INSTITUTE of INFORMATION SECURITY

博士請求論文 発表会

Proposals of the IoT Device Security Quality Metrics Method (IoT-SQMM)

IoT機器のセキュリティ品質評価手法の提案

情報セキュリティ大学院大学
情報セキュリティ研究科　情報セキュリティ専攻

5685102　伊藤　公祐

発表アジェンダ

INSTITUTE of INFORMATION SECURITY

1. 本研究の概要

   参考：本論の構成

2. 本研究の必要性
3. 調査手法
4. 既存手法の課題（IoTベンダにとっての不足点）
5. 提案手法の概要
6. 提案手法の効果検証
7. 社会貢献の考察、今後の課題、まとめ
8. 外部発表

1. 本研究の概要

INSTITUTE of INFORMATION SECURITY

背景：IoT機器の脆弱性に対するサイバー攻撃が発生
大規模DDoS攻撃, クルマや医療機器のリモート操作,
重要インフラ操業停止等.

課題：IoT機器のセキュリティ対応が求められ、多くのIoT機器向け
セキュリティ対策ガイドラインが発行されるも、
IoT機器のセキュリティ対応はなかなか進展せず.

セキュリティをIoTベンダの品質管理体系の中で取り扱える方法論が必要（仮説）

**IoTベンダ向けの
セキュリティ品質メトリクスを設定する方法の提案**

1. 本研究の概要

INSTITUTE of INFORMATION SECURITY

目的：IoTベンダに適したIoT機器セキュリティ品質メトリクス設定手法の提案.

様々なIoTセキュリティ文献
からメトリクス候補を抽出

ソフトウェア品質分野に浸透する
メトリクス設定手法GQMの考え方

IoT機器のセキュリティ品質評価手法(IoT-SQMM)

- IoT機器のセキュリティ品質の要件
- IoT機器セキュリティ品質透明性モデル
- 品質メトリクスの設定手法
  ＋サンプルメトリクスの構築

IoT-SQMMの効果検証

検証1: IoTベンダ導入可能性	検証2: IoTセキュリティ要件の特徴把握ツールの有効性	検証3: 市販IoT機器セキュリティ品質評価

参考：本論の構成

1章：序論

2章：本研究の必要性（研究の動機, 既往研究, 視覚化の理由）

3章：IoT機器セキュリティ品質に関する調査

（研究手法, スコープの定義, 文献・先行研究調査）

4章：IoT機器セキュリティ品質に関する項目出し

(IoT機器セキュリティ品質の定義, 要求事項, 透明性モデル, セキュリティ品質メトリクスの提案/GQMとゴール及びサンプル, 質問とメトリクスの設定, 専門家レビューと意見分析）

5章：提案手法によるメトリクスの効果検証

(IoTベンダへの導入可能性, IoTセキュリティ要件の特徴評価ツールとしての利便性の検証）

6章：市販IoT機器のセキュリティ品質評価の検証

7章：本研究の社会的貢献の考察

8章：今後の課題

9章：結論

参考：本論の構成

INSTITUTE of INFORMATION SECURITY

10章：参考文献

11章：研究業績（Appendix に組み込む予定）

12章：Appendix

2. 本研究の必要性

INSTITUTE of INFORMATION SECURITY

本論の必要性について、IoTベンダがセキュリティ対応しない6つの原因を想定し、２つの側面から確認した。

仮説： IoTベンダがセキュリティを品質管理体系の中で取り扱える方法があれば、IoT機器のセキュリティ対応は進む

想定されるセキュリティ対応しない６つの原因：

1. 製品安全＝法規制あり、対応は義務化
   製品セキュリティ≠一部を除き、法規制なく、義務化もなし
2. セキュリティ対応の最低レベルが一般化されていない
3. セキュリティ対応コストに見合うインセンティブが不明確
4. 理想的なセキュリティ対応はIoT機器を高価にし、IoT普及を阻害
5. ユーザの求めるセキュリティ要件が不明確
6. セキュリティ品質の高さをユーザに伝える標準的な方法がない
   （品質投資価値を訴求できない）

2. 本研究の必要性

２つの側面から必要性を確認：

1. 過去に同様の手法が提案されていないか？（新規性）
   ⇒ **文献調査の結果、既存の研究・文献は存在しないことを確認した。**
   - 品質管理のアプローチでセキュリティ対応を議論する文献はなかった
   - セキュリティのために誰がいつ何を検討すべきかを明確にした文献もなし

2. セキュリティ対策の取り組みを明文化する必要はあるか？（意義）
   ⇒ **品質管理の取組みにはISO 9001に従った標準文書と取組結果の明文化の意義を確認した。**
   - 製品開発プロセスに、セキュリティの取り組みが定義されなければ、重要なことであっても実施されない（時間的余裕とコスト次第）.
   - セキュリティ対応事項をプロセス中に定義することで、セキュリティ対策に取り組みやすくなる

2. 本研究の必要性

INSTITUTE of INFORMATION SECURITY

貢献のポイント：

- IoTベンダにおけるセキュリティ品質メトリクスの設定を推進.
- IoT機器のセキュリティ品質・セキュリティ対応能力の向上.
- 安全なIoT機器の普及とそれを求めるユーザの選択肢の拡大.

筆者は，IoT機器にスコープを絞り，従来型のV字開発プロセスと顕在化しているセキュリティ問題を前提に議論したため，本手法の適用はその範囲に限定される.

IoTとは

“The internet of things (IoT)” は、Auto-IDセンタの共同創設者Ashton氏が1999年に初めて発表したコンセプト [12]

“相互連携するコンピューティングデバイス、機械、デジタルマシン、物体、動物、または人間からなるシステムで、固有の識別子（UID）を備え、人間対人間または人間対コンピュータの相互作用を必要とせずにネットワーク上でデータを転送する能力を持つもの。”

Patel et al. [13]やIoT推進コンソーシアム [14]など多くの文献がIoTの特徴を示している。

ISO/IEC 30141で、標準的アーキテクチャが定義された。

[12]Ashton K.; That 'Internet of Things' Thing; RFID J., Jun. 2009
[13]K. K. Patel, S. M. Patel, “Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges,”
[14]IoT Security Guidelines ver. 1.0, IoT Acceleration Consortium, Ministry of Internal Affairs and Communications Ministry of Economy, Trade and Industry, Japan, Jul. 2016

IoTとは

INSTITUTE of INFORMATION SECURITY

IoTアーキテクチャの例 [13]

