平成 12 年度

修士学位論文

Book 型情報閲覧システムにおける セキュリティ方式

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

1035006　　井上 富幸

指導教員　　情報システム工学科 清水 明宏

2001 年 1 月 29 日

高知工科大学大学院 工学研究科 基盤工学専攻

情報通信ネットワークコース

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

目次

第 1 章

まえがき

コンピュータ，情報ネットワークの急激な発展に伴って情報をいかにしてユーザに提供するか，また情報の内容も文字を中心としたものから，画像，音声，動画とより多くの情報量を提供できるように研究開発が行われてきた．これらの研究開発によって一般の人々がマルチメディア情報に触れる機会が増えてきた．しかし従来のウェッブブラウザに見られるようなリンクを順次たどって必要な情報に到達する方式には，必要な情報の場所がわかりにくいという欠点があった．これは異なる空間に存在する情報がリンクによって接続され，複雑にからみ合った構成となっていることが原因となっている．

また我々は文字を含めた視覚的な情報を記憶して再利用しようとした時，レイアウト情報から必要な情報を再発見する傾向が強い．しかし，従来のウェッブブラウザでは，表示領域に入り切らないデータを閲覧するためにスクロールを行う設計となっている，これではレイアウト情報が変化してしまい情報の認識効率が低下するという問題が生じる．これらの問題の解決方法の一つとして提案しているマルチメディア情報閲覧システムが CyberBook である．[1]

CyberBook はコンテンツを作成する Author と閲覧する Viewer から構成され，Author では本型のユーザインターフェースを持つコンテンツを GUI 環境で容易に作成することができる．Viewer では Author で作成したコンテンツを本型のインターフェースで閲覧することができる．現在 CyberBook システムはすでに 1000 件近いコンテンツがインターネット上で公開されており自由に閲覧ができるようになっている．

CyberBook はテキスト等のコンテンツを主に取り扱う電子本ととらえることもできるし，音声動画等を主に取り扱うマルチメディアコンテンツとしてもとらえることができる．

電子本に対する様々なビジネスのアプローチが行われており，国内だけでも次のような電子本に対する動きがある．[2] [3] [4]

1. CD-ROM 黎明期における電子本の出版例

   1985 年　三修社，国内初の CD-ROM『最新科学技術用語辞典』刊行

   1987 年　岩波書店『広辞苑 第三版 CD-ROM 版』刊行，電子出版加速される

   1988 年　三省堂『模範六法 昭和 62 年版 CD-ROM 版』＋検索ソフト　　自由国民社『現代用語の基礎知識』

2. 日本電子出版協会

   設立　1986 年 7 月

   目的　日本の電子出版の普及促進と各種情報の提供

   活動　CD-ROM マルチメディアフォーマットの調査 ISO9660 の日本語拡張 (1990)
   World Font CD の制作と配布 Unicode 漢字フォント付き (1996)

3. 電子ブックコミッティ

   設立　1991 年

   目的　電子ブック (8cm CD-ROM) の普及

   活動　電子ブックタイトルの普及

   タイトル数　300　内 100 は海外タイトル。辞書系以外に学習参考書，旅行ガイド，電話帳などの実用書も豊富

4. EPWING コンソーシアム

   設立　1991 年 10 月 (岩波書店，ソニー，大日本印刷，凸版印刷，富士通)

   目的　CD-ROM 辞書検索を目的とした EPWING 規約の普及

   活動　JIS X4081「日本語電子出版検索データ構造」として，EPWING 規約を JIS 化 (1997)

   タイトル数　40　広辞苑，知恵蔵など辞書系を中心にマニュアル，白書など

5. PictROM 研究会

設立　1993 年頃

目的　コミックや CTS 化されていない書籍を，画像で CD-ROM に貯える

タイトル　少年サンデー (小学館)，ガロ (青林堂)，マルクス全集 (大月書店) など

6. NEC デジタルブック

設立　1993 年

目的　読書端末の黎明期　ＦＤで供給されるコンテンツを，パソコン経由でデジタルブックに入れる

タイトル　200 点以上　小説から囲碁まで広範囲に展開

7. 電子書籍コンソーシアム

設立　1998 年 10 月 (実証実験期間は 2000 年 3 月まで)

目的　電子書籍システムの仕様検討とプロモーション活動

ブックオンデマンド実証実験 (通産省の補助)

読書端末　シャープ (180DPI 液晶)，日立，松下，ソニーなど

タイトル数　5000 冊の画像化 (最大 1 冊 15MB) を予算に盛り込む

8. BookWorld

設立　1998 年 (実証実験期間は 1999 年 9 月まで)

目的　通産省の補助金を使った実証実験

活動　コンテンツのダウンロードとカードによる決済が可能

雑誌の記事など細かい単位で，50 円，100 円という小額購読が可能

データ形式は，PDF，独自フォーマットなど

またすでに著作権管理システムなどのセキュリティ機能を持ってコンテンツ配信サービスを行っているものとして音楽配信システムがある．一部の例を下記に示す.

1. a2b music

a2b music 社による音楽配信システム

音声圧縮，データの暗号化，ライセンス管理システムで構成される

電子ライセンスシステム「PolicyMaker」によって，使用期間や複製権，再生回数に合わせたライセンスのカスタマイズが可能

2. DAWN 2001

JASRAC による音楽著作権管理のデジタル化構想

音楽著作物の作品届受付，使用届受付などの情報を統合したデータベースを構築し，業務をデジタル化する

ネットワーク上の音楽コンテンツについては，電子透かしによりコンテンツに埋め込まれた著作者情報と，統合データベースを照合し，利用された (購入された) 楽曲 1 件 1 件の著作物使用を把握する

3. DRM (Digital Rights Management)

Intertrust 社によるデジタル著作権管理システム

コンテンツ提供者が，コンテンツを制限を加えパッケージングして配布，ユーザは，コンテンツパッケージを入手した後，ライセンスサーバへ接続してライセンスを受け取る

4. EMMS (Electronic Music Management System)

米 IBM による音楽配信システム

専用のクライアントソフト，認証サーバ，コンテンツ制作システムなどで構成されている

5. InfoBind

NTT と神戸製鋼所の共同開発による音楽配信システム

固有の識別番号 (ID) 付きスマートメディアを利用し，特定のメディアにのみ記録可能なことによる不正コピー防止機能を持っている

6. InterTrust

著作権管理機能を組み込んだ音楽配信システム

コンテンツは，音楽データや歌詞，クレジットのほか，著作権情報，端末機器への

コピー制限情報などをまとめて暗号化され「Digibox」というファイルに収められて配信される

著作権保護には，著作権管理システム「DRM」が使われ，コンテンツの追跡調査も可能になっている．

音楽を聴くには，専用の再生ソフトが必要，再生ソフトは，ジャケット写真，リンクボタン，歌詞などを表示する機能を持っている。

ユーザ認証は，課金/認証センタで行なわれる。

7. Liquid Audio

Liquid Audio 社による音楽配信システム

データには，RSA 暗号鍵による暗号化，電子透かしによる著作権侵害防止策が施されている

ユーザは，音楽購入時に「Liquid Passport」が発行され，その購入に使用した専用の再生ソフト「Liquid Music Player」のみで再生することができる

