

ISO/IEC JTC1/SC27の動向

—IoTに関連した国際標準化活動の概観—

中尾康二
JNSA副会長、標準化部会長
主管研究員、情報通信研究機構（NICT）
客員教授、横浜国立大学

まず、“Cybersecurity”とは

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1205

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Overview of cybersecurity

ITU-T Recommendation X.1205: Overview of Cybersecurity

Recommendation ITU-T X.1205



Definition of Cybersecurity in 2008 (X.1205)

3.2.5 cybersecurity:

サイバーセキュリティとは、サイバー環境と組織およびユーザの資産を保護するために使用できるツール、ポリシー、セキュリティコンセプト、セキュリティセーフガード（対策）、ガイドライン、リスクマネジメントアプローチ、アクション、トレーニング、ベストプラクティス、保証、テクノロジーの集合体である。

services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality.

ISO/IEC 27032: Guideline for Cybersecurity

4.20

Cybersecurity (Cyberspace security)

Preservation (維持) of confidentiality, integrity and availability of information in the Cyberspace

NOTE 1 In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009.

FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/IEC
FDIS
27032

ISO/IEC JTC 1

Secretariat: ANSI

Voting begins on:
2012-04-26

Voting terminates on:
2012-06-26

Information technology — Security
techniques — Guidelines for
cybersecurity

*Technologies de l'information — Techniques de sécurité — Lignes
directrices pour la cybersécurité*

RECIPIENTS OF THIS DRAFT ARE INVITED TO
SUBMIT, WITH THEIR COMMENTS, NOTIFICATION
OF ANY RELEVANT PATENT RIGHTS OF WHICH
THEY ARE AWARE AND TO PROVIDE SUPPORT-
ING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS
BEING ACCEPTABLE FOR INDUSTRIAL, TECHNO-
LOGICAL, COMMERCIAL AND USER PURPOSES,
DRAFT INTERNATIONAL STANDARDS MAY ON
OCCASION HAVE TO BE CONSIDERED IN THE
LIGHT OF THEIR POTENTIAL TO BECOME STAND-
ARDS TO WHICH REFERENCE MAY BE MADE IN



Reference number
ISO/IEC FDIS 27032:2012(E)

© ISO/IEC 2012

ISO/IEC TS 27100 (2020) : Cybersecurity – Overview and Concept

3.2

cybersecurity

safeguarding of people, society, organizations and nations from cyber [risks \(3.7\)](#)

Note 1 to entry: Safeguarding means to keep cyber risks at a tolerable level.

3.7

risk

effect of uncertainty on objectives

Note 1 to entry: Cyber risk can be expressed as effect of uncertainty on objectives of entities in [cyberspace \(3.5\)](#).

Note 2 to entry: Cyber risk is associated with the potential that threats will exploit vulnerabilities in cyberspace and thereby cause harm to entities in cyberspace.

サイバーリスクから人、社会、組織、国家を守る(3.7)
注1「守る」とは、サイバーリスクを許容可能なレベルに保つことを意味する。

サイバーセキュリティの国際標準化

－目的、サイバーリスク、標準化の効果－

International CYBER Standards：目的

世界のサイバースペースコミュニティ、開発者、関係者の目的は、サイバー犯罪と闘うための国際的なサイバーセキュリティとプライバシーの標準を開発することである。

- 国際的なサイバー標準の導入は、組織や政府にとって次のようなことに役立つ：
- サイバーリスクの軽減と最小化
 - サイバー攻撃の影響と破壊的影響を最小化
 - 使用しているITベースのシステム、サービス、インフラへの投資を保護し、機密かつ重要な情報を保護

サイバーセキュリティリスク

• THREATS AND RISKS

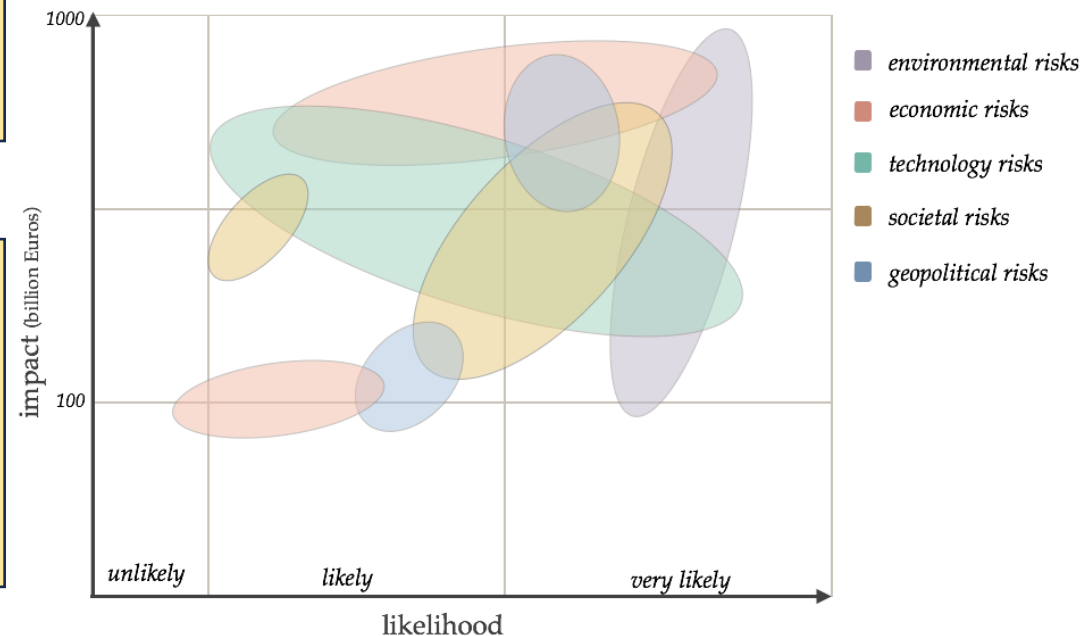
- 業務、情報、人、プロセス、サービス、アプリケーション、技術に対するリスク
- 社会および消費者に対する脅威
- 国家インフラへの脅威

• IMPACT

- サイバー攻撃/インシデントの破壊力による、システムやサービスへの金銭的損失、混乱、損害
- 重要な機密情報の漏洩、盗難、破壊

• CYBER SECURITY RISK THRESHOLDS（閾値）

- サイバー攻撃の破壊力とエネルギーの制限
- サイバー防御／準備、対応、復旧



サイバーセキュリティ標準の効果

協力、共有、学習、合意形成を通じて国際的なサイバー・スタンダードを策定することで、以下のことが実現する：

- すべての関係者の保護、セキュリティ、安全性の向上
- 適合性評価（認証、試験、検査）の基盤
- コミュニケーション、イノベーション、取引、グローバル・ガバナンスを促進するための相互理解と共通言語の基盤
- 各国のサイバー政策とプログラムの補完・支援

国際標準化への参加団体



World Standards
Cooperation (WSC)

Regional Standards Bodies

Asia-Pacific

Europe (CEN, CENELEC, ETSI)

Americas

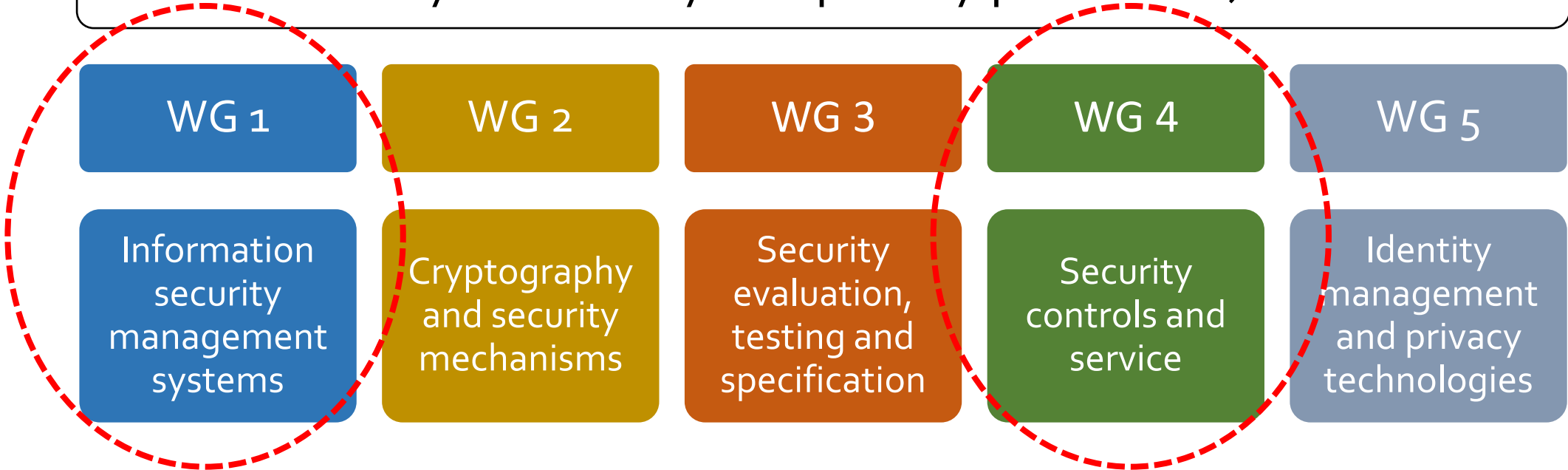
Liaisons (industry
groups, consumer
groups etc.)

