- CIIREX2012 -

参考資料6

「2012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

2013年3月14日

内閣官房情報セキュリティセンター（NISC）

「CIIREX 2012 」（シーレックス2012）
<Critical Infrastructure Incident Response EXercise 2012>

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

第1次行動計画（2006～2008年度）

【目的】官民連携の充実

2006年度

目標： 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

目標： 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

目標： 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（2009～2013年度）

【目的】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

目標

(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	2012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	重要インフラ複合障害＋便乗型ITインシデント
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	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 サブシナリオの拡充 ⑥ 重要インフラ分野、事業者間の連携推進 ⑦ 第三者による助言の導入

2. 演習の概要

1. 日時: 2012年12月10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):
42組織148名が参加(内3組織15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、ガス事業者(4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、ガスセプターがサブシナリオ策定

(関係機関) IPA、JPCERT／CC

(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

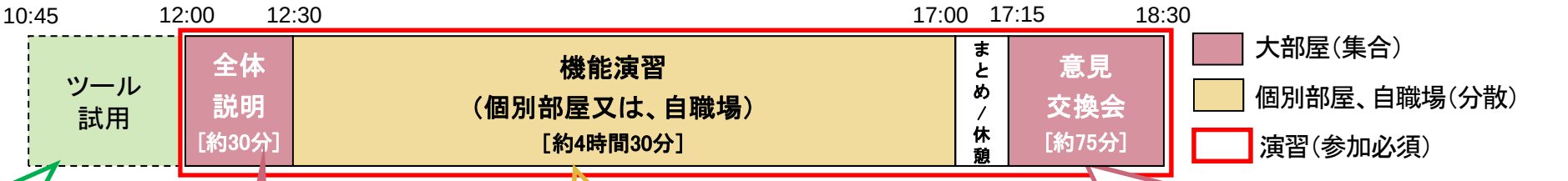
(政府)
重要インフラ所管省庁、内閣官房情報セキュリティセンター

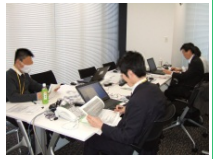
4. 概要
20XX年XX月XX日、我が国の首都圏を中心として大規模な重要インフラ(電力、通信)の複合障害、及び複合障害に便乗した情報セキュリティインシデントが発生した。その結果、各重要インフラ分野においてはサービスへの影響の確認が必要となり、IT障害の未然防止・被害最小化のために対応を迫られた。

3. 分野横断的演習とは～演習の様子

機能演習では、事務局からの状況付与（各種障害状況、攻撃状況等）に従い、プレイヤーは、“メール”、“電話”、“掲示板（仮想HP）”等を用いて、他プレイヤーとの情報共有を行ないながら、発生した事象への対応をおこなう。
また、演習で得られた気づきは、演習後の意見交換会において、演習参加者間で共有する。

［演習当日のタイムスケジュール］



機能演習で使用する各種ツール（メール、掲示板等）の試使用、ホワイトボード書込み準備、通信確認などを事前におこなう。（自由参加）



演習参加者全員が集合し、機能演習における各事業者の対応内容の紹介や他分野事業者等への質問など意見交換をおこない、更なる気づきを得る（参加必須）
※2月の拡大WGでも意見交換会を追加実施。


演習参加者全員が集合し、演習開会式の後、機能演習に関する留意事項等について説明をおこなう。（参加必須）

［演習事務局、関係機関等、コントローラ事業者］



・演習事務局は、各種障害状況、攻撃状況等を“メール”で付与する。
・関係機関、コントローラ事業者は、“メール”又は、“掲示板（仮想HP）”でシナリオに則した関連情報の提供と共に、プレイヤー（事業者等）からの問合せ対応等もおこなう。

［事業者等、セプター］



［NISC、所管省庁］


［ｾﾌﾟﾀｰｶｳﾝｼﾙ事務局］

演習参加組織毎に個室に分散し、演習事務局から与えられる状況付与（各種障害状況、攻撃状況等を“メール”で送信）や、関係機関、コントローラ事業者からシナリオに則した関連情報の提供（メールもしくは、掲示板［仮想HP］）に従い、プレイヤーは、“メール”、“電話”、“掲示板（仮想HP）”、“ホワイトボード”等を用いて、他プレイヤーとの情報共有を行ないながら、発生した事象への対応をおこなう。

