# 自律分散制御路側網システムのセキュリティ機能の開発

福澤寧子[†] 石田修一[†]
平岩賢志[††] 瀬戸洋一[†]

ITS（高度道路交通システム）におけるスマートゲートウェイシステムでは，基地局などを自律分散制御する路側網通信システムと，路側網と高速走行する車両間を DSRC（Dedicated Short Range Communication：狭帯域通信）で接続する路車間通信システムを用いて，多種多様なサービスの提供が検討されている．路側網，路車間通信システムは，様々な攻撃の対象となりうることから，不正アクセス，データの盗聴や改ざんを防止するなどのセキュリティ機能要件が高い．一方，路側網システムは大規模であり，システムの既設部を停止することなく段階的に拡張することが望ましく，各装置が自律的に動作し，他装置へ影響を与えることのない自律分散制御システム（ADS: Autonomous Decentralized Systems）であることが有効である．しかしながら，従来の ADS は，事業所内で管理される比較的信頼性の高いものであったため，セキュリティについては議論されていない．本論文では，不正アクセス，データの盗聴や改ざんを防止するために，自律分散制御される路側網システムのセキュリティ要件と実現要件を明確化し，そのうえで路側網システムのセキュリティ機能を開発，評価した．その結果，実用にむけた適用可能性を確認した．

# Development of Security Functions for Roadside Network by Autonomous Decentralized Control

Yasuko Fukuzawa,[†] Shuuichi Ishida,[†] Masasi Hiraiwa[††] and Youichi Seto[†]

The smart gateway system for intelligent transport systems (ITS) is intended to connect vehicles with a network and to provide drivers with a variety of services. The roadside network consists of base stations (BSs), a gateway, and a local server (LS). The BS's antennas are placed alongside the road, and they communicate with vehicles by using Dedicated Short Range Communication (DSRC), a wireless communication protocol. The BSs, the GW, and the LS form the Autonomous Decentralized System (ADS). Equipment connected to the ADS acts autonomously, which has two advantages. The system can be extended easily, and even if the part of the system breaks down, the rest of the system can remain operational. ADS in the past has been vulnerable to certain attacks. To prevent such attacks, we have proposed security counter measures that establish secure communications in the roadside network. This paper describes the security requirements that are suitable for the ADS roadside network, implementations of these measures, and evaluations of the performance of the security process on the smart gateway system.

## 1. はじめに

ITS（高度道路交通システム）における，知能化された道路と自動車が協調して機能するスマートゲートウェイシステムでは，事故情報や渋滞情報などの交通情報の提供や，課金・決済などをともなう多種多様なサービスの提供が検討されている[1)]．

ITS を実現する移動体通信としては，FM 多重などの放送系，IMT2000 などのセルラ系，DSRC（Dedicated Short Range Communication：狭帯域通信）などがある．ETC（Electronic Toll Collection：自動料金収受）システムにすでに適用されている DSRC をより高度化し適用する方法は，仕様的には直径 30 m のスポットで 4 Mbps の通信を実現し，通信容量が大きく確保できる点で優位性がある[2)]．

一方，基地局を含む路側網システムは大規模なネットワークシステムであり，システムを段階的に既設部を停止することなく拡張する必要があることから，各装置が自身の動きを把握し，自律的に動作することで，他装置への影響を与えることなくシステムを動作でき

† 株式会社日立製作所システム開発研究所
Hitachi, Ltd., Systems Development Laboratory
†† 株式会社日立製作所ネットワークソリューション事業部
Hitachi, Ltd., Network Systems Solution Division

る自律分散型の制御が有効である．これまで，システムの信頼性，拡張性，保守性向上を狙いとした自律分散概念の提案[3]と，この概念に基づくシステムが構築され，鉄道交通や産業分野の情報制御システムで実用化[4]されており，その通信プロトコルの業界標準化の報告もある[5]．

しかしながら，従来の鉄道や産業分野の情報制御などの自律分散制御システム（ADS: Autonomous Decentralized Systems）は，自律分散制御下の装置でクローズなネットワークを構成し，事業所内で管理される比較的信頼性の高いものであったため，ADS におけるセキュリティのあり方については議論されていない．

スマートゲートウェイシステムにおける自律分散制御下の基地局を含む路側網は，一般の利用者が車両と基地局との通信で利用し，直径 30 m の通信範囲に明示的に基地局が設置されることから，一般利用者からの様々な攻撃の対象となりうる．したがって，スマートゲートウェイシステムにおいては，路側網は高速走行する車両を捕捉・追尾するとともに，不正アクセス，データの盗聴や改ざんを防止するために，路側網通信および路車間通信システムで提供する基本的セキュリティ機能の実現が課題である．

