

## 【パネリスト発表②】

### 東京大会における政府のセキュリティ・交通対策について

内閣官房東京オリンピック競技大会・パラリンピック競技大会推進本部事務局

セキュリティ推進統括官

山本 仁

#### はじめに

私は、内閣官房において、オリンピック・パラリンピック東京大会のセキュリティと交通輸送の政府の施策を取りまとめる統括官（内閣審議官）をしている。出身は警察庁で前職は警視庁の交通部長であった。

#### 1 東京大会開催における政府の役割

政府としては、東京大会の課題は3つあると考えている。1つは交通輸送、2つ目がセキュリティ、3つ目が暑さ対策。暑さ対策については、主として組織委員会、東京都が対策を講じているので、政府としては最初の2つにしっかりと対応する必要があると考えている。

オリンピックを直接運営するのは組織委員会であり、開催都市の東京都にはオリンピック・パラリンピック準備局がある中で、内閣官房東京オリンピック・パラリンピック推進本部事務局は一体何をしているのかというお尋ねを皆様からよく受ける。東京大会における国の役割の多くは、組織委員会や東京都の支援調整である。例えば、各国選手の練習場所となるホストタウンのマッチング、機運の醸成、大会に合わせた日本文化の発信、障害者の方のためのユニバーサルデザインの普及等である。

しかし、私の担当しているセキュリティと交通輸送については、国の立ち位置は若干異なり、ある意味、現場と向き合っている。その理由は、東京大会が世界最大かつ長期間のイベントであるためである。例えばG7、G20と比べてみると、G7、G20の警備や交通規制は警察が数日間がっちりと統制して成功しているが、オリンピック・パラリンピックとなると、それだけではうまくいかない。

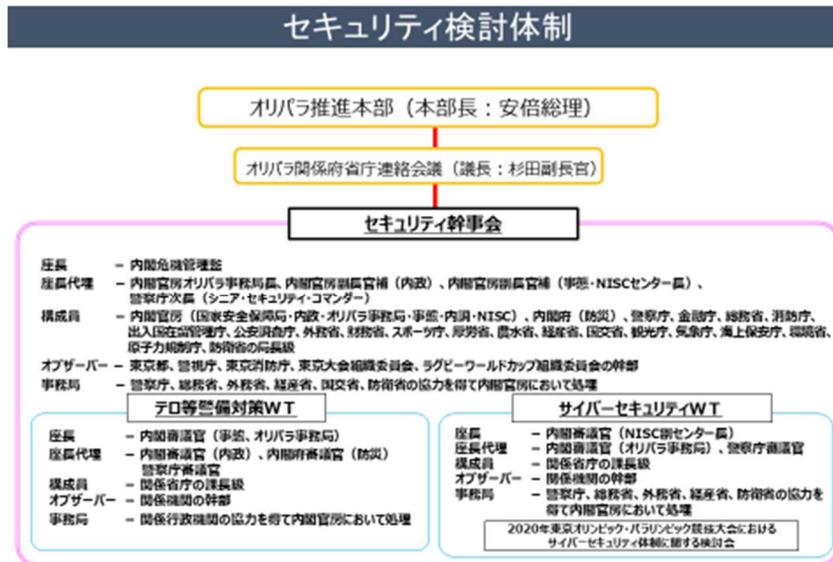
セキュリティの面では、大会の競技会場だけでなく、多数の鉄道駅、空港、路線、繁華街等を、事業者を巻き込んで長期間守っていく必要がある。また、大会運営を支える電力、ガス、通信、水道等の重要インフラが、テロやサイバー攻撃はもちろんのこと、昨年（平成30年）関西を襲った水害や今年（令和元年）の台風のような自然災害で止まったり、インフラの劣化により鉄道が運休したりすることで、大会運営に支障が出ることは、最大限避けなければならない。さらに、感染症対策も重要である。平昌大会では、ノロウイルスにより、当初、ボランティアが活動できなくなった。このような感染症の発生を抑える必要もある。

すなわち、国を挙げてのトータルなセキュリティが長期間求められる。また、東京大会を契機として、国家のセキュリティ基盤を1段階引き上げ、これをレガシーとしたいと考えている。そこで、幅広い意味でのセキュリティに関係する様々な省庁の施策を調整促進するという、内閣官房の役割が生じることになる。

また、交通輸送についても、高度の交通規制だけで大会関係車両を通そうとすれば、都内の一般道路は大渋滞になってしまう。鉄道も観客と通勤客によってあふれてしまうことになる。このような状

態が長期間続けば市民生活と経済に多大な影響が出るので、東京だけではなく全国の関係業界や経済団体に交通量の抑制をお願いする必要がある。また、交通政策のレガシーとなる首都高速道路の料金施策であるとか、鉄道事業者の運行ダイヤの組替えも行う必要がある。このようなことから、自治体や警察だけでなく、国の旗振りが必要となっている。

