DSRC システムにおけるクレジット決済適用のためのガイドライン

ITS FORUM RC-002

平成 15 年 2 月 10 日　　策　定　　第 1.0 版

ITS情報通信システム推進会議

路側通信システム専門委員会

改版履歴

版数	年月日	改版箇所	改版理由	改版内容
1.0	平成 15 年 2 月 10 日	策定	新規策定	―

目　次

1　本書の目的

本書は、DSRC（狭域通信：Dedicated Short Range Communications）システム環境用に端末アプリケーションとしての IC クレジットアプリケーションを搭載する際の路側機器・車載機・店舗サーバ等関連機器に対する概要要件である。本書は、各国際クレジットブランド発行カード会社が発行する EMV 仕様 IC クレジットカード（以下 IC クレジットカード）の DSRC 環境下における相互運用性を確保するとともに、IC カード、関連機器製造メーカ、システム構築ベンダー等における当該開発部分のコスト低廉化、さらには DSRC システム利用機会の拡大・普及を期待して制定するものである。

2　本書の範囲

本書では IC クレジットカード、決済端末、決済ネットワークについては、IC クレジットにおける従来インフラの活用を前提とし、主に DSRC 環境での IC クレジット利用を実現可能とする端末の構成と機能の拡張について言及する。記述にあたっては、各種諸規格との整合性と、将来の拡張性についても配慮する。また、本書は 10 章　参照規格に列挙した諸規格と併せて読まれることを前提とし、重複する部分は参照箇所を都度指摘することとする。

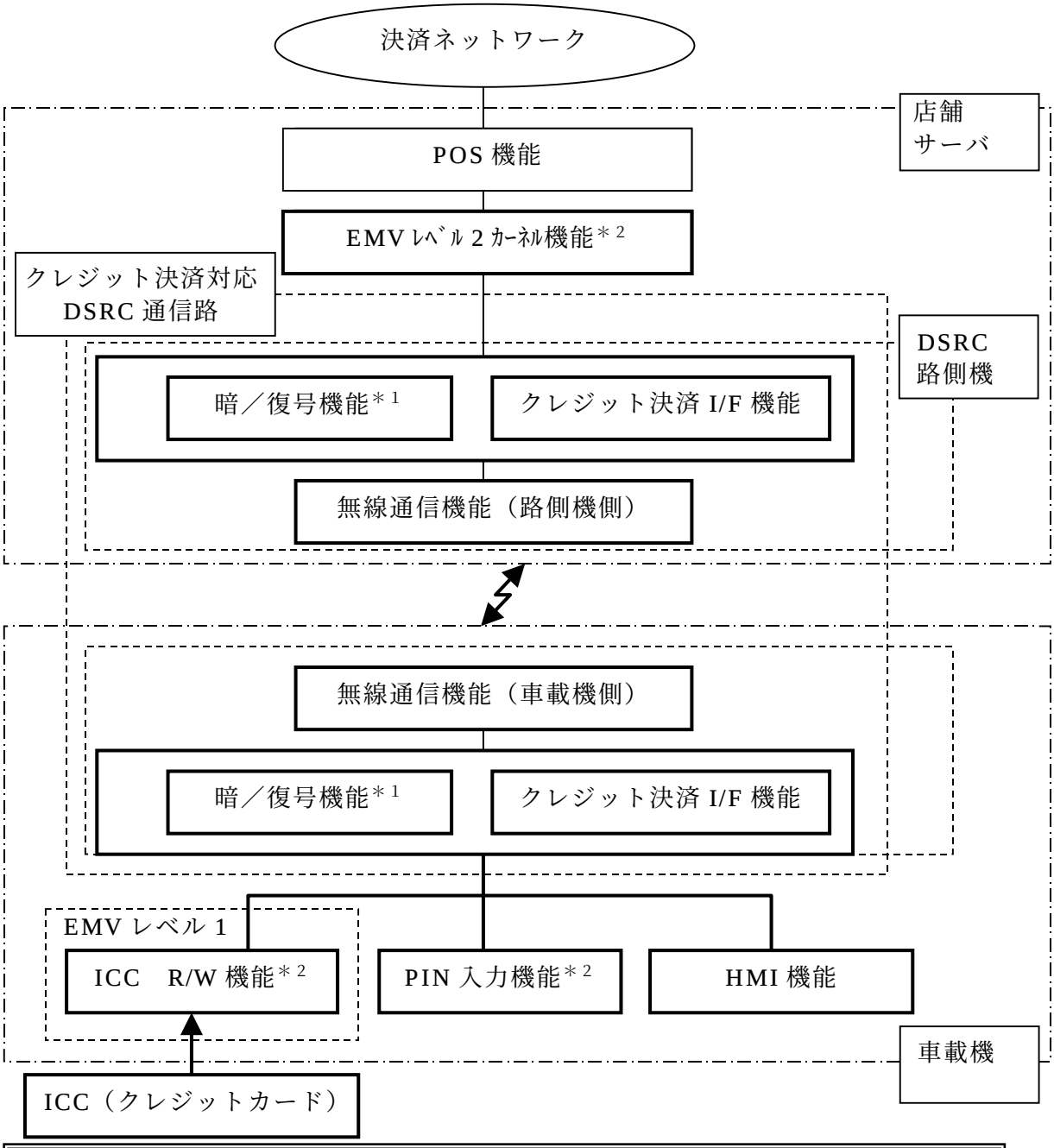
<注>　本書は端末への実装の自由度を制約するものではなく、実装に際しては、端末開発、製造主体者（情報処理センタ、メーカ等）に委ねられる。実現時には、国際クレジットブランド、カード発行会社、加盟店契約会社、ネットワーク会社など関連する諸団体との協議を経て、実装主体が目的とする業務やアプリケーションに適した形での実装が可能である。IC クレジットアプリケーションを使用するためには各ブランド等の端末認定の実施などについて今後検討が必要である。

また、利用者保護の観点から、本書で記述する既存インフラの拡張部分におけるセキュリティや信頼性が確保されることを前提とし、DSRC 環境の運営主体によって定期的に見直しを図る必要がある。

3　クレジット決済対応 DSRC 通信路の機能構成

3.1　機能構成図

DSRC 通信路を用いたクレジット決済処理に必要な機能構成を以下に示す。



注

＊1　秘密情報（秘密鍵）あるいは個人情報が暗号化されない状態にある個所（筐体）については、機密性を確保するために耐タンパー性を有すること。

＊2　店舗サーバでの EMV レベル 2 カーネル、あるいは、車載側での ICC R/W、PIN 入力機能が、暗／復号機能と同一の個所（筐体）に入らない場合は、別途この個所（筐体）との間のデータは、ISO9564-1（あるいはそれ相当）に従い暗号化されること。

図 3.1-1　機能構成図

3.2　各機能の概要

機能構成図で示した各機能の概要について以下に示す。

3.2.1　EMV レベル 2 カーネル、EMV レベル 1

EMV 仕様の機器として EMVCo.により指定された認証機関で取得する認定レベル。

EMV レベル 1：IC カードの電気機械的特性、論理インターフェース、転送プロトコルに対する端末仕様の、EMV における規定部分。

EMV レベル 2 カーネル：EMV で規定したアプリケーション機能を実行する、ライブラリを含めたソフトウェアモジュール。

3.2.2　無線通信機能（路側機側）、無線通信機能（車載機側）

DSRC（狭域通信：Dedicated Short Range Communications）方式を用いた無線通信を実現する。本無線通信機能は路側機側と車両に搭載される車載機側とにより構成され、無線通信仕様は ARIB 標準規格 STD-T75（DSRC システム）に準拠する。

3.2.3　PIN 入力機能

本人認証のための PIN（Personal Identification Number）の入力を実現する。入力された PIN は暗号化され（暗／復号機能）、DSRC（無線通信機能）を経由し、EMV レベル 2 カーネルへ伝達される。

3.2.4　暗／復号機能

クレジット決済対応 DSRC 通信路における PIN などの情報の暗号化および復号化を実現する。

3.2.5　クレジット決済 I/F 機能

クレジット決済で実行されるプロトコルを DSRC 上で透過的にデータ転送するための変換を実現する。また、DSRC を用いたクレジット決済に必要なコマンドなども本機能に含まれる。

3.2.6　ICC　R/W 機能

ICC（クレジットカード）に対しデータアクセスを実現する。本機能は EMV レベル 1 を取得した機器により実現される。

3.2.7　HMI 機能

クレジット決済時の利用者と店舗側との通信のための入出力を実現する。利用者への出力としては PIN 入力指示、処理結果などを行う。入力としては、サービスの選択、処理の確認などを行う。

3.3　クレジット決済対応 DSRC 通信路の階層

OSI モデルを基本とした、クレジット決済対応の DSRC 通信路の階層を以下に示す。

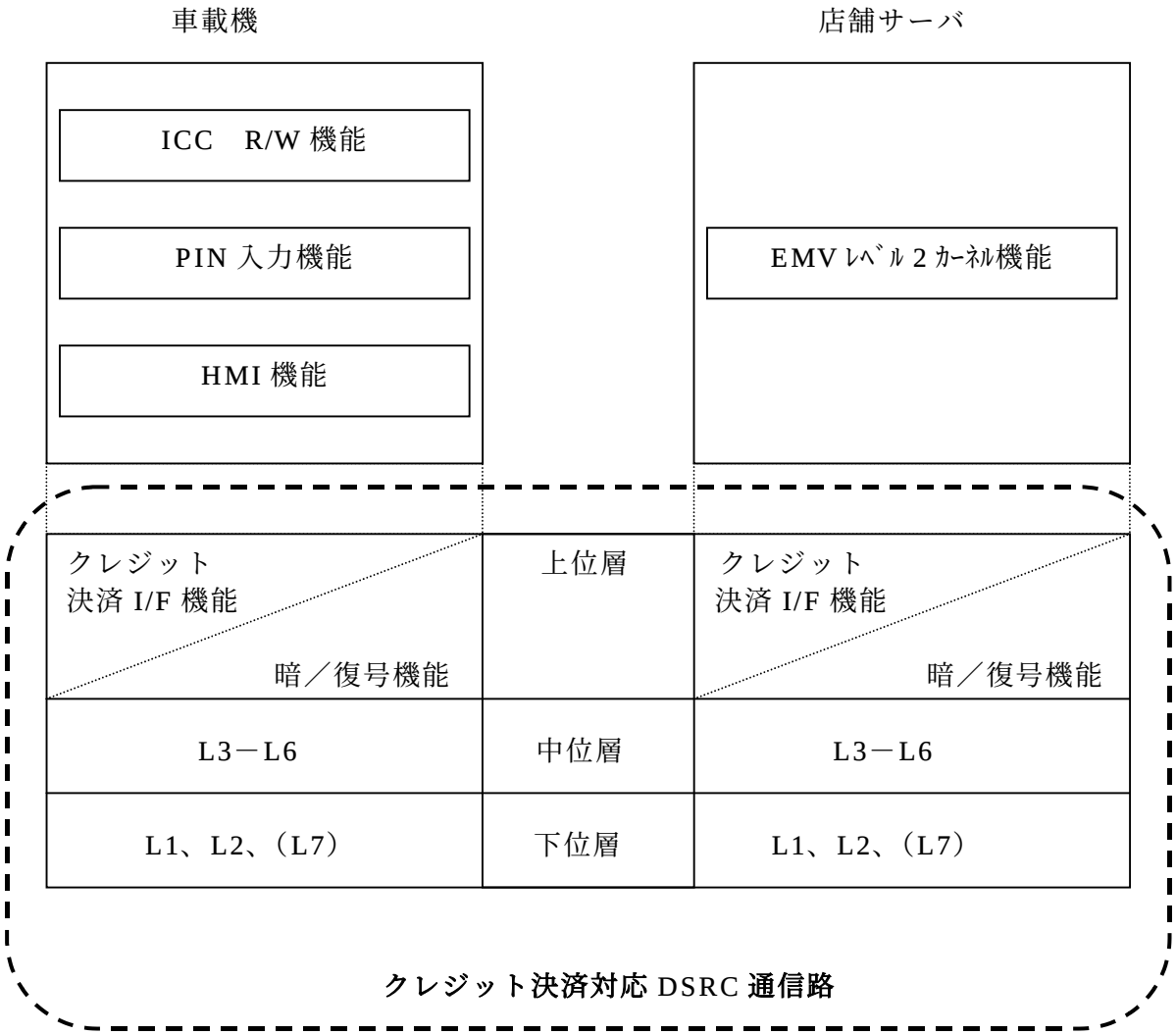
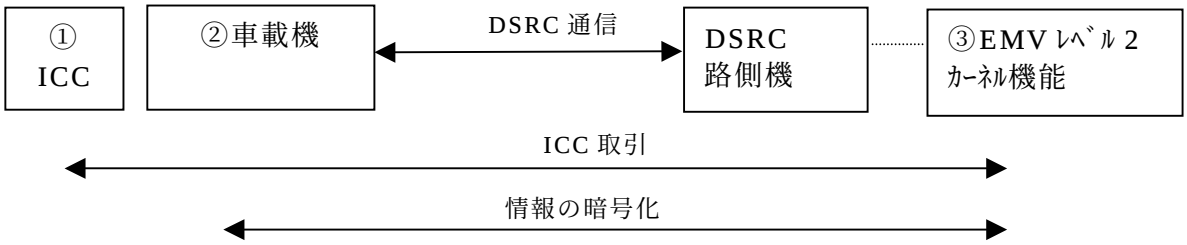


