

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-318856

(P2004-318856A)

(43) 公開日 平成16年11月11日(2004. 11. 11)

(51) Int.Cl.⁷

G06F 15/00

G06F 17/60

G09C 1/00

F I

G06F 15/00

G06F 17/60

G09C 1/00

330A

410E

640E

テーマコード (参考)

5B085

5J104

審査請求 未請求 請求項の数 28 O L (全 50 頁)

(21) 出願番号 特願2004-92375 (P2004-92375)
 (22) 出願日 平成16年3月26日 (2004. 3. 26)
 (31) 優先権主張番号 特願2003-92647 (P2003-92647)
 (32) 優先日 平成15年3月28日 (2003. 3. 28)
 (33) 優先権主張国 日本国 (JP)

(71) 出願人 000002185
 ソニー株式会社
 東京都品川区北品川6丁目7番35号
 (74) 代理人 100082131
 弁理士 稲本 義雄
 (72) 発明者 板橋 達夫
 東京都品川区北品川6丁目7番35号 ソ
 ニー株式会社内
 (72) 発明者 松田 哲
 東京都品川区北品川6丁目7番35号 ソ
 ニー株式会社内
 Fターム(参考) 5B085 AA08 AC04 AE23 AE29 BE04
 BG01 BG02 CA02 CA04 CA08
 5J104 KA01 PA07 PA11

(54) 【発明の名称】 情報処理システム、情報処理装置および方法、並びにプログラム

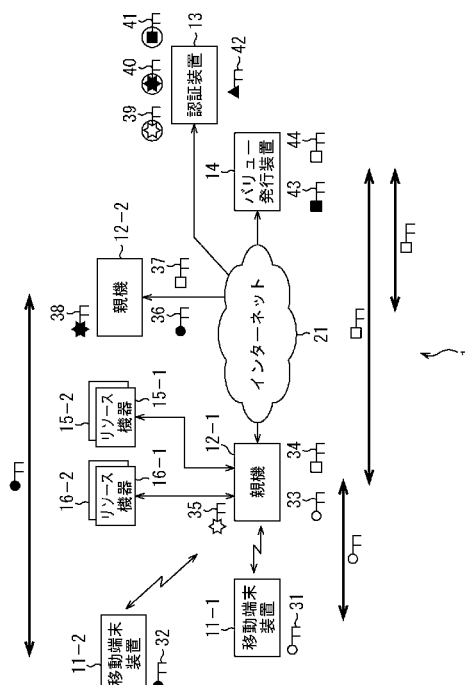
(57) 【要約】

【課題】 ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作することができるようにする。

【解決手段】 移動端末装置11-2は、親機12-2にリソース機器15のリソースを要求する。親機12-2は、親機12-1にリソース許可を要求し、親機12-1は、親機12-2に対してリソースを許可するために必要な対価を通知する。親機12-2は、バリュ発行装置14に対価の移動を要求する。バリュ発行装置14は、親機12-2の対価を親機12-1に移動し、振込み通知書を親機12-1に送信する。親機12-1は、その振込み通知書を受信し、リソース利用の権利を親機12-2を経由して移動端末装置12-2に与える。本発明は、無線通信システムに適用することができる。

【選択図】 図1

図1



【特許請求の範囲】

【請求項 1】

ユーザにより操作される端末と、
リソースを提供する第 1 の親機と、
前記ユーザの個人情報記憶する第 2 の親機と、
電子バリューを管理するバリュー装置と
を備える情報処理システムにおいて、
前記端末は、

前記第 1 の親機が提供するリソースを要求する信号を、前記第 2 の親機に送信するリ
ソース要求信号送信手段と、

10

前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得す
る第 1 の利用権取得手段と

を有し、

前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用し、

前記第 1 の親機は、

前記リソースの提供に対する対価としての電子バリューが、前記第 2 の親機から前記
第 1 の親機に振り込まれたことの振込み通知を、前記バリュー装置から受信する振込み
通知受信手段と、

前記振込み通知に応じて、前記第 2 の親機に対して、前記利用権を発行する利用権発
行手段と

20

を有し、

前記端末が、前記利用権を提示した場合に、自身が有するリソースの利用を許可し、
前記第 2 の親機は、

前記端末装置から送信されてくる、前記リソースを要求する信号に応じて、前記第 1
の親機への前記電子バリューの振込みを、前記バリュー装置に要求する電子バリュー振
込み要求手段と、

前記電子バリューの振込みに応じて、前記第 1 の親機が発行する前記利用権を取得す
る第 2 の利用権取得手段と、

前記第 2 の利用権取得手段において取得された前記利用権を、前記端末に提供する利
用権提供手段と

30

を有し、

前記バリュー装置は、

前記第 2 の親機からの要求に応じて、前記第 1 の親機に前記電子バリューを振り込む
電子バリュー振込み手段と、

前記第 1 の親機への前記電子バリューの振込み通知を、前記第 1 の親機に送信する振
込み通知送信手段と

を有する

ことを特徴とする情報処理システム。

【請求項 2】

40

ユーザにより操作される情報処理装置において、

リソースを提供する第 1 の親機が提供するリソースを要求する信号を、前記ユーザの個
人情報を記憶する第 2 の親機に送信するリソース要求信号送信手段と、

前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得する
利用権取得手段と

を備え、

前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用
する

ことを特徴とする情報処理装置。

【請求項 3】

50

前記第 2 の親機との間で、前記ユーザが前記第 2 の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段を

さらに備えることを特徴とする請求項 2 に記載の情報処理装置。

【請求項 4】

前記リソース要求信号送信手段と前記利用権取得手段は、前記第 1 の親機を介して、前記第 2 の親機とやりとりする

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 5】

前記リソース要求信号送信手段と前記利用権取得手段は、前記第 2 の親機との間で、データを暗号化してやりとりする

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 6】

前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 7】

ユーザにより操作される情報処理装置の情報処理方法において、

リソースを提供する第 1 の親機が提供するリソースを要求する信号を、前記ユーザの個人情報記憶する第 2 の親機に送信するリソース要求信号送信ステップと、

前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用する

ことを特徴とする情報処理方法。

【請求項 8】

ユーザにより操作される情報処理装置に実行させるプログラムであって、

リソースを提供する第 1 の親機が提供するリソースを要求する信号を、前記ユーザの個人情報記憶する第 2 の親機に送信するリソース要求信号送信ステップと、

前記第 1 の親機が提供するリソースを利用する利用権を、前記第 2 の親機から取得する利用権取得ステップと

を含み、

前記利用権を、前記第 1 の親機に提示して、前記第 1 の親機が提供するリソースを利用する

ことを特徴とするプログラム。

【請求項 9】

ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置において、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段と

を備え、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理装置。

【請求項 10】

前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備える

ことを特徴とする請求項 9 に記載の情報処理装置。

10

20

30

40

50

【請求項 1 1】

前記振込み通知が正当であることの認証を行う認証手段をさらに備える

ことを特徴とする請求項 9 に記載の情報処理装置。

【請求項 1 2】

前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求項 9 に記載の情報処理装置。

【請求項 1 3】

ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置の情報処理方法において、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップと

を含み、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とする情報処理方法。

【請求項 1 4】

ユーザにより操作される端末に、自身が有するリソースを提供する情報処理装置に実行させるプログラムであって、

前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、

前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップと

を含み、

前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する

ことを特徴とするプログラム。

【請求項 1 5】

ユーザにより操作される端末の前記ユーザの個人情報を記憶する情報処理装置において、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段と、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段と、

前記利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段と

を備えることを特徴とする情報処理装置。

【請求項 1 6】

前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備える

ことを特徴とする請求項 1 5 に記載の情報処理装置。

【請求項 1 7】

前記端末との間で、前記ユーザが前記個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備える

ことを特徴とする請求項 1 5 に記載の情報処理装置。

10

20

30

40

50

【請求項 18】

前記リソースは、装置、情報、または情報に対するライセンスであることを特徴とする請求項 15 に記載の情報処理装置。

【請求項 19】

ユーザにより操作される端末の前記ユーザの個人情報記憶する情報処理装置の情報処理方法において、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、 10

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とする情報処理方法。

【請求項 20】

ユーザにより操作される端末の前記ユーザの個人情報記憶する情報処理装置に実行させるプログラムにおいて、

前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、 20

前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、

前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップと

を含むことを特徴とするプログラム。

【請求項 21】

電子バリューを管理する情報処理装置において、

ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報記憶する第 2 の親機からの要求に応じて行う電子バリュー振込み手段と、 30

前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信手段と

を備えることを特徴とする情報処理装置。

【請求項 22】

前記第 1 または第 2 の親機との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段を

さらに備えることを特徴とする請求項 21 に記載の情報処理装置。

【請求項 23】

前記第 1 と第 2 の親機の電子バリューを記憶する記憶手段をさらに備え、

前記電子バリュー振込み手段は、前記記憶手段に記憶された電子バリューを書き換えることにより、前記第 2 の親機から前記第 1 の親機に対して、前記電子バリューを振り込むことを特徴とする請求項 21 に記載の情報処理装置。 40

【請求項 24】

前記電子バリュー振込み手段は、前記第 2 の親機から電子バリューを取得し、その電子バリューを前記第 1 の親機に送信することにより、

前記第 2 の親機から前記第 1 の親機に対して、前記電子バリューを振り込む

ことを特徴とする請求項 21 に記載の情報処理装置。

【請求項 25】

前記リソースは、装置、情報、または情報に対するライセンスである

ことを特徴とする請求項 21 に記載の情報処理装置。 50

【請求項 26】

前記電子バリューは、口座という形で管理され、

前記口座は、前記親機の証明書にある機器 ID、または、その機器 ID に対応付けられた ID により管理される

ことを特徴とする請求項 21 に記載の情報処理装置。

【請求項 27】

電子バリューを管理する情報処理装置の情報処理方法において、

ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第 2 の親機からの要求に応じて行う電子バリュー振込みステップと、

10

前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信ステップと

を含むことを特徴とする情報処理方法。

【請求項 28】

電子バリューを管理する情報処理装置に実行させるプログラムであって、

ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第 2 の親機からの要求に応じて行う電子バリュー振込みステップと、

前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信ステップと

20

を含むことを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理システム、情報処理装置および方法、並びにプログラムに関し、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のままユーザの嗜好に合わせた操作性で操作させることができるようにした情報処理システム、情報処理装置および方法、並びにプログラムに関する。

【背景技術】

【0002】

30

近年、携帯型のパーソナルコンピュータ、携帯電話などが普及し、多くのユーザがこれら通信機能、情報処理機能を有する小型の装置を携帯し、屋外で、あるいは移動先においてネットワークに接続してネットワークを介する通信を行っている。

【0003】

ここで、既存のインフラを利用したシステムとして、すでに存在する様々な通信網を適宜切り替えて利用するパーソナル通信サービス分散システムが提案されている（例えば特許文献 1）。このシステムは、例えば電子メールサービスや電話サービス等の異なるネットワーク通信網を統合して利用することを可能としたシステムである。

【0004】

しかしながら、このようなシステムにおいて、ユーザが外出中のような状況で、ユーザにメッセージを伝達することはできても、出先に有るたまたま身近な機器を、自らの所有する同種機種と同じ感覚で利用するなど、周囲に置いてある機器を自分に合わせた使い方をすることはできず、結局ユーザは、使い慣れた端末（例えば、PC など）を持ち運ばなくてはならなかった。

40

【特許文献 1】特開平 8-56263 号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

このような問題に対して、自宅のホームサーバに自分の嗜好等の情報を持ち、その情報を基に出先の機器の振る舞いを変化させるシステムを、本出願人が先に、特願 2003-

50

292587号で提案している。

【0006】

しかしながら、この方法では、一方的に他者のリソースを使い続けるユーザや、他者のリソースを使う機会が少ないにもかかわらず、自ら所有するリソースを提供し続けるユーザがいる場合、需給のバランスがとれなくなる恐れがある。

【0007】

そこで、ユーザが、他者の所有するリソースを利用するために必要な対価を、自分と他者の対価を管理する装置を介して支払うシステムが必要となる。

【0008】

このためには、例えばクレジットカード番号をやり取りすることによりリソースの提供者とリソースのユーザ側との間で対価をやり取りする方法が考えられる。 10

【0009】

しかしながら、クレジットカード番号はプライバシー情報のため、他者に知られるには抵抗があり、また、クレジットカードを利用するためには自分の個人情報をカード会社に登録しなければならず、つまりユーザの個人情報は対価を管理する装置に管理される。従って、ユーザが対価を管理する装置に対しても匿名のまま対価を支払い、他者の所有するリソースを利用することは困難であった。

【0010】

このため、対価を前提に公共の場で通信サービスを行っている無線LAN (Local Area Network) 等の事業者とのシームレスなサービスをユーザに提供することは困難であった。 20

【0011】

本発明は、このような状況に鑑みてなされたものであり、ユーザが移動する場合においても、移動した空間にある機器を、自分の慣れ親しんだ操作方法で操作できるなど、自分の嗜好などの個人の情報を基に機器の動作を変化させ、かつ匿名のままその対価を支払うことができるようにするものである。

【課題を解決するための手段】

【0012】

本発明の情報処理システムは、ユーザにより操作される端末と、リソースを提供する第1の親機と、ユーザの個人情報を記憶する第2の親機と、電子バリューを管理するバリュー装置とを備える情報処理システムであって、端末は、第1の親機が提供するリソースを要求する信号を、第2の親機に送信するリソース要求信号送信手段と、第1の親機が提供するリソースを利用する利用権を、第2の親機から取得する第1の利用権取得手段とを有し、利用権を、第1の親機に提示して、第1の親機が提供するリソースを利用し、第1の親機は、リソースの提供に対する対価としての電子バリューが、第2の親機から第1の親機に振り込まれたことの振込み通知を、バリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、第2の親機に対して、利用権を発行する利用権発行手段とを有し、端末が、利用権を提示した場合に、自身が有するリソースの利用を許可し、第2の親機は、端末装置から送信されてくる、リソースを要求する信号に応じて、第1の親機への電子バリューの振込みを、バリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、第1の親機が発行する利用権を取得する第2の利用権取得手段と、第2の利用権取得手段において取得された利用権を、端末に提供する利用権提供手段とを有し、バリュー装置は、第2の親機からの要求に応じて、第1の親機に電子バリューを振り込む電子バリュー振込み手段と、第1の親機への電子バリューの振込み通知を、第1の親機に送信する振込み通知送信手段とを有することを特徴とする。 30 40

【0013】

本発明の第1の情報処理装置は、リソースを提供する第1の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信手段と、第1の親機が提供するリソースを利用する利用権を、第2の親機から取得する利用権取得手段とを備え、利用権を、第1の親機に提示して、第1の親機が提供するリソースを利用することを特徴とする。

【0014】

第2の親機との間で、ユーザが第2の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

【0015】

リソース要求信号送信手段と利用権取得手段は、第1の親機を介して、第2の親機とやりとりするようにすることができる。

【0016】

リソース要求信号送信手段と利用権取得手段は、第2の親機との間で、データを暗号化してやりとりするようにすることができる。

【0017】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【0018】

本発明の第1の情報処理装置の情報処理方法は、リソースを提供する第1の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信ステップと、第1の親機が提供するリソースを利用する利用権を、第2の親機から取得する利用権取得ステップとを含み、利用権を、第1の親機に提示して、第1の親機が提供するリソースを利用することを特徴とする。

【0019】

本発明の第1の情報処理装置のプログラムは、リソースを提供する第1の親機が提供するリソースを要求する信号を、ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信ステップと、第1の親機が提供するリソースを利用する利用権を、第2の親機から取得する利用権取得ステップとを含み、利用権を、第1の親機に提示して、第1の親機が提供するリソースを利用することを特徴とする。

【0020】

本発明の第2の情報処理装置は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段と、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段とを備え、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可

【0021】

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

【0022】

振込み通知が正当であることの認証を行う認証手段をさらに備えるようにすることができる。

【0023】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【0024】

本発明の第2の情報処理装置の情報処理方法は、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

【0025】

本発明の第2の情報処理装置のプログラムは、リソースの提供に対する対価としての電子バリューが、ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、

10

20

30

40

50

電子バリューを管理するバリュー装置から受信する振込み通知受信ステップと、振込み通知に応じて、親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップとを含み、端末が、親機から取得した利用権を提示した場合に、自身が有するリソースの利用を許可することを特徴とする。

【0026】

本発明の第3の情報処理装置は、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段と、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段と、利用権取得手段において取得された利用権を、端末に提供する利用権提供手段とを備えることを特徴とする。 10

【0027】

バリュー装置との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

【0028】

端末との間で、ユーザが個人情報に対応する正当なユーザであることの認証を行う認証手段をさらに備えるようにすることができる。

【0029】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。 20

【0030】

本発明の第3の情報処理装置の情報処理方法は、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供ステップとを含むことを特徴とする。

【0031】

本発明の第3の情報処理装置のプログラムは、端末からの要求に応じて、端末にリソースを提供する親機への、リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップと、電子バリューの振込みに応じて、親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップと、利用権取得ステップの処理において取得された利用権を、端末に提供する利用権提供ステップとを含むことを特徴とする。 30

【0032】

本発明の第4の情報処理装置は、ユーザにより操作される端末にリソースを提供する第1の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第2の親機からの要求に応じて行う電子バリュー振込み手段と、第2の親機から第1の親機への電子バリューの振込みが行われたことを表す振込み通知を、第1の親機に送信する振込み通知送信手段とを備えることを特徴とする。 40

【0033】

第1または第2の親機との間で、電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

【0034】

第1と第2の親機の電子バリューを記憶する記憶手段をさらに備え、電子バリュー振込み手段は、記憶手段に記憶された電子バリューを書き換えることにより、第2の親機から第1の親機に対して、電子バリューを振り込むようにすることができる。

【0035】

電子バリュー振込み手段は、第2の親機から電子バリューを取得し、その電子バリューを第1の親機に送信することにより、第2の親機から第1の親機に対して、電子バリュー 50

を振り込むようにすることができる。

【0036】

本発明の第4の情報処理装置の情報処理方法は、ユーザにより操作される端末にリソースを提供する第1の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第2の親機からの要求に応じて行う電子バリュー振込みステップと、第2の親機から第1の親機への電子バリューの振込みが行われたことを表す振込み通知を、第1の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

【0037】

リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。 10

【0038】

本発明の第4の情報処理装置のプログラムは、ユーザにより操作される端末にリソースを提供する第1の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、ユーザの個人情報を記憶する第2の親機からの要求に応じて行う電子バリュー振込みステップと、第2の親機から第1の親機への電子バリューの振込みが行われたことを表す振込み通知を、第1の親機に送信する振込み通知送信ステップとを含むことを特徴とする。

【0039】

本発明においては、端末により、第1の親機が提供するリソースを要求する信号が、第2の親機に送信され、記第1の親機が提供するリソースを利用する利用権が、第2の親機から取得される。そして、利用権が、第1の親機に提示され、第1の親機が提供するリソースが利用される。また、第1の親機により、リソースの提供に対する対価としての電子バリューが、第2の親機から第1の親機に振り込まれたことの振込み通知が、バリュー装置から受信され、振込み通知に応じて、第2の親機に対して、利用権が発行される。また、第1の親機により、端末により利用権が提示された場合に、自身が有するリソースの利用が許可される。第2の親機により、端末装置から送信されてくる、リソースを要求する信号に応じて、第1の親機への電子バリューの振込みが、バリュー装置に要求され、電子バリューの振込みに応じて、第1の親機が発行する利用権が取得される。また、第2の親機により、取得された利用権が、端末に提供される。バリュー装置により、第2の親機からの要求に応じて、第1の親機に電子バリューが振り込まれ、第1の親機への電子バリューの振込み通知が、第1の親機に送信される。 20 30

【発明の効果】

【0040】

本発明によれば、特に、ユーザが移動する場合においても、移動した空間にある機器を、匿名のまま操作させることができる。また、そのとき発生する対価の支払いを自動的に行うことができる。さらに、利便性がよく、安全な通信をすることができる。

【発明を実施するための最良の形態】

【0041】

以下に本発明の実施の形態を説明するが、請求項に記載の構成要件と、発明の実施の形態における具体例との対応関係を例示すると、次のようになる。この記載は、請求項に記載されている発明をサポートする具体例が、発明の実施の形態に記載されていることを確認するためのものである。従って、発明の実施の形態中には記載されているが、構成要件に対応するものとして、ここには記載されていない具体例があったとしても、そのことは、その具体例が、その構成要件に対応するものではないことを意味するものではない。逆に、具体例が構成要件に対応するものとしてここに記載されていたとしても、そのことは、その具体例が、その構成要件以外の構成要件には対応しないものであることを意味するものでもない。 40

