我が国のサイバーセキュリティ推進体制の機能強化のポイント

総務省 MIC Ministry of Internal Affairs and Communications

参考1

総務省の取組

○ 2020年の東京五輪開催を見据え、省内で**東京五輪推進本部を開催**（サイバーセキュリティ対策も含む）。

○ サイバーセキュリティの推進体制の強化にあたり、具体的なポイントは以下の3つ。

① 先端的・実用的な**研究開発の強化**

② サイバー攻撃に対する**組織的な実践演習**や**個人の自発的な対応**の推進

③ **多国間・二国間の連携の強化**

「サイバーセキュリティ立国」の実現には、構想だけではなく、
具体的な戦略の実践と**スピード**が必要不可欠。

政府全体の取組

○ **情報セキュリティ政策会議及び内閣官房情報セキュリティセンター（NISC）を法的に位置付け**、司令塔機能を強化

○ **各省が連携し、統一的な対策**を実施

総合的な情報セキュリティ対策の推進

「スマート・ジャパンICT戦略」骨子（5/13発表）より抜粋

○ 2020年東京五輪の安心・安全な開催に向けて、多角的な情報セキュリティプロジェクトを実施するとともに、得られた成果を国際的に展開することで「サイバーセキュリティ立国」の実現に貢献。

2020年東京五輪に向けた安全な情報通信ネットワークの確保

◆ 2012年ロンドン五輪では、公式サイトに2億回を超えるサイバー攻撃が発生するなど情報セキュリティの確保は最重要課題の一つ。

◆ 安心・安全な2020年東京五輪の開催に向けて、IoT（Internet of Things）の広がりなどICT環境の変化を見据え、**サイバー攻撃対応体制の強化**や**認証連携の実現、機器間通信（M2M）、ITS等新たな情報セキュリティ上の課題の解決**を促進。

国内のサイバー攻撃への防御能力の向上

◆ 官公庁・大企業向けに**実践的なサイバー演習「CYDER」**を2013年から開始。従来の手口だけではなく、最新の攻撃の特徴を踏まえた模擬攻撃を行い、より高い実践性を確保。

※CYDER（CYber Defense Exercise with Recurrence）

◆ 一般利用者向けに**マルウェア配布サイト対策「ACTIVE」**を2013年から開始。利用者の拡大、海外展開を推進。

※ACTIVE（Advanced Cyber Threats response InitiatiVE）

「サイバーセキュリティ立国」の実現

国際連携の更なる展開

日・ASEAN

◆ 2013年9月に行われた「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」を踏まえ、次の取組を推進。

○ **JASPER（Japan-ASEAN Security PartnERship）**※1

・ シンガポール、フィリピン等7カ国が参加中。今後も未参加国への呼びかけを実施。

○ **日・ASEANサイバーセキュリティ人材育成イニシアティブ**※2

・ 相手国のニーズを踏まえた研修メニューを作成し、JICA等と連携して研修開始。

日・米

◆ 2012年からサイバー攻撃に関する情報共有について合意。リアルタイムの共有に発展。

日・EU

◆ ベストプラクティスの共有など連携を強化。

※1 （独）情報通信研究機構のnicterの技術を基礎とした国内プロジェクト（PRACTICE及びDAEDALUS）から成る、日・ASEAN間の技術協力プロジェクト

※2 政府職員を対象に、5年間で1,000人という大規模な人材育成を実施。