

- 2020年東京オリンピック・パラリンピック競技大会を3年半後に控え、IoT機器・サービスが急速に普及する中、IoT時代に対応したサイバーセキュリティを早急に確立すべく、2017年に、総務省は関係府省・団体・企業等との緊密な連携の下、下記のサイバーセキュリティ施策を実施

1. サイバーセキュリティタスクフォースの開催

- ✓ IoT/AI時代のサイバーセキュリティに関する基盤・制度、人材育成、国際連携のあり方等、包括的な政策推進についてICT関係部署の司令塔の役割を担うサイバーセキュリティタスクフォースを開催、必要な施策を検討・実施

2. IoT機器セキュリティ対策の実施

- ✓ IoTによる大規模サイバー攻撃が発生する中、脆弱性のあるIoT機器を把握し、その機器の管理者に注意喚起を行うとともに、IoTセキュアゲートウェイの実証を行うなど、今後の抜本的なIoT機器セキュリティ対策を確立

3. セキュリティ人材育成のスピードアップ

- ✓ 2016年度内に、2020年オリパラ東京大会に向けた演習(「サイバーコロッセオ」)及びセキュリティ競技大会(「サイバーコロッセオ×SECCON」)を実施するとともに、引き続きサイバー防御演習を実施し、セキュリティ人材を発掘・育成
- ✓ ナショナルサイバートレーニングセンター(仮称)をNICTに組織し、サイバー防御演習を47都道府県に拡大、東京大会に向けた演習の強化、若手セキュリティエンジニアの育成(新規)を実施(2017年度政府予算案)

4. 総務大臣表彰制度の創設

- ✓ 企業・団体等サイバーセキュリティ対応の最前線(現場)において優れた功績を挙げている個人・団体を顕彰する総務大臣表彰制度を創設

5. 国際連携の推進

- ✓ ASEANにおけるサイバー防御演習の拡大(現在2ヶ国)、セキュリティコンテストの実施に向けて、関係各国との連携体制を強化し、サイバーセキュリティ能力の向上及びセキュリティ人材の国際交流に貢献