェーンのサイバーリスク管理に関連する施策が実施されています。

本章では、G7や金融分野において先進的な取り組みが行われているとされる欧州、米国、英国、シンガポールにおける金融機関のサプライチェーンのサイバーセキュリティリスクに関連する法規制やガイドラインをご紹介します。

2.1 G7

- **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**

G7ではCEGが設置され、各国の金融当局によりサイバーセキュリティに関するさまざまな取り組みが進められています。CEGは2022年10月、2018年に公表した「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に関するG7の基礎的要素」を改訂し、サードパーティとの関係のみならずICTサプライチェーン管理にも焦点を当てました。同文書では、サードパーティおよびICTサプライチェーンについて右のように定義しています。

サードパーティ	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
ICTサプライチェーン	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

2：https://www.banque-france.fr/en/economics/international-relations/international-groups-g20g7/focus-g7-cyber-expert-group
3：https://www.fsa.go.jp/inter/etc/20221021/thirdparty_kariyaku.pdf

同文書では、金融機関はサードパーティのICTサービスを利用することにより、金融サービスのイノベーションの向上や中核的事業への集中、IT支出を効率化できる一方で、利用の規模や複雑性が増すことによりサイバーリスクの理解、測定、軽減が困難になると指摘されています。改訂版では、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を注意喚起するためとして、それまでの6つの基礎的要素に加え、新たに「要素7」が追加されました。基礎的要素は、金融機関およびサードパーティが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可能であるとされています。以下に7つの基礎的要素の概要を紹介します。

要素1：ガバナンス

金融機関のガバナンスに関する組織（取締役会や役員会など）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および実行に関する最終的な責任を有する。監視、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
- サードパーティおよ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
- 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、責任および説明責任の明確化
- 金融機関内部、サードパーティおよ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およびエスカレーションのプロセス確立

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について、以下に例示するポイントを含め、サードパーティに関するサイバーリスクを特定、評価、監視、報告するなどのライフサイクル全体を通じて管理する有効なプロセスを有すること。

- 全てのサードパーティの重要性を特定し、リスト化
- 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さらに評価することが推奨される（例：ソフトウェア供給者からオープンソースソフトウェア（OSS）のソフトウェアを構成するライブラリのリストを入手する）
- サードパーティおよびICTサプライチェーンがもたらす潜在的なサイバーリスクや脆弱性を評価、管理
- サイバーリスクの評価は取引前および契約中も実施
- 再委託のサイバーリスクやICTサプライチェーンも考慮した契約の構成
- 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すICTサプライチェーン上の事象が発生した場合の報告
- リスクの重要度に応じて、厳格さや頻度を考慮したモニタリング

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、可能な範囲で関係組織間の共同演習を実施すること。

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、また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、自組織での対応や他のサードパーティへの移管による対応など、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。

要素5：潜在的なシステミックリスクのモニタリング

複数の金融機関が共通のサードパーティを使用している場合、当該サードパーティのリスクは金融セクター全体に影響（システミックな影響）を及ぼす可能性がある。個々の組織にとどまらず、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、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。

要素6：セクター横断的な調整

セクターをまたが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。

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と。また、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。

2.2 欧州

EU

- **Digital Operational Resilience Act（DORA）[4]**

EUの金融業界のデジタル・オペレーショナル・レジリエンスに関する新しい規制で、EU内に拠点を置いている金融機関は2025年初頭までに本規制に準拠する必要があります。以下の5項目がフォーカスされており、そのうち「ICTサードパーティのリスク管理」では、外部委託にかかわるリスクの監視や再委託によるリスクの考慮、契約時の留意事項など、サードパーティがもたらすリスクの管理を強化するよう求められています。

