資料１

【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３回会合

事務局資料

中間整理に向けた確認・討議事項等

2021年４月

内閣官房　内閣サイバーセキュリティセンター

1　中間整理のイメージ（これまでの意見・議論の整理）

2　東京大会後における活用方策に関する基本的な考え方に係る確認・討議

3　各取組の東京大会後における活用方策に関する具体的な考え方に係る確認・討議事項

1　中間整理のイメージ（これまでの意見・議論の整理）

1　背景・取組を推進してきた経緯等

情勢認識（過去大会におけるサイバー攻撃の発生状況等）、東京大会に向けたサイバーセキュリティ対策を推進してきた経緯、取組の概要等を紹介。

2　東京大会後における活用方策に関する基本的な考え方

- 大規模国際イベントのみに対象を限定することなく取組を継続（取組が不十分な範囲等を分析・整理）。
- 事案の性質、事業分野等によって窓口が多岐にわたるものについて、窓口機能のワンストップ化等により合理化するとともに、政府全体の取組等を俯瞰して手が届いていない領域への対応を推進。
- 公益性の観点から取組を推進。
- 職員の経験やノウハウを組織的に継承。
- 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対応。

中間整理の取りまとめに向けて確認・討議
（各論、全体像に係る討議等を実施）

3　各取組の東京大会後における活用方策に関する具体的な考え方

(1) 対処態勢の整備

(1-1) 対処調整に係る機能について、どのようなサービスを提供するか整理が必要。
(1-2) 脅威情報の提供・共有に当たり、政府で把握した確度の高いインディケータ情報を提供することが有用。
(1-3) ISAC、ISAOにおけるプラットフォームとしてJISPの活用が有用。
(1-4) 事案対処の場面において組織がどのように動くかという観点からの能力の底上げが必要。
(1-5) 東京大会向けの取組の全国展開に当たり、中小企業を含めたすべての事業者に範囲を広げることは現実的でなく、対象を限定。

(2) リスクマネジメントの促進

(2-1) リスクアセスメントのコンテンツ等の不断の見直し等を進め、取組を改良していくことが重要。
(2-2) 参加事業者等が自ら問題意識を持って取り組むことが重要。
(2-3) 参加事業者においてリスクアセスメントを有効に活用した事例等を整理・周知することが重要。
(2-4) 自己学習用コンテンツ等の成果物等を広く公開。
(2-5) スポーツ関係団体に対する勉強会に関するノウハウ等を、ISACの構築支援等に活用。
(2-6) 東京大会向けの取組を全国展開するに当たり、中小企業を含めたすべての事業者に範囲を広げることは現実的でなく、対象を限定。

(3) 大規模国際イベントへの対応

体制等を継続した上で以後の大規模国際イベントに対応。

4　今後の検討の進め方

東京大会開催期間中の対応を含めたセキュリティ対策の総括
体制参加事業者等からの意見聴取結果等を踏まえ、今後の活用方策について議論をより一層深掘り

2　東京大会後における活用方策に関する基本的な考え方に係る確認・討議

これまでの意見・議論

- 大規模国際イベントのみに対象を限定することなく取組を継続。
- 事案の性質、事業分野等によって窓口が多岐にわたるものについて、窓口機能のワンストップ化等により合理化するとともに、政府全体の取組等を俯瞰して手が届いていない領域への対応を推進
- 公益性の観点から取組を推進。
- 職員の経験やノウハウを組織的に継承。
- 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対応。

基本的な方針

- （経済社会を支える組織とそれを支えるベンダー）国内組織が、必要最低限のサイバーセキュリティを確保できること、最近のサイバー攻撃事情（APT激化やSPC攻撃）に対応できることを目指し、東京大会向けに構築した対処体制を継続的なものとし、重大なインシデント発生時等に関係組織が一丸となって対処可能となるようにする
- デジタル化の機会と影響があらゆる主体に例外なく及び、セキュリティインシデントの与える影響の範囲、深刻度が増大する中、セキュリティ対策の強化が急務となる領域等に対して、東京大会に向けて取り組んだリスクマネジメントを始めとした効果的なセキュリティ対策の支援を継承する
- ただし、公益性の高い取組に重点化するなど、民間における取組との切り分けを意識しつつ、メリハリをつけて取組を進める
- 大規模国際イベントにおけるサイバーセキュリティ上のリスクの高まりを踏まえ、東京大会に向けた取組で得られた知見、ノウハウを活用して大規模国際イベントのセキュリティ対策を促進する

