資料4

National center of Incident readiness and Strategy for Cybersecurity

官民連携演習等について

2024年10月８日
内閣官房 内閣サイバーセキュリティセンター

1. 分野横断的演習について

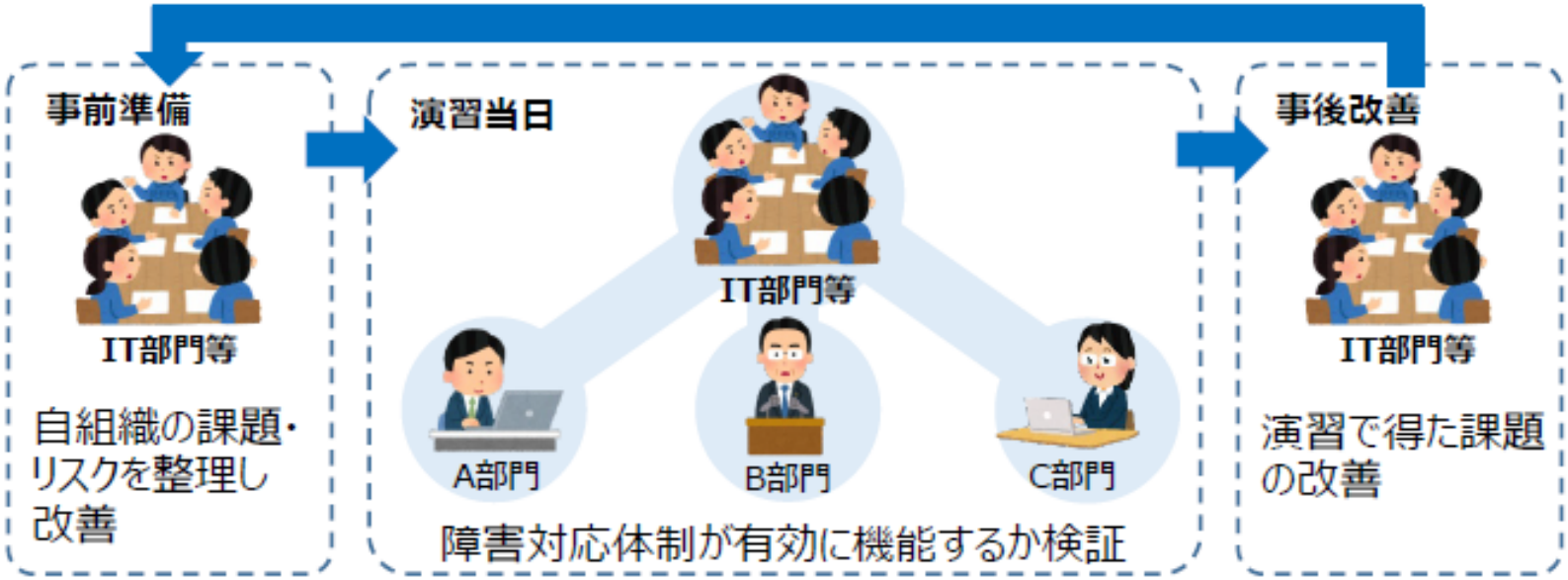
＜目的＞

分野横断的演習は、「重要インフラのサイバーセキュリティに係る行動計画（以下、重要インフラ行動計画という）」の主要5施策のうち「防護基盤の強化」の**「障害対応体制の有効性検証」**に位置付けられ、以下の目的として実施するものである。

- **関係主体の組織全体の障害対応体制が有効に機能しているか**どうかを確認し、改善につなげていくこと
- 重要インフラ行動計画の他施策に資すること

（注） 重要インフラ行動計画は、サイバーセキュリティ基本法及びサイバーセキュリティ戦略（閣議決定）に基づき、重要インフラ防護に係る基本的な枠組みとして、政府と重要インフラ事業者等との共通の行動計画を定めたものである。重要インフラ行動計画においては、任務保証の考え方を踏まえ、重要インフラ事業者等は自らの責任においてサイバーセキュリティ対策を実施するとともに、継続的な改善に取り組むこととされ、政府は、必要な支援を行うこととされている。

