

平成15年度

# 情報家電協調基盤整備事業

(多機能ICチップ等を活用した新領域ITサービスに関する研究開発・実証事業)

## 報告書

平成16年3月

財団法人ニューメディア開発協会

## 「多機能 IC チップと知的創造社会」

1994年8月、日本政府は高度情報通信社会推進本部を設置し、我が国の社会全体の情報化を進める決断をした。この時から、ITを活用した情報化社会の構築が始まり、その後、2001年1月には本格的な実現を目指したIT戦略本部が発足した。そして現在は、世界最高の電子政府を2005年度中に実現することを目標として、必要な環境整備とその構築が進められている。また一方では、我が国が知的創造社会へと進化・発展するための基本戦略を策定するために、2002年2月には知的財産戦略会議が開催され、策定された戦略の着実な実施を図るために、知的財産戦略本部が2003年3月に発足している。

近年、インターネット利用者の増加とブロードバンドの普及に伴ない、その利便性と効果が広く認識された反面、相手の顔が見えないことなどに起因するさまざまな危険性も指摘されている。また、B2Bの電子商取引や電子政府においては、安全性を確保する手法として、IP-VPNを用いたイントラネットも実用化されている。このような状況から、自由なアクセスと利用を基本とするインターネットにおいても、必要ときには十分な安全性を確保することで利用者に安心感を与えることが、IT社会の構築に不可欠であることが分かる。

一方では、知的財産戦略大綱に書かれているように、デジタルコンテンツの権利者保護と不正利用の防止を図るとともに、これまでのCDやDVDなどの媒体に加えてインターネット等を介したコンテンツの流通を促進することが重要になっている。このためには、著作権等の権利を有している権利者（N人）と利用者（M人）の任意の契約が成立し、利用者が持つ使用許諾を常に電子的に確認できる仕掛けを作ることが極めて有効である。こうすることで従来のように、ソフトウェアや音楽などの利用権を使用するPCや媒体に固定する必要がなくなり、利用者にとってはいつでもどこでも使用許諾を受けたデジタル情報の利用が可能になる。そしてそのためには、人と機器、さらにコンテンツの正当性を認証することが不可欠である。

本事業で取り扱った多機能ICチップは、次世代スマートカード用に開発されたものであるが、人、機器、コンテンツを認証するための証明書や認証鍵を電子空間で簡便に取り扱うことを可能にする。したがってこの技術の利用に加えて、利用者の使用許諾等を認証する新たな認証局を立ち上げることで、使用許諾を含めた各種の権利を利用者本人に帰属する属性として認証することが可能になる。これはまさしく、新たな認証のフレームワークであり、コンテンツの安全な利用を実現する。我が国が目指す知的創造社会やIT社会の実現に、多機能ICチップが大きく貢献することを期待する。

平成16年3月

新領域ITサービスに関するあり方検討委員会 委員長 大山 永昭

# 目次

第Ⅰ編 工程管理等の委託業務に関する報告 .....	1
1. 事業概要.....	2
第Ⅰ編 工程管理等の委託業務に関する報告 .....	3
2. 実施内容.....	4
2. 1 公募業務 .....	4
2. 2 企画運営に関する業務 .....	5
2. 3 委員会運営業務.....	8
2. 4 工程管理業務 .....	20
2. 5 汎用性向上業務.....	22
第Ⅱ編 研究開発・実証事業の実施報告 .....	29
1. 多機能 IC チップ等を活用した新領域 IT サービスに関する研究開発・ 実証事業の概要 .....	30
1. 1 背景.....	30
1. 2 目的.....	30
1. 3 事業概要 .....	30
1. 4 実施体制 .....	34
第Ⅱ編 研究開発・実証事業の実施報告 .....	37
2. テーマ種別 1 .....	38
2. 1 事業概要 .....	38
2. 2 多機能 IC チップフレームワークに基づくドメイン間の相互運用に 関する検討.....	41
2. 3 多機能 IC チップフレームワーク以外の IC チップフレームワークに 基づくドメインを含めた相互運用に関する検討.....	49
2. 4 まとめ.....	57
第Ⅱ編 研究開発・実証事業の実施報告 .....	59
3. テーマ種別 2 .....	60
3. 1 事業概要 .....	60
3. 2 技術的基盤の検討.....	63

3. 3	マルチメディアコンテンツ流通サービスの実効性検証 .....	70
3. 4	会員権サービスの実効性検証 .....	81
3. 5	多機能 IC チップを搭載した携帯電話への適用の検討 .....	90
3. 6	まとめ .....	99
第Ⅱ編	研究開発・実証事業の実施報告 .....	103
4.	テーマ種別 3 .....	104
4. 1	事業概要 .....	104
4. 2	プロファイルポータビリティに関する研究 .....	104
4. 3	実証実験 .....	111
4. 4	検証項目 .....	118
4. 5	検証結果 .....	119
4. 6	まとめ .....	135

## 第 I 編 工程管理等の委託業務に関する報告

# 1. 事業概要

---

## 1. 事業概要

(財)ニューメディア開発協会（以下「当協会」という。）では、経済産業省が実施した平成15年度情報家電協調基盤整備事業（多機能 IC チップ等を活用した新領域 IT サービスに関する研究開発・実証事業）（以下「本事業」という。）に関する工程管理業務等を受託した。

この工程管理業務に係る実施期間及び業務内容は以下の通りである。

### 実施期間

平成 15 年 6 月 2 日～平成 16 年 3 月 31 日

### 業務内容

#### ◎公募関連業務

- ・ 公募の実施及び審査委員会の運営

#### ◎企画運営業務

- ・ 技術的妥当性の検討に係る事務
- ・ 制度的課題の検討に係る事務

#### ◎委員会開催業務

- ・ 新領域 IT サービスに関するあり方検討委員会
- ・ 技術検討小委員会
- ・ 制度検討小委員会

#### ◎進捗管理業務

- ・ コンソーシアム定例連絡会議による進捗管理
- ・ テーマ種別毎のワーキンググループ等を通じた状況確認

#### ◎汎用性向上業務

- ・ 東京工業大学との共同研究の実施

以下では、当協会において実施した上記業務の結果報告を行うこととする。

## 第 I 編 工程管理等の委託業務に関する報告

# 2. 実施内容

---

## 2. 実施内容

### 2. 1 公募業務

#### (1) 公募の経緯

経済産業省が昨年度実施した「情報経済基盤整備（地域情報化及びその基盤整備要素技術等に関する調査研究事業）」では、「多機能 IC チップフレームワーク検討委員会」において、ネットワーク上で人や機器の認証や権利の保証を実現するための手段としての多機能 IC チップの有効性並びに多機能 IC チップの利用分野ニーズ及びその運用フレームワークについての方向性について検討し、取りまとめた。

経済産業省は、安全で安心できる社会基盤としての多機能 IC チップインフラを確立するとともに、それを活用した新領域 IT サービスの実証実験により、システム導入に伴う技術面・利用面での課題を検証し、官民間問わずその成果を広く活用することを目的として本事業を推進し、その研究員を公募により選定することとした。

本事業の研究員公募は、経済産業省により平成 15 年 7 月 1 日から平成 15 年 7 月 15 日までの期間で行われた。当該公募に対して、公募期間内に 3 件の申請があった。当協会では、経済産業省より研究員公募の申請受付や問い合わせ対応を含め選定に係る業務を実施した。

公募されたテーマは以下のとおりである。

- ①テーマ種別 1（多機能 IC チップドメイン間の相互運用性を確保するための運用管理手法及び管理システムの研究開発）
- ②テーマ種別 2（マルチメディア情報流通等のアプリケーションを活用した多機能 IC チップフレームワークシステムの研究開発及び実効性検証）
- ③テーマ種別 3（プロファイルポータビリティサービスに係る開発・実証研究）  
※プロファイルポータビリティ・・・電子チケットや会員制サービス等、個人の属性情報や環境情報、端末情報等のプロファイルを登録管理、移動、利用すること

#### (2) 審査委員会の設置

研究員公募に伴い、企業から提案された複数の研究テーマに対して、本事業の目的や意義、技術理解度等の要件を鑑み、適切な研究員を選定審査を行う機関として、「審査委員会」を設置した。

審査委員会は、多機能 IC チップ及び次世代 IC カード技術に関する学識経験者ならびに専門家、多機能 IC チップを活用した IT サービスの有望分野に関する専門家等により構成されている。



### (3) 結果

本事業の公募に対して、審査委員会にて複数企業から提案された研究テーマの選定審査を行い、以下の1件の研究員の選定を行った。

コンソーシアム名	代表研究員名
新ITビジネス創出のためのスマートセキュリティチップ活用開発・実証コンソーシアム	エヌ・ティ・ティ・コミュニケーションズ株式会社

また、この公募結果は、平成15年7月31日に経済産業省のホームページにおいて、発表された。

## 2. 2 企画運営に関する業務

### 2. 2. 1 具体的実施内容の検討支援

当協会は、研究員が本事業の目的に合致した研究テーマを円滑、かつ、確実に実施できるよう、「新ITビジネス創出のためのスマートセキュリティチップ活用開発・実証コンソーシアム（以下「コンソーシアム」という。）」との具体的実施内容に関する管理業務を実施した。

#### (1) 事業概要

コンソーシアムは、NTT コミュニケーションズ株式会社を主たる研究員とし、松下電器産業株式会社を始めとした11社が参加した。

コンソーシアムでは、以下の研究テーマを実施した。

#### ①テーマ種別1（多機能ICチップドメイン間の相互運用性を確保するための運用管理手法及び管理システムの研究）

多機能ICチップを活用できる有効な範囲と定義される「多機能ICチップドメイン」は、多機能ICチップの発行主体や中立の第三者機関によって運用される「登録認定機関」により運用され、多機能ICチップの様々な利用形態やビジネス上の要請に応じて複数の異なったドメインが並立して運営されることが想定される。このような状況下では、異なったドメイン間同士の相互運用性を確保し、あるドメインで発行された多機能ICチップが異なるドメインで提供されているサービスを受けられるようにすることが求められるようになる。

テーマ種別1では、異なったドメイン間での相互運用性を確保するための多機能ICチップの運用管理手法及び管理システムについての研究を行った。

## ②テーマ種別 2 (マルチメディア情報流通等のアプリケーションを活用した多機能 IC チップフレームワークシステムの研究開発及び実効性検証)

音楽コンテンツを中心としたデジタルコンテンツのネットワーク配信は、品質を劣化させることなく容易に複製が可能であることや、個人間でのコンテンツ交換ソフトウェアの出現等も関係して、個人の不正な二次流通が問題となっている。そのため、著作権者やコンテンツ製作者等の著作隣接権者、コンテンツ配信事業者はネットワークを介したコンテンツ配信事業に必ずしも積極的でなく、実際には著作権保護機能を付与し、多重複製の防止や機器の限定等、利用者の利便性を低下させる要因になっている。

多機能 IC チップフレームワークでは、人が保有する IC カードと機器に搭載される多機能 IC チップの組み合わせにより、取り扱う情報の秘匿性や偽造防止が可能である。テーマ種別 2 では、権利情報として「デジタルコンテンツを利用する許諾」と「会員権」を対象として、共通的な仕組みの検討を行った。

また、デジタルコンテンツ利用者の利便性を低下させることなく、また、著作権者や著作隣接権者等の権利者が安心してコンテンツを提供でき、コンテンツ配信事業者が共通の仕組みを利用することで市場への参入障壁を低減できるようなマルチメディア情報流通サービスの研究を行い、アプリケーション開発を通じてその実効性検証を行った。

さらに、会員権アプリケーションを保有している利用者のみサービスを追加・削除できるような会員権サービスのアプリケーション開発及び実証実験 (テーマ種別 3 と同じ実証場所) や、多機能 IC チップフレームワークの携帯電話への適用を行った。

## ③テーマ種別 3 (プロファイルポータビリティサービスに係る開発・実証研究)

多機能 IC チップフレームワークでは、アプリケーションの追加や削除を可能とする一方で、異なるアプリケーション間の責任範囲を明確にするために、相互に関連性を持っていない。しかしながら、実現されるサービスによっては、個人情報保護やセキュリティを確保しつつ、相互に情報を連携させることにより、今までになかった新しいサービスの実現や既存サービスの高度化が可能となるようなビジネスモデルが考えられる。

そこで、テーマ種別 3 では、多機能 IC チップに利用者の属性情報を格納し、イベント会場での電子チケットサービスを中心とした各種サービスを利用することにより、その活用履歴に応じて、新しいサービスが実現される実証実験を展開し、技術面、業務面における高付加価値サービスの有効性を検討した。

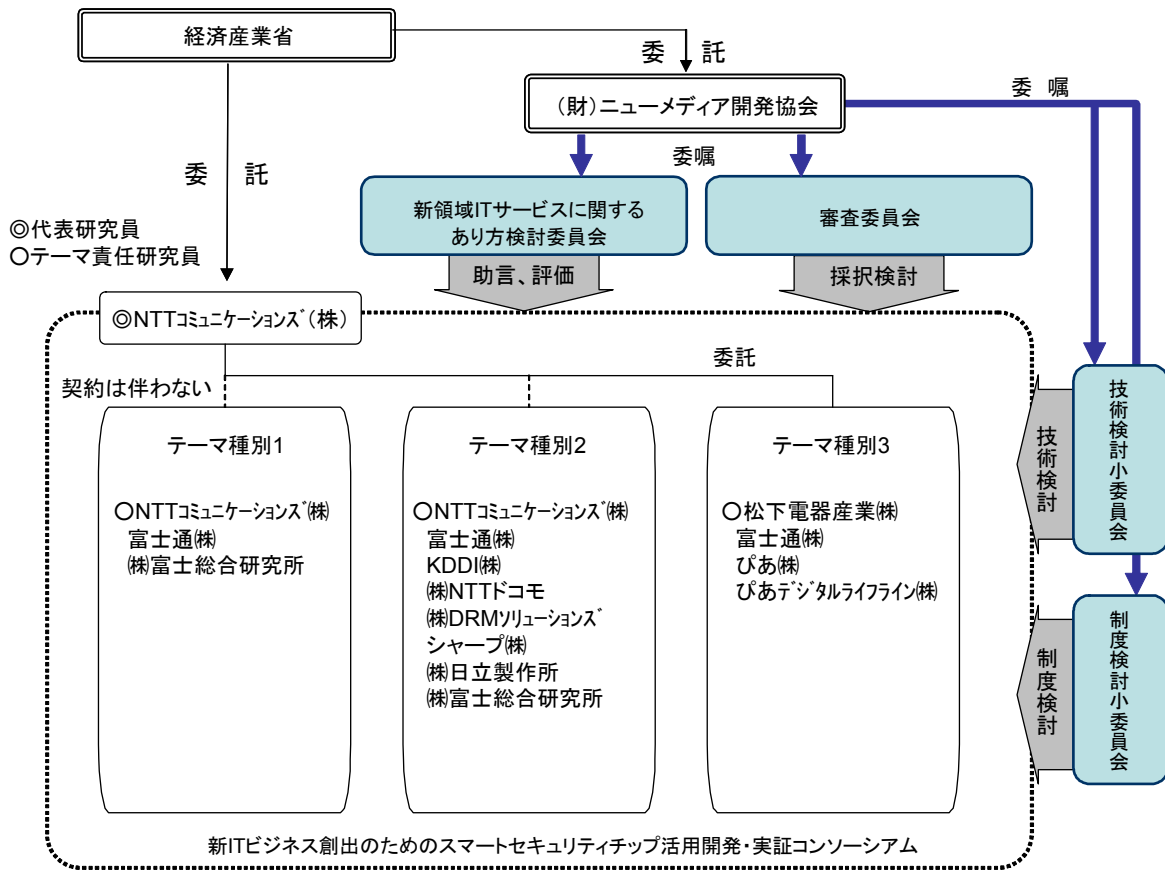


図 2 - 1 実施体制

## 2. 2. 2 技術的妥当性の検討に係る事務

当協会では、本事業の技術的妥当性の検討を行うために技術検討小委員会を設置し、その委員会運営事務を実施した。

技術検討小委員会では、本事業の技術的な基盤である「多機能 IC チップフレームワーク」及び「権利流通管理システム」に関する要件書について、技術的な観点からその評価・助言を行った。

## 2. 2. 3 制度的課題の検討に係る事務

当協会では、本事業の制度的課題の検討を行うために制度検討小委員会を設置し、その委員会運営事務を実施した。

制度検討小委員会では、本事業で提供するサービスである「マルチメディア情報流通サービス」及び「プロフィールポータビリティサービス」について、制度的な観点からその評価・助言を行った。

## 2. 3 委員会運營業務

本事業では、事業の円滑な推進及び管理を行う観点から、以下の委員会及び小委員会を設置した。

### ◎ 新領域 IT サービスに関するあり方検討委員会

新領域 IT サービスに関するあり方検討委員会（以下「検討委員会」という。）は、各テーマ種別の研究、開発、実証に向けて、研究員に対して実施手順や内容に対する評価及び助言を行うための機関であり、主に、本事業の推進方策や本事業の成果の普及等についての検討を行った。

### ◎ 技術検討小委員会

技術検討小委員会は、本事業の技術推進方策の提言や技術検討成果の普及に係る助言等の技術的な観点からの評価及び助言を行うための機関であり、主に、本事業の技術的な基盤である「多機能 IC チップフレームワーク」及び「権利流通管理システム」について、マルチメディア情報流通サービス及びプロファイルポータビリティサービスへの適用について検討した。

### ◎ 制度検討小委員会

制度検討小委員会は、本事業の制度面での推進方策の提言やビジネスモデル上の制度的課題の解決に向けた助言等の制度的な観点からの評価及び助言を行うための機関であり、主に「マルチメディア情報流通サービス」への著作権法等の法制度の適用と「プロファイルポータビリティサービス」への個人情報保護やセキュリティ管理等の適用について検討した。

なお、小委員会の編成については、当初、マルチメディア情報流通推進小委員会とプロファイルポータビリティ推進小委員会を編成し、技術検討及び制度検討を各分野にて実施することを予定していた。その後、経済産業省及び検討委員会の委員等からの助言があり、検討委員会での了承のもと、技術検討小委員会と制度検討小委員会に再編成した。（このため、技術検討小委員会の第 1 回目は、マルチメディア情報流通推進小委員会として実施した。）

以下では、委員会及び小委員会の構成及び会議内容についてその概要を示す。

## 2. 3. 1 新領域 IT サービスに関するあり方検討委員会

### (1) 構成

本委員会は、多機能 IC チップ等を活用した新領域 IT サービスについて総合的に評価可能な学識経験者及び専門家等により構成されている。

また、経済産業省、コンソーシアム企業や多機能 IC チップ関連企業がオブザーバとして参加し、事務局は当協会が担当した。

委員長	東京工業大学 フロンティア創造共同研究センター	教授	大山 永昭
委員	早稲田大学大学院 アジア太平洋研究科	教授	岩村 充
委員	財団法人ニューメディア開発協会	理事長	岡部 武尚
委員	社団法人日本音楽著作権協会	常務理事	加藤 衛
委員	株式会社 電通 APソリューション局 e-プロモーションプランニング部	主管	斎藤ようこ
委員	ネットワーク音楽著作権連絡協議会	代表世話人	佐々木隆一
委員	経済産業省 商務情報政策局情報プロジェクト室	室長	牧内 勝哉
委員	ぴあ株式会社	取締役	宮崎 眞行

(50 音順)

(2) 開催日時及び審議内容

第1回 新領域 IT サービスに関するあり方検討委員会

日程：平成 15 年 6 月 27 日（金）

場所：（財）ニューメディア開発協会 B 会議室（三田国際ビル 23 階）

内容：①委員紹介及び委員長選出

②事務局による平成 14 年度多機能 IC チップフレームワーク検討委員会報告書の概要に関する説明

③事務局による検討委員会の設置要綱に関する説明

④本事業の事業概要及び実施体制に関する審議

⑤本事業の実施スケジュールに関する審議

⑥本事業の公募要綱に関する審議

第2回 新領域 IT サービスに関するあり方検討委員会

日程：平成 15 年 9 月 29 日（月）

場所：虎ノ門パストラル 新館 4 階 プリムローズ

内容：①事務局による公募結果に関する説明

- ②事務局による小委員会の設置及び実施体制に関する説明
- ③事務局によるコンソーシアムの事業概要に関する説明
- ④研究員による多機能 IC チップドメイン間の相互運用性に関する説明
- ⑤研究員によるマルチメディア情報流通サービスの事業内容に関する説明
- ⑥研究員によるプロファイルポータビリティサービスの事業内容に関する説明
- ⑦本事業の事業内容に関する審議

### 第 3 回 新領域 IT サービスに関するあり方検討委員会

日程：平成 15 年 12 月 11 日（木）

場所：虎ノ門パストラル 新館 5 階 マグノリア

- 内容：①事務局によるマルチメディア情報流通推進小委員会の経過に関する説明
- ②研究員による多機能 IC チップドメイン間の相互運用性の検証内容に関する説明
  - ③研究員によるマルチメディア情報流通サービスの検証内容に関する説明
  - ④研究員による多機能 IC チップフレームワークの携帯電話適用についての検証内容に関する説明
  - ⑤研究員によるプロファイルポータビリティサービスの検証内容に関する説明
  - ⑥本事業の検証内容に関する審議

### 第 4 回 新領域 IT サービスに関するあり方検討委員会

日程：平成 16 年 1 月 29 日（木）

場所：松下電器産業株式会社 パナソニックセンター 3 階 会議室 4・5・6

- 内容：①小委員会の再編成に関する審議
- ②研究員によるプロファイルポータビリティサービスに関するデモンストレーションの実施
  - ③研究員によるマルチメディア情報流通サービスに関するデモンストレーションの実施
  - ④研究員による多機能 IC チップフレームワークの携帯電話適用に関するデモンストレーションの実施
  - ⑤研究員による多機能 IC チップドメイン間での相互運用性に関する進捗状況に関する説明
  - ⑥事務局による本事業の運営管理に関する状況報告

### 第 5 回 新領域 IT サービスに関するあり方検討委員会

日程：平成 16 年 3 月 19 日（金）

場所：ダイヤモンドホテル ローズルーム

- 内容：①（財）医療情報システム開発センターによる「医療システム機器のリモートサービスにおける多機能 IC チップを利用したセキュリティ推進事業」の紹介

- ②事務局による小委員会に関する活動報告
- ③研究員による多機能 IC チップドメイン間の相互運用性に関する研究結果の報告
- ④研究員によるマルチメディア情報流通サービスに関する実効性検証結果の報告
- ⑤研究員による多機能 IC チップフレームワークの携帯電話適用に関する検討結果の報告
- ⑥研究員によるプロファイルポータビリティサービスの実証実験結果の報告
- ⑦本事業の報告書の確認

(3) 成果

検討委員会での助言内容及び審議内容については、「多機能 IC チップ等を活用した新領域 IT サービスに関する研究開発・実証事業 報告書」として取り纏めた。

2. 3. 2 技術検討小委員会

(1) 構成

技術検討小委員会は、多機能 IC チップ技術やマルチメディア関連技術等に関する以下の学識経験者及び専門家等により構成されている。

また、経済産業省、コンソーシアム企業や多機能 IC チップ関連企業がオブザーバとして参加し、事務局は当協会が担当した。

委員長	東京工業大学 フロンティア創造共同研究センター	教授	大山 永昭
委員	(株) ディアールエムソリューションズ	代表取締役社長	穴澤 健明
委員	ネットワーク音楽著作権連絡協議会	代表世話人	佐々木隆一

(50 音順)

また、下記の委員は、第 1 回 (マルチメディア情報流通推進小委員会として開催) のみ委嘱した。(その後、制度検討委員会の委員として委嘱)

委員	社団法人日本音楽著作権協会	常務理事	加藤 衛
委員	あさひ・狛法律事務所	弁護士	宮下 佳之

(50 音順)

また、下記の委員は、第2回技術検討小委員会にて追加選任を行った。

委員	日本電信電話株式会社 NTT情報流通プラットフォーム研究所	所長	畠中 優行
委員	東京工業大学 像情報工学研究施設	客員助教授	谷内田益義
委員	財団法人ニューメディア開発協会 IT 装備都市研究事業推進室	部長	山崎 正

(50音順)

(2) 開催日時及び審議内容

第1回 マルチメディア情報流通推進小委員会

日程：平成15年12月4日(木)

場所：虎ノ門パストラル 新館5階 ローレル

内容：①委員紹介及び委員長選出

- ②事務局によるマルチメディア情報流通推進小委員会の設置要綱に関する説明
- ③本事業の事業概要及び実施体制に関する説明
- ④宮下委員より知的財産をめぐる最新動向についての説明
- ⑤研究員より多機能ICチップフレームワークの説明
- ⑥穴沢委員より著作権保護技術についての説明
- ⑦マルチメディア情報流通サービスに関する全体審議

第2回 技術検討小委員会(マルチメディア情報流通推進小委員会から改称)

日程：平成16年2月9日(月)

場所：虎ノ門パストラル 新館4階 ミント

内容：①事務局による小委員会の再編成に関する説明

- ②事務局による技術検討小委員会の設置要綱に関する説明
- ③研究員による本事業の技術基盤に関する説明
- ④研究員による多機能ICチップフレームワークの技術要件に関する概要説明
- ⑤多機能ICチップフレームワーク要件書の審議

第3回 技術検討小委員会

日程：平成16年3月8日(月)

場所：虎ノ門パストラル 新館4階 アイリスガーデン

内容：①事務局による各サービスのフレームワーク検討に関する説明

- ②研究員によるプロファイルポータビリティモデルの技術検討に関する説明
- ③研究員による権利流通管理システムの技術要件に関する概要説明
- ④権利流通管理システム要件書の審議



(3) 成果

技術検討小委員会では、より多くの事業者が本事業の技術的な成果を活用するための共通的な要件書として、「多機能 IC チップフレームワーク要件書」及び「権利流通管理システム要件書」を取り纏めた。

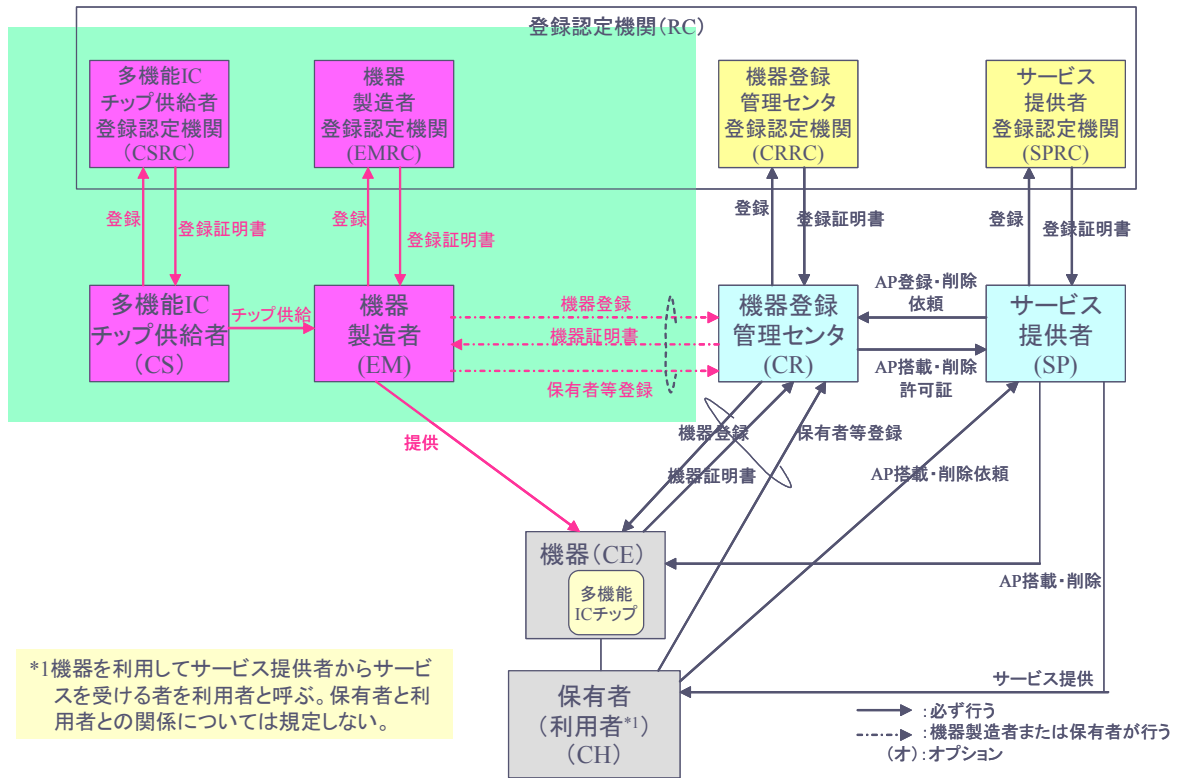


図 2-2 多機能 IC チップフレームワーク

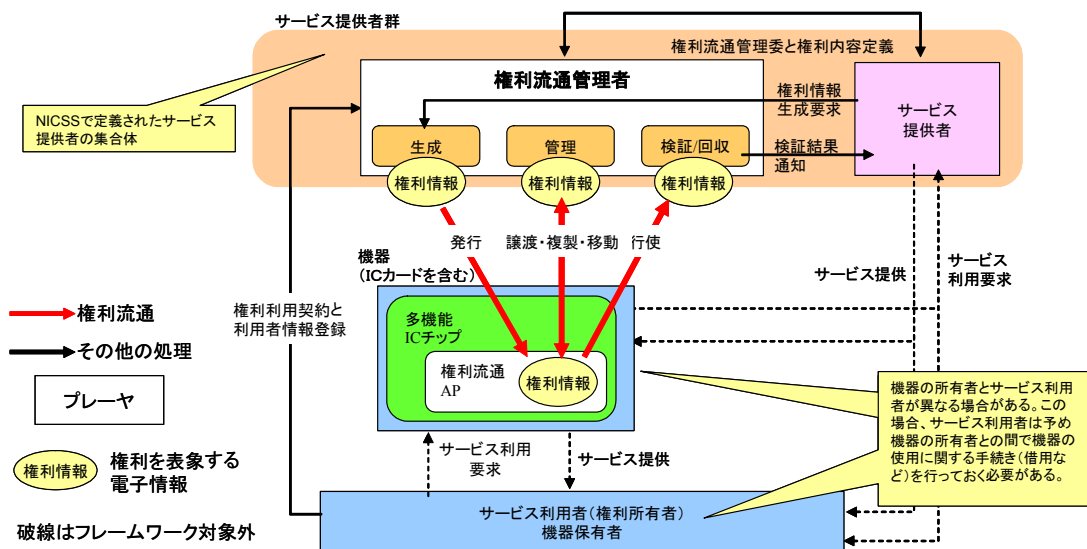


図 2-3 権利流通管理システムモデル

## 2. 3. 3 制度検討小委員会

### (1) 構成

制度検討小委員会は、知的財産保護、個人情報保護、消費者保護等の制度に関する以下の学識経験者・専門家等により構成されている。

また、経済産業省、コンソーシアム企業や多機能 IC チップ関連企業がオブザーバとして参加し、事務局は当協会が担当した。

委員長	早稲田大学大学院 アジア太平洋研究科	教授	岩村 充
委員	社団法人日本音楽著作権協会	常務理事	加藤 衛
委員	埼玉大学 経済学部 青森大学 社会学部	非常勤講師 非常勤講師	原 早苗
委員	牧野総合法律事務所	弁護士	牧野 二郎
	(プロファイルポータビリティモデル制度検討ワーキング 主査)		
委員	あさひ・狛法律事務所	弁護士	宮下 佳之
	(マルチメディア情報流通モデル制度検討ワーキング 主査)		

(50 音順)

### (2) 開催日時及び審議内容

#### 第 1 回 制度検討小委員会

日程：平成 16 年 1 月 26 日（月）

場所：虎ノ門パストラル 新館 5 階 マグノリア

内容：①委員紹介及び委員長選出

- ②事務局による制度検討小委員会の設置要綱に関する説明
- ③事務局による本事業の事業概要及び実施体制に関する説明
- ④研究員によるマルチメディア情報流通モデルに関する説明
- ⑤研究員によるプロファイルポータビリティモデルに関する説明
- ⑥各モデルの制度検討における論点の討議
- ⑦制度検討ワーキングの組成に関する審議

#### 第 2 回 制度検討小委員会

日程：平成 16 年 3 月 9 日（火）

場所：虎ノ門パストラル 新館 6 階 ヴィオレ

内容：①事務局によるマルチメディア情報流通モデル制度検討ワーキングの活動経過に関する説明

- ②研究員によるマルチメディア情報流通サービスに関する詳細説明

- ③宮下委員（主査）によるマルチメディア情報流通モデルの制度検討に関する論点の説明
- ④マルチメディア情報流通モデルの制度検討に関する討議

### 第3回 制度検討小委員会

日程：平成16年3月15日（月）

場所：虎ノ門パストラル 新館4階 アイリスガーデン

- 内容：①事務局によるプロファイルポータビリティモデル制度検討ワーキングの活動経過に関する説明
- ②研究員によるプロファイルポータビリティモデルの制度検討結果に関する説明
  - ③牧野委員（主査）によるプロファイルポータビリティモデルの制度検討に関する論点の説明
  - ④プロファイルポータビリティモデルの制度検討に関する討議
  - ⑤制度検討報告書に関する審議

### (3) 成果

制度検討小委員会では、今後、検討した各サービスをビジネスとして展開する上でより多くの事業者が本事業の制度的な検討成果を活用できるように、マルチメディア情報流通サービス制度検討ワーキング報告書及びプロファイルポータビリティサービス制度検討ワーキング報告書として取り纏め、各テーマ種別の報告書にその内容を盛り込んだ。

#### ①マルチメディア情報流通サービス制度検討ワーキング報告書概要

マルチメディア情報流通サービス制度検討ワーキング報告書の目次を以下に示す。

1. 本プロジェクトの概要
2. 検討の視点
3. 本プロジェクトに係る権利関係の整理
4. 本プロジェクトにおいて流通されるコンテンツの各流通過程において問題となる権利の概要
5. 本プロジェクトの関係者間の契約関係について
6. その他の問題点

マルチメディア情報流通サービス制度検討ワーキングでは、マルチメディア情報流通に係る権利関係を整理するとともに、暗号化されたコンテンツとそのコンテンツを再生するための鍵（復号するための鍵）についての論点整理を行った。

以下に、その論点の概略を説明する。

論点1：暗号化されたコンテンツの著作権法上の性格について	
検討結果	<p>暗号化されたコンテンツであっても、復号することにより知覚可能な状態になることから、著作物が有形的に再生されたものと解するのが相当であり、著作権法上の「複製物」と解すべきである。CDやDVDその他の典型的な著作物の複製物も、所定の再生機器を用いなければ、著作物の内容を知覚できず、その点において、暗号化されたコンテンツと異なる。</p>
論点2：暗号化されたコンテンツを復号するための鍵の著作権法上の性格について	
検討結果	<p>暗号化されたコンテンツを復号するための鍵は、コンテンツを有形的に複製したものではないので、著作権法上の複製物とは解し難い。復号鍵は、著作物を視聴することを可能にする点において、重要な機能を果たすものであるが、現行の著作権法においては、積極的に復号鍵自体を保護することは想定されていないと解される。ただし、復号鍵がなければ著作物を視聴できないようにする方法は、著作権法上「技術的保護手段」に該当するので、「技術的保護手段」の回避を行うことを専らその機能とする装置やプログラムを公衆に提供することは、刑事罰の対象となり、技術的保護手段の回避によって可能となった複製を知らずに行う行為は、私的複製にならないものとされている。</p>
論点3：暗号化されたコンテンツを復号するための鍵の法的な保護について	
検討結果	<p>復号鍵を構成する情報は、事業活動に有益な情報であり、秘密として管理され、公然と知られていないものであるため、不正競争防止法上の「営業秘密」に該当するものと考えられる。よって、復号鍵を構成する情報の不正取得行為や不正開示行為、並びに不正取得行為や不正開示行為が介在されたことを知って又は重大な過失により知らずに行われた当該情報の取得、使用又は開示については、不正競争防止法違反が問題となる。上記の点を勘案すれば、復号鍵自体を不正開示、またはその他の方法による第三者への提供から法的に守るためには、「営業秘密」としての保護や一般の不法行為の法理に頼らざるを得ない。しかし、不正競争防止法は、「事業者間の公正な競争」を確保することを目的とするものであるため、事業者以外の者による行為に対して、どの程度不正競争防止法違反を主張し得るのかを検討する必要がある。</p>

<b>論点4：暗号化されたコンテンツを復号することの著作権法上の意味について</b>	
検討結果	<p>暗号化されたコンテンツ自体が著作物であるとする、復号及び再生の過程で、著作物の複製その他の利用行為があると解される余地がある。しかし、復号及び再生の過程で、ごく一部のデータがRAM上で一時的に蓄積されて順次消去されているに過ぎず、当該復号及び再生によって公衆が当該著作物を視聴できるようにされていないため、現行法上、当該復号及び再生が著作物の利用行為を構成するものと解し難いのではないかと考えられる。</p> <p>従って、マルチメディア情報流通サービスを法制度面でも補完するためには、むしろ暗号化されたコンテンツを復号する過程で行われるバッファリングやRAM上への一時的蓄積を複製ととらえる解釈論又は復号許諾権のような新たな権利を創設する等の立法的な解決も検討すべきものと考えられる。</p>
<b>論点5：暗号化されたコンテンツを違法に復号する行為の法的な意味について</b>	
検討結果	<p>技術的保護手段を回避することを専らその機能とする装置やプログラムを公衆に提供した場合には、著作権法に基づき刑事責任が問われることとなり、また、技術的制限手段により制限されているコンテンツの利用を可能とする機能のみを有する装置やプログラムを提供する行為は、不正競争防止法上の不正競争に該当し、差し止め及び損害賠償請求の対象となる。</p> <p>また、ライセンスを受けていない者が復号する行為が複製行為を構成するものと解することができれば、複製権侵害も問題となる。</p>

## ②プロファイルポータビリティサービス制度検討ワーキング報告書概要

プロファイルポータビリティ制度検討ワーキング報告書の目次を以下に示す。

1. プロファイルポータビリティサービスの定義
2. 制度面からの基本要件
3. プロファイルデータの明確化
4. プロファイルデータの流通方式/データ管理方式
5. 利用者における情報コントロール
6. 実証実験システムについて
7. 課題提起

プロファイルポータビリティサービス制度検討ワーキングでは、プロファイルを有効利用することで、より活性化されたビジネスを形成、促進させること、また、利用者には有益な情報を的確に提供する仕組みを提供することを視野に入れて、その過程で問題となる法的問題の洗い出し、検討を行った。

以下に、全ての議論を網羅するものではないものの、法的問題に関する概要の一端を記載する。

論点1：個人情報の解釈について	
検討結果	<p>個人情報とは「生存する<u>個人に関する情報①</u>であって、当該情報に含まれる氏名、生年月日その他の記述等により<u>特定の個人を識別することができるもの②</u>（<u>他の情報と容易に照合することができ、それにより特定の個人を識別することができること③</u>となるものを含む。）をいう。」</p> <p>立法担当者園田逸夫氏編集「個人情報保護法の解説」によれば、次のように説明されている。</p> <p>①個人に関連する一切の情報であり、きわめて広範囲のもので、個人に関係付けられるものすべてを意味する</p> <p>②特定の個人が識別できることで、名寄せの危険、個人の権利侵害が考えられる。匿名の個人情報の場合には、本人以外通常わからない上、もしそれを含めると、個人情報の範囲が際限なく広がるため、「特定の個人が識別可能なもののみを『個人情報』と定義した。</p> <p>③それ自体としては個人識別性がないが、特別な手間を必要とせず通常の業務で一般的な方法で容易に照合できることを言う。他事業者への特別な照会を必要とする場合、内部でもシステムが異なるなどの事情により技術的に照合が困難な場合には容易に照合できるとは言えない。日常的組織的・経常的に情報交換が行われている場合などは容易に照合できる場合と考えられる。</p>
論点2：プロフィール情報は個人情報か？	
検討結果	<p>プロフィール情報は、購買履歴、サービス利用履歴、事故歴、アンケート回答内容、抽選への応募状況等、顧客としての行動履歴情報が利用されると想定され、個人を特定、識別できる情報（氏名、住所、生年月日、性別）に紐付けられる情報であることから、個人情報と考えられる。</p> <p>①プライバシー問題としての検討</p> <p>履歴を通して個人の行動パターンや志向性、性格的な特徴、趣味嗜好、さらには本人の意識しない興味や関心などについて類型化されてしまうことも考えられる。そのため、収集する情報、解析する手法、利用できる環境などによっては、個人をモニタリングする可能性も生まれてくるため、情報提供者である本人に対して、情報利用の可能性について相当な理解を得られるような努力が必要となると思われる。</p> <p>③センシティブ情報の収集について</p> <p>信用情報や健康情報、医療関連情報、就労関係情報等の個人に関係して知られにくいと強く思われる情報の一群（センシティブ情報）については、個人情報保護法では、現時点では特別な注意義務は課せられていないため、他の個人情報と同様な対応を求めているものと思われる。しかし、事業者はセンシティブ情報の取り扱いについてはさらに慎重になる必要がある。</p>

論点3：プロフィール情報を流通させる場合の法的問題について	
検討結果	<p>①ICチップ購入登録による個人情報の取り扱い</p> <p>個人情報の取り扱いについての厳格な管理体制の確立がもとめられる。</p> <p>②個人情報（プロフィール情報）を事業者が蓄積することの可否</p> <p>本人のみが利用する場合、事業者が利用する場合、他事業者へ提供する場合に分けて、同意の取得方策、消費者への理解方策等を検討する必要がある。</p> <p>③個人情報（プロフィール情報）を、他の事業者に提供する場合の条件</p> <p>ア、原則、合意が必要</p> <p>イ、提供する事業者の例示が必要か</p> <p>新規事業者の参入時の問題や第三者同意の必要性等</p> <p>ウ、提供する事業者の安全管理に関する保証の意味を持つか</p> <p>提供先の事業者からの情報漏洩等についての責任分界の考え方。</p> <p>④決済システムとの関係</p> <p>決済情報の利用に関する規制、ルール等の必要性。</p>
論点4：企業・事業者の負担を軽減するひとつのアイデアの可能性と課題	
検討結果	<p>①プロフィールデータの分散管理手法</p> <p>個人情報とそれに関連する属性情報を分離して、それぞれを第三の番号等を利用して結合する手法。通常の保管利用に際しては、別々のデータベースから参照するという手法とすることで分散管理が可能となる。</p> <p>さらに、利用の側面で安全性を確保する手法として、サービス提供者が、場合によっては、個人情報（特定識別情報）を保持せずに、属性情報と第三の番号情報（個人情報と紐付けられているが、通常は個人を特定できないもの）をのみ持つ方式をとることで安全性を確保したうえで、利用できると考えられる。</p> <p>②個人情報と切り離したプロフィール情報利用の可能性</p> <p>現在の個人情報保護法の視点から見た場合、個人情報を持つことによる開示請求などの対応はきわめて過大な負担となることが予想される。そこで、仮に、個人情報と属性情報を分離することが可能であり、なおかつ、業務として属性情報のみを利用できるビジネス展開であれば属性情報のみを移転させるということも可能になると思われる。</p> <p>この場合のビジネスモデルは、属性情報のみを活用し、個人情報を徹底して削除し利用しない体制を作り上げることで、個人情報保護法の範囲外としての業務が可能となると思われる。新しい可能性であるが、さらに検討の余地がある部分でもある。</p>

## 2. 4 工程管理業務

本事業では、事業スケジュール表にあるような計画に基づいて事業を推進した。その中で、当協会では研究員及びコンソーシアムの事業実施に関する工程管理業務を実施した。

### 2. 4. 1 コンソーシアム定例連絡会議

当協会では、以下の3つのテーマの事業実施に関する進捗管理を行った。

- ①（テーマ種別1）多機能 IC チップドメイン間の相互運用性を確保するための運用管理手法及び管理システムの研究
- ②（テーマ種別2）マルチメディア情報流通等のアプリケーションを活用した多機能 IC チップフレームワークシステムの研究開発及び実効性検証
- ③（テーマ種別3）プロファイルポータビリティサービスに係る開発・実証研究

当協会では、事業の進捗管理を行うために、隔週火曜日にコンソーシアム定例連絡会議を設置し、「スケジュール管理」及び「実施内容の確認」を行った。このコンソーシアム定例連絡会議は、事業期間中に合計15回、主に当協会の会議室において実施した。

結果、研究開発・実証事業は図2-4に示す事業スケジュールの通り実施され、進捗管理業務は一定の成果を上げることができた。

### 2. 4. 2 各コンソーシアムのワーキンググループ等

コンソーシアムでは、テーマ種別毎にワーキンググループ及びサブワーキンググループ等を設置し、事業推進上の個別課題の検討及び進捗状況の確認を行った。当協会では、進捗管理業務の一環として、各テーマ種別毎に設置されるワーキンググループ等への出席を通じて、状況確認を行った。



