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施策の取組状況について

2023年12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

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（Ver. 3.0）

～サイバーセキュリティを確保し、安心・安全かつ利便性の高い金融サービスの実現へ～

サイバー空間の変化

- 国家の関与が疑われる**組織化・洗練化されたサイバー攻撃**や、国際的なハッカー集団等による**ランサムウェア攻撃の多発**
- デジタライゼーションの進展による**金融サービスの担い手の多様化**と、キャッシュレス決済などの**連携サービスの進展**
- クラウドサービスをはじめとした**外部委託の拡大、サプライチェーンの複雑化・グローバル化**等による**リスク管理の難度の高まり**

新たな取組方針（以下、５項目）

１．モニタリング・演習の高度化

金融機関の規模・特性やサイバーセキュリティリスクに応じて、検査・モニタリングを実施し、サイバーセキュリティ管理態勢を検証する。
共通の課題や好事例については業界団体を通じて傘下金融機関に還元し、金融業界全体のサイバーセキュリティの高度化を促す。特に

- ✓ 3メガバンクについては、**サイバー攻撃の脅威動向の変化への対応**や**海外大手金融機関における先進事例**を参考にしたサイバーセキュリティの高度化に着目しつつ、モニタリングを実施する
- ✓ 地域金融機関については、**サイバーセキュリティに関する自己評価ツールを整備**し、各金融機関の自己評価結果を収集、分析、還元し、**自律的なサイバーセキュリティの高度化を促す**
- ✓ サイバー演習については、引き続き、**サイバー攻撃の脅威動向**や**他国の演習**等を踏まえて高度化を図る

２．新たなリスクへの備え

- ✓ **キャッシュレス決済サービス**の安全性を確保するため、リスクに見合った**堅牢な認証方式の導入等**を促す**（セキュリティバイデザインの実践）**
- ✓ クラウドサービスの安全な利用に向けて、**利用実態**や**安全対策**の把握を進めるとともに、**クラウドサービス事業者との対話**も実施

３．サイバーセキュリティ確保に向けた組織全体での取組み

- ✓ 経営層の積極的な関与の下、**組織全体でサイバーセキュリティの実効性**の向上を促す（セキュリティ人材の育成も含む）

４．関係機関との連携強化

- ✓ サイバー攻撃等の情報収集・分析、金融犯罪の未然防止と被害拡大防止への対応を強化するため**関係機関（NISC、警察庁、公安調査庁、金融ISAC、海外当局等）との連携を強化**

５．経済安全保障上の対応

- ✓ 政府全体の取組みの中で、機器・システムの利用や業務委託等を通じたリスクについて適切に対応を行う

金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅷ）について

金融分野のサイバーセキュリティを巡る状況

- 世界各国において、大規模なサイバー攻撃が発生しており、攻撃手法は一層高度化・複雑化
- 我が国においても、サイバー攻撃による業務妨害、重要情報の窃取、金銭被害等の被害が発生している状況
- こうしたサイバー攻撃の脅威は、金融システムの安定に影響を及ぼしかねない大きなリスクとなっており、金融業界全体のインシデント対応能力の更なる向上が不可欠

これまでの演習の概要

- ✓ 過去7回、演習を実施
- ✓ 2016年度は77先・延べ約900人、2017年度は101先・延べ約1,400人、2018年度は105先・延べ約1,400人、2019年度は121先・延べ約2,000人、2020年度は114先・延べ約1,700人、2021年度は150先・延べ約2,700人、2022年度は160先・延べ約3,500人が参加
- ✓ 参加金融機関の多くが規程類の見直しを実施・予定しているほか、社内及び外部組織との情報連携の強化に関する対応を実施・予定しており、本演習を通じて対応態勢の改善が図られている

金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅷ）

- 2023年10月、**金融庁主催による8回目の「金融業界横断的なサイバーセキュリティ演習」（Delta Wall Ⅷ（注））を実施**

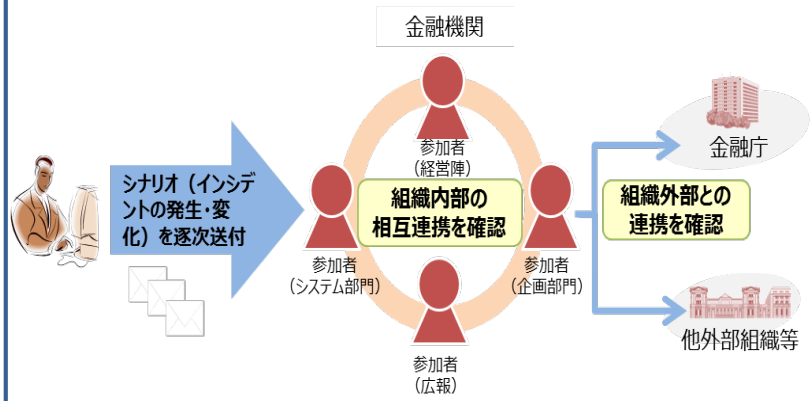
（注）Delta Wall: サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の3つの視点（Delta）＋防御（Wall）

- 昨年度対象外としていた保険会社を対象としつつ、重要インフラ事業者の参加率向上の観点から、**165先が参加**（昨年度から5先増）
- 銀行業態については、これまでの演習の成熟度を踏まえ、重要な業務に影響が波及するようなシナリオで難度を高めつつ、インシデント時の業務の優先度など経営層を含めたディスカッションの内容や十分性を検証。その他のシナリオについてもインフラシステムの停止等を含め難度を高めつつ、演習の高度化を図る
- 昨年度に引き続き、テレワーク環境下での対応も含めたインシデント対応能力の向上を図るため、**参加金融機関は自職場やテレワーク環境下で演習に参加**

演習の特徴

- ✓ インシデント発生時における**初動対応、技術的対応を含めた攻撃内容の調査・分析、封じ込め・根絶、顧客対応、復旧対応等の業務継続**を確認
- ✓ 経営層や多くの関係部署（システム部門、広報、企画部門等）が参加できるよう、**自職場参加方式**で実施
- ✓ 対応できなかった項目の自己分析結果を提出することとし、評価の要因を明確化することで、演習効果を高める
- ✓ 参加金融機関がPDCAサイクルを回しつつ、対応能力の向上を図れるよう、具体的な改善策や優良事例を示すなど、**事後評価に力点**
- ✓ 本演習の結果は、参加金融機関以外にも**業界全体にフィードバック**

演習スキーム



【演習シナリオの概要】

- **銀行**
  - ✓（ブラインド方式のため非開示）
- **信金・信組**
  - ✓ 業務システムや端末の停止等が発生（業態内インフラシステムの停止含む）
- **証券**
  - ✓ 業務システムの停止等が発生（証券インフラシステムの一部停止含む）
- **生命保険会社・損害保険会社・資金移動業者・前払式支払手段発行者・暗号資産交換業者**
  - ✓ ネットワーク機器の脆弱性を端緒とした業務システムの停止等が発生