資料34－2－1

欧米動向と国際標準化の現状

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　主管研究員
横浜国立大学　客員教授
内閣官房　サイバーセキュリティ補佐官

中尾 康二

国際標準化(ISO)を推進している組織

- SC27 “IT security techniques”
  - WG4 “Security controls and services”
  - WG5 “Identity management and privacy technologies”

- 国内委員会
  - 情報規格調査会
    - 「SC27/WG4小委員会」
    - 「IoTセキュリティガイドライン SC 27/WG 4対応 小委員会」

国際標準化に向けた検討経過(１)

2016年

- **SC27/WG4においてIoTセキュリティへの取組みについての予備的検討を実施。**
  既存規格で未対応の（“gap”）要素等の調査・検討。

✓Gap 1: Gateway Security

✓Gap 2: Network Function Virtualization security

✓Gap 3: Management and measurement of IoT security (IE – metrics)

✓Gap 4: Open Source assurance and security

✓Gap 5: IoT Risk Assessment techniques

✓Gap 6: Privacy and Big Data

✓Gap 7: Application Security Guidance for IoT

✓Gap 8: IoT Incident Response Guidance

本GAP分析はあまり役に立たなかった。日本からは２０１７年からのガイドライン化を提案した。（次ページ）

国際標準化に向けた検討経過（２）

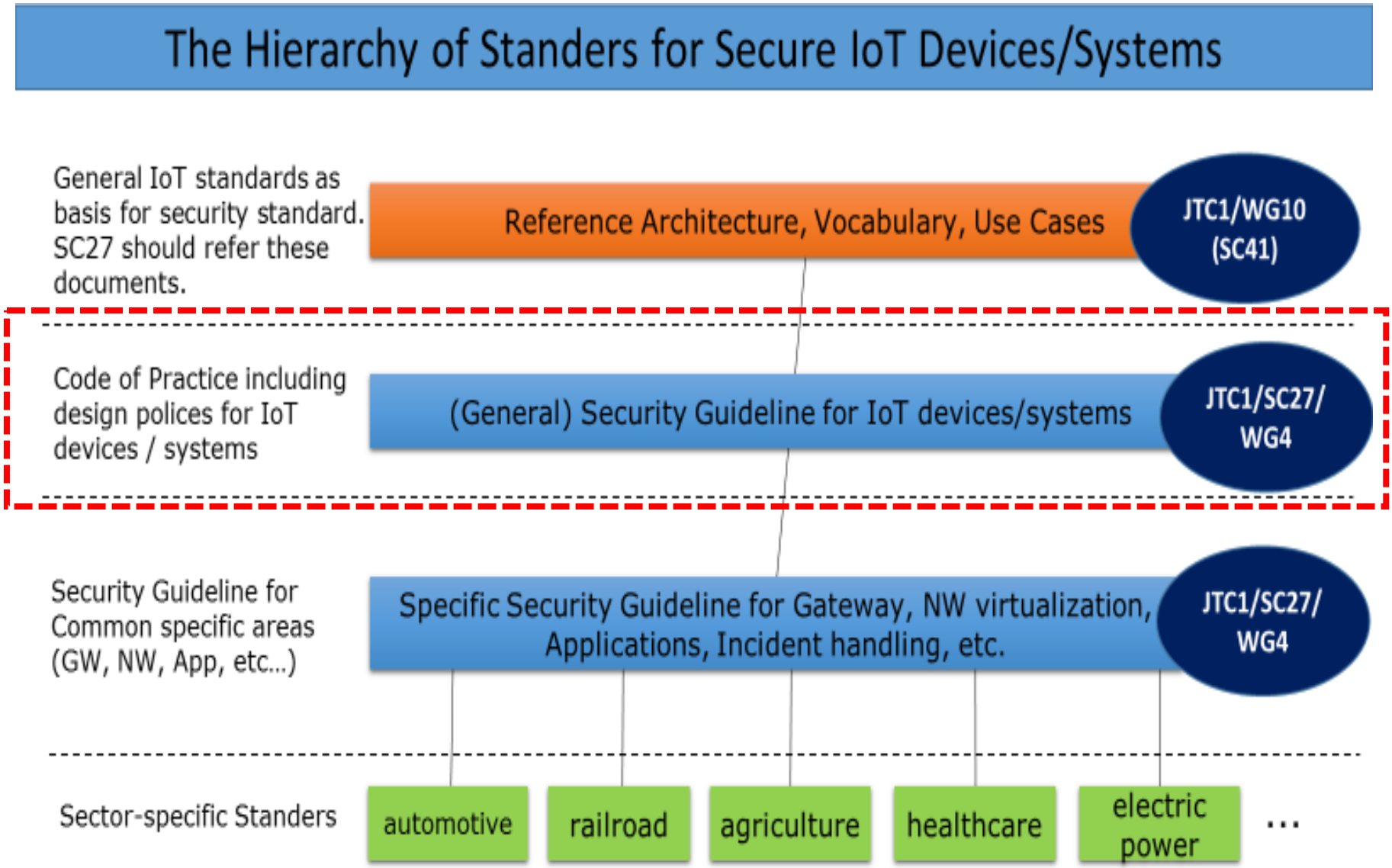
2017年4月～10月/11月

- 指針開発に向けた検討期間 (SC27/WG4)
  “Study Period on Guideline for Security and Privacy for IoT”
- 6月～9月　3回のWeb-EX会議
- 11月1日/2日　SC27会議 (ベルリン) の中で審議
  - プロジェクト開始のための New Work Item Proposal の内容を決定した。 → 資料 SC27 N17772, N17773
  - 添付する Preliminary Draft に「IoTセキュリティガイドライン」(IoT推進コンソーシアム/総務省/経済産業省) の内容を反映している。

