

ETC(有料道路自動料金収受)システムを支える セキュリティシステム

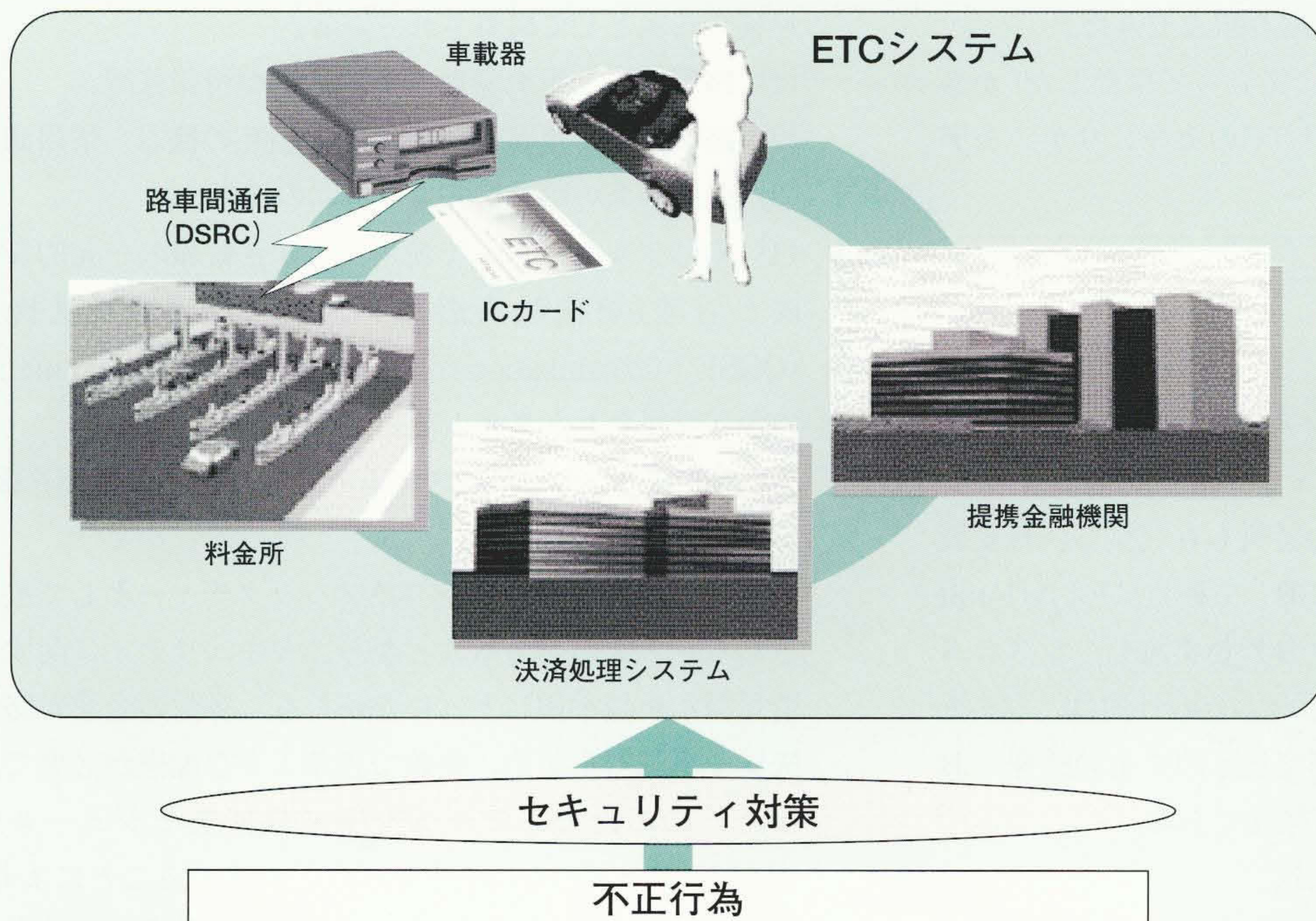
Security Systems for Electronic Toll Collection

堀江 武 Takeshi Horie

山本勝之 Katsuyuki Yamamoto

川村 巧 Takumi Kawamura

福澤寧子 Yasuko Fukuzawa



注：略語説明

ETC (Electronic Toll Collection)

DSRC (Dedicated Short-Range Communication)

