資料２

【機密性2情報】

東京オリンピック・パラリンピック競技大会等の大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組の今後の活用方策に関する有識者会議
第２回会合

事務局説明資料

各取組を推進する中で得られた成果と今後の課題等

2021年３月

内閣官房　内閣サイバーセキュリティセンター

1　継続に向けて検討する各取組事項（整理）

2　各取組を推進する中で得られた成果と今後の課題等

【リスクマネジメントの促進】

(1)　リスクアセスメント
(2)　横断的リスク評価
(3)　スポーツ関係団体に対する勉強会

【対処態勢の整備】

(4)　対処支援調整
(5)　サイバー攻撃への対処能力の向上
(6)　予防・検知に関する情報の発信・共有
(7)　情報共有プラットフォーム（JISP）の提供

1　継続に向けて検討する各取組事項（整理）

		取組の実施手順・ノウハウ	システム、ツール	人材	対象組織との関係構築
リスクマネジメントの促進	リスクアセスメント	○　関係組織において実施するリスクアセスメントのガイドライン等 ○　NISCによるフィードバックレポートの作成	—	【NISC】 ○　国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上 【重要サービス事業者等】 ○　リスクアセスメント等に従事する職員が能力向上	○　重要サービス事業者等 約300組織
	横断的リスク評価	○　NISCが実施するリスクアセスメントの手順等（リスクシナリオ検証、チェックリスト検証） ○　NISCによるフィードバックレポートの作成	—	【NISC】 ○　国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上	【リスクシナリオ検証】 ○　選定した重要サービス事業者等 ○　大会組織委員会 【チェックリスト検証】 ○　競技会場等
	スポーツ関係団体に対する勉強会	○　勉強会、演習、自己学習のコンテンツ ○　セキュリティ関係情報の発信・共有 ○　webサイトに対する簡易チェック	—	【NISC】 ○　国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上 【スポーツ関係団体】 ○　セキュリティ対策等に従事する職員が能力向上	○　東京大会に関係するスポーツ関係団体等
対処態勢の整備	対処支援調整	○　関係組織からの支援要請、相談への対応手順等(運用要領、運用手順書等) ○　関係組織向け説明会のコンテンツ	（○　JISP（そうだんの窓口）） （○　JIRA（センター内インシデント管理））	【NISC】 ○　国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上	○　重要サービス事業者等、大会関係組織、情報セキュリティ関係機関、セプター、スポーツ関係団体、関係省庁等 約360組織
	サイバー攻撃への対処能力の向上	○　演習説明会、演習のコンテンツ、結果レポート ○　意見交換会のコンテンツ、結果レポート	（○　JISP（演習環境）） （○　オンライン会議ツール）	【NISC】 ○　国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上 【重要サービス事業者等】 ○　事案対処等に従事する職員が能力向上	
	予防・検知に関する情報の発信・共有	○　脅威情報の収集・発信・共有に係る対応手順等（運用手順書等） ○　観測情報の管理・発信・共有に係る対応手順等（運用手順書等）	（○　JISP（情報提供(一般・プロ)、観測情報提供、インディケータ情報(STIX/TAXII)等））	【NISC】 ○　国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上	
	情報共有プラットフォーム（JISP）の提供	○　システムの利用・運用に係る手順等（利用手順・運用手順書等） ○　体制参加・システムの利用に係る文書(申込書・規約等)	○　JISP（情報共有のプラットフォーム） ○　JIRA（センター内インシデント管理） ○　その他（Web会議ツール、通訳機器等） ※　以上全て、NISCにおいて整備・運用（2023年度以降は更新等の必要あり）	【NISC】 ○　国家公務員（他省庁等からの出向者）、民間事業者からの派遣職員が能力向上	
参考　関係省庁の取組（抜粋）	金融業界横断的なサイバーセキュリティ演習（Delta Wall）（金融庁）	○　演習のコンテンツ ○　金融分野におけるサイバーセキュリティ強化に向けた取組方針（H30.10） ○　金融分野のサイバーセキュリティレポート（R2.6）	—	【金融庁】 ○　担当職員が能力向上 【金融関係事業者】 ○　事案対処等の判断を行う経営層が能力向上 ○　事案対処等に従事する職員が能力向上	○　金融関係事業者　約110社 （令和2年度）
	東京大会に向けた実践的サイバー演習（サイバーコロッセオ）（総務省）	○　実機を使った演習：演習シナリオ（事前学習資料・当日資料） ○　座学による講習：講習用資料	○　仮想のネットワーク環境を構築可能な大規模計算機環境 ○　演習環境を自動構築する演習システム	【大会組織委員会・関連組織】 ○　情報システムやセキュリティ等に携わる職員が能力向上	○　大会組織委員会・関連組織

