JNSA標準化部会ビギナーズセミナー

ISO/IEC における IoTセキュリティ標準化

2022年11月16日

国立研究開発法人 情報通信研究機構 (NICT)
山下　真
ISO/IEC JTC 1/SC 27/WG 1, WG 4

自己紹介

現職　　国立研究開発法人 情報通信研究機構（NICT）
サイバーセキュリティ研究所

経歴　　民間企業でミドルウェアの開発と社内の情報セキュリティ施策を担当
2018年より現職

標準化活動

2009年に ISO/IEC JTC 1/SC 27 における標準化活動に加わり、以後、ISO/IEC 27001, ISO/IEC 27002 を中心とする情報セキュリティマネジメントに関する国際標準等の開発に参加。

はじめに

　この講演では、ISO/IECにおけるIoTセキュリティの標準化について以下の側面を解説します。

- 標準化組織
- 関係する国際標準文書
- IoTセキュリティのガイドラインを示す ISO/IEC 27400 の概要
- ISO/IECにおけるIoTセキュリティ標準化の意味

1. IoTセキュリティ標準化を担当する国際組織

ISO: International Organization for Standardization　国際標準化機構

IEC: International Electrotechnical Commission　国際電気標準会議

JTC 1: Joint Technical Committee 1, “Information Technology”

SC 27: Subcommittee 27, “Information security, cybersecurity and privacy protection
「情報セキュリティ、サイバーセキュリティ及びプライバシー保護」

