



**National center of Incident readiness and
Strategy for Cybersecurity**

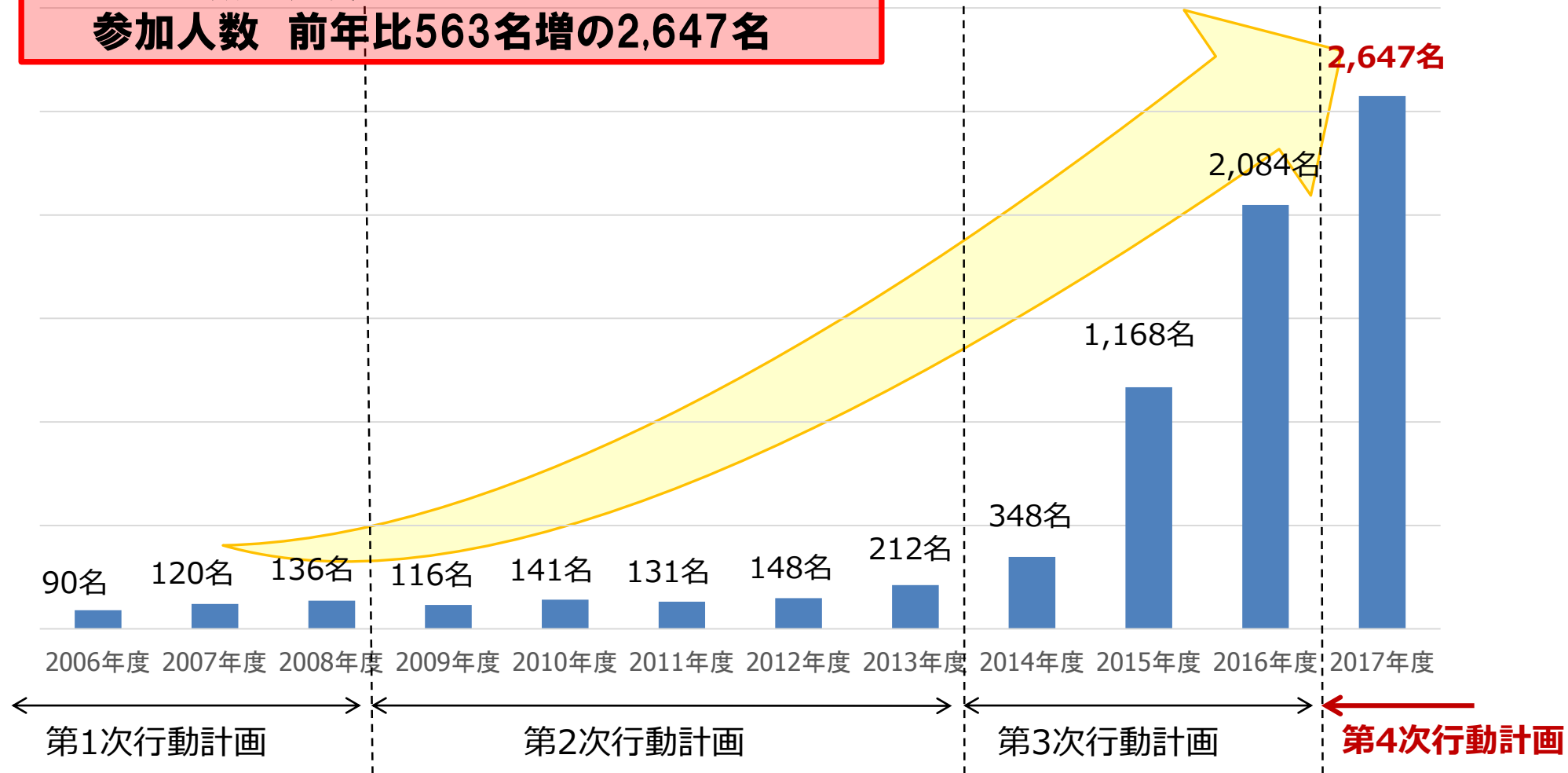
2017年度「分野横断的演習」について

2018年3月20日

内閣官房 内閣サイバーセキュリティセンター(NISC)

