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

中間整理

令和３年７月 16 日

目次

1　はじめに

1.1 取組を進めてきた経緯・背景

2020 年東京オリンピック・パラリンピック競技大会（以下「大会」という。）は国際的にも最高度の注目を集めて開催される行事となり、大会の機会を狙ったサイバー攻撃等の発生が懸念されている。

大会の準備、運営を担う大会組織委員会、競技会場を始めとする大会関係施設、大会の運営に不可欠な重要サービス等に対するサイバー攻撃が行われた場合、円滑な大会運営に支障を来す懸念があるほか、大会を支える重要なサービスが停止、制御不能となる深刻な影響が生じることになれば、アスリートや観客等の安全が脅かされる事態に発展するおそれもあることから、そのサイバーセキュリティ対策は重要な課題となっている。

現に、2012 年ロンドン大会や 2016 年リオ大会では大会関係のウェブページ等に対して様々なサイバー攻撃がなされたほか、2018 年平昌大会では開会式運営への妨害を企図したサイバー攻撃が行われたと報道されている。このようにオリンピック・パラリンピック競技大会を標的としたサイバー攻撃は現実の脅威となっており、大会を標的としたサイバー攻撃にも十分な警戒が必要となった。

こうした情勢の中、政府においては、サイバーセキュリティに係る諸施策の目標及び実施方針を示す「サイバーセキュリティ戦略」（平成 30 年 7 月 27 日閣議決定）において、大会運営に影響を与える可能性のある重要サービス事業者等におけるサイバーセキュリティ上のリスク評価及びそれにより明確となる各種リスクへの対策を促進するとともに、大会関係組織間でサイバーセキュリティに係る脅威情報の共有と事案発生時に大会関係組織が皆で力を合わせて対応するために国が調整役となるための組織であるサイバーセキュリティ対処調整センター（以下「対処調整センター」という。）の構築を推進するとの方針を示した。

また、大会に係るサイバーセキュリティ対策の円滑な準備に資するよう、関係府省庁の所管する事務を調整するため、セキュリティ幹事会（平成 27 年 7 月 24 日 2020 年東京オリンピック・パラリンピック競技大会関係府省庁連絡会議議長決定）等を設置し、セキュリティ対策に係る基本的な考え方、対策の方向性等を示す「2020 年東京オリンピック競技大会・東京パラリンピック競技大会に向けたセキュリティ基本戦略」の決定、改訂等を行ってきた。同戦略においても、サイバーセキュリティ対策の強化を重要課題の一つとして挙げ、サイバーセキュリティ上のリスク評価及びそれにより明確となったリスクへの対策を促進するとともに、サイバーセキュリティに係る脅威・インシデント情報（以下「脅威情報等」という。）の共有等を担う中核的組織

としての対処調整センターを構築し、その運用改善を図るなどして、事案発生の未然防止及び発生時における迅速かつ的確な検知・対処のために必要となる体制の構築・強化を図るとの方針を示した。加えて、同幹事会において、対処調整センターを構築等し、同センターの運用は、内閣サイバーセキュリティセンターが東京オリンピック競技大会・東京パラリンピック競技大会推進本部事務局と緊密に連携して行うこととされた。

こうした政府の方針等に基づき、内閣サイバーセキュリティセンターでは、大会におけるサイバーセキュリティの確保に万全を期すべく、関係組織との緊密な連携の下、大会の円滑な運営に不可欠なサービスを提供する事業者等（以下「重要サービス事業者等」という。）に対してリスク評価等の支援を行う「リスクマネジメントの促進」に係る取組、大会組織委員会や重要サービス事業者等との間で的確な情報共有、インシデント発生時の対処調整等を行う「対処態勢の整備」に係る取組を推進しているところである。

1.2 大会後の活用方策に向けた検討

オリンピック憲章では、オリンピック競技大会の有益な遺産（レガシー）について、開催都市のみならず、開催国として引き継ぐことが期待され、1964年東京大会においては、新幹線、首都高速道路、ごみのない美しい町並みなど、現在にも残る数々のレガシーが生み出された。1964年東京大会のレガシーとして今日に残っているものは、大会前からの官民を挙げた不断の準備・努力によって成し遂げられた成果が大会において高く評価され、大会後に継続されて現在も残っているものである。この度の大会においても、大会の開催に向けて推進された様々な取組、整備された施設、開催によって得られた文化的な恩恵等が、大会後も長期にわたって継承・享受されていくことが期待されている。

この点、大会におけるサイバーセキュリティの確保に向けて整備された仕組み、その運用経験及びノウハウは、大会を契機に関係組織間で協力して作り上げられた重要な成果であり、有用な取組等は大会後においても継承されていくことが求められる。この方針については、サイバーセキュリティ戦略においても、「2020年東京大会後も各種施策は適用範囲を拡大して引き続き推進し、整備した仕組み、その運用経験及びノウハウは、レガシーとして、以降の我が国の持続的なサイバーセキュリティの強化のために活用していく」と記述されている。

他方、その活用に当たっては、大会に向けた取組等を単純に継続するだけでは適当ではなく、これまでの取組の成果等を正確に評価しつつ、デジタル化の進展に伴い変容するサイバーセキュリティを取り巻く現下の課題を踏

まえ、その活用方策についてしっかりと検討する必要がある。

また、近年、Emotet のような強力な感染力を持つマルウェアによるばらまき型攻撃、国家等の関与が疑われる特定の組織を標的とする高度な攻撃、テレワークの普及等の環境変化をタイムリーに捉えた攻撃等が猛威を奮っているところであるが、これらの脅威は大会後も途絶えることなく存在することも念頭に置いておく必要がある。こうした背景にある中、大会向けの各取組を、大会終了をもって一度止めてしまうと、これまで醸成してきた関係組織間における協力・連携体制等が損なわれることになり、取組を再開する際に関係組織との信頼関係を一から構築し直さなければならず、結果的にサイバーセキュリティ上の脅威への対応に遅れを来すおそれがある。そのため、大会に向けた取組の今後の活用方策等に関する検討に際しては、大会の完遂を待たずして進めていく必要がある。

こうした点を踏まえ、内閣サイバーセキュリティセンターでは、大会に向けた取組の成果等を整理するとともに、これらの取組を今後の我が国のサイバーセキュリティ対策の強化に活用するための方策、課題等について外部有識者の視点も踏まえて検討、整理するため、「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」を令和３年１月に設置した。

本有識者会議においては、これまでに内閣サイバーセキュリティセンターが推進してきた各取組の内容、その成果、大会後の活用方策、課題等について討議を行ってきたところ、この度、その結果を中間整理として取りまとめることとした。

２　これまでの取組・成果

本有識者会議において討議を行うに当たり、これまでの内閣サイバーセキュリティセンターにおける取組の推進状況、その成果を確認した。これらを整理した結果を以下のとおり示す。

