2020年東京オリンピック・パラリンピックに向けた政府の取り組み

山内 智生 ●内閣官房内閣サイバーセキュリティセンター

サイバーセキュリティの確保は2020年東京大会成功に欠かすことのできない要件の一つ。NISCはリスクマネジメントの促進と対処態勢の整備を進める。

■過去の大会では膨大なサイバー攻撃

執筆時点で、2020年東京オリンピック・パラリンピック競技大会（以下「2020年東京大会」と呼ぶ）まであと約半年となった。2020年東京大会には、世界中から多数のアスリート、要人、観客等が集まり、国際的にも最高度の注目を集めて開催される。

過去の大会を振り返ると、2012年のロンドン大会では、大会の運営には影響はなかったものの、膨大な数のサイバー攻撃があったとされる。2016年のリオデジャネイロ大会においても2018年の平昌大会においても、相当数のサイバー攻撃が行われ被害を受けた[1]との報道がある。2020年東京大会においても、過去の大会以上のサイバー攻撃が想定されるところであり、サイバーセキュリティの確保は、大会の成功に欠かすことのできない要件の一つと言えるだろう。

■2020年東京大会のサイバーセキュリティ検討体制

資料4-1-4に検討体制の全体像を示す。政府では、「サイバーセキュリティ戦略」[2]やその年次計画「サイバーセキュリティ2019」[3]においても、「2020年東京大会とその後を見据えた取組」と項目を立てて、2020年東京大会のサイバーセキュリティの確保のための取組について記載している。

具体的な取組については、「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推進本部」の下に設置された「セキュリティ幹事会」、「サイバーセキュリティワーキングチーム」等においてサイバーセキュリティ対策を検討する。それとともに、2020年東京大会のセキュリティの基本的な考え方、対策等をとりまとめた「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」[4]に基づき対策を推進している。

資料4-1-5は、大会に関連する各種のサービスについて、誰が責任を持ってサイバーセキュリティを確保するのかを表している。大会の基幹システム等、大会の運営のために組織委員会が準備するサービスについては、主に組織委員会が取組を実施することとしている。また、大会の開催・運営に間接的に影響を与えるサービスについては国の主導で取組を実施することとしている。

直接的に影響を与えるサービスの場合は、基本的に組織委員会が事業者との契約により実施させるサービスであることから、契約の範囲で組織委員会が取組を実施する。そして契約で対応が困難

な部分については国が主導する取組を実施するなどの役割分担を行っている。事業者が提供するサービスについては、基本的には事業者の責任で対策を実施することになるが、国は関係機関と連携してその対策が適切なものとなるよう各種の取組を実施する。

■NISCの取組

大会全般に関連して、内閣サイバーセキュリティセンター（以下「NISC」という）がサイバーセキュリティの確保のために行っている取組は、「リスクマネジメントの促進」と「対処態勢の整備」の2つに大別される。

リスクマネジメントについては、大会の運営に大きな影響を及ぼし得る重要なサービスを提供する事業者（重要サービス事業者）に対して、NISCが作成したリスク評価手順書を提供し自主的にリスク評価の実施（リスクアセスメント）を依頼するものと、サービスの相互依存性に着眼して分野を横断して評価（横断的リスク評価）する2種類の評価を実施し、それに基づき事業者における対策を促進している。

一方、対処体制の整備は、関係府省庁、大会組織委員会、東京都、競技会場のある地方公共団体、重要サービス事業者、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を共有するとともに、事案発生時に大会関係組織が連携し協力して対応する「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）を構築し、緊密に連絡調整を図るための態勢を整備している。

●リスクマネジメントの促進

リスクマネジメントの促進の内容を具体的に説明する。

まず、重要サービス事業者の選定である。オリンピック・パラリンピック競技大会に関わる様々な人物を設定し、その人物が大会への参加を考え、参加して帰宅するまでに利用し得るサービスを洗い出す。次に、そのサービスが停止した場合に大会の開催・運営に影響し得るサービスを洗い出す。これらを総合して、優先順位付けした上で、上位にあるサービスとそのサービスを提供する事業者を特定した。現時点で、重要サービス事業者は、23分野[5]及び会場の約300者となっている。