再生ソフトは，ジャケット写真や歌詞，クレジットなどを表示が可能

8. MagicGate

ソニーによる，半導体メディアやパソコン用の音楽著作権保護技術

コンテンツを暗号化するとともに，メモリースティックなどの半導体メディアと対応機器の間で，お互いが，MagicGate による音楽著作権保護に対応しているかどうかの認証を行ない，認証されたメディアと機器間でのみ音楽コンテンツの再生や移動が可能となる

このように，様々な方式が提案され実用化されている．しかし，これらの中にはテキスト，動画，音声など全てのマルチメディアコンテンツ構成要素を統合的に管理しセキュリティ機能を持っているシステムはない．

そこで，CyberBook のコンテンツを構造化，暗号化しセキュリティ構造を持たせ有料閲覧サービスに対応させ，きめ細かな課金方法を実現しマルチメディア統合配信ビジネスの基

盤アプリケーションとして提案する.

第 2 章

CyberBook について

2.1　Book 型インターフェース

前述のように CyberBook はマルチメディア情報を情報端末で誰でも手軽に閲覧できるように，紙に書かれた従来の本に類似したユーザインターフェースを持つ情報閲覧システムである．[1]

図 2.1 に示すように一般的な本と同じイメージを情報端末上で再現しており，初心者のユーザにとっても受け入れやすいインターフェースとなっている．[5]

図 2.1　CyberBook の例

電子計算機上で実現されているシステムである特徴をいかして音声，動画等のマルチメ

ディアコンテンツをも簡単に電子本上から閲覧することを可能にしている．すでにこのシステムによってデータを電子化した本として整理し，インターネット経由での配付や電子図書館 (InterShelf) としてのデータの蓄積，一括管理システムが実現している．[6]

2.2　システム構成

CyberBook は大きくわけるとコンテンツを生成する Author とコンテンツを閲覧する Viewer の２つのシステムで構成されている．

Author では各種音声，静止画，動画，テキストといったマルチメディアデータを電子計算機上で本のインターフェースで扱えるように編集を行うために次のような機能をもっている．

図 2.2　Author の機能

- ページ作成機能（本文，目次，索引，等）
- 内容作成機能（領域部品-１０種類，アイコン部品-５種類）

- マルチメディア情報編集機能

表 2.1　編集対象ファイル形式

種類	ファイル形式
音声	μ-law/WAV
動画	QT(MOV)/AVI
静止画	GIF/JPEG/XWD
テキスト	テキストデータ

- HTML 文書の変換機能

Author で編集されたコンテンツはテキストをデータ化したブックファイル (.bok)，静止画ファイル (.fig)，キーワードファイル (.key)，参考文献ファイル (.lit)，音声ファイル (.wav など)，動画ファイル (.mov など) の各ファイルで構成されるなおブックファイル，静止画ファイル，キーワードファイル，参考文献ファイルの最小基本構成の４つのファイルを圧縮して１つのアーカイブファイル (.bma) としている．

Viewer では Author で作成したコンテンツを閲覧するために次の機能をもっている．

- ページめくり機能（タグ，付箋などの機能を含む）
- 検索機能（文字列検索，キーワード検索など）
- マルチメディア情報表示機能（ポップアップ表示，ズーム表示，アニメなど）
- 簡易メモ機能

以上の Author，Viewer が動作するために必要なハードウェアの環境の一例を表 2.2 に示す．この表からわかるとおり現在一般的に使用されているパーソナルコンピュータ程度の処理能力があれば CyberBook を十分使用することができる．ここでは Windows 版における例を示したが他にも Macintosh，UNIX 用のシステムもあり Windows，Macintosh，UNIX 間でのデータの共有が実現している．[**?**]

表 2.2　必要なシステム要件

項目	必要環境
CPU	Intel x86，Pentium，PentiumII，PentiumIII など
OS	Windows95，98
メモリ	３２ MB 以上
ディスク容量	１０ MB 以上の空き領域が必要

2.3　コンテンツ閲覧方式

現在の CyberBook システムでは次のような方法でコンテンツの配信が行われている．一つは図 2.3 に示すようなコンテンツ全体を一度にダウンロードし閲覧する方法である．この方法では画像，音声等も含めた全てのコンテンツを一度にダウンロードするのでダウンロードに時間がかかる．しかし，閲覧に必要なデータを全てディスクに保存することによってオフラインでの閲覧が可能である．

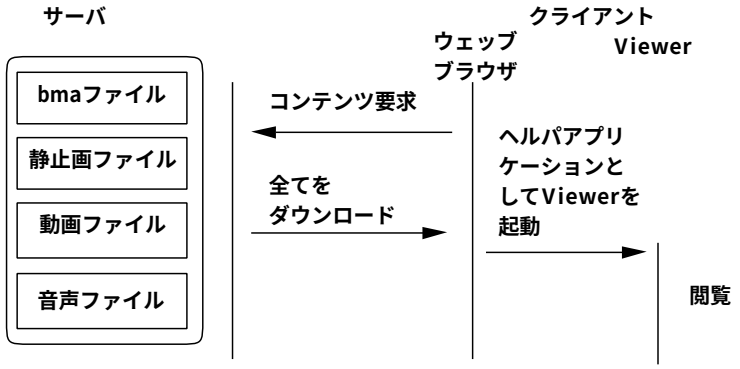

図 2.3　一体型

もう一つの方法は図 2.4 に示すように本文を含む最小基本構成の bma ファイルのみをダウンロードしておき閲覧途中で画像等の部分では逐次必要なファイルをダウンロードしなが

ら閲覧する方法である.

この方法では最初のダウンロードには時間がかからないがオフラインでの閲覧時には本文の

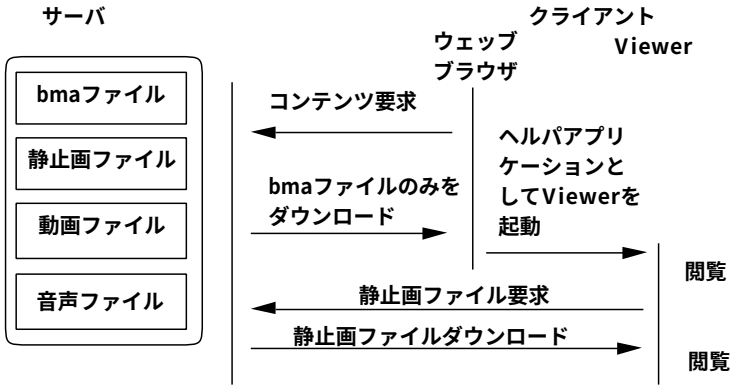

図 2.4　逐次型

みの閲覧は可能であるが画像等の部分は見ることができない．ただしバッファを有効にしておくことによりバッファの有効な場合には閲覧可能である場合もある.

