卒論チェックシート

学籍番号　8535022x　　氏名　川村 水蘭

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．

近年、IoT の技術が発展するとともに、IoT 機器の脆弱性を狙ったサイバー攻撃の脅威が増大していることからセキュリティ対策が必須となっている。特にセンサ情報がプライバシーや非公開情報である場合には、認証や暗号通信による機密性や情報の完全性の確保を行うことが重要である。一般的に IoT 機器は低消費電力で情報を通信できるように設計されているが、PC に比べると処理能力は低い。そのため IoT 機器のための軽量な認証方式が検討されている。その 1 つとしてワンタイムパスワード認証方式である SAS-L2 が提案されているが、SAS-L2 の IoT 機器においての実装は未だ検討されていない。本研究では、実際に処理能力に低い IoT 機器 TWELITE と呼ばれる無線機能を持ったマイコンモジュールにおいて、SAS-L2 を実装し、認証のための計算時間の評価を行い、TWELITE および IoT 機器における SAS-L2 の有効性を示すことを目的とする。

本文におけるページ番号：1~2

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）

本研究で、処理能力の低い IoT 機器 TWELITE 間の無線通信に SAS-L2 を実装し、SAS-L2 の有効性を示すことで、他の IoT 機器にも幅広い領域においてセキュリティ対策を実現することができる。

本文におけるページ番号：1~2

（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．

無線通信機能をもった IoT 機器 TWELITE を 2 台用意し、SAS-L2 におけるサーバ側とユーザ側それぞれの認証プログラムを作成する。システムの開発は各 TWELITE をノートパソコンに接続し、TWELITE を開発したモノワイヤレス社から提供されているプログラムをコンパイル、実行するためのアプリを使用し、サーバ側およびユーザ側の認証を可視化することで SAS-L2 の認証が正しいかどうか確認し、認証にかかる計算時間を評価する。

本文におけるページ番号：25~28

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）

処理性能の低い IoT 機器への SAS-L2 の実装をした無線通信を実現することで、TWELITE における SAS-L2 の有効性を示すとともに、他の IoT 機器に対しても SAS-L2 を採用する有意性があるといえる。

本文におけるページ番号：1~2, 29

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．

実験の結果により、TWELITE 間における無線通信において SAS-L2 を実装し、認証が正しく行われていることが確認できた。また、認証にかかる時間を計測し、SAS-L2 におけるユーザ側の計算時間がサーバ側に比べて短く、ユーザ側の処理負荷が少ないことが確認できた。

本文におけるページ番号：27~28

[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．

本論文では、第 1 章で卒業研究の背景・目的・目標を示し、第 2 章では、本研究で

使用する一方向性関数であるハッシュ関数について説明し、第 3 章では、第 2 章で説明したハッシュ関数を利用した SAS-2 および SAS-L2 認証方式について説明する。そして第 4 章では本研究で使用する IoT 機器 TWELITE について説明し、第 5 章では TWELITE に SAS-L2 を実装するための方法、およびその結果について述べる。最後に、第 6 章では本研究のまとめを述べる。

以上