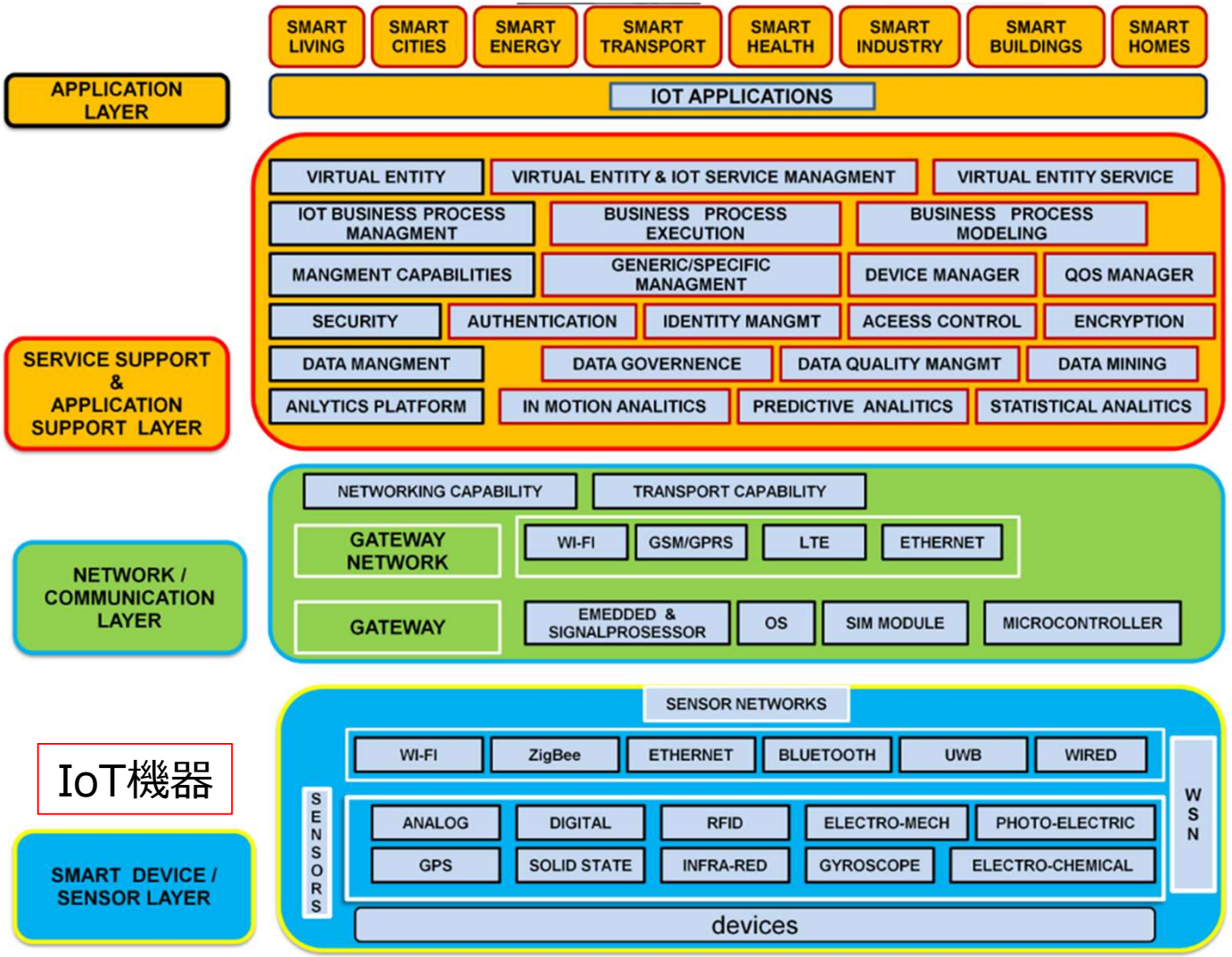
IoTサービス提供者

クラウド基盤提供者

ネットワーク提供者

IoT機器

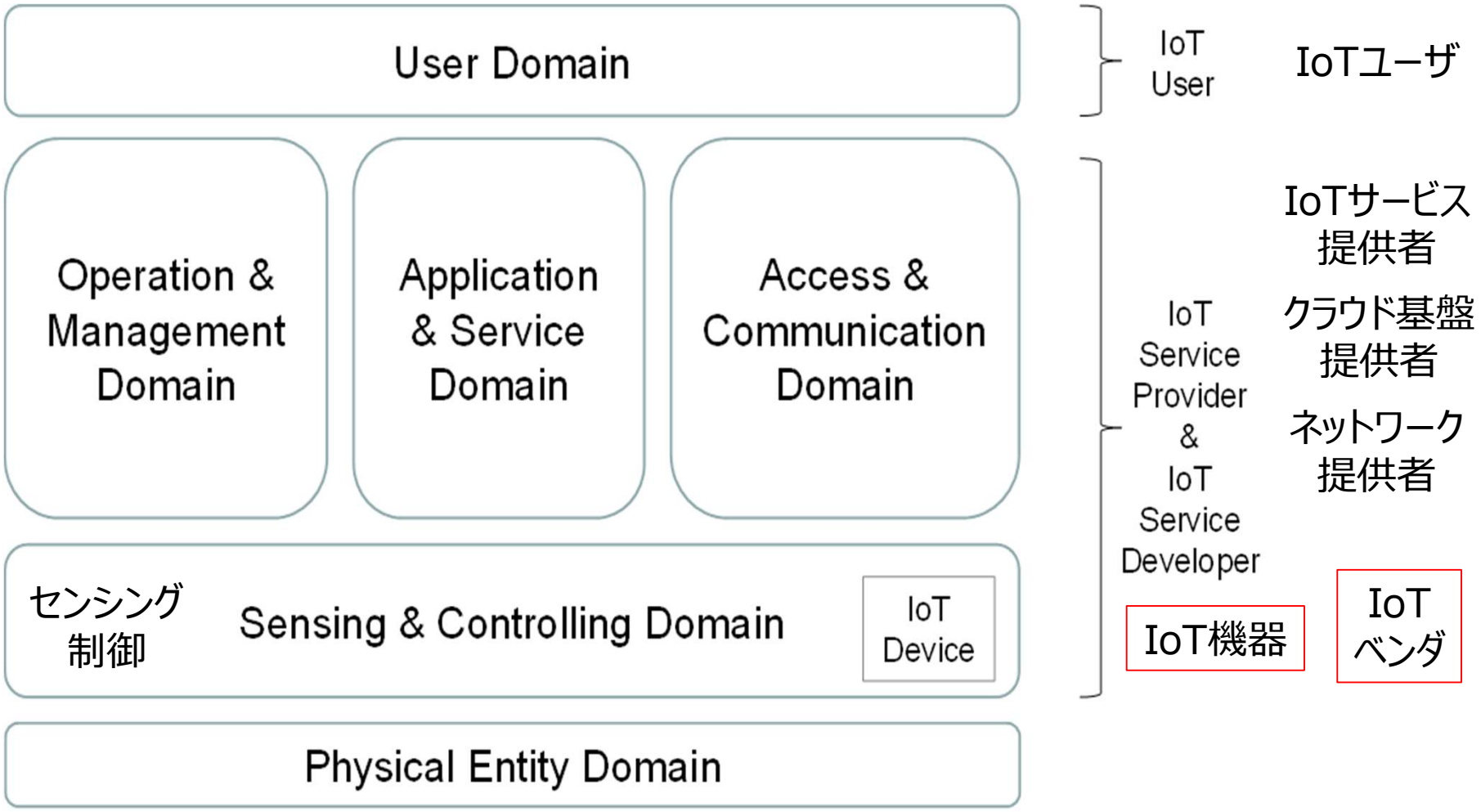
IoT ベンダ



各種センサ
接続I/F
組込み
電子機器

IoTとは

ISO/IEC 30141 Reference Architecture [15]



IoTとは

IoTアーキテクチャの主な構成：

- サイバー空間上のアプリケーションとサービス（運営管理機能含む）
  ⇒IoTサービス提供者（主にITベンダ）

- アプリ/サービスとIoT機器をつなぐネットワーク
  ⇒ネットワーク提供者（主にITベンダ）

- 様々な通信手段をもち、物理空間の状態をセンシングしたり、物理空間で動作したりするIoT機器
  ⇒IoTベンダ（主に電子機器ベンダ）

IoTとは

INSTITUTE of INFORMATION SECURITY

IoTの特徴 [13]
1） インターコネクティビティ
2） モノに関するサービス
3） 異質性
4) ダイナミックな変化
5) 巨大なスケール
6) 安全性
7） コネクティビティ

IoTの特徴 [14]
特徴1：サイバー攻撃時の広範囲への大きな影響力
特徴2：IoTのライフサイクルの長さ
特徴3：IoTの監視が困難であること
特徴4：IoT機器側とネットワーク側のステークホルダー間の相互理解が不十分
特徴5：IoTの機能・演算性能の限界
特徴6：メーカーの意図しないIoTのネットワーク接続

IoT機器に関係する特徴：

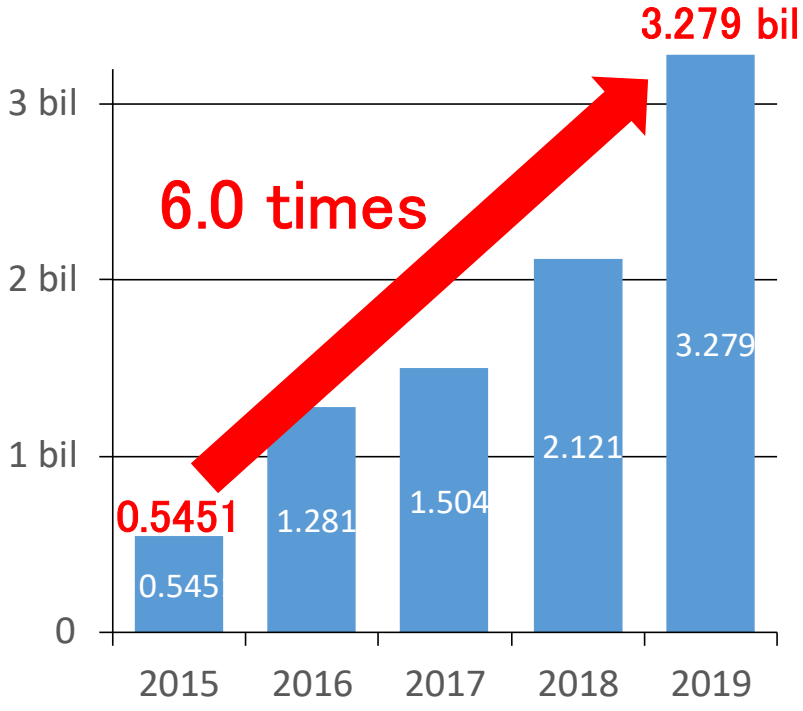
6) 安全性、	特徴2: ライフサイクルの長さ、
7) コネクティビティ、	特徴5: 機能・演算能力の限界、
	特徴6: 意図しないネットワーク接続

IoTを狙う攻撃

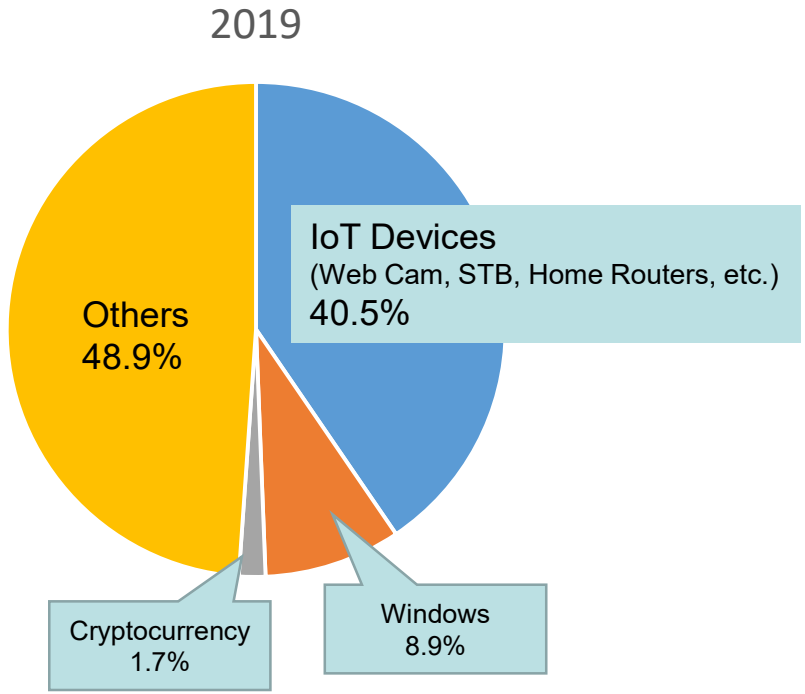
INSTITUTE of INFORMATION SECURITY

2019年に観測したサイバー攻撃に関連する通信＝2015年の約６倍，
IoT機器向けが４割

（NICT[49]）



Number of Attacks observed



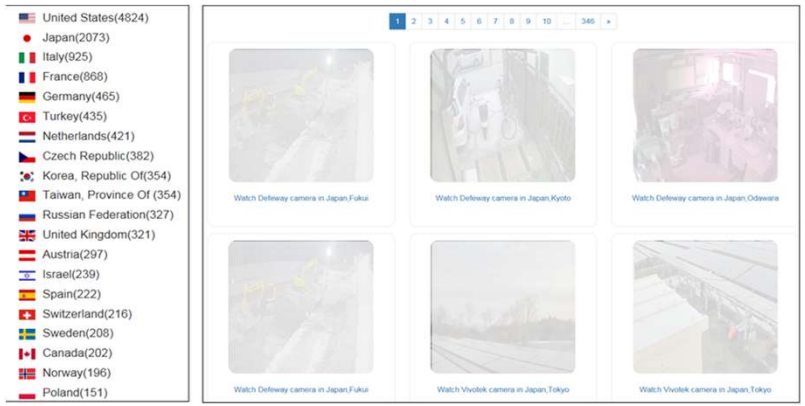
Ratio of Attacks observed in 2019

IoTを狙う攻撃

INSTITUTE of INFORMATION SECURITY

IoTに関する注目すべきセキュリティインシデント：

1. Insecam：出荷時ID/PWD等で運用されている無防備なWebカメラ
   ⇒多くのユーザは**工場出荷時のままや推測し易いID/PWD設定で使用している事実**
   工場出荷時のセキュリティ設定の必要性

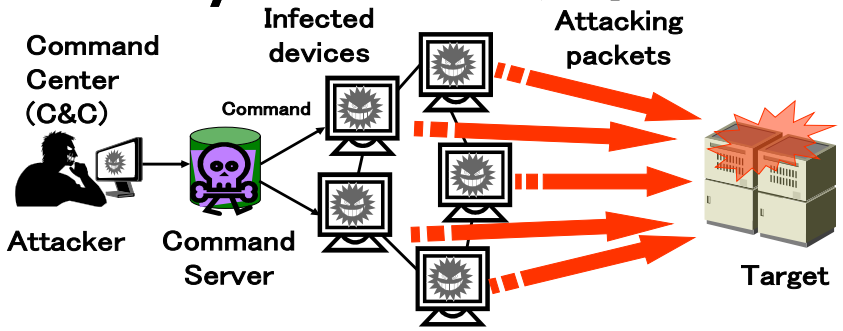


2. Jeep, Black Hat 2015：
   物理的改造をせずリモートハッキングできることを実証
   ⇒**リコール**に発展したことで、自動車業界全体が
   セキュリティ重要視へ一変
   学び：ハードウェア解析される前提のセキュリティ確保
   通信事業者やヘッドユニットのサプライヤとの責任分担
   アップデートコマンドにも要認証

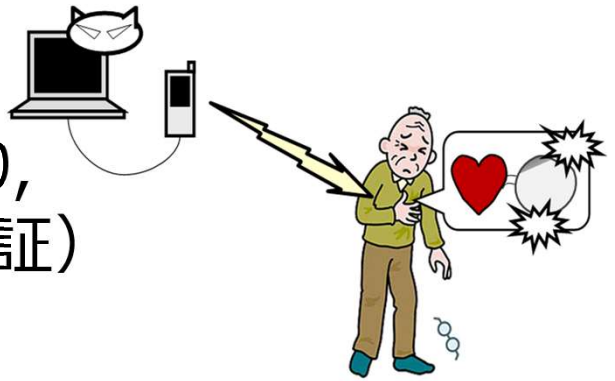
Photo: WIRED

IoTを狙う攻撃

3. Mirai, 2016：Telnet 23ポートを狙うBotnet化マルウェア.
   ⇒**大規模DDoS攻撃**による世界的規模のサービス停止
   学び：**不要ポート･不要機能の削除**
   もしくはIoT機器へのアクセス認証の**ID/PWDの難解化**



