コンピュータセキュリティ　10－30
（2000．　7．25）

ＩＴＳのためのセキュリティアーキテクチャの検討

田中 俊昭　　中尾 康二　　竹森 敬祐

（株）ＫＤＤ研究所
〒356-8502　埼玉県上福岡市大原 2-1-15，TEL:0492-78-7406
e-mail: tl-tanaka@kdd.co.jp

あらまし　ＩＴＳ（高度道路交通システム）では、多種多様な通信処理システムを介して、移動中あるいは停止中の車両に対して、サービス予約/決済/走行支援などの様々なサービスを提供することを想定しているが、安全性の高い各種ＩＴＳサービスを実現するためのセキュリティ機能についてこれまで体系的に検討がなされていなかった。本稿では、ＩＴＳの各種サービスを実現するためのセキュリティアーキテクチャを提案する。具体的には、ＩＴＳの４つの代表的なサービスモデルをベースとして、そのリスク分析を行い、リスクを回避するためのセキュリティ機能を洗い出し、セキュリティアーキテクチャを導出する。さらに、ＩＴＳ特有のサービスに着目し、具体的なセキュリティプロトコルを提案する。

キーワード：　ＩＴＳ、セキュリティアーキテクチャ、セキュリティプロトコル、リスク分析

Study on the security architecture for Intelligent Transportation Systems

Toshiaki Tanaka　　Kouji Nakao　　Keisuke Takemori

KDD R & D Laboratories Inc.
2-1-15 Ohara Kamifukuoka-shi Saitama 356-8502, Japan
TEL: +492-78-7406
e-mail: tl-tanaka@kdd.co.jp

Abstract　ITS(Intelligent Transportation Systems) supports a lot of communication services , such as reservation service, payment service, driver support service and etc, by connecting various kinds of communication systems. However, no security architecture to cover wider area of such ITS communication services has been proposed. Therefore, this paper proposes security architecture for ITS services. Precisely speaking, we analyze the risk against four typical ITS services, and summarize security functionality for these ITS services to derive security architecture. Finally, we propose a few concrete security mechanisms for some specific ITS services in order to show the feasibility of the proposed security architecture.

keywords:　ITS, security architecture, security protocols, risk analysis

1. はじめに

昨今、ＩＴ技術の重要な一分野であるＩＴＳ（高度道路交通システム）が脚光を浴びている。ＩＴＳでは、車に搭載される情報通信端末（車載器とよぶ）、路側機、および、各種サービスを提供するセンタなど、多種多様な通信機器やシステムにより構成され、それらを組み合わせることにより、移動中あるいは停止中の車両[1]に対して、道路交通情報/ナビゲーション情報等の提供サービス、ホテルなどの各種予約サービス、既存インターネットとの接続サービス、有料道路/駐車場/オンラインショッピングなどの決済サービス、交通事故や障害物などの緊急通報サービスなど様々なサービスを提供できる。従って、ＩＴＳのネットワークも、電話網やインターネットと同様に、一大ネットワークとなることが予想され、汎用性や信頼性を考慮したネットワークアーキテクチャを検討することが必須のテーマとなっている。このなかでも、ＩＴＳサービスを安全に提供・享受するためには、各種セキュリティ機能の観点からも検討が必要となる。しかしながら、ＩＴＳのセキュリティ機能を網羅的・体系的に扱ったアーキテクチャがこれまで検討されておらず、ＥＴＣ（自動料金収受システム）などの具体的なサービスに従ったセキュリティ機能が個別に検討されているのみである。今後、利便性と相反するセキュリティ機能をさまざまなＩＴＳサービスに対して、必要最小限に効率的に導入するためには、各種ＩＴＳサービスに対するリスク分析を行い、そのリスクを回避するためのセキュリティ機能を検討することによる、網羅的、体系的なセキュリティアーキテクチャの提示が解決すべき、急務の課題であると考えられる。従って、本稿では、代表的なＩＴＳサービスに対して、そのリスクを分析し、セキュリティアーキテクチャを導出するとともに、いくつかのＩＴＳサービスにおける具体的なプロトコルを提案する。

本稿の構成としては、２章において、ＩＴＳのネットワークモデルを定義し、３章において、そのネットワークモデルに従ったＩＴＳのセキュリティアーキテクチャについて検討する。さらに４章において、具体的なセキュリティプロトコルの提案を行い、５章にて、今後の課題を述べる。

