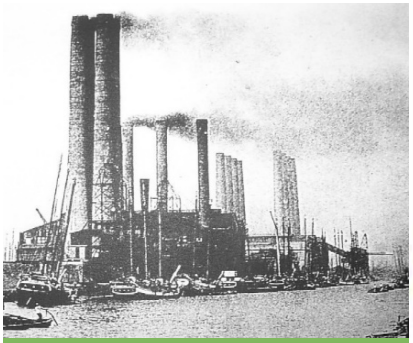
安全なIoTシステムのセキュリティ
～IoT標準化のための標準の必要性～

平成28年12月12日
内閣サイバーセキュリティセンター(NISC)
基本戦略グループ(分析担当)
企画官 結城 則尚

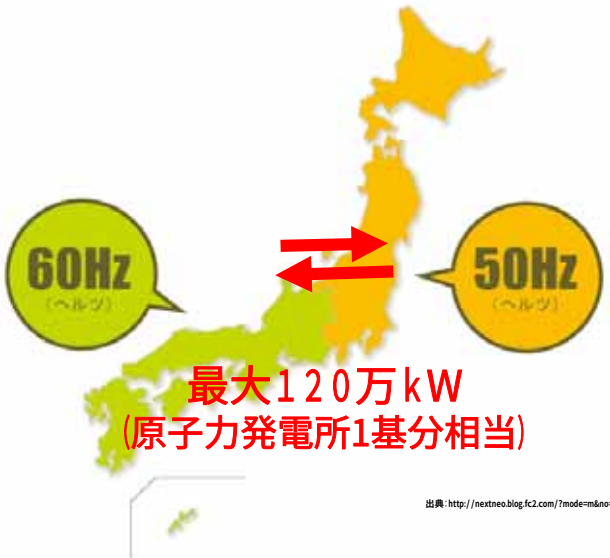
1．歴史から学ぶ

ネットワークにつながるモノの標準化は不可欠

1890年代、交流電化を始めた時、将来送電線網で相互につながるとは想像できなかっただろう
それよりも当時は個性を重視したらしい？



大阪 1888年交流配電開始
GE(米国) 交流発電機
60Hz
2.3kV AC, 150kW



東京1893年交流配電開始
AEG(ドイツ) 交流発電機浅草発電所
50Hz
3kV AC, 265kVA

自動車はどの車でも運転できるが

- **運転に必要な操作がどれも同じ**
  - アクセル　右側
  - ブレーキ　左側
  - 変速レバー　**車中央側**
  - 方向指示器　**窓側**
  - ワイパー　**車中央側**

- **アメリカ居住時の混乱**
- 右側通行　左ハンドル
  - **原則がわかるまでは冷や汗ものだった**
  - 方向指示器を出そうと思うとワイパーが動作
  - 変速しようとするとドアをたたく
  - 交差点に入ると左に入りそうになり衝突寸前

自動車はどの車でも運転できるが

- **運転に必要な操作がどれも同じ**
  - アクセル　　右側
  - ブレーキ　　左側
  - 変速レバー　　**車中央側**

そもそも車の通行方向を統一しておけば、
世界中の車を混乱なく運転できたし
製造コストも下がっただろう

- **原則がわかるまでは冷や汗ものだった**
- 方向指示器を出そうと思うとワイパーが動作
- 変速しようとするとドアをたたく
- 交差点に入ると左に入りそうになり衝突寸前

2．IoTの健全な発展のための課題

カテゴリー毎のモノの標準にはテンプレートが必要

自動車同士がつながる

自動車以外とつながる

カテゴリー毎のモノの標準にはテンプレートが必要

自動車同士がつながる

自動車以外とつながる

設計思想が違うものが
相互に接続されると
利便性向上と同時に
新たな脆弱性、不具合を産む懸念

IoTの標準は安全の標準であることが重要

IoTの標準は安全の標準であることが重要

モノがITシステムに接続されることによって
ITシステムのトラブルが物理的影響を与える
CyberとPhysicalが一体化
情報セキュリティのCIAにSafetyを考慮
CIAからS-CIAへの転換

データに関する横断的な標準が必要

出典：ソフトバンク株式会社

出典：ソフトバンク株式会社

出典：農林水産省

データに関する横断的な標準が必要

あらゆるものがネットを介してつながる
データ利活用により得られるメリットを活用
その前提として、
データの標準化、プライバシー、データ所有権
等あらかじめ横断的に定めておく必要がある

出典：ソフトバンク株式会社

出典：ソフトバンク株式会社

出典：農林水産省

IoTシステムにおけるセキュリティバイデザインの必要性

- ボットネット「MIRAI」
  - 2016年10月21日、米DNS代行サービスへの大規模なDDoS攻撃
    - 多くのオンラインサービスが停止
      - 工場出荷時に設定された初期パスワードを使ってIoT機器にマルウェアを感染させる手口が目立っている
    - IoT機器が悪用される理由
      ① 初期パスワードを使った侵入が容易である
      ② 高速インターネットに24時間365日接続しているため、継続的に悪用できる
      ③ 一般的に設置後の整備や保守が行われないため、問題が発覚しづらい
      - IoT機器は、2013年時点で約158億個あり、2020年までに約530億個まで増加すると予想されている
      - インターネット全体に影響を及ぼすような大規模なDDoS攻撃が発生する前に実効性のある対策に見直す必要があると言える

IoTシステムにおけるセキュリティバイデザインの普及が急務

3．行政としての取り組み

サイバーセキュリティ戦略(平成27年9月4日閣議決定)の概要

1 サイバー空間に係る認識
- サイバー空間：「無限の価値を産むフロンティア」である人工空間
- 連接／融合⇒サイバー攻撃の社会的影響が年々拡大、脅威の更なる深刻化