4. ペースメーカへのFDA警告：
   無線によるペースメーカーの
   ファームウェア設定が無認証で実行可能
   ⇒ FDAがリコールを要求
   学び：JEEPでも同様（無認証）の問題があり,
   過去の教訓（設定コマンド実行時の認証）
   の共有の重要性



IoTを狙う攻撃

INSTITUTE of INFORMATION SECURITY

- Mirai, 2016 — 開発用デバッグ用
- Insecam — 出荷時
- Jeep, Black Hat 2015 — アップデート用
- ペースメーカへのFDA警告 — 設定用

脆弱なID/PWDを狙う

製品ベンダに対するリコール（クルマや医療器分野に限定的）

すべてIoT機器がターゲット
ID/PWD問題は、技術的なセキュリティ脆弱性以前の問題
リコール事例⇒メーカー責任、品質問題の意識

IoTを狙う攻撃

INSTITUTE of INFORMATION SECURITY

IoT機器を狙う攻撃手法の特徴：

- IoT機器を物理的に入手しやすい
  ⇒**オンライン攻撃だけでなく、物理攻撃により脆弱性を探すことが可能**

攻撃のタイプ	**オンライン攻撃**	**物理攻撃**
開発・デバッグに使用するインタフェースからの攻撃	不要ポート探索	基盤上のJTAGやUARTからの解析
外部接続インタフェースからの攻撃	Wi-Fi/Blutoothの仕様上の脆弱性悪用 内部構造探索	USB接続による内部構造探索
使用するチップへの攻撃		クレデンシャル情報詐取（サイドチャネル）

IoTベンダとは

IoTベンダ（電子機器ベンダ）の特徴：

- **法規制遵守：**消費生活用製品安全、電気安全、製造物責任（PL）、環境負荷低減（リサイクル）等
- **知的財産権遵守：**ソフトウェア（特にオープンソース）
- **省リソース：**組込み機器の制御ロジックとしてハードウェアの一部の意識、ソフトウェアはSoC化、できるだけソフトウェアのフットプリントは小さく！
- **品質確保の基本：**ISO 9001
- **コストと不良率（歩留まり）の低減：**品質管理で製品開発する文化
  ⇒動作確認のとれた製品資産（設計、モジュール、部品、ソフト）の再利用、顧客サポート不要の使いやすさ・不具合の無さ
- **製品ライフサイクルにおける品質管理を部門で分担：**製品企画部門、設計・開発部門、品質保証部門、生産部門、市場サポート部門

これらに、「セキュリティ」はなかった.

IoTベンダのセキュリティ対応のハードル

IoTベンダにとっての「セキュリティ」＝一般的に「情報セキュリティ」

ISO27001、情報資産管理の重要性は認知されている。
　⇒ただし、一般的に、IT部門の管轄　という意識

では、製品のセキュリティとは？
従来の品質管理プロセスに、「セキュリティ」対応は定義されていない。

製品のセキュリティ対応の定義が必要
どの部門が何をどのプロセスで対応すればよいか、
だれも答えがない

IoTベンダの問題の捉え方

ビデオレコーダーのセキュリティ問題（スパムメール発信の踏み台）
⇒2004年（10年以上も前）。
なぜ、このような基本的な問題が、いまだに解決されないのだろうか？

筆者の推察：

- ユーザの使いやすさ、Plug＆Playの設計方針が優先された
- ユーザにとって、踏み台となったビデオレコーダーは正常に機能しており、不利益はなかった⇒気づかないユーザも多かった可能性あり
- ベンダは，ユーザが適切なパスワード設定をせずに使用したユーザ責任問題もしくはマニュアルでの案内不足と認識した

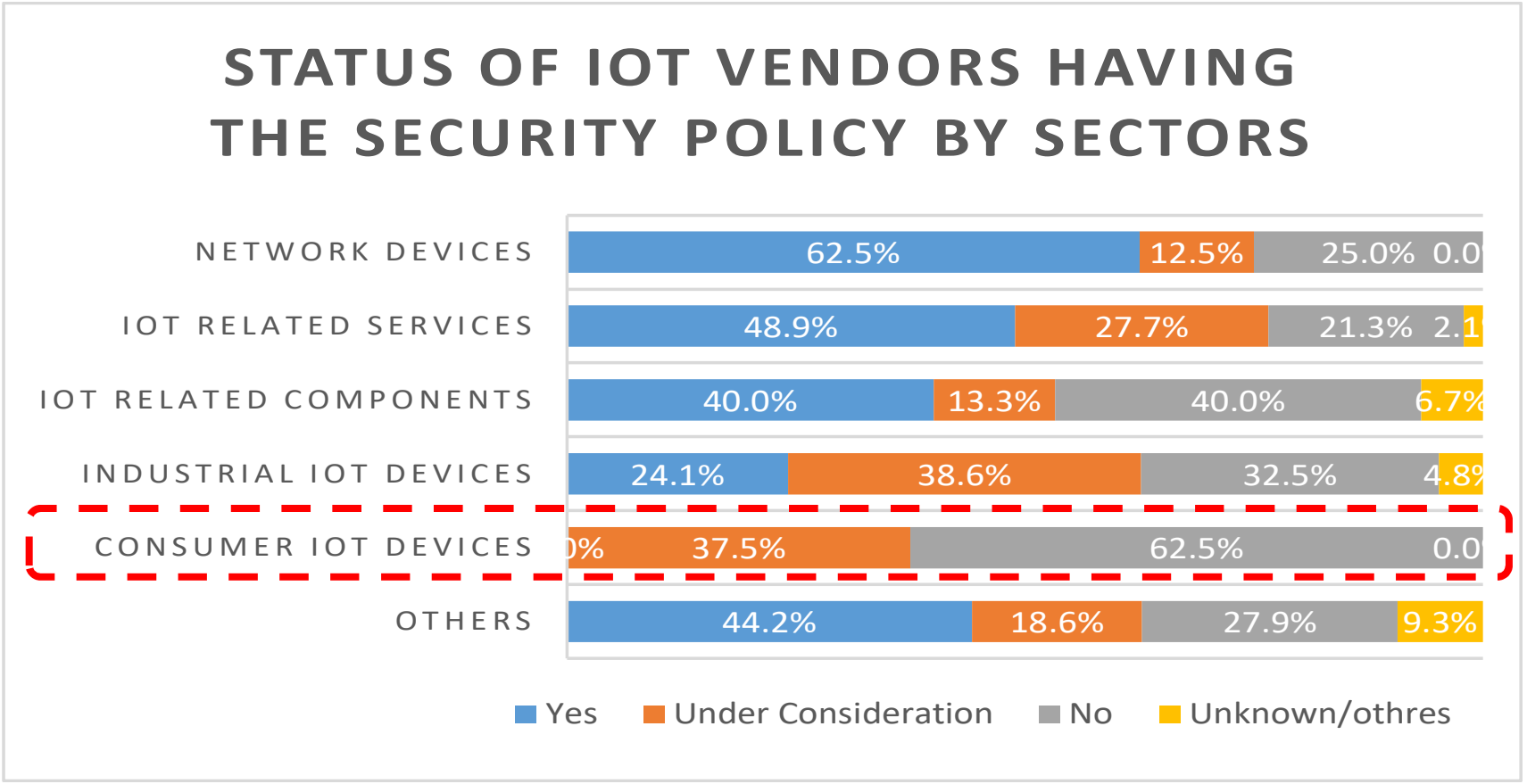
→ **製品の品質問題・セキュリティ問題とは認識しなかった**

ベンダのセキュリティ意識

INSTITUTE of INFORMATION SECURITY

セキュリティポリシーをもつコンシューマIoTベンダ＝0%

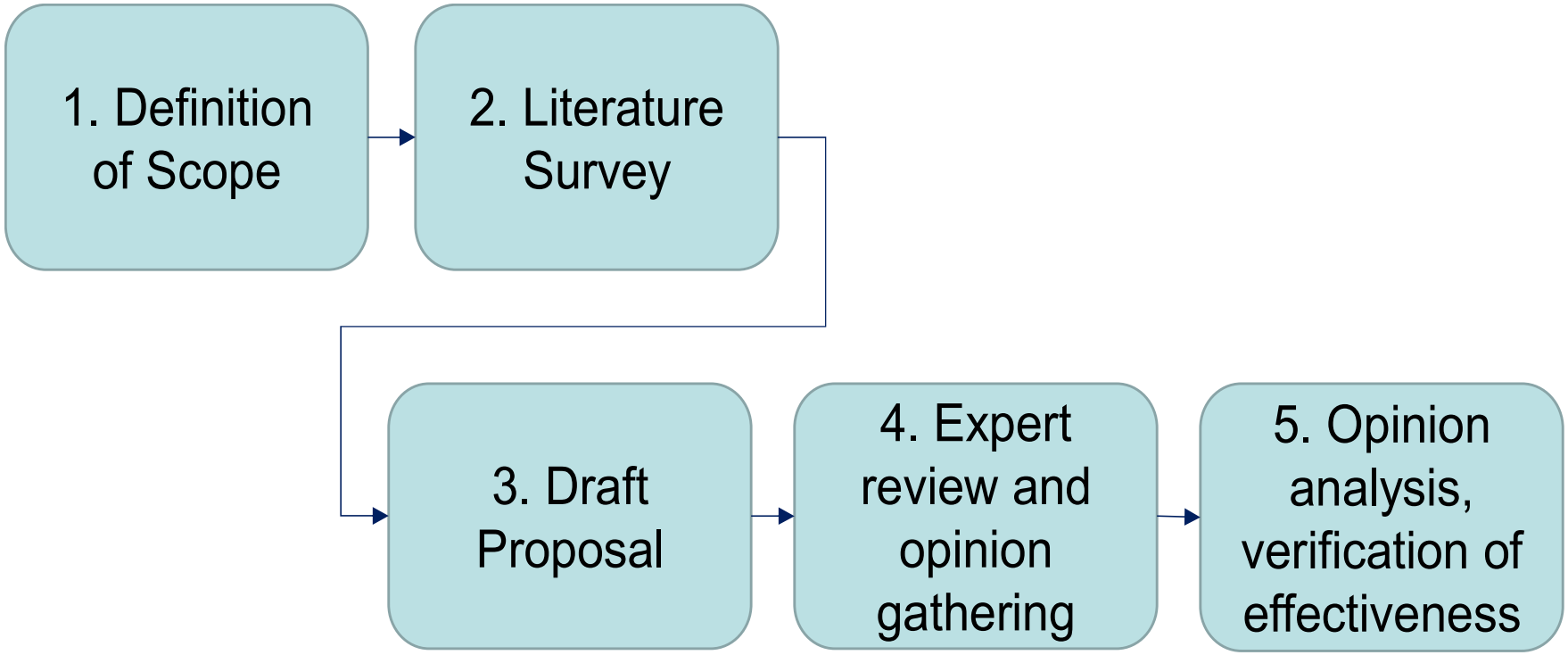
（IPA調査(2018)[48]）



IoT機器セキュリティ品質メトリクス項目出し

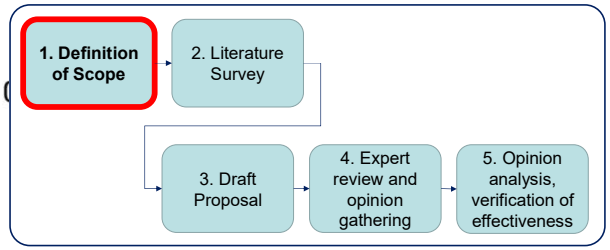
3. 本研究の調査手法

調査は，ENISA[30]でも採用されている手法で行った.



