4　共通機能の要件の検討

本章では、基本 API（ITS FORUM RC-004 に規定された、基本アプリケーションインタフェース）を引用して、共同研究の成果をまとめ、共通機能として記述する。

4.1　通信機能

挟域通信システム（DSRC）技術を用いた、「道路上における情報提供サービス」、「道の駅等における情報接続サービス」、「公共駐車場決済システム」等を対象とする新しいサービスを提供するため通信機能としては、以下の機能に対応する。

⑴IP 通信を利用できるとともに、動的なアドレス割当て機能

⑵非 IP 通信を利用した一対一通信、及び同報通信機能

また、非 IP 通信時においては、以下の機能に対応する。

⑴指示応答機能

⑵メモリアクセス機能

⑶ID 通信機能

⑷IC カードアクセス機能

⑸プッシュ型情報配信機能

⑹共通セキュリティ機能

4.1.1　プロトコル構成

図 4.1-1 に通信機能を実現するための、DSRC 路側無線装置及び ITS 車載器におけるプロトコル構成を示す。

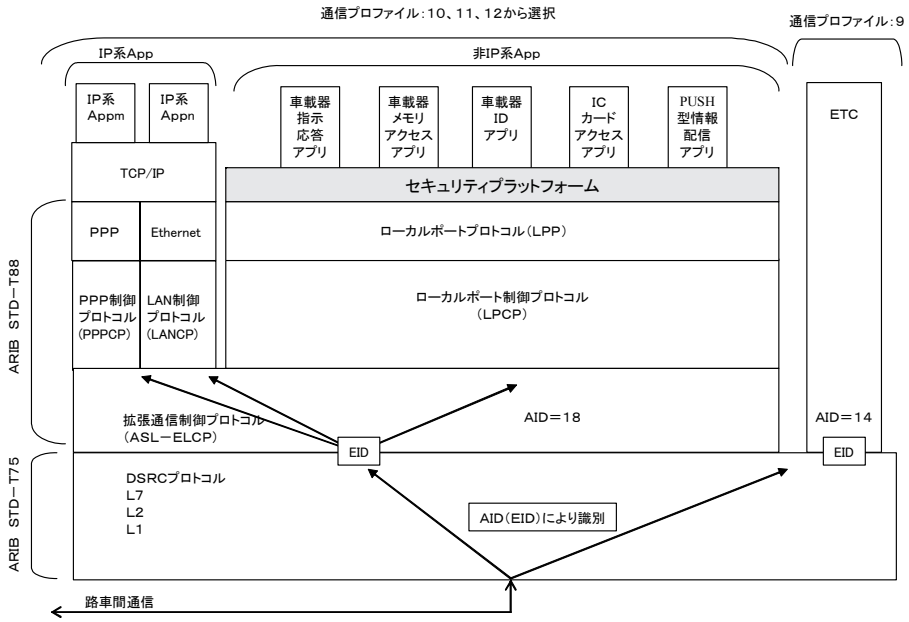

図 4.1-1　プロトコル構成

適用する通信仕様として、狭域通信（DSRC）システム標準規格　ARIB STD-T75、狭域通信（DSRC）アプリケーションサブレイヤ標準規格 ARIB STD-T88、ITS 情報通信システム推進会議　狭域通信（DSRC）基本アプリケーションインタフェース仕様ガイドライン ITS FORUM RC-004 により、IP 通信及び非 IP 通信、一対一通信及び同報通信、並びに、非 IP 通信における共通機能を実現する。

4.1.2　IP 通信機能

IP 通信機能を実現する制御プロトコルとして、PPP 制御プロトコルと LAN 制御プロトコルがある。

PPP 制御プロトコルは、DSRC を媒体としてポイント・ツー・ポイントプロトコル（PPP）接続を行うために、PPP 回線に対してインタフェースを提供する機能を有する。

LAN 制御プロトコルは、DSRC を媒体としてローカルエリアネットワーク（LAN）接続を行うために、LAN 側のデータリンク層とのインタフェースを提供する機能を有する。

現段階では TCP/IP など上位プロトコルが搭載されるカーナビゲーションとの接続性等を考慮し、PPP 制御プロトコルを利用するものとし、LAN 制御プロトコルは、将来的に LAN 制御プロトコルを搭載した車載器が標準市販機器に可能な段階で対応するものとする。

4.1.2.1　IP アドレス割り当て方式

(1)PPP 制御プロトコル

PPP 制御プロトコルを適用した場合、PPP プロトコルにより、動的に IP アドレスを割り当てることが出来る。

(2)LAN 制御プロトコル

LAN 制御プロトコルを適用した場合、DHCP や PPPoE 機能により動的に IP アドレスを割り当てることが出来る。

4.1.3　非 IP 通信機能

4.1.3.1　アプリケーション利用ポート

各基本 API が使用するローカルポート番号については、0x0C00～0x0C1F のエリアを使用することとし、さらに、情報の流れに着目して、そのエリアを 4 種類に分類した。表 4.1-1 に基本 API のローカルポート番号の一覧を示す。

表 4.1-1　基本 API のローカルポート番号

通常ポート	セキュアポート	アプリケーション	備考
0x0C00	0x0C20	車載器 ID 通信アプリケーション	＜情報の流れ＞ 路←車
0x0C01　～ 0x0C07	0x0C21　～ 0x0C27	将来拡張用	
0x0C08	0x0C28	車載器基本指示アプリケーションに採番済み	＜情報の流れ＞ 路→車
0x0C09	0x0C29	車載器指示応答アプリケーション	
0x0C0A	0x0C2A	プッシュ型情報配信アプリケーション	
0x0C0B　～ 0x0C0F	0x0C2B　～ 0x0C2F	将来拡張用	
0x0C10	0x0C30	IC カードアクセスアプリケーション	＜情報の流れ＞ 路←→車 カード利用
0x0C11　～ 0x0C17	0x0C31　～ 0x0C37	将来拡張用	
0x0C18	0x0C38	メモリアクセスアプリケーション	＜情報の流れ＞ 路←→車 メモリ利用
0x0C19　～ 0x0C1F	0x0C39　～ 0x0C3E	将来拡張用	
-	0x0C3F	セキュリティプラットフォーム管理ポート	

4.2　指示応答機能

狭域通信（DSRC）基本アプリケーションインタフェース仕様ガイドライン（ITS FORUM RC-004、ITS 情報通信システム推進会議）を参照のこと。

4.3　メモリアクセス機能

狭域通信（DSRC）基本アプリケーションインタフェース仕様ガイドライン（ITS FORUM RC-004、ITS 情報通信システム推進会議）を参照のこと。

4.4　IC カードアクセス機能

狭域通信（DSRC）基本アプリケーションインタフェース仕様ガイドライン（ITS FORUM RC-004、ITS 情報通信システム推進会議）を参照のこと。

4.5　プッシュ型情報配信機能

プッシュ型情報配信機能については、狭域通信（DSRC）基本アプリケーションインタフェース仕様ガイドライン（ITS FORUM RC-004、ITS 情報通信システム推進会議）を参照のこと。

