要 旨

モバイル環境における
セキュアなコンテンツ流通方式

谷藤喜彦

ブラウザフォンの爆発的な普及に伴い，新しいコンテンツの流通経路としてモバイルインターネットが注目されている．ネットワーク上でコンテンツを取り引きする場合，「宣伝したいが，対価を取るまでは全体を見せたくない」，「内容が見られないので買いにくい」という売り手，買い手双方の取引抑制要因があり，内容を提示しかつ確実な取り引きが可能なメカニズムの確立が望まれている．

本論文では，モバイル環境における，安全性が十分でないネットワークを介して，オリジナルコンテンツから，可逆性のある半開示暗号化コンテンツと復元のための鍵情報を生成し，安全にディジタルコンテンツを流通させる方式を提案する．SAS-K パスワード認証を用いて毎回異なる認証データを送信するため，ネットワーク上を流れるデータの盗取や再利用は困難となる． さらに，コンテンツ復元用鍵を暗号化して配送する際に，暗号化鍵を今回認証データとすることで，ユーザが復号鍵の配送を受けることなく，暗号化したコンテンツ復元用鍵を取得可能である．本方式では，SAS-K パスワード認証方式を応用して，暗号通信に必要な認証，暗号，鍵配送を同時に満たすプロトコルを設計した．

キーワード　モバイル　インターネット　コンテンツ流通　電子商取引　SAS 認証　半開示　暗号化

Abstract

A Secure Digital Contents Communication Services in Mobile Environments

Yoshihiko TANIFUJI

According to the explosive introduction of "Browser Phone", the internet using mobile environments will be a new communication method. In those communications, both of users and contents providers require secure contents communications mechanism because of anxious using in network transactions.

In this paper, a secure contents communications method is proposed, which has secure protocols using encrypted contents and there decryption key. The method uses SAS key one time authentication protocol which brings its secure communications and key distribution for contents decryption. The introduction of SAS-K which is bring secure interfaces because of doing authentication and key communication at the same time.

key words Mobile Internet Contents delivery Electronic Commerce SAS authentication Half the indication Cryptosystems