[1] サービスのなかには、一部、歩行者支援といったものも考えられている。

2. ITSのネットワークモデル

様々なＩＴＳサービスを実現するためのネットワーク技術として、現在、政府を始めとするいくつかの団体において、研究・開発および標準化の作業が進められている。本稿では、そのなかでも郵政省で進められているＩＴＳ推進会議において、定義されたネットワークモデル[1]をベースとし、本モデルを単純化するとともに、車両側の構成も含めて検討を行う。以下、単純化したネットワークモデルについて述べる。

2.1 ITSネットワークの構成要素

ＩＴＳネットワークは、以下の構成要素によって成り立っている（図１参照）。

- ＩＴＳ-ＡＰセンタ（Ａ）
  本センタは、各種ＩＴＳサービスをＩＴＳ利用者に提供する。構築方法によっては後述のＩＴＳサービスセンタと機能を一体化した物理的な構成をとることも可能である。また、本センタは、インターネット等の外部網を介してサービスを提供する外部のＡＰセンタも含む。
- ＩＴＳサービスセンタ(C)
  本センタはＩＴＳ-ＡＰセンタと連携して、情報収集、情報加工、情報マージなどの統合情報処理機能を提供する。
- 路側処理システム（路側機：Ｓ）
  ＤＳＲＣ無線通信により車両と通信を行い、ＩＴＳセンタと車両通信との中継をするとともに、センサやカメラ等の路側機器を含み、収集した情報をＩＴＳサービスセンタに送る。
- 車載器（Ｏ）
  車両の中に設置され、ＤＳＲＣ、移動体、放送ネットワークなどを介して、センタ側と通信を行う。また、センタ型からの情報を表現する情報端末の機能も保有する。本装置内には車両を識別する情報が埋め込まれる。
- ＩＣＣ（Ｉ）
  耐タンパー機能を有するスマートカードを想定する。車載器を介して、センタ側と通信を行う。本モジュールは、利用者個人が保有することを前提とする。
- 各種ネットワーク

各構成要素を接続するネットワークとして、ＩＴＳサービスセンタおよびＩＴＳ-ＡＰセンタを相互接続するバックボーンネットワーク、路車間通信のための路側ネットワーク、車両と路側のシステムが情報交換を行うための路車間ネットワーク、ＩＣＣと車載器とを接続する車内ネットワークがある。

2.2 ITSにおけるサービスモデル

ＩＴＳ推進会議においては、その代表的なＩＴＳサービスとして以下の４つのタイプに集約されている。

・ 情報収集型サービス
情報の収集、加工、蓄積を目的として、路側機のセンサが測定・収集した道路交通情報をＩＴＳサービスセンタが収集するサービスを指す。送信データとしては、測定値等のデータ通信系とカメラ等で撮影したリアルタイム通信系の２種類が考えられる。データ通信系プロトコルは、１時間～３時間に１００Kbyte程度の転送を想定する。

・ 情報配信型サービス
蓄積された情報の配信を目的として、ＩＴＳ-ＡＰセンタから交通情報、旅行者情報、緊急情報、娯楽情報などを配信するサービスを指す。

・ コマンド・レスポンス型サービス
情報の検索、予約の登録、決済などを目的として、利用者がＩＴＳ-ＡＰセンタに対して要求を行い、当該センタから応答を受取るサービスを指す。

