資料４

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

分野横断的演習について（2019年度）

令和元年7月

内閣官房　内閣サイバーセキュリティセンター
(NISC)

２０１９年度分野横断的演習概要

NISC

目的

- 第4次行動計画に基づく重要システム障害時の情報連絡・情報提供の手順や情報連絡様式の周知徹底、迅速かつ的確な情報伝達の確認
- 2020年東京大会期間中のシナリオに基づき、通常とは違う連絡体制及び連絡頻度におけるNISCをはじめとした政府内連携の確認
- 上記の体制や障害対応に係る手順等について、演習から知り得た知見を施策へ反映

日時

- 2019年11月8日（金）　午前　・機器等の習熟・試験送信（30分程度）
  ・演習（1時間程度）
  午後　・演習（3時間程度）

演習形態/規模

- 原則自職場環境で参加
- 参加者：NISC、内閣官房副長官補（事態対処・危機管理担当）付、所管省庁、重要インフラ事業者（一部の重要サービス事業者(※)を含む）、JPCERT/CC 、IPA　等

  ※2020年東京大会 の開催・運営に重要なサービスを提供している事業者
- 昨年度は　事業者数約3,000名（約400組織）が参加

演習設計方針

- 第４次行動計画に基づく情報連絡を実施し、情報の連絡・提供には、「情報連絡様式」「情報提供様式」の利用を想定
- 演習時計はオリンピック期間中とする
  - -重要サービス事業者の場合は、対処調整センター情報共有システムを使用した情報連絡を実施
  - -2020年東京大会期間中における政府内の情報共有体制の確認
- 参加者の情報連絡における正確性やスピード等測定の実施を検討

（３）東京大会を支える重要サービス事業者である重要インフラ事業者から見たサイバーセキュリティ協議会に加入するメリット

※「情報インシデント状態」：ここでは、サイバー攻撃の存在を検知・認知できた場合における情報システムの被害の確認の調査等を目的とする対応を行っている状態をいう。
※「サービスレベル低下状態」：ここでは、平常時（情報システムによるサービスが安全かつ持続的に提供されている状態）よりサービスレベルが低下し、サービスの継続等を目的とするコンティエンジェンシープラン等に基づく対応を行っている状態をいう。なお、情報システムの被害を確認する前の段階（そもそも攻撃の存在を検知・認知していないケースを含む。）で既に対外的なサービス障害等が生じて外形的に事象が公知となっているような場合（上記「例２」）においては、事実上、情報インシデント状態での対応が完了する前にサービスレベル低下状態への対応が（並走して）始まることとなる。
※「CISTA」：経済産業省予算事業「CISTA・検体分析機能の実用性調査及び開発」事業で運用する、情報共有・検体解析ポータルシステムをいう。
※「行動計画に基づく情報連絡」：ここでは、重フラ行動計画「2.1 情報連絡を行う場合」の対象となる情報のうち、事業者における事案発生の疑いの段階での事案の連絡、相談を気兼ねなく安心して行うことができる情報共有体制における取扱いが適すると考えられる情報（例：事業者等が検知した情報で非公知のもの、特定分野間に限定されるもの、機微性が高いもの、詳細な内容のものなどをいう。）を除いたものの情報連絡をいう。
※協議会が重要インフラ以外の主体から得られた情報等に基づき重要インフラ分野においても早期対処が必要と判断した場合には、提供者の同意を得た上で行動計画側等に提供することがあり得る。これに対し、行動計画側等から協議会側に早期対処の情報連絡を行う必要が生じるケースは、現実的にほぼ想定されない。
※図中「①行動計画」と「②ＣＳ対処調整センター」に関し、東京大会を支える重要サービス事業者である重要インフラ事業者については、①②それぞれに情報連絡を行うことも可能であるが、事業者側における業務負担の軽減を図る観点から、いずれか一方のみにご連絡いただくことも可能とする。いずれか一方のみにご連絡いただいた場合には、ＮＩＳＣ側の処理で、その提供された情報を他方にも共有することとする。この場合において、事業者がどちらに情報連絡を行うべきかの判断の目安として、東京大会の期間中及びその直前期（現時点では来年５月ごろ以降を想定）は②に対し連絡を行い、それ以外の期間は①に対し連絡を行うものとする。

