ITSにおけるセキュリティ

Security of Intelligent Transport Systems

上野　秀樹　■ UENO Hideki
鈴木　勝宜　■ SUZUKI Katsuyoshi
青木　恵　■ AOKI Megumi

道路インフラシステムの分野においてもITS（高度道路交通システム）の発展とともに，従来とは処理する内容が大きく変わってきており，個人情報や決済情報などについて，データ保護のためのセキュリティ対策が必要となってきた。実用化が進んでいるETC（ノンストップ自動料金収受システム）における個人情報や決済情報，歩行者ITSにおける個人情報など，身近なところで既に導入が進んでいる。

当社は，独自に開発した次世代暗号方式において国内外から高い評価を受けており，ITS分野において今後新たなサービスが展開された場合にも，国際標準を考慮しつつ対応していく。

With the expansion of Intelligent Transport Systems（ITS）, security systems for personal data and settlement information are becoming increasingly important in the field of road transportation. Security systems have already been introduced in familiar fields such as the Electronic Toll Collection（ETC）system and pedestrian ITS.

Toshiba's original new cipher method has been highly evaluated in many countries. We will continue making efforts to respond to new services in ITS fields taking international standards into consideration.

1 まえがき

情報処理の分野においては，近年のネットワーク化やコンピュータの処理能力の向上により，取り扱うデータの増大，処理の高度化，業務範囲の拡大が進んでいる。このため，システムやデータが攻撃にさらされるリスクは高まっている。また，ひとたび被害が発生すると，その影響は非常に大きなものになる。

一方，道路インフラシステムは従来，道路・交通に関する情報処理や監視制御を目的としていた。しかし，ITSの導入に伴い，取り扱うデータや処理内容は大きく変わってきている。

例えば，課金情報や個人情報など，従来の道路インフラシステムでは取り扱わなかったようなデータも取り扱うようになってきている。このような背景のなか，ITS分野においてもセキュリティの必要性，重要性が次第に高まってきている。

ここでは，ITSにおけるセキュリティの位置づけと当社の取組み，今後の展望について述べる。

2 セキュリティとは

インターネットに代表されるオープンネットワークシステムが急激に普及している。このようなネットワーク化やコンピュータ利用の一般化により便利になる反面，第三者による通信データの盗聴や改ざん，センターシステムへの侵入による不正行為など様々な問題が生じる。

これらの問題に対応するため，セキュリティ対策を施す必要がある。一口にセキュリティ対策といっても，ネットワークを介しての不正侵入を防ぐファイアウォールから，データの暗号化，建物の入退室管理まで幅広い。以下にセキュリティ要素技術について，いくつか例を挙げて概要を説明する。

2.1 ネットワークを介した不正の防止

“ファイアウォール”とはその名前のとおり，もともとは火災時に他の建物へ火が回るのをせき止める防火壁のことである。ネットワークシステムにおいては，外部からの不正アクセスをせき止めるために，ネットワーク間に設置して通信を制御する装置及びその仕組みを言う(**図1**)。

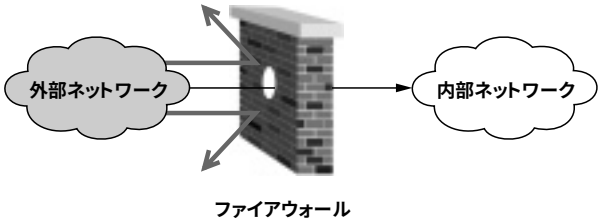

図1. ファイアウォール ― 外部からの不正アクセスをせき止める。
Firewall

ファイアウォールには，方式により“パケットフィルタリング”，“アプリケーションゲートウェイ”，“サーキットゲートウェイ”の3方式に大別できる。実際のファイアウォール製品では，複数の方式を採用して能力を上げていることが多い。

また，ファイアウォールでは防ぐことのできない不正アクセスやサービス妨害攻撃を検出し，即座に遮断するような製品や，近年被害が多発しているコンピュータウイルスを検知し駆除する製品なども注目されている。

