平成16年度

先導的分野における戦略的情報化推進事業

多機能ICチップ等を活用した情報サービスシステム基盤の構築・検証及びリモートサービスのセキュリティに関する研究開発・実証事業

報　告　書

平成17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、環境整備と各種システムの導入が進められている。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 月に発足した。

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など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、利用者認証や情報の秘匿技術などを用いて、利用者に安心感を与えることが、IT 社会の構築に不可欠なことが明らかになっている。

一方、知的財産戦略大綱に書かれているように、ディ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と予想される。そしてこのような手法が実現すれば、ソフトウエアや音楽などの利用権を 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ィジタル情報の利用が可能になる。

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、その実現により「正当な人が安全な機器で正しい情報にアクセスする」という革新的な環境を作り出すと期待される。本事業で得た成果は、新たな認証のフレームワークの実現が可能であることを明らかにしており、我が国が目指す知的創造社会や IT 社会の実現に、この成果が大きく貢献することを期待する。

平成 17 年 3 月

（多機能 IC チップ等を活用した情報サービスシステム基盤の構築・検証及びリモートサービスのセキュリティに関する研究開発・実証事業）　　推進委員会委員長　大山　永昭

平成16年度先導的分野における戦略的情報化推進事業

多機能 IC チップ等を活用した情報サービスシステム基盤の構築・検証及びリモートサービスのセキュリティに関する研究開発・実証事業

目　次

はじめに

本事業の全体概要

経済産業省が平成 16 年度に行った「先導的分野における戦略的情報化推進事業（多機能 IC チップ等を活用した情報サービスシステム基盤の構築・検証及びリモートサービスのセキュリティに関する研究開発・実証事業)」（以下「本事業」という。）では、平成 15 年度における検討を踏まえたサービスを実現するためのインフラを実現する事業と位置付け、サービス実施において必要となる機能の実装を行った。サービスを実現するためのシステム（機能）として、「機器登録管理センタ」（以下「登録センタ」という。）の機能である多機能 IC チップ登録機能をサーバ上に実装し、多機能 IC チップの登録処理が可能であることを研究開発し確認した。また、登録処理を行う対象の機器は、多機能 IC チップが搭載（組み込まれた）されたものを利用し、デジタルコンテンツ流通等の電子的に権利を行使するサービスやマルチベンダでの医療システム機器等のリモートサービスの検証を行い、登録センタの機能についての技術面及び利用面の課題を整理した。

これらの研究開発を通じて本事業の成果を活用することにより、今後、登録センタを構築し実運用する上での基盤技術として、多機能 IC チップ等を活用したサービスシステムの基盤を整備することを目的とした。

業務区分及び実施体制

本事業は、工程管理等に関する業務と研究開発及び実証事業とに分類され、工程管理等に関する業務については、財団法人ニューメディア開発協会が受託した。また、3 つのテーマで構成された研究開発及び実証事業については、エヌ・ティ・ティ・コミュニケーションズ株式会社を代表研究員とするコンソーシアムが受託し、それぞれのテーマについて責任研究員を設け、事業を推進した。

以下に、各業務の実施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

1. 事業概要

財団法人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 16 年度「先導的分野における戦略的情報化推進事業（多機能 IC チップ等を活用した情報サービスシステム基盤の構築・検証及びリモートサービスのセキュリティに関する研究開発・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。

この工程管理に係る実施期間及び業務内容は以下のとおりである。

実施期間

平成 16 年 9 月 1 日～平成 17 年 3 月 31 日

業務内容

◎ 公募関連業務

・本事業の研究員の公募実施及び審査委員会の運営

◎ 委員会・会議等開催業務

- 推進委員会
- Steering　Board 会議

◎ 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

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。

2. 実施内容

2. 1　公募業務

2. 1. 1　公募の経緯

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)」では、多機能 IC チップを活用できるサービスの適用領域と、それを実現する多機能 IC チップのフレームワークの検討を行い、取りまとめた。

経済産業省は、昨年度における検討を踏まえたサービスを実現するための機能を研究開発し、当該機能をデジタルコンテンツ流通等の電子的に権利を行使するサービスやマルチベンダでの医療システム機器等のリモートサービスにおいて検証し、技術面及び運用面の課題を整理し、官民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、経済産業省より平成 16 年 10 月 8 日から平成 16 年 10 月 22 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 1 件の申請があった。当協会では、経済産業省の委託に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 1：多機能 IC チップ等を活用したサービスを提供するための基盤となる登録センタ機能の研究開発及び実証実験

② テーマ 2：登録センタの機能を活用したデジタルコンテンツ流通サービスの研究開発及び実証実験

③ テーマ 3：登録センタの機能を活用した医療システム機器等のリモートサービスの研究開発及び実証実験

2. 1. 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研究テーマに対して、研究テーマの先進性、具体性、適正性等を勘案し、かつ公平性をもって研究開発及び実証実験内容を審査し、研究員の選定を行う機関として、「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した。

2．1．3　結果

本事業の公募に対して、審査委員会にて申請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
多機能 IC チップ等を活用したサービスシステムの基盤整備コンソーシアム	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 16 年 11 月 29 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　業務内容

当協会では、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「多機能 IC チップ等を活用したサービスシステムの基盤整備コンソーシアム」（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、株式会社 NTT ドコモをはじめとした 10 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 1：多機能 IC チップを活用したサービスを提供するための基盤となる登録センタ機能の研究開発及び実証実験

多機能 IC チップが搭載された機器によるサービス実施において必要となる機器登録等を行う登録センタの研究開発を行うとともに、テーマ 2、テーマ 3 で用いる多機能 IC チップ搭載機器の登録・運用管理を行い、機能的な検証を行った。また、ネットワークを持たない多機能 IC チップ搭載機器と連携して登録・アプリケーション追加、アプリケーション削除等を行うための可搬型リーダライタについての研究、及び多機能 IC チップ搭載機器の機器としてのセキュリティ管理やライフサイクル管理のあり方についての検討を行った。

②テーマ 2：登録センタの機能を活用したデジタルコンテンツ流通サービスの研究開発及び実証実験

多機能 IC チップフレームワークを活用したデジタルコンテンツ再生機器によるコンテンツ流通サービスの事業化に向けた検証を行うため、テーマ 1 で構築する登録センタに対してデジタルコンテンツ再生機器を登録する機能、利用権を持っているコンテンツに関して複数の機器での再生を実現する機能、複数の機器で再生した場合でもコンテンツの利用料や権利料の分配を可能にするための利用者認証用 IC カードへのコンテンツ再生ログ保管機能及びコンテンツの利用期間制御を行うサービスを実現するためにデジタルコンテンツ再生機器内の多機能 IC チップにコンテンツ再生終了日時を保管する機能について研究開発及び実証実験を行った。

③テーマ 3：登録センタの機能を活用した医療システム機器等のリモートサービスの研究開発及び実証実験

テーマ 1 で構築する登録センタを活用するとともに、昨年度に開発した認証接続管理サービスを発展させることにより、インターネット回線を利用した安全な通信基盤を実現させるための研究を行った。また、医療システム機器の予防保守サービスに資する定期的な状態監視や、システムダウンに対する早期バックアップサービスなどの機能を開発し、前述の通信基盤に接続することにより、安全な医療サービス実現に向けた研究開発及び実証実験を行った。

2．2．2　実施体制

事業全体の実施体制を図 2-1 に示す。

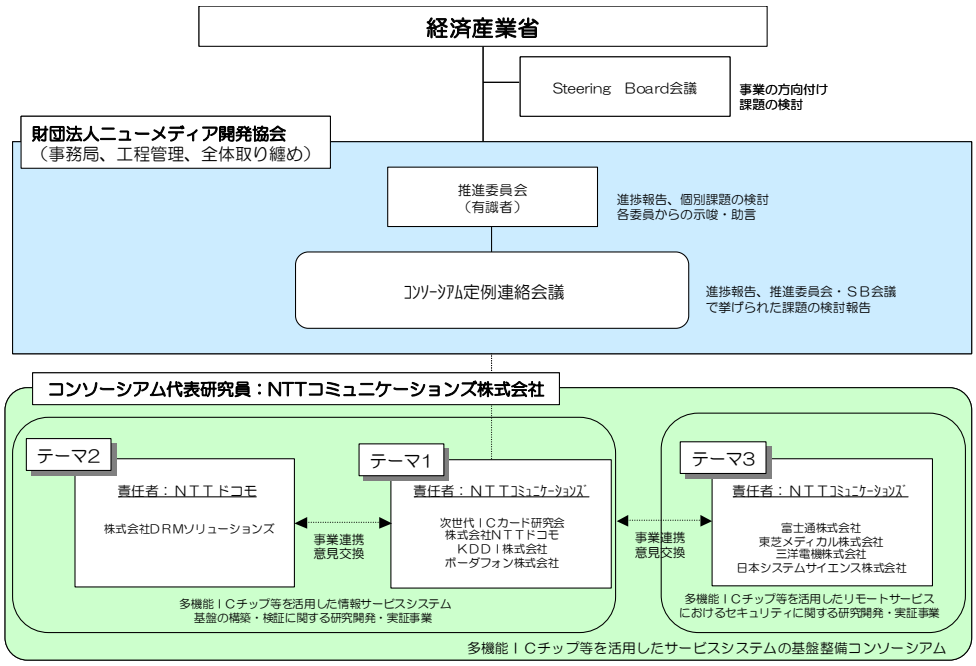


図 2－1　実施体制図

2. 3　委員会等運営業務

本事業では、事業の円滑な推進及び管理を行う観点から、以下の委員会の設置及び会議体を開催した。

2. 3. 1　推進委員会

(1) 目的

推進委員会は、本事業の諮問機関として本事業の円滑な実施を図ることを目的とし、以下のことを行った。

① 本事業の推進方策の提言
② 本事業の円滑な実施ならびに本事業の成果の普及に係る助言及び助力
③ 本事業の評価
④ その他本事業の目的を達成するために必要な事項に関する検討

(2) 構成

推進委員会は、多機能 IC チップ等を活用した情報サービスシステム基盤及びリモートサービスのセキュリティについて総合的に評価可能な学識研究者及び専門家等により構成した。

また、経済産業省、コンソーシアム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。

推進委員会の構成員は以下のとおり。

委員長	東京工業大学 フロンティア創造共同研究センタ	教授	大山　永昭
委員	独立行政法人 産業技術総合研究所	研究コーディネータ（情報通信担当）	大薪　和仁
委員	社団法人 日本音楽著作権協会	常務理事	加藤　衛
委員	東京工業大学 像情報工学研究施設 IT 都市創造工学研究部門	特任教授	喜多　紘一
委員	慶應義塾大学　大学院 政策・メディア研究科	助教授	北川　和裕
委員	財団法人ニューメディア開発協会	常務理事	国分　明男
委員	株式会社電通 統合マーケティング局　IMC 推進室	主管	斎藤　ようこ
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

（50 音順）

(3) 開催日時及び審議内容

第 1 回　推進委員会

日程：平成 17 年 1 月 26 日（水）

場所：芝パークホテル　桜の間　（東京都港区芝公園 1-5-10）

内容：①委員紹介及び委員長選出

②事務局による事業概要、実施体制、スケジュールに関する説明

③事務局による委員会の設置、役割に関する説明

④研究員による本事業の実施内容に関する説明

⑤本事業の実施内容に関する審議

第 2 回　推進委員会

日程：平成 17 年 3 月 1 日（火）

場所：NTT コミュニケーションズ株式会社　竹橋ビル

（東京都千代田区一ツ橋 1-2-2）

内容：①実証実験概要説明

②各テーマの実験見学・参加

第 3 回　推進委員会

日程：平成 17 年 3 月 17 日（木）

場所：芝パークホテル　アイビーホール　（東京都港区芝公園 1-5-10）

内容：①前回議事録について

②事業報告及び実証実験の結果報告

・財団法人ニューメディア開発協会より事業報告

・研究員より事業報告

③報告書の取りまとめについて

2．3．2　Steering　Board 会議

(1) 目的

Steering　Board 会議は本事業の技術推進方策の検討や技術検討結果に係る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、主に本事業の根幹である登録センタへの機器の登録方式について検討した。

(2) 構成

Steering　Board 会議は、本事業における推進委員会委員長である大山教授、経済産業省、ならびにコンソーシアム企業にて構成され、事務局は当協会が担当した。

(3) 開催日時及び審議内容

第 1 回　Steering　Board 会議

日程：平成 16 年 12 月 7 日（火）

場所：NICSS 事務局

（東京都港区西新橋 2-14-1 興和西新橋ビル B 棟 16 階　1604 号）

内容：①Steering　Board 会議について

②実施計画書に基づく実施内容について

③進捗状況について

④今後について

・課題の整理

・次回 Steering　Board 会議に向けて

第 2 回　Steering　Board 会議

日程：平成 16 年 12 月 15 日（水）

場所：NICSS 事務局

（東京都港区西新橋 2-14-1 興和西新橋ビル B 棟 16 階　1604 号）

内容：①第 1 回 Steering　Board 会議議事録の確認

②前回の課題の検討状況について

・テーマ 1 の機能と役割分担の整理

・テーマ 3 の機器の障害時対応の整理

・可搬型リーダライタの検討

③各テーマの進捗状況について

④今後の予定について

・課題の整理

・推進委員会について

・次回 Steering　Board 会議について

第 3 回　Steering　Board 会議

日程：平成 16 年 12 月 24 日（金）

場所：財団法人ニューメディア開発協会　24 階　会議室

（東京都港区三田 1 丁目 4 番 28 号　三田国際ビル 24 階）

内容：①前回の課題の検討状況について

・テーマ 1 の機能と役割分担の整理

②今後の予定について

・推進委員会について

第 4 回　Steering　Board 会議

日程：平成 17 年 2 月 8 日（火）

場所：NICSS 事務局

（東京都港区西新橋 2-14-1 興和西新橋ビル B 棟 16 階　1604 号）

内容：①テーマ 1

・実証実験の概要について

・方式検討状況について

②テーマ 2

・実証実験の概要について

・来年度の検討について

③テーマ 3

・実証実験の概要について

・来年度の検討について

第 5 回 Steering　Board 会議

日程：平成 17 年 3 月 7 日（月）

場所：NICSS 事務局

（東京都港区西新橋 2-14-1 興和西新橋ビル B 棟 16 階　1604 号）

内容：①実証実験の結果について

②テーマ 1 の機器登録方式について

③報告書の目次案について

④来年度に向けて

2．4　工程管理業務

本事業では、事業スケジュール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 1：多機能 IC チップ等を活用したサービスを提供するための基盤となる登録センタ機能の研究開発及び実証実験

②テーマ 2：登録センタの機能を活用したデジタルコンテンツ流通サービスの研究開発及び実証実験

③テーマ 3：登録センタの機能を活用した医療システム機器等のリモートサービスの研究開発及び実証実験

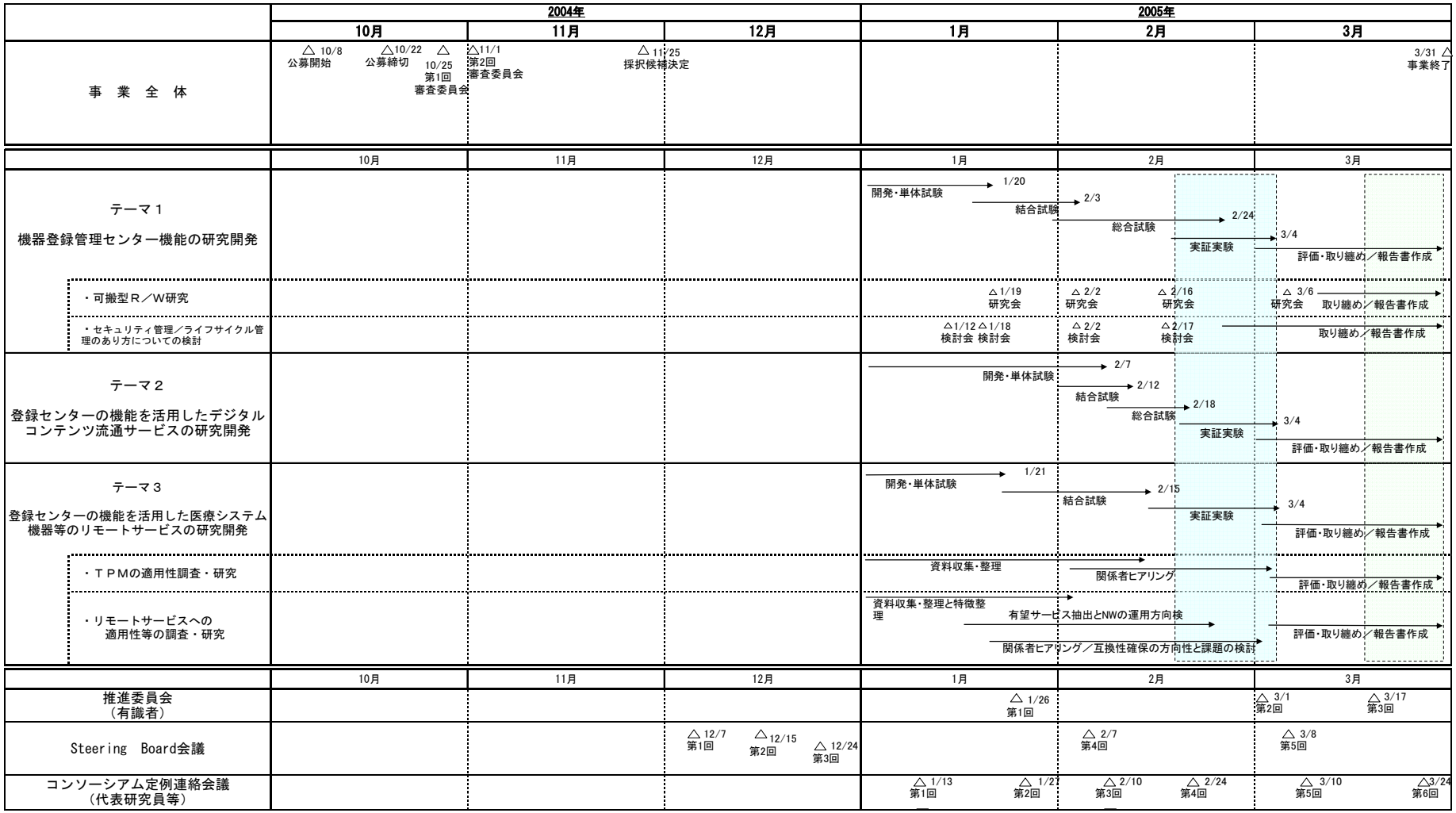
当協会では、本事業の進捗管理を行うために、隔週木曜日にコンソーシアム定例連絡会議を設置し、「スケジュール管理」、「実施内容の確認」及び「課題の有無、解決状況の確認」を行った。このコンソーシアム定例連絡会議は、事業期間中に合計 6 回、当協会の会議室において実施した。

その結果、本事業は表 2-2 に示す事業スケジュールのとおり実施された。

2．4．2　その他工程管理業務

上記コンソーシアム定例連絡会議の他に、Steering　Board 会議または推進委員会の円滑な進行を目的に同会議・同委員会前を中心に随時、コンソーシアムとの課題の検討等の打合せを実施した。

表２−２　事業スケジュール



第Ⅱ編

研究開発・実証実験の実施報告

Ⅱ－1
テーマ 1

多機能 IC チップ等を活用したサービスを提供するための基盤となる登録センタ機能の研究開発及び実証実験

1. 事業概要

1. 1　背景

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)」では、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を「多機能 IC チップフレームワーク要件書」として取りまとめた。また事業の一環として、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ならびに実効性検証も併せて行った。

具体的には、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、著作権者や著作隣接権利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マルチメディア情報流通サービスにおける基本機能について研究開発した。そして、アプリケーション開発を通じての実効性検証を行うことにより、多機能 IC チップフレームワークを基盤としたマルチメディア情報流通サービスの適用可能性の高さが確認できた。

また、同じく経済産業省が実施した平成 15 年度「情報経済基盤整備事業（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）」では、多機能 IC チップを搭載した医療システム機器に対するリモートメンテナンスの実効性確認を行った。ここでは、IC カードと多機能 IC チップ搭載医療システム機器を利用して、人と機器とを識別し、第三者による不正アクセスを防止するのはもちろんのこと、保守作業者が確実に対象となる機器に接続することができ、かつ対象以外の機器には接続することができない安全なリモートメンテナンスを実現した。

一方で、具体的なサービスの実現に向けては、実際の機器への多機能 IC チップの搭載を含む、より実環境に近い形での実証と多機能 IC チップの破損や紛失の際の再発行といった実サービスを想定した機能拡張の必要性等が課題として指摘されている。

1. 2　目的

多機能 IC チップ等を活用したサービスを提供するための基盤となる機器登録管理センタ機能の研究開発及び実証実験（以下「テーマ 1」という。）を行った。

具体的には、サービスを実現するためのシステム（機能）として、機器登録管理センタの機能である多機能 IC チップ登録機能をサーバ上に実装し、多機能 IC チップの登録処理が可能であることを確認した。

またテーマ 1 で実装した機器登録管理センタをデジタルコンテンツ流通サービスの研究開発及び実証実験（以下「テーマ 2」という。）及び、医療システム機器等のリモートサービスの研究開発及び実証実験（以下「テーマ 3」という。）で実際に活用することにより、多機能 IC チップ搭載型デジタルコンテンツ再生機器や、多機能 IC チップ搭載型医療システム機器等が機器登録管理センタに機器登録され、機器登録処理後に音楽の再生や医療システム機器

保有データの転送等のサービスが実際に利用可能であることを確認した。

加えて、ネットワーク接続機能を持たない多機能 IC チップ搭載機器と連携して機器登録、AP 追加・AP 削除等を行うための可搬型リーダライタと、多機能 IC チップ搭載機器のセキュリティ機構及びライフサイクル管理のあり方について調査研究した。

これらの研究開発や調査研究を通じた成果を活用し、多機能 IC チップ等を活用したサービスシステムの基盤を整備することを本テーマの目的とした。

1．3　実施概要

テーマ 1 の実施概要について以下に記述する。

1．3．1　機器登録管理センタの機器登録機能の研究開発と実証実験

多機能 IC チップが搭載された機器によるサービス実施において必要となる機器登録管理センタ機能の研究開発を行い、テーマ 2、テーマ 3 で利用する各多機能 IC チップ搭載機器の登録・運用管理を行うことにより機能的な検証を行った。（以下「テーマ 1-1」という。）

1．3．2　可搬型リーダライタの研究

ネットワーク接続機能を持たない多機能 IC チップ搭載機器と連携して機器登録、AP 追加、AP 削除等を行うための可搬型リーダライタについて調査研究した。（以下「テーマ 1-2」という。）

1．3．3　多機能 IC チップ搭載機器のセキュリティ機構やライフサイクル管理のあり方に関する研究

多機能 IC チップの認証によって搭載機器の安全を信頼できるとするための機器に対するセキュリティ機構のあり方や、機器の修理や譲渡、中古品流通といった流れを含む多機能 IC チップ搭載機器のライフサイクル管理のあり方について調査研究した。またそれらの検討を踏まえ、多機能 IC チップ搭載機器の管理における NICSS フレームワーク関連技術の応用可能性を整理した。（以下「テーマ 1-3」という。）

1．4　実施体制

テーマ 1 の実施体制を図 1-1に示す。

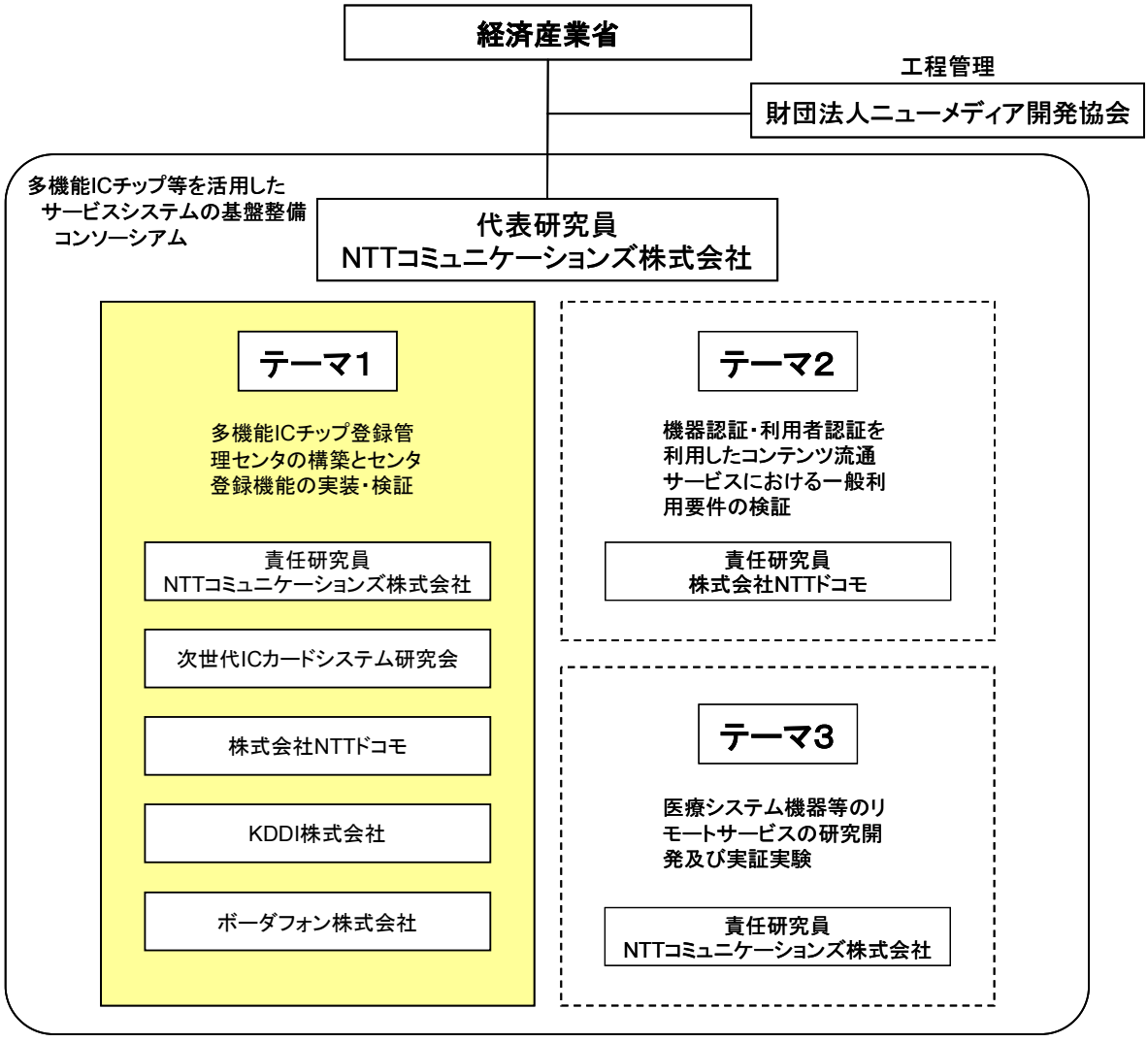


図 1-1　実施体制図

2. 多機能 IC チップフレームワークについて

2. 1　昨年度実証事業の成果と今年度の目標

昨年度の実証事業においては、利用者の手元に渡る前に、機器製造者が機器登録管理センタへ多機能 IC チップ搭載機器の機器登録を行う登録形態（既存の IC カードと同様の手順、以下「事前登録」という。）としていた。また、機器に組み込むべき多機能 IC チップも実在していなかったため、機器に IC カードを挿入した IC カードリーダライタをつなぐことで多機能 IC チップ搭載機器を実現していた。しかし、多機能 IC チップフレームワークでも指摘されているように、機器は IC カードと異なり、通常、機器を購入する直前まで利用者が決まっていないため、利用者の手元に渡った後に登録できる形態（以下「事後登録」という。）が望まれる。そこで今年度の実証事業では、利用者が機器保有後（購入後）に多機能 IC チップ搭載機器を機器登録できる機能を実装した機器登録管理センタを構築することを目標とした。

また、機器の事後登録に際して、多機能 IC チップフレームワークの基本要件をもとに想定される脅威を検討し、正当な多機能 IC チップが正当な機器登録管理センタへ登録されることを確実とした機能の実現を目指した。

このほかに今年度の実証事業では以下の点も考慮した。

IC カードに使われているものと同等の IC チップをパッケージ化した多機能 IC チップ（図 2-1）を実際に組み込んだ機器を用いることにより、昨年度のように IC カードを代用していては分からない、機器それぞれに適した登録の方法について考察した。

多機能 IC チップフレームワークの目的の 1 つである、さまざまな業界分野がこの基盤に参加できることを示すため、全く異なったサービスであるテーマ 2：コンテンツ流通と、テーマ 3：医療リモートサービスに対して、それぞれで用いられる機器を共通の機器登録管理センタに登録できることを示した。

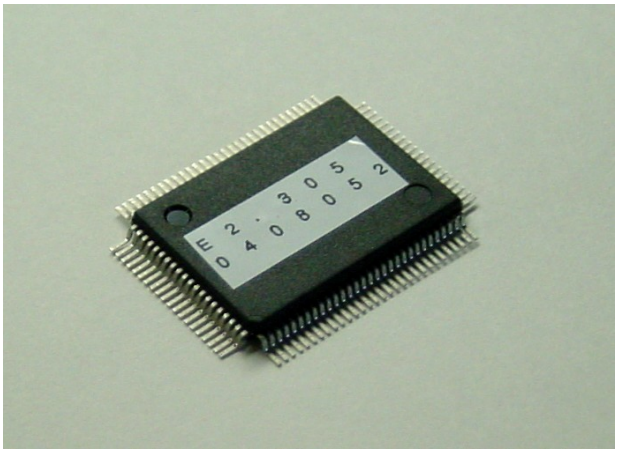


図 2-1　パッケージ化多機能 IC チップ

2. 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場合がある。

- AP（Application）：アプリケーション
- AID（Application Identifier）：アプリケーション識別子
- API（Application Program Interface）：アプリケーションプログラムインタフェース
- AP_ID（Application　Program Identifier）：アプリケーションプログラム識別子
- APP（AP Provider）：アプリケーションプロバイダ
- CA（Certificate Autnority）：認証局
- CH（CH：Chip embedded equipment Holder）：保有者（利用者）
- CM（Chip Manager）：チップマネージャ
- CR（Chip embedded equipment Registry）：機器登録管理センタ
- CS（Chip Supplier）：IC チップ供給者
- EM（Equipment Maker）：機器製造者
- NICE（Network-based IC Card Environment）：IC カード発行管理システム
- 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
- 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

3. 機器登録管理センタの機器登録機能の研究開発と実証実験

3. 1　研究開発の概要

本節では、テーマ 1 の 3 つのサブテーマのうち、テーマ 1-1 における研究開発の概要について記述する。

3. 1. 1　研究開発の内容

前章で紹介したように、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)」では、多機能 IC チップフレームワークが研究された。そして、多機能 IC チップの登録やその運用状況を管理する機器登録管理センタに対して、新たに機器登録処理が規定された。この機器登録機能は、多機能 IC チップを搭載したさまざまな機器の正当性を担保する基盤を提供するための機能である。

2 つの機器登録方法である「事前登録」と「事後登録」は、それぞれ機器の性格に合わせて使い分けされると考えられる。つまり、高額医療機器のように受注生産される機器や、あらかじめ利用者が特定さている IC カード（ここでは IC カードも機器の一種と見なす）のように、利用前から利用者を特定できる機器の場合は、「事前登録」により登録され、デジタルコンテンツ再生機器やネットワーク機器、IC チップ内蔵メモリ媒体などの比較的低額で小売店にて販売される機器のように、大量に生産され、かつ、あらかじめ保有者を特定できない機器の場合は、「事後登録」により登録されるであろう。どちらの機器登録も、現実的な方法なので、開発する機器登録管理センタは両方の登録方法をサポートする必要がある。前述したとおり、事前登録は IC カードの発行手順と同じで、既存の IC カード発行・管理システムと同等の機能を機器登録管理センタが有していれば実現できる。しかし、事後登録については、既存の IC カード発行・管理システムではこのような登録が想定されていないため、IC カード発行・管理システムの機能を拡張して、機器登録管理センタの機能として事後登録機能を追加する必要がある。

テーマ 1-1 では、機器登録管理センタの事業化及び多機能 IC チップ搭載機器によるサービスの事業化に向けた基盤整備を行うため、上記の課題を見据えて機器登録管理センタの機器登録機能を研究開発し、テーマ 2、3 で利用する機器の機器登録に利用することにより機能的な実証を行った。

3．1．2　本研究開発におけるポイント

本研究開発におけるポイントを以下に示す。

- 機器登録管理センタの構築と、多機能 IC チップ搭載機器の事後登録機能の実装を行う。機器登録におけるポイントは、複数のサービスの共通基盤となるように、1 つの機器登録管理センタでテーマ 2 とテーマ 3 で利用する全く異なる機器を登録する点にある。事後登録を行う機器は、テーマ 2 で利用するデジタルコンテンツ再生機器と多機能 IC チップ搭載携帯電話、それにテーマ 3 で利用するネットワーク機器である。また、利用者の認証用等に用いる IC カードなどは事前登録とする。
- 事後登録が安全に行われる仕組み、機器の事後登録の際に、機器登録管理センタと多機能 IC チップ搭載機器における相互認証を行う。相互認証により、機器登録管理センタの正当性と多機能 IC チップ搭載機器の正当性を確保した後、機器登録を実施する仕組みとした。
- 製造者課金モデルに対応できるように、多機能 IC チップ内に格納された機器製造者情報（機器製造者名、機器型番、製造番号など）を読み出し、機器登録管理センタで登録・管理が可能な実装とした。
- 登録の仕方が機器の種類に大きく依存しないよう、機器登録操作をできるだけ共通化・簡単化することで、利用者の利便性を損なわないように配慮した。
- 多機能 IC チップのパッケージ化を行い、テーマ 2 において使用するデジタルコンテンツ再生機器、テーマ 3 で使用するネットワーク機器への組み込みを行った。

3．1．3　実証事業のスコープ

今年度実証事業における多機能 IC チップフレームワークでのポイントは下記の 4 つ。

- CM、仮鍵、仮証明書は EM ではなく CS がチップに格納する
- EM と SP とは密接に関連している場合がある
- CR はさまざまな機器に対応するが、EM の製造するすべての機器について、その機能、性能や搭載サービスの詳細を知り、機器全体の安全性に責任を持つ必要はない
- CR による EM へのチップ管理料課金を可能にする

3．1．4　他のテーマとのかかわり

テーマ 1-1 では、異なるサービスに供される機器を登録可能な多機能 IC チップフレームワークで実現し、テーマ 2、テーマ 3 で使用する機器の登録を行う。それぞれのテーマでは、多機能 IC チップを搭載した機器を用いることにより、機器認証を確実にしたクオリティやセキュリティの高いサービスを提供することを目的としている。

具体的には、テーマ 2 では、テーマ 1-1 で構築した機器登録管理センタに多機能 IC チップ搭載デジタルコンテンツ再生機器を事後登録し、その機器を使って著作権物であるコンテンツを安心して流通できるサービスを実現した。

テーマ 3 では、テーマ 1-1 で構築した機器登録管理センタに多機能 IC チップ搭載ネットワーク機器を事後登録し、その機器を使ってリモートサービスの一環として医療システム機器の運用保守情報をインターネット VPN で安心してやりとりするサービスを実現した。

なお、各サービスの具体的な内容については、各テーマの報告書を参照のこと。

3. 2　実証実験の環境

3. 2. 1　概要

テーマ 1-1 の実証実験は、テーマ 2 とテーマ 3 の実証実験の環境において、テーマ 2 及びテーマ 3 で利用する多機能 IC チップ搭載機器を登録するという形で実施された。

（1）実施概要

テーマ 1-1 における実証実験の実施は、テーマ 2 及びテーマ 3 のシナリオに組み込まれた形で行われたため、それぞれのテーマと共通の実証実験環境で行われた。テーマ 2 に関連した機器登録の実証実験は市ヶ谷の Dali インターナショナル（株）に設置された実証実験会場で行った。また、テーマ 3 に関連した機器登録の実証実験については、竹橋の NTT コミュニケーションズ（株）に設置された実証実験会場で行われた。機器登録管理センタの実体であるサーバは、竹橋の実証実験会場にあるサーバルームに設置された。

（2）実証実験のシナリオ

テーマ 1-1 における実証実験のシナリオは、テーマ 2 及びテーマ 3 の実証実験の環境に合わせて実施するため、以下の 2 種類がある。

（ア）テーマ 2 の実証実験環境での実証実験シナリオ

テーマ 2 におけるテーマ 1 の実証実験の実施概要を、表 3-1に示す。

表 3-1　テーマ 2 に関するテーマ 1-1 の実証実験シナリオ

流れ	項目	内容
準備作業	実験機器の初期化	機器の事後登録直前まで準備が実施された状態でデモを開始。
被験者への事前説明	機器登録のねらい	機器登録により信用できる機器を使ったコンテンツ配信サービスが実施できることを説明。
機器登録の実施	操作説明	リモコン操作、画面の説明。
	被験者による機器登録作業	実際にリモコンを使って、機器の登録を行う。
アンケートとヒアリング	利用者向け	全員に実施。
	権利者向け	該当者に実施。
	事業者向け	該当者に実施。

（イ）テーマ 3 の実証実験環境での実証実験シナリオ

テーマ 3 の実証実験の実施概要を、表 3-2に示す。

表3-2　テーマ 3 に関するテーマ 1-1 の実証実験シナリオ

流れ	項目	内容
準備作業	実験機器の初期化	機器の事後登録直前までの準備が実施された状態でデモを開始（IP アドレスなどは設定済み)。
被験者への事前説明	機器登録のねらい	機器登録により、信用できる機器で安心できるリモートサービスが実施できることを説明。
	シナリオ説明	医療機関に機器が 1 台追加されたことによる機器登録作業の発生。
機器登録の実施	操作説明	管理端末の操作、画面の説明
	被験者による機器登録作業	実際に設定用 PC 端末を使って、機器の登録を行う。
アンケートとヒアリング	機器ベンダ	該当者に実施。

