金融分野のサイバーセキュリティレポート（令和2年6月）の概要

背　景

○「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」（2018年10月アップデート）に基づき、これまで官民が一体となって、金融分野のサイバーセキュリティ強化に向けた取組みを実施

○ 同取組方針に基づく令和元事務年度の取組みにおいて、把握した実態や共通する課題等を取りまとめレポートとして公表

1．金融分野を巡るサイバーセキュリティの現状について

（1）近年の脅威動向等

- 国内金融機関においては、これまでに大規模なサイバーインシデントは発生していないものの、**攻撃者が金融機関などを装った偽のウェブサイトに利用者を誘導**し、**不正送金やクレジットカード情報が窃取される**等の被害が発生。
- 海外金融機関においては、**個人情報の漏えいやサービスの停止につながる大規模なサイバーインシデント**が発生。

（2）国内金融機関のサイバーインシデントについて

- **リスト型攻撃による不正ログインやDDoS攻撃に関する報告**が多く、他金融機関においても同様のインシデントが発生する恐れがあることから、2019年10月、**金融機関に注意喚起を発出**し、所要の対応を求めた。
- 今後も**新たな脅威や脆弱性をタイムリーに把握・分析**し、金融分野のサイバーセキュリティ管理態勢の強化を図る必要。

（3）新型コロナウイルス感染症等によるサイバーセキュリティへの影響

- **新型コロナウイルス感染症に便乗したサイバー攻撃**や**テレワーク環境を狙ったサイバー攻撃**などが数多く発生。
- 国内金融機関では、重大な問題は発生していないものの、**テレワークを活用した新しい働き方や金融サービスの電子化が一層進展することが想定**されるため、**セキュリティ対策にも留意していく必要**。

金融分野のサイバーセキュリティレポート（令和2年6月）の概要

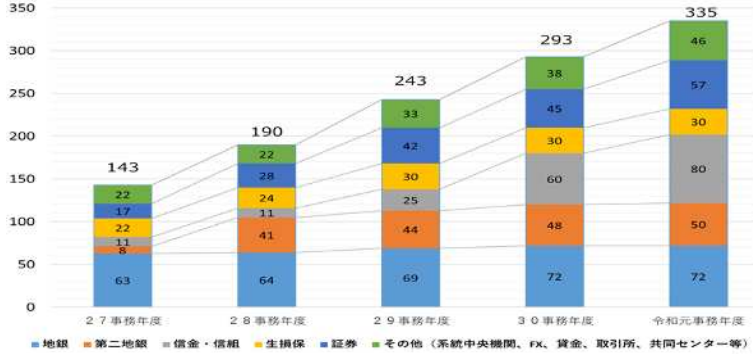
2. 金融分野のサイバーセキュリティ強化に向けた取組み状況 （1/3）

（1）①平時のサイバー対策

ア. 中小金融機関等

- ✓ これまで、中小金融機関については、実態把握（対話によるモニタリング）を通じて、基礎的なサイバーセキュリティ管理態勢の整備状況を検証
- ✓ 令和元事務年度は、業界全体の底上げの観点から、基礎的なサイバーセキュリティ管理態勢の整備の遅れが懸念される先を中心に、実態把握を実施

【業態別実態把握先の推移（実態把握先の累計（2巡目含む））】



業態名	取組結果等の概要
地域銀行・信金・信組	・一部の先では、自主的に強化を図っている状況。他方、**依然として基礎的な態勢整備に課題**がある先もみられた ・課題がみられた先については、**経営陣が主体となった取組みの推進態勢の整備**を促進
証券会社等	・取組みが進展している金融機関が増えている一方、**依然として取組みの進展が停滞状態**の先もみられた ・課題がみられた先については、**経営陣が主体となった取組みの推進態勢の整備**を促進

イ. 大手金融機関等

- ✓ これまで、大手金融機関については、グローバルな動向等を念頭に、定期的な対話を通じて議論
- ✓ 令和元事務年度は、高度化が期待されるグループ・グローバルの管理態勢の高度化、TLPTの活用状況を中心に確認
- ✓ また、信託銀行やネット銀行等については、アンケートを通じたオフサイトモニタリングを実施