・ 路側応答型サービス
車両の走行支援を目的として、センサが測定・収集した緊急情報などを、車両に通知するサービスを指す。

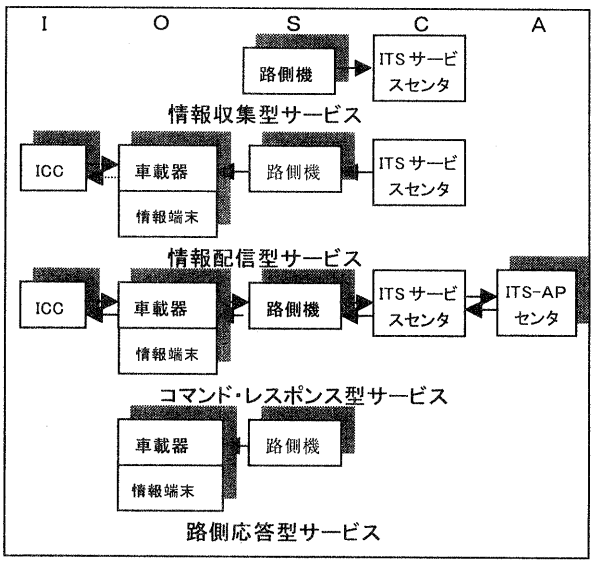

図1 ITSの代表的なサービス構成図

3. ITSにおけるセキュリティアーキテクチャの提案

3.1 ITSにおけるリスク(脅威)とそのセキュリティ対策

ＩＴＳにおけるセキュリティ機能を検討するには、各種ＩＴＳサービスにおけるリスク（脅威）を明確化し、その脅威を分析することにより、脅威を回避するためのセキュリティ機能の洗い出しが必要となる。例えば、ISO/IEC１５４０８（セキュリティ評価基準）[2]では、PP（プロテクションプロファイル）やST(セキュリティターゲット)を規定することで、そのセキュリティ要件が明確になる。上記標準では、様々な観点からの脅威及び、セキュリティ機能が規定されているが、本稿では、図１に示すように、2.1節の構成要素を用いた４つのサービスをベースに脅威を分析する。図２にＩＴＳの各構成要素に対するハイレベルな

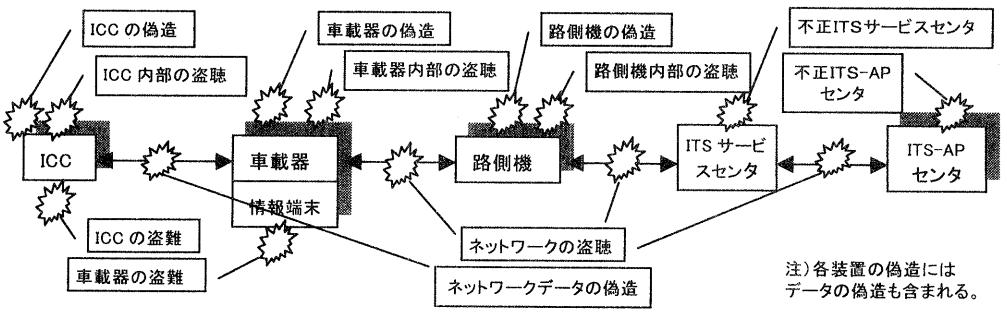

図2 ITSにおける脅威

脅威を示す。ここで、ＩＴＳの特長として、

・ ＩＣＣは個人が管理する装置、車載器は車両に設置される装置、路側機はセキュリティ管理のない場所に設置される点から、これらの装置に対しては、盗難や物理的な攻撃の可能性があること、

・ ＩＣＣ－車載器間は車内ネットワークで接続される場合を想定する、車載器―路側機間は、ＤＳＲＣなどの無線区間である、路側機―ＩＴＳセンタにおいては、路側機側がセキュリティ管理がない、ＩＴＳサービスセンター―ＩＴＳ-ＡＰセンタ間は、ＩＴＳ-ＡＰセンタがインターネットなどの外部ネットワークと接続されている可能性があることから、すべてのネットワークは攻撃される可能性がある。

・ コマンド・レスポンス型のような決済を有する処理においては、別途商品の物流などの処理が発生する場合もあるため、取引間で通信（取引）の事実を、後で否定する攻撃の可能性がある。

という点を考慮する必要がある。

表１にＩＴＳにおける脅威とそのセキュリティ対策を示す。本表では、ＩＴＳにおけるセキュリティの具体的な脅威と、その脅威に対応する情報セキュリティの観点からの脅威、さらに、その脅威に対する一般的なセキュリティ対策をあらわしている。なお、システムの製造・開発過程・初期設定での脅威、システムのバグ、特権利用者の不正利用、運用上のセキュリティホールを用いたネットワーク攻撃、などに対する機密性、安全性は確保されていることを前提とする。また、攻撃対象側で現状効率的な回避策がないＤＯＳ(Denial of Service)攻撃については検討の対象外とする。

一般的に、不正な機器によるなりすましや不正アクセスについては相手認証機能を、ネットワーク上での改竄に対してはメッセージ認証機能を、ネットワークの盗聴に対しは秘匿機能を、通信の否認については、否認防止機能を、機器の偽造については耐タンパー機能を用いることにより、安全性を保障することが可能となる。