National Standards Bodies (AFNOR, ANSI, BSI, DIN, SAC etc.)

Regulatory Bodies, Government Bodies ...

Cybersecurity standards in ISO/IEC JTC1/SC27

ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection)



Cover the area of Cyber Security

ISO/IEC 27001 ISMS

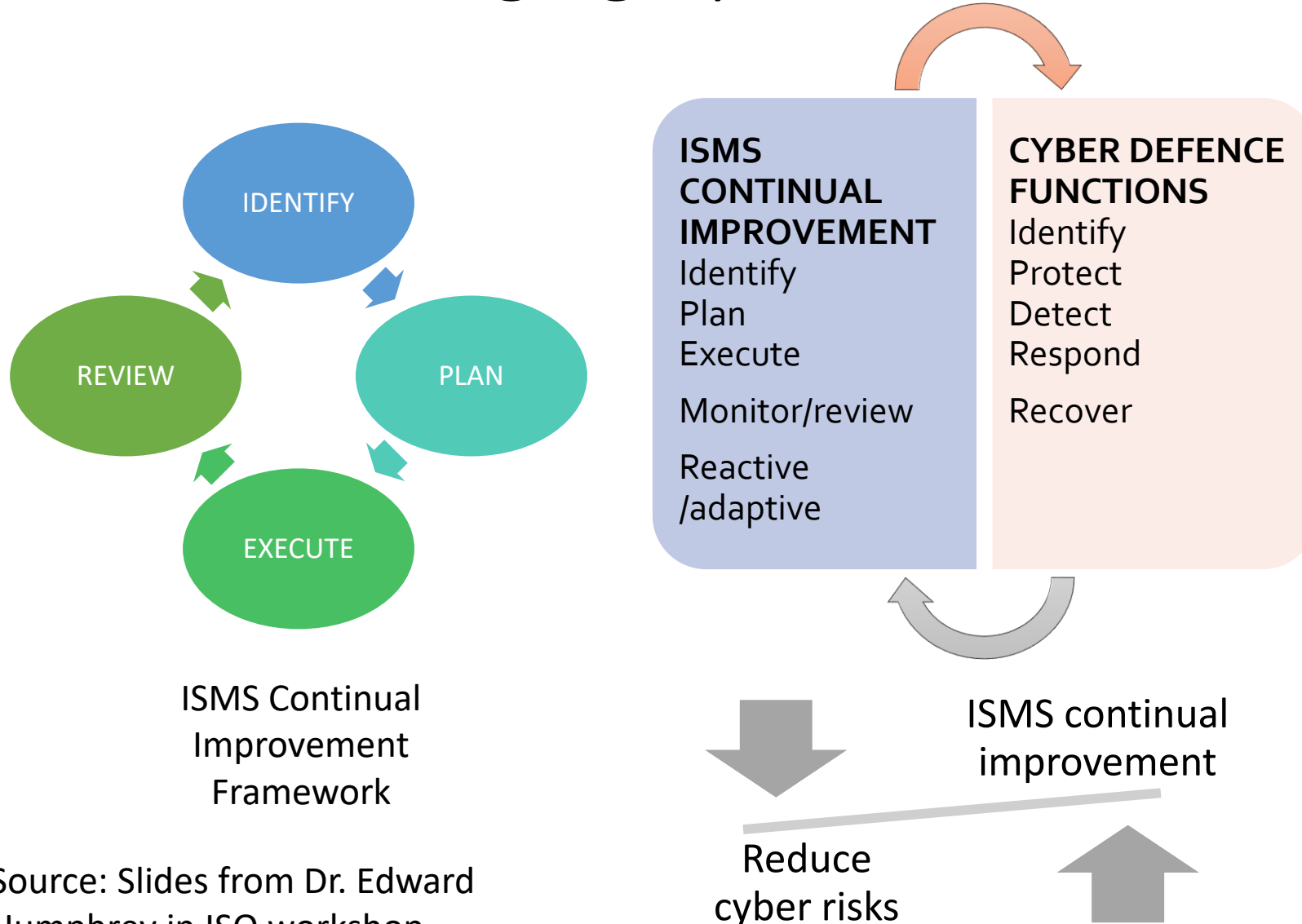
The on-going management of cyber risk through the process of continual improvement:

- Anticipate
- Prepare
- Protect
- Reactive & Responsive
- Adaptive (*business plasticity*)
- **CONTINUAL IMPROVEMENT**

継続的改善プロセスによるサイバーリスクの継続的管理が重要



ISO/IEC 27001 ISMS - Managing Cyber Risk



ISO/IEC 27103

IDENTIFY	Business Environment and Context Risk Assessment Risk Management Strategy Governance Asset management
PROTECT	Access Control Aware and Training Data Security Information Protection Policies, Processes and Procedures Maintaining Controls
DETECT	Monitoring and Detection Processes Incident Handling Management Processes
RESPOND	Response Planning and Management Process Continual Improvements Communications
RECOVER	Recovery Planning and Management Processes Continual Improvements Communications

WG 1 Projects related to Cybersecurity

Cybersecurity

ISO/IEC TS 27100: 2020	Cybersecurity – Overview and Concepts
ISO/IEC 27102:2019	Information security management — Guidelines for cyber-insurance
ISO/IEC TR 27103: 2018	Cybersecurity and ISO and IEC Standards
ISO/IEC TS 27110: 2021	Cybersecurity framework development guidelines

WG 4 Projects 1/11

Guidance for information security controls 1/2

ISO/IEC 27031:2011 [Revision: FDIS]	Guidelines for information and communication technology (ICT) readiness for business continuity
ISO/IEC 27033, Part 1 – Part 6	Network security
ISO/IEC 27034, Part 1 – Part 7	Application security
ISO/IEC 27035, Part 1 – Part 4	Information security incident management
ISO/IEC 27036, Part 1 – Part 4	Information security for supplier relationships

WG 4 Projects 2/11

Guidance for information security controls 2/2

ISO/IEC 27039:2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
ISO/IEC 27040:2024 [Revision: 完了]	Storage security

WG 4 Projects 3/11

ISO/IEC 27033, Network security

Part 1:2015, Overview and concepts

Part 2:2012, Guidelines for the design and implementation of network security

Part 3:2010, Reference networking scenarios -- Threats, design techniques and control issues

Part 4:2014, Securing communications between networks using security gateways

Part 5:2013, Securing communications across networks using Virtual Private Networks (VPNs)

Part 6:2016, Securing wireless IP network access

Part 7:2023, Guidelines for network virtualization security

WG 4 Projects 4/11

ISO/IEC 27035, Information security incident management

Part 1:2023, Principles and processes [Revision:完了]

Part 2:2023, Guidelines to plan and prepare for incident response
[Revision:完了]

Part 3:2020, Guidelines for ICT incident response operations

Part 4, Coordination [DIS]

WG 4 Projects 5/11

Investigation, digital evidence and electronic discovery

ISO/IEC 27037:2012	Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27041:2015	Guidance on assuring suitability and adequacy of incident investigative method
ISO/IEC 27042:2015	Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043:2015	Incident investigation principles and processes
ISO/IEC 27050, Part 1 – Part 4	Electronic discovery

WG 4 Projects 6/11

Cybersecurity

ISO/IEC 27032:2012
[Revision: FDIS]

Guidelines for cybersecurity
Revision:

Cybersecurity — Guidelines for Internet security

ISO/IEC 24392 [IS]

Security reference model for industrial internet platform

WG 4 Projects 7/11 : IoTの部分

IoT security and privacy, CPS

ISO/IEC 27400:2022	IoT security and privacy – Guidelines
ISO/IEC 27402:2023	IoT security and privacy – Device baseline requirements
ISO/IEC 27403: 2024	IoT security and privacy – Guidelines for IoT-domotics
ISO/IEC 27404 [CD2]	IoT security and privacy – Cybersecurity labelling framework for consumer IoT
ISO/IEC 5689 [WD1]	Security frameworks and use cases for cyber physical systems

- Base documents of SC 41 “Internet of Things and digital twin”
 - ISO/IEC 30141:2018, Internet of Things (IoT) – Reference architecture
 - ISO/IEC 20924:2021, Internet of things (IoT) – Vocabulary

