NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

資料５

２０１５年度　分野横断的演習について

２０１６年３月２５日

内閣官房　内閣サイバーセキュリティセンター(NISC)

２０１５年度分野横断的演習検討会　全体の流れ

検証課題、取組事項等に関する意見の聴取
［所管省庁及び分野代表へのヒアリング］

↓

検証課題、取組事項の決定
第１回作業部会(7/3)
第１回検討会(7/9)

↓

検証課題の具体化、演習アウトラインの決定
第２回拡大作業部会(10/1)

↓

分野横断的演習事前説明会
全体説明会(10/23)
サブコントローラー向け説明会(10/23,28,30)

↓

分野横断的演習（演習当日）
(12/7)

↓

事後の意見交換会、中間報告
意見交換会(1/22)

↓

最終報告案、成果展開用資料案の検討
第３回作業部会(2/26)

↓

最終報告
第２回検討会(3/3)

目次

１．２０１５年度分野横断的演習の概要

２．分野横断的演習の取組にあたって

３．２０１５年度の各取組と、今後の方針

１．２０１５年度分野横断的演習の概要

２０１５年度分野横断的演習　開催概要 ～2006年度より実施～

＜事前説明会＞
全体向け　：　２０１５年１０月２３日（金）
サブコン向け　：　２０１５年１０月２３日（金）、２８日（水）、３０日（金）
場　所　：　東京会場（全体向け説明会の模様について、演習当日まで動画配信）
内　容　：　①重要インフラ防護施策の概要説明（第３次行動計画、情報共有体制）
②分野横断的演習の事前説明
③最新動向等についての有識者講演　等

規程類の事前確認、個別検証課題の確認・調整

＜演習当日＞
日　時　：２０１５年１２月７日（月）１２：１５～１８：１５
場　所　：東京会場、大阪会場、自職場
参 加 者　：３０２組織１，１６８名（うち、６６組織１４９名が大阪会場、
３６組織３１５名が自職場より参加。初参加事業者２０８組織）
【重要インフラ事業者等：１３分野　合計２７７機関】
【セプター：１３分野１８セプター】
【関係機関、分野横断的演習検討会有識者、政府機関　等】


演習の模様(遠藤大臣による視察)


全体振り返りの模様

演習内容：
○第１部　各分野においてサービスへの影響が小さいＩＴ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。（標的型攻撃）
○第２部　サービスへ影響が生じるＩＴ障害が発生し、事業継続が脅かされる事態を想定し、事業継続計画の発動方法や、その手順を確認するなど、事態への対処を検証。（ＤＤｏＳ攻撃、ＯＳ脆弱性、制御システム）

演習を通じた内規・体制等の課題抽出

＜事後の意見交換会＞
日　時：２０１６年1月２２日（金）１４：００～１７：３０
場　所：東京会場、大阪会場
内　容：①分野をまたいだ事業者等間での情報共有（グループディスカッション）
②最新動向等についての有識者講演　等

他事業者等との情報共有を通じた改善の促進

２０１５年度分野横断的演習　報告概要

取組にあたって

第３次行動計画

✓ 重要インフラ全体の防護能力の維持・向上を図る

分野横断的演習の基本方針

- ✓ 事業者等による障害対応能力の向上
- ✓ 重要インフラ全体の対策水準の底上げ
- ✓ 関係主体間の連携・維持の強化
- ✓ 国は事業者等の自律的かつ継続的な取組を支援

分野横断的演習の取組の方向性

- ✓ 課題抽出を通じた改善の促進
- ✓ 参加対象の裾野拡大
- ✓ 情報共有体制の検証
- ✓ NISCの施策への活用

2015年度の取組と今後の取組方針

2015年度の取組実績

- ✓ 演習当日及び前後の説明会・意見交換会等の充実
- ✓ 中堅・中小規模事業者の参加拡大と初心者向け見学会開催
- ✓ 情報共有体制やインシデント対応能力の実効性検証

