

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2002年5月16日 (16.05.2002)

PCT

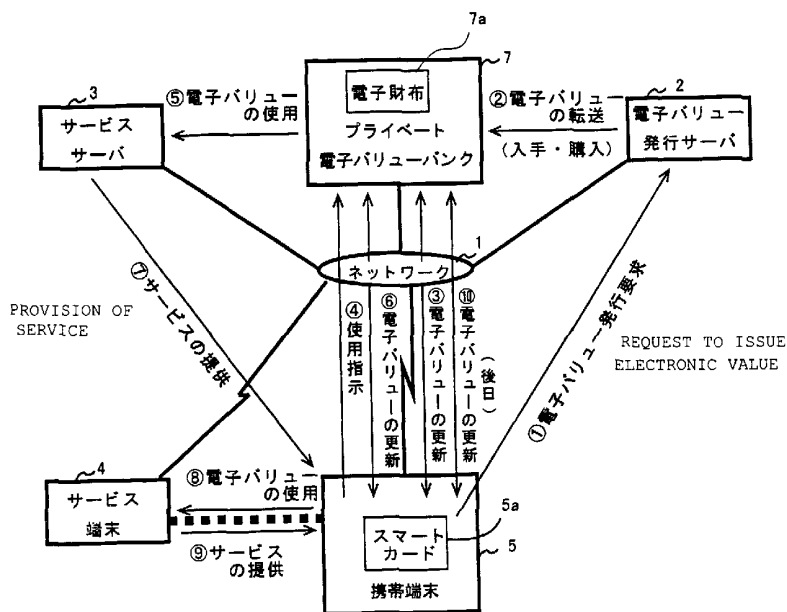
(10) 国際公開番号
WO 02/39342 A1

- (51) 国際特許分類: G06F 17/60 (72) 発明者; および
(21) 国際出願番号: PCT/JP01/09740 (75) 発明者/出願人 (米国についてのみ): 高山久 (TAKAYAMA, Hisashi) [JP/JP]; 〒156-0043 東京都世田谷区松原 5-6-12 Tokyo (JP). 川口京子 (KAWAGUCHI, Kyoko) [JP/JP]; 〒156-0057 東京都世田谷区上北沢 5-39-18 Tokyo (JP). 五十川孝夫 (ISOGAWA, Takao) [JP/JP]; 〒228-0812 神奈川県相模原市相南 2-11-20 Kanagawa (JP).
(22) 国際出願日: 2001年11月7日 (07.11.2001)
(25) 国際出願の言語: 日本語
(26) 国際公開の言語: 日本語
(30) 優先権データ: 特願2000-341062 2000年11月8日 (08.11.2000) JP (74) 代理人: 工藤一郎 (KUDO, Ichiro); 〒100-0006 東京都千代田区有楽町1丁目8-1 日比谷パークビル Tokyo (JP).
(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP). (81) 指定国 (国内): CN, JP, US.
(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB).

[続葉有]

(54) Title: PRIVATE ELECTRONIC VALUE BANK SYSTEM

(54) 発明の名称: プライベート電子バリューバンクシステム



- 3...SERVICE SERVER
(5)...USE OF ELECTRONIC VALUE
4...SERVICE TERMINAL
(8)...USE OF ELECTRONIC VALUE
(9)...PROVISION OF SERVICE
7...PRIVATE ELECTRONIC VALUE BANK
7a...ELECTRONIC WALLET
1...NETWORK
(4)...INSTRUCTION OF USE
(6)...UPDATE OF ELECTRONIC VALUE
(3)...UPDATE OF ELECTRONIC VALUE
(10)...(LATER) UPDATE OF ELECTRONIC VALUE
5...PORTABLE TERMINAL
5a...SMART CARD
(2)...TRANSFER OF ELECTRONIC VALUE (ACQUIRING/PURCHASING)
2...ELECTRONIC VALUE ISSUING SERVER

(57) Abstract: In order that an electronic value may be used while retaining safety, convenience and economy for both the service over the network and the real service the electronic value to be issued to a user is managed in an electronic wallet (7a) of a private electronic value bank (7), and the electronic value managed in the electronic wallet of the bank is cashed to a mobile electronic wallet (5b) in a smart card (5a) of a portable terminal (5) of the user. The two electronic wallet are so connected that the electronic wallet is operated through the network when the mobile electronic wallet is operated. When the electronic value in the smart card is used for a service provided in a real environment, for example, at a ticket gate of a railway station, no on-line transaction occurs upon each use, but

[続葉有]



添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

the electronic wallet of the bank is updated when the portable terminal and the bank communicate later.

(57) 要約:

ネット上のサービスとリアル上のサービスの両方に対して安全性と利便性と経済性を確保しつつ電子バリューを利用可能にするために、ユーザに発行される電子バリューはプライベート電子バリューバンク 7 の電子財布 7 a 上で管理され、ユーザの携帯端末 5 のスマートカード 5 a 上のモバイル電子財布 5 b には、バンクの電子財布上で管理されている電子バリューがキャッシュされ、モバイル電子財布が操作された場合にネットを介して電子財布が操作されるように結びつけられている。駅の改札などのリアル環境で提供されるサービスに対してスマートカード上の電子バリューを使用する場合に、使用毎にオンラインのトランザクションが発生しないで、その後携帯端末とバンクが通信したときに、バンクの電子財布がアップデートされる。

明細書

プライベート電子バリューバンクシステム

5 技術分野

本発明は、電子情報化されたチケット、マネー、プリペイドマネー、クーポン、クレジットカード、ロイヤルティポイント、会員証など、さらには電子チケットや電子マネーに限らずネットワーク上で個人の所有する各種の情報（例えば音楽、画像、映像、ソフトウェアプログラム、
10 権利など）を含む電子バリューをユーザが使用するためのプライベート電子バリューバンクシステム、携帯端末、スマートカード、電子財布及びプライベート電子バリューバンクに関する。

背景技術

15 図6は従来例として、電子バリューをユーザの携帯端末（内蔵メモリ）にダウンロードして管理するシステムを示し、このシステムはネットワーク1を介して電子バリュー発行サーバ2と、サービスサーバ3とユーザの携帯端末5が接続されて構成されている。サービスサーバ3はネットワーク1上に存在し、ユーザにより使用される電子バリューに対応してサービスを提供するサーバであり、サービス
20 端末4は実際にサービスが提供される現場にリアルに存在し、ユーザにより使用される電子バリューに対応してサービスを提供する端末であって、例えばPOS端末、自販機、自動改札機などである。

図6に示すシステムにおいて、①②は電子バリューの入手手順を示し、
25 ③④はサービスサーバ3に対する電子バリューの使用手順を示し、⑤⑥はサービス端末4に対する電子バリューの使用手順を示す。すなわち、

①携帯端末 5 が電子バリュー発行サーバ 2 に対して電子バリュー発行（購入）を要求すると、②電子バリュー発行サーバ 2 がこれを受けて携帯端末 5 に対して電子バリューを発行（ダウンロード）する。

③携帯端末 5 が電子バリューを使用してサービスサーバ 3 からサービス
5 を購入すると、

④サービスサーバ 3 がこれを受けて携帯端末 5 に対してサービスを提供する。

⑤また、携帯端末 5 が電子バリューを使用してサービス端末 4 からサービスを購入すると、

10 ⑥サービス端末 4 がこれを受けて携帯端末 5 に対してサービスを提供する。

図 7 は他の従来例として、電子バリューをサーバ上で管理するシステムを示し、このシステムはネットワーク 1 を介して電子バリュー発行サーバ 2 と、サービスサーバ 3 と、ユーザの携帯端末 5 と、電子バリュー
15 を管理する電子財布サーバ 6 が接続されて構成されている。

図 7 に示すシステムにおいて、①②は電子バリューの入手手順を示し、③④⑤はサービスサーバ 3 に対する電子バリューの使用手順を示し、⑥⑦⑧はサービス端末 4 に対する電子バリューの使用手順を示す。すなわち、

20 ①携帯端末 5 が電子バリュー発行サーバ 2 に対して電子バリュー発行を要求すると、

②電子バリュー発行サーバ 2 がこれを受けて電子財布サーバ 6 に対して電子バリューを転送する。

③携帯端末 5 がサービスサーバ 3 からサービスを購入するために、電子
25 財布サーバ 6 に対して電子バリュー使用を指示すると、

④電子財布サーバ 6 がこれを受けてサービスサーバ 3 に対して電子バリ

ユーを使用し、次いで

⑤サービスサーバ 3 がこれを受けて携帯端末 5 に対してサービスを提供する。

⑥また、携帯端末 5 がサービス端末 4 からサービスを購入するために、

5 電子財布サーバ 6 に対して電子バリュー使用を指示すると、

⑦電子財布サーバ 6 がこれを受けてサービス端末 4 に対して電子バリューを使用し、次いで

⑧サービス端末 4 がこれを受けて携帯端末 5 に対してサービスを提供する。

10 しかしながら、図 6 に示すように電子バリューをユーザの携帯端末 5 (内蔵メモリ) にダウンロードして管理するシステムでは、ユーザが携帯端末 5 自体を紛失又は破損した場合に電子バリューも失うことになるので、安全性に問題がある。

これに対し、図 7 に示すように電子バリューをサーバ (電子財布サーバ 6) 上で管理するシステムでは、上記の安全性の問題は解決することができるが、駅の改札などのリアル環境で提供されるサービスに対して電子バリューを使用する場合に、使用毎にオンラインのトランザクションが発生するので、通信コストや処理速度に問題がある。

本発明は上記従来例の問題点に鑑み、ネット上のサービスとリアル上のサービスの両方に対して、安全性と利便性と経済性を確保しつつ電子バリューを利用することができるプライベート電子バリューバンクシステム、携帯端末、スマートカード、電子財布及びプライベート電子バリューバンクを提供することを目的とする。

25 発明の開示

本発明のプライベート電子バリューバンクシステムは、上記目的を達

成するために、ユーザの要求に応じて発行された電子バリューを管理するための第 1 の電子財布を備えたプライベート電子バリューバンクと、前記第 1 の電子財布上に管理されている電子バリューの内、少なくとも一つ以上の電子バリューが管理されている第 2 の電子財布を備えた携帯
5 端末とを有し、前記第 2 の電子財布が操作された場合にネットを介して前記第 1 の電子財布が操作されるように結びつけられているように構成した。

上記構成により、ユーザの電子バリューがプライベート電子バリューバンクにより管理されているので、リアル上のサービスに対してユーザ
10 が電子バリューを使用する場合に、第 2 の電子財布上に管理されている電子バリューを使用するとともに、その後にプライベート電子バリューバンクと携帯端末が通信した際に更新して前記第 1、第 2 の電子財布上の電子バリューを関連付けることにより、ネット上のサービスとリアル上のサービスの両方に対して、安全性と利便性と経済性を確保しつつ電
15 子バリューを利用することができる。

本発明のプライベート電子バリューバンクシステムはまた、前記第 1 の電子財布上に管理されている電子バリューを操作する場合に前記第 1、第 2 の電子財布の間で相互に認証を行うことを特徴とする。

上記構成により、ユーザの携帯端末に管理されている電子バリューと
20 プライベート電子バリューバンク上に管理されている電子バリューを一致させることができ、また、不正使用を防止することができる。

本発明のプライベート電子バリューバンクシステムはまた、ネット上のサービスに対してユーザが電子バリューを使用する場合に、前記第 1 の電子財布上に管理されている電子バリューをネットを介して使用する
25 とともに、前記第 2 の電子財布上に管理されている電子バリューをネットを介して更新することを特徴とする。

上記構成により、ネット上のサービスに対して、安全性と利便性と経済性を確保しつつ電子バリューを利用することができる。

本発明のプライベート電子バリューバンクシステムはまた、リアル上のサービスに対してユーザが電子バリューを使用する場合に、前記第2
5 の電子財布上に管理されている電子バリューを使用するとともに、その後前記プライベート電子バリューバンクと携帯端末が通信した際に更新することにより、前記第1、第2の電子財布上の電子バリューを関連付けるようにしたことを特徴とする。

上記構成により、リアル上のサービスに対して、安全性と利便性と経済性を確保しつつ電子バリューを利用することができる。
10

本発明のプライベート電子バリューバンクシステムはまた、ユーザの要求に応じて電子バリューを発行して前記プライベート電子バリューバンクに転送する電子バリュー発行サーバを更に備え、前記プライベート電子バリューバンクは電子バリューを発行せず、電子バリューの管理のみを行うことを特徴とする。
15

上記構成により、電子バリュー発行サーバとプライベート電子バリューバンクが独立しているので、種々の形態のビジネスに応用することができる。

本発明のプライベート電子バリューバンクシステムはまた、電子バリューを管理する第1の電子財布を備えたプライベート電子バリューバンクと、要求に応じて電子バリューを発行する電子バリュー発行サーバと、第1の電子財布と1対1に対応する第2の電子財布を備えた携帯端末とを有し、第2の電子財布が生成する電子バリューの発行要求に対し、電子バリュー発行サーバが生成した電子バリューを第1の電子財布に送信し、第1の電子財布が電子バリュー発行サーバから電子バリューを受信し、管理するように構成した。
20
25

上記構成により、ネットを介した電子バリューの発行と電子バリューの管理における安全性を向上させることができる。

本発明のプライベート電子バリューバンクシステムはまた、ユーザが前記電子バリュー発行サーバから電子バリューを購入する際に、前記プ
5 ライベート電子バリューバンクと前記電子バリュー発行サーバとの間でその代金の支払の決済をすることを特徴とする。

上記構成により、ネットを介した電子バリューの発行とその決済における安全性を向上させることができる。

本発明のプライベート電子バリューバンクシステムはまた、ユーザが
10 前記電子バリュー発行サーバから購入するために、前記携帯端末が前記電子バリュー発行サーバに対し、発行指示情報と、前記プライベート電子バリューバンクの第1の電子財布宛に電子封書化された購入指示情報を含む電子バリュー発行要求メッセージを送信し、前記電子バリュー発行サーバが前記電子封書化された購入指示情報を取り出して前記プ
15 ライベート電子バリューバンクに送信し、前記プライベート電子バリューバンクが前記電子封書化された購入指示情報を開封して検証し、正しい場合に前記電子バリュー発行サーバとの間で電子バリューの代金の支払の決済を行うとともに、前記電子バリュー発行サーバが前記プライベート電子バリューバンクに電子バリューを発行し、前記発行された電子バ
20 リューに応じた第1の電子財布の内容に基づいて前記第2の電子財布の内容を更新することを特徴とする。

上記構成により、ネットを介した電子バリューの発行とその決済における安全性を向上させることができる。

25 図面の簡単な説明

図1は、本発明に係るプライベート電子バリューバンクシステムの一

実施形態を示すブロック図である。

図 2 は、図 1 の電子財布とモバイル電子財布の構成及び対応関係の一例を示す説明図である。

図 3 は、図 1 の電子バリュー購入手順を詳しく示す説明図である。

5 図 4 は、電子バリュー発行要求メッセージのデータ構造を示す説明図である。

図 5 は、電子バリュー購入処理のタイミングを説明するための図である。

図 6 は、従来のプライベート電子バリューバンクシステムを示すブロック図である。
10

図 7 は、他の従来のプライベート電子バリューバンクシステムを示すブロック図である。

図 8 は、実施の形態 2 におけるプライベート電子バリューバンクの構成を示す図である。

15 図 9 は、実施の形態 2 における電子バリュー発行サーバの機能ブロック図である。

図 10 は、実施の形態 2 における電子バリュー発行サーバの動作を説明するフローチャートである。

図 11 は、実施の形態 2 におけるプライベート電子バリューバンクの機能ブロック図である。
20

図 12 は、バンク共有管理部で管理される表の一例を示す図である。

図 13 は、実施の形態 2 におけるプライベート電子バリューバンクの動作を説明するフローチャートである。

図 14 は、実施の形態 2 における携帯端末の機能ブロック図である。

25 図 15 は、端末共有管理部で管理される表の一例を示す図である。

図 16 は、実施の形態 2 における携帯端末の動作を説明する図である。

図 1 7 は、実施の形態 2 における電子バリュー発行サーバと、プライベート電子バリューバンクと、携帯端末の相互作用を説明するシーケンス図である。

図 1 8 は、バンク共有管理部がバンク共有管理部プライベート鍵と端末共有管理部証明書を有している状態を示す図である。

図 1 9 は、バンク共有管理部がバンク共有管理部プライベート鍵とバンク共有管理部証明書を有している状態を示す図である。

図 2 0 は、端末共有管理部が端末共有管理部プライベート鍵とバンク共有管理部証明書を有している状態を示す図である。

10 図 2 1 は、端末共有管理部が端末共有管理部プライベート鍵と端末共有管理部証明書を有している状態を示す図である。

図 2 2 は、実施の形態 3 におけるプライベート電子バリューバンクシステムの構成を示す図である。

図 2 3 は、実施の形態 3 における電子バリュー発行サーバの機能ブロック図である。

図 2 4 は、実施の形態 3 における電子バリュー発行サーバの動作を説明するフローチャートである。

図 2 5 は、実施の形態 3 におけるプライベート電子バリューバンクの機能ブロック図である。

20 図 2 6 は、実施の形態 3 におけるプライベート電子バリューバンクの動作を説明するフローチャートである。

図 2 7 は、実施の形態 3 における携帯端末の機能ブロック図である。

図 2 8 は、実施の形態 3 における携帯端末の動作を説明するフローチャートである。

25 図 2 9 は、実施の形態 3 における電子バリュー発行サーバと、プライベート電子バリューバンクと、携帯端末との相互作用を説明するシーケ

ンス図である。

図 3 0 は、実施の形態 4 におけるプライベート電子バリューバンクシステムの構成を示す図である。

図 3 1 は、実施の形態 4 におけるプライベート電子バリューバンクの
5 機能ブロック図である。

図 3 2 は、実施の形態 4 における携帯端末の機能ブロック図である。

図 3 3 は、実施の形態 4 における携帯端末の動作を説明するフローチャートである。

図 3 4 は、実施の形態 4 におけるサービスサーバの機能ブロック図で
10 ある。

図 3 5 は、実施の形態 4 におけるサービスサーバと、プライベート電子バリューバンクと、携帯端末との相互作用を説明するシーケンス図である。

図 3 6 は、実施の形態 5 におけるプライベート電子バリューバンクシ
15 ステムの構成を示す図である。

図 3 7 は、実施の形態 5 におけるプライベート電子バリューバンクの機能ブロック図である。

図 3 8 は、実施の形態 5 におけるプライベート電子バリューバンクの動作を説明するフローチャートである。

20 図 3 9 は、実施の形態 5 における携帯端末の機能ブロック図である。

図 4 0 は、実施の形態 5 における携帯端末の動作を説明するフローチャートである。

図 4 1 は、実施の形態 5 におけるサービスサーバの機能ブロック図である。

25 図 4 2 は、実施の形態 5 におけるサービスサーバと、プライベート電子バリューバンクと、携帯端末との相互作用を示すシーケンス図である。

図 4 3 は、実施の形態 6 におけるプライベート電子バリューバンクシステムの構成を示す図である。

図 4 4 は、実施の形態 6 における電子バリュー発行サーバの機能ブロック図である。

5 図 4 5 は、実施の形態 6 におけるプライベート電子バリューバンクの機能ブロック図である。

図 4 6 は、実施の形態 6 におけるプライベート電子バリューバンクの動作を説明するフローチャートである。

図 4 7 は、電子バリュー発行サーバと、プライベート電子バリューバ
10 ンクと、携帯端末との相互作用を示すシーケンス図である。

図 4 8 は、実施の形態 7 におけるプライベート電子バリューバンクの機能ブロック図である。

図 4 9 は、実施の形態 7 におけるプライベート電子バリューバンクの動作を説明するフローチャートである。

15 図 5 0 は、実施の形態 7 における携帯端末の機能ブロック図である。

図 5 1 は、実施の形態 7 における携帯端末の動作を説明するフローチャートである。

図 5 2 は、実施の形態 7 における電子バリュー発行サーバと、プライベート電子バリューバンクと、携帯端末との相互作用を示すシーケンス
20 図である。

図 5 3 は、プライベート電子バリューバンクで保持される電子バリューの識別子に携帯端末で保持される電子バリューの識別子を含む状態を示す図である。

図 5 4 は、実施の形態 8 におけるプライベート電子バリューバンクシ
25 ステムの構成を示す図である。

図 5 5 は、実施の形態 8 における電子バリュー発行サーバの機能プロ

ック図である。

図 5 6 は、実施の形態 8 における電子バリュー発行サーバの動作を説明するフローチャートである。

図 5 7 は、実施の形態 8 におけるプライベート電子バリューバンクの
5 機能ブロック図である。

図 5 8 は、実施の形態 8 におけるプライベート電子バリューバンクの動作を説明するフローチャートである。

図 5 9 は、実施の形態 8 における携帯端末の機能ブロック図である。

図 6 0 は、実施の形態 8 における携帯端末の動作を説明するフローチャートである。
10

図 6 1 は、実施の形態 8 における電子バリュー発行サーバと、プライベート電子バリューバンクと、携帯端末との相互作用を示すシーケンス図である。

図 6 2 は、実施の形態 9 におけるプライベート電子バリューバンクシステム
15 の構成を示す図である。

図 6 3 は、実施の形態 9 における電子バリュー発行サーバの機能ブロック図である。

図 6 4 は、実施の形態 9 における電子バリュー発行サーバの動作を説明するフローチャートである。

図 6 5 は、実施の形態 9 におけるプライベート電子バリューバンクの
20 機能ブロック図である。

図 6 6 は、実施の形態 9 におけるプライベート電子バリューバンクの動作を説明するフローチャートである。

図 6 7 は、実施の形態 1 0 におけるプライベート電子バリューバンク
25 システムの構成を示す図である。

図 6 8 は、実施の形態 1 0 におけるプライベート電子バリューバンク

の機能ブロック図である。

図 6 9 は、実施の形態 1 0 におけるプライベート電子バリューバンクの動作を説明するフローチャートである。

図 7 0 は、実施の形態 1 0 における携帯端末の機能ブロック図である。

5 図 7 1 は、実施の形態 1 0 における携帯端末とプライベート電子バリューバンクの相互作用を示すシーケンス図である。

図 7 2 は、実施の形態 8 における電子バリュー発行要求の構造を示す図である。

図 7 3 は、実施の形態 9 における電子バリュー発行サーバと、プライベート電子バリューバンクと、携帯端末との相互作用を示すシーケンス
10 図である。

図 7 4 は、実施の形態 8 におけるデータの移動を模式的に表した図である。

図 7 5 は、実施の形態 8 におけるデータの移動を模式的に表した図で
15 ある。

図 7 6 は、実施の形態 8 におけるデータの移動を模式的に表した図である。

図 7 7 は、実施の形態 8 におけるデータの移動を模式的に表した図である。

20 図 7 8 は、実施の形態 8 におけるデータの移動を模式的に表した図である。

図 7 9 は、実施の形態 9 におけるデータの移動を模式的に表した図である。

図 8 0 は、実施の形態 9 におけるデータの移動を模式的に表した図で
25 ある。

図 8 1 は、実施の形態 9 におけるデータの移動を模式的に表した図で

ある。

図 8 2 は、実施の形態 9 におけるデータの移動を模式的に表した図である。

図 8 3 は、実施の形態 9 におけるデータの移動を模式的に表した図である。

図 8 4 は、実施の形態 9 におけるデータの移動を模式的に表した図である。

図 8 5 は、実施の形態 9 における携帯端末の機能ブロック図である。

図 8 6 は、実施の形態 9 における携帯端末の動作を説明するフローチャートである。

発明を実施するための最良の形態

(実施の形態 1)

以下、図面を参照して本発明の実施の形態について説明する。図 1 は本発明に係るプライベート電子バリューバンクシステムの一実施形態を示すブロック図、図 2 は図 1 の電子財布とモバイル電子財布の構成及び対応関係の一例を示す説明図、図 3 は図 1 の電子バリュー購入手順を詳しく示す説明図、図 4 は電子バリュー発行要求メッセージのデータ構造を示す説明図、図 5 は電子バリュー購入処理のタイミングを説明するための図である。

図 1 に示すシステムは、ネットワーク 1 を介して電子バリュー発行サーバ 2 と、サービスサーバ 3 と、ユーザの携帯端末 5 と、プライベート電子バリューバンク（以下、単にバンクともいう）7 が接続されて構成されている。携帯端末 5 は、通信機能として、携帯電話などの公衆無線通信手段と、ブルートゥースや赤外線などのローカル無線通信手段を備え、この公衆無線通信手段を用いて電子バリュー発行サーバ 2、サービ

サーバ 3、及び、バンク 7 と通信し、ローカル無線通信手段を用いてサービス端末 4 と通信する。

バンク 7 は、ユーザ（顧客）が所有する電子バリューを管理する電子財布 7 a（アプリケーション）を有し、電子財布はユーザ毎に存在する。

- 5 一方、携帯端末 5 は、メモリ及び CPU などの処理系を有する着脱自在なスマートカード（(USIM: Universal Subscriber Identity Module) などのスマートカードモジュールであつてもよい）5 a を有し、スマートカード 5 a には、アプリケーションとしてモバイル電子財布 5 b（図 2）が搭載されている。このモバイル電子財布 5 b は、バンク 7 上の電子財
- 10 布の内の一つの電子財布 7 a と 1 対 1 に対応し、モバイル電子財布 5 b には、電子財布 7 a 上で管理されている電子バリューがキャッシュされている。このモバイル電子財布 5 b が搭載されたスマートカード 5 a は、モバイル電子財布 5 b がキャッシュしている電子バリューの所有者、つまり、バンク 7 のユーザ（顧客）が所有し、携帯端末 5 に装着して使用する。モバイル電子財布 5 b には、個人認証情報（例えば、PIN (Personal Identity Number)）が管理されており（図 2 には未記載）、モバイル電子
- 15 財布 5 b は、ユーザがモバイル電子財布 5 b を操作する際、この個人認証情報を用いてユーザを認証する（例えば、ユーザが入力する PIN を照合する）。

- 20 バンク 7 側の電子財布 7 a には、電子バリューの一種として電子的なクレジットカード又はデビットカードが管理されており、このカード情報が電子バリュー発行サーバ 2 から電子バリューを購入する際の代金を決済するために用いられる。また、携帯端末 5 側のモバイル電子財布 5 b には、対応するバンク 7 側の電子財布 7 a のデジタル証明書である電
- 25 子財布証明書 7 2 と、モバイル電子財布 5 b 固有のプライベート鍵とそのデジタル証明書であるモバイル電子財布プライベート鍵 5 1 とモバイ

ル電子財布証明書 5 2 とが管理されており、一方、モバイル電子財布 5 b に対応するバンク 7 側の電子財布 7 a には、モバイル電子財布 5 b のデジタル証明書であるモバイル電子財布証明書 5 2 と、電子財布 7 a 固有のプライベート鍵とそのデジタル証明書である電子財布プライベート
5 鍵 7 1 と電子財布証明書 7 2 とが管理されている。携帯端末 5 側のモバイル電子財布 5 b とバンク 7 側の電子財布 7 a とが通信をする際には、これらのプライベート鍵や証明書を用いて、両者間で相互認証を行い、セッション鍵を交換して、常に、セキュアセッションが確立される。

ユーザは、スマートカード 5 a を装着した携帯端末 5 を用いて、モバ
10 イル電子財布 5 b にキャッシュされている電子バリュー、及び、バンク 7 側の電子財布 7 a で管理されている電子バリューを操作することができる。その際には、常に、ユーザが所有する携帯端末側のモバイル電子財布 5 b による認証が必要となる。本システムでは、電子バリューを電子バリュー発行サーバ 2 から入手・購入する場合には、まず、モバイル
15 電子財布 5 b が電子バリューの発行要求を生成して、電子バリュー発行サーバ 2 へ送信し、電子バリューの発行要求に基づいて電子バリュー発行サーバ 2 が発行した電子バリューは、バンク 7 の電子財布 7 a に送信され、次に、電子財布 7 a から携帯端末 5 のモバイル電子財布 5 b にキャッシュされる。つまり、発行された電子バリューは、全てバンク 7 の
20 電子財布 7 a で管理され、その内、使用される確率の高い電子バリューがモバイル電子財布 5 b でも管理される。

また、電子バリューをサービスサーバ 3 が提供するサービス（オンラインショッピング、オンラインライブ中継など）に使用する場合には、まず、モバイル電子財布 5 b が電子バリューの使用指示を生成し、バン
25 ク 7 側の電子財布 7 a へ送信し、電子財布 7 a が管理している電子バリューをサービスサーバ 3 に対して使用して、サービスサーバ 3 からサー

ビスが提供される。この時、モバイル電子財布 5 b にキャッシュされている電子バリューも更新される。

また、電子バリューをサービス端末 4 が提供するサービス（POS 端末に対する代金の支払、チケットの自動改札など）に使用する場合には、

5 モバイル電子財布 5 b がキャッシュしている電子バリューをサービス端末 4 に対して使用して、サービス端末 4 からサービスが提供される。モバイル電子財布 5 b がキャッシュしている電子バリューを使用するので、電子バリューの使用の処理を高速に行うことが出来る。電子財布 7 a で管理されている電子バリューの更新は、その後、電子財布 7 a とモバイル

10 ル電子財布 5 b とが通信をした際に行われる。したがって、オンラインのトランザクションが、電子バリューを使用する度に発生するということはない。ただし、使用する電子バリューがモバイル電子財布 5 b にキャッシュされていなかった場合には、電子財布 7 a と通信して、使用する電子バリューをキャッシュしてから使用する。

15 また、バンク 7 には、サービスサーバ 3 及びサービス端末 4 から電子バリューの使用履歴情報が定期的に送信される。バンク 7 の電子財布 7 a は、管理している電子バリューとその使用履歴情報との整合性を検証する。

また、ユーザが所有する電子バリューは、全てバンク 7 の電子財布 7

20 a で管理されているので、ユーザが、モバイル電子財布 5 b が搭載されたスマートカード 5 a を、紛失又は破損した場合には、バンク 7 は、厳密なユーザ認証した上で、電子財布 7 a で管理されている電子バリューと、電子バリューの使用履歴情報とに基づいて電子バリューを復元する。

図 2 は電子財布 7 a とモバイル電子財布 5 b の構成及び対応関係の一例を示している。プライベート電子バリューバンク 7 上の電子財布 7 a

25 には、ユーザが所有する複数の電子バリュー A ~ F が管理される。電子

財布 7 a と 1 対 1 に対応するモバイル電子財布 5 b には、電子財布 7 a
で管理されている電子バリュー A ~ F の内、一部の電子バリュー A ~ C
(電子バリューのキャッシュ) が管理される (モバイル電子財布 5 b 側
の容量に余裕がある場合には、電子財布 7 a で管理されている電子バ
5 ユー A ~ F の全てが管理されていてもよい)。電子バリュー A ~ F の各々
は、実際の電子バリューデータと、そのデータを特定する識別情報 (電
子バリュー識別情報: 例えば電子バリューの URL 又は URI) を含む。
そして、図 2 において、モバイル電子財布 5 b にキャッシュされていな
い、例えば電子バリュー D を電子財布 7 a からモバイル電子財布 5 b に
10 キャッシュする場合、電子財布 7 a とモバイル電子財布 5 b の間で上記
の相互認証を行った後、上記の電子バリュー認識情報により電子バリュー
D を特定する。

図 1 において、① ~ ③ は電子バリュー発行サーバ 2 からの電子バリュー
の入手手順を示し、④ ~ ⑦ はサービスサーバ 3 に対する電子バリュー
15 の使用手順を示し、⑧ ~ ⑩ はサービス端末 4 に対する電子バリューの使用
手順を示す。すなわち、① 携帯端末 5 が電子バリュー発行サーバ 2 に
対して電子バリュー発行を要求すると、

② 電子バリュー発行サーバ 2 がこれを受けてバンク 7 に対して電子バリュー
を転送し、次いで

20 ③ バンク 7 と携帯端末 5 が交信してそれぞれ電子財布 7 a 上、モバイル
電子財布 5 b 上の電子バリューを更新する。

④ 携帯端末 5 がサービスサーバ 3 からサービスを購入するために、バンク
7 に対して電子バリュー使用を指示すると、

⑤ バンク 7 がこれを受けてサービスサーバ 3 に対して電子バリューを使
25 用し、また、

⑥ バンク 7 と携帯端末 5 が交信してそれぞれ電子財布 7 a 上、モバイル

電子財布 5 b 上の電子バリューを更新し、また

⑦サービスサーバ 3 が携帯端末 5 に対してサービスを提供する。

⑧また、携帯端末 5 がサービス端末 4 からサービスを購入するために、サービス端末 4 に対して電子バリューを使用すると、

5 ⑨サービス端末 4 がこれを受けて携帯端末 5 に対してサービスを提供する。

⑩そして、その後、バンク 7 と携帯端末 5 とが通信した際に、それぞれ電子財布 7 a 上、モバイル電子財布 5 b 上の電子バリューを更新する。

図 3 は上記の①～③における電子バリューの入手手順（購入手順）を
10 詳しく示す。図 4 は図 3 ①において携帯端末 5 から電子バリュー発行サーバ 2 に送られる電子バリュー発行要求メッセージのデータ構造を示し、このメッセージは発行指示情報と購入指示情報を含む。発行指示情報は、電子バリュー発行サーバ 2 に対して、電子バリューの代金の決済処理を
15 バンク 7 側の電子財布 7 a との間で行い、電子バリューをバンク 7 側の電子財布 7 a に発行するように指示する情報であり、詳しくは以下のよう
な情報が含まれる。

- ・発行する電子バリュー
- ・代金の決済方法、決済金額
- ・代金の決済処理を行う電子財布の URL 又は URI
- 20 ・電子バリューを配送する電子財布の URL 又は URI
- ・セッション番号

ただし、通常、代金の決済処理を行う電子財布と電子バリューを配送する電子財布の URL 又は URI は同じである。なお、異なる場合を書いてよい。

25 購入指示情報は、バンク 7 側の電子財布 7 a に対して、電子バリューの購入処理（代金の決済と電子バリューの入手）を指示する情報であり、

さらに、モバイル電子財布 5 b によってユーザの電子署名がされ、さらに、バンク 7 側の電子財布 7 a 宛てに電子封書化されている。電子バリュー発行サーバ 2 は、購入指示情報をバンク 7 側の電子財布 7 a に送信し、バンク 7 側の電子財布 7 a は、受信した購入指示情報に基づいて電子バリュー発行サーバとの間で電子バリューの購入処理（代金の決済と電子バリューの入手）を行う。

すなわち、電子バリュー発行サーバ 2 にとって、購入指示情報の内容はわからない。購入指示情報には、以下のような情報が含まれる。

- ・購入する電子バリュー
- 10 ・代金の決済方法、決済金額
- ・電子バリュー発行サーバ（マーチャント）の URL 又は URL
- ・セッション番号

そして、電子バリュー発行サーバ 2 は発行指示情報に、プライベート電子バリューバンク 7 の電子財布は購入指示情報にそれぞれ基づいて、両者間で、電子バリューの代金の決済との配送を行う。このため、携帯端末 5 側に、代金の決済処理のための各種のプログラムを搭載する必要がなくなる。また、電子バリューが購入と同時に電子バリュー発行サーバ 2 側で管理され、紛失の恐れがない。

図 3 に示す購入手順を以下に詳しく示す。

- 20 ①携帯端末 5 が電子バリュー発行要求を生成し、電子バリュー発行サーバ 2 に送信する。モバイル電子財布 5 b が購入指示情報に電子署名、及び、電子財布 7 a 宛てに電子封書化する。
- ②電子バリュー発行サーバ 2 は、受信した電子バリュー発行要求の中の発行指示情報を解釈し、発行指示情報に基づいて、指定されたプライベート電子バリューバンク 7 の電子財布 7 a に購入指示情報を送信する。
- 25 ③プライベート電子バリューバンク 7 の電子財布 7 a は、受信した購入

指示情報の封書を開封し、署名を検証する。署名が正しい場合、購入指示情報にも基づいて電子バリュー発行サーバ2との間で電子バリューの代金の決済処理を行う。

④電子バリュー発行サーバ2は電子バリューを生成し、プライベート電子バリューバンク7の電子財布7aに送信する。

⑤プライベート電子バリューバンク7の電子財布7aとモバイル電子財布5bはセッション鍵を交換してセキュアセッションを確立する。

⑥プライベート電子バリューバンク7の電子財布7aの内容に基づいてモバイル電子財布5bの内容を更新する。

10 すなわち、購入指示情報が、マーチャント（電子バリュー発行サーバ2）経由でモバイル電子財布5bに結び付けられたネット上の電子財布7aに送信され、代金の決済処理と商品（電子バリュー）の配送が、マーチャント2とネット上の電子財布7aとの間で行われる。

次に図5を参照して電子バリューの購入処理のタイミングについて説明する。図5における①電子バリュー発行要求、②電子バリューの転送、③電子バリューの更新の処理のタイミングは、

- ・ 電子バリュー発行要求の内容
- ・ 電子バリューの内容
- ・ 電子財布の設定

20 などによって決まる。

- ・ 電子バリュー発行要求の内容によって決まる場合

発行指示情報、購入指示情報の中で、②③の処理のタイミングが直接的又は間接的に規定される場合であり、例えば、ユーザは、電子バリューをモバイル電子財布5bにダウンロードする時期を指定できる。

25 ・ 電子バリューの内容によって決まる場合

電子バリューに含まれる情報として、③の処理のタイミングが規定さ

れる場合であり、例えば、電子バリューの発行者は、電子バリューがモバイル電子財布 5 b で管理されている期間を限定できる。

・電子財布の設定によって決まる場合

電子財布の設定によって、③の処理のタイミングを制御する場合であり、例えば、ユーザは、あらかじめ電子バリューの種類に応じて電子バリューをモバイル電子財布 5 b にダウンロードする時期を指定できる（電子プリペイドマネーは、すぐダウンロードするが、日時が先の電子チケットの場合には、公演が近くなった時にダウンロードするなど）。

このプライベート電子バリューバンクシステムの実際の運用形態としては、次のような形態を想定している。ユーザは、プライベート電子バリューバンク 7 の顧客であり、プライベート電子バリューバンク 7 は、銀行やその他の金融機関、又は、通信事業会社、その他の第三者機関、又は、それらの共同出資会社として運営され、モバイル電子財布 5 b のアプリケーションを搭載したスマートカード 5 a は、プライベート電子バリューバンク 7 からユーザに発行される。ユーザは、発行されたスマートカード 5 a を携帯端末 5 に装着することにより、プライベート電子バリューバンク 7 から、安全性の高い電子バリューの購入と管理、電子バリューのネットサービス及びリアルサービスへの利用を可能にするサービスが提供される。プライベート電子バリューバンク 7 は、電子バリュー発行サーバ 2 を運用するイベント会社、チケット発行会社、小売販売会社又はプリペイドカード発行会社などの事業者に対し、ユーザが電子バリューを安全に購入・使用するプラットフォームを提供することにより、これらの事業者から手数料を得ることが出来る。また、プライベート電子バリューバンク 7 は、サービスサーバ 3、サービス端末 4 を運用する事業者に対して、顧客への電子バリューを利用したサービス提供の機会を提供することにより、事業者から手数料を得ることが出来る。

また、プライベート電子バリューバンク 7 は、電子財布 7 a に基づく、ポータルサービスをユーザに提供することが出来、ポータルサイトに掲載する広告による収益を得ることが出来る。また、ユーザの電子バリューの利用を、匿名化して統計をとることにより、この統計情報をマーケティング情報として他の事業者の販売することも可能である。プライベート電子バリューバンク 7 は、ユーザが所有する価値情報を集中して管理することが出来るので、ユーザ（顧客）が関連する各種の情報サービスの一つのノードとして利用することが出来る。具体的には、例えば、銀行の場合には、顧客の囲い込み、顧客への付加価値サービスに利用することが出来る。

なお、プライベート電子バリューバンク 7、電子バリュー発行サーバ 2、サービスサーバ 3、サービス端末 4 を運用する事業者は、それぞれ、異なる事業者である必要はなく、各種の組み合わせで、同一の事業者であってもよい。

15 （実施の形態 2）

図 8 は、本発明の実施の形態 2 にかかわるプライベート電子バリューバンクシステムの構成を示す図である。本実施の形態において、プライベート電子バリューバンクシステムは、電子バリュー発行サーバ 8 0 1 と、プライベート電子バリューバンク 8 0 2 と、携帯端末 8 0 3 とを備える。本実施の形態において、携帯端末 8 0 3 から電子バリュー発行サーバ 8 0 1 へ電子バリュー発行要求が出力され（矢印 8 0 4）、電子バリュー発行サーバ 8 0 1 よりプライベート電子バリューバンク 8 0 2 へ電子バリューが転送され（矢印 8 0 5）、プライベート電子バリューバンク 8 0 2 から携帯端末 8 0 3 へ電子バリューが送信され（矢印 8 0 6）、プライベート電子バリューバンク 8 0 2 と携帯端末 8 0 3 とで電子バリューが共有される（矢印 8 0 7）。

図 9 は、電子バリュー発行サーバ 8 0 1 の機能ブロック図を例示する。電子バリュー発行サーバ 8 0 1 は、電子バリュー発行要求受付部 9 0 1 と電子バリュー転送部 9 0 2 とを有する。また、電子バリュー生成部（図示せず）も有する。

- 5 電子バリュー発行要求受付部 9 0 1 は、携帯端末 8 0 3 から電子バリュー発行要求を受け付ける。「電子バリュー発行要求」とは、電子バリュー発行サーバ 8 0 1 に対する電子バリューの発行の要求であり、電子バリューの種類、電子バリューの量、電子バリューの発行のための決済処理に必用となる情報を含む。
- 10 電子バリュー生成部は、電子バリュー発行要求受付部 9 0 1 で受け付けた電子バリュー発行要求に応じて、すでに存在する電子バリューをコピーすることや、新しく電子バリューを作り出すことにより、電子バリューを生成することを行なう。

- 電子バリュー転送部 9 0 2 は、電子バリュー発行要求受付部 9 0 1 で
- 15 受け付けた電子バリュー発行要求に応じて、プライベート電子バリューバンク 8 0 2 に電子バリューを転送する。「電子バリュー発行要求に応じて」とは、電子バリュー発行要求により指定された通りに電子バリュー生成部で電子バリューが生成されるということを意味する。電子バリュー転送部 9 0 2 は、電子バリュー発行要求受付部 9 0 1 で受け付けた
- 20 電子バリュー発行要求で指定され、電子バリュー生成部により生成された、電子バリュープライベート電子バリューバンク 8 0 2 へ転送することになる。また、電子バリューの転送の前に決済のための処理が終了していることを確認してから電子バリューを転送するようにしてもよい。

- 図 1 0 は、電子バリュー発行サーバ 8 0 1 の動作を説明するフローチャートである。まず、携帯端末 8 0 3 から電子バリュー発行要求を、電子バリュー発行要求受付部 9 0 1 により受け付ける（ステップ S 1 0 0
- 25

1)。次に、電子バリュー発行要求に応じて、電子バリュー生成部が電子バリューを生成し、電子バリュー転送部 902 によりプライベート電子バリューバンク 802 へ電子バリューを転送する(ステップ S1002)。

図 11 は、プライベート電子バリューバンク 802 の機能ブロック図を例示する。プライベート電子バリューバンク 802 は、転送電子バリュー受取部 1101 と、バンク電子バリュー保持部 1102 と、電子バリュー送信部 1103 と、バンク共有管理部 1104 とを有する。

転送電子バリュー受取部 1101 は、電子バリュー発行サーバ 801 から転送される電子バリューを受取る。

10 バンク電子バリュー保持部 1102 は、電子バリューを保持する。

電子バリュー送信部 1103 は、バンク電子バリュー保持部 1102 の電子バリューを携帯端末 803 に送信する。「バンク電子バリュー保持部 1102 の電子バリュー」とは、バンク電子バリュー保持部 1102 で保持されている電子バリューである。電子バリュー送信部 1103
15 は、バンク電子バリュー保持部 1102 に保持されている全ての電子バリューを送信してもよいし、一部の電子バリューを送信するようにしてもよい。

バンク共有管理部 1104 は、バンク電子バリュー保持部 1102 で保持されている電子バリューと携帯端末 803 で保持されている電子バリューを共有されるように管理する。「携帯端末 803 で保持されている電子バリュー」とは、後述の携帯端末 803 の電子バリュー保持部で保持されている電子バリューであり、「共有」とは、バンク共有管理部 1104 で保持されている電子バリューと携帯端末 803 で保持されている電子バリューとの間に共通部分があるということである。特に、携帯
20 端末 803 で保持されている電子バリューがバンク電子バリュー保持部 1102 で保持されている電子バリューの一部となるようになっていて

もよい。「共有されるように管理する」とは、バンク電子バリュー保持部
1 1 0 2 で保持される電子バリューのうち、どれが携帯端末 8 0 3 によ
っても保持されているかを図 1 2 に例示する表 1 2 0 0 で判別できるよ
うにしたり（表 1 2 0 0 の各行が電子バリュー毎に共有されているかど
5 うかを示している。各行の列 1 2 0 1 に示された電子バリューが携帯端
末 8 0 3 とで共有される場合には、列 1 2 0 2 の値が「共有」になり、
共有されない場合は列 1 2 0 2 の値が「非共有」となる）、バンク電子バ
リュー保持部 1 1 0 2 と携帯端末 8 0 3 との両方で保持されている電子
バリューがプライベート電子バリューバンク 8 0 2 により使われた場合
10 には、携帯端末 8 0 3 で保持されている電子バリューを削除（または、
電子バリューのステイタスを「使用済み」に変更）したり、あるいは、
反対に、携帯端末 8 0 3 により電子バリューが使用された場合には、バ
ンク電子バリュー保持部 1 1 0 2 で保持されている電子バリューを削除
（または、電子バリューのステイタスを「使用済み」に変更）したりす
15 ることである。

図 1 3 は、プライベート電子バリューバンク 8 0 2 の動作を説明する
フローチャートである。まず、電子バリュー発行サーバ 8 0 1 から転送
される電子バリューを、転送電子バリュー受取部 1 1 0 1 にて受け取る
（ステップ S 1 3 0 1）。受け取られた電子バリューを、バンク電子バリ
20 ュー保持部 1 1 0 2 にて保持する（ステップ S 1 3 0 2）。バンク電子バ
リュー保持部 1 1 0 2 によって保持された電子バリューのうち一部また
は全部を携帯端末に、電子バリュー送信部 1 1 0 3 により送信する（ス
テップ S 1 3 0 3）。そして、バンク共有管理部 1 1 0 4 により、電子バ
リューが共有されるように管理する（ステップ S 1 3 0 4）。例えば、図
25 1 2 に示す表 1 2 0 0 に、どの電子バリューが共有され、どの電子バリ
ューが共有されていないかを記録する。