## 2 セキュリティ検討体制（スライド1参照）



〈スライド1〉

国としては、セキュリティについて、総理大臣を長とする東京オリンピック・パラリンピック推進本部の下に、内閣危機管理監を座長として関係府省庁の局長級をメンバーとするセキュリティ幹事会を設けて、関係府省庁の施策を定期的に促進している。この幹事会には2つのWT（ワーキングチーム）が設けられており、物理的なテロを対象とするテロ等警備対策WT、サイバーセキュリティの施策を担当するサイバーセキュリティWTが活動している。我々の東京オリンピック・パラリンピック推進本部事務局は体制が弱い組織であるため、テロ等警備対策WTは内閣官房の事態対処・危機管理担当が、サイバーセキュリティWTは内閣サイバーセキュリティセンター（NISC: National center of Incident readiness and Strategy for Cybersecurity）が実務を担っている。

### 3 2020 東京大会に向けたセキュリティ対策について（「基本戦略」決定以降のもの）（スライド2 参照）

**2020年東京大会に向けたセキュリティ対策について(「基本戦略」決定以降のもの)** 平成31年3月現在

**体制構築等の取組**

- 2020年東京大会に向けたセキュリティ基本戦略を決定（平成28年3月21日）
- セキュリティ情報センターを整備（平成29年7月24日）
- オリパラ・テロ対策推進本部を決定（平成29年12月11日）
- 国際テロ対策等情報共有センターを内閣官房に設置（平成30年3月1日）
- サイバーセキュリティ対策調整センターを内閣官房に設置（平成31年4月1日）
- セキュリティ調整センター（仮称）を内閣官房に設置（大会期間中）

**情報収集・分析の強化**

- 「セキュリティ情報センター」において大会の安全に関する情報を集約し、大会の安全に対する脅威及びリスクの分析・評価を実施
- オリパラ・テロ対策推進本部に基づき、「国際テロ情報収集ユニット」等の活動を拡大・強化

**競技会場等の安全の確保・アスリート、観客等の安全安心の確保**

- 関係省庁・機関等が連携した実証的取組を実施
- 警備計画等の策定に向けた競技会場等予定地の実地踏査、施設確保等の確保を実施
- 外国人来訪者や観客等が利用する施設における災害情報の伝達及び避難誘導に関するガイドラインを策定し、公表
- 食品防御ガイドライン等を作成し、東京大会で飲食提供を行う事業者に対して助言

**重要サービスの継続性確保**

- 電力、鉄道等の重要サービスについて、大会運営に支障を来さないための課題を特定し、確保対策を確立
- 競技会場等において、電線の多量化、通信の冗長化措置等の確保にとらわれていることを確認

**水際対策の強化**

- 入国管理官や税関等の人的・物的確保を充実・強化
- 取得したPCR(新型コロナウイルス)を分析、活用
- 競技会場による会場内感染防止や会場内外の感染対策を実施
- 海上・臨海部テロ対策協議会における机上訓練を実施

**重要施設、ソフトウェア等の警戒監視の強化**

- 新幹線において緊急に誘導すべき当番の対策を取りまとめ、遠方実施するほか、公共交通機関に搭乗するテロ対策を強化
- 各種イベント主催者等と連携し、物理的防護措置を徹底する等、車両進入テロ対策を推進
- 競技会場ネットワークの構築や同ネットワークに基づく各種情報の交換、海上・臨海部テロ対策協議会の開催等、官民一体となったテロ対策を推進

**テロリストに武器等を入手させないための取組の強化**

- 銃砲・火薬類を取り扱う個人・事業者に対する規制、指導を徹底
- 爆発物、毒物、病原体・毒薬、放射線物質等につき取扱事業者等の適正な保管・管理を要請
- 物品検査の指し指の身元確認を徹底、違法民泊施設の取締りを推進

**サイバーセキュリティ対策の強化**

- 重要サービス事業者等によるリスクアセスメントの実施とこれに基づいた対策を促進
- 「サイバーセキュリティ基本法の一部を改正する法律案」を国会に提出(平成30年12月成立)
- 「原子力施設情報システムセキュリティ対策ガイドライン」を策定し、原子力施設の情報システムに対する脅威を事業者に提示

**国際連携の強化**

- 国際情報犯罪防止条約の国内批准法を整備、同条約を締結
- 韓国・日本・米国との共同テロ対策協議会を強化し、東京大会に向けたテロ対策に際し、高層の協力を共有することを一貫し、ほか、ロシア、中国等と二国間テロ対策協議会を強化
- インドネシアに対し、共同テロ対策システムを供与するなど、アジア(特に東南アジア)地域のテロ対策を支援
- 「セキュリティ情報センター」において国際連携を推進

**自然災害への対応**

- 防災基本計画等に基づき、震度対策、風水害対策等を推進するとともに、防災対策について不届の見直し
- 大会期間中の首都圏下地震・大規模水害を想定した初動対応訓練(机上訓練)を実施
- 災害種別別対応の追加・改善、国際標準化、基盤に必要情報共有の多言語化による発信を推進

**緊急事態対応能力の強化**

- 緊急事態対応の特性(災害)等に関する情報、警備員機材、救急・災害対応訓練等を整備
- 天然痘ワクチン、化学テロ対策用医薬品を準備
- チケットの購入に向けた検閲職員増員(リユーム)等の実施、競技会場等の緊急時対応に向けた海外対応協議会における検討等、緊急事態体制を強化
- 関係機関や事業者から連携し、訓練・記録を逐次実施

