ISO/IEC 27000 ファミリー規格の最新動向

2020年12月18日

国立研究開発法人 情報通信研究機構 (NICT)
山下　真
ISO/IEC JTC1 SC27 WG1, WG4 エキスパート

目　次

国際標準化組織

JTC 1: 情報技術 (Information technology)

SC 27: 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

WG 1: 情報セキュリティマネジメントシステム

WG 4: セキュリティ・コントロールと
セキュリティ・サービス

ISO/IEC 27000 ファミリー規格概観　1/5

文書番号	内容	備考
ISO/IEC 27000:2018	ISMS－概要及び用語 （JISは用語部分を採用）	
ISO/IEC 27001:2013	ISMS－要求事項	
ISO/IEC 27002:2013	情報セキュリティ管理策の実践のための規範	改定作業中 DIS
ISO/IEC 27003:2017	ISMS－指針	
ISO/IEC 27004:2016	情報セキュリティマネジメント－監視、測定、分析及び評価	
ISO/IEC 27005:2018	情報セキュリティ・リスクマネジメント	改定中　CD

ISO/IEC 27000 ファミリー規格概観　2/5

文書番号	内容	備考
ISO/IEC 27006:2015	ISMSの審査及び認証を行う機関に対する要求事項	
ISO/IEC TS 27006-2	ISMSの審査及び認証を行う機関に対する要求事項－第2部：　プライバシー情報マネジメントシステム（PIMS） ・分野別規格 ISO/IEC 27701：2019 に対応する認定のための要求事項	新規出版準備中
ISO/IEC 27007:2020	ISMS監査の指針	
ISO/IEC 27008:2019	情報セキュリティ管理策の評価指針	
ISO/IEC 27009:2020	分野別ISMS要求事項を定める規格に対する要求事項（規格開発者向け）	

ISO/IEC 27000 ファミリー規格概観　3/5

文書番号	内容	備考
ISO/IEC 27010:2015	セクター間及び組織間のコミュニケーションにおける情報セキュリティマネジメント	定期レビュー投票　投票期限は3月初旬
ISO/IEC 27011:2016	ISO/IEC 27002 に基づく通信事業者のための情報セキュリティ管理策の実践の規範	改定作業中 WD ・改定ISO/IEC 27002対応 ・ISO/IEC 27009対応
ISO/IEC 27013:2015	ISO/IEC 27001 及び ISO 20000-1 の統合実施の手引	改定作業中 DIS ・改定ISO/IEC 27000-1 対応

ISO/IEC 27000 ファミリー規格概観　4/5

文書番号	内容	備考
ISO/IEC 27014:2015	情報セキュリティガバナンス	改定版出版準備中
ISO/IEC 27016:2014	情報セキュリティマネジメントー組織活動の経済性	
ISO/IEC 27017:2015	ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範	定期レビュー投票　投票期限は3月初旬
ISO/IEC 27019:2017	エネルギー産業向け情報セキュリティ管理策	
ISO/IEC 27021:2017	ISMS専門家向け要求事項	

ISO/IEC 27000 ファミリー規格概観　5/5

文書番号	内容	備考
ISO/IEC TS 27022	ISMSプロセスモデルの指針 ・ISO/IEC 33004 に定めるプロセス参照モデルによる ISMSプロセスの記述	出版準備中
ISO/IEC TR 27023:2015	ISO/IEC 27001, ISO/IEC 27002 管理策の2005年版対2013年版対応表	

目　次

1. ISO/IEC 27000 ファミリー規格概観
2. ISO/IEC 27002 改定について
3. 分野別ISMS関連規格群の動向
4. サイバーセキュリティ と IoTにおけるセキュリティ/プライバシー関連規格群の展開

ISO/IEC 27002 改定の目的と方針　1/3

- 改定作業前の検討（2016/04−）の成果として、改定方針を決定（2017/10）:

1. 現行版の価値を継承する。
   a. 広汎な管理策群を提示
   b. 管理策の実施に向けて十分な手引を提供

2. 二つの用途に対応する。
   a. ISO/IEC 27001 と併用、これを補完
   b. 独立の手引書、参考書

ISO/IEC 27002 改定の目的と方針　2/3

3. 管理策体系の自由度を高める。
   2013年版の箇条5～18の構成は体系の一例。
   a. 管理策の分類を箇条5～8に簡素化：
      5. 組織の管理策、6. 人の管理策、
      7.物理的管理策、8. 技術的管理策
   b. さらなる分類の手がかりとして、管理策ごとに属性を付与する／付与可能とする。
      - ① CIA、② サイバーセキュリティ・フレームワーク　等
      - 組織独自の属性定義も想定する。
      - 2013年版との管理策対応表も、附属書として規格に含める。

ISO/IEC 27002 改定の目的と方針　3/3

4. 追加する管理策は、各国、各エキスパートごとの課題意識に基づくもの。
   - 改定方針（2017/10）において、管理策の追加・変更に関する方針（管理策案の受容可・不可判断基準等）を確立していたわけではない。
   - 管理策の追加・変更に関する提案と審議は、2017年10月以降の改定作業でも継続して行わることとなった。
5. 標題

   Information security controls

   情報セキュリティ管理策

最近の会議とその後の最新ドラフト

- 2020年9月～10月、SC 27/WG 1会合（リモート）にて 2nd CD へのコメントを審議
  - 7日間、通算20数時間
  - コメント数　約1800
  - 40名前後

- 審議結果を反映したDISが12月3日に配布された。
  - 投票・コメント期限は20週間後（4月22日）。

管理策の数 （ISO/IEC 27002, DIS）

章	管理策の数	2013年版から継承	新規
5. 組織の管理策	37	34	3
6. 人の管理策	8	8	0
7. 物理的管理策	14	13	1
8. 技術的管理策	34	27	7
全管理策	93	82 (89%)	11 (12%)

- 全管理策数は 114 (2013年版) から 93 に減少
- 89% の管理策は2013年版から継承（新旧対照表）
- 新規管理策は技術的管理策に集中

ISO/IEC 27002:2013 管理策の継承

2013年版管理策総数	改定版DISへ継承	改定版DISで削除
114	113	1

- 2013年版管理策のうち、削除したもの（新旧対照表）は 1 件：
  「11.2.5 資産の移動（持出し）」
  “Removal of assets”
- 113件は、DISで継承する管理策が特定されている（新旧対照表）。

ISO/IEC 27002, DIS　新規管理策　1/3

管理策	説明
5.7　脅威インテリジェンス	情報セキュリティに関する脅威情報の収集と分析
5.23　クラウドサービスの利用における情報セキュリティ	クラウドサービスの取得、利用、管理及び終了のプロセスの確立 組織が、特定のクラウドサービスの利用を検討し、利用する前に準備する、利用方針や利用手続きを整備することを想定している。
5.30　事業継続のためのICTの備え	事業継続のためのICTの備えの計画、実施、維持及び試験 ISO/IEC 27002:2013, 17.1.1, 17.1.2, 17.1.3 の情報セキュリティ継続は、DIS 5.29 に継承。 ISO/IEC 27002:2005, 14.1（事業継続管理における情報セキュリティの側面）を DIS 5.30 に継承。

ISO/IEC 27002, DIS　新規管理策　2/3

管理策	説明
7.4　物理セキュリティにおける監視	施設の常時監視（モニタリング）
8.9　構成管理	ハードウェア、ソフトウェア、サービス及びネットワークの構成の決定、文書化、実装、監視及び見直し
8.10　情報の消去	情報システム及び機器からの情報の消去
8.11　データマスキング	文書やデータを提供にあたって実施するアクセス制御の一つであるデータマスキング
8.12　データ漏洩の防止	機微なセンシティブ情報を扱うシステム、ネットワーク及びエンドポイント機器における漏洩対策