図 1 4 は、携帯端末 8 0 3 の機能ブロック図を例示する。携帯端末は、電子バリュー発行要求出力部 1 4 0 1 と、電子バリュー受信部 1 4 0 2 と、電子バリュー保持部 1 4 0 3 と、端末共有管理部 1 4 0 4 とを有する。

- 5 電子バリュー発行要求出力部 1 4 0 1 は、電子バリュー発行サーバ 8 0 1 に対して電子バリュー発行要求を出力する。

電子バリュー受信部 1 4 0 2 は、プライベート電子バリューバンク 8 0 2 から送信される電子バリューを受信する。

電子バリュー保持部 1 4 0 3 は、電子バリューを保持する。

- 10 端末共有管理部 1 4 0 4 は、バンク電子バリュー保持部 1 1 0 2 で保持されている電子バリューと、携帯端末 8 0 3 で保持されている電子バリューとが共有されるように管理する。「携帯端末 8 0 3 で保持されている電子バリュー」とは、電子バリュー保持部 1 4 0 3 で保持されている電子バリューであり、「共有されるように管理する」とは、電子バリュー保持部 1 4 0 3 で保持されている電子バリューのうち、どれがバンク電子バリュー保持部 1 1 0 2 で保持されているかを識別できるようにしたり、電子バリュー保持部 1 4 0 3 で保持され、かつ、バンク電子バリュー保持部 1 1 0 2 で保持されている電子バリューが、プライベート電子バリューバンク 8 0 2 により使用された場合には、電子バリュー保持部 1 4 0 3 から使用された電子バリューを削除（または、電子バリューのステータスを「使用済み」に変更）したり、携帯端末 8 0 3 により使用された場合には、バンク共有管理部 1 1 0 4 に対して使用した電子バリューをバンク電子バリュー保持部 1 1 0 2 により削除（または、電子バリューのステータスを「使用済み」に変更）をすることを要求したり
- 15 することである。また、端末共有管理部 1 4 0 4 は、図 1 5 に例示する表 1 5 0 0 により、列 1 5 0 1 に出現する電子バリューの状態を列 1 5
- 20
- 25

02によって管理するようにしてもよく、列1502に「使用済」という状態が記録されている電子バリューをバンク電子バリュー保持部102より削除（または、電子バリューのステイタスを「使用済み」に変更）するようにバンク共有管理部1104に要求するようにしてもよい。

- 5 図16は携帯端末803の動作を説明するフローチャートであり、電子バリュー発行サーバに対して電子バリュー発行要求を、電子バリュー発行要求出力部1401により出力する（ステップS1601）。次にプライベート電子バリューバンク802から送信される電子バリューを、電子バリュー受信部1402により受信する（ステップS1602）。受信された電子バリューを、電子バリュー保持部1403により保持する（ステップS1603）。そして、電子バリューを、端末共有管理部1404により共有するように管理する（ステップS1604）。なお、ステップS1601が実行されると即座にステップS1602とが実行されずに、ステップS1601が実行されてしばらく時間が経過してからステップS1602が実行されるようになっていてもよい。これは、携帯端末803とプライベート電子バリューバンク802とが常に通信ができる状態にあるわけではないからである。
- 10
- 15

- 図17は、電子バリュー発行サーバ801と、プライベート電子バリューバンク802と、携帯端末803との相互作用を時間の経過に従って記述したシーケンス図である。まず、携帯端末803より電子バリュー発行サーバ801に電子バリュー発行要求が出力され（ステップS1701）、電子バリュー発行サーバ801は、電子バリューをプライベート電子バリューバンク802へ転送する（ステップS1702）。プライベート電子バリューバンク802は、携帯端末803へ電子バリューを送信する（ステップS1703）。その後、プライベート電子バリューバンク802と携帯端末803との間で電子バリューの共有のための管理
- 20
- 25

が行なわれる（ステップ S 1 7 0 4）。

このような実施の形態により、携帯端末 8 0 3 より電子バリュー発行サーバ 8 0 1 へ電子バリュー発行要求が送られ、その結果、電子バリューがプライベート電子バリューバンク 8 0 2 へ送られ、プライベート電子バリューバンク 8 0 2 によって電子バリューが保持され、プライベート電子バリューバンク 8 0 2 と携帯端末 8 0 3 とで電子バリューが共有されるようになる。その結果、プライベート電子バリューバンク 8 0 2 が電子バリューのバックアップを持つことになり、携帯端末 8 0 3 を紛失してしまう事態が生じて、電子バリューが失われることがなくなる。

10 （実施の形態 3）

図 2 2 は、本発明の実施の形態 3 にかかわるプライベート電子バリューバンクシステムの構成を示す図である。本実施の形態において、プライベート電子バリューバンクシステムは、電子バリュー発行サーバ 2 2 0 1 と、プライベート電子バリューバンク 2 2 0 2 と、携帯端末 2 2 0 3 とを備える。本実施の形態において、携帯端末 2 2 0 3 から電子バリュー発行サーバ 2 2 0 1 へ電子バリュー購入オーダーが出力され（矢印 2 2 0 4）、電子バリュー発行サーバ 2 2 0 1 より購入インストラクション 2 2 0 5 が送信される。携帯端末 2 2 0 3 は、プライベート電子バリューバンク 2 2 0 2 へ電子バリュー購入指示を送信し（矢印 2 2 0 6）、プライベート電子バリューバンク 2 2 0 2 より電子バリュー発行サーバ 2 2 0 1 へ電子バリュー購入要求が送信され（矢印 2 2 0 7）、電子バリュー発行サーバ 2 2 0 1 よりプライベート電子バリューバンク 2 2 0 2 へ電子バリューが転送され（矢印 2 2 0 8）、プライベート電子バリューバンク 2 2 0 2 より携帯端末 2 2 0 3 へ電子バリューが送信され、その後、プライベート電子バリューバンク 2 2 0 2 と携帯端末 2 2 0 3 との間で電子バリューの共有のための管理が行なわれる（矢印 2 2 1 0）。

図 2 3 は、電子バリュー発行サーバ 2 2 0 1 の機能ブロック図を例示する。本実施の形態において、電子バリュー発行サーバ 2 2 0 1 は、電子バリュー購入オーダー受付部 2 3 0 1 と、購入インストラクション送信部 2 3 0 2 と、電子バリュー購入要求受信部 2 3 0 3 と、電子バリュー転送部 2 3 0 4 とを有している。また、電子バリュー生成部（図示せず）も有している。

電子バリュー購入オーダー受付部 2 3 0 1 は、携帯端末 2 2 0 3 から電子バリュー購入オーダーを受け付ける。「電子バリュー購入オーダー」とは、携帯端末 2 2 0 3 の所持者が電子バリューの発行を受けたいことを表すデータである。

購入インストラクション送信部 2 3 0 2 は、携帯端末 2 2 0 3 に対して購入インストラクションを送信する。「購入インストラクション」とは、電子バリューを電子バリュー発行サーバ 2 2 0 1 から得るための情報であり、例えば、電子バリュー発行サーバ 2 2 0 1 の I P アドレス、ポート番号、U R L など、電子バリュー発行サーバ 2 2 0 1 を特定すべき情報、どのような種類の電子バリューを電子バリュー発行サーバ 2 2 0 1 が発行できるか、電子バリューの発行に伴う決済の方法、などが例として挙げられる。

電子バリュー購入要求受信部 2 3 0 3 は、購入インストラクション送信部 2 3 0 2 から送信された購入インストラクションに基づいたプライベート電子バリューバンク 2 2 0 2 からの電子バリューの購入要求である電子バリュー購入要求を受信する。「購入インストラクションに基づいた」とは、購入インストラクション送信部 2 3 0 2 から送信された購入インストラクションの内容に従って生成されたという意味である。

電子バリュー生成部は、電子バリュー購入要求受信部 2 3 0 3 で受信した電子バリュー購入要求に応じて、すでに存在する電子バリューをコ

ピーしたり、新しく電子バリューを作り出したりすることにより、電子バリューを生成する。

電子バリュー転送部 2304 は、電子バリュー購入要求受信部 2303 で受信した電子バリュー購入要求に応じて電子バリューをプライベート電子バリューバンクに転送する。「電子バリュー購入要求に応じて」とは、電子バリュー購入要求により指定された通りに電子バリュー生成部で電子バリューが生成されるということを意味する。電子バリュー購入要求により指定された種類の電子バリュー、指定された数量の電子バリューが電子バリュー生成部にて生成され、電子バリュー転送部 2304
10 よりプライベート電子バリューバンクに転送される。

図 24 は、電子バリュー発行サーバ 2201 の動作を説明するフローチャートである。携帯端末 2203 から電子バリュー購入オーダーを、電子バリュー購入オーダー受付部 2301 にて、受け付け（ステップ S2401）、その受け付けに応じて、携帯端末 2203 に対して購入イン
15 ストラクションを、購入インストラクション送信部 2302 により送信する（ステップ S2402）。その後、プライベート電子バリューバンク 2202 から電子バリュー購入要求を、電子バリュー購入要求受信部 2303 にて受信し（ステップ S2403）、電子バリューを、電子バリュー生成部にて生成し、生成された電子バリューを、電子バリュー転送部
20 2304 より、プライベート電子バリューバンク 2202 に転送する（ステップ S2404）。

なお、ステップ S2403 は、ステップ S2402 の処理が終わって即時に実行されなくてもよい。これは、後述のように電子バリュー購入要求は、携帯端末 2203 からプライベート電子バリューバンク 220
25 2 の通信の後に送信されてくるようになっており、携帯端末 2203 とプライベート電子バリューバンク 2202 とは常に通信できるとは限ら

ないからである。また、携帯端末 2203 から電子バリュー発行サーバ 2201 へ送信される電子バリュー購入オーダーの中に電子バリューの種類、数量が含まれており、電子バリュー発行サーバは、ステップ 2401 で電子バリュー購入オーダーを受け付けたときにオーダー番号（取引の識別情報）および電子バリューの種類、数量を記憶しておき、ステップ S2403 においてプライベート電子バリューバンクから電子バリュー購入要求を受信したときに、電子バリュー購入要求に含まれるオーダー番号（取引の識別情報）電子バリューの種類、数量とを比較して、同じである場合にのみ、ステップ S2404 において電子バリューをプライベート電子バリューバンクに転送するようにしてもよい。

図 25 は、本実施の形態におけるプライベート電子バリューバンク 2202 の機能ブロック図を例示している。プライベート電子バリューバンク 2202 は、電子バリュー購入指示受信部 2501 と、電子バリュー購入要求送信部 2502 と、転送電子バリュー受取部 2503 と、バンク電子バリュー保持部 2504 と、電子バリュー送信部 2505 と、バンク共有管理部 2506 とを有する。

電子バリュー購入指示受信部 2501 は、携帯端末 2203 から購入インストラクションに基づいて生成された電子バリュー購入指示を受信する。「購入インストラクションに基づいて生成された電子バリュー購入指示」とは、電子バリュー発行サーバ 2201 の購入インストラクション送信部 2302 から送信され、携帯端末 2203 が受信した購入インストラクションの内容に基づいて生成された電子バリューを購入するための情報である。例えば、購入インストラクションに電子バリュー発行サーバ 2201 を特定する情報が含まれていれば、その特定される情報が電子バリュー購入指示に含まれる。また、購入インストラクションに決済方法が指定されていれば、その決済方法を実行するために必要な

情報、例えば、クレジットカード番号、銀行預金口座番号、暗証番号などが含まれる。

電子バリュー購入要求送信部 2 5 0 2 は、電子バリュー購入指示受信部 2 5 0 1 で受信した電子バリュー購入指示に基づいて電子バリュー発行サーバ 2 2 0 1 に対して電子バリュー購入要求を送信する。例えば、電子バリュー購入指示に電子バリューの種類、数量が含まれていれば、その種類、数量の電子バリューを電子バリュー発行サーバ 2 2 0 1 から購入するためのデータが電子バリュー購入要求送信部 2 5 0 2 より送信される。その他に、指定された決済方法に従って電子バリューの対価の支払いが行なわれたという第 3 者の証明書なども電子バリュー購入要求に含まれてもよい。

転送電子バリュー受取部 2 5 0 3 は、電子バリュー購入要求送信部 2 5 0 2 から送信された電子バリュー購入要求に応じて電子バリュー発行サーバ 2 2 0 1 から転送される電子バリューを受取る。

15 バンク電子バリュー保持部 2 5 0 4 は、電子バリューを保持する。

電子バリュー送信部 2 5 0 5 は、バンク電子バリュー保持部 2 5 0 4 の電子バリューを携帯端末 2 2 0 3 に送信する。この送信は、バンク電子バリュー保持部 2 5 0 4 で保持されている全ての電子バリューを送信してもよいし、一部の電子バリューであってもよい。また、電子バリュー送信部 2 5 0 5 は、転送電子バリュー受取部 2 5 0 3 で受取られた電子バリューの全てを送信してもよいし、一部を送信してもよい。

バンク共有管理部 2 5 0 6 は、バンク電子バリュー保持部 2 5 0 4 で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理する。このバンク共有管理部 2 5 0 6 は、
25 実施の形態 2 のバンク共有管理部 1 1 0 4 と同じ働きをする。

図 2 6 は、プライベート電子バリューバンク 2 2 0 2 の動作を説明す

るフローチャートであり、携帯端末 2203 から電子バリュー購入指示を、電子バリュー購入指示受信部 2501 で受信し（ステップ S2601）、電子バリュー発行サーバ 2201 に対して電子バリュー購入要求を、電子バリュー購入要求送信部 2502 により送信する（ステップ S2602）。その後、電子バリュー発行サーバ 2201 から転送される電子バリューを、転送電子バリュー受取部 2503 で受取り（ステップ S2603）、受け取った電子バリューを、バンク電子バリュー保持部 2504 にて保持し（ステップ S2604）、保持した電子バリューを、電子バリュー送信部 2505 にて、携帯端末 2203 に送信する（ステップ S2605）。そして、電子バリューを共有するように管理する（ステップ S2606）。

図 27 は、携帯端末 2203 の機能ブロック図を例示している。携帯端末 2203 は、電子バリュー購入オーダー出力部 2701 と、購入インストラクション受信部 2702 と、電子バリュー購入指示送信部 2703 と、電子バリュー受信部 2704 と、電子バリュー保持部 2705 と、端末共有管理部 2706 とを有している。

電子バリュー購入オーダー出力部 2701 は、電子バリュー発行サーバ 2201 に対して電子バリュー購入オーダーを出力する。この出力は、携帯端末を所持する者の操作によって引き起こされる。

購入インストラクション受信部 2702 は、電子バリュー購入オーダー出力部 2701 から出力された電子バリュー購入オーダーに応じて電子バリュー発行サーバから購入インストラクションを受信する。

電子バリュー購入指示送信部 2703 は、購入インストラクション受信部 2702 で受信した購入インストラクションに応じてプライベート電子バリューバンク 2202 に対して電子バリュー購入指示を送信する。この送信は、購入インストラクションを購入インストラクション受信部

2702で受信した後、即座に行なわれてもよいし、購入インストラクション受信部2702で受信された購入インストラクションの内容を、携帯端末2203の所持者が見て判断を行なった結果の操作によって引き起こされてもよい。

- 5 電子バリュー受信部2704は、電子バリュー購入指示送信部2703から送信された電子バリュー購入指示に応じてプライベート電子バリューバンク2202から送信される電子バリューを受信する。

電子バリュー保持部2705は、電子バリューを保持する。

- 10 端末共有管理部2706は、バンク電子バリュー保持部2504で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理する。実施の形態2の端末共有管理部1404と同じ働きをする。

- 図28は、携帯端末2203の動作を説明するフローチャートである。まず、電子バリュー発行サーバ2201に対して電子バリュー購入オーダーを、電子バリュー購入オーダー出力部2701より出力し（ステップS2801）、電子バリュー発行サーバ2201から購入インストラクションを、電子バリュー購入オーダー出力部2701にて受信する（ステップS2802）。そして、プライベート電子バリューバンク2202に対して電子バリュー購入指示を、電子バリュー購入指示送信部2703より送信し（ステップS2803）、プライベート電子バリューバンク2202から電子バリューを、電子バリュー受信部2704にて受信し（ステップS2804）、受信した電子バリューを、電子バリュー保持部2705で保持し（ステップS2805）、端末共有管理部2706を用いて、電子バリューを共有するように管理する（ステップS2806）。

- 25 図29は、電子バリュー発行サーバ2201と、プライベート電子バリューバンク2202と、携帯端末2203との相互作用を時間の経過

- に従って記述したシーケンス図を例示する。まず、携帯端末 2203 より電子バリュー発行サーバ 2201 に電子バリュー購入オーダーが出力され (ステップ S 2901)、電子バリュー発行サーバ 2201 は携帯端末 2203 に購入インストラクションを送信する (ステップ S 2902)。
- 5 携帯端末 2203 は、購入インストラクションから電子バリュー購入指示を生成し、プライベート電子バリューバンク 2202 へ送信し (ステップ S 2903)、プライベート電子バリューバンク 2202 は、電子バリュー購入要求を電子バリュー発行サーバ 2201 へ送信し (ステップ S 2904)、電子バリュー発行サーバ 2201 は、電子バリューをプライベート電子バリューバンク 2202 へ転送する (ステップ S 2905)。
- 10 その後、プライベート電子バリューバンク 2202 は、電子バリューを携帯端末 2203 へ送信し (ステップ S 2906)、プライベート電子バリューバンク 2202 と携帯端末 2203 との間で電子バリューの共有のための管理が行なわれる (ステップ S 2907)。
- 15 このような実施の形態により、電子バリュー発行サーバ 2201 により発行された電子バリューが携帯端末 2203 だけではなくプライベート電子バリューバンクにも保持されるため、携帯端末 2203 の紛失や故障により電子バリューを失うことがなくなる。また、電子バリュー発行サーバ 2201 が購入インストラクションを送信することにより、電
- 20 子バリュー発行サーバ 2201 の指定した方式やプロトコルで電子バリューをプライベート電子バリューバンク 2202 に発行することができるようになる。また、携帯端末 2203 に電子バリュー購入指示を送信する機能が備わっていなくても、購入インストラクションに電子バリュー購入指示を送信する機能を端末に持たせるプラグインを含ませること
- 25 により、携帯端末 2203 に、電子バリュー購入指示を送信可能とする機能を持たせることができるようになる。

(実施の形態 4)

図 30 は、本発明の実施の形態 4 にかかわるプライベート電子バリューバンクシステムの構成を例示する。本実施の形態において、プライベート電子バリューバンクシステムは、プライベート電子バリューバンク
5 3001 と、携帯端末 3002 と、サービスサーバ 3003 とを備える。
本実施の形態において、プライベート電子バリューバンク 3001 と携帯
端末 3002 は電子バリューを共有しており、携帯端末 3002 は、
サービスサーバに対して電子バリューの送信を行ない（矢印 3004）、
その後、携帯端末 3002 とプライベート電子バリューバンク 3001
10 とが通信を行ったときに、プライベート電子バリューバンク 3001 と
携帯端末 3002 とで共有される電子バリューから、携帯端末 3002
からサービスサーバ 3003 へ送信された電子バリューを削除（または、
電子バリューのステイタスを「使用済み」に変更）する（矢印 3005）。

図 31 は、プライベート電子バリューバンク 3001 の機能ブロック
15 図を例示しており、プライベート電子バリューバンク 3001 は、バン
ク電子バリュー保持部 3101 とバンク共有管理部 3102 とを備えて
いる。

バンク電子バリュー保持部 3101 は、電子バリューを保持すること
を行なう。

20 バンク共有管理部 3102 は、バンク電子バリュー保持部 3101 で
保持されている電子バリューと、携帯端末 3002 で保持されている電
子バリューとが共有されているように管理する部であり、実施の形態 2
および実施の形態 3 のバンク共有管理部と同じ動作をする。

図 32 は、携帯端末 3002 の機能ブロック図を例示しており、携帯
25 端末 3002 は、電子バリュー保持部 3201 と、端末共有管理部 32
02 と、電子バリュー支払部 3203 とを備えている。

電子バリュー保持部 3 2 0 1 は電子バリューを保持する。電子バリュー保持部 3 2 0 1 で保持されている電子バリューは、バンク電子バリュー保持部 3 1 0 1 で保持されている電子バリューの一部であってもよし、全てであってもよい。

- 5 端末共有管理部 3 2 0 2 は、バンク電子バリュー保持部 3 1 0 1 で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されているように管理する部であり、実施の携帯 2 および実施の形態 3 の端末共有部と同じ動作をする。

- 10 電子バリュー支払部 3 2 0 3 は、サービスサーバ 3 0 0 3 に対して電子バリューを支払うために送信する。「電子バリューを支払うために送信する」とは、データとして表現されている電子バリューそのものを送信することのみならず、電子バリューそのものの代わりに預金などの振替指示情報などを送信する場合も含む。

- 図 3 3 は、携帯端末 3 0 0 2 の動作を説明するフローチャートである。
- 15 まず、サービスサーバに対して電子バリューの送信を、電子バリュー支払部により行なう（ステップ S 3 3 0 1）。そして、端末共有管理部 3 2 0 2 により、プライベート電子バリューバンクと電子バリューが共有されるにする（ステップ S 3 3 0 2）。具体的には、サービスサーバ 3 0 0 3 へ携帯端末 3 0 0 2 よりステップ S 3 3 0 1 において送信された電子
- 20 バリューをプライベート電子バリューバンクのバンク電子バリュー保持部 3 1 0 1 から削除（または、電子バリューのステイタスを「使用済み」に変更）することを行なう。なお、ステップ S 3 3 0 1 の処理が終わった後で、サービスサーバからサービスを受け入れる場合もある。また、ステップ S 3 3 0 1 の処理が終わって即時にステップ S 3 3 0 2 が実行
- 25 されず、携帯端末 3 0 0 2 とプライベート電子バリューバンク 3 0 0 1 とが通信できるようになった場合にステップ S 3 3 0 2 が実行されるよ

うになっていてもよい。

図 3 4 は、サービスサーバ 3 0 0 3 の機能ブロック図を例示しており、サービスサーバ 3 0 0 3 は、電子バリュー領収部 3 4 0 1 と、サービス提供部 3 4 0 2 とを備えている。

5 電子バリュー領収部 3 4 0 1 は、携帯端末 3 0 0 2 の電子バリュー支払部 3 2 0 3 から送信された電子バリューを領収するために受信する。

「電子バリューを領収するために受信する」とは、データとして表現されている電子バリューそのものを受信することのみならず、電子バリューそのものの代わりに預金などの振替指示情報などを受信する場合も含

10 む。

サービス提供部 3 4 0 2 は、携帯端末 3 0 0 2 の電子バリュー支払部 3 2 0 3 から受信した電子バリューに応じてサービスの提供のための処理を行なう。具体的には、サービスサーバ 3 0 0 3 が音楽の配信サービスを行なう場合には、携帯端末 3 0 0 2 に対して音楽のダウンロードを
15 許可し、ダウンロードを実行させる。また、サービスサーバ 3 0 0 3 が自動改札機であれば、ゲートを開く操作を開始したり、サービスサーバ 3 0 0 3 が飲料物の自動販売機であれば、飲料物を提供する。サービスサーバ 3 0 0 3 が音楽のダウンロードを行なう場合には、携帯端末 3 0 0 2 とサービスサーバ 3 0 0 3 とは、一般的にインターネットなどのネッ
20 トワークを介して接続されることになるが、サービスサーバ 3 0 0 3 が自動改札機や自動販売機などのリアルなサービスを提供する場合には、携帯端末 3 0 0 2 とサービスサーバ 3 0 0 3 とは赤外線通信やローカル無線通信などによって直接的に送受信ができるようになっていけばよい。

図 3 5 は、プライベート電子バリューバンク 3 0 0 1 と、携帯端末 3
25 0 0 2 と、サービスサーバ 3 0 0 3 との相互作用を時間の経過に従って記述したシーケンス図を例示する。まず、携帯端末 3 0 0 2 よりサービ

サーバ 3003 に対して電子バリューが送信される（ステップ S 3501）。サービスサーバ 3003 は、電子バリューを受信するとサービスを提供する（ステップ S 3502）。図 35 では、サービスは携帯端末 3002 に提供されるように書かれているが、サービスサーバ 3003 より携帯端末 3002 に提供される必要はなく、上述のように携帯端末 3002 以外の自動改札機や自動販売機などにより携帯端末 3002 の所持者に対してサービスが提供されるようになっていてもよい。携帯端末 3002 とプライベート電子バリューバンク 3001 とが通信ができるようになると、電子バリューの共有のための管理が行なわれる（ステップ S 3503）。すなわち、携帯端末 3002 より送信された電子バリューをプライベート電子バリューバンク 3001 より削除（または、電子バリューのステータスを「使用済み」に変更）したり、プライベート電子バリューバンク 3001 に保持されるようになった電子バリューを携帯端末 3002 へ送信したりする。

このように、サービスの提供のために携帯端末 3002 より電子バリューを送信し、携帯端末 3002 とプライベート電子バリューバンク 3001 とが通信可能になったときに、携帯端末 3002 とプライベート電子バリューバンク 3001 とで保持される電子バリューが共有されるように管理することにより、プライベート電子バリューバンク 3001 が電子バリューのバックアップをもっており携帯端末 3002 の破損、紛失などに対応することができ、しかも、携帯端末 3002 とプライベート電子バリューバンク 3001 とが通信できない状態でも携帯端末 3002 より電子バリューの使用が可能となる。

（実施の形態 5）

図 36 は、本発明の実施の形態 5 にかかわるプライベート電子バリューバンクシステムの構成を例示する。本実施の形態において、プライベ

ート電子バリューバンクシステムは、プライベート電子バリューバンク
3601と、携帯端末3602と、サービスサーバ3603とを備える。
本実施の形態において、携帯端末3602よりプライベート電子バリュ
ーバンク3601へ電子バリュー支払要求が送信され（矢印3604）、
5 プライベート電子バリューバンク3601よりサービスサーバ3603
に、電子バリューを支払うために送信することが行なわれる（矢印36
05）。その後、プライベート電子バリューバンク3601と携帯端末3
602との間で電子バリューの共有のための処理が行なわれ、プライベ
ート電子バリューバンク3601からサービスサーバ3603に取得さ
10 せる処理を行なった電子バリューが、プライベート電子バリューバンク
3601と携帯端末3602とで共有されている場合には、携帯端末3
602よりその電子バリューを削除（または、電子バリューのステイタ
スを「使用済み」に変更）することを行なう（矢印3606）。

図37は、プライベート電子バリューバンク3601の機能ブロック
15 図を例示する。プライベート電子バリューバンク3601は、バンク電
子バリュー保持部3701と、バンク共有管理部3702と、電子バリ
ュー支払要求受付部3703と、電子バリュー処理出力部3704とを
有する。

バンク電子バリュー保持部3701は、電子バリューを保持する。
20 バンク共有管理部3702は、バンク電子バリュー保持部3701で
保持されている電子バリューと、携帯端末3602で保持されている電
子バリューとが共有されるように管理する部であり、実施の形態2、3、
4のバンク共有管理部と同じ動作をする。

電子バリュー支払要求受付部3703は、携帯端末3602から電子
25 バリューのサービスサーバ3603への支払のための処理を行なうこと
の要求である電子バリュー支払要求を受け付ける。

電子バリュー処理出力部 3704 は、電子バリュー支払要求受付部で受け付けた電子バリュー支払要求に応じて、サービスサーバ 3603 で電子バリューを取得させるための処理を行なう。「電子バリューを取得させるための処理」とは、データとして表現されている電子バリューそのものを送信することのみならず、電子バリューそのものの代わりに預金などの振替指示情報などを送信する場合も含む。

図 38 は、プライベート電子バリューバンク 3601 の動作を説明するフローチャートである。まず、携帯端末 3602 から電子バリュー支払要求を、電子バリュー支払要求受付部 3703 にて受け付ける（ステップ S3801）。次に、サービスサーバ 3603 で電子バリューを取得させるための処理を行ない（ステップ S3802）、電子バリューが共有されるように管理する（ステップ S3803）。すなわち、ステップ S3802 においてサービスサーバ 3603 で電子バリューを取得させるための処理を行なった電子バリューがプライベート電子バリューバンク 3601 と携帯端末 3602 とで共有されている場合には、携帯端末 3602 からその電子バリューを削除（または、電子バリューのステータスを「使用済み」に変更）することを行なう。

図 39 は、携帯端末 3602 の機能ブロック図を例示する。携帯端末 3602 は、電子バリュー保持部 3901 と、端末共有管理部 3902 と、電子バリュー支払要求送信部 3903 とを有している。

電子バリュー保持部 3901 は、電子バリューを保持する。

端末共有管理部 3902 は、バンク電子バリュー保持部 3701 で保持されている電子バリューと、携帯端末 3602 で保持されている電子バリューとが共有されるように管理する。「携帯端末 3602 で保持されている電子バリュー」とは、電子バリュー保持部 3901 で保持されている電子バリューである。

電子バリュー支払要求送信部 3 9 0 3 は、プライベート電子バリューバンク 3 6 0 1 に対して電子バリュー支払要求を送信する。この電子バリュー支払要求の送信は、携帯端末 3 6 0 2 の所持者が携帯端末 3 6 0 2 を操作することにより行なわれる。

- 5 図 4 0 は、携帯端末 3 6 0 2 の動作を説明するフローチャートである。まず、プライベート電子バリューバンクに対して電子バリュー支払要求を、電子バリュー支払要求送信部 3 9 0 3 より送信する（ステップ S 4 0 0 1）。その後、プライベート電子バリューバンク 3 6 0 1 で電子バリューの支払のための処理が行なわれるので、バンク電子バリュー保持部
10 で保持されている電子バリューと、携帯端末 3 6 0 2 で保持されている電子バリューとが共有されるように管理する（ステップ S 4 0 0 2）。

- 図 4 1 は、サービスサーバ 3 6 0 3 の機能ブロック図を例示する。サービスサーバ 3 6 0 3 は、電子バリュー取得部 4 1 0 1 を有する。電子バリュー取得部 4 1 0 1 は、プライベート電子バリューバンクの処理に
15 よって取得すべき電子バリューを取得する。すなわち、電子バリュー取得部 4 1 0 1 は、プライベート電子バリューバンク 3 6 0 1 の電子バリュー処理出力部 3 7 0 4 により処理が行なわれた結果として電子バリューを取得する。ここに、「電子バリューを取得する」とは、データとして表現される電子バリューそのものを取得する場合に限られることはなく、
20 電子バリューの使用による預金の振替情報を取得するなど、電子的に移動する価値を取得する場合も含まれる。

- サービスサーバ 3 6 0 3 は、電子バリュー取得部 4 1 0 1 で取得した電子バリューに応じてサービスを提供する部を有していてもよい。その部は、例えば、電子バリューに対して音楽のダウンロードを許可したり
25 する。なお、電気、ガスなどの公共料金の支払や、税の支払のために、サービスサーバが電子バリューを取得する場合には、そのようなサービ

スを提供する部は無くてもよい。

図 4 2 は、プライベート電子バリューバンク 3 6 0 1 と、携帯端末 3 6 0 2 と、サービスサーバ 3 6 0 3 との相互作用を時間の経過に従って記述したシーケンス図を例示する。まず、携帯端末 3 6 0 2 よりプライベート電子バリューバンク 3 6 0 1 へ電子バリュー支払要求が送信される(ステップ S 4 2 0 1)。プライベート電子バリューバンク 3 6 0 1 は、サービスサーバ 3 6 0 3 に対して電子バリューを取得させるための処理を行なう(ステップ S 4 2 0 2)。プライベート電子バリューバンク 3 6 0 1 からサービスサーバで取得させた電子バリューが携帯端末で保持されている場合には、携帯端末からその電子バリューを削除(または、電子バリューのステイタスを「使用済み」に変更)する(ステップ S 4 2 0 3)。

このような実施の形態により、携帯端末 3 6 0 2 よりプライベート電子バリューバンク 3 6 0 1 に送信される電子バリュー支払要求に応じて、プライベート電子バリューバンクがサービスサーバに電子バリューの取得をさせるので、プライベート電子バリューバンク 3 6 0 1 が保持する電子バリューを携帯端末 3 6 0 2 の操作により使用することができ、また、使用された電子バリューが携帯端末 3 6 0 2 に保持されている場合には、その電子バリューは削除(または、電子バリューのステイタスを「使用済み」に変更)されるので、電子バリューが 2 重に使用されてしまうことを防止することができる。また、(電子バリューの種類ごとの)電子バリューを使用するための機能を携帯端末 3 6 0 2 が備える必要がなくなり、携帯端末 3 6 0 2 の構造が簡略化できる。

(実施の形態 6)

図 4 3 は、本発明の実施の形態 6 にかかわるプライベート電子バリューバンクシステムの構成を例示する。本実施の形態において、プライベ

ート電子バリューバンクシステムは、電子バリュー発行サーバ4301と、プライベート電子バリューバンク4302と、携帯端末4303とを備えており、これは実施の形態2と実施の形態3の構成と同じである。本実施の形態の特徴は、電子バリュー発行サーバ4301からプライベート電子バリューバンク4302へ電子バリューの更新要求である電子バリュー更新要求が送信され（矢印4304）、その後、プライベート電子バリューバンク4302と携帯端末4303との間で、更新された電子バリューの共有が行なわれるようにする（矢印4305）。これにより、例えば、電子バリューが入場券である場合には、公演の日程が変更になった場合など、入場可能な日時を変更することが可能になる。

図44は、電子バリュー発行サーバ4301の機能ブロック図であり、本実施の形態に関連する部分を例示している。電子バリュー発行サーバ4301は、電子バリュー更新要求送信部4401を有している。電子バリュー更新要求送信部4401は、プライベート電子バリューバンク4302のバンク電子バリュー保持部に保持されている電子バリューの更新要求である電子バリュー更新要求をプライベート電子バリューバンク4302に送信する。この送信のためには、電子バリュー発行サーバ4301は、どのプライベート電子バリューに対して、どの種類の電子バリューをどれだけ転送したかの転送履歴を記録しておく必要がある。ある種類の電子バリューの変更が必要になったときは、その転送履歴を参照して、その種類の電子バリューが転送されたプライベート電子バリューバンクに電子バリュー更新要求を送信する。

図45は、プライベート電子バリューバンク4302の機能ブロック図であり、本実施の形態に関連する部分を例示している。プライベート電子バリューバンク4302は、電子バリュー更新要求受信部4501と、電子バリュー更新部4502と、バンク電子バリュー保持部450

3 と、バンク共有管理部 4 5 0 4 とを有している。

電子バリュー更新要求受信部 4 5 0 1 は、電子バリュー発行サーバ 4 3 0 1 から送信された電子バリュー更新要求を受信する。

5 電子バリュー更新部 4 5 0 2 は、電子バリュー更新要求受信部 4 5 0 1 で受信した電子バリュー更新要求に応じてバンク電子バリュー保持部 4 5 0 3 に保持された電子バリューを更新する。

バンク電子バリュー保持部 4 5 0 3 は、電子バリューを保持する。実施の形態 2 および実施の形態 3 のバンク電子バリュー保持部と同じ動作であるが、電子バリュー更新部 4 5 0 2 によって保持している電子バリューが更新できるようになっている。

バンク共有管理部 4 5 0 4 は、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理する。本実施の形態においては、バンク共有管理部 4 5 0 4 は、実施の形態 2 などに示されたバンク共有管理部と同じように、電子バリューがプライベート電子バリューバンク 4 3 0 2 に転送されて増えた場合には、携帯端末 4 3 0 3 に増えた電子バリューを転送したり、プライベート電子バリューバンク 4 3 0 2 が電子バリューを使用した場合には、使用された電子バリューを携帯端末 4 3 0 3 が保持していれば削除（または、電子バリューのステータスを「使用済み」に変更）を行い、また、携帯端末 4 3 0 3 が電子バリューを使用した場合には、使用された電子バリューをプライベート電子バリューバンク 4 3 0 2 から削除（または、電子バリューのステータスを「使用済み」に変更）する。また、本実施の形態に特有の機能として、電子バリュー更新部 4 5 0 2 によって更新された電子バリューが携帯端末 4 3 0 3 にも保持されている場合には、携帯端末 4 3 0 3 に保持されえている電子バリューを更新することをも行なう。そのために、バンク共有管理部 4 5 0 4 は、

バンク電子バリュー保持部 4 5 0 3 で保持されている電子バリューが、どのように更新されたかを電子バリューごとに保持しておき、携帯端末 4 3 0 3 と通信が可能になったときに、携帯端末 4 3 0 3 で保持されている電子バリューの更新を行なう。

- 5 図 4 6 は、プライベート電子バリューバンク 4 3 0 2 の動作を説明するフローチャートである。まず、電子バリュー発行サーバ 4 3 0 1 から送信された電子バリュー更新要求を、電子バリュー更新要求受信部 4 5 0 1 で受信し（ステップ S 4 6 0 1）、その電子バリュー更新要求に従って、バンク電子バリュー保持部 4 5 0 3 に保持された電子バリューを、
- 10 電子バリュー更新部 4 5 0 2 によって更新する（ステップ S 4 6 0 2）。プライベート電子バリューバンク 4 3 0 2 と携帯端末 4 3 0 3 とが通信可能な状態になれば、電子バリューが、プライベート電子バリューバンク 4 3 0 2 と携帯端末 4 3 0 3 とで共有されるように、バンク共有管理部 4 5 0 4 によって管理する。

- 15 図 4 7 は、電子バリュー発行サーバ 4 3 0 1 と、プライベート電子バリューバンク 4 3 0 2 と、携帯端末 4 3 0 3 との相互作用を時間の経過に従って記述したシーケンス図を例示する。電子バリュー発行サーバ 4 3 0 1 から電子バリュー更新要求がプライベート電子バリューバンク 4 3 0 2 へ送信される（ステップ S 4 7 0 1）。これにより、バンク電子バ
- 20 リュー保持部 4 5 0 3 で保持されている電子バリューが更新され、その更新が行なわれた後もプライベート電子バリューバンク 4 3 0 2 と携帯端末 4 3 0 3 とで電子バリューが共有されるように管理が行なわれる（ステップ S 4 7 0 2）。

- このような構成により、電子バリュー発行サーバによって電子バリュー
- 25 が発行された後で、必要に応じて発行した電子バリューを更新することが可能となる。また、電子バリューがどのように流通しても、プライ

ベート電子バリューバンク 4 3 0 2 へ電子バリューの更新要求を送信することにより、電子バリューを更新することが可能となる。

(実施の形態 7)

実施の形態 6 において、電子バリュー発行サーバは無条件に発行した
5 電子バリューを更新することもできるが、更新するかどうかを、携帯端末の所持者に問い合わせ、所持者が更新する必要性を確認してから電子バリューを更新するようにしてもよい。

図 4 8 は、電子バリューの更新の必要性を確認する場合のプライベート電子バリューバンク 4 3 0 2 の機能ブロック図を例示する。本実施の
10 形態において、プライベート電子バリューバンク 4 3 0 2 は、電子バリュー更新要求受信部 4 5 0 1 と、更新要求問合せ送信部 4 8 0 1 と、更新要求問合せ結果受信部 4 8 0 2 と、更新判断部 4 8 0 3 と、電子バリュー更新部 4 5 0 2 と、バンク電子バリュー保持部 4 5 0 3 と、バンク共有管理部 4 5 0 4 とを有する。このうち、電子バリュー更新要求受信部 4
15 5 0 1 と、電子バリュー更新部 4 5 0 2 と、バンク電子バリュー保持部 4 5 0 3 と、バンク共有管理部 4 5 0 4 とは実施の形態 6 の説明において説明した。

更新要求問合せ送信部 4 8 0 1 は、電子バリュー更新要求受信部 4 5 0
1 で受信した電子バリュー更新要求を受け入れるか受け入れないかを携
20 帯端末 4 3 0 3 に問い合わせる更新要求問合せを送信する。

更新要求問合せ結果受信部 4 8 0 2 は、更新要求問合せ送信部 4 8 0 1 から送信された更新要求問合せに応じて携帯端末 4 3 0 3 から返信される更新要求問合せ結果を受信する。

更新判断部 4 8 0 3 は、更新要求問合せ結果に応じて電子バリュー更新
25 部 4 5 0 2 での電子バリューの更新の可否を判断する。

図 4 9 は、プライベート電子バリューバンク 4 3 0 2 の動作を説明す

るフローチャートである。まず、電子バリュー発行サーバ 4 3 0 1 から送信された電子バリュー更新要求を、電子バリュー更新要求受信部 4 5 0 1 にて受信し（ステップ S 4 9 0 1）、携帯端末 4 3 0 3 に、更新要求問合せ送信部 4 8 0 1 により、更新要求問合せを送信する（ステップ S 4 9 0 2）。次に、携帯端末 4 3 0 3 から返信される更新要求問合せ結果を、更新要求問合せ結果受信部 4 8 0 2 により、受信し（ステップ S 4 9 0 3）、電子バリュー更新が可能であるかどうかを、更新判断部で判断し（ステップ S 4 9 0 4）、もし更新可能であれば、バンク電子バリュー保持部 4 5 0 3 で保持された電子バリューを、電子バリュー更新部 4 5 0 2 により、更新し（ステップ S 4 9 0 5）、電子バリューが共有されるように、バンク共有管理部 4 5 0 4 によって、管理する（ステップ S 4 9 0 6）。

図 4 9 では、電子バリューが更新可能であるかどうかを判断した結果、更新が不可能であれば何もしないで処理を終えるようになっているが、例えば、電子バリュー発行サーバ 4 3 0 1 に対して、更新ができない旨のメッセージを送信するようになっていてもよい。

図 5 0 は、電子バリューの更新の必要性を確認する場合の携帯端末 4 3 0 3 の機能ブロック図を例示する。本実施の形態に特有のものとして、携帯端末 4 3 0 3 は、更新要求問合せ受信部 5 0 0 1 と、更新要求問合せ結果取得部 5 0 0 2 と、更新要求問合せ結果送信部 5 0 0 3 と、端末共有管理部 5 0 0 4 とを有する。

更新要求問合せ受信部 5 0 0 1 は、プライベート電子バリューバンク 4 3 0 2 から送信された更新要求問合せを受信する。

更新要求問合せ結果取得部 5 0 0 2 は、更新要求問合せ受信部 5 0 0 1 で受信した更新要求問合せに対して電子バリューの更新の可否に関する情報である更新要求問合せ結果を取得する。例えば、更新要求問合せ受信部 5 0 0 1 で受信した更新要求問合せの内容を携帯端末 4 3 0 3 の持つ表示部に

表示し、携帯端末 4 3 0 3 の所持者に更新の可否を尋ね、その所持者の操作を取得することにより、更新要求問合せ結果を取得する。

更新要求問合せ結果送信部 5 0 0 3 は、更新要求問合せ結果取得部 5 0 0 2 で取得した更新要求問合せ結果をプライベート電子バリューバンク 4 3 0 2 へ送信する。

端末共有管理部 5 0 0 4 は、プライベート電子バリューバンク 4 3 0 2 のバンク電子バリュー保持部 4 5 0 3 で保持されている電子バリューが変更された場合に、携帯端末 4 3 0 3 で保持されている電子バリューを更新することを行なう。

10 図 5 1 は、携帯端末 4 3 0 3 の動作を説明するフローチャートである。まず、プライベート電子バリューバンク 4 3 0 2 から送信された更新要求問合せを、更新要求問合せ受信部 5 0 0 1 にて、受信し（ステップ S 5 1 0 1）、更新要求問合せ結果取得部 5 0 0 2 により、電子バリューの更新の可否に関する情報である更新要求問合せ結果を取得し（ステップ S 5 1 0 15 2）、更新要求問合せ結果を、更新要求問合せ結果送信部 5 0 0 3 により、プライベート電子バリューバンク 4 3 0 2 へ送信する。

図 5 2 は、電子バリュー発行サーバ 4 3 0 1 と、プライベート電子バリューバンク 4 3 0 2 と、携帯端末 4 3 0 3 との相互作用を時間の経過に従って記述したシーケンス図を例示する。まず、電子バリュー発行サーバ 4 3 0 1 よりプライベート電子バリューバンク 4 3 0 2 へ電子バリュー更新要求が送信され（ステップ S 4 7 0 1）、プライベート電子バリューバンク 4 3 0 2 より携帯端末 4 3 0 3 へ更新要求問合せが送信され（ステップ S 5 2 0 1）、携帯端末 4 3 0 3 よりプライベート電子バリューバンク 4 3 0 2 へ更新要求問合せ結果が送信される（ステップ S 5 2 0 25 2）。その後、プライベート電子バリューバンク 4 3 0 2 と携帯端末 4 3 0 3 との間で電子バリューの共有のための管理が行なわれる（ステップ

S 4 7 0 2)。

このような構成により、発行された電子バリューが携帯端末の所持者の知らない間に更新されることが防止でき、また、携帯端末の所持者が望まない更新が行なわれることを防止することができる。

5 (実施の形態 8)

図 5 4 は、本発明の実施の形態 8 にかかわるプライベート電子バリューバンクシステムの構成を例示する。本実施の形態において、プライベート電子バリューバンクシステムは、電子バリュー発行サーバ 5 4 0 1 と、プライベート電子バリューバンク 5 4 0 2 と、携帯端末 5 4 0 3 とを備える。本実施の形態においては、携帯端末 5 4 0 3 より電子バリュー発行サーバ 5 4 0 1 へ電子バリュー発行要求が出力され (矢印 5 4 0 4)、電子バリュー発行サーバ 5 4 0 1 からよりプライベート電子バリューバンク 5 4 0 2 へ電子バリュー購入指示情報が送信され (矢印 5 4 0 5)、電子バリュー発行サーバ 5 4 0 1 とプライベート電子バリューバンク 5 4 0 2 との間で決済のための処理が行なわれ (矢印 5 4 0 6)、電子バリュー発行サーバ 5 4 0 1 よりプライベート電子バリューバンク 5 4 0 2 へ電子バリューが転送される (矢印 5 4 0 7)。その後、プライベート電子バリューバンク 5 4 0 2 より携帯端末 5 4 0 3 へ電子バリューが送信され (矢印 5 4 0 8)、電子バリューの共有のための管理が行なわれる (矢印 5 4 0 9)。

図 5 5 は、電子バリュー発行サーバ 5 4 0 1 の機能ブロック図を例示する。本実施の形態において、電子バリュー発行サーバ 5 4 0 1 は、電子バリュー発行要求受付部 5 5 0 1 と、電子バリュー購入指示情報送信部 5 5 0 2 と、電子バリュー転送部 5 5 0 3 とを有している。

