要 旨

P2P 型ネットワークへの
ワンタイムパスワード認証方式の適用

西 田　雄 治

近年，P2P(Peer-to-Peer) 型ネットワークを利用したアプリケーションの普及が目覚しく，様々なサービスが提供されるようになってきている．ネットワークを利用したサービスを安全に提供するためには，ユーザ認証を行うことが必要となる．P2P 型ネットワークでは，認証サーバを設置したり，公開鍵基盤 (PKI) を利用して認証が行われているが，どちらの方法でも，サーバや認証局 (CA) を設置，運用する必要がある．そのため，低コストで運用可能，耐障害性が高いといった P2P 型ネットワークの利点が失われることになる．本論文では，P2P 型ネットワークの利点を生かしながら，安全なユーザ認証を行う方法を提案する．認証方式としては，ワンタイムパスワード認証方式 2GR を利用し，認証情報を分散ハッシュテーブルを利用してネットワーク内で分散，保持する．

キーワード　P2P, 認証, 分散ハッシュテーブル, ワンタイムパスワード, 2GR

Abstract

Application of One-Time Password Authentication Protocol to Peer-to-Peer Network

NISHIDA, Yuji

In recent years, the spread of the application using the P2P(Peer-to-Peer) network is remarkable, and various services come to be provided. User authentication is necessary to provide safety service on the network. In the P2P network, user authentication is done by setting up the authentication server, and using Public Key Infrastructure(PKI). However, either method should set up and operate server and Certification Authority(CA). Therefore, the advantage of the P2P network that it is possible to operate low-cost and high fault tolerance will be lost. In this paper, we propose a method of user authentication while making the best use of the advantage of the P2P network. We use One-Time Password Authentication Protocol 2GR, and authentication data is distributed in the network using Distributed Hash Tables.

key words P2P, Authentication, Distributed Hash Tables, One-Time Password, 2GR