金融庁サイバーセキュリティ対策
ガイドライン解説レポート

Librus株式会社
コンサルティングサービス事業部

1. はじめに

金融分野におけるサイバーセキュリティの重要性

近年、技術の発展や地政学リスクの高まりを背景に、サイバーセキュリティに関するリスクが顕著に増大しています。特に金融機関は、顧客の重要な資産や情報を扱うため、サイバー攻撃の標的となりやすく、攻撃が成功した場合の影響も甚大です。外部委託先を含むサプライチェーンの弱点を悪用した攻撃による被害も発生しており、国家等が関与・支援している主体によると見られる高度なサイバー攻撃も出現しています。

サイバー攻撃の特徴と課題

- 攻撃の高度化・巧妙化（標的型攻撃、持続的な攻撃など）
- サプライチェーンを通じた間接的な攻撃の増加
- 国家が関与する高度な攻撃の出現
- 被害範囲の拡大と影響の深刻化
- 金融システム全体への波及リスク

金融庁の取り組み背景と目的

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ます。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す。

こうした状況を踏まえ、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」に基づき、金融業界との対話・協働を通じて、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進してきました。2024年10月には、これまでの検査・モニタリングの結果や金融セクター内外の状況変化を踏まえ、「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」を公表しました。

対応の必要性と緊急性

金融庁の検査・モニタリングの結果、以下のような基本的な対策が不十分な事例が散見されています：

- 経営者の主体的な関与の不足
- 情報資産の把握及び管理の不徹底
- セキュリティパッチの迅速な適用などの脆弱性管理の欠如
- IDアクセス権管理の不備
- 定期的な脆弱性診断及びペネトレーションテストの未実施

2. 金融庁サイバーセキュリティガイドラインの概要

策定背景・経緯

現行の各業態の監督指針・事務ガイドラインにおけるサイバーセキュリティに関する規定は、2015年の改正時に導入されたものであり、近年のサイバーリスクの深刻化に対処していくために、改定が不可欠となっていました。金融庁は、これまでの実態把握及び建設的対話における体制整備促進並びに各種の注意喚起及び要請を行ってきましたが、検査・モニタリングの結果、基本的な対策が不十分な事例が散見されていることが明らかになりました。
このような実態に鑑み、2024年10月4日に監督指針等を改正するとともに、「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」を策定しました。また、2025年7月4日には、サイバー対処能力強化法整備法の一部施行に伴う技術的な改正も行われています。

基本的考え方

本ガイドラインは、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を規定し、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」を明確化しています。

区分	定義・説明
基本的な対応事項	いわゆるサイバーハイジーン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
対応が望ましい事項	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

重要なポイント：リスクベース・アプローチ
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す。

適用対象

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以下の金融機関等を対象としています：

- 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
- 金融商品取引所

ガイドラインの構成

ガイドラインは以下の3つの主要セクションで構成されています：

1. 基本的考え方：サイバーセキュリティに係る基本的考え方、金融機関等に求められる取組み、業界団体や中央機関等の役割、適用対象等
2. サイバーセキュリティ管理態勢：管理態勢の構築、リスクの特定、防御、検知、インシデント対応及び復旧、サードパーティリスク管理
3. 金融庁と関係機関の連携強化：情報共有・情報分析の強化、捜査当局等との連携、国際連携の深化、官民連携

3. サイバーセキュリティ管理態勢の構築

経営陣の関与・ガバナンス

サイバーインシデントによる業務中断、機密情報の漏洩は、金融機関の事業及び経営を揺るがしかねない重大な影響をもたらし得るものであり、ひいては金融システムの安定を揺るがしかねないものです。サイバーセキュリティの強化には経営者の認識及びイニシアティブによるところが大きいため、経営陣のリーダーシップの下で、サイバーセキュリティに関するガバナンスの確立が必要です。