2 （１）リスクマネジメントの促進（リスクアセスメント）

取組の概要等

○ サイバー攻撃等による東京2020大会の準備・運営への影響の未然防止や軽減等のため、大会を支える周辺サービスを提供する事業者等によるリスクマネジメントの強化を通じ、想定されるサイバーセキュリティ上のリスクへの対策を促進。

【対象】東京2020大会会場周辺（１都１道８県）の事業者等（23分野）及び会場（約300組織）
【実績】第１回(2016年10-12月)、第２回(2017年8-10月)、第３回(2018年6-8月)、第４回(2019年2-4月)、第５回(2019年9-12月)、第６回(2020年11-1月)
- 資料の提供：ガイドライン（実施手順書）、分野別の事業・重要サービス・経営資源の例、リスク源の例、リスク/演習シナリオ 等
- 説明会の開催：実施手順の説明等、10都道県で53回開催。約2000名が参加
- 情報交換会の開催： リスクアセスメントの体験学習等、5都道県で13回開催。約450名が参加
- フィードバックレポートの作成：実施結果をNISCが分析し各事業者へフィードバック（第3回より実施）

取組の成果、大会後に活用するに当たっての課題等

【取組の主な成果】

○ 重要インフラ事業者等のみならず、大会を支える周辺サービスを提供する事業者等を対象に統一的にリスクアセスメント実施を促し、関係組織における対策を促進することで、サイバー攻撃等による東京大会の準備・運営への影響の未然防止や軽減等を推進

○ 事業者等によるリスクアセスメント結果に対して個別にフィードバックレポートを回答することによって、取組の実効性を確保

【大会後に取組を継続的に推進するに当たっての課題等】

○ イベント（大阪万博等）時のみならず、平時から取組を促進する場合の対象領域の整理
- 大会後にリスクアセスメントの対象とする地域、事業者等の範囲の整理
- 継続して平時においても取り組む際のリスクアセスメントの観点（想定すべき脅威、達成すべき対策の水準）の整理
- 事業者等の分野、重要性、規模、能力等に応じて異なる評価方法の検討　等

○ 各事業の所管省庁等における既存の取組との役割の整理

○ 各事業者、分野が自らのリスクを気づくことができる仕組みの検討

○ リスクの低減等の効果を確認、評価するに当たっての仕組み、考え方の検討（どの範囲でどのように効果を確認・評価するか等）

○ 取組のレベルを維持、向上させる上で必要となる、取組を促進する側の支援力の向上（担当職員の育成）　等

2 （2）リスクマネジメントの促進（横断的リスク評価）

取組の概要等

○ 重要サービス事業者等において想定されるサイバーセキュリティリスクに基づき、サイバーセキュリティ対策の実施状況をNISCが検証。

【対象・実績】
- リスクシナリオに基づく検証：選定した重要サービス事業者等、大会組織委員会等を対象に検証（2018-2020年度）
- チェックリストに基づく検証：会場等（仮設や情報資産を持たない会場を除く）を対象に、書面及び訪問による検証（2019-2020年度）
- 技術的対策の検証：選定した会場を対象にペネトレーションテストを実施

取組の成果、大会後に活用するに当たっての課題等

【取組の主な成果】

○ 大会の成功にとって重要な機能が継続して提供されることを確認するとともに、不備があった場合は、重要サービス事業者等へフィードバックすることにより、当該重要な機能が継続して提供されることの確からしさを向上

【大会後に取組を継続的に推進するに当たっての課題等】

○ 事業者等のリスクについて、国が直接的に確認、分析する必要があるケース、対象領域の整理
- 継続して取り組む際の横断的リスク評価の観点（想定すべき脅威、達成すべき対策の水準）の整理　等

