サイバーセキュリティ標準化動向
ーISO/ITU-Tを中心にー

中尾　康二
JNSA　副会長、標準化部会長
情報通信研究機構　主管研究員
横浜国大　客員教授

JNSAにおける標準化部会（標準化）とは

サブタイトル

JNSA　標準化部会

- 業種・業界・分野等の標準化・ガイドライン化などを推進する。
  特に、JNSA目線のセキュリティベースラインの提供、情報セキュリティ対策ガイドラインの策定などを進める。また、国際標準/国際連携との親和性の高い案件については、国際標準への提案やコメント、国際連携案件も視野に入れて、議論を進める。

- 部会長：中尾 康二（国立研究開発法人情報通信研究機構）
  副部会長：松本 泰（セコム株式会社）

標準化部会にあるWG

デジタルアイデンティティWG　　リーダー：宮川 晃一（日本電気株式会社）

活動目的：広くデジタルアイデンティティに関する様々な課題を検討し、デジタル社会の基礎となるIDの重要性の啓蒙やプライバシー関連の問題提起や標準化に向けた意見交換を行う。

電子署名WG　　リーダー：宮崎 一哉（三菱電機株式会社）

活動目的：電子署名関連技術の相互運用性確保のための調査、検討、標準仕様提案、相互運用性テスト、及び電子署名普及啓発を行う。

日本ISMSユーザグループ　　リーダー：魚脇 雅晴（NTTコム ソリューションズ株式会社）

活動目的：ISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることでISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、 日本における健全かつ効果的なISMS普及・促進に貢献する活動を行う。

PKI相互運用技術WG　　リーダー：松本 泰（セコム株式会社）

活動目的：PKI の技術、標準化、法制度等の情報交換及び、議論を行う。関連して、eKYC, 暗号鍵管理勉強会等を企画する。

IoT機器セキュリティログ検討WGは終了、**国際化JNSA活動バックアップWG**は休止

JNSA目線での国際標準化の目的、効用

サブタイトル

サイバーセキュリティの国際規格の目的等

目的：
グローバルなサイバースペースコミュニティ、開発者、および利害関係者における国際規格化の目的は、サイバー犯罪との戦いを支援するための国際的なサイバーセキュリティおよびプライバシー基準を開発すること。

国際サイバー標準の実装は、組織、政府等において、以下の視点から役立つ

- サイバーリスクの軽減および最小化
- サイバー攻撃の影響と破壊的な影響を最小化する
- 使用するITベースのシステム、サービス、インフラストラクチャへの投資を保護し、機密情報や重要な情報を保護する

サイバーセキュリティ国際規格の効用

国際サイバー基準の開発は、参加メンバの協力、情報共有と学習、および合意形成を通じて、以下の利点を提供：

- すべての利害関係者の保護、セキュリティ、安全性の向上
- 適合性評価の基礎（認証、試験、検査）
- コミュニケーション、イノベーション、貿易、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礎
- 組織や個人だけではなく、国のレベルのサイバーセキュリティポリシーとセキュリティプログラムの補完や支援

