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

令和６年 10 月４日

金融庁

目　次

1. 基本的考え方

1.1. サイバーセキュリティに係る基本的考え方

金融庁設置法第３条において、金融機能の安定の確保や預金者の保護等が金融庁の任務とされている。サイバー攻撃の脅威は、金融サービス利用者の利益を害し、金融システムの安定に影響を及ぼしかねないものとなっているため、金融庁がその任務を全うする上で、金融セクター全体のサイバーセキュリティを強化することは不可欠である。また、金融機関等[1]は、各業法において、業務の健全かつ適切な運営等を確保しなければならないこととされており[2]、業務の健全性及び適切性の観点から、サイバーセキュリティの確保が重要である。

こうした下、金融庁では、「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（改定版を含む）に記載しているとおり、金融業界との対話・協働を通じ、連携して金融セクター全体のサイバーセキュリティの強化を促してきた。また、金融庁は、各業法に基づく金融機関等のサイバーセキュリティ管理態勢に関する監督の中で留意すべき点を各監督指針・事務ガイドライン（監督指針等）において定めており、その規定に基づく検査・モニタリング等において、個別金融機関等との対話を行うとともに、検査・モニタリング等の結果を一般化して業界全体に還元することにより、金融セクター全体のサイバーセキュリティの強化を促進してきた。

今般、これまでの検査・モニタリングの結果及び金融セクター内外の状況の変化を踏まえ、監督指針等とは別に、更に詳細な本ガイドラインを策定した。まず、本節において、金融機関等に求められるサイバーセキュリティに関する基本的な考え方、情報共有機関及び業界中央機関の役割並びに本ガイドラインの位置付け及び監督上の対応について記載した後、第 2 節において、サイバーセキュリティの観点から見たガバナンス、特定、防御、検知、対応、復旧、サードパーティリスク管理に関する着眼点について規定し、それぞれについて金融機関等において「基本的な対応事項」及び「対応が望ましい事項」を明確化している（注）。第 3 節では、当庁の関係者・関係機関との連携に関する基本的な考え方について述べている。

（注）「基本的な対応事項」は、いわゆるサイバーハイジーン[3]と呼ばれる事項その他の金融機関等が一般的に実施する必要のある基礎的な事項を指す。「対応が望ましい事項」は、金融機関等の規模・特性等を踏まえると、インシデント発生時

[1] 本ガイドラインにおける金融機関等の定義は、第 1.4 節を参照のこと。
[2] 銀行法第 12 条の２第２項、金融商品取引法第 35 条の３、保険業法第 100 条の２の１第１項等
[3] IT 資産の適切な管理、セキュリティパッチ適用などの基本的な行動を組織全体に浸透させる取組みを指す。

に、地域社会・経済等に大きな影響を及ぼしうる先において実践することが望ましいと考えられる取組みや、他国の当局又は金融機関等との対話等によって把握した先進的な取組み等の大手金融機関及び主要な清算・振替機関等が参照すべき優良事例を指す。金融機関等の規模・特性は様々であることから、「基本的な対応事項」及び「対応が望ましい事項」のいずれについても、一律の対応を求めるものではなく、金融機関等が、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずること（いわゆる「リスクベース・アプローチ」を採ること）が求められることに留意が必要である。

金融庁としては、引き続き、金融機関等の規模・特性に応じ、リスクベース・アプローチで検査・モニタリングを実施し、その中で個別金融機関等のサイバーセキュリティ管理態勢を検証していく。モニタリングに当たっては、本ガイドラインへの対応については、金融機関等において、自らが直面するリスクを評価し、重要性・緊急性に応じて優先順位をつけた上、リソース制約を踏まえ、その低減措置に取り組むべきであることに留意する。同時に、検査・モニタリング等の結果把握した事例（金融機関等に共通する課題や好事例など）を、業界団体等を通じて広く金融機関等に還元することにより、金融セクター全体のサイバーセキュリティの強化を促進していく。

1.2. 金融機関等に求められる取組み

1.2.1. サイバーセキュリティ管理態勢

我が国におけるサイバーセキュリティの確保については、サイバーセキュリティ基本法において、関連施策の基本となる事項が定められており、その施策の推進は、国、重要社会基盤事業者等の多様な主体の連携により、積極的に対応すべきことが基本理念の一つとして定められている。また、銀行等、生命保険、損害保険、証券及び資金決済分野の事業者は、サイバーセキュリティ基本法上の重要社会基盤事業者（重要インフラ事業者）に指定されている。同法において、重要インフラ事業者は、その責務として、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めることとされている。

加えて、重要インフラ事業者以外の者も含め、金融機関等は、銀行法、保険業法、金融商品取引法等の各業法に基づき、業務の健全かつ適切な運営等を確保しなければならないこととされており、サイバーセキュリティの確保もこれに含まれる。

金融機関等がグループ（海外拠点等を含む）を形成している場合には、第２節に掲げるサイバーセキュリティ管理態勢に係る事項について、傘下グループ会社及び拠点の規模・特性による違いを踏まえ、グループとして整合性のある態勢を整備することにより、グループ全体のサイバーセキュリティを確保することが求められる。

また、変化し続ける脅威に対応する上では、組織的・技術的な対応態勢を不断に機動的に見直す必要がある。このためには、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求められるとともに、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がある。また、サイバーセキュリティは、サイバーセキュリティ担当部署やIT担当部署だけでは確保できないため、経営陣をはじめとして、組織全体で態勢構築と運営を行う必要がある。

こうした状況の下、金融機関等には、本ガイドラインを形式的に遵守することのみを重視したリスク管理態勢とならないように留意し、関係法令、監督指針等及び本ガイドライン等の趣旨を踏まえ、実質的かつ効果的な対応を行うことが求められている。その際、本ガイドライン以外にも、関連するガイドライン[4]を参照されたい。

1.2.2. 経営陣の関与・理解

サイバーインシデント[5]による業務の中断は、顧客に大きな影響を与え、金融機関等ひいては金融システムの信頼に大きな影響を与えかねない重大なリスクである。こうしたリスクの性質に鑑みれば、サイバーセキュリティは、IT・システム部門の問題に止まらないことは明らかであり、経営責任が問われかねない問題である。また、サイバーインシデント発生時に、顧客、金融システムへの影響を最小化し、極力早期の復旧を目指すためには、各業務所管部、企画、広報、コンプライアンス、リスク管理、監査などの各部門間の連携が不可欠であるし、また、現場担当者に止まらず、経営陣の主体的な関与が求められる。さらに、顧客、法執行機関、情報共有機関、当局等との連携も求められる。こうした組織全体としての対応を実現するためのガバナンスの確立が必要であり、そのためには経営陣のリーダーシップが不可欠である。

取締役等の役員は、民法、会社法その他各業法等の規定に基づく責務を負うため、自

[4] （参考）参考資料として、「重要インフラのサイバーセキュリティに係る行動計画」及び「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（サイバーセキュリティ戦略本部決定）、「金融機関等コンピュータシステムの安全対策基準・解説書」（公益財団法人金融情報システムセンター編）、米国国立標準技術研究所（NIST）による Cybersecurity Framework、米国 The Cyber Risk Institute（CRI）による The Profile などがある。

[5] 監督指針等における「サイバーセキュリティ事案」と同義とする。

組織の規模、特性又はサイバーセキュリティリスクに鑑みてサイバーセキュリティ管理態勢が不十分なことに起因して自組織や第三者に損害が生じた場合、善管注意義務違反や任務懈怠による損害賠償責任を問われ得る。

1.3. 業界団体や中央機関等の役割

サイバー空間における脅威情報や、最新の攻撃手法の動向の把握等について、個別金融機関等による対応のみでは必ずしも効率的・効果的ではない場合がある。特に、規模が小さい又は取引範囲が限定的な金融機関等においては、十分な情報や対応のノウハウの蓄積が困難なことも考えられる。

我が国金融セクター全体の底上げの観点からは、業界団体や中央機関等が、必要に応じて当局と連携しながら、金融機関等にとって参考とすべき情報や対応事例の共有、態勢構築に関する支援その他業態全体のサイバーセキュリティ強化のための活動（演習、シナリオ分析[6]、人材育成など）等の共助の取組みを推進することにより、金融機関等による対応の向上に中心的・指導的な役割を果たすことが望ましい。

そのため、金融機関等は、共助機関である金融 ISAC[7]等が支援している、技術的な課題への対応、ベストプラクティスの共有、最新のサイバー攻撃の動向や脆弱性情報の分析などの知見を、必要に応じ、積極的に活用することが望ましい。また、金融業界以外の業界等とも連携することが望ましい。

例えば、多くの協同組織金融機関においては、基幹システムの構築・運用等を共同センターに委託したり、業界内のネットワークシステムや他業態システムと接続するネットワークシステムの構築・運用等を各業態の中央機関と業態センターに委託（又は同センターを共同利用）したりしている。また、インターネット環境等のネットワーク、ホームページ又はインターネットバンキングなども、同様に、業態センターが提供するサービスを共同利用している場合がある。したがって、サイバー攻撃によるシステム障害時の対応を勘案すれば、サイバーセキュリティ対策における業界団体や中央機関等の果たす役割は大きい。このため、各協同組織金融機関においては、個別の金融機関に対して経営支援機能を有する中央機関等による業務補完・支援を活用し、また、中央機関等はサイバーセキュリティに関する業務補完・支援の集約及び充実を図ることを通じ、業態内の相互扶助の充実を図ることが望ましい。