(3) 被験者の内訳

実証実験に参加した被験者の内訳を表 3-3に示す。

表3-3　テーマ 1-1 に関する被験者の内訳

分類		被験者数
テーマ 2	コンテンツ事業者	30 人
	コンテンツ権利者	13 人
	その他	1 人
テーマ 3	医療機器ベンダ	3 人
合計		47 人

3. 2. 2　システム構成

(1) 実証実験の検証環境の全体図

実証実験システムの全体構成を図 3-1に示す。機器登録管理センタサーバは、テーマ 2、テーマ 3 に共通して利用される。それぞれのサービスで用いられるサーバ（コンテンツ流通で用いるポイント管理・コンテンツ配信サーバと医療リモートサービスで用いる認証接続管理サーバ）は、それぞれ別のサーバ筐体に実装されており、設置場所もそれぞれ異なる。これらのサーバと、機器を配置した実証実験場とは ADSL 回線を使ったインターネットで接続した。

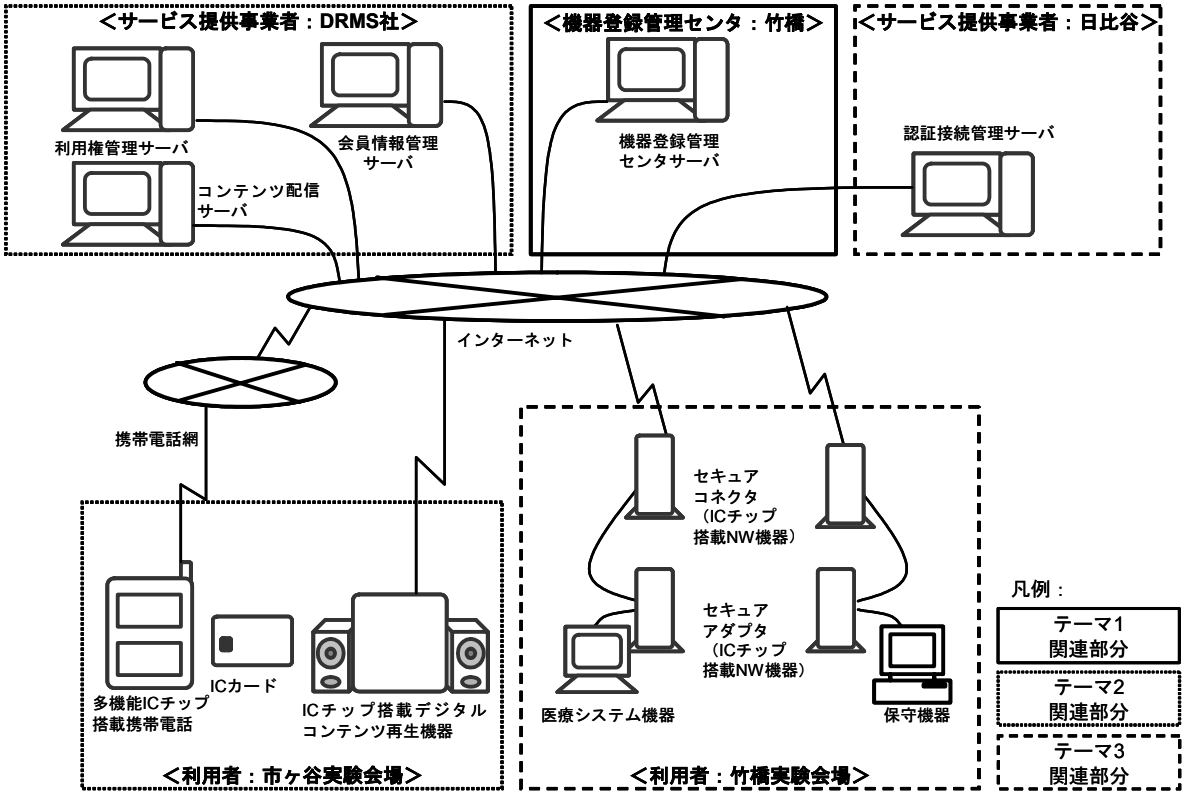


図3-1　実証実験システムの全体構図

(2) 機器登録管理センタのシステム構成

図 3-2に、テーマ 1 の実証実験となる機器登録管理センタのシステム構成を示す。機器登録管理センタサーバには、RC としての登録認定機関 AP、機器登録管理センタとしてのチップの発行管理システム、機器登録 AP の他に、コンテンツ流通及び医療リモートサービスにおけるサービスプロバイダが提供するチップ AP のダウンロード管理をする AP 管理システムと AP ダウンロード FEP を同一サーバ筐体に実装した。

機器登録の対象となる機器は、デジタルコンテンツ再生機器、ネットワーク機器、IC カード、それに IC チップ搭載携帯電話である。デジタルコンテンツ再生機器とネットワーク機器はサービスを提供するための機器であり、これらの機器に搭載された多機能 IC チップは接触 IF（ISO/IEC 7816）による通信を行う。また、IC カードと IC チップ搭載携帯電話は利用者認証等に利用する機器であり、これらは非接触 IF（ISO/IEC 14443 TypeB）にて通信を行う。

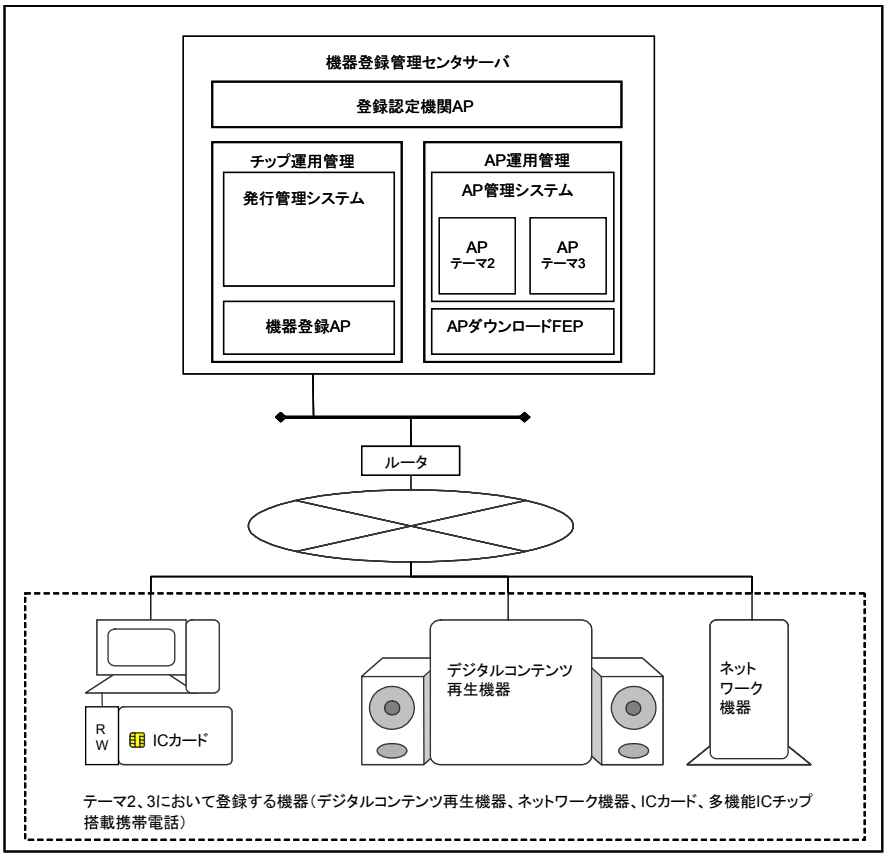


図3-2　実証実験環境

機器登録管理センタサーバにおいて新規に開発したソフトウェアについて、表 3-4 に示す。

表3-4　機器登録管理センタサーバの新規に開発したソフトウェア

項番		アプリケーション名／機能	概要
1		機器登録 AP	多機能 IC チップ搭載機器の機器登録管理センタへの事後登録を行う。
	1-1	登録機器 IF 機能	チップを搭載した各種機器に対する登録要求の受付・制御を行う。
	1-2	相互認証機能	機器登録管理センタと、事後登録要求を行う機器との間で、仮鍵を利用して相互認証を行う。
	1-3	機器情報登録機能	機器情報（製造者、型番、製造番号等）を機器から取得し、機器登録管理センタに登録する。
	1-4	事後登録用多機能 IC チップ書込機能	CM 鍵ペア、機器（CM）証明書を事後登録の結果として機器へ書き込む。
2		AP ダウンロード FEP	事後登録後のチップ搭載機器にチップ AP をダウンロードする際に、AP 管理システムと機器の間に入り、処理の媒介を行う。

(3) デジタルコンテンツ再生機器の構成

デジタルコンテンツ再生機器において、新規に開発したソフトウェアについて、表3-5に示す。

表3-5　デジタルコンテンツ再生機器の新規に開発したソフトウェア

項番	アプリケーション名	概要
1	機器登録 AP	Web ベースの機器登録をリモコンから行うためのアプリケーション。
2	初期化ツール	搭載された多機能 IC チップを事後登録前の状態に戻すツール。
3	利用者認証 AP	IC カード／多機能 IC チップ搭載携帯電話を使って利用者を認証するためのチップ AP。
4	ログ AP	曲を聴いた回数を管理するためのチップ AP。
5	ミュージックプレーヤ AP	テーマ 2 のサーバと連携して、利用者の認証により暗号化音楽情報を復号して、音楽を再生するプログラム。

（4）セキュアアダプタ／セキュアコネクタの構成

ネットワーク機器であるセキュアコネクタ／セキュアアダプタにおいて、新規に開発したソフトウェアについて、表 3-6に示す。

表3-6　セキュアコネクタ／セキュアアダプタの新規に開発したソフトウェア

項番	アプリケーション名	概要
1	機器登録 AP	Web ベースの機器登録を、代理の設定端末（管理端末）から行うためのアプリケーション。既存の認証接続管理 AP の初期化シーケンスに組み込む形で実装。
2	初期化ツール	搭載された多機能 IC チップを事後登録前の状態に戻すツール。

3. 2. 3　機器登録のシーケンス

機器登録管理サーバと多機能 IC チップ搭載機器との間で行う機器登録の形態は、デジタルコンテンツ再生機器（テーマ 2）の場合とネットワーク機器（テーマ 3）の場合の 2 通りあるが、入出力機器に差があるものの登録のシーケンスや登録画面のデザインを共通化し、リスト選択とボタン押下のみの簡単な操作で機器登録ができる仕組みとした。

デジタルコンテンツ再生機器（テーマ 2）から登録する場合は、機器のビデオ出力をテレビ画面で見ながらリモコンを使って機器登録を行う。また、ネットワーク機器（テーマ 3）から登録する場合は、ネットワーク機器に LAN 内の設定用端末からアクセスして、ブラウザを使って機器登録を行った。

以下の表に利用者が実際に行う機器登録作業を示す。

表3-7　機器登録作業の流れ

手順	処理	概要
1	機器登録開始処理	機器登録処理を開始し、機器登録開始画面を表示する。
2	機器登録チェック処理	機器登録済であるかを確認する。
3	機器登録管理センタ選択処理	機器登録管理センタを選択する。 今回の実証試験の環境では、3 つのセンタを登録している。
4	登録作業進捗確認処理 1	機器登録申請にあたって、機器登録管理センタと搭載多機能 IC チップの正当性について相互認証を行う。
5	登録作業進捗確認処理 2	機器登録管理センタに機器情報を登録し、チップに CID（機器登録 ID)、CM 鍵、CM 鍵証明書を設定する。
6	AP 使用許諾処理	AP がダウンロードされる前の使用許諾の確認をする。
7	登録作業進捗確認処理 3	送信されたダウンロード情報をもとにサービスに必要なチップ AP のダウンロードを行う。
8	登録作業進捗確認処理 4	AP のダウンロード処理を終了する。
9	機器登録完了処理	機器登録を完了する。
_	サポートヘルプ処理	異常で機器登録に失敗した際に表示する。

手順 3、手順 4 に該当する表示画面を以下の図 3-3、図 3-4に示す。

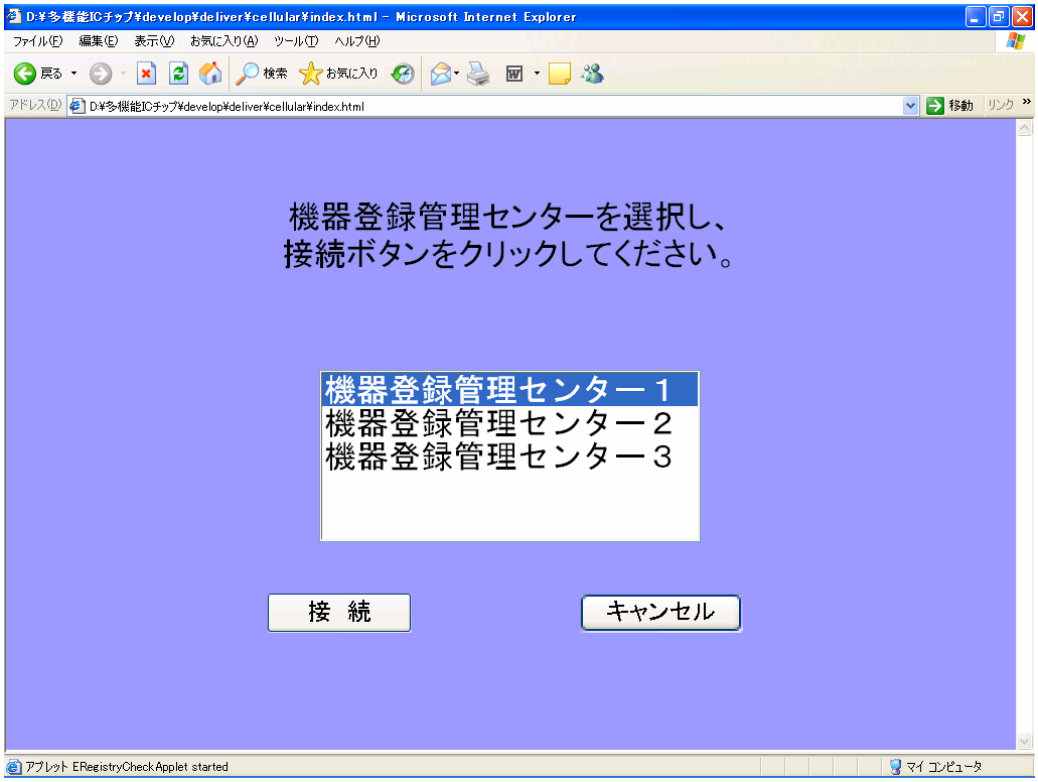


図3-3　機器登録管理センタ選択画面

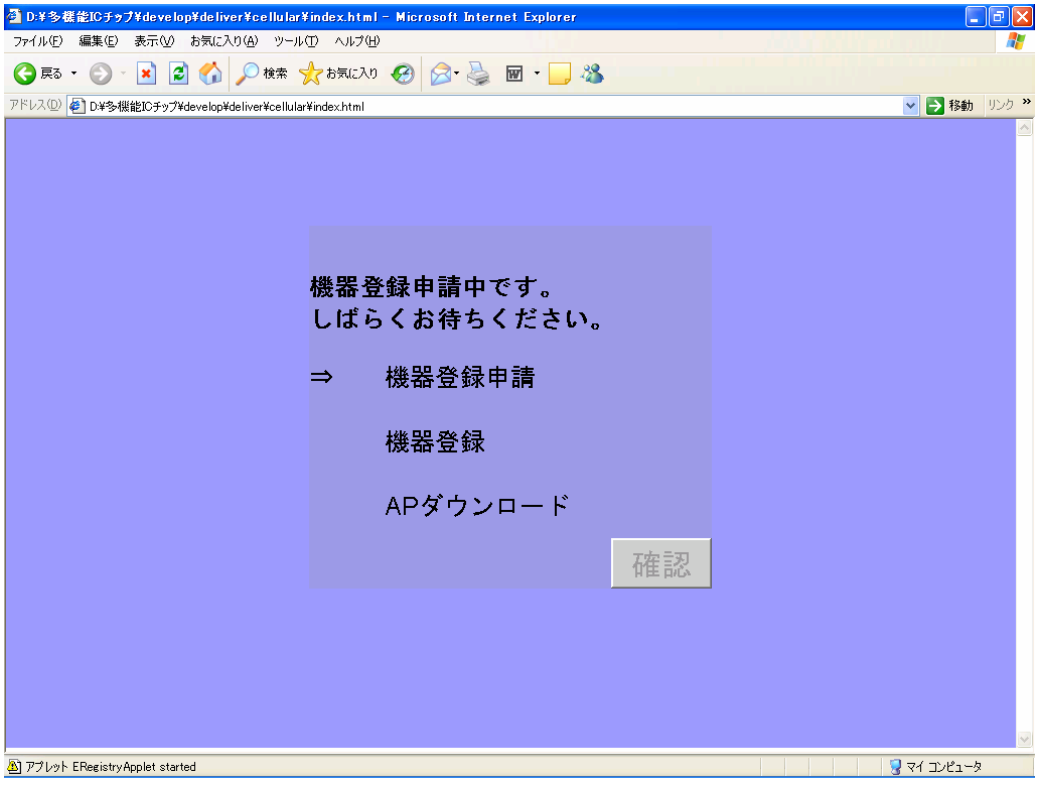


図3-4　登録作業進捗確認画面 1

3．3　実証実験の環境

3．3．1　事後登録機能を中心とした機器登録管理センタの機能検証

事後登録機能が、多機能 IC チップフレームワーク要件書で想定された脅威等に対して有効な対策を有しているか、本フレームワークを実際のサービスとして事業展開する際に、利便性や課金形態の多様性を確保するための基盤となる機能を有しているかについて、設計検証及び動作確認を行った。

(1) 検証方法

実証実験での動作検証、及び検証すべき要件について設計検証を行った。

(2) 検証項目

事後登録の登録形態を実現するために要求される要件には、以下の項目がある。本検証では、機器登録管理センタに対するこれらの要件について、設計検証及び実装システムの動作確認による機能検証を行う。

(a) 事前登録と事後登録の両方に対応すること

(b) 利用者の操作を極力簡便にすること

(c) 複数の CR を選択できること

(d) 事後登録に伴うセキュリティ脅威への対応をすること

想定される下記のセキュリティ脅威に対策を講じる。

- チップ内の格納情報の改ざん
- 不正な機器（チップ）の登録
- 不正な CR に対する登録
- 不正な利用者情報による登録
- 不正な EM または利用者の希望する以外のサービス提供者（SP）からのアプリケーション追加

(e) 機器製造者課金に必要な仕組みを持つこと

(f) さまざまな機器に対応する登録インタフェースを持つこと

テーマ 2、3 で利用する下記の機器に対応する。

- デジタルコンテンツ再生機器（事後登録）
- 医療システム機器（事後登録）
- 非接触 IC チップ搭載携帯電話機（事後登録）
- IC カード（事前登録）

3. 3. 2　事後登録機能のユーザビリティに関する検証

機器登録の被験者を対象として、登録機能のユーザビリティを評価するために、アンケート票、ヒアリングシートを作成し、被験者に対して実施した。なお、テーマ 1 のアンケートやヒアリングは単独では行わず、各テーマのアンケートやヒアリングの中にテーマ 1 の設問を追加する形で実施した。

(1) 検証方法

テーマ 2、3 の被験者に事後登録作業を見学・実施してもらい、その後、機器の事後登録機能に関する使いやすさや、操作に対するレスポンスなどについてアンケートやヒアリングを行った。ここでは被験者に利用者の立場からの回答を得るため、一般ユーザ（機器を利用する人）＝利用者になったつもりで回答してもらった。

(2) アンケート項目

主なアンケート項目は次の 3 つとし、各項目に数点の質問を設けた。

・機器登録の手続・操作について
・機器登録により提供されるサービスについて
・登録費用の支払い方について

(3) ヒアリング内容

ヒアリングはアンケート後にアンケート内容を補足する形で行った。主な質問内容は機器各種の手続・操作についてとし、状況に応じて適宜、質問の内容や問い方を変えながら進めた。

3. 3. 3　機器登録管理センタの運営にかかわる意識調査

機器登録管理センタの運営形態を検討するにあたり、テーマ 2、3 の被験者に対して、事業者、コンテンツ権利者の立場でアンケートやヒアリングを行い、期待される機器登録料の徴収方法や運営主体に関する意識調査を行った。

(1) 検証方法

前出のテーマ 2、3 の被験者に対して、所属する会社や団体により事業者、権利者に分類し、それぞれの立場から、課金方法や運営主体についてアンケートやヒアリングを行った。

(2) アンケート項目

以下の項目についてアンケートを実施した。なお、テーマ 1 のアンケートは単独では行わず、各テーマのアンケートの中にテーマ 1 の設問を追加する形で行った。

・機器登録管理センタの運営主体について
・機器登録料の課金方法について（事業者のみを対象とする）

(3) ヒアリング内容

ヒアリングはアンケート後にアンケート内容を補足する形で行い、状況に応じて、適宜、質問の内容や問い方を変えながら進めた。

3．4　検証結果

3．4．1　機器登録管理センタの検証

今年度の機器登録管理センタ（CR）サーバシステムの開発にあたっては、既存の NICSS フレームワーク準拠製品である NTT コミュニケーションズ株式会社製の NICE システムを活用し、NICE 発行者サーバシステム（Card Issuer：CI）へ新規開発により機能追加することで多機能 IC チップフレームワークに準拠する CR の実装を行った。

3．3で挙げた、事後登録の登録形態を実現するための要件に対して、今年度の実装でどのような対策を実施しているかについて、以下の動作検証及び設計検証により検証を行った。

(a) 事前登録と事後登録に対応すること

テーマ 2、3 で利用する機器としては、前述のとおり多機能 IC チップが搭載された①デジタルコンテンツ再生機器、②ネットワーク機器、③利用者認証機器（携帯電話）、④利用者認証機器（個人認証用 IC カード）があるが、①～③については事後登録により登録し、④については事前登録により登録を行った。これらはすべて同じ CR サーバシステムに登録され、それぞれの機器に対応したチップ AP を搭載後、テーマ 2、3 のサービスに利用することにより正常な動作が確認された。

(b) 利用者の操作を極力簡便にすること

今年度の実装では、デジタルコンテンツ再生機器については機器自体を、その他の機器については外部接続された登録用 PC を利用して事後登録を行うこととした。これらの登録用端末のオペレーションシステム等はさまざまなものが想定されるが、今後のネットワーク対応を考えれば、これらの機器システムがサーバからブラウジングしたスクリプトプログラムを実行可能な汎用 HTTP ブラウザ機能を有していると想定することが現実的だと考えられる。

このため、今年度は汎用ブラウザ（Microsoft 社の Internet Explorer を利用）と Java アプレットを用いて登録処理を実装し、基本的にマウス、リモコンによる操作のみにより簡便な登録処理ができる仕組みを実現した。

(c) 複数の CR を選択できること

本来、機器チップを管理する CR は、完全に自由な利用者意思によって決定されるべきであるが、入出力デバイスとして十分なものを想定できないため、任意の URL 入力による選択ではなく、あらかじめ機器に格納された HTML ファイルからプルダウンメニューにより選択する形態で実装し、複数の CR を選択可能とした。ここで問題となるのは、EM が機器に格納する当該 HTML ファイルに記載される CR と EM との関係の整理と、当該ファイルの改ざんリスクとなる。前者については、機器の種別によって業界団体等が設立した CR や、提携契約を行った CR を記載することは、機器製造者として自然であると考える。例えば PC を購入すると、提携した ISP への申し込みサイトへのリンクが張られたアイコンがプレインストールされている場合が多いが、これと同様の形式と考えられる。また後者に関しては、当該ファイルへの EM の電子署名を付けるなどの対策が考えられるが、今年度は未実装とした。

(d) 事後登録に伴うセキュリティ脅威への対応

今年度のシステムでは、以下の対策を行った。

- CS は、仮鍵、仮証明書（仮鍵に対して CS が発行する証明書)、CS 証明書（CS 鍵に対する登録認定機関（RC）の証明書)、RC 公開鍵を出荷時にチップ内に格納する。仮鍵、仮証明書は、登録により正式な CM 鍵、CM 証明書が格納されることにより無効化する。チップへの書き込み権限は RC をルートとする外部認証により与える。
- EM は、仮鍵による RC をルートとする内部認証により、多機能 IC チップフレームワーク準拠のチップであることを確認する。また、チップに対して RC をルートとする外部認証により書き込み権限を得て、EM の電子署名付きの機器情報（製造者 ID、機器型番、製造番号）と、基本機能の動作に必要な必須チップ AP の AP ダウンロード情報リスト（SP の URL、SPID、APID）を格納する。
- CR は、仮鍵による RC をルートとする内部認証により、多機能 IC チップフレームワーク準拠のチップであることを確認する。また、チップに対して RC をルートとする外部認証により書き込み権限を得て、CM 鍵、CM 証明書を格納する。また、EM の電子署名付きの機器情報（製造者 ID、機器型番、製造番号）を確認し、チップごとに管理する。また、チップ内に格納された AP ダウンロード情報リスト（SP の URL、SPID、APID）をもとに、AP ダウンロード処理を行う。
- SP は、EM の電子署名付きの機器情報（製造者 ID、機器型番、製造番号）を確認し、自らのサービスを搭載可能な安全性を有する機器であることを確認し（未実装)、AP ダウンロード処理を行う。

これにより、3. 3で挙げたセキュリティ脅威について表 3-8 のように対策が施されている。

表3-8　セキュリティ脅威とその対策

セキュリティ脅威	対策
チップ内の格納情報の改ざん	外部認証による書き込み権限確認。
不正な機器（チップ）の登録	仮証明書によるチップの内部認証・正当性確認、EM の署名付き機器情報。
不正な CR に対する登録	チップに対する CR 証明書による外部認証。
不正な利用者情報による登録	＜保有者登録は未実装＞
不正な（EM または利用者の希望する以外の）サービス提供者（SP）からのアプリケーション追加	AP ダウンロード情報による SP 指定、チップに対する SP 証明書による外部認証。

（e）機器製造者課金を実現すること

CR は、EM の電子署名付きの機器情報（製造者 ID、機器型番、製造番号）を確認し、チップごとに管理することにより機器製造者を特定し、課金可能となる。

ただし、実際の課金システムは、今年度は未実装とした。

（f）さまざまな機器に対応する登録インタフェース

今年度の実装では、各機器がスクリプトプログラムを実行可能な汎用 HTTP ブラウザ機能を有していることを想定し、CR からダウンロードされる Java アプレットを用いて登録処理を行なっている。

多機能 IC チップフレームワークに準拠する限り、基本的に個別の詳細な登録プロトコルは CR によるものと考えられるが、アプレットを CR の所有とすることにより、どの CR を選択しても機器側に影響が出ない仕組みとしている。

CR 側では、すべての機器に対して同じアプレットを用いることにより、さまざまな機器で処理を変えることなく登録を行える仕組みとしている。

また、この登録用アプレットは、チップ内から読み出した AP ダウンロード情報リストをもとに、逐次該当する SP への接続を行ない、SP からダウンロードした AP ダウンロード用アプレットによってチップ AP がダウンロードされる仕組みとしている。

3．4．2　事後登録機能のユーザビリティに関する検証

機器登録の体験者を対象としたアンケートにより、登録機能のユーザビリティに対する以下の検証項目について意見を収集した。

・機器登録の手続・操作について
・機器登録により提供されるサービスについて
・登録費用の支払い方について

さらに、ヒアリングにより、登録処理における操作感等、全般的な意見を収集した。

(1) 機器登録の手続・操作について

本システムを操作した被験者へのアンケートで、「処理手順のわかりやすさに対する評価」、「レスポンス時間に対する評価」、「機器登録全般に対する評価」を行った。

【処理手順のわかりやすさ】

処理手順の分かりやすさについては、肯定的・否定的意見がほぼ半数に分かれている。しかし、どちらともいえないという意見も 3 割を占めていることや、“そう思わない”や“とてもそう思う”のような強い意見が少数であることを見ると、積極的に肯定するわけでも、否定するわけでもない様子が見受けられた。ヒアリングの意見でも、「操作は分かりやすかった。」という意見がある反面、「利用者から見ると何をしているのかわからない。」という意見も多く、被験者の多くが、操作性そのものを評価しているというより機器登録という行為そのものを、サービスを受ける上で必要な操作であるものの理解しにくいと感じた結果と思われる。

【レスポンス時間】

この時間については、過半数を超える利用者が、不満を感じている。特に最も時間がかかる AP ダウンロードは画面の遷移がないので、ユーザは時間を長く感じやすかったと思われる。

テーマ 2 の被験者の多くが不満を訴えたのに比べて、テーマ 3 の被験者からの不満の意見はなかった。

【機器登録全般に対する評価】

機器登録の手間については、全体の 20%程度が “どちらともいえない”と回答したが、残りは肯定的な意見と否定的な意見のほぼ半数に分かれた。

ヒアリングにおける意見として、肯定的・否定的意見どちらの意見をもった被験者についても登録処理がより簡便にできる方法を望む意見が多かった。

また機器登録の操作性に関して、テーマ 3 の利用者から、現場でネットワークを構築する時に多数の機器を登録する場面が想定されるため、複数の機器を一括して登録できる仕組みを望むコメントがヒアリングにおいて挙げられていた。

下記図 3-5にアンケート結果のグラフを示す。

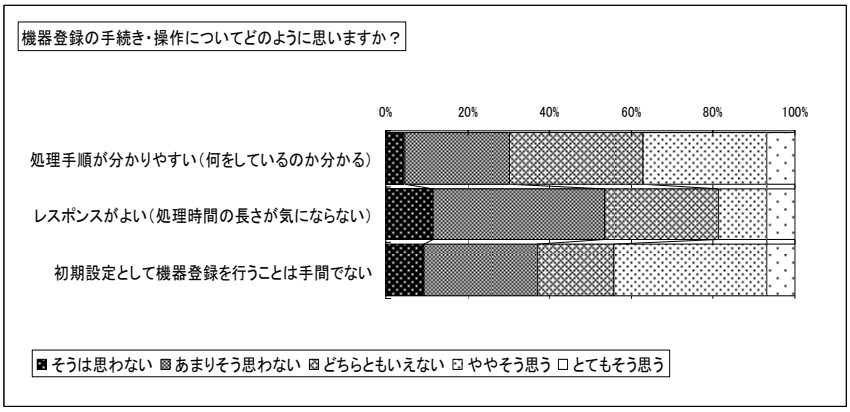


図3-5　機器登録の手続・操作について

(2) 機器登録により提供されるサービスについて

利用者に対して、機器登録を行うことにより、提供を受けることができるサービス例を 5 つ提示し、提供が望まれるサービスの傾向を調査した。

【提供が望まれるサービスについて】

提示した 5 つのサービスすべてについて、約 8 割を超える被験者から肯定的な回答が得られたことから、全般的にこれらのサービスが有用であると考えられる。その中でも、機器の欠陥やリコールに関する通知については、9 割近くの利用者が肯定的な意見を回答しており、“そう思わない”と強く否定した利用者はいなかったことから、強く支持されたといえる。

下記図 3-6にアンケート結果のグラフを示す。

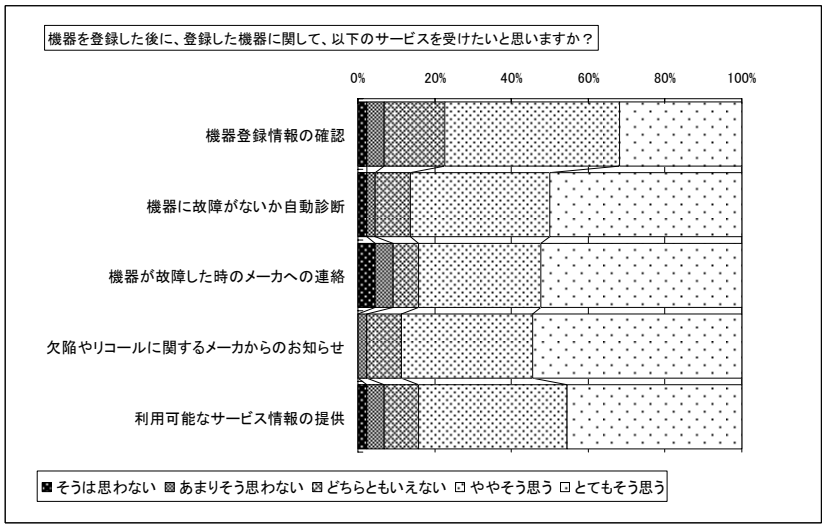


図3-6　提供が望まれるサービスについて

(3) 登録費用の支払い方について

機器登録料を支払うことを前提に、その料金を支払うタイミングについて、利用者に対して 3 つの項目を提示し、利用者として望む形態の傾向を調査した。

機器購入代金やサービス利用料金に含めた場合、機器登録料を支払うことに対する意識は薄くなると思われるが、その中でも機器購入金額に含めて支払う方法を支持する意見が半数以上を占めた。また、サービス利用料金に含めて支払う方法については、否定的な意見から肯定的な意見に分布が広がり、意見が分かれていた。

一方、機器の登録時に別途支払う方法については、支持する意見が少なかった。「いちいち機器を登録する際に別途支払いを行うのは面倒だ。」という理由や、「支払いに際しての支払方法（決済手段）を考えるのが面倒だ。」という声があった。

機器購入金額に含めることに支持が高いのは、登録料金に比して高額である機器代金に上乗せしやすいためと考えられる。

下記図 3-7にアンケート結果のグラフを示す。

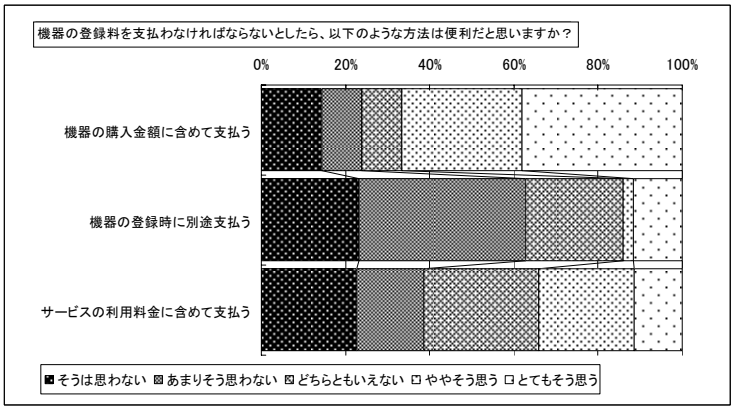


図3-7　機器の登録料の支払い方について（対利用者）

3. 4. 3　機器登録管理センタの運営主体についての検証

事業者、権利者の立場として、機器登録管理センタの運営主体として、5 つの団体等を提示し、意識調査を行った。

【望まれる運営主体について】

運営主体については、サービス事業者の業界団体に対する回答が比較的多かった。それに続いて第三者の民間企業が続いた。グラフの結果からはサービス事業者の業界団体を支持する意見が多いが、「サービス事業者は事業者ごとに色々な主張をするだろう」、「サービス事業者に任せてしまえば良いが、嫌がるであろう」など、サービス事業者が運営主体をする上での困難性を指摘する意見も聞かれた。しかし、運営主体の持つ性格として、第三者性・適正な利潤（儲けすぎたりしない・できない）のみを確保するという性格を求める意見がヒアリングにおいては多く挙げられていた。また、ある機器メー

カの被験者は、「機器登録するということで、自社の機器がどれくらい売れているかが分かってしまうので、機器登録管理センタを民間の一企業に任せるわけにはいかない。」という意見も挙げていた。

下記図 3-8アンケート結果のグラフを示す。

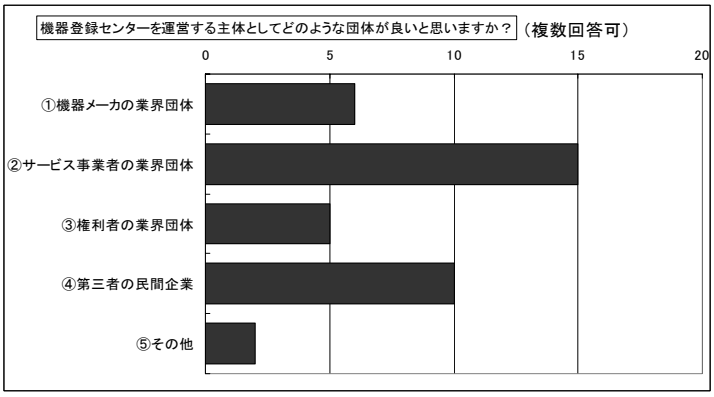


図3-8　機器登録管理センタの運営主体について

3．4．4　機器登録料の課金方法についての検証

事業者、権利者に対して、機器登録料の課金方法として、3 つのモデルを提示し、意識調査を行った。

【望まれる課金方法について】

利用者に対して質問した結果と同様に、機器購入代金に含めるという意見が多かった。また、ユーザに対して機器登録のためのコストを、事業者として明示的に意識させたくないという理由を挙げる声もあり、「機器の登録時に別途支払う」を選択する意見は3．4．2（3）における利用者からの回答と比較しても少なかった。ヒアリングにおいては、ユーザに機器登録を理解させることの困難さや、利用者に機器登録の料金を明示的に意識させたくないという意見が挙げられていた。

また、録音保証金を機器や媒体の代金に含めて利用者から回収するモデルが現在あることから、これと同様の仕組みで利用者に課金する方法が導入しやすいのではないかという意見がヒアリングでは挙げられていた。

下記図 3-9にアンケート結果のグラフを示す。

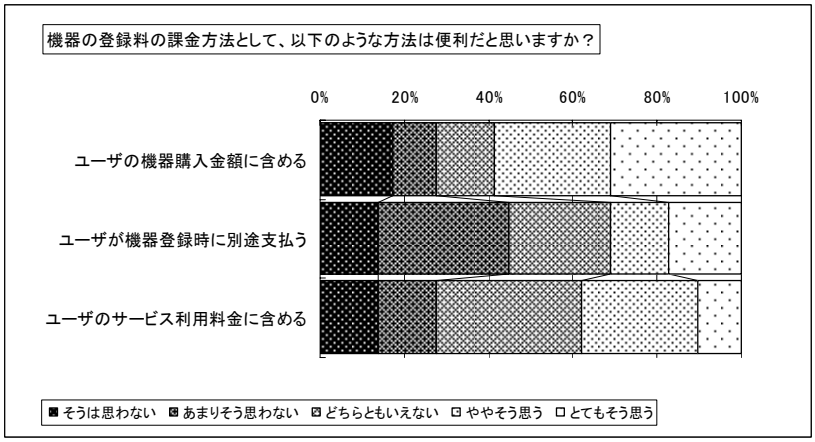


図3-9　機器の登録料の課金方法について（対事業者・権利者）

3. 5　考察

本節では、3. 4で検証した検証結果に基づいた考察をするとともに、機器への利用権限設定に関する次年度以降の課題の整理についても合わせて考察する。

3. 5. 1　機器登録管理センタの設計検証

今年度の機器登録管理センタの研究開発では、テーマ 2 で利用するデジタルコンテンツ再生機器や、テーマ 3 で利用するネットワーク機器の事後登録を実現する事後登録機能の開発を行い、実証事業の中でその実効性を検証した。本研究開発では、機器登録管理センタの事業化に向けて、事後登録に関するセキュリティ脅威への対策や、製造者課金を実現するための仕組み、さまざまな機器に対応するための簡便な事後登録機能の実装、複数 CR の選択などを実現する設計を行い、その有効性を検証した。

