平成 12 年度

学士学位論文

# モバイル環境における
# セキュアなコンテンツ流通方式

## A Secure Digital Contents Communication Services in Mobile Environments

1010408　　谷藤喜彦

指導教員　　清水明宏

2001 年 2 月 5 日

高知工科大学 情報システム工学科

# 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

# 目次

# 第 1 章

# はじめに

ブラウザフォン[*1]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．ここでは，物品の取り引きというよりは，画像データや着信メロディ等の音楽データ，占い等のテキストデータ等のディジタルコンテンツが主に取り引きされている．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．

また，インターネット上でコンテンツを送受信しようとした場合，インターネットを流れるデータは第 3 者によって盗聴される危険性があるため，ネットワーク上を流れるデータに対するセキュリティが必要となる．

一般にセキュリティをより強固なものにするほど，通信や各端末の処理に要する負荷が大きくなってしまう．本研究では，それほど処理能力の高くないブラウザフォンを利用するため，端末における負荷が問題となる．

本論文では，ユーザ，コンテンツ提供者，課金管理センタの 3 者間において，安全性が十分でないネットワークを介して，安全に決済を行い，ディジタルコンテンツを流通する方式として，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，ユーザが復号鍵の配信を受けることなく暗号化されたコンテンツ復元用鍵を取得可能な方法を提案し，その安全性と有効性を検討する．

[*1] インターネットアクセス機能付き携帯電話

# 第 2 章

# 研究の背景

## 2.1 モバイル EC 市場の形成

1999 年に火がついた「モバイルとインターネットの融合」．手のひらに乗る小さな携帯電話端末で，インターネットの広大な世界にアクセスできるようになった．この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 EC[*1]市場が活況を呈しており，ビジネスチャンスを探るコンテンツ事業者にも，新たなビジネスチャンスが生まれた．

現在，携帯電話の利用者は約 5,800 万人，PHS のユーザを含んだ移動電話の利用者は約 6,400 万人 (表 2.1，表 2.2 参照)．そのうち 46%，約 3,000 万人がモバイルインターネットの利用者である (表 2.3，表 2.4 参照)．また，携帯電話はほとんどの人が 24 時間，365 日，肌身離さず持っているメディアであるという強みがある．こうしたメディアは他になく，PC インターネット以上に魅力的なメディアであると考えられる．

モバイルとインターネットの融合領域は，携帯キャリアだけでなく個々の利用者とコンテンツを提供するコンテンツ事業者の 3 者がそれぞれに利益を得る市場になりつつある．

## 2.2 コンテンツ事業の現状

コンテンツ事業者がこの市場へ参入する際に，携帯キャリアの提供する公式サイトへ登録する方法と独立系一般サイト向け検索サイトへの登録，及び一般サイトとして参入する方法

[*1] Electronic Commerce：電子商取引

表 2.1　携帯電話：各グループごとの加入者数および総計 (単位：台)

| 事業者名 | 平成 12 年 12 月 | | 平成 12 年 11 月 |
|---|---|---|---|
| | 純増数 | 累計 | 累計 |
| NTT ドコモグループ | 657,000 | 34,218,000 | 33,561,000 |
| au グループ | 197,500 | 10,480,100 | 10,282,600 |
| ツーカーグループ | 43,200 | 3,840,300 | 3,797,100 |
| J-PHONE グループ | 156,700 | 9,468,200 | 9,311,400 |
| 総計 | 1,054,500 | 58,006,600 | 56,952,100 |

(社団法人電気通信事業者協会)

表 2.2　PHS：各グループごとの加入者数および総計 (単位：台)

| 事業者名 | 平成 12 年 12 月 | | 平成 12 年 11 月 |
|---|---|---|---|
| | 純増数 | 累計 | 累計 |
| DDI ポケットグループ | -23,800 | 3,232,400 | 3,256,200 |
| NTT ドコモグループ | 39,000 | 1,728,000 | 1,689,000 |
| アステルグループ | -8,800 | 916,000 | 924,800 |
| 総計 | 6,400 | 5,876,400 | 5,870,000 |

(社団法人電気通信事業者協会)

が考えられる.

### 2.2.1　公式サイト

コンテンツ事業者がアクセス数を増やそうとする場合，まず考えるのが公式サイトへの登録である．公式サイトであれば，料金回収代行システムを持ち，ビジネスモデルも立て易

表 2.3　携帯電話：インターネット接続サービス契約数 (単位：台)

| サービス名 | 平成 12 年 12 月 | | 平成 12 年 11 月 | グループ名 |
|---|---|---|---|---|
| | 純増数 | 累計 | 累計 | |
| i モード | 1,751,000 | 17,161,000 | 15,410,000 | NTT ドコモグループ |
| EZweb | 590,700 | 5,168,900 | 4,578,200 | au グループ<br>(12 月末累計:4,282,300)<br>ツーカーグループ<br>(12 月末累計: 86,600) |
| J-sky | 494,200 | 4,462,400 | 3,968,200 | J-PHONE グループ |
| 総計 | 2,835,900 | 26,792,300 | 23,956,400 | |

(社団法人電気通信事業者協会)

表 2.4　PHS：インターネット接続サービス契約数 (単位：台)

| サービス名 | | 平成 12 年 12 月 | | 平成 12 年 11 月 |
|---|---|---|---|---|
| | | 純増数 | 累計 | 累計 |
| DDI ポケット | H” LINK | 0 | 2,480,000 | 2,480,000 |

*NTT ドコモグループ、アステルは利用者数未公開

(社団法人電気通信事業者協会)

く，カテゴリ分類されたキャリア・ポータルのメニューから簡単にアクセスできるため，このメニューを全てのユーザが必ず通過するための広告といった手段は不要になる．

しかし，公式サイトへの登録においては，内容に対する審査が厳しく，公認に要する検討期間も長いため，経営基盤が弱くアイデアだけで勝機を伺うベンチャー企業にとっては，アイデアが盗用されてしまうのではといった不安がつきまとう状況にある．そして，一部のコ

ンテンツ事業者からは「携帯キャリアのハードルの高さはインターネットではない.」との声もあり，公式サイトへの登録は企業でないと厳しい状況にあることが伺える.

また，いくらビジネスモデルが立て易いとはいっても，現状の料金徴収代行システムの場合，例えば月額 300 円などといった月々の定額料金のため，ただ一度だけ利用したい人の購買意欲を失わせることにもなりかねず，利用者の立場を考慮した場合，利便性の高いシステムであるとは言いがたい.

### 2.2.2　一般サイト

現在，圧倒的なシェアを誇る i モード[*2]の場合，公式サイトが約 1,400 であるのに対して，約 32,000 もの一般サイトを抱えている．さらに，独立系サイト向け検索エンジンには約 20,000 サイトが登録されており，無数の独立系コンテンツが増殖し，それぞれに進化しはじめている．図 2.1 に示すように，公式サイトのみを利用するユーザは 37%にとどまり，それ以外の約 60%のユーザは一般サイトを利用していることになる．すでに一部のユーザにとっては，公式サイトよりもまず独立系一般サイト向け検索エンジンへ行ったり，併設されているディレクトリ型メニューを利用する動きがあり，公式サイト以上のポータルサイトへと成長する可能性は否定できない状況にある.

しかし，人気ページへの成長を目指す独立系一般サイトにおいては，決済手段が問題視され，情報量や物品の代金を回収するための決済システムの実現を求める声が高く，新規参入を伺うコンテンツ事業者にとってこれが一番のネックとなっている.

ようやく本年年頭より，表 2.5 に示すような，クレジットカード決済や，固定電話料金と一括して料金回収するシステムやプロバイダによる料金回収代行システムといったブラウザフォン向けの課金システムが運用され始め，ビジネスモデルが立て易くなり始めた.

[*2] NTT ドコモが，1999 年 2 月から提供を始めた携帯電話による文字情報サービスのこと.


図 2.1　携帯電話単体での公式サイトとそれ以外のサイトの利用状況

## 2.3　モバイル EC における決済手段

2.2.2 小節で述べたように，本年年頭よりブラウザフォン向けの課金システムが運用され始めた．しかし，これらには，以下に示すさまざまな問題点がある．

まず，ISP[*3]料金と一括で回収するシステムの場合，図 2.2 に示すように，携帯電話・PHS で EC を利用したい人のうち 75.2%は，自宅のパソコンでインターネットを利用していない人であること．固定電話の料金と一括して請求するシステムでは，現在，携帯電話の利用者数が固定電話の利用者数を上回っていることにも象徴されるように，必ずしも携帯電話の利用者が固定電話を契約しているとは限らないことなど，両者とも利便性の高いシステムであるとは言いがたい．

そこで， 本節では，モバイル EC に適応できる決済方法について考察する．

ブラウザフォンは PC と比較すると，メモリ容量や画面サイズなどの機能が限定されているため，モバイルインターネットで流通されるコンテンツは，ディジタル化された音楽や，画像，電子新聞などの情報の切り売りなど，小単位で小額のコンテンツが売買されることが考えられる．しかも，携帯電話の利用シーンは，屋外での短時間の利用が多く，PC の利用

[*3] Internet Service Provider

表 2.5　料金回収代行システムの例とその概要

| システム名 | 当事者名 | 概要 |
|---|---|---|
| ¥楽 (えんらく) | 株式会社オン・ザ・エッヂ | 音声回線を併用した，モバイル専用クレジットカード決済システム. |
| IP SQUARE | 株式会社 コムスクエア | 音声回線を併用した認証システムを持つクレジットカード決済の課金システム. |
| mobile@nifty | ニフティ株式会社 | 料金はニフティがプロバイダ料金と一括で回収する課金システム. |
| カルレ | NTT コミュニケーションズ株式会社 | ユーザーがインターネット上で購入したコンテンツなどの料金を，東西 NTT の電話料金と一緒に請求する料金回収代行サービス. |

シーンとは異なっているため，欲しい時に欲しいものだけを購入するという，「ペイ・パー・ビュー」，「ペイ・パー・クリック」を実現することが期待されている [4].

ブラウザフォンにおける決済方法には，以下のものが考えられる.