本論文では，基地局などの装置からなり，自律分散制御される路側網通信システムにおけるセキュリティ方式を開発した．

以下，2 章においてスマートゲートウェイシステムと自律分散制御システムの概要を述べ，そのうえで自律分散制御される路側網システムのセキュリティ機能要件を明確化し，3 章において ADS 路側網システムのセキュリティ機能提案，4 章において ADS 路側網システムのセキュリティ機能開発について述べる．

## 2. 自律分散制御路側システムと課題

スマートゲートウェイシステムと ADS の概要を述べ，そのうえで ADS である路側網通信システム（以下，路側網）のセキュリティ機能要件を明確化する．

### 2.1 スマートゲートウェイシステムの概要

スマートゲートウェイシステムは，**図 1** に示すように，路側網は，路側に設置された複数の基地局，走行支援系などのサービスを行う Local application Sarver（LS），IP（Internet Protocol）ネットワークへの接続点となる GW（GateWay）から構成される ADS である．IP ネットワークには，利用者資格確認や汎用課金，各種汎用サービスを提供するサーバが接続される．

高速走行する移動局である車両と基地局間の無線通信には DSRC が適用されるが，DSRC はセキュリティ機能として簡易なスクランブル機能のみを有している．このため，DSRC を利用した ETC システムでは，自動料金収受処理に特化したアプリケーション固有のセキュリティ機能を実装している．しかし，DSRC の汎用化，高機能化利用を図るうえでは，DSRC においてネットワークノード間で保証すべき基本的なセキュリティ機能の実現が課題である．

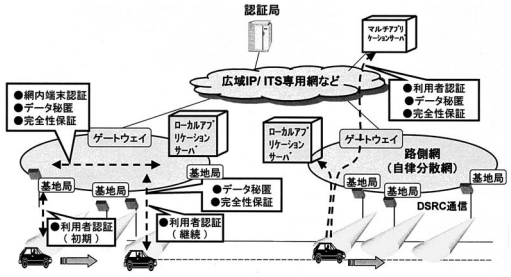



**図 1** スマートゲートウェイの概要
Fig. 1 Architecture of the Smart Gateway system.

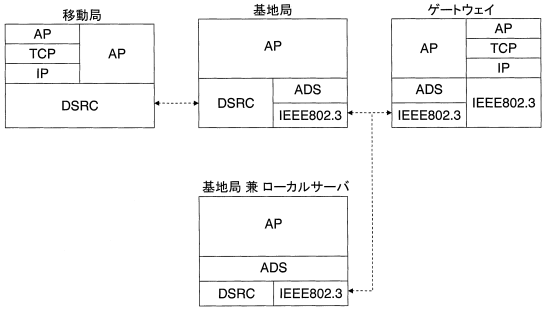



**図 2** 通信レイヤ構成
Fig. 2 Communication layer.

スマートゲートウェイでは，基地局は 30 m 間隔に設置し，180 km/h で通行する車両にまで対応することを考慮しており，数百ミリ秒から数秒に 1 回の割合で，車両の通信相手である基地局が別の基地局に変わるというハンドオーバが発生する．このため，DSRC のセキュリティ機能としては，ハンドオーバに対応して実現する必要がある[6)~9)]．

一方，路側網は，システムを逐次拡張し，オンラインメンテナンスに対応するなどの点で ADS とすることが有効である．しかし，従来の ADS にはセキュリティは考慮されておらず，ADS において導入すべき基本的なセキュリティ機能の実現が課題である[6)]．

**図 2** は，各装置における通信レイヤの構成を示す．基地局と，移動局である車両の車載器には DSRC を実装し，無線通信を行う．DSRC の上位には IP レイヤと走行支援などの非 IP 系アプリケーションを実装する．IP レイヤの上位には Web ブラウザなどの IP

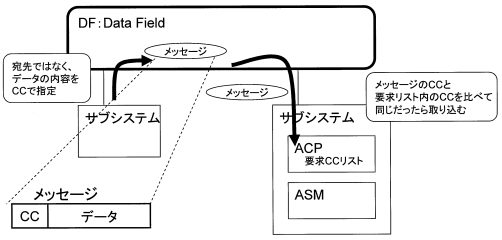



**図 3** Autonomous Decentralized System の概要
Fig. 3 Architecture of Autonomous Decentralized System.

系アプリケーションを実装する．走行支援などの非 IP 系アプリケーションは，路側網内の LS に搭載する．基地局，LS，GW には ADS レイヤを実装し，ADS レイヤを介して，自律分散制御を行う．GW には外部のネットワークと接続するための IP レイヤを実装する．本論文では，ADS レイヤにセキュリティ機能を組み込み，セキュアな自律分散網を構築する．