これまで、「X.509」、「ISMS」等の規格化が衝撃的

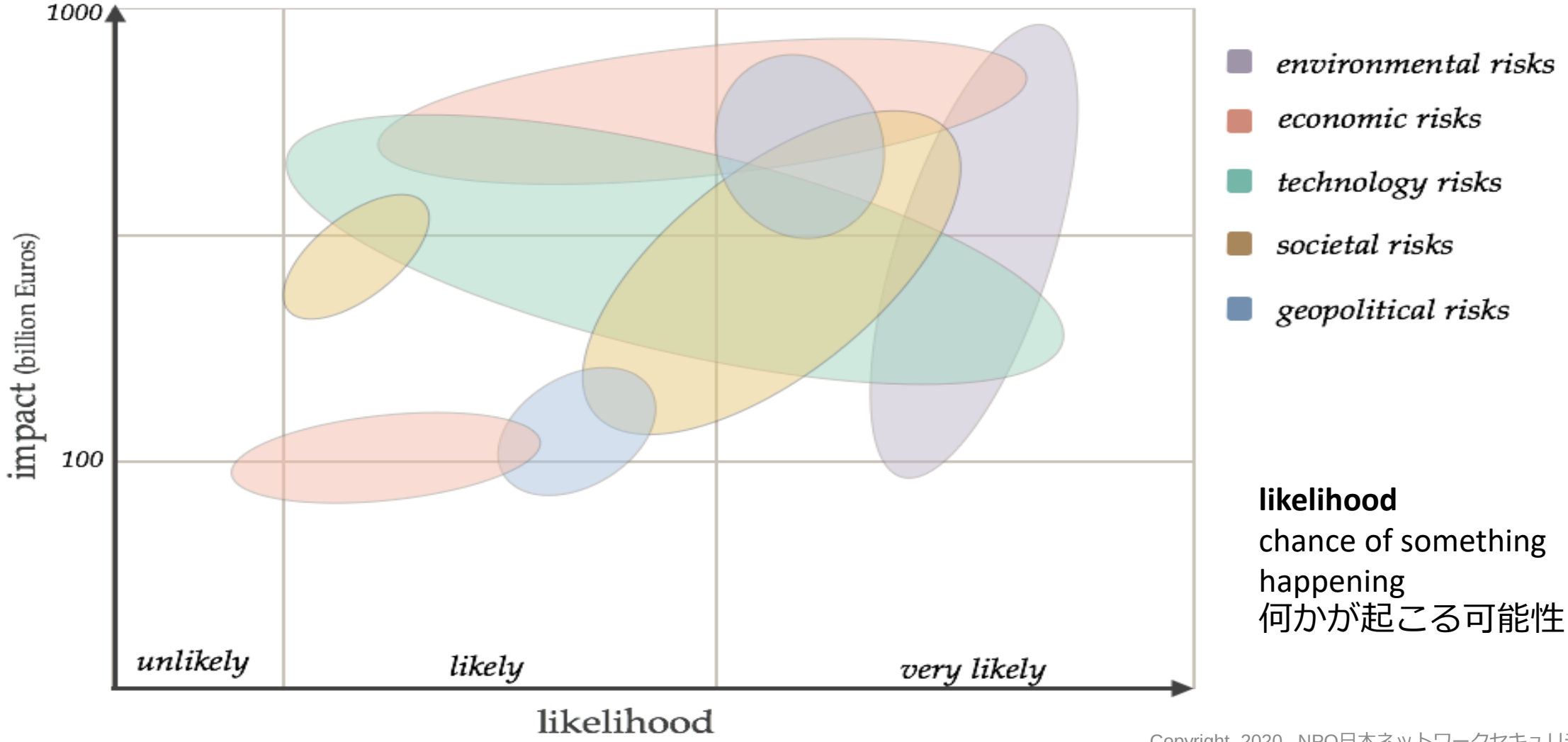
サイバーセキュリティリスクとは（概観）

JNSA

- **脅威とリスク**
  - 運用、情報、人、プロセス、サービス、アプリケーション、およびテクノロジーに対するリスク
  - 社会と消費者への脅威
  - 国のインフラへの脅威

- **インパクト**
  - サイバー攻撃/インシデントの破壊力による経済的損失、システムおよびサービスの中断または損傷
  - 重要で機密性の高い情報の漏洩、盗難、破壊

リスク：LikelihoodとImpact



likelihood
chance of something happening
何かが起こる可能性

あらためて、情報セキュリティリスクとは

- 「リスク」の定義：
  目的に対する不確かさの影響（ISO/IEC 27000:2014/2016, 2.68）

- 派生して
  「情報セキュリティリスク」
  ：情報セキュリティ目的に対する不確かさの影響

- 「顧客情報管理システム」 を事例にリスクを説明
  - 組織内で運用している情報システム
  - 個人顧客の個人情報約1万件を保有
  - 個人情報へのアクセス権は、業務上必要な部門・従業員として、マーケティング担当、営業担当、コールセンター、情報システム運用・保守担当などに与えられている。
  - 本システムの稼働は、20分を越えて停止しないことが求められている。

事例　情報セキュリティ目的とリスク特定の場面

JNSA

会社の
情報セキュリティ目的

個人情報を適正に管理し、
お客様の信頼を得る。

部門の
情報セキュリティ目的

顧客情報管理システムで扱う情報の
機密性及び可用性を維持する。

・・・

顧客情報管理システムに持つ情報を資格のない者に漏洩しない［機密性］

顧客情報管理システムが停止した場合でも、20分以内に復旧する。［可用性］

リスク特定の場面
1. パスワードの不適切な管理
2. 運用担当者の不正
3. 情報システム又はネットワークの不備
4. APT攻撃

リスク特定の場面
1. 復旧処理の設計不備
2. 復旧手順の不備
3. ・・・
4. ・・・

事例　場面1のシナリオ　リスク源、事象、結果

情報セキュリティ目的	顧客情報管理システムに持つ情報を資格のない者に漏洩しない。
場面1　　パスワードの不適切な管理	
リスク源	1. 従業員に対して情報セキュリティの重要性やパスワード使用についての教育が十分にされていない。 2. 資格のある者が他人にパスワードを教えて使わせる。 3. 資格のある者が弱いパスワードを設定し使う。 4. 資格のない者が当該情報に興味を持つなどによって、これを見たり取り出したりしたいと思う。
事象	1. 資格のない者が他人のパスワードを知ったり探り当たりてる。 2. 資格のない者が他人のパスワードで不正にログインする。 3. 資格のない者が情報を見たり、取得したりする。 4. 資格のない者が情報を漏洩したり悪用したりする。
結果	1. お客様が不利益を被る。 2. 会社の信頼を損なう。 3. 会社が経済的損害を被る。

リスク =
場面1 のシナリオにおいて
結果が組織にもたらす影響

事例　場面2のシナリオ　リスク源、事象、結果

情報セキュリティ目的	顧客情報管理システムに持つ情報を資格のない者に漏洩しない。
場面2　　運用担当者の不正	
リスク源	1. 運用担当者に対する教育と意識づけが足りない。 2. 運用担当者が情報を悪用しようと思う。 3. サーバにある情報が、USBメモリなどに容易に取り出せる機器構成・設定になっている。 4. 運用規則が足りない。（記憶媒体持込み禁止が明文化されていない。サーバルームの入退室手順が簡易である。） 5. 不正・悪用を牽制するモニタリングの仕組みがない。
事象	1. 運用担当者がサーバルームに記憶媒体を持ち込む。 2. 運用担当者が情報を持ち出す。 3. 運用担当者が持ち出した情報を悪用する。
結果	1. お客様が不利益を被る。 2. 会社の信頼を損なう。 3. 会社が経済的損害を被る。

リスク =
場面2 のシナリオにおいて
結果が組織にもたらす影響

事例　場面3のシナリオ　リスク源、事象、結果

情報セキュリティ目的	顧客情報管理システムに持つ情報を資格のない者に漏洩しない。
場面3　　情報システム又はネットワークの不備	
リスク源	1. 顧客情報を情報システムに持つ。 2. 顧客情報管理システムをインターネットにつながる内部ネットワークに置く。 3. セキュリティ設定について担当者の技術力が足りない。 4. 脆弱性情報の収集と脆弱性への対応が不十分である。 5. 顧客情報管理システム又はネットワークの設定に不備がある。 6. 外部から不正侵入を試みる者が存在する。
事象	1. 組織の内部ネットワークに外部者が侵入する。 2. 情報システムに外部者が侵入する。 3. 外部者が顧客情報を見たり取得したりする。 4. 外部者が顧客情報を悪用する。
結果	1. お客様が不利益を被る。 2. 会社の信頼を損なう。 3. 会社が経済的損害を被る。