【0042】

さらに、この記載は、発明の実施の形態に記載されている具体例に対応する発明が、請 50

求項に全て記載されていることを意味するものではない。換言すれば、この記載は、発明の実施の形態に記載されている具体例に対応する発明であって、この出願の請求項には記載されていない発明の存在、すなわち、将来、分割出願されたり、補正により追加される発明の存在を否定するものではない。

【0043】

請求項1に記載の情報処理システムは、ユーザにより操作される端末（例えば、図1の移動端末装置11-2）と、リソースを提供する第1の親機（例えば、図1の親機12-1）と、前記ユーザの個人情報を記憶する第2の親機（例えば、図1の親機12-2）と、電子バリューを管理するバリュー装置（例えば、図1のバリュー発行装置14）とを備え、前記端末は、前記第1の親機が提供するリソースを要求する信号を、前記第2の親機に送信するリソース要求信号送信手段（例えば、図19のステップS209の処理を実行するCPU61）と、前記第1の親機が提供するリソースを利用する利用権（例えば、リソース利用権）を、前記第2の親機から取得する第1の利用権取得手段（例えば、図19のステップS210の処理を実行するCPU61）とを有し、前記利用権を、前記第1の親機に提示して、前記第1の親機が提供するリソースを利用し（例えば、図19のステップS211, S212の処理を実行するCPU61）、前記第1の親機は、前記リソースの提供に対する対価としての電子バリューが、前記第2の親機から前記第1の親機に振り込まれたことの振込み通知を、前記バリュー装置から受信する振込み通知受信手段（例えば、図19のステップS265の処理を実行する親機12-1のCPU111）と、前記振込み通知に応じて、前記第2の親機に対して、前記利用権を発行する利用権発行手段（例えば、図19のステップS268の処理を実行する親機12-1のCPU111）とを有し、前記端末が、前記利用権を提示した場合に、自身が有するリソースの利用を許可し（例えば、図9のステップS83, S84の処理）、前記第2の親機は、前記端末装置から送信されてくる、前記リソースを要求する信号に応じて、前記第1の親機への前記電子バリューの振込みを、前記バリュー装置に要求する電子バリュー振込み要求手段（例えば、図19のステップS318の処理を実行する親機12-2のCPU111）と、前記電子バリューの振込みに応じて、前記第1の親機が発行する前記利用権を取得する第2の利用権取得手段（例えば、図19のステップS321の処理を実行する親機12-2のCPU111）と、前記第2の利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段（例えば、図19のステップS324の処理を実行する親機12-2のCPU111）とを有し、前記バリュー装置は、前記第2の親機からの要求に応じて、前記第1の親機に前記電子バリューを振り込む電子バリュー振込み手段（例えば、図16のステップS167の処理を実行するバリュー発行部135）と、前記第1の親機への前記電子バリューの振込み通知を、前記第1の親機に送信する振込み通知送信手段（例えば、図19のステップS344の処理を実行するバリュー発行部135）とを有することを特徴とする。

【0044】

請求項2に記載の情報処理装置は、リソースを提供する第1の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信手段（例えば、図19のステップS209の処理を実行するCPU61）と、前記第1の親機が提供するリソースを利用する利用権を、前記第2の親機から取得する利用権取得手段（例えば、図19のステップS210の処理を実行するCPU61）とを備え、前記利用権を、前記第1の親機に提示して、前記第1の親機が提供するリソースを利用する（図19のステップS211, S212の処理）ことを特徴とする。

【0045】

前記第2の親機との間で、前記ユーザが前記第2の親機が記憶している個人情報に対応する正当なユーザであることの認証を行う認証手段（例えば、図19のステップS205乃至ステップS208の処理を実行するCPU61）をさらに備えるようにすることができる。

【0046】

前記リソース要求信号送信手段と前記利用権取得手段は、前記第1の親機を介して、前

記第2の親機とやりとりするようにすることができる。

【0047】

前記リソース要求信号送信手段と前記利用権取得手段は、前記第2の親機との間で、データを暗号化してやりとりするようにすることができる。

【0048】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【0049】

請求項7に記載の情報処理方法、および請求項8に記載のプログラムは、リソースを提供する第1の親機が提供するリソースを要求する信号を、前記ユーザの個人情報を記憶する第2の親機に送信するリソース要求信号送信ステップ（例えば、図19のステップS209）と、前記第1の親機が提供するリソースを利用する利用権を、前記第2の親機から取得する利用権取得ステップ（例えば、図19のステップS210）とを含み、前記利用権を、前記第1の親機に提示して、前記第1の親機が提供するリソースを利用する（図19のステップS211，S212の処理）ことを特徴とする。

【0050】

請求項9に記載の情報処理装置は、前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信手段（例えば、図19のステップS265の処理を実行する親機12-1のCPU111）と、前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行手段（例えば、図19のステップS268の処理を実行する親機12-1のCPU111）とを備え、前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する（例えば、図9のステップS83，S84の処理）ことを特徴とする。

【0051】

前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段をさらに備えるようにすることができる。

【0052】

前記振込み通知が正当であることの認証を行う認証手段（例えば、図19のステップS266，S267の処理を実行する親機12-1のCPU111）をさらに備えるようにすることができる。

【0053】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【0054】

請求項13に記載の情報処理方法、請求項11に記載の記録媒体、および請求項14に記載のプログラムは、前記リソースの提供に対する対価としての電子バリューが、前記ユーザの個人情報を記憶する親機から振り込まれたことの振込み通知を、電子バリューを管理するバリュー装置から受信する振込み通知受信ステップ（例えば、図19のステップS265）と、前記振込み通知に応じて、前記親機に対して、自身が有するリソースを利用する利用権を発行する利用権発行ステップ（例えば、図19のステップS268）とを含み、前記端末が、前記親機から取得した前記利用権を提示した場合に、自身が有するリソースの利用を許可する（例えば、図9のステップS83，S84の処理）ことを特徴とする。

【0055】

請求項15に記載の情報処理装置は、前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求手段（例えば、図19のステップS318の処理を実行する親機12-2のCPU111）と、前記電

子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得手段（例えば、図19のステップS321の処理を実行する親機12-2のCPU111）と、前記利用権取得手段において取得された前記利用権を、前記端末に提供する利用権提供手段（例えば、図19のステップS324の処理を実行する親機12-2のCPU111）とを備えることを特徴とする。

【0056】

前記バリュー装置との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段（例えば、図19のステップS319、S320の処理を実行する親機12-2のCPU111）をさらに備えるようにすることができる。

【0057】

前記端末との間で、前記ユーザが前記個人情報に対応する正当なユーザであることの認証を行う認証手段（例えば、図19のステップS311乃至ステップS314の処理を実行する親機12-2のCPU111）をさらに備えるようにすることができる。

【0058】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【0059】

請求項19に記載の情報処理方法、および請求項20に記載のプログラムは、前記端末からの要求に応じて、前記端末にリソースを提供する親機への、前記リソースの提供に対する対価としての電子バリューの振込みを、電子バリューを管理するバリュー装置に要求する電子バリュー振込み要求ステップ（例えば、図19のステップS318）と、前記電子バリューの振込みに応じて、前記親機が発行する、その親機が有するリソースを利用する利用権を取得する利用権取得ステップ（例えば、図19のステップS321）と、前記利用権取得ステップの処理において取得された前記利用権を、前記端末に提供する利用権提供ステップ（例えば、図19のステップS324）とを含むことを特徴とする。

【0060】

請求項21に記載の情報処理装置は、ユーザにより操作される端末にリソースを提供する第1の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第2の親機からの要求に応じて行う電子バリュー振込み手段（例えば、図16のステップS167の処理を実行するバリュー発行部135）と、前記第2の親機から前記第1の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第1の親機に送信する振込み通知送信手段（例えば、図19のステップS344の処理を実行するバリュー発行部135）とを備えることを特徴とする。

【0061】

前記第1または第2の親機との間で、前記電子バリューを扱う正当な装置であることの認証を行う認証手段（例えば、図19のステップS342、S343の処理を実行する共通秘密鍵認証部133）をさらに備えるようにすることができる。

【0062】

前記第1と第2の親機の電子バリューを記憶する記憶手段（例えば、図15のバリュー記憶部140）をさらに備え、前記電子バリュー振込み手段は、前記記憶手段に記憶された電子バリューを書き換えることにより、前記第2の親機から前記第1の親機に対して、前記電子バリューを振り込むようにすることができる。

【0063】

前記電子バリュー振込み手段は、前記第2の親機から電子バリューを取得し、その電子バリューを前記第1の親機に送信することにより、前記第2の親機から前記第1の親機に対して、前記電子バリューを振り込むようにすることができる。

【0064】

前記リソースは、装置、情報、または情報に対するライセンスであるようにすることができる。

【0065】

10

20

30

40

50

請求項 27 の情報処理方法、および請求項 28 のプログラムにおいて、ユーザにより操作される端末にリソースを提供する第 1 の親機に対する、そのリソースの提供に対する対価としての電子バリューの振込みを、前記ユーザの個人情報を記憶する第 2 の親機からの要求に応じて行う電子バリュー振込みステップ（例えば、図 16 のステップ S 167）と、前記第 2 の親機から前記第 1 の親機への前記電子バリューの振込みが行われたことを表す振込み通知を、前記第 1 の親機に送信する振込み通知送信ステップ（例えば、図 19 のステップ S 344）とを含むことを特徴とする。

【0066】

以下、図を参照し本発明の実施の形態について説明する。

【0067】

10

図 1 は、本発明を適用した情報処理システム 1 の構成例を示すブロック図である。

【0068】

この情報処理システム 1 では、親機 12 とバリュー発行装置 14 間の処理を安全確実にを行うために用いられた公開鍵暗号（PKI（Public Key Infrastructure））系の暗号技術を用いてセキュリティを確保する。

【0069】

図 1 の例においては、2 人のユーザが、それぞれ移動端末装置 11-1 と移動端末装置 11-2 を有している。ユーザは、必ず 1 つの親機にユーザの個人情報（利用履歴、嗜好、決済関連等）を格納し、ユーザの認証情報として共通秘密鍵を取得する。この例では、ユーザと親機が共通秘密鍵として同じパスフレーズを有しており、ユーザと親機は、同じ 20

20

パスフレーズを有することを確認することで、ユーザを認証する。

【0070】

また、この例では、移動端末装置 11-1 のユーザは親機 12-1 に、移動端末装置 11-2 のユーザは親機 12-2 に、ユーザの個人情報を格納している。

【0071】

さらに、移動端末装置 11-1 は、その移動端末装置 11-1 のユーザの個人情報を格納した親機 12-1 と直接無線で通信可能な位置にあり、移動端末装置 11-2 は、その移動端末装置 11-2 のユーザの個人情報を格納した親機 12-2 とは遠隔地に設置された、親機 12-1 と直接無線で通信できる位置にある。従って、移動端末装置 11-2 は、親機 12-2 とは無線で通信することが困難であるが、親機 12-1 とは直接無線で通信 30

30

できる。

【0072】

移動端末装置 11-1 と移動端末装置 11-2 は、ユーザとともに移動し、無線通信を用いてユーザからの指示に対応する信号を親機 12-1 に送信する。また、移動端末装置 11-1 と移動端末装置 11-2 は、無線通信を用いて、親機 12-1 からの信号を受信する。

【0073】

以下、移動端末装置 11-1 と移動端末装置 11-2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、移動端末装置 11 と称する。

【0074】

40

この移動端末装置 11 とユーザとは、依存関係がなく、ユーザが移動端末装置 11 を利用するときのみ、移動端末装置 11 は、ユーザの認証を行う。従って、移動端末装置 11 には、ユーザの認証情報の入力機能が備えられている。

【0075】

図 1 の例においては、移動端末装置 11-1 および移動端末装置 11-2 のユーザは、ユーザの認証情報として、共通秘密鍵 31 および共通秘密鍵 32 を、それぞれ入力している。

【0076】

親機 12-1 は、所定の空間に配置され、無線通信を用いて、移動端末装置 11 から送信された信号を受信するとともに、移動端末装置 11 に信号を送信する。また、親機 12 50

50

ー 1 は、ユーザに提供する情報であるコンテンツ等のリソースを有するリソース機器 1 5ー 1、リソース機器 1 5ー 2、リソース機器 1 6ー 1、およびリソース機器 1 6ー 2 と接続されている。さらに、親機 1 2ー 1 は、インターネット 2 1 を介して、認証装置 1 3 およびバリュウ発行装置 1 4 と接続されている。

【0077】

ここで、親機 1 2ー 1 は、例えば、移動端末装置 1 1ー 1 のユーザのユーザ宅の、いわゆるホームサーバで構成することができる。同様に、親機 1 2ー 2 も、例えば、移動端末装置 1 1ー 2 のユーザのユーザ宅のホームサーバで構成することができる。

【0078】

以下、リソース機器 1 5ー 1 とリソース機器 1 5ー 2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器 1 5 と称する。また、リソース機器 1 6ー 1 とリソース機器 1 6ー 2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、リソース機器 1 6 と称する。 10

【0079】

これにより、移動端末装置 1 1 は、親機 1 2ー 1 を介して、親機 1 2ー 1 に接続されたリソース機器 1 5、リソース機器 1 6、およびインターネット 2 1 を介して接続された機器との通信ができる。

【0080】

また、親機 1 2ー 1 は、ユーザの認証情報として共通秘密鍵 3 3 を格納している。即ち、この共通秘密鍵 3 3 は、移動端末装置 1 1ー 1 のユーザに入力された共通秘密鍵 3 1 と等しくなっている。さらに、親機 1 2ー 1 は、バリュウ発行装置 1 4 により送信された共通秘密鍵 3 4 と、自らの正当性を証明する秘密鍵 3 5 を記憶している。 20

【0081】

親機 1 2ー 2 は、インターネット 2 1 を介して、親機 1 2ー 1、認証装置 1 3、およびバリュウ発行装置 1 4 と接続されている。

【0082】

また、親機 1 2ー 2 は、ユーザの認証情報として共通秘密鍵 3 6 を格納している。この共通秘密鍵 3 6 は、移動端末装置 1 1ー 2 のユーザに入力された共通秘密鍵 3 2 と等しくなっている。さらに、親機 1 2ー 1 は、バリュウ発行装置 1 4 により送信された共通秘密鍵 3 7 と、自らの正当性を証明する秘密鍵 3 8 を記憶している。 30

【0083】

以下、親機 1 2ー 1 と親機 1 2ー 2 のそれぞれを個々に区別する必要がない場合、適宜、まとめて、親機 1 2 と称する。

【0084】

認証装置 1 3 は、親機 1 2ー 1 の秘密鍵 3 5 に対応する公開鍵 3 9、親機 1 2ー 2 の秘密鍵 3 8 に対応する公開鍵 4 0、およびバリュウ発行装置 1 4 の後述する秘密鍵 4 3 に対応する公開鍵 4 1 を記憶する。また、認証装置 1 3 は、自らの正当性を証明する秘密鍵 4 2 を記憶する。

【0085】

認証装置 1 3 は、他の装置からの要求に応じて公開鍵を検索し、その公開鍵を他の装置に送信する。秘密鍵とそれに対応する公開鍵は、一方の鍵に基づいて生成された暗号文を他方の鍵を用いて復号できる関係にある。また、認証装置 1 3 は、電子証明書（図 1 1）の発行および鍵の失効管理を行う。 40

【0086】

バリュウ発行装置 1 4 は、親機 1 2ー 1 と親機 1 2ー 2 に対し、バリュウ（電子バリュウ）の発行および流通管理を行う。バリュウ発行装置 1 4 は、自らの正当性を証明する秘密鍵 4 3 および共通秘密鍵 4 4 を記憶している。バリュウ発行装置 1 4 は、共通秘密鍵 4 4 をバリュウを発行する相手である親機 1 2ー 1 と親機 1 2ー 2 に送信し、親機 1 2ー 1 に共通秘密鍵 3 4 として記憶させるとともに、親機 1 2ー 2 に共通秘密鍵 3 7 として記憶させる。即ち、共通秘密鍵 3 4、共通秘密鍵 3 7、および共通秘密鍵 4 4 は等しい。 50

【0087】

ユーザは、自身の個人情報（利用履歴、嗜好、決済関連情報等）を自身の親機12-1, 12-2にのみ格納し、共通秘密鍵33, 36を取得する。そして、この共通秘密鍵を用いて、全ての通信を行うことにより、ユーザは、匿名性を保ち、安全に通信を行うことができる。

【0088】

なお、上述の例では、2個の移動端末装置が存在するが、移動中のユーザが多数いる場合、その数だけの移動端末装置が存在するものとする。また、上述の例では、2個の親機が存在するが、各空間には、それぞれの空間に必要な数だけの親機が存在するものとする。

10

【0089】

また、共通秘密鍵31と共通秘密鍵32は、移動端末装置11のユーザを認証するための鍵である。共通秘密鍵34、共通秘密鍵37、および共通秘密鍵44は、バリュを扱う正当な装置であることを認証するための鍵である。秘密鍵35、秘密鍵38、および秘密鍵43は、自らの正当性を証明するための鍵であり、装置間における通信中の改ざんを防止する。

【0090】

以上のように構成される通信システム1によって、例えば、移動端末装置11-2のユーザがその個人情報を記憶していない親機12-1のリソースを利用する場合には、移動端末装置11-2は、親機12-1の利用したいリソースを指定し、個人情報を記憶している親機12-2に、そのリソースの利用を要求する。親機12-2は、移動端末装置11-2からリソースが要求されると、親機12-1に対するリソース利用に必要なバリュの支払いを、バリュ発行装置14に要求する。

20

【0091】

バリュ発行装置14は、親機12-2のバリュを親機12-1に移動させ、親機12-1にバリュの振込みが行われたことを表す振込み通知を発行する。親機12-1は、バリュ発行装置14から振り込み通知を受信すると、親機12-2にリソースを利用する利用権を発行する。親機12-2は、親機12-1から利用権が発行されると、その利用権を移動端末装置11-2に送信する。移動端末装置11-2は、その利用権を親機12-1に提示し、リソースを要求する。親機12-2は、移動端末装置11-2から利用権を提示された場合、リソースの利用を許可する。

30

【0092】

次に、図2は、図1の移動端末装置11の詳細構成例を示している。

【0093】

図2の例では、移動端末装置11-1を説明するが、移動端末装置11-2も同様に構成される。

【0094】

移動端末装置11-1は、CPU(Central Processing Unit)61、ROM(Read Only Memory)62、RAM(Random Access Memory)63、表示部64、リーダライタ65、送信部66、アンテナ67、受信部68、暗号/復号部69、および操作入力部70から構成される。

40

【0095】

なお、移動端末装置11-1のユーザは、あらかじめ取得した共通秘密鍵31、自身の親機12-1が接続しているリソースの情報、および自身の親機12-1のネットワーク上のアドレスを格納した非接触IC(Integrated Circuit)カード71を有している。

【0096】

このように、共通秘密鍵31を改ざんが困難な非接触ICカードに安全に格納することにより、通信システムの安全性と利便性を向上させることができる。また、非接触ICカードは、非接触のインターフェースであるので、利用時の利便性が向上し、かつ簡単な操作で処理が可能になる。

50

【0097】

この非接触ICカードとしては、例えば、FeliCa（商標）のような対タンパ性の高いICチップが用いられる。なお、共通秘密鍵31などは、非接触型ではなく接触型のデバイスに格納することも可能である。但し、便利性及びデバイスの劣化に対する耐性を考えると、接触型ではなく、非接触型を採用するのが望ましい。

【0098】

CPU61は、ROM62に記憶されているプログラムに従って各種の処理を実行する。RAM63には、CPU61が各種の処理を実行する上において必要なデータなどが適宜記憶される。

【0099】

表示部64は、CPU61からの指令により、例えば、移動端末装置11-1が利用できるリソースの情報を表示する。リーダライタ65は、ユーザが有する非接触ICカード71に封じ込められた（格納された）共通秘密鍵31、ユーザの個人情報を記憶した親機12-1が接続しているリソースの情報、および個人情報を記憶した親機12-1のネットワーク上のアドレスを読み込み、CPU61に共通秘密鍵31、リソース情報、およびアドレスを供給する。ここで、また、リーダライタ65は、CPU61からの指令により、必要に応じて非接触ICカード71にデータを書き込む。

【0100】

送信部66は、CPU61からの指令により、親機12-1に送信する信号をアンテナ67に供給する。アンテナ67は、送信部66から供給された信号を、無線通信を用いて親機12-1に送信する。さらに、アンテナ67は、親機12-1から送信された信号を受信し、その信号を受信部68に供給する。受信部68は、アンテナ67から供給された信号を、CPU61に供給する。