今年度はチップ供給者、機器製造者、機器登録管理センタの役割、オペレーション等についての考え方を、昨年度策定された多機能 IC チップフレームワークを基本としつつも、実社会への適応を考慮に入れて修正した。この考え方については、今後実際のチップ供給者や機器製造者となるメーカからの意見も加味しつつ、フレームワークの修正としてどう反映させていくか検討が必要である。また、今年度は機器登録に伴って行われる保有者登録処理は実装しなかったが、保有者課金の実現や機器の法的責任者の特定のためには保有者の個人情報を登録することが必要となるため、今後実装することが望ましい。

3. 5. 2　事後登録機能のユーザビリティに関する検証

ユーザビリティについては、画面の作り込み等により、利用者の操作性を向上させることが可能であるが、基本的に購入時のみに使用する登録機能は利用者に操作をさせることはあまり好ましくないと考えられる。

ヒアリング等における利用者からの要望にもあったように、機器販売時の店頭での実施や、ボタン 1 つで完了する仕組みが望ましいと思われる。

店頭での実施に関しては、機器の箱等の包装を店頭において開梱する必要があるため、店

頭における作業スペース、他人に開梱されることに対する機器購入者の心理的抵抗感等も想定され、対象となる機器の大きさ、特性等に応じて適応性が変化してくると予想される。

ボタン操作での機器登録に関しては、ユーザにおける簡便さが高い反面、機器登録管理センタの選択ができないことや、利用する AP 使用許諾への同意の取り方に関するサービスが低下することが想定される。

また、機器登録管理センタから提供されることを期待するサービスとして評価の高かった“機器の欠陥やリコールの通知”については、サービスを利用するにあたって多機能 IC チップ搭載機器の機器情報が機器登録管理センタへ必ず登録されているので、その機器がリコール対象かどうかを正確に判断できる点で、既存のリコール通知方法と比べて優れているので期待が集まったものと思われる。既存のリコール方法は、メーカがメディアなどを使って通知したリコール情報を利用者が入手する必要があるが、利用者が自分の持っている機器をよく認識していないこともあり、必ずしも確実に通知が伝わるとは限らないという課題があった。

テーマ 2 における利用者とは違った側面として、テーマ 3 における利用者からは機器登録におけるレスポンス（処理時間）はあまり気にならないというコメントが挙げられた。これは、テーマ 3 の機器については業務において利用するネットワーク機器であり、そうしたネットワーク機器を普段利用している利用者は、PC 等の操作を実施する中でシステムのインストール業務等に慣れている。そのため、それらの作業と比較すると今回の機器登録の処理は簡易であり、処理時間も苦にならなかったからではないかと想定される。ここから、使用する機器（一般消費者向け機器と業務用機器）により、同じ処理時間でも利用者が感じる負担に違いが出るということがあると考えられる。

3. 5. 3　機器登録管理センタの運営主体についての検証

運営主体についてはアンケート等を通しても特に一定の傾向がみられず、いずれの団体も主体となりうる可能性があると思われる。

しかし、運営主体の持つ性格として、第三者性・適正な利潤（儲けすぎたりしない）のみを確保するという性格を求める意見が多かったことから鑑みるに、特定の企業集団に属さない会社や、業界各社での共同運営（業界各社によって共同で設立した会社による運営)、公共性の高い機関による運営が期待されていると考えられる。また、機器登録管理センタの運営形態について、立ち上がり期においては複数の業界・サービスにおいて利用する機器をまとめて登録する形態となり、展開期においては業界やサービス特性によって分類された複数の機器登録管理センタが運営されるのではないかという意見もあり、機器登録管理センタに求められる機能についても展開フェーズによって違いが出てくるものと考えられる（今回の実証実験においては、立ち上げ期において必要となると思われる、複数種類機器の登録の機能を実装)。

機器登録管理センタの運営主体については、テーマ 3 においてもテーマ 2 と同じ傾向の意見であった。

3. 5. 4　機器登録料の支払い・課金方法についての検証

利用者、事業者とも機器登録料を「支払う・課金する」ということについて明示的には意識したくないという意見が多かった。

これは、利用者としては機器登録のような作業はあまり意識したくない（今回の実証実験の例でいえば、音楽を聴きたいから機器を買ってきているので、それ以外の作業はあまりやりたくない・面倒だ）ということがあると思われる。

また事業者としては、利用者はサービスを利用するために機器を購入しているので、機器代金やサービス利用料に機器登録料が含まれていても違和感がないとしていることが伺えた。利用者に明示的に代金がかかることを改めて意識させるよりも、機器代金やサービス利用料に含めて課金したいという意向があると思われる。

機器登録料の支払・課金方法については、テーマ 3 においてもテーマ 2 と同じ傾向の意見であったが、テーマ 2 における利用者とは違った側面として、テーマ 3 における利用者からは、機器登録時に個々の機器の登録料を支払う形態では、手間がかかる（業務用途で利用するため、複数・多量の台数の機器を登録する）ことが想定されるので、機器代金もしくはサービス利用料に機器登録料が含まれている形態のほうが望ましいとしていた。

3. 5. 5　機器への利用権限設定に関する考察

近年、デジタル家電をはじ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顕在化してきている。外出先からでも家庭内の電子機器に接続することができれば、これを利用した新たなサービスモデルが創出される。一方、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になってきている。ここで認証として考慮すべきなのは、以下の 2 方向の認証である。

- 利用者（人または機器）が、利用する機器を認証する必要がある（機器から見た場合、内部認証と呼ばれる）
- 利用される機器が、利用者（人または機器）を認証する必要がある（機器から見た場合、外部認証と呼ばれる）

ここでいう認証とは、単に有効な暗号鍵による動的認証（チャレンジ・レスポンス認証）により、認証対象を特定することのみを指し、機器の正当性や、利用者の正当性、所属といった属性認証の要素は含まないものとする。

本節では、上記の認証について、今年度の研究開発では実装されなかった部分について考察し、次年度以降の課題として整理する。

3. 5. 5. 1　機器の認証（内部認証）について

機器の内部認証については、昨年度、今年度とも、機器認証 AP を多機能 IC チップ内に格納し、サービスごとに認証局（CA）から発行された公開鍵証明書により認証を行うこととした。これは、多機能 IC チップ上に搭載される個々のサービスによって必要とする認証内容

（属性認証を含む）はさまざまであろうと考えたため、機器認証についても 1 つの個別サービスとして考えたためである。

しかし、属性認証要素を廃し、単純な機器の身元証明（個体識別）のみに利用する認証機能であれば、機器登録管理センタ等のプレーヤを CA とする機器証明書を用いて、多機能 IC チップフレームワークの一部として、全サービス AP から利用できる形で実装することは、十分活用が期待できる。

実装方式としては、

①デフォルトサービス AP としてあらかじめ機器認証 AP を搭載しておく

②チップマネジャ（CM）の機能として提供する

③サービス AP から利用できるライブラリ機能として提供する。

が考えられる。しかし、①、②の場合、IC カードのような機器の認証に用いる場合、機器認証完了からサービス AP 選択までの間に IC カードを差し替えられても、一般にサービス端末やサービスサーバの側から検出できない場合が考えられるため、有効な認証とはいえない。このため、③の実装が望ましいが、サービス AP に対して開示する API や、ISO/IEC14443-4 で規定された Internal Authentication コマンドに準拠した認証鍵の指定ルール、利用する暗号アルゴリズムと鍵長等について検討する必要がある。

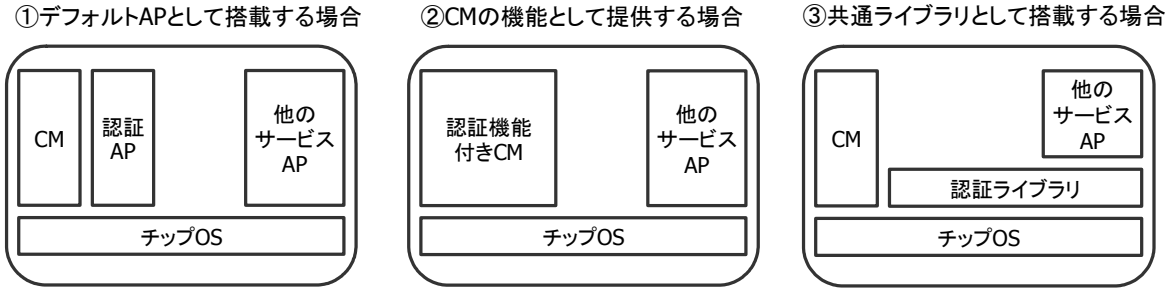


図3-10　内部認証機能の実装方式

3．5．5．2　利用者の認証（外部認証）について

利用者の外部認証については、昨年度、今年度とも、サービス AP 内で解決すべき問題として、特に共通的な機能は用意しなかった。これは、多機能 IC チップ上に搭載される個々のサービスによって必要とする認証内容（属性認証を含む）はさまざまであろうと考えたためである。

しかし、個々のサービスから独立した共通機能としての管理者認証、利用者認証（外部認証）機能を実装することは、十分活用が期待できるものである。

機器または機器上の各サービスにとって、認証すべき対象は以下の 2 つに分類される。

(1) 利用者

機器の各サービスを利用する者。利用者公開鍵とその権限範囲の設定は、多機能 IC チップ上のサービス AP ごとに管理されるべきである。

(2) 管理者

機器全体を管理する者。利用者公開鍵とその権限範囲の設定を変更する権限を持つ。また、管理者公開鍵は初回のみ無条件で設定可能だが、2 回目以降の管理者公開鍵登録、変更には既に登録された管理者公開鍵による外部認証を必要とする。管理者秘密鍵の紛失、失効等に対処するため、常時 2 つ以上の管理者公開鍵が設定されているべきである。

以下に、機器による管理者認証、利用者認証について検討する。

(a) 登録すべき情報と失効管理について

一般に外部認証を行う場合には、あらかじめ認証すべき相手の公開鍵を入手しておくか、信用できる CA の公開鍵を持ち、その CA が発行した公開鍵証明書を提示される必要がある。前者の方法は、認証すべき対象が特定の少数である場合に有効であり、後者は認証すべき対象が不特定多数となる場合に有効である。

機器にとっての利用者認証の場合、認証すべき対象は機器の管理者（所有者）や、管理者に許可された利用者のみであるため、あらかじめ認証対象の公開鍵を登録しておく方式が適している。

ただし、この場合に注意が必要なのは、これらの利用者公開鍵の有効性については、あくまでその登録を許可した機器管理者が責任を負うということである。外部の CA の存在を前提としないため、公開鍵の暗号寿命による有効期限切れや、秘密鍵の紛失・漏洩による失効などは、その都度機器管理者が副管理者鍵で認証の上で、責任をもって登録抹消処理などを行う必要がある。

(b) 機器利用者鍵リストの格納場所と認証タイミングについて

利用者公開鍵の格納場所と、認証時の利用方法については、以下の 3 つのパターンが考えられる。

1）機器チップ内に格納し、設定変更時には管理者鍵を、利用時に利用者鍵を用いて機器との間で直接認証。

メリット	デメリット
・サービス利用、設定変更がセンタアクセス無しで実施できる。 ・機器登録の際の保有者登録と別に機器の管理者、利用者が設定できるため、自由度が大きい。	・多機能 IC チップの容量を圧迫する可能性がある。 ・管理者鍵、利用者鍵さまざまな認証プロトコル（暗号アルゴリズム、鍵長、認証手順等）への対応が比較的難しい。

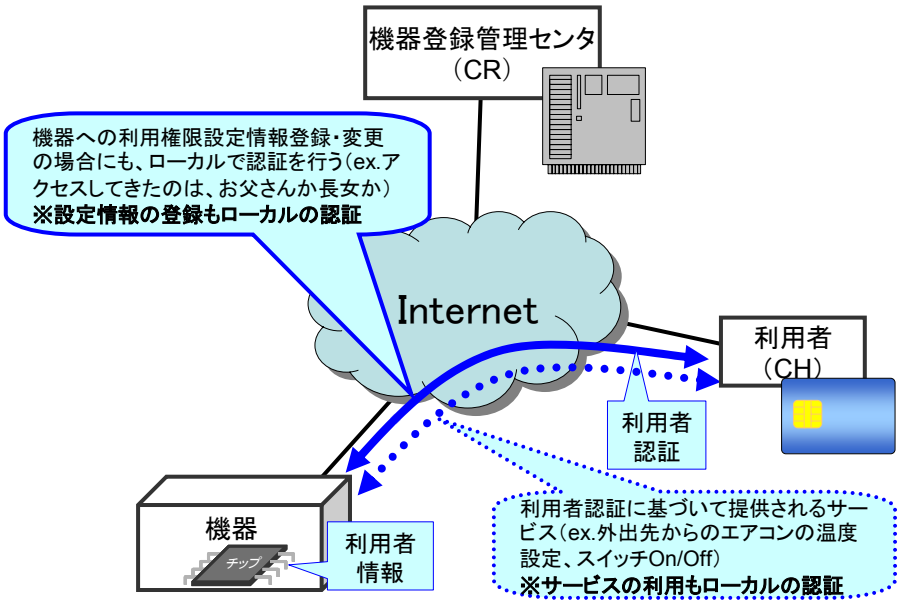


図3-11　利用者と機器が直接認証する場合

2）CR サーバに格納し、設定変更時には管理者鍵を、利用時には利用者鍵を用いて CR サーバ経由で認証。

メリット	デメリット
・複数の機器の設定変更が一括して行なえる。 ・管理者鍵、利用者鍵、センタが各 CA への有効性確認を行うことにより、確実な有効性チェックができる。 ・管理者公開鍵登録を、機器登録の際の保有者登録と兼ねることができる。 ・さまざまな認証プロトコル（暗号アルゴリズム、鍵長、認証手順等）への対応が比較的に容易。	・CR が個人情報としての権限設定を知り、管理する必要がある。 ・サービス利用ごとにセンタアクセスが必要になる。 ・センタがダウンした場合、機器のサービスが利用できなくなる。

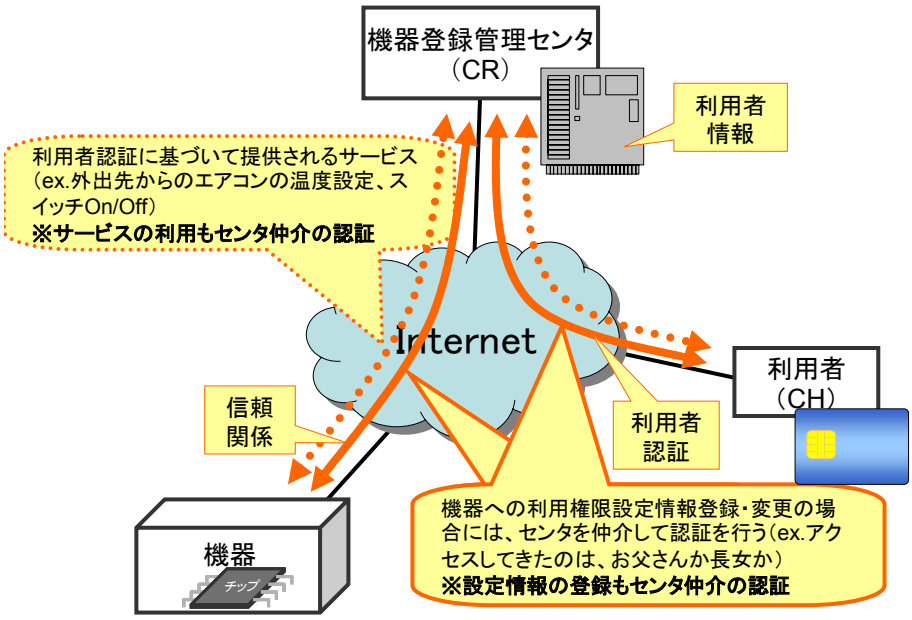


図3-12　利用者と機器が CR を介して認証する場合

3）CR サーバ、機器にそれぞれ保管し、設定変更時のみ CR サーバ経由で認証を行い CR サーバ、機器の設定を変更するが、個々のサービス利用時には機器との間で直接認証。

メリット	デメリット
・複数の機器の設定変更が一括して行なえる。 ・管理者鍵の有効性についてセンタが各 CA への有効性確認を行うことにより、確実な有効性チェックができる。 ・管理者公開鍵登録を、機器登録の際の保有者登録と兼ねることができる。 ・さまざまな認証プロトコル（暗号アルゴリズム、鍵長、認証手順等）への対応が比較的に容易。	・CR が個人情報としての権限設定を知り、管理する必要がある。 ・設定変更の場合にセンタアクセスが必要になる。 ・センタがダウンした場合、設定変更ができなくなる。

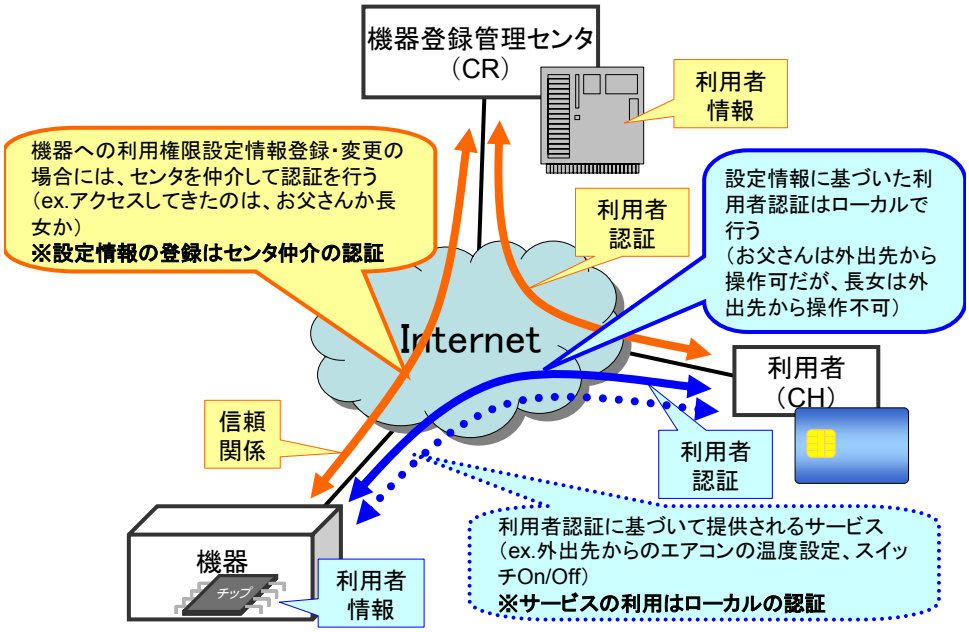


図3-13　直接認証、CR を介した認証の併用

これらの案の何れが適しているかについては、機器上の各サービス、CR の提供すべきサービス等を総合的に勘案した上で、さらに検討を深める必要がある。

（c）機器チップ内に格納する場合の実装の仕方について

管理者鍵、利用者鍵を機器チップ内に格納する場合について、実装方式としては内部認証機能の場合と同様に、

①デフォルトサービス AP としてあらかじめ利用者認証 AP を搭載しておく

②チップマネジャ（CM）の機能として提供する

③サービス AP から利用できるライブラリ機能として提供する

が考えられる。管理者認証については、全サービスに共通であるため、どの方式でも問題ないが、利用者認証については、サービスごとに異なり、また全サービス AP から呼び出せる機能になっている必要があるため、③の方式で、管理者鍵は共通ライブラリ部分に、利用者鍵は各サービス AP 部分に格納するのが良いと思われる。ただし、サービス AP に対して開示する API や、ISO/IEC14443-4 で規定された External Authentication コマンドに準拠した認証鍵の指定ルール、利用する暗号アルゴリズムと鍵長等について検討する必要がある。

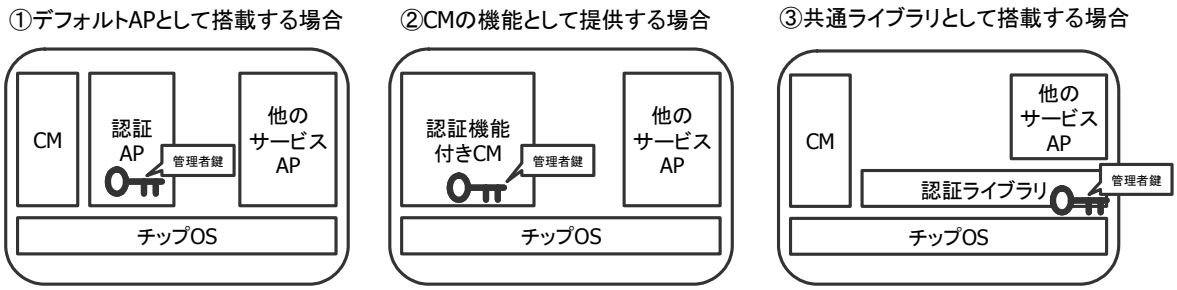


図3-14　外部認証機能の実装方式

3．5．5．3　まとめと残存課題

ネットワーク接続する機器の認証として、内部認証と外部認証が必要であり、それぞれ属性認証を伴わない単純な個体識別としての認証であれば、多機能 IC チップフレームワークの一部としてプラットフォーム化できる可能性があることがわかった。

内部認証については、各サービス AP から呼び出される共通ライブラリとして実装することが望ましいが、機器個体識別用証明書を発行する認証局を機器登録管理センタが行うか、別のプレーヤが行うかについては議論が必要である。

また、個々のサービス AP が利用する Internal Authentication コマンドと共存する形で ISO/IEC14443-4 に準拠した実装ができるかについても検討が必要である。

外部認証については、管理者鍵・利用者鍵を機器に登録するか、CR サーバ等のセンタで管理するかについて、引き続き検討が必要である。機器内で管理する場合、やはり認証機能の実装方法としては、各サービス AP から呼び出される共通ライブラリとして実装することが望ましいが、個々のサービス AP が利用する External Authentication コマンドと共存する形で ISO/IEC14443-4 に準拠した実装ができるかについては検討が必要である。

4. 可搬型リーダライタの研究（テーマ１−2）

4．1　研究の概要

4．1．1　背景と目的

利用者が多機能 IC チップ搭載機器を機器登録管理センタに登録して、サービス提供者から AP 追加を実施するためには、多機能 IC チップをネットワークに接続し、各サーバと多機能 IC チップとの間で通信を行う必要がある。機器登録管理センタ等への接続形態には、図 4-1 にあるように、①多機能 IC チップ搭載機器自身がネットワーク接続機能を持ち、インターネットを経由して機器登録管理センタ等に接続する形態と、②多機能 IC チップ搭載機器自身にはネットワーク接続機能はなく、外部のネットワーク接続可能な機器に接続した上でインターネットを経由して機器登録管理センタ等に接続する形態の 2 つの形態が考えられる。

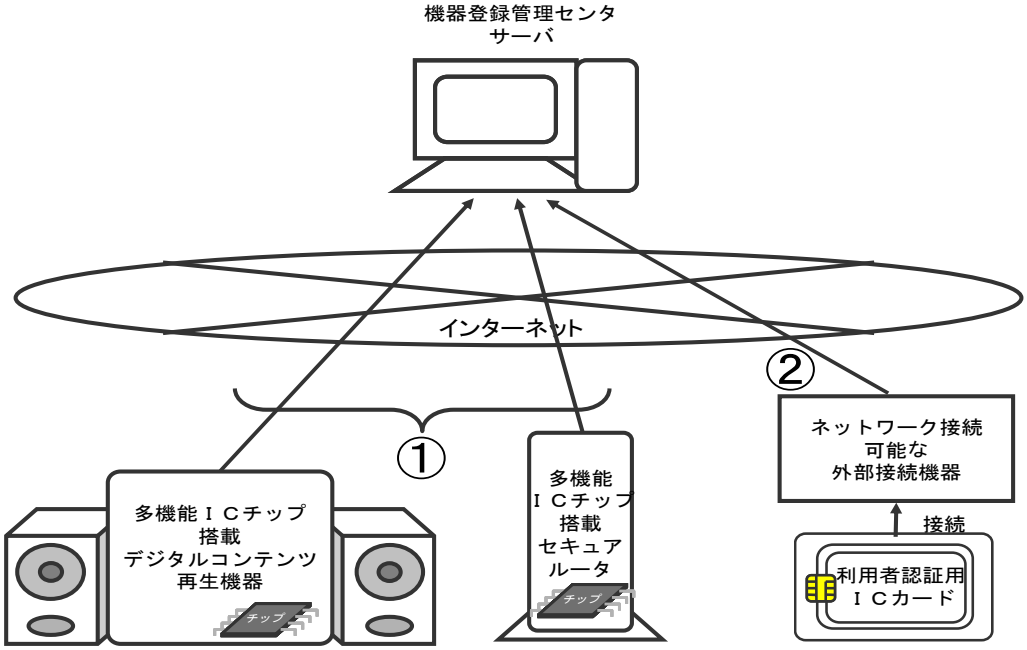


図4-1　2 つの接続形態

本テーマでは、②の形態に注目し、ネットワーク接続機能を備えていない多機能 IC チップ搭載機器と連携して、登録・AP 追加・AP 削除等を行うための持ち運び可能なリーダライタ機器（以下「可搬型リーダライタ」という。）について、その有効性と相互互換性確保に関する条件の整理を行った。具体的には、可搬型リーダライタを活用することによって、どのような利用やサービスが創出されるのかを整理し、多機能 IC チップ等によるサービス実現に向けての有効性を明らかにした。またその一方で、可搬型リーダライタに求められる機能要件及びその実現課題を整理し、可搬型リーダライタの実現可能性を検討した。

なお、可搬型のリーダライタを搭載する機器としては PDA やノート型 PC、携帯電話端末等が考えられる中で、ここでは実装条件は厳しい一方、普段の生活の中で最も身近に使用さ

れている携帯電話を主な候補として検討した。またネットワーク接続機能を持たない多機能 IC チップ搭載機器としては、非接触 IC カードを主な対象として検討した。

4．1．2　用語

以下に、本章で使用する用語を定義する。

可搬型機器	携帯電話等、保有者により持ち運びが可能な機器。
可搬型リーダライタ	非接触 IC カードリーダライタを搭載した可搬型機器。
機器外チップ	多機能 IC チップ搭載機器（カード）に搭載された多機能 IC チップ。
機器内チップ	可搬型機器に搭載された UIM や、多機能 IC チップ等その他の組み込みチップ。
外部機器	機器外チップを搭載した機器。
機器 AP	可搬型リーダライタ搭載機器に搭載されたリーダライタを制御するためのアプリケーションまたはアプリケーション群。
チップ AP	機器外チップに搭載され、機器外チップ上で動作するアプリケーションプログラム。

4．1．3　研究の進め方

本サブテーマでは、主題となる①可搬型リーダライタの有効性、②相互互換性を確保するための検証を実施するための条件を整理するため、以下の手順で研究を行った。

（1）基本要件の整理
（2）想定利用シーンの検討
（3）考慮事項の検討
（4）機能要件の検討

4．2　基本要件とサービスモデル

本節では、可搬型リーダライタに求められる最低限の機能に関して基本要件として抽出し、その基本要件を満たす可搬型リーダライタの有効性を検証するため、非接触 IC カードリーダライタが可搬型になった場合の利用シーンを検討した。

4．2．1　可搬型リーダライタの基本要件

可搬型リーダライタは、自らはネットワーク接続機能を持たない多機能 IC チップ搭載機器（以下「外部機器」という。）と接続し、機器登録管理センタ（CR）への事後登録実施、サービス提供者（SP）とのチップ AP 追加・削除を可能にする機能を基本機能とする。このように可搬型リーダライタを利用する場合、可搬型リーダライタ機器に求められる基本機能について検討した。検討した結果は以下のとおりである。

・ネットワーク接続機能を持つこと
CR、SP への接続を可能とするネットワーク接続機能を持つ必要がある。

・外部機器とのローカル通信機能を持つこと
外部機器と直接接続できるインタフェースを持つ必要がある。ローカル通信インタフェースとしては、シリアル接続（USB、IEEE1394 を含む）、IrDA、Bluetooth、非接触 IC カード（ISO/IEC14443 TypeB）等が考えられる。外部機器として IC カードも含まれるため、特に ISO/IEC14443 TypeB インタフェースを持つことが望ましい。

・コンテンツブラウザ機能を持つこと
CR、SP への接続や、各種サービス提供を受けるために、HTTP、WAP などのコンテンツを表示するコンテンツブラウザ（以下「ブラウザ」という。）機能を持つことが望ましい。

・リーダライタ機器上に機器 AP を実行する AP 実行環境があること
CR、SP への接続を行っての登録処理や、チップ AP の追加・削除処理、各種サービスを提供するための機器 AP を実行できる AP 実行環境を持つことが望ましい。

・選択、決定操作等ができる入力デバイスを持つこと
CR への登録処理、SP との AP 追加・削除処理の際、利用者意思の確認や選択が必要になるため、利用者が選択操作等を行うことができる入力デバイスを持つ必要がある。可能であれば、キーボードやテンキー等の入力デバイスがあることが望ましい。

・利用者への操作ガイドが可能な表示デバイスを持つこと
CR への登録処理、SP との AP 追加・削除処理の際、利用者意思の確認や選択が必要になるため、選択操作等を利用者にガイドすることができる表示デバイスを持つ必要がある。

・動作状態を示すインジケータを持つこと

前項の表示デバイスによる表示や、LED による表示などを用い、電源 ON 状態、通信中、電源 OFF 状態など、リーダライタの動作状態を表示できる必要がある。

次節では、可搬型リーダライタが上記の基本機能を満たしている場合に、その応用として想定されるサービスを検討する。

4．2．2　応用サービス

本節では、前節で検討された基本機能を持つ可搬型リーダライタを活用して、ネットワークを利用したサービスであること、可搬型リーダライタの外部にある多機能 IC チップ搭載機器と連携したサービスであること、可搬型ならではの特徴である時間、場所にとらわれないサービスであることを条件として応用サービスを検討した。

検討の結果、表 4-1の 7 つの応用サービスが抽出された。

表4-1　応用サービス一覧

項番	サービス名	サービス概要
1	カードビューア	機器外チップの内容を、出力デバイスを使って表示する。
2	バリューダウンロード	ネットワークを利用して機器外チップに電子マネー等のバリューを書き込む。
3	公的カードによる本人確認	ネットワークを経由して公的サービスや民間サービスを利用する際の本人確認に、広く普及した公的カードを利用する。
4	無記名カード受領後会員登録	機器外チップにネットワークを経由して本人情報等を書き込む。
5	バリュー利用（リアル）	販売員への支払い等、利用者と事業者が対面形式で電子マネー等のバリューを利用する。
6	バリュー利用（バーチャル）	ネットワークを介して利用者と事業者が非対面形式で電子マネー等のバリューを利用する。
7	他機器連携	他の可搬型リーダライタ機器と連携して利用する。

(1) カードビューア

現行の IC カードを活用した一般的なサービスでは、カード内部に記憶されたサービスデータを利用者が参照する場合、リーダライタが搭載された固定式の専用機器、または汎用 PC に接続されたリーダライタを利用の上、これら機器に搭載された表示用画面、プリンタ等の出力機器を利用する必要がある。画面表示機能を持つ携帯電話等の可搬型機器にリーダライタを搭載することで、利用者は時間や場所にとらわれることなく、いつでもどこでも既存サービスの情報を参照することができるようになる。

(2) バリューダウンロード

現行の IC カードを活用したサービスでは、電子マネーや電子チケット等のバリューを入手する場合は、リーダライタが搭載された固定式の専用機器、または汎用 PC に接続されたリーダライタを利用の上、これら機器に接続されたネットワークを介してバリュー管理センタ等に接続し、カード内部への書き込みを行うのが一般的である。ネットワーク接続機能を持つ携帯電話等の可搬型機器にリーダライタを搭載することで、利用者は時間や場所にとらわれることなく、いつでもどこでもバリューを入手することができるようになる。

(3) 公的カードによる本人確認

各自治体で交付されている住民基本台帳カードを可搬型リーダライタにかざして公的個人認証サービスを活用することにより、各自治体の提供する印鑑証明書や住民票の取得、公共施設の予約等の住民サービスを、いつでもどこでもネットワークを介して利用できる。また、将来実現が期待される電子投票等、信頼性の高い本人確認が求められるサービスを受けることができるようになる。

また、インターネット上で行われる民間の新規会員サービスへの加入等、本人確認が求められるサービスの申込シーンで、住民基本台帳カードや IC パスポート、IC 運転免許証等、IC カードを使った証明書を可搬型リーダライタにかざすことで、身分証明として利用することができ、場所・時間にとらわれることなく、いつでもどこでもサービスへの申込やサービスを受けることができるようになる。

(4) 無記名カード受領後会員登録

IC カードを使ったポイントサービス等の会員証サービスの入会時に、会員証アプリケーションは搭載されているが、会員との関連付け（パーソナライズ）がされていない多機能 IC チップ搭載会員証等の無記名カードを受け取り、その場で利用を開始する。利用者は、後から可搬型リーダライタを利用して、IC カードに会員情報を書き込む。

従来の紙のメンバーズカード等で一般的な無記名台紙（カード）を配布し、利用者が自ら記名する方式と同様に、利用者が会員登録をした直後からポイントサービス等の会員サービスを受けることができるだけでなく、事業者は会員個別の会員証発行をする必要がないため安価に会員証カードを配布できるようになる。

(5) バリュー利用（リアル）

通常固定されているリーダライタが可搬型になることで、店頭のみで使用されていた IC カード決済が、いつでもどこでもでも利用できるようになる。

例えば野球場等の野外施設で、移動販売員の持つ可搬型リーダライタ機器にデビットカードや電子マネー、クレジットカード等の IC カードをかざすことで、それぞれの決済手段による支払いが可能となる。

ただし、店頭利用の場合と同様に、移動販売員の端末に利用者 PIN 等のデータが残らない仕組みが求められる。

（6）バリュー利用（バーチャル）

インターネット上で提供される有料コンテンツ配信サービスやショッピングサイトでの決済は、クレジットカード番号と有効期限のみの指定で許されるものなど、セキュリティの低いものが見受けられる。IC デビットカードや電子マネー、IC クレジットカード等を用いれば、決済のセキュリティを高めることができるが、さらに可搬型リーダライタが利用できれば、いつでもどこでも欲しいと思ったその場で簡単にセキュアな決済ができるようになる。

（7）他機器連携

可搬型リーダライタ同士で、外部インタフェースを活用して、読取った IC カードの情報を相互に利用することができる。

例えば、IC カードに格納されたゲームキャラクターを可搬型リーダライタに読み込み、対戦相手の可搬型リーダライタへ外部インタフェース（Bluetooth、IrDA 等）を介して送ることで対戦するようなゲームへの活用が期待できる。

名刺交換のかわりに、自分の IC 社員証を可搬型リーダライタで読み取り、相手の可搬型機器に送ることで、相手は名刺の情報を顧客情報としてデータ化する手間が省けるだけでなく、ペーパーレスな情報交換が可能となる。

4．2．3　本節のまとめ

本節では、可搬型リーダライタに求められる基本機能を定義し、基本機能を活用した場所・時間にとらわれない応用サービスをいくつか抽出した。

このように可搬型リーダライタが実現すれば、新たなサービスシーンが広がり、利用者の利便性向上が望めることから、利用者増加による既存サービスの活性化、新たなサービス事業者の参入等に結びつくと考えられ、多機能 IC チップ等によるサービス実現に向けての有効性が認められた。

次節では、本節で抽出されたサービスが、不特定多数の人々が集まる公共の場所で利用される場合に想定すべき利用者への脅威や、利便性の観点等、実社会で可搬型リーダライタが利用される場合に考慮すべき事項を検討し、それらへの対策として基本要件に追加されるべき機能要件を検討する。

4．3　考慮事項と機能要件

本節では前節で想定された利用シーンから、実社会で可搬型リーダライタが利用される場合に考慮すべき事項を抽出し、抽出された考慮事項に対応するための要件を検討した。これにより、可搬型リーダライタがメーカ各社から提供された際の最低限の相互互換性を確保する。

4．3．1　考慮事項の検討

本節では、可搬型リーダライタの各利用シーンで考慮すべき事項を検討した。検討した結果は以下のとおりである。

・可搬型リーダライタ保有者の意図した利用時に安定して利用できるための考慮事項
可搬型リーダライタは、携帯されることが望まれるため、リーダライタ利用に必要な電力は、搭載されたバッテリーに依存する。利用者が利用したい場面において、電力不足により利用不能に陥る可能性を極力排除する必要がある。

・IC カード等の機器外チップ保有者の意図しない機器外チップ利用に対する考慮事項
可搬型リーダライタは、機器外チップへの通信手段として利用されるため、機器外チップ保有者の意図しない利用（混雑場所での盗み読み、サイバースリ、IC カード紛失時の拾得者による利用等）による、機器外チップ保有者への経済的、精神的損害を与えないための対処が必要である。

・可搬型リーダライタ保有者の意図しない可搬型リーダライタ利用に対する考慮事項
可搬型リーダライタ保有者の意図しない利用（盗難、無意識操作、可搬型リーダライタ紛失時の拾得者による利用等）による機器保有者への経済的、精神的損害を与えないための対処が必要である。

・可搬型リーダライタ保有者の安全を確保するための考慮事項
可搬型リーダライタは、常時利用者が保有することが見込まれるため、リーダライタの動作中、スタンバイ中を問わず、人体への障害を与える危険性を排除する必要がある。

・ネットワーク接続と連動した利用に対する考慮事項
可搬型リーダライタは、ネットワークへの接続機能を持ち、ネットワークを経由したサービスを提供する可能性が高いため、ネットワーク上の脅威（盗聴、改ざん、成りすまし、不正なサービスサーバ、不正な機器 AP 等）への対処が必要である。

・可搬型リーダライタを使ったサービスの利便性向上のための考慮事項
可搬型リーダライタによる多彩なサービスが想定されるため、その操作方法は、利用者にとってわかりやすく、操作しやすい必要がある。また、機器によるサービス提供者が

