National center of Incident readiness and Strategy for Cybersecurity

# 2022年度分野横断的演習
# 実施結果

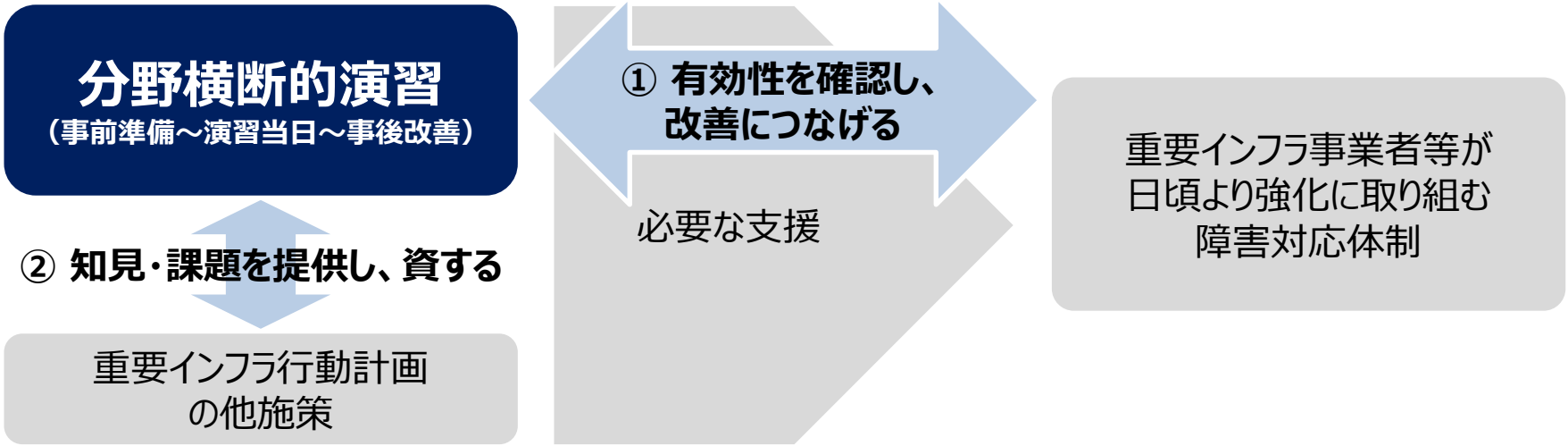
2023年5月

内閣官房　内閣サイバーセキュリティセンター

# 1. 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」）において「障害対応体制の有効性検証」に位置付けられるものであり、①**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**、さらに②**重要インフラ行動計画の他施策に資すること**を目的として実施するものである。

（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。



# 2. 実施概要

＜演習の形態＞

- 机上演習
- **集合会場と自職場等（テレワーク環境を含む）のハイブリッド形式**

集合会場にて演習する参加者

＜参加者数、参加組織数＞

- **5,719名、 754組織** ※疑似体験プログラム参加者含む
  - 重要インフラ事業者［14分野（20セプター）］
  - 重要インフラ所管省庁
  - サイバーセキュリティ関係機関　等

＜演習の概要＞

- 重要インフラサービス障害発生時における一連の対応について、参加事業者自身が成すべき対応についてしっかりと事前に整理し**必要な改善を行ったうえで演習当日に臨み**、限られた時間及び変化する状況下で、**準備したものが有効に機能するかを検証**する。
- 政府は、演習を通じて得た知見・課題を参考資料として重要インフラ行動計画の他施策に提供する。演習参加事業者等は以下の取り組みを通じて継続的な改善を行う。
  **＜事前準備＞**　自組織における課題・リスクの状況を洗い出し、**改善**を行った上で演習当日に参加
  **＜演習当日＞**　演習の中で自組織の規定・マニュアル・BCP/IT-BCP等が機能するかどうかを確認し新たな**課題を抽出**
  **＜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**に取り組む
- 演習から得られた重要インフラ防護に関する知見の普及・展開によって、**更なる障害対応体制の強化に資する**。

# 3. 基本コンセプトと関係者

＜基本コンセプト＞

- 分野横断的演習は、事前準備、演習当日、事後改善により構成。
- 重要インフラ事業者等が、一連の分野横断的演習を活用し、日頃より強化に取り組む障害対応体制の有効性を継続的に検証・改善することを期待。