2 目的
- 「自由、公正かつ安全なサイバー空間」を創出・発展

3 基本原則
①情報の自由な流通の確保②法の支配③開放性④自律性⑤多様な主体の連携

4 目的達成のための施策

経済社会の活力の向上及び持続的発展	国民が安全で安心して暮らせる社会の実現	国際社会の平和・安定 我が国の安全保障
■安全なIoTシステム ■企業経営層の意識改革 ■ビジネス環境の整備	2020年・その後に向けた基盤形成 ■国民・社会 ■重要インフラ ■政府機関 の防護	サイバー空間における積極的平和主義 ■我が国の安全確保 ■平和・安定 ■協力・連携

横断的施策：■研究開発の推進　■人材の育成・確保

5 推進体制
- 官民等連携強化、オリンピック・パラリンピック東京大会等に向けた対応

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

日本語 http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf
英　語 http://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf


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

1. 目的


General Framework for Secure IoT Systems

1. General Framework Objective

2. Perspectives of the General Framework

- ○平成27年9月
  サイバーセキュリティ戦略
  閣議決定
- ○平成28年6月2日
  研究開発専門調査会(第4回)
  で審議
- ○平成28年6月10日～6月24日
  国内外に対してパブコメ実施
  国内外から16者68件の意見
  が提出、全25件修正
  特に米国から肯定的な意見
  が多く寄せられた
- ○平成28年8月26日
  「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」発行

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

今後明確化していくべき6つの要素

a) 定義・範囲
b) 安全性・機密性・完全性・可用性
c) 確実な動作に必須な事項
d) 法律等からの要求事項
e) 迅速な復旧
f) 責任分界点、データの扱い方

米国商務省国家通信情報管理局による
IoTの利益･課題･政府の役割についてパブリックコメント

- 2016年4月6日
  - 「IoTの進展を促進するための利益、課題及び政府に求められる役割に関するコメント要求」を告示し、2016年6月2日までの期間で意見を募集
- 2016年8月2日
  - 寄せられた意見が公開される
  - 「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」の訴求内容と整合している。

- **連邦政府は、IoTが広まっていく際に唯一国全体を把握できる立場であることを認識し、透明性を持って情報を共有し、産業界がIoT全体の広がりを理解できるようにすることでIoTの発展に寄与**できる。
  - IoTに関する最大の課題は、**連邦政府がバラバラに推進している**こと。
  - **連邦政府がIoTへ取り組むには、まずIoTの定義を考慮すべき**である。
  - IoTの課題は、**プライバシー、セキュリティ、透明性、知的財産権、継続性、選択権、救済制度の整備**である。
  - IoTのセキュリティは大きな課題であり、**相互接続される性質上、脆弱性の影響は大きくなる。**
  - **消費者がIoTに参加しないことを選択できるかどうかも重要な課題**となる。

今後どうやって課題解決に向かっていくか

□現状認識

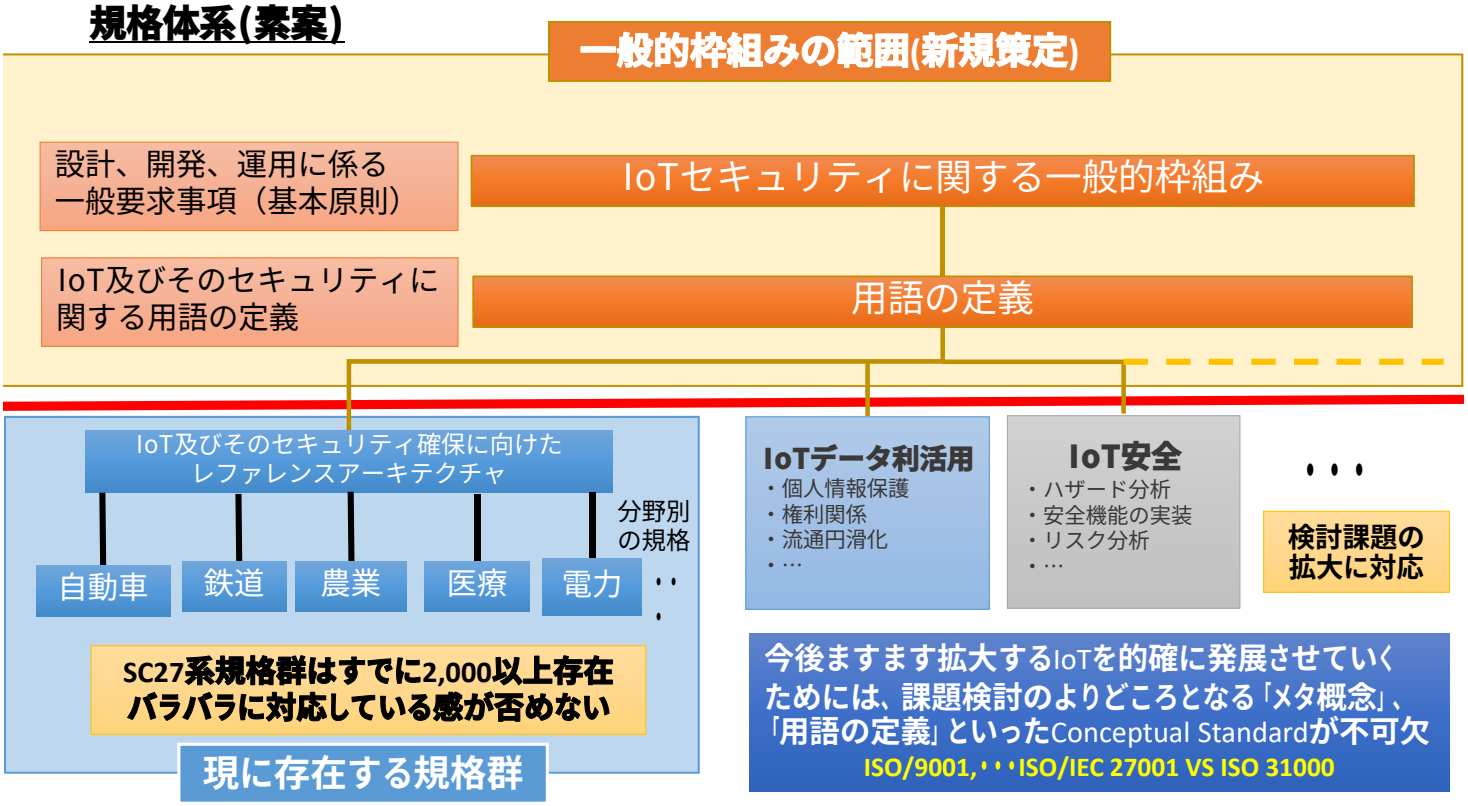
- IoTブームに伴い、セキュリティ対策の事例集が多数策定されている
- 情報系のセキュリティの延長線で作成されているものが主
- **我が国の強み**である**「安全」**や機能が提供する**「品質の高さ」**の確保と関連付けていく取り組みが必要
- こうした取り組みを通じて、**我が国の高い製品の品質を「セキュリティ」の局面においてもブランド価値**として、国際競争力強化に活かし、セキュリティ対策の強化を推進していく。
- この手段として、「安全なIoTシステムのためのセキュリティに関する一般的枠組」を基礎として、多国間連携を行いつつ、最終的には国際標準化を目指す