2.2　データの防御

データを防御する暗号技術は，情報セキュリティを実現するうえで欠かすことのできない基本技術である。暗号を機能分類すると大きく以下の三つに分けられる。

⑴　情報秘匿
⑵　相手認証
⑶　情報改ざんチェック

このうち情報秘匿とは，いわゆるデータの暗号化である。**図2**に示すように，「ABC…」という平文が，鍵による暗号化により「KJN…」というような暗号文に変換される。平文の内容を知るためには鍵を用いて復号する必要がある。したがって，鍵を知らない第三者が暗号文を盗み見したとしても，平文の内容を知ることができない。このような暗号方式には，暗号化と復号の際に用いる鍵が同じ共通鍵方式と，暗号化と復号では異なる公開鍵方式があり，状況に応じて使い分ける。

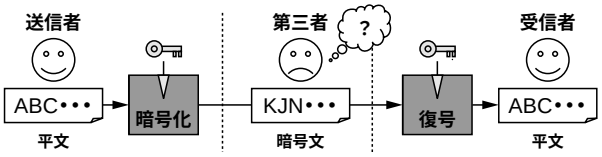

図2．情報秘匿 ― 暗号化することにより，第三者にデータの内容がわからないようにする。
Data secrecy

相手認証とは，送信データを受信者の鍵で暗号化して返信した暗号文が送信者側の鍵で復号した結果，元の送信データどおりであることを確認できた場合，受信者を信頼（鍵を保持）できる相手であると確認する方法である。

また，情報改ざんチェックには，共通鍵方式を用いたメッセージ認証と公開鍵方式を用いたデジタル署名がある。両方式とも，受信したデータが改ざんされていないかをチェックできるとともに，送信者が正しい相手であることを確認できる方式である。

2.3　ユーザー管理（個人認証）

ファイアウォールや暗号技術の適用によりネットワーク上におけるセキュリティ対策を施しても，内部に忍び込んで直接コンピュータを操作するなどの不正行為の脅威が存在する。このような不正に対しては，許可されたもの以外が建物の内部に侵入することを防ぐための入退室管理や，たとえ侵入されたとしても，コンピュータを操作する際のログオン管理などの個人認証が有効になる。

この場合，暗証番号やパスワードの確認による簡単な認証から，ICカードによる認証技術を使用したもの，指紋照合や顔照合のような生体認証によるものなど，重要度に応じた対策が必要である。

3　ITSにおけるセキュリティ

ITSにかかわるシステムにおいては，IT（情報技術）の急激な発展を背景に相互に接続されたコンピュータがネットワーク網を形成し，サービスを提供する。これらのシステムは，無線通信を利用するもの，インターネット網を利用するもの，独自の専用回線を利用するものなど様々である。

また，ネットワーク上を流れるデータや管理している情報は，課金・決済情報を扱うものや個人情報を扱うものが多い。

このため，情報の漏えい・改ざん防止を考慮する必要があり，外部からの不正アクセスを防ぐためのファイアウォールの設置や通信データの暗号化や認証など，2章で述べたセキュリティ対策が密接にかかわってくる（**図3**）。

図3．ITSにかかわるセキュリティ要素部分 ― ITSにかかわるシステムでは，各要素でセキュリティ対策が必要である。
ITS security elements

したがって，ITSにかかわるシステムを構築するためには，ユーザーに提供するサービスの利便性向上を図るとともに，セキュリティ対策を十分に検討したうえで，システムを設計する必要がある。

以下に，具体的なITSサービスを例に挙げ，どのようなセキュリティ対策が必要であるか（又は，実際に対応しているか）を述べる。

3.1 ETC

ETCは，高速道路において利用料金の支払いを，無線通信により停止することなく自動で行うシステムである（**図4**）。

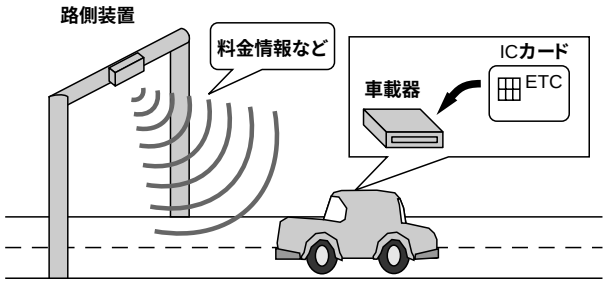

図4．ETC のイメージ ― 車側設備（ICカード，車載器）と路側装置の間で，料金のやり取りを無線で行う。
Conceptual diagram of ETC

ETCにおいては，プライバシー保護や確実な料金収受を図るために，車と料金所の路側装置との間で無線通信によりやり取りされている情報は，認証や暗号化などのセキュリティ処理が施されている。ETCで施されているセキュリティ対応要素を**図5**に示す。