リスク ＝
場面3 のシナリオにおいて
結果が組織にもたらす影響

リスク特定のポイント

- リスク源、事象、結果を文で記述して、場面、状況、シナリオを明らかにする。

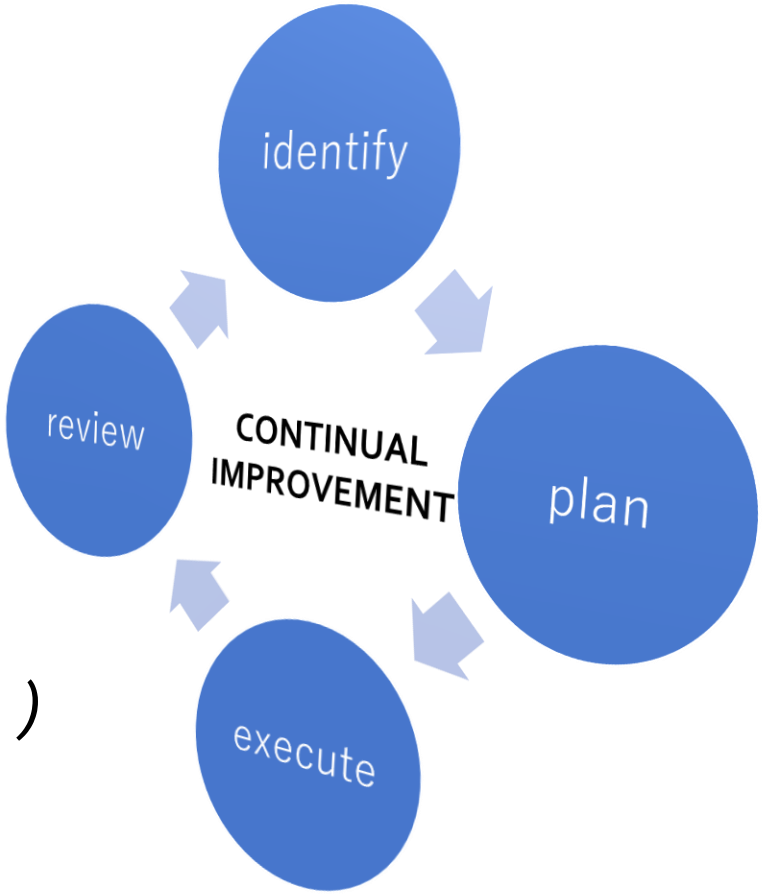
- リスク源、事象、結果のいずれも、場面ごとに一つとは限らない。
  - 状況の展開を想定する。
  - 複数のリスク源、複数の事象、複数の結果の間に関係や構造がある。

- **リスク**（目的に対する不確かさの影響）とは、場面について描いたシナリオにおける、「結果」が組織にもたらす影響

ISO/IEC 27001 ISMS (Information security management system)

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

- Anticipate
- Prepare
- Protect
- Reactive & Responsive
- Adaptive *(business plasticity（変化への対応）)*
- **CONTINUAL IMPROVEMENT** 改善



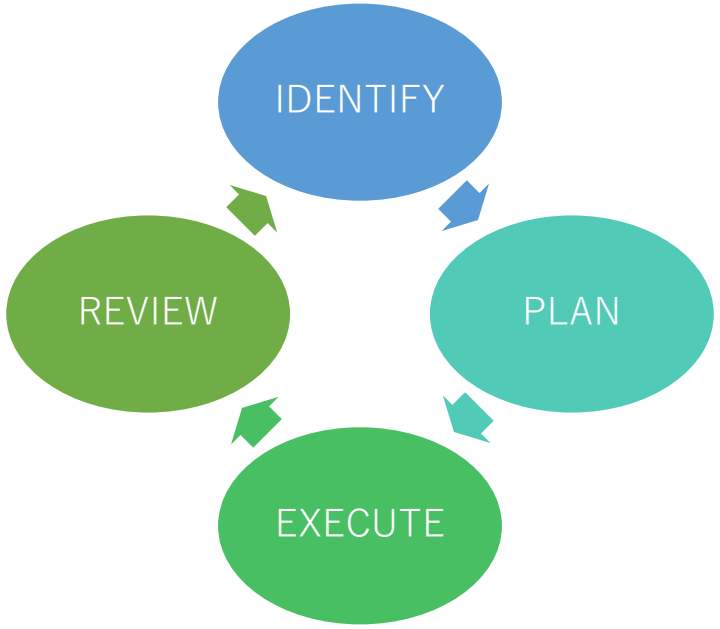
From Dr. Edward Humphreys

ISO/IEC 27001:2005
Number of certificates per country for 2017

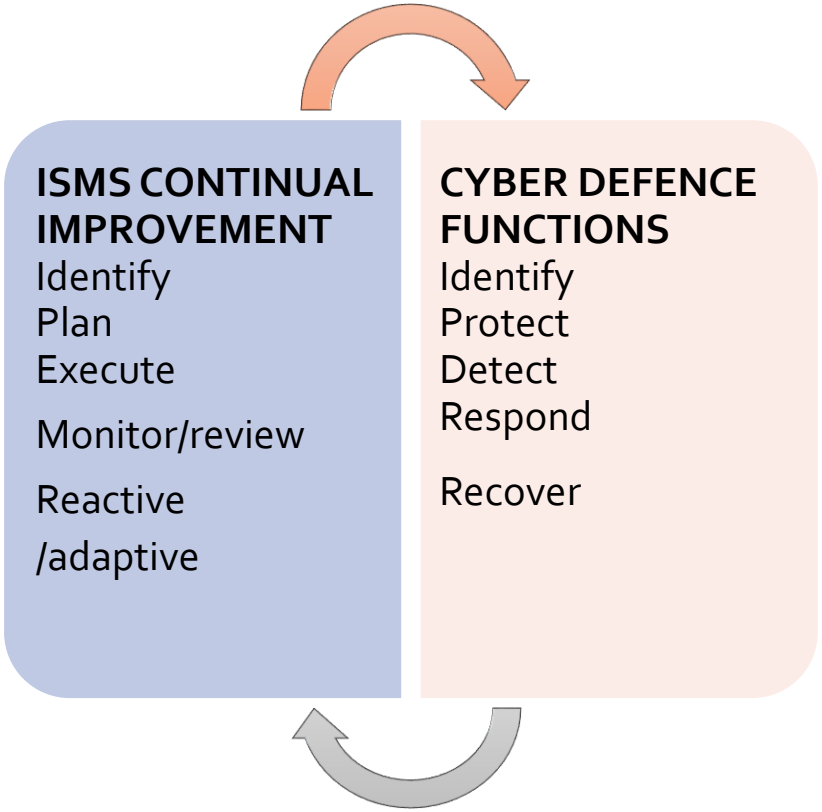
	Country	Number of Certificates
1	Japan	9161
2	China	5069
3	United Kingdom of Great Britain and Northern Ireland	4503
4	India	3272
5	United State of America	1517
6	Germany	1339
7	Taiwan, Province of China	994
8	Italy	958
…	…	…
Total	160 countries	39501