ただし、アプリケーションタイプ及びコンテンツタイプについては、安全運転支援アプリへの適用を考慮し検討を行ったうえで、共同研究では安全運転支援に関するアプリケーションタイプ及びコンテンツタイプを以下のとおり定義する。

表 4.5-1　アプリケーションタイプ

アプリケーション	識別子	値	備考
		:	
テキスト表示アプリ	text-display	0x09	テキストデータを表示する。
安全運転支援アプリ	**safety**	**0x0A**	
その他	others	0x0B-0xFE	
任意アプリ	private	0xFF	任意のテキストでアプリケーション種別を指定

表 4.5-2　コンテンツタイプ

コンテンツタイプ	値	pushBody の型式	備考
		:	
dsrc/mime	0x83	MIME エンコーディングされたテキストファイル	MIME エンコーディングされたデータ
dsrc/safety	**0x84**		**安全運転支援アプリ用データ**
otherType	0x85-0xEF		
private	0xF0-FF		private 用(任意使用可)

4.6　ID 通信機能

狭域通信（DSRC）基本アプリケーションインタフェース仕様ガイドライン（ITS FORUM RC-004、ITS 情報通信システム推進会議）を参照のこと。

4.7 DSRC 通信部の共通セキュリティ機能（DSRC-SPF）

4.7.1 機能概要

4.7.1.1 構成

DSRC セキュリティプラットフォーム(DSRC-SPF)は、ITS 車載器－路側システムにおいて相互認証を行い、機器認証を行う。また相互認証で交換した鍵を用いて、基本アプリケーションの暗号通信に利用する。SPF が使用するセキュリティ種別については、複数のものから選択可能な仕様とする。

図 4.7-1 に示すようにセキュリティプラットフォームは基本アプリケーションと LPP の間に位置し、SPF に割り当てられたローカルポート番号(LP1)を利用して、セキュリティ種別の交渉、相互認証及び鍵交換処理を行うと共に、この認証・鍵交換フェーズで選択したセキュリティ種別および交換した鍵を利用して、基本アプリケーションから渡された送信データの暗号化や、LPP から渡された受信データの復号化を行う。また、各基本アプリケーションは、SPF を使用するポート（セキュアポート:LP3）と SPF を使用しないポート（通常ポート:LP2）の２つのポートを有し、LPP のトランザクション単位でデータを SPF で処理するか（セキュアポートへの送信)、SPF をバイパスするか（通常ポートへの送信）を選択できる。

（注）SPF で使用可能なセキュリティ種別の選択肢が増えたとしてもセキュリティの種類毎にローカルポートを増やしていく必要はない。

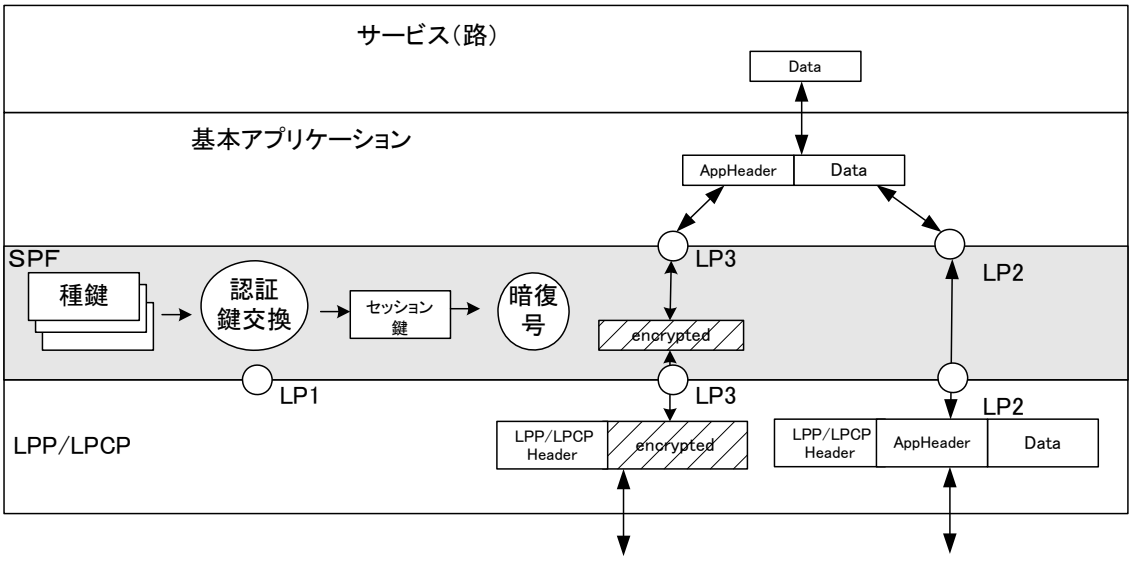

図 4.7-1 DSRC セキュリティプラットフォームの構造

セキュリティ種別で規定するセキュリティ処理の詳細は、本報告書の検討範囲外であり、別途規定されているものとする。

4.7.1.2　処理手順

路車間通信におけるセキュリティ処理は、接続処理時の『認証・鍵交換フェーズ』とその後のの送受信処理時の『サービスセッションフェーズ』において実行される。

認証・鍵交換フェーズでは、路車間の相互認証を行う。認証・鍵交換フェーズで行われる通信についてもデータの暗号化／復号化や MAC 生成／付与を行うことが可能である。また、認証・鍵交換フェーズの最初に路側から ITS 車載器に対して提供者識別子の通知と、路車間で利用するセキュリティ種別の交渉を行う。認証・鍵交換フェーズで通知された提供者識別子は、ITS 車載器側でのサービス種別・提供者の識別に用いられ、各基本アプリケーションにて定義されるアクセス制御機能を実現可能とする。また、認証・鍵交換フェーズで選択されたセキュリティ種別はサービスセッションに引き継がれる。

サービスセッションフェーズでは、認証・鍵交換フェーズで選択したセキュリティ種別と交換したセッション鍵を用いて、送受信データの暗復号処理を行う。なお SPF による暗号化範囲はアプリケーションデータ全体とし、アプリケーション毎には規定しない。また送信側は各トランザクション単位で、(1)暗号化のあり／なし、(2)データ認証のあり／なしを選択できる。サービスセッションフェーズにおいてセキュアポートを通して交換される PDU には、送信側でヘッダが付与され、受信側では、このヘッダによって(1)暗号化のあり／なし、(2)データ認証のあり／なしを判断できる。図 4.7-2 に DSRC-SPF の概略手順を示す。

