参考資料2

「2011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

2012年3月15日

内閣官房情報セキュリティセンター（NISC）

「CIIREX 2011 」（シーレックス2011）
<Critical Infrastructure Incident Response EXercise 2011>

1. 演習の背景－第2次行動計画における分野横断的演習の目標と実績

第1次行動計画（2006～2008年度）

＜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等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（2009～2011年度）

【目標】重要インフラ防護対策の向上 ～事業継続計画（BCP）の充実等～

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

年度	2009年度	2010年度	2011年度
テーマ	広域停電	大規模通信障害	重要インフラ複合障害
取組み	① シナリオ、実施方法、検証課題等を企画 ② 早期復旧手順・事業継続計画等の検証、共有 ③ 演習の実施方法等に関する知見の集約・蓄積	① シナリオ、実施方法、検証課題等を企画 ② 早期復旧手順・事業継続計画等の検証、共有 ③ 演習の実施方法等に関する知見の集約・蓄積 ④ 自職場演習の導入	① シナリオ、実施方法、検証課題等を企画 ② 早期復旧手順・事業継続計画等の検証、共有 ③ 演習の実施方法等に関する知見の集約・蓄積 ④ 自職場演習の拡充 ⑤ サブシナリオの導入 ⑥ 重要インフラ分野、事業者間の連携推進

2. 演習の概要

1. 日時: 2011年12月12日(月) 12:00 ～ 18:30
※ 10:40～11:50 受付
※ 10:45～11:45 ツール試用 (参加自由)

2. 場所: 株式会社三菱総合研究所(東京都千代田区永田町2－10－3) 4階会議室
一部事業者における自職場

3. 参加者(プレイヤー、コントローラーを含む):
37組織131名が参加(内3組織12名が自職場参加)

(重要インフラ事業者等: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
※ 証券事業者(1社)及び物流事業者(1社)が自職場演習、物流事業者(1社)がサブシナリオ策定

(セプター:10分野 14セプター)
※ 証券セプターが自職場演習

(関係機関)

(分野横断的演習検討会 有識者委員)
慶應義塾大学大学院 大林教授(座長) 他

(政府)
重要インフラ所管省庁、内閣官房情報セキュリティセンター

4. 概要
20XX年X月X日、我が国の首都圏を中心として大規模な重要インフラ(電力、通信、水道、ガス)の複合障害が発生した。その結果、各重要インフラ分野においてはサービスへの影響の確認が必要となり、IT障害の未然防止・被害最小化のために対応を迫られた。

3. 演習において得られた主な気づき（1）

■ 一部組織における自職場演習やサブシナリオの導入、演習説明会での「事業者における東日本大震災の対応について」の講演の実施等、より実践的な機能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電力・通信・水道・ガスの複合障害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。

複合障害を想定した演習において得られた主な気づき①（全20項目）

（1）複合障害発生から復旧までの社内対応（8項目）

- バックアップセンター復旧手段の確認の必要性
- 断水の長期化に伴う、各種影響の把握及び、バックアップセンターへの切替判断の必要性
- 長時間の停電や計画停電時の、非常用発電機等の稼動継続のための燃料調達方法の確認の必要性
- インフラサービス復旧の目処が立たない状況でのサービス継続判断の重要性
- 同業他社との連携を考慮したサービス再開の判断の重要性
- 障害に便乗した風説に対する社内対応や顧客への周知方法の必要性（フィッシング等への対応）
- 障害に便乗した標的型攻撃に対応する必要性（通常時と異なる体制や混乱時の対応）
- 標的型攻撃に関する具体的情報の有効性（攻撃元の特定、注意喚起等）

3. 演習において得られた主な気づき（2）

複合障害を想定した演習において得られた主な気づき②（全20項目）

（2）関連部署・外部事業者との連絡（2項目）

- 通信障害時の社内関係部署及び外部事業者（取引先、委託先、ベンダー等）との多様な通信手段の確保（優先電話、衛星電話等）の必要性
- 復旧に関わる分野間の連携について、平時から意見交換を行う必要性

（3）BCP等の発動（1項目）

- 原因不明の複合障害発生時におけるBCPの発動及び危機管理体制の確立の必要性

（4）所管省庁・マスコミ・顧客を含む外部対応（8項目）

- 障害発生時の顧客側の視点に立った情報発信の有効性
  （輻輳時のコールセンター番号変更案内や公衆電話等代替連絡手段の周知　等）
- 外部発表のフォーマットを事前に準備することの重要性
- 外国人向けの情報発信の必要性
- マスコミによる適切な情報発信の有効性（全体状況の把握、優先順位の見極め　等）
- 各分野からマスコミへの情報提供の在り方検討の有効性
  （全体の状況、前回情報提供分との変更点の明確化、サービス提供への影響有無　等）
- 障害発生時の情報収集における、マスコミ報道の有効性
- 国民に対して安心情報を発信することの重要性（サービス障害が発生していない情報の開示）
- 障害発生時における各分野が共有できる掲示板の有効性

