

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構築等、**対処態勢の整備**を推進中。

## 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、**リスクアセスメント**の実施を依頼。2016年度から2020年6月末まで計6回を予定。第3回目においては、対象の事業者を全国へ拡大、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。

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**を実施。2020年3月末までに計3回を予定。第1回目においては、電力、通信、水道、鉄道、放送等から5者を対象に実地検証、全重要サービス事業者等から20者を対象に書面検証を実施。

### ○今後の取組

**リスクアセスメントの取組**については、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、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、引き続き、重要サービス事業者等（競技会場(レガシー部分)を含む。）を対象として検証を実施するとともに、競技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東京大会組織委員会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構築等）

### ○取組状況

情報共有・事案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、**運用方針等を決定**した。また、サイバー脅威情報の提供について4社から協力を受けることを決定するとともに、大会組織委員会、東京都等を交えた机上演習を実施した。

**情報共有システム**の構築が完了し、2019年4月に**サイバーセキュリティ対処調整センター**を設置した。

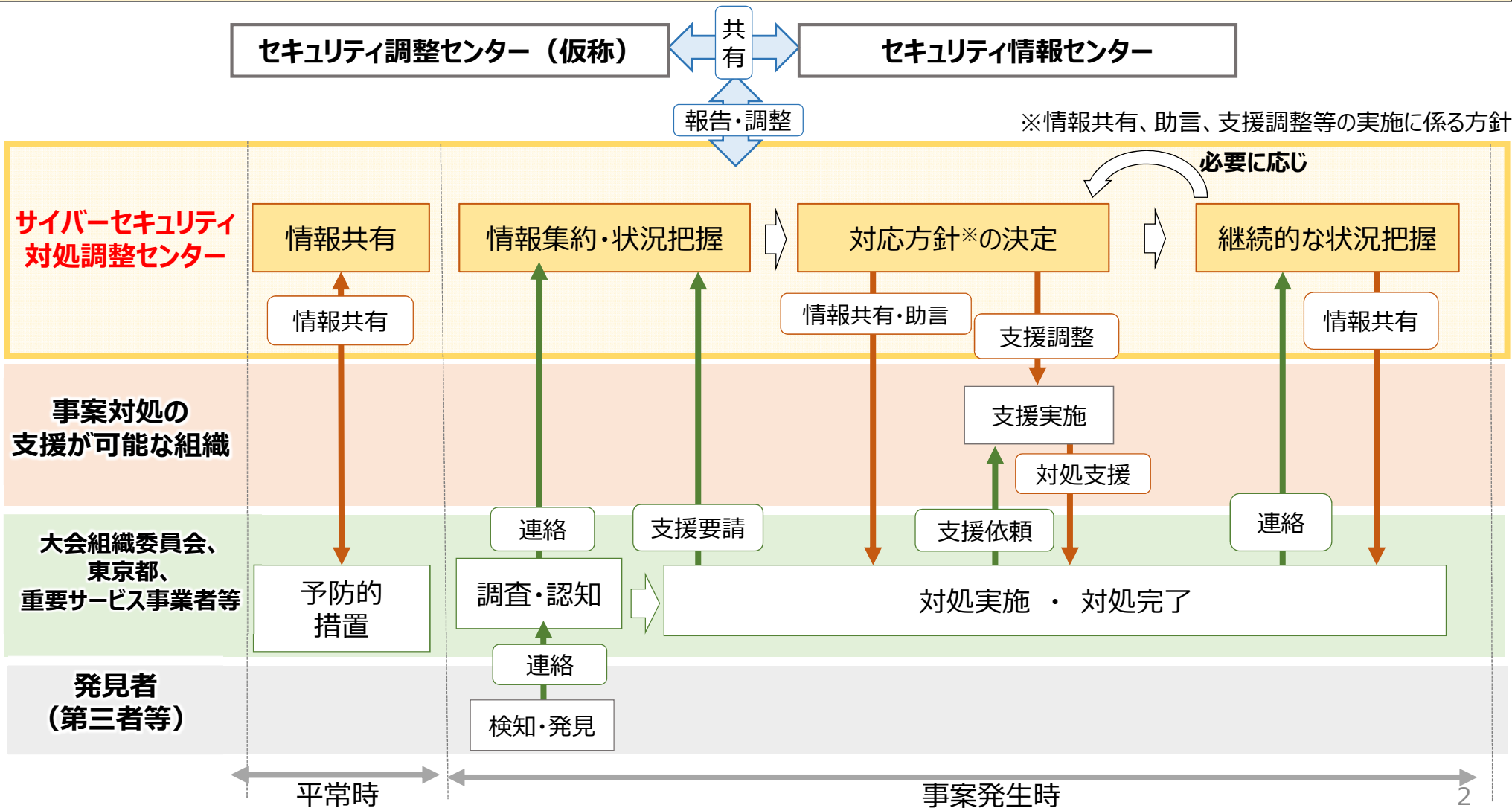
### ○今後の取組

サイバーセキュリティ対処調整センターは、大会関係組織と情報共有システムを介した**情報共有**の促進及び**インシデント発生時の対処支援調整**を実施。また、重要サービス事業者等も参加する情報共有及びインシデント発生時の対処支援調整等の**訓練・演習**を実施し、大会関係組織間で緊密に連絡調整を図るための態勢を整備。さらに、大会までの大規模イベント（G20大阪サミット、ラグビーワールドカップ等）において情報共有及びインシデント発生時の対処に係る試験運用を実施。