図 3.3-1　DSRC 通信路の階層

3.4　暗号化の範囲

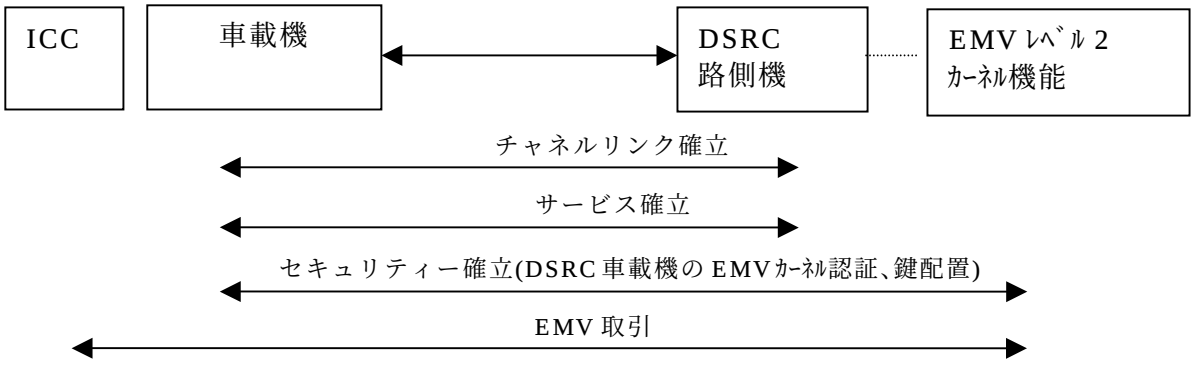
DSRC 通信路を用いたクレジット決済処理の暗号化の範囲を以下に示す。

3.4.1　システム構成例

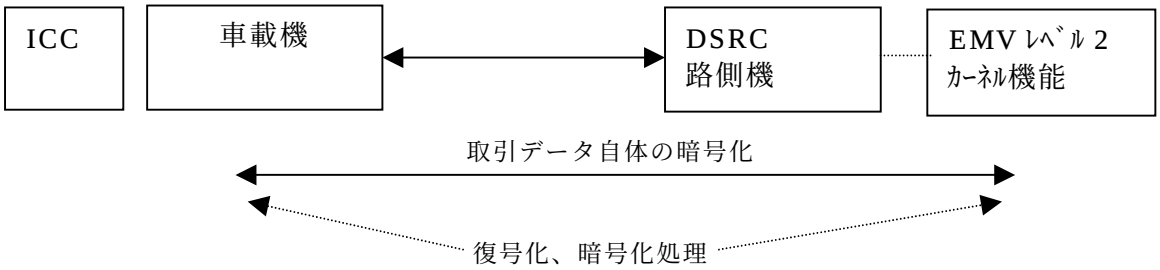


①EMV 仕様クレジットカード(V.3.1.1 以上)
②EMV レベル 1 認定済で PIN 入力装置付き
③EMV レベル 2 認定

3.4.2　通信フローの概要



3.4.3　EMV 取引での情報秘匿



データの暗号化方式
①公開鍵方式　　車載機生成の鍵を公開鍵で暗号化。EMV レベル 2 カーネルへ配信後、
　　秘密鍵で復号化。取引データは配信された鍵で暗号化。
②共通鍵方式　　車載機が予め持つ鍵(SAM 等で供給)でデータ暗号化

4　クレジット業務要件

4.1　前提事項

本書は EMV 仕様準拠の汎用クレジット決済アプリケーションによる課金スキームを、決済時に一旦停車した状態において DSRC を介して課金を実現しようとする場合に対応が必要と考えられる概要要件を整理したモデルケースである。

従って、移動（走行）中における利用環境は本書においては想定外であるほか、DSRC を活用した汎用クレジット決済スキームの検討を行う場合には、本書に加え、ISO（International Organization for Standardization：国際標準化機構）7816、EMV 仕様、各国際クレジットブランドにおける IC クレジットアプリケーション仕様書（10 章参照）などの各仕様書を参照し検討する必要がある。

また、決済ネットワークに関しては IC クレジットにおける従来インフラを活用することを前提とし、DSRC 無線を介した決済環境については、利用者の当該 IC カードによる決済意思の確認や、カード～端末間の指向（特定）性、無線通信の信頼性など DSRC クレジット利用環境のセキュリティや信頼性が、その運営主体によって EMV 仕様における加盟店端末設置環境と同等に確保されることを取り組みの前提とする。

なお、EMV 仕様を鑑みた対応要件は本書に記述した通りであるが、実現されるアプリケーションや決済対象商品の性質･環境などによって必ずしも本書記述内容通りにしか実現されないと限定されるものではなく、具体的実現策は国際クレジットブランド・カード発行会社・加盟店契約会社・ネットワーク会社など、実現される DSRC 決済スキームに関与する主体との協議が必要である。

<注>　IP 系サービスサーバ接続について

DSRC を活用したサービスには、IP 系サービスサーバ接続により実現されるアプリケーションも想定される。IP 系サービスサーバを活用した決済スキームには、既にインターネットにおけるネットショッピングに代表されるバーチャル取引環境下の決済スキームが複数存在するが、これらは購入商品を郵送することで受益者を特定したり、多くのリスク負担を加盟店側が負うなど、商取引環境・条件が DSRC 決済環境とは全く異なることから、そのまま DSRC 環境における決済スキームとして活用することはできず、DSRC 環境における決済スキームは、あくまで本書の DSRC クレジット仕様に基づく決済スキームにて実現される

IP 系サービスサーバ接続により決済以外のアプリケーションが実現される場合には、路側機を介し IP 系サービスサーバと EMV レベル２カーネルが接続されることがないことが保証されなければならない。また、IP 系サービスサーバ側からクレジットアプリケーションが選択された場合は拒否できなければならない。

ただし、将来的に EMV 処理がインターネット上で実現された場合には IP 系サービスサーバ接続によるクレジット決済スキームの活用も検討されうるが､ユーザ側でバーチャル上の正規の加盟店と取引していることを認識できることを前提に処理開始できるよう対応する必要がある。

4.2　対象カード

EMV3.1.1 以上に準拠した国際ブランド IC クレジットカード

4.3　対象業務

本仕様書が対象とする業務処理は 1 回払いの売上処理とする。その他の業務処理に関しては、DSRC を使用せず「IC カード対応端末機能仕様書／日本クレジットカード協会」に準じ通常端末で行うものとする。

4.4　売上処理

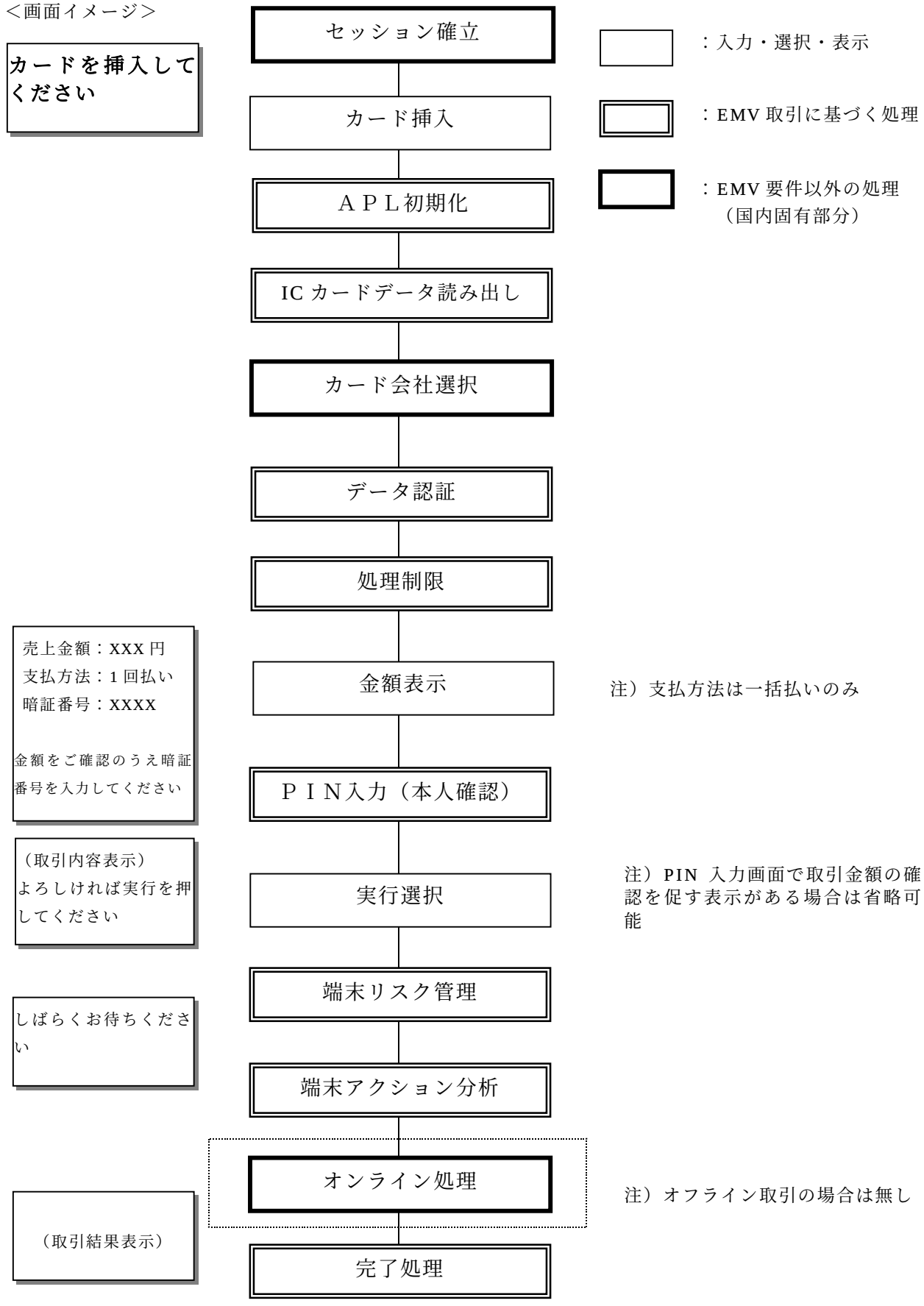
4.4.1　売上処理

売上処理は、車載機と店舗サーバ間の DSRC のセッション確立後、IC カードと店舗サーバの間で EMV 仕様に規定されるデータ認証、処理制限、本人確認及び端末リスク管理等の処理を実行し、IC クレジットカードが決済の可否の判定を行う。また、オンラインにてイシュア（発行者）が IC クレジットカードの利用可否を判定する場合も発生する。

なお、車載機と店舗サーバの間で交信されるクレジットデータは、第 3 章及び 6 章にて記述される方法にて暗号化されるものとする。

4.4.2　売上処理フロー

以下は、標準的な処理フロー例である。



(1)　セッション確立
　DSRC のセッション確立後に車載機と店舗サーバの通信のセキュリティを確保し、店舗端末と同様の EMV 処理を実施する環境を構築する。

(2)　カード挿入
　車載機に IC クレジットカードを挿入する。

(3)　APL 初期化
　業務処理に際し、IC クレジットカード処理に用いるデータ要素を初期化する。

(4)　IC カードデータ読み出し
　IC クレジットカードから取得したファイル情報をもとに、IC クレジットカードに格納されている IC カード情報を読み出す。

(5)　カード会社判定
　読み出された情報を基に取扱いカード会社を判定する。判定方法は、「IC カード対応端末機能仕様書／日本クレジットカード協会」の規定に準じる。

(6)　データ認証
　店舗サーバが、IC クレジットカードの真正性の検証を行う。

(7)　処理制限
　IC クレジットカードから取得したアプリケーションバージョン情報、アプリケーションの使用制限情報及びアプリケーションの有効期限より当該カードが利用可能かの検証を行う。

(8)　金額表示
　店舗サーバより入力された売上金額を車載機のディスプレイに表示し、会員が金額確認及び支払方法（本仕様書では一括払いのみ）を行うことを可能とする。