開発しやすい環境である必要がある。

次節では、これらの事項を考慮した場合に可搬型リーダライタに求められる機能要件を検討する。

4．3．2　機能実装についての考察

本節では、前節で列挙した事項に対して考慮された各機能の要件を検討した。検討した結果は以下のとおりである。

（1）一般的な要件

・消費電力が低いこと
可搬型機器は、電池等の可搬型電源を利用する必要があるため、電源容量を圧迫しない低消費電力化が求められる。

・リーダライタモジュール（アンテナ、回路）の物理的サイズが小さいこと
可搬型機器は、その利便性から手に持ちやすい、あるいはハンドバッグ等に入れても邪魔にならないサイズが求められるが、リーダライタモジュールはその内部に作り込まれるため、より小さいものが求められる。

・公的 IC カード（住民基本台帳カード、運転免許証、パスポート、健康保険証等）や、非接触クレジットカード等、今後普及が予想される非接触 IC カードが読み書きできる非接触通信性能（アンテナ特性、電波出力等）を持つこと
可搬型リーダライタは、CR に対する保有者登録に公的個人認証カード等の公的な IC カードを利用したり、その他の公的サービス（電子投票、電子申請等）を利用したりと、広く応用可能な機器となることが想定されるため、普及が予想される各種 IC カードを広くサポートし、読み書きできることが求められる。

・リーダライタが搭載されていること、アンテナ位置が見た目で判ること
可搬型リーダライタを使って、IC カード保有者の意思に反して IC カードを読み取られる危険性があるため、リーダライタ搭載機器であることが見た目で判別できることが求められる。

・リーダライタ動作時に音を出すこと
可搬型リーダライタを使って、IC カード保有者の意思を伴わない盗み読みを検知しやすくするため、IC カードにアクセスしリーダライタの動作時に音を出すことが求められる。

・電波到達距離は限定的であること

混雑した電車内など、他人と接近した状況に置かれた場合に、あまり電波到達距離が長すぎると、可搬型リーダライタを使って、IC カード保有者の意思を伴わない盗み読みをされる可能性があるため、例えば 10 cm 以内程度といった IC カード保有者が安心できる電波到達距離であることが求められる。

・発熱が少ないこと

高温で火傷や機器変形をしないことはもちろんだが、可搬型リーダライタでは、低温でも常時発熱している場合、低温火傷を引き起こすことも考えられるため、タイムアウト機能と合わせた発熱条件の設定が必要である。

・2 枚以上の同時アクセスに対応する必要はない

電源容量が小さい可搬型リーダライタでは、複数枚通信可能な出力を確保することが難しい。また、公共交通機関の自動改札やコンビニエンスストアの POS レジ等のリーダライタのように高速処理を求められる場合と異なり、同時に 2 枚以上のカードへのアクセスを行なわず、カードを 1 枚ずつかざし替えるようサービス利用者に求めることで、同時には 1 枚のカードにアクセスすることで十分サービス可能と考えられる。このため、複数枚の IC カードが可搬型リーダライタと通信可能な領域内にある場合でも、先に応答したカードとの通信のみ行なえば十分である。

(2) リーダライタ起動・終了パターンに関する要件

・可搬型リーダライタ機器上の機器 AP から API により起動、操作できること

IC カードをはじめ多機能 IC チップでチップ AP を利用する場合には、AP 選択時に AID を指定する必要があり、携帯電話のカメラによる QR コード等の読み込みのように汎用的なデータ読み込みはできないため、必ず何らかの機器 AP を通じて起動、操作される必要がある。

・適切なタイムアウトによる出力オフができること

可搬型リーダライタの場合、カバンやポケットの中に入れて持ち運ばれることが予想されるため、利用者が意識しないボタン押下が発生し、電波出力が行われる危険がある。このような誤起動の場合にも、電源消費を一定に抑えるために、一定時間の APDU 送受信がない場合には出力停止を行う等のタイムアウト処理が必要である。

・適切な電源容量に満たない場合は起動できなくすること

IC カード処理途中での電源低下により、サービスのトランザクションが維持できなくなる可能性があるため、一定量の電源容量が確保できない状態ではリーダライタ機能を起動できなくする必要がある。

・起動時に利用者の確認を取ること
不正な IC カードアクセスを目的とする機器 AP や、誤操作による起動等による、利用者が意識しない IC カードアクセスを防ぐため、リーダライタ起動時には必ず利用者への確認を行う必要がある。

（3）アプリケーションに関する要件

・機器 AP に PIN を明かさない Verify API を持つこと
悪意の機器 AP によるフィッシング（PIN を入力させて盗み取ること）を防ぐため、PIN を機器 AP に明かさずに IC チップに対して Verify を実行する API が必要である。

・機器 AP 終了時に利用したメモリを確実に解放すること
使用済みメモリからデータが読み取られることを防ぐため、確実にメモリ解放する仕組みが必要である。

（4）ネットワーク接続、機器内チップ、その他の外部接続に関する要件

・ネットワーク接続、機器内チップ、その他のローカルインタフェース利用と機器外チップアクセスは同時に維持できること
機器外チップへのアクセスと、ネットワーク接続や機器内チップ、その他の外部接続を利用の都度切り替える場合、煩雑な動作によりサービスの利便性が低下し、チップ AP のトランザクション維持が困難になる。このため、機器外チップへのアクセスは、これらのインタフェースの利用と相互に干渉せずに利用できる必要がある。

4．3．3　機能要件一覧

本節では、前節で検討された各機能要件を一覧表に整理する。表 4-2 のとおり、可搬型リーダライタに求められる考慮事項に対応した各機能要件について、基本要件、追加要件を合わせて 24 項の要件として整理した。

表4-2　機能要件一覧表

項番	区分	要件
1	基本要件	
1-1		ネットワーク接続機能を持つこと。
1-2		外部機器とのローカル通信機能を持つこと。
1-3		コンテンツブラウザ機能を持つこと。
1-4		リーダライタ機器上に機器 AP を実行する AP 実行環境があること。
1-5		選択、決定操作等ができる入力デバイスを持つこと。
1-6		利用者への操作ガイドが可能な表示デバイスを持つこと。
1-7		動作状態を示すインジケータを持つこと。
2	追加要件	
2-1		消費電力が低いこと。
2-2		リーダライタモジュール（アンテナ、回路）の物理的サイズが小さいこと。
2-3		公的 IC カード（住民基本台帳カード、運転免許証、パスポート、健康保険証等）や、非接触クレジットカード等、今後普及が予想される非接触 IC カードが読み書きできる RF 性能（アンテナ特性、電波出力等）を持つこと。
2-4		リーダライタが搭載されていること、アンテナ位置が見た目で判ること。
2-5		リーダライタ動作時に音を出すこと。
2-6		電波到達距離は限定的であること。
2-7		発熱が少ないこと。
2-8		2 枚以上の同時アクセスに対応する必要はない。
2-9		可搬型リーダライタ機器、またはそれに接続された外部機器上の AP から API により起動、操作できること。
2-10		適切なタイムアウトによる出力オフができること。
2-11		適切な電源容量に満たない場合は起動できなくすること。
2-12		起動時に利用者の確認を取ること。
2-13		機器 AP に PIN を明かさない Verify API を持つこと。
2-14		ネットワーク接続と外部チップアクセスは同時に維持できること。
2-15		内部チップアクセスと外部チップアクセスは同時に維持できること。
2-16		機器 AP 終了時に利用したメモリを確実に解放すること。
2-17		その他のローカルインタフェース利用と外部チップアクセスは同時に維持できること。

4．3．4　本節のまとめ

上記のとおり、可搬型リーダライタ機器の基本要件に加え、実社会で可搬型リーダライタによって場所や時間にとらわれないサービスが提供された場合に考慮すべき事項への対策として追加要件を検討した。これにより、可搬型リーダライタがメーカ各社から提供された際の相互互換性を確保するための最低限の要件が整理されたものと考えられる。しかしここで整理された要件は概念的なものが多く、来年度以降さらにこれらの要件についての具体化、詳細化等の検討が必要である。

4．3．5　残存課題

今年度の検討の中で、4．3．2で抽出された機能要件以外にも、いくつかの検討すべき事項が指摘された。本節では、それらの残存検討課題について記述し、簡単な考察を加える。

(1) 処理速度等スペックに関する要件について

可搬型リーダライタの起動速度性能、終了速度性能、読み取り・書き込み性能について、要件化を検討した。しかし、公共交通機関での自動改札機やコンビニエンスストアの POS レジ端末のように、1 台のリーダライタで複数の利用者の処理を連続して行なわねばならない場合と違い、可搬型リーダライタの場合には利用者が 1 人でリーダライタを占有して利用できるため、処理速度性能に対する厳しい要求は必要ないものと考えられるため、今回要件としては定義しなかった。

(2) リーダライタの個体識別に関する要件について

可搬型リーダライタを紛失、盗難等で第三者に利用されることを防ぐための、ネットワーク経由で遠隔停止できる機能についても検討した。しかし、この機能の実現には、可搬型リーダライタ自体に機器内チップを搭載するなどして個体識別を可能にし、かつ可搬型リーダライタの保有者を登録する仕組みを検討する必要があるため、今年度の要件化は見送った。

(3) ブラウザからのリーダライタ操作の可能性について

多彩なサービスが提供できることを考慮し、サービス提供者が開発しやすい環境を整えるとの観点から、機器 AP を開発しなくても、HTTP や WAP のコンテンツに特殊なタグを定義するなどしてブラウザからのリーダライタ操作を実現することは、簡易にチップアクセスできる仕組みとして有望である。しかし、SSL 等による盗聴防止をした場合にも、悪意のサーバによる PIN のフィッシング（騙し取り）等を防止する必要があるため、PIN 等の秘密情報を取り扱う場合、TTP サーバ（信用できる第三者サーバ）による中継を必須とする等の仕組みを検討する必要がある。また、HTTP や WAP でのタグの標準化等の課題も残っており、今年度の要件化は見送った。

(4) ユーザ AP・機器 AP の開発者に対する認定制度整備の可能性について

機器 AP に任意の APDU の利用を許可してしまうと、正当なサービス提供者になりすました組織による悪意の機器 AP による不正利用が発生しないか懸念される。これを防ぐため、任意の APDU を利用できる機器 AP は開発元の届出を必要とし、届出のない開発元による機器 AP の場合、特定のコマンド群（例えば Verify 以外の JICSAP コマンド等）のみ利用可能とする等、AP 実行環境に制約を設けることも検討すべきである。しかし、安易な制限の設定は、可搬型リーダライタを利用したサービスの発展を阻害する可能性もあり、慎重な検討が必要である。

(5) カード AP 設計時に考慮すべき事項について

可搬型リーダライタ機器そのものに求められる要件ではないが、チップ AP 開発の際に考慮すべき事項について以下に指摘する。これらは従来の IC カード AP 開発でも意識すべき内容であるが、特に可搬型リーダライタの出現により注意が必要な事項である。

・カード AP のデータ参照機能に、ある程度のアクセス権限確認を持たせること
従来の IC カード AP では、利用者 ID（会員番号など)、バリュー残高、利用履歴等の参照機能には利用権限確認を行なわないものが多いが、利用者のプライバシー保護のためには、自由な閲覧を制限することも必要となる。ただし、閲覧ごとに PIN 入力を求める等の処理は、利用者の利便性を大きく損なうため、その制限の程度については慎重な検討が必要である。

・バリュー操作（チャージ、支払など）など利用者に金銭的損害を与える可能性のある処理を行う場合には確実に権限確認を行うこと
従来の IC カード AP では、IC カードをリーダライタにかざす動作により IC カード利用者の利用意思確認を兼ねる場合が多いが、リーダライタが可搬型になることにより、IC カード利用者意思の有無にかかわらず、リーダライタ側を動かしてかざすことにより IC カードアクセスが可能である。このため、利用者意思確認として PIN 入力をさせる等、確実な利用者の本人確認が必要である。

・PIN 入力を行う際には、ソフトウェア的に毎回キー配列を変更する等入力動作による PIN 解読を回避すること
銀行 ATM、デビット店舗端末のように PIN 入力を必要とするリーダライタでは、通常、PIN 入力の覗き見を防止するためのついたてやカバーを設置する。しかし、可搬型リーダライタの場合、そのような物理的な防止策を期待することができないため、ソフトウェア的にキー配列を毎回変更する等の対策により、覗き見による PIN 情報解読を防止する必要がある。

4．4　考察

以上のように、可搬型リーダライタによる今までにない新たなサービス利用シーンが想定されることから、可搬型リーダライタの有効性は大いに期待できることが分かった。

また、リーダライタを可搬型にするための基本要件に加え、実社会でのサービスを提供しようとした場合、多岐にわたる考慮事項が存在し、これらに対応するために、追加要件を検討したことで可搬型リーダライタと IC カード等機器外チップとの相互互換性確保のための最低限の機能要件を整理した。

しかしながら、今年度整理した各要件は概念的なものも多く、今後可搬型リーダライタを利用したサービスを実現しようとした場合には、実際に機器に実装するための詳細かつ具体的な要件について決定する必要がある。来年度以降は、可搬型機器メーカや、リーダライタメーカ等と協力して試作機を開発し、それを利用してサービス事業者を含めたサービスの実証実験等を行う等、運用性の検討も含めたさらなる検討が必要になると思われる。

5. 多機能 IC チップ搭載機器のセキュリティ機構やライフサイクル管理のあり方についての研究（テーマ1－3）

5. 1　概要

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）」では、従来の IC カードに対する運用フレームワークである NICSS の「IC カードフレームワーク要件書 Ver1.20」と「IT 装備都市研究事業　実証実験用　共通システム要件書」を参考に、「多機能 IC チップフレームワーク要件書」が取りまとめられた。この取りまとめに際し、次のような課題が明らかになった。

・多機能 IC チップは、耐タンパ性の高い部品として機器に組み込まれ、機器内の利用権等を管理することができる。しかし、このような多機能 IC チップを搭載した機器は現状存在しない。今後、多機能 IC チップによるサービスを本格的に普及するためには、セキュリティの高いサービスを提供できるように、多機能 IC チップ搭載機器そのもののセキュリティ機構を検討することが必要である。
・また、これまでは、多機能 IC チップ搭載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きた。しかし、多機能 IC チップ搭載機器のライフサイクルは、IC 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。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も併せて整理していく必要がある。

そこで、本テーマでは、多機能 IC チップフレームワークを利用したシステムの実用化及び普及を展望し、以下に示す調査研究を行った。調査研究の概要を下記の図 5-1に示す。

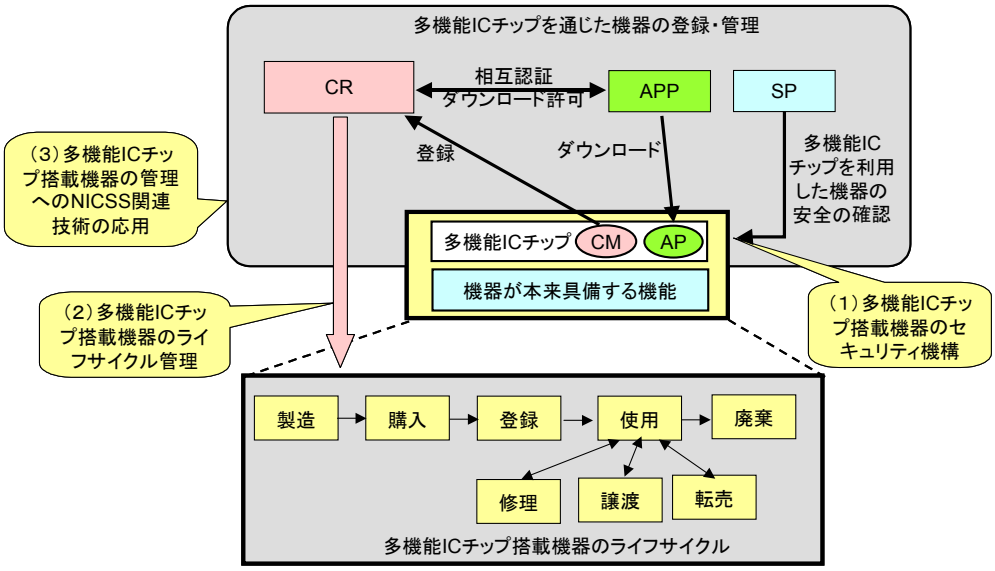


図5-1　調査研究の概要

5．2　検討の対象と機器のモデル化

図 5-2に示すように多機能 IC チップを搭載した機器と、機器に関連するさまざまな場面において機器を操作・運用管理する主体（ここではプレーヤという）及びその役割が、本検討の対象である。

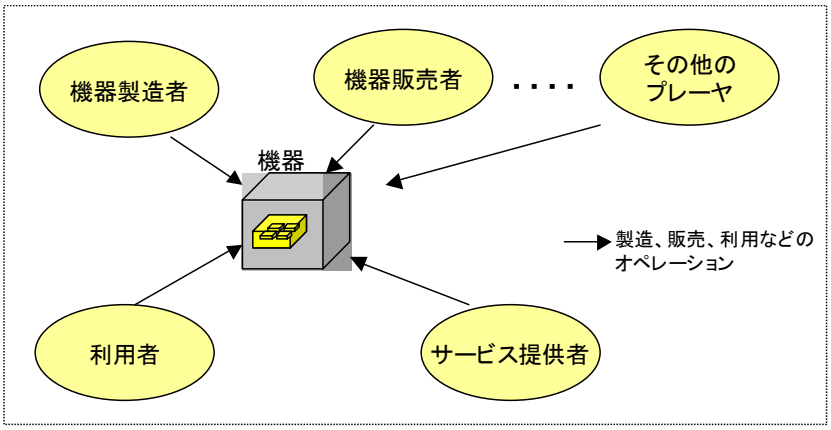


図5-2　検討の対象

また、5．3以降の検討を容易にするために、多機能 IC チップ搭載機器の機能を抽象化し、これを機能モデルとする。機能モデルを図 5-3　機器の機能モデルに示す。

機能モデルは①機器ハード、②機器 AP、③多機能 IC チップ（チップハード／チップ AP）の構成部品からなり、人あるいは他の機器に対して提供されるサービスは、機器 AP とチップ内のチップ AP が連携することで実現される。

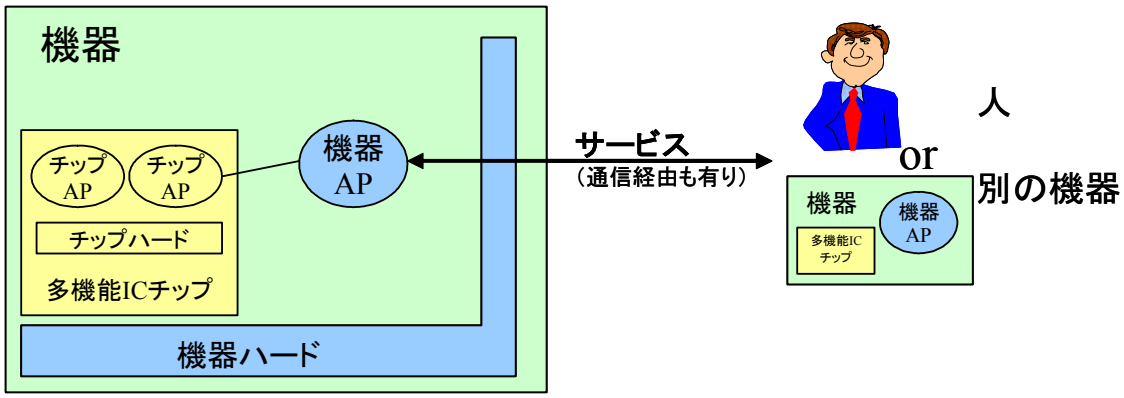


図5-3　機器の機能モデル

5．3　多機能 IC チップ搭載機器のセキュリティ機構について

多機能 IC チップを搭載することによって何が安全になるのか、またどのように安全になるのかについて機器の機能モデルを前提に検討した。

5．3．1　多機能 IC チップ搭載機器の安全性について

多機能 IC チップを搭載した機器は搭載していない機器と比べて、チップ AP と機器 AP が連携して提供されるサービスが安全になると考えられる。ここでは、どのようにサービスが安全になるのかを検討する。なお、本研究では「安全性を脅威とその防御策で記述できる」ものとしてとらえる。

安全性を明らかにするために、多機能 IC チップの基本機能から導き出される基本サービスをもとに防御できる脅威について検討する。多機能 IC チップを利用することによって、防御できる脅威は、①盗聴、②なりすまし、③不正侵入、④改ざん、⑤否認、⑥不正読み書きであると考えられる。防御できる脅威を図 5-4に示す。

これらに脅かされる可能性のあるサービスでは、多機能 IC チップを搭載することでそれぞれの脅威から守られ、安全にサービスを提供するまたは享受することができるようになる。

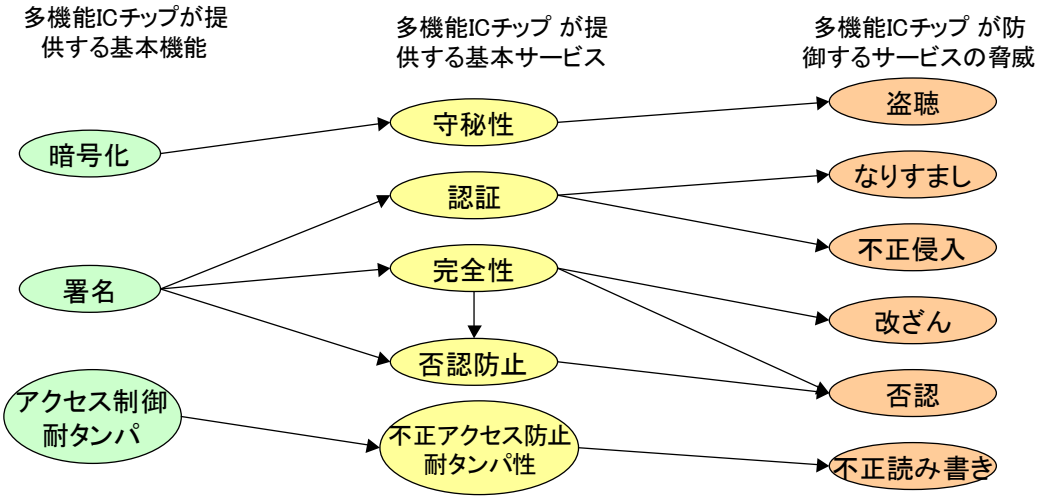


図5-4　防御できる脅威

5．3．2　多機能 IC チップ搭載機器の安全性の確認方法

現在、利用者が機器を購入する時には、その品質や安全性がよく分からないまま選択しないように、また機器の取扱に失敗するなどの不利益を被らないように、各種の品質表示や認証マーク等が活用されている。

多機能 IC チップ搭載機器においても、利用者が安心して機器を購入し利用できるように、安全性認定マークの制定が必要と考える。そのためには、業界ごとに機器の安全基準を規定し、それを評価及び試験する「第三者認証機関」の設立が必要となる。

また、業界毎の認定マークとは別に、総括的な製品システムのセキュリティ評価方法であり、国際的なセキュリティ評価・認証制度である ISO／IEC15408 の「コモン・クライテリア（Common Criteria）」や、「FIPS 140-2(Federal Information Processing Standard：連邦情報処理規格)」からも多機能 IC チップ搭載機器について認証を受けることが望ましい。

5．3．3　相互認証フレームワークと安全性

多機能 IC チップフレームワークの相互認証フレームワークの特徴は、次の 3 点である。

①第三者認証機関の公開鍵証明書を信頼して、対象を認証する。
②認証の対象は、者（プレーヤ）と物（機器）である。
③正当性の確認であり、安全性の確認について規定していない。

フレームワークにおけるプレーヤの認証を図 5-5に示す。者（プレーヤ）の認証は、機器登録認定機関（RC）が発行する公開鍵証明書を信頼して認証する。

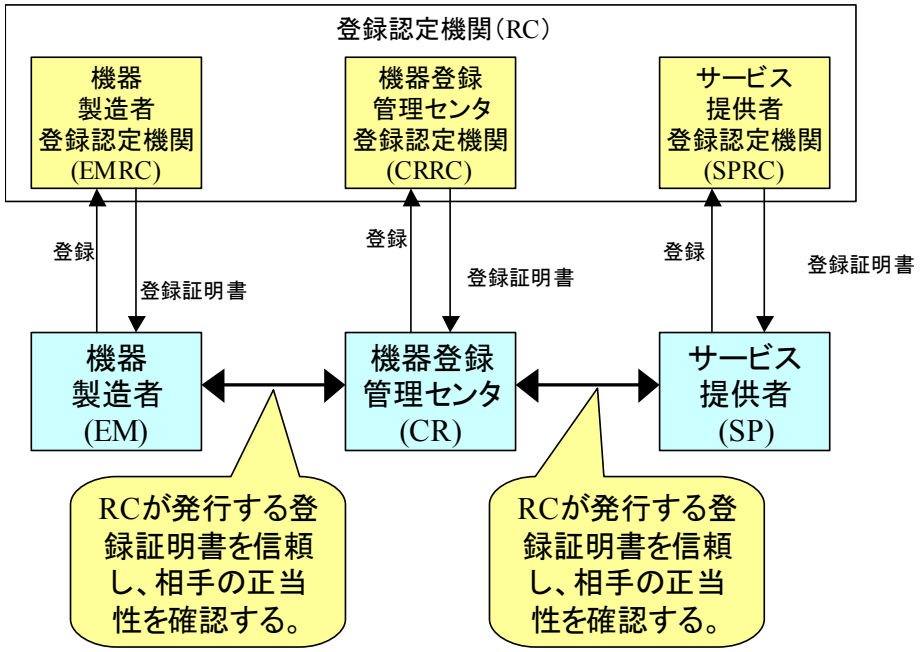


図5-5　フレームワークにおけるプレーヤの認証

フレームワークにおける機器の認証を図 5-6に示す。物（機器）の認証は、機器に証明書を書き込んだプレーヤを信頼し、その証明書を利用して認証する。

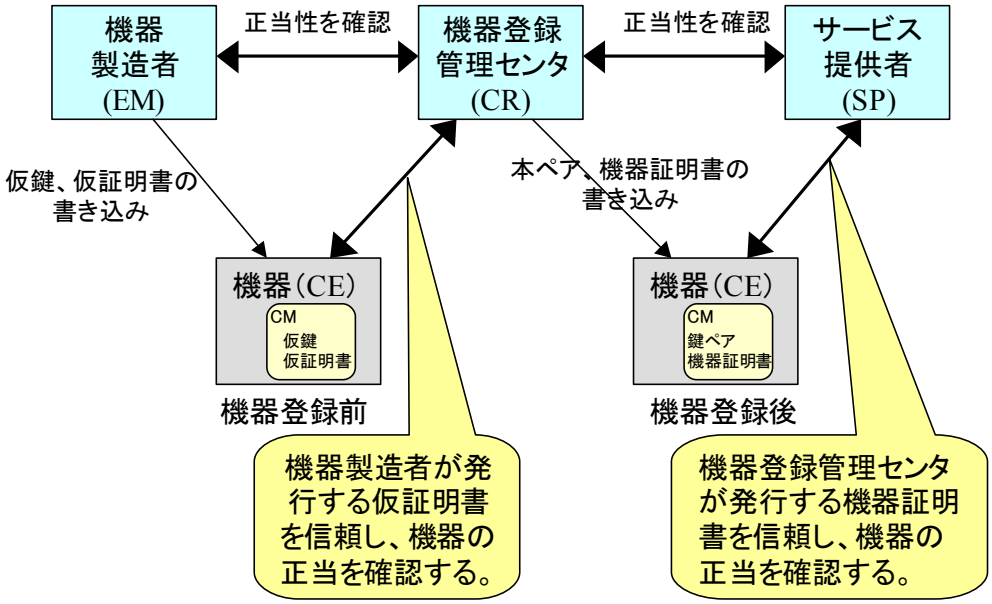


図5-6　フレームワークにおける機器の認証

この相互認証フレームワークは、不正なプレーヤや機器が入り込むという脅威に対して防御することができるので、安全性を確保していると考えられる。

5. 4　多機能 IC チップ搭載機器のライフサイクル管理について

「多機能 IC チップフレームワーク要件書」に基づき、多機能 IC チップを搭載した機器が「機器登録管理センタ」に登録・管理されることで、多機能 IC チップ上に複数のアプリケーションプログラムが搭載されサービスを利用できることを想定し、このサービス利用におけるさまざまな手続や機器（または構成部品）の運用状態変化を機器のライフサイクルと捉え、各手続における運用要件について検討を行った。さらに多機能 IC チップフレームワークのプレーヤによる機器のライフサイクル管理についてプレーヤ間の役割や管理上の課題について検討した。

5. 4. 1　多機能 IC チップ搭載機器のライフサイクルと管理

利用者が多機能 IC チップ搭載機器の機能を使ってサービスを利用するためには、幾つかの手続が必要である。ここでは、以下のような手続を想定する。この手続に対する処理フローを図 5-7に示す。

(1) 機器購入からサービス利用まで
(2) サービスの追加変更
(3) サービスの利用契約解除
(4) 機器更改
(5) 機器休止、譲渡
(6) 機器失効
(7) 機器紛失や故障など

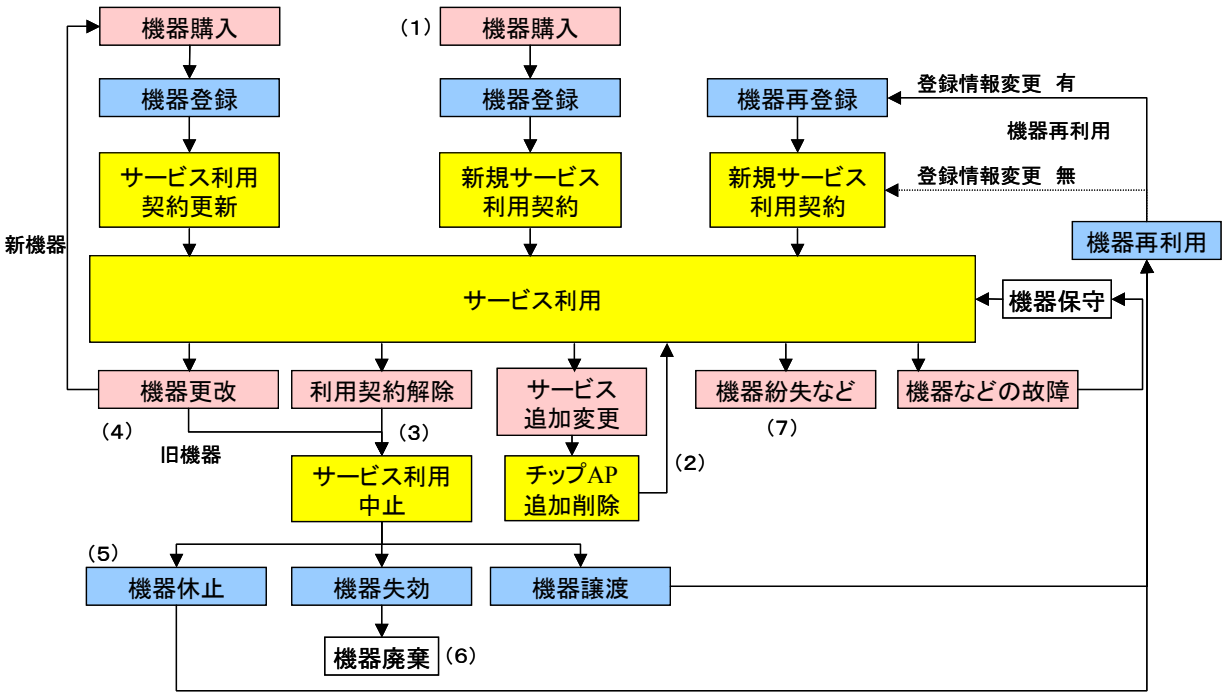


図5-7　多機能 IC チップ搭載機器を使ったサービスに関する手続のフロー図

これら手続は利用者（保有者）が主体となって、サービス提供に関係するプレーヤとの間で処理が行われる。この手続に伴い、機器構成部品の運用状態はさまざまに変化する。この変化を踏まえて、多機能 IC チップフレームワークのプレーヤによる機器のライフサイクル管理とプレーヤ間の役割や管理上の課題について、次に検討する。

機器は、サービス手続の違いにより構成部品毎で運用状態が変化することから、機器内に運用状態を保持できる機能を有したほうがよいと考えられる。また各プレーヤは、直接構成部品にアクセスして運用状態を確認するだけでなく、プレーヤ内でも運用状態の情報を保持・管理することが望ましい。さらに機器には故障を修理しサービス利用を再開することも想定されるため、各プレーヤは構成部品の保守や修理責任が発生しうる。

上記を踏まえ、各プレーヤの機器の運用管理に関する役割を以下のように分担する。

・多機能 IC チップ（チップハードを含む）の運用状態管理･･･機器登録管理センタ
・サービスの運用保守とチップ AP 及び機器 AP の保守及び運用状態管理･･･サービス提供者
・機器ハード（チップハードを含む）及び機器全体の保守･･･機器製造者
・機器の動作及びサービス提供の状態確認･･･利用者

利用者が機器を使ってサービスを利用するための手続と各プレーヤによる機器の運用状態管理をモデル化したものを図 5-8に示す。

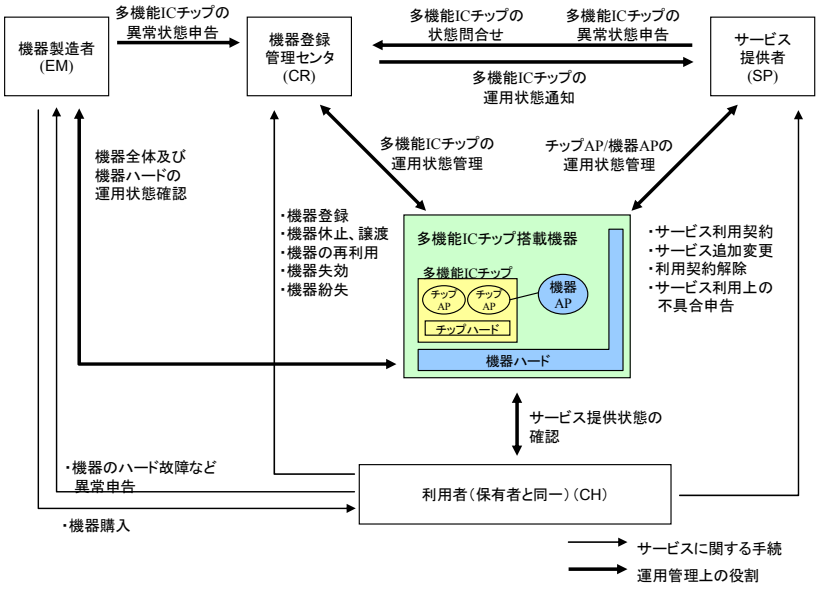


図5-8　多機能 IC チップフレームワークにおけるライフサイクル管理モデル

機器登録管理センタは機器を登録することで、多機能 IC チップに対してチップ AP のダウンロードを可能にするとともに、多機能 IC チップの運用状態管理を開始する。サービス提供者が多機能 IC チップの有効性（登録の有無や運用状態）を機器登録管理センタへ問い合わせた場合には、機器登録管理センタはこれに回答しなければならない。

上記のほか、利用者が機器を紛失した時の手続とプレーヤによる機器の運用状態管理、機器の不正検知によるサービス提供者からの運用状態通知、機器の故障修理による機器製造者からの運用状態通知に関してもモデル化を図った。その結果、機器のライフサイクル管理は、機器の利用目的や安全性などさまざまな観点から保守体制も含めた運用ポリシーとして、機器を利用する業界内で決定されるべきものであることが分かった。

5. 5　多機能 IC チップ搭載機器管理への NICSS 関連技術の応用と課題の抽出

IC カード分野及びその発展分野で実績を積み重ねてきた NICSS 関連技術に関する検討を基礎として、多機能 IC チップ搭載機器を活用したサービスの展開ならびにその管理機構の実現に向けた課題を整理した。

5. 5. 1　多機能 IC チップ搭載機器を活用したサービスにおける論点

IC カードと多機能 IC チップ搭載機器とでは、サービスモデルが大きく異なる場合がある。多機能 IC チップフレームワークと IC カードを対象として運用されている NICSS フレームワークにおいても、以下のような相違点を持つ。

- カード供給者に対応するプレーヤとして、多機能 IC チップを製造するチップ供給者と機器製造者に分離。
- それぞれのプレーヤを登録認定する機関として、チップ供給者登録認定機関と、機器製造者認定機関を設置。
- 機器はカードのような配布ではなく、提供（購入）というオペレーションへの変更であるため、カード発行者に対応するプレーヤとして、機器を登録管理するプレーヤとしての機器登録管理センタを設置。（機器登録というオペレーションも追加）
- カードの場合は、カードとカード保有者は 1 対 1 であったが、機器の場合は、人と結び付かない機器もあることから、機器と保有者を分離。

上記の課題の論点として、以下の項目を取り上げた。

- 多機能 IC チップフレームワーク要件書におけるセキュリティ要件の修正。
- セキュリティ評価認証の適用可能性。
- 多機能 IC チップ搭載機器の状態管理に関するプレーヤモデル。

5. 5. 2　多機能 IC チップフレームワーク要件書におけるセキュリティ要件の修正案

多機能 IC チップフレームワーク要件書の 2. 3 セキュリティの考え方では、オペレーションに対する脅威について示されているが、結局、対策はプレーヤへのセキュリティ要件となるので、最初からプレーヤへの脅威として示すほうが良く、図 5-9 のように修正することが望まれる。