平成 31 年 1 月 17 日
内閣サイバーセキュリティセンター

2020 年オリパラ東京大会に向けた分野横断的演習のあり方について

1　今後の方向性

分野横断的演習については、重要インフラ事業者における事業継続計画や官民・分野横断的な情報共有体制に関する実効性の検証及び課題の抽出を行うことにより、障害対応体制の強化を図ることを目的として、平成 18 年度から全国規模で実施しているところである。

ここで、2020 オリパラ東京大会まで 2 年を切り、2020 オリパラ東京大会までの分野横断的演習の開催は来年度を残すのみとなった状況を踏まえ、2020 オリパラ東京大会までに万全の準備をした上で、同大会を迎えるために、分野横断的演習の機会を 2020 オリパラ東京大会に向けて最大限に活用することとする。

2　分野横断的演習をめぐる現状と今後の課題

①　現状の分野横断的演習は、初めて参加する事業者や練度が低い事業者にも配慮したベースシナリオとしており、複数回参加している事業者や高練度者に向けては、各参加者が作成するサブシナリオにおいて追加の状況付与を加えることで、より高度なシナリオとすることも可能としているが、その結果、参加者毎個別のシナリオとなっている。

しかしながら、2020 オリパラ東京大会に向けた対応を一層万全なものとするためには、全ての参加者が共通シナリオに基づく演習を行うことが必要と思われる。

②　現状の分野横断的演習においては、時間的制約もあり、情報連絡及び情報提供の演習が十分には行えていない。また、事案発生時の情報連絡を行う段階の演習がメインとなっており、事案対処内容を情報共有する段階の演習は不十分となっている。

③　過去には、自然災害発生時の分野横断的な情報共有をベースシナリオに組み込んだことがある一方、近年は、サイバー攻撃への対処演習となっている中で、分野横断的に一堂に会してはいるものの、全体として分野横断的な障害対応を行う演習には必ずしもなっていなかったところである。

3　来年度の分野横断的演習のあり方について

以上を踏まえ、来年度の分野横断的演習においては、自職場からの参加の推奨等により演習未経験者の新規参加を促し、全国の重要インフラ事業者の取組の裾野拡大を図るとともに、重要インフラ関係のオリパラ重要サービス事業者が東京オリパラ大会開催時に想定されるより困難な脅威にも適切に対応できる状態に達することを目指す。また、その際には、政府関係機関の対処方についても合わせて確認する。

具体的には、以下の方向で、今後、関係者と調整を行う。

① 来年度の演習においては、演習時計は共通のものとするとともに、演習時間の拡大を図る。

② 第一部は従来どおり全国の重要インフラ事業者等を念頭に置いたシナリオの下、演習を実施する。

③ 第二部は、現実離れしないことに留意しつつ、システム障害により他分野に影響を与える重要インフラサービス障害が発生するといったより困難な共通の内容のシナリオの下、重要インフラ関係のオリパラ重要サービス事業者を主な対象として、事案対処内容（ＮＩＳＣからの情報提供を踏まえた方針決定等）の情報共有を含めた分野横断的な障害対応を行う内容の演習を実施する。（ただし、オリパラ重要サービス事業者以外も排除はしないこととする。）

④ サイバーセキュリティ対処調整センターの情報共有システムも使用する。

⑤ 他の東京オリパラ大会関係のサイバー演習との連携を図る。

2018年度分野横断的演習

NISC

1．目的
　重要インフラ事業者における事業継続計画や官民・分野横断的な情報共有体制に関する検証及び課題の抽出を行うことにより、障害対応体制の強化を図ることを目的とする。

2．日時
平成30年12月13日（木）

3．参加者（過去最大の3077名が参加）
・重要インフラ事業者（電力、情報通信、金融など14分野）
・重要インフラ所管省庁
・情報セキュリティ関係機関　等

4．その他
・分野横断的演習は、2006年度より実施し、本年度は13回目の実施。
・東京、大阪、福岡の会場参加のほか、事業者の自職場からも参加

櫻田大臣による御挨拶

今年度の演習模様

分野横断的演習の参加者数の推移

実施イメージ

■ 重要インフラ事業者等は、状況付与に対し、事業継続計画等に基づき以下の行動を実施。

- ✓ 状況整理、所管省庁への情報連絡
- ✓ 対応方針検討
- ✓ 関係機関、他事業者等との情報共有　等

従来の分野横断的演習と来年度の分野横断的演習の比較イメージ