---

[6] リスク評価やテスト、演習等に用いるサイバー攻撃や影響の波及経路等に関するシナリオの分析を指す。

[7] 我が国の金融機関によるサイバーセキュリティに関する情報の共有及び分析を行い、金融システムの安全性の向上を推進することにより、利用者の安心・安全を継続的に確保することを目的として設立（2014年８月）された一般社団法人。ISAC は Information Sharing and Analysis Center の略。

また、清算・振替機関等においては、安定的に業務を提供するため、参加者等がこれらの機関にもたらすリスクを管理することが求められる。この観点から、清算・振替機関等においては、リスクの状況に応じて、参加者等に対し、リスクに関連する合理的な参加要件等において、本ガイドラインを参考にすることが考えられる。

1.4. 本ガイドラインの適用対象等

本ガイドラインは、サイバーセキュリティ管理について監督指針等に定めのある、主要行等、中小・地域金融機関、保険会社、少額短期保険業者、金融商品取引業者等、信用格付業者、貸金業者、前払式支払手段発行者、電子債権記録機関、指定信用情報機関、資金移動業者、清算・振替機関等、金融サービス仲介業者、為替取引分析業者、暗号資産交換業者、銀行代理業、電子決済手段等取引業者、電子決済等取扱業者、電子決済等代行業者、農漁協系統金融機関のほか、金融商品取引所（本ガイドラインにおいて「金融機関等」）を対象とする。

本ガイドラインにおける用語の定義は、特に定めがない限り、業態ごとの監督指針等の定義に従うこととする。

（注）サイバーセキュリティ管理に関する監督指針等の規定は、監督指針等の中で、システムリスク管理に関する規定の一部を構成している。本ガイドラインの理解にあたっては、必要に応じ、システムリスク管理に関する監督指針等の記載も参照すべきである。

2. サイバーセキュリティ管理態勢

2.1. サイバーセキュリティ管理態勢の構築

2.1.1. 基本方針、規程類の策定等

【基本的な対応事項】

① 取締役会等は、サイバーセキュリティリスクを組織全体のリスク管理の一部としてとらえ、サイバーセキュリティ管理の基本方針を策定すること。サイバーセキュリティ管理の基本方針には、例えば、以下の事項を記載すること。
- セキュリティ対策の目的や方向性

・ 関係主体等（顧客、地域社会、株主、当局等）からの要求事項への対応及び法規制等への対応
・ 経営陣によるコミットメント

② 取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、組織の経営目標にとってのサイバーセキュリティの確保の重要性を認識し、関係主体等からの要求事項や、法規制等の内外環境を踏まえ、必要なサイバーセキュリティ管理態勢を整備すること。また、サイバーセキュリティ管理態勢について少なくとも１年に１回レビューを行うなどにより、十分な検証、議論を行うこと[8]（必要に応じ、外部専門家によるレビューを含む）。

③ 経営陣は、サイバーセキュリティについて、組織体制の整備のほか、以下のようなサイバーセキュリティ管理態勢の整備を行うこと。
・ 情報共有機関等を通じた早期警戒のための情報収集・共有・分析体制
・ SOC[9]等のサイバー攻撃に対する監視体制（外部のリソースの活用を含む）
・ サイバー攻撃を想定した危機管理態勢（サイバー攻撃を受けた際の報告及び広報体制、組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制を含む） 等

④ 経営陣は、サイバーセキュリティ管理の基本方針に基づいて、サイバーセキュリティに係る戦略、取組計画[10]（含む複数年計画）を策定し、当該取組計画の実効性及び十分性を確保すること。また、年次及び重要な変更が生じた時点で、必要な見直しを行うこと。

⑤ 経営陣は、金融商品・サービスを導入する場合や、デジタルトランスフォーメーションを推進する場合には、セキュリティ・バイ・デザイン[11]を含むサイバーセキュリティ確保に向けた取組みも同時に推進すること。

⑥ 経営陣は、サイバーセキュリティを経営方針における重要課題の一つとして位置づけ、自らリーダーシップを発揮して、サイバーセキュリティ確保に向けた組織風土を醸成するとともに、自組織の重要な業務[12]やリスクを把握した上で、それに応じた対策を推進すること（対策の進捗状況の管理や追加対策の指示、必要なリソースの配分など）。

---

[8] 必要に応じて、日本経済団体連合会が公表している「サイバーリスクハンドブック（取締役向けハンドブック）」も参照されたい。

[9] SOC（Security Operation Center）とは、ネットワークやサーバ等の各デバイスを監視し、サイバー攻撃の検出や分析等を行う組織。

[10] 取組計画は、具体的な施策、スケジュール、実施体制等を含むものであり、例えば以下のような施策を記載することが考えられる。
・リスク評価の結果を踏まえ、具体的に作成したリスク対応
・人材育成
・インシデント対応（演習・訓練の実施等）
・サードパーティリスク管理の強化

[11] 金融商品・サービスの企画・設計段階から、セキュリティ要件を組み込む考え方。

[12] 本ガイドラインにおいて「重要な業務」とは、その中断が金融機関等の業務又は利用者もしくは金融システムに著しい悪影響を生じさせるおそれのある金融サービスをいう。

⑦ 経営陣は、サイバーセキュリティ担当部署及び各関係者の役割と責任及び権限を明確化すること。職員の急な退職・異動等により業務の継続（知見の集積等）に支障が生ずることのない人員の配置をすること。サイバーセキュリティを統括管理する責任者（CISO 等）を経営陣の責任において任命すること。

⑧ 経営陣は、少なくとも１年に１回、以下の報告を担当部署等に求めること。

- 自組織を取り巻くサイバーセキュリティリスクの状況（自組織におけるサイバーインシデント発生状況、国内外・業界におけるサイバーインシデント発生状況、重大な脆弱性情報、等）
- サイバーセキュリティに関するリスク評価の結果（必要に応じ、外部専門家による評価を含む）
- 取組計画の進捗状況

⑨ 経営陣は、サイバーセキュリティに関する監査の結果や、関係主体等（顧客、地域社会、株主、当局等）からの要求事項や、法規制等の内外環境を踏まえ、サイバーセキュリティ管理態勢の継続的改善を行うこと。

【対応が望ましい事項】

a. 経営陣が適切な経営判断を行うための前提として重要なサイバーセキュリティに係るガバナンスの確保のため、サイバーセキュリティに関する十分な知識を利用（外部専門家の利用を含む）できるようにしておくこと。これには、一般的な３線防衛態勢（業務部門、リスク管理部門及び内部監査部門）の下、サイバーセキュリティに関する各部門の役割分担の明確化[13]や外部専門家を利用した検証の仕組みを構築することを含む。

b. 取締役会等は、サイバーセキュリティリスクを統合的リスク管理の一部として位置づけ、リスク選好度（リスクアペタイト）[14]、リスク耐性度（リスクトレランス）[15]を設定すること。

（参考）金融庁「オペレーショナル・レジリエンス確保に向けた基本的な考え方」（令和５年４月）

c. 経営陣は、可能な範囲で、自組織のサイバーセキュリティに関する取組みの意義を内外の関係者に表明するために、攻撃者の攻撃を助長する可能性を考慮の上、その内容を対外公表すること。公表内容は、例えば、以下の事項が考えられる。

---

[13] 2.1.4 節、2.1.5 節を参照のこと。

[14] リスク選好度（リスクアペタイト）とは、自社の戦略目標や事業計画を実現するために、リスクキャパシティ（組織が許容できる最大のリスク量）の範囲内において、進んで受け入れるリスクの種類と総量をいう。

[15] リスク耐性度（リスクトレランス）とは、リスク選好度（リスクアペタイト）を設定した上で、重要な業務と特定した金融サービスについて、未然防止策を尽くしてもなお、業務中断が必ず生じることを前提に最低限維持すべき水準をいう。

- サイバーセキュリティ管理の基本方針
- 維持するサービス範囲・水準
- リスク管理体制
- サイバーセキュリティに関する責任者の知見
- 資源の確保
- リスクの把握と対応計画策定
- 緊急対応体制・復旧体制
- インシデントの発生状況

d. 経営陣は、少なくとも１年に２回、以下の報告を担当部署等に求めること。
   - サイバーセキュリティにかかるパフォーマンス指標（KPI）[16]及びリスク指標（KRI）[17]

e. 経営陣は、自組織におけるサイバーセキュリティを統括管理する責任者（CISO 等）としてサイバーセキュリティに関する十分な知識・経験を有し、かつ、経営陣に日常的に直接レポートできる立場の者を配置し、平時及び有事に、経営トップと直接コミュニケーションする関係を構築すること。そのため、経営陣は、CISO がその役割を果たすに足るサポート、権限及び資源を提供すること。また、業務部門にも、サイバーセキュリティに関する十分な知識・経験を有し、CISO と業務部門との連携を円滑にする役割を持つ責任者を配置すること。

