「金融業界横断的なサイバーセキュリティ演習（Delta Wall 2025）」の実施

金融庁では、今年で10回目となる金融業界横断的なサイバーセキュリティ演習「Delta Wall 2025」を、10月15日から28日にかけて開催しました。

1．金融分野のサイバーセキュリティを巡る状況

近年、サイバー攻撃の手法は一層巧妙化・複雑化しています。金融分野においても、証券口座の不正取引の事案や、オンラインバンキング等へのDDoS攻撃、サードパーティプロバイダーへのランサムウェア攻撃等、様々なサイバー攻撃が多数発生している状況にあります。こうしたサイバー攻撃の脅威は、金融システム全体に影響を及ぼしかねないトップリスクの１つとなっており、こうしたリスクに対処するためには、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です。

このような背景を受けて、金融庁では、毎年、金融業界全体でのサイバーセキュリティ対策の底上げを目的とした「金融業界横断的なサイバーセキュリティ演習」（通称：Delta Wall）を実施しています。

2．今年の演習（Delta Wall 2025）の概要

Delta Wallは今年で10回目の開催となりました。今回は、これまで演習未実施だった中小金融機関等の参加を促進した結果、演習参加金融機関数が過去最多の177社となるなど、年々規模を拡大して実施しています。

Delta Wallの特徴として、演習シナリオを金融業態別に作成していることが挙げられます。これにより、業態特有のシステム構成等を踏まえた演習を実施しています。

特に、今年は、直近のサイバー脅威の高まりや、業態の特殊性を踏まえ、暗号資産交換業者向けのシナリオを新たに作成しています。

シナリオの内容としては、「境界型防御の限界を前提としたゼロトラスト[1]の意識醸成」を共通のテーマとし、技術的対応を含めた攻撃内容の調査や、初動対応、顧客対応、復旧対応等の業務継続態勢を検証可能とする構成としました。

3．西野内閣府大臣政務官からの挨拶

演習初日の冒頭では、西野内閣府大臣政務官が、「サイバー攻撃の脅威は顕著に台頭し続けている。演習を通じて、インシデント対応能力の更なる向上を図っていただきたい」と挨拶しました。

写真：西野内閣府大臣政務官による冒頭挨拶

[1] ファイアウォール等による境界型防御だけでは対応できない脅威に対処するため、社内外すべてを信頼できない領域とし、すべての通信を検知・認証するセキュリティの考え方。

金融業界横断的なサイバーセキュリティ演習（Delta Wall 2025）

金融分野のサイバーセキュリティを巡る状況

- 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、我が国においても、サイバー攻撃による業務妨害、情報の窃取、金銭被害等が発生
- こうした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

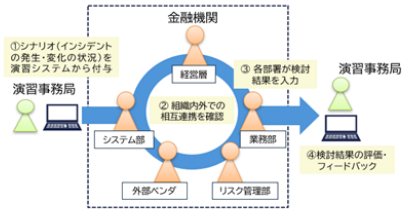
金融業界横断的なサイバーセキュリティ演習（Delta Wall 2025）

- 2025年10月、**金融庁主催による10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 2025（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）
- インシデント対応能力の底上げを目的として、演習未実施の中小金融機関の参加を促した結果、過去最多の**177先**が参加
- シナリオについては境界型防御の限界を踏まえた内部対策やゼロトラスト（※）の意識の向上を図ることが目的の一つ
- 昨年度に引き続き、テレワーク環境下での対応も含めたインシデント対応能力の向上を図るため、**参加金融機関は自職場やテレワーク環境下で演習に参加**

演習の特徴

- ✓ インシデント発生時における**初動対応、攻撃内容の調査・分析、顧客対応、復旧対応等の業務継続**を確認
- ✓ 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、具体的な改善策や優良事例を示すなど、**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】

- **銀行、信金・信組・労金**
  - ✓（ブラインド方式のため非開示）
- **証券**
  - ✓サイバー攻撃により顧客情報漏えいが発生
- **資金移動業者・前払式支払手段発行者**
  - ✓サイバー攻撃により顧客資産の流出が発生
- **暗号資産交換業者**
  - ✓サイバー攻撃により暗号資産の流出が発生

※境界型防御では対応できない脅威に対処するため、社内外すべてを信頼できない領域とし、すべての通信を検知・認証する考え方

4．演習結果の評価とフィードバック

本演習は、単発的なイベントとして終わらせるのではなく、参加金融機関が自らの対応能力を継続的に高める契機とすることを重視しています。特に、インシデント対応能力の強化に向けては、演習において対応が不十分であった事項を各金融機関が的確に把握し、改善に向けた取組を継続的に推進することが不可欠です。

このため、運営事務局では、演習後の事後評価に重点を置き、個別の金融機関に対して、具体的な改善策等をフィードバックすることに加え、預金取扱金融機関には振り返り研修も実施しています。

また、演習中に対応が困難であった項目、または不十分であった項目については、金融機関による自己分析を依頼し、課題の明確化と改善につなげる工夫をしています。

更に、演習結果は個別機関への還元にとどまらず、インシデント対応の優良事例等を業界全体にも共有することで、金融業界全体のサイバーセキュリティ対策の底上げを図っています。

写真：演習の模様