今後どうやって課題解決に向かっていくか

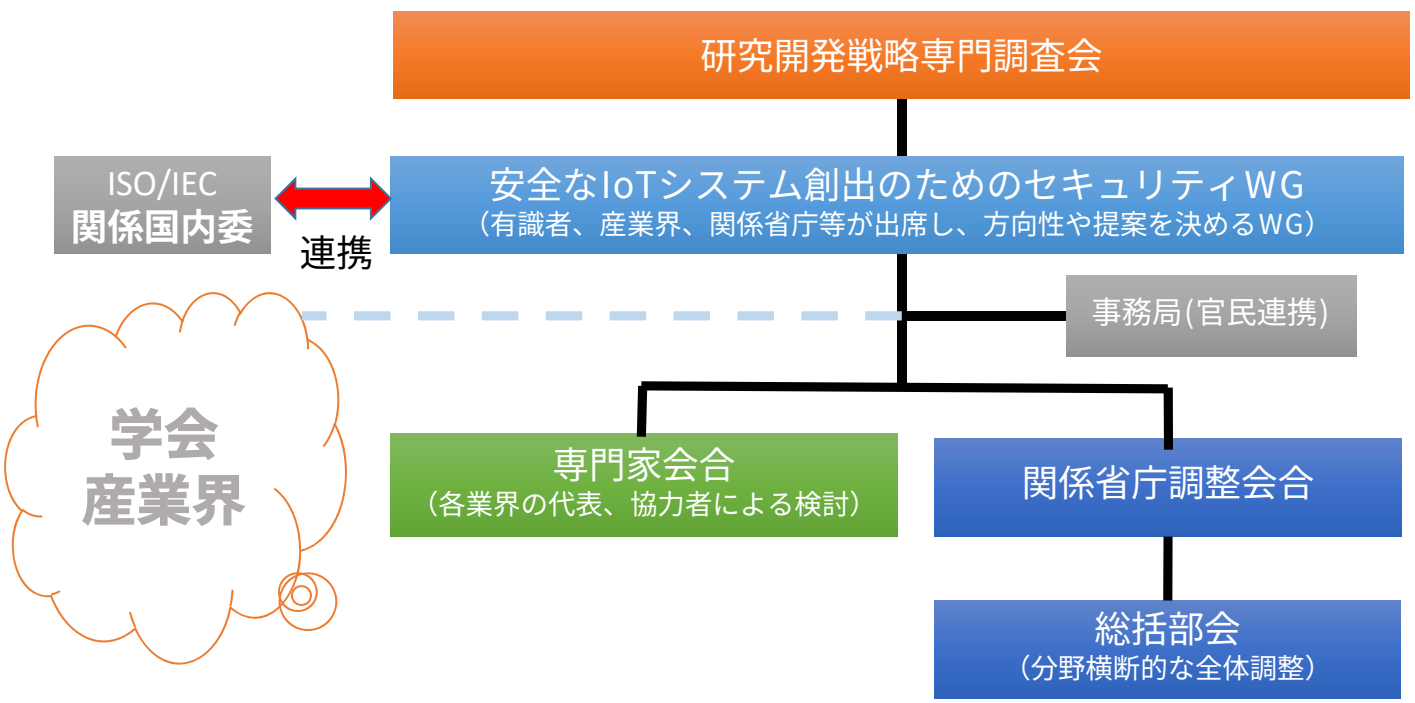
1. **IoTセキュリティのフレームワークの国際標準化に向けた日本案の策定**
   - 一般的枠組をベースにしつつ、国内で議論･調整を行い国際標準を目指す
2. **フレームワークを各分野に適用するための関係者の理解促進やアクションプランの策定**
   - IoTセキュリティのフレームワークをベースとした関係者への普及･啓発
   - 具体的なサービスインに向けた**分野別の規格等の策定**や、**製品や事業に対する法令要求に適合するIoTセキュリティに関する基準**策定の方向性検討を行っていく

