4-2 モバイルイーサネット上のセキュアサービスフレームワーク

4-2 Secure Service Framework on Mobile Ethernet

井上大介　黒田正博
INOUE Daisuke and KURODA Masahiro

要旨

次世代の無線ネットワーク上で展開されるモバイルサービスは、更に高度化・多様化が進み、利用者は携帯端末内に蓄えられた多数の権限情報を安全に管理する必要に迫られることになる。モバイルサービスが今後も普及・発展を遂げるためには、利便性と安全性を兼ね備えたサービス基盤の構築が必須である。本稿では、新世代モバイルネットワーク研究開発プロジェクトにおいて推進してきたモバイルイーサネット上のセキュアサービスフレームワークと、そのプロトタイプ実装について述べる。

Diverse and highly-developed mobile services will arise on next generation wireless networks. Users on the networks will have to securely manage a lot of credentials in their mobile terminals. It is necessary to provide a secure and easy-to-use framework for managing credentials independent of mobile terminals. In the New Generation Mobile Network Project, we have designed a secure service framework that separates credentials from a mobile terminal and stores them into a tamper resistant smartcard. This paper describes an overview of the secure service framework and its prototype implementation.

【キーワード】
セキュアサービスフレームワーク，権限委譲，非接触型 IC カード，サービス認証，
モバイルイーサネット
Secure service framework, Self-delegation, Contact-less smart card, Service authentication, Mobile Ethernet

1 まえがき

第 3 世代の携帯電話や無線 LAN 等に代表される無線通信技術の普及に伴い、電子メイルや Web ブラウジングはもとより、Blog や SNS サービス、電子商取引、電子オークション、電子行政サービス、オンラインバンキングなど、多種多様なサービスがモバイル環境で利用可能となってきている。無線通信技術は、高速無線 LAN や無線 MAN、第 4 世代携帯電話等の実現に向かって高速化・広域化を続けており、次世代の無線ネットワーク上で展開されるモバイルサービスもまた、更なる高度化が見込まれる。しかしながら、利用者側の観点から見ると、サービス提供者ごとに認証方法、課金方法が異なり、ある携帯電話で契約したサービスを他の端末で利用できないなど、サービスの利便性や柔軟性は高いとは言い難く、モバイルサービスの今後の普及・発展を促進するためには、一貫性を有し、利便性・柔軟性に富むサービスフレームワークが必要である。

一方、携帯電話やノート PC、PDA などの端末（以下、「携帯端末」という。）は、モバイルサービスにアクセスするための権限情報（キャッシュされたパスワードや各種証明書、携帯電話の場合にはサブスクライバ ID とそれに対応した鍵など）を端末内部に保持するようになっている。また、最近では FeliCa[1] 機能を内蔵した携帯電話も数多く登場しており、携帯端末に個人や金銭にかかわる重要な情報が集約されつつある。多くの携帯端末は、端末内部の権限情報を利用する際に、パス

ワードやバイオメトリクスによる個人認証機能を備えているが、利用者にとっては利便性が著しく低下するため、それら認証機能を利用者自身が無効化して活用しないことも多々ある。そのため、携帯端末の紛失や盗難に遭った際に被る被害はいまだ甚大である。次世代のモバイルサービスには、利便性と安全性を兼ね備えたセキュアなサービスフレームワークの構築が求められる。

以上のような要求にかんがみ、新世代モバイルネットワーク研究開発プロジェクト[2]では、安全かつ利便性の高い、次世代のモバイルサービスの基盤構築を目指した、セキュアサービスフレームワークの研究開発を行った。本稿では、このセキュアサービスフレームワークについての概要を述べ、さらに、異種無線を統合するモバイルイーサネット上での該フレームワークのプロトタイプ実装について報告する。

2 セキュアサービスフレームワークの概要

次世代の無線ネットワーク上では、多種多様なモバイルサービスの普及・発展が見込まれ、現在にも増して多くのサービス提供者の参入が期待される。また、新世代モバイルネットワーク研究開発プロジェクトにおいて研究開発を行った異種無線統合ネットワークであるモバイルイーサネット[3]では、大小複数のオペレータ(通信キャリア)が標準化されたインターフェイスに従って、様々な無線システムを相互運用するモデルを提唱している。次世代の無線ネットワークでは、複数の異なるオペレータが管理するネットワークにシームレスにアクセスし、その上で各種のモバイルサービスを享受するために、利用者がネットワークレベル及びアプリケーションレベルの権限情報を多数持つ状況が生まれてくると考えられる。

このような状況下で、利用者の利便性とシステム全体の安全性を両立させるべく、携帯端末と非接触型 IC カード、さらにそれら 2 デバイス間の権限委譲プロトコルを核としたセキュアサービスフレームワークを設計した(図 1)。