以降、各ＩＴＳサービスにおける、セキュリティ要件の詳細化を行う。この際、システムやサービス要求を満足し、しかも、効率性を考慮し、通信資源、計算資源を最小にする最適な設計を行う必要がある。

表１ ITSにおける脅威とそのセキュリティ対策

ITSにおける脅威	情報セキュリティとしての脅威	一般的なセキュリティ対策	カテゴリ
ICCの偽造		耐タンパー性の保証	i-0
	なりすまし	相手認証	i-1
	不正アクセス	相手認証	i-2
	通信の否認	ログ、否認防止	i-3
ICC内部の盗聴	情報の不正入手	耐タンパー性の保証	i-4
ICCの盗難	他人へのなりすまし	PIN等による本人認証	i-5
ICC／車載器ネットワークの盗聴	情報の不正入手	情報の秘匿	Ni-1
ICC／車載器ネットワークのデータの偽造	情報の改竄	メッセージ認証	Ni-2
車載器の偽造		耐タンパー性の保証	o-0
	なりすまし	相手認証	o-1
	不正アクセス	相手認証	o-2
車載器内部の盗聴	情報の不正入手	耐タンパー性の保証	o-4
車載器の盗難	他車へのなりすまし	物理鍵？？	o-5
車載器／路側機ネットワークの盗聴	情報の不正入手	情報の秘匿	No-1
車載器／路側機ネットワークのデータの偽造	情報の改竄	メッセージ認証	No-2
路側機の偽造		耐タンパー性の保証	s-0
	なりすまし	相手認証	s-1
	不正アクセス	相手認証	s-2
路側機内部の盗聴	情報の不正入手	耐タンパー性の保証	s-4
路側機／ITSサービスセンタネットワークの盗聴	情報の不正入手	情報の秘匿	Ns-1
路側機／ITSサービスセンタネットワークのデータの偽造	情報の改竄	メッセージ認証	Ns-2
不正ITSサービスセンタ	なりすまし	相手認証	c-1
	不正アクセス	相手認証	c-2
	通信の否認	ログ、否認防止	c-3
ITSサービスセンタ／ITS-APセンタネットワークの盗聴	情報の不正入手	情報の秘匿	Nc-1
ITSサービスセンタ／ITS-APセンタネットワークのデータの偽造	情報の改竄	メッセージ認証	Nc-2
不正ITS-APセンタ	なりすまし	相手認証	a-1
	不正アクセス	相手認証	a-2
	通信の否認	ログ、否認防止	a-3

3.2 セキュリティ機能の前提条件

前節の脅威に対して、各ＩＴＳサービスのセキュリティ機能を詳細化するにあたり、各サービスでの共通的なセキュリティの前提条件を以下に述べる。

(1)相手認証（Entity Authentication）

本稿では、相手認証の前提条件は以下のとおりとする。

1) 2章のネットワークモデルでは、様々なエンティティが存在するが、認証は基本的に各ＩＴＳサービスのサービス提供側とサービス享受側の対で行うこととする。

2)本人認証

ＩＣＣは、可搬性がある反面、盗難された場合には、他人により、不正使用される可能性がある。これを防ぐため、ＩＣＣの利用に際しては、ＰＩＮやバイオメトリクスなどによる本人認証を行うことを前提とする。

3)利用者認証

有料配信型や、コマンド・レスポンス型の予約、決済型のサービスでは、車両よりも個人としての利用契約が主であると考えられるため、利用者個人を認証する必要がある。このため、ＩＣＣは、この利用者個人を認証するためのエンティティとする。従来のインターネットのように、ＩＴＳ以外のプラットフォームで外部ＡＰセンタと通信することも想定する。

4)車両認証

路側応答型サービスにおける走行支援では、車両を対象としたサービスを想定するため、車両を認証する必要が生じる。従って、車載器は車両が認証されるためのエンティティとする。また、車両を認証するエンティティとしては、路側機、ＩＴＳサービスセンタのいずれかが考えられるが、