ETCシステムとセキュリティ対策

ETCシステムは、料金所(車線)機器、車載器、ICカード、決済処理システム、金融機関などから成る複合的なシステムである。このシステムの安全性を確保するためには、総合的なシステムセキュリティを検討し、全般にわたるセキュリティ対策を実施する必要がある。

ETC(Electronic Toll Collection)システムは、有料道路を通行する自動車と料金所に無線機を設置し、料金収受に関する情報を交信することにより、料金所で停止することなく料金収受を実現するシステムである。

わが国のETCは2000年から本格運用を開始し、さらに今後3年間で全国の高速道路の主要な料金所をETC化することが計画され、そのために大規模な公共投資も予定されている。

一方、ETCは、無線を用いて課金情報の伝送を行うことや、不特定多数の利用者が車載器やICカードを所有するシステムであるため、システムセキュリティへの配慮が必須であった。

日立製作所は、ETCのシステムセキュリティに関する研究開発に努め、セキュリティモジュールや、かぎ情報発行システムなどの製品化・構築を進めてきた。これらにより、安全で正確な通行料の収受と、利用者のプライバシー保護に貢献している。

1 はじめに

ETC(Electronic Toll Collection)システムは、有料道路の通行料金を電子的に「キャッシュレス」で収受するためのシステムである。通行車両と料金所の間で料金計算や決済に関する情報を無線通信によってやり取りすることから、車両は停止することなく料金所を通過できるようになる。

ETCの導入により、以下のような効果が期待されて

いる。

- (1) 料金所渋滞の緩和・解消
- (2) キャッシュレス化による利便性の向上
- (3) 有料道路事業者の管理コストの削減
- (4) 料金所建設費の削減
- (5) 料金所周辺の大気汚染や騒音などを抑えることによる環境改善

ETCシステムは、料金所(車線)に設置される路側機器と車両に搭載される車載器、決済情報を保持するICカー

ド(ETCカード：車載器に挿入して使用)，料金後払いのための決済システムなどで構成される。

一方，不正行為への対抗上とプライバシー保護の必要性から，システムセキュリティへの配慮も欠かせない。日立製作所は，これまでETCのシステムセキュリティについて研究開発に努め，車載器用のセキュリティモジュールを製品化するなど積極的に取り組んできた。

ここでは，ETCの運用開始に先立って稼動した「かぎ情報発行システム」を中心に，ETCのセキュリティモデルについて述べる。

2 ETCセキュリティモデル

2.1 ETCの特質

ETCは電子的に決済を行うシステムであるため，一般的な電子課金システムのセキュリティ上の特質を持つが，これに加えて，ETC独自の特質も存在する。日立製作所は，ETCのセキュリティに関して独自にFTA(Fault Tree Analysis)を用いたリスク分析を実施し，システムセキュリティ上の特質を検討した。その目的は，(1) 正確な料金収受の実施，(2) 道路交通上の安全の確保，および(3) 個人のプライバシーの保護である。

(1) 無線を用いた課金情報の伝送

前述したように，ETCでは，通行料金の計算に必要な情報(通行区間，車種，課金用IDなど)が，無線を用いて伝送される。このため，有線系の情報通信を利用した課金システムに比べて，盗聴やデータ改ざんなどの脅威に対して脆(ぜい)弱である。

これに対応するため，無線通信部分の情報秘匿に関して十分な対策が必要である。

(2) 無人取り引き

これまで有料道路の料金収受は原則的に有人の料金所で行われてきたが，ETCの導入後は，無人で運用する料金所(車線)が増えるものと考えられる。

テレホンカードや500円硬貨の偽造問題でもわかるように，無人の料金収受では，有人の場合に比べて不正行為を実行しやすい。

このため，無人となった料金所(車線)の監視や，各機器の正当性の確認処理(認証)が重要と考えられる。

(3) 車載器の利用者所有

わが国のETCでは，車載器およびそれと組になって利用されるICカードは，利用者が対価を負担して自己所有することが原則である。普及促進の観点から，利用者に関する事前チェックには限界があるため，車載器やICカ

ードが改造，偽造されることを考慮しなければならない。

この点からも車載器やICカードの正当性について，厳重な確認処理(認証)が必要である。

2.2 セキュリティモデル

以上の特質を十分に考慮した結果，わが国のETCセキュリティモデルは，次のようなシステムセキュリティ対策を基本として構築されている。

- (1) 路側機器と車載器間の無線通信の情報秘匿
- (2) 路側機器－車載器－ICカード相互の機器・情報認証
- (3) 強度の高い暗号アルゴリズムの採用
- (4) 暗号アルゴリズムで使用するかぎ情報の一元的な生成と管理〔財団法人道路システム高度化推進機構(ORSE：Organization for Road System Enhancement)のかぎ情報発行システムを利用するもの〕