基本的な対応事項

取締役会等による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た基本方針の策定
サイバーセキュリティ管理態勢の年1回以上のレビュー実施（必要に応じ外部専門家によるレビューを含む）
サイバーセキュリティを統括管理する責任者（CISO等）の経営陣の責任において任命
サイバーセキュリティに係る戦略、取組計画（複数年計画含む）の策定と見直し
セキュリティ・バイ・デザインを含むサイバーセキュリティ確保に向けた取組みの推進
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、組織風土の醸成
少なくとも年1回、サイバーセキュリティリスク状況、リスク評価結果、取組計画の進捗状況の報告受領

対応が望ましい事項

経営陣が適切な経営判断を行うための前提として、サイバーセキュリティに関する十分な知識の利用（外部専門家の活用を含む）
リスク選好度・耐性度（リスクアペタイト・リスクトレランス）の設定
サイバーセキュリティへの取組みの対外公表
KPI（主要業績評価指標）・KRI（主要リスク指標）の経営陣への報告
経営陣に相当する者としての責任者（CISO等）の配置、経営陣と直接コミュニケーションする関係の構築

基本方針・規程の策定

金融機関等は、取締役会等がサイバーセキュリティ管理の基本方針を策定し、それに基づいた規程類や業務プロセスを整備することが求められています。基本方針には、セキュリティ対策の目的や方向性、関係主体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などを含める必要があります。

サイバーセキュリティ管理態勢の主要な構成要素

- 基本方針と規程類
- 組織体制と責任の明確化
- 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等のサイバー攻撃に対する監視体制
- 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等の緊急時対応及び早期警戒のための体制を含む）

組織体制と人材育成

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し、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が必要です。また、サイバーセキュリティ人材の確保・育成は喫緊の課題となっています。

基本的な対応事項

サイバーセキュリティの重要性を踏まえた経営資源の配分
サイバーセキュリティ管理の基本方針と整合的な人材育成・確保計画の策定
最新の脅威情報等を踏まえた計画的な教育・研修プログラムの策定と実施
経営陣を対象とする研修・訓練の実施

4. サイバーセキュリティリスクの特定

情報資産管理

これまでの検査・モニタリングの結果、情報資産管理は基本的な対策が不十分な事例が散見された領域の一つです。適切な情報資産管理は、効果的なサイバーセキュリティ対策の基盤となります。

基本的な対応事項

情報資産のライフサイクル、重要度に応じた管理
情報システム・外部システムサービス、ハードウェア・ソフトウェア、顧客・機密情報等の台帳の整備・管理
データフロー図・ネットワーク図の作成・管理

リスク管理プロセス

金融機関等は、組織的・体系的なリスク管理プロセスを確立し、定期的にリスクを評価・対応する必要があります。

基本的な対応事項

- 脅威情報・脆弱性情報の収集・分析
- リスクの特定・評価（境界防御型セキュリティの突破、内部不正等の可能性を含む）
- リスク対応（回避、軽減、受容、移転）、リスク対応計画の経営陣への報告
- リスク評価に基づく継続的な改善活動

脆弱性管理

ハードウェア・ソフトウェア等の脆弱性管理は、サイバーセキュリティ対策の基本中の基本です。特にセキュリティパッチの迅速な適用は、多くのサイバー攻撃を防ぐ上で極めて重要です。

基本的な対応事項

- 脆弱性管理に関する手続等の策定
- システムの重要度や脆弱性の深刻度に応じたパッチ適用等の管理
- 定期的なパッチ適用状況の確認と報告

脆弱性診断及びペネトレーションテスト

脆弱性診断やペネトレーションテストは、システムやネットワークの脆弱性を実際に確認し、対策を講じるための重要な手段です。これらを定期的に実施することで、セキュリティレベルを継続的に向上させることができます。