【0101】

暗号/復号部69は、非接触ICカード71から読み込まれた共通秘密鍵31を暗号化したり、受信部68で受信した暗号化された共通秘密鍵を復号し、その復号した共通秘密鍵をさらに暗号化する。操作入力部70は、ユーザにより操作され、その操作に対応する信号がCPU61に供給される。

【0102】

図3は、図2の移動端末装置11がリソースを取得する処理を説明するフローチャートである。なお、ユーザは、予め個人情報を自身の親機に格納しており、共通秘密鍵31（32）、その親機に接続されているリソースの情報、およびその親機のネットワーク上のアドレスは非接触ICカード71に記憶されているものとする。図3の処理は、例えば、ユーザが操作入力部70を操作して親機12-1に接続されているリソースの取得を要求したときに開始される。

【0103】

ステップS1において、CPU61は、移動端末装置11を使用するユーザの個人情報が格納されている自身の親機（以下、適宜、本親機と称する）と無線通信が可能であるかどうかを判定する。例えば、移動端末装置11は、無線通信が可能な機器を検索し、検索された機器の中に本親機が含まれているかどうかを判定する。

【0104】

ステップS1で、CPU61は、本親機と無線通信が可能であると判定した場合、ステップS2に進み、CPU61は、本親機（例えば、移動端末装置11-1の場合、親機12-1）との間で共通秘密鍵認証処理を行ない、ステップS3に進む。この共通秘密鍵認証処理の詳細は、図4で後述する。

【0105】

ステップS3では、CPU61は、ユーザが操作入力部70を操作することにより指定したリソースを要求する信号を、送信部66を制御して、アンテナ67から本親機である、例えば、親機12-1に送信する。即ち、ユーザは、非接触ICカード71に記憶され、リーダライタ65から読み込まれたリソース情報を表示部64に表示させ、そのリソース

10

20

30

40

50

情報を見て、取得したいリソースを指定する。これにより、そのリソースを要求する信号がアンテナ 6 7 から送信される。なお、以下の説明では、CPU 6 1 が送信部 6 6 を制御して、信号を送信することを、単に、CPU 6 1 が信号を送信するという。

【0106】

ステップ S 3 の処理後は、ステップ S 4 に進み、アンテナ 6 7 は、ステップ S 3 のリソース要求信号に対応して親機 1 2 - 1 から送信されたリソース（を使用するのに必要な情報）を受信し、受信部 6 8 を介して CPU 6 1 に供給する。そして、CPU 6 1 は、そのリソースを RAM 6 3 に保持する。なお、以下の説明では、アンテナ 6 7 が信号を受信し、受信部 6 8 を介して、CPU 6 1 にその信号を供給することを、単に、CPU 6 1 が信号を受信するという。

10

【0107】

一方、ステップ S 1 で、CPU 6 1 は、本親機と無線通信が可能ではないと判定した場合（例えば、移動端末装置 1 1 - 2 が、親機 1 2 - 2 と通信できない場合）、ステップ S 5 に進み、リソース情報取得処理を行ない、ステップ S 6 に進む。即ち、例えば、移動端末装置 1 1 - 2 については、現在、その移動端末装置 1 1 - 2 と通信できる親機 1 2 - 1 が本親機ではないので、移動端末装置 1 1 - 2 は、親機 1 2 - 1 が接続しているリソースの情報を非接触 IC カード 7 1 に記憶していない。従って、移動端末装置 1 1 - 2 は、親機 1 2 - 1 が接続しているリソースの情報を取得する必要があるため、このため、ステップ S 5 において、リソース情報取得処理が行なわれる。このリソース情報取得処理の詳細は、図 5 で後述する。

20

【0108】

ステップ S 6 において、CPU 6 1 は、本親機（親機 1 2 - 2）との間で共通秘密鍵認証処理を行い、ステップ S 7 に進む。なお、いまの場合、移動端末装置 1 1 - 2 は、本親機である親機 1 2 - 2 と直接無線通信することはできないため、ステップ S 6 の共通秘密鍵認証処理は、後述するように、移動端末装置 1 1 - 2 と親機 1 2 - 2 との間で、親機 1 2 - 1 およびインターネット 2 1 を介した通信を行うことにより実行される。この共通秘密鍵認証処理の詳細は、図 4 で後述する。

【0109】

ステップ S 7 では、CPU 6 1 は、非接触 IC カード 7 1 から、親機 1 2 - 2 のアドレスを読み出す。そして、ユーザが操作入力部 7 0 を操作することにより指定したリソースを要求する信号（リソース利用権発行要求）を親機 1 2 - 2 のアドレスとともに、親機 1 2 - 1 に送信し、インターネット 2 1 経由で親機 1 2 - 2 に送信する。即ち、ユーザは、ステップ S 5 で取得した親機 1 2 - 1 が接続しているリソースのリソース情報を表示部 6 4 に表示させ、そのリソース情報を見て、取得したいリソースを指定する。これにより、そのリソースを利用する権利を要求する信号として、リソース利用権発行要求が、移動端末装置 1 1 - 2 から、親機 1 2 - 1 およびインターネット 2 1 を介して、本親機である親機 1 2 - 2 に送信される。

30

【0110】

ここで、移動端末装置 1 1 - 2 は、上述のように、親機 1 2 - 2 のアドレスを親機 1 2 - 1 に知らせる。これにより、移動端末装置 1 1 - 2 は、無線通信可能な親機 1 2 - 1 とインターネット 2 1 を介して、本親機である親機 1 2 - 2 と通信が可能になる。

40

【0111】

ステップ S 7 の処理後は、ステップ S 8 に進み、CPU 6 1 は、親機 1 2 - 1 から、リソースを取得する権利を記載した権利文のデータであるリソース利用権を受信したか否かを判定する。ステップ S 8 で、CPU 6 1 は、親機 1 2 - 1 から権利文を受信したと判定した場合、移動端末装置 1 1 - 2 は、親機 1 2 - 1 に接続しているリソースを利用する権利があるので、ステップ S 9 に進み、親機 1 2 - 1 に、受信した権利文とリソース要求信号を送信する。ステップ S 9 の処理後は、ステップ S 10 に進み、CPU 6 1 は、リソース要求信号に対応して、親機 1 2 - 1 から送信されたリソース（を利用するのに必要な情報）を受信し、そのリソースを RAM 6 3 に保持して、処理を終了する。

50

【0112】

この場合、移動端末装置11-2は、本親機でない親機12-1のリソースを使用することができる。

【0113】

一方、ステップS8で、CPU61は、親機12-1から権利文を受信していないと判定した場合、ステップS11に進み、親機12-2から、親機12-1を介して、リソースを取得する権利を記載した権利文を発行できないことを示すエラー通知を受信したか否かを判定する。ステップS11で、CPU61は、親機12-1からエラー通知を受信していないと判定した場合、ステップS8に戻り、上述した処理を繰り返す。

【0114】

また、ステップS11において、CPU61は、親機12-2からエラー通知を受信したと判定した場合、移動端末装置11-2は、親機12-1に接続しているリソースを取得する権利がないので、処理を終了する。

【0115】

図4は、図3のステップS2とステップS6の共通秘密鍵認証処理を説明するフローチャートである。この処理は、移動端末装置11とそのユーザの本親機との間で行われる。

【0116】

図4の例では、移動端末装置11-1における共通秘密鍵認証処理を説明するが、移動端末装置11-2における場合も同様の処理が行われる。但し、移動端末装置11-2の場合は、本親機である親機12-2と無線通信が可能ではないので、無線通信可能な親機12-1にその本親機である親機12-2のアドレスを通知し、親機12-1を介して、インターネット21経由で本親機である親機12-2と通信する。

【0117】

ステップS21において、CPU61は、リーダライタ65を制御して、非接触ICカード71から、ユーザの認証情報である共通秘密鍵31を読み込み、RAM63に保持する。ステップS21の処理後は、ステップS22に進み、CPU61は、共通秘密鍵31を暗号化し、ステップS23に進む。即ち、移動端末装置11-1は、認証装置13から親機12-1（本親機）の秘密鍵35に対応する公開鍵39を取得し、RAM63に保持する。CPU61は、RAM63に保持した公開鍵39を、共通秘密鍵31とともに暗号/復号部69に供給する。暗号/復号部69は、その公開鍵39を用いて、共通秘密鍵31を暗号化する。

【0118】

ステップS23では、CPU61は、ステップS22で暗号化した共通秘密鍵31を、本親機である親機12-1に送信し、ステップS24に進む。ステップS24において、CPU61は、親機12-1（本親機）から、後述する図8のステップS64で送信されてくる秘密鍵35で暗号化された共通秘密鍵33を受信したかどうかを判定し、暗号化された共通秘密鍵33を受信していないと判定した場合、受信されるまで待機する。

【0119】

ステップS24において、CPU61は、親機12-1から暗号化された共通秘密鍵33を受信したと判定した場合、ステップS25に進み、暗号/復号部69を制御し、その暗号化された共通秘密鍵33を、ステップS22の処理でRAM63に保持した、秘密鍵35と対の公開鍵39を用いて復号する。このとき、秘密鍵35とそれに対応する公開鍵39は、一方の鍵に基づいて生成された暗号文（パズフレーズ）を他方の鍵を用いて復号できる関係にあるので、秘密鍵35に基づいて暗号化された共通秘密鍵33（パズフレーズ）が、親機12-1から送信され、移動端末装置11-1で受信されるまでの間に改ざんされなかった場合、その暗号化された共通秘密鍵33は、公開鍵39に基づいて復号されると、共通秘密鍵33となる。

【0120】

ステップS25の処理後は、ステップS26に進み、CPU61は、暗号/復号部69を制御して、復号した共通秘密鍵33を、ステップS22の処理でRAM63に保持した公開鍵39を用いて暗号化し、その暗号化した共通秘密鍵を親機12-1（本親機）に送信し、

10

20

30

40

50

ステップ S 2 7 に進む。ステップ S 2 7 において、CPU 6 1 は、親機 1 2 - 1 (本親機) から、後述する図 8 のステップ S 6 8 の処理で秘密鍵 3 5 を用いて暗号化された共通秘密鍵 (親機 1 2 - 1 が、ステップ S 2 3 で親機 1 2 - 1 に送信された暗号化した共通秘密鍵 3 1 を秘密鍵 3 5 を用いて復号し、さらに暗号化した共通秘密鍵) 3 1 を受信したかどうかを判定する。

【0 1 2 1】

ステップ S 2 7 で、CPU 6 1 は、親機 1 2 - 1 から暗号化された共通秘密鍵 3 1 を受信したと判定した場合、ステップ S 2 8 に進み、暗号/復号部 6 9 を制御して、その暗号化された共通秘密鍵 3 1 を、秘密鍵 3 5 と対の RAM 6 3 に保持した公開鍵 3 9 を用いて復号する。ステップ S 2 8 の処理後は、ステップ S 2 9 に進み、ステップ S 2 8 で復号された共通秘密鍵が、ステップ S 2 1 で RAM 6 3 に保持された共通秘密鍵 3 1 と等しいかどうかを判定する。 10

【0 1 2 2】

ステップ S 2 9 において、CPU 6 1 は、復号された共通秘密鍵 3 1 が、RAM 6 3 に保持された共通秘密鍵 3 1 と等しいと判定した場合、図 3 のステップ S 3 または図 3 のステップ S 7 にリターンする。即ち、この場合、ステップ S 2 3 で公開鍵 3 9 を用いて暗号化された共通秘密鍵 3 1 が、親機 1 2 - 1 により秘密鍵 3 5 を用いて正常に復号され、共通秘密鍵 3 1 が得られている。そして、その共通秘密鍵 3 1 が、親機 1 2 - 1 において秘密鍵 3 5 を用いて暗号化され、その暗号化された共通秘密鍵 3 1 が、移動端末装置 1 1 - 1 において、公開鍵 3 9 を用いて正常に復号され、共通秘密鍵 3 1 が得られている。 20

【0 1 2 3】

従って、秘密鍵 3 5 とそれに対応する公開鍵 3 9 は、一方の鍵に基づいて暗号化された共通秘密鍵 3 1 を他方の鍵を用いて復号できる関係にあるので、移動端末装置 1 1 - 1 は、移動端末装置 1 1 - 1 と親機 1 2 - 1 が通信する間で改ざんがなかったことを認識できる。

【0 1 2 4】

一方、ステップ S 2 9 において、CPU 6 1 は、ステップ S 2 8 で復号された共通秘密鍵が、RAM 6 3 に保持された共通秘密鍵 3 1 と等しくないと判定した場合、秘密鍵 3 5 とそれに対応する公開鍵 3 9 は、一方の鍵に基づいて生成された共通秘密鍵 3 1 を他方の鍵を用いて復号できる関係にないので、移動端末装置 1 1 - 1 と親機 1 2 - 1 が通信する間で改ざんがあった、あるいは、親機 1 2 - 1 が正当な装置でないと認識し、処理を終了する。 30

【0 1 2 5】

このように、移動端末装置 1 1 - 1 は、移動端末装置 1 1 - 1 と親機 1 2 - 1 が通信する間で改ざんがなかったと認識できたときのみ、図 3 のステップ S 3 または図 3 のステップ S 7 に進み、親機 1 2 - 1 にリソースを要求する信号を送信するので、移動端末装置 1 1 - 1 と親機 1 2 - 1 の両者間での通信中のデータ秘匿が可能となる。

【0 1 2 6】

一方、ステップ S 2 7 において、CPU 6 1 は、親機 1 2 - 1 から暗号化された共通秘密鍵 3 1 を受信していないと判定した場合、ステップ S 3 0 に進み、後述する図 8 のステップ S 7 1 で親機 1 2 - 1 が送信した、親機 1 2 - 1 と移動端末装置 1 1 - 1 の関係が正当ではないことを示すエラー通知を受信したか否かを判定する。ステップ S 3 0 において、CPU 6 1 は、親機 1 2 - 1 からエラー通知を受信していないと判定した場合、ステップ S 2 7 に戻り、上述した処理を繰り返す。 40

【0 1 2 7】

一方、ステップ S 3 0 において、CPU 6 1 は、親機 1 2 - 1 からエラー通知を受信したと判定した場合、親機 1 2 - 1 と移動端末装置 1 1 - 1 の関係は正当ではないので、処理を終了する。

【0 1 2 8】

図 5 は、図 3 のステップ S 5 の処理を説明するフローチャートである。 50

【0129】

ステップS41において、例えば、移動端末装置11-2のCPU61は、直接無線通信することができる本親機でない親機12-1にデバイス探索を要求する。

【0130】

ステップS41の処理後は、ステップS42に進み、CPU61は、親機12-1から、デバイス探索を許可された（後述する図12のステップS121で送信されたデバイス探索許可の通知を受信した）かどうかを判定する。ステップS42において、CPU61は、親機12-1からデバイス探索が許可されたと判定した場合、ステップS43に進み、親機12-1にリソース情報を要求する。

【0131】

ステップS43の処理後は、ステップS44に進み、CPU61は、リソース情報要求に対応して、親機12-1から送信されたリソース情報を受信し、そのリソース情報をRAM63に保持する。

【0132】

一方、ステップS42において、CPU61は、親機12-1から、デバイス探索を許可されていないと判定した場合、ステップS45に進み、デバイス探索に対応して親機12-1から送信されたデバイス探索の不許可を示すエラー通知が、受信されたかどうかを判定する。ステップS45において、CPU61は、エラー通知が受信されていないと判定した場合、ステップS42に戻り、上述した処理を繰り返す。

【0133】

また、ステップS45において、CPU61は、エラー通知が受信されたと判定した場合、親機12-1にデバイス探索が許可されず、親機12-1からリソース情報を得ることができないので、処理を終了する。

【0134】

図6は、図1の親機12の詳細構成例を示している。

【0135】

図6の例では、親機12-1を説明するが、親機12-2も同様に構成される。

【0136】

親機12-1は、CPU91、ROM92、RAM93、アンテナ94、受信部95、送信部96、入出力部97、データバス98、リソース制御部99、および通信部100から構成されている。

【0137】

CPU91は、ROM92に記憶されているプログラムに従って各種の処理を実行する。例えば、CPU91は、受信部95から供給された受信データの供給先を判定し、入出力部97を制御して、その供給先に、受信データを供給する。RAM93には、CPU91が各種の処理を実行する上で必要なデータなどが適宜記憶される。

【0138】

アンテナ94は、移動端末装置11から送信された信号を受信し、その信号を受信部95に供給する。また、アンテナ94は、送信部96から供給された信号を移動端末装置11に送信する。

【0139】

受信部95は、アンテナ94から供給された信号をCPU91に供給する。送信部96は、CPU91からの指令に基づいて、移動端末装置11に送信する信号をアンテナ94に供給する。

【0140】

入出力部97は、データバス98を介してリソース制御部99と通信部100に接続されるとともに、リソース機器16-1とリソース機器16-2に接続されている。リソース制御部99は、リソース機器15-1とリソース機器15-2にそれぞれ接続されている。

【0141】

10

20

30

40

50

通信部 100 は、CPU 91 からの指令に基づき、インターネット 21 を介して、親機 12-2、認証装置 13、およびバリュウ発行装置 14 に信号を送信するとともに、親機 12-2、認証装置 13、およびバリュウ発行装置 14 から信号を受信する。

【0142】

図 7 は、図 6 のリソース制御部 99 の詳細構成例を示している。

【0143】

リソース制御部 99 は、CPU 111、ROM 112、RAM 113、入出力部 114、リーダライタ 115、表示部 116、および暗号/復号部 117 から構成される。

【0144】

CPU 111 は、ROM 112 に記憶されているプログラムに従って各種の処理を実行する。RAM 113 は、ユーザの個人情報を格納しており、CPU 111 は、個人情報を管理している。また、RAM 113 には、CPU 111 が各種の処理を実行する上において必要なデータなどが適宜記憶される。 10

【0145】

CPU 111 は、入出力部 114 を介して、リソース機器 15-1 とリソース機器 15-2 に接続されており、リソース機器 15-1 とリソース機器 15-2 から供給されたリソースを、データバス 98 および入出力部 97 を介して、CPU 91 に供給する。リーダライタ 115 は、親機 12-1 に備えられた非接触 IC カード 121 から、データを読み込んだり、データを書き込む。

【0146】

非接触 IC カード 121 には、個人認証用の情報の格納領域と電子バリュウのための認証用の情報の格納領域が設けられている。個人認証用の情報の格納領域には、移動端末装置 11-1 の共通秘密鍵 31 と同一の共通秘密鍵 33 と自らの正当性を証明するための秘密鍵 35 が格納されている。電子バリュウのための認証用の情報の格納領域には、バリュウ発行装置 14 により発行された共通秘密鍵 34 等が格納されている。なお、電子バリュウのための認証用の情報の格納領域は、認証用と電子バリュウ用の領域に分けることができる。認証用の領域には、秘密鍵 34 が格納され、電子バリュウの領域には、電子バリュウ（例えば、権利文）が格納される。 20

【0147】

このように、共通秘密鍵 33、共通秘密鍵 34、および秘密鍵 35 を改ざんが困難な非接触 IC カード 121 に安全に格納することにより、通信システムの安全性と利便性を向上させることができる。 30

【0148】

表示部 116 は、CPU 111 の指令により、例えば、リソース情報を表示する。暗号/復号部 117 は、鍵、その他の情報を暗号化または復号する。

【0149】

なお、親機 12-1 は、物理的に 1 つの筐体で構成する必要はなく、データバスを経由して複数の機器が協調して機能を実現するように構成してもよい。

【0150】

図 8 は、図 7 の親機 12 のリソース制御部 99 がリソースを制御する処理を説明するフローチャートである。この処理は、例えば、移動端末装置 11 から信号を受信したとき開始される。 40

【0151】

以下の説明では、親機 12-1 がリソースを制御する処理を説明するが、親機 12-2 における場合も同様の処理が行われる。

【0152】

ステップ S61 では、CPU 111 は、リーダライタ 115 を制御し、非接触 IC カード 121 から共通秘密鍵 33 を読み込み、その共通秘密鍵 33 を RAM 113 に保持する。ステップ S61 の処理後は、ステップ S62 に進み、CPU 111 は、図 4 のステップ S23 で移動端末装置 11-1 から送信された暗号化した共通秘密鍵 31 が受信されたかどうか 50