産学官一体となってものづくり大国日本の強みを発揮させる

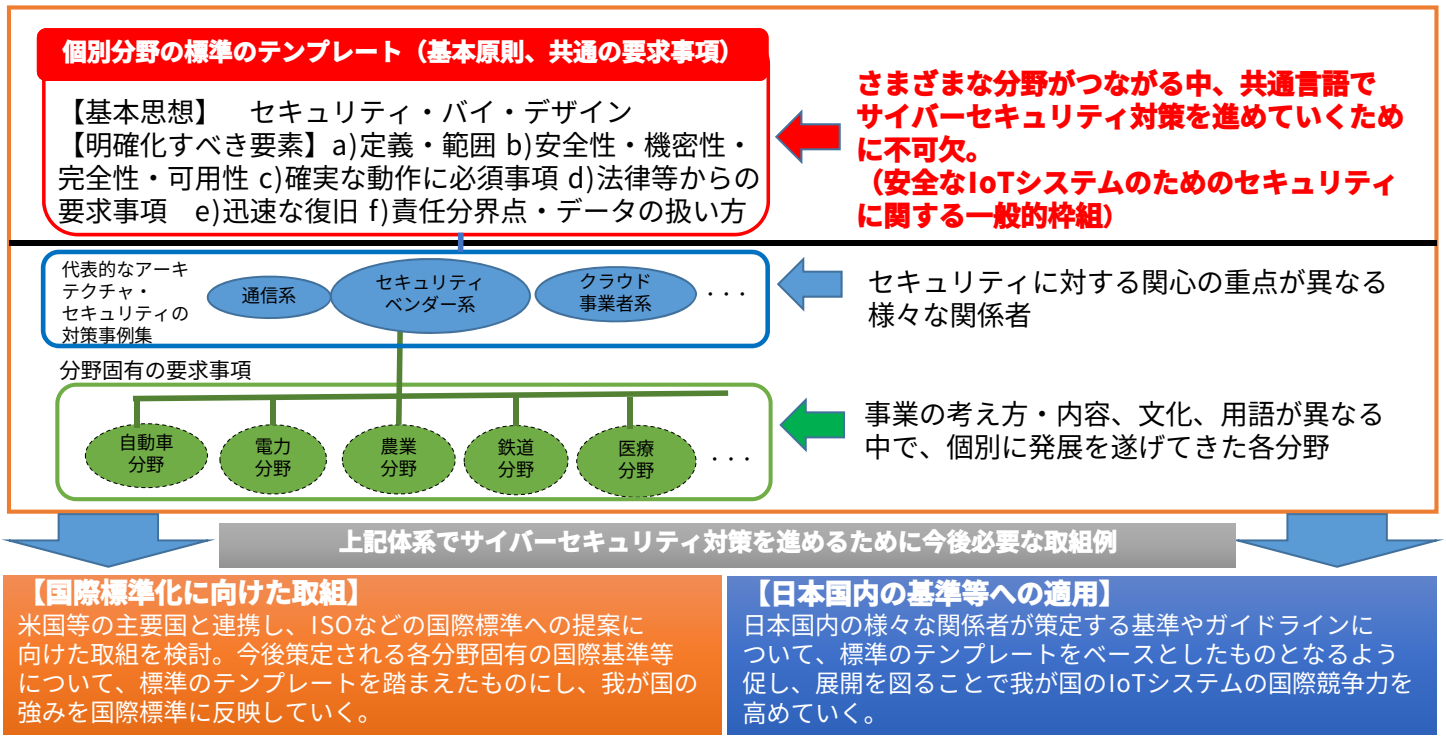
規格体系(素案)



○検討体制(素案)



【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】（2016年8月 NISC）



【国際標準化に向けた取組】
米国等の主要国と連携し、ISOなどの国際標準への提案に向けた取組を検討。今後策定される各分野固有の国際基準等について、標準のテンプレートを踏まえたものにし、我が国の強みを国際標準に反映していく。

【日本国内の基準等への適用】
日本国内の様々な関係者が策定する基準やガイドラインについて、標準のテンプレートをベースとしたものとなるよう促し、展開を図ることで我が国のIoTシステムの国際競争力を高めていく。

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解説

1．目的

- IoTシステムについては、モノが接続される
  → Cyber Physical System
  - 新たに**安全確保**が重要
- 将来、個々のシステムが相互に接続される
  - **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、**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。
  - 早急にすべてのIoTシステムに係る設計、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
- 安全なIoTシステム(以下、「IoTシステム」という。)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

2．検討の視点

- IoTシステムの集合体である“System of Systems (SoS)”
  - 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
  - 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
  - 追加的な付加価値が創出される反面、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
- 4つの要件を確保する
  1. **安全性(これがこれまでにない取り組み)**
  2. 機密性
  3. 完全性
  4. 可用性

3．基本原則

- 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
  - 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
- 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、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
  - 両者の接続によって所要の安全性や性能を満たさない、法令違反等になる懸念
  - 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
  - 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
- **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**
  - **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
  - **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
- IoTシステムの設計･構築･運用
  - 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
  - 当該システムの**稼働前に確認･検証**できる仕組み
  - **IoTシステムのセキュリティ確保のための要件の明確化**

3．基本原則

- 検討を要する事項

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

4．取組方針

1. **要求事項の明確化**
   - 関連する法令･規制要求事項等の明確化
2. **IoTシステムのモデル化**
   - 分析･検討を行う等適切なモデル化を行い、そのモデルを参照しながら、セキュリティ要件を議論していく。
3. **リスクに応じた対応**
   - リスクアセスメントを適宜活用するもの
4. **性能要求と仕様要求の適切な適用**
   - 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。
5. **段階的･継続的アプローチ**
   - 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。
6. **役割分担及び連携した対処のあり方の明確化**
   - IoTシステムに関連する者の役割分担の明確化
   - 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の明確化
7. **その他運用ルールの検討**
   - IoTシステムとの連携、データの利活用、個人情報保護の仕組み等
   - 機器認証の在り方等