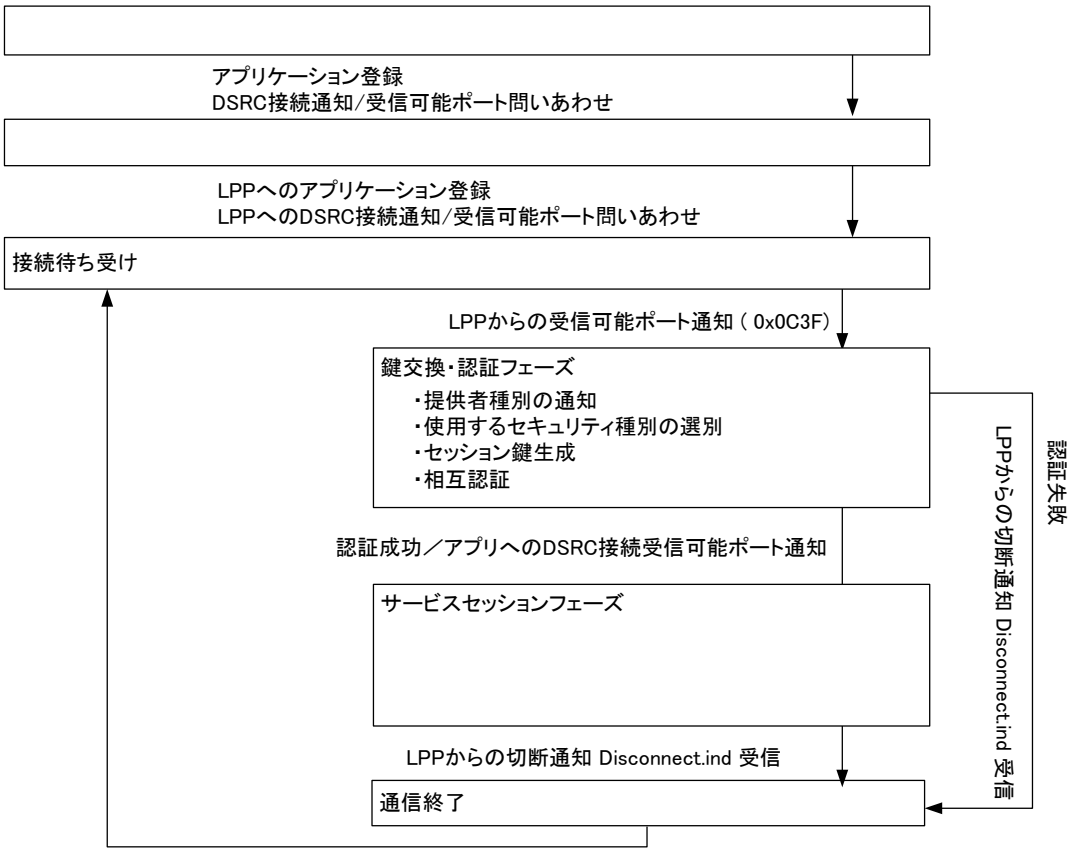

図 4.7-2　DSRC-SPF の概略手順

(1)認証・鍵交換フェーズの動作

認証・鍵交換フェーズでは、路側から初期接続時に提示されるセキュリティ種別及び提供者種別に応じた相互認証・鍵交換を行い、機器の相互認証とサービスセッションフェーズでの暗復号処理で使用するセッション鍵の生成を行う。

(2)サービスセッションフェーズの動作

サービスセッションフェーズでは、認証・鍵交換フェーズでネゴシエーションしたセキュリティ種別で指定されるセキュリティライブラリと認証・鍵交換フェーズで交換したセッション鍵を用いて、アプリケーションデータ(APP PDU)に対して暗号化・復号化処理を行う。以下にサービスセッションフェーズにおける SPF の動作について示す。

・送信時に基本アプリケーションから SPF に渡されたデータ（セキュアポートに対する送信）は、暗号化／データ認証の指示に従い暗号化／MAC 付加処理を行い、該当するコマンドを生成する。
・受信時に LPP から SPF に渡されたデータ（セキュアポートに対する受信）は、ヘッダの内容に応じて、復号化及びデータ認証処理を行う。
・暗号化・復号化に用いるセキュリティライブラリは認証・鍵交換フェーズでネゴシエーションしたセキュリティ種別のものを用いる。
・暗号化・復号化に用いるセッション鍵は認証・鍵交換フェーズで交換した鍵を用いる
・セキュリティ強度を調整するためのオプション機能が組み込まれている SPF において、認証・鍵交換フェーズ時に選択したオプションと矛盾する暗号化・データ認証の指示があった場合には、相手局へのデータ送信を行わず、そのトランザクションを破棄すること。

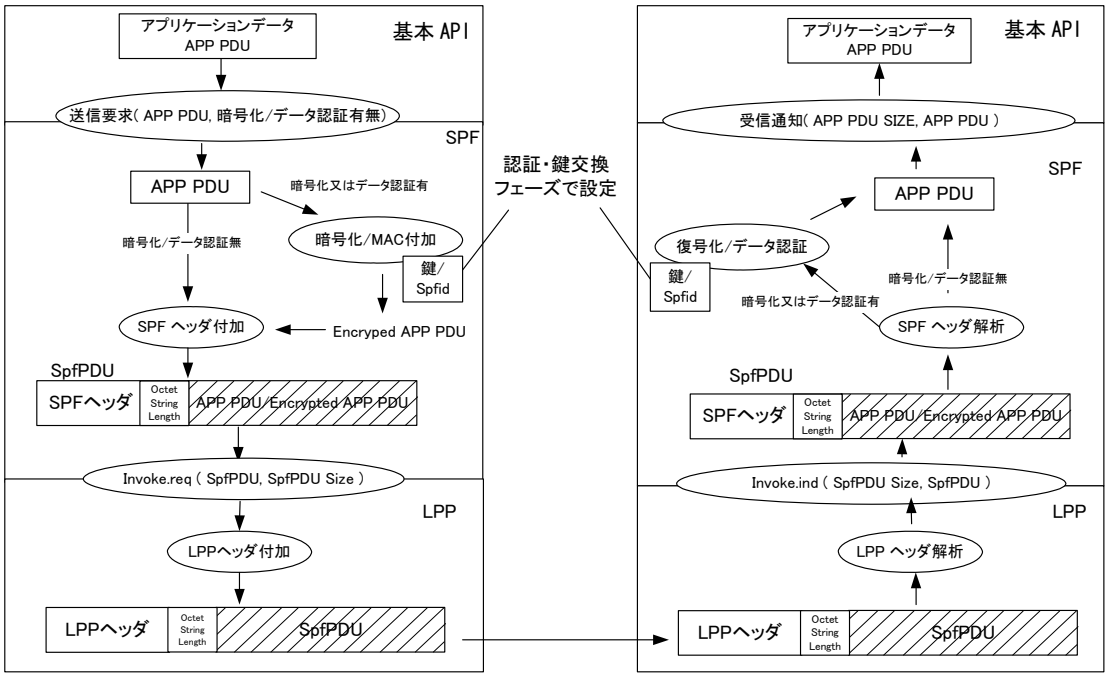

図 4.7-3　サービスセッションフェーズにおける暗号化/復号化処理の例

4.7.1.3　認証・鍵交換フェーズとサービスセッションフェーズの関係

・認証・鍵交換フェーズで選択されたセキュリティ種別はサービスセッションに引き継がれる。

・セキュリティ種別の中にはセキュリティ強度を調整するためのオプション機能が組込まれている場合がある。このような SPF のサービスセッションフェーズにおいては、認証・鍵交換フェーズ時に選択したオプションで利用可能なセキュリティ機能のみを使用すること。

