

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第3604151号

(P3604151)

(45) 発行日 平成16年12月22日(2004.12.22)

(24) 登録日 平成16年10月8日(2004.10.8)

(51) Int.Cl.⁷

G06F 17/60

F I

G06F 17/60 410E

G06F 17/60 432A

請求項の数 13 (全 43 頁)

(21) 出願番号	特願平8-531976	(73) 特許権者	592255202
(86) (22) 出願日	平成8年4月19日(1996.4.19)		シティーバンク エヌ、エー、
(65) 公表番号	特表平11-504144		Citibank, N. A.
(43) 公表日	平成11年4月6日(1999.4.6)		アメリカ合衆国、ニューヨーク州 100
(86) 国際出願番号	PCT/US1996/005521		43、ニューヨーク、パーク アベニュー
(87) 国際公開番号	W01996/033476		399
(87) 国際公開日	平成8年10月24日(1996.10.24)	(74) 代理人	100059959
審査請求日	平成10年7月10日(1998.7.10)		弁理士 中村 稔
(31) 優先権主張番号	08/427,287	(74) 代理人	100067013
(32) 優先日	平成7年4月21日(1995.4.21)		弁理士 大塚 文昭
(33) 優先権主張国	米国(US)	(74) 代理人	100065189
			弁理士 穴戸 嘉一
		(74) 代理人	100074228
			弁理士 今城 俊夫

最終頁に続く

(54) 【発明の名称】 電子マネーシステム

(57) 【特許請求の範囲】

【請求項1】

電子モジュールの間で電子ノートを移転するためのシステムにおいて、各々がプロセッサとメモリを有し、暗号保証チャネルを形成することができ且つ該暗号保証チャネルを介して電子ノートを移転したり受信したりすることができ、且つそれぞれの前記メモリに前記電子ノートを記憶する電子モジュールを備えており、

各記憶される電子ノートは、該電子ノートと関連した貨幣的価値を示すデータを含むデータフィールドのボディーグループと、移転記録リストを含むデータフィールドの移転グループとを備えており、各移転記録は、移転元電子モジュールによって作成され、移転された電子ノートを、共通の前記移転元電子モジュールから移転され、共通の電子ノートから作成した1つ又はそれ以上の他の移転された電子ノートから区別するシーケンス番号を含むことを特徴とするシステム。

【請求項2】

前記貨幣的価値は、前記電子ノートに関連した原始貨幣的価値であり、前記移転記録は、さらに、移転された貨幣的価値を含む請求項1記載のシステム。

【請求項3】

プロセッサベースド電子モジュールの間で電子ノートを移転するための方法において、移転元電子モジュールと移転先電子モジュールとの間に暗号保証セッションを確立し、前記移転元電子モジュールに記憶される電子ノートに、前記電子ノートの貨幣的額のすべて、またはある部分が移転されているかを示す移転記録を付加することにより、前記移転

10

20

元電子モジュールにおいて移転電子ノートを作成し、
前記移転電子ノートを前記移転元電子モジュールから前記移転先電子モジュールへと移転し、
前記移転記録は、前記移転元電子モジュールにおいて作成され、前記移転電子ノートを、前記移転元電子モジュールからの別の移転電子ノートと区別するシーケンス番号を含むことを特徴とする方法。

【請求項 4】

移転元電子モジュールから移転先電子モジュールへ所定の全貨幣的価値の電子ノートを移転する方法において、

(a) 前記全貨幣的価値を与える一つもしくはそれ以上の電子ノートを前記移転元電子モジュールが選択し、 10

(b) 前記移転元電子モジュールのそれぞれの移転記録とデジタル署名とを前記一つもしくはそれ以上の電子ノートへ加えることにより一つもしくはそれ以上の移転電子ノートを前記移転元電子モジュールがつくり、一つもしくはそれ以上の移転電子ノート毎に前記それぞれの移転記録は、前記一つもしくはそれ以上の電子ノートの総てもしくはある部分が移転されているか、否かを示しており、

(c) 前記移転元電子モジュールは前記一つもしくはそれ以上の移転電子ノートを前記移転先電子モジュールへ送り、

(d) 前記移転先電子モジュールは前記一つもしくはそれ以上の移転電子ノートの正当性を検証し、 20

(e) 前記移転先電子モジュールは前記一つもしくはそれ以上の移転電子ノートの各々に情報を蓄積し、そして

前記段階 (d) では前記一つもしくはそれ以上の移転電子ノートの移転電子ノート毎に、前記移転電子ノートとのマッチのため、前記移転先電子モジュールに蓄積され、前記移転先電子モジュールへ又はそこから以前に移転された他の電子ノートを表すノート情報を検査し、そして前記移転電子ノートに認識されたマッチに基づきノート移転ツリーの表示を解析することにより、ノートを重複検査することの特徴とする方法。

【請求項 5】

前記移転記録はシーケンス認識番号を含み、前記一つもしくはそれ以上の電子ノート毎に前記シーケンス識別番号はそれからつくられたすべての移転電子ノートを区別する請求項 4 に記載の方法。 30

【請求項 6】

前記一つもしくはそれ以上の移転電子ノートの移転電子ノート毎に、前記段階 (d) では前記移転記録と他の移転元電子モジュールによって加えられたすべての他の移転記録とを検査して、直前の移転で移された貨幣的価値よりも大きくない貨幣量が移転毎に移されたことを確認する請求項 4 に記載の方法。

【請求項 7】

前記一つもしくはそれ以上の移転電子ノートの各移転電子ノートは、前記移転電子ノートの履歴にわたって各移転元電子モジュールのデジタル署名と認証とを含んでおり、前記段階 (d) では各デジタル署名と認証の正当性を検証する請求項 4 に記載の方法。 40

【請求項 8】

前記一つもしくはそれ以上の移転電子ノートの各移転電子ノートは期限切れ日付けを含んでおり、そして前記移転先電子モジュールは取引電子モジュールであり、前記段階 (d) では前記移転先電子モジュールが各電子ノートの期限切れ日付を検証する請求項 4 に記載の方法。

【請求項 9】

前記電子ノートは期限切れ日付けと貨幣価値とを有する通貨の電子的表示であり、前記段階 (a) は、

(a) 所定の全貨幣的価値を与え、そして最小数の電子ノートを使用するためのすべてのあり得る選択を求め、 50

(b) 前記すべてのあり得る選択の中で最小数の移転を含む要素からなるセットを求め、そして

(c) そのセットが一つよりも多い要素を含んでいる場合、電子ノートの満期日までの日数とその電子ノートの残りの貨幣的価値との積を表す値を貨幣単位日とし、そのセットの要素のすべてのノートにわたって集計した最小数の貨幣単位日を含むセットの要素を選択する請求項4に記載の方法。

【請求項10】

前記段階(d)では前記移転先電子モジュールは、移転された前記所定の貨幣的価値が予期した値に一致することを検証する請求項4に記載の方法。

【請求項11】

移転元電子モジュールから移転先電子モジュールへ電子ノートに移転する方法において、

(a) 前記移転元電子モジュールのそれぞれの移転記録を前記一つもしくはそれ以上の電子ノートに加えることにより一つもしくはそれ以上の移転電子ノートを前記移転元電子モジュールがつくり、

(b) 前記移転元電子モジュールは前記一つもしくはそれ以上の移転電子ノートを前記移転先電子モジュールへ送り、

(c) 前記移転元電子モジュールは前記一つもしくはそれ以上の移転電子ノートの正当性を検証し、

前記一つもしくはそれ以上の移転電子ノートの各移転電子ノートは前記移転電子ノートの履歴にわたっての各移転先電子モジュールの独自の識別子を含み、そして、前記移転先電子モジュールが取引電子モジュールである場合には、前記段階(c)は、前記独自の識別子の各々が前記移転先電子モジュールに保存された不良電子モジュールの独自の識別子リストにあるかどうかを検証する段階を含むことを特徴とする方法。

【請求項12】

移転元電子モジュールから移転先電子モジュールへ電子ノートに移転する方法において、

(a) 前記移転元電子モジュールのそれぞれの移転記録を前記一つもしくはそれ以上の電子ノートに加えることにより一つもしくはそれ以上の移転電子ノートを前記移転元電子モジュールがつくり、

(b) 前記移転元電子モジュールは前記一つもしくはそれ以上の移転電子ノートを前記移転先電子モジュールへ送り、

(c) 前記移転先電子モジュールは前記一つもしくはそれ以上の移転電子ノートの正当性を検証し、

前記一つもしくはそれ以上の移転電子ノートの各移転電子ノートは移転電子ノートの履歴にわたり移転先電子モジュールのそれぞれ独自の識別子を含み、そして前記移転先電子モジュールは取引電子モジュールであり、前記段階(c)では各前記の独自の識別子の何れかが前記移転先電子モジュールに蓄積されている不良電子モジュールの独自の識別子のリストにのっているか、否かを検査することの特徴とする方法。

【請求項13】

それぞれが複数のモジュールタイプの一つであるプロセッサベースド電子モジュールの間で電子ノートに移転するシステムにおいて、プロセッサベースド電子モジュールを備え、各プロセッサベースド電子モジュールは独自のモジュール識別子を蓄積し、そしてそれぞれは暗号で安全を保証されたチャネルをつくり、そしてこの暗号で安全を保証されたチャネルを介して電子ノートに移転したり、受け取ったりすることができ、そして前記電子モジュールの各々は前記電子ノートを蓄積するメモリを有し、

前記複数のモジュールタイプの各々はモジュールタイプ変数の独自の範囲と関連しており、そして前記独自のモジュール識別子の各々は、所定の素数より小さい独自の整数値であり、前記電子モジュールの各々に蓄積されモジュールタイプに応じて電子モジュールの認証を与える暗号のマッピング機構に従って、前記モジュールタイプへ割り当てられた前記独自の範囲内の前記タイプの変数の値へマップし、前記素数の原始根を、前記所定の素数を法とする剰余演算を通じて前記独自の認識子の値で累乗することにより前記タイプ変数

10

20

30

40

50

の値を発生させ、前記複数の電子モジュールの各々は、前記原始根と前記素数とを蓄積するものであることを特徴とするシステム。

【発明の詳細な説明】

この出願は、1994年4月28日に提出された出願係属中の米国特許出願第08/234,461号の一部継続出願である。

発明の分野

本発明は、現金、小切手、クレジット及びキャッシュカード、並びに電子資金振替に対する経済取引の代替媒体として電子マネー取引を実行するための電子マネーシステムに関する。

発明の背景

今日、毎年約3500億の硬貨及び通貨取引が、個人と企業の間で発生している。硬貨及び通貨取引の大規模な使用は、購入、運賃、並びに銀行口座預金及び引出しのような個々の取引の自動化を制限している。個々の現金取引は、正しい金額を有すること及びその釣銭を用意することの必要性によって負担になる。更に、ペーパーキャッシュ及び硬貨の取扱い、及び管理（保護を含む）は、個人及び金融機関の両方に対して不便であり、費用が掛かり、かつ時間の浪費である。米国だけでも、単に貨幣を移動するために一年に600億ドルが貨幣取扱者によって費やされるということが推定される。更に、紙幣のセキュリティは、例えば、広範囲にわたりアクセス可能な、高性能カラー複写機を使用することにより比較的容易な偽造によって著しく脅かされている。

小切手は、口座において利用可能な金額までは、どんな特定の金額についても記入できるけれども、小切手は、振替可能性が非常に限られており、かつ物理的な機関から供給を受けなければならない。紙をベースとする小切手振出しシステムは、現金取引の制限を十分に緩和せず、小切手を処理することに関連付けられた固有な遅延を追加すると同時に通貨を取扱うことの不都合の多くを共有する。この点で、経済取引は、改良されたセキュリティを求めると同時に、より低いコストでのより大きな便宜を求めて努力している。

自動化は、コンピュータ化された電子資金振替（“EFT”）システムを通して大きな取引に対するこれらの品質をある程度は達成した。電子資金振替は、本質的に銀行制度の集中コンピュータ取引を通して達成される価値交換の処理である。EFTサービスは、大きな商業組織によって主に用いられる、電子“小切手”を利用する支払いの振替である。

自動決済機構（ACH）及び販売時点（POS）システムは、近年における実質的基準で小売り及び商業組織によって用いられるようになった電子資金振替システムの例である。しかしながら、これらの型のEFTシステムを通して行われる支払いは、銀行組織なしにそれらを実行することができないという点で限られている。更に、ACH取引は、業務外時間中に通常実行することができない。

ホームバンキング請求書支払いサービスは、支払いを行うために個人によって用いられる電子資金振替システムの例である。現在、ホームバンキング構想は、ほとんど顧客を見出していない。パーソナルコンピュータを用いて電話回線上で支払い、口座取引及び情報に対するサービスを提供する銀行では、銀行の顧客の1%未満がサービスを用いている。ホームバンキングが成功した製品ではない一つの理由は、顧客がこの型のシステムでは必要に応じて貨幣を預金及び引出しできないからである。

小売り業者の口座と顧客の口座の間のような、口座間で貨幣を取引するためにオンラインシステムで用いられる、現行のEFTシステム、クレジットカード、キャッシュカードは、バンキングシステムの外で汎用的に受け入れられる経済価値の振替を与える自動取引システムに対する必要性を満たすことができない。更に、クレジット及びキャッシュカードシステムは、不正に対して一般的に安全ではなくかつ適切なプライバシーを与えるものではない。

振替を仲介することをバンキングシステムに要求せず、かつある形の経済価値を提供できる、自動で、しかもより便利な取引システムを実行するために、オフライン電子資金振替に向かう傾向があった。例えば、通常の通貨及び小切手型の支払いシステムに対する代替としてキャッシュレス支払い取引において用いることができるある形の“電子マネー”

10

20

30

40

50

に対して多数のアイデアが提案されている。“METHOD AND APPARATUS FOR IMPLEMENTING ELECTRONIC CASH”という発明の名称の米国特許第4,977,595号公報、及び“MODULAR FUNDS TRANSFER SYSTEM”という発明の名称の米国特許第4,305,059号公報を参照のこと。

更によく知られた技術としては、所与の金額について購入されかつ特定の目的に対してそれから前払い価格を控除をできる磁気ストライプカードがある。経済価値の消耗により、カードは、破棄される。他の例としては、価値を示す情報を繰り返し記憶させることができ、この価値が特定の目的に対して同様に控除されるように構成された通称スマートカードまたはメモリカードがある。

しかしながら、これらの提案されたシステムは、貨幣としての銀行預金の重要性と、発行されうる汎用的に受け入れられるマネー表示であればどんな形式のものでもバックできることの必要性を十分に認識できていないものである。これらのシステムでは、電子的であれ、紙であれ、経済価値の表示は、それらの資産に対する見返りとしての等価負債の保証なしで発行される。

10

これらの提案されたペーパーレス支払いシステムのいずれも、仲介するシステムなしで、加入者間で、電子資金またはマネーを加入者が振替できるようにする自動装置を含むだけでなく、電子マネーによって表示された価値を発生し、システム内のマネーバランスを維持するために設けられた銀行及び金融機関の電子マネー口座を決済しかつ支払うための全バンキングシステムを備え、包含する多目的電子マネーシステムを実行できるほど十分に包括的ではない。

それゆえに、金融機関の仲介なしで支払元から支払先への共通した経済的為替取引を許容し、かつ個人への支払い過程の管理を与えるシステムに対する必要性が存在する。更に、現行EFTシステムの制限を有さない、あらゆる大きさの商業的支払いに対して大きな組織によって用いることができる経済的為替取引のシステムを与えることに対する必要性が存在する。

20

ここで参考文献として採り入れられる、本出願人に譲渡された1991年11月15日に出願の、米国特許出願第07/794,112号には、上述した、及び他の従来技術の制限を克服することができ、通常の現金と交換可能でありかつ汎用的に受け入れられる電子マネーを利用する完全な電子マネーシステムを提供できる電子マネーシステム（EMS）が記述されている。この発明によるEMSは、加入者の間、金融機関の間、及び加入者と金融機関の間で、通貨及びクレジットを含む経済価値を安全かつ確実に振替る方法及びシステムを提供する。また、EMSは、多種通貨の形式における電子マネーを与える。それにも係わらず、安全性かつ現実性の最優先は、EMSに対する更なる向上の必要性を生成する。

30

従って、本発明の目的は、再使用、複製及び偽造から守られた経済取引に対する向上したEMSシステム及び関連方法を提供することである。

本発明の別の目的は、紛失マネーを請求するためのシステム及び処理を提供することである。

本発明の更に別の目的は、購入者から品物の小売り業者へのマネーのリアルタイム振替に対して確実にかつ安全に使用されうるユーザフレンドリな電子支払いシステム及び方法を提供することである。

本発明の上記目的及び効果は、本発明によって達成することができるものの例示であり、すべてを記述したものではなく、また、認識することができる可能な効果を制限することを企図するものでもない。それゆえに、本発明のこれら及び他の目的及び効果は、ここに実施されたもの、または当業者において自明でありうるあらゆる変更を考慮して修正を加えられたものの両方を含む意味で、この記述から自明であるかまたは本発明を実施することにより学ぶことができるものである。従って、本発明は、ここに示しかつ説明した新規な方法、構成、組合せ及び改良にある。

40

発明の要約

上記、及び他の目的を達成するために、本発明の方法及び装置は、（１）要求払い預金及び電子クレジット授權によって裏付けられた電子通貨を含んでいる電子マネーを発生し、加入している顧客に対して発行するためのマネー発生装置に連結された銀行または金融機