25 電子バリュー発行要求受付部 5 5 0 1 は、携帯端末 5 4 0 3 から、電子バリュー発行要求を受け付ける。この電子バリュー発行要求は、プラ

イベート電子バリューバンク 5 4 0 2 において検証可能な電子署名が付
された購入指示情報と電子バリューの発行先であるプライベート電子バ
リューバンク 5 4 0 2 を指定した発行指示情報とを含む。図 7 2 は、電
子バリュー発行要求を模式的に例示している。図 7 2 において、電子バ
5 リュー発行要求 7 2 0 1 は、電子署名 7 2 0 3 が含まれる購入指示情報
7 2 0 2 と発行指示情報 7 2 0 4 とを含んでいる。発行指示情報には、
購入指示情報を送るべきプライベート電子バリューバンクの指定や、ど
の電子バリューをどれだけの数量購入する予定であるかといった電子バ
リューの発行予約のための情報などが含まれている。購入指示情報 7 2
10 0 2 には、プライベート電子バリューバンクが電子バリューを購入する
ために必要な情報が含まれており、どの電子バリュー発行サーバからど
の電子バリューをどれだけ購入するべきかの情報などが含まれている。
このような電子バリュー発行要求 7 2 0 1 により、発行指示情報 7 2 0
4 で指定されたプライベート電子バリューバンクへ購入指示情報 7 2 0
15 2 を送ることができるようになる。なお、電子署名とは、データの真正
性を判断するための情報であり、通常は、ハッシュ値が一致するような二
つの異なるデータを見つけることが計算量的に困難であるハッシュ関数
によるデータのハッシュ値に対して、公開鍵暗号方式の秘密鍵で暗号化
したデータである。本実施の形態においては、購入指示情報 7 2 0 2 に
20 付された電子署名 7 2 0 3 は、携帯端末 5 4 0 3 の秘密鍵によって暗号
化されたものである。

また、購入指示情報 7 2 0 2 には、クレジットカード番号など、プラ
イベート電子バリューバンク 5 4 0 2 が電子バリューの発行を受けるた
めの決済の情報を含ませることが可能である。しかし、クレジットカード
25 ド番号は、携帯端末 5 4 0 3 とプライベート電子バリューバンク 5 4 0
2 に知られてよいが、それ以外の電子バリュー発行サーバ 5 4 0 1 に知

られると不都合である。そこで、購入指示情報 7 2 0 2 は、プライベート電子バリューバンク 5 4 0 2 が復号できるが、電子バリュー発行サーバ 5 4 0 1 には復号できないように暗号化しておいてもよい。すなわち、携帯端末 5 4 0 3 とプライベート電子バリューバンク 5 4 0 2 との間の
5 共通鍵で暗号化されていたり、あるいは、プライベート電子バリューバンク 5 4 0 2 の公開鍵（この公開鍵は、例えば、バンク共有管理部に保持される）によって暗号化されていたりしてもよい。

電子バリュー購入指示情報送信部 5 5 0 2 は、電子バリュー発行要求受付部 5 5 0 1 で受け付けた電子バリュー発行要求を解釈し、発行指示
10 情報にて指定されたプライベート電子バリューバンク 5 4 0 2 に対して電子バリュー購入指示情報を送信する。

電子バリュー転送部 5 5 0 3 は、電子バリュー購入指示情報送信部 5 5 0 2 から送信された電子バリュー購入指示情報に応じてプライベート電子バリューバンクとの間でなされる決済の処理に応じてプライベート
15 電子バリューバンク 5 4 0 2 に電子バリューを転送する。すなわち、電子バリュー購入指示情報送信部 5 5 0 2 から電子バリュー購入指示情報が送られたプライベート電子バリューバンク 5 4 0 2 と電子バリュー発行サーバ 5 4 0 1 との間で、対価が支払われる決済処理が行なわれ、その結果として電子バリューが電子バリュー発行サーバ 5 4 0 1 から
20 プライベート電子バリューバンク 5 4 0 2 へ転送されることになる。

図 5 6 は、電子バリュー発行サーバ 5 4 0 1 の動作を説明するフローチャートである。まず、携帯端末 5 4 0 3 から電子バリュー発行要求を、電子バリュー発行要求受付部 5 5 0 1 にて受け付ける（ステップ S 5 6 0 1）。電子バリュー発行要求には、プライベート電子バリューバンク 5
25 4 0 2 を指定した発行指示情報が含まれるので、それに従って、指定されたプライベート電子バリューバンク 5 4 0 2 に対して電子バリュー購

入情報を、電子バリュー購入指示情報送信部 5 5 0 2 より送信する（ステップ S 5 6 0 2）。その後、電子バリュー購入情報が送られたプライベート電子バリューバンク 5 4 0 2 により決済のための処理が行なわれ、それに応じてプライベート電子バリューバンク 5 4 0 2 に電子バリュー
5 を、電子バリュー転送部 5 5 0 3 より転送する。

図 5 7 は、プライベート電子バリューバンク 5 4 0 2 の機能ブロック図を例示する。本実施の形態において、プライベート電子バリューバンク 5 4 0 2 は、電子バリュー購入指示情報受信部 5 7 0 1 と、電子署名
検証部 5 7 0 2 と、転送電子バリュー受取部 5 7 0 3 と、バンク電子バ
10 リュー保持部 5 7 0 4 と、電子バリュー送信部 5 7 0 5 と、バンク共有
管理部 5 7 0 6 とを有する。

電子バリュー購入指示情報受信部 5 7 0 1 は、電子バリュー発行サーバ 5 4 0 1 から送信される購入指示情報を受信し、購入指示情報が暗号化されている場合には復号化する。この購入指示情報には、電子署名が
15 付されており、その購入指示情報が真正なものであるかどうか判断できるようになっている。

電子署名検証部 5 7 0 2 は、電子バリュー購入指示情報受信部で受信した購入指示情報に含まれる電子署名を検証する。上述のように、本実施の形態においては、購入指示情報に含まれる電子署名は、携帯端末 5
20 4 0 3 の秘密鍵（この秘密鍵は、例えば、端末共有管理部に保持される）で署名されたものであるので、携帯端末 5 4 0 3 の証明書の中の公開鍵を用いて電子署名の検証を行うことになる。

転送電子バリュー受取部 5 7 0 3 は、電子署名検証部 5 7 0 2 での電子署名の検証に応じて電子バリュー発行サーバ 5 4 0 1 との間でなされる決済のための処理に応じて電子バリュー発行サーバ 5 4 0 1 から転送
25 される電子バリューを受け取る。すなわち、電子署名検証部 5 7 0 2 で

の電子署名の検証により、購入指示情報の真正性が肯定されれば、電子バリュー発行サーバ 5401 から電子バリューの転送を受けるための決済のための処理を行い、その処理が終了すると、転送電子バリュー受取部 5703 は、電子バリュー発行サーバ 5401 より転送される電子バ

5 リューを受け取る。

 バンク電子バリュー保持部 5704 は、電子バリューを保持する。

 電子バリュー送信部 5705 は、バンク電子バリュー保持部 5704 の電子バリューを携帯端末 5403 に送信する。

 バンク共有管理部 5706 は、バンク電子バリュー保持部 5704 で

10 保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理する。

 図 58 は、プライベート電子バリューバンクの動作を説明するフローチャートである。まず、電子バリュー発行サーバ 5401 から送信される購入指示情報を、電子バリュー購入指示情報受信部 5701 にて受信

15 する（ステップ S5801）。購入指示情報に含まれる電子署名を、電子署名検証部 5702 にて検証する（ステップ S5802）。電子署名が検証できた場合には（ステップ S5803 で Y へ分岐する場合）、購入指示情報は、携帯端末 5403 から出力されたものであると判明するので、決済のための処理に応じて、電子バリュー発行サーバ 5401 から転送

20 される電子バリューを、転送電子バリュー受取部 5703 にて受け取る（ステップ S5804）。受け取った電子バリューを、バンク電子バリュー保持部 5704 で保持し、携帯端末 5403 へ電子バリューを、電子バリュー送信部 5705 により送信する（ステップ S5805）。そして、電子バリューがプライベート電子バリューバンク 5402 と携帯端末 5

25 403 とで共有されるように、バンク共有管理部 5706 にて管理する（ステップ S5806）。なお、ステップ S5803 で電子署名が検証で

きなかった場合には、図 5 8 では、何もしないで処理を終了しているが、
検証できない電子署名が付された購入指示を受け取った旨のメッセージ
を電子バリュー発行サーバ 5 4 0 1 や携帯端末 5 4 0 3 へ送信して、悪
意を持った者による不正行為が行われたのではないかなどの注意を促す
5 ようにしてもよい。

図 5 9 は、携帯端末 5 4 0 3 の機能ブロック図を例示する。本実施の
形態において、携帯端末 5 4 0 3 は、電子バリュー発行要求出力部 5 9
0 1 と、電子バリュー受信部 5 9 0 2 と、電子バリュー保持部 5 9 0 3
と、端末共有管理部 5 9 0 4 とを有する。

10 電子バリュー発行要求出力部 5 9 0 1 は、プライベート電子バリュー
バンク 5 4 0 2 において検証可能な電子署名が付された購入指示情報と
電子バリューの発行先であるプライベート電子バリューバンク 5 4 0 2
を指定した発行指示情報とを含む電子バリュー発行要求を電子バリュー
発行サーバに対して出力する。この時、購入指示情報は、プライベート
15 電子バリューバンクで復号できるように暗号化されていてもよい。

電子バリュー受信部 5 9 0 2 は、プライベート電子バリューバンク 5
4 0 2 から送信される電子バリューを受信する。

電子バリュー保持部 5 9 0 3 は、電子バリューを保持する。

端末共有管理部 5 9 0 4 は、バンク電子バリュー保持部 5 7 0 4 で保
20 持されている電子バリューと、携帯端末で保持されている電子バリュー
とが共有されるように管理する。

図 6 0 は、携帯端末 5 4 0 3 の動作を説明するフローチャートである。
まず、電子バリュー発行要求を電子バリュー発行サーバ 5 4 0 1 に対し
て、電子バリュー発行要求出力部 5 9 0 1 にて、出力する（ステップ S
25 6 0 0 1）。その後、プライベート電子バリューバンク 5 4 0 2 から送信
される電子バリューを、電子バリュー受信部 5 9 0 2 にて、受信する。

受信した電子バリューを、電子バリュー保持部 5 9 0 3 にて保持する。
そして、電子バリューがバンク電子バリュー保持部 5 7 0 4 と電子バリュー保持部 5 9 0 3 とで共有されるように、端末共有管理部 5 9 0 4 によって管理する。

- 5 図 6 1 は、本実施の形態における電子バリュー発行サーバ 5 4 0 1 と、
プライベート電子バリューバンク 5 4 0 2 と、携帯端末 5 4 0 3 との相互作用を例示するシーケンス図である。まず携帯端末 5 4 0 3 から電子バリュー発行サーバ 5 4 0 1 へ電子バリュー発行要求が出力される（ステップ S 6 1 0 1）。電子バリュー発行サーバ 5 4 0 1 はプライベート電子バリューバンク 5 4 0 2 へ購入指示情報を送信する（ステップ S 6 1 0 2）。その後、電子バリュー発行サーバ 5 4 0 1 とプライベート電子バリューバンク 5 4 0 2 との間で決済のための処理がなされ（ステップ S 6 1 0 3）、電子バリュー発行サーバ 5 4 0 1 からプライベート電子バリューバンク 5 4 0 2 へ電子バリューが転送される（ステップ S 6 1 0 4）。
10 プライベート電子バリューバンク 5 4 0 2 は、携帯端末 5 4 0 3 へ電子バリューを転送し（ステップ S 6 1 0 5）、プライベート電子バリューバンク 5 4 0 2 と携帯端末 5 4 0 3 とにより共有のための管理が行なわれる（ステップ S 6 1 0 6）。
15

- 図 7 4 から図 7 8 までは、本実施の形態におけるデータの流れを模式的に例示する。図 7 4 において、携帯端末 5 4 0 3 から電子バリュー発行サーバ 5 4 0 1 へ発行指示情報 7 4 0 1 と購入指示情報 7 4 0 2 とを含む電子バリュー購入要求が出力される（矢印 5 4 0 4）。図 7 5 においては、購入指示情報 7 4 0 2 が電子バリュー発行サーバ 5 4 0 1 からプライベート電子バリューバンク 5 4 0 2 へ送信される（矢印 5 4 0 5）。
20 図 7 6 において、決済のための処理が行なわれ（矢印 5 4 0 6）、電子バリュー 7 6 0 1 が電子バリュー発行サーバ 5 4 0 1 よりプライベート電
25

子バリューバンク 5 4 0 2 へ転送される（矢印 5 4 0 7）。図 7 7 において、電子バリュー 7 6 0 1 がプライベート電子バリューバンク 5 4 0 2 から携帯端末 5 4 0 3 へ送信され（矢印 7 7 0 1）、図 7 8 に示すようにプライベート電子バリューバンク 5 4 0 2 の保持する電子バリュー 7 6 0 1 と携帯端末 5 4 0 3 の保持する電子バリュー 7 8 0 2 が共有されるように管理される（矢印 7 8 0 1）。

このような実施の形態により、携帯端末 5 4 0 3 より直接、電子バリュー発行サーバ 5 4 0 1 へ電子バリュー発行要求を出力することができ、電子バリューがチケットの場合には、予約も同時に行なえることになる。

10 また、購入指示情報をプライベート電子バリューバンク 5 4 0 2 が復号できるように暗号化することにより、クレジットカード番号などの電子バリューの転送を受けるための決済のための情報を電子バリュー発行サーバ 5 4 0 1 に知られることなくプライベート電子バリューバンク 5 4 0 2 へ送信することができるようになる。

15 （実施の形態 9）

図 6 2 は、本発明の実施の形態 9 にかかわるプライベート電子バリューバンクシステムの構成を示す図である。本実施の形態において、プライベート電子バリューバンクシステムは、電子バリュー発行サーバ 6 2 0 1 と、プライベート電子バリューバンク 6 2 0 2 と、携帯端末 6 2 0 3 とを備える本実施の形態において、携帯端末 6 2 0 3 より電子バリュー発行サーバ 6 2 0 1 へ電子バリュー発行要求が出力され（矢印 6 2 0 4）、電子バリュー発行サーバ 6 2 0 1 は、それに応じて携帯端末 6 2 0 3 に対して購入インストラクションを送信する（矢印 6 2 0 5）。携帯端末 6 2 0 3 は、署名付きの電子バリュー購入指示をプライベート電子バ

20 リューバンク 6 2 0 2 へ送信する（矢印 6 2 0 6）。署名付きの電子バリュー購入指示を受信したプライベート電子バリューバンク 6 2 0 2 は電

25

子バリュー発行サーバ 6 2 0 1 へ電子バリュー購入要求を送信し（矢印 6 2 0 8）、電子バリュー発行サーバ 6 2 0 1 は電子バリューをプライベート電子バリューバンク 6 2 0 2 へ転送し（矢印 6 2 0 9）、プライベート電子バリューバンク 6 2 0 2 は携帯端末 6 2 0 3 へ電子バリューを送信し（矢印 6 2 1 0）、その後、プライベート電子バリューバンク 6 2 0 2 と携帯端末 6 2 0 3 との間で電子バリューの共有のための管理が行なわれる（矢印 6 2 1 0）。

図 6 3 は、電子バリュー発行サーバ 6 2 0 1 の機能ブロック図を例示する。本実施の形態において、電子バリュー発行サーバ 6 2 0 1 は、電子バリュー発行要求受付部 6 3 0 1 と、購入インストラクション送信部 6 3 0 2 と、電子バリュー購入要求受信部 6 3 0 4 と電子バリュー転送部 6 3 0 5 とを有している。

電子バリュー発行要求受付部 6 3 0 1 は、携帯端末 6 2 0 3 から電子バリュー発行要求を受け付ける。「電子バリュー発行要求」とは、携帯端末 6 2 0 3 の所持者が電子バリューの発行を受けたいことを表すデータである。

購入インストラクション送信部 6 3 0 2 は、電子バリュー発行要求受付部で受け付けた電子バリュー発行要求に応じて、携帯端末 6 2 0 3 に対して購入インストラクションを送信する。「購入インストラクション」とは、電子バリューを電子バリュー発行サーバ 6 2 0 1 から得るための情報であり、例えば、電子バリュー発行サーバ 6 2 0 1 の IP アドレス、ポート番号、URL など、電子バリュー発行サーバ 6 2 0 1 を特定すべき情報、どのような種類の電子バリューを電子バリュー発行サーバ 6 2 0 1 が発行できるか、電子バリューの発行に伴う決済の方法、などが例として挙げられる。

電子バリュー購入要求受信部 6 3 0 4 は、購入インストラクション送

信部 6 3 0 2 から送信された購入インストラクションに基づいたプライベート電子バリューバンクからの電子バリューの購入要求である電子バリュー購入要求を受信する。「購入インストラクションに基づいた」とは、購入インストラクション送信部 6 3 0 2 から送信された購入インストラクションの内容に従って生成されたという意味である。

電子バリュー転送部 6 3 0 5 は、電子バリュー購入要求受信部 6 3 0 4 で受信した電子バリュー購入要求に応じて電子バリューをプライベート電子バリューバンク 6 2 0 2 に転送する。「電子バリュー購入要求に応じて」とは、電子バリュー購入要求により指定された通りということの意味する。電子バリュー購入要求により指定された種類の電子バリュー、指定された数量の電子バリューが電子バリュー転送部 6 3 0 5 よりプライベート電子バリューバンクに転送される。

図 6 4 は、電子バリュー発行サーバ 6 2 0 1 の動作を説明するフローチャートである。まず、携帯端末 6 2 0 3 より電子バリュー発行要求を、電子バリュー発行要求受付部 6 3 0 1 で受け付ける（ステップ S 6 4 0 1）。受け付けられた電子バリュー発行要求に応じて、携帯端末 6 2 0 3 に対して購入インストラクションを、購入インストラクション送信部 6 3 0 2 により送信する（ステップ S 6 4 0 2）。その後、プライベート電子バリューバンク 6 2 0 2 から電子バリュー購入要求を、電子バリュー購入要求受信部 6 3 0 4 にて受信し（ステップ S 6 4 0 3）、プライベート電子バリューバンク 6 2 0 2 に電子バリューを、電子バリュー転送部 6 3 0 5 により転送する（ステップ S 6 4 0 4）。

なお、ステップ S 6 4 0 3 は、ステップ S 6 4 0 2 の処理が終わって即時に実行されなくてもよい。これは、後述のように、電子バリュー購入要求は、携帯端末 6 2 0 3 とプライベート電子バリューバンク 6 2 0 2 との通信の後に送信がされるようになっており、携帯端末 6 2 0 3 と

プライベート電子バリューバンク 6 2 0 2 は常に通信ができるとは限らないからである。また、携帯端末 6 2 0 3 から電子バリュー発行サーバ 6 2 0 1 へ送信される電子バリュー発行要求の中に電子バリューの種類、数量などが含まれており、電子バリュー発行サーバ 6 2 0 1 は、ステップ S 6 4 0 1 で電子バリュー発行要求を受け付けたときに電子バリューの種類、数量などを記憶しておき、ステップ S 6 4 0 3 においてプライベート電子バリューバンクから電子バリュー購入要求を受信したときに、電子バリュー購入要求に含まれる電子バリューの種類、数量などとを比較して、記憶されたものと同じである場合にのみ、ステップ S 6 4 0 4 において電子バリューをプライベート電子バリューバンク 6 2 0 2 へ転送するようにしてもよい。

図 6 5 は、本実施の形態におけるプライベート電子バリューバンク 6 2 0 2 の機能ブロック図を例示している。プライベート電子バリューバンク 6 2 0 2 は、電子バリュー購入指示受信部 6 5 0 1 と、署名検証部 6 5 0 2 と、電子バリュー購入要求送信部 6 5 0 3 と、転送電子バリュー受取部 6 5 0 4 と、バンク電子バリュー保持部 6 5 0 5 と、電子バリュー送信部 6 5 0 6 と、バンク共有管理部 6 5 0 7 とを有する。

電子バリュー購入指示受信部 6 5 0 1 は、携帯端末 6 2 0 3 から購入インストラクションに基づいて生成された署名付の電子バリュー購入指示を受信する。「購入インストラクションに基づいて生成された」とは、電子バリュー発行サーバ 6 2 0 1 の購入インストラクション送信部 6 3 0 2 から送信され、携帯端末 6 2 0 3 が受信した購入インストラクションの内容に基づいて生成されたという意味である。「署名」とは、実施の形態 8 における電子署名と同義であり、「署名付の電子バリュー購入指示」とは、電子バリュー購入指示に、携帯端末 6 2 0 3 の電子署名が付加されていることを意味する。電子バリュー購入指示には、電子バリュー

一発行サーバ6201を特定するためのIPアドレスやURLが含まれ、また、購入インストラクションに決済の方法が指定されていれば、その決済の方法を実行するために必要な情報、例えば、クレジットカード番号、銀行預金口座番号、暗証番号などが含まれる。

- 5 署名検証部6502は、電子バリュー購入指示受信部6501で受信した電子バリュー購入指示の署名の検証を行う。「電子バリュー購入指示の署名」とは、電子バリュー購入指示に付加された署名であり、この署名の検証を行うことにより、電子バリュー購入指示が携帯端末6203で生成されたものであるかどうかを確認できる。
- 10 電子バリュー購入要求送信部6503は、署名検証部6502での検証により電子バリュー購入指示が真正であると検証された場合に、電子バリュー購入指示受信部6501で受信した電子バリュー購入指示に基づいて電子バリュー発行サーバ6201に対して電子バリュー購入要求を送信する。例えば、電子バリュー購入指示に電子バリューの種類、数量が含まれていれば、その種類、数量の電子バリューを電子バリュー発行サーバ6201から購入するための電子バリュー購入要求が、電子バリュー購入要求送信部6503で生成され電子バリュー発行サーバ6201へ送信される。

- 20 転送電子バリュー受取部6504は、電子バリュー購入要求送信部6503から送信された電子バリュー購入要求に応じて電子バリュー発行サーバ6201から転送される電子バリューを受け取る。

バンク電子バリュー保持部6505は、電子バリューを保持する。

電子バリュー送信部6506は、バンク電子バリュー保持部6505の電子バリューを携帯端末6203に送信する。

- 25 バンク共有管理部6507は、バンク電子バリュー保持部6505で保持されている電子バリューと、携帯端末6203で保持されている電

子バリューとが共有されるように管理する。

図 6 6 は、プライベート電子バリューバンク 6 2 0 2 の動作を説明するフローチャートである。まず、携帯端末 6 2 0 3 より電子バリュー購入指示を、電子バリュー購入指示受信部 6 5 0 1 にて受信する（ステップ S 6 6 0 1）。次に、電子バリュー購入指示の署名の検証を、署名検証部 6 5 0 2 で行なう（ステップ S 6 6 0 2）。署名の検証の結果、真正な署名と判断された場合には（ステップ S 6 6 0 3 で Y に分岐した場合）、電子バリュー発行サーバ 6 2 0 1 に対して電子バリュー購入要求を、電子バリュー購入要求送信部 6 5 0 3 より送信する。電子バリュー発行サーバ 6 2 0 1 が電子バリューを転送すると、その電子バリューを転送電子バリュー受取部 6 5 0 4 で受け取り（ステップ S 6 6 0 5）、電子バリューを、バンク電子バリュー保持部 6 5 0 5 で保持する。その後、バンク共有管理部 6 5 0 7 にて、電子バリューが共有されるように管理する（ステップ S 6 6 0 7）。

図 8 5 は、本実施の形態における携帯端末 6 2 0 3 の機能ブロック図を例示する。携帯端末 6 2 0 3 は、電子バリュー発行要求出力部 8 5 0 1 と、購入インストラクション受信部 8 5 0 2 と、電子バリュー購入指示送信部 8 5 0 3 と、電子バリュー受信部 8 5 0 4 と、電子バリュー保持部 8 5 0 5 と、端末共有管理部 8 5 0 6 とを有する。

電子バリュー発行要求出力部 8 5 0 1 は、電子バリュー発行サーバ 6 2 0 1 に対して電子バリュー発行要求を出力する。

購入インストラクション受信部 8 5 0 2 は、電子バリュー発行要求出力部 8 5 0 1 から出力された電子バリュー発行要求に応じて電子バリュー発行サーバ 6 2 0 1 から購入インストラクションを受信する。

電子バリュー購入指示送信部 8 5 0 3 は、購入インストラクション受信部 8 5 0 2 で受信した購入インストラクションの応じてプライベート

電子バリューバンク 6 2 0 2 に対して署名付の電子バリュー購入指示を送信する。

電子バリュー受信部 8 5 0 9 は、電子バリュー購入指示送信部 8 5 0 3 から送信された電子バリュー購入指示に応じてプライベート電子バリューバンク 6 2 0 2 から送信される電子バリューを受信する。

電子バリュー保持部 8 5 0 5 は、電子バリューを保持する。

端末共有管理部 8 5 0 6 は、バンク電子バリュー保持部 6 5 0 5 で保持されている電子バリューと、携帯端末 6 2 0 3 で保持されている電子バリューとが共有されるように管理する。「携帯端末 6 2 0 3 で保持されている電子バリュー」とは、携帯端末 6 2 0 3 の電子バリュー保持部 8 5 0 5 で保持されている電子バリューである。

図 8 6 は、携帯端末 6 2 0 3 の動作を説明するフローチャートである。まず、電子バリュー発行サーバ 6 2 0 1 に対して電子バリュー発行要求を、電子バリュー発行要求出力部 8 5 0 1 にて出力し（ステップ S 8 6 0 1 ）、電子バリュー発行サーバ 6 2 0 1 から購入インストラクションを、購入インストラクション受信部 8 5 0 2 にて受信する（ステップ S 8 6 0 2 ）。プライベート電子バリューバンク 6 2 0 2 に対して署名付の電子バリュー購入指示を、電子バリュー購入指示送信部 8 5 0 3 にて送信する（ステップ S 8 6 0 3 ）。次に、プライベート電子バリューバンク 6 2 0 2 から電子バリューを、電子バリュー受信部 8 5 0 4 にて受信し（ステップ S 8 6 0 4 ）、電子バリューを、電子バリュー保持部 8 5 0 5 にて保持する（ステップ S 8 6 0 5 ）。その後、端末共有管理部 8 5 0 6 により、電子バリューを共有するように管理する（ステップ S 8 6 0 6 ）。

図 7 9 から図 8 4 までは、本実施の形態におけるデータの流れを模式的に表したものである。まず、図 7 9 に示すように、携帯端末 6 2 0 3 より電子バリュー発行要求 7 9 0 1 が電子バリュー発行サーバ 6 2 0 1

へ出力され（矢印 6 2 0 4）、電子バリュー発行サーバ 6 2 0 1 から携帯
端末 6 2 0 3 へ購入インストラクション 7 9 0 2 が送信される（矢印 6
2 0 5）。図 8 0 に示すように、携帯端末 6 2 0 3 とプライベート電子バ
リューバンク 6 2 0 2 との通信が開始され（矢印 8 0 0 1）、図 8 1 に示
5 すように、携帯端末 6 2 0 3 からプライベート電子バリューバンク 6 2
0 2 へ電子バリュー購入指示 8 1 0 1 が送信される（矢印 6 2 0 6）。図
8 2 に示すように、電子バリュー購入指示 8 1 0 1 に基づいて、プライ
ベート電子バリューバンク 6 2 0 2 から電子バリュー発行サーバ 6 2 0
1 に対して電子バリュー購入要求が送信され（矢印 6 2 0 7）、図 8 3 に
10 示すように、電子バリュー発行サーバ 6 2 0 1 からプライベート電子バ
リューバンク 6 2 0 2 へ電子バリュー 8 3 0 1 が転送される（矢印 6 2
0 8）。その後、図 8 4 に示すように、プライベート電子バリューバンク
6 2 0 2 から携帯端末 6 2 0 3 へ電子バリュー 8 4 0 1 が送信され（矢
印 6 2 0 9）、電子バリュー 8 3 0 1 と電子バリュー 8 4 0 1 とがプライ
15 ベート電子バリューバンク 6 2 0 2 と携帯端末 6 2 0 3 で共有されるよ
うに管理される（矢印 6 2 1 0）。

このように、携帯端末 6 2 0 3 からの電子バリュー発行要求に応じて、
電子バリュー発行サーバ 6 2 0 1 が購入インストラクションを送信する
ことによって、電子バリュー発行サーバ 6 2 0 1 は、自身が発行できる
20 電子バリューの種類、数量を携帯端末 6 2 0 3 に示したり、電子バリュ
ーを手に入れるための決済方法などを指定することができる。また、電
子バリューの実際の入手のプロセスは、プライベート電子バリューバン
ク 6 2 0 2 と電子バリュー発行サーバ 6 2 0 1 とで行なわれるため、
様々なプロトコルに基づいて電子バリューの入手ができ、新しいプロト
25 コルにも対応することができる。また、発行された電子バリューはプラ
イベート電子バリューバンク 6 2 0 2 と携帯端末 6 2 0 3 とで共有され

るため、携帯端末 6 2 0 3 を紛失したり、携帯端末 6 2 0 3 が故障するなど、携帯端末 6 2 0 3 が使用できない状態に陥っても、プライベート電子バリューバンク 6 2 0 2 に電子バリューのバックアップがあるので、電子バリューが失われることがなくなる。また、携帯端末 6 2 0 3 に電子バリュー購入指示を送信する機能が備わっていなくても、購入インストラクションに電子バリュー購入指示を送信する機能を端末に持たせるプラグインを含ませることにより、携帯端末 6 2 0 3 に、電子バリュー購入指示を送信可能とする機能を持たせることができるようになる。また、署名付きの電子バリュー購入指示がプライベート電子バリューバンク 6 2 0 2 へ送信されることにより、悪意を持った第 3 者が送信した電子バリュー購入指示情報を検出することができ、不正を防止することができる。

(実施の形態 1 0)

図 6 7 は、本発明の実施の形態 1 0 にかかわるプライベート電子バリューバンクシステムの構成を示す図である。本実施の形態において、プライベート電子バリューバンクシステムは、プライベート電子バリューバンク 6 7 0 1 と、携帯端末 6 7 0 2 と、携帯端末 6 7 0 5 とを備える。プライベート電子バリューバンク 6 7 0 1 と携帯端末 6 7 0 2、およびプライベート電子バリューバンク 6 7 0 1 と携帯端末 6 7 0 5 は、電子バリューを共有するように管理しており(矢印 6 7 0 3、矢印 6 7 0 6)、携帯端末 6 7 0 2 よりプライベート電子バリューバンク 6 7 0 1 へ電子バリュー譲渡要求が出力され(矢印 6 7 0 4)、この出力により、携帯端末 6 7 0 2 がプライベート電子バリューバンク 6 7 0 1 とが共有している電子バリューが、携帯端末 6 7 0 5 とプライベート電子バリューバンク 6 7 0 1 とが共有している電子バリューとなる。

図 6 8 は、プライベート電子バリューバンク 6 7 0 1 の機能ブロック

図を例示する。プライベート電子バリューバンク 6701 は、少なくとも 2 以上のバンク電子バリュー保持部 6801、6802 と、バンク共有管理部 6803 と、電子バリュー譲渡要求受付部 6804、電子バリュー移動制御部 6805 とを有する。

- 5 バンク電子バリュー保持部 6801、6802 は、電子バリューを保持する。バンク電子バリュー保持部には、携帯端末が一台あるいは複数台対応しており、対応するバンク電子バリュー保持部と携帯端末とは、後述のバンク共有管理部 6803 により電子バリューが共有される。

- 10 バンク共有管理部 6803 は、バンク電子バリュー保持部 6801、6802 で保持されている電子バリューと、バンク電子バリュー保持部に対応して定められる携帯端末で保持されている電子バリューとが共有されるように管理する。図 68 においては、バンク共有管理部は一つしか示されておらず、これが全てのバンク電子バリュー保持部と、それに対応する携帯端末とで保持される電子バリューの共有の管理をするよう
- 15 になっているが、一つのバンク電子バリュー保持部に一つのバンク共有管理部が対応して、そのバンク電子バリュー保持部と携帯端末との間での電子バリューの共有の管理をするようになっていてもよい。

- 20 電子バリュー譲渡要求受付部 6804 は、電子バリュー譲渡要求を携帯端末 6702 から受け付ける。「電子バリュー譲渡要求」とは、バンク電子バリュー保持部で保持されている電子バリューを他のバンク電子バリュー保持部を指定して移動することによる電子バリューの譲渡の要求である。「他のバンク電子バリュー保持部」を指定するためには、プライベート電子バリューバンク 6701 の中のバンク電子バリュー保持部を識別する名前などで指定してもよいし、他のバンク電子バリュー保持部
- 25 に対応する携帯端末を指定する。例えば、携帯電話番号、所持者の住所氏名、携帯端末に割り振られた IP アドレス、携帯端末の識別符号など

によって携帯端末を指定して、その指定された携帯端末に対応するバンク電子バリュー保持部が指定されるようになっていてもよい。

電子バリュー移動制御部 6805 は、電子バリュー譲渡要求受付部 6804 で受け付けた電子バリュー譲渡要求に応じて、前記電子バリュー
5 譲渡要求を出力した携帯端末に対応するバンク電子バリュー保持部から、前記電子バリュー譲渡要求により指定されるバンク電子バリュー保持部へ電子バリューを移動する処理を実行する。例えば、バンク電子バリュー保持部 6801 が携帯端末 6702 に対応しており、携帯端末 6702 がバンク電子バリュー保持部 6802 を指定して電子バリュー譲渡要求を出力した場合には、電子バリュー移動制御部 6805 は、バンク電子バリュー保持部 6801 からバンク電子バリュー保持部 6802 へ電子バリューを移動する処理を実行する。
10

図 69 は、プライベート電子バリューバンク 6701 の動作を説明するフローチャートである。まず、電子バリュー譲渡要求を携帯端末から、
15 電子バリュー譲渡要求受付部 6804 にて受け付け（ステップ S6901）、電子バリューを、電子バリュー移動制御部 6805 により移動する（ステップ S6903）。その後、電子バリューが共有されるように、バンク共有管理部 6803 により管理する。すなわち、電子バリューが譲渡されたバンク電子バリュー保持部に対応する携帯端末に、譲渡された
20 バンク電子バリューが保持されている場合には、それを削除（または、電子バリューのステイタスを「使用済み」に変更）することを行なう。また、必要に応じて、電子バリューが譲受されたバンク電子バリュー保持部に対応する携帯端末に、譲受された電子バリューを保持させ、バンク電子バリュー保持部と電子バリューを共有するようにする。

25 図 70 は、携帯端末 6702 の機能ブロック図を例示する。携帯端末 6702 は、電子バリュー保持部 7001 と、端末共有管理部 7002

と、電子バリュー譲渡要求出力部 7 0 0 3 とを有する。

電子バリュー保持部 7 0 0 1 は、電子バリューを保持する。

端末共有管理部 7 0 0 2 は、携帯端末 6 7 0 2 で保持されている電子バリューと、携帯端末 6 7 0 2 に対応して定められるバンク電子バリュー保持部で保持されている電子バリューとが共有されるように管理する。

電子バリュー譲渡要求出力部 7 0 0 3 は、プライベート電子バリューバンク 6 7 0 1 に対して他のバンク電子バリュー保持部を指定して電子バリューを移動することによる譲渡の要求である電子バリュー譲渡要求を出力する。上述のように、他のバンク電子バリュー保持部を指定するには、バンク電子バリュー保持部を指定する場合と、バンク電子バリュー保持部に対応する携帯端末を指定する場合とがある。

図 7 1 は、携帯端末とプライベート電子バリューバンクとの相互作用を示すシーケンス図である。まず、ステップ S 7 1 0 1 において、携帯端末よりプライベート電子バリューバンクへ電子バリュー譲渡要求が出力さる。その後、ステップ S 7 1 0 2 において共有の管理がされる。すなわち、譲渡された電子バリューが携帯端末より削除される。その後ステップ S 7 1 0 3 において電子バリューが譲渡されたバンク電子バリュー保持部に対応する携帯端末との間で、電子バリューの共有の管理が行なわれ、電子バリューが譲渡されたバンク電子バリュー保持部とそのバンク電子バリュー保持部に対応する携帯端末との間で譲渡された電子バリューの共有が行なわれる。

このような構成により、端末に、電子バリューの譲渡に対応する電子バリューの譲受の機能が無くても、電子バリューの譲渡が行なえる。また、譲渡された電子バリューは、プライベート電子バリューバンク 6 7 0 1 と携帯端末とで共有されるため、携帯端末を失ったり、携帯端末が故障しても、電子バリューを失うことがない。また、電子バリューの譲

渡を、プライベート電子バリューバンク 6 7 0 1 を経由して行なうことにより、電子バリューの譲渡の履歴がプライベート電子バリューバンク 6 7 0 1 に残る。もし、電子バリューの譲渡の後に不正な電子バリューの使用（例えば、電子バリューの譲渡を行ない、電子バリューの所持を失った者が、譲渡した電子バリューを使用することなど）があった場合には、この電子バリューの譲渡の履歴により、電子バリューを不正に使用した者を探すことができる。

（実施の形態 2 から実施の形態 1 0 までに共通の実施の形態）

実施の形態 2 から実施の形態 1 0 までにおいて、電子バリューは電子バリューを一意に識別する電子バリュー識別子で識別されるようになっていてもよい。ただし、一意に識別できる範囲は、プライベート電子バリューバンクのバンク電子バリュー保持部とそれに対応する携帯端末の電子バリュー保持部の間で一意に識別できればよい。このように電子バリューが識別できる場合において、電子バリューの識別子を「電子バリュー識別子」と呼ぶことにする。この場合、プライベート電子バリューバンクのバンク共有管理部と携帯端末の端末共有管理部とは、プライベート電子バリューバンクのバンク電子バリュー保持部で保持される電子バリューの電子バリュー識別子に、携帯端末の電子バリュー保持部で保持される電子バリューの電子バリュー識別子を含むように管理するようにしてもよい。この様子を例示するのが図 5 3 であり、電子バリューは「電子バリュー A」のように識別子により一意に識別され、携帯端末 5 3 0 3 の電子バリュー保持部 5 3 0 4 で保持されている電子バリューの識別子である電子バリュー B、電子バリュー F は、プライベート電子バリューバンク 5 3 0 0 のバンク電子バリュー保持部 5 3 0 1 で保持されている電子バリューの識別子に含まれるようになっている。このようにすることにより、携帯端末の電子バリュー保持部で保持される電子バ

ユーは、必ず、それに対応するプライベート電子バリューバンクのバンク電子バリュー保持部で保持されることになるので、携帯端末を紛失したり、携帯端末が故障したりして、携帯端末が使用不可能な状態になっても、対応するプライベート電子バリューバンクのバンク電子バリュー保持部に電子バリューが保持されているので、電子バリューを失うことがない。このようにプライベート電子バリューバンクのバンク電子バリュー保持部に保持されている電子バリューの電子バリュー識別子に携帯端末の電子バリュー保持部に保持されている電子バリューの電子バリュー識別子が含まれるようにするためには、電子バリュー発行サーバから転送される電子バリューが必ずプライベート電子バリューバンクに転送されるようになっていれば実現することができる。

実施の形態 2 から実施の形態 10 までにおけるプライベート電子バリューバンクと携帯端末とは、通信を行なう必要があり、この通信の中で電子バリューの共有の管理が行なわれる。したがって、この通信は安全に行なう必要がある。そこで、バンク共有管理部は、図 18 に示すように、バンク共有管理部プライベート鍵 1801（図 2 における電子財布プライベート鍵 71 に相当する）と端末共有管理部証明書 1802（図 2 におけるモバイル電子財布証明書 52 に相当する）を有するようになっていてもよい。バンク共有管理部プライベート鍵 1801 は、公開鍵暗号方式の通信に用いるバンク共有管理部の有する秘密鍵であり、端末共有管理部証明書 1802 は、携帯端末からの署名を認証するためのものであり、携帯端末の端末共有管理部の有する公開鍵を認証者である第三者が署名を施したものである。このバンク共有管理部プライベート鍵 1801 と端末共有管理部証明書 1802 とにより、プライベート電子バリューバンクと携帯端末との間で暗号化が施された安全な通信を実現することができる。あるいは、図 19 に示すように、バンク共有管理部

は、バンク共有管理部プライベート鍵 1 8 0 1 とバンク共有管理部証明書 1 9 0 1 とを有するようになっていてもよい。バンク共有管理部証明書 1 9 0 1 は、プライベート電子バリューバンクの署名を他の携帯端末において認証させるためのものであり、プライベート電子バリューバン
5 クのバンク共有管理部の有する公開鍵を第 3 者が署名を行なったものである。プライベート電子バリューバンクと携帯端末とが通信を行なう際には、プライベート電子バリューバンクから携帯端末へバンク共有管理部証明書 1 9 0 1 が送られ、安全な通信が行われる。

同様に、図 2 0 と図 2 1 とに示すように、端末共有管理部は、端末共
10 有管理部プライベート鍵 2 0 0 1 及び、バンク共有管理部証明書 2 0 0 2 又は、端末共有管理部証明書 2 1 0 1 を有するようになっていてもよい。端末共有管理部プライベート鍵 2 0 0 1 は、公開鍵暗号化方式の暗号化に用いるものであり、携帯端末の端末共有管理部が有する秘密鍵である。バンク共有管理部証明書 2 0 0 2 は、プライベート電子バリュー
15 バンクからの署名を認証するためのものであり、端末共有管理部証明書 2 1 0 1 は携帯端末の署名をプライベート電子バリューバンクにおいて認証させるためのものである。

なお、プライベート電子バリューバンクは、複数の端末に対応して複数のバンク電子バリュー保持部を有していてもよい。この場合、1 つの
20 プライベート電子バリューバンクに対して、バンク共有管理部の有するバンク共有プライベート鍵が 1 つだけであってもよい。また、バンク共有プライベート鍵が、携帯端末に対応するバンク電子バリュー保持部それぞれに対応して複数個存在し、結果として、1 つのプライベート電子バリューバンクに対してバンク共有プライベート鍵が複数個あってもよ
25 い。

また、図 1 1 に示すように、実施の形態 2 におけるプライベート電子

バリューバンク 802 の電子バリュー送信部 1103 は、携帯端末 803 に電子バリューを送信する際に、バンク共有管理部 1104 の有するバンク共有管理部プライベート鍵で暗号化を行なうために、バンク共有管理部 1104 に対して電子バリューの暗号化を実行させ、その結果を
5 受け取るようになっていてもよい。他の実施の形態におけるプライベート電子バリューバンクにおいても同様であり、バンク共有管理部以外の部であって携帯端末と暗号化された通信を行う部は、バンク共有管理部に暗号化と復号化を実行させるようになっていてもよい（例えば、携帯端末より電子バリュー発行要求などを受信する場合も、復号化をバンク
10 共有管理部に実行させるようになっていてもよい）。同じように、携帯端末の端末共有管理部以外の部であって、プライベート電子バリューバンクで暗号化された通信を行なう部は、端末共有管理部に暗号化と復号化を実行させるようになっていてもよい。

また、携帯端末は、スマートカードなどの IC カードを付属させること
15 とができるようになっていてもよく、携帯端末の機能の一部がスマートカードなどの IC カードを使用して実現されるようになっていてもよい。例えば、端末共有管理部の有する端末共有管理部プライベート鍵がスマートカードなどの IC カードに格納される形態がある。この形態においては、端末共有管理部プライベート鍵が格納されたスマートカードなどの
20 IC カードを携帯端末に付属させることにより、その携帯端末を上述の携帯端末として機能させることができる。また、スマートカードなどの IC カードに端末共有管理部プライベート鍵が格納されるとともに、電子バリューも格納され、電子バリュー保持部がスマートカードなどの IC カードによって実現される 2 番目の形態もある。すなわち、この 2
25 番目の形態においては、スマートカードなどの IC カードは、端末共有管理部プライベート鍵を格納し、また、電子バリューを保持する電子バ

リユー保持部を有していることになる。このスマートカードなどの I C カードを携帯端末に付属させることにより、その携帯端末を上述の携帯端末として機能させることができる。また、端末共有管理部と電子バリュー保持部とが、スマートカードなどの I C カードのアプリケーションとして実現される 3 番目の形態もある。ここに示した 3 番目の形態においても、端末共有管理部プライベート鍵は、スマートカードなどの I C カードに格納される。すなわち、スマートカードなどの I C カードのアプリケーションにより端末共有管理部と電子バリュー保持部とが実現され、このようなスマートカードなどの I C カードを携帯端末に付属させることにより、その携帯端末を上述の携帯端末として機能させることができる。このようなスマートカードや I C カードを携帯端末とは別に発行することにより、スマートカードや I C カードの発行をビジネスとして展開することができる。

15 産業上の利用可能性

以上説明したように本発明によれば、ユーザの電子バリューがプライベート電子バリューバンクにより管理されているので、リアル上のサービスに対してユーザが電子バリューを使用する場合に、第 2 の電子財布上に管理されている電子バリューを使用するとともに、その後にプライベート電子バリューバンクと携帯端末が通信した際に更新して前記第 1、第 2 の電子財布上の電子バリューを関連付けることにより、ネット上のサービスとリアル上のサービスの両方に対して、安全性と利便性と経済性を確保しつつ電子バリューを利用することができる。

また、ユーザの携帯端末に管理されている電子バリューとプライベート電子バリューバンク上に管理されている電子バリューを一致させることができ、また、不正使用を防止することができる。

また、ネット上のサービスに対して、安全性と利便性と経済性を確保しつつ電子バリューを利用することができる。

また、リアル上のサービスに対して、安全性と利便性と経済性を確保しつつ電子バリューを利用することができる。

- 5 また、電子バリュー発行サーバとプライベート電子バリューバンクが独立しているので、種々の形態のビジネスに応用することができる。

また、ネットを介した電子バリューの発行と電子バリューの管理における安全性を向上させることができる。

- 10 また、ネットを介した電子バリューの発行とその決済における安全性を向上させることができる。

また、電子バリューの発行後の内容の変更や、電子バリューの譲渡が行なえる。

請求の範囲

1. ユーザの要求に応じて発行された電子バリューを管理するための第
1の電子財布を備えたプライベート電子バリューバンクと、 前記第1
5の電子財布上に管理されている電子バリューの内、少なくとも一つ以上
の電子バリューが管理されている第2の電子財布を備えた携帯端末とを
有し、 前記第2の電子財布が操作された場合にネットを介して前記第
1の電子財布が操作されるように結びつけられているプライベート電子
バリューバンクシステム。
- 10 2. 前記第1の電子財布上に管理されている電子バリューを操作する場
合に前記第1、第2の電子財布の間で相互に認証を行うことを特徴とす
る請求の範囲第1項に記載のプライベート電子バリューバンクシステム。
3. ネット上のサービスに対してユーザが電子バリューを使用する場合
に、前記第1の電子財布上に管理されている電子バリューをネットを介
15して使用するとともに、前記第2の電子財布上に管理されている電子バ
リューをネットを介して更新することを特徴とする請求の範囲第1項又
は請求の範囲第2項に記載のプライベート電子バリューバンクシステム。
4. リアル上のサービスに対してユーザが電子バリューを使用する場合
に、前記第2の電子財布上に管理されている電子バリューを使用すると
20ともに、その後に前記プライベート電子バリューバンクと携帯端末が通
信した際に更新することにより、前記第1、第2の電子財布上の電子バ
リューを関連付けるようにしたことを特徴とする請求の範囲第1項ない
し請求の範囲第3項のいずれか1つに記載のプライベート電子バリュー
バンクシステム。
- 25 5. ユーザの要求に応じて電子バリューを発行して前記プライベート電
子バリューバンクに転送する電子バリュー発行サーバを更に備え、前記