5．情報技術(IT)　からの視点
運転技術(OT)　からの視点

ITとOTとの歩み寄りからIoTが始まる

IT+OT=IoT？

- 情報技術（IT)と運転技術(OT)の融合
  - 米国でも日本でもITとOTは相性が悪い
    - 情報通信技術の目覚ましい進歩
    - 多機能化、省力化の必要性
- 便利なITを上手にOTに使うことこそ時代の要請
    - NISCの安全なIoTの枠組み第3章柱書はこうした背景から記載
- 異文化コミュニケーションの始まり
    - あらゆるモノが繋がる
    - 異文化を受け入れる寛容さが必要

SCIAを産業別に考える

セキュリティの要素	安全（S）	機密性（C）	完全性（I）	可用性（A）
情報セキュリティ		●	●	●
モノづくり	●		●	●

- 情報セキュリティ分野からのアプローチ
  - 安全性を強化する
- モノづくりからのアプローチ
  - 機密性を強化する

**これまでの業種の強みを活かし、
弱いところを補強し、
相互に連携することが益々重要となってくる**

6．これまでの経験からのIoT

学生時代のICS研究→レガシープラント運転保守
→新規プラント設計建設→原子力安全規制→電力安全規制
→製品安全→サイバーセキュリティ

業務用プラントの運転、保守管理、設計建設の経験から

- **初任地の業務用プラントでのレガシーショック**
  - 大学で計測制御を専攻、コンピュータによる制御を志す
  - 1985年初任地でハードワイヤードシーケンス（H/W)による業務用プラントに従事
  - レガシー過ぎて、現実を受け止められないショックを受ける
  - コンピュータ制御に実験しようと提案したら、「商売道具であることを理解しろ」と諭される
- **現場の先生である父から受けた説得**
  - 「世の中のほとんどがリレーシーケンス（H/W)であることを受け止めよ」
  - それ以降、プラントの運転、保守の経験を重ねるにつれ、過去の歴史から人間工学を踏まえた信頼性重視設計であることを知る
- **PLCやデジタル制御導入のジレンマ**
  - 1990年代コストカットで渋々シーケンサ(PLC)やLANを導入
  - マスコンからマウスオペレーションに切り替えの苦渋の決断
    - 運転員は反対するとの予想に反して、使い勝手が良いとの評判にショックを受ける
    - 設計、建設したプラント3か所(特高変電所及び送電線、水力発電所、工業用水道プラント)
  - このころからITベンダがプラントの制御系に進出し、信頼性設計、安全性、運転知見を理解しようとしない強引さにショックを受ける‥結局信頼性低下によるトラブル頻発を経験
  - 重要部はH/W、コストカットはデジタル制御という記憶のまま、1991年プラント実務から去る

原子力安全設計審査･検査での経験

- 安全設計思想
  - 確率論的安全評価(リスク情報の活用)
  - 法令遵守、ルールベース
  - フェールセーフ
  - 機能別安全重要度区分
  - 信頼性
  - 冗長性(多重性、多様性、独立性)
  - Quality Assurance
  - ヒューマンファクター
  - サプライチェーンマネジメント、検査･検定制度
  - ホールドポイント＆リリース
  - Operation & Maintenance (O&M)

火力安全規制からの経験

- 一つのルール(電気事業法)による多様な事業主体の共存
  - 火力の一般則
    - 問題があれば、止めて修理し、確認後運転するといった事業者の裁量が多い
    - その前提には、**技術基準という統一的なルールの存在**
  - 溶接検査
    - 原子力事業者、電力会社から自家発電まで電気事業法で共存
    - 法目的を達成するための方法を**事業者の規模、性質によって区分**するよう制度改正して、**事業者の自主性を高めるインセンティブ規制**に制度変更
    - 同じ法の下でも、保安の方法の**バリエーションを提供することで、円滑な運用**を行うことができた

電気用品安全規制での経験

- 1962年に制定されたルールを抜本的に改正
  - 高度成長期の追い付け追い越せの時代背景
    - ローテク品の大量生産には適した仕様規定を国が制定し、保証
    - 50年経過した2009年でもそのルールが変わらず、ハイテク品の新規開発には向いていない
  - **仕様規定から性能規定**へ抜本改正
    - 2009年から検討を開始し、2013年に数百ページにわたる技術基準を20条からなる性能規定に改正
    - **事業者の裁量により、新技術導入を容易**にした
    - しかし、長年の政府保証に慣れた事業者には、自己責任で新たなチャレンジをすることが進まず、昔のように国が詳細仕様を定めたほうが良いという意見まで出てくる始末
    - 日本には米Apple型企業は生まれる風土はないと感じる

製品安全サイドからのIoTに対する過去のアプローチ(2012-13年度)

遠隔操作に対する技術基準の解釈の追加要望
(平成25年3月8日電気用品調査委員会)
http://www.eam-rc.jp/pdf/result/remote.pdf


遠隔操作に対する技術基準の解釈の追加要望

平成25年3月8日
電気用品調査委員会

目次

- 電気製品の遠隔操作は、過去に音声式リモコンの誤動作から火災を起こし、国会審議(1972年3月8日衆議院)によって、原則禁止になった。
- 昨今のモバイル通信の低価格化を踏まえ、遠隔操作の規制緩和を規制当局から業界へ提案(2012年2月15日)
- 電気用品の遠隔操作に関する電安法技術基準解釈の改正(2013年5月10日)
- 製品安全に関する法令要求を踏まえたIoTのアプローチの事例として紹介
- IoTにつながるモノ側からのアプローチの例は、モノによって異なると思われるが、手順は基本的に統一できるのではないかと思われる。
- なお、この事例では、機密性については十分考慮されていない。