2.1　対処態勢の整備

内閣サイバーセキュリティセンターでは、平成 31 年４月に内閣官房に設置された対処調整センターを運用し、以下の取組を推進している。

①　インシデント等に対する対処調整

【取組の概要】

対処調整センターでは、大会の安全・円滑な準備及び運営並びに継続性

を確保するため、大会の運営を支えるサービスを提供する関係機関等[1]との間における相互の信頼関係を築き、サイバーセキュリティに係る脅威・インシデントに対し各組織が自律的に未然対処及び事案対処ができるよう必要となる体制（以下「対処体制」という。）を構築・運用している。現在、対処体制に参加する組織（以下「対処体制参加組織」という。）は約350組織となっている。

インシデント対処に当たっては、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役割を担い、これにより関係組織が連携してインシデントに対応できるようになっている。インシデント対処に係る主な流れは以下のとおりである。

（対処調整の流れ）

1　大会の運営に影響を及ぼし得るインシデント等が発生した場合又は発生するおそれがある場合等に、被害組織は対処調整センターが整備した情報共有プラットフォーム（Japan cyber-security Information Sharing Platform の略。以下「JISP」という。）を通じて、同センターに対して対処に係る支援要請又は相談を行うことができる。

2　要請等を受けた対処調整センターは、被害組織に対して助言を行うとともに、必要に応じて情報セキュリティ関係機関[2]と連携して対処に係る支援の調整を行う。

3　情報セキュリティ関係機関は、対処調整センターとの調整結果を踏まえて、被害組織におけるインシデント対処を迅速かつ積極的に支援する。

4　1から3の流れについては、被害組織が、事業所管省庁、大会組織委員会、治安機関等の関係組織を情報共有先として指定することで、ワンストップでの情報共有が可能となり、関係組織が共通の認識でインシデントに対応することができる。

【取組による成果】

○　インシデント発生時等に被害組織が関係組織に個別に連絡・報告等をしなければならないこれまでの状態から、ワンストップでの情報共有が可能となり、被害組織における情報の報告作業及びその問合せ対応等の合理化を図ることができた。

1　関係府省庁、大会組織委員会（スポンサー含む。）、東京都、競技会場のある地方公共団体（都道県警察を含む。）、重要サービス事業者等、競技会場の管理者、スポーツ関連団体等

2　国立研究開発法人情報通信研究機構、独立行政法人情報処理推進機構、一般社団法人JPCERTコーディネーションセンター及び一般社団法人日本サイバー犯罪対策センター

○　被害組織からの支援要請等に応じて対処調整する枠組みを整備したことで、個別の組織の対処能力に依存していたこれまでの状態から、関係組織が協力してインシデントに対応できるようになり、総合的に対処能力が向上し、被害拡大防止等を推進することができた。
○　支援要請や相談を行うことができる窓口を提供することで、対処体制参加組織における安心感を醸成できた。

②　予防・検知に関する情報の発信・共有

【取組の概要】

対処調整センターでは、オープンソースや国内セキュリティベンダー等から得られた脅威情報等を対処体制参加組織に提供している。脅威情報等の提供に当たっては、対処体制参加組織の知識・技能が多様であることにかんがみて、「一般用」、「プロ用」と内容を書き分け、情報の受け手である対処体制参加組織の知識・技能にあった情報を提供できるように配慮している。

また、情報セキュリティ関係機関において行っている、サイバー攻撃の発生、又は予兆に係る情報の観測等の活動の中で把握された対処体制参加組織に関する情報及びダークウェブ上のサイバー攻撃の呼びかけ活動、漏洩したアカウント情報の売買、公開等の情報（以下「観測情報」という。）を、JISP を通じて対象組織に個別に提供している。

本取組については、運用開始以降、令和３年５月末までの間に約 1,800 件の脅威情報等を提供しているところである。

【取組による成果】

○　様々な組織等から発信される脅威情報等が、JISP においてワンストップで、かつ情報の受け手の知識・技能に応じて書き分けられた内容で提供されることで、対処体制参加組織が効果的、効率的に情報を入手・活用できるようになり、被害の未然防止及び極小化につながった。
○　情報セキュリティ関係機関等の協力により、各組織では独自に収集することが困難な観測情報を得られるようになり、被害の未然防止及び極小化につながった。

③　インシデント等への対処能力の向上

【取組の概要】

対処調整センターでは、対処体制参加組織におけるインシデントの未然防止及びインシデント対処能力の向上を目的とした JISP を用いたサイバ

ーインシデント対応演習（以下「演習」という。）、対処体制参加組織間の相互の信頼関係づくりを目的とした意見交換会を開催してきた。

演習においては、攻撃者グループによるAPT攻撃、テレワークや休日中に確認されたサイバー攻撃、システムへの被害により物理面での被害が生じるサイバー攻撃等、現下のサイバーセキュリティ情勢をタイムリーに捉えたシナリオ等を用いて、大会までの間に計５回の演習を積み重ねてきた（第１回：平成31年10月から11月、第２回：令和２年１月から２月、第３回：令和２年８月、第４回：令和３年１月、第５回令和３年６月に開催。）。

意見交換会においては、対処体制参加組織におけるサイバーセキュリティ上の課題等をグループで討議する意見交換会を、大会までの間に計３回開催した（第１回：令和２年９月、第２回：令和３年２月、第３回：令和３年７月に開催。）。このような場を提供することで、各組織において東京大会に向けての運用上の課題解決に資する気づきが得られるとともに、各組織間の相互の信頼関係づくりが推進された。

【取組による成果】

○　演習の開催により、インシデント発生時等における参加組織の内部、関係組織間の情報連絡等をシミュレーションするとともに、各組織においてセキュリティ上の課題解決に資する気づきを得ることができるようになり、対処体制参加組織のインシデント対処能力を高めることができた。

○　意見交換会の開催では、業種を問わない他組織と交流し、自組織のサイバーセキュリティ対策を改善する上で参考となる他組織の情報（体制、課題、好事例等）が共有されるとともに、対処体制参加組織間の相互の信頼関係が構築され、サイバーセキュリティ対策に係る活動を活性化することができた。

④ 情報共有プラットフォームの提供

【取組の概要】

対処調整センターでは、対処体制参加組織間において、脅威情報等を共有するとともに、インシデントの被害組織からの報告・支援要請に対する助言や対処調整を実施している。これらの活動をワンストップで効率的に実施するため、JISPを整備し、平成31年４月から運用している。

JISP では上記のほか、対処体制参加組織間で、個別にコミュニティを作成し、当該コミュニティ内における情報共有、演習訓練等にも活用できるようになっており、現に特定の業界内、地域内におけるコミュニティが