**事前準備**
自組織における課題・リスクの状況を洗い出し改善を行った上で演習当日に参加

→

**演習当日**
演習の中で自組織の規定・マニュアル・BCP/IT-BCP等が機能するかどうかを確認し新たな課題を抽出

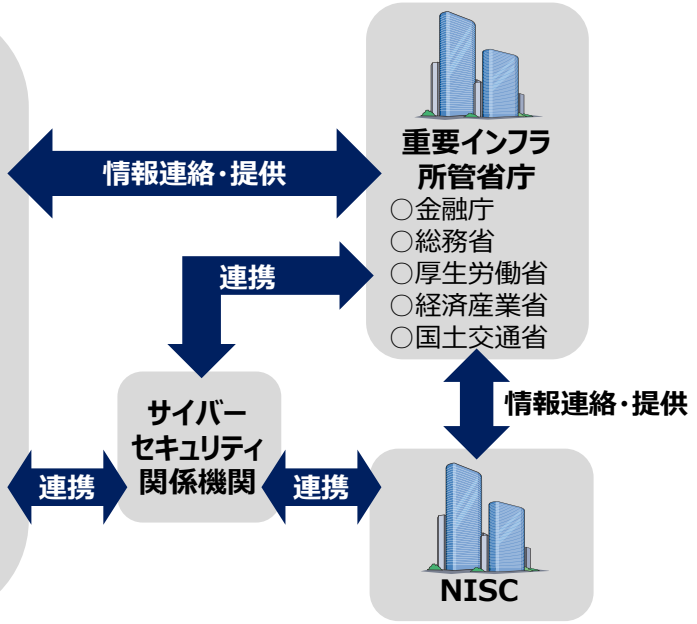
→

**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に取り組む

＜関係者＞

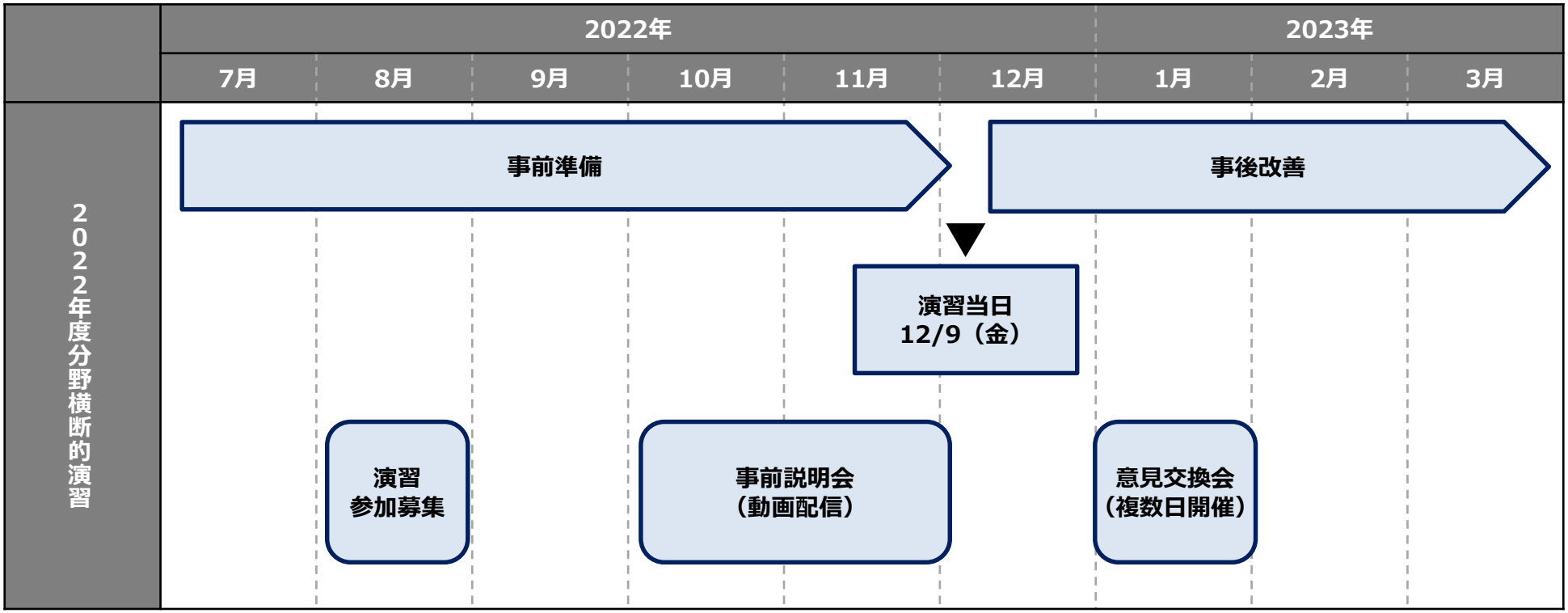
**重要インフラ**
**14分野20セプター**
**（情報共有・連携）**

情報通信（電気通信役務、放送、ケーブルテレビ）、金融（銀行等、生命保険、損害保険、証券、資金決済）、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



