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

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

最終報告概要

令和３年12月７日

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（最終報告）

これまでの取組・成果の整理

NISCが中心となって大会に向けて推進した取組の概要等を以下のとおり示す。

対処態勢の整備

取組	概要	取組による成果
① インシデント等に対する対処調整	関係組織との間で対処体制を構築し、インシデント発生時等には、サイバーセキュリティ対処調整センターが被害組織における対処への支援を調整するなどして、関係組織が連携してインシデント等に対応。	関係組織が一丸となってインシデントに対応する枠組みを整備し、インシデントの未然防止、被害拡大防止等に向けた対応を推進。ワンストップでの情報共有が可能となり、報告ルート等を合理化。
② 予防・検知に関する情報の発信・共有	大会のサイバーセキュリティに係る脅威情報、関係組織を標的としたサイバー攻撃に係る観測情報等を対処体制参加組織に共有。	様々な脅威情報等をワンストップで共有することで、各組織における情報の把握・収集を効率化。
③ サイバー攻撃への対処能力の向上	インシデント発生時の対処手順の習熟を目的とした演習を開催。対処体制の運用上の課題を改善、解決等するため、関係組織間で意見交換会を開催。	演習により対処体制全体の事案対処能力を強化し、意見交換会により各組織のセキュリティ対策を推進。
④ 情報共有プラットフォームの提供	関係組織間でインシデント情報等をワンストップで共有し、被害組織からの支援要請、当該要請を受けたサイバーセキュリティ対処調整センターからの対処調整等を効率的に実施するための情報共有プラットフォーム（JISP）を整備し、関係組織に提供。 さらに、インディケータ情報を機械連携の仕組みを活用して共有。	利便性、信頼性が高いプラットフォームを用いることで関係組織間における情報共有の効率性、安全性が向上。

リスクマネジメントの促進

取組	概要	取組による成果
① リスクアセスメント	NISCが作成した手順書に沿って重要サービス事業者等のリスクアセスメントを促進（個別の実施結果をNISCが分析し、フィードバックを実施）。	サイバー攻撃等による影響の未然防止、軽減等を推進。NISCによるフィードバックで取組の実効性を確保。
② 横断的リスク評価	特に大会への影響度が大きい重要サービス事業者等、競技会場の一部を対象に、複数のリスクシナリオ等を活用してセキュリティ対策の実施状況をNISCが検証。 さらに、競技会場の制御システムに対して、実際の攻撃手法を用いた攻撃に耐えられるかという観点で、その技術的対策の実施状況を検証。	大会の成功に不可欠な機能が継続して提供されることの確からしさを向上。
③ スポーツ関連団体に対する勉強会	スポーツ関連団体等を対象に、セキュリティに係る基本的な知識やインシデント発生時等の対処手法を習得することを目的とした勉強会、演習等を実施。	スポーツ関連団体のセキュリティ対策に係る水準を底上げ。各団体及びNISC間、業界内における相互の信頼関係を構築。

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（最終報告）

大会期間中におけるNISCの活動結果等

対処態勢の概要

○　関係組織との情報共有、相談や報告の受付、インシデント対処等に24時間対応可能な体制を構築・運用
○　個別のインシデント対応を担当するチームを複数構成し、関係組織間でリエゾンの派遣、受け入れを実施

活動結果

大会運営に影響を与えるようなサイバー攻撃は確認されなかった。

大会期間中の主な対応

○　インシデント等に対する対処調整
　インシデント等を認知した場合、被害組織等との間で、その影響範囲、復旧に向けた対応方針等について情報共有を行い、必要に応じて助言を実施。
　インシデント情報等をセキュリティ調整センターとの間で適切に情報共有するとともに、体制参加組織に対してインシデントの発生状況等に関する情報を発信。

○　予防・検知に関する情報の発信・共有
　情報セキュリティ関係機関の協力等によって把握した脅威情報について、体制参加組織に注意喚起を実施。
　情報セキュリティ関係機関の協力等によって把握した観測情報について、対象組織に個別に連絡し、対処・対策の実施を働きかけ。

大会期間中の主なトピック（大会運営への影響なし）

- サイバー攻撃に関するSNS上の書き込み等
- 米国コンテンツ配信サービス企業における障害
- 不正な動画配信サイト

サイト接続後に案内される不正なアカウント登録画面

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（最終報告）

これまでの取組等を踏まえた大会後の活用方策　大会後のNISCにおける取組の活用方策を以下のとおり示す。

大会に向けた取組を今後活用するに当たっての基本的な考え方

【構成員からの意見・指摘】

○　**持続的なサイバーセキュリティ対策としての活用**

大会に向けて整備した仕組み、推進した取組のうち有効なものは、大規模国際イベントのみに限定することなく、平時の持続的な取組として継承していくべきである。持続的な取組と大規模国際イベント向けの取組で同水準の対策を求めるのではなく、その必要性等に応じてメリハリをつけて推進すべき。

