特集　車載情報プラットフォームにおけるセキュリティの研究開発*

R&D of In-vehicle Infomation Platform Security

柳川博彦　Hirohiko YANAGAWA
高橋寿平　Juhei TAKAHASI

Next generation in-vehicle platforms are required so that information can be utilized through various onboard communication media and portable electronic equipment can be connected. The security system for their in-vehicle information platforms has been studied.

Various architecture of in-vehicle platforms have been compared, mainly PLANETS (Platform for Automotive info NET System) that was proposed by JSK in 2000, in terms of their degree of protection against unlawful threats and costs.

Using PLANETS architecture, which provides a high level of protection against threats, concrete examples of application and threats in AMI-C message sets have been studied and the specified security requirements have been tabulated. Furthermore advantages and disadvantages of two kinds of security function layouts for the chosen in-vehicle information platforms have been studied. One is distributed to two gateways and the other is centralized to one gateway.

Key words : In-vehicle platform, Security, Gateway, AMI-C, Message sets, Protection

１．はじめに

ITSの進展とともに，車両に携帯電話，デジタル放送，狭域通信（DSRC）等の，様々な通信媒体が搭載されつつある．今後，通信インフラと協調した最適なITS社会を築くためには，自動車において，乗員及び車両に必要な情報を常に利用可能にする新しい仕組みを構築する必要がある．JSK（自動車走行電子技術協会）では，2000年度に，今後想定されている新しい通信媒体に対応し，シームレスにITSアプリケーションを利用可能にする車載情報プラットフォームの開発を行った.[1)]

しかしながら，車両の安全性を確保しつつ，車外ネットワークと既存の制御系LANを接続するためには，インタフェースとなる車載情報プラットフォームの構築とともに，車載情報プラットフォームにおけるセキュリティの仕組みも同時に構築する必要がある．このような背景の中，JSKでは，2001年度に，上記問題を解決するために，車載情報プラットフォームで実現すべきセキュリティの要件及び仕組みを検討したので報告する．なお，本研究は，経済産業省から受託した「ITSの規格化事業」の一環として実施したものである．

２．車載情報プラットフォームのコンセプト

JSKが2000年度に提案した車載情報プラットフォームは，将来の通信環境への対応と車載機器の互換性や相互運用を目指して開発したもので，下記のような特徴を有している．

（１）車載機器の特性及び自動車メーカの車載機器プラットフォームに対する考え方を継承し，エンジンやブレーキを制御する機器が接続される「制御系ネットワーク」，オーディオ等のビルトイン機器を接続する「OEM情報系ネットワーク」，サードパーティーの持ち込み機器を接続する「OPEN情報系ネットワーク」と，ネットワーク間を接続する二つのゲートウェイ（制御系ゲートウェイ，情報系ゲートウェイ）によるシステム構成とする．

（２）OEM及びOPENネットワークはマルチメディア通信が可能なIDB-M（ITS Data Bus for Multimedia）とし，TCP/IP，UDP/IPを共通の上位プロトコルとする．