業態名	取組結果等の概要
3メガグループ等	・**グループ・グローバルベースの一元的な管理態勢の高度化**に取り組んでいる。**アクセスコントロールの強化、サイバーレジリエンスの高度化**等を通じて、管理態勢の強化を図っていくことを期待 ・TLPTをより実効性のあるものとするため、**各種ガイドラインへの準拠**に加え、**国際的なフレームワーク を活用したインシデント対応能力の評価等の高度化、高度な専門人材の育成**を継続することを期待
信託・ネット銀行等	・サイバーセキュリティの高度化に向けた取組みを推進している先がみられた。他方、一部銀行では、**経営陣が主体となった取組推進やリスク認識に改善の余地**がみられ、意見交換を通じて課題を共有し自主的な改善活動を促進

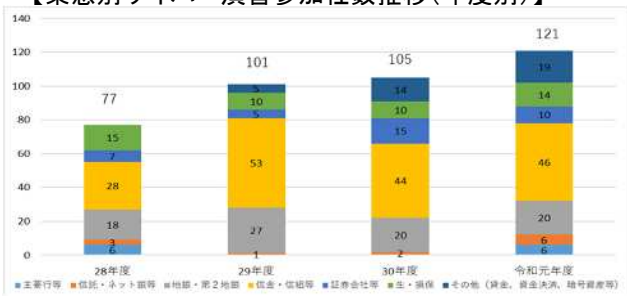
金融分野のサイバーセキュリティレポート（令和2年6月）の概要

2. 金融分野のサイバーセキュリティ強化に向けた取組み状況 （2/3）

（1）②有事のサイバー対策

- 金融庁では、毎年、金融機関の対応能力強化を図るため、「金融業界横断的なサイバーセキュリティ演習（Delta Wall）」を実施
- 令和元事務年度は、東京2020大会に向け、業界全体の底上げの観点から中小・大手金融機関に加え、資金移動業者等が参加（121社（約2,000名））
- 金融庁のほか、様々な団体が多様な演習を実施しており、こうした演習への参加を通じて**インシデント対応能力の更なる向上を図っていくことが重要**

【業態別サイバー演習参加社数推移（年度別）】



業態名	金融業界横断的なサイバーセキュリティ演習結果の概要
大手銀行、地域銀行	・全般として対応が概ねできていたものの、**復旧対応や顧客対応に課題**が一部みられた ・**金融機関内での深度ある議論が求められるような形式**とするなど、更なる高度化を図っていく
その他	・**トリアージや顧客対応、再発防止策の検討など、全体的に改善の余地**がみられた ・引き続きインシデント対応能力の向上を図っていく必要

（1）③東京2020オリンピック・パラリンピック競技大会の開催を見据えた管理態勢の強化

- 東京2020大会の開催を見据え、金融機関のサイバーセキュリティ管理態勢の強化に向けた取組みを実施

ア. 基礎的なサイバーセキュリティ管理態勢の実効性向上

業態名	取組結果等の概要
地域銀行、信金・信組	・2020年3月末までに、**①脆弱性診断、②演習・訓練、③監視・分析状況の整理等、を実施するよう要請** ・多くの金融機関は上記①～③の**実施を完了**。一部は対応に遅れがみられ、**協会と連携しフォロー**を実施
その他 （都市銀行、資金決済事業者、証券、生損保、貸金業等）	・上記①～③の各事項について確認 ・特段の課題はみられなかったが、今後も必要に応じて取組み状況の把握やフォローを実施

イ. 要請対応やアンケートを通じて把握した事例や実効性向上への課題

要請事項	良好・課題事例
脆弱性診断	・リスクを踏まえ計画的に診断を実施する先がある一方、リスク認識不足で対策実施が停滞している先がみられた
演習・訓練	・演習・訓練によりコンチプランを見直している先がある一方、参加後の振返り等を実施していない先がみられた
監視・分析	・インシデントの早期検知・分析態勢を整備している先がある一方、ログの確認・分析には至っていない先がみられた