ETCの特質とETCシステムセキュリティの関連を図1に示す。

また，ETCは公共インフラストラクチャーとして整備されるシステムであることから，セキュリティに関する情報開示を最小限にとどめながらも，多数の企業が路側機器や車載器を製造，供給できるような配慮が必要であった。このため，セキュリティ機能をモジュール化(SAM：Secure Application Module)することにより，特定の条件を満たした企業だけがこれを製造できるような仕組みとしている。路側機器・車載器の製造会社は，このモジュールを購入して製品に組み入れることにより，高度なセキュリティを持った路側機器・車載器を製造することができる。

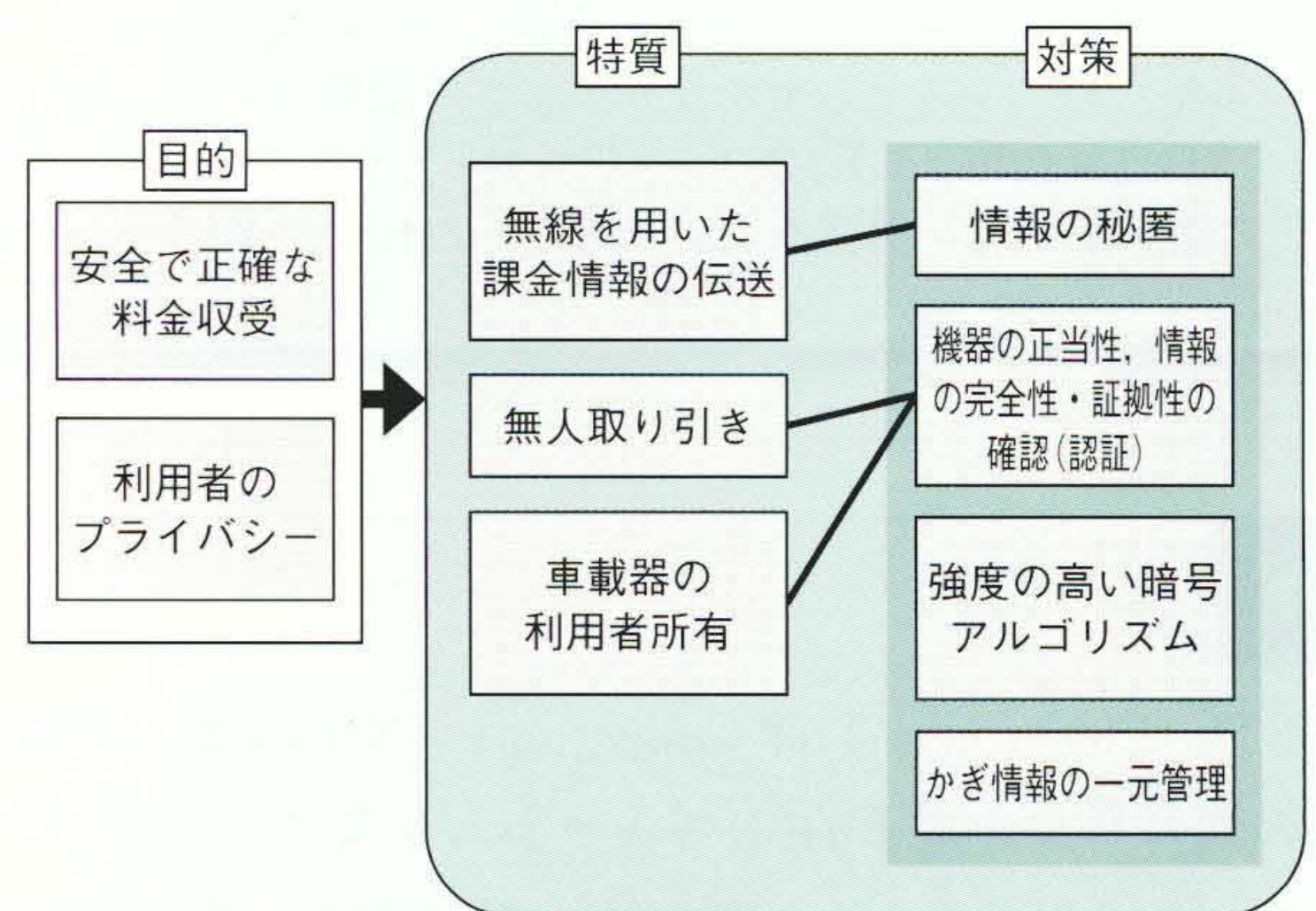


図1 ETCの特質とセキュリティ対策の関連

安全で正確な料金収受と利用者のプライバシー保護を実現するためには，情報の秘匿と機器の認証が重要である。これらを効果的に実現するために，強度の高い暗号アルゴリズムの採用と，かぎ情報の一元管理が実施されている。

なお、わが国のETCに関するセキュリティの全体モデルの詳細は、ORSEが管理する「ETCセキュリティ規格書」などによって規定されている。これらの規格では、ETCのセキュリティ機能の開示・閲覧は、製造する企業以外には厳しく制限されるなど、運用上も厳格な管理が行われている。

3 ETCかぎ情報発行システム

ETCの運用と機器の製造開始に先立ち、セキュリティ関連規格の管理と、システムで使用するかぎ情報の一元的な生成・管理を目的として、ORSEが1999年9月に設立された。日立製作所は、その中枢となる「かぎ情報発行システム」の検討・構築に参加した。

かぎ情報発行システムは、(1) セキュリティ機能製造会社からのかぎ情報発行依頼を受け付け、(2) 依頼に合わせたかぎ情報を生成し、(3) セキュリティ機能製造会

社へ配信し、(4) 生成から配信までの履歴を管理することを主な機能としている。

具体的な機能は、以下のとおりである。

- (1) 車載器SAMを開発、製造する「SAMメーカー」への車載器SAM用かぎ情報の提供
- (2) ETCカードを製造する「カードメーカー」へのICカードかぎ情報の提供
- (3) 路側機器を整備、運用する「有料道路事業者」への路側機器SAM用かぎ情報の提供
- (4) 車載器の初期化を行う「セットアップ者」への初期化情報の提供

ここで言うかぎ情報とは、プライバシー保護や確実な料金収受を行うことを目的として暗号アルゴリズムが使用する情報であり、初期化情報とは、確実な料金収受を行うために必要な車両情報などを指している。