を判定する。

【0153】

即ち、CPU 91は、アンテナ 94により受信され、受信部 95を介して供給された信号が、親機 12-1に対するものである場合、入出力部 97を制御し、データバス 98を介して、その信号をリソース制御部 99のCPU 111に供給し、CPU 111は、その信号が暗号化された共通秘密鍵 31であるかどうかを判定する。なお、以下の説明では、このようにCPU 91がアンテナ 94により受信された信号をリソース制御部 99のCPU 111に供給することを、単に、CPU 111が信号を受信するという。

【0154】

ステップ S 62において、CPU 111は、移動端末装置 11-1から暗号化された共通秘密鍵 31が受信されたと判定した場合、ステップ S 63に進み、非接触 IC カード 121から秘密鍵 35を読み込み、その暗号化された共通秘密鍵 31と秘密鍵 35をRAM 113に保持する。そして、CPU 111は、暗号/復号部 117を制御し、ステップ S 61でRAM 113に保持した共通秘密鍵 33を、秘密鍵 35を用いて暗号化する。 10

【0155】

ステップ S 63の処理後は、ステップ S 64に進み、CPU 111は、ステップ S 62で暗号化された共通秘密鍵 33を、移動端末装置 11-1に送信し、ステップ S 64からステップ S 65に進む。ステップ S 65では、CPU 111は、図 4のステップ S 26で移動端末装置 11-1から送信された暗号化された共通秘密鍵が受信されたかどうかを判定し、移動端末装置 11-1から暗号化された共通秘密鍵が受信されるまで待機する。 20

【0156】

ステップ S 65において、CPU 111は、移動端末装置 11-1から暗号化された共通秘密鍵が供給されたと判定した場合、ステップ S 66に進み、その暗号化された共通秘密鍵を復号し、ステップ S 67に進む。即ち、CPU 111は、暗号/復号部 117を制御し、ステップ S 63でRAM 113に保持した、公開鍵 39と対の秘密鍵 35を用いて、暗号化された共通秘密鍵を復号する。

【0157】

ステップ S 67では、CPU 111は、その復号された共通秘密鍵が、RAM 113に保持された共通秘密鍵 33と等しいかどうかを判定する。ステップ S 67において、CPU 111は、その復号された共通秘密鍵がRAM 113に保持された共通秘密鍵 33と等しいと判定した場合、ステップ S 68に進む。 30

【0158】

即ち、この場合、ステップ S 63で秘密鍵 35を用いて暗号化された共通秘密鍵 33が、移動端末装置 11-1において、公開鍵 39を用いて正常に復号され、共通秘密鍵 33が得られている。そして、その秘密鍵 33が移動端末装置 11-1において、公開鍵 39を用いて暗号化され、その暗号化された共通秘密鍵 31が、親機 12-1において、秘密鍵 35を用いて正常に復号され、共通秘密鍵 33が得られている。

【0159】

従って、秘密鍵 35とそれに対応する公開鍵 39は、一方の鍵に基づいて暗号化された共通秘密鍵 33を他方の鍵を用いて復号できる関係にあるので、親機 12-1は、移動端末装置 11-1と親機 12-1が通信する間で改ざんがなかったことが認識できる。 40

【0160】

その後、ステップ S 68において、CPU 111は、ステップ S 62で移動端末装置 11-1から受信し、RAM 113に保持した暗号化された共通秘密鍵 31を、RAM 113に保持した公開鍵 39と対の秘密鍵 35を用いて復号する。

【0161】

ステップ S 68の処理後は、ステップ S 69に進み、CPU 111は、ステップ S 68で復号した共通秘密鍵が、RAM 113に保持した共通秘密鍵 33と等しいかどうかを判定する。ステップ S 69において、CPU 111は、その復号した共通秘密鍵がRAM 113に保持した共通秘密鍵 33と等しいと判定した場合、ステップ S 70に進む。 50

【0162】

即ち、この場合、図4のステップS22で移動端末装置11-1により公開鍵39を用いて暗号化された、秘密鍵33と同一の共通秘密鍵31が、ステップS68で親機12-1により秘密鍵35を用いて正常に復号され、共通秘密鍵31が得られている。そして、移動端末装置11-1が有する共通秘密鍵31と親機12-1が有する共通秘密鍵33が同一であることが検証、つまり、移動端末装置11-1のユーザが、親機12-1のユーザであることが検証されている。

【0163】

従って、秘密鍵35とそれに対応する公開鍵39は、一方の鍵に基づいて暗号化された共通秘密鍵31を他方の鍵を用いて復号できる関係にあるので、親機12-1は、移動端末装置11-1と親機12-1が通信する間で改ざんがなかったことが認識できる。また、移動端末装置11-1が有する共通秘密鍵31と親機12-1が有する共通秘密鍵33が等しくなっているので、親機12-1は、移動端末装置11-1のユーザが個人情報を格納したユーザであることを認識する。 10

【0164】

その後、ステップS70において、暗号/復号部69を制御して、その復号した共通秘密鍵を、RAM113に保持した秘密鍵35を用いて暗号化し、移動端末装置11-1に送信する。

【0165】

一方、ステップS67において、CPU111は、ステップS66で復号された共通秘密鍵がRAM113に保持する共通秘密鍵33と等しくないと判定した場合、またはステップS69で、ステップS68で復号された共通秘密鍵がRAM113に保持する共通秘密鍵33と等しくないと判定した場合、移動端末装置11-1と親機12-1が通信する間で改ざんがあったか、または親機12-1が移動端末装置11-1の本親機ではないので、ステップS71に進み、移動端末装置11-1と親機12-1の関係が正当ではないことを示すエラー通知を送信し、処理を終了する。 20

【0166】

このように、親機12-1は、移動端末装置11-1と親機12-1が通信する間で改ざんがなく、かつ移動端末装置11-1の本親機であると認識できたときのみ、復号した共通秘密鍵31を暗号化して移動端末装置11-1に送信する。 30

【0167】

この後、移動端末装置11-1は、移動端末装置11-1と親機12-1が通信する間で改ざんがなかったと認識できたときのみリソースを要求する信号を親機12-1に送信するので、移動端末装置11-1は、移動端末装置11-1と親機12-1が通信する間で改ざんがなかったと移動端末装置11-1と親機12-1の両方で認識（双方向認証）され、かつ親機12-1が移動端末装置11-1の本親機である場合のみ、リソースを要求し、利用することができる。

【0168】

これにより、移動端末装置11-1と親機12-1の両者間での通信中のデータ秘匿が可能となる。 40

【0169】

ステップS62において、CPU111は、移動端末装置11-1からリソース要求信号が供給されたと判定した場合、ステップS73に進み、リソース送信処理を行い、その後、処理を終了する。リソース送信処理の詳細は、図9と図10で後述する。

【0170】

一方、ステップS72において、CPU111は、リソース要求信号が供給されていないと判定した場合、ステップS62に戻り、上述した処理を繰り返す。

【0171】

図9は、移動端末装置11-1および11-2と直接無線通信が可能な親機12-1が図8のステップS73の処理で行うリソース送信処理を説明するフローチャートである。 50

【0172】

ステップS81において、親機12-1のCPU111は、図8のステップS72で受信したリソース要求信号が自身が本親機となる移動端末装置（移動端末装置11-1）からのリソース要求信号であるかどうかを判定する。ステップS81において、親機12-1のCPU111は、受信したリソース要求信号が自身が本親機となる移動端末装置11-1からのリソース要求信号であると判定した場合、ステップS82をスキップしてステップS83に進む。

【0173】

ステップS83では、親機12-1のCPU111は、入出力部114を制御し、移動端末装置11-1からのリソース要求信号に基づいて、移動端末装置11-1から要求されているリソースを有するリソース機器15からリソースを取得し、ステップS84に進む。ステップS84では、親機12-1のCPU111は、そのリソースを、移動端末装置11-1に送信してリターンする。 10

【0174】

即ち、親機12-1は、個人情報情報を格納しているユーザが使用する移動端末装置11-1から、親機12-1の接続するリソース機器15の有するリソースを要求された場合、無条件に利用を許可する。

【0175】

一方、ステップS81において、親機12-1のCPU111は、図8のステップS72で受信したリソース要求信号が、自身が本親機とならない移動端末装置からのリソース要求信号である（移動端末装置11-2からのリソース要求信号である）と判定した場合、ステップS82に進み、権利文の提示がある（リソース要求信号とともに権利文が送信されてきた）かどうかを判定する。ステップS82において、親機12-1のCPU111は、権利文の提示がなかったと判定した場合、移動端末装置11-2はリソースを利用する権利がないので、処理を終了する。 20

【0176】

ステップS82において、親機12-1のCPU111は、権利文の提示があったと判定した場合、ステップS83に進み、入出力部114を制御し、移動端末装置11-2からのリソース要求信号に基づいて、移動端末装置11-2から要求されているリソースを有するリソース機器15からリソースを取得し、ステップS84に進む。ステップS84では、親機12-1のCPU111は、そのリソースを、移動端末装置11-2に送信する。 30

【0177】

即ち、親機12-1は、個人情報情報を格納していないユーザが使用する移動端末装置11-2から、親機12-1に接続しているリソース機器15の有するリソースを要求された場合、移動端末装置11-2がリソースを利用する権利文を取得している場合のみ、リソース利用を許可する。逆に言えば、移動端末装置11-2のユーザは、本親機12-1のリソースを、そのリソースを利用する権利文を、親機12-1に提示したときのみ利用することができる。

【0178】

なお、親機12-1は、親機12-2が移動端末装置11-2のユーザを認証するときのやりとり時に、移動端末装置11-2は、そのユーザの個人情報情報を、その本親機である親機12-2から取得する。ここで、個人情報には、そのユーザがリソースを利用したときの操作履歴などが含まれる。即ち、移動端末装置11-2の本親機である親機12-2は、例えば、そのユーザが自身の有するリソースを利用したときに、その利用時の操作履歴などを個人情報として登録する個人情報管理機能を有する。移動端末装置11-2は、親機12-1のリソースを利用するときに、ユーザの個人情報に応じて、移動端末装置11-2のユーザの嗜好に合わせた操作性（ユーザI/F）を提供する。 40

【0179】

図10は、移動端末装置11-2がその本親機である親機12-2と直接無線通信できない場合に、その親機12-2が図8のステップS71の処理で行うリソース送信処理を 50

説明するフローチャートである。なお、親機 12-2 は、認証装置 13 から発行された電子証明書（図 11 で後述する）を既に受信し、RAM 113 に保持しているものとする。

【0180】

ステップ S100 において、親機 12-2 の CPU 111 は、暗号化した利用権発行要求文と、RAM 113 に保持している電子証明書を作成し、その利用権発行要求文と電子証明書を、移動端末装置 11-1 がリソースを利用しようとする本親機でない親機 12-1 に送信する。即ち、親機 12-2 の CPU 111 は、直接無線通信することができない移動端末装置 11-2 から送信されたリソース要求信号に基づいて、リソース情報の識別子と利用方法を明記した利用権発行要求文を作成する。

【0181】

また、親機 12-2 の CPU 111 は、リーダーライタ 115 を制御し、非接触 IC カード 121 から読み込んだ秘密鍵 38 を RAM 113 に保持する。CPU 111 は、暗号/復号部 117 を制御し、RAM 113 に保持した秘密鍵 38 を用いて、電子署名を暗号化し、利用権発行要求文を付加する。そして、CPU 111 は、その利用権発行要求文を電子証明書とともに、移動端末装置 11-2 がリソースを利用しようとしている親機 12-1 に送信する。

【0182】

なお、利用権発行要求文とは、ここでは、移動端末装置 11-2 が、その本親機でない親機 12-1 のリソースの利用をするための利用権の発行を、親機 12-1 に要求するメッセージである。

【0183】

また、移動端末装置 11-2 が本親機である親機 12-2 に送信するリソース要求信号には、その移動端末装置 11-2 がリソースを利用しようとする本親機でない親機 12-2 へアクセスするためのアクセス情報が含まれている。そして、親機 12-2 は、このアクセス情報に基づいて、利用権発行要求文を親機 12-1 に送信する。

【0184】

ステップ S100 の処理後は、ステップ S101 に進み、親機 12-2 の CPU 111 は、後述する図 13 のステップ S147 で、利用権発行要求文を受信した親機 12-1 が親機 12-2 に対して送信するリソースの利用を許可するための対価（バリュー）と対価の送信先口座情報を記載したリソース利用条件文と電子証明書を受信したかどうかを判定する。ステップ S101 において、親機 12-2 の CPU 111 は、リソース利用条件文と電子証明書を受信したと判定した場合、暗号/復号部 117 を制御し、電子証明書に含まれる、親機 12-1 の秘密鍵 35 に対応する公開鍵 39 を用いて、リソース利用条件文に含まれる電子署名を復号し、ステップ S101 からステップ S102 に進む。

【0185】

ステップ S102 において、親機 12-2 の CPU 111 は、リソース利用条件文が正当であるかどうかを判定する。即ち、CPU 111 は、リソース利用条件文に含まれる電子署名が正常に復号されたかどうかを判定する。ステップ S102 において、CPU 111 は、リソース利用条件文が正当ではないと判定した場合、親機 12-1 の秘密鍵 35 で暗号化された電子署名が、それと対の公開鍵 39 で復号できていないので、親機 12-1 と親機 12-2 が通信する間で改ざんが行われたと判定し、処理を終了する。

【0186】

また、ステップ S102 において、親機 12-2 の CPU 111 は、リソース利用条件文が正当であると判定した場合、秘密鍵 35 で暗号化された電子署名が、公開鍵 39 で復号できるので、親機 12-1 と親機 12-2 が通信する間で改ざんが行われず、親機 12-1 と親機 12-2 が正当な関係であると認識し、ステップ S102 からステップ S103 に進む。

【0187】

このように、電子署名を用いてリソース利用条件文が正当であるかどうかを判定することにより、通信システム 1 の安全性をさらに高めることができる。

10

20

30

40

50

【0188】

ステップS103において、親機12-2のCPU111は、リソース利用条件文に基づいて、親機12-2から親機12-1にバリュウを移動する（対価を支払う）ためのバリュウ移動要求をバリュウ発行装置14に送信する。

【0189】

ステップS103の処理後は、ステップS104に進み、親機12-2のCPU111は、バリュウ発行装置14から、後述する図16のステップS162で送信される暗号化された共通秘密鍵44を受信したかどうかを判定する。ステップS104において、CPU111は、バリュウ発行装置14から暗号化された共通秘密鍵44を受信していないと判定した場合、バリュウ発行装置14から暗号化された共通秘密鍵44が受信されるまで待機する。 10

【0190】

ステップS104において、親機12-2のCPU111は、バリュウ発行装置14から暗号化された共通秘密鍵44を受信したと判定した場合、ステップS105に進み、親機12-2のCPU111は、バリュウ発行装置14の有する秘密鍵43に対応する公開鍵41を、認証装置13から取得し、RAM113に保持する。そして、親機12-2のCPU111は、暗号/復号部117を制御し、RAM113に保持した公開鍵41を用いて、暗号化された共通秘密鍵44を復号し、復号した共通秘密鍵44をRAM113に保持する。

【0191】

ステップS105の処理後は、ステップS106に進み、親機12-2のCPU111は、リーダライタ115を制御して、共通秘密鍵37を読み込み、RAM113に保持し、ステップS107に進む。ステップS107では、親機12-2のCPU111は、RAM113から復号した共通秘密鍵44と共通秘密鍵37を読み出し、両者が等しいかどうかを判定する。 20

【0192】

ステップS107において、親機12-2のCPU111は、復号した共通秘密鍵44と共通秘密鍵37が等しいと判定した場合、即ち、後述する図16のステップS161でバリュウ発行装置14により秘密鍵43を用いて暗号化された共通秘密鍵44が、ステップS106で親機12-2により公開鍵41を用いて正常に復号され、共通秘密鍵37と等しい共通秘密鍵44が得られている場合、親機12-2のCPU111は、バリュウ発行装置14と親機12-2が通信する間で改ざんがなかったことが認識し、ステップS107からステップS108に進む。 30

【0193】

従って、CPU111は、S108では、親機12-2のCPU111は、暗号/復号部117を制御し、RAM113に保持した公開鍵41を用いて、RAM113に保持した共通秘密鍵37を暗号化する。ステップS109の処理後は、ステップS110に進み、親機12-2のCPU111は、その暗号化した共通秘密鍵37を、バリュウ発行装置14に送信し、リターンする。

【0194】

一方、ステップS107において、親機12-2のCPU111は、ステップS106で復号した共通秘密鍵と共通秘密鍵34が等しくないと判定した場合、バリュウ発行装置14と親機12-2が通信する間で改ざんがあったと認識し、ステップS110に進み、バリュウ発行装置14に、バリュウ発行装置14と親機12-2の関係は正当ではないことを示すエラーを通知してリターンする。 40

【0195】

また、ステップS101において、親機12-2のCPU111は、移動端末装置12-2がリソースを利用しようとする親機12-1からのリソース利用条件文を受信していないと判定した場合、ステップS111に進み、親機12-1から、後述する図13のステップS148で送信されたリソース利用条件文を発行できないことを示すエラー通知を受信したかどうかを判定する。ステップS110において、親機12-2のCPU111は 50

、親機 12-1 からエラー通知を受信していないと判定した場合、ステップ S101 に戻り、上述した処理を繰り返す。

【0196】

また、ステップ S111 において、親機 12-2 の CPU111 は、親機 12-1 からエラー通知を受信したと判定した場合、即ち、親機 12-1 がリソース利用条件文を発行せず、移動端末装置 11-2 によるリソース利用を許可しなかった場合、処理を終了する。

【0197】

図 11 は、電子証明書の例を示す図である。

【0198】

この電子証明書は、図 11 に示されるように、証明書のバージョン番号、証明書の通し番号、署名に用いたアルゴリズムとパラメータ、認証装置 13 の名前、証明書の有効期限、発行された装置の ID、および装置の公開鍵が含まれている。 10

【0199】

この電子証明書は、認証装置 13 により、親機 12-1、親機 12-2、およびバリュエ発行装置 14 に対して発行される。親機 12-1、親機 12-2、およびバリュエ発行装置 14 は、自らの正当性を証明するために他の装置に、暗号文とともにこの電子証明書を送信する。受信した装置は、この電子証明書に含まれる装置の公開鍵を用いて、この電子証明書とともに送信されてくる暗号文を復号し、その暗号文の正当性を認識することができる。

【0200】

図 12 は、図 6 の親機 12-1 がリソース情報を送信する処理を説明するフローチャートである。この処理は、例えば、親機 12-1 が図 5 のステップ S41 で移動端末装置 11-2 から送信されるブロードキャスト要求信号を受信したとき開始される。 20

【0201】

ステップ S120 において、親機 12-1 の CPU91 は、移動端末装置 11-2 によるブロードキャスト要求を許可するかどうかを判定する。ステップ S120 において、親機 12-1 の CPU91 は、ブロードキャスト要求を許可すると判定した場合、ステップ S121 に進み、移動端末装置 11-2 にブロードキャスト要求許可の通知を送信する。

【0202】

ステップ S121 の処理後は、ステップ S122 に進み、親機 12-1 の CPU91 は、移動端末装置 11-2 から図 5 のステップ S43 でリソース情報要求信号が送信されて来るのを待って受信し、ステップ S123 に進む。 30

【0203】

ステップ S123 において、親機 12-1 の CPU91 は、入出力部 97 を制御し、データバス 98 とリソース制御部 99 を介して、リソース機器 15-1 とリソース機器 15-2 から、移動端末装置 12-2 に提供することができる、または提供してもよいリソースのリソース情報を取得する。同様に、CPU91 は、入出力部 97 を制御し、データバス 98 を介して、リソース機器 16-1 とリソース機器 16-2 からリソース情報を取得する。そして、CPU91 は、取得したリソース情報を移動端末装置 11-2 に送信して処理を終了する。 40

【0204】

一方、ステップ S120 において、CPU91 は、移動端末装置 11-2 からのブロードキャスト要求を許可しないと判定した場合、ステップ S124 に進み、移動端末装置 11 にブロードキャスト要求を許可しないことを示すエラー通知を送信し、処理を終了する。

【0205】

図 13 は、図 6 の親機 12-1 が、リソース利用条件文を発行するときに行うリソース利用条件文発行処理を説明するフローチャートである。この処理は、親機 12-1 が図 10 のステップ S100 の処理で親機 12-2 から送信された、暗号化された利用権発行要求文と電子証明書を受信したとき開始される。なお、親機 12-1 は、認証装置 13 から発行された電子証明書（図 11）を既に受信し、RAM113 に保持しているものとする。 50

