要 旨

Book 型情報閲覧システムにおける セキュリティ方式

井上 富幸

インターネットに代表される情報通信関連技術の発達により，様々な形でデジタル情報がやりとりされるようになってきている．このようなデジタル情報の円滑な流通には，利用者の操作性向上が重要な技術ポイントとなる．筆者らはデジタル情報利用者の操作性向上を目的に，古来より広く用いられ一般の利用者に親和性の高い「本」の操作性を応用した，CyberBook と呼ぶ Book 型情報閲覧システムについて，NTT 研究所と共同で研究開発を進めている．CyberBook は，デジタル情報の閲覧に必要な機能を有し，テキストのみならず音声，動画等にも対応したマルチメディア情報閲覧システムである．

近年のモバイルコンピューティングの発展に見られるように，情報閲覧の多様化，高付加価値化，パーソナル化が一層進展してくるにつれ，CyberBook の優れたユーザインタフェースと総合マルチメディア閲覧機能に，課金や認証に代表されるセキュリティ機能を付加したいという需要が高まってきている．

コンテンツ流通における課金や認証機能の実現を目的に，当研究室では SAS と呼ぶワンタイムパスワード認証方式の研究を進めている．CyberBook のセキュリティ機能実現においても，この SAS を中核におくが，ある種の攻撃法に対する安全性の向上が求められていた．そこで筆者はまず，卒業研究生を指導し，CyberBook のセキュリティ方式実現の中核となるワンタイムパスワード認証方式 SAS の安全性向上という課題に取り組み，簡易でかつ安全な方式を完成させた．この成果については，卒業研究として別途発表する．

本論文では，一連の研究の中から特に，SAS の応用としての CyberBook のセキュリティ

方式について述べる．まず，CyberBook に対するセキュリティ要件を整理し，安全なコンテンツ配信を実現するとともに，有料情報の閲覧サービス等にも柔軟に対応できるセキュリティ方式について提案し，評価した結果についてまとめる．

キーワード　Book 型情報閲覧システム，SAS，暗号化構造

Abstract

A Study on Security Methods for a Book-style Multimedia Document Viewer

Inoue Tomiyuki

Various ways of digital contents communications have been getting popular, owing to the development of information communication technologies, particularly the Internet. In those contents communications, human machine interface is one of the important technical elements to improve the user-friendliness of the digital contents viewing system.

Our laboratories have been developing a new type of digital contents viewer, called CyberBook, being partnering with NTT Laboratories. The CyberBook is a multimedia contents viewer with a book-style icon and handles text, voice, image data and video. Users can use the CyberBook as if they turn the pages of a real book, and they can make bookmarks of the data they want to retrieve as if they place an actual bookmark in the book.

In the development of the CyberBook, the recent task is to add security functions, such as for billing and authentication. This is because the information viewing methods have been diversified, value-added and personalized particularly as various mobile computing tools have been introduced, aiming at their application to electronic commerce systems.

Our Laboratories, therefore, has been developing a one-time password authentication method, called SAS, to realize the billing and authentication function for digital contents communications. The SAS is a key technology of the CyberBook's security functions.

In particular, we have been focusing of the enhancement of its robustness against a certain attack method and its user-friendliness. For its details, we will announce it later as part of our academic research.

In this thesis, the CyberBook security function based on SAS will be explained, followed by our proposal for secure distribution of the digital contents and for the charged contents services.

key words Book-style Multimedia Document Viewer, SAS,Cipher System