National center of Incident readiness and Strategy for Cybersecurity

2023年度 分野横断的演習
実施結果

2024年3月
内閣官房 内閣サイバーセキュリティセンター

1. 2023年度 分野横断的演習 概要
2. 演習参加者の障害対応体制の強化の取組状況
及び演習当日の結果
3. 演習事後における振り返り（意見交換会）

（参考1）「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
（参考2）重要インフラのサイバーセキュリティに係る安全基準等策定指針
（参考3）内閣サイバーセキュリティセンターからの公開情報

1. 2023年度 分野横断的演習 概要

1-1. 目的

各重要インフラ事業者等において、**自組織の障害対応体制の有効性を検証・改善する**とともに、内閣官房（NISC）と重要インフラ所管省庁等が連携し、**演習を通じて得た知見・課題を踏まえて演習その他の施策の改善を図る**こと。

1-2. 演習の概要

- **机上演習**で実施（集合会場と自職場（テレワーク含む）のハイブリッド形式）
- **演習シナリオ**について、最新のサイバー情勢等を踏まえ、インシデント対応における**経営層の参画**や**取引先等を含むサプライチェーンリスク対策を踏まえた状況付与**を実施。
  - ① 重要インフラ事業者等が**ランサムウェア攻撃**を受けた結果として、自組織のシステム障害が発生し、**関係先（重要インフラサービス提供先を含むサプライチェーン）に影響を与える**とともに、システム障害の原因究明や復旧対応に数日間を要することを想定。
  - ② **組織統治の一部としてのサイバーセキュリティを実践**するため、「重要インフラサービス提供レベルの低下」、「ステークホルダーへの広報」等の**経営判断を伴うインシデント対応**を想定。
- 演習当日の集合会場において、演習参加者等同士が有識者も交えて**対面で意見交換を行う座談会**を開催し、重要インフラ事業者等間の**平時からの情報共有体制の構築を促進**。

1-3. 参加者

- 重要インフラ事業者等
  （情報通信、金融、電力等の14分野）
- 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）
- 事案対処省庁　（警察庁、防衛省　※2023年度初参加）
- サイバーセキュリティ関係機関　（IPA、JPCERT/CC）
- 2023年度実績：集合会場とオンライン参加を合わせて**6,574名**、**819組織**

※疑似体験プログラム参加を含む

開会式にて挨拶を行う河野大臣（2023年度）

集合会場の模様（2023年度）

1-4. 演習全体の流れ

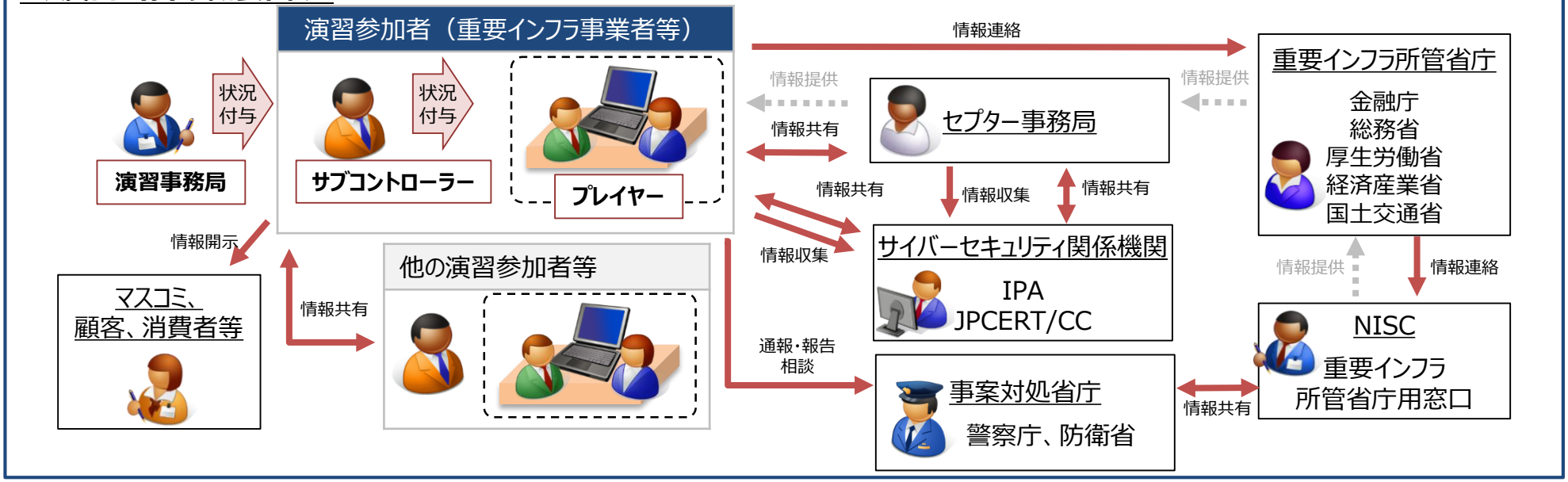
演習参加にあたっては、自組織における課題・リスクの状況を洗い出し改善（事前準備）を行った上で、演習当日に参加いただき、演習当日に抽出した新たな課題を基に改善（事後改善）に取り組む。

