MC-05

サービス提供機関から携帯電話端末の安全な耐タンパデバイス利用に関するガイドライン

平成 25 年 5 月 20 日　　1.0 版

一般社団法人電波産業会

高度無線通信研究委員会

モバイルコマース部会

サービス提供機関から携帯電話端末の安全な耐タンパデバイス利用に関するガイドライン

目次

1. はじめに.....1
1.1 対象範囲.....1
1.2 目的.....1
1.3 モバイルアクセスシステム概要.....3
1.4 前提条件.....5
1.5 セキュリティ要件.....6
1.6 用語.....8
2. モバイルアクセスシステム.....9
2.1 機能.....9
2.2 インタフェース.....10
2.3 プロトコル.....11
2.4 セキュリティ対策.....14
【付録】インタフェースの詳細(実装例).....16
1. 共通アプリ起動インタフェース.....17
2. APDU 移譲インタフェース.....19
3. 共通アプリ連携インタフェース.....21
4. APDU 実行結果通知インタフェース.....25
5. 再アクセスインタフェース.....27

本ガイドラインは、平成 23 年度　総務省「行政業務システム連携推進事業（アクセス手段としての携帯電話の利便性向上方法の検証）の研究成果の一部をガイドライン化したものである。
なお、本ガイドラインは、携帯電話会社やサービスプロバイダ及び利用者に対しても、強制力や責務を負うものではない。

1. はじめに

1.1 対象範囲

本ガイドラインは、図 1-1 に示すように、複数のサービス提供機関が、携帯電話端末利用者の耐タンパデバイスへの認証情報や個人情報などの ID 情報を書き込む。また、書き込んだ ID 情報を読み込んでサービス提供に利用する。このような、耐タンパデバイスへの ID 情報の書き込みと読み込みを安全かつ容易に行うことを本ガイドラインの対象範囲とする。

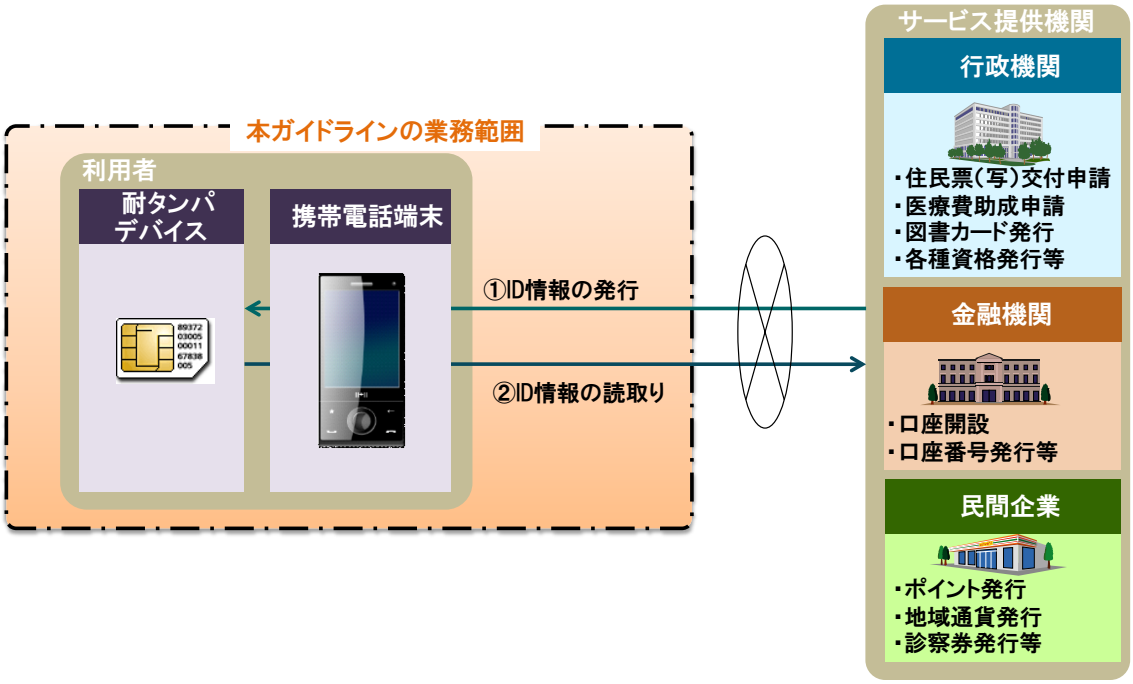

図 1-1 本ガイドラインの業務範囲

1.2 目的

複数のサービス提供機関が、携帯電話端末利用者の耐タンパデバイスへの ID 情報の書き込みや読み込みを行おうとする場合、現状では図 1-2 に示すように、サービス提供機関ごとに携帯電話端末アプリケーションを開発・運用する必要がある。また、利用者は各サービス提供機関が提供する携帯電話端末アプリケーションを個別にダウンロード・インストールする必要がある。さらに今後は携帯電話端末の OS のオープン化が進むことが想定されるため、携帯電話端末アプリケーションのセキュリティを確保する仕組みも必要となる。

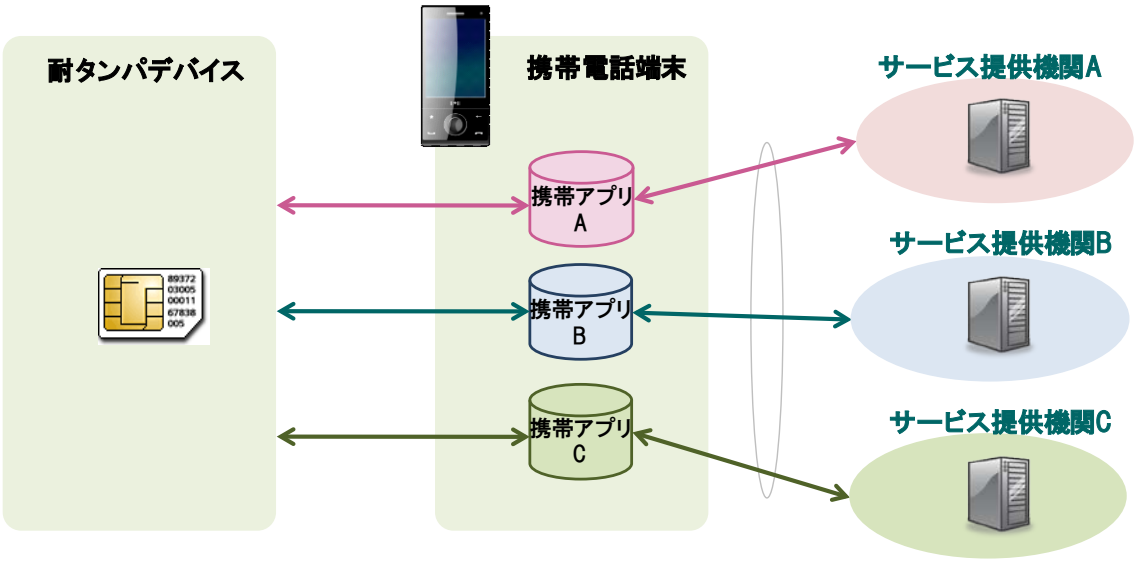

図 1-2 業務範囲の現状と課題

上記現状の課題を解決するために、図 1-3 に示す構成のモバイルアクセスシステムに関し、本ガイドラインを定める。具体的には、サービス提供機関が耐タンパデバイスにアクセスする際に共通的に利用できるモバイルアクセスサーバおよび携帯電話端末上の共通アプリからなるモバイルアクセスシステムに関するガイドラインを定める。