○　**様々な機関等が推進する取組、整備する連絡系統等を考慮した上での合理的・効果的な対策の推進**

NISCの役割に照らして、社会全体を俯瞰して十分に対応が進められていない領域へのサポート、東京大会に向けて取り組んだ窓口のワンストップ化を推進するなど、我が国のサイバーセキュリティの底上げに向けた対策を推進すべき。

○　**公益性の観点に立った取組の推進**

事業者等によって様々なサービスが既に提供されていることにかんがみ、公益性の観点から真に政府が取り組む必要がある内容になっているか十分に留意するべきである。

○　**サイバーセキュリティ対処調整センター等としての能力の維持**

業務を通じて職員が得たノウハウや、インシデント対処等に係る経験が組織的にしっかりと継承できるようにすることが重要である。

○　**大会後の大規模国際イベントにおける取組の活用**

この度の大会における経験を、2025年日本国際博覧会を始めとした大規模国際イベントにおけるサイバーセキュリティ対策にしっかりと引き継ぎ、生かしていく必要がある。

構成員からの意見・指摘を踏まえた今後の活用方策

大会に向けて推進した取組から得た経験やノウハウを十分に活用しながら、我が国のサイバーセキュリティを底上げできる仕組み作り及び取組を推進し、社会経済を支えるサービスを安全安心に利用できるようにする必要がある。
上記の各構成員からの意見・指摘に沿って、国として取り組むべき施策を力強く推進することが重要。

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（最終報告）

これまでの取組等を踏まえた大会後の活用方策　大会後のNISCにおける取組の活用方策を以下のとおり示す。

各取組に関する大会後の活用方策等

対処態勢の整備

取組	構成員からの主な意見・指摘	大会後の活用方策
①　インシデント等に対する対処調整	対処に係る支援内容は、インシデントの早期把握、被害拡大防止等の観点からの初動対応のように公益性の観点から取り組む必要がある内容となっているか留意する必要がある。 個別のインシデント等への対応のみに止まらず、インシデント対処等により得た情報を元に、分析結果から明らかになった攻撃者等に関する情報の発信、指令サーバのテイクダウンを始めとする対処に関する企画・支援を行うことにも期待したい。	被害組織単独での対処が困難なインシデント対処を迅速・的確に実施できるよう、相談や支援要請をワンストップで受け付ける窓口を設け、関係組織と緊密に連携してインシデント対処への初動対応に係る支援等を実施する。 また、インシデント対処等により得た情報を元に、積極的なサイバーセキュリティ対策を推進する。
②　予防・検知に関する情報の発信・共有	二次被害を防止するために、実被害案件に係る原因や技術的対策の情報を共有するべきである。 政府で把握等した有害なインディケータ情報等を、各事業者等が活用しやすい形式で積極的に共有するべきである。	各組織におけるインシデント被害の未然防止やインシデント対処に資するよう、様々な機関、事業者等から発信される脅威情報等のワンストップでの共有、サイバー攻撃等に係る観測情報等の提供を実施する。
③　サイバー攻撃への対処能力の向上	演習・訓練の際は、被害が急増している又はそのおそれがある事例等最新の情勢を捉えるなどして、民間事業者が既に提供する講習等のサービスとの役割を整理した上で取り組むべきである。	各組織においてインシデントへの自律的な対処が可能となるような知識・技能を習得するとともに、関係組織間の連携を強化するため、JISPを利用した情報連絡訓練、インシデントの対処能力強化に向けた実践的な演習、各組織間の意見交換会を開催する。
④　情報共有プラットフォームの提供	JISPを信頼性の高い基盤の一つとして提供することで、サイバーセキュリティ対策に係るコミュニティの立ち上げ等の活性化、コミュニティ内の連携の円滑化が図られると期待する。 インディケータ情報の共有に当たっては、機械連携の仕組み等を用いて、効率的に情報共有を行うべきである。	関係組織間における安全かつ効率的な情報共有が可能となるよう、JISPを整備・運用し、関係組織にその環境を提供するとともに、ISAC、ISAO等のコミュニティの立ち上げ、活動の活性化等に貢献する。

