要 旨

携帯端末に適した
VoIP 暗号化通信システムの構築

石井　勇太

近年, 公衆電話網と IP ネットワーク網を統合する動きが進んでいる. その中で, IP ネットワークを用いた音声通信の仕組みとして, VoIP(Voice over Internet Protocol) 通信が利用されている. しかし, 公衆網を利用した VoIP 通信は, 悪意ある第三者に通話内容を盗聴される可能性がある. この問題を解決するために, VoIP over SSL(VoIPs) を利用する方法があるが, VoIPs は通話中に同一の暗号鍵を利用する. そのため, 通話中に暗号鍵を盗まれると, 通話内容の秘匿性を保てない. この問題を解決するために, 先行研究では一定時間ごとに暗号鍵を変更する, 秘匿性の高い VoIP 通信を提案している. 先行研究では, 携帯端末を用いた同一 LAN 内の VoIP 通信を実現している.

本研究では異なる LAN 間の VoIP 通信を実現するために, VoIP 通信を中継するロビーサーバを設置し, サーバを経由して通信する.

キーワード　VoIP, 暗号化, ワンタイムパスワード, SAS-2, ロビーサーバ, IP ネットワーク, 携帯電話

Abstract

An encrypted VoIP communication system for mobile telephones

Yuta, Ishii

In recent years, movement to integrate the public telephone net and the IP network is advanced. In the movement, VoIP(Voice over Internet Protocol) to communicate the voice-data by the IP network is used. However, VoIP using the public network has danger. In order to solve this problem, there is a method of using VoIPs(VoIP over SSL). However, VoIPs keeps using the same encryption key while talking over the mobile phone. Therefore, when he/she had the encryption key stolen, hiding the content of the telephone call secretly can not be kept. As the earlier study, the VoIP communication that improve degree of hiding the content of the telephone call have been As the earlier study, the VoIP communication in same LAN with a portable terminal has been achieved.

In this study, we have achieved the VoIP communication with different LAN, and exchanged address information of the lobby server with other party beforehand.

key words VoIP, Encryption, One-time password, SAS-2, lobby server, IP network, mobile phone