【0206】

ステップS141において、親機12-1のCPU111は、親機12-2から利用権発行要求文とともに受信した電子証明書から公開鍵40を取得し、ステップS142に進む。ステップS142では、親機12-1のCPU111は、親機12-2から受信した利用権発行要求文から秘密鍵38を用いて暗号化された電子署名を取得する。CPU111は、暗号/復号部117を制御して、電子署名を、ステップS141で取得した、秘密鍵38と対の公開鍵40を用いて復号する。

【0207】

ステップS142の処理後は、ステップS143に進み、親機12-1のCPU111は、利用権発行要求文が正当であるかどうかを判定する。即ち、親機12-1のCPU111は、ステップS142で電子署名が正常に復号されたかどうかを判定し、電子署名が正常に復号された場合、秘密鍵38で暗号化された電子署名が、秘密鍵38に対応する公開鍵40で正常に復号されているので、親機12-1と親機12-2が通信する間で改ざんが行われていないと認識し、利用権発行要求文が正当であると判定する。 10

【0208】

ステップS143において、親機12-1のCPU111は、利用権発行要求文が正当ではないと判定した場合、リソース利用を許可することはできないので、ステップS148に進み、リソース利用の不許可を示すエラー通知を送信して処理を終了する。

【0209】

ステップS143において、親機12-1のCPU111は、利用権発行要求文が正当であると判定した場合、ステップS144に進み、親機12-2から受信した電子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装置13に送信し、ステップS145に進む。 20

【0210】

ステップS145では、親機12-1のCPU111は、認証装置13から、図18のステップS183またはステップS184で送信される電子証明書の評価を受信したかどうかを判定し、電子証明書の評価を受信していないと判定した場合、電子証明書の評価を受信するまで待機する。

【0211】

ステップS145において、親機12-1のCPU111は、認証装置13から電子証明書の対価を受信したと判定した場合、ステップS146に進み、その認証装置13からの電子証明書の評価が有効であるかどうかを判定する。ステップS146において、親機12-1のCPU111は、認証装置13から電子証明書は有効であるという評価を受信したと判定した場合、即ち、利用件発行要求とともに送信されてきた電子証明書が失効していない（無効でない）場合、ステップS147に進み、リソース利用を許可するための対価を記載したリソース利用条件文を電子的に作成する。 30

【0212】

このとき、親機12-1のCPU111は、暗号/復号部117を制御して、自らの正当性を証明するために、秘密鍵35を用いて電子署名を暗号化し、リソース利用条件文に電子署名を付加する。そして、CPU111は、電子署名を付加した利用条件文と、RAM113に保持した電子証明書を、親機12-2に送信し、処理を終了する。 40

【0213】

一方、ステップS146において、親機12-1のCPU111は、認証装置13から電子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース利用を許可することはできないので、ステップS148に進み、リソース利用の不許可を示すエラー通知を親機12-2に送信し、処理を終了する。

【0214】

なお、親機12-1がリソースを利用する権利を記載した権利文を発行する処理も、図13と同様にして行われる。但し、この権利文を発行する処理は、バリュウ発行装置14から、後述する図16のステップS168で送信される暗号化された振込み通知書と電子 50

証明書を受信したとき開始される。

【0215】

即ち、図14は、図6の親機12-1がリソースを利用するための権利文を発行するときに行う権利文発行処理を説明するフローチャートである。この処理は、親機12-1が後述する図16のステップS168の処理でバリュ発行装置14から送信される、振込み通知書と電子証明書を受信したとき開始される。なお、親機12-1は、認証装置13から発行された電子証明書（図11）を既に受信し、RAM113に保持しているものとする。

【0216】

ステップS151において、親機12-1のCPU111は、バリュ発行装置14から
、振込み通知書とともに受信した電子証明書から公開鍵41を取得し、ステップS152に進む。ステップS152では、親機12-1のCPU111は、バリュ発行装置14
から受信した振込み通知書から秘密鍵43を用いて暗号化された電子署名を取得する。親
機12-1のCPU111は、暗号/復号部117を制御して、電子署名を、ステップS151
で取得した公開鍵41を用いて復号する。 10

【0217】

ステップS152の処理後は、ステップS153に進み、親機12-1のCPU111は
、振込み通知書が正当であるかどうかを判定する。即ち、CPU111は、電子署名が正常
に復号されたかどうかを判定し、電子署名が正常に復号された場合、秘密鍵43で暗号化
された電子署名が、秘密鍵43に対応する公開鍵41で正常に復号されているので、親機 20
12-1とバリュ発行装置14が通信する間で改ざんが行われていないと認識し、振込
み通知書が正当であると判定する。

【0218】

ステップS153において、親機12-1のCPU111は、振込み通知書が正当では
ないと判定した場合、リソース利用を許可することはできないので、ステップS158に進
み、リソース利用の不許可を示すエラー通知を送信して処理を終了する。

【0219】

また、ステップS153において、親機12-1のCPU111は、振込み通知書が正当
であると判定した場合、ステップS154に進み、バリュ発行装置14から受信した電
子証明書が有効であるかどうかの判定を要求する評価要求信号を、認証装置13に送信し 30
、ステップS155に進む。

【0220】

ステップS155では、親機12-1のCPU111は、認証装置13から、後述する図
18のステップS183またはステップS184で送信される電子証明書の評価を受信し
たかどうかを判定し、電子証明書の評価を受信していないと判定した場合、電子証明書の
評価を受信するまで待機する。

【0221】

そして、ステップS155において、親機12-1のCPU111は、認証装置13から
電子証明書の評価を受信したと判定した場合、ステップS156に進み、CPU111は、
認証装置13から電子証明書は有効であるという評価を受信したかどうかを判定する。 40
ステップS156において、CPU111は、認証装置13から電子証明書は有効であるとい
う評価を受信したと判定した場合、ステップS157に進み、リソースを利用する権利を
記載した権利文を電子的に作成する。このとき、親機12-1のCPU111は、暗号/復号
部117を制御して、自らの正当性を証明するために、秘密鍵35を用いて電子署名を暗
号化し、権利文に電子署名を付加する。そして、親機12-1のCPU111は、電子署名
を付加した権利文と、RAM113に保持した電子証明書を、親機12-2に送信して処理
を終了する。

【0222】

一方、ステップS156において、親機12-1のCPU111は、認証装置13から電
子証明書は有効ではない（無効である）という評価を受信したと判定した場合、リソース 50

利用を許可することはできないので、ステップ S 1 5 8 に進み、リソース利用の不許可を示すエラー通知を親機 1 2 - 2 に送信して処理を終了する。

【0 2 2 3】

図 1 5 は、図 1 のバリュ発行装置 1 4 の詳細構成例である。

【0 2 2 4】

バリュ発行装置 1 4 は、通信部 1 3 1、データバス 1 3 2、共通秘密鍵認証部 1 3 3、公開鍵認証部 1 3 4、バリュ発行部 1 3 5、共通秘密鍵記憶部 1 3 6、秘密鍵記憶部 1 3 7、証明書記憶部 1 3 8、発行履歴記憶部 1 3 9、およびバリュ記憶部 1 4 0 から構成されている。

【0 2 2 5】

通信部 1 3 1 は、インターネット 2 1 を介して、親機 1 2 - 1、親機 1 2 - 2、および認証装置 1 3 からの信号を受信するとともに、親機 1 2 - 1、親機 1 2 - 2、および認証装置 1 3 に信号を送信する。通信部 1 3 1 は、データバス 1 3 2 を介して、共通秘密鍵認証部 1 3 3、公開鍵認証部 1 3 4、およびバリュ発行部 1 3 5 に接続されている。

【0 2 2 6】

共通秘密鍵認証部 1 3 3 は、共通秘密鍵記憶部 1 3 6 に記憶された共通秘密鍵 4 4 に基づいて、バリュ発行装置 1 4 にアクセスしてきた親機 1 2 が正当であるかどうかを判定する。また、共通秘密鍵認証部 1 3 3 は、バリュ発行装置 1 4 がバリュを管理する親機 1 2 に対して、共通秘密鍵 4 4 と同一の秘密鍵 3 4 または 3 7 を送信し、親機 1 2 の非接触 I C カード 1 2 1 に記憶させる。

【0 2 2 7】

このように、親機 1 2 の非接触 I C カード 1 2 1 にバリュ発行装置 1 4 の共通秘密鍵 4 4 と等しい共通秘密鍵 3 4 または 3 7 を記憶させることにより、親機 1 2 とバリュ発行装置 1 4 との間での認証が可能となり、ユーザが、その親機 1 2 と通信が可能な移動端末装置 1 1 を使用するだけで、バリュ発行装置 1 4 を介して、親機 1 2 どちらの間でのバリュの移動をすることができる。

【0 2 2 8】

公開鍵認証部 1 3 4 は、秘密鍵記憶部 1 3 7 に記憶された秘密鍵 4 3 や、証明書記憶部 1 3 8 に記憶された電子証明書を用いて、親機 1 2 - 1、親機 1 2 - 2、および認証装置 1 3 との間で通信部 1 3 1 を開始、公開鍵暗号系の処理を行う。

【0 2 2 9】

バリュ発行部 1 3 5 は、バリュ記憶部 1 4 0 に記憶されたバリュ（電子バリュ）に基づき、バリュを発行し、その発行履歴を発行履歴記憶部 1 3 9 に記憶させる。

【0 2 3 0】

なお、バリュ発行装置 1 4 は、物理的に 1 つの筐体に入る必要はなく、データバス 1 3 2 を経由して複数の機器が協調して機能を実現してもよい。

【0 2 3 1】

また、バリュ発行装置 1 4 は、発行したバリュに応じた対価を決済できるようにしてもよい。さらに、親機 1 2 は、所有する電子バリュをネットワークでの決済に使用してもよい。

【0 2 3 2】

また、電子バリュの形式は何でもよい。電子バリュはバリュ発行装置 1 4 のバリュ記憶部 1 4 0 に口座という形で格納してもよい。この場合、より高い安全性を提供することができる。

【0 2 3 3】

口座を表す I D は、親機の証明書にある機器 I D、あるいはそれに対応させた別の I D を用いることにより、ユーザは個人情報に結びつかない匿名性の高い口座を持つことができる。

【0 2 3 4】

さらに、バリュは、バリュ発行装置 1 4 のバリュ記憶部 1 4 0 に口座という形で

10

20

30

40

50

記憶されるだけでなく、親機 1 2 の安全なデバイス（例えば、非接触 IC カード 1 2 1）の記憶領域へ格納されてもよい。この場合、バリュ発行装置 1 4 のバリュ発行部 1 3 5 で発行された電子バリュは、親機 1 2 の非接触 IC カード 1 2 1 に転送される。例えば、バリュ発行装置 1 4 が、親機 1 2 - 2 から親機 1 2 - 1 に対してバリュを振り込む場合、バリュ発行装置 1 4 は、親機 1 2 - 2 からバリュを取得し、バリュを親機 1 2 - 1 に送信する。なお、バリュの送受信は、バリュを暗号化して安全に行われる。

【0235】

また、バリュは、バリュ発行装置 1 4 のバリュ記憶部 1 4 0 および親機 1 2 の安全なデバイスの両者の組み合わせによって記憶されてもよい。この組み合わせとして、バリュ発行装置 1 4 は、ユーザの電子バリュをバリュ記憶部 1 4 0 の中でそれぞれのユーザの口座として記憶し、その口座を管理しつつ、必要な額だけをユーザのデバイス（例えば、非接触 IC カード）へ移動させ財布のように利用させてもよい。

10

【0236】

図 1 6 は、図 1 5 のバリュ発行装置 1 4 が振り込み通知書を親機 1 2 - 1 に送信する処理を説明するフローチャートである。この処理は、バリュ発行装置 1 4 が、親機 1 2 - 2 が図 1 0 のステップ S 1 0 3 で送信したバリュ移動要求を受信したとき開始される。なお、バリュ発行装置 1 4 は、認証装置 1 3 が発行した電子証明書を、既に証明書記憶部 1 3 8 に記憶しているものとする。

【0237】

20

ステップ S 1 6 1 において、共通秘密鍵認証部 1 3 3 は、共通秘密鍵記憶部 1 3 6 から共通秘密鍵 4 4 と、秘密鍵記憶部 1 3 7 から秘密鍵 4 3 を読み出し、秘密鍵 4 3 を用いて、共通秘密鍵 4 4 を暗号化する。ステップ S 1 6 1 の処理後は、ステップ S 1 6 2 に進み、共通秘密鍵認証部 1 3 3 は、その暗号化された共通秘密鍵 4 4 を親機 1 2 - 2 に送信し、ステップ S 1 6 3 に進む。即ち、共通秘密鍵認証部 1 3 3 は、暗号化された共通秘密鍵 4 4 を、データベース 1 3 2 を介して通信部 1 3 1 に供給し、通信部 1 3 1 は、その暗号化された共通秘密鍵 4 4 を親機 1 2 - 2 に送信する。

【0238】

ステップ S 1 6 3 において、通信部 1 3 1 は、親機 1 2 - 2 から、図 1 0 のステップ S 1 0 9 で送信された暗号化された共通秘密鍵 3 7 を受信したかどうかを判定する。ステップ S 1 6 3 において、通信部 1 3 1 は、親機 1 2 - 2 から暗号化された共通秘密鍵 3 7 を受信していないと判定した場合、ステップ S 1 6 4 に進み、親機 1 2 - 2 から、図 1 0 のステップ S 1 1 0 で送信される、バリュ発行装置 1 4 と親機 1 2 - 2 の関係が正当ではないことを示すエラー通知を受信したかどうかを判定する。ステップ S 1 6 8 において、通信部 1 3 1 は、エラー通知を受信していないと判定した場合、ステップ S 1 6 3 に戻り、上述した処理を繰り返す。

30

【0239】

ステップ S 1 6 4 において、通信部 1 3 1 は、エラー通知を受信したと判定した場合、バリュ発行装置 1 4 と親機 1 2 - 2 の関係が正当ではないので、バリュ移動の不許可を示すエラー通知を送信して処理を終了する。

40

【0240】

一方、ステップ S 1 6 3 において、通信部 1 3 1 は、親機 1 2 - 2 から暗号化された共通秘密鍵 3 7 を受信したと判定した場合、その暗号化された共通秘密鍵 3 7 を公開鍵認証部 1 3 4 に供給し、ステップ S 1 6 3 からステップ S 1 6 5 に進む。ステップ S 1 6 5 において、公開鍵認証部 1 3 4 は、暗号化された共通秘密鍵 3 7 を、秘密鍵記憶部 1 3 7 に記憶している秘密鍵 4 3 を用いて復号する。

【0241】

ステップ S 1 6 5 の処理後は、ステップ S 1 6 6 に進み、公開鍵認証部 1 3 4 は、共通秘密鍵認証部 1 3 3 に、ステップ S 1 6 5 で復号した共通秘密鍵 3 7 を供給し、共通秘密鍵認証部 1 3 3 は、復号した共通秘密鍵 3 7 と共通秘密鍵記憶部 1 3 6 に記憶している共

50

通秘密鍵 4 4 が等しいかどうかを判定する。

【0 2 4 2】

ステップ S 1 6 6 において、共通秘密鍵認証部 1 3 3 は、復号した共通秘密鍵 3 7 と共通秘密鍵 4 4 が等しいと判定した場合、親機 1 2 - 2 とバリュウ発行装置 1 4 の関係は正当であると認識して、ステップ S 1 6 6 からステップ S 1 6 7 に進む。即ち、この場合、親機 1 2 - 1 において公開鍵 4 1 を用いて暗号化された共通秘密鍵 3 7 が、バリュウ発行装置 1 4 において、公開鍵 4 1 に対応する秘密鍵 4 3 を用いて正常に復号され、共通秘密鍵 3 7 が得られているので、バリュウ発行装置 1 4 は、親機 1 2 - 2 とバリュウ発行装置 1 4 が通信する間で改ざんが行われていないと認識する。

【0 2 4 3】

さらに、バリュウ発行装置 1 4 は、親機 1 2 - 2 が有する共通秘密鍵 3 7 とバリュウ発行装置 1 4 が有する共通秘密鍵 4 4 が等しいので、親機 1 2 - 2 がバリュウを管理することを認められている相手であることを認識する。即ち、バリュウ発行装置 1 4 は、バリュウ発行装置 1 4 の有する共通秘密鍵 4 4 と同一の秘密鍵 3 7 を、親機 1 2 - 2 に備えられる安全なデバイス（非接触 IC カード 1 2 1）に配布し、親機 1 2 - 2 が共通秘密鍵 4 4 と等しい共通秘密鍵 3 7 を有することを認識することによって、正しい親機 1 2 - 2 からのアクセスであることを認識する。

【0 2 4 4】

ステップ S 1 6 7 において、バリュウ発行部 1 3 5 は、親機 1 2 - 2 から親機 1 2 - 1 にバリュウを移動する。即ち、バリュウ発行部 1 3 5 は、バリュウ記憶部 1 4 0 に記憶された親機 1 2 - 2 の所定の対価に対応するバリュウを削除し、親機 1 2 - 1 のバリュウに所定の対価に対応するバリュウを追加し、これにより、親機 1 2 - 2 のユーザの電子バリュウが、そのユーザが移動端末装置 1 1 - 2 によってリソースを利用しようとしている親機 1 2 - 1 のユーザに対し、そのリソースの利用に対する対価として振り込まれる。さらに、ステップ S 1 6 7 では、バリュウ発行部 1 3 5 は、バリュウの移動完了を示す取引結果通知を生成する。

【0 2 4 5】

これにより、ユーザは、バリュウ発行装置 1 4 を経由して、他のユーザとの間で、電子バリュウの授受を行うことができる。

【0 2 4 6】

ステップ S 1 6 7 の処理後は、ステップ S 1 6 8 に進み、公開鍵認証部 1 3 4 は、秘密鍵記憶部 1 3 7 に記憶された秘密鍵 4 3 を用いて、自らの正当性を証明するために電子署名を暗号化する。そして、公開鍵認証部 1 3 4 は、その暗号化した電子署名を付加した振込み通知書を作成する。この振込み通知書は、バリュウの振込みを知らせるための振込み通知と、バリュウの振込みの詳細が記載されたレシートから構成されている。そして、公開鍵認証部 1 3 4 は、その振込み通知書、証明書記憶部 1 3 8 に記憶された電子証明書、および電子バリュウの移動完了を示す取引結果通知を、バリュウの振込先であるユーザの親機 1 2 - 1 に送信して処理を終了する。

【0 2 4 7】

一方、ステップ S 1 6 6 において、共通秘密鍵認証部 1 3 3 は、ステップ S 1 6 5 で復号した共通秘密鍵と共通秘密鍵 4 4 が等しくないと判定した場合、親機 1 2 - 2 とバリュウ発行装置 1 4 の関係は正当ではないので、バリュウ移動の不許可を示すエラー通知を送信して処理を終了する。

【0 2 4 8】

図 1 7 は、図 1 の認証装置 1 3 の詳細構成例を示している。

【0 2 4 9】

認証装置 1 3 は、通信部 1 5 1、データバス 1 5 2、公開鍵認証部 1 5 3、秘密鍵記憶部 1 5 4、証明書記憶部 1 5 5、公開鍵記憶部 1 5 6、証明書記憶部 1 5 7、および証明書失効リスト記憶部 1 5 8 から構成されている。

【0 2 5 0】

10

20

30

40

50

通信部 151 は、インターネット 21 を介して、親機 12-1、親機 12-2、およびバリュウ発行装置 14 から送信された信号を受信するとともに、親機 12-1、親機 12-2、およびバリュウ発行装置 14 に信号を送信する。通信部 151 は、データベース 152 を介して、公開鍵認証部 153 と接続されている。

【0251】

公開鍵認証部 153 は、公開鍵記憶部 156 に記憶された公開鍵と、一般公開用証明書記憶部 157 に記憶された一般公開用証明書を公開したり、電子証明書を発行する。また、公開鍵認証部 153 は、電子証明書が有効であるかどうかを判定する。

【0252】

秘密鍵記憶部 154 には、秘密鍵 42 が記憶される。証明書記憶部 155 には、認証装置 13 の電子証明書が記憶される。公開鍵記憶部 156 には、親機 12-1 の秘密鍵 35 に対応する公開鍵 39、親機 12-2 の秘密鍵 38 に対応する公開鍵 40、およびバリュウ発行装置 14 の秘密鍵 43 に対応する公開鍵 41 が記憶される。