かぎ情報発行システムは、現在、オフラインで初期化

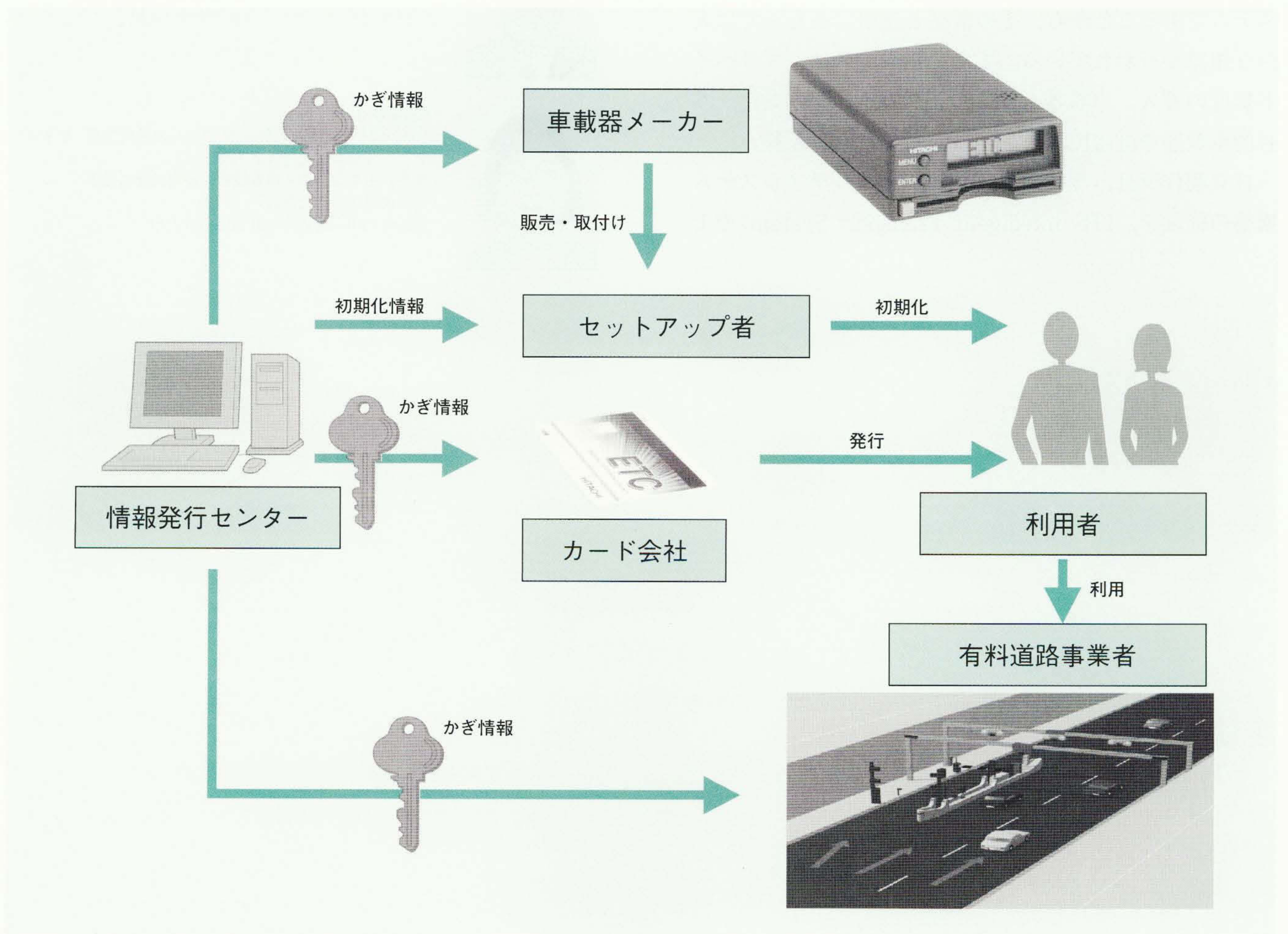


図2 かぎ情報発行・運用の概要

かぎ情報はかぎ情報発行システムで一元的に生成され、車載器メーカー・取付け業者・カード会社などを経由して利用者の手もとに渡る。利用者は、車載器とETCカードを入手してETCのサービスを利用する。

情報提供を行っているが、急激なETC利用者の増大に対応できるようにするため、オンラインによる初期化情報提供を計画している。

また、これらかぎ情報と初期化情報のやり取りでも、必要な強度で秘匿・認証の処理が実施されており、システム全体でのセキュリティが確保できるように配慮している。

かぎ情報発行関連の運用の概要を図2に示す。

4 おわりに

ここでは、ETCを支えるセキュリティモデルについて述べた。

わが国のETCシステムでは、2000年からのサービス開始に備えて、接続試験が実施されている。ETCシステムは、路側機器、車載器、ICカード、セキュリティモジュール、決済システム、かぎ情報発行システムなど、多数の機器が多数の企業によって構築されるマルチベンダシステムであることから、その構築と運用にあたっては入念な確認が行われている。また、将来的には、プリペイド制度の導入、車載器セットアップのオンライン化、多目的車載器や汎用ICカードへの展開など課題も多い。

日立製作所は、今回のETC情報セキュリティシステム構築の経験を、ITS(Intelligent Transport System)やモ

バイル情報システム、電子決済システムに広く活用し、安全でシームレスな情報社会の早期実現に貢献できるよう、鋭意努めていく考えである。

執筆者紹介



堀江 武

1986年日立製作所入社、システム事業部 公共・社会システム本部 公共システム部 所属
現在、ITS関連システムの取りまとめに従事
E-mail: horie @ cm.head.hitachi.co.jp



山本勝之

1982年日立製作所入社、電力・電機グループ 社会システム事業部 情報システム部 所属
現在、ITS関連システムの計画に従事
E-mail: katsuyuki_yamamoto @ pis.hitachi.co.jp



川村 巧

1977年日立製作所入社、公共システムグループ 公共システム事業部 官公システム第5部 所属
現在、ITS関連システムの開発・設計に従事
E-mail: t-kawamura @ jkk.hitachi.co.jp



福澤寧子

1985年日立製作所入社、システム開発研究所 セキュリティシステム研究センタ 所属
現在、セキュリティ基盤技術の研究開発に従事
電子情報通信学会会員
E-mail: fukuzawa @ sdl.hitachi.co.jp