# 博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

| | | |
|---|---|---|
| **論文題目** | : | Proposals of the IoT Device Security Quality Metrics Method (IoT-SQMM) |
| **申請者** | : | 伊藤　公祐　Kosuke Ito |
| **審査委員会** | : | 主査　教授　後藤　厚宏 |
| | | 副査　教授　大久保 隆夫 |
| | | 副査　教授　藤本　正代 |
| | | 副査　教授　松井　俊浩 |

## Ⅰ. 論文内容の要旨

本論文は，IoT 機器のセキュリティ対策を促進させるため，機器ベンダには従来より品質管理の取組みが定着していることに着目し，IoT 機器の製品ライフサイクル全般にわたる品質管理の一環としてのセキュリティ品質を明らかにするメトリクスの設定方法を提案する.

具体的には，GQM（Goal/Question/Metric）手法にヒントを得て，IoT 機器の開発フェーズでのセキュリティ品質と，生産および保守フェーズの取組みにおけるセキュリティ品質を明らかにするメトリクスの設定方法（IoT-SQMM）を提案し，その適用性と効用を検証している．この手法により，ベンダは自社製品が既存のセキュリティベースラインや認証プログラムの要件に沿って開発されているかどうかを検証することができ，また，与えられたセキュリティ要件を満たすようにベンダが品質要件を調整することができる.

本論文は 9 つの章からなる.

第 1 章「Introduction」では，本研究の背景と対象とする IoT 機器の定義を示した上で，本研究のスコープを IoT 機器に置く理由を示している.

第 2 章「Necessity of this Study」では，これまで IoT ベンダが製品のセキュリティ能力を品質管理の一環として考慮していなかったこと，IoT ベンダにとって適切な IoT セキュリティ品質の一般的なメトリクスは存在しておらず，各ベンダが独自にセキュリティ品質のメトリクスを設定しなければならない状況であったこと，その独自のメトリクスは一貫性を欠き，対外的に正当化することは困難であったことが本研究の必要性としている.

本研究では，ENISA などが用いている５つのステップ（1. スコープの定義，2. 文献調査，3. メトリクスの下案の作成，4. 専門家によるレビューと意見収集，5. レビュー結果の分析と修正したメトリクスの効果測定）の調査手法を採用している.

第 3 章「Research on IoT Device Security Quality」では，上記の調査手法の 1. スコープの定義，2.

文献調査について述べている．文献調査では，雪だるま（Snowballing）式に調査を進めていくシステマティック文献調査方法で実施している．

第4章「Itemizing IoT Device Security Quality Metrics」では，文献調査の結果を総括し，GQM手法の考え方によるメトリクスの一次ドラフトを示している．製品ライフサイクルのすべてを網羅するようにメトリクスを設定するために， the Transparency Model of IoT Device Security Qualityというフレームワークを考案し，セキュリティと品質の両専門家グループのレビューによる修正を通して，IoT機器のセキュリティ品質メトリクスとしている．

第5章「Effectiveness of the Proposed Method (Step 5)」では，企業ヒヤリング2社，および既存の法規制・ガイドライン等との要件比較により本手法の有効性を評価している．

第6章「Evaluation of the IoT Devices with the Proposed Method」では，２つの実製品比較によって本手法の有効性評価をしている．

第7章「Considerations on Social Contributions」では，本研究の貢献を，セキュリティ専門的知識がなくてもセキュリティの取組みを開始できる品質メトリクスの設定方法の提示により，多くのIoTベンダによるセキュアなIoT機器の開発と普及につながることとしている．また，本研究の社会的波及効果として，セキュアな製品を望むユーザに選択肢を与えることに加え， IoT機器ベンダとユーザの間における，IoT機器のセキュリティ品質に関するコミュニケーションツールとしても貢献するとしている．

最後に第8章「Future Direction」では将来課題を示し，第9章「Conclusion」では，セキュアなIoTの普及への貢献について結論つけている．

## Ⅱ. 論文審査結果の要旨

本論文は，IoT機器を製造するIoTベンダーの環境に適したセキュリティ品質評価手法を提案するものである．IoTベンダーでの品質管理に着目し，IoT機器の開発・生産・出荷後の保守フェーズにわたるライフサイクル全体の品質管理にセキュリティ品質のメトリクスを設定し，その適用性や効用を検証できることを示すものであり，これらの研究成果による情報学への貢献は大変大きく，本論文は，博士（情報学）の論文として合格と認められる．

## Ⅲ. 審査経過

本審査委員会は,2022年1月14日に論文内容とこれに関連する事項について口述試問を行い,その後,2022年2月 5 日にこれに関連する事項の最終試験審査を行った．審査に当たっては，博士学位のディプロマ・ポリシーに基づいて総合的に評価し，申請者が学位取得にふさわしい知見を持つものと判断した．