50

関；（２）電子マネーを受入れかつ分配するコルレス銀行；（３）電子マネーを記憶し、参加銀行のオンラインシステムでマネー取引を実行するため、またはオフライン取引における他の類似する取引装置と電子マネーを交換するために加入者によって用いられる複数の取引装置；（４）発行銀行及びコルレス銀行に取引装置をプロセスハンドリングしかつインターフェイスし、かつ発行銀行及びコルレス銀行自体の間でインターフェイスするために、発行銀行及びコルレス銀行に関連付けられた、テラー装置；（５）異なる発行銀行の電子マネー口座をバランスするための決済銀行；（６）システムの全てのコンポーネントに通信サービスを与えるためのデータ通信ネットワーク；及び（７）システムの完全性を維持し、かつシステム内の偽造及び不正変更を発見するためのセキュリティ構成を有している電子マネーシステムの形式の好ましい実施例を採り入れる。

10

好ましい実施例では、マネー発生装置、取引装置、及びテラー装置の機能は、互いにネットワークされうる不正変更されないコンピュータハードウェア及びアプリケーションソフトウェアモジュールの組合せによって実行される。情報は、不正検査からの保証を与えるために暗号化された形式で伝送される。電子マネーは、有効化、及び変更また偽造からの保証を与えるべくデジタル署名で伝送される。

これらの装置によって交換された電子マネーは、通貨またはクレジットの電子表示でありうる。電子通貨の重要な形態は、それが銀行ノートと等価なものでありかつ発行銀行における預金に対する引き出し要求を通して通常の紙幣と交換可能であるが、発行銀行及びコルレス銀行の両方において引出しまたは預金できるということである。しかしながら、発行銀行だけが電子通貨を発生することができ、かつその償還に対して責任がある。

20

発行銀行は、今日の銀行産業によって現在実行されているように、銀行システムにおけるマネーバランスを維持するために銀行間決済及び支払い処理を後で利用する。

電子マネー表示は、代替可能であり、汎用的に受け入れられ、かつ発行銀行から申し分なく償還可能である、即ち、それらは、マネー取引の特性を有する。電子マネーシステムの保全性を保存するために、電子マネーの各交換は、他の情報と一緒に、クレジットまたは通貨のマネー単位、（即ち、ドル、円、等）、クレジットまたは通貨の単位の金額、電子クレジットまたは通貨を発行している銀行及び複数のデジタル署名、を識別するデータを含む。

本発明の広い態様によれば、電子マネーシステムは、現金取引の代わりに銀行の要求払い預金、及び電子クレジット授權によって裏付けられた電子通貨を含んでいる電子マネーを利用する取引を提供する。本発明の実施例では、EMSは、電子マネーを発生するためのマネーモジュール；電子マネーを発行、分配、及び受け入れるためのマネーモジュール；及び他の受け入れマネーモジュール間及び受け入れマネーモジュールと発行マネーモジュール間で電子マネーを受け入れ、記憶し、かつ振替るためのマネーモジュールを備えている。

30

本発明の更なる態様によれば、電子マネーシステムは、銀行の預金の債権及び電子クレジット授權を通して通常のマネーと相互交換可能な電子通貨を含む電子マネーを実行しかつ維持するために設けられている。

本発明の実施例では、システムは、複数の発行銀行；電子マネーを生成するための発生器モジュール；電子マネーの受け入れ及び分配を含む取引のようなテラー取引を実行し、他のテラーモジュールと相互作用させるために、発生器モジュールに結合されたテラーモジュール；電子マネーシステムの全体としての保全性を与えるためのセキュリティシステム；個別の発行銀行の電子マネー口座をバランスし、かつ発行銀行によって発行された電子マネーを決済するための決済及び支払い処理；及び取引モジュール間及び取引モジュールとテラーモジュールの間で電子マネーを振替るための、承認されたユーザにより所有される複数の取引モジュール；及び紛失マネーのクレームを処理し、かつ銀行アクセスを与えるべくマネーモジュールに口座を連結するための顧客サービスモジュールを含む。

40

本発明の別の形態によれば、発生器モジュール、取引モジュール、テラーモジュール、及び顧客サービスモジュールの機能は、互いにネットワークされうるいたずらよけコンピュータハードウェア及びアプリケーションソフトウェアの組合せによって実行される。

50

発行銀行またはクレジット授権における要求払い預金によって裏付けられた通貨の電子表示でありうる、これらのモジュールによって交換される電子マネーは、無権限変更または偽造からのセキュリティを与えるべくデジタル署名と共に伝送されうる。好ましい実施例では、偽造及び不正変更からの保証は、また、電子マネーのモジュール及び個々のユニットに周期的に書換えられるように要求することによって供給される。モジュール間のノートの移転は、ノート移転履歴照合を容易にすべくシーケンス識別番号を含むのが好ましい。オフエンディングモジュールまたは偽造電子マネーは、それらが発見されると直ぐに流通から除去することができる。

また、本発明の更なる形態によれば、紛失マネーを請求するための方法が提供され、それにより取引モジュール所有者／保持者は、顧客サービスモジュールを介して銀行組織に請求を提出しうるし、かつ銀行組織によるノート移転履歴照合に続いて、所有者／保持者は、請求された紛失ノートを回復しうる。

10

本発明の更なる形態は、マネーモジュールにおける各クレジット口座に対して一つのクレジットノートのみが存在するようにクレジットを更新するための取引モジュールに対する方法を提供する。

また、本発明の好ましい形態によれば、商人から品物を安全かつ確実に購入するために取引モジュールの所有者／保持者に対する方法が提供される。

【図面の簡単な説明】

本発明の更なる形態、特徴、及び効果は、本発明が添付した図面に関連してなされた以下の説明に照らして考慮される場合に理解されかつより容易に明らかになるであろう。

20

図1Aは、EMSセキュリティ階層構造を示す図である。

図1Bは、主要セキュリティサーバと通常のセキュリティサーバの間のセキュリティネットワーク通信を示す図である。

図2は、EMSに対するセキュリティネットワーク構成を示す図である。

図3Aは、セキュリティサーバの機能コンポーネントを示す図である。

図3Bは、ネットワークサーバの機能コンポーネントを示す図である。

図4Aは、顧客サーバモジュールの機能コンポーネントを示す図である。

図4Bは、主要セキュリティサーバの機能コンポーネントを示す図である。

図5は、ネットワークサインオン手順の概観を示す図である。

図6A-6Kは、ネットワークサインオンプロトコルを示す図である。

30

図7A-7Eは、EMSにおけるエスタブリッシュセッションプロトコルを示す図である。

図8A-8Bは、移転ノートプロトコルを示す図である。

図9A-9Dは、外国為替プロトコルを示す図である。

図10は、EMSにおけるモジュールに対する委任プロトコルを示す図である。

図11A-11Bは、EMSにおけるモジュールに対する中止取引プロトコルを示す図である。

図12A-12Cは、販売時点（POS）支払いプロトコルを示す図である。

図13A-13Bは、更新クレジット形式発行銀行プロトコルを示す図である。

図14は、設定クレジットプロトコルを示す図である。

図15A-15Bは、要求クレジットプロトコルを示す図である。

図16は、ノート移転履歴の例を示す図である。

40

図17は、ノート移転ツリーを示す図である。

図18A-18Cは、銀行アクセスプロトコルに対する銀行口座へのリンクマネーモジュールを示す図である。

図19A-19Cは、銀行口座プロトコルへの再確認マネーモジュールを示す図である。

図20は、有効口座番号プロトコルを示す図である。

図21A-21Bは、生成紛失ノート請求プロトコルを示す図である。

図22A-22Eは、請求紛失ノートプロトコルを示す図である。

実施例

本発明は、安全かつ確実に経済価値を変換するための電子媒体を用いている改良されたマネーシステムを提供する。システムは、新規のデータ処理システムを現行の世界中の銀行

50

組織で実行することができる他の手順と統合することによって実行することができる。本発明によれば、ここに参考文献として採り入れる、本出願人に譲渡された1991年11月15日出願の、米国特許出願第07/794,112号に開示された、電子マネーシステムに複数の型の改良が加えられる。これらの改良は、改良された外国為替 (F/X) 及び移転ノート取引処理、紛失マネーを請求するための処理、銀行アクセスに対するマネーモジュールをリンクするための処理、販売地点の支払いに対する処理、及びクレジットを更新するための処理を含んでいる一組のセキュリティ改良を含む。

セキュリティ

マネーシステムに対する有効セキュリティは、3つの特性を有する：偽造を禁止し、偽造を検出し、かつ偽造者を制止する。上記EMSは、3つの特性の全てを示すコンポーネントを有するべく設計される。偽造を禁止するために、マネーモジュールは、対称及び非対称キー暗号を用いて通信する。いかなるメッセージも明文ではない。モジュールのプロトコルは、また、不正防止ハードウェアによって物理的に保護される。

偽造は、ノート照合処理によって検出される。全システム時間プロトコル (例えば、ノート満期) は、電子ノートに規則的に照合されることを強制する。電子ノートは、また、銀行取引が実行される場合に新しくされる (即ち、新たな満期日を有する新たなノートで置換される)。

マネーモジュールは、複製されたまたは偽造されたノートがそれらにタイバックされるならば、ブロックされる (例えば、不良IDリストに配置される)。また、これらのモジュールを通過したノートは、移転することを許されない。ノートが満了するかまたは最終的に銀行に預金されるので、複製または偽造ノートの移転は、制止される。更に、重要なシステムセキュリティ問題の場合には、EMSは、全地球的な証明更新を要求して、次にそれらがEMSネットワークにサインするときに取引マネーモジュールを含む、全てのモジュールに証明更新するように要求する。

次の改良の一覧表は、モジュール間の対話を聞いている立ち聞き者から全ての情報を保護することを意図している。全ての情報は、公開キー及びモジュール識別子でさえも、覆い隠される。改良されたセキュリティ特徴の一覧表は、以下のものを含む。

1) 図5を参照して以下に説明するように、だれもマネーモジュールをだますかまたは明文でその情報のいずれも妨害することができないようにネットワークサインオンを確保すること。

2) セキュリティサーバ、マネー発生器、及びテラー識別子を割り当てる方法を生成すること (モジュール番号付けスキームを参照)。

これらの識別子は

a) セッションを確立すること (図7参照) ;

b) ノートを移転 (転送) することー移転記録をチェックする (図8参照)

でチェックされる。

3) 全てのモジュールは、主要セキュリティサーバの公開キー、及び全ての他のモジュールを証明するセキュリティサーバを運ぶような、主要セキュリティサーバを含んでいる、2層セキュリティサーバ構成 (セキュリティ階層構造及びセキュリティネットワークを参照) を実行すること。

4) 支払いのノートまたは外国為替 (F/X) を受け入れる前に全ての移転に対して不良ID一覧表をチェックし、かつ複製ノートをチェックするために移転ノートを改良すること (図8参照)。

5) セキュリティサーバの非公開キーを用いて全ての証明を暗号化すること (証明構成及び有効化参照)。

6) 動的に公開キーの大きさを変化させること (セキュリティネットワーク及び図6参照)。

7) 故障がマネーの複製を生じないようにコミットプロトコルを変更すること (図10参照)。

8) マネーを受け取りマネーを送らないことによって、確実にごまかしを行うためにコミ

10

20

30

40

50

ットを妨害することを、いずれのパーティもできないようにするために、F/Xを変更すること（図9参照）。

9) 支払人がコミットするが受取人がアボートした場合に、失敗したコミットに情報をログするためにアボートを変更すること（図11参照）。

10) 必要に応じて地球的証明更新ができるようにすること（セキュリティネットワーク及び図6参照）。

セキュリティ改良の上記一覧表は、本発明の強化されたセキュリティシステムによってもたらされるセキュリティ特性の幾つかを挙げたものである。これら及び他の改良は、EMSに対するセキュリティシステムの代替の好ましい実施例のそれに続く詳細な説明から更に理解することができるであろう。

セキュリティ階層構造

本発明によれば、EMSシステムセキュリティに対する別の実施例は、次のように構成できる。図1Aを参照すると、EMSは、主セキュリティサーバ1182及び通常セキュリティサーバ1184の二つの型のセキュリティサーバを有する。主セキュリティサーバ1182は、（通常）セキュリティサーバ1184を証明する。セキュリティサーバ1184は、システムの全ての他のモジュール（取引MMs1186、テラーMMs1188、マネー発生器モジュール1190、及び顧客サービスモジュール1192）を証明する。

主サーバ1182は、他の主サーバ1182またはセキュリティサーバ1184とだけ対話する。図2を参照すると、主セキュリティサーバ1182は、セキュリティLAN1194によって互いに接続された安全なファシリティに収容される。LAN1194は、セキュリティネットワーク1196に安全なゲートウェイを通して接続される。セキュリティサーバだけがこのネットワークで通信する。全てセキュリティサーバは、物理的に保護された装置である。

セキュリティサーバ1184は、EMSネットワーク1198及び銀行ローカルネットワーク1200にも取り付けられている。セキュリティサーバは、それらが偽造されたかのように取り扱われ、他のすべてのモジュールとの対話により有効にされる。

セキュリティサーバ1184及びモジュールのみが証明を有する。主セキュリティサーバの公開キーは、これらの装置によって運ばれる。二つの型の証明が存在する：セキュリティサーバ及びモジュール。

証明構成及び有効化

証明の構成は、次に示す通りである：

$$\text{Cert}(\text{SS}) = E_{\text{PSS}} [\text{SS}(\text{id}) \parallel \text{SS}(\text{PK}) \parallel \text{満了日} \parallel$$

$$\sigma_{\text{PSS}}(\text{X})] \parallel [\text{PSS}(\text{id}) \quad \text{XOR} \quad \text{C}]$$

$$\text{-----X-----}$$

$$\text{Cert}(\text{M}) = E_{\text{SS}} [\text{M}(\text{id}) \parallel \text{M}(\text{PK}) \parallel \text{満了日} \parallel \sigma_{\text{SS}}(\text{Y})] \parallel$$

$$\text{Cert}(\text{SS})$$

$$\text{-----Y-----}$$

証明有効化プロトコルは、：

1) Cert(SS)を有効化する

a) $\text{PSS}(\text{id}) = [\text{PSS}(\text{id}) \text{ XOR } \text{C}] \text{ XOR } \text{C}$

b) $D_{\text{PSS}}(E_{\text{PSS}}(\text{X} \parallel \sigma_{\text{PSS}}(\text{X}))) = \text{X} \parallel \sigma_{\text{PSS}}(\text{X})$

c) SS(id)が本物であるかどうかをチェックする（モジュール番号付スキーム参照）

d) 日付が有効かどうかチェックする

e) $D_{\text{PSS}}(\sigma_{\text{PSS}}(\text{X})) = h(\text{X})$ かどうかチェックする

2) Cert(M)を有効化する

a) Cert(SS)を有効化する

b) $D_{\text{PSS}}(E_{\text{SS}}(\text{Y} \parallel \sigma_{\text{PSS}}(\text{Y}))) = \text{Y} \parallel \sigma_{\text{PSS}}(\text{Y})$

10

20

30

40

50

c) $M(id)$ が本物であるかどうかをチェックする (モジュール番号付スキーム参照)

d) 日付が有効かどうかチェックする

e) $D_{PSS}(\sigma_{PSS}(Y)) = h(Y)$ かどうかチェックする

ここで、PSS=主セキュリティサーバ

SS=セキュリティサーバ

M=モジュール

$\parallel$ =連鎖

id=識別番号

h = ハッシュ関数

C = 全てのモジュールにより共有される一定の乱数

PK=公開キー (キーの長さを含む)

σ = デジタル署名 = Eh

Cert=証明

E = デジタル署名を暗号化しかつ生成するために用いられる非公開キーを有するアルゴリズム

D = デジタル署名を暗号解読しかつチェックするために用いられる公開キーを有するアルゴリズム

他のアプリケーションに応用される場合にノート E 及び D もまたそれぞれ暗号解読及び暗号化に用いられる。

主セキュリティサーバ1182、セキュリティサーバ1184、テラマネーモジュール1188、マネー発生器モジュール1190、顧客サービスモジュール1192、及び取引マネーモジュール1186は、番号を真偽についてチェックすることができるように識別番号 (id's) が割り当てられている。48ビット素数「p」が発生され、原始根 a についての p を法とする剰余演算 (ここで、すべての $1 \leq n < p-1$ に対して $a^n \neq 1 (p)$ である) が、安全処理過程を通じて行われる。a 及び p の両方は、それらが製造される場合に主セキュリティサーバによって安全にシステムの全てのモジュールにロードされる。

スキームは、次に示すように作用する：

$a^n \equiv m (p)$ でありかつ

(1) $1 \leq m \leq 99,999$ であれば、n は、主セキュリティサーバの id として割り当てられ、

(2) $100,000 \leq m \leq 999,999$ であれば、n は、セキュリティサーバの id として割り当てられ、

(3) $1,000,000 \leq m \leq 6,999,999$ であれば、n は、テラマネーモジュールの id として割り当てられ、

(4) $7,000,000 \leq m \leq 9,999,999$ であれば、n は、テラマネー発生器モジュールの id として割り当てられ、

(5) $10,000,000 \leq m \leq 11,999,999$ であれば、n は、顧客サービスモジュールの id として割り当てられ、

(6) $m \geq 12,000,000$ であれば、n は、取引マネーモジュールの id として割り当てられる。

モジュールまたはサーバが証明を有効化しているならば、それは、 $a^n \equiv m (p)$ を計算することによって識別番号 (例えば、 $M(id)$ 、 $SS(id)$ 、または $PSS(id)$) n の真偽をチェックしそして m が正しい範囲にあるかどうかをチェックする。