2017年12月～2018年4月

- 12月～3月：SC27武漢会合への準備、NWIPの投票
- 2018年4月18日、19日：武漢会合で審議
  （以下、武漢会合の結果要約）

日本提案のガイドラインの位置づけ：ハイレベルな規格化を目指して



SC27武漢会合報告（2018年　春）

“Guidelines for security and privacy in Internet of Things (IoT)”のNWI化

NWI:新課題（規格化検討がスタート）

審議内容

- Acting Chair：Faud Khan （カナダ）

審議

- NWI化の投票結果の確認（次ページ）
- ベースドキュメント
  - N17772　（NWIP）
  - N17773　（PD)
- 寄書の紹介と議論
  - 日本寄書
  - フランス寄書
  - ドイツ　コメント
  - カナダ　SC41へのNWIの紹介（口頭のみ）

NWI化の投票結果

賛成国：21（日本、米国、フランス、ドイツ、カナダ、韓国など）

反対国：2（コスタリカ、オランダ）

- コスタリカ：
  Proposal lacks of clear information security objectives definition for IoT systems, such that risks identification/evaluation can be defined appropriately. Then, section 13 for security and privacy controls is not sustainable because the required basis are not well defined. As a minor observation, most definitions and abbreviations of sections 3 and 4 are missing, for example, SaaS, PaaS, IaaS, multi-tenancy, LOB, etc.
- オランダ：
  a document like this might be relevant, but should not be developed within ISO

棄権国：29（英国など）

一応、上記の結果から、NWIは承認。プロジェクト化が決定！

日本寄書の審議結果

1. IoT環境におけるリスクをどのように決め、設定していくのか
   リスクについては、PDに章立てがあり、今後の検討事項となる
2. IoT環境におけるライフサイクルのための初期アイディアの提案
   原案としてはよいかもしれないが、廃棄や継続メンテナンスなど、改良が必要との指摘あり（英国）
3. どのようにセキュリティ管理策を開発していくのか
   この部分も明確な意見はなし。今後の検討

日本のコメントは、PDをベースに作られる第1版のWDにおいて、エディタノートとして追記される予定。

N2077_Draft_PDの目次原案

1. Scope
2. Normative references
3. Terminology
4. Abbreviations
5. Overview
    - 5.1 General
    - 5.2 Stakeholders (IoT Service provider, IoT Service developer, IoT user)
    - 5.3 Reference Model (based on ISO/IEC 30141 (IoT RA))
    - 5.4 IoT life cycle
6. Security and Privacy Principles
    - 6.1 Security Principles
    - 6.2 Privacy Principles
7. Security and Privacy Controls
    - 7.1 Security Controls
    - 7.2 Privacy Controls

Bibliography

Annex: Security Considerations for Gaps

Proposed “Security Principles” from JP

Principle 1
Establish a policy for security of IoT.

Principle 2
Identify risks on IoT security.

Principle 3
Apply secure design basics in IoT.

Principle 4
Apply network controls.

Principle 5
Maintain security of IoT. Inform relevant parties of updates on risks and controls (for sharing them).

IoT推進コンソーシアムで策定されたセキュリティガイドラインがベースになっている。

Proposed “Security Controls” from JP

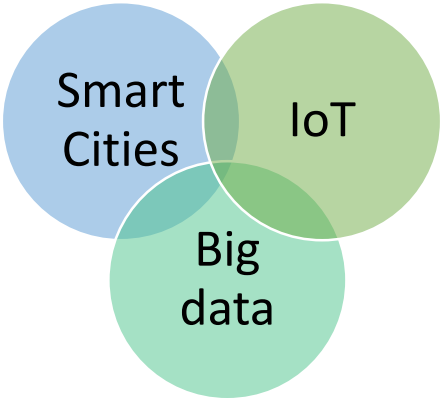
1. **Management commits to IoT security**
2. **Prepare against internal fraud or human errors**
3. **Identify what to protect**
4. **Identify risks derived**
5. **Identify the impacts systems**
6. **Identify risks off-pre**
7. **Learn from experiences**
8. **Design and implement security controls against risks from various risk sources in IoT**
9. **Design and implement security functions and operations against abnormalities of IoT devices and systems**