基本的な対応事項

- システムの重要度に応じた定期的な脆弱性診断の実施
- 重要なシステムに対する定期的なペネトレーションテストの実施
- 結果に基づく対策の実施と経営陣への報告

対応が望ましい事項

- 脅威ベースのペネトレーションテスト（TLPT: Threat-Led Penetration Testing）の実施

演習・訓練

サイバーインシデントへの対応力を高めるためには、定期的な演習・訓練が不可欠です。特に、実際のインシデント発生時に備えた実践的な訓練が重要となります。

基本的な対応事項

- 定期的な演習・訓練の実施
- 必要に応じた業界横断的な演習への参加
- 経営陣等による演習・訓練への関与
- 顧客への深刻な影響かつ現実に起こりうるシナリオの検討及び見直し
- 演習・訓練を通じたコンティンジェンシープラン等の有効性の定期的検証

5. サイバー攻撃の防御対策

認証・アクセス管理

適切な認証・アクセス管理は、不正アクセスを防ぐ上で重要な役割を果たします。特にIDアクセス権管理は、検査・モニタリングの結果、基本的な対策が不十分な事例が散見された領域の一つです。

基本的な対応事項

- 方針・規程等の策定・見直し
- 最小権限の原則に基づくアクセス権限の限定
- ID・認証情報の適切な管理（定期的なレビュー、特権IDの厳格管理等）

システム・情報の重要度に応じた認証要件の決定（多要素認証の導入等）
第三者による不正防止（メールの送信ドメイン認証など）
物理的アクセスの管理

データ保護

金融機関が扱う機密データや個人情報を保護するためには、適切なデータ保護対策を講じる必要があります。

基本的な対応事項

重要度・リスクに応じたデータの管理方針の策定
暗号化等のデータ保護措置の導入
バックアップ・復旧に係る手続の整備

対応が望ましい事項

データ損失防止（DLP: Data Loss Prevention）ソリューションの導入
データライフサイクル全体にわたるデータガバナンス体系の整備

システムのセキュリティ対策

金融機関のシステムを保護するためには、様々な技術的対策を組み合わせて多層防御を実現する必要があります。

基本的な対応事項

ハードウェア・ソフトウェア管理（システム構成・保守等）
ログ管理（取得・監視・保存の手続策定・レビュー等）
セキュリティ・バイ・デザインの実践
インフラストラクチャ（ネットワーク等）の技術的対策
クラウドサービス利用時の対策

対応が望ましい事項

ハードウェアのセキュアな調達のための基準設定
セキュリティ・バイ・デザインの管理プロセスの整備・運用（セキュアコーディングの基準策定等）
開発環境・テスト環境の本番環境からの分離
ゼロトラストアーキテクチャの段階的導入

教育・研修

サイバーセキュリティは技術だけでなく、人的な要素も重要です。すべての役職員に対する教育・研修は、セキュリティ意識の向上と基本的なセキュリティ対策の徹底に不可欠です。

基本的な対応事項

経営陣を含むすべての役職員への教育・研修の実施
役割・職責に応じた教育内容の提供
サードパーティにおける教育（サードパーティによる社内教育・研修の実施状況の確認を含む）
標的型メール訓練等の実践的な訓練の実施

対応が望ましい事項

顧客へのセキュリティ啓発活動の実施
専門人材の育成・確保のための中長期的な計画の策定と実施

6. サイバー攻撃の検知

サイバー攻撃の巧妙化を踏まえ、侵入を前提とした検知体制の構築が必要となっています。
様々な監視ポイントやデータソースを活用して、異常を早期に検知することが重要です。

基本的な対応事項

検知のための監視・分析・報告に係る手続等の策定・見直し
サイバー脅威に応じた監視・分析
ハードウェア・ソフトウェア・ネットワークの監視
役職員によるアクセスの監視
外部プロバイダによるアクセス（保守など）の監視
インシデント該当性・影響範囲・重要度の分析・報告

対応が望ましい事項

24時間365日の監視体制の確立
SIEM（Security Information and Event Management）などの高度な監視ツールの活用
AI・機械学習を活用した異常検知の導入
定期的なアラート閾値の見直しと最適化