セキュリティネットワーク

図2に示すように、セキュリティネットワーク1196及びセキュリティLAN1194は、セキュリティサーバ1184を主セキュリティサーバ1182に接続する。セキュリティサーバ1184は、製造においてマネーモジュール及び顧客サービスモジュール1192を最初に証明する。そのようなセキュリティサーバは、モジュール製造LAN1202に接続できる。それらは、不良id一覧表及びセキュリティサーバの一覧表並びにそれらの公開キー (パブリックキー) のようなセキュリティ情報をモジュールにパスする。不良id一覧表は、マネーモジュール、顧客サーバモジュール、及び取引から阻止されるセキュリティサーバの識別を包含する。こ

10

20

30

40

50

これらのモジュールの証明更新は、ネットワークサインオンフロー図に続いて記述される。

セキュリティサーバ1184は、製造において主セキュリティサーバ1182によって最初に証明される。そのような主セキュリティサーバは、セキュリティサーバ製造LAN1204に接続できる。図1Bを参照すると、セキュリティサーバ1184は、それらが他のモジュールにパスする種々のセキュリティ情報を受取る。セキュリティサーバは、それらが更新されたセキュリティ情報をパスするネットワークサインオンのような、EMSネットワーク1198及び銀行LANs1200に対するセキュリティサービスを供給する。セキュリティサーバ1184は、セキュリティネットワーク1196にわたり主セキュリティサーバ1182からこの情報を受取る。取引マネーモジュール1186は、ネットワークサーバ1206（NS）を介してEMSネットワーク1198と通信する。参加銀行は、テラマネーモジュール1188そしてたぶんそれらのLANs1200に接続されたマネー発生器1190を有する。

セキュリティネットワーク1196は、リンク暗号化される。更に、主セキュリティサーバ及びセキュリティサーバは、共通対称キー（セキュリティネットワーク暗号化キー）を共有する。このキーは、公開キー、キー交換により指定された主サーバ1182によって周期的に変更される。

不良id'sの一覧表は、指定された主サーバ1182によって維持される。一覧表は、参加銀行、法の執務管轄庁、及びシステムへの加入者との対話から累積される。

周期的にセキュリティサーバ及びモジュールに対する公開キーの長さは、変更される。キーの長さは、高いセキュリティレベルを維持するために通常長くされる。新しく指定されたキーの長さは、指定された主サーバによって主セキュリティサーバに通信される。新しい長さは、不要id一覧表が送られる場合または証明更新により主サーバによってセキュリティサーバと通信される。セキュリティの危険な違反の場合には、主セキュリティサーバは、汎用証明更新を呼出することができる。

各主サーバに対する公開キーの長さは、変わらない。主セキュリティサーバの実行及び撤去を計画するタイムテーブルが生成される。新しいサーバは、増加した取引量によりそれらが実行されない限りより長いキーを有するであろう。アクティブPSS公開キーの一覧表は、主セキュリティサーバによって生成されかつその非公開キー（プライベートキー）を有するサーバによってサインされる。一覧表は、次いで、他のセキュリティサーバに放送される。

図3Aは、セキュリティサーバ1184の機能コンポーネントを示す。外部インターフェイス機能1208は、ネットワークインターフェイスングに対する通信層を供給する。セッションマネージャ機能1210は、取引セッションのセキュリティ形態を制御する。ネットワークサインオン機能1212は、ネットワークサインオンに対するセキュリティ機能を管理する。生成証明機能1214は、あらゆるマネーモジュールに対する証明を証明する（主セキュリティサーバでは、この機能は、セキュリティサーバを証明する）。分配証明となるキー機能1218は、有効主セキュリティサーバ公開キーの証明エージェンシーの一覧表をマネーモジュールに分配する（主セキュリティサーバは、また、汎用証明更新メッセージも分配する）。制御不良ID一覧表機能1220は、不良識別子の一覧表を制御しかつ分配する。同期日付／時間機能1222は、システム時間に同期されたマネーモジュールクロック／タイマサービスを保持する。クロック／タイマ1224及び暗号化機能1226は、マネーモジュールにおけるそれらの機能と同じである。

図3Bは、ネットワークサーバ1206の機能的コンポーネントを示す。外部インターフェイス機能1228は、ネットワークインターフェイスングに対する通信層を供給する。通信セッションマネージャ機能1230は、マネーモジュール間、及びマネーモジュールとセキュリティサーバの間の通信セッションを管理する。ネットワークサインオン機能1232は、マネーモジュールネットワークサインオン処理を制御する。ルートメッセージ機能1234は、ルーティングメッセージに対するディレクトリサービスを提供し、サインオンの間中及びマネーモジュールセッションの間中メッセージルーティングを制御する。直接対銀行サービス機能1236は、参加銀行によって供給されたサービスに情報を供給する。暗号化機能12

10

20

30

40

50

38は、対称キー機能1240及び乱数発生器機能1242を供給する。対称キー機能1240は、ネットワークサーバ1206とネットワークをアクセスしているモジュールの間、及びネットワークサーバ1206とセキュリティサーバ1184の間でメッセージを暗号化する。乱数発生器機能1242は、暗号化キー及び有効化メッセージに対する乱数を発生する。

本発明によれば、別の安全処理コンポーネント、顧客サービスモジュール（CSM）1192が採り入れられるのが好ましい。CSMは、口座プロフィールを生成しかつ更新するために用いられるいたずらされない（不正操作防止）装置である。CSMsは、マネーモジュール及びセキュリティサーバにおいて見出されたような独自の証明を包含する。CSMsは、他のモジュール（例えば、セキュリティサーバ）を有する安全セッションを確立することができる。CMSは、顧客サービス代理及びオンライン銀行組織へのインターフェイスのためにホストを必要とする。

10

CSMは、二つの主機能を有する。第1に、CMSは、マネーモジュールが銀行口座をアクセスし、銀行口座へのマネーモジュールリンクを再有効化し、かつ口座番号を有効化することができるように口座プロフィールを生成する。これらの取引は、図18～20を参照して以下により完全に記述される。第2に、CMSは、ホスト顧客サービス代理からの要求に応じて紛失ノードを請求すべく機能し、それらは、図21及び図22にさらに詳しく記述される。CMSは、マネーモジュールと同じセキュリティ機能及びその識別子に対する番号の特別な範囲を有する（“Module Numbering Scheme”を参照）。CSMによるこれらの機能の性能は、テラーモジュールに対する有効化口座番号処理を簡略化する。

CSMを採り入れるEMSの実施例によれば、各銀行に対する口座プロフィール構成は、

20

-----X-----

に変わる。

ここで、M(id) = モジュール識別子

B(id) = 銀行識別子

LA = 口座番号及び口座の型（預金またはローン）の一覧表

σ_{CSM} = CSMの署名

Cert(CSM) = (CSM)の証明

|| = 連鎖

30

である。

そのようなプロフィールに対する有効化手順は、図20を参照して以下に記述する。

図4Aは、顧客サービスモジュール（CSM）1192の機能的コンポーネントを示す。外部インターフェイス3000は、顧客サービスモジュールホスト（CSMH）プロセッサ内の他の処理及び通信手段にCSMをインターフェイスする；セッションマネージャ3001は、CSMと取引マネーモジュールまたは顧客サービス代理の間の取引セッションを制御及びコミット（即ち、最終的に決定する）、または中止すべく作動する。生成口座プロフィール機能3002は、マネーモジュールに加入者の異なる銀行口座をアクセスさせる口座プロフィールを顧客口座情報から構築する。公開キー機能は、銀行口座プロフィールを証明しかつサインする。CMSが顧客サービス代理及びオンライン銀行組織にインターフェイスするためにホストを必要とするので対ホスト機能3006は、CSMアプリケーションとホストアプリケーションの間のデューティの分離を調停する。請求紛失ノート機能3008は、CSMが有効化しかつ発行銀行に分配する加入者紛失ノート請求に応答する。維持セキュリティ機能3004は、偽造マネーモジュールの一覧表を管理し、証明に適用し、クロックを同期し、かつ新しいデジタルキーの生成を管理する。クロック／タイマ3012及び暗号化機能3010は、マネーモジュールにおけるそれらの機能と同じである。

40

図4Bは、主セキュリティサーバ1182の機能的コンポーネントを示す。外部インターフェイス機能3020は、ネットワークインターフェイスングに対する通信層を供給する。セッションマネージャ機能3002は、それらが偽造されうるように扱われる、セキュリティサーバで、及び他の主セキュリティサーバでセッションのセキュリティ形態を制御する。生成証明

50

機能3024は、あらゆるセキュリティサーバに対する証明を生成する。分配証明となるキー機能3026は、証明エージェントの有効主セキュリティサーバ公開キーの一覧表をセキュリティサーバに分配する。分配セキュリティネットワークキー機能3032は、主セキュリティサーバの間でセキュリティネットワークキーを管理しかつセキュリティサーバに分配する。セット汎用証明更新機能3030は、汎用証明更新が要求されるかどうかを決定し（例えば、セキュリティの危険な不履行により）、かつ必要と思われる場合に汎用証明更新を呼出す。分配不良ID一覧表機能3028は、不良識別子の一覧表を制御しかつ分配する。クロック／タイマ3034及び暗号化機能3036は、マネーモジュールにおけるそれらの機能と同じである。

ネットワークサインオン

ネットワークサインオン手順の概観は、図5を参照して供給される。サインオンプロトコルは、モジュール1243が再証明、預金、引出し、または他の理由に対するEMSネットワーク1198へのアクセスを所望する状況を記述する。モジュール1243は、取引マネーモジュール1186、テラマネーモジュール1138、マネー発生器モジュール1188、または顧客サービスモジュール1192でありうる。（a）モジュール1243とネットワークサーバ1206の間に通信を確立する。（b）モジュールの証明をネットワークサーバ1206へパスする。（c）ネットワークサーバ1206は、乱数有効化番号V及び乱数キーKを発生する；ネットワークサーバは、次いで、モジュールの証明、V、及びKを、セキュリティサーバ1184へパスする（NS/SSキーによって暗号化される）。（d）モジュール1243及びセキュリティサーバ1184は、（セッションキー（MM/SS）を介して）安全通信セッションを確立する。（e）セキュリティサーバ1184は、時間／日付、更新不要ID一覧表、主セキュリティサーバ公開キーの更新一覧表、公開キーの長さ、汎用再証明（必要ならば）、及び再証明されたモジュール証明（必要ならば）をパスする。（f）モジュール1243を有するセッションを終了しかつV及びKをモジュール1243へ送る。（g）KでVを暗号化しかつネットワークサーバ1206へ送る。（h）ネットワークサーバ1206は、モジュール1243へネットワークサインオンを肯定応答する。（i）モジュール1243は、それが接続されることを望む宛先（もしあれば）のネットワークサーバ1206を次いで報告する。（j）ネットワークサーバ1206は、宛先への接続を確立する。

ネットワークサインオンは、だれもモジュール1243をだますかまたは明文のその情報のいずれかを妨害することができないように設計される。図6は、ネットワークサインオン手順の詳細のフローを記述する。

通信Aは、EMSネットワーク1198との通信を確立する（ステップ1244）。維持セキュリティAは、その証明をネットワークサーバ1206へ送る（ステップ1246）。NSネットワークサインオンは、証明を受取る（ステップ1248）。NS乱数発生器は、乱数キーK及び乱数有効化番号Vを発生する（ステップ1250）。NS対称キーは、NS/SSキーでモジュールの証明、K及びVを暗号化する（ステップ1252）。NS/SSキーは、ネットワークサインオンに対して通信するネットワークサーバ1206及びセキュリティサーバ1184に設置された局所対称キーである。NSネットワークサインオンは、証明、K及びVをセキュリティサーバ1184へ送り、そこでSSネットワークサインオンは、メッセージを受取りかつSS対称キーは、メッセージを暗号解読する（ステップ1254－1258）。SSネットワークサインオンは、K及びVを記憶してモジュール証明を有効化のためにSS公開キーへ送る（ステップ1260－1264）。再証明の可能性を許容するために、SS公開キーは、モジュール証明の有効化を決定することにおいて満了日を考慮しない。

モジュール証明が有効でなければ、SSネットワークサインオンは、ネットワークサーバ1206及びモジュール1243への伝送に対するアクセスを否定するためにメッセージを生成する（ステップ1266）。SS公開キーは、モジュールの公開キーでモジュール1243へのメッセージを暗号化しかつSSセッションマネージャは、ネットワークサーバへメッセージを送る（ステップ1268－1270）。NSネットワークサインオンは、メッセージを受取りかつアクセスが否定されたことに気付く。暗号化されたメッセージは、次いでモジュールへ送られ、かつネットワークサーバは、切断する（ステップ1272）。セッションマネージャAは、

10

20

30

40

50

メッセージを受取り、公開キーAは、メッセージを暗号解読し、かつセッションマネージャAは、サインオンが否定されたということに気付く（ステップ1274-1278）。サインオンを要求している装置が取引マネージャモジュールであれば、対加入者Aは、加入者に報告する（ステップ1280-1282）。さもなければ、対銀行Aは、銀行に報告する（ステップ1284）。

他方、モジュールの証明が有効であれば、SS制御不良ID一覧表は、モジュールのidが不良id一覧表にあるかどうかをチェックする（ステップ1286-1288）。idが一覧表にあれば、ネットワークアクセスは、否定される。さもなければ、SS乱数番号発生器は、乱数R及び有効化メッセージを生成する（ステップ1290）。SSネットワークサインオンは、R及びA'sの公開キーを用いてSS公開キーによって暗号化されるメッセージにおける有効化メッセージをアセンブルする。公開キーAは、また、セキュリティサーバの証明を付加することによってこの暗号化されたメッセージを増大する（ステップ1292-1294）。メッセージは、公開キーAがメッセージを暗号解読しかつセキュリティサーバの証明を有効化するときのAに送られる（ステップ1298）。

証明が無効であれば、Aは、セッション終了に気がつきかつ加入者または銀行のいずれかに報告する（ステップ1304-1306）。証明が有効であれば、維持セキュリティAは、セキュリティサーバのidが不良id一覧表にあるかどうかをチェックする（ステップ1308-1310）。一覧表にあれば、セッションは、終了される（ステップ1300-1306）。一覧表になれば、乱数発生器Aは、乱数R（A）を生成する（ステップ1312）。維持セキュリティAは、操作R（A） XOR Rによってセッションキー（MM/SS）を形成しそしてセッションキーを記憶する（ステップ1314）。

有効化メッセージ及びR（A）を含んでいるメッセージは、アセンブルされかつセキュリティサーバの公開キーで暗号化される（ステップ1316）。セッションマネージャAは、メッセージをSSネットワークサインオンへ送るかつSS公開キーは、メッセージを暗号解読する（ステップ1318-1322）。

SSネットワークサインオンは、有効化メッセージがそれが生成されたものであるということの有効化する（ステップ1324-1326）。そうでなければ、セキュリティサーバは、ネットワークアクセスを否定する。有効化メッセージが正しければ、SS対称キーは、R（A） XOR Rによってセッションキー（MM/SS）を形成する（ステップ1328）。SSセッションマネージャは、セッションの開始に気がつきかつセンドメッセージサブルーチンによって肯定応答をAに送る（ステップ1330-1332）。セッションマネージャAは、肯定応答を受取りかつセッションの開始に気付く（ステップ1334）。

クロック／タイマAは、時間及び日付を、それをセキュリティサーバに送るセッションマネージャに送る（ステップ1336-1340）。SS同期日付／時間は、時間及び日付を受取りかつそれがパラメータ内であるかどうかをチェックする（ステップ1342-1344）。パラメータ内でなければ、SS同期日付／時間は、新しい時間及び日付をセッションマネージャAに送る（ステップ1346-1350）。チェック／タイマAは、次いで時間及び日付を調整する（ステップ1352）。Aは、次いでその日付及び時間を再チェックのためにセキュリティサーバに再送付する。クロック同期がセット回数よりも多く試みられたならば、クロック障害は、加入者または銀行へ報告され、もし望ましいならば再試みされうる（ステップ1354-1362）。

しかしながら、時間及び日付がパラメータ内であれば、SSネットワークサインオンは、不良id一覧表、主セキュリティサーバ公開キー（分配証明となるキー機能からくる）の新しい一覧表、及び公開キーの長さ（公開キーの大きさは、周期的に変化する）を含んでいるメッセージをアセンブリする（ステップ1364）。SS生成証明は、汎用再証明が呼出されたかどうかをチェックし、かつ汎用再証明に対する期間が満了していないことを確実にする（ステップ1366-1368）。そのような期間は、全ての証明が再証明されるかまたは満了するように十分に長くなければならない。機能は、また、それが汎用再証明の期間中に証明されたならば、再証明の必要がないので、モジュールが最後に再証明された場合をチェックすべきである。

10

20

30

40

50

再証明が必要であれば、SS生成証明が先のメッセージに加えられる：モジュールは、再証明すべきである（ステップ1370）。そして、再証明が呼出されたかどうか、SS公開キーは、メッセージをサインする（ステップ1372）。メッセージは、公開キーAがメッセージ上のデジタル署名をチェックするところのAに送られる（ステップ1374-1378）。署名が無効であれば、セッションは、終了される。維持セキュリティAは、次いで、その不良id一覧表、公開キー一覧表、及びキーの長さを更新する（ステップ1382）。

モジュールAは、次いで（汎用再証明オーダーによるかまたは期限切れ証明によるかのいずれかにより）その証明が再証明されることを必要とするかどうかをチェックする（ステップ1384-1386）。新しい証明が要求されるならば、維持セキュリティAは、新しい証明の発生を始める（ステップ1388）。公開キーAは、新しいキーを発生しかつその古い非公開キーで新しい公開キーにサインする（ステップ1390）。セッションマネージャAは、サインした新しい公開キーをセキュリティサーバのSS証明に送る（ステップ1392-1396）。次いで、SS公開キーは、新しい公開キー上の署名を有効化する（ステップ1398-1400）。有効な署名でないならば、セキュリティサーバは、ネットワークアクセスを否定する。署名が有効ならば、SS公開キーは、モジュールの新しい証明にサインしかつそれをモジュールに送る（ステップ1402）。セッションマネージャAは、証明を受取り、維持セッションAは、証明を有効化することを引受け、かつ公開キーAは、署名を有効化する（ステップ1404-1410）。

