資料2－1

IoTセキュリティ対策の論点及び方向性（案）について

平成29年3月8日

事務局

IoTセキュリティ対策の論点（案）

1．論点（案）

（1）既に流通している脆弱性を有するIoT機器（ソフトウェアを含む。）のセキュリティ対策をどのように実施していくべきか。

① 対策を取るべきIoT機器の種類・範囲

② 脆弱性を有するIoT機器の特定方法

a) 誰が、b) 誰の負担で、c) いつまでに、d) どのように行うか

③ 特定された脆弱性を有するIoT機器への対応

a) 誰が、b) 誰の負担で、c) いつまでに、d) どのように行うか

（2）今後製造するIoT機器のセキュリティ対策をどのように実施していくべきか。

① 設計・製造において、セキュリティ・バイ・デザインをどのように実現するか。

② 販売・輸入において、脆弱性を有する機器の流通をどのように防ぐか。

③ 構築・接続において、セキュアなシステム構築をどのように実現するか。

④ 運用・保守において、安全安心な状態の維持をどのように実現するか。

検討に当たって必要な視点（案）

2. 検討に当たって必要な視点（案）

【利用者の視点】

・利用者にとって、安全かつ信頼できる仕組みとすべきではないか。

・利用者が対策の必要性を理解できる仕組みとすべきではないか。

【事業者の視点】

・事業者にとって、コストメリットのある仕組みとすべきではないか。

・自由なビジネスの進展を阻害しない仕組みとすべきではないか。

【全体的な視点】

・常時セキュアな環境が全体として確保される仕組みとすべきではないか。

・自己責任を原則としつつ、各主体が補い合えるような仕組みとすべきではないか。

・国際的な連携が可能となる仕組みとすべきではないか。

IoTセキュリティ対策の方向性（案）①

3. 方向性（案）

（1）既に流通している脆弱性を有するIoT機器（ソフトウェアを含む。）のセキュリティ対策をどのように実施していくべきか。

① 対策を取るべきIoT機器の種類・範囲

→ （例）サイバー攻撃の踏み台になることによりネットワークに悪影響を与え、国民生活・社会経済活動に多大なる影響を与えるおそれがある機器

② 脆弱性を有するIoT機器の特定方法

a) 誰が、b) 誰の負担で、c) いつまでに、d) どのように行うか

→ （例）IoT機器の脆弱性調査の実施
調査結果から脆弱性のあるIoT機器のデータベースを作成
※ この場合、誰が、誰の負担で行うのか。

③ 特定された脆弱性を有するIoT機器への対応

a) 誰が、b) 誰の負担で、c) いつまでに、d) どのように行うか

→ （例）脆弱性のあるIoT機器の利用者に対して注意喚起
IoT機器の製造業者に対して情報提供
※ この場合、誰が、誰の負担で行うのか。

IoTセキュリティ対策の方向性（案）②

3. 方向性（案）

（2）今後製造するIoT機器のセキュリティ対策をどのように実施していくべきか。

① 設計・製造において、セキュリティ・バイ・デザインをどのように実現するか。

→ （例）IoT機器の製造業者に対する意識啓発・支援

② 販売・輸入において、脆弱性を有する機器の流通をどのように防ぐか。

→ （例）認証マークの仕組みを作り、セキュリティに適合しているIoT機器に認証マークを付与
IoT機器のセキュリティについて比較サイトを通じた情報提供

③ 構築・接続において、セキュアなシステム構築をどのように実現するか。

→ （例）IoT機器とインターネットの境界上にセキュアゲートウェイを設置する取組の推奨

④ 運用・保守において、安全安心な状態の維持をどのように実現するか。

→ （例）継続的な安全性を確保するための検査の仕組み作りと対策が不十分なIoT機器への対応
利用者に対する意識啓発（ID/パスワード設定、ファームウェアのアップデート、Wifi設定）
利用者からの相談・調整窓口の設置
脆弱性を調査する民間サービスの実施促進

⑤ ①～④の各段階にとどまらず、ネットワーク全体のセキュリティをどのように確保するか。

→ （例）総合的にIoTセキュリティ対策を実施する機関において対応