2.1.2. 規程等及び業務プロセスの整備

【基本的な対応事項】

① 経営陣は、サイバーセキュリティに係る規程及び業務プロセスを整備し、少なくとも１年に１回見直しを行うこと。サイバーセキュリティに係る規程等には、例えば以下の事項を含めること。
   - 情報資産管理
   - リスク評価
   - 脆弱性管理
   - 脆弱性診断及びペネトレーションテスト（侵入テスト）
   - 演習・訓練
   - 認証・アクセス管理
   - 教育・研修
   - データ管理
   - ログ管理

[16] KPI の例：標的型メール訓練の報告率、脆弱性対応率、情報資産棚卸進捗率、トレーニング受講率等。
[17] KRI の例：サイバー攻撃試行件数、監査指摘件数、インシデント件数、未対応の脆弱性件数等。

・ セキュリティ・バイ・デザイン
・ 技術的対策（物理的セキュリティ、ネットワークセキュリティ等）
・ インシデント対応及び復旧
・ サードパーティリスク管理

② 経営陣は、サードパーティ[18]からもたらされるリスクも含め、サイバーセキュリティリスクにかかる、組織横断的な報告・連絡・協議ルートや指揮命令系統を整備すること。

2.1.3. 経営資源の確保、人材の育成

【基本的な対応事項】

① 経営陣は、サイバーセキュリティの重要性を踏まえた上で、サイバーセキュリティ担当部署等に、専門性を有する人材を配置し、また、必要な予算を配分するなどにより、適切な資源配分を行うこと。
② 経営陣は、サイバーセキュリティ管理の基本方針と整合的な人材の育成・確保のための計画（人材育成計画、採用計画及び教育研修・訓練計画など）を策定すること。定年や退職者の代替人員の育成などの観点を含む、持続可能な人事政策を敷くこと。資質・意欲のある職員に対し、人材育成を阻害するような人事異動を避け、人材育成の観点から中長期的かつ計画的に人事配置を行い、内外の教育の機会を提供するなどにより、外部からの採用や外部人材の活用だけではなく、内部人材の育成も考慮すること。
③ サイバーセキュリティにかかる経営陣によるガバナンスやサイバーセキュリティ確保に向けた組織風土の醸成に資するスキルやノウハウの修得に向けて、経営陣は積極的に研修・訓練等に参加すること。担当部門や外部組織が実施する、経営陣を対象とした啓発活動や研修・訓練などを活用することも考えられる。
④ 人材の育成については、例えば、以下のような人材を外部人材の活用も含めて計画的に確保していくこと。
・ 新たなデジタル技術の導入に際し、生じ得るサイバーセキュリティに関するリスク評価を行う人材
・ サイバーセキュリティ戦略・計画の企画・立案を行う人材
・ サイバーセキュリティに関する研修や人材育成を行う人材

[18] サードパーティとは、自組織がサービスを提供するために、業務上の関係や契約等を有する他の組織をいう（例：システム子会社やベンダー等の外部委託先、クラウド等のサービス提供事業者、資金移動業者等の業務提携先、API 連携先）。外部委託先とは、業務を委託している組織をいう（金融機関等が金融サービスを提供するために外部委託するシステム（共同センター等を含む）のベンダーなど。形式上、外部委託契約が結ばれていなくともその実態において外部委託と同視しうる場合や当該外部委託された業務等が海外で行われる場合も含む）。

- サイバーセキュリティの観点からシステムの設計・開発を行う人材
- サイバーセキュリティ脅威、脆弱性に関する情報収集やシステムへの脆弱性対応を行う人材
- ログの監視・モニタリングを行う人材
- サイバーインシデント発生時に対応を行う人材
- フォレンジック調査[19]等を行う人材
- 脆弱性診断やペネトレーションテストを行う人材
- サイバーセキュリティ監査を行う人材

2.1.4. リスク管理部門による牽制

【基本的な対応事項】

① リスク管理部門は、サイバーセキュリティ管理態勢が有効に機能しているかについて、業務部門等から独立した立場から監視・牽制を行うこと。
② リスク管理部門は、サイバーセキュリティ管理の実施状況について、リスク管理担当役員（CRO 等）及び取締役会等に報告すること。

【対応が望ましい事項】

a. リスク管理部門にサイバーセキュリティに係る適切な知識及び専門性等を有する職員を配置すること。

2.1.5. 内部監査

【基本的な対応事項】

① 内部監査部門は、必要に応じて外部専門家を利用しつつ、独立した立場から、リスクベース・アプローチに基づき、サイバーセキュリティに係る内部監査計画を策定し、サイバーセキュリティ（整備状況・運用状況、対応・復旧、法規制の遵守状況、サードパーティリスク管理を含む）をテーマとする内部監査を実施すること。
② 内部監査部門は、内部監査で指摘した重要な事項について遅滞なく代表取締役及び取締役会等に報告するとともに、指摘事項の改善状況を的確に把握すること。

[19] 電子機器や電子記録媒体内にある電子データを分析して、不正行為等の証拠を見つけ出す手法を利用した調査を指す。

【対応が望ましい事項】

a. 内部監査部門にサイバーセキュリティに係る適切な知識及び専門性等を有する職員を配置すること。

2.2. サイバーセキュリティリスクの特定

2.2.1. 情報資産[20]管理

【基本的な対応事項】

① 情報資産をライフサイクル（取得・使用・保管・廃棄）に応じて管理する手続等を策定し、必要に応じて見直すこと。
② 情報資産は、その重要度（機密性、完全性、可用性）に応じて保護の優先度を分類し、管理すること。

なお、情報資産管理については、業態ごとの監督指針等における「情報セキュリティ管理」の項目[21]も参照すること。

2.2.1.1. 情報システム及び外部システムサービス

【基本的な対応事項】

① 情報システム及び外部システムサービスを適切に管理するための台帳等を整備し、メンテナンス手順を定めるなど、最新の状態を網羅的に把握できるようにすること。各部門が所管する情報システムも含むこと。当該台帳等は、2.2.1.2 節及び 2.2.1.3 節に規定する台帳等と相互参照可能にすること。

[20] 情報資産とは、①情報システム及び外部システムサービス（外部委託先、クラウドサービス）、②その構成要素であるハードウェア・ソフトウェア等及び保管される情報（データ）並びに③ネットワークを指す。
[21] 例えば、主要行等向けの総合的な監督指針については、Ⅲ－３－７－１－２－（４）情報セキュリティ管理。

2.2.1.2. ハードウェア・ソフトウェア等

【基本的な対応事項】

① ハードウェア（ネットワーク機器やアプライアンス製品[22]を含む）及びソフトウェア（仮想マシンを含む）等（管理を外部委託している自組織の資産を含む）を適切に管理するための手続・台帳等を整備し、メンテナンス手順を定めるなど、最新の状態を網羅的に把握できるようにすること。台帳等には、以下の項目を含めること。
- サポート期間（サポート終了予定日、サポート期間延長の可否）
- ソフトウェアの場合、バージョン情報

【対応が望ましい事項】

a. 複合機・特定用途機器[23]を台帳等による管理対象とすること。
b. 必要に応じて、サードパーティの資産についても管理対象とすること[24]。
c. ハードウェア及びソフトウェア等に係る情報資産の分類に当たっては、重要な業務のサードパーティへの依存関係を考慮したリスク管理が実施できるようにすること。
d. 管理対象外となっている個人所有端末等の情報資産や未承認のクラウドサービスの利用（シャドーIT 等）を特定し、管理対象とするか使用を中止するなど、適切に対応すること。
e. 以下に掲げるものに関するソフトウェア部品表[25]（SBOM、Software Bill of Materials）を整備すること。
- 自社開発のソフトウェア
- 利用しているサービス（当該サービス事業者が SBOM を提供している場合）

[22] 専用のソフトウェアが機器に固定的に組み込まれたものであり、特定の用途に特化した製品。
[23] 「政府機関等のサイバーセキュリティ対策のための統一基準群」における定義に従い、テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている、又は内蔵電磁的記録媒体を備えているものをいう。
[24] 対象とするサードパーティは、リスクベースで検討することが必要であることに留意が必要である（2.6 節参照）。
[25] ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リストのこと。

2.2.1.3. 情報（データ）

【基本的な対応事項】

① 顧客情報や機密情報等を適切に管理するための台帳等を整備し、メンテナンス手順を定めるなど、最新の状態を網羅的に把握できるようにすること。

2.2.1.4. データフロー図・ネットワーク図

【基本的な対応事項】

① 全体を俯瞰してデータフロー及びネットワークを適切に管理するため、データフロー図・ネットワーク図を作成し、メンテナンス手順を定めるなどにより、最新の状態を把握できるようにすること（モバイル接続、外部接続、ネットワークに接続するサードパーティ及び内部システムを含む）。