ISO/IEC 27400 – Published

この規格は、日本の「IoT セキュリティガイドライン ver 1.0」に基づき、ISO の規格化を求めたものである。

- **Title: Cybersecurity – IoT security and privacy – Guidelines**

- Scope

This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

- Main Structure

- Clause 5 : IoT concept and reference model

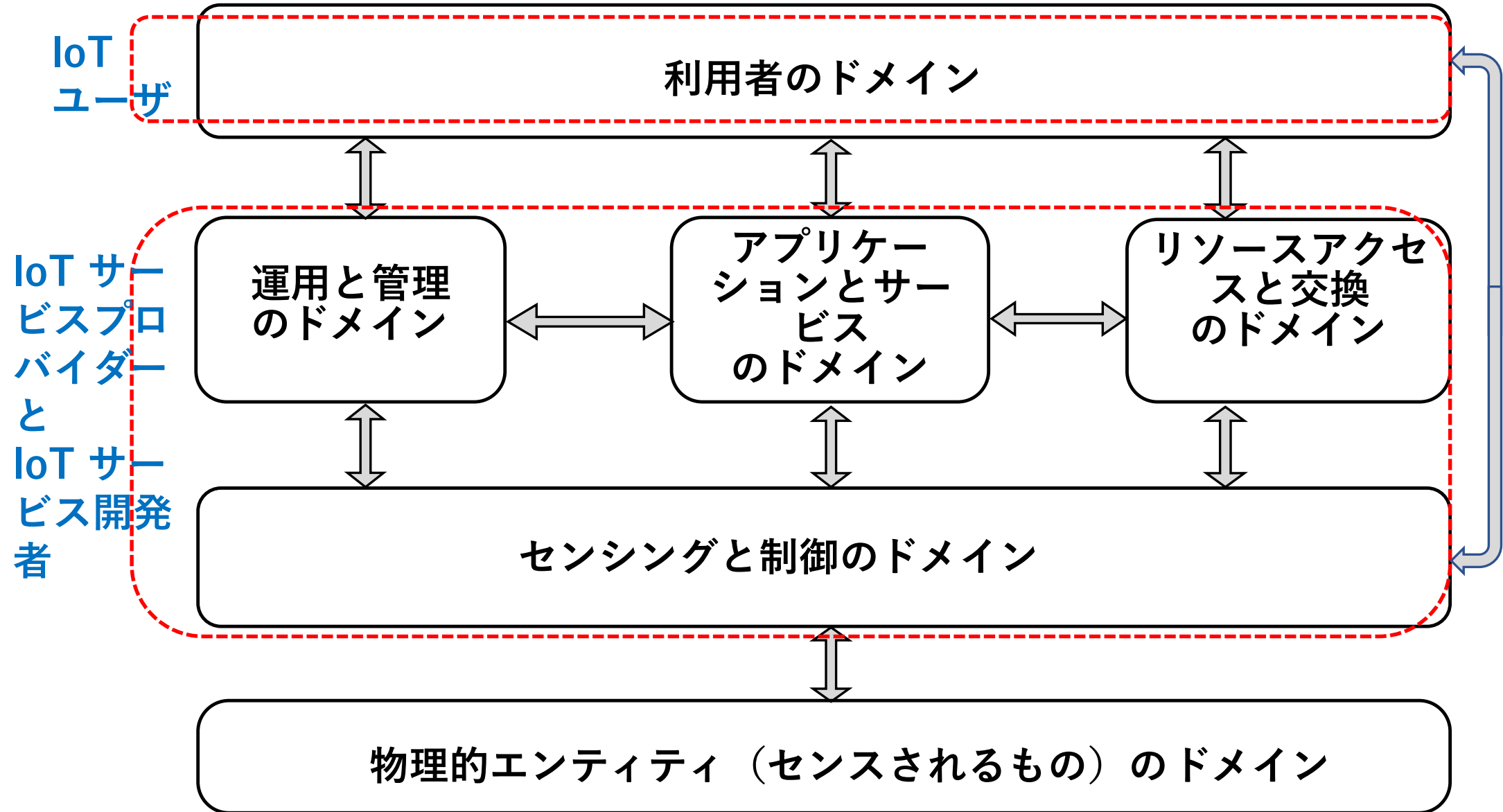
- Clause 6 : Risk management for IoT systems

- Clause 7 : Security controls and privacy controls

1.4 対象読者	9
1.5 ガイドラインの全体構成	10
第2章 IoTセキュリティ対策の5つの指針	
2.1【方針】指針1 IoTの性質を考慮した基本方針を定める	
要点1. 経営者がIoTセキュリティにコミットする	
要点2. 内部不正やミスに備える	
2.2【分析】指針2 IoTのリスクを認識する	
要点3. 守るべきものを特定する	18
要点4. つながることによるリスクを想定する	20
要点5. つながりで波及するリスクを想定する	22
要点6. 物理的なリスクを認識する	24
要点7. 過去の事例に学ぶ	25
2.3【設計】指針3 守るべきものを守る設計を考える	27
要点8. 個々でも全体でも守れる設計をする	28
要点9. つながる相手に迷惑をかけない設計をする	31
要点10. 安全安心を実現する設計の整合性をとる	33
要点11. 不特定の相手とつなげられても安全安心を確保できる設計をする	35
要点12. 安全安心を実現する設計の検証・評価を行う	36
2.4【構築・接続】指針4 ネットワーク上での対策を考える	38
要点13. 機器等がどのような状態かを把握し、記録する機能を設ける	39
要点14. 機能及び用途に応じて適切にネットワーク接続する	40
要点15. 初期設定に留意する	42
要点16. 認証機能を導入する	44
2.5【運用・保守】指針5 安全安心な状態を維持し、情報発信・共有を行う	45
要点17. 出荷・リリース後も安全安心な状態を維持する	46
要点18. 出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える	47
要点19. つながることによるリスクを一般利用者に知ってもらう	51
要点20. IoTシステム・サービスにおける関係者の役割を認識する	52
要点21. 脆弱な機器を把握し、適切に注意喚起を行う	53

IoTセキュリティガイドライン V.1.0の目次

ISO/IEC 27400におけるRA (based on ISO/IEC 30141)



Security Controls in ISO/IEC 27400

Security controls for IoT service developer and IoT service provider

24 controls

- 7.1.2.1 Policy for IoT security
- 7.1.2.2 Organization of IoT security
- 7.1.2.3 Asset management
- 7.1.2.4 Equipment and assets located outside physical secured areas
- 7.1.2.5 Secure disposal or re-use of equipment
- 7.1.2.6 Learning from security incidents
- 7.1.2.8 Secure development environment and procedures
- 7.1.2.9 Security of IoT systems in support of safety
- 7.1.2.10 Security in connecting varied IoT devices
- 7.1.2.11 Verification of IoT devices and systems design
- 7.1.2.12 Monitoring and logging
- 7.1.2.13 Protection of logs
- 7.1.2.14 Use of suitable networks for the IoT systems
- 7.1.2.15 Secure settings and configurations in delivery of IoT devices and services
- 7.1.2.16 User authentication
- 7.1.2.17 Provision of software and firmware updates

7.1.2.18 Sharing vulnerability information

7.1.2.19 Security measures adapted to the lifecycle of IoT system and services

7.1.2.20 Guidance for IoT users on the proper use of IoT devices and services

7.1.2.21 Determination of security roles for stakeholders

7.1.2.22 Management of vulnerable devices

7.1.2.23 Management of supplier relationships in IoT security

7.1.2.24 Information security in IoT devices

Security controls for IoT user

4 controls

7.1.3.1 Contacts and support service

7.1.3.2 Initial settings of IoT device and service

7.1.3.3 Deactivate unused devices

7.1.3.4 Secure disposal or re-use of IoT device

Privacy controls in ISO/IEC 27400

Privacy controls for IoT service developer and IoT service provider

14 controls

- 7.2.2.1 Prevention of privacy invasive events
- 7.2.2.2 IoT privacy by default
- 7.2.2.3 Collection and use of personal data
- 7.2.2.4 Verification of IoT functionality
- 7.2.2.5 Consideration of IoT users
- 7.2.2.6 Management of IoT privacy controls
- 7.2.2.7 Unique device identity
- 7.2.2.8 Fail-safe authentication
- 7.2.2.9 Minimization of indirect data collection

- 7.2.2.10 Communication of privacy preferences
- 7.2.2.11 Verification of automated decision
- 7.2.2.12 Accountability for stakeholders
- 7.2.2.13 Unlinkability of PII
- 7.2.2.14 PII protection in IoT devices

Privacy controls for IoT user

3 controls

- 7.2.3.1 User consent
- 7.2.3.2 Connecting with other devices and services
- 7.2.3.3 Certification/validation of PII protection

Example 7.1.2.10 Security in connecting varied IoT devices

Control-10

IoTシステムは、多様なIoTデバイス（機器）を接続する際のセキュリティを確保・維持するように設計・実装されることが望ましい。

Purpose

To maintain security of IoT system in connecting varied IoT devices including those not necessarily verified by the IoT service developer or the IoT service provider.

