# セキュア携帯電話システム

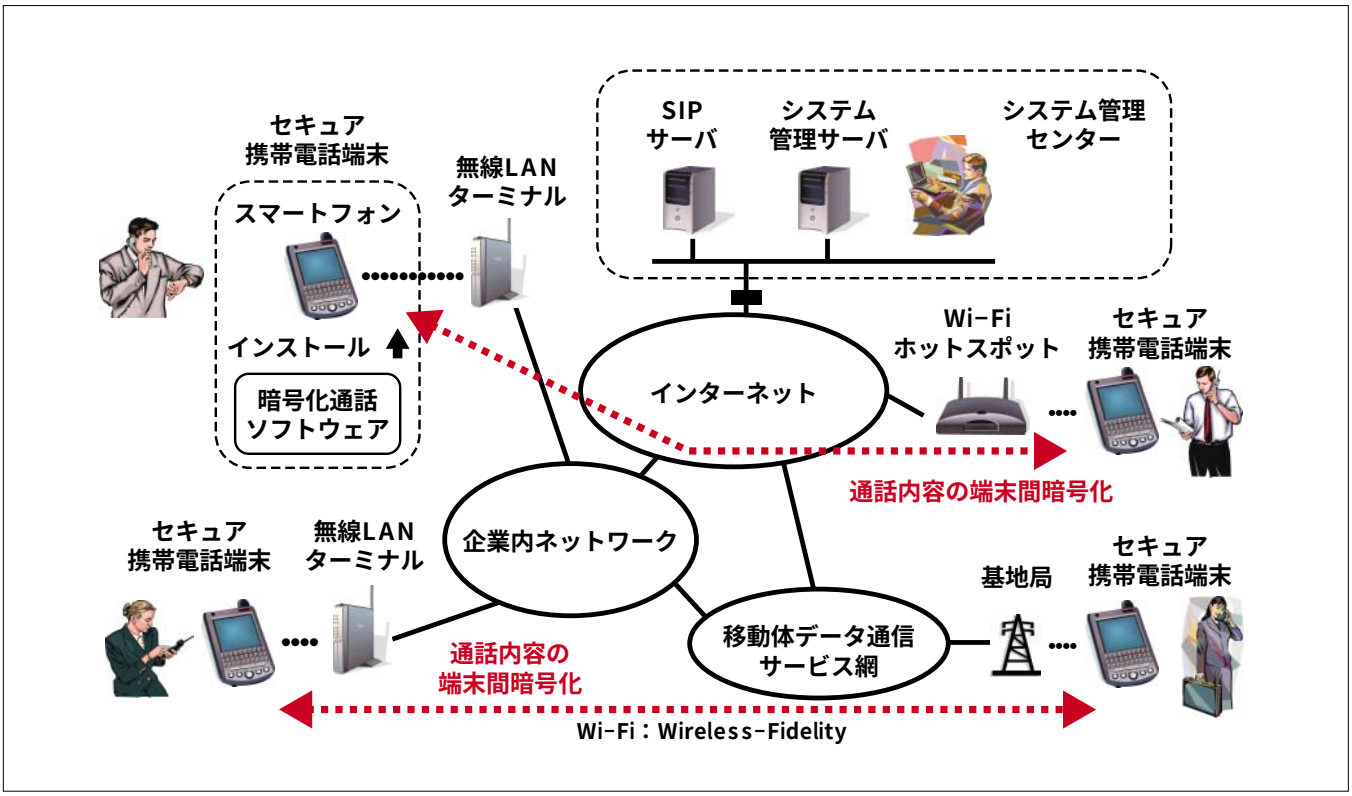
辻　宏郷*
米田　健**

## *Secure Mobile Phone System*

*Hirosato Tsuji, Takeshi Yoneda*

**要　旨**

モバイル通信端末の高性能化・高機能化や無線通信サービスの帯域拡大に伴い，端末間で音声・テキスト・静止画・動画等をリアルタイムで通信することが可能になった。機密性の高い業務に利用する場合，端末間の通信内容の盗聴防止は必要不可欠である。携帯電話と基地局，携帯情報端末と無線LAN(Local Area Network)アクセスポイント等の無線通信区間には，暗号化による盗聴防止対策が施されているが，その先のネットワークやインターネット上での通信は保護されていないため，確実な盗聴防止には，端末と端末の間でEnd-to-Endの暗号化を行う必要があり，端末同士で暗号鍵(かぎ)を共有する技術が不可欠である。また，端末を紛失した場合に備えて，端末内情報の漏洩(ろうえい)や成りすましによる不正利用等の脅威に対する対策が必要である。モバイル通信端末間通信用の暗号鍵の共有方式として，システム管理サーバで暗号鍵を一括生成し，各端末に事前配布することによって通信開始時の鍵共有処理を不要とする鍵配布・共有プロトコルを設計した。また，端末紛失・盗難時に端末の不正利用防止や端末内機密情報の保護を実現する端末管理プロトコルを開発した。これらの暗号鍵・端末の管理方式の応用例として，モバイル通信端末の音声通話を端末間のEnd-to-Endで暗号化することによって通話内容の盗聴防止を実現したセキュア携帯電話システムを設計・試作した。セキュア携帯電話端末間で暗号化通話が可能であること，通話内容の暗号化処理に伴うオーバーヘッドは無視できる範囲内であること，パケット伝達遅延や消失の少ないネットワーク状況で違和感なく通話できることを確認した。




**セキュア携帯電話システム**

セキュア携帯電話システムは，モバイル通信端末間でEnd-to-Endの暗号化を行うことによって，通話内容の盗聴を防止するシステムである。暗号化に用いる鍵は，システム管理サーバで一括生成し，各々の端末に事前配布することで，暗号化通話開始時，端末間の鍵共有処理を不要とする。端末紛失・盗難発生時に，システム管理サーバからの遠隔操作によって，端末の不正利用防止や端末内のプログラム・暗号アルゴリズム・データ等の機密情報を消去する機能を提供する。スマートフォンに暗号化通話ソフトウェアをインストールしてセキュア携帯電話端末とする。

*情報技術総合研究所　**同研究所(工博)