1. 金融機関経由の振り込み
2. クレジットカード決済 (後払い)
3. 電子現金 (即時払い)
4. プリペイド決済 (前払い)

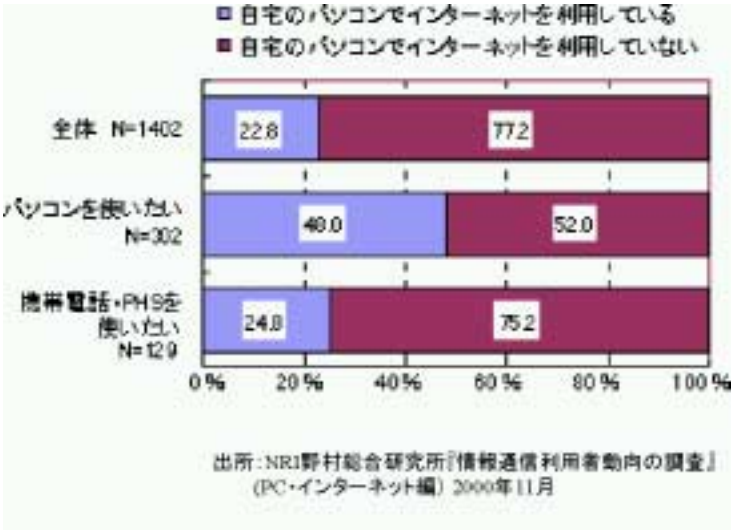


図 2.2　パソコンや携帯電話・PHS で EC を利用したい人の特徴

1 の場合，金融機関への振り込み確認を待つのでは，「手軽に，素早く，どこでも」というブラウザフォンのコンセプトからあまりにもかけ離れており，ユーザの支持が得られない可能性がある．

2 のクレジット決済は，現在，電子商取引の決済手段として最も普及しており，表 2.5 に示されるようなシステムが，本年年頭より運用されている．しかし，クレジットカードを受け付ける店舗は，クレジットカード会社に対して，加盟店手数料として売り上げ金額の数%を支払う必要があるなど，ディジタルコンテンツのような小額商品の売買にはクレジットカードによる支払いでは手数料が高く，コンテンツ事業者が利益を上げることが困難となる．

3 の電子現金を利用した決済では，ネットワーク上を電子現金の情報そのものが流れる場合があるため，より強固なセキュリティが必要となる．しかし，セキュリティを強固なものにすると，端末での処理負担が大きくなるという問題がある．

これらに対して，4 のプリペイド決済では，ユーザが予め，ネットワーク上でのみ利用可能な購入資格を取得するため，コンテンツの購入の際に現金情報がネットワーク上を流れることがなく，プリペイドカード購入時などで生じる手数料も低くおさえることが可能であり，数円〜数百円単位の小額決済に有効である [2].

## 2.4　コンテンツ流通システム

現状のブラウザフォン向けの課金システムでは，コンテンツの提供部分は，コンテンツ事業者のシステムと密接に関係するため，コンテンツ事業者にて管理すべきものであり，ユーザ認証，課金認証等を行なう認証業者では対応不可である（ただし，コンテンツ提供サーバを認証業者が提供する場合については対応可能）という認識のもと，ユーザとコンテンツの提供部分が分離して考えられていることが多く，ユーザ，および課金認証に関する安全性は運用面で補われている．このような状況において，コンテンツ提供に関する安全性は保証されているとは言いがたい．

また，図 2.3 に示すように，この 2 年間で EC を利用する際に，個人情報 (自分に関するデータ) が洩れることに不安を抱く人の割合が上昇している．依然として，思い通りの商品が届かないことに不安や障害を感じる人の割合が高い状況にある．さらに，自分が注文していない商品が届いて，代金を請求される可能性があるという人の割合も高い．課金機能を有するコンテンツ流通では，安全で確実なコンテンツ提供と決済を行うことが不可欠である．

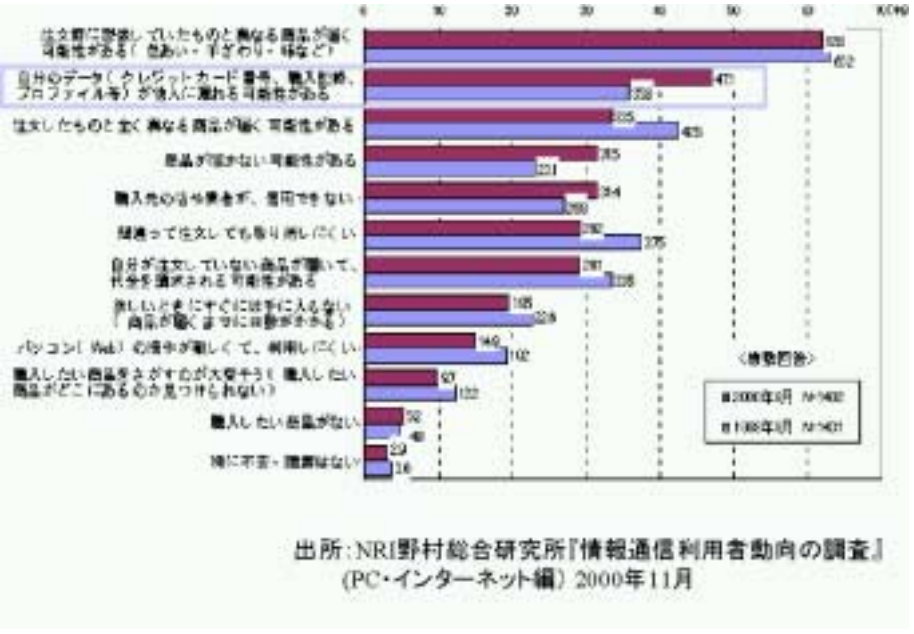


図 2.3　EC を利用する際に感じる不安や障害

一般的に，インターネット等の安全性が十分保証されていないネットワークでは，盗聴を容易に行うことが可能であるため，ユーザの正当性を証明するデータ (認証データ) や， 提供するコンテンツ自体に対する暗号化が不可欠である．しかし，現状では，通信プロトコルレベルでセキュリティを強化したものや，端末にある程度の処理能力を要する公開鍵暗号方式を用いたものが多く，この場合，利用可能な端末が制限されてしまう可能性がある．そのため，処理能力の低いブラウザフォンにおける，コンテンツ提供に関する安全性を高めるためには，既存通信プロトコルを用い，比較的処理が軽く，アプリケーションレベルでのセキュリティを強化したものが必要であると考えられる [3].

コンテンツを取り引きする場合，買い手はどのコンテンツが自らの要求に合うのか内容が分からないと安心して購入できない．売り手はディジタル化されたコンテンツの違法なコピーを防止するため，正当な支払いを得るまではコンテンツそのものを利用者に渡すことは避けたい．この売り手，買い手双方の相反する取引抑制要因があり，内容を提示しかつ確実な取引が可能なメカニズムが望まれている [5].

そこで，これを満たす技術として半開示技術 [6] があり，これを用いた情報流通プラットフォームとして，Infoket がある [7]．以下に，半開示技術，および，情報流通プラットフォーム Infoket の概要を示し，モバイル環境へ適応性を検討する．

### 2.4.1　半開示技術

静止画，動画，音声等のコンテンツを安全に流通するための仕掛けとして，半開示技術がある．この方法は，概要が理解できる程度に品質を劣化させた半開示コンテンツを用いて，コンテンツを流通させ，購入時にコンテンツ情報を復元することにより，流通過程における不正コピーを防止することができる．また，コンテンツの一部を半開示することにより，情報提供者が商品を宣伝したり，利用者が購入の前にコンテンツを評価するのに使用できる．

### 2.4.2　情報流通プラットフォーム Infoket

情報流通プラットフォーム Infoket とは，購入者が先に暗号化されたディジタルコンテンツを取得し，その後決済を行うと同時に復号鍵を入手する鍵配送型情報販売方式のプラットフォームである．現在は，インターネット上を基盤としてさまざまな情報の販売を行っている．

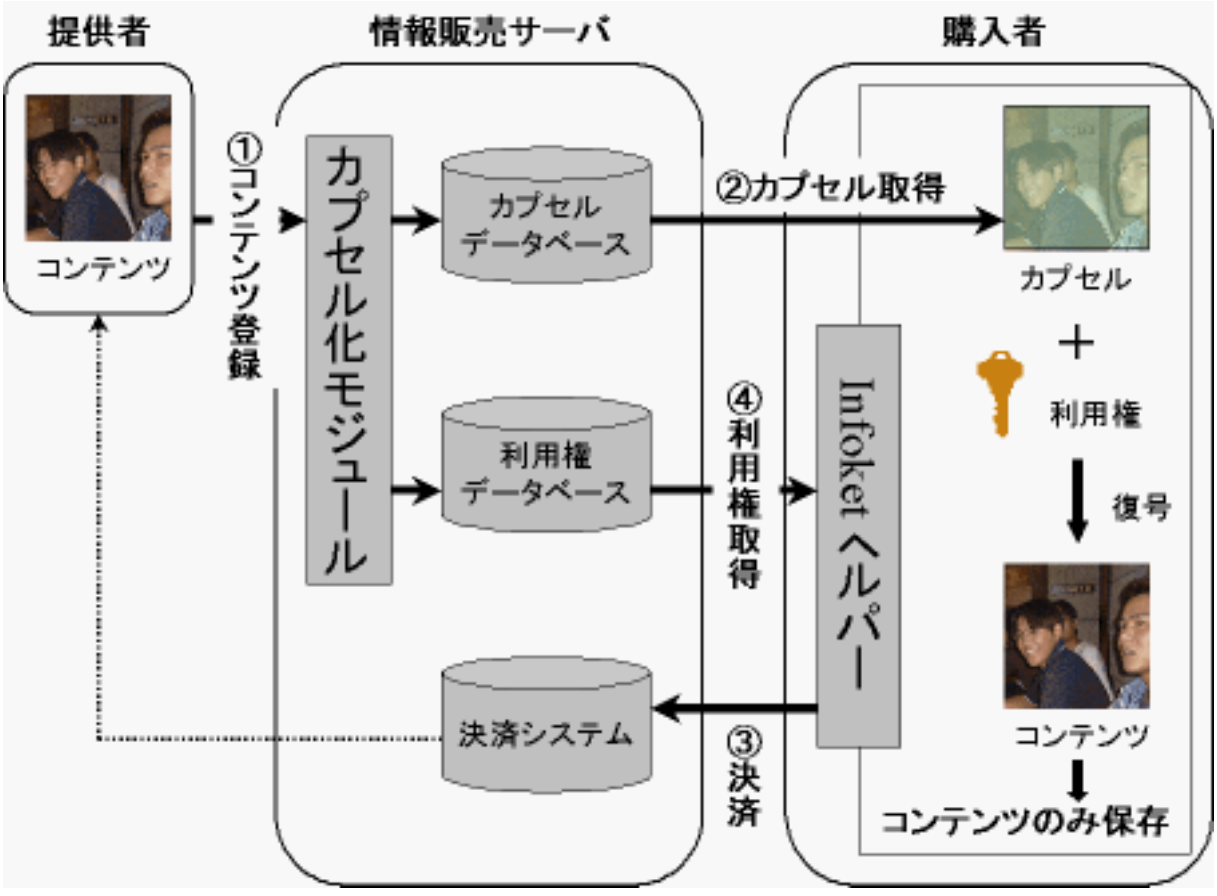


図 2.4　infoket 構成図

Infoket は，図 2.4 に示すように，ディジタルコンテンツの販売者 (販売端末)，情報販売サーバ (カプセルデー タベース，利用権データベース，決済システム)，購入者 (購入端末) から成り立つ．販売者は，販売するディジタルコンテンツを情報販売サーバに登録する．登録されたコンテンツはカプセル化モジュールによって電子署名や利用権サーバのアドレス等