### 2.2 自律分散制御システムの概要

次に，路側網を構成する ADS の基本仕様を**図 3** に示す[1),2)]．ADS を構成するサブシステムは，ACP（Autonomous Control Processor）と ASM（Application software module）から構成され，各サブシステムは DF（Data Field）によって接続される．メッセージには宛先を示す情報は含まれず，データの内容を示す CC（Content Code）とデータからなり，サブシステムから DF 上をブロードキャストされる．各サブシステムは，必要なデータの CC を ACP に登録しておき，DF 上を流れるデータの CC を見て自律的に判断を行い，必要なものを適宜取り込み，ACP から受け取ったデータを元に，データドリブンで動作を行う．これは，データの内容に従った自律的な動作であるため，ADS には，システム全体を変更することなく，サブシステムの追加が可能であり，一部のサブシステムが故障しても，システム全体は動作を続けるなどの特長がある．

CC としては，ADS を実装するシステムの特徴に応じて，グループコードや送信者識別コードなど各種想定されるが，路側網ではサービスを識別するコード：SID（Service ID）を用いる．

### 2.3 ADS 路側網通信システムのセキュリティ機能実現にむけた課題の整理

#### 2.3.1 セキュリティ上の要件

路側網システムの図 2 の ADS レイヤについて，リスク評価を行った．リスク評価では，通信データや鍵などのセキュリティ情報を資産とし，第 3 者，内部者，運用者（管理者）による脅威を洗い出した．ただし，基地局装置内のメモリなど LSI を直接解析して，秘密情報を不正に入手するなどの物理的攻撃への対策は，半導体技術と密接に関わるセキュリティ技術であり，ここでは耐タンパ性は保証されているものとし，本脅威は検討の範囲外とした．

評価の結果，以下の要件は，リスクを受容，転化，移転させるより，情報セキュリティ技術で対策することで，リスクを回避するのが妥当と判断したものである．

(1) 端末認証

不正な端末が正規の端末になりすまして，路側網に接続し，ネットワークリソースを不正に利用するという脅威が存在する．これに対して，不正な基地局などの接続を防止するために，接続された装置を認証し，路側網への接続が許可されたノードであることを確認する．

(2) データ暗号化・改ざん防止

通信路上データ（SID およびデータ）の盗聴，解析などによる情報の漏洩を防止し，プライバシーを保護するために，通信データを暗号化し，機密性を保証する．データは第 3 者による盗聴だけでなく，ADS ネットワークに接続された端末間においても，非受信の SID 情報については，盗聴，改ざんができないようにする．

(3) 接続端末のセキュリティ状態の維持

端末の認証，接続後，不正な端末に差し替えるという脅威に対し，端末の接続状態を再確認し，データ暗号化のための暗号鍵などを更新する．

#### 2.3.2 ADS 路側網のセキュリティ機能実現上の要件

2.2 節に記載した ADS の概念に則り，路側網のセキュリティ機能を実現するにあたり，まず，ADS のセキュリティモデルの要件を明確化し，さらにスマートゲートウェイシステムにおける路側網のセキュリティモデルの要件を明確化する．

(1) ADS のセキュリティ機能実現モデル要件

セキュリティモデルを構築するうえで，以下の項目について，その実現性を検討する．

〈発行系における管理者の想定〉

セキュアなネットワークシステムを構成するための基本となるセキュリティ情報（固有の秘密鍵など）をいかに配布するかが重要になる．秘密鍵情報の生成，配布などを管理し，各ノードが固有の秘密鍵を保持した状態をつくる発行モデルにおいて，管理者の存在を仮定できるか否かで，セキュリティ実現方式が異なる．管理者の存在が仮定できるモデルでは，セキュリティ情報が一元管理され，モデルが簡素化できる．

〈鍵共有における管理者の想定〉

ノード間で行うデータ暗号化のための鍵共有においても，管理者が想定できるモデルは実現が簡易になる．

一般的なネットワークモデルでは，認証サーバがクライアント装置やユーザを認証し，データ暗号化のための鍵の共有，更新を一元的に管理する認証サーバが存在する．一方，認証サーバが存在しないモデルでは，任意のグループ構成に応じて，鍵を共有する[10]．