第 3 章

CyberBook へのセキュリティ機能要件

3.1 セキュリティ要件

CyberBook は従来の HTML などで構成されたファイルや文書，マニュアル類を本型のインターフェースで閲覧できる形にコンバートすることができ，これらコンバートしたコンテンツなどからマルチメディア電子書籍を作成することができる．しかし，現状では CyberBook のシステム内にセキュリティ機能がなく，現在のシステムのままの CyberBook で有料コンテンツを配信しようとした場合には何らかの方法でユーザ認証をした後，コンテンツ全体を有料で配信するしか方法がない．しかし，この方法ではコンテンツの内容を購入以前のユーザによる部分的閲覧を許可するなど（書店での立ち読みにあたる），柔軟なアクセス制限ができない．また，辞書，百科事典的なコンテンツであれば全てを購入せず閲覧したい部分のみを購入したいといったニーズにも対応できない．ここでは CyberBook をこのような問題にも対応できる統合マルチメディアコンテンツ配信ビジネスの為のシステムと考えた場合に必要とされるセキュリティ機能を整理する．

1. セキュリティ配信機能
   - コンテンツの改ざん等を防ぐためのコンテンツの暗号化．
   - 時間経過，閲覧回数による閲覧制限を可能にし適切な課金を行う．
   - コンテンツの不正な複写を防止する．

- オフライン状態での閲覧をも可能にする.

2. ユーザ認証機能
   - ユーザの確認を行う.
   - コンテンツの部分閲覧を可能にする.
   - ユーザごとに異なるアクセス制限を可能にする.
3. 決済機能
   - 安全な課金方式.

3.2　セキュリティ実現の為に必要な技術

前節のセキュリティ要件を満たすために現状の CyberBook システムに不足している機能は次の通りである.

- コンテンツが課金対象となる部分とならない部分とに別れていない.
- コンテンツが暗号化されていない.
- ユーザ認証機能がない.
- 課金機能がない.

3.2.1　コンテンツの構造化と暗号化

現在の CyberBook ではコンテンツは最小基本構成の bma ファイルとその他音声，画像等のファイルは別構造となっているが最小基本構成ファイルそのものは１つのファイルになっており，たとえば最初の１０ページに関しては体験的に閲覧が自由であるがそれ以後のページに関しては有料であるといったコンテンツを作成することができない．しかし，今後のマルチメディアコンテンツの有料配信を考えた場合にはユーザがそのコンテンツを必要とするかどうかを判断しやすくするために部分的に開示しておく事は重要な要素であると考えられる．また，非公開の部分については事前にユーザに暗号化したファイルとして渡しておく方法と必要になった時にサーバから送る方法とが考えられるがサーバから送る場合であっ

ても盗聴，改ざん等の危険からコンテンツを保護するためにはコンテンツの暗号化は必ず必要であると考えられる．

3.2.2　認証機能

ユーザ管理を行い認証が成立した場合に課金を行い閲覧を許可する方式を導入する必要がある．コンテンツの構造化と暗号化でも述べたように部分的な閲覧をも可能にするためにはコンテンツの閲覧途中でのユーザ認証が必要となる．したがってコンテンツそのものも認証機能を配慮した構造とする必要がある．

3.2.3　課金機能

認証機能と連動して適切な課金を行う機能が必要である．また，ユーザの様々な要求に対応し，例えば大きな百科事典のようなコンテンツの一つのキーワードに対するの画像情報のみを有料で閲覧したいといったことを可能にする柔軟な課金をも可能にする．

第 4 章

CyberBook システムのセキュリティ機能

4.1 コンテンツの構造化と暗号化

コンテンツを安全に配信し改ざん，盗聴を防ぐためにはコンテンツの暗号化は不可欠である．しかし，従来のようにコンテンツを自由に閲覧する部分とアクセス制限を行う部分とに分けて暗号化していたのでは，ユーザごとにアクセス制限をする範囲をかえる必要が発生した場合や一体型の配信方式から逐次型の配信方式に変更したりした場合には，新たにコンテンツの暗号化を行いコンテンツの再構築を行わなければならない．また，ユーザからの要求があった時点でコンテンツを暗号化していたのではサーバに対する負荷が非常に大きなものとなってしまう．ここでは，コンテンツ全体を構造化してその部分ごとに事前に全ての部分を暗号化しユーザごとに異なる公開する部分の鍵のみを公開することによって柔軟にユーザごとに異なるアクセス制限を可能にする方式を提案する．構造化し暗号化する方式としては次の 3 つの方式が考えられる．

- ページ方式　コンテンツをページ単位で暗号化する．
- 部分方式　　コンテンツを文字領域，図形領域などの部分にわけ部分単位で暗号化する．
- 要素方式　　コンテンツを構成する要素を行，或いは文字といったより細かな要素単位で暗号化する．

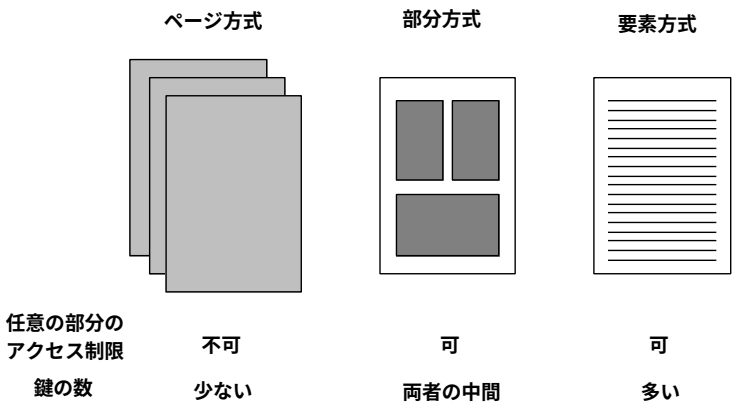

図 4.1　コンテンツの暗号化構造

ページ方式では復号鍵の数はあまり多くはならないがページ内に含まれる図形領域だけを暗号化するなどということができない．また，要素方式では復号のための鍵が膨大な数必要となる．したがって必要な部分のみを暗号化することができ復号のための鍵もあまり多くならない部分方式が CyberBook においては最適の方式である．また，従来の CyberBook においてもコンテンツの各ページ内は部分単位で管理されており部分方式であれば従来のシステムに新しい機能を付加する程度の改変で組み込むことが可能である．暗号化は，図 4.2 に示すように基本的には一つの鍵によって行われる．