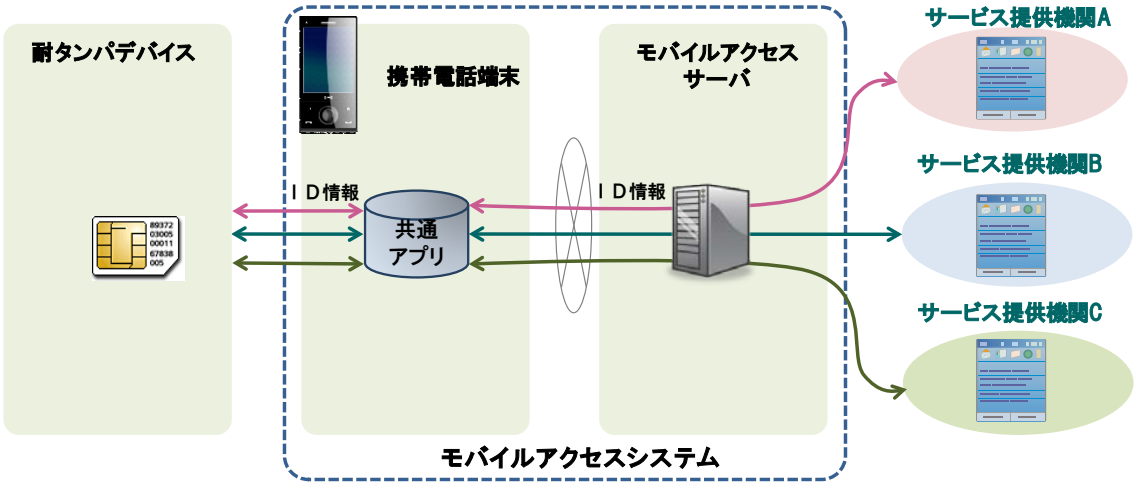

図 1-3 現状課題の解決方法

1.3 モバイルアクセスシステム概要

モバイルアクセスシステムの全体構成を図 1-4 に示す。行政機関や、金融機関や民間企業なども含めて複数のサービス提供機関が、携帯電話端末を使う利用者に対して種々のサービスを提供することを想定している。今回対象とするサービスは、何らかの価値を有する情報（ID 情報）を利用者に付与して、その ID 情報を利用することを前提としたサービスを対象とする。ID 情報は、利用者の携帯電話端末からアクセスできる耐タンパデバイスに保存するものとする。

耐タンパデバイスへの情報の書き込み、および読み込みには、通常、サービス提供機関が個別に耐タンパデバイスの自身の領域に対してセキュアなチャネルを構築し、そのチャネルを経由してのみ読み書きが可能となる。本ガイドラインでは、複数のサービス提供機関への負担を軽減するために、前記耐タンパデバイスへの情報の読み書きを代行するモバイルアクセスサーバをモバイルアクセスシステム側に用意し、サービス提供機関の負担を軽減する。

また、耐タンパデバイスと直接データの送受信を行う携帯電話端末アプリケーションに関しても、従来であれば個々のサービス提供機関が自身のサービスのために携帯電話端末アプリケーションを個別に開発する必要があったが本ガイドライン、今回の提案では、複数のサービス提供機関が共通的に利用できる共通アプリで処理することとする。

また、耐タンパデバイスへの ID 情報の読み書きに対する結果通知サービスや、耐タンパデバイスからの ID 情報の読み込みを本人認証に利用したのちの実際のサービスなどは、Web ベースで提供されることを想定している。よって、携帯電話端末内での共通アプリとブラウザの連携、モバイルアクセスシステム内でのモバイルサイトとモバイルアクセスサーバの連携を実現することで安全なサービス提供の基盤を実現する。

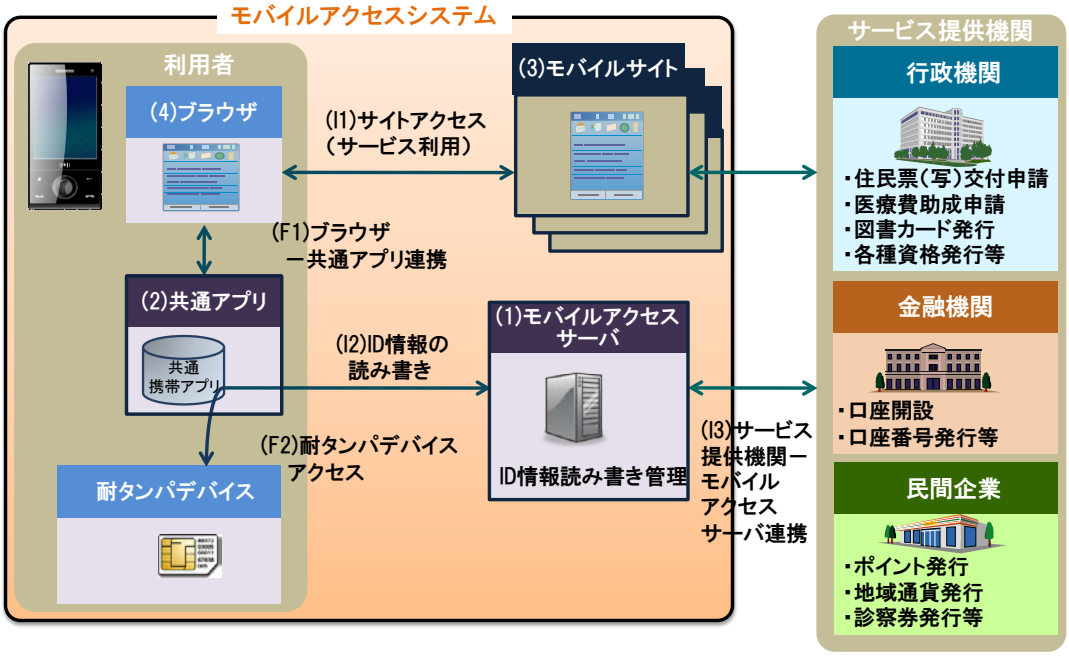

図 1-4 モバイルアクセスシステムの全体構成

エンティティの説明

- サービス提供機関:行政機関や金融機関､民間企業などの ID 情報を利用者に付与して、その ID 情報を利用することを前提としたサービスを提供する機関
- モバイルサイト：サービス提供機関ごとに構築する携帯電話端末向けサイト
- モバイルアクセスサーバ：サービス提供機関との契約に基づいて、利用者の耐タンパデバイスとセキュアな通信路を確保し暗号化した IC カードコマンドの送受信を行うサーバ。
- 共通アプリ：モバイルアクセスサーバと通信を行い、受信したデータを耐タンパデバイスに送信し、耐タンパデバイスからのレスポンスをモバイルアクセスサーバに返信する携帯電話端末アプリケーション。共通アプリ自身は秘密情報を保持しない設計とすることでオープンな携帯電話端末においても安全性を確保する。また、共通アプリとブラウザは一つの携帯電話端末内のアプリとして実装することもできる。
- 耐タンパデバイス：IC チップを搭載したデバイス。デバイスは、UICC（Universal Integrated Circuit Card）などを想定する。

具体的には、下記の流れで処理が実行される。

1. 利用者が携帯電話端末内のブラウザでモバイルサイトにアクセスする(**図 1-4** の(I1))。
2. モバイルサイトからのレスポンスによってブラウザから共通アプリが起動される（**図 1-4** の(F1))。
3. 共通アプリからモバイルアクセスサーバに接続し、モバイルアクセスサーバから ID 情報の読み書き要求を受ける（**図 1-4** の(I2))。
4. ID 情報の管理はサービス提供機関が行う。当該 ID 情報をサービス提供機関からモバイルアクセスサーバに通知する。(**図 1-4** の(I3)のようにサービス提供機関とモバイルアクセスサーバ間で直接通知する方法と､(I1)と(I2)のインタフェースを使って共通アプリを経由して通知する方法がある)。
5. 上記ステップで ID 情報を共通アプリが耐タンパデバイスに書き込む(**図 1-4** の(F2))。
6. 書き込み後の結果通知は、モバイルアクセスサーバを経由して、さらにブラウザを経由して、モバイルサイトに通知され、最終的にブラウザの画面でユーザに通知される。

1.4 前提条件

以下に本ガイドラインにおける前提条件を示す。なお、ID 体系の仕組みやその管理方法に関する仕様、個別のサービスに関する仕様は、本章の範囲外とする。

■携帯電話端末に関する前提条件

- データ通信が行える端末を前提とする。音声通話だけしかできない端末は対象としない。
- 今後は携帯電話端末の OS のオープン化が進むことが想定される。そのような OS 上でも安全に耐タンパデバイスへアクセスできるようにするため、携帯電話端末上ではマルウェア等が動作する可能性があり、必ずしも安全性が確保されるとは限らない。つまり耐タンパデバイスへアクセスする鍵などの秘密情報の管理を正しく行うことができない場合があるという前提を置いたうえで仕様の検討を行うものとする。
- ブラウザから携帯電話端末内のアプリが起動できるものとする（ただし、共通アプリとブラウザを一つの携帯電話端末のアプリとして実装する場合は、その限りではない)。
- 逆に、携帯電話端末内のアプリからブラウザを起動できるものとする（ただし、共通アプリとブラウザを一つの携帯電話端末のアプリとして実装する場合は、その限りではない)。
- 耐タンパデバイスにアクセスできる機能を有するのもとする。