構築され有効に活用されている。

また、機械連携（STIX/TAXII）の仕組みを活用して、インディケータ[3]情報の共有も行っている。

【取組による成果】

○　JISP は、利便性、信頼性が高いプラットフォームとして、対処調整センター等との連絡に用いられるほか、個別のコミュニティ内における連絡ツールとしても活用され、対処体制参加組織間の連携強化に大きく貢献している。

○　機械連携の仕組みの活用により、当該仕組みを活用する機関において効果的かつ効率的にサイバーセキュリティ対策を強化できることが実証された。

2.2　リスクマネジメントの促進

内閣サイバーセキュリティセンターでは、大会を標的としたサイバー攻撃に係るリスクの低減と最新のリスクへの対応を進めるため、大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象に、以下の取組を推進している。

①　リスクアセスメント

【取組の概要】

内閣サイバーセキュリティセンターでは、サイバーセキュリティ上のリスクの低減と最新のリスクへの対応を目的としてリスクアセスメントの手順書を作成し、約 300 者の重要サービス事業者等を対象にリスクアセスメントの取組を促進した。

リスクアセスメントについては、各重要サービス事業者等におけるサービスが安全かつ継続的に提供されるよう、維持・継続することが必要なサービスの特定、サービス提供の維持等に必要な業務や経営資源に係る要件の分析・評価、サービスの維持等に影響することが想定されるインシデントの結果からのリスク源の分析を行う、いわゆる機能保証の観点に立った取組を推進した。

また、各事業者等におけるリスクアセスメントの取組を単に促すだけでなく、内閣サイバーセキュリティセンターが各事業者等から提出された実施結果を分析し、リスク等の洗い出しが不十分と思われる点、サイバーセキュリティ対策の運用状況の懸念点等について個別にフィードバックを行っている。

---

[3] サイバー攻撃の痕跡を示すもので、攻撃者が使用した不正プログラムのファイル名やハッシュ値、通信先の IP アドレス等の情報のことをいう

リスクアセスメントの取組は、サイバーセキュリティ対策の改善を目的に、その対策の実施状況を確認するため、平成 28 年 10 月から、東京都内の事業者等を対象とした取組を始め、段階的にその対象範囲を拡大し、大会までの間に計６回の取組を実施した。

本取組に関する取組状況は以下のとおりである。

（取組状況）

第１回：平成 28 年 10 月から 12 月、東京都 23 区内の重要サービス事業者等を対象に約 70 組織でリスクアセスメントを実施

第２回：平成 29 年８月から 10 月、東京都、埼玉県、千葉県及び神奈川県内の重要サービス事業者等を対象に約 120 組織でリスクアセスメントを実施

第３回：平成 30 年６月から８月、全競技会場の管理者及び競技会場が所在する都道県の重要サービス事業者等を対象に約 190 組織でリスクアセスメントを実施し、NISC から個別に実施結果に関するフィードバックを実施

第４回：平成 31 年２月から４月、全競技会場の管理者及び競技会場が所在する都道県の重要サービス事業者等を対象に約 270 組織でリスクアセスメントを実施し、NISC から個別に実施結果に関するフィードバックを実施

第５回：令和元年９月から 12 月、全競技会場の管理者及び競技会場が所在する都道県の重要サービス事業者等を対象に約 280 組織でリスクアセスメントを実施し、NISC から個別に実施結果に関するフィードバックを実施

第６回：令和２年 11 月から令和３年１月、全競技会場の管理者及び競技会場が所在する都道県の重要サービス事業者等を対象に約 270 組織でリスクアセスメントを実施し、NISC から個別に実施結果に関するフィードバックを実施

【取組による成果】

○　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、統一的な手法でのリスクアセスメントを促進したことで、サイバー攻撃等による大会の準備・運営への影響の未然防止や軽減等を推進することができた。

○　各重要サービス事業者等によるリスクアセスメント結果を分析し、懸念事項等について個別にフィードバックを行うことで、取組の実効性を確保することができた。

② 横断的リスク評価

【取組の概要】

重要サービス事業者等におけるリスクアセスメントの促進に加えて、特に大会への影響度が大きい重要サービス事業者等、既存の施設を利用する競技会場等を対象に、サイバーセキュリティ対策の実施状況を内閣サイバーセキュリティセンターが検証した。

重要サービス事業者等に対する検証では、大会に関わるリスクが顕在化するリスクシナリオを策定、活用し、その検証を行った。具体的には、検証対象となる個々の事業者等の業務、システム構成等を把握した上で、攻撃者が当該事業者等のどのような経営資源に対してどのような手法で攻撃を実行するか、又は事故・災害がどのような経営資源に対してどのように影響するかについて時系列で整理し、最終的にリスクが顕在化することを想定したシナリオを複数策定し、シナリオごとに検証項目等をブレークダウンし、当該検証項目等に基づいたヒアリング、実地・書面での確認を実施した。また、競技会場等に対する検証では、チェックリストを策定・活用し、確認を行った。具体的には、各競技会場等の業務、情報システム等を把握した上で、その機能を継続的かつ適切に提供されることを確認する上で必要なチェックリストを策定し、当該チェックリストに基づいて書面による検証、現場視察等を行った。

横断的リスク評価の結果については、改善対策案を含め対象事業者等にフィードバックし、大会までの間にその改善状況等を確認するフォローアップを継続して行っている。

更に、競技会場におけるリスクを明確化することを目的として、大会の継続を支える特に重要な競技会場の制御システムに対しては、攻撃者が実際に用いる手法での攻撃に耐えられるかという観点から攻撃シナリオを策定した上で、技術的対策の実施状況を検証し、その対策の改善に向けて必要な助言等を行っている。

これらの取組の実施状況は以下のとおりである。

（取組状況）

リスクシナリオに基づく検証

平成 30 年度：電力、通信、水道、鉄道、放送分野から５者を対象に訪問検証、全重要サービス分野から 19 者を対象に書面検証を実施

令和元年度：鉄道、放送、大会運営分野から３者を対象に訪問検証を実施

令和元年度–令和３年度：検証結果を踏まえたフォローアップを実施

チェックリストに基づく検証

令和元年度：仮設や情報資産を持たない競技会場を除く 30 会場を対象に、書面及び訪問による検証を実施

令和２年度-令和３年度：検証結果を踏まえたフォローアップを実施

技術的対策の検証

令和元年度-令和３年度：７つの競技会場を対象に検証

【取組による成果】

○　大会の成功に不可欠な機能が継続して提供されることを第三者の立場で客観的に確認するとともに、不備があった場合には、フィードバックを行うことで、当該機能が継続して提供されることの確からしさを向上させることができた。