○ イベント（大阪万博等）の成功に関して重要な役割を担う組織等に協力いただくに当たっての実施方法、メリット等の整理
- インテリジェンス情報を活用した想定すべき脅威及びそれに基づくリスクシナリオの提示　等

○ 各事業の所管省庁等における既存の取組との役割の整理

○ リスクの低減等の効果を確認、評価した結果の活用方策の検討（所管省庁を含む政府内での情報共有等）

○ 取組のレベルを維持、向上させる上で必要となる、取組を促進する側の支援力の向上（担当職員の育成）　等

2 （３）リスクマネジメントの促進（スポーツ関係団体に対する勉強会）

取組の概要等

○　リオ2016大会でスポーツ関連団体がサイバー攻撃の被害にあったことを受け、NISCとスポーツ庁が事務局となり勉強会を開催。

【対象】JOC、JPC、日本スポーツ協会の加盟団体やその他希望する競技団体
【実績】
- 勉強会（演習含む）の開催：2017年から17回開催
- 自己学習用コンテンツの提供：2020年9～12月に15回提供
- CTI情報の発信：2018年２月から東京2020大会まで隔週で配信
- 簡易Ｗｅｂチェックの実施：希望する団体に対して2019年から実施

取組の成果、大会後に活用するに当たっての課題等

【取組の主な成果】

○　サイバーセキュリティ対策のノウハウ等が蓄積されていない団体等を対象に、対策に必要な知識等を様々な方法で網羅的に提示し、サイバーセキュリティ対策の水準を底上げ

○　業界内の横の関係構築が強固でない団体等との間で、有事対応に必要不可欠な相互の関係性を構築

【大会後に取組を継続的に推進するに当たっての課題等】

○　イベント（大阪万博等）時のみならず、平時から取組を推進する場合の対象領域の整理
- 支援の対象とする事業分野等の範囲、優先順位づけ等の整理　等

○　対象の事業分野等に対して、セキュリティの基本的な知識・能力を一から養成するに当たってのパッケージ・手法の検討

○　持続可能な自助に必要な支援を行う上での取組の内容、期間、取組の引き継ぎ先（業界ISAC等）等の整理

○　取組のレベルを維持、向上させる上で必要となる、取組を促進する側の支援力の向上（担当職員の育成）　等

2 （4）対処態勢の整備（対処支援調整）

取組の概要等

○　インシデント（のおそれ含む。）が発生したときに、関係組織間で情報を共有しつつ、サイバーセキュリティ対処調整センターが中心となり、被害組織からの相談・支援要請に対して必要な助言・支援を実施。

【対象】
・ サイバーセキュリティ対処体制参加組織（大会組織委員会、重要サービス事業者等、会場管理者、関係府省庁、情報セキュリティ機関、治安機関等）約360組織

【実績】
・約40件の対応（「そうだんの窓口」トピック数。ー2020年12月末。）

取組の成果、大会後に活用するに当たっての課題等

【取組の主な成果】

○　大会関係組織間でワンストップでの情報共有の仕組みを構築し、情報の報告ルート等を合理化

○　参加組織からの要請・相談に対して助言及び支援調整を実施する体制を構築し、事案の未然防止、被害拡大抑止等を推進

【大会後に取組を継続的に推進するに当たっての課題等】

○　イベント（大阪万博等）時のみならず、平時から取組を推進する場合の対象領域の整理

・　大会後に取組の対象とする地域、事業者等の範囲の整理（ICT等の活用が著しく進む重要事業分野（製造、webビジネス、情報ビジネス）、各事業者等のシステム整備、サイバーセキュリティ対策を担うベンダー等）　等

○　イベント（大阪万博等）時のみならず、平時から取組を推進する場合の実施内容の検討

・　迅速な対処支援を行う上で対処調整センターに求められる初動調査等の対処能力の検討　　等

○　他の省庁、関係機関等における既存の取組との役割の整理

・　発生事象（システム障害、災害等）ごとに異なる報告、対応ルートがあることを踏まえつつ、 報告ルート等の整理

○　取組のレベルを維持、向上させる上で必要となる、知見やスキルの維持継続、取組を担当する職員の育成　等

2（5）対処態勢の整備（サイバー攻撃への対処能力の向上）

取組の概要等

○　体制確立の確認及び運用手順の確立のため、信頼関係づくり及び手順習熟を目的としたサイバーインシデント対応演習を実施。また、大会に向けての運用上の課題解決を進めるため、関係組織間で課題や演習の状況等を話し合う意見交換会を実施。