の情報を付加して暗号化し，カプセル化される．そして，カプセル化したコンテンツはカプセルデータベースへ，カプセル化時に利用した復号鍵を利用権として利用権サーバにそれぞれ保存する．

購入者はカプセル化コンテンツをインターネットや CD-ROM 等を経由して入手し，購入端末に保存する．さらに決済処理を行って利用権を利用権サーバから入手する．そして，この利用権と先に入手したカプセル化コンテンツを Infoket ヘルパーを用いて復号し，復号したディジタルコンテンツのみを購入端末に保存して利用する．

この Infoket システムの場合，公開鍵暗号方式を用いた電子署名や秘密通信プロトコルを使用しており [8]，処理能力の低いブラウザフォンでの利用は困難である．

# 第 3 章

# セキュアコンテンツ流通方式

本章では，モバイル上の，ユーザ，コンテンツ提供者，課金管理センタの 3 者間で，プリペイド決済方式による課金機能を有し，安全性が十分でないネットワークを介して，安全にコンテンツを流通させる方式として，鍵配送型コンテンツ流通方式を提案する．

本方式では，流通させるディジタルコンテンツを，可逆性のある半開示暗号化し，それ自体は無料で提供する．その半開示暗号化コンテンツを取得した利用者が，オリジナル版のコンテンツを購入する際には，半開示を解くための復号鍵 (以下，利用権) を取り引きする．

以下に，本方式のシステム構成，事前登録，コンテンツ購入手順について述べる．

## 3.1 システム構成

本システムは，課金管理センタ，コンテンツ提供者，ユーザの 3 者で構成される．

課金管理センタは，ユーザに対してユーザの与信照会を行ったり，使用可能限度額等を管理する課金情報管理機関である．さらに，正当なユーザ，つまり購入資格を有し使用可能限度額がコンテンツ価格を上回っていると判断できる場合に，ユーザに対してコンテンツの利用権を配信する，利用権管理機関でもある．課金管理センタでは下記のデータを管理する．課金管理センタではユーザの個人情報を管理しない．

- ユーザに関するデータベース (User-DB)
  - ユーザ ID 番号　$\cdots\cdots$　$U_{ID}$
  - 認証データ　$\cdots\cdots$　$Au$
  - 使用可能限度額　$\cdots\cdots$　$U_{sum}$

  - 購入履歴 (前回購入したコンテンツ ID 番号)　……　$L - C_{ID}$

- コンテンツ提供者に関するデータベース (Provider-DB)
  - コンテンツ提供者 ID 番号　……　$IP_{ID}$
  - パスワード　……　$IP_{pass}$
  - 利用者の使用額分を移すための口座　……　$IP_{gain}$
- コンテンツデータベース (Contents-DB)
  - コンテンツ ID 番号　……　$C_{ID}$
  - コンテンツ価格　……　$C_{price}$
  - コンテンツ利用権　……　$C_{key}$

コンテンツ提供者は，オリジナルのディジタルコンテンツを半開示暗号化し，ユーザからの閲覧，及びダウンロードを可能にすると共に，下記のデータを安全な方法で課金管理センタに登録し，コンテンツ利用権の販売を依頼する．

- コンテンツ番号
- コンテンツの利用権 (復号鍵)
- コンテンツ価格

ユーザは，課金管理センタからコンテンツ購入資格を取得し，コンテンツ提供者からインターネットを介して半開示暗号化されたコンテンツを閲覧，取得する．オリジナルコンテンツの購入を希望した場合のみ，課金管理センタにコンテンツ利用権の購入を依頼し，利用権を取得する．

## 3.2　事前登録

本節では，コンテンツ提供者，ユーザ，各々の事前登録について述べる．

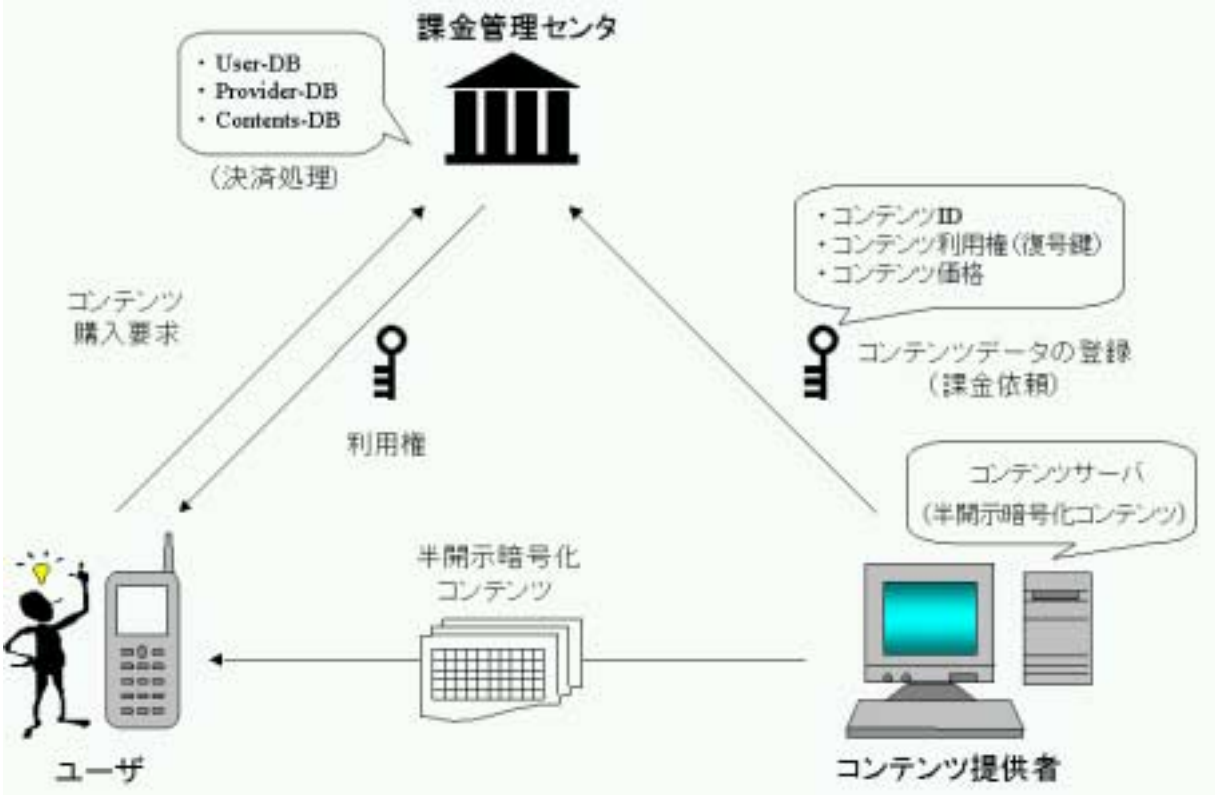


図 3.1　システム構成

### 3.2.1　コンテンツ提供者

コンテンツ提供者は，コンテンツ暗号化鍵 $K_{ID}$ を生成する．所有するオリジナルコンテンツ $C$ を $K_{ID}$ を用いて半開示暗号化し，コンテンツ復号鍵 (以下，利用権)$K_{ID}$ をコンテンツ ID 番号 $C_{ID}$，コンテンツ $C_{ID}$ の価格 $C_{ID-price}$ と共に安全な方法で課金管理センタに登録する (図 3.2 参照).

### 3.2.2　ユーザ

本方式において用いる，プリペイド決済方式におけるコンテンツ購入資格の取得方法として，銀行口座への振り込み，プリペイドカードの購入や情報料回収代行サービスの利用などがあげられる [2]．ユーザは，これらの手続きと共に，ユーザ ID 番号 A とパスワード S を

## 3.2　事前登録

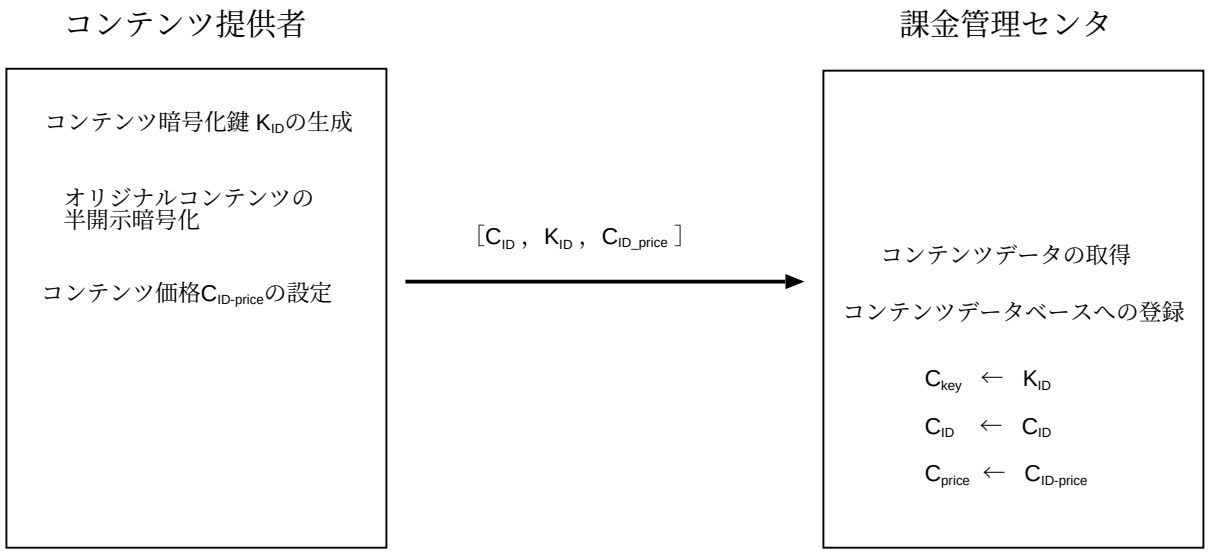


図 3.2　コンテンツ提供者による事前登録

基に，初回余信照会に用いる初回認証データ $E_0^2$ を算出し，課金管理センタにユーザ ID 番号 A と使用可能限度額 $U_{money}$ と共に登録する (図 3.3 参照).