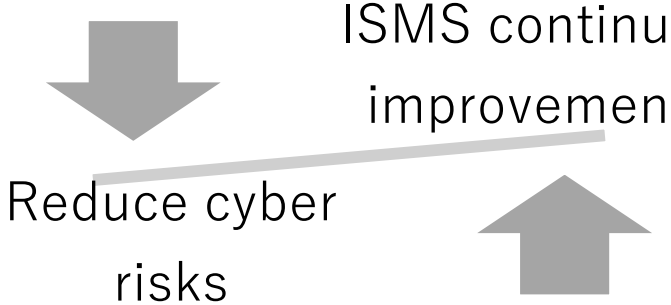
古いデータですみませんが、最新データ更新がなされていない

ISO/IEC 27001 ISMS - Managing Cyber Risk



ISMS Continual Improvement Framework





From Dr. Edward Humphreys

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

国際標準化のプレイヤー

JNSA

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 …

ISO/IEC JTC1/SC27

"Information security, cybersecurity and privacy protection"

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

WG 1	WG 2	WG 3	WG 4	WG 5
Information security management systems	Cryptography and security mechanisms	Security evaluation, testing and specification	Security controls and service	Identity management and privacy technologies

75 countries (NSB) involved (51 P-members and 25 O-members)
36 external liaison bodies (L-members), 32 internal liaisons
950+ experts (NSB + Liaison Bodies)

ISO/IEC JTC 1/SC 27

Information Security Management Organistion of Standards Work Within SC 27

Information security management system (ISMS) requirements

plus

ISMS supporting guidance - codes of practice of information security controls, ISMS risk management, ISMS performance evaluation and ISMS implementation guidance

ISMS sector specific security controls *(including application and sector specific e.g. Cloud, Telecoms, Energy, Finance)* **and sector-specific use of ISMS requirements standard**

Security services and controls *(focusing on contributing to security controls and mechanisms, covering ICT readiness for business continuity, IT network security, 3rd party services, supplier relationships (including Cloud), IDS, incident management, cyber security, application security, disaster recovery, forensics, digital redaction, time-stamping and other areas)*

Identity management and privacy technologies *(including application specific (e.g. cloud and PII), privacy impact analysis, privcy framework, identity management framework, entity authentication assurance framework, biometric information protection, biometric authentication)*

ISMS accreditation, certification and auditing *(including acreddited CB requirements, guidance on ISMS auditong and guidelines for auditors on ISMS controls)*

Security Evaluation, Testing and Specification *(including evaluation criteria for IT security, framework for IT security assurance, methodology for IT security evaluation, cryptographic algorithms and security mechanisms conformance testing, security assessment of operational systems, SSE-CMM, vulnerability disclosure, vulnerability handling processes, physical security attacks, mitigation techniques and security requirements)*

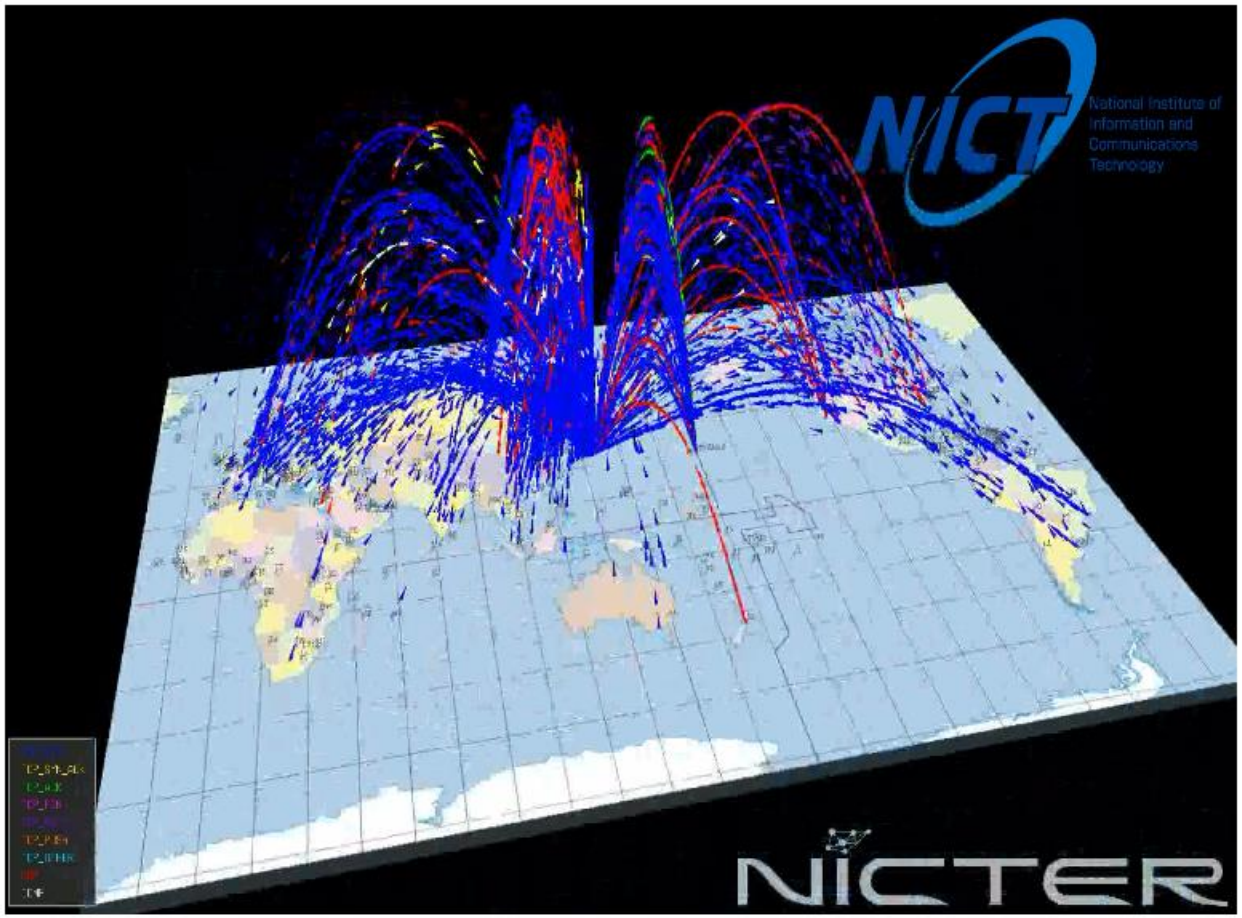
Cryptographic and security mechanisms *(including encryption, digital signature, authentication mechansisms, data integrity, non-repudiation, key management, prime number generation, random number generation, hash functions)*