# 4. スケジュール

- 2022年度分野横断的演習のスケジュールは以下の通り。




※疑似体験プログラムは12/9～12/21に実施

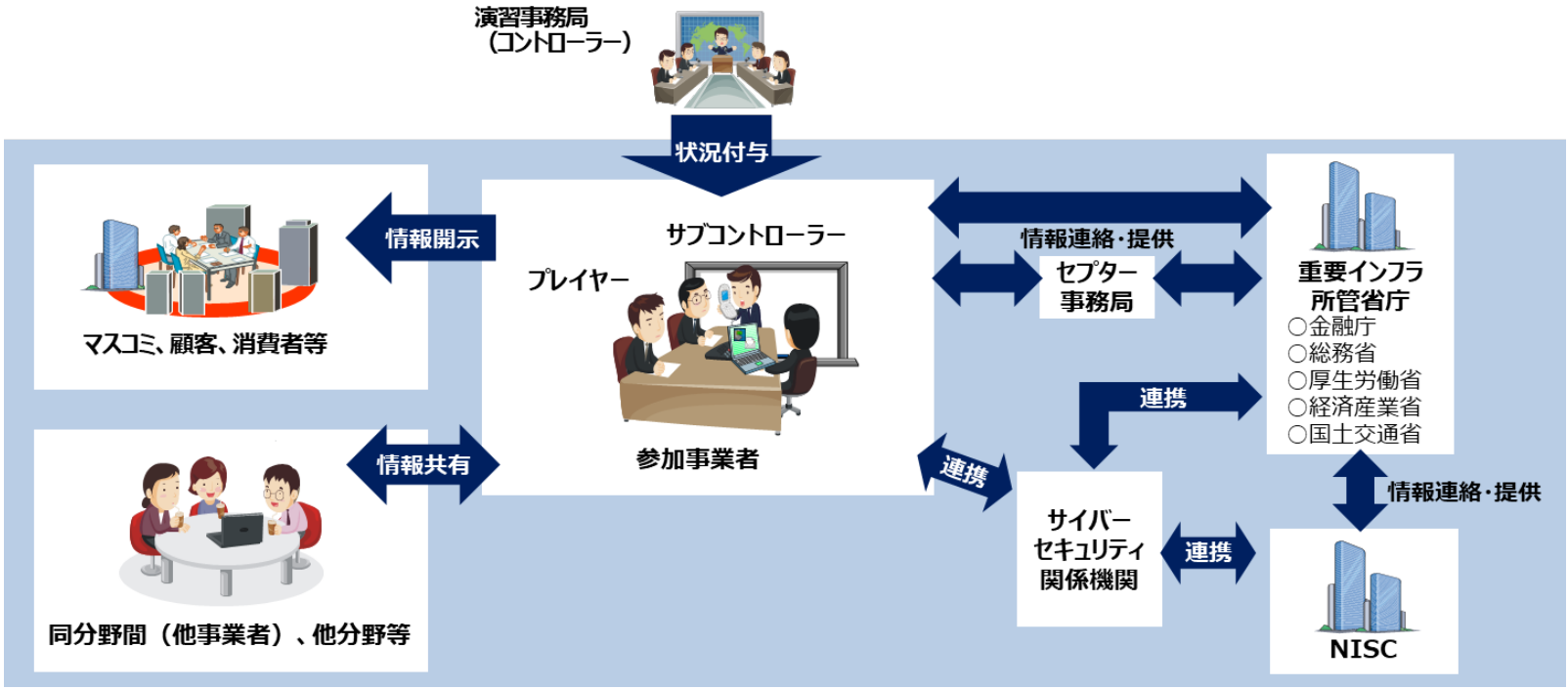
# 5. 演習当日の実施概要

＜演習当日の実施概要＞

- 日時：2022年12月9日（金）13:00 ～ 17:00
- 実施形態：集合会場と自職場等（テレワーク環境含む）のハイブリッド形式

＜演習当日の全体イメージ＞

- 演習当日は、演習事務局からの状況付与をきっかけに、**ランサムウェア攻撃やEmotet（エモテット）への感染時の対応について確認**することで、障害対応体制の有効性検証を行った。
- 演習時の行動を振り返る際の材料を得るために、行動記録シートを演習参加者向けに作成した。行動記録シートは、演習中の行動を時系列に沿って記録し、対応状況を確認するものである。演習参加者が記録した行動記録シートを演習終了後に収集し、演習結果の分析に活用した。