- ICTリスク管理
- ICT関連インシデント報告
- デジタル運用のレジリエンステスト
- ICTサードパーティのリスク管理
- 情報共有

ENISA
（The European Union Agency for Cybersecurity：欧州連合サイバーセキュリティ機関）

- **Threat Landscape for Supply Chain Attacks[5]**

2020年から2021年7月の間に確認された24件のサプライチェーン攻撃の分析結果から脅威状況をまとめたレポートです。各事例においてサプライヤー側と顧客側双方の、攻撃に使用された手法と、標的とされた資産について説明され、概況がまとめられています。また、サプライチェーン攻撃のリスクを軽減するため、顧客とサプライヤーへの推奨事項が記載されています。

2.3 米国

米国では、2021年5月に公表された国家のサイバーセキュリティの向上に関する大統領令（EO：Executive Order）14028においてソフトウェアサプライチェーンのセキュリティ強化が示され、関連機関で対応が進められています。

NIST
（National Institute of Standards and Technology：米国国立標準技術研究所）

- **NIST Special Publication, NIST SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations[6]**

組織のサプライチェーン全体のサイバーセキュリティリスクを特定、評価、および軽減するためのガイダンスです。同文書は、サイバーセキュリティサプライチェーンリスク管理（C-SCRM）戦略実施計画、C-SCRM方針、C-SCRM計画、製品およびサービスのリスク評価の策定に関する指針を含む、多階層のC-SCRM特有のアプローチを適用することにより、C-SCRMを組織のリスク管理活動に統合するものです。2015年に初版が公開され、EO14028を受けて2022年5月に改定版Rev.1が公開されました。改定版では、想定読者を製品やソフトウェア、サービスの取得者やエンドユーザに広げており、組織がサプライチェーン内およびサプライチェーン全体でサイバーセキュリティリスクを管理する際に採用すべき主な施策が提供されています。

- **Cybersecurity Framework[7]**

重要インフラ事業者などが自主的にサイバーセキュリティリスクを管理するためのフレームワークとして、2014年に第1版が公開されました。サイバーセキュリティ対策の全体像が「特定」「防御」「検知」「対応」「復旧」の5つの機能に分類され、対策や参考情報が提供されています。2018年に公開された第1.1版では、サプライチェーンのリスク管理の重要性が追記されており、サプライチェーンの関係組織間でサイバーセキュリティ要求事項に関するコミュニケーションを行う際や、購買の際の要求事項において当該フレームワークが活用できると説明されています。CSF2.0版のドラフトを作成にむけて公開されたコンセプトペーパー[8]では、サイバーセキュリティサプライチェーンリスク管理の重要性を強調していくという方向性が示されています。

4：https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=EN
5：https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
6：https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf
7：https://www.nist.gov/cyberframework/framework
8：https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf

U.S. Department of the Treasury（米国財務省）

- **The Financial Services Sector's Adoption of Cloud Services**[9]

金融機関によるクラウドサービスの利用増加に伴う潜在的な利点と課題についてまとめたレポートです。金融サービスにおいてクラウドサービスが使用されている状況を整理し、金融機関がクラウドを導入する際に参照可能なフレームワークや実施すべき対応が記載されています。またクラウドサービス利用における金融機関の主な課題として以下の6件が挙げられています。

- 金融機関がデューデリジェンスや監視を実施するためのクラウドサービスプロバイダーからの情報開示が不十分
- 金融機関がクラウドサービスを安全に展開するためのクラウドサービスプロバイダーの人材や技術支援ツールの不足
- 一つのクラウドサービスプロバイダーのインシデントが広範な金融機関に連鎖的に影響を与える可能性
- クラウドサービスプロバイダーの数が限定的であることが金融セクターの回復力に及ぼす潜在的な影響
- クラウドサービスプロバイダーの数が限定的であることによる金融機関との交渉における優位性
- クラウドテクノロジーへの各国の規制の違いへの対応から最終的にコスト上昇など、利用企業の不利益になる可能性

米国財務省はこれらの課題への監視と対処を行うにあたり、関連当局間でCloud Services Steering Group（クラウドサービス運営グループ）を設立し、民間金融機関や他国の関係機関と協力して以下を実施していくと説明しています。