〈グループ鍵の構成〉

情報を共有するセキュアなグループを構築するうえで，グループが動的に構成されるか，静的に構成されるかによって，実現モデルは異なる[10]．

ADS では，ネットワークへの接続時に，各ノードがそれぞれ受信すべき SID を把握していることで，各ノードが自律的に動作することを可能にしている．これは，各ノードに受信すべき SID 情報を取得するという発行フェーズがあることを意味しており，発行管理者を想定することができる．

また，各ノードはネットワーク接続時には，それぞれの役割を把握していることから，鍵共有モデルでのノードの役割として，鍵共有における管理者を想定することができる．ただし，ADS では，各ノードが自由にネットワークに接続，離脱できることを特長としており，必ずしもつねに，管理者がネットワーク上に存在しているとは限らない．

さらに，ADS では SID にともなう情報の送受信グループを構成するが，ネットワーク接続時には，すでに各ノードが受信すべき SID を把握していることから，グループは任意のメンバによって動的に構成されるのではなく，発行系モデルの管理者によって静的に構成されるといえる．

(2) 路側網のセキュリティ機能実現モデル要件

路側網は，図 1 に示したように，GW と基地局，LS から構成される．基地局，LS はネットワークに自由に接続，離脱することは想定できる．

一方，IP ネットワークとの接続点である GW は，システムの構成上，不在になることはなく，GW がネットワークを離脱し，不在になる時間がわずかに存在する可能性はあるものの，GW が ADS から不在になるシステムは想定できない．

## 3. 路側網における ADS セキュリティプロトコルの提案

2 章に基づき，自律分散制御される路側網のセキュリティ機能を実現する．

以下，提案方式の概要と実装方式を述べる．

### 3.1 提案方式概要

ADS 路側網において，セキュリティ機能を担う 3 つのエンティティと，その処理概要を以下に定義する．

(1) 発行管理者：路側網を構成する各ノードに対し，ノード固有の秘密鍵を発行し，また各ノードが送受信する SID，役割情報を発行する．これらの情報の発行に責任を有し，信頼できる後方系機関と位置付ける．

(2) 認証マネージノード：発行管理者によって付与された役割に従い，路側網において認証サーバ機能を担い，路側網に接続されるユーザノードを認証し，SID を保護する SID 暗号鍵，ユーザノードが送受信する SID にともなうデータを保護する鍵（データ暗号化用鍵，改ざん検知用鍵）を配布する．また，ユーザノード固有の再認証鍵を配布する．本ノードには GW が対応し，IP ネットワークとの接続機能を担い，システムの連続性を保証する．このため，GW は路側網システムからきわめて短い時間離脱する可能性はあるものの，本質的には常設である．GW がネットワークから離脱する場合には，路側網のセキュリティステータスはロック状態になり，新たなユーザノードの接続は認めない．GW は，先に配布した再認証鍵を用いてユーザノードを再認証し，ユーザノードのなり代わりを検知する．また，SID にともなうデータ暗号化鍵を更新する．

(3) ユーザノード：発行管理者によって付与された役割に従い，路側網においてクライアント機能を担う．SID 情報についての発信者にも受信者にもなりうる．本ノードには，基地局，LS に相当し，システムの運用において，自由にネットワークに接続，離脱できる．

### 3.2 実現方法

2.3.1 項に示したセキュリティ要件を，以下のセキュリティ機能で満たす．

(1) ノード情報発行

発行管理者は，GW，基地局，LS のネットワークへの接続に先立ち，各ノードに固有の非対称暗号鍵や送受信できる SID，役割情報を付与し，これらの情報は電子証明書として正当な情報であることが保証される．

(2) 路側網接続端末の認証

路側網への新規接続端末を認証する．**図 4** に，(2) 接続端末の認証と，(3) 鍵配布の処理フローを示す．なお，ここでは，電子証明書の正当性検証処理は省略する．