■耐タンパデバイスに関する前提条件

- 携帯電話端末を使ってデータの送受信ができるものとする。
- 耐タンパデバイスには、カードアプリケーションが格納されているものとする。
- Security Domain は、PERSONALIZED、カードアプリケーションが SELECTABLE になっている状態とする。
- 耐タンパデバイス内の処理は、安全に行えるものとする。つまり、耐タンパデバイス上で動作するアプリケーションは、正当なサービス提供機関によって作成され、正当な方法で耐タンパデバイス内へ格納されており、その動作も正しく動くものとする。
- 耐タンパデバイスは、マルチアプリケーション対応とし、複数のサービス提供機関が相乗りできるものとする。異なるサービス提供機関のＩＣカードアプリケーションはファイアウォールで適切に守られているとする。
- 平成２１年度の総務省の調査研究「携帯電話から電子行政サービス等へのアクセス技術の調査研究」で対象とされた携帯電話端末内に国が発行する情報を書き込み利用する公的認証情報方式における UICC（Universal Integrated Circuit Card）を前提とする。

- 携帯電話端末に対して OTA(Over the Air)で耐タンパデバイスへアクセスするための唯一の世界標準である GlobalPlatform に準拠した UICC を前提とする。

■ネットワークに関する前提条件

- サービス提供機関とモバイルアクセスサーバはインターネットに接続されるため、携帯電話端末とサービス提供機関間、携帯電話端末とモバイルアクセスサーバ間は、モバイル網以外のオープンなネットワークを通ることになる。このため、必ずしも安全性が確保されるとは限らないものとする。 つまり、携帯電話端末とサービス提供機関間、携帯電話端末とモバイルアクセスサーバ間は、ネットワーク上のデータの盗聴や改ざんの恐れがあるとする。
- サービス提供機関とモバイルアクセスサーバ間の通信は VPN や専用線などで保護されるため安全であるとする。

■サービス提供機関に関する前提条件

- 偽造や改ざん、漏洩などから守るべき何らかの価値を有する情報（ID 情報）を携帯電話端末に接続された耐タンパデバイスに対して付与し、また、耐タンパデバイスから読み込み、その ID 情報を利用することをおこなうサービス提供機関を対象とする。
- サービス提供機関の動作は、運用も含め正しく安全に行われるものとする。
- サービス提供機関とモバイルアクセスサーバは事前の契約に基づいて鍵の共有などを行っているものとする。

■モバイルアクセスサーバに関する前提条件

- モバイルアクセスサーバ内の動作は、運用も含め正しく安全に行われるものとする。
- サービス提供機関とモバイルアクセスサーバは事前の契約に基づいて鍵の共有などを行っているものとする。

1.5 セキュリティ要件

前述の前提条件のもとで、本ガイドラインのシステムは、以下に示すセキュリティ要件を満たす必要がある。

(1) 不正な携帯電話端末アプリケーションへの対応

(1-1) 悪意のある携帯電話端末アプリケーションが耐タンパデバイス内のセキュアデータへのアクセスの防止

(2) 通信路の安全性の確保

(2-1) サービス提供機関―(共通アプリ)―モバイルアクセスサーバ間の通信路の安全性の確保

(2-2) モバイルアクセスサーバー(共通アプリ)－耐タンパデバイス間の通信路の安全性の確保

(2-3) サービス提供機関－モバイルアクセスサーバ間の通信路の安全性の確保

(3) 成りすまし防止

(3-1) サービス提供機関の成りすましの防止

(3-2) モバイルアクセスサーバの成りすましの防止

1.6 用語

略語	説明
携帯電話アプリケーション	携帯電話端末上で動作するユーザ向けのインターフェースを提供するアプリケーション。
UICC	Universal Integrated Circuit Cardの略。電話番号を特定するための固有のID番号が記録されたICカード。
カードアプリケーション	UICC上で動作するJavaCardアプリケーション。
Security Domain	カードアプリケーションを管理するためのカードアプリケーション。設定に応じて、カードアプリケーション等のインストールや削除などを行う。
PERSONALIZED	必要な個人化データや鍵が設定された状態
SELECTABLE	カードアプリケーションを選択可能な状態。
OTA	Over The Air の略。無線ネットワークを利用したデータの受信・同期などを行う。
Globele Platform	多機能 IC カードを実現するために必要な IC カードの発行およびその管理、アプリケーションの管理、端末などの標準仕様の開発や管理を行う非営利組織。
APDU	Application Protocol Data Unitの略。 ISO7816仕様で規定された携帯電話端末やサーバなどとUICC内のカードアプリケーション間のプロトコルでやりとりされるリクエストとレスポンス内容。
JavaScript	Web ブラウザなどでの利用に適した簡易プログラミング言語。
HTTP	Hypertext Transfer Protocolの略。 Webサーバとクライアント(Webブラウザなど)間でデータを送受信するのに使われるプロトコル。
XML	Extensible Markup Language の略。 文書やデータの意味や構造を記述するためのマークアップ言語の一つ。

2. モバイルアクセスシステム

2.1 機能

以下に、各エンティティの機能を記述する。

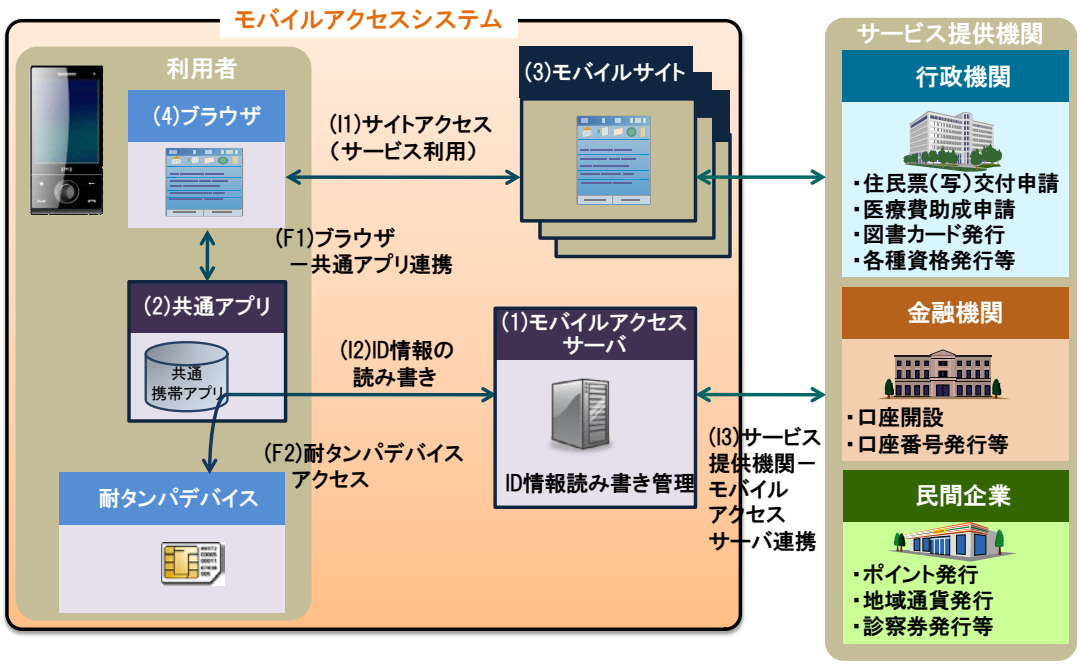

図 2-1 モバイルシステム図

（1）モバイルアクセスサーバ（全機能）（図 2-1 の(1)）

- 受付処理機能：
  サービス提供機関から送信された情報(サービス事業者 ID、受付番号、APDU 生成年月日、APDU 実行順序、APDU コマンド)を受け取り、情報が正しい場合は、受け取った情報を DB に登録する。
- 共通アプリアクセス機能：
  サービス提供機関から共通アプリ経由で転送されるデータが本当に正しいサービス提供機関から送信されたデータなのかを確認する。さらに、携帯電話端末内の共通アプリを経由して、耐タンパデバイスとセキュアセッションを確立し、携帯電話端末内の共通アプリに対して暗号化されたコマンドを送受信し、結果をサービス提供機関に返信する。