＜障害対応体制の有効性検証＞



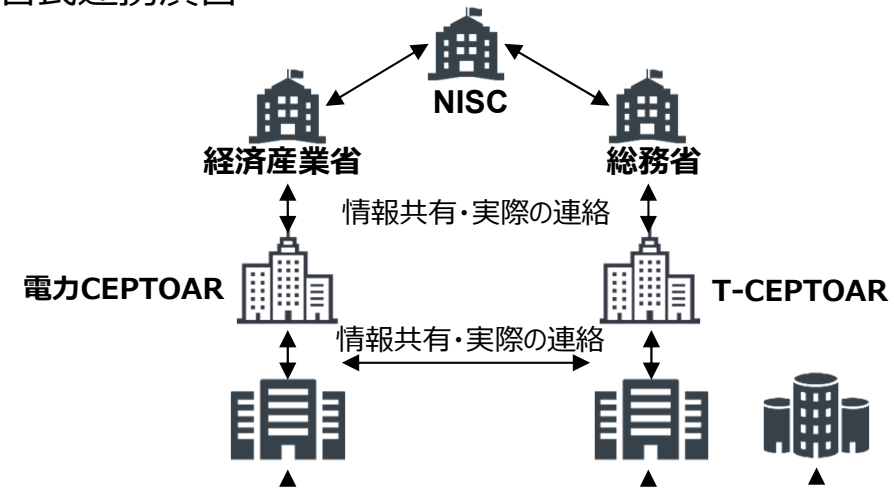
＜実績＞

2006年度から毎年度実施しており、昨年度は全14分野の重要インフラ事業者等から、集合会場とオンライン参加を合わせて過去最多となる819組織（6,574名）が参加。

3. 2024年度 演習概要

3-1. 演習の全体像

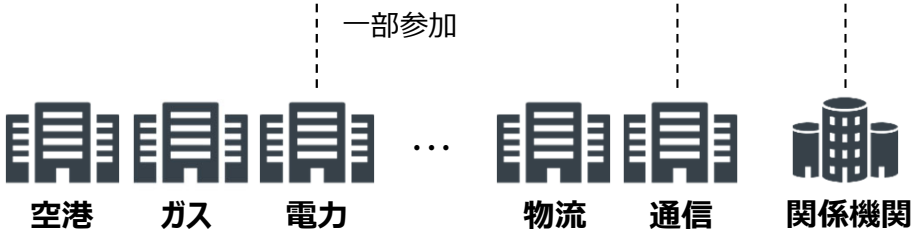
①官民連携演習



演習の特徴
- 一部の重要インフラ事業者を対象に、試行的に実施。NISCや所管省庁等も含め、組織間での双方向の連携を実施し、官民連携（連絡体制・情報共有・助言等）の手順を重点的に確認及び強化。

演習の規模
- 重要インフラ事業者や関係省庁及びNISC等を含め約17組織、最大約110名が、同一会場に集まって、演習を実施する想定。

②全分野一斉演習



演習の特徴
- 幅広く重要インフラ事業者が参加。
- 各事業者における対処を確認及び強化（他組織との連携は片方向または状況付与のみ）。
- 官民連携演習に準じたシナリオを想定。

演習の規模
- 2023年度の実績から、800組織以上、6,000名以上のオンライン参加を想定。

③経営層向け啓発コンテンツ

活動の特徴
- 全分野一斉演習に参加する重要インフラ事業者等の経営層を対象とした普及・啓発コンテンツ動画を配信。

3. 2024年度 演習概要

3-2. 官民連携演習

① 日時、形態、参加者

日　時：予行　2024年10月16日（水）（13時から17時を予定）
　　試行　2025年　2月13日（木）（予行演習を踏まえて調整）

場　所：紀尾井カンファレンス（赤坂見附）

形　態：机上演習（集合及び来場が困難な地方の事業者等はオンラインも可）
【特徴】・集合会場で行うことで、演習に集中できる
・他の演習参加者等の対応状況が把握できる
・他の演習参加者等とのディスカッションがスムーズに可能となる

参加者：内閣官房内閣サイバーセキュリティセンター（NISC）
重要インフラ所管省庁（総務省、経済産業省）
重要インフラ事業者等・セプター（情報通信分野、電力分野）
サイバーセキュリティ関係機関（IPA、JPCERT/CC）　（最大110名程度を想定）

② 演習全体の流れ

予行では、演習企画・設計に重点を置き、試行と同様の演習を実施し、試行に向けての課題・リスクの洗い出しと、改善を行う。
試行において、参加者が自組織の障害対応体制や官民連携が機能するかの課題を抽出し、解決策を検討する。