IoT推進コンソーシアムで策定されたセキュリティガイドラインがベース

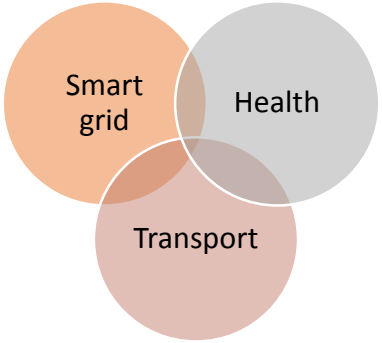
10. Design security and safety considering their interactions
11. Design security of IoT devices and systems adaptable to varied security levels of connecting devices or systems in the network
12. Verify and evaluate the design to ensure safety and security
13. Implement network controls with monitoring and recording functions
14. Utilize the networks suitable to the IoT devices and services
15. Ensure secure settings and configurations
16. Implement authentication functions
17. Maintain security of IoT systems and services in operation
18. Monitor and analyze risks of IoT systems and services in operation, and keep relevant parties informed of the risks and actions
19. Inform personal users of IoT risks
20. Determine the roles of the stakeholders of IoT systems and services
21. Identify vulnerable devices and provide appropriate alerts

フランス（Afnor）寄書の紹介

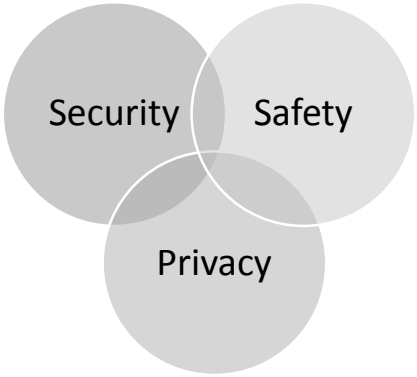
ICT Trend towards Complex Ecosystems



Ecosystems



Domains



Concerns

フランスの寄書のポイントは、今回のIoT規格化は、エコシステムとしての整理学が必要で、これまで検討されている規格の構成も参考とすべき。

武漢会合の結論の要約

1. NWIは成立、今後、WDを作成し、次回のSC27でコメント処理を進めていく(通常のプロセス)
2. 寄書は、日本、フランス、ドイツ(コメント)からあり、それらは会合で共有。また、SC41におけるカナダの提案紹介があり、その提案への賛同を求められたが、無反応。
3. メインエディタ:Faud Khan (カナダ)
   共同エディタ:Antonio Kung (フランス)、Luc Poulin (カナダ)、
   中尾 康二 (日本)
4. 第1版WDについては、Faud Khan氏が作成。共有した寄書やコメントについては、WD内部にエディターノートとして記載。今後のWDへのコメントの参考とする。作成されるFaud氏のWDについては、共同エディタと共有され、修正される予定。
5. 次回のノルウェー会議の前までに、2回のWebEx会合を開催予定。
   第1回:June 12 @ 13:00 UTC
   第2回:July 10 @ 13:00 UTC
6. 認証に関する件については、未審議。

認証スキームの方向性

ー認証に関わる考察ー

認証に関わる議論
（武漢にてローカルに）

- 現状、どのような方向かは決まっていない。
- また、どのような方向で審議を進めるかの議論もされていない。（Gradingの話もあり・・）
- **英国：**SC27のIS（国際規格）に基づいて決めるべき。基本、ISMS的な認証となることが示唆される。
- **米国：**IoTに関わる産業系参加者／専門家を集め、本ISO規格への取り組みを活性化しようとしている段階。その中の重要な課題には認証がある。27001に基づく方法も一案との意見あり。
- **仏：**Afnorの寄書に基づき、体系的な提案を進めており、現状は認証について、直接的な言及がない。しかし、ISO/IEC 27001をベースにするイメージを持っている。SC27とSC41との規格をベースに認証を組み立てたいとの意向が感じられる。
- **独：**まだ直接的なISO/IEC 27030への貢献なし。ただし、政府レベルで具体的活動を推進したいとの意向あり。

一つの考え方として：

ISO/IEC 27001:2013, ISO/IEC 27002:2013 に基づく分野別規格とする方向もあり

IoTセキュリティガイドライン SC 27/WG 4対応 小委員会　資料

分野別規格とその開発規定

- ISO/IEC 27001:2013 及び ISO/IEC 27002:2013 に基づく分野別規格（sector-specific standard）では、当該分野に固有の要件を ISO/IEC 27001:2013 及び ISO/IEC 27002:2013 に加える。
  - 通信事業　ISO/IEC 27011
  - クラウドサービス　ISO/IEC 27017
  - エネルギー産業における制御システム　ISO/IEC 27019

- 分野別規格が満たすべき事項を要求事項として定めている規格が ISO/IEC 27009 である。
  - ISO/IEC 27009 の読者は、分野別規格の作成者である。

IoTに関連する認証スキームの方向性と今後

- ✓ ISO/IEC JTC1/SC27の規格(27030)は、ハイレベルなガイドライン制定を狙い、４年後の制定を目指しているが、２年程度で固める必要あり。（私見）
- ✓ ISO/IEC JTC1/SC27の規格(27030)の開発途中から、IoT認証について議論は開始すべき。大きな流れは、ISO/IEC 27001に基づく認証スキームを設計する方向がもっとも実現的。（私見）
- ✓ IoT機器認証を暫定的に試行し、総合的なIoT認証スキームにつなげていく案もあるかと（私見）