(9)　PIN 入力（本人確認）
　会員に対し、金額・支払方法確認後、暗証番号の入力を促す画面を車載機のディスプレー上に表示する。車載機で標準的にサポートすべき本人確認方法は、原則、オフライン PIN とする。

(10)　実行選択
　取引内容を画面に表示し、取引に実行確認を行う。
　＊PIN 入力画面で取引内容の確認を促す表示がある場合は省略可能。

(11)　端末リスク管理
　IC クレジットカードから送信された情報及び予め登録されたパラメータを基に、店舗サーバで一定の取引チェックを行う。

(12)　端末アクション分析
　店舗サーバで検証した結果（TVR）と店舗サーバに予め登録されている判定基準（Terminal Action Code）及び IC クレジットカードの判定基準（Issuer Action Code）をもとに、店舗サーバが IC クレジットカードに対して要求する取引内容（オフライン承認、オフライン拒否、オンライン処理）を判定する。

(13)　オンライン処理

店舗サーバが、IC クレジットカードからオンライン要求を受信した場合にオンライン処理を行う。センターからのオーソリ電文の結果に従って店舗サーバは取引の承認又は否認を IC クレジットカードに要求する。

(14)　完了処理

IC クレジットカードは、店舗サーバよりの判定要求に基づき、取引可否の最終判定を行い、店舗サーバは、結果を車載機のディスプレイに表示する。

有人対応にて商品を受領する際に IC クレジットカードの利用伝票を受領する。

伝票のレイアウトについては各ブランドの仕様及び各情報処理センター接続仕様に基づくものとするが「DSRC クレジット取引」の旨が表示されることが望ましい。

4.5　取消・返品処理

DSRC クレジット取引による売上取引の取消・返品処理は、原則、店舗にて有人対応する。取扱いは「IC カード対応端末機能仕様書／日本クレジットカード協会」に準じる。

（注）DSRC による取消・返品の取扱いは、実装時の検討事項とする

4.6　承認後売上

DSRC クレジット取引では承認後売上は取り扱わない。
必要な場合は店舗にて有人対応する。

有人での取扱いは「IC カード対応端末機能仕様書／日本クレジットカード協会」に準じる。

4.7　事前承認（オーソリ予約）

DSRC クレジット取引では事前承認は取り扱わない。
必要な場合は店舗にて有人対応する。

有人での取扱いは「IC カード対応端末機能仕様書／日本クレジットカード協会」に準じる。

4.8　無効カードチェック

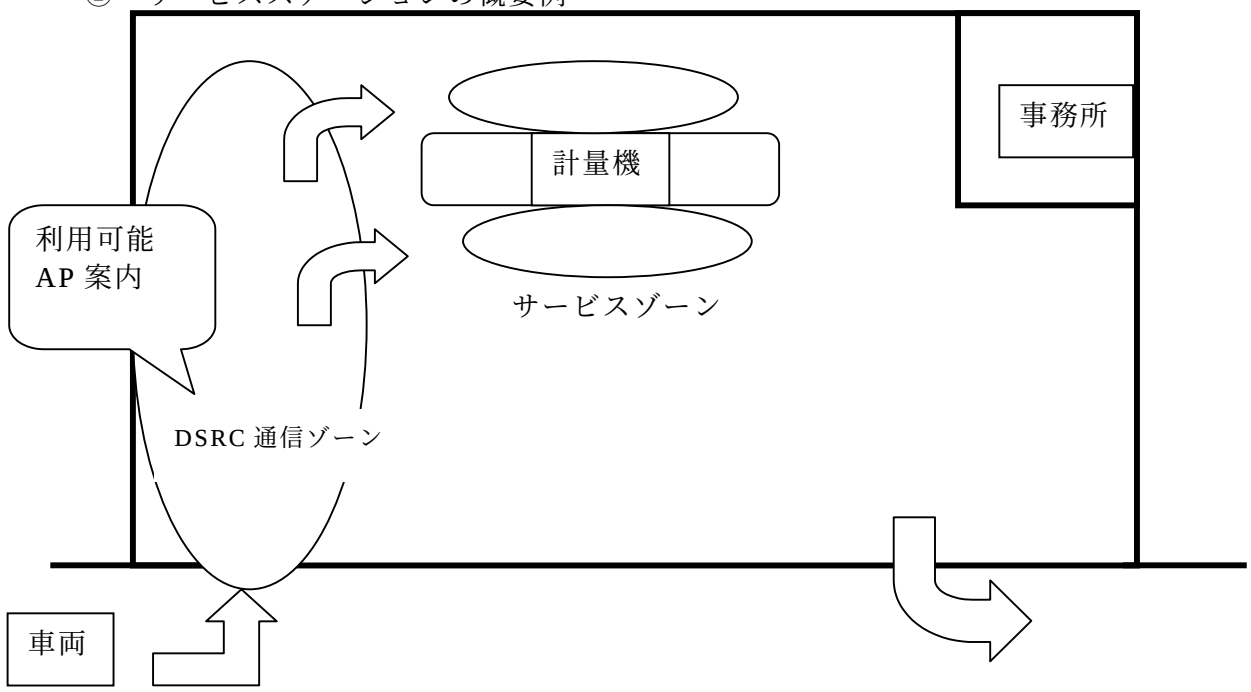
DSRC クレジット取引では無効カードチェックは取り扱わない。
必要な場合は店舗にて有人対応する。

有人での取扱いは「IC カード対応端末機能仕様書／日本クレジットカード協会」に準じる。

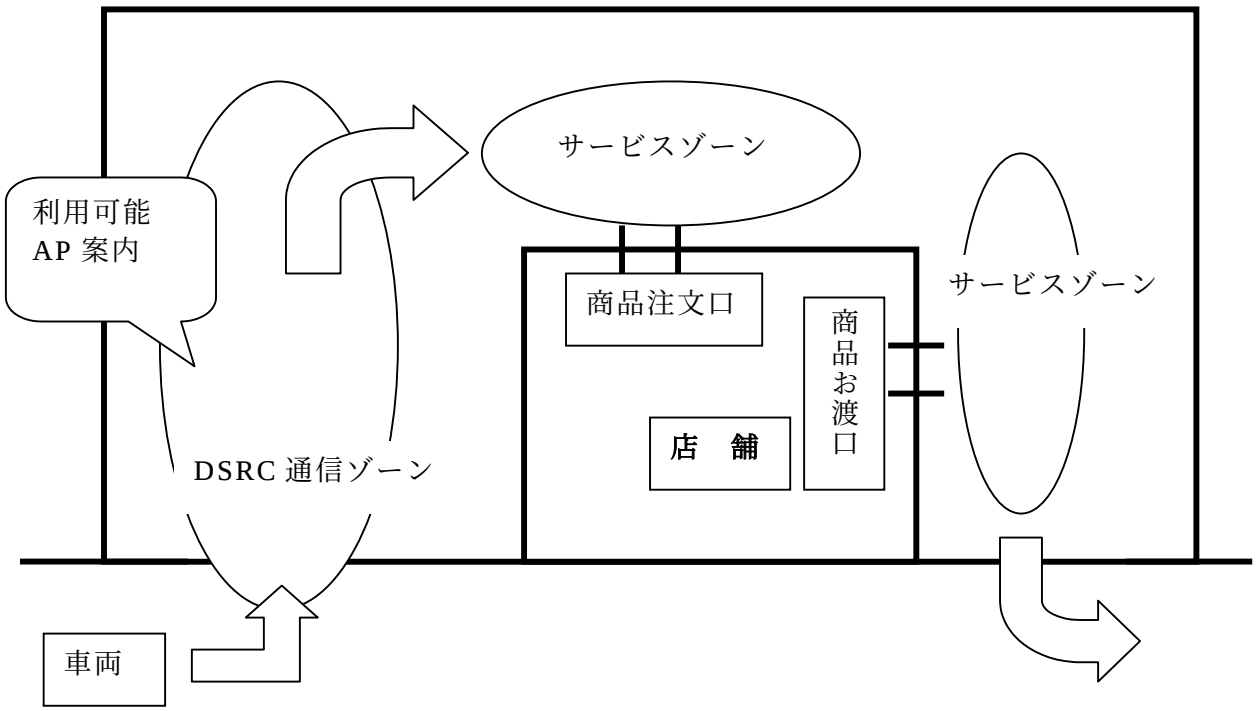
5　アプリケーションフロー

5.1　利用環境概要例

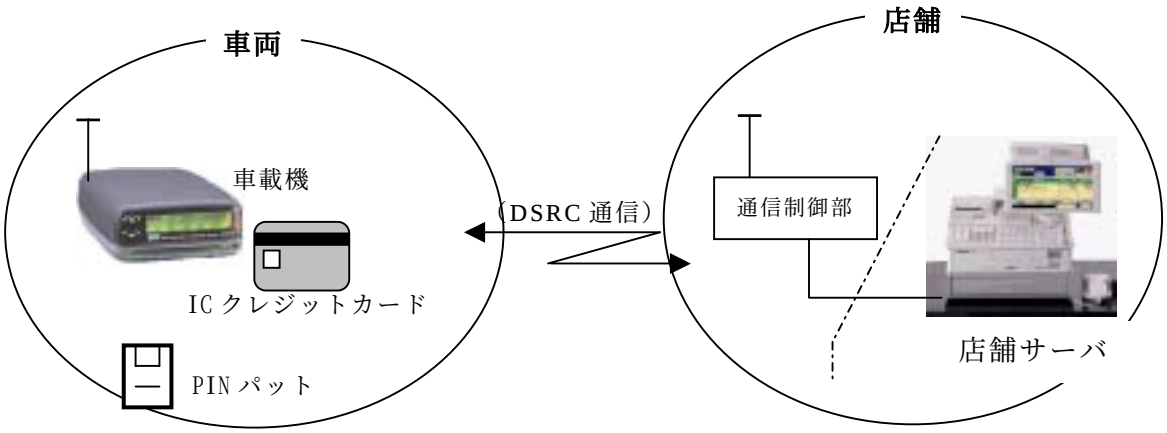
①　サービスステーションの概要例



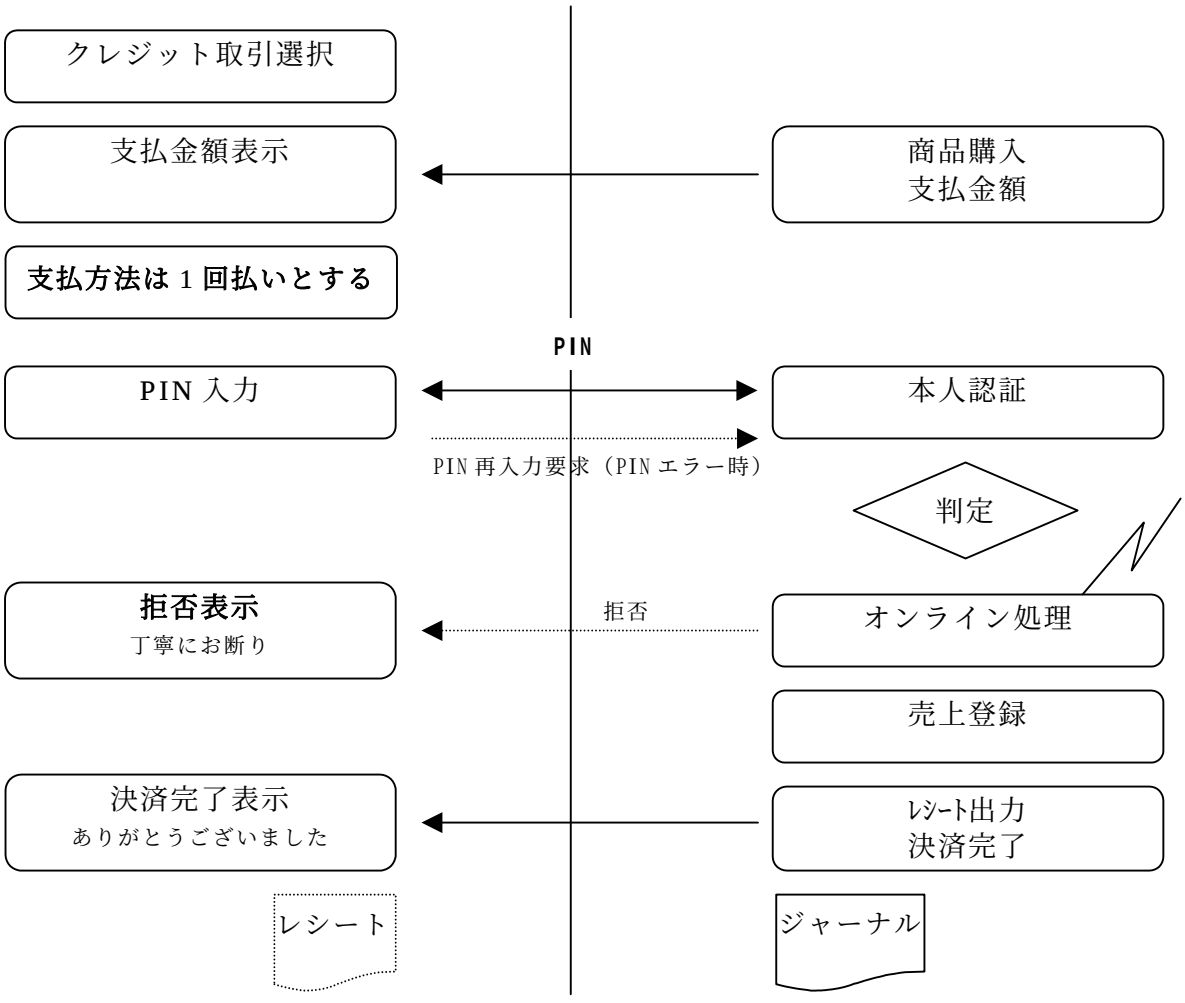
②　ロードサイド店舗の概要例



5.2　利用手順概要



DSRC 通信ゾーンに停車後、IC クレジットカードを車載機リーダーに挿入しクレジット決済を選択する。車載機は事前に店舗での利用可能アプリケーションの案内がされる。



