金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅳ）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、サイバー攻撃は大手金融機関のみならず、中小金融機関や暗号資産交換業者にまで拡大しており、実効性のあるサイバーセキュリティ対策は急務
- 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3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人が参加
- 多くの金融機関がコンチプラン等の見直しや社内外の情報連携強化に向けた対応を実施し、演習を通じて対応態勢を改善。一方、インシデント対応時における委託先との連携や顧客対応等が不十分、インシデント対応に必要な人員が確保できていないなどの課題が認められ、対応能力の向上を図っていく必要

金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅳ）

◆ 本年10月上旬、2020年東京オリパラ大会に向けた、大規模インシデントの発生に備え、中小金融機関のみならず大手金融機関等も参加して、**金融庁主催による4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 Ⅳ（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）

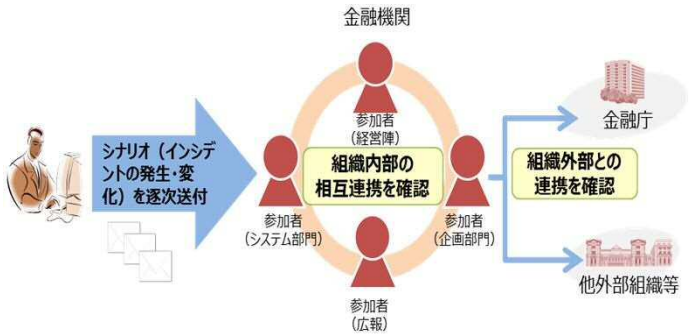
◆ 本演習の対象となっていなかった業態（資金移動業者、前払式手段発行者、監査法人等）**を追加**し、**約120社が参加**

◆ **2020年東京オリパラ大会の開催時におけるリスク等を想定したシナリオ**とし、預金取扱金融機関・証券会社等向けシナリオとその他業界向けシナリオで実施

演習の特徴

- インシデント発生時における金融機関内外の情報連携に係る対応体制や手順の確認を目的とした**机上演習**
- 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



【演習シナリオの概要】

預金取扱金融機関、証券会社等向け

- ✓ 東京2020大会開催期における、ネットワーク障害の発生及びホームページへのDDoS攻撃
- ✓ 他の金融機関との連携を担うネットワーク機器異常による決済システムの停止
- ✓ システム異常の原因及びDDoS攻撃の種類が判明

その他業界（生損保、暗号資産交換業者、監査法人等）向け

- ✓ 東京2020大会に関わるサイバー攻撃についての注意喚起
- ✓ ホームページへのDDoS攻撃、標的型メール攻撃
- ✓ DDoS攻撃の種類及びインシデントの発生原因が判明