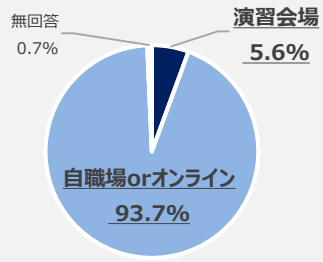
# 6. 演習当日の実施結果（１／２）

## ● 演習の実施形態

- ➢ 2022年度は集合会場及び自職場等からの演習参加（ハイブリッド形式）で演習を実施した。
- ➢ 2023年度の演習に参加すると回答した組織のうち、**5.6%が集合会場の参加を希望**、**93.7%の組織が自職場又はオンラインの参加を希望**した。

来年度も参加すると回答した組織に対し
希望する参加形態について
回答組織数＝287

演習会場： 5.6%（16組織）
自職場orオンライン：93.7%（269組織）
無回答： 0.7%（2組織）

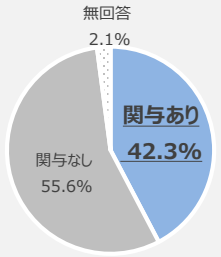



## ● 経営層の参加

- ➢ 2022年度は演習に経営層が参加するよう事業者との各接点で周知を実施した。
- ➢ **事前準備において、42.3%の組織で経営層の関与**があり、55.6%の組織で関与がなかった。
  - **関与例**：シナリオや課題内容の確認、演習参加と目的の確認
  - **関与なしの理由例**：経営層の担当箇所は既に決定済み、担当部署のみで実施のため
- ➢ **演習当日において、55.3%の組織で経営層の関与**があり、42.8%の組織で関与がなかった。
  - **関与例**：経営層や組織の各階層における対応、コンティンジェンシープランに基づく対応、緊急時における事業継続の対応
  - **関与なしの理由例**：経営層の演習参加が不要と判断、業務都合、経営層を含む演習は別途実施

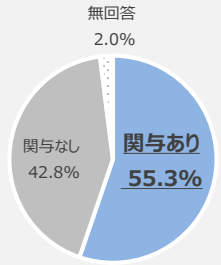
事前準備における経営層の関与
回答組織数＝475

関与あり：42.3%（201組織）
関与なし：55.6%（264組織）
無回答： 2.1%（10組織）




演習当日における経営層の関与
回答組織数＝456

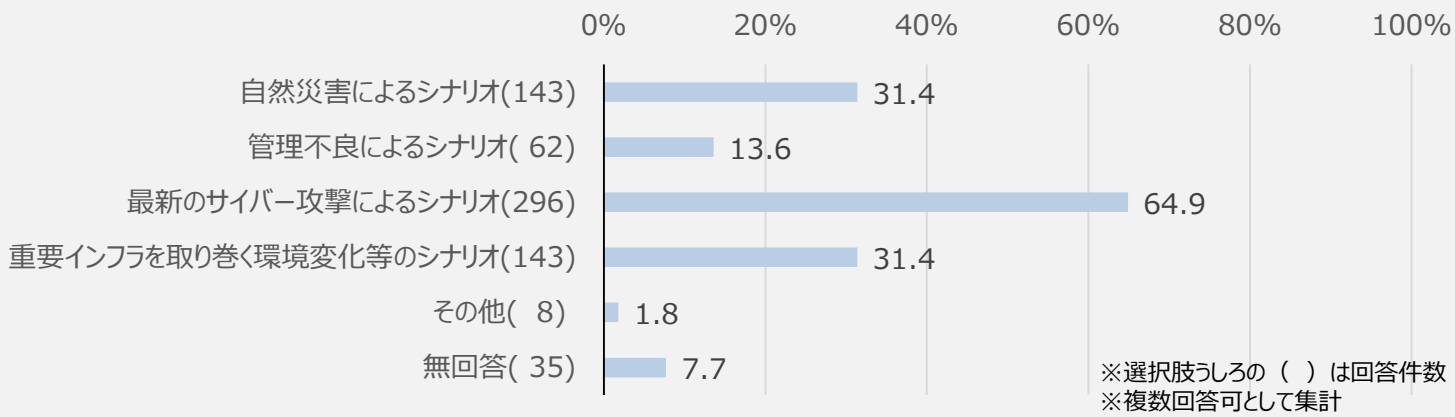
関与あり：55.3%（252組織）
関与なし：42.8%（195組織）
無回答： 2.0%（9組織）



