「対応の方向性（案）」概要－①

資料2－1

1　検討の背景

インターネットの通信障害等が頻発しており、インターネットの円滑な利用環境の確保が極めて重要な課題。

【要因】
- インターネットが社会基盤となる一方、DDoS攻撃等が増加
- IoT機器の爆発的増加と、セキュリティの脆弱なIoT機器の悪用リスクの高まり
- 2020年のオリンピック・パラリンピック開催に伴うDDoS攻撃等の脅威の増大

⇒　インターネットの障害防止に向けた抜本的な対策の実施が急務。

2　基本的な考え方

通信ネットワークに関わる者全体が連携することが肝要。

関係者が連携してインターネットの障害の防止や予防を図るためには以下の対応が必要。

【対応の方向性】①電気通信事業者によるDDoS攻撃等の事前予防
②情報共有と相互連携
③IoT機器等の端末設備のセキュリティ対策

推進の際は通信の秘密やプライバシー等に十分な配慮が必要。また、国民のセキュリティ意識の醸成も必要。

3　電気通信事業者によるDDoS攻撃等に対する防止措置の推進

【対策】
- 攻撃の事前予防のための、マルウェア感染の可能性が高い端末利用者に対する注意喚起
- 指令サーバ※のブラックリスト等を用いたマルウェア感染が疑われる端末等の検知
- マルウェア感染者等の通信を利用した未知の指令サーバの検知

※　マルウェア感染端末にサイバー攻撃を命令する機器で、このような機器と通信する端末はマルウェア感染が疑われる。

【課題と今後の対応】　通信の秘密等との観点から、具体的な実施方法や留意すべき事項等について精査。

「対応の方向性（案）」概要－②

4　情報共有、分析基盤の構築

【対策】　第三者機関を中心とした情報共有基盤を構築

∵　①IoT機器の増加に伴い個別の情報共有が困難となっているため、情報共有の結節点が必要

②情報を集約して集中的に分析、検証することで、対策の実効性向上が可能

【課題と今後の対応】

通信の秘密に該当する情報を関係者間で共有することから、実施に向けて具体的な体制等を検討し、裏付けとなる法制度を整備。

5　IoT機器を含む脆弱な端末設備のセキュリティ対策

【対策】　IoT機器等の端末設備において、基本的なセキュリティ対策を実施

【課題と今後の対応】

国際競争力確保等の観点も踏まえ、IoTサービスや機器の普及の阻害とならないよう、諸外国の検討状況等を踏まえた上で関係者から広く意見聴取し、検討。

6　大規模なインターネット障害発生時の対策

【対策】
- インターネットの経路情報の送受信を適切に制御する経路フィルターの設定を推奨
- インターネット障害に関する情報共有体制の整備

【課題と今後の対応】

ガイドライン等においてルータの設定につき規定するとともに、電気通信事業者から総務省への迅速な障害報告の在り方を含めた情報共有体制を検討。