プライベート電子バリューバンクは電子バリューを発行せず、電子バリューの管理のみを行うことを特徴とする請求の範囲第1項ないし請求の範囲第3項のいずれか1つに記載のプライベート電子バリューバンクシステム。

- 5 6. 電子バリューを管理する第1の電子財布を備えたプライベート電子バリューバンクと、要求に応じて電子バリューを発行する電子バリュー発行サーバと、前記第1の電子財布と1対1に対応する第2の電子財布を備えた携帯端末とを有し、前記第2の電子財布が生成する電子バリューの発行要求に対し、前記電子バリュー発行サーバが生成した電子バリューを第1の電子財布に送信し、前記第1の電子財布が電子バリュー発行サーバから電子バリューを受信し、管理するプライベート電子バリューバンクシステム。

7. 前記電子バリュー発行サーバから電子バリューを購入する際に、前記プライベート電子バリューバンクと前記電子バリュー発行サーバとの間でその代金の支払の決済をすることを特徴とする請求の範囲第5項に記載のプライベート電子バリューバンクシステム。

8. ユーザが前記電子バリュー発行サーバから購入するために、前記携帯端末が前記電子バリュー発行サーバに対し、発行指示情報と、前記プライベート電子バリューバンクの第1の電子財布宛に電子封書化された購入指示情報を含む電子バリュー発行要求メッセージを送信し、前記電子バリュー発行サーバが前記電子封書化された購入指示情報を取り出して前記プライベート電子バリューバンクに送信し、前記プライベート電子バリューバンクが前記電子封書化された購入指示情報を開封して検証し、正しい場合に前記電子バリュー発行サーバとの間で電子バリューの代金の支払の決済を行うとともに、前記電子バリュー発行サーバが前記プライベート電子バリューバンクに電子バリューを発行し、前記発行さ

れた電子バリューに応じた第1の電子財布の内容に基づいて前記第2の電子財布の内容を更新することを特徴とする請求の範囲第6項に記載のプライベート電子バリューバンクシステム。

9. 請求の範囲第1項ないし請求の範囲第7項のいずれか1つに記載の
5 携帯端末。

10. 請求の範囲第1項ないし請求の範囲第7項のいずれか1つに記載の携帯端末に着脱自在な第2の電子財布の内容を記憶する記憶媒体と処理系を有するスマートカード。

11. 請求の範囲第1項ないし請求の範囲第7項のいずれか1つに記載
10 の携帯端末に着脱自在な電子財布。

12. 請求の範囲第1項ないし請求の範囲第7項のいずれか1つに記載のプライベート電子バリューバンク。

13. 電子バリュー発行サーバと、電子バリューを利用するためのプライベート電子バリューバンクと、電子バリューを利用するための携帯端
15 末と、からなるプライベート電子バリューバンクシステムであって、電子バリュー発行サーバは、携帯端末から電子バリュー発行要求を受け付ける電子バリュー発行要求受付部と、電子バリュー発行要求受付部で受け付けた電子バリュー発行要求に応じて、プライベート電子バリューバンクに電子バリューを転送する電子バリュー転送部と、を有し、プライ
20 ベート電子バリューバンクは、電子バリュー発行サーバから転送される電子バリューを受け取る転送電子バリュー受取部と、電子バリューを保持するバンク電子バリュー保持部と、バンク電子バリュー保持部の電子バリューを携帯端末に送信する電子バリュー送信部と、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されてい
25 る電子バリューとが共有されるように管理するバンク共有管理部と、を有し、携帯端末は、電子バリュー発行サーバに対して電子バリュー発行

要求を出力する電子バリュー発行要求出力部と、プライベート電子バリューバンクから送信される電子バリューを受信する電子バリュー受信部と、電子バリューを保持する電子バリュー保持部と、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理する端末共有管理部とを有するプライベート電子バリューバンクシステム。

1 4. 電子バリュー発行サーバと、電子バリューを利用するためのプライベート電子バリューバンクと、電子バリューを利用するための携帯端末と、からなるプライベート電子バリューバンクシステムであって、電子バリュー発行サーバは、携帯端末から電子バリュー購入オーダーを受け付ける電子バリュー購入オーダー受付部と、電子バリュー発行要求受付部で受け付けた電子バリュー発行要求に応じて、携帯端末に対して購入インストラクションを送信する購入インストラクション送信部と、購入インストラクション送信部から送信された購入インストラクションに基づいたプライベート電子バリューバンクからの電子バリューの購入要求である電子バリュー購入要求を受信する電子バリュー購入要求受信部と、電子バリュー購入要求受信部で受信した電子バリュー購入要求に応じて電子バリューをプライベート電子バリューバンクに転送する電子バリュー転送部と、を有し、プライベート電子バリューバンクは、携帯端末から購入インストラクションに基づいて生成された電子バリュー購入指示を受信する電子バリュー購入指示受信部と、電子バリュー購入指示受信部で受信した電子バリュー購入指示に基づいて電子バリュー発行サーバに対して電子バリュー購入要求を送信する電子バリュー購入要求送信部と、電子バリュー購入要求送信部から送信された電子バリュー購入要求に応じて電子バリュー発行サーバから転送される電子バリューを受け取る転送電子バリュー受取部と、電子バリューを保持するバンク電子

- バリュー保持部と、バンク電子バリュー保持部の電子バリューを携帯端末に送信する電子バリュー送信部と、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理するバンク共有管理部と、を有し、携帯端末は、
- 5 電子バリュー発行サーバに対して電子バリュー購入オーダーを出力する電子バリュー購入オーダー出力部と、電子バリュー購入オーダー出力部から出力された電子バリュー購入オーダーに応じて電子バリュー発行サーバから購入インストラクションを受信する購入インストラクション受信部と、購入インストラクション受信部で受信した購入インストラクシ
- 10 ョンに応じてプライベート電子バリューバンクに対して電子バリュー購入指示を送信する電子バリュー購入指示送信部と、電子バリュー購入指示送信部から送信された電子バリュー購入指示に応じてプライベート電子バリューバンクから送信される電子バリューを受信する電子バリュー受信部と、電子バリューを保持する電子バリュー保持部と、バンク電子
- 15 バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理する端末共有管理部とを有するプライベート電子バリューバンクシステム。
15. 電子バリューを利用するためのプライベート電子バリューバンクと、電子バリューを利用するための携帯端末と、電子バリューの支払い
- 20 に応じてサービスを提供するためのサービスサーバと、からなるプライベート電子バリューバンクシステムであって、プライベート電子バリューバンクは、電子バリューを保持するバンク電子バリュー保持部と、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理するバンク共有
- 25 管理部を有し、携帯端末は、電子バリューを保持する電子バリュー保持部と、バンク電子バリュー保持部で保持されている電子バリューと、携

帯端末で保持されている電子バリューとが共有されるように管理する端末共有管理部と、サービスサーバに対して電子バリューを支払うために電子バリューの送信を行う電子バリュー支払部と、を有し、サービスサーバは、携帯端末の電子バリュー支払部から送信された電子バリューを
5 領収するために受信する電子バリュー領収部と、携帯端末の電子バリュー支払部から受信した電子バリューに応じてサービスの提供のための処理を行うサービス提供部を有するプライベート電子バリューバンクシステム。

1 6. 携帯端末の電子バリュー支払部と、サービスサーバの電子バリュー
10 ー領収部との間は、ネットワークを介せずに直接的に送受信を行う請求の範囲第 1 5 項に記載の電子バリューバンクシステム。

1 7. 電子バリューを利用するためのプライベート電子バリューバンクと、電子バリューを利用するための携帯端末と、電子バリューの支払いに応じてサービスを提供するためのサービスサーバと、からなるプライベート電子バリューバンクシステムであって、プライベート電子バリュー
15 ーバンクは、電子バリューを保持するバンク電子バリュー保持部と、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理するバンク共有管理部と、携帯端末から電子バリューのサービスサーバへの支払のための
20 の処理を行うことの要求である電子バリュー支払要求を受け付ける電子バリュー支払要求受付部と、電子バリュー支払要求受付部で受け付けた電子バリュー支払要求に応じて、サービスサーバで電子バリューを取得させるための処理をおこなう電子バリュー処理出力部と、を有し、携帯端末は、電子バリューを保持する電子バリュー保持部と、バンク電子バ
25 リュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理する端末共有管理部と、プ

ライベート電子バリューバンクに対して電子バリュー支払要求を送信する電子バリュー支払要求送信部と、を有し、サービスサーバは、プライベート電子バリューバンクの処理によって取得すべき電子バリューを取得する電子バリュー取得部と、を有するプライベート電子バリューバンクシステム。

18. 電子バリュー発行サーバと、電子バリューを利用するためのプライベート電子バリューバンクと、電子バリューを利用するための携帯端末と、からなるプライベート電子バリューバンクシステムであって、電子バリュー発行サーバは、プライベート電子バリューバンクのバンク電子バリュー保持部に保持されている電子バリューの更新要求である電子バリュー更新要求をプライベート電子バリューバンクに送信する電子バリュー更新要求送信部を有し、プライベート電子バリューバンクは、電子バリュー発行サーバから送信された電子バリュー更新要求を受信する電子バリュー更新要求受信部と、電子バリュー更新要求受信部で受信した電子バリュー更新要求に応じてバンク電子バリュー保持部に保持された電子バリューを更新する電子バリュー更新部と、をさらに有する請求の範囲第13項または請求の範囲第14項に記載のプライベート電子バリューバンクシステム。

19. プライベート電子バリューバンクは、電子バリュー更新要求受信部で受信した電子バリュー更新要求を受け入れるか受け入れないかを携帯端末に問い合わせる更新要求問合せを送信する更新要求問合せ送信部と、更新要求問合せ送信部から送信された更新要求問合せに応じて携帯端末から返信される更新要求問合せ結果を受信する更新要求問合せ結果受信部と、更新要求問合せ結果に応じて電子バリュー更新部での電子バリューの更新の可否を判断する更新判断部とを有し、携帯端末は、プライベート電子バリューバンクから送信された更新要求問合せを受信する更新要求問合せ受信

部と、更新要求問合せ受信部で受信した更新要求問合せに対して電子バリューの更新の可否に関する情報である更新要求問合せ結果を取得する更新要求問合せ結果取得部と、更新要求問合せ結果取得部で取得した更新要求問合せ結果をプライベート電子バリューバンクに送信する更新要求問合せ結果送信部とを有する請求の範囲第18項に記載のプライベート電子バリューバンクシステム。

20. 電子バリュー発行サーバと、電子バリューを利用するためのプライベート電子バリューバンクと、電子バリューを利用するための携帯端末と、からなるプライベート電子バリューバンクシステムであって、電子バリュー発行サーバは、携帯端末からプライベート電子バリューバンクにおいて検証可能な電子署名が付された購入指示情報と電子バリューの発行先であるプライベート電子バリューバンクを指定した発行指示情報とを含む電子バリュー発行要求を受け付ける電子バリュー発行要求受付部と、電子バリュー発行要求受付部で受け付けた電子バリュー発行要求を解釈し、発行指示情報にて指定されたプライベート電子バリューバンクに対して電子バリュー購入指示情報を送信する電子バリュー購入指示情報送信部と、電子バリュー購入指示情報送信部から送信された電子バリュー購入指示情報に応じてプライベート電子バリューバンクとの間でなされる決済のための処理に応じてプライベート電子バリューバンクに電子バリューを転送する電子バリュー転送部と、を有し、プライベート電子バリューバンクは、電子バリュー発行サーバから送信される購入指示情報を受信する電子バリュー購入指示情報受信部と、電子バリュー購入指示情報受信部で受信した電子バリュー購入指示情報に含まれる電子署名を検証する電子署名検証部と、電子署名検証部での電子署名の検証に応じて電子バリュー発行サーバとの間でなされる決済のための処理に応じて電子バリュー発行サーバから転送される電子バリューを受け取

- る転送電子バリュー受取部と、電子バリューを保持するバンク電子バリュー保持部と、バンク電子バリュー保持部の電子バリューを携帯端末に送信する電子バリュー送信部と、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理するバンク共有管理部と、を有し、携帯端末は、プライベート電子バリューバンクにおいて検証可能な電子署名が付された購入指示情報と電子バリューの発行先であるプライベート電子バリューバンクを指定した発行指示情報とを含む電子バリュー発行要求を電子バリュー発行サーバに対して出力する電子バリュー発行要求出力部と、
- 5 プライベート電子バリューバンクから送信される電子バリューを受信する電子バリュー受信部と、電子バリューを保持する電子バリュー保持部と、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理する端末共有管理部とを有するプライベート電子バリューバンクシステム。
- 10 21. 購入指示情報は、プライベート電子バリューバンクにおいて復号できるように暗号化されていることを特徴とする請求の範囲第20項記載のプライベート電子バリューバンクシステム。
22. 電子バリュー発行サーバと、電子バリューを利用するためのプライベート電子バリューバンクと、電子バリューを利用するための携帯端末と、からなるプライベート電子バリューバンクシステムであって、電子バリュー発行サーバは、携帯端末から電子バリュー発行要求を受け付ける電子バリュー発行要求受付部と、電子バリュー発行要求受付部で受け付けた電子バリュー発行要求に応じて、携帯端末に対して購入インストラクションを送信する購入インストラクション送信部と、購入インストラクション送信部から送信された購入インストラクションに基いたプ
- 20
- 25 プライベート電子バリューバンクからの電子バリューの購入要求である電

子バリュー購入要求を受信する電子バリュー購入要求受信部と、電子バリュー購入要求受信部で受信した電子バリュー購入要求に応じて電子バリューをプライベート電子バリューバンクに転送する電子バリュー転送部と、を有し、プライベート電子バリューバンクは、携帯端末から購入

5 インストラクションに基づいて生成された署名付の電子バリュー購入指示を受信する電子バリュー購入指示受信部と、電子バリュー購入指示受信部で受信した電子バリュー購入指示の署名の検証を行う署名検証部と、署名検証部での検証により電子バリュー購入指示が真正であると検証された場合に、電子バリュー購入指示受信部で受信した電子バリュー購入

10 指示に基づいて電子バリュー発行サーバに対して電子バリュー購入要求を送信する電子バリュー購入要求送信部と、電子バリュー購入要求送信部から送信された電子バリュー購入要求に応じて電子バリュー発行サーバから転送される電子バリューを受け取る転送電子バリュー受取部と、電子バリューを保持するバンク電子バリュー保持部と、バンク電子バリュー

15 ユー保持部の電子バリューを携帯端末に送信する電子バリュー送信部と、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理するバンク共有管理部と、を有し、携帯端末は、電子バリュー発行サーバに対して電子バリュー発行要求を出力する電子バリュー発行要求出力部と、電子バ

20 リュー発行要求出力部から出力された電子バリュー発行要求に応じて電子バリュー発行サーバから購入インストラクションを受信する購入インストラクション受信部と、購入インストラクション受信部で受信した購入インストラクションに応じてプライベート電子バリューバンクに対して署名付の電子バリュー購入指示を送信する電子バリュー購入指示送信

25 部と、電子バリュー購入指示送信部から送信された電子バリュー購入指示に応じてプライベート電子バリューバンクから送信される電子バリュー

ーを受信する電子バリュー受信部と、電子バリューを保持する電子バリュー保持部と、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末で保持されている電子バリューとが共有されるように管理する端末共有管理部とを有するプライベート電子バリューバンクシステム。

23. 電子バリューを利用するためのプライベート電子バリューバンクと、電子バリューを利用するための携帯端末と、からなるプライベート電子バリューバンクシステムであって、プライベート電子バリューバンクは、電子バリューを保持する少なくとも二以上のバンク電子バリュー保持部と、バンク電子バリュー保持部で保持されている電子バリューと、
- 10 バンク電子バリュー保持部に対応して定められる携帯端末で保持されている電子バリューとが共有されるように管理するバンク共有管理部と、バンク電子バリュー保持部で保持されている電子バリューを他のバンク電子バリュー保持部を指定して移動することによる電子バリューの譲渡
- 15 の要求である電子バリュー譲渡要求を携帯端末から受け付ける電子バリュー譲渡要求受付部と、電子バリュー譲渡要求受付部で受け付けた電子バリュー譲渡要求に応じて、前記電子バリュー譲渡要求を出力した携帯端末に対応するバンク電子バリュー保持部から前記電子バリュー譲渡要求により指定されるバンク電子バリュー保持部へ電子バリューを移動す
- 20 る処理を実行する電子バリュー移動制御部と、を有し、携帯端末は、電子バリューを保持する電子バリュー保持部と、携帯端末で保持されている電子バリューと、携帯端末に対応して定められるバンク電子バリュー保持部で保持されている電子バリューとが共有されるように管理する端末共有管理部と、プライベート電子バリューバンクに対して他のバンク
- 25 電子バリュー保持部を指定して電子バリューを移動することによる譲渡の要求である電子バリュー譲渡要求を出力する電子バリュー譲渡要求出

力部と、を有するプライベート電子バリューバンクシステム。

24. 電子バリューは、電子バリューを一意に識別する電子バリュー識別子で識別され、プライベート電子バリューバンクのバンク共有管理部と、携帯端末の端末共有管理部とは、電子バリューバンクのバンク電子バリュー保持部で保持される電子バリューの電子バリュー識別子に、携帯端末の電子バリュー保持部で保持される電子バリューの電子バリュー識別子を含むように管理する請求の範囲第13項から請求の範囲第23項に記載のプライベート電子バリューバンクシステム。

25. バンク共有管理部は、バンク電子バリュー保持部で保持されている電子バリューと、携帯端末の電子バリュー保持部とで保持されている電子バリューとを共有させるための管理に利用する公開鍵暗号化方式の通信に用いるバンク共有管理部プライベート鍵及び、携帯端末からの署名を認証するための端末共有管理部証明書又は、自身の署名を他の携帯端末において認証させるためのバンク共有管理部証明書を有し、端末共有管理部は、電子バリュー保持部で保持されている電子バリューと、プライベート電子バリューバンクのバンク電子バリュー保持部で保持されている電子バリューとを共有させるための管理に利用する公開鍵暗号化方式の通信に用いる端末共有管理部プライベート鍵及び、プライベート電子バリューバンクからの署名を認証するためのバンク共有管理部証明書又は、自身の署名を他のプライベート電子バリューバンクにおいて認証させるための端末共有管理部証明書を有する、請求の範囲第13項から請求の範囲第23項に記載のプライベート電子バリューバンクシステム。

26. 請求の範囲第13項から請求の範囲第25項に記載の携帯端末。

27. 請求の範囲第13項から請求の範囲第25項に記載のプライベート電子バリューバンク。

28. 端末共有管理部プライベート鍵を格納し、携帯端末に付属させることにより、その携帯端末を請求の範囲第25項に記載の携帯端末として機能させるスマートカード。

29. 端末共有管理部プライベート鍵を格納し、電子バリューを保持する電子バリュー保持部を有し、携帯端末に付属させることにより、その携帯端末を請求の範囲第25項に記載の携帯端末として機能させるスマートカード。

30. 端末共有管理部と電子バリュー保持部とを実現するアプリケーションを有し、携帯端末に付属させることにより、その携帯端末を請求の範囲第25項に記載の携帯端末として機能させるスマートカード。