証明が有効でないならば、セッションマネージャAは、センドメッセージ機能によって“証明無効”メッセージ及び証明をセキュリティサーバへ送る（ステップ1412-1413）。SSネットワークサインオンは、メッセージを受取りかつSS公開キーは、署名を有効化する（ステップ1414-1418）。セキュリティサーバは、証明が実際に有効であるということを決めたならば、それは、ネットワークへのモジュールアクセスを否定する。しかしながら、証明が無効であれば、SSセキュリティマネージャは、それがネットワークから切断されるということをネットワークサーバに報告する（ステップ1420）。NSネットワークサインオンは、障害をモジュールに報告する（ステップ1422）。モジュールは、次いで再試みに対して加入者または銀行に照会する（ステップ1424-1432）。

他方、モジュールがその新しい証明が有効であるということを決めたならば、セッションマネージャAは、肯定応答をセキュリティサーバに送る（ステップ1434）。同様に、新しい証明が要求されないならば、維持セキュリティAは、肯定応答メッセージをセキュリティサーバに送る（ステップ1436-1438）。いずれの場合においても、SSセッションマネージャは、肯定応答を受取りかつモジュールでそのセッションの終わりに気付く（ステップ1440）。SSネットワークサインオンは、次いでK及びVをAに送る（ステップ1442-1444）。セッションマネージャAは、メッセージを受取りかつ対称キーAは、V及びKを有する宛先を暗号化しかつメッセージをネットワークサーバへ送る（ステップ1446-1448）。NSネットワークサインオンは、メッセージを受取りかつNS対称キーは、メッセージを暗号解読しかつVがそれが先に生成したものと同一Vであるかどうかをチェックする（ステップ1450-1454）。

Vが正しくないならば、NSネットワークサインオンは、アクセス否定メッセージをAに送りそして切断する（ステップ1456-1458）。Vが正しいならば、NSネットワークサインオンは、宛先へのリンクを確立しかつ肯定応答をAに送る（ステップ1460）。そして、セッションマネージャAは、肯定応答を受取りかつAがEMSネットワーク1198にサインオンされたということに気付く（ステップ1462）。

セッション確立

図7はセッションプロトコールを示す。セキュリティ維持Aはセッションマネージャへモジュール有効化を送り、そしてセッションマネージャAはその有効化を受け、そしてマネーモジュールAがネットワークへ接続されているか、否かを調べる（ステップ1464-1466）。もしマネーモジュールAがネットワークへ接続されていないと、セッションマネージャAはセキュリティ維持Aから受けた有効化を行き先Bへ送る（ステップ1476）。又は、もしマネーモジュールAがネットワークへ接続されていると、対称キーAは有効化

10

20

30

40

50

をKで暗号に書き直し、そしてセッションマネージャAはその暗号に書き直した有効化をネットワークサーバーへ送る（ステップ1468-1472）。ネットワークサーバーはKでその有効化を解読し、そしてその有効化を行き先Bへ送る。

有効化を送ったのがネットワークサーバーであろうと、セッションマネージャAであろうと、そのことに係わりなくセッションマネージャBはその有効化を受取、そしてセキュリティ維持Bがその有効化を有効とする（もしBがセキュリティサーバーであれば、そのときはこの機能はセッションマネージャにより遂行される）（ステップ1480-1482）。もし有効化が有効でなければ、そのときはセッションマネージャBは、セッションが終了したことを確認し、そしてサブスクライバーもしくは銀行のどちらかに知らせる（ステップ1486-1492）（もしBがセキュリティサーバーであると、そのときはBはその取引が終了したことを確認するだけである）。

10

もし有効化が有効であれば、そのときはセキュリティ維持Bは、Aが不良idリストに載っているか、否かを調べる。もしもAが不良idリストに載っていると、そのときはセッションを終了する。もしもAが不良idリストに載っていないと、そのときは乱数ジェネレータBが乱数R（B）とB有効化メッセージとをつくる（ステップ1498）。クロックタイマーBは日時を回収する（ステップ1500）。セキュリティ維持BはR（B）、B有効化メッセージそして日時をメッセージに組み立てる（ステップ1502）。パブリックキーBはメッセージをAのパブリックキーで暗号に書き直し、そしてセッションマネージャBはBの有効化を暗号に書き直したメッセージへ加え、そしてそのメッセージをAへ送る（ステップ1504-1506）。

20

セッションマネージャAはそのメッセージを受け、パブリックキーAはそのメッセージの暗号に書き直した部分を解読し、そしてセキュリティ維持AはBの有効化を有効とする（ステップ1508-1514）。もし有効化が有効でなければ、そのときはセッションマネージャAはセッションの終了を確認して、サブスクライバーもしくは銀行のどちらかに知らせる（ステップ1516-1522）。もし有効化が有効であると、そのときはセキュリティ維持AはBが不良idリストに載っているか、否かを調べる（ステップ1524-1526）。もしもBが不良idリストに載っていると、そのときはセッションを終わらせる。もしBが不良idリストに載っていないと、そのときはセキュリティ維持Aが日時を回収し、そしてそれをBの日時と比較する（ステップ1528-1530）。もしも日時が範囲外であると、そのときはセッションを終わらせる。

30

もしも日時が範囲内であると、そのときは乱数ジェネレータAは乱数R（A）と有効化メッセージとをつくる（ステップ1532）。その場合セキュリティ維持AはR（A）XOR R（B）の演算によりセッションキーを形成する（ステップ1534）。A有効化メッセージ、B有効化メッセージ、日時そしてR（A）がメッセージとして組み立てられ、そしてBのパブリックキーで暗号に書き直す（ステップ1536）。メッセージはセッションマネージャAによりBへ送られる（ステップ1538）。セッションマネージャBはメッセージを受け、パブリックキーBがそのメッセージを暗号に書換え、そしてセキュリティ維持BがB有効化メッセージを調べる（ステップ1540-1546）。もしもB有効化メッセージが不正確であると、セッションを終了させる。もしもB有効化メッセージが正確であると、セキュリティ維持BはR（A） XOR R（B）によりセッションキーを形成する（ステップ1548）。日時を回収し、そしてAの日時と比較してその日時がそれぞれの既定の範囲内にあるか、否かを調べる。もしも日時が範囲外であると、そのときはセッションを終わらせ、その場合セッションマネージャBはセッションの開始を確認する（ステップ1552）。セッションマネージャBは確認とA有効化メッセージとをAへ送る（ステップ1554-1556）。セッションマネージャAはメッセージを受け取り、そしてセキュリティ維持AはA有効化メッセージを調べる（ステップ1558-1562）。もし有効化メッセージが正しくないと、セッションを終わらせる。もし有効化メッセージが正しいと、セッションマネージャAはセッションの開始を確認する（ステップ1564）。

40

ノート移転

図8はノート移転プロトコールを示す。ノートディレクトリーXは移転のノートと価値と

50

を選択し、ノート額とシーケンス番号とを更新し、それからメッセージをノートへ送る（ステップ1566）。移転のためのノートを選択するときを生じることのある目的は、（１）デジタル署名の数（これは処理時間を必要とする）の最小化、（２）パケットの寸法の最小化、（３）移転しているサブスクライバーへ残っている電子ノートの有効性を最大化する（すなわち満期までに残されている最短時間でノートをパスする）ことである。このような目的は以下のノート移転アルゴリズムにより達成される。（１）最小数のノートを含むすべてのあり得る選択肢を決定し、（２）これらの選択肢のどれが最小数の移転を有するかを決定し、（３）一つよりも多い選択肢がステップ２から残されていると、最小数の金融単位日を有しているものを選ぶ。金融単位日とは移転しようとするノートの残存価値とノートの満期まで残されている日数との積の、そのパケット内の総てのノートについて
10

の集計である。
ノートディレクトリXからのメッセージを受けたときノートXは、移転されている各ノートへ加えようとする移転をつくる（ステップ1568）。パブリックキーXはノートのための署名をつくる（ステップ1570）。その場合、パケットマネージャーXはそのノートと新規の移転とを組み合わせさせてパケットとし、そのパケットをYへ送る（ステップ1572－1574）。パケットマネージャーYはパケットを受取り、そしてそれを分解する（ステップ1576）。

Y有効化はノートにおけるすべての有効化を有効とする（例えば、マネージェネレータ有効化とすべての移転有効化）。その場合、移転グループ内の認識番号が、電子ノートの履歴にわたっての署名と有効化とのグループにおける有効化のモジュール認識番号と一致することを有効化Yは確認する。また、電子ノートの履歴を通して次々の移転で移される額が直前の移転の額よりも少ないことを確実にすることにより各ノートの移転額の一致性を有効としている。加えて、移転された全額を調べてそれが予期された額であることを保証する（ステップ1578－1580）。もしも無効であると、そのときは移転は行われない（ステップ1582）。

もし有効で、そしてYが取引マネーモジュールであると、そのときは有効化Yはノートの満期を有効化する（ステップ1584－1588）。ノートの何れかが満期となっていると、そのときはその取引は行われない。もしいづれも満期となっていないと、そのときは有効化Yは不良idリストでそのノートのトランスファーの個別のidを調べる（ステップ1590－1592）。もし何れかのノートのトランスファーの個別のidが不良idリストに載っていれば、そのときは取引は行われない。
30

もしトランスファーのidが不良リストに載っていなければ（もしくはYが取引マネーモジュールでないと）、そのときはパブリックキーYはノートの照明の有効性を有効化する（ステップ1594－1596）。もしも署名のうちのどれかが有効でないと、その取引は行われない。もし署名が有効であると、そのときはノートアプリケーションにより蓄積されている、もしくはトランログに入っているノートボディーとそのノートボディーが一致するかを有効化Yが調べる（ステップ1598－1600）。一致しているノートボディー毎にノート移転ツリーをつくって、ノート複製があったか、なかったかを決定する（ステップ1602－1604）。もしもノートのどれかが複製されていると、そのときは取引は行われない（すなわち、ステップ1602－1604）。この複製チェック（すなわち、ステップ1598－1604）は、偽造取引マネーモジュールを使用する「自己取引」によりノートを移すことによりマネーをつくらうとする個人の行為を阻止する。
40

複製がない、もしくはノートボディーの一致が認識されないと、そのときはノートYはノートをマネーホルダー内に置く（ステップ1606）。最後に、ノートディレクトリYはノートの位置と額とを更新し、そしてシーケンス番号を初期化する（ステップ1608）。

移転ノートプロセスはノートの調停を容易とするためシーケンス番号を更新し、そして初期化するステップを含み（「イッシュしたマネーの調停」参照）、いづれかのノートのトランスファーが不良idリストに載っているかどうかを調べ、そしてノート複製を調べる。これらの追加の特徴とステップとは、複製されたノートを当事者が導入し、循環させ、そして循環している複製ノートを検出する能力を高めるのを困難としている。
50

外国為替

ドルとポンドとを例としての貨幣単位として使用する外国為替取引のプロトコルを図9に示す。最初、 $\$/\pounds$ の為替レートでポンド（ $\pounds$ ）をドル（ $\$$ ）に変えることをAはBと契約する。その場合、AとBとは彼らのマネーモジュールに署名し、そしてモジュールは取引のそのタイプに対し加入者を誘導する（ステップ1604-1610）。Aは外国為替を買うことを選択し、そしてBは外国為替を売ることを選択する。AとBは安全な取引セッションを確立する（ステップ1616-1620）。

対加入者Aは、彼が交換を望んでいるドルのノートのタイプによる額をAの所有者／所持者に督促する（ステップ1622）。支払い／交換Aはその額を受取り、そしてノートダイレクトリーAはAが十分なファンドを有しているか、否かを調べる（ステップ1624-1628）。

10

もしファンドが十分でないと、そのときは対加入者Aは、既存のファンドに対して再びチェックされる新規な額を督促する（ステップ1630-1632）。もし新規の額が入れられなければ、そのときは取引は行われぬ（ステップ1634）。

もしファンドが十分であると、そのときは支払い／交換Aはドルの額をBへ送る（ステップ1636-1638）。その場合対加入者Bは、ドルに対して彼が交換を望んでいるポンドの額を選択してBの所有者／所持者を督促するか、もしくはドルに対する交換レートだけを促す（ステップ1640）。ノートダイレクトリーBは十分なファンドについてチェックする（ステップ1642-1644）。もしファンドが不十分であると、そのときは対加入者Bは新しいレートを督促し、そして再び既存のファンドが十分かをチェックする（ステップ1446-1648）。

20

しかしながら、新しいレートが選択されないと、そのときは支払い／交換BがAにその額のファンドが不十分であることを知らせる（ステップ1650-1652）。Aは交換の新しい額を選択するか、もしくは取引を中止する（ステップ1630-1634）。Bが取引に十分なファンドを有していると、そのときは支払い／交換BはAに確認と、交換しようとするポンドの額とを送る（均等レートも送る）（ステップ1654-1656）。対加入者Aはポンドの額とレートの有効化を督促する（ステップ1658-1660）。もし額とレートとが不正確であると、そのときは、支払い／交換AはBに、その額とレートとは不正確であることを告げる（ステップ1662-1664）。対加入者Bは新しいレートを督促する（ステップ1666-1668）。もし新しいレートが選ばれないと、そのときは取引は行われぬ（ステップ1670）。

もしAが取引の正確な額とレートとを有効化すると、そのときは、支払い／交換Aはドル額をマネーホルダーに渡す（ステップ1672）。ドルのノートはAからBへ移される（ステップ1674）。支払い／交換Bはポンドをそのマネーホルダーへ渡す（ステップ1676）。ポンドのノートはBからAへ移される（ステップ1678）。

30

取引のこの点でAとBとの両方が正確な外国為替レートを仮に保持している。AとBとはそれぞれが2つの取引に酸化している。Aの取引では、（1）AがドルをBに移転し、（2）AはBからポンドを受け取る。Bの取引では、（1）BがドルをAに移転し、（2）BはAからドルを受け取る。外国為替取引を完結するにはAはその2つの移転を両方とも今コミットしなければならない（すなわち、終わりにして、取引ログに永久に記録する）。同様に、Bもその2つの移転を両方とも今コミットしなければならない。Aは外国為替取引A→B（AからBへドル）をコミットし、そして別に、外国為替取引B→A（BからAへポンド）をコミットしてもよいことに注意されたい。同様にBは外国為替取引A→Bを、そして別に、外国為替取引B→Aをコミットしてもよい。

40

外国為替プロトコルの次の部分は、当事者のどちらも取引マネーモジュールがコミットする順序を知らないように設計されている。このような不確かさは当事者が取引で不正を意図的に働こうとするのを断念させる。背景として、ファンクションS（X）は、 $S(0) = A$ 、そして $S(1) = B$ となるように決められている。ここでAとBとはマネーモジュールAとBを言うものとする。こうして、もしXが0もしくは1にランダムに選択されると、マネーモジュールAとBはランダムに指示される。

以下のルーチンを使って、AとBとが共通にランダムXを確立する。R（A）とR（B）とはセッション確立サブルーチン中AとBとにより発生された乱数である。R（A）

X0 50

R R (B) のパリティは、(R (A) XOR R (B) の各ビットをエクスクルーシブオアすることにより) 決定される。このパリティは乱数 X である。X' は X のコンリメントである (X' = X XOR 1)。

図9を参照する。トランログ A は条件付きでその取引ログを更新して S (X) から S (X') への移転を記録する (ステップ1680)。もし X を計算して 0 となると、そのときは A から B への移転 (すなわち、ドル移転) が条件付きで記録される。もし X を計算して 1 となると、そのときは B から A への移転 (すなわち、ポンド移転) が条件付きで記録される。ログは条件付きで記録されるので、多くのマネーモジュール A が取引を中止する事態ではそれはロールバックされる。更新ログは、(流れ図に説明されているように、もしくはコミット中に暗黙で) ログ更新が一度無条件に設定されると永久となる。そのとき、セッションマネージャー A は「ログ更新」メッセージを B へ送る (ステップ1682-1684)。応答して、トランログ B も条件付きでそのログを更新し、S (X) から S (X') への移転を記録する (ステップ1686)。

もし X = 1 であると、トランログ B はログ更新を無条件にセットする (ステップ1688-1690)。こうして、この時点で B は A へのそのポンドの移転をコミットする。次に、B は図10を参照して説明するコミットプロトコールに従う (ステップ1692)。この状態で、A はその移転の両方にコミットし (すなわち、ドルを移転し、そしてポンドを受ける)、そして B は一つの未処理の (コミットされていない) 移転、すなわちドル受領をコミットする。

もし X = 0 であると (ステップ1688)、セッションマネージャー B は「コミット開始」メッセージを A へ送る (ステップ1694-1696)。そのとき、ログ A はそのログ更新を無条件に設定し (ステップ1698)、そのドル移転をコミットする。図10のコミットプロトコールが読みだされる (ステップ1700)。このプロトコール (後述する) 中、B はその両方の移転 (すなわち、ポンドを移転し、ドルを受領する) をコミットし、そして A はその未処理の移転、ポンド受領をコミットする。

理解されるように、F/X取引はノートの各移転をコミットし、ノートが複製されないようにし、そのような複製はコミットがただ一回だけだと起きることがえる。外国為替プロトコールは、誰の移転 (A のドルもしくは B のポンド) が最初コミットされるかは当事者のどちらも知らない。このことが取引で不正を働こうという気持ちを当事者に持たせないようにする。それぞれの移転が別個にコミットされるが、コミットの順序が2つのモジュールによりでたらめに選ばれる。取引に干渉しようとする第3者は金を失う確率は50-50である。また、その失われた金の返還を主張できるのでコミットに干渉しようという気持ちにはならない (紛失マネーの請求参照)。