③ スポーツ関連団体に対する勉強会

【取組の概要】

2016 年リオ大会においては、スポーツ関連団体がサイバー攻撃によって重大な被害を受けたことを踏まえ、内閣サイバーセキュリティセンター及びスポーツ庁が協力して、平成 29 年７月から、大会の競技種目となる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、演習を開催した（全 17 回）。勉強会で用いたコンテンツについては、各団体等において理解度を確認するとともに、その内容を振り返ることができるよう、クイズ形式の自己学習用コンテンツとして提供するなど、更なる知識の定着を図っている。

また、JISP で提供される脅威情報等について、スポーツ関連団体のリテラシーを考慮して編集した内容を隔週の頻度（内容の深刻度、緊急度を踏まえてタイムリーに提供する場合もあった）で提供した（計 30 回、令和３年５月末時点。）。

更に、独立行政法人情報処理推進機構の協力を得て、外部からの攻撃を受けやすいスポーツ関連団体のウェブサイトを対象に、サイバー攻撃の被害を受けやすい脆弱な状態となっていないか調査を行い、問題がある場合には修正対応案を提示するなどの取組を行った。

【取組による成果】

○　サイバーセキュリティ対策に係る知見を有する人材、組織的なノウハウの蓄積が十分とは言えないスポーツ関連団体等を対象に、様々な方法で対策を講じる上で必要な知識等を提示し、対策に関する水準の底上げを図ることができた。

○　業界内の横の関係が強固に構築されていない団体等の間で、有事の対応に必要不可欠な相互の信頼関係を構築することができた。

３　英国、米国におけるサイバーセキュリティ対策（調査結果）

内閣サイバーセキュリティセンターでは、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の今後の活用方策等を検討するに当たって、その課題を明確化する目的で、国内外のサイバーセキュリティ対策の推進体制等に係る調査を行った。その中から、サイバーセキュリティ対策における官民連携等を検討する上での参考事例となる、「ロンドン 2012 大会後の英国の施策とその成果」及び「米国のサイバーセキュリティに関する情報共有体制」の概要を以下のとおり示す。

3.1　ロンドン 2012 大会後の英国の施策とその成果

ロンドン 2012 大会後の英国は、当時抱えていた多くの課題を解決するために、大会での経験も踏まえ、政府のサイバーセキュリティ対策に関する機能を国家サイバーセキュリティセンター（以下「NCSC」という。）へ統合し、「国家サイバーセキュリティ戦略 2016-2021」を推進している。この中で、政府が主導する英国内の民間事業者等のサイバーセキュリティを確保する取組として、重要インフラ事業者や公共・民間組織に対しての情報提供、実運用の有償・無償サポートを含む包括的な支援を積極的に実施している。主な取組を以下のとおり示す。

なお、内閣サイバーセキュリティセンターでは、ロンドン 2012 大会で英国が得た教訓、その教訓等を踏まえて推進された NCSC の取組を参考に、「対処態勢の整備」に係る取組を推進している。

① 重要な国家インフラ事業者等のサイバーセキュリティ運用への積極的な支援

NCSC では、サイバーセキュリティ対策に係るサービスの信頼性を確保する取組を推進している。具体的には、アドバイス、サポート、ガイド、脅威インテリジェンスの提供、重要なサービスを提供する組織に対してのセキュリティ運用支援等に係る多様な各種製品・サービス等について、NCSC が独自の基準に基づいた検証・認定を行った上で、公式にこれらのサービス等の有償提供を仲介するなどして、サイバーセキュリティ対策に係る運用面での積極的な支援を実施している。NCSC において検証・認定を受けて提供される製品・サービス数は、現在では 200 件を超えて、ペネトレーションテスト、業務向け製品セキュリティ、セキュリティコンサル、インシデントレスポンス、トレーニング等のサービスが英国内の多くの組織で活用されている。

② 非重要インフラ事業者等におけるサイバーセキュリティの確保に向けた積極的な支援

サイバー攻撃による被害があらゆる領域に拡大し、その影響が深刻化していることを踏まえ、NCSC では、重要インフラ分野のみに止まらず、国全体のサイバーセキュリティ対処能力を高めるため、ログイン管理、フィルタリング、脆弱性チェック、インシデント対処訓練等のサイバー攻撃の被害を防ぐ上で重要な対策サービスを認定ベンダー又は NCSC が自ら広く一般に提供している。

③ Cyber Security Information Sharing Partnership (CiSP)

NCSC では、登録組織向けに、政府や関係組織と安全な環境で連携することができ、また脅威情報の随時取得や組織間での情報交換、相談が可能となるプラットフォームとコミュニティを提供している。このプラットフォームとコミュニティの利用に当たっては、通信手段等で一定の基準を満たした組織等が利用できるようになっており、その利用者数は毎年右肩上がりで拡大し、英国全体のサイバーセキュリティを支えるコミュニティに成長している。

3.2 米国のサイバーセキュリティに関する情報共有体制

米国では、サイバーセキュリティの脅威に関する情報共有、分析等の取組を、各主体の相互協力により推進する活動が活発に行われている。

① Information Sharing and Analysis Center (ISAC)

ISAC は、重要インフラ分野を始めとして同一の業界内の事業者同士で、サイバーセキュリティに関する情報を共有するなどして、サイバー攻撃に対する防御力を高めることを目指して活動する民間組織である。

米国では、現在までに 24 の ISAC が組織されていて、各分野における情報共有等が推進されている。また、各 ISAC は、全米 ISAC 協議会(NCI) を通じて政府と相互に連携・調整を行っている。現在 24 の組織から構成されており、各部門において情報共有と運営を担っている。

我が国でも、ISAC が組織されているが、その組織数は米国よりも少ない。

② Information Sharing and Analysis Organizations (ISAO)

ISAO は 2013 年 2 月の大統領令に基づき国土安全保障省 (DHS) に設置促進が指示されたもので、ISAC と同様にサイバーセキュリティに係る脅威の情報共有と分析を行う組織であるが、ISAC が組織されていない分野や ISAC のメンバーでない民間企業など幅広い分野において情報共有等を行うことを目的としている。ISAC とは異なり、産業分野ごとに関連付けられるものではなく、広く産官学の分野や地域等においてコミュニティが組織

されたものとなっている。

政府は、国土安全保障省サイバーセキュリティ・インフラセキュリティ庁（CISA）の官民連携による情報共有分析組織である国家サイバーセキュリティ通信統合センター（NCCI）を通じて、ISAO と継続的に連携するとともに、包括的な調整を行っている。

4　これまでの取組等を踏まえた大会後の活用方策

本有識者会議では、これまで内閣サイバーセキュリティセンターが推進してきた取組の内容、その成果を踏まえ、今後の活用方策についての課題や期待される取組について討議を行った。その結果を以下のとおり示す。