① ネットワークへの接続を要求する基地局 1 は，参加要求を送出し（省略可），GW は，初期認証用の乱数 A をブロードキャストする．

② ネットワークへの接続を要求する基地局 1 は，

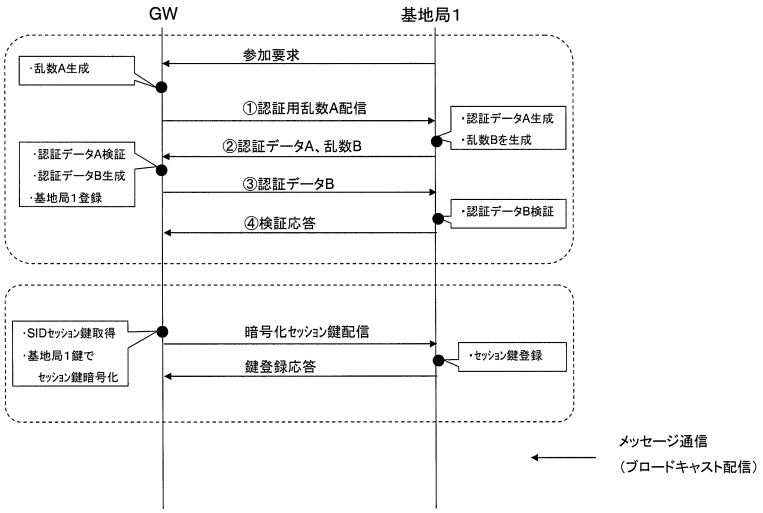



**図 4** 路側網接続端末認証，鍵配布処理フロー
Fig. 4 Initial authentication and key distributing.

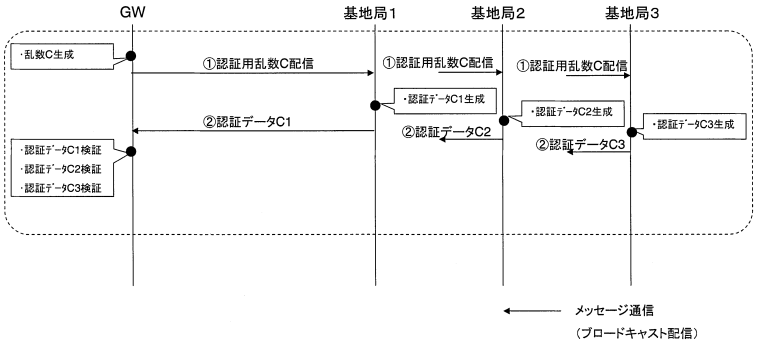



**図 5** 接続状態確認処理
Fig. 5 Continuous authentication.

固有の非対称暗号鍵（秘密鍵）を用いて，乱数 A に対する認証データ A を生成し，また GW 確認用の乱数 B を生成し，送出する．基地局 1 の非対称暗号鍵（公開鍵）もあわせて送付してもよいし，あらかじめ GW が保持していてもよい．

③ GW は，基地局 1 の非対称暗号鍵（公開鍵）を用いて認証データ A の正当性を確認すると，GW は，GW 固有の非対称暗号鍵（秘密鍵）を用いて，乱数 B に対して認証データ B を作成し，送出する．

④ 基地局 1 は，GW 固有の非対称暗号鍵（公開鍵）を用いて認証データ B の正当性を確認すると，検証完了のメッセージを送出する．

(3) 鍵配布，暗号化

SID および SID に応じた通信データの暗号化，MAC（Message Authentication Code）の付加による改ざん検知を行う．

GW が，(2) で認証した基地局に対し，全ノード共通の対称暗号鍵である SID 暗号鍵，SID ごとの対称暗号鍵であるセッション鍵（暗号化用鍵，MAC 生成用鍵）を発行する．また，以後のユーザノード再認証のために，ノード固有の非対称暗号鍵対応に，対称系暗号鍵の再認証鍵を配布する．この配信には，各ノード固有の非対称暗号鍵（公開鍵）を利用する．

なお，再認証鍵の利用の目的は，主として認証処理の効率化である．また，SID ごとのグループで共通の暗号鍵を用いる方式は，ADS の宛先を指定しない通信方式に則って実現できる．