遠隔操作の追加検討の必要性

【旧来の遠隔操作】
赤外線リモコンなど
機器が見える位置から操作

操作する人が電気用品の
状況を直視できる。

【これからの遠隔操作】
インターネット回線を利用して、機器が
見えない位置から操作

操作する人が電気用品の状況を直視できない。

インターネットの普及による利便性要求への対応

この間のリスクについて検討

遠隔操作に関する技術基準改正の経緯 (2012-2013)

【2012.2 技術動向を踏まえ全面禁止としている遠隔操作の限定解除を関係業界に提案】
A. 遠隔操作機構の誤動作により危険が生じない用品
B. 遠隔操作機構の誤動作が危険となる可能性がある電気用品
C. 遠隔操作により人がいない状態で使用されると危険となる可能性がある電気用品

【2012.5.10 業界回答】
「エアコンを例にして、使用される状況によって危険性が変化することを考えると、製品毎の要求レベルを決めることはできない」などの回答。エアコンでさえ、危険となる可能性があるとの指摘。

当初、TF設置を呼びかけるもメンバー集まらない。

2012.9 大手メーカーはスマホで遠隔操作可能なエアコン発売のプレス発表。

関係課（情通課、情経課、電安課、製安課）及びメーカー6社等で対応を協議し、迅速な対応策を検討することとした。

2013.3.8 電気用品の固有の安全性、遠隔操作に伴うリスクを踏まえ、**7項目の追加条件が必要**として改正提案を発表
（官民連携による20回以上にも及ぶTF等実施）

2013.5.10 電安法技術基準の解釈改正。これを機にリスクを考慮した製品が市場に発売された

電気用品安全法での検討事項

室内外から家電製品を遠隔操作するため、安全確保を前提に、遠隔操作の範囲を次のように拡大するための検討を行った。

1. 遠隔操作可能な電気用品の明確化
遠隔操作を行っても危険の生じるおそれのない電気用品の考え方を明確にする。

2. 遠隔操作を行う場所の拡大
動作状況を操作者が直接確認できる範囲内から室内外からの遠隔操作へと拡大する。その際、動作状況が直接確認できない場所からの遠隔操作を安全、確実に行うため、所要の対策を講じる。

3. 遠隔操作に使用する通信方式の拡大
動作状況を操作者が直接確認できる範囲内の通信方式として、赤外線、電力線搬送波、音声の3種類が規定されていたが、近年の技術の進歩に伴い各種通信方式を柔軟に採用できるように、室内外から安全、確実に遠隔操作するための通信方式に対する要求を明確にする。

電気用品安全法が求める“危険が生じるおそれがない”とは

〔技術基準の解釈（当時、省令）〕

解釈別表第八　令別表第1第6号から第9号まで及び別表第2第7号から第11号までに掲げる交流用電気機械器具並びに携帯発電機
1　共通の事項
(2)　構造
イ　**通常の使用状態において危険が生ずるおそれのない**ものであつて、形状が正しく、組立てが良好で、かつ、**動作が円滑であること**。

遠隔操作においては、次を満たすことにより、“危険が生じるおそれがない”と見なされる。

1. 通常の使用状態（合理的に予見な可能誤使用を含む）において危険が生ずるおそれがない。
2. 動作が円滑である。

室内外から遠隔操作を行うために必要な安全確保対策Ⅰ
【通常の使用状態において危険が生ずるおそれがない】

①通信回線の故障に対して電気用品が安全な状態を維持すること

使用者により公衆回線を含めた遠隔操作に使用する通信回線の品質確保を徹底できないため、電気用品の安全性が通信回線の一時的な途絶や故障にみだりに左右されないよう、**電気用品自身で最終的な安全を確保することを基本**とする。
なお、遠隔操作に使用する通信回線が故障し、復旧の見込みがない場合は、遠隔操作される電気用品の安全機能により安全な状態を確保する。

②遠隔操作を行うことができる電気用品の判定方法の明確化

リスクアセスメント手法を活用し、遠隔操作に伴う使用及び予見可能な誤使用を踏まえて、遠隔操作可能な電気用品と不可能な電気用品に分類する。

③不意な動作の抑制対策を講じること

遠隔操作によって危険が生じないよう、**不意な動作の抑制対策**を施す。

室内外から遠隔操作を行うために必要な安全確保対策Ⅱ
【動作が円滑である】

④動作が確実であること

遠隔操作を行うコントローラーの操作が確実に行われるよう、所要の対策を講じる。

⑤使用する宅内通信回線において動作が円滑であること

スマートフォン等外部から操作を行う際、宅内通信が健全でなければ、外部からの操作が不可能であるため、使用する宅内通信は動作が円滑であるものとする。また、遠隔操作を安全･確実に行うために、通信方式に対する要求を明確化する。