・走行支援サービスにおいては、運転者への即時通知が必要となるため、高速認証を行う必要がある。

・路側機～ＩＴＳサービスセンタに至るまでのネットワークリソースに対する、不正な車載器からの使用を防止する。

という点を考慮し、路側機で車両の認証を行う方が望ましい。この場合、車載器の失効状況（ブラックリスト）の管理を路側機で行う必要がある。

(2)メッセージ認証（Message Authentication）

メッセージ認証は以下の前提条件を満足する。

1)メッセージ認証機能は、その通信データの重要度により選択的に機能を提供できる。

2)メッセージ認証機能は、情報の発信元と発信先のエンティティ間で提供する。

(3)秘匿（Confidentiality）

秘匿機能は以下の前提条件を満足することとする。

1)秘匿機能は、その通信データの重要度により選択的に機能を提供できる。

2)秘匿機能は、情報の発信元と発信先のエンティティ間で提供する。

(4) 否認防止機能(Proof of Origin)：

否認防止機能は、以下の前提条件を満足することとする。

1）否認防止機能は、決済時など必要に応じて、選択的に機能を提供できる。

2)否認防止機能は、データの送信事実、受信事実を保証するエンティティ間で提供する。

(5)耐タンパー性（Tamper Resistant）

ＩＣＣ、車載器および、路側機に関しては、物理攻撃の脅威が存在するため、耐タンパーモジュールを保有していることを前提とする。特に、車載器及び路側機の耐タンパーモジュールをＳＡＭと呼ぶ。

3.3 各ITSサービスでのセキュリティ機能

上記の前提条件を満足する具体的なＩＴＳサービス個々のセキュリティ機能について検討する。

(1)情報収集型サービス

- 相手認証機能：　路側機で渋滞情報や事故情報などを検知（センス）して、ＩＴＳサービスセンタに情報を提供するため、表１中の脅威 x-1(x:s,c, 1:1,2)を考慮して、ＩＴＳサービスセンター路側機間で相互認証する必要がある。
- メッセージ認証機能：　脅威 Ns-2 を考慮して路側機で生成されたメッセージの正当性を認証する必要がある。
- 秘匿機能：車を特定するナンバープレートなどの情報が収集される場合があるので、脅威 Ns-1 を考慮して秘匿が必要となる。
- 否認防止機能：　データを収集することによりサービスが完結する即時的なサービスであるので本機能は不要である。

(2)情報配信型サービス

- 相手認証機能：　本サービスでは、利用者毎に利用可能なサービスが異なる有料型サービス、および、利用者を特定しない無料型サービスの２つが考えられる。前者の場合は、前節(1)-3)および脅威 x-1(x:i,c, 1:1,2)を考慮して、ＩＣＣとＩＴＳサービスセンタ間で相互認証を行う。ここで、本稿の前提条件（前節(1)-4）)では、車載器で車両を認証するため、ＩＣＣ－ＩＴＳサービスセンタ間で相手認証を行ったとしても、脅威 x-1(x:o,s, 1:1,2)を考慮し、車載

器―路側機間の相互認証は必要となる。
また、後者の場合は、利用者を特定しないため、脅威 c-1(1:1,2)のみを考慮して車載器がＩＴＳサービスセンタを認証する必要がある。

・ メッセージ認証機能： 脅威 Nx-2(x:o,s)を考慮し、情報発信元であるＩＴＳサービスセンタからのメッセージを発信先である車載器が認証する。
・ 秘匿機能： 車載器―ＩＴＳセンタ間で利用者を特定する有料情報配信の場合のみ、脅威 Nx-1(x:o,s)を考慮し、情報秘匿機能が必要となる。
・ 否認防止機能： 情報の配信によりサービスが完結するため、不要である。

(3)コマンド・レスポンス型サービス

・ 相手認証機能： 本ＩＴＳサービスにおいては、①ＩＴＳサービスセンタを仲介して、複数のＩＴＳ内部のＩＴＳ-ＡＰセンタにアクセスし、その結果をまとめて、利用者に返送する場合と、②ＩＴＳサービスセンタを経由して外部のＩＴＳ-ＡＰセンタに直接アクセスする場合が考えられる。①の場合、前節(1)-3)および脅威 x-1(x:i,c, 1:1,2)を考慮し、ＩＴＳサービスセンタとサービス利用者であるＩＣＣの間で相互認証を行う。かつ、脅威 x-1(x:c,a, 1:1,2)を考慮し、ＩＴＳサービスセンタとＩＴＳ-ＡＰセンタ間でセンタ間相互認証を行う。ここでは、ＩＴＳサービスセンタは、利用者になりかわり各種ＩＴＳ-ＡＰセンタと通信することになり、一種のエージェントとしての機能を有する点が特長となっている。②の場合は、前節(1)-3)および脅威 x-1(x:i,a, 1:1,2)を考慮し、ＩＣＣとＩＴＳ-ＡＰ間で相互認証を行う。

