# 東京2020大会に向けた取組状況について

資料7

サイバーセキュリティ基本法に基づく「サイバーセキュリティ戦略」に基づき、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とした**リスクマネジメントの促進**や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの運用等、**対処態勢の整備**を推進中。これらの仕組み、運用経験及びノウハウは、東京大会のみならず、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。

さらに、新型コロナウイルスの感染拡大及び大会の延期に伴い生じる環境変化や新たな事象・リスク等を踏まえ、**必要な見直しを実施**。

## リスクマネジメントの促進

○ **取組状況**

手順書を作成するとともに、東京大会において開催・運営に影響を与える重要サービス事業者等を選定し、リスクの低減と最新のリスクへの対応のため、2016年度から**リスクアセスメント**の実施を依頼。実施結果について横断的に分析し各事業者等にフィードバック。2019年９月から12月末にかけて第5回目の取組を実施。

また、競技会場に提供されるサービスの重要度に応じて対象事業者等を選定の上、サイバーセキュリティ対策の実施状況をNISCが検証する**横断的リスク評価**を2020年３月末までに計３回実施。2019年度においては、第2回目及び第3回目を実施。

○ **今後の取組**

**リスクアセスメントの取組**については、2021年３月末までに第６回目の取組を実施し、引き続き、重要サービス事業者等のリスクアセスメントにおいて、情報資産、リスクの洗い出しの網羅性及び要対応リスクに対する対策の網羅的な検討を促進するとともに、**環境変化を踏まえたリスクの見直し**、残存リスクが顕在化した場合の対応体制の強化を促進。

**横断的リスク評価の取組**については、第２回目及び第３回目の取組の対象であった重要サービス事業者等（会場(レガシー部分)を含む。）及び東京大会組織委員会に対するフォローアップを実施するとともに、**病院分野及び会場の変更がある場合には新規会場を対象として検証を実施**。

## 対処態勢の整備（サイバーセキュリティ対処調整センターの運用等）

○ **取組状況**

情報共有システムを構築し、2019年４月に設置した**サイバーセキュリティ対処調整センター**から**情報共有システム**を使用した恒常的な関係組織・機関への迅速な情報提供を実施するとともに　情報共有及びインシデント発生時の対処に係る**訓練・演習**を重ねている。情報セキュリティ関係機関等の協力により観測活動を実施するとともに、サイバー脅威情報の提供について５社から協力を受けている。

また、2019年度は、大会までの大規模イベント（G20大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において運用を実施し多くの教訓を得た。その結果を踏まえ、情報共有及びインシデント発生時の態勢について関係府省庁、大会組織委員会、東京都等と協議して決定した**対応手順等**について改善を実施した。

○ **今後の取組**

**新型コロナウイルスの感染拡大に伴う情勢の変化(テレワークの普及・大会運営の変更等)**及び**大会が１年延期となったことで新たに発生・判明する事象等**を踏まえた関係組織・機関への**情報提供**の継続と**訓練・演習**の積み重ねにより、大会関係組織間の緊密な連絡調整を図るための態勢を強化するとともにインシデント対処能力を向上する。

