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

資料6

2020年東京オリンピック・パラリンピック競技大会（以降、大会）を成功へと導くためには、大会の開催・運営を支える重要サービスにおけるサイバーセキュリティを確保し、安定したサービスを供給することが不可欠との認識の下、関係機関と連携し取組を検討。

【検討体制】

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
（本部長：安倍総理）

2020年オリンピック・パラリンピック東京大会関係府省庁連絡会議
（議長：杉田副長官）

セキュリティ幹事会

座長 － 内閣危機管理監
座長代理 － 内閣官房オリパラ事務局長、内閣官房副長官補（内政）、内閣官房副長官補（事態対処・危機管理）、警察庁次長
構成員 － 関係省庁の局長級
オブザーバー － 東京都、組織委、警視庁、東京消防庁の幹部
事務局 － 警察庁、総務省、外務省、経産省、国交省、防衛省の協力を得て内閣官房（内政・事態・NISC）において処理

テロ対策ＷＴ

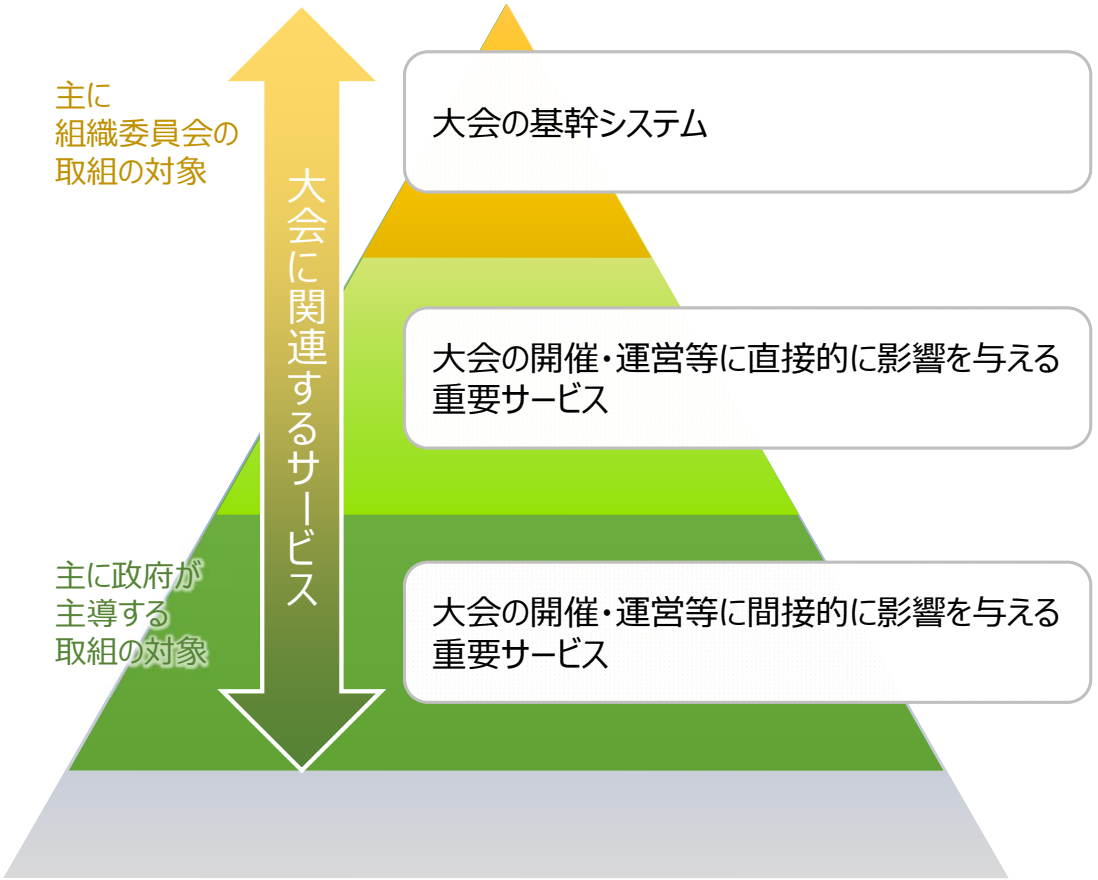
座長 － 内閣審議官（事態・内政）
座長代理 － 内閣審議官（オリパラ事務局）警察庁審議官
構成員 － 関係省庁の課長級
オブザーバー － 関係機関の幹部
事務局 － 警察庁、国交省、防衛省の協力を得て内閣官房（事態・内政）において処理