Controlling

Guidance

...

IoTサービス開発者とIoTサービス提供者は、このような状況に備えた安全なIoTシステムを設計し、実装する必要がある。IoT システムには、必要に応じて以下の機能を持たせることができる：

- a. ホワイトリストを使用して IoT デバイス（機器）を選択的に接続する。
- b. 該当する場合、デバイス（機器）と接続交渉を行う際に、デバイス（機器）の仕様、例えば、プロバイダ名、モデル、製造年、関連規格への適合性などを取得し、接続要求の可否を判断する、あるいは、利用可能な機能、サービス、情報の範囲を限定する。

7.1.3.2 Initial settings of IoT device and service

Control-26

IoTデバイス（機器）やサービスの初期設定は、正確に実施することが望ましい。

Purpose

To ensure secure initial settings of IoT devices and service.

Audience: IoT user

IoT Domain: User

Guidance

IoT機器の「工場出荷時設定ID」や「デフォルトパスワード」などの認証情報のデフォルト設定は、取扱説明書が公開されていることから、一般に知られていると考えられる。デフォルトの認証情報は、IoT利用者がリセットする必要がある。新しい設定は、元の設定と同じであってはならず、他のIoTデバイスの設定と共有されてはならず、容易に推測可能であってはならず、インターネット上で利用可能な一般的なID/パスワードのリストにあってはならない。

ISO/IEC 27402: 2023

- **Title: Cybersecurity – IoT security and privacy – Device baseline requirements**

- Scope

This document provides baseline requirements for IoT devices and their developers to support security and privacy controls.

Excluding any of the requirements specified in 5.1 is not acceptable when an organization claims conformity to this document.

セ ク タ ー A	セ ク タ ー B	セ ク タ ー C	セ ク タ ー D	垂 直 市 場 A	垂 直 市 場 B	垂 直 市 場 C	垂 直 市 場 D
IoT機器のためのICTセキュリティの基本要件							

Note:

This figure is depicted from
“introduction” of ISO/IEC 27402

Security Baseline Requirements in ISO/IEC 27402

5 Requirements

5.1 Requirements for IoT device developers

- 5.1.1 Risk management

- 5.1.2 Information disclosure

- 5.1.3 Vulnerability disclosure and handling processes

5.2 Requirements for IoT devices

- 5.2.1 General

- 5.2.2 Configuration

- 5.2.3 Software reset

- 5.2.4 User data removal

- 5.2.5 Protection of data

- 5.2.6 Interface access

- 5.2.7 Software and firmware updates

- 5.2.8 User notifications

ISO/IEC 27403: 2024

- **Title: Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics**
- Scope

This document provides guidelines to analyse security and privacy risks and identifies controls that need to be implemented in IoT-domotics systems.

Note:

IoT-domotics:

一般的に家庭内または電子ウェアラブルとして使用されるネットワーク、デバイス、サービス、ユーザーで構成されるIoTシステム

ISO/IEC 27404 – CD2→DIS

• Title: Information technology — Security techniques — Cybersecurity labelling framework for consumer IoT

本規格案は、消費者向けIoT製品のサイバーセキュリティラベリングプログラムを開発・実施するためのサイバーセキュリティラベリングフレームワークを定義し、以下のトピックに関するガイダンスを含む。

- 消費者向けIoT製品に関連するリスクと脅威
- 利害関係者、役割、責任
- 関連規格とガイダンス文書
- 適合性評価の選択肢
- ラベリング発行及び保守要件
- 相互承認の考慮事項

本規格の対象範囲は、複数のデバイス が接続されるIoTゲートウェイ、基地局、ハブ、スマートカメラ、テレビ、スピーカー、ウェアラブルデバイス、コネクテッド煙探知機、ドアロック、窓センサー、コネクテッドホームオートメーション及び アラームシステム、洗濯機や冷蔵庫等のコネクテッド家電、スマートホームアシスタント、コネクテッド子供用玩具及びベビーモニター等の消費者向けIoT製品に限定される。消費者向けではない製品は、この規格から除外される。除外されるデバイスの例としては、主に製造、ヘルスケア、その他の産業用途を目的としたものがある。

本規格案は、消費者、開発者、サイバーセキュリティラベル発行機関、独立試験機関に適用される。

ラベリングの枠組みの必要性和意義

－ ラベリングの枠組みの必要性

消費者向けIoTラベリング制度は、特定の地域や市場におけるサイバーセキュリティの懸念に対応するために個別に策定されているため、ラベリングされた製品を比較することが難しくなり、国際市場に混乱をもたらす可能性がある。そのため、各消費者向けIoTサイバーセキュリティラベルが示すサイバーセキュリティ要件の整合を図るためのサイバーセキュリティラベリングの枠組みが必要とされている。

－ 枠組み（フレームワーク）の意義

サイバーセキュリティのラベリングフレームワークは、既存の広く使用されている規格（例えば、ETSI EN 303 645、TS 103 701、NIST IR 8259、NIST IR 8259A、NIST IR 8425、ISO/IEC 27400、ISO/IEC 27402）からのサイバーセキュリティ要件を整合させる。このフレームワークに基づいて消費者向けIoTサイバーセキュリティラベリングスキームを実装することで、相互認証とそのプロセスを簡素化することができる。更に、追加の特殊性（テストケースや能力等）を提供するサイバーセキュリティラベリングスキームの実装は、このフレームワークを補完するものである。

成果達成の側面

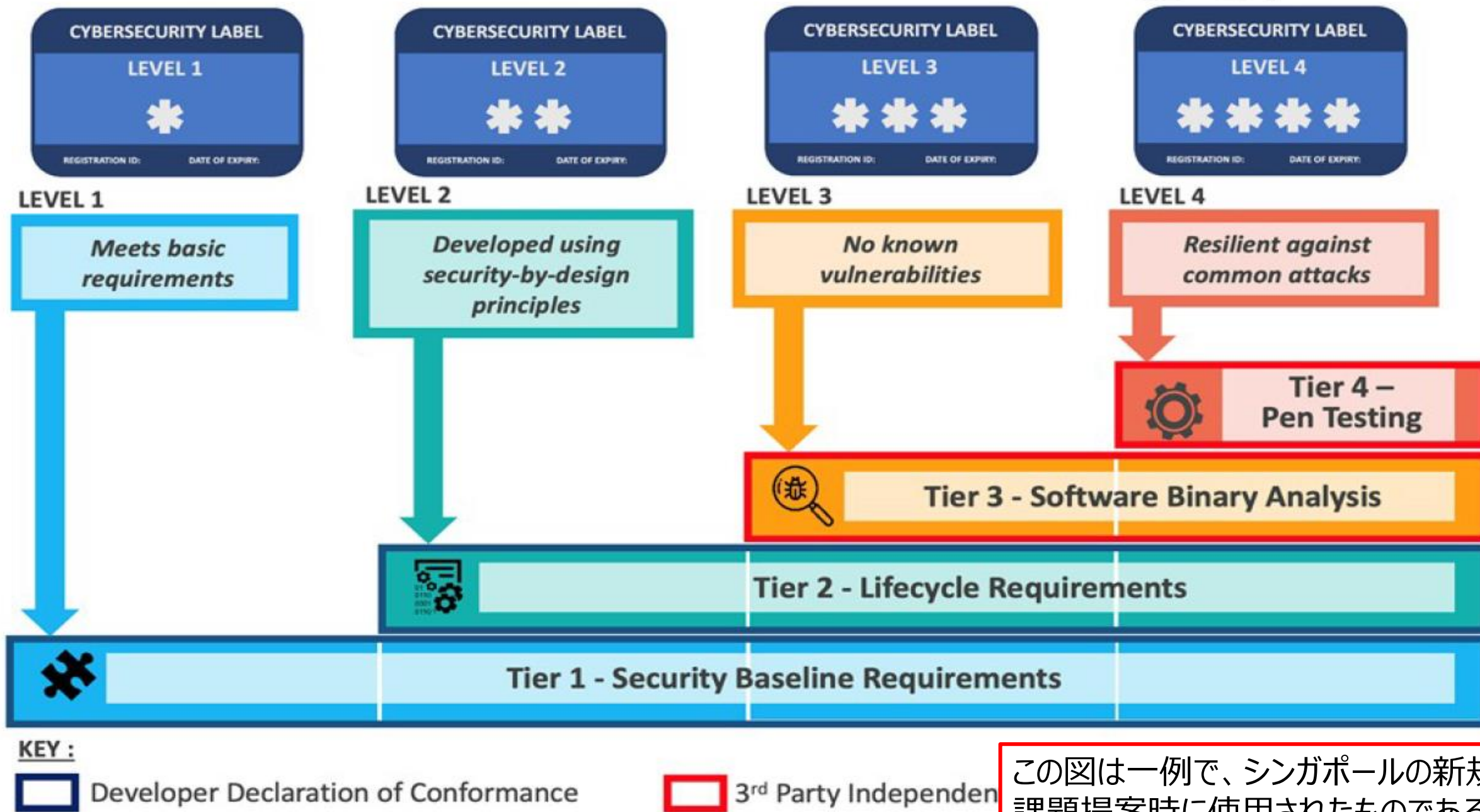
サイバーセキュリティのラベリング枠組みは、以下の側面で成果を達成することを目指している。