- クラウドサービスに関する米国の規制当局間のより緊密な国内協力の促進
- クラウドサービスプロバイダーや金融機関と協調した机上演習の実施
- クラウドサービスへの依存度が高まっていることを考慮し、セクター全体のインシデント対応手順の見直し
- セクター全体のクラウドサービスへの依存度を適切に測定する方法を検討し、関連するリスクを評価する
- 金融サービス業界で効果的なリスク管理を促進する方法の特定

FFIEC（Federal Financial Institutions Examination Council：米国連邦金融機関検査協議会）

- **Outsourcing Technology Services**[10]

金融機関におけるアウトソーシングの増加に伴うリスクを説明し、法律や関連する当局の規制やガイダンスをベースに、金融機関がサードパーティへ委託を実施する際のリスク管理プロセスを確立し、当該プロセスを評価するための手順を示すガイドラインです。

9：https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf
10：https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx

2.4 英国

英国は金融機関と直接契約を取り交わすサードパーティだけではなく、その再委託先であるフォースパーティ以降のリスク管理についても、直接の監査権限を保有するなど明記されているのが特徴です。

NCSC（National Cyber Security Centre：英国国家サイバーセキュリティセンター）

- **Supply chain security guidance**[11]

組織のサプライチェーンセキュリティに関する認知度を向上させ、リスク管理の継続的な実施を支援するために作成されたガイダンスです。「リスクの理解」「管理策の確立」「対策の確認」「継続的な改善」の4セクションにおける12原則について説明されています。また、サプライチェーンに対する攻撃について事例をベースに解説されています。なお、本ガイダンスの活用はGDPR（General Data Protection Regulation：EU一般データ保護規則）の準拠にも有用であるとしています。

PRA（Prudential Regulation Authority：英国健全性監督機構）

- **Outsourcing and third party risk management**[12]

PRAの規制対象となる金融機関が、業務委託やサードパーティリスクマネジメントを実施するにあたって遵守すべきPRAの規制要件や期待を具体的に定めた、Supervisory Statement（SS：監督声明）です。サードパーティのサービスプロバイダーへの委託に関して、「ガバナンスおよび記録管理」「アウトソーシング前のフェーズ」「アウトソーシングの契約」「データセキュリティ」「アクセス権、監査権、情報に関する権限」「再委託」「業務継続計画およびアウトソーシング終了計画」の各フェーズにおいて実施すべき点が説明されています。「再委託」のフェーズでは、金融機関は当該業務が再委託可能か判断し、以下のような点などを含め、委託先や再委託先に対して留意すべき事項が記載されています。

- 金融機関が委託先と契約を締結する前に再委託先に関連するリスクを評価すること
- 金融機関は委託先に再委託先を含めた最新のリストを維持するよう依頼し、金融機関も把握すること
- 再委託先に、適用される全ての法律や規制、契約上の義務を遵守させること
- 委託先と再委託先との契約において、金融機関にも委託先と同様に再委託先へのアクセス権、監査権、情報に関する権限を付与すること
- 重要な委託先との契約に悪影響を与えうる再委託が提案された場合や、リスクの増加につながる可能性がある場合は、金融機関は再委託に異議を唱え、必要に応じて契約を終了する権利を行使できること

2.5 シンガポール

国の実情から、国外への業務委託に関して、カントリーリスクの可能性に関する指摘や、考慮すべき事項に関する具体的な記載があるのが特徴です。

MAS（Monetary Authority of Singapore：シンガポール金融管理局）

- **GUIDELINES ON OUTSOURCING**[13]

金融機関におけるアウトソーシングについて、金融サービス提供の安定化やセキュリティ確保などを目的に策定されたガイドラインです。本ガイドラインの5章では業務委託に関するリスク管理について、経営層の役割、リスク評価、契約など、業務委託に関する各フェーズにおいて実施すべき事項が記載されています。とりわけ5章10項「国外への業務委託（Outsourcing Outside Singapore）」では、国外のサービスプロバイダーへ業務委託する際には以下の点に留意するよう説明されています。