セキュアサービスフレームワークの特徴を以下に示す。

(A) 携帯端末と権限情報を分離し、権限情報は耐タンパー性 *1 を持つ非接触型 IC カードに格納する。

(B) 携帯端末は非接触型 IC カードリーダと複数の無線インターフェイス(及び後述するバイオメトリック個人認証のためのセンサ)を備える。

(C) 利用者が非接触型 IC カードを携帯端末にかざすと、IC カード内で権限情報を基に一時

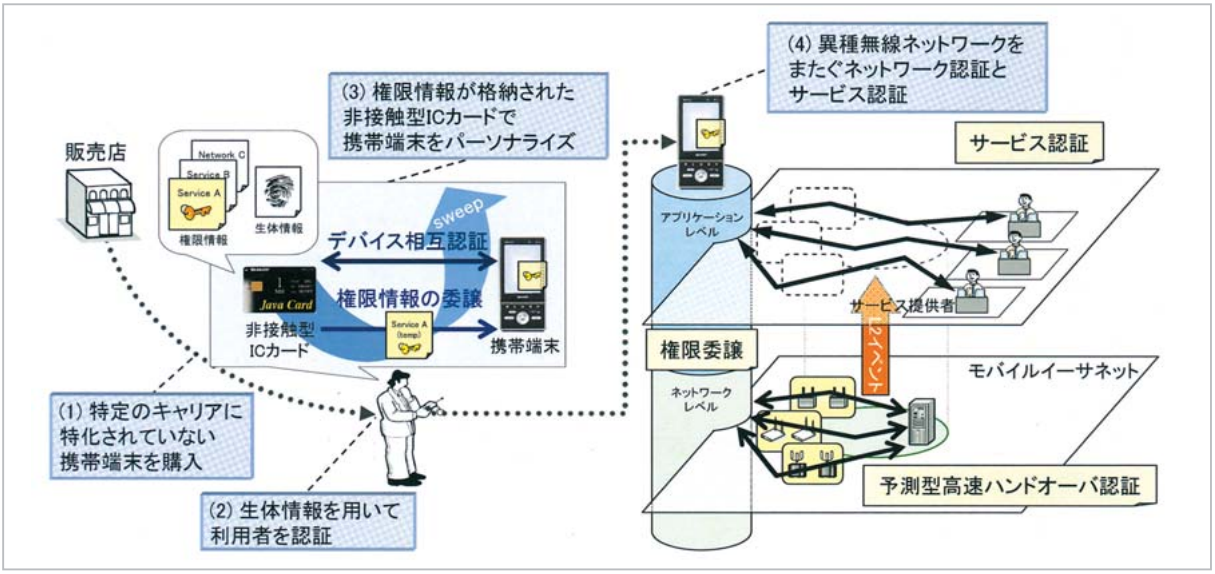

図1 セキュアサービスフレームワークの概要

*1 ソフトウェアやハードウェアの内部構造やそれらが保持している情報を、外部から不正に解析することが困難な性質。

的に有効な権限情報（以下、「一時権限」という。）が計算され、その一時権限が携帯端末へ伝送（権限委譲）される。

(D) 利用者は携帯端末に権限委譲された一時権限によって、ネットワーク認証やサービス認証を行い、モバイルサービスを享受する。

(E) 一時権限の有効期間もしくは有効回数は、サービスに応じて柔軟に設定可能である。

非接触型 IC カードには、ネットワークレベル及びアプリケーションレベルの権限情報を複数格納することができ、利用者が持つ権限情報を 1 枚の非接触型 IC カードで一元的に管理することができる。利用者は IC カードを携帯端末にかざすという簡易な操作で、一時権限を携帯端末に委譲する。携帯端末は恒久的な権限情報を内部に保持せず、IC カードから委譲された一時権限を用いて、ネットワーク／サービス認証を行う。一時権限は、サービスの種類によって有効期間や有効回数が設定可能であり、例えばネットワークアクセスのための一時権限は 24 時間有効、オンラインバンキングのための一時権限は 1 回の使用のみ有効など、柔軟な運用が可能である。そのため、携帯端末が紛失や盗難に遭った際にも、サービスの不正利用による被害を軽減することが可能である。

このように、権限情報を携帯端末から分離し、非接触型 IC カードに格納することで、利用者が安全に管理すべき対象は、携帯端末から非接触型 IC カードに移ることになる。非接触型 IC カードは耐タンパー性を有し、また、キャッシュカードやクレジットカードと同様の形状であることから利用者が使い慣れているため、携帯端末と比べて利用者は安全に管理しやすいと考えられる。しかしながら、非接触型 IC カードが盗難等に遭い、不正利用される場合の技術的な対策も講じておく必要がある。そのため、上記（A）～（E）に加え、本フレームワークは以下のようにバイオメトリック認証を導入した。

(F) 非接触型 IC カードには、利用者の生体情報（バイオメトリック情報）を格納する。

(G) 利用者が非接触型 IC カードを利用する際には、バイオメトリック認証で利用者が提示した生体情報と IC カード内の生体情報とを照合する。

(H) 照合に合格すれば、IC カードは権限委譲が可能な状態にアクティベートされる。

非接触型 IC カード内にバイオメトリック認証のための生体情報を格納し、その生体情報を用いて、利用者がカードの正当な所有者であるかどうかを検証することができる。バイオメトリック認証に合格しない限り、IC カードはアクティベートされず権限委譲を行うことはできないため、カードの盗難等による不正利用を防止できる。なお、バイオメトリック認証を行うためのセンサは携帯端末に搭載され、照合は携帯端末を介して行うことを想定している。

本フレームワークによって多数の権限情報が 1 枚の非接触型 IC カードに集約される。利用者は簡易な操作によって権限を携帯端末に委譲し、モバイルサービスを利用する。携帯端末及び IC カードは紛失や盗難に遭った際にも、その被害は従来よりも軽減される。

3 セキュアサービスフレームワークのプロトタイプ実装

本章では、セキュアサービスフレームワークのプロトタイプ実装について述べる。本プロトタイプでは、非接触型 IC カードと携帯端末間の権限委譲プロトコル及び携帯端末とサービス提供者間のサービス認証プロトコルを実装した。なお、モバイルイーサネットのネットワーク認証技術である予測型高速ハンドオーバ認証については文献[4]を参照のこと。