4. 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「近年のサイバー攻撃の動向」「標的型メールの最近の動向」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・通信の複合障害時の情報システムの稼働継続及びBCPの策定・改訂に向けた気づき、複合障害に便乗した情報セキュリティインシデントへの効果的な対応に関する気づきを得ることができた。

演習において得られた主な気づき（複合障害）

●電力、通信等のリソース確保に関する気づき
- ・データセンター等の重要設備に関わる非常用電源の容量や負荷状況把握の重要性
- ・計画停電の除外対象地域に関する事前確認の必要性
- ・優先して対処すべき通信インフラを事前に把握しておくことの必要性
- ・情報システム稼働のための機器における、水確保の重要性

●情報共有・情報開示に関する気づき
- ・非常時の他事業者、所管省庁とのコミュニケーションの必要性
  （計画停電除外、燃料割当て、通信サービス復旧優先順位の調整依頼等）
- ・通信手段が限定された中での情報収集方法を事前に把握しておくことの必要性
- ・情報共有が必要な相手先の整理と、連絡経路の確認・設定の必要性
- ・インターネット等が使えない場合の他事業者との情報連絡手段や情報開示手段検討の必要性
- ・情報共有先の通信手段が使えない場合の物理的対応も含めた代替手段検討の必要性

●サービスへの影響に関する気づき
- ・現場業務機会（安全点検、保守、代行サービス遂行など）への影響把握の必要性

4. 演習において得られた主な気づき（2）

演習において得られた主な気づき（情報セキュリティインシデント）

●インシデント対応に関する気づき
- ・情報セキュリティインシデント発生時のサーバ切り離し等、影響の局所化を図ることの有効性
- ・複合障害による混乱状態における、情報セキュリティインシデント対応への備えの必要性
- ・社内関連部署、パートナー企業（ITベンダ等）、ISP、通信事業者との障害対応策検討・立案の必要性
  （原因の切り分け、攻撃先の特定、遮断措置、攻撃パケットのフィルタリング依頼や解除タイミングなど）
- ・契約する通信事業者やCDN事業者、ISPなどのサポート内容の事前確認の重要性
- ・インシデントの収束を見据えた、対応体制レベル変更の判断基準など、組織内ポリシー策定の重要性
- ・監視、連絡体制の強化や早期解決に向けた取り組みに関する、政府、関係機関、分野間における情報共有の重要性
- ・標的型攻撃に関する具体的情報の有効性
- ・BCPに重要システム障害時の対応の記載を含めることの重要性

●風評・デマへの対応に関する気づき
- ・「風評・デマ」など、判別困難なリスクに対する備えについての検討の必要性
- ・対応判断基準の設定が困難な風評・デマ発生時の事実確認や対応判断のための平時からの体制構築の重要性

●情報共有・情報開示に関する気づき
- ・DDoS攻撃への対応時のISPや通信事業者との連絡先の事前確認、連絡手段確保の有効性
- ・情報セキュリティインシデント発生時の複数の情報共有方法の整理の必要性
- ・情報連絡や情報開示の際のテンプレートや報告先の事前整理の必要性
- ・セプターカウンシル、JPCERT/CC、IPA以外の情報収集先や情報収集方法の事前検討の必要性

4. 演習において得られた主な気づき（3）

演習において得られた主な気づき（共通）

●情報共有・情報開示に関する気づき

・他の重要インフラ分野に確認すべきポイントを事前に抑えておく必要性
・障害発生時の他の重要インフラ分野からの問合せを想定した回答を準備する必要性
・障害発生時の情報開示のための自治体やマスコミなどの他分野を活用することの有効性
・連絡がない場合にも能動的な確認を行うことや影響がない場合も積極的に情報連絡・開示を行うことの必要性
・障害状況・復旧状況を正確に把握するための連絡ルートを関係者間で確立しておく必要性
・入手情報と発信状況の把握・整理と、社内部門間での密な情報共有の必要性
・以前の提供情報との差分となる情報を整理し、情報の受け手を意識した続報の発信を行うことの重要性
・演習で用いた情報共有ツールの実環境においての活用の検討