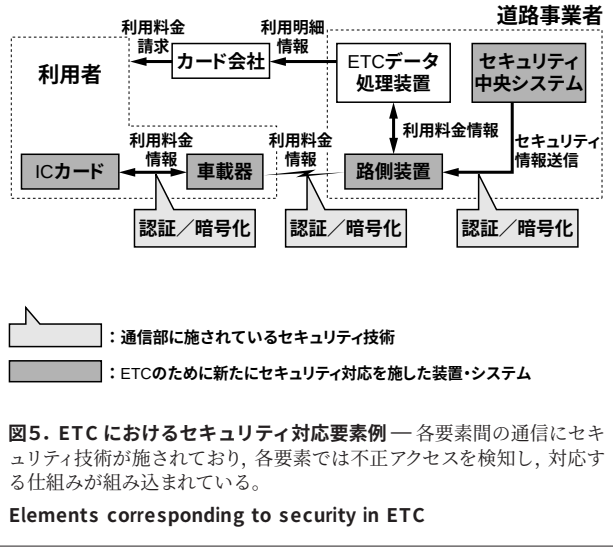

図5．ETC におけるセキュリティ対応要素例 ― 各要素間の通信にセキュリティ技術が施されており，各要素では不正アクセスを検知し，対応する仕組みが組み込まれている。
Elements corresponding to security in ETC

更に，ETCにおけるセキュリティの仕組みを実現するために，認証や暗号に用いる鍵情報の発行・管理を行う別のセキュリティ対策が必要となり，システム面及び運用面を含めて厳重に管理している。

3.2 歩行者 ITS

携帯電話やPDA（携帯情報端末）の普及に伴い注目されてきている歩行者支援システム（歩行者ITS）では，利用者により適した情報を提供するために，個人特性や行動履歴などの個人情報が扱われる場合がある。このため，プライバシー保護の観点から，個人情報流出を防ぐ対策を施す必要が生じてくる（**図6**）。

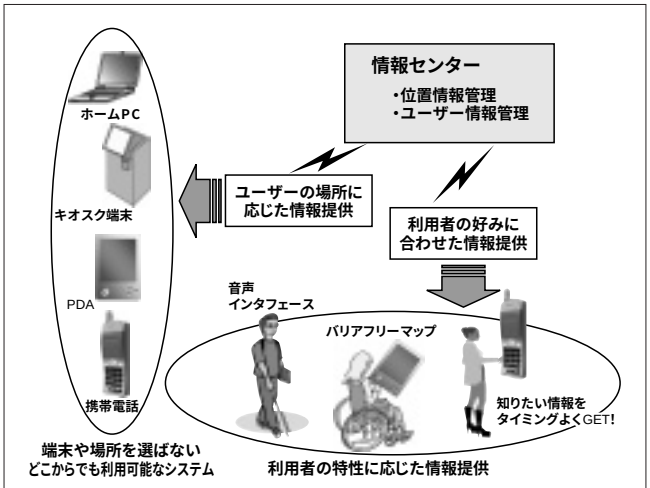

図6．歩行者 ITS における例 ― 歩行者ITSでは，個人情報を取り扱う機会が増えてくる。
Example of pedestrian ITS

3.3 車載器への情報提供

DSRC（狭域無線通信）応用システムなど，車載器への情報提供システムが実験段階に入り，注目されている。これらのシステムにおいても，情報の有償化や商品・サービス購入に伴う決済処理が発生することが予想されるため，万全のセキュリティ対策を施す必要がある。

