IoT セキュリティのための一般的枠組(案)

平 成 ２ ８ 年 ６ 月 １ ０ 日
内閣サイバーセキュリティセンター

1. 目的

IoT(Internet of Things)システムについては、将来、個々のシステムが相互に接続されることを見据え、セキュリティ・バイ・デザイン(Security by Design)の思想で設計、構築、運用されることが不可欠である。こうしたことを合理的に実現させるためには、早急にすべての IoT システムにかかる設計、構築、運用に求められる事項を一般要求事項として明確化し、その上で、個々の分野の特性を踏まえた分野固有の要求事項を追装する２段階のアプローチが適切であると考えられる[1]。

本枠組は、こうした考え方に基づき、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することを目的とする。

本枠組に基づく IoT システムの相互運用性の確保とセキュリティ要件の実装を促すことにより、産業界による IoT システムの積極的な開発等の取組を促すとともに、利用者が安心して IoT システムを利用できる環境を生み出すことが期待される。

2. 検討の視点

本枠組において、IoT システムはモノ同士がインターネットを介して接続されることにより新たな価値を生み出すものである。しかし、IoT システムが他の IoT システムと接続されることによって追加的な付加価値が生みだされる反面、一つの IoT システムのリスクが他の IoT システムに波及する可能性があることに鑑み、本枠組においては、IoT システムの集合体である”System of Systems (SoS)”として捉える。

[1] IoT 推進コンソーシアム・総務省・経済産業省「IoT セキュリティガイドライン(案)」は、本枠組の基本的考え方を参照しつつ、IoT システムに関するセキュリティ確保のための具体的要件を整理している。個別の IoT システムに関するセキュリティガイドラインの策定に際しては、これらのガイドラインを基礎としつつ、個別の領域の特性を考慮して行うことが推奨される。

IoT システムの構成は多層的であるが、機器、ネットワーク、認証等のプラットフォーム、サービスの４つの機能層（レイヤー）に分けて分析・検討を行い、どのレイヤーのセキュリティ要件を議論しているかという点について明確化することが関係者の認識共有の観点から望まれる。

その際、各レイヤーの機能は以下のとおり整理される。第一に、機器層は、センサー及びアクチュエーター等の機器を指し、それを構成するチップ、ファームウェア、組み込みソフトが含まれる。第二に、ネットワーク層は、有線もしくは無線通信網を指し、自営網と通信事業者等が提供する商用の通信網が含まれる。第三に、プラットフォーム層は、機器層から獲得し、ネットワーク層を経由して収集されたデータを集約し、これらデータの相互参照によりサービス提供に有意な情報を生成する機能を含む。第四に、サービス層は、下位の３層で構成される機能を使って IoT システムとして実現される役務を指す。