各調査ステップと調査結果について後述する.

ステップ１：スコープの定義

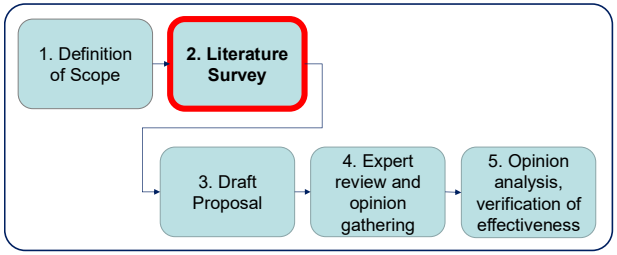


スコープ：IoT機器とそれを開発するIoTベンダ

✍ 以下の理由による.

1. IoT機器への攻撃が急増
2. IoT機器はセキュリティに不慣れなIoTベンダが開発
3. IoT機器は物理空間とサイバー空間をつなぎ、サイバー空間の異常状態を物理空間にいるユーザに影響を及ぼすポジションにある
4. IoTベンダは，製品によるセキュリティリスクを意識せずにIoT機器を開発

ステップ２：文献調査



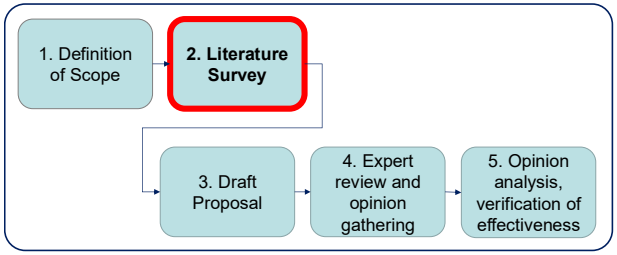
IoT機器のセキュリティ品質を評価するための項目を特定する.

調査対象：

1. ベンダのIoTセキュリティ意識の現状
2. IoTに関する注目すべきセキュリティインシデント
3. 製品の品質管理
4. 製品に関する製造物責任
5. ソフトウェアの品質メトリクス
6. セキュリティ評価方法
7. IoTセキュリティガイドライン

雪だるま式に調査を進めるシステマティック文献調査[44]を実施.

ステップ２：文献調査　サマリ



結果１：IoT機器のセキュリティ品質メトリクスを定義する研究や文献を見つけることはできなかった。

結果２：ソフトウェア品質の国際標準では「セキュリティ」が品質カテゴリとして定義されている。セキュリティを品質として扱う合理性はある。

結果３：品質は、「製品品質」と「プロセス品質」で確保される。
そのため品質メトリクスは、その両面から評価する構造が必要。

結果４：品質をどう測り，どう示すか，は一概には決められず、時代と共に変化することが明らかになった。

結果５：IoTのセキュリティガイドラインでは，当初はセキュリティ対策機能要件が多く示されたが、次第にセキュリティ設計プロセスや販売後のセキュリティ保守サービスの要件も追加されるようになった。

ステップ２：文献調査　サマリ

INSTITUTE of INFORMATION SECURITY

結果6： 既存の認証スキームは、第三者認証を要し、コストとスピード優先のコンシューマ向けIoT機器には不向き.
また、評価対象が、製品ライフサイクルの一部で、ライフサイクル全体をカバーしない。

4. 既存手法の課題：

- CC認証：
  - 製品のセキュリティ設計とその実装と評価の適切性を評価。
    ⇒**セキュリティ対策の強度、IoTベンダのプロセスや市場サポートは評価対象外**
  - IoT向けPPは存在するが、**TOEはセキュアエレメントに限定的。**
    ⇒**ID/PWD問題のような基礎的な観点が明文化されていない**
  - 認定された機関による**第三者認証が必須。しかも長期で高コスト**
    ⇒コンシューマIoT機器に不向き
- EDSA認証：
  - CC認証同様、**第三者認証、長期高コスト** ⇒ コンシューマIoT機器に不向き
  - 制御システムのエンドデバイスが対象。
    評価対象が、通信の堅牢性、設計成果物に限定的。
    ⇒**出荷後のサポートフェーズが対象外**
- 成熟度モデル：
  - システム運用者（利用者）視点の評価システム
    ⇒**IoT機器を提供するIoTベンダの視点に合わない**
    （利用者視点に立った脅威分析・リスク評価などの参考となる項目有り）

5. 提案手法の概要
IoT機器セキュリティ品質に関する項目出し
（ドラフト案と専門家意見収集・分析）

IoT機器セキュリティ品質評価項目出し

INSTITUTE of INFORMATION SECURITY

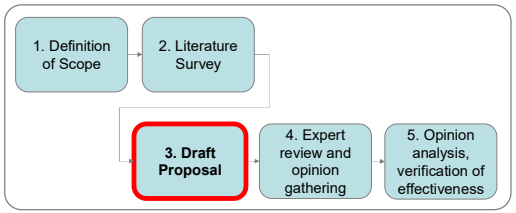
①IoT機器セキュリティ品質の定義
②IoT機器セキュリティ品質の要件
＋ガイドライン等の推奨事項

IoT機器セキュリティ
品質透明性モデル

IoT機器セキュリティ品質メトリクスの提案

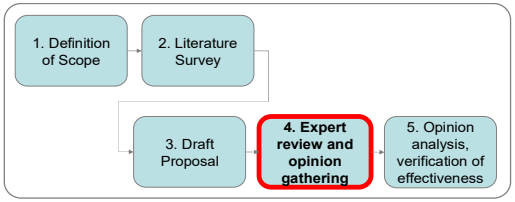
1. 候補項目出し（ドラフトメトリクス項目）

Step 3



2. セキュリティと品質の専門家レビュー・意見集約
3. ①定義、②要件、GQM手法を基にした
透明性モデルの各エリアのゴール設定、
専門家意見を反映した
サンプルQuestionとメトリクスの設定

Step 4



IoT機器セキュリティ品質の「サンプルメトリクス」の導出

IoT機器セキュリティ品質の定義と要件

INSTITUTE of INFORMATION SECURITY

①IoT機器のセキュリティ品質の定義：

⇒ 製品の**セキュリティ性能**と開発**プロセス品質**の組み合わせ

②定義したセキュリティ品質の要件

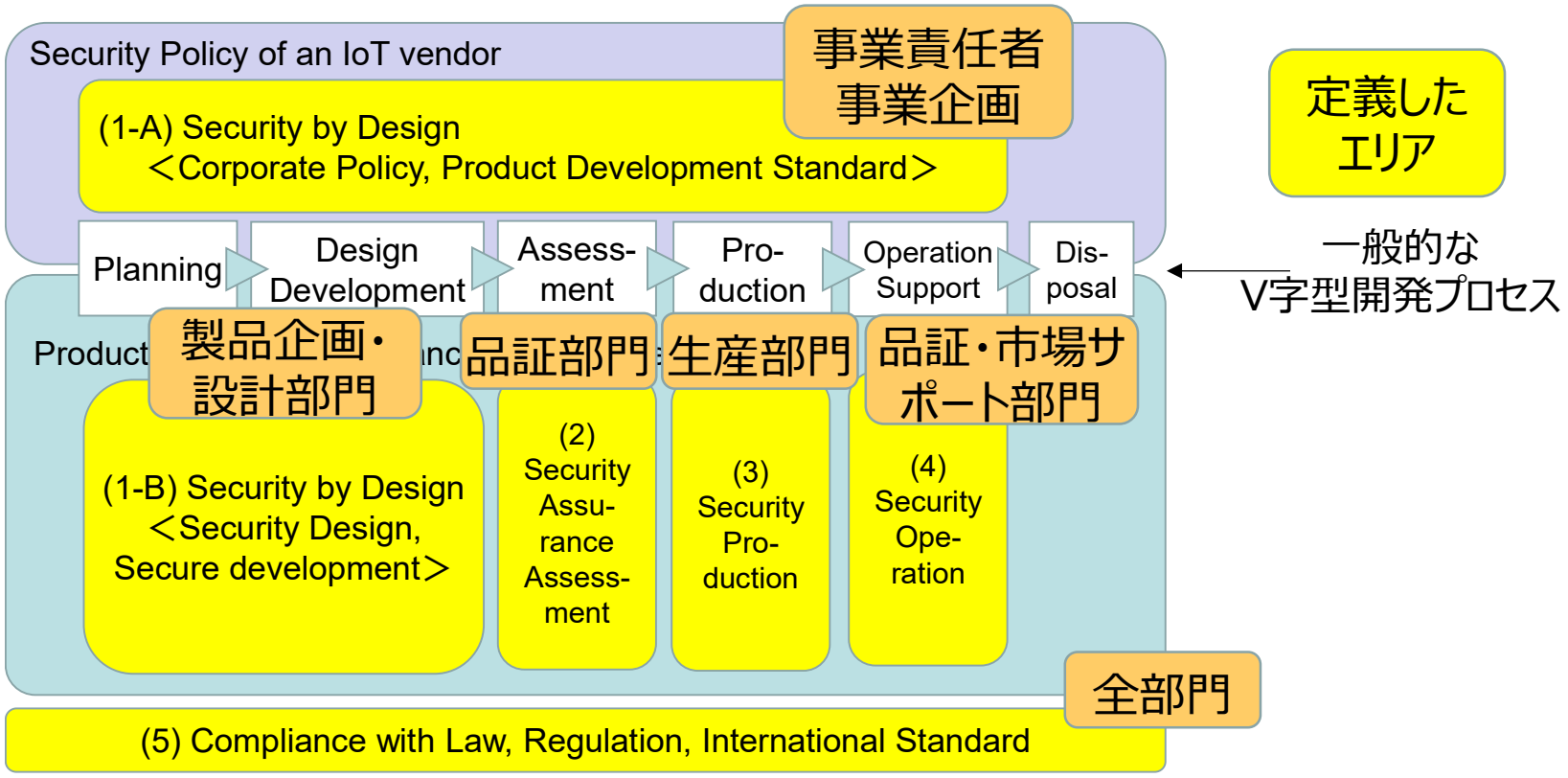
Requirements	Aspect
R1: 開発プロセスの透明性の確保	1: IoTベンダーのセキュリティポリシ
	2: セキュリティ開発**プロセス品質**
R2: セキュリティ能力の適切な表示	**製品**の**セキュリティ性能の品質**
R3: 市場のニーズや要求への対応	1: 法規制による要求事項の網羅
	2: 国際標準やガイドラインの勧告への追従
R4: セキュリティ保守プログラム (販売後)	セキュリティ監視、脆弱性情報の受信、アップデート提供など
R5: その他ユーザの信頼を得られること	–

IoT機器セキュリティ品質透明性モデル

INSTITUTE of INFORMATION SECURITY

V字型開発プロセスを基に，製品ライフサイクルを主体的担当部門が担うプロセスを「エリア」で分割したフレームワークを考案

目的：IoT機器のセキュリティ品質メトリクス項目を適切なエリアに割り当て，
担当部門が実施すべきことを明確化する．



IoT機器セキュリティ品質透明性モデル

IoT機器セキュリティ品質透明性モデル

製品**品質の信頼を得る**ために、製品を**提供する過程の透明性が重要**となる。

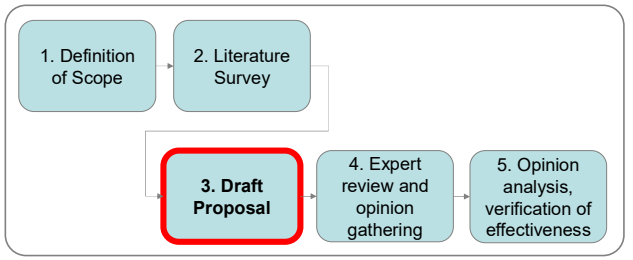
多くの組織が品質の信頼性のために透明性を強調。例：総務省統計局、JQA (認証機関)
セキュリティ分野でも同様。例：Microsoft、Kaspersky

