

# 卒論チェックシート

学籍番号 8535009K 氏名 内山田 隆太

## 目的

卒論本文に関して、以下の項目 1) ～ 5) に関する記述が必要です。5 項目についての記述も卒論評価の 1 部とします。この卒論チェックシートを完成させ、卒論提出前に記入漏れがないことを確認してください。なお、このシートは卒論審査資料の一つとなります。卒論と同様にしっかり完成させ、卒論と一緒に主査と副査へ提出してください。

## 提出方法

1. チェック項目について明確・簡潔に回答を記入する。また、対応記述を含む本文のページ番号を明記する（例：3 ページ, 3,5,7 ページ, 3-10 ページなど）。全ての項目について回答し、卒論チェックシートを完成させる。
2. 完成した卒論チェックシートを、卒論を収めたファイルの最後尾に綴じる。
3. 主査（1 名）と副査（2 名）に卒論と卒論チェックシートを綴じたファイルを提出する（従って、卒論とともに卒論チェックシートも 3 部用意する、卒論チェックシートの記述内容は 3 部とも同一で良い）。

### 1) 研究の目的・目標を明確に設定できる。（卒論評価項目 1）

**【チェック項目】** 研究目的・目標を説明してください。

本研究は、処理能力の低い IoT 機器間の相互認証機能およびデータ通信を暗号化する機能を有するセキュアな組込みシステムを、組込みシステム開発手法に従ってチームで開発することを目的とする。

組込みシステムの認証と暗号通信を実現するために、軽量な SAS-L2 認証方式と、その認証方式に基づいた暗号化方式を IoT 機器に実装することを目標とする。

本文におけるページ番号： 1,2 ページ

### 2) 人類や社会に望まれ、貢献する研究目標を立てられる。（卒論評価項目 2）

**【チェック項目】** 論文に示された研究目標が、情報工学を応用し人類・社会に貢献するものであることを説明してください。（社会との関わりなど）

私たちの身の回りには様々な IoT 機器があり、IoT 機器のセキュリティ機能が求められている。しかしながら、IoT 機器にはコスト要因で処理能力の低い機器が多数存在する。本研究のシステムを開発することで、処理能力の低い IoT 機器に対して、認証機能およびデータの暗号化機能を実装し、セキュリティ機能を搭載することができる。

本文におけるページ番号： 1,2 ページ

3) 研究の目的・目標を実現するための具体的研究方法を示し、実行できる。(卒論評価項目 3)

**[チェック項目]** 論文に示された研究方法の具体性や、研究目的・研究目標の達成を目指すためにどのような意味がありそのような研究方法を採用したのか説明してください。

本研究では、始めに、チームでシステムの要件定義、UML を使用した基本設計を行った。次に、エッジ側とサーバ側の実装をチーム内で分担し、それぞれ UML を使用した詳細設計を行い、SAS-L2 認証機能およびデータの暗号化通信機能を実装した。実装の際、エッジデバイスには Arudino、サーバには RASPBERRY PI を利用し、それぞれのデバイスをモニターに接続して処理の流れを表示している。最後に、テストを行い、実装したシステムに対する評価を行った。

このような研究方法を採用することで、処理能力の低い IoT 機器に正確に認証機能およびデータの暗号化機能が搭載できているか評価することができる。また、組込みシステム開発手法に従って、チームでシステムを開発することができる。

本文におけるページ番号： 17-50 ページ

4) 研究の内容が、情報工学技術の発展や応用に貢献するものである。(卒論評価項目 4)

**[チェック項目]** 論文で示された研究内容が、情報工学技術の発達や応用に貢献するものであることを説明してください。(研究内容の新規性など)

本研究では、SAS-L2 認証および SAS-L2 認証メカニズムに基づいたデータ通信の暗号化機能を有したシステムを開発し、処理能力の低い IoT 機器に本システムを実装した。本研究は、処理能力の低い IoT 機器にセキュリティ機能の強化に貢献していると考ええる。

本文におけるページ番号： 17-28 ページ

5) 卒業論文、卒業論文発表において、卒業研究の目的・目標、研究方法、研究成果が論理的に述べられる。(卒論評価項目 6)

**[チェック項目]** 論文で示された研究成果について説明してください。

SAS-L2 認証処理およびデータ通信の暗号化処理を正常に行っていることを確認することができた。また、仕様設計、基本設計、詳細設計で定めた機能を実装できていることが確認できた。このことから、システム開発手法に従って、チームで SAS を用いたセキュアな IoT システムを開発することができたといえる。

本文におけるページ番号： 44-50 ページ

**[チェック項目]** 卒業研究の目的・目標、研究方法、研究成果がどのような章立てで述べられているか説明してください。

第 1 章では、研究背景、研究の目的・目標を述べる。第 2 章では、本研究に用いたアルゴリズムや用語の説明を述べる。第 3 章では、SAS-L2 認証メカニズムに基づいたデータ通信の暗号化について述べる。第 4 章では、本システムの仕様設計および基本

設計を述べる。第 5 章では、本システムのサーバの詳細設計および実装方法について述べる。第 6 章では、開発したシステムの実装結果および評価を述べる。第 7 章では、本研究に対しての考察を述べる。第 8 章では、あとがきを述べる。

以上