資料38－2

IoTセキュリティ対策に関する諸外国の政策動向について

平成30年4月27日

IPネットワーク設備委員会
事務局

米国におけるIoTボットネット対策に関する報告書案の公表

○ 米国の商務省及び国土安全保障省は、本年1月5日に大統領への報告書案「ボットネット等の脅威に対するインターネットの強固性と通信のエコシステムの強化」を公表。報告書案では、IoTセキュリティに関し、技術及び政策面から、5つの目標及び行動計画を示している。

○ IoT機器のセキュリティ対策については、製造時の課題とともに、初期設定及び自動ソフトウェア更新機能の重要性を指摘し、機器の大半は国外に存在するため、国際的に認められた標準に基づくセキュリティの向上が重要としている。

○ 民間セクターによる、任意のIoT機器のセキュリティ認証が有効とする一方、規制庁においては、分野別に基本的なセキュリティ要件を産業界と連携して定めることができるとしている。

○ 報告書案に対しては、「政府は分野別にIoT機器のセキュリティ確保の枠組みを検討すべき（USテレコム）」、「政府は従来の脆弱なIoT機器による損害に対する責任や消費者保護に関する規制がどのように適用されるか明らかにすべき（ISOC）」及び「国際標準に基づく柔軟かつ任意の取組に賛同する（BSA）」等、多数の意見が提出されており、それらを踏まえ、本年5月に最終報告書が纏められる予定。

5つの目標及び行動計画 （行動計画は、端末セキュリティ関係のみ抜粋）

（目標1） 適応可能、維持可能かつ安全な技術市場に向けた道筋の明確化

行動計画1.1： 家庭及び工業用のIoT機器に対する現実的かつ基盤的なセキュリティ基準の決定と、二国間及び国際標準を通じた国際的な採用の促進。米国政府において使用されるIoT機器に対するセキュリティ基準の採用。

（目標2） 進化する脅威に対し、動的に適応可能な通信インフラの実現に向けたイノベーションの促進

（目標3） サイバー攻撃の防止、発見及び回避のためのネットワークの末端におけるイノベーションの促進

行動計画3.2： IoT機器等のセキュリティ機能に関するユーザーインターフェースの改善

（目標4） 国内外におけるセキュリティ、通信インフラ及び制御技術分野の団体間の連携構築

行動計画4.2： 規制庁は産業界と連携して不当な広告活動を抑止し、分野別に適切なセキュリティ要件を推進すべき

（目標5） 通信のエコシステムにおける啓発及び教育活動の推進

行動計画5.1： 消費者にも分かりやすい柔軟かつ費用対効果の高い任意の認証制度の構築・運用

行動計画5.2： 重要インフラ分野で使用される工業用IoT機器のための柔軟かつ費用対効果の高い任意の認証制度の構築

欧州における「ICTサイバーセキュリティ認証に関する規則案」の公表

○ 2017年9月、欧州委員会はサイバーセキュリティ強化に向けた政策パッケージを公表。現在の欧州ネットワーク情報セキュリティ機関（ENISA）を強化する「EUサイバーセキュリティ庁」の創設を提言するとともに、「ICTサイバーセキュリティ認証に関する規則案」を公表。

○ 「ICTサイバーセキュリティ認証に関する規則案」では、ICTに係る機器、システム及びサービスについて、EUにおけるサイバーセキュリティの認証の枠組み（欧州サイバーセキュリティ認証）を提案。

○ EU内において協調を図るため、「ICTサイバーセキュリティ認証に関する規則案」が採択された段階で、ICTに係る機器及びサービスに係る国別の認証制度は効果を失う。

○ 欧州サイバーセキュリティ認証については、国別に認定主管庁が定められ、適合性の評価は、国から認定を受けた機関が行う。

○ 欧州サイバーセキュリティ認証の目的は、

- データが偶発的もしくは不正に破壊されたり、書き換えられること等を防ぐ
- 権限のある者等に限り、データにアクセスできるように保証する
- 物理的又は技術的な障害が発生した場合でも、データやサービス等が利用できるように復旧する
- ICT機器やサービスに対し、既知の脆弱性を含まないソフトウェアが提供され、安全にソフトウェア更新がおこなわれることを保証する　等

○ 欧州サイバーセキュリティ認証について、EUにおいて法制化しない限り、任意としている。

○ 「ICTサイバーセキュリティ認証に関する規則案」に対しては、「IoT機器のセキュリティレベルを上げるには、任意の機器認証では不十分であり、認定マークの強制や、不十分なセキュリティ対策に対する製造物責任の法制化が必要（ドイツテレコム）」、「可能な限り国際標準に基づいた任意の認証フレームワークに賛同（Business Europe、Digital Europe）」等、多数の意見が提出されており、引き続き、EUの議会で検討が行われている。

（参考）「IoTセキュリティガイドラインver1.0」について（IoT推進コンソーシアム IoTセキュリティWGにおいて策定）

○本ガイドラインは、IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの（平成28年7月5日公開）。

○各指針等においては、具体的な対策を要点としてまとめている。

	指針	主な要点
方針	IoTの性質を考慮した基本方針を定める	• 経営者がIoTセキュリティにコミットする • 内部不正やミスに備える
分析	IoTのリスクを認識する	• 守るべきものを特定する • つながることによるリスクを想定する
設計	守るべきものを守る設計を考える	• つながる相手に迷惑をかけない設計をする • 不特定の相手とつなげられても安全安心を確保できる設計をする • 安全安心を実現する設計の評価・検証を行う
構築・接続	ネットワーク上での対策を考える	• 機能及び用途に応じて適切にネットワーク接続する • 初期設定に留意する • 認証機能を導入する
運用・保守	安全安心な状態を維持し、情報発信・共有を行う	• 出荷・リリース後も安全安心な状態を維持する • 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える • IoTシステム・サービスにおける関係者の役割を認識する • 脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		• 問合せ窓口やサポートがない機器やサービスの購入・利用を控える • 初期設定に気をつける • 使用しなくなった機器については電源を切る • 機器を手放す時はデータを消す