■過去最大規模の開催

参加人数 前年比563名増の2,647名



日時：2017年12月13日（水）12：30～17：00
（見学説明会 14：10～16：00）

場所：東京会場、大阪会場、福岡会場、自職場



演習内容：

- 第1部 各分野において重要インフラサービスへの影響が小さい障害が発生したことを想定し、分野間・官民間での連携を図ることによる情報共有体制の実効性を検証（ランサムウェアによる攻撃）
- 第2部 重要インフラサービスへ影響が生じる障害が発生し、事業継続が脅かされる事態を想定した、事業継続計画の発動方法やその手順を確認するなど、各社の対応を検証（DDoS攻撃、ネットワーク機器のマルウェア感染、制御システムのマルウェア感染）

演習における新たな取り組み

- ①演習シナリオのより一層の充実
 - ・第4次行動計画における新しい概念として「機能保証」、「サービス維持レベル」を踏まえたシナリオ設計
- ②情報伝達の有効性の検証
 - ・他事業者との横連携
 - ・セキュリティ関係機関からの情報収集
- ③サブコントローラーが経営層の役割を担い、プレイヤーのインシデント対応状況等を評価
- ④オリパラ大会を見据えた情報共有体制の確認（一部事業者のみ）

意見交換会の開催概要

日時：2018年1月24日（水） 14:00～17:30

場所：東京会場、大阪会場、福岡会場

目的：

- ・演習当日に得た気づき、改善に向けた取組み、困っていること、工夫していること等について、他の参加者事業者等と意見交換を実施することにより、今後の取組みに活用
- ・サイバーセキュリティの担当者相互の繋がり（顔の見える関係）を確保し、平素より情報交換が行える関係性を構築



意見交換会における新たな取組み

- ①分野の関連性を考慮した座席配置
- ②意見交換テーマを複数（10テーマ）を提示し、ニーズに応じたテーマの選択
 - ・現状の問題点・今後の課題
 - ・有効な情報連携の手法について（匿名化による情報の集約 等）
 - ・各組織のサイバーセキュリティに対する考え方・組織体制について
 - ・サイバーセキュリティに対する経営層の関与について
 - ・演習を通じて、規則・基準・組織体制等で改善の必要性を感じたこと
 - ・事業継続計画やコンティプラン（緊急時対応計画）の発動・解除のための連絡体制、意思決定の仕組み、対応について
- ③意見交換の進捗を可視化するため、模造紙に意見交換のやりとりの内容等を記録

目的

- ✓ これから分野横断的演習に参加することを検討している重要インフラ事業者を対象として、分野横断的演習の全体像、および事前準備から演習当日、演習後に至る一連の取組みを説明する。
- ✓ 分野横断的演習を自社における対応能力強化に積極的に活用している事業者の取組事例を「グッドプラクティス」として提示する。

テキストブックの主な内容

- ▶ テキストブックの目的
 - ▶ サイバーセキュリティの重要性
 - ▶ 演習参加に向けた事前準備
 - ▶ プレイヤー・サブコントローラーが果たすべき役割
 - ▶ 演習シナリオの考え方
 - ▶ 演習当日の実施イメージ
 - ▶ 演習効果を向上させるための留意事項
(規程類見直し、経営層参加)
 - ▶ グッドプラクティス
 - 複数部門により構成されたCSIRTの有効性について検証を行った事例
 - 経営層が直接的に参画するセキュリティ確保のための体制を構築した事例
- など12事例掲載

本テキストブックについて

本テキストブックの目的と対象

サイバー攻撃等に起因する情報システムの停止により、重要インフラ事業者のサービス提供が停止した場合、当該事業者に留まらず国民生活や社会経済活動に重大な影響を及ぼす可能性が極めて高くなっている。

重要インフラ事業者等がサービスの持続的な提供を行うためには、その社会的責任の重要性に見合う重要インフラサービス障害への事前準備が必要である。具体的には、発生時における迅速な対応・復旧を実現する組織的対応能力の強化を目的とした行動計画の作成や演習の実施が必要である。また、各関係主体間の連携の強化が重要となっている。