Challenges for Cyber Security and Privacy Standards
New and Emerging Areas of Standardization within ISO and IEC

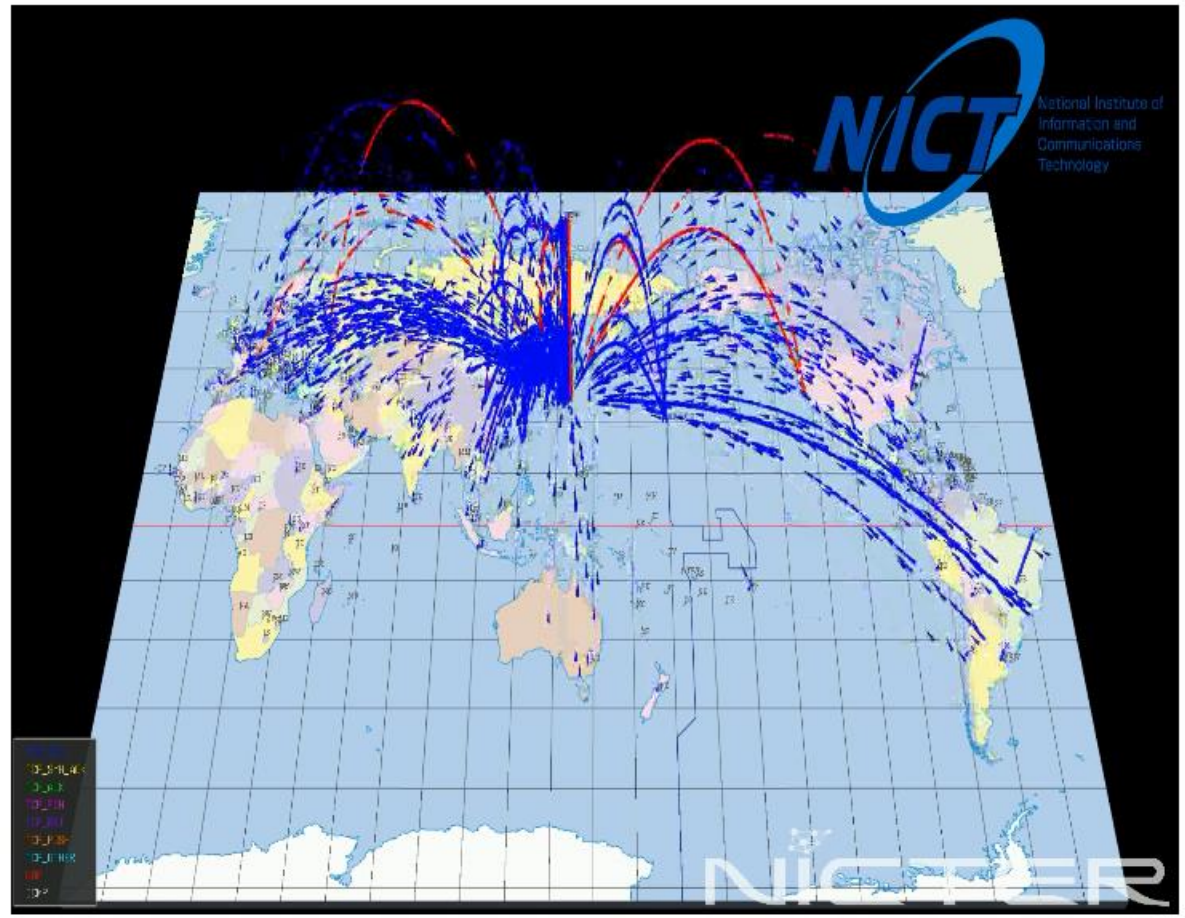
Together with ISO/IEC 27001 standard

- *IoT (Internet of Things)*
- *Smart Cities, Systems and Devices*
- *Big Data, Cloud*
- *AI systems and Machine Learning*
- *Blockchain-Distributed Ledger Technology evolution/revolution*
- *5G applications and services*
- *Quantum computing – QKD…*
- *Active Information Sharing*
- *Etc.*

IoT機器からの脅威の例（NICTERから）



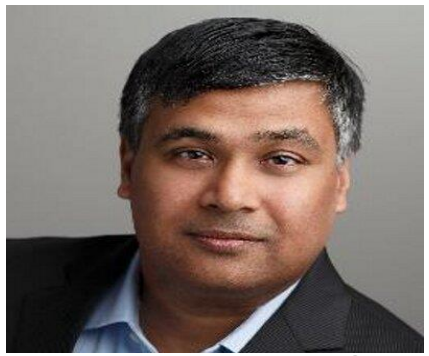
NICTERにおける全スキャン



NICTERにおけるIoT機器からのスキャン

事例：IoTセキュリティの国際規格化動向

ISO/IEC 27400 の事例




ISO/IEC JTC 1/SC 27/WG 4 **N 4624**

ISO/IEC JTC 1/SC 27/WG 4 "Security controls and services"
Convenorship: **ILNAS**
Convenor: **Amsenga Johann Mr**

Text for ISO/IEC 3rd CD 27400

Document type	Related content	Document date	Expected action
Project / Draft	Project: ISO/IEC CD 27400.2	2020-12-25	INFO

Information technology – Security techniques – Guidelines for security and privacy in Internet of Things (IoT)

further processing.