【0253】

一般公開用証明書記憶部 157 には、公開鍵認証部 153 が発行した一般公開用の電子証明書が記憶され、この電子証明書が親機 12 やバリュウ発行装置 14 に提供される。証明書失効リスト記憶部 158 には、失効した電子証明書を示す証明書失効リストが記憶される。即ち、一般公開用証明書記憶部 157 に記憶された電子証明書が何らかの理由により失効したとき、その電子証明書が、その証明書失効リストにエントリされる。

【0254】

図 18 は、図 17 の認証装置 13 が電子証明書の判定を行う処理を説明するフローチャートである。この処理は、親機 12 などから電子証明書の有効性の判定を要求する信号を受信したとき開始する。

【0255】

ステップ S181 において、公開鍵認証部 153 は、証明書失効リスト記憶部 158 から、失効した電子証明書を示す証明書失効リストを読み出し、ステップ S182 に進む。ステップ S182 において、公開鍵認証部 153 は、親機 12 から受信した電子証明書の判定を要求する信号に基づいて、判定の対象となる電子証明書が失効しているかどうかを判定する。即ち、公開鍵認証部 153 は、ステップ S181 で読み出された証明書失効リストに、判定の対象となる電子証明書があるかどうかを判定する。

【0256】

ステップ S182 において、公開鍵認証部 153 は、判定の対象となる電子証明書が失効していると判定した場合、ステップ S183 に進み、データベース 152 を介して通信部 151 から、親機 12 に電子証明書の無効通知を送信して処理を終了する。

【0257】

ステップ S182 において、公開鍵認証部 153 は、判定の対象となる電子証明書が失効していないと判定した場合、ステップ S184 に進み、データベース 152 を介して通信部 151 から、親機 12 に電子証明書の有効通知を送信して処理を終了する。

【0258】

図 19 は、図 1 の通信システム 1 の全体の処理を説明するフローチャートである。即ち、図 19 のフローチャートは、移動端末装置 11-1 と移動端末装置 11-2 が親機 12-1 とのみ直接無線通信することができる場合に、その親機 12-1 に接続されたリソース機器 15-1 を利用するときの通信システム全体の処理を示している。

【0259】

なお、図 19 では、移動端末装置 11-1、移動端末装置 11-2、親機 12-1、親機 12-2、認証装置 13、およびバリュウ発行装置 14 は、それぞれが通信する間で改ざんが行われず、正当な関係であるとする。

【0260】

また、図 19 では、まず最初に、移動端末装置 11-1 がその本親機である親機 12-1 にリソースを要求し、その後、移動端末装置 11-2 が、無線通信できるが本親機でな

い親機 1 2 - 1 にリソースを要求するものとする。

【0 2 6 1】

ステップ S 2 3 1 において、移動端末装置 1 1 - 1 は、その本親機である親機 1 2 - 1 と双方向認証するために、共通秘密鍵 3 1 を暗号化して、親機 1 2 - 1 に送信する。

【0 2 6 2】

ステップ S 2 5 1 において、親機 1 2 - 1 は、移動端末装置 1 1 - 1 から暗号化された共通秘密鍵 3 1 を受信する。ステップ S 2 5 2 において、親機 1 2 - 1 は、共通秘密鍵 3 3 を暗号化し、移動端末装置 1 1 - 1 に送信する。

【0 2 6 3】

ステップ S 2 3 2 において、移動端末装置 1 1 - 1 は、親機 1 2 - 1 から暗号化された共通秘密鍵 3 3 を受信する。ステップ S 2 3 3 において、移動端末装置 1 1 - 1 は、その暗号化された共通秘密鍵 3 3 を復号し、復号した共通秘密鍵 3 3 を暗号化して、暗号化した共通秘密鍵 3 3 を親機 1 2 - 1 に送信する。 10

【0 2 6 4】

ステップ S 2 5 3 において、親機 1 2 - 1 は、暗号化された共通秘密鍵 3 3 を、移動端末装置 1 1 - 1 から受信する。ステップ S 2 5 4 において、親機 1 2 - 1 は、暗号化された共通秘密鍵 3 3 を復号する。親機 1 2 - 1 は、復号した共通秘密鍵 3 3 から、親機 1 2 - 1 と移動端末装置 1 1 - 1 の関係が正当であるかどうかを判定する。この例では、親機 1 2 - 1 と移動端末装置 1 1 - 1 は正当な関係であるので、親機 1 2 - 1 は、ステップ S 2 5 1 で移動端末装置 1 1 - 1 から受信した暗号化された共通秘密鍵 3 1 を復号し、その復号した共通秘密鍵 3 1 を暗号化して、移動端末装置 1 1 - 1 に送信する。 20

【0 2 6 5】

ステップ S 2 3 4 において、移動端末装置 1 1 - 1 は、親機 1 2 - 1 から暗号化された共通秘密鍵 3 1 を受信し、その暗号化された共通秘密鍵 3 1 を復号する。移動端末装置 1 1 - 1 は、復号した共通秘密鍵 3 1 から、親機 1 2 - 1 と移動端末装置 1 1 - 1 の関係が正当であるかどうかを判定する。この例では、親機 1 2 - 1 と移動端末装置 1 1 - 1 の関係は正当であるので、双方向認証を完了し、ステップ S 2 3 5 において、移動端末装置 1 1 - 1 は、リソースを要求する信号を親機 1 2 - 1 に送信する。

【0 2 6 6】

即ち、移動端末装置 1 1 - 1 は、その本親機である親機 1 2 - 1 と双方向認証することにより、移動端末装置 1 1 - 1 を使用するユーザが正しいユーザであることを、通信システム 1 のユーザに保証する。 30

【0 2 6 7】

ステップ S 2 5 5 において、親機 1 2 - 1 は、移動端末装置 1 1 - 1 からリソースを要求する信号を受信する。ステップ S 2 5 6 において、親機 1 2 - 1 は、リソースを要求する信号に基づいて、要求対象となるリソース機器 1 5 - 1 にリソースを要求する信号を送信する。

【0 2 6 8】

ステップ S 2 9 1 において、リソース機器 1 5 - 1 は、親機 1 2 - 1 からリソースを要求する信号を受信する。ステップ S 2 9 2 において、リソース機器 1 5 - 1 は、リソースを要求する信号に基づいて、要求対象となるリソースを親機 1 2 - 1 を介して、移動端末装置 1 1 - 1 に送信する。 40

【0 2 6 9】

ステップ S 2 3 6 において、移動端末装置 1 1 - 1 は、リソース機器 1 5 - 1 から親機 1 2 - 1 を介して、リソースを受信し、これにより、リソース機器 1 5 - 1 を利用することが可能な状態となる。

【0 2 7 0】

一方、移動端末装置 1 1 - 2 は、ステップ S 2 0 1 において、リソース情報を取得するために、その本親機でない親機 1 2 - 1 にデバイス探索を要求する信号を送信する。

【0 2 7 1】

ステップ S 2 5 7 において、親機 1 2 - 1 は、移動端末装置 1 1 - 2 からデバイス探索を要求する信号を受信し、デバイス探索要求を許可するかどうかを判定する。図 1 9 では、ステップ S 2 5 8 において、親機 1 2 - 1 は、デバイス探索を許可し、デバイス探索を許可する信号を、移動端末装置 1 1 - 2 に送信する。

【0 2 7 2】

ステップ S 2 0 2 において、移動端末装置 1 1 - 2 は、親機 1 2 - 1 からデバイス探索を許可する信号を受信する。ステップ S 2 0 3 において、移動端末装置 1 1 - 2 は、親機 1 2 - 1 が取得できるリソースの情報（親機 1 2 - 1 が、移動端末装置 1 1 - 2 に提供することができるリソースの情報）を要求する信号を、親機 1 2 - 1 に送信する。

【0 2 7 3】

ステップ S 2 5 9 において、親機 1 2 - 1 は、移動端末装置 1 1 - 2 からリソースの情報を要求する信号を受信する。ステップ S 2 6 0 において、親機 1 2 - 1 は、リソース情報を移動端末装置 1 1 - 2 に送信する。

【0 2 7 4】

ステップ S 2 0 4 において、移動端末装置 1 1 - 2 は、親機 1 2 - 1 からリソース情報を受信する。ステップ S 2 0 5 において、移動端末装置 1 1 - 2 は、親機 1 2 - 2 と双方向認証をするため、共通秘密鍵 3 2 を暗号化し、その暗号化した共通秘密鍵 3 2 を親機 1 2 - 2 に送信する。

【0 2 7 5】

ステップ S 3 1 1 において、親機 1 2 - 2 は、移動端末装置 1 1 - 2 から、暗号化された共通秘密鍵 3 2 を受信する。ステップ S 3 1 2 において、親機 1 2 - 2 は、共通秘密鍵 3 6 を暗号化し、暗号化した共通秘密鍵 3 6 を移動端末装置 1 1 - 2 に送信する。

【0 2 7 6】

ステップ S 2 0 6 において、移動端末装置 1 1 - 2 は、親機 1 2 - 2 から暗号化した共通秘密鍵 3 6 を受信し、暗号化した共通秘密鍵 3 6 を復号する。移動端末装置 1 1 - 2 は、復号した共通秘密鍵 3 6 から、移動端末装置 1 1 - 2 と親機 1 2 - 2 の関係が正当であるかどうかを判定する。この例の場合、移動端末装置 1 1 - 2 と親機 1 2 - 2 の関係は正当であるので、ステップ S 2 0 7 において、移動端末装置 1 1 - 2 は、復号した共通秘密鍵 3 6 を暗号化し、暗号化した共通秘密鍵 3 6 を親機 1 2 - 2 に送信する。

【0 2 7 7】

ステップ S 3 1 3 において、親機 1 2 - 2 は、移動端末装置 1 1 - 2 から暗号化した共通秘密鍵 3 6 を受信し、その暗号化した共通秘密鍵 3 6 を復号する。親機 1 2 - 2 は、復号した共通秘密鍵 3 6 から、親機 1 2 - 2 と移動端末装置 1 1 - 2 の関係は正当であるかどうかを判定する。この例の場合、親機 1 2 - 2 と移動端末装置 1 1 - 2 の関係は正当であるので、ステップ S 3 1 4 において、親機 1 2 - 2 は、ステップ S 3 1 1 で移動端末装置 1 1 - 2 から受信した暗号化された共通秘密鍵 3 2 を復号し、復号した共通秘密鍵 3 2 を暗号化する。親機 1 2 - 2 は、その暗号化した共通秘密鍵 3 2 を移動端末装置 1 1 - 2 に送信する。

【0 2 7 8】

ステップ S 2 0 8 において、移動端末装置 1 1 - 2 は、親機 1 2 - 2 から暗号化された共通秘密鍵 3 2 を受信し、その暗号化された共通秘密鍵 3 2 を復号する。移動端末装置 1 1 - 2 は、復号した共通秘密鍵 3 2 から、移動端末装置 1 1 - 2 と親機 1 2 - 2 の関係が正当であるかどうかを判定する。この例では、移動端末装置 1 1 - 2 と親機 1 2 - 2 の関係が正当であるので、双方向認証を完了し、ステップ S 2 0 9 において、移動端末装置 1 1 - 2 は、リソースを要求する信号を親機 1 2 - 2 に送信する。

【0 2 7 9】

ステップ S 3 1 5 において、親機 1 2 - 2 は、移動端末装置 1 1 - 2 から、リソースを要求する信号を受信する。ステップ S 3 1 6 において、親機 1 2 - 2 は、親機 1 2 - 1 にリソース情報の識別子と利用方法を明記した利用権発行要求と電子証明書を、親機 1 2 - 1 に送信する。

10

20

30

40

50

【0280】

ステップS261において、親機12-1は、親機12-2から利用権発行要求と電子証明書を受信する。ステップS262において、親機12-1は、その電子証明書が有効であるかどうかの判定要求を認証装置13に送信する。

【0281】

ステップS361において、認証装置13は、親機12-1から電子証明書の判定要求を受信し、その電子証明書が有効であるかどうかを判定する。なお、ここでは、電子証明書は有効であるものとし、ステップS362において、認証装置13は、親機12-1に対象の電子証明書が有効であることを示す信号を送信する。

【0282】

ステップS263において、親機12-1は、認証装置13から電子証明書が有効であることを示す信号を受信する。ステップS264において、親機12-1は、リソースの利用を許可するための対価を記載したリソース利用条件文と電子証明書を、親機12-2に送信する。

【0283】

ステップS317において、親機12-2は、親機12-1からリソース利用条件文と電子証明書を受信する。ステップS318において、親機12-2は、バリュウ発行装置14にバリュウ移動要求を送信する。

【0284】

ステップS341において、バリュウ発行装置14は、親機12-2からバリュウ移動要求を受信する。ステップS342において、バリュウ発行装置14は、親機12-2と双方向認証するため、共通秘密鍵44を暗号化して、暗号化した共通秘密鍵44を親機12-2に送信する。

【0285】

ステップS320において、親機12-2は、バリュウ発行装置14から、暗号化された共通秘密鍵44を受信し、その暗号化された共通秘密鍵44を復号する。親機12-2は、復号した共通秘密鍵44から、親機12-2とバリュウ発行装置14の関係が正当であるかどうかを判定する。この例の場合、親機12-2とバリュウ発行装置14の関係は正当であるので、ステップS320において、親機12-2は、共通秘密鍵37を暗号化し、暗号化した共通秘密鍵37をバリュウ発行装置14に送信する。

【0286】

ステップS343において、バリュウ発行装置14は、親機12-2から暗号化された共通秘密鍵37を受信し、その暗号化された共通秘密鍵37を復号する。バリュウ発行装置14は、復号した共通秘密鍵37から、バリュウ発行装置14と親機12-2の関係が正当であるかどうかを判定する。この例の場合、バリュウ発行装置14と親機12-2の関係は正当であるので、ステップS344において、バリュウ発行装置14は、ステップS341で受信したバリュウ移動要求に応じてバリュウを移動し、即ち、ここでは、親機12-1のユーザから親機12-1のユーザにバリュウを移動し、バリュウが移動されたことを示す振込み通知と電子証明書を、親機12-1に送信する。

【0287】

ステップS265において、親機12-1は、バリュウ発行装置14から、振込み通知書と電子証明書を受信する。ステップS266において、親機12-1は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置13に送信する。

【0288】

ステップS363において、認証装置13は、親機12-1から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機12-2の電子証明書は有効であるので、ステップS364において、認証装置13は、親機12-1に対象の電子証明書が有効であることを示す信号を送信する。

【0289】

ステップS267において、親機12-1は、認証装置13から電子証明書が有効であ

10

20

30

40

50

ることを示す信号を受信する。ステップ S 2 6 8 において、親機 1 2 - 1 は、リソースを利用する権利を記載した権利文を発行し、その権利文と電子証明書を親機 1 2 - 2 に送信する。

【0 2 9 0】

ステップ S 3 2 1 において、親機 1 2 - 2 は、親機 1 2 - 1 から送信されてくる権利文と電子証明書を受信する。ステップ S 3 2 2 において、親機 1 2 - 2 は、その電子証明書が有効であるかどうかの判定を要求する信号を認証装置 1 3 に送信する。

【0 2 9 1】

ステップ S 3 6 5 において、認証装置 1 3 は、親機 1 2 - 2 から、電子証明書の判定を要求する信号を受信し、その電子証明書が有効であるかどうかを判定する。この例の場合、親機 1 2 - 1 の電子証明書は有効であるので、ステップ S 3 6 6 において、認証装置 1 3 は、親機 1 2 - 2 に対象の電子証明書が有効であることを示す信号を送信する。 10

【0 2 9 2】

ステップ S 3 2 3 において、親機 1 2 - 2 は、認証装置 1 3 から電子証明書が有効であることを示す信号を受信する。ステップ S 3 2 4 において、親機 1 2 - 2 は、ステップ S 3 2 1 で、親機 1 2 - 1 から受信した権利文を、移動端末装置 1 1 - 2 に送信する。

【0 2 9 3】

ステップ S 2 1 0 において、移動端末装置 1 1 - 2 は、親機 1 2 - 1 から権利文を受信する。ステップ S 2 1 1 において、移動端末装置 1 1 - 2 は、その権利文とリソースを要求する信号を、親機 1 2 - 1 に送信する。 20

【0 2 9 4】

ステップ S 2 6 9 において、親機 1 2 - 1 は、移動端末装置 1 1 - 2 から、権利文とリソースを要求する信号を受信する。ステップ S 2 7 0 において、親機 1 2 - 1 は、リソース機器 1 5 - 1 にリソースを要求する信号を送信する。

【0 2 9 5】

ステップ S 2 9 3 において、リソース機器 1 5 - 1 は、親機 1 2 - 1 からリソースを要求する信号を受信する。ステップ S 2 9 4 において、リソース機器 1 5 - 1 は、親機 1 2 - 1 から要求されたリソースを親機 1 2 - 1 を介して、移動端末装置 1 1 - 2 に送信する。

【0 2 9 6】

ステップ S 2 1 2 において、リソース機器 1 5 - 1 から、リソースを受信する。 30

【0 2 9 7】

以上により、移動端末装置 1 1 - 2 は、親機 1 2 - 1 から権利文を取得することにより、親機 1 2 - 1 に接続されたリソース機器 1 5 - 1 を利用できる環境を得ることができる。

【0 2 9 8】

以上のように、通信システム 1 では、バリュー発行装置 1 4 は、バリューの管理をする親機 1 2 に対して共通秘密鍵 4 4 と同一の秘密鍵 3 4 や 3 7 を送信し、親機 1 2 の非接触 I C カード 1 2 1 に記憶させる。親機 1 2 は、個人情報情報を格納するユーザに、親機 1 2 と通信可能にするための共通秘密鍵を格納した非接触 I C カード 7 1 を発行する。これにより、ユーザは、非接触 I C カード 7 1 の情報を移動端末装置 1 1 に読み込ませるだけで、本親機である親機 1 2 と通信をし、バリューの移動をすることができる。そして、ユーザは、上述した一連の処理を、例えば、非接触 I C カード 7 1 を移動端末装置 1 1 に、ワンタッチすることで行わせることができ、この場合、利便性の高い付加価値を提供することができる。 40

【0 2 9 9】

さらに、認証情報やそれに伴うユーザの個人情報情報を管理する本親機となる親機 1 2 を、例えばユーザ宅のホームサーバという形で、移動端末装置 1 1 とは別に設けたので、ユーザと移動端末装置 1 1 とは依存関係がなく、リソースの利用時にのみユーザの認証を行えば済む。また、ユーザは、個人情報情報をバリュー発行装置に管理させることなく、自らの所 50

有する親機 1 2 に格納し、バリューの決済情報だけを親機 1 2 とバリュー発行装置 1 4 との間でやりとりするだけで済む。さらに、ユーザが移動する場合においても、ユーザは、移動した空間にある機器（リソース）を、匿名のままユーザの嗜好に合わせた操作性で操作することができる。

【0300】

また、図 1 の通信システム 1 によれば、ユーザが、移動した空間にある移動端末装置 1 1-2 を操作することにより、そのユーザが個人情報管理する親機（本親機） 1 2-2 が、バリュー発行装置 1 4 の仲介の下、他人の親機 1 2-1 に電子バリューを支払って、その親機 1 2-1 のリソースの利用権を入手し、その利用権を、移動端末装置 1 1-2 が受け取って、親機 1 2-1 に提示することで移動端末装置 1 1-2 のユーザは、他人の親機 1 2-1 のリソースを、匿名のまま利用することができる。即ち、バリュー発行装置 1 4 は、移動端末装置 1 1-2 のユーザの親機 1 2-2 から他人の親機 1 2-1 に対しての電子バリューの振込みを仲介するだけであり、ユーザの個人情報の管理は、親機 1 2 で行われる。従って、電子バリューの決済の場合と、個人情報の管理の場合とが完全に分離されているといえることができる。なお、移動端末装置 1 1-2 からバリュー発行装置 1 4 にアクセスし、電子バリューを、リソースを利用しようとする親機 1 2-1 に振込み、移動端末装置 1 1-2 から親機 1 2-1 のリソースを利用することも可能である。但し、この場合、親機 1 2-1 に対する、移動端末装置 1 1-2 のユーザの匿名性は確保されるが、移動端末装置 1 1-2 のユーザの個人情報の管理は、移動端末装置 1 1-2 がアクセスするバリュー発行装置 1 4 で行われることになる。

【0301】

さらに、移動端末装置 1 1-2 は、リソースを利用する親機 1 2-1 を介して、本親機である親機 1 2-2 にアクセスして、そのリソースの利用権を取得するので、利用したいリソースに近い位置で、その利用権を得ることができる。

【0302】

ここで、移動端末装置 1 1 としては、例えば、PDA(Personal Digital Assistant)や、携帯用コンピュータ、携帯電話機、腕時計、デジタルスチルカメラ、デジタルビデオカメラなどの携帯性に優れた装置を採用することが可能である。