サイバーセキュリティＷＴ

座長 － 内閣審議官（NISC副センター長）
座長代理 － 内閣審議官（オリパラ事務局）警察庁審議官
構成員 － 関係省庁の課長級
オブザーバー － 関係機関の幹部
事務局 － 警察庁、総務省、外務省、経産省、防衛省の協力を得て内閣官房（NISC）において処理

2020年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ体制に関する検討会

【大会の開催・運営を支える重要サービスのイメージ】

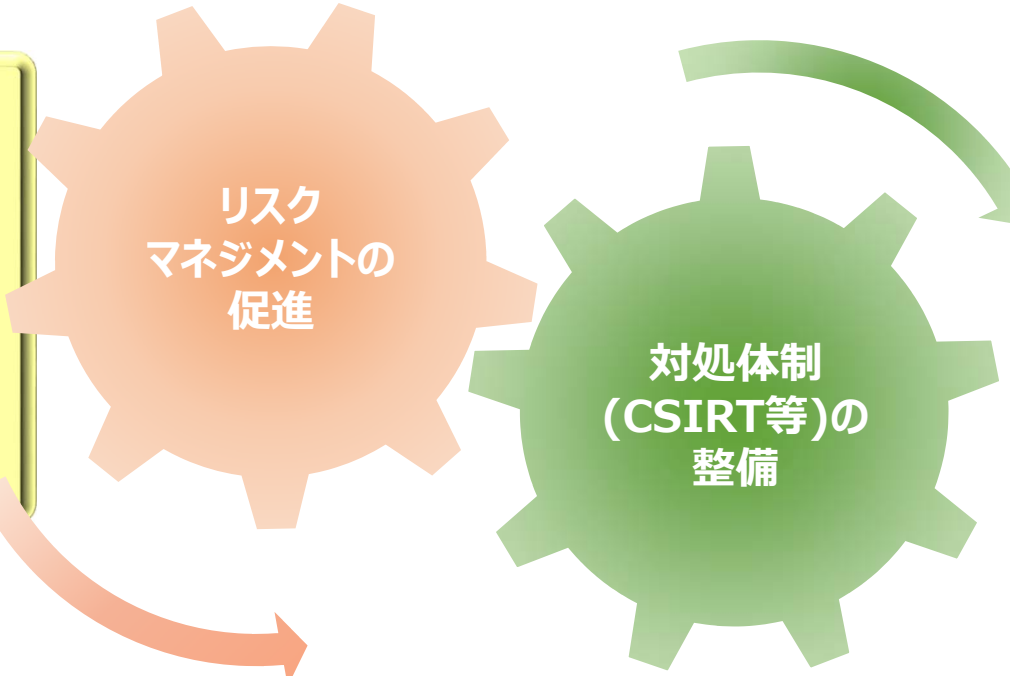


主な取組

大会の開催・運営に影響を与えうる重要サービスにおけるサイバーセキュリティ確保のため、以下の2つを柱とし取組を推進。

○ 大会の開催・運営に影響を与えうる重要サービスを提供する事業者を選定。

○ サイバーセキュリティ上のリスクを特定・分析・評価するための手順をとりまとめ、選定された事業者を中心としてリスクマネジメントの実施を促進。



○ 関係組織に対して対処のための的確な情報共有を担う中核的組織としてのオリンピック・パラリンピックCSIRTを整備。

○ 整備にあたっては、2020年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ体制に関する体制検討会を通じ、政府/関連組織の役割を整理し、具体的な体制を検討。