取組実績等を通じて得た気づき等

- ✓ 年々高まるセキュリティ意識と対策とのギャップ認識の存在
- ✓ ＰＤＣＡサイクルを通じた継続的な訴求の必要性
- ✓ 演習取組全体に対するニーズと有益性の声
- ✓ 情報共有体制の誤認や課題の存在

今後の取組の観点

2015年度の基本方針・取組・演習運営を踏襲しつつ、以下観点の改善についても検討

- ✓ セキュリティ意識の高まりと旺盛な演習ニーズに応える会場新設や参加モデルに係る検討
- ✓ 各事業者のセキュリティ対策・ＰＤＣＡに資する演習運営の検討
- ✓ 情報共有体制の実効性向上に係る施策の検討
- ✓ 分野横断的演習の運営ノウハウや知識等の還元に関する検討

２．分野横断的演習の取組にあたって

分野横断的演習の取組の経緯

第１次行動計画　（2006～2008年度）

【目標】 官民連携の充実

官民連携の仕組みづくり	官民連携体制の機能向上	官民連携体制の実効性向上

年度	2006年度	2007年度	2008年度
人数	90名	120名	136名
テーマ	災害 災害に伴うＩＴ障害の発生 【机上演習】	意図的要因 サイバー攻撃に伴うＩＴ障害の発生	意図的要因 ＩＴ障害の発生 原因を関係者間の情報共有で特定

第２次行動計画　（2009～2013年度）

【目標】 重要インフラ事業者におけるＢＣＰ等の実効性の確認・問題点抽出

① 分野横断的な脅威に対する共通認識の醸成
② 他分野の対応状況把握による自分野の対応力強化
③ 官民の情報共有をより効果的に運用するための方策

2009年度	2010年度	2011年度	2012年度	2013年度
116名	141名	131名	148名	212名
広域停電	大規模通信障害	重要インフラ複合障害	重要インフラ複合障害　＋便乗型ＩＴインシデント	情報セキュリティインシデント

第３次行動計画　（2014年度～）

【目標】 重要インフラ全体の防護能力の維持向上を図る為、事業者等による情報セキュリティ対策の実施及び実効性確認等を通じた障害対応能力の向上を目指す

✓ 事業者等による障害対応能力の向上
✓ 重要インフラ全体の対策水準の底上げ
✓ 関係主体間の連携・維持の強化
✓ 国は事業者等の自律的かつ継続的な取組を支援

年度	2014年度	**2015年度**
人数	348名	**1168名**
テーマ	IT障害発生時の対応に関する事項を軸とし、情報共有体制を含む障害対応体制の実効性を検証	

分野横断的演習の基本方針とその骨格

第３次行動計画が目指す方向性

○ 分野内外の重要インフラ事業者等やサイバー空間関連事業者との依存関係が強くなる中、重要インフラ全体の防護には、全体の対策水準の底上げや関係主体間の連携の維持・強化が重要。

