資料3

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

2022年度分野横断的演習について

内閣サイバーセキュリティセンター
重要インフラグループ
2023年３月22日

Copyright(c) National center of Incident readiness and Strategy for Cybersecurity

2022年度分野横断的演習について（１／２）

１．目的

- 分野横断的演習は、重要インフラ行動計画 において「障害対応体制の有効性検証」に位置付けられるものであり、 **①関係主体の組織全体の障害対応体制が有効に機能しているかどうかを確認し、改善につなげていくこと**、さらに **②重要インフラ行動計画の他施策に資すること**を目的として実施するものである。

（注） 重要インフラ行動計画は、サイバーセキュリティ基本法及びサイバーセキュリティ戦略（閣議決定）に基づき、重要インフラ防護に係る基本的な枠組みとして、政府と重要インフラ事業者等との共通の行動計画を定めたものである。重要インフラ行動計画においては、任務保証の考え方を踏まえ、重要インフラ事業者等は自らの責任においてサイバーセキュリティ対策を実施するとともに、継続的な改善に取り組むこととされ、政府は、必要な支援を行うこととされている。

２．演習の形態・日時

- 机上演習 **集合会場と自職場等（テレワーク環境を含む）のハイブリッド形式**
- 2022年12月９日（金）13:00～17:00

３．参加者

- 参加者全体：5,719名（754組織）
- 重要インフラ事業者［情報通信、金融、電力等の14分野］：4,990名（525組織）
- 重要インフラ所管省庁、サイバーセキュリティ関係機関 等

４．演習の概要

- 重要インフラサービス障害発生時における一連の対応について、参加事業者自身が成すべき対応についてしっかりと事前に整理し**必要な改善を行ったうえで演習当日に臨み**、限られた時間及び変化する状況下で、**準備したものが有効に機能するかを検証**する。
- 政府は、演習を通じて得た知見・課題を参考資料として重要インフラ行動計画の他施策に提供する。
- 演習参加事業者等は以下の取り組みを通じて継続的な改善を行う。

＜事前準備＞ 自組織における課題・リスクの状況を洗い出し、改善を行った上で演習当日に参加する。
＜演習当日＞ 演習の中で自組織の規定・マニュアル・BCP/IT-BCP等が機能するかどうかを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、課題の改善に取り組む。

- 演習から得られた重要インフラ防護に関する知見の普及・展開によって、更なる障害対応体制の強化に資する。

2022年度分野横断的演習について（２／２）

５．演習の実施状況

- **ランサムウェア攻撃(基本事象)、サプライチェーン攻撃及びEmotet(関連事象)**に対する対応について確認するなど**重要インフラ事業者等の障害対応体制に対してその有効性の検証**を行った。

- 重要インフラ行動計画を基に見直した検証項目(ベンチマーク)を用いて、障害対応体制の有効性検証を行った。
  参加者における障害対応体制の有効性に係る現状は以下の通り。

  ✓ 演習シナリオのインシデント発生時の対応について

・ 自組織の判断基準に沿った対応状況	対応できた 91.0%, できなかった 2.0%
・ 適切な責任の権限のもとの対応状況	対応できた 91.7%, できなかった 6.8%
・ IT-BCPに沿って対応できた程度	81.2% ※平均値、アンケートは0-100%の1%刻みで回答
・ IT-BCPからBCPに円滑に移行できた程度	84.9% ※平均値、アンケートは0-100%の1%刻みで回答
・ CSIRTが対応できた程度	83.4% ※平均値、アンケートは0-100%の1%刻みで回答
・ 内規やマニュアル等で対応できた程度	83.8% ※平均値、アンケートは0-100%の1%刻みで回答
・ 情報連携や開示の手順に沿って対応できた程度	84.9% ※平均値、アンケートは0-100%の1%刻みで回答

  ※今年度は**障害対応体制の有効性に係る現状の見える化**を行った。
  ※次年度以降は、これら値の推移を見ることで**障害対応体制の有効性に係る推移の把握**を図る。

- 参加者が洗い出した課題について、主なものは以下の通り。
  これら課題や演習を通じて得た知見を基に**障害対応体制の強化に係る施策(分野横断的演習含む)の改善**を図る。
  - ✓ インシデント発生時の手順について、**より詳細・より具体的な行動マニュアル**が必要と感じた。
  - ✓ **経営層の責任範囲・指揮系統・報告手段等**について、より明確化が必要と感じた。
  - ✓ **指揮者不在時の権限移譲ルール**が必要と感じた。
  - ✓ **緊急時の対応に係る演習**の必要性を改めて感じた。
  - ✓ **サプライチェーンに対して**連絡する旨は計画に記載していたが**実際に連絡する場面の想定**が不十分であった。
  - ✓ **マスコミやステークホルダーへの情報開示の基準・タイミング**について、より明確化が必要と感じた。