各取組を並行して実施し、補完し合いながら推進

※平成27年11月27日閣議決定

【参考】「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の準備及び運営に関する施策の推進を図るための基本方針」※抜粋

3．大会の円滑な準備及び運営

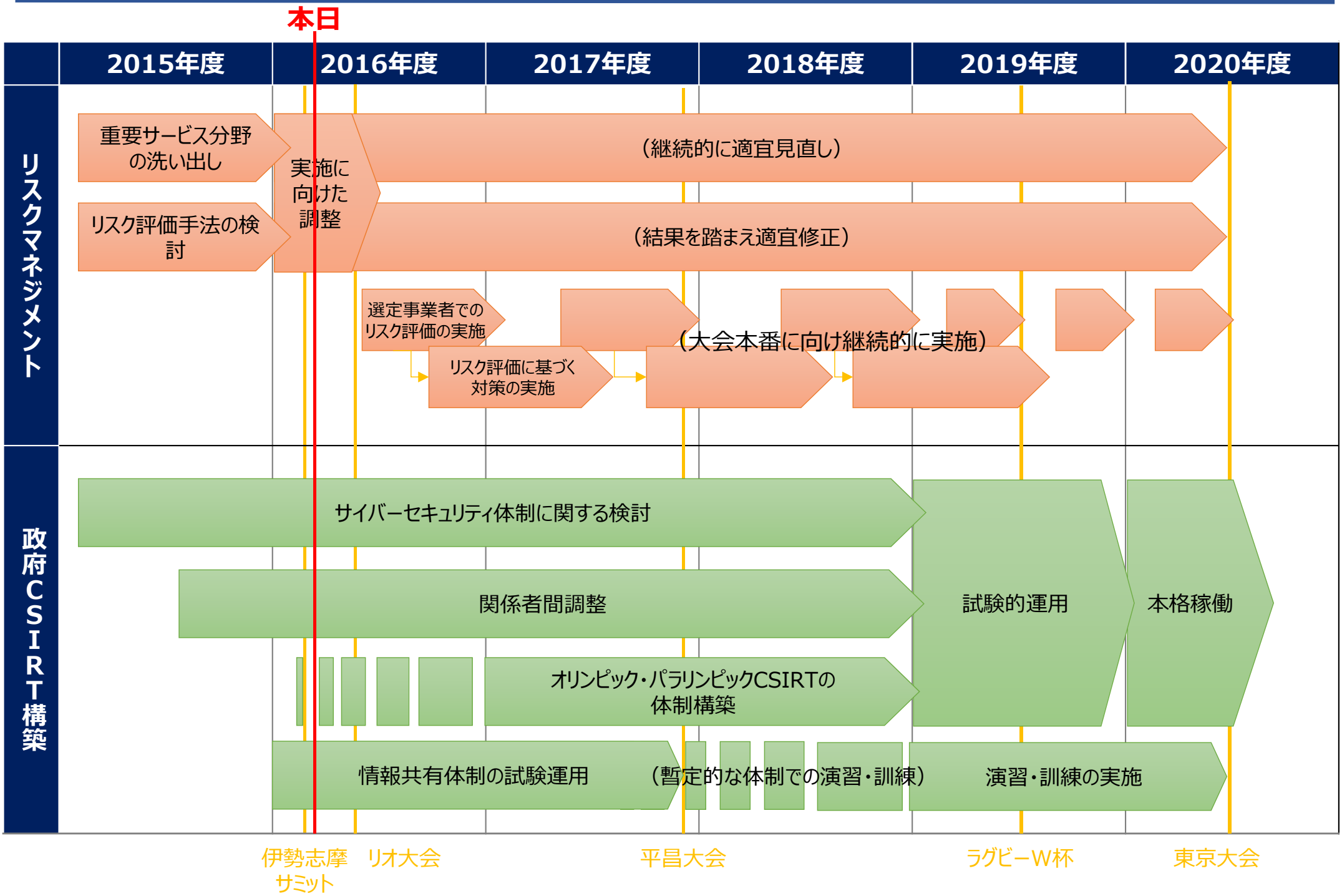
① セキュリティの万全と安全安心の確保

：

サイバーセキュリティ対策については、国全体としてのサイバーセキュリティ戦略を着実に実施するほか、当該戦略に基づき、大会に係るサイバーセキュリティ上のリスクを明確にした上で、各関係主体で必要な対策を施していくとともに、脅威・インシデント情報の共有等を担う中核的組織としてのオリンピック・パラリンピックCSIRT（Computer Security Incident Response Team）の構築、運用を図る。

：

スケジュール（全体想定）


本日
2015年度
2016年度
2017年度
2018年度
2019年度
2020年度
リスクマネジメント
重要サービス分野の洗い出し
リスク評価手法の検討
実施に向けた調整
（継続的に適宜見直し）
（結果を踏まえ適宜修正）
選定事業者でのリスク評価の実施
リスク評価に基づく対策の実施
（大会本番に向け継続的に実施）
政府CSIRT構築
サイバーセキュリティ体制に関する検討
関係者間調整
試験的運用
本格稼働
オリンピック・パラリンピックCSIRTの体制構築
情報共有体制の試験運用
（暫定的な体制での演習・訓練）
演習・訓練の実施
伊勢志摩サミット
リオ大会
平昌大会
ラグビーW杯
東京大会

【参考】関連取組の全体像

リスクマネジメント

■大会運営に影響を与える重要サービス事業者の選定。
■サイバーセキュリティに係るリスク評価手順の策定。
■上記手順に基づくリスクマネジメントの実施。（複数回）。