金融分野のサイバーセキュリティレポート（令和2年6月）の概要

2. 金融分野のサイバーセキュリティ強化に向けた取組み状況 （3/3）

（1）④デジタライゼーションの加速的な進展を踏まえた対応

- 国内外の金融機関やITベンダー等にヒアリングを行い、デジタライゼーションの進展状況等の把握・分析を実施

ア. クラウドサービス全般
- ✓ 大手金融機関では、**研修の受講、認定資格保有者数の目標設定、新サービスの説明会やイベントへの参加**等を通して、新サービスの早期活用、継続的なスキルアップを図っている

イ. 新たなセキュリティモデルへの転換
- ✓ 大手金融機関では、**ゼロトラストを意識したセキュリティ対策に本格的に取り組む**動きがみられる

（2）①情報共有の枠組みの実効性向上

- これまで、「共助」の意義について、機会を捉えて、金融機関に周知してきたところ、**金融ISAC の加盟金融機関数は着実に増加**
- 今後、さらなるサイバーセキュリティ強化を図るためには、**業界団体との連携等を一層充実**させていくことにより、サイバーセキュリティ対策の提供を含めた「共助」を深化していくことが期待され、引き続きこうした活動を積極的に支援

（2）②大規模インシデント発生時の連携

- サイバーセキュリティ対策関係者連携会議（2019年6月立上げ）を活用し、東京2020大会の開催を見据えた大規模インシデント発生時の連携態勢について、**連携手順の整備やサイバー演習等を通じて業界全体の連携態勢**を強化
- 今後は、**情報共有システムを利用したメンバー間での情報連携**について、**演習により有効性・実効性**等を確認

（2）③国際的な連携

- 2019年6月、大規模なサイバーインシデントの発生を想定した合同演習を実施し、G7諸国の当局を中心とした**クロスボーダーの連携を確認**
- 最近の国際的な議論においては、クラウドサービスなどの**サードパーティやサイバーインシデントからの復旧・回復といったレジリエンス**の考え方が取り上げられ、こうした議論を含め**国際的な動向を的確に把握・対応**していくことが重要

3. 当局の今後の取組み

○ 新型コロナウイルス感染症の拡大に伴う外部環境の変化や2021年に延期された東京2020大会など、金融機関を取り巻くサイバーリスクは一層高まっている状況

○ 今後当局としても、金融分野における更なるサイバーセキュリティ対策の強化を図っていくために、以下の取組みを重点的に推進

金融分野の環境変化への対応

- 金融分野では、デジタライゼーションが進展する中、新型コロナウイルス感染症への対応としてオンライン化・リモート化が加速しており、金融機関を取り巻く環境は大きく変化。こうした新たな金融サービス・インフラの前提として、サイバーセキュリティの確保はますます重要な課題
- 金融庁としては、こうした環境の変化を踏まえた新たなセキュリティに関する脅威の動向について、**デジタライゼーションの進展を踏まえたサイバーセキュリティへの取組みとあわせて、積極的に情報収集**を行い、**必要な対応を促進**

金融機関のサイバーセキュリティ強化に向けた対応

- 中小金融機関に対しては、**業界団体等との連携を通じた基礎的なサイバーセキュリティ管理態勢の実効性の維持・向上**を促すとともに、**サイバー演習によりインシデント対応能力の底上げ**を図る。また、**各業態の取組みに進展がみられる先との意見交換**を通じてプラクティスを収集し、好事例を積極的に還元
- 大手金融機関に対しては、国際的な議論の動向を念頭に、**グループ・グローバルベースでのサイバーセキュリティに関するリスク管理の高度化、TLPTの実効性向上**を通じたサイバーセキュリティ対策のより一層の高度化を促進。また、検知の遅れにより長期間ネットワーク内で活動するリスク等を踏まえ、**サイバーレジリエンスへの取組み**についても対話を行う