第３次行動計画において分野横断的演習で目指すこと

○ 重要インフラ全体の防護能力の維持・向上を図るため、事業者等による情報セキュリティ対策の実施及び実効性確認等を通じた障害対応能力の向上を目指す。

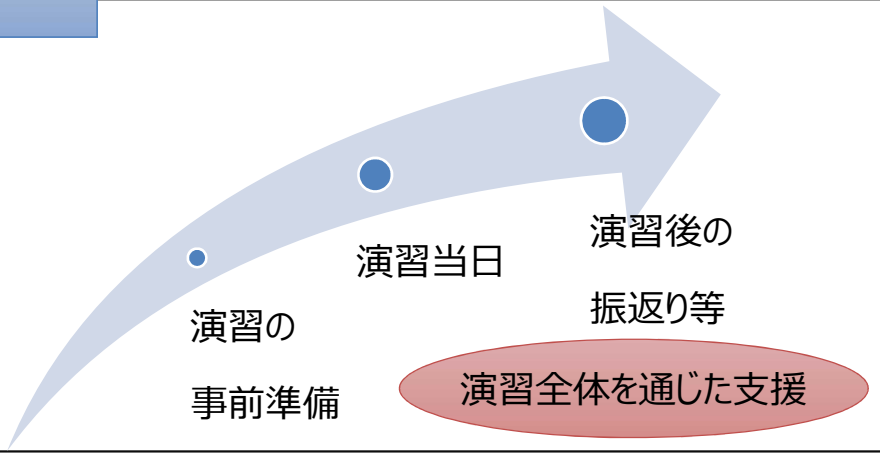
○ 国は、この取組が事業者等によって自律的かつ継続的に行われるよう支援。

分野横断的演習の骨格

○ 事業者等による実効性確認の機会としての演習当日に加え、事前準備及び事後の振り返りにて構成。

・演習当日は、日々の情報セキュリティに関する取組の実効性を確認するための１日でしかない。

・演習の事前準備と事後の振返り等を通じて、事業者等が365日、対策を進めていくことを支援。



演習当日に参加することが重要ではなく、演習当日の気づきを基に、内規や体制をいかに改善できるかが重要。

分野横断的演習の基本方針に基づく取組の方向性

◆ ２０１４年度第１回検討会において、「基本方針」とそれに基づく４つの「取組の方向性」を決定。
◆ NISCは方向性①・②・③に基づいて実施した取組に対して、方向性④の観点から振返りを実施。

目的

重要インフラ全体の
防護能力の維持向上

基本方針

- 事業者等による
  障害対応能力の向上
- 重要インフラ全体の
  対策水準の底上げ
- 関係主体間の
  連携・維持の強化
- 国による事業者等の自律的
  かつ継続的な取組の支援

取組の方向性

①課題抽出を通じた改善の促進
・演習当日及び前後の説明会・意見交換会の充実等

②参加対象の裾野拡大
・中堅・中小規模の事業者等へも参加勧奨

③情報共有体制の検証
・情報共有体制を含む障害対応体制の実効性を検証

④NISCの施策への活用
・本演習の改善点の抽出・分析
・NISCの他施策の改善に活用

２．分野横断的演習の取組にあたって

２０１５年度の取組実績（１/３）

取組実績１：演習当日及び前後の説明会・意見交換会等の充実

事前準備

＜事前説明会＞
- ✓ 演習の検証課題を事前に示し、関連する規程の有無や対策状況の確認を促進
- ✓ 第３次行動計画、情報共有体制について説明を実施

＜サブコン説明会＞
- ✓ サブコンの目的/役割/作業タスクについて個別説明を実施
- ✓ 各事業者の実態に即した演習シナリオの策定や組織の現状把握を推進

＜セプター訓練の実施＞
- ✓ セプター訓練を本演習の前に実施し、分野内の情報共有体制における改善点を抽出

演習当日

＜演習取組＞
- ✓ 東京会場、大阪会場、自職場間で相互連携可能な演習実施環境を設営
- ✓ 演習時間、振り返り時間等を鑑みたタイムラインを確保
- ✓ サブコン中心による演習推進や振り返りリードを実施

＜見学会＞
- ✓ 演習参加を検討している事業者向けの見学会を実施

事後の振返り

＜意見交換会＞
- ✓ 東京会場、大阪会場にて事業者間のグループディスカッションを実施
- ✓ セキュリティに関する対策や課題等の意見交換や人脈形成を促進
- ✓ 「安全基準等」策定指針について説明を実施

２０１５年度の取組実績（２/３）

取組実績２：中堅・中小規模事業者の参加拡大と初心者向け見学会開催

参加者裾野拡大を目指した参加勧奨

- ✓ 参加勧奨用のＤＶＤ動画の配布やYouTubeによる演習施策の報知
- ✓ 所管省庁、セプター事務局等を通じた中堅・小規模事業者への参加勧奨
- ✓ 演習結果や課題抽出をネガティブ化しないステークホルダー全体の演習意識の定着

