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

資料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・多様化
- 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
- サイバー攻撃は金融システムの安定に影響を及ぼしかねない大きな脅威となっており、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

## 前回（初回）の演習概要

- 77金融機関（銀行、信金・信組、証券、生損保）、延べ約900名が参加
- 大手金融機関は、概ね想定されるインシデント対応を実施していた一方、多くの中小金融機関は、①外部からの情報収集、②業務・顧客への影響評価、③再発防止策を検討・実施した上での復旧、等の対応が不十分

## 金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅱ）

◆ 本年10月末、金融業界全体の更なる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2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 Ⅱ（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）

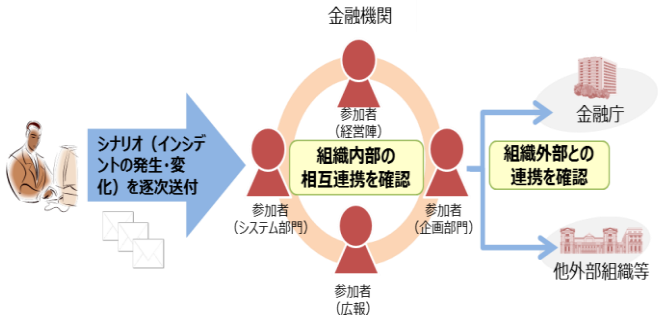
◆ **中小金融機関の参加枠の拡充**に加え、**新たな業態**として労働金庫、貸金業者**を追加**し、**約100社が参加**

◆ 前回の演習で判明した課題について、**具体的な対応**が確認できるシナリオを作成

### 演習の特徴

- 演習実施までの間に自主的なインシデント対応能力の向上を促すために、**シナリオの骨子を事前に開示**（オープンシナリオ方式）
- 多くの関係部署（経営層、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、**参加者に「気づき」を与える**ことができる内容
- 参加金融機関が「つつがなく演習をクリア」したことで良しとしないよう、「とり得た他の選択肢」等を提示するなど**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】（身代金要求を伴ったDDoS攻撃（注））

（注）データを大量に送り付け、ウェブサイト等をダウンさせる攻撃

- ✓ DDoS攻撃により他の金融機関でサービス停止
  - ➢ 外部への情報収集、内部連携
- ✓ 複数の顧客から、当社のホームページにアクセスができないとの苦情
  - ➢ 被害状況の確認、業務・顧客への影響評価
- ✓ ビットコインを支払えば攻撃を回避できるとの脅迫メールを受信
  - ➢ 監視態勢の強化
- ✓ その後、自社もDDoS攻撃を受けていたことが判明
  - ➢ 攻撃元のアクセス遮断、再発防止策の検討・実施

（※）本演習では、上記のほか、「脆弱性攻撃による顧客情報の漏えい」のシナリオを用意