ISO/IEC 27400の発端は、日本のガイドライン JNSA

- IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの（平成28年7月5日公開）。

	指針	主な要点
方針	**IoTの性質を考慮した基本方針を定める**	• 経営者がIoTセキュリティにコミットする • 内部不正やミスに備える
分析	**IoTのリスクを認識する**	• 守るべきものを特定する • つながることによるリスクを想定する
設計	**守るべきものを守る設計を考える**	• つながる相手に迷惑をかけない設計をする • 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 • 安全安心を実現する設計の評価・検証を行う
構築・接続	**ネットワーク上での対策を考える**	• 機能及び用途に応じて適切にネットワーク接続する • 初期設定に留意する • 認証機能を導入する
運用・保守	**安全安心な状態を維持し、情報発信・共有を行う**	• 出荷・リリース後も安全安心な状態を維持する • 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 • IoTシステム・サービスにおける関係者の役割を認識する • 脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		• 問合せ窓口やサポートがない機器やサービスの購入・利用を控える • 初期設定に気をつける • 使用しなくなった機器については電源を切る • 機器を手放す時はデータを消す

27400のスコープと目次

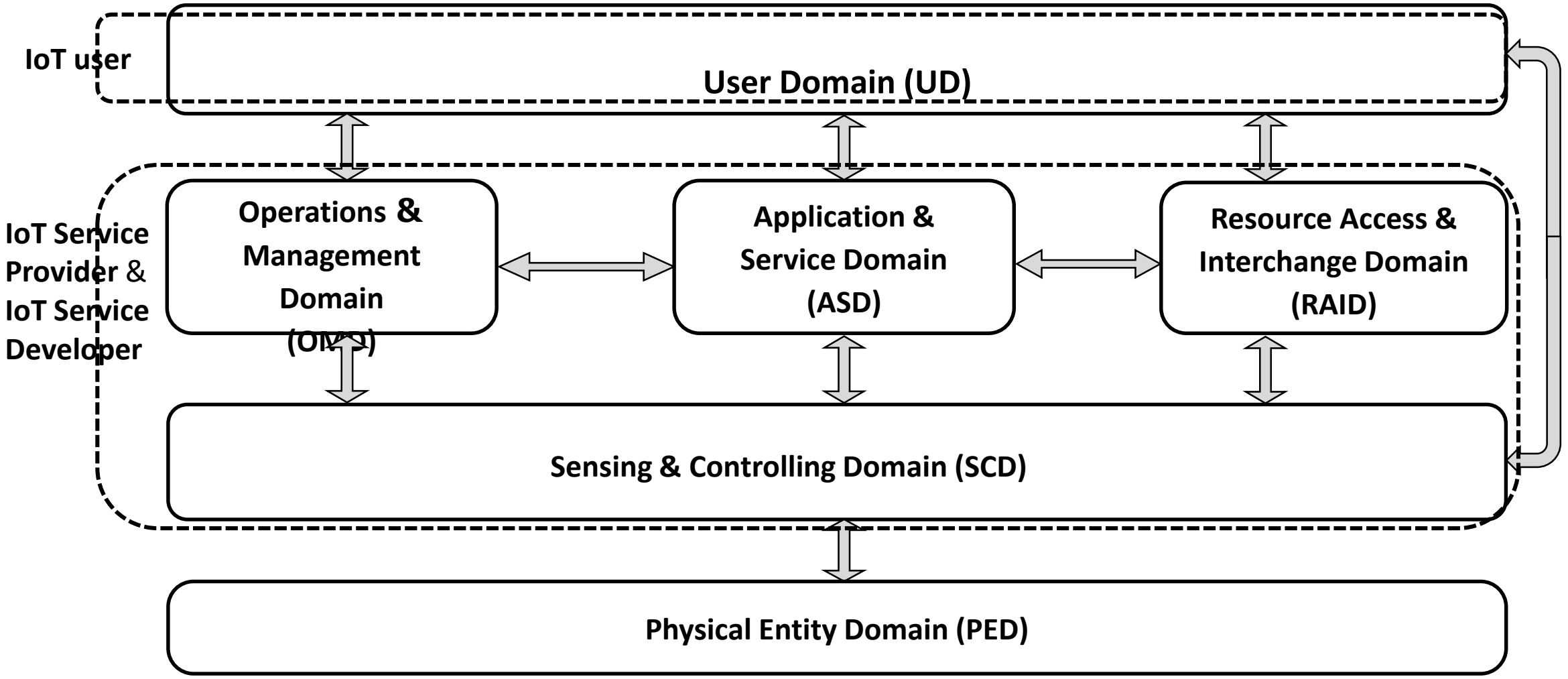
JNSA

5 IoT concepts and reference models
5.1 General
5.2 Characteristics of IoT systems
5.3 Stakeholders of IoT systems
5.4 IoT ecosystem
5.5 IoT Service Lifecycle
5.6 Domain based Reference Model
6 Risk management for IoT Systems
6.1 Introduction
6.2 Risk Sources
6.3 Risk scenarios and risks of an IoT system
7 Security and privacy controls
7.1 Security controls
7.1.1 General
7.1.2 Security controls for IoT service developer and IoT service provider
7.1.3 Security controls for IoT user
7.2 Privacy controls
7.2.1 General
7.2.2 Privacy controls for IoT device developer and IoT service provider