（１-1）対処調整に係る機能について、どのようなサービスを提供するか整理が必要

対処調整について

【想定される取組】
○ 報告相談支援等のインシデント窓口（関係組織とのワンストップでの情報共有等を目指す）
○ インシデント対処のための支援調整関係組織との連携
○ テイクダウンを始めとした対処手法の企画・調整等

【御議論をいただきたい事項】
○ 対処調整に係るサービスの範囲について
・ 各組織でインシデントが発生した際の支援として、政府がどのような事案に対し、どのような形で支援をし、どこまで関与・フォローしていくべきか、その考え方についてご議論をいただきたい。
・ セキュリティベンダー等によるインシデントの対処、発生原因の分析等の有償サービスが提供されているが、政府が対処調整を実施するに当たっての民間企業との役割分担とその考え方についてご議論をいただきたい。

○ 事業所管省庁、治安機関、情報セキュリティ関係機関等との連携について
・ インシデントに対して、役割に応じて各組織が被害の実態把握・収束・拡大防止、復旧、再発防止等の被害の二次被害防止等の対処等を一丸となって連携して行うことになるが、その中で、対処調整センターが担うべき役割についてご議論をいただきたい。

（１-2）脅威情報の提供・共有に当たり、政府で把握した確度の高いインディケータ情報を提供することが有用

予防・検知に関する情報の発信・共有について

【想定される取組】
○ JISPを用いたワンストップでの脅威情報の提供（講ずべき対策まで含めたもの）
○ 参加組織に関する観測情報の提供（DDoS被害、情報漏洩、未対策の脆弱性等に関する情報等）
○ IoCの機械連携
○ サイバーセキュリティ対処調整センターにおいて把握したインシデント情報の提供（サニタイズした情報）

【御議論をいただきたい事項】
○ 脅威情報の提供・共有に係るサービスの範囲について
・ セキュリティベンダー等によるサイバーセキュリティに関する脅威情報等を提供するサービスがあるが、政府が脅威情報及び観測情報を提供するに当たっての民間企業との役割分担とその考え方についてご議論をいただきたい。
・ 民間事業者以外にも、情報セキュリティ関係機関等の様々な情報提供組織がある中、NISCその他政府機関からの提供が期待される情報についてご議論をいただきたい。

（１-3） ISAC、ISAOにおけるプラットフォームとしてJISPの活用が有用

JISPの提供について

【想定される取組】
○ 情報共有体制全体のワンストップのためのプラットフォーム（インシデントレスポンス、情報共有）
○ ISAC、ISAO等のコミュニティの構築と活性化のためのプラットフォーム

【御議論をいただきたい事項】
○ コミュニティにおけるJISPの活用について
・ JISPは東京大会におけるサイバーセキュリティ確保のための体制だけでなく、地方自治体や金融機関のコミュニティにおいても情報共有ツールとしても活用されているが、これまでの活用方法に加え、新たなコミュニティの構築・活性化に資する、コミュニティ内及びコミュニティ間における情報共有ツールとしての活用方法とその考え方についてご議論いただきたい。

（１-4）事案対処の場面において組織がどのように動くかという観点からの能力の底上げが必要

サイバー攻撃への対処能力の向上について

【想定される取組】
○ 最低限のインシデントレスポンス、政府（NISC）を始めとした外部組織と連携を行えるようになるための訓練
○ 流行のサイバー攻撃に関する高度な演習訓練
○ 業界横断的な事業者間の交流の場の提供
○ 高度化複雑化するサイバー攻撃に関する情報交換の場の提供

【御議論をいただきたい事項】
○ 政府（NISC）で実施すべき演習・訓練の内容について
・ 東京大会に向けてインシデント発生時の組織内における対処方針の検討手順、政府等への報告、支援要請の手順等を確認する演習・訓練を実施してきたところであるが、情報の活用やインシデント対処能力を向上する演習・訓練等、大会後の情報共有体制において開催が期待される内容とその考え方についてご議論をいただきたい。

○ 官民及び事業者間の交流の場提供について
・ 官民及び事業者間の交流の場の提供について、業界横断的な事業者間の交流、サイバー攻撃に関する情報交換等、大会後の情報共有体制において開催が期待される内容とその考え方についてご議論をいただきたい。