4.1　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

大会に向けた取組の全体を捉えた基本的な考え方について、構成員から示された意見・指摘は以下のとおりである。

【各構成員からの意見・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、推進した取組は、これまでに関係組織間で相当の期間、コストを費やして準備してきたものであり、我が国のサイバーセキュリティ対策として有効なものは、大会後の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しっかりと継承していくべきである。大会に向けた取組と比較すると、平時の持続的な取組の重要性は理解されづらいものであることから、そのブランディング・プロモーションについても重視していく必要がある。

○　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な運用

取組等の継承に当たっては、内閣サイバーセキュリティセンターがサイバーセキュリティ対策に係る総合調整の事務等を担う観点から、社会全体を俯瞰し、十分に対応が進められていない領域を整理するなどした上で、必要な取組を推進していくべきである。また、大会に向けた取組において、インシデント発生時等の相談・報告の窓口のワンストップ化を目指した工夫が講じられたところであるが、大会終了後においても窓口等が多岐にわたるものは同様にワンストップ化を図るなど、合理的・効果的に取組を推進することが重要である。各府省庁、情報セキュリティ関係機関が、それぞれの役割に応じて様々なサイバーセキュリティ対策に係る取組を推進しているが、内閣サイバーセキュリティセンターにおいては、全体が効果的に運用されるための仕組み作り、取組を推進するべきである。

○　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イバーセキュリティ対策に係るサービスが既に提供されていることにかんがみ、大会に向けた取組を今後活用する際には、公益性の観点から真に政府が取り組む必要がある内容となっているか十分に留意しなくてはならない。

○　対処調整センター等における能力の維持

この度整備した規程、ガイドライン等の成果物は、大会後の取組にも活用できる重要な財産となるが、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も重要なものである。行政機関では、人事異動が定期的に行われているところであるが、職員の人事異動周期への配慮のほか、これまでに蓄積された職員の経験やノウハウが組織的にしっかりと継承される仕組み、工夫を講じ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

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は、今後も重要な課題となり、大会と同様に政府を中心とした対策が求められる。大会に向けた取組を踏まえ、2025 年日本国際博覧会（以下「大阪・関西万博」という。）を始めとした大規模国際イベントにおいてサイバーセキュリティ対策を強化するべきである。

【意見・指摘を踏まえた大会後の活用方策】

社会経済を支えるサービスへの高度な攻撃が急増しており、大会に向けて推進した取組を十分に活用しながら、社会経済を支えるサービスの安全な維持・運用を確保する必要がある。そのため、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である。

4.2　各取組に関する大会後の活用方策等

大会に向けて推進された個別の取組について、大会後にどのような役割が期待されるか、どのような点に留意するべきかなど、今後の活用方策等について討議を行った。各取組に対する構成員からの意見・指摘、これらの意見・指摘を踏まえた大会後の活用方策とその具体例を以下のとおり示す。

4.2.1　対処態勢の整備

①　インシデント等に対する対処調整

【各構成員からの意見・指摘】

○　インシデントの被害を受けた場合、被害組織においては自組織で調査等を行うことになるが、その被害が深刻な場合等には外部の機関等に対して助言や支援を求めたりする場合があるほか、被害状況の公表が不可欠な場合や、治安機関、地方自治体、事業所管省庁等の関係組織への報告が必要な場合がある。個別の場面によって対応が異なるもの

の、サイバーセキュリティ対策に十分な態勢を設けられていない事業者等からすると、このように相談先・報告先として複数の関係組織が存在する中で、どの組織に、どのような連絡を行えばよいかわからなというケースも少なくない。この点、助言や対処調整をワンストップで受け付ける窓口を設けたことは、各組織においてインシデント被害を受けた際の報告等に係る負担を大きく低減したと評価できる。

○　インシデントの被害は特定組織のみでなく、広範囲に渡っていることも考えられることから、早期に政府としてインシデントを認知し、対処することが望まれる。他方、事業者等によっては、どのようなレベルのインシデントで相談、支援の要請を行えばよいかイメージできず、躊躇することがある。大会後も対処調整センターにおける対処調整に係る機能等を継続するのであれば、被害組織から積極的なインシデント被害に係る報告、相談がなされるよう、想定するインシデント等の事例を積極的に示すなどして、報告等を促すことが重要である。

○　被害組織に対する支援内容については、セキュリティ関係事業者において既にインシデントの原因調査、対策の提案等に係るサービスが多数提供されているが、被害組織のニーズに十分に応えられない場合もある。重大な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真に政府が取り組む必要がある内容については、政府がスピード感をもって積極的に支援を実施していくべきである。

○　報告を受けたインシデント等への助言、対処調整を多く実施するようになれば、個々の被害情報等のみでは確認、特定が難しい攻撃者の情報を分析することが可能になる。そのため、対処調整に際しては、個別のインシデントへの対処のみに止まらず、被害情報等を総合的に分析し、指令サーバのテイクダウンを始めとする広義の対処に関する取組を企画、支援できるようになることも期待したい。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「インシデント等に対する対処調整」に係る取組は、各組織における自律的なインシデント対処を原則としつつ、被害組織単独で対応が困難なインシデント対処を迅速、的確に支援することを主たる目的に、内閣サイバーセキュリティセンターにおいて被害組織等からの支援要請、相談、報告等をワンストップで受け付ける窓口を設け、インシデント対処への初動支援等を行うことが望まれる。また、支援要請等によって享受可能なメリットの周知等を通じて事業者等への働きかけを行うとともに、大会に向けた取組と同様に、内閣サイバーセキュリテ

ィセンターが、インシデント対処に係る助言や支援を行うことができる情報セキュリティ関係機関、被害組織の事業所管省庁、治安機関等の関係組織と緊密に連携して対応に当たることが望まれる。さらに、個別のインシデント対処のみならず、指令サーバのテイクダウンを始めとする対処に係る企画、支援を行うなど被害拡大防止に向けた取組についても積極的に進めることが望まれる。想定される具体的な取組事例を以下のとおり示す。

○　インシデントの被害組織等からの報告、相談、支援要請等に係る関係組織間のワンストップでの窓口
○　各組織が自組織内で対処が困難なインシデント対処に係る支援、情報セキュリティ関係機関との対処調整
○　サイバーセキュリティに関する相談等の促進及び相談等への助言
○　不正サイトのテイクダウン等の対処手法に係る企画、調整