コンテンツを各部分ごとに連続した部分番号 n と基本鍵 K との和を一方向性関数 E にかけ

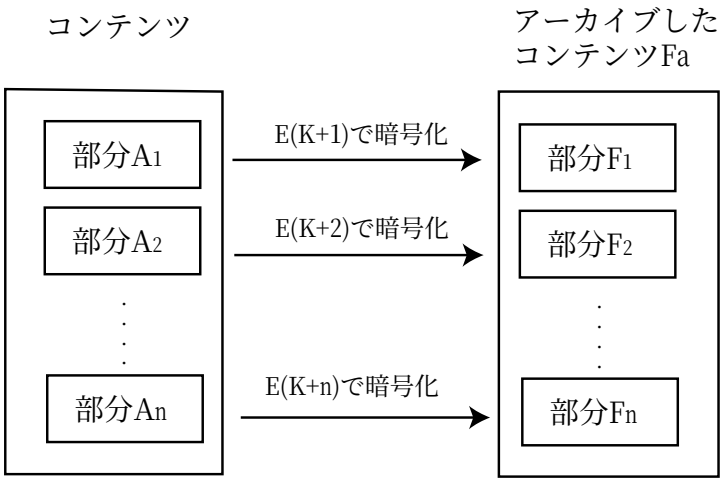

図 4.2　コンテンツの部分暗号化

た En=E(K+n) を鍵として暗号化を行う．これにより各コンテンツの部分 An を En を鍵として暗号化関数 F によって暗号化した Fn=F(An,En) を保存することになる．コンテンツサーバでは Fn をまとめてアーカイブした Fa と K を保存することになる．
以上のようなコンテンツ部分暗号化方式を使用すれば，コンテンツは１度作成すれば配信範囲や配信方法の変更があってもコンテンツの再構築をする必要はなく必要に応じて基本鍵から必要な部分を復号するための鍵を生成するだけでよい．

4.2　ユーザ認証

CyberBook を閲覧するための情報端末が，従来のパーソナルコンピュータを基本としたものから，携帯電話にインターネット接続機能を組み込んだ小型情報端末まで様々な端末の利用が可能となるようにシステムを構築するためには CPU の処理能力が十分でなく使用できるメモリ量が少なくても使用できる処理負荷の少ない方式を採用しなければならない．したがって，SSL などのような処理負荷の大きい公開鍵暗号方式ではなく，ワンタイムパスワード認証方式である Simple And Secure 認証方式 (SAS）が今回の目的には最適である．ここではセキュリティ機能をより向上させた SAS-K を採用する．これによってインターネット上での簡易で安全な認証を実現する．

4.2.1　ワンタイムパスワード認証 (SAS-K)

図 4.3 に SAS-K 認証の概要を示す．SAS-K では認証以前にユーザ登録段階においてユーザ ID(A) 及び E_0^2 を認証サーバにセキュアなルートで登録する．また，クライアント側では乱数 N_0 を記録しておく．
第１回目の認証においてはクライアント側ではユーザがユーザ ID(A) とパスワード (S) を入力する．これらの値と記録してある乱数 N_0 から次のものを求める．

$$E_0^1 = E(A, N_0 \oplus S)$$
$$E_0^2 = E(A, E_0^1)$$

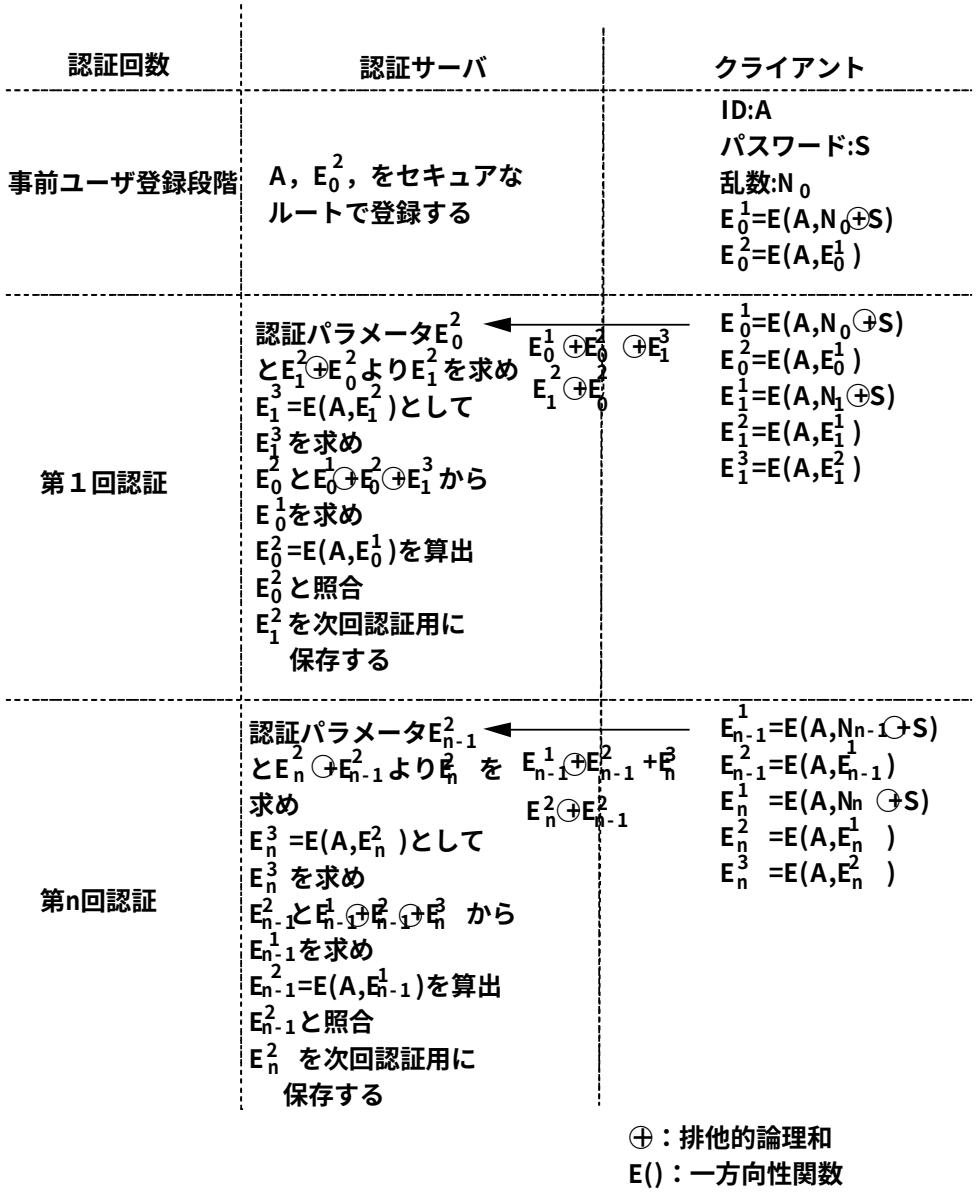

図 4.3　SAS-K 認証方式の概要

$$E_1^1 = E(A, N_1 \oplus S)$$

$$E_1^2 = E(A, E_1^1)$$

$$E_1^3 = E(A, E_1^2)$$

求められた E_0^1，E_1^2，E_1^3 からそれぞれ次のように排他的論理和を取ったものを認証用データとしてサーバに送る．

$E_0^1 \oplus E_0^2 \oplus E_1^3)$

$E_1^2 \oplus E_0^2$

また，E_1^2 は次回認証用の認証パラメータとしてクライアントに保存される．
サーバでは登録してあった E_0^2 との排他的論理和を取ることにより E_1^2 を取り出すことができる．