- 政府の政策
- 政治的、社会的、経済的状況
- 外国における法律および規制の進展
- 委託先のサービスプロバイダーを効果的に監視し、事業継続管理計画と出口戦略を実行する自社（金融機関自体）の機能

11：https://www.ncsc.gov.uk/collection/supply-chain-security

12：https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf?la=en&hash=5A029BBC764BCC2C4A5F337D8E177A14574E3343

13：https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/%20%20Outsourcing-Guidelines_Jul-2016-revised-on-5-Oct-2018.pdf

3 先進的な取り組み事例と提言

有識者ヒアリングから得られた先進的な取り組みのうち、国内組織において取り入れられる要素を検討し、以下に提言します。なお、本章は網羅的なベストプラクティスではなく、参考になる示唆を各組織の目的に応じて検討のうえ、ご活用いただくことを想定しています。

3.1 委託先、サービスなどの選定時のセキュリティリスク評価

ここでは、外部から取得可能な情報を用いて評価する場合を想定しています。

取り組み事例	・公開情報の分析による企業のセキュリティリスク評価において、代用可能な項目は外部サービスによる評価結果を利用し、評価プロセス全体の効率化を図る ・セキュリティ関連の認証取得状況を参照する
提言	**＜評価項目、方法＞** 委託先選定に向けた企業のセキュリティリスク評価をする際、一般的なセキュリティ関連認証の取得状況の確認と併せて公開情報を収集・分析し、企業のセキュリティリスク評価を実施します。その際、代用可能な項目は外部のサイバーセキュリティリスク評価サービスを利用することで、評価プロセスの効率を高めることが期待できます。 **＜公開情報分析によるセキュリティ評価の留意事項＞** 公開情報分析による評価結果は企業のセキュリティ状況を示す一つの側面であり、実態と乖離がある可能性があります。その前提を踏まえたうえで評価結果を使用することが肝要です。

3.2 契約時のセキュリティリスク評価

取り組み事例	・委託先や外部のサービスを評価するチームには、技術的なセキュリティに明るいメンバーも参画する。 ・基準などをベースとした評価項目に加え、トレンドの脅威シナリオに応じて関連する評価を取り入れる。 ・評価対象や内容に応じて、自動化可能な部分は評価ツールを取り入れる。 ・必要に応じてエビデンスの提出や委託先のサイトでのレビューを行う。 ・委託先による再委託先管理の方法を確認し、必要に応じて再委託先のセキュリティ評価のエビデンスを求める。 ・インシデント発生時やその疑いがある場合を想定し、委託先の責任範囲や報告時限をSLAに定める。 ・特にリスクレベルの高いシステムは、高頻度での評価を実施できるよう契約時に定めておく。
提言	**＜評価チーム＞** 契約時に委託先を評価するチームのメンバーには、従来の調達メンバーに加え、契約の範囲に含まれるシステムのセキュリティに詳しいテクニカルなメンバーも参画することで、契約段階でのセキュリティ要件定義がより効果的になることが期待できます。 **＜評価内容＞** 評価項目は、従来の一般的な基準などに応じた項目に加えて、トレンドの脅威に特化した分析をし、そのシナリオに応じた評価が重要です。特に複雑化するサプライチェーンにおいて、実際の攻撃事例を参考にし、自社が同様の攻撃を受けた場合を想定して評価し対策する必要性が高まっています。なおセキュリティ要求を満たしていない項目は実情を把握し、残存リスクとして管理することが肝要です。 **＜評価対象、範囲＞** リスクレベルに応じて、委託先のオンサイトでのレビューを実施して実情を把握することを推奨します。重要なシステムにおいては、委託先のみならず、再委託先からもエビデンスの提出を求めて評価することを推奨します。 **＜脆弱性やインシデント発生時の対応＞** 委託先での脆弱性の発見時やインシデント発生時の対応については、検知後一定時間以内の報告、委託先が対応する責任範囲、問い合わせへの一次回答までの時間などを具体的にSLAに定めることを推奨します。 **＜要件の見直しや契約の終了＞** 委託先の評価はその時点のものであり、時間の経過とともに変わってゆくため、リスクレベルの高いシステムは四半期に一度など、高頻度での評価を実施できるよう契約に含めることを推奨します。セキュリティが脅かされる場合には、契約の終了を選択できるような準備をしておくことを推奨します。