6　通信フロー

6.1　IP 方式

6.1.1　概要

IP 方式は、TCP/IP 上で新たに定義する決済プロトコルにより決済を行う。

6.1.2　アプリケーション／プロトコルスタック

IP 方式では通信メディアとして DSRC を使用する場合、その上位プロトコルとして DSRC ASL 仕様書で規定される「IP over DSRC」を使用する。決済プロトコルの詳細については6.1.5　で記述する。

IP 方式のアプリケーション／プロトコルスタックを図 6.1.2-1に示す。

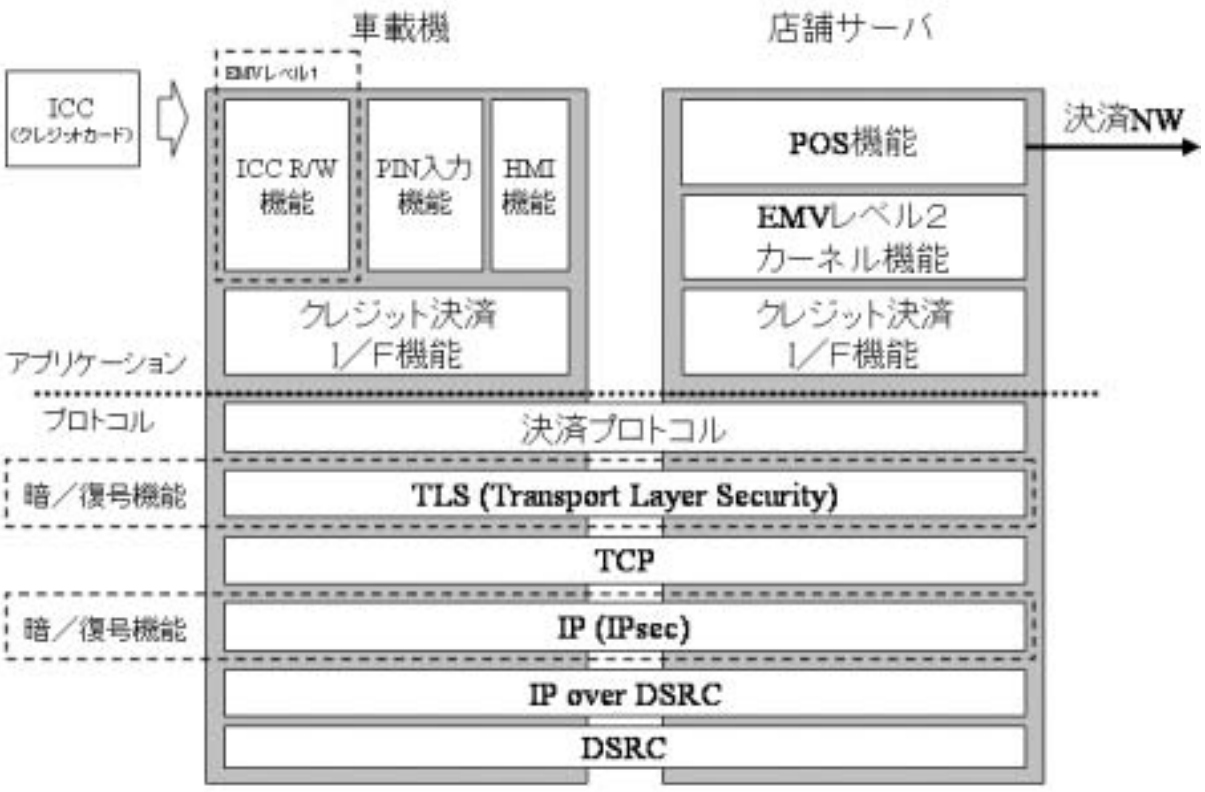


図 6.1.2-1　IP 方式のアプリケーション／プロトコルスタック

6.1.3　DSRC 通信ポート

DSRC ASL 仕様書に従う。

6.1.4　セキュリティ

IP 方式では次のセキュリティ対策を講じる。

(1)　TLS/IPsec による認証および通信の暗号化

インターネット上で広く利用されている暗号化通信技術である TLS（Transport Layer Security）または IPsec の利用により認証・通信の暗号化を行う。

(2)　ネットワーク機器／ホスト設定による閉域接続

店舗サーバと車載機間の通信に他の（故意／偶然にかかわらず）余計なトラヒックが影響を及ぼさないためにネットワーク機器／ホスト設定により閉域接続を行なう。具体的には店舗サーバに対する通信を車載機が発信元となっているものに制限する。同時に車載機に対する通信のうち決済に関するものを店舗サーバが発信元となっているものに限定する。

6.1.5　決済プロトコル

6.1.5.1 コネクションの確立

IP 方式では、ストリーム型 SOCKET（TCP/IP）を使用してコネクションを確立する。車載機側・店舗側で使用するポート番号は別途規定する。

6.1.5.2 サービスプリミティブ論理体系

決済メッセージは、4 種類のサービスプリミティブ（要求（A-DATA.req）、指示（A-DATA..ind）、応答（A-DATA.res）、確認（A-DATA.cnf）を使用して交換される。サービスプロバイダは、完全透過のため、A-DATA.req と A-DATA.ind および A-DATA.res と A-DATA.cnf は完全に一致する。図 6.1.5-1にサービスプリミティブ交換の論理体系を示す。

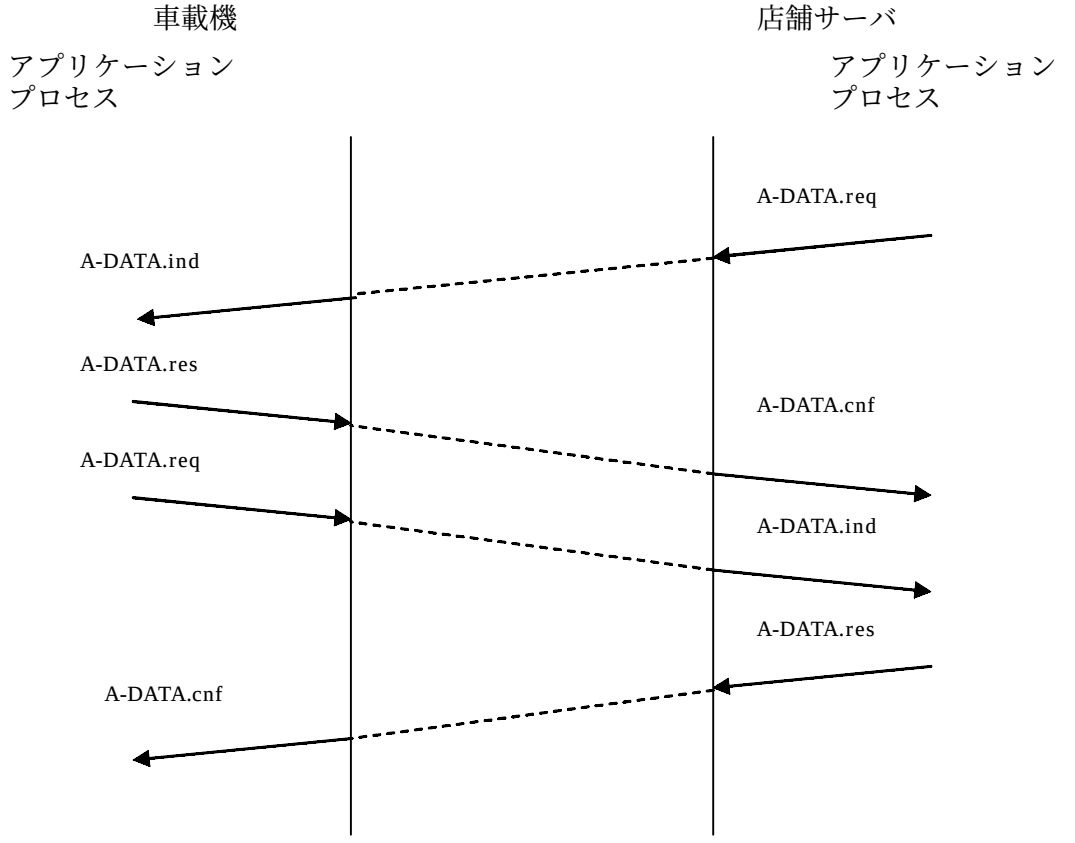


図 6.1.5-1　サービスプリミティブ交換の論理体系

6.1.5.3 サービスプリミティブ構造

要求プリミティブ（A-DATA.req）、応答プリミティブ（A-DATA.res）はパラメータとして以下のものを含む。これらは ASN.1 の PER(Packed Encoding Rules)に基づきエンコードされる。

(1) DSRCCreditCommand

DSRCCreditCommand の定義を以下に示す。

```
DSRCCreditCommand::= SEQUENCE {
        versionIndex     Version,
        creditCommand CreditCommand
}

Version::= SEQUENCE {
        majorVersion INTEGER(0..15), --当初は 1 とする。
        minorVersion INTEGER(0..15) --当初は 0 とする。
}

CreditCommand::=CHOICE{
        authenticateCommand   [0] AuthenticateCommand, --IP 方式では未使用
        operationCommand      [1] OperationCommand,
        dummy                 [2-254 ] NULL, --将来拡張用
        obeDenialResponse     [255] ObeDenialResponse
                                        --車載機からの否定応答
}
```

(2) OperationCommand

OperationCommand は IC クレジット取引で使用するデータを送受信する際に使用する。OperationCommand の定義を以下に示す。

```
OperationCommand::=SEQUENCE{
        opCommandType         OpCommandType,
        opSecurityProfile     OpSecurityProfile,
        opCommandBody         OCTET STRING(SIZE(0..261))
                                        --IC カードコマンドの最大値
}

OpCommandType::=ENUMERATED{
        iCCCommand            (0), --IC カードコマンドコマンドメッセージ
        pinEntryRequest       (1), --PIN 入力要求
        endRequest            (2), --終了通知
        initRequest           (3), --開始通知
        reservedForFutureUse  (4-127), --将来拡張用
        iCCResponse           (128), --IC カードコマンドレスポンスメッセージ
        pinEntryResponse      (129), --PIN 入力データ
        endResponse           (130), --終了通知に対する応答
        initResponse          (131), --開始通知に対する応答
        reservedForFutureUse  (132-255) --将来拡張用
}
```

```
OpSecurityProfile::=SEQUENCE{
        encryptionAlgorithmId  INTEGER(0..255),
        keyNumber              INTEGER(0..255)
}
```

(3)　ObeDenialResponse

ObeDenialResponse は、車載機側の異常状態を通知するために使用する。
ObeDenialResponse の定義を以下に示す。

```
ObeDenialResponse::=SEQUENCE{
        status                 INTEGER(0..255), --ステータスコード
        supplementInfo         OCTET STRING(SIZE(0..127)) --補足情報
}
```

status として下記のコードを定義する。

00　　使用せず
01～31　共通領域
　01:PIN 入力キャンセル（利用者が PIN の入力を拒否）
　02:ICC 未挿入
　03:ICC 未応答
　04:バージョン不一致
32～63　非 IP 用の領域
64～95　IP 用の領域
96～127　予備
128～255　プライベート利用

(4)　opCommandBody

(A)　iCCCommand の場合

IC カードコマンドを店舗サーバから車載機に送付する場合に使用する。データフォーマットは以下の通り。

ISO/IEC 7816-4 の Command APDU （可変長）

(B)　iCCResponse の場合

IC カードコマンドの応答を車載機から店舗サーバへ送付するときに使用する。データフォーマットは以下の通り。

ISO/IEC 7816-4 の Response APDU （可変長）

(C)　pinEntryRequest の場合

PIN 入力要求を店舗サーバから車載機に送付するときに使用する。データフォーマットは下記の通り。

PIN 入力試行回数 （1 バイト固定）

(D)　pinEntryResponse の場合

PIN 入力結果を車載機から店舗サーバに送付するときに使用する。データフォーマットは下記の通り。

PIN 入力データ (ASCII コード、可変長)