（5）リアルな演習における効果（1項目）

- IT部門から広報部門へのスムーズな情報発信の情報開示における有効性

4. 演習の総括－2011年度演習の結果

検証課題毎の評価	
(1)複合障害発生から復旧までの社内対応	・電力（計画停電を含む）、通信、水道、ガスの複合障害への対応手順等について実践的な環境において、概ね検証することができた。
(2)緊急対応体制と社内外の連絡体制の整備	・障害規模や復旧見込みの把握のために、障害発生した各分野とそれ以外の事業者等において積極的な情報共有がなされた。また、複合障害発生時の連絡方法については、複数の通信手段等を検討する必要性が認識された。
(3)BCP等の発動	・BCP等（マニュアル等も含む）については、各事業者等で概ね複合障害に対応していることが確認できた。サプライチェーンの混乱や標的型攻撃への対応も含め、BCP等の改善に向けた気づきも得られた。
(4)所管省庁・マスコミ・顧客を含む外部対応	・多くの事業者等が、障害発生時のサービスへの影響の有無や復旧状況について積極的に情報開示を行った。特に、代替サービスの案内、風評等に対する正しい情報、フィッシングに関する注意喚起など、顧客視点の情報開示も見られた。
(5) リアルな環境における演習の効果	・自職場演習及び初めて導入したサブシナリオ策定を通じて、より実践的な情報共有体制の実効性や、広範囲で高度な情報共有・意思決定が検証できた。

演習運営面での評価

・自職場演習は昨年度より1事業者が増え、自職場からの参加を促進できた。
・サブシナリオ策定には1事業者が参加し、今後の各分野別のシナリオ策定のための課題が抽出できた。
・演習参加者の情報共有を充実させるための、意見交換会の活性化、他分野に聞きたいことに関する事前ヒアリング、検討会メンバー以外の演習参加者のオブザーバ参加などの取り組みにより、演習の更なる活性化が図れた。

演習全般を通して得られた成果

1. 自職場演習及びサブシナリオの導入、また、サプライチェーンの混乱や標的型攻撃を組み合わせたシナリオを用いた実践的な演習を通じて、各重要インフラ事業者等において、複合障害時の効果的な対応に向けた多くの気づきを得ることができた。

2. 複合障害によって連絡手段が限定された場合の代替通信手段等を確認することにより、関係者間の情報共有の実効性向上に寄与した。

4. 演習の総括－3ヵ年の分野横断的演習の結果

	2009年度	2010年度	2011年度
テーマ	広域停電	大規模通信障害	重要インフラ複合障害 （電力、通信、水道、ガス）
取り組み	①シナリオ、実施方法、検証課題等を企画 ②早期復旧手順、事業継続計画等の検証、共有 ③演習の実施方法等に関する知見の集約・蓄積	①シナリオ、実施方法、検証課題等を企画 ②早期復旧手順、事業継続計画等の検証、共有 ③演習の実施方法等に関する知見の集約・蓄積 ④自職場演習の導入	①シナリオ、実施方法、検証課題等を企画 ②早期復旧手順、事業継続計画等の検証、共有 ③演習の実施方法等に関する知見の集約・蓄積 ④自職場演習の導入 ⑤サブシナリオの導入 ⑥重要インフラ分野、事業者間の連携促進
結果	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。	1．自職場演習の導入や世間の風評掲示への対応等、実践的な演習を通じて、各重要インフラ事業者等において、通信障害時の効果的な対応に向けた多くの気づき（通信困難時の情報共有手段や対応策、適時かつ確実な情報開示、グループ間の対応手順の整合性確保等の必要性等）を得ることができた。 2．IT障害時に連絡手段が限定された場合の対応策の検討により、官民の情報共有体制の実効性を確認できた。	1．自職場演習及びサブシナリオの導入、また、サプライチェーンの混乱や標的型攻撃を組み合わせたシナリオを用いた実践的な演習を通じて、各重要インフラ事業者等において、複合障害時の効果的な対応に向けた多くの気づきを得ることができた。 2．複合障害によって連絡手段が限定された場合の代替通信手段等を確認することにより、関係者間の情報共有の実効性向上に寄与した。

1．3ヶ年に渡る段階的な分野横断的演習の実施により、演習参加者においてBCPの策定・改訂に向けた気づきの獲得、課題の抽出を行うことができた。

2．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実効性の検証を行い、障害発生時も有効に機能していることが確認できた。

5. 課題と対応の方向性

2011年度に得られた主な課題

－演習参加者において、
より多くの気づきを得る－

より効果的な演習の実施

更なる情報共有の活性化

**演習成果の普及促進と
演習参加者の拡充**

2012年度以降の演習に対する方向性

■ **より効果的なシナリオ策定**
- 分野横断的な連携の強化や新たな環境変化に対応した演習テーマの検討
- 演習参加者の対応能力向上につながる演習シナリオの検討（虚実判断が難しい風評、代替システムが絶たれた状況での対応など）
- 各事業者又は、各分野の事情に応じた独自のサブシナリオの策定
- 演習シナリオ作成のための十分な準備期間の確保
- 演習参加者が十分に課題の検証を行えるような演習シナリオの効果的な時間配分

■ **助言方法のあり方の検討**
- 演習参加者の判断・行動を、専属の助言者によってアドバイスする仕組みの導入
- アドバイスすべき視点の明確化

■ **演習実施環境の習熟**
- 事前説明会等における、演習ツール（PC、メーリングリスト、掲示板等）試用機会の提供

■ **より効果的な情報共有方法の検討**
- 官民及び分野間における情報共有の活性化を考慮したシナリオ及び検証課題の検討

■ **演習における気づきの共有を目的とした意見交換会の活性化**
- 各参加者の関心が高い論点の抽出
- 自職場から意見交換会へ参加する為の環境整備

※演習の終了後に演習参加者による意見交換会を開催し、気づきの共有を図っている。

■ **演習成果の普及促進**
- 演習成果展開用の資料作成（演習で得られた気づき、事前確認事項のチェックリスト化など）
- 効果的な演習成果の展開

■ **自職場演習及び首都圏以外の参加者拡充に向けた取り組み**
- 演習テーマ、シナリオ概要等の早期決定と演習参加候補者への早期情報提供