（１-5）東京大会向けの取組の全国展開に当たり、中小企業を含めたすべての事業者に範囲を広げることは現実的でなく、対象を限定

対処態勢の整備の対象とする領域の考え方について

【想定される領域】
○　経済社会を支える事業者等
○　事業者等の属する業界団体
○　事業者の情報システム等を支えるベンダー企業

【御議論をいただきたい事項】
○　取組の対象とする領域の考え方について
・　現時点で、中小企業を含めた全国、全分野の事業者等を対象に対処態勢（※）を整備することは現実的ではないところ、対象とする領域を設定するに当たっての考え方についてご議論いただきたい。
（※）　対処調整、予防・検知に関する情報の発信・共有、JISPの提供、サイバー攻撃への対処能力の向上等

（2-1） リスクアセスメントのコンテンツ等の不断の見直し等を進め、取組を改良していくことが重要
（2-2） 参加事業者等が自ら問題意識を持って取り組むことが重要
（2-3） 参加事業者においてリスクアセスメントを有効に活用した事例等を整理・周知することが重要
（2-4） 自己学習用コンテンツ等の成果物等を広く公開

リスクアセスメントについて

【想定される取組】
○ 対象事業者等による自主的なリスクアセスメントの支援（リスクアセスメントの手順等を提供・公表）
○ リスクアセスメントに係る自己確認自動化ツール等の提供・公表
○ リスクアセスメント結果に対するフィードバック

【御議論をいただきたい事項】
○ リスクアセスメントで評価する範囲等について
・ 東京大会の運営に支障を来すようなインシデントが生じないようにすることを念頭に、事業継続性の観点を重視したリスクアセスメントの取組を推進してきたところ、東京大会後にも実施する場合にどのような観点でリスクアセスメントを行うべきか、どのように事業者が実施した評価の正確性を確認するべきかについてご議論をいただきたい。
・ 同一の手法、内容で全ての対象事業者へのリスクアセスメントを実施することは実効的でないと考えられるところ、リスクアセスメント対象（p11（３(2）)で討議を実施予定）のセキュリティ対策状況等のレベルに応じて取組を実施することについて、そのやり方や考え方についてご議論をいただきたい。

○ 持続可能なリスクアセスメントのための支援内容等について
・ 特定の国際イベント等のみを対象としない持続可能なリスクアセスメントを事業者に実施いただくために、既存の組織・枠組みとどのように協力するのか、どのような支援を、どの程度の期間実施するのかなどについてご議論をいただきたい。

（2-5）スポーツ関係団体に対する勉強会に関するノウハウ等を、ISAO等の構築支援等に活用

コミュニティの構築支援について（スポーツ関係団体に対する勉強会等）

【想定される取組】
○ 支援対象コミュニティに対する勉強会の開催
○ セキュリティ情報ニュースの発信・共有
○ 簡易ウェブサイトチェック
○ 机上演習
○ JISP

【御議論をいただきたい事項】
○ コミュニティ構築・醸成の支援方法等について
・ 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事業者が多い分野等を対象にした、コミュニティ構築・醸成への支援の必要性・方法・期間等についてご議論いただきたい。

（2-6）東京大会向けの取組の全国展開に当たり、中小企業を含めたすべての事業者に範囲を広げることは現実的でなく、対象を限定

リスクマネジメントの促進の対象とする領域の考え方について

【想定される領域】
○ 経済社会を支える事業者等
○ 事業者等の属する業界団体
○ 事業者の情報システム等を支えるベンダー企業

【御議論をいただきたい事項】
○ 取組の対象とする領域の考え方について
・ 現時点で、中小企業を含めた全国、全分野の事業者等を対象にリスクアセスメントを実施することは現実的ではないところ、対象とする領域を設定するに当たっての考え方についてご議論いただきたい。

○ ISAC、ISAO等のコミュニティ構築、業界横断的な取組に向けた支援について
・ 事業分野等ごとにデジタル活用が進んでいる、又は今後の活用が見込まれ、セキュリティ対策やその意識の向上が課題となる分野に対し、ISAC、ISAO等のコミュニティ構築、業界横断的な取組を支援することについて、その方法や考え方についてご議論いただきたい。

体制等を継続した上で以後の大規模国際イベントに対応。

東京大会後の大規模国際イベント等に向けた対応について

【想定される取組】
○ イベントの関係事業者等を対象とした対処態勢の整備（対処調整、サイバー攻撃への対処能力の向上、予防・検知に関する情報の発信・共有、JISPの提供等）
○ イベントの関係事業者等を対象としたリスクマネジメントの促進（リスクアセスメント、横断的リスク評価、関係事業者等を対象とした勉強会等）

【御議論をいただきたい事項】
○ 取組の必要性や内容について
・ 大阪万博等の大規模国際イベントが開催される際に、サイバーセキュリティの確保に向けて政府が関与する必要性、関与する場合の取組内容等についてご議論いただきたい。