⑥公衆回線を利用する場合の安全対策が施されていること

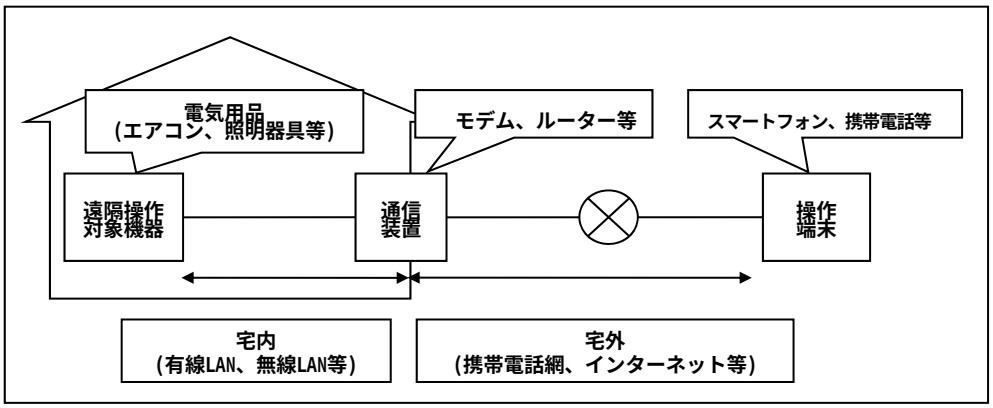
スマートフォン等公衆回線を使用する場合においては、ビル内や地下などの圏外への移動、電池切れ、震災時の長期間にわたる通信障害の発生などを踏まえ、公衆回線の一時的途絶や故障によって電気用品の安全性に影響を与えないようにする。

⑦適切な誤操作防止対策が施されていること

スマートフォン等を遠隔操作に使用する場合、タッチパネル等の特性を考慮しつつ、様々な人が機器を操作することを前提に、人間工学やユニバーサルデザインを考慮した設計を行う。

1．通信回線の故障に対する安全状態の維持

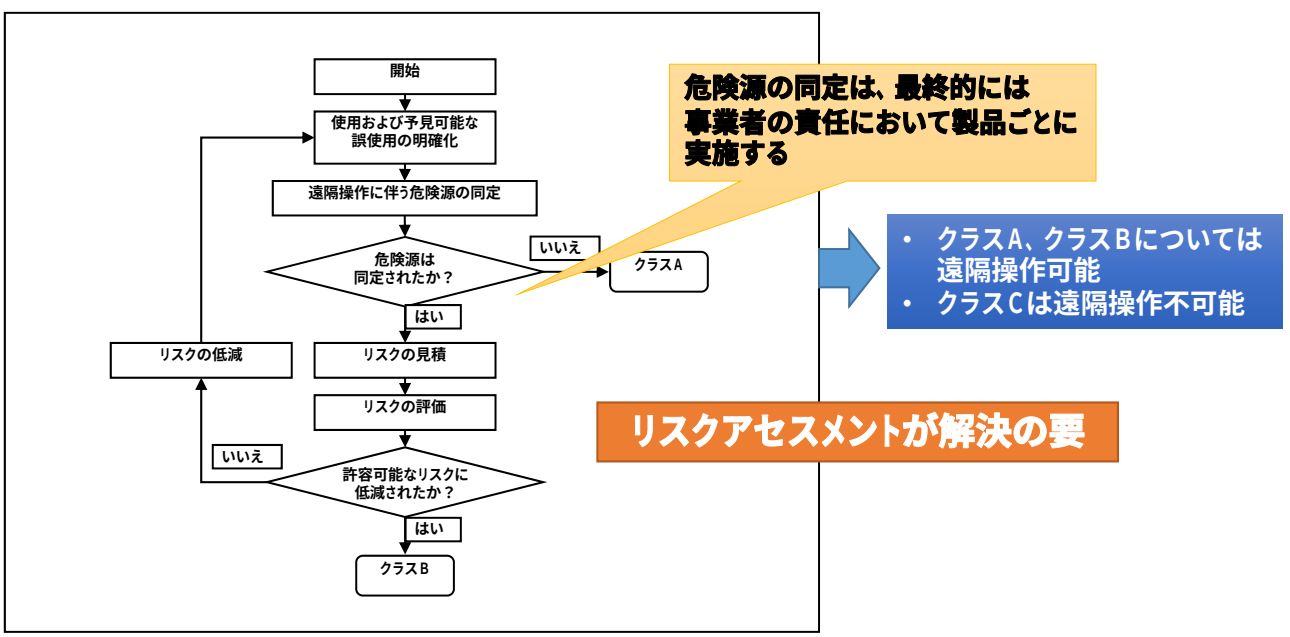
安全状態を確保するとは、「IEC 60335-1（家電機器の安全性通則）第5版22.49項」を参考に、通信回線故障時には直ちにもしくは一定時間後に「電源を切る」ことを基本とし、危険が生じることがない場合は「故障前の状態を維持」とする。



※ 照明器具などは、故障前の状態を維持しても危険がないものとされているが、エアコンは、施工上の問題も含めると事故例の多さから、通信回線故障時には「電源を切る」ものとしている。

2．遠隔操作を行うことができる電気用品の判定方法

○クラスA 遠隔操作に伴う危険源の無いもの
○クラスB 遠隔操作に伴い危険源が同定されるがリスクアセスメントによって、危険が生じるおそれのないと評価されるもの
○クラスC 遠隔操作を行うことによって、危険が生じるおそれのあるもの、あるいは遠隔操作を意図していないもの



3．不意な動作の抑制対策を講じること

遠隔操作は、特に操作者が機器の見えない位置から操作する場合に、
機器の近くにいる人が危険な状態になることが考えられる。
このため、機器の近くにいる人が危険を感じた場合に対応できるよう、
次に示す遠隔操作における不意な動作の抑制対策を講じる。

1. **手元操作**は、遠隔操作よりも**優先**されること。
2. **遠隔操作回線の切り離し**ができること。

4．動作が確実であること

1. 操作結果のフィードバック

動作状況を操作者が確認できない位置からの遠隔操作も対象とするため、直接確認可能な場合と同等の確実性を求めるには、操作結果が遠隔操作を行うコントローラーにフィードバックされ、操作が失敗した場合、再操作が行われるものとする。