2.2.2. リスク管理プロセス

2.2.2.1. 脅威情報及び脆弱性情報の収集・分析

【基本的な対応事項】

① 自組織の脅威情報（自組織におけるサイバーインシデント等）のほか、公的機関や情報共有機関、サードパーティから、サイバー攻撃（過失や内部不正によるものを含む）の脅威情報（他組織の事例を含む）及び脆弱性情報（演習・訓練等で判明した脆弱性を含む）を収集すること。
② 収集した情報を整理・分析し、これらによるサイバーセキュリティリスクが自組織の事業・情報資産に与える影響を評価すること。
③ 情報の収集元及び収集・分析の方法を少なくとも１年に１回は見直し、必要に応じて改善を図ること。

【対応が望ましい事項】

a. 自組織の業務に即して、金融 ISAC 等の専門性の高い情報共有活動や、業界横断的な団体、国際的な団体等に積極的に参画し、脅威情報や脆弱性情報等を収集し共有すること。
b. 脅威分析を行う際に、過去に発生したことがない場合でも、深刻だが現実に起こ

りうるサイバー攻撃の脅威を対象に含めること。

c. 新技術（AI、量子コンピュータ等）、地政学的動向、偽情報、業界動向などの組織を取り巻く状況に留意し情報収集を行うこと。

2.2.2.2. リスクの特定・評価

【基本的な対応事項】

① サイバーセキュリティリスクの特定・評価に係る手順を定めること。
② 脅威情報及び脆弱性情報を踏まえたサイバー攻撃の発生可能性、並びにサイバー攻撃が発生した場合の自組織の事業や情報資産に与える影響に基づき、サイバーセキュリティリスクを少なくとも１年に１回評価すること。また、重大な脅威や脆弱性が判明した時や、新規商品又はサービスの提供時にも評価すること。
③ リスク評価に当たっては、境界防御型セキュリティが突破されるリスクや内部不正などの脅威も考慮し、内部ネットワークセグメントに設置したシステムへのリスクも対象とすること。

【対応が望ましい事項】

a. リスク評価に当たっては、重要な業務を特定し、重要な業務を継続するために必要な組織内の人員、設備、システム、サードパーティの相互依存度を考慮すること。
b. リスク評価に当たっては、シナリオ分析、机上演習又はストレステスト等を通じて、組織における脆弱性を特定し、重要なシステム及び業務に対する潜在的な影響を考慮すること。シナリオについては、深刻だが現実に起こりうる多様なシナリオを考慮すること。

2.2.2.3. リスク対応

【基本的な対応事項】

① リスク評価の結果に基づき優先順位付けを行い、リスク対応計画（リスク回避、リスク軽減、リスク受容、リスク移転）を策定すること。
② リスク対応における例外的な取扱いやリスク受容などの取扱いに関する手続を定めること。また、当該手続きによる対応に際しては、経営陣等の承認を得ること。
③ リスク対応計画（残存リスクの評価を含む）は、定期的に経営陣に報告すること

（あるいは、取締役会等が設定するリスク選好度の範囲内であることを確認すること）。

2.2.2.4. 継続的な改善活動

【基本的な対応事項】

① 内外の環境変化に応じてサイバーセキュリティに関するリスク評価のプロセスを少なくとも１年に１回は評価するとともに、継続的な改善活動を実施すること。
② サイバーセキュリティリスク管理態勢の整備状況及び運用状況の有効性を少なくとも１年に１回は評価し、改善すること。
③ 演習・訓練、脆弱性診断及びペネトレーションテスト、監査、リスク評価、及び実際のインシデントから得られた推奨事項、発見事項、教訓については、関連手続等に従って改善すること。

【対応が望ましい事項】

a. 脅威環境の変化、技術の進歩、得られた教訓に応じて、監視・検知に係る関連手続を少なくとも１年に１回は評価し、改善すること。
b. パフォーマンス指標（KPI）及びリスク指標（KRI）を測定・評価し、経営陣に報告する仕組みを整備すること。また、具体的な目標及び達成指標を設定し、改善の状況及び課題を特定すること。

2.2.3. ハードウェア・ソフトウェア等の脆弱性管理

【基本的な対応事項】

① ハードウェア・ソフトウェア等の脆弱性管理に係る手続等を策定し、必要に応じて見直すこと。当該手続等には、以下の点を含めること。
   - 脆弱性情報の入手先及び情報を入手するためのプロセスに関すること（当該情報の入手先として、公的機関、情報共有機関及びサードパーティ等を含めること）
   - 入手した脆弱性の深刻度、影響の大きさ及び影響範囲の評価に関すること
   - 脆弱性への対応方法と対応期限の決定、及び対応状況の管理に関すること
   - 例外的な取扱いをする際の意思決定プロセスに関すること
② 入手した脆弱性情報は、ハードウェア・ソフトウェアの脆弱性管理に係る手続等に基づき、対応の要否を判断すること。

③ システムの重要度、リスク又は脆弱性の深刻度に基づいたパッチ適用等の対応期限を設定するとともに対応実績を管理すること（例えば、業務系ネットワークとインターネット系ネットワークを分離していないなどのリスクの高い構成である場合には、パッチ適用の影響調査を実施の上、迅速にまたは一定の対応期間内にパッチ適用を行うなど）。例外的にパッチ適用等の対応を実施しない場合には、実施しないことと実施しないことのリスクについて経営陣等から承認を得ること。

④ 深刻度の高い脆弱性が判明した場合、情報システム及びハードウェア・ソフトウェア等に関する台帳等に基づき、影響を受ける情報システム等を特定し、速やかに対応すること（2.2.1.1 及び 2.2.1.2 参照）。

⑤ 深刻度の高い脆弱性については、グループ会社、海外拠点が保有するシステムについても、脆弱性対応の範囲に含めること。

⑥ 深刻度の高い脆弱性については、重要なサードパーティ[26]が保有するシステム（共同利用型のシステムを含む）の脆弱性対応の管理を行うこと。なお、管理にあたっては、第三者保証による報告書（SOC2 など）や契約書等を活用することが考えられる。

【対応が望ましい事項】

a. 深刻度の高い脆弱性については、クラウド事業者を含むサードパーティ（上記⑥のサードパーティを除く）が保有するシステムの脆弱性対応の管理を行うこと。なお、管理にあたっては、第三者保証による報告書や契約書等を活用することが考えられる。

2.2.4. 脆弱性診断及びペネトレーションテスト

【基本的な対応事項】

① システムの脆弱性対策やセキュリティの問題点を特定し、改善するために、リスクの大きさやシステムの重要度等も考慮した上で脆弱性診断及びペネトレーションテストを定期的に実施すること。また、関連する手続等を策定し、必要に応じて見直すこと。手続等においては、以下の点に留意すること。

- 脆弱性診断の対象範囲（外部に直接接続している機器（VPN 機器など）を含む）、実施頻度、実施時期（システムのリリース前を含む）及び実施工程を含めること。

[26] 重要なサードパーティとは、自組織として業務運営上重要と認識しているサードパーティをいう。

- 外部公開ウェブサイト（ホームページやインターネットバンキングサイト等、外部公開 API を含む）については、脆弱性診断として、プラットフォーム診断[27]に加え、ウェブアプリケーション診断[28]も実施すること。
- モバイルアプリケーションを対象とする脆弱性診断を実施すること。
- リスクの高い構成である場合（業務系ネットワークとインターネット系ネットワークを分離していない場合等）には、外部公開サーバや内部環境のセキュリティ上の根幹となる機器（Active Directory サーバ、ファイルサーバ等）に対する脆弱性診断を実施すること。
- 特定された問題を優先順位付けし、対応方法と対応期限を決定し、対応状況を管理すること。
- 脆弱性診断及びペネトレーションテストの結果のうち、重要性のあるものについては迅速に経営陣等に報告すること。

【対応が望ましい事項】

a. 脆弱性診断及びペネトレーションテストは、インターネットに直接接続していない VPN 網、内部環境も対象とすること。
b. 定期的に脅威ベースのペネトレーションテスト（TLPT）を実施すること。実施する際には、以下の点に留意すること。
   - 必要な経験及びスキルを持つ業者を選定すること（テスターの資格や経歴の確認等のバックグラウンドチェックを含む）。
   - 脅威インテリジェンスを踏まえ、実際の攻撃者が行う水準のテクニックを用いたテストを行うこと。
   - 関係主体等に対するサービスの提供に影響を及ぼしうる、深刻だが現実に起こりうる脅威シナリオをテスト計画において考慮すること。
   - テストでは、防御側の担当者（ブルーチーム）によるインシデント対応能力の評価（防御・検知・報告・封じ込め等）を行うこと。
   - テストは、本番環境を利用し、防御側の担当者（ブルーチーム）に予告することなく、実施すること。
   - 判明した課題を経営陣に報告し、改善活動を行うこと。

   （参考）金融庁「諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書」（平成 30 年５月）、金融情報システムセンター「金融機関等における TLPT 実施にあたっての手引書」（令和元年９月）、金融庁「金融機関のシステム障害に関する分析レポート」（令和６年６月）別紙 1「コラ