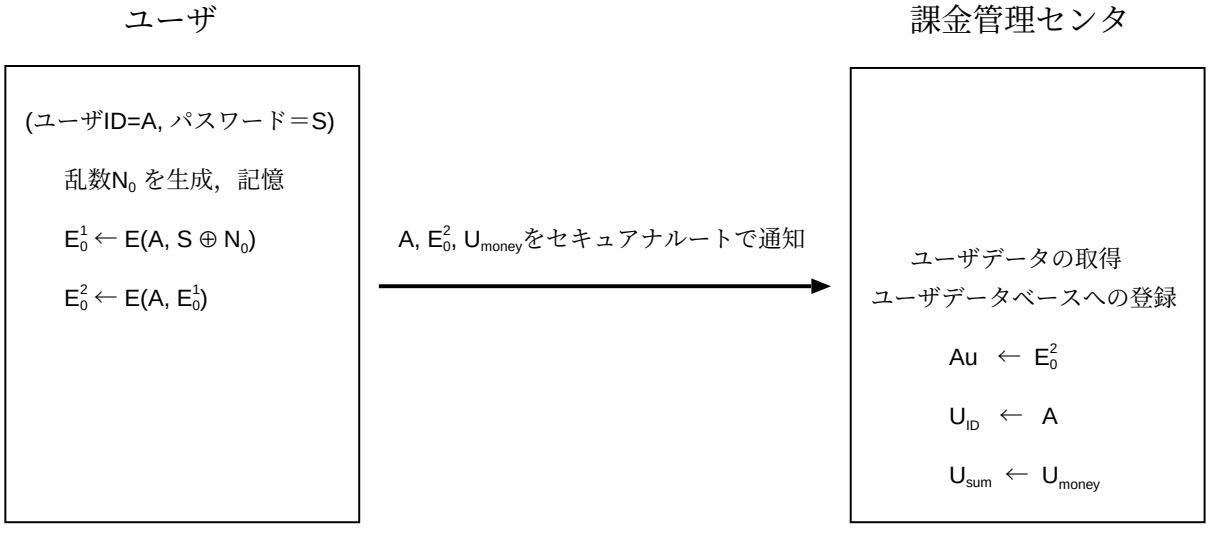


図 3.3　ユーザによる登録

## 3.3　コンテンツ購入手順

本節では，コンテンツの購入に関する一連の手順について述べる (図 3.5，図 3.6 参照).

### 3.3.1　コンテンツ閲覧，および取得

ユーザは，コンテンツ提供者の持つコンテンツサーバに対して，コンテンツの検索に行く．コンテンツサーバには，半開示暗号化されたコンテンツが置いてあり，この時点で，コンテンツの閲覧，取得が可能である．取得したコンテンツは制限付き (半開示状態) で利用可能であり，使用料は無料である (図 3.4 参照).

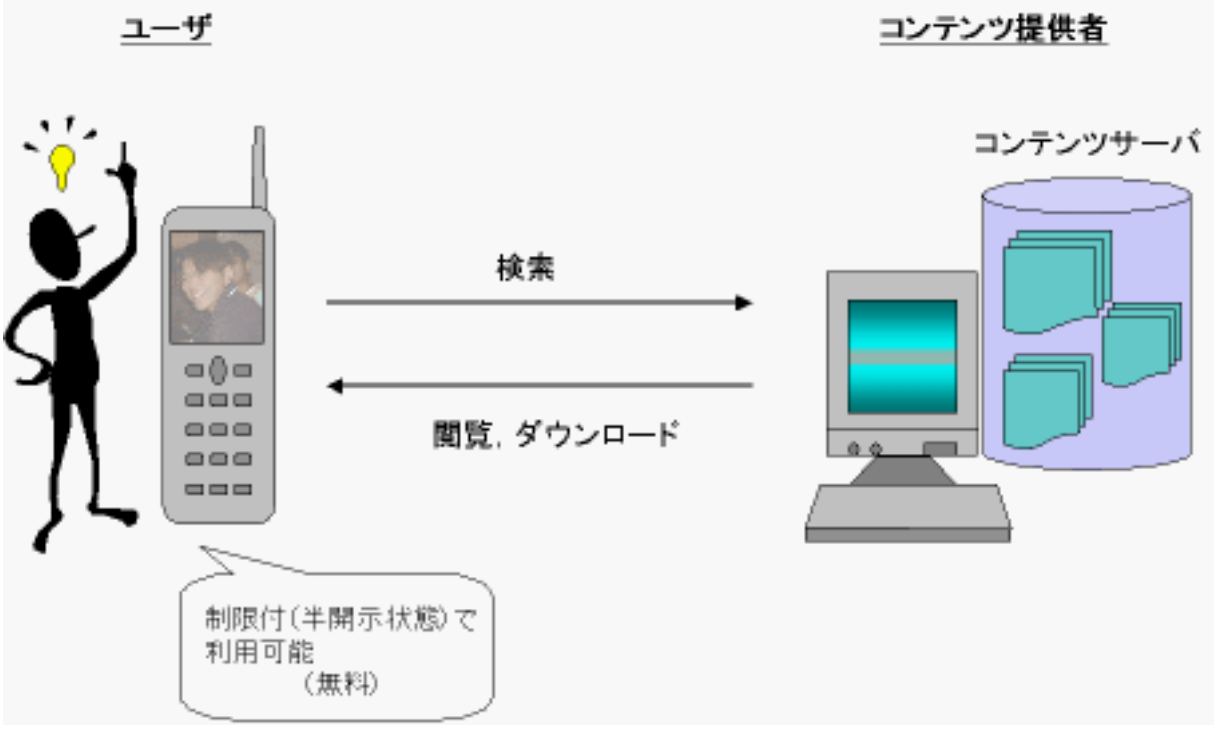


図 3.4　コンテンツの検索と取得

### 3.3.2　余信照会

ユーザは半開示暗号化コンテンツ取得時，もしくは取得後，オリジナルコンテンツの購入を希望した場合，当研究室で研究開発を進めている SAS-K パスワード認証方式 (付録 A 参照) を用いて認証を行う．SAS-K パスワード認証方式では，共通鍵暗号方式 FEAL(付録 B 参照) を一方向性関数に用いている．

まず，ユーザはユーザ ID 番号 $A$ とパスワードを基に，今回 (k 回目) の与信照会で用いる認証データを算出する．式中の”E”は一方向性関数による暗号化を示し，”$\oplus$”は排他的論理和，$N_k$ は k 回目の認証時に生成する乱数を示す．

$$E_k^1 = E(A, N_k \oplus S)$$

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

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

$$E_{k-1}^1 = E(A, N_{k-1} \oplus S)$$

$$E_{k-1}^2 = E(A, E_{k-1}^1)$$

$$E_{k-1}^1 \oplus E_{k-1}^2 \oplus E_k^3 \tag{3.1}$$

$$E_k^2 \oplus E_{k-1}^2 \tag{3.2}$$

また，算出したデータで，課金管理センタに登録されてある認証データ $E_{k-1}^2$ を鍵として，購入を希望するコンテンツ ID 番号 $C_{ID}$ を暗号化し (3.3)，ユーザ ID 番号 $A$，認証データ (3.1，3.2) と共に課金管理センタへ送信する．

$$E_{k-1}^2 \rightarrow E(C_{ID}, E_{k-1}^2) \tag{3.3}$$

課金管理センタは，保持している認証データ $Au = E_{k-1}^2$ を用いて，ユーザから受信した認証データの検証を行う．式中の”cmp”は比較を示す．

$$(E_k^2 \oplus E_{k-1}^2) \oplus Au = Au'$$

$$X = E(A, Au')$$

$$(E_{k-1}^1 \oplus E_{k-1}^2 \oplus E_k^3) \oplus X \oplus Au = Y$$

$$Z = E(A, Y)$$

$$Au \quad cmp \quad Z$$

ユーザの正当性が証明され，認証が成立した場合，Au' をユーザ $A$ の新しい認証データ (次回認証データ) $Au = E_k^2$ として記憶する．

ユーザ認証成立後，次のように決済処理を行う．

まず，ユーザから受信したデータの中からユーザの希望するコンテンツ ID 番号を算出する．ユーザ認証が成立した際の認証データ $E_{k-1}^2$ を用いて，受信した暗号化されたコンテンツデータ $E(C_{ID}, E_{k-1}^2)$ を復号し，コンテンツ ID 番号を取得する．

$$E(C_{ID}, E_{k-1}^2) \rightarrow C_{ID}$$

もし，暗号化されたコンテンツ ID 番号を復号できない場合は，配送途中で何らかのエラーが発生したものとみなし，ユーザに対してエラーメッセージを送信する．

次に，取得したコンテンツ ID 番号と Contents-DB に保存されてある，前回購入したコンテンツ ID 番号 $L - C_{ID}$ とを比較する．

$$L - C_{ID} \quad cmd \quad C_{ID}$$

一致した場合は，ネットワークの不調等により利用権が正しくユーザに配信されなかったとみなし，決済処理を行わずに利用権を配信する．一致しなかった場合は，ユーザ A の使用可能額が，コンテンツ ID 番号のコンテンツ価格を上回っているかどうかを確認する．

$$U_{sum} \quad > \quad C_{ID-price}$$

ユーザの使用可能額がコンテンツの価格を上回っていると認められた場合は，ユーザの使用可能額から，コンテンツ価格分がコンテンツ提供者の口座に振り替えられる．上回っていない場合は，購入不可のエラーメッセージをユーザに返す．

$$U_{sum} \ = \ U_{sum} \ - \ C_{ID-price}$$

$$IP_{gain} \ = \ IP_{gain} \ + \ C_{ID-price}$$

### 3.3.3　利用権の配送

決済処理終了後，課金管理センタは，$C_{ID}$ に対応する利用権 $K_{ID}$ を検出する．ユーザ認証が成立した際の認証データ $E^2_{k-1}$ を暗号化鍵として，利用権 $K_{ID}$ を暗号化し，ユーザに配信する．