(スライド2)

このスライドは、セキュリティ幹事会において具体的にどのようなことが行われているかを示したものである。セキュリティ幹事会では「東京大会に向けたセキュリティ基本戦略」を定めており、これに基づいて各省庁の施策が推進されている。

スライドの上の部分に、大会のセキュリティを支える政府の体制が記されている。このうちの「国際テロ対策等情報共有センター」は内閣情報調査室に置かれている常設の組織であるが、オリンピック・パラリンピックに向け、さらに3つのセンターが政府に設けられる。1つ目は、セキュリティに関するあらゆる情報を集約する「セキュリティ情報センター」で、既に警察庁に設けられ動き出している。2つ目は、大会に関係する官民のあらゆるサイバー事案に対処する「サイバーセキュリティ対処調整センター」で、今年（平成31年）4月から内閣官房に設けられており、既にG20で運用を試行し、この後もラグビーワールドカップ、即位礼等で経験値を上げる予定である。因みに、官民全てのサイバーセキュリティ事案を対象とする組織はこれまで日本に設けられていなかったもので、これも東京大会のレガシーになると考えている。3つ目として、聖火リレーのスタートから大会本番の期間にかけて、官邸に「セキュリティ調整センター」が設置される予定であり、暑さや感染症を含む幅広いトラブルに備えることとなる。

各省庁で進められている主な施策は、資料の中段以下に掲げられている。9つある枠のうち一番左上段の「競技会場等の安全の確保・アスリート、観客等の安全安心の確保」については、例えば、食品防御ガイドラインというものを作成した。東京大会で提供される飲食には、このガイドラインが適用される。

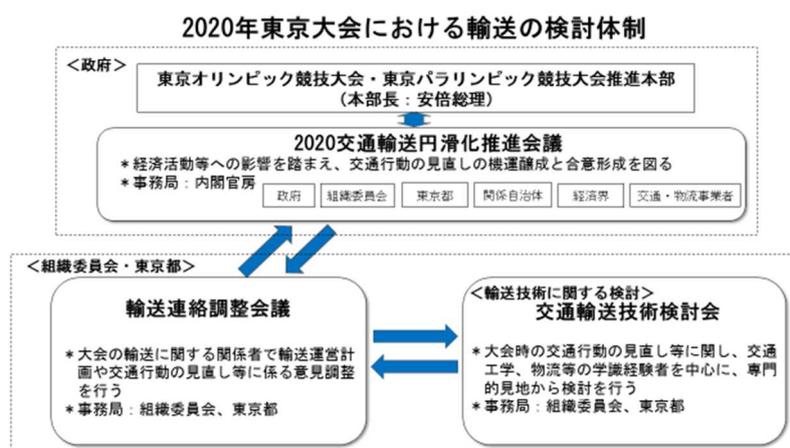
また、右隣の「重要サービスの継続性確保」については、電力、鉄道、通信の重要サービス事業者において、対策をしっかりと講じていただくとともに、大会本番はトラブルに備えて臨時的体制を編

成していただく。重要インフラのトラブルはシステムの更新によって発生することがあるため、来年（令和2年）春からは原則としてこうした更新も止めていただき、大会に備えることとしている。

その下の「テロリストに武器等を入手させないための取組の強化」については、例えば、違法民泊施設の取締り強化や指導を進めている。さらに、中段一番右の「サイバーセキュリティ対策の強化」についても、重要インフラ事業者のリスクマネジメントなどの様々な施策を推進している。

今後の課題としては、重要サービスの継続性確保に加えて、自然災害等が多発する中で、多言語による訪日外国人への情報発信等が重要と考えている。

#### 4 2020年東京大会における輸送の検討体制（スライド3参照）



〈スライド3〉

交通輸送についても、国に「2020 交通輸送円滑化推進会議」が設けられ、これまでの講演でお話しされたような取組を、組織委員会、東京都と連携して進めている。同会議は、関係府省庁、組織委員会、東京都、関係自治体、交通・物流関係の事業者・協会のほかに、日本経営者団体連盟、日本商工会議所、東京商工会議所、経済同友会等の経済団体が主要メンバーとなっており、この会議を通じて、各経済団体の参加企業に対して、東京大会の TDM (Travel Demand Management : 交通需要マネジメント) における具体的な行動等呼びかけている。

また、このスライドにはないが、今年（令和元年）の秋から国土交通省、経済産業省等を中心に、物流関係の事業者や主な荷主に対して、東京大会時の交通量削減に向けた具体的な対応を働きかけていくこととしている。宅配便の事業者は大手3社で9割以上のシェアがあるため、働きかけの効果は大きいと考えている。

さらに、国として、政府広報等の様々な手段を通じて、TDM、TSM (Traffic System management : 交通システムマネジメント) への協力を国民に呼びかけていく。あらゆる対策がしっかりと講じられるよう国としても全力を尽くして、東京大会の成功につなげてまいりたい。