資料３－１

金融庁
Financial Services Agency

金融庁におけるサイバーセキュリティに関する取組状況

2024年10月

金融庁総合政策局リスク分析総括課
ITサイバー・経済安全保障監理官室

目次

１．2024事務年度　金融行政方針

2024事務年度　金融行政方針（抜粋）

II．金融システムの安定・信頼と質の高い金融機能を確保する

１．業態横断的な課題への対応

（６）台頭するリスクへの対応

③ サイバーセキュリティの強化

技術の発展や地政学リスクの高まりを背景に、近年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る。例えば、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り金融機関でも被害が発生しているほか、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が出現している。

こうした環境変化を踏まえ、政府としてサイバーセキュリティに関する取組を一層強化する中、金融市場インフラや金融商品取引所を含めた金融業界全体のサイバーレジリエンス向上を図るべく、各金融機関による「自助」の取組、金融業界による「共助」の取組、当局による「公助」を一層促進するとともに、国際的な議論への参画や海外当局等との連携を深化させる。

具体的には、金融システム上の重要性・リスクなどを勘案の上、新たに策定した「**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**」（2024年６月パブリックコメント案公表）の運用などを通じて、金融機関におけるサイバーセキュリティ管理態勢の強化を促す。また、**金融機関がサイバーセキュリティ管理態勢の成熟度を自己評価するためのツールの提供**や、**金融業界横断的なサイバーセキュリティ演習の実施**、**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の実施促進**などに取り組む。

金融庁ウェブサイト：https://www.fsa.go.jp/news/r6/20240830/20240830.html

2. 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(案)の概要

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(案)について

（参照）金融庁「「主要行等向けの総合的な監督指針」等の一部改正（案）及び「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」（案）の公表について」（2024年６月28日）
https://www.fsa.go.jp/news/r5/sonota/20240628-2/20240628.html

経緯及び趣旨

- 現行の各業態の監督指針・事務ガイドライン（以下、監督指針等）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、当該規定の改定が不可欠となっている。
- 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。

上記の実態に鑑み、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

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
- 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

- 金融機関等の規模・特性は様々
- そのため、いずれの事項についても、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）が必要
- 重要性・緊急性に応じて優先順位をつけたうえ、リソース制約を踏まえ、順次対応することが必要

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(案)の概要

※変更可能性あり

（検査・モニタリングにおける発見事項等）

対策が不十分な領域

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

サイバーリスクの動向（例）

- サードパーティ・サプライチェーンのサイバーセキュリティリスク（クラウドに係るものを含む）

（現行監督指針・事務ガイドライン）

- 取締役会等による態勢整備
- 組織体制整備、社内規程作成、監視、広報、CSIRT及び情報収集・共有体制の整備
- 入口、内部、出口対策
- サイバー攻撃の被害拡大防止措置
- 脆弱性対策（OSの最新化、セキュリティパッチの適用等）
- 侵入検査、脆弱性診断等の実施
- 非対面取引のセキュリティ確保（認証、検知等）
- 不正なオンライン取引防止のための手続き策定
- コンチプラン策定、訓練、見直しの実施、演習への参加
- 人材育成計画の策定、実施

これらに対応・底上げを図るため、ガイドラインに詳細を規定。

サイバーセキュリティに係る国内外のフレームワーク等（※）とも整合させる。

（ガイドラインの構成）

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
1.2. 金融機関等に求められる取組み
1.3. 業界団体や中央機関等の役割
1.4. 本ガイドラインの適用対象等

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
2.2. サイバーセキュリティリスクの特定
2.3. サイバー攻撃の防御
2.4. サイバー攻撃の検知
2.5. サイバーインシデント対応及び復旧
2.6. 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

3.1. 情報共有・情報分析の強化
3.2. 捜査当局等との連携
3.3. 国際連携の深化
3.4. 官民連携

※ サイバーセキュリティ戦略本部による「重要インフラのサイバーセキュリティに係る行動計画」（2022年６月）、「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」（2023年７月）、金融情報システムセンターによる「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」、米国National Institute of Standards and Technology （NIST：国立標準技術研究所）によるCybersecurity Framework (CSF) 2.0（2024年2月）、米国Cyber Risk InstituteによるThe Profile v2.0（2024年2月）、CPMI-IOSCOによるGuidance on cyber resilience for financial market infrastructures（2016年6月）、G7サイバー・エキスパート・グループ（CEG）による各種「基礎的要素」など。

（以下、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(案)の詳細）

経営陣の主体的な関与・ガバナンス

ガイドライン案1.2.2節、2.1節
※変更可能性あり

- サイバーインシデントによる業務中断、機密情報の漏えいは、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
- 他のトップリスク、経営資源の制約とのバランスは必要だが、サイバーセキュリティの強化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**であることを明記

基本的な対応事項

- 基本方針、組織体制、管理態勢など
  - ✓ 基本方針、戦略・取組計画の策定
  - ✓ サイバーセキュリティに係る組織体制・管理態勢の整備
  - ✓ DXにおけるサイバーセキュリティの織込み（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の確保に向けた組織風土の醸成
  - ✓ 重要な業務やリスクの把握とそれに応じた対策の推進
  - ✓ サイバーセキュリティ担当の役割・責任・権限の明確化（サイバーセキュリティを統括する責任者の任命を含む）
  - ✓ 経営陣への報告の体制
  - ✓ 継続的改善
- リソースの確保、人材の育成
  - ✓ 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
  - ✓ 基本方針と整合的な人材育成・確保計画の策定
  - ✓ 経営陣を対象とする研修・訓練
- リスク管理部門による牽制
- 内部監査