$$E_1^3 = E(A, E_1^2)$$

としてクライアントから送られてきた値から E_1^3 を算出する．続いて E_1^3 と E_0^2 と $E_0^1 \oplus E_0^2 \oplus E_1^3)$ の排他的論理和を取り E_0^1 を取り出すことができる．

$$E_0^2 = E(A, E_0^1)$$

としてクライアントから送られてきた値から E_0^2 を算出しサーバに登録してあった E_0^2 との比較を行い等しければアクセスを許可し E_1^2 を次回認証用の認証パラメータとして登録する．以下アクセスの度にこれら一連の処理がくり返される．

4.2.2　SAS-K を応用した鍵の共有

図 4.3 にあるように，SAS-K 認証方式を用いることで，クライアント-サーバ間であるパラメータ (図中の E_{n-1}^2) を共有化できる．すなわち，認証パラメータ E_{n-1}^2 を共通鍵とすることで共通鍵方式だけでは困難な鍵配送の問題を回避できる．この共通鍵を使用することによって，認証終了後安全にサーバから必要なデータをクライアントに送ることが可能となる．

4.3　アクセス制限情報（ACL：Access Control List）

きめ細かなアクセス制限を実現するためにはアクセス制限状況を管理する必要がある．CyberBook で考えられるアクセス制限の基本的な要素は，次の 3 つである．

- 入金しているかなどの入金情報（M）
- 利用回数を制限している場合の利用回数情報（C）
- 利用時間を制限している場合には利用時間情報（T）

これらの要素をまとめてアクセス制限情報 (ACL) として管理する．図 4.4 に ACL による

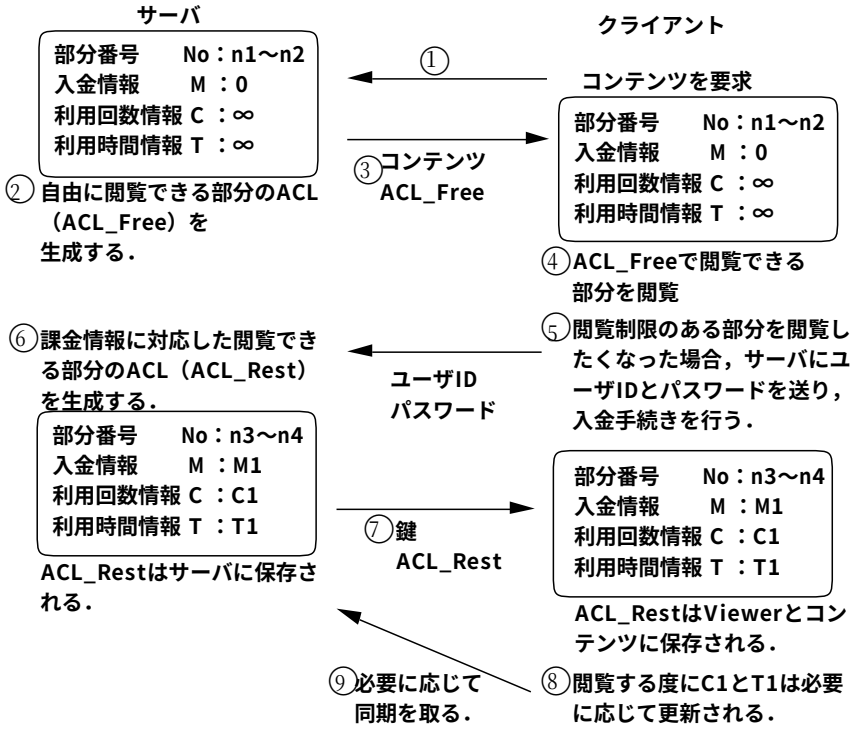

図 4.4　ACL の概要

アクセス制限の概要を示す．閲覧制限のない部分を閲覧する場合には ACL_Free を参照して閲覧を行い．閲覧制限のある部分を閲覧する場合にはサーバから ACL_Rest を取得しこれを参照し許可されている範囲内で閲覧を行うことになる．この時閲覧するたびに利用回数情報，利用時間情報は更新される．なお，たとえば利用回数情報が 0 $(C1 = 0)$ になったりした場合には，もう一度ユーザ ID とパスワードを送り認証を受け新たに ACL_Rest を取得しなおすこととなる．また，サーバにも ACL_Rest を保存していることにより事故によってクライアントの ACL_Rest が失われた場合にも回復が可能である．

4.4　プロダクト ID（product ID)

コンテンツの不正複写に対応するため Viewer にプロダクト ID(PID) を付加することとする．このプロダクト ID は Viewer ごとに異なる価を持っており事前にサーバ側とクライアント側の双方で共有しているものとする．具体的な例としては Viewer をパッケージとしてユーザに配付する時点でパッケージにプロダクト ID を付加しておく．これを Viewer のインストール時に入力し Viewer 内部にプロダクト ID が書き込まれる．ユーザがあるコンテンツのアクセス許可を取得した場合，コンテンツに ACL を書き込むと同時にこのプロダクト ID ををもコンテンツに記録する．これによって異なる Viewer による閲覧を防止する．これら一連のプロダクト ID の動きを図 4.5 に示す.

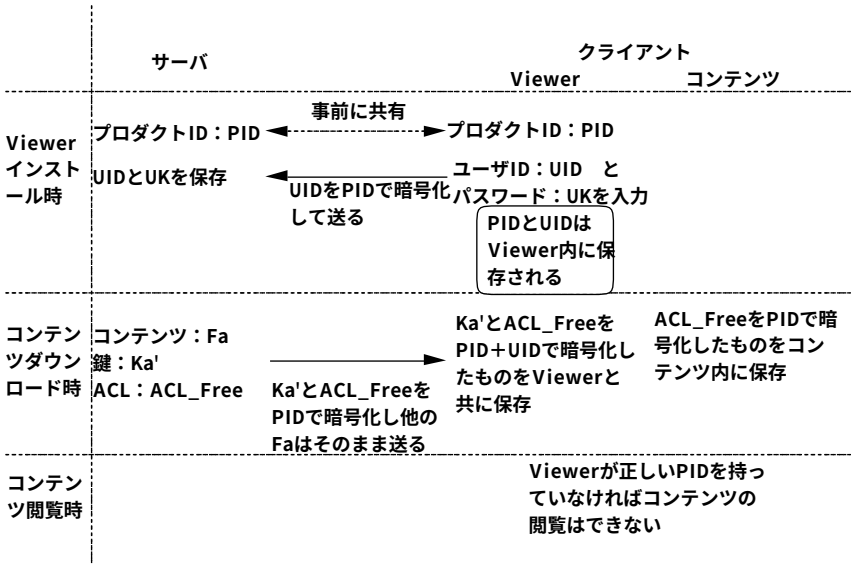

図 4.5　プロダクト ID の機能

4.5　データベース

コンテンツ配信サービスを行う場合には何らかの方法でユーザ，コンテンツ，課金情報を管理しなければならない．ここではこれらの情報をデータベースにて管理するものとし最低限必要と思われる内容について整理する.

