セキュリティ技術（携帯個人認証，携帯情報保護）

米田　健*

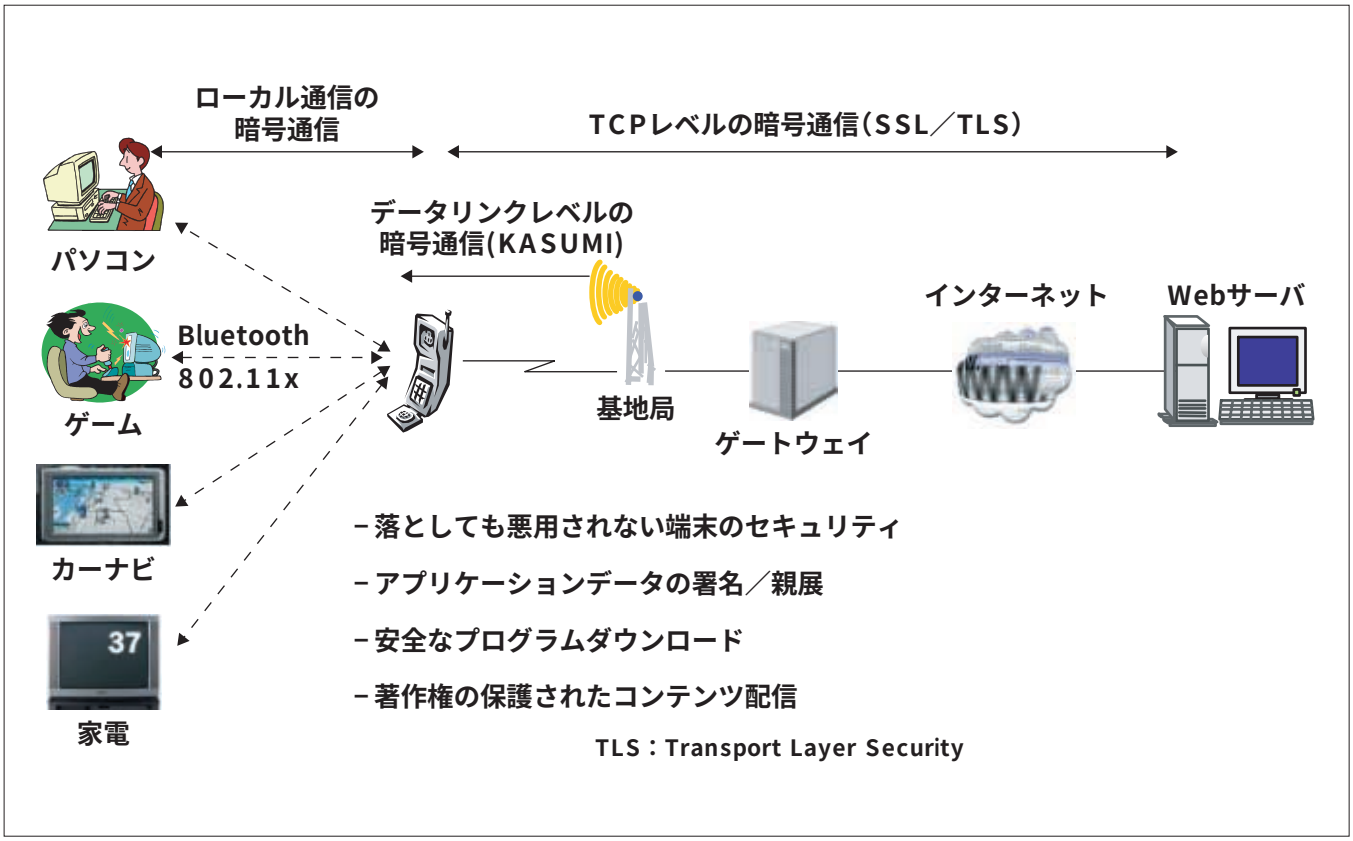
Information Security Technologies for Mobile Phones(User Authentication and Information Protection for Mobile Phones)

Takeshi Yoneda

要　旨

携帯電話の進歩は著しい。携帯電話にば“話す”という基本機能だけでなく，インターネットブラウザ，メール機能を備えるようになった。そして，第三世代携帯電話が普及し始めた今日では，デジカメ，テレビ，ラジオ，音楽再生，財布の機能まで備えつつある。

しかし，携帯電話の高機能化は，セキュリティの脅威を増大させる。主な脅威としては，通信データの盗聴，改ざん，なりすまし，オンラインコマースの取引の否認，悪性プログラムのダウンロード，コンテンツの不正コピー，落としたときの悪用，等が挙げられる。そこで，これら脅威から携帯電話を守るセキュリティ機能を組み込むことが必要となる。三菱電機は，第三世代携帯電話のW-CDMA(Wideband-Code Division Multiple Access)方式における携帯電話と網間の無線通信の暗号化に，“MISTY”をベースとした“KASUMI”を導入することに成功した。これは，第三世代携帯電話で装着が不可欠となったICチップ：UIM(User Identity Module)のデジタル署名機能を利用した，携帯電話上のブラウザとインターネット上のWebサーバの間の認証暗号通信である，SSL(Secure Socket Layer)のクライアント認証のフィジビリティを他社に先駆けて実証した。今後は，通信の上位となるアプリケーションが扱うデータに対するセキュリティ機能，携帯電話にダウンロードされるプログラムやコンテンツに対するセキュリティ機能が強化される方向に技術は進歩していくと考えられる。



携帯電話に適用されるセキュリティ技術

携帯電話のセキュリティの適用先は，通信とアプリケーションに分類できる。通信としては，データリンクの通信，End-to-endのTCP(Transmission Control Protocol)レベルの通信，ローカルな機器との通信が，また，アプリケーションとしては，落としても悪用されないセキュリティ，アプリケーションデータの署名／親展，安全なプログラムダウンロード，著作権の保護されたコンテンツ配信が挙げられる。

*情報技術総合研究所(工博)