3.3 委託先のリスク管理

取り組み事例

- 評価の頻度はシステムの重要度に応じて定め、高リスクなシステムは頻度高く評価を行う。その際、新しい攻撃パターンに応じた脅威シナリオをベースとした評価も取り入れる。
- 高リスクなシステムを取り扱う委託先に対しては、委託先の拠点をオンサイト訪問して確認を行う。
- 委託先からペネトレーションテスト（ペンテスト）のスケジュール、脆弱性、パッチ適用時期などの情報を入手する。必要に応じて、許可を得て委託先のサイトにおいてペンテストを実施する。
- 再委託を行う場合、再委託先のセキュリティ管理は委託先が実施するよう要求する。それ以降の再委託がある場合も同様に、各委託元が自社への要求と同レベルのセキュリティ管理を実施するよう依頼する。
- クラウド環境において、大規模リリース時は許可を得てペンテストを実施する。

提言

＜リスクレベルに応じた管理の設定＞

委託先のリスク管理は、関連するシステム・サービスによって委託先の重要度付けを行い、レベルに応じた内容・頻度でセキュリティ評価を行うことを推奨します。高リスクな場合は、委託先拠点をオンサイト訪問したうえでの確認や、許可を得て委託先の拠点においてペンテストを実施することもご検討ください。特に定型的なセキュリティ管理については、ツールを使用することでの効率化が期待できます。

＜残存リスクの管理＞

残存リスクはリスクレベルに応じた優先度にて改善計画を立案し、受容可能なリスクレベルに低減されるまで定期的なレビューを実施することを推奨します。

＜再委託先以降の管理＞

再委託先であるフォースパーティ以降のセキュリティについては、委託先に課すのと同様の要件が担保されるよう各委託元が管理すること、高リスクな場合は必要に応じて対策実施のエビデンスを求めて確認することを推奨します。

3.4 ソフトウェア管理

取り組み事例

- ソースコードはリポジトリで一元管理する。
- ソフトウェア構成管理は製品などを導入して徹底し、脆弱性管理につなげる。SBOMの利用も検討する。
- ソフトウェア導入時に脅威シナリオベースのセキュリティテストを行う。
- オープンソースソフトウェア（OSS）の管理にはツールを活用し、選定時の判断や依存関係の洗い出しなどを効率化する。
- OSS含めソフトウェア選定時はサードパーティの評価と併せて他の事業者の利用状況を調べて指標とする。

提言

＜資産管理、構成管理＞

ソースコードは自社内のリポジトリで一元管理し、そこで複数の解析ツールを使用してスキャンすることで効果的にセキュリティを担保できるため、実施の検討を推奨します。

ソフトウェア構成管理では、特に米国では委託先が提供するSBOMを利用した管理が行われている一方で、再委託先以降の組織からSBOMを完全に取得するのは現実的に難しいため、実施可能な部分から活用を推奨します。

資産管理や構成管理は煩雑ですが、脆弱性管理の遂行には必須事項です。委託先からSBOMの提供を受けられる場合はそれを利用し、社内で総合的に管理して着実に継続していくことが求められます。管理ソフトウェアなどを導入し、可視性や効率性を高めることを推奨します。

＜オープンソースソフトウェア（OSS）の管理＞

OSSを管理するツールを利用することで、選定時のポリシー管理や依存関係の洗い出しに関する負担軽減が期待できます。

＜選定＞

OSS、商用ソフトウェアを問わず、選定には第三者評価と併せて、同業他社や他の大企業の利用状況を一つの指標として判断するという意見がありました。企業間のつながりで得られる情報も一つの参考指標になると考えられます。