【0303】

また、出先のユーザが移動端末装置 1 1 から利用するリソースとしては、例えば、「装置」や、「情報」、「情報に対するライセンス」などがある。

【0304】

リソースとしての「装置」には、例えば、無線アクセスポイントや、テレビジョン受像機、電話機などが含まれる。リソースとして「装置」を利用するケースとしては、例えば、出先のユーザが、移動端末装置 1 1 から、他人の無線アクセスポイントを利用してインターネットに接続する場合がある。

【0305】

また、リソースとしての「情報」には、いわゆるホームサーバやチャンネルサーバなどで構成される親機 1 2-1 が管理するコンテンツその他の情報などが含まれる。リソースとして「情報」を利用するケースとしては、例えば、出先のユーザが、親機 1 2-1 としてのチャンネルサーバに蓄えられたコンテンツを視聴する場合がある。

【0306】

さらに、リソースとしての「情報に対するライセンス」には、情報が暗号化されている場合に、その暗号化を解くための鍵などが含まれる。リソースとして「情報に対するライセンス」を利用するケースとしては、例えば、携帯端末装置 1 1 に、ネットワーク経由でダウンロードした、暗号化されたコンテンツを視聴する場合に、そのコンテンツを視聴するためのライセンスとしての暗号鍵を取得するときなどがある。

【0307】

なお、上述した一連の処理では、移動端末装置 1 1-1 と移動端末装置 1 1-2 のユーザは異なっていたが、同一ユーザの親機や移動端末装置間でも同様に電子バリューの移動

をすることができる。

【0308】

上述した実施の形態に関し、具体例を挙げてさらに説明を加える。

【0309】

図20は、ユーザBがユーザAの家で、ユーザAのPC（パーソナルコンピュータ）を借り、その対価を支払う例を説明するための図であり、そのような場合におけるシステムの構成例を示している。移動端末装置201-1は、ユーザAが所持する装置であり、移動端末装置201-2は、ユーザBが所持する装置である。移動端末装置201-1、201-2は、それぞれ携帯電話や、携帯可能なCDプレーヤなどである。

【0310】

移動端末装置201-1には、ユーザAのホームサーバ202-1のアドレスが登録され、移動端末装置201-2には、ユーザBのホームサーバ202-2のアドレスが登録されている。

【0311】

ユーザAが管理するホームサーバ202-1は、同じくユーザAが管理しているPC203やTV（テレビジョン受像機）204を管理する。このPC203やTV204は、家庭内ネットワークを介してホームサーバ202-1と接続されているリソースである。また、ホームサーバ202-1は、ユーザAの個人情報も保管している。

【0312】

同様に、ユーザBが管理するホームサーバ202-2は、ユーザBが管理するリソースを管理すると共に、ユーザBの個人情報も保管する。ホームサーバ202-1やホームサーバ202-2は、それぞれ無線により直接的に、または、アクセスポイント（図20においては不図示）を介して他のホームサーバと通信することができるよう構成されている。

【0313】

また、携帯端末装置201-1、201-2は、接続したホームサーバ202-1、202-2を介し、そしてインターネット205を経由し、他のホームサーバなどと通信することができるよう構成されている。

【0314】

インターネット205には、認証装置206も接続されている。認証装置206は、PKI処理のための証明書を発行する機関が管理する装置であり、証明書の管理を行うための装置である。インターネット205には、バリュウ発行装置207も接続されている。バリュウ発行装置207は、各ユーザのバリュウの交換を仲介する装置（対価の支払いに係わる処理を実行する装置）である。

【0315】

ここで、図20に示したシステムと図1に示したシステムとの対応関係を記載しておく。移動端末装置201-1は、移動端末装置11-1であり、移動端末装置201-2は、移動端末装置11-2である。ホームサーバ202-1は、親機12-1であり、ホームサーバ202-2は、親機12-2である。PC203は、リソース機器16-2であり、TV204は、リソース機器15-2である。

【0316】

インターネット205は、インターネット21であり、認証装置206は、認証装置13である。バリュウ発行装置207は、バリュウ発行装置14である。このように、図20は、図1と対応関係があり、図1およびそれ以降の図を参照して説明した事項は、図20に示したシステムに関する事項として適用できるため、既に説明した部分については、適宜説明を省略する。

【0317】

次に、図21のフローチャートを参照し、ユーザBが移動端末装置201-2を保持している状態でユーザA宅に行き、ユーザA宅に設置され、ユーザAにより管理されているPC203を使用するときに、図20に示したシステムで行われる処理について説明する

10

20

30

40

50

。なお、以下の説明においては、認証局（認証装置 206）で P K I により行われる、各ユーザのアクセスの信頼性を確認する手順については、既に説明した事項と重なるため省略する。

【0318】

まず、移動端末装置の初期化に係わる処理が実行される。移動端末装置の初期化に係わる処理は、ここでは、移動端末装置 201-2 とホームサーバ 202-2 との間で行われる。まずステップ S 401 において、ユーザ B が保持する移動端末装置 201-2 は、ホームサーバ 202-2 にアクセスする。

【0319】

ステップ S 471 において移動端末装置 201-2 からのアクセスを受けたホームサーバ 202-2 は、ステップ S 472 において、自己が管理しているユーザ B の個人情報の一部を送信する。送信された個人情報は、ステップ S 402 において、移動端末装置 201-2 に受信され、保持される。 10

【0320】

移動端末装置 201-2 には、ホームサーバ 202-2 のアドレスが登録されているため、ホームサーバ 202-2 にアクセスすることが可能とされている。また、移動端末装置 201-2 は、ユーザ B が登録されており、ユーザ B しか使うことができないように構成されている。例えば、ユーザ B の指紋が登録されており、指紋認証が正常に行われな限り、移動端末装置 201-2 は起動されないように構成されている。

【0321】

そして、指紋認証などが用いられた認証処理が正常に行われた後（この場合、ユーザ B であると確認がとれた後）、移動端末装置 201-2 は、使用可能な状態とされる。使用可能な状態とされた後、ホームサーバ 202-2 とアクセス可能であれば、上述したような処理が、移動端末装置 201-2 とホームサーバ 202-2 との間で実行される。 20

【0322】

移動端末装置 201-2 は、ユーザ B の個人情報を保持した後の時点で、定期的にデバイス探索要求を発信している（ステップ S 403）。その定期的に発信されているデバイス探索要求を、ステップ S 421 の処理として受信したホームサーバ 202-1 は、ステップ S 422 において、自己のアドレス、デバイス探索要求を発信してきた端末（この場合、移動端末装置 201-2）に一時的に与える I D、および、移動端末装置 201-2 がインターネット 205 を介して他の装置とデータの授受を行えるようにするために必要となる情報（例えば、デフォルトルータのアドレスなど）を、移動端末装置 201-2 に通知する。 30

【0323】

このようなホームサーバ 202-1 からのデータは、ステップ S 404 において、移動端末装置 201-2 に受信され、記憶される。ステップ S 405 において、移動端末装置 201-2 は、ホームサーバ 202-2 に対してリソース要求を出す。移動端末装置 201-2 は、先程の処理で、ホームサーバ 202-2 のアドレスを取得し記憶しているため、ホームサーバ 202-2 と通信することが出来る状態とされている。なお、この通信の際、必要に応じ、ホームサーバ 202-1 から与えられた I D も用いられる。 40

【0324】

ステップ S 423 において、ホームサーバ 202-1 は、リソース要求を受信すると、ステップ S 424 の処理として、自己の管理するリソースに関する情報を、移動端末装置 201-2 に対して通知する。リソース情報として、ホームサーバ 202-1 から移動端末装置 201-2 に対して通知される情報について説明する。

【0325】

リソース情報は、リソースの名前、設置場所、現在使用中であるか否かを表す情報、使用する際に必要となる対価、移動端末装置から操作できる操作のリストなどを含む情報である。例えば、図 20 を参照するに、ホームサーバ 202-1 には、P C 203 が接続されている。P C 203 に関するリソース情報としては、P C 203 という名称であり、例 50

えば、居間に設置され、現在使用中ではなく、対価として例えば100円を必要とし、移動端末装置201-2から操作できる操作のリストを含む情報である。

【0326】

同様のリソース情報が、ホームサーバ202-1に接続されているTV204に関しても作成され、PC203のリソース情報と合わせて、移動端末装置201-2に対して通知される。

【0327】

このようなリソース情報を、ステップS406の処理として受信した移動端末装置201-2は、そのリソース情報を記憶する。

【0328】

このようにして、リソース情報を取得した移動端末装置201-2は、次に、リソースの選択に係わる処理を実行する。

【0329】

まず前提として、移動端末装置201-2は、取得したリソース情報を基に、ユーザにリソースに関する情報を提示する。提示の仕方は、どのようなものでも良いが、例えば、移動端末装置201-2は、図2に示すような構成を有し、表示部64を有していれば、その表示部64を用いて提示が行われるように構成する。具体的には、まず表示部64に、リソースの一覧（この場合、例えば、PC203とTV204が列記されたものである）が表示される。その一覧を参照しユーザBが、使用したいリソース（機器）を選択すると、その選択された機器に関する詳細な情報に、表示部64の表示が切り換えられる。

【0330】

このようにして、ホームサーバ202-1から詳細情報まで含まれるリソース情報が通知され、段階的にユーザに提示されるようにしても良い。

【0331】

他のリソース情報の提示の仕方としては、リソース（例えば、PC203）と直接的に近接通信を行うことにより、そのリソースの詳細な情報が取得されるようにしても良い。例えば、まず、ステップS407において、移動端末装置201-2からPC203に対して、近接通信によりリソース情報の要求が出される。

【0332】

そのような要求をステップS451において受信したPC203は、ステップS452において、自己の詳細な情報（例えば、使用するのに必要とされる金額など）を移動端末装置201-2に対して通知する。そのような通知を、ステップS408において受信した移動端末装置201-2は、その受信した情報を、ユーザBに対して提示する。

【0333】

いずれの手順により、リソース情報が移動端末装置201-2に対して通知されるようにしても良いが、結果としてユーザBは、リソース情報を参照し、使用したい機器を選択する。ここでは、ユーザBは、PC203を使用したい機器として選択したとして説明を続ける。

【0334】

ユーザBが、使用したい機器としてPC203を選択すると、移動端末装置201-2の表示部64には、“1時間100円で使用しますか？”といったようなメッセージが表示される。これは、ユーザAが所有するPC203を使用することにより、その対価を支払わなくてはならないといったようなことをユーザBに認識させるためのものである。ユーザBは、そのようなメッセージを確認し、対価を支払ってPC203を使用する場合、所定の操作、例えば、表示部64に表示された“YES”といったようなボタン（不図示）を操作する。

【0335】

そのような操作が行われた場合、移動端末装置201-2は、ステップS409において、ホームサーバ202-2に対して、使用したいリソース（この場合、PC203）と、そのリソースを管理するホームサーバ（この場合、ホームサーバ202-1）のアドレ

10

20

30

40

50

スを通知する。このような通知を、ステップS 4 7 3の処理として受信したホームサーバ2 0 2－2は、ステップS 4 7 4において、ホームサーバ2 0 2－1に対して、当該リソースの使用を要求する旨と、使用条件（この場合、例えば、1時間使用するという条件）を通知する。

【0 3 3 6】

このような通知を、ステップS 4 2 5の処理として受信したホームサーバ2 0 2－1は、ステップS 4 2 6において、自己に登録された機器（リソース）情報から、通知された使用条件（この場合、1時間使用するという条件）を満たすために、ユーザBが支払うべき対価（この場合、1時間×1 0 0円＝1 0 0円という計算がなされる）を算出し、その算出結果を、トランザクション番号と共に、ホームサーバ2 0 2－2に対して通知する。 10

【0 3 3 7】

ステップS 4 7 5において、ホームサーバ2 0 2－1からの通知を受信したホームサーバ2 0 2－2は、ステップS 4 7 6において、バリュウ発行装置2 0 7に対して、トランザクション番号と共に、ホームサーバ2 0 2－1宛にバリュウの振り込み要求を行う。バリュウ発行装置2 0 7は、ステップS 4 9 1において、ホームサーバ2 0 2－2からの通知を受信すると、ホームサーバ2 0 2－1との間で、バリュウの振り込みの処理が実行される（ステップS 4 9 2、ステップS 4 2 7）。

【0 3 3 8】

またバリュウ発行装置2 0 7は、ホームサーバ2 0 2－2との間で、バリュウの減額処理を実行する（ステップS 4 9 3、ステップS 4 7 7）。このようにして、バリュウ発行装置2 0 7は、ホームサーバ2 0 2－1に対してバリュウの振り込みの処理を実行し、その振り込みされるバリュウを、ホームサーバ2 0 2－2から減額するという処理を実行する。 20

【0 3 3 9】

バリュウの振り込み、減額の処理がそれぞれ正常に行われると、バリュウ発行装置2 0 7は、ステップS 4 9 4において、ホームサーバ2 0 2－1に対して、トランザクションが正常に終了されたことを、トランザクション番号と共に通知する。

【0 3 4 0】

ホームサーバ2 0 2－1は、このような通知をバリュウ発行装置2 0 7から、ステップS 4 2 8において受信すると、ステップS 4 2 9において、トランザクション番号から、使用を許可する（使用を要求されていた）機器、その使用条件、および、使用権を、ホームサーバ2 0 2－2に対して発行する。同様の情報を、ステップS 4 3 0において、ホームサーバ2 0 2－1は、P C 2 0 3に対しても発行する。 30

【0 3 4 1】

ステップ4 7 8において、ホームサーバ2 0 2－1により発行された使用権などを受信したホームサーバ2 0 2－2は、ステップS 4 7 9において、移動端末装置2 0 1－2に対して、使用権を渡す。

【0 3 4 2】

ステップS 4 1 0において、ホームサーバ2 0 2－2から使用権を受信した移動端末装置2 0 1－2は、ステップS 4 1 1において、P C 2 0 3に対して、使用権を提示する。この提示は、ホームサーバ2 0 2－1を介して行われても良いし、直接的に近距離無線通信などが用いられて行われるようにしても良い。使用権を提示されたP C 2 0 7は、ステップS 4 5 5において、まず、ホームサーバ2 0 2－1から渡された使用権と、移動端末装置2 0 1－2から提示された使用権が一致するか否かを判断する。 40

【0 3 4 3】

使用権が一致すると判断された場合、ステップS 4 5 5において、P C 2 0 7は、移動端末装置2 0 1－2に対してアクセス許可を通知する。なお、使用権が一致しないと判断された場合、P C 2 0 7は、アクセス許可を通知しない（アクセス許可をしないということを知らせるようにしても良い）。

【0 3 4 4】

PC207は、アクセス許可を通知することにより、また、移動端末装置201-2は、アクセス許可を通知されることにより、互いにデータの授受が行える状態とされる。すなわち、PC207は、移動端末装置201-2からの操作指示を受け入れる状態とされる。このように、移動端末装置201-2で、PC207を操作できる状態とされた場合、移動端末装置201-2の所有者であるユーザBの嗜好が反映された形でPC207を操作できるようにするための情報が、移動端末装置201-2からPC207に対して通知される。

【0345】

すなわち、ステップS413において、移動端末装置201-2は、PC207に対して、自己が管理しているユーザBの嗜好情報を通知する。PC207は、そのような嗜好情報を受信すると、その嗜好情報に基づき、ユーザB用にカスタマイズされた環境を構築する。例えば、嗜好情報として、ユーザBがいつも使用しているログイン画面に関する情報が通知された場合、その画面がログイン時にPC207のディスプレイ（不図示）上に表示される。

【0346】

このように、本発明を適用することにより、他のユーザが管理する装置を対価を支払って使用することが可能となる。

【0347】

なお、本明細書において、フローチャートに記載された処理は、ステップとして記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0348】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。

【図面の簡単な説明】

【0349】

【図1】本発明を適用した通信システムの構成例を示すブロック図である。

【図2】図1の移動端末装置の構成例を示すブロック図である。

【図3】図2の移動端末装置におけるリソース取得処理を説明するフローチャートである。

【図4】図3のステップS2およびステップS6の共通秘密鍵認証処理を説明するフローチャートである。

【図5】図3のステップS5のリソース情報取得処理を説明するフローチャートである。

【図6】図1の親機の構成例を示す図である。

【図7】図6のリソース制御部の構成例を示す図である。

【図8】図6の親機におけるリソース制御処理を説明するフローチャートである。

【図9】図8のステップS71のリソース送信処理を説明するフローチャートである。

【図10】図8のステップS71のリソース送信処理を説明するフローチャートである。

【図11】電子証明書の例を示す図である。

【図12】図6の親機におけるリソース情報送信処理を説明する図である。

【図13】図6の親機におけるリソース利用条件文発行処理を説明するフローチャートである。

【図14】図6の親機における権利文発行要求処理を説明するフローチャートである。

【図15】図1のバリュウ発行装置の構成例を示す図である。

【図16】図15のバリュウ発行装置における振込み通知書送信処理を説明するフローチャートである。

【図17】図1の認証装置の構成例を示す図である。

【図18】図17の認証装置における電子証明書判定処理を説明する図である。

【図19】図1の通信システムにおけるリソース取得処理を説明する図である。

【図20】他のシステムの構成例を示す図である。

10

20

30

40

50

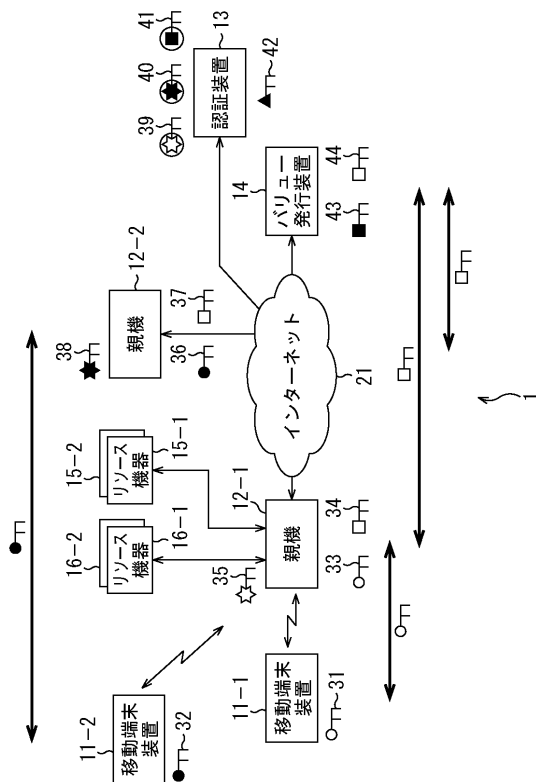
【図 2 1】図 2 0 に示したシステムの動作を説明するフローチャートである。

