

ユビキタスカードビジネス向け「KeyMobile 簡易発行システム」の開発

Development of KeyMobile Isuance System for Ubiquitous Card Business

近年、ユビキタスという言葉が一般的に使われるようになり、あらゆるモノがネットワークを介して接続される。いつでも、どこでも、誰でも、どのような機器からでも必要な情報をやり取りできるユビキタス情報社会が現実のものになってきている。

(株)日立東日本ソリューションズ（以下、当社と記す）は、このようなユビキタス情報社会に向けたユビキタスカードの研究・開発を、(株)日立製作所 ID ソリューション事業部の下で進めてきた。そして KeyMobile と呼ばれる、新しいカードを実ビジネスへ展開するにあたり KeyMobile 簡易発行システムを当社のソフトウェアパッケージ製品として開発した。当システムの開発では、安価なシステム構成で KeyMobile に効率良く認証データを書き込む（発行と呼ぶ）ことを課題とし、発行スキームや前提とする機器、大量発行時の運用面を中心に検討を進め、1 台の PC で複数の KeyMobile を同時発行するシステムを実現した。

今後は、当製品に対する顧客評価を踏まえて、より一層、実ビジネス環境で活用できるものに改良していくとともに、KeyMobile ビジネスとして企業情報システム向けのソリューション展開、さらにはユビキタス情報社会に向けたソリューションの拡充を図っていく。

畠山 誠基	Hatakeyama Seiki
梅津 徹	Umetsu Toru
藤田 文暢	Fujita Fuminobu
村上 雄一	Murakami Yuuichi

1. はじめに

ユビキタスという言葉がコンピュータの世界で初めて使われたのは、1988 年、米 Xerox のパロ・アルト研究所の「Ubiquitous Computing」の研究によってである。

当時は、研究段階であったこの言葉が、近年、実ビジネスの世界で使われるようになってきた。それは、携帯電話網を経由したインターネット接続サービスが実用化され、3G 携帯電話の登場、さらに高速な接続環境として Bluetooth、無線 LAN を搭載した端末の登場、一般家庭に浸透した ADSL をはじめとするブロードバンドの普及があり、その先には、あらゆるモノが IP ネットワーク化するとさえ言われていることが背景としてあげられる。

このような背景から、(株)日立製作所と(株)ルネサステクノロジは、あらゆる情報端末で利用出来るユビキタスカードの研究を進め、2005 年 4 月から当カードのビジネス展開を開始した。

当社では、このビジネス展開に合わせて、当カードにアプリケーションや認証情報を効率よく書き込むソフトウェアパッケージ製品を開発し、顧客業務を支援するサービス商品群と合わせてソリューション販売を開始した。

2. ユビキタス情報社会と KeyMobile

2.1 ユビキタス情報社会のイメージ

ユビキタスコンピューティングのパラダイムが支配する世界、すなわちユビキタス情報社会では、人々はコンピュータをコンピュータと意識することなく、自動車の中や公共施設、商店、街路などといったオフィスや家庭などのホームポジションから離れた場所から情報をアクセスする。端末も PC や携帯電話に限らず、PDA、車載機、キオスク端末、自販機、ゲーム機、セットトップボックスなど、多種多様にわたる（図 1）。様々な機器、様々なネットワークを使用して時間的、場所的制約を受けずに様々な情報へアクセスする世界、それが、ユビキ

タス情報社会である。そして、様々な情報へアクセスするにあたり、アクセス者の ID を明示するためのキーコンポーネントとして開発されたのが KeyMobile である。

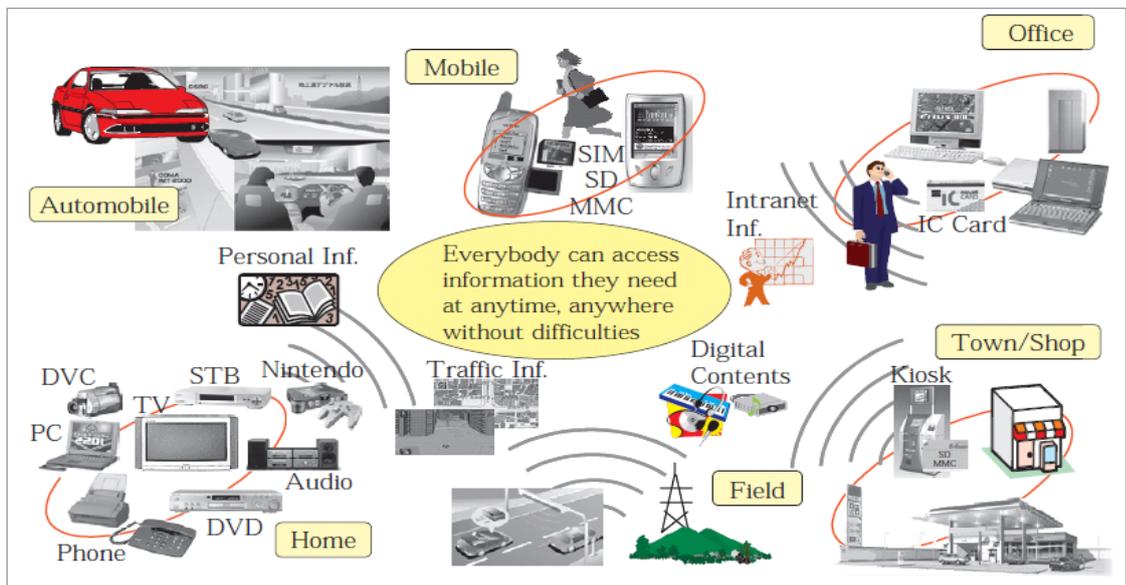


図 1 ユビキタス情報社会のイメージ © 株式会社 日立製作所

2.2 KeyMobile の特徴

(1) 形状

KeyMobile は、既に市場に流通している SD/MMC メモリカードと同じ形状で、ノート PC や PDA、デジタルカメラ、デジタル家電に搭載されているメモリカードスロットが利用できる。KeyMobile の外形を図 2 に示す。KeyMobile は、大容量のフラッシュメモリと IC カードマイコンが搭載されており、通常のメモリデバイスとして利用出来るだけでなくクレジットカードや住基カードに代表される IC カード機能を利用した本人認証により、機密性の高い情報を扱うことに適している。

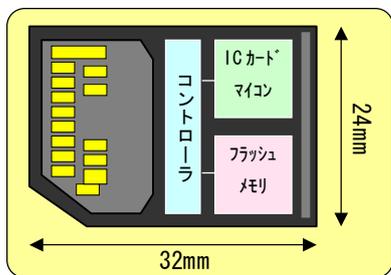


図 2 KeyMobile の外形

(2) 認証方式

KeyMobile に格納する本人を特定する認証情報は IC カード領域に格納される。この IC カード領域は

耐タンパ性と呼ばれるハッキングに抵抗する機能に守られているため、書き込んだ認証情報を不正に読み出すことは出来ない。そのため、高度な認証として、PKI (Public Key Infrastructure : 公開鍵基盤) で利用する秘密鍵やバイオメトリクス情報を格納することに適している。

一方、アクセスする情報の性質によっては、必ずしも高度な認証を必要とするものばかりではない。アクセスする情報が利用者を限定しないオープンな情報の場合は、KeyMobile を端末に差し込むことで認証を完了する簡易な手段も必要である。KeyMobile は、このような高度な認証から簡易な認証までをアクセスする情報に合わせて最適化していくことができる。

(3) 優位性

現在、市場に流通している IC カードを端末との接続性を中心に比較した結果を表 1 に示す。クレジットカードや施設の入退出管理に利用されている IC カードは、利用者に浸透している。この IC カードに電話番号などの情報を格納し、携帯電話機に内蔵したものが UIM (User Identity Module)、モバイル PC などに USB (Universal Serial Bus) インタフェースで接続して利用するものが USB トークンである。様々な機器や様々なネットワークを通じて安全に情報アクセ

スするためには、ICカード機能が必要であり、様々な端末との接続性や携帯性を評価すると KeyMobile が優位であると考えられる。また、もう1つの優位性

としてデジタルカメラを中心に広がったフラッシュメモリは記録メディアとして利用者に幅広く浸透して

表 1 ICカードの比較

比較項目	KeyMobile	ICカード	UIM ※1	USB トークン
接続性 (PC)	○ SD/MMC スロット	△ USB アダプタが必要	△ USB アダプタが必要	○ USB-IF
接続性 (PDA)	○ SD/MMC スロット	△ USB アダプタが必要	△ USB アダプタが必要	△ USB-IF
接続性 (携帯電話)	○ SD/MMC スロット	× IF なし	○ 携帯電話内蔵	× IF なし
携帯性 (外形)	○ コンパクトサイズ	△ R/W も携帯	○ コンパクトサイズ	○ コンパクトサイズ
フラッシュメモリ	○ 64MB~256MB	× 搭載なし	× 搭載なし	× 搭載なし
その他	ゲーム機、車載機など セキュアコンテンツ	クレジットとの連携 入退出との連携	コンビチップにより 非接触対応も可能	(用途限定)

※1 携帯電話には UIM (User Identity Module) と呼ばれる加入者識別用の IC カードが埋め込まれている。

いることから近い将来、KeyMobile がセキュリティ対応のブリッジングメディアとして普及することが期待されている。

3. KeyMobile 簡易発行システムの開発

3.1 KeyMobile 発行作業の検討

KeyMobile の発行作業は図 3 に示す手順で実施する。当社では (株) ルネサステクノロジーがサンプルカードの提供を開始した 2004 年 4 月から (株) 日立製作所 ID ソリューション事業部を支援するかたちで発行支援ツールの開発やカード発行作業を実施してきた。その作業では、セキュリティ面、発行スキームについて検討した。

(1) 発行時のセキュリティ検討

当カードは、認証に利用されるものであることから発行中や郵送中の盗難、すり替え、スキミング、改竄に備えて、これらの脅威に対策を施す必要がある。その為、作業工程毎にセキュリティ脅威を抽出し、それぞれの対策目標を検討した。ただし、ここで検討した対策目標は、設備や情報システム投資と密接な関係があり、実ビジネスに適用する際は、業務要件、システム要件を確定させ、守るべき情報のレベルを検討した上で、対策を決定する方針とした。

(2) 発行スキームの検討

また、この検討を踏まえて、図 3 に示す手順を「カード発行者」が実施する作業と「サービス提供事業者」が実施する作業の 2 つに分けることを考慮した。

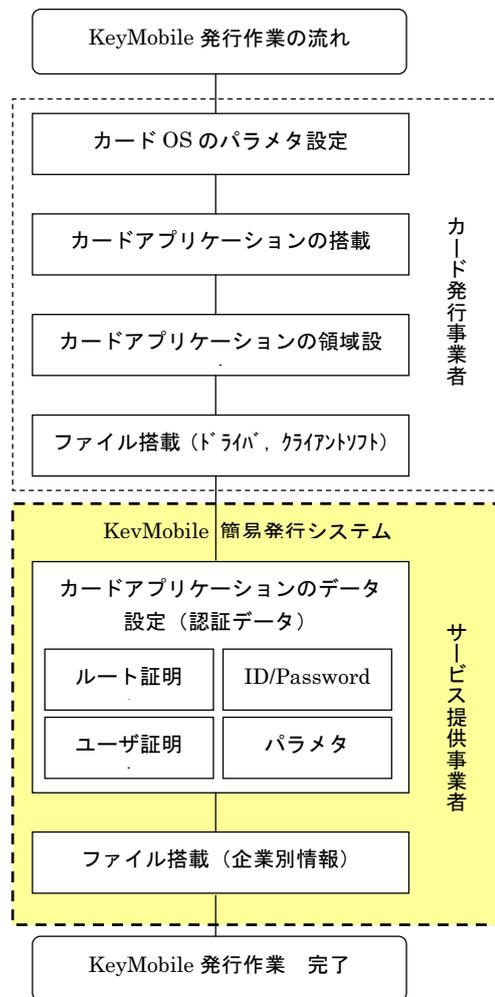


図 3 KeyMobile 発行作業の流れ

KeyMobile に設定する認証データは企業の情報や直接の利用者に紐づく情報であり、情報漏えいの観点からカード発行事業者などの第 3 者へ認証データを提供せず

サービス提供事業者が設定できることが望ましい。その為にはサービス提供事業者自身が KeyMobile へ認証データを書き込むためのツールが必要になる。それが今回開発した KeyMobile 簡易発行システムである。

3.2 KeyMobile 簡易発行システムの方式検討

KeyMobile に認証データを書き込むソフトウェアを開発するにあたり、月産 1 万枚の大量発行を視野に入れて実現方式を検討した。

(1) 発行設備の検討

KeyMobile の発行では、一般の IC カード発行装置にみられる、情報セキュリティを高めるオペレータ認証装置や秘密鍵の漏洩を防止する暗号モジュール装置などは標準構成に含めず、顧客の要件に応じて追加する構成を検討した。また、大量発行を考慮すると 1 台の PC で複数のカードを同時に発行することが出来れば発行効率が上がると考え、リーダーライタのドライバ制御も含めて並列同時発行の方式を検討した。その際も、特殊な装置を開発するのではなく市場に流通している市販の USB-HUB を使用して実現性を検討した。

(2) 大量発行の検討

大量発行を実施する場合、1 枚の KeyMobile 毎に毎回画面を介して書き込み情報を入力するのでは操作が煩雑になり、オペレーションミスで誤った認証情報を書き込む恐れがあると考えた。そのため、書き込む情報を予め CSV ファイルに纏めて入力しておき、オペレータはカードをリーダーライタへセットして実行するのみとすることが望ましいと考えた。また、操作状況を発行済みと未発行を一目で確認出来るものとする事で、さらに作業の効率が上がると考えた。操作画面のイメージを図 4 に示す。画面には、CSV ファイルの情報が一覧表示され、発行済みのものと未発行のものが区別されて表示される。

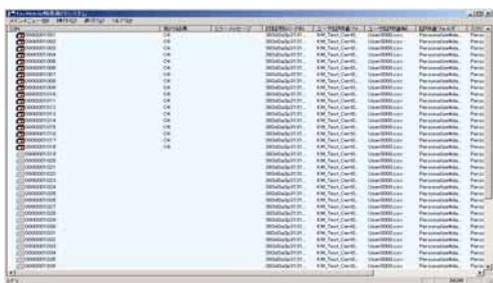


図 4 操作画面イメージ

(3) 発行運用の検討

KeyMobile は、表面にシリアル No が刻印されており、発行時にこの番号を目視確認した上でリーダーライタへ挿入する運用となる。しかしながら、この目視確認は少ない数の発行では、特に気になる作業ではないが、大量発行になるとオペレータがストレスを感じる作業であることが評価作業で明らかになった。そこで挿入されたカード内の情報をプログラムで読み出し、対応する発行情報を自動的に取得する機能を付加することでオペレータは、シリアル No を毎回確認することなく運用出来るように改良した。

(4) 発行性能の評価

発行性能は、4 ポートの USB-HUB と並列同時書き込みのサンプルプログラムを用いて実施した。その結果、1 枚の発行を 4 回繰り返した場合の時間に比較し 4 枚を同時に発行した場合の方が約 1/3 の時間で完了することが解った。また、より多重度を上げることで更なる短縮率アップが期待出来ることから性能面での並列同時書き込みの有効性は高いと考える。

(5) オペレーション端末のパフォーマンス

通常の WindowsPC を使用し、並列同時書き込みを実施することから、発行時間の実測に合わせてオペレーション端末のメモリ使用量と CPU 使用率のモニタリングを実施した。その結果、単体発行と並列同時発行の双方で、実行時の増加メモリ容量が約 15 MB であり、大きな差異は見られなかった。また、CPU 使用率に関しても、平均 10% 程度で特異な点は見られなかった。このことから、オペレーション端末のパフォーマンスは問題ないと考える。

3.3 KeyMobile 簡易発行システムの特徴

KeyMobile 簡易発行システムの概要を図 5 に示す。当システムは、カード発行事業者とサービス提供事業者がそれぞれの情報を書き込む機能を保有している。また、カードに対して効率よく認証データを書き込むために並列書き込み機能や一括発行のための CSV データ I/F、そして発行時のオペレーションを簡易なものとする GUI を提供する。オプションには顧客要件に合わせた暗号装置との連携や発行データの管理機能をカスタマイズサービスで対応することを予定している。当システムは

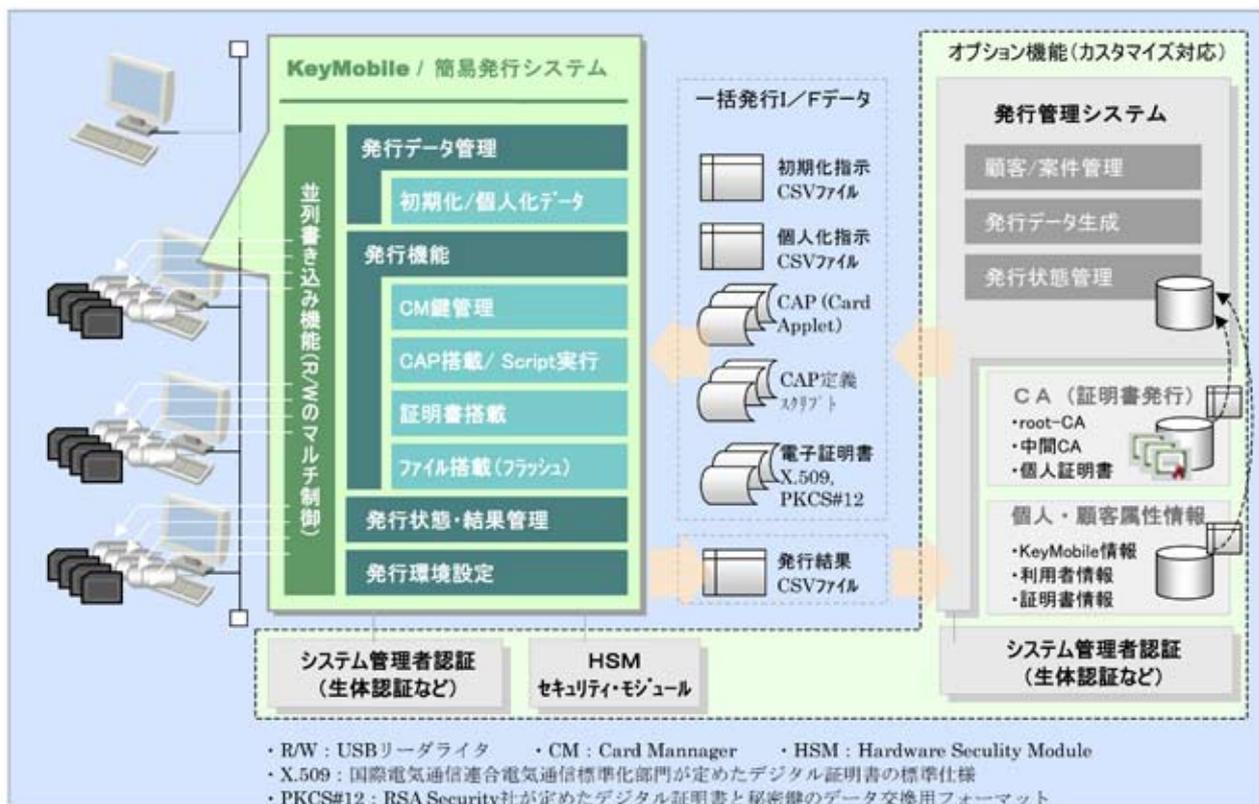


図5 KeyMobile 簡易発行システムの概要

WindowsPC を前提ハードウェアとする標準的な Windows アプリケーションとして開発しており、MFC (Microsoft Foundation Class) による GUI とマルチスレッド機能を実装している。KeyMobile リーダライタは USB 接続し、並列書き込み機能を使用する場合は、USB-HUB により複数の KeyMobile リーダライタを接続する。KeyMobile リーダライタは、KeyMobile を利用するユーザが使用するものと同じものが利用出来るため発行専用の装置を必要としない点も特徴の1つである。

3.4 サービスメニュー

(1) サービスメニュー

当システムは、顧客のサイトに KeyMobile の発行環境を構築し、顧客自らが認証データを書き込む作業を実施することを想定している。提供する GUI は、標準的な Windows アプリケーションであるため、発行の操作は簡易なものである。しかしながら、認証データそのものを扱うことに不慣れな場合、いくら操作が簡易なものであっても、実運用は難しいものである。そこで、環境構築から運用代行までを一貫してサポートするサービス群も合わせて提供している。表3にサービス内容を示す。尚

2005年6月に販売を開始してから10サイトの顧客へ製品を提供しており、2005年10月現在、約1万枚の発行実績がある。

表3 サービスメニュー

No.	サービス名称	サービス内容
1	簡易発行システム構築サービス	顧客サイトに KeyMobile 発行環境をセットアップする出張サービス
2	KeyMobile 発行代行サービス	顧客サイトで KeyMobile 発行を代行する出張サービス
3	簡易発行システム保守サービス	問合せ対応、問題解決支援、バージョンアップ、情報提供

(2) 顧客評価

適用頂いた顧客、ならびに適用を検討して頂いている顧客からの要望を表4に示す。要望については次期バージョンでのエンハンス対応を検討中である。

表4 顧客要望事項

No.	要望事項
1	入力 CSV ファイルの作成に手間がかかる
2	証明書データを書き込んだ後に自動削除して欲しい
3	サポートする電子証明書の形式を増やして欲しい
4	CA とのデータ授受方法に親和性をもって欲しい。

4. KeyMobile ビジネスの展開

4.1 「どこでも MyDeskPC」ソリューション

(株)日立製作所は、2005年1月、HDD非搭載のモバイル端末を使うことで情報漏えいを抜本的に防止するシステムを自社に導入すると発表した。セキュリティPCと呼ばれるこの端末には、業務データを一切格納できず、PC本体の盗難や紛失による情報漏えいを防止することが狙いである。この端末は、ネットワークを介して社内情報システムへアクセスするもので、ネットワークの認証データ、アクセス権の認証データ、リモートコントロール用のソフトウェアなどがKeyMobileに格納されている。当ソリューションは、2005年4月から販売を開始しており、弊社が開発したKeyMobile簡易発行システムを利用することで顧客が運用する認証基盤システムに合わせた認証データを書き込むことができる。個人情報保護法への対応、企業情報の漏洩防止に有効なソリューションとして拡販を推進していく。

4.2 モバイルコマースへの展開

2002年8月に設立されたMOPASSコンソーシアムは(株)日立製作所、松下電器産業(株)、(株)東芝の3社が幹事会社となり、金融、サービスプロバイダ、通信事業者、製造業者などの多数の業界に参加を求め、2005年度現在、49社が参加しており、MOPASSカードの活用・普及促進を目的として活動している。当コンソーシアムの狙いは、MOPASSカードによるモバイルコマースの実現であり、各種端末との接続仕様の共通化やアプリケーションの検討が行われている。MOPASSカードとは、PKI機能を搭載したICカード機能とメモリカード機能を持ち、フラッシュメモリカード用モバイルコマース拡張機能(Mc-EX)仕様、GlobalPlatform™仕様に準拠したカードである。KeyMobileにMOPASS仕様のアプリケーションを搭載することで、当カードはMOPASSカードとなる。KeyMobileの一般市場への普及に向けて(株)日立製作所を通じて、コンソーシアムに働きかけていく方針である。

5. おわりに

KeyMobile簡易発行システムは、安価なシステム構成でKeyMobileの大量発行を効率よく行うためのツールとして開発を進めてきた。この開発を通して、ICカード、認証技術、暗号化技術などの情報セキュリティ分野を経験した。ユビキタス情報社会に受け入れられるユビ

キタカードとして始まったKeyMobileビジネスは、ICカードが持つセキュリティとデジカメや映像・音楽コンテンツの世界で浸透したメモリカードという2つの機能が融合することで、あらたな価値、ビジネスフィールドを形成していくと期待できる。様々な機器、様々なネットワークを活用したサービスインフラが構築される中でKeyMobileを活かした、ユビキタス情報社会に受け入れられるソリューションが提供出来るよう、邁進していく所存である。

参考文献

- 1) 平成17年度総務省重点施策(ユビキタスネット社会(u-Japan)の実現):
<http://www.soumu.go.jp>
- 2) 郵政研究所月報(No.168 ユビキタスカード):
<http://www.japanpost.jp>
- 3) (株)日立製作所 Secure Client Solution:
http://www.hitachi.co.jp/products/secure_ubiquitous_office/secure_client_solution/sc_solution.html
- 4) MOPASS コンソーシアム:
<http://www.mopass.info>



畠山 誠基 1991年入社
ユビキタスソリューション本部
ソリューションサービス提供
sehatake@hitachi-to.co.jp



梅津 徹 1992年入社
ユビキタスソリューション本部
KeyMobile簡易発行システム開発
toumetsu@hitachi-to.co.jp



藤田 文暢 2002年入社
ユビキタスソリューション本部
ソリューションサービス提供
f-fujita@hitachi-to.co.jp



村上 雄一 2003年入社
ユビキタスソリューション本部
KeyMobile簡易発行システム開発
yumura@hitachi-to.co.jp