「2009年度重要インフラの分野横断的演習に関する調査」の結果について

2010年9月9日
内閣官房情報セキュリティセンター（NISC)

1. 分野横断的演習の背景

重要インフラ事業者のIT障害対策における課題を抽出するため、分野横断的な演習を2006年度から継続的に実施

1.1 第1次行動計画における分野横断的演習の概要

	2006年度	2007年度	2008年度
目的	**官民連携の仕組み作り** 官民連携の仕組みづくり、官民連携の枠組みの実効性の向上のための取組みや課題の発見	**仕組みの妥当性検証** （仕組みが適切に構築されているかどうか） 官民の情報共有、連絡連携の仕組みの妥当性の検証	**仕組みの実効性検証** （仕組みが各主体にとって有効に機能しているかどうか） 官民の情報共有、連絡連携の仕組みの実効性の検証
手法	研究的演習・机上演習	機能演習	機能演習（フェーズ2）
結果	1. 分野を超えて情報を把握する仕組みの構築の必要性、情報連絡や共有に関して効果的なコラボレーションが図られる環境や仕組みづくりの必要性が認識できた。 2. 多様な脅威や状況を想定した演習、情報共有の意義を実感する演習の実施の必要性を認識できた。	1.「NISC、所管省庁、セプター、重要インフラ事業者等からなる情報共有の仕組み」の検証において、事業者等とNISCを両端とした情報の流れが想定通り機能することが確認された。 2. 情報共有レベルや情報連絡・提供フォーマットといった実際に情報連絡・情報提供を行う際の、運用上の具体的課題が明らかになった。	1. 状況に応じた情報連絡、情報提供、情報共有が行われ、現在の官民の情報共有体制が概ね有効に機能していることが確認された。 2. 情報共有体制の更なる実効性向上のため、緊急時に共有すべき情報の内容やIT障害発生時の各主体の対応等について、引き続き検討を進めていく必要性が認識されている。

1. 3ヶ年に渡る段階的な分野横断的演習の実施により、行動計画に基づく現在の官民の情報共有体制の仕組みの妥当性や実効性の検証を行い、概ね有効に機能していることが確認された。
2. 情報共有体制の更なる実効性向上のため、今後も演習による課題の抽出などを引き続き行い、検討を継続していく必要性が認識されている。

1.2　第2次行動計画における演習の展開

第1次行動計画

＜2006年度＞
官民連携の仕組みづくり

研究的演習
演習実施概念、演習課題設定、演習手法の理解等を主眼として実施。

机上演習
脅威として災害を設定し、会議形式の演習を実施。

＜2007年度＞
官民連携体制の機能向上

機能演習
脅威としてDDoS攻撃を設定し、チーム毎に個室に分かれ、メールのみを利用した演習を実施。

＜2008年度＞
官民連携体制の実効性向上

機能演習
参加者にIT障害の発生原因を知らせないなどより現実に近い状況で、起こった現象に関する関係者間の情報共有により原因を特定し、サービスの維持・早期復旧や事業継続等を行っていく演習を実施。

分野横断的な演習手法に関する知見

第2次行動計画 *

分野横断的な重要インフラ防護対策の向上

目標

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

得るもの

演習に関する施策

① シナリオ、実施方法、検証課題等を企画し、演習を実施
② IT障害発生時の早期復旧手順・事業継続計画の検討状況等を把握し、その結果を演習参加者等に提供
③ 演習の向上策検討
④ 演習の実施方法等に関する知見の集約・蓄積


机上演習状況


機能演習状況

＊「重要インフラの情報セキュリティ対策に係わる第2次行動計画」における分野横断的演習の推進方策

演習の検討、実施を通じて得られた演習シナリオ、状況付与及び演習手法などに関する課題や知見の整理を行う。
整理した課題や知見は、次回の分野横断的演習のシナリオ作成や演習手法の検討等に反映するとともに、知見の継続的な拡充に努める。
これらの課題や知見は、関係者に示すことにより共有し、各重要インフラ分野の情報セキュリティ対策の強化のための取組みへの活用を推進する。