さらに、情報配信型有料型サービスと同様に、前提条件（前節(1)-4）)および脅威 x-1(x:o,s, 1:1,2)を考慮し、車載器―路側機間の相互認証は必要となる。

・ メッセージ認証機能： メッセージ認証については、前述の①, ②のいずれの場合においても、センタ側の情報発信元は、ＩＴＳ-ＡＰセンタである。一方、車両側については、ＩＣＣおよび車載器のいずれかが可能である。前者は、ＩＣＣが電子マネーのように耐タンパー装置内で処理を行うＩＴＳサービス（ＩＣＣ決済型と呼ぶ）が想定され、表中の脅威 Nx-2(x:i,o,s,c)を考慮し、相互のメッセージ認証が、後者は映像やソフトウェアのダウンロードが考えられ、同様に脅威 Nx-2(x:o,s,c)を考慮し、ＩＴＳ-ＡＰセンタに対するメッセージ認証が必要となる。
・ 秘匿機能：メッセージ認証と同様に、ＩＣＣ―ＩＴＳ-ＡＰセンタ、および車載器―ＩＴＳ-ＡＰセンタのいずれかにおいて、前者の場合、脅威 Nx-1(x:i,o,s,c)、後者の場合、脅威 Nx-1(x:o,s,c)を考慮し、相互秘匿が必要となる。
・ 否認防止機能： 決済プロトコルなどのように通信の事実を取引事実として保証する証拠能力が要求される場合に、脅威 x-3(x:i,a)を考慮し、ＩＣＣ決済型およびダウンロード型双方のサービスにおいてＩＣＣ－ＩＴＳ-ＡＰセンタ間で必要となる。

(4)路側応答型サービス

・ 相手認証機能： 路側機側から複数台の車載器に対して一方的に走行支援情報を送信するためには、路側機の認証は不要である。一方、路側機のセンサでスピードオーバなどを検知して、利用者（ドライバー）に減速を促すような走行支援サービスにおいては、その特定の車両に対して、個別にデータを送信する必要があるため、脅威 o-1(1:1,2)を考慮して車載器を簡易認証する必要がある。
・ メッセージ認証機能： 不正な走行支援情報は事故につながる可能性があるため、脅威 No-2 を考慮して、路側機に対するメッセージ認証が必要となる。
・ 秘匿機能： 第３者に対しては無益な緊急情報であり不要である。
・ 否認防止機能： 即時的なサービスであるので不要である。

情報配信型サービスおよびコマンド・レスポンス型サービスのように、ＩＣＣを利用する場合には、脅威 x-1(x:i,o, 1;1,2)を考慮して、ＩＣＣ―車載器間で相互認証を行う必要がある。

また、ＩＴＳサービスとは直接関連がないが、ＩＴＳセンタから路側機に対して、失効情報（ブラックリスト）を送付する場合には、路側機がＩＴＳセンタを認証する必要がある。

これら各ＩＴＳサービスにおけるセキュリティ機能についてまとめた結果を表２に示す。

表2　各ＩＴＳサービスで必要となるセキュリティ機能

	相手認証	メッセージ認証	秘匿	否認防止
情報収集型	S⇔C	S→C	S→C	—
情報配信型（有料型）	I⇔C O⇔S I⇔O	O←C	O←C	—
情報配信型（無料型）	O←C	O←C	—	—
コマンドレスポンス型（ICC 決済型）	(I⇔C∧C⇔A) ∨ I⇔A O⇔S I⇔O	I⇔A	I⇔A	I⇔A
コマンドレスポンス型(ダウンロード型)	(I⇔C∧C⇔A) ∨ I⇔A O⇔S I⇔O	O←A	O⇔A	I⇔A
路側応答型	O→S	O←S	—	—

x←y: xy 間における y の x に対するセキュリティ機能

x→y：xy 間における x の y に対するセキュリティ機能

x⇔y: xy 間における相互セキュリティ機能

—：N/A（不要）

Ｉ：ＩＣＣ、Ｏ：車載器、Ｓ：路側機、Ｉ：ＩＴＳサービスセンタ、Ａ：ＩＴＳ-ＡＰセンタ

3.4 ITSにおけるセキュリティアーキテクチャの提案

前節で述べた各ＩＴＳサービスにおけるセキュリティ機能を実現するためのアーキテクチャを図3に示す。本アーキテクチャにおいては、セキュリティ機能は基本的にＡＰ層で実現する。ただし、ＤＳＲＣの無線区間においては、下位層（例えばＩＰ層）で実現される。ＡＰレベルのセキュリティ機能、下位レベルのセキュリティ機能は各ＩＴＳサービスにより一意に選択される。これらは、ＩＴＳセキュリティプロファイルとして必要な機能を選択できるようプロトコルに折衝機能を持たせる必要がある。