4 当社の取組み

今後のITSと道路インフラシステムにおいて，セキュリティは更に重要性を増してくることが予想され，当社でも様々な検討がされている。ここでは，3.3節で述べた車載端末への情報提供を例に取り，必要となるセキュリティ技術のいくつかと当社の取組みを紹介する。

車載端末への情報提供では，サービスプロバイダーと車載端末間で，個人情報や課金情報と，様々なコンテンツデータがやり取りされることになる。

4.1 共通鍵暗号 Hierocrypt$_{TM}$

セキュリティ技術の基本技術は暗号技術であり，共通鍵暗号はこの数年でこれまでのDES（Data Encryption Standard）やTriple-DESに代わる次世代暗号の開発が行われてきている。当社も独自暗号方式としてHierocrypt$_{TM}$-3（128ビットブロック暗号）及びHierocrypt$_{TM}$-L1（64ビットブロック暗号）を開発し，国内外の専門家の評価において，安全性及び処理性能の面で高い評価を受けている。当社開発の一部の道路関係システムにおいても，データ秘匿の暗号方式として導入されている。今後も，当社が開発するITSと道路

インフラシステムの暗号化機能の実装には，Hierocrypt$_{TM}$の採用を進めていく。

4.2　データベースのセキュリティ

ITSと道路インフラシステムでは，個人情報や課金・決済情報などの重要情報を扱うシステムが増加している。そして，システムがインターネットなどのオープンなネットワークに接続するようになり，外部からのなりすましやデータ改ざんの危険が増大している。個人情報や課金・決済情報などの重要情報をサーバで管理する場合，その取扱いには注意が必要である。当社では，個人情報などをデータベースで管理する場合のセキュリティ対策の一つとして，データベースに保存するデータの暗号化の実現方法を検討し，一部のシステムで導入している。また，データベースのセキュリティでは，ユーザーのデータベースへのアクセス権限のチェックが重要であり，システム構築にあたっては，ユーザーの運用を十分に考慮して実装している。

4.3　耐タンパソフトウェア

車載器への情報提供システムでは，車載器や路側装置などの中継端末に認証機能や様々のアプリケーションが搭載されると予想される。端末にはソフトウェアで機能を実装する場合が増えるはずである。その場合，ソフトウェアの解読や改ざん防止のためには，ソフトウェアの耐タンパ機能(注1)が重要となってくる。当社ではソフトウェアの耐タンパ機能の研究開発を行っており，実システムへの適用も行われている。

コンテンツの配信に伴う課金・決済については，様々な方式が考えられる。ETCのようにクレジットカードによる決済も考えられるし，プリペイド方式も考えられる。車載端末の一つとして，携帯電話やPDAの利用が予想されるが，当社では携帯電話やPDAにバリューを持たせて決済を行うモバイルキャッシュの試作も行っている。

4.4　コンテンツ配信技術

車載器への情報提供システムでは，動画像などのコンテンツが配信されるようになる。当社では，コンテンツプロバイダー向けのコンテンツ配信システムの開発や，電子透かしを利用したコンテンツの保護と不正利用防止についても研究開発を行っている。

4.5　システム信頼性保証技術

実際にセキュリティ機能を実現する場合，システム全体の信頼性を確保することが重要であり，国際標準であるISO15408に準拠したセキュリティ設計及び開発が要求される。ISO15408については，電子政府システムをはじめとする官公庁向けシステムの調達要件となってくる傾向があり，ITSと道路インフラシステムなどの重要な社会インフラシステムでも適用されると予想され，対応を進めていく必要がある。

5　あとがき

ITSは実用化が始まったところであり，今後ますます広がっていくものと考えられる。

当社は，その中の基盤技術の一つであるセキュリティについていち早く着手し，ITS分野への実現を図ってきた。

今後も積極的に取り組み，ITSの高度化や発展に伴う様々な要求に応えていく。

文　献

(1)　上野秀樹，ほか．ETCシステムにおけるセキュリティ．東芝レビュー．**56**，7，2001，p.50－53.

（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。

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課長。料金収受システム，ETC，ITSの研究・開発とエンジニアリング業務に従事。

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 戦略企画担当参事。情報セキュリティ技術の研究・開発に従事。

System Integration Technology Center