[27] 推測可能なパスワードの存在や OS・ミドルウェアの設定不備等、Web アプリケーションの土台となるサーバ上に生じうる欠陥の有無を調査するもの。
[28] SQL インジェクションやクロスサイトリクエストフォージェリ等、Web アプリケーションの作りこみによって生じうる欠陥の有無を調査するもの。

ム：金融機関における脅威ベースのペネトレーションテスト（TLPT）の好事例及び課題」

c. 自組織のシステム環境を熟知する内部人材によるペネトレーションテスト（レッドチーム（TLPT における攻撃側の担当者）によるテストを含む）を実施すること。
d. ペネトレーションテストの方法及び結果を定期的にレビューし、新たな独立した視点を得るためにテストベンダーの交代要否を検討すること。

2.2.5. 演習・訓練

【基本的な対応事項】

① 組織におけるサイバーインシデント対応計画及びコンティンジェンシープランの実効性を確認し、課題を把握した上で継続的に改善するために、定期的な演習・訓練を実施すること（他組織主催の演習・訓練への参加を含む）[29]。また、必要に応じて、演習・訓練への外部委託先の参加を検討するほか、業界横断的な演習に参加すること。
② 経営陣、サイバーセキュリティを統括管理する責任者（CISO 等）及び業務部門の責任者が自らサイバー演習・訓練等に関与し、その結果を把握すること。
③ 演習・訓練のシナリオには、顧客に深刻な影響を与え、かつ現実に起こりうるシナリオを含めて検討すること。
④ 演習・訓練を通じて、業務継続等の観点でサイバーインシデント対応計画及びコンティンジェンシープランの有効性を定期的に検証し、演習・訓練で得られた課題や教訓等を踏まえ見直すこと。
⑤ 演習・訓練の手法・シナリオ等について、最新の脅威動向等に応じて見直しすること。

【対応が望ましい事項】

a. 実機等を用いた復旧訓練においては、システムやデータの復旧手順の適切性や、復旧目標（目標復旧時点（RPO）[30]、目標復旧時間（RTO）[31]）の妥当性の確認を含めること。
b. 自組織への影響が大規模かつ長期間継続するインシデントや、取引所、清算・振替機関等への接続障害等が生じるインシデントなど、金融システム全体に深刻な

[29] 清算・振替機関等については、参加者等やその他の関係先も演習・訓練の対象に含めること。
[30] 目標復旧時点（Recovery Point Objective）。
[31] 目標復旧時間（Recovery Time Objective）。

影響が波及するシナリオを用いた演習・訓練を実施すること。

c. 演習・訓練を通じて判明した課題の改善内容については、再度演習等を行い、その有効性を検証すること、又は残存リスクを許容することについて経営陣等の承認を得ること。

d. 訓練・演習等（内部のもの、ベンダーが提供するもの、業態内のもの、当局主催のものなど）について、それぞれの規模・特性を踏まえ、これらを組み合わせて実施すること。

2.3. サイバー攻撃の防御

【基本的な対応事項】

① サイバー攻撃に備え、不正侵入を防止するための境界ネットワーク対策、内部ネットワークでのシステム不正利用を防止するための対策、外部への情報漏洩対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じること。

2.3.1. 認証・アクセス管理

【基本的な対応事項】

① 認証及びアクセス権の付与に係る方針及び規程等を策定し、定期的に見直すこと。その際、以下の観点を踏まえること。
- ユーザ（システムを含む）のアクセス権限を必要最小限に制限し、職務の分離を考慮すること。
- アカウントのライフサイクル（作成、使用、終了）を管理すること及びアカウントの定期的な棚卸しや操作履歴のレビューを実施すること並びに無権限者によるアカウントの不正使用を防止すること。
- 特権アカウントの利用を厳格に制限し、管理すること（多要素認証、操作のダブルチェック、アカウントの時間制限の設定等）。
- 外部委託先によるアクセス権の利用を適切に管理すること。

② システムへのアクセス権限は、正当な業務上の要請があり、承認され、適切に教育・研修を受け、管理されている個人に対してのみ付与すること。また、ユーザによる機器及びシステムへのアクセス権限は、システムや情報の重要度を考慮して付与すること。

③ 機器（API に認証情報を組み込むことを含む）及びユーザの ID 及び認証情報を適切に管理すること（初期設定されたパスワードの変更、パスワード強度の要件、

ID の自動失効、システム責任者による定期的なアクセスレビュー等）。

④ ID を認証し、システムへのアクセスを許可する前にユーザのアクセス権限の適切性を検証すること。また、アクセスしたユーザを特定できる措置を講じ、処理内容をログに記録し、ユーザの操作内容と対応させること。

⑤ システムや情報の重要度に応じて、認証要件（多要素認証、リスクベース認証等、認証時におけるリスク低減策等）を決定すること。特に、重要なシステムへのリモートアクセスには、多要素認証を使用すること。

⑥ 第三者による不正行為を阻止するための仕組みや取組みを活用すること（メールの送信ドメイン認証（SPF/DKIM/DMARC）、安全なファイル交換機能、顧客へのサポートと啓発活動（注意喚起やセミナー）等）。

⑦ シングルサインオンや外部認証連携等、システム間又はセキュリティ境界にまたがる認証及び認可における機密性、完全性及び真正性等を確保すること。

⑧ 機密性の高い区域及びコンピュータ室、データ保管室等重要な室への物理的アクセスを管理し、保護し、記録すること。

2.3.2. 教育・研修

【基本的な対応事項】

① 経営陣を含むすべての役職員に対して、役割と責任に応じたサイバーセキュリティの意識向上に係る教育・研修を定期的に実施すること。

② サードパーティ在籍の担当者が、業務を適切に行う上で必要となるサイバーセキュリティの教育・研修を受講（必要に応じて、金融機関に関するインシデント対応及び復旧計画における役割及び運用手順に係る内容を含む）していることを確保すること[32]。なお、本対応には、サードパーティによる社内教育・研修が実施されていることを金融機関等が確認することをもって受講を確保することも含まれる。

③ 顧客に対し、必要に応じ、サイバー攻撃の脅威及びサイバーセキュリティの意識向上に資する取組み（フィッシングメールに係る注意喚起をウェブサイトに掲載すること等）を実施すること。

④ IT 又はセキュリティを所管する部門の役職員に対して、脅威及び対策の変化等、最新の知識とスキルを維持するための教育・研修を定期的に実施すること。

⑤ すべての役職員に対して、自身がインシデントの当事者となった場合に適切な対応を行うために、必要な教育・研修等の機会を確保すること。また、インシデント対応及び復旧計画における役割及び運用手順に係る教育・研修を、関係する役

[32] 対象とするサードパーティは、リスクベースで検討することが必要であることに留意が必要である（2.6 節参照）。

職員に対して、定期的に実施すること。

【対応が望ましい事項】

a. フォレンジック調査等を内部の役職員で実施する場合は、該当する役職員のスキルと知識を維持・向上させること。
b. 脆弱性診断やペネトレーションテストを内部の役職員で実施する場合は、該当する役職員のスキルと知識を維持・向上させること。

2.3.3. データ保護

【基本的な対応事項】

① 情報の重要度と、使用される技術環境における固有のリスクに応じて、データの管理方針を策定すること。管理方針には、データの管理、データの保存、適切な暗号化方式を採用することや、暗号鍵と電子証明書を、そのライフサイクルを通じて管理し、保護すること、危殆化時の対応などを含めること。
（参考）CRYPTREC「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（最終更新：令和６年５月 ）
② 情報の重要度に応じてデータを分類し、分類に応じた管理方針に従ってデータを保護（暗号化、認証、秘匿化、アクセス制御等）すること。
③ 外部記憶媒体の保護と使用（使用制限、暗号化、マルウェアスキャンなど）に係る管理手続を策定し、実施すること。
④ ライフサイクル全体（媒体の廃棄、データの安全な消去、外部委託先によるデータの取得・返却・破棄に至るまでの過程を含む）を通じて、データを適切に管理すること。
⑤ システム及び情報の重要度に応じたバックアップ要件、バックアップデータの隔離と保護、整合性の検証、復旧テストの実施等を含む、バックアップに関する規程等を整備し実装すること。また、清算・振替機関等においては、バックアップデータの完全性の確保のために、必要に応じて、関係者との間において、データ共有に係る取決めを行っておくこと。
　特に、ランサムウェア攻撃のリスクを考慮して、バックアップの期間や頻度を検討すること。また、同一ネットワーク内のバックアップファイルを探索して削除するランサムウェアのタイプがあることを踏まえて、改ざん耐性バックアップシステムの利用、組織内ネットワークから切り離した複数の環境での保管や媒体等へのバックアップを実施すること。

なお、情報資産管理については、業態ごとの監督指針等における「情報セキュリティ

管理」の項目も参照すること。

【対応が望ましい事項】

a. DLP[33]又はそれに相当するものを導入し、役職員や外部関係者によるデータ漏えい（機密データの窃取や破壊を含む）を監視し、保護すること。
b. 法令上の責任や組織の資産としての情報の重要性に従って、データ・ガバナンスに関する方針及び規程等を策定すること。