・認証・鍵交換フェーズで取得した提供者識別子は各基本アプリケーションに引き継がれ、サービスセッションフェーズにてアクセス制御のために利用される。

・認証が完了するまでセキュアポートに対する送受信を廃棄する機能を有する

4.7.2　コマンド定義

4.7.2.1　認証・鍵交換フェーズ

(1)コマンド体系

認証・鍵交換フェーズで使用するコマンド(CertificationCommand)を以下に示す。なお、各コマンドの定義は、ASN.1 の PER(Packed Encoding Rules)に基づき表 4.7-1 に規定する。

表 4.7-1　CertificationCommand のコマンド体系図

1		2
versionIndex		majorVersion
		minorVersion
securityCommand	[0]authenticateCommand	[0]NegotiateRequest
		[1]NegotiateResponse
		[2]SetupMessageRequest
		[3]SetupMessageResponse
		[4-255] reserved
	[1-254]reserved	
	[255]obuDenialResponse	status
		supplementInfo

表 4.7-1 において背景を色づけしたコマンドは、そのうちのいずれかが選択されるもの(CHOICE 型、ENUMERATED 型で定義されているコマンド)である

(2)コマンド定義

1)AuthenticateCommand

AuthenticateCommand は、認証・鍵交換処理を行うために使用するデータを送受信する際に用いられる。AuthenticateCommand の構成を以下に示す。

表 4.7-2　AuthenticateCommand の構成

	7(MSB)	6	5	4	3	2	1	0
1	メジャーバージョン (1)				マイナーバージョン (0)			
2	セキュリティコマンド識別子　authenticateCommand(0)							
3	Authenticate コマンド識別子							
4	Authenticate コマンドのパラメータ							

(a)メジャーバージョン/マイナーバージョン

プロトコルのバージョンを格納する。現時点のバージョンはメジャーバージョンが 1、マイナーバージョンが 0。

(b)セキュリティコマンド識別子

AuthenticateCommand を示す識別子 authenticateCommand(0)を格納する。

(c)Authenticate コマンド識別子

Authenticate コマンドの種類を示す識別子を格納する。

(d)Authenticate コマンドのパラメータ

Authenticate コマンド識別子で指定される各コマンドのパラメータを格納する

以下に、各 Authenticate コマンドの詳細を示す。

a)NegotiateRequest

NegotiateRequest は、初期接続時にセキュリティ種別及び提供者種別などの情報を路側から提示するために使用する。パラメータとして、セキュリティ種別と提供者種別および路側付加情報からなるデータ(SpfRSUParameter) をリスト形式で用いる。SpfRSUParameter の構成は表 4.7-5 に示す。

b)NegotiateResponse

NegotiateResponse は、初期接続時に路側から提示されたセキュリティ種別の中から、車載側で選択したセキュリティ種別を路側システムに通知するために使用する。パラメータとして、セキュリティ種別と車載付加情報からなるデータ(SpfOBUParameter) を用いる。SpfOBUParameter の構成は表 4.7-7 に示す。

c)SetupMessageRequest

SetupMessageRequest は、SPF の認証・鍵交換のコマンドを路側システムから ITS 車載器へ送付する場合に使用する。パラメータとして、SPF の認証・鍵交換のコマンドを ASN.1 符号化規則における OCTET STRING の形式で用いる。

d)SetupMessageResponse

SetupMessageRequest は、SPF の認証・鍵交換のコマンドに対する応答を ITS 車載器から路側システムへ送付する場合に使用する。パラメータとして、SPF の認証・鍵交換のコマンドを ASN.1 符号化規則における OCTET STRING の形式で用いる

2)ObuDenialResponse

ObuDenialResponse は、ITS 車載器の異常状態を路側システムに通知するために使用する。ObuDenialResponse の構成を以下に示す。

表 4.7-3 ObuDenialResponse の構成

	7(MSB)	6	5	4	3	2	1	0
1	メジャーバージョン (1)				マイナーバージョン (0)			
2	セキュリティコマンド識別子 ObuDenialResponse(255)							
3	車載器異常状態識別子							
4	車載器異常状態付加情報の長さ							
	車載器異常状態付加情報の内容							

(a)メジャーバージョン/マイナーバージョン

プロトコルのバージョンを格納する。現時点のバージョンはメジャーバージョンが 1、マイナーバージョンが 0。

(b)セキュリティコマンド識別子

ObuDenialResponse を示す識別子 ObuDenialResponse(255)を格納する。

車載器異常状態識別子

ITS 車載器の異常状態を示す識別子を格納する。車載器異常状態識別子の一覧を表 4.7-4 に示す。

(c)車載器異常状態付加情報の長さ

後続する車載器異常状態付加情報のデータ長を指示する。単位はオクテット。

(d)車載器異常状態付加情報の内容

車載器異常状態付加情報の内容で不定長データを格納する。

表 4.7-4　車載器異常状態識別子の一覧

ステータスコード	意味
0	使用せず
1	セキュリティ種別エラー
2-3	将来拡張用
4	バージョン不一致
5	SPF 内部エラー
6-15	将来拡張用
16	異常なサービスプリミティブ（解釈不能）
17	認証未完了
18	未対応の提供者識別子
19-254	将来拡張用
255	その他の ITS 車載器内部エラー

(3)パラメータ

認証・鍵交換フェーズの各コマンドで利用されるパラメータを以下に示す。

1)SpfRSUParameter

SpfRSUParameterはDSRC路側無線装置からITS車載器に対して使用可能なセキュリティ種別、提供者種別などの情報を通知するためのパラメータで、NegotiateRequestコマンドにおいてリスト形式で用いられる。以下にこのパラメータの構成と各フィールドの内容を示す。

表 4.7-5　SpfRSUParameterの構成

	7(MSB)	6	5	4	3	2	1	0
1	preamble	fill(0)			SPF識別子			
2	提供者識別子							
3								
4								
5	SPF路側付加情報の長さ							
	SPF路側付加情報の内容							

(a)preamble

SPF付加情報が付加されているかどうかを識別する識別子

(b)SPF識別子（SpfId）

セキュリティ種別を表す識別子を格納する。SPF識別子の一覧を表 4.7-6に示す。

表 4.7-6　SPF識別子の一覧

値	セキュリティ種別
0	ORSE
1..15	予約

a)提供者識別子

提供者識別子には、サービス提供者の種別を表す識別子を格納する。提供者識別子の定義は表 4.7-8に示す。

b)SPF路側付加情報の長さ

後続するSPF路側付加情報のデータ長を指示する。単位はオクテット。この長さ識別子のエリアサイズはASN.1符号化規則に従い拡張する

c)SPF 路側付加情報の内容

SPF 路側付加情報の内容で不定長データを格納する。SPF 路側付加情報の詳細については Spfid 毎に別途規定する。

2)SpfOBUParameter

SpfOBUParameter は DSRC 路側無線装置から提示された使用可能なセキュリティ種別から、実際に使用するセキュリティ種別を DSRC 路側無線装置に通知するためのパラメータで、NegotiateResponse コマンドで用いられる。以下にこのパラメータの構成と各フィールドの内容を示す。

表 4.7-7　SpfOBUParameter の構成

	7(MSB)	6	5	4	3	2	1	0
1	preamble	fill (0)			SPF 識別子			
2	SPF 車載付加情報の長さ							
	SPF 車載付加情報の内容							

