

ETCシステムにおけるセキュリティ

Security in ETC System

上野 秀樹
UENO Hideki

鈴木 勝宜
SUZUKI Katsuyoshi

青木 恵
AOKI Megumi

近年注目されているITS(Intelligent Transport Systems:高度道路交通システム)の中で,ETCシステム(Electronic Toll Collection System:ノンストップ料金収受システム)が実用化段階に入った。ETCシステムでは,利用者のプライバシーの保護や確実な料金収受を図るために,認証や暗号などの様々なセキュリティ技術が用いられている。

当社は,長年にわたる料金収受システムのノウハウと高度なセキュリティ技術を活用し,幅広い範囲でETCシステムの構築を行っており,今回,わが国で最初に導入された“ETCセキュリティ中央システム”を開発した。

Intelligent transport systems (ITS) are expected to bring about innovation in the social system in the 21st century. As part of the ITS project, the Electronic Toll Collection (ETC) system is now entering the stage of practical utilization. Various security techniques are used in the ETC system in order to protect the privacy of users and secure the proper functioning of the toll collection system.

Toshiba is utilizing its long accumulated know-how in toll collection systems and advanced security technologies in the construction of a wide range of ETC systems. We have now developed a “central system for ETC security” and introduced this system for the first time in Japan.

1 まえがき

近年,世界的規模でITSが注目されている。わが国においては,国家プロジェクトとして,社会全体の情報化を進める“高度情報通信社会推進本部(本部長:内閣総理大臣)の下,国土交通省や警察庁などの各省庁及び産学が連携し,ITS化を進めている⁽¹⁾。

ITSの開発分野の一つであるETCシステムは,高速道路の料金所において現金の受渡しをなくし,無線で料金の情報をやり取りし決済するシステムである。特に,慢性化した高速道路における渋滞を解消する手段として注目を浴びており,2000年4月から首都高速道路や日本道路公団の高速道路の一部で試行運用が開始され,実用化段階に入ってきている(図1)。

ETCシステムでは,プライバシー保護や確実な料金収受を図るため,車と料金所の路側装置との間を無線通信でやり取りされる情報は,認証や暗号などのセキュリティ処理が施されている。このセキュリティの仕組みを実現するために,認証や暗号の際に用いる鍵(かぎ)情報を道路事業者が一元管理し,必要に応じて路側装置とデータをやり取りするセキュリティ中央システムが必要になる。

以下に,ETCシステムの概要,セキュリティの必要性,及び当社が開発したセキュリティ中央システムの役割について述べる。



図1. 運用中のETC料金所例 ETCに対応した料金所が既に実用化段階に入っている。

Example of ETC tollgate in operation

2 ETCシステムの概要

ETCシステムは,車両に搭載する(ICカードが挿入された)車載器と料金所ゲートに設置する路側無線装置との間で,車両の通行や料金に関する情報を無線通信によって交信し,自動的に料金を収受するシステムである。

ETCシステムのイメージを図2に示す。

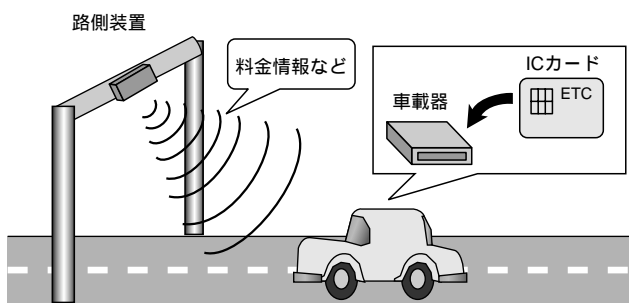


図2 . ETCシステムのイメージ 車側装置(ICカード,車載器)と路側装置の間で,料金のやり取りを無線で行う。
Image of ETC system

ETCシステムでは,利用者は料金所をノンストップで通過できる。そのため,1レーン当たりの料金収受処理能力が,従来の現金を支払う方式に比べ3~4倍となり,料金所での渋滞の解消・緩和につながると期待されている。

