# 要 旨

## SAS-2 の同期問題解決手法に関する研究

相川　由樹

近年，個人情報漏洩の増加に伴い通信を安全に行えるワンタイムパスワード認証方式が注目されている．SAS-2(Simple And Secure password authentication protocol, ver.2) を暗号鍵交換に応用した方式では，ユーザ_サーバ間の通信経路遮断によって，認証情報が不一致となる問題（同期問題）が生じる. これを解決するために中原らが開発した方式では，第三者による成りすましの危険性がある. さらに, この成りすましを防ぐための方式では，同期問題が複数回発生した場合に脆弱性が残り，サーバからの返信情報が遅延した場合に認証が不成立となる場合がある.

本稿では，SAS-2 の同期問題発生時に発生する成りすましを防ぐと共に，サーバからの返信情報遅延の影響を受けない手法の提案を行う.

キーワード　ワンタイムパスワード，認証，同期問題，SAS，SAS-2，なりすまし

# Abstract

## Study on Methods to Resolve Asynchronous Problem of SAS-2

AIKAWA, Yuuki

In recent years, with the increase of the leakage of personal information, one-time password authentication protocol that allows secure communication has been focused.

One-time password authentication protocol SAS-2(Simple And Secure password authentication protocol, Ver.2) has a problem that authentication information stored in the server and the client is not corresponding when a communication route between the server and the client is broken by unexpected reasons.In the method to solve this, there is a risk of spoofing by a third party.

In addition, in the method to prevent this spoofing, there remains the vulnerability if the synchronization problem occurs more than once, it is not established authentication when the reply information from the server is delayed.

In this paper, we propose a secure authentication protocol to resolve these problems.

***key words*** One-time password, Authentication, Asynchronous Problem, SAS, SAS-2