（３）車載機器の増設時や車内に持ち込まれたモバイル情報機器の操作環境が構築できるPlug & Playシステムの実現を目指す．

PLANETSにおけるシステム構成概念図をFig. 1に示す．Fig. 1に示すように，二つのゲートウェイを有するアーキテクチャが特徴となっている．

＊ 2002年12月19日　原稿受理

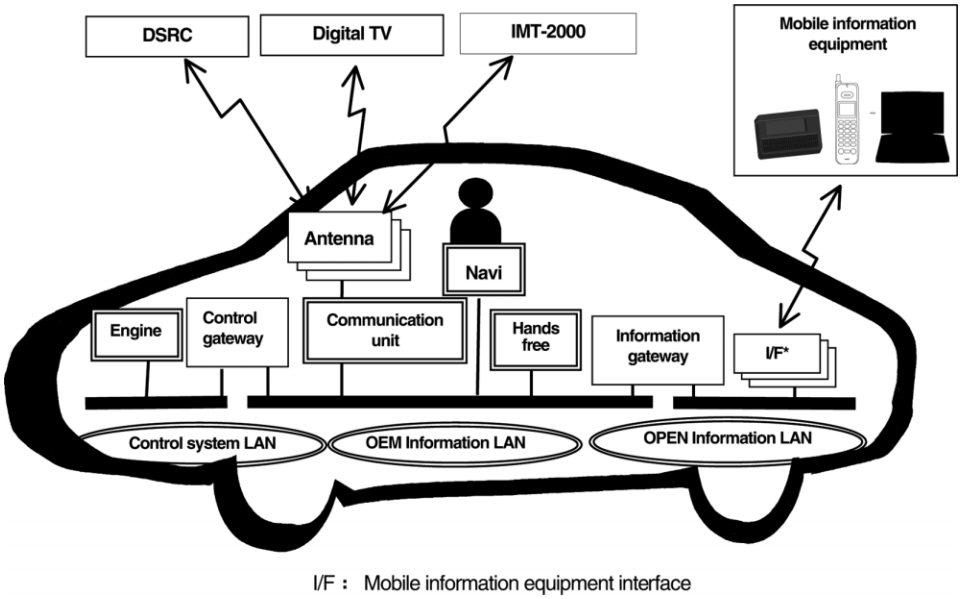

Fig. 1 Conceptual system diagram of in-vehicle information platform

３．アーキテクチャの比較検討

ITSの様々なアプリケーションにおいて，車外と車両システム間で通信が行われる．そのため，車外からの不正なアクセスによる車両のコントロールや車両情報の不正取得を防ぐような仕組みが必要となる．

本研究では，セキュリティに関する検討をインターネットでのセキュリティ対策技術をベースにして行った．セキュリティ対策は，ネットワークのアーキテクチャによって左右されるため，このアーキテクチャを具体的に想定する必要がある．そのため，まず，車載情報プラットフォームで考えられるゲートウェイや通信機器の配置によるアーキテクチャモデルをすべて抽出し，これらモデル間でのセキュリティ比較を行なった．

ゲートウェイ配置は，PLANETSで代表される2GW型と１個のゲートウェイを有する1GW型とに大別される．また，通信機器の配置によって，様々なモデルが考えられ，本研究では，PLANETSのモデルとして五つ，1GW型として四つのモデルを仮定した．下記に各モデルを簡単に説明する．

（1）PLANETS1：前述のアーキテクチャであり，外部通信機器・後付機器は，OPEN情報系LANに接続される．モデルとしてはFig. 2のモデルからOEM情報系LANの外部通信機器を外したものである．

（2）PLANETS2：LAN，ゲートウェイ構成はPLANETS1と同じであるが，汎用通信を行う外部通信機器がOEM情報系LANにも接続される．Fig. 2に，アーキテクチャモデルを示す．

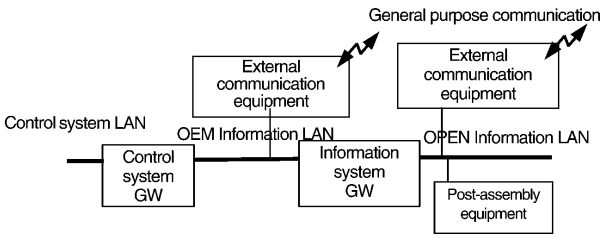

Fig. 2 PLANETS2 architecture model

（3）PLANETS3：PLANETS2のアーキテクチャモデルと同様であるが，OEM情報系LANに接続された外部通信機器にセキュリティ機能を配置する．

（4）PLANETS4：PLANETS2のアーキテクチャモデルと同様であるが，OEM情報系LANに接続された外部通信機器のデータは情報系ゲートウェイに必ずルーティングされる機構である．