	2003年							2004年		
	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月
事業全体		△ 7/31 採択候補発表	△ 8/16 契約締結					△ 1/30,31 モニタ 説明会	△ 2/28 実効性検証 完了	△ 3/31 納品
テーマ種別1 相互運用に係る研究開発				フレームワーク モデル検討						
テーマ種別2 マルチメディア情報流通				フレームワーク モデル検討	設計	開発	テスト		実効性検証 ／実証実験	評価・まとめ
テーマ種別3 プロファイルポータビリティ				フレームワーク モデル検討	設計	開発	テスト			評価・まとめ
あり方検討委員会 (有識者)	△ 6/27 第1回			△ 9/29 第2回			△ 12/11 第3回	△ 1/29 第4回		△ 3/19 第5回
技術検討小委員会 (有識者)							△ 12/4 第1回	△ 2/9 第2回		△ 3/8 第3回
制度検討小委員会 (有識者)								△ 1/26 第1回		△ △ 3/9 3/15 第2回第3回
コンソーシアム定例連絡会議							隔週開催			
ワーキンググループ (テーマ種別毎：コンソーシ アム主催)			△	△	△	△	△	△	△	△

図2-4 事業スケジュール

## 2. 5 汎用性向上業務

当協会では、東京工業大学と共同で、多機能 IC チップの汎用性向上のため、「異なるプラットフォームの多機能 IC チップの共通利用に関する調査」を実施した。

本調査は、今後、複数のベンダが異なるプラットフォームで多機能 IC チップの機能が実現される状況下で、プラットフォームが異なっても多機能 IC チップの提供する機能を組み合わせることで共通の機能の実現方策についての調査を行った。

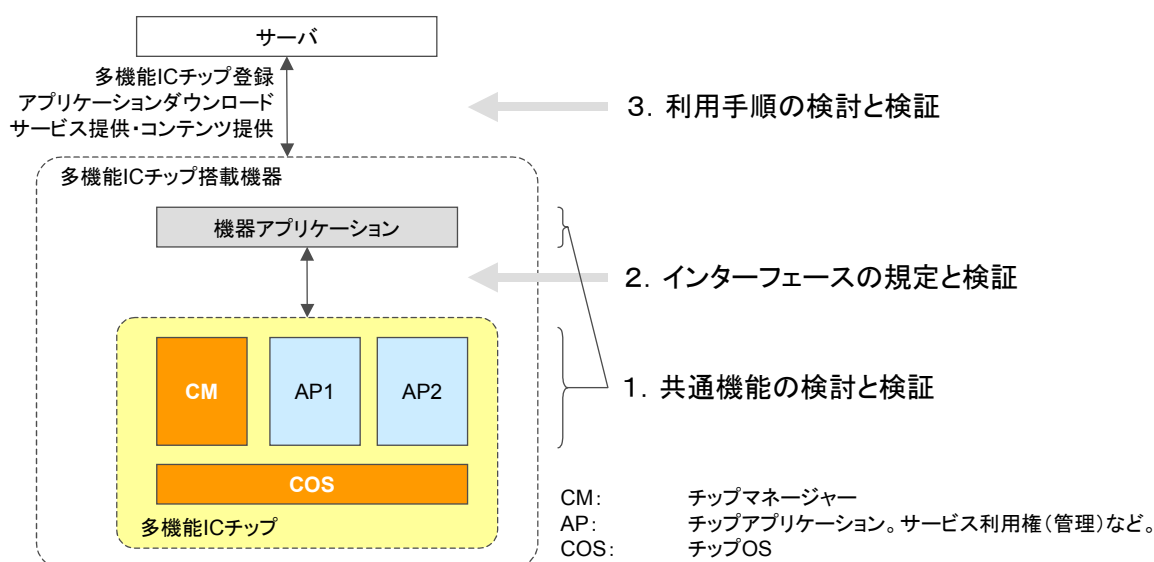


図 2-5 異なるプラットフォームの多機能 IC チップの共通利用に関する調査

### 2. 5. 1 共通機能について

機器本来の機能や提供されるサービスの内容によらず、「サービスの利用権を多機能 IC チップで管理し、当該機器で安全にサービスを実現する」ために必要な機能を、多機能 IC チップの共通機能として抽出・整理した。

多機能 IC チップの共通機能は、機器アプリケーション、チップマネージャ、利用権管理アプリケーションとして位置付けられる。

#### (1) 機器アプリケーションの機能

機器アプリケーションについて、共通に必要な機能を以下に示す。

なお、機器アプリケーションと連動して機器本来の機能を提供する機器インタフェースについては、ユーザインタフェースが機器ごとに異なること、及び外部通信機能はインターネット上の様々な通信プロトコル等を利用することが考えられることから、共通機能として検討の対象とはしない。

表 2-1 機器アプリケーションの共通機能

大機能	中機能	機能概要
チップ制御機能	通信中継機能	APDU の送受信
	AP セレクト機能	利用権管理 AP のセレクト サービスと AID の紐付け
サービス制御機能 (一例)	利用権セレクト機能 (一例)	利用権のセレクト (一例) コンテンツ ID と EF-ID の紐付け (一例)

(2) チップマネージャの機能

多機能 IC チップの状態管理の詳細な方法は、多機能 IC チップの OS 等実装方法によって異なるため、共通機能として整理することは現時点では困難であるが、サービス側から見た CM の機能はできる限り共通機能とし、アプリケーションの開発者がチップの違いを意識する必要性が生じる範囲ができる限り小さくなることが望ましい。チップマネージャが共通に持つべき機能を以下に示す。

表 2-2 チップマネージャの共通機能

大機能	中機能	機能概要
認証機能	証明書アクセス機能	CM 鍵証明書の読み出し
	相互認証機能	内部認証 チャレンジコードの生成 証明書検証 外部認証
AP 管理機能	AP 管理機能	AP の状態管理 (ロード、(停止、Active)、 削除)
SM 鍵設定機能	SM 鍵設定機能	セキュアメッセージング用セッション鍵 格納
SM 通信機能	CM 鍵格納機能	セキュアメッセージングで送られてきた チップマネージャ鍵を登録する
	APDL 機能	セキュアメッセージングによって取得 したアプリケーションをメモリ領域内 にダウンロードする

### (3) 利用権管理アプリケーションの機能

利用権管理アプリケーションの機能はサービスによって異なると考えられるが、機器アプリケーションやサーバが利用者にサービスを提供するために必要な情報を安全に確保し、必要な際に取り出すという点では、共通の機能を持つと考えられる。利用権管理アプリケーションが共通に持つべき機能について以下に示す。

表 2-3 利用権管理アプリケーションの機能

大機能	中機能	機能概要
認証機能	証明書アクセス機能	利用権管理 AP 公開鍵証明書の読み出し
	相互認証機能	内部認証 チャレンジコードの生成 証明書検証 外部認証
SM 鍵設定機能	SM 鍵設定機能	セキュアメッセージング用セッション鍵の格納
SM 通信機能	AP パーソナライズ機能	利用権管理 AP 秘密鍵の格納 利用権管理 AP 公開鍵証明書の格納
	利用権格納機能	要素 ID 及び利用権の格納
サービス連携機能 (例)	利用権管理機能	利用権管理 AP 内部からの利用権の読み出し/利用権によるコンテンツ復号化 (例)

## 2. 5. 2 インターフェースの規定

共通機能として抽出した機能では、製造者ごとの違いがあることが自明となっているアプリケーションダウンロード機能と、多機能チップとネットワーク接続先との APDU の送受信を中継する機器アプリケーションの機能以外は、IC カードに対するコマンドと同様のコマンド例として位置付けることができる。

なお、機器アプリケーションのサービス制御機能及びチップマネージャのアプリケーションダウンロード機能は、以下の理由によりインターフェース検討の対象としていない。

- 利用権管理アプリケーションに対する機能であり、サービスごとに必要とされる機能が異なる
- アプリケーションのダウンロード方式が現状、多機能 IC チップの製造ごとに異なる

表 2-4 機器アプリケーションにおける共通機能のインタフェース

大機能	中機能	機能	コマンドまたは I/F
チップ制御機能	通信中継	APDU の送受信	TransAPDU (CmdAPDU, ResAPDU)
	AP セレクト機能	AP セレクト	SELECT FILE
サービス制御		(対象外)	(対象外)

表 2-5 チップマネージャにおける共通機能のインタフェース

大機能	中機能	機能	コマンド
認証機能	証明書アクセス機能	CM 鍵証明書の読み出し	GET DATA/READ
	相互認証機能	内部認証	INTERNAL AUTHENTICATE
		チャレンジコードの生成	GET CHALLENGE
		公開鍵証明書の検証	VERIFY CERTIFICATE
		外部認証	EXTERNAL AUTHENTICATE
AP 管理	AP 管理機能	AP のダウンロード	APPROVE APPLICATION/LOAD APPLICATION
		AP の停止	DEACTIVATE APPLICATION
		AP の活性化	ACTIVATE APPLICATION
		AP の削除	REMOVE APPLICATION
SM 鍵設定	SM 鍵設定機能	SM 用鍵の格納	PUT DATA
SM 通信	CM 鍵格納機能	CM 鍵の格納	CHANGE REFERENCE DATA
	APDL 機能	AP のダウンロード機能	(対象外)

表 2-6 利用権管理アプリケーションにおける共通機能のインタフェース

大機能	中機能	機能	コマンド
認証機能	証明書アクセス機能	CM 鍵証明書の読み出し	GET DATA/READ
	相互認証機能	内部認証	INTERNAL AUTHENTICATE
		チャレンジコードの生成	GET CHALLENGE
		証明書検証機能	VERIFY CERTIFICATE
		外部認証機能	EXTERNAL AUTHENTICATE
SM 鍵設定	SM 鍵設定機能	SM 用鍵格納機能	PUT DATA
SM 通信	AP パーソナライズ機能	利用権管理 AP の秘密鍵の格納	CHANGE REFERENCE DATA
		利用権管理 AP の公開鍵証明書の格納	PUT DATA
	利用権格納機能	要素 ID 及び利用権の格納	PUT DATA
サービス連携機能 (一部)	利用権管理機能	利用権の読み出し(例)	GET DATA (例)

### 2. 5. 3 利用手順について

サービス利用までの段階について、サービス利用までの手続きの段階と処理フェーズについて、以下のように整理し、利用手順を検討した。

表 2-7 サービス利用までの段階と処理フェーズ

手続きの段階	処理フェーズ
機器購入	(処理フェーズなし)
機器登録	機器登録
サービス利用申請	サービス利用登録
サービス申込	要素登録
	利用権取得
サービスの利用	サービス利用

以下に機器登録についてのイメージとそのシーケンスを示す。

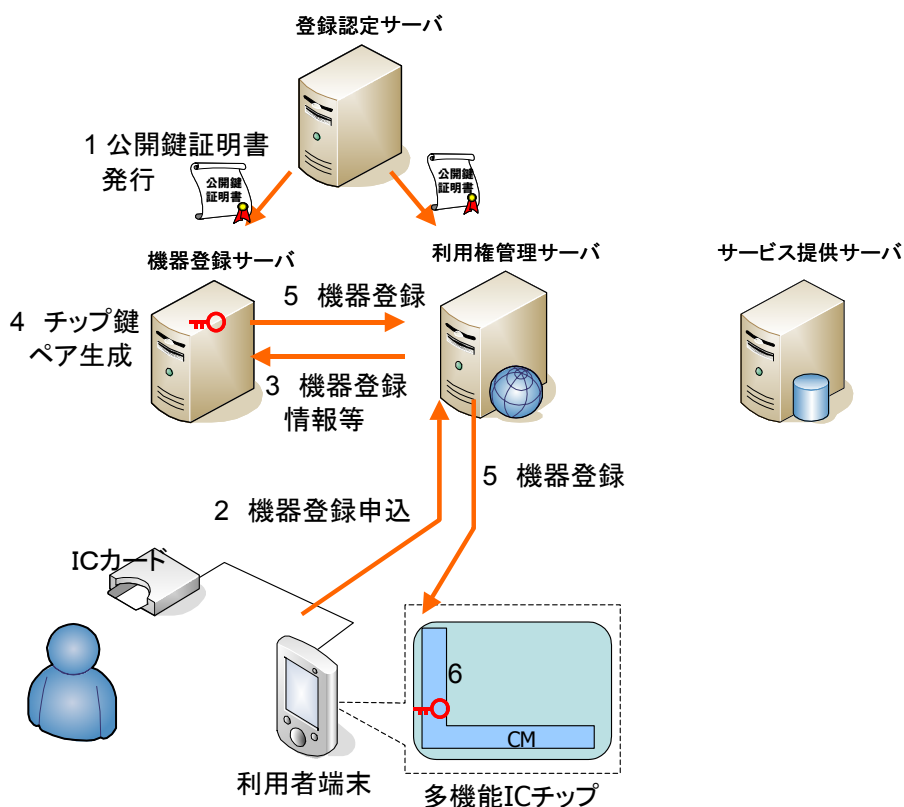


図 2-6 機器登録のイメージ

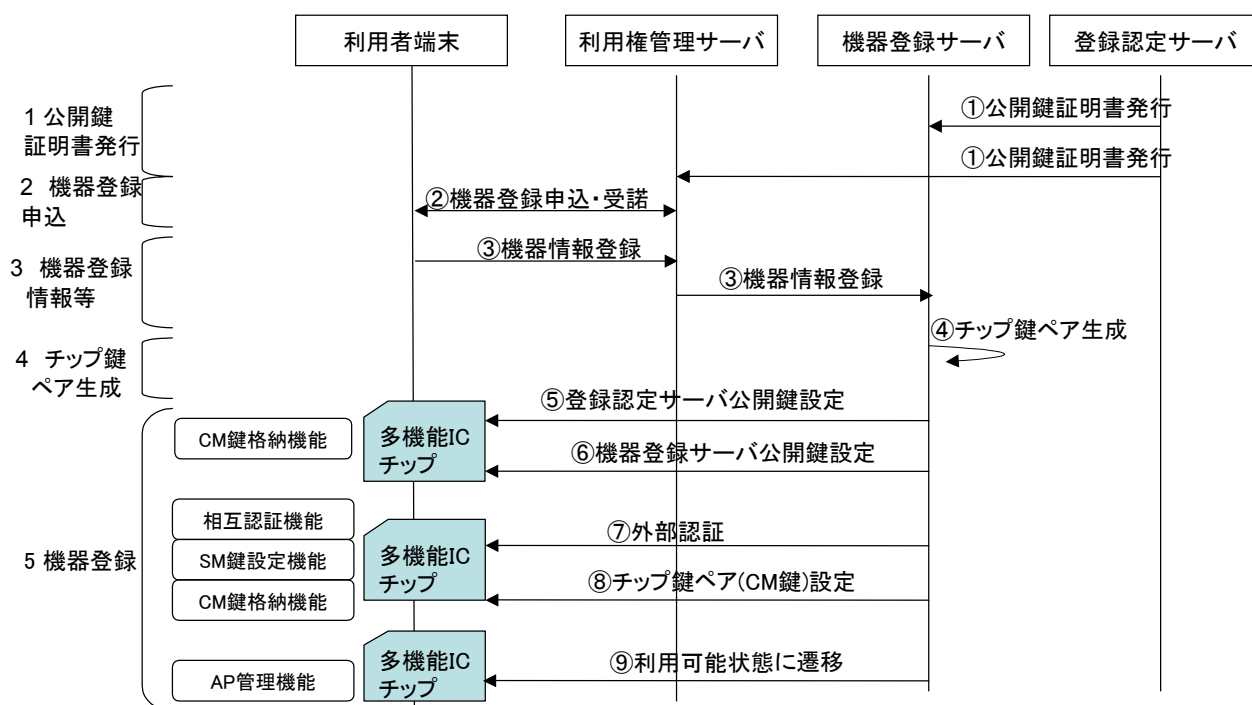


図 2-7 機器登録のシーケンス

## 2. 5. 4 本研究の展望

### (1) 多機能 IC チップ搭載機器の実現と普及

多機能 IC チップは、機器に組み込まれることによって機器の機能等の属性を保証し、機器内の耐タンパ製の高い部品として利用権を管理することによって、ネットワークを通じて提供されるサービス等でのセキュリティを確保することを目的としている。しかしながら、本研究の実施時点で、この目的を満たす状態で多機能 IC チップを搭載した機器は普及しておらず、研究開発・実証事業における実効性検証や実証実験も、PC にリーダーライターを通じて IC カードを接続してのシミュレーションや、多機能 IC チップの一部機能を持つ IC チップを利用した機能面やサービス面の検証、実証を行っている状況である。

今後、多機能 IC チップによるサービスを本格的に実現・普及するためには、これまでの実効性検証や実証実験で行われてきた取り組みに加えて、多機能 IC チップ搭載機器そのものの実現を図るための研究開発が必要であると考えられる。

### (2) セキュリティの実現方法

多機能 IC チップを搭載する機器としては、マルチメディアコンテンツの再生、e-ラーニング、ネットワーク接続などが想定されるが、実際にはサービスごと、機器ごとに、要求されるセキュリティの強度は異なる。従って、共通機能についても、一部の機能については具体的な実装に幅を持たせ、サービスごとに実装方法を規定することも検討に値すると思われる。ただし、その場合の相互運用性の確保には留意が必要である。

### (3) 機器アプリケーションと多機能 IC チップのインタフェース

本研究では、機器アプリケーションと多機能 IC チップの間のインタフェースについては、ISO/IEC 7816-4 に規定される IC カードのコマンド・レスポンスを前提として検討を行ってきた。しかしながら、機器に実装する場合、多機能 IC チップは IC カードと異なり、チップの大きさについてカード形状の制約を受けないため、電力消費や通信バッファにおいて従来の IC カードの実装面での制約を受けない。このため、コマンドの送受信方法においては、IC カードよりも効率の良い方法を採用することが期待される。

### (4) 機能・性能の保証

多機能 IC チップには、機器の機能・性能を保証する役割を持つことが期待されるが、そのための実装方法については、今後検討が必要である。これまでの認証機能やマルチアプリケーションの実現といったソフトウェア的な観点だけでなく、機器本体へのソフトウェア、ファームウェア、さらにはハードウェア、配線といったレベルでの改造を検知し、サービスにおけるサービス提供者の権利や利用者の自由な活用が保護されるような仕組みを維持できなければ、実際のサービスへの導入・普及は困難なものとなってしまふと懸念される。

### (5) サービスと機器の普及

多機能 IC チップを活用したサービスは、従来の、セキュリティ機能あるいはサービスの使い勝手に制約の多いサービスと競合する関係になることも予想される。多機能 IC チップを活用したサービスの普及は多機能 IC チップ搭載機器の普及に伴うことになるため、サービスと機器が相互に普及する関係にならなければ、機器が普及していない→サービスの利用者が増えない→消費者の機器購入のモチベーションが喚起されない、といった関係で、多機能 IC チップの普及を阻害する要因になってしまう事態も懸念される。サービスの実現と普及にあたっては、当初には従来機器を利用した限定的なサービスを提供するなど柔軟な運用も検討すべきであると考えられる。



## 第Ⅱ編 研究開発・実証事業の実施報告

# 1. 多機能 I C チップ等を活用した新領域 I T サービスに関する 研究開発・実証事業の概要

---

## 1. 多機能 ICチップ等を活用した新領域 ITサービスに関する研究開発・実証事業の概要

### 1. 1 背景

近年、デジタル家電を始めとする電子機器がインターネットに接続されることで新たな展望や課題が見られるようになってきている。例えば、外出先からでも家庭の電子機器に接続することが可能となることで新たなビジネスモデルの創発が期待される一方で、その基盤要素としてネットワーク接続機器の安全確実な利用のための認証が必要不可欠なものとなっている。

経済産業省が平成 14 年度に実施した「地域情報化及びその基盤整備要素技術等に関する調査研究事業」では、「多機能 IC チップフレームワーク検討委員会」において、ネットワーク上で人や機器の認証や権利の保証を実現するための手段としての多機能 IC チップの有効性並びに多機能 IC チップの利用分野ニーズ及びその運用フレームワークについての方向性について検討し、取りまとめたところである。

### 1. 2 目的

平成 15 年度「多機能 IC チップ等を活用した新領域 IT サービスに関する研究開発・実証事業」では、安全で安心できる社会基盤としての多機能 IC チップインフラを確立するとともに、それを活用した新領域 IT サービスの実証実験により、システム導入に伴う技術面・利用面での課題を検証し、官民間問わずその成果を広く活用することを目的とし、多機能 IC チップフレームワークシステムの研究開発・実証実験を実施した。

### 1. 3 事業概要

本事業では、テーマ種別 1 からテーマ種別 3 の三つのテーマ種別に係わる研究、開発、実効性検証並びに実証実験を行い、多機能 IC チップ等を活用した新領域 IT サービスの実現を図るとともに、当該 IT サービスが近い将来に普及するための技術面、利用面の要件について整理する。

テーマ種別 1 では、多機能 IC チップフレームワークにおいて、多機能 IC チップが発行された IC チップドメインと異なるドメインにおいて多機能 IC チップにチップアプリケーションをロードし、サービスを利用するための運用管理手法及び管理システムについて研究を行った。

テーマ種別 2 では、多機能 IC チップフレームワークを利用してマルチメディア情報流通サービスや会員権サービスの利用権を管理するための仕組みを開発し、多機能 IC チップフレームワークを基礎としたサービスモデル構築の観点から実効性の検証を行った。新領域 IT サービスの実現の観点では、マルチメディア情報流通サービスについて、サービスとしての有効性について検証した。なお、会員権サービスについては、この観点についての実効性検証をテーマ種別 3 で実施した。

テーマ種別 3 では、多機能 IC チップフレームワークに基づくプロファイル・ポータビリティサービスの本格的な実用化に向けて、実際の事業環境に近いフィールドにて実証実験を

行い、実現状況や課題等について評価した。  
実施内容の構成について図1-1に示す。

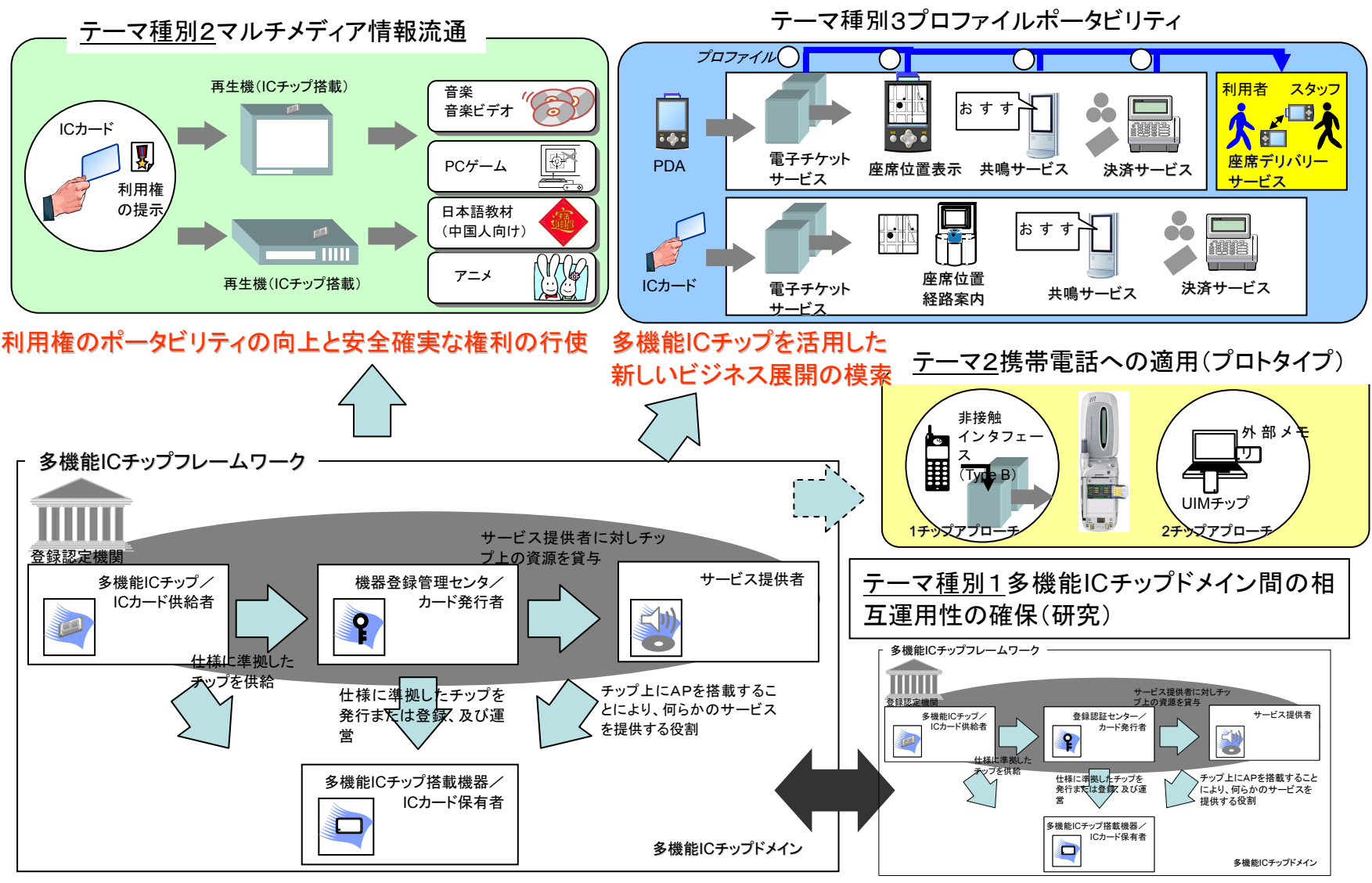


図1-1 事業全体概要

本事業のテーマ種別と実施内容について表 1 - 1 に示す。

表 1 - 1 本事業のテーマ種別と実施内容の対比

テーマ種別	実施テーマ	実施内容
1	多機能 IC チップドメイン間の相互運用性を確保するための運用管理手法及び管理システムの研究	<ul style="list-style-type: none"> <li>多機能 IC チップドメイン間でのチップアプリケーションのダウンロード及びサービスの利用を実現するための運用管理手法及び管理システムの研究</li> <li>利用者にとって、チップが発行されたドメインを意識することなくアプリケーションを追加して新たなサービスを利用開始できる環境を整備する方法を研究する</li> </ul>
2	多機能 IC チップフレームワークを利用したマルチメディア情報流通等の実効性検証	<ul style="list-style-type: none"> <li>多機能 IC チップフレームワークの利用によるマルチメディア情報流通サービスの枠組みの検討</li> <li>多機能 IC チップフレームワークによる PKI 技術の活用により、事業者と利用者双方の権利を確保するマルチメディア情報流通サービスを検討する</li> </ul>
		<ul style="list-style-type: none"> <li>マルチメディア情報流通サービスを実現する利用権管理基盤の研究開発及び実効性検証</li> <li>利用者と機器の双方が持つ多機能 IC チップの活用により、利便性と安全性の高い仕組みを開発・検証する</li> </ul>
		<ul style="list-style-type: none"> <li>多機能 IC チップフレームワークを活用した会員権サービスの研究開発及びサービスモデル構築の観点での実効性検証</li> <li>多機能 IC チップフレームワークを活用し、PKI を活用して各種サービスを追加して会員権サービスに応用する仕組みを開発・検証する</li> </ul>
		<ul style="list-style-type: none"> <li>多機能 IC チップフレームワークの携帯電話への適用の検討</li> <li>非接触 IC チップを搭載した携帯電話のプロトタイプを開発し、多機能 IC チップフレームワークへの適用を検討する。</li> </ul>
		<ul style="list-style-type: none"> <li>携帯電話上の多機能 IC チップを想定したサービス提供システムの研究開発及び検証</li> <li>多機能 IC チップフレームワークの携帯電話向けサービスへの適用可能性及び課題について、プロトタイプ的な検証環境構築を通じて検討する</li> </ul>
3	プロフィールポータビリティサービスに係る研究開発・実証実験	<ul style="list-style-type: none"> <li>プロフィールポータビリティサービス用チップを用いた多機能 IC チップフレームワークの実現方法の研究</li> <li>大容量メモリ型多機能 IC チップを多機能 IC チップフレームワークに適用するための技術的課題及び解決方法について検討する</li> </ul>
		<ul style="list-style-type: none"> <li>複数種の IC チップを活用したプロフィールポータビリティサービスに係る実証実験</li> <li>イベント会場での電子チケット、物品販売等のサービスを、大容量メモリ型多機能 IC チップを挿入した PDA 端末と非接触 IC カードによって実現を図る</li> <li>プロフィールポータビリティサービスの実現に向けた事業性について評価する</li> </ul>

## 1. 4 実施体制

事業の全体実施体制図を図1-2、テーマ種別1の実施体制図を、テーマ種別2の実施体制図を、テーマ種別3の実施体制図をに示す。

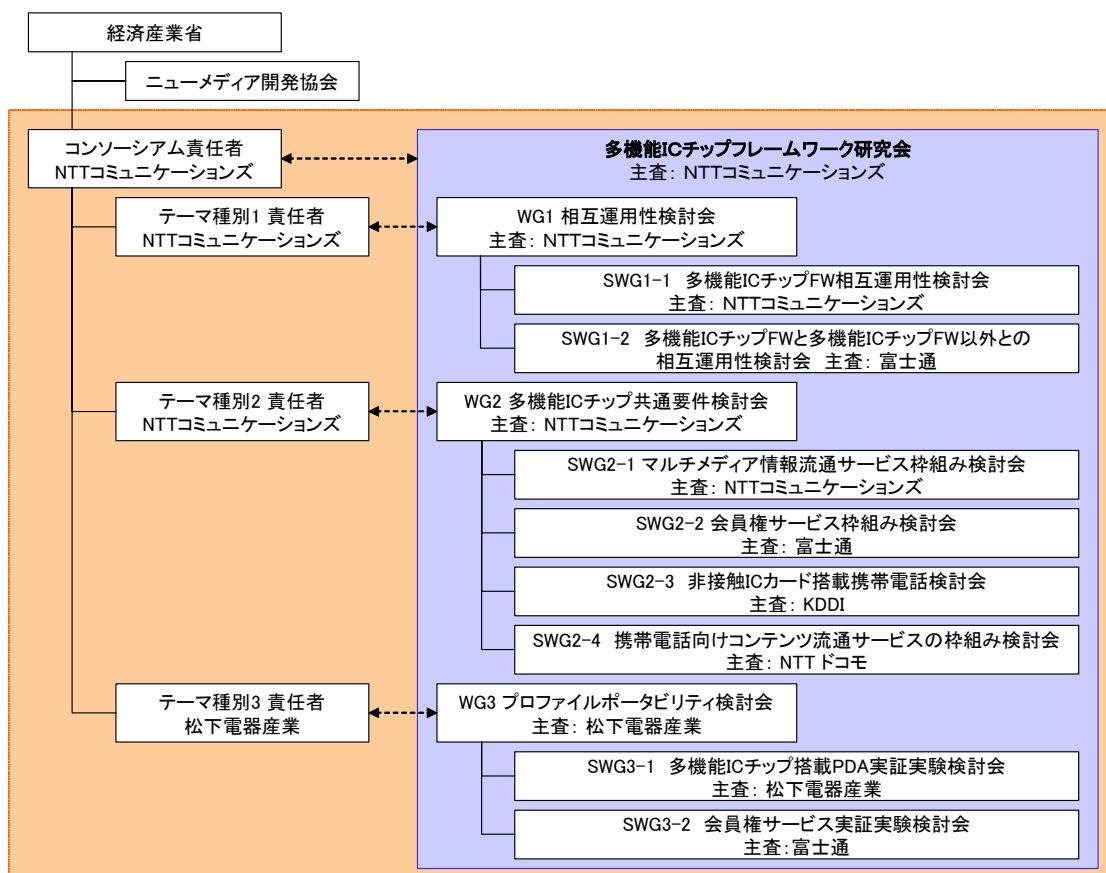


図1-2 事業全体の実施体制図

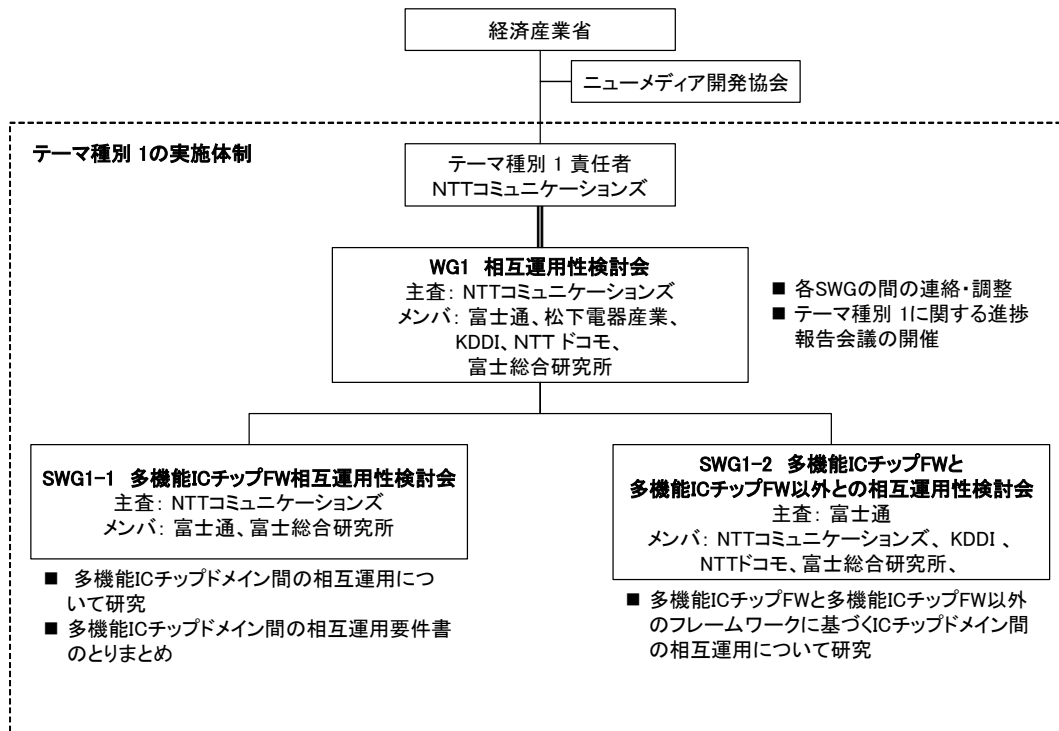


図 1-3 テーマ種別 1 の実施体制図

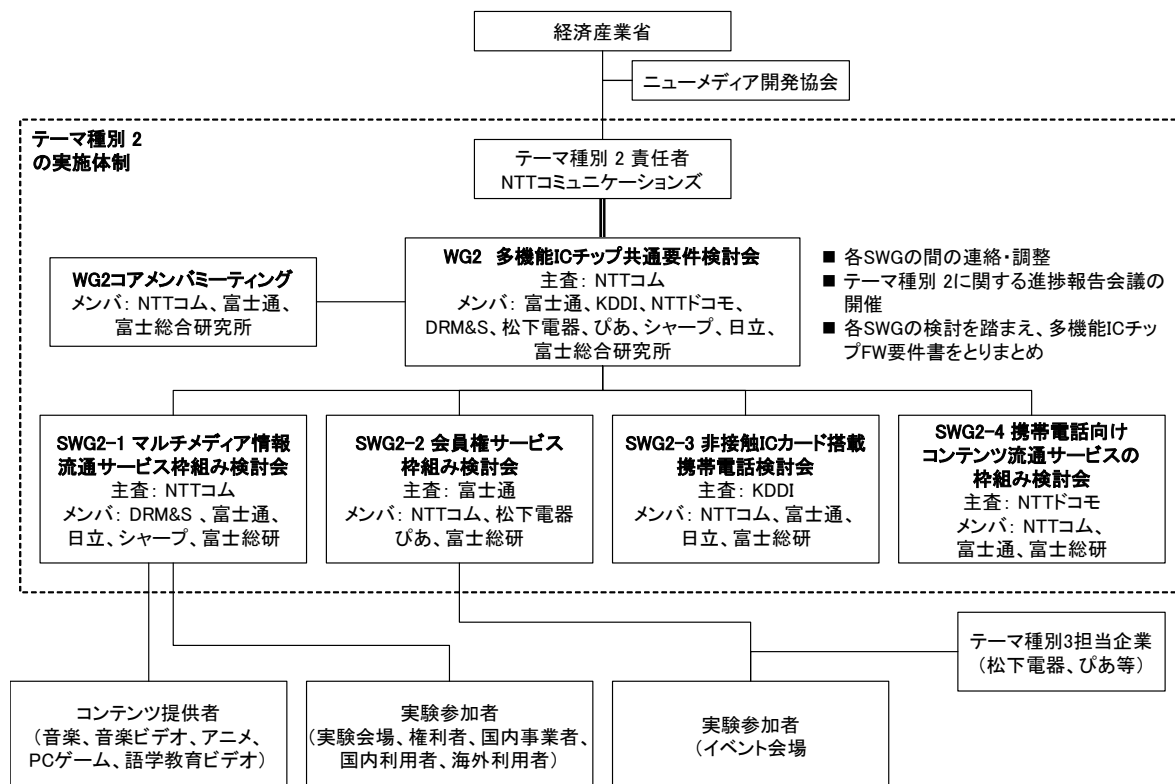


図 1-4 テーマ種別 2 の実施体制図

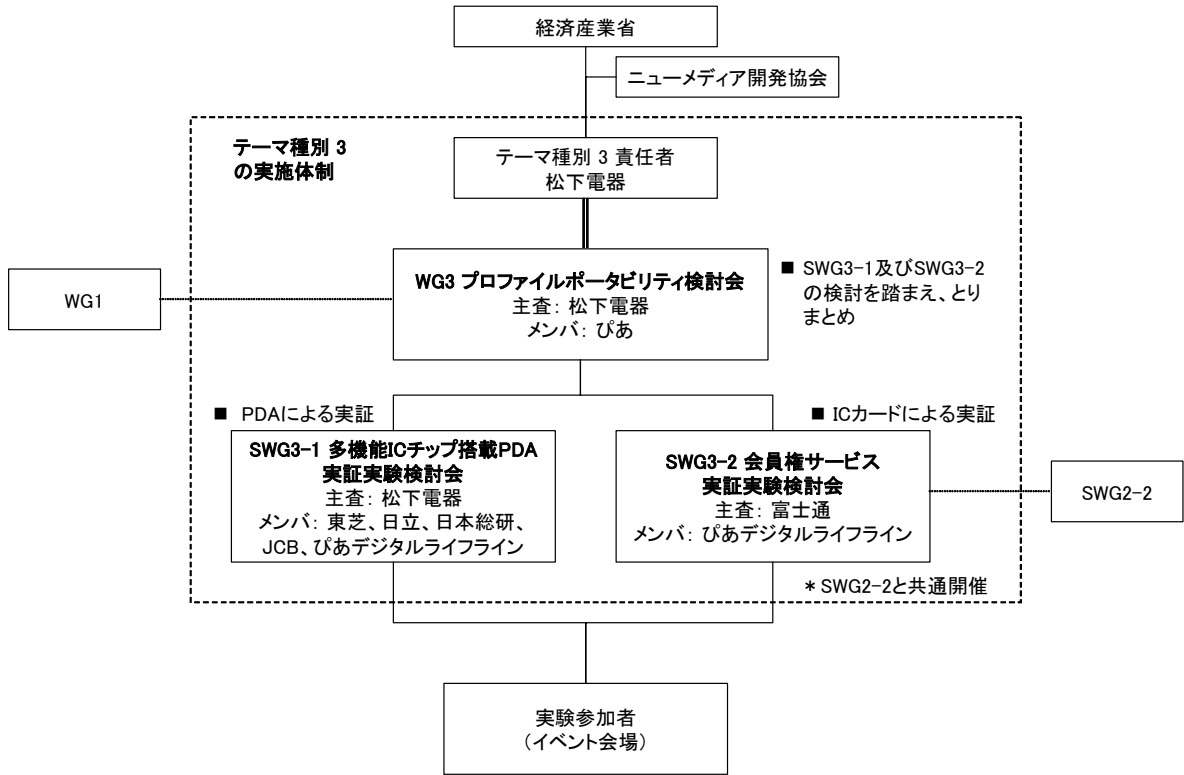


図 1 - 5 テーマ種別 3 の実施体制図



## 第Ⅱ編 研究開発・実証事業の実施報告

### 2. テーマ種別1

---

## 2. テーマ種別 1

### 2. 1 事業概要

#### 2. 1. 1 背景

多機能 IC チップフレームワークでは、「登録認定機関（RC : Registration Center（以下「RC」という。））」に登録された多機能 IC チップを活用できる有効な範囲を「多機能 IC チップドメイン（以下「ドメイン」という。））」と呼ぶ。RC は多機能 IC チップの発行主体や中立の第三者機関によって運用され、多機能 IC チップのさまざまな利用形態やビジネス上の要請に応じて複数の異なるドメインが並立して運営されることが想定される。このような状況においては、ドメイン間同士の相互運用性を確保し、あるドメインで発行された多機能 IC チップが異なるドメインで提供されているサービスを受けられるようにすることが求められるようになる。

一方、携帯電話やメモリカード等の分野においては、それぞれの要件に対応した IC チップフレームワークに基づくサービスが既に運用されている。このような、既に異なる IC チップフレームワークで提供されているサービスが、多機能 IC チップフレームワークに準拠した機器や多目的 IC カードなどで利用できるようになることで、多機能 IC チップを活用したサービス領域の拡大につながることを期待される。逆に、多機能 IC チップフレームワークに則ったサービスを携帯電話等の異なる IC チップフレームワークを基盤とした機器やカードで受けられるようにすることで、より多様なサービス提供者が多機能 IC チップを活用したサービス基盤に参入できるようになる。

#### 2. 1. 2 目的

以上のような背景のもと、複数の IC チップのドメインが存在する環境下を想定し、異なるドメインにおいて提供されるサービスを他のドメインで発行された多機能 IC チップ搭載機器が利用可能となるようなドメイン間の相互運用を実現するための方式ならびにその要件について検討した。

#### 2. 1. 3 事業概要

本事業テーマ種別 1 の研究内容は大きく以下の 2 つのテーマについて研究を行った。

- ① NICSS フレームワーク（次世代 IC カードシステム研究会（NICSS : New Generation IC Card System Study Group）が定めた次世代 IC カードのためのフレームワーク）のコンセプトに基礎を置く多機能 IC チップフレームワークのドメイン間の相互運用を想定し、NICSS フレームワークベースの既存プロダクト間での相互運用を実現するための可能な方式について検討した。

②既に活用されている IC チップを搭載した携帯電話やセキュリティ機能付メモリーカード等については、Global Platform (GP) や、第三世代携帯電話に利用されている UIM (User Identity Module) のプラットフォームを挙げることができる。このような多機能 IC チップフレームワークとは異なるプラットフォームに基づく IC チップドメインと多機能 IC チップフレームワークのドメインとの相互運用性を実現するための課題と実現可能性について研究を行った。

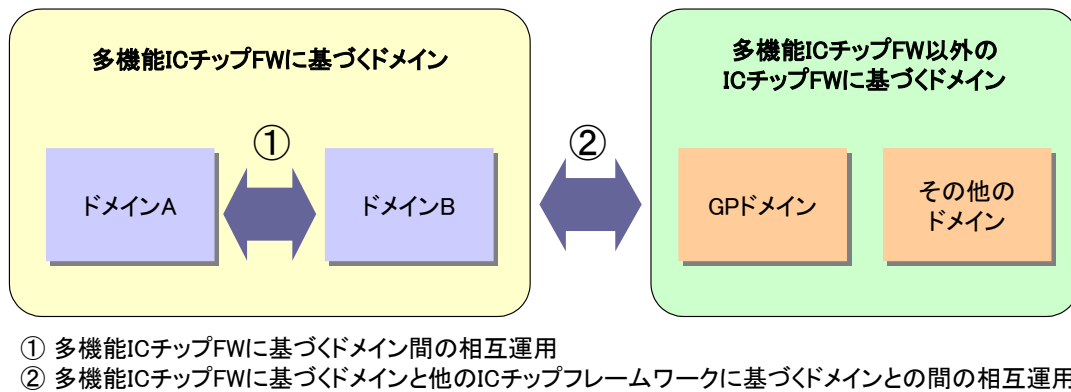


図 2-1 テーマ種別 1 における研究の全体図

(1) 本事業テーマ種別 1 の検討におけるドメイン間の相互運用の位置づけ

① 「多機能 IC チップドメイン」について

「多機能 IC チップドメイン」とは、多機能 IC チップフレームワークにおける登録認定機関 (RC) に登録された IC チップを活用できる有効な範囲と定義される。実質的には、「機器登録管理センタ (CR)」が属している RC 管理下で運用されるサービスの実体 (範囲) と捉えることができる。

本テーマ種別においては、多機能 IC チップフレームワーク以外の IC チップフレームワークについても考慮し、ドメインを「IC チップに対するオペレーションにおいてセキュリティが確保されている範囲 (安全性が確認できる範囲)」であると再定義した。