- 消費者 - 透明性：消費者向けIoT製品のサイバーセキュリティの提供は、一般消費者には不透明である。サイバーセキュリティのラベリングを利用することで、消費者は消費者向けIoT製品を購入する際に十分な情報を得た上で選択することができ、デジタルの世界でサイバーセキュリティの考え方を取り入れることができる。
- 開発者 - ブランディング：サイバーセキュリティのラベリングは、開発者が製品を差別化し、ブランドの質を高めることで、より積極的に持続可能な産業を育成できる。また、開発者にとっては、より安全な製品を製造し、製品にサイバーセキュリティを提供するために費やした努力を収益化するインセンティブとなる。
- 経済／エコシステム - 相互承認：デジタル経済の成長に伴い、サイバーセキュリティのラベリングに互換性を持たせることで、国境を越えた重複したテストの必要性を減らし、開発者のコンプライアンスにかかるコストを削減して市場アクセスを向上させ、ラベリングの推進により各国間で相互または相互承認する道を開くことができるとしている。

保証の限界

消費者向けIoT製品のサイバーセキュリティラベリングは、正式なセキュリティ保証を提供するものではない。消費者向けIoT製品は、そのラベリング状況に関係なく、悪意のある攻撃者によって侵害される可能性がある。

より高いセキュリティ保証を求めるユーザ（企業、製造業、産業アプリケーション、ヘルスケア等）は、正式な評価・認証スキーム（ISO/IEC 15408-1:2022に記載されているもの等）で認証された製品を検討することを強く推奨している。



この図は一例で、シンガポールの新規課題提案時に使用されたものである。

Figure 1 — Levels of universal labelling framework and assessment tiers

Annex A (informative) Types and features of cybersecurity labels.....	24
A.1 General	
A.2 Static cybersecurity labels	
A.3 Dynamic cybersecurity labels	
A.4 Dual modality cybersecurity labels (Static and dynamic)	24
A.5 Validation of cybersecurity labels	25
Annex B (informative) Illustrative example of multi-level labelling scheme	26
B.1 General.....	26
B.2 Cybersecurity labelling scheme from Singapore	26
B.3 Cybersecurity labelling scheme of Japan.....	31
Annex C (informative) Illustrative examples of binary labelling schemes	34
C.1 General	34
C.2 Overview of labelling scheme from the United Kingdom (UK)	34
C.3 Comparison of Singapore's multi-level and UK's binary schemes.....	34
C.4 Overview of the IT Security Label Scheme in Germany	35
C.5 Mutual recognition of Germany's and Singapore's schemes	38

ISO/IEC 27404 Annexes (DIS)

B.3 Cybersecurity labelling scheme of Japan

B.3.1 Overview of labelling scheme from Japan (JC-STAR)

© ISO/IEC 2024 – All rights reserved

Annex B.3に日本のスキーム が掲載される

ISO/IEC DIS 27404.1

JC-STAR is a voluntary scheme and targets a wide range of “IoT products” premised on the definition of an IoT product as an IoT device and its associated services.

The JC-STAR comprises multiple cybersecurity levels, with each higher level being more comprehensive in security requirements and conformity assessment requirements. Security requirements differ among different product categories.

B.3.2 Scope of products covered by JC-STAR

Referring to definitions in both domestic standards and schemes and those of other countries, the scope of products covered by JC-STAR includes the following IoT devices that have the ability to send and receive data using Internet Protocol (IP), and their associated services.

- Devices that can be connected to the Internet: Devices with the ability to send and receive data over the Internet using IP
- Devices that can be connected to a network: Devices that are connected to “devices that can be connected to the Internet” or other “devices that can be connected to a network” and have the ability to send and receive data using IP

As with certain existing domestic and other countries' schemes, general-purpose IT products (PCs, tablets, smartphones, etc.) to which users can easily alter security measures such as via software products are excluded. IoT products with a general-purpose OS are considered to be in scope if users cannot easily add security measures to the product itself.

B.3.3 Security Requirements in JC-STAR

JC-STAR establishes security requirements to address minimum threats common to all IoT products in scope as a unified baseline (**STAR-1**), as well as security requirements per product category to address

As with certain existing domestic and other countries' schemes, general-purpose IT products (PCs, tablets, smartphones, etc.) to which users can easily alter security measures such as via software products are excluded. IoT products with a general-purpose OS are considered to be in scope if users cannot easily add security measures to the product itself.

B.3.3 Security Requirements in JC-STAR

JC-STAR establishes security requirements to address minimum threats common to all IoT products in scope as a unified baseline (**STAR-1**), as well as security requirements per product category to address characteristics of each product category (**STAR-2**, **STAR-3**, and **STAR-4**). Figure B.3.3 shows an image of the security requirement levels in JC-STAR.

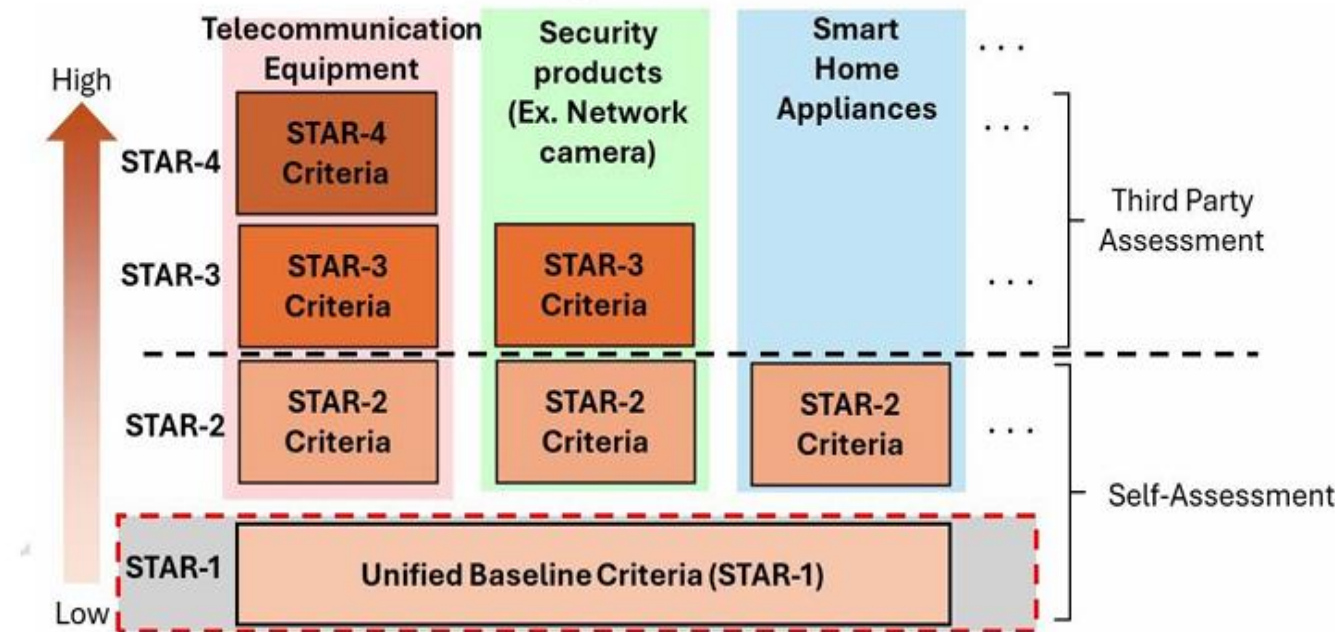


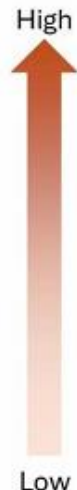
Figure B.3.3 - Security requirement levels in JC-STAR

B.3.4 Conformity assessment levels in JC-STAR

For **STAR-1** and **STAR-2**, labels are granted based on self-declarations of conformity by IoT product vendors. For **STAR-3** and **STAR-4**, labels are granted based on a third-party evaluation by an accredited independent test laboratory, as **STAR-3** and above are intended for procurement use by government

agencies and critical infrastructure providers and require high reliability. Table B.3.4 shows the conformity assessment levels of JC-STAR.

