

要 旨

アドレスを変動させる通信アーキテクチャへの OTP 認証を用いたアドレス生成手法の適用

小 松 佐 典

IPv4 から IPv6 への移行に伴う, 通信プロトコルの刷新を機に, それまでに顕在化した問題を解決するために多くの通信アーキテクチャが提案されている. その一つにアドレスを変動させて通信の安全性を高める通信アーキテクチャがあるしかし, 先行方式では安全性の面で問題があり, 改良の余地がある.

本研究では, 先行方式のアドレス生成の処理にワンタイムパスワード認証方式の中でも低処理負荷な SAS-2 認証方式を適用した方法を提案し, 先行方式と安全性を比較評価した. その結果, 先行方式よりも高い安全性を確保できた.

キーワード IPv6, SAS-2, セキュリティ

Abstract

Application of the address generation method using OTP authentication to communication architecture to use changeable address

Komatsu, Sasuke

Opportunity to accompany the transition to IPv6 from IPv4, the renewal of the communication protocol, in order to solve the problem that was not up to it, a lot of communication architecture has been proposed. There is a communication architecture to increase the safety of the communication address varying one of them. However, the prior method has a problem in terms of safety, therefore room for improvement.

In this paper, we have proposed a method of applying an authentication method SAS-2 low processing load among the one-time password authentication processing of the prior system address generation. And I was to evaluate safety and compare the preceding method. As a result, I was able to secure a high level of safety than the preceding method.

key words IPv6, SAS-2, Security