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）の概要

資料3

背　景

○ 2015年7月、「金融分野のサイバーセキュリティ強化に向けた取組方針」を策定・公表し、同方針に沿った取組みを推進

○ デジタライゼーションの加速的な進展、国際的な議論の進展、2020年東京オリンピック・パラリンピック競技大会の開催など、近年、金融機関を取り巻く状況が大きく変化。加えて、政府全体の基本戦略である「サイバーセキュリティ戦略」の改訂（2018年7月）等を踏まえ、同方針をアップデート

本取組方針の目的

○ 新たな課題に対応するとともに、これまでの取組みの進捗・評価を踏まえ、官民が緊密に連携を図り、金融分野のサイバーセキュリティ対策の更なる強化を図る

目的達成のための主な施策

新たな課題への対応

1．デジタライゼーションの加速的な進展を踏まえた対応

- ✓ デジタライゼーションの進展が金融業に与える影響、**サイバーセキュリティに係るリスクやその対応策等について把握・分析**に取り組む
- ✓ **変化への対応を金融機関に促す**とともに、こうした変化に対応した当局のモニタリングのあり方等について検討

2．国際的な議論への貢献・対応

- ✓ **サイバー攻撃に国際的に協調して対応するため**、G7財務大臣・中央銀行総裁会議をはじめとするサイバーセキュリティに関する国際協調の議論に対して、**各国当局と連携しつつ貢献・対応**していく

3．2020年東京オリパラ大会等への対応

- ✓ 金融分野の連携態勢を整備するため、**関係省庁、関係団体との連携を一層緊密にし、危機管理態勢を構築**
- ✓ サイバー攻撃の増加、各分野を跨がるような攻撃や大規模インシデントの発生などに備え、**広く情報収集・分析**に取り組む

これまでの進捗・評価を踏まえた施策の推進

1．金融機関のサイバーセキュリティ管理態勢の強化

ア.平時のサイバー対策

大手	✓ **海外の動向を念頭**に対話を通じて**より一層の高度化**を促す
中小	① **業界団体を通じた底上げ**（業界の共通課題等について幅広く問題提起を行い必要な対応を促す） ② 実態把握（基礎的な態勢整備と脆弱性診断等の実効性確認） ③ 立入検査（自主的改善が見込まれない等リスクが高い場合）

イ.インシデント対応

大手	✓ 国際的な合同演習への参加、**実践的な侵入テスト（TLPT）の実施**
中小	✓ **金融庁演習**（内容は継続的に見直し）、NISC等の演習への参加

2．情報共有の枠組みの実効性向上

- ✓ 「共助」の取組みの第一歩となるよう、金融ISAC・FISC等とも連携し**地域内の情報共有**を推進

3．金融分野の人材育成の強化

- ✓ 財務（支）局とも連携し**経営層向け地域 セミナー**を全国的に開催
- ✓ 「サイバーセキュリティ戦略」で掲げられた、「戦略マネジメント層」の育成・定着に向けて、海外や他分野の優良事例等を収集し還元

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

金融分野のサイバーセキュリティを巡る状況

- 昨今、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個人情報の大規模な漏えいや、複数の中小金融機関が狙われるサイバー攻撃が発生しており、攻撃の裾野も拡大
- 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2回演習を実施。28年度は77先・延べ約900人、29年度は101先・延べ約1,400人が参加
- これまでの演習において、銀行業態は他業態と比較して必要なインシデント対応を実施。一方、多くの中小金融機関（信金・信組、中小証券、中小保険等）は、シナリオで提示された攻撃への対応のみに目がいきがちであるなど、インシデント発生時におけるより広い視野での対応に課題

金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅲ）

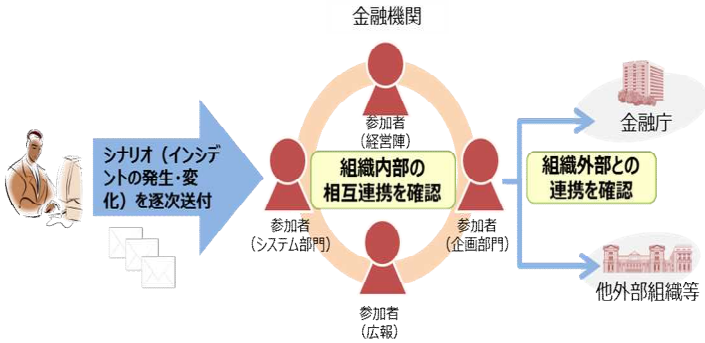
- 本年10月末、特に中小金融機関のインシデント対応能力の底上げを図ることを目的に、**金融庁主催による3回目の「金融業界横断的なサイバーセキュリティ演習」（Delta Wall Ⅲ（注））を実施**

  （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）
- 昨今の脅威動向を踏まえ、**新たな業態**としてFX業者、仮想通貨交換業者**を追加**し、**約100社が参加**
- 共通シナリオだけでなく、業務特性を反映した**業態毎のシナリオ**も実施。地銀・第二地銀については成熟度を踏まえ、より実践的な、シナリオの骨子を事前開示しない「**ブラインド方式**」を採用

演習の特徴

- 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（⇔会場集合方式）
- 民間の**専門家の知見や攻撃の実例分析等を参考**にしつつ、金融機関が陥りやすい弱点が浮き彫りとなり、**参加者が「気づき」を得る**ことができる内容
- 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



【シナリオの一例】

Webサイトの改ざん（信金、信組、労金）

- ✓ 顧客より、利用していないにも関わらずオンラインサービスの利用通知が届いたとの問合せ
- ✓ Webサイトが改ざんされ、HPを閲覧するとフィッシングサイトに誘導され、ログインID・パスワードを不正に入力させられることが発覚
- ✓ 改ざんの原因がWebサイトの脆弱性であることが判明

オンラインサービスページへのDDoS攻撃（証券、FX）

- ✓ DDoS攻撃が発生し、顧客から、オンラインサービスへのアクセスが行えないとの問合せ
- ✓ DDoS攻撃と並行して、標的型メール攻撃により職員の端末がフリーズし、犯人からの身代金を要求する脅迫文が表示
- ✓ DDoS攻撃は収束し、攻撃の種類が判明