Table B.3.4 – Conformity assessment levels in JC-STAR



STAR-3 and above	<ul style="list-style-type: none"> General conformity criteria for each IoT product category in addition to STAR-2. Evaluated and certified by an independent third party. Intended for use in critical systems of government agencies, critical infrastructure providers, and large companies.
STAR-2	<ul style="list-style-type: none"> Basic conformity criteria for each IoT product category in addition to STAR-1. IoT product vendors self-declare conformity.
STAR-1	<ul style="list-style-type: none"> Unified baseline conformity criteria for all IoT products in scope. IoT product vendors self-declare conformity.

B.3.5 STAR-1 - Unified baseline level for security requirements and conformity assessment requirements in JC-STAR

For **STAR-1**, security requirements, conformance criteria (16 criteria in total), and evaluation procedures are organised to address threats common to all IoT products in scope. The **STAR-1** requirements are designed based on an analysis of overlapping requirements in both domestic standards or schemes and those of other countries including ETSI EN 303 645 and NISTIR 8425.

Approach to global standardization of IoT security

ISO/IEC JTC1/SC27
27400, 27402, and 27404 (CD2→DIS)

Common parts

- Terminologies
- Reference Architecture
- Use Cases
- Certification Framework

- Risk Analysis
- Security/Privacy Controls

-US – CTIA
IoT Cybersecurity
Certification,
-SP 800-213(NIST)
IoT Device
Cybersecurity
Guidance for the
Federal Government
- NIST TR 8425

-UK – IASME IoT
Cyber Scheme, etc
-EU – ETSI, Cyber
Security for Consumer
IoT: Baseline Req.
EN 303 645
-EU – ENISA
Cybersecurity
Certification – EUCC
Candidate Scheme

Japan – CPSF (METI), Device Requirements (MIC), IoT device
Certification Scheme (under study), etc.

段階的なステージによるIoTセキュリティと国際標準との関係

1. IoT機器を発売する前のセキュリティ対策 (Security by Designを含む)
ISO/IEC 27400, 27402, 27404, etc.
2. 実際に使用 (運用) しているIoT機器への対策
Finding Vulnerable IoT devices (NOTICE等) ,
ISO/IEC 27400, etc.
3. 寿命がきたIoT機器対策
ISO/IEC 27400, 27402, etc.

ISO/IEC TS 5689

Title: Cybersecurity –Security frameworks and use cases for cyber physical systems

Scope

本書は以下の内容を提供する：

CPS 概念モデルとその具体的な特徴

- サイバーフィジカルシステム（CPS）の概念モデルとその一般的特徴；
- 他の関連概念と比較した CPS の具体的な特徴；

懸念とセキュリティの枠組み

- 概念モデルに基づいて、CPS のセキュリティリスクとセキュリティ対策を議論するための基礎となるセキュリティ上の懸念；
- これらのセキュリティ上の懸念に対処するためのいくつかのセキュリティ・フレームワーク；

CPSの実用的なユースケース

- CPSのためのそれぞれのセキュリティフレームワークに基づくユースケース；

CPSのための実用的なユースケース -CPSのためのそれぞれのセキュリティフレームワークに基づくユースケース -セキュリティフレームワークの具体的な使用方法に関するユースケースの可視性の提供 など

Connections in cyber space

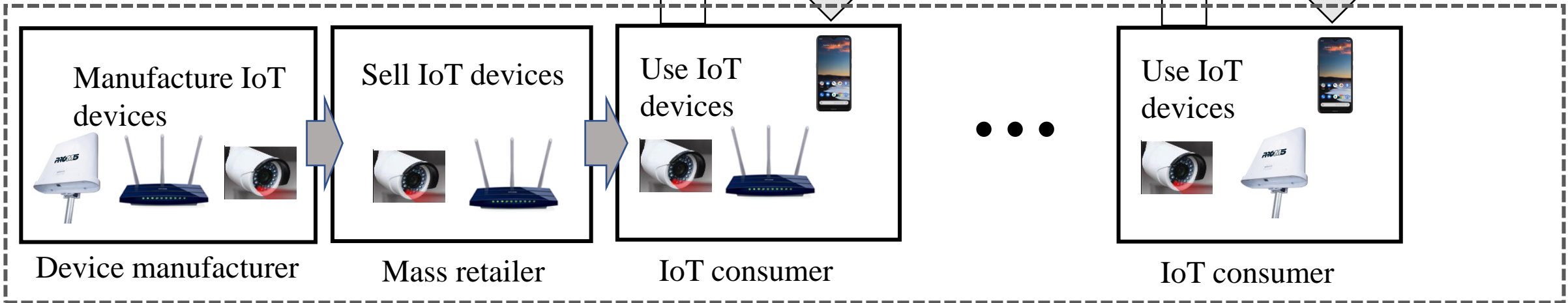
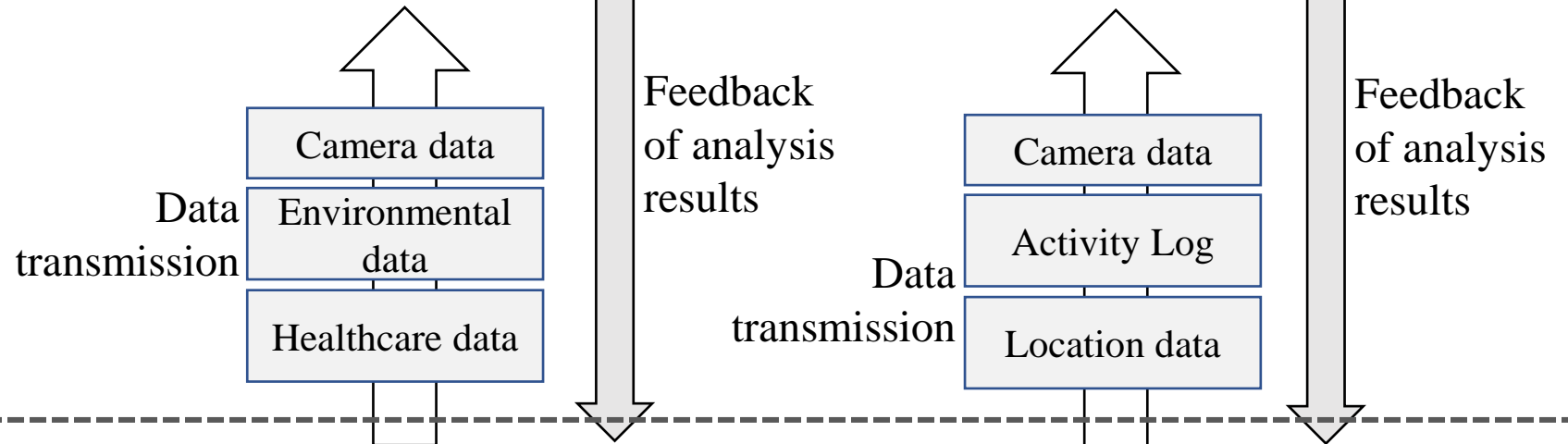
Data processing, analysis, management

(Integrated analysis of data collected at multiple points, processing and accumulation, and feedback of appropriate analysis results to IoT consumers in Physical space)

Analysis servers



Data transcription in Cyber/Physical



Connections in physical space

CPSの概念モデル（本図は規格には採用されず。。。）

Figure 3. An example of 3-tier conceptual model for cyber physical systems

The Third Layer

(Connections in cyberspace)