# 6. 演習当日の実施結果（２／２）

- **演習シナリオ**
  - 2022年度は、最新のインシデントの動向や過去の重要インフラサービス障害の事例等を踏まえ、**ランサムウェア攻撃**を基本事象として取り扱い、また関連事象として**サプライチェーン攻撃**及び**Emotet**を取り扱った。
  - 2023年度以降に希望するシナリオは、**最新のサイバー攻撃によるシナリオが64.9%**であった。

来年度以降、希望するシナリオ
回答組織数＝456



# 7. 障害対応体制の有効性検証：実施概要

- 重要インフラ行動計画を基に見直したベンチマークを用いて、**障害対応体制の有効性検証**を行った。
- ベンチマークは重要インフラ行動計画に基づく指標や取組内容等を確認するものであり、ベンチマークを基にしたアンケートを設計・実施・分析することで、重要インフラ事業者等が障害対応体制の強化にどれだけ取り組んだか現状把握を行った。
- **2023年度以降**、検証結果の推移を見ることで**障害対応体制の有効性の推移を把握**することができる。

## 重要インフラ行動計画

**理想とする将来像**
- ・責務の明確化
- ・組織統治
- ・重要インフラ事業者等における 自組織に最適な 防護対策の確保
- ・脅威への包括的な取組
- ・コミュニケーション
- ・社会 との共存共栄
- ・定期的な評価・見直し

**ベンチマーク**
指標（率）や取組内容等の確認

**1.障害対応体制の強化**
- 1.1 組織統治の一部としての障害対応体制
- 1.2 障害対応体制の強化に向けた取組
  - (1) BCP/IT-BCP
  - (2) CSIRTの効果的な運用
  - (3) 安全基準等の活用（**2.安全基準等の整備及び浸透**）
  - (4) 情報共有体制の強化（**3.情報共有体制の強化**）
  - (5) リスクマネジメントの活用（**4.リスクマネジメントの活用**）
  - (6) 障害発生に関する対応
  - (7) 監査検証
  - (8) その他取組（**5.防護基盤の強化**）

# 8. 障害対応体制の有効性検証：実施結果

- 演習当日の参加者における**障害対応体制の有効性検証の実施結果**は以下の通り。
  - 演習シナリオにおけるインシデント発生時の対応について

| | |
|---|---|
| **IT-BCPに沿って対応出来た程度** | **81.2%** |
| **IT-BCPからBCPに円滑に移行できた程度**<br>※IT-BCPに沿って対応した組織のうち、IT-BCPからBCPへ移行した組織が対象 | **84.9%** |
| **CSIRTが対応できた程度** | **83.4%** |
| **内規やマニュアル等で対応できた程度** | **83.8%** |
| **情報連携や開示の手順に沿って対応できた程度** | **84.9%** |

- ✓ 演習当日の参加者を対象に、演習シナリオに対する自己評価についてアンケートによりデータを集計
- ✓ 値は平均値、アンケートは0-100%の1%刻みで回答

# 9. 検証課題による検証結果（１／２）

- 参加事業者等は、今年度新たに見直した**検証課題より検証**すべき課題を事前に設定し、演習当日に検証を行った。
- 検証課題を用いた検証については、**行動記録シート**を設計・配布・回収・分析することで、参加事業者等が考える課題及び対応方針等について現状把握を行った。

※アンケートではベンチマークに基づいた検証を行い、行動記録シートでは検証課題に基づいた検証を行う。

| # | 検証課題 |
|---|---|
| ① | **情報収集（CSIRTの活動）**<br>自組織のCSIRTが情報収集を行い、運用手順に沿って適切な関係部署や対象者へ周知することができたか |
| ② | **インシデント対処（CSIRTの対応）**<br>重要インフラサービス障害発生時の初動対応から復旧に向け、自組織のCSIRTが対応手順に沿って問題なく機能し、その指示のもと動くことができたか |
| ③ | **経営層や組織の各階層における対応**<br>重要インフラサービス障害発生時のコンティンジェンシープランや事業継続計画（IT-BCP等含む）の発動・解除に関して、経営層や組織の各階層における適切な責任と権限のもとで判断し対処することができたか |
| ④ | **所管省庁やセプターへの情報共有**<br>重要インフラサービス障害に関する情報を所管省庁やセプターへ、運用手順に沿って共有できたか |
| ⑤ | **サイバーセキュリティ関係機関（IPAやJPCERT/CC等）への情報共有・活用**<br>重要インフラサービス障害に関する情報をIPAやJPCERT/CCへ報告や相談を行い、収集した情報を活用できたか |
| ⑥ | **サプライチェーン全体への情報共有**<br>重要インフラサービス障害に関する情報を分野内外や取引先を含むサプライチェーン全体へ、運用手順に沿って共有ができたか |
| ⑦ | **緊急時の対応（コンティンジェンシープランに基づく対応）**<br>重要インフラサービス障害発生時のコンティンジェンシープランが対応手順通りに行うことができたか　※発動が必要と判断になった場合 |
| ⑧ | **緊急時における事業継続の対応（事業継続計画（IT-BCP等含む）に基づく対応）**<br>重要インフラサービス障害発生時の事業継続計画（IT-BCP等含む）が対応手順通りに行うことができたか　※発動が必要と判断になった場合 |
| ⑨ | **サービス利用者への情報発信**<br>サービスへの影響や復旧に関する情報の発信についての内容・タイミング・手段（ネット上での急速な情報流布への対応を含む）について適切な責任と権限のもとで発信されたか |