	２０１３年度	２０１４年度	２０１５年度
参加機関	61組織 (38事業者等)	94組織 (70事業者等)	302組織 (277事業者等)
参加者	212名	348名	1,168名
（大阪会場）	－	10組織32名	66組織149名
（自職場参加）	3組織10名	15組織59名	36組織315名

※今年度演習初参加の事業者等は２０８組織

参加者層を意識した演習シナリオ設計

- ✓ 全参加者のレベルを意識したベースシナリオを策定
- ✓ 事業者のサービス実現方式を鑑みた複数シナリオを整備し、選択方式を採用
- ✓ シナリオの高度化や多様化の要素は、サブコンにてカスタマイズを行い柔軟に実現

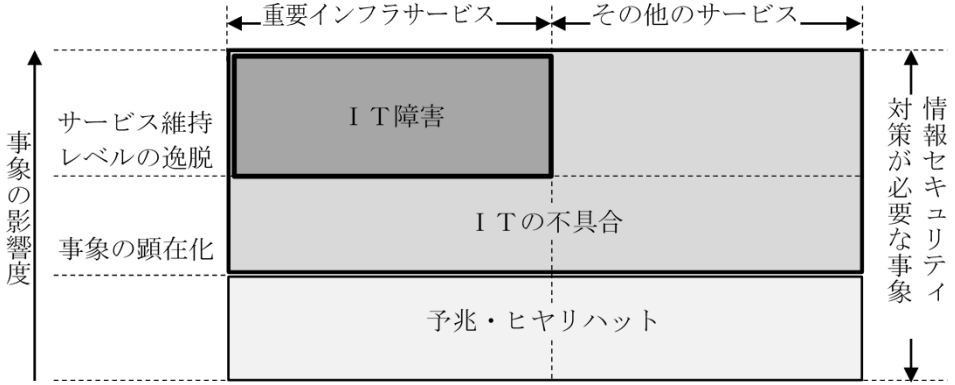
初心者向け見学会開催

- ✓ 演習参加にハードルを感じる事業者向けに演習会場を解放し見学会を開催
- ✓ 演習会場の雰囲気の把握や演習施策内容の理解浸透を促進
- ✓ 来年度の参加検討に向けた土台を形成

２０１５年度の取組実績（３/３）

取組実績３：情報共有体制やインシデント対応能力の実効性検証

■ ２０１５年度の検証課題
- ✓ ＩＴ障害時の対応を軸とし、情報共有体制を含む障害対応体制の実効性を検証
- ✓ 情報共有の対象範囲が、ＩＴ障害だけでなく、ITの不具合や予兆・ヒヤリハットも含まれる点について実効性を検証



（上図）情報共有の対象範囲（第３次行動計画 P45）

＜振返りシートから抽出した気付き・課題＞

◆ ＩＴ障害等における対外的な情報共有
- ✓ 所管省庁への情報連絡の内容、タイミング、基準が曖昧であり今後整備が必要
- ✓ 官民間の情報共有は、ＩＴ障害の未然防止、拡大防止、迅速な原因究明などに効果がある
- ✓ 自組織外からの情報収集や対外的な情報発信については、体制・ルールに一部課題がある

◆ ＩＴ障害等の対応における内部的な判断や意思決定
- ✓ ＢＣＰは策定しているが、セキュリティインシデントを対象としたＢＣＰは策定出来ていない
- ✓ 緊急時に迅速に判断出来るよう、社内へ対応ルールを周知徹底する必要がある
- ✓ 緊急時における判断や対応は、継続的な訓練や演習が重要

【実績まとめ】

１．事前の取組

①スケジュール設計

サブコントローラの役割が正しく機能する事前準備が演習の肝となっていたが、準備期間/説明イベントを充実したことや、各事業者の演習理解度や前向きな姿勢により、予定通りの演習が推進された。