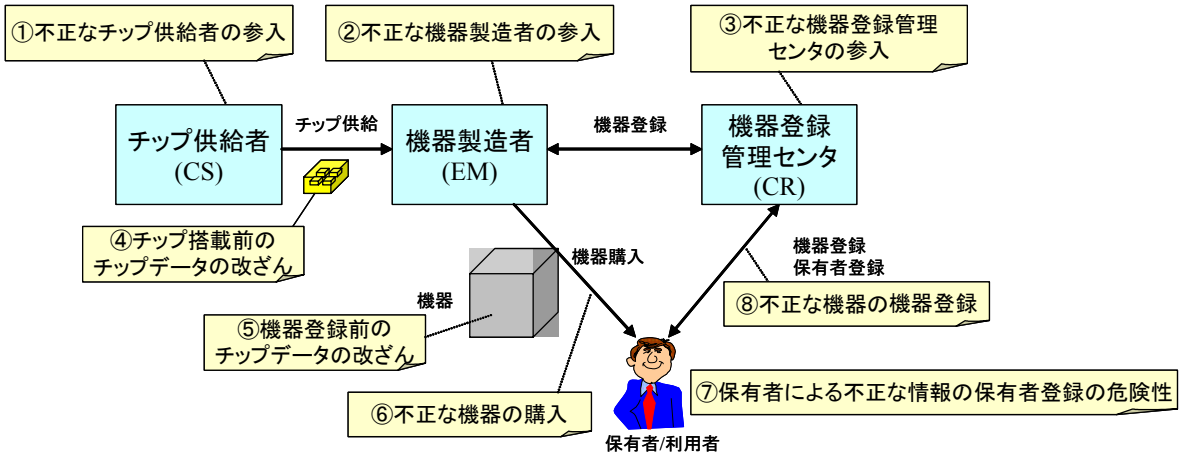


図5-9　多機能 IC チップフレームワークのセキュリティ脅威（改訂後）

図 5-9の脅威に対する対策は以下の表 5-1 ようになる。

表 5-1　多機能 IC チップフレームワークのセキュリティの脅威に対する対策

	脅威	対策
①	不正なチップ供給者の参入	チップ供給者登録認定機関への登録認定
②	不正な機器製造者の参入	機器製造者登録認定機関への登録認定と、発行された公開鍵証明書による身元の明確化と PKI による相互認証
③	不正な機器登録管理センタの参入	機器登録管理センタ登録認定機関への登録認定と発行された公開鍵証明書による身元の明確化と PKI による相互認証
④	チップ搭載前のチップデータの改ざん	チップ供給者による輸送鍵の設定とチップの耐タンパ性
⑤	機器登録前のチップデータの改ざん	機器製造者による仮鍵の機器の仮鍵と仮証明書の設定と耐タンパ性
⑥	不正な機器の購入	機器認証機関発行の機器認証マークや機器製造者登録認定機関発行のリストによる機器製造者確認などさまざま
⑦	保有者による不正な情報の保有者登録の危険性	住所・氏名・電話番号などの確認や IC カードによる個人認証など方式はさまざま
⑧	不正な機器の機器登録	機器製造者の公開鍵証明書と仮鍵、仮証明書による機器の製造者の確認

5. 5. 3　セキュリティ評価と機器認証機関

セキュリティ評価の対象について考察した。

セキュリティ評価の対象としては、以下のものがあると考えられる。

①チップのセキュリティ評価（チップ供給者が実施)。

②チップ及び周辺モジュールのセキュリティ評価（機器製造者が実施)。

③機器を利用したサービスのシステム評価（サービス提供者が実施)。

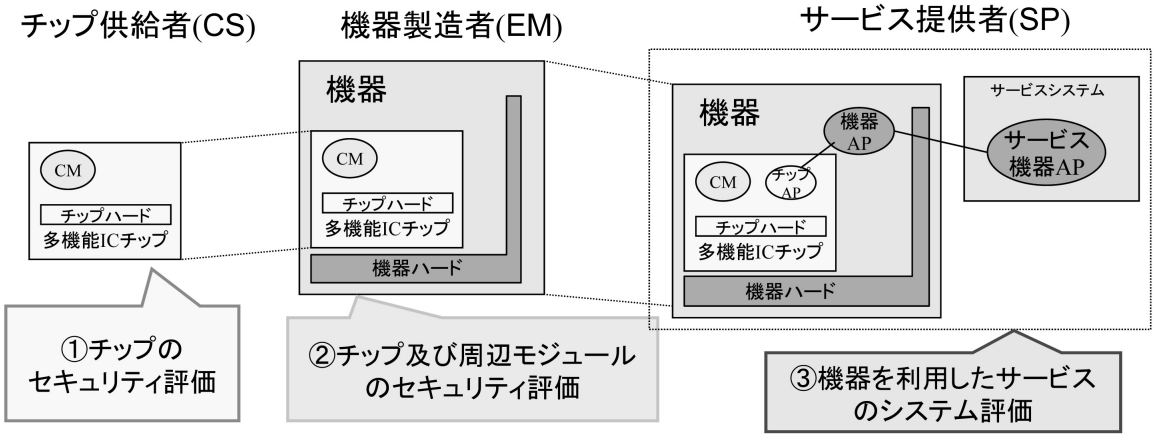


図5-10　セキュリティ評価の対象（その 1）

さらに評価の対象としては、以下も考えられる。

④外部プレーヤのバックエンドシステムのシステム評価（機器登録管理センタ実施)。

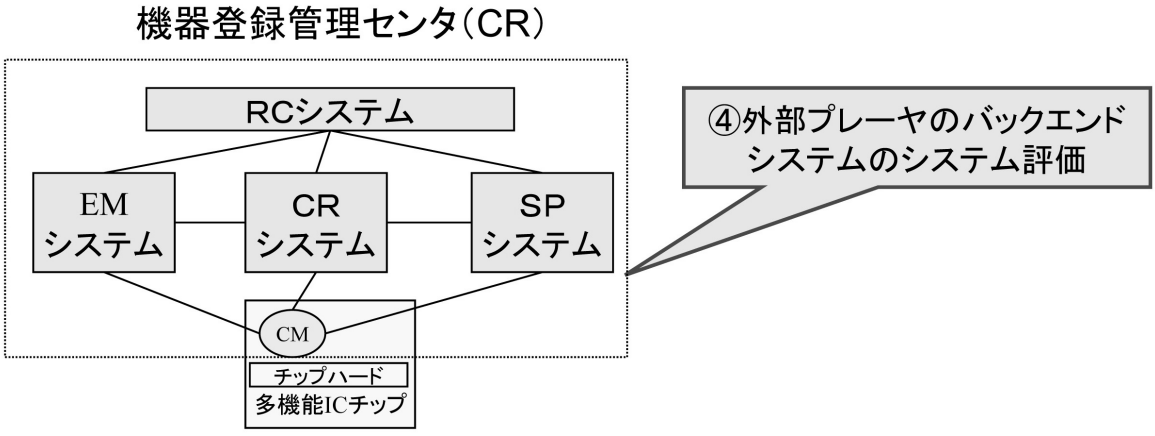


図5-11　セキュリティ評価の対象（その 2）

セキュリティ評価に ISO／IEC15408 を適用する場合、製品設計の上流工程でセキュリティ設計仕様書に相当する「セキュリティターゲット（Security Target：ST)」を作成する。セキュリティターゲットには、以下の各ステップを記載する。

1）対象とする製品に関係するセキュリティ脅威の機能及び、これに対抗するためのセキュリティ対策を明らかにする。
2）ISO／IEC15408 が提供する機能要件集を活用しながら、対策として製品に組み込むべきセキュリティ機能をなぜこの機能で必要十分かという根拠とともに記述する。
3）セキュリティ機能を正しく実装することを保証するための開発者への要求事項と保証の手段を記述する。

①のチップのセキュリティ評価についてはこれまでに幾つかの評価が実施されており参考にできるが、②については対象とする機器が多種多様なので、上記(1)～(3)のステップを実施しなければならない。さらに、③機器利用のサービスシステム評価、④バックエンドシステムのシステム評価に関しては、どのようにセキュリティ評価を行なえばよいかを含め今後の課題である。

5．5．4　機器認証機関とプレーヤ

機器の安全性を評価する機器認証機関が設立されたと仮定して、機器認証機関が多機能 IC チップフレームワークのプレーヤとして必要かどうかを検討した。

安全性が認証された機器は、その機器製造者に対して、機器認証証明書（仮称）と、安全マーク（S マーク）の表示許可を与えると考えられる。安全マークは、利用者が機器を購入する場合の判断基準となり、機器認証証明書は、機器登録管理センタ（CR）やサービス提供者（SP）がそれを参照して、機器の安全性を確認することができる。

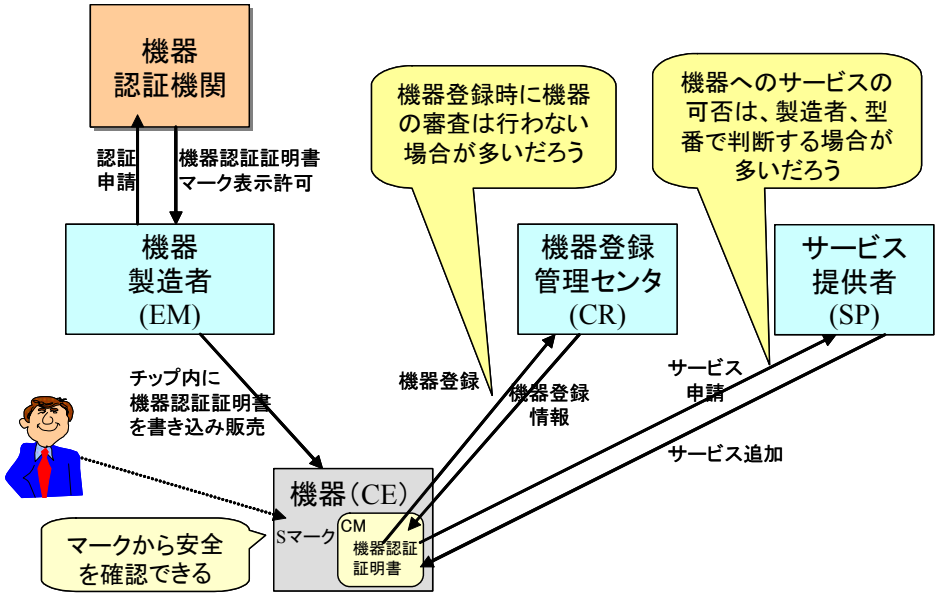


図5-12　機器認証機関の位置付け

5．5．5　多機能 IC チップ搭載機器のライフサイクル管理に関する課題

多機能 IC チップ搭載機器のライフサイクル管理には、機器の所有と運用管理に関する課題がある。図 5-13に IC カード及び多機能 IC チップ搭載機器におけるプレーヤ間の関係を示す。IC カードの場合、カードの所有はカード発行者に帰属するためカードの運用管理はカード発行者の運用ポリシーで実施することができる。一方、機器の場合、その所有は保有者にあることから機器登録管理センタが多機能 IC チップを運用管理する際には、保有者からの許諾が必要と考えられる。また保有者と利用者が異なる場合には、利用者も保有者との間において機器の使用に関する許諾が必要であると思われる。

サービス提供者としても、機器登録の有効性や多機能 IC チップの運用状態を知ることはサービス提供において必要な要素であるものの、サービス提供者自身が個別に管理するのは非効率であり費用面においても負担が大きくなると考えられる。そのため、機器登録管理センタが一元的に状態管理することにメリットがある。

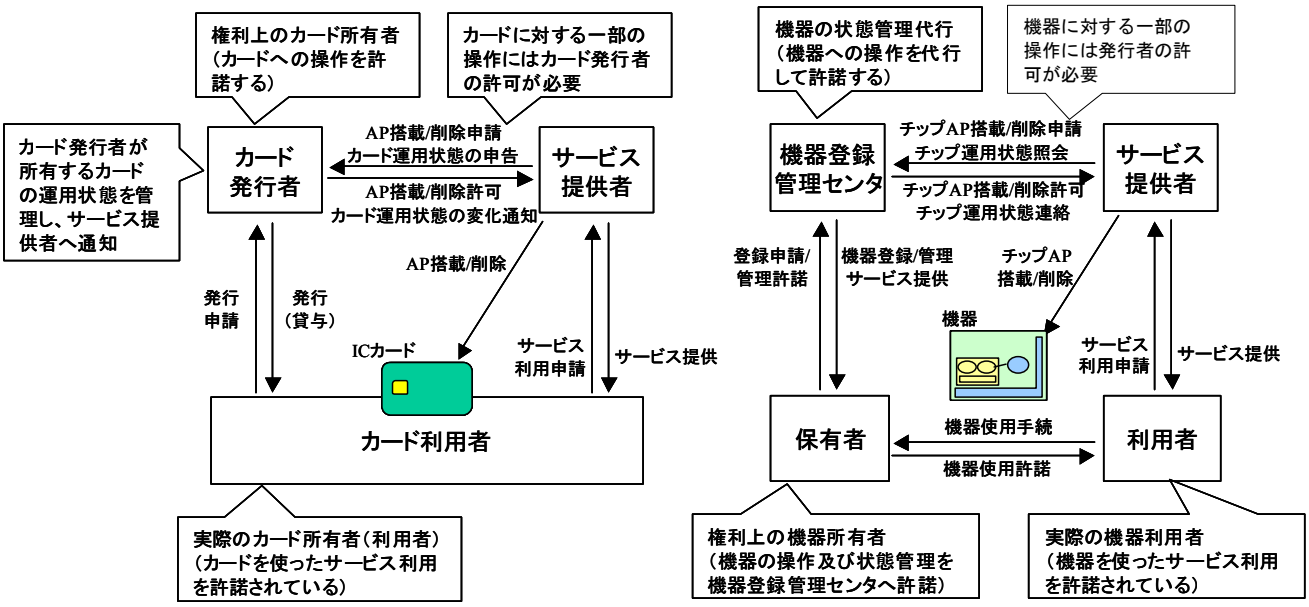


図5-13　IC カード及び多機能 IC チップ搭載機器におけるプレーヤ間の関係について

このように機器登録管理センタによる多機能 IC チップの運用状態管理は、サービス提供者のサービス提供方針や運用ポリシーによって必要性が検討され、サービス提供者の管理業務の一部を代行するサービスとしてとらえる一方で、利用者がサービスを利用できる条件として機器登録管理センタへの機器登録とともに、保有者による機器登録管理センタへの機器の運用状態管理許諾など特別な手続を必要とするのではないかと考えられる。

この手続の中で、本研究では機器登録のタイミングを利用者（保有者）が機器を購入後に実施する場合について検討を行ったが、この他に機器製造時や機器購入時の登録も想定される。利用者への利便性や不正流通の防止などの観点から、機器登録後の販売流通のあり方や運用状態管理についてさらに検討を重ねる必要がある。

また、機器の譲渡や再利用、故障など特徴的な手続について検討を行ったが、これらは必ずしも実施されるものではなく、機器の利用目的や業界の運用ポリシーによって選択されると考えられる。また、機器登録管理センタが保有者情報を管理しない場合には、機器紛失や機器失効による機器の運用状態管理が正常に実施されるための仕組み作りが今後の課題となる。

5. 6　まとめ

5. 6. 1　多機能 IC チップ搭載機器のセキュリティ機構に関する考察

多機能 IC チップ搭載機器のセキュリティ機構の検討では、多機能 IC チップ搭載機器の機能を抽象化した機能モデルを定義して、多機能 IC チップを搭載することによって何が、どのように安全になるのかを検討した。多機能 IC チップには暗号機能、署名機能、アクセス制御機能、耐タンパ機能が備わっている。これらの機能は、盗聴、なりすまし、不正侵入、改ざん、否認、不正読み書きの脅威を防ぐことができ、これらの脅威に脅かされているサービスでは、多機能 IC チップを搭載することによって、安全にサービスを提供できるようになることが確認できた。

また、多機能 IC チップ搭載機器がセキュアなサービスを提供するために、機器として必要であるセキュリティ要件について検討した。チップハード及びチップ AP については、過去に IC カードチップに関する PP（プロテクションプロファイル）の検討が行われているので、それが参考となった。しかし、機器ハード、機器 AP については、多種多様の機器とサービスがあるため規定は難しい。

機器全体を耐タンパにしてセキュアにすることは、コストもかかり現実的ではない。チップハードとチップ AP はセキュアであるとし、そのチップ AP と機器 AP が提供するサービスによって、人や他の機器に対してセキュアなサービスを提供するだけではなく、機器自身の機器 AP や機器ハードをセキュアに変えていくことは可能であると考える。このようにして機器の中のセキュアな部分を多くすることができる。ただし、セキュアにするにはコストがかかるので、機器においてセキュアでなければならない部分を極小化し明確にすべきである。

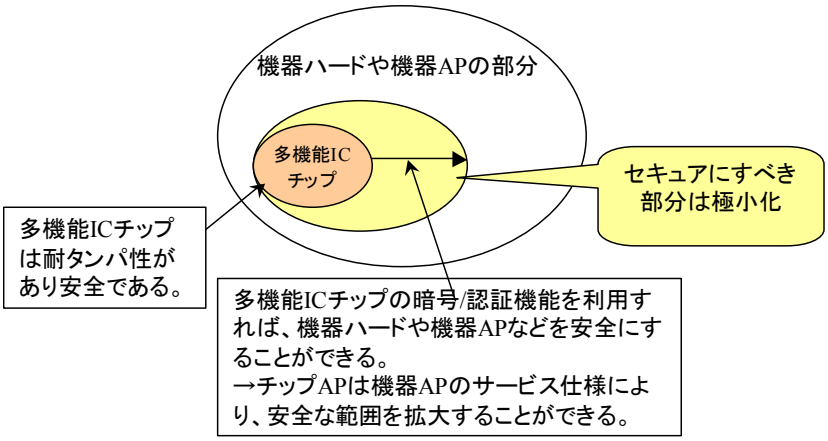


図5-14　セキュア部分の拡大と極小化

フレームワークのプレーヤに適用することはしなかったが、機器の安全性を向上させるためにも機器を認証する機関の設立は必要であり評価基準も含め今後の検討事項である。

NICSS フレームワークは、ネットワーク経由でカード AP の追加・削除が安全に行えることを目的にしており、多機能 IC チップフレームワークにおいても、ネットワーク経由でチップ AP の追加・削除が安全に行えることを目的にしている。この安全のために、プレーヤ、

機器、AP の認証を中核として要件を規定している。ただし、この場合の機器というのは、特殊なチップ AP である CM であり、機器全体ではない。この意味で機器ハードや機器 AP、さらにはチップ AP と機器 AP が提供するサービスについては対象外として規定がなく、機器ハード及び機器 AP に対するセキュリティ要件の記述もない。

IC カードの場合は、機器 AP が無く、リーダライタから直接カード AP を起動しサービスを提供することができたが、機器の場合はサービスを提供するためには機器 AP が必要である。NICSS の基本方針はサービスや業界に依存しないことであるが、多機能 IC チップフレームワークにおいて、この機器 AP をどのような位置づけにするかは今後の課題である。

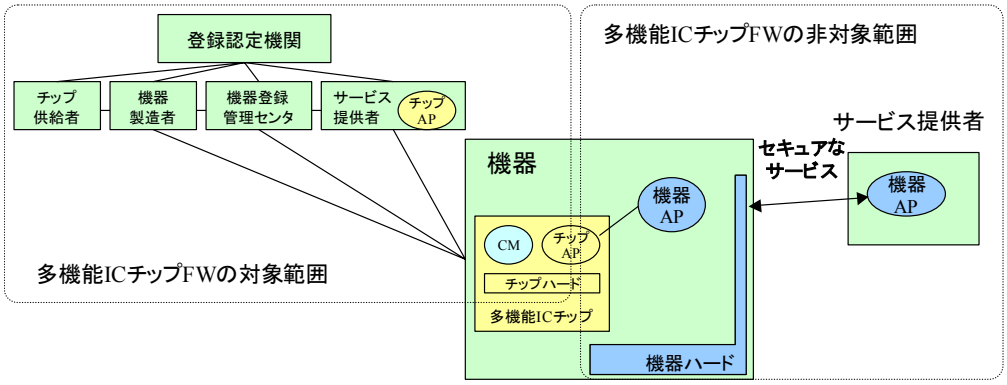


図5-15　機器 AP の位置付け

5. 6. 2　多機能 IC チップ搭載機器のライフサイクル管理に関する考察

多機能 IC チップ搭載機器のライフサイクル管理では、まずはモデル化した機器構成品について運用状態を定義し、サービス提供に関するさまざまな手続、特に機器の譲渡や再利用、故障修理といった特徴的な手続を想定して構成品の運用状態の変化や運用要件、手続上の課題について検討した。これを受けて、多機能 IC チップフレームワークのプレーヤによる機器構成品の運用管理モデルとプレーヤ間の役割や管理上の課題について検討した。機器の運用管理は保守にも関係することから、機器が利用される目的や求められる安全性などさまざまな観点を考慮した運用ポリシーとして機器を利用する業界内で決定されるべき事項であると考える。

そして、機器のライフサイクル管理における機器の所有と運用管理について IC カードの場合と比較し、その違いと課題を明確にした。特に機器登録管理センタについてはサービス提供者や保有者との関係について再度整理し、保有者の持つ機器に対する権限やサービス提供者の要求を踏まえた役割、手続を検討する必要があると思われる。

6. まとめ

6. 1　成果

テーマ 1-1 においては、今年度の研究開発・実証事業を通して機器登録管理センタを構築し、実装した機器登録機能をテーマ 2、3 で使用する機器を登録・利用することによって、システムの機能を確認することができた。

機器登録においては事後登録機能を開発し、主に以下の 3 つの内容について実現した。

①利用者による事後登録を実現するための多機能 IC チップ搭載機器と機器登録管理センタの相互認証

②機器登録における多機能 IC チップ搭載機器に応じた登録インタフェース

③機器登録管理センタへの機器情報登録

また、事後登録機能の開発にあたっては、登録におけるセキュリティの確保を考慮し、多機能 IC チップフレームワークにおいて想定されているセキュリティに対する脅威への対応を考慮した設計を実施した。

これらを通して、利用者の手により事後登録される機器について、当該機器に搭載されている多機能 IC チップの正当性を確認し、機器登録管理センタで機器情報を登録・管理できることを確認した。また、テーマ 2、3 で利用される多機能 IC チップ搭載機器を登録し、アプリケーションをダウンロードできることを機能的に検証できた。

更に、機器登録を行った機器の利用を通して、被験者にアンケート・ヒアリングを実施することにより、サービス性や、事業性についての意見を収集することができ、多機能 IC チップを活用したサービスシステムの基盤構築に向けて、利用者・事業者のニーズの傾向を把握することができた。

テーマ 1-2 の研究においては、可搬型リーダライタ機器の基本要件を整理した。実社会で可搬型リーダライタによって、場所や時間にとらわれないサービスが提供された場合のサービスの可能性と、そうしたサービスが提供された場合に考慮すべき事項への対策としての追加要件を検討した。このことにより、可搬型リーダライタがメーカ各社から提供された際の相互互換性を確保するための最低限の要件が整理され、メーカによる機器の開発・提供に向けた基礎的な要件を整理することができた。

テーマ 1-3 の研究においては、多機能 IC チップ搭載機器におけるセキュリティ要件と、ライフサイクル管理における運用要件を整理した。これらの要件を考慮することにより、機器製造事業者等に対する機器の提供に際しての留意点等が整理され、機器製造事業者の参入を促すものと思われる。

6. 2　展望と課題

本事業において、機器登録管理センタにおける機能を実装し、機器登録管理センタとしての機能性の検証を実施したが、今後のサービス提供を検討するにあたって、主に以下の 3 つの点についての課題が見えてきた。

・機器登録管理センタへの機器登録に関連して、登録する機器の認定の方法について

現状の仕組みでは、メーカに対して認証を与え、製造された機器を信頼しているが、メーカが製造した機器自体を認定する仕組みの必要性についての検討である。サービスの提供に向けて、機器の正当性を確保していくためには今後必要な検討であると思われる。

・機器保有者登録について

機器登録管理センタの運用において、機器を登録するだけでなく、保有者情報も管理するかについての検討である。機器を管理している人としての保有者情報を登録することによって、より確実に機器を管理することができる。しかし、匿名性を持った形でのサービスの利用や個人情報の扱い方等を含めた検討が必要と思われる。

・機器登録管理センタの運営ビジネスモデルについて

機器登録管理センタを実社会の中で運営する場合の運営主体についての検討である。本事業において実施したアンケート・ヒアリングからもさまざまな意見が挙げられており、その中では運営主体に対する要望や、関連する事業者間での合意形成の難しさについての意見があった。ビジネスとして展開していくにあたっては今後も検討を深め、ビジネスモデルを形成していく必要があると思われる。

Ⅱ－2

テーマ 2

登録センタの機能を活用したデジタルコンテンツ流通サービスの研究開発及び実証実験

1. 事業概要

1. 1　背景

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)」においては、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として「多機能 IC チップフレームワーク」について検討を行った。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。

また、平成 15 年度の事業の一環として、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を行った。その際には、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、著作権者や著作隣接権利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マルチメディア情報流通サービスにおける基本機能について研究を行った。さらに、アプリケーション開発を通じて実効性を検証し、多機能 IC チップフレームワークを基盤としたマルチメディア情報流通サービスの適用可能性の高さが確認できたところである。

一方で、具体的なサービスの実現に向けては、実際の機器への多機能 IC チップの搭載を含む、より実環境に近い形での実証と多機能 IC チップの破損や紛失の際の再発行といった実サービスを想定した機能拡張の必要性等が課題として指摘されている。

1. 2　目的

デジタルコンテンツ流通サービスの研究開発及び実証実験（以下「本テーマ」という。）では、多機能 IC チップが搭載されたデジタルコンテンツ再生機器（以下「デジタルコンテンツ再生機器」という。）を使ったコンテンツ流通サービスの事業化に向けた検証を行うため、以下の機能を研究開発することを目的とした。

- 機器登録管理センタ機能の研究開発及び実証実験（以下「テーマ 1」という。）で構築した機器登録センタに対して多機能 IC チップ搭載デジタルコンテンツ再生機器を登録する機能
- 利用権を持っているコンテンツに関しては複数の機器での再生を実現する機能
- 複数の機器で再生した場合でもコンテンツの利用料や権利料の分配を可能にするための利用者認証用 IC カードへのコンテンツ再生ログ保管機能
- コンテンツの利用期間制御を行うサービスを実現するためにデジタルコンテンツ再生機器内の多機能 IC チップにコンテンツ再生終了日時を保管する機能

1．3　実施概要

デジタルコンテンツ再生機器によるコンテンツ流通サービスの実施において必要となる機能の研究開発を行った。開発に際しては昨年度の事業成果を活用するとともに、多機能 IC チップ搭載デジタルコンテンツ再生機器をテーマ 1 で構築する機器登録センタに登録した。

実証実験においては、昨年度行った技術的基盤及び権利流通についての検証結果をもとに、本事業テーマ 1 において研究開発した基盤を活用して、サービス提供者側の要望を踏まえたより実サービスに近い形での適用可能性についての検証を行った。具体的内容は以下のとおりである。

- 多機能 IC チップを搭載したデジタルコンテンツ再生機器を使用し、機器登録管理センタへの事後登録により利用開始とすることで、より実サービスに近いものとした。
- 利用権を持つ人が、複数の機器で再生した場合でもコンテンツの利用が可能となり、かつ利用料や権利料の分配を可能となるよう再生ログを採り、実サービスへの有用性を評価した。（図 1-1参照）
- 多機能 IC チップフレームワークを活用したアルバムコンテンツに対する利用権管理を可能とし、流通サービス実現の可能性を実証した。

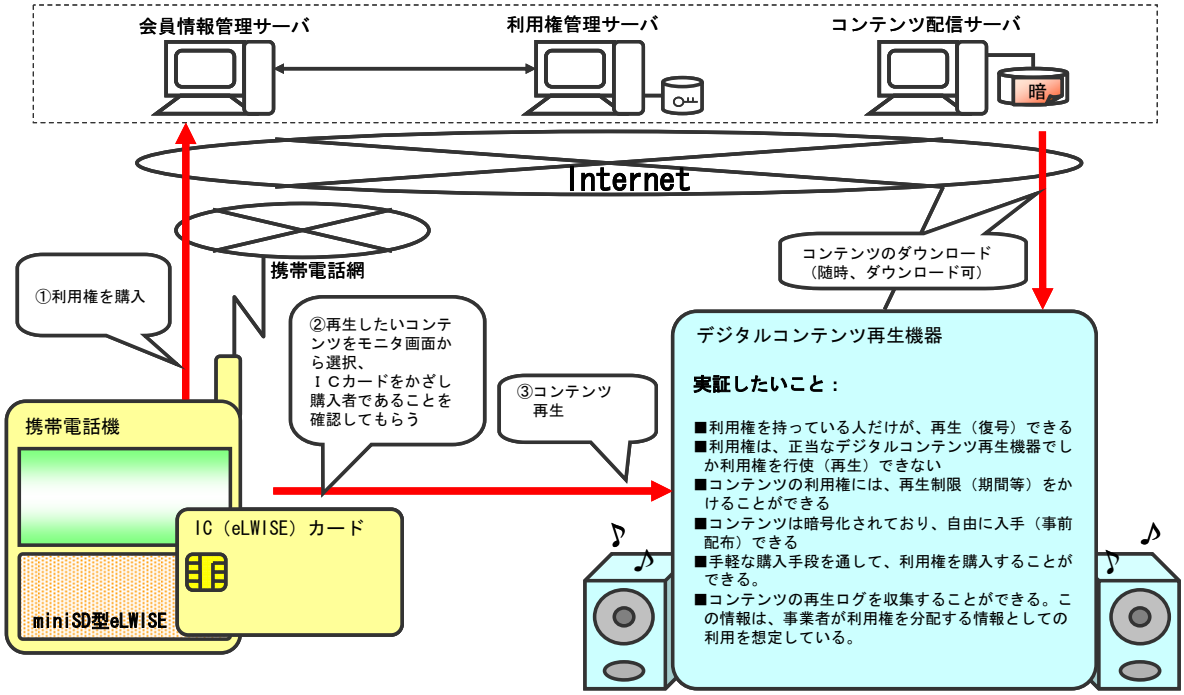


図1-1　本テーマの実施イメージ

1．4　実施体制

テーマ 2 の実施体制を図 1-1に示す。

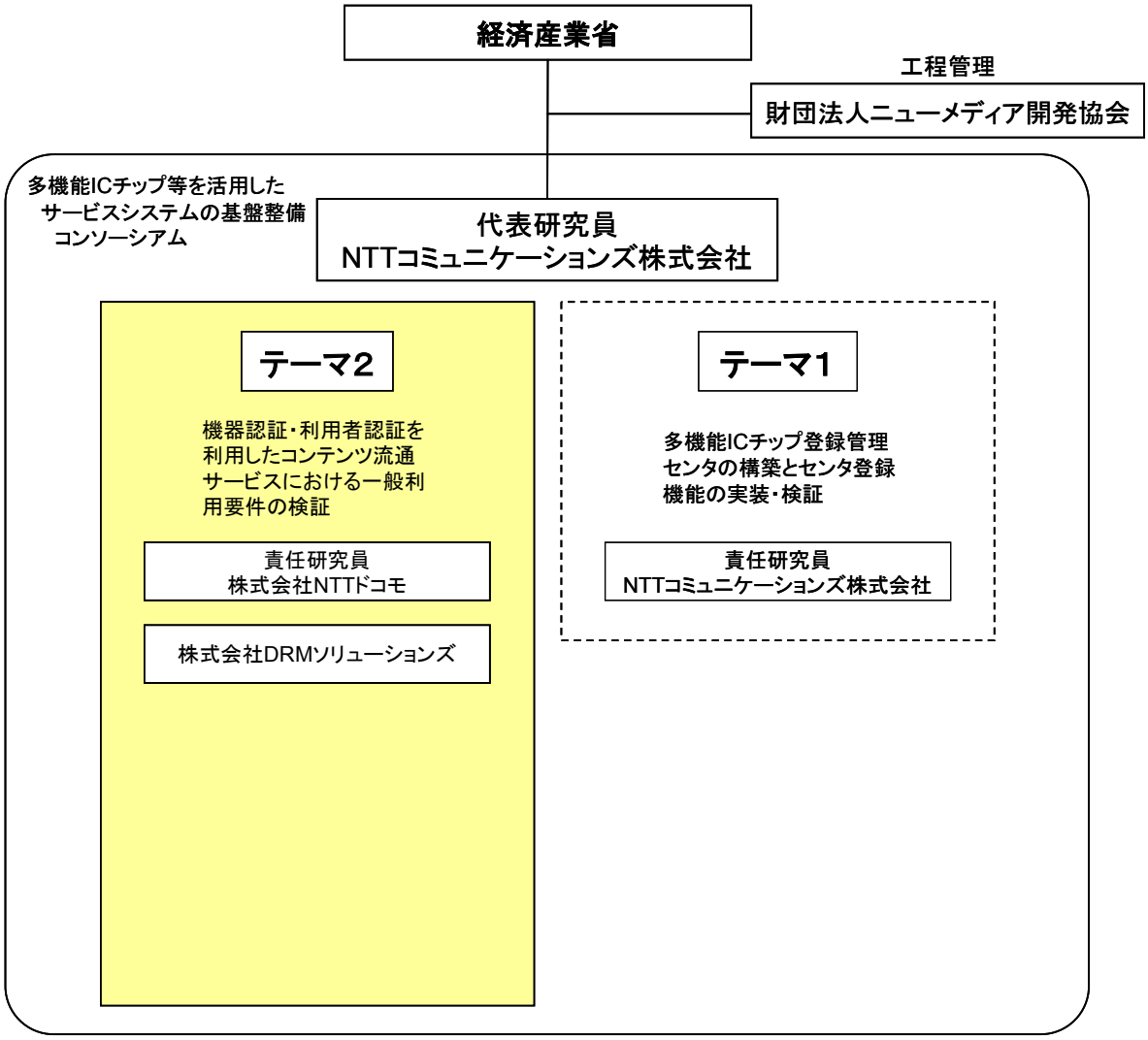


図1-2　実施体制図

2. 次世代コンテンツ流通サービスについて

2. 1　次世代コンテンツ流通サービスの概要

「次世代コンテンツ流通サービス」とは、現状のコンテンツ流通サービスの問題点を改善し、コンテンツの著作権を保護しながら、利用者が「安心」、「安全」、「便利」にコンテンツの流通・購入ができる仕組みを持った流通サービスのことである。次世代コンテンツ流通サービスは、認証や利用権情報の含まれていない状態の暗号化コンテンツを流通させ、これとは分離した形で多機能 IC チップ等に保存された個人や機器の認証情報・利用権情報が機器間を移動する。そして、利用権取得済みのデジタルコンテンツは携帯電話や PC、さらにはインターネット接続した情報家電や対応オーディオ等で多機能 IC チップ他を挿入することで再生可能となる。図 2-1に次世代コンテンツ流通のイメージを示す。

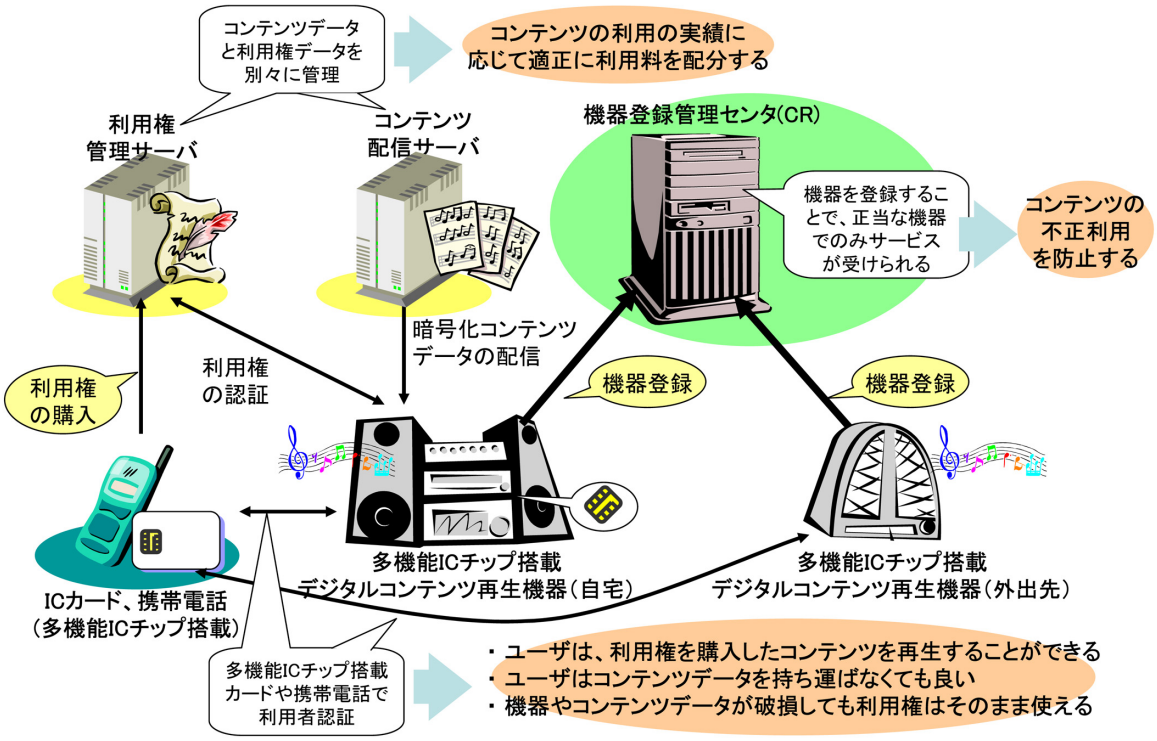


図2-1　次世代コンテンツ流通のイメージ

次世代コンテンツ流通サービスにおいては、「安全」、「安心」、「便利」なサービスモデルを実現することが重要となる。安全は権利者や事業者にとって特に重要であり、便利は利用者にとって特に重要である。安心は関係するすべての人の橋梁によって確立され享受される必要がある。

このようなサービスを実現するためには、正当な利用者が特定され、有料サービスでは正当な決済が行なわれ、正当な権利者、正当な事業者に対価が支払わなければならない。

利用者の使用する機器も正当な機器でなければならないし、その機器を使用する利用者も正当な利用者でなければならない。このようなシステムは、権利者との権利利用許諾契約記

載の条件を満足する形で条件が設定できる必要がある。

また、正当性が疑われる時の対策や保護システムが破壊された時の対策も備えていなければならない。このような対策や手続をコンテンツセキュリティの管理計画と呼ぶことができるが、サービス開始前に関係者の了解を得た管理計画によって、当事者間の紛争を避けるため第三者機関によって管理が実施されることが望ましい。以上は安全、安心を実現する上で欠かせないことがらである。

また、次世代コンテンツ流通サービスに使用するシステムは、安全性が確認されている国際標準または国際標準に準じた規格（内容が明らかにされているもの）に則していることが望ましい。この場合、誰もが安全性を評価することができるため、結果として安心につながり、さまざまなサービスが並存した場合に相互運用を実現する上で極めて重要である。相互運用は利用者の便利を実現する上で欠かせないものである。