(E)　endRequest の場合

DRSC クレジットトランザクションの終了通知を店舗サーバから車載機へ通知する。データフォーマットは、下記の通り。

データなし(SIZE(0))

(F)　endResponse の場合

DSRC クレジットトランザクションの終了通知に対する応答を車載機から店舗サーバへ送付するときに使用する、データフォーマットは下記の通り。

データなし(SIZE(0))

(G)　initRequest の場合

DSRC クレジットトランザクションの開始通知を店舗サーバから車載機へ送付するときに使用する。データフォーマットは下記の通り。

データなし(SIZE(0))

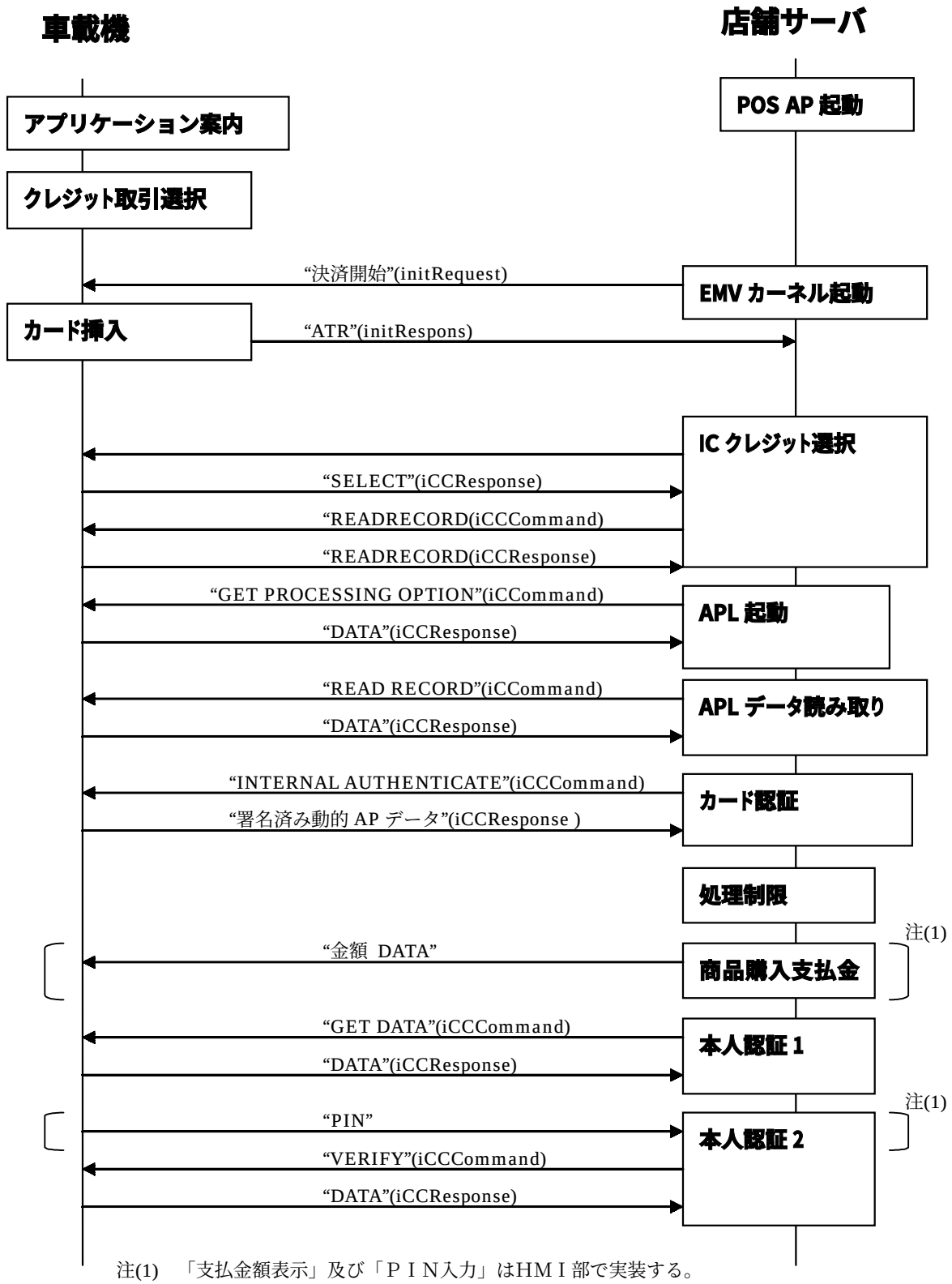
(H)　initResponse の場合

DSRC クレジットトランザクションの開始通知に対する応答を車載機から店舗サーバへ送付するときに使用する。データフォーマットは下記の通り。

IC カードから取得した ATR の値 (可変長)

6.1.5.4 動作シーケンス例

動作シーケンスの例を図 6.1.5-2、図 6.1.5-3に示す。



注(1)　「支払金額表示」及び「ＰＩＮ入力」はＨＭＩ部で実装する。

図 6.1.5-2　通信シーケンス例

（続く）

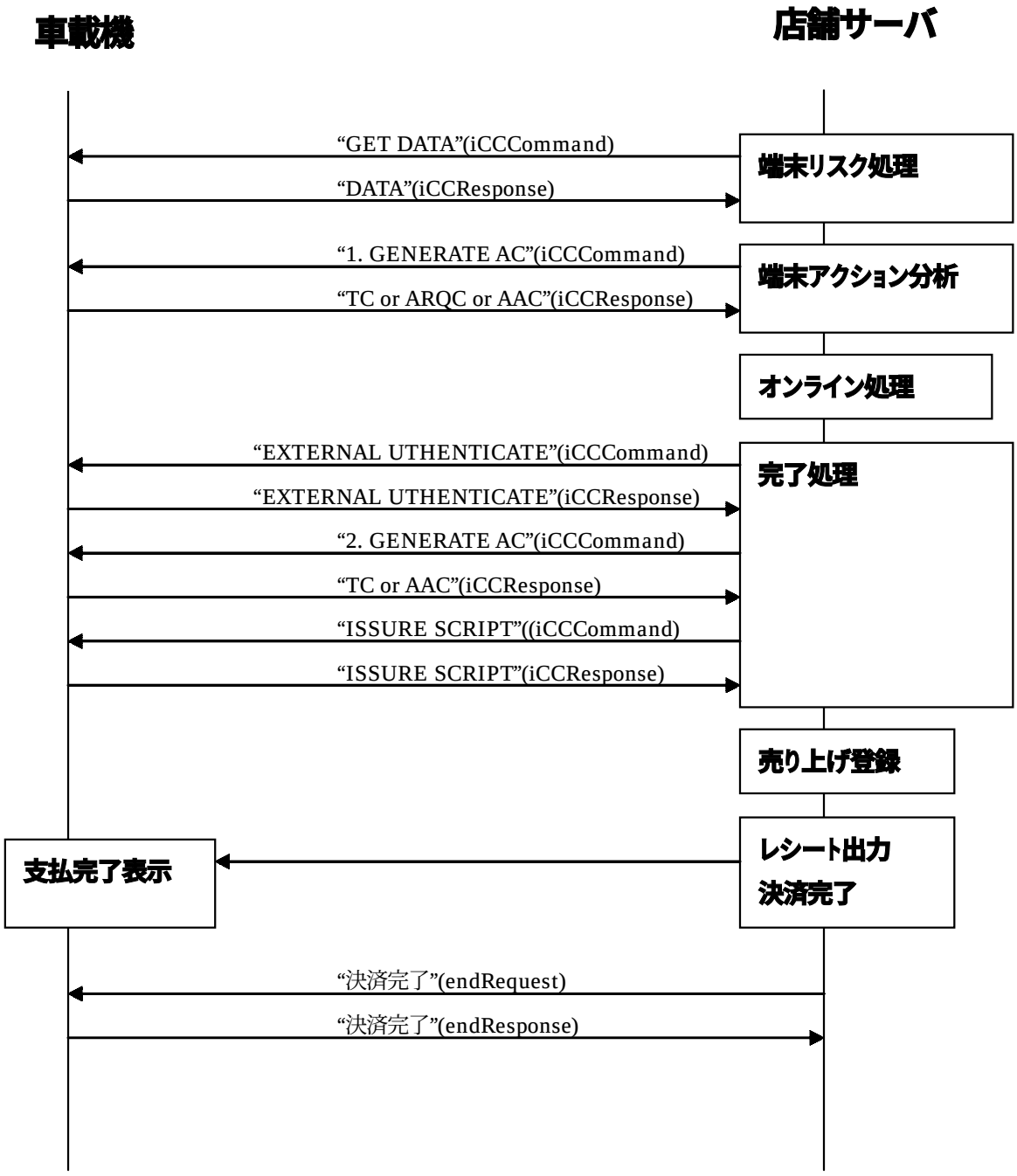


図 6.1.5-3　通信シーケンス例

6.2　非 IP 方式

6.2.1　概　要

非 IP 方式は、DSRC Application Sub-Layer 仕様書で規定されるローカルポート制御プロトコルを使用する。

非 IP 方式のプロトコルスタックを図 6.2.1-1 に示す。クレジット決済アプリケーションで使用されるデータは、アクセス点識別子とローカルポート番号により、他のアプリケーションと明確に分離する。

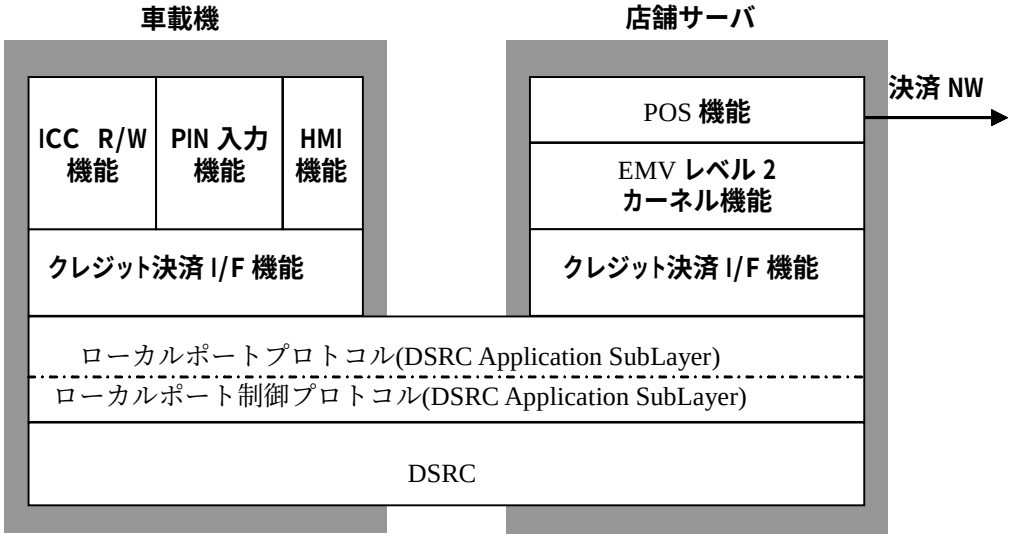


図 6.2.1-1　非 IP 方式におけるプロトコルスタック

(1)　DSRC ASL 通信制御プロトコルとの関連

非 IP 方式では、DSRC ASL 通信制御プロトコルで規定されている機能のうち、サーバ／クライアント型通信制御を利用する。サーバ／クライアント型通信制御では、基地局から移動局へのデータ送信に用いるデータ送信サービスと、移動局からのデータ送信を待ち受けるための送信問い合わせサービスが規定されており、クレジット決済アプリケーションでは以下の情報が対象となる。

(A)　データ送信サービス

①　IC カードコマンドコマンドメッセージ

②　PIN 入力要求　等

(B)　送信問い合わせサービス

①　IC カードコマンドレスポンスメッセージ

②　PIN データ　等

(2)　DSRC ASL ネットワーク制御プロトコルとの関連

非 IP 方式では、DSRC ASL ネットワーク制御プロトコルで規定されている機能のうち、ローカルポート制御プロトコルを利用する。DSRC ASL ネットワーク制御プロトコルでは、ローカルポート制御プロトコルを示すアクセス点識別子は“1”と定義されており、DSRC クレジットアプリケーションはローカルポート番号 0x1000 を使用して行われる。