② 「相互運用」について

本テーマ種別における相互運用の検討範囲は「CH が、あるドメインで発行・登録された CE に、他のドメインでサービスに供されている AP を安全にダウンロード及び削除ができること」とした。

## (2) 略語一覧

以下に、本報告書で使用されている略語を示す。以下本文では、各用語は略語にて表記する。

- 3GPP (3rd Generation Partnership Project)
- 3GPP2 (3rd Generation Partnership Project 2)
- AID (Application Identifier) : アプリケーション識別子
- AP\_ID (Application Program Identifier) : アプリケーションプログラム識別子
- APP (AP Provider) : アプリケーション提供者
- APRC (AP Registration Center) : 共通 AP 登録認定機関
- BRC (Bridge RC) : ブリッジ RC
- BRC\_ID (Bridge RC Identifier) : ブリッジ RC 識別子
- CE (Chip embedded Equipment) : 多機能 IC チップ搭載機器
- CE\_ID (Chip embedded Equipment Identifier) : 機器登録識別子
- CH (CH : Chip embedded equipment Holder) : 保有者 (利用者)
- CM (Card Manager) : カードマネージャ
- CR (Chip embedded equipment Registry) : 機器登録管理センタ
- CR\_ID (Chip embedded equipment Registry Identifier) : 機器登録管理センタ識別子
- CRL (Certificate Revocation List) : 証明書失効リスト
- CS (Chip Supplier) : IC チップ供給者
- ETSI (European Telecommunications Standards Institute)
- GP (Global Platform)
- MOPASS (Mobile PassPort)
- MAM (Multi Application Management System)
- NICE (Network-based IC Card Environment)
- NICSS (the Next generation Ic Card System Study group) : 次世代 IC カードシステム研究会
- RC (Registration Center) : 登録認定機関
- RC\_ID (Registration Center Identifier) : 登録認定機関識別子
- SIM (Subscriber Identity Module)
- SP (Service Provider) : サービス提供者
- SP\_ID (Service Provider Identifier) : サービス提供者識別子
- UICC (Universal IC Card)
- UIM (User Identity Module)

## 2. 2 多機能 IC チップフレームワークに基づくドメイン間の相互運用に関する検討

### 2. 2. 1 概要

多機能 IC チップドメイン間の相互運用に関わる要件について検討した。本研究事業での検討範囲は、特に「利用者が、あるドメインで発行・登録された多機能 IC チップに、他のドメインでサービスに供されているアプリケーションを安全にダウンロード、および削除ができること」を実現するための機能要件、運用要件、セキュリティ要件についての研究に限定するものとする。すなわち、本章においては「相互運用範囲内にある、すべての多機能 IC チップフレームワークに基づくドメインに登録された SP から、すべてのドメインの機器にアプリケーションが安全・確実にダウンロード・削除できること」が実現目標であり、これは実質的に「相互運用範囲内のすべてのドメインの SP と、すべてのドメインの CR、CE とが相互認証できること」と考えることができる。

本研究は以下のステップに従って実施した。

- ・ ステップ 1：多機能 IC チップフレームワークを実現しているプラットフォームに関する調査
- ・ ステップ 2：ドメイン間相互運用の概念モデルの検討
- ・ ステップ 3：多機能 IC チップに基づく多機能 IC チップドメインの相互運用に関する相互運用要件の検討

### 2. 2. 2 NICSS フレームワークを実現しているプラットフォームに関する調査

「平成 12 年度 IC カードの普及等による IT 装備都市研究事業（以下「IT 装備都市研究事業」という。）」で開発したプロダクトでの相互運用実現性を検討するが、最初のステップとしてそれぞれのプロダクトで実装面について違いがあるかどうかについて、調査を行った。具体的には各プロダクトの基本となるプレーヤ構成、証明書の発行方法について調査、比較した。

調査結果からは、各プロダクトのプレーヤモデルについて、どちらのプラットフォームも NICSS 要件書に準拠しているため、各プレーヤ間の認証方法に大きな差異は認められない。AP 搭載許可証については IT 装備都市研究事業の際に規定しており、各プロダクトとも同じインタフェースを実装している。このことから、プレーヤモデル、認証の論理的な構成に相互運用を阻害する程の差分はないと考えることができる。

以降の相互運用についての検討では、AP ダウンロードに関わる 4 つのプレーヤに注目して検討を行った。

- ・ 登録認定機関 (RC)
- ・ 機器登録管理センター (CR)
- ・ サービス提供者 (SP)
- ・ 保有者/利用者 (CH)、機器 (CE)

## 2. 2. 3 ドメイン間相互運用の概念モデル

### (1) ドメイン間相互運用の概念モデル案

「相互運用範囲内のすべてのドメインの SP と、すべてのドメインの CR、CE との間で相互認証ができること」という観点から以下の①～⑤の 5 つのモデル案を抽出し、検討を行った。

#### ① 厳密な階層構造モデル案 (Strict-Hierarchy)

全ドメインの信頼点 (信頼の基点となる登録認定機関) となるルート RC (RRC) を設立し、RRC が各ドメインの RC へ公開鍵証明書を発行することにより、RC を階層化して相互運用を行うモデル案。

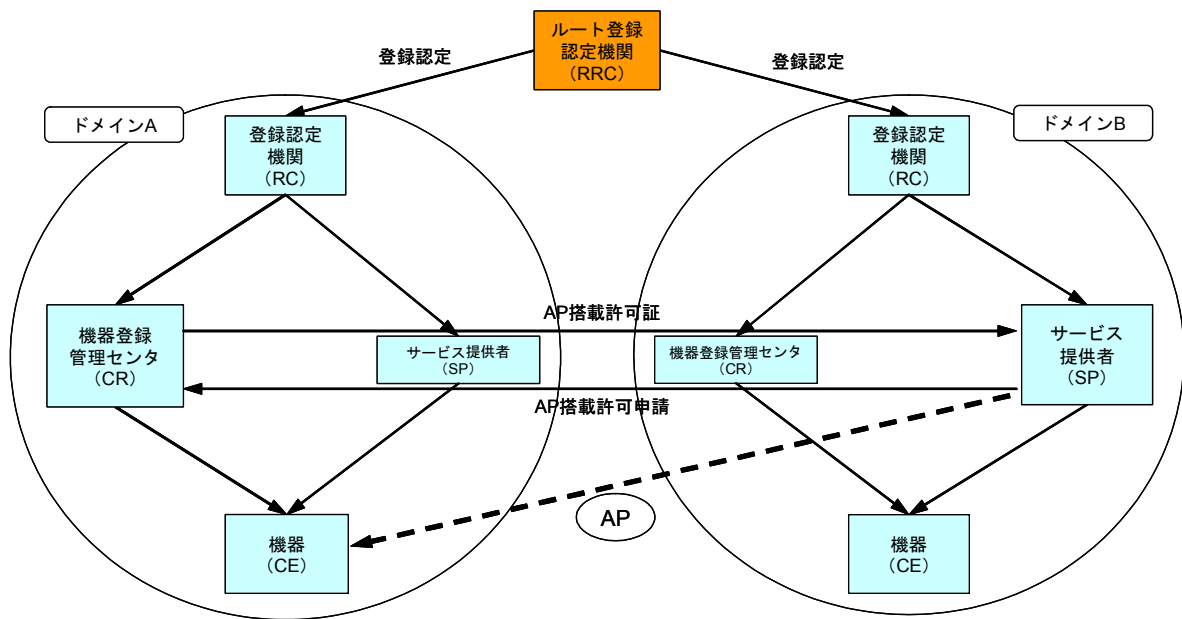


図 2-2 厳密な階層構造モデル案

②相互認証モデル案 (Cross-Certification)

各ドメインの RC 同士が証明書を発行し合うことにより相互運用を行うモデル案。

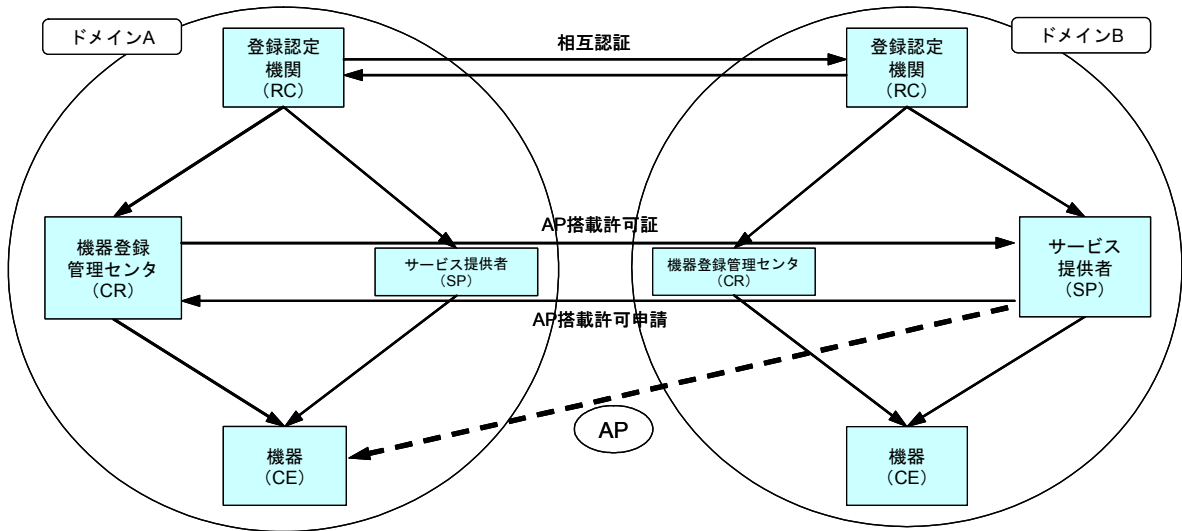


図 2-3 相互認証モデル案

③ブリッジ RC モデル案 (Bridge RC)

各ドメインの RC 同士の相互認証の中継点としてブリッジ RC (BRC) を設立し、BRC と各 RC が証明書を発行し合うことにより相互運用を行うモデル案。

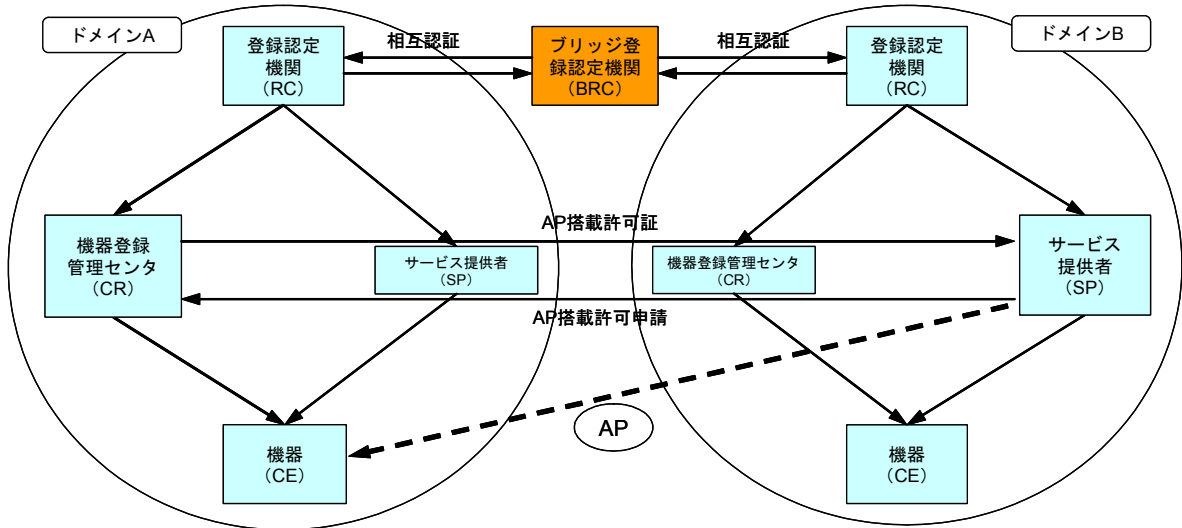


図 2-4 ブリッジ RC モデル案

④CR 相互認証モデル案 (CR Cross-Recognition)

CE の登録先である CR が他ドメインの RC へ登録することにより相互運用を行うモデル案。

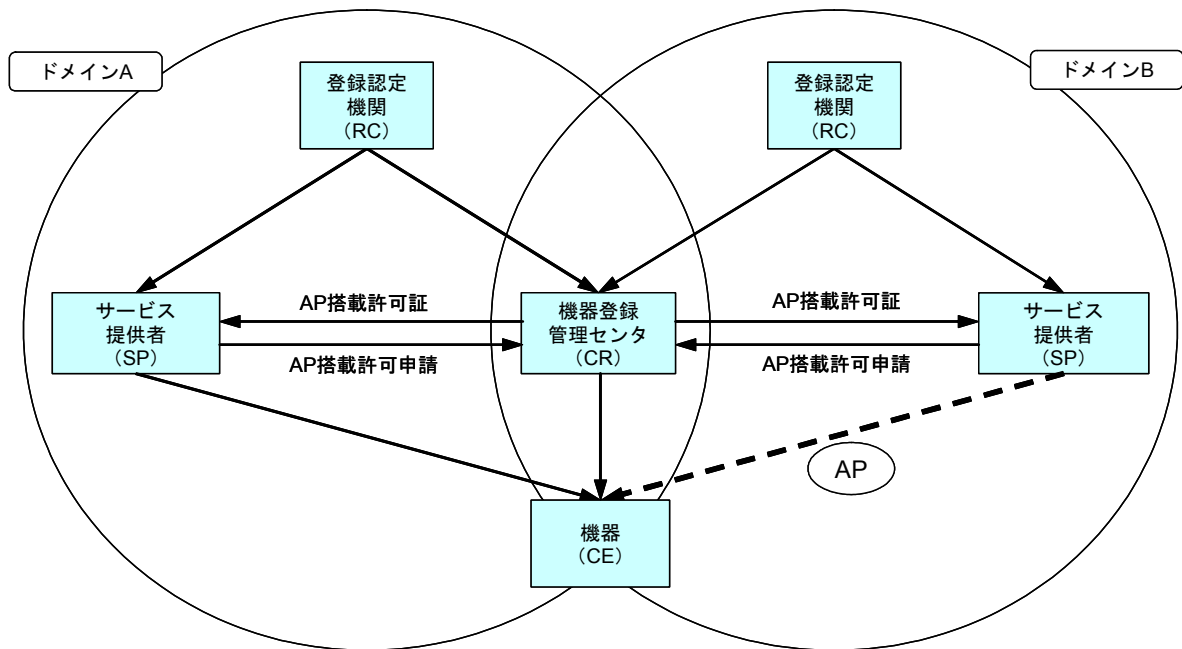


図 2-5 CR 相互認証モデル案

⑤SP 相互認証モデル案 (SP Cross-Recognition)

その AP を提供している SP が、CE の登録先である CR の属するドメインの RC へ登録することにより相互運用を行うモデル案

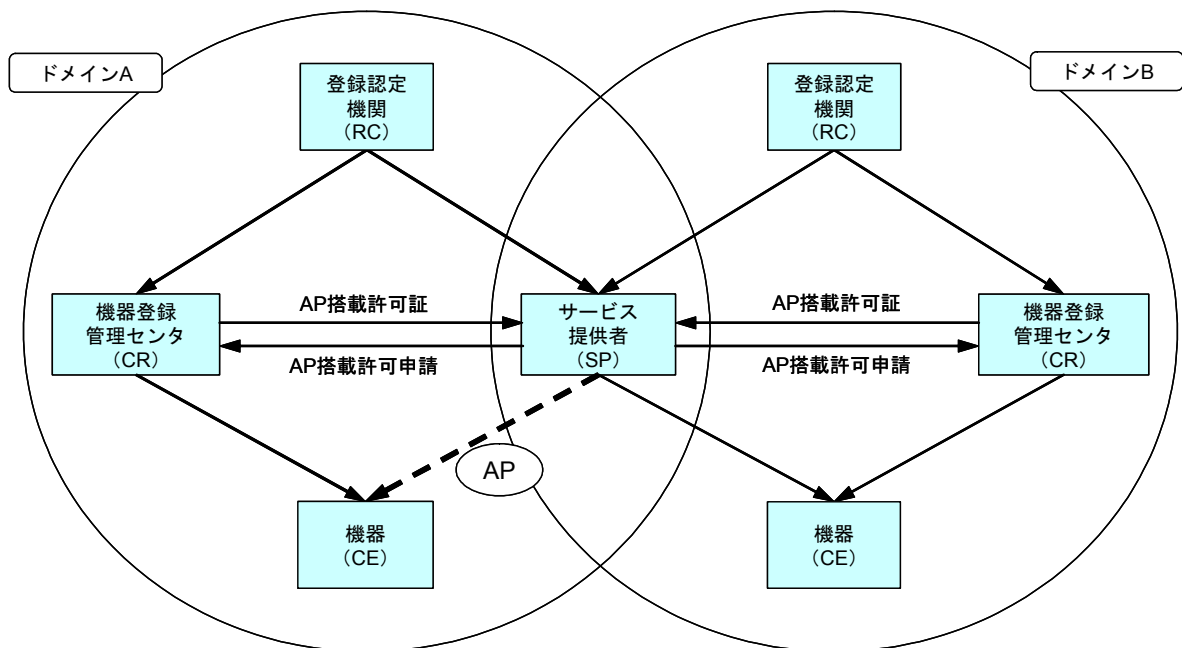


図 2-6 SP 相互認証モデル案



(2) ドメイン間相互運用の概念モデル案の評価

相互運用要件検討のためのケーススタディの準備として、これら 5 つの相互運用モデルについて、ビジネス性、各プレーヤへの影響、セキュリティ等の観点から評価を行った。

表 2-1 に各概念モデルの総合評価を示す。

表 2-1 概念モデル総合評価

		厳密な階層構造モデル案	相互認証モデル案	ブリッジRCモデル案	CR相互認証モデル案	SP相互認証モデル案
<b>モデル分類</b>		A 信頼出来る第三者機関の設立が必要	B 信頼出来る第三者機関の設立が不要	A 信頼出来る第三者機関の設立が必要	B 信頼出来る第三者機関の設立が不要	B 信頼出来る第三者機関の設立が不要
<b>新規参入</b> ○:影響なし △:1度だけ影響あり ×:ドメインが増える毎に影響あり	RC	△ ・RRCに対して登録手続きが必要 ・ドメインが増えても影響なし	× ・ドメインが増える毎に相互認証が必要になる	△ ・BRCに対して登録手続きが必要 ・ドメインが増えても影響なし	○ 影響なし	○ 影響なし
	CR	○ 影響なし	○ 影響なし	○ 影響なし	× ・ドメインが増える毎に登録が必要	○ 影響なし
	SP	○ 影響なし	○ 影響なし	○ 影響なし	○ 影響なし	× ・ドメインが増える毎に登録が必要
<b>セキュリティ・信頼性</b> (トラストポイントの信頼失墜) ○:影響範囲をドメイン内に抑止 △:ドメイン内運用は可能であるが、相互運用は不可 ×:全ドメインに影響あり ※例:ブリッジRCモデル案のトラストポイントについてはBRCとする		× ・RRCが信頼を失った場合、全ドメインに影響	○ ・RCが信頼を失った場合、影響範囲をドメイン内に抑止可能	△ ・BRCが信頼を失った場合、ドメイン内運用は可能であるが、相互運用は不可	○ ・RCが信頼を失った場合、影響範囲をドメイン内に抑止可能	○ ・RCが信頼を失った場合、影響範囲をドメイン内に抑止可能
<b>カード実装</b> ○:影響なし △:1度だけ影響あり ×:ドメインが増える毎に影響あり		△ ・RRC公開鍵証明書をカードに搭載	△ ・検証に必要な証明書を取得出来るシステムであれば実現可能	△ ・検証に必要な証明書を取得出来るシステムであれば実現可能	× ・新たに相互運用を行うドメインのRC公開鍵証明書を毎回搭載	○ ・既存カードで相互運用可能

総合評価の結果から、相互運用要件の検討の対象とするモデルを選出する。信頼できる第三者機関が必要な場合とそうでない場合それぞれについて、次の二つモデルを抽出した。

■ 信頼できる第三者機関が必要なモデルの場合 → ブリッジ RC モデル

■ 信頼できる第三者機関が不要なモデルの場合 → SP 相互認証モデル

## 2. 2. 4 多機能 IC チップドメイン間の相互運用要件に関する検討

2. 2. 3 (2) の検討において選定したブリッジ RC モデル、SP 相互認証モデルの各モデルについてケーススタディを行うことで相互運用要件の抽出を行った。

ブリッジ RC モデルの場合のケーススタディ

(1) ブリッジ RC モデルに基づいた相互運用の例を図 2-7 に示す。

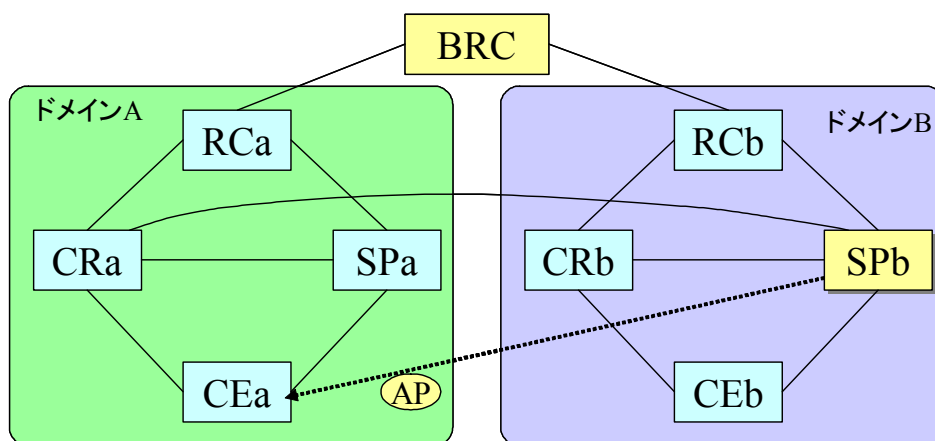


図 2-7 ブリッジ RC モデルに基づいた相互運用の例

ブリッジ RC モデルの相互運用要件を抽出するために、以下の設定で AP ダウンロード/削除までのケーススタディを行った。

<設定>既に運用されている多機能 IC チップドメインが、ドメイン A、B を含めて複数存在し、ドメイン A、B にまたがってサービスを利用したい利用者が多いため、両ドメインの RC はブリッジ RC を設立し、相互運用を開始する。

本モデルに基づいた場合の、SPb が CEa に対し AP ダウンロード/削除を行うまでの手順は以下の流れになる。

### ①BRC の設立と BRC 公開鍵証明書の配付

既にサービス運用されているドメイン A の RCa とドメイン B の RCb との間で、ドメイン間の相互運用を行うために調整を行い、BRC を設立しなければならない。BRC が設立された後、RCa と RCb は BRC に登録し、発行された BRC 公開鍵証明書を CR および SP に配布する。CR および SP は配布された、BRC 公開鍵証明書を利用することによって、他のドメインに属しているプレーヤの認証を行うことができる。

## ②Ra と SPb の契約

サービス提供者 SPb は、機器 CEa に AP ダウンロードするために、まず、CEa が機器登録管理されている機器登録管理センタ CRa と契約を結ばなければならない。多機能 IC チップフレームワーク（NICSS フレームワークを含む）において、この契約とはお互いの公開鍵証明書の交換を意味する。お互いの公開鍵証明書を保持することにより、オンライン環境での確実な相互認証や暗号通信が実現できる。

## ③CEa への AP ダウンロード

CRa への AP 登録が終わって始めて、CEa（正確には機器の所有者）からの AP ダウンロード要求に対して、SPb は AP ダウンロードを行うことができるようになる。

AP ダウンロードは多機能 IC チップフレームワーク（NICSS フレームワークを含む）のオペレーションに従って、SPb が CRa に対して AP 搭載許可証を申請し、受け取った AP 搭載許可証と AP 実体を CEa に送信し、CEa がデータを検証し、多機能 IC チップに AP を搭載する。

## (2) ブリッジ RC モデルの場合の要件

表 2-2 にブリッジ RC モデルの場合の要件の概要を示す。

表 2-2 ブリッジ RC モデルの場合の要件（概要）

プレーヤ	各プレーヤ個別の要件の内容
ブリッジ登録認定機関（BRC）	<ul style="list-style-type: none"> <li>(1) ブリッジ登録認定機関の設立</li> <li>(2) 証明書の発行と取得</li> <li>(3) ドメイン間相互運用のための運用</li> <li>(4) 公開鍵証明書の失効・更新</li> <li>(5) 公開鍵証明書の公開・削除</li> </ul>
登録認定機関（RC）	<ul style="list-style-type: none"> <li>(1) 証明書の発行と取得</li> <li>(2) ドメイン間相互運用のための運用</li> <li>(3) 公開鍵証明書の失効・更新</li> <li>(4) 公開鍵証明書の公開・削除</li> </ul>
機器登録管理センタ（CR）	<ul style="list-style-type: none"> <li>(1) 機器登録処理</li> <li>(2) サービス提供者との契約</li> <li>(3) サービス提供者からの AP 登録</li> <li>(4) AP ダウンロードにおけるサービス提供者間の処理</li> <li>(5) AP 削除におけるサービス提供者間の処理</li> </ul>
サービス提供者（SP）	<ul style="list-style-type: none"> <li>(1) 機器登録管理センタとの契約</li> <li>(2) 機器登録管理センタへの AP 登録</li> <li>(3) AP ダウンロードにおける機器登録管理センタ間の処理</li> <li>(4) AP 削除における機器登録管理センタ間の処理</li> <li>(5) AP ダウンロードにおける機器間の処理</li> <li>(6) AP 削除における機器間の処理</li> </ul>
機器（CE）	<ul style="list-style-type: none"> <li>(1) 機器の保持情報</li> <li>(2) AP ダウンロード</li> <li>(3) AP 削除</li> </ul>

(3) SP 相互認証モデルの場合のケーススタディ

SP 相互認証モデルに基づいた相互運用の例を図 2-8 に示す。

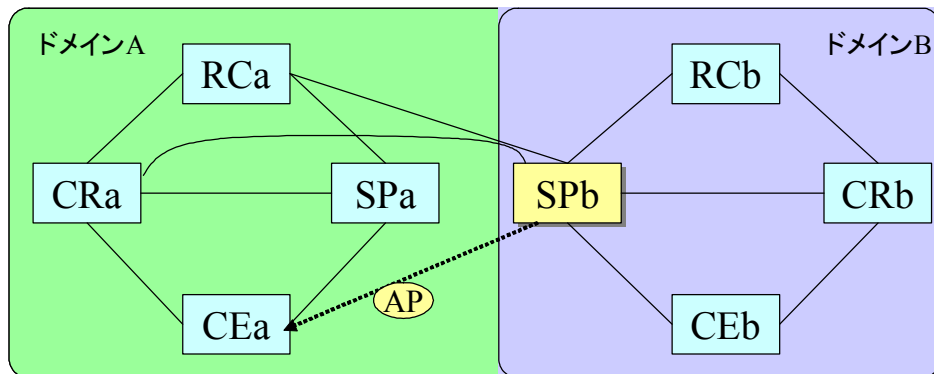


図 2-8 SP 相互認証モデルに基づいた相互運用例

ブリッジ RC モデルの相互運用要件を抽出するために、以下の設定で AP ダウンロード/削除までのケーススタディを行った。

<設定>既に運用されている多機能 IC チップドメインが、ドメイン A、B を含めて複数存在し、ドメイン A、B にまたがってサービスを利用したい利用者が多いため、ドメイン B に属している SPb がドメイン A のサービス利用者獲得のため相互運用を開始する。

本モデルに基づいた場合の、SPb が CEa に対し AP ダウンロード/削除を行うまでの手順は以下の流れになる。

①RCa への SP 登録/RCa への AP 登録

既にサービス運用されているドメイン B の SPb はドメイン A との相互運用を行うために、ドメイン A の RCa へ SP 登録を行わなければならない。発行された SP 公開鍵証明書を利用することによって、ドメイン A に属しているプレーヤの認証を行うことができる。また、ドメイン A で AP を提供するために、ドメイン A の RCa へ AP 登録を行わなければならない。

②CRa と SPb の契約

サービス提供者 SPb は、機器 CEa に AP ダウンロードするために、まず、CEa が機器登録管理されている機器登録管理センタ CRa と契約を結ばなければならない。多機能 IC チップフレームワーク (NICSS フレームワークを含む) において、この契約とはお互いの公開鍵証明書の交換を意味する。お互いの公開鍵証明書を保持することにより、オンライン環境での確実な相互認証や暗号通信が実現できる。

③CEa への AP ダウンロード

CRa への AP 登録が終わって始めて、CEa (正確には機器の所有者) からの AP ダウンロード要求に対して、SPb は AP ダウンロードを行うことができるようになる。

AP ダウンロードは多機能 IC チップフレームワーク (NICSS フレームワークを

含む)のオペレーションに従って、SPbがCRaに対してAP搭載許可証を申請し、受け取ったAP搭載許可証とAP実体をCEaに送信し、CEaがデータを検証し、多機能ICチップにAPを搭載する。

(4) SP相互認証モデルの場合の要件

表2-3にSP相互認証モデルの場合の要件の概要を示す。

表2-3 SP相互認証モデルの場合の要件(概要)

プレーヤ	各プレーヤ個別の要件の内容
登録認定機関(RC)	(1) 機器登録処理
サービス提供者(SP)	(1) 登録認定機関への登録 (2) APダウンロードにおける機器間の処理 (3) AP削除における機器間の処理
機器(CE)	(1) 機器の保持情報

2. 3 多機能ICチップフレームワーク以外のICチップフレームワークに基づくドメインを含めた相互運用に関する検討

2. 3. 1 概要

フレームワークの相違を超えたドメイン間でのサービスの相互運用の実現に向けて、多機能ICチップフレームワークに基づくドメインと多機能ICチップフレームワーク以外のICチップフレームワークに基づくドメインとの間におけるアプリケーションダウンロードに関する相互運用の可能性について検討し、その課題と解決の方向について調査研究を行った(図2-9)。

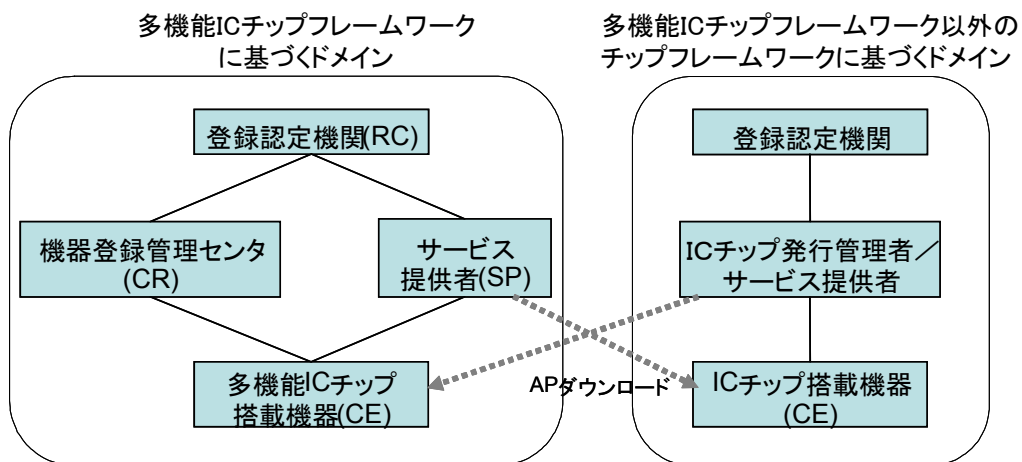


図2-9 本調査研究の検討範囲

本研究は以下のステップに従って実施した。

- ステップ 1： 対象とする IC チップフレームワークの調査
- ステップ 2： サービスモデルによる相互運用パターン抽出
- ステップ 3： 相互運用に向けた課題整理と方式検討

## 2. 3. 2 多機能 IC チップフレームワーク以外の IC チップフレームワークに関する調査

### (1) 検討対象とする IC チップフレームワーク

多機能 IC チップフレームワーク以外のフレームワークに基づく既存の IC チップフレームワークとして、各種の既存 IC チップフレームワークの中で、携帯電話や PDA などの機器への搭載が可能な IC チップとして今後の普及が見込まれる表 2-4 のフレームワークを検討対象とした。

表 2-4 検討対象とする IC チップフレームワーク

検討対象とするフレームワーク	関連仕様
UIM	3GPP
	3GPP2
MOPASS	GlobalPlatform、WAP (OMA) 等

相互運用検討の検討対象である「アプリケーションダウンロード」に注目した場合、いずれの仕様も GlobalPlatform 仕様を共通のベースとして持つ (図 2-10)。

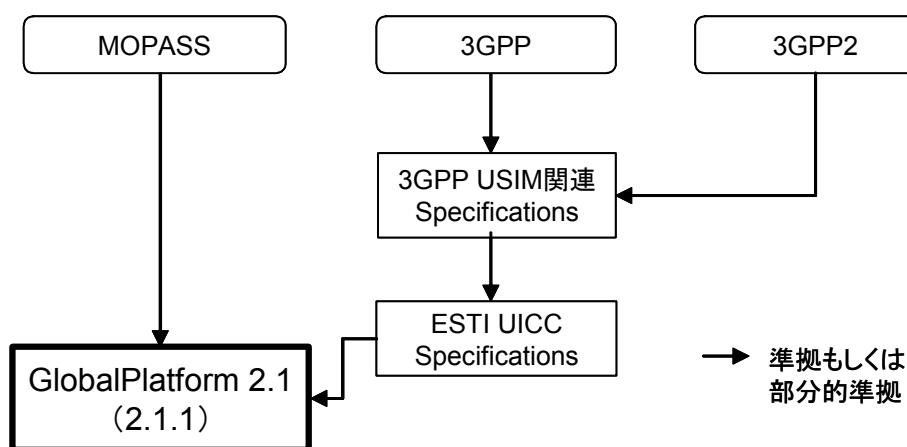


図 2-10 標準仕様間の関係

### (2) IC チップフレームワークのプレーヤモデル検討

携帯電話 UIM フレームワークのプレーヤモデルと MOPASS フレームワークのプレーヤモデルから、本研究で検討対象とする以下の二つのプレーヤモデルを抽出した。

### ①CR 中心型モデル

携帯電話事業者による UIM の運用形態から CR 中心型モデルを抽出する。CR 中心型モデルでは、携帯電話事業者などの大きな権限を持つ事業者が、機器登録管理センタ CR とアプリケーション提供者 APP の役割を併せ持つ。そうしたプレーヤをモデル化するために、このモデルでは機器登録管理センタとアプリケーション提供者を統合した新たなプレーヤとして「機器登録管理センタ/アプリケーション提供者 (CR/APP)」を導入する。

図 2-1 1 に CR 中心型のプレーヤモデルを示す。

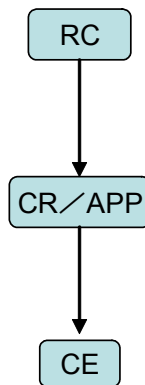


図 2-1 1 CR 中心型モデルのプレーヤモデル

### ②NICSS 型モデル

MOPASS フレームワークのプレーヤモデルから NICSS 型モデルを抽出する。MOPASS フレームワークは、多機能 IC チップフレームワークと同様、機器登録管理センタとアプリケーション提供者が異なる事業者によって運営される。このモデルは、多機能 IC チップフレームワークがそのベースとする NICSS フレームワークから受け継いだモデルであり、ここではこれを NICSS 型モデルと呼ぶ。

図 2-1 2 に NICSS 型のプレーヤモデルを示す。

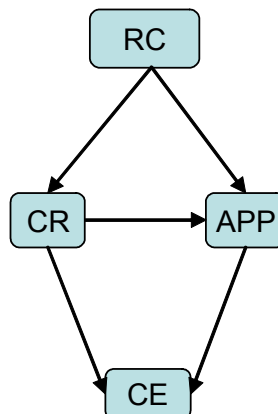


図 2-1 2 NICSS 型モデルのプレーヤモデル

### 2. 3. 3 ドメイン間相互運用の方式検討

それぞれのプレーヤモデルに基づく IC チップドメインを想定し、多機能 IC チップフレームワークに基づくドメインとの間の相互運用を実現するための基本要件について検討した。また、Global Platform のプレーヤ間インタフェースについて仕様検討を行い、GP ドメインの IC チップに対して AP ダウンロードを行う場合の要件について検討した。

#### (1) 多機能 IC チップドメインと CR 中心型モデルとの相互運用課題検討

CR 中心型モデルは、チップ登録管理センタ CR がアプリケーション提供者 APP の役割を兼ねるプレーヤとして、自身が管理する IC チップ搭載機器に対してのアプリケーションダウンロードを一手に引き受ける。このプレーヤを特別に「機器登録管理センタ兼 AP 提供者 (CR/APP)」と呼ぶ。このモデルの IC チップフレームワークとの間の相互運用パターンと実現するための課題は次の通りである (図 2-13)。

- ・ドメインをまたがるプレーヤ間の信頼パス構築
- ・機器登録管理センタ CR による AP 搭載許可証の発行
- ・チップ登録管理センタ兼 AP 提供者 CR/APP に対する AP 提供

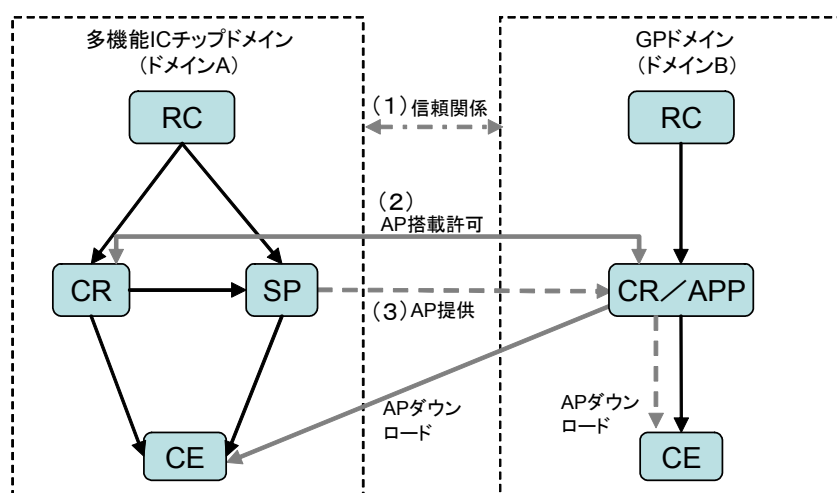


図 2-13 CR 中心型モデルとの相互運用パターンと課題



(2) 多機能 IC チップドメインと NICSS 型モデルとの相互運用課題検討

NICSS 型モデルでは、チップ登録管理センタ **CR** とアプリケーション提供者 **APP** が独立したプレーヤであり、アプリケーションの提供に関する運用形態の可能性を拡大している。このモデルの IC チップフレームワークとの相互運用パターンと実現するための課題は次の通りである (図 2-14)。

- ・ドメインをまたがるプレーヤ間の信頼パス構築
- ・機器登録管理センタ **CR** による **AP** 搭載許可証の発行
- ・チップ登録管理センタ **CR** による **AP** 搭載許可証 (相当の証明書情報) の発行

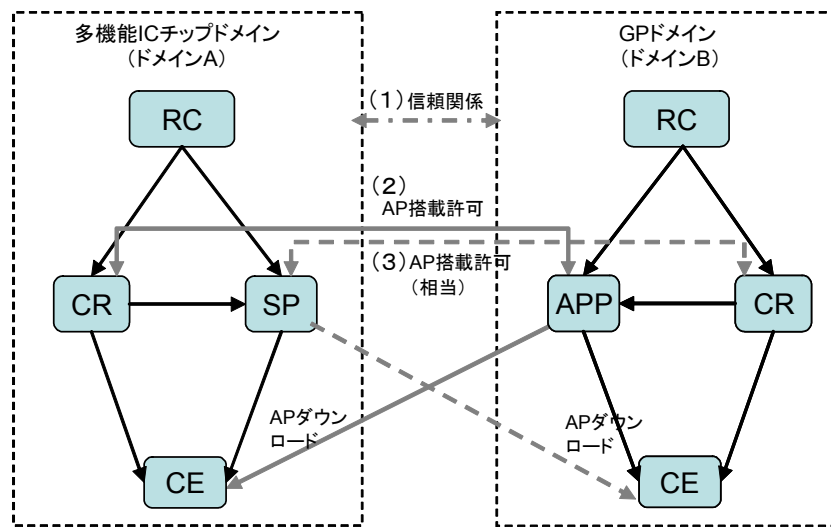


図 2-14 NICSS 型モデルとの相互運用パターンと課題

(3) 多機能 IC チップドメインと CR 中心型モデルとの相互運用方式検討

多機能 IC チップドメインと GP ドメインの CR 中心型モデルとの間のアプリケーションダウンロードに関する相互運用の方式検討を行った。本モデルにおいては、GP ドメインから多機能 IC チップドメインへの AP ダウンロードを方式検討の対象とする。

ドメインをまたがるプレーヤ間の信頼パス構築と AP 搭載許可証の発行の観点から検討した結果に基づいて、APP の登録認定先ドメインに関する方式の違いが関連するプレーヤに対してどのような影響を与えるかを表 2-5 にまとめる。

表 2-5 方式検討のまとめ (CR 中心型モデル)

	① GP ドメインの RC から登録認定を受ける場合		② 多機能 IC チップドメインの RC から登録認定を受ける場合	
APP の登録認定先(AP 証明書発行元)	GP ドメインの RC (RC(B))		多機能 IC チップドメインの RC (RC(A))	
各プレーヤにおける利点/欠点	利点	欠点	利点	欠点
RC(A)	—	他ドメイン RC と信頼関係を結ぶ手続きが必要	他ドメイン RC と信頼関係を結ぶ必要なし	—
CR(A)	—	他ドメイン RC が発行する AP 証明書の発行ポリシーの整合性を確認(ポリシー認定)する必要あり	自ドメイン発行の AP 証明書であり、十分信頼できる	—
APP(B)	・自ドメインの RC のみへの登録であり、手続きは容易	・ CR によっては AP ダウンロード要求を拒否する場合あり ・ チップ認証には他ドメイン発行の証明書の検証が必要	チップ認証が容易	接続ドメイン毎の登録が必要であり、手続きの負担が大きい
CE(A)	—	そのままでは APP(B)の認証は不可能(ただし、チップ更新時に他ドメインとの相互認証証明書を格納すれば可能)	変更なしで APP(B)の認証が可能	—

#### (4) 多機能 IC チップドメインと NICSS 型モデルとの相互運用方式検討

多機能 IC チップドメインと GP ドメインの NICSS 型モデルとの間のアプリケーションダウンロードに関する相互運用の方式検討を行った。本モデルにおいては、GP ドメインから多機能 IC チップドメインへの AP ダウンロード、ならびに、多機能 IC チップドメインから GP ドメインへの AP ダウンロードを方式検討の対象とした。

GP ドメインから多機能 IC チップドメインへの AP ダウンロードに関する方式検討については、(3) と同様の結論が得られた。

逆に、多機能 IC チップドメインから GP ドメインへの AP ダウンロードに関しては、GP のダウンロードシーケンスやダウンロードの際に使用される情報についてのセキュリティ上の考慮が必要となることから、多機能 IC チップドメインの APP は GP ドメインに登録する方式が推奨されることが知見として得られた。

### 2. 3. 4 ドメイン間相互運用の実現可能性の検討

ドメインをまたがるアプリケーションダウンロードの各方式について技術的観点からの検証と運用面を含めた実現可能性の検討を行った。

#### (1) GP ドメインから多機能 IC チップドメインへのアプリケーションダウンロードの方式検証

AP 証明書発行の 2 つの方式について比較検討を行った結果は以下のようまとめられる。

##### ①自ドメイン (GP ドメイン) による AP 証明書発行

関係する各プレーヤそれぞれで移行手続きが発生し全体的なコスト負担が大きい。しかし、アプリケーション提供者への負担はさほど大きくない。

##### ②相手ドメイン (多機能 IC チップドメイン) による AP 証明書発行

アプリケーション提供者以外の各プレーヤには移行手続きが発生しない。ただし、アプリケーション提供者は接続先ドメインごとの登録が必要であり、手続き的な負担が大きい。

GP ドメインのアプリケーションの提供者が接続する先の多機能 IC チップドメインの数が比較的少数であるか多数であるかによって、実現可能性の検討結果は変わる。

##### (a) 接続先ドメイン数が比較的少数である場合

接続先ドメインが少数であればアプリケーション提供者のコストはさほど増加せず、かつ全体のコストも抑えられるため実現可能性は高い。

##### (b) 接続先ドメイン数が比較的多数である場合

アプリケーション提供者への負担が小さいことが利点。関係するプレーヤのコスト負担を減らす方策として、複数の多機能 IC チップドメインにおけるアプリケーシ

ン提供者および AP の登録認定を集中して実施する「共通 AP 登録認定機関」を設置することが有効（図 2-15）。

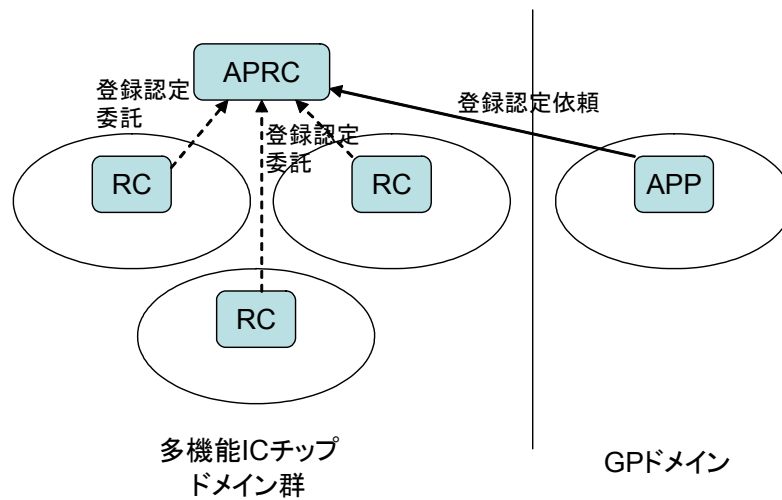


図 2-15 共通 AP 登録認定機関へ登録する場合

(2) 多機能 IC チップドメインから GP ドメインへのアプリケーションダウンロードの方式検証

AP 証明書発行に関して、想定される 2 つの方式について比較検討を行った結果は以下のようにまとめられる。

①RC 間の信頼関係構築を利用する方式

多機能 IC チップドメインの SP(A)が自ドメインの RC である RC(A)から登録認定を受け、公開鍵証明書の発行を受ける。SP(A)が GP ドメインのプレーヤである CR(B)との間で PKI ベースの相互認証を行うには、RC(A)と RC(B)の間での信頼関係を構築しておく必要がある。