(a)preamble

SPF 付加情報が付加されているかどうかを識別する識別子

(b)SPF 識別子 (SpfID)

NegotiateRequest コマンドによって ITS 車載器が選択したセキュリティ種別を表す識別子を格納する。

(c)SPF 車載付加情報の長さ

後続する SPF 車載付加情報のデータ長を指示する。単位はオクテット。この長さ識別子のエリアサイズは ASN.1 符号化規則に従い拡張する

(d)SPF 車載付加情報の内容

SPF 付加情報の内容で不定長データを格納する。SPF 車載付加情報の詳細については Spfid 毎に別途規定する。

3)提供者識別子

サービス提供者の種別を表す識別子である。鍵を区別するグループ識別子と鍵を区別しないサービス識別子から構成される。

表 4.7-8　サービス提供者識別子の構成

	7(MSB)	6	5	4	3	2	1	0
	グループ識別子							
	サービス識別子							

(a)グループ識別子

鍵を共有するグループを表す識別子。上位 4 ビットは使用するセキュリティ種別を表す SPF 識別子と同じ値を使用する。

(b)サービス識別子

提供されるサービスの種別を表す識別子。詳細については別途定義する。識別を行わない場合は(0)を使用する。

表 4.7-9　グループ識別子の一覧

値	グループ種別
0	公共サービス 1 (SpdID = ORSE)
1	民間サービス 1 (SpdID = ORSE)
2..15	予約 (SpdID = ORSE)
16..255	予約

(4)データ構成定義

1)CertificationCommand

CertificateCommand の定義を以下に示す。

```
CertificateCommand ::= SEQUENCE {
    versionIndex            Version,
    securityCommand         SecurityCommand
}

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

SecurityCommand ::= CHOICE {
    authenticateCommand     [0]     AuthenticateCommand,
    reserved                [1-254] NULL,           --将来拡張用
    obuDenialResponse       [255]   ObuDenialResponse
}
```

2)AuthenticateCommand

AuthenticateCommand の定義を以下に示す。

```
AuthenticateCommand ::= CHOICE {
    NegotiateRequest        [0]     SpfRsuParameterList,
    NegotiateResponse       [1]     SpfObuParameter,
    SetupMessageRequest     [2]     OCTET STRING,
    SetupMessageResponse    [3]     OCTET STRING,
    reserved                [4-255] NULL
}

SpfRsuParameterList ::= SEQUENCE(0..255) OF SpfRsuParameter

SpfRsuParameter ::= SEQUENCE {
    fill                    BIT STRING(SIZE(3)),        -- 0
    spfId                   SpfId,                      -- SPF 識別子
    serviceId               SpfProviderId,              -- 提供者種別
    supplementInfo          OCTET STRING OPTIONAL       -- 初期化データ等
}
```

```
SpfObuParameter ::= SEQUENCE {
    fill                    BIT STRING(SIZE(3)),            -- 0
    spfid                   SpfId,
    supplementInfo          OCTET STRING    OPTIONAL    -- 初期化データ等
}

SpfId ::= INTEGER{
    ORSE            (0)
    -- SpfId の値 1 から 15 は予約とする
} (0..15)

SpfProviderId ::= SEQUENCE {
    group                   GroupID,        -- 上位 4 ビットは SpfId と同値
    service                 INTEGER(0..65535)       -- デフォルト値は(0)
}

GroupID ::= INTEGER{
      orse_public           (0),
      orse_private0         (1)
      -- GroupID の値 2 から 255 は予約とする
} ( 0.. 255 )
```

3)ObuDenialResponse

ObuDenialResponse の定義を以下に示す。

```
ObuDenialResponse ::= SEQUENCE {
    status              INTEGER(0..255),
    supplementInfo      OCTET STRING(SIZE(0..127))
}
```

4.7.2.2　サービスセッションフェーズ

(1)コマンド定義

サービスセッションフェーズで使用するコマンド（SpfPDU）を以下に示す。SpfPDU は LPP の SDU にマッピングされる。なお、コマンドは ASN.1 の PER(Packed Encoding Rules) に基づき規定する。

表 4.7-10　SpfPDU の形式

(MSB)	7	6	5	4	3	2	1	0
0	dummy						encrypt	dataAuth
1	APP PDU/Encryped APP PDU の長さ							
	APP PDU/ Encryped APP PDU の本体							

(a)encrypt フィールド

encrypt フィールドには暗号化の有無を表す値を格納する。0 が暗号化無し、1 が暗号化有りを表す

(b)dataAuth フィールド

dataAuth フィールドにはデータ認証処理の有無を表す値を格納する。0 がデータ認証無し、1 がデータ認証有りを表す。

(2)データ構成定義

```
SpfPDU ::= SEQUENCE {
        spfHeader               SpfHeader,
        spfSdu                  OCTET STRING
}

SpfHeader ::= SEQUENCE {
          res                   BIT STRING(6), -- 常に 0
        encrypt                 BOOLEAN,       -- 暗号化の有無
        dataAuth                BOOLEAN        -- データ認証の有無
}
```

4.7.3　他規格との関連

4.7.3.1　認証・鍵交換フェーズ

認証・鍵交換フェーズで使用する他の DSRC 関連規格との関係は以下の通りである。

表 4.7-11　認証・鍵交換フェーズにおける他の DSRC 関連規格のパラメータ

番号	規格		項目	内容
1	ARIB STD-T75		AID	18
2	ARIB STD-T88	ELCP	アクセス点識別子	LPCP(1)
3		LPCP	ローカルポート番号	0x0C3F (案)
4	LPP		トランザクション種別	リクエスト・レスポンス型(1)

4.7.3.2　サービスセッションフェーズ

サービスセッションフェーズで使用する他の DSRC 関連規格との関係は以下の通りである。

表 4.7-12　サービスセッションフェーズにおける他の DSRC 関連規格のパラメータ

番号	規格		項目	内容
1	ARIB STD-T75		AID	18
2	ARIB STD-T88	ELCP	アクセス点識別子	LPCP(1)
3		LPCP	ローカルポート番号	0x0C20～0x0C3E アプリケーションが指定する値による
4	LPP		トランザクション種別	アプリケーションが指定する値による

4.7.4　シーケンス例

4.7.4.1　認証・鍵交換フェーズ

以下に、認証・鍵交換フェーズにおける通信シーケンスを示す。シーケンス図において、Authpath*1*～Authpath*n* は Spfid で規定された認証・鍵交換コマンドメッセージを示す。なお、Authpath*1*～Authpath*n* の詳細については本報告書の検討範囲外であり、セキュリティ種別毎に別途規定されているものとする。