$$E^2_{k-1} \ \rightarrow \ E(K_{ID}, E^2_{k-1})$$

その後，購入履歴 $L - C_{ID}$ に $C_{ID}$ を記憶する．

$$L - C_{ID} \ \leftarrow \ C_{ID}$$

ユーザは，コンテンツ購入要求時に算出した認証データ $E^2_{k-1}(3.1)$ を用いて，課金管理センタから受信した $E^2_{k-1} \ \rightarrow \ E(K_{ID}, E^2_{k-1})$ を復号化し，利用権を取得する．

$$E(K_{ID}, E^2_{k-1}) \rightarrow K_{ID}$$

先に取得しておいた半開示暗号化されたコンテンツに対し，取得したコンテンツ利用権 $K_{ID}$ を用いてコンテンツを復号し，オリジナルコンテンツを取得する．

$$E(C, K_{ID}) \ \rightarrow \ C$$

もし，暗号化された利用権を復号できない場合は，配送途中で何らかのエラーが発生したものとみなし，再度課金管理センタに向けて購入要求を行なう．

## 3.3 コンテンツ購入手順

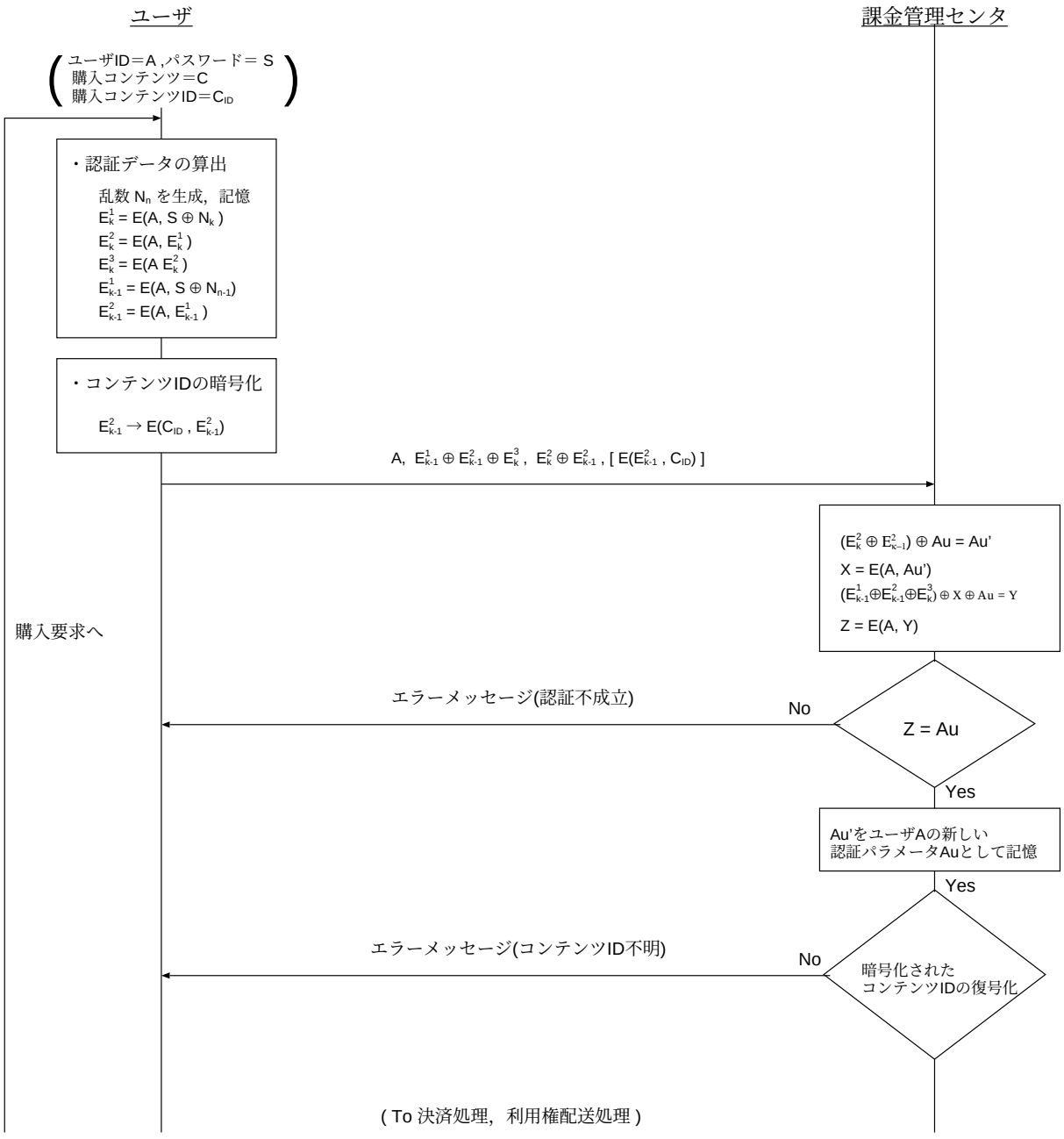


図 3.5　コンテンツ購入手順 (ユーザ・コンテンツ ID 認証)

## 3.3 コンテンツ購入手順

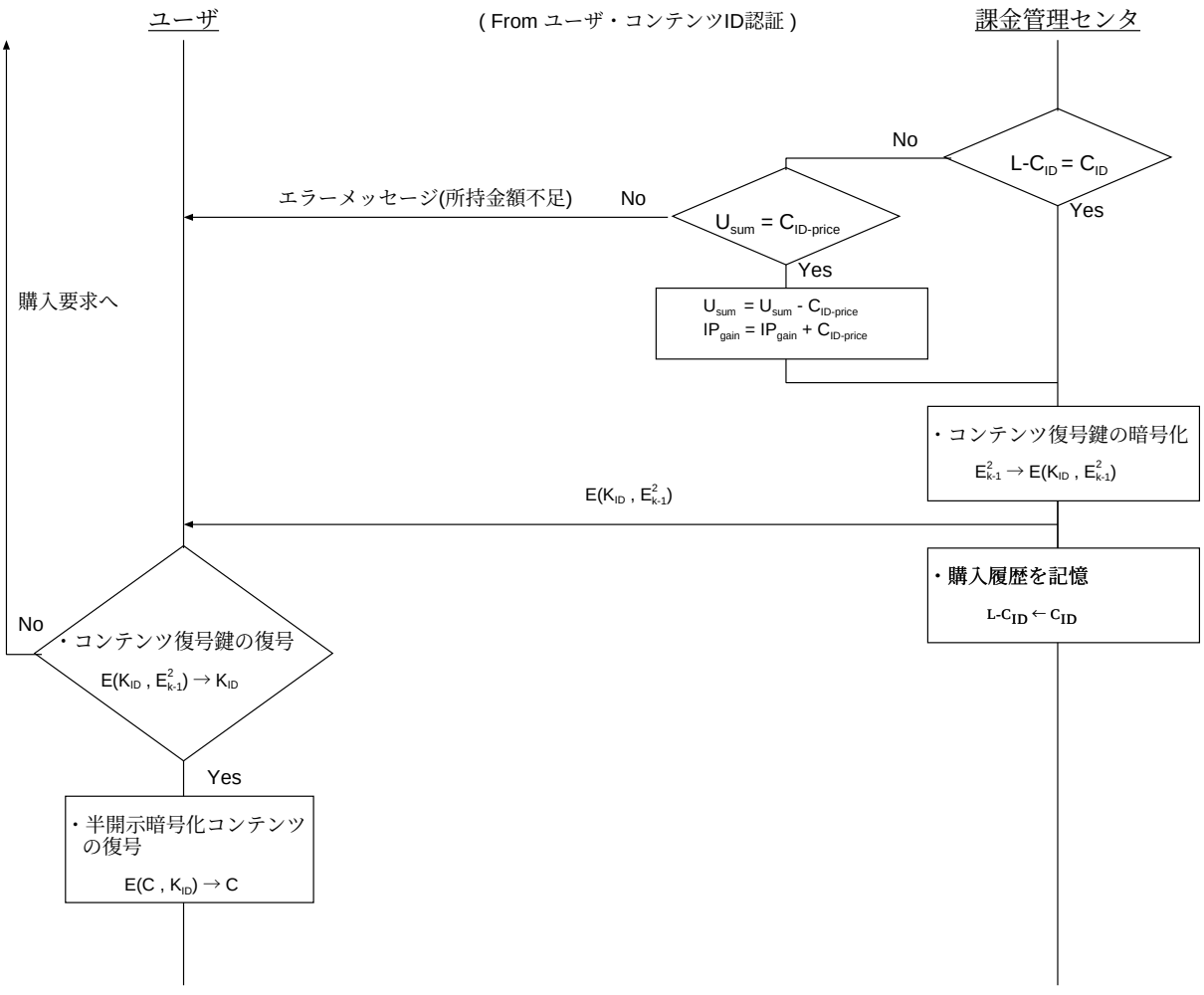


図 3.6　コンテンツ購入手順 (決済処理，利用権の配送処理)

# 第 4 章

# 考察

本方式では，モバイル上の，ユーザ，コンテンツ提供者，課金管理センタの 3 者間で，プリペイド決済方式による課金機能を有し，安全性が十分でないネットワークを介して，安全にコンテンツを流通させる方式を提案した．本章では，本方式の安全性と有効性について考察する．

## 4.1 決済処理に関する安全性

### 4.1.1 課金情報

本方式で用いた，プリペイド決済方式では，ユーザの資格認証後，課金管理センタで利用可能額から実際の利用額を差し引くだけでよいため，インターネット上を現金情報そのものが流れないという点で安全である．

ただし，ユーザの情報管理ミス等によりパスワードが漏洩し，ユーザの知らない間に課金された場合に備え，サービス利用，直ちに課金されたことをユーザに通知する仕組みが必要である．

### 4.1.2 不当請求

コンテンツ提供者のアカウントへユーザの利用額分を振り替える際に，利用権を取得したにもかかわらず，ユーザが振り替えを拒否する可能性があるが，本方式では，決済処理を行なった後に利用権の配送を行なうことで対処している．しかし，配送途中に，ネットワーク

の不調などによって，利用権が正しくユーザに配信されない可能性があり，不当に請求する可能性がある．それに対しては，課金センタにある User-DB に前回購入履歴を保存し，決済処理の際に，今回購入するコンテンツと前回購入したコンテンツを照合し，一致した場合は決済処理を行なわないことで対処する． しかし，必ずしも同じコンテンツを連続して購入要求を行なうことは保証できない．そのため，それ以前の履歴を残して対処するのか，その他の運用面で対処するのかについては，今後検討が必要である．

## 4.2　コンテンツ購入に関する安全性

本方式では，比較的処理能力の低いブラウザフォンを考慮して，ユーザ認証には，共通鍵暗号方式 FEAL を一方向性関数に用いた SAS-K パスワード認証方式を用いている．