（2）共通アプリ（全機能）（**図 2-1** の(2)）

- APDU 転送機能：
  モバイルアクセスサーバから受信した暗号化されたコマンドを耐タンパデバイスへ送信し、耐タンパデバイスからのレスポンスをモバイルアクセスサーバに返信する。

（3）モバイルサイト（一部機能）（**図 2-1** の(3)）

- ID 情報送信機能：
  耐タンパデバイスに送信したいコマンドをモバイルアクセスサーバに移譲し、かつ、携帯電話端末のブラウザを経由して、共通アプリを起動させ、耐タンパデバイスに ID 情報を送信する。
- 処理結果受信機能：
  モバイルアクセスサーバから耐タンパデバイス内での処理結果を受信し、返される処理結果が本当に正しいモバイルアクセスサーバから送信されたデータなのかを確認する。

（4）ブラウザ（**図 2-1** の（4））

- ブラウザから携帯電話端末内のアプリを起動する。
- 携帯電話端末内のアプリからブラウザが起動される。。

2.2 インタフェース

以下に、各インタフェースを記述する。

（1）共通アプリ起動インタフェース（**図 2-1** の I1 および F1）

- JavaScript で共通アプリを起動する。
- 要求元：モバイルサイト（ブラウザ経由）、応答先：共通アプリ
- 通信形式：実行時パラメータ

（2）共通アプリ連携インタフェース（**図 2-1** の I2 および F2）

- 耐タンパデバイスに対してセキュアにアクセスするために共通アプリとモバイルアクセスサーバが通信する。
- 要求元：共通アプリ、要求先：モバイルアクセスサーバ
- 通信形式：HTTPS（XML）

（3）APDU 移譲インタフェース（**図 2-1** の I3）

- 耐タンパデバイスに対して実行する APDU コマンドをサービス提供機関からモバイルアクセスサーバに移譲する。
- 要求元：サービス提供機関、要求先：モバイルアクセスサーバ

- 通信形式：HTTPS（XML）

（４）APDU 実行結果通知インタフェース（**図 2-1** の I3）

- 耐タンパデバイスに対して実行した APDU コマンドの結果をモバイルアクセスサーバからサービス提供機関に通知する。
- 要求元：モバイルアクセスサーバ、要求先：サービス提供機関
- 通信形式：HTTPS（XML）

（５）再アクセスインタフェース（**図 2-1** の I1、I2 および F1）

- モバイルアクセスサーバから共通アプリに処理終了を通知し、共通アプリからサービス提供機関へ再アクセスする。
- 要求元：モバイルアクセスサーバ（共通アプリ経由、ブラウザ経由）、要求先：サービス提供機関
- 通信形式：HTTPS

2.3 プロトコル

以下に各エンティティ間のデータの流れ（プロトコル）に関して記述する。**図 2-2** は、サービス提供機関による耐タンパデバイスとの ID 情報の書き込み、及び読み込みの際のデータの流れを示す簡易的な図である。

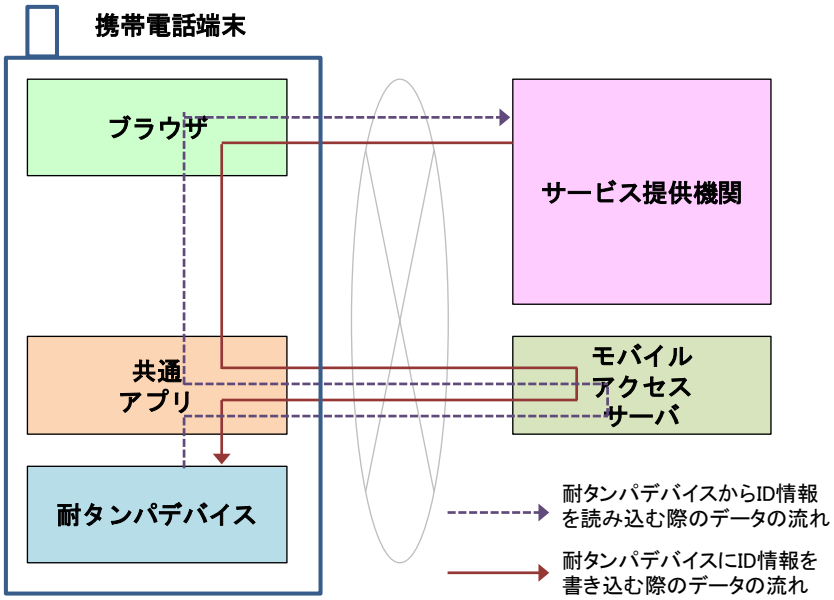

図 2-2 データの流れを示す簡略図

図 2-2 に示す実線の矢印が、サービス提供機関から耐タンパデバイスへ送信する ID 情報の流れである。サービス提供機関はブラウザ経由で共通アプリを起動し、その後、共通アプリからモバイルアクセスサーバに接続され、モバイルアクセスサーバは、共通アプリ経由で耐タンパデバイスに ID 情報を送信する。その際に、モバイルアクセスサーバと耐タンパデバイスはセキュアな通信路を確立する。点線の矢印は、耐タンパデバイスからモバイルアクセスサーバへ送信する ID 情報の流れである。サービス提供機関は、ブラウザ経由で共通アプリを起動し、その後、モバイルアクセスサーバ経由で共通アプリから耐タンパデバイスにアクセスし、ID 情報をモバイルアクセスサーバに送信する。モバイルアクセスサーバは、共通アプリ、ブラウザ経由でサービス提供機関に ID 情報を送信する。

