資料36－3

IoT機器を含む脆弱な端末設備のセキュリティ対策について

―円滑なインターネット利用環境の確保に関する検討会「対応の方向性」より―

平成30年3月6日
事務局

IoT機器を含む脆弱な端末設備のセキュリティ対策について

○　総務省では、近年サイバー攻撃等によりインターネットに重大な支障が発生していることを踏まえ、電気通信事業におけるこれらの障害への対処を促進することを目的として、「円滑なインターネット利用環境の確保に関する検討会」を開催し、本年２月に「対応の方向性」をとりまとめた。

○　「対応の方向性」において、攻撃の踏み台とされる脆弱なIoT 機器等がインターネットに接続されている限り、DDoS 攻撃等の発生源となるおそれがあることから、インターネットの障害の発生を防止するためには、ネットワークに接続されるIoT 機器を含む端末設備についても基本的なセキュリティ対策を実施することが不可欠とされた。

端末設備におけるセキュリティ対策の必要性

（IoT機器が乗っ取られ、電気通信事業に影響が及んだ事例）

➢　米国の事例（マルウェア「Mirai」）

○　60 組の簡単なID・パスワードの組み合わせでログイン可能な機器が標的となり、約50 万台に及ぶIoT機器が事前に乗っ取られ、インターネットに障害が発生。

➢　国内事例（無線LAN ルータの脆弱性）

○　機器の管理画面がインターネット側からアクセス可能になっていたため、インターネット接続に関するID・パスワードが流出し、不正アクセスに利用された。

（基本的な考え方）

・　いずれの事案も、端末設備に基本的なセキュリティ対策が講じられていれば、その被害を相当程度抑止することができたと考えられる。

・　脆弱性を有する端末設備については、仮に悪意を持つ者に乗っ取られ、悪用された場合であっても、必ずしもその利用者に直接の被害が及ぶわけではないことから、セキュリティ対策が進まないという側面もある。

IoT機器を含む脆弱な端末設備のセキュリティ対策について

端末設備のセキュリティ対策の現状

・ IoT 機器のセキュリティ対策に関し、2016 年7月にIoT推進コンソーシアムにおいて「IoT セキュリティガイドライン ver 1.0」が策定されている。

（「IoT セキュリティガイドライン ver 1.0」の記載事項例）

	指針	主な要点
構築・接続	ネットワーク上での対策を考える	・ 初期設定に留意する ・ 認証機能を導入する

・ 電気通信事業法においては、電気通信事業者の回線設備に障害を与えない、他の利用者に迷惑を及ぼさないといった観点から、当該回線設備に接続される端末設備に関し、接続の技術基準を定めているが、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設けられていない。

今後の対応の方向性

➢ 情報通信ネットワークの安全・信頼性を確保するためのIoT機器の基本的なセキュリティ対策については、どのような対策が有効か、技術的な観点から専門的な検討を行っていくことが必要。

➢ その際は、諸外国の検討状況や技術の進展の動向等十分に踏まえた上で、通信事業者、IoT 機器メーカ等の関係者から広く意見を聴取し、慎重に検討を進めていくことが求められる。