4. 具体的なセキュリティメカニズム

３章で導出したセキュリティ機能を実現するＩＴＳのプロトコルについて、ＩＴＳ特有のデータフローを有するいくつかのＩＴＳサービスに着目し、その具体的にメカニズムについて述べる。

4.1 情報配信型サービス（無料型サービスにおける相手／メッセージ認証）

無料の情報配信型サービスは、不特定多数に利用者に対して、同報のメッセージ認証を行うという点で特徴的である。ここで、

・ＩＴＳセンタから路側機への一方向通信であること、

・複数の車載器に同報すること、

・データ量が比較的大きいこと、

等の点を考慮し、1-path で非同期の認証・鍵共有プロトコルが必要となる。すなわち、

STEP 1　Send O←C:　Cert ‖ Sig (Time ‖ r) ‖ Time　‖ r ‖ M ‖ HMAC(K_share, M)

STEP 2　O:verify Cert and Sig(Time ‖ r)

STEP 3　O、C:K_share ← HMAC(K ‖ r)

STEP 4　O:　verify HMAC(K_share, M)

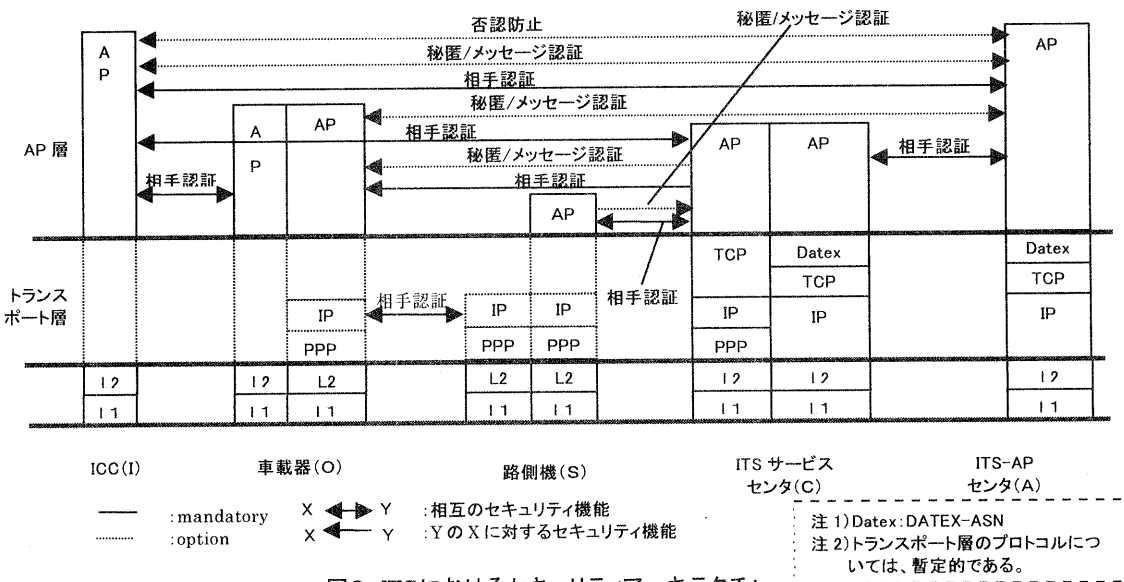

図3　ITSにおけるセキュリティアーキテクチャ

ここで、Cert：ＩＴＳセンタの公開鍵証明書[3]、Sig( )：安全性が保証されたＩＴＳセンタの署名処理(例えば、文献[3])、Time:時変情報、r:乱数、M:配信情報、HMAC:鍵付きMAC[4]、K_share:ＯＣ間の共有鍵、K:共有鍵作成のためのマスタ鍵、||:データの結合を、それぞれ表す。r（鍵）はＩＴＳサービスセンタが有効期間を管理しており、一定期間を経過後、更新される。また、マスタ鍵Kは車載器内のＳＡＭに保管される。

