応般

❺ 政府におけるセーフティとセキュリティの取組み

結城則尚（内閣官房内閣サイバーセキュリティセンター企画官）

安全な IoT を発展させていく重要性

IoT（Internet of Things）システムについては，モノが接続されることから，情報通信技術と物理的システムが融合したシステムとして捉える必要がある．IoT システムが提供するサービスには，従来からの情報セキュリティの確保に加え，新たな安全確保が重要となる．また，将来，個々のシステムが相互に接続されることを見据え，システム相互間の接続が新たな脆弱性となる懸念があることを踏まえ，システムの企画・設計・構築・運用の各段階でセキュリティを考慮するセキュリティ・バイ・デザイン（Security by Design）の思想で対応することが不可欠である．

こうしたことは，2015 年 9 月 4 日に閣議決定された「サイバーセキュリティ戦略☆1」に記載されている（図 -1 参照）．

IoT でサイバー空間と物理空間がつながることにより，得られる便益は計りしれないものとなるが，同時に，サイバー空間でのトラブルが，物理空間に影響を与えることにより，思わぬ人身災害，物理災害が発生するリスクも必然的に高くなる．また，個人や企業が所有するデータといった無形資産までもが盗取，改ざん，毀損されてしまうリスクも高くなる．

このように，IoT システム導入によってもたらされる「ベネフィット」と「リスク」は対称性があることを踏まえ，リスクを上手にコントロールできるか否かが，ベネフィットを享受できるか否かの重要な要素となる．すなわち，利便性，セーフティ，セキュリティを同時に達成することが必要となる．

しかし，これまで，ICT 分野，情報セキュリティ分野，産業保安分野が協業する機会がほとんどなかったのではないだろうか．安全な IoT システムの創出に向け，関係者が共通の概念，理念を共有することが不可欠である．こうした状況の下，2016 年 8 月，内閣官房内閣サイバーセキュリティセンター（NISC）は，国内外のパブリックコメントを経て，サイバーセキュリティ戦略における訴求内容を具現化した「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☆2」（以下，「一般的枠組」という）を発行した．これをもとに，関係者間の検討が進められてきている．

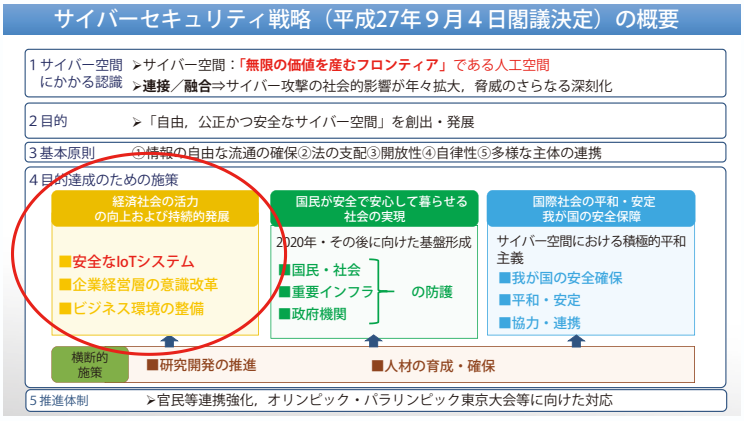

図 -1　サイバーセキュリティ戦略における安全な IoT システムの位置付け

なぜ，一般的枠組が必要なのか

なぜ，一般的枠組が必要なのかについて，3 つの側面から解説する．1 点目は，新し

☆1 https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf

☆2 https://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf

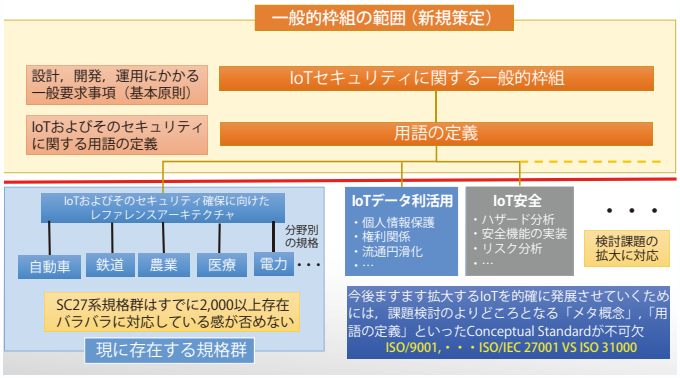

図 -2　安全な IoT システムにおける「NISC の一般的枠組」の関係

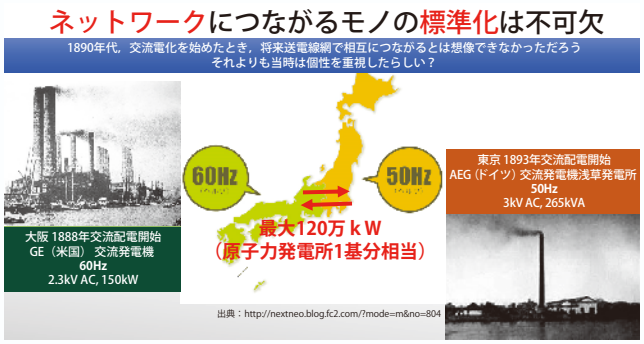

図 -3　日本における電源周波数による電力網の分断

い課題への挑戦であることを踏まえた考え方の体系化の必要性の面からである．安全な IoT システムについて，体系化を試みると，図 -2 のようになる．

現に存在する規格群は，情報セキュリティに関する国際標準化を行う ISO と IEC の合同委員会（ISO/IEC JTC 1/SC27）において策定される規格等が多い．今後，データ利活用，IoT システム安全など種々の課題を解決していく必要があることから，IoT システムの理念や用語をあらかじめ明確にしておくことが重要であり，現時点で可及的速やかにとりかかるべき課題であると考えている．