https://www.iso.org/committee/45306.html

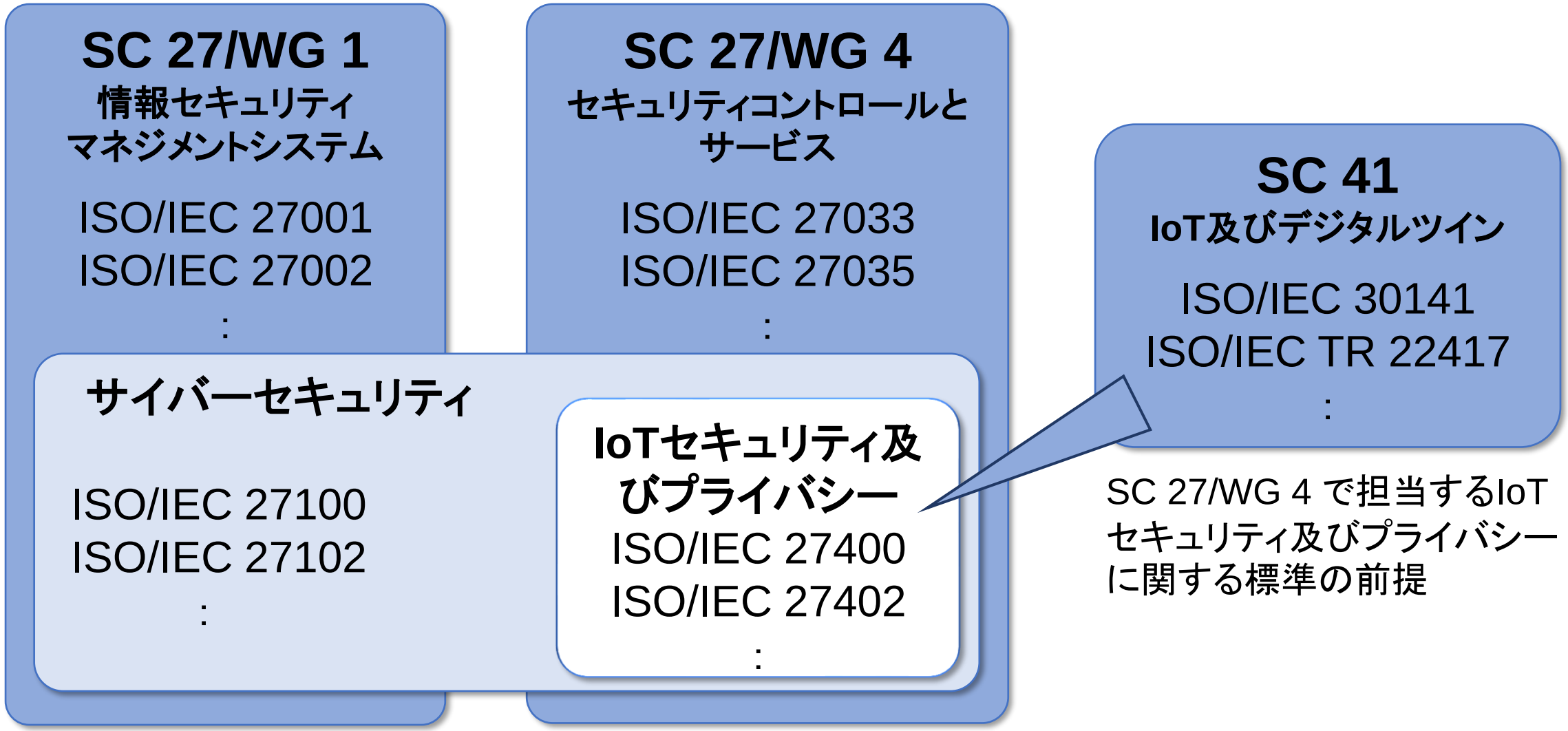
https://committee.iso.org/home/jtc1sc27

WG 4: Working Group 4, “Security controls and services”
「セキュリティ・コントロールとサービス」

2. 国際組織と国内組織の対応

国際組織	国内委員会
JTC 1	情報規格調査会 https://itscj.ipsj.or.jp/index.html 技術委員会
SC 27	SC 27 専門委員会
WG 4	WG 4 小委員会

3. IoTセキュリティとその周囲の標準化分野



4. IoTセキュリティの標準文書

番号、標題	内容	備考
ISO/IEC 27400, Cybersecurity – IoT security and privacy – **Guidelines**	● IoTのセキュリティ及びプライバシーに関する基本文書 ● 事業者向けと利用者向けの指針を管理策（コントロール）として示す ● IoTシステムにおけるリスク源を提示	2022年6月出版
ISO/IEC 27402, Cybersecurity – IoT Security and Privacy – **Device baseline Requirements**	● IoT機器の基礎的な要求事項 ● IoT機器の要求仕様を策定する際に本文書を活用することを想定	Committee draft から Draft International Standardへ
ISO/IEC 27403, Cybersecurity – IoT security and privacy – **Guidelines for IoT-domotics**	● ISO/IEC 27400 を前提として、居住環境においてIoT機器を使う場面での考慮を追加 ● 事業者向け指針	Committee draft から Draft International Standardへ
ISO/IEC 27404, Cybersecurity – IoT security and privacy – **Universal cybersecurity labelling framework for consumer IoT**	● 消費者用IoT機器のセキュリティ・プライバシー評価基準と評価のラベリング	NWIP（新規提案）

5. ISO/IEC 27400 の構成

1. 適用範囲
2. 引用規格
3. 用語及び定義
4. 略語
5. IoTの概念
6. IoTシステムにおけるリスク源
7. セキュリティ及びプライバシーの管理策
    7.1 セキュリティ管理策
    7.2 プライバシー管理策

この規格の開発にあたり、日本から「IoTセキュリティガイドライン ver 1.0」（IoT推進コンソーシアム、総務省、経済産業省）の内容を提案

6. IoTシステムの例

IoTシステムの適用例が、次の文書に多数掲載されている。

ISO/IEC TR 22417:2017, Information technology — Internet of things (IoT) use cases

- 個人利用者向け
  - スマート・ホーム・システム
- 産業システム
  - プラントの制御、装置の遠隔管理 （産業系制御システム又はその一部として）
  - 倉庫の物品管理
  - 農業における生育管理
- 災害監視・警報システム　　等々

7. IoTシステムの特徴 － ISO/IEC 27400 －

IoTシステムの一般的な特徴： ISO/IEC 27400 より（要約）

- IoTシステムは、用途に応じたIoT機器を構成要素に持つ。
- IoT機器は、
  - 物理的なモノや状態とつながりを持って働く。
  - ネットワークに接続し、データを受信し送信する。
  - 多くは、対象の状態や動きなどを感知する「センサー」を持つ。
  - 対象の状態や動きなどを制御する「アクチュエータ」を持つものもある。
- IoTシステムのアプリケーションは、
  - IoT機器で感知したデータを処理し、制御データを送出する。

8. IoTシステムの関係者　－ ISO/IEC 27400 －

ISO/IEC 27400 では、ISO/IEC 30141（※）に定める IoTシステムの関係者（stakeholders）である

- IoTユーザ (IoT user)
- IoTサービス開発者 (IoT service developer)
- IoTサービス提供者 (IoT service provider)