図 1

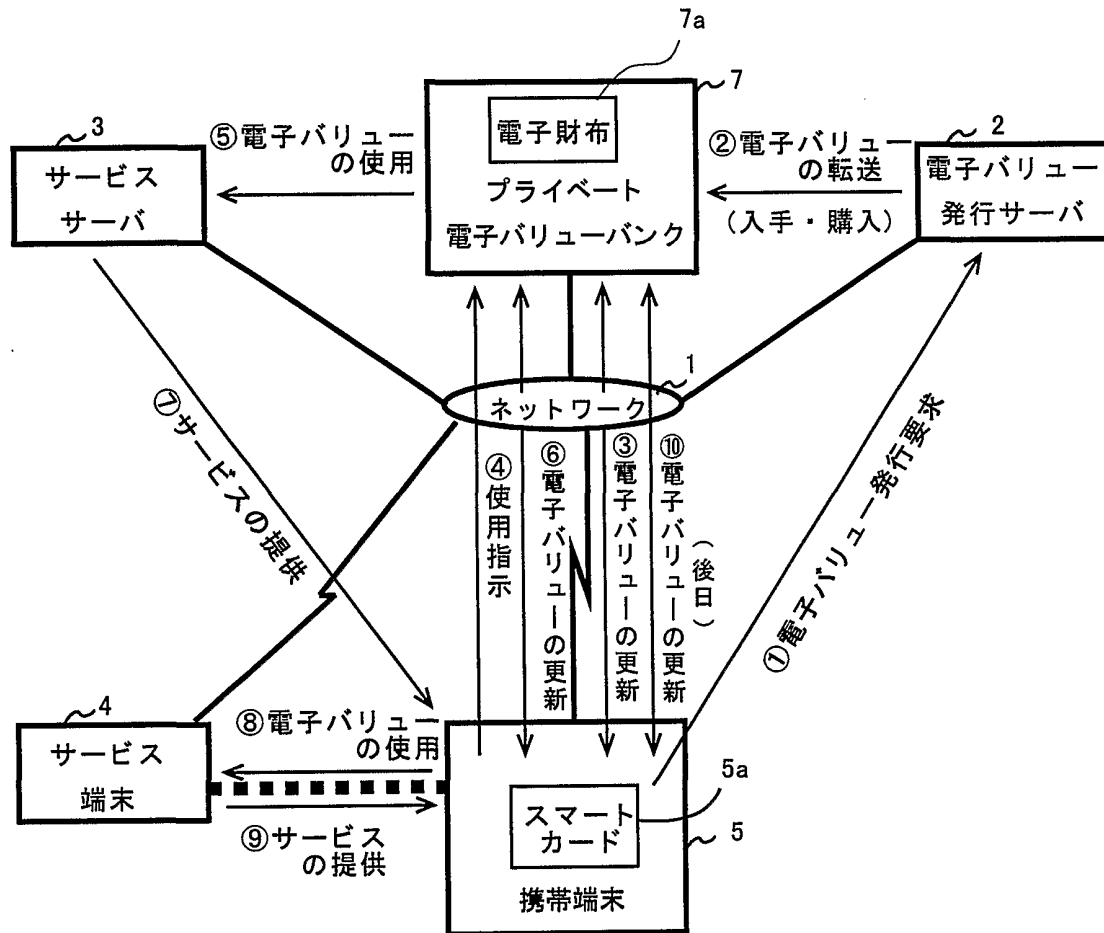


図 2

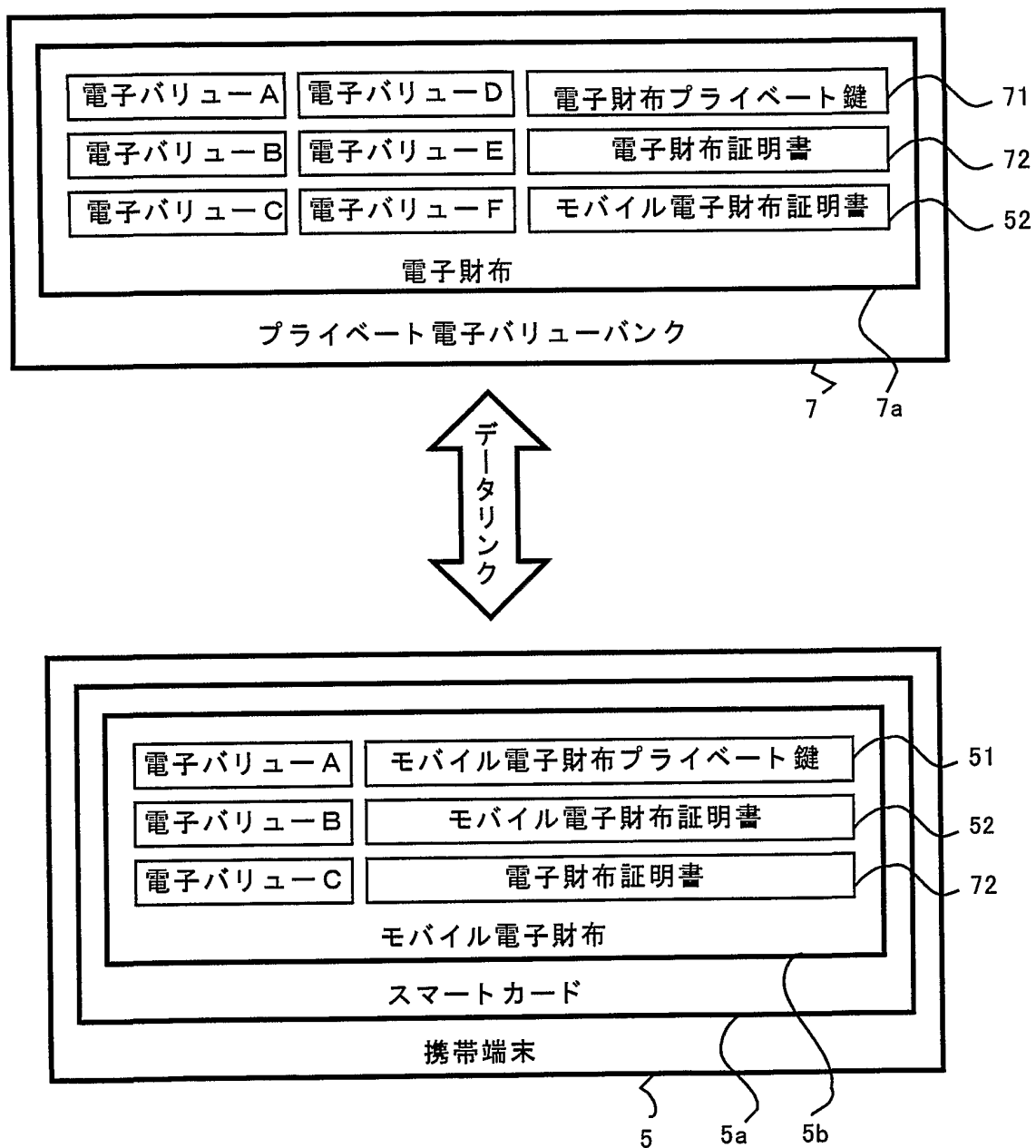


図 3

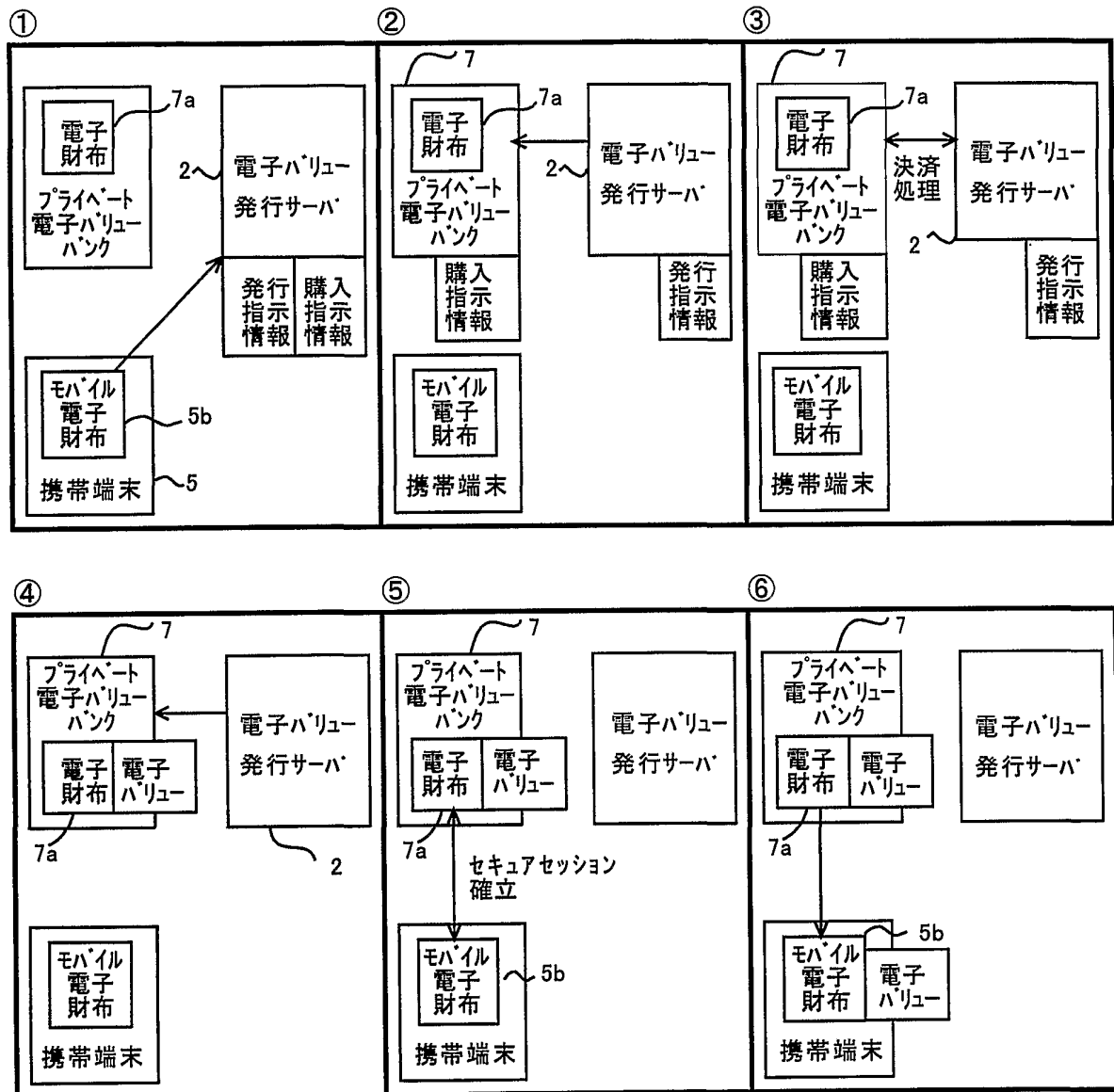


図 4

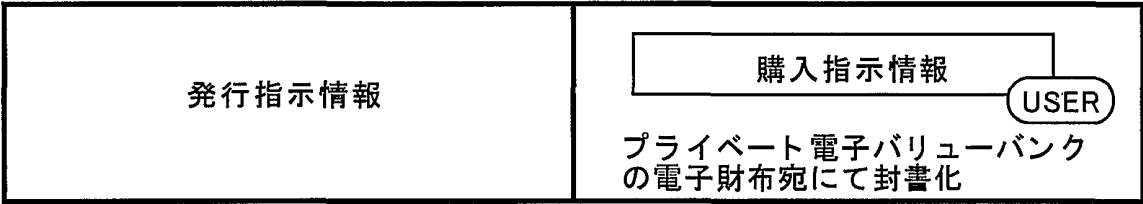


図 5

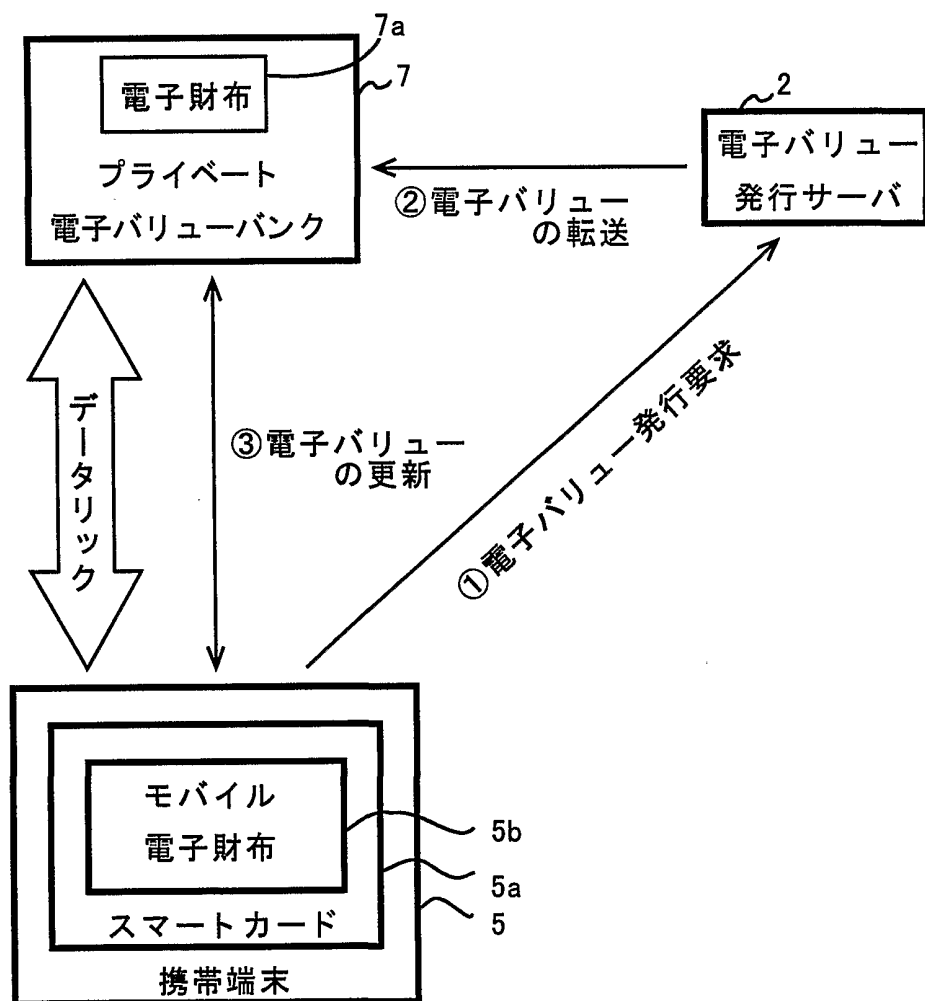


図 6

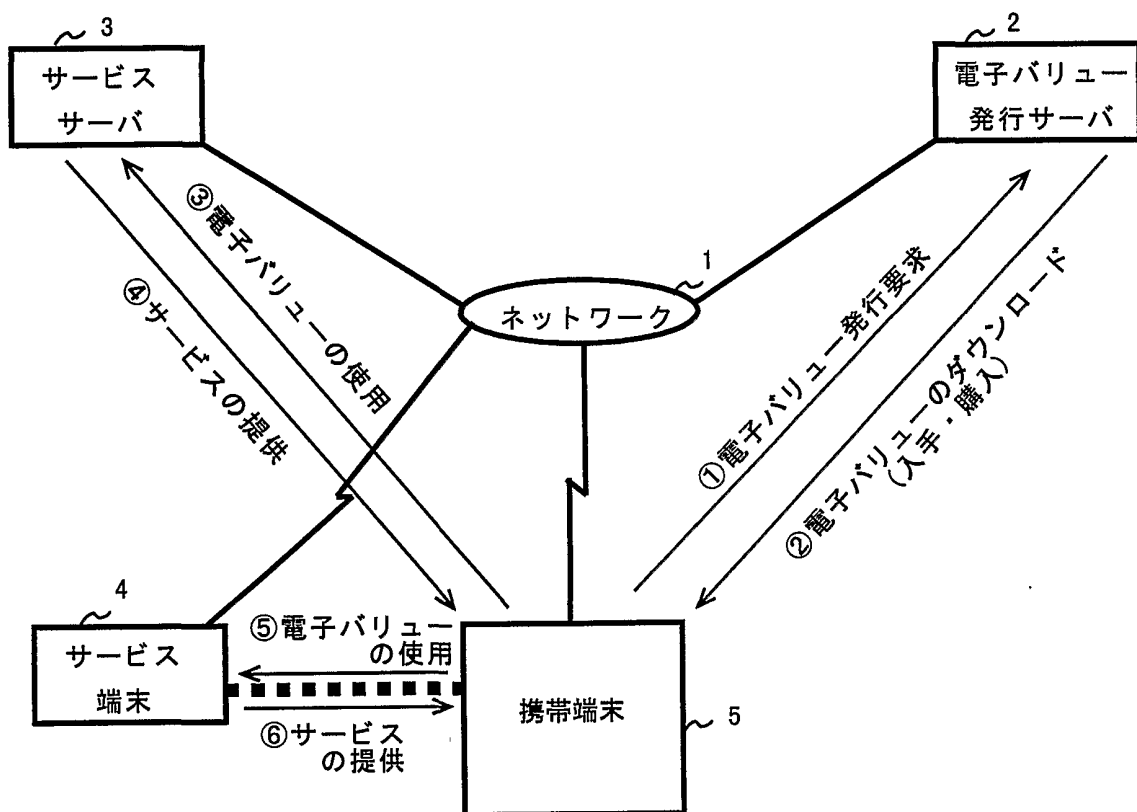


図 7

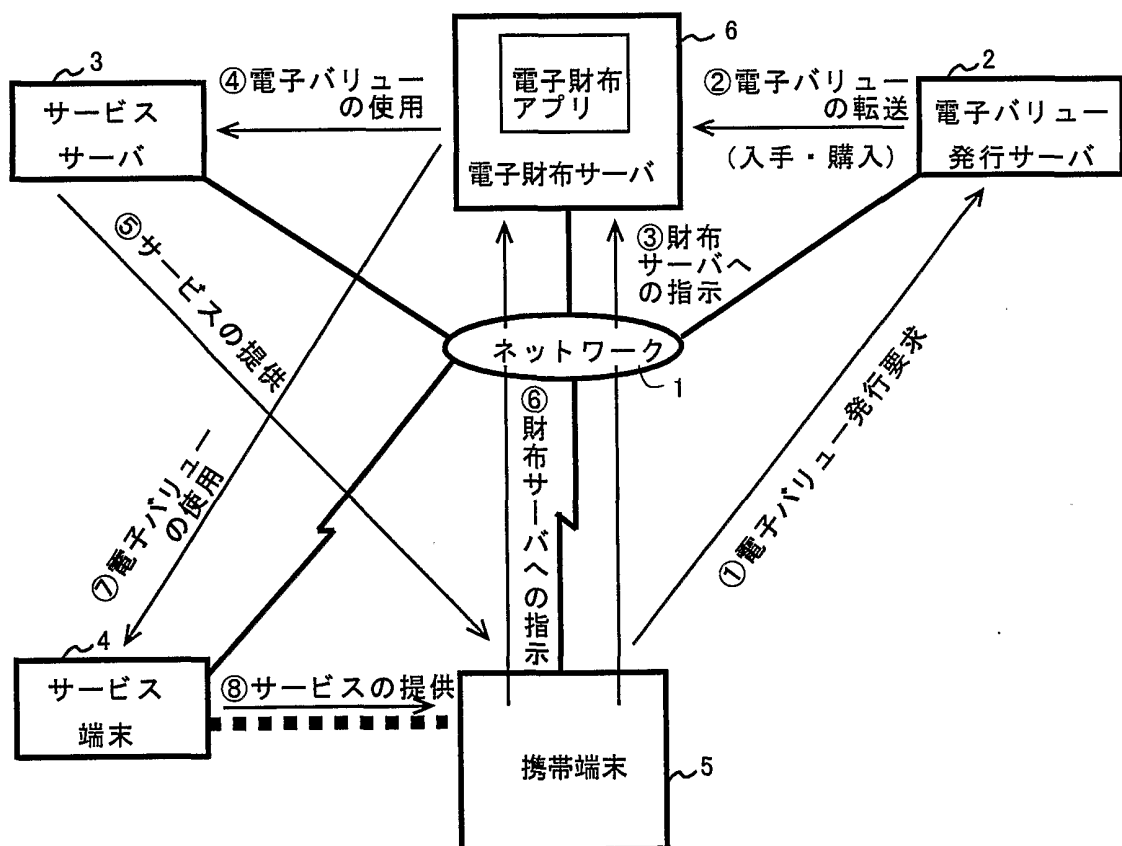


図 8

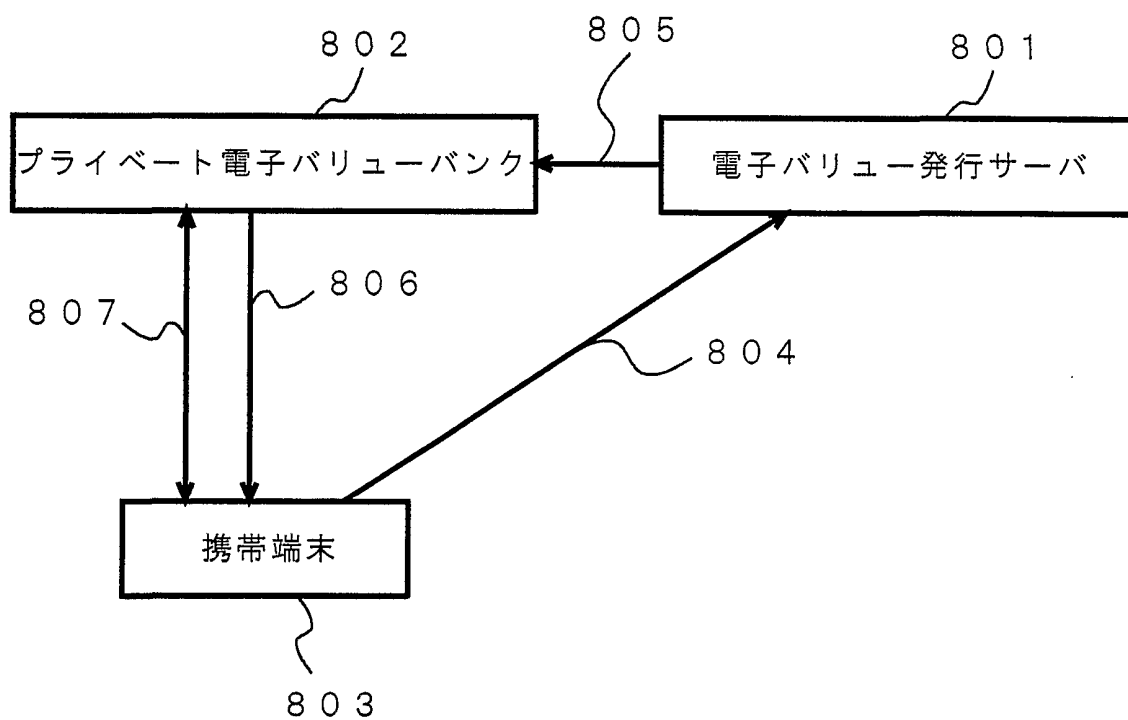


図 9

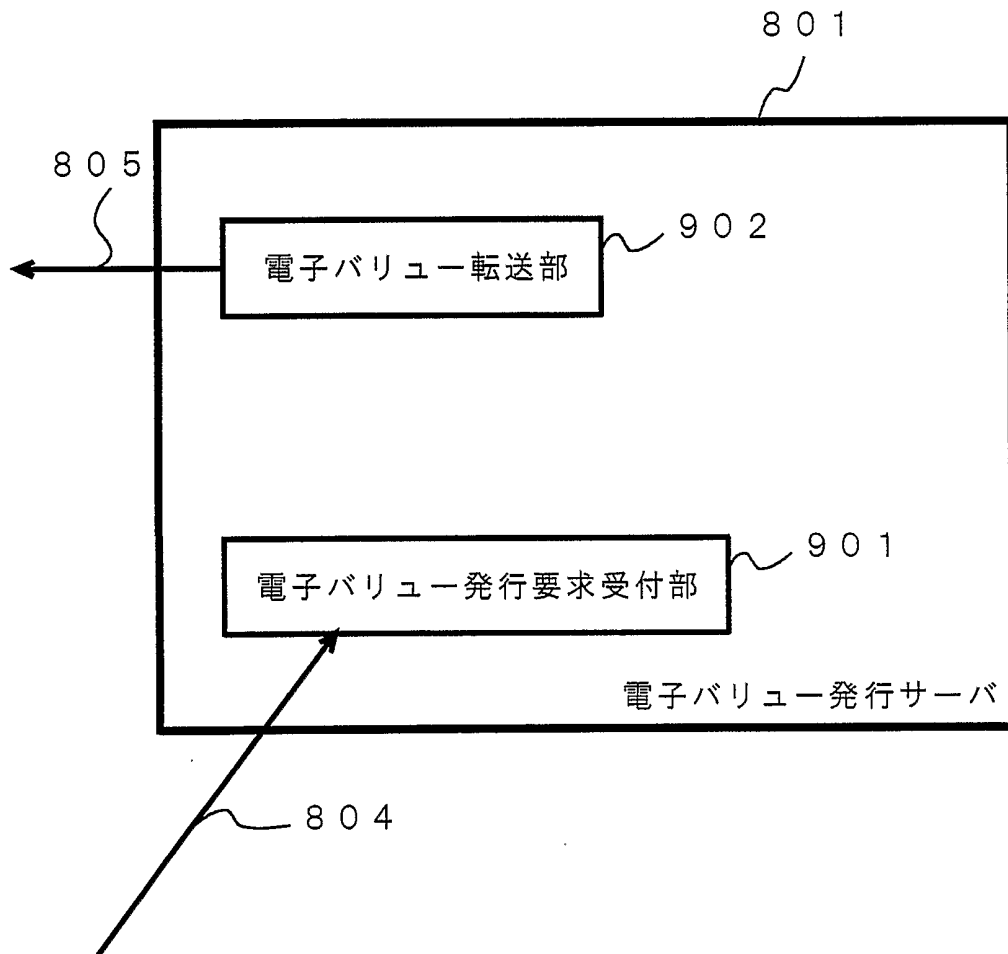


図 10

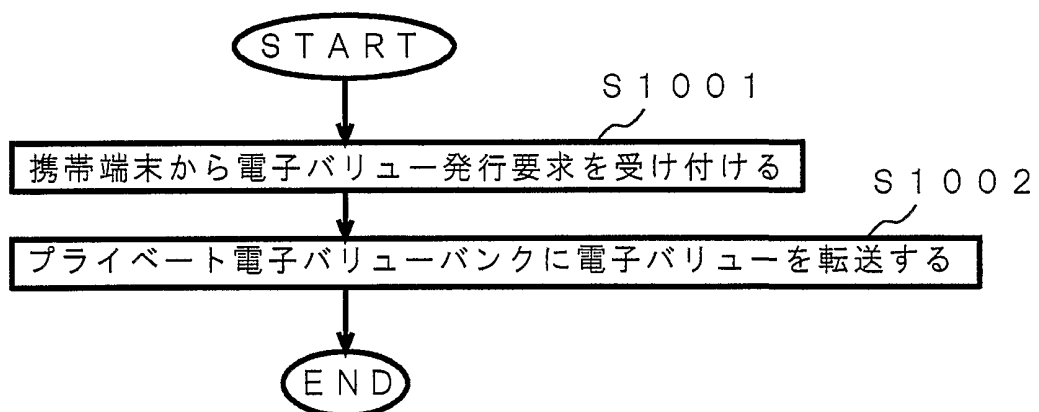


図 1 1

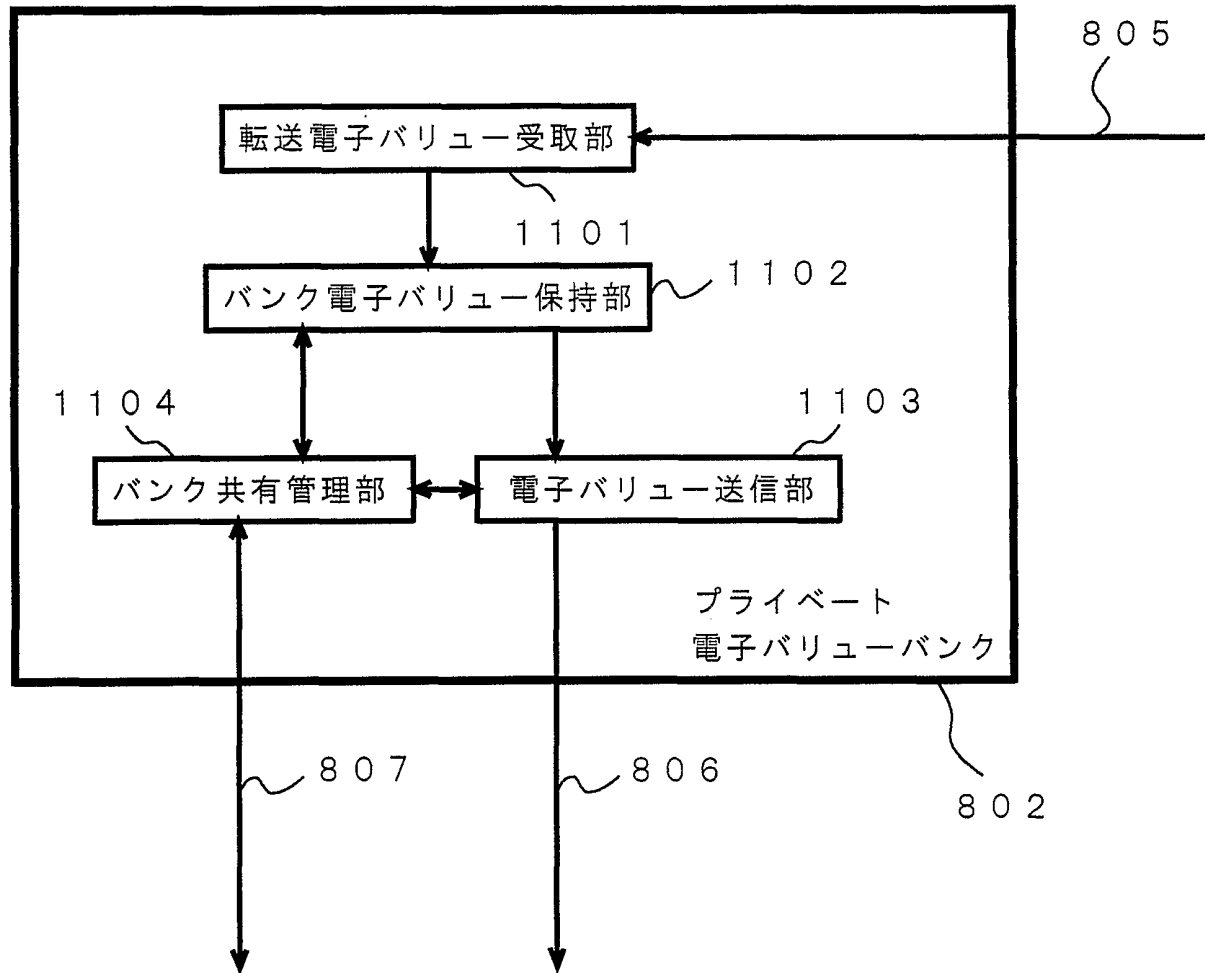


図 1 2

1 2 0 1		1 2 0 2	
電子バリュー A		非共有	
電子バリュー B		共有	
電子バリュー C		共有	
⋮		⋮	

1 2 0 0

図 1 3

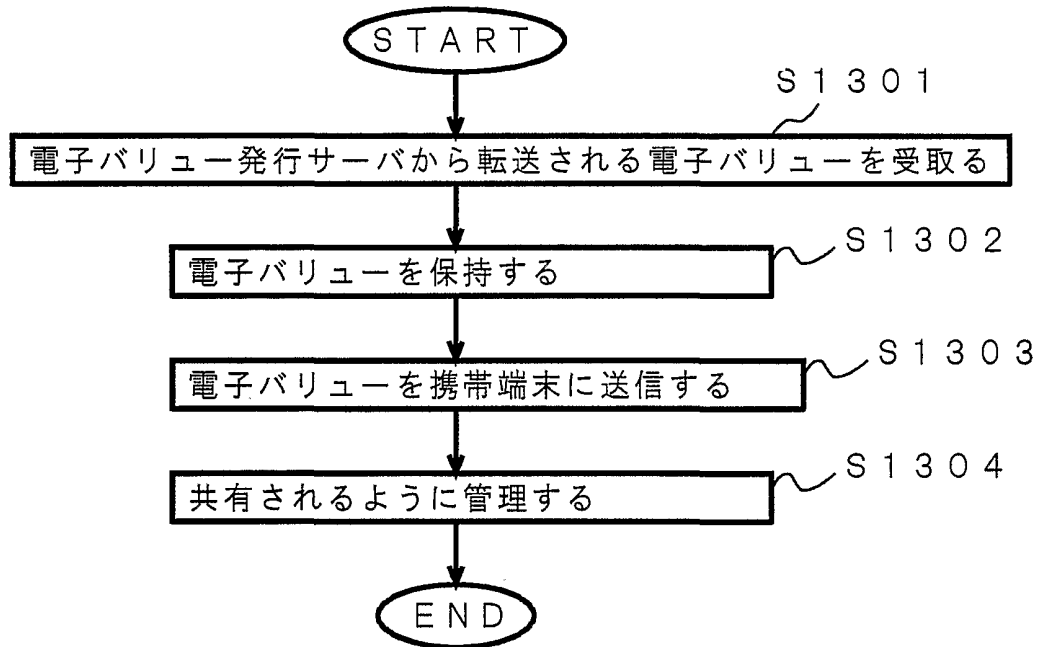


図 1 4

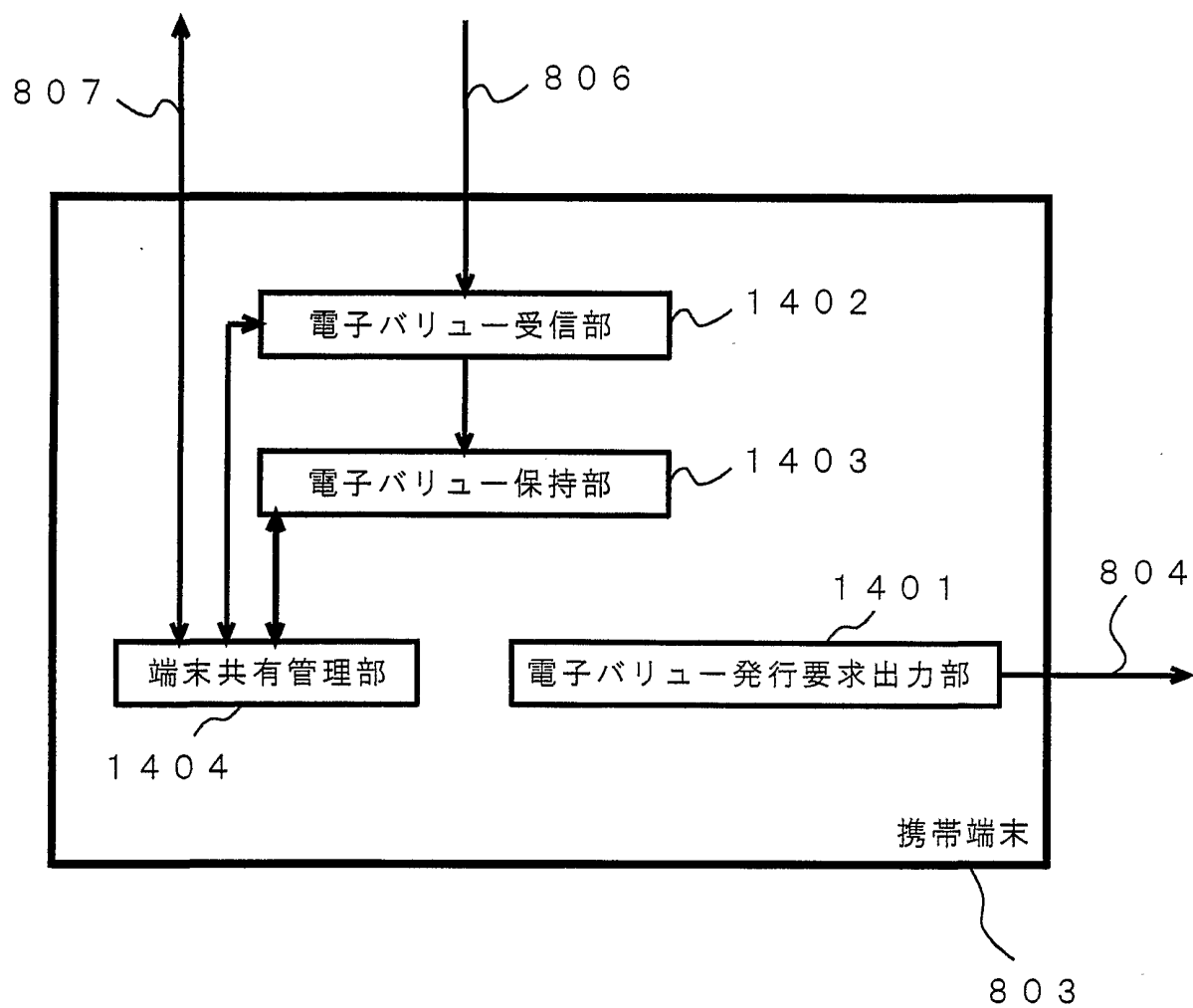


図 1 5

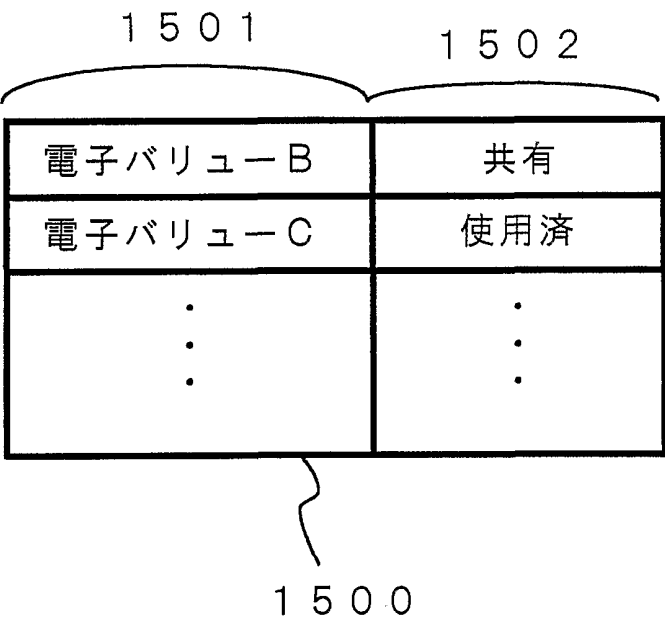


図 16

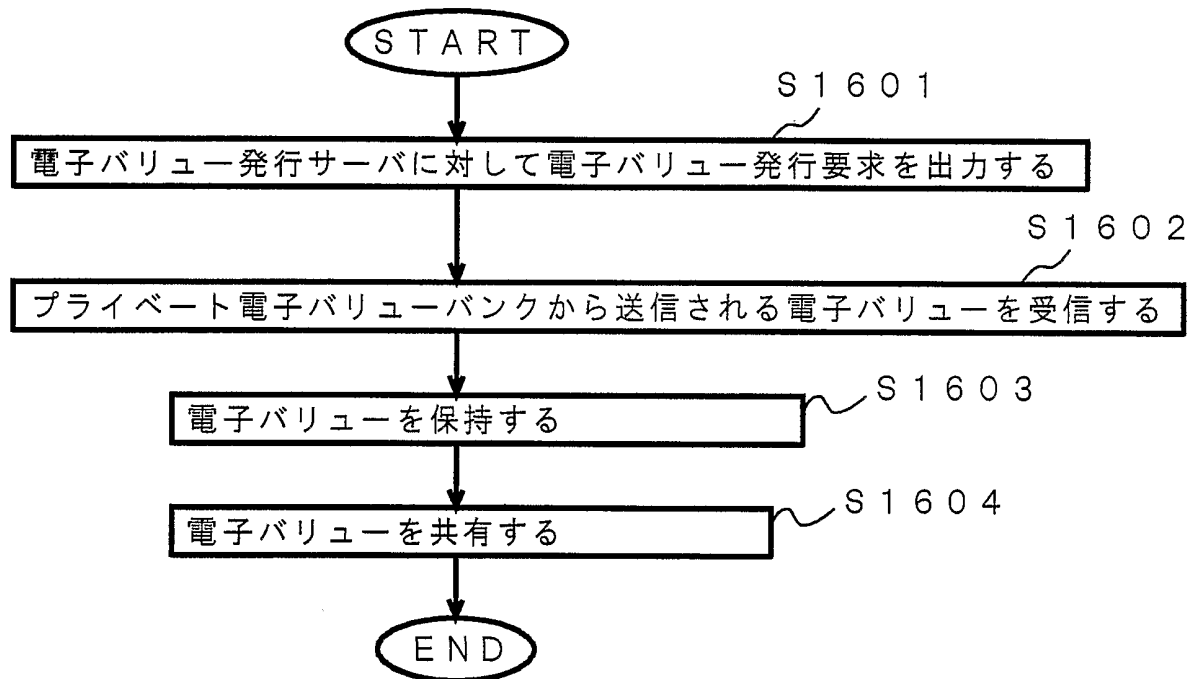


図 17

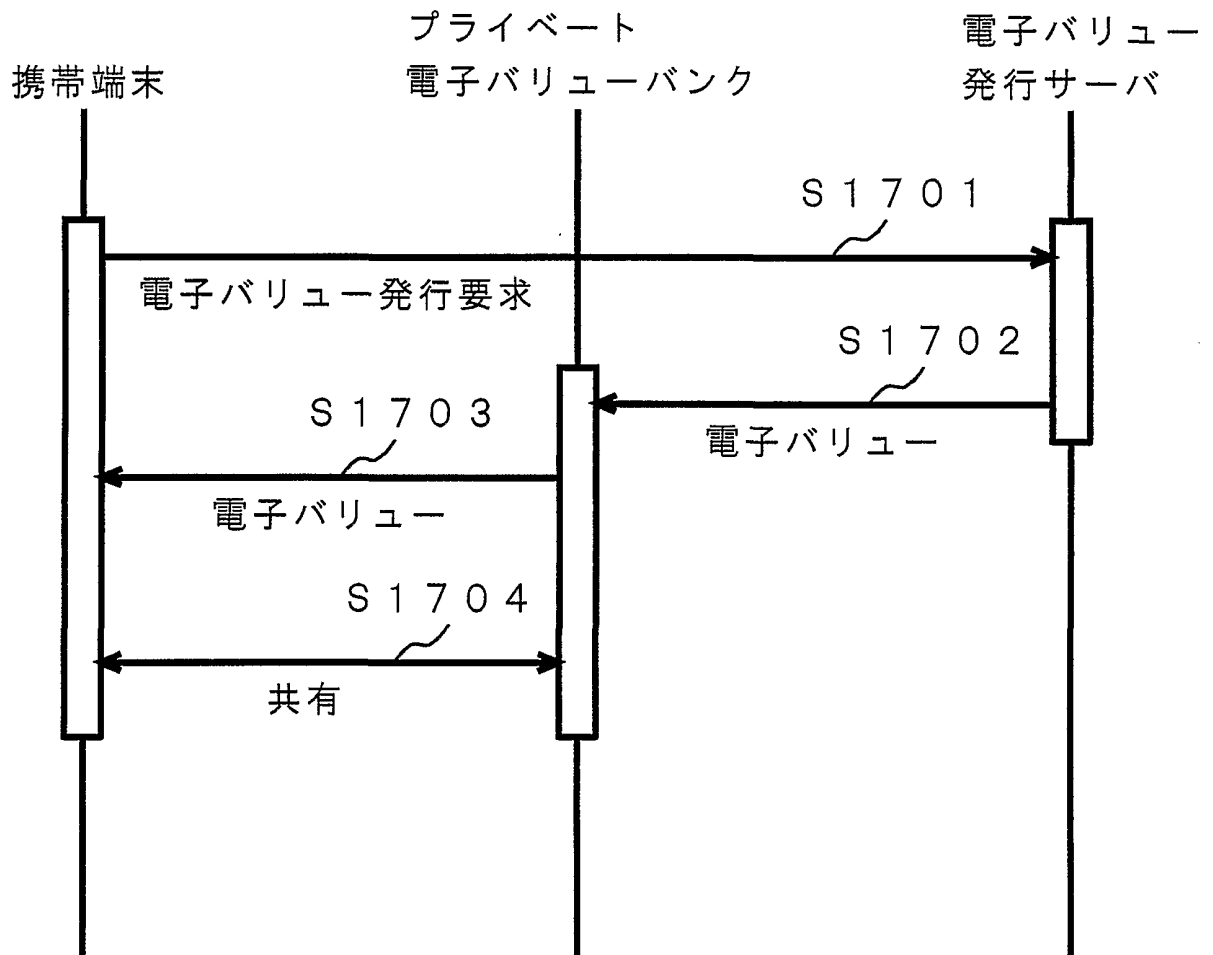


図 18

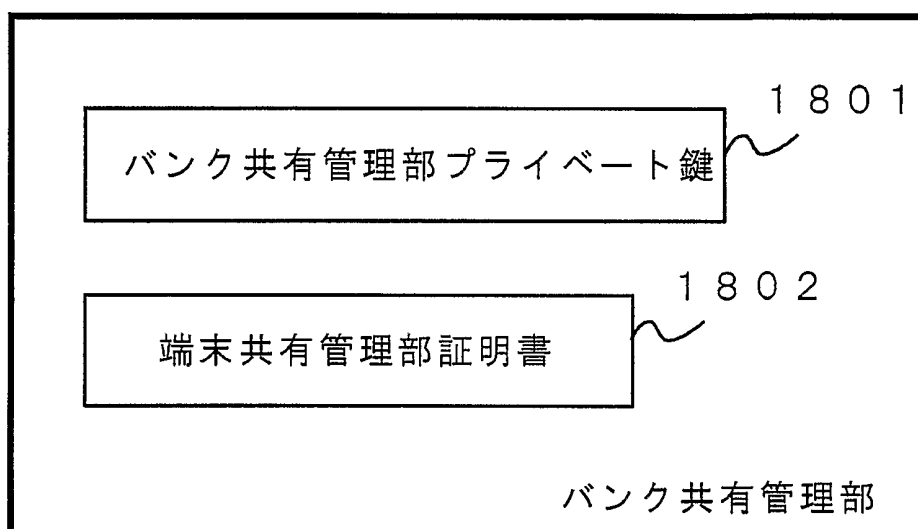


図 19

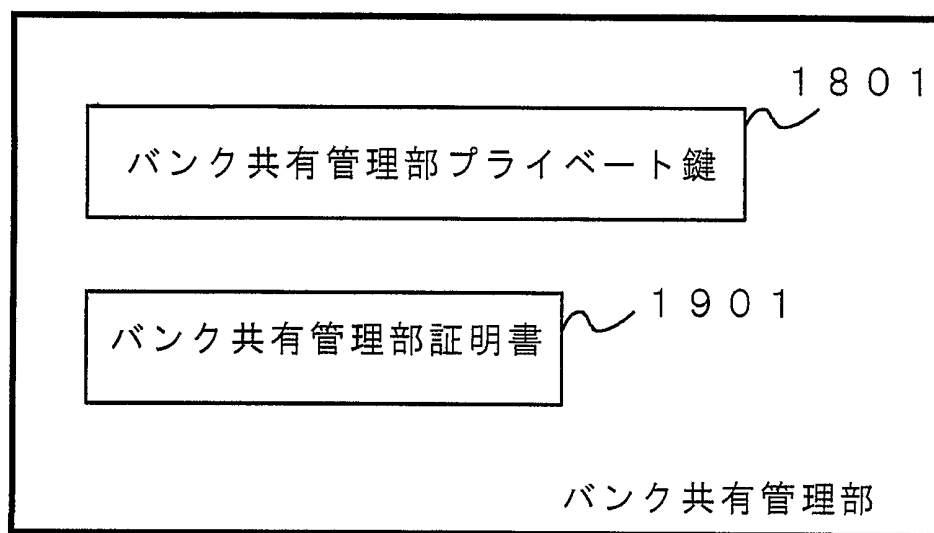


図 20

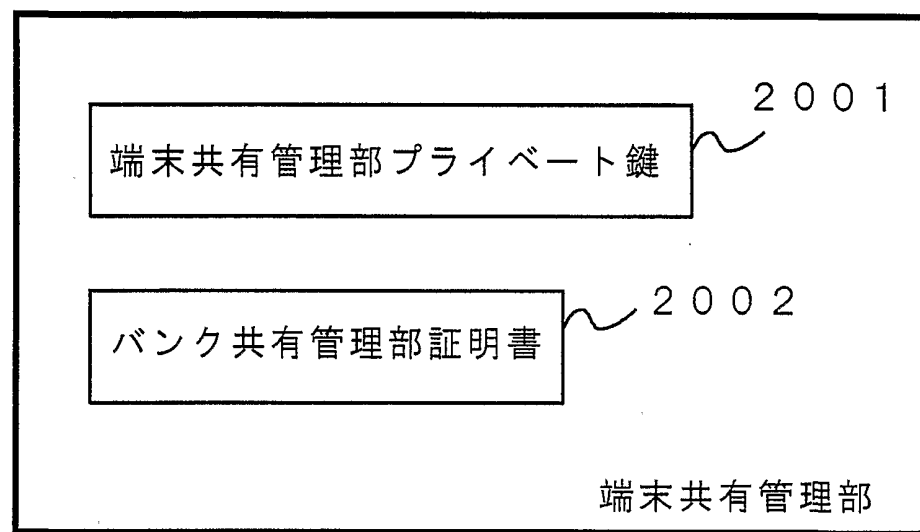


図 2 1

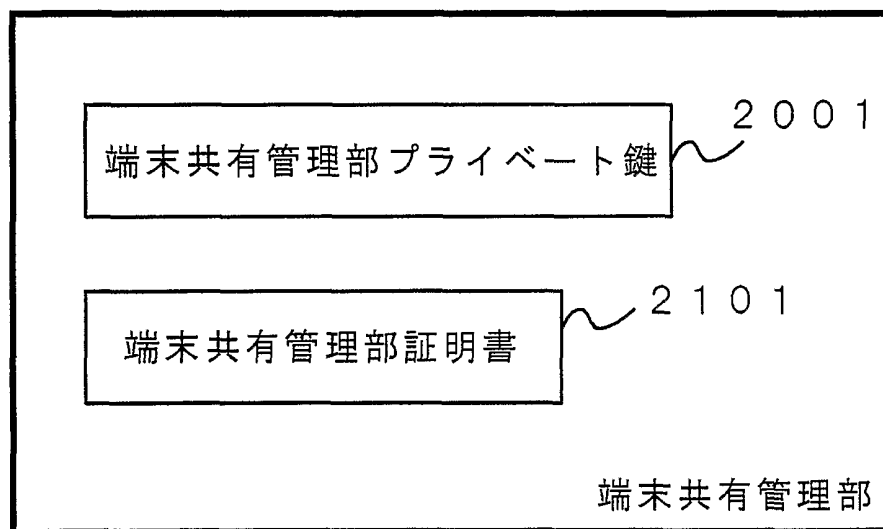


図 2 2

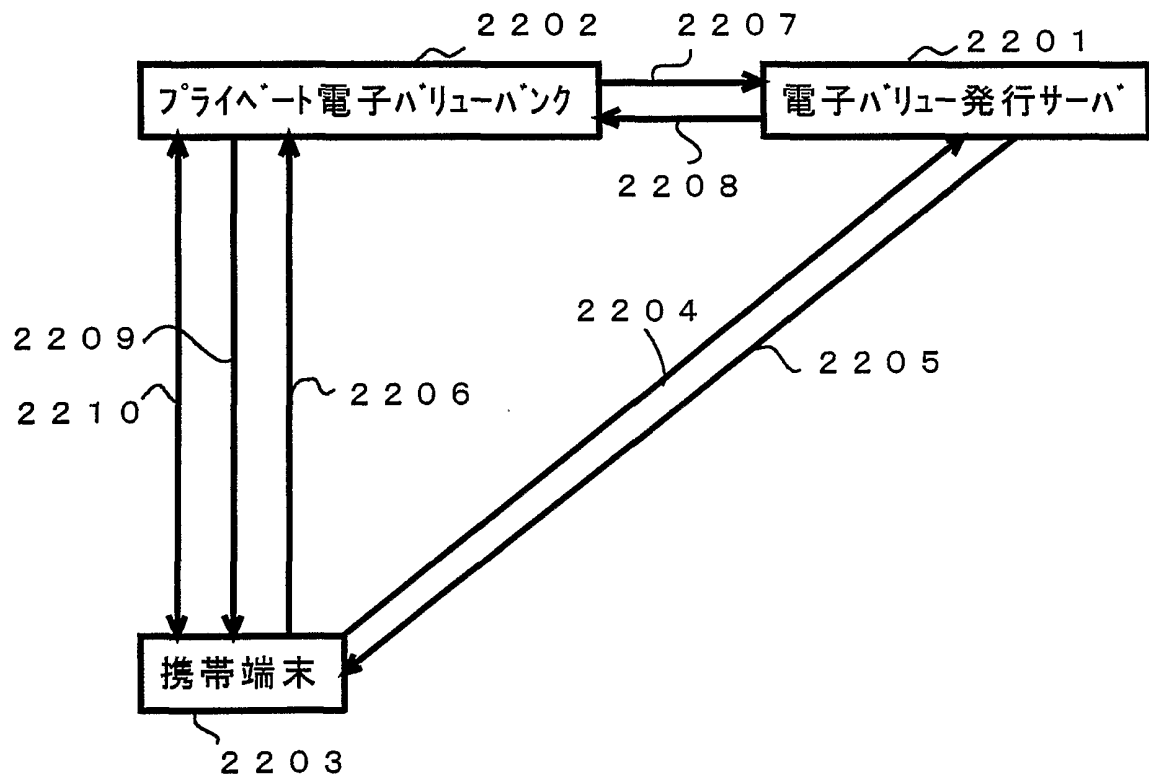


図 23

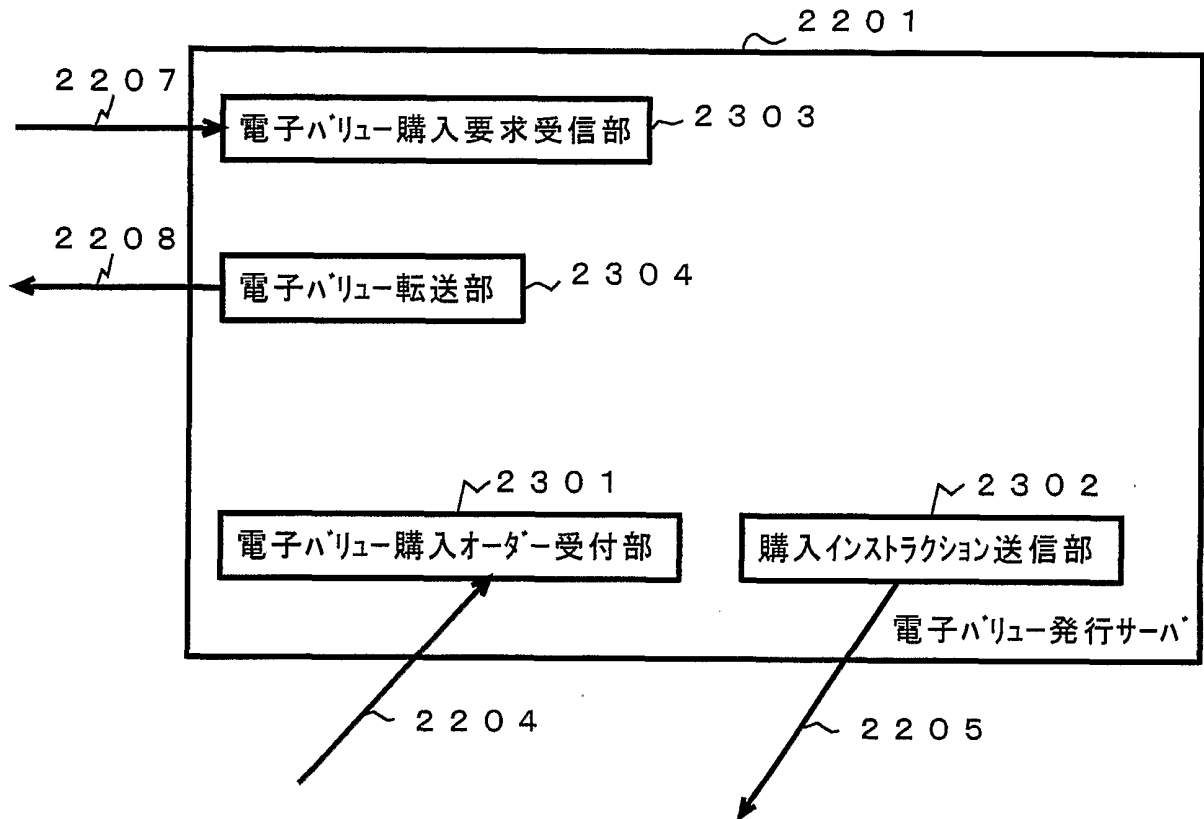


図 2 4

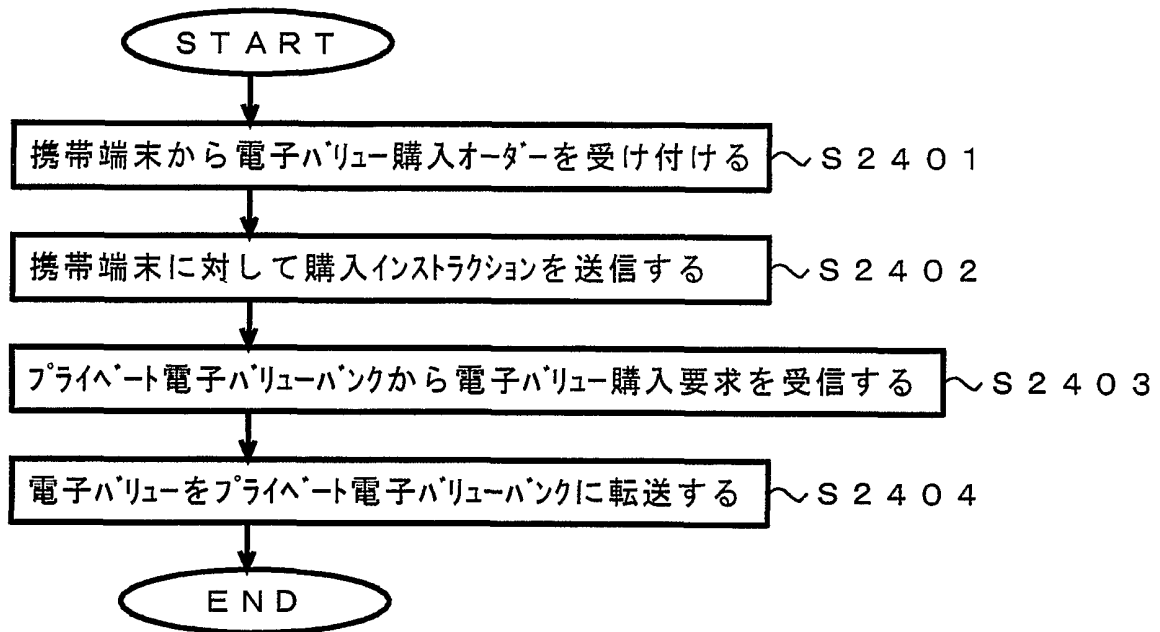


図 2 5

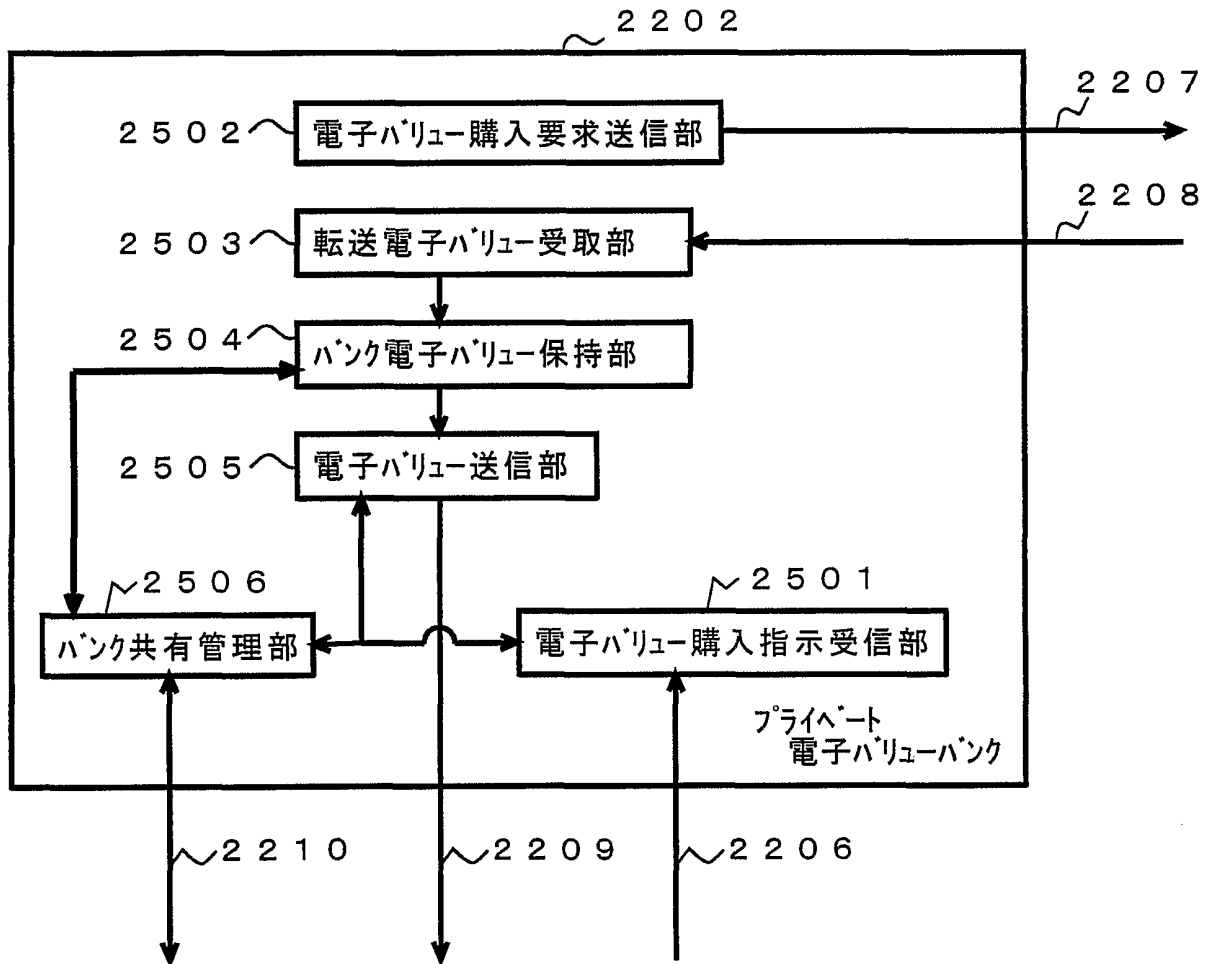
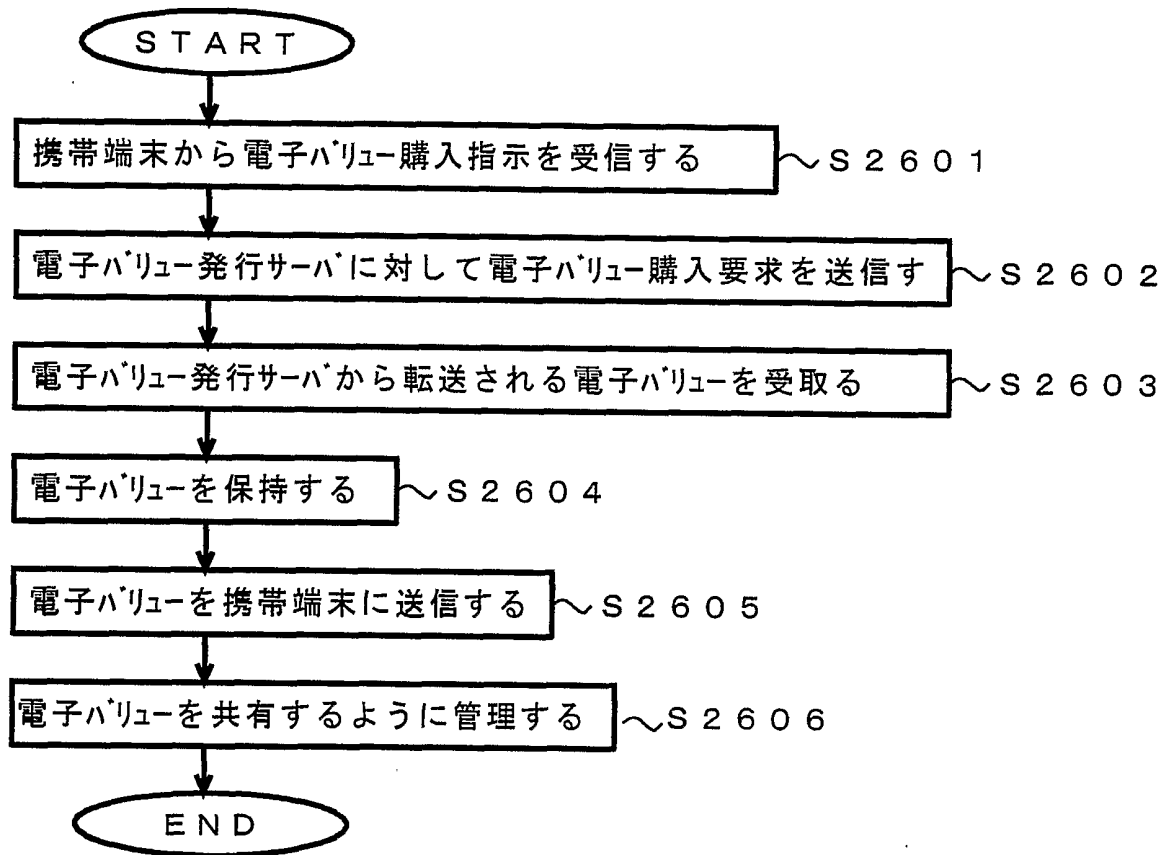