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（最終報告）

これまでの取組等を踏まえた大会後の活用方策　大会後のNISCにおける取組の活用方策を以下のとおり示す。

各取組に関する大会後の活用方策等

リスクマネジメントの促進

取組	構成員からの主な意見・指摘	大会後の活用方策
①　リスクアセスメント	自組織に適した方法・内容でリスクアセスメントを自ら効果的・効率的に実施できるような仕組み・ツールを設けるなど、NISCと事業者両者に負担が生じない取組を講じていくことも重要である。 個々の事業者のサービス、情報資産等に応じた複数のアプローチによる評価手法、事業者の規模や対策のレベルに応じた手法、内容を検討するべきである。	各組織のサイバーセキュリティ上のリスクを軽減できるよう、個々の組織のサービス等に応じた評価手法を準備するとともに、その結果に対するフィードバックを実施（ツールの開発等も推進）する。 その際、各組織でどのようにリスクアセスメントの機会を活用するべきであるかなどの観点についてガイダンスを示すことが有用である。
②　横断的リスク評価	自主的なセキュリティ対策には限界があり、今後の大規模国際イベントでも政府自ら直接的にサイバーセキュリティ対策の実施状況を検証するべきである。 システム上の脆さ等の課題が確認されることを想定し、当該課題に対処できる期間を考慮したスケジュールで取組を実施するべきである。	大規模国際イベント時等において特に重要な役割を担う事業者等のサービスの継続性を確保できるよう、最新の攻撃手法等を踏まえた攻撃シナリオ等を用いて、特に重要な役割を担う事業者等におけるサイバーセキュリティ対策状況を検証する。
③　スポーツ関連団体に対する勉強会	業界内等における情報共有、連携強化は二次被害等を防ぐ上で重要である。 コミュニティ内のセキュリティ対策のレベルの底上げ等を図る上で有効であり、コミュニティの立ち上げ等の活性化を図る支援策として期待される。	サイバーセキュリティ対策に係る能力の底上げが急務となる組織において基本的な知識・技能を習得できるよう、事業所管省庁等と連携して、事業分野全体でITやセキュリティに関する専門知識、業務経験が乏しい分野等に対して必要な支援を実施する。

大規模国際イベントにおけるサイバーセキュリティ対策

取組	構成員からの主な意見・指摘	今後の活用に向けた方策
大規模国際イベントにおけるサイバーセキュリティ対策	大規模国際イベント時は、平時には業務上の関係がない組織と連携する機会が生じるため、この度の大会における対処体制と同様の体制を構築し、それぞれの取組を連携させていくべきである。 大規模国際イベントの運営等に提供する事業者等のサービスの重要度等に照らし、メリハリをつけた対策を講じるべきである。	国が主体的な役割を担うイベントにおけるサイバーセキュリティを確保できるよう、大会におけるサイバーセキュリティの確保に向けた取組に倣って、関係組織との間で「対処態勢の整備」、「リスクマネジメントの促進」に係る取組を推進する。

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（最終報告）

これまでの取組等を踏まえた大会後の活用方策　大会後のNISCにおける取組の活用方策を以下のとおり示す。

各取組に関する大会後の活用方策等

取組を推進するに当たって対象とする領域

課題認識等

サイバーセキュリティの確保に向けて、**各組織における自律的な取組のほか、多様な組織の緊密連携が不可欠**

・　各組織で講ずるべきサイバーセキュリティ対策に求められる水準が高度化、複雑化
→　政府から各組織に対して、**自律的なサイバーセキュリティ対策（インシデント対処を含む。）を講じることができるよう必要な支援を積極的に実施**

・　デジタル化の更なる進展に向けて、各組織におけるサイバーセキュリティ対策はより一層重要となるものの、個々の自主的な取組のみでの対応には限界
→　ISAC、ISAO等のコミュニティにおける各組織間の強固な連携等のように、**相互の支援・連携が強化されるよう政府において必要な支援を実施**

対象とする領域等

【これまで対象としてきた領域】

東京大会の関係組織間で対処体制を構築し、「対処態勢の整備」及び「リスクマネジメントの促進」に係る取組を推進

大会後に取組の対象とする領域

【大会後に対象とする領域】

持続的なサイバーセキュリティ対策

社会全体のサイバーセキュリティの確保に向け、重点的に対策を講じてきた重要インフラ事業者等に加え、**社会経済を支えるサービスを提供する組織を対象**に、

・　事業所管省庁等と連携し、対処体制に参加する事業分野、事業者等の範囲を調整し、必要な対策を推進（各組織で自立的な取組が可能となるような支援）
・　また、事業所管省庁等と連携して、優先度の高まっている分野におけるコミュニティの構築・運営への支援を推進（各組織間の支援連携が機能するような支援）

※　NISCが利用者側の目線に立って、**取組の必要性、有益性等について対象となる各組織等からの理解を得ながら取組を推進することが重要**

大規模国際イベントにおけるサイバーセキュリティ対策

大規模国際イベントの関係組織間で、対処体制を構築し、必要な対策を推進