コミット

図10は、モジュールのためのコミットプロトコルを示している。セッションマネージャ X は、レディーコミットメッセージを Y へ送る (ステップ1702-1704)。これにより、コミットオブリゲーションがそのメッセージを受信するモジュールへ通される。通常マネー移転シナリオにおいては、コミット義務を通すこの方法は、先ず、マネー複製の可能性を排除するように最初にマネーを移転する当事者がコミットすることを保証するために、使用される。

それから、セッションマネージャ Y は、確認を X へ送り (ステップ1706-1708)、その取引ログを更新することによって、未済の取引をコミットする (ステップ1710)。また、もし、Y が取引マネーモジュールであるならば、対加入者 Y は、その加入者に、取引がうまくいったことを通知する (ステップ1712-1714)。セッションマネージャ Y は、セッションの終りを確認する (ステップ1716)。

取引ログ X は、Y から確認を受信し、その取引ログを更新し、未済の移転をコミットする。X は、Y と同じようにしてそのコミットを完了する (ステップ1718-1724)。

取引中止

図11は、モジュールのための取引中止プロトコルを示している。セッションマネージャ X は、変化をロールバックして、その取引が中止されることを確認する (ステップ1726

10

20

30

40

50

）。それから、セッションマネージャXは、コミットレディーメッセージが送られたかをチェックする（ステップ1728-1730）。もし、そうならば、Xは、コミットレディーメッセージを送った後に中止されたXを記録し且つノート移転プロトコル中に受信された各ノートの額およびノート識別子を記録することによって、その取引ログを更新する（ステップ1732）。このようにして、中止プロトコルは、失敗コミットサブルーチン中に中止サブルーチンが呼び出される時の情報を記録する。

もし、Xが取引マネーモジュール1186であり、コミットレディーメッセージが送られた場合には、対加入者Xは、その加入者に、その取引が中止されたこと、およびマネー移転エラーがあったかもしれないことを知らせる（ステップ1734-1738）。

もし、Xが出納マネーモジュール1188であるならば、対銀行Xは、その銀行に、その勘定取引をリバースすべきこと（適当なデビットおよびクレジットによって）を知らせる（ステップ1740-1742）。もし、Xが取引マネーモジュール1186であり、コミットレディーメッセージが送られていない場合には、対加入者Xは、その加入者に、その取引が中止されたことを知らせる（ステップ1744）。

いずれの場合においても、セッションマネージャXは、Yに、その取引が完了され得ないことを示すメッセージを送る（ステップ1746-1748）。セッションマネージャYは、その変化をロールバックし、その取引が中止されたことを確認する（ステップ1750）。それから、Yは、その加入者に、その取引が中止されたことを知らせる（ステップ1752-1754）か、または、その銀行に、その勘定取引をリバースすべきことを知らせる（ステップ1756-1758）。

前述したように、もし、コミットプロトコル中に取引が中止される場合には、ノートが紛失する可能性がある。もし、このようなことが起こる場合には、移転先が中止したのに対して、移転元がノートの移転をコミットしたというようなことがありうる。この場合において、移転先マネーモジュールは、受信すべきであったノートについての情報を記録し、その加入者に、問題がありうること（すなわち、Aによって送られたノートを受信していなかったというようなこと）を知らせる。このような状況において、移転元マネーモジュールに関する限り、この移転元マネーモジュールは、正しくノートを移転したということが考えられる。

移転先マネーモジュール加入者は、そのマネーについてのクレイムを有効化エージェンシーに対してなすことができる。クレイム情報は、失敗した取引のログ記録を含む。有効化エージェンシーは、ノートが折り合いがついたかを知るために発行銀行でチェックすることができる。ある時間期間の後、もし、ノートが折り合いがついていない場合には、加入者は、自分のマネーをリクレイムすることができる。

POS支払い

図12は、販売時点（POS）支払いプロトコルを示している。POS支払いプロトコルは、買手の取引マネーモジュール1186と売手の取引マネーモジュール1186との間で行われる支払いを簡単化しようとしているものである。売手の取引マネーモジュール1186は、例えば、スーパーマーケットのキャッシュレジスタに配置されうる。

最初に、Aは、Bから物品またはサービスを購入することに同意する（ステップ1760）。取引マネーモジュールAの所有者／所持者は、自分のマネーモジュールにサインオンする（ステップ1762）。対加入者Aは、その所有者／所持者に取引を督促し、Aは、POS支払いすることを選択する（ステップ1764-1766）。一方、売手は、総購入価格を決定する（ステップ1768）。対加入者Bは、取引を督促し、Bは、POS支払いを受けることを選択する（ステップ1770-1772）。AおよびBは、保証セッションを確立する（ステップ1774-1776）。

対加入者Bは、支払い額を督促し、支払い／交換Bは、その額を受信し、それをAへ送る（ステップ1778-1782）。それから、対加入者Aは、その加入者に要求額を検証することを督促する（ステップ1784-1786）。さらにまた、加入者は、総額で要求額に等しくなるようにどのノートで（例えば、通貨またはクレジットで）どれくらいの額を支払うかを選択するように要求される。もし、要求額が正しくない場合には、支払い／交換Aは、Bに

10

20

30

40

50

、要求額が正しくないことを示すメッセージを送る（ステップ1788-1790）。それから、対加入者Bは、そのホストに新しい額を督促する（ステップ1792-1794）。もし、新しい額が選択されない場合には、その取引は中止される（ステップ1796）。

もし、要求額が正しい場合には、支払い／交換Aは、ノートのタイプによる額を受信する（ステップ1798）。それから、ノートディレクトリAは、十分なファンドかについてチェックする（ステップ1800-1802）。もし、ファンドが不足である場合には、対加入者Aは、ノートのタイプによる新しい額を督促する（ステップ1804-1806）。もし、新しい額が入力されない場合には、支払い／交換Aは、Bに、それがファンド不足であることを示すメッセージを送る（ステップ1808、1790）。対加入者Bは、ホストに新しい額を督促する（ステップ1792-1794）。もし、新しい額が選択されない場合には、その取引は中止される（ステップ1796）。もし、新しい額が選択される場合には、その支払い取引が再開される。

10

もし、ファンドが充分である場合には、支払い／交換Aは、その額をマネーホルダーへ通す（ステップ1810）。それから、ノートがAからBへ移転される（ステップ1812）。最後に、取引マネーモジュールがコミットする（ステップ1814）。

理解しうるように、POS支払いは、買手に対して簡単化される。何故ならば、それが被支払い人始動支払いであるからである。一般的に、POS支払いは、商品についての売手に対する支払いのために使用されるのに対して、加入者対加入者（STS）支払いは、各顧客支払い、または手形支払いのために使用される。

発行銀行からのクレジットの更新

20

図13は、発行銀行取引クレジット更新プロトコルを示しており、特に、加入者が予め許可されたクレジット支払い媒体であるクレジットノートを如何にして取得するかを記述している。加入者は、その加入者が所有する各クレジット勘定口座について1つまでのクレジットノートを保有しうる。加入者に更新クレジットノートを受信しうるようにするどの銀行もそれらのクレジットノートについて発行銀行である。

クレジット更新取引をセットアップするプロセスの流れは、マネーモジュールAと銀行の出納マネーモジュールBとの間のクレジットセットアッププロセスで始まり（ステップ1854）、それについては、図14を参照して以下に説明する。

クレジットセットアップ

クレジット引出しセットアッププロセスは、取引マネーモジュールAの所有者／所持者がクレジット更新をなすことを決定し、自分のマネーモジュールにサインオンするときに始まる（ステップ1876）。例えば、加入者Aは、クレジットノートを所有するが、そのクレジット額を、ゼロまで減少させることを含めて変更（例えば、増大または減少）することを望むかもしれないし、または、現在、クレジットノートを所有していないが、1つのクレジットノートを取得することを望むかもしれない。対加入者Aは、その所有者／所持者に取引を督促し、Aは、特定の銀行および勘定口座からの特定の額のクレジット更新をなすことを選択する（ステップ1878-1880）。この実施において、加入者によって指定されたクレジット額は、加入者Aが保有したい総クレジット額である。それから、取引マネーモジュールAは、前述したネットワークサインオン手順を通してそのネットワークにつながることにより、選択された銀行と通信するための手順を開始する（ステップ1882）。

30

40

マネーモジュールサインオン、取引選択およびネットワークサインオンのステップが完了した後、AおよびBは、保証セッションを確立する（ステップ1884）。それから、取引マネーモジュールAは、図15に関してより充分に説明されるクレジット要求手順にしたがって、出納マネーモジュールBからクレジット要求をなす（ステップ1886）。

クレジット要求

図15を参照して、クレジットを要求するプロセスについて説明する。図はXおよびYを当事者として示しているが、後述するプロセスステップにおいて、それらは、出納マネーモジュールと取引しするどのマネーモジュールにも適用されうる。

開始するのに、もし、選択された勘定口座に対するクレジットノートがある場合には、ノ

50

ートディレクトリXは、このクレジットノートの額を対出納Xへ送る（ステップ1897）。対出納Xは、加入者Aによって要求された総クレジット額とそのクレジットノート額との間の正味の差を決定し、クレジット更新要求を出納マネーモジュールへ送り、クレジットの特定の正味額が特定の勘定口座から許可されるように要求する。更新クレジット要求のその送信において、勘定口座番号および勘定プロフィールが、正味クレジット額と共に、要求マネーモジュールから出納マネーモジュールへと送信される（ステップ1898）。このメッセージは、メッセージ送出プロトコルに従って送出される（ステップ1900）。そのメッセージ送出プロトコルにおいては、そのメッセージは、記述した暗号化法を使用して暗号化される。

クレジット引出し要求および勘定口座番号およびプロフィールが出納マネーモジュールへ送信されるとき、勘定口座番号を確認する手順が開始される（ステップ1902）。勘定口座番号が如何にして確認されるかを示すフロー図を図20に示している。これについては、説明を簡単化するために以下に別に説明する。

勘定情報が確認された場合には、対銀行Yは、クレジット更新要求額を支持するに十分なクレジットがあることを検証する（ステップ1904）。十分なクレジットの場合には、対取引引きYに、確認をXへ送ることを督促する。Xは、その対出納アプリケーションファンクションを通して確認を受信する（ステップ1906-1912）。

しかしながら、クレジットの額が不足であると、加入者に、そのクレジット更新についての新しい額を入力するように督促する（ステップ1914-1918、図15B参照）。加入者によってクレジット更新についての新しい額が入力されると、その結果として、対出納アプリケーションが、最近の要求額をカバーするに十分なファンドがあるかを知るために、その新しいクレジット額をその出納マネーモジュールの対銀行アプリケーションへ送り（ステップ1922-1924）、図15Aのステップ1904に戻る。もし、新しい額が加入者によって要求されない場合には、その取引引きは、中止される（ステップ1926）。

図14を参照するに、クレジット引出し要求プロセスから戻るとき、対出納Aは、その勘定についての総通貨ノート、移転クレジットノート（すなわち、前の取引引きにおいて受信されたクレジットノート）およびクレジットノートのその出納マネーモジュールへの移転を発動する（ステップ1888）。もし、クレジット引出し要求がなされたときに取引引きマネーモジュールにノートが保持されていない場合には、対出納マネーモジュールAアプリケーションは、ノートがないことを示すメッセージを出納マネーモジュールに送る（ステップ1892-1894）。しかしながら、もし、取引引きマネーモジュールにノートが保持されている場合には、図8に関して前述したノート移転手順にしたがって、電子ノートが、Aから出納Bへと移転される（ステップ1896）。

図13に戻って、対取引引きBは、通貨ノートおよび移転クレジットノートが移転されたかをチェックし（ステップ1856-1858）、そして、ノートのこれらのタイプのいずれかが実際に取引引きマネーモジュールAから移転された場合には、勘定取引引きが対銀行アプリケーションBによってこの状態を反映するために掲示されるウステップ1860）。マネーモジュールからノートが移転されなかった場合にも、ステップ1860において勘定取引引きが掲示された後においても、出納マネーモジュールとマネージェネレータモジュールとの間にセッションが確立される（ステップ1862）。対銀行Bは、利用しうる総クレジットを得るためにクレジットの利用しうるラインにそのクレジットの額（もし、あるならば）を加え、その利用しうる総クレジットからその要求されたクレジット額を差し引くことにより、そのクレジットラインを更新する。もし、要求クレジット額がゼロであり且つ通貨ノートが移転されていないために、ノート（通貨ノートおよびクレジットノートを含む）を作成すべきでない場合には、マネーモジュールは、図10に関して前述したコミット手順にしたがってその取引引きを完了させる（ステップ1865-1875）。

しかしながら、もし、非ゼロクレジット額および／または移転通貨ノートのために、いずれかのノート（クレジットまたは通貨）を作成すべき場合には、ノート要求手順にしたがってマネージェネレータモジュールから出納Bによってノートが要求される（ステップ1865-1866）。マネージェネレータモジュールにおける要求ノートは、電子ノートを移転す

るための前述したノート移転プロセス（図8参照）を使用して出納マネーモジュールBへ移転される（ステップ1868）。それから、ノートが、同じノート移転プロセスを使用して、出納マネーモジュールBから取引マネーモジュールへと移転される（ステップ1870）。最後に、クレジット更新手順を首尾良く完了させるために、マネーモジュールは、図10に関して前述したコミット手順にしたがってその取引を完了させる。そのコミット手順は、先ず、その取引を出納マネーモジュールBとコミットする取引マネーモジュールによって開始させられる（ステップ1872）。それから、そのコミットプロセスは、出納マネーモジュールBとマネージェネレータモジュールとの間で実行される（ステップ1874）。これにより、発行銀行からの1つの完全なクレジット更新の処理が完了させられる。

発行マネーの一致

ノート一致のプロセスは、ノートの偽造と複製をチェックし、図16と図17を参照して記述する。発行マネー一致システムは、発行マネーマスターファイルに記憶された情報に基づき、ノートの移転履歴を表すノート移転ツリーを構成する。

図16は、識別子番号「1」を有するマネー発生モジュール（マネー発生器1という）と、識別子番号「2」を有するテラーモジュール（テラーモジュール2という）と、整数の識別子番号3から6を有する4つの取引マネーモジュール（取引モジュール3-6という）との間の、マネー発生器1が1:00:00で示す日／時間に発生した1つのノートに関連する仮定の一連の取引を図式的に表す。

図16に示す移転履歴の例に関連して、図17は通貨の電子表示の移転により、マネー発生モジュールにより生じた初期のノートから誘導されて通貨の電子表示のツリー状構造がどのように生じるかを示す。ノートの個々の移転（ツリーブランチの一部）がノートの更新に従って預金されるかバンキングシステムに戻ると、図17のノート移転ツリーが発行マネー一致システムにより作られる。この例では、マネー発生器1（モジュール識別子はデジタル署名した証明内に含まれる）は、データフィールドの本体グループとデータフィールドの移転グループとを有する通貨の電子表示2300を生じる。この説明を明確にするため一部を図式的に示す。さらに、便宜上データフィールドの署名及び証明グループは示さない。データフィールドの本体グループは、ノート識別子（例えば、「N12」）と、マネー発生器モジュール識別子（例えば、「MG1」）と、発行銀行識別子（例えば、「銀行名」）と、発行日（例えば、「1:00:00」）と、満了日（例えば、「12:00:00」）と、ノートの金額と通貨単位識別子（例えば、「\$ 50」）を含む。ノートの種類等他の本体グループのデータフィールドは、便宜上示さない。電子ノートの色々のデータフィールドを例示のため日：時間：分の形式で示す。他の時間モニター形式（例えば秒を含む）ももちろん可能である。

データフィールドの移転グループは、移転先識別番号と移転日と移転金額とを有する移転レコードを含む。移転グループは、個々の移転後に移転元のノートディレクトリによりインクリメントされるシーケンス番号を含むのが好ましい。通常、移転の日／時間と移転IDは、移転を独自のものと識別するのに十分である。しかし、移転間で時間調整され、同じ金額が同じモジュールに移転されるなら、移転、移転先ID、日／時間、及び金額は、2重にすることができる。従って、この潜在的な問題を避けるには、移転を独自のものと識別するため、シーケンス番号（seq）を移転レコードとノートディレクトリに加えるのが好ましい。シーケンス番号は、個々の移転後にノートディレクトリによりインクリメントされる。もし、シーケンス番号がリセットされると、これは複製であると検出されるであろう。

従って、通貨の電子表示2300がテラーモジュール2に移転されると、移転レコード2302が移転グループに付加され、これは移転先識別番号（例えば、「2」）と、移転日（例えば、「1:00:00」）と、移転金額（例えば、「\$ 50」）と、シーケンス番号（例えば、「1」）とを含む。例示の便宜のため、図17に示すノートの移転は、移転されたノートの新しく付加された移転レコード部分のみを示す。また便宜上、移転の総数を示す移転グループデータフィールドは示さない。

マネー発生器からの通貨の電子表示2300は、テラーモジュール2に記憶される。取引モジ

10

20

30

40

50

ジュール 3 による \$ 50 の引き出しの一部として、テラーモジュール 2 は、移転レコード 2302 により増加した通貨の電子表示のデータフィールドのコピーに移転レコード 2304 を付加することにより、通貨の電子表示を形成する。このノートは、引き出しの完了により、取引モジュール 3 に記憶される。ノート移転ツリーの個々のノードは、移転されたノートの新しく付加された移転レコードを示すことが分かるであろう。