NISCは、対象となる重要サービス事業者に対して所管省庁を通じてリスクアセスメントを依頼して、上述の手順書により自主的に実施していただいた評価結果に基づき、事業者における対策を促進している。大会までに計6回の実施を予定している。自らのリスクアセスメント結果に関する助言等の要望があることから、各事業者のリスクアセスメント結果を分析し、個々の事業者に対してフィードバックを行っている。

リスクマネジメントでは、事業者自身のリスクアセスメントへの取組と並行して、横断的リスク評価を実施している。これは、大会において想定されるべきサイバーセキュリティリスクに基づき情報セキュリティ対策の実施状況を検証することによって、大会の成功に重要なサービスが正しく提供されることを確認するとともに、不備があった場合には、重要サービス事業者にフィードバックする。これにより、当該サービスが正しく提供されることの確度を高めるものである。

電力、通信、水道、鉄道、放送等の重要サービス事業者から5者程度を対象とした実地検証と、全重要サービス事業者から20者程度を対象とした書面検証を実施している。

具体的には、特定のリスクが顕在化し大会の運営に大きな影響が発生するシナリオを作成し、各事業者等が設定したルールの妥当性や実効性につ

いて検証することとしている。その際には、対象となるシステムの相互依存性に考慮して、相互のシステムのサービス水準等についても確認を行っている。

NISCでは事業者等を対象に情報交換会を実施している。リスクアセスメントの実施要領等の説明等、アセスメントの効率的・効果的な実施の促進とそのための必要な情報提供をするとともに、同業分野の事業者等の担当者間での交流の場を提供し、意見交換の促進を図っている。

また、スポーツ関連団体に対してもサイバー攻撃が行われたというリオデジャネイロ大会の教訓から、スポーツ関連団体のサイバーセキュリティの確保についての勉強会を実施し、関係する方々の意識の向上を図り、サイバーセキュリティ対策の促進を行っている。

●対処態勢の整備

次に対処態勢の整備について述べる。情報共有・対処体制について、大会のサイバーセキュリティに係る脅威・インシデント情報を収集し、これらの情報を、大会組織委員会をはじめとした関係機関等に提供し、必要がある時には関係機関等のインシデント対応の対処支援を調整する態勢を整備している。

2019年4月には、オリパラ推進本部の下で、オリパラ推進本部事務局と緊密に連携し、NISCが中心となって運用を行うサイバーセキュリティ対処調整センターを立ち上げた。2019年には、G20大阪サミット及び関係閣僚会合、ラグビーワールドカップ、皇位継承に係る行事等の大規模な行事が実施されたことから、対処調整センターを運用し当該行事のサイバーセキュリティの確保を行い、その運用経験とノウハウを2020年東京大会に活用することとしている。

また、対処調整センターの運用に当たり、効率的・効果的な情報共有を行うためのシステム「JISP（Japan cyber-security Information Sharing Platform）」を構築した。このシステムでは、スマートフォンやパソコンで何時でもアクセスでき、必要な相手に情報の送受信を容易にかつ適切に行うことができるよう、情報の内容によっては、共有する相手方を限定し、ユーザー自らが発信する情報の共有範囲を設定できるようにしている。

また、JISPには、訓練機能を持たせており、訓練参加の募集から、訓練そのものの実施、アンケートの集約まで可能となっており、単独・複数の組織による訓練等をいろいろな形態で実施できるようになっている。重要サービス事業者、スポーツ関連団体等から非常に多くのユーザー登録をしていただいている。システムの操作方法に慣熟して、2020年東京大会本番までに情報共有ツールとして活用していただくとともに、JISP上によるものを含め、インシデント発生時の対処調整に関わる各種の訓練・演習を経験していただきたいと考えている。

リスクマネジメント、対処態勢の双方に共通して重要なことは、リスクはゼロにはならないことを念頭に取り組むことである。リスク分析に基づいてサイバーセキュリティ対策を事前に講じることは当然必要であるが、リスク、すなわち不確かさを全て除去することは困難である。リスク分析の結果、自らがどこまで対策できているかを確認するとともに、万一、サービス提供が停止する、あるいは停止しかねない状況が生じた時にとるべき対応についても事前に検討し、その対応を想定通り実施することができるか否かを訓練・演習により確認することも必要である。これらの取組を通じて、各事業者の方々に「万全の態勢」で臨んでいただきたいと考えている。