6.2.2　トランザクションモデル

DSRC クレジットトランザクションモデルは、DSRC クレジットアプリケーションインタフェースで規定する初期設定段階及びトランザクション段階から構成する。

初期設定段階が完了しないと、トランザクション段階に移ることはできない。DSRC クレジットの各種機能はトランザクション段階で実行する。

(1)　初期設定段階

初期設定手順は、ARIB STD T-75 狭域通信（DSRC）システム標準規格 4.4.5「初期接続（設定）手順」で規定する「標準接続手順」とする。ここで使用される BST、VST については、DSRC ASL の規定に従う。なお、DSRC ASL の規定では、parameter に基地局、移動局の通信プロファイルを定義することとなっており、非 IP 通信の場合は LocalPort を登録する。

(2)　トランザクション段階

(A)　クレジット決済 I/F 機能の確認

初期設定段階の完了後、DSRC ASL は Notify ApplicationRSU プリミティブにより接続とリンク ID の通知を受ける。また、VST により、VehicleProfile と EID の通知をうける。以降はこのリンク ID 及び EID に基づいて通信を行うことになるが、実際のクレジットアプリケーションの情報をやり取りするのに先立って、図 6.2.2-1 の手順により店舗側、車載機側ともに受信可能ポートを相手に通知することにより、クレジット決済 I/F 機能が存在することを確認する。なお、この機能はローカルポートプロトコルの接続管理サービス利用することとする。

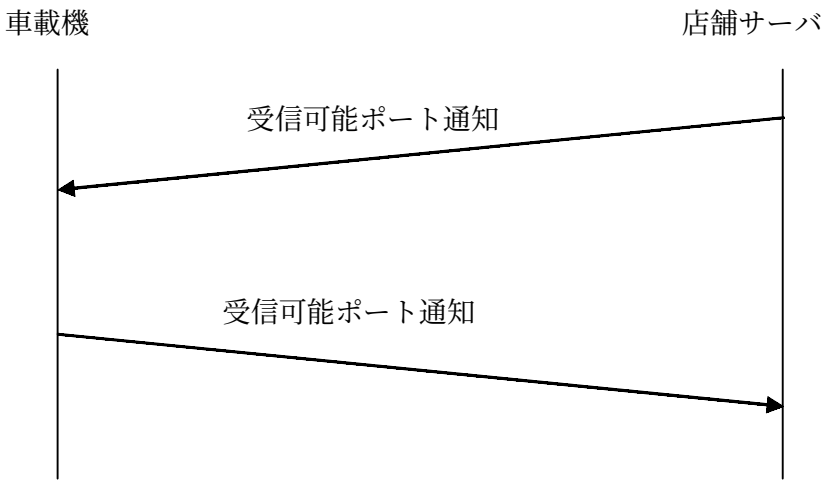


図 6.2.2-1　クレジット決済 I/F 機能確認シーケンス

(B)　DSRC クレジットトランザクション

DSRC クレジットトランザクションを実施する際、店舗サーバのアプリケーションは 6.2.3 項で定義する機能を使用しなければならない。店舗サーバのアプリケーションは DSRC クレジット機能シーケンスを呼び出し、DSRC クレジットトランザクションを実施する。車載機は店舗サーバに呼び出された DSRC クレジット機能に応答しなければならない。呼び出しがない場合、車載機はいかなる DSRC クレジット機能も開始してはならない。

DSRC クレジットトランザクションは、ローカルポートプロトコルが提供する 2 種類のトランザクションサービスのうち、単方向データ送信トランザクションサービスを使用する。この方式では、店舗側及び車載機側ともにデータ送信の際に Invoke プリミティブを使用することになり、6.2.3 項で定義する各コマンドは Invoke PDU のデータ部に格納されることになる。

6.2.3　DSRC クレジットの機能

DSRC クレジットで使用するコマンドを以下に示す。コマンドは、通常のコマンドと認証用のコマンドに大別され、それぞれ複数のコマンドに細分される。なお、データのコーディングにあたっては、ASN.1 の PER(Packed Encoding Rules)に基づき length 部と Contents 部にコーディングする。

(1)　DSRCCreditCommand

DSRCCreditCommand の定義を以下に示す。

```
DSRCCreditCommand::= SEQUENCE {
        versionIndex     Version,
        creditCommand CreditCommand
}

Version::= SEQUENCE {
        majorVersion INTEGER(0..15), --当初は 1 とする。
        minorVersion INTEGER(0..15) --当初は 0 とする。
}

CreditCommand::=CHOICE{
        authenticateCommand   [0] AuthenticateCommand,
        operationCommand      [1] OperationCommand,
        dummy                 [2-254 ] NULL, --将来拡張用
        obeDenialResponse     [255] ObeDenialResponse
                                                --車載機からの否定応答
}
```

(2)　AuthenticateCommand

AuthenticateCommand は、機器の相互認証とデータ保護のための暗号鍵の生成に用いる。AuthenticateCommand の定義を以下に示す。

```
AuthenticateCommand::=CHOICE{
        authPath1             [0]       OCTET STRING,
        authPath2             [1]       OCTET STRING,
        authPath3             [2]       OCTET STRING,
        authPath4             [3]       OCTET STRING,
        dummy                 [4-255]   NULL
    }
```

相互認証手順を図 6.2.3-1 に示す。

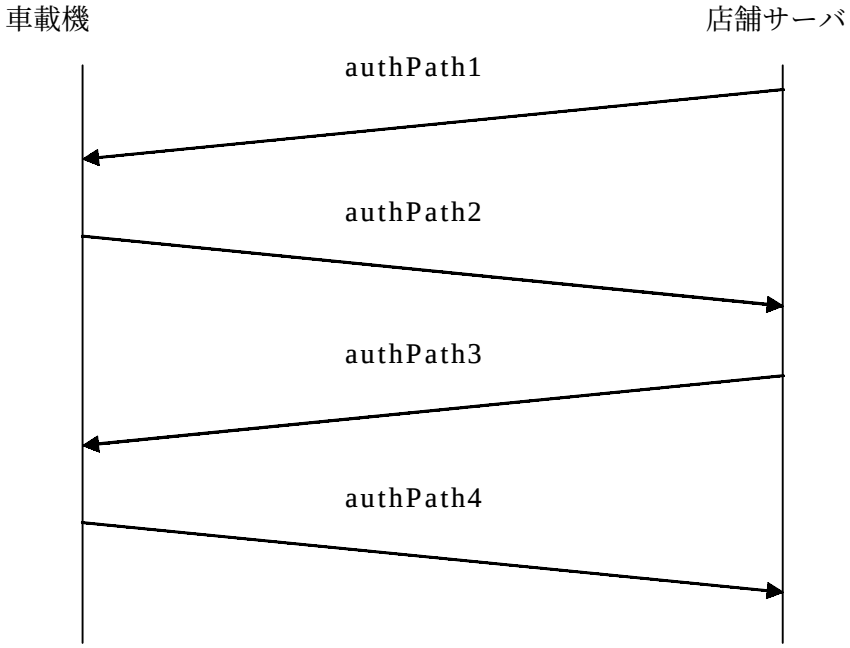


図 6.2.3-1　相互認証手順

相互認証に使用するデータの形式及び暗号鍵の生成の詳細については、別途規定する。

(3)　OperationCommand

OperationCommand は IC クレジット取引で使用するデータを送受信する際に使用する。OperationCommand の定義を以下に示す。

```
OperationCommand::=SEQUENCE{
        opCommandType       OpCommandType,
        opSecurityProfile   OpSecurityProfile,
        opCommandBody       OCTET STRING(SIZE(0..261))
                                        --IC カードコマンドの最大値
}

OpCommandType::=ENUMERATED{
        iCCCommand          (0), --IC カードコマンドコマンドメッセージ
        pinEntryRequest     (1), --PIN 入力要求
        endRequest          (2), --終了通知
        initRequest         (3), --開始通知
        reservedForFutureUse (4-127), --将来拡張用
        iCCResponse         (128), --IC カードコマンドレスポンスメッセージ
        pinEntryResponse    (129), --PIN 入力データ
        endResponse         (130), --終了通知に対する応答
        initResponse        (131), --開始通知に対する応答
        reservedForFutureUse (132-255) --将来拡張用
}
```

注）OpCommandType が 0,128,129 の場合、opCommandBody は暗号化を必須とする。暗号化処理の詳細については別途規定する。

```
OpSecurityProfile::=SEQUENCE{
        encryptionAlgorithmId    INTEGER(0..255),
        keyNumber                INTEGER(0..255)
}
```

(4)　ObeDenialResponse

ObeDenialResponse は、車載機側の異常状態を通知するために使用する。
ObeDenialResponse の定義を以下に示す。

```
ObeDenialResponse::=SEQUENCE{
        status                  INTEGER(0..255), --ステータスコード
        supplementInfo          OCTET STRING(SIZE(0..127)) --補足情報
}
```

status として下記のコードを定義する。

00　　使用せず
01～31　共通領域
　01:PIN 入力キャンセル（利用者が PIN の入力を拒否）
　02:ICC 未挿入
　03:ICC 未応答
　04:バージョン不一致
32～63　非 IP 用の領域
64～95　IP 用の領域
96～127　予備
128～255　プライベート利用

(5)　opCommandBody

(A)　iCCCommand の場合

IC カードコマンドを店舗サーバから車載機に送付する場合に使用する。データフォーマットは以下の通り。

ISO/IEC 7816-4 の Command APDU（可変長）

(B)　iCCResponse の場合

IC カードコマンドの応答を車載機から店舗サーバへ送付するときに使用する。データフォーマットは以下の通り。

ISO/IEC 7816-4 の Response APDU（可変長）

(C)　pinEntryRequest の場合

PIN 入力要求を店舗サーバから車載機に送付するときに使用する。データフォーマットは下記の通り。

PIN 入力試行回数（1 バイト固定）

(D)　pinEntryResponse の場合

PIN 入力結果を車載機から店舗サーバに送付するときに使用する。データフォーマットは下記の通り。

PIN 入力データ (ASCII コード、可変長)

(E)　endRequest の場合

DRSC クレジットトランザクションの終了通知を店舗サーバから車載機へ通知する。データフォーマットは、下記の通り。

データなし(SIZE(0))

(F)　endResponse の場合

DSRC クレジットトランザクションの終了通知に対する応答を車載機から店舗サーバへ送付するときに使用する、データフォーマットは下記の通り。

データなし(SIZE(0))

(G)　initRequest の場合

DSRC クレジットトランザクションの開始通知を店舗サーバから車載機へ送付するときに使用する。データフォーマットは下記の通り。

データなし(SIZE(0))

(H)　initResponse の場合

DSRC クレジットトランザクションの開始通知に対する応答を車載機から店舗サーバへ送付するときに使用する。データフォーマットは下記の通り。

IC カードから取得した ATR の値 (可変長)