ノート移転ツリーにより表されるように、取引モジュール TR3 は、1:00:05 に、移転レコード 2306 により取引モジュール 4 に \$ 10 支払う。取引モジュール 3 は、1:01:00 に移転レコード 2308 により取引モジュール 5 に \$ 10 支払う。取引モジュール 3 は、3:08:01 に移転レコード 2310 により取引モジュール 5 に \$ 25 支払う。取引モジュール 3 は、4:11:08 に移転レコード 2312 により取引モジュール 6 に \$ 5 を移転する。

10

取引モジュール 4 は、2:00:01 に移転レコード 2314 により取引モジュール 6 に \$ 5 移転する。取引モジュール 4 は、2:01:07 に移転レコード 2315 により取引モジュール 6 に追加の \$ 5 を移転し、取引モジュール 6 は次に、3:07:05 に移転レコード 2321 により取引モジュール 3 に \$ 5 を移転する。

取引モジュール 5 は、2:00:06 に移転レコード 2316 により取引モジュール 3 に \$ 10 のノート全体を移転する。取引モジュール 5 が、3:08:01 に取引モジュール 3 から受け取った \$ 25 のノートから、取引モジュール 5 は、3:09:12 に移転レコード 2318 により取引モジュール 6 に \$ 20 支払い、残りの \$ 5 を 4:12:05 に移転レコード 2320 によりテラーモジュール 2 に預金する。

取引モジュール 6 は、4:10:00 に移転レコード 2322 に従い取引モジュール 5 に \$ 10 を移転し、5:00:06 に移転レコード 2324 により取引モジュール 3 に残りの \$ 10 を移転する。本発明の実施例により、取引モジュールから銀行へマネーを預金すると、取引モジュール内の全てのノート（クレジットノートを含む）は、バンキングシステムに送られ更新されることが分かる。それ故、上述の移転レコード 2320 により表される取引モジュール 5 からテラーモジュール 2 への預金とほぼ同時に、移転レコード 2326 で表される追加で同時の移転が自動的に起こる。次に、\$ 5 の価値を有する新しいノートが（取引モジュール 3 がクレジットノートを有さないと仮定する）、マネーモジュール 1 により発生し、適当な移転レコードを付加して（図示せず）テラーモジュール 2 を経由して取引モジュール 3 へ移転される。従って、取引モジュールとテラーモジュール間の取引（例えば、預金又は引き出し）による取引マネーモジュール内の全てのノートを更新することは、ノートをバンキングシステムに戻すことに別の手段を提供することにより、ノート一致プロセスを容易にする。取引モジュール 3 は、5:00:10 に移転レコード 2328 により、テラーモジュール 2 に \$ 10 を預金する。取引モジュール 5 の預金について上述したように、移転レコード 2328 により表される取引モジュール 3 の預金と同時に、取引モジュール 3 が所有した全てのノート（移転レコード 2316 と移転レコード 2321 で表されるものを含む）のバンキングシステムへの追加で同時の移転（図示せず）が起こる。次に、バンキングシステムは、取引モジュール 3 に更新の為バンキングシステムに送られた合計のノート（例えば、\$ 15）に等しい価値を有するノートに戻す。

20

30

従って、この時点で、取引モジュール 6 のみが、移転ノート 2312 と 2314 で表されるように、当初のノート 2300 の移転可能な形跡を所有する。もし、取引モジュール 6 が、これらのノートを他の移転マネーモジュールに移転する前に、テラーモジュールと取引（例えば、預金又は引き出し）をすれば、当初のノート 2300 に関連する移転可能なノートは流通していないことになる。当初のノート 2300 の取引から派生する全てのノートは、バンキングシステムに戻され、図 17 に示すようなノート移転ツリーの完全な構成ができる。満了日より、ノートが移転される時間を制限することで、ノートの一致が容易になる。

40

ノート移転ツリーから、ノートが偽造されたら、預金された第 1 ピースにマッチするノート本体はないことが分かるであろう。もし、移転が複製されれば、後の移転は上位の移転金額より大きな値になるであろう。例えば、もし取引モジュール 6 が、5:00:06 に取引モジュール 3 に \$ 10（即ち、移転レコード 2324）の代わりに \$ 20 移転すると、移転レコード 2318（即ち、SEQ1、3:09:12、TR6、\$ 20）の下に移転は合計 \$ 30 になり、取引モジュール

50

6が移転を複製したことを示すであろう。

銀行アクセスのため銀行口座にマネーモジュールをリンク

図18は、銀行にアクセスするため、銀行口座にマネーモジュールをリンクするプロトコルを示す。加入者が、顧客サービス代理（CRS）に自分を明らかにし、CRSに加入者の口座をマネーモジュールへリンクすることを要請するとき、このプロセスが始まる（ステップ1928）。CRSは、識別された加入者の口座をリンクする要請をCSMホストA（CSMA）に入れ、CSMAは、バンキングシステムから識別された加入者の口座情報にアクセスする（ステップ1930-1934）。次に、加入者とCRSが、口座情報を有効化し、加入者はどの口座をマネーモジュールにリンクさせるかを選択する（ステップ1936）。

加入者が、自分のマネーモジュールBを銀行口座にリンクすることを要請し、CSRがCSMHA 10
を通してCSMAが銀行口座にリンクすることを要請した後、加入者のマネーモジュールBとCSMAの間で安全セッションが行われる（ステップ1938-1946）。次に、CSMAのホストAへからの要請に応じて、HCSMAは、口座情報をCSMAに送り、それは口座情報を受け取り、それから口座プロフィールを構成する（ステップ1948-1952）。次に、公開キーAが口座プロフィールにサインし、口座プロフィール生成で、口座プロフィールからメッセージと署名を構成し、このメッセージをマネーモジュールBに送る（ステップ1954-1958）。セキュリティ保持Bが、メッセージを受け取り、公開キーBがメッセージのデジタル署名をチェックする（ステップ1958-1962）。もし、署名が無効であれば、このセッションは中止される（ステップ1966）。

もし署名が有効であれば、加入者Bへは、顧客が口座プロフィールを有効化するため、プ 20
ロフィールをホストに送る。もし、顧客が口座プロフィールを肯定しなければ、取引は中止される。もし、顧客が口座プロフィールを肯定すれば、セキュリティB保持は、口座プロフィールにCSM証明を追加する（ステップ1968）。

次に、テラーBへは、最近生じた（「新しい」）口座プロフィールに関連する口座プロフィールが既に銀行に記憶されているかを求めるチェックをする。もし、テラーBへの適用の中に銀行の口座プロフィールが既に存在すれば、テラーBへは新しい口座プロフィールに置き換える。そうでなければ、テラーBへで新しい口座プロフィールを追加する（ステップ1970-1974）。

マネーモジュールの銀行口座へのリンクの再確認

図19は、加入者がマネーモジュールのリンクを銀行口座に再確認するプロトコルを示す。 30
加入者が自分のマネーモジュールにサインするときプロセスが始まり、加入者Aへで生じる取引のプロンプトに応じて、加入者は、顧客サービスモジュール（CSM）Bと関連する銀行への銀行口座リンクを再確認することを選択する（ステップ1978-1982）。マネーモジュールは、図6に関連して上述したネットワークのサインオンプロトコルを呼び出して実行し、マネーモジュールAとCSBMの間で安全セッションが確立される（ステップ1986）。テラーAへは、銀行口座の口座プロフィールをCSBMに送る（ステップ1988-1990）。口座プロフィールB生成はメッセージを受け取り、セキュリティB保持でCSM証明と口座プロフィールの署名を確認する（ステップ1992-1995）。もし、証明又は署名が無効であれば、CSMは取引を中止する（ステップ2000）。もし、証明が有効であれば、ホストBへは口座プロフィールからの口座のリストをCSMホスト（CSMH）に送り、それがオンライン 40
のバンキングシステムで個々の口座が現在アクティブであるかを求める（ステップ1996-2001）。口座のどれかが満了していれば、CSMHはCSMに中止メッセージを送信し（ステップ2010）、CSMは次に中止プロセスに従い取引を中止する（ステップ2000）。

もし全ての口座がアクティブなら、CSMHはCSMに再確認指示を送信し、口座プロフィールB生成でメッセージを受け取り、口座情報から口座プロフィールを構成する（ステップ2002-2004）。公開キーBが口座プロフィールにサインし、口座プロフィールB生成で、口座プロフィールからのメッセージと署名を構成し、このメッセージをマネーモジュールAに送る（ステップ2006-2010）。公開キーAは、メッセージを受け取り、デジタル署名を有効化する（ステップ2012）。もし署名が無効であれば、マネーモジュールAは取引を中止する（ステップ2018）。もしそれが有効であれば、口座プロフィールにプロフィール 50

署名とCSM証明が追加され（ステップ2014）、マネーモジュールAは取引をコミットする（ステップ2016）。

口座番号の確認

上述した顧客サービスモジュール（CSM）を使用する本発明の実施例に従って、どのように口座番号が確認されるかを示すフローチャートを図20に示す。

このプロセスで、セキュリティY保持が、口座番号とCSM証明を含む口座プロフィールを受け取り、CSM証明を有効化する（ステップ2020）。無効な証明は、2つのマネーモジュールの間の取引を中止させる（ステップ2028）。

もし、証明が有効であれば、セキュリティ保持Yで、CSM署名を有効化するため、口座プロフィールを公開キーYに伝達する（ステップ2022）。無効な署名は、セキュリティY保持でセッションマネージャーに口座プロフィールが無効であると通知させ（ステップ2026）、2つのマネーモジュールの間の取引は中止される（ステップ2028）。

署名テストが、有効な署名であると確かめると、手順は銀行Yへに進み、そこで受け取った口座番号を銀行のオンラインコンピューターシステムに送る（ステップ2024）。アクティブでない口座は、セキュリティ保持Yがセッションマネージャーに活動していない口座を知らせるようにし（ステップ2030）、取引を中止させる（ステップ2028）。アクティブな口座は、口座番号の確認プロセスから口座番号確認プロセスを呼び出したオペレーションのフローの次のステップにリターンさせる。

口座番号確認プロセスは、本発明の実施例と比較して、CSMを含まないテラマネーモジュールでは簡単になっている。

紛失マネーの請求

前述したように、電子マネーは、（1）マネーモジュールが損傷し、もはや機能しない、（2）マネーモジュールを紛失したか又は盗まれた、（3）コミットが失敗した等のいくつかの理由で紛失することがある。マネーシステムの有用性には、加入者が自分のマネーは無事であるとシステムを信頼できることが重要である。従って、移転先はシステムの故障で紛失したマネーを再度請求できることが重要である。電子的な故障は物理的損傷による紙の紛失より起こりそうなので、マネーモジュールが損傷したときマネーを置き換えられることが、信頼を改善する。マネーモジュールを紛失したか盗まれた災難によって、マネーを置き換えることは、より問題がある。このような請求を許すと、加入者が紛失に対して用心しなくなるので、システムに広い請求を招くことになる。

どの場合も、本発明で具体化されるのは、これらのどの場合のマネー紛失でも置き換えられる方法である。最初の2つの場合（即ち上の場合（1）と（2））、加入者は周期的にマネーモジュールの外部に記憶できる紛失ノート請求を生成しなければならない（図21参照）。故障すると、加入者の識別と共に発行銀行に請求を提出することができる（図22参照）。請求は、加入者のマネーモジュールの最後の分かる状態を含むであろう。請求されたノートの記述は、確認され、発行銀行に配送することができる。発行銀行は、請求されたノートが預金されていなければ、ある期間の後マネーを置き換えることができる。

コミットが失敗した場合（即ち上の場合（3））、マネーモジュールがまだ機能するなら、マネーモジュールと顧客サービスモジュールの間に請求が交互に生成される（図22参照）。この請求は、場合（1）と（2）と同様に、発行マネー調査システムに渡され、それが預金されたマネーに対して請求をモニターする。発行銀行は、不正の適用に対して入ってくるマネーをモニターでき、志願者の識別を持っているので、信頼して紛失したマネーを置き換えることができる。

これらの方法は、図21と図22を参照してより詳しく記述する。

紛失ノート生成請求

図21Aを参照すると、本発明の実施例に関連して実行できる紛失ノートの生成請求のプロセスが示される。加入者が、マネーモジュールにサインオンするときプロセスが開始し、加入者Aへは加入者に取引をプロンプトし、加入者が紛失ノート生成請求のオプションを選択する（ステップ2032-2036）。

次に、全てのノートと請求されない失敗コミットを統合するいくつかのステップが起こる

(ステップ2038-2042)。特に、ノートディレクトリAは、独自の請求シーケンス番号（請求を識別するのに使用する）を生成し、ノートディレクトリのコピーをシーケンス番号と共にパケットマネージャーに運ぶ。ノートAは、全てのノートのコピーを署名と証明と共にパケットマネージャーに運ぶ。次に、TranLogAは、中止プロセスの間に記録された全ての請求されない取引のコミットを失敗したものをパケットマネージャーに運ぶ。

次に、公開キーAが、マネーモジュール非公開キーを使用し、請求シーケンス番号と、ノートディレクトリと、ノートと、パケットマネージャーに送られた失敗コミットにサインし、パケットマネージャーAは、アセンブルしたデータに署名を追加し、その結果アセンブルしたデータパケットになり（ステップ2044-2046）、それが次に公開キーAにより暗号化される（ステップ2048）。暗号化した請求に、公開キーAは、請求シーケンス番号と、請求の合計金額の値と、マネーモジュールAの識別とからなる請求記述を追加する（ステップ2050）。加入者Aへは、この請求をマネーモジュールホストへ送り、それが請求を受け取り、将来の使用のため、マネーと独立の媒体上に請求を記憶する（ステップ2052-2054）。

10

それ故、紛失ノート請求プロセスは、マネーモジュールの損傷又は故障により破壊されない潜在的マネー請求を発生し保護する方法を提供することがわかる。

紛失ノートの請求

図22は、紛失ノートを請求するプロトコルを示し、加入者が顧客サービス代理（CSR）に紛失ノートの請求することを頼むとき、プロセスは始まり、加入者の識別がCSRに明かされる（ステップ2056）。CSRは次に、加入者の識別を顧客サービスモジュールホスト（CSM）Aに伝達し、請求が失敗したコミットによるか、又はマネーモジュールの紛失又は破壊によるかをチェックする（ステップ2058-2060）。もし、失敗したコミットが請求の元であり（加入者のマネーモジュールは紛失も損傷もしていなければ）、加入者のマネーモジュールから紛失したノートの請求をするという選択と、CSRのマネーモジュールから紛失したノートの請求を受け入れるという選択により、加入者のマネーモジュールのセッションマネージャーBと顧客サービスモジュール（CSM）のセッションマネージャーAは、顧客サービス代理と共に（顧客サービスモジュールホスト（HCSM））を通じて、それぞれ呼び出され、CSM AとマネーモジュールBの間で安全セッションを確立する（ステップ2062-2070）。

20

いったん安全セッションが確立されると、CSMのホストAへで、加入者の識別を求め、HCSM Aが、加入者の識別を含むメッセージをCSMに送ることにより、この請求に応答する（ステップ2072-2074）。紛失ノートA請求で、このメッセージを受け取り、請求を送るべきと指示するメッセージをマネーモジュールBに送る（ステップ2076-2078）。

30

TranLogBが、このメッセージを受け取り、請求されていない失敗したコミットの記録を引き出す（ステップ2080）。失敗したコミットの記録がなければ、取引は中止される（ステップ2083）。そうでなければ、加入者Bへは、失敗コミットの記録から引き出された情報（即ち、データ、時間、金額）を加入者に再調査のため送る（ステップ2082）。この情報から、加入者は請求する取引を選択する（ステップ2084）。例えば加入者は、別に解決した失敗したコミット取引を選択しないであろう。次に、加入者が選択した個々の失敗したコミット取引のため、TranLogBは、これらの取引の記録情報を含むメッセージを構成し、このメッセージをCSMに送る（ステップ2086-2088）。

40

紛失ノート請求Aは、このメッセージを受け取り、将来請求を参照するため請求の識別子（即ち、コンファメーション番号）を含む承認をBに送る（ステップ2092）。TranLogBは、承認を受け取り、個々の選択した失敗コミット取引記録に、請求の日／時間とCSMにより提供された請求の識別子を記す（ステップ2094）。次に、Bは、取引をコミットする（ステップ2096）。

コミットの手順が終了した後、失敗したコミット取引情報を含む受け取ったメッセージから、紛失ノート請求Aは発行マネー調査システム（MITS）に送る請求を構成する。MITSは、取引調査システムの一部を形成することが好ましい。ホストAへで、この請求をHCSMAに送り、それは請求を受け取り、さらに請求をMITSに送る（ステップ2098-2102）。

50

図22のステップ2060に戻り、請求が失敗したコミットによる（即ち、紛失した又は損傷したマネーモジュールによる）のでなければ、加入者は、図21を参照して前述した紛失ノート生成の請求のプロセスに従って、発生しマネーモジュール計算環境から（即ち、フラッシュメモリー上へ）外された加入者の請求のどれかにアクセスを有するホストBからの紛失ノートを請求する選択をすることができる。CSRは、別にマネーモジュールホストからの紛失ノートの請求を受け取るプロセスを開始し、ホストは公知の技術に従ってコミュニケーションのリンクを設立する（ステップ2104－2108）。

次に、加入者ホストBが、マネーモジュール証明を含む請求をCSMHAに送り、それは請求をCSMAに送る（ステップ2108－2112）。紛失ノート請求Aは、請求を受け取り、請求を公開キーAに送り、それがマネーモジュールの証明を再確認する（ステップ2114－2116）。もし、マネーモジュール証明が無効であれば、ホストAへは、請求は拒絶されたことを示すメッセージをCSMHAに送り、CSMHAはこのメッセージを加入者ホストBに送り、紛失ノート請求プロセスは終了する（ステップ2120－2121）。

