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

資料４－２

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

- 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）

◆ 30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）

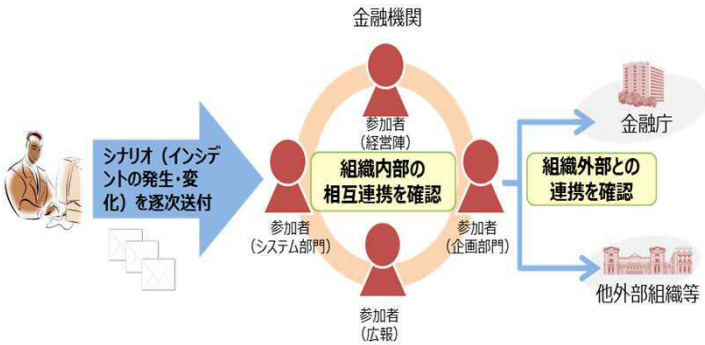
◆ 昨今の脅威動向を踏まえ、**新たな業態**としてFX業者、仮想通貨交換業者**を追加**し、**約100社が参加**

◆ 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