「金融業界横断的なサイバーセキュリティ演習（Delta Wall 2026）」の実施

金融庁では、今年で11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 2026」を、10月6日(火)から22日(木)にかけて開催しています。

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高度化・高速化しています。金融分野においても、ランサムウェア攻撃、サプライチェーン攻撃、情報窃取、不正送金など、さまざまなサイバー攻撃による被害が発生しています。また、最近では、フロンティアAIを含む高度なAI技術の進展により、サイバー攻撃のさらなる高度化・高速化が懸念されています。

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トップリスクの一つとなっており、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となっております。

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 2026）の概要

Delta Wall は今年で11回目の開催となります。今回も昨年に引き続き、これまで本演習に参加していなかった中小金融機関の参加を促進した結果、参加金融機関数は過去最多の181先となり、演習の規模は年々拡大しています。

Delta Wallの特徴として、演習シナリオを金融業態別（預金取扱金融機関向け、証券会社向け、保険会社向け、資金決済業者向け、暗号資産交換業者向け）に作成していることが挙げられます。これにより、業態によって特徴の異なるシステム構成を踏まえた演習を実施しています。

シナリオの内容として、今年度はフロンティアAIを含む高度なAI技術の進展など、サイバー攻撃の高度化を踏まえ、基幹システム等が攻撃を受けた場合の対応態勢の実効性向上を目的の一つとするシナリオを設定しています。実際の演習では、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体制を検証できるような構成としています。

なお、預金取扱金融機関及び保険会社については、インシデント対応能力のより一層の高度化を図る観点から、事前にシナリオを開示しないブラインド方式で実施しています。その他の業態については、事前にシナリオの骨子を共有した上で演習を実施しています。

3．根本内閣府大臣政務官からの挨拶

演習初日の冒頭では、根本内閣府大臣政務官が、「フロンティアAIの登場など、サイバー攻撃の脅威が日に日に増しており、高度化するサイバー攻撃のもとでは、防御だけではなく、攻撃を受けた後の対応や復旧、業務継続体制の確認が不可欠となる。本演習を通じて、金融業界全体のインシデント対応能力の更なる向上を図っていきたい。」と挨拶を行いました。

金融業界横断的なサイバーセキュリティ演習（Delta Wall 2026）

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、ランサムウェア攻撃、サプライチェーン攻撃、情報窃取、不正送金等による被害が発生。近年は、フロンティアAIを含む高度なAI技術の進展に伴い、サイバー攻撃の高度化・高速化が懸念されるなど、金融機関を取り巻く脅威は一層複雑化
- こうした脅威の複雑化は、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、金融業界全体のサイバーレジリエンス及びインシデント対応能力の更なる向上が不可欠

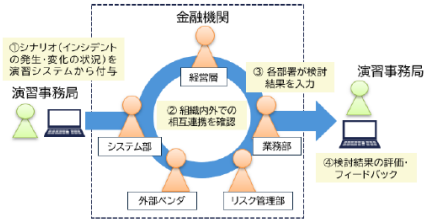
金融業界横断的なサイバーセキュリティ演習（Delta Wall 2026）

- 2026年10月、**金融庁主催による11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 2026（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、今回は過去最多の**181先**の金融機関が自職場やテレワーク環境下で演習に参加
- シナリオについてはサイバー攻撃の高度化を踏まえ、基幹システム等が攻撃を受けた場合の対応態勢の実効性向上を目的の一つとする

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・系統金融機関**
  （ブラインド方式のため非開示）
- **証券**
  - ✓ サイバー攻撃により不正アクセスおよび不正取引が発生
- **生命保険会社、損害保険会社**
  （ブラインド方式のため非開示）
- **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情報漏えい・不正決済が発生
- **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

4．演習結果の評価及びフィードバック

本演習は、単なる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、具体的な改善策や優良事例を含むフィードバックを提供するとともに、演習に参加した全ての金融機関を対象とする振り返り研修を実施しています。

また、演習中に対応が困難又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。

さらに、演習結果は個別の金融機関への還元にとどまらず、金融業界全体にも共有することで、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：根本内閣府大臣政務官による冒頭挨拶



写真：演習の模様