本方式の大きな特徴として，購入要求時のコンテンツ ID 番号と利用権の配送時に行なう暗号化・復号鍵に，ユーザ自身が算出したユーザ認証に用いる，今回認証データを利用することにより，暗号化されたコンテンツ ID 番号と利用権の復号鍵をわざわざ取得する必要がない点があげられる．

また，利用権の暗号化・復号鍵には，SAS-K パスワード認証方式を用いてワンタイム性を有する認証データを用いているため，異なるユーザが同じコンテンツの購入を要求した場合でも，取得した暗号化された利用権は異なり，正当なユーザのみコンテンツを利用することが可能である．

### 4.2.1　購入要求

コンテンツの購入を希望した際，ユーザは保持しているユーザ ID 番号とパスワードを基に認証データを算出する．そして，今回認証データを暗号化鍵として用い，購入を希望するコンテンツ ID 番号を暗号化し，認証データの排他的論理和を取ったものと共に課金管理センタに送信する．ユーザの正当性が証明されると同時に復号鍵を共有し，暗号化されたコンテンツ ID 番号は復号される．もし，復号できなかった場合は，配送途中で第 3 者にすり替

えられたことが発覚し，コンテンツの購入に関する処理は行なわれず，ユーザに対してエラーメッセージを送信する．このように，本方式を用いることで，ユーザの正当性が認証されると同時に希望するコンテンツも明確になる．

### 4.2.2　利用権の配送

購入要求時と同様に，ユーザと課金管理センタで共有している今回認証用データを暗号化鍵として，利用権を暗号化して送信する．ユーザは受け取った暗号化された利用権を，保持している今回認証用データを用いて復号する．復号化が可能な場合は，利用権を取得しオリジナルコンテンツを復元することができる．しかし，復号できない場合は，配送途中でエラーが発生したことを意味する．この際，エラーメッセージを課金管理センタに送信するのではなく，再度購入要求を行なう． 本方式では決済処理を行なう際に，前回購入履歴に保存されてあるコンテンツ ID 番号と今回購入を希望するコンテンツ ID 番号が一致した場合は，前回同じコンテンツの購入を要求しており，配送途中で何らかのエラーが発生したものとみなし，決済処理は行なわれずに利用権の配送を行なう．

## 4.3　本方式の有効性

本方式は，半開示技術を用いているため，図 4.1 に示すように，現在ブラウザフォンで利用率の高い，着信メロディや画像のような，比較的静的なコンテンツの取引きを考慮した方式である．この場合，半開示暗号化することで，不正コピーの心配なしにコンテンツの宣伝をすることが可能である．これにより，利用者の購買意欲を高めることができ，更なるコンテンツ提供者の収益を高める要因ともなりうる．

一方で，ニュースや天気予報などのリアルタイムな情報を，いちいち暗号化して，暗号化されたコンテンツが流通してからでないと使用できないとなると，情報としての価値が下がってしまう．よって，本方式の適応は困難である．

今後，これらのリアルタイムな情報のセキュリティを確保したコンテンツ流通方式につい

て検討を行なう必要がある．

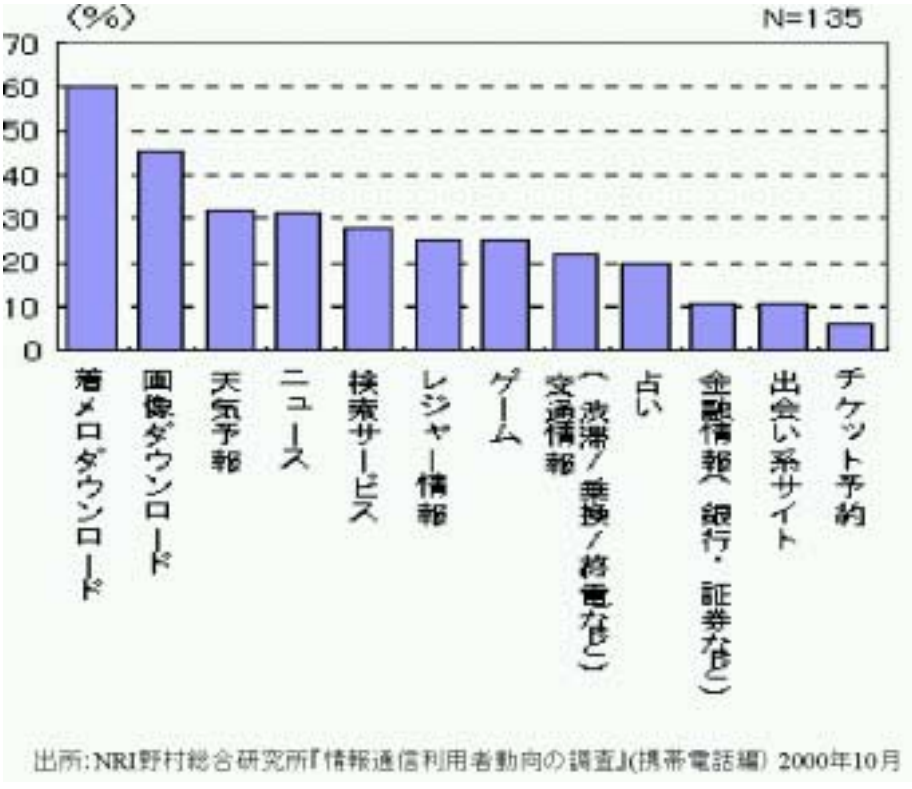


図 4.1　ブラウザフォン単体で閲覧するコンテンツの種類

# 第 5 章

# おわりに

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，コンテンツ提供者がユーザ に，オリジナルコンテンツから，可逆性のあるスクランブルコンテンツと復元のための鍵情報を生成し，安全にコンテンツを流通させる方式を提案した．

本方式では，利用権の取り引き時に，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，鍵配送を満たすプロトコルを設計した．認証に用いた今回認証データを利用することにより，暗号化された利用権の復号鍵をユーザが取得する必要がない．また，利用権の暗号化・復号鍵には，SAS-K パスワード認証方式を用いているため，異なるユーザが同じコンテンツの購入を要求した場合でも，取得した暗号化された利用権は異なり，正当なユーザのみコンテンツを利用することが可能で，利用者からの対価支払いも保証できる．

今後の課題として，本方式を実装しユーザの利便性を考慮した決済処理について評価，検討する必要がある．また，半開示暗号化アプリケーションとユーザ端末におけるビューワを開発する必要がある．さらに，天気予報やニュースなどのリアルタイムな情報のセキュリティを確保したコンテンツ流通方式について検討を行なう必要がある．

# 謝辞

本学情報システム工学科 清水明宏助教授には，本論文をまとめるにあたり懇切丁寧なる御指導，御鞭撻を賜わった．ここに謹んで深謝申し上げる．

また，本学大学院工学研究科基盤工学専攻 井上富幸氏には，研究途上において有益な御議論，御助言を頂いた．ここに心からお礼を申し上げる．

また，NTT アドバンステクノロジ株式会社システムインテグレーション事業部 第一技術部 渋谷充喜主査には，本研究に対し有益な御助言を頂いた．ここに記して謝意を表する．

清水研究室学部生 大石恭裕氏，林竜也氏をはじめ研究室の方々には，研究途上において有益な御議論を頂いた．諸氏に心より感謝する．

# 参考文献


[1] 堀岡，清水／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，電子情報通信学会技術研究報告，OFS，オフィスシステム，Vol.97 Num.55 pp.7-12 (1998.01)

[2] 堀岡，竹下，清水／課金機能を有する暗号化コンテンツ，提供方式，電子情報通信学会技術研究報告，OFS，オフィスシステム，Vol.98 Num.1 pp.1-6 (1998.05)

[3] 堀岡，山中／ PERM 認証を用いたコンテンツ提供方式の検討，電子情報通信学会技術研究報告，OFS，オフィスシステム，Vol.99 Num.70 pp.7-12 (1999.05)

[4] 服部，菅野／マイクロペイメント：ディジタルコンテンツ流通のキーを握る決済手段（情報処理最前線），情報処理，Vol.39 Num.1 pp1-5 (1998.01)

[5] 藤井, 山中他/映像情報流通方式の検討, 情報処理学会全国大会講演論文集, Vol. 第 50 回平成 7 年前期 Num. 3 pp.157-158 (1995.03)

[6] 安原隆一・６．EC の技術動向：デジタルコンテンツ作成流通技術（＜特集＞：「エレクトロニック・コマース」），情報処理，Vol.38 Num.9 pp.785-791 (1997.09)

[7] 庵, 玉井他/不正コピー防止を考慮した情報販売方式, 情報処理学会研究報告. DPS, マルチメディア通信と分散処理, Vol. 99 Num. 4 pp.139-144 (1999.01)

[8] 森保, 明石他/情報流通システムにおける鍵配送通信の実装, 情報処理学会研究報告. マルチメディア通信と分散処理研究会報告, Vol. 96 Num. 108 pp.83-88 (1996.11)

[9] 清水, 宮口/高速データ暗号アルゴリズム FEAL, 信学論 D-I, Vol. J73-D-I,No. 7,pp.630-636,Jul.1987.

