安全なIoTシステムのためのセキュリティに関する一般的枠組について（概要）

参考資料1

目的

- IoT(Internet of Things)システムは、従来の情報セキュリティの確保に加え、新たに**安全確保が重要**
- **セキュリティ・バイ・デザイン**の思想で設計・構築・運用されることが不可欠
- 安全なIoTシステムが具備すべき**一般要求事項としてのセキュリティ要件の基本的要素**を明らかにしたもの

安全なIoTシステムのためのセキュリティに関する一般的枠組み（個別分野の標準の**"テンプレート"**）

個別分野固有の要求事項

自動車分野　電力分野　農業分野　鉄道分野　医療分野　・・・

検討の視点

- 一つのIoTシステムリスクが他のIoTシステムに波及する可能性→**System of Systems**としての捉え方
- **機密性、完全性、可用性に加え、安全性**の要件確保

基本原則

- 関係者間の相互理解及び相互信頼の下、ネットワーク側とモノ側が、一体となり**システム全体としてセキュリティ確保**を図ることが必要。
- **セキュリティ・バイ・デザイン**を基本原則とし、**システム稼働前に確認・検証できる仕組**が必要。
- その際、基本方針の設定、リスク評価、システム設計、システム構築、運用・保守の**各段階の要件定義**が必要であり、以下の項目の明確化が必要。
  - ✓ 定義・範囲
  - ✓ 安全性・機密性・完全性・可用性
  - ✓ 確実な動作に必須事項、障害発生時の回復に必要な要件
  - ✓ 法律等からの要求事項
  - ✓ サイバー攻撃時の機能確保と迅速な復旧
  - ✓ 責任分界点、データの扱い方

取組方針

- **法令等の要求事項の明確化**
- IoTシステムの構成を**適切にモデル化**し、モデルを参照しながらセキュリティ要件を議論
- リスクアセスメントを活用した**セキュリティ対策や実装方法等の明確化**。ただし、リスクに応じた**柔軟な対応が必要**。
- 普遍的な**性能要求**とその時点での有効な手段の具体的方法を示す**仕様要求**の適切な適用
- 技術革新を前提とした**段階的・継続的アプローチ**
- IoTシステムに関連する者の**役割分担**（連携・協調によるセキュリティ確保の在り方や責任分界点の明確化を含む）
- データの利活用と個人情報保護の仕組み、機器認証の在り方などの**運用ルールの明確化**