効果的な検知のためのポイント

1. 多層的な監視：エンドポイント、ネットワーク、アプリケーション、クラウドなど複数の層での監視
2. ログの統合管理：様々なシステムやデバイスからのログを一元的に収集・分析
3. アラート管理：重要度に応じたアラートの適切な設定と対応プロセスの確立
4. 継続的な改善：検知の精度向上のための定期的な見直しと調整

7. サイバーインシデント対応及び復旧

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の策定

サイバーインシデントが発生した場合に備えて、事前に対応計画やコンティンジェンシープランを策定しておくことが重要です。これにより、インシデント発生時の混乱を最小限に抑え、迅速かつ効果的な対応が可能となります。

基本的な対応事項

サイバー攻撃の種別ごとのインシデント対応計画・コンティンジェンシープランの策定
対応の優先順位・目標復旧時間・目標復旧水準の設定
報告ルート、判断権者、対外的な連携体制の明確化
役職員へのインシデント対応計画等の周知と教育

対応が望ましい事項

大規模な被害が生じるインシデント（資金清算インフラにおけるインシデントなど）に対応するためのコンティンジェンシープランの整備
インシデント対応に関する契約内容の事前整理（顧問弁護士、フォレンジック調査会社など）

インシデントへの対応及び復旧

サイバーインシデント発生時には、初動対応から復旧までの一連のプロセスを迅速かつ的確に実施する必要があります。また、インシデント後の分析と改善も重要です。

基本的な対応事項

初動対応：インシデントの検知・トリアージ、証跡保全、初期封じ込め

分析：被害状況・影響範囲の特定、原因の分析
顧客対応・組織内外の連携・広報：顧客・当局・業界団体等への報告、広報対応
封じ込め：被害の拡大防止、感染機器の隔離
根絶：侵入経路の特定と封鎖、マルウェアの排除
復旧：システムの復旧、バックアップからの回復、正常稼働の確認
教訓化：インシデント発生原因等の分析、対応の評価、再発防止策の実施

対応が望ましい事項

封じ込めに当たってのサードパーティへの通知
高度なフォレンジック調査の実施
顧客への補償等の対応方針の事前整理

インシデント対応におけるよくある課題

- 初動対応の遅れ（検知の遅れ、報告ルートの不明確さなど）
- 証跡保全の不備（ログの上書き、重要な証拠の消失など）
- 影響範囲の特定の難しさ（潜伏期間の存在、侵害の全容把握の困難さ）
- コミュニケーションの問題（部門間の連携不足、情報共有の遅れなど）
- 復旧の複雑さ（バックアップデータの完全性確認、マルウェアの残存リスクなど）

8. サードパーティリスク管理

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、金融機関が多大な影響を受ける事例が発生していることを踏まえ、サードパーティリスク管理の重要性が高まっています。金融機関は、自社のシステムやデータにアクセスする外部委託先やサービス提供者のセキュリティリスクを適切に管理する必要があります。

サードパーティリスク管理の重要性

近年、金融機関のサイバーインシデントの多くは、直接的な攻撃よりもサプライチェーンを通じた間接的な攻撃によるものが増加しています。こうした攻撃は、セキュリティ対策が比較的弱い委託先やクラウドサービスプロバイダーを標的とすることで、最終的には金融機関のシステムやデータにアクセスすることを狙っています。

基本的な対応事項

サプライチェーン全体にわたる戦略の策定・管理態勢の整備：サードパーティリスク管理に関する方針・規程の策定、体制の整備
ライフサイクル全体を通じたリスク管理：
    取引開始時のデューデリジェンス（セキュリティ対策状況の確認、リスク評価）
    サイバーセキュリティ要件の契約・SLAにおける明確化（監査権限、インシデント通知、データ保全等）
    継続的モニタリング（定期的な評価、脆弱性対応状況の確認等）
    インシデント対応計画・コンティンジェンシープランへのサードパーティ関連事項の組み込み
    契約終了時の対応（データ返却・消去の確認、アクセス権の削除等）
リスク評価・リスクに応じた対応：サードパーティの重要度分類、リスクに応じた管理レベルの設定