②SP が直接 GP ドメインの RC に登録する方式

多機能 IC チップドメインの SP(A)が GP ドメインの RC に対して直接登録認定を受け、公開鍵証明書の発行を受ける。これは、SP(A)が単独で GP ドメインに参加することに対応する。

GP ドメインで管理される IC チップに対するアプリケーションダウンロードにどの方式が望ましいかは、実際の運用形態に大きく依存すると結論付けられる。

## 2. 4 まとめ

### 2. 4. 1 成果

本テーマ種別においては、複数の IC チップドメインが存在する環境下において、異なるドメイン間で相互に IC チップにアプリケーションをダウンロードし、サービスが利用できる環境の実現に向けて、技術上、運用上において求められる要件や課題等について検討を行った。

本テーマ種別では、IC チップドメイン間の相互運用について「所有者／利用者（CH : Chip embedded equipment Holder）が、あるドメインにおいて発行／登録された多機能 IC チップ搭載機器（CE : Chip embedded Equipment）に、他のドメインで提供されているサービスを受けられるようにすること」と定義し、実際上の検討の範囲として、「CH が、あるドメインで発行・登録された CE に、他のドメインでサービスに供されているアプリケーション（AP）を安全にダウンロード及び削除ができること」と設定した。

相互運用を行うドメインの範囲の違いから、次の二つの観点に基づき検討を行った。

- ①多機能 IC チップフレームワークに基づくドメイン間の相互運用に関する検討
- ②多機能 IC チップフレームワークに基づくドメインと多機能 IC チップフレームワーク以外の IC チップフレームワークに基づくドメインとの間の相互運用に関する検討

### 2. 4. 2 展望と課題

- (1) 多機能 IC チップフレームワークに基づくドメイン間の相互運用の実現に向けて

相互運用モデルに共通する課題として、以下のような項目について引き続き検討が必要である。

- ・制度的・契約的な問題（約款、契約書ガイドラインなど）
- ・運用的な問題（管理体制、連絡体制、障害時の対応など）
- ・ビジネスモデルの問題
- ・実装システム間のインタフェース差異吸収の問題

SP 相互認証モデルに関して、サービス提供者の負担を軽減し、参入を促すために各プラットフォームに共通な機能を統合化する「統合 SP サーバ」を実装することが有効な解決策の一つになると考えられる（図 2-16）。

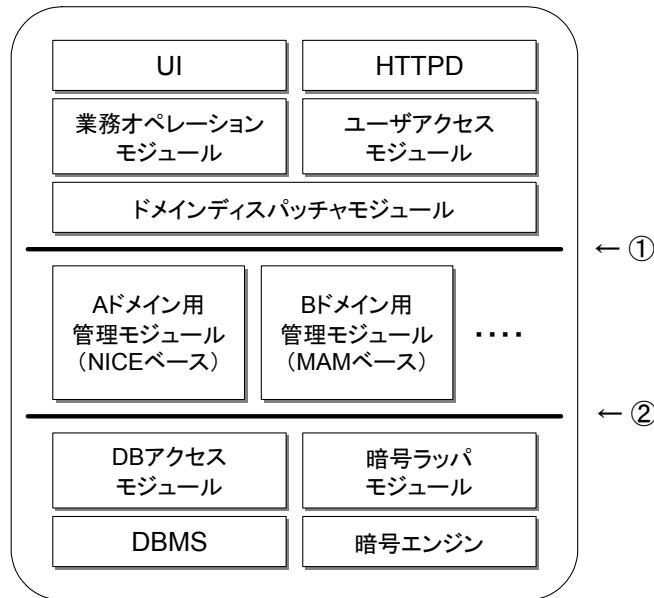


図 2-16 統合 SP サーバのモジュール構成案

(2) 多機能 IC チップフレームワーク以外の IC チップフレームワークに基づくドメインを含めた相互運用の実現に向けて

異なるフレームワークに基づくドメイン間での相互運用を実現するためには、技術面・運用面での課題が残されている。

特に、以下のような項目について引き続き検討が必要である。

①技術面での課題

- ・異なるフレームワークを実現するプラットフォーム間での、プロトコルやデータフォーマットの差異を吸収する方式を具体化
- ・NICSS フレームワークにおけるアダプタの概念の適用可能性の検討

②運用面での課題

- ・RC 間が信頼関係を結ぶために必要な運用ポリシーの認定
- ・複数の多機能 IC チップドメインが共通に信頼できる共通 AP 登録認定機関の実現・運用

## 第Ⅱ編 研究開発・実証事業の実施報告

### 3. テーマ種別2

---

### 3. テーマ種別 2

#### 3. 1 事業概要

##### 3. 1. 1 背景

「多機能 IC チップフレームワーク」とは、多機能 IC チップを搭載する媒体を活用することによって、すべてのプレーヤの正当な既得権利を安全に行使できる仕組みであり、高い安全性と信頼性の基盤をサービス提供者に提供することでその参入を促し、一方、利用者に対しては、さまざまなサービスを受受できるような環境を提供することを目的とするものである。今後、多機能 IC チップを組み込んだ機器やカード等が普及するにつれて、より多様な分野において多機能 IC チップフレームワークを基礎としたサービスが提供されるようになることが期待されている。

##### 3. 1. 2 目的

テーマ種別 2「多機能 IC チップフレームワークを利用したマルチメディア情報流通等の実効性検証」は、多機能 IC チップを搭載する機器や、それを活用した新たなサービスの実現や普及のために、多様なサービスの提供者が新規に参加できるような環境を整えることを目的として実施した。

実施の具体的な目的は、以下のように整理される。

###### (1) 基盤技術の整備

多機能 IC チップを IT サービスに活用するための基盤となる技術的な枠組みの要件を整理し、サービス提供者が容易に多機能 IC チップの利点を生かした新しいサービスを開始できるような環境を整備すること。

###### (2) サービスにおける実効性検証

多機能 IC チップを実際のサービスに適用した場合の、利用者やサービス提供者にとっての技術面、運用面のメリット、デメリットについて調査し、多機能 IC チップの導入によりこれまでのサービスと比較してどのような変化がもたらされるのかを明らかにすること。

###### (3) 多様なデバイスへの多機能 IC チップの適用

多機能 IC チップが搭載されたデバイスを拡大し、利用者にとって多機能 IC チップが身近に感じられ、サービス提供者にとっては顧客が日常的に利用するものとして広く普及するよう、環境整備を図ること。



### 3. 1. 3 事業概要

テーマ種別 2 での実施概要について以下に記述する。

#### (1) 多機能 IC チップフレームワーク

多機能 IC チップの状態管理およびアプリケーション管理を行なう枠組み全般について整理した。多機能 IC チップと同様の機能を持つ IC カードのフレームワークである NICSS フレームワークを基礎とし、IC カードにはない機器登録の手順を中心に、技術的要件の検討を行った。

#### (2) 権利流通管理システムモデル

マルチメディアコンテンツ流通サービスおよび会員権サービスで実装されているサービス提供の手順やプレーヤ間の関係に基づき、利用者がコンテンツやサービスを利用するための権利に関する情報の流通を管理する仕組みについて検討を行った。その結果、多機能 IC チップを搭載した機器及び利用者の中で、サービス提供者が許諾した範囲で、権利に関する情報の生成、流通、及び行使を管理する方法や、関係するプレーヤの役割について整理した。

#### (3) マルチメディア情報流通サービス

多機能 IC チップを活用することにより、デジタルコンテンツを流通させる新たなサービスの仕組みとして、権利者、事業者、利用者が受容可能な、マルチメディア情報流通サービスの実現を図る研究開発および実効性検証を行い、ビジネスやセキュリティの観点から評価した。

また、コンテンツ流通サービスを利用する端末の拡大を意図し、多機能 IC チップの PDA への実装について検討を行った。

#### (4) 会員権サービス

多機能 IC チップを活用した IT サービスにおける利用権管理の活用分野として、多機能 IC チップによって会員権及びそれに関連付けられた各種サービスの利用権を管理する、会員権サービスの実現を図る研究開発および実効性検証を行い、会員権と他のサービスを関連付けて多機能 IC チップで管理するサービス形態について、有効性や利便性、セキュリティに関する利用者の受容について評価した。

また、多機能 IC チップと超小型 ID チップとの組み合わせによるサービスの展開について検討を行った。

なお、会員権サービスに基づいた電子チケットサービスの実効性検証はテーマ種別 3 で実施した。

#### (5) 多機能 IC チップを搭載した携帯電話への適用の検討

日常的に持ち運ぶことができ、かつ画面を持って利用者に直接サービスを提供できる媒体である携帯電話を対象に、多機能 IC チップ対象機器としての適用について検討を行なった。

具体的には、多機能 IC チップフレームワークへの適用に向けて非接触インタフェースを保持した携帯電話の試作を行なった。また、多機能 IC チップフレームワークへの適用を想定した、UIM の PKI 機能を活用した情報流通サービスの検証を行った。

テーマ種別 2 の実施項目の位置付けについて図 3 - 1 に示す。

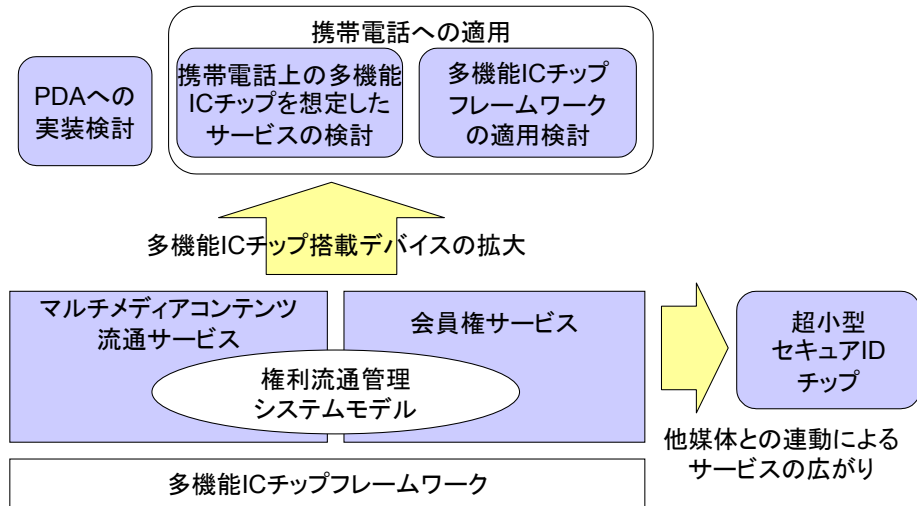


図 3 - 1 テーマ種別 2 の実施項目の位置付け

### 3. 1. 4 略語一覧

以下に、本章で使用されている略語を示す。

- AP\_ID (Application Program Identifier) : アプリケーションプログラム識別子
- APP (AP Provider) : アプリケーション提供者
- CE (Chip embedded Equipment) : 多機能 IC チップ搭載機器
- CE\_ID (Chip embedded Equipment Identifier) : 機器登録識別子
- CH (CH : Chip embedded equipment Holder) : 保有者 (利用者)
- CM (Card Manager) : カードマネージャ
- CR (Chip embedded equipment Registry) : 機器登録管理センタ
- CR\_ID (Chip embedded equipment Registry Identifier) : 機器登録管理センタ識別子
- CS (Chip Supplier) : IC チップ供給者
- NICSS (the Next generation Ic Card System Study group) : 次世代 IC カードシステム研究会
- RC (Registration Center) : 登録認定機関
- RC\_ID (Registration Center Identifier) : 登録認定機関識別子
- SIM (Subscriber Identity Module)
- SP (Service Provider) : サービス提供者
- SP\_ID (Service Provider Identifier) : サービス提供者識別子
- UIM (User Identity Module)

### 3. 2 技術的基盤の検討

多機能 IC チップフレームワークに基づくサービス提供環境を実現するために必要となる技術面、および業務面にかかわるさまざまな要素について、多機能 IC チップを適用したサービス提供環境を実現する技術的基盤について研究する。

上記の目的を達成するため、次に示す検討を行った。

#### (1) 多機能 IC チップフレームワーク

多機能 IC チップの機能を活用してネットワークを介して提供するサービスにおいて、セキュリティと利便性を確保する枠組みを、IC カードから IC チップを搭載した機器に拡大する。

#### (2) 権利流通管理システムモデル

ネットワークを利用したマルチメディアコンテンツ配信や会員権サービスにおいて、利用権や会員権を流通および管理する共通の権利流通管理システムについて、上記多機能 IC チップフレームワークの適用を前提にそのシステムモデルを明確にする。

### 3. 2. 1 全体コンセプトと技術基盤の概要

上記各階層を構成するプレーヤとそれぞれの関係を概略したプレーヤモデルを図 3-2 に示す。

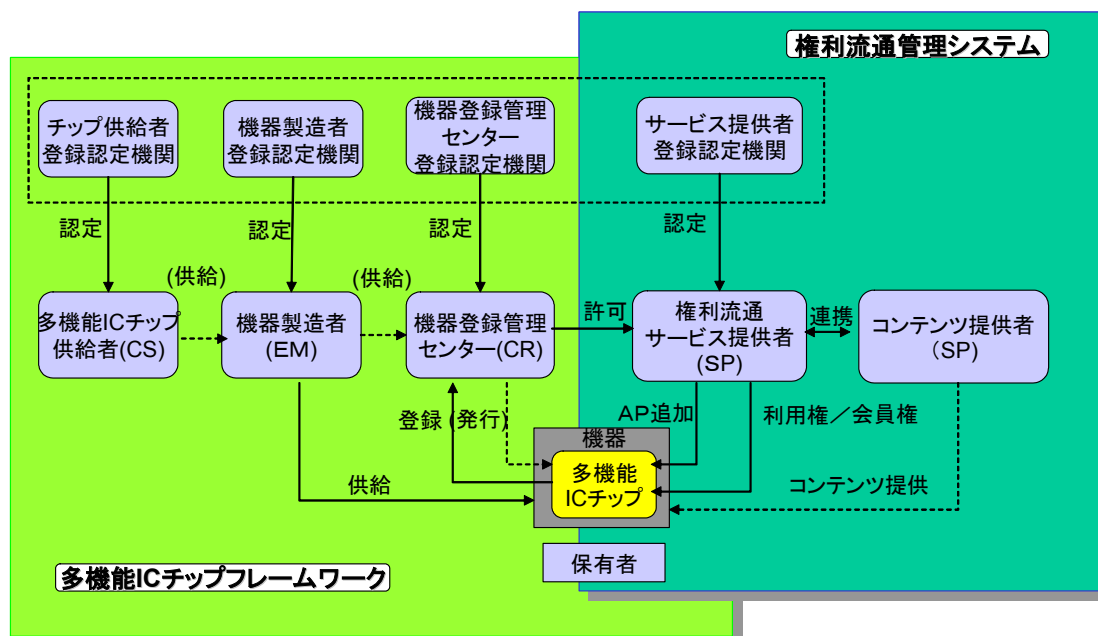


図 3-2 全体構成 (プレーヤモデル)

本事業における多機能 IC チップは、機器製造者が IC チップを調達し、さまざまな機器に安全に装着することを基本とする。そのため、多機能 IC チップフレームワークでは、

新たに「IC チップ供給者 (CS)」や「機器製造者 (EM)」をプレーヤとして定義し、その役割と他のプレーヤとの間の関係について規定する。

また、多機能 IC チップフレームワークでは、多機能 IC チップを内蔵した機器を購入した後で、機器を「機器登録管理センタ (CR)」に登録するプロセスを想定しており、対応する CR の役割を規定している。

さらに、マルチメディア情報流通サービスや会員権サービスにおけるマルチメディアコンテンツ利用のための利用権や会員権、および会員権サービスにおける会員権などを流通することを対象とした権利流通管理システムのシステムモデルを取りまとめる。

なお、本事業における権利流通管理システムモデルでは、上記以外の実際の著作権等にかかわるさまざまな個人や業者などのプレーヤについてはシステムモデルの対象としていない。

また、マルチメディア情報流通サービスなどでは、権利が守られることが主眼目であるが、利用者に渡る利用権などの権利だけでなく、暗号技術などで保護されたデジタルコンテンツ自体も、利用権行使時点以降、再生終了まで保護されなければならない。つまり保護化されたデジタルコンテンツを安全にデジタルコンテンツに解凍し、また、アナログコンテンツなどにして、保護の必要のない状態になるまで、耐タンパーを保証しなければならない。本検討におけるシステムモデルでは、利用権行使以降のこのようなデジタルコンテンツの保護策や耐タンパの保証措置については前提としてはいるが、詳細については検討の対象としていない。

### 3. 2. 2 各階層に対応した検討の位置付け

本事業が目指す多機能 IC チップフレームワークと権利流通管理システムモデルの位置付けを、次世代 IC カードシステム研究会 (NICSS) が策定し、IT 装備都市研究事業のベースとなった IC カードのフレームワークである「NICSS フレームワーク」と対比したものを図 3-3 に示す。

多機能 IC チップフレームワークは、多機能 IC チップの供給から登録、発行、および運用を行う「多機能 IC チップ階層」(1 階層)として、権利流通管理システムモデルは、その上でサービスを提供する「サービス階層」(2 階層)として、それぞれ位置付けられる。各階層におけるそれぞれのプレーヤはインターネットなどのオープンなネットワークを介して自由に構成されることを基本とするため、実現の技術基盤として PKI を適用する。

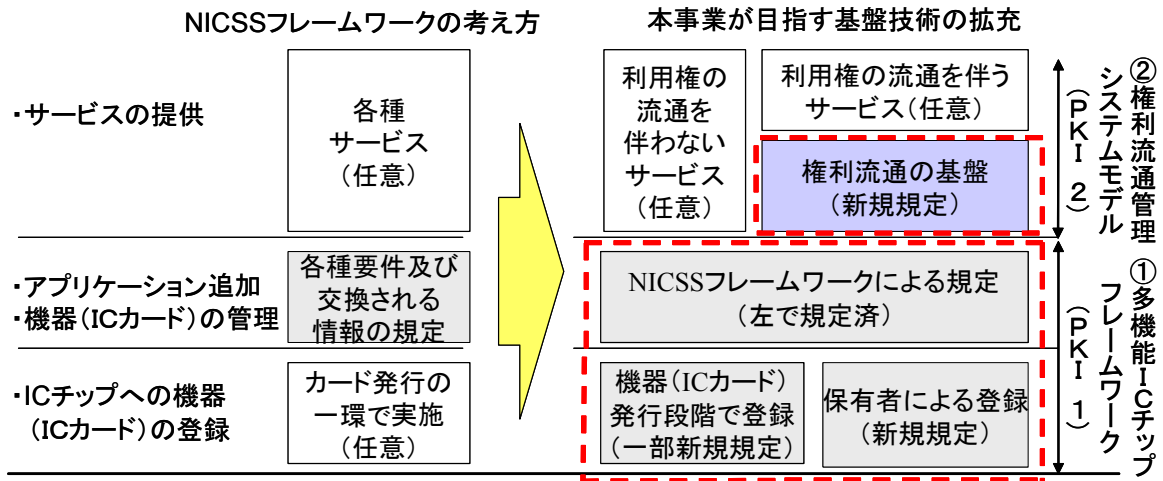


図 3-3 本事業における各フレームワークの位置付け

### 3. 2. 3 多機能 IC チップフレームワークの検討

#### (1) 多機能 IC チップフレームワークの検討背景

インターネットのブロードバンド化の進展に応じて電子機器がインターネットに接続され利用されるようになってきている。遠隔地からネットワークを経由して電子機器に接続し、安全に操作を行う場合には、電子機器とそれを操作する人、あるいは機器との間の認証は不可欠な要素である。ネットワーク上で人や機器の認証や権利の保証を実現するための確実かつ信頼の置ける手段として、多機能 IC チップの利用が有効である。

本テーマ種別においては、多機能 IC チップを用いて、認証などのさまざまなサービスを安全に受けることができる基本的な枠組みとして、「多機能 IC チップフレームワーク」を検討した。

多機能 IC チップフレームワークの要点を示す。

- ①多機能 IC チップには複数のアプリケーションプログラム (AP) を格納し、チップ自身が自律的に多様なサービスを提供するなど 1 個の多機能 IC チップを多目的に利用できる。
- ②機器の購入 (入手) 後に多機能 IC チップに対し、ネットワーク経由で安全に AP (サービスを利用するために多機能 IC チップに格納されるアプリケーション) の追加・削除を行うことができる。
- ③多機能 IC チップを搭載した機器が多機能 IC チップを搭載した他の機器や IC カードとの間で PKI による相互認証、署名、および暗号処理を行うことができる。

#### (2) 機器登録

機器登録管理センターあるいはサービス提供者が機器を認証 (内部認証)、および機器が機器登録管理センターあるいはサービス提供者を認証 (外部認証) するために、当該機器に対し、次の機能を持つ。

- ・機器登録管理センタ内でユニークな ID（機器登録 ID）を払い出す。
- ・当該機器の非対称暗号方式の秘密鍵とその公開鍵に対する公開鍵証明書を生成し、機器に搭載されている多機能 IC チップに書き込む。

秘密鍵と公開鍵の生成には、主に次の方法がある。

- ①多機能 IC チップ内で生成
- ②機器製造者が生成
- ③機器登録管理センタが生成

①の方法以外は、鍵生成環境のセキュリティ確保が必要となる。以降の説明では③の機器登録管理センタが生成する場合で説明する。

多機能 IC チップフレームワークでは、機器登録管理センタにおいて機器登録することは必須の機能であるが、登録の内容と登録に際しての認証方法については、機器とサービスによるものとし選択事項とした。

また、機器の所有者（利用者）を登録して個人情報を蓄積管理する場合には、個人情報保護の観点から特別の処置が必要になる。また、機器やサービスに依存する機器の属性の登録と管理を機器登録管理センタが行うのではなく、実現の 1 つの方法として、認証や登録および管理をサービスと位置付け、機器登録管理センタ以外でサービスとして提供することも考えられる。また、機器の所有者（利用者）を登録して個人情報を蓄積管理する場合には、個人情報保護の観点から特別の処置が必要になる。また、機器やサービスに依存する機器の属性登録と管理を機器登録管理センタが行うのではなく、実現の 1 つの方法として、認証や登録および管理をサービスと位置付け、機器登録管理センタ以外で業界ごとにサービスとして提供することも考えられる。

機器登録の基本的な機能要件を図 3 - 4 に示す。

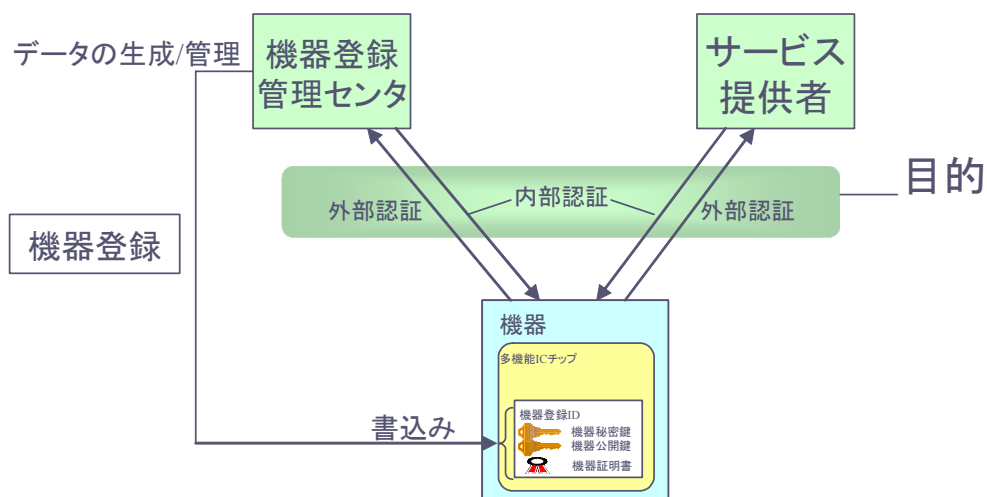


図 3 - 4 機器登録の基本的な機能要件

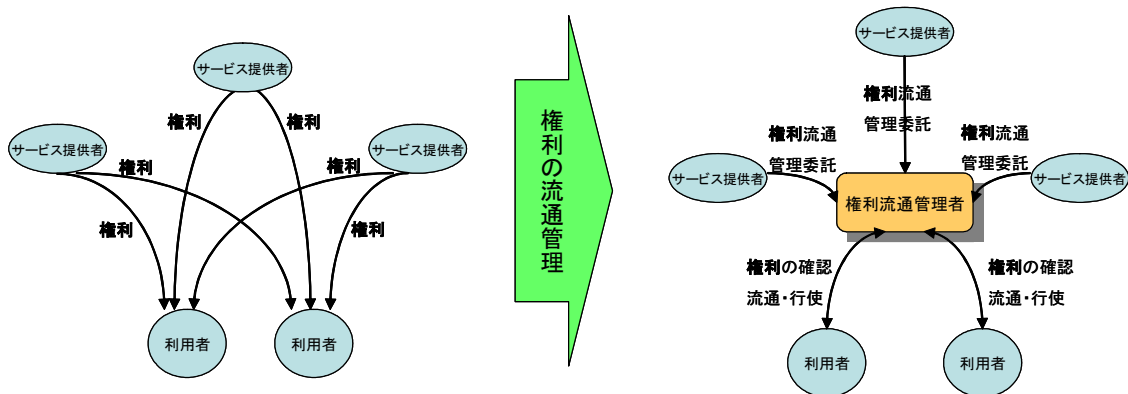
機器登録のシーケンスとしては、ICカードのような場合には、機器をICカードとみなし、(1) 機器登録管理センターがICカードの発行者になり、ICカードの供給を受けチップの登録を行ってから保有者の元に発行する。機器の場合には(2) 多機能ICチップが装着された機器が保有者の元に渡った後に、保有者自身で行う場合と(3) 保有者に渡される前に保有者の了解の下に機器販売者を含む機器製造者が実施する場合に大別される。

### 3. 2. 4 権利流通管理システムモデル

#### (1) 権利流通管理システムの検討背景

デジタルコンテンツ配信ビジネスなどでは、コンテンツを暗号化し、暗号化コンテンツと再生などができる利用権を利用者に別々に配信することが既に行われている。

本節では、こういったビジネスのさらなる普及拡大のために、デジタルコンテンツの利用権等の権利を信頼できる流通管理者に委託し、サービス提供者および利用者とも、ネットワークを経由して権利の所有を確認しつつ、権利のさまざまな行使を安全、かつ自由に行える権利流通管理のためのシステムモデルについて検討した。



**暗号化コンテンツは別途配信されることが前提**

図3-5 権利流通管理者の位置付け

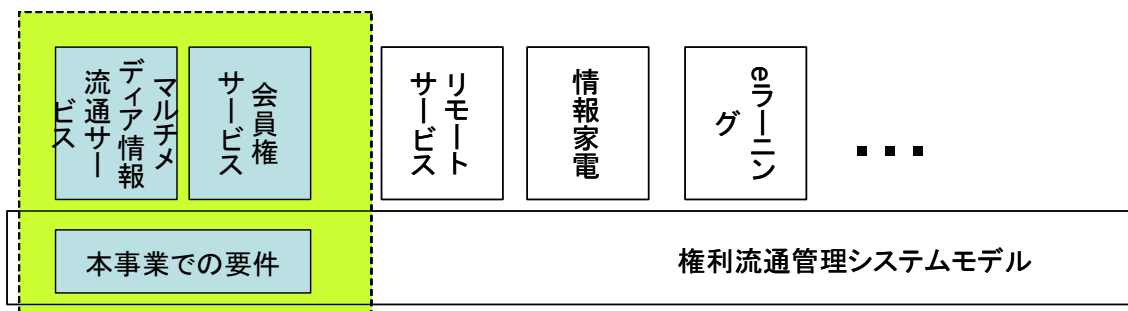
本事業では、次の2つの実効性検証サービスにおける権利とシステム機能を検討のターゲットとした(図3-6)。

#### ①対象とするサービスと権利

- ・会員権および利用権：マルチメディア情報流通サービス
- ・会員権：会員権 サービス

#### ②対象とするシステム機能

- ・権利情報の生成、発行、譲渡、移動、複製、行使
- ・権利情報の確認(PKIによる検証)、回収
- ・権利情報の再発行、失効：ただし、本事業では未検討



本事業でのシステムモデルの検討範囲

図3-6 権利流通管理システムモデルの検討範囲

(2) 権利流通管理システムモデルの位置付け

例えば、コンテンツ流通分野では、図3-7に示すように、前段の「著作権管理」と中段の「コンテンツ流通および権利流通」、さらに後段の「機器でのコンテンツ利用」に大きく分けられる。権利流通管理システムモデルは中段に位置し、その中でも、「権利流通管理」にフォーカスするものである。

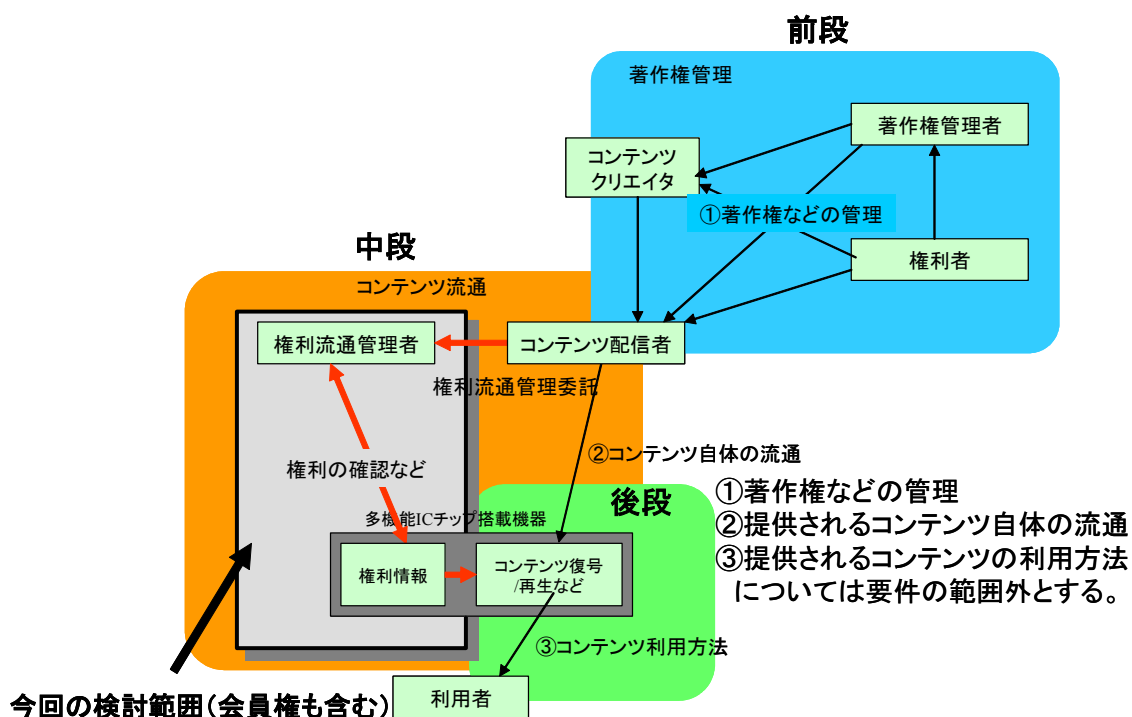


図3-7 権利流通管理システムの位置付け

権利流通管理システムモデルでは、サービス利用が可能とする権利を電子情報として表象した権利情報に対して管理を担う信頼できる第三者機関を「権利流通管理者」とし、多機能 IC チップを搭載した機器との間で権利流通管理を行うモデルとして提案する。



本検討の対象とした 2 つの実効性検証サービスに共通した論理的なシステムモデルを図 3-8 に示す。

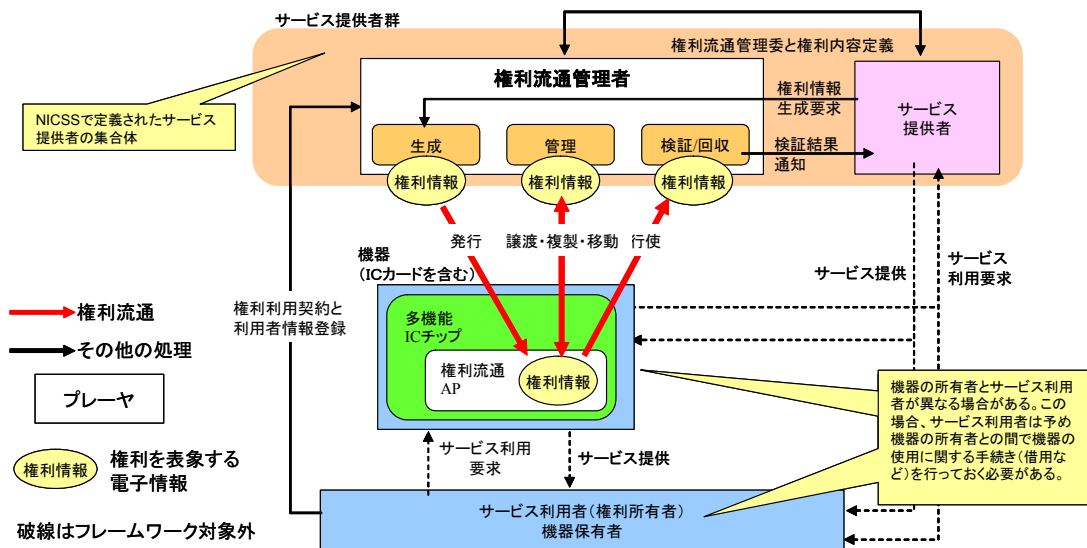


図 3-8 権利流通管理システムモデル

権利流通管理システムモデルは、多機能 IC チップフレームワークからみれば、サービス階層に位置付けられ、ここに登場する IC チップ階層の利用機器および IC カードは多機能 IC チップフレームワークを基盤として採用することを基本とする。したがって、権利流通管理のためのチップ上へのアプリケーション搭載は多機能 IC チップフレームワークのアプリケーションダウンロード機能による。

権利流通管理システムモデルにおける権利流通管理者とサービス提供者のうち、サービス提供者は権利流通管理者から見ると権利の流通管理委託契約元であるが、実際のビジネスでは、個人事業者を含め、著作権やコンテンツを取り扱う多くのプレーヤから構成されており複雑である。システムモデルでは権利流通管理者の役割を述べたものなので、これらサービス提供者群は一体のもととして単にサービス提供者とした。

権利流通管理者の役割は、会員権情報や利用権情報の生成、管理および検証・回収であるが、利用機器や IC カードのチップアプリケーションの機能としては、それぞれ、権利情報の発行、流通および行使として実現される。このうち、権利情報の流通機能には、譲渡、複製、移動などがある。

その他、権利流通管理者の役割と機能オペレーションには、権利の再発行や無効化などのオペレーションがありうると考えられる。これらは利用者メリットに直接結びつくものがあると期待されるものであるが、本事業では、検討範囲外として、詳細に検討していない。

権利情報の生成については、利用者の特定を必要としており、利用者認証を必須とする。一方、利用機器の認証は、会員権サービスのように利用機器を特定する必要のないサービスもあることから、選択事項としている。なお、利用者情報をどこまで管理する

かは、個人情報保護の観点などからサービスがおかれた環境によっても異なると考えられることから、厳密なモデル化は行わず、考え方を示すに留めた。

### (3) 権利流通のオペレーション

本テーマ種別の実効性検証システムで実装し、かつ権利流通管理システムモデルで対象とした権利情報の流通管理オペレーションを以下に列挙する。

発行——権利流通管理者がサービス利用者に対して権利情報を生成し、利用者の多機能 IC チップに格納する。

行使——サービス利用者が持つ権利情報の行使を権利流通管理者に求める。

譲渡——権利流通管理者の管理の下で、サービス利用者が持つ権利情報を他のサービス利用者へ受け渡す。

複製——権利流通管理者の管理の下で、サービス利用者が持つ権利情報の複製を作成する。

移動——権利流通管理者の管理の下で、サービス利用者が持つ権利情報を別のサービス利用者が所有する機器へ移動する。

## 3. 3 マルチメディアコンテンツ流通サービスの実効性検証

近年のブロードバンドの普及に伴い、インターネットの発達はめざましいものがある。インターネットは音楽、映像などのコンテンツ流通を行う上で非常に有効な手段であるが、その一方、コンテンツの違法コピーによる権利侵害問題が問題となっている。コンテンツ流通を行ういくつかのサービスでは、権利保護の仕組みはできているものの再生機器が限定されてしまう等の制約がある。

本事業では、多機能 IC チップを活用し、ユーザにとって利便性を考慮すると共に、権利者にとっても権利保護できる安全な仕組みを研究開発し、実効性検証を行った。

### 3. 3. 1 マルチメディアコンテンツ流通サービスの概要

マルチメディア情報流通サービスは、暗号化されて流通するコンテンツとは別に、復号するための復号鍵を含むコンテンツを再生する条件をコンテンツの利用権として管理し、コンテンツを再生、視聴する許諾を受けた利用者に流通するサービスである。

#### (1) サービスの概要

権利者もしくはそれを代理するコンテンツ提供者からコンテンツの提供を受けたコンテンツ配信者が、当該コンテンツを暗号化し、暗号化されたコンテンツの復号鍵及び再生条件を「利用権」として、利用権流通管理者を通じて流通する。暗号化されたコンテンツ自体は、コンテンツ配信者がオンラインで、あるいは CD-ROM 等に格納して配布するが、暗号化された状態では、公衆に無償で配布されることも想定している。また、暗号化されたコンテンツ自体は、自由に複製して、他者に提供することも許容する考え

方である。この暗号化されたコンテンツは、当該コンテンツに特有の復号鍵によって復号されなければ、再生、鑑賞することはできない。そこで、利用者は、「利用権」として復号鍵及び再生条件を購入して、この復号鍵を用いて、暗号化されたコンテンツを復号し、鑑賞することになる。

## (2) コンテンツ流通の概要

マルチメディア情報流通サービスでは、暗号化されたコンテンツの流通と利用権の流通を分離することに特徴がある。また、コンテンツ配信者や利用権流通管理者として複数のプレーヤが参加可能である。コンテンツの流通や再生に係わる機器や利用者、流通業者（利用権流通管理者）にはPKIを活用した証明書を発行し、一部のプレーヤが権利侵害を行った場合には、証明書の失効管理によって該当するプレーヤだけを無効にすることにより、権利侵害の局所化を可能とする。

## (3) 特徴

本事業にて推進するマルチメディア情報流通モデルの特徴を、以下に整理する。

- ・機器に多機能ICチップを搭載し、利用者ICカードと合わせて認証することにより、厳密な機器・利用者認証が可能となり、事前に設定した条件のもとでのコンテンツの再生を管理できる（権利侵害の排除）。
- ・利用権とコンテンツ（音源や映像等）を分離することで、それだけでは再生できない状態のコンテンツについては、自由度の高い配布・流通が可能となる（利便性の確保）。
- ・利用権の二次流通（譲渡）が可能となる（利便性の確保）。
- ・利用権を紛失・破損した際の対応（再発行等）が可能となる（利便性の確保）。
- ・再生機器、回数、期間、利用者等の条件を設定した利用権の販売が可能であり、様々な形態でのサービスを実施できる（事業者の参加しやすさ）。
- ・オープンな技術基盤を活用し、複数の事業者が同時に参画できる形態であるため、中小事業者の事業参入が容易になる（事業者の参加しやすさ）。

## (4) サービスの流れ

サービス利用者は、次のような手順でコンテンツを入手、再生する。

- ①暗号化されたコンテンツ（保護化コンテンツ）を入手する。
- ②サービス提供者に対して、ICカードで利用者認証、機器に内蔵された多機能ICチップで機器認証を行い、利用権を入手する。利用権は、ICカードに格納される。
- ③サービス利用者は、多機能ICチップに格納している利用権を利用することにより、利用権にある利用条件の範囲内でコンテンツを利用することができる。

このとき、利用権は、別の機器に移動したり、他人に譲渡したりといった、パッケージと同様の利便性で取り扱うことができる。

なお、権利者の要求やサービスの多様性の観点から、移動の制限、再生機器の限定、再生期間の限定、利用者の限定など、利用権にさまざまな利用条件を設定することができる。

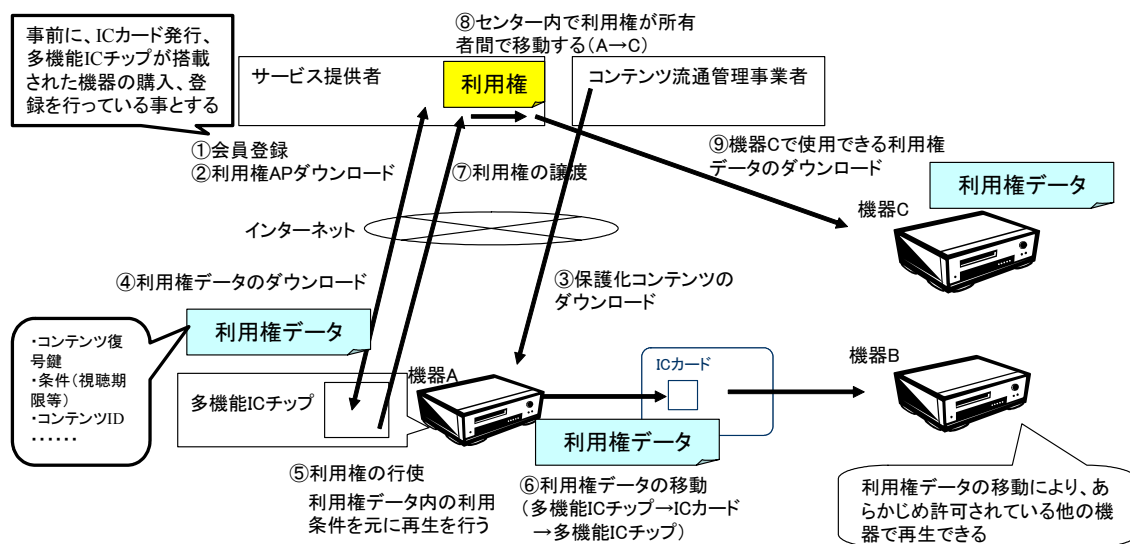


図 3-9 利用権データの流通の仕組み

### 3. 3. 2 実効性検証の環境

実効性検証では、マルチメディア情報流通サービスに関連する環境として、コンテンツ再生機器としての PC に、内蔵されている多機能 IC チップに相当する IC カードと、利用者の IC カードに相当する IC カードを接続し、多機能 IC チップおよび IC カードの活用によるマルチメディア情報流通の機能を実現した。そのうえで、コンテンツ流通にかかわる関係者に対してシステムのデモンストレーション (デモ) を行い、アンケートやヒアリングによる評価を集めると共に、開発関係者による技術的な検証を通じて、サービスおよびシステムの実効性検証を行った。