IoTベンダ（電子機器ベンダ）は、**一定の品質で製品を提供するために**、
製品ライフサイクル全体の**プロセスを定義し、繰り返し実行**する。

IoTベンダの中で、**各プロセスの主体的な担当部門は変化**する。

- 製品企画・機能要件定義＝製品企画部門
- 設計・開発＝設計部門、
- 評価検証＝品質保証部門
- 量産＝製造部門
- 出荷後＝品証・市場サポート部門

IoT機器セキュリティ品質メトリクスの提案（Step 3）



1．ドラフト項目の作成：

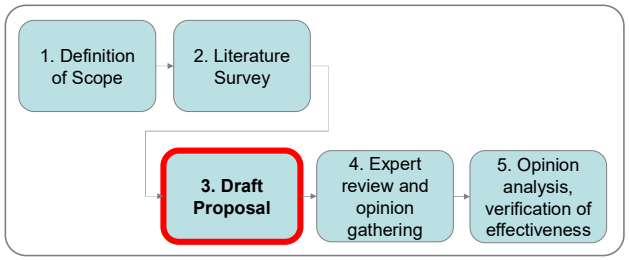
- セキュリティガイドライン等が掲げるプラクティスを共通項で集約（Appendix 1）

ガイドライン文献

メトリクスのドラフト項目

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
		NIST Cybersecurity FW v1.1	NIST SP800-64 v2 Sec Consideration in System DLS	NIST SP800-183 Network of Things	NIST SP800-193 Platform Firmware Resiliency Guidelines	NIST Cybersecurity White paper IoT Trust Concern	NIST SP800-160 System Security Engineering	Online Trust Alliance IoT Security & Privacy Trust Framework v2.5	US DoHS Strategic Priciples for Securing IoT	FTC Internet of Things Privacy & Security in a Connected World	FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	FDA Postmarket Management of Cybersecurity in Medical Devices	IETF Best Current Practices for Securing IoT devices	IIC IoT Security FW	IIC IoT Security Maturity Model	BSIMM/Synopsys	vBSIMM/Synopsys	UL2900-1 (ANSI compliant)	Security Engineering/Ross J. Anderson	HP 9 ways to improve IoT device security	ISACA INTERNET OF THINGS: RISK AND VALUE CONSIDERATIONS	BITAG IoT Security and Privacy Recommendations	CSA Future-proofing the Connected World 13 steps to develop secure IoT	OWASP IoT Security Guidance - Manufacturer	GSMA IoT Security Guidelines for Endpoint Ecosystem	UK Code of Practices for consumer IoT Security	ETSI EN303 645 Cybersecurity for Consumer IoT	ENISA Baseline Security Recommendations for IoT	NISC General Framework for Secure IoT Systems	IoT Acceleration Consortium IoT Security Guidelines v1.0	IPA Guide for Safe and Secure IoT Devices and Development (High Reliability)	IPA Guide to Ensuring the Quality of IoT Devices and Systems	CCDS Certification Program General Requirements 2021	ISO/IEC/IEEE 15288 Systems and software engineering - System life cycle processes	ISO 21827 System Security Engineering - Capability Maturity Model	IEC62443 ISASecure EDSA Certification	ITU-T Y.4806 : Security capabilities supporting safety of the Internet of things	oneM2M TR-0008 -v2.0 Security
		15	14	1	2	8	7	12	12	5	5	7	10	8	26	14	10	11	7	10	5	16	15	10	9	6	6	12	9	14	11	14	5	13	6	7	2	6
Product Security Policy (Documentation)	7														1	1				1								1	1	1								
Product Security Development Process Standard (Doc)	12		1					1							1	1		1		1	1		1					1				1	1	1			
IThreat analysis result	23	1	1				1	1		1	1		1	1	1	1		1	1		1		1		1			1	1	1		1	1	1	1			1
IRisk Assessment result	24	1	1				1	1		1	1		1	1	1	1		1	1		1		1		1			1	1	1		1		1	1	1		1
ICorresponding threat selection/countermeasure design	11		1				1				1					1		1					1						1		1		1	1		1	
Result of the evaluation of the effectiveness of countermeasures Implemented	2						1				1																										
Workaround/warning for the threats accepted in the user manuals?	2								1		1																										
Handling the personal data (vital data, action data, etc.)	11							1		1					1					1		1	1	1		1	1	1									1
Secure-coding Rule(s) to apply	1																																				1
IOS (including library, driver)	6	1				1			1						1	1	1																				
IOSS (open source software) utilized	6	1				1			1						1	1	1																				
IProcured 3rd-party components	6	1				1			1						1	1	1																				
In-house coding component	4								1						1	1	1																				
ISecure coding rule conformance test	3															1	1						1														
IStatic analysis	12		1				1					1	1		1		1	1					1							1		1		1				1
IUnnecessary port scan	14		1				1					1	1		1	1	1	1				1	1	1						1		1		1				
IKnown vulnerability check , penetration testing	13		1				1		1				1		1	1	1					1	1	1						1		1		1				
IFuzzing (zero day) evaluation	12		1						1				1		1	1	1	1	1			1	1							1		1		1				
Applying Security patches to OS/OSS	8		1						1									1				1	1							1		1			1			
IEvaluation of acceptance for procured 3rd-party components	6								1							1	1					1	1		1													
Check cloud service level (SLA evaluation)	1																							1														
nProduct Security Incident Response system (PSIRT)	15	1	1						1			1		1	1					1		1		1					1	1	1		1	1	1			
IIncident response process (documentation)	14	1	1					1				1	1	1	1					1		1							1	1	1	1			1			
IVulnerability reporting contact	9	1						1				1		1	1							1							1	1		1	1					
IVulnerability disclosure	13	1						1				1	1		1					1		1				1	1		1	1	1	1						
Information control, personal information protection law compliance, system to comply with GDPR regulations	6							1		1					1							1	1	1														
IUpdate (repair) function	17	1			1	1			1			1	1		1						1	1		1		1	1	1	1		1		1	1				
IConfiguration scanning function (for automatic update)	3	1													1																1							
IEncryption function	19	1				1		1	1				1	1	1			1		1	1	1		1	1	1	1	1		1	1					1		
ILog recording function	20	1		1		1		1					1	1	1			1	1	1		1	1	1	1	1	1	1			1					1		1
IMalfunction detection	7				1															1			1	1	1			1			1							
IDegenerating function to terminate connectivity because of security maintenance	1																														1							
Easy deleting function of user setting data	7		1					1																		1	1				1		1	1				
Monitoring the corresponding cloud service level	7							1						1					1									1		1	1	1						
nManagement of Customer Information in the services	2																					1										1							
nIn-house manufacturing management, line-workers, parts and materials control	0																																					
nODM (manufacturing consignment), line audit	6	1													1							1			1			1						1				
Production with all genuin parts?	6	1													1							1			1			1						1				
nLaws and regulations complied	4									1					1				1						1													
International standard complied	5		1			1									1				1																1			
nSecurity Certification granted	5		1			1												1		1															1			
nSecurity maintenance period, guaranteed range of SLA(disclair	2																					1									1							

IoT機器セキュリティ品質メトリクスの提案（Step 3）



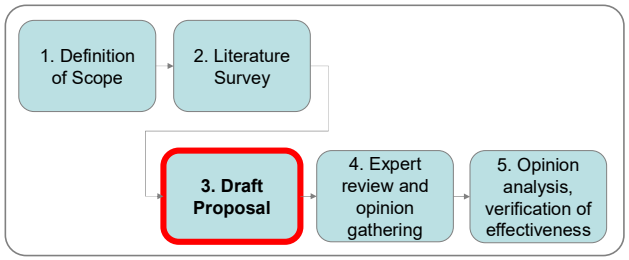
- IoT機器の**セキュリティ性能**とIoTベンダの**プロセス**に関わる項目で文献に多く取り上げられている項目を中心に選定
- 透明性モデルの各エリアに割り当て⇒ドラフト項目

特に顕著な項目：

- Threat Analysis and Risk Assessments (37文献中22が挙げた項目)

1) Security by Design			Metrics	supplementary information if exits
a		Product Security Policy (documented)	○＝Exist, ×＝No	
b		Product Security Development Process (documented)	○＝Exist, ×＝No	
	b-1	**Threat Analysis (results)**	**○＝Exist, ×＝No**	
	b-2	**Risk Assessment (results)**	**○＝Exist, ×＝No**	
	b-3	Selection of threats and design of countermeasures	○＝Exist, ×＝No	
	b-4	Results of evaluation of effectiveness of countermeasure implemented	○＝Exist, ×＝No	
c		Counter measured Threat List	○＝Exist, ×＝No	
	c-1	Accepted threats	○＝Exist, ×＝No	
	c-2	Security operation handling manual/warning	○＝Exist, ×＝No	
		:		:
		:		:

IoT機器セキュリティ品質メトリクスの提案（Step 3）



１．ドラフト項目の作成

その他、多く挙げられた項目：

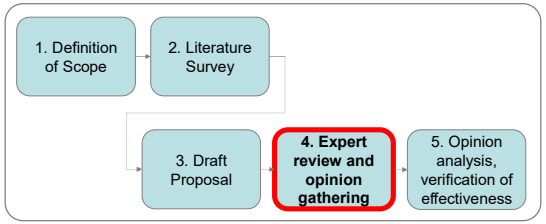
- 個人情報取り扱い・管理体制　⇒エリア1-A ポリシー、エリア4 オペレーション
- リスク緩和策・セキュリティ対策機能　⇒エリア1-B セキュリティ設計
  （アップデート、暗号化、アクセス認証）
- SAST/DAST/パッチ適用　⇒ エリア2 評価・検証
- PSIRT/脆弱性情報受付体制　⇒ エリア4 オペレーション

多くはなかったが重要と思われる項目：

- セキュリティポリシー　⇒エリア1-A ポリシー
- 受容したリスクリスト　⇒ エリア1-B セキュリティ設計
- SBOM/外注コンポーネントの特定　⇒ エリア1-B セキュリティ開発
- セキュリティ保守期間の明確化　⇒ エリア4 オペレーション
- 法規制対応　⇒ エリア5 法規制・国際標準