7　取引シーケンス

7.1　商品売上シーケンス例

本例は車載機と EMV カーネルが一対一の場合である。

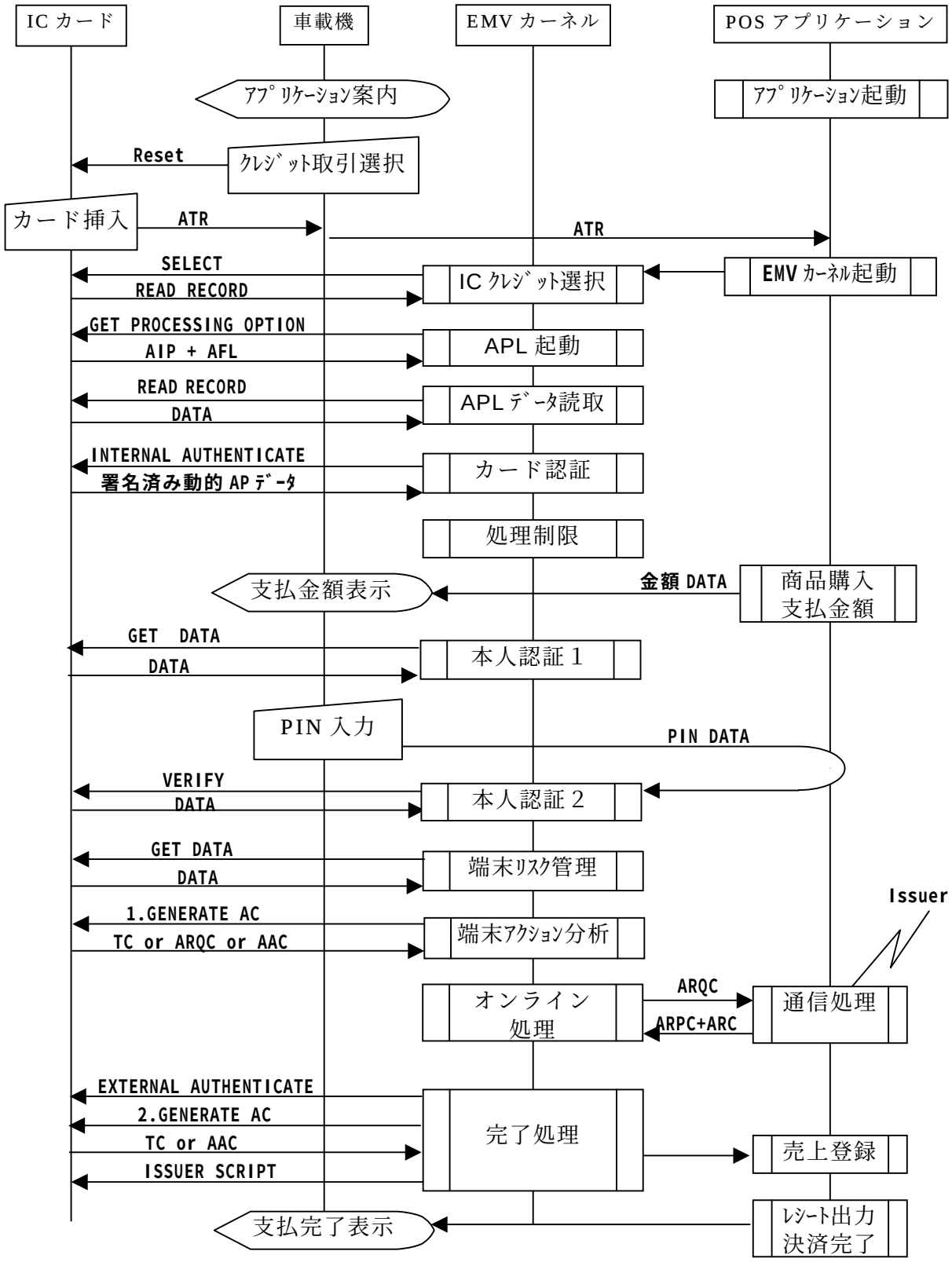


図 7.1-1　商品売上シーケンス例

7.2　処理詳細

(1)　アプリケーション起動

車両が DSRC 通信ゾーンに入ると店舗サーバと車載機で通信が開始され、利用アプリケーションの候補リストが車載機に表示される。

お客様は所定の位置に停車後、決済にクレジットを希望する場合は車載機に IC クレジットカードを挿入し、アプリケーションを選択（クレジット取引を指示）する、これにより車載機は IC クレジットカードに Reset を発行し処理を開始する。

この時店舗側の POS アプリケーションは事前に起動されている。

(2)　EMV カーネル起動

IC カードが挿入されると ATR を受け取り、正常であれば EMV カーネルを起動する。

(3)　IC クレジット選択
(4)　APL 起動
(5)　カード認証
(6)　処理制限
} EMV 仕様に準拠

(7)　商品決済金額

支払い金額を車載機に表示する。

(8)　PIN 入力

顧客は金額を確認し、IC クレジットで支払う場合は PIN 入力を行う。

IC クレジット決済しない場合は、中断指示により処理を終了する。

その場合 EMV カーネル処理は中断され起動待ちに戻る。

(9)　本人認証
(10)　端末リスク管理
(11)　端末アクション分析
(12)　オンライン処理
(13)　完了処理
} EMV 仕様に準拠

(14)　決済完了表示

正常に処理終了後、車載機に決済完了表示を行うこと。また、顧客にレシートを発行するが望ましい。

8　電文フォーマット

8.1　チップ－EMV カーネル間

ISO および EMV 仕様に準拠するためここに記述はしない。

CLA	INS	意味
'8x'	'1E'	APPLICATION BLOCK
'8x'	'18'	APPLICATION UNBLOCK
'8x'	'16'	CARD BLOCK
'0x'	'82'	EXTERNAL AUTHENTICATE
'8x'	'AE'	GENERATE APPLICATION CRYPTOGRAM
'0x'	'84'	GET CHALLENGE
'8x'	'CA'	GET DATA
'8x'	'A8'	GET PROCESSING OPTIONS
'08'	'88'	INTERNAL AUTHENTICATE
'8x'	'24'	PERSONAL IDENTIFICATION NUMBER (PIN) CHANGE/UNBLOCK
'0x'	'B2'	READ RECORD
'0x'	'A4'	SELECT
'0x'	'20'	VERIFY
'8x'	'Dx'	決算システム用 RFU
'8x'	'Ex'	決算システム用 RFU
'9x'	'xx'	独自の INS 符号化に対する製造者用 RFU
'Ex'	'xx'	独自の INS 符号化に対する発行者用 RFU

表 8.1-1　コマンド命令バイトの符号化一覧

8.2　車載機－EMV カーネル間

車載機はチップと EMV カーネルの電文をスルーするためここに記述しない。

8.3　車載機－上位アプリケーション間

8.3.1　電文種別

①支払金額通知電文
（POS アプリケーション　→　車載機）　　データ種別　ｘｘｘ
②PIN 電文
（車載機　→　POS アプリケーション）　　データ種別　ｘｘｘ
③オンライン中断電文Ⅰ
（POS アプリケーション　→　車載機）　　データ種別　ｘｘｘ
④PIN 中断電文Ⅱ
（車載機　→　POS アプリケーション）　　データ種別　ｘｘｘ
⑤PIN 再入力要求電文
（POS アプリケーション　→　車載機）　　データ種別　ｘｘｘ
⑥決済完了電文
（POS アプリケーション　→　車載機）　　データ種別　ｘｘｘ

8.3.2　電文フォーマット

項番	1	2	
項目	データ部種別	メッセージ	余　　白
桁数	××	××	

8.4　EMV カーネル－上位アプリケーション間

互換性の確保を必要としないため規定しない

8.5　IC クレジット部分のソフトウェア構造

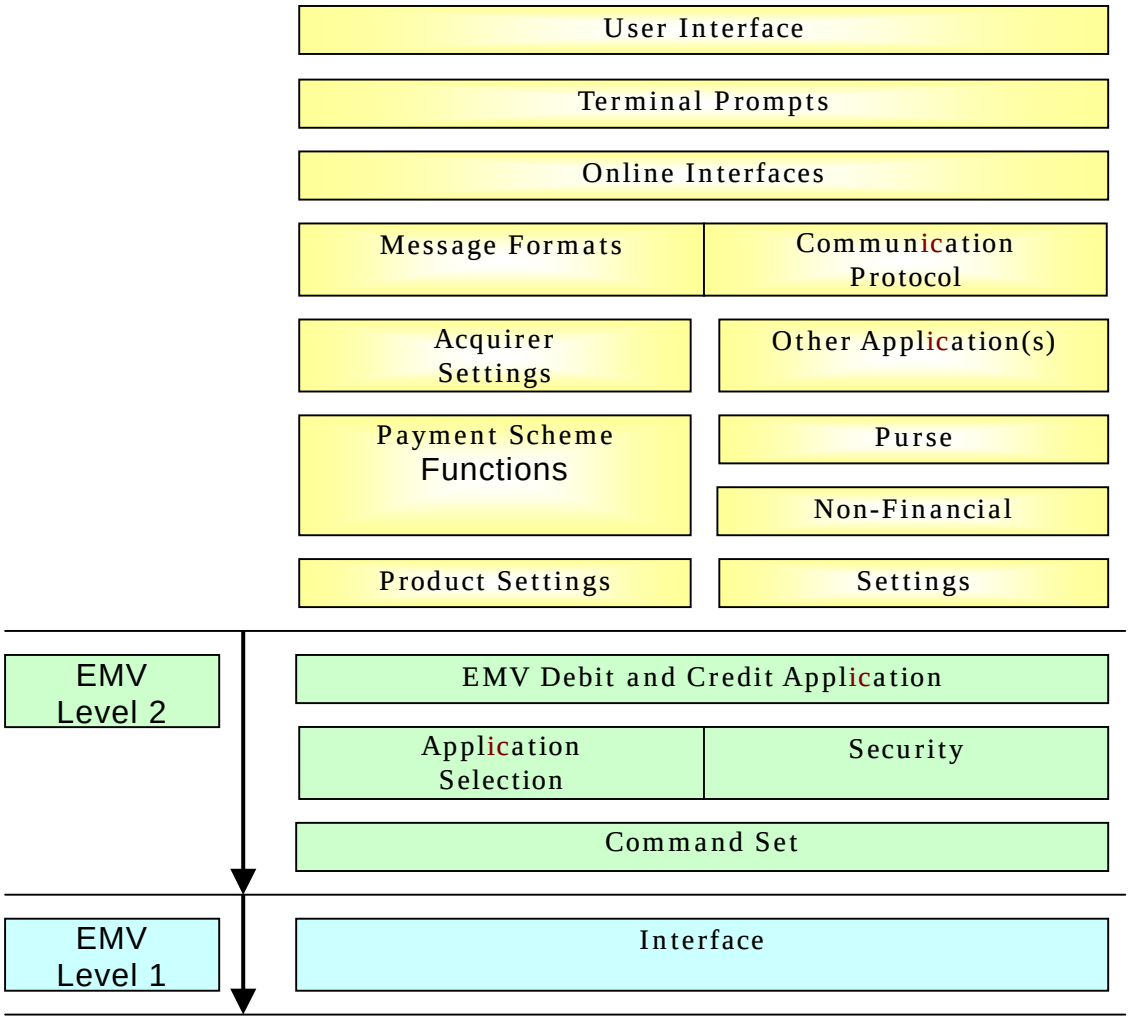


図 8.5-1　ソフトウェア構造

9　運用性確保の考え方

この章では、システムの運用性を確保することを目的とし、通信としての相互接続性確保および機密データ（秘密鍵・個人情報等）のセキュリティ確保の方策についての考え方を示す。

相互接続性確保のためには、仕様書のほかに、仕様書では記述できない点に関して、別途、接続試験仕様などが必要となることがある。

データのセキュリティ確保に関しては、暗号化の方式によって大きく対応が異なる。データの暗号化には、基本的に、共通鍵のみを利用するもの（以下、共通鍵方式）と共通鍵に加え公開鍵を併用するもの（公開鍵方式）がある。いずれの方式においても、暗号アルゴリズム、鍵、証明書の管理などの詳細については別途規定が必要である。

以下、エンドユーザが直接的に使用する車載機を中心に、暗号方式を考慮しながら IP 方式と非 IP 方式に分けて、次のような階層毎に、相互接続性確保とセキュリティ確保についての考え方を示す。

・車載ハードウエア
・通信路下位層
・通信路中位層
・通信路上位層
・アプリケーション

9.1　IP 方式

IP 方式での暗号方式としては、汎用インターネット技術である公開鍵方式の TLS または IPsec（6.1.2 を参照）を利用することが現実的であり、共通鍵方式は省いて記述する。図 9.1-1 に IP-公開鍵方式での運用性確保のための対応の全体を示す。

<table>
<tr><th>大分類</th><th>中分類</th><th>規格類</th><th>既存認定機関等</th><th>今回のクレジット決済での運用性確保のための対応</th></tr>
<tr><td>ｱﾌﾟﾘｹｰｼｮﾝ</td><td>EMV ｱﾌﾟﾘｹｰｼｮﾝ</td><td>EMV 規格（EMV ﾚﾍﾞﾙ 2）</td><td>EMVco</td><td>左項を利用</td></tr>
<tr><td rowspan="2">DSRC 通信路上位層</td><td>ｸﾚｼﾞｯﾄ決済 I/F 機能</td><td>今仕様書</td><td>－</td><td>相互接続性確保の検討要</td></tr>
<tr><td>暗／復号機能
TLS-公開鍵併用方式</td><td>－</td><td>－</td><td rowspan="2">セキュリティ運用仕様の別途作成要</td></tr>
<tr><td rowspan="2">DSRC 通信路中位層</td><td>TCP/IP(IPsec)</td><td rowspan="2">ARIB 規格
制定の見込み</td><td rowspan="3">民間 DSRC 向けの相互接続確保の仕組を設立見込み</td></tr>
<tr><td>ASL AID=18</td><td rowspan="3">左項を利用</td></tr>
<tr><td rowspan="3">DSRC 通信路下位層</td><td>L7</td><td rowspan="3">ARIB 規格
T75／TR-T16</td></tr>
<tr><td>L2</td></tr>
<tr><td>L1</td><td>技適認定機関</td><td>左項を利用</td></tr>
<tr><td rowspan="3">車載ﾊｰﾄﾞｳｴｱ</td><td>ICC R/W 機能</td><td>EMV ﾚﾍﾞﾙ 1</td><td>EMVco</td><td>左項を利用</td></tr>
<tr><td>鍵保持機能</td><td>－</td><td>－</td><td>セキュリティ運用仕様の別途作成要</td></tr>
<tr><td>個人情報保護機能</td><td>今仕様書</td><td>－</td><td>今仕様書にて規定</td></tr>
</table>