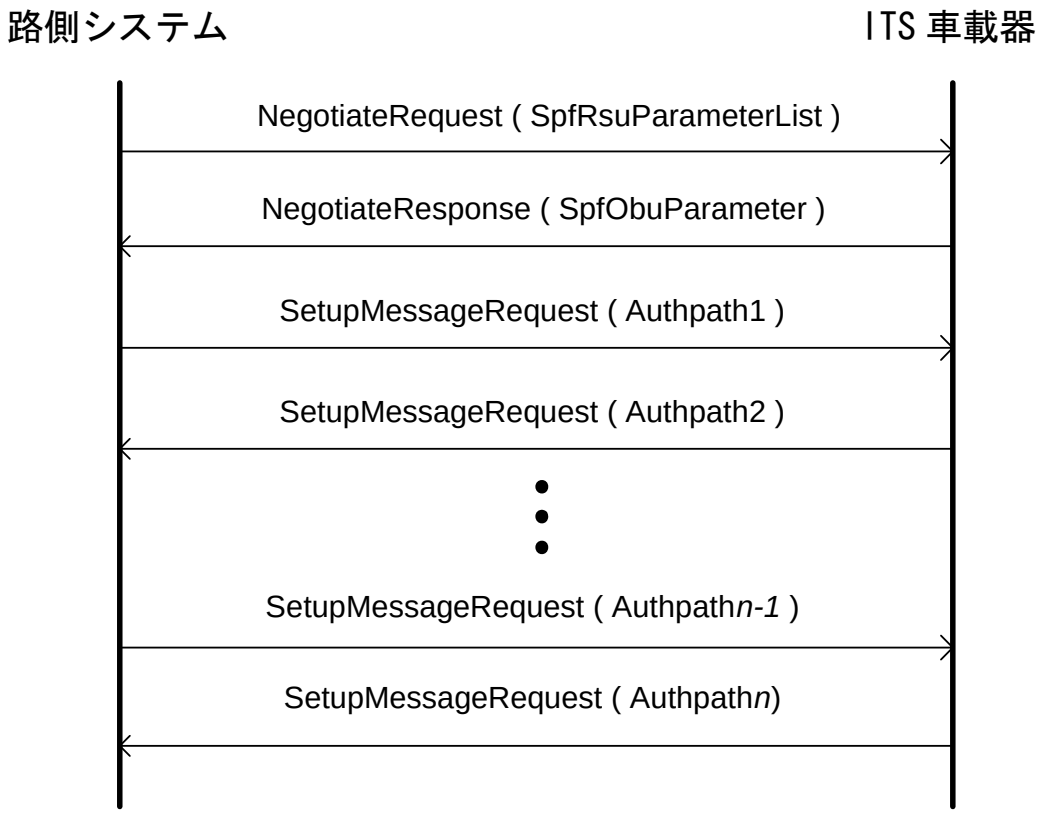

図 4.7-4　認証・鍵交換フェーズにおける処理シーケンス例

4.7.4.2　サービスセッションフェーズ

以下に、セッションフェーズにおける通信シーケンスを示す。

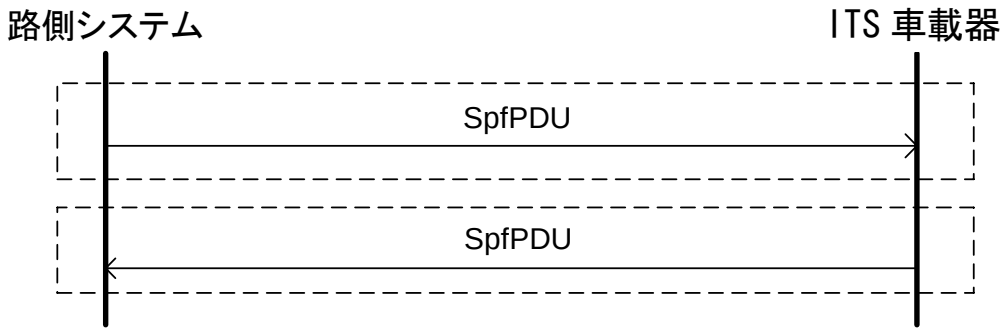

図 4.7-5　サービスセッションフェーズにおける通信シーケンス例

4.7.5　ローカルポート番号一覧

SPF を使用しない場合、基本 API のローカルポート番号は、従来の 0x0C00～0x0C1F のエリアを通常ポートエリアとしてそのまま使用することとし、さらに、SPF 用として 0x0C20～0x0C3F（案）のエリアを別途セキュアポートとして使用する。セキュアポートエリアにおける基本 API の分類、配置については、通常ポートエリアにおける基本 API の分類、配置に準ずるものとする。また 0x0C3F は DSRC セキュリティプラットフォームの管理ポートとし、認証・鍵交換フェーズにて使用するものとする。表 4.7-13 に基本 API のローカルポート番号の一覧を示す。

表 4.7-13　基本 API のローカルポート番号

通常ポート	セキュアポート	アプリケーション	備考
0x0C00	0x0C20	車載器 ID 通信アプリケーション	＜情報の流れ＞ 路←車
0x0C01～ 0x0C07	0x0C21～ 0x0C27	将来拡張用	
0x0C08	0x0C28	車載器基本指示アプリケーションに採番済み	＜情報の流れ＞ 路→車
0x0C09	0x0C29	車載器指示応答アプリケーション	
0x0C0A	0x0C2A	プッシュ型情報配信アプリケーション	
0x0C0B～ 0x0C0F	0x0C2B～ 0x0C2F	将来拡張用	
0x0C10	0x0C30	IC カードアクセスアプリケーション	＜情報の流れ＞ 路←→車 カード利用
0x0C11～ 0x0C17	0x0C31～ 0x0C37	将来拡張用	
0x0C18	0x0C38	メモリアクセスアプリケーション	＜情報の流れ＞ 路←→車 メモリ利用
0x0C19～ 0x0C1F	0x0C39～ 0x0C3E	将来拡張用	
-	0x0C3F	DSRC セキュリティプラットフォーム管理ポート	

4.7.6　SPF を利用する基本 API の留意点

4.7.6.1　アプリケーション内個別セキュリティとの関係

アプリケーション内個別セキュリティ属性と共通 SPF は独立して利用可能である。従って、セキュアポートでは、SPF 単独及び SPF とアプリケーション内セキュリティを二重に実施することも可能である。共通 SPF のみ使用する場合、アプリケーション内ではセキュリティなし(平文)として扱い、SPF で暗号/復号を実施すること。

4.7.6.2　SPF を利用した ITS 車載器のアクセス制御

各アプリケーションのセキュアポートは、SPF 認証・鍵交換フェーズが完了後のみ、通信が可能となることを想定している。

(1)車載器 ID 通信アプリケーション

車載器 ID 通信アプリケーションにおいて、SPF を利用して車載器 ID を送信可能とする場合、車載器 ID の状態において spf(TRUE(1))に設定すること。メンテナンスコマンドのアクセス制御として SPF を利用する場合、通常ポートからのメンテナンスコマンドは禁止とし、セキュアポートからのみメンテナンスが可能とすること(ただし、相互確認試験等の場合は除く)。

(2)IC カードアクセスアプリケーション

IC カードアクセスアプリケーションにおいては、通常ポートからのアクセスは禁止とする(ただし、相互確認試験等の場合は除く)。

(3)プッシュ型情報配信アプリケーション

プッシュ型情報配信アプリケーションにおいては、セキュアポートが通信可能となった時点で、クライアント情報通知(ClientInformation)を通知すること。なお、通常ポートと併用する場合、ClientInformation はポート単位とし、セキュアポートと通常ポートで受信可能なコンテンツの異なる設定が可能である。