これにより、大会に向けて万全の対処態勢を目指す。

# リスクマネジメントの促進のための取組の概要

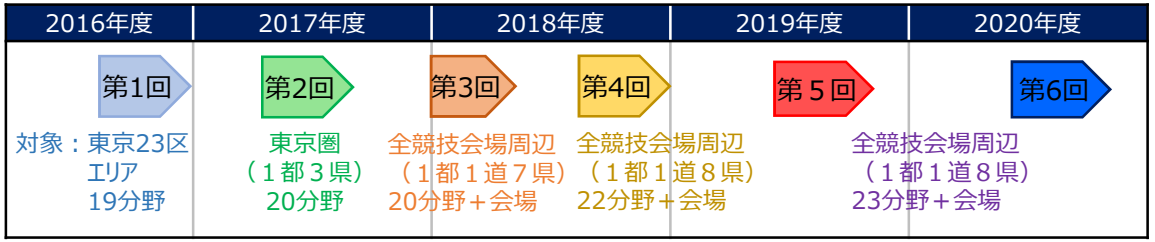
## ●リスクアセスメントの取組

サイバー攻撃等による東京2020大会の準備・運営への影響の未然防止や軽減等のため、大会を支える周辺サービスを提供する事業者等によるリスクマネジメントの強化を通じ、想定されるサイバーセキュリティ上のリスクへの対策を促進。
第６回の取組では、大会延期や新型コロナウイルスの感染拡大に伴う環境変化を踏まえたリスクの見直しに加え、要対応リスクに対する対策の網羅的な検討及び残留リスクが顕在化した場合の対応体制の強化を促進していく。

○ リスクマネジメントの促進のため、サイバーセキュリティリスクを特定・分析・評価する手順をNISCで作成

○ 大会の準備・運営に影響に与えうる重要サービス分野から、
重要サービス事業者等を関連する所管省庁と調整の上で選定

重要サービス分野 ＋ 会場（競技会場及び非競技会場）
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、会場



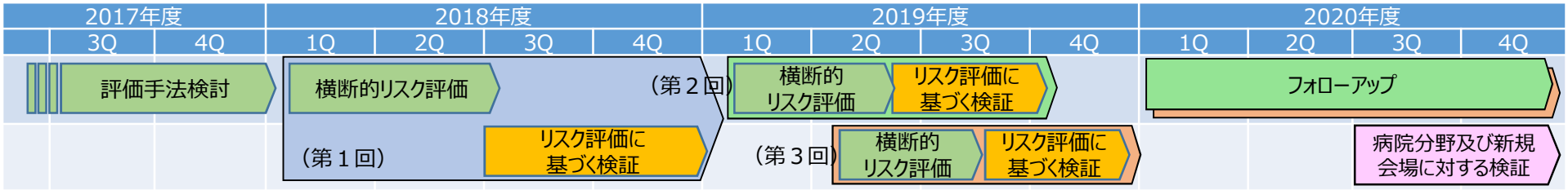

○ NISCが想定する『「事業・重要サービス・経営資源（情報資産）」のモデルケース（重要サービス分野ごと）』、『業務の阻害につながる事象の結果、結果を生じ得る事象（脅威）及びリスク源』を作成、各事業者等へ経営資源、リスク源等の洗い出しの漏れの可能性をフィードバックすることによって、より網羅的なリスクアセスメントの実施を促進

○ サイバーセキュリティ対策の運用状況について、NISCからフィードバックを実施し、必要に応じて助言を実施

## ●横断的リスク評価の取組

重要サービス事業者等において想定されるサイバーセキュリティリスクに基づき、サイバーセキュリティ対策の実施状況をNISCが検証する。
これにより、大会の成功にとって重要な機能が継続して提供されることを確認するとともに、不備があった場合は、重要サービス事業者等へフィードバックすることにより、当該重要な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。

○ 大会に関わるリスクが顕在化するシナリオをリスクシナリオとして策定・活用し、重要サービス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
○ 第１回の取組においては、電力、通信、水道、鉄道、放送等５者程度を対象に実地検証。全重要サービス分野から20者程度を対象に書面検証
○ 第２回及び第３回の取組においては、重要サービス事業者等（会場（レガシー部分）を含む。）を対象に検証（実地又は書面）
なお、会場のオーバーレイ部分の対策の整備状況及び監督状況については、組織委を対象に実地検証
○ 2020年度においては、病院分野及び会場の変更がある場合には新規会場を対象に検証（実地又は書面）



# 対処態勢の整備（サイバーセキュリティ対処調整センターの運用等）の活動予定

2021年度の東京2020大会に向けて、「体制運営活動」「対応手順等の改善」「情報共有・インシデント対処」「情報共有プラットフォームの提供」を継続及び改善し、大会の対処態勢を万全なものとしていく。