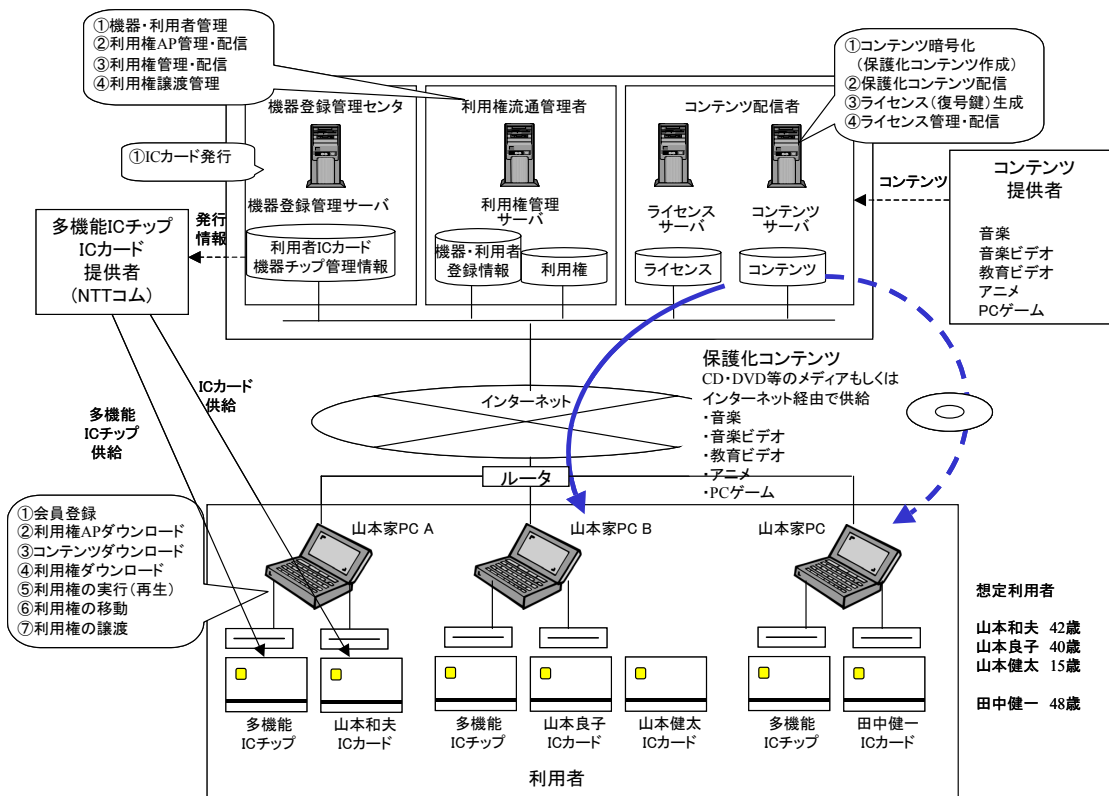


図 3-10 システム構成図

### 3. 3. 3 検証結果

実効性検証では、マルチメディア情報流通サービスの構築および実験環境での運用によって解決される課題や明らかになる項目についての仮説を立て、システムの動作や利用者へのアンケート、技術面における机上での検討等の方法によって検証を行った。

多機能 IC チップフレームワークを活用したサービス提供の有効性分析

(1) 多機能 IC チップフレームワークを利用したマルチメディア情報流通サービスを現実のコンテンツ流通サービスとして実現する可能性について検証した。

#### ①関係者間の契約関係に関する整理

制度検討小委員会での討議を踏まえ、本サービスの関係者間での契約関係について、以下の観点により整理した。

- ・各権利者とコンテンツ配信者との契約関係
- ・各権利者と利用者との契約関係
- ・コンテンツ配信者と利用権流通管理者との契約関係
- ・コンテンツ配信者と利用者との契約関係
- ・利用権流通管理者と利用者との契約関係
- ・多機能 IC チップを搭載した機器の製造者との契約関係

## ②事業者・権利者の意見

総じて高い割合のモニタが、マルチメディア情報流通サービスに対して好意的であるが、同時に、普及に向けては機器の普及および仕組みのわかりやすさが課題であることが、いずれの立場からも指摘されている。今後サービスの実用化に向けては、対応機器を普及する際に利用者や事業者の負担感を少なくするための工夫が必要であること、サービスの仕組みについて、利用者にとって分かりやすく理解できるようにすることが必要であることが明らかになっている。

利用者の利用希望について図3-11に示す。

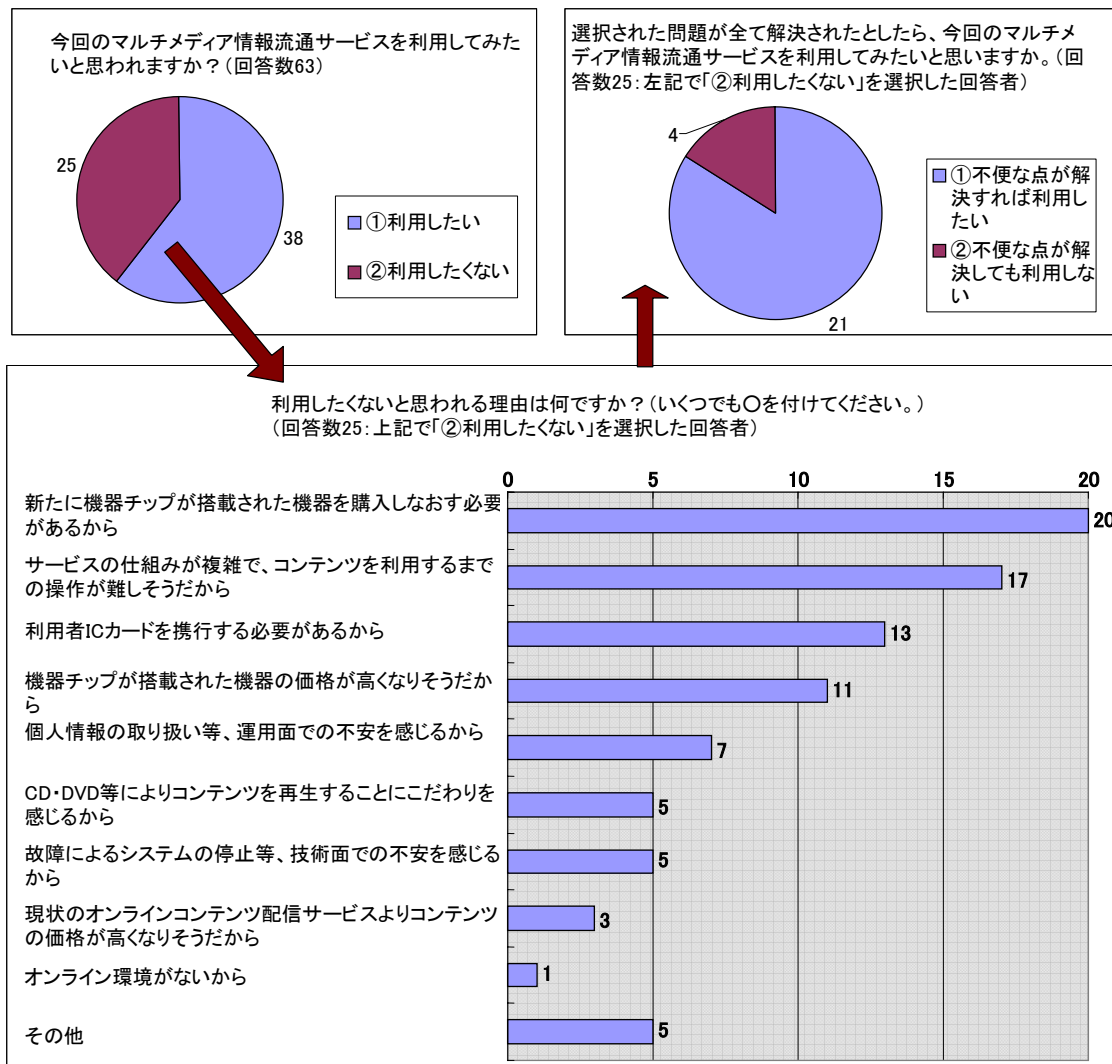


図3-11 サービスに対する利用者の利用希望

(2) 多機能 IC チップフレームワークを活用したサービスのセキュリティ評価

① モニタによるアンケートの評価

図 3-12 では、設問「インターネットを利用したコンテンツ配信を行う上で問題だと思われることは何ですか」（複数回答）に対して「著作権の保護が不十分になる」を挙げた集合をグループ A、設問「今回の多機能 IC チップを活用したマルチメディア情報流通サービスが普及すれば、ネット上での音楽コンテンツ配信事業を行う上での利便性向上や、事業における売上増加に結びつくと思われませんか」に対して「結びつくと思う」と回答した集合をグループ B、グループ B のうち、その理由（複数回答）に「著作権の保護強化が可能になるから」を挙げた集合をグループ C としている。

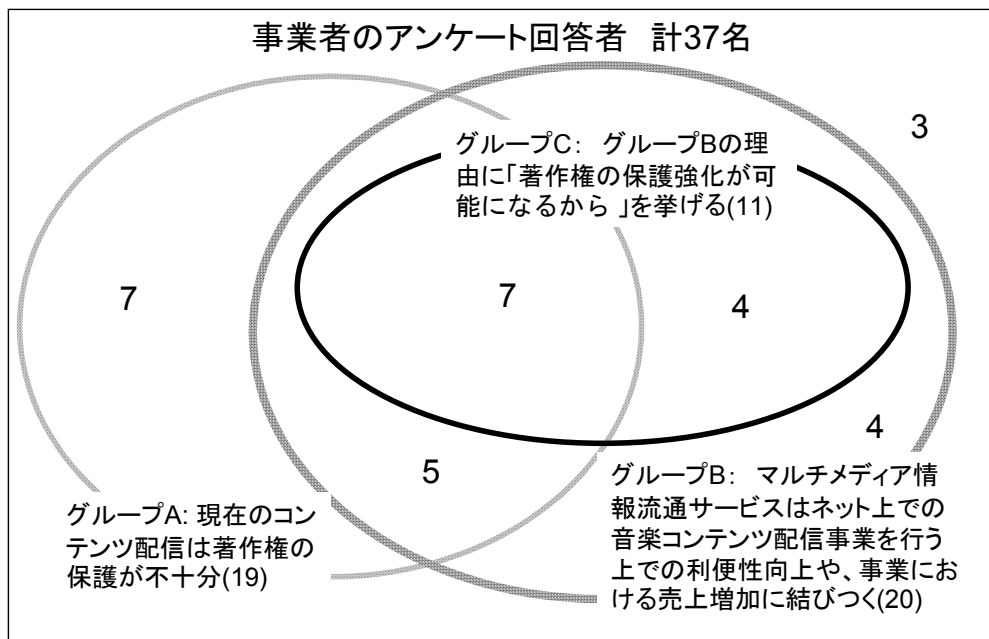


図 3-12 事業者によるセキュリティへの評価

上記の結果より、システムのセキュリティに対しては多くの関係者が期待をもち、多機能 IC チップフレームワークを活用したサービスの実現に対して、モニタの多くは、セキュリティ面を好意的に捉えていると理解できる。

② 権利侵害への対応範囲

公開鍵暗号方式によってコンテンツ流通における権利侵害を防止することもできても、コンテンツに対する権利侵害の全てを防止することはできない。表 3-1 に、前述した権利侵害に対する、上記サービスモデルでの対処範囲を示す。

表3-1 公開鍵暗号方式によるサービスモデルで対策可能な権利侵害

権利侵害のパターン	サービスモデルでの対応可否
(ア) 流通以前の段階（権利者周辺）での権利侵害	
正規に流通しているコンテンツの権利者を装う権利者のなりすまし	流通業者と権利者の間に認証を採用することで技術的には対応可能
権利者の不注意や盗難等による許諾されていないコンテンツの流出	暗号化以前のコンテンツの流出には権利者や流通業者の対策が別途必要
内容を不正に利用して別のコンテンツとして流通させる盗作等	デジタルデータを活用する盗作は機器の認証で防止可能。内容の盗作は既存の枠組みで対処
(イ) 流通段階での権利侵害	
正規品と同じ製品を無断で追加製造し流通させるオーバープレッシング	コンテンツ視聴のための復号鍵の流通は厳密に管理可能。ただし、暗号化以前のコンテンツの流出には権利者や流通業者の対策が別途必要
正規製品とは異なる海賊盤の流通	暗号化以前のコンテンツの流出には権利者や流通業者の対策が別途必要
販売店でのパッケージの窃盗（万引き）	パッケージに記録されたコンテンツは暗号化されているため万引きによる被害を極小化
(ウ) 不正な再生機器および製造業者	
権利保護の仕組みを働かなくした再生機器の流通	コンテンツの不正使用が可能なことが明らかになった機器での再生を停止可能
利用者が再生機器やコンテンツ記録媒体を改造して権利保護を解除	コンテンツの不正使用が可能なことが明らかになった機器での再生を停止可能
権利保護の仕組みが働かないよう再生機器を改造	権利保護の仕組みのない再生機器は認証されないため、コンテンツは再生されない
(エ) 利用者での権利侵害	
カラオケ教室等での違法な複製	再生機器でデジタルデータでの複製は防止
個人用に購入したパッケージによる商業的利用	コンテンツの再生場所や表示・演奏方法まで制限することは難しく、別途対策が必要

(3) 法制度等との整合性評価

マルチメディアコンテンツ流通サービスにかかわる以下の操作場面について、関係者間で処理されるべき権利について整理した。

- ・暗号化されたコンテンツの生成
- ・暗号化されたコンテンツのサーバへの蓄積
- ・暗号化されたコンテンツのダウンロードその他の方法による入手
- ・暗号化されたコンテンツのユーザによる端末への蓄積
- ・利用権としてのコンテンツ復号鍵の配信
- ・暗号化されたコンテンツの復号又は再生
- ・復号されたコンテンツのユーザ端末への蓄積
- ・暗号化されたコンテンツの譲渡
- ・利用権の譲渡



サービスの実現のためには、関係者が保持する権利とサービスで提供しようとする機能、発生する場面に基づき、関係者が持つ権利を利用者に許諾する契約を結ぶ必要が生じる。

これらの契約によって権利関係が整理された状況下においては、本事業のシステムは、個別のコンテンツに関する使用許諾を安全に管理するシステムとして位置付けられる。

#### (4) 既存サービスとの相互運用性評価

本事業で開発したマルチメディア情報流通サービスのシステムは、PKI を活用して保護化コンテンツの利用権の流通を管理する。従って、暗号化されたコンテンツを復号・再生するための情報の流通を、PKI を利用して実施しているサービスは、コンテンツやサービスの相互運用の可能性がある。

PKI を利用して利用権の流通を管理する複数のサービスの間での相互運用には、以下のケースが考えられる。

- ・一種類の保護化コンテンツを、複数のサービスで利用権を設定して流通させる（保護化コンテンツの相互利用）。
- ・一方のサービスから提供される利用権を、他方のサービスを通じて入手し、保護化コンテンツを再生できる（利用権配信の相互利用）。
- ・一方のサービスに利用している再生ソフトウェアに、他方のサービスで流通させている保護化コンテンツと利用権データを記録してコンテンツを再生できる（利用権の相互利用）。

上記のうち、保護化コンテンツの相互利用と利用権の相互利用は技術的に実現可能だが、利用権流通の相互利用については相互運用性がないことが確認された。なお、利用権の相互利用では、利用権に含まれる回数、期間、利用者、譲渡の可否といった、詳細な使用許諾条件の表現方法や管理方法に相互運用性がなければ、実際にコンテンツを再生することはできない。

#### (5) 情報の分野ごとの利用者の要求調査

利用者のアンケートから、情報の分野ごと、あるいはサービスによらない、コンテンツ流通サービスに対する利用者の要求を調査した結果について以下に示す。

マルチメディア情報流通サービスによってインターネットでの各種コンテンツの入手が便利になると予想するか否かの質問に対して「便利になる」と回答した理由を表3-2に整理する。

表3-2では、コンテンツ毎に回答数上位3種の選択肢に網掛けをしている。利用権を複数の機器で利用できること、利用期間の限定による現在よりも安価なコンテンツへの期待、利用権の再発行への期待が共通に挙げられている。

音楽コンテンツでは、他のコンテンツと比較して、複数の機器での利用、及び利用権の再発行への期待が高い。映像コンテンツでは、他のコンテンツと比較して、利用期間、利用回数を限定することによりコンテンツを安価に入手することへの期待が高い。コンピュータゲームでは、他のコンテンツと比較して、コンテンツの譲渡への期待が高い。

表 3-2 本サービスに利便性を感じた理由

【今回の多機能ICチップを活用したマルチメディア情報流通サービスにより、インターネット上での音楽コンテンツ／映像コンテンツ／コンピュータゲームの購入とその利用は、便利になると思われますか？（1つだけ○を付けてください。）で「① 便利になる」を選択した方にお伺いします】なぜそのように思われますか？（いくつでも○を付けてください。）				
理由	コンテンツ	音楽 コンテンツ	映像 コンテンツ	コンピュ ータ ゲーム
① 購入したコンテンツが複数の自分の機器や家族の機器で利用できるから。		30 (71%)	27 (56%)	21 (47%)
② 事業者による利用期間の設定が可能になり、利用期間に応じた価格の音楽を購入することができるから。		15 (36%)	19 (40%)	15 (33%)
③ 事業者による利用回数の設定が可能になり、利用回数に応じた価格のコンテンツを購入することができるから。		7 (17%)	13 (27%)	10 (22%)
④ コンテンツの利用権を譲渡できるから。		13 (31%)	12 (25%)	17 (38%)
⑤ 利用権データやコンテンツが記録されている機器・媒体を紛失・破損しても、利用権の再発行を受けられるから。		19 (45%)	15 (31%)	15 (33%)
⑥ 提供者が、コンテンツの利用に年齢制限を設けることができるから。		6 (14%)	7 (15%)	6 (13%)
⑦ その他		1 (2%)	4 (8%)	2 (4%)
回答者数(全アンケート回答者66名中、それぞれのコンテンツについて「便利になる」を選択した回答者数)		42 (100%)	48 (100%)	45 (100%)

注：コンテンツごとに回答者数はことなり、また複数回答のため各選択肢の合計と回答者数は一致しない。  
コンテンツごとの選択肢のうち上位3種には網掛けを、また、選択肢ごとに最も多い割合が回答しているコンテンツを斜体および下線で、それぞれ表示している。

## (6) マルチメディア情報流通サービスにおける機能検証

### ① システム動作による機能検証

機器登録のなされている複数の機器、登録がなされた複数の利用者を前提に、コンテンツの利用権が異なるシナリオを準備し、利用権の移動、譲渡等の操作を行い、利用権管理機能の有効性を検証した。

利用権の設定の範囲での操作と、利用権の設定範囲を超える操作を試みた。その結果を表3-3に示す。利用権の移動、譲渡および利用権の行使によるコンテンツの再生について、あらかじめ利用権に設定することで制限可能なことと、同時に、設定された制限の範囲内では、利用者は自由に利用権およびコンテンツを利用できることが確認された。

表 3-3 検証結果

シナリオ	動作	結果
許可された範囲でのコンテンツの移動	自分が管理する他の機器へ利用権を移動	本人の IC カードでのみ利用可
	他人の機器へ利用権を移動	本人の IC カードでのみ利用可
利用権の制限に基づく移動の禁止	自分が管理する設定外の機器へ利用権を移動	利用不可
	他人が管理する機器へ利用権を移動	利用不可
年齢制限に基づく利用の禁止	年齢制限を満たす家族が利用	制限年齢以上の家族の IC カードで利用可
	年齢制限を満たさない家族が利用を試みる	制限年齢未満の家族の IC カードで利用不可
許可された範囲でのコンテンツの譲渡	他の利用者を指定して利用権を譲渡	譲渡先の利用者が利用権をダウンロード後、利用可
年齢制限に基づく譲渡の禁止	制限年齢に達しない利用者を指定して利用権を譲渡	利用権はもとの利用者に残り、譲渡先の利用者に移動できない
再生回数の制限	継続的にコンテンツを利用	設定された回数の利用後は再生ができない
再生期間の制限	継続的にコンテンツを利用	設定期間以降の日時には再生ができない

## ②利用権への制限に対するモニタの評価

モニタへのアンケートによって、利用権の制限を付したコンテンツの流通について感想を求めた。利用者、事業者、権利者のそれぞれの立場を考慮し、異なる設問で感想を求めた。

- ・利用者に対しては、利用権を制限することによって利用権のないコンテンツよりも安価に提供される可能性について感想を求めた。
- ・事業者に対しては、本サービスによるネット上でのコンテンツ配信事業への効果を期待する利用者に対して、その理由の選択肢として提示した。
- ・権利者に対しては、本サービスへの利便を感じる点についての設問として、利用権の制限を含む本サービスの特徴について選択肢を提示した。
- ・結果として、利用制限を含むコンテンツの利用、及び提供については、それぞれの層から利用したいという希望があることが明らかになっている。

## ③利用権の譲渡に対する権利者及び事業者の感想

利用権の譲渡については、事業者、権利者とも、3割から4割「コンテンツを配信したい」という前向きな回答が得られた一方、同程度の回答が「その他」と、デモと説明の範囲では明確な回答がされていない。

事業者からの回答の「その他」としては、ユーザメリットが見えない、(譲渡行為に課金することについて)利用者の理解が得られない、といった意見が得られた。

権利者からの回答の「その他」としては、事業者任せたい、普及状況による、といった意見が得られた。

### 3. 3. 4 多様な利用者端末への対応に関する検討

多機能 IC チップの実装が期待される端末として、PDA を中心に機能要件及び実装条件について整理をした。

#### (1) 機能要件の整理

PDA に必要な機能要件として、以下を抽出した。

- ・利用者端末登録機能
- ・利用権管理機能
- ・コンテンツ移動時の利用者および利用者端末認証機能（オプション）
- ・オフライン利用権確認機能（オプション）
- ・コンテンツ送信時の利用権自動確認機能（オプション）
- ・コンテンツ再生における耐タンパ処理機能

#### (2) 実装に関する考察

検討結果に基づき、想定される実装上の問題点について整理をする。

##### ①PDA に埋め込む多機能 IC チップの耐タンパ性実現

- ・ PDA を分解し、多機能 IC チップを取り出し、他の PDA に組み込むという、成りすまし目的の違法改造を防止するために、内蔵する多機能 IC チップだけでなく、PDA 自身にも多機能 IC チップと同等の耐タンパ性を持たせる必要がある。内部に接着剤を充填するなど分解不可能な構造とすることは可能だが、工程や修理時の作業性およびコストとの両立が必要である。
- ・ 万が一分解され、多機能 IC チップを取り出される場合のことを考えると、分解の過程を検出し多機能 IC チップに分解されたという刻印を記録しておく対策が考えられるが、刻印のための電源の確保および修理などの正規の分解との識別方法も問題となる。

##### ②コンテンツ再生における耐タンパ処理機能の負荷

- ・リアルタイム性が求められるコンテンツの再生において、復号・解凍エンジンをソフトウェアとして実現するのは、PDA にとって負荷が大きいため、場合によっては専用チップとして組み込む対策が必要になる。
- ・またメモリ上に展開したデータを外部から取り出せないように設計することも必要である。バスから切り離れた復号・解凍エンジン専用のメモリ領域を用意する必要がある。

### 3. 4 会員権サービスの実効性検証

多機能 IC チップフレームワークの適応事例として、顧客情報を会員情報として多機能 IC チップ上に搭載し、安全性を確保したうえで、さまざまなサービスから利用することで利便性の向上を図る「会員権サービス」の実効性検証を行った。

#### 3. 4. 1 会員権サービスの概要

会員権サービスとは、会員であることで、会員限定のさまざまなサービスを利用できるサービスを言う。

会員権サービスでは、多機能 IC チップを搭載した IC カードに、会員向けのサービスを利用することのできる権利である「会員権」を搭載し、その会員権に基づき、個人個人が自ら使ってみたい会員向けサービスを IC カードにダウンロードできる、という仕組みを提供する。ここで言う会員権とは、個人に紐付けられた権利情報であり、権利流通管理システムで言う「利用権」に相当し、個人を識別する識別情報のほか、個人の属性情報、PKI の秘密鍵と公開鍵証明書を有している。

この仕組みの導入により、次のようなことが可能となると考えられる。

- ・会員権を利用してさまざまなサービスを利用できる。
- ・個別のサービスは、ネットワークを通じて、随時、IC カードへの追加や削除ができる。
- ・個別のサービス利用時の利便性が向上できる（利用権の持つ情報をサービスに利用できる。例えば、簡単な手続きで新しいサービスの利用が可能）。
- ・一度会員になれば、利用権（会員権）はさまざまな多機能 IC チップを搭載した機器、媒体に格納することが可能（いつでもどこでも、その場面に合った機器でのサービス利用が可能）。

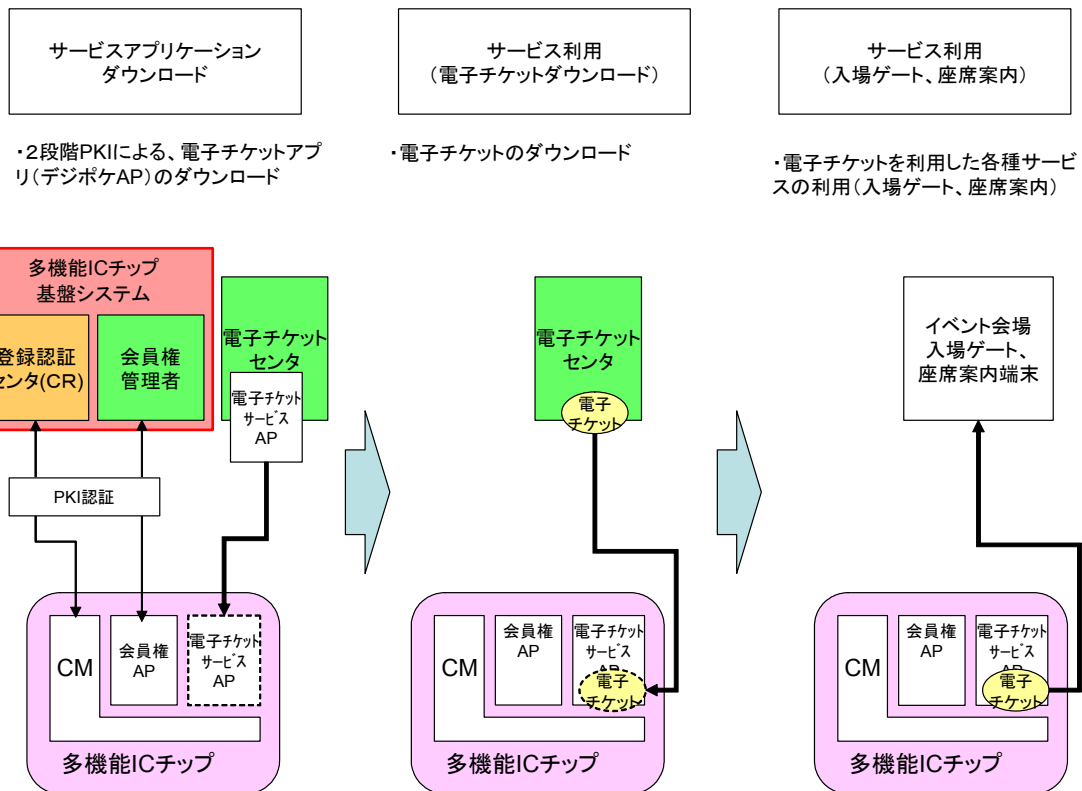


図 3 - 1 3 サービス利用手順

### 3. 4. 2 実効性検証の概要

図 3 - 1 4 に実効性検証環境の概要を示す。カード基盤センタに、多機能 IC チップの発行運用管理の機能を持たせると共に、会員権管理、サービスアプリケーションのダウンロード機能を持たせ、既存の電子チケットセンタと連携することで、会員権サービスの提供を行った。利用者は、モニタ説明会場にて電子チケットサービス AP のダウンロードを行った後、家庭や会社にて電子チケットのダウンロードを行った。以上の手続きを経たうえで、イベント会場にて提供される入場ゲートや座席案内のサービスを利用した。

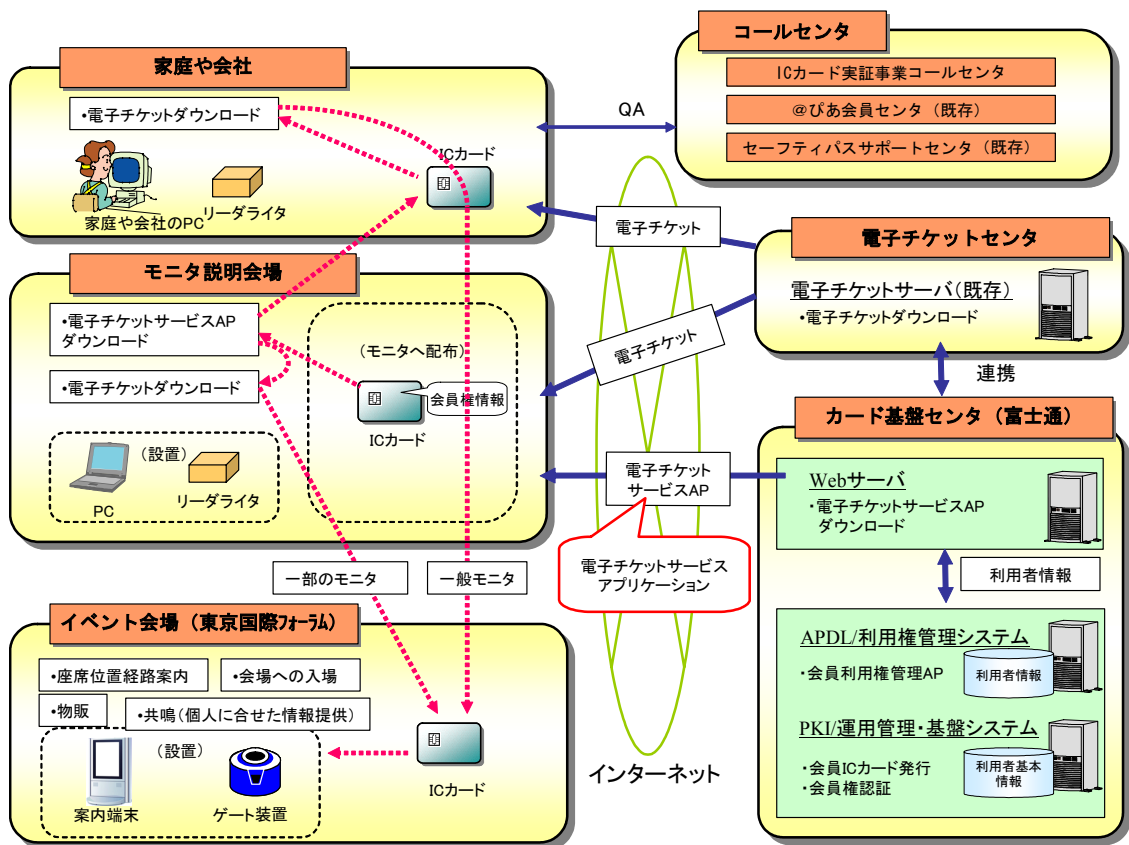


図3-14 実効性検証環境の概要

### 3. 4. 3 検証結果

実効性検証においては、多機能 IC チップフレームワークを活用した会員権サービスの有効性、および既存サービスとの相互運用性、といった 2 つの観点で検証を行った。さらにそれぞれの観点に対し詳細化を行い、合計 4 つの検証項目について検証を行った。検証にあたっては、実証データとして、アンケート結果、ヒアリング結果、および処理時間等のデータ、を収集し、検証項目に従って、評価分析を行った。

#### (1) 多機能 IC チップフレームワークを活用したサービス実施のためのフレームワーク有効性

サービス実施のためのフレームワークにおける多機能 IC チップフレームワークの有効性について検証を行った。

##### ①利用者側のメリット・デメリット

###### (a) 利用者の AP ダウンロード操作性

操作自体を手間だと感じたかどうかについて、図3-15に結果を示す。

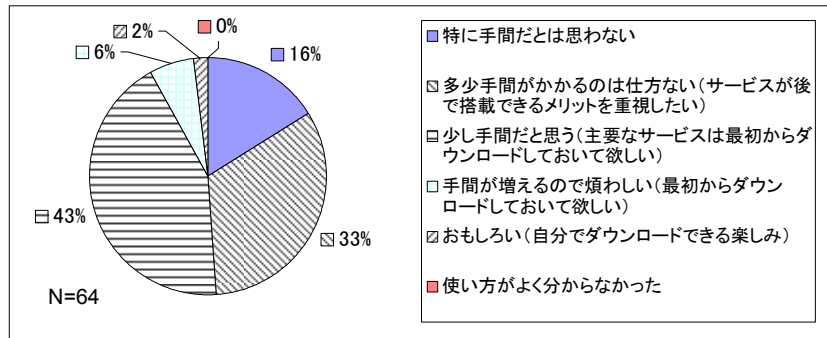


図3-15 APダウンロード操作への感想(モニタ説明会后アンケートより)

また、ダウンロードにかかる時間についての評価を、図3-16に示す。

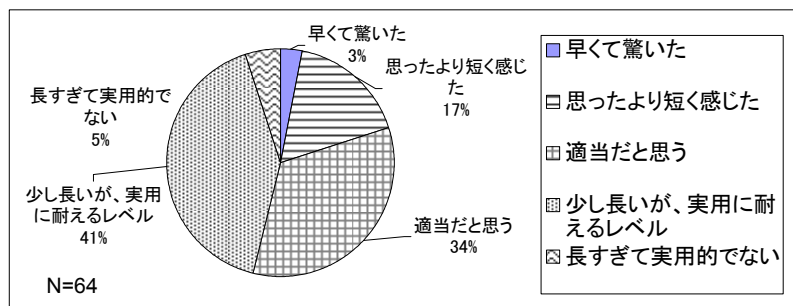


図3-16 ダウンロード所要時間への感想(モニタ説明会后アンケートより)

操作に関しては、ほぼすべての利用者が問題ないと答えている一方、約半数の利用者は、事前にAPダウンロードしておいて欲しいと答えている。

また、ダウンロード時間が長く感じたことと、手間が増えると感じることの間には相関関係が見られなかったため、利用者にとっては純粹に手順が増えること自体が手間であったと認識できる。一方、ダウンロード自体を全く必要ないと考える利用者は、1割以下しかおらず、メリットがあれば操作自体に対しては、大きな抵抗感は見受けられなかった。ただし、本実証でのモニタに、PC習熟者が多い点には注意する必要がある。

#### (b) 利用者のAPダウンロード時間の評価

本実効性検証においてのAPダウンロード時間は平均約52秒(47秒~56秒)であった。これに対し、半数近い利用者は、時間を長く感じていた。ただし、この時間に対して、実用的でないと答えた利用者は、5%しかおらず、おおむねこの程度の時間まではストレスなく操作してもらえるとと言える。



(c) 会員権に基づくサービス登録時の入力項目数の評価

会員権サービスの特徴として、会員権を取得する際に登録した情報を個別サービスにも活用することにより、個別サービス開始時の利用者情報の登録を減らすことができることが挙げられる。会員権情報として分類 1 の情報を持つことで、1 サービスあたりの平均登録項目数 14 項目の内、7.5 項目の入力が不要となり入力項目数を約 50%程度削減することができる。さらに、分類 2 の情報を含めると 10 項目の入力が不要となり、70%程度の削減が期待できる。

(d) 会員権に基づくサービスの追加・削除の評価

会員権に基づくサービスの追加・削除について有効性を利用者に対し、どのような点に有効性を感じるかを調査した結果を、図 3-17 に示す。

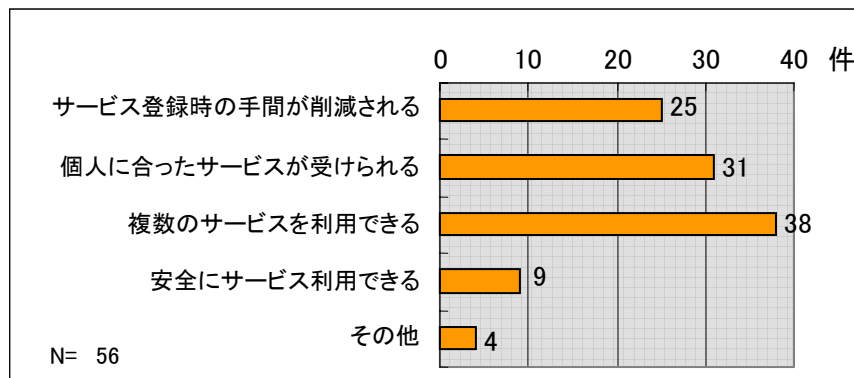


図 3-17 有効性を感じる理由（複数回答）（モニタ説明会后アンケート）

多くの利用者が会員権に基づくサービスの追加・削除機能について有効性を感じていると言える。特に、会員情報によりサービス登録時の入力の手間が削減される点や、個人にカスタマイズしたサービスが提供できる点など、利便性の向上に対して評価が高い。

一方、少数ではあったが、有効性を感じないと答えた利用者の挙げた理由としては、手間の増加と安全性の不安にほぼ集約された。

②サービス提供側のメリット・デメリット

多機能 IC チップフレームワークを適応したサービスの提供を通じて、サービス提供者から見たメリット・デメリットについて検証した。

(a) サービス利用媒体、機器の評価（利用者側）

会員権サービスでのサービス追加機能について、利用者がサービスを受けたい場所について調査した結果を図 3-18 に示す。

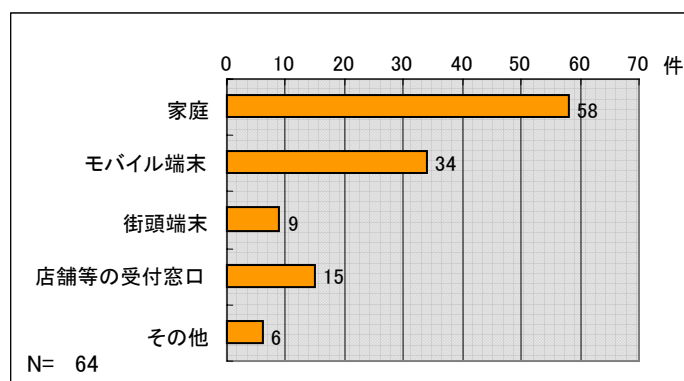


図3-18 サービスを受けたい場所（複数回答）（モニタ説明会后アンケート）

サービス利用場所については、家庭を望む声が非常に高く、半数程度の利用者では、モバイル環境での利用に対する要望も高かった。その他の意見として、職場や、コンサート会場などのサービス導線上を望む意見というものもあった。一方、街頭端末や店頭での利用への希望は少なく、利用者が自分の行動に合わせた場所でサービス利用したいという意識が高いことがわかる。

(b) サービス提供者メリットの評価

サービス提供者が会員権サービスに参加することで得られるメリットについて調査した結果を図3-19に示す。

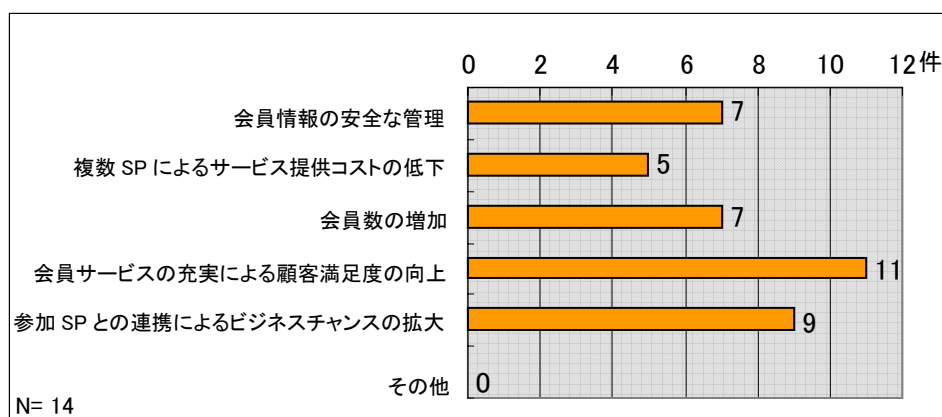


図3-19 会員権サービスによるサービス提供者のメリット（複数回答）（ヒアリングより）

以上のように、サービス提供者にとっては、他サービス提供者との連携による顧客の獲得、ビジネスチャンスの拡大や、サービスの充実による顧客満足度の向上といった観点でのメリットを感じている。ただし、複数のサービス提供者が連携することによる、セキュリティの確保、責任の切り分け、といった点に十分注意する必要がある。

## (2) 多機能 IC チップフレームワークを活用したサービスのセキュリティ

会員権サービスにおいて、本実効性検証で実施したセキュリティ対策が適切なものであったか、セキュリティ対策による負担増やサービス低下の影響、実用性について検証した。

### ①運用性の評価

#### (a) 利用者側のサービス低下評価（処理時間増（AP ダウンロード時））

多機能 IC チップフレームワークでの、1 階層目の PKI 認証が、2 項目の「CM と SP との相互認証」となり、2 階層目の PKI 認証が、4 項目の「利用権確認」となる。これらの処理時間の合計約 8 秒程度が、2 階層 PKI を行うことにより増加する処理時間である。

AP ダウンロード時に限って言えば、全体処理時間約 52 秒の 16%程度の割合であり、多大なサービス低下を招くとは言えない。しかし、ある程度の処理速度が要求されるサービス等においては、サービス利用時の処理時間は数秒であり、この処理時間増はサービスの利用感に影響するため、サービス低下に成り得る可能性も否定できない。

#### (b) 運用者側の負担増評価（利用者情報の受け渡し）

本実効性検証ではセキュリティ対策における運用面での大きな負担は生じなかったと言える。ただし、複数プレーヤ（企業等）が個人情報を取り扱う場合、各社で取り決めたセキュリティポリシー、および運用ガイドラインに則った厳格なセキュリティ運用が必要となり、各社間の合意や役割分担の明確化にかかる負荷、コストの増加に関して考慮する必要がある。

### ②セキュリティ向上意識の評価

多機能 IC チップフレームワークを適応することによる、利用者のセキュリティに対する意識の違いについて検証する。

#### (a) 利用者のセキュリティに対する意識

住所・氏名やユーザ ID といった直接個人と結びつく情報については、約 9 割の利用者が情報の利用に際して安全性の確保を求めており、高い安全性に対する要望が非常に高いことがわかる。

#### (b) 利用者の安心感の評価

IC カードの保持に関しては、ほとんどの利用者が不安を感じていない。

半数近い利用者が、今までのカードと同様なため、とりたてて不安はないと答えているが、言い換えれば、利用者はカードに搭載した情報の違いについてはあまり意識していないことがわかる。一方、多機能 IC チップやフレームワークのセキュリティの高さに関連した理由によるものは 30%強であった。本実証においては、実証モニタに対してサービス利用前に、多機能 IC チップとフレームワークについての安全性について説明を行ったが、直接の安心感にはつながっては

いないようであった。

以上のように、会員権搭載の IC カードを保有すること自体についての不安は見受けられないが、安全性の周知については考慮する必要がある。

### (3) 法的スキームとの整合性

#### ①個人情報の第三者提供に関する条項

本実効性検証においては、モニタから収集した個人情報を第三者に提供することが想定される点が特徴となる。

本実効性検証においては、実証モニタに対して、モニタ参加規約により、個人情報の定義を行ったうえで、使用目的、および使用範囲を明確化し、同意を取ることでも対処した。また、複数企業で個人情報を利用することになるため、個人情報管理規約に沿って、管理運用を行った。

前項に示した法律およびガイドラインに対する、本実証での具体的対応を、表 3-4 に示す。

表 3-4 本実証での具体的対応

項	法律・ガイドライン名	本実効性検証対応結果	本実効性検証個人情報運用管理規約	本実効性検証モニタ参加規約
1	個人情報の保護に関する法律	<p>実証実験担当会社および再委託先は、モニタ参加者に対し、個人情報収集の目的、収集する情報の範囲、実証実験担当会社から再委託先に対し、実験の目的の範囲内で必要な個人情報を提供することを事前にモニタに示し同意を求める。</p> <p>モニタはプロフィール情報（住所、氏名、電話番号、職業、性別、クレジットカードデータ等）の提供をするものとし、実証実験担当会社が再委託先に対してプロフィール情報を本実験の目的の範囲内で使用するために提供することに同意する。</p> <p>実証実験担当会社および再委託先は、関連する法およびガイドラインに基づき定めた個人情報運用規約に従い、モニタのプロフィール情報を本実験で必要な範囲で利用する。</p>	管理規約第 1 項～第 7 項	第 6 条（モニタの義務）の 3 第 11 条（プロフィール情報の保護）第 12 条（プロフィール情報の管理運用）
2	電気通信事業における個人情報保護に関するガイドライン			
3	個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q 15001）			
4	サイバービジネスに係る個人情報の保護に関するガイドライン			
5	情報サービス産業 個人情報保護ガイドライン			
6	電子ネットワーク運営における個人情報保護に関するガイドライン			
7	民間部門における電子商取引に係る個人情報の保護に関するガイドライン			

以上のように、本実効性検証において行った個人情報保護についての対策について、法制度との整合を確認した。また、新たなサービス追加に対しては、制度小委員会での内容を踏まえ、利用者に対し、その都度同意を取ることが必要となる。

#### (4) 既存サービスとの相互運用性

会員権サービスにより利用できるサービスとしては、既存の電子チケットサービス等を利用する。これらサービスを会員権サービスと連携させるにあたり、既存サービスとの相互運用性を確保することが必要となる。