4.5.1　ユーザ情報

表 4.1　ユーザ情報

項目		内容	型	備考
UserID		ユーザ ID	文字列	Primary Key
ProductID		Viewer のプロダクト ID	文字列	
SAS 認証用	times	認証回数	整数	
	param	認証パラメータ	整数	
個人情報	name	ユーザ名	文字列	
	mail	メールアドレス	文字列	
	type	ユーザ分類	文字列	
課金用情報	account	口座番号やクレジットカード番号など	文字列	

ユーザ情報の管理はサーバ側で行い表 4.1 のような項目を管理する必要がある．ここではユーザ 1 人に対してプロダクト ID を 1 つとしているので，閲覧できる Viewer が 1 つだけということになってしまっているこの点に関しては今後検討の余地がある．

4.5.2　ブック情報

ブック情報では，ブック ID に従って，ブックのファイル名，タイトルといった情報を管理する．課金用情報は著者に著作権料等を振り込むことを想定している．

表 4.2　ブック情報

項目		内容	型	備考
BookID		ブック ID	文字列	Primary Key
ブック全体に関する情報	Structure Info	Structure Infomation のファイル名	文字列	
	Title	ブックのタイトル	文字列	
	author	ブックの著者名	文字列	
	Key	基本鍵	文字列	
課金用情報	Account	口座番号など	文字列	

4.5.3　ACL 情報

ACL 情報では，利用可能時間，利用可能回数，利用料金などユーザに提供するサービスにたいするアクセス制限情報の基本的な値を保存する．したがって無料閲覧サービスと，有料閲覧サービスが一つのコンテンツに対して実施されている場合には ACL 情報として無料閲覧サービスにおける ACL と有料閲覧サービスにおける ACL の最低 2 フィールドの情報を持っていることとなる．

表 4.3　ACL 情報

項目		内容	型	備考
BookID		ブック ID	文字列	Primary Key
Component		閲覧可能な部分の番号	文字列	
利用可能 User	type	ユーザ分類	文字列	
ACL の内容	times	利用可能回数	整数	
	period	利用可能時間	整数	
	charge	利用料金	整数	

4.5.4　UserACL 情報

UserACL 情報は，ユーザがコンテンツの有料部分を閲覧しようとして，サーバにアクセスし閲覧手続きが終了すると生成されこのデータベースに蓄積される．したがって１ユーザ１契約に対して１フィールド必要となる．

表 4.4　UserACL 情報

項目		内容	型	備考
UserID		ユーザ ID	文字列	Primary Key
BookID		ブック ID	文字列	Primary Key
Component		閲覧可能な部分の番号	文字列	
ACL の内容	times	利用可能回数	整数	
	period	利用可能時間	整数	
	credit	入金情報	整数	

4.5.5　各データベースの関連

図 4.6 のようにユーザ情報，ブック情報，ACL 情報のそれぞれの PrimaryKey により UserACL 情報と相互に結び付けられる．

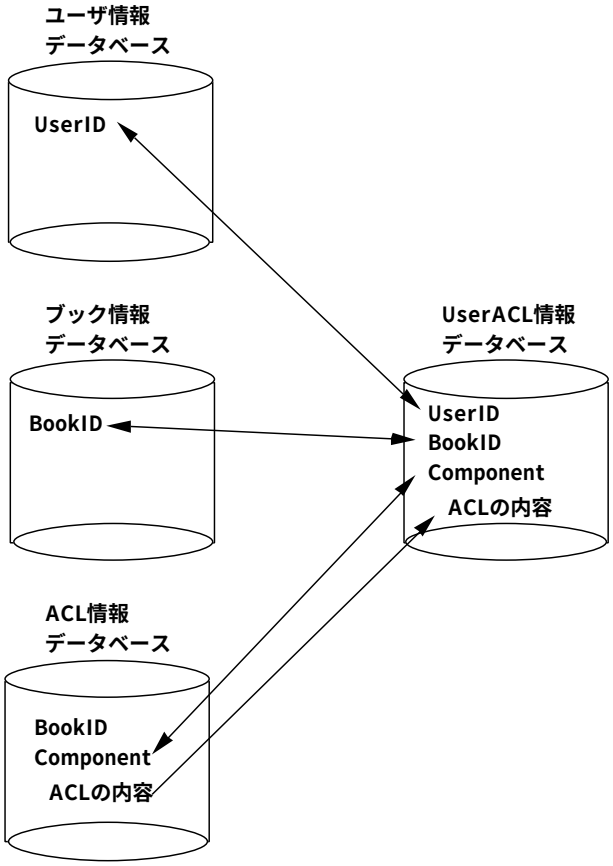

図 4.6 各データベースの関連

4.6 CyberBook システムの運用

セキュリティ機能を持った CyberBook システムの全体像を図 4.7 に示す．ここではすでに Viewer のインストールが行われユーザ登録も終了しているものとする．

1. クライアントはコンテンツのダウンロード時にコンテンツ全体と閲覧制限のない部分の鍵と ACL をまとめて取得する．
2. 閲覧制限のある部分を閲覧するためにはサーバから該当する部分の ACL と鍵を取得しなければならない．ここでユーザ認証の為に SAS を用いる．
3. サーバ側でユーザ認証が成立すれば該当する ACL と基本鍵から生成した必要な部分の鍵を生成する．
4. サーバ内のデータベースにユーザごとに ACL を保存する．

