要 旨

秘密分散法のファイルシステムへの応用

澤野 充明

情報に秘匿性や対災害性を持たせて保管する方法に秘密分散法 (SSS: Secret Sharing Scheme) がある。現在、SSS の実装として UNIX 上の ssar コマンドがある。ssar コマンドはユーザに SSS を利用していることを意識させてしまうという問題点がある。本研究の目的はユーザに SSS を意識させないようなファイルの保管手法を与えることである。今回は、SSS を UNIX ファイルシステムへ応用することの提案を行い、それの実装に必要な暗号化/復号化モジュールの作成を行った。

キーワード　秘密分散法、対災害性、秘匿性、UNIX ファイルシステム

Abstract

An Application of Secret Sharing Scheme to UNIX File System

SAWANO Mitsuharu

SSS (Secret Sharing Scheme) is a method to data storages to have disaster prevent property and secarity. There is a command named ssar implemented on UNIX. The command has a problem that user must be conscious of SSS. The purpose of this research shows a method for file storage that users are not conscious of SSS. I made proposal of the application of SSS to UNIX File System. I created the encrypt/decrypt module that necessary to implementation of SSS.

key words Secret Sharing Scheme, disaster prevention property, Security, UNIX File System