ISO/IEC 27002, DIS　新規管理策　3/3

管理策	説明
8.16　監視活動	ネットワーク、システム及びアプリケーションを対象とする監視と対処 ISO/IEC 27002:2013,「12.4 ログ取得及び監視」の管理策及び実施の手引において、監視の記述が不足していたことに対処する改善。
8.22　ウェブ・フィルタリング	外部のウェブサイトへのアクセスの管理
8.28　セキュア・コーディング	ソフトウェア開発におけるセキュア・コーディングの適用 ISO/IEC 27002:2013,「14.2.5 セキュリティに配慮したシステム構築の原則」の関連情報に、セキュア・コーディングに相当する簡潔な記述があった。これを新たに管理策にするもの。

ISO/IEC 27002 改定と ISO/IEC 27001:2013 の関係　1/5

2013年版とは異なり、今回は ISO/IEC 27002 改定の検討が先行している。その影響について、Q & A 形式で整理した。

Q1 ISO/IEC 27002 の改定版はいつごろ出版されますか？

A1 今月配布されたDISの次にFDISへ進むことを想定した場合、およそ1年後に出版となる可能性が高いと思われます。

ISO/IEC 27002 改定と ISO/IEC 27001:2013 の関係　2/5

Q2 改定版 ISO/IEC 27002 と ISO/IEC 27001:2013 が併存する場合、取得済のISMS認証に影響はありますか？

A2 取得済のISMS認証は、引き続き有効であると想定されます。ISMSの要求事項は ISO/IEC 27001:2013（本文と附属書A）で完結しているためです。
ISO/IEC 27002 の内容は、ISMSの要求事項を直接に規定するものではありません。

ISO/IEC 27002 改定と ISO/IEC 27001:2013 の関係　3/5

Q3 改定版 ISO/IEC 27002 と ISO/IEC 27001:2013 が併存する場合、改定版 ISO/IEC 27002 の用途は？

A3

(1) 情報セキュリティ管理策に関する、
ISO/IEC 27001 から独立した情報源として

(2) ISO/IEC 27001:2013 に基づく ISMS において、
ISO/IEC 27002:2013 を補う情報源として

- 既存の管理策に対する新しい手引
- 組織で独自に追加する管理策の材料

ISO/IEC 27002 改定と ISO/IEC 27001:2013 の関係　4/5

Q4 ISO/IEC 27001 の改定はいつごろになりますか？

A4 現時点では未定です。改定 ISO/IEC 27002 が DIS に至ったことから、ISO/IEC 27001 の改定について検討を始めることになると見られます。

ISO/IEC 27002 改定と ISO/IEC 27001:2013 の関係　5/5

Q5 ISO/IEC 27001 の改定では、何が変わると考えられますか？

A5 ISO/IEC 27002 を受けて、その管理策を附属書Aに反映することが考えられます。
マネジメントシステム規格の共通テキスト・共通用語定義が改定されていますので、その最新版を採用することも想定されます。
本文のその他の（共通テキスト以外の）要求事項は、今後の検討によって決めることになります。

目　次

分野別ISMS関連規格とは

- ISO/IEC 27001・・・ 汎用のISMS要求事項
- ISO/IEC 27002・・・ 汎用の情報セキュリティ管理策と手引
- 分野別 (sector-specific) ISMS関連規格

  ・・・ 分野に固有の要件を加えるために
  - 固有のISMS要求事項を追加
  - 固有の管理策、手引と関連情報を追加

分野： 事業分野 (domain)
適用分野 (application area)
市場 (market)