■警察庁や総務省の取組

NISC以外の政府機関においても、各種のサイバーセキュリティに関わる取組が実施されており、以下のとおり「サイバーセキュリティ2019」に記載されている。

「警察庁に構築したセキュリティ情報センターにおいて、国の関係機関の協力を得て、サイバーセキュリティに係るものを含む2020年東京オリンピック・パラリンピック競技大会の安全に関する情報集約を一層推進するとともに、大会の安全に対する脅威及びリスクの分析、評価を行い、国の関係機関等に対し必要な情報を随時提供する」

「警察庁及び都道府県警察において、2020年東京大会その他の大規模国際イベントを見据えたサイバー攻撃対策を推進するとともに、態勢の運用を通じて得た情報収集・分析、管理者対策、事案対処等に関する教訓やノウハウの効果的活用を推進する。また、法務省（公安調査庁）において、人的情報収集・分析を行うとともに、その過程で得られた教訓やノウハウについて、庁内での周知及び活用を推進する」

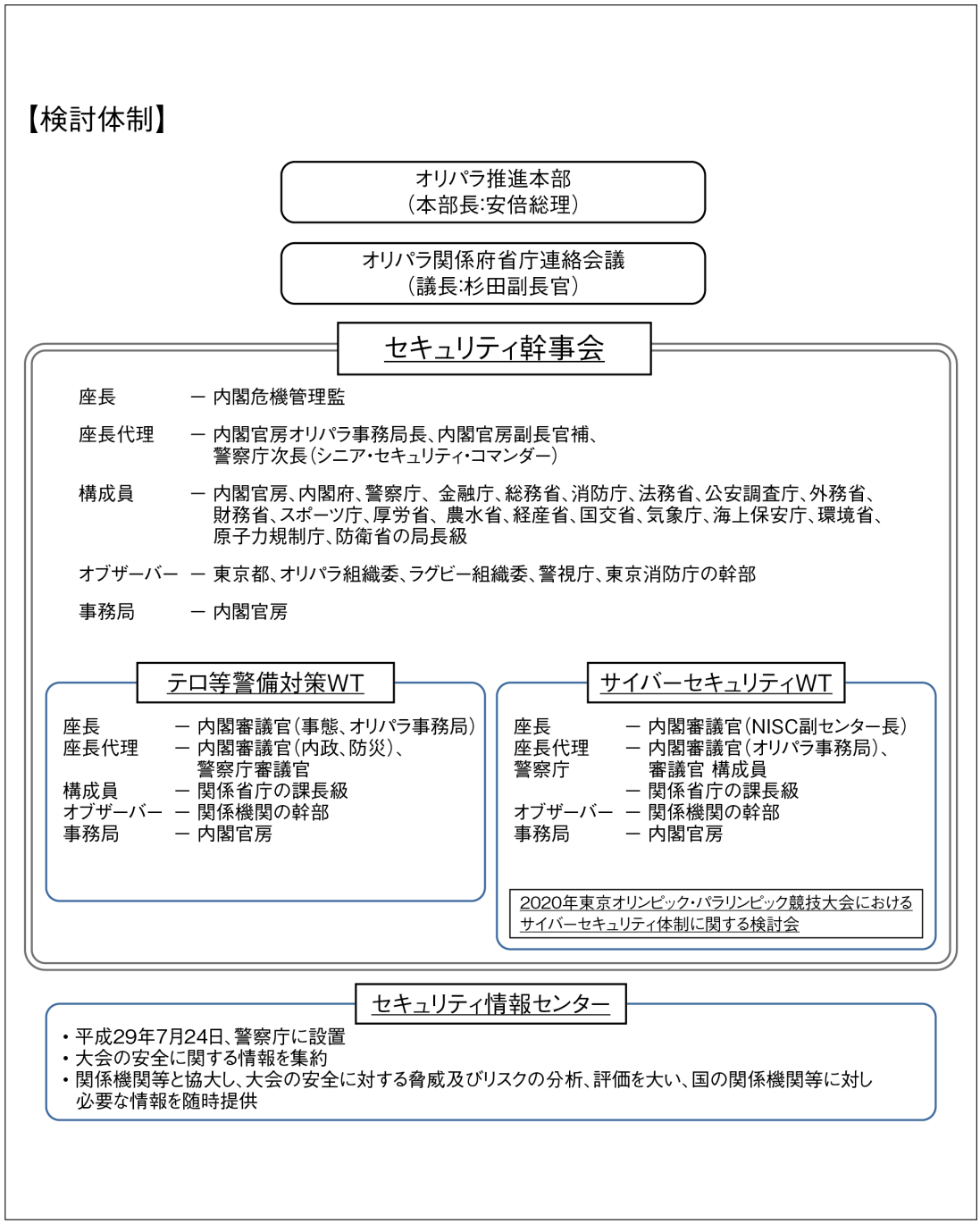
「総務省において、NICTの「ナショナルサイバートレーニングセンター」を通じ、2020年東京オリンピック・パラリンピック競技大会のセキュリティ担当者のサイバー攻撃への対処能力の向上を図るための実践的サイバー演習である「サイバーコロッセオ」[6]を、更なる内容の拡充と受講機会の拡大を図りつつ実施する」