これらが満足された上で、ユーザに便利を提供するシステムが実現されなければならなく、使い勝手の良さは極めて重要である。

これらのことから、次世代コンテンツ流通サービスに必要とされる基本的な要件を列記すると以下のようになる。

1. 権利者の認証
2. 事業者（サーバを含む）の認証
3. 個々の利用者の認証
4. 個々の機器の認証
5. 機器に搭載されるデジタル著作権管理（以下「DRM（Digital Rights Management)」という。）の認証
6. 現状十分だと認められる安全性を持った権利管理機構
7. 公開され誰でも安全性の評価や相互運用性の評価ができるシステム（国際標準準拠が望ましい)
8. 権利者との権利使用許諾契約に対応できる柔軟性を持ったシステム
9. 関係者の同意を得たコンテンツセキュリティの管理計画の制定
10. 同計画書に基づく管理
11. 使い勝手の優れた利用者システム
12. 利用者に受け入れられるサービス価格、端末価格の実現

次世代コンテンツ流通サービスに必要とされる基本的な要件のうち、今年度の研究開発・実証事業では、上記 3、4、5、6、7 の各項に対応したサービスの実証実験を行った。3 の利用者認証では携帯電話及び IC カードを用いた利用者認証、4 の機器認証では、機器として AV 機器を使用し多機能 IC チップによる機器登録機能を開発する（テーマ 1)。加えて、「8. 権利者との権利使用許諾契約に対応できる柔軟性を持ったシステム」という要件に対応したサービスの一例として、「まとまったコンテンツ」に対する利用権の発行と利用、権利料分配時に必要な利用ログの管理手法について実証した。（まとまったコンテンツによるサービスモデルについては2．3．2を参照）

2．2　多機能 IC チップフレームワークとの関係

本節では、次世代コンテンツ流通サービスと多機能 IC チップフレームワークとの関係について触れる。前節でとりあげた次世代コンテンツ流通サービスに必要とされる基本的な要件のうち「3.個々の利用者の認証」と「4.個々の機器の認証」に関係する利用者登録、機器登録、セキュアチップへのアプリケーションダウンロードの部分については、多機能 IC チップフレームワークを用いることができる。

多機能 IC チップフレームワーク利用の概要については本事業テーマ 1 に説明が加えられているので参照されたい。

2．3　次世代コンテンツ流通サービスのサービスモデルの例

以下に音楽を中心に個々のコンテンツ購入モデル、まとまったコンテンツの月定額モデル、多種類コンテンツ流通モデル、多種類流通モデルについてビジネスモデルの検討を行った。

2．3．1　個々のコンテンツ購入モデル

従来型の配信での流通モデルであり、これまでは携帯電話や携帯端末を対象としたヒット曲中心の流通であった。現状ある程度の実績を示し、今後の拡大も望めるが、趣味の多様化に対応した幅広いコンテンツの流通を実現するためには、さらなるサービスモデルの革新が求められる。

携帯電話、iPod サービス等に習い価格を 1 曲 100 円程度とし、前項のコストモデル例から音楽のみのダウンロード販売を行う場合に採算を取るとなると、月当たり約 30 万曲程度の販売曲数が必要となる。これは、1 人の利用者が仮に月平均 3 曲購入するとすれば、端末台数は 10 万台以上普及していなければならないことになる。これまでの配信では、一人当たり 2 曲を実現することは容易ではないといわれており、この場合採算を取るためには、15 万台以上普及していなければならないことになる。もちろん、価格を倍にして同じ曲数が売れるのであれば必要とされる端末普及台数は半分になる。魅力的でなおかつ安価なコンテンツを多数揃えることと端末の普及が、本サービスが機能するビジネスモデルには欠かせない。

2．3．2　まとまったコンテンツの月定額利用モデル

「まとまったコンテンツ」とはアルバムのように複数の曲の組み合わせで提供する形態のサービスを指す。1 曲単位の売り切りではなく、月額料金制など新しいサービスモデルが考えられる。

広く普及している類似のサービスとして、購入曲数を制限し月定額制を取り入れた携帯電話の着メロサービスを挙げることができる。このサービスは、通常の音楽分野では新しいサービスモデルとなるが、利用者にとってはその趣味の多様化に対応でき、権利者にとってはこれまで倉庫に眠っていた幅広いコンテンツの活用が可能となる。従来の流通では、在庫返品のリスクが伴うが、本流通でこのリスクがほぼ回避できることの効果は、事業者にとって極めて大きいと考えられる。

本モデルは個々の楽曲の購入にも対応できるため、上記2．3．1項の個々のコンテンツ購

入モデルも包含でき、リスクを回避したより確実なビジネスモデルを構築することができる。月額制のサービスの場合、一度その楽しさを理解してもらえれば、次の月も契約が継続されることが期待できることから受け入れやすいサービスとなる場合も考えられる。

ただし、まとまったコンテンツの魅力を増すためには、充実した解説の付加、解説の有無選択再生等に対応する必要がある。また、まとまったコンテンツの中のどの楽曲が利用されたか履歴（ログ）を取得することにより、利用料金を正当な権利者に支払う仕組みについて考案することが可能となる。

2．3．3　多種類コンテンツ流通モデル

音楽だけでなく映画等のビデオソフトやゲーム等、多種類のコンテンツを流通させることにより、固定費を大幅に増加させることなく、顧客の獲得や端末普及台数の増加をはかることができると考えられる。

コンテンツによって全く異なる権利保護方式や流通方式を採用した場合に比較し大きなコスト削減が可能であり、ビジネスリスクの回避にもつなげることが可能であろう。

2．3．4　多種類流通モデル

配信だけでなく、パッケージ流通や店頭端末での販売による流通も併用することにより、利用者が好みの流通形態を選ぶことが可能となる。これによりリスクを回避し売上の拡大、端末の普及も見込めると考えられる。

一方、権利保護の仕組み、コンテンツ ID、プロトコル等に互換性がある他のサービスについても、権利者や事業者からの許諾が得られれば、相互運用を行うことができ、コストの削減、売上の拡大、リスクの回避、端末の普及に寄与できる。これまではこのような統合サービスに適したシステムが存在しなかったため全く行なわれてこなかったが、これからのマルチメディア流通では欠かせない事柄と考えられる。

3. 次世代コンテンツ流通サービスの研究開発と実証実験

3. 1　実証実験の環境

3. 1. 1　概要

コンテンツ流通サービスシステムとしては、利用権データの生成・配信を行う利用権管理サーバ、携帯電話で会員登録を行うための会員情報管理機能とコンテンツ配信機能を同一躯体に組み込んだサーバを用意し、それぞれインターネットに接続した。

サービスを受ける利用者機器としては、インターネットに接続されている多機能 IC チップ搭載デジタルコンテンツ再生機器、会員登録手続及び多機能 IC チップを搭載し利用者認証を行う携帯電話または多機能 IC カードを用意し、テーマ 1 で研究開発される機器登録管理センタに機器登録してコンテンツ流通サービスの利用を開始した。

多機能 IC カードまたは多機能 IC チップ搭載携帯電話を利用者認証用機器として活用し、携帯電話については利用権購入手続においても利用した。

なお、デジタルコンテンツ再生機器には非接触 IC カードリーダライタ、スピーカー、赤外線リモコン、TV モニタが付属する。

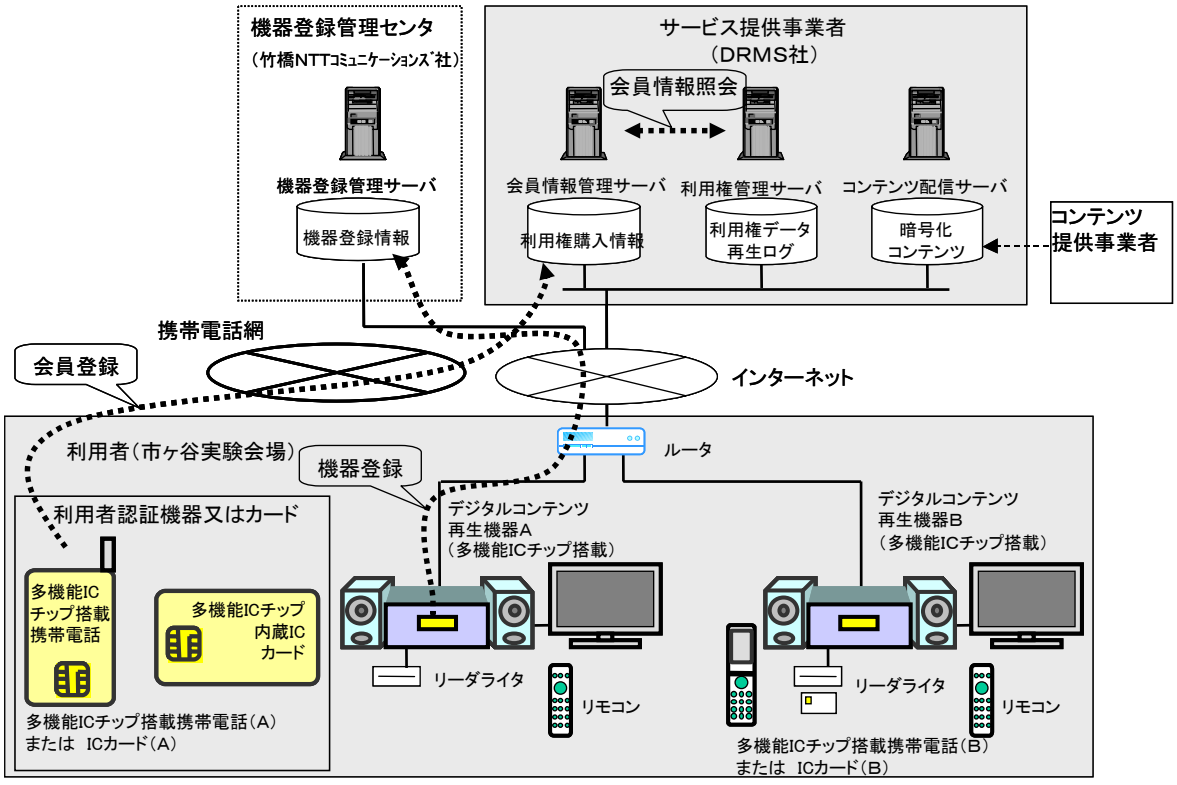


図3-1　実証実験の環境

3．1．2　システム構成

3．1．2．1　利用権管理サーバ

（1）ソフトウェア構成

利用権管理サーバのソフトウェア構成を図 3-2に示す。

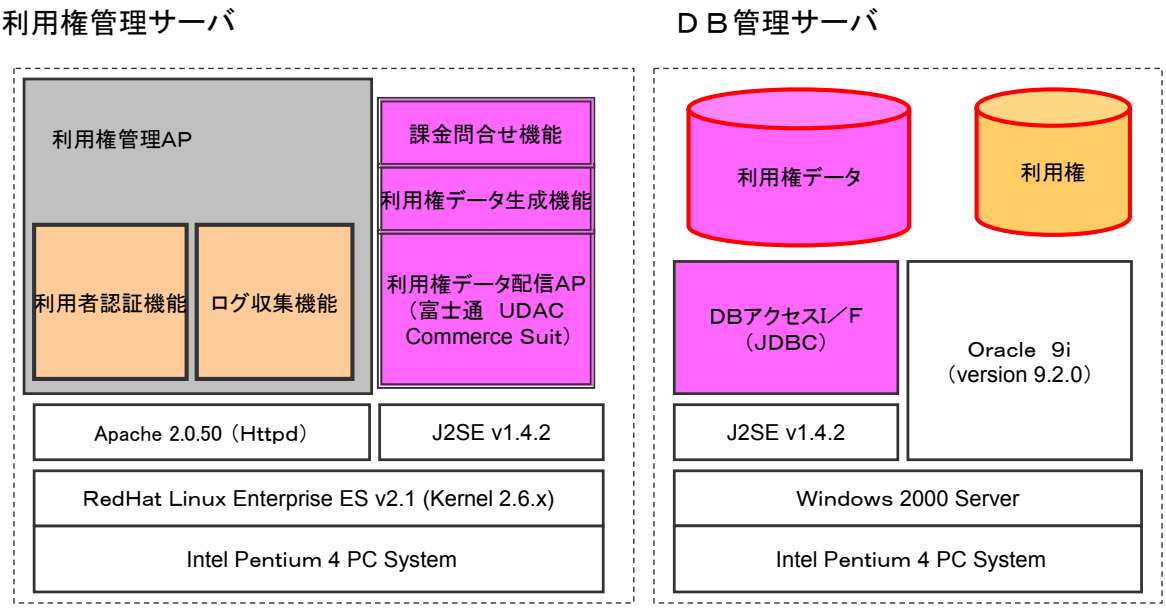


図3-2　利用権管理サーバのソフトウェア構成

3．1．2．2　会員情報管理サーバとコンテンツ配信サーバ

（1）ソフトウェア構成

会員情報管理サーバ・コンテンツ配信サーバのソフトウェア構成を図 3-3に示す。

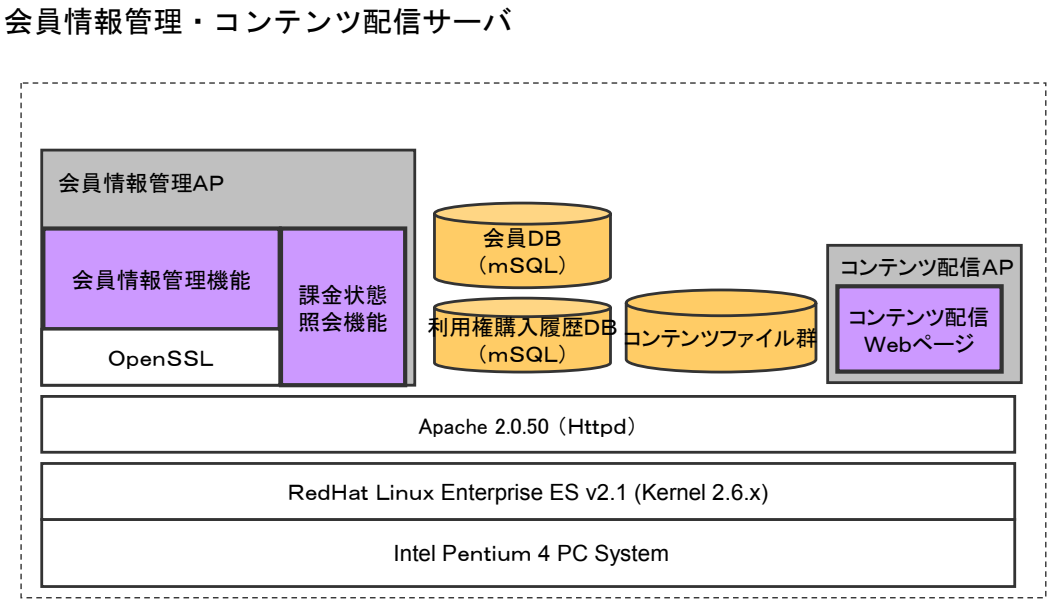


図3-3　会員情報管理サーバ・コンテンツ配信サーバのソフトウェア構成

3．1．2．3　デジタルコンテンツ再生機器

デジタルコンテンツ再生機器は、暗号化された多数のコンテンツをあらかじめインストールした、いわばジュークボックスのような機器であり、インターネットに接続して使用する。機器登録やコンテンツの購入などの操作は、インターネット上の各センタにアクセスして実行する。これにより、家庭だけでなく喫茶店・レストランなどに設置して、利用権を取得している音楽を楽しむことができる機器となっている。

（1）ハードウェア構成

デジタルコンテンツ再生機器のハードウェア構成は以下のとおりである。

(a) デジタルコンテンツ再生機器本体

Visual Technology 社製 VT－100（Intel Pentium4 プロセッサ搭載 PC）

(b) IC カード／IC カードリーダライタ

NTT コミュニケーションズ製 多機能 IC チップ搭載 IC カード 及び非接触型 IC カードリーダライタ PD2102P

(c) 機器チップ

NTT コミュニケーションズ製 多機能 IC チップ

図3-4　デジタルコンテンツ再生機器概観図

（2）ソフトウェア構成

デジタルコンテンツ再生機器のソフトウェア構成を図 3-5に示す。

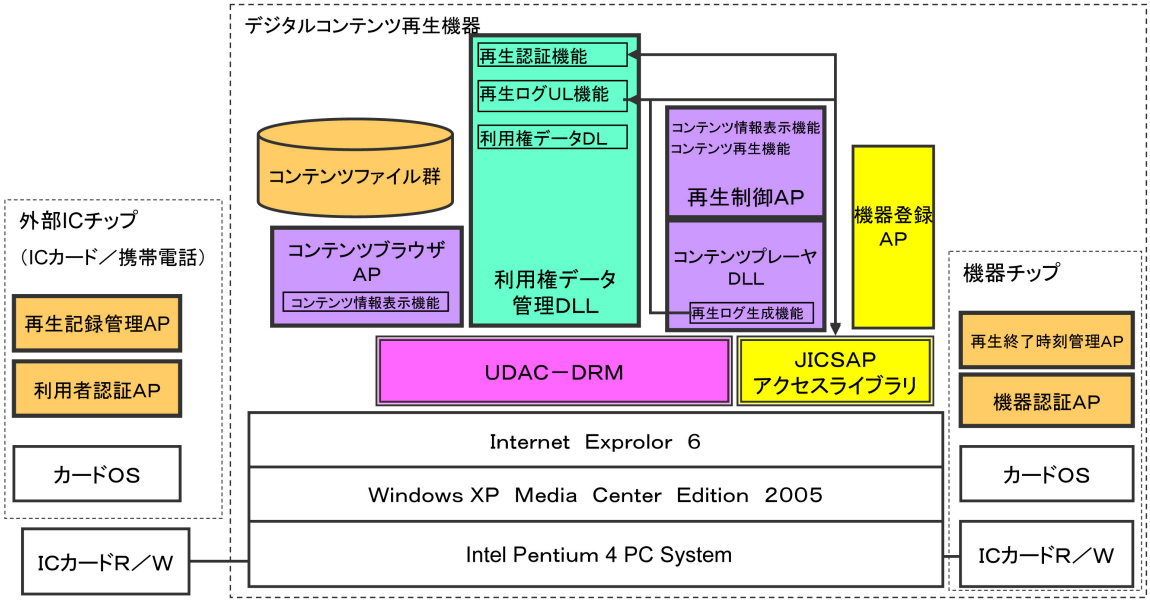


図3-5　デジタルコンテンツ再生機器のソフトウェア構成

3．1．3　コンテンツ流通方式

3．1．3．1　コンテンツの利用形態

デジタルコンテンツ再生機器に格納するコンテンツは 2 つの種類とした。音楽が 1 曲のみ入っている「個々のコンテンツ」（実装上イメージが湧きやすいように以下「シングルコンテンツ」という。）と、約 10 曲入った「まとまったコンテンツ」（以下「アルバムコンテンツ」という。）である。デジタルコンテンツ再生機器の画面ではアイコンでシングル・アルバムの区別がつくようになっている。アルバムコンテンツの中の曲は自由に選んで聞くことができる。

シングルコンテンツは買取り方式で再生期限が無いためいつでも利用できるが、アルバムコンテンツはレンタル方式で一定の有効期限に限って利用できる想定である。

3．1．3．2　コンテンツの登録処理

デジタルコンテンツは、あらかじめオフラインで暗号化しライセンス情報を生成して利用権管理サーバに登録する。この処理は UDAC-MB（Universal Distribution with Access Control - Media Base)システムで実現する。

UDAC-MB システムとは、保護コンテンツのオンライン配信・移動・再生の際の DRM 間相互運用方式・仕様で、以下の要件を満たすことを可能にし、2．1 節において検討した基本的要件項目の 5、6、7 を実現する機能を持つ。

①暗号化コンテンツとライセンス（＝コンテンツ複合鍵＋利用許諾鍵）を分離し各々単独で購入、複製、移動できる。
②ハードウェア TRM（Tamper Resistant Module）内処理で保護
③不正の局所封印
④完全にオープンな DRM 間相互接続仕様が存在

3．1．3．3　利用権データの生成手順

利用権データとは、デジタルコンテンツ再生機器が暗号化コンテンツ再生のために必要とする情報を指す。利用権データを利用権管理サーバから取得する手順を以下に示す。

①利用者認証と機器認証（2．1 節の基本的要件項目 3、4）を実行する。すなわち、IC カードまたは IC チップ内蔵携帯電話内の利用者の IC チップと機器の IC チップから証明書情報を取得して利用権管理サーバの利用権管理 AP に渡し、認証された証明としてワンタイムパスワードを取得する。
②IC カードの証明書情報と上記ワンタイムパスワードを認証情報に設定し、その認証情報を指定して UDAC-DRM のクライアントから利用権管理サーバ内利用権データ配信 AP のライセンス配信機能を呼び出してライセンスを取得する。
③利用権管理サーバ内の利用権データ配信 AP のライセンス配信機能では、端末側から渡された認証情報からワンタイムパスワードを取り出し、認証・課金問合せ機能に渡して認証チェックを依頼する。このとき渡されたコンテンツ ID と利用者情報から購入履歴を検索する。
④認証・課金問合せ機能では、ワンタイムパスワードを利用権管理 AP の利用者認証機能に渡し、利用者認証機能が渡されたワンタイムパスワードをチェックしてライセンス配信可能か否かを返す。
⑤ライセンス配信機能では、ワンタイムパスワードのチェックが OK であれば要求されたコンテンツのライセンスを検索し、そのライセンスの他 DRM 許諾条件設定領域に端末から送られてきた認証情報の中の証明書情報を設定し、UDAC プロトコルによりデジタルコンテンツ再生機器に利用権データを配信する。

図 3-6に利用権データのダウンロード手順を示す。

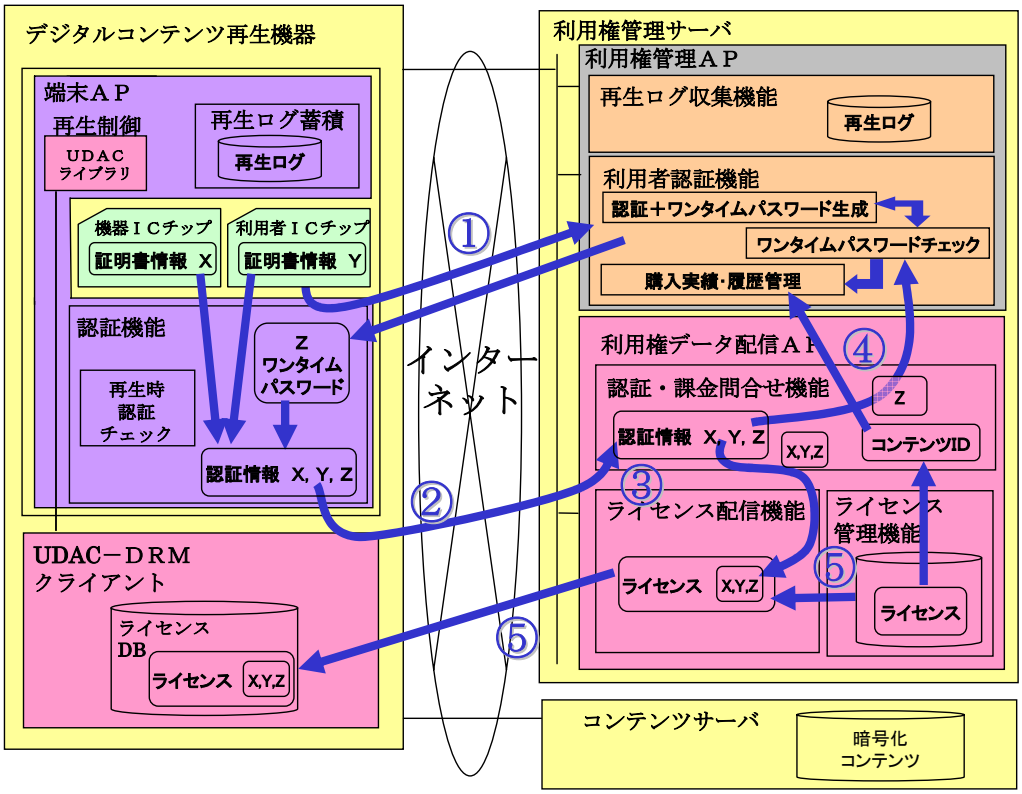


図3-6　利用権データのダウンロード

3．1．3．4　コンテンツの再生手順

デジタルコンテンツ再生機器のコンテンツブラウザ AP では、利用権データを使って暗号化コンテンツを再生する際に、事前に取得済利用権データがデジタルコンテンツ再生機器と利用者 IC チップで利用可能かどうかをチェックする。

①コンテンツブラウザ AP は UDAC-DRM クライアントの機能により再生対象暗号化コンテンツに対応するライセンスの情報を取得し、利用者認証と機器認証（2．1 節の基本的要件項目 3、4）を実行する。すなわち、利用権データに内蔵されている証明書情報が利用者 IC チップとデジタルコンテンツ再生機器の機器チップの証明書情報に一致しているかチェックする。一致していれば再生可能と判断する。（一致する利用権データが無い場合、当該利用者が利用権を購入しているかチェックし、購入している場合は利用権管理サーバから利用権データをダウンロードする。未購入コンテンツの場合は、購入ガイダンスを表示する。）

②コンテンツブラウザ AP は UDAC ライブラリ経由 UDAC-DRM クライアントで利用権データを取得し、読み込んだ暗号化コンテンツのデータを随時復号し再生する。

③コンテンツブラウザは暗号化コンテンツ復号時に再生ログを出力し、利用権管理サーバのログ収集機能に送る。

図 3-7にコンテンツの再生手順を示す。

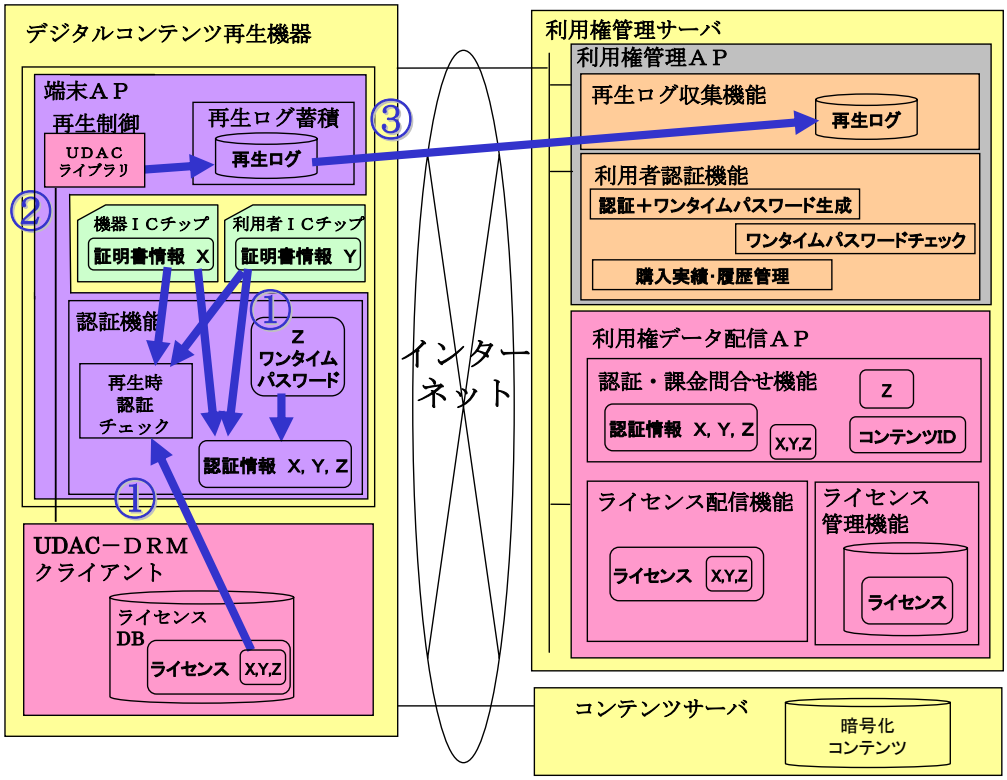


図3-7　コンテンツ再生手順

3．1．4　利用シーケンス

利用シーケンスのイメージを図 3-8に示す。

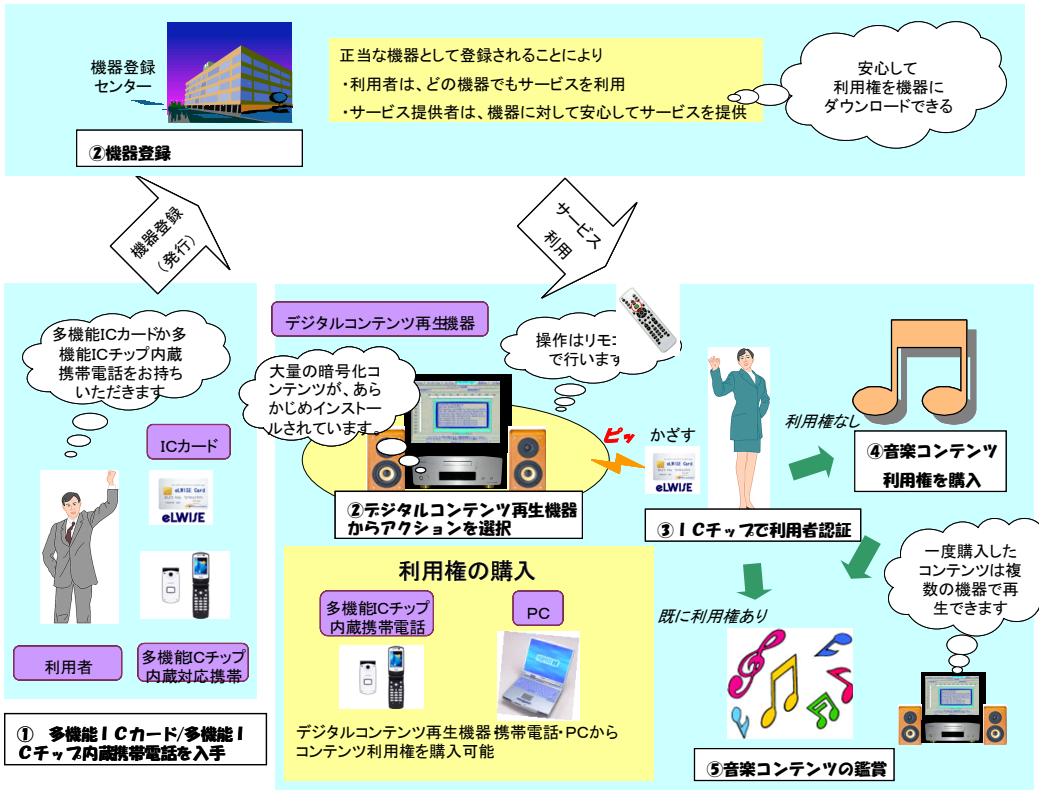


図3-8　利用シーケンス・イメージ図

3. 2　検証項目

本テーマでは、多機能 IC チップを活用した次世代コンテンツ流通サービスの有効性や実現可能性等について検証することを目的として実証実験を行った。実際のサービスイメージを想定した環境を構築して、利用者、サービス事業者、コンテンツ権利者といったステークホルダ（利害関係者）を対象にデモンストレーションを行い、アンケート及びヒアリングを通じて評価データを収集した。

本実証実験において設定した評価項目及びその内容を表 3-1に示す。

表3-1　次世代コンテンツ流通サービスの研究開発と実証実験の検証項目及び検証内容

検証項目		検証内容
テーマ 1 との連携及び昨年度の成果を活用したコンテンツ流通サービスに関する検証	テーマ 1 の機器登録センタに事後登録ができる多機能 IC チップを搭載したデジタルコンテンツ再生機器による機器登録の有効性検証	安全なコンテンツ流通サービスを実現するためにデジタルコンテンツ再生機器の利用開始時に機器登録を行うことの有効性についての検証。
	多機能 IC チップ搭載携帯電話または多機能 IC カードを利用した利用者認証の有効性検証	安全なコンテンツ流通サービスを実現するためにデジタルコンテンツ再生機器の利用時に利用者認証を行うことの有効性について検証。
コンテンツ流通サービスに関する検証	利用権を持っているコンテンツに関して複数の機器での再生を実現する機能の利便性・有用性検証	一人の利用者が認証された多機能 IC カードを持つことで、機器認証された複数機器で同じコンテンツを再生できることの利便性・有用性を調査・評価。
	コンテンツ再生ログを多機能 IC チップ内に保管し、コンテンツの利用期間制御や権利料などの分配に利用することの有用性に関する検証	再生期間制限付コンテンツのサービスを実現するためにコンテンツの再生ログ（再生終了日時）を機器内の多機能 IC チップ内に保管することの有用性を調査・評価。
		アルバムコンテンツに含まれる個別コンテンツの権利管理者・権利者による権利料・利用料の分配に活用するため、再生ログを収集し利用者認証用多機能 IC チップ内に保管することの有用性を調査・評価。
	携帯電話を利用してコンテンツ利用形態に対応した会員登録（課金方式）の利用者にとっての利便性、コンテンツ流通サービスにおける有用性に関する検証	レンタル・買い取りなどのコンテンツ利用形態に応じた携帯電話利用の定額払い・都度払いなどの課金方式の利用者にとっての利便性、事業者にとってのサービス実施上での有用性を調査・評価。

3．3　検証結果

3．3．1　実証実験実施概要

（1）実験期間

平成 17 年 2 月 21 日～3 月 4 日

（2）実証実験会場

実証実験会場：Dali インターナショナルジャパン株式会社　オフィス

図3-9　実証実験機器

（3）被験者

参加者数：44 名

内訳：コンテンツ流通サービス事業者、コンテンツ権利者、サービス利用者

表3-2　被験者内訳

項番	参加者区分	人数	備考
1	コンテンツ流通サービス事業者	30 名	機器製造業者を含む
2	コンテンツ権利者	13 名	
3	サービス利用者	44 名	コンテンツ流通サービス事業者、コンテンツ権利者を含む

(4) アンケート及びヒアリングの実施

評価項目に合致したアンケート項目を設定し、以下の種類のアンケート用紙及びヒアリングシートを作成した。

a. 利用者・事業者用アンケート用紙
b. 利用者・権利者用アンケート用紙
d. ヒアリングシート

次節以降では、アンケート及びヒアリングの結果について示す。なお、グラフ図中の番号は、アンケート票の質問番号に対応する。

3. 3. 2　テーマ 1 との連携及び昨年度の成果を活用したコンテンツ流通サービスに関する検証

(1) テーマ 1 の機器登録センタに事後登録ができる多機能 IC チップを搭載したデジタルコンテンツ再生機器による機器登録の有効性検証

①機器登録の手続・操作（利用者に対する項目）

機器登録の手続・操作については、分かりやすさ・手間など、意見は賛否二分した。処理時間に関してはやや長いと感じた意見が多かった。

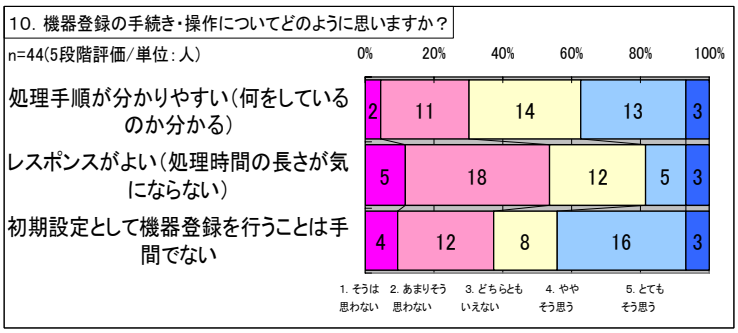


図3-10　機器登録の手続・操作について

操作性についてヒアリングを行ったところ、分かりやすかった／面倒であった／実験だから評価できない、など意見は 1 つに収束しなかった。操作そのものに関しては、リモコンの他にもデジタルコンテンツ再生機器の前面パネル、ディスプレイのタッチパネル、携帯電話などいろいろな方法があるほうが良いとの意見もあった。

一方、機器登録の意義についてはさまざまな疑問や意見があったので下記に列記する。

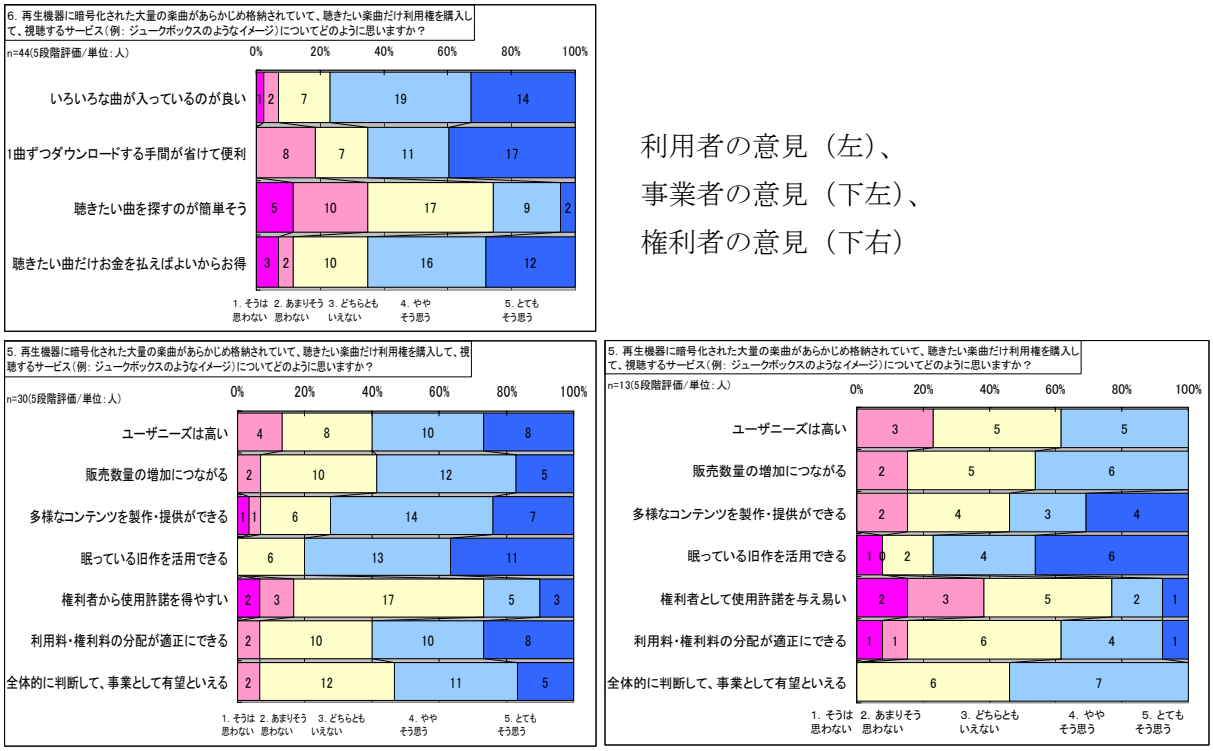
(A) あらかじめ登録されているか、電源オンで自動的に実行されれば良い。
　そもそも利用者には機器登録する意味・意義が分からない。
　何か怪しげなことをやっている、という印象を与える。
(B) 認証させるというのは拘束的。利用者にやらせるものではない。
(C) なぜ機器登録時に所有者の登録はしないのか