前章で述べたセキュアサービスフレームワークでは、携帯端末が非接触型 IC カードリーダ及びバイオメトリック認証のセンサを搭載していることを想定しているが、カードリーダの物理的サイズやそれらを搭載した携帯端末の消費電力等にかんがみると、現行の市場製品を用いて最終形を実現することはまだ難しいといえる。そこで、現行製品を用いたプロトタイプ実装を行うために、本来携帯端末に搭載されるべき非接触型 IC カードリーダとバイオメトリック認証のセンサを、携帯端末とは別のエンティティに搭載する。この新たに導入するエンティティを権限委譲ユニットと呼ぶ。

非接触型 IC カードと携帯端末との間の一時権限の委譲は、権限委譲ユニットを介して行う（図 2）。また、非接触型 IC カード内の生体情報

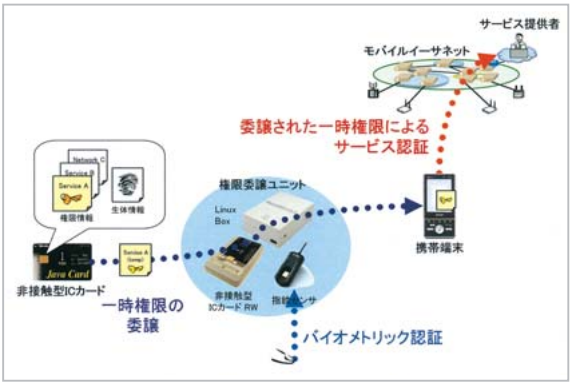

図2 権限委譲ユニットを介した権限委譲のフロー

を用いたバイオメトリック認証の処理についても権限委譲ユニット上で行う *2。なお、本プロトタイプ実装では、バイオメトリック認証に指紋認証方式を採用した *3。

携帯端末はモバイルイーサネットを介してサービス提供者にアクセスする。また、サービス提供者が提供するサービスはビデオストリーミング配信サービスとする。なお、今回のプロトタイプ実装は、共通鍵暗号系のみを用いてプロトコルを構成した。公開鍵暗号系を用いた権限委譲プロトコルについては文献[4][6]を参照のこと。

3.1 ハードウェア構成

図3に本プロトタイプのハードウェア構成を示す。

(1) 携帯端末

携帯端末はシャープ社製 Zaurus SL-6000W を使用した。SL-6000W は Bluetooth と IEEE802.11b 無線 LAN を内蔵し、コンパクトフラッシュカードスロットに 3G ネットワークカード(FOMA カード)を装着する。携帯端末は内蔵 Bluetooth を用いて権限委譲ユニットと PAN 接続し、内蔵無線 LAN 及び FOMA カードを用いてモバイルイーサネットと接続する。

(2) 権限委譲ユニット

権限委譲ユニットはぷらっとホーム社製の Linux ボックス、OpenBlockS 266 を使用した。OpenBlockS 266 は、本体に増設した 2 台の PCMCIA アダプタに Bluetooth カードと USB カードを装着する。さらに USB カードに非接触型 IC カードリーダライタと指紋センサを接続する。権限委譲ユニットは Bluetooth を用いて携帯端末と PAN 接続し、非接触型 IC カード RW を用いて IC カードと ISO/IEC14443 Type B 準拠の非接触通信を行う。

(3) 非接触型 IC カード

非接触型 IC カードは Java Card 2.1.1 [7] に準拠したシャープ社製 IC カードを使用した。本 IC カードは 16 ビット CPU と 8 KB の RAM 及び 1 MB のフラッシュメモリを内蔵する。非接触型 IC カードは、内蔵アンテナを用いて権限委譲ユニットと ISO/IEC14443 Type B 準拠の非接触通信を行う。また、IC カード登録 PC と ISO/IEC7816 準拠の接触通信を行う。

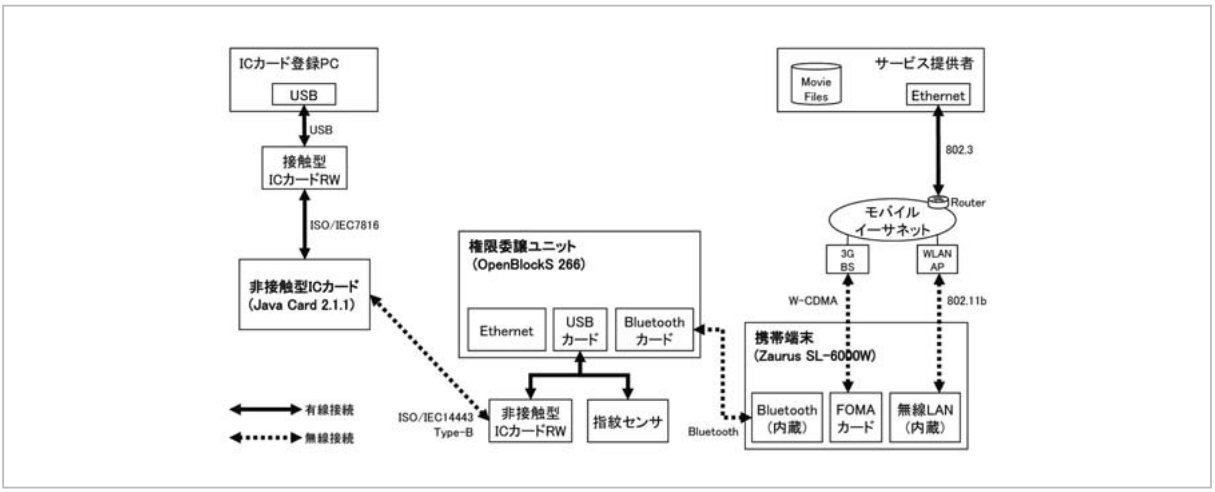

図3 ハードウェア構成

*2 ICカードの処理速度が許せば、生体情報をカード外に出さず、カード上で照合処理を行うオンカードマッチング方式が好ましい。

*3 指紋認証方式に対しては、ゼラチンを用いた指紋偽造の危険性が広く知られている[5]。将来的には虹彩認証や音声認証など複数の方式を組み合わせたマルチモーダルバイオメトリック認証の導入を検討する必要がある。

(4) サービス提供者

サービス提供者は汎用の Linux PC を使用した。サービス提供者は Ethernet インターフェイス経由でモバイルイーサネットに接続されたルータと LAN 接続する。

(5) IC カード登録 PC

IC カード登録 PC *4 は汎用の Windows PC を使用した。IC カード登録 PC は接触型 IC カードリーダライタと USB 接続し、IC カードリーダライタ経由で IC カードと ISC/IEC7816 準拠の接触通信を行う。

図 4 に実装したプロトタイプの概観を示す。

図4　プロトタイプの概観

3.2　ソフトウェア構成

図 5 に本プロトタイプのソフトウェア構成を示す。

ソフトウェア構成の詳細説明については割愛し、ここでは処理の流れについて概説する。

(1)　前準備として、IC カード登録 PC を用いて非接触型 IC カードに権限情報（鍵情報）と生体情報（指紋テンプレート）を登録する。

(2)　権限委譲ユニットに非接触型 IC カードをかざすと、権限委譲ユニットと IC カード間で事前共有鍵によるデバイス相互認証 *5 を行う。

(3)　非接触 IC カードから権限委譲ユニットに指紋テンプレートを送信する。

(4)　利用者が権限委譲ユニットの指紋センサに指紋を提示して指紋認証を行う。認証に合格すると、権限委譲ユニットは非接触型 IC カードと携帯端末間の通信を許可する。

(5)　非接触型 IC カードと携帯端末間で事前共有鍵によるデバイス相互認証 を行う。

(6)　非接触型 IC カード内で一時権限を計算し、携帯端末に権限委譲する。

(7)　携帯端末からモバイルイーサネットを介してサービス提供者の Web 閲覧を行う。

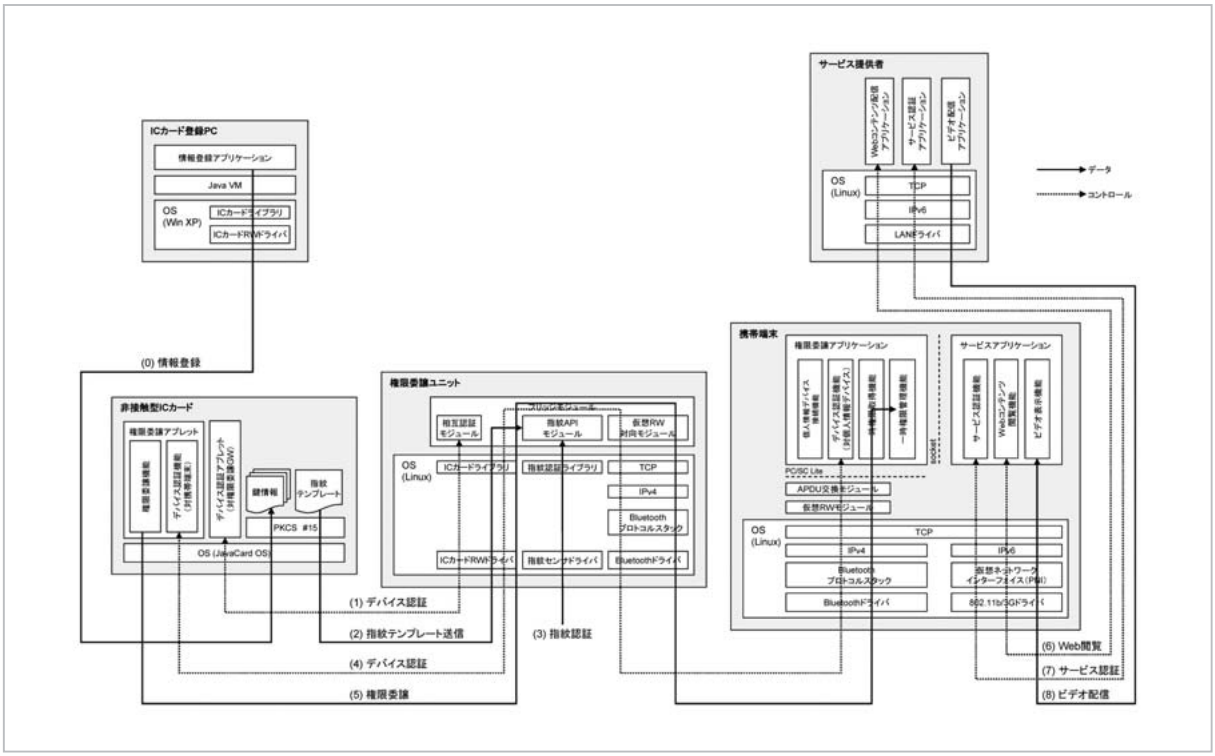

図5　ソフトウェア構成

(8)　サービス認証が必要なビデオコンテンツを閲覧する際に、携帯端末とサービス提供者間で、一時権限を鍵としたサービス認証 *6 を行う。

(9)　サービス認証に合格すると、サービス提供者がビデオ配信を開始する。

図 6 に権限委譲アプリケーション（携帯端末上）の GUI 画面の遷移例を示す。上記 (2) ～ (6) のステップに相当する。

3.3　権限委譲プロトコルとサービス認証プロトコル

非接触型 IC カードと携帯端末間で行われる権限委譲プロトコルと、携帯端末とサービス提供者間で行われるサービス認証プロトコルの詳細を示す。

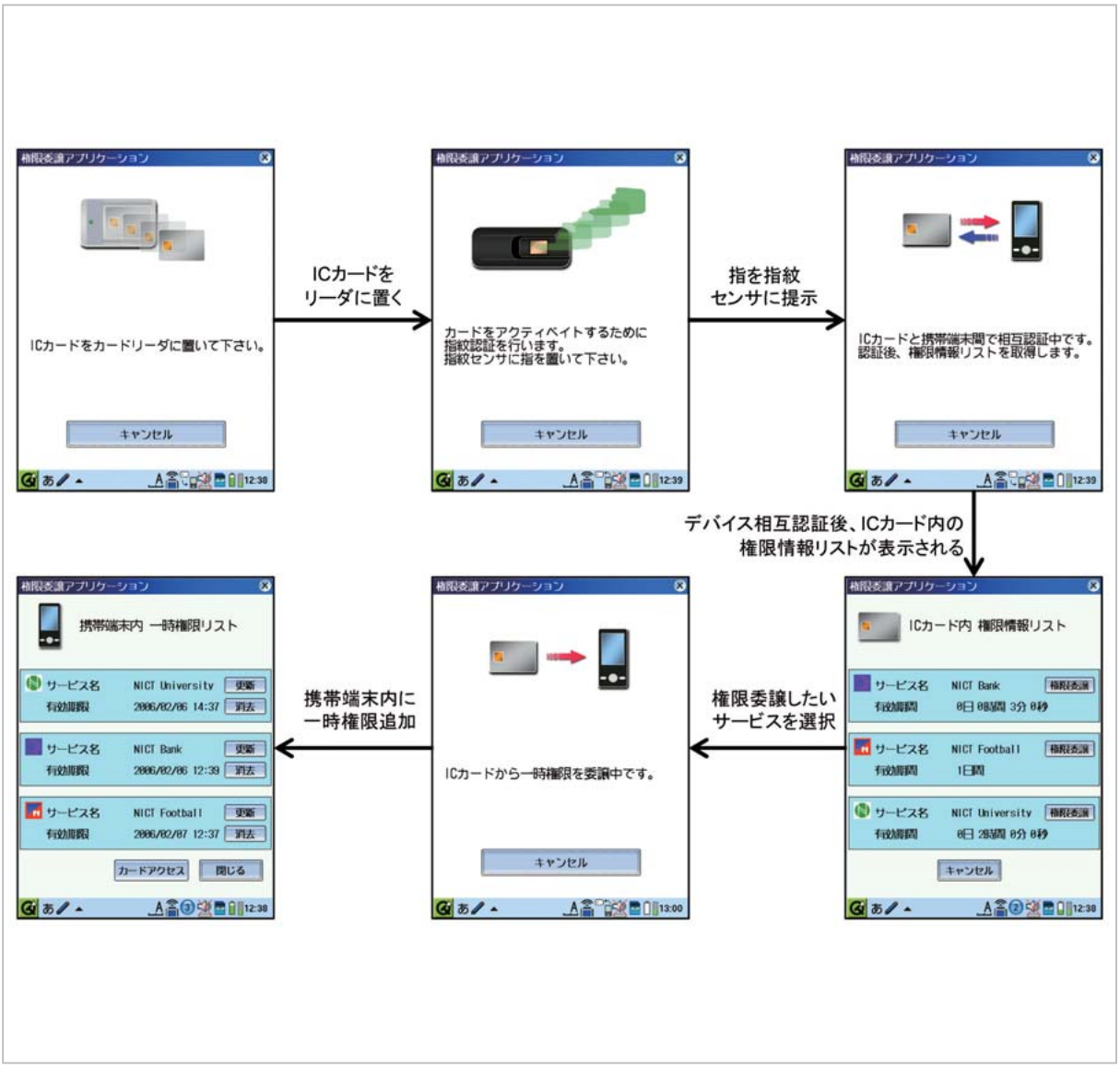

図6　権限委譲アプリケーション GUI 画面遷移例（携帯端末上）

＊4　非接触型ICカードに権限情報や生体情報を登録するためのPC。運用上はサービス提供者の機能と考えられる。
＊5　3DESを用いたチャレンジ＆レスポンス方式。権限委譲ユニットの機能が携帯端末に組み込まれた場合は必要のない処理。なお、ここで3DESを用いているのはJava Cardのバージョン上の制約である。
＊6　HMAC SHA-1を用いたチャレンジ＆レスポンス方式。なお、SHA-1は衝突が発見されているため、将来的にはSHA-256等、別のハッシュ関数に置き換えが必要である。

3.3.1 記号定義

以下に、本章以降で用いる記号を定義する。

PID	非接触型 IC カード（Personal Identity Device）
MT	携帯端末（Mobile Terminal）
SP	サービス提供者（Service Provider）
SList	SP が提供するサービス情報のリスト サービス情報（Sid，Uid，Sname，ValidTerm，SExpTime，K_{PS}）
SListMT	SList の内、携帯端末に渡す情報（Sid，Sname，ValidTerm）
Sname	SP が提供するサービスの名称
Sid	SP が提供するサービスに割り当てられた一意のサービス ID
Uid	SP が提供するサービスのユーザに割り当てられた一意のユーザ ID
R_n	乱数
ValidTerm	一時権限の有効期間
CurtTime	現在時刻
ExpTime	一時権限の有効期限， ExpTime＝CurtTime＋ValidTerm
SExpTime	サービスの有効期限
h(k，m)	メッセージ m に対する鍵 k を用いた鍵付ハッシュ関数演算
E(k，m)	メッセージ m に対する鍵 k を用いた暗号化演算
MK_s	サービスプロバイダのマスタ鍵
K_{PM}	PID と MT 間の事前共有鍵
K_{PS}	PID と SP 間の事前共有鍵（権限情報）， $K_{PS}=h(MK_s，Uid)$
EK_{PM}	PID と MT 間の暗号通信に用いられる暗号化鍵
TK_{MS}	PID と SP 間の一時的な共有鍵（一時権限）
||	データの連接
⊕	排他的論理和

3.3.2 プロトコル詳細

図 7 に権限委譲プロトコルとサービス認証プロトコルを示す。図中 (1) ～ (13) が権限委譲プロトコル、(14) ～ (21) がサービス認証プロトコルである。前提として、非接触型 IC カードと携帯端末間で共通鍵 KPM を、非接触型 IC カードとサービス提供者間で共通鍵 KPS を、それぞれ事前に共有しているものとする。また、利用者はバイオメトリック認証済であり、非接触型 IC カードは権限委譲を行えるようアクティベートされた状態からプロトコルはスタートしている（権限委譲ユニットは非接触型 IC カードと携帯端末との間で透過的に動作するため図 7 では省略する。）。

各ステップの処理の概要は以下のとおりである。

(1) ～ (7)　：非接触型 IC カードと携帯端末間のデバイス相互認証と暗号化鍵 (EK_{PM}) 共有。

(7) ～ (11)　：非接触型 IC カードから携帯端末へサービス情報のリスト (SListMT) を暗号化して送信。携帯端末から権限委譲を求めるサービス ID (Sid) と現在時刻を暗号化して送信。

(11) ～ (13)：非接触型 IC カード内で一時権限 (TK_{MS}) を計算し、ユーザ ID と一時権限の有効期限とともに暗号化して、携帯端末に送信。携帯端末は復号して、一時権限を取得。

(14) ～ (21)：携帯端末とサービス提供者間で一時権限を用いてサービス認証（相互認証）。

4 パフォーマンス評価

本章では、利用者の利便性に最も影響を与えると考えられる、非接触型 IC カードと携帯端末間の権限委譲プロトコルについて、パフォーマンス評価を行う。権限委譲ユニット (GW) を含めたプロトコルの詳細な動作を図 8 に示す。

図 8 の各ステップについて 100 回の時間計測を行い、その平均値を算出した。なお、非接触型 IC カード上では時間計測を行えないため、IC カード上での処理時間の計測は、計測対象の処理を行うアプレットを IC カードに載せて通信時間を含めた時間を計測し、次に何も処理を行わないアプレットを載せて通信時間を計測し、その時間差を IC カード上の処理時間とした。また、IC カードと携帯端末間の通信時間の計測は、計測対象となる評価項目ごとに携帯端末からデータを受信して規定のサイズのデータを返信するアプレットを IC カードに載せ、計測した時間を通信時間とした。

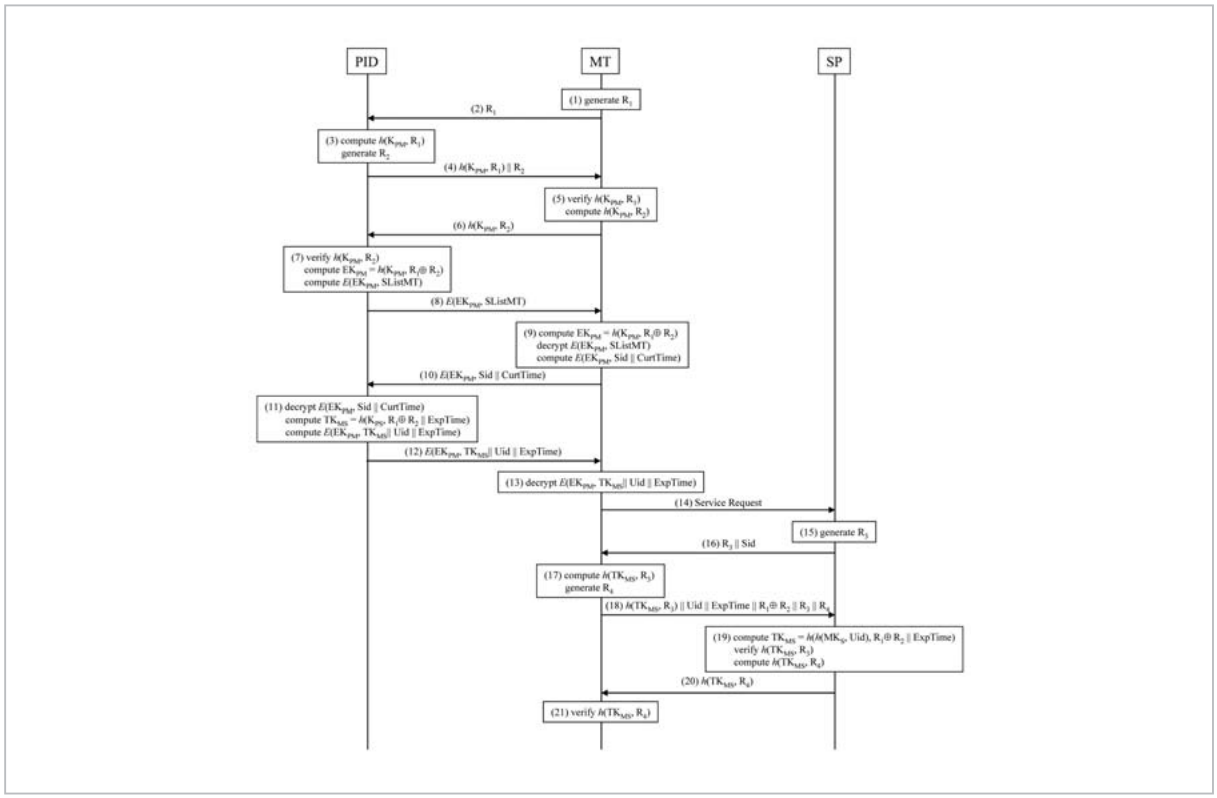

図7 権限委譲/サービス認証プロトコル

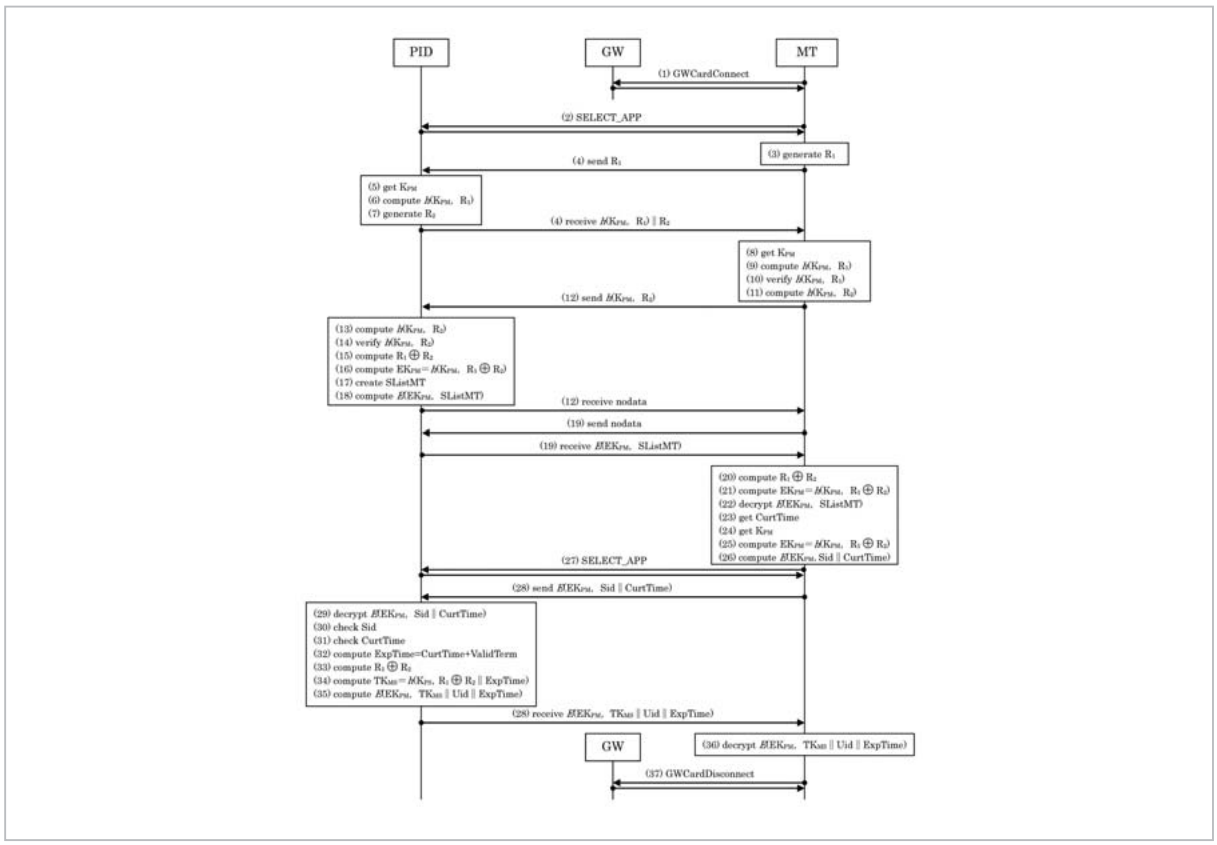

図8 権限委譲プロトコルの詳細動作

表1にパフォーマンス評価結果を示す。

表1より、携帯端末の共通鍵暗号演算（2鍵の3DES）、ハッシュ関数演算（HMAC SHA-1）にかかる時間は、どちらも5ms前後となっており、権限委譲が終了するまでの携帯端末の処理時間の合計は80msに満たない。

一方、非接触型ICカードの共通鍵暗号演算、ハッシュ関数演算はそれぞれ100ms前後となっており、権限委譲が終了するまでのICカードの処理時間の合計は1100ms強となった。

権限委譲プロトコルの中で最も時間を費やしている箇所は、権限委譲ユニットを介した通信部分であり、携帯端末とICカードとの間の往復は多くの場合300msを超えている。権限委譲が終了するまでの通信時間の合計は2600ms強であり、携帯端末と権限委譲ユニット間のBluetooth通信がボトルネックとなっている。ただし、**2**で述べたように、携帯端末が非接触型ICカードリーダと指紋センサを搭載すれば、この通信時間は無視できるようになる。