図 2-3 にデータの流れを表わす。さらに詳細なフローを示す。

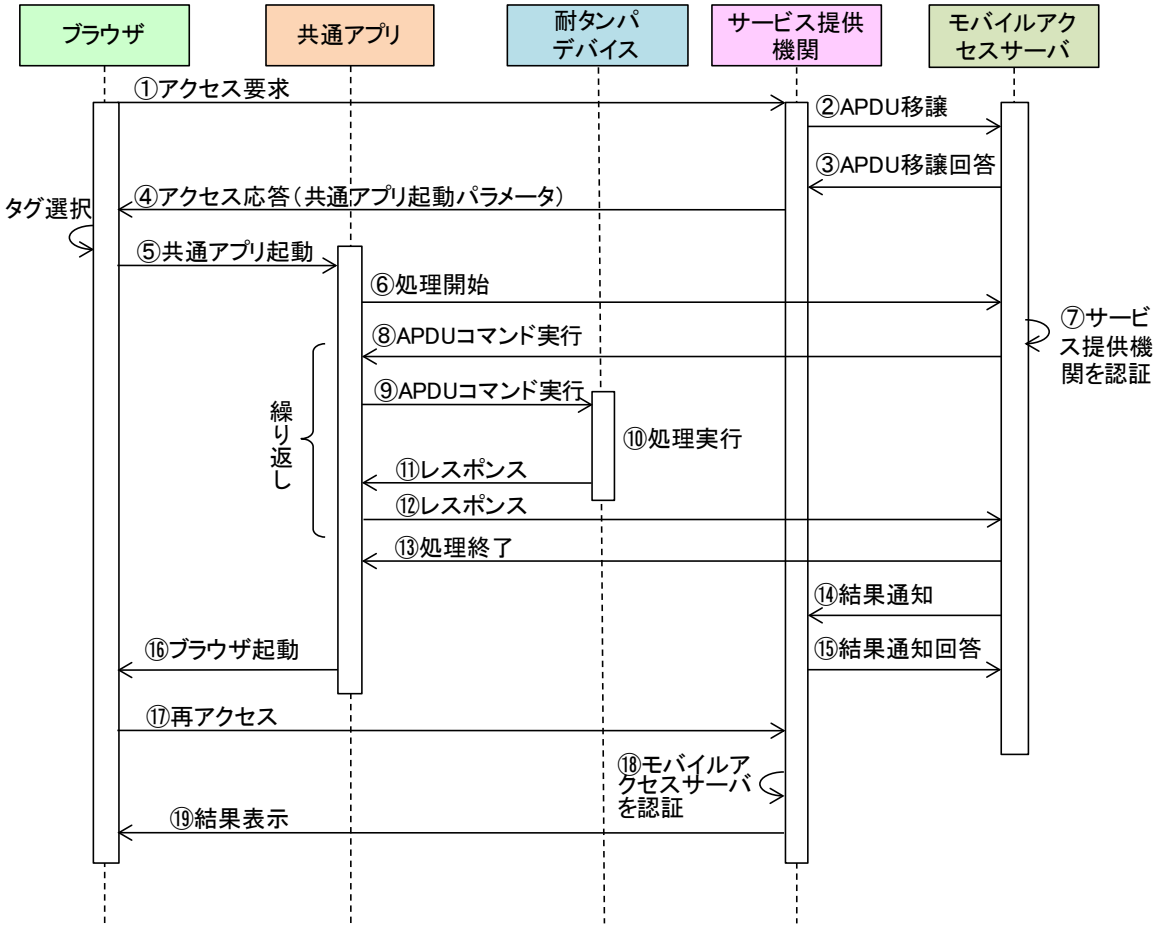

図 2-3 データの流れを示す詳細図

まず、利用者が携帯電話端末のブラウザ経由でサービス提供機関にアクセスする①。サービス提供機関からモバイルアクセスサーバに対して、耐タンパデバイスに送るべき APDU コマンドを送信し②、回答を受信する③。

次にサービス提供機関から、アクセス応答として、ブラウザに対して共通アプリ起動パラメータを送信する④。ブラウザは、共通アプリを起動し、サービス提供機関から受信したデータを共通アプリに渡す⑤。

耐タンパデバイスにアクセスするための秘密情報を保持しない共通アプリは、そのままでは耐タンパデバイスにアクセスできないため、モバイルアクセスサーバに処理開始要求をを送信する⑥。④、⑤、⑥でサービス提供機関からモバイルアクセスサーバに送信されるデータは暗号化されている。モバイルアクセスサーバは、共通アプリから転送された処理開始要求データが正しいサービス提供機関から送信された要求データだということを確認する⑦。モバイルアクセスサーバは、耐タンパデバイス内のサービス提供機関の管理下の領域の IC カードアプリケーションに送信するための APDU コマンドを共通アプリに返信する⑧。共通アプリは受信した APDU コマンドを耐タンパデバイスに転送する⑨。耐タンパデバイスは、APDU コマンドに従って耐タンパデバイス内で処理を実行し⑩、結果をレスポンスデータとして共通アプリ経由でモバイルアクセスサーバに返す⑪⑫。APDU コマンドは複数回実行されることが想定されるため⑧～⑫が繰り返される。なお、この APDU コマンド送受信の初期の段階で、モバイルアクセスサーバと耐タンパデバイス内のサービス提供機関の管理下の領域の IC カードアプリケーションとの間で、セキュアセッションの確立（暗号通信を行うための鍵共有）が行われ、以降の APDU コマンドは安全な通信路内で送受信される。よって APDU コマンドは共通アプリを経由するが共通アプリはその内容を見ることはできない。

サービス提供機関は耐タンパデバイスでの処理結果をモバイルアクセスサーバから受信し⑬、受信結果をモバイルアクセスサーバに返信する⑭。

モバイルアクセスサーバは、共通アプリに対して処理終了通知を送信し⑮、共通アプリはブラウザを起動する⑯。起動されたブラウザでサービス提供機関に再度アクセスする⑰。⑬、⑯、⑰でモバイルアアクセスサーバからサービス提供機関に送信されるデータは暗号化されている。サービス提供機関は共通アプリからブラウザ経由で転送されたデータが正しいモバイルアクセスサーバからのデータであるか否かを確認する⑱。最後にサービス提供機関からブラウザに対して結果を表示させる⑲。

なお、**図 2-3** では、②、③と⑬、⑭のステップにおいて、直接サービス提供機関とモバイルアクセスサーバの間で、APDU コマンドの送信と処理結果の受信を行っているが、②の APDU コマンドの移譲の代わりに、④～⑥のそれぞれの送信データに移譲すべき APDU コマンドを含めることもできる。その場合には、⑬、⑭の処理結果受信の代わりに、⑮～⑰のそれぞれの送信データに処理結果を含める。

また、⑬、⑭の処理結果通知処理は、⑧～⑫の繰り返しが終わった後に一括して行っているが、⑫のレスポンスを受け取る都度、サービス提供機関に処理結果を通知しても良い。

2.4 セキュリティ対策

本節では、1.7 節で示したセキュリティ要件に対する対策を示す。

(1) 不正な携帯電話端末アプリケーションへの対応

(1-1)

【要件】悪意のある携帯電話端末アプリケーションが耐タンパデバイス内のセキュアデータへのアクセスの防止

【対策】耐タンパデバイスへアクセスするためには、耐タンパデバイスと相互認証を行ったうえで安全な通信路を確保（セキュアセッションの確立）するようにし、共有鍵を持たない携帯電話端末アプリケーションは、耐タンパデバイスにアクセスできないようにした。また、共通アプリも共有鍵を持たず、モバイルアアクセスサーバ側に共有鍵を持たせることで、共通アプリがマルウェアやウィルスに感染しても共有鍵が漏洩することがないような設計にした。

(2) 通信路の安全性の確保

(2-1)

【要件】サービス提供機関―(共通アプリ)―モバイルアクセスサーバ間の通信路の安全性の確保

【対策】**図 2-3** のデータの流れを示す詳細図の④、⑤、⑥のサービス提供機関からモバイルアクセスサーバへ送信されるデータおよび、⑬、⑯、⑰でモバイルアアクセスサーバからサービス提供機関に送信されるデータは暗号化される。よって安全性が確保されるとは限らない共有アプリを経由してもデータは漏えいしない。

(2-2)

【要件】モバイルアクセスサーバー(共通アプリ)－耐タンパデバイス間の通信路の安全性の確保

【対策】モバイルアクセスサーバと耐タンパデバイス間は、GlobalPlatform 仕様に基づく相互認証および暗号通信を行うため安全性は確保される。

(2-3)

【要件】サービス提供機関－モバイルアクセスサーバ間の通信路の安全性の確保

【対策】1.6 節のネットワークに関する前提条件で示したように、サービス提供機関－モバイルアクセスサーバ間の通信路の安全性は確保されているという前提を置いている。

(3) 成りすまし防止

(3-1)

【要件】サービス提供機関の成りすましの防止

【対策】**図 2-3** のデータの流れを示す詳細図の⑦で示したように、共通アプリを経由してモバイルアクセスサーバが受信したデータには、サービス提供機関の署名が付与されており、モバイルアクセスサーバはその署名を検証することで、正しいサービス提供機関から送信されたデータだということを確認できる。

(3-2)

【要件】モバイルアクセスサーバの成りすましの防止

【対策】**図 2-3** のデータの流れを示す詳細図の⑱で示したように、共通アプリを経由してサービス提供機関が受信したデータには、モバイルアクセスサーバの署名が付与されており、サービス提供機関はその署名を検証することで、正しいモバイルアクセスサーバから送信されたデータだということを確認できる。