（5）PLANETS5：PLANETS2のアーキテクチャモデルと同様であるが，情報系ゲートウェイに外部通信モジュール（汎用通信）が１対１接続される．Fig. 3に，アーキテクチャモデルを示す．

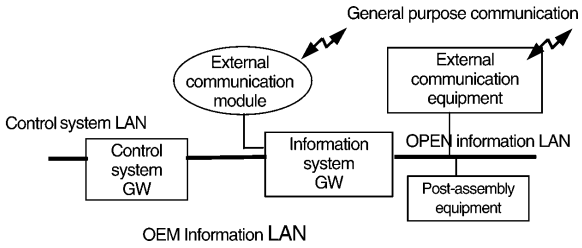

Fig. 3 PLANETS5 architectural model

（6）1GW型１：この方式は，制御系LANと情報系LANがゲートウェイで接続され，情報系LANにOEM系機器，後付機器，及び外部通信機器が接続される．Fig. 4にアーキテクチャモデルを示す．

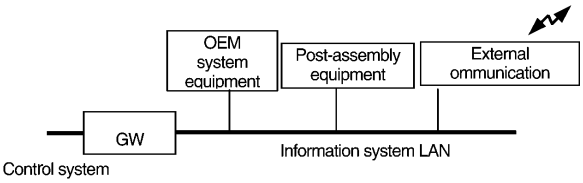

Fig. 4 1GW type1 architectural model

（7）1GW型２：この方式は，制御系LANとOEM情報系LANが制御系ゲートウェイで接続され，OEM情報系LANが情報系ゲートウェイに接続される．情報系ゲートウェイに外部通信モジュール，及び後付機器が１対１接続される．Fig. 5に，アーキテクチャモデルを示す．

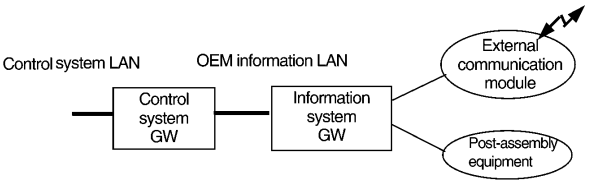

Fig. 5 1GW type2 architecture model

（8）1GW型３：この方式は，制御系LANと情報系LANが制御系ゲートウェイで接続される．情報系LANには外部通信I/F，及び後付機器が接続され，外部通信I/Fに外部通信モジュールが接続される．Fig. 6に，アーキテクチャモデルを示す．

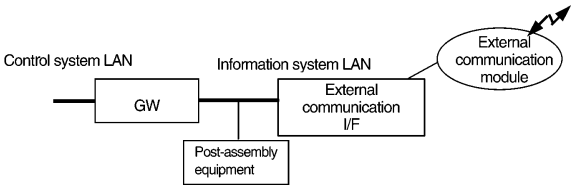

Fig. 6 1GW type3 architectural model

（9）1GW型４：この方式は，制御系LANとOEM情報系LANが制御系ゲートウェイで接続されており，制御系ゲートウェイに後付機器，及び外部通信モジュールが１対１接続される．Fig. 7に，アーキテクチャモデルを示す．

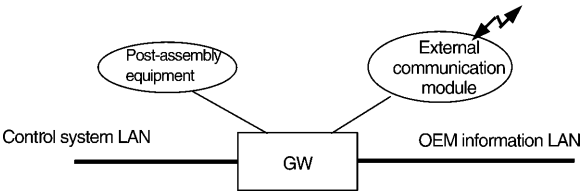

Fig. 7 1GW type4 architectural model

上記９モデルを以下に示す項目について比較評価した．

① 脅威への対応強度：脅威として「不正アクセス」，「盗聴」，「DOS攻撃」を取上げ，対応力を評価した．
○：強い　△：中間　×：弱い

② フェールセーフ：セキュリティ処理機能を有するゲートウェイの故障によりデータ伝送が不可能になる程度を分析評価した．
○：ダウン影響が小さい　△：中間
×：ダウン影響が大きい