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

＜ 演習当日の概要図 ＞



1-5. 取組実績（事前準備、演習当日、事後改善）

2023年度 分野横断的演習の取組実績は以下の通りである。

事前準備

・参加募集（資料配付）：8/3(木)～8/31(木) ※9/15(金)まで延長
重要インフラ所管省庁を介して、重要インフラ事業者等へ参加募集を実施

・事前説明動画の公開：9/29(金)～12/6(水)
演習の進め方（検証課題の設定、シナリオのカスタマイズ、演習実施環境の確認等）の説明に加え、
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、改善したうえで演習当日に臨むことを説明

演習当日

・サブコン座談会：12/7(木) 10:00-11:15

参加者　：有識者委員 8名、8事業者（13名）　※集合会場の演習参加者のうち、希望者のみ。
テーマ　：「演習当日までの事前準備で取り組んだ点」、「演習当日までの事前準備より相談したい点」
※事業者（演習参加者）と有識者委員を交え、テーマに沿って討議。

・演習本番：12/7(木) 13:00-17:00

形　態　：机上演習（集合会場とオンライン（自職場、自宅等）のハイブリッド形式）
参加数　：819組織、6,574名　※疑似体験プログラムの参加数含む

＜ 演習中の取組 ＞

・広報サイト（13事業者 / 20事業者（集合会場の演習参加者））
演習中の状況に応じて、自組織の判断のもと広報サイトに情報を公開。

・疑似ホームページ（問合せ件数　IPA：261件　JPCERT/CC：258件　警察庁：352件）
演習中の状況に応じて、自組織の判断のもと関係機関へ問合せ・相談等を実施。

事後改善

・意見交換会：23/12/14(木)、12/19(火)、12/21(木)、24/1/17(水)、1/18(木)の複数日開催

形　態　：WEB開催
参加数　：83組織 286名
内　容　：「2023年度 分野横断的演習当日の振り返り」、「自組織のサイバーセキュリティ確保について」

2. 演習参加者の障害対応体制の強化の取組状況及び演習当日の結果

2-1. 障害対応体制の強化の取組状況及び演習当日の結果　1/2

障害対応体制の強化の取組状況及び演習当日の結果は以下の通りである。

#	取組内容	取組状況	23年度
組織統治の一部としての障害対応体制			
	経営層・CISOの役割と責任の整理状況	整理済み	83.5%
	適切な責任の権限のもとの対応状況（**演習当日**）	対応できた	93.3%
	影響度に合わせた判断基準の整理状況	整理済み	74.4%
	自組織の判断基準に沿った対応状況（**演習当日**）	対応できた	93.7%
BCP/IT-BCP			
	IT-BCPの整備状況	整備済み	59.7%
	IT-BCPに沿って対応できた程度（**演習当日**）	できた程度（平均値）	83.3%
CSIRTの効果的な運用			
	CSIRTの整備状況	整備済み	68.4%
	CSIRTが対応できた程度（**演習当日**）	できた程度（平均値）	83.8%
安全基準等の活用			
	内規やマニュアル等の整備状況	整備済み	77.8%
	内規やマニュアル等で対応できた程度（**演習当日**）	できた程度（平均値）	85.1%
情報共有体制の強化			
	インシデント発生時における組織内の情報共有体制や運用等の整理状況	整理済み	81.6%
	手順に沿って対応できた程度（**演習当日**）	できた程度（平均値）	86.9%
障害発生に関する対応			
	コンティンジェンシープランの整備状況	整備済み	76.9%
	コンティンジェンシープランに沿って対応できた程度（**演習当日**）	できた程度（平均値）	83.6%