	予行	試行
	試行に向けて、官民連携演習における課題・リスクを洗い出し、改善を行う	演習の中で、自組織の障害対応体制や官民連携が機能するか、新たな課題を抽出する
イベント	・演習当日（予行）	・演習当日（試行）

3. 2024年度 演習概要

3-3. 全分野一斉演習

①日時、形態、参加者

日　時：2024年12月５日（木）

形　態：机上演習（オンライン（自職場、自宅等）のみ）
【特徴】 ・普段の業務環境で演習に取り組むことができる
・各組織の実態に即した、より実践的な演習にできる

参加者：内閣官房内閣サイバーセキュリティセンター（NISC）
重要インフラ所管省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）
重要インフラ事業者等（15分野）
セプター（15分野21セプター）　※参加募集状況･･･838組織（5,951名） ９月20日現在

②演習全体の流れ

事前準備、演習当日、事後改善により構成されており、各イベントを通じて演習を実施する。

	事前準備 演習当日に向けて、自組織における課題・リスクを洗い出し、改善を行う	演習当日 演習の中で、自組織の規定・マニュアル・BCP/IT-BCP等が機能するか確認し、新たな課題を抽出する	事後改善 演習当日に抽出した新たな課題を基に、課題の改善を行う
イベント	• 23年度フォローアップアンケート • 参加募集 • 事前説明動画 • 事前準備アンケート	• 演習当日	• 演習事後アンケート • 意見交換会 （意見交換会アンケート） • 24年度フォローアップアンケート

3. 2024年度 演習概要

3-4. 経営層向け啓発コンテンツ

① 日時、形態、対象者

日　時：2024年10月 ～ 12月

形　態：オンデマンド配信

【特徴】

- 重要インフラ事業者等における経営層を対象とした啓発コンテンツ動画を配信。
- 全分野一斉演習の事前準備として経営層向け啓発コンテンツを提供することで、参加事業者の経営層は、全分野一斉演習においてインシデント発生時の重要インフラ事業者等における対応を確認・検証することができる。
- 全分野一斉演習参加事業者の責任者・担当者においては、事前に自社の経営層に啓発コンテンツを活用することで、経営層がサイバー事案対処の重要性を認識し、経営層に求められる知識、能力及び判断等の向上に繋がることが期待できる。

対象者：全分野一斉演習に参加する重要インフラ事業者等（15分野）の経営層

3. 2024年度 演習概要

3-5. スケジュール

会議体及びイベントのスケジュールは以下のとおり。

		2024年									2025年					
		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月
会議体						▼ 第1回 有識者部会（7/31（水）） ▼ 第1回 検討会（9/24（火））					▼ 第2回 有識者部会（1月下旬） ▼ 第2回 検討会（3月上旬）					
官民連携演習	参加調整						予行				試行					
	事前レビューシート										1月中旬 ～ 下旬					
	改善シート											2月中旬 ～ 下旬				
	演習事後アンケート							10月中旬 ～ 下旬				2月中旬 ～ 下旬				
	演習当日							★ 予行（10/16（水））★ 試行（2/13（木））								
全分野一斉演習	フォローアップアンケート				7/11（木） ～ 7/25（木） ※8/9（金）まで延長											
	参加募集					8/1（木） ～ 8/30（金） ※9/20（金）まで延長										
	事前説明動画							10月上旬 ～ 12月上旬								
	事前準備アンケート								11月中旬 ～ 下旬							
	演習当日									★ 演習当日（12/5（木））						
	疑似体験プログラム									12/5（木） ～ 12/20（金）						
	演習事後アンケート									12月中旬 ～ 下旬						
	意見交換会									12月中旬 ～ 下旬						
	意見交換会アンケート										1月中旬 ～ 下旬					
	フォローアップアンケート														5月中旬 ～ 下旬	
経営層啓発	経営層向け啓発							10月 ～ 12月								