本実効性検証においては、制限付きではあるが、既存サービスに影響を与えることなく既存サービスとの相互運用性を確保し、サービスを提供することができた。ただし将来的に、現在のサービスで使用していない多様な機器への対応を想定する場合や、役割分担を明確化した運用体制の確立等において、既存サービスへの影響が不可避であると考えられる。

### 3. 4. 4 超小型セキュア ID チップとの連動に関する検討

紙のチケットに入れ込んで発行され、偽造防止や改札の省力化を実現するとの期待の高い超小型セキュア ID チップと、利用者が持つ多機能 IC チップ実装機器とを組み合わせることによって、サービスの連携を行う仕組みの検討を行った。

超小型セキュア ID チップの特長として、①安価であること、②超小型であること、が挙げられる。このため、紙にすきこむことやプラスチックカードに入れることもでき、入場券として利用することに適している。逆にデメリットとしては暗号化処理ができないため、暗号化通信を使ったサービス等には適さない。一方、多機能 IC チップは CPU とメモリを保有しており、暗号化処理も可能である。そこで、超小型セキュア ID チップの利便性と多機能 IC チップのセキュリティを併せることにより、多彩なサービスを実施することができると期待される。

超小型セキュア ID チップと多機能 IC チップを組み合わせたサービスの一例として、イベント会場等での利用を想定し、超小型セキュア ID チップ搭載入場券を保有している来場者のみがコンテンツを利用できるサービスを検討する。

これにより、ID を搭載した入場券を使用し、来場者へのサービスやセキュリティの向上を実現することができる。このイメージを図 3-20 に示す。

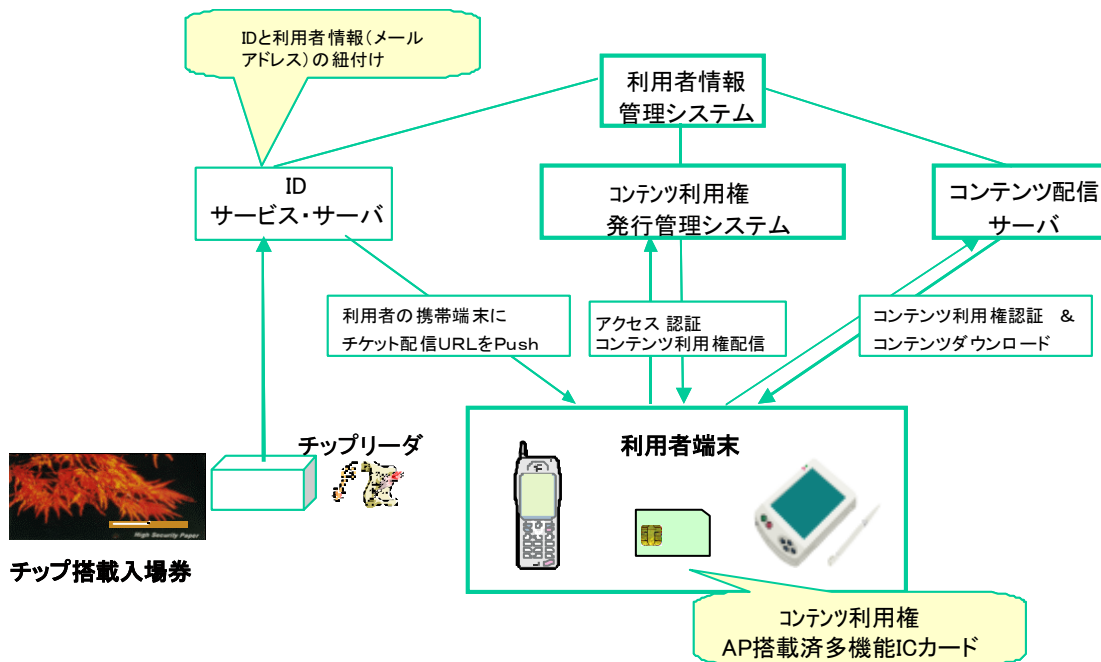


図 3-20 入場券とサービスの連携 (PDA、携帯端末の利用)

具体的なサービスとしては、利用者のイベント会場や会場内の様々な場所への来場を、チケットの確認と同時に超小型セキュア ID チップによって認識し、利用者の多機能 IC チップ搭載端末に、利用者が利用しているイベントやアトラクション等に関連するコンテンツを提供する。多機能 IC チップ搭載機器の活用によってセキュリティを確保するため、利用者の趣味、嗜好といった個人情報や、撮影した写真など活用したコンテンツを、利用者の安心のもとに提供することができると期待される。

### 3. 5 多機能 IC チップを搭載した携帯電話への適用の検討

本事業では、携帯電話の非接触 IC カード機能や UIM 機能を利用して、多機能 IC チップ搭載機器としての活用を図るための検討及び検証を行なった。

- ・ ISO/IEC 14443 TypeB インタフェースを持つ携帯電話の試作および実効性検証
- ・ UIM の PKI 認証機能と大容量データの蓄積が可能な外部メモリカードを活用したセキュアなコンテンツ配信サービスの検討および実効性検証

#### 3. 5. 1 多機能 IC チップフレームワークの携帯電話への適用の検討

##### (1) 概要

ISO/IEC14443 タイプ B 準拠の多機能 IC チップを IC チップ向けアンテナが搭載された携帯電話に搭載し、プロトタイプ機を 2 台 (MT-01 機、MT-02 機) 作成した。多機能 IC チップの搭載は図 3-21 に示す通り、第三世代の携帯電話の UIM (User Identity Module) カードスロットに装着した。

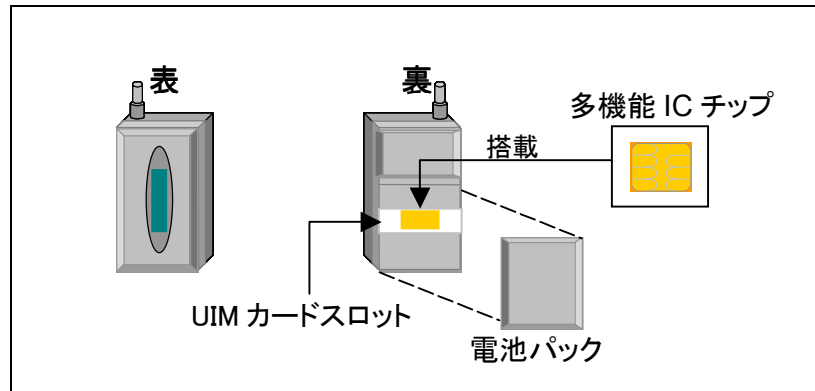


図 3-21 多機能 IC チップ搭載携帯電話の概要

本研究では、多機能 IC チップ（タイプ B）に搭載する、携帯電話上に搭載する Java アプリケーションと多機能 IC チップの連携、および多機能 IC チップとリーダーライタ間の非接触インタフェース通信の仕組み・性能・操作性などを検証した。

多機能 IC チップは、携帯電話内の Java アプリケーションから接触インタフェースを通じたデータ入出力と、非接触インタフェースによるデータ入出力の双方の機能を持つ。また、携帯電話には多機能 IC チップに格納されているデータを画面に表示する機能を持つ。

## (2) 実効性検証の環境

本実効性検証では、実際に携帯電話商用通信網を利用（セキュリティ（SSL など）については本実効性検証の対象外）し、プロトタイプ機と施設予約サーバを連携させ、電子チケットのダウンロード、および多機能 IC チップ（タイプ B）への格納を行った。

また、ダウンロード後、プロトタイプ機を用いて、模擬入場ゲート環境（施設受付端末）による施設入場処理を実施した。施設入場処理には、多機能 IC チップでの認証を公開鍵（楕円曲線暗号）方式を用いて実現したうえで、電子チケットの認証を行う方式を採用した。

システム構成の全体図を図 3-22 に示す。

施設予約サーバ、施設受付端末、および非接触 R/W（施設の入場ゲートを想定）は施設予約サービス提供者が運営するシステムと想定している。

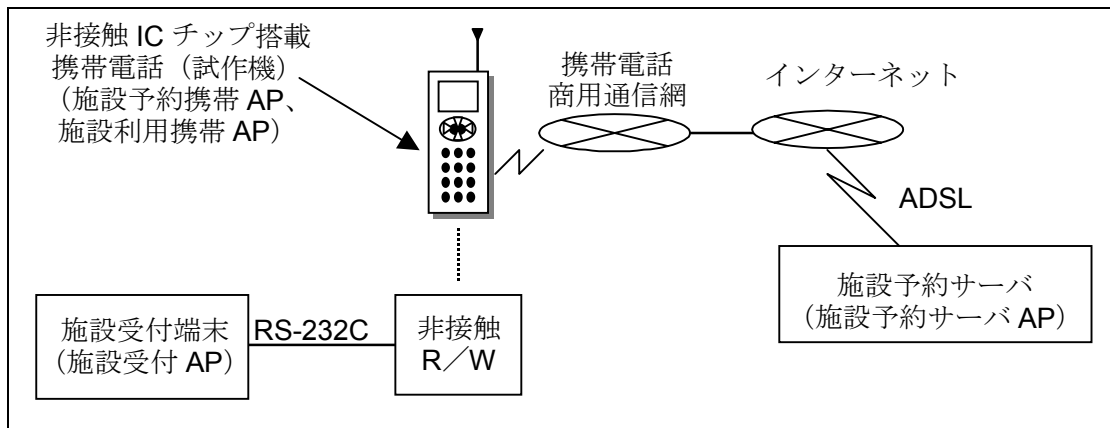


図 3-2-2 実効性環境のシステム構成

(3) 検証結果

①施設予約処理検証結果

チケットダウンロード処理 (チケット容量は 32 バイト)、および Java アプリケーション起動処理における IC チップアクセス処理時間の割合はそれぞれ、約 1.8%、約 1.4%であった。したがって、本実効性検証においては、IC チップ処理時間が全体に及ぼす影響は少なく、実運用でも適用可能である性能であると評価される。

チケットダウンロード処理時間内訳のグラフを図 3-2-3 に示す。

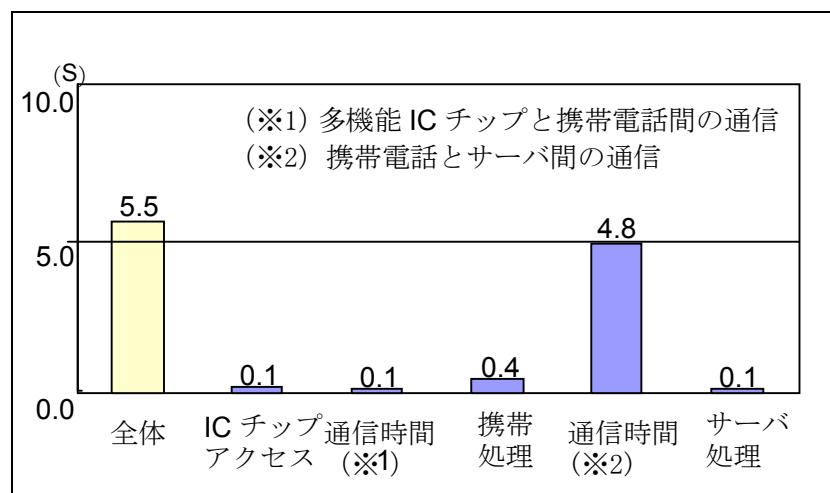


図 3-2-3 チケットダウンロード処理時間内訳

Java アプリケーション起動処理における測定結果を図 3-2-4 に示す。



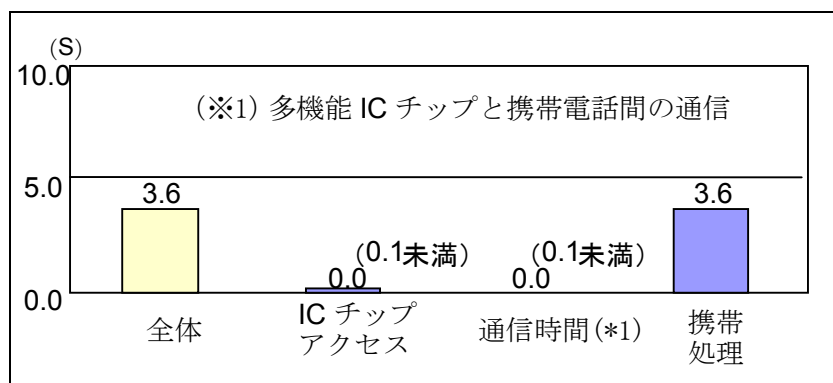


図3-24 Javaアプリケーション起動処理時間内訳

## ②施設入場処理検証結果

リーダライタにアンテナ面をかざした場合、最大通信距離は 74mm であった。測定環境、リーダライタの性能などに違いはあるが、本プロトタイプ機も実運用に適用可能であると思われる。また、多機能 IC チップ搭載携帯電話の状態が待ち受け時、通話時のいずれの場合でもほぼ同等の通信距離性能であることが確認されており、実運用に適用できると考えられる。

待ち受け状態において、F アンテナ面をかざし、X 軸、Y 軸、Z 軸にそれぞれ移動した場合の測定距離を図3-25に示す。

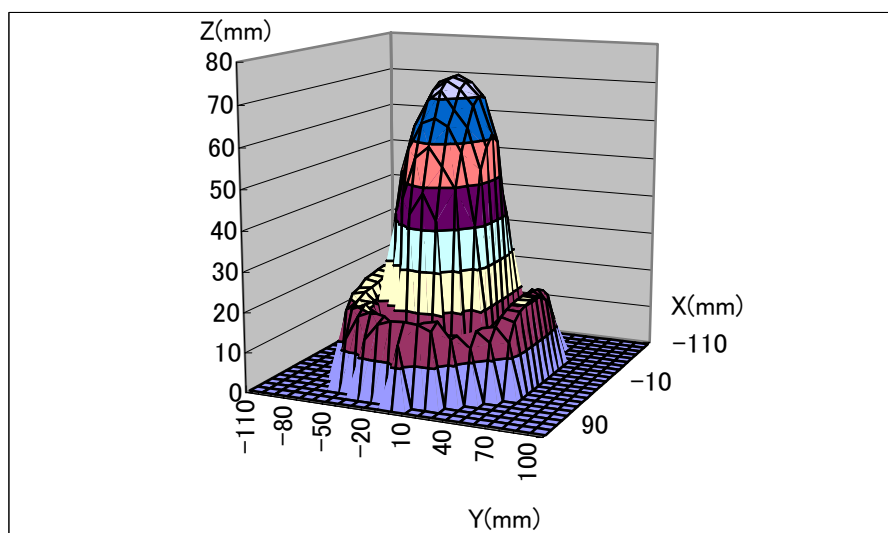


図3-25 非接触通信距離範囲 (XYZ 軸)

電源 OFF 状態においても、待受、および通話状態と同等の距離範囲を確保できていると考えられ、同様に実運用に適用可能であると思われる。

リーダライタに携帯電話の上面、下面をかざした場合、距離測定が不可能であった。これは、リーダライタの磁束線はリーダライタから垂直に伸びており、多機能 IC チップ搭載携帯電話のアンテナで磁界が打ち消されているためと考えられる。

チケット認証の速度については、IC チップ検出後から、チケット認証（施設受付端末画面表示処理含む）が完了するまで約 345ms であった。また、IC チップ処理については、IC チップ認証に関する処理が約 208ms、チケット読み出しの処理は約 7ms であった。

したがって、本プロトタイプ機を実運用に適用した場合、利用者に対して、高い利便性を提供できる可能性があると考え

### ③体感モニタによる操作性検証結果

体感モニタによる操作性検証結果を以下に示す。体感モニタ試験は、表 3-5 に示すように、体感モニタを 3 グループに分けて実施した。

表 3-5 体感モニタのグループ概要

項番	グループ	R/W との距離	携帯電話をかざす時間
1	A グループ	タッチしない	自由
2	B グループ	タッチしない	R/W 上で少し止める
3	C グループ	タッチする	R/W 上で少し止める

検証の結果、A グループと B グループでは、1 度の操作では認証処理を正常に実施することができなかったが、C グループでは全てのモニタが、1 度の操作で処理を正常に実施できた。

以上より、多機能 IC チップ搭載携帯電話は、「タッチ+僅かのストップ」であれば、実用化が可能であると考えられる。

## 3. 5. 2 携帯電話上の多機能 IC チップを想定したサービス提供システムの研究開発および検証

### (1) 概要

第三世代携帯電話端末に搭載された UIM カードの PKI 機能を活用し、視聴権に基づくコンテンツ配信サービスの仕組みを検討すると共に、実験用システムを用いた実効性検証を実施した。

コンテンツデータや視聴権の格納にはメモリカードを用い、メモリカードと UIM カードの連携によってコンテンツや視聴権を管理する。検討の対象とするサービスの概要を図 3-26 に示す。

なお、本検証では、コンテンツの再生にかかわる権利情報について、その機能、形態、流通管理の方法等がマルチメディア情報流通サービスで「利用権」とは異なることから、「視聴権」という名称で位置付ける。

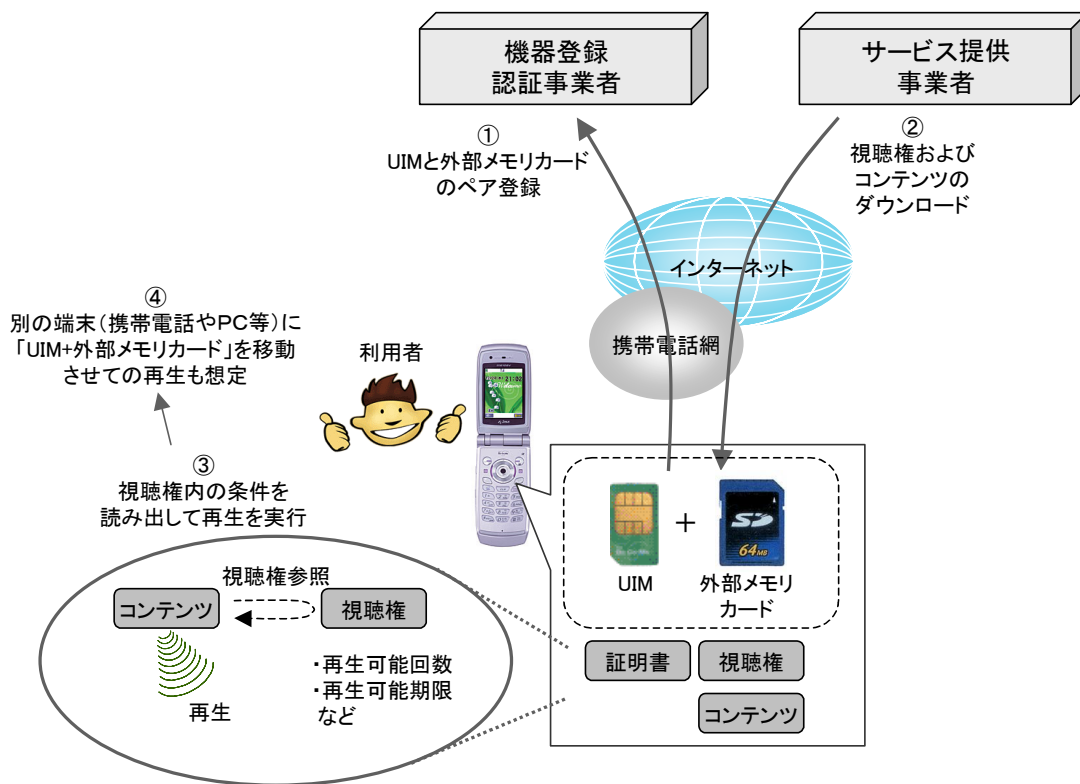


図3-26 本事業において検討するサービスの概要

(2) 実効性検証の環境

検証用システムを用いたモニタ検証は、本サービス提供システムに基づくコンテンツ配信サービスを実際に体験利用してもらうことにより、本サービス提供システムによって実現され得る携帯電話向けコンテンツ配信サービスに関する利用者の評価を測定するものとした。

モニタは、机上に設置したノートパソコンを利用して一連のサービスフローを実施した。実効性検証の環境について図3-27に示す。

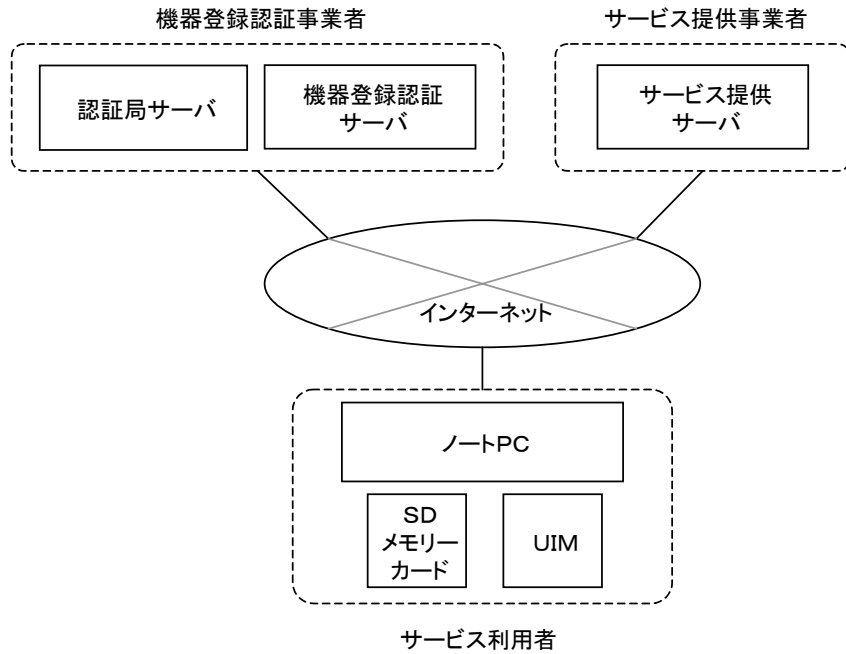


図 3-27 実効性検証環境の概要

(3) 検証結果

①利用者にとっての有効性

携帯電話端末による有料リッチコンテンツの利用に対して「興味がある」と回答した、全モニタ中 85%にあたる 39 人のモニタに対して魅力要因を質問したところ、図 3-28 に示される通り、半数以上のモニタが「場所やタイミングを問わず利用できる」点を挙げ、それが最大の魅力要因であることが確認された。

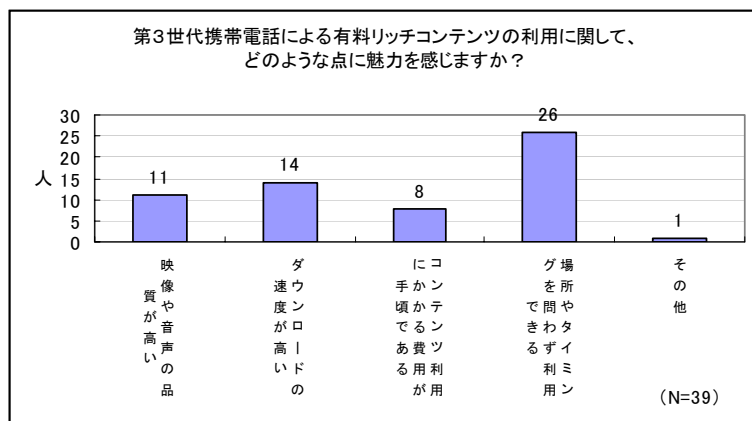


図 3-28 携帯電話による有料リッチコンテンツ利用の魅力要因

また、本サービス提供システムが想定している、「利用者自身が再生回数等の視聴条件を指定し、それに応じて対価が決まる仕組み」に対する評価を確認するため、具体的な利用イメージを提示して利用意向を確認したところ、図 3-29 に示される通り、87%が「利用してみたい」（「ぜひ利用してみたい」または「やや利用してみたい」）と回答した。

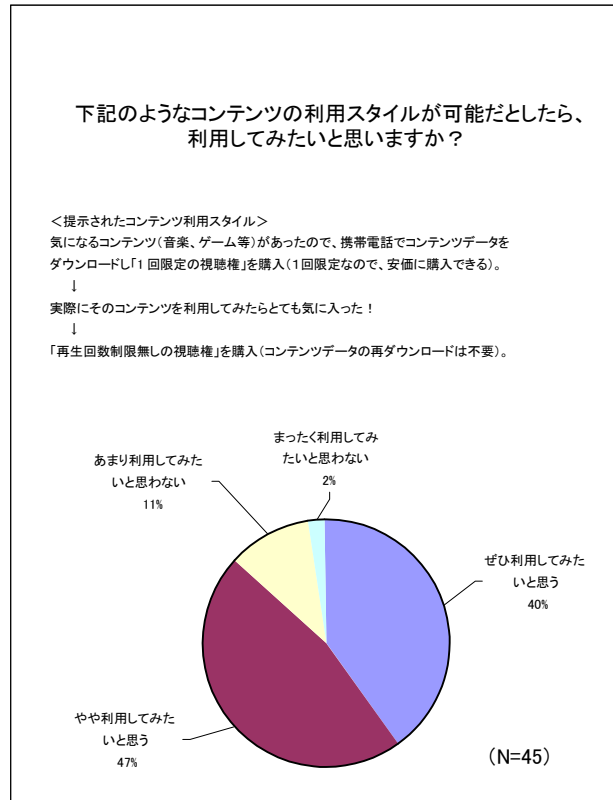


図3-29 視聴条件指定、それに連動した対価決定の仕組みへの評価

## ②携帯電話端末への実装可能性

現時点における携帯電話端末の仕様上の制約から、実装上の課題となると考えられる点は次の2点である。

- ・携帯電話端末上の JAVA アプリケーションによる、外部メモリへのデータのリードライト
- ・携帯電話端末上の複数 JAVA アプリケーション間の連携動作

UIM の PKI 認証機能と、携帯電話端末上の JAVA アプリケーションの機能を組み合わせることにより、「UIM+携帯電話端末」は多機能 IC チップの機能要件を一定程度満たすことが可能である。以下に、表3-6に示される多機能 IC チップの機能要件への対応について言及する。

表 3-6 多機能 IC チップの機能要件

	要件
①認証機能	<ul style="list-style-type: none"> <li>•自らの身元を検証できるデータを提供できること</li> <li>•相手を認証するための方法を提供すること</li> <li>•相手からのメッセージの内容が検証できること</li> <li>•自ら出力したデータであることを確認できる情報を付加できること</li> </ul>
②耐タンパ性	<ul style="list-style-type: none"> <li>•外部からの操作により保持内容が分かるような状態にならないこと</li> <li>•許可されていない方法による外部からの操作により保持データやアプリケーションは改竄されないこと</li> </ul>
③暗号機能	<ul style="list-style-type: none"> <li>•現状十分安全とされる暗号方式を採用すること</li> </ul>
④アプリケーション制御機能	<ul style="list-style-type: none"> <li>•複数のチップアプリケーションの搭載/更新/削除が可能であること</li> <li>•各チップアプリケーションはサービス単位で独立して動作すること</li> </ul>
⑤外部とのI/F機能	<ul style="list-style-type: none"> <li>•安全性で問題となる端子を設けないこと</li> <li>•入出力が可能であること</li> <li>•通信データが盗用されても実用上解読できないこと</li> </ul>

①については、UIM の PKI 認証機能を活用した、JAVA アプリケーションとサーバ間の SSL 相互認証機能により実現されることが考えられる。

②については、携帯電話端末内の JAVA アプリケーションのコピーやデータ取り出しが困難な仕様になっていることから、一定のデータ安全性は担保されることが考えられる。

③については、携帯電話の無線通信路のデータ解析が不可能であること、および SSL 暗号化機能により、十分な暗号強度を保つものであると考える。

④については、携帯電話のメモリ領域への複数の JAVA アプリケーションの搭載、更新、削除が可能である。また各アプリケーションは基本的に独立しており、メモリの共有も行われていない。

⑤については、ローカル入出力 I/F より JAVA アプリケーションやコンテンツの読み出しは仕様上不可能である。また、通信データは前述のように無線通信路のデータ解析が不可能であることと SSL 暗号化機能により、盗聴されても解読できない。

### ③安全性

本サービス提供システムにおける相互認証の実現状況に基づき、相互認証の強化策を検討すべきポイントを整理すると表 3-7 の通りとなる。

表 3-7 相互認証に関して強化策を検討すべきポイント

処理ステップ	本サービス提供システムにおける実現状況	強化策を検討すべきポイント
サービス利用登録	機器は、サービス提供事業者の公開鍵証明書を検証する（信頼点：サービス提供事業者に公開鍵証明書を発行した CA）。	（ア）信頼点は、アプリケーション登録認定機関であるべき。
アプリケーションロード	機器は、サービス提供事業者の公開鍵証明書を検証する（信頼点：サービス提供事業者に公開鍵証明書を発行した CA）。ダウンロードするアプリケーションに関しては、特段の検証処理は行わない。	（ア）信頼点は、アプリケーション登録認定機関であるべき。 （イ）機器は、ロードされるアプリケーションに関して、アプリケーション登録認定機関が発行したアプリケーション証明書および CR が発行したアプリケーションロード許可証を確認すべき。

### 3. 6 まとめ

#### 3. 6. 1 成果

テーマ種別 2 では、基盤技術の整備、サービスにおける実効性検証、多様なデバイスへの多機能 IC チップの適用、という 3 種の観点から各種の研究開発や実効性検証を行った。

##### (1) 基盤技術の整備

多機能 IC チップフレームワークの検討では、機器登録に関する基本的要件を整理した。この中で、機器登録のタイミングでの鍵生成・保存の方法や、機器の購入や保有の形態による機器登録の方法の違いについて検討を行った。

また、権利流通管理システムモデルの検討では、サービスを利用するための権利情報を利用者が保持する複数の多機能 IC チップの間や、複数の利用者が保持する多機能 IC チップの間で流通させる仕組みについて整理した。具体的には、サービスの手続き全体における権利流通管理の位置付けや、権利情報の流通を媒介する権利流通管理者の位置付け及び機能を中心に検討を行った。

##### (2) サービスにおける実効性検証

マルチメディア情報流通サービスの実効性検証では、多機能 IC チップの利用によって、コンテンツに関する権利者の権利を守りながら、利用者の私的利用の範囲での自由な利用を確保する仕組みについて、PC と IC カードの環境で実効性検証を行うと共に、権利関係、契約関係等のサービスの実現を裏付ける条件について整理した。その結果、コンテンツの流通に関する諸権利とマルチメディア情報流通サービスのプレーヤ間の役割分担及び契約関係の対応を明らかにしてコンテンツ流通ビジネスにおける位置付けを整理するとともに、開発したシステムが権利情報の流通を管理する仕組みとして十分な機能をもつことを検証した。利用者、権利者、及び事業者へのアンケートの結果か

ら、回数や期間の限定などコンテンツの再生条件を設定することにより多様なサービスが提供でき、かつ複数の機器での再生を実現する仕組みとして提供されるコンテンツ流通の仕組みとして、マルチメディア情報流通サービスが期待されていることが明らかになった。また、PDAに多機能ICチップを実装するための基本的な構造について整理した。

会員権サービスでは、会員権に基づいてさまざまなサービスを追加可能な仕組みについて、利用者からの期待が寄せられると共に、事業者にとっての個人情報管理に関する業務を削減する可能性もあることが明らかになった。実用面では、ICカードへのアプリケーションのダウンロードにおける機能や性能について、利用者の多くから許容範囲との回答を得ることができ、利用者の多機能ICチップに新規に利用するサービスをダウンロードしながら提供するサービスの提供方法に展望が持てた。また、超小型セキュアICチップとの連動によるサービスの広がりについて考察を行った。

### (3) 多様なデバイスへの多機能ICチップの適用

携帯電話に多機能ICチップを搭載した場合の非接触インタフェースを試作し、実運用上有効と言える性能を発揮できること、及びこの機能の活用により、携帯電話通信網を通じて多機能ICチップに利用権等のデータを記録して、イベント会場等で非接触インタフェースを通じてサービスを利用するような用途の実用性が明らかになった。また、多機能ICチップを携帯電話に導入した場合のコンテンツ配信サービスについてPC環境を利用した実効性検証を行い、携帯電話を利用して各種コンテンツの配信を受けるサービスについて利用者から大きな期待があることが明らかになった。

テーマ種別2による研究開発全体を通じて、多機能ICチップを活用したサービスが、利用者及びサービス提供者の双方にとって潜在的な魅力のある技術であることが明らかになったと言える。

## 3. 6. 2 展望と課題

テーマ種別2の研究結果に基づき、多機能ICチップを活用したサービスの実現や普及に向けた展望と、明らかになった課題について以下に整理する。

### (1) 基盤技術の整備

多機能ICチップフレームワークの研究では、機器の登録以降のライフサイクルをICカードにおけるフレームワークと同様のものとして整理している。しかしながら、多機能ICチップを搭載した機器のライフサイクルは、カードのライフサイクルとは異なるものとして整理される可能性がある。多機能ICチップを搭載した機器の開発、普及に向けては、機器のライフサイクルにおける多機能ICチップの管理要件について整理し、多機能ICチップのライフサイクルについて機能、セキュリティに関する要件を必要に応じて追加する必要がある。

多機能ICチップを活用したサービスの利用権の取り扱いには、権利情報を多機能チ



ップに流通させる方法だけでなく、権利情報自体はサービス提供者側に保持してそのアクセス権を付与する方法もあり、この2つの方法で提供できるサービスに差が出る可能性があることが明らかとなった。具体的には、権利情報をサービス提供者側に保持することによって、多機能 IC チップの破損や紛失の際には再発行ができるサービスを提供できる可能性があることが挙げられる。また、個人情報とサービスの利用履歴が結びつくことによってより高度な個人情報が形成されることから、匿名でサービスを利用する方法について検討する必要があることが明らかになっている。

## (2) サービスにおける実効性検証

マルチメディア情報流通サービスでは、利用者からの否定的な回答として「サービスを利用できる機器がまだ普及していない」「操作が難しい」などの回答が寄せられており、サービスの実用に向けて、利用手順及び操作手順の簡略化と、サービスを実現する多機能 IC チップ搭載機器の実現及び普及が課題として顕在化している。なお、多機能 IC チップ搭載機器の開発と普及については、PDA への多機能 IC チップの実装に関する検討を通じて、多機能 IC チップの特徴を生かすためのセキュリティの確保が、デバイスの製造における課題として挙がっており、今後に向けた課題として明らかになっている。

会員権サービスでは、アプリケーションのダウンロード時間が大きな障害にはならないことが明らかになり、今後のサービスの普及に向けて明るい見通しを得た一方で、家庭でアプリケーションをダウンロードする環境を整備する際には、家庭の PC 環境の違いを背景にしたトラブルが発生する可能性があること、イベントの運営において多機能 IC チップを利用しない参加者と双方が混在する場合の、案内やサービス提供といった運営面でのリスクや、運営体制を整備するためのコストも明らかになってきている。多機能 IC チップを保持する利用者と保持しない利用者が混在する環境での円滑なサービス運用には、課題が残ったと言える。

## (3) 多様なデバイスへの多機能 IC チップの適用

携帯電話の電話網による通信と非接触インタフェースによる通信を組み合わせることで多機能 IC チップで利用することにより、セキュアで利便性の高いサービスを提供できる可能性が高いことが明らかになった。また、コンテンツ配信サービスにおいては、画面の小ささにもかかわらず、利用者が携帯電話でのサービスを望んでいることも明らかになった。

一方で、携帯電話でコンテンツを取り扱う際には、実装上の各種の制約もあるため、利用者の利便性を損なわない範囲でどのようなサービスを提供できるかが課題と言える。

## 第Ⅱ編 研究開発・実証事業の実施報告

### 4. テーマ種別3

---

## 4. テーマ種別 3

### 4. 1 事業概要

#### 4. 1. 1 背景

近年のサービス多様化に伴い、個人の属性情報や環境情報、端末情報のようなプロフィールデータをネットワーク上で利用する機会が増加しており、安全な情報の受け渡しが求められている。多機能 IC チップフレームワークでは、情報の受け渡しを行う各プレーヤの役割概要と、責任分界の概要を定義し、プレーヤ間の通信に PKI を利用する。多機能 IC チップ内のデータセキュリティだけでなく、多機能 IC チップへ受配信されるデータの安全性も確保されるため実ビジネスに向けた応用への関心が高い。

#### 4. 1. 2 目的

本事業のテーマ種別 3 における研究（以下「本研究」という。）においては、多機能 IC チップフレームワークに基づくサービス提供環境を実現し、プロフィールポータビリティサービスの実証実験を行った。プロフィールポータビリティサービスとは、属性情報、環境情報、端末情報等のプロフィールデータを登録管理、移動、利用することによって提供が可能となるサービスのことである。実証実験を通して、プロフィールデータの取り扱いや利用、システム導入について、技術面、業務面における様々な課題を明らかにし、新領域 IT サービスであるプロフィールポータビリティサービスの有効性の検証を行うことを目的として実施した。

#### 4. 1. 3 事業概要

本研究では、全体的な計画立案の後、システム開発や実証環境の整備を行い、実証実験に臨んだ。

本研究におけるプロフィールポータビリティサービスは、コンサートをサービスフィールドとして想定したライブ・エンタテインメント分野において適用するものとし、実際のコンサート会場にて実証実験を行った。

本研究では、実証実験を行うにあたり、以下に示す各項目について検討を行った。

①プロフィールデータの管理・利用についてのモデルと機能

②実証実験にて行うサービスの具体化

### 4. 2 プロファイルポータビリティに関する研究

#### 4. 2. 1 プロファイルポータビリティサービスの定義と特徴

本研究におけるプロフィールポータビリティサービスとは、属性情報、環境情報、端末情報等のプロフィールデータを登録管理、移動、利用することによって提供が可能となるサービスのことである。

利用者は各自の端末にプロフィールデータを格納し、このデータを利用することで様々なサービスを受けることができる。また、サービス提供者は各サービスにおいて利用、生成されたプロフィールデータを横断的に利用することにより、利用者の要求に応じて連鎖

的にサービスを提供すること（以下、「サービス連鎖」という。）ができる。サービス連鎖のモデルを図4-1に示す。サービス提供者が所有するプロフィールデータを共有し、サービス提供者間で利用できるような機能を実現するため、プレーヤとして第三者的な機関を設置した。

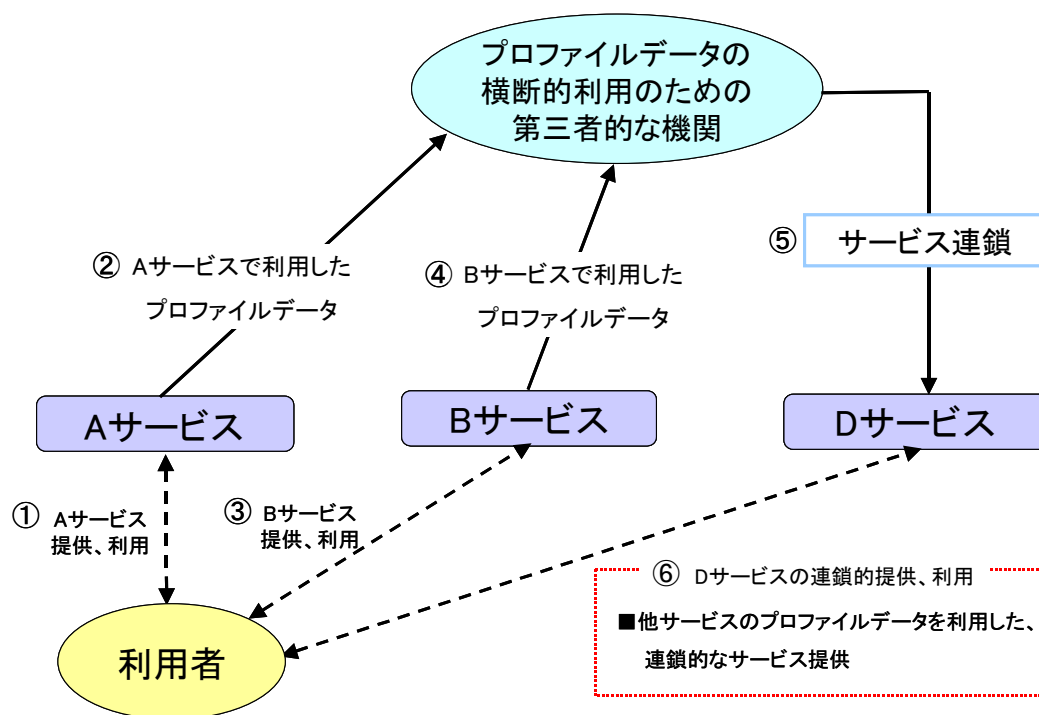


図4-1 プロファイルポータビリティサービスのサービス連鎖イメージ

サービス連鎖の手順を以下に例示する。

- ① 利用者がAサービスを利用する。
- ② 第三者的な機関がAサービスで利用したプロフィールデータを収集・管理する。
- ③ 利用者がBサービスを利用する。
- ④ 第三者的な機関がBサービスで利用したプロフィールデータを収集・管理する。
- ⑤ Bサービスと提携しているDサービスが、AサービスとBサービスでのプロフィールデータを活用する。
- ⑥ 利用者はサービス連鎖によってDサービスを受ける。

#### 4. 2. 2 プロファイルデータの分類と管理・流通方式の検討

##### (1) プロファイルデータの分類

プロフィールデータの管理や流通の方式を検討するために、管理上の安全性の面から、プロフィールデータを以下の3つの情報に分類した。

##### ①個人基本情報

名前や住所、eメールアドレスなど当該情報によって個人が特定可能であったり、個人に直接連絡をとることが可能となったりする情報。ライブ・エンタテインメント分野では、利用者への課金等を行うためや、個人へ直接連絡をとるために利用される。

## ②センシティブ情報

勤務先企業名や行動履歴など当該情報のみで個人の特特定が不可能であり、客観的な表現が可能となるような、個人にとって外部的な情報。ライブ・エンタテインメント分野では、電子チケットデータ、サービス利用履歴等の情報がこれにあてはまる。

## ③プライバシー情報

性格や感情など当該情報のみで個人の特特定が不可能であり、個人にとって内面的な情報。程度概念的情報であり、センシティブ情報と比較して個人にとって内部的な情報である。ライブ・エンタテインメント分野では、好きな音楽や映画等の趣味嗜好情報がこれにあてはまる。

### (2) ネットワーク上を流通させるプロフィールデータについて

本研究では、サービス提供者が個人を特定するためにシリアル No.を用いた。そして、シリアル No.以外の個人基本情報がネットワーク上を流通しない仕組みを採用した。

表 4-1 に、ネットワーク上を流通させるプロフィールデータを示す。

表 4-1 ネットワーク上を流通させるプロフィールデータ

プロフィールデータの種類	具体的なプロフィールデータ
個人基本情報	サービス利用者に紐づくシリアル No.
センシティブ情報	サービス利用履歴、サービスに付随する情報等
プライバシー情報	趣味嗜好情報等

なお、事業者やサービス間にてプロフィールデータを横断的に利用するためには、利用者から事前に同意を得る必要がある。また、シリアル No.については取り扱い方針の策定等、適切なセキュリティ対策が必要である。

### (3) プロフィールデータの管理方式

図 4-1 のようなプロフィールデータの連携によるサービス連鎖を実現するためには以下の 3 種類のデータ管理機関が必要である。

- ・個人情報やシリアル No.を一元管理する機関
- ・プロフィールデータの横断的利用のための第三者的な機関
- ・サービスを提供する既存の機関

各データ管理機関の管理する情報、役割、責任範囲について、表 4-2 に示す。

表 4-2 データ管理機関の役割、責任分界

機関	管理する情報	役割	責任範囲
データ管理機関 A	個人情報（基本 4 情報 + α） シリアル No. シリアル No.の失効情報 等	サービス利用申請受付 等	サービス利用者に関する情報管理（個人がどのサービスを利用しているかは分からない）
データ管理機関 B	シリアル No. センシティブ情報（サービス利用履歴等） プライバシー情報（趣味・嗜好情報等） 等	サービスの提供 サービス利用者に対する情報発信 等	サービス利用に関する情報管理（シリアル No.が誰であるかは分からない）
データ管理機関 C	シリアル No. センシティブ情報（サービス利用履歴等） プライバシー情報（趣味・嗜好情報等） 等	サービス連鎖情報の管理、発信 等	サービス利用に関するサービス連鎖情報管理（シリアル No.が誰であるかは分からない）

#### 4. 2. 3 プロファイルポータビリティサービスモデル

表 4-2 で検討したデータ管理機関の「管理する情報と役割・責任範囲」に照らし、多機能 IC チップフレームワークの仕組みに基づいたデータ管理機関としてのプレーヤを抽出した。各データ管理機関とプレーヤの対応を表 4-3 に、プレーヤ図を図 4-2 に示す。

表 4-3 各データ管理機関とプレーヤの対応

データ管理機関 A	多機能 IC チップサービス管理センタ	個人基本情報やシリアル No.を一元管理する機関
データ管理機関 B	サービス提供者	サービス提供者
データ管理機関 C	プロファイルデータ収集管理機関 サービス連鎖管理機関	プロファイルデータの横断的利用のための第三者的な機関