[10] 藤井, 谷口他/スクランブル映像を用いたネットワークにおける映像情報流通方式, 情報処理学会全国大会講演論文集, Vol. 第 51 回平成 7 年後期 Num. 2 pp.85-86 (1995.09)

[11] 中村勝洋・５．EC の技術動向：セキュリティ技術（＜特集＞：「エレクトロニック・コマース」），情報処理，Vol.38 Num.9 pp.778-84 (1997.09)

[12] 松井充/3. モバイルコンピューティングを支えるソフトウェア技術 3-3 情報セキュリ

ティ技術 (¡特集¿モバイルコンピューティング), 電子情報通信学会誌, Vol. 80 Num. 4 pp.364-369 (1997.04)

[13] 宮崎, 中嶋他/セキュアデジタルコンテンツ配布方式の検討, 情報処理学会全国大会講演論文集, Vol. 第 55 回平成 9 年後期 Num. 3 pp.246-247 (1997.09)

[14] 塚田, 福永他/MOCHA におけるリアルタイム情報配送方式の検討, 情報処理学会全国大会講演論文集, Vol. 第 55 回平成 9 年後期 Num. 3 pp.624-625 (1997.09)

[15] 近藤, 灘本他/2000-DBS-122-26 モバイル環境における検索エンジンの出力結果の再構成と呈示, 情報処理学会研究報告. DBS, データベース・システム, Vol. 2000 Num. 69 pp.199-206 (2000.07)

[16] http://www.tca.or.jp/

[17] http://www.nri.co.jp/news/2000/001108/index.html

[18] http://www.nri.co.jp/news/2000/001025/index.html

[19] http://research.goo.ne.jp/

# 付録 A

# SAS-K パスワード認証方式

SAS-K[*1]パスワード認証方式は，被認証者から認証者への認証依頼毎にパスワード等の認証情報を変更して認証を行なう方法である．そして，SAS は通信プロトコルに組み込める程，簡易なプロセスで認証を行なうことができる方式で，携帯電話上を含めた，コンテンツ流通のプリペイド課金やマイクロペイメントシステムへの応用等が可能である．

以下に SAS-K の概要を示す．

## A.1 定義と記法

本論文で用いる定義と記法は以下の通りである．

1. User を，認証用プロトコルを用いるコンピュータユーザとする．
2. Host を，ユーザを認証するサーバとする．
3. A を，ユーザの ID とする．
4. S を，ユーザのパスワードとする．
5. n を，認証セッション回数を表す 0 以上の整数とする．
6. $N_n$ を，n 回目の認証に対応する乱数とする．
7. E を，暗号用のハッシュ関数とする．また，$E_n^m$ とは，$N_n$ を使い，$(S \oplus N_n)$ が m 回ハッシュされたことを示す．
8. $\oplus$ は，ビット毎の排他的論理和を表す．

[*1] Simple and Secure KUT version

## A.2 SAS-K プロトコル

このプロトコルは，登録フェーズと認証フェーズからなる．登録は一度だけ行われ，認証はユーザがログインするたびに毎回行われる．各々の過程を，図 A.1，図 A.2 に示す．

### A.2.1 登録フェーズ ($n = 0$)

User: $E_0^2 = E^2(S \oplus N_0)$ を計算する．

User: A，$E_0^2$ を Host に安全なチャネルを用いて送信する．

Host: A，$E_0^2$ を保存する．

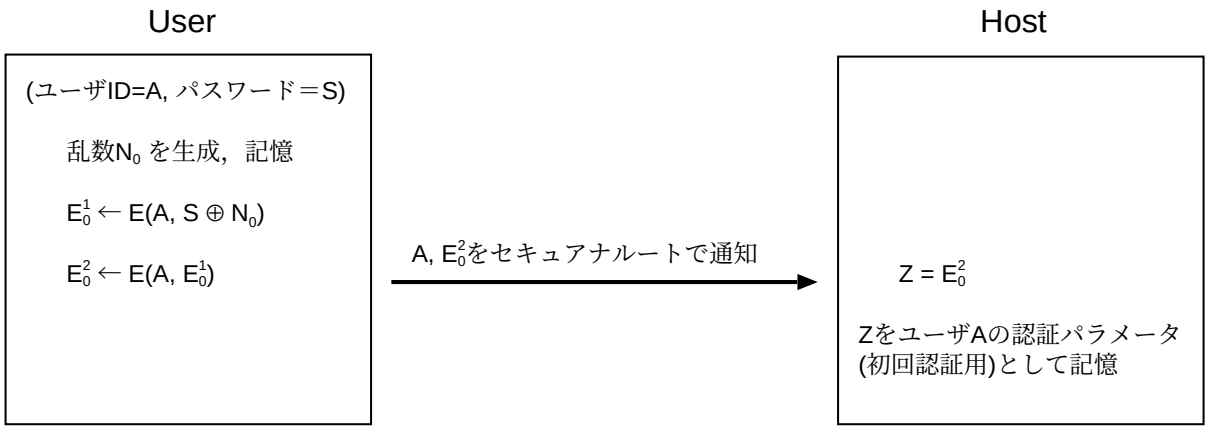


図 A.1 登録フェーズ

### A.2.2 認証フェーズ ($n = k$)

User:以下のデータを計算し，ユーザ IDA と共に Host に送信する．

$$E_{k-1}^1 \oplus E_{k-1}^2 \oplus E_k^3, \quad E_k^2 \oplus E_{k-1}^2$$

その後，Host 側では，

$$(E_k^2 \oplus E_{k-1}^2) \oplus E_{k-1}^2 = E_k^2$$

により，次回認証用データを取得する．そして，

$$E(E_k^2) = E_k^3$$

を計算する．次に，先程得られた $E_k^3$ を使い，

$$(E_{k-1}^1 \oplus E_{k-1}^2 \oplus E_k^3) \oplus E_k^3 = E_{k-1}^1 \oplus E_{k-1}^2$$

を計算し，さらに，登録されている $E_{k-1}^2$ を使い，

$$(E_{k-1}^1 \oplus E_{k-1}^2) = E_{k-1}^1$$

を導出する．そして，そのデータにもう一度ハッシュ関数を適用し，$E_{k-1}^2$ を得る．

$$E(E_{k-1}^1) = E_{k-1}^2$$

そして，このデータと登録されている $E_{k-1}^2$ を比較することによって認証を行う．こうすることによって，認証用データの正当性が検証された認証を可能にする．

## A.2　SAS-K プロトコル

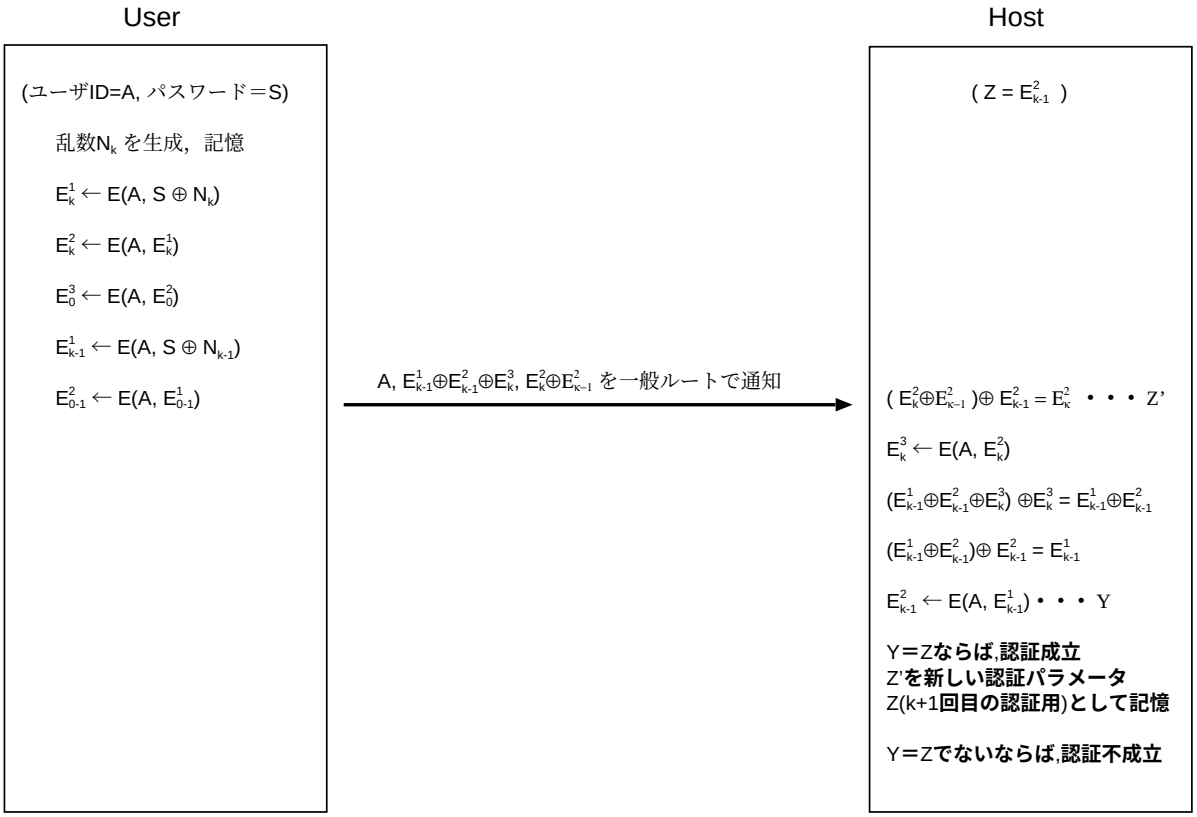


図 A.2　認証フェーズ

# 付録 B

# FEAL(Fast Data Encipherment Algorithm)

FEAL 暗号は，鍵ブロックが 64 ビットであるような 64 ビットのブロック暗号である．鍵ブロックの全ビットが暗号化と復号に使われる．ここで述べる FEAL 暗号は，厳密には FEAL-8(Fast Data Encipherment Algorithm 8-round Version) と呼ばれるものである．

## B.1 基本構造

FEAL 暗号は，データランダム化部と鍵生成部とから構成される．データランダム化部内部は，8 段のインボリューションと，入力部と出力部の簡単なインボリューションとからなる．

鍵生成部で，64 ビットの鍵から，256 ビット (16 ビット ×16) の鍵 $K_i(1 \leq i \leq 16)$ が生成される．

## B.2 FEAL 暗号の構成

### B.2.1 記法

本節で用いる記法を以下に示す．

1. 8 ビットを 1 バイトとする．
2. ブロックデータに対する右下の添字は，複数バイトブロックデータを構成する部分

ブロックデータの左から数えた際の順番を示す．部分ブロックデータには，1 バイト ($\alpha_1$, $\beta_1$ など)，2 バイト ($K_i$，$i = 0 \sim 15$)，4 バイト ($A_0$, $B_0$, $L_0$, $R_0$ など) を単位とするものがある．

3. $(a, b, c, \cdots)$ は $a, b, c, \cdots$ のこの順序の連結 ( Concatenation ) を表す．
4. $a \oplus b$ は，ブロック a と b の排他的論理和を示す．
5. $\Phi$ は，すべて 0 の 4 バイトブロックデータを表す．
6. 等号 $(=)$ は，右辺の左辺への代入を表す．