【符号の説明】

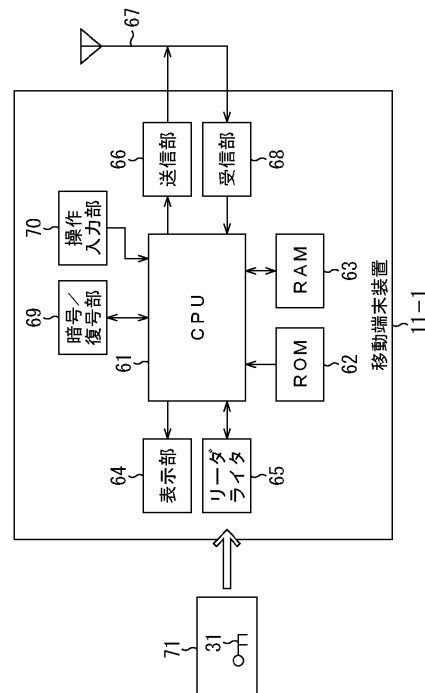
【0 3 5 0】

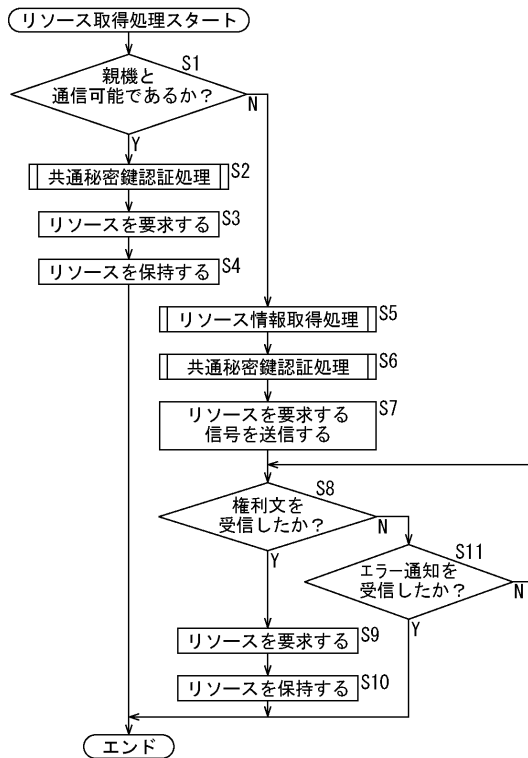
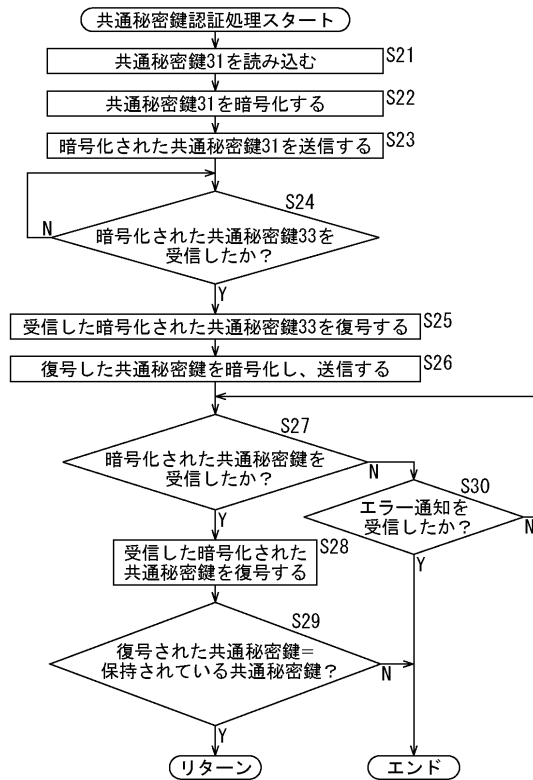
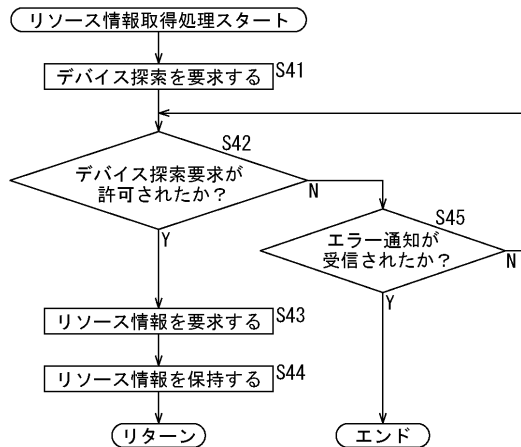
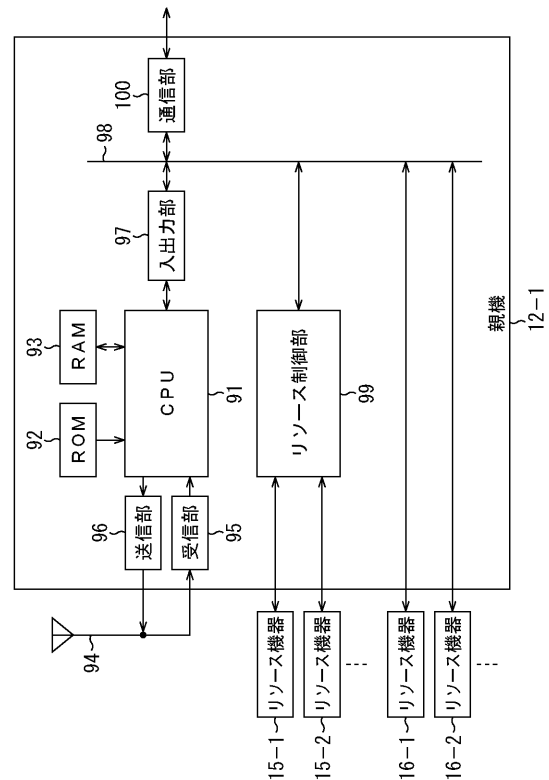
1 1 移動端末装置, 1 2 親機, 1 3 認証装置, 1 4 バリユー発行装置,
1 5 リソース, 1 6 リソース, 2 1 インターネット, 3 1 共通秘密鍵,
3 2 共通秘密鍵, 3 3 共通秘密鍵, 3 4 共通秘密鍵, 3 5 秘密鍵, 3
6 共通秘密鍵, 3 7 共通秘密鍵, 3 8 秘密鍵, 3 9 公開鍵, 4 0 公開
鍵, 4 1 公開鍵, 4 2 秘密鍵, 4 3 秘密鍵, 4 4 共通秘密鍵, 6 9
暗号/復号部 7 1 非接触 I C カード, 1 2 1 非接触 I C カード, 1 1 7 暗号/
復号部 1 3 3 共通秘密鍵認証部, 1 3 4 公開鍵認証部, 1 3 5 バリユー発行 10
部, 1 5 3 公開鍵認証部, 1 5 8 証明書失効リスト記憶部

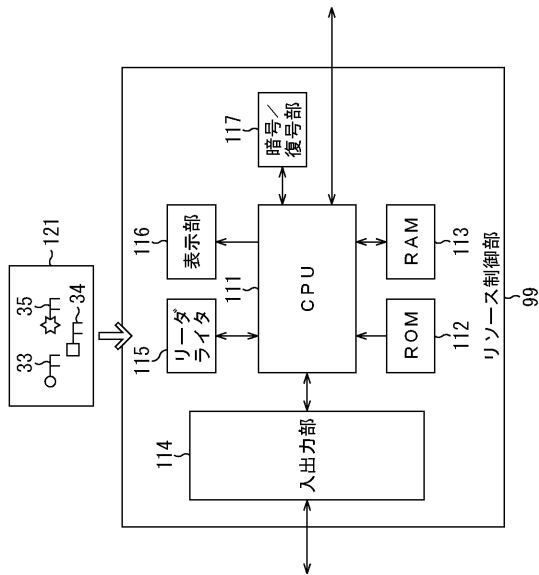
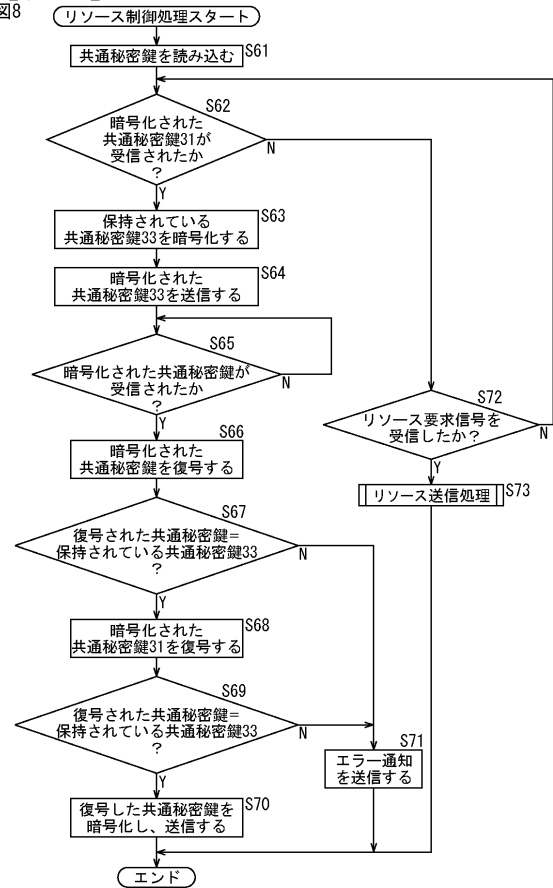
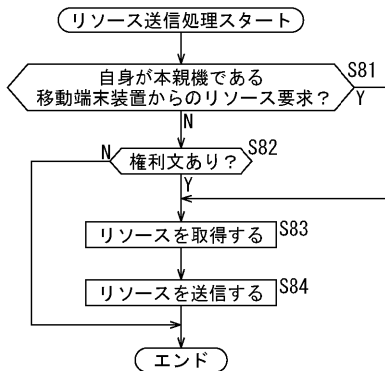
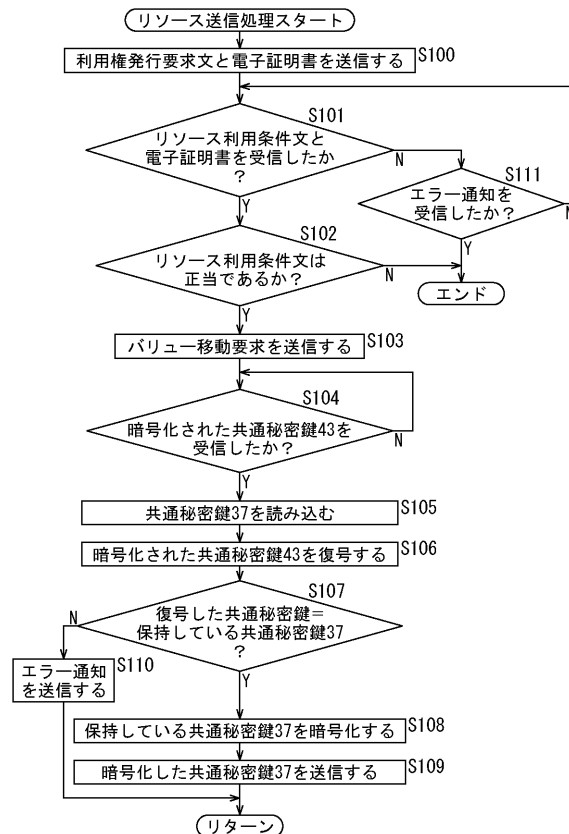
【図 1】
図1

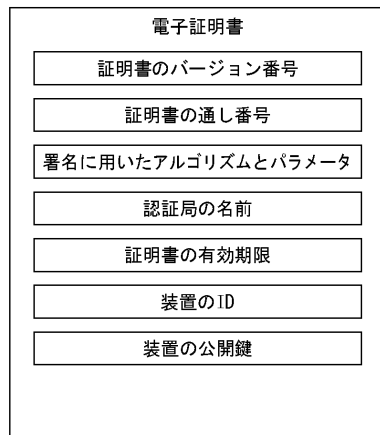
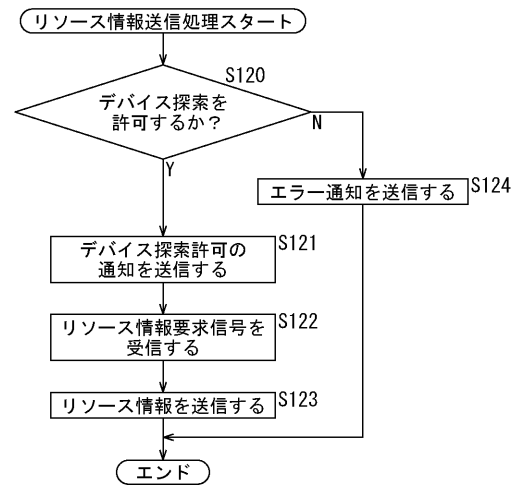
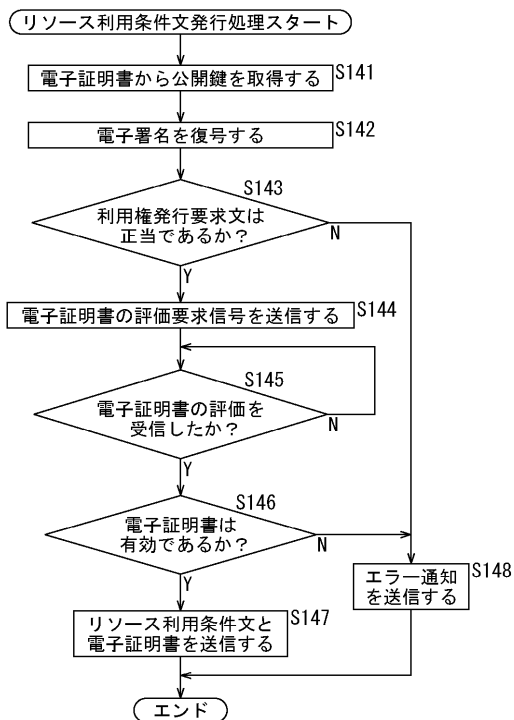
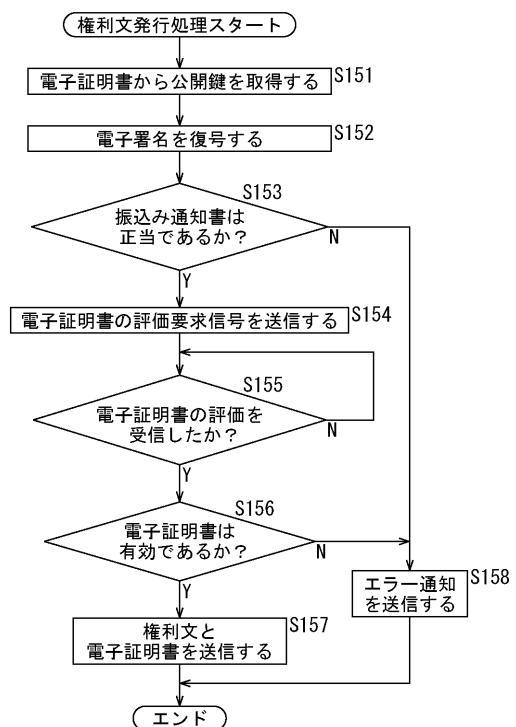


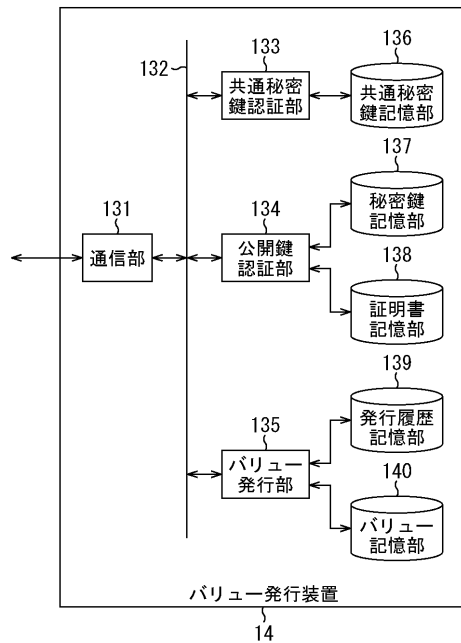
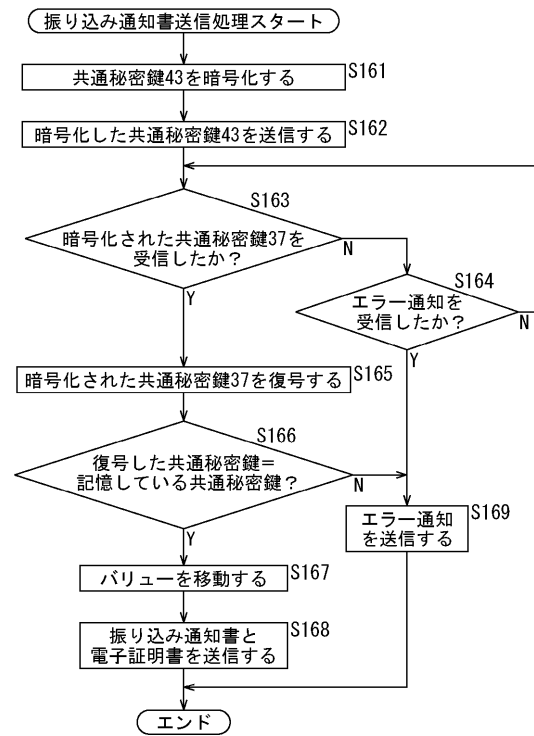
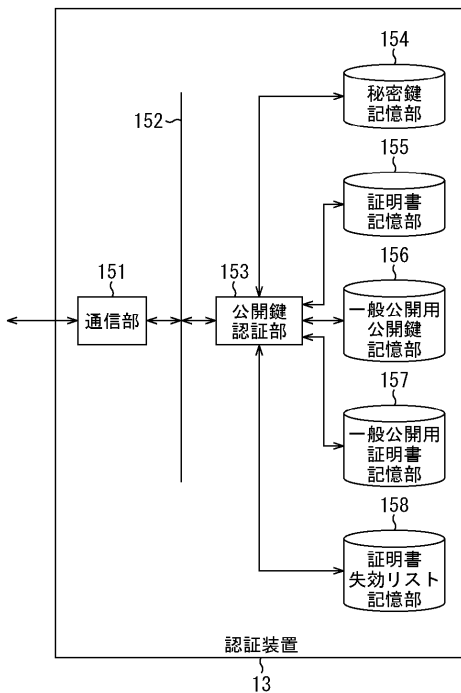
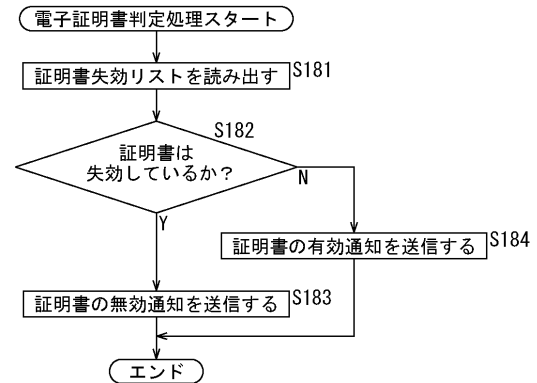
【図 2】
図2



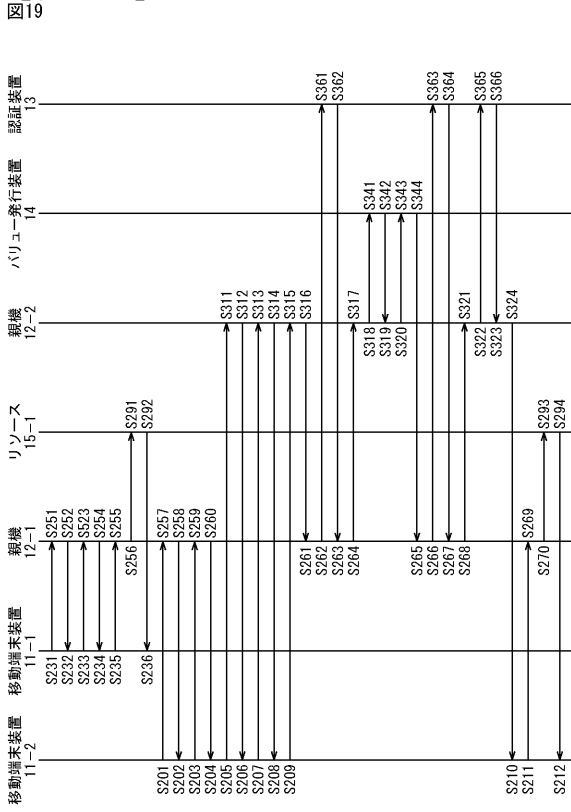
【図 3】
図3【図 4】
図4【図 5】
図5【図 6】
図6

【図 7】
図7【図 8】
図8【図 9】
図9【図 10】
図10

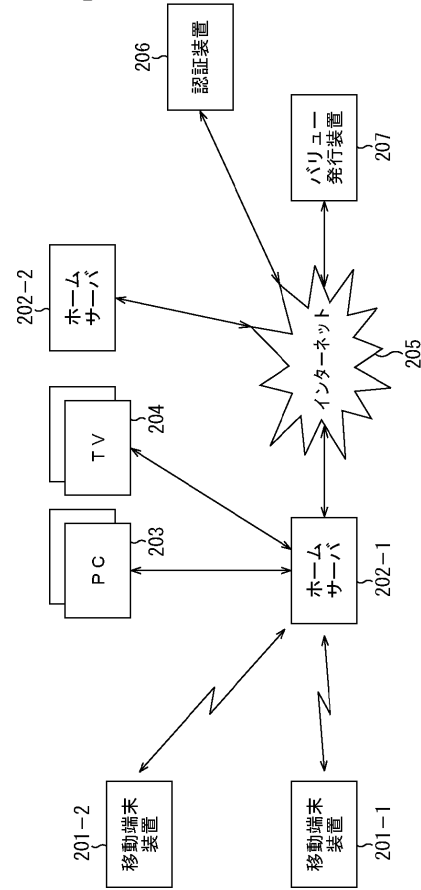
【図 1 1】
図11【図 1 2】
図12【図 1 3】
図13【図 1 4】
図14

【図 15】
図15【図 16】
図16【図 17】
図17【図 18】
図18

【図 19】



【図 20】



【図 21】