Scope

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

IoT　参照モデル（ISO/IEC 30141より）



開発中のセキュリティ管理策（１）

- Security controls for IoT service developer and IoT service provider
- 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 Mobile device policy
- 7.1.2.5 Equipment and assets located outside physical secured areas
- 7.1.2.6 Secure disposal or re-use of equipment
- 7.1.2.7 Learning from security incidents
- 7.1.2.8 Secure IoT system engineering principles
- 7.1.2.9 Secure development environment and procedures
- 7.1.2.10 Security of IoT systems in support of safety
- 7.1.2.11 Security in connecting varied IoT devices
- 7.1.2.12 Verification of IoT devices and systems design
- 7.1.2.13 Monitoring and logging
- 7.1.2.14 Protection of logs
- 7.1.2.15 Use of suitable networks for the IoT systems

開発中のセキュリティ管理策（２）

- 7.1.2.16 Secure settings and configurations in delivery of IoT devices and services
- 7.1.2.17 User authentication
- 7.1.2.18 Applying updates during operation
- 7.1.2.19 Sharing vulnerability information
- 7.1.2.20 Notification of risks and required actions
- 7.1.2.21 Security measures adapted to the lifecycle of IoT system and services
- 7.1.2.22 Guidance for IoT users on the proper use of IoT devices and services
- 7.1.2.23 Determination of security roles for stakeholders
- 7.1.2.24 Management of vulnerable devices
- 7.1.2.25 Management of supplier relationships for information security
- 7.1.2.26 Information security in IoT devices

Security controls for IoT user

- 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

7.1.2.11 Security in connecting varied IoT devices

管理策11（多様なIoT機器を接続する際のセキュリティ）の例

Control-11

An IoT system should be designed and implemented to ensure and maintain security in connecting varied IoT devices.

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.

Audience:IoT service developer / IoT service provider

IoT Domain:Operations & Management / Application & Service / Resource Access & Interchange / Sensing and Controlling

Guidance

The IoT service developer and the IoT service provider design and implement an IoT system and require the IoT devices to meet defined specifications. The IoT devices are tested as components of the IoT system.

There is possibility that the IoT devices not yet tested as components of the IoT system are adopted. This is possible because testing all of the new models of supported devices can be impracticable. Or, IoT users, as consumers, can choose the devices available at market.

27400へのコメント対応など

- エディタを議長として、毎回各国から提出されるコメントを一つずつ精査し、結果をドラフトに反映。
- 国際規格化は、技術を決める中で、参加メンバの**「共通言語」としての規格化を進める**ため、「言葉」の使い方については、非常にセンシティブである。
- 現在のISO/IEC 27400 は、第3版のCDである。
  （PWI→WD→CD→DIS→FDIS→発行）
  - コメントの主な提出国：
    スイス、日本、フランス、ドイツ、米国、インド、中国等
  - 次のステップは、DIS化を目指している。

米国、英国におけるIoTセキュリティ動向（参考）

34

米国の事例

IoT Cybersecurity Certification

DHSからの資料

CTIA: the U.S. wireless communications industry

35

New Wireless Industry Cybersecurity Tool

CTIA Certification announces IoT Cybersecurity Certification Program

- Developed in collaboration with wireless providers, technology companies, and **certification test labs**
- Program will certify **cellular-connected IoT devices**, including those that connect to Wi-Fi （セルラー接続のIoT機器の認証を）
- **Highly experienced third-party test labs will perform the testing certification**
- Builds on CTIA Certification's 25-year history of wireless device certification and testing programs
- Test labs began accepting devices for certification on **October 29, 2018（継続中）**

36

Three Types of Certification

IoT device manufacturers may seek one of three types of certification depending on sophistication of device and security characteristics needed:

Level 1 - Core	Level 2 - Enhanced	Level 3 - Advanced
In-home cellular personal ERS	Connected streetlight	Perishable goods tracking device（生鮮品追跡装置）
Consumer drone	Industrial router	Blood glucose monitoring meter（血糖値モニターメーター）
GPS tracker	Home security console	Water, gas, electricity meters
Traffic monitor	Smart home controller	Industrial LTE gateway
GPS dog collar	Mobile payment devices	Secure services gateway

37

Test Elements （テストの要素、項目）

IoT Cybersecurity Certification Program test elements:

Level 1 - Core

- Terms of Service and Privacy Policy
- Password management
- Authentication test
- Access controls
- Patch management
- Software upgrades

Level 2 - Enhanced

- Includes Level 1 elements
- Audit log
- Encryption of data in transit
- Multi-factor authentication
- Remote deactivation
- Secure boot
- Threat monitoring
- IoT device identity

Level 3 - Advanced

- Includes Level 2 elements
- Digital signature validation
- Encryption of data at rest
- Tamper resistance
- Design-in features

38

Key Benefits

IoT Cybersecurity Certification Program:

- Creates an industry benchmark for IoT security on wireless networks
（ワイヤレスネットワークでのIoTセキュリティの業界ベンチマークの策定）

- Builds on IoT security recommendation from NTIA (National Telecommunications and Information Administration) and NIST
（NTIA/NISTからのIoTセキュリティ勧告に基づいて構築）

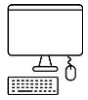
- Helps protect consumers and wireless infrastructure, while creating a more secure foundation for smart cities, connected cars, mHealth, and other IoT applications
（スマートシティ、コネクテッドカー、mHealth、その他のIoTアプリケーションのより安全な基盤を構築しながら、消費者とワイヤレスインフラストラクチャの保護を支援）

39

IoT Cybersecurity Certification Processes

1 

IoT device vendor creates new device

2 

Device vendor submits a request for certification via the CTIA Certification LLC database at ctiacert.org/

3 

Device vendor selects a Test Lab that has been authorized by CTIA Certification LLC

4 

Authorized Test Lab tests the device based on the level of certification chosen by the device vendor

5 

Authorized Test Lab and device vendor each submit required documentation to the certification database upon completion of testing