### B.2.2　基本関数

FEAL-8 の基本関数について述べる．

#### s 関数

s 関数は以下に示すように，法 256 の加算および 2 ビットの左循環回転演算で構成される 8 ビット (1 バイト) データ変換関数である． $+1$ のあるなしによって，$s_1$ と $s_0$ に区別する．

$$s_\delta\,(x_1, x_2, \delta) = ROT2(w)$$

ただし，$w = (x_1 + x_2 + \delta) mod\ 256$，$\delta = 0$ または 1(定数) である．

また，ROT2 は，8 ビットデータを 2 ビット左方向へ循環して 8 ビットのデータを得る関数である．

#### $f_k$ 関数

$f_k$ 関数は，4 バイトブロックデータ交換関数である．$f_k\,(\alpha, \beta)$ を $f_k$，$\alpha$ を $(\alpha_0, \alpha_2, \alpha_3)$, $\beta$ を $(\beta_0, \beta_1, \beta_2, \beta_3)$ と表す場合，$f_k = (f_{k0}, f_{k1}, f_{k2}, f_{k3})$ は以下の手順で算出する．

$$f_{k1} = \alpha_1 \oplus \alpha_0$$

$$f_{k2} = \alpha_2 \oplus \alpha_3$$

$$f_{k1} = s_1(f_{k1},\, (f_{k2} \oplus \beta_0))$$
$$f_{k2} = s_0(f_{k2},\, (f_{k1} \oplus \beta_1))$$
$$f_{k0} = s_0(\alpha_0,\, (f_{k1} \oplus \beta_2))$$
$$f_{k3} = s_1(\alpha_3,\, (f_{k2} \oplus \beta_3))$$

**f 関数**

f 関数は，4 バイトブロックデータ変換関数である．$f(\alpha,\, \beta)$ を，$\alpha$ を $(\alpha_0,\, \alpha_1,\, \alpha_2,\, \alpha_3)$，$\beta$ を $(\beta_0,\, \beta_1,\, \beta_2,\, \beta_3)$ と表す場合，$f = (f_0,\, f_1,\, f_2,\, f_3)$ は以下の手順で算出する．

$$f_1 = \alpha_1 \oplus \beta_0 \oplus \alpha_0$$
$$f_2 = \alpha_2 \oplus \beta_1 \oplus \alpha_3$$
$$f_1 = s_1(f_1,\, f_2)$$
$$f_2 = s_0(f_2,\, f_1)$$
$$f_0 = s_0(\alpha_0,\, f_1)$$
$$f_3 = s_1(\alpha_3,\, f_2)$$

### B.2.3　鍵処理

図 B.1 に FEAL-8 の鍵処理を示す．鍵処理は，64 ビットの共通鍵ブロック K から，中間鍵 $K_i (i = 0 \sim 15$，各 2 バイト) を定める．共通鍵ブロックの左右 32 ビットのデータを $A_0$ および $B_0$ とする．最初に，$D_0 = \Phi$ とし，$r = 1 \sim 8$ について，以下の手順で $K_i \quad (i = 0 \sim 15)$ を定める．

$$D_r = A_{r-1}$$
$$A_r = B_{r-1}$$
$$B_r = f_k(\alpha,\, \beta) = f_k(A_{r-1},\, B_{r-1} \oplus D_{r-1})$$
$$K_{2(r-1)} = (B_{r0},\, B_{r1})$$
$$K_{2(r-1)+1} = (B_{r2},\, B_{r3})$$

### B.2.4　暗号化／復号処理

図 B.2 に FEAL-8 の暗号化／復号処理を示す．まず，暗号化処理は以下の通りである．平文ブロックの左右それぞれ 4 バイトのブロックを $L_0$，$R_0$ として，最初に以下の処理を行う．

$$(L_0, R_0) = (L_0, R_0) \oplus (K_8, K_9, K_{10}, K_{11})$$

$$(L_0, R_0) = (L_0, R_0) \oplus (\Phi, L_0)$$

続いて，$r = 1 \sim 8$ について，$R_r$ と $L_r$ を逐次算出する．

$$R_r = L_{r-1} \oplus f(R_{r-1}, K_{r-1})$$

$$L_r = R_{r-1}$$

次に，$R_8, L_8$ に対して以下の処理を行い，暗号文ブロック $(R_8, L_8)$ を得る．

$$(R_8, L_8) = (R_8, L_8) \oplus (\Phi, R_8)$$

$$(R_8, L_8) = (R_8, L_8) \oplus (K_{12}, K_{13}, K_{14}, K_{15})$$

次に，復号処理は以下の通りである．暗号文ブロックの左右それぞれ 4 バイトのブロックを $L_0$，$R_0$ として，最初に以下の処理を行う．

$$(R_8, L_8) = (R_8, L_8) \oplus (K_{12}, K_{13}, K_{14}, K_{15})$$

$$(R_8, L_8) = (R_8, L_8) \oplus (\Phi, R_8)$$

続いて，$r = 8 \sim 1$ について，$L_{r-1}$ と $R_{r-1}$ を逐次算出する．

$$L_{r-1} = R_r \oplus f(L_r, K_{r-1})$$

$$R_{r-1} = L_r$$

最後に，$L_0$，$R_0$ に対して以下の処理を行い，平文ブロック $(L_0, R_0)$ を得る．

$$(L_0, R_0) = (L_0, R_0) \oplus (\Phi, L_0)$$

$$(L_0, R_0) = (L_0, R_0) \oplus (K_8, K_9, K_{10}, K_{11})$$

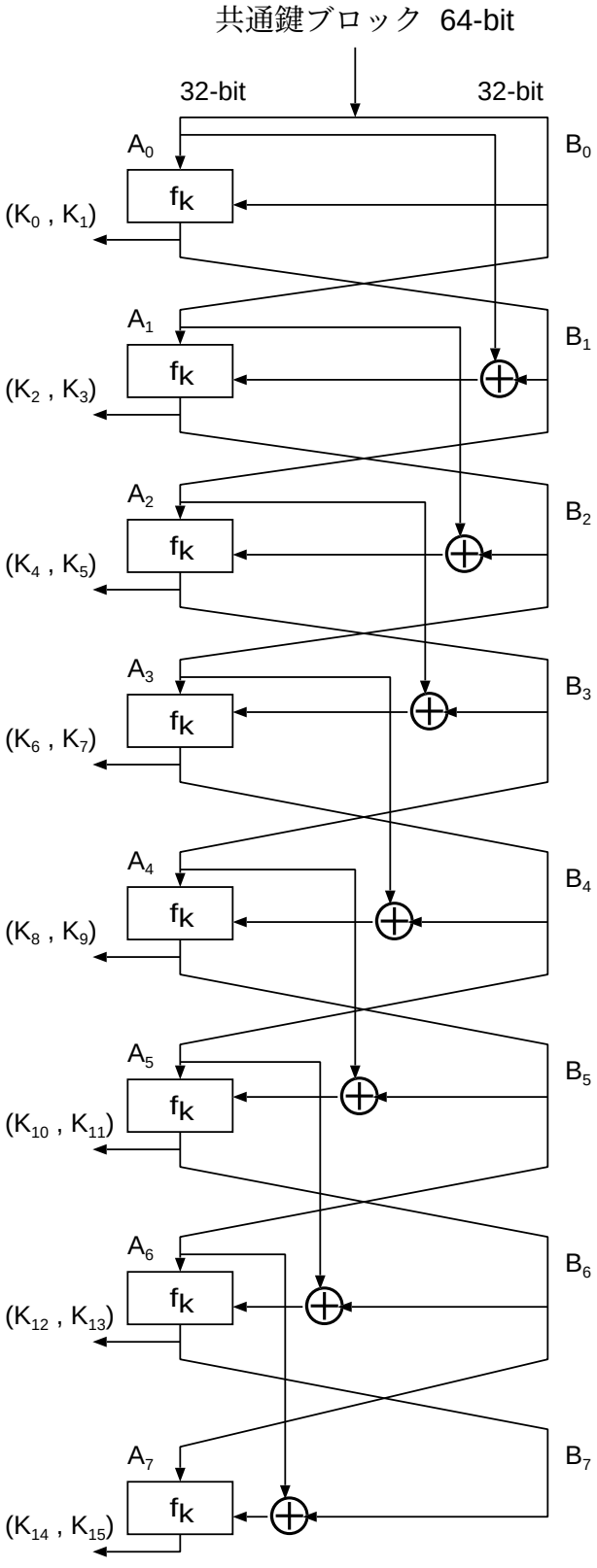


図 B.1　FEAL-8 の鍵処理

B.2　FEAL 暗号の構成

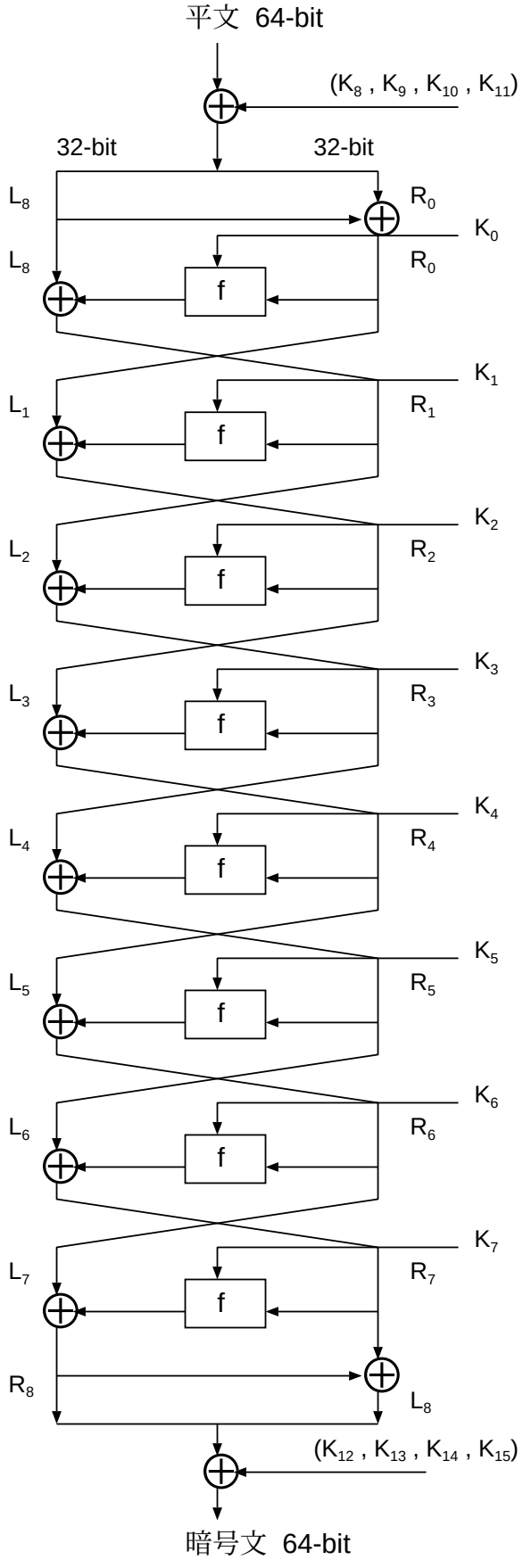


図 B.2　FEAL-8 の暗号化／復号処理