【付録】インタフェースの詳細（実装例）

実装例として、ブラウザ、共通アプリ、耐タンパデバイス、サービス提供機関、モバイルアクセスサーバの各エンティティ間のインタフェースに関して詳細を記述する。

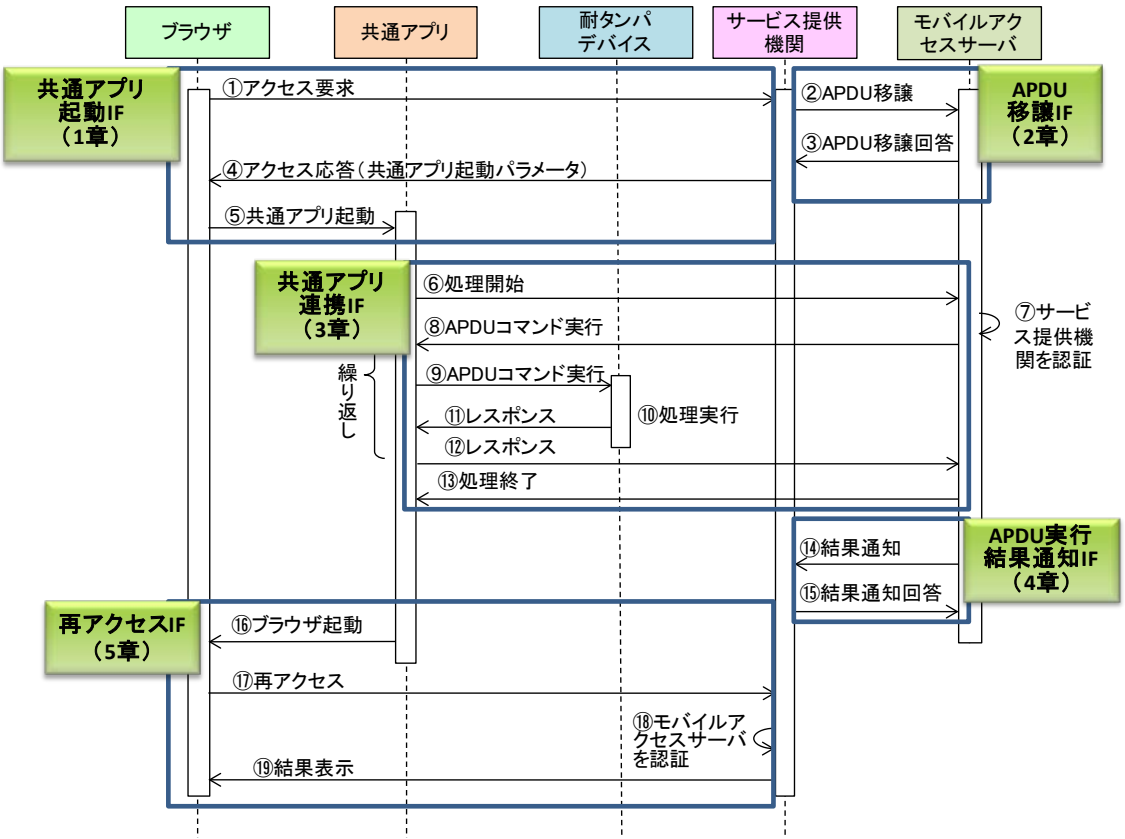

図 1-1 エンティティ間のインタフェース

本システムで使用する通信 IF を下の表に示す。

表 1-1 インタフェース一覧

#	IF 名	内容	要求元	応答先	通信形式
1	共通アプリ起動	JavaScript で共通アプリを起動する。	ブラウザ	共通アプリ	実行時パラメータ
2	APDU 移譲	耐タンパデバイスに対して実行する APDU コマンドをサービス提供機関からモバイルアクセスサーバに移譲する。	サービス提供機関	モバイルアクセスサーバ	HTTPS／※XML
3	共通アプリ連携	耐タンパデバイスに対してセキュアにアクセスするために共通アプリとモバイルアクセスサーバが通信する IF。	共通アプリ	モバイルアクセスサーバ	HTTPS／※XML
4	APDU 実行結果通知	耐タンパデバイスに対して実行した APDU コマンドの結果をモバイルアクセスサーバからサービス提供機関に通知する。	モバイルアクセスサーバ	サービス提供機関	HTTPS／※XML
5	再アクセス	共通アプリからサービス提供機関の処理結果画面へ接続する IF	共通アプリ	サービス提供機関	HTTPS

1. 共通アプリ起動インタフェース

共通アプリを起動する際の起動パラメータ（Android OS の場合）を以下に示す。

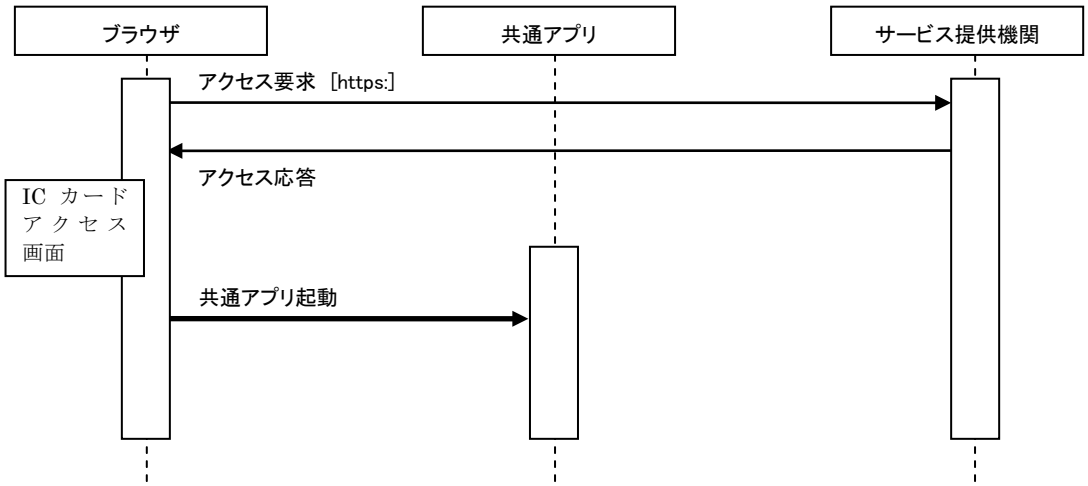

図 1-2 共通アプリ起動シーケンス図

表 1-2 共通アプリ起動時の要求例

```
function startCommonApl(param){
var hrefString="commonApl: " + param;
location.href=hrefString;
}
```

表 1-3 共通アプリ起動時のパラメータ

#	項目名	パラメータ名	属性	桁数	説明
1	起動パラメータ	param	varchar	-	共通アプリの起動パラメータ

表 1-4 起動パラメータの構成

```
spId=XXXXXXXX&rcptNum=XXXXXXXXXXXXXXXX&rtnUrl=XXXXXXXXXXXXXXX&masUrl=XXX
XXXXXXXXXXXXX&spSign=XXXXXXXXXXXXXXXX
```

※spId=、&rcptNum=、&rtnUrl=、masUrl、spSign が必ず存在すること。

表 1-5 起動パラメータの構成要素の詳細

#	項目名	パラメータ名	属性	桁数	説明
1	サービス事業者 ID	spId	char	8	サービス事業者 ID
2	受付番号	rcptNum	char	16	サービス提供機関が採番した受付番号(日付+8 桁の番号)
3	戻り URL	rtnUrl	varchar	-	戻り URL
4	モバイルアクセスサーバ URL	masUrl	varchar	-	モバイルアクセスサーバの URL
5	SP 署名	spSign	varchar	256	Base64 エンコードした SP 署名

2. APDU 移譲インタフェース

耐タンパデバイスに対して実行する APDU コマンドをサービス提供機関からモバイルアクセスサーバに移譲する通信インタフェースを以下に示す。

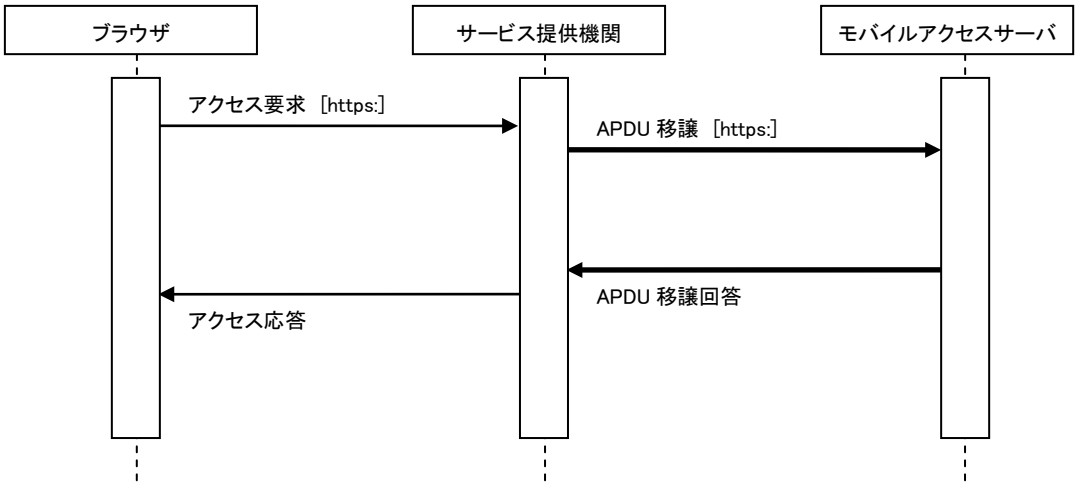

図 1-3 APDU 移譲シーケンス図

表 1-6 APDU 移譲時の要求例

```
POST /xxxxx/xxxx/xxxxx HTTPS/1.1
Host: xxxxx.com
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<request>
  <strSpId>XXXX</strSpId>
  <strRcptNum>XXXX</strRcptNum>
  <strApduGeneDate>XXXX</ strApduGeneDate >
  <apduCmnds>
    <apduCmnd>
      <iApduOrder>XXXX</iApduOrder>
      <byApduCmndAry>XXXX</byApduCmndAry>
    </apduCmnd>
    ・・・<apduCmnd>は実行する APDU の数分定義する
  </apduCmnds>
</request>
```