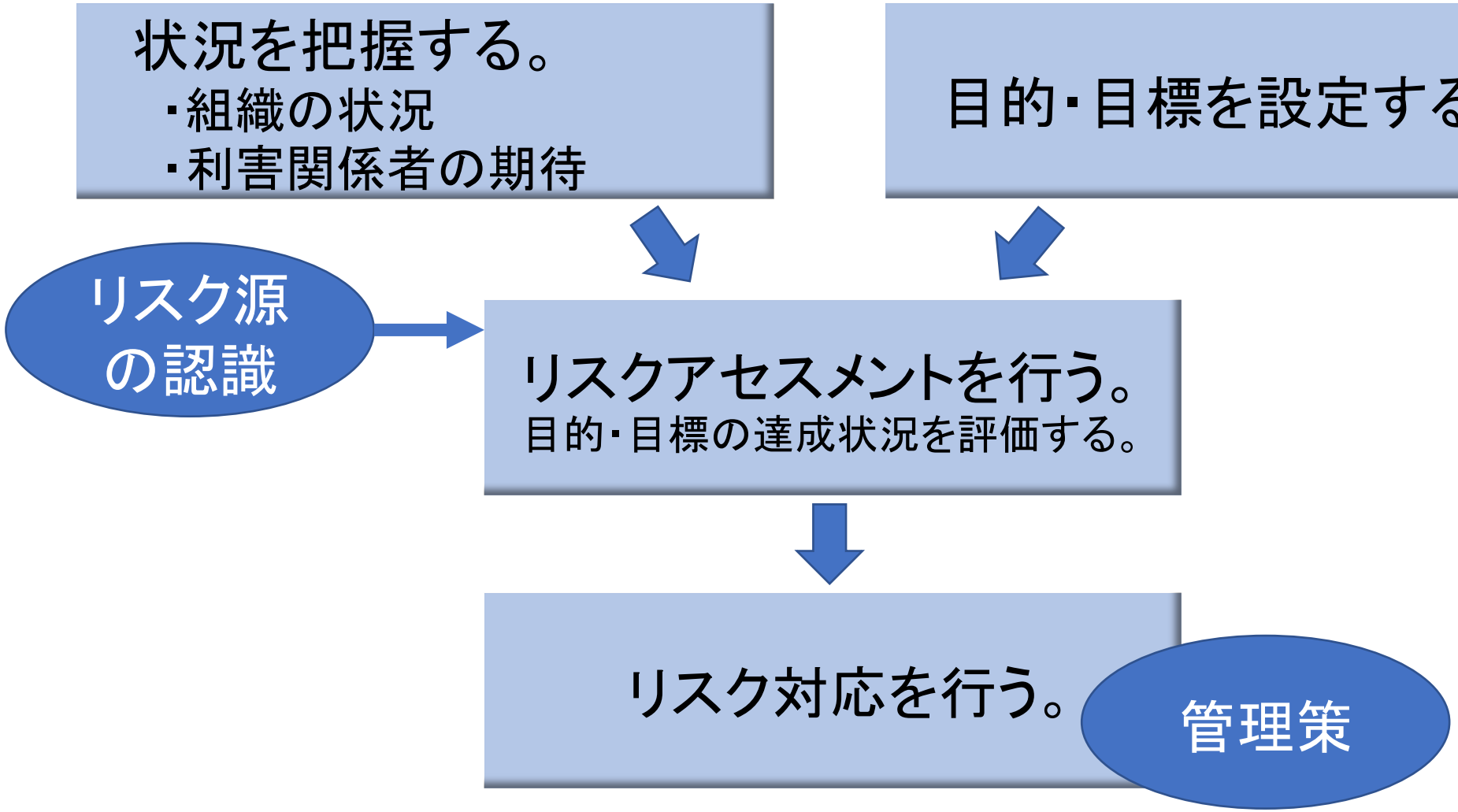
に向けて、それぞれの立場で実施するセキュリティ及びプライバシーの管理策を例示している。

※　ISO/IEC 30141,
　　Internet of Things (IoT) – Reference architecture

9. ISO/IEC 27400 で想定するリスクマネジメント

- セキュリティに関する文書において、管理策（対策）を示す例がある。
  - 国際標準においても、製品・サービスの説明においても、管理策が必要とされ有効な場面の認識につながる説明があると理解しやすい。
  - ISO/IEC 27002:2022 では、管理策ごとに Purpose を記載。
- ISO/IEC 27400 は、管理策ごとに Purpose を記載し、さらにリスク源も示している点に特徴がある。
  - IoTサービス開発者、IoTサービス提供者が、リスクマネジメントを通してIoTサービスに備える管理策を決定することを想定。
  - リスクマネジメントにおいて、リスクシナリオの中で上流にある要素として認識すべきリスク源（リスクを生じさせる可能性を持つもの）を例示。
  - リスクマネジメントは一般的なプロセスを採用することを想定し、ISO/IEC 27400 では説明していない。