これらの取組を通じて、大会に向けて万全の対処態勢の整備を目指す。

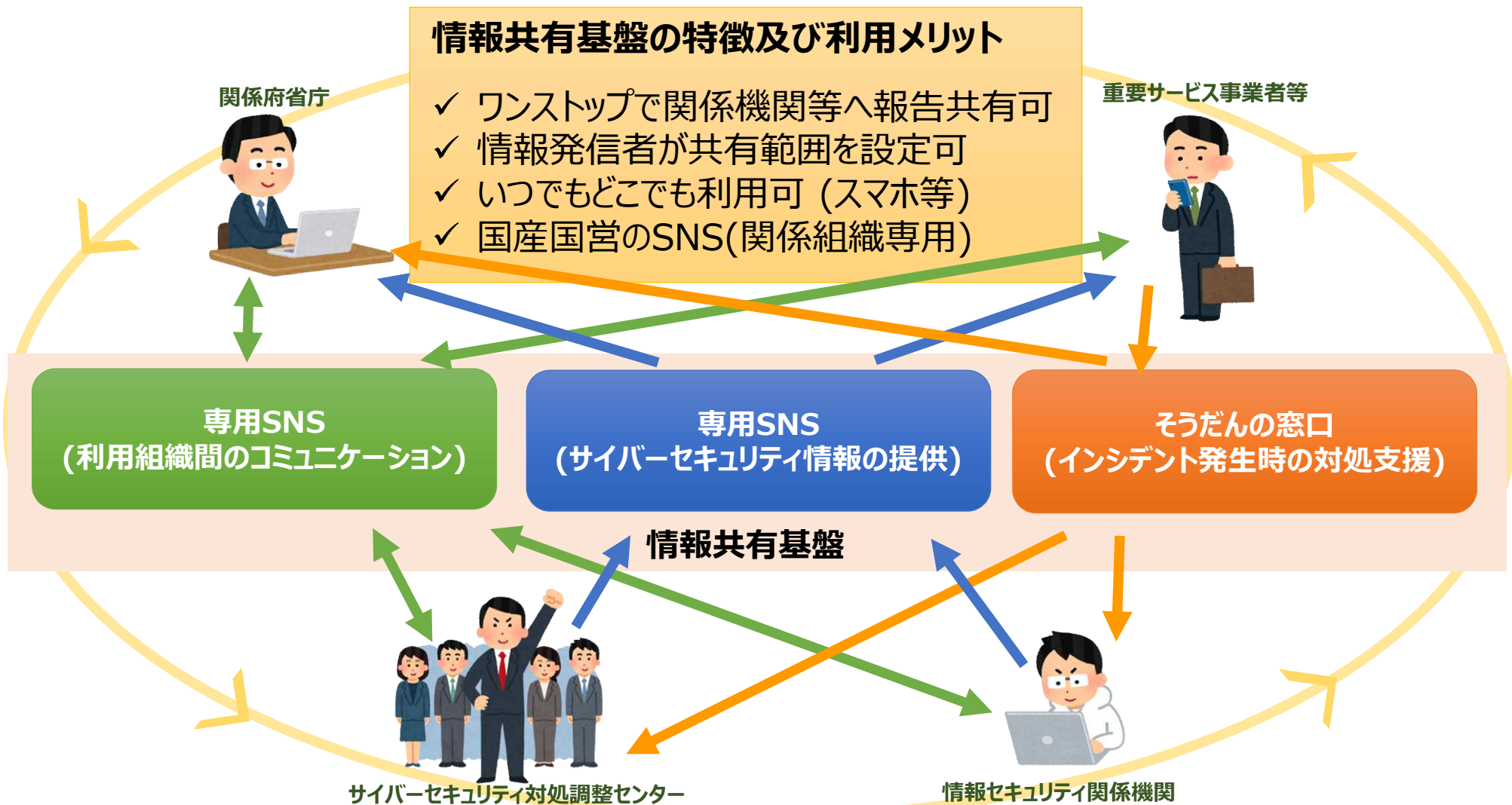
# (参考) サイバーセキュリティ対処調整センターについて

- 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、これら情報を大会組織委員会を始めとした関係機関等に提供、必要があるときには関係機関等のインシデント対処に対する**対処支援調整**を実施



# (参考) 情報共有基盤について

- 2019年4月より、対処調整センターは利用組織(※)に情報共有基盤を介してサービスを提供する。
- 情報共有基盤を活用して、連絡体制確立のための演習・訓練を開催予定。



※大会組織委員会、会場管理者、東京都、会場のある地方公共団体、重要サービス事業者等、スポーツ関連団体、情報セキュリティ関係機関、政府機関、警察等を想定している。

# (参考) 対処調整センターの今後の活動計画について

対処調整センターは、2020東京大会に向けて、下図のとおり「情報共有及びインシデント対処」「演習訓練」「対応手順等の改善」の活動を行い、大会の対処態勢を万全なものとしていく。