なお、ＩＣＣと車載器の間で、相互認証後に安全な通信路が確保されるという前提で、ＩＣＣでStep 2,3を処理することも可能である。

4.2 コマンドレスポンス型サービス
（ダウンロード型サービスの鍵共有）

本サービスは、

・相手認証とメッセージ認証のエンティティ　が異なる、すなわち、ＩＣＣ—ＩＴＳ-ＡＰセンタ間の相手認証と車載器—ＩＴＳ-ＡＰセンタ間のメッセージ認証である。

という点が特徴的である。これより、メッセージ認証及び暗号化の鍵を共有する、ＩＴＳ-ＡＰセンタ、ＩＣＣおよび車載器による鍵交換メカニズムについて、以下に具体的なアルゴリズムを示す。

STEP 0: p: prime　∧　q | p-1,　q:prime,
　　g: mod pの位数qの原始元
STEP 1: Ｉ：乱数r（r:0＜r＜q-1）を選択、
　　x←g^r mod p
　　Ｏ：乱数s（s:0＜s＜q-1）を選択、
　　y←g^s mod p
　　Ａ：乱数t（t:0＜t＜q-1）を選択
　　z←g^t mod p
STEP 2: sendＩ→Ａ:x,　Ｏ→Ａ:y
STEP 3: sendＡ→Ｉ,Ｏ：z
STEP 4: Ａ：K_s ←(xy)^t mod p
STEP 5: if ＩＯ-Authentication succeeded
　　then send Ｉ→Ｏ:z^r mod p
STEP 6: Ｏ：K_s ←(z^s)(z^r)

本プロトコルでは、ＩＣＣ内では、共有鍵を作成できない。また、ＩＣＣ－ＩＴＳ-ＡＰセンタ間の認証が成立しない限り、車載器は共有鍵を作成できない点で条件を満足している。この共有鍵を用いて、メッセージ認証は鍵つきMACを、秘匿は一般的な共通鍵暗号方式で機能を実現する。

4.3 路側応答型サービス

路側応答型サービスは、以下の観点を考慮し、簡易なメッセージ認証方式とする。

・路側機のメッセージ認証を行う。
・緊急情報通知が主たる目的であるため高速性が必要

STEP 1: Send S←O: M || Time || HMAC(K_m, M ||Time)
STEP 2: O: verify Time and HMAC(K_m, M || Time)

ここで、M:電文、K_m: マスタ鍵、T:時間情報とする。また、マスタ鍵は、車載器および路側機のＳＡＭの中に安全に保管されることを前提とする。

5　むすび

本稿では、ＩＴＳの４つの代表的なサービスモデルをベースとして、これらのサービスにおけるＩＴＳのさまざまな脅威を分析し、その脅威を防ぐためのセキュリティ機能について、それぞれのサービスに対する洗い出しを行い、これらのセキュリティ機能を実現するためのセキュリティアーキテクチャの検討を行った。さらに、そのなかからＩＴＳ特有のセキュリティ機能について、具体的な実現プロトコルを提示した。本稿では、可能な限り体系的、網羅的な検討を進めてきたが、非常に広範囲なサービスをカバーするＩＴＳに関しては、いくつか引き続き検討が必要な課題が残されている。具体的には、コマンド・レスポンス型サービスにおいてＩＴＳサービスセンタが利用者の代理として各ＩＴＳ-ＡＰセンタへアクセスする際の安全性、無線区間における車両移動にともなう効率的な車載器—路側機間の認証方法の検討、ＤＯＳ攻撃対策などがあり、これらの課題についても今後、検討を進める予定である。

参考文献

[1] ITS 情報通信システム推進会議、ITS プラットフォーム専門委員会　平成１１年度報告書, 2000.
[2] ISO/IEC15408 Evaluation Criteria for IT security part1～3, 1999.
[3] ITU-T X.509 Authentication Framework, 1997.
[4] M. Bellare and P. Rogaway.　Optimal Asymmetric Encryption-How to Encrypt with RSA.　Eurocrypt '94, pp. 92-111, 1994.
[5] M. Bellare, R. Canetti and H. Krauczyk. Keying Hash Functions for Message Authentication, LNCS 1109, pp. 1-15. Crypto'96, 1996.