# 9. 検証課題による検証結果（２／２）

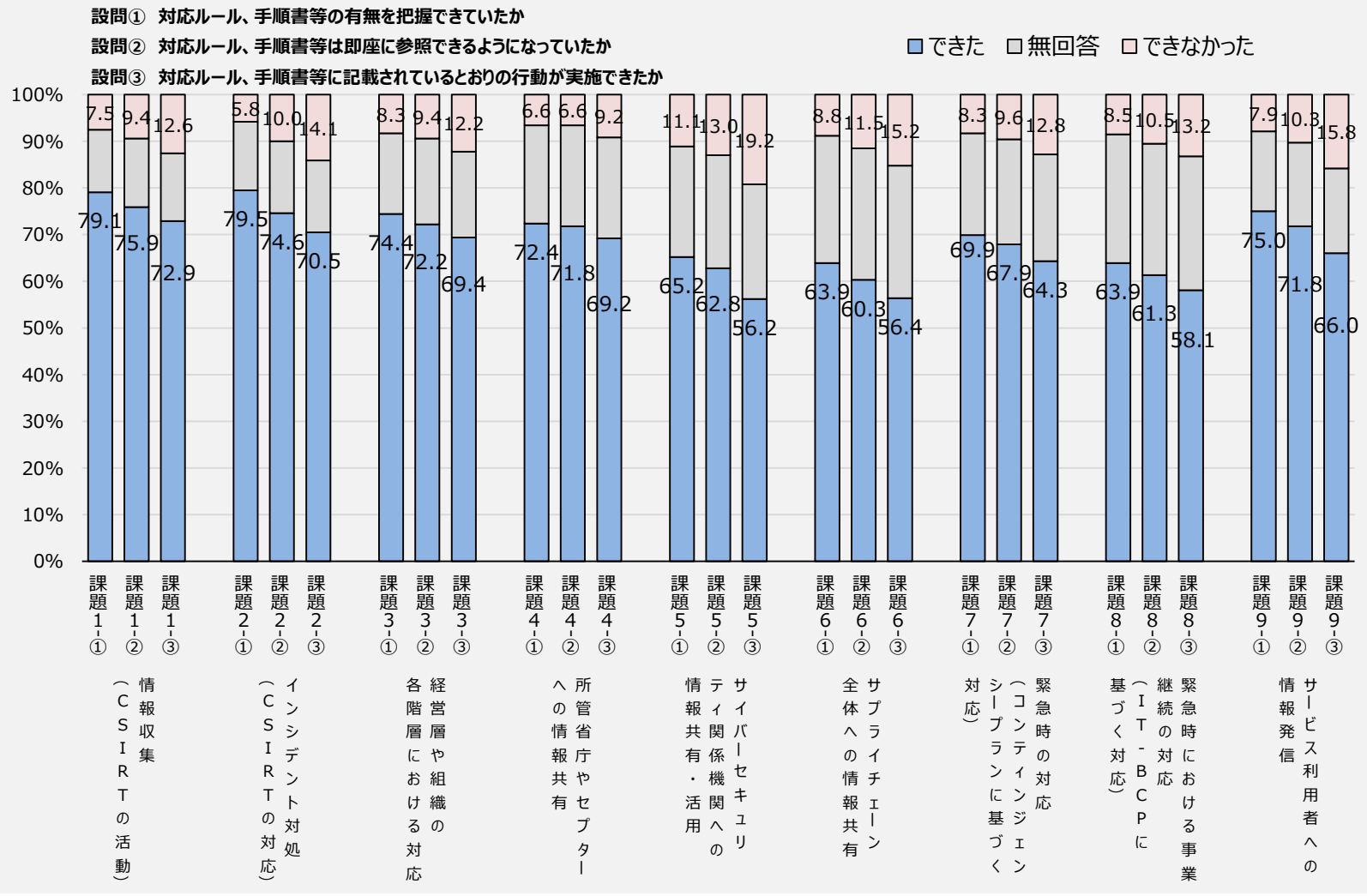
＜検証課題を用いた検証結果＞

- 設問③で「できた」と回答した割合が高いものは上から課題1,2,3であり、低いものは下から課題5,6,8であった。
- 事業者が組織統治に係る取り組みを強化するよう事前準備で支援を行った。課題3-③で「できた」と回答したのは69.4%であった。
- 情報共有体制について演習の事前にセプター訓練で検証を実施した。設問①→③の傾きが最も小さいのは課題4であった。

**2022年度**
**回答組織数 ＝468**

(※回答は、
「よく対応できた」
「対応できた」
「あまり対応できなかった」
「ほとんど対応できなかった」
「無回答」 のうち、

「よく対応できた」＋「対応できた」
を、『できた』として集計
「あまり対応できなかった」＋
「ほとんど対応できなかった」を、
『できなかった』として集計)