(4)車載器メモリアクセスアプリケーション

車載器メモリアクセスアプリケーションにおいて、パスワード付きコマンドを使用する場合は、セキュアポートを使用することを推奨する。

4.7.6.3　車載器 ID 通信アプリケーションに関する実装例と留意事項

車載器 ID 通信アプリケーションのアプリケーション内セキュリティについて、DSRC-SPF（で使用されているライブラリ）を採用する際の例を示す。またアプリケーション内セキュリティを取り扱わない場合、取り扱う場合の留意点について示す。なおセットアップ方法は本報告書の範囲外であり、別途規定されるものとする。

(1)アプリケーション内セキュリティとして DSRC-SPF を採用した場合の例

車載器ID通信アプリケーションのアプリケーション内セキュリティとしてDSRC-SPFを採用した場合について例示する。

1)アプリケーション内セキュリティと DSRC-SPF の位置と機能

DSRC-SPF と車載器 ID 通信アプリケーションのアプリケーション内セキュリティの位置を図 4.7-6 に示す。DSRC-SPF は機器間の認証や暗号通信を目的としており、事業者ごとに異なるアクセス制御を実施できない。

それに対してアプリケーション内セキュリティは、その実施方法や鍵の発行が事業者ごとに選択、決定できるため、事業者ごとに異なるアクセス制御や暗号通信を実施できる。またアプリケーション内セキュリティとして DSRC-SPF（ライブラリ）を利用することもできる。このとき、ITS 車載器にセットアップされているセキュリティプロファイルを用いて、使用する SPF や SPF に用いるパラメータを選択する。

セキュリティプロファイルとは、SPF の種別、SPF に用いるパラメータに関するデータを指す。セキュリティプロファイルは取得者 ID と紐付けされており、このセキュリティプロファイルに従って使用する SPF や SPF に用いるパラメータが選択される。セキュリティプロファイルは、SPF 毎に別途規定されることとする。

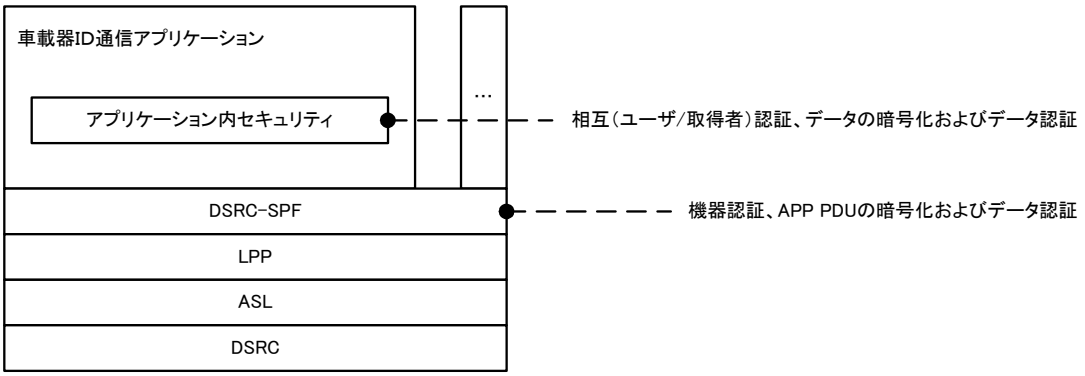

図 4.7-6　アプリケーション内セキュリティと DSRC-SPF の位置

2) 具体的仕様

車載器 ID 通信アプリケーションのアプリケーション内セキュリティとして DSRC-SPF を採用した場合の具体的な仕様について解説する。

(a)コマンドの形式

ここでは AuthenticateCommand 型変数（authPath1～authPath4）との詳細な定義と SeconIDRequest 型変数の使用方法について解説する。

a) authPath1(NegotiateRequest)

authPath1 には、DSRC-SPF の NegotiateRequest が格納される。

表 4.7-14　authPath1 の形式

	7(MSB)	6	5	4	3	2	1	0
1	version				fill(0)			
2	コマンドタイプ authenticateCommand(0)							
3	操作タイプ authPath1(0)							
4	NegotiateRequest の長さ							
	NegotiateRequest							

b) authPath2(NegotiateResponse)

authPath2 には、DSRC-SPF の NegotiateResponse が格納される。

表 4.7-15　authPath2 の形式

	7(MSB)	6	5	4	3	2	1	0
1	version				fill(0)			
2	コマンドタイプ authenticateCommand(0)							
3	操作タイプ authPath2(1)							
4	NegotiateResponse の長さ							
	NegotiateResponse							

c) authPath3 (SetupMessageRequest)

authPath3 には DSRC-SPF の SetupMessageRequest が格納される。

表 4.7-16　authPath3 の形式

	7(MSB)	6	5	4	3	2	1	0
1	version				fill(0)			
2	コマンドタイプ authenticateCommand(0)							
3	操作タイプ authPath3(2)							
4	SetupMessageRequest の長さ							
	SetupMessageRequest							

d)authPath4 (SetupMessageResponse)

authPath4 には DSRC-SPF の SetupMessageResponse が格納される。

表 4.7-17　authPath4 の形式

	7(MSB)	6	5	4	3	2	1	0
1	version				fill(0)			
2	コマンドタイプ authenticateCommand(0)							
3	操作タイプ authPath4(3)							
4	SetupMessageResponse の長さ							
	SetupMessageResponse							

e)SecondIDResponse 型変数の使用方法

```
SecondIDResponse::=SEQUENCE{
  encryptionAlgorithmId  INTEGER(0..255),
                --ID 秘匿用暗号アルゴリズム(アプリケーション内セキュリティ用)
  keyNumber              INTEGER(0..255),
                --ID 秘匿用鍵番号（アプリケーション内セキュリティ用）
  encryptedId            OCTET STRING
                --暗号化 ID 情報（アプリケーション内セキュリティ用）
}
```

encryptionAlgorithmId、keyNumber の値は SPF 毎に別途規定されることとする。encryptedId には DSRC-SPF の SpfPDU を格納する。

f)否定応答 status

アプリケーション内セキュリティ用として使用する否定応答 status を表 4.7-18 に示す。表中のステータスコードから 32 を引いた値が DSRC-SPF のステータスコードと一致する。ただし「認証未完了」と「その他の ITS 車載器内部エラー」についてはそれぞれ 32、255 を使用する。

表 4.7-18　アプリケーション内セキュリティ用の否定応答 status の内容

ステータスコード	意味
33　(32+1)	セキュリティ種別エラー
34-35	将来拡張用
36　(32+4)	(DSRC-SPF の) バージョン不一致
37　(32+5)	SPF 内部エラー
38-47	将来拡張用
48　(32+16)	異常なサービスプリミティブ
49	将来拡張用
50　(32+18)	未対応の提供者識別子
51-63	将来拡張用