③ 処理負荷：ゲートウェイにおける処理負荷の大小を比較した．
○：処理負荷が軽い　△：中間
×：処理負荷が重い

④ コスト：コストは“セキュリティ機能の配置数”と“処理負荷”に比例する．
○：コストが低い　△：中間
×：コストが高い

その検討の概要をTable 1に示すが，脅威への対応強度は，PLANETS1，PLANETS3，PLANETS5，1GW型２が優れていること，また，脅威への対応強度では弱いが，コストを重視する場合には，1GW型１が優れていることが分かった．総合的に判断して，

PLANETSは他のアーキテクチャと比較して優れているため，以降の検討はゲートウェイの配置としてはPLANETSのアーキテクチャ，（通信機器の配置モデルとしてはPLANETS1）をベースに行うこととした．

Table 1 Comparison of architectures

	Unlawful access	Theft	DOS attack	Fail safe	Processing load	cost
PLANETS1	○	△	○	△	△	△
PLANETS2	△	△	×	○	△	△
PLANETS3	○	△	○	○	△	△
PLANETS4	○	△	△	△	△	△
PLANETS5	○	△	○	△	×	×
1GW type1	×	×	×	○	○	○
1GW type2	○	○	○	△	×	×
1GW type3	△	×	×	△	○	△
1GW type4	△	○	×	×	×	△

４．セキュリティ機能の抽出

必要なセキュリティ機能を抽出するために，異なる自動車メーカ間で共通に使用されることが想定されるAMI-Cのメッセージセット[2]を用いて，メッセージごとにアプリケーションの例及び考えられる脅威の具体例を検討した．たとえば，Doors lock or unlock stateというメッセージに対しては，キーレスエントリによるドアロック／アンロックというアプリケーションが考えられ，脅威の具体例としては，メッセージの盗聴及び所有者へのなりすましによってドアロックを解除し，車両／車内物品の盗難が考えられる．

さらに，それぞれの脅威の具体例について不正手段（盗聴，改ざん，不正アクセス等）を対応させ，これに対して，セキュリティ必要性の程度（大：人命に影響，中：金銭／プライバシーに影響，小：いたずら目的等被害軽微，なし：被害なしの４段階）を検討し，これに対応し得るセキュリティの仕組み（暗号化，MAC，PIN認証等）及びセキュリティの強度（秘密鍵方式，公開鍵方式等）を導き出した．

AMI-C以外に考えられるITSアプリケーションに使用されるメッセージについてもこれらを検討し，車載情報プラットフォームとして必要なセキュリティ機能を抽出した．この検討結果の一部をTable 2に示す．Table 2は，ISO15408におけるセキュリティ要件表に相当する．

検討結果より，車載情報プラットフォームにはセキュリテイの仕組みとして盗聴に対する暗号化，改ざんに対応するMAC（Message Authentication Code）認証及び不正アクセスに対応するPIN（Personal Identification Number）認証を実現させる必要があることが判明した．

５．ゲートウェイにおけるセキュリティ機能及び配置

セキュリティ機能を二つのゲートウェイにどのように配置するかについては，アーキテクチャ，カーメーカの方針，セキュリティの仕組み，各ゲートウェイの性質などによって異なってくる．そこで，本研究では前述した検討結果よりPLANETS1のアーキテクチャモデルをベースに，セキュリティ機能配置方法として機能分散型と機能集中型の二つを検討した．

Fig. 8とFig. 9に，機能分散型と機能集中型の機能配置を示す．Fig. 8とFig. 9の共通点は，ゲートウェイ，通信機器及びプロトコル変換機能の配置である．プロトコル変換機能は，情報系でのTCP/IPプロトコルを制御系LANでのプロトコルに変換する機能のため，必然的に制御系ゲートウェイに配置される．