単方向の赤外線リモコンを遠隔操作に使用する場合など、
通信にフィードバックがない場合

2. 動作保証及び使用者への注意喚起

- 公表している赤外線リモコンの保証到達距離になるような位置に遠隔操作装置を設置し、確実に動作することを確認する。
- 使用条件や設置条件により動作の確実性が保証されない場合もあることから、赤外線リモコンと遠隔操作される電気用品の設置条件、設置時の動作確認、障害物による動作支障、リモコンの電池切れによる動作支障など、これらの付帯事項を取扱説明書等に記載する。

5．使用する宅内通信回線において動作が円滑であること

1. **識別管理**

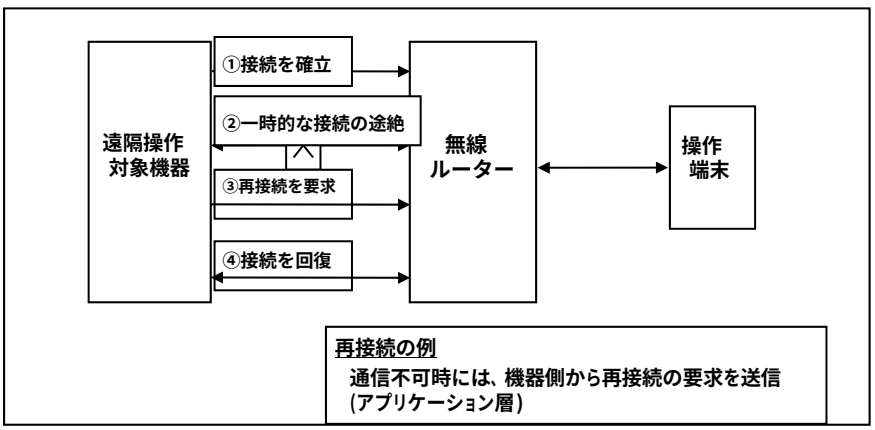
→ 関連付けされた遠隔操作機構以外からの遠隔操作は受け付けない。

2. **誤動作対策**

→ 外来ノイズなどにより正しい操作信号が伝送できず、誤動作しないような物理的、論理的な誤動作防止対策が施されている。（イミュニティ試験の実施）

3. **再接続機能(常時ペアリングが必要な通信方式に限る)**

→ ペアリングが切断された場合、自動的に再ペアリングを行う機能を有する。



6．公衆回線を利用する場合の安全対策が施されていること

公衆回線の一時的途絶や故障によって電気用品の安全性に影響を与えないよう電気用品側で安全対策を講じる。

スマートフォン等を遠隔操作に使用することを想定している
スマートフォン等においては、ビル内や地下などの圏外への移動や
電池切れや、震災時の長期間にわたる通信障害の発生などを
踏まえ、**公衆回線の一時的途絶や故障によって電気用品の安全性に影響を与えないよう電気用品側で設計上の配慮**を行う。

7．適切な誤操作防止対策が施されていること

○ユニバーサルデザインを考慮した操作設計

1．不用意な操作を避けたい操作ボタンは、他の操作ボタンなどから離している。

2．不用意な操作を避けたい操作ボタンに対し、ダブルアクションによる決定、スクリーンロックによる誤操作防止機能が付いている。

3．意図しない操作に対し、少ない手順で元の状態へ復帰するか、やり直しができる。

○通信機能を熟知していない使用者への配慮

4．遠隔操作機能を不要と考えている人が、その機能の無効にする方法が分からず、知らない間に勝手に動作することなども考えられる場合は、**出荷状態において、遠隔操作機能を無効**にしておく。

○同時に外部の2か所以上から遠隔操作する場合の設計上の配慮

5．同時に外部の2か所以上から遠隔操作する場合、**相反する操作を抑制する対策**を講じる。

→ 具体的には、ユーザーIDとパスワードを割り振る識別管理、操作者以外の操作を抑制する仕組みなどを基本とした対策をとる。

電気用品の遠隔操作の安全確保要件検討のまとめ

- 遠隔操作によって生じるリスクアセスメントと万一の対策を検討
- 宅外からの遠隔操作は、**遠隔操作を行っても危険が生じるおそれがない電気用品**とする。
- 遠隔操作を付加する場合、公衆回線の品質はメーカー･ユーザーともに管理できないことを前提に、**安全性、完全性、可用性**の観点から**7つの項目**を追加
- ポイントは以下の通り
  - 電気用品が有する固有の安全性を基本とする
  - 電気用品の近くにいる人が遠隔操作よりも優先して操作できるようにする
  - 人の意図通りの操作が行われたかどうかを操作者にフィードバックする
  - 通信手段が途絶え一定期間以上経過したら、安全な状態に遷移する
  - 消費者に対して、遠隔操作機能付加による「メリット」とともに、「デメリット」について、正しい使用方法の説明、使用上の注意も併せて強化

7．おわりに

IoTの爆発的な流行の前に標準化

- 過去の歴史から学ぶ
  - 萌芽期の**「使えればよい」**というまま、**将来を考えずに発展させる**と、ある時点で後戻りできなくなり、**発展性にも、経済的にも支障をきたす**という**知見の反映**
  - **将来を見据えたIoTの標準化を図ることができる時期は今しかない**
- 設計思想、信頼性が異なる様々なものがつながっていく
  - つながるモノの性質を踏まえて、つなげることの**ベネフィット**と**リスク**を勘案して、どうつなげるべきか、どうリスクを分散させるかを考える
  - 異文化コミュニケーション、相互信頼、協働、協業が重要
- データの相互利用の円滑化の前提
  - あらかじめ、責任分界点、データの標準化、プライバシー等を検討することが大前提

内閣サイバーセキュリティセンター

ご清聴ありがとうございました