(4) 接続状態の再確認

定期的あるいは任意のタイミングで，ユーザノードの正当性確認を行い，SID 暗号鍵，SID 対応のセッション鍵を更新する．処理フローを**図 5** に示す．

① GW は，確認用の乱数 C を適切な頻度でブロー

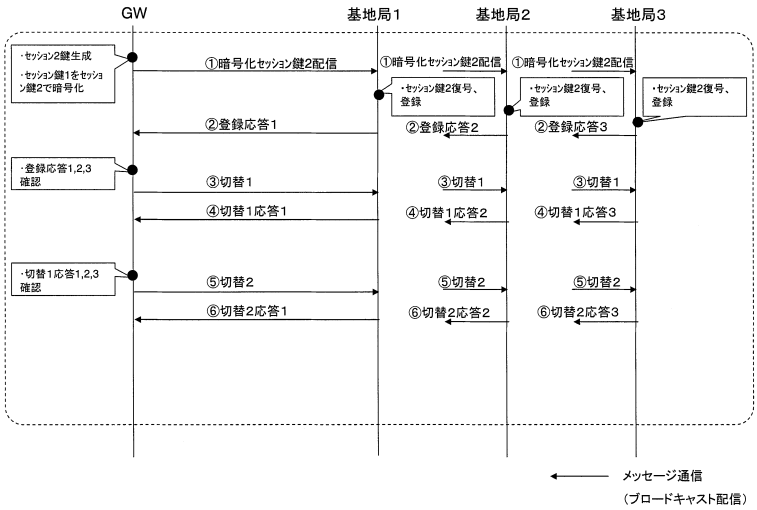



**図 6** 暗号鍵更新処理
Fig. 6 Update of encryption keys.

ドキャストする．

② 路側網への接続を継続する基地局 1〜3 の各ノードは，(3) で配布された再認証鍵で，確認用乱数 C に対する認証データ C ＊を生成，送信する．

③ GW は，認証データ C ＊を検証し，基地局 1〜3 の各ノードの接続状態を確認する．一定期間内に認証データが届かない基地局または LS があった場合，SID 暗号鍵，SID 対応の対称鍵暗号のセッション鍵（暗号化用鍵，MAC 生成用鍵）を生成し，再配布する．

(5) 暗号鍵の更新

SID ごとの鍵更新は定期的に実行する．鍵更新処理シーケンスを**図 6** に示す．

① GW は SID 対応の新しいセッション鍵（乱数）を生成する．新セッション鍵を旧セッション鍵で暗号化し，鍵更新要求とともに送信する．

② 各基地局は，鍵更新要求と暗号化された新セッション鍵を旧セッション鍵で復号し，新セッション鍵を得，鍵更新応答を送信する

以後の処理においては，各基地局は暗号化には旧セッション鍵，復号にも旧セッション鍵を用い，旧セッション鍵で復号できない場合に新セッション鍵を用いる．暗号化と復号のセッション鍵不一致は，通信データを復号した際に，通信データに付与された MAC が不正と判断されることで検知できる．

③ GW は鍵更新応答を全ノードから受信後，鍵切替え要求 1 を送出する．

④ 各基地局は，鍵切替え要求 1 を受信後，鍵切替え応答 1 を送出する．以後の処理において，各ノードは暗号化には新セッション鍵，復号には新セッション鍵を用い，新セッション鍵で復号できない場合には旧セッション鍵を用いる．

⑤ GW は鍵切替え応答 1 を全ノードから受信後，鍵切替え要求 2 を送出する．

⑥ 各ノードは鍵切替え応答 2 を受信後，鍵切替え応答 2 を送出する．以後の処理において，各ノードは暗号化，復号ともに新セッション鍵を用いる．以上で置き換えを完了する．GW は，鍵更新がうまくいかなかった端末からは，鍵切替えなどの応答を得られない．そこで，GW は再送処理を行う．なお，SID 暗号鍵についても同様である．

## 4. セキュリティプロトコル開発

### 4.1 開発内容

3 章に記載の提案方式に則り，ADS 路側網セキュリティ機能を開発した．開発環境は以下である．

GW OS ：BSD/OS v4.2
メモリ：512 MByte
CPU ：Intel Pentium4 1.5GHz
基地局 OS ：VxWorks 5.1.2
メモリ：96 MB
CPU ：Hitachi SH4 200MHz

また，暗号方式としては以下を用いて実装した．

- 接続端末の認証：RSA（1,024 ビット）
- 接続状態の再確認：Multi-S01（256 ビット）[11)]
- 鍵配布（共有）：HIME (R)（1,024 ビット）[11)]
- 暗号化・完全性保証（データ通信）：Multi-S01 [11)]