図 2 6



27/86

図 27

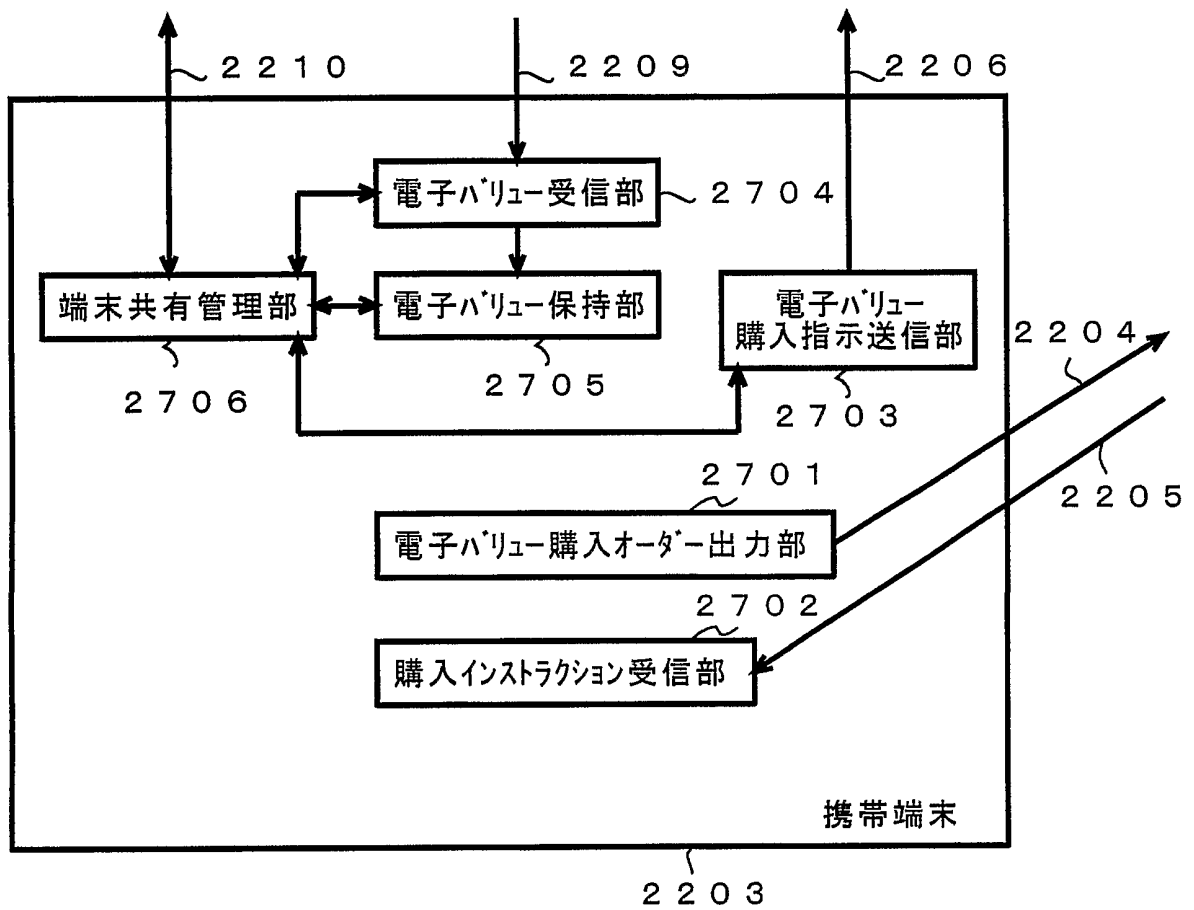


図 28

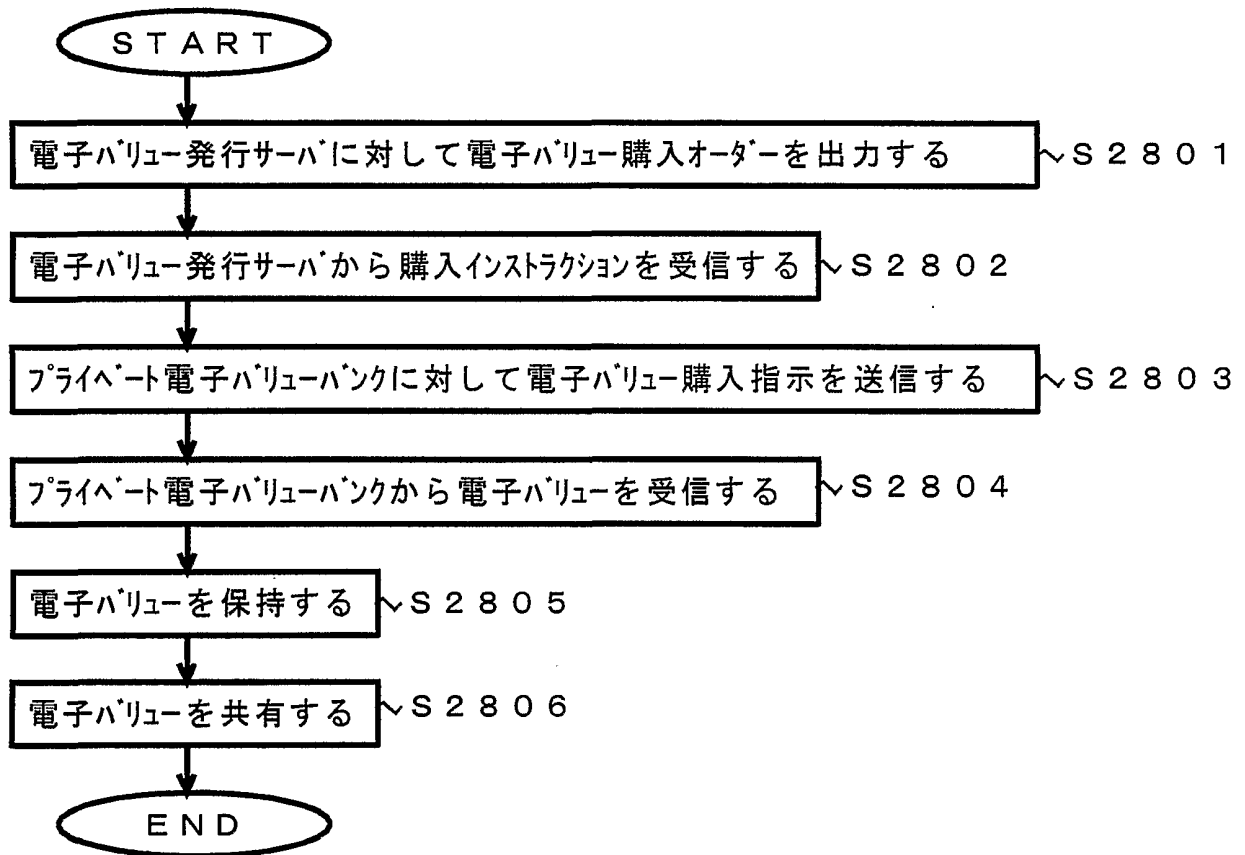


図 2 9

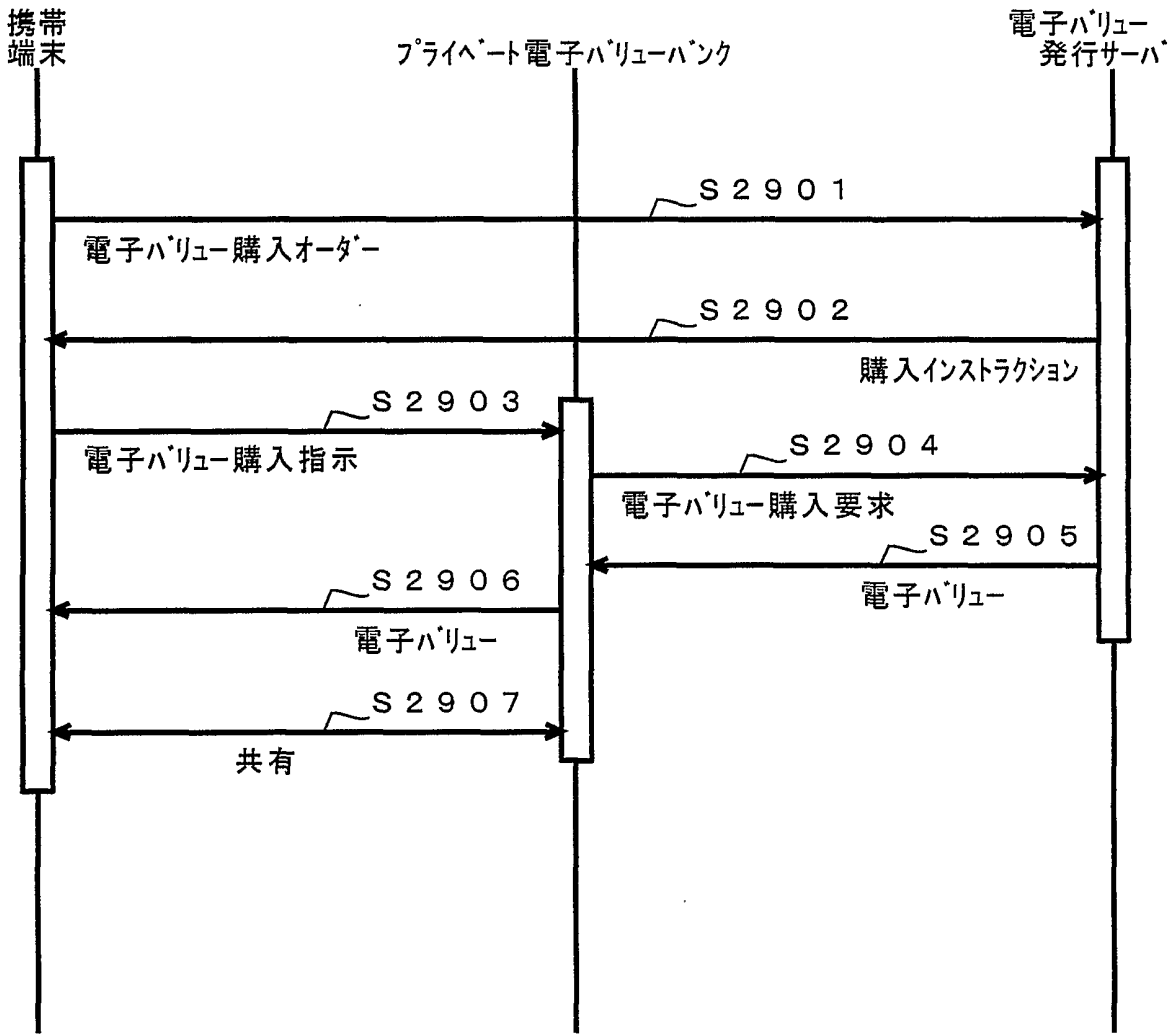


図 30

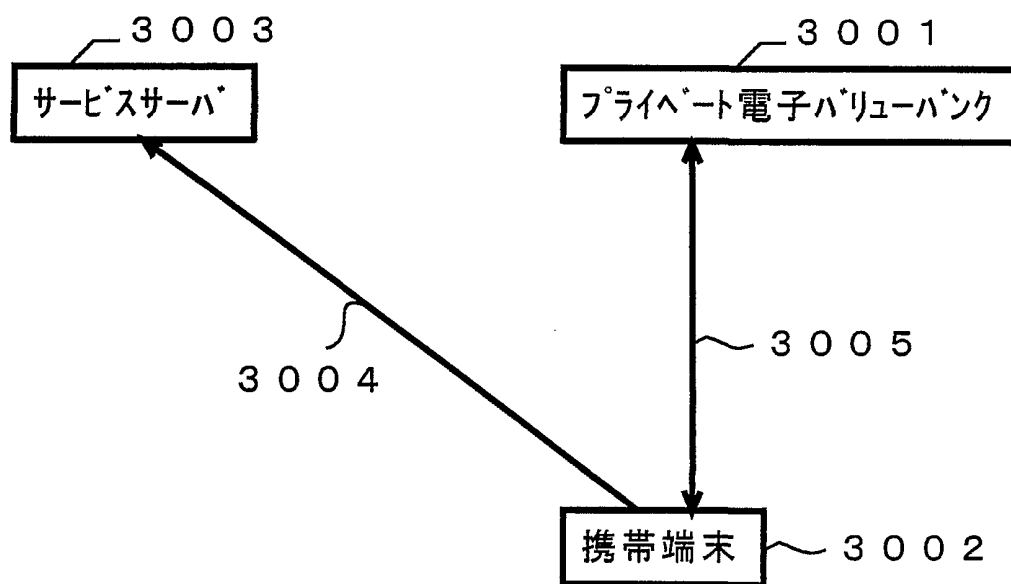


図 3 1

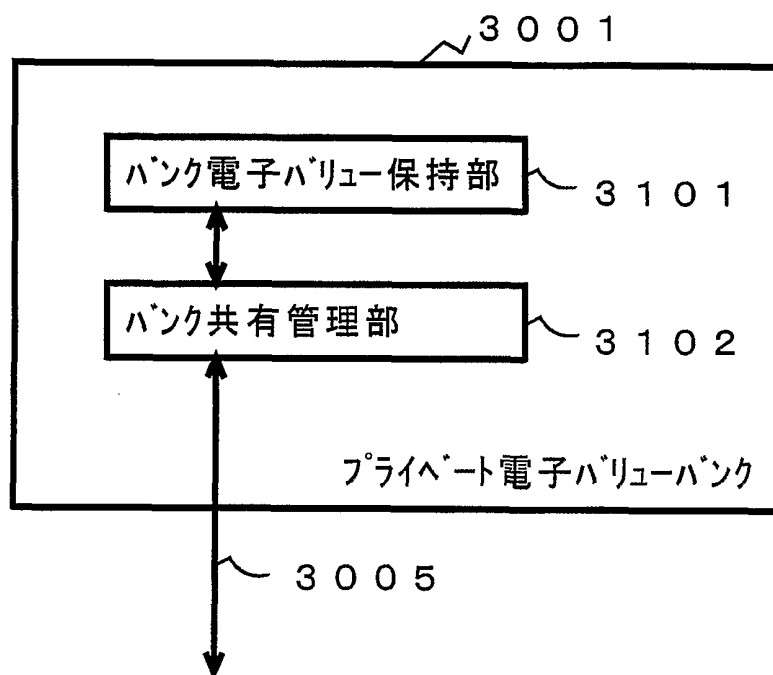


図 3 2

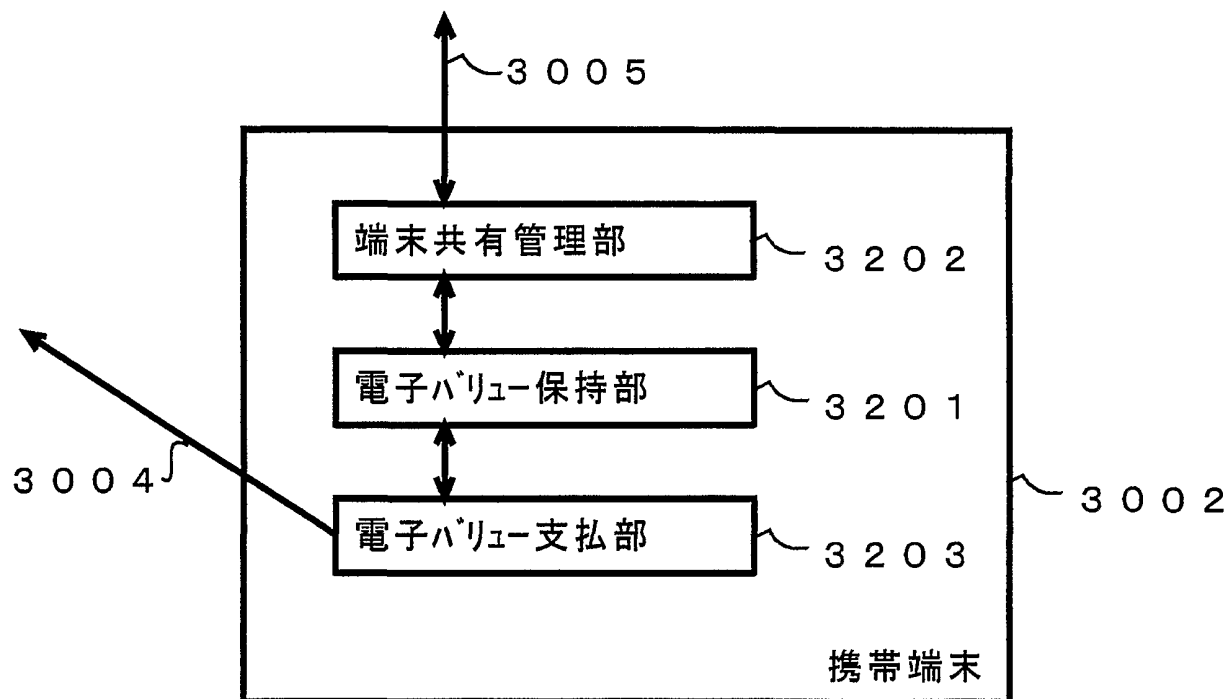


図 3 3

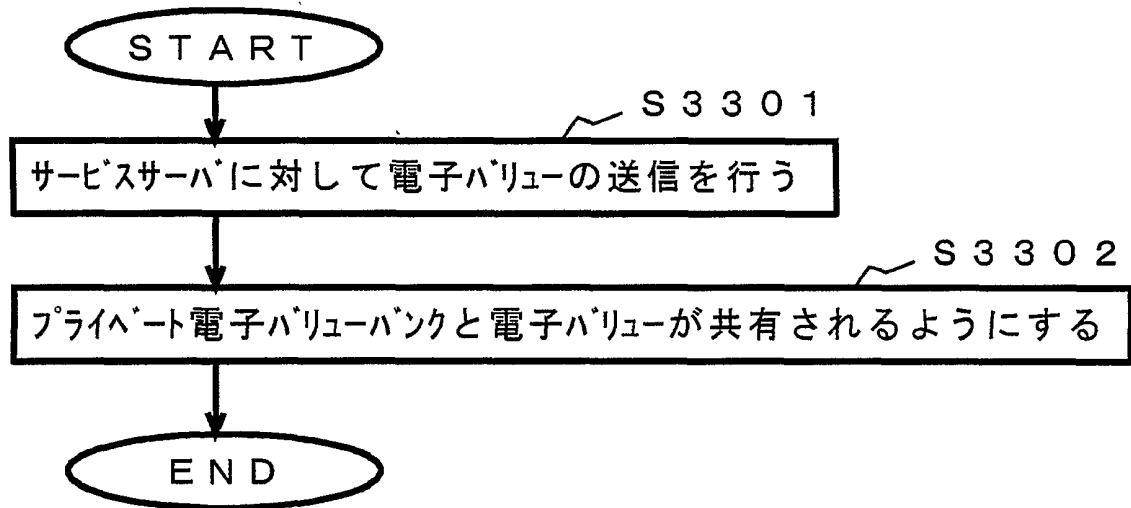


図 3 4

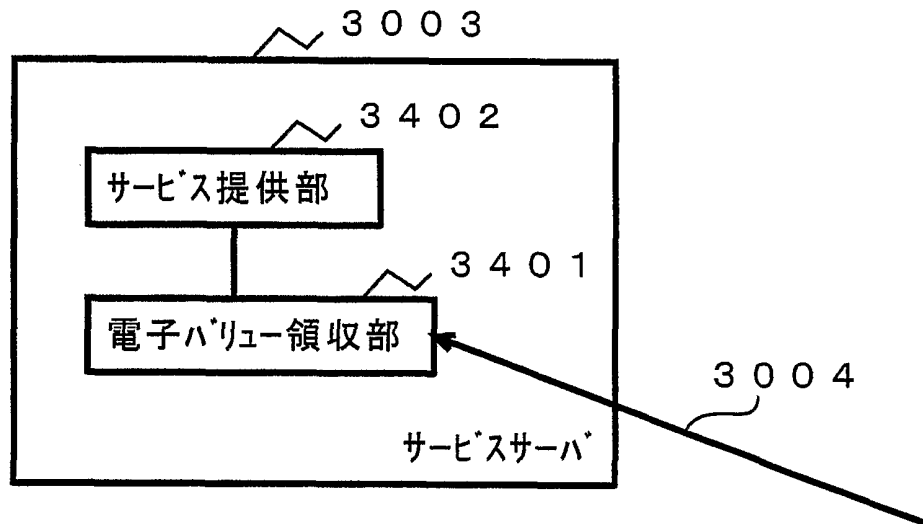


図 3 5

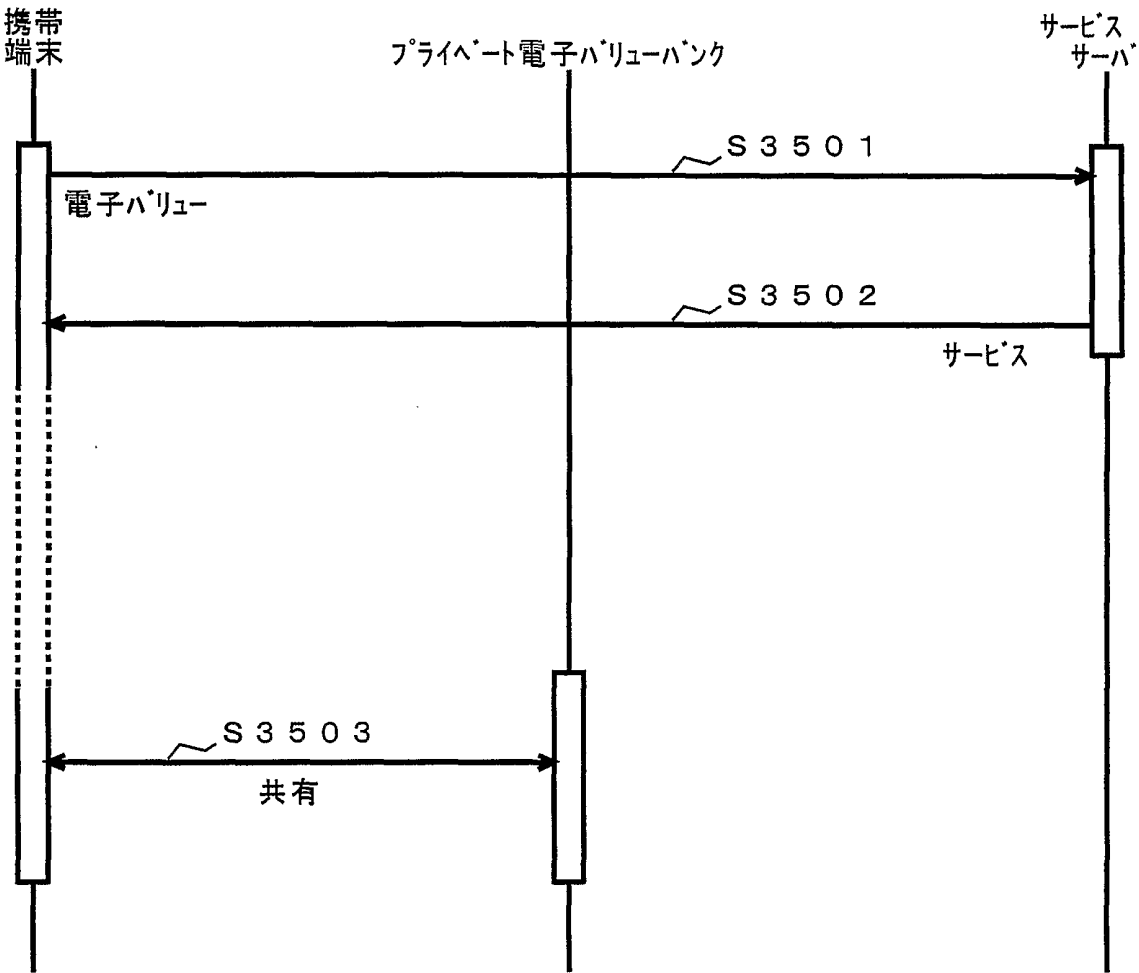


図 3 6

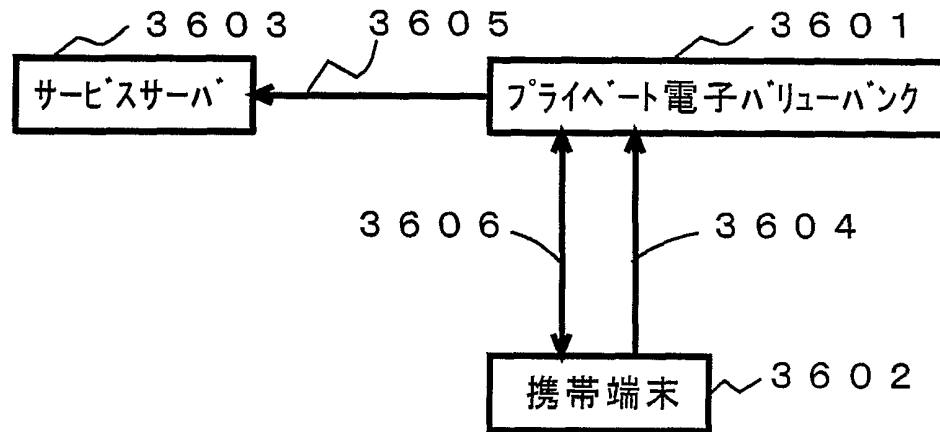
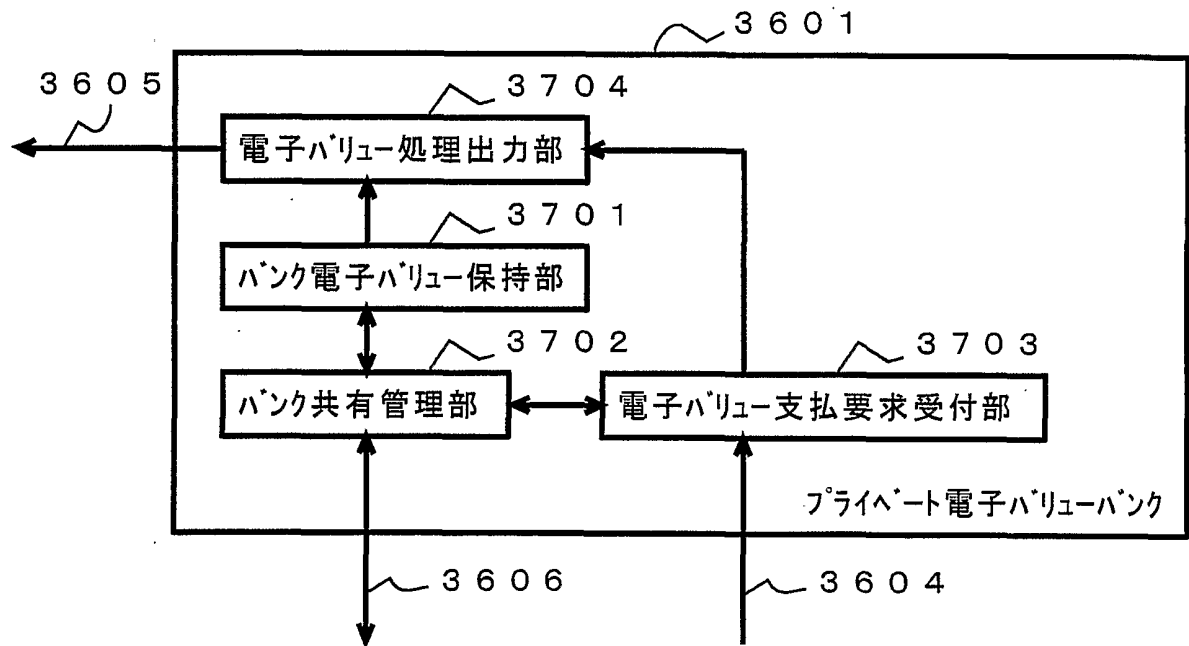