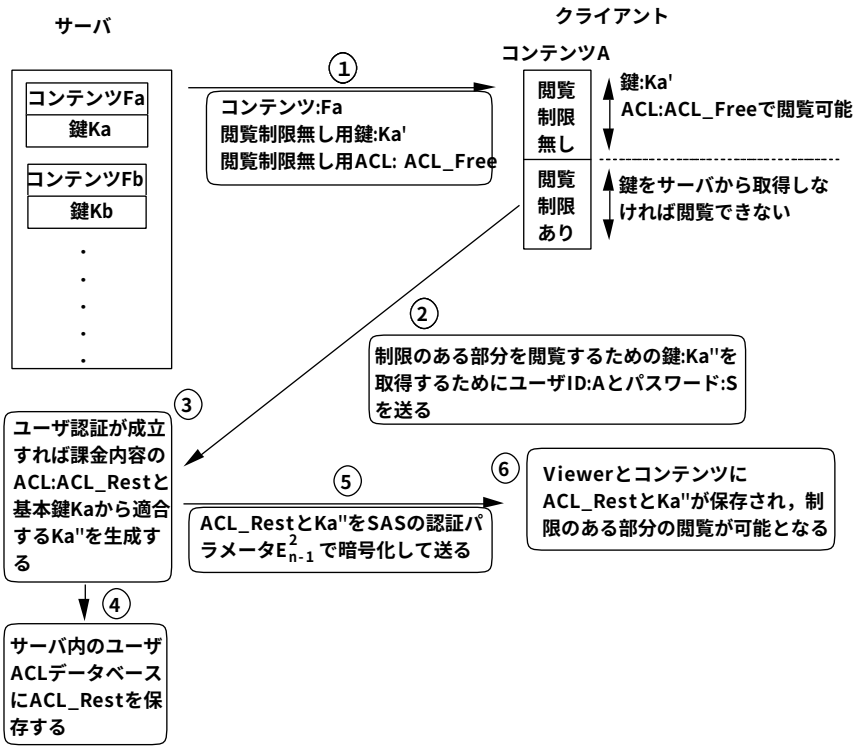

図 4.7 CyberBook システムの概要

5. サーバで生成された ACL と鍵を SAS の認証パラメータで暗号化してクライアントに送る.
6. Viewer とコンテンツに ACL と鍵を保存する．コンテンツには ACL を Viewer のプロダクト ID で暗号化して書き込む．Viewer は ACL を保存するデータベースを別に持ちここに鍵とともに保存する.

サーバ，コンテンツ及び Viewer に ACL を保存するのは次の 2 つの理由による.

- 誤ってユーザがコンテンツを紛失してしまった場合にリカバリを行うため.
- Viewer とコンテンツで同じもの (ACL, プロダクト ID) を共有させ，これをチェックすることにより不正な複写を防ぐ.

第 5 章

評価実験

5.1　テキストファイルの暗号化と復号

今回の方式で最も問題となる点の一つに復号時間の問題がある．この方式ではファイル全体が部分には別れて全て暗号化されている．これを閲覧する時点で復号しながら閲覧しなければならない．したがって復号速度があまりにも遅すぎるとユーザにとって快適なシステムであるとはいえない．また小型情報端末での使用を考えた場合にはアルゴリズム自体が高速でプログラムサイズの小さい方式である必要がある．そこで，以上の目的に最適な方式である FEAL を採用しコンテンツの暗号化と Viewer で復号しながらコンテンツを閲覧する実験を行った．

5.1.1　実験１

表 5.1　実験環境

項目	規格
CPU	MMX Pentium 300MHz
RAM	64MB
ディスプレイアクセラレータ	NeoMagic MagicGraph 128XD
OS	Windows98
使用言語	Java2 SDK 1.2.2

テキストファイルの一部に暗号化を示すタグを入れることにより Author にて自動的に暗

号化し，Viewer で暗号化された部分が閲覧できない状態と鍵を入力して閲覧できる状態と２つの状態でストレスなく閲覧できるかを確認するため表 5.1 の環境により実験を行った．なお Viewer は applet としウェッブブラウザから閲覧出来るものとした．

1. 実験用 Author にてテキストファイルに暗号化を示すタグを入れタグのついている部分を暗号化する．

図 5.1　テキストデータの暗号化

2. 実験用 Viewer にて暗号まじりのテキストを復号せずに閲覧する．

図 5.2　Viewer による閲覧（1）

3. 実験用 Viewer にて暗号まじりのテキストを復号しながら閲覧する．

図 5.3　Viewer による閲覧（2）

5.1.2　実験２

実験 1 と同じ環境でテキストファイルを全てを段落ごとに Author にて自動的に暗号化し，Viewer でストレスなく閲覧できるかを確認した．

5.1　テキストファイルの暗号化と復号

1. 実験用 Author にてテキストファイルを段落ごとに暗号化する．

図 5.4　テキストデータの暗号化

2. 実験用 Viewer にてテキストを復号しながら閲覧する．

図 5.5　Viewer による閲覧

5.1.3　実験結果

今回の実験機材は現在の水準からすれば処理速度の遅い物であったが，実験１，実験２のどちらの場合においても 800 文字程度の暗号文を復号するのに１秒かからず処理速度に問題はなく，自然に閲覧を行うことできた.

第 6 章

むすび

本論文では CyberBook の本型コンテンツ閲覧システムとしての面のみならず，統合マルチメディア閲覧システムとしての可能性に着目しコンテンツ配信ビジネスに欠かすことのできないセキュリティ機能の付加について検討を行った．近年の急速なモバイル情報端末の発展からみて，大形コンテンツの配信のみならずコンテンツの中の部分的でユーザが必要とする部分にのみ課金することができ，コンテンツをその度に再構成する必要のない今回提案したコンテンツ部分暗号化方式は重要な技術の一部になると考えられる．

今回の研究ではシステムの全体像設計と基本的な技術部分の検証を中心に行なった．研究の途中でワンタイムパスワード認証方式 SAS のセキュリティ向上が必要となり SAS の改良を行い，SAS-K と命名したがこの方式は仕様メモリも少なくモバイル情報端末にも最適の方式でありセキュリティも向上した．また，筆者自身は Java の処理速度に不安を持っていたが今回の研究における実験で予想以上の復号速度が得られた．FEAL の優れたアルゴリズムによるところが多いがこれだけの復号速度が得られれば，Java 内蔵携帯電話において今回検討を行ったシステムを応用して SAS-K を用いてユーザ認証を行い，コンテンツを暗号化して配信し携帯電話で復号して閲覧することも十分可能だと思われる．

今後の課題として今回の実験ではコンテンツ部分暗号化を行った場合に閲覧時間に問題が生じないかという実験と逐次型コンテンツ配信によるユーザ認証実験を行ったが，一体型コンテンツ配信によるユーザ認証実験とサーバにデータベースを導入して課金システムの模擬実験を行う必要がある．また，コンテンツの著作権保護の観点からは暗号化だけではなく電子透かしなどの導入も検討の必要がある部分である．

謝辞

高知工科大学情報システム工学科学科長の寺田浩詔教授を始め指導教員の清水明宏助教授など情報システム工学科の先生方から御指導，御助言をいただき本論分をまとめることができた諸先生方に衷心より感謝申し上げる．

共同研究を行った NTT アドバンステクノロジ (株) の安田哲，真島大介のお二人からは有益な御議論をいただき，その上システム設計資料及び SAS のプログラムまで提供していただいた．御協力に感謝する．

また，クライアントサーバシステムのプログラミングと SAS-K の改良に取り組んでくれた大石恭裕君，Java によるプログラミングを手伝ってくれた三宮秀次君その他，研究室で共にがんばってきた皆さんに心からお礼を申し上げる．

参考文献

[1] 小澤英昭，吉宗俊哉，浜田洋，小川克彦，”ブックメタファ：マルチメディア情報の閲覧における「本」インタフェース ”，画像電子学会 論文，25-5，pp.454-463，1996.