対処体制（政府CSIRT）

■NISCを中心に、政府機関、重要インフラ事業者、セキュリティ関連組織等の情報共有・対処体制の確立。
■ラグビーワールドカップ時（１９年夏）に稼働。

連携

組織委員会CSIRT（CIRT※2 2020）

■大会の基幹システムを中心とするサイバーセキュリティ対策の推進。

演習・訓練

■組織委と連携しつつ、上記関係者による演習・訓練を実施（複数回）。

連携

主要国

■二国間サイバー協議等を通じた情報共有体制等の確立。
■IWWN※3等の国際情報共有体制も活用。
■G7各国との密接な連携の推進。

一体的に推進

重要インフラ防御能力の強化

■ロードマップ※1（１６年３月）に従った強化対策の検討・実施。
■具体的には、①サイバー攻撃に対する体制強化、②重要インフラに係る防護範囲の見直し、③多様な関係者間の連携強化を中心に検討。
■本年秋頃に行動計画見直し骨子（案）、年内に見直し（案）を策定・公表。年度内に結論。

人材確保・育成

■人材育成総合強化方針（１６年３月）に基づく人材育成の推進。
■特に、教育の充実、演習環境の整備、能力の可視化（資格試験）等を推進。

研究開発

■戦略的イノベーション創造プログラム（SIP)における研究開発“重要インフラ等におけるサイバーセキュリティの確保”（１５～１９年度）
■本プログラムにおいて「サプライチェーンリスク対策技術（動作時完全性確認技術）」、「情報共有プラットフォーム構築・運用支援技術」、「セキュリティ運用の人材育成」等を実施。

※1 重要インフラの情報セキュリティ対策に係る第3次行動計画の見直しに向けたロードマップ（16年3月）

※2 Cyber Incident Response Team。
※3 International Watch and Warning Network。サイバー空間の脆弱性、脅威、攻撃に対応する国際的取組の促進を目的として、先進15ヶ国の政府機関が参加する会合。