【対象】
- サイバーセキュリティ対処体制参加組織　約360組織

【実績】
- 計４回の演習、計２回の意見交換会を実施（ー2021年２月末）
- 大会本番までに演習、意見交換会を各１回実施予定

取組の成果、大会後に活用するに当たっての課題等

【取組の主な成果】

○　演習・訓練により、インシデント発生時における参加事業者等内部、関係組織間の情報共有等を通じての事案対処能力を強化

○　業種を問わず他組織の対策に係る体制、課題、好事例等を把握できる意見交換会により、各組織における実現可能な対策を推進

【大会後に取組を継続的に推進するに当たっての課題等】

○　情報連携にとどまらない、より実践的な対処能力向上を目的とした演習・訓練の内容の検討（底上げが急がれる能力等）

○　参加事業者等によりサイバーセキュリティ対策に係る目的・レベルが異なる中、効果的な訓練・演習の手法等の整理

○　参加組織が負うコストを意識した上でのモチベーションの維持向上のための取組、共通の目的(課題)、成果の共有

○　他の省庁、関係機関等における既存の取組との役割の整理

○　取組のレベルを維持、向上させる上で必要となる、知見やスキルの維持継続、取組を担当する職員の育成　等

2（6）対処態勢の整備（予防・検知に関する情報の発信・共有）

取組の概要等

○　オープンソースを元に作成したニュース情報、協力ベンダー等からの情報により、体制参加組織に最新の脅威情報を提供。また、セキュリティ関係機関の協力等を得て、体制参加組織を標的としたサイバー攻撃の発生、又はその予兆に係る情報を観測等し、該当情報を当該組織に提供。

【対象】
- サイバーセキュリティ対処体制参加組織　約360組織

【実績】
- 脅威情報の提供　約2300件（ー2020年12月末）
- 観測情報の提供　約100件（ー2020年12月末）、ダークweb等から収集した脅威情報の提供　約50件（ー2020年12月末）

取組の成果、大会後に活用するに当たっての課題等

【取組の主な成果】

○　様々な組織等から発信されるサイバー脅威情報等を整理した上でワンストップで提供（利用者のレベルに合わせ、同一情報を異なるレベル（プロ・一般）で情報を提供）することで事業者等が効果的、効率的に情報を入手

○　情報セキュリティ関係機関、体制参加事業者等の協力により、各組織での独自入手が困難な脅威情報を提供

【大会後に取組を継続的に推進するに当たっての課題等】

○　他の省庁、関係機関等における既存の取組との役割の整理

○　東京大会後に国として発信・共有する情報の対象範囲の明確化

○　NISCが入手した脅威情報の二次利用(官民連携)に係る方針の整理

○　取組のレベルを維持、向上させる上で必要となる、知見やスキルの維持継続、情報を発信する側の担当職員の育成　等

2 （7）対処態勢の整備（情報共有プラットフォーム（JISP）の提供）

取組の概要等

○　脅威情報、インシデント情報等をワンストップで共有でき、参加組織からのインシデント報告に対して、要請に応じて助言及び対処支援調整を効率的に実施するため、情報共有プラットフォームを（JISP）運用。

【対象】
・　サイバーセキュリティ対処体制参加組織　約360組織
【実績】
・　累積のログイン数　約14.5万、参照数 約34.1万、投稿数　約0.6万、コメント数 約2.0万
（月平均 ログイン数　6,885、参照数 16,241、投稿数　270、コメント数 943）　（ー2020年12月末）

取組の成果、大会後に活用するに当たっての課題等

【取組の主な成果】

○　利便性・信頼性が高い基盤として、対処調整センターとの情報連絡のほか、個別コミュニティ内における連絡ツールとしても機能

○　機械連携（STIX/TAXII）の仕組みの活用により、組織委員会における効果的、効率的なサイバーセキュリティ対策を推進

【取組のレガシー化に当たっての課題等】

○　JISPによる情報共有の位置づけの整理（既存の情報共有スキームで使用しているシステムとの関係整理 等）

○　機械連携（STIX/TAXII等）による国内のインジケータ情報連携の方向性の検討