2.3.4. システムのセキュリティ対策

2.3.4.1. ハードウェア・ソフトウェア管理

【基本的な対応事項】

① 必要な機能（ポート、プロトコル、サービス等）のみを提供するようにシステムを構成すること。
② システムの保守におけるサイバーセキュリティを確保するための手続を定めること（リモート保守やオンサイト保守時の保守要員、作業手順、作業に用いるツール・交換部品を承認する手続など）。
③ サポートの終了に伴うハードウェア・ソフトウェアの廃止・更改を計画的かつ安全に実施すること。ソフトウェアについてサポート対象バージョンへの更新が困難な場合には、補完的な措置を講じるとともに、迅速にサポートが得られるソフトウェアを利用したシステム・ビジネスプロセスへの移行計画を立て、着実に実行すること。
④ システムをマルウェアの感染から保護すること。例えば、以下の方法が考えられる。
  - マルウェア対策ソフトの導入、マルウェアシグニチャ（パターンファイル）及び動作プロファイル（ふるまい定義）の自動更新
  - 不正なコード（JavaScript、ActiveX、VBScript、PowerShell など）に対する保護機能の導入
  - メールのマルウェア又は不正サイトへのリンクの検出、隔離、ブロック
  - 悪意あるウェブサイト、未承認の SNS サービス、ファイル交換サービス等への接続制御

[33] DLP（Data Loss Prevention）とは、機密情報等を特定し、監視・保護するツールをいう。

【対応が望ましい事項】

a. システムで利用するサードパーティのライブラリやミドルウェア、ハードウェアについては、不正侵入の経路となるバックドア等が含まれることのないように、セキュリティ・バイ・デザインやセキュリティ・バイ・デフォルト[34]等の安全な開発手法を製品開発に取り入れている事業者から提供される安全なプロダクトを選定すること。
b. サプライチェーンのリスク評価の中で、ハードウェアに関するサイバーセキュリティリスク（不正なファームウェア導入のリスク等）を評価対象とすること。
c. ハードウェア（機器、ファームウェア、UEFI 又は BIOS 等）の真正性を確保し、また、不正な書き換えを防止するための対策（改竄検知など）を導入すること。
d. ハードウェアの調達基準等にセキュアな調達のための基準を設けること。調達基準や取引基準の中で、調達先又は取引先の法令順守、自組織のセキュリティ基準又は倫理基準などの社内基準の遵守を求めること。法令、社内基準、国連制裁等を踏まえたサプライヤーリスト又は制裁対象リストを作成、維持し、これらを踏まえた調達を実施すること。

2.3.4.2. ログ管理

【基本的な対応事項】

① ログの取得・監視・保存のための手続を策定し、定期的にレビューすること。手続には、例えば、以下の事項を含むこと。
- ログに記録する内容
- 対象範囲（監視対象のハードウェア、ソフトウェア、サービス等）
- ログへのアクセス制御
- 監視方法
- ログの改ざん防止
- 保存期間
- 保存方法

② 情報システムのイベントログや運用担当者の作業ログの適切性を定期的又は必要に応じて都度確認すること。

[34] ユーザー（顧客）が、追加コストや手間をかけることなく、購入後すぐに IT 製品（特にソフトウェア）を安全に利用できること。

2.3.4.3. セキュリティ・バイ・デザイン

【基本的な対応事項】

① 金融商品・サービスの企画・設計段階から、セキュリティ要件を組み込む「セキュリティ・バイ・デザイン」を実践すること。サービス全体の流れの中で、重要なサードパーティも含めてリスクを検証し対策を講ずること。
② 自組織にシステムを提供する重要なサードパーティにおいて、セキュリティ・バイ・デザインを実施できる体制となっているかを確認すること。

（参考）デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」（令和６年１月）

【対応が望ましい事項】

a. セキュリティ・バイ・デザインにかかる管理プロセスを、以下の点も考慮のうえ、整備し、運用すること。
   - セキュアコーディングに係る基準を策定し、実施すること。
   - データの機密性、アクセス管理、イベントログ取得等のセキュリティ要求事項を明確化していること。
   - セキュリティ技術・アーキテクチャーに係る設計標準を策定すること。
   - アプリケーションソフトウェアのリリース前及びリリース後定期的に、アプリケーションの脆弱性診断を実施すること。
   - システムへの脆弱性の混入及び作込みを未然に防止し、早期に検知するツール（ソースコード解析ツール等）を活用すること。

2.3.4.4. インフラストラクチャ（ネットワーク等）の技術的対策

【基本的な対応事項】

① 不正侵入を防止するため、外部ネットワーク（オープンネットワーク、リモートアクセス等）と内部ネットワークの接続部分に適切な不正侵入防止策（物理的な分離・論理的な分離等）を講ずること。また、外部ネットワークと内部ネットワークとの間のデータ授受に対する不正侵入防止策を講ずること。
② ネットワーク機器の設定（ファイアウォールルール、ポート、プロトコルなど）を定期的及びシステム環境の更新時に点検し、必要に応じて更新すること。ファイアウォールは必要な通信のみを許可する設定とすること。
③ 情報の機密性や完全性等を保護する観点から、専用線や暗号技術の活用等を通じ

てネットワークのセキュリティを確保すること。

④ 無線 LAN ネットワークへのアクセスは、適切な認証機能及びアクセス制御機能を実装し、不正利用を防止すること。

⑤ テレワークやベンダーによる保守等においてリモートアクセスの対象とするシステムを制限し、適切に管理すること（セッションタイムアウト、利用者認証や通信内容を含むログの取得・保存・監視など）。また、重要なシステムについては、多要素認証や暗号化接続を使用すること。

【対応が望ましい事項】

a. DDoS/DoS 攻撃対策、DNS に係るサイバーセキュリティ対策、代替通信経路の制御などによって、組織の通信及びネットワークサービスの耐性度を強化すること。

b. 開発環境及びテスト環境を本番環境から分離するとともに、不正アクセスや情報資産の不正な変更を防止すること。

c. ネットワークセグメントを細分化し、マルウェアの水平移動（ラテラルムーブメント）を阻止することなどにより、サイバー攻撃の被害拡大防止を図ること。

2.3.4.5. クラウドサービス利用時の対策[35]

【基本的な対応事項】

① 利用するクラウドサービスの仕様を確認し、理解を深めること。

② 責任共有モデル[36]を理解し、クラウド事業者との責任範囲等を明確にすること。

③ 情報公開等の設定にミスがないか確認すること。設定の妥当性の確認においては、必要に応じて、専門家によるシステム監査や誤設定の自動検知等の診断サービス等を利用すること。

④ 責任分界に応じて、サービス仕様が変わる際には影響を確認すること。

⑤ 多岐にわたる関係主体等を把握し、情報共有体制・インシデント対応体制を構築すること。

⑥ クラウドサービスの利用終了時における、クラウドサービス上のデータの取扱い（論理的な廃棄）について確認すること。

---

[35] （参考）「クラウドサービス利用・提供における適切な設定のためのガイドライン」（総務省）も参照すること。

[36] 利用者とクラウド事業者が、責任分界点を定めるだけではなく、運用責任を共有し合っているという考え方。

2.4. サイバー攻撃の検知

【基本的な対応事項】

① アノマリ（異常値）、IoC（侵害の痕跡）などのサイバー攻撃の端緒の検知のための監視・分析・報告に係る手続等を策定し、必要に応じて見直すこと。なお、利用するクラウドサービスがサイバー攻撃の端緒となるリスクを踏まえ、責任分界に応じて、監視の対象には、クラウドサービスも含めること。なお、クラウドサービスの監視には、クラウド事業者のシステム監視状況を同事業者から提供されるレポート等により確認することを含む。
② サイバー攻撃に対するリスク低減を図るために、サイバー攻撃の脅威に応じて、必要な監視・分析などの対策を講ずること。なお、これらの対策を外部委託している場合には、当該委託先で実施している対策の具体的な内容を把握するとともに、対策の講じられていない領域が判明した場合には、必要な措置をとること。

2.4.1. 監視

【基本的な対応事項】

サイバー攻撃の端緒を検知するために、以下について継続的な監視を実施すること。

① ハードウェア・ソフトウェアについて、例えば、以下の監視をすること。
- 未承認のハードウェアや組織内ポリシーに違反するハードウェアのネットワークへの接続。
- 未承認のソフトウェアのインストール
- ソフトウェア、ファームウェアの更新時に当該ソフトウェア、ファームウェアの改ざん等が行われていないこと。
- サーバや端末における不審な挙動。
- ソフトウェアのパッチ適用状況。

② ネットワークについて、例えば、以下の監視をすること。
- 組織内ネットワークへの不正侵入（IPS[37]や IDS[38]の利用等による監視）。
- DDoS 攻撃等によるネットワークフローやトラフィックの異常値。
- 不正又は通常と異なるネットワーク接続やデータ転送。
- 悪意のあるウェブサイト、未承認の SNS サービス、ファイル交換サービス