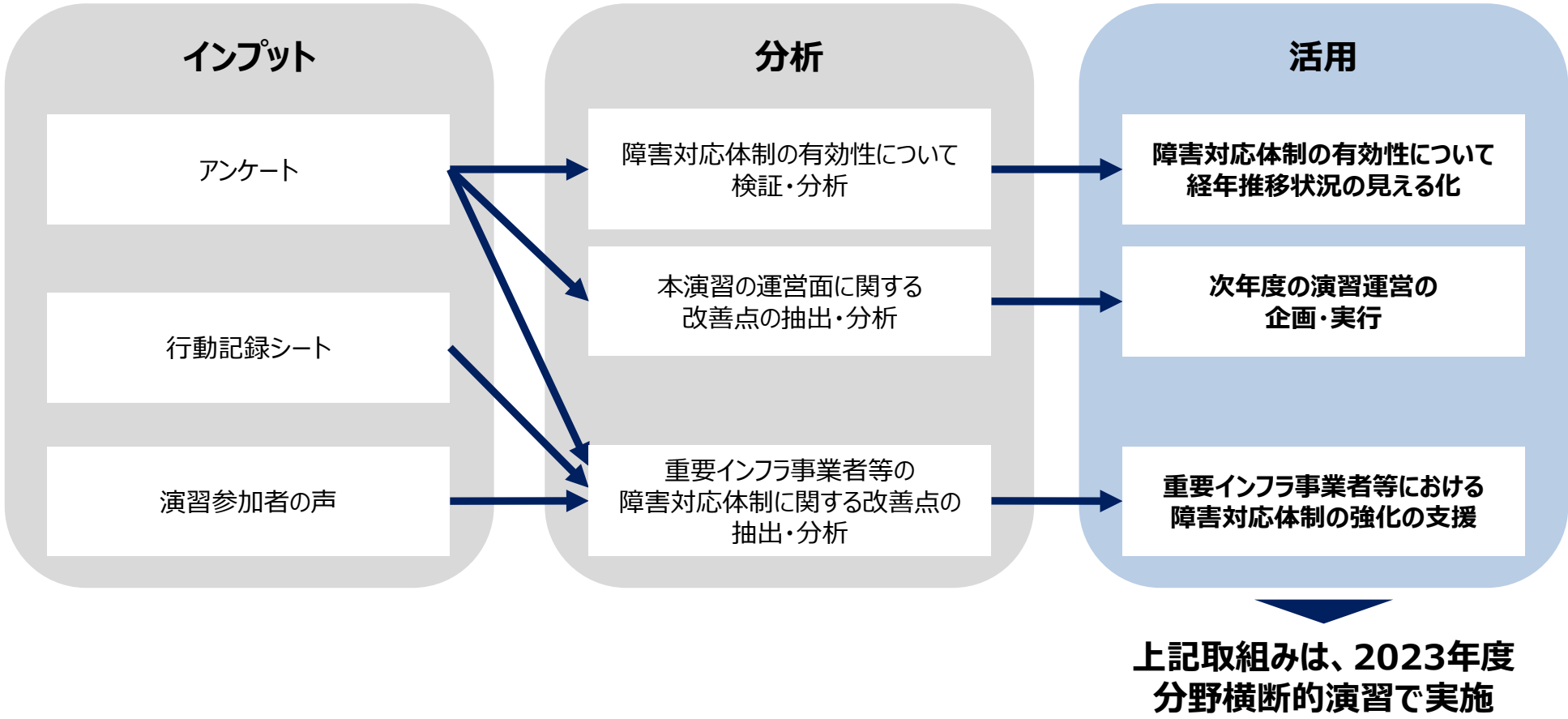


# 10. 演習参加者が洗い出した課題例

- 行動記録シートや意見交換会を活用することにより、重要インフラ事業者等における障害対応体制の強化に資するものとして、以下の課題を抽出した。
  - 全体
    - 重要インフラサービス障害発生時において、より詳細かつ具体的な行動マニュアルの必要性
    - より具体的な使用場面を想定した行動マニュアルの必要性
    - 重要インフラサービス障害発生時の対応に係る演習機会確保の必要性
  - 経営層や組織の各階層における対応に関する気づき
    - より明確な経営層の責任範囲・指揮系統・報告手段等の必要性
    - 指揮者不在時の権限移譲ルールの必要性
    - 休日・夜間等における対応（代替連絡ルート等）の必要性
  - サービス利用者への情報発信に関する気づき
    - より明確な情報発信の基準・タイミングの必要性
    - インターネット利用不可の場合の代替手段の必要性
  - サプライチェーン全体への情報共有に関する気づき
    - 連絡先リストの作成・更新の必要性
    - 情報共有内容・粒度について、より具体的な判断基準の必要性

# 11. 実施結果の活用

- アンケート、行動記録シート、演習参加者の声等を基に分析した2022年度分野横断的演習の実施結果は以下の取組みに活用する。
  - 障害対応体制の有効性について経年推移状況の見える化
  - 次年度の演習運営の企画・実行
  - 重要インフラ事業者等における障害対応体制の強化の支援



# 12. 2023年度分野横断的演習に向けた取組の方向性（案）

現在、2023年度分野横断的演習に向けた取組の方向性として、以下の４つを検討しております。

- **集合会場及び自職場からの演習参加（ハイブリッド形式）の継続**
  - 基本方針は自職場参加
  - 参加者の対応状況の見える化等の仕組みを検討

- **経営層の参加促進を強化**
  - 経営層参加のイメージや効果等に係る情報発信の内容更新

- **演習シナリオの継続的改善**
  - 最新のインシデントの動向や過去の重要インフラサービス障害の事例等を踏まえ、時宜に応じた演習シナリオを検討

- **安全基準等策定指針等の改訂状況に応じた取組強化**
  - 最新の重要インフラ行動計画を踏まえた安全基準等策定指針等の改訂状況に応じ、障害対応体制の有効性を検証できる演習シナリオの設計、ベンチマーク及びアンケートの内容更新