なお、以下において、「モノ側」とは、機器層の機能を指し、「ネットワーク側」とは、ネットワーク層及びプラットフォーム層で実現される機能を指す。

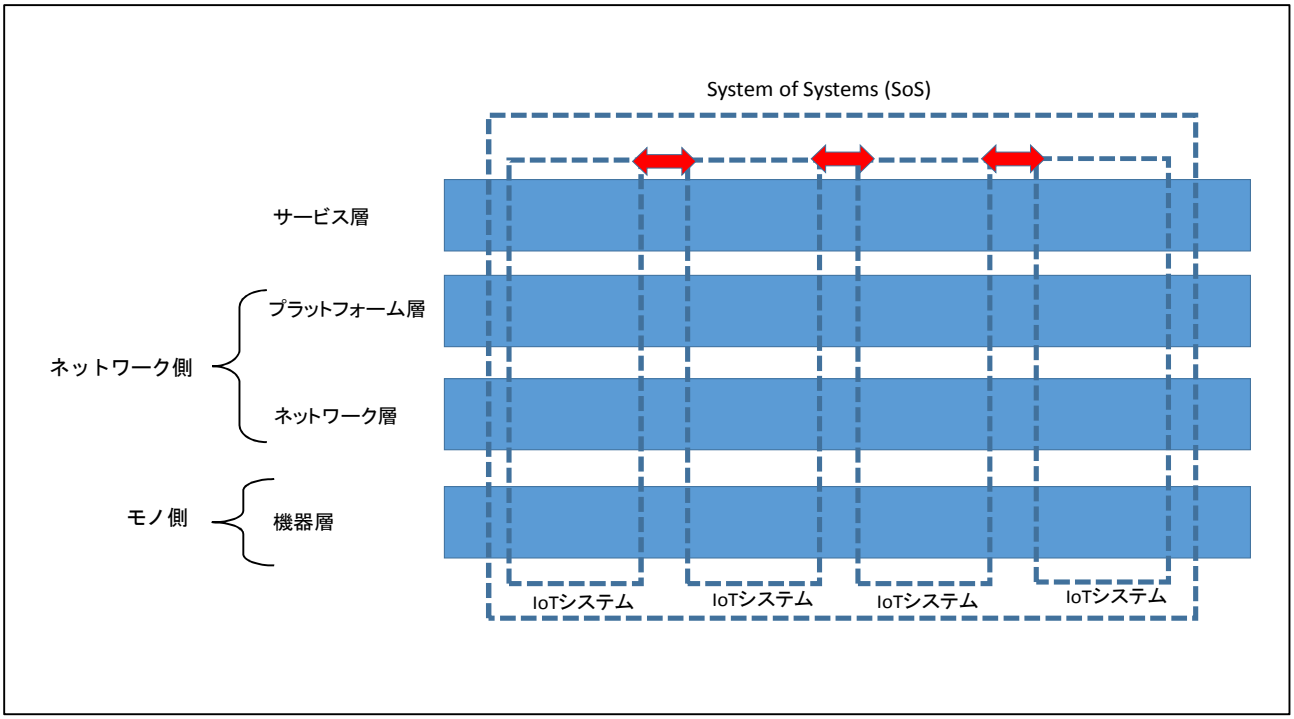

図 1 IoT システムレイヤーについて

3. 基本原則

接続されるモノには、既存の安全確保や性能に関する法令要求、慣例等が存在している。また、ネットワークは、その維持・管理の主体、通信方式、ネットワーク構成、接続範囲、品質等が多様であり、提供されるサービスの要求条件を満たす最適なネットワークを選択して使用されることが必要である。

しかしながら、モノ側とネットワーク側の双方において、それぞれに有する業態の環境や特性を相互に必ずしも熟知していないため、両者の接続によって所要の安全性や性能を満たさず、法令違反等になる懸念がある。特に、ネットワーク側の環境が、モノ側のセキュリティ要件を変化させる可能性があり、将来の運用も含めた安全確保をあらかじめ考慮しておく必要がある。

ネットワーク側とモノ側が連携し、関係者間の相互理解及び相互信頼の下、ネットワークとモノを融合して新たな付加価値を産み出すため、官民の緊密な連携によりセキュアなIoTシステムを産み出す環境を整備する必要がある。特に、IoTシステムが従来の情報システムと異なる特性を有することを考慮して、モノ側とネットワーク側が一体となり、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である。

上記の必要性を踏まえ、IoTシステムの設計・構築・運用に際しては、セキュリティを事前に考慮するセキュリティ・バイ・デザインを基本原則とし、これが確保されていることが当該システムの稼働前に確認・検証できる仕組みが求められる。その際、IoTシステムのセキュリティ確保のための要件としては、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・保守の各段階で求められる要件を定義することが必要であり、その際、以下の項目について明確化することが必要である。

① IoTシステムについて、範囲、対象を含めた定義を改めて明確にするとともに、IoTシステムが多岐にわたることから、リスクを踏まえたシステムの特性に基づく分類を行う。
② IoTシステムに係る情報の機密性、完全性及び可用性の確保並びにモノの動作に係る利用者等に対する安全確保に必要な必須要件を明確化する。
③ 機能保証の制定を含め、確実な動作の確保、障害発生時の迅速なサービス回復に必要な必須要件を明確化する。
④ その上で、接続されるモノ及び使用するネットワークに求められる安全確保水準(法

令要求、慣習要求）を明確化する。

⑤ 接続されるモノ及びネットワークの故障、サイバー攻撃等が発生しても上記②から④の各項目が確保されることを明確化する。

⑥ IoT システムに関する責任分界点、情報所有権を明確化する。

なお、IoT システム間の接続に係る要件等についても上記①から⑥の各項目が適用される。

4. 取組方針

4.1. 要求事項の明確化

接続するモノと使用するネットワークに関連する①法令・規制要求事項、②明示されていないが不可欠な要求事項、③業界等が必要と判断する追加要求事項について明確化する必要がある。

4.2. リスクに応じた対応

あらゆるモノがネットワークに接続されるとした際、接続によってもたらされるメリットとリスクは不可分であり、その両面を客観的に捉え、当初は想定されていなかったリスクが生じうることも含め、採られるべきセキュリティ対策や実装方法等をあらかじめ明確にする必要がある。リスク及び許容されるリスクは、ユースケースによっても異なること及び時間の経過とともに変化することを踏まえ、機能保証の観点から柔軟に対応できるようにする必要がある。

このため、リスクアセスメントを適宜活用するものとする。その際、特定の IoT システムに起因するリスクが他の IoT システムに波及するシステミックリスクを遮断する仕組みについても明確化する必要がある。

4.3. 性能要求と仕様要求の適切な適用

IT を取り巻く環境変化は急激であるため、要求事項は、普遍的な性能要求とその時点で有効な手段の具体的方法を示す仕様要求の２つの要求から構成するものとする。

このうち、仕様要求は、対象とする IoT システムを明確化し、柔軟に最適な手段を選択できるよう作成される仕組みとする。

4.4. **段階的・継続的アプローチ**

IoT システムは、技術革新等の環境変化によって継続的に機能等が変化していくものであることを踏まえ、まずは、基本的な機能要件を定め、段階的・継続的にそれを進化させていくものとする。

4.5. **役割分担及び連携した対処のあり方の明確化**

産、官、学はもちろんのこと、IoT システムに関連する者の役割分担を明確にする。あわせて、情報共有も含め、各主体の連携・協調によるセキュリティ確保のあり方や各主体間の責任分界点を明確にする。

4.6. **その他運用ルールの検討**

IoT システムの連携と個人情報保護の仕組みについて、領域を越えた社会的ルールの具体化を図る。また、機器認証の在り方等について、主体の在り方(複数の主体による連携を含む。）や運用ルールを明確化する。

5. 留意事項

本枠組は現時点で想定される IoT システムを前提として策定されたものであり、技術革新等による IoT システムの機能の高度化等に併せ、適宜見直しを図ることとする。その際、広く関係者(マルチステークホルダー)の意見や議論を踏まえたものとする。

以　上