2-1. 障害対応体制の強化の取組状況及び演習当日の結果　2/2

#	取組内容	取組状況	23年度
リスクマネジメントの活用			
	リスクマネジメントの改善を行う仕組み状況	仕組みあり	66.7%
	－（演習当日）	－	－
	サプライチェーン・リスクマネジメントの整備状況	整理済み	24.4%
	－（演習当日）	－	－
監査検証			
	監査の実施状況	年1回以上	83.7%
	－（演習当日）	－	－

2. 演習参加者の障害対応体制の強化の取組状況及び演習当日の結果

2-2. 行動記録シートにおける検証課題の結果　1/3

演習参加者（重要インフラ事業者等）は、個別シナリオの作成に合わせて、下記の検証課題を設定していただき、演習当日の行動記録シートにおいて振り返りを行っている。

	No	検証課題（有効に機能しているかどうかを確認）	重要インフラ行動計画の「1. 障害対応体制の強化」に紐づく取組
Ⅰ. 障害対応体制の強化	①	**情報収集（CSIRTの活動）** 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	1.2 障害対応体制の強化に向けた取組 (2) CSIRTの効果的な運用
	②	**インシデント対処（CSIRTの対応）** 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	1.2 障害対応体制の強化に向けた取組 (2) CSIRTの効果的な運用
	③	**経営層や組織の各階層における対応** 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	1.1 組織統治の一部としての障害対応体制
	④	**重要インフラ所管省庁やセプターへの情報共有** 重要インフラサービス障害に関する情報を重要インフラ所管省庁やセプターへ、運用手順に沿って共有できたか	1.2 障害対応体制の強化に向けた取組 (4) 情報共有体制の強化（3.情報共有体制の強化）
	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** 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	1.2 障害対応体制の強化に向けた取組 (4) 情報共有体制の強化（3.情報共有体制の強化）
	⑥	**サプライチェーン全体への情報共有** 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	1.2 障害対応体制の強化に向けた取組 (4) 情報共有体制の強化（3.情報共有体制の強化）
	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）** 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	1.2 障害対応体制の強化に向けた取組 (6) 障害発生に関する対応
	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）** 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	1.2 障害対応体制の強化に向けた取組 (1) BCP/IT-BCP
	⑨	**サービス利用者への情報発信** 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	1.1 組織統治の一部としての障害対応体制
Ⅱ. その他	⑩	**独自の課題設定** 参加事業者等において、独自に検証したい課題を自由に設定可能（複数設定することも可能）	－