また，脅威はOPEN情報系LANに配置される通信機器からのみ侵入し，自動車メーカ保証のため安全（セキュア）な範囲とみなせる制御系LAN，OEM情報系LANに配置される機器からは侵入しない．そのため，セキュリティ機能を制御系，情報系いずれのゲートウェイに配置しても制御系における車両安全性は確保できる．

Fig. 8の機能分散型の場合，暗号化におけるセキュリティ処理量がMAC，PIN認証に比して大きく，かつ，MAC，PIN認証に先んじて復号化の処理をしなければならないため，情報系ゲートウェイに暗号化，制御系ゲートウェイにMAC，PIN認証の配置になる．

Fig. 9の機能集中型の場合，脅威に対して水際作戦（情報系ゲートウェイで対応）を採り，制御系，OEM情報系ともに脅威から守れるよう情報系ゲートウェイにセキュリティ機能を集中させる配置とした．

セキュリティ機能配置の比較結果をTable 3に示す．

Table 3より，セキュリティ機能開発を情報系ゲートウェイに集中させる（制御系ゲートウェイをプロトコル変換だけの既存の回路，ICで構成し，新規開発不要にできる）機能集中型を追及した方が開発効率上良いと判断できる．

Table 2 Example of AMI-C vehicle interface service and security

Interface service category	Kind of interface service	Message (explain)	Direction	Application example	Threat example	Unlawful measure	Protection object	Security needs	System
Vehicle status services	Distance	Odometer, Delta of odometer, Trip meter, Vehicle speed etc.	Control system→ Information system → Outside	Fuel consumption calculation using fuel information (measure actual value)	Driving distance data theft.	Theft, Tampering.	Driving distance information	Low	PIN certification + MAC grant at control GW.
	Airbag	Enable or Disable, Deployed or not	Control system→ Information system → Outside	Message to HELP center when air bag is deployed.	Tampering with air bag activation data. Mischief (be informed to center with no accident).	Theft, Tampering.	Air bag activation information	High	PIN certification + MAC grant at control GW, +encryption at information GW.(with OPEN key)
	Fuel	Fuel type, Unit (liter, gallon), Rest, Threshold	Control system→ Information system → Outside	Fuel consumption calculation with distance information	Fuel consumption data theft, or tampering with fuel type. Mischief (different type fuel supply)	Theft, Tampering.	Fuel information	Low	PIN certification + MAC grant at control GW.
	Warning lights vector	Oil,engine, AirBag, Brakes, Traction_ Control ,Battery ,ABS,Doo _Ajar,etc	Control system→ Information system → Outside	Inform dealers and store the information into drive recorder data.	Monitor abnormal condition from outside and use it for sales.	Theft.	Warning indicator condition	Medium	Encryption at information GW.
	Trac-tion control	Enable, Disable Engaged or not	Control system→ Information system → Outside	Display control condition.	Obtain information with unlawful access.	Theft.	Control information	None	(Note) theft is impossible at OEM control system and information system.
	Cruise control	Enable Disable, Engaged or not Vehicle cruise speed	Control system → Information system → Outside	Send info mation to center and use it as traffic information.	Monitor externally and use it as charged service information.	Theft.	Control information	Medium	Encryption at information GW.
	Suspen-sion control	enable, disable, status	Control system → Information system	Display road condition change on NAVI at the simultaneously .	Get information with unlawful access.	Theft.	suspension condition information	None	(Note) theft is impossible at OEM control system and information system.