Trustworthiness of data is a key for secured products and services

The Second Layer

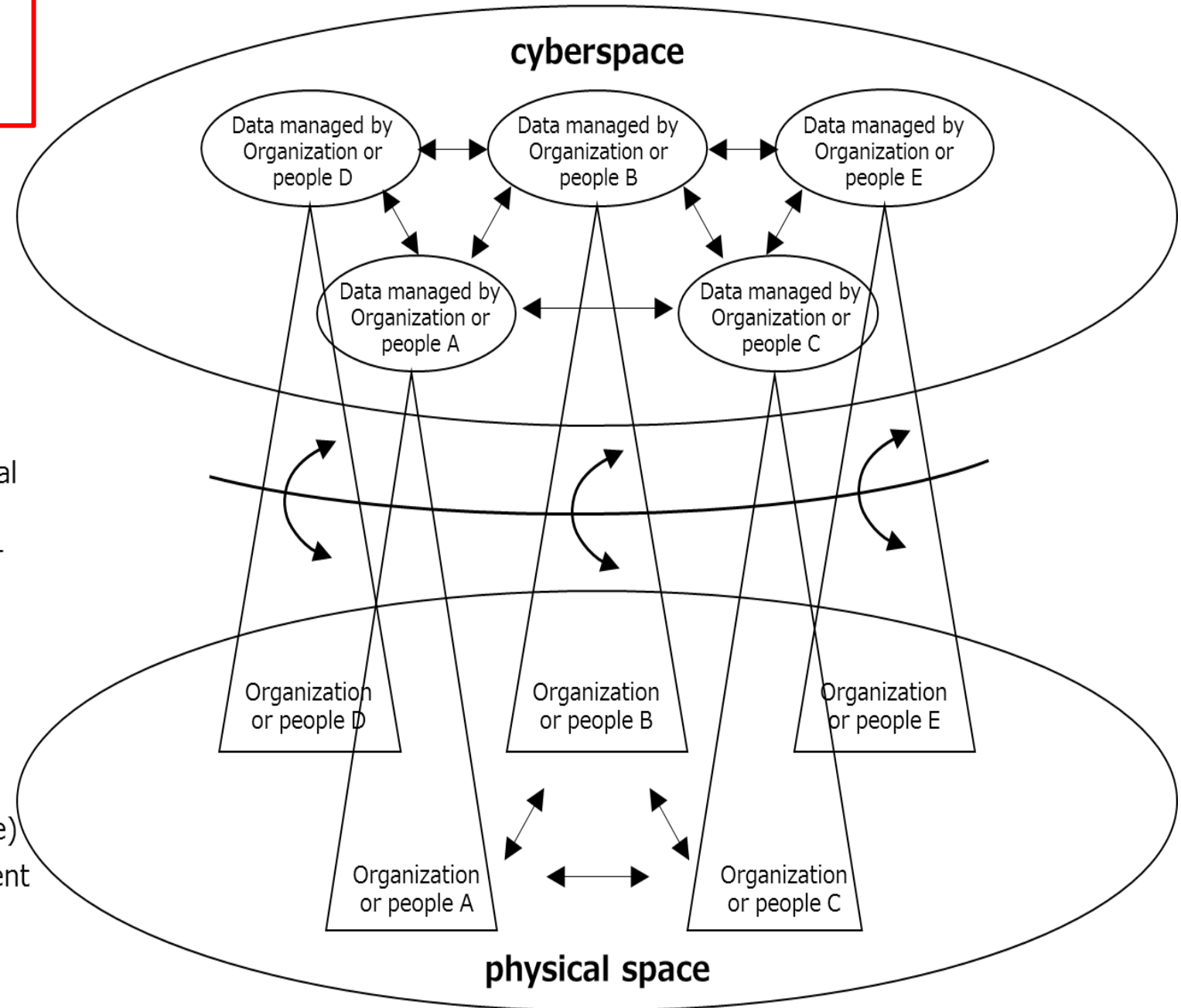
(Mutual connections between cyber & physical space)

Trustworthiness of "transcription" is a key for normal operation of cyber-physical systems

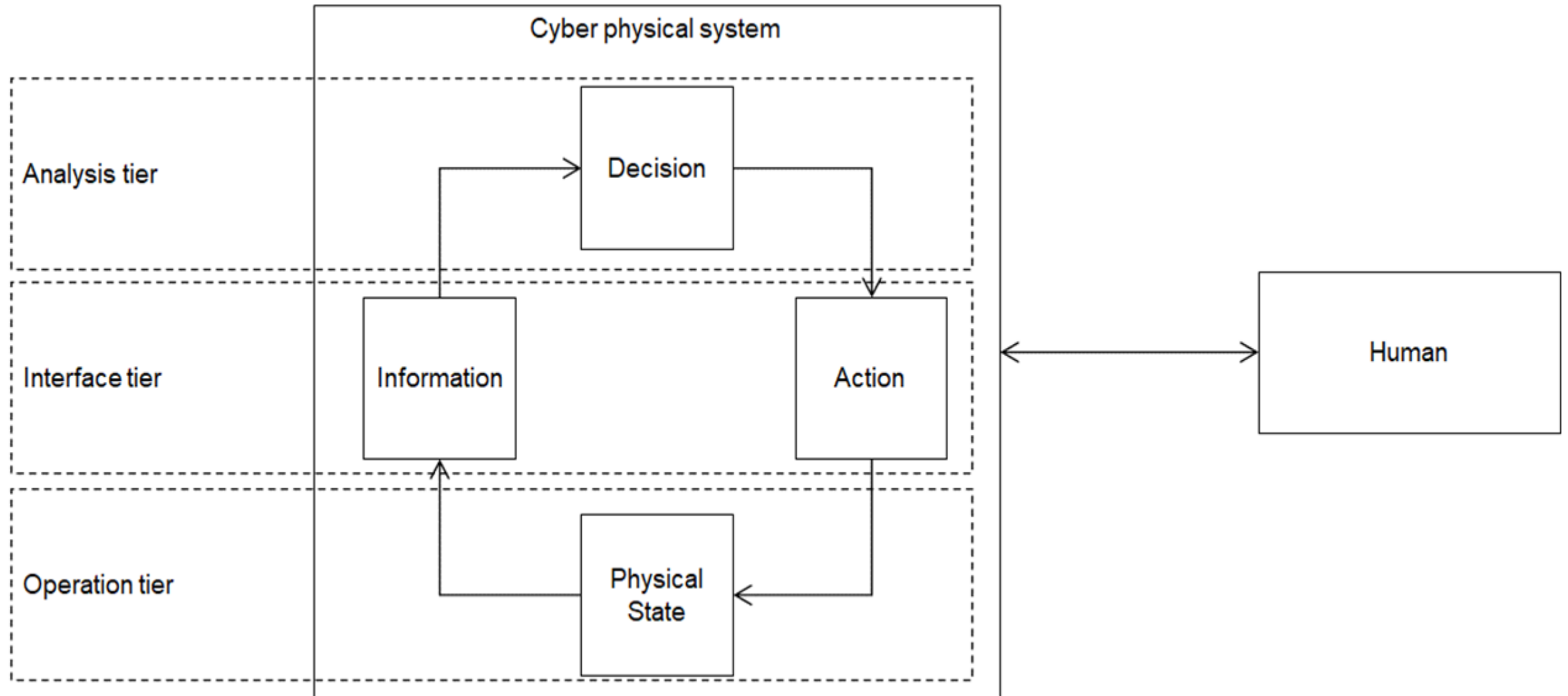
The First Layer

(Connections among Organizations or people)

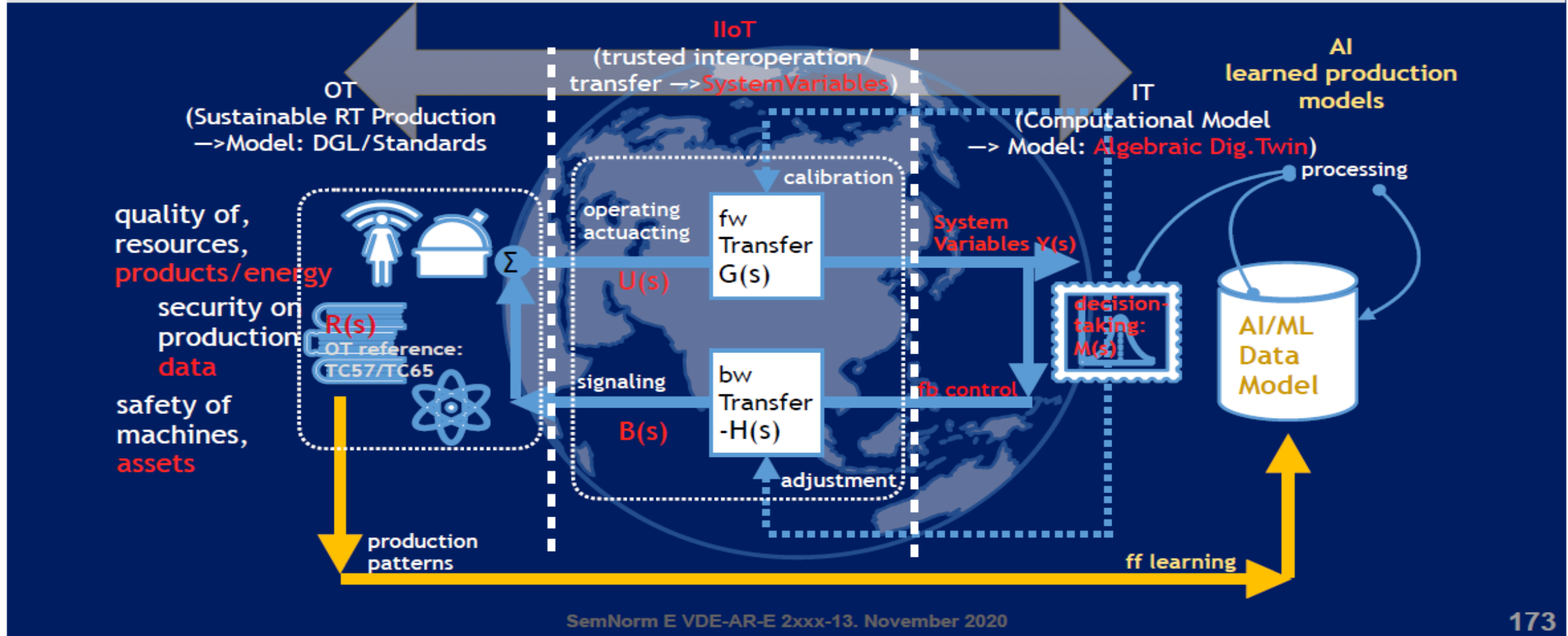
Trustworthiness of organization's management is a key for secured products and services