図 37



38/86

図 3 8

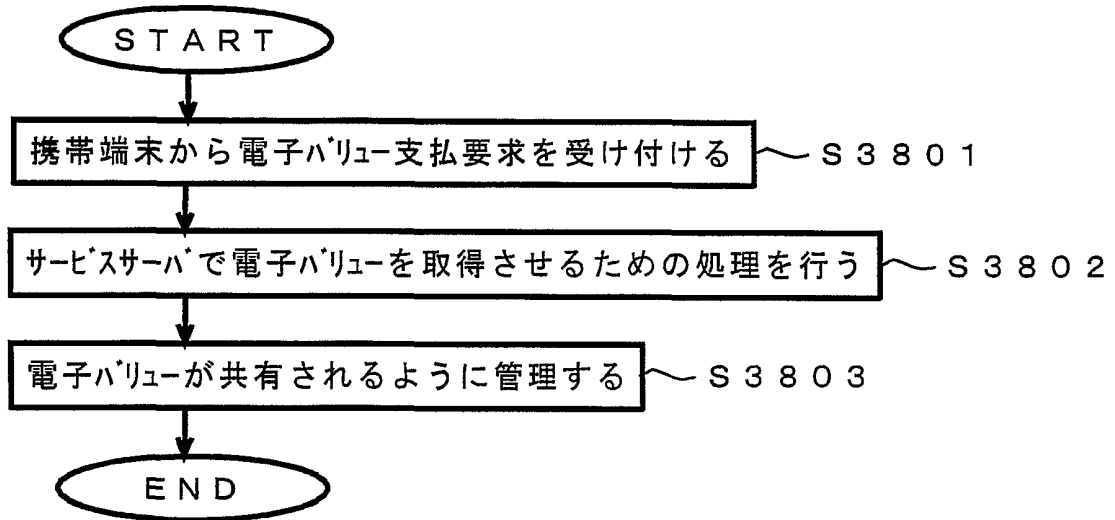


図 39

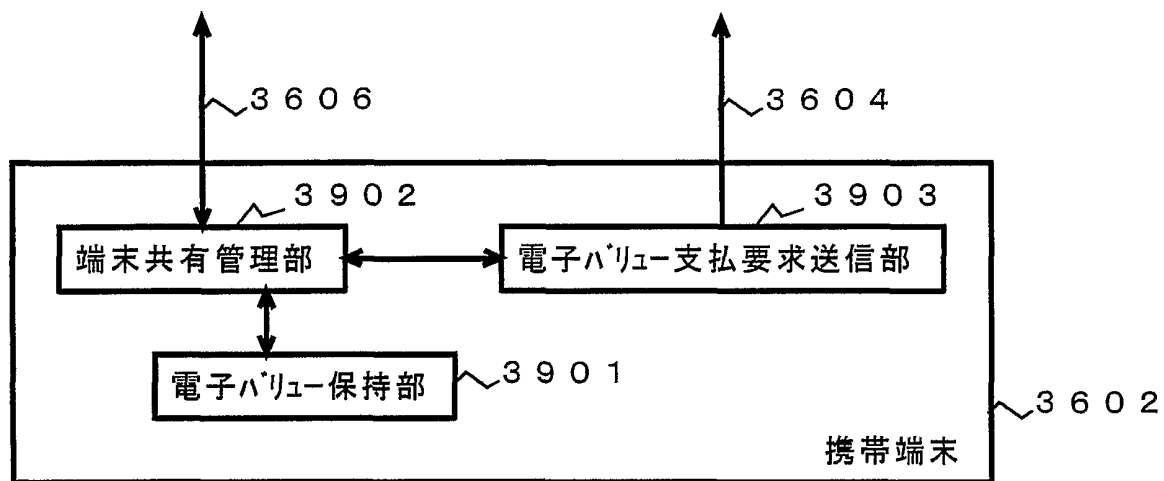


図 4 0

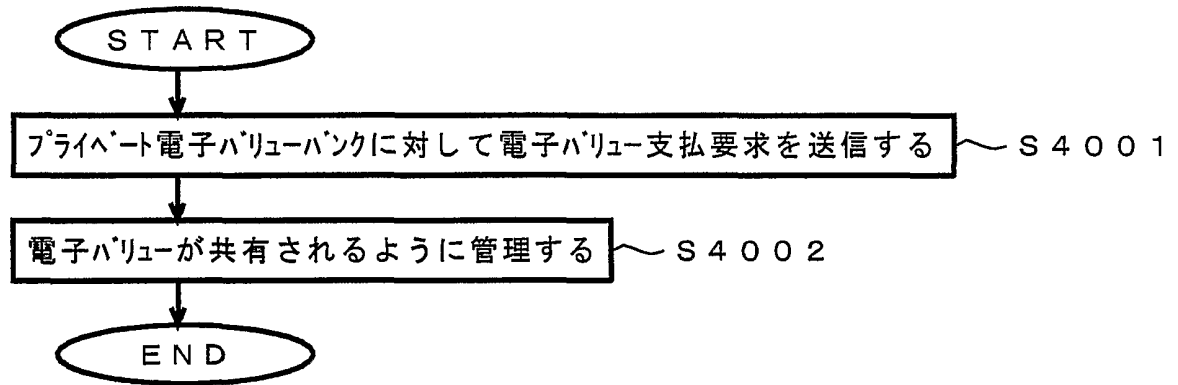


図 4 1

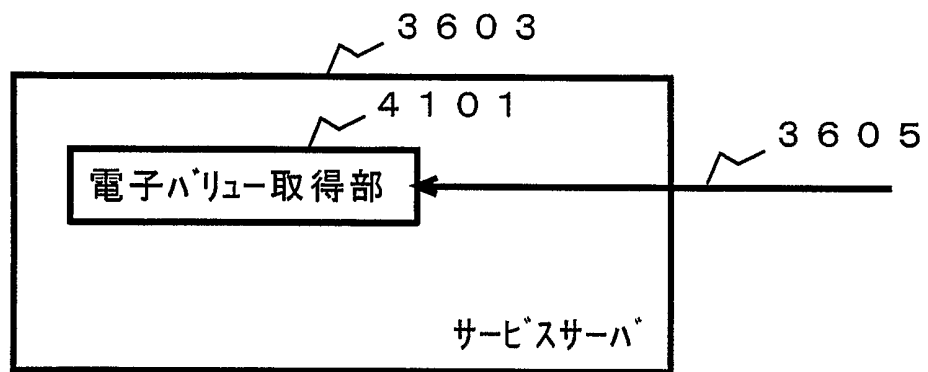


図 4 2

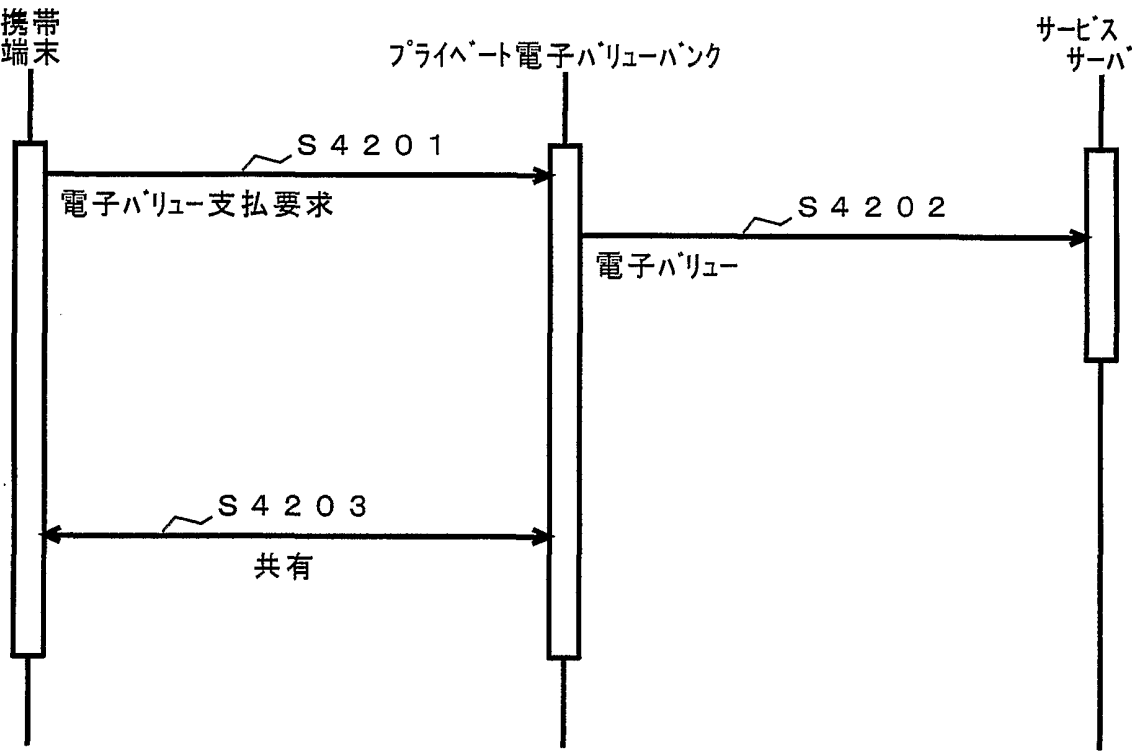


図 4 3

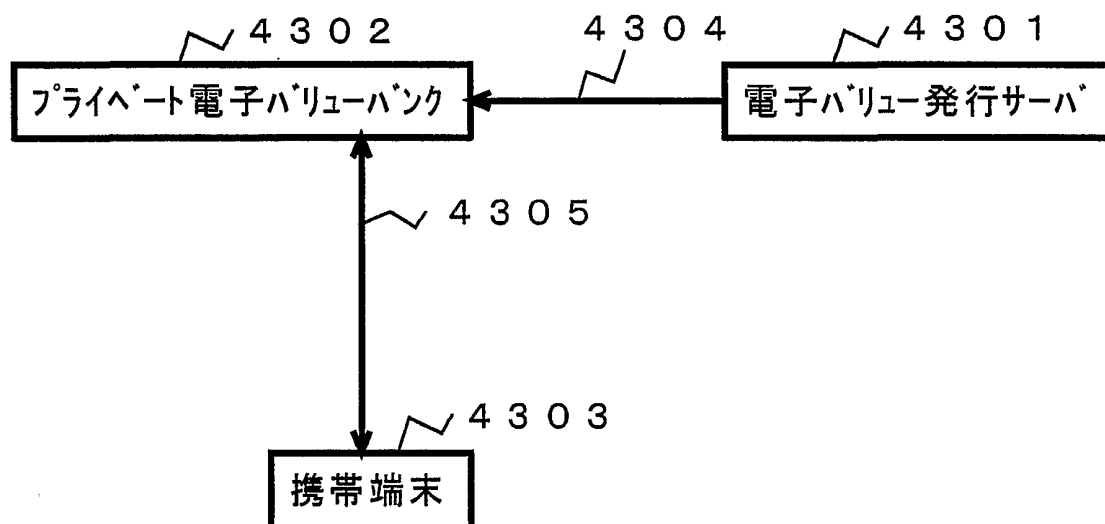


図 4 4

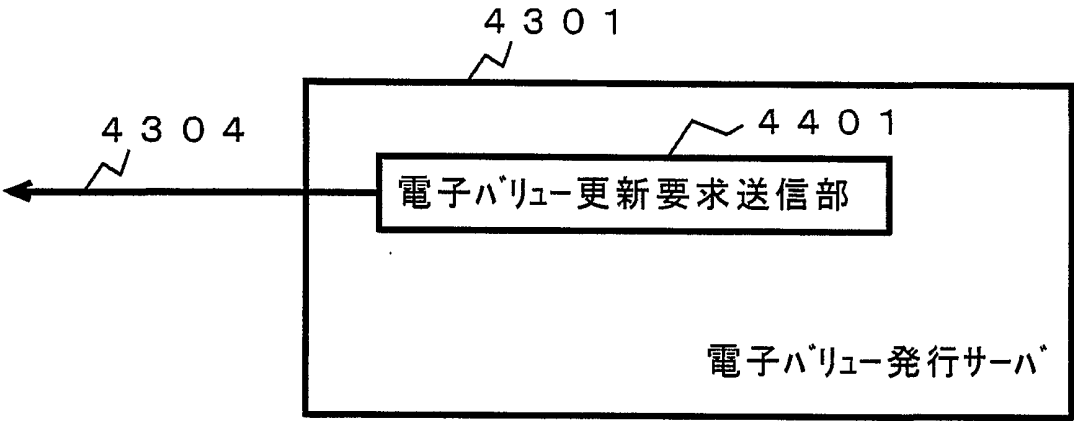


図 4 5

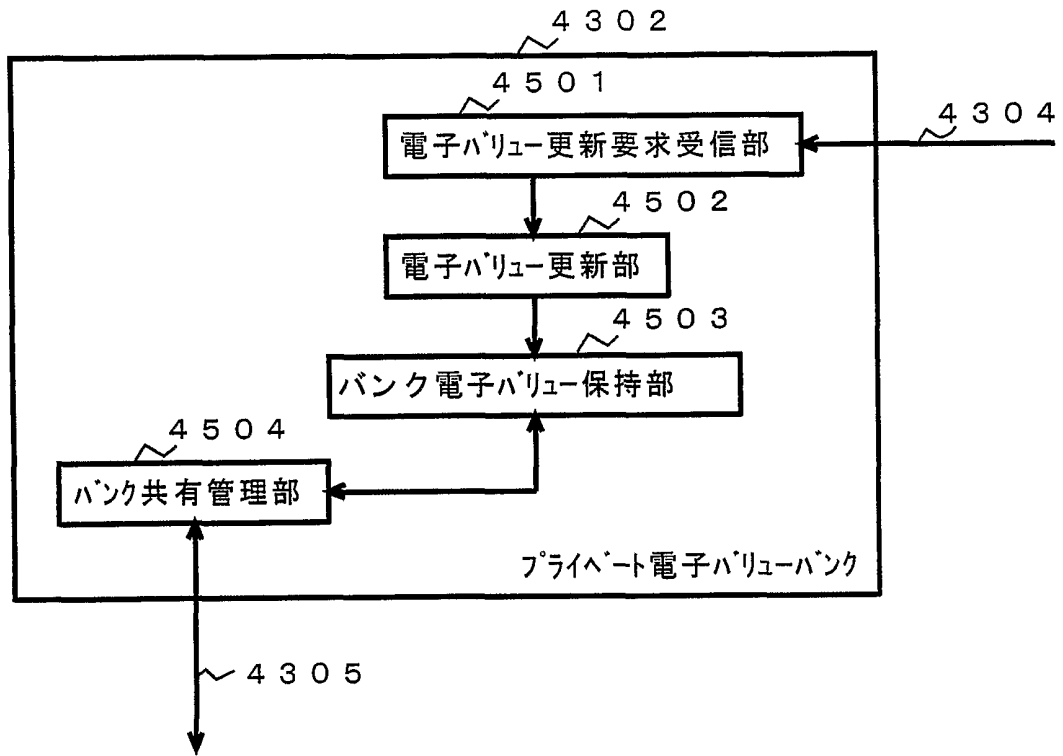


図 4 6

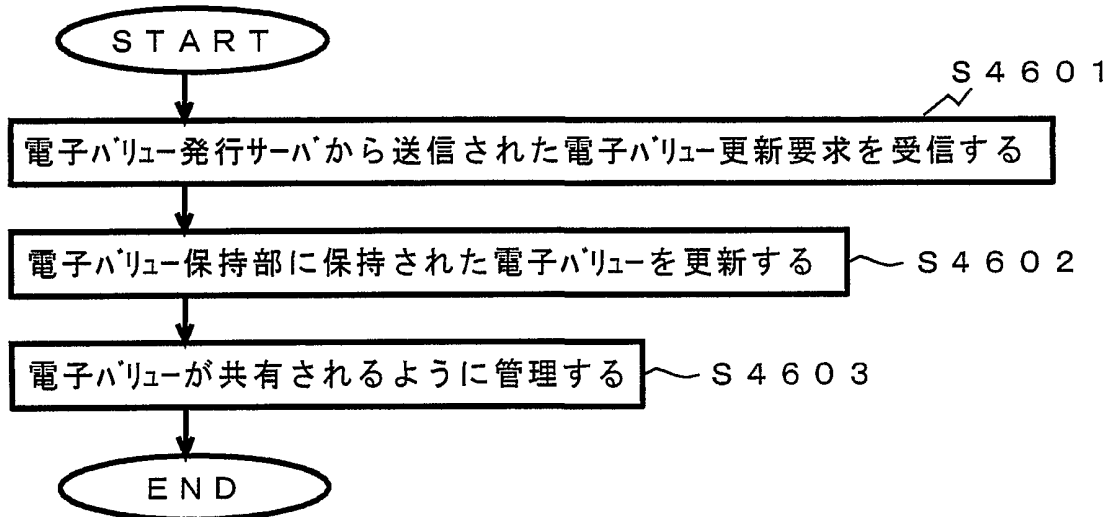


図 4 7

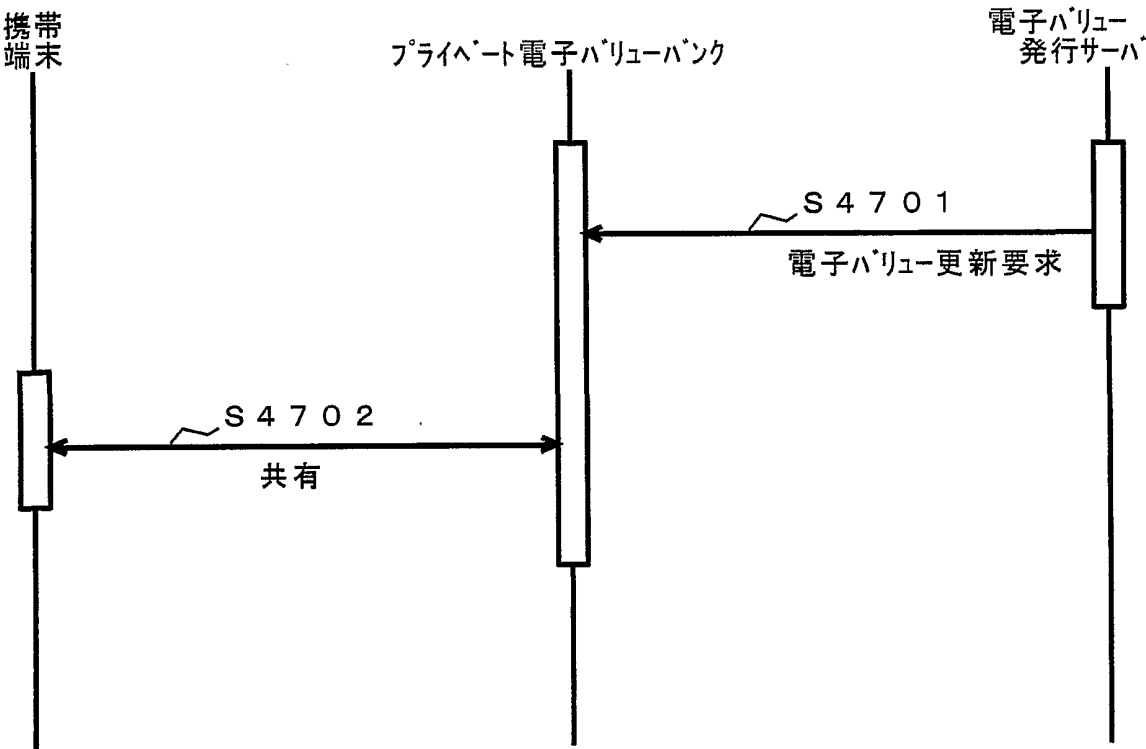


図 4 8

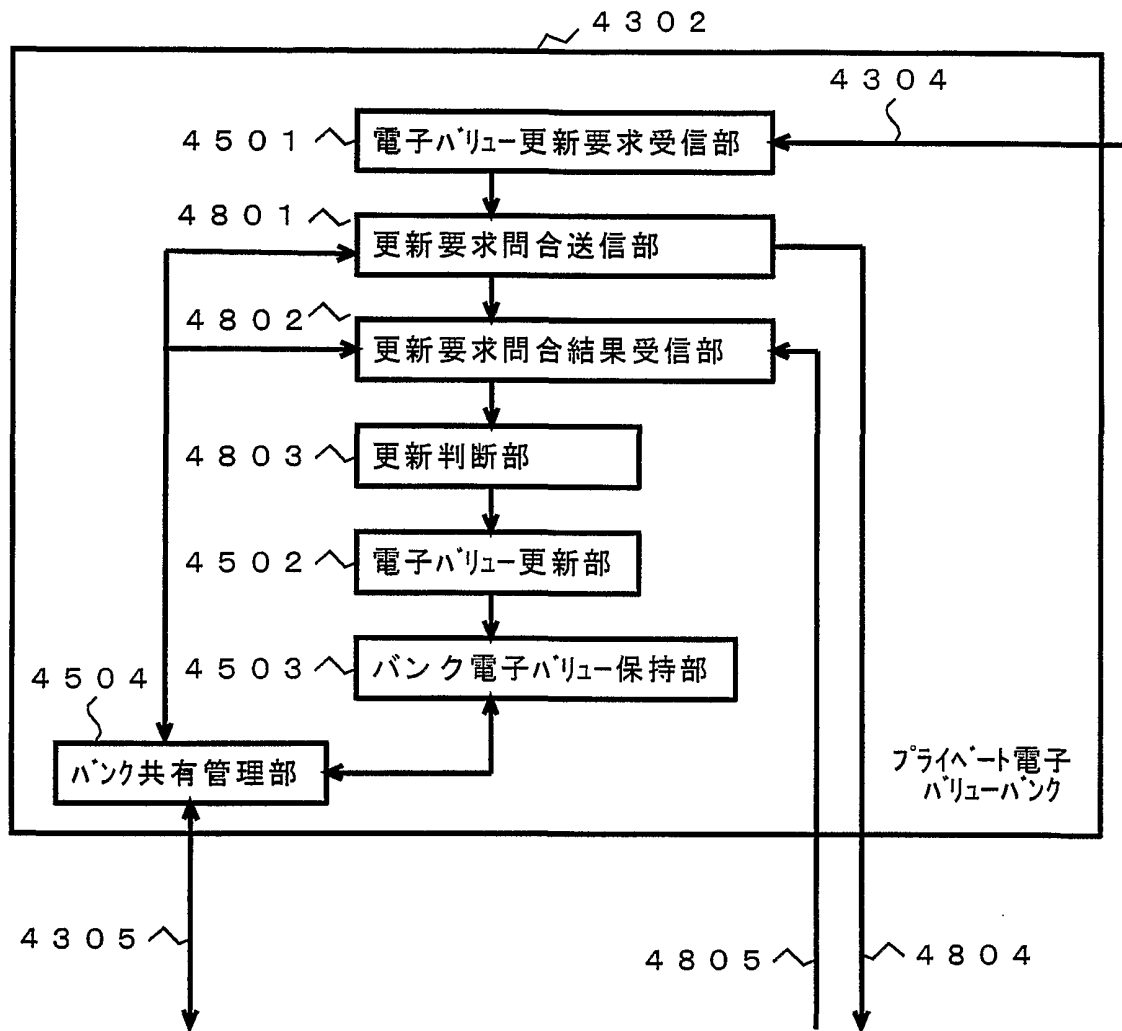


図 4 9

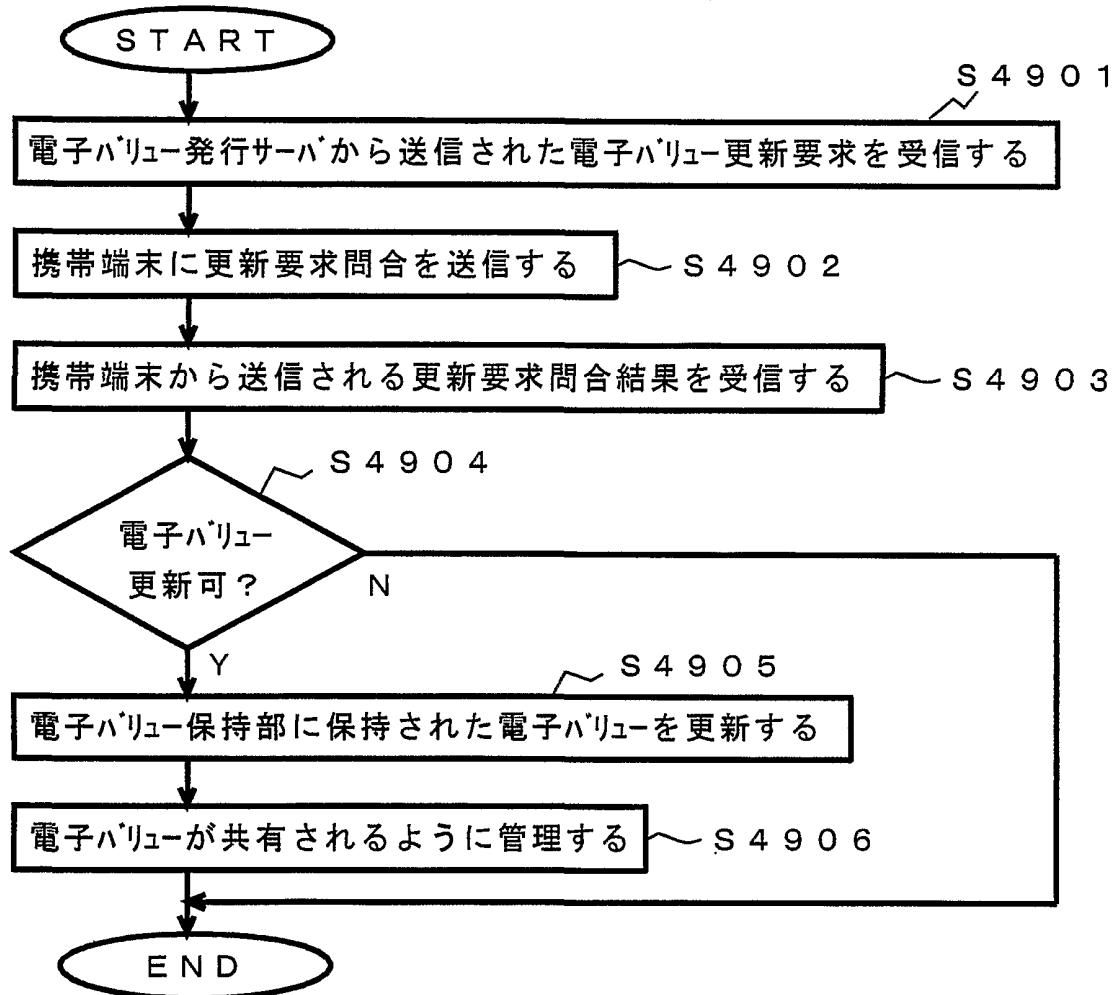


図 50

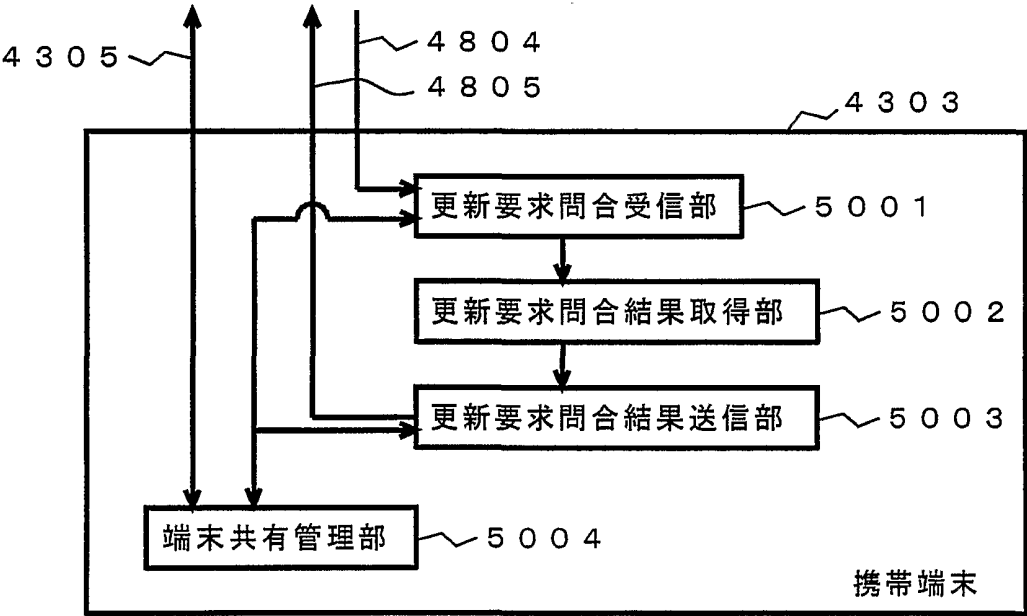


図 5 1

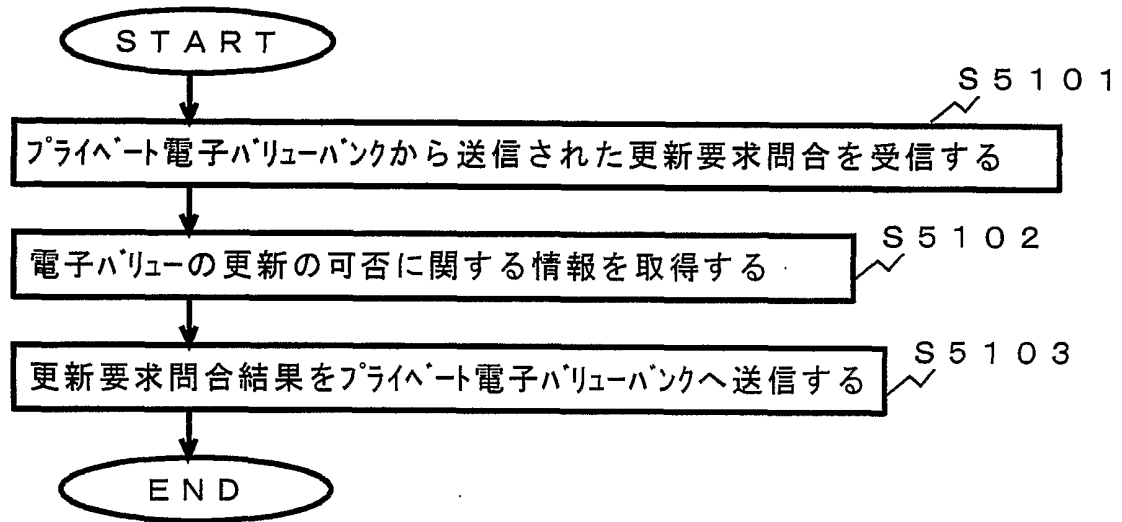


図 5 2

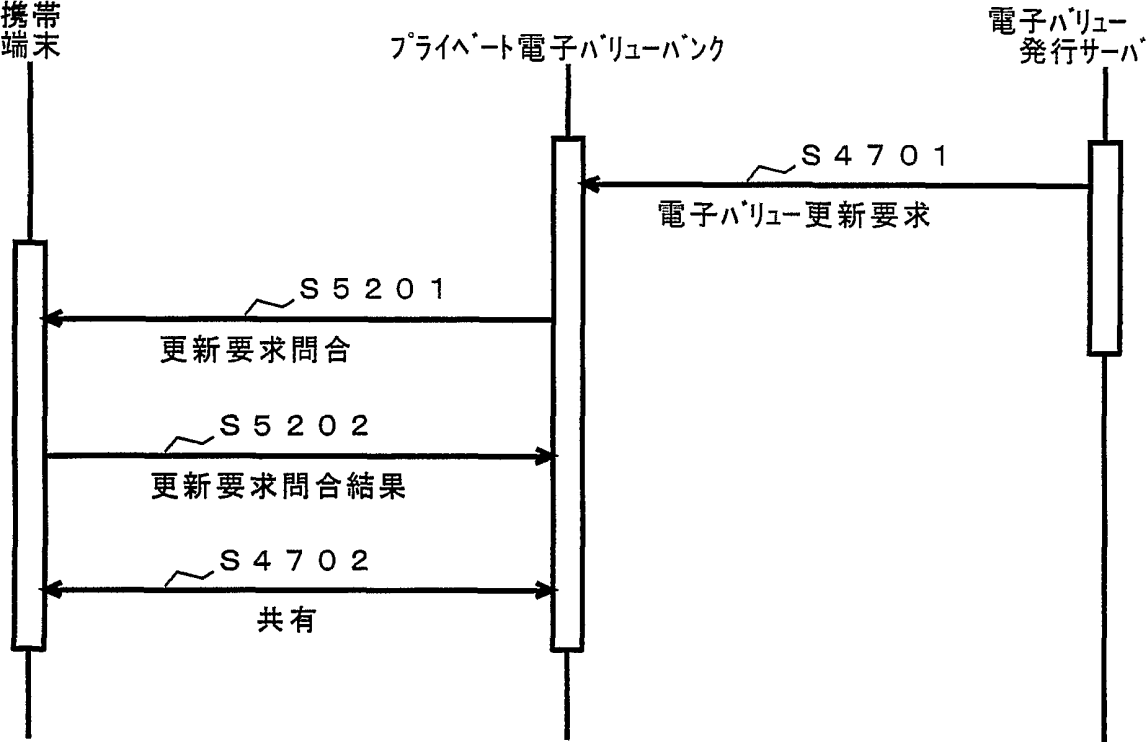


図 5 3

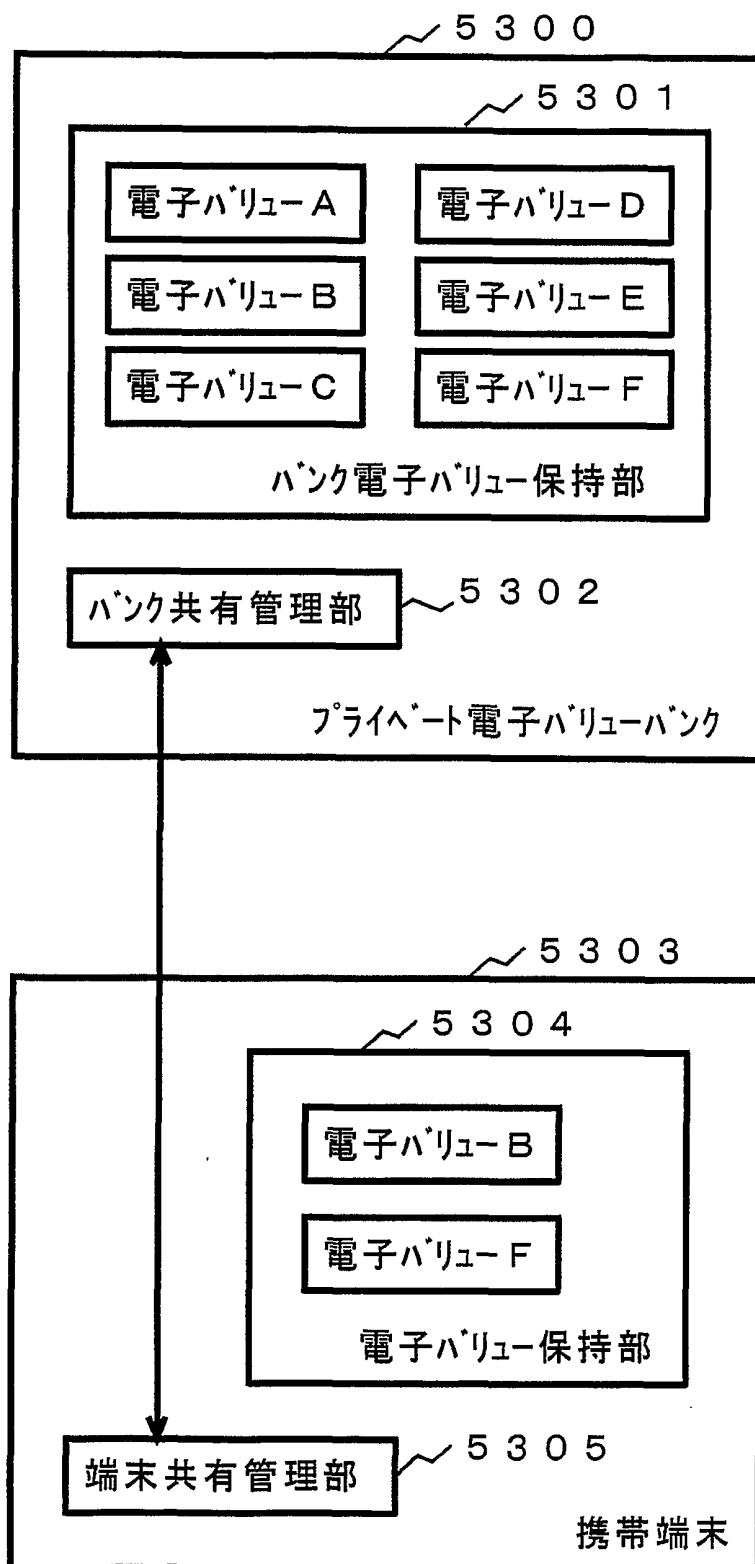


図 5 4

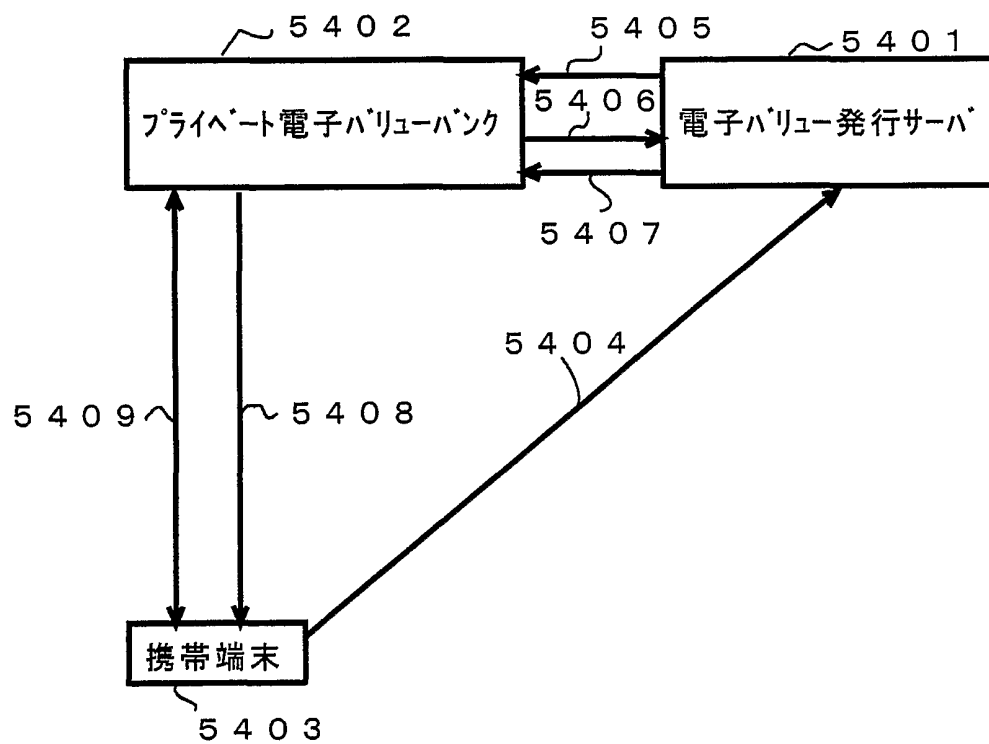


図 5 5

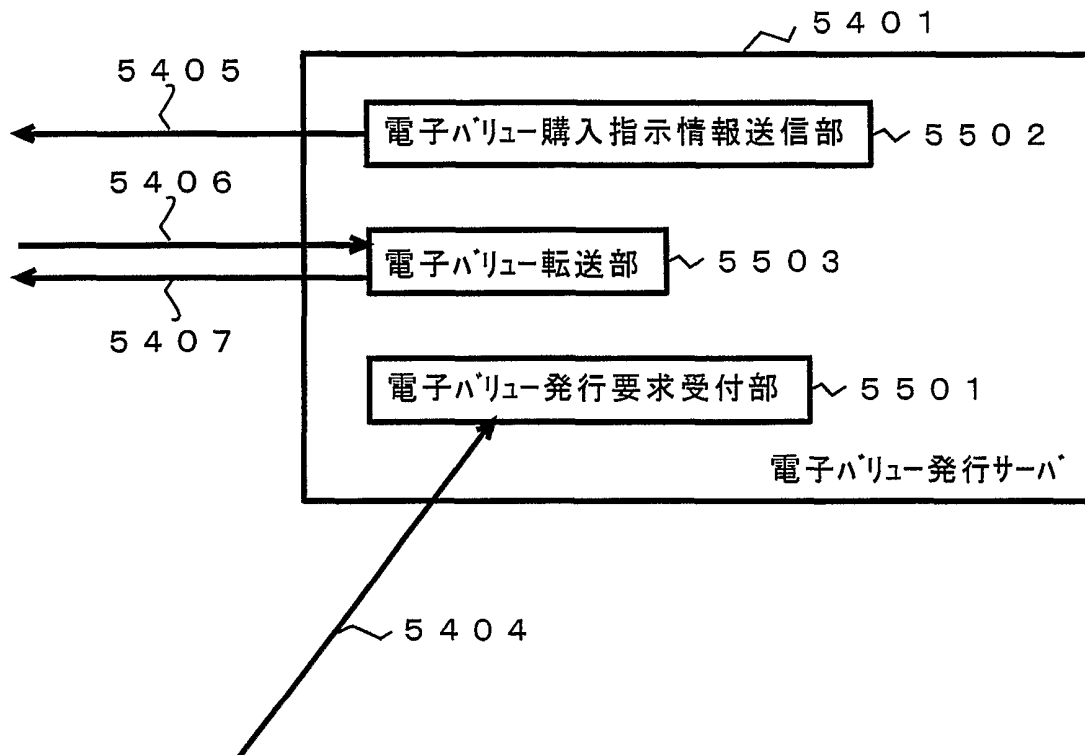


図 5 6

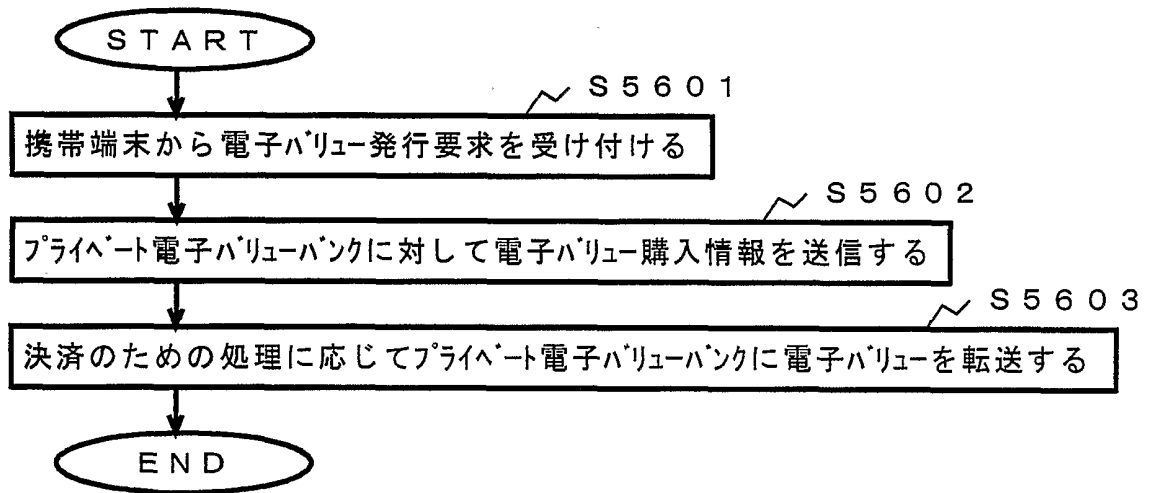


図 5 7

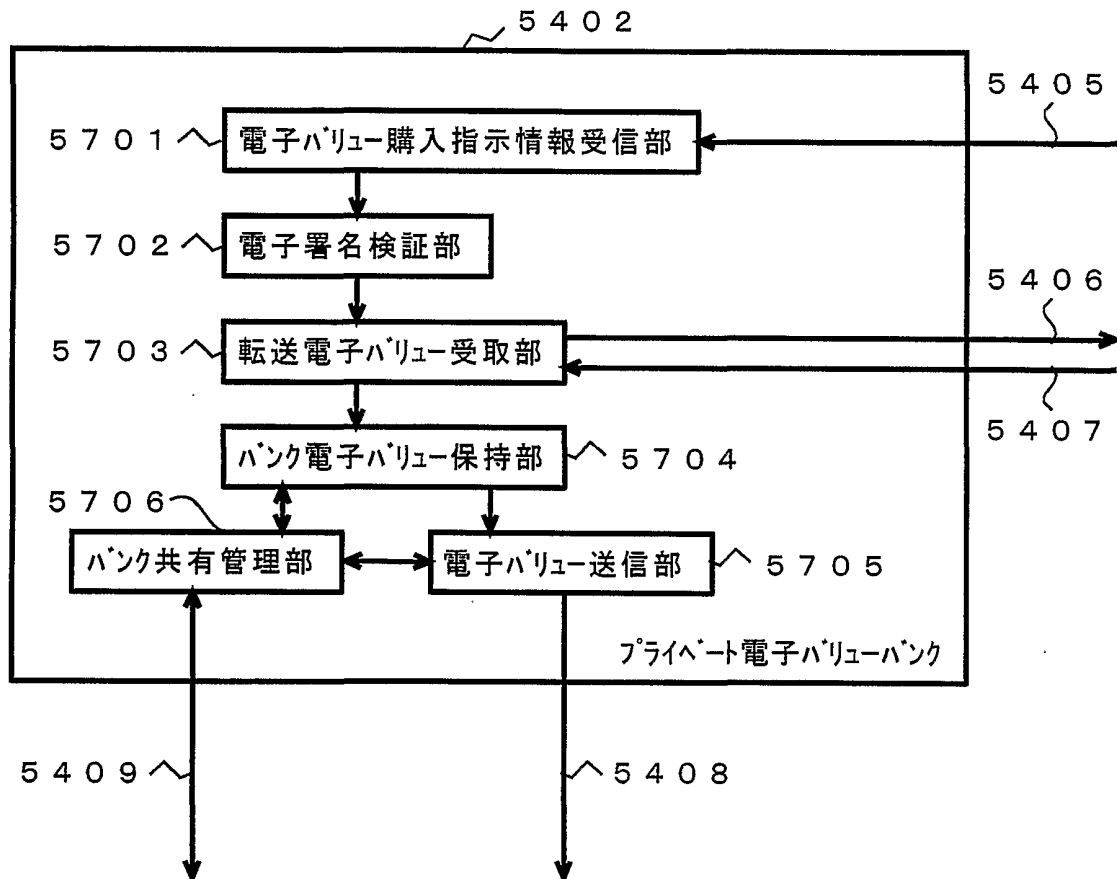


図 5 8

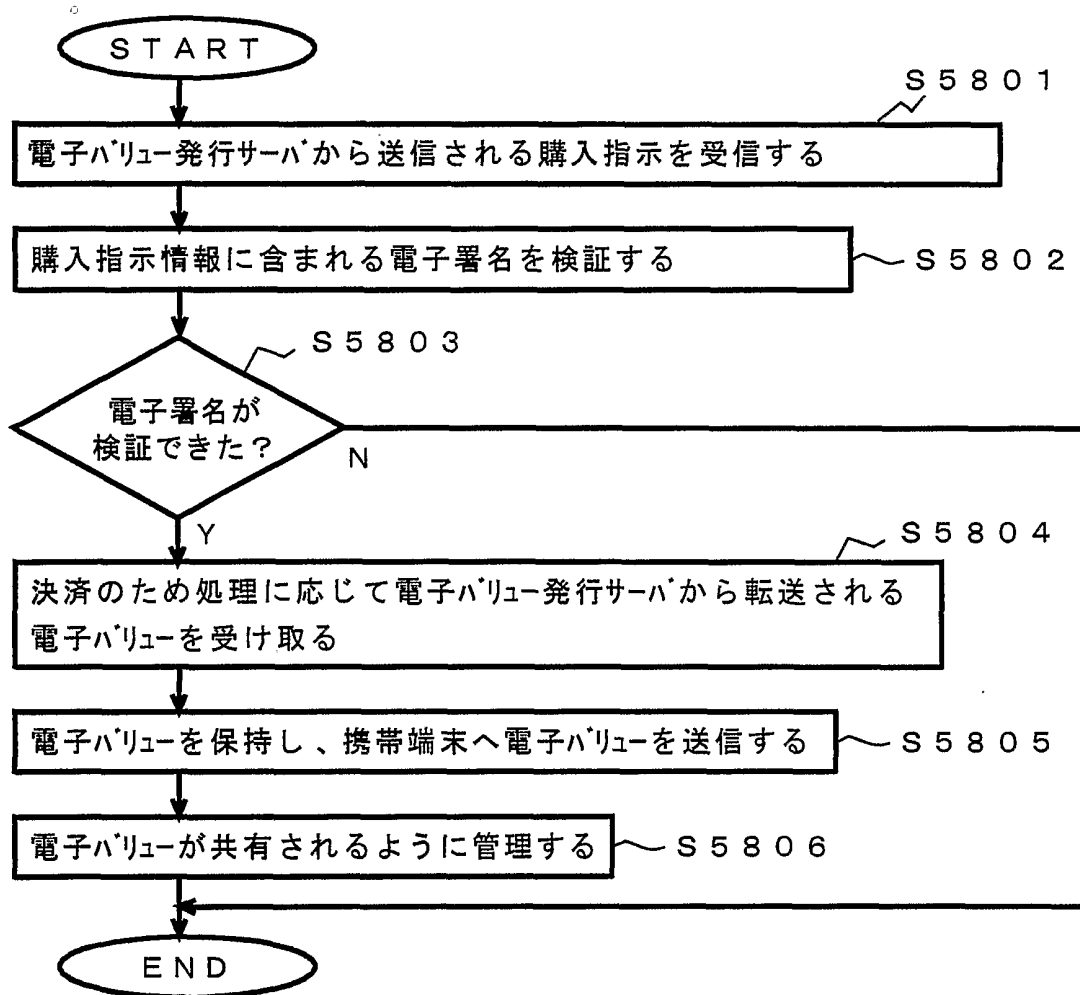


図 5 9

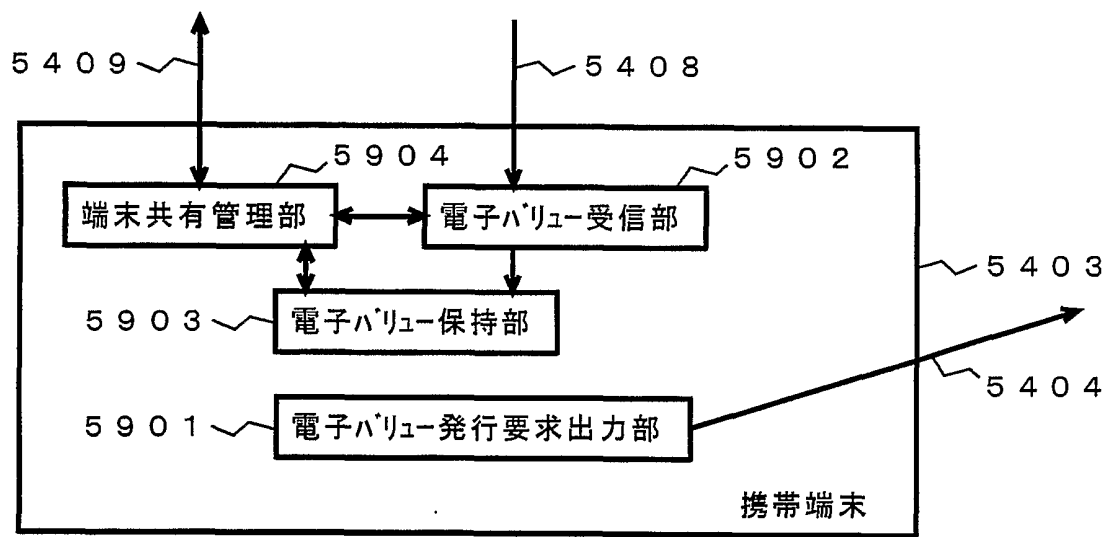


図 6 0

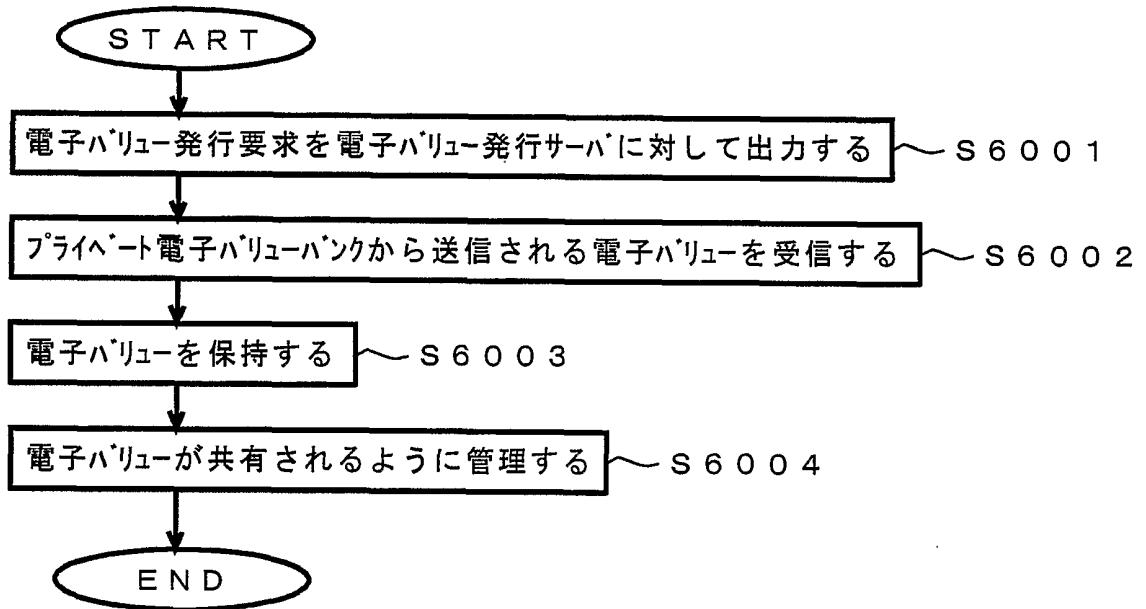


図 6 1

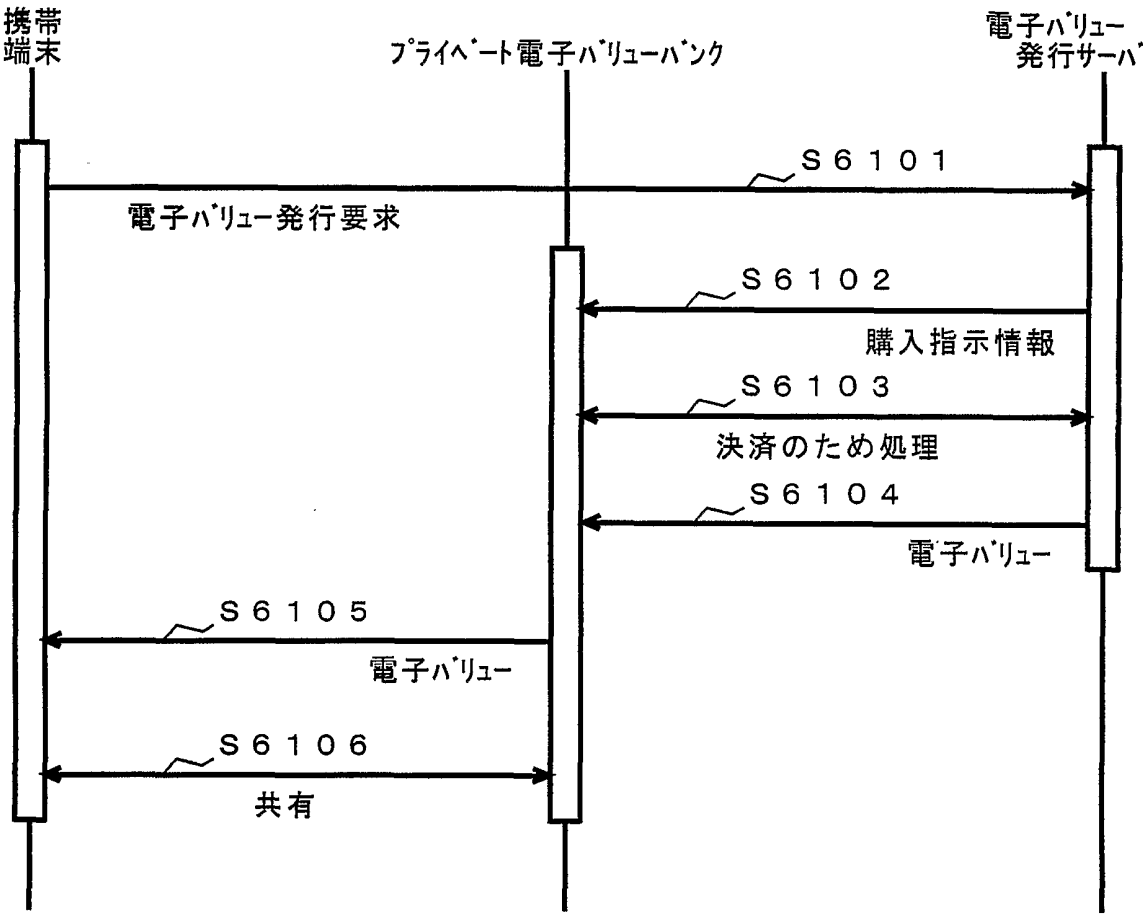


図 6 2

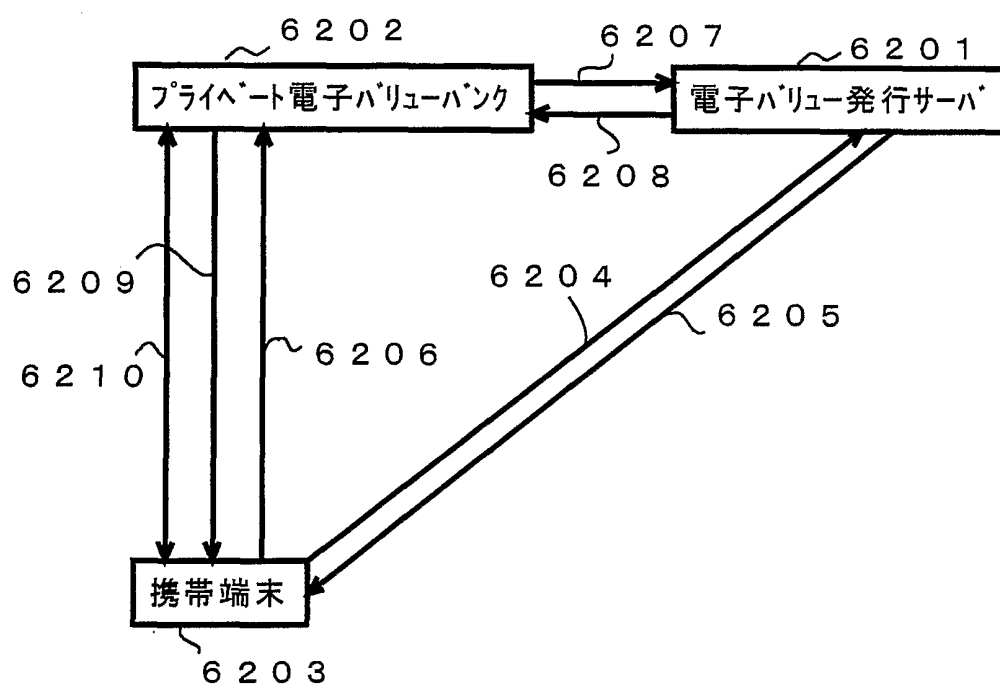


図 6 3

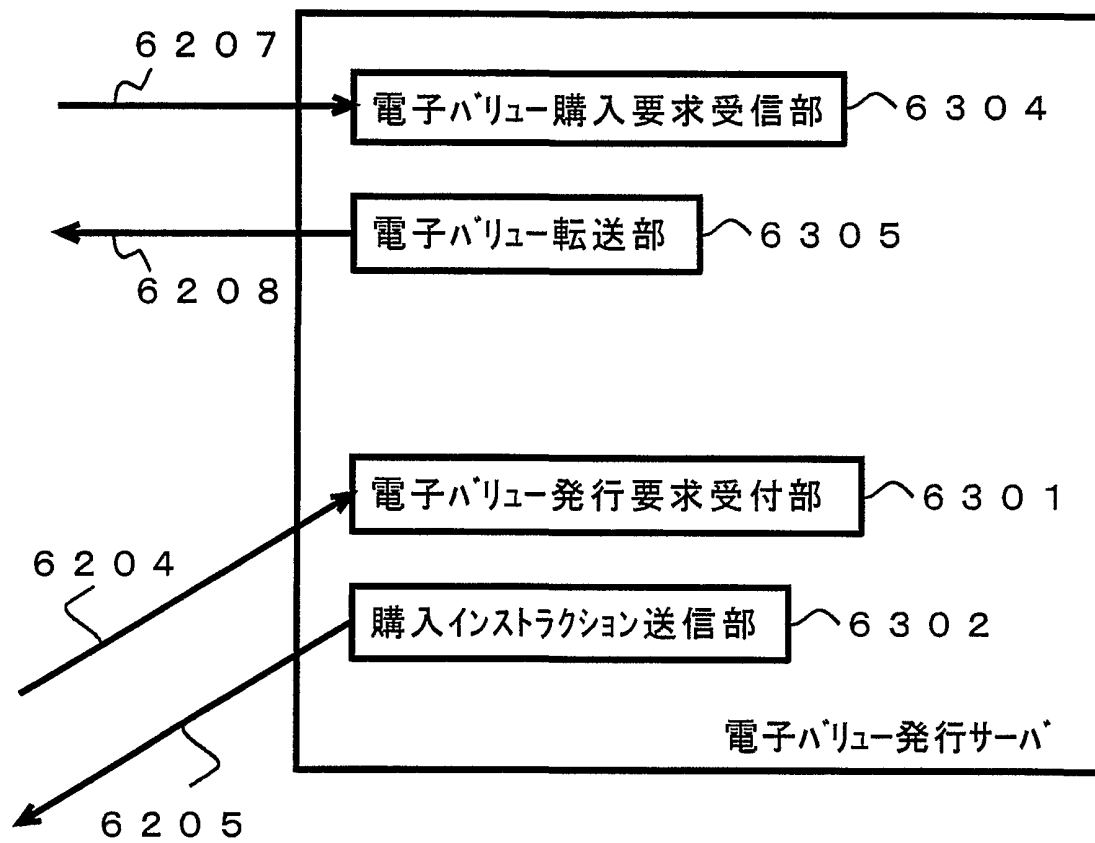
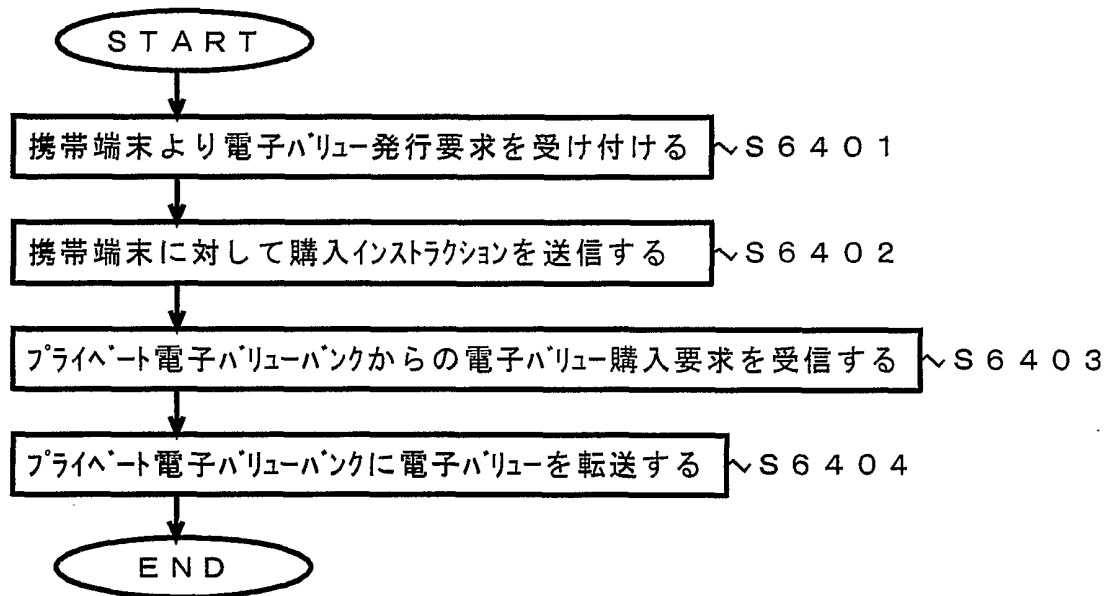