②検証課題の設計

演習で検証出来なかった課題として、「他事業者等（分野内・分野間）との情報共有」が挙げられた。（回答の２３％）

「情報共有アクション」が、検証出来なかった主な理由は以下が推測される。

○個社毎のシナリオ作成により、「官民の情報共有体制の検証」と、「事業者内部の対応」に重点が置かれた為。

○他事業者等（分野内・分野間）の情報共有ルール、体制が不十分な為。

○業法等の定めが無い事象に関する官民間の情報共有について基準不明確とする意見や誤認が存在する為。

⇒ 縦／横の情報共有体制の実効性検証について継続的な取組が必要。

２．演習当日

演習会場、自職場のそれぞれのメリット/デメリットに関する意見が寄せられた。

⇒ 演習参加者のそれぞれ異なるニーズにマッチする柔軟な参加モデルが必要。

３．事後の意見交換会

事後の意見交換会では、自由に意見交換できる環境づくりを行うことで、活発に情報共有・意見交換が行われ、事業者間のネットワーク形成に資することができた。

⇒ 他事業者のセキュリティ対策に関する考え方、ルール、設計等の情報を得られる場は、参加者にとって非常に貴重であり、継続的な取組が必要。

取組実績等を通じて得られた気づきと今後の取組の観点

アンケート、振り返りシート等による得られた内容

- ✓ 2014年フォローアップアンケートの結果、約90.2%の事業者が、演習により課題抽出出来たと回答。
- ✓ 19.1%の事業者が、「リソース不足」等を理由に改善に取組めていない。
- ✓ 23.5%の事業者がセキュリティインシデントを経験

取組実績等を通じて得た気づき等

◆ 各参加事業者においてセキュリティ意識は、年々高まっているが、現状の対策については課題が残存。その対策に対しては、リソース等の問題により、ギャップが存在。

◆ 事業者へのＰＤＣＡサイクルを通じた継続的な訴求の必要性

- ✓ アンケートの結果、99%の事業者が演習が有益であったと回答。
- ✓ サブコントローラ施策により39%の事業者が演習が円滑に進行したという意見
- ✓ 緊急時の対応には継続的な演習が必要という振り返りシートの声
- ✓ 2015年度演習では、重要インフラ事業者以外からの演習参加希望や見学希望の声があり、個別に対応

◆ 本演習の有益性や必要性については、参加者から高評価を得ている。さらなる演習ニーズに対し応える必要がある。

- ✓ アンケートの結果、検証出来なかった項目の23.1%が他事業者（分野内や分野間）との情報共有を挙げている。
- ✓ 行動記録メモ／メール内容の分析の結果、縦の情報共有のルート誤りが存在

◆ 官民間の情報共有体制について誤認が存在する。また、横の情報共有に関する課題が存在する。

取組実績等を通じて得られた気づきと今後の取組の観点

取組実績等を通じて得た気づき等

- 年々高まるセキュリティ意識と対策とのギャップ認識の存在
- ＰＤＣＡサイクルを通じた継続的な訴求の必要性
- 演習取組全体に対するニーズと有益性の声
- 情報共有体制の誤認や課題の存在

今後の取組の観点

２０１５年度の基本方針／取組／演習運営を踏襲しつつ、さらなる改善について検討を行う。

➢ セキュリティ意識の高まりと旺盛なニーズに応える会場新設や参加モデルに係る検討

（例）
- 九州会場の新設
- 会場/自職場/両立等の参加モデル
- 他サイバー演習の運営ノウハウの取り込み

➢ 各事業者のセキュリティ対策・ＰＤＣＡに資する演習運営の検討

（例）
- サブコン施策による教育、スキル継承
- 経営理解の増進
- CSIRT能力向上

➢ 情報共有体制の実効性向上に係る施策の検討

（例）
- 金融ＩＳＡＣ、Telecom-ISAC等との演習連携強化
- 分野内外の情報共有を促すシナリオ設計

➢ 分野横断的演習の運営ノウハウや知識等の還元に関する検討

（例）
- E-learning等の仮想演習環境の導入
- 国際連携（海外組織との連携強化）