10

もし、マネーモジュール証明が有効であれば、公開キーAが請求を暗号化し、請求内の全てのノート証明と署名を有効化する（ステップ2118）。ノート証明と署名の何方かが有効でなければ、取引は終了する（ステップ2119－2121）。ノート証明と署名が有効であれば、紛失ノート請求Aは、移転金額の一致性を有効化し、個々のノートの移転履歴により、移転先に運ばれたマネーの値は移転元が受け取った値より大きくないことを保証する（ステップ2122－2123）。もし一致しなければ、取引は終了する（ステップ2120－2121）。

しかし、移転金額が全てのノートについて一致性があれば、紛失ノート請求Aは、MIISへ送る請求を構成し、また請求に対応する請求の識別子を発生する。ホストAへは、構成した請求と請求の識別子をCSMHAへ送り、それが請求と請求の識別子を受け取り、請求の識別子を加入者ホストBへ発送し、請求をMIISへ送り（ステップ2124－2128）、従って紛失ノート請求プロセスを完了する。

20

上述の記述は、多くの特性を与えるが、これらの実施可能な詳細は、本発明の範囲を制限すると解釈すべきでなく、本発明はこの範囲から離れずに又伴う利点をなくすることなく多くの改変、適応、均等な実行が可能であることが、当業者には分かるであろう。それゆえ、本発明は開示された実施例に制限されず、請求の範囲に従って定義される。