[37] IPS（Intrusion Prevention System）とは、検知した不正な通信を自動的に遮断する機能を備えているシステムをいう。
[38] IDS（Intrusion Detection System）とは、ネットワーク上の通信を監視し、不正侵入やマルウェアなど不審な通信を検知・通知するシステムをいう。

等の接続。

③ 役職員によるシステムへのアクセスについて、例えば、以下の監視をすること。
- 通常利用とは異なるアクセスパターン等の不審な振る舞い

④ 外部のサービスプロバイダによるシステムへのアクセス（保守作業等）について監視をすること。

⑤ サイバー攻撃の端緒がインシデントに該当するかどうかを分析（影響範囲・重要度を含む）し、速やかにしかるべき責任者に報告すること。

⑥ サイバー攻撃の端緒を検知するためのアラート基準や閾値等の妥当性を定期的に検証すること。

⑦ データセンターやサーバ室への出入や不審な活動を監視すること。

【対応が望ましい事項】

a. おとりアカウントやサーバを用いて、攻撃の初期段階に検知するための仕組みを導入すること。
b. 顧客サービスの提供内容を踏まえた常時監視（24 時間 365 日）を行うこと。
c. SIEM[39]等のツールを活用して、複数の監視情報（ソーシャルメディア、ダークウェブ等の外部情報を含む）を集約し、情報の相関関係を含めて、リアルタイムにサイバー攻撃の端緒がインシデントに該当するかどうかを分析すること。

2.5. サイバーインシデント対応及び復旧

2.5.1. インシデント対応計画及びコンティンジェンシープランの策定

【基本的な対応事項】

① サイバー攻撃を想定したインシデント対応計画及びコンティンジェンシープラン（復旧計画まで含む）を、サイバー攻撃の種別ごと[40]に策定すること。その中で対応の優先順位や目標復旧時間、目標復旧水準を定めておくこと。左記について、定期的あるいは必要に応じて見直しを実施すること。

---

[39] SIEM（Security Information and Event Management）とは、ファイアウォールや IDS／IPS、プロキシなどから出力されるログやデータを一元的に集約し、それらのデータを組み合わせて相関分析を行うことにより、ネットワークの監視やサイバー攻撃やマルウェア感染などのインシデントを検知することを目的とする

[40] DDoS 攻撃、Web サイト改ざん、マルウェア（電子メールや Web サイトの閲覧等で悪意のある不正プログラムを PC やサーバ等の機器に感染させることにより、システムやデータの破壊・改ざん当を行う攻撃)・ランサムウェアといった標的型攻撃等、脆弱性の悪用（ターゲットのシステムやその使用しているソフトウェアに存在する脆弱性を悪用し、情報の窃取を行う攻撃)、不正送金を引き起こす攻撃など。

【対応が望ましい事項】

a. コンティンジェンシープランにおいては、資金清算インフラや決済インフラ等におけるインシデントや、データセンターやクラウド等を含めたサードパーティが提供するサービス等が長期間利用できないようなインシデントなど、大規模な被害が生じるサイバーインシデントに対応するためのコンティンジェンシープランも整備すること。

2.5.2. インシデントへの対応及び復旧

インシデント対応計画及びコンティンジェンシープランにおいては、以下の事項を考慮すること[41]。

2.5.2.1. 初動対応（検知・受付、トリアージ）

【基本的な対応事項】

① 2.4 に掲げる事項を含め、各種システムの監視や、顧客等からの問合せ、セキュリティ対応機関など外部組織からの連絡により、インシデントを検知すること。
② 検知・受付時に収集した情報を基に、事実関係を確認のうえ、インシデント対応の要否を判断すること。
③ インシデントは、業務影響等に応じた優先順位付けを行い、あらかじめ定められた基準に従い、インシデント対応組織の管理者や、サイバーセキュリティを統括管理する責任者（CISO 等）、経営陣に報告すること。

2.5.2.2. 分析

【基本的な対応事項】

① 対応が必要と判断したインシデントについて、攻撃の手口や原因・経路、システムへの影響、現在発生している業務影響及び今後発生しうる業務影響等について分析すること。特に、分析を行う際は事前にログ等の証跡を保全し、分析は保全したログ等に対して行うこと。

[41] 「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書」（公益財団法人金融情報システムセンター編））の「IV　サイバー攻撃・情報漏えいの考慮事項」等も参照されたい。

② インシデントの検知・受付から復旧までのフェーズに関し、記録（インシデントの内容、その対応において取られた行動内容や調査における収集ログの一覧等）を残しておくこと。

2.5.2.3. 顧客対応、組織内外の連携、広報

【基本的な対応事項】

① インシデント対応計画やコンティンジェンシープラン（復旧計画含む）に基づき、サイバーセキュリティを統括管理する CISO 等の責任者や担当者、各コンティンジェンシープランの関係者（サードパーティの組織内の担当者等を含む）が、それぞれの役割、必要な連絡先、必要な対応手順[42]について習熟すること。
② 情報漏えい等により顧客に二次被害などの影響がある場合は、影響範囲や注意事項、対応方法等を当該顧客に伝達すること。
③ インシデント発生時は、法令等に従い、規制当局等に速やかに報告をすること。
④ 法令等に基づき、公表が必要な場合や、二次被害防止、顧客保護等の観点から公表が適切な場合は、サイバー攻撃による被害、対応状況、復旧見込み等の判明している事実について、顧客や自組織等のセキュリティ上のリスクを配慮した上で、適切かつ速やかに公表すること。
⑤ 攻撃者の TTP（Tactics（戦術）、Techniques（技術）、Procedures（手順））等、他機関にとっても有効となる攻撃技術情報について、機密情報を除いた上で、必要に応じ、金融 ISAC や JPCERT/CC 等の情報共有機関に共有すること。
（参考）内閣サイバーセキュリティセンター「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和５年３月８日）

2.5.2.4. 封じ込め

【基本的な対応事項】

① サイバー攻撃による被害拡大を防止するための対応（封じ込め）を行うにあたり、事前に以下の点を考慮すること。
- 被害の拡大防止のために通信の遮断やシステム停止等を行うに当たっては、事前に対応の実施を判断する権限者を明確にしておくこと。また、判断する際の検討要素として、停止する時間帯や期間、停止するサービスの範囲に応じた業務影響、業務の代替手段や通信経路等を整理しておくこと。

② 実際の封じ込めに当たって、情報漏えいによる再発及び二次的被害の可能性が危

[42] 清算・振替機関等については、インシデント発生時における参加者等やその他関係先との連絡及び対応の連携に係るものを含む。

惧される場合には、発生を防ぐための対策を実施すること。その際には、以下の点を考慮すること。

・ 通信の遮断やシステム停止等を行う場合、封じ込めと証拠保全のいずれを優先すべきか、インシデントの状況や自組織の方針に従い判断すること。
・ 必要に応じて、外部専門家を活用して封じ込めを実施すること。

（参考）金融情報システムセンター「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書（第４版）」（令和６年１月）２.(3)d 封じ込めを参照のこと。

【対応が望ましい事項】

a. 封じ込めの際には、対応によって影響が生じる可能性のあるサードパーティに適切に通知を行うこと。

2.5.2.5. 根絶

【基本的な対応事項】

① サイバー攻撃により被害が発生した原因を除去すること（マルウェアの駆除、パッチの適用等による脆弱性の修正等）。その際、以下の点を考慮すること。
・ セキュリティを高めるための対策（ネットワークの監視レベルの引上げ、ファイアウォールやセキュリティ装置の設置及びアクセス制御の適切な実施等）を検討すること。
・ 必要に応じて、外部専門家を活用して根絶を実施すること。

（注）「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書」（公益財団法人金融情報システムセンター編）第４編Ⅳ２.(3)e 根絶を参照のこと。

2.5.2.6. 復旧

【基本的な対応事項】

① 復旧計画において、復旧完了し業務再開を判断する際には、判断権限者を明確にしておくとともに、判断要素を整理しておくこと。被害を受けた原因を特定しないまま復旧を行うことにより、再度同様の攻撃を受け、被害が発生することが想定されるため、業務再開の判断要素には、原因への対応がなされたことの確認を含めること。
② 復旧作業においては、被害を受けた機器の初期化、システム再構築等を行い、シ

ステムを通常の運用状態に戻して正常稼働を確認すること。

③ バックアップからの復旧の際には、攻撃の手法に応じて、既にバックアップデータ等が改ざんされている可能性や、マルウェア等に感染している可能性に留意すること。清算・振替機関等においては、バックアップからの復旧の際に、例えば、参加者等が指図したものの未達のものがある場合等には、当該指図の再送信を参加者等に求めること。

④ 被害を受けたシステムと他システムを再接続する前に、システムの正常な稼働や接続がなされていることを確認すること。

⑤ 復旧作業に際しては、重要な業務が適切な手順で復旧され、通常どおりの業務が稼働していることをシステム責任者と共に確認するなど、復旧が適切に行われたことを確認すること。