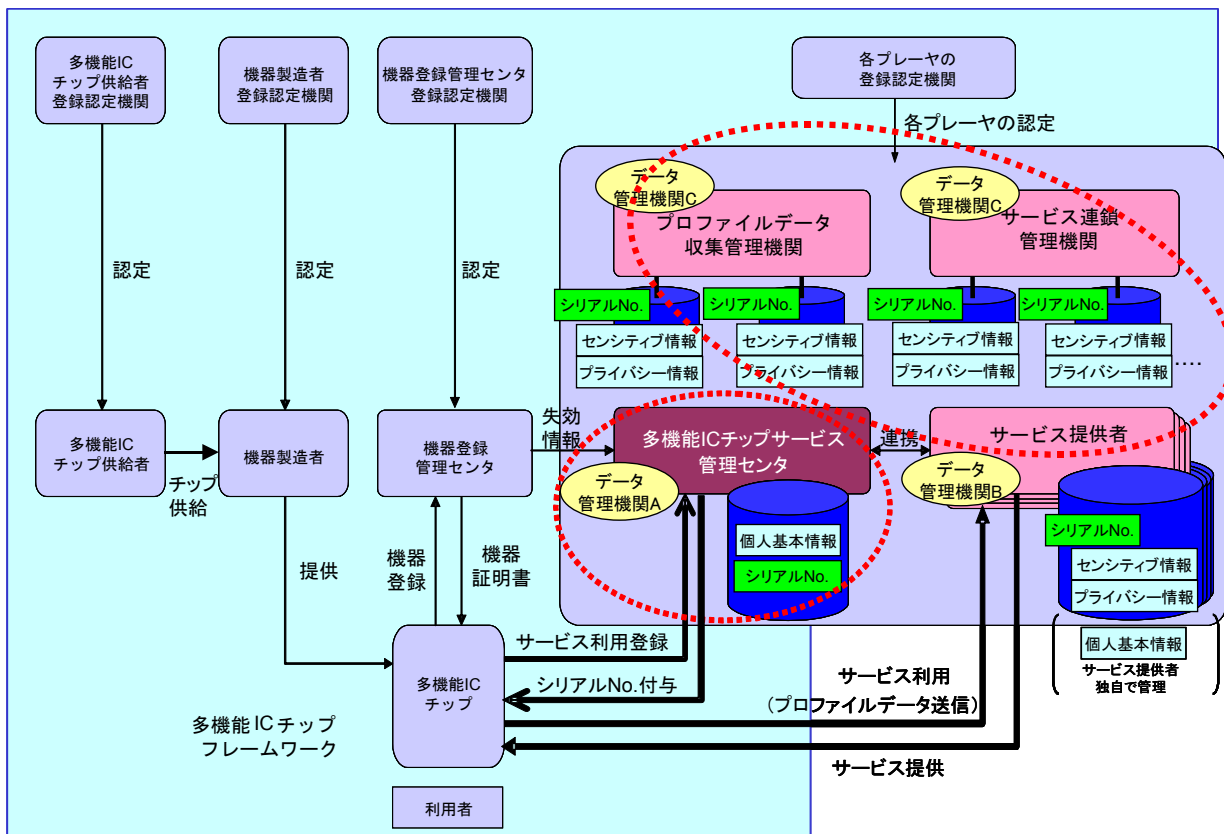


図4-2 プロファイルポータビリティサービスにおけるプレーヤ図

図4-2に示したようなプレーヤ図では、多機能ICチップサービス管理センターで個人基本情報やシリアル No.を一元管理し、個人基本情報をネットワーク上に流通させない。そして、サービス提供者、プロフィールデータ収集管理機関、サービス連鎖管理機関の間では、シリアル No.とセンシティブ情報、プライバシー情報が流通し、ネットワーク上を流通するデータだけでは個人特定が困難な構造になっている。

また、サービス提供者からのサービス連携・プロフィールデータ送信等の依頼を受付けるようなサービス提供者との窓口としての役割と、プロフィールデータの収集管理を行うような役割とを分離して区別するために、データ管理機関Cをプロフィールデータ収集管理機関とサービス連鎖管理機関の2つに分離した。

各プレーヤの役割を表4-4に示す。

表 4-4 各プレイヤーの役割

プレイヤー名	役割
多機能 IC チップサービス管理センタ	<ul style="list-style-type: none"> <li>個人基本情報の登録管理を行う。</li> <li>利用者に対してシリアル No.を払い出す。</li> </ul>
プロフィールデータ収集管理機関	<ul style="list-style-type: none"> <li>利用者のプロフィールデータをサービス提供者毎に管理する。</li> </ul>
サービス連鎖管理機関	<ul style="list-style-type: none"> <li>サービス提供者間のサービス連携の要求に応じて、プロフィールデータ収集管理機関からプロフィールデータを取得する。</li> </ul>
サービス提供者	<ul style="list-style-type: none"> <li>利用者にサービスを提供する。</li> <li>プロフィールデータ収集管理機関に対して流通を許すプロフィールデータを送る。</li> <li>サービス連鎖管理機関に対してプロフィールデータの取得依頼を行う。</li> </ul>

#### 4. 2. 4 プロファイルポータビリティサービスの具体化

実証実験において想定する事業者、サービス連鎖による機能を図 4-3 に示す。

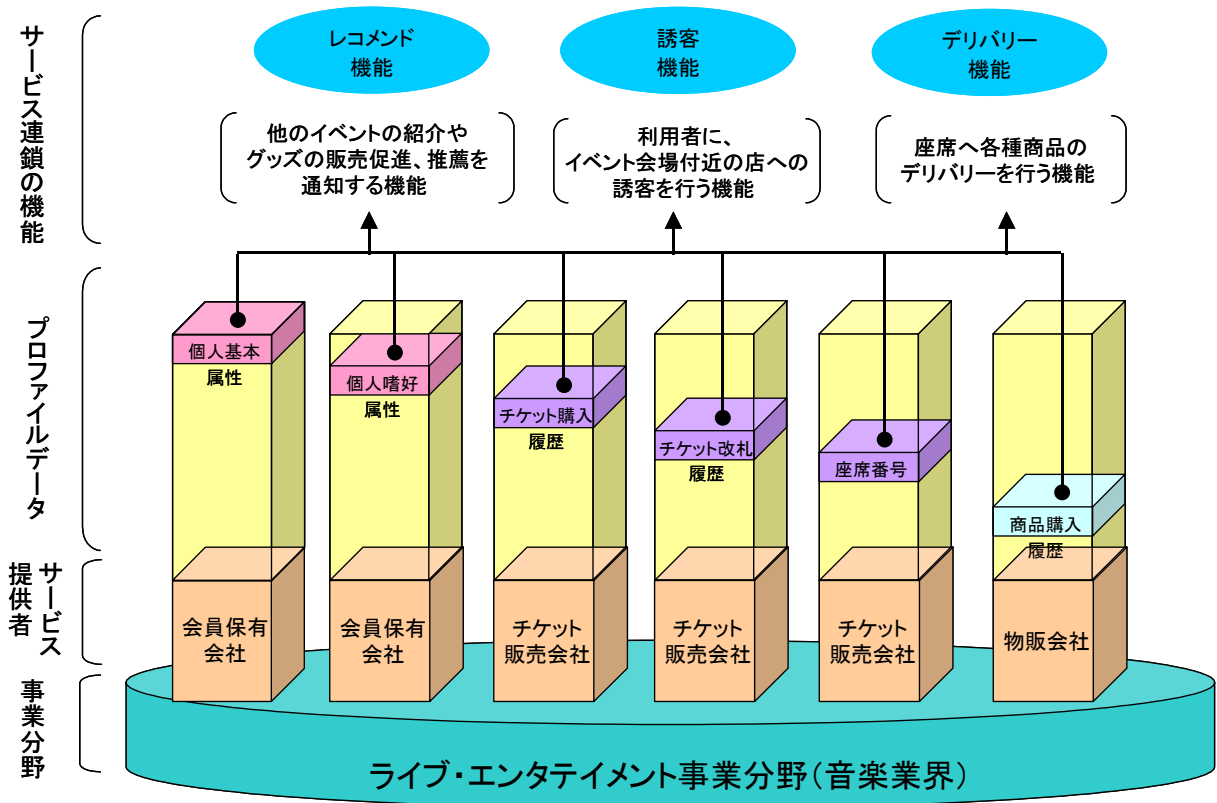


図 4-3 ライブ・エンタテインメント分野でのサービス機能



本実証実験では、表 4-5 に示す誘客機能とデリバリー機能に対応するサービスを行った。

表 4-5 プロファイルデータの横断的利用を行うサービス

実施サービス名	機能	想定される事業者	サービス概要
お楽しみコンテンツサービス	誘客機能	物販会社	行動履歴に基づき、コンテンツを提供する。
デリバリーサービス	デリバリー機能	物販会社	座席情報と行動履歴に基づき、物品のデリバリーを行う。

また、横断的利用を行うプロフィールデータを得るためのサービスを、表 4-6 に示す。

表 4-6 プロファイルデータを収集するサービス

実施サービス名	想定される事業者	サービス概要
電子チケットサービス	チケット販売会社	電子チケットによる改札、座席位置表示を行う。
共鳴サービス	会員保有会社	嗜好情報に応じたコンテンツを提供する。
物販・決済サービス	物販会社	商品を販売する。

サービス連鎖を行う上で横断的利用を行うプロフィールデータや、各サービスの位置づけ、新領域 IT サービスとして期待される部分について図 4-4 に示す。

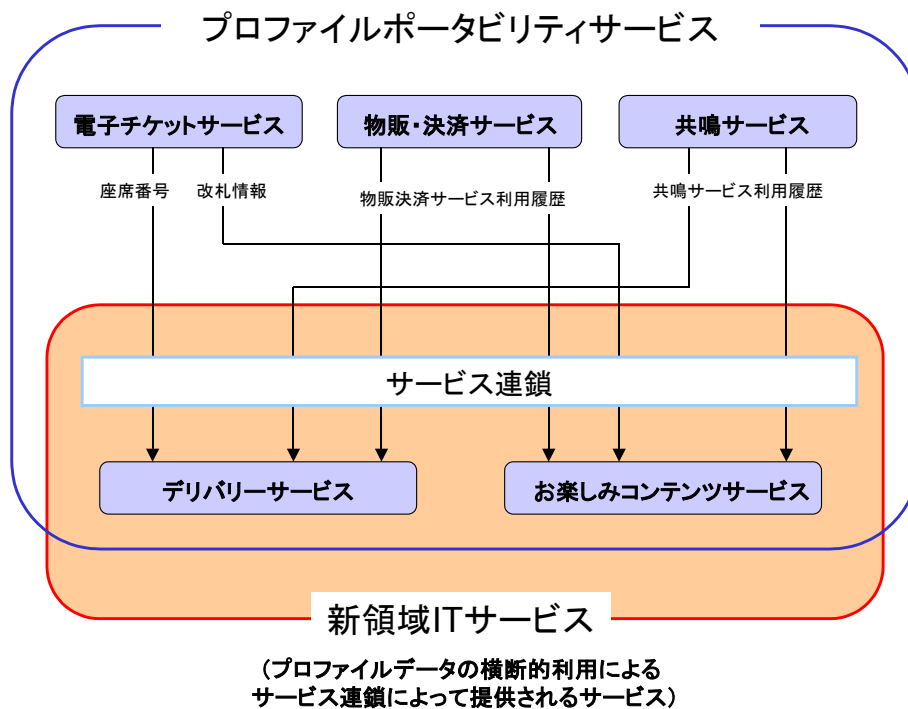


図 4-4 プロフィールポータビリティサービスと新領域 IT サービスの位置づけ

#### 4. 3 実証実験

##### 4. 3. 1 実証実験におけるサービス内容

「4. 2. 4」の具体化をふまえ実施したサービスの内を表4-7に示す。

表4-7 サービスの一覧

サービス名	サービス内容	
電子チケットサービス (※)	電子チケットのダウンロード	インターネットを介して、電子チケットを多機能 IC チップ内に格納する。
	電子チケットの内容表示	ダウンロード済みチケットの内容を表示する。
	改札	改札端末を用いた改札を行う。
	座席位置表示	座席位置の表示を行う。
物販・決済サービス	クレジット決済	多機能 IC チップに格納されているクレジット情報を用いて、インターネット上でのネット決済、会場内の店舗での決済を行う。
共鳴サービス	個人向け情報提供	多機能 IC チップに格納されている個人の趣味嗜好情報を送信し、個人向けの情報を大型表示装置(以下、「PDP」という)に表示させる。 PDA 側にも静止画像を送信し、PDA 上でも閲覧可能にする。
デリバリーサービス	物品の客席へのデリバリー	プロファイルデータを横断利用して物品のデリバリーを行い、受取証の授受を行う。
お楽しみコンテンツサービス	コンテンツの配信	プロファイルデータを横断利用して、利用者端末へコンテンツの配信を行う。

(※) 電子チケットは、商用で利用されているシステムを利用

各サービスは図4-5に示す実証実験環境にて提供が行われた。

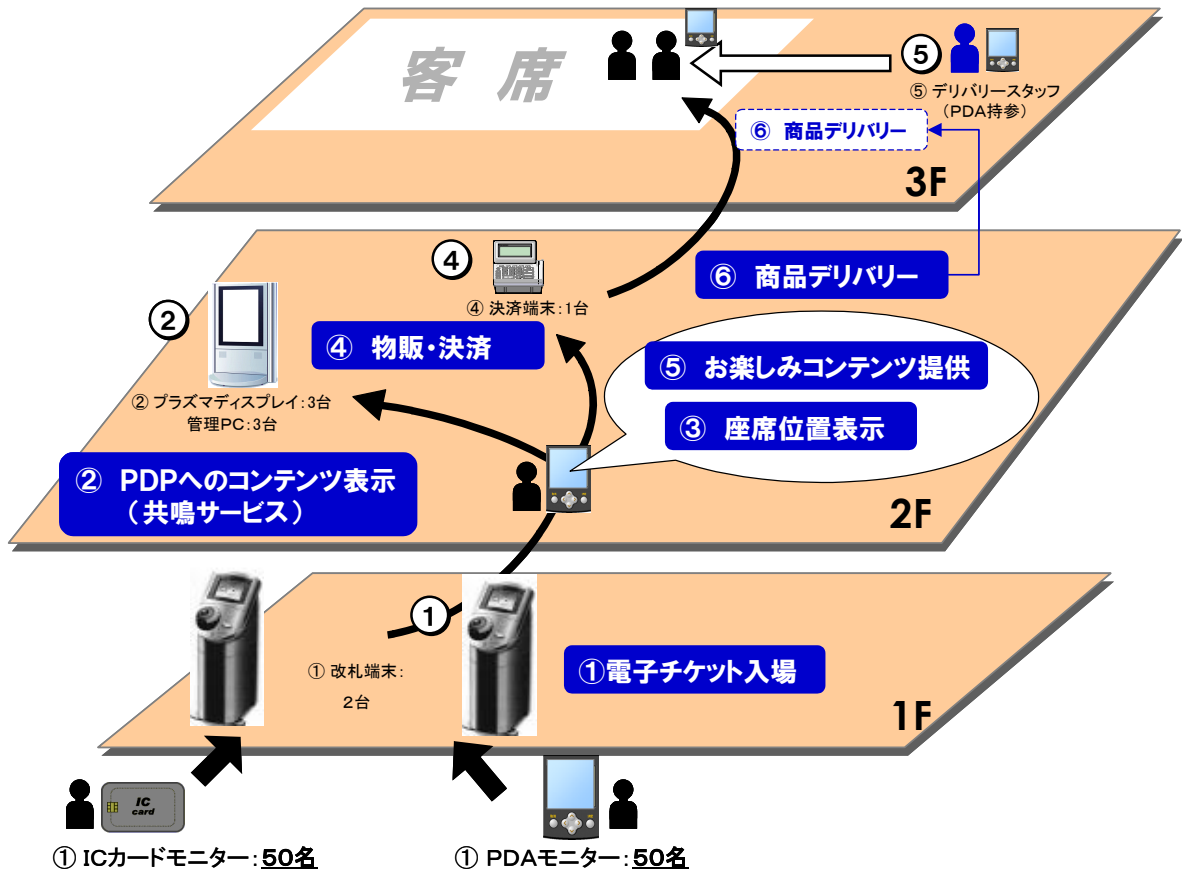


図4-5 実証実験環境の概要図

<各サービスの利用の流れ>

コンサート実施前（自宅等）
利用者はまず、多機能 IC チップ内に電子チケットのダウンロードを行う。任意であるが、実証実験以前にネット物販サービスにてグッズ購入も可能である。
コンサート当日（コンサート実施会場）
①電子チケットサービス 多機能 IC チップ内に格納されている電子チケットを用いて改札を行う。
②共鳴サービス 2階に移動した後、大型表示装置であるプラズマディスプレイ（以下「PDP」という。）での情報表示を行う。
③座席位置表示サービス PDA の画面上に会場内の地図を表示し、座席位置を確認する。
④物販・決済サービス イベント関連グッズの販売を行い、購入の際は、PDA に搭載されている多機能 IC チップ内に格納されたクレジット情報を用いて、決済を行った。ネット物販サービスと同様に物販・決済サービスの利用は実際に課金が行われることから任意で行うこととした。
⑤お楽しみコンテンツサービス 電子チケットの改札サービス、共鳴サービス、物販・決済サービスを利用することで、お楽しみコンテンツサービスの利用が可能となる。
⑥デリバリーサービス また、電子チケットの改札サービス、共鳴サービス、ネット物販サービスを利用することでネット物販した商品や、共鳴サービスの利用者に送られる個人の嗜好に合わせた記念品の、デリバリーサービスを受けることができる。 デリバリーサービスにおいてはスタッフ用の PDA も用いて、配送先の座席情報の表示や、利用者との受取証の受け渡しを行った。

また、各サービスで用いるプロファイルデータと、サービス連鎖によって横断的に利用されるプロファイルデータの内容について、デリバリーサービスの場合を図 4-6 に、お楽しみコンテンツサービスの場合を図 4-7 に示す。

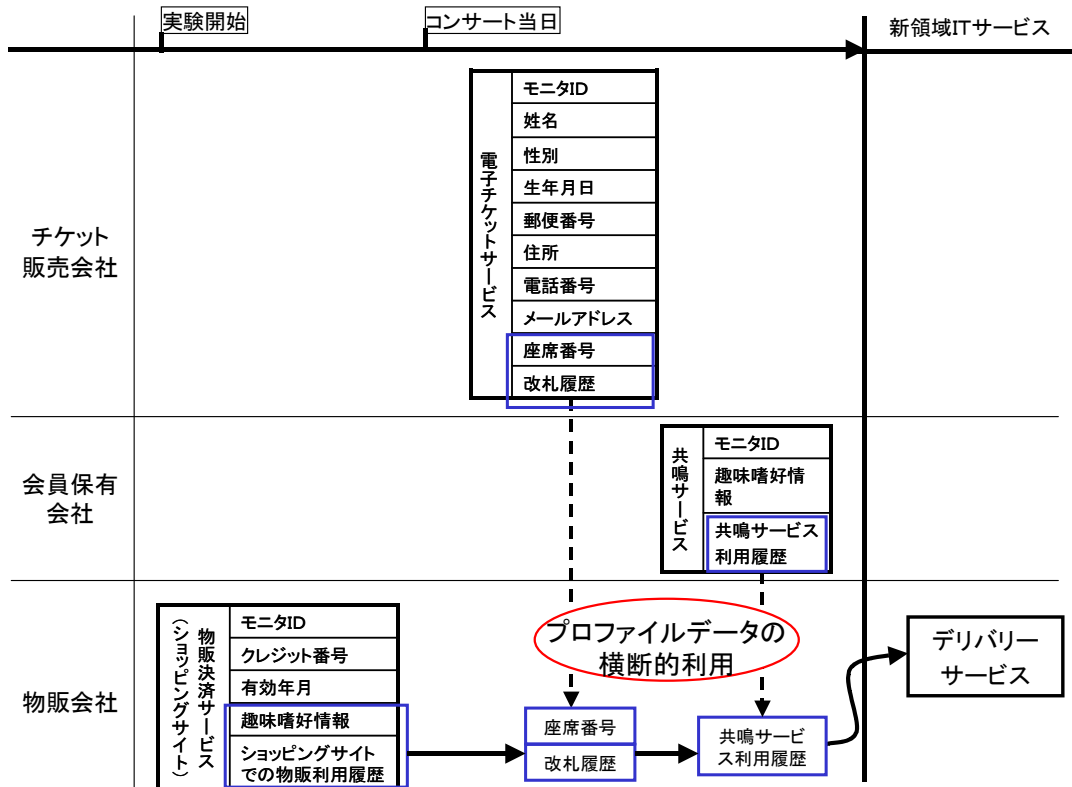


図 4-6 デリバリーサービスにおけるプロフィールデータの横断的利用

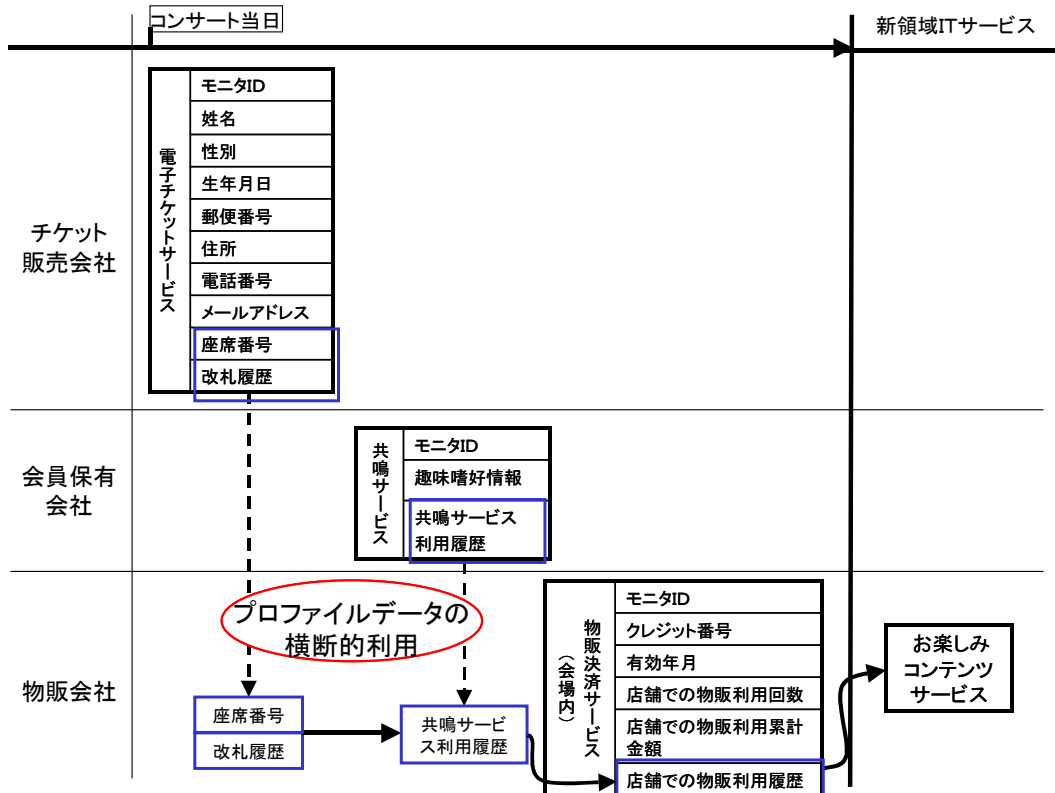


図 4-7 お楽しみコンテンツサービスにおけるプロフィールデータの横断的利用

#### 4. 3. 2 実証実験におけるシステム構成

今回の実証実験において構築した実験システムの構成図を図4-8に示す。

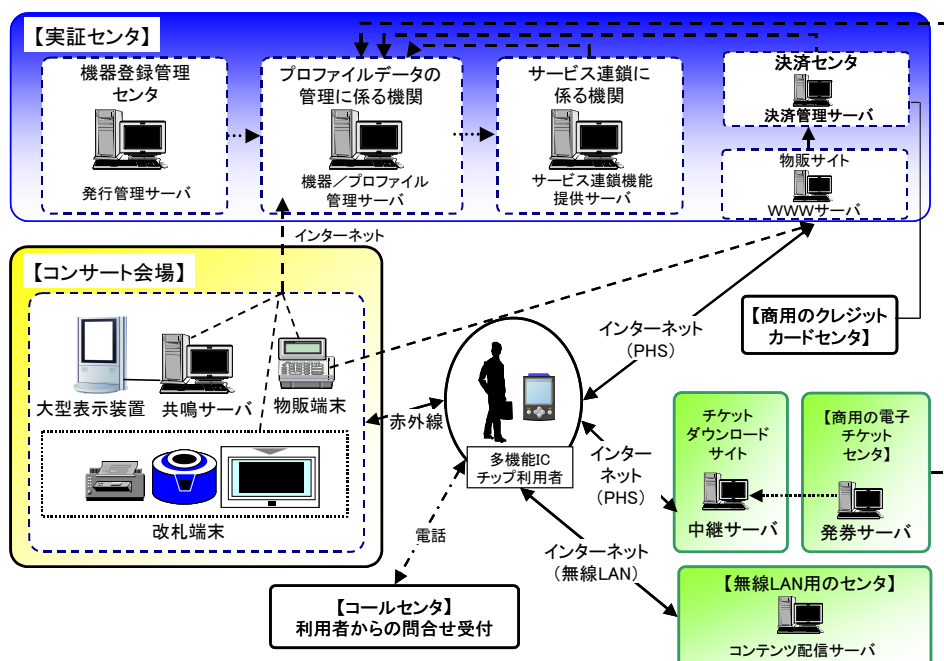


図4-8 実験システムの構成図

各サーバや端末の機能は表4-8の通りである。

表4-8 設置ハードウェアの機能一覧

設置ハードウェア	機能説明
発行管理サーバ	多機能 IC チップの発行管理を行う機能
機器/プロフィール管理サーバ	機器情報やサービス等のプロフィールデータを収集する機能
サービス連鎖機能提供サーバ	機器/プロフィール管理サーバと連携し、デリバリーサービスに必要な情報を取得する機能
決済管理サーバ	クレジット情報をもとに、クレジット会社へ決済処理を行う機能
WWW サーバ	実証実験サービスを行うための機能
大型表示装置	共鳴サービスでの動画コンテンツを表示する機能
共鳴サーバ	利用者の嗜好情報を元に利用者に応じた動画コンテンツを再生し、利用者の PDA に画像コンテンツを送信する機能
物販端末	決済管理サーバへクレジット情報の送信を行う機能
改札端末セット	電子チケットの改札に必要な機能
座席位置経路案内端末	電子チケットの座席情報から座席位置を表示する機能
発券サーバ	電子チケットを発券する機能
中継サーバ	電子チケットをダウンロードするためのサーバ機能
コンテンツ配信サーバ	コンテンツを配信する機能

4. 2. 3にて検討を行ったプレーヤとの関係は表4-9の通りである。

表4-9 各プレーヤの実証実験システムにおける実現機能

プレーヤ	実証システムにおける該当機器、対象
登録認定機関	登録認定機関は未設置
多機能 IC チップ供給者	製造業者
機器製造者	製造業者
機器登録管理センタ	発行管理サーバ
多機能 IC チップサービス管理センタ	機器/プロフィール管理サーバ
プロフィールデータ収集管理機関	サービス連鎖機能提供サーバ
サービス連鎖管理機関	
サービス提供者	各種サービス提供サーバ、端末
機器	PDA (コンテンツの閲覧や操作において、画面表示を必要とするため)

#### 4. 3. 3 モニタの選定と検証グループの設定

モニタの選定にあたって、以下に示す通り、一般モニタと関係者モニタを募集した。

##### ①一般モニタ

本事業に参加している企業で、事業内容・実験趣旨に賛同するモニタを 60 名募集した。この 60 名の一般モニタのうち、30 名をテーマ種別 3 のモニタ、残りの 30 名をテーマ種別 2 のモニタとした。

##### ②関係者モニタ

テーマ種別 3 とテーマ種別 2 の実験趣旨の違いを理解している本事業の関係者を対象に、モニタ 40 名を選定した。このモニタは IC カードと多機能 IC チップの比較を行うために、2 回の実証実験通じてテーマ種別 2 とテーマ種別 3 の両方の実験に参加した。

図 4-9 に、一般モニタと関係者モニタの構成と 2 回の実験への対応関係を示した。

### モニター構成

- ◆ 一般モニター 60名 (テーマ種別3:PDA30名、テーマ種別2:ICカード30名)
- ◆ 関係者モニター 40名 (テーマ種別3:PDA20名、テーマ種別2:ICカード20名)

※ICカード、PDAの各実証実験における関係者モニターについては、実験評価者数を増やすこと及び各テーマを比較検証することを目的に、実証実験の1回目と2回目に対象者の入替えを行う。

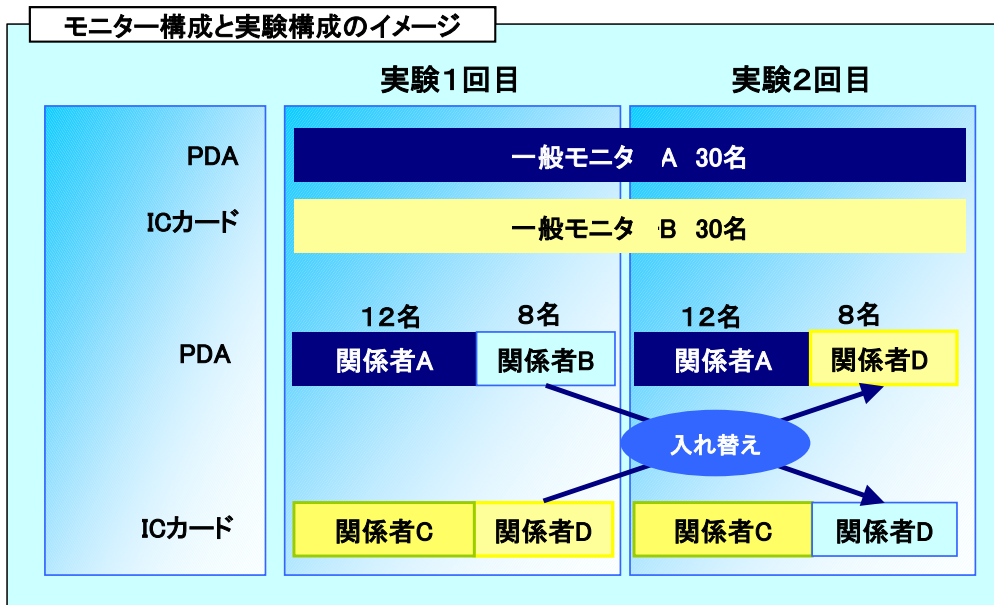


図4-9 モニターの構成

#### 4. 3. 4 実験の実施日時と概要

##### (1) モニタ説明会

会場： パナソニックセンター

日時： 1月30日 (金) 17:00~19:00 あるいは

1月31日 (土) 13:30~15:30 に参加

モニタ説明会では実証実験ガイドを配布し、実証実験の主旨、各サービスの利用方法を説明した後、グループ単位でツアー形式により、各サービスのデモを行った。また、1回目の実証実験に参加するモニターにはPDAの配布を行い、借用書の受領を行った。説明会后、アンケートを行い、回収した。

##### (2) 第1回実証実験

第1回コンサート

会場： 都内の5000人収容のホール

日時： 2月15日 (日) 15:00 開場 16:00 開演



PDA モニタは開場前の 14 時 45 分にホール入り口に集合し、PDA の状態確認、動作確認の後、サービス利用の流れについての説明を受け、入場を行った。

4. 3. 1 に記載の通り、モニタがサービスの利用を行うことができるよう誘導を行った。

また、デリバリーサービスについては会場の座席の都合上、通路に面した座席のモニタを対象に実施した。

実証実験のアンケートはインターネット上での WEB アンケートとして集計、取りまとめた。

### (3) 第 2 回実証実験

#### 第 2 回コンサート

会場： 第 1 回と同じく、都内の 5000 人収容のホール

日時： 3 月 14 日（日） 16:00 開場 17:00 開演

PDA モニタは開場前の 15 時 45 分に集合し、PDA の状態確認、動作確認の後、サービス利用の流れについての説明を受け、入場した。

以下、第 1 回と同様の運用を行った。アンケートも同様に WEB アンケートにて集計を行った。また、実証実験終了後に事業者に対するヒアリングを行った。

## 4. 4 検証項目

本研究では、実証実験を通して、プロファイルポータビリティサービスの提供に係る技術面、業務面における様々な課題を明確にし、新領域 IT サービスとしてのプロファイルポータビリティサービスの有効性を検証することを目的とした。

新領域 IT サービスの検証にあたり、利用者から見た有効性と事業者から見た有効性の 2 通りの視点から行う。

### 4. 4. 1 利用者から見た新領域 IT サービスの有効性の検証

利用者から見た新領域 IT サービスの有効性の検証について、検証項目ならびに検証内容について表 4-10 に示す。

表 4-10 利用者における検証項目

検証テーマ	検証項目	検証観点	検証方法
利用者から見た新領域 IT サービスの有効性の検証	利用者の関心度	新領域 IT サービスに対して、利用者が求める観点	アンケート
	利便性	各サービスにおける点、利用者端末に求められる点、	アンケート
	安全性	プロファイルデータ提供の条件	アンケート

#### 4. 4. 2 事業者から見た新領域 IT サービスの有効性の検証

事業者から見た新領域 IT サービスの有効性を、机上検討ならびに実証実験参加事業者へのヒアリングをもとに検証した。検証項目、検証内容ならびに各項目における検証方法について表4-11に示す。

表4-11 事業者における検証項目

検証テーマ	検証項目	検証観点	検証方法
事業者から見た新領域 IT サービスの有効性の検証	利便性	システムアーキテクチャ (操作性、通信性能)	システムログ、アンケート
	事業性	プロファイルデータの横断的利用を行うことによる事業性	ヒアリング

#### 4. 5 検証結果

##### 4. 5. 1 本実証実験の評価について

本実証実験では、モニタへのアンケート調査、事業者へのヒアリング調査を行い評価、分析を行った。具体的な実施環境としては表4-12のとおりである。アンケートはモニタ説明会当日、第1回イベント後、第2回イベント後の計3回実施し、ヒアリングは第2回イベント後に、イベント主催者、チケット販売会社、クレジットカード会社に対して実施した。

表4-12 アンケートの実施環境

	名称	実施日	対象	設問数	手段
1	モニタ説明会当日アンケート	1/30,31	多機能ICチップを搭載したPDA提供モニタ 70名 ・1,2回イベントともPDA :30名 ・1回目イベントのみPDA:20名 ・2回目イベントのみPDA:20名	9	紙
2	第1回イベント後アンケート	2/16~	1回目コンサートでのPDA利用者:50名 ・1,2回イベントともPDA :30名 ・1回目イベントのみPDA:20名	33	WEB
3	第2回イベント後アンケート	3/15~	2回目コンサートでのPDA利用者:50名 ・1,2回イベントともPDA :30名 ・2回目イベントのみPDA:20名	36	WEB

##### 4. 5. 2 利用者にとっての有効性に関する評価・考察

###### (1) 利用者の関心度の評価・考察

モニタが実証実験を終了した後に、新領域 IT サービスの商用化に向けて、調査を行った結果を以下に示す。

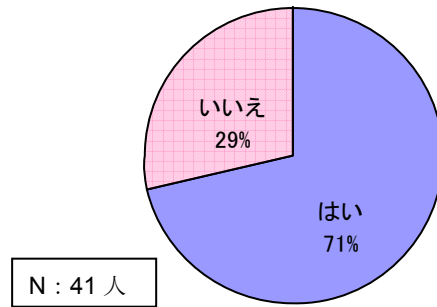


図 4-10 Q. 商用化されれば利用するか？（第1回アンケートより）

図 4-10 から分かるとおおり、全モニタの約 8 割が利用に関しての要望を持っていた。  
 図 4-10 の利用すると答えたモニタについて、新領域 IT サービスとして評価される具体的な要件を調査した結果は図 4-11 のとおりであった。

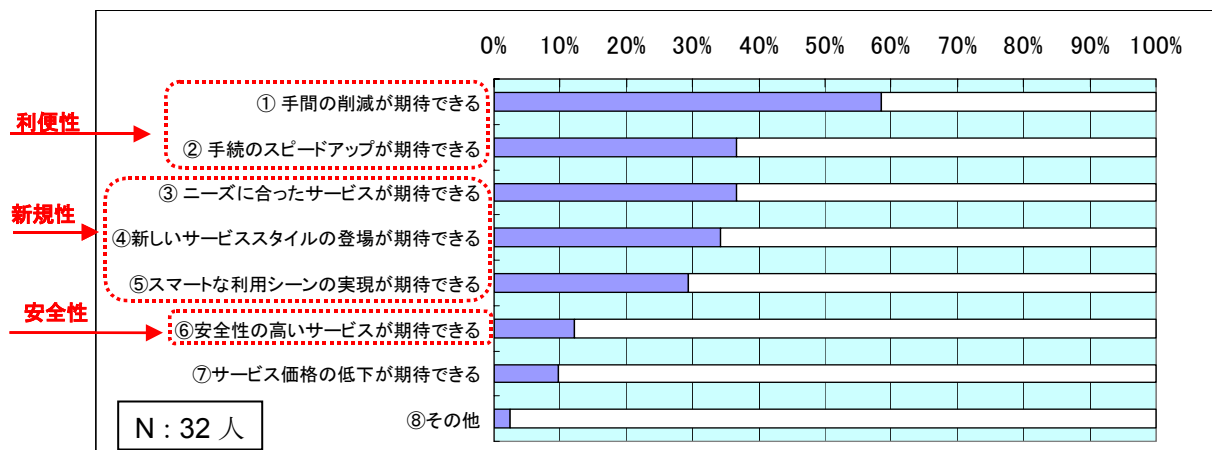


図 4-11 Q. 新領域 IT サービスのどの点を評価しているか？（第1回アンケートより）

モニタは「利便性の向上」という観点では「手間の削減」「スピードアップ」を、新規性という観点では「新しいサービススタイル」「ニーズに合致したサービス」「スマートな利用シーンの実現」を、評価していることがわかった。つまり、新領域 IT サービスでは、従来の利便性を損なわないか、更なる利便性の向上を図ることを前提としながら、新規性の充実に関心が高いことが分かった。

## (2) 利用者にとっての利便性の評価、考察

利便性の評価として、サービス毎の評価と、利用者端末の評価の二点から行う。

### ① サービス毎の利便性の評価、考察

電子チケットサービス（座席位置表示機能）、共鳴サービス、デリバリーサービス、お楽しみコンテンツサービスの 4 サービスについての検証結果を示す。

(ア) 電子チケットサービス（座席位置表示機能）に関する利便性について

本実証実験において、電子チケットサービスの機能である座席位置表示機能は新しく実現された機能であった。以下では、座席位置表示機能に関する検証を行った。座席位置表示機能を利用したモニタの感想は図4-12のとおりであった。

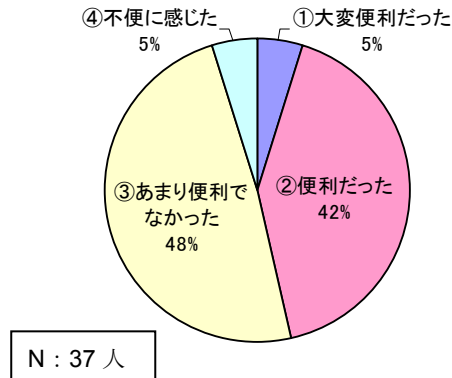


図4-12 Q. 座席位置表示機能についての感想は？（第2回アンケートより）

座席位置表示機能について、肯定的な意見と否定的な意見に二分されていることが分かる。「あまり便利でない」、「不便に感じた」というモニタに対して、原因を調査した結果、20%を超えるモニタが不便と感じた点は、「表示に時間がかかった」、「表示が見つらなかった」、「表示できる通信範囲が限定されていた」といった実装上の点であった。したがって、携帯可能な利用者端末で位置表示を行うサービスは、表示までの時間の短縮、操作のしやすさ、いつでもどこでも表示できる機能が充実すれば利用の機会が十分あると考えられる。

(イ) 共鳴サービスに関する利便性について

共鳴サービスを利用したモニタの評価は図4-13のとおりであった。

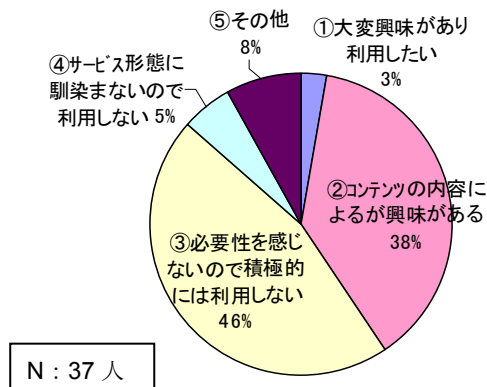


図4-13 Q. 共鳴サービスが実用化されれば利用したいか？（第2回アンケートより）

共鳴サービスでは販売促進に関する情報や他のイベント情報を表示するため、事業者にとってメリットの大きいサービスであるが、利用者にとっては、コンテンツに興味があれば、十分なメリットを感じることができないと考えられる。したがって、コンテンツの充実が必要であり、利用者の趣味・嗜好情報に対する分析手法の充実や、利用者が共鳴コンテンツを得る行動シーン（目的、時間、場所）についての検討が必要と考えられる。

表4-13にモニタが提供を望む利用シーンや情報を示す。

表4-13 Q. 共鳴サービスでは、どのような利用シーンでどのような情報を得たいか？（第2回アンケートより）

どのような利用シーンで	どのような情報を得たいか
洋品店や商店で	自分の前回までの購入履歴を見たい
駅やイベント会場で	近隣の（飲食店や映画館等）情報を見たい
ホテルのテレビやサロンなどの個室で	自分の嗜好にあった情報を見たい
飲食店や座席での待ち時間に	

表4-13より、自分の嗜好情報に関係するような情報は、公衆の目に触れない私的な空間で得たいと利用者が考えていることがわかった。また、購入履歴のような利用者にとってセンシティブな情報も、店舗で直接参照できることが求められていることが分かった。これは、利便性の向上のためだけでなく、各店舗が情報を持つことに対して、利用者の拒否感が弱いためであると考えられる。一方、駅やイベント会場といった不特定多数の人が周囲にいる状況では、利用者に関する情報ではなく、近隣の情報が求められていることが分かった。

共鳴サービスでは、自分専用のテレビのような表示機能が求められるシーンと、街頭にある案内版のような表示機能を求められるシーンの2種類が考えられ、場合分けを行いコンテンツの検討を行う必要があることが分かった。

### (ウ) デリバリーサービスに関する利便性について

デリバリーサービスを利用したモニタに対して行った調査結果を、図4-14に示す。

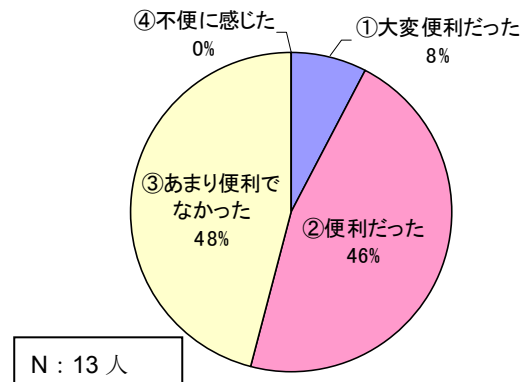


図4-14 Q. デリバリーサービスを利用した感想は？（第2回アンケートより）

本実証実験におけるデリバリーサービスの評価は肯定的な意見と否定的な意見の2つに割れている。これは、物品を手渡す際にかかった時間や、座席位置等の個別環境の差に起因したものと考えられる。

「あまり便利でなかった」としたモニタについて調査した結果、20%を超えるモニタが不便と感じた点について、以下に原因を述べる。

- ・商品受け渡しまでに時間がかかった  
受領証の授受に要した時間、つまり赤外線を用いた通信や端末の操作に時間がかかったことが考えられる。
- ・会場内で目立つ  
実証実験会場では、一部のスタッフがサービス利用者であるモニタの座席付近で立ち往生する光景が見られたことが原因と考えられる。
- ・会場が狭かった  
デリバリーサービスは通路に面した座席の利用者のみに行ったが、座席によっては通路が狭くなっていたことが原因と考えられる。

また、その他も20%を超えるモニタが挙げていたが、受領証の送受信に時間がかかった、周囲に迷惑がかかるといった意見が中心であった。

以上より、デリバリーサービスの商用化に向けては、受領証の授受についての性能向上に加えて、受領証の授受を行うシーンの再検討、会場内でのデリバリーを行う場所や運用方法について、会場毎の計画が必要であることが分かった。