1.3　演習におけるインシデント設定の考え方

検証課題　重要インフラ事業者等における事業継続計画（BCP）の策定・改訂に向けた課題の抽出

・3年間の進め方

重要インフラ事業者等がBCPで想定しているインシデントを各年度毎に設定して行うこととし、重要インフラ事業者等からの希望が多かった、他分野のサービス障害の自分野システムへの波及、または自分野のサービス障害の他分野への波及に関する検証を行う。

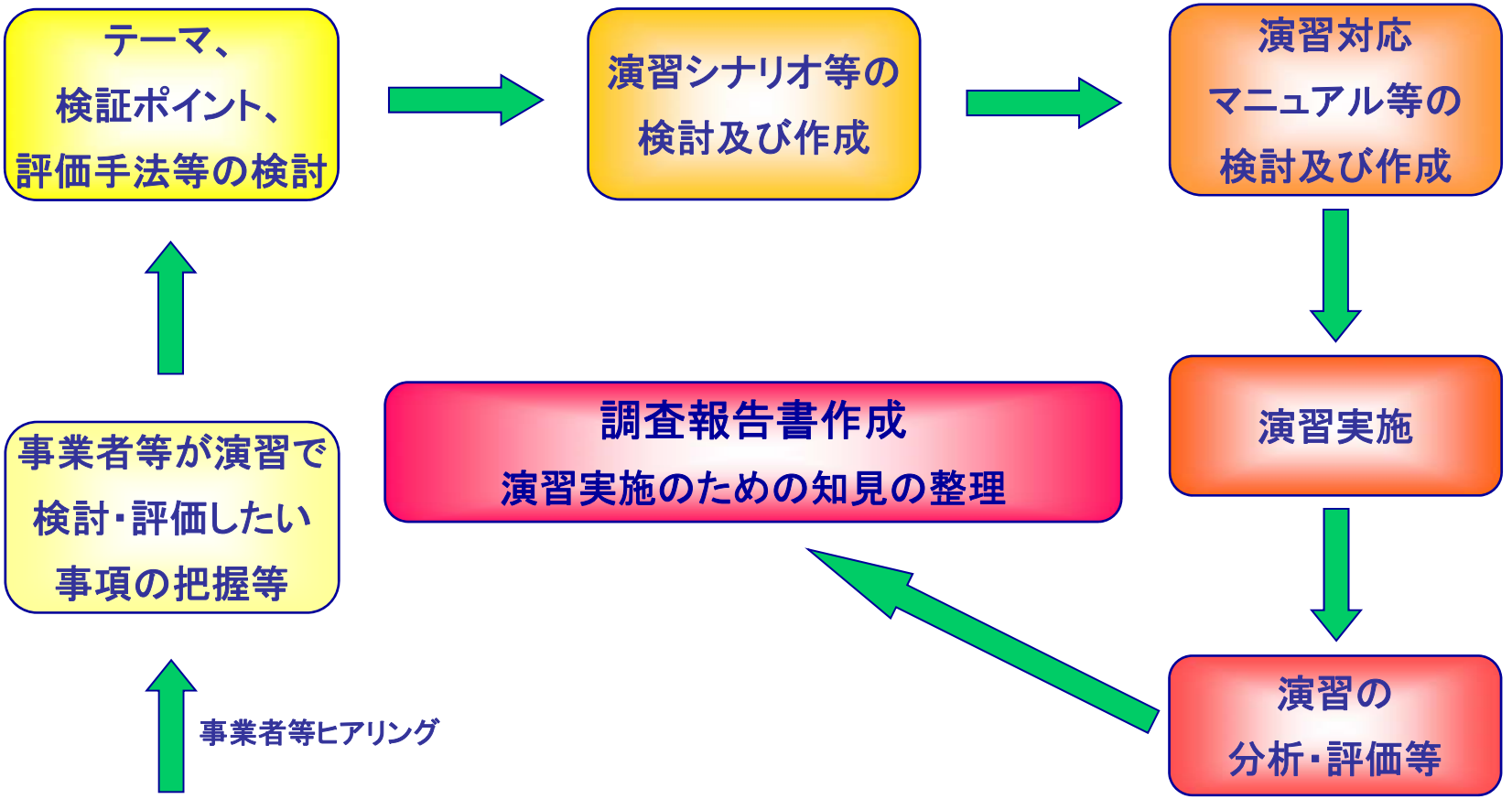
	2009年度	2010年度	2011年度
他分野の波及の例	電力＋α	通信＋α	水道＋α