⑥ インシデントからの復旧後、当該インシデントの発生原因や被害の拡大に関する原因等を分析し、対応の評価を行うこと。また、当該評価を基に、インシデント対応計画やコンティンジェンシープランを含むサイバーセキュリティ管理態勢の見直しや改善を行うこと。

2.6. サードパーティリスク管理

金融機関等のサードパーティへの依存が増大するとともに、金融機関等のサプライチェーンは拡大・複雑化しており、金融機関等にとってそのリスク管理の難度は増大している。こうした中、サプライチェーンに由来するサイバーインシデントにより、金融機関等が多大な影響を受ける事例が発生している。金融機関等は、こうした状況を踏まえ、サプライチェーンのサイバーセキュリティリスクを適切に管理する必要がある。なお、サードパーティリスク管理については、本ガイドラインのほか、監督指針等において、外部委託（二段階以上の委託に関するものを含む）に関する一般的な着眼点及びシステムリスク管理における外部委託管理の着眼点が示されている[43]。また、本節④に記載のとおり、サードパーティリスク管理には、リスクベースの対応が求められることに留意が必要である。

加えて、金融機関等にサービス等を提供するサードパーティは、金融機関等によるサイバーセキュリティリスクの適切な管理のために、必要な支援（当該サードパーティに関するサイバーセキュリティリスクを含め、金融機関が必要な情報を利用できるようにすることなど）を行うべきである。これに関連して、金融当局は、業法[44]に基づき、特に必要があると認めるときは、その必要の限度において、外部委託先に対して、報告徴求命令の発出や立入検査を実施する権限等を有しており、監督指針等でその監督対応・

[43] 例：主要行等向けの総合的な監督指針III－３－３－４。
[44] 例えば、銀行法第 24 条第２項、同第 25 条第２項。

手法が示されている。

【基本的な対応事項】

① サイバーセキュリティに係る戦略、取組計画を策定する際にはサプライチェーン全体を考慮すること。また、サードパーティを含む業務プロセス全体を対象としたサイバーセキュリティ管理態勢を整備すること。
② サードパーティのリスク管理のライフサイクル全体を通じ、サードパーティに起因するサイバーセキュリティリスクを管理するために必要な態勢を整備し、サードパーティリスク管理の方針を策定すること。
③ サードパーティリスクを管理するための組織体制の整備（一元的に管理する統括部署の設置や、関係部署間の連携を含めた各部署の役割及び責任の明確化）、組織内規程の策定を行うこと。
④ サードパーティを特定し、サードパーティやサードパーティが提供する商品・サービスの自組織業務における位置づけ・役割・重要度、重要な情報（個人情報や営業機密等）の取扱いの有無、組織内システムへの接続状況（インターネット接続等の外部からのアクセスの容易さ）などをふまえ、サードパーティのリスク評価を行い、そのリスクに応じた対応をすること。
⑤ サードパーティを管理するための台帳等を整備し、維持すること（管理項目の例：サードパーティの名称、提供する商品・サービス及び機能、サードパーティが自組織のシステムに対し有するアクセスレベル、サードパーティが保持又は処理する自組織のデータの種類や機密性及び場所）。
⑥ サイバーインシデント対応計画やコンティンジェンシープランにおいては、インシデント対応等を行うサードパーティを含めた態勢を整備すること[45]。
⑦ サードパーティとの取引開始に当たっては、事前に定めた基準に基づき、デューデリジェンスを行うこと。デューデリジェンスでは、例えば、以下の事項について、評価すること。なお、デューデリジェンスは、外部評価（第三者保証報告書、第三者認証）の活用によるものも含まれる。
   - サードパーティとの取引がもたらす潜在的なサイバーセキュリティリスクや脆弱性の評価。
   - 自組織がサードパーティに求めるサイバーセキュリティ（契約等で求める事項）の充足状況
   - 過去のインシデントの発生状況、当該インシデントへの対応、復旧、再発防止策の状況等

   特に重要なサードパーティに対しては、サイバーセキュリティ管理態勢、サイバーインシデント対応計画、コンティンジェンシープランについても、評価を行

[45] 詳細は、2.5 節を参照のこと。

うこと。

⑧ サードパーティが遵守すべきサイバーセキュリティ要件を明確化の上、重要度に応じ、サードパーティ等との契約やSLA（サービスレベルアグリーメント）等において、例えば、以下の項目を明記すること。

- サードパーティとの役割分担・責任分界
- 監査権限
- 再委託手続
- 実施すべきセキュリティ対策
- サードパーティの役職員が遵守すべきルール
- インシデント発生時の対応及び報告
- 脆弱性診断等の実施及び報告
- 深刻な脆弱性が判明した場合の対応及び報告
- サイバーセキュリティに係る演習・訓練の実施（共同演習・訓練への参加を含む）
- データの所在・保管・保持・移転・廃棄に関する取決め
- 契約終了の条件及び契約終了時の取決め
- 外部評価等の実施（第三者保証報告書の提出、第三者認証の取得を含む）

⑨ サードパーティ及びその製品・サービスによってもたらされるサイバーセキュリティリスク並びに契約の履行状況等について、リスクの重大性に応じて、継続的にモニタリングすること。

⑩ サードパーティとの取引終了時の管理プロセス（データ廃棄、組織内システムへのアクセス遮断措置など）を整備すること。

【対応が望ましい事項】

a. サードパーティリスク管理に係る統括部署に適切な知識等を有する人員の配置をすること。

b. サードパーティリスク管理において、重要な業務のサードパーティへの依存関係、サードパーティの集中リスク、地政学リスクの影響、フォースパーティ[46]の影響を考慮すること。

c. 重要なサードパーティがそのサードパーティ（２以上のサードパーティ（自組織から見たフォースパーティ、フィフスパーティ及びＮ番目のパーティ）を含む）を管理する能力及びそのサプライチェーンリスク、集中リスク等について、定期的にモニタリングすること。

d. 重要なサードパーティの事業撤退や業務停止、契約関係の終了に備えて、適切なコンティンジェンシープランと出口戦略を事前に策定し、定期的に代替手段のテ

[46] サードパーティの再委託先など。

スト等をすること。

e. 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律に基づき、特定社会基盤事業者が、特定重要設備の導入やその重要維持管理等の委託を行おうとする場合に提出する届出において記載することとされているリスク管理措置（特定妨害行為の手段として使用されるおそれを低減させるためのもの）を講じること。

（参考）金融庁ウェブサイト「金融分野における経済安全保障対策」
（https://www.fsa.go.jp/news/r5/economicsecurity/231117infrastructure.html）

3. 金融庁と関係機関の連携強化

3.1. 情報共有・情報分析の強化

脆弱性情報をいち早く把握、共有し、金融機関における脆弱性への対応を促すことで、サイバー攻撃の被害を未然に防ぎ、あるいは、その影響を極小化するため、金融庁は、サイバーセキュリティの司令塔である内閣サイバーセキュリティセンター（NISC）、日本銀行、金融 ISAC、金融情報システムセンター（FISC）及び各 CEPTOAR[47]等との連携を維持、強化する。

また、サイバー攻撃の主体や目的が多様化し、脅威動向の把握が難しくなる中、情報収集・分析能力（インテリジェンス）をより強化するため、公安調査庁等との情報連携を推進する。

3.2. 捜査当局等との連携

新技術を活用した新たな金融サービスが生み出される一方、金融犯罪においては、従来のインターネットバンキングに係る不正送金に加えて、暗号資産取引に関する匿名化技術を悪用し、ランサムウェア攻撃で身代金を暗号資産で要求するなど、新たなサービスや技術を悪用した犯罪が増加している。また、高度な技術を持たない悪意のある者へ、マルウェアや不正出金の手段などを組織的に提供するエコシステムが確立され、不正な収益獲得が可能となったと指摘されている。犯罪行為の誘因を下げ、サイバー攻撃を抑止する捜査当局の取組みを後押しするため、金融庁は、金融犯罪における手口の変化を注視し、注意喚起や啓発による金融犯罪の未然防止と被害拡大防止のための活動を警察及び業界団体等と連携して行う。

[47] CEPTOAR（セプター。Capability for Engineering of Protection, Technical Operation, Analysis and Response の略）とは、重要インフラ事業者等の情報共有・分析機能等を担う組織をいう。

3.3. 国際連携の深化

国境を跨ぐ脅威、国際的に影響が波及するインシデント、サードパーティ・サプライチェーンリスク、AI、量子コンピューティングによる暗号技術の危殆化などの国境を跨ぐ問題に適切に対応するため、金融庁としては、こうした国際的な議論に参画し、海外当局と連携する。加えて、こうした国際連携から得られた知見を国内でのモニタリング及び業界との連携に活用する。

3.4. 官民連携

サイバーセキュリティは、金融サービスの利用者、金融機関等、当局その他関係者を含めたエコシステム全体での強化が必要であるため、金融庁は、共助機関及び金融機関等と連携して金融セクター全体の取組みを推進するとともに、モニタリング等を通じ、個々の金融機関等及び業界の底上げを進める。また、民間における共助の取組みを一層促進する。

令和６年 10 月４日制定