図 6 4



65/86

図 65

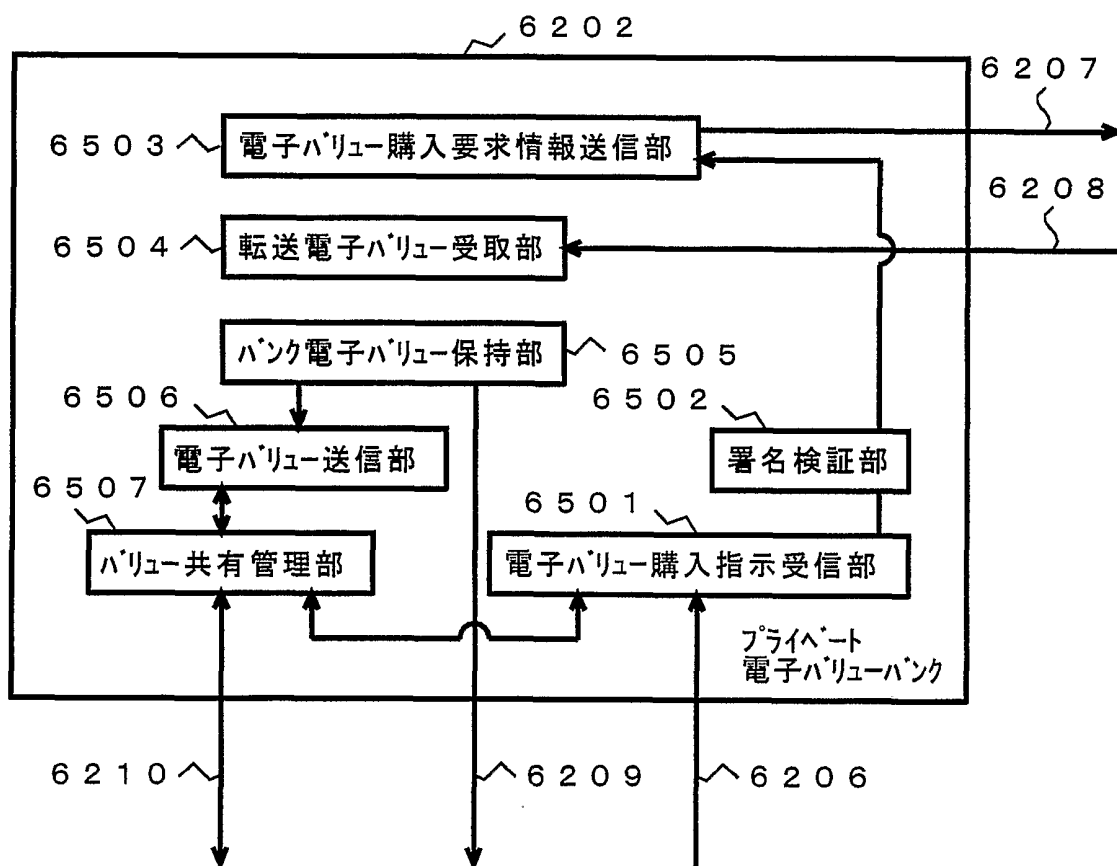


図 6 6

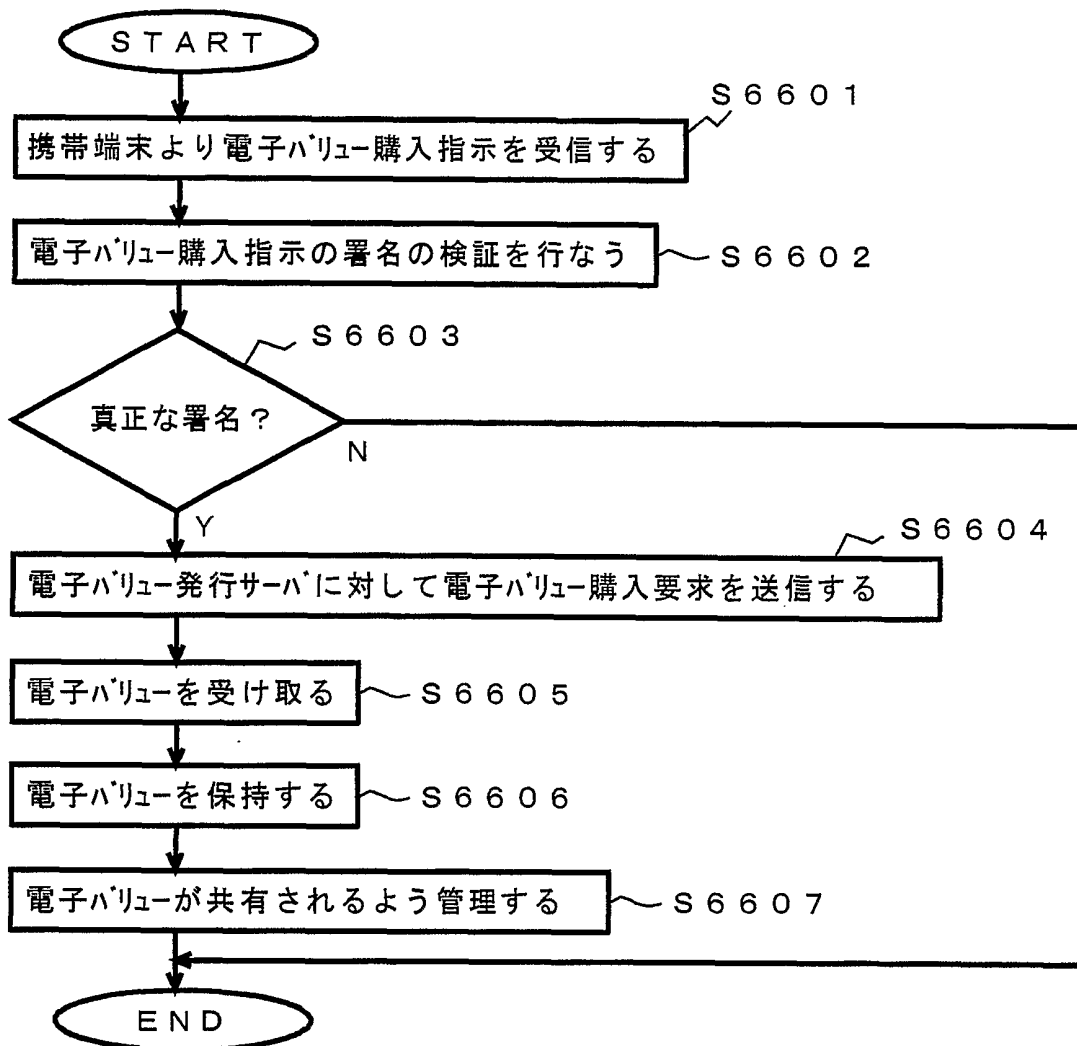


図 6 7

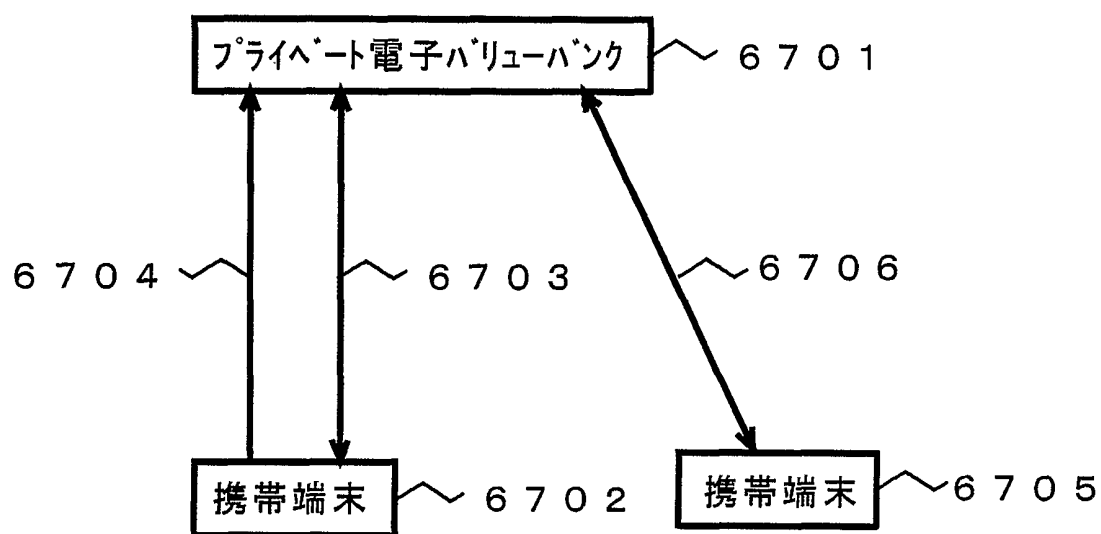


図 68

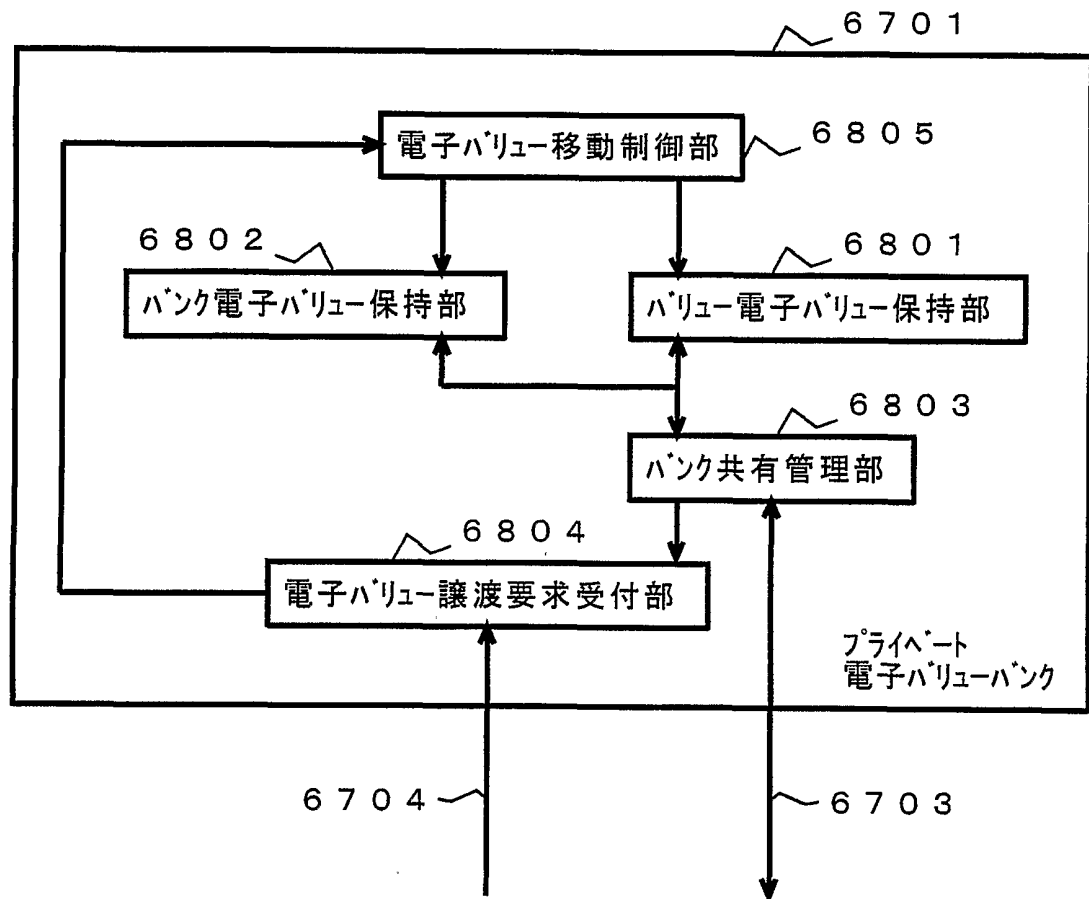


図 6 9

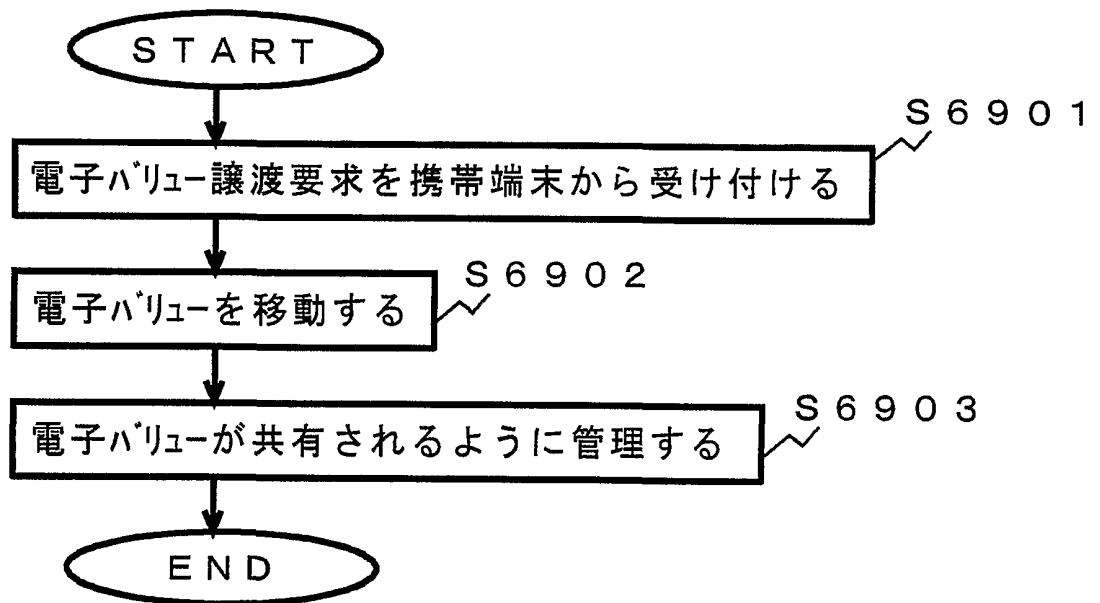
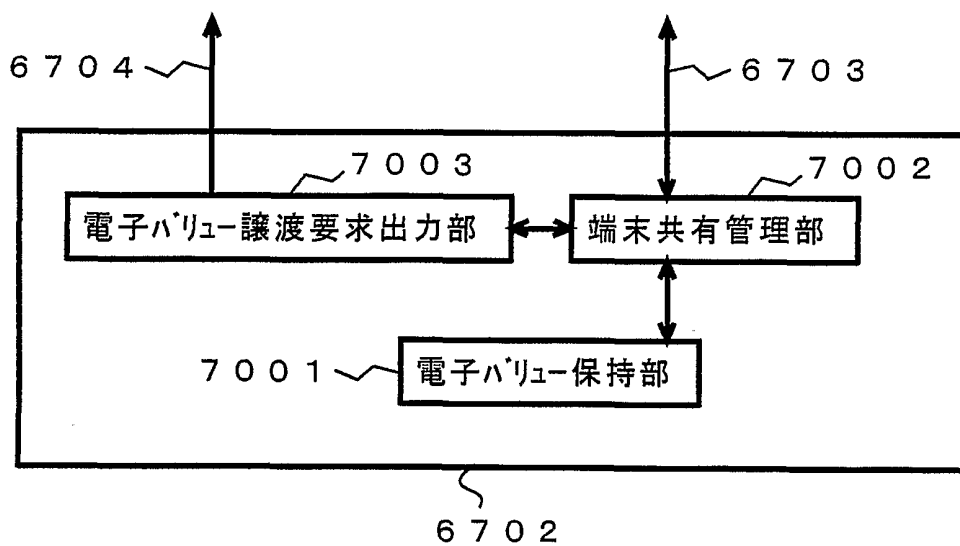
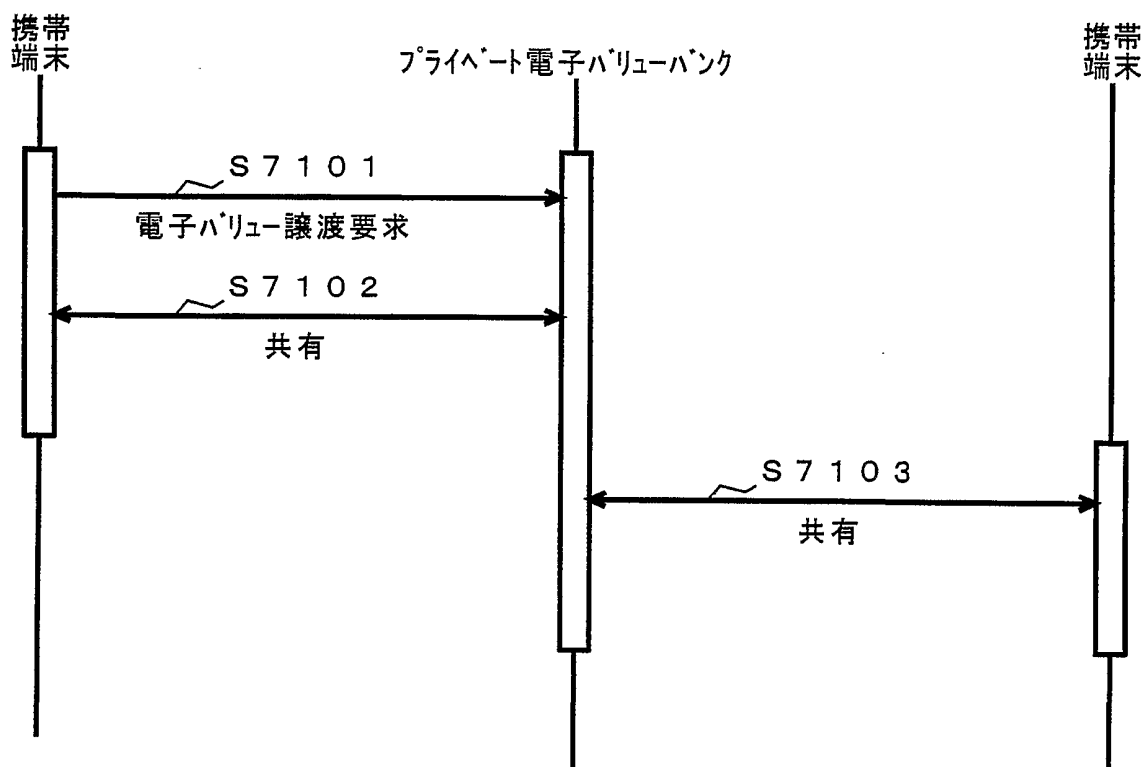


図 7 0



71/86

図 7 1



72/86

図 7 2

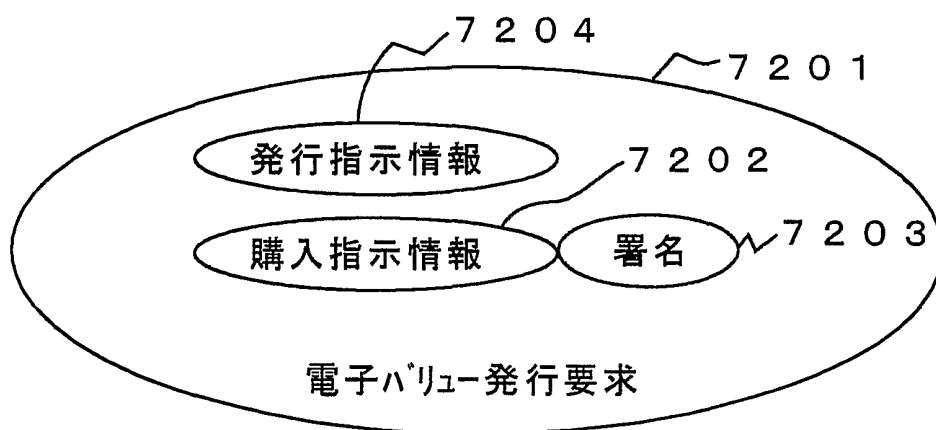


図 7 3

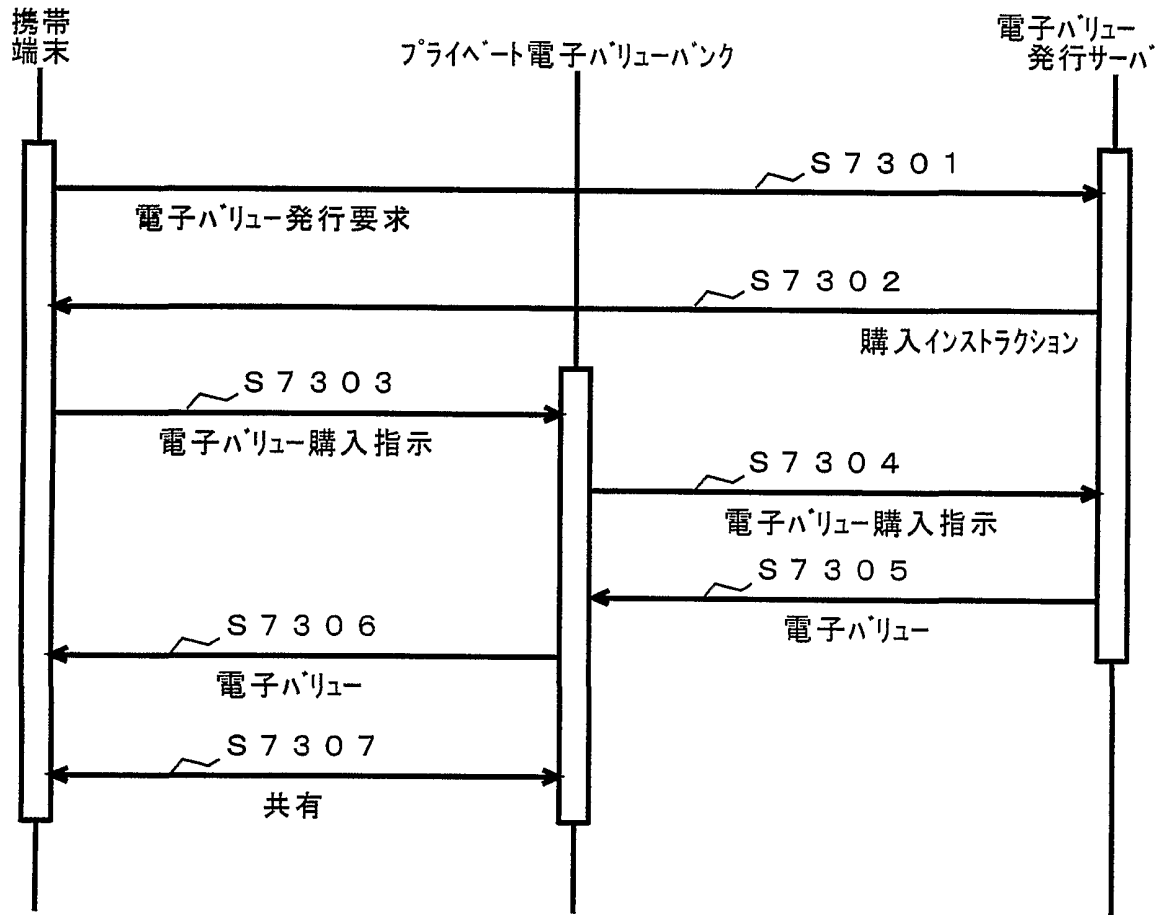


図 7 4

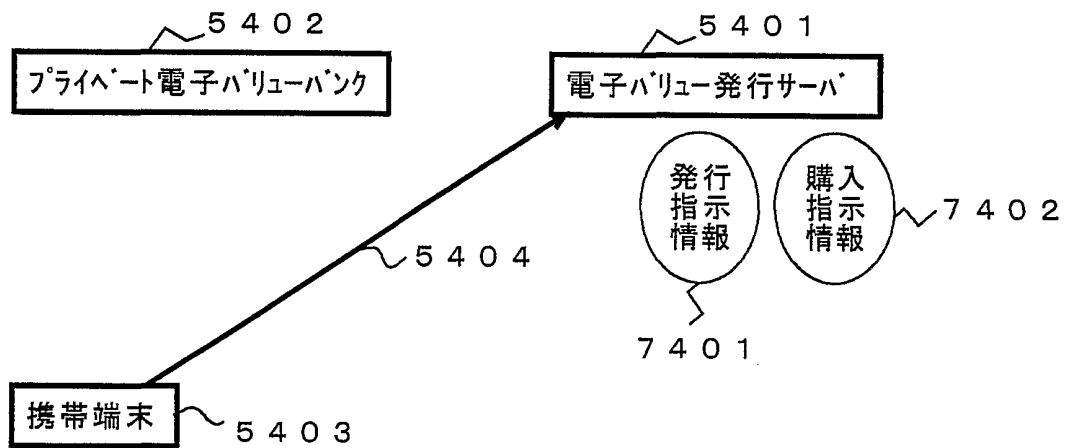


図 7 5

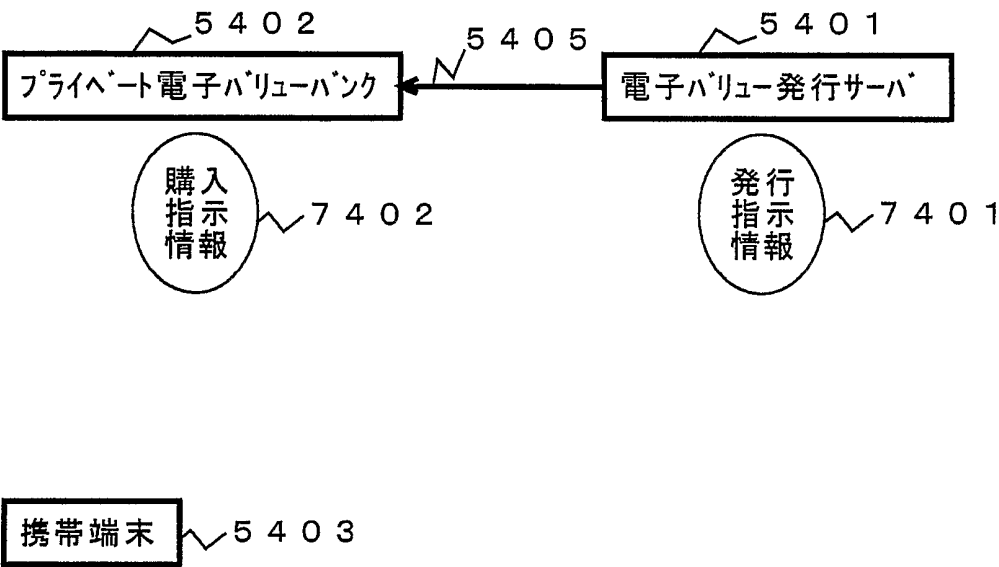
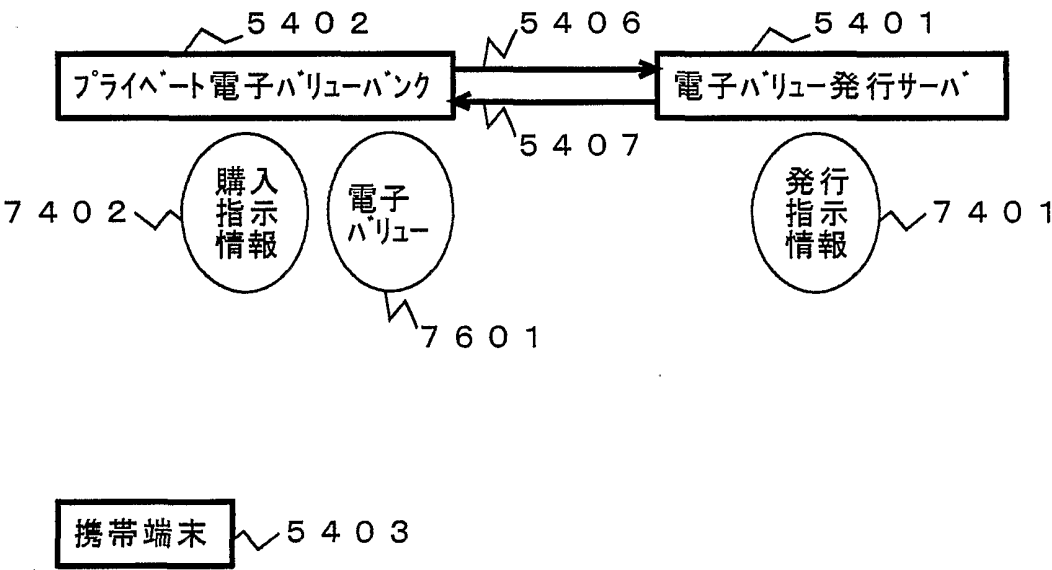
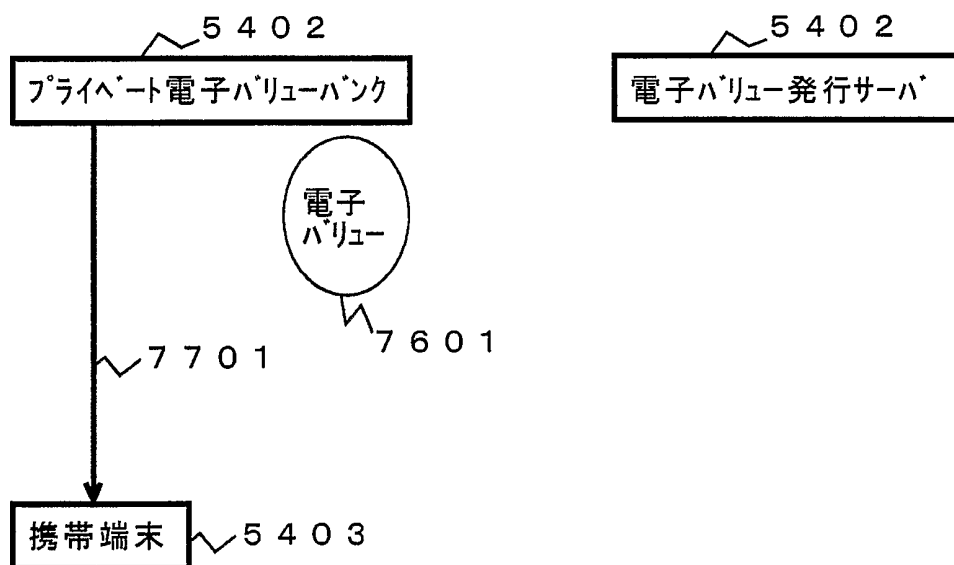


図 7 6



77/86

図 7 7



78/86

図 7 8

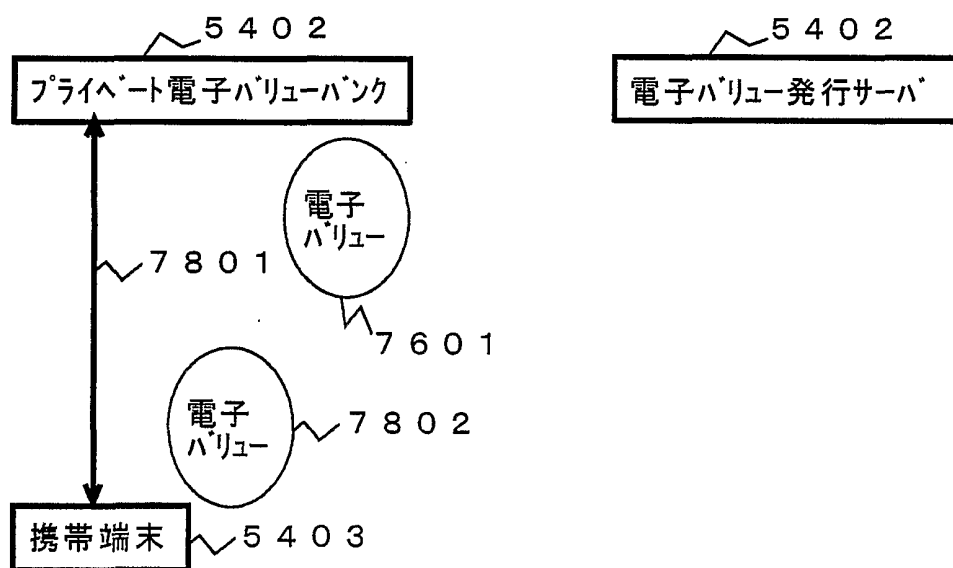


図 7 9

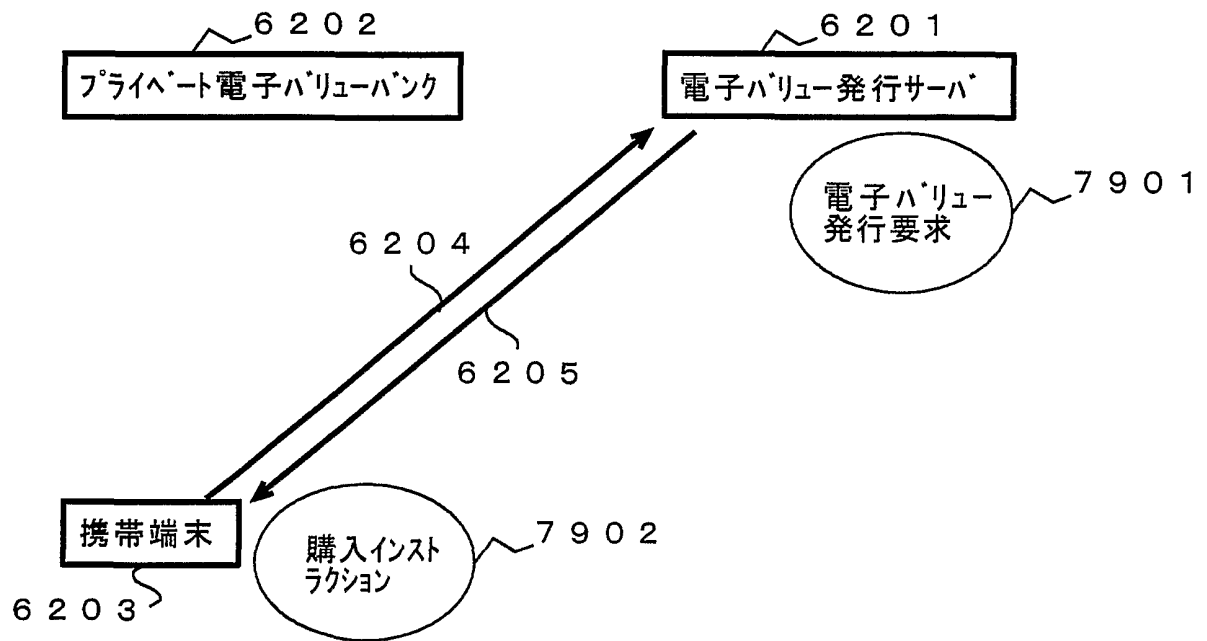


図 80

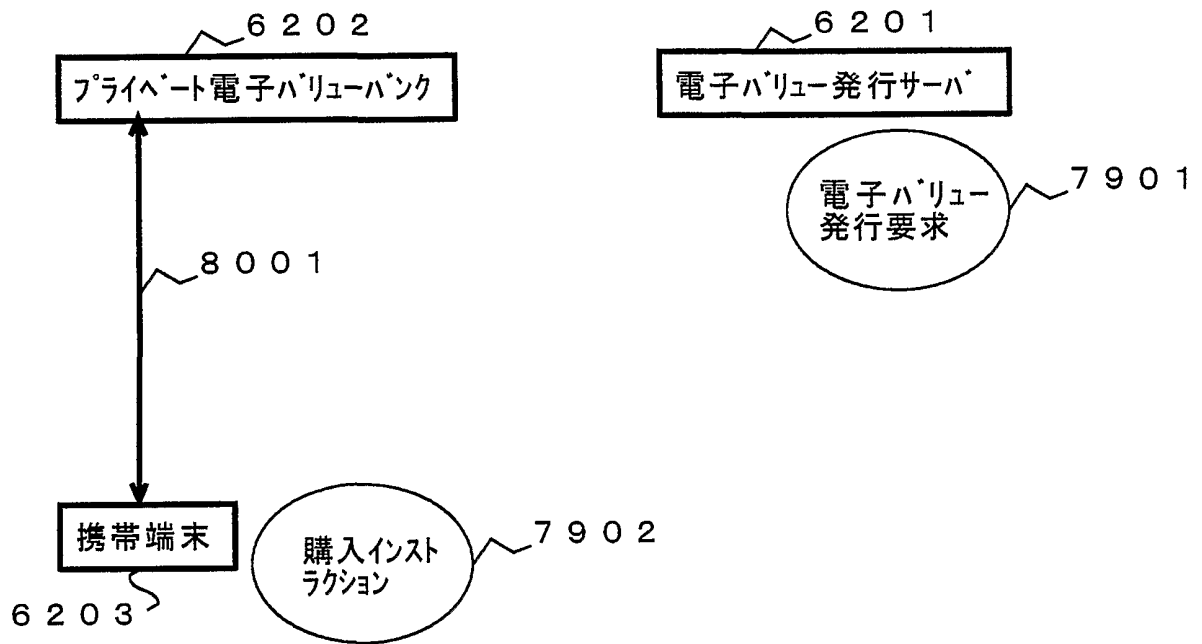


図 8 1

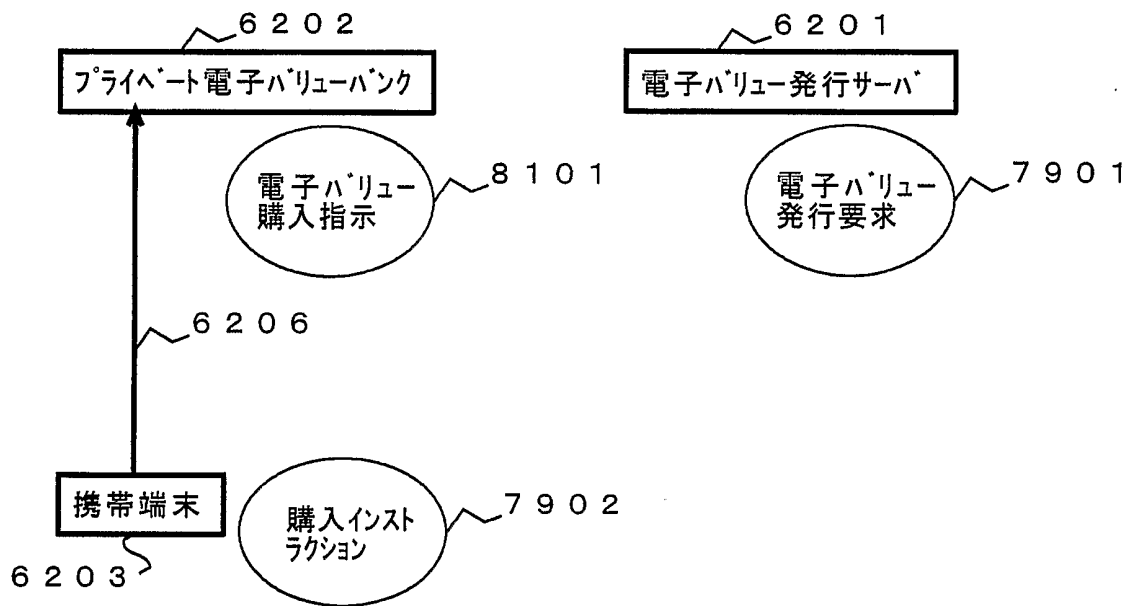


図 8 2

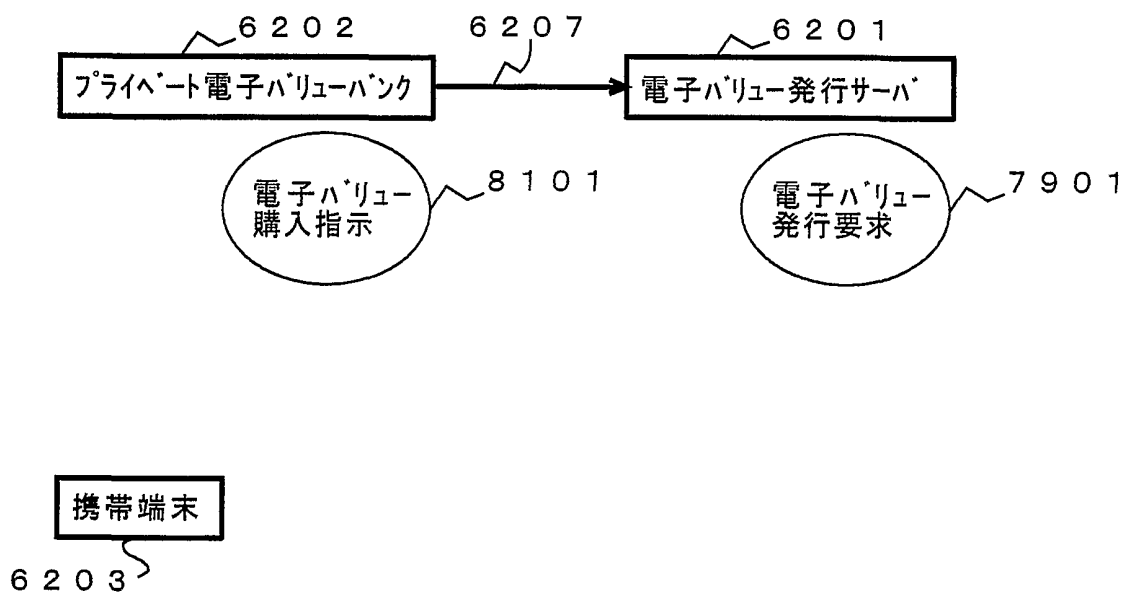


図 8 3

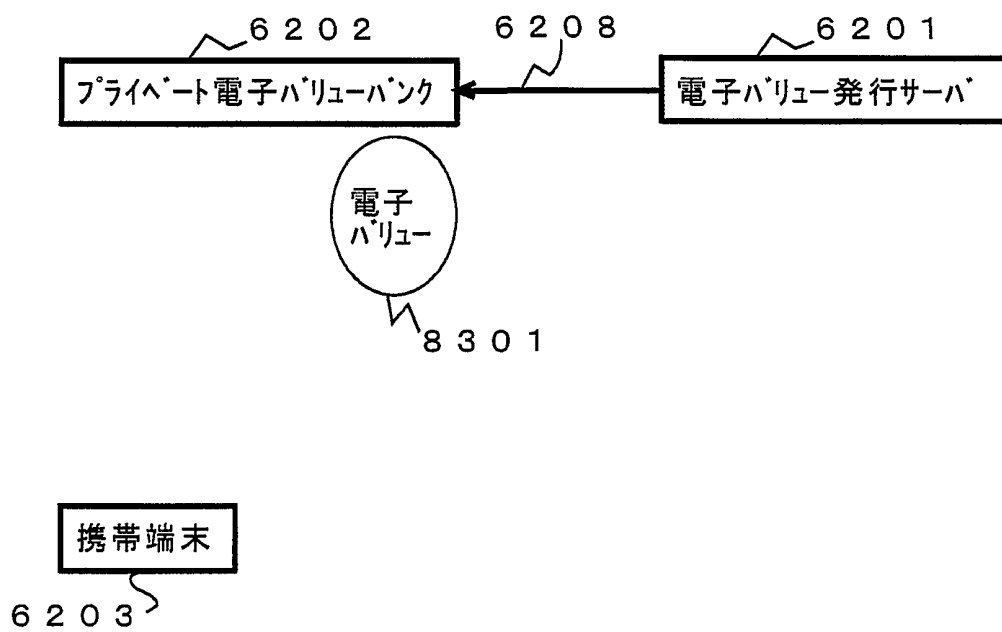
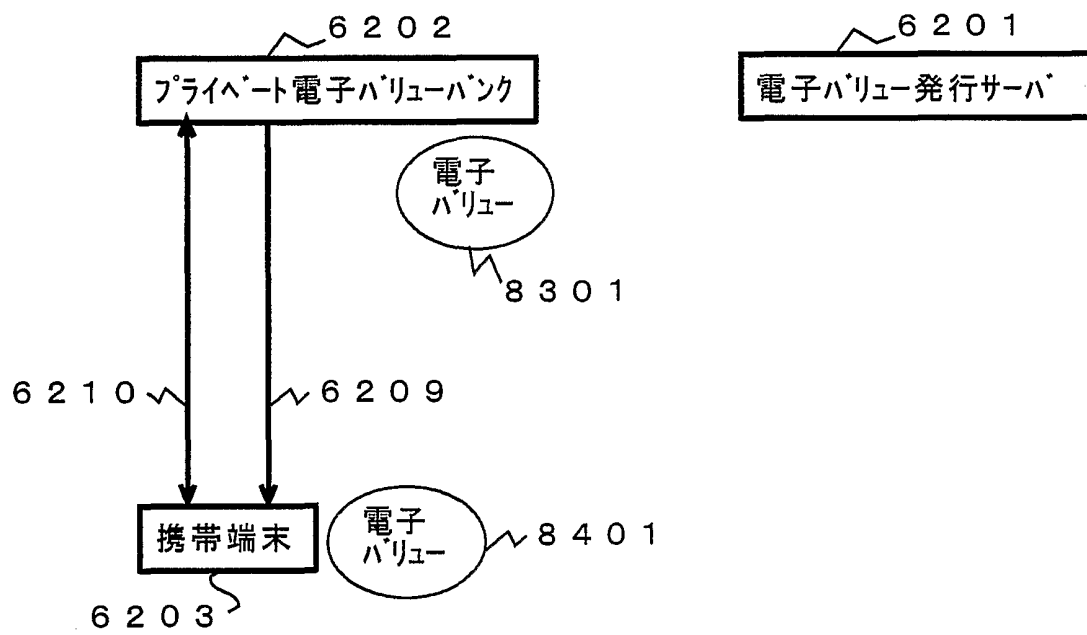


図 8 4



85/86

図 8 5

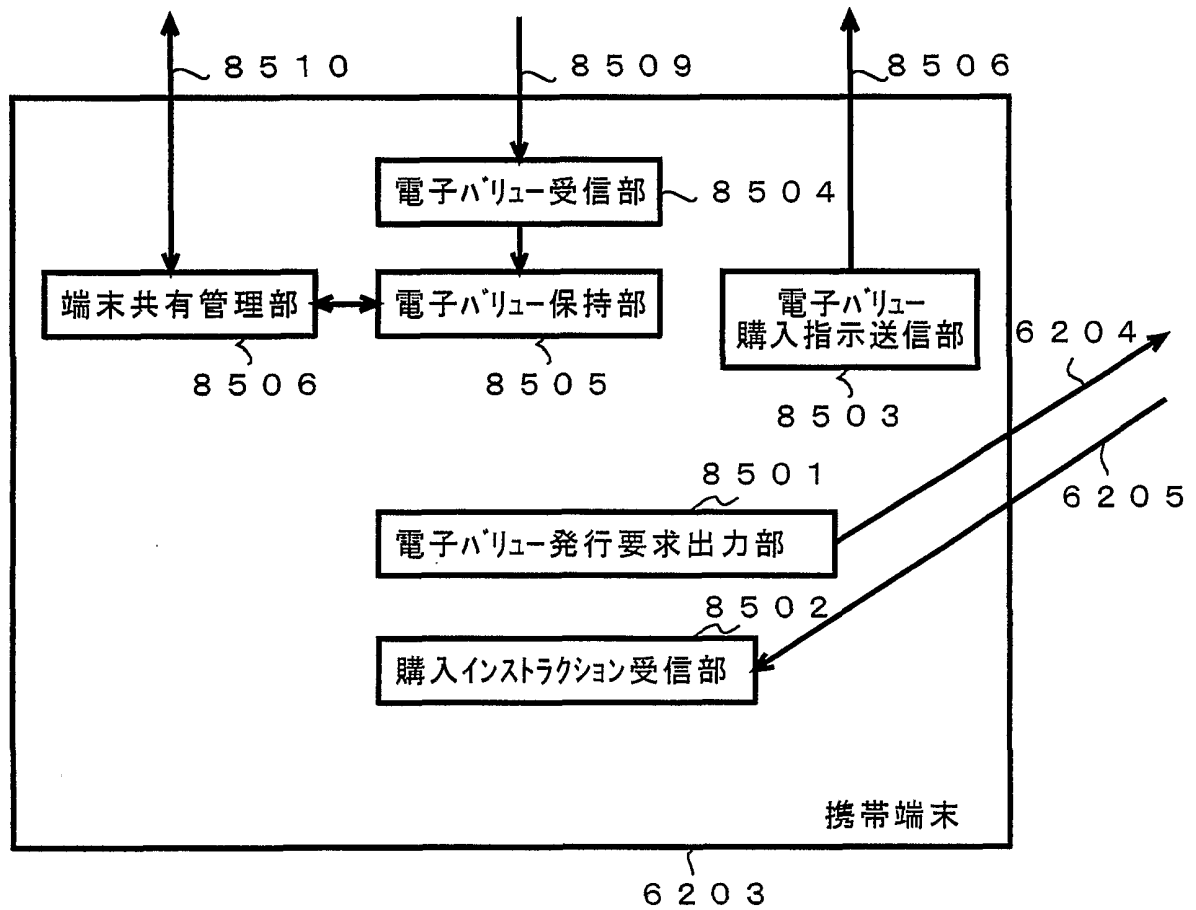
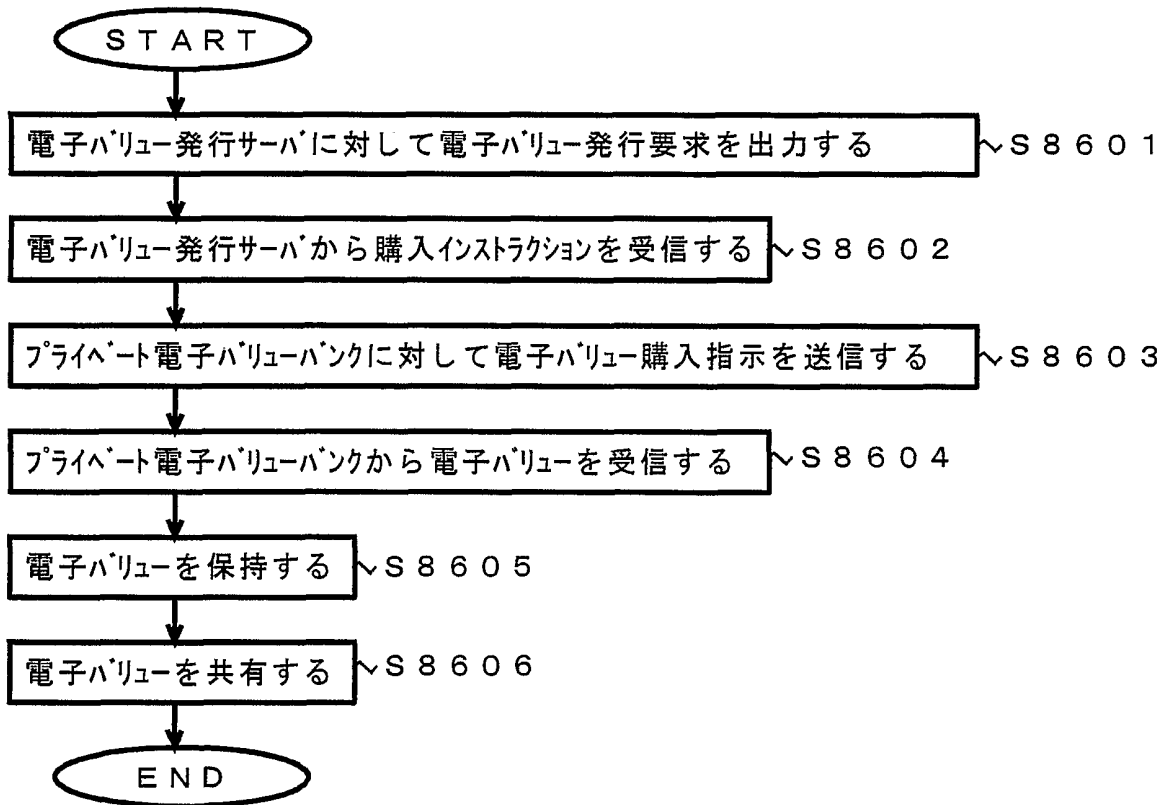


図 8 6



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/09740

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl.⁷ G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl.⁷ G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST FILE (JOIS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 917120 A2 (Citicorp Development Center, Inc.), 19 May, 1999 (19.05.99),	1, 2
Y	Full text & JP 11-232348 A & WO 99/24892 A2	3-13, 15-17, 23-30
A		14, 18-22
Y	JP 2000-67140 A (NTT Data Corporation), 03 March, 2000 (03.03.00),	3-13, 15-17
A	Full text (Family: none)	23-30
Y	JP 11-184947 A (Daiwa Institute of Research, Ltd.), 09 July, 1999 (09.07.99),	13, 15-16, 23-30
	Full text (Family: none)	
Y	JP 10-162088 A (NTT Data Tsushin K.K.), 19 June, 1998 (19.06.98),	23
	Full text (Family: none)	

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family
--	---

Date of the actual completion of the international search
06 December, 2001 (06.12.01)

Date of mailing of the international search report
18 December, 2001 (18.12.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/09740

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-198863 A (Hitachi, Ltd.), 31 July, 1998 (31.07.98), Full text (Family: none)	24
A	JP 11-338946 A (Glory, Ltd.), 10 December, 1999 (10.12.99), Full text (Family: none)	1-30
A	JP 10-154193 A (NTT Data Tsushin K.K.), 09 June, 1998 (09.06.98), Full text (Family: none)	1-30

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl ⁷ G06F17/60		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl ⁷ G06F17/60		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2001年 日本国登録実用新案公報 1994-2001年 日本国実用新案登録公報 1996-2001年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
JICSTファイル (JOIS)		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	EP 917120 A2 (CITICORP DEVELOPM ENT CENTER, INC.) 19. 5月. 1999 (19.	1, 2
Y	05. 99), 全文 & JP 11-232348 A & WO 99/24892 A2	3-13, 15-17, 23-30
A		14, 18- 22
Y	JP 2000-67140 A (株式会社エヌ・ティ・ティ・デ ータ) 3. 3月. 2000 (03. 03. 00), 全文 (ファミリ ーなし)	3-13, 15-17,
☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願		
の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	06. 12. 01	国際調査報告の発送日
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 小山 満
		5 L 9458 電話番号 03-3581-1101 内線 3560

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A		23-30
Y	JP 11-184947 A (株式会社大和総研) 9. 7月. 1999 (09. 07. 99), 全文 (ファミリーなし)	13, 15- 16, 23- 30
Y	JP 10-162088 A (エヌ・ティ・ティ・データ通信株式会社) 19. 6月. 1998 (19. 06. 98), 全文 (ファミリーなし)	23
Y	JP 10-198863 A (株式会社日立製作所) 31. 7月. 1998 (31. 07. 98), 全文 (ファミリーなし)	24
A	JP 11-338946 A (グローリー工業株式会社) 10. 12月. 1999 (10. 12. 99), 全文 (ファミリーなし)	1-30
A	JP 10-154193 A (エヌ・ティ・ティ・データ通信株式会社) 9. 6月. 1998 (09. 06. 98), 全文 (ファミリーなし)	1-30