※2010年度及び2011年度のサービス障害が発生する分野は、当該年度の検討会で最終的に確定する

・上記の留意点

・主として、他分野のサービス障害が各分野の分野システムに与える影響に関して、BCP等の策定・改訂の視点から検証を行う
・サービス障害が発生する分野については、シナリオ作成面からの協力もお願いする
・上記演習のほか、ミニ演習を実施し、多様なテーマを取り上げる

2. 演習の進め方



＜基礎的調査＞

① IT障害等に係る国内事例及び最新動向の把握等

② 情報セキュリティ対策に係る周辺状況及び最新動向の把握等

③ 過去に実施された演習におけるテーマ、検証ポイント、手法、抽出された課題等の把握

※演習の検討に際しては、有識者、重要インフラ事業者等からなる検討会を設置し、適宜意見を聴取しながら実施。

3. 2009年度演習の全体像

目的

重要インフラにおける分野横断的演習の実施により、分野横断的な脅威に対する共通認識の醸成、他分野の対応状況把握による自分野の対応力強化、官民の情報共有をより効果的に運用するための方策検討を推進し、分野横断的な重要インフラ防護対策の向上を目指すことを目的とした。

検証課題と検証項目

・重要インフラ事業者等における事業継続計画（BCP）の策定・改訂に向けた課題の抽出

（1） 停電直後の対応　（2） 停電中の対応　（3） 復電前後の対応
（4） 関連部署・組織との連絡　（5） BCPの発動基準　（6） 停電時間による対応の違い

本年度演習のポイント

○サービスの波及への注目

他分野のサービス障害が各分野のシステムに与える影響に関して、昨年度までに実施した相互依存性解析の結果も踏まえ、BCP等の策定・改訂の視点から検証を行った。

○事業者におけるシナリオ作成

サービス障害が発生する分野がシナリオ作成にも関わることで、関係者における演習に関する知見の蓄積を促進した。

○演習前の事前確認の重視

演習の成果として、演習当日の対応に加え、演習前に各分野の状況を確認し、各自が気づきを得る部分を重視した。

○多様なテーマからの検討（ミニ演習の実施）

複数のミニ演習を実施し、多様なテーマを検討することで、BCPについて複数の観点からの検証を行った。

シナリオ概要

20XX年8月3日（火）朝10:00、熱帯夜明けの良く晴れた暑い日に、我が国において広域的な停電が発生し、通信・水道のサービス提供の一部に影響が波及した。その結果各重要インフラ分野においては、IT障害の未然防止・被害最小化のために対応を迫られた。

成果

- 重要インフラ事業者等におけるBCP等の策定・改定への活用
- 重要インフラ分野における演習実施のための知見集の策定

4. 演習の実施

1. 日時: 2009年11月27日(金) 12:30 ～ 18:30
※ 10:45～12:15 受付
※ 11:00～12:00 ツール試用 (参加自由)

2. 場所: 株式会社三菱総合研究所 2階セミナー室、大・小会議室

3. 参加者(プレイヤー、コントローラーを含む):116名

(政府)
内閣官房情報セキュリティセンター、重要インフラ所管省庁

(重要インフラ分野:10分野)
情報通信(通信、放送)、金融(銀行、生命保険、損害保険、証券)、航空、鉄道、電力、ガス、
政府・行政サービス、医療、水道、物流

(セプター:10分野 14セプター)

(関係機関)

(共通脅威分析および分野横断的演習検討会 有識者)
慶應義塾大学大学院 大林教授(座長) 他

4. 概要
我が国において広域的な停電が発生し、通信・水道のサービス提供の一部に影響が波及した。その結果、各重要インフラ分野においては、IT障害の未然防止・被害最小化のために対応を迫られた。

5. 演習全体を通じて得られた主な気づき

■ 討論形式のミニ演習を通じ、重要インフラ分野における演習及びBCPに関する最新の動向・知見を共有し、効果的な機能演習・机上演習を実施することで、各重要インフラ事業者等において停電時の情報システムの稼働継続に関わるBCPの策定・改訂に向けた気づきを得ることができた。