② 予防・検知に関する情報の発信・共有

【各構成員からの意見・指摘】

○　脅威情報等の提供に当たっては、推奨される具体的な対策等も含めて提供することが重要であるが、その点、対処調整センターの情報発信等は、対処体制参加組織のリテラシーに合わせて対策等の内容が示されているため有効である。
○　情報セキュリティ関係機関、民間のセキュリティ事業者等においてもサイバーセキュリティ上の脅威情報は様々なものが発信されているが、注意喚起する組織が多いほど脅威の深刻性が高いと判断する材料になる。特に内閣サイバーセキュリティセンターから発信される脅威情報であれば注目度も高まることから、脅威になり得る情報は躊躇することなく積極的に提供するべきである。
○　政府として把握、分析した結果、通信遮断等を行うことが好ましいと判断された有害なインディケータ情報等は、各事業者等で活用しやすい形式に加工して積極的に提供していくべきである。
○　国内におけるサイバー攻撃被害について報道されることがあるが、どのような弱点を突かれて被害が生じたのか、その技術的な原因を把握できるようなケースは多くない。実被害が生じたものこそ、他の事業者等で二次的な被害を受けないようしっかりと対策を講じていく必要がある。そのため、インシデント被害の相談等を扱う中で把握された被害情報等については、可能な範囲で、被害組織及びそのシステム等の機微な情報をサニタイズした上で共有していくべきである。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「予防・検知に関する情報の発信・共有」に係る取組は、インシデント被害の未然防止や各組織におけるインシデント対処を支援することを目的に、高度な情報発信機能が求められる内閣サイバーセキュリティセンターにおいて、様々な機関、事業者等から発信される脅威情報等をワンストップで活用しやすい内容で共有するとともに、情報セキュリティ関係機関等と連携した上で各組織に関する観測情報を個別に提供することが望まれる。また、国内事業者等におけるインシデント被害の原因とその技術的な対策に係る情報、そのサイバー攻撃で実際に用いられたインディケータ情報等を必要に応じてサニタイズした上で提供するなど、更なる被害の拡大防止に向けた積極的な情報共有も望まれる。想定される具体的な取組事例を以下のとおり示す。

○　内閣サイバーセキュリティセンターにおいて収集した脆弱性情報、攻撃予見情報等の脅威情報、国家レベルの攻撃グループの攻撃動向に係る情報、インシデント情報（被害組織が特定できる情報をサニタイズしたもの）等を、各組織のリテラシーが異なることを考慮しつつ、対処方法等を含めた上で、JISP を用いてワンストップで積極的に提供

○　各組織における個別具体の脅威について、情報セキュリティ関係機関等の協力を受けた上で観測された情報を提供

○　内閣サイバーセキュリティセンターにおいて把握・分析した有害なインディケータ情報を機械連携の仕組み等を活用して提供

③ インシデント等への対処能力の向上

【各構成員からの意見・指摘】

○　取組の継続に際しては、対処体制参加組織間の情報連携に止まらず、基本的な対処能力の底上げに向けた実践的な演習・訓練にも取り組んでいくべきである。他方、サイバーセキュリティ対策に係る演習等は民間のセキュリティ企業のサービスを始め多方面で開催されていることから、内閣サイバーセキュリティセンターにおける演習・訓練にあっては、定型化したインシデント対応の手法等を題材にするのではなく、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、民間のセキュリティ企業等が既に提供するサービスとの役割を整理した上で取り組むべきである。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「サイバー攻撃への対処能力の向上」に係る取組は、インシデント発生時における関係組織間の連携強化だけでなく、被害組

織による自律的なインシデント対処及び未然防止が可能となるような知識・技能の習得を目的に、内閣サイバーセキュリティセンターにおいて、既存の訓練や演習との役割分担に留意しながら、JISP を利用した実践的な演習を開催することが望まれる。また、演習だけでなく、サイバーセキュリティ対策の強化が急務となるテーマや、高度化・進化するサイバー攻撃への対処をテーマに各組織で意見交換会を開催するなどの取組が望まれる。想定される具体的な取組事例を以下のとおり示す。

○　インシデント発生時に政府を始めとする関係組織と的確に情報共有する手順に加えて、各組織が自律的に最低限の対処を行うために必要な能力等を習得するための訓練・演習の開催

○　高度化・複雑化するサイバー攻撃への対処に必要な能力を習得するための訓練・演習の開催

○　サイバーセキュリティ対策に係る取組事例、サイバー攻撃への対処方法、ノウハウ等の情報を業界に捕らわれずに多様な組織間で情報交換できる場の提供

④ 情報共有プラットフォームの提供

【各構成員からの意見・指摘】

○　標的とする情報の窃取等について明確な目的を持って行われる組織的・国家的なサイバー攻撃による被害が顕著になる中、同一の活動目的又は業界内の組織間における情報共有や連携強化が、二次被害等を防ぐ上で重要となる。このような特定のコミュニティ内での情報共有では機微な情報を扱うことになるため、情報共有プラットフォームのサイバーセキュリティ対策が非常に重要となるが、事業者間で調整してこのような基盤を準備することは容易ではない。政府が整備・運用する JISP を信頼性の高い基盤の一つとして提供可能になれば、コミュニティの立ち上げ、活動の活性化が図られるほか、コミュニティ内、コミュニティ間の情報連絡、連携も円滑になることが期待される。

○　インディケータ情報の共有は、体制参加組織において実効的なサイバーセキュリティ対策を講じる上で、有効な取組である。円滑に対策が講じられるよう機械連携等の仕組みを用いつつ、積極的な情報共有を行うべきである。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「情報共有プラットフォームの提供」に係る取組は、情報共有に参加する組織が信頼関係を構築する際の礎となるものであることから、各組織間での情報共有を安全かつ効率的に行うことを目的

に、内閣サイバーセキュリティセンターが、持続可能性等に留意しながらJISPを整備・運用し、各組織に提供していくことが望まれる。また、JISPの提供は、サイバーセキュリティの確保を目的とした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ことも期待される。また、情報共有プラットフォームにおける機能の一つとして、機械連携等の仕組みを用いたインディケータ情報の提供についても期待される。想定される具体的な取組事例を以下のとおり示す。

○　インシデント発生時における被害組織からの報告や対処支援要請、内閣サイバーセキュリティセンターからの脅威情報等の提供等、各機能を提供する統一窓口としての運用

○　インシデント発生時における情報共有等が必要となる関係組織（ISAC、セプター、システム整備事業等の委託先となるベンダー事業者、大規模国際イベント関連組織等）の参加促進に係る調整

○　ISAC、ISAO等の設立、運営に用いるプラットフォームとしての提供

○　内閣サイバーセキュリティセンターにおいて把握・分析した有害なインディケータ情報を機械連携の仕組み等を活用して事業者等に提供（再掲）

4.2.2　リスクマネジメントの促進

①　リスクアセスメント

【各構成員からの意見・指摘】

○　複数の事業者等が共通の手法でリスクアセスメントに取り組むことで、自組織の幹部とサイバーセキュリティ対策についての考え方、その手法等についての議論を行ったり、同一業種内の他事業者等との間で効果的な対策について意見交換を行ったりする機会が作られた。自組織における対策を見直すような機会が設けられることは貴重であり、対策を促進していく上で効果的である。