3.5 ハードウェア管理

取り組み事例

- 資産管理を徹底し、ファームウェアの迅速なアップデートが可能な体制を整備する。
- 脅威シナリオベースのセキュリティテストを行う。
- 海外からの調達など法域をまたがる場合は、調達先企業のセキュリティの観点を含めた健全性を確認し、また、制裁を含む最新の法規制への対応を確認し、徹底する。

提言

＜資産管理＞

管理の行き届いた大手組織でも、個々のデバイスまでの徹底した資産管理には苦労しているとの意見が聞かれます。日常的に資産管理を徹底し、ファームウェアの迅速なアップデートが可能な体制を整備することが求められます。ソフトウェアの資産管理と同様、管理ソフトウェアなどを導入し、可視性や効率性を高め、着実な資産管理を継続することが肝要です。

＜テスト＞

重要な機器に関しては、一般的な受け入れテストと併せて、ハードウェアの脅威シナリオに応じたセキュリティテストの実施を推奨します。

＜規制の順守＞

海外からの調達は、調達元が準拠しているセキュリティ規制やセキュリティに関する信頼性を確認することと併せて、輸入に関する規制の遵守が必要です。社会状況に応じた法規制などの最新動向を把握することが求められます。

3.6 経営層への報告

取り組み事例

- 委託先などの統制や管理におけるサプライチェーンのサイバーセキュリティリスクを理解する経営層が増加してはいるものの、ビジネスへの影響、収益、顧客満足度、ビジネスの評判、顧客ロイヤリティへの影響といったトータルコストを、ビジネス用語で整理して報告する。
- サイバーセキュリティリスクを経営層へ報告する経路は組織により最適解が異なるため、リスクベース、金額ベース、ITベースなど、各組織に適した経路を検討する。その際、CIOとCISOの利益相反が生じない工夫をする。

提言

＜報告の際の工夫＞

欧米では、経営層がテクニカルなトレーニングを受け、サプライチェーンサイバーリスクを含むサイバーセキュリティ全般に明るいボードメンバーが増えてきている流れはあるものの、引き続き簡潔、明瞭かつ非技術的にビジネス用語で整理して報告することを推奨します。

＜報告経路＞

サプライチェーンを含め、サイバーセキュリティリスクを経営層へ報告する経路は、CISOからCROを経由する、CISOからCIOを経由する、CISOからCOOを経由するなど、組織によりさまざまなパターンを試行しているといった意見があり、最適経路を模索している現状が把握できました。ITの推進とセキュリティ確保に利益相反が生じず、各組織の運営に最適な報告経路を検討することを推奨します。

3.7 契約における留意事項

発注元の企業が委託先企業にサイバーセキュリティ対策の実施を要請するにあたって、その方法や内容によっては、独占禁止法や下請法上の問題となる可能性があります。公正取引委員会は2022年10月、「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて[14]」において、取引先への対策の支援・要請についての考え方を3点にまとめて提示しています。各点に対する当社の推奨事項を紹介します。

取引の対価の一方的決定

委託先企業に対し、妥当なコスト上昇分を考慮することなくサイバーセキュリティ対策の要請を行うと、独占禁止法上問題となる可能性があります。

推奨事項
一例として、契約締結後に新たに確認された脅威や脆弱性などの影響により、追加のセキュリティ要求を実施するにもかかわらず、追加の費用が支払われない場合は問題になると考えられます。セキュリティに関する要求を半期や四半期で見直せるように取り決めておくことや、緊急時に対応可能な工数をあらかじめ包括した契約にするなど、新たな脅威が顕在化した場合でも柔軟に対応できる実現可能な体制を確保した契約を推奨します。

セキュリティ対策費の負担の要請

委託先企業に対し、セキュリティ対策費などの負担を算出根拠なく要請して不利益を与える場合には、独占禁止法上問題となります。また、下請法の規制対象となる取引において、親事業者が下請事業者に対し、金銭、役務などを提供させることによって取引先の利益を不当に害する場合には、下請法上の「不当な経済上の利益の提供要請」として問題となります。

