サイバーセキュリティ政策推進に関する提言 概要

（平成27年5月22日 総務省 情報セキュリティ アドバイザリーボード）

別紙２

１．検討の背景

IoT（Internet of Things）社会の本格的到来によりサイバー空間と物理空間との融合が進展。各分野で新たな価値が生み出されイノベーションが創発する一方、サイバー攻撃の脅威が大幅に増大。

2014年11月にサイバーセキュリティ基本法が成立。2015年1月に全面施行され、同年6月を目途に我が国の新たなサイバーセキュリティ戦略が策定予定。

2020年にはオリンピック・パラリンピック東京大会を開催。安全な大会開催も見据えたサイバーセキュリティの確立が急務。

２．基本理念・基本原則

【基本理念】 情報の自由な流通の確保と、それによる社会経済発展の主導

【基本原則】 サイバー空間の基盤である安全な情報通信ネットワーク環境の確立
ICTの著しい環境変化への柔軟かつダイナミックな対応
あらゆる関係主体の自律した取組と相互連携の促進
国際的な協調・協力関係の発展

３．守るべき対象

ICTインフラ防護等の観点から、「守るべき対象」とその懸念を以下の４項目に整理。

- ネットワーク基盤を守る ［脆弱なネットワーク機器の存置、IoT機器へのセキュリティ技術の未実装 等の懸念］
- 組織を守る ［標的型攻撃の巧妙化・複雑化、情報共有体制の未成熟、人材不足 等の懸念］
- 個人を守る ［マルウェアの高度化・拡大、リテラシーの不足 等の懸念］
- 我が国のネットワーク環境を守るとともに、国際社会に貢献する ［国境を越えたサイバー攻撃 等の懸念］

４．講ずべき方策

「守るべき対象」を防護しサイバーセキュリティを確立するため、以下の６つの方策を提言。

（１）通信ネットワーク基盤の安全の確保
新たなDDoS攻撃であるリフレクション攻撃に対し、攻撃の踏み台等となるブロードバンドルータ等の利用者を特定し注意喚起するための制度的検討・実証を実施 等 （総務省で実施中のACTIVE 等の取組を発展）

（２）IoT社会におけるサイバーセキュリティ上の脅威への対応
IoT機器等に関する脅威分析・リスク評価を実施し、その特徴を踏まえたセキュリティ技術の開発や安全な機器運用のためのガイドライン作成を実施 等

（３）情報共有体制の強化
ICT関連事業者間等における情報共有・連携の体制を一層強化。また、情報共有・連携の基盤となるプラットフォームを構築 等 （Telecom-ISAC Japanにおける情報共有 等の体制・取組を拡充）

（４）人材育成・周知啓発の推進
サイバー攻撃防御のための共通的な演習基盤を構築・活用して実践的なセキュリティ人材を育成。また、初等・中等教育段階からのセキュリティ教育や、ハイブリッド人材の育成を推進 等 （総務省で実施中のCYDER 等の取組を発展）

（５）研究開発の推進
攻撃観測技術やAI、ビッグデータ等の活用により、サイバー攻撃に対して先手を打った「プロアクティブな」対応を可能とする技術を開発 等 （NICTで実施中の研究開発 等を一層強化）

（６）国際連携の更なる展開
先進国との先導的な共同研究開発プロジェクトを実施。また、ASEAN等重点地域において、現地ニーズを踏まえた能力構築を支援 等

５．2020年オリンピック・パラリンピック東京大会に向けた取組

【基本的考え方】 東京大会は「おもてなし」と「セキュリティ」の両立が成功の鍵。東京大会を共通の目標として、国を挙げてサイバーセキュリティ対策を推進するとともに、構築したセキュリティ基盤を2020年以降も資産（レガシー）として持続・発展させ、我が国がIoT社会におけるセキュリティで世界をリードしていくことが必要。

⇩

【今後求められる取組】 IoT社会に対応した脅威分析、情報共有体制・仕組みの構築、実際の大会を想定した演習の実施、期間や地域を限定した特別な取組の検討 等