内閣官房内閣サイバーセキュリティセンター（以下、NISC）では、重要インフラ事業者の重要インフラサービス障害発生時における組織的な対応能力強化や各関係主体間の連携の強化を目的として、「分野横断的演習」を平成18年度から継続的に開催しており、分野横断的演習を中心とする各種施策を通じて重要インフラ全体の防護能力の維持・向上を図ってきたところである。

近年、演習の重要性の浸透に伴い、分野横断的演習の参加事業者数も飛躍的に拡大した。しかし、いまだ分野横断的演習未経験の重要インフラ事業者も多数存在し、我が国全体の重要インフラサービスの対応能力の向上のためには、更なる参加者のすそ野拡大が必要となっている。

本書は、これから分野横断的演習に参加することを検討している重要インフラ事業者を対象として、分野横断的演習の全体像、および事前準備から演習当日、演習後に至る一連の取組プロセスの概要を整理したものである。また、分野横断的演習を自社のIT障害への対応能力強化に活用している先進的な事業者の取組事例をグッドプラクティスとしてまとめたものである。

テキストブックの目的

分野横断的演習の概要

- 分野横断的演習とは、NISCが平成18年度から開催しており、重要インフラ分野の重要インフラサービス障害体制を強化する中核的な取組みとして位置づけられています。

- 主催
内閣官房内閣サイバーセキュリティセンター

- 参加対象
・重要インフラ事業者等
・重要インフラ所管行政セクター事務局
・情報セキュリティ関係機関（IPA、JPCERT/CC）

- 実施時期
12月上旬

■ 分野横断的演習は、以下の二つの事項を目的としています。

- ✓ 『第4次行動計画』に基づく種々の施策の実効性の検証
- ✓ 重要インフラサービス障害が発生した際の情報セキュリティ関係能力の維持・向上

※重要インフラ分野に属する事業者等及び当該事業者等から構成される「重要インフラ分野」は、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「防災」及び「その他」の15分野を指している。

分野横断的演習とは

サイバーセキュリティとは

- サイバー攻撃とは、攻撃者によってネットワーク経由で企業の保有する情報資産の機密性、完全性、可用性を損なう行為です。
 - 機密性：アクセスを許可された者だけが、アクセスをすることを確実にすること
 - 完全性：情報および処理方法が正確であること、および完全であることを保護すること
 - 可用性：許可された利用者が、必要な時に、情報および関連する資産にアクセスできることを確保すること

情報資産

攻撃者

サイバー攻撃

情報資産

サイバーセキュリティとは、そのようなサイバー攻撃から情報資産の安全を確保することです。

サイバーインシデントとは

分野横断的演習の実施イメージ (2/2)

- プレイヤーはサブコントローラーによる状況付与に基づき、所管省庁へIT障害の発生時の状況報告等を行います。
- 必要に応じて、情報セキュリティ関係機関への問い合わせや、他事業者との情報連携等を行います。

プレイヤーの行動イメージ

サブコントローラー

プレイヤー

情報提供

セクター事務局

情報提供

所管省庁

情報提供

NISC

プレイヤー

情報提供

情報連携

情報セキュリティ関係機関

他事業者

ネットワークには演習中に発生した状況や対応した内容等の記録に活用する。

分野横断的演習の概要

➤ より実践的な演習機会の提供

- 実時間に近い時間軸の検討
- 実環境に即したサブシナリオの検討
(サブコントローラーへの支援の充実)
- オリパラへの対応
- 国際・地域的な視点の考慮

➤ 自職場参加の推進

- 自職場参加者への説明の充実
- 自職場参加者を意識したシナリオの準備
- 経営層への理解浸透

➤ 重要インフラ全体での防護能力の底上げ

- 参加が少ない業界の参加推進
(場所、実施日程等の検討)
- セプター事務局向け説明の充実
- 第4次行動計画に基づく情報共有体制に関する理解の増進

➤ 情報共有体制の実効性の向上

- 「普段やっていることを検証する」だけでなく
「(必ずしも普段できていなくても)やるべきことを
しかるべく実行するためのきっかけづくりとなる」
演習へ
- 事業者等が使用するツール等を踏まえた演習
の検討