(b)シーケンス例

アプリケーション内セキュリティとして DSRC-SPF を採用する場合のシーケンス例を図 4.7-7 に示す。

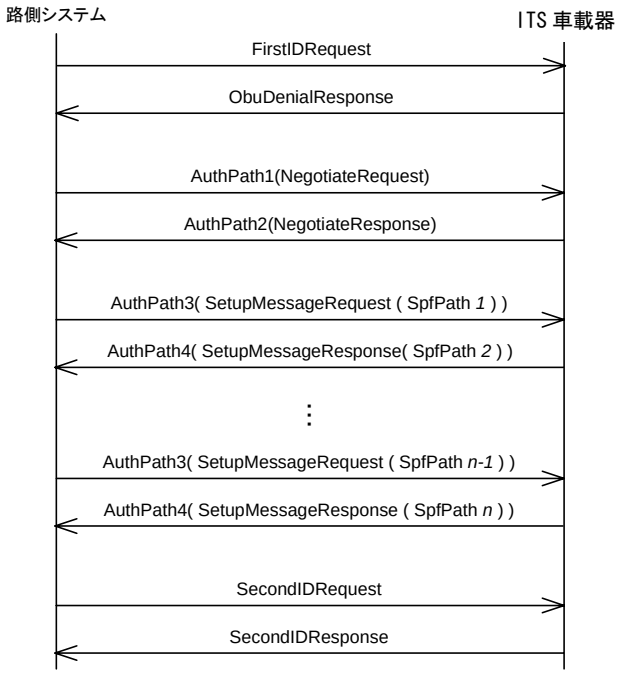

図 4.7-7　シーケンス例

(c)アプリケーション内セキュリティとして DSRC-SPF を採用した場合の ID 取得手順

アプリケーション内セキュリティとして DSRC-SPF を採用した場合の手順を示す。

①DSRC 路側無線装置から ITS 車載器に firstIDRequest を通知する。

②ITS 車載器は、firstIDRequest を受信すると、ID 登録情報を参照し、以下の条件で firstIDResponse もしくは obuDenialReponse を DSRC 路側無線装置に通知する。

a)取得者 ID に対応する車載器 ID の状態が plaintextIDRefusal(FALSE(0))の場合は、firstIDResponse を DSRC 路側無線装置に通知する。

plaintextIDRefusal(TRUE(1))の場合は、obuDenialResponse にて、status(32)「平文送信拒否、認証失敗、未認証」を通知する。

b)ITS 車載器に全く車載器 ID が登録されていない場合、status(12)「登録車載器 ID なし」の ObuDenialResponse を通知する。

c)当該取得者に対応する車載器 ID が登録されていない場合、obuDenialReponse にて status(2)「取得者 ID に対応する登録車載器 ID なし」を通知する。

③②a)の処理によって、ITS 車載器から obuDenialResponse にて status(32)を受信した DSRC 路側無線装置は、authPath1(NegotiateRequest)により DSRC-SPF の使用可能なパラメータリストを ITS 車載器に通知する。

④ITS 車載器は、authPath1(NegotiateRequest)を受信すると、firstIDRequest で指定された取得者 ID に対応するセキュリティプロファイルを参照し、以下の条件で authPath2(NegotiateResponse)もしくは obuDenialResponse を DSRC 路側無線装置に通知する。

a) authPath1(NegotiateRequest)で通知されたパラメータリストの中から使用するパラメータを選択し、authPath2(NegotiateResponse)にて通知する。

b) authPath1(NegotiateRequest)内に使用可能なパラメータがない場合、obuDenialResponse にて、status(33)「セキュリティ種別エラー」を通知する。

⑤④a)の処理によって、ITS 車載器から authPath2(NegotiateResponse)を受信した DSRC 路側無線装置は、authPath2(NegotiateResponse)内から ITS 車載器が指定したパラメータを取得する。

⑥DSRC 路側無線装置は ITS 車載器に指定されたパラメータを用いてリクエストを生成し、authPath3(SetupMessageRequest)にて ITS 車載器に通知する。

⑦authPath3(SetupMessageRequest)を受信した ITS 車載器は、指定したパラメータを用いてレスポンスを生成し、authPath4(SetupMessageResponse)にて DSRC 路側無線装置に通知する。

⑧以降、SPF のシーケンスが終了するまで⑥、⑦の処理を繰り返す。

⑨SPF のシーケンスが終了した後、DSRC 路側無線装置は ITS 車載器に secondIDRequest を通知する。

⑩ITS 車載器は、secondIDRequest を受信すると、ID 登録情報を参照し、以下の条件で secondIDResponse もしくは obuDenialReponse を DSRC 路側無線装置に通知する。

a) 取得者 ID に対応する車載器 ID の状態と④～⑧の処理による結果とが一致する場合、secondIDResponse を DSRC 路側無線装置に通知する。

b) 取得者 ID に対応する車載器 ID の状態と④～⑧の処理による結果とが一致しない場合、obuDenialResponse にて、status(32)「平文送信拒否、認証失敗、未認証」を DSRC 路側無線装置に通知する。

(d)アプリケーション内セキュリティを取り扱わない場合の留意点

アプリケーション内セキュリティを取り扱わない ITS 車載器が、以下のコマンドを受信した場合、status(32)の ObuDenialResponse を返信する。

・AuthenticateCommand

・secondIDRequest

ID の状態(IDCondition)は、アプリケーション内セキュリティを使用しない値を用いる。

(e)アプリケーション内セキュリティを取り扱う場合の留意点

アプリケーション内セキュリティは、事業者の責任において適切に選択もしくは決定するものとする。以下、アプリケーション内セキュリティを取り扱う場合の留意点を以下に示す。

a)ID の状態

ID の状態の ciphertextIDRefusal フィールドおよび mutualAuthentication フィールド(表 3.5-1)は、事業者の方針に従って暗号化/認証の要否を定め設定する。設定を DSRC 通信で実施する場合は、メンテナンスコマンドの ID 状態変更要求コマンドを使用して実施する。ほかの手段を使用することは妨げない。

b)データ認証

車載器 ID のデータ認証が必要な場合は、ObuID の mACForOriginalText(3.5.3 データ構成定義)を用いる。

c)AutheticateCommand

実装するアプリケーション内セキュリティの仕様に基づき、AuthenticateCommand (3.5.3 データ構成定義の IDAcquisitionCommand)を用いて路車間で必要な情報の交換・相互認証を行う。

d)SecondIDResponse

SecondIDResponse の内容は、AuthenticateCommand にて実施したセキュリティに必要な情報の交換により確定する。

e)車載器否定応答

obuDenialResponse で用いる status の 32～63 の定義(表 4.6-9)は、アプリケーション内セキュリティ用である。アプリケーション内セキュリティの仕様に合わせて 33～63 を使用する。

・業者およびアプリケーション内セキュリティがそれぞれ複数存在する場合

事業者が複数のアプリケーション内セキュリティを使い分けるケース、逆に複数の事業者が同一のアプリケーション内セキュリティを共用する場合が想定される。

前者の場合、ITS 車載器の機能として、各セキュリティ間で適切な Firewall が施されていること、取得者 ID と複数のアプリケーション内セキュリティの対応を管理する機能を有すること、AuthenticateCommand にてアプリケーション内セキュリティの選択の手順を規定することが望ましい。具体的な仕様はアプリケーション内セキュリティ毎に規定することとする。

後者の場合、ITS 車載器の機能としてアプリケーション内セキュリティと複数の取得者 ID の対応を管理する機能を有することが望ましい。