卒論チェックシート

学籍番号　8535080y　　氏名　吉本　智哉

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，インターネットの技術の発展により、世界中の様々なものがインターネットに接続されている。IoT機器の増加にともない、サイバー攻撃が大きな問題になっている。そこで、IoTのための認証手法であるSAS-L(3)の実装および安全性に関する検討を行い、SAS-L(3)の有効性について検討することが研究目的である。

本文におけるページ番号：1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）

SAS-L(3)の安全性と実用性の有効性を示すことでＰＣになどに比べると処理能力が低いIoT機器において、安全性を確保しつつ処理コストを抑えたセキュリティ対策が可能となる。そして、センサやICタグのような小型かつ低スペックのIoT機器に搭載でき、人類、社会に貢献することができる。

本文におけるページ番号：1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-L(3)の安全性の検証において、リプレイアタックの脅威が存在するSAS-L(1)と比較することでSAS-L(3)の安全性を確認する。演算適用回数が少ないことで、CPU計算時間が高速化される目標を確認するために、SAS-L(3)と類似しているSAS-L(4)とCPU計算時間を比較する方法を採用した。

本文におけるページ番号：1,14,15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）

SAS-L(1)～(4)の4種類のバージョンのうち、SAS-L(3)のみ安全性の検証と実装による評価がない。そのため、ほかのSAS-Lと比較しながらSAS-L(3)の安全性や、演算処理負荷の有効性を示すことで、情報工学技術の発達や応用に貢献する。

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．

本研究では、ワンタイムパスワード認証方式SAS-L(3)の安全性を評価し、SAS-L(1)では存在したリプレイアタックの脅威がSAS-L(3)に存在しないことを確認した。さらにSAS-L(3)を計算機上に実装し、SAS-L(4)と比較してサーバおよびユーザの認証フェーズが短縮できることを示した。

本文におけるページ番号：19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、研究の背景および目的について述べる。第2章では、SASで用いられる暗号技術について述べる。第3章では、SAS-L(3)およびSAS-L(4)のプロトコルについて述べる。第4章では、評価実験の方法および結果を示す。第5章では、本研究のまとめおよび今後の課題について述べる。

以上