2. 演習参加者の障害対応体制の強化の取組状況及び演習当日の結果

2-2. 行動記録シートにおける検証課題の結果　2/3

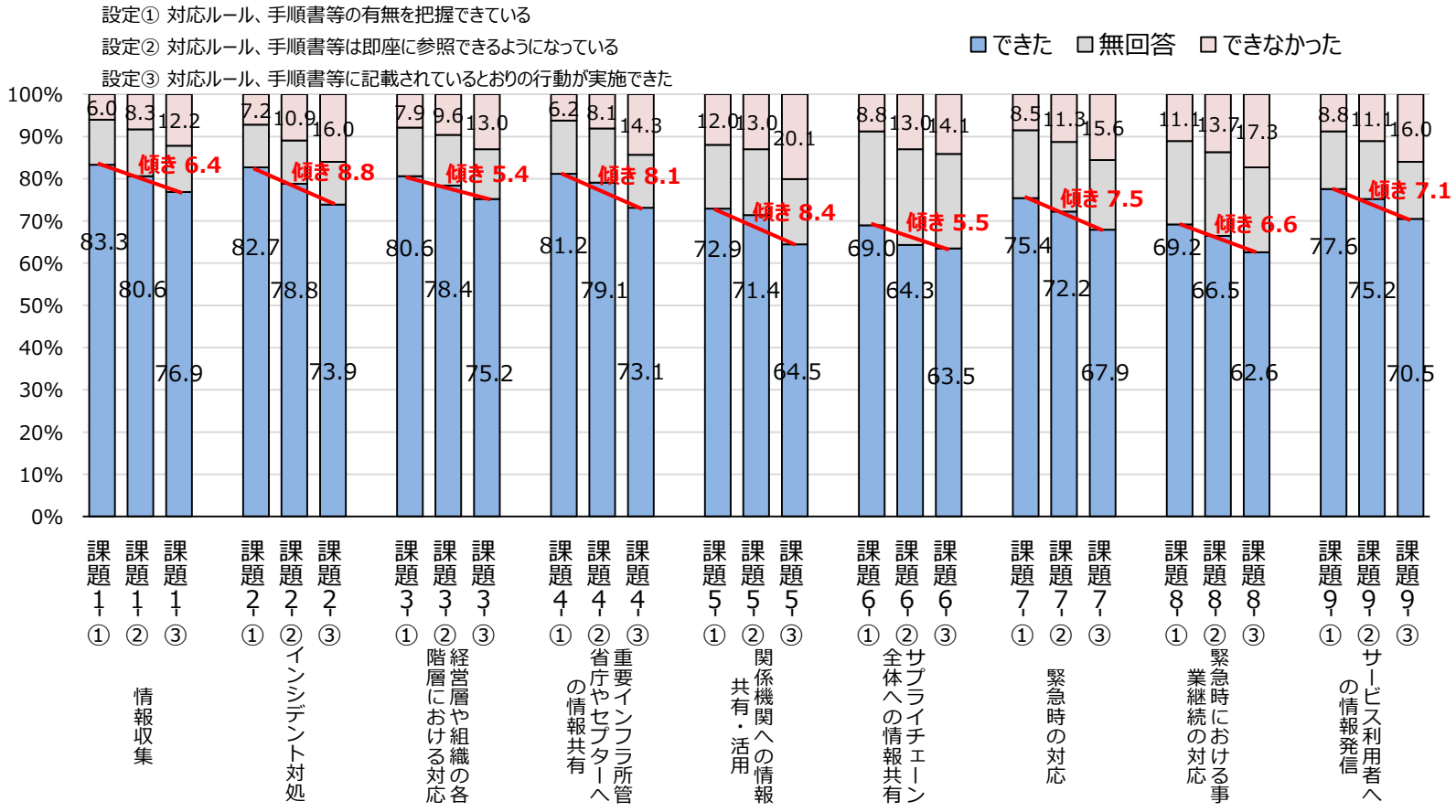
- 全体的に検証課題は、手順書等の有無（設定①）、参照（設定②）、行動（設定③）ができた傾向が高いが、低い割合となったのは検証課題6,8（サプライチェーン全体への情報共有、緊急時における事業継続の対応）であった。
- 個々の検証課題の中で、速やかに対応が取れた（設定①→③の傾きが小さい）のは、検証課題3,6（経営層や組織の各階層における対応、サプライチェーン全体への情報共有）であった。
- 手順書等の有無は把握できているが、即座に参照及び行動が取れていない（設定①→③の傾きが大きい）のは、検証課題2,4,5（インシデント対処、重要インフラ所管省庁やセプターへの情報共有、関係機関への情報共有・活用）であった。