表 1-7 APDU 移譲時の要求 IF

#	項目名	パラメータ名	属性	桁数	説明
1	サービス事業者 ID	strSpId	char	8	サービス事業者 ID
2	受付番号	strRcptNum	char	16	サービス提供機関が採番した受付番号 (日付+8 桁の番号)
3	APDU 生成年月日	strApduGeneDate	char	14	APDU を生成した年月日 (YYYYMMDDhhmmss)
4	APDU 実行順序	iApduOrder	varchar	3	APDU コマンドの実行順序
5	APDU コマンド	byApduCmndAry	varchar	※説明参照	Base64 エンコードした APDU コマンド ※桁数は生成した APDU の約 3 分の 4 倍

※実行する APDU の数だけ APDU 実行順序と APDU コマンドのペアが存在する

表 1-8 APDU 移譲時の応答例

```
HTTPS/1.1  200  OK
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<response>
  <strProcStatus>XXXX</strProcStatus>
  <strErrInfo>XXXX</strErrInfo>
  <strApduRcptDate>XXXX</strApduRcptDate>
</response>
```

表 1-9 APDU 移譲時の応答 IF

#	項目名	パラメータ名	属性	桁数	説明
1	処理ステータス	strProcStatus	char	2	処理ステータス
2	エラー情報	strErrInfo	varchar	20	エラー情報
3	APDU 受付年月日	strApduRcptDate	char	14	APDU を受け付けた年月日 (YYYYMMDDhhmmss)

3. 共通アプリ連携インタフェース

耐タンパデバイスに対してセキュアにアクセスするために共通アプリとモバイルアクセスサーバ間でデータを送受信する通信インタフェースを以下に示す。

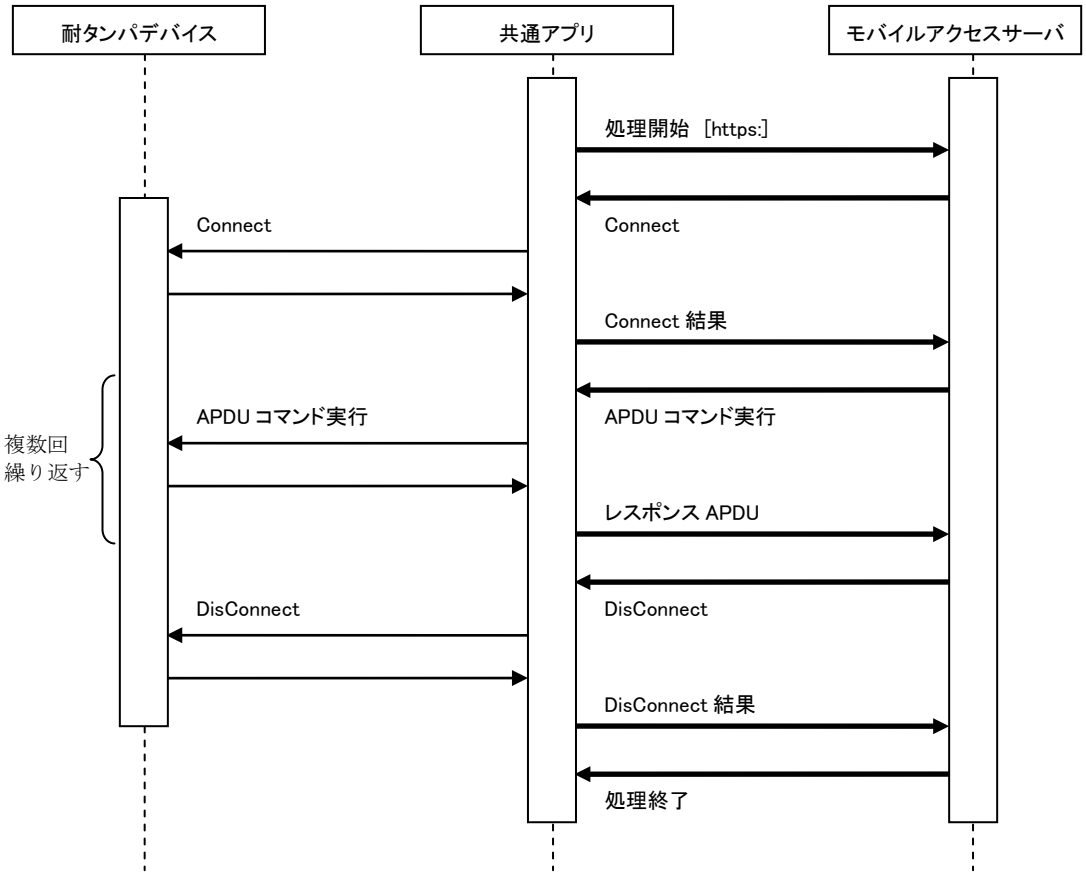

図 1-4 共通アプリ連携シーケンス

表 1-10 共通アプリ連携時の要求例

```
POST /xxxxx/xxxx/xxxxx HTTPS/1.1
Host: xxxxx.com
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<request>
  <strProcId>XXXX</strProcId>
  <strProcStatus>XXXX</strProcStatus>
  <strSpId>XXXX</strSpId>
  <strRcptNum>XXXX</strRcptNum>
  <byRespSWAry>XXXX</byRespSWAry>
  <byRespApduDataAry>XXXX</byRespApduDataAry>
  <strConnectCard>XXXX</strConnectCard>
  <strErrInfo>XXXX</strErrInfo>
  <strSpSign>XXXX</strSpSign >
</request>
```

表 1-11 共通アプリ連携時の要求 IF

#	項目名	パラメータ名	属性	桁数	説明
1	処理 ID	strProcId	char	3	処理 ID
2	処理ステータス	strProcStatus	char	2	処理ステータス
3	サービス事業者 ID	strSpId	char	8	サービス事業者 ID ※未設定の場合あり
4	受付番号	strRcptNum	char	16	サービス提供機関が採番した受付番号 (日付+8 桁の番号) ※未設定の場合あり
5	SW1、SW2	byRespSWAry	char	3	Base64 エンコードした APDU コマンド実行結果 ※未設定の場合あり
6	レスポンス APDU	byRespApduDataAry	varchar	※説明参照	Base64 エンコードしたレスポンス APDU ※未設定の場合あり ※桁数はレスポンス APDU の約 3 分の 4 倍
7	カード情報	strConnectCard	char	2	Connect したカードの情報 ※未設定の場合あり
8	エラー情報	strErrInfo	varchar	20	エラー情報
9	SP 署名	strSpSign	varchar	256	Base64 エンコードした SP 署名 ※処理 ID：001 の場合のみ設定する

表 1-12 共通アプリ連携時の要求 IF における処理 ID

#	コード	説明
1	001	処理開始
2	002	Connect 結果
3	003	レスポンス APDU
4	004	DisConnect 結果

表 1-13 共通アプリ連携時の要求 IF におけるカード情報

#	コード	説明
1	01	UICC カード

表 1-14 共通アプリ連携時の応答例

```
HTTPS/1.1  200  OK
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<response>
  <strProcIdRtn>XXXX</strProcIdRtn>
  <byApduAry>XXXX</byApduAry>
  <byApduAry>XXXX</byApduAry>
</response>
```

表 1-15 共通アプリ連携時の応答 IF

#	項目名	パラメータ名	属性	桁数	説明
1	処理 ID(戻り)	strProcIdRtn	varchar	3	処理 ID(戻り)
2	APDU コマンド	byApduAry	varchar	※説明参照	Base64 エンコードした APDU コマンド ※桁数は APDU コマンドの 3 分の 4 倍 ※未設定の場合あり
3	MAS 署名	strMasSign	varchar	256	Base64 エンコードした MAS 署名 ※処理 ID(戻り)：104 の場合のみ設定する