分野別ISMS関連規格の例：ISO/IEC 27017

- ISO/IEC 27002:2013 に対して追加：
  - クラウドサービス固有の7つの管理策とその手引・関連情報

    例：　CLD.6.3.1　クラウドコンピューティング環境における役割及び責任の共有及び分担

  - ISO/IEC 27002:2013 の管理策に対して、クラウドサービス固有の手引・関連情報
- 規格の種類：　手引/指針
- 規格の利用者：

  クラウドサービスカスタマ

  クラウドサービスプロバイダ

分野別ISMS関連規格の展開　1/4

分類1　管理策・手引（実施の手引）等の拡張

- ISO/IEC 27002 の拡張
- 規格の種類：手引/指針
  - 認証基準の分野別拡張はない。

- 規格例：
  - ISO/IEC 27011:2016　　通信事業者向け
  - ISO/IEC 27017:2015　　クラウドサービス カスタマ、クラウドサービスプロバイダ向け

分野別ISMS関連規格の展開　2/4

分類2　ISMS要求事項の拡張　（1/2）

- ISO/IEC 27001 と ISO/IEC 27002 の拡張
- 認証基準の拡張、手引/指針の拡張
- 追加管理策を、情報セキュリティリスク対応における参照管理策群に含める。

ISO/IEC 27001:2013,6.1.3）

b) 管理策を決定する。

c) 決定した管理策を拡張した参照管理策群（ISO/IEC 27001, Annex A 及び 分野別規格の Annex A）と比較する。

d) 適用宣言書を作る。管理策不採用の理由を説明する。

分野別ISMS関連規格の展開　3/4

分類2　ISMS要求事項の拡張　（2/2）

- ISO/IEC 27001:2013, 6.1.3 b), c) 以外のISO/IEC 27001 本文への追加も可能

- 規格例：
  - ISO/IEC 27019:2017
    エネルギー産業の制御システム
  - ISO/IEC 27701:2019
    プライバシー情報マネジメント（PIMS）
    ISO/IEC 27001:2013 本文（6.1.3 c), d) 以外）への要求事項追加あり