(エ) お楽しみコンテンツサービスに関する利便性について

お楽しみコンテンツサービスを利用したモニタの評価を図4-15に示す。

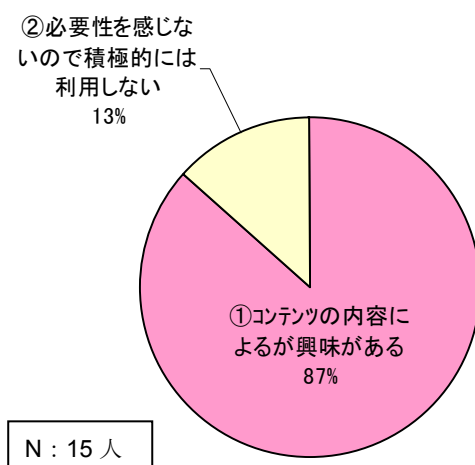


図4-15 Q. お楽しみコンテンツサービスが実用化されれば利用するか？（第2回アンケートより）

図4-15より、実用化はコンテンツ内容に大きく依存することがわかった。

利用者にとって、お楽しみコンテンツサービスが有効となるような利用シーンやコンテンツ内容について、調査結果を表4-14に示す。

表4-14 Q. お楽しみコンテンツサービスが有効と思われる利用シーンやコンテンツ内容は？（第2回アンケートより）

利用シーン	コンテンツ内容
映画館の待ち時間で	予告編を見たい
大型店舗内で	おすすめの商品情報の案内を受けたい
競技場内で	解説や選手のデータ、再生シーンを見たい
遊園地内での待ち時間	
	周辺のレストラン情報、各種クーポンを入手したい
	テレビ映像、映画、ゲームの配信を受けたい
	イベントに関する情報を見たい
	ニュース、運行情報、スポーツの結果速報を見たい

コンテンツの提供にあたっては、利用者が空き時間を利用した情報収集を目的としているのか、現在地に関する情報を主体的に得たいと考えているのかについて区分けを行い、コンテンツの絞込みを行う必要があると考えられる。

具体的には、空き時間を利用した情報収集ならばイベント情報等の放送に近いコンテンツを、場所に関する主体的な情報収集ならば近隣情報や交通情報といったコンテンツの提供が考えられる。

## ②利用者端末の利便性の評価、考察

以下では、PDA と IC カードの比較調査の結果をもとに、最適な利用者端末について考察を行う。

IC カードを利用したことがあるモニタは全体の 96%である一方、PDA を利用したことがあるモニタは 36%であった。したがって、PDA は IC カードと比較して日常的に接する機会が少なく、大部分のモニタが PDA の操作に対して習熟していないことが考えられる。

また、PDA と IC カードの両方を利用したモニタについて、操作性、処理時間を比較調査した結果を図 4-16、図 4-17 に示す。

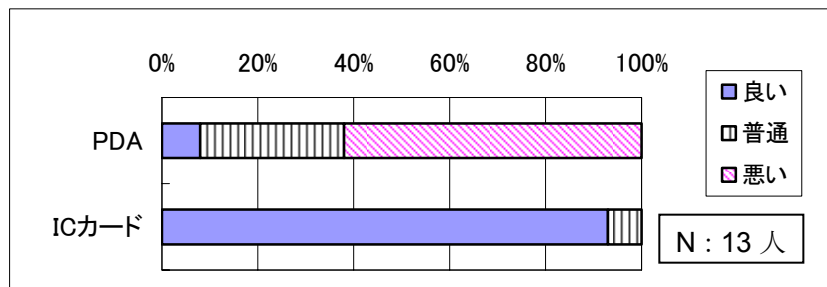


図 4-16 Q. PDA と IC カードの操作性は？ (第 2 回アンケートより)

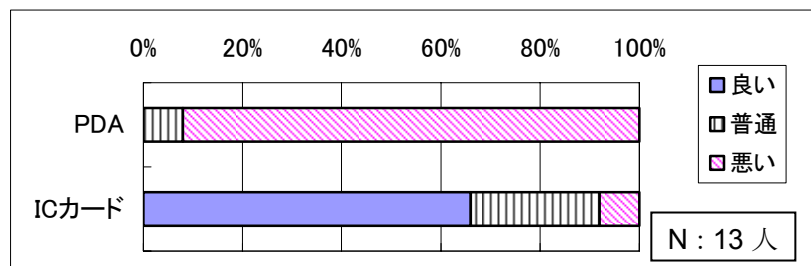


図 4-17 Q. PDA と IC カードの処理時間は？ (第 2 回アンケートより)

以上から分かるとおり、IC カードと PDA を操作性、処理時間において比較すると、PDA には大きなデメリットがあるといえる。

一方、図 4-18 に示すとおり、PDA では進行状況の把握や、インターネットや様々なコンテンツを PC 同様に利用できる点がメリットとして挙げられている。



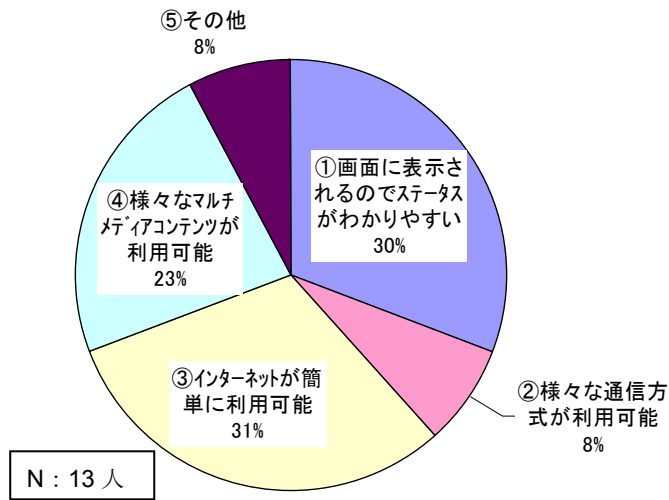


図4-18 Q. PDAを利用したメリットは？（第2回アンケートより）

PDAはICカードと比較して操作性、処理時間に関してはデメリットがあったが、進行状況把握、コンテンツ利用、インターネット利用に関してはメリットがあった。これらのメリットは携帯電話でも実現可能である。図4-19に示すとおり、利用者は本サービスを利用する上で携帯電話とICカードが最適であると考えていることが分かった。

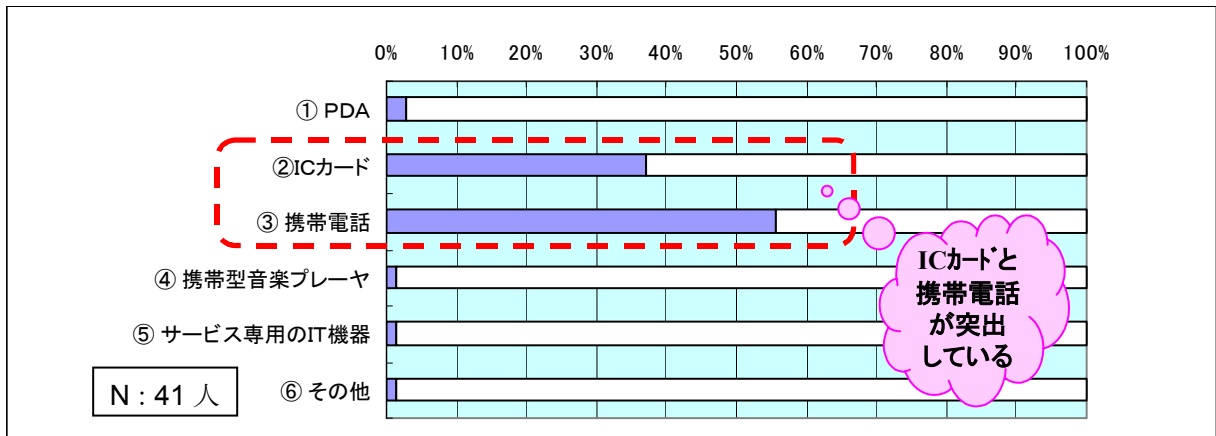


図4-19 Q. 本サービスに最適だと思う端末は？

したがって、最も望ましい端末は、非接触インターフェイスをもつ携帯電話に多機能ICチップを内蔵または挿入したものであると考えられる。携帯電話は利用者にとって身近である上、PDAのメリットも達成できると考えられる。

#### 4. 5. 3 利用者にとっての安全性における評価、考察

利用者の「安心感」を獲得するために、プロフィールデータに対する利用者の考えについて分析を調査した。モニタにとってプロフィールデータとして連想される情報は調査の結果、表4-15に示す4種類の情報であった。以下、この4種類の情報について分析を行う。

表4-15 プロフィールデータとして連想される4種類の情報

①住所・氏名などの個人を特定する情報	個人基本情報	個人に「到達」可能な情報
②利用者 ID などのサービス内で割り当てられる識別情報	個人基本情報	
③購入・利用履歴などのサービス内で作り出される情報	センシティブ情報	個人に「到達」困難な情報
④属性・嗜好情報などのサービス提供者への登録情報	プライバシー情報	

この4種類の情報を利用者が提供してもよいとする条件は以下のとおりであった。

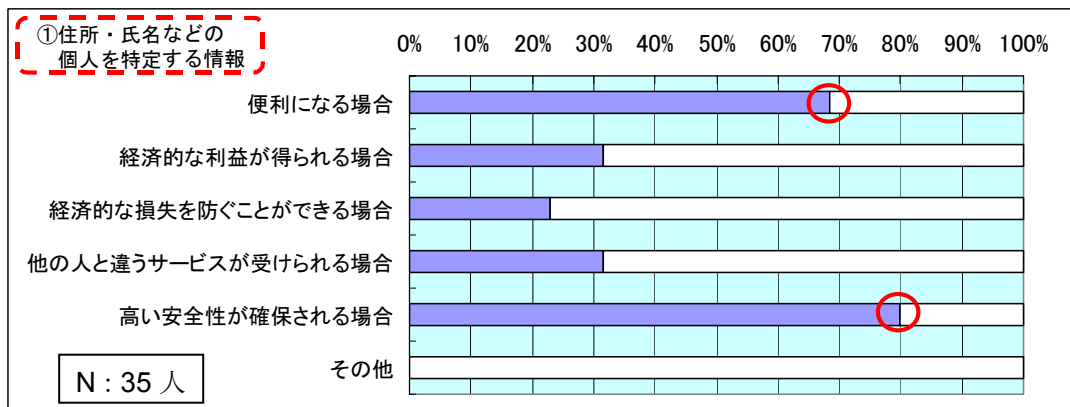


図4-20 Q. 住所・氏名を提供してもよい条件は？ (第1回アンケートより)

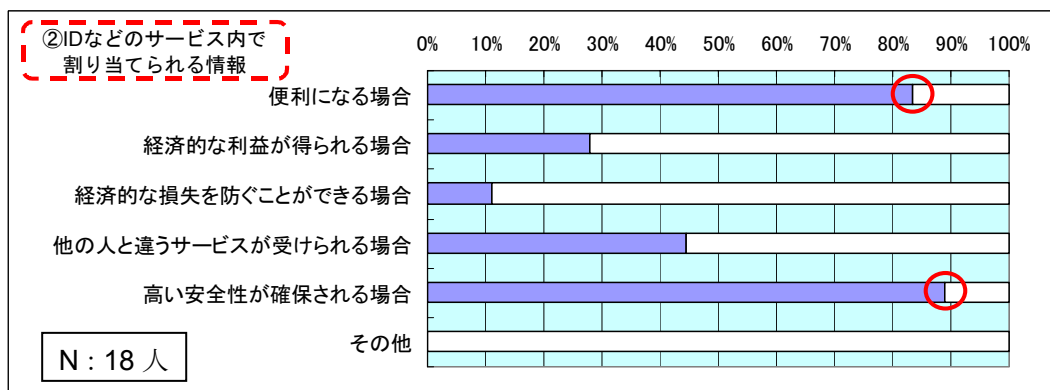


図4-21 Q. ID等を提供してもよい条件は？ (第1回アンケートより)

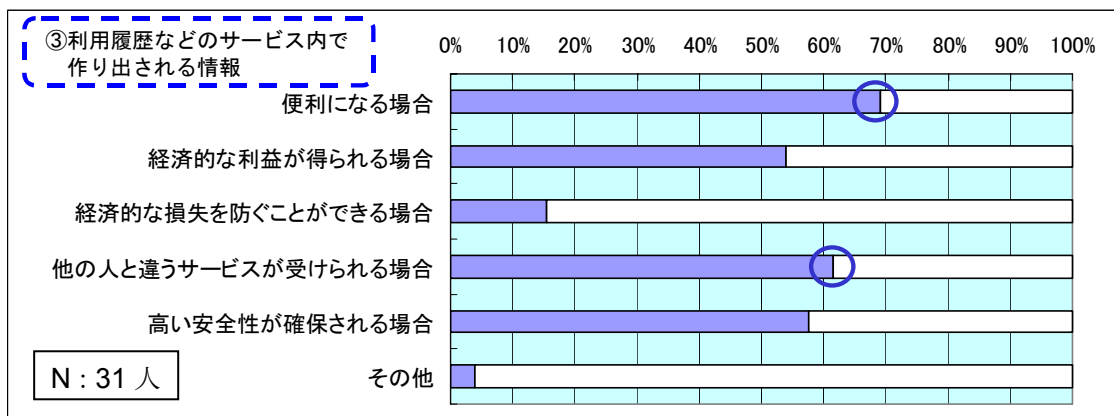


図4-22 Q. 利用履歴等を提供してもよい条件は？（第1回アンケートより）

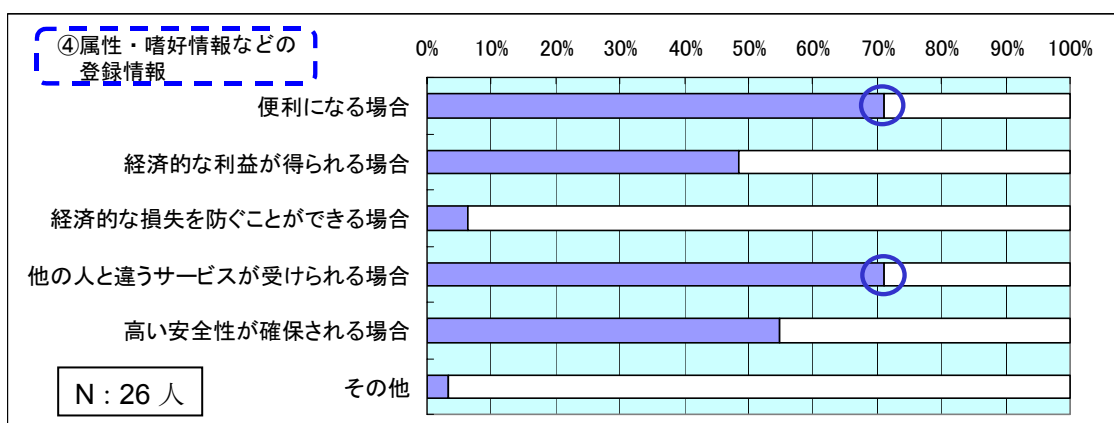


図4-23 Q. 嗜好情報を提供してもよい条件は？（第1回アンケートより）

図4-20と図4-21に示すように、個人に「到達」可能な情報について、利用者は利便性に加えて、高い安全性の確保を強く求めていることが分かる。

一方、図4-22と図4-23に示すように、個人に「到達」困難な情報について、利用者は利便性に加えて、他との差別化が図れるサービスの提供が求めていることが分かる。

サービス提供者にとって有用である利用履歴や嗜好情報を利用者から得るには、匿名性の高いサービス提供により、安全性を確保し、利用者に対して安心感を与えられる仕組みを作った上で、新規性の高いサービスの提供を模索することが必要であることが分かった。

#### 4. 5. 4 事業者にとっての有効性に関する評価・考察

##### (1) 事業者から見た利便性の評価・考察

本実証実験のアプリケーションについて事業者側の視点から利便性の評価、考察を行う。本実証実験のアプリケーションについて改善点を調査した結果を図4-24に示す。

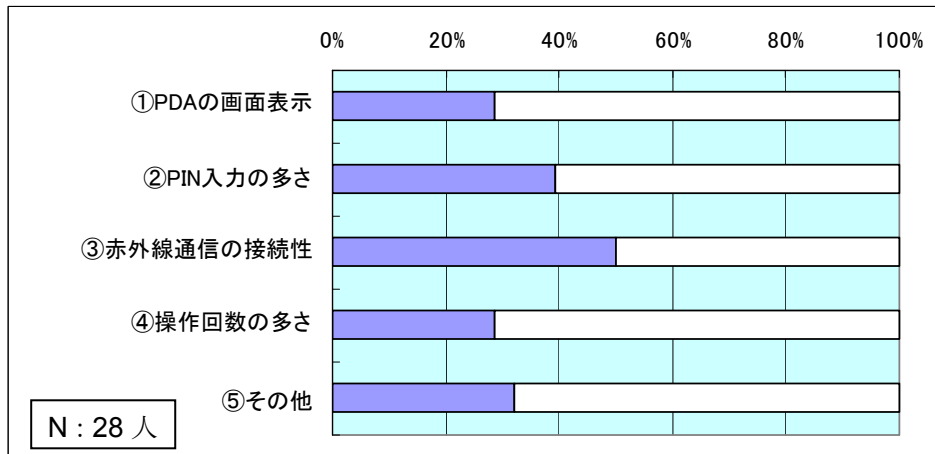


図4-24 Q. アプリケーションの改善必要性について

改善点として、赤外線通信による時間、PIN 入力の多さが上位に挙げられた。その他においても通信時間の短縮や PIN 入力の操作の改善が挙げられた。以下では、この二点について解決策の検討を行う。

#### ①PIN 入力に代わる認証方式

本実証実験では、利用者以外の者による不正利用を防止するため、サービス利用の最初の手順として PIN（暗証番号）入力を必須としたが、改善が必要であることが確認された。改善手法としてサービス利用時の個人認証回数の削減が考えられる。

ある特定の機関で認証が完了すれば、サービス個別の認証を必要としないようなシングルサインオン方式の採用が考えられる。シングルサインオンの想定イメージを図4-25に示す。

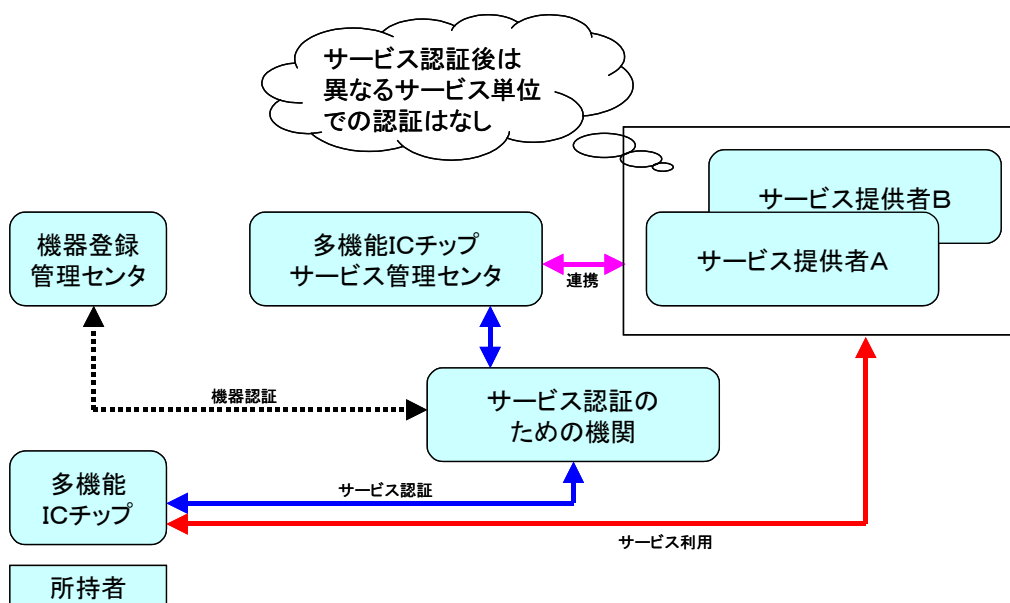


図4-25 シングルサインオン想定イメージ

## ②通信時間の短縮

本実証実験では図4-26に示すように、赤外線通信によって相互認証を実行した上で暗号化によるデータ通信を行った。

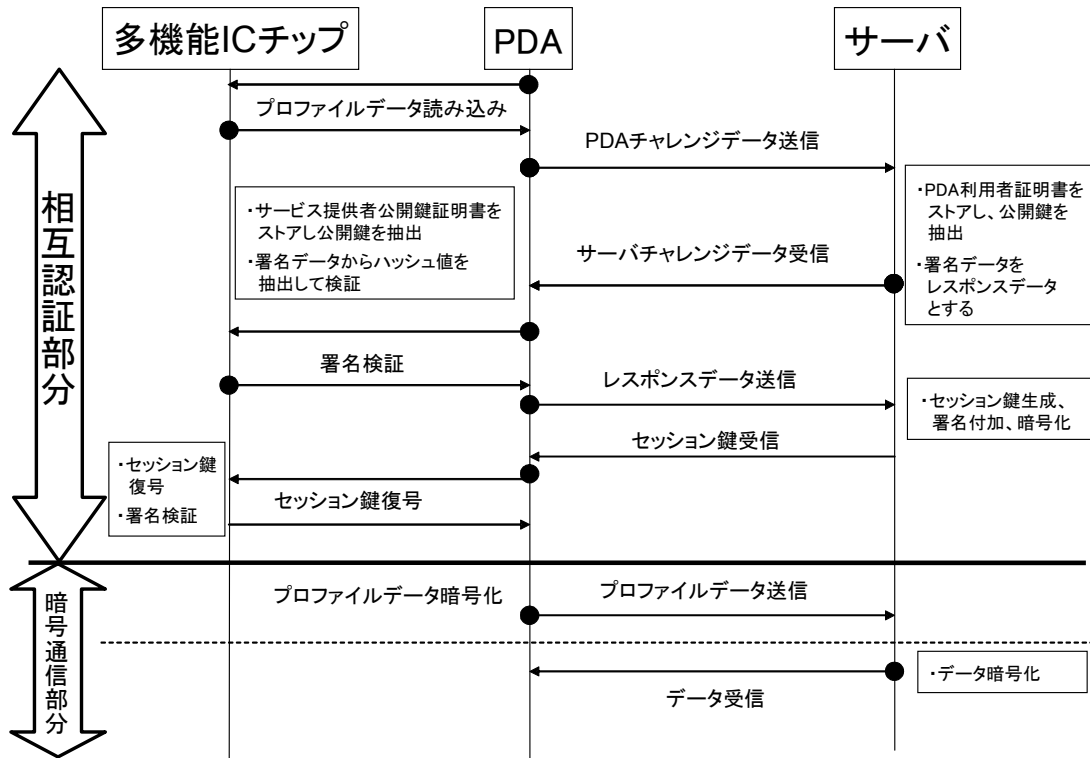


図4-26 相互認証とデータ通信の処理フロー

共鳴サービスについて、相互認証を利用したコンテンツ配信処理時間の解析を行った。利用者端末（PDA）側で行った処理にかかった平均時間は表4-16のとおりであった。

表4-16 PDAの平均処理時間（計測回数：10回）

処理名	平均処理時間[秒]
赤外線セッション確立	2.7
プロファイルデータ読み込み	6.5
PDA チャレンジデータ送信	0.1
サーバチャレンジデータ受信	0.7
署名検証	1.5
レスポンスデータ送信	0.4
セッション鍵受信	0.5
セッション鍵復号	0.0
プロファイルデータ暗号化	1.1
プロファイルデータ送信	0.7
コンテンツ受信	26.6
赤外線通信切断	0.4
合計	41.2

共鳴サービスは改札処理のような即応性が強く求められる処理ではないが、赤外線通信を利用した処理時間が長いことがわかった。また、アンケートにおいても、図4-17に示したとおり、利用者にとっては時間がかかるという意見が多かった。

実証実験での通信性能に影響した要因として以下の理由が考えられる。

- ・多機能 IC チップとサーバとの通信に PDA が仲介されている
- ・トランザクションが最適化されていない
- ・赤外線通信におけるセッション確立に時間がかかっている

これらの3点を解決することにより、ICカードに準じた処理時間でサービス提供ができると考えられる。

## (2) 事業者から見た事業性に関する評価・考察

多機能 IC チップサービス管理センター、プロファイルデータ収集管理機関、サービス連鎖管理機関等のプロファイルデータを収集管理する事業者や、サービス提供者における事業性に関して、事業者ヒアリングを行った結果を表4-17に示す。

表 4-17 事業性のヒアリング結果

ヒアリング観点	ヒアリング内容	ヒアリング結果
事業性	プロフィールデータを収集管理する事業者の立場になった場合、そこに事業性を見出せるか。	<p>(イベント主催者、チケット販売会社) 事業性は低い。役割や機能上、公平性、中立性が必要。特定の企業がこのポジションを担うことや、営利を目的とした事業インフラとして、位置づけることは困難。</p> <p>(クレジットカード会社) 事業性は見出せる。プロフィールデータの分析情報を横断的に利用可能とする方式が考えられる。</p>
	サービス提供者の立場の場合、プロフィールポータビリティサービスを利用したサービスに事業性を見出せるか。	<p>(イベント主催者、チケット販売会社、クレジットカード会社) 事業性は高い。情報収集管理におけるリスク、コストをミニマイズした、パーソナルマーケティングへ応用可能。</p>

以下にプロフィールデータを収集管理する事業者、サービス提供者の立場に関する意見をまとめた。また、プロフィール連携する際のサービスの組み合わせやその連携モデルについて、検討した結果をまとめた。

①プロフィールデータを収集管理する事業者の立場の場合

効果がコストに見合うかが課題であり、プロフィールデータを収集管理する事業者は、公平性や中立性が求められる第三者的な機関として位置づける方がよいとの意見が挙げられた。

一方、クレジットカード会社では、プロフィールデータの分析に関する実績をもとに、利用者の分析情報を横断的に利用可能とする方式が考えられる。図 4-27 に示すモデルによって、クレジットカード会社はプロフィールデータを収集管理する事業者の立場をとり、他のサービス提供者である加盟店と協調関係を強化することが期待されていた。

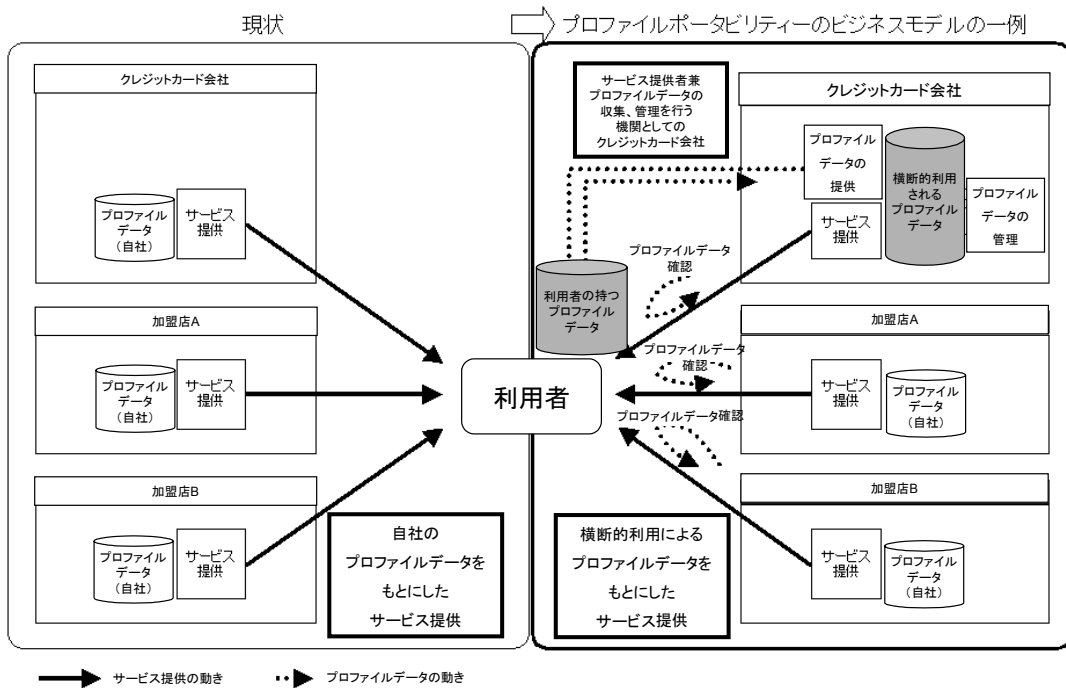


図4-27 プロファイルポータビリティサービスの活用モデル

## ②サービス提供者の立場の場合

プロファイルデータを収集するためのリスク、コストを縮小し、従来よりも個々の顧客に合わせた販売促進を行いやすい環境が構築できると期待されることから、事業性が高いことを確認した。しかし、以下のような検討課題も挙がった。

- 個人情報保護法への対応の観点

サービス提供者が個人情報保護法上、どのような扱いとなり、どの程度の責務を負うことになるのかは、現段階では判断できない。

- サービス提供者の参加

ある程度プロファイルデータが蓄積され、プロファイルデータの流通が円滑に行われるような状態になってから参加するほうが、サービス提供者にとってメリットが大きいと考えられる。サービス提供者は参加に際して、仕組みが成熟するまで静観しあい、結果的に仕組みの成熟が困難となるという悪循環が起きる可能性がある。独自では得られないような情報が得られる、情報の提供に対する報酬が得られるような仕組み作りが必要である。

- サービス提供者によるプロファイルデータの流通の制御

他事業者へのプロファイルデータの流通を拒絶したい場合があることから、対応できる仕組み作りが必要である。



- 事業者間での責任の明確化

本研究のモデルを複数事業者間で行う場合においても、従来どおり、責任範囲の明確化を行う必要があり、契約等による手続きが軽減されるか検討を要する。また、情報の漏洩があった際は、法的な対処だけでなく利用者への対応が必要であり、第三者的な管理機関での情報管理についても責任を負う必要がある。

- 事業者間連携と不正競争

事業者間の連携が不正競争防止の観点から問題になる可能性がある。

以上より、今後ビジネスモデルを検討する上で、サービス提供者や第三者的な管理機関へのキックバックの仕組み（例として、ポイントの流通等）の検討や、サービス提供者にとってこの仕組みが有効なケースの検討、個人情報保護に関する一層の法制度的な検討が必要であることがわかった。また、複数の一般サービス事業者による連携を仮定する前に、グループ企業間において個人情報を取り扱う方式として、本研究のモデルを検討するといったアプローチが、現実的と考えられる。

### ③プロファイルポータビリティサービスの連携モデルの検討

プロファイルポータビリティサービスを実現する上での連携モデルについて、利用者の視点及び立場を想定し、プロファイル連携が有効と考えられるサービスの組み合わせについての検討を行った。その結果、図4-28 図4-29に示すような連携サービスの可能性について示唆することができた。

以下のようなサービスの実現に向けては、ポイントから電子マネーへの交換等の制度的な課題について検討する必要がある一方で、既に実用化されているICカード等の既存のインフラストラクチャとの連携や融合等、利用面での課題について検討する必要もある。また、複数のサービスを1枚の多機能ICチップやICカードに集約し、日々活用することにより、紛失や盗難等によるリスクを軽減する手法についての検討も必要である。

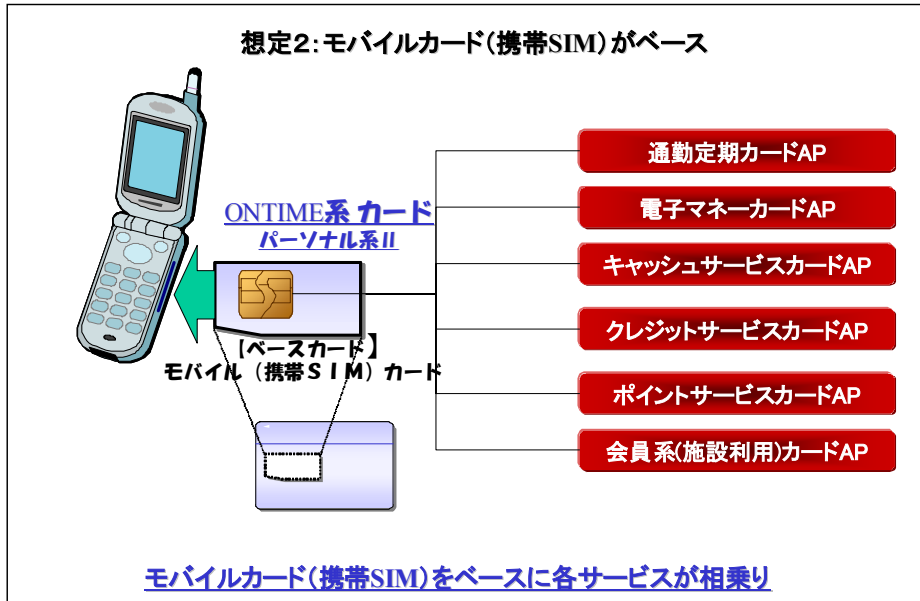


図 4-28 モバイルカード(携帯SIM)が連携ベースの場合

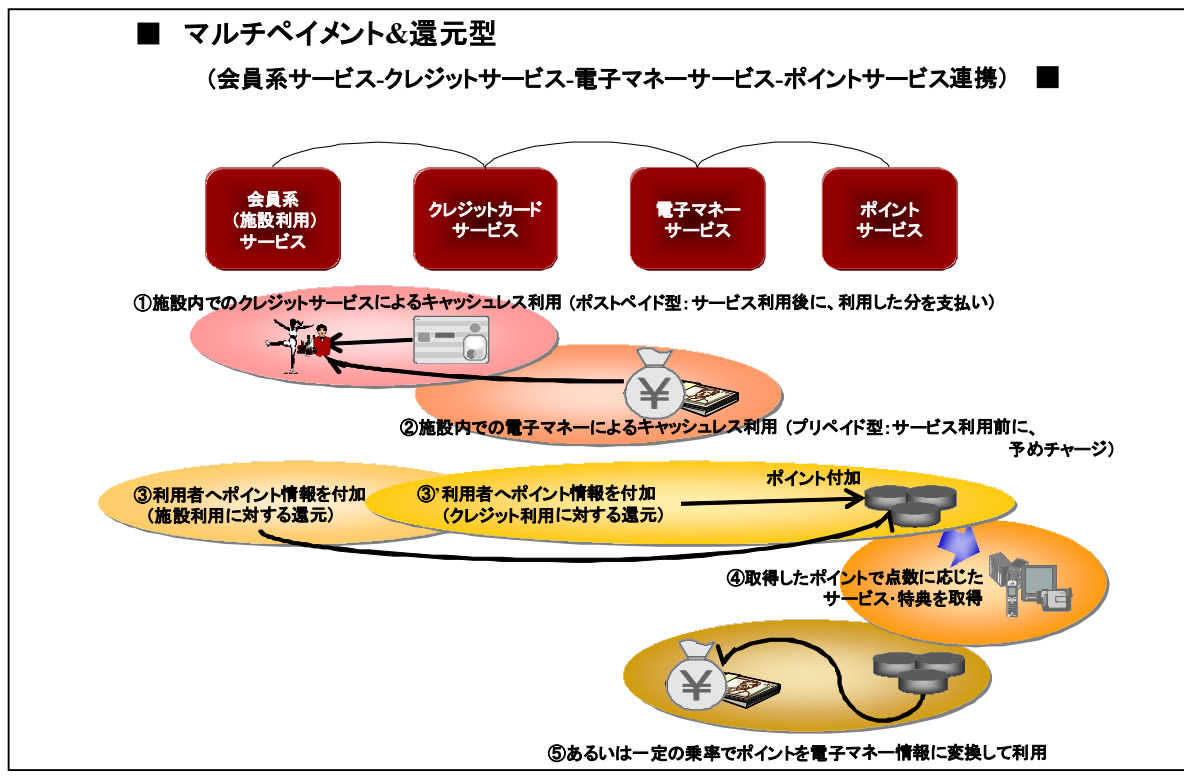


図 4-29 マルチペイメント&還元型連携サービス







4. 6 まとめ

4. 6. 1 プロファイルポータビリティサービスの有効性について

以上のとおり、本研究では、プロフィールデータを利用することによって、利用者の嗜好情報に基づいたサービスや、プロフィールデータの横断的な利用によって連鎖的に提供されるサービスの有効性について検証を行った。

利用者から見た各検証テーマにおける課題と強化すべきポイント、ならびに今後の取り組みの方向性を表4-18に示す。

表4-18 利用者からの視点による検証項目別課題と今後の取り組みの方向性

検証項目	課題と強化すべきポイント	今後の取り組みの方向性
利用者の関心度	◇商用化にむけた利便性と安全性の充実 (新領域ITサービスの利用に対して、関心度は高い[利用したい:92%]が、商用化の際の利用については課題がある[利用したい:78%]。) 	◆安全性を保ちながら、利便性向上を図る (操作性や認証方式の工夫により、手間の削減や手続きのスピードアップを図る。) 
利便性	◇各サービスにおける利用者の満足度向上 (検証を行った4サービスでは、サービスが便利であった、今後も利用したいという意見が全体の半数以下にとどまった。無料なら利用する、コンテンツに依存するとの意見が挙げられた。) ◇ハード面での性能向上 (操作性、処理時間、携帯性について改善が必要) 	◆サービス提供の速度向上 (受領証の受け渡し等にかかる時間の短縮を図るため、通信手段や処理を見直す) ◆利用シーンとコンテンツの整理、検討 (利用シーン別にニーズのあるコンテンツを検討、充実を図る。) ◆ICチップ内蔵タイプの携帯電話によるサービス検証 (操作性、処理時間、携帯性を改善し、普及の面や利用者にとっても親和性の高い機器での検証を目指す) 
安全性	◇新領域ITサービスに関する安心感の醸成 (個人に直接「到達」できる情報は安全性が、個人に直接「到達」できない情報はサービスに付加価値が求められる。) 	◆匿名性による当該サービスの実装 (個人を特定できない形式での高付加価値サービスの提供を目指す。) 

考察より、プロフィールポータビリティサービスでは、安心を与える仕組みをもとにして、新規性ならびに十分な利便性を確保したサービス展開が重要であることがわかった。

また、サービスを利用するための利用者端末の性能向上は必須であり、利用者はICチップ内蔵タイプの携帯電話を望んでいることがわかり、今後の検討対象としても期待が高いことがわかった。

次に事業者から見た各検証テーマにおける課題と強化すべきポイント、ならびに今後の取り組みの方向性を表4-19に示す。

表4-19 事業者からの視点による検証項目別課題と今後の取り組みの方向性

検証項目	課題と強化すべきポイント	今後の取り組みの方向性
利便性	<ul style="list-style-type: none"> <li>◇ハード面での性能向上                             <ul style="list-style-type: none"> <li>（通信時間が長く、サービス提供に時間がかかった</li> <li>暗証番号の入力が繰り返し必要であり、手続きが煩雑</li> </ul> </li> <li>◇サービス連鎖によるサービス提供の充実                             <ul style="list-style-type: none"> <li>（運用面や利用者に対するメリットを与えられるサービスの検討</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>◆ハードウェアの改善、トランザクションの最適化                             <ul style="list-style-type: none"> <li>（多機能ICチップとサーバ間で直接通信を行う方式の検討や</li> <li>処理時間と安全性を勘案したトランザクションの最適化を行う</li> </ul> </li> <li>◆安全を確保した個人認証手続きの軽減                             <ul style="list-style-type: none"> <li>（生体認証やシングルサインオンによる負担の軽減を図る</li> </ul> </li> <li>◆サービス連鎖によって提供される新たなサービスの検討                             <ul style="list-style-type: none"> <li>（利用シーンとコンテンツの整理を行い、サービス連鎖によって提供できるサービスの具体化を行う</li> </ul> </li> </ul>
事業実現可能性	<ul style="list-style-type: none"> <li>◇ビジネスモデルの具体化</li> <li>◇個人情報保護に関する法制度面での検討の深耕</li> <li>◇複数事業者間での契約や責任範囲の明確化</li> </ul>	<ul style="list-style-type: none"> <li>◆サービス提供者間でのプロフィールデータの利用に対する制御方式の検討</li> <li>◆サービス提供者における個人情報保護法への対応検討</li> <li>◆プロフィールデータの利用や提示にかかるコストモデルや報酬の仕組み検討</li> <li>◆グループ内企業への適用検討</li> </ul>

商用化に向けては、本実証実験のサービス内容の改善が必要であることがわかった。利用シーンに応じたコンテンツの具体化と充実や、利用者端末や認証方式の検討が必要である。

本研究におけるプロフィールデータの収集管理や横断的利用に係る仕組みでは、サービス提供者にとって、メリットがあることを確認したが、実現に向けてはビジネスモデルの検討や法制度面での検討が必要である。サービス提供者が参加することによるコスト対効果の明確化、個人情報保護法との関連、複数事業者での合意形成のあり方といった課題がある。

#### 4. 6. 2 利用実現に向けた課題解決に向けて

新領域 IT サービスとしてのプロフィールポータビリティサービスの実現、商用化に向けて、技術面での課題、法制度・ビジネスモデルといった業務面での課題と、その解決の方向性について以下に示す。

##### (1) 技術面での検討課題とその解決の方向性

技術面において抽出した課題と解決の方向性について以下にまとめた。

###### ①利用者によるプロフィールデータのアクセス許可方式の検討

サービス毎に数多く存在するプロフィールデータをサービス提供者間で共有するためには、利用者の許可に基づきプロフィールデータへのアクセスを制御する仕組みを構築することが必要である。そのため、サービス種類、サービス提供者などを限定するためのアクセス権の付与を検討する必要がある。

###### ②事業者間によるプロフィールデータのアクセス許可方式の検討

プロフィールデータのアクセス許可は各事業者間の契約にも対応する必要がある。契約に基づく細かな設定ができるようにアクセス権を付与する必要がある。

###### ③認証方式の工夫

PIN 認証は容易に本人確認をすることができるが、認証の度に利用者が PIN を入力しなければならない。そこで、サービス利用中における認証回数の低減が必要である。例えば、シングルサインオンなどの一度認証が完了すれば他のタイミングにおける認証を必要としないような方式の構築が挙げられる。

上記の第 1 点と第 2 点は、利用者や各サービス提供者がプロフィールデータの利用許可を与えるものである。プロフィールデータをコンテンツとして考えた場合、コンテンツの利用権について検討したテーマ種別 2 の仕組みに類似点が認められる。たとえば、サービス提供者間でプロフィールデータの連携を行う場合、利用者が他サービス提供者に対し利用者のプロフィールデータを参照するため許可を与えたことを検証する必要があり、サービス提供者間で利用者の署名入り証明書を授受することが想定される。利用者や各サービス提供者が許諾を与えるこの仕組みにおいては、コンテンツ流通における権利者側が所有する権利を扱う仕組みの議論との関連が深い。

##### (2) 業務面での検討課題とその解決の方向性

業務面において抽出した課題と解決の方向性について以下にまとめた。

###### ①個人情報保護法に基づく対応の検討

事業者にとって本研究のプロフィールポータビリティサービスのモデルに参加を判断するには、サービス提供者やプロフィールデータの管理を行う機関に求められる個人情報保護法への対応や、利用者に対して負うべき責任範囲を明確にする必要がある。

## ②匿名式によるサービス利用の検討

実運用段階では、サービス提供者が独自に収集した個人基本情報とプロフィールデータの管理を行うことが想定されるため、サービスの利用履歴等が個人基本情報と紐付けされて管理されることが想定される。サービス利用者が個人基本情報の管理を行わないような、匿名式でのサービス利用方式について、実現可能性の検討が必要である。また、その際、サービス提供者は個人情報保護法に基づいて、どのような対応をとらなければならないのかを明確にする必要がある。

## ③他事業者との連携によるメリットの明確化

他事業者との連携によって、実際にどのようなプロフィールデータの横断的利用が可能となり、サービス提供者にとってメリットが与えられるのかを明確にする必要がある。収集したプロフィールデータの利用を許可するサービス提供者への報酬の仕組みや、提携のあり方について検討が必要である。

## ④利用者にとって分かりやすい仕組み作り

新規サービスの創出やサービス提供者の参加に伴い、利用者に対して通知や確認を行う必要があり、手続きが煩雑になる恐れがある。利用者にとって幾重にもなる確認作業が行われる場合にはサービス提供者や各機関の相互の違いを正確に理解することが困難となる。登録の意味、利用範囲、今後の個人情報の利用について、どのように説明するか、注意が必要となる。

## ⑤プロフィールデータのモニタリングについて

収集する情報、解析する手法、利用できる環境などによっては、個人をモニタリングする可能性も生まれてくるため、そうしたモニタリング効果についても十分な配慮が必要となる。すなわち、情報提供者である本人に対して、情報利用の可能性について相当な理解を得られるような努力が必要である。

上記課題の第1点目、第2点目は、今後の個人情報保護のあり方とも密接に関わる点である。

第3点目については、参加事業者にとって、どのような体制が望ましいのかについて検討が必要である。合意形成等の障壁を考慮すると、グループ企業群への本事業モデルの適用検討が必要であると思われる。

上記課題の第4点、第5点目は利用者に対する配慮の問題である。利用者にとって分かりやすい仕組み作りがビジネスモデルの検討において不可欠である。また、事故が起こった際の責任の所在や対処法について議論を行い、対策コスト等を勘案することがビジネス展開において必要である。