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