IoT機器セキュリティ品質メトリクスの提案（Step 4）

INSTITUTE of



２．セキュリティと品質の専門家によるドラフト項目のレビューと意見分析：

結論：プロセス品質と製品品質の両面で品質メトリクスの配置は適切と評価された。

- セキュリティの専門家は、気になる点を細かくチェックしたがる傾向が強く、
- 品質の専門家は、顧客の要望や知りたがると考える形でチェックする傾向が強かった

IoT機器セキュリティ品質メトリクスの提案（Step 4）

INSTITUTE of INFORMATION SECURITY

☞ 透明性を高めることへの懸念について：

品質専門家より：

機密扱いの製品情報であっても、顧客から製品の対策レベルが漏洩する可能性があるため、開示すべき項目の選定は慎重になる必要性あり

⇒ 開示する・しないによらず、問題が発生した場合にユーザへの説明責任を果たせる証跡を残しておくことが重要。
だれに何を開示するか、情報の表現方法は別議論である

IoT機器セキュリティ品質メトリクスの提案（Step 4）

３．メトリクス項目の目的と意義（意味付け）

GQM手法の活用

品質分野で一般的に浸透する品質の評価項目の設定方法

- 何を達成する必要があるか（Goal＝品質目標）、
- そのために何を評価するか（Question）
- その評価方法として何を使うか（Metric）

⇒単なるチェックリストとしない**評価項目の目的と意味付けをする手法**

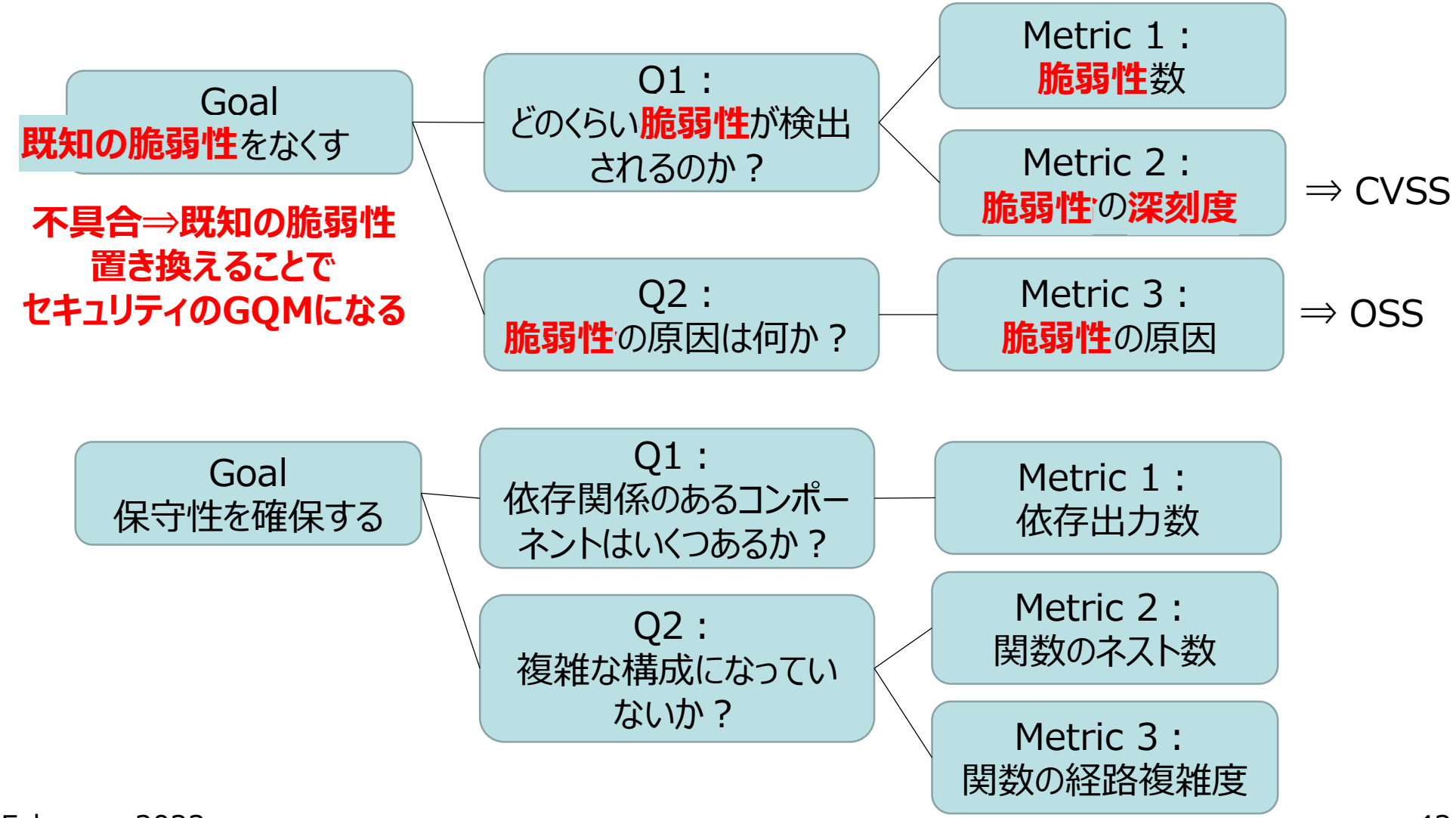
GQM手法のメリット：

- **品質業界に浸透している手法のため、品質部門への理解が得られやすい**
- 何のためのメトリクスか、評価の意図・理由を明確にできる
- 品質目標を明確にすることで、関係者が同じ目標に向かうことができる
- 品質メトリクスにより評価のムラや見落としを減らせる

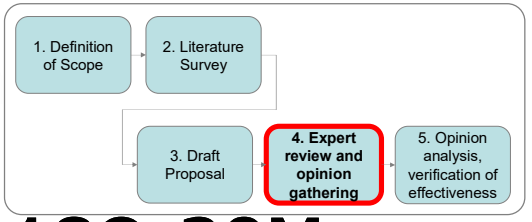
IoT機器セキュリティ品質メトリクスの提案（Step 4）

INSTITUTE of INFORMATION SECURITY

ソフトウェア製品の一般的なGQM設定例：



IoT機器セキュリティ品質メトリクスの提案（Step 4）

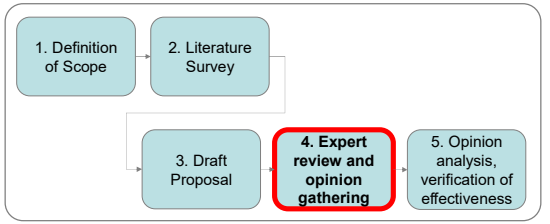


GQM設定：エリア１　1-A: 2G-2Q-2M, 1-B: 1G-18Q-20M

Area	Goals	主体部門	Questions（例）	Metrics（例）
1-A.	G1A-1: セキュアな製品の提供	事業責任者・企画	企業ポリシーはあるか？	ポリシーの有無
	G1A-2:製品ライフサイクルを通じた製品開発プロセスの設定	同上	セキュリティ開発プロセスはあるか？	プロセスの有無
1-B.	G1B:製品企画段階から、セキュリティに配慮した製品の開発	商品企画/設計部門	脅威分析・リスク評価は？	評価結果の有無
			セキュリティ対策機能は？	設計文書、対処／受容したリスクのリスト、保護すべき個人情報
			セキュアな開発手法は？	Coding Ruleの有無
			採用するソフトウェアコンポーネントは？	OS/OSS/外注開発ソフトの版,開発元の明確化
			セキュリティ保守に必要な機能は？	更新機能、認証機能、暗号化の有無
			廃棄時を考慮した機能は?	ユーザ個人情報の消去機能の有無

IoT機器セキュリティ品質メトリクスの提案（Step 4）

INSTITUTE of

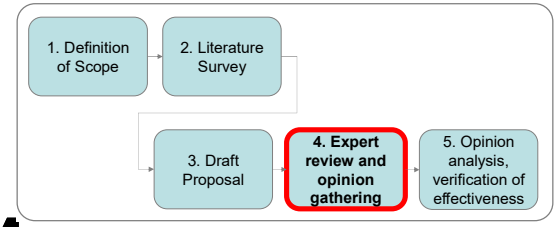


GQM設定：**エリア２ 主体：品証部門、1G-9Q-23M**

Area	Goals	Questions（例）	Metrics（例）
2.	G2:セキュアな製品の開発と確認	設計通りにセキュアな製品が開発されているか？	各種の評価結果(評価ツール名・版、評価日)の有無
		Secure Coding Rule、	Secure Coding Ruleの準拠評価
		既知脆弱性の確認は？	既知の脆弱性の静的解析評価
		採用したOS/OSSは最新か？	OS/OSSセキュリティパッチ適用状況確認
		ユーザに不要なI/Fは封鎖されているか？	JTAG/UART封鎖確認 不要サービス削除確認
		外注コンポーネントは安全か？	外注開発コンポーネントのセキュリティ評価結果
		連携先クラウドサービスのセキュリティサービスは確認したか？	連携先クラウドのセキュリティSLA確認、等

IoT機器セキュリティ品質メトリクスの提案（Step 4）

INSTITUTE of

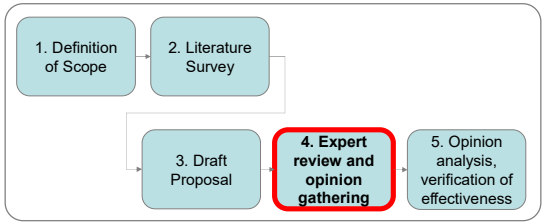


GQM設定：エリア３　主体：生産部門、2G-7Q-9M

Area	Goals	Questions（例）	Metrics（例）
3.	G3-1:セキュリティリスクを混入させない生産実施	セキュアな生産プロセスか？ 生産委託先ODMの生産プロセスは確認したか？ パーツの真贋は確認したか？ 固有PWD設定可能か？	従事者リスト、生産システムアクセス認証記録 生産国、プロセス監査記録の確認 パーツ生産元の純正証明の確認 機器固有PWD設定能力の確認
	G3-2:供給継続性の確保	生産システムにセキュリティ対策は施されているか？	生産システムのセキュリティ対策の有無 攻撃検知機能の有無 防御対策の有無 CSIRT体制の有無

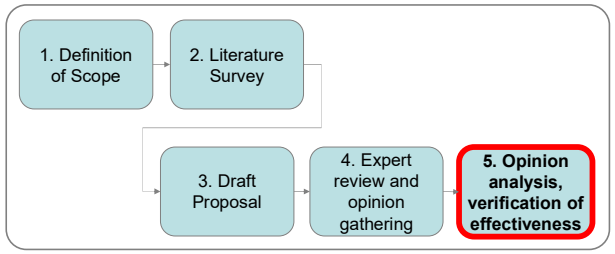
IoT機器セキュリティ品質メトリクスの提案（Step 4）

INSTITUTE of



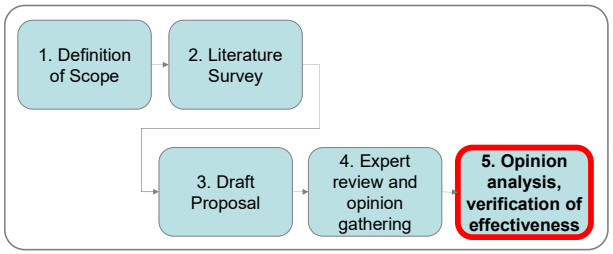
GQM設定：エリア４ 1G-8Q-9M、エリア５ 1G-4Q-4M

Area	Goals	主体部門	Questions（例）	Metrics（例）
4.	G4:製品にセキュリティリスクが顕在化した場合の迅速な対応	市場サポート部門	製品のインシデント対応体制はあるか？	監視体制(SOC)、PSIRT体制の有無
				インシデント対応プロセスの有無
				受付窓口情報の有無
			個人情報管理体制はあるか？	個人情報保護方針と管理体制の有無
			IoT機器の安定的運用の仕組みはあるか？	連携先のクラウド運用者の連絡先管理、クラウド運用状況の確認、顧客情報管理ルールの有無
5.	G5:仕向け地の法規制や国際標準に準拠した製品の提供	全部門	仕向け地の法規制・業界標準に準拠しているか？	遵法確認、国際標準・民間認証の適合証明の確認


1. Definition of Scope
2. Literature Survey
3. Draft Proposal
4. Expert review and opinion gathering
5. Opinion analysis, verification of effectiveness