●組織内の対応や方針に関する気づき

・イレギュラーを常に準備して考えておくことの必要性
・入手情報を追い越し、事態の流れの一歩先を予測し、アクションプランを準備しておくことの重要性
・業界内の他社の対応を認識し、自社の対応検討に活用することの有効性
・重要インフラ防護の実効性を高めるための、NISCの役割や所管省庁の連携のありかたについて検討の必要性

5. 演習の総括

検証課題毎の評価	
(1)複合障害発生から復旧までの対応	・電力（計画停電を含む）、通信の複合障害への復旧フェーズにおける対応手順等について実践的な内容において、概ね検証することができた。
(2)複合障害時の緊急対応体制の構築と社内外への連絡手段	・重要インフラに関する網羅的な障害状況の把握手段として、実施細目による情報共有が有効であることを検証できた。 ・障害規模や復旧見込みの把握、優先復旧の調整や計画停電の除外要請において、障害発生した各分野との情報共有が有効であることを検証できた。
(3)情報セキュリティインシデントへの対応	・情報セキュリティインシデントに関する情報収集や対応手順等について、実践的な内容で概ね検証することができた。
(4)情報セキュリティインシデントへの対応体制の構築と社内外への連絡手段	・情報セキュリティインシデントの状況把握のために、関係機関等との積極的な情報共有がなされた。また、通信事業者に対して、事業者からインシデントへの対応依頼が行われた。 ・実施細目やセプターカウンシルを通じた標的型メールに関する情報共有体制において、官民、事業者等・セプター間での情報共有が有効であることを検証できた。
(5) BCP等の発動・解除方法	・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。 ・BCP等において、情報セキュリティインシデントを想定することの重要性が認識された。
(6)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。また、情報開示のための自治体やマスコミ等、他分野活用の重要性が認識された。

演習運営面での評価

・サブシナリオ策定に1分野4事業者（首都圏以外の事業者を含む）が参加し、分野内の事業者間連携や個々の対応等についての相互理解を深めることができた。
・演習当日の意見交換会に加え、作業報告メモやアンケート結果、有識者からの助言を踏まえた後日の意見交換会を開催することで、意見交換の活性化と更なる気づきの共有を図ることができた。
・演習の成果展開を目的とした、事業者等向けの演習成果説明会を3セプターで開催し、演習参加者の拡充や演習成果の普及を実現した。

演習全般を通して得られた成果

実践的な演習を通じて、各重要インフラ事業者等における、複合障害復旧時及び複合障害に便乗した情報セキュリティインシデント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。本演習の継続により、より深い課題を検証し、段階的にレベルアップすることが期待できる。

※演習において得られた具体的な気づきについては、P4-6を参照

6. 課題と対応の方向性

2012年度演習の課題	今後の演習の方向性
より深い課題の検証	●情報共有の実効性を高める検証課題やシナリオの設定 ・環境変化を踏まえた、事業者の関心の高いテーマ及び検証課題の設定 ・各分野に特化したサブシナリオ、状況付与の検討 ・障害状況の推移予測に基づく対応の試行錯誤が必要となる演習シナリオの策定
更なる気づきの創出	●気づきを促す演習実施方法の検討と情報共有の活性化 ・第三者からの助言方法の改善 （モニタリング方法の改善、事業者等からの助言者の設定　等） ・演習中に気づきを促す状況付与の検討、体制整備 ・実践に近い演習環境や使いやすいツールの整備 ・演習中のベストプラクティスの共有 ・障害発生時における他分野の対応や要望等の共有
成果の普及・展開	●成果展開の充実 ・演習成果の各分野への事業者等全体（首都圏以外の事業者も含む）への普及 ・自職場参加も活用した各分野の参加者（首都圏以外の事業者も含む）の拡充 ・演習参加経験のない人でも、演習の実態が容易に理解できる資料の作成