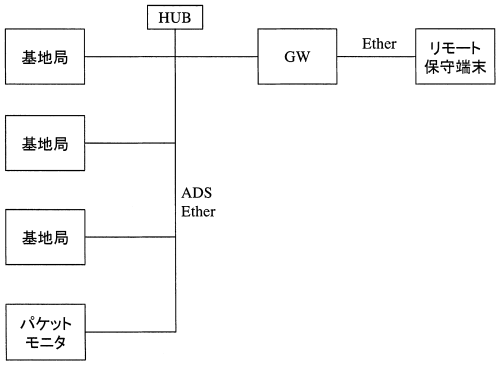



**図 7** 評価システムの構成
Fig. 7 Experiment system.

MAC の生成は，Multi-S01 の特徴である改ざん検知機能を利用した．

### 4.2 評　　価

**図 7** は 100 Mbps のイーサネットを使用した ADS のセキュリティ機能性能測定システム構成を示す．基地局接続時の認証と鍵共有，基地局の接続状態の確認（再認証），鍵更新，暗号通信の処理を評価した．評価結果は，CPU および通信処理時間である．

(1) 接続時の認証と鍵共有

GW と 1 台の基地局間で，図 4 に従い，基地局が GW から暗号鍵を配布されるまでの時間を測定した．基地局が接続して接続要求を送信してから，検証応答を送信するまでの相互認証の時間が約 1.20 秒，基地局が検証応答を送信してから，鍵登録応答を送信するまでの鍵配布の時間が約 0.54 秒である．1 台の GW 配下に 256 台の基地局，LS が接続されると想定した場合，すべて基地局との接続時の認証と鍵共有処理が行われるシステム立ち上げ時は，最大約 7 分半となる．運用時には，CPU のセキュリティ処理負荷を 1%程度に制御することが必要である．

(2) 接続状態の確認（再認証）

GW に対して基地局を 3 台接続し，GW の接続確認要求から，すべての基地局の認証が終了までの処理時間は，2.30 msec である．

1 台の GW 配下に 256 台の基地局を接続した場合には，最大約 0.2 秒かかる．サービスの連続性を保証するため，CPU のセキュリティ処理負荷を 1%以下に抑えた場合，20 秒に 1 回接続確認が可能である．これは，攻撃者が基地局を攻撃するために基地局を物理的に切断した場合に，これを検知するのに十分な頻度と考える．基地局，LS の離脱を検知した場合には，(1) 接続時の認証と鍵共有における鍵共有で，再共有する必要があり，$0.54 \times 256$ 台で，最大 2 分半を必要とするため，実際の運用では，(3) と同様に，再配布する新鍵と，旧鍵が共存できる工夫が必要になる．

(3) 鍵更新

GW に対して基地局を 3 台接続し，1 種の SID に対応する暗号鍵の更新が，全基地局で完了するまでの処理時間は，6.68 msec である．1 台の GW 配下に 256 台の基地局が接続され，各基地局が 100 種の SID 暗号鍵を持つと想定し，すべての基地局の暗号鍵を更新には約 60 秒かかる．基地局が実際に攻撃を受けている場合には，通信の負荷を増やしても通信の安全性を保護することが必要であるが，定期的な鍵更新は，3.2 節 (5) に記したように，新旧の鍵が共存できる運用を可能とするため，問題ないと考える．運用時には，CPU のセキュリティ処理負荷を 1%程度に制御することや，トラフィックが少ない時間帯に行うことが望ましい．また，基地局が持つ暗号鍵の数を絞ることも有効である．

(4) GW と基地局間の暗号通信

**表 1** は，GW 基地局間の暗号通信において，各サイズ長のパケットを送信した際のスループットを示す．暗号化を行うと，通信速度は，暗号化を行わない場合の 25%から 52%程度に低下した．

実際の利用状況を考えた場合，DSRC のアンテナが 2 Mbps の実効性能とすると，今回の評価結果で最もスループットがでるパケットサイズ 3,000 byte でのスループットは 27.8 Mbps で，約 14 台までのアンテナを収容できる．システム構成を考慮し，暗号処理の専用チップ化，暗号化対象データの絞り込みなど配慮する必要がある．

**表 1** 暗号化処理速度
Table 1 Result of encryption.

| 通信方向 | サイズ（byte） | 非暗号化時の速度（Mbps） | 暗号化時の速度（Mbps） | 割合（%） |
|---|---|---|---|---|
| GW → BS | 30 | 1.86 | 0.97 | 52.2 |
| | 100 | 6.16 | 3.18 | 51.6 |
| | 1000 | 56.3 | 25.2 | 44.8 |
| | 3000 | 61.0 | 27.8 | 45.6 |
| BS → GW | 30 | 0.65 | 0.23 | 35.4 |
| | 100 | 1.97 | 0.71 | 36.0 |
| | 1000 | 16.8 | 4.75 | 28.3 |
| | 3000 | 20.7 | 5.17 | 25.0 |