6. 提案手法の効果検証

提案手法によるメトリクスの効果検証（Step 5）



手法の有効性を実際の製品開発を通じて検証することは困難なため、
考案した手法の有効性について、サンプルメトリクスを用いて
次の観点で検証した。

検証1：IoTベンダによる提案手法の導入の実現性

検証2：IoT関連の規制やガイドライン、認証制度などの要求事項の
特徴を把握するためのツールとしての有効性

検証3：市販IoT機器のセキュリティ品質評価の検証

結果：すべての検証で、サンプルメトリクスの有効性が確認できた。

提案手法の効果検証（Step 5）

INSTITUTE of INFORMATION SECURITY

検証1：IoTベンダによる提案手法の導入の実現性

目的：提案手法を、既存の製品開発プロセスに取り入れ可能かをヒアリング
対象：国際的に有名なブランドを持つ企業１社
　　IoTスタートアップ企業１社
検証基準：
　a) 既存の開発プロセスに矛盾する項目がないこと
　b) IoT機器に対する市場要求と矛盾する項目がないこと

評価結果 a)　両社とも既存プロセスに導入可能と判断
評価結果 b)　両社とも矛盾する項目はないと表明

結論：提案したメトリクスは、IoT機器ベンダの規模の大小にかかわらず、
実装可能であることが確認された。
※大企業では実際に導入を開始した。

提案手法の効果検証（Step 5）

INSTITUTE of INFORMATION SECURITY

検証2：IoT関連の規制やガイドライン、認証制度などの要求事項の特徴を把握するためのツールとしての有効性

対象：IoTセキュリティの**法規制**、**ガイドライン**、**認証制度**の要求事項

評価方法：

- エリアごとにメトリクス総数と要求事項数を比較する。
  その結果を棒グラフの形で示す。
- 要求事項数の大小で、各要求事項の求めるエリアの特徴を読み取る。

縦軸のパーセンテージは、エリアのサンプルメトリクス総数に対する各エリアにマッチする文献中の要件数との比率を表す。横軸はエリアとエリア内のメトリクス総数を示す。

提案手法の効果検証（Step 5）

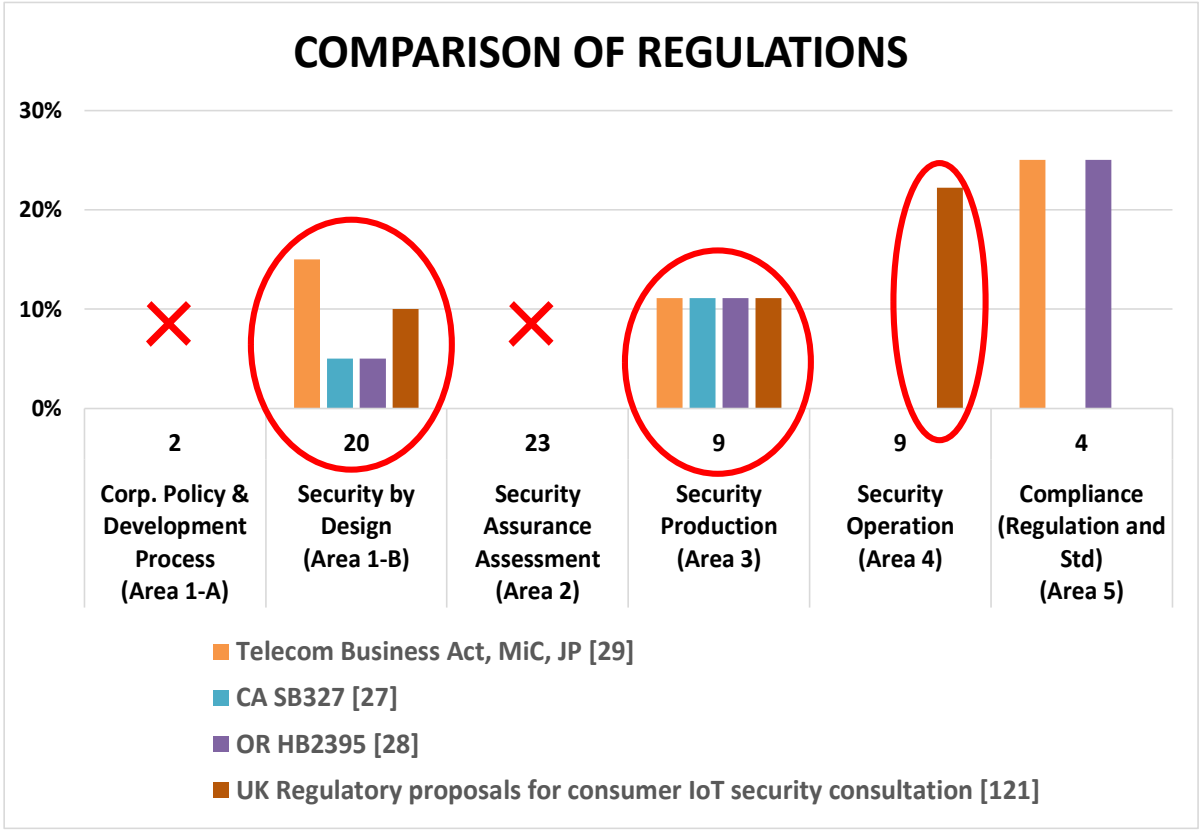
INSTITUTE of INFORMATION SECURITY

検証2：要求事項の特徴を把握するためのツールとしての有効性

評価１：4つの規制要件の検証

対象：カリフォルニア州法No.327、オレゴン州法2395、総務省の技術基準適合要件、
英国消費者IoTセキュリティ規制案

- IoTベンダの姿勢(1-A)や評価(2)は要求されていない。
- いずれもエリア1-Bと3 (機器固有ID/PWD設定) に着目している。
- 英国は製品販売後の運用体制を求めている。



提案手法の効果検証（Step 5）

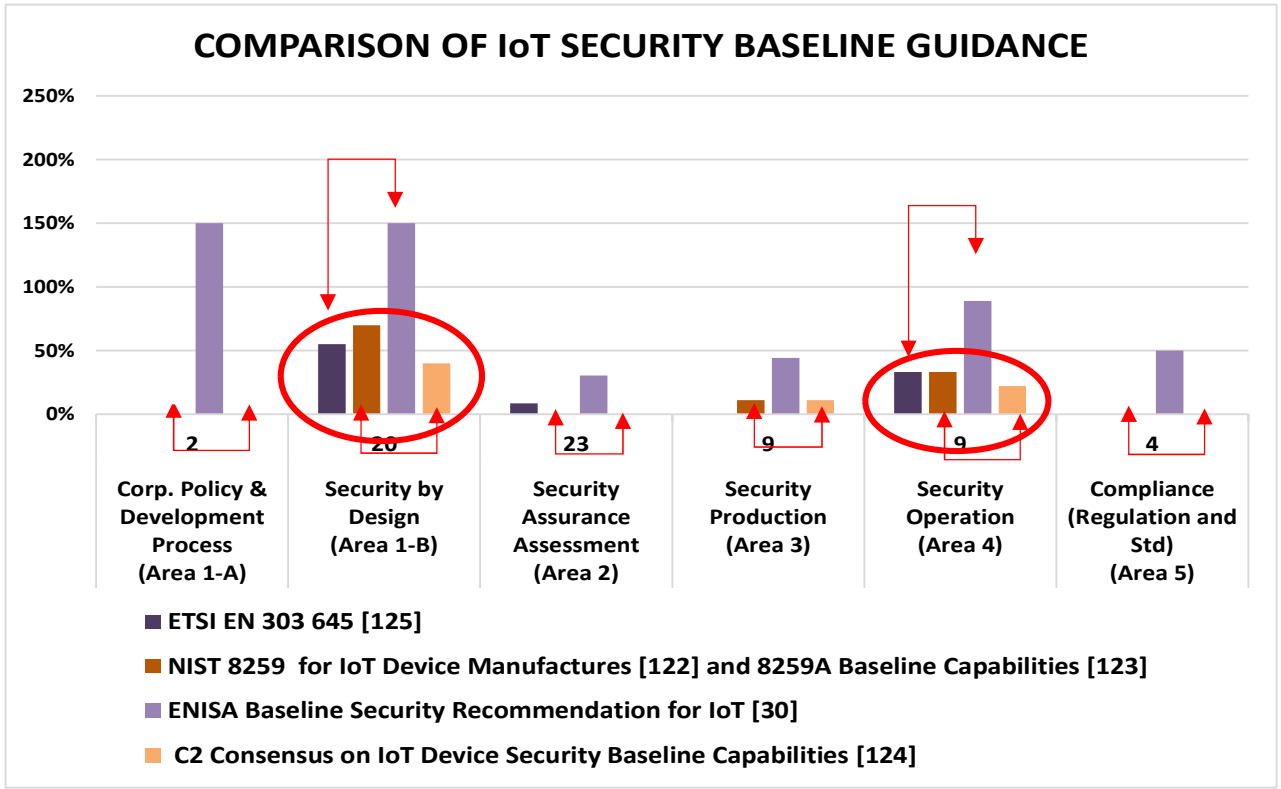
INSTITUTE of INFORMATION SECURITY

検証2：要求事項の特徴を把握するためのツールとしての有効性

評価2：各ベースライン要件の検証

対象：米国NISTIR 8259＆8259A、C2 Con-sensus on IoT Device Security Baseline Capabilities、ENISAベースライン、ETSI EN 303 645

- 米国の２つの要件分布は似ており、ベースライン要件に求める考え方が近いと言える。
- 欧州の２つは異なり、考え方の違いがわかる。
  ENISAは全領域、特にエリア1-Bで多くの要件がある。
  ETSIは米国と類似。



提案手法の効果検証（Step 5）

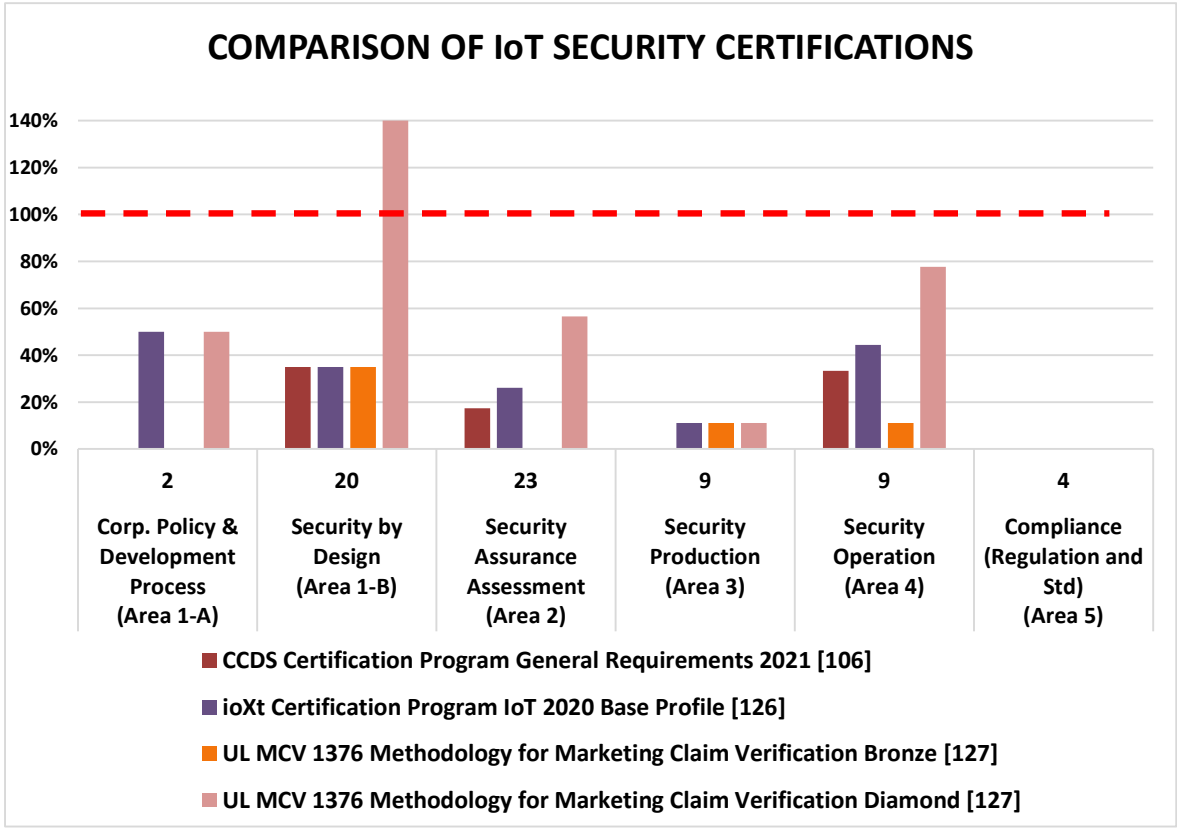
INSTITUTE of INFORMATION SECURITY

検証2：要求事項の特徴を把握するためのツールとしての有効性

評価３：民間のIoTセキュリティ認証プログラム要件の検証

対象：日本 CCDS、米国 ioXt アライアンス、
米国 UL IoT Security Rating の 2 グレード（Bronze と Diamond）

- UL Diamondの要求事項を除いて他のプログラムは同様の数の要求事項があり、これらはメトリクスでカバーされる（100%ライン以下）
- UL Diamondのセキュリティ機能要件はENISAベースライン要件と同レベルに厳しい(100%超え)ことが見て取れた。



