DSRCシステムにおけるセキュリティ技術

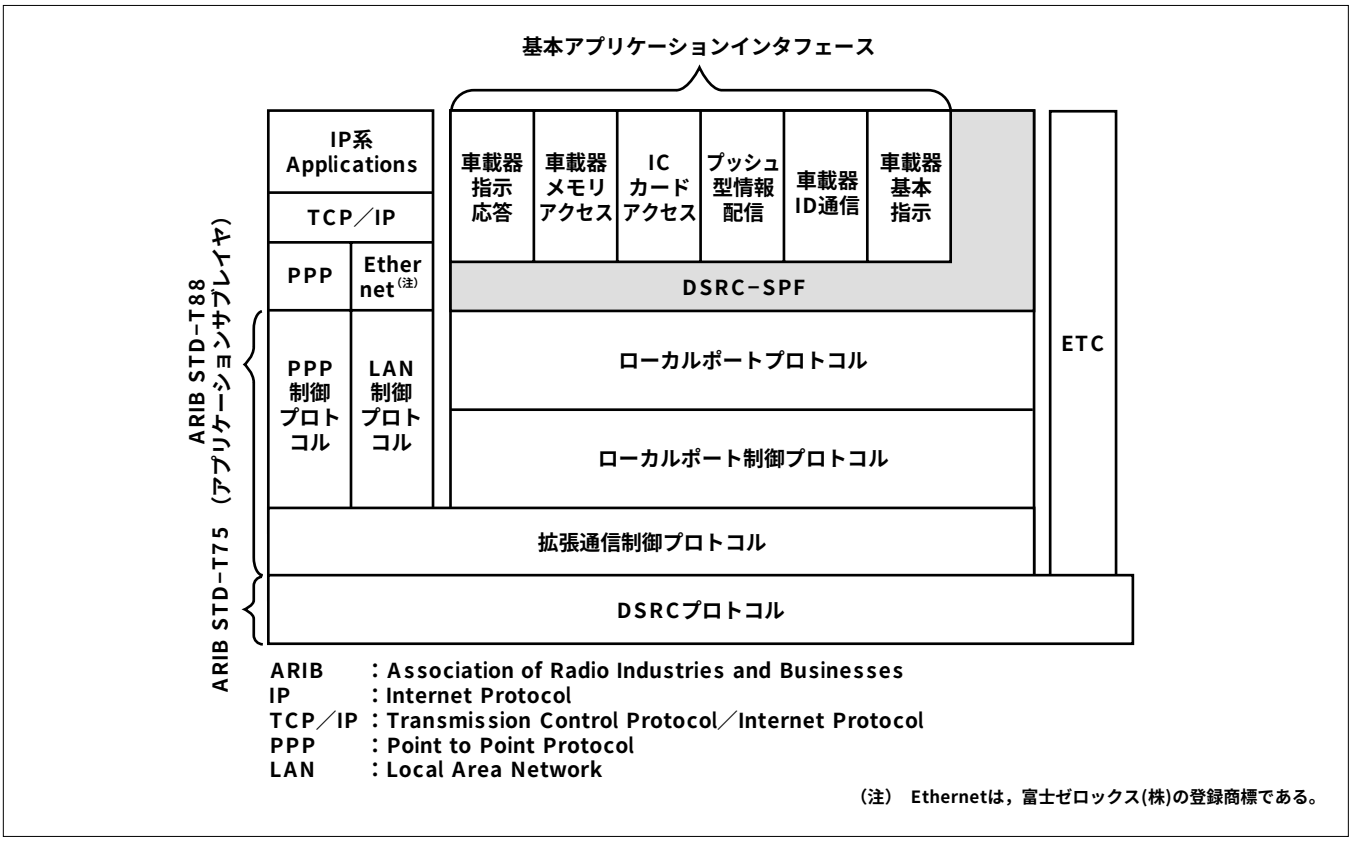
三澤　学*　　小泉　薫†
伊川雅彦**
岡　賢一郎***

Security Technology for DSRC Systems

Manabu Misawa, Masahiko Ikawa, Kenichiro Oka, Kaoru Koizumi

要　旨

DSRCシステム(Dedicated Short-Range Communication System)とは，車両に搭載された車載器と道路に設置された路側機とが通信を行うことで多様なサービスを提供するシステムである。ETC(Electronic Toll Collection System：有料道路自動料金支払いシステム)はDSRCシステムの一つのサービスとしてすでに運用され，利用率70%を超えるほどに普及している(2008年１月国土交通省)。ETC以外のサービスとしては，駐車場自動入退場，ガソリンスタンド自動決済，各種情報提供等が開始されており，DSRCシステムは，ITS(Intelligent Transport Systems)の中核システムの一つとして位置付けられている。DSRCシステムのプロトコルは，路側機－車載器間の無線インタフェースについて規定した(社)電波産業会規格ARIB STD-T75，同規格のDSRCプロトコルの通信機能を補完し複数アプリケーションの実行を可能にするARIB STD-T88(アプリケーションサブレイヤ)，各アプリケーションに対してセキュリティ機能を提供するDSRC-SPF(Security PlatForm)，DSRCシステムで必要とされる基本機能を定義した基本アプリケーションインタフェースで構成される。DSRC-SPFは多種の認証プロトコルに対応可能で，上位のアプリケーションに対して選択可能なセキュリティ機能を提供する柔軟なプロトコルである。



DSRCシステムのプロトコル構成

DSRCのプロトコル構成を示す。DSRCシステムのセキュリティ機能を担うDSRC-SPFは，アプリケーションサブレイヤのローカルポートプロトコルの上位に位置する。DSRC-SPFは車載器－路側器間の相互認証と基本アプリケーションインタフェースのプロトコルデータユニットの暗号化／復号，MAC(Message Authentication Code)生成／検証を行う。

*情報技術総合研究所　**先端技術総合研究所　***姫路製作所　†鎌倉製作所