また,渋滞の解消・緩和に伴い,排気ガスの削減などによる環境面での効果も期待できる。更に,キャッシュレス化などによる利便性の向上も図れる。

3 ETCシステムの運用とセキュリティ

3.1 ETCシステムの構成

ETCシステムは,具体的には図3に示すように,ICカード,車載器,路側装置,ETCデータ処理装置,セキュリティ中央システム,などで構成されており,主に以下の(1)~(5)の手順によって運用される。

- (1) ETC用のICカードを車載器にセットする。
- (2) (1)の状態料金所ゲートに進入する。
- (3) 車載器と路側装置の間で,無線によって料金情報をやり取りする。
- (4) ETCデータ処理装置で,利用明細情報を作成し,カード会社に送る。
- (5) 後日,カード会社より利用者に料金が請求(引き落とし)される。

3.2 セキュリティ対応要素

一方,これまで高速道路における料金収受は有人(収受員による徴収)によって行われていたが,図2,図3に示すように,ETCシステムでは無人での運用ができる。したがって,今後ETCシステムの導入が増えるに伴い,無人運用の料金所も増えてくると予測される。

しかし,無人での料金収受は,自動販売機における偽造500円硬貨による不正などのように,有人の場合に比べて不正を行いやすい環境にある。すなわち,無人で運用すると,不正に料金収受を逃れようとする機会も多くなることになる。

したがって,ETCシステムにおいても,このような不正が起きる可能性があることを事前に想定し,その不正を防ぐための工夫を施す必要がある。

そこで,ETCシステムでは,次のような仕組みが,図4に示すように各装置や装置間で行われている。

- (1) 取扱いデータについては,データ送受信時の認証,情報秘匿のためのデータ暗号化,データ改ざん防止のためのデータ正当性チェックを行う。
 - (2) 不正アクセスを検知し,対処する仕組みを導入する。
- 以下に,その対応について具体的に述べる。

3.2.1 ICカードと車載器 ICカードと車載器は,利用者の手元に置かれるため,偽造などの不正の対象になりやすい。そのため,ICカードや車載器内におけるデータは暗号化して管理し,データをやり取りする際には認証や暗号化などを行っている。

このとき,認証や暗号化を行うための鍵情報は,漏洩すると偽造カードや偽造車載器を製造できる可能性があり,漏洩しないための工夫が必要である。そのため,鍵情報はセキュリティアプリケーションモジュール(SAM)と呼ばれるモジュールに格納されている。そして,盗聴などの不正アクセスを検知した場合には,鍵情報を保護する耐タンパ性^(注1)を考慮した設計になっている。

(注1) 不正アクセスを検知した場合に,データを保護するための機能及び仕組み。

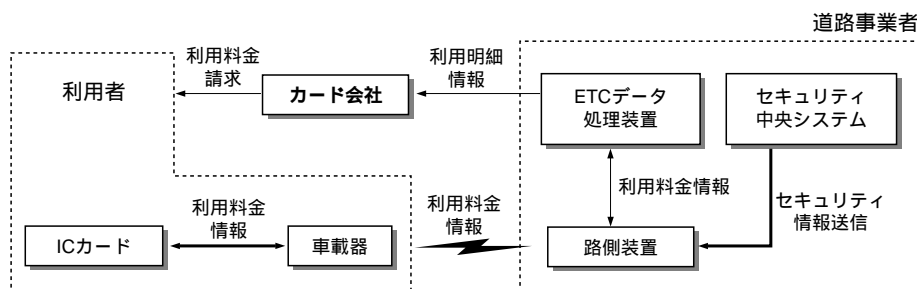


図3 . ETCシステムの構成要素 ETCシステムの処理フローを示す。車載器と路側装置の間で料金のやり取りが行われ,後日カード会社から料金が請求(引き落とし)される。
Components of ETC system