提案手法の効果検証（Step 5）

INSTITUTE of INFORMATION SECURITY

検証2：要求事項の特徴を把握するためのツールとしての有効性

結果：提案メトリクスは、製品ライフサイクルの中で取り組みの過不足を把握するツールとして有効であることが確認された。

- メトリクスは各要件群の取組み比重を可視化でき、各エリアのセキュリティ対応工数の調整に役立つ
- 要求事項は製品ライフサイクルを通じて均等な配分ではないことがわかる。
- 法規制の要件はミニマム、
  ベースライン要件と認証要件は、ミニマム型と多くの対策を求める考え方に分かれた。

提案手法の効果検証（Step 5）

検証3：市販IoT機器のセキュリティ品質評価の検証

対象：ほぼ同じ製品機能仕様の市販ドライブレコーダー2機種
（製品A、製品B）どちらもODMベンダから提供される製品

2製品の類似点：

- オンラインや店頭で購入できるコンシューマー向け製品
- フルハイビジョン高画質録画
- GPSによる位置情報記録
- スマートフォンとのWi-Fi（ワイヤレス）接続
- 16GBのストレージ容量
- シガーソケットからの給電で簡単に設置
- 本体と機能連携するスマートフォン・PC用アプリケーション付属

2製品の相違点：

- 製品デザイン：形状、色
- 価格：**製品Aは**製品Bより**安い**

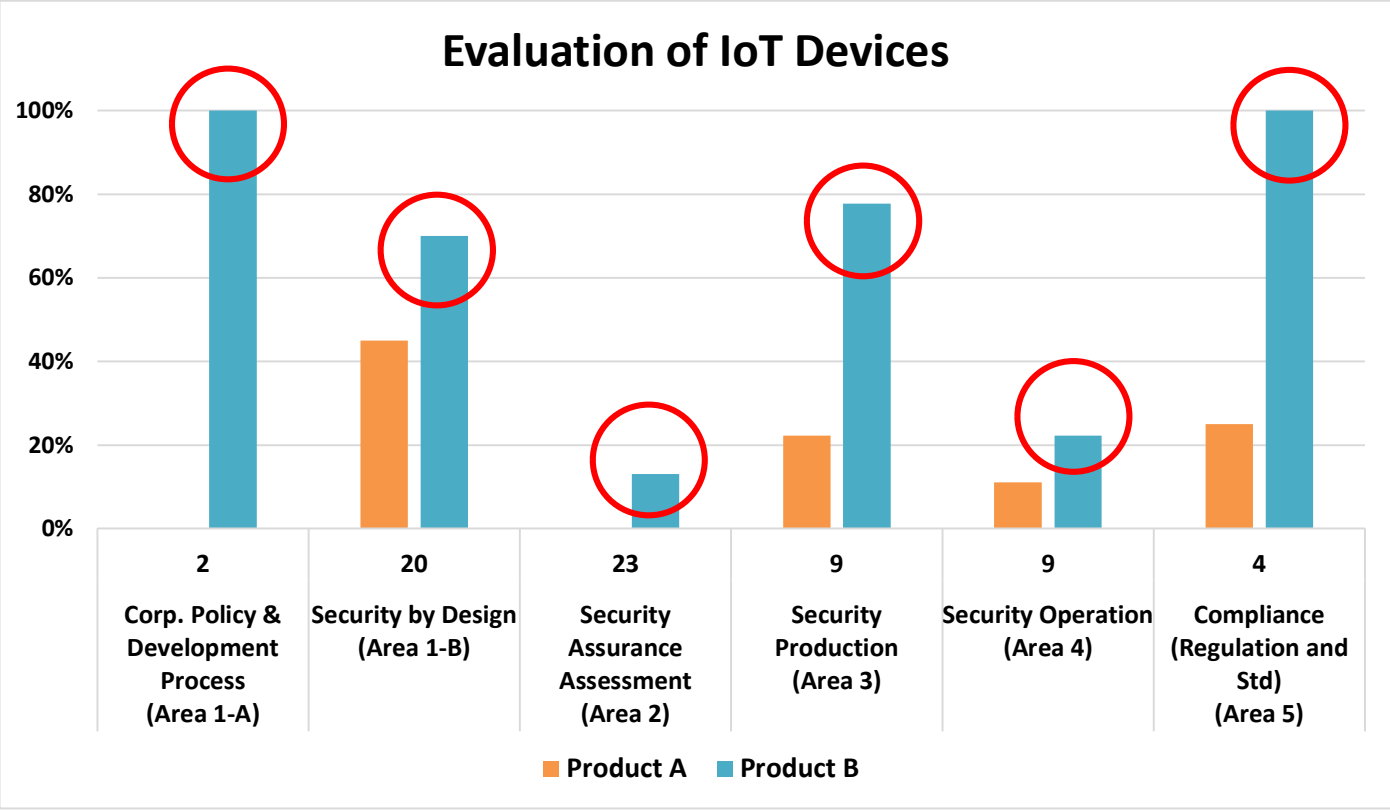
提案手法の効果検証（Step 5）

INSTITUTE of INFORMATION SECURITY

検証3：市販IoT機器のセキュリティ品質評価の検証

サンプルメトリクスに照らし、ODMに確認できた範囲で2製品のセキュリティ品質を評価・比較した。

結果：２つの製品のセキュリティ品質の違いを可視化できた。
製品Bは製品Aよりセキュリティ品質が高いと推察できる。



提案手法の効果検証（Step 5）

検証3：市販IoT機器のセキュリティ品質評価の検証

☞提案メトリクスにより、機能仕様が似ていても、カタログからは見えない製品のセキュリティ品質の違いを明らかにできた（＝透明性を上げられた）.
製品Bの価格が高い要因の１つにセキュリティ対応コストが考えられる。

現状、製品選定の際、ユーザには一般的に製品の機能仕様と価格しか判断材料がなく、セキュリティ品質を確認することは容易ではない.

⇒ 本手法は、IoTベンダにとって、セキュリティ品質をユーザに訴求するツールとして貢献する可能性を持つ。

7. 社会貢献の考察, 今後の課題, まとめ

社会貢献の考察

INSTITUTE of INFORMATION SECURITY

社会貢献のポイント：

- IoTベンダにおけるセキュリティ品質メトリクスの設定を推進.
- IoT機器のセキュリティ品質・セキュリティ対応能力の向上.
- 安全なIoT機器の普及とそれを求めるユーザの選択肢の拡大.

☞ IoTユーザにとって，IoT機器のセキュリティ品質を確認する方法となることが期待される.

☞ IoT機器のサプライチェーンの関係者間で、セキュリティ品質のメトリクス情報を共有し、IoT機器のセキュリティ品質の管理手段となることが期待される.

☞ 将来のIoTベンダ向けサイバー保険市場の創生に必要な評価材料の一つとして活用されることも期待できる.

今後の課題

主に２つの課題

1. メトリクスの分類
   - 今後、製品品質とプロセス品質の項目を一目で見分けられるメトリクスの表記方法を検討し、両面の網羅性を確認しやすくする.

2. 評価結果のカバレッジ状況の可視化方法
   - カバレージを可視化する方法として, レーダーチャートなど他の可視化方法を検討し、製品間の比較や改善状況を把握しやすくする.

さらに,

- IoT攻撃の進化や市場の要請の変化に対応できる様、GQMの見直し、および見直しサイクルの検討が必要.

まとめ

- IoT機器のセキュリティ対応を促進させるため、
  IoTベンダの品質管理プロセスの中でIoT機器のセキュリティ対応を進める方法「IoT機器のセキュリティ品質メトリクス設定手法」を提案した.
- この手法の特徴は、
  1. IoT機器の製品ライフサイクルにおいて、IoTベンダ内の品質管理の主担当部門明確にする「IoT機器セキュリティ品質透明性モデル」でメトリクスの配置をフレームワーク化
  2. ソフトウェア品質分野に浸透する品質メトリクス設定手法「GQM手法」にヒントを得たメトリクスを自己設定・調整できる方法
  3. IoT機器のセキュリティ能力だけでなく、IoTベンダの執るべきプロセスの両面をカバー
- ３つの検証方法により提案手法の有効性を確認

まとめ

IoT機器のセキュリティ品質評価手法(IoT-SQMM)が、IoTベンダにとって、セキュリティ的に安全で安心して使えるIoT機器の開発とサポートを、従来の品質管理の一環で組み込めるよう、その一助になれば幸いである。

8. 外部発表（本研究に関連するもの）

外部発表（1）

INSTITUTE of INFORMATION SECURITY

ジャーナル：

IoT (ISSN 2624-831X)
タイトル:IoT Security Quality Metrics Method and its Conformity with Emerging Guidelines
筆者： Kosuke Ito, Shuji Morisaki, Atsuhiro Goto
発行元：Multidisciplinary Digital Publishing Institute (MDPI AG)
発行日： 2021年12月15日刊行（Vol.2 No.4, pp761-785）
DOI: 10.3390/iot2040038（https://doi.org/10.3390/iot2040038）

主な内容：
・本論のコアアイデア全般
- 背景、本研究の必要性、サンプルメトリクスアイテム策定の概要
- メトリクスによるIoTセキュリティ法規要件、ベースライン要件、認証要件の特徴抽出検証
- メトリクスによる市販IoT機器のセキュリティ品質検証
- 本研究の貢献

外部発表（2）

INSTITUTE of INFORMATION SECURITY

国際学会（査読付き）

会議名： ISA Asia-Pacific Singapore 2019
主催者： The International Studies Association
開催日： 2019年7月4日～6日
タイトル: A Study Toward Quality Metrics for IoT Device Cybersecurity Capability
発表日： 2019年7月4日13:40～15:25 TC08: Cybersecurity

主な内容：
・以下の調査と研究結果を報告：
- IoT機器のセキュリティに関する課題の共有
（セキュリティ問題の露呈、セキュアなIoT機器を知る方法の欠如）
- IoTセキュリティに関するガイドラインなどの文献調査の結果
- 調査結果から導き出した、安全や環境とは異なる品質として、IoT機器のセキュリティ品質評価指標の案
（GQMによるメトリクスにする前の段階）

Thank You for Your Attention!