図 9.1-1　IP-公開鍵方式での運用性確保のための対応

9.1.1　車載ハードウエア

(1)　ICC R/W

EMV アプリケーションの一部として、各製造メーカーが EMV レベル 1 の認定を取得することによってこのシステムでの相互接続性を確保する。

(2)　鍵保持

ここでは、公開鍵方式を使用しており、この場合には、データの暗号化のための共通鍵は、通信の都度生成している。公開鍵のみ実装される箇所においては、鍵のセキュリティについての特別な配慮は不要である。

(3)　個人情報保護

個人情報が取り扱われることから、他者に個人情報が盗聴される危険を回避するために、暗号化されていない平文が読み出せる部分に関しては耐タンパー性を確保する。（参照：第 3 章(1)機能構成図の注）

9.1.2　通信路下位層

この階層は、ETC でも利用している ARIB 標準規格 STD-T75（DSRC システム）の領域と同一であり、ARIB 技術資料 TR-T16 （DSRC システム陸上移動局の接続性確認に係る試験項目・試験条件）で接続性確保のための試験条件を規定している。

L1（STD-T75 に規定されている）の電波通信仕様に関しては、電波法に定める技術基準に適合している認証を受けることが義務付けられており、財団法人テレコムエンジニアリングセンターが指定証明機関となっている。

L2、L7（ともに STD-T75 に規定されている）に関しては、今後、DSRC 民間応用向けの相互接続性確保の仕組が新設されると予測され、これを利用することが可能である。いずれにしても、この階層に関しては、クレジット決済独自の規格・試験仕様などは作成しないことが妥当である。

9.1.3　通信路中位層

この階層の ASL は、DSRC の民間応用のためにも必須となる仕様である。今後、ARIB 規格として制定され、これと平行して相互接続性を確保する仕組も新設されると予測されるため、これを利用することが可能である。いずれにしても、独自の規格・試験仕様などは作成しないことが妥当である。

また、TCP/IP の部分に関しては、汎用化したインターネットプロトコールの領域であり、新たな規格化は不要である。

9.1.4　通信路上位層

この階層の暗／復号機能は汎用のインターネット仕様であるが、クレジット決済 I/F 機能は、今仕様書固有のものである。よって、後日、今仕様書以外に、接続性確保のための試験仕様追加の是非について検討していく必要がある。

暗／復号機能は、汎用化したインターネット仕様として確立した TLS/IPsec を利用することから、新たな仕様化は不要である。ただし、使用する暗号アルゴリズム、証明書の運用などの詳細については、別途規定する必要がある。

9.1.5　EMV アプリケーション

この階層は、EMV 仕様 IC クレジットカードのシステムとして、既に確立し利用されている。新たな仕様化は不要である。さらに、相互接続性確保も、既存のものを利用するものとする。

9.2　非 IP 方式

非 IP 方式でのデータの暗号方式として、公開鍵方式および共通鍵方式を利用するものについて示す。図 9.2-1 に非 IP-公開鍵方式での運用性確保のための対応の全体を示し、図 9.2-2 に非 IP-共通鍵方式での運用性確保のための対応の全体を示す。

大分類	中分類	規格類	既存認定機関等	今回のクレジット決済での運用性確保のための対応
ｱﾌﾟﾘｹｰｼｮﾝ	EMV ｱﾌﾟﾘｹｰｼｮﾝ	EMV 規格（EMV レベル 2）	EMVco	左項を利用
DSRC 通信路上位層	ｸﾚｼﾞｯﾄ決済 I/F 機能	今仕様書	－	相互接続性確保の検討要
	暗／復号機能 公開鍵併用方式	－	－	セキュリティ運用仕様の別途作成要
DSRC 通信路中位層	ASL AID=XX	ARIB 規格制定の見込み	民間 DSRC 向けの相互接続確保の仕組を設立見込み	左項を利用
DSRC 通信路下位層	L7	ARIB 規格 T75／TR-T16		
	L2			
	L1		技適認定機関	左項を利用
車載ﾊｰﾄﾞｳｴｱ	ICC R/W 機能	EMV ﾚﾍﾞﾙ 1	EMVco	左項を利用
	鍵保持機能	－	－	セキュリティ運用仕様の別途作成要
	個人情報保護機能	今仕様書	－	今仕様書にて規定

図 9.2-1　非 IP-公開鍵方式での運用性確保のための対応

大分類	中分類	規格類	既存認定機関等	今回のクレジット決済での運用性確保のための対応
ｱﾌﾟﾘｹｰｼｮﾝ	EMV ｱﾌﾟﾘｹｰｼｮﾝ	EMV 規格（EMV レベル 2）	EMVco	左項を利用
DSRC 通信路上位層	ｸﾚｼﾞｯﾄ決済 I/F 機能	今仕様書	－	相互接続性確保の検討要
	暗／復号機能 共通鍵方式	－	－	セキュリティ運用仕様の別途作成要
DSRC 通信路中位層	ASL AID=XX	ARIB 規格制定の見込み	民間 DSRC 向けの相互接続確保の仕組を設立見込み	左項を利用
DSRC 通信路下位層	L7	ARIB 規格 T75／TR-T16		
	L2			
	L1		技適認定機関	左項を利用
車載ﾊｰﾄﾞｳｴｱ	ICC R/W 機能	EMV ﾚﾍﾞﾙ 1	EMVco	左項を利用
	鍵保持機能	－	－	セキュリティ運用仕様の別途作成要
	個人情報保護機能	今仕様書	－	今仕様書にて規定

図 9.2-2　非 IP-共通鍵方式での運用性確保のための対応

9.2.1　車載ハードウエア

(1)　ICC R/W

EMV アプリケーションの一部として、各製造メーカーが EMV レベル１の認定を

取得することによってこのシステムでの相互接続性を確保する。

(2)　鍵保持

(ア) 公開鍵方式

ここでは、公開鍵方式を使用しており、この場合には、データの暗号化のための共通鍵は、通信の都度生成している。公開鍵のみ実装される箇所においては、鍵の管理については特別な配慮は不要である。

(イ) 共通鍵方式

この方式では、車載機の筐体内に、データの暗号化のための秘密の情報（共通鍵）が事前に搭載されているため、鍵情報の漏洩についての十分な対策が必要である。

(3)　個人情報保護

個人情報が取り扱われることから、他者に個人情報が盗聴される危険を回避するために、暗号化されていない平文が読み出せる部分に関しては耐タンパー性を確保する。（参照：第 3 章(1)機能構成図の注）

9.2.2　通信路下位層

この階層は、ETC でも利用している ARIB 標準規格 STD-T75（DSRC システム）の領域と同一であり、ARIB 技術資料 TR-T16 （DSRC システム陸上移動局の接続性確認に係る試験項目・試験条件）で接続性確保のための試験条件を規定している。

L1（STD-T75 に規定されている）の電波通信仕様に関しては、電波法に定める技術基準に適合している認証を受けることが義務付けられており、財団法人テレコムエンジニアリングセンターが指定証明機関となっている。

L2、L7（ともに STD-T75 に規定されている）に関しては、今後、DSRC 民間応用向けの相互接続性確保の仕組が新設されると予測され、これを利用することが可能である。いずれにしても、この階層に関しては、クレジット決済独自の規格・試験仕様などは作成しないことが妥当である。

9.2.3　通信路中位層

この階層の ASL は、DSRC の民間応用のためにも必須となる仕様である。今後、ARIB 規格として制定され、これと平行して相互接続性を確保する仕組も新設されると予測されるため、これを利用することが可能である。いずれにしても、独自の規格・試験仕様などは作成しないことが妥当である。

9.2.4　通信路上位層

クレジット決済 I/F 機能は、今規格固有のものである。よって、後日、今仕様書以外に、接続性確保のための試験仕様追加の是非について検討していく必要がある。一方、暗／復号機能については、汎用化した仕様がないため、別途、セキュリティ運用仕様の作成が必要となる（(ア)公開鍵方式、(イ)共通鍵方式とも）。

9.2.5　EMV アプリケーション

この階層は、EMV 仕様 IC クレジットカードのシステムとして、既に確立し利用されている。新たな仕様化は不要であり、相互接続性確保も、既存のものを利用するものとする。

10　参照規格

以下の緒規格が、本書において引用され、本書の一部をなしている。

ISO/IEC 7816-1：1998 Identification cards - Integrated circuit(s) cards with contacts - Part 1： Physical characteristics

ISO/IEC 7816-2：1999 Information technology - Identification cards – Integrated circuit(s) cards with contacts - Part 2：Dimensions and location of the contacts

ISO/IEC 7816-3：1997 Information technology - Identification cards – Integrated circuit(s) cards with contacts – Part 3：Electronic signals and transmission protocols

ISO/IEC 7816-4：1995 Information technology - Identification cards – Integrated circuit(s) cards with contacts - Part 4：Interindustry commands for interchange

ISO/IEC 7816-4：1995/Amd 1：1997 secure messaging on the structures of APDU messages

ISO/IEC 7816-5：1994 Identification cards - Integrated circuit(s) cards with contacts - Part 5： Numbering system and registration procedure for application identifiers

ISO/IEC 7816-5：1994/Amd 1：1996

ISO/IEC 7816-6：1996 Identification cards - Integrated circuit(s) cards with contacts - Part 6：Interindustry data elements

ISO/IEC 7816-6：1996/Amd 1：2000 IC manufacturer registration

ISO/IEC 7816-8：1999 Identification cards - Integrated circuit(s) cards with contacts - Part 8： Security related interindustry commands

ISO/IEC 7816-9：2000 Identification cards -Integrated circuit(s) cards with contacts - Part 9： Additional interindustry commands and security attributes

ISO/IEC 7816-10：1999 Identification cards - Integrated circuit(s) cards with contacts - Part 10：Electronic signals and answer to reset for synchronous cards

EMV：2000 EMV2000 Integrated Circuit Card Specification for Payment Systems Book 1
- Application Independent ICC to Terminal Interface Requirements Ver4.0

EMV：2000 EMV2000 Integrated Circuit Card Specification for Payment Systems Book 2
- Security and Key Management Ver4.0

EMV：2000 EMV2000 Integrated Circuit Card Specification for Payment Systems Book 3
- Application Specification Ver4.0

EMV：2000 EMV2000 Integrated Circuit Card Specification for Payment Systems Book 4
- Cardholder, Attendant, and Acquirer Interface Requirements Ver4.0

EMV：2000 EMVCo Type Approval Terminal Level 1 Administrative Process

EMV：2000 EMVCo Type Approval Terminal Level 1 Requirements Process

EMV：2000 EMVCo Type Approval Terminal Level 1 Test Cases Process

EMV：2000 EMVCo Type Approval Terminal Level 2 Requirements

EMV：2000 EMVCo Type Approval Terminal Level 2 Test Cases

株式会社ジェーシービー：ジェーシービーIC カード仕様書 1.2 版

株式会社ジェーシービー：ジェーシービー端末仕様書 1.2 版

株式会社ジェーシービー：ジェーシービー仕様書付録 1.2 版

株式会社ジェーシービー：ジェーシービーEMV2000 対応要件

株式会社ジェーシービー：ジェーシービーEMV2000 対応要件　付録

株式会社ジェーシービー：ジェーシービーIC カード仕様書　JPO 編 1.2 版

株式会社ジェーシービー：ジェーシービー端末仕様書　JPO 編 1.2 版

株式会社ジェーシービー：ジェーシービー仕様書付録　JPO 編 1.2 版

※各仕様書参照には株式会社ジェーシービーへの仕様書開示依頼書の提出が必要になります。

MasterCard International：MasterCard Chip-Recommended Specifications for Debit and Credit Version4
MasterCard International：MasterCard Chip-Minimum Card Requirements for Debit and Credit Version4
MasterCard International：MasterCard Chip-Terminal Requirements for Debit and Credit Version4

Visa International：2001 Visa Integrated Circuit Card Application Overview Version 1.4.0
Visa International：2001 Visa Integrated Circuit Card Card Specification Version 1.4.0
Visa International：2001 Visa Integrated Circuit Card Terminal Specification Version 1.4.0

日本クレジットカード協会：2001　IC カード対応端末機能仕様書 1.1

社団法人電波産業会（ARIB）：2001 ARIB STD-T75　狭域通信（DSRC）システム標準規格 1.0 版
社団法人電波産業会（ARIB）：2001 ARIB TR-T16　狭域通信（DSRC）システム陸上移動局の接続性確認に係る試験項目・試験条件　技術資料　1.0 版

財団法人道路新産業開発機構（HIDO）：2002　インフォメーションシャワー基本仕様　－DSRC アプリケーションサブレイヤー　0.00.5 版

JIS X 5603：1990　開放型システム間相互接続の抽象構文記法１（ASN.1）仕様
JIS X 5606-2：1998　情報技術　－　ＡＳＮ．１符号化規則　－　第２部：圧縮符号化規則（PER）の仕様