卒論チェックシート

学籍番号　　8535002B　　氏名　　浅野美咲

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．

本研究では，処理能力の低いセンシングデバイスで構成される IoT システムにおいて，エッジデバイスとエッジサーバー間の安全なデータ通信を行うセキュアな組込みシステムを開発することを目的とする．具体的には，高知工学科大学の清水明宏教授が処理能力の低い装置へのセキュリティ機能実装のために開発したワンタイムパスワード認証方式 SAS-L2 を IoT センシングデバイスに実装することで,デバイス間の相互認証およびセンシングデータの暗号化通信を実現する.

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）

近年では,IoT が普及し様々なものがインターネットに繋がっていることから,IoT におけるセキュリティ対策が求められている.そのセキュリティ対策の一つとして,認証・暗号化通信が挙げられる.対象となる IoT 機器の処理性能は様々であり,処理性能の低いセンシングデバイスの場合,従来の暗号化アルゴリズムを導入することが困難である.

本研究で,処理性能の低いセンシングデバイスに SAS-L2 認証を実装し,認証と暗号化通

信を実現することで,認証・暗号化通信による,センシングデバイスのセキュリティ強化につながる.

本文におけるページ番号：　1-2 ページ

（裏にもあります）

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.

SAS-L2 を実装し認証・暗号化通信を実現するために,エッジデバイスとしてセンサを接続した Arduino 用いて IoT システムを構築した.また,システムの開発では UML を使用して設計をすることで,エッジデバイスとサーバーのそれぞれの機能や,認証・暗号化通信の流れを可視化し,チーム内での分担やシステムの評価を行った.

本文におけるページ番号：　18-32 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）

処理負荷が大きいことから従来の暗号化方式の実装が困難である処理性能の低いセンシングデバイスに対して,軽量な認証方式である SAS-L2 を実装しサーバーとの相互認証と暗号化通信を実現することに新規性がある.本システムの開発により,処理性能の低いセンシングデバイスに対して,認証・暗号化通信によるセキュリティの強化に貢献できる.

本文におけるページ番号：　1 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 認証方式をセンシングデバイスに実装し,サーバーとの認証・暗号化通信を行うことができ,センシングデバイスで取得したセンシングデータをサーバーが受信し正常にデータベースへ保存できた.

本文におけるページ番号：　33-48 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.

1 章では,卒業研究の背景・目的・目標を示し,2 章では,本研究で必要な用語について説明する.そして 3 章では SAS-L2 認証方式について説明する.4 章では SAS-L2 を用いたデータ通信の暗号化方法について説明する.5 章では SAS-L2 を用いたセキュアな組込

みシステムの仕様について説明する.6 章では SAS-L2 を用いたセキュアな組込みシステムの設計について説明する.7 章では,検証の結果や考察を示し,8 章では本研究のまとめを述べる.

以上