■ ITシステムの運用には、人、電力、冷却水等が必要であるが、ITシステム担当者が把握していない事項があり、まだ改善の余地があることに気づいた。

演習より得られた主な気づき

1. バックアップ電源に接続している重要負荷の確認（負荷の優先度再確認）
2. バックアップ電源への切替動作検証および電源正常動作検証の定期的な実施
3. 停電時でもBCP等の必要書類を確認可能な環境整備（紙で保管等）
4. 停電が長引いた際の対応（負荷の絞込み、電源燃料の確保等）の明確化
5. 水冷式機器に必要な水の確保方法の明確化
6. 復電のタイミングに関する社内の意思決定方法の明確化
7. 停電や復電に関する情報開示、情報収集におけるマスコミの活用
8. 交代を含む要員の確保（居住地、連絡先のリスト化、宿泊先確保等）

6. 参加者による演習の評価

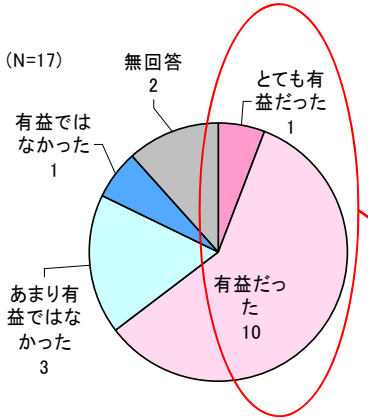
■ ミニ演習や事前調査、演習を通じ、多数の気づきが得られたとの意見が多数寄せられた。

■ 一部分野のシナリオ策定への参加や、演習前の事前確認の強化など、新たに採り入れた演習手法について有用との評価が得られた。

■ 全5回のミニ演習へは延べ159名、機能演習・机上演習へは116名が参加し、2009年度の分野横断的演習の参加者は合計275名に達した。

■ 機能演習について「有益だった」とする事業者等は17者中11者（65%）であった。

自組織の停電対応について
事前確認を行う演習の有益度
（事業者向けアンケート結果）



【主な意見（要約）】

・自家用発電機の状況、縮退運転の手順、水冷方式機器の存在等を再確認することで、認識を深め、新たな知見を得られた。

・停電時の対応について、担当者だけでなくBCP本部でも把握する契機とできた。

・データセンター等の自家用発電機継続時間等を確認できた。

・基本的な対応部分に業界内差異がないことを確認できた。

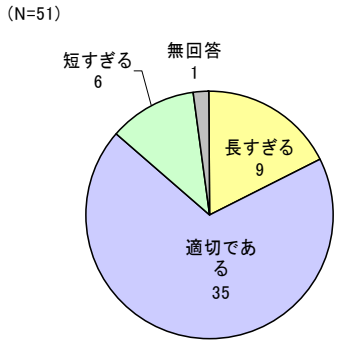
・演習本番より事前確認によって得られた課題があった。

7. 今後の演習に対する意見

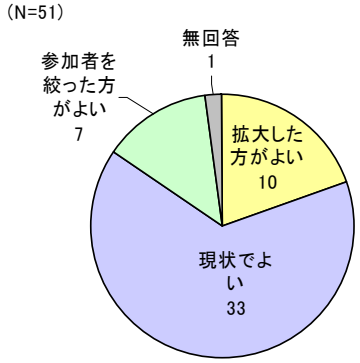
■ 演習時間や演習規模に関しては、今年度と同等の演習に対するニーズが多かった。

■ シナリオについては、サイバーセキュリティの要素を強めた演習や分野間のサービス波及を重視した演習に対する要望が、また演習手法については、職場環境を含めた演習や重要インフラの共有リソースを採り入れた演習に対する要望が多かった。