  - 事業者による障害対応体制の強化を支援する情報発信の内容更新
    ※関係省庁、サイバーセキュリティ関係機関等の取り組みについても情報発信を行う。

# （参考）重要インフラサービス障害への対応

重要インフラサービス障害への対応として、**「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」**の記載を紹介します。本内容を改めて確認し**必要な改善**を行うことを推奨します。

- **サイバー攻撃に備えたコンティンジェンシープラン及び事業継続計画の策定**
  - 重要インフラサービス障害の発生に備えた対処態勢をあらかじめ整備することが重要となるため、初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープラン」及び事業継続を目的とした復旧対応の方針等を定めた「事業継続計画」を策定するとともに、当該計画の実行に必要な組織体制を整備する。
  - 特に、サイバー攻撃に備えたコンティンジェンシープラン及び事業継続計画を策定・改定する場合には「【別紙３】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照することが期待される。

- **CSIRT等の整備、関連部門との役割分担等の合意**
  - サイバー攻撃リスクの特性を考慮したコンティンジェンシープラン及び事業継続計画の実行に必要な組織体制のひとつとして、CSIRTを重要インフラ事業者等の内部に整備する。
  - CSIRTは、役割分担や対応手順等について、あらかじめ関連部門と合意しておくことが重要である。

- **対応計画に基づく被害拡大防止・サービス復旧**
  - 実際にサイバー攻撃等の事象を検知し、トリアージの結果、対応が必要と判断された場合には、コンティンジェンシープラン及び事業継続計画に従って、事象の詳細分析、関係主体等との情報共有・調整、被害拡大の防止・サービスの復旧等の対応を実施する。
  - 重要インフラサービス障害への対応で得られた新たな教訓等については、将来の対応活動や対策に活かすべく、コンティンジェンシープラン及び事業継続計画の継続的な改善プロセスの中において取り入れる。

（参考）NISC「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」
https://www.nisc.go.jp/pdf/policy/infra/shishin5rev.pdf