「対応の方向性（案）」の概要と今後の取組の進め方

参考資料

1．電気通信事業者による攻撃通信の発生の防止

・マルウェア感染の疑われる利用者に対する注意喚起、指令サーバとの通信遮断、未知のマルウェア感染端末等を検知。

※ 事業者が、利用者の同意なく、注意喚起、検知等のために利用者の通信に係るIPアドレスやタイムスタンプ等を利用することは、通信の秘密の窃用に該当し得る。

→ 通信の秘密に配慮した実施方法等を整理し、民間のガイドラインに反映。

2．情報共有、分析基盤の構築

・1．の対策の実効性を高めるため、第三者機関が指令サーバ等に関する情報を集約し、分析・検証した上で電気通信事業者との間で情報共有。

※ 本取組においては、第三者機関が、通信の秘密を集約、分析・検証、共有することとなる。

→ 第三者機関が通信の秘密に該当する情報を扱うことから、裏付けとなる法制度を整備。

3．IoT機器を含む脆弱な端末設備への対策の検討

・DDoS攻撃等の発生源となりうる脆弱なIoT機器について、基本的なセキュリティ対策を実施。

※ 事業者のネットワークに接続される端末設備の技術基準には、現時点ではサイバー攻撃等によるインターネットの障害に関する規定はない。

→ ネットワークの安全・信頼性を確保するための端末のセキュリティ対策について、国際動向等を踏まえ、情報通信審議会で検討。

4．昨年8月に発生した大規模なインターネット障害の検証を踏まえた対策の検討

・事業者においてインターネットの経路情報を適切に制御する技術的対策を実施するとともに、事業者間でインターネット障害に関する情報を共有。

→ 情報通信ネットワーク安全・信頼性基準（ガイドライン）の改訂や、事業者から総務省へのインターネット障害の報告の在り方について検討。