表 1-16 共通アプリ連携時の応答 IF における処理 ID(戻り)

#	コード	説明
1	101	Connect
2	102	APDU コマンド実行
3	103	DisConnect
4	104	処理終了

4. APDU 実行結果通知インタフェース

耐タンパデバイスに対して実行した APDU コマンドの結果をモバイルアクセスサーバからサービス提供機関に通知する通信インタフェースを以下に示す。

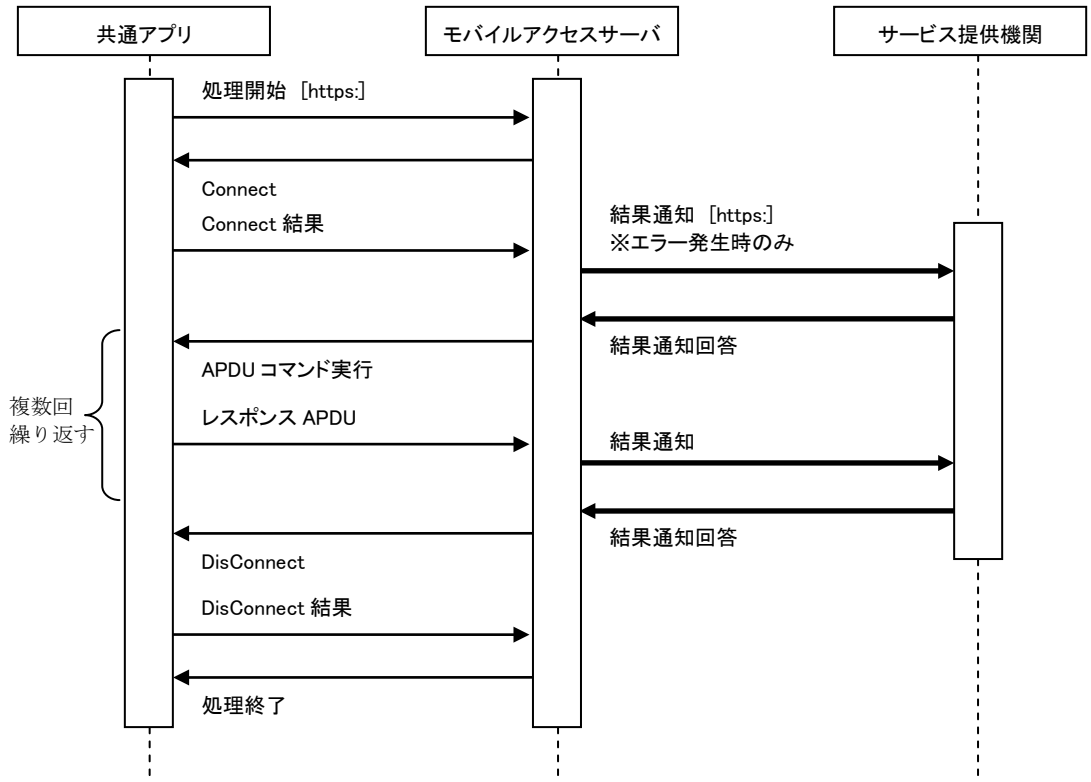

図 1-5 APDU 実行結果通知シーケンス図

表 1-17 APDU 実行結果通知時の要求例

```
POST /xxxxx/xxxx/xxxxx HTTPS/1.1
Host: xxxxx.com
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<request>
  <strRcptNum>XXXX</strRcptNum>
  <iApduOrder>XXXX</iApduOrder>
  <iRespApduNum>XXXX</iRespApduNum>
  <byRespSWAry>XXXX</byRespSWAry>
  <byRespApduDataAry>XXXX</byRespApduDataAry>
  <strProcStatus>XXXX</strProcStatus>
  <strErrInfo>XXXX</strErrInfo>
</request>
```

表 1-18 APDU 実行結果通知時の要求 IF

#	項目名	パラメータ名	属性	桁数	説明
1	受付番号	strRcptNum	char	16	サービス提供機関が採番した受付番号(日付+8 桁の番号)
2	APDU 実行順序	iApduOrder	varchar	3	APDU コマンドの実行順序
3	APDU レスポンス番号	iRespApduNum	varchar	3	APDU レスポンス番号
4	SW1、SW2	byRespSWAry	char	3	Base64 エンコードした APDU コマンド実行結果 ※未設定の場合あり
5	レスポンス APDU	byRespApduDataAry	varchar	※説明参照	Base64 エンコードしたレスポンス APDU ※未設定の場合あり ※桁数はレスポンス APDU の約 3 分の 4 倍
6	処理ステータス	strProcStatus	char	2	処理ステータス
7	エラー情報	strErrInfo	varchar	20	エラー情報 ※未設定の場合あり

表 1-19 APDU 実行結果通知時の応答例

```
HTTPS/1.1 200 OK
Content-Type: application/xml
Content-Length: バイト数

<?xml version="1.0" encoding="UTF-8" ?>
<response>
  <strResult>XXXX</strResult>
</response>
```

表 1-20 APDU 実行結果通知時の応答 IF

#	項目名	パラメータ名	属性	桁数	説明
1	処理結果	strResult	varchar	5	処理結果 true：正常、false：異常

5. 再アクセスインタフェース

共通アプリからサービス提供機関の処理結果画面へ接続するインタフェースを以下に示す。

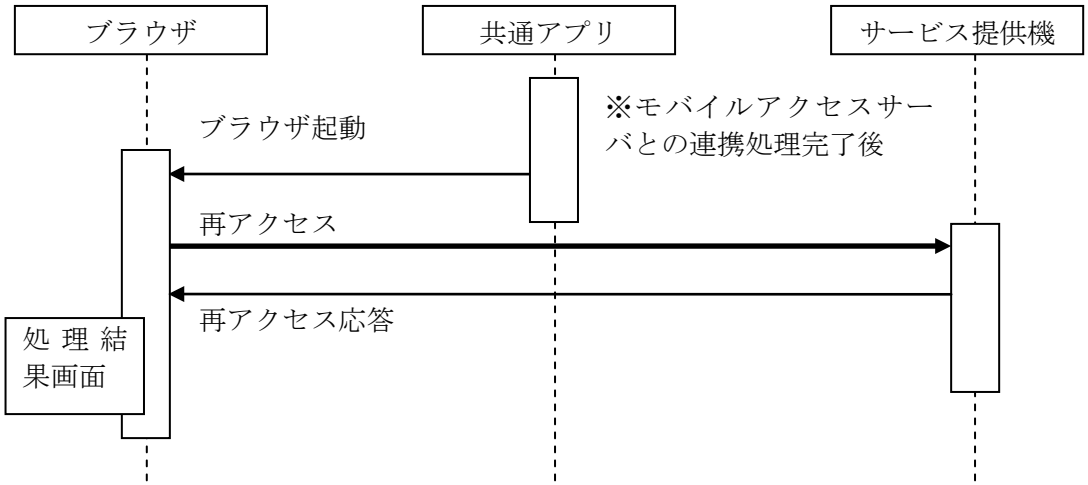

図 1-6 再アクセスシーケンス図

表 1-21 再アクセス時の要求例

https://(戻りURL)?rcptNum=XXXXXXXXXXXXXXXX&masSign=XXXXXXXXXXXXXXXX

※rcptNum=、masSign=が必ず存在すること。

表 1-22 再アクセス時における要求の構成要素

#	項目名	パラメータ名	属性	桁数	説明
1	戻り URL	-	varchar	-	サービス提供機関の処理結果画面の URL
2	受付番号	rcptNum	char	16	サービス提供機関が採番した受付番号 (日付+8 桁の番号)
3	MAS 署名	masSign	varchar	256	Base64 エンコードした MAS 署名

サービス提供機関から携帯電話端末の安全な
耐タンパデバイス利用に関するガイドライン

MC-05　1.0 版

平成 25 年 5 月　1.0 版第 1 刷発行

発　行　所

一般社団法人　電　波　産　業　会
高度無線通信研究委員会モバイルコマース部会
〒100-0013　東京都千代田区霞が関１－４－１
日土地ビル１１階
電　話　03-5510-8594
ＦＡＸ　03-3592-1103

禁無断転載