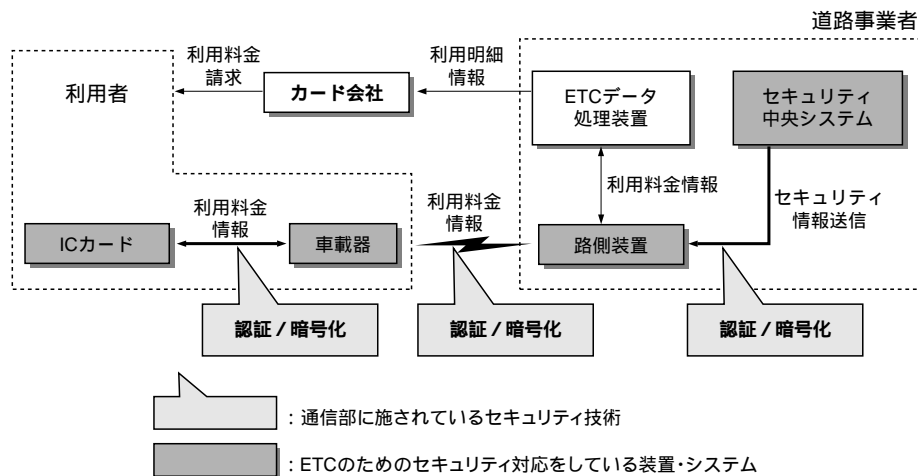


図4.セキュリティ対応要素 各要素間の通信にセキュリティ技術が施されており、各要素には不正アクセスを検知し、対応する仕組みが組み込まれている。
Components for security of ETC system

3.2.2 路側装置とセキュリティ中央システム 路側装置は、車載器との間で料金情報などのデータを無線でやり取りする。このため、認証やデータの暗号化通信を行うために、路側装置にはそれらに用いる鍵情報を保有している。したがって、車載器と同様に鍵情報はSAMに格納され保護されている。具体的には、不正なアクセスなどを検知した場合に、みずから保有している鍵情報を消滅させることによって、鍵情報が外部に漏れないような仕組みになっている。

また、不正アクセス検知以外でも、路側装置の電源がオフになった場合においても、同様にSAM上の鍵情報を消去する仕組みになっている。このため、路側装置の保守点検やその他の工事によって路側装置の電源をオフするたびに、鍵情報は消去されてしまうことになる。したがって、再度ETCサービスを開始するためには、鍵情報を路側装置に組み込む必要がある。

このとき、料金所の現場において、そのつど、鍵情報を保存している媒体から組み込むことは効率的でなく、また、鍵情報が保存されている媒体を持ち歩くことは、セキュリティ上たいへん危険である。

このため、鍵情報を中央で一元的に管理し、必要時に安全に鍵情報を配信する仕組みが必要となる。これを実現するのがセキュリティ中央システムである。

セキュリティ中央システムは、路側装置から鍵配信要求があった場合には、安全かつ確実な方法で鍵情報を自動送信する。

今回、当社は、わが国で最初に導入されたセキュリティ中央システムを開発した。開発にあたっては、セキュリティチームを社内に設置し、人の出入りを制限するなど、徹底したセキュリティ管理を行った。

4 鍵情報の発行について

今後、日本全国各地の高速道路で導入されるETCシステムで利用できるように、鍵情報を一元的に発行し、管理する第三者的機関が必要になる。この第三者的機関が、(財)道路システム高度化機構(ORSE)である。

ORSEでは、ETCシステムの開発にあたり、関連する道路事業者、メーカー、カード会社などと鍵発行契約を結んだうえで、各企業(道路事業者を含む)からの申請に基づき必要な鍵情報を発行し、高度なセキュリティ管理の下、申請企業(道路事業者を含む)に対して提供する。

各道路事業者においては、ORSEから受け取った鍵情報を安全に管理し、必要に応じて路側装置に提供する(図5)。

ETCシステムではプライバシー保護と確実な料金収受を図るために、データの認証・暗号化が行われているほか、二重三重の保護が施されている。

これらのセキュリティ規格の詳細は、“ETCセキュリティ標準規格書”などによって規定されており、これらの開示は、“ETCセキュリティ標準規格書”の貸与協定を結んだ製造メーカー以外には一切開示しないなど、運用上も厳格に管理されている。

5 当社の取組み

冒頭で述べたように、ETCは非常に注目を浴びているシステムである。当社は1995年から、建設省(当時)を中心としたETCシステムの共同研究に参画し、研究を重ねてきた。また、長年にわたる高速道路の料金収受システムの技術・ノウハウを生かし、ETCシステムの仕組み作りにも貢献してきた。そして現在、ICカードから路側装置、ETCデータ処理装