推奨事項
委託先との契約にサイバーインシデントが発生した際の支援内容を不明瞭に記載し、インシデント発生時に過度な支援を依頼することは下請法の問題になる可能性があります。支援内容は契約上で明確にすることが重要であり、例えば、関連する問い合わせをした際には何時間以内に回答を行う、またエンジニアによる緊急サポートの提供可能な時間数など、実施可能なサービスを明文化して、双方で認識を合わせたうえで契約を締結することを推奨します。

購入・利用強制

委託先企業に対し、サイバーセキュリティ対策の実施の要請に自己の指定する商品の購入や役務の利用を強制する場合には、独占禁止法上問題となる可能性があります。また、下請法の規制対象となる取引において、親事業者が下請事業者に対し自己の指定する物の購入や役務の提供を強制する場合には、下請法上の「購入・利用強制」として問題となります。

推奨事項
特定のセキュリティ要求を取引先に課す場合は、その範囲と要求事項を明確化し、双方が合意し必要なコストが支払われることで実現可能となります。昨今では、取引先の業務従事者へ自社のデバイス貸与や、仮想デスクトップサービスのアカウントを発行するなど、リモートでも自社のセキュリティ要求が担保される環境を提供することが一般的に行われています。また、自社のセキュリティ要件を満たした環境に他社からアクセス可能な領域を用意し、そこへのアクセス権を割り当てて作業を実施する例もあります。

以上のように、金融機関と委託先との関係は、事前に検討されたセキュリティ要求事項だけでなく、社会情勢に応じた追加の要求やインシデントへの対応など、柔軟な対策を重ねられる形態であることが理想です。組織のセキュリティに関する予算も、それに対応可能な形での準備が求められます。双方のセキュリティ担当者、関係者、およびその意思決定層とコミュニケーションを定期的に行い、課題を理解しあえる関係を構築しておくことが推奨されます。

14：https://www.jftc.go.jp/dk/guideline/unyoukijun/cyber_security.html

4 おわりに

本調査では、金融機関のサプライチェーンリスク管理の強化に向けて、海外の金融機関のサイバーセキュリティ専門家へのインタビューにて先進的な事例を調査し、国内の金融機関において取り入れられる要素を検討しました。

1章では、サプライチェーンにおいて想定されるサイバーリスクを整理し、また本調査で対象とするスコープを示しました。

2章では、G7や欧州、米国、英国、シンガポールで金融機関向けに発行されているサプライチェーンのサイバーセキュリティリスクに関連する規制やガイドラインを紹介しました。

3章では、海外の金融機関のサイバーセキュリティ専門家へのインタビューにて得られた先進的な取り組み事例を整理し、国内の金融機関で取り入れられる要素を提言としてまとめました。また、公正取引委員会が公示した文書をもとに、金融機関が委託先企業と契約する際に法的に問題となりうる点について推奨事項を示しました。

攻撃者がサプライチェーンを悪用する攻撃は継続して確認されており、サプライチェーンにおけるサイバーセキュリティ向上のための取り組みは、各国・地域、また各組織において進められています。今後も公的なガイドラインの更新や発行、各社の取り組みの進展が予想されるため、金融機関は脅威動向の把握と併せて、他の組織と協力しながら継続して有効な対策を採用していくことが肝要です。

執筆者情報

丸山 満彦

Mitsuhiko Maruyama

パートナー、PwCコンサルティング合同会社

上杉 謙二

Kenji Uesugi

ディレクター、PwCコンサルティング合同会社

小林 由昌

Yoshimasa Kobayashi

ディレクター、PwCあらた有限責任監査法人

マハッレ アンジャリ

Anjali Mahalle

シニアアソシエイト、PwCコンサルティング合同会社

染谷 方子

Masako Someya

シニアアソシエイト、PwCコンサルティング合同会社

北野 雄大

Yudai Kitano

アソシエイト、PwCコンサルティング合同会社

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwCあらた有限責任監査法人、PwC京都監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約9,400人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界152カ国に及ぶグローバルネットワークに328,000人以上のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。

発刊年月：2023年5月　　管理番号：I202304-08