2 点目は，サイバーセキュリティ戦略で訴求しているように，安全な IoT システムの創出により，安全や品質といった我が国の強みをもって世界に貢献するというものである．

3 点目は，我が国の交流送配電の歴史から学ぶことである．19 世紀後半，大阪で 60Hz，数年後東京で 50Hz の交流電化がそれぞれ開始された．以降，送電線が急激に拡充され，電源周波数によって国内は 2 分化されている（図 -3 参照）．この弊害は，2011 年 3 月の東日本大震災で東日本の原子力発電所がすべて停

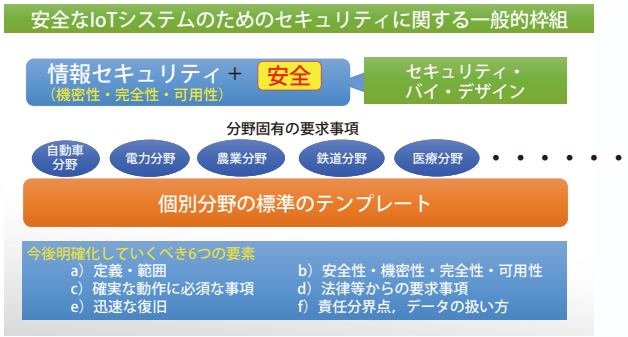

図 -4　安全な IoT システムのためのセキュリティに関する一般的枠組の全体像

止した際に顕在化した．電気に余裕がある西日本から東日本への電力融通は，異なる電源周波数により制限を受け，首都圏で計画停電が発生した．交流電化を始めた際には，日本が電力網でつながるとは思ってもいなかったことだろう．この教訓を活かし，IoT システム萌芽期にある今日，「当初からつながる前提で進める」ことが必要であると考える．

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

一般的枠組は，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みを促すとともに，利用者が安心して IoT システムを利用できる環境を創出することを基本コンセプトとしている．（図 -4 参照）

検討の視点

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創出するものである．モノが接続されることから，安全性に対しても考慮する必要がある．このため，セキュリティの 3 要件である機密性（Confidentiality），完全性（Integrity），可用性（Availability）に，安全性（Safety）を加えた 4 つの要件（S-CIA）を確保することを前提としている．

基本原則

IoT システムの要素であるモノには，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，IoT システムに使用されるネットワークは，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，現状においては，モノ側とネットワーク側の双方において，相手方の業態の環境や特性を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ないだけでなく，法令違反等になってしまう懸念すら存在している．こうしたことを踏まえ，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および相互信頼の下，ネットワークとモノを融合して新たな付加価値を生み出すため，官民の緊密な連携により安全な IoT システムを生み出す環境を整備する必要がある．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，当該システムの稼働前にこれが確保されていることを確認・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，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る．その際，表 -1 に示す 6 項目の課題について明確化していくことが必要である．

安全な IoT システム創出にかかる取組み状況

2016 年 10 月，サイバーセキュリティ戦略本部令（平成二十六年政令第四百号）に基づき設置された研究開発戦略専門調査会において，一般的枠組を踏まえ，安全な IoT システムの創出にかかる取組みについて，国として検討する体制が審議され，図 -5 に示す体制で検討を開始した．

a）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い，その結果に応じた対応を明確化する．
b）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要件を明確化する．
c）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要件を明確化する．
d）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．
e）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機密性，完全性，可用性，安全性の各項目が確保されるとともに，障害発生時の迅速なサービス復旧を行うことを明確化する．
f）IoT システムに関する責任分界点，情報の所有権に関する議論を含めたデータの取扱いの在り方を明確化する．

表 -1　安全な IoT システム創出のために明確化すべき 6 項目（一般的枠組より抜粋）

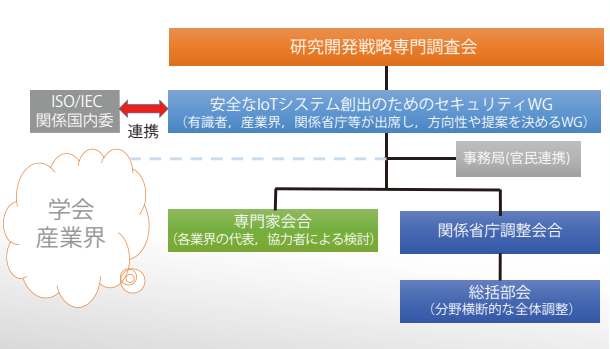

図 -5　IoT の検討体制（素案）

IoT システムは国全体として取り組むべきものであることから，省庁間が円滑に連携できるよう，関係省庁会議を設置し，専門家の意見を聴きながら，国としての方針を調整していくこととしている．