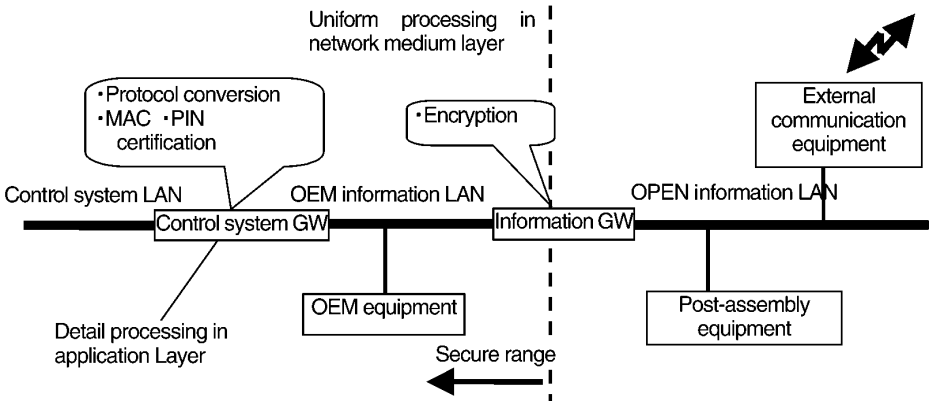

Fig. 8 Functional layout of distributed function type

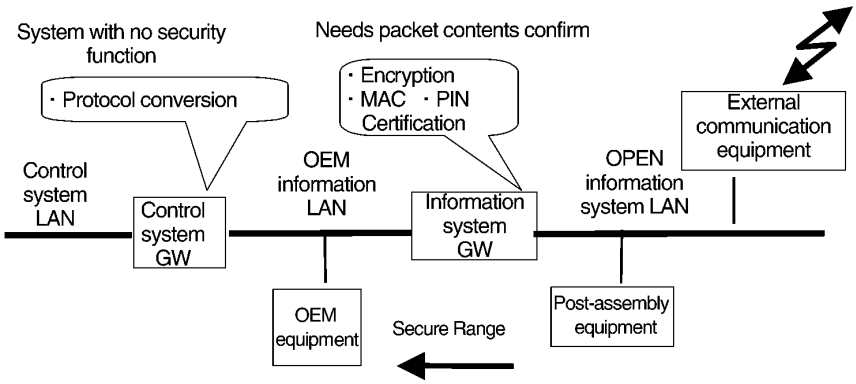

Fig. 9 Functional layout for centralized function type

Table 3 Comparison of security function layout

Function layout	Advantage	Disadvantage
Distributed type	- Correspond to high speed transmission without checking packet contents at the information GW. - Low cost design of the information GW is possible.	- New security system is needed to control GW which may increase cost. - For security function new version, both side GW must be changed simultaneously.
Centralized type	- Installation GW only needs conversion of existing protocol. Therefore hardware/software can be made simpler compared to a distributed type. - Centralized management of security function is possible (including new versions, failure correction etc).	- Because information GW load become heavy a new system to cope with high speed transmission is needed, and increased costs are expected. - Failure in information GW security function may affect control system equipment. Therefore highly reliable methods such as dual GW system are required.

６．おわりに

2001年度は，2000年度提案した車載情報プラットフォームのセキュリティ機能について検討した．2000年度提案したものも含め９種類のアーキテクチャモデルについて，比較を行うとともに，AMI-Cのメッセージセット及びそれ以外に想定されるメッセージをもとにして具体的なセキュリティ機能を抽出した．明らかにされたセキュリティ機能を実現するための具体的仕組みと，二つのゲートウェイへのセキュリティ機能配置を提案した．今後は，提案したセキュリティ機能　及び　配置を検証するための実証実験並びに標準化提案のための仕様明確化を推進していく．

＜参考文献＞

1) 新エネルギー・産業技術総合開発機構・財団法人自動車走行電子技術協会編：「高度情報化対応型車内情報基盤技術研究開発」（2001年3月）
2) AMI-C SPEC 3002-0-0 Common Message Set-Release1

＜著　者＞

柳川　博彦
（やながわ　ひろひこ）

ITS開発部
画像処理,次世代LANなどを用いた車載アプリケーションの開発に従事

高橋　寿平
（たかはし　じゅへい）

財団法人 自動車走行電子技術協会
高精度位置標定,基準道路シーンなどに関する車載システム標準化研究に従事