要 旨

安全な遠隔操作方式に関する研究

新貝　達朗

近年，通信キャリアを中心として，駅，空港，街中などあらゆる場所で公衆 Wi-Fi サービスを提供している．このサービスはパソコンやスマートフォンで Wi-Fi の規格に対応している端末を所持していれば，誰でも手軽に利用することができる．しかし，こうした公衆 Wi-Fi サービスではノンパスワードで提供されている場合がある．そうした場合に，悪意のある第三者から通信内容を盗聴される危険性がある．この問題を解決する方法として，遠隔操作がある．しかし，既存製品では，一度のセッションで一つの暗号化鍵を利用し続けるため，鍵を盗聴されると通信内容の秘匿性が保てない．

そこで本論文では，一定時間ごとに暗号化鍵を変更する遠隔操作の提案とアプリケーションの開発を行った．これにより，公衆 Wi-Fi のような，安全性が確保されていないネットワークにおいて，提案方式を適用した遠隔操作アプリケーションを利用することで，既存製品と比較して秘匿性の高い通信が可能となった．

キーワード　遠隔操作，SAS，SAS-2，公衆 Wi-Fi，ワンタイムパスワード，安全

Abstract

A Study on Secure Remote Control Methods

SHINGAI, Tatsuro

In recent years, communication carriers provides public Wi-Fi services in train stations, airports, the city.This service if you are in possession of the terminal corresponding to the standard of Wi-Fi, you can be utilized.However, sometimes it is provided in a non password in such public Wi-Fi service.In such a case, there is a risk of eavesdropping the communication content from the malicious third party. To solve this problem, there is a remote control.However, the existing products, continue to use a single encryption key. Therefore, it is not maintained confidentiality of communication contents to be eavesdropping key.

In this paper, I proposed a method to change the encryption key at regular time intervals and went the application development of applying the proposed method.As a result, In a network that does not safety is secured, it has become possible higher than the existing products confidential communication.

key words Remote-Control, SAS, SAS-2, Wi-Fi, One-time password, Secure