TS 5689 : 採用されたシンプルな概念モデル



SemNorm PoC: IIoT Transfer Functions Part of ((OT || IT)==CPS Logical Model) To Derive Provenance of Data from CPS Trajectories



Another Application of CPS
framework (will be described in 7.3)

WG 4 Projects 8/11

AI and big data security and privacy

ISO/IEC 20547-4:2020	Big data reference architecture — Part 4: Security and privacy
ISO/IEC 27045 [PWI]	Big data security and privacy — Processes
ISO/IEC 27046 [CD]	Big data security and privacy — Implementation guidelines
ISO/IEC 27090 [WD4]	Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems
ISO/IEC 5181 [WD]	Information technology – Security and privacy – Data provenance
ISO/IEC 6109 [PWI]	Guidelines for data security monitoring based on logging (Proposed title)
ISO/IEC TS 7709 [PWI]	Security and privacy-preserving guidelines for multi-sourced data processing

- Base documents of SC 42 “Artificial intelligence”
 - ISO/IEC FDIS 22989:2022, Artificial intelligence — Artificial intelligence concepts and terminology
 - ISO/IEC 20546:2019, Big data — Overview and vocabulary
 - ISO/IEC 20547-3:2020, Big data reference architecture — Part 3: Reference architecture

WG 4 Projects 9/11

Cloud computing security and privacy

ISO/IEC 19086,
Part 4:2019

Cloud computing — Service level agreement (SLA) framework —
Part 4: Components of security and of protection of PII

- Base documents of SC 38 “Cloud computing and distributed platforms”
 - ISO/IEC 19086, Cloud computing — Service level agreement (SLA) framework
 - Part 1: Overview and concepts
 - Part 2: Metric model
 - Part 3: Core conformance requirements

WG 4 Projects 10/11

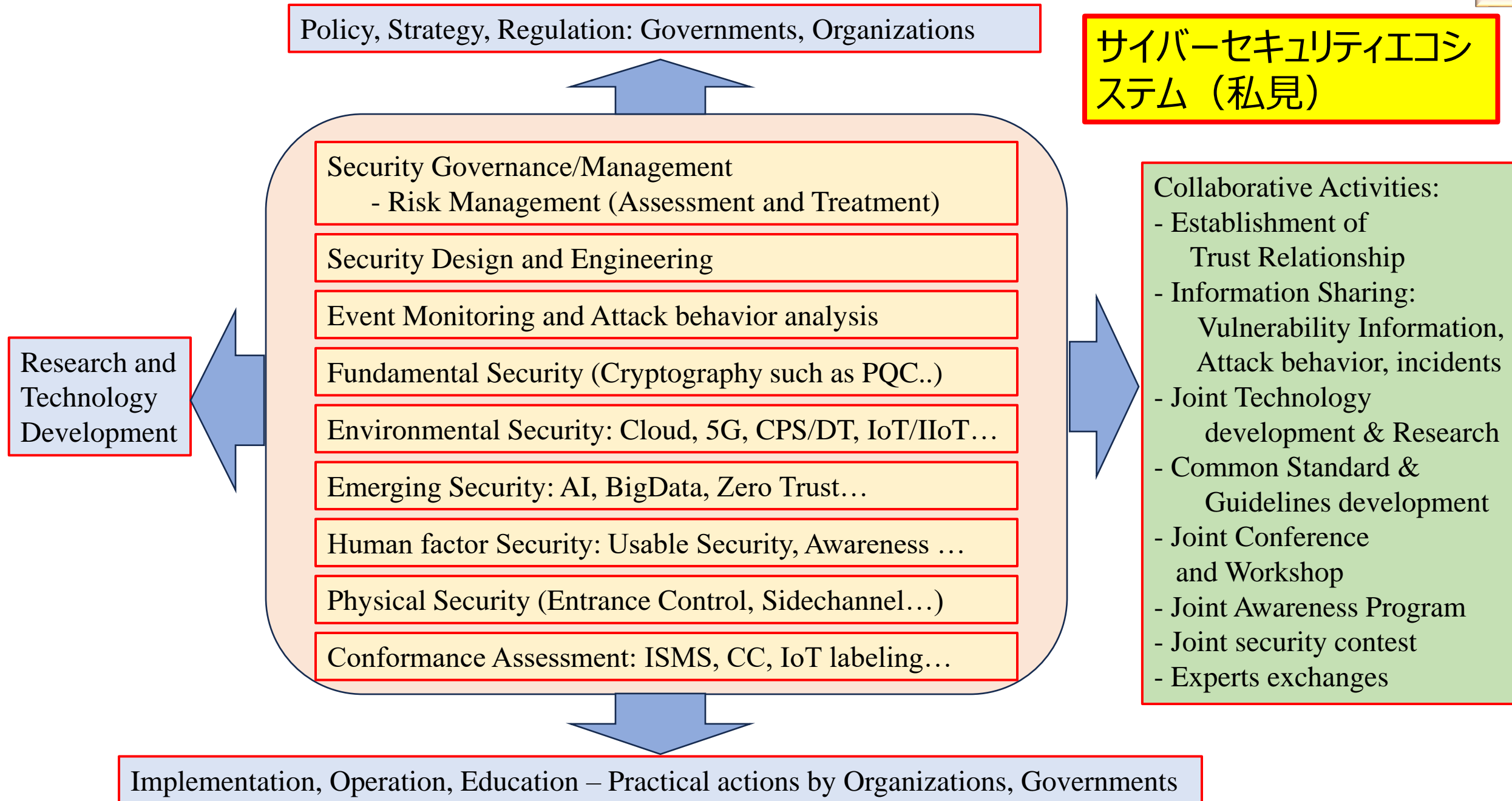
Security in virtualization technologies

ISO/IEC 21878:2018	Security guidelines for design and implementation of virtualized servers
ISO/IEC 27070:2021	Requirements for establishing virtualized roots of trust
ISO/IEC 27071 [IS]	Security recommendations for establishing trusted connections between devices and services

WG 4 Projects 11/11

Other projects for emerging areas

ISO/IEC 13133 [PWI]	Information technology – Security techniques – Security reference model for digital currency hardware wallet
ISO/IEC 17603 [PWI]	Information security – Security techniques – Confidential computing



最後に

1. 国際標準化はIoTデバイスに限定されるものではない。IoTシステムやその組み合わせとして様々な実装形態があることに留意が必要。さらに、5G、CPS / DT、OT/IT、スマートシティなどへの応用が世界的に活発に検討されている。環境が複雑化しているため、標準化内容が多様化
2. 上記の環境において、サイバーセキュリティの確保は最優先事項になっている。
3. その意味で、世界の関連諸国と日本との積極的な情報共有は極めて有効な対策手段となり得る：
 - 共有とはリスク管理活動- 共有することで早期警戒を得る（提供する）ことができる
 - 協力により、防衛コストを削減できる- 追跡していなかったアクターや脅威を特定することができる。
 - 情報を共有することで、サプライヤー、パートナー、競合他社の企業の安全確保を支援できる
4. 国際標準化の視点から、以下の点を考慮することが重要となろう：
 - 標準化戦略：国内の研究プロジェクトの出口の一つが国際標準化になる可能性があることは承知しているが、国際標準化はイベントドリブンではなく、戦略ドリブンである。日本におけるサイバーセキュリティの中に、国際標準化戦略をきちんと盛り込むことが重要となる。戦略の内容と研究開発戦略は強くリンクする。
 - 友好国との綿密な連携の促進：国際標準化は、多くの国とのハーモナイゼーションにより成り立つ。特に、友好国との戦略を含めた意見交換や国際標準化の進め方・提案内容の連携を促進し、日本だけではなく、他の国にとっても有効な国際規格化を推進できることが望ましい。関係するキーパーソンとの密なコミュニケーションがとれるような人間関係の構築も重要となる。
 - 国際標準への参画の推進：若手の技術者の国際規格化への参加を強化する必要がある。

Thank you for listening