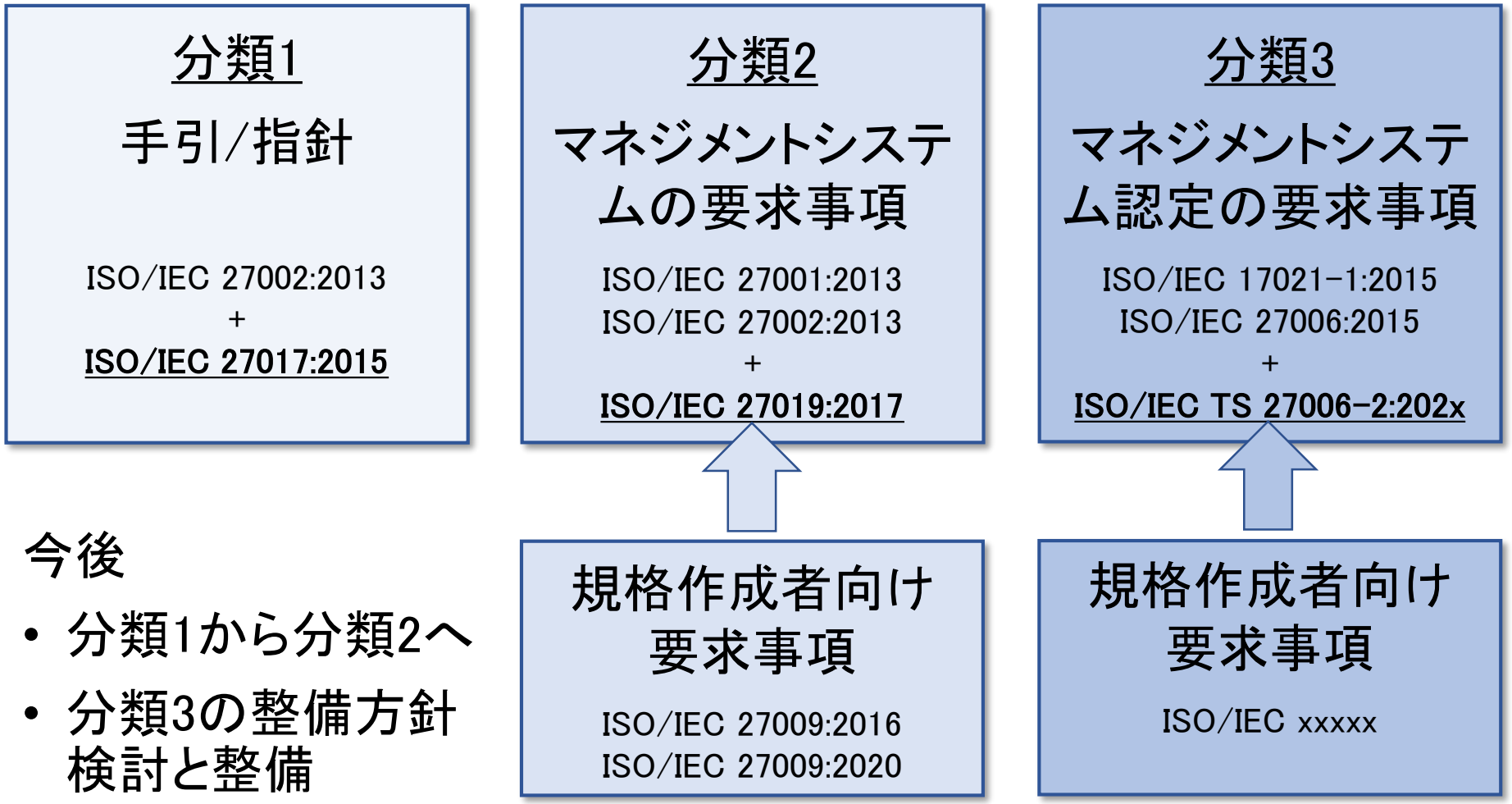
分野別ISMS関連規格の展開　4/4

分類3　ISMS認証機関に対する要求事項の拡張

- ISO/IEC 17021-1 と ISO/IEC 27006 の拡張
- 審査機関、審査員に対する要求事項を規定：認定基準の分野対応拡張

- 規格例：
  - ISO/IEC TS 27006-2:202x ISO/IEC 27001:2013 及び ISO/IEC 27701:2019 に基づく認証のための拡張認定基準
    - 拡張認定基準の先行事例をTSとして出版（TS発行後、ISへの改定を予定）

分野別ISMS関連規格の今後



今後

- 分類1から分類2へ
- 分類3の整備方針検討と整備

目　次

1. ISO/IEC 27000 ファミリー規格概観
2. ISO/IEC 27002 改定について
3. 分野別ISMS関連規格群の動向
4. サイバーセキュリティ と IoTにおけるセキュリティ/プライバシー関連規格群の展開

サイバーセキュリティ関連規格群　一般　1/2

文書番号	内容	備考
ISO/IEC TS 27100	サイバーセキュリティの概要及び概念	近く出版予定
ISO/IEC 27102:2019	情報セキュリティリスクマネジメントにおけるサイバー保険活用の説明	
ISO/IEC TR 27103:2018	サイバーセキュリティ・フレームワーク*とISO/IEC 27001、ISO/IEC 27002 その他の文書との対応関係	
ISO/IEC 27032	インターネット・セキュリティの指針 ISO/IEC 27032:2012, サイバーセキュリティの指針 から対象範囲を変えて改定作業中	改定作業中

TS: Technical Specification, 技術仕様書
TR: Technical Report, 技術報告書
*　Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2018

サイバーセキュリティ関連規格群　一般　2/2

文書番号	内容	備考
PWI (ISO/IEC TR 27109 予定)	サイバーセキュリティの教育・訓練	プロジェクト開始前検討中
ISO/IEC 27110	サイバーセキュリティ・フレームワーク策定指針*（規格開発者向け）	近く出版予定
PWI 5689	サイバー・フィジカル・システムの概要と参照アーキテクチャ **	プロジェクト開始前検討中

* Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2018 の内容と整合性がある。
** 「サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0」（経済産業省、2019年4月）を基礎に日本から提案したプロジェクト。

サイバーセキュリティ関連規格群　IoT関連

文書番号	内容	備考
ISO/IEC 27400	IoTにおけるセキュリティ及びプライバシーの指針* Cybersecurity – IoT security and privacy – Guidelines	作成中
ISO/IEC 27402	IoT機器のセキュリティ対策基本要求事項 Cybersecurity – IoT Security and Privacy– Device baseline requirements	作成中
ISO/IEC 27403	居住環境におけるIoTセキュリティ・プライバシーの指針 Cybersecurity – IoT security and privacy – Guidelines for IoT–domotics	作成中

* 「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、2016年7月）の内容を日本から提案し、この文書のセキュリティ管理策に反映されている。

サイバーセキュリティ関連標準化の成果　1/4

基本文書となる ISO/IEC TS 27100 の出版が確定したこの機会に、サイバーセキュリティ関連規格群検討の成果をまとめると　・・・

1. サイバーセキュリティの概要・概念について、評価・検討の対象となる文書を作った。
    - サイバーセキュリティの捉え方が多様で流動的な状況のもとで、一つの成果
    - 委員会（国際SC 27/WG1, SC 27/WG 4）の中でも、理解の共有が進展
        - ISO/IEC TS 27100 プロジェクト開始前の状態（2017年）とは大差

サイバーセキュリティ関連標準化の成果　2/4

2. 情報セキュリティとサイバーセキュリティの関係を文書にして示した。SC 27 ゆえの成果。
   - 重なりがありつつ視点は異なることの説明
     - ISO/IEC TS 27100
   - 情報セキュリティにの管理策や指針がサイバーセキュリティにも活用できる共通の財産であることの明示：　対応付けと参照
     - ISO/IEC 27002（改定）において、管理策にNISTサイバーセキュリティ・フレームワークの機能(Identify, Detect, Protect, Respond, Recover)を対応付け
     - ISO/IEC TS 27100 の中で、ISO/IEC 27035（情報セキュリティ・インシデント管理）、ISO/IEC 27036（供給者関係における情報セキュリティ）を参照。

サイバーセキュリティ関連標準化の成果　3/4

3. 国際的に通用する文書を作る上で必要な、国際標準化活動（SC 27 の活動）と各国国内標準・指針との間の交流がまわりはじめている。
   - サイバーセキュリティ・フレームワーク（NIST）との関係
   - 日本からの「IoTのセキュリティ・ガイドライン ver 1.0」の貢献

サイバーセキュリティ関連標準化の成果　4/4

4. IoTにおけるセキュリティ/プライバシーに関する指針の作成が進展している。
   - 国際的に共有しているリスク認識を基礎に、具体的な指針/手引の策定が進められている。
     - ISO/IEC 27400
       IoTにおけるセキュリティ及びプライバシーの指針
       Cybersecurity – IoT security and privacy – Guidelines
     - ISO/IEC 27402
       IoT機器のセキュリティ対策基本要求事項
       Cybersecurity – IoT Security and Privacy – Device baseline requirements

サイバーセキュリティ関連標準化　課題

1. 前提の安定性
   - サイバーセキュリティの概念や基本的理解について、今後もゆらぎが残ることから、文書の更新は必須。
   - ISO/IEC TS 27100 は、3年後の定期見直しが点検の機会となる。

2. 用語体系の整合性
   - サイバーセキュリティと情報セキュリティのそれぞれの用語体系がある。文書の相互活用や共通化に際して、不便を感じる。
   - 短期間での解決はなく、日常用語の展開を見つつ対応を考えることになる。

目　次

1. ISO/IEC 27000 ファミリー規格概観
2. ISO/IEC 27002 改定について
3. 分野別ISMS関連規格群の動向
4. サイバーセキュリティ と IoTにおけるセキュリティ/プライバシー関連規格群の展開