【図 1 A】

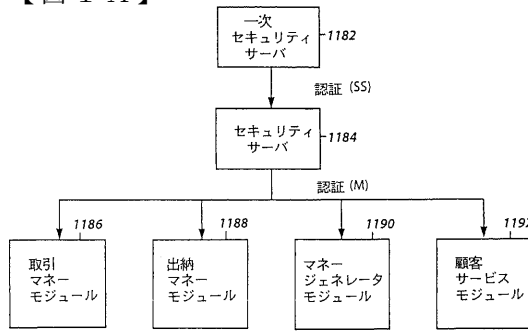


Figure 1A

【図 1 B】

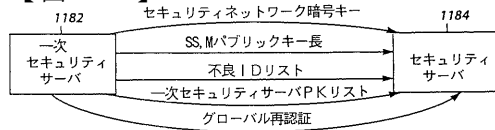


Figure 1B

【図 2】

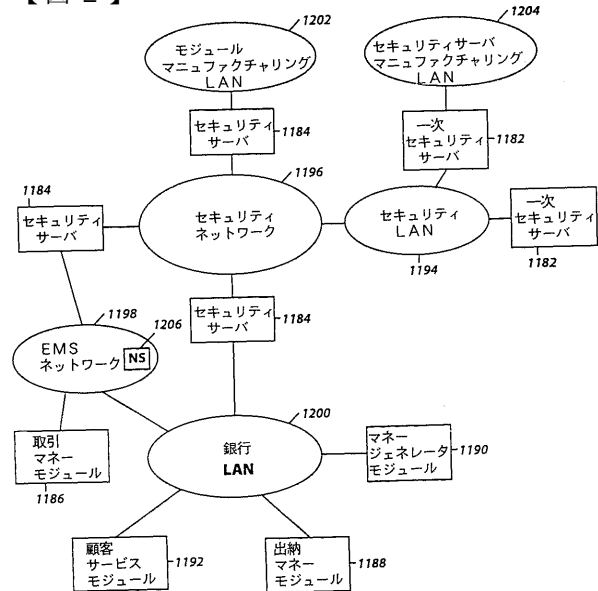


Figure 2

【図 3 A】

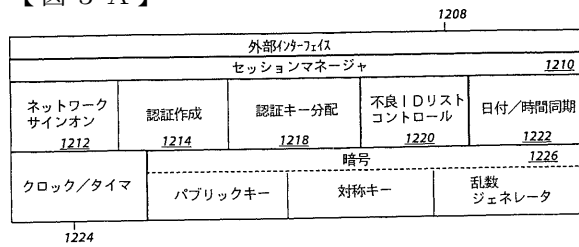


Figure 3A

【図 4 B】

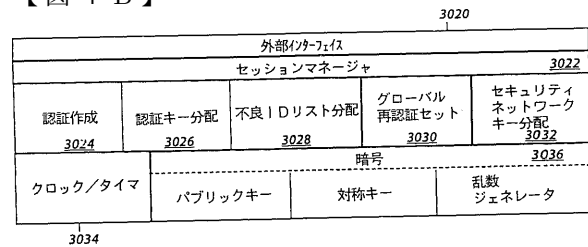


Figure 4B

【図 3 B】

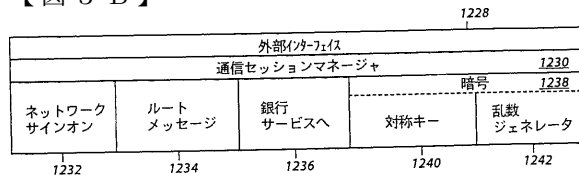


Figure 3B

【図 4 A】

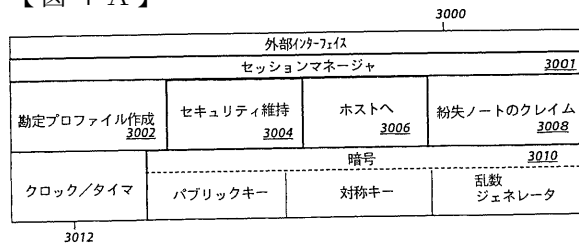


Figure 4A

【図 5】

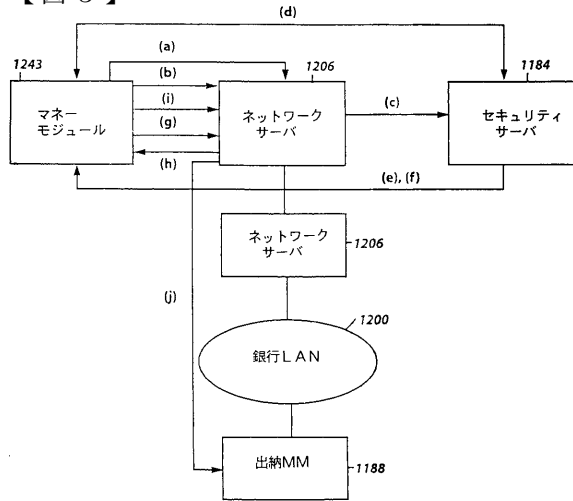


Figure 5

【図 6 A】

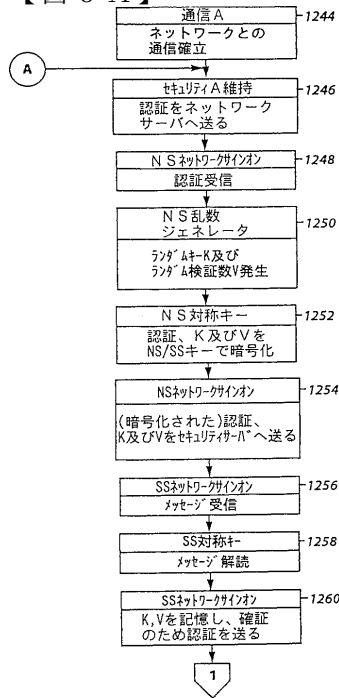


Figure 6A

【図 6 B】

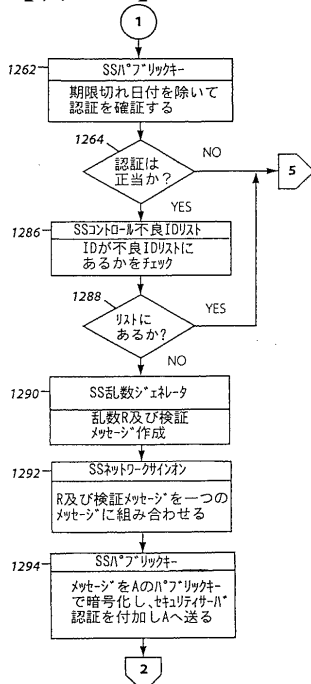


Figure 6B

【図 6 C】

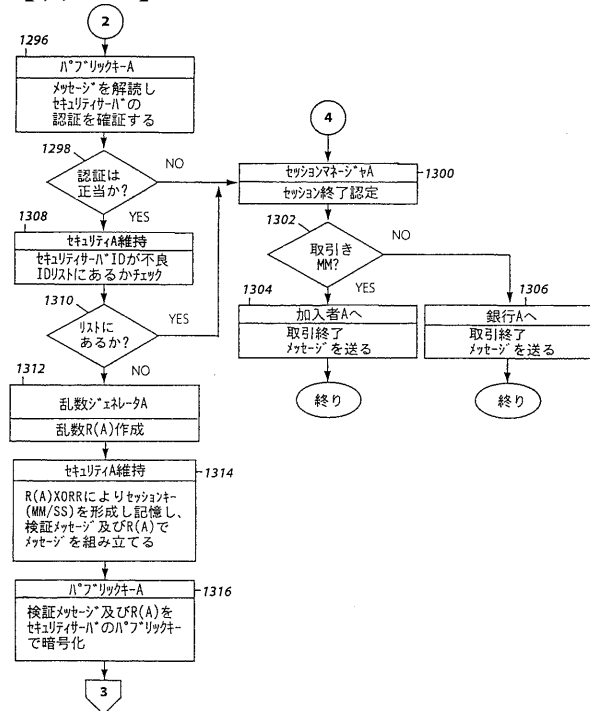


Figure 6C

【図 6 D】

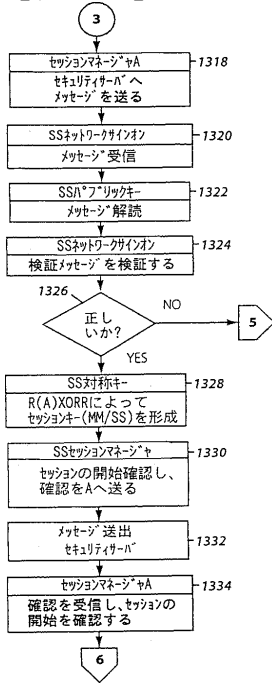


Figure 6D

【図 6 I】

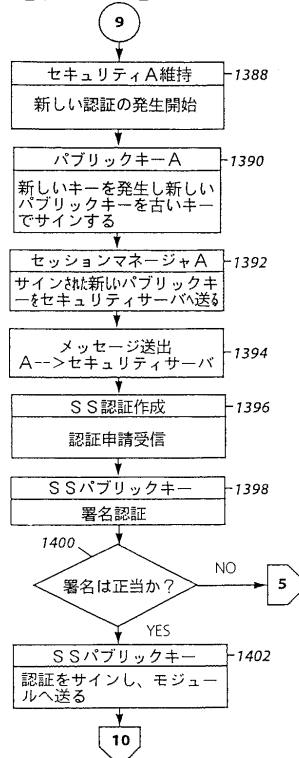


Figure 6I

【図 6 E】

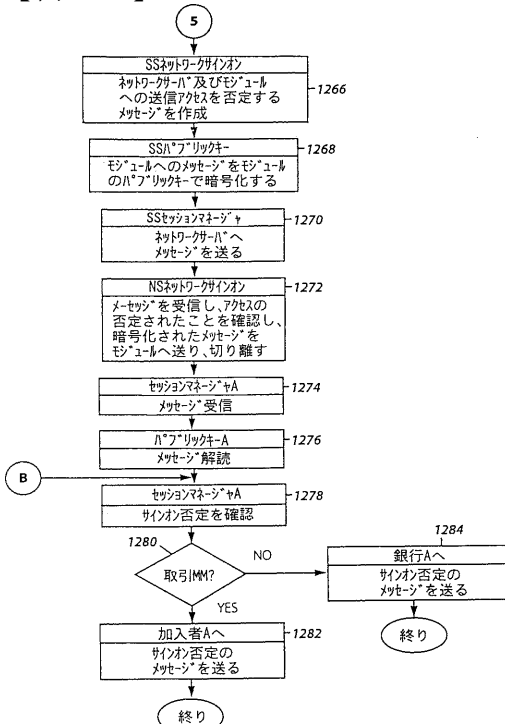


Figure 6E

【図 6 F】

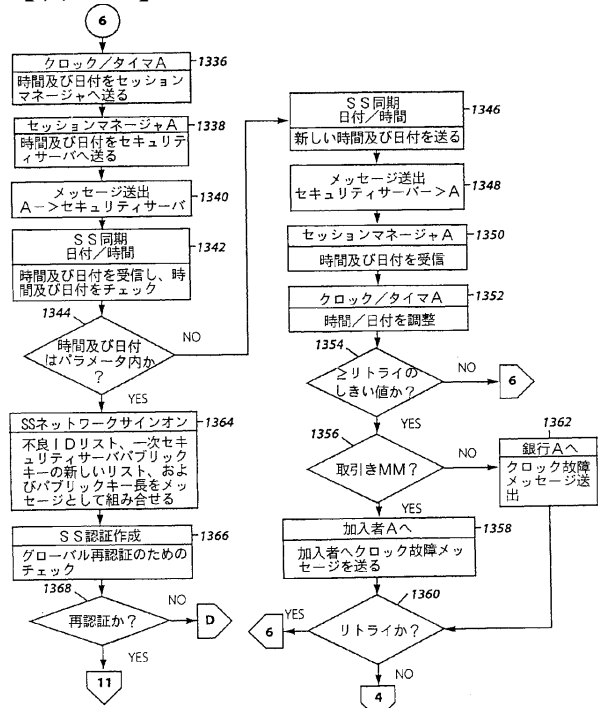


Figure 6F

【図 6 G】

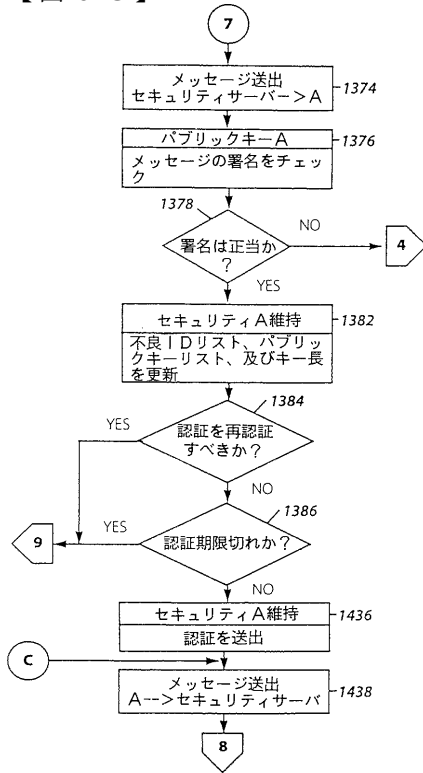


Figure 6G

【図 6 H】

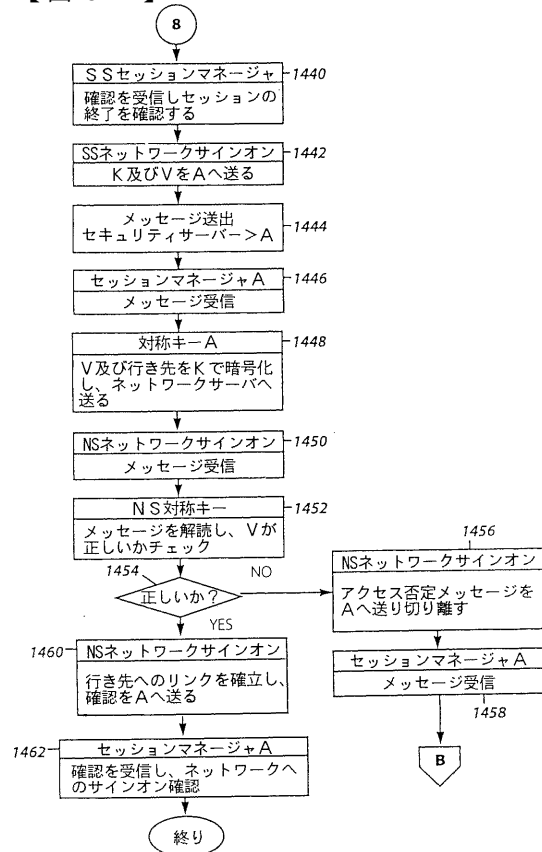


Figure 6H

【図 6 J】

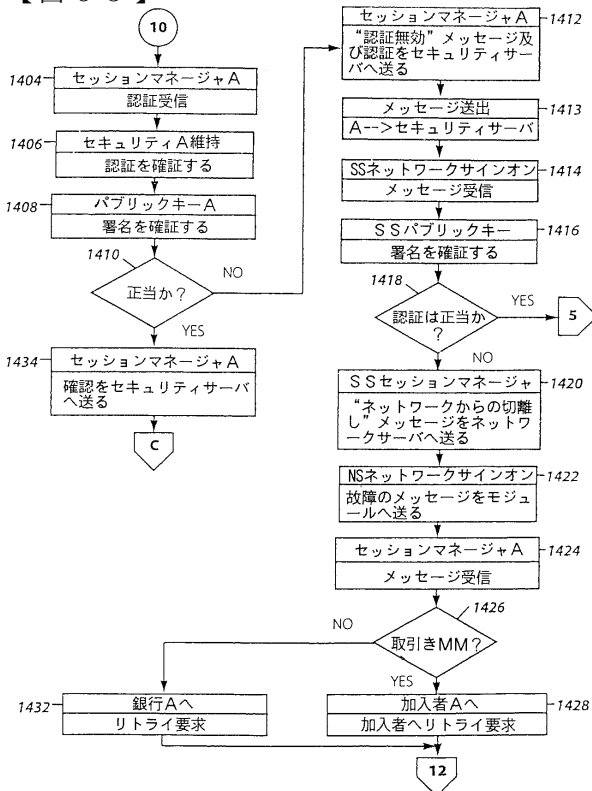


Figure 6J

【図 6 K】

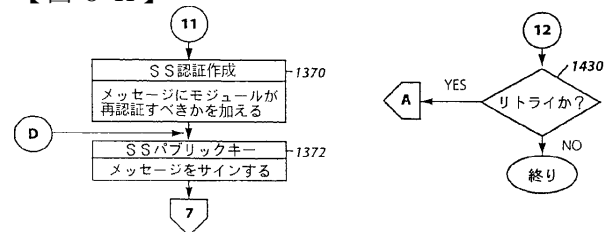


Figure 6K

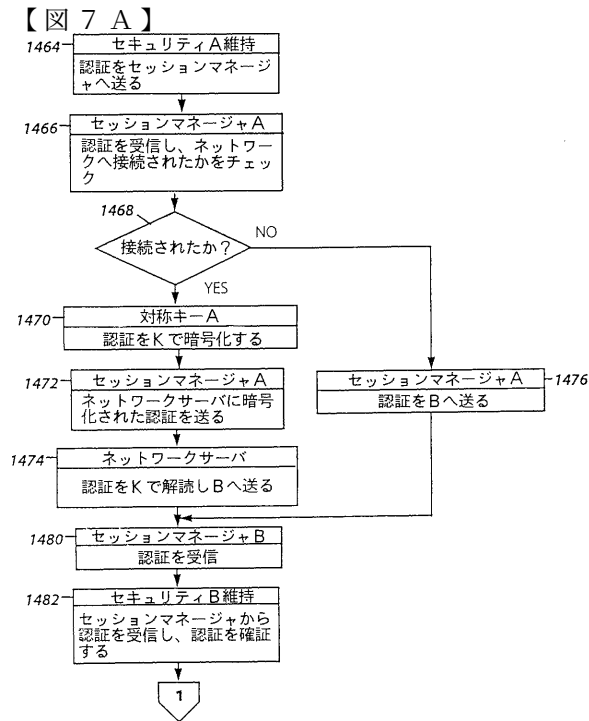


Figure 7A

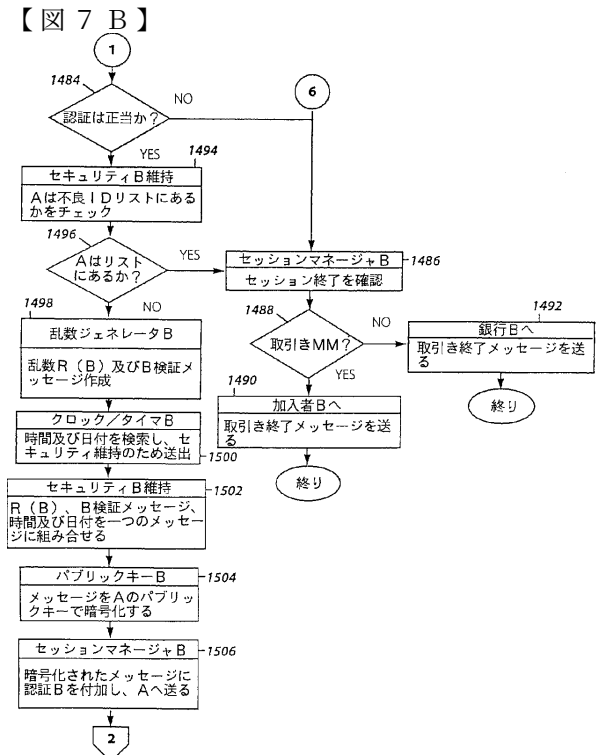


Figure 7B

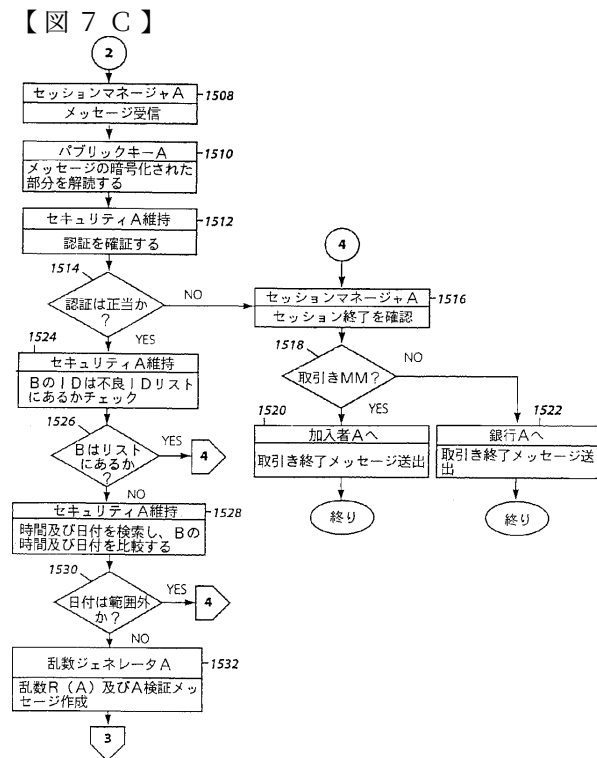


Figure 7C

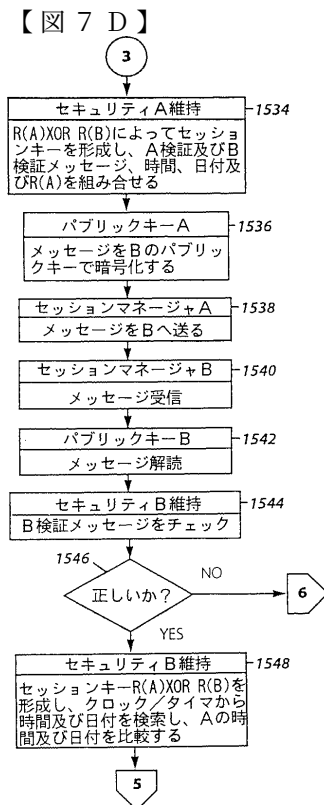


Figure 7D

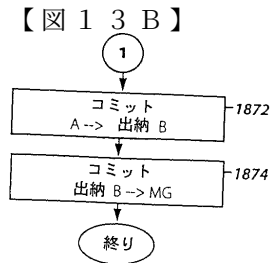


Figure 13B

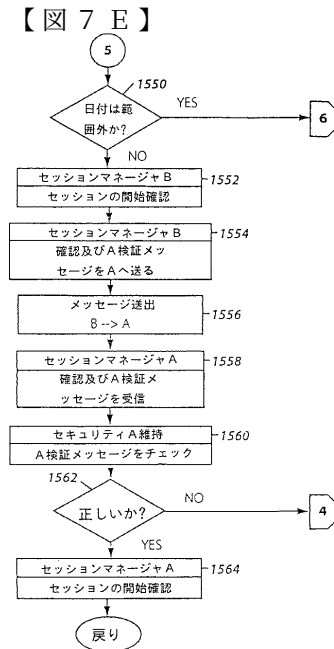


Figure 7E

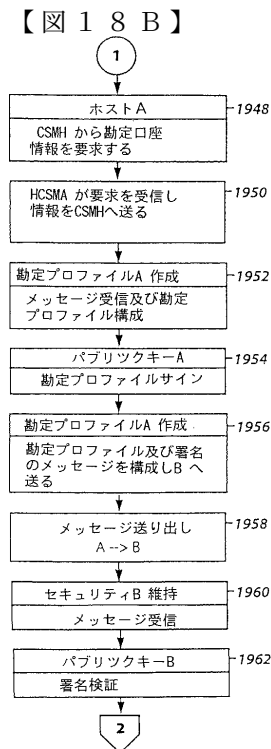


Figure 18B

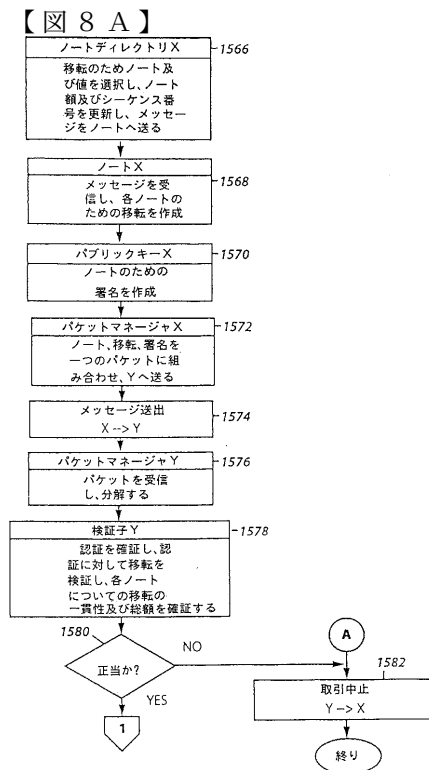


Figure 8A

【図 8 B】

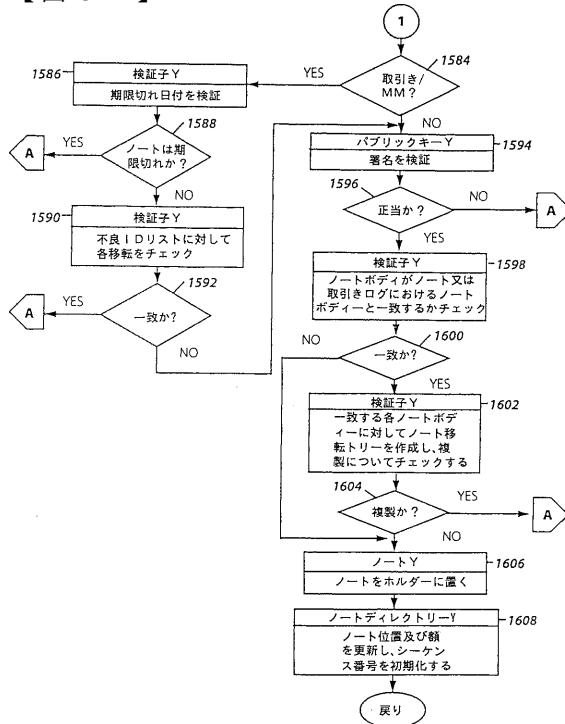


Figure 8B

【図 9 A】

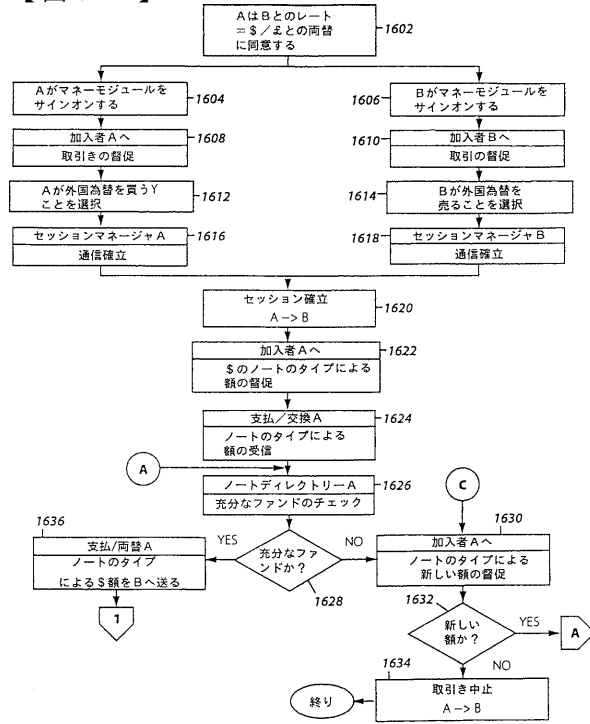


Figure 9A

【図 9 B】

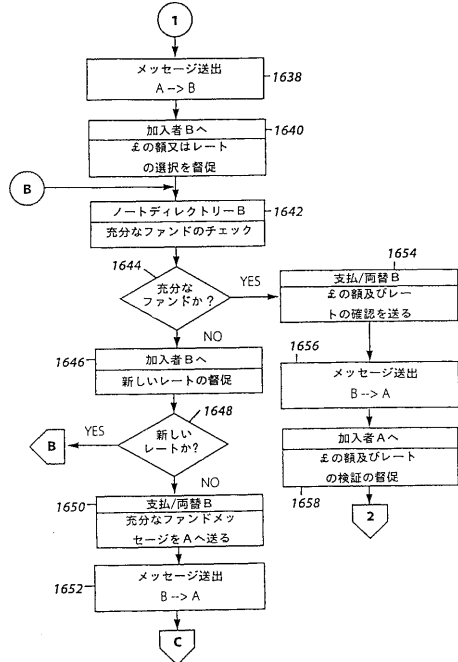


Figure 9B

【図 9 C】

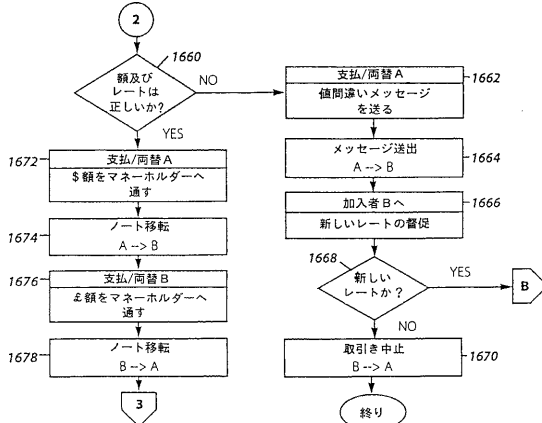


Figure 9C

【図 9 D】

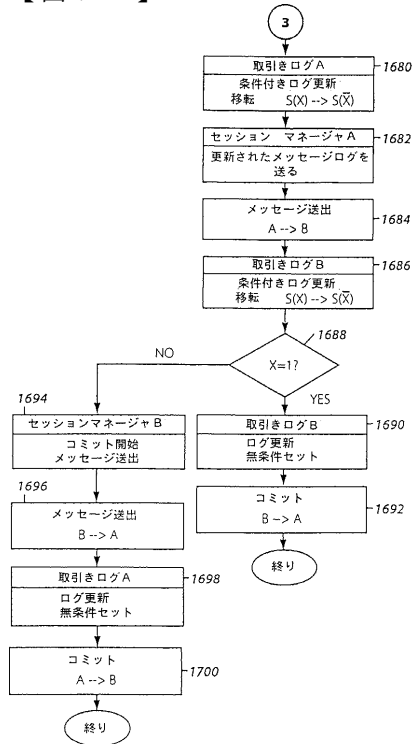


Figure 9D

【図 10】

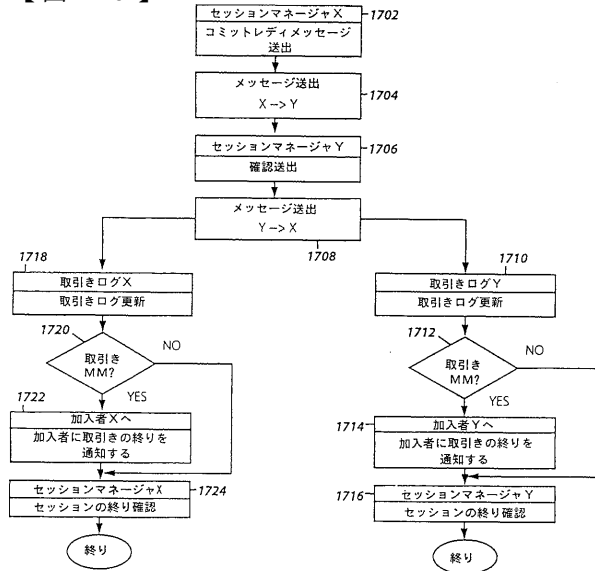


Figure 10

【図 11 A】

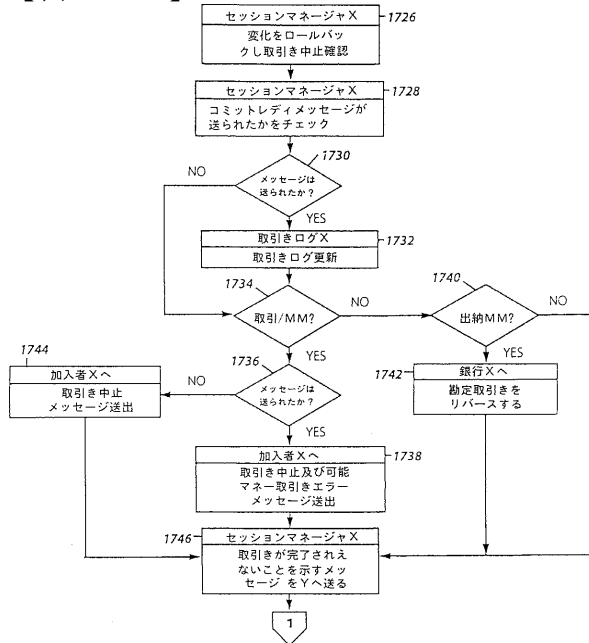


Figure 11A

【図 11 B】

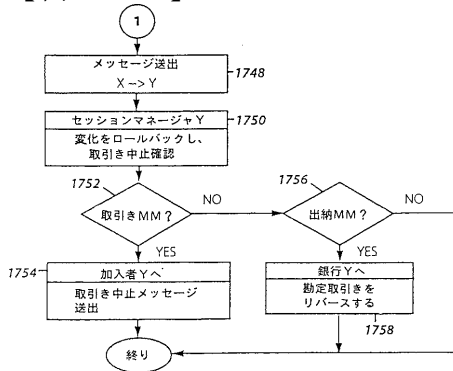


Figure 11B

【図 12 A】