これらの取組のほとんどは、2020年東京大会後もレガシーとして活用することを想定しており、その枠組みや手法を我が国全体に拡大することで、我が国のサイバーセキュリティの確保のために使う予定である。

政府の一員であり、そのサイバーセキュリティに関する施策をとりまとめる立場であるNISCとして、間近に迫った2020年東京大会の運営に大きな支障が生じないよう取り組みを進める予定であり、皆様の御協力と御支援を賜れば幸いである。

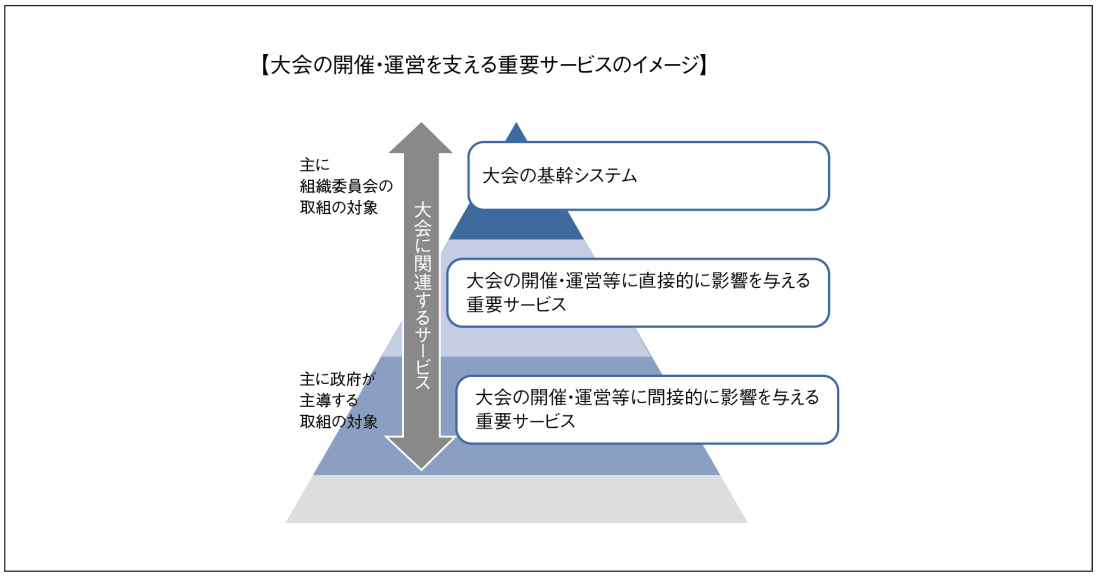
1. https://www.nisc.go.jp/conference/cs/dai10/pdf/10shiryou08.pdf（リオ大会）
   https://www.nisc.go.jp/conference/cs/dai18/pdf/18shiryou04.pdf（平昌大会）
2. https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf
3. https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf
4. https://www.kantei.go.jp/jp/singi/tokyo2020_suishin_honbu/pdf/20190730_security_honnbun.pdf
5. 通信、放送、金融、航空、鉄道、電力、ガス、上水道、物流、クレジット、行政サービス（地方公共団体）、下水道、空港、道路・海上・航空交通管制、緊急通報、気象・災害情報、出入国管理、高速道路、熱供給、バス、警備、旅行、病院
6. https://colosseo.nict.go.jp/

資料4-1-4　2020年東京オリンピック・パラリンピック競技大会に向けた取組



出典：NISC 作成

資料 4-1-5　大会の開催・運営を支える重要サービス



出典：NISC 作成

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2020年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp