ポータブルソフトウェアキー（貸し借り可能な電子鍵）

納富, 貞嘉
九州大学システムLSI研究センター

馬場, 謙介
九州大学大学院システム情報科学研究院

出版情報：九州大学大学院システム情報科学研究院　２１世紀ＣＯＥプログラム　第７回研究活動説明会資料, pp.39-44, 2004-09. 九州大学大学院システム情報科学研究院
バージョン：
権利関係：

ポータブルソフトウェアキー（貸し借り可能な電子鍵）

納富 貞嘉*　　馬場 謙介**
* 九州大学システムLSI研究センター　〒816-8580　春日市春日公園6-1
E-mail: noutomi@slrc.kyushu-u.ac.jp
** 九州大学大学院システム情報科学研究院　〒816-8580　春日市春日公園6-1
E-mail: baba@c.csce.kyushu-u.ac.jp

あらまし
近年，ICチップの大容量化，高速化に伴い，非接触型ICカード機能を搭載した携帯電話が開発され，大きな注目を集めている．本研究では，建物への入退室アプリケーションを実現する，貸し借りが可能な電子鍵「ポータブルソフトウェアキー」の開発を行っている．本技術は，デジタル情報による権限の貸与，委譲に注目しこれらをセキュアに実現する．

1　はじめに

近年，非接触型ICカードを備えた携帯電話が開発され[1]，電子マネーやクレジットカードなどの様々な機能を備えることが可能である．扉の施錠・解錠に用いられる鍵としても，従来の物理的形状の鍵に代わり，ICカードによる，いわば「ソフトウェアキー」の普及が予想される．

ここで，従来の物理的形状の鍵を考えたとき，一時的に鍵を貸し出すこと，複製して渡すことはよくあることである．しかし，前述のように様々な機能を備えた携帯電話において，あるソフトウェアキーを貸そうとすると，クレジットカード機能などその携帯電話に格納されたすべての機能を貸すことになり大きなリスクを伴う．このようなことを考えると，多機能な携帯電話において，多くの機能の中からある特定のソフトウェアキーのみを貸与，複製することができれば利便性は非常に高いと考えられる．携帯電話上のソフトウェアキーに制限しなければ，このような鍵の管理ためのプロトコルは様々提案されており[2,3]，また，鍵の概念を個人に与えられる一般的な権限にまで拡張すると，権限の委譲についても考慮したものが存在する[4,5]．

本研究では，携帯電話にソフトウェアキーを搭載するためのシステムを提案する．非接触ICカードを備えた携帯電話に，様々なソフトウェアキーを搭載する機能があることを想定し，その中である特定のソフトウェアキーだけを安全に貸与，複製するプロトコルを提案する．携帯電話に特有の条件として，内部に電源を有し，通信機能（Bluetooth，赤外線通信）を持っている特徴を活かし，他の機器を介さない携帯電話間のみでのPeer to Peerによる貸与，複製を可能にする．さらに，従来の物理的形状の鍵では不可能であったユーザ毎の回数による制限や時間による制限を付加することにより，より柔軟性の高い機能を提案する．

2　準備

2.1　基本概念

ソフトウェアキーを管理，提供するシステムにおいて，ある利用者の行為に対して扉やドアを解錠・施錠することをサービスと呼ぶ．また，そのシステムの中で扉やドア，及びそれを管理するもののことをサービス提供者と呼び，サービスを受ける可能性がある者をユーザと呼ぶ．このようなシステムにおいて，サービス提供者はすべてのユーザに対して，サービスを提供するわけではなく，各ユーザについて一意な情報の照合による認証を基にサービスを提供するか否かを決定する．このとき，サービス提供者は，ユーザとサービスとの関係についての情報を保持している．また，実際には様々な観点からのサービスの分類が考えられるが，本システムでは特に時間と回数による制限に注目する．例えば，「一度だけ入室を許可する」とか，「17時までこの部屋への入室を許可する」といったものである．

先に述べたようにサービスを受ける権利を，ユーザの裁量で他のユーザに貸与，複製できることが便利な場合がある．この機能の実現は，サービス提供者が，

ユーザとサービス(およびその制限)との関係についての情報を随時更新することで技術的には容易であるが，サービス提供者の情報管理の負担が大きく，ユーザがソフトウェアキーを貸与，複製しようとした状況においてサービス提供者の情報を更新するための環境が必要となる．

本システムは，ユーザ，回数，時間によるサービス提供の管理を，(情報の漏洩等を防ぐという意味の安全性に加えて，サービス提供者の設定する制限を侵さないという意味での)安全性を保ちつつ，ユーザ間でのサービスを受ける権利の複製および譲渡を，該当するユーザ間だけでの情報の授受によって可能にする．

2.2 構成要素と表記

2.2.1 ソフトウェアキー

本研究で管理の対象とする要素であり，以下の，サービス，制限回数，および制限時間によって構成される．

型 : サービス，制限回数，および制限時間の三つ組み

表記: $k = (q, n, t) \in K$

サービス

ソフトウェアキーによって与えられる権利の内容を表す．必要ならば，回数および時間以外の制限を含む．本システムの一部，または本システムに(オンラインまたはオフラインで)接続されたシステムの変化によって表される．

型 : 文字列

表記: $q \in Q$

制限回数

サービスの回数による制限を表す．0 を含む整数，または，いくつかの条件文を伴う整数の列によって表される．

型 : 整数，または，整数と文字列の対の列

表記: $n \in N$

制限時間

サービスの時間による制限を表す．時間，または，サービスが無効の状態から有効になる時刻および有効である時間，または，サービスの失効する時刻によって表される．

型 : 整数，または，整数の対

表記: $t \in T$

2.2.2 サービス提供者

ソフトウェアキーを管理する，つまり，ユーザとソフトウェアキーの関係についての情報を保持する者．また，ユーザの認証のための情報保持し，ユーザの認証のためのデバイスを提供する．

型 : ID，ユーザ照合テーブルおよびソフトウェアキー照合テーブルを表す値の三つ組み

表記: $S = (id_S, G_S, J_S)$

2.2.3 ユーザ

サービス提供者と，認証のための情報を共有している者．後述のユーザ関数を保持している．

型 : ID，ユーザ関数およびサービス提供者照合テーブルを表す値の三つ組み

表記: $A = (id_A, f_A, H_A)$, $B = (id_B, f_B, H_B)$

2.2.4 ID

各サービス提供者およびユーザが保持する一意な文字列．

型 : 文字列

表記: $id \in ID$

2.2.5 ユーザ関数

各ユーザが保持しており，ある文字列を別の文字列へ変換する可逆関数．ユーザごとに異なる．

型 : 文字列の集合から文字列の集合への可逆関数

表記: $f \in F$

2.2.6 ユーザ照合テーブル

サービス提供者が保持しており，ユーザのIDとユーザ関数(の逆関数)との関係を表す．

型 : IDの集合からユーザ関数の逆関数の集合への関数

表記: G

2.2.7 サービス提供者照合テーブル

ユーザが保持しており，サービス提供者のIDと，そのサービス提供者について行使できる可能性のあるソフトウェアキーとの関係を表す．

型 : IDの集合からソフトウェアキーの集合の集合への関数

表記: H

2.2.8 ソフトウェアキー照合テーブル

サービス提供者が保持しており，ユーザのIDと，そのユーザが行使できる可能性のあるソフトウェアキーとの関係を表す．

型 ： IDの集合からソフトウェアキーの集合の集合への関数
表記: J

2.3 システムの構成

システム構成は次の2つにより構成される.

ユーザ

携帯電話のことを指す.
データとして, IDとしてid, ユーザ関数 f, および サービス提供者照合テーブルH を保持する.

サービス提供者

携帯電話とのインタフェースとなるリーダ及びそこから得られる情報を管理するサーバ, 管理対象となる扉・ドアより構成される.
データとして, IDとしてid, ユーザ照合テーブルG, およびソフトウェアキー照合テーブルJ を保持する.

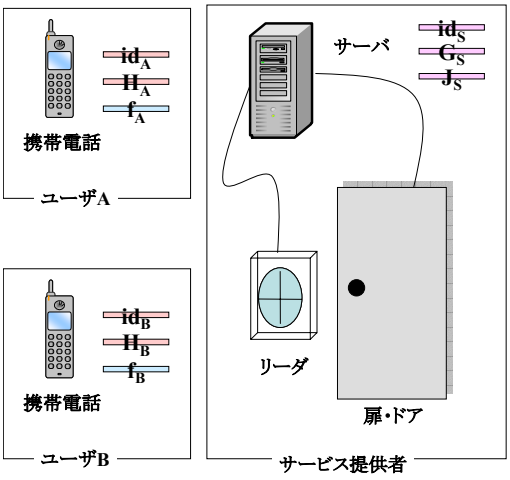

図1. システム構成

3 要求される機能

3.1 要求機能

本システムでは, 以下の機能を実現する. ここで, 本研究の位置づけを明確にするために従来の物理的形状の鍵でも機能的に実現されていた機能には★印を, 従来のソフトウェアキーでも実現されていた機能には☆印を付ける. 何も印がないもの, ★印のみのものは本研究で提案するソフトウェアキーの新しい機能である.

サービス制限の設定

サービス提供者は, 各ユーザについて, 各サービスごとの制限回数と制限時間を設定できる.

ソフトウェアキーの発行 ★ ☆

サービス提供者は, あるユーザについて設定した, あるサービスの制限回数と制限時間を, ソフトウェアキーとして与えることができる.

ソフトウェアキーの行使 ★ ☆

ユーザは, サービス提供者にソフトウェアキーを渡すことによって, 希望のサービスを受けることができる.

ソフトウェアキーの複製 ★

ユーザは, ソフトウェアキーを別のユーザに複製することができる.

複製を考慮したサービス制限の設定

サービス提供者は, 発行した各ソフトウェアキーについて, それを複製した場合の, 各ユーザについての制限回数と制限時間を設定できる.

ユーザ間のみの情報の授受 ★

ソフトウェアキーの複製によって変更される可能性があるのは, 該当する二つのユーザが保持する情報のみであり, サービス提供者との間で情報の通信は行わない.

ユーザの制限 ★

ある複製によってソフトウェアキーを得たユーザ以外のユーザが, その複製により, 新たにソフトウェアキーを得ることはない.

サービスの制限 ★ ☆

ある複製によってソフトウェアキーを得たユーザが, その複製により, そのサービス以外のサービスを受けられるようになることはない.

回数の制限

サービス提供者が設定した制限回数は, ソフトウェアキーの複製により侵害されることはない.

時間の制限

サービス提供者が設定した制限時間は, ソフトウェアキーの複製により侵害されることはない.

複製の再帰性 ★

ユーザは, 複製によって得たソフトウェアキーを, 別

のユーザに対して複製することができる. また, サービス提供者は, この再帰性による深さを制限できる.

複製履歴の取得
サービス提供者は, ユーザがソフトウェアキーを行使するための認証の際に, ソフトウェアキーの複製についての履歴を得ることができる.

3.2 要求機能の定式化

あるサービス提供者$S = (ids, Gs, Js)$ に対し, $A = (id_A, f_A, H_A)$ と $B = (id_B, f_B, H_B)$ をそれぞれ異なるユーザとする. 本システムの要求機能を以下のように定式化する.

サービス制限の設定
S はJ_S を作成できる

ソフトウェアキーの発行
S は, A に k を与えることができる. このとき, id_A のJ_S による写像には k が含まれている

ソフトウェアキーの行使
A は, S に k を渡すことによって, q を受けることができる

ソフトウェアキーの複製
A は B にソフトウェアキー $k' = (q, n', t')$ を与えることができる

複製を考慮したサービス制限の設定
S は, B から k' を受けた際の q について制限回数と制限時間を設定できる

ユーザ間のみの情報の授受
A がB へk' を与えることによって変更される可能性があるのは, A の R_A, H_A,および B の R_B, H_B のみであり, S は変わらない

ユーザの制限
A が B へ k' を渡すことによって, B 以外のユーザが新たにソフトウェアキーを得ることはない

サービスの制限
B がk' を行使して受けられるサービスは, 少なくとも q ∧ q' によって制限される

回数の制限
B が k' を行使して q を受けられる回数は, 少なくとも n ∧ n' によって制限される

時間の制限
B が k' を行使して q を受けられる時間は, 少なくとも t ∧ t' によって制限される

複製の再帰性
B は, k' を別のユーザに対して複製することができる. また, S は, この再帰性による深さを制限できる

複製履歴の取得
S は, ユーザがソフトウェアキーを行使するための認証の際に, ソフトウェアキーの複製についての履歴を得ることができる

4 提案する認証方式

4.1 プロトコル

4.1.1 通常ソフトウェアキー行使プロトコル

(1) S は, A へid_S を送る
(2) A は, id_S とH_A から, S に対して行使できるソフトウェアキーの集合を取得する
(3) A は, (2) で得たソフトウェアキーの集合の中から行使するソフトウェアキー k を選択し, S へ $id_A, f_A(k)$ を送る
(4) S は, id_A とGs から$f^{-1}{}_A$ を取得し, $f^{-1}{}_A(f_A(k)) = k$ を得る
(5) S は, id_A とJ_S からA が行使できるソフトウェアキーの集合を取得し, (4) で得たk と比較してA にサービスを提供する

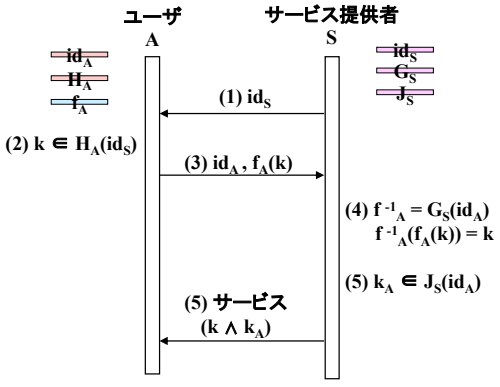

図2. 通常ソフトウェアキー行使プロトコル

4.1.2 ソフトウェアキー複製プロトコル

(1) B は, A へid_B を送る
(2) A は, B へ譲渡するソフトウェアキーの対象のサービスIDであるid_S とH_B からSに対して行使できるソフトウェアキーの集合を取得する.
(3) A は(2)で得たソフトウェアキーの集合の中から譲渡するソフトウェアキーを選択し, B へid_S, id_A, f_A (k, id_B) を送る
(4) B は, H_B を更新し, id_S にk' = (id_A, f_A (k, id_B)) を対応させる

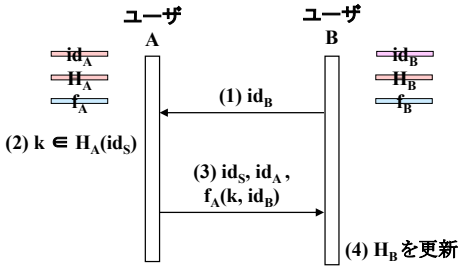

図3. ソフトウェアキー複製プロトコル

4.1.3 複製ソフトウェアキー行使プロトコル

(1) S は, B へid_S を送る
(2) B は, id_S と.H_B から, S に対して行使できるソフトウェアキーの集合を取得する
(3) B は, (2) で得たソフトウェアキーの集合の中から行使するソフトウェアキー(ここではk')を選択し, S へid_B, f_B (k') を送る
(4) S は, id_B とGs から$f^{-1}{}_B$ を取得し, $f^{-1}{}_B$ (f_B (k')) = k' = (id_A, f_A (k, id_B))を得る
(5) S は, id_A とGs から$f^{-1}{}_A$ を取得し, $f^{-1}{}_A$ (f_A(k, id_B)) = (k, id_B) を得る
(6) S は, (5) で得たid_B が(3) で得たものと一致することを確かめる
(7) S は, (4)で得たid_A とJ_S からA が行使できるソフトウェアキーの集合を取得し, (5)で得たk と比較してB にサービスを提供する

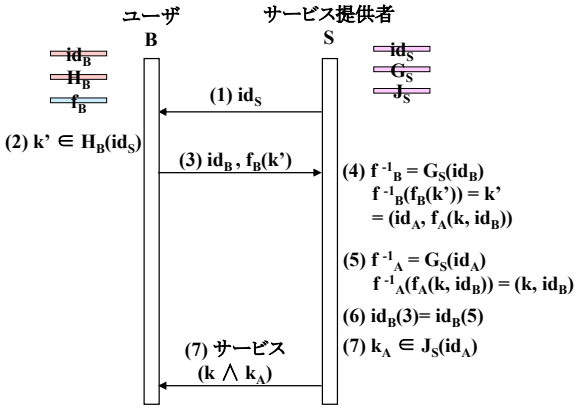

図4. 複製ソフトウェアキー行使プロトコル

4.2 検証

4.1で示したプロトコルにおいて,「3. 要求機能」が満たされていることを検証する.

サービス制限の設定

サービス提供者の持つ, ユーザ照合テーブルGにおいてIDが存在しないユーザはサービスを受けることができない. また, ユーザ照合テーブルGにおいて, IDが存在しても, ソフトウェアキー照合テーブルJ において, 該当するキーの集合が "0" であればサービスを受けることはできない.

ソフトウェアキーの発行

サービス提供者S の持つ, ユーザ照合テーブルG, ソフトウェアキー照合テーブルJ を更新することによりユーザにソフトウェアキーを発行することができる.

ソフトウェアキーの行使

ユーザAはサービス提供者にソフトウェアキーk を渡すことにより, サービスq を受けることができる.

ソフトウェアキーの複製

ユーザAは, ユーザB に対しサービス提供者にソフトウェアキーk を渡すことにより, サービスq を受けることができる.

複製を考慮したサービス制限の設定

サービス提供者は, ユーザB が行使しようとするソフトウェアキーが後に記す「複製履歴の取得」が可

能なため，複製されたキーに対する特定の制限を与えることができる．

ユーザ間のみの情報の授受

ユーザが携帯電話であることを考慮すると，Bluetoothや赤外線通信といった通信機能を使用することにより，ユーザ間のみでの情報の授受が可能となる．また，サービス提供者がその情報の授受が行われたことにより，自らの情報を更新する必要はない．

ユーザの制限

4.1.3 複製ソフトウェアキー行使プロトコル(6)において，id_B の一致を確認しているため，ユーザAがユーザBに対して複製したソフトウェアキーをユーザB以外が使用することはできない．

サービスの制限 ・ 回数の制限 ・ 時間の制限

4.1.3 複製ソフトウェアキー行使プロトコル(7)において，ユーザBの持つソフトウェアキーとサービス提供者がソフトウェアキー照合テーブルによって得られたソフトウェアキーのANDをとっているため，ユーザAがAの持つソフトウェアキーの制限を超えるようなキーを複製してもユーザBは行使することはできない．

複製の再帰性

ユーザB はユーザAにより複製されたソフトウェアキーを別のユーザに対しても複製することが可能である．また，サービス提供者は，次に記す「複製履歴の取得」が可能なため，複製回数による制限を与えることができる．

複製履歴の取得

サービス提供者は，4.1.3 複製ソフトウェアキー行使プロトコル(4)において，キーの複製元がユーザAであることを知ることができ，またそれがユーザBに対して複製されたソフトウェアキーであることを知ることができる．

5 まとめ

本研究では，近年開発された非接触ICカードを搭載した携帯電話に着目し，それによって近い将来ソフトウェアキーや電子マネーなどの様々な機能が携帯電話のみで実現されることを想定し，その中のソフトウェアキーのみを安全に複製するプロトコルを提案した．

本研究で提案したプロトコルは以下の機能を満たすプロトコルであった．

- 携帯電話間のみでソフトウェアキー複製が可能であり，複製によりサービス提供者が自らの情報を更新する必要はない
- 複製によるソフトウェアキーの乱用を防ぐ
- 別のユーザによる不正な利用を防ぐ
- 時間・回数の制限をソフトウェアキーの複製元のユーザの意志で決定できる
- 履歴の取得が可能なため，サービス提供者側で様々な制限を設けることができる．

今後の課題としては，実用に向けてプロトコルにおいて乱数の交換などを織り交ぜることにより更なる安全性の向上をはかること，また，サービス提供者が保持する照合テーブルに該当しないユーザへの複製を可能にすることが考えられる．

参考文献

[1] "iモードFelica", 株式会社エヌ・ティ・ティ・ドコモ. http://www.nttdocomo.co.jp/p_s/service/felica/

[2] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis. "The KeyNote Trust-Management System, Version 2" Request For Comments (RFC) 2704, September 1999. http://www.cis.upenn.edu/~keynote/

[3] B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen,"SPKI Certificate Theory", September 1999. http://www.ietf.org/html.charters/spki-charter.html

[4] D. Ferraiolo, R. Sandhu, S. Gavrila, R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control", ACM Transactions on Information and System Security, Vol.4, No. 3, pp.224--274, 2001.

[5] E. Barka and R. Sandhu, "A Role-based Delegation Model and Some Extensions", Proceedings of 23rd National Information Systems Security Conference, pp.101--114, 2000.