2023年度
回答組織数 ＝468

回答選択
「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」

・「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。



2-2. 行動記録シートにおける検証課題の結果　3/3

検証課題より、洗い出された課題については以下の通りである。

#	検証課題	洗い出された課題（代表的な意見）
①	**情報収集（CSIRTの活動）**	• CSIRTの組織づくりは現在の組織では人員数などで難しい。 • 連絡網の整備等は行っているのだが、そのアップデートを綿密に行う必要性がある。 • この判断を行う役割が誰なのかを改めて確認し、次回の演習では重点的にチェックする必要がある。 • どの段階からCSIRTメンバーとしてインシデント対応に加わるのか、基準があいまいであった。
②	**インシデント対処（CSIRTの対応）**	• CSIRTとしてどう動くべきか戸惑っているようにみえた。対応手順書の内容を再考する必要がある。 • 有事の際に限られたメンバーでどう対応するか、参加者の意識の向上が必要である。 • マニュアルの格納場所を把握しておらず、マニュアルに目を通す習慣がなかった。マニュアルに沿った対応が行えなかった。
③	**経営層や組織の各階層における対応**	• 夜間帯や休日の際に各責任者に連絡が取れなかった際の副担当、関係者の連絡先も十分に把握する必要がある。 • 経営者層へ報告する段階的なタイミングを障害発生時マニュアル等へ明記する必要がある。 • 経営層の判断・方針決定までは検討しきれていなかった。
④	**所管省庁やセプターへの情報共有**	• どういった被害が想定されたら、誰がどのタイミングで、どこの外部機関へ情報共有するかが文書化されていない。 • 各連絡先の連絡フォーマットの項目数が多く、担当者が入力に戸惑っていた。 • 報告先についてはリストアップしているが優先順位は決まっていないため、どこから報告すべきか都度判断が必要となった。 • 連絡を行う事務方担当とサイバー関係部署の担当で情報関係の知識に差があり、報告する入力項目の記載に時間を要した。
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**	• 全項目が判明し記載できることは稀なため、記載必須項目を明記いただくか、記載項目の絞り込みをいただけるとありがたい。 • 機関ごとに様式が異なり、報告にあたって何を洗い出しておくべきかの判断に時間がかかった。 • CSIRT人員不足により複数個所との機動的な情報連携が困難な状態にある。態勢強化が必要と認識した。 • 報告先が複数あり、各報告先から色々な指示やアドバイスを受けた場合の優先順位を決めておく必要がある。
⑥	**サプライチェーン全体への情報共有**	• サプライチェーン全体の把握が不完全であった。情報発信内容のレベル分けなどが明確になっていなかった。 • どのサービスに支障が出た時に、誰に対して情報共有が必要かを一元化して纏めておくべきと感じた。 • サプライチェーン全体への情報共有について要領に定めていなかった。サプライチェーンの一覧が作成されていなった。
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）**	• システムが長期にわたり使用不能に陥った場合、どのレベルまでのサービスを維持するか？など決めていなかった。 • コンティンジェンシープランに子細に規定されていない事項も多く、検討しきれていない対応があった。 • コンティンジェンシープラン・事業継続計画が実情に合っていない・見直しができていない。
⑧	**緊急時における事業継続の対応（IT-BCPに基づく対応）**	• サイバー攻撃事案をプレスリリースする際に、セキュリティ部門として事故の詳細を広報部門や経営層に共有する必要がある。 • 組織全体のBCP、IT-BCPでは大まかなフローや判断基準が定められているものの、それに向け対応する人員により品質や情報の整理などに差が生じ、BCPに関わる決断で必要となる迅速で正しい情報の整理が出来ていない。
⑨	**サービス利用者への情報発信**	• 発信を行うべきレベルやタイミングについては、関係各署（総務部門・報道部門など）を交えて事前の再精査が必要である。 • あらかじめ、障害発生時の速報用文書を作成、準備し、複数の従業員が対応できるようにしておく必要もある。 • SNS利用も促進しているのでそちらからの発信も今後検討が必要である。

2-3. 演習当日の実施結果（サブコン座談会）

＜ 発表テーマ、発言内容 ＞

演習当日までの事前準備で取り組んだ点		
個別シナリオ作成	…	インシデントにおける相互依存性を踏まえたシナリオ作成やサービス利用者の生命に関わるシナリオ作成が困難。
BCPとサイバーの関係性	…	BCPにサイバーを含めると組織内の体制や動きが変わり煩雑になるが、改めて機器の状況を確認することに繋がる。
演習当日までの事前準備より相談したい点		
経営層関与	…	経営層の参加や理解を深めてもらうために、サプライチェーン先への影響やインシデントにおける影響範囲を説明。 また、当事者意識を高めるために、記者会見のイメージなどを説明。
情報共有や情報源	…	情報共有のフォーマットが難しい。自組織内ならまだ大丈夫だが、グループ会社等に影響があるときなど、情報の確かさが曖昧になるなど困難。信用できる情報を1ヶ所だけでなく、また多くなりすぎない様に整理が必要。
情報報告の基準	…	組織内への報告する判断基準が難しい。担当で判断してしまわないように、体制などの整備が先ずは重要。