今回のプロトタイプ実装では、権限委譲プロトコルを共通鍵暗号系のみを用いて構成したため、利用者の利便性を損なわない程度のパフォーマンスが実現できた。しかしながら、権限委譲の相手を事前鍵共有したデバイスに限定しない柔軟なプロトコルを実現するためには、共通鍵暗号系と比較して計算負荷が格段に高い公開鍵暗号系を利用する必要があり、非接触型ICカードの処理能力向上が必要となってくる。

5　おわりに

本稿では、次世代の無線ネットワーク上で安全かつ利便性の高いモバイルサービス環境を実現するための、セキュアサービスフレームワークについて述べ、そのプロトタイプ実装及びパフォーマンス評価結果を示した。本フレームワークを発展させていけば、利用者が自身の権限情報を格納した非接触型ICカードのみを持ち、街中に遍在するあらゆる端末を権限委譲によって一時的にパーソナライズして利用できるようなユビキタス環境を実現できる可能性がある。

表1　パフォーマンス評価結果

評価項目番号	評価項目	時間[ms]
(1)	GWCardConnect ・非接触型ICカードRWにPIDなし	270
	GWCardConnect ・非接触型ICカードRWにPIDあり ・指紋認証前	271
	GWCardConnect ・非接触型ICカードRWにPIDあり ・指紋認証後	282
(2)	SELECT_APP	383
(3)	generate R_1	7
(4)	send R_1 + receive $h(K_{PM}, R_1) \| R_2$	337
(5)	get K_{PM}	82
(6)	compute $h(K_{PM}, R_1)$	108
(7)	generate R_2	18
(8)	get K_{PM}	6
(9)	compute $h(K_{PM}, R_1)$	5
(10)	verify $h(K_{PM}, R_1)$	5
(11)	compute $h(K_{PM}, R_2)$	5
(12)	send $h(K_{PM}, R_2)$ + receive nodata	327
(13)	compute $h(K_{PM}, R_2)$	92
(14)	verify $h(K_{PM}, R_2)$	76
(15)	compute $R_1 \oplus R_2$	74
(16)	compute $EK_{PM}=h(K_{PM}, R_1 \oplus R_2)$	91
(17)	create SlistMT	80
(18)	compute $E(EK_{PM}, SListMT)$	94
(19)	send nodata+ receive $E(EK_{PM}, SListMT)$	336
(20)	compute $R_1 \oplus R_2$	10
(21)	compute $EK_{PM}=h(K_{PM}, R_1 \oplus R_2)$	5
(22)	decrypt $E(EK_{PM}, SListMT)$	5
(23)	get CurtTime	5
(24)	get K_{PM}	6
(25)	compute $EK_{PM}=h(K_{PM}, R_1 \oplus R_2)$	5
(26)	compute $E(EK_{PM}, Sid \| CurtTime)$	5
(27)	SELECT_APP	384
(28)	send $E(EK_{PM}, Sid \| CurtTime)$ + receive $E(EK_{PM}, TK_{MS} \| Uid \| ExpTime)$	316
(29)	decrypt $E(EK_{PM}, Sid \| CurtTime)$	103
(30)	check Sid	9
(31)	check CurtTime	8
(32)	compute ExpTime=CurtTime+ValidTerm	6
(33)	compute $R_1 \oplus R_2$	74
(34)	compute $TK_{MS}=h(K_{PS}, R_1 \oplus R_2 \| ExpTime)$	105
(35)	compute $E(EK_{PM}, TK_{MS} \| Uid \| ExpTime)$	95
(36)	decrypt $E(EK_{PM}, TK_{MS} \| Uid \| ExpTime)$	5
(37)	GWCardDisconnect	277

□ 携帯端末の処理
▨ 非接触型ICカードの処理
■ 通信処理

参考文献

1 http://www.sony.co.jp/Products/felica/

2 H.Harada, M.Kuroda, H.Morikawa, H.Wakana, and F.Adachi, "The overview of the new generation mobile communication system and the role of software defined radio technology", IEICE Trans, Commun., Vol.E86-B, No.12, Dec.2003.

3 M.Kuroda, M.Inoue, A.Okubo, T.Sakakura, K.Shimizu, and F.Adachi, "Scalable Mobile Ethernet and Fast Vertical Handover", Proc. IEEE Wireless Communications and Networking Conference 2004, Vol.2, pp.659- 664, Mar.2004.

4 M.Kuroda, M.Yoshida, R.Ono, S.Kiyomoto, and T.Tanaka, "Secure Service and Network Framework for Mobile Ethernet", Kluwer Wireless Personal Communications Special Issue on Security for Next Generation Communications, Vol.29, Issue 3-4, pp.161-190, June.2004.

5 T.Matsumoto, H.Matsumoto, K.Yamada, and S.Hoshino "Impact of Artificial "Gummy" Fingers on Fingerprint Systems", Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV, Vol.4677, pp.275-289, Jan.2002.

6 S.Kiyomoto, T.Tanaka, M.Yoshida, and M.Kuroda, "Design of Security Architecture for Beyond 3G Mobile Terminals", IPSJ Journal, Vol.45, No.8, pp.1856-1872, Aug.2004.

7 http://java.sun.com/products/javacard/JC211SpecRelease.pdf

井上大介（いのうえだいすけ）
情報通信セキュリティ研究センターインシデント対策グループ研究員（旧無線通信部門ワイヤレスアプリケーショングループ研究員） 博士（工学）
情報セキュリティ

黒田正博（くろだまさひろ）
新世代ワイヤレス研究センターユビキタスモバイルグループ主任研究員（旧無線通信部門ワイヤレスアプリケーショングループ研究員） 工学博士
ユビキタスモバイルネットワークとその無線セキュリティ