これまでの会議で示された活用方策（中間整理の概要）

資料３

大会後のNISCにおける取組の活用方策を以下のとおり示す。

大会に向けた取組を今後活用するに当たっての基本的な考え方

社会経済を支えるサービスへの高度な攻撃が急増している背景を踏まえ、**大会に向けて推進した取組を十分に活用しながら、社会経済を支えるサービスの維持・運用の確保に向けて、国として取り組むべき施策を力強く推進。**

【構成員からの意見・指摘】
- 持続的なサイバーセキュリティ対策としての活用
- 様々な機関等が推進する取組、整備する連絡系統等を考慮した上での合理的な運用
- 公益性の観点に立った取組の推進
- サイバーセキュリティ対処調整センター等としての能力の維持
- 大会後の大規模国際イベントにおける取組の活用

各取組の大会後の活用方策等

課題認識等

サイバーセキュリティの確保に向けて、**各組織における自律的な取組のほか、多様な組織の緊密連携が不可欠**

- 各組織で講ずるべきサイバーセキュリティ対策に求められる水準が高度化、複雑化
  → 政府から各組織に対して、**自律的なサイバーセキュリティ対策（インシデント対処を含む。）を講じることができるよう必要な支援を積極的に実施**
- デジタル化の更なる進展に向けて、各組織におけるサイバーセキュリティ対策はより一層重要となるものの、個々の取組のみでの対応には限界
  → ISAC、ISAO等のコミュニティにおける各組織間の強固な連携等のように、**相互の支援・連携が強化されるよう政府において必要な支援を実施**

大会後に対象とする領域等

持続的なサイバーセキュリティ対策

社会全体のサイバーセキュリティの確保に向け、重点的に対策を講じてきた重要インフラ事業者等に加え、**社会経済を支えるサービスを提供する組織を対象**に、

- 事業所管省庁等と連携して、対処体制に参加する事業分野、事業者等の範囲を調整し、必要な対策を推進（**各組織で自律的な取組が可能となるような支援**）
- また、事業所管省庁等と連携して、 優先度が高まっている分野におけるコミュニティの構築・運営への支援を推進（**各組織間の支援連携が機能するような支援**）

大規模国際イベントにおけるサイバーセキュリティ対策

大規模国際イベントの関係組織間で、サイバーセキュリティを確保するための体制を構築し、必要な対策を推進