○　リスクアセスメントは、その対象事業者等が外部からの求めでやらされているという認識では効果が期待できず、自ら問題意識を持って取り組む組織を対象に取組を推進するべきである。

○　より多くの事業者等で取り組まれるよう、ガイドライン等機微な情報が含まれない資料は積極的に公開するとともに、効果的な活用事例等を整理して周知するなどして、取組についての考え方や必要性をしっかりと社会に広げていくことが重要である。その際、ISACや事業所管省庁と連携して、コミュニティ内において一斉に取組を実施するなどキャンペーンとして推進することも有効である。

○　リスクアセスメントの結果等について個別にフィードバックを得ることができるという点が事業者等にとってのメリットであるが、各組織が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、内閣サイバーセキュリティセンター及び事業者等の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。

○　この度の取組では、事業継続に重点を置いた取組を推進したとのことであるが、リスクとして捉えるものは、個々の事業者等のサービス、情報資産等によって異なることから、複数のアプローチによる評価手法を検討するほか、事業者等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。

○　リスクアセスメントの評価結果は、自組織の対策状況を評価する上でわかりやすい指標となるものの、総合的な評価として他の事業者等と比較して「よくできている」「足りていない」等の単純な結果を示してしまうと、その子細についての確認がなされずに満足されてしまうおそれがある。個々の事業者等のサイバーセキュリティ対策は、一概に並べて比較することができるものではないという点に留意し、その評価結果が短絡的に捉えられないよう配慮するべきである。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「リスクアセスメント」に係る取組は、特に経済・社会活動を支える事業者等を対象としてサイバーセキュリティ上のリスクを軽減させることを目的に、内閣サイバーセキュリティセンターが、リスクアセスメントの手法等を提供していくことが望まれる。その際、個々の組織のサービス、情報資産等に応じた複数のアプローチによる評価手法、各組織の規模や対策のレベルに応じた評価手法を準備・公表することが望まれるほか、各組織がリスクアセスメントの機会をどのように位置づけ、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。また、リスクアセスメント結果に対するフィードバックによって取組の実効性を確保することも重要であり、対象事業者等にとって取り組みやすく、かつその負担が軽減されるように、評価結果の充足性等を効果的・効率的に確認できる仕組み・ツールの開発等の取組を推進することが望まれる。想定される具体的な取組事例を以下のとおり示す。

○　リスクアセスメントに関する位置づけ、活用方策、手順等の提供・公表を含めた各組織による自主的なリスクアセスメントの支援

○　事業者の分野、規模、対策レベル等に応じて活用できるリスクアセ

スメント手法の開発・普及

○　サイバーセキュリティに係るリソースが十分でない組織等に対するリスクアセスメント結果をフィードバックする点検ツール等の提供

②　横断的リスク評価

【各構成員からの意見・指摘】

○　サプライチェーン対策等の重要性が認識され始めたが、各組織における自主的なサイバーセキュリティ対策のみでは限界がある。政府自らが直接的にセキュリティ対策の実施状況に係る検証を実施したことは、セキュリティの確保に不可欠であり、今後の大規模国際イベント等でも積極的に取り組むべきである。

○　攻撃シナリオを使って、事業者等にその対処方法をシミュレーションさせたり、又は、多層防御のどこでそのような攻撃を防御可能になっているのかを考えさせたりする取組について、このような攻撃シナリオは自社の内情を知っているからこそ各事業者内で作成することが難しく、外部からの目線でシナリオを作成することが効果的である。今後の大規模国際イベント等において、国を挙げてサイバーセキュリティ対策を講ずる際にも、セキュリティ動向や攻撃パターンを知るNISC が主導して大会に向けた取組と同様の取組を推進するべきである。

○　サイバーセキュリティ対策の検証において事業者内で対応しなければならないシステム上の脆さ等が確認された際に、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。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「横断的リスク評価」に係る取組は、大規模国際イベントにおいて特に重要な役割を担う事業者等を対象として、各組織における自主的なサイバーセキュリティ対策では不十分と考えられる場合や、十分な公益性が認められる場合に、内閣サイバーセキュリティセンターが、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について検証を行い、その対策を改善していくことが望まれる。想定される具体的な取組事例を以下のとおり示す。

○　大規模国際イベントにおいて特に重要なサービスを提供する事業者等のサイバーセキュリティ対策に関する攻撃シナリオ等を用いた早期の政府による検証

○　大規模国際イベントにおける会場施設等に対するペネトレーションテスト

③　スポーツ関連団体に対する勉強会

【各構成員からの意見・指摘】

○　標的とする情報の窃取等について明確な目的を持って行われる組織的・国家的なサイバー攻撃による被害が顕著になる中、同一の活動目的又は業界内の組織における情報共有や、連携強化が、二次被害等を防ぐ上で重要となる。（再掲）

○　情報共有、連携強化のためのコミュニティの立ち上げ、運営に際しては、仮にサイバーセキュリティ対策についての問題意識を事業者等の間全体で共有していた場合でも、事業者等の間でセキュリティに係る人的リソースやコミュニティ運営に係るノウハウが一定程度保有されていなければ、その実現は容易ではない。その点、大会に向けてスポーツ関連団体に対して行った取組は、コミュニティ内のサイバー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、ISAC、ISAO等のコミュニティの立ち上げ、活動の活性化を図るための支援策として有効に機能することが期待される。

○　ISAC、ISAO 等の特定のコミュニティ内での情報共有は機微な情報を扱うことが想定され、情報共有プラットフォームのサイバーセキュリティ対策が非常に重要になるものの、各事業者等の間で調整してこのような基盤を準備することは決して容易なことではない。政府が整備・運用する JISP のような信頼性の高い基盤が一つの選択肢として提供されるのであれば、コミュニティの立ち上げ、活動の活性化が図られるほか、コミュニティ内、コミュニティ間の情報連絡、連携も円滑化すると期待する。

【意見・指摘を踏まえた大会後の活用方策】

「スポーツ関連団体に対する勉強会」に係る取組は、大会後における新たなコミュニティの立ち上げ・運営を支援する取組において有用である。そのため、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ける基本的な知識・技能の習得等を目的に、内閣サイバーセキュリティセンターが、事業所管省庁等と連携して取組を加速することが望まれる。特に、事業分野全体でデジタル化の推進が期待されるものの、IT やセキュリティに関する専門知識や業務経験が乏しい分野等に対して必要な支援を重点的に実施していくことが重要である。また、コミュニティ内では安全で効率的な情報共有が求められるため、信頼性の高い情報共有基盤が必要となる。想定される具体的な取組事例を以下のとおり示す。

○　支援対象のコミュニティに係る事業所管省庁等との調整
○　支援対象のコミュニティに対する勉強会・机上演習の開催、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等の実施、JISP の提供等