（2）多機能 IC チップ搭載携帯電話または多機能 IC カードを利用した利用者認証の有効性検証

①暗号化コンテンツがプレインストールされていて、利用権を購入して視聴するジュークボックス型サービスの利便性（利用者・事業者・権利者に対する項目）

利用者からは 70%前後の肯定意見という高い評価を得た。その理由としてはいろいろな曲が揃っていること、1 曲ずつダウンロードする手間が省け便利であること、聞きたい曲だけにお金を払えば良いことを挙げているが、一方では聞きたい曲を探すことが難しそうであると判断された。

事業者・権利者からは概ね肯定的評価が得られた。その理由としては、眠っている旧作を活用できること、多様なコンテンツを制作・提供できること、販売数量の増加につながること、などが約半数の賛同を得ることができ、事業として有望と考えられているが、反面、権利の許諾の得られやすさ・与えやすさについては意見が分かれた。



利用者の意見（左）、
事業者の意見（下左）、
権利者の意見（下右）

図3-11　ジュークボックスのようなサービスについて

3．3．3　次世代コンテンツ流通サービスに関する検証

（1）利用権を持っているコンテンツに関して複数の機器での再生を実現する機能の利便性・有用性検証

①利用権を購入してコンテンツを楽しむサービスの利便性の評価と利用に対する要望

（利用者に対する項目）

利用権を購入した後のサービスについては 80%以上肯定的に使いたいと評価されたが、利用権を貸したり譲ったりする必要性については賛否意見が分かれた。

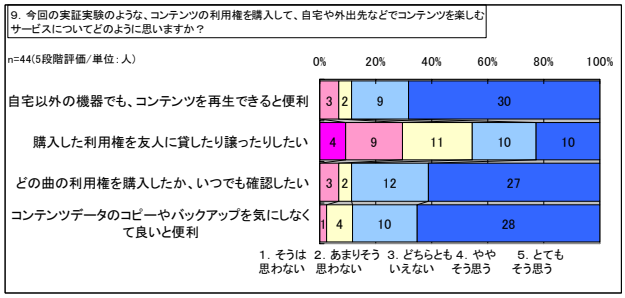


図3-12　自宅や外出先などでコンテンツを楽しむサービスについて

ビデオやゲームなど音楽以外のコンテンツで利用権を使いたいか、自宅以外でダウンロードした利用権を利用するシーンをイメージできるか、など利用権購入シーンについてヒアリングを行った結果、このような利用形態は、本来は音楽以外に適しているだろうという意見が大勢を占めた。

(A) 複雑な操作でも良いから映画・ゲームなどリッチなコンテンツにこそ向いているのではないか

(B) ゲームは商売になるかもしれない

ホテルのデマンドシステムで認証を売りにする

ゲームはカテゴリに細分化しており 20 タイトル程度あれば商売になるかも

(C) 書籍がいいかもしれない

相互引用などの機能が必要

(D) 音楽はコンテンツとしての価値が低い

最大公約数的な数量取り揃えが必要なので、プレインストールは大変

コンピレーションあるいはレアなものを売りにするなら用途があるかも

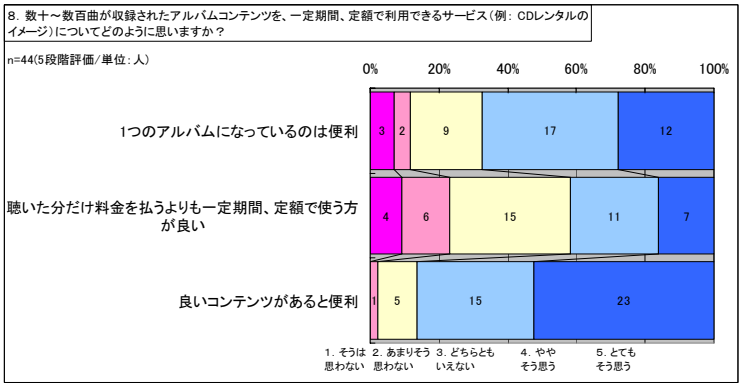
(E) 現状は権利が取れないのでドラマは考えられない

（2）コンテンツ再生ログを多機能 IC チップ内に保管し、コンテンツの利用期間制御や権利料などの分配に利用することの有用性に関する検証 ①

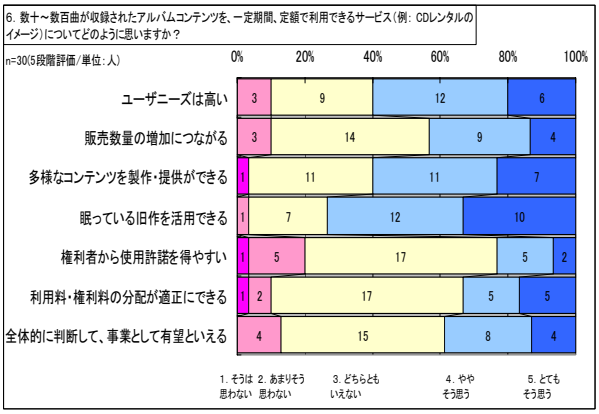
①アルバムコンテンツを一定期間定額で利用するサービスについてのニーズと利用に対する要望（利用者・事業者・権利者に対する項目）

利用者は、良いコンテンツがあれば便利、1 つのアルバムになっているので便利という点については良い評価をしたが、一定期間定額で使うことの利点については意見が分かれた。

事業者・権利者ともに、眠っている旧作を活用できる、多様なコンテンツを制作・提供できる、ユーザニーズが高いことについて良く評価した。また、事業者の一部は販売量の増加、利用料・権利料の分配の適正さに関してもある程度評価しているが、一方権利者はこれらの項目について意見が分かれているだけではなく、そもそも事業として有望かについても意見が分かれた。



利用者の意見（左）、
事業者の意見（下左）、
権利者の意見（下右）



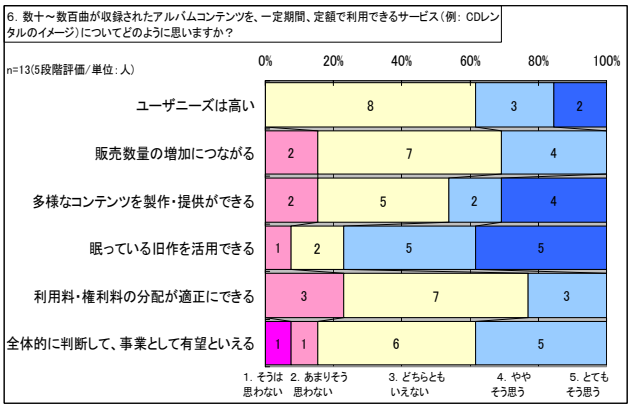


図3-13　アルバムコンテンツについて

さらに、アルバムコンテンツの有効性についてヒアリングを行ったところ、利用者・事業者の視点からは一定期間定額サービスは以下のようなものが向いているとの意見であった。

(A) 映画、ゲーム、旧作、しかし探すのが手間。低単価決済なら便利
(B) 定額の中で、ライブラリの中の曲が全部聞き放題のサービス
(C) コンピレーション、季節もの・誕生日セットなど、あるいはお薦めもの
(D) スニークレビュー、プレビュー版
　作成中にアップし、無料とする　→気に入った人が予約・購入

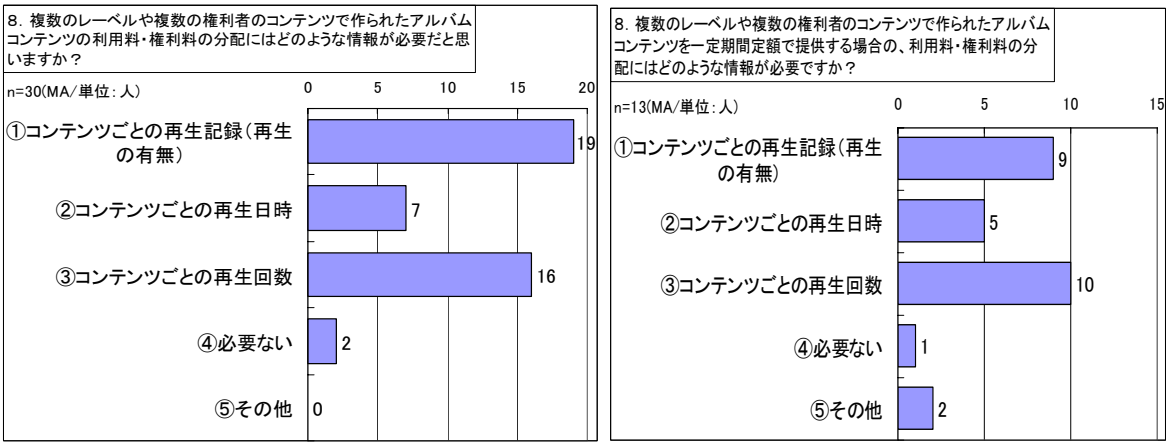
一方で権利者の意見では、一定期間定額サービスとしては以下のようなものが向いているとの意見であった。

(A) 喫茶店、ボーリング場などサービス提供者向け
(B) 映画
(C) 有名人リコメンド（バーチャルウルフマンジャック＝有名 DJ）
　発信者が決める、アーティスト側が決めるもの。
　こういう売り方もできますよ的。途中で購入に切り替えられると便利
(E) 毎週のオリコン上位の一定期間利用
(F) レンタカーサービスとの連携で一定期間利用
　レンタルより IP ラジオに近いと思う。

（3）コンテンツ再生ログを多機能 IC チップ内に保管し、コンテンツの利用期間制御や権利料などの分配に利用することの有用性に関する検証②

①アルバムコンテンツの利用料・権利料の分配に必要な情報に関するニーズ（事業者・権利者に対する項目）

事業者・権利者ともにコンテンツごとの再生有無または、再生回数が必要であると回答したが、事業者は再生有無が必要と回答した人が多く、権利者は再生回数が必要と回答した人のほうが多かった。



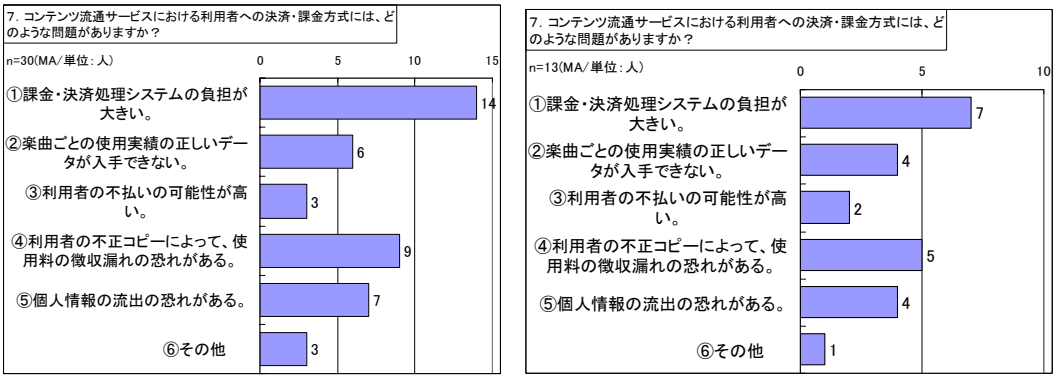
事業者の意見（左）と権利者の意見（右）

図3-14　正当な権利料を受け取るために必要な情報

（4）コンテンツ流通サービスにおける携帯電話を利用した決済・課金方式に関する検証

①利用者への決済・課金方式の問題点（事業者・権利者に対する項目）

事業者・権利者ともに、課金・決済処理システムの負担が大きいという意見がほぼ半数から出され、利用者の不正コピーによる使用料の徴収漏れ、個人情報の流出の危険性がこれに続く結果となった。



事業者の意見（左）と権利者の意見（右）

図3-15　コンテンツ流通サービスにおける利用者への決済・課金方式

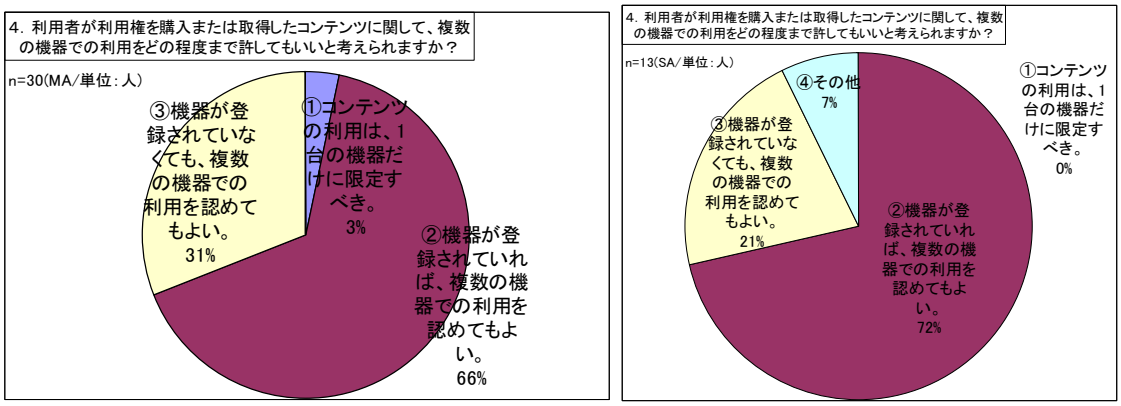
3. 3. 4　一般的なインターネットサービスに関する検証

アンケートを実施するにあたっては、検証項目に関する調査質問の前に、導入部としてインターネットサービスに関する一般的な質問を行った。以下にその結果を記述する。

①複数の機器での利用許容度（事業者・権利者に対する項目）

事業者では 1 台に限るという意見はほとんどなく、機器登録されていれば複数の機器で使えるべきであるという意見と、登録されていなくても複数の機器で使えるべきであるという意見に分かれている。

権利者は 1 台に限定すべきという意見は全くなく、登録された複数の機器で使えるべきであるという意見が 70%を超え、登録されていなくても良いという意見と合わせると 90%以上が複数機器での使用が必要と考えているという結果となった。（図 3-16）



事業者の意見（左）と権利者の意見（右）

図3-16　複数の機器での利用

②実証実験全般に関する意見（利用者・事業者・権利者に対する項目）

今回の実証実験全般に関して、あるいは次世代コンテンツ流通に関して意見を求めたところ寄せられた意見を以下に列記する。

【コンテンツ流通について】

(A) プレインストールの意味がない

ダウンロードが十分早くできれば不要。使うときだけダウンロードすれば良い。

(B) カードに利用権が入る訳ではなく、サーバにある利点がよく分からない

ビジネス的にどうなるのか、機器登録センタは、成り立つのか

(C) 利用権とコンテンツの分離は良い。

家と車などコンテンツを持ち歩くリスクを考えると便利。映像ストリーミングなら良いかも。しかし履歴が取れないか。みんな iPod にコンテンツを入れるのに苦労しているのでこのサービスは便利。個人情報 DB が膨大になる。

(D) 利用権とコンテンツの分離は有り得無い

ユーザ側から見るとメリットがあまり感じられない。操作が面倒である、今の時代

このモデルが必要とは思えない。CD、インターネットなど各人はコンテンツ入手をそれぞれ使い分けている。この分野に普及の余地があるとしてもニッチなものになるだろう。コンシューマからすれば過度な DRM はいやだ。

(E) ジュークボックス型と個人用のサービスを別けたほうがよい
プレインストールは曲の集め方が難しい

(F) ログを利用者カードに入れるのはおかしい。
ユーザメリット不明。コンテンツプロバイダに報告しなければ利用できない。自動的にアップするか、ポイント・マイレージ風にして報告させる必要がある。サーバにあれば良い。曲が終わった時点で自動的にログ更新すれば良い。

(G) 暗号化コンテンツのダウンロードも権利者に支払いが必要なので複製権をどうするのか解決する必要がある。最近は超流通に関しての特例もある。

(H) DSRC との連携も面白い

(I) 音楽の場合、歌詞、ジャケット、写真なども欲しくなる。

(J) 新曲は自動ダウンロード、古い曲は自分でダウンロードというのはどうか?

(K) 利用者として買った後も管理されている感じが強い
（現在の CD は買った後は比較的自由なので違和感がある）

【運営・経営について】

(A) プレーヤとしてプロバイダ、ネットワークもある

(B) 社会人教育は携帯／IC カードを利用者に持たせるのは良いが、受講料以外に金がかかるのはだめ→デジタルコンテンツ再生機器でも PC でも同じ。

(C) 権利コンテンツ
ビデオ／DVD／ストリーミングいずれでも受講料先払い、利用者・期間の特定が必要、機器特定は不要。“どこでも”が売り

(D) アルバムレンタル単価
200～300 円／99 ¢ 程度か。

【画面・操作について】

(A) 実証実験なので操作性は評価できないが、手順を少なく
今何をやっているのか表示があったほうが良い

(B) 操作性（携帯、PC、VT）はアクセスする手段は分かりやすいものが 1 つあれば良い。いろいろな機器があるといろいろな使い方を覚える必要がある

(C) 購入前に試聴機能が必須

(D) 検索機能をつけたほうが良い

(E) 購入した利用権が表示される必要がある
カードをおいたときだけ自分の購入したものがわかるのがよい
センタコンテンツも購入したものがわかるほうがよい

(F) ケータイは認証を自動的に。利用者はいかにボタンを押さずに使えるか

権利者の意見を下記に列記する。

【コンテンツ流通について】

(A) なぜダウンロードではいけないのか
ネット接続しているなら聞くときにダウンロードすれば良い。ジュークボックスでなくても暗号化 DVD でも同じサービスができる。別にダウンロードするのは大変。

(B) 権利を買う発想は良い
買った感覚ない。コーヒーは飲むとき毎回支払うが音楽も同じようになるか？実用化するなら貸し借りも考える必要がある。
グリーティングなど、カードをプレゼントとして使い回す為チャージできれば良い、期間限定にする、などアプリはいろいろ考えられる。
一定期間コンテンツより、会費を取って会員制にするのはどうか？

(C) 最終的に流通はプレイリストのみで、コンテンツはストリーミングではないか。

(D) 巨大資本しかできない（コストの問題）
→競争原理が働かず料金が高くなるのでは？

(E) 装置は持ち運べる必要あり
携帯を置いて認証した時に曲が入れば良い。あるいは、携帯でデジタルコンテンツ再生機器を操作できれば。

(F) 機器に利用者リーダライタが入っていない。機器チップと一本化が必要。

【運営・経営】

(A) 音楽は幅が広すぎる
トヨタの車の音楽サービスとの乗り入れ。着うたなど他のサービスとの乗り入れが普及のカギ。今回のシステムは前提として音楽 DB が必要

【画面系・操作系】

(A) ダウンロード済・購入済のものが表示される必要あり
反面、前の人がどんなものを購入したか分かる（ビデオならアダルト向け作品を見た）

(B) 試聴機能が必要
頭だけ AV 機器に入れておいてあとはストリーミング（容量を減らせる）

(C) 使い勝手はソフトだからうまく作れば何とでもなる。核だけしっかり作って AP は自由にさせる方法もある。ユーザインタフェース改良の余地有、利用者として操作が煩わしい

3．4　考察

3．4．1　「一般利用者の視点による意見」に対する考察

一般利用者の意見としては、「多くの機器が対応し」、「タイトルが揃い」、「サイトを見つけやすくし」、「希望する決済方法が揃えば」、インターネット上での有料コンテンツを利用していきたいと考えていると思われる。

また今回の実証実験での一般利用者は、「大量の楽曲が揃い」、「聞きたい楽曲だけ利用権を購入できるサービス」、「携帯電話で利用権を購入したアルバムコンテンツを一定期間定額で利用できるサービス」、「利用権を購入した後のサービス」については積極的な評価を示している。機器登録については、「格別の抵抗はなく」、「登録料は購入価格に含むようにして欲しい」との具体的な要望が出るとともに、「機器登録後のサービスを期待する」意見が積極的に出されている。

またサービス全体を通じて「楽曲が揃っていること」、「良いコンテンツが揃っていること」が強く要望されている。

3．4．2　「サービス事業者の視点による意見」に対する考察

事業者は、写真動画付コンテンツ、アルバム、カラオケ等のダウンロード販売、パッケージのネット販売、ストリーミング販売に興味を持ち、良い決済方式の導入を望み、機器が登録されていなくても複数の機器で使えることを望む人が多く、複数権利者からの許諾取得の困難さを心配している。

また事業者は、大量の楽曲が揃い、聞きたい楽曲だけ利用権を購入できるサービスについては、権利の許諾が得られやすいかに関して楽観視していないものの有望なサービスと判断している。またアルバムコンテンツを一定期間定額で利用できるサービスについては評価しているものの、権利の許諾等に関して疑問を持ち、より消極的な評価を示している。事業者は課金・決済方式を心配し、コンテンツごとの再生記録が利用料・権利料の分配に役立つと考え、機器登録センタの運用はサービス事業者の業界団体が行うことを好ましいと考えている。また事業者は機器登録料の徴収機関については明確な考えを持っていない。

なお、事業者は権利者の許諾が得られるかを心配し、利用者の要望に沿って、多数のコンテンツを揃えられるか、良いコンテンツが揃えられるかを気にしている。

3．4．3　「コンテンツ権利者の視点による意見」に対する考察

権利者はシングル、アルバム、旧作、新作コンテンツのダウンロード販売、パッケージの通信販売、ストリーミング販売に関心を持ち、利用登録された機器のみによる複数機器での利用を望んでいる。一方、不正利用の増加を懸念し、複数機器での利用を許可した場合の許諾範囲を超えた利用及び不正利用を心配している。

今回の実証実験での権利者は、大量の楽曲が揃い、聞きたい楽曲だけ利用権を購入できるサービスについては、眠っている旧作を活用できるが有望なサービスとあまり考えられないと判断している。アルバムコンテンツを一定期間定額で利用できるサービスについても有望なサービスとして評価しているものの、権利の許諾等について容易でないとの意見を持っている。権利者は課金・決済処理システムの負担が大きいこと、利用者の不正コピーによって使用料の徴収漏れがあることなどを心配している。また権利者は、機器登録センタの運用主体として機器メーカの業界団体を希望している。

4. まとめ

4. 1　成果

本テーマでは、多機能 IC チップを用いて機器や利用者の認証を行い、コンテンツの利用権を購入して、これを楽しむことができるところまでを一貫して実現し、体験することができるシステムを構築した。具体的には、①テーマ 1 で構築する機器登録センタに対して多機能 IC チップ搭載デジタルコンテンツ再生機器を登録する機能、②利用権を持っているコンテンツに関しては複数の機器での再生を実現する機能、③利用者認証用 IC カードへのコンテンツ再生ログ保管機能、④デジタルコンテンツ再生機器内の多機能 IC チップにコンテンツ再生終了日時を保管する機能を実現した。

今回の実証実験により、「大量の楽曲が揃い」、「聞きたい楽曲だけ利用権を購入し」、「コンテンツを複数の機器で楽しめるサービスとアルバムコンテンツを利用できるサービス」については、利用者から高い評価を受け、事業者・権利者からも評価された。また、このようなサービスでの権利保護の強度や仕組みについても権利者をはじめ、事業者・利用者からの評価が得られた。

アルバムコンテンツの利用に関しては、利用者・事業者・権利者ともに有用との意見が大勢を占めた。利用者からは便利、事業者・権利者から利用者ニーズが高いと、双方から評価された。またここでは、事業者・権利者の意見が一致して、眠っている旧作を活用することができるという意見が多いことを考えると、流通させたいができていないコンテンツを非常に多く抱えていることが業界の問題点として想定される。

利用したアルバム内タイトルの再生ログを利用者認証用 IC カード内に格納する機能についても、事業者・権利者からの賛同を得られた。しかし事業者は再生の有無があればよいと考える意見が多かったのに対して、権利者は再生回数も必要であるとの意見が多かった。このことにより各々の立場の相違点を垣間見ることができる結果となった。今回の実証実験で扱った携帯電話での利用権の購入についても、利用者は是非使いたいという反応を示し、むしろ多くの人が所有して慣れ親しんでいる携帯電話を使うことができるのが当然と考えられていることが分かった。さらに購入した利用権がいろいろな機器で使えると良いという意見が大勢を占めているため、今後、各種機器での対応が必要とされる。

デジタルコンテンツ再生機器内の多機能 IC チップにコンテンツ再生終了日時を保管する機能に関してはその安全性については評価できるが、今回のデジタルコンテンツ再生装置のようにネットワークに接続することが前提の装置の場合は、むしろインターネット上の時間サーバを利用する手法なども有用であると考えられる。

利用者認証に関しては、今回は 1 曲利用するごとに認証する方式でシステムを実現したが、利用者のニーズとしてはユーザログオンして、既に当該利用者が購入しているコンテンツをすべて表示するような使い方に対するニーズが高かったことを考えると、公共の場所に設置するジュークボックス型機器における個人情報の表示に関して、前に利用した人の情報をいつ消すか等、今後の工夫が必要であると思われる。

4．2　展望と課題

本テーマの研究結果にもとづき、多機能 IC チップを活用した次世代デジタルコンテンツ流通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) 音楽コンテンツ

現在、世の中ではコンテンツを購入してダウンロードする形態のサービスが普及しつつあるが、今回の実証実験で試みたものはこれとは異なり利用権を購入するという流通形態のビジネスモデルである。このような流通形態においては暗号化コンテンツそのものがどこにあるべきかという議論に関して、ジュークボックス型あるいはオンデマンドダウロード型いずれにも大きな優位性は認められなかった。さらにはヒアリングの時にはストリーミングで良いとの意見も聞かれたことを考慮すると、利用者にコンテンツの所在を意識させない流通形態というものを検討する必要がある。この場合、利用者に提示すべきものは単なるコンテンツリスト（商品リスト）というよりも、おすすめ曲を提示してくれるプレイリスト（リコメンドサービス）になることが考えられる。このあたりのサービス形態についてより深く検討することにより、まさに「次世代」の流通サービスモデルの予測が可能ではないかと考えられる。いずれにしても、利用者に対してダウンロードストレスを感じさせないだけのネットワーク速度、あるいはコンテンツボリュームというものを意識する必要があるのは当然である。

上記の議論を考慮すると、コンテンツの所在を意識させない流通形態が望まれることが予想されるので、この方向でのビジネスモデルを研究すれば実用化に向けて前進することが可能であるといえる。

(2) アルバムコンテンツ

一定期間定額で利用する、いわゆるレンタル的な運用に関しては、特に有用であるという明確な回答を得られなかった。これは、実証実験においてレンタル的利用、すなわち時間とともに利用権が消滅するようなシーンを利用者に体験させることができなかったため、具体的なイメージを与えることができなかったのではないかと思われる。アルバムコンテンツの有用性についてさらに実証実験を行う場合は、利用権のこの点について更なる工夫が必要であると思われる。また、利用したアルバム内タイトルの再生ログを利用者認証用 IC カード内に格納する機能については、ログを活用するためにはむしろこの情報はサービス提供者のサーバにあるべきだとの意見に集中したので、利用者認証用 IC カード内に記録する利点が鮮明となるようなモデルの研究が必要である。

利用者は、限られた機器ばかりでなく、各種の機器での対応を望み、利用者、事業者ともに、各種コンテンツへの対応、コンテンツの取り揃えを強く望んでいるため、今後の対応が必要とされる。

以上をまとめると、「まとまったコンテンツ」と利用ログの取得に関して実装は実現できたので、具体的な用途を想定すれば有用なビジネスモデルの評価が行えるものと思われる。

(3) 機器登録

事業者・権利者の意向を見ると、約 7 割の人が機器登録されていれば複数の機器でのコンテンツの利用を認めても良いと考えていることがわかる。さらに、機器の保守サービスなど機器登録によって実現できるサービスに対する利用者の意向も高いという結果が得られた。これらを受けて、今後機器登録を行った複数機器での再生を可能にする場合、家庭内での使用制限も含めて再生できる機器をどの範囲に留めるかの議論が必要となり、登録をどのように行うかについて検討する必要がある。特定の機器を対象とした業務用のサービスについては、現在の仕組みを導入できる部分が多いと考えられるが、一般家庭向けのサービスについてはさらなる検討が必要であるといえる。

(4) 一般的コンテンツ流通への拡張

今回実証実験で使用した音楽コンテンツの品質（サンプリングレート）は高くなかったため、ファイル容量はたいへん小さかった。これに対して映画やハイビジョンテレビなどの大規模映像コンテンツの場合では、ファイル容量が大きくなるため、どのような流通形態であれば実用的なサービス品質を達成できるか検討する必要がある。

また、コンテンツ流通サービスが普及していくためには暗号化方式や利用権データフォーマットなどの規格統一が不可欠である。このため、規格作成から統一・普及へ向けての展開なども検討すべき項目として残っている。どのような暗号化方式を何年間利用するか、時代に合わせて改変していく柔軟性なども重要な項目であると思われる。

まとめると、本システムでは基本的な流通の仕組みの実効性が評価できたので、今後は大規模コンテンツの流通に適用した場合、あるいは複数のサービスプロバイダ・複数の機器ベンダが参加した場合へフィールドを拡大してその実効性を評価したい。

(5) 実サービスに向けて

本テーマにおいてはシステム構築の外とした課金・決済手段についても検討が必要である。携帯電話や PC でインターネットアクセスした後、どのプレーヤがどのような手段で課金徴収するか、またその安全性や利用者に対する安心感なども具体的に検討する必要がある。携帯電話を活用したコンテンツ購入は、利用者からの利用に対する要望が大きいため、利用者の行動の流れなどの動態を把握し、サービスを検討することによりサービスの幅が広がり、普及していくと想定される。ただ、インターネットを使ったコンテンツ購入が増えつつある状況の中で、いまだにインターネットに対する不安点はカード番号・パスワード・個人情報などの漏洩・盗難に対するものである。この不安が集中するのが支払い決済という操作に対してであることから、利用者に安心感を与える決済手段というものを模索する必要がある。

(6) 課題項目のまとめ

最後に今後への課題項目をまとめておく。

【音楽コンテンツに関して】

・利用者にコンテンツの所在を意識させない流通形態

・コンテンツダウンロードに関して手間とストレスのないネットワーク設計

【アルバムコンテンツに関して】

・アルバムコンテンツのレンタル的運用の生きるサービス形態

・利用者 IC カードにログを格納する利点を実感できるサービス形態

【機器登録に関して】

・機器の使用範囲の限定

・一般家庭向け機器の登録操作

【一般的コンテンツ流通に関して】

・大規模コンテンツの場合の実用的な流通方式

・暗号化方式や利用権データフォーマットなどの規格統一

【その他】

・最適な課金・決済手段

・生活の中での利用シーンを想定した携帯電話利用サービス形態

Ⅱ－3
テーマ 3

登録センタの機能を活用した医療システム機器等
リモートサービスの研究開発及び実証実験

1. 事業概要

1. 1　背景

すべての国民が IT（情報技術）のメリットを享受できる豊かな生活を実現し、IT の活用を通じた新規事業の創出と既存産業の効率化を達成するために、高度情報通信ネットワーク社会の実現に不可欠なインフラ（基盤）を形成すること及び、電子政府・電子商取引等の促進により、このインフラを活用した取引や活動を活性化することが急務となっている。

このような背景のもと、近年では電子カルテシステムを始めとする医療システム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えてきた。例えば、外部からでも医療機関の医療システム機器に接続することが可能となることで新たなリモートサービスモデルの創出が期待される一方で、その基盤要素としてネットワーク機器の安全確実な利用のための認証が必要不可欠になってきている。

1. 2　目的

経済産業省が実施した平成 16 年度「先導的分野戦略的情報化推進事業（多機能 IC チップ等を活用したリモートサービスにおけるセキュリティに関する研究開発・実証事業)」（以下「本事業」という。）では、平成 15 年度に実施した実証・検討を踏まえたサービスを実現するための基盤技術を開発する事業と位置付け、機器登録管理基盤及び平成 15 年度に開発した認証接続管理サービスを発展させた通信基盤を利用して、医療システム機器の予防保守サービスに資する定期的な状態監視や、システムダウンに対する早期バックップサービスなどを安全に行うことにより、安定した医療サービスの実現を図ることを目的とした。

また、上記の研究開発・実証事業と並行し、多機能 IC チップを活用したセキュアな情報サービスシステム基盤が、将来の保健医療分野が必要とするネットワーク基盤として有効であるかについて調査研究を行った。

1. 3　実施概要

(1) リモートサービスのセキュリティに関する研究開発

保守事業者側、医療機関側がともに無人環境でリモートサービスが実施されることを想定して、保守機器対医療機器を、多機能 IC チップを利用して相互認証するセキュリティシステムによりネットワーク環境を構築し、以下の医療で使用されるシステムにリモートサービスにおけるデータ送受信の確実性を担保する仕組みを開発した。

①モダリティのリモートサービスの開発
②医事会計システムのリモートサービスの開発
③電子カルテシステムのリモートサービスの開発

(2) 実証実験

保守事業者側、医療機関側がともに無人環境でリモートサービスが実施されることを想定して、以下の検証を行った。

①ネットワーク基盤の安全性の検証

②リモートサービスの運用性の検証

(3) 保健医療分野への基盤としての適用に関する調査研究

将来、多機能 IC チップを活用したセキュアな情報サービスシステム基盤について、保健医療分野において必要とするネットワーク基盤として有効であるかを以下の内容について調査研究を行った。

①現在、PC 業界に普及しつつある PC セキュリティ基盤としての TPM（Trusted Platform Module）の、多機能 IC チップ等を活用した情報サービスシステム基盤への適用性

②医療分野リモートサービスへの多機能 IC チップを活用したセキュアなネットワーク基盤の適用性と複数のセキュアネットワーク間での相互運用性確保のあり方

1．4　実施体制

本事業の実施体制を図 1-1に示す。

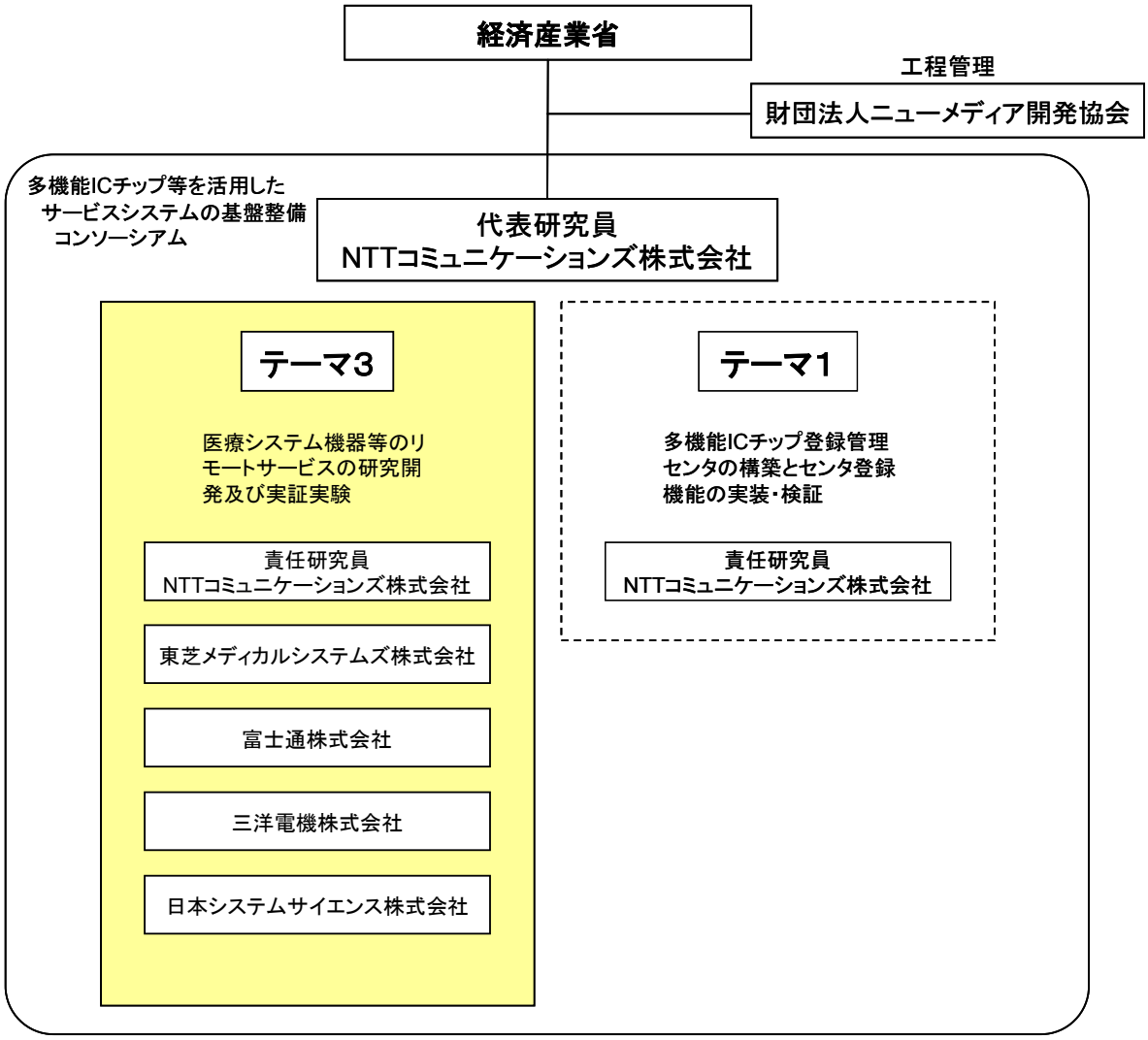


図1-1　実施体制

2. リモートサービスのセキュリティに関する研究開発と実証実験

2. 1　リモートサービスのセキュリティに関する研究開発

2. 1. 1　システム概要

多機能 IC チップ等を運用管理するための機器登録管理センタの機能を利用し、多機能 IC チップ搭載型医療機器システム等を登録して、多機能 IC チップフレームワークを活用した機器認証、医療認証機関が保証する機器対機器の相互認証を実現する。また、情報が無人環境で、かつ自動的に送受信されることを想定して、モダリティのリモートサービス、医事会計システムのリモートサービス、電子カルテシステムのリモートサービスを研究開発した。