演習時間



演習規模



【その他の主な意見】

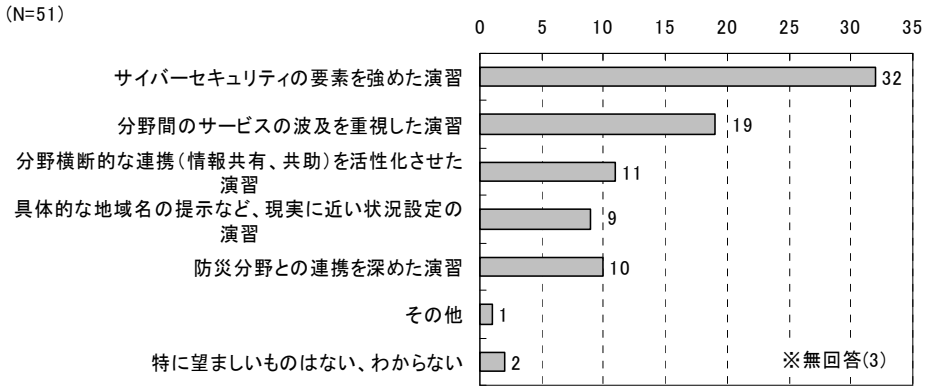
・もっと長い停電を検証したかった。

・演習の目的は、情報共有に関する事項の確認・検証か、各事業者等の対策の強化・検証なのか明確にしてほしい。

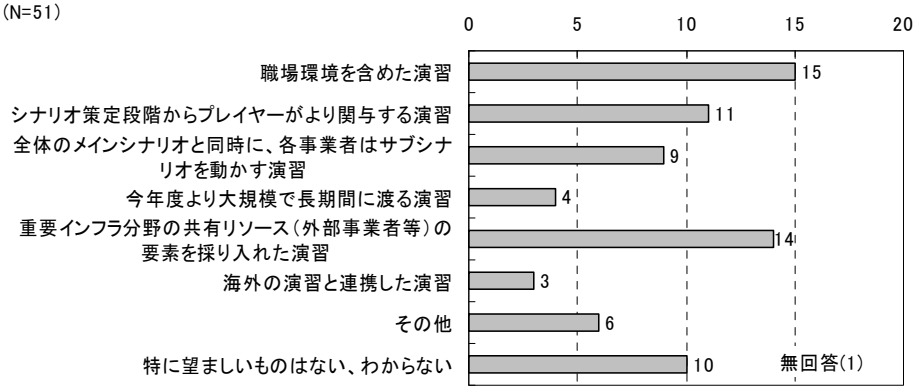
・意見交換会の進め方の改善。

・NISCに集まる情報をいかに適切に展開すべきか。

シナリオに対する要望



手法に対する要望



8. 演習のまとめ

2009年度分野横断的演習における成果

1. 分野横断的演習を通じ、各重要インフラ事業者等において停電時の情報システムの稼働継続に関わるBCPの策定・改訂に向けた気づきを得ることができた。
2. 分野横断的演習に対しては、多数の参加者が必要性を感じており、今後も重要インフラ防護の観点からシナリオや手法に関して関係者との検討を重ねつつ、継続して実施する意義が再認識された。
3. 過去3年間で構築されてきた官民の情報共有体制を通じてIT障害発生時に円滑な情報共有がなされることが再確認できた。

2009年度分野横断的演習で得られた主な課題

●分野横断的演習の意義を増すためには、共有リソース（ベンダや燃料等）の輻輳を想定したシナリオも検討する必要がある。

●BCPを始めとする重要インフラ防護対策の検証のためには、よりクリティカルな状況（期間や規模等）についても想定する必要がある。

次年度以降の演習に対する方向性

■重要インフラの防護力の向上を目的として、クリティカルな状況設定の必要性や、サイバーセキュリティや分野間の波及を重視して欲しい等の要望も加味し、参加者の負担を考慮しつつ、重要インフラサービスのカスタマーである国民・社会の視点も含めた上で、今後も最適なシナリオを検討する必要がある。

■情報共有を図る上で通信手段確保の重要性が改めて認識されており、通信サービスが与える影響を次年度の演習シナリオとして検討してはどうか。

■次年度以降は、職場環境における演習の実施等、新たな手法を検討してはどうか。

■事業継続のためのリソース確保の観点から、制度的な課題の整理も必要ではないか。

■共通脅威分析の成果を考慮して、演習シナリオを検討してはどうか。