[2] 加藤寿郎，”電子出版の現状 ”，情報処理，39-6，pp.536-539，1998.

[3] 西川秀男，長谷川秀記，高田和彦，前田俊秀，”電子出版の実務－マルチメディア時代のビジネス－ ”，日本エディタースクール出版部，1997.

[4] 富田倫生，”本の未来 ”，株式会社アスキー，1997.

[5] 上野香里，鈴木健也，小澤英昭，”本型ブラウザと紙巻型ブラウザの使い易さの比較 ”，情報処理学会 第 54 回全国大会，54-4，pp.75-76，1997.

[6] 鈴木健也，小澤英昭，外村佳伸，”BookWare：本と本棚メタファによるマルチメディア情報ハンドリング ”，情報処理学会ヒューマンインターフェース研究会，HI72-12，pp.67-72，1997.

[7] 庵祥子，玉井誠，三宅延久，曽根岡昭直，”不正コピー防止を考慮した情報販売方式 ”，マルチメディア通信と分散処理，91-24，1999.

[8] 情報通信セキュリティ技術に関する研究開発プロジェクト，”共通鍵ブロック暗号の選択／設計／評価に関するドキュメント ”，通信・放送機構，2000.

[9] 岡本龍明，山本博資，”現代暗号 ”，産業図書株式会社，1997.

[10] 堀岡力，竹下敦，清水明宏，”課金機能を有する暗号化コンテンツ提供方式 ”，信学技報 OFS，98-1，pp.1-6，1998.

[11] 堀岡力，清水明宏，”暗号化および課金機能を有するコンテンツ提供方式の検討 ”，信学技報 OFS，97-55，pp.7-12，1998.

[12] 宇田隆哉，砂田智，井上亮文，重野寛，松下温，”ソフトウェアベースの音楽配信プラットフォーム ”，情報処理学会論文誌，Vol41，No.8，pp.2237-2245，2000.

[13] 三石大，布川博士，白鳥則郎，宮崎正俊，野口正一，”ネットワーク電子本の提案 ”，情

報処理学会第４８回全国大会，Num4，145-146，1994.

[14] 三石大，布川博士，佐藤究，白鳥則郎，宮崎正俊，野口正一，”コミュニケーションメディアのためのネットワーク電子本の設計 ”，情報処理学会研究報告．データベース・システム研究会報告，Vol.98，pp.105-112，1994.

[15] スコット・モスコウィッツ，”電子透かし ”，セレンディップ，1999.

付録 A

A.1　暗号化アルゴリズム (FEAL)

今回提案しているようなコンテンツ構造であると，コンテンツのいかなる部分を閲覧する場合にも，暗号化されたデータを復号しながら閲覧しなければならない，したがって暗号化アルゴリズムには高速な処理速度が要求される．また，コンテンツを改ざん，盗聴の危険から保護する意味においては十分な暗号強度が必要となる．これらの要求事項に対応できる高

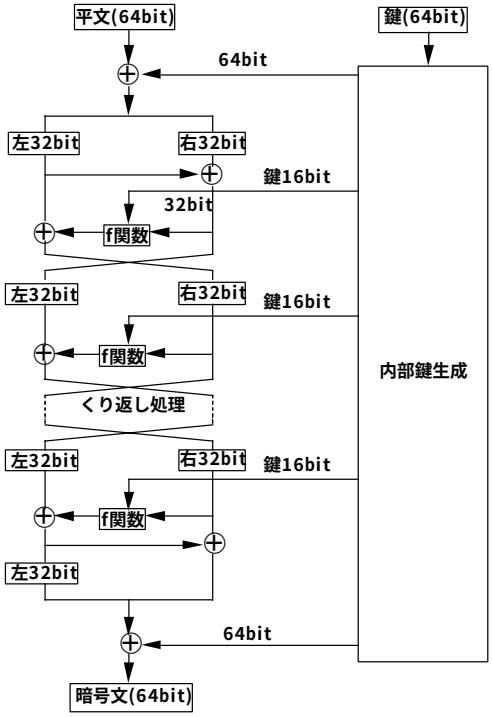

図 A.1　FEAL のアルゴリズム

速暗号化アルゴリズムとして FEAL(Fast Encipherment Algolithm) を採用することとする．FEAL は他の暗号化アルゴリズムに比べ高速で撹拌効率が高い，またプログラムサイズもコンパクトであり今回の目的には最適であると言える．

A.1　暗号化アルゴリズム (FEAL)

FEAL では図 A.1 に示したように入力された平分データを 64bit 単位で 64bit の鍵で暗号化を行い，暗号化された暗号文も 64bit で出力される．

入力された平分データは鍵との EX-OR を取り，左右 32bit づつのブロックに分割される．

f 関数では共通鍵から生成された 16bit の内部鍵と，左右 32bit に分けたデータの EX-OR により計算される．

これらの計算の後に左右のブロックが交換されこれをくり返す．

f 関数（暗号化関数）では入力されたデータは 8bit ずつの４つのブロックに分割され 16bit の内部鍵と図 A.2 のようなあみだ状のデータ撹拌構造によって撹拌が行われる．s 関数では

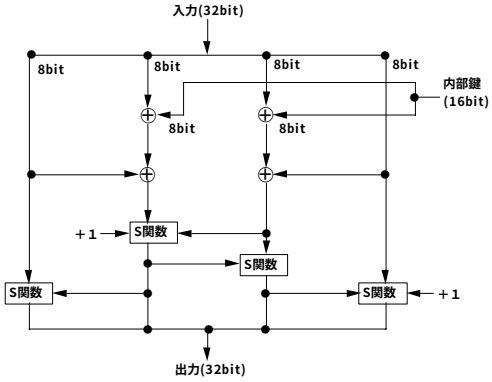

図 A.2　f 関数（暗号化関数）

図 A.3 のように 8bit ずつの加算とデータの 2 ビット左巡回シフトによって演算が行われる．

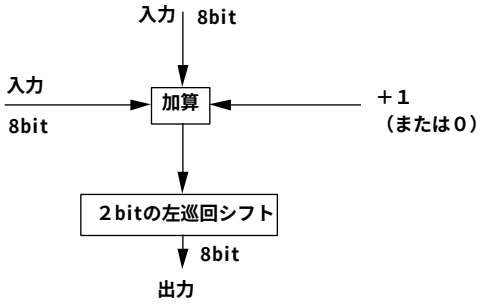

図 A.3　s 関数