さらに，IoT システムのメインプレーヤは民であり，学会や産業界との連携が重要であることから，2016 年 10 月以降，IoT 推進コンソーシアム幹事会社の主要参加企業をはじめ，関係者と鋭意検討を進めてきている．これまでにない広範囲の価値観や文化の異なる関係者との議論における論点は，予想以上に多く，議論百出の状況が続いてきている．検討を進めていくと，官民連携における官民のスタンスの違いが明らかになってきた．

官は，「IoT システムのメインプレーヤは民であり，民が十全に取り組めるよう制度面を含め支援する」という考えで対処してきたが，議論が進むにつれ，民は，「官の指示に従う」として，双方の認識

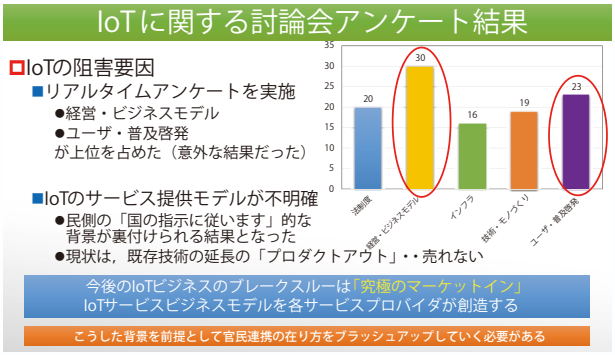

図 -6　公開討論会におけるアンケート結果

に齟齬が感じられるようになってきた．

2017 年 4 月に小職は，公開討論会で IoT システムの阻害要因に関してアンケートを実施した．図 -6 に示す通り，「将来，IoT システムによってどのようなサービスを実施するのか，ユーザにどのように訴求をするのかが明確になっていない」ことが，IoT システムの阻害要因であることが明らかになった．さまざまな分野が繋がり，新しい付加価値を生む IoT システムに関する経営・ビジネスモデルは，リスクをコントロールして投資を行うための戦略や経営者のリーダシップが必要であることを示唆しているのではないか．

こうした事実関係を踏まえ，官民連携の在り方について，ブラッシュアップしていくこととしている．

加えて，関係者の議論の内容を踏まえると，一般的枠組で訴求している検討目的，検討範囲，検討粒度について，官民での認識共有が不十分であるように思える．また，関係者が拡大し，多方面からの検討が必要である．多様な価値観を相互に認め合うためには，一定の時間が必要であると考えられる．

IoT システムにおける新技術について

IoT システムにおける新技術は，既存要素技術の組合せによって新たな付加価値を創造する技術ではないかと考える．しかし，これは要素技術に秀でている日本にとって，最も苦手なものではないか．これが前述の「将来，IoT によってどのようなサービスを実施するのか，ユーザにどのような訴求をするのかが明確になっていない」に影響しているものと思われる．今では当たり前になっているスマートフォンは，発売当初，タッチパネル操作，音楽はダウンロード前提など，かなり奇抜であったかもしれないが，開発者が将来のサービスモデルを見据えての究極のマーケットインであったと思う．採用されている要素技術は，ほとんど我が国がすでに開発したものであり目新しくはない．しかし，潜在的にマーケットが何を望んでいるのかを十分把握した上で，これまでにない新しいサービスモデルを既存技術の組合せで打ち出した奇抜な発想が成功の鍵であった．

IoT システムにおける新技術は，この例と同様，将来を見据えて奇抜な発想を既存技術の組合せによって実現することではないかと思われる．次に，組合せによって裏目に出るリスクを的確に把握し，コントロールすることが必要である．

安全な IoT システムの普及に向けて

IoT システムが今後爆発的に流行することをだれも否定しないだろう．その前に過去の歴史から学ぶ必要がある．技術の萌芽期における「使えればよい」という認識を発展期においても持ち続けてしまうと，ある時点で後戻りできなくなる．開発が滞るだけでなく国民経済的にも支障をきたすというこれまでの経験・知見を反映する必要がある．こうしたことを踏まえると，将来を見据えた IoT システムの標準化を図ることができる時期は，萌芽期である今しかない．機密性，完全性，可用性に，安全性を加えた 4 つの要件（S-CIA）を確保することがその前提である．

いずれにせよ，インターネットを介して異なった文化背景のモノが次々と接続されることにより新たな価値を生み出す IoT システムを発展させていくためには，予想以上に調整すべき案件が多い．しかし，これを乗り越えて得られるベネフィットは強大であることはいうまでもない．

（2017 年 7 月 27 日受付）

結城則尚 ■ yuki-n28n@cyber.go.jp
内閣サイバーセキュリティセンター重要インフラ担当，経産省製品安全課，保安院電力安全課，同原子力発電検査課，資源エネルギー庁原子力産業課，米国原子力規制委員会原子炉規制局，通産省原子力発電安全企画審査課等を歴任．東北大学工学部機械工学科卒業．