10. 組織のリスクマネジメント･プロセスの概略



11. IoTにおけるリスク源　― ISO/IEC 27400 ―

- リスク源とは:　リスクを生じさせる可能性を持つもの
- ISO/IEC 27400 では、場面ごとに典型的なリスク源を列挙

例:　共通（場面によらない）のリスク源

a. IoTシステム／アプリケーション／サービスの脆弱性
b. 関係者の知識不足、技能不足
c. 人的エラー
d. 悪意を持つ攻撃者の存在
e. IoTシステム／アプリケーション／サービスの品質不良
f. サイバー攻撃に悪用される外部のシステム・機器の存在　　等

12. 管理策とリスクの定義　－ ISO/IEC 27400 －

- ISO/IEC 27400 において、「管理策」と「リスク」の定義は
  ISO 31000 における定義を採用している。

  管理策の定義：

  リスクを維持又は修正する対策

  リスクの定義：

  目的に対する不確かさの影響

  すなわち、リスクとは、
  「目的」と「管理策を実施した結果として想定する状態」の乖離
  （の影響）

ISO 31000, Risk management – Guidelines

13. 管理策の例　－ ISO/IEC 27400 －（1）

IoTサービス提供者・開発者向け:　24項目より

a. サービスを提供し又は開発する組織として、組織内の役割及び責任を定め、割り当てる。[7.1.2.2]
b. IoTシステムの設計・開発において、セキュリティ対策を組み込む。[7.1.2.7]
c. IoTシステムの設計・開発において、安全性確保に寄与するセキュリティ対策を組み込む。[7.1.2.9]
d. IoT機器及びIoTシステムの設計を検証する。[7.1.2.11]
e. IoT機器及びIoTサービスの提供時（出荷時）に、セキュリティを考慮した構成と設定を適用する。[7.1.2.15]
f. ソフトウェア及びファームウェアの更新を提供する。[7.1.2.17]

14. 管理策の例　－ ISO/IEC 27400 －（2）

IoT利用者向け:　4項目

a. サポート窓口が提示されているIoT機器・IoTサービスを使う。
b. IoT機器・IoTサービスの初期設定を正しく行う。
c. 使わなくなったIoT機器は、認証情報を無効にして、電源を切る。
d. IoT機器は、廃棄又は再利用する前に、データ及びソフトウェアを消去する。

15. IoTセキュリティの標準文書　再掲

番号、標題	内容	備考
ISO/IEC 27400, Cybersecurity – IoT security and privacy – **Guidelines**	● IoTのセキュリティ及びプライバシーに関する基本文書 ● 事業者向けと利用者向けの指針を管理策（コントロール）として示す ● IoTシステムにおけるリスク源を提示	2022年6月出版
ISO/IEC 27402, Cybersecurity – IoT Security and Privacy – **Device baseline Requirements**	● IoT機器の基礎的な要求事項 ● IoT機器の要求仕様を策定する際に本文書を活用することを想定	Committee draft から Draft International Standardへ
ISO/IEC 27403, Cybersecurity – IoT security and privacy – **Guidelines for IoT-domotics**	● ISO/IEC 27400 を前提として、居住環境においてIoT機器を使う場面での考慮を追加 ● 事業者向け指針	Committee draft から Draft International Standardへ
ISO/IEC 27404, Cybersecurity – IoT security and privacy – **Universal cybersecurity labelling framework for consumer IoT**	● 消費者用IoT機器のセキュリティ・プライバシー評価基準と評価のラベリング	NWIP（新規提案）

16. IoTセキュリティにおけるリスク対応の構成

- IoTセキュリティ対策は、国際的な、国としての、あるいは組織としてのそれぞれの貢献を組み上げて構成する。
  - 社会的強制力・誘導：
    - 法令・規制、行政指針、業界規制・指針、政策
  - 事業者：
    - 組織のマネジメント
    - 技術、運用
  - 知識・リテラシー・意識の向上、蓄積・継承

- 国際標準は、
  - これらの活動の基礎となる概念と知識の共有を支える。
  - 国内標準・指針との間で成果を共有しつつ展開する。