資料 20－２

我が国のサイバーセキュリティ強化に向け早期に取り組むべき事項［緊急提言］の概要（案）

（１）IoT 機器のセキュリティ対策の拡充

- 脆弱な状態にあるIoT機器について注意喚起方法の一層の改善を図ることが必要。
- 国内の重要施設に設置されているIoT機器のうち、その管理画面の表示内容に問題のある機器の所有者・運用者等に対し、新たに注意喚起を実施することが必要。

（２）地方公共団体向け実践的サイバー防御演習（CYDER）の繰り上げ実施等

- 実践的サイバー防御演習（CYDER）について、未受講の地方公共団体を中心とした集中的な受講機会を大会前に設けるとともに、オンライン受講を早期に開始することが必要。

（３）サイバーセキュリティに関する情報共有体制の強化

- サイバー攻撃については、原因究明に一定の期間を要する場合もあるが、個人情報などの流出が疑われる時点で、影響を受ける主体との関係なども踏まえつつ、速やかに情報の公表を検討することが望ましい。また、類似の被害の拡大を防ぐ観点から、インシデントに関する情報の共有を速やかに行うことが求められる。
- 通信業界において先行的に始まったISACの知見やノウハウの展開を通じた他の重要インフラ分野等におけるISACの立ち上げを促進するとともに、国際間を含むISAC間の連携を促進することが必要。

（４）公衆無線 LAN のセキュリティ対策

- 2020年東京大会に向けて、公衆無線LANサービスの利用者及び提供者に対し、公衆無線LANのセキュリティ対策の状況や自ら講じるべきセキュリティ対策の周知を強化するため、ガイドラインを年度内に改定し、ホテル、病院、学校等への周知を強化することが必要。

（５）制度的枠組みの改善

- サイバーセキュリティ対策や事故報告についての法令への位置づけ、分野ごとの所管省庁や業界団体によるガイドラインや基準の策定を通じてサイバーセキュリティ対策を効果的に進めていく取組について、あらゆる機会を通じて周知し、対応の強化を呼びかけていくことが必要。
- 放送分野において、放送設備のサイバーセキュリティ確保に関する省令改正を速や

かに実施することが必要。

- 地方公共団体分野について、各地方公共団体における情報セキュリティ対策及び緊急時連絡体制の確保等の徹底を図ることが必要。また、昨今の地方公共団体における重大インシデントを踏まえ、「地方公共団体における情報セキュリティポリシーに関するガイドライン」に反映することも念頭に対応策の検討等を行い、地方公共団体へ通知することが必要。