対応が望ましい事項

リスク管理に係るスキル及び経験のある人員の配置
重要な業務のサードパーティへの依存関係、集中リスク等の考慮
重要なサードパーティがそのサードパーティ（フォースパーティ）を管理する能力等のモニタリング
重要なサードパーティとの契約関係等の終了に備えた出口戦略等の策定

経済安全保障推進法上のリスク管理措置の実施

クラウドサービス利用時のリスク管理

クラウドサービスの利用が拡大する中、クラウド特有のリスクを適切に管理することが重要です。特に責任分界点の明確化や、クラウドサービス固有のセキュリティ要件に注意が必要です。

クラウドサービス利用時のポイント

- 責任共有モデルの理解（クラウド事業者と利用者の責任範囲の明確化）
- クラウド環境に適したセキュリティ対策の実施（アイデンティティ管理、暗号化、アクセス制御等）
- シャドーIT（IT部門の把握・管理外のクラウドサービス利用）の管理
- データの所在地・法的規制の把握
- 出口戦略の策定（サービス終了時のデータ移行計画等）

9. FISC安全対策基準との関係

FISC安全対策基準の概要

金融情報システムセンター（FISC）が策定する「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」（通称：FISC安全対策基準）は、金融機関の情報システムの安全性を確保するための具体的な技術と運用の対策を詳細に定めています。1985年の初版以来、時代の変化に合わせて改訂を重ね、2025年3月に最新の第13版が公表されました。

FISC安全対策基準の位置づけ

FISC安全対策基準は、金融機関のシステムリスク管理において業界標準として広く参照されている指針です。金融機関はこの基準を参考に自社のセキュリティ対策を検討・実施することで、適切なセキュリティレベルを確保することができます。また、外部委託先の評価基準としても活用されています。

金融庁ガイドラインとの整合性

2024年10月の金融庁ガイドライン公表を受け、2025年3月に公表されたFISC安全対策基準第13版では、金融庁ガイドラインとの整合性が取られています。金融機関は、金融庁ガイドラインで示されたサイバーセキュリティ管理態勢の枠組みを踏まえつつ、FISC安全対策基準に示された具体的な技術と運用の対策を参考にすることで、より効果的なサイバーセキュリティ対策を実施することができます。

観点	金融庁ガイドライン	FISC安全対策基準
主な目的	金融機関における経営陣をはじめとした組織全体のサイバーセキュリティ管理態勢の枠組みを示す	金融機関の情報システムの安全性を確保する具体的な技術と運用の対策を詳細に定める
対象範囲	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金融機関等	金融機関の情報システム全般

特徴	リスクベース・アプローチに基づき「基本的な対応事項」と「対応が望ましい事項」を明示	基礎基準と付加基準の2段階の要求レベルを設定し、具体的な実装方法を示す

第13版の重要ポイント

FISC安全対策基準第13版では、以下の内容を反映しています：

- 経済安全保障推進法に関する改訂：経済安全保障推進法における「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に係る取引を行う事業者が講ずべき安全管理措置等に関する対応指針」を踏まえた内容
- 金融庁ガイドラインとの整合：金融庁の「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」との整合性確保
- クラウドサービスの活用：クラウドサービスの普及を踏まえたセキュリティ対策の強化
- サードパーティリスク管理：サプライチェーンのセキュリティリスク管理の強化
- 最新の脅威への対応：新たなサイバー脅威に対する対策の追加

両者を活用したセキュリティ対策のポイント
金融機関は、金融庁ガイドラインとFISC安全対策基準を補完的に活用することで、より効果的なセキュリティ対策を実現できます：

1. 金融庁ガイドラインに基づいて経営レベルでのサイバーセキュリティ管理態勢を構築
2. FISC安全対策基準に基づいて具体的な技術対策と運用プロセスを整備
3. リスクベース・アプローチを採用し、自社の規模・特性に応じた対策レベルを設定
4. 定期的な評価と改善を通じて、セキュリティレベルの継続的な向上を図る