＜ 参加事業者からの評価（アンケート結果） ＞

#	設問	回答内容（母数：8事業者）
1	有意義であったか。	非常に有意義：6事業者　　有意義：2事業者
2	有意義であった理由。	・専門家（有識者）の意見や異業種組織の対策が聞けて参考になった ・他組織の状況や色んな視点・視座での意見を聞くことができた
3	時間（60分）は、適切であったか。	適切：8事業者
4	同じグループであった事業者との交流は促進されたか。	促進された：6事業者　　促進されなかった：2事業者
5	不参加事業者の理由	業務都合または他業務との兼ね合い：6事業者 ハードルが高い、必要ないと感じた、テーマに合致しない、事前準備で課題が無かった：各1事業者

3. 演習事後における振り返り（意見交換会）

3-1. 意見交換会の内容

意見交換会での内容は以下の通りである。

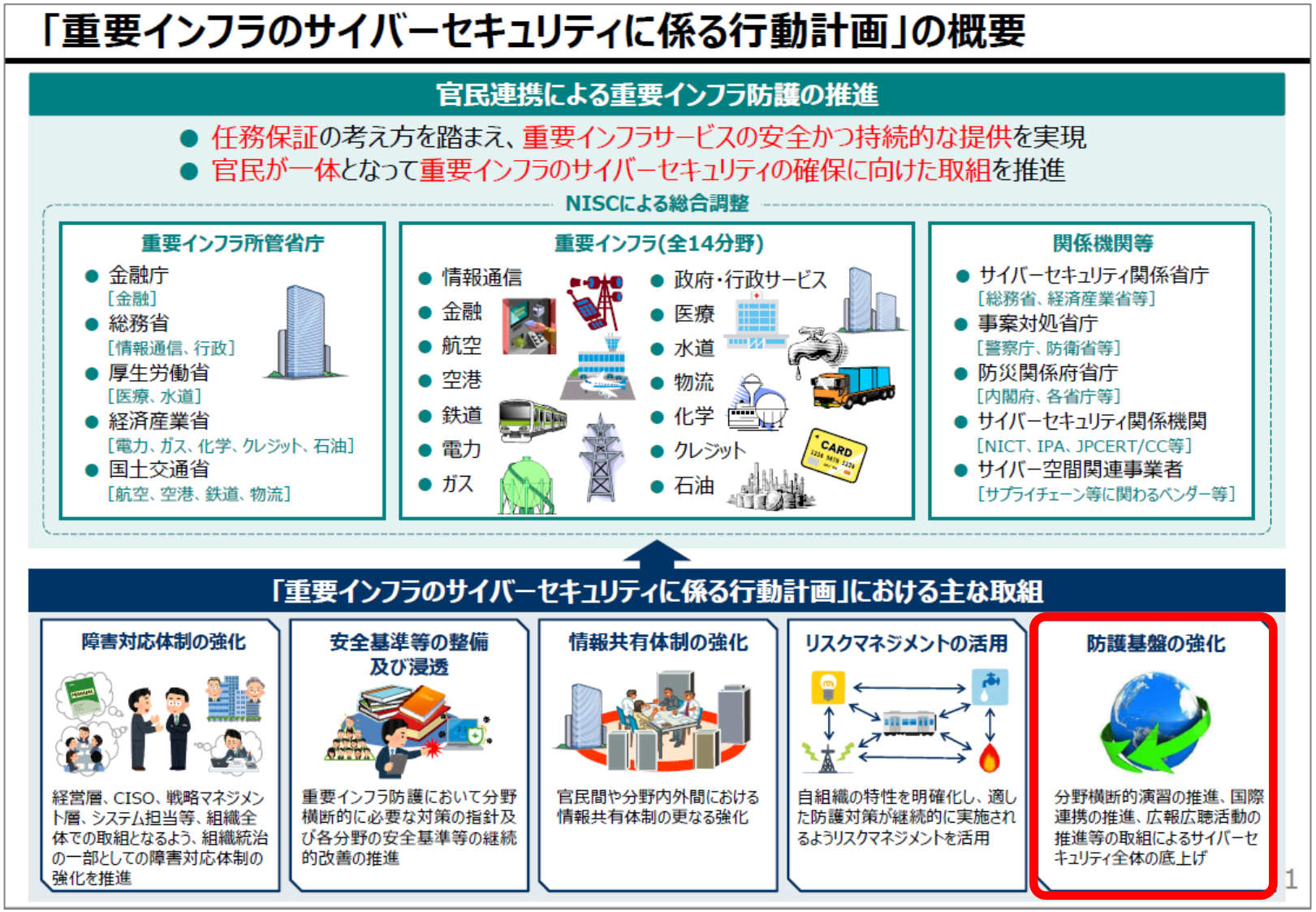
意見の種類	意見の内容
マニュアルの不備	● マニュアルで定めた対応手順など、実際にインシデントが発生したときにそのとおり対応できるのかが課題 ● バックアップをどのように守るかが課題であり、バックアップについては復旧手順まで含めて確認しておく必要がある ● ランサムの手順が無い、手順はあるが詰めていく必要がある ● 規定で全て詰めず、明確にするところ、応用で対応し記録を残すべきところを区分するほうが良い
情報公開	● マスコミへの周知の方針、対外広報のタイミングが課題 ● ホームページが利用できないときの情報公開、広報をどのように行うかが課題 ● 利用者の視点に立つ必要がある。広報にどのような情報を渡すかについても検証が必要である
体制構築	● 平時のCSIRTの運用について、CSIRTを設けている組織と設けていない組織がある ● CSIRT等社内組織だけでなくサプライチェーンやベンダーにも入ってもらいコミュニケーションを高めることが重要 ● 経営を巻き込み、管理、総務、広報等より多くの部門にサイバーセキュリティに協力頂く必要がある
情報共有、伝達、報連絡	● インシデントの判断の遅れ、CSIRTへの連絡の遅れが課題 ● 外部向け連絡網はあるが、実際の運用に不安がある ● 連絡先には復旧支援、犯罪捜査等の立場がある。連絡先と自組織の責任分界点を明らかにしておく必要がある
インシデントの判断	● 通常のエラーがサイバーインシデントに変化するというシナリオであり、公表のタイミングが課題である ● システム障害とサイバーインシデントの判断が課題 ● サイバーインシデントからの復旧の判断について、何をもって復旧とするか難しい
サプライチェーン	● 情報共有を行うサプライチェーンの範囲としてどこまでを含めていくかが課題