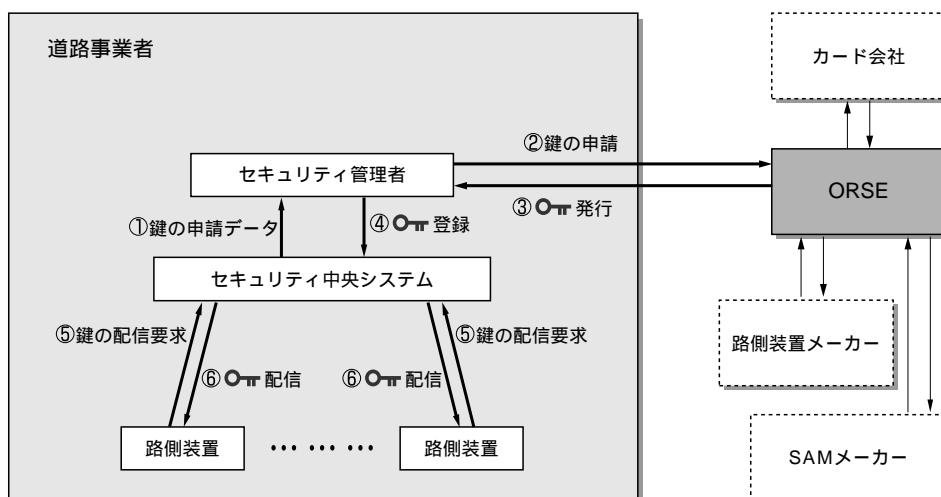


図5 . ORSEと道路事業者 道路事業者からの申請に基づき ,ORSEは鍵を発行し ,道路事業者のセキュリティ中央システムから必要に応じて自動的に配信される。

ORSE and highway operator

置 ,及びセキュリティ中央システムまで幅広く取り組み ,高い信頼性や顧客ニーズに合ったシステムを構築している。特に ,セキュリティ技術に関しては ,専門のセキュリティ技術者を中心とし ,ソフトウェア設計者 ,システム技術者が一体となって開発に当たってきた。

2000年4月からのモニタ車を対象とした試行運用においては ,当社が開発したETCシステムも稼働しており ,実績及びノウハウを積み重ねている。

6 あとがき

ETCシステムのセキュリティ中央システムを開発・納入してから1年以上経つが ,その間大きなトラブルもなく ,順調に24時間365日連続稼働している。

一方 ,ETCシステムは ,これから数年の間に全国の主な高速道路に導入される計画である。更に ,首都高速や阪神高速においては ,将来的にETCシステム対応車両だけしか利用できなくなると発表されており ,料金所での渋滞がわが国からなくなる日も夢ではないかもしれない。

また ,ETCシステムの技術を応用して ,駐車場でのキャッシュレス化やその他のサービスも検討されている。

このように ,今後IT(情報技術)化の波に乗って ,ETCシステムに限らず ,様々な形で電子料金を扱った仕組みが拡

大していくと思われる。これに伴い ,プライバシーの保護や確実な料金徴収を行うために ,セキュリティ技術がますます重要な要素となることが想定される。

文 献

- (1) ITS HAND BOOK :(財)道路新産業開発機構 ,2000 - 1.



上野 秀樹 UENO Hideki

社会インフラシステム社 社会・産業システム事業部 官公システム技術部。システムエンジニアとして道路交通システムの開発に従事。交通工学研究会会員。

Public & Industrial Systems Div.



鈴木 勝宜 SUZUKI Katsuyoshi

社会インフラシステム社 社会・産業システム事業部 官公システム技術部グループ長兼ITS・自動車事業統括部参事。ETCをはじめとするITS関連及び道路情報システムの開発に従事。

Public & Industrial Systems Div.



青木 恵 AOKI Megumi

e-ソリューション社 SI技術開発センター SI技術担当主務。情報セキュリティ技術の研究・開発に従事。

Systems Integration Technology Center