6 

CTIA Certification LLC ensures all requirements have been met

7 

CTIA Certification LLC sends certification notice to the IoT device vendor

40

英国の事例

英国情報通信政策（IoTセキュリティ行動規範）の公表

2018年10月14日、デジタル・文化・メディア・スポーツ省（Department for Digital, Culture, Media and Sport: DCMS）は、インターネットに接続する機器のセキュリティを向上するため、消費者向けIoT製品の設計段階で安全性が確保されるよう、製品の開発、製造、販売に関わる利害関係者が遵守すべき事項をまとめた行動規範を公表した。

消費者向け IoT 製品のセキュリティに関する行動規範

タイトル

消費者向け IoT 製品のセキュリティに関する行動規範

日付

2018 年 10 月

概要

私たちの身のまわりには、インターネットに接続するデバイスが増加しています。それに伴い、これまでオフラインで利用していた製品や家電の「モノのインターネット（IoT）」化も進んでいます。

IoTは、新しい時代の象徴です。テクノロジが人々の暮らしの一部となり、より便利でより楽しい生活を実現します。多くの個人データがオンライン上のデバイスやサービスに保存されている今、こうした製品に対するサイバーセキュリティ対策は、自宅の防犯強化と同じくらい重要なものになっています。

本行動規範は、消費者向け IoT 製品の設計段階で安全性が確保されるように、またユーザーがデジタルの世界を安心して楽しめるようにガイドラインを設けることで、こうした製品の開発、製造、販売に携わる利害関係者を支援することを目的として作成されています。

本行動規範は、IoT のセキュリティにおけるベストプラクティスを、成果に焦点を当てた 13 項目のガイドラインにまとめたものです。本行動規範は、デジタル・文化・メディア・スポーツ省（DCMS）が、国家サイバーセキュリティセンター（NCSC）と協力し、産業界、消費者団体、学界とも連携して作成しました。本行動規範の草案は、2018 年 3 月に、Secure by Design 報告書の中で発表されました。[1]

はじめに

モノのインターネット（IoT）は、人々に大きなチャンスをもたらします。しかし、市場に出回っているデバイスのほとんどについて、基本的なセキュリティ対策が施されているとはいえない状況です。インターネット接続を利

---

[1] DCMS、2018 年、「Secure by Design: Improving the cyber security of consumer Internet of Things: Report（セキュリティバイデザイン：消費者向け IoT 製品のサイバーセキュリティの強化）」
https://www.gov.uk/government/publications/secure-by-design

【ポイント】

- 本行動規範は、2018年3月に公表された「セキュア・バイ・デザイン」報告書の中で草案が示されていたものであり、今般、正式に公表に至ったもの。
- 本行為規範は、消費者向けIoT製品を利用するユーザーのセキュリティに関する負担を軽減することを目的に、その開発、製造及び販売の段階で安全が確保されるよう、**製造メーカー等が実践すべき対策をベストプラクティスとしてまとめたもの**。**規範的なものではない**。
- 本行為規範は、DCMSを中心に、国家サイバーセキュリティセンター（National Cyber Security Centre: NCSC）と協力し、産業界、消費者団体、学界等と連携して作成。
- テック企業であるHP及びCentria Hiveは、本行為規範への遵守を表明した最初の企業。

具体的な内容

（１）本行為規範は、IoTセキュリティにおけるベストプラクティスについて
　　成果に焦点を当てた13項目のガイドラインにまとめたもの。
（２）13項目の内容は以下の通り。
ア） 初期パスワードを設定しない
イ） 脆弱性に関する情報の公開方針を導入する
ウ） ソフトウェアを定期的に更新する
エ） 認証情報とセキュリティ上重要なデータを安全に保存する
オ） 安全に通信する
カ） 攻撃対象になる場所を最小限に抑える
キ） ソフトウェアの整合性を確認する
ク） 個人データの保護を徹底する
ケ） 昨日停止時のシステムの復旧を確保する
コ） システムの遠隔データを監視する
サ） 消費者が個人データを容易に削除できるように配慮する
シ） デバイスを容易に設置してメンテナンスできるように配慮する
ス） 入力データを検証する

国際標準化の活用の方向性（私見）

活用方法の例

JNSA

「認証(Certification)」とその関連技術として活用、e.g.

- ✓ ISO/IEC 27001/27002 + ITU-T X.1603 | ISO/IEC 27017
- ✓ IoT Stakeholders (user, provider, developer): ISO/IEC 27030 and ITU-T X.sc-iot (under development)

新しいセキュリティ技術の方向性提示として活用、e.g.

- ✓ IoT 分野、CPS・・・
- ✓ 5G 分野、繋がる車分野、ブロックチェーン・・・

インシデント管理をより改善するために活用、e.g.

- ✓ ISO/IEC 27035, ITU-T X.1056

標準的な言語や基本体系として活用、e.g.

- ✓ ASN.1, X.509 certificate, STIX/TAXII

今後の方向性（私見）

a. ISMS認証スキームを適用することに同意。 ただし、既存のISMSは、動的に変化する多様な最新の脅威を正しくカバーしていないことが問題。
b. サイバー攻撃（脅威）を効果的・迅速に管理するには、実行可能なISMS継続的改善プロセスモデルに関連して、実行可能なサイバーセキュリティ管理の導入が必要。
c. このアプローチでは、脅威の分析と、サードパーティ等による監視機能の調整を伴う効果的な監視手法が重要。
d. 組織内のFW、IDSなどの対策間の相関、 AVとPKIは重要。 さらに、インシデントを検出するには、効果的な監視スキームの準備が必要。（ただし、近年、ゼロトラストなどの議論もでてきている）
e. 外部との協調的調整のために、利害関係者間での効果的なサイバーセキュリティ情報交換と、有効な分析および監視機能を信頼できる外部と実施する必要がある。
f. このアプローチは、継続的な改善プロセスのためにさらに検討される必要がある。
g. 上記を達成するために国際的な意味のある「リファレンス」を提供するための重要な手段として、「国際標準化」の活用が期待される。

Thank you for listening Q&A