対応が望ましい事項

- 専門知識の利用可能性の確保
- リスク選好度・耐性度の設定
- 取組の対外公表
- KPI・KRI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

リスクの特定

ガイドライン案2.2節
※変更可能性あり

これまでの検査・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・事項（**情報資産管理、脆弱性管理、定期的な脆弱性診断・ペネトレーションテストの実施、IDアクセス権管理**など）を含めて規定

基本的な対応事項

- 情報資産管理
  - ✓ 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
  - ✓ 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
- ハードウェア・ソフトウェア等の脆弱性管理
  - ✓ 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
- 脆弱性診断・ペネトレーションテストの定期的な実施
- 演習・訓練の定期的な実施
  - ✓ 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

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）の実施　など

防御

ガイドライン案2.3節
※変更可能性あり

基本的な対応事項

- 多層防御
- 認証・アクセス管理
  - ✓ 方針・規程等の策定・見直し
  - ✓ アクセス権限の限定
  - ✓ ID・認証情報の適切な管理
  - ✓ アクセスの検証
  - ✓ システム・情報の重要度に応じた認証要件の決定
  - ✓ 第三者による不正防止（メールの送信ドメイン認証など）
  - ✓ シングルサインオン・外部認証連携などのシステム間又はセキュリティ境界にまたがる認証等のセキュリティ確保
  - ✓ 物理的アクセスの管理
- 教育・研修
  - ✓ 経営陣を含むすべての役職員への教育・研修の実施
  - ✓ 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）
- データ保護
  - ✓ 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
  - ✓ バックアップ・復旧に係る手続の整備　　など
- システムのセキュリティ対策
  - ✓ 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　　など

検知、対応・復旧

ガイドライン案2.4、2.5節
※変更可能性あり

サイバー攻撃の巧妙化を踏まえ、侵入を前提に、検知及び対応・復旧について詳細を規定

基本的な対応事項

- サイバー攻撃の検知
  - ✓ 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　　など
- サイバーインシデント対応
  - ✓ 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
  - ✓ 初動対応、分析、顧客対応・組織内外の連携・広報、封じ込め、根絶
- 復旧
  - ✓ 復旧計画における復旧判断権者・判断要素の整理
  - ✓ 被害を受けた機器の初期化・正常稼働の確認
  - ✓ バックアップデータ改ざんの可能性の考慮
  - ✓ 復旧手順の確認
  - ✓ 復旧後のインシデント発生原因等の分析及び対応の評価の実施

  など

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
- 封じ込めに当たってのサードパーティへの通知　　など

サードパーティリスク管理

ガイドライン案2.6節
※変更可能性あり

- 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も踏まえ、サードパーティリスク管理について詳細を規定
- 金融機関等にサービスを提供するサードパーティは、金融機関に対して必要な支援を行うべきであることも記載

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
- 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
  - ✓ サイバーセキュリティ要件の契約・SLAにおける明確化
  - ✓ 継続的モニタリング
  - ✓ インシデント対応計画・コンチプラン
  - ✓ 出口戦略
- 体制整備・組織内規程の策定
- リスク評価・リスクに応じた対応

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

3. 耐量子計算機暗号（PQC）への対応に関する検討会の開催

耐量子計算機暗号（PQC）への対応

令和６年７月４日
金融庁

「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」の開催について

１．趣旨

量子コンピュータが実用化されると、現在広く利用されている公開鍵暗号の安全性が損なわれることが指摘されており、耐量子計算機暗号（Post-Quantum Cryptography、PQC）への移行に向けた検討が国内外で始まっています。金融庁では、金融分野における課題や留意事項について、幅広い関係者と議論を行ってきました。

今般、上記の検討の一環として、PQCへの移行を検討する際の推奨事項、課題及び留意事項について関係者と更に検討するため、本検討会を開催します。

２．構成

▸「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」メンバー等名簿（PDF：261KB）

３．会議の開催について

第１回目の会議を令和６年７月18日（木曜）に開催する予定です。
会議は非公開としますが、会議後、議事要旨を金融庁ウェブサイト上で公表する予定です。

「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」

メンバー等名簿

（敬称略、五十音順）

座長	寺井　理	株式会社みずほフィナンシャルグループ グループ執行役員・情報セキュリティ担当（グループ CISO） 金融 ISAC FinTech セキュリティワーキンググループ座長
メンバー	安藤　彰英	株式会社名古屋銀行　執行役員　業務部長
	岩崎　三郎	株式会社静岡銀行　リスク統括部長
	宇根　正志	日本銀行　金融研究所　参事役
	大城　徹	株式会社しんきん情報システムセンター　上席執行役員
	菅野　洋平	労働金庫連合会　情報システム部　副部長
	白井　大輔	株式会社三井住友フィナンシャルグループ グループ CISO
	高瀬　徹	農林中央金庫　IT 統括部部長（システムリスク管理担当）
	松本　泰	特定非営利活動法人日本ネットワークセキュリティ協会 フェロー
	峰　匡親	株式会社三菱 UFJ フィナンシャル・グループ グループ CISO　サイバーセキュリティ推進部　部長
	村山　朋彦	信組情報サービス株式会社　常勤取締役
オブザーバー	一般社団法人金融 ISAC、CRYPTREC 事務局、公益財団法人金融情報システムセンター、日本銀行　金融機構局、内閣サイバーセキュリティセンター	
事務局	金融庁	

引用元：金融庁 https://www.fsa.go.jp/singi/pqc/index.html