＜ 参加事業者からの評価（アンケート結果） ＞

#	設問	回答内容（回答組織数：79事業者）
1	有意義であったか。	有意義：89.9%　どちらでもない：7.6%　有意義でなかった：2.5%
2	有意義であった理由。	・他組織の対策状況や課題等について知ることができた ・他組織と意見交換をすることができた
3	時間（150分）は、適切であったか。	適切：88.6%　長い：8.9%　短い：2.5%

（参考1）「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

分野横断的演習は、重要インフラ行動計画の主要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」に位置付けられています。



（参考1）「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

分野横断的演習は、重要インフラ行動計画の主要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」に位置付けられています。

（参考2）重要インフラのサイバーセキュリティに係る安全基準等策定指針

2023年7月、重要インフラ行動計画を踏まえて安全基準等策定指針を改定しております。

- 安全基準等策定指針とは、安全基準等（＊）において規定が望まれる項目を整理・記載し、重要インフラ事業者や重要インフラ所管省庁の「安全基準等」の策定・改定を支援することを目的とするもの。
- 2023年7月、行動計画を踏まえて改定した安全基準等策定指針では、**組織統治に関するセクションを新設**し、また、委託先等との契約を通じた実効性の確保により**サプライチェーンリスク対策を強化**。

（※）関係法令に基づき国が定める「強制基準」、関係法令に準じて国が定める「推奨基準」及び「ガイドライン」、関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な「業界標準」及び「ガイドライン」、関係法令や国民・利用者等からの期待に応えるべく事業者等が自ら定める「内規」等が含まれる。

組織統治

■ 組織方針・サイバーセキュリティ方針の策定
- ✓ サイバーセキュリティ確保の目的・方向性、維持するサービスの範囲・水準、経営層によるコミットメント等を記載（※）