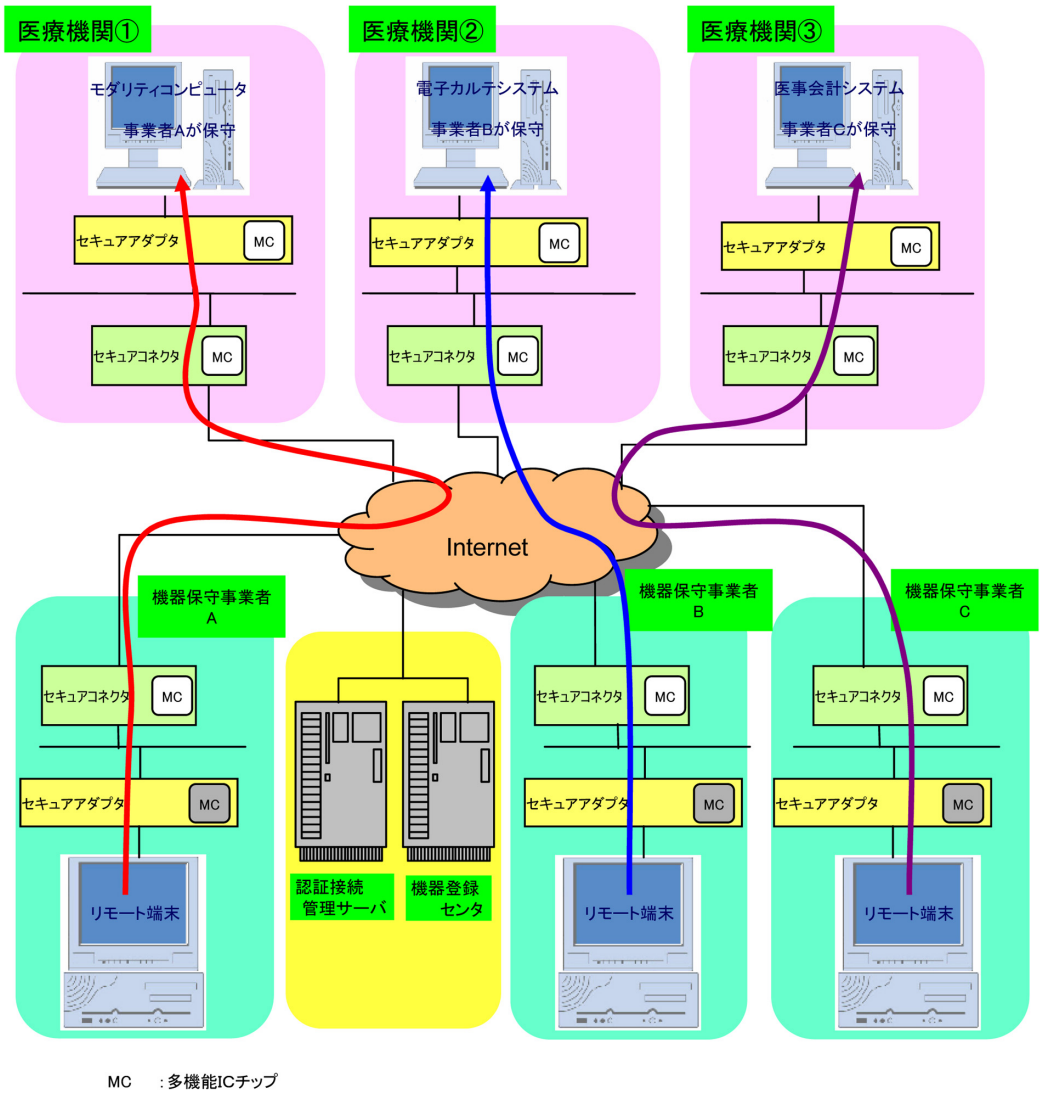


図2-1　システム全体図

2．1．2　開発システム

構築された実証実験環境の上で、リモートサービスの対象となるシステムの状態を監視する機能や設定ファイル等を、定期的なスケジュールで自動的にバックアップする機能を開発した。

(1) モダリティのリモートサービス

医療機関内にあるモダリティの稼働状況を常時監視し、定期的に稼働状況を示すファイルを保守事業者側に転送する機能を研究開発した。

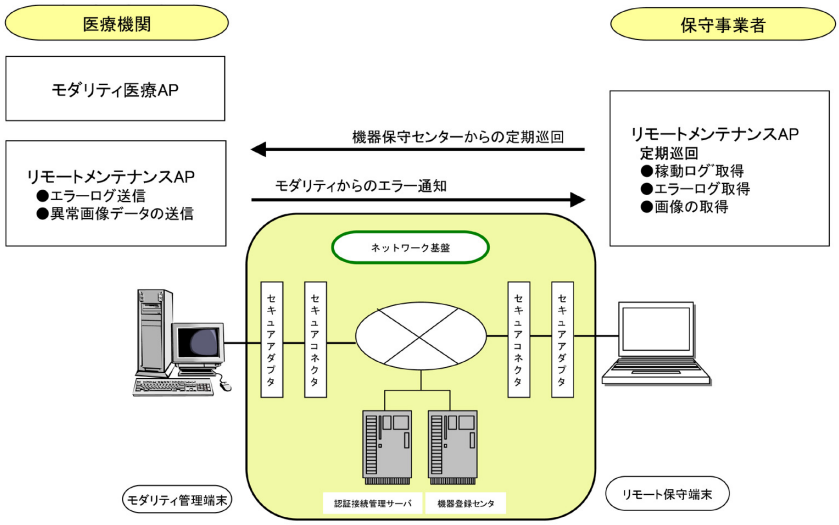


図2-2　モダリティのリモートサービス概要

(2) 医事会計システムのリモートサービス

医事会計システムのリモートサービスでは、医事会計用 PC 上のファイルをスケジュールに基づいて保守事業者のリモート保守端末に自動転送する「ファイル自動転送機能」と、医事会計用 PC 上で発生したイベント情報を自動的に通知する「イベント自動通知機能」の 2 つの機能を研究開発した。

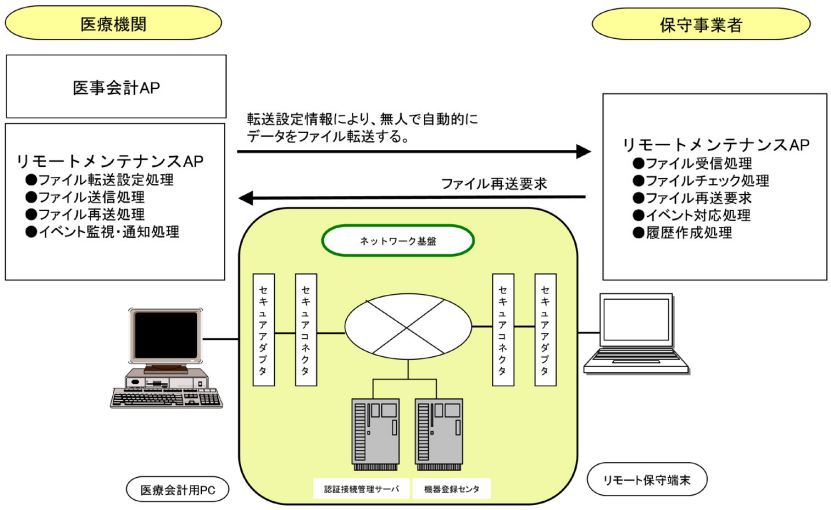


図2-3　医事会計のリモートサービス概要

(3) 電子カルテシステムのリモートサービス

医療機関内にある電子カルテシステムの稼働状況を常時監視し、定期的に稼働状況を示すファイルを機器保守事業者側に転送する機能を研究開発した。

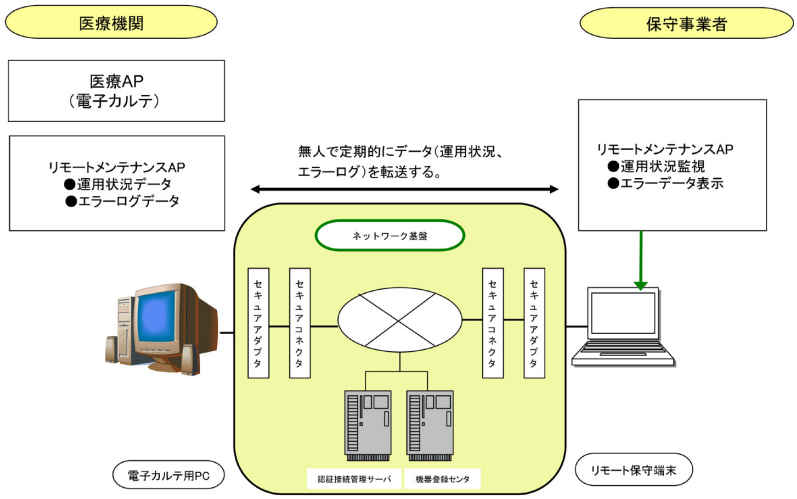


図2-4　電子カルテシステムのリモートサービス概要

2．2　医療機関向けリモートサービスの実証実験

2．2．1　実証実験の目的

多機能 IC チップ等を運用管理するための機器登録管理センタの機能を利用し、多機能 IC チップ搭載型医療機器システム等を登録して、多機能 IC チップを活用した機器認証及び医療認証機関が保証する機器対機器の相互認証を実現する。また、情報が無人環境で自動的に送受信されることを想定して、リモートサービスの実現の可能性を実証する。

2．2．2　実証実験の実施概要

(1) 検証項目と検証内容

モダリティ、医事会計システム、電子カルテシステムの各リモートサービスの運用を通じて実証実験を行った。

検証項目と検証内容を、表 2-1に示す。

表2-1　検証項目と検証内容

検証テーマ	検証項目	検証内容
ネットワーク基盤の安全性の検証	機器対機器の相互認証の有効性	機器の増設を想定した機器の登録と認証接続を行い、設定した内容で確実にセキュアな通信路が構成されているか検証する。 ・セキュアコネクタ、セキュアアダプタへのアクセスの検証 ・認証関連の検証
	通信経路の安全性	構築された実証実験環境が安全な通信経路を実現しているかを検証する。 ・不正アドレスへの送信不可の確認 ・認証接続状態の有効/無効の確認
リモートサービスの運用性検証	リモートサービスの運用性	リモートサービスの動作検証を行う。 ・モダリティのリモートサービス ・医事会計システムのリモートサービス ・電子カルテシステムのリモートサービス
	セキュアなネットワーク環境構築の効率性	環境設定作業と機器増設作業を行い、作業の簡便性の検証を行う。 ・環境設定の簡便性の検証 ・接続先の設定 ・増設機器の登録

(2) 検証方法

実証実験室内において機能検証及びヒアリング調査を下記内容で実施した。

(a) 機能検証

システムのセキュリティや機能に関する検証は、実証実験環境で検証項目にしたがって機能試験を実施した。機能試験はシステム開発を担当した企業の従業員とヒアリング調査のため実証実験実施場所に招聘したヒアリング調査対象者で実施した。

実施期間：平成 17 年 2 月 18 日～平成 17 年 3 月 18 日
実施場所：NTT コミュニケーションズ（株）竹橋実験会場

(b) ヒアリング調査

医師、医療機関関係者、大学関係有識者、医療システム機器の保守作業者、ネットワーク機器構築作業者、医療システムベンダの従業員を被験者として、実証実験実施場所でリモートサービスの動作検証作業の実施と、それに対する評価をヒアリング調査した。

実施期間　：2 月 18 日～3 月 18 日
実施場所　：実証実験実施場所と同じ
調査対象者：15 機関（会社）　20 名

（内訳）	
医療関係者（医師）	2 名
医療機関職員	2 名
大学関係有識者	2 名
医療機器メーカ	4 名
医療システムベンダ	10 名

ヒアリング調査項目：
- 機能の操作性、利便性
- 機能の有効性、効率性
- リモートサービスの運用性評価
- 機器登録の仕組み
- 認証接続管理の仕組み
- 機器増設時の操作性
- セキュアなネットワーク基盤構築の安全性
- セキュアなネットワーク基盤に関する意見

2．2．3　検証結果のまとめと考察

（1）ネットワーク基盤の安全性

本テーマでは機器登録管理センタの機能を利用し、医療システム機器等に機器の正当性を担保するとともに、認証接続管理サーバの機能を利用し、クロスチェックによる通信路を確保することで、多機能 IC チップフレームワークを活用した機器認証及び機器対機器の相互認証できるセキュアなネットワーク基盤を構築した。

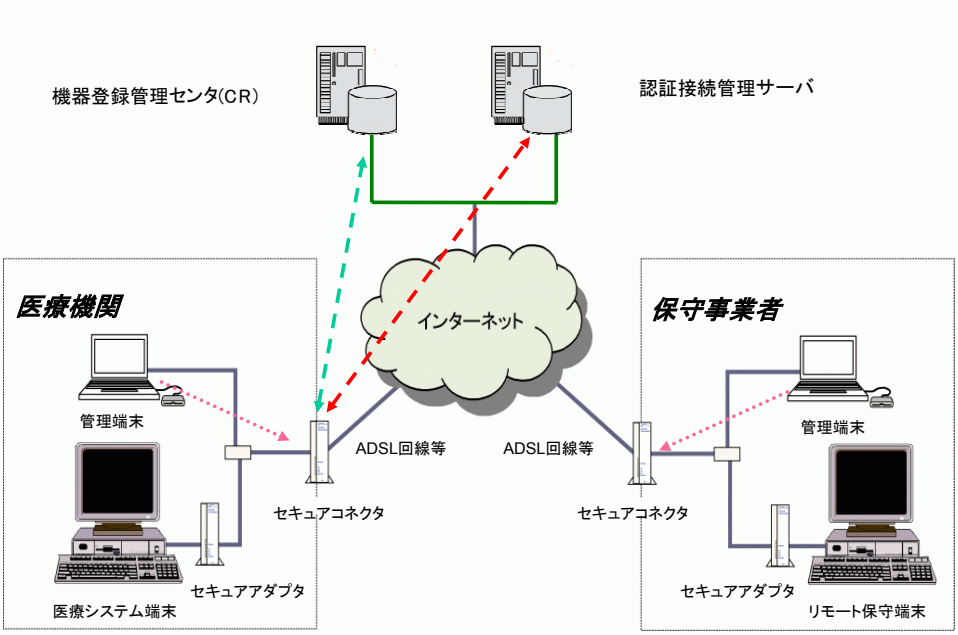


図2-5　ネットワーク基盤の構成

実証実験で実施した動作検証により、以下のことが実証された。

・セキュアコネクタ、セキュアアダプタに対して不正アクセスができないこと。
・セキュアコネクタ対セキュアコネクタ間の通信では通信データが暗号化されていること。
・ある一つのセキュアコネクタ、セキュアアダプタに障害が発生しても、他の正常なセキュアコネクタ、セキュアアダプタには影響を与えないこと。

これらの機能が有用かつ有効であることが実証され、機器対機器の相互認証の有効性と通信経路の安全性が確認されたことにより、本事業の検証テーマであるセキュアなネットワーク基盤の安全性が有効に担保された仕組みが実現されたといえる。

しかし、このセキュアなネットワーク基盤の普及のためには、いくつかの課題が明らかになった。

・認証接続管理サーバのバックアップ等ネットワーク基盤関連の障害対策の検討
・SPC 要件（Security and Privacy Requirements for Remote Servicing）の未対応事項の検討
・機器登録管理センタ、認証接続管理システムの運用方法の確立

(2) リモートサービスの運用性

(a) リモートサービスの運用性検証

実証実験で実施したリモートサービスの運用性検証により、以下のことが実証された。

- 従来のネットワーク環境での実施結果とセキュアなネットワーク基盤上での実施結果を比較したが、リモートサービス運用上の差異はまったくなかった。
- 保守対象のシステムに一切手を加えることなく、また既存のリモートメンテナンスのアプリケーションがそのまま稼働した。
- セキュアなネットワーク基盤の環境構築にあたって、既存のネットワーク環境に特別な対策を行うことなく、リモートサービスが行えることが確認された。

また、ヒアリング調査により、以下の評価を得た。

- 保守事業者からの意見としては、セキュアなネットワーク基盤導入により保守事業者の作業効率が上がることに対する期待感がうかがえる評価を得た。
- 医療関係者からの意見としては、レスポンスの向上など、保守サービスの品質向上がメリットであるとの評価を得ているが、通信経路以外の部分から個人情報が漏洩する危険性に関して危惧を抱いていることが明らかになった。
- リモートサービスを実現するためには、通信経路のセキュリティ確保だけでなく、サービスを実現する環境全体における個人情報保護に関する対策の整理が求められた。

セキュアなネットワーク基盤での常時接続が可能な環境によって、予防保守の運用からリモートサービスの実施まで、一連の運用が行えることが確認された。このことによって、モダリティ、医事会計システム、電子カルテシステムの予防保守等の新しい運用が可能となると考えられ、医療機関へ新しい保守サービスの提案が今後できるものと考えられる。

(b) セキュアなネットワーク環境構築の効率性

医療機関において新規設置または機器増設に関して、セキュアアダプタと保守対象のシステムを物理的に増設した後、医療機関側と保守事業者側それぞれのセキュアアダプタに対し接続情報を設定することによって、簡便に機器増設が行えること、また、増設後の通信が問題なく行えることが確認された。

セキュアネットワーク基盤の障害時の影響については、総じて障害発生時の状況に関する情報の入手のしやすさや分かりやすさについて改善の余地があると考えられる。これらについては、セキュアネットワーク基盤の本質的な問題ではなく、基盤を実装するアプリケーションの機能やインタフェースの改善で対処が可能であると考えられる。

（c）その他

セキュアコネクタの最大の利点はセキュリティの確保の他に、複数の保守事業者からのアクセスポイントを医療施設内で 1 つに統合できる点である。このことは、外部からの不正侵入のアクセスポイントを減らし、医療機関にとっても回線工事や管理の面で大きなメリットとなる。

3. 多機能 IC チップ等を活用した情報サービスシステム基盤における TPM の適用性の調査研究

3. 1　TPM の概要

3. 1. 1　TPM の概要

TPM（Trusted Platform Module）は PC プラットフォームにおけるセキュリティ技術の業界団体 TCG（Trusted Computing Group）が策定した仕様に準拠したチップである。

TPM は、OS や他のハードウェアから独立して機能するセキュリティ用ハードウェアチップなので、国内の PC 市場では「セキュリティチップ」と表記されたりしている。外部からの攻撃にも強く、従来は HDD に格納していた認証に用いる暗号鍵などの情報を安全に格納・管理することができる。暗号処理専用のマイクロプロセッサとセキュア通信で利用される秘密鍵を含んだ EEPROM が内蔵されており、PC のマザーボード上に実装され、TPM が PC 起動時に BIOS の不正改ざんやチップの不正交換などをチェックし、なんらかの異常を発見すると起動させない。また、チップ内に保存された秘密鍵は決してチップ外に出さない。更に、その秘密鍵を使ってファイルの暗号化も可能である。RSA 暗号、乱数生成、ハッシュ処理はチップ内にて行うといった特徴がある。

3. 1. 2　TPM の活用

PC のセキュリティを確保するためにはソフトウェアのみでは不十分でハードウェアによる保護が必要と考えられる。なぜなら、ソフトウェアで高度なセキュリティを構築してもハードウェアで守られていない限り、ハードディスクへのダイレクトアクセスやウィルス等の悪意あるソフトウェアによって改ざん、盗聴といった危険性が潜んでいるからであり、たとえ、暗号化されて記録されたデータでも、鍵データが流出すれば何の防御にもならないのである。

(1) ID、パスワード管理／自動入力

TPM のパスワード管理機能を使用することで、サーバアプリケーションを変更することなく複数アプリケーションのパスワードを TPM の一つのパスワードにまとめることができる。例えば Web アプリケーションの ID・パスワードをユーザに代わって管理・入力することができ。利用者のパスワード管理負荷を大幅に軽減し、強固に保護することができる。

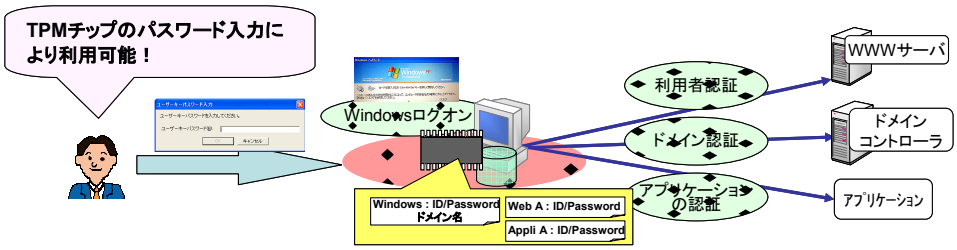


図3-1　ID、パスワード管理/自動入力

(2) ファイル／フォルダ暗号化

暗号化されたファイルでも通常は同じハードディスク内に暗号鍵を持っていることが多いので、データを解読される恐れがある。しかし、TPM で暗号化されたデータの暗号鍵はそのチップで管理され、ハードディスクを丸ごとコピーしたとしても暗号ファイルを解読できない。暗号化フォルダを指定すると、そのフォルダの中のファイルはすべて暗号化されます。暗号化されたファイルは直接アプリケーションで読み書きが可能です。万が一の PC の盗難や不正使用に安心です。

図3-2　ファイル／フォルダ暗号化

（3）PC の機器監査

PC の機能を制限するために BIOS の設定をしていても不正に変更されてしまうことがある。しかし、TPM を利用することで、利用者による BIOS、Boot Block コードや BIOS 設定、盗難者によるハードウェアデバイスの不正な変更を検知し、ログオンを制限することができる。

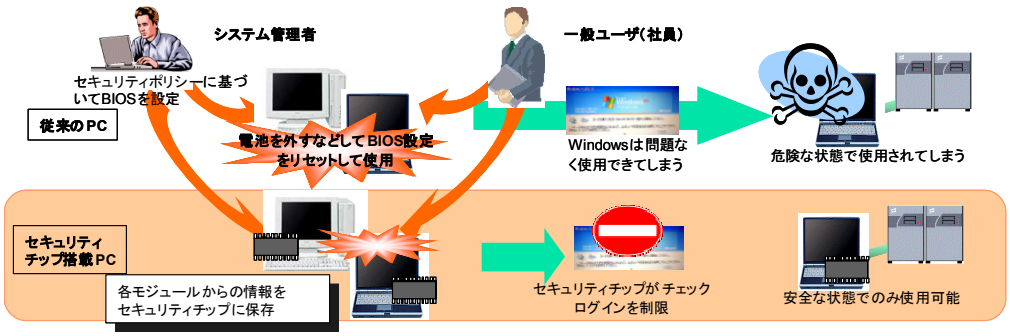


図3-3　PC の機器監査

3．1．3　TPM による PC セキュリティの普及状況

国内で TPM を搭載した PC を出荷しているのは、富士通、NEC、IBM、HP の 4 社（2004 年 10 月現在）である。但し、いずれも TCG 仕様の TPM を搭載しているが、各社で用意している TPM を使用して動作するアプリケーションの機能は異なる。

3. 2　多機能 IC チップ等を活用した情報サービスシステム基盤における TPM の適用性

TPM が多機能 IC チップ等を活用した情報システム基盤に適用できるかどうかを、多機能 IC チップの基本機能、多機能 IC チップフレームワーク機能、医療システム機器におけるセキュアネットワーク機能の 3 点から比較・検討を行った。

(1) チップ基本機能の適用性

認証機能、耐タンパ性、暗号機能といった機能レベルにほぼ差はないが、TPM は多機能 IC チップの最大の特長であるアプリケーション制御機能（アプリケーション追加・削除機能及び実行機能）を有さないため、チップ単体レベルでの TPM の多機能 IC チップへの代替はできない。但し、PC 上のアプリケーションとの連携により多機能 IC チップ相当の機能の実現の可能性はある。

(2) 多機能 IC チップフレームワーク機能における TPM の適用性

多機能 IC チップフレームワーク機能について、TPM の適用性を以下のとおり検討した。

- 多機能 IC チップフレームワーク機能における機器登録 ID（識別子及び製造番号）の格納機能については、TPM にその機能がないため、基本的には多機能 IC チップと全く同じ機能とはならず、TPM ではこれらの情報を暗号化して HDD 上に置き、暗号化した鍵を TPM 内部で管理する方法となる。よって適用性については、上位のミドルウェア、アプリケーションを含めた全体の機能による実装方式を検討する必要がある。
- 輸送鍵及び仮鍵によるロック機能は、TPM にはこの機能がないため、適用することができない。
- 仮証明書及び機器登録情報については、識別子の場合と同様に、情報を暗号化して HDD 上に置き、暗号化した鍵を TPM 内部で管理する方法となり、適用性については実装方式及び運用方法についての調査検討を必要とする。
- AP 管理については、TPM がチップ内にアプリケーションをダウンロード／実行／削除などの管理機能を持たないため、多機能 IC チップの最大の特徴であるチップ内での処理は行うことができない。しかし、最上位の業務アプリケーションからの機能として考えると、TPM の適用性については、前述のように情報を暗号化して HDD 上に置き、暗号化した鍵を TPM 内部で管理する方法を使って、実装方式及び運用方法について調査検討を行うことにより同等の機能を実現することが可能である。

多機能 IC チップフレームワーク機能への適用における TPM の技術面の最大の課題は、チップ自身の持つ AP 管理で、TPM ではこの機能は定義されておらず、また根本的なアーキテクチャが異なっている。対策として、多機能 IC チップ内のアプリケーションの機能を TPM-PC の OS 上のアプリケーションで実現する方法が考えられる。

(3) 医療システム機器におけるセキュアネットワーク機能への適用性

ユーザポリシー（アクセス許可情報）設定及び認証接続管理事業者への通知機能についても、ユーザポリシー情報のローカルでの管理方法、認証接続管理事業者への通知方法それぞれが、TPM チップでは上位の OS 上のアプリケーションで実現することになる。一部のネットワーク機器のように、OS またはその OS 上のアプリケーションの動作環境が存在しない場合には、この機能を実現することは難しいと考えられる。

以上の技術面、運用面での検討の結果から、TPM は、機能の精査、アプリケーションレベルでの実装、セキュリティ部分の詳細分析、運用形態などの点について、いくつかの課題を残しつつも、適用の可能性があると考えられる。このことから、TPM のシステムを適所に配置することにより、既存 PC アプリケーションの流用性や全体コストの低減が期待され、幅広い医療機関でのセキュアネットワーク環境の適用に対してプラスに働くものと考えられ、結果として医療分野でのセキュアネットワーク環境の進展に寄与するものと考えられる。

4. 医療分野リモートサービスへの多機能 IC チップを利用したセキュアなネットワーク基盤の適用性、複数のセキュアネットワーク間での相互運用性確保のあり方に関する調査研究

医療分野リモートサービスへの多機能 IC チップを用いたセキュアなネットワーク基盤の適用性として、機能的な適用性と効果・メリット・市場性等について検討を行った。医療分野リモートサービスでの今後のセキュリティ基盤構築の方向性を明らかにするとともに、多機能 IC チップを用いた複数のセキュアネットワーク間での相互運用性確保のあり方について検討を加え、医療分野への導入についての将来方向について検討した。

本調査における調査項目と調査方法を表 4-1 に示す。

表4-1　調査項目と調査方法

調査テーマ	調査項目	調査方法
医療分野リモートサービスへの多機能 IC チップを用いたセキュアなネットワークの適用性	多機能 IC チップを用いたセキュアなネットワークの特徴	NICSS 資料、有識者ヒアリング等により、従来のセキュアネットワーク技術や VPN 装置技術と比較した多機能 IC チップを用いたセキュアネットワークの特徴を以下の観点で整理する。 機能面、運用面、利用面、導入条件、その他。
	医療分野で考えられるリモートサービスやネットワーク活用型サービスの分類、整理	国内及び欧米・アジアの先進事例や計画事例等を参考に医療分野でのリモートサービスやネットワーク活用型サービスを分類・整理するとともにネットワークセキュリティ上のニーズ特性を分類・整理する。
	多機能 IC チップを用いたセキュアネットワークの適合性の検討と有望サービス抽出	・ネットワークセキュリティ要件と機能的適合性、効果・メリットの検討。 ・市場性と普及条件の検討。
多機能 IC チップを用いた複数のセキュアネットワーク間での相互運用性確保のあり方	多機能 IC チップを用いたセキュアネットワーク技術の概要と特徴	認証基盤のフレームワーク、プロトコル（通信手順／レイヤ／メッセージ形式）、暗号化手法、証明書などの検討。
	認証サービス等に関する互換性確保の方法と特性	・異種ネットワーク間の接続等に関する主な手法と適用上の留意点の検討。 ・PKI 相互運用性確保のための主な手法と適用上の留意点の検討。
	医療分野における互換性確保の方向性と課題	方向性、課題の検討。

4．1　医療分野リモートサービスへのセキュアなネットワーク基盤の適用性

オープンネットワークとの親和性、個人の特定の厳格性、多段階認証、アプリケーションの市場性、という視点から整理し、検討を行った。

(1) 医療分野リモートサービスの分類

各種資料を参考に医療分野リモートサービスのアプリケーション技術を大きく 5 つの観点「医対医」、「医対患」、「医対ベンダ」、「テレケア」、「医対行政」（便宜上、医療従事者と医療機関の医療側を「医」、患者を「患」という）で分類を行った。その分類を以下の図 4-1で示す。

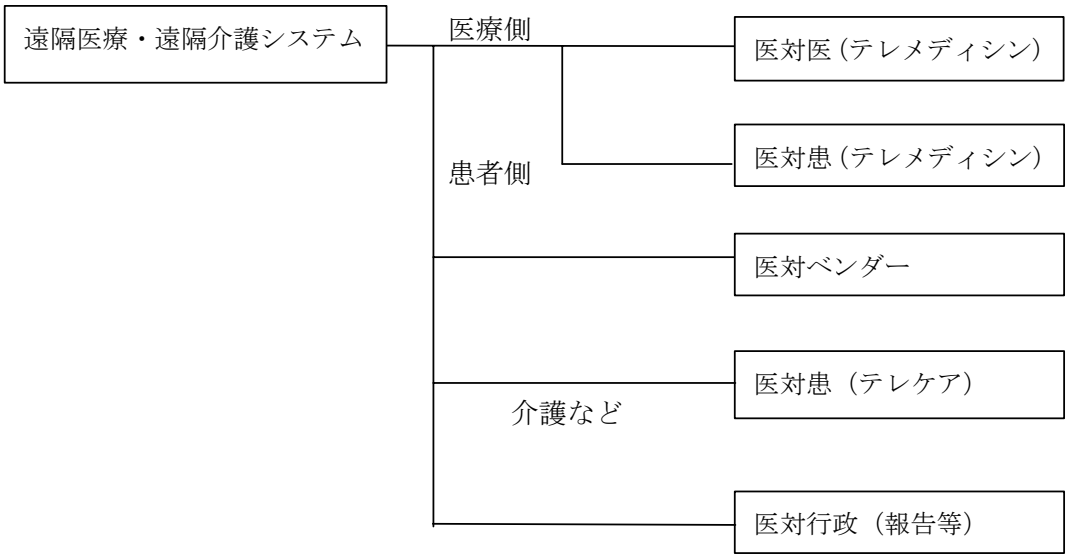


図4-1　医療分野でのリモートサービスの大分類

(2) 多機能 IC チップを用いたセキュアなネットワーク基盤の適用に関する特性

分類したそれぞれのアプリケーション技術に対して、オープンネットワークへの親和性、個人の特定の厳格性、多段認証階層、アプリケーションの市場性、という視点からセキュアなネットワーク基盤の適用度を検討した。

(a) 医対医（医療機関連携テレメディシン）アプリケーション

インターネットのオープン性や回線状況の安定性、HPKI 確立の問題などからそのまま適用可能かは、現時点では課題が残されている。

(b) 医対患（対患者テレメディシン）アプリケーション

現状ではサービス例は少ないが潜在的なニーズは高く、適用が有望なアプリケーションが多い。IC カード認証のインターネット VPN と同じネットワークにより SARS など感染症情報の収集やレセプト請求などとの複合利用を行っているなどの例があり、中長期的には適用が有望と考えられる。

(c) 医対ベンダアプリケーション

必ずしも大きな市場ではないが、確実な需要があり、また多段認証のニーズが高いことなどから、短中期的には適用が有望と考えられる。

(d) 医対患者（テレケア）アプリケーション

医対患（対患者テレメディシン）アプリケーションとほぼ同様と考えられる。

(e) 医対行政等請求・報告アプリケーション

多段認証のニーズは高くないが、リモートメンテナンスとの複合や特定の疾患情報の収集など、オンデマンド型での VPN 構築ケースなどの適用性が高いと考えられる。

4．2 複数のセキュアネットワーク間での相互運用性確保のあり方

(a) 認証ポリシー、認証実施規定、認証システムの実装方式、条件別の VPN 設定可否などの運用ルールといった、レイヤ毎の相互運用基準の確立が必要である。

(b) 相互運用基本方式の検討（機器レベル認証の相互確認・信頼方法)、VPN 設定情報及びその交換方法、VPN 管理情報の管理方法（交換方法）など、異種チップによる認証ドメイン間をまたがる機能について検討が必要である。

(c) IPSec での採用モードや機能、ネゴシエーション等に関するデファクトの実装規約の採用などを検討する必要がある。

(d) 院内外でのオンライン電子保存基準や SPC（Security and Privacy Requirements for Remote Servicing）基準、IHE（Integrating the Healthcare Enterprise）の ITI（IT Infrastructure）との適合性確認と医療分野での実装レベルの標準化推進が求められる。

(e) 医療情報ネットワーク基盤検討会（平成 15 年 6 月～平成 16 年 12 月）の HPKI の拡張として機器認証、メンテナンス要員の認証が必要であるが、別の認証実施基準に基づくかどうかの検討も含めた認証方式の標準化が求められる。

5. まとめ

5. 1　成果

5. 1. 1　研究開発・実証実験

(1) 実証実験について

本事業では多機能 IC チップを活用したセキュアなネットワーク基盤を構築し、保守事業者と医療機関との間で医療システム機器の無人リモートサービスの実現を目指した実証実験を行った。

モダリティ、医事会計システム及び電子カルテシステムの予防的保守サービスのための状態監視や自動ファイル転送等の研究開発を実施し、それら機能の実証実験を行った。その結果、リモートメンテナンスの安全性と運用の有効性や効率性が実証された。また、実運用に向けての課題や問題点を抽出した。

実証実験で明らかになった成果は以下のとおりである。

(a) ネットワーク基盤の安全性

セキュアなネットワーク基盤における機器対機器の相互認証と通信経路の安全性が確認されたことにより、本事業のネットワーク基盤の安全性が実証された。リモートサービスの普及のために必要な仕組みが実現された。

(b) リモートサービスの運用性

セキュアなネットワーク基盤での常時接続可能な環境によって、予防保守の運用からリモートサービスの実施まで、一連の運用が行えることが確認された。保守事業者にとっては、作業効率の向上による保守コストの削減や、予防保守サービスの実現など新たな保守サービスを医療機関に提供することが可能になった。医療機関にとっても、複数の保守事業者からのアクセスポイントを医療施設内では 1 つのセキュアコネクタに統合することが可能となるため、外部からの不正侵入のアクセスポイントを減らし、医療施設内の回線工事や管理の面で大きなメリットとなる。

5. 1. 2　調査研究

(1) 多機能 IC チップ等を活用した情報サービスシステム基盤への TPM の適用性

技術面、運用面での調査の結果から、TPM は、機能の精査、アプリケーションレベルでの実装、セキュリティ部分の詳細分析、運用形態などの点について、いくつかの課題を残しつつも、多機能 IC チップ等を活用した情報サービスシステム基盤適用の可能性があると考えられる。このことから、TPM のシステムを適所に配置することにより、既存 PC アプリケーションの流用性や全体コストの低減が期待され、幅広い医療機関でのセキュアネットワーク環境の適用に対してプラスに働くものと考えられ、結果として医療分野でのセキュアネットワーク環境の進展に寄与するものと考えられる。

(2) 医療リモートサービス分野への多機能 IC チップを利用したセキュアなネットワーク基盤の適用性、複数のセキュアネットワーク間での相互運用性確保のあり方

医療リモートサービス分野への多機能 IC チップを用いたセキュアなネットワーク基盤の適用性の調査研究として、機能的な適用性と効果・メリットと市場性等について検討を行った。今後の医療分野のセキュリティ基盤構築の方向性が明らかになり、多機能 IC チップを用いた複数のセキュアネットワーク間での相互運用性確保のあり方について検討することによって、医療リモートサービス分野への多機能 IC チップを用いたセキュアなネットワーク基盤導入についての将来方向が明らかになった。

5. 2　展望と課題

今回の実証事業からビジネス展開していく上で課題は下記のとおりである。

(1) 実証実験についての課題

セキュアなネットワーク基盤上でリモートサービスの実証実験を実施して、下記の課題が明らかになっている。

- ネットワーク基盤の障害対応の充実
  （認証接続管理のバックアップ機能等）
- SPC（Security and Privacy Requirements for Remote Servicing）要件の未対応事項の展開
  （操作のトレーサビリティを担保できる操作ログの取得等）
- 個人情報保護の観点から運用面、体制面を含めた取組み

(2) 調査研究からの課題

異種ネットワーク間の相互運用性の確保については、下記の課題が明らかになっている。

- IPsec の通信モードの整合
- 異種ネットワーク接続時の認証
- レイヤ別の認証運用基準の設定

TPM の多機能 IC チップ機能への適用性については、PC 上のミドルウェア開発により多機能 IC チップ相当の機能を実現すべきである。

(3) 今後の展望

上記（1)、(2）の課題より医療分野における多機能 IC チップを活用したセキュアなネットワーク基盤の普及に向けて、下記内容での研究開発と実証実験が必要であると考える。

- 実フィールドでの実証実験を実施し、実際の運用面から個人情報保護対策などを含めた検証を行うこと。
- VPN 間、認証方式間での相互運用性に関する実証実験を行うこと。
- 多機能 IC チップを活用したネットワーク基盤と TPM を利用した 2 階層 PKI 方式の実証実験を行うこと。

これらの実証実験を行うためには、医療情報の地域連携を考慮した実施体制の構築が望まれる。