4-1. 重要インフラ行動計画における位置付け（1/2）

「防護基盤の強化」の「障害対応体制の有効性検証」に位置付けられている。

「重要インフラのサイバーセキュリティに係る行動計画」の概要

官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

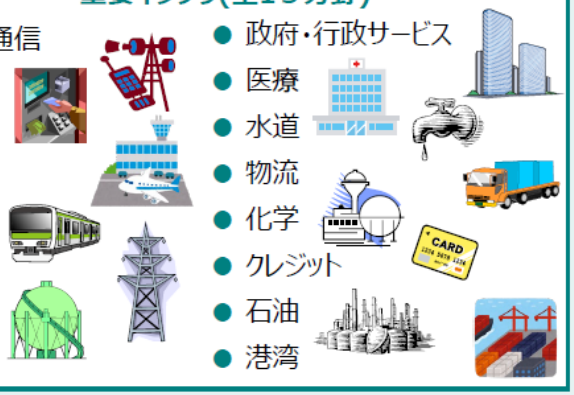
NISCによる総合調整

重要インフラ所管省庁

- 金融庁 ［金融］
- 総務省 ［情報通信、行政］
- 厚生労働省 ［医療］
- 経済産業省 ［電力、ガス、化学、クレジット、石油］
- 国土交通省 ［航空、空港、鉄道、水道、物流、港湾］

重要インフラ(全15分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油
- 港湾



関係機関等

- サイバーセキュリティ関係省庁 ［総務省、経済産業省等］
- 事案対処省庁 ［警察庁、防衛省等］
- 防災関係府省庁 ［内閣府、各省庁等］
- サイバーセキュリティ関係機関 ［NICT、IPA、JPCERT/CC等］
- サイバー空間関連事業者 ［サプライチェーン等に関わるベンダー等］

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

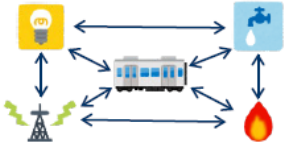
安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

4-1. 重要インフラ行動計画における位置付け（2/2）

「防護基盤の強化」の「障害対応体制の有効性検証」に位置付けられている。

行動計画の取組⑤： 防護基盤の強化

重要インフラの防護基盤の強化のため、障害対応体制の有効性検証、人材育成、関係機関との連携、国際連携、広報広聴活動等、行動計画の全体を支える共通基盤的な取組を推進する。

取組のポイント

- ✓ 障害対応体制の有効性検証の実施
- ✓ IT部門だけでなく、幅広い部門の人材育成
- ✓ 効果的な広報チャネルを活用した情報発信　　等

行動計画期間中の取組

（1）障害対応体制の有効性検証
- 分野横断的演習による障害対応体制の検証
- 演習で得た課題を活用した障害対応体制の改善

（2）人材育成等の推進
- 経営層と緊密な連携を行えるよう、戦略マネジメント層の育成
- IT部門に限らない、組織全体の意識向上

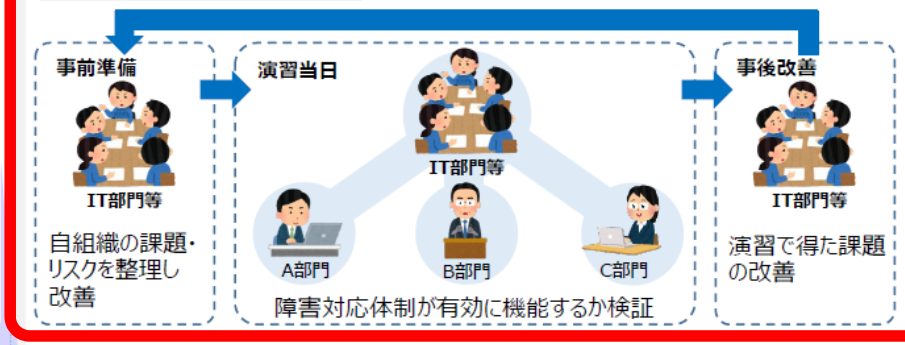
（3）国際連携の推進
- 政府間や事業者間の様々な枠組みを活用した多面的・多角的な国際連携の推進

（4）警察・デジタル庁との連携強化
- サイバー犯罪や、DXに伴う新たな技術に対する意識向上による全体としてのセキュリティ確保の推進

（5）広報広聴活動の推進
- 行動計画の枠組みや取組の国民への積極的な発信
- 関連文書及び関連規格の整備

防護基盤の強化に向けた取組

障害対応体制の有効性検証



人材育成等

- 戦略マネジメント層の育成
- 組織全体の意識向上

国際連携

二国間、地域間、多国間の連携

警察・デジタル庁との連携強化

警察庁 National Police Agency　デジタル庁

- サイバー犯罪の警察への通報等
- DXに伴う新技術への意識向上を通じたサイバー空間の安全確保

広報広聴活動

Webサイト、SNS、ニュースレター、講演等を通じた発信