■ 組織内外のコミュニケーション
- ✓ セキュリティリスク、インシデント等に関するコミュニケーション

■ リスク管理体制
- ✓ サイバーセキュリティリスクを評価・管理する体制の構築

■ 責任及び権限の割当て・資源の確保
- ✓ サイバーセキュリティに関する責任者の任命
- ✓ 経営層による予算・人材等の配分

■ 監査・モニタリング
- ✓ 経営層の責任における監査の実施
- ✓ 脆弱性診断、ペネトレーションテスト等の実施（※）

■ 情報開示
- ✓ サイバーセキュリティ方針、リスク管理体制（※）等の開示

■ 継続的改善
- ✓ 監査・モニタリング、演習・訓練等を踏まえた改善

リスクマネジメント・危機管理

※の箇所は推奨事項

■ 組織状況の理解
- ✓ 重要インフラサービスの外部環境、内部環境の把握
- ✓ リスク管理体制・個別対策の現状把握

■ リスクアセスメントの実施
- ✓ 組織状況と資産を踏まえたリスクアセスメントの実施
- ✓ 目標とする将来像の決定

■ セキュリティ対策・程度の決定
- ✓ 将来像と現状のかい離を埋めるための対策の検討
- ✓ 成熟度モデルの活用により対策の程度・優先順位を決定

■ 個別方針の策定
- ✓ 個々のセキュリティ対策に対する個別方針の策定

■ リスク対応計画の策定
- ✓ 実施事項、責任者、達成期限、評価方法（※）等の明文化

■ サプライチェーン・リスクマネジメントの実施
- ✓ 不正機能の埋め込み、サービスの供給途絶等のリスクへの対応
- ✓ 事業者間の契約におけるサイバーセキュリティリスクへの対応の役割と責任範囲の明確化

■ 事業継続計画等の策定
- ✓ コンティンジェンシープラン、事業継続計画等の策定
- ✓ IT-BCPの策定（※）

■ 人材育成・意識啓発の実施
- ✓ 部署・役職に応じて必要なサイバーセキュリティに関する能力の確保
- ✓ サイバー被害事例の共有（※）等による意識啓発

■ CSIRT等の整備
- ✓ 情報システム等の監視、問題発生時の解析・調査等を実施する体制の構築
- ✓ 制御システム関連部門との連携体制の整備（※）

■ 平時の運用
- ✓ セキュリティ対策の導入、運用プロセスの確立・実行
- ✓ 組織内外との情報共有

■ 危機管理の実施
- ✓ 事業継続計画に則った初動・復旧対応の実施

■ 演習・訓練の実施
- ✓ リスクマネジメント・危機管理体制の有効性検証のための演習・訓練の実施

対策を例示

対策項目

■ 組織的対策
- ✓ 資産の管理
- ✓ 供給者管理
- ✓ システムの取得・開発・保守
- ✓ インシデント管理　等

■ 人的対策
- ✓ 従業員の管理
- ✓ 委託先管理
- ✓ テレワーク・遠隔制御
- ✓ エスカレーション　等

■ 物理的対策
- ✓ セキュリティ確保領域の管理
- ✓ 設備配置等における災害対策
- ✓ 装置の管理　等

■ 技術的対策
- ✓ 利用者アクセスの管理
- ✓ 情報システム等のアクセス制御
- ✓ 暗号を活用した情報管理
- ✓ 多層防御　等

■ 動向を踏まえた対策
- ✓ ランサムウェア対策
- ✓ クラウドサービス利用時の対策

（参考3）内閣サイバーセキュリティセンターからの公開情報

内閣サイバーセキュリティセンターのホームページにて、以下情報を公開しております。

No.	資料名 / URL / 備考	
1	資料名	重要インフラのサイバーセキュリティに係る行動計画
	URL	https://www.nisc.go.jp/policy/group/infra/index.html
2	資料名	重要インフラのサイバーセキュリティに係る安全基準等策定指針
	URL	https://www.nisc.go.jp/policy/group/infra/policy.html
3	資料名	重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書
	URL	https://www.nisc.go.jp/policy/group/infra/policy.html
4	資料名	情報共有の手引書
	URL	https://www.nisc.go.jp/policy/group/infra/policy.html
5	資料名	クラウドを利用したシステム運用に関するガイダンス
	URL	https://www.nisc.go.jp/policy/group/infra/cloud_guidance.html
6	資料名	重要インフラにおける安全基準等の継続的改善状況等の調査について（2021年度）
	URL	https://www.nisc.go.jp/policy/group/infra/policy.html
	備考	P.2 重要インフラ所管省庁のガイドライン、業界固有の基準等の確認にご活用ください。