10. 今後の展望と対応のポイント

金融機関に求められる対応

金融庁ガイドラインとFISC安全対策基準の公表を受けて、金融機関は以下のような対応が求められています：

優先的に取り組むべき事項

1. 現状評価：ガイドラインに照らした自社のサイバーセキュリティ管理態勢の評価
2. 経営陣の関与強化：サイバーセキュリティを経営課題として位置づけ、経営陣の主体的関与を促進
3. 情報資産管理の徹底：情報資産の棚卸しと重要度に応じた管理の実施
4. 脆弱性管理の強化：セキュリティパッチ適用等の脆弱性管理プロセスの整備
5. アクセス権管理の改善：IDアクセス権限の適切な管理と定期的なレビュー
6. サードパーティリスク管理の強化：外部委託先のセキュリティリスクの評価と管理

中長期的な取り組み

1. サイバーセキュリティ戦略の策定：中長期的な視点でのサイバーセキュリティ戦略の策定と実行
2. 人材育成・確保：サイバーセキュリティ人材の育成・確保のための計画的な取り組み
3. 高度な対策の導入：AIや自動化技術を活用した先進的なセキュリティ対策の検討
4. レジリエンス強化：インシデント発生を前提とした対応力・復旧力の強化
5. 情報共有の促進：業界内外での脅威情報共有の活性化と活用

実効性ある対策の進め方

サイバーセキュリティ対策を効果的に進めるためのポイントは以下の通りです：

4つの主要施策

1. 経営陣の主体的関与と組織全体での対応
    - サイバーセキュリティを「経営リスク」としてとらえる
    - 経営陣は十分な専門知識を利用して判断（外部専門家の活用を含む）
    - KPI・KRIを用いたモニタリングの実施
2. インシデント発生を前提とした管理態勢
    - 対応プロセスの可視化
    - あらゆる脅威に対処できる管理態勢の整備
    - 様々なリスクシナリオの最新化と定期的な訓練の実施
3. サプライチェーン全体を考慮した管理態勢
    - 外部委託先の特性に基づき想定される脅威に応じた管理・モニタリング
    - 契約内容へのセキュリティ基準の明示
    - 定期的な監査の実施
4. セキュリティ技術基盤の連携と統合管理
    - 資産管理の徹底（ハードウェア、ソフトウェア、クラウドサービス、データ等）
    - 「ゼロトラスト」の考え方に基づく段階的な技術導入
    - 組織全体での共通の方向性や計画の策定

官民連携と情報共有の重要性

金融セクター全体のサイバーセキュリティ強化には、「自助」「共助」「公助」の三位一体の取り組みが重要です。特に、以下の連携・情報共有の枠組みを活用することが推奨されます：

- 金融ISAC：金融機関同士の脅威情報共有・分析
- 国家サイバー統括室（旧NISC）：政府全体のサイバーセキュリティ対策との連携
- JPCERT/CC：脆弱性情報や対策情報の入手
- 業界団体・中央機関：業界全体のサイバーセキュリティ強化のための支援

最後に

サイバーセキュリティは、単なる規制対応ではなく、金融機関の事業継続と顧客保護のために不可欠な要素です。経営陣をはじめとした組織全体で、サイバーセキュリティ対策の継続的な強化と実効性の検証を行うことが重要です。また、サイバーセキュリティへの対応は自社だけで完結できるものではなく、外部のリソースや専門的な知見の活用も有効です。

金融庁は引き続き、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としています。モニタリングにおいては、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ことに留意するとしています。

監修者：
鎌田光一郎:青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティンク゛合同会社に転籍。金融機関に対するコンサルティンク゛業務に従事。その後、Librus株式会社を設立、代表取締役に就任。

お問い合わせ先
Librus株式会社（代表取締役 鎌田光一郎）
105-0004東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F
03-6772-8015

お問い合わせフォーム
https://librus.co.jp/contact