## 5. おわりに

スマートゲートウェイシステムの路側に設置する基地局などから構成され，自律分散制御される路側網通信システムにおけるセキュリティ機能を開発した．

データの送信先を指定しない自律分散制御型の通信

方式，および管理方式の特性を考慮し，後方系は発行管理者による鍵などのセキュリティ情報発行とし，通信データに付与される SID に従ってデータの受信・非受信を判断する通信方式に則り，SID に基づく鍵管理，接続端末の再確認などを含むセキュリティ方式を提案，開発した．その結果，実用にむけた適用可能性を確認した．

今後は，認証マネージノードの自由な接続，離脱を可能とするネットワーク構成への適用を可能にするために，認証マネージノードの権限を他のノードに委譲するなどの機能を加えることで，本提案方式をより一般化し，ITS 同様にオープン化や無線利用が進む自律分散制御システムにおいて，共通的に適用できる方式に拡張する．

なお本研究は，通信・放送機構の委託研究「走行支援システム実現のためのスマートゲートウェイ技術の研究開発（H12〜H14 年度）」によって実施した．

## 参 考 文 献

1) 重野ほか：特集 ITS，情報処理学会誌，Vol.40, No.10, 959/992 (1999).
2) Oyama, S.: DSRC standards and ETC systems development in Japan, *Proc. 7th World Congress on Intelligent Transport Systems* (2000).
3) 森ほか：自律分散概念の提案，電学論 C，104, 12, 303 (1984).
4) Mori, K.: Autonomous decentralized systems: Concept data field architecture and future trends, *ISADS '93*, pp.28–34 (1993).
5) 新：ADS–net と国際標準化活動，計測と制御，Vol.39, No.3, pp.209–215 (2000).
6) 通信・放送機構：平成 13 年度研究開発成果報告書走行支援システム実現のためのスマートゲートウェイ技術の研究開発 (May 2002).
7) 福澤ほか：スマートゲートウェイシステムにおけるセキュリティ技術の開発，情報処理学会，ITS 研究会 (May 2001).
8) Ishida, S., et al.: Security Techniques for Smart Gateway Systems, *Proc. 8th World Congress on Intelligent Transport Systems* (2001).
9) Ishida, S., et al.: Study of Security Techniques in the Vehicle-Road Communications System, *Proc. 9th World Congress on Intelligent Transport Systems* (2002).
10) Fiat, A. and Naor: Broadcast Encryption, *CRYPTO'93*, LNCS (1993).
11) http://www.sdl.hitachi.co.jp/crypto/index-j.html

(平成 15 年 4 月 2 日受付)
(平成 15 年 9 月 5 日採録)

**福澤 寧子**（正会員）

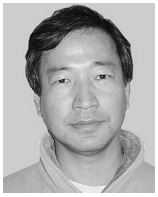
1985 年日本女子大学家政学部家政理学科物理学系卒業．同年（株）日立製作所システム開発研究所入所．以来，ソフトウェアの生産性，情報セキュリティシステムの研究開発に従事．現在，ITS 等のモバイルシステムにおけるセキュリティ技術の研究開発を行っている．同研究所主任研究員．電子情報通信学会会員．

**石田 修一**（正会員）

1997 年東京工業大学総合理工学研究科物理情報工学専攻修士課程終了．同年日立製作所入社．以来，日立製作所システム開発研究所にて，情報セキュリティ技術の研究開発に従事．主に暗号モジュール利用システムや，ネットワークにおける認証技術の開発を行っている．

**平岩 賢志**（正会員）

1981 年東京大学理学部情報科学科卒業．同年（株）日立製作所入社．交換システム開発，ITS 関連システムをはじめネットワークソリューション開発に従事．IEEE 会員．



**瀬戸 洋一**（正会員）

1979 年慶應義塾大学大学院修士課程修了．同年（株）日立製作所に入社．システム開発研究所に配属．以来，衛星画像処理システム，地図情報システム，医療情報システム，情報セキュリティ，ITS システムの研究開発に従事．セキュリティシステム研究センタ副センタ長，セキュリティビジネスセンタセンタ長を歴任，現在ユビキタスセキュリティ担当主管研究員．ISO/IEC JTC1/SC37 専門委員会委員長．工学博士，技術士（情報工学部門）．電子情報通信学会，IEEE 等の会員．著書：『情報セキュリティ事典』（共立出版），『生体認証技術』（共立出版），『情報セキュリティ』（昭晃堂）等．