4.2.3　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

【各構成員からの意見・指摘】

○　イベントが開催される際は、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、平時の取組をベースに、この度の大会で構築した対処態勢と同様の体制を構築することにより、各関係組織におけるサイバーセキュリティ対策やインシデント対応を他の体制参加組織の取組と有機的に結びつけていくべきである。
○　リスクマネジメントを促進するため、大規模国際イベントに際しては、関係事業者等における自主的なリスクアセスメントのほか、内閣サイバーセキュリティセンターが関係事業者等の対策状況を検証する横断的リスク評価、ペネトレーションテスト等の取組を推進することによって、実効的な対策を関係組織が講じていくようにすることが重要である。一方で、あらゆる関係事業者等を対象に同一の水準で対策を講じることは現実的でなく、非効率な面もあることから、当該イベントにおけるサービスの重要性等に照らし、メリハリをつけた対策が講じられるようにするべきである。

【意見・指摘を踏まえた大会後の活用方策】

大会後における「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」に係る取組は、特に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の確保を目的に、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、内閣サイバーセキュリティセンターにおいて、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」に係る取組を推進していくことが望まれる。想定される具体的な取組事例を以下のとおり示す。

○　平時の取組をベースにした大規模国際イベント等の関係組織間での対処態勢の整備（インシデント等に係る対処調整、予防・検知に関する情報の発信・共有、サイバー攻撃への対処能力の向上、情報共有プラットフォームの提供等）、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、勉強会の開催等）

4.2.4　取組を推進するに当たって対象とする領域

サイバー空間の秩序の維持に当たっては、様々な社会システムがそれぞれの任務・機能を自律的に実現し、あらゆる主体がその役割や責任を果たすことが必要となる。他方、サービスの進化・多様化が進む一方で、サイバー空間の脅威の増大、脆弱性の顕在化等、不確実性が増す情勢にあり、各主体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は高度化、複雑化していると言える。デジタル化の更なる進展に向けて、各主体に求められる対策は今後より一層重要になると考えられるものの、個々の自律的な取組のみで対応していくには限界がある。我が国のサイバーセキュリティ対策をより高い水準に引き上げるには、英国において取り組まれる政府から事業者等への積極的なサイバーセキュリティ対策を参考に、政府から事業者等に対する支援を推進するとともに、米国における ISAC、ISAO 等の特定の目的を共有するコミュニティ内又はコミュニティ間での強固な連携等を参考に、各主体における相互の支援・連携の強化に向けた支援を推進することが重要であると考える。

内閣サイバーセキュリティセンターが大会を契機に関係機関等における相互の信頼関係を築き、サイバーセキュリティに係る脅威・インシデントに対し関係機関等が自律的に未然対処及び事案対処ができるよう整備・運用した対処調整センター、準備・運営への影響の未然防止や想定されるサイバーセキュリティ上のリスクへの対策の促進のために推進してきたリスクマネジメントは、サイバーセキュリティの確保に向けて、業種分野等の隔たりなく、関係組織が緊密に連携・協力して取り組んできたものであるが、こうした取組は前述の課題認識や社会的要請に応えられるものであると期待できる。

これまでの取組は、大会の関係組織を対象に実施してきたものであるが、大会後にあっては取組の対象領域を、社会経済を支えるサービスを提供する事業者等に拡大し、各主体において適切にサイバーセキュリティが確保されるようにするべきである。取組の対象領域の拡大に当たっては、サイバー脅威情勢等を考慮することとし、公益性等の観点から優先度の高い分野について、事業所管省庁等と連携した上で、コミュニティの構築・運営支援や対処体制の追加等を通じて、徐々にその対象を拡大していくことが望まれる。一方、持続的な対策としての各取組の推進に当たっては、様々な既存の取組における現状と課題を踏まえた上で各取組との整合性を確保すること、対象拡大の方法や基準の考え方を整理すること、取組の必要性や有益性について各主体

の理解を得ること等の運用上の課題が存在するところ、大会後においても各取組が確実に機能するよう、内閣サイバーセキュリティセンターが全体を俯瞰しながら、これらの課題を関係組織との間でしっかり調整するなど丁寧な対応が求められる。

また、令和５年に我が国での開催が予定されるＧ７サミット、７年の大阪・関西万博といった大規模国際イベント開催時には、大会と同様に、関係組織間で緊密に連携した上で対処体制を構築し、イベントの安全、円滑な準備及び運営における継続性の確保に向けてサイバーセキュリティ対策を進めていくべきである。特に、大阪・関西万博は、「未来社会の実験場」をテーマに ICT を含む様々な最先端技術を発信する場に位置づけられ国内外から大きな注目を集めるほか、大会と同様に、関係する機関、事業者等が多岐にわたるなどの特徴を有していることから、サイバーセキュリティ対策上の課題も多岐にわたると考えられる。そのため、同イベントへの対策については大会の終了を待つことなく、速やかに準備を進めていくべきである。

加えて、サイバーセキュリティリスクが多様化・高度化する中で、国内外の関係者と協調しながら、こうした取組を継続的に進めるため、内閣サイバーセキュリティセンターにおいては、これまで以上にしっかりとした体制を整備することが求められる。

５　今後の検討の進め方

以上のとおり、本有識者会議では、大会に向けた取組のこれまでの推進状況、成果を踏まえつつ、今後の我が国のサイバーセキュリティ対策の強化に活用するための方策、課題等について討議を行い、一定の方向性を整理できたと考える。

現在、内閣サイバーセキュリティセンターを始めとした関係組織の事前の対策、準備は佳境となり、いよいよ大会の開催を迎えようとしているところである。大会に向けた取組は、本中間整理で取り上げたように、現時点で既に一定の成果を確認できたものもあるが、大会期間中におけるサイバーセキュリティ対策の運用結果等から、これまでの取組に関する教訓や反省が多く得られると考えられる。本有識者会議では、これらの教訓や反省、対処体制参加組織からの取組の評価等を踏まえ、大会後に速やかに最終報告に向けて更に議論を深める必要がある。

また、世界から最高度の注目を集めるイベントであるオリンピック・パラリンピック競技大会をコロナ禍という異例な環境下で開催する機会は、我が国としてこれまで経験したことがないものであるが、内閣サイバーセキュリテ

ィセンターを中心とした大会関係組織では、そのサイバーセキュリティ対策をコロナ禍におけるテレワークの導入を始め情報通信技術の活用形態が大きく変動したことなども踏まえながら推進してきた。このような対策は、今後の「ニューノーマル」を見据えた場面でも十分に活用可能で、対策を推進する中で得られた貴重な知見やノウハウを、国内外の関係者と共有しつつ、後世に残していくことは重要な意義があると考えられる。最終報告に向けては、このような機会であるからこそ得られた経験や教訓についての積極的な議論も行う必要がある。