要 旨

携帯電話における
VoIP 暗号化通信の提案

小 野　豊

近年，設備維持費や，通話料の軽減を目的とし，VoIP(Voice over Internet Protocol) を導入する企業が年々増加している．さらに，VoIP をカフェや，空港のラウンジなどの公衆網で利用することにより，さらなる通話料軽減が可能である．しかし，公衆網を利用した VoIP は，悪意ある第三者に通話内容を盗聴される危険性がある．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．しかしながら VoIPs は，通話中に同一の暗号鍵を利用し続けるため，鍵を盗まれると通話内容の秘匿性が保てない．さらに，携帯電話に VoIPs を実装した場合，計算コストの課題がでてくる．

そこで本論文では，携帯電話に適し，秘匿性や通信帯域を考慮した，通信プロトコルの提案・評価を示す．本提案プロトコルを用いることにより，一定時間の暗号鍵を盗まれた場合においても，通話内容の秘匿性が従来よりも高い通話が可能となった．

キーワード　VoIP, 暗号化, ワンタイムパスワード, SAS-2, 携帯電話, RSA, Diffie-Hellman 鍵交換, S/Key

Abstract

Encrypted communication of VoIP with a mobile phone

ONO, Yutaka

In recent years, the company which introduces VoIP(Voice over Internet Protocol) for cost reduction is increasing every year. Furthermore, the reduction of the charge for a call is possible by using VoIP in a cafe. 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. And, if we implemented VoIPs to a mobile phone, there will be problem of the calculation cost.

In this paper, we propose the protocol that consider confidentiality of telephone. As a result, even if a encryption key is stolen, confidentiality can be kept.

key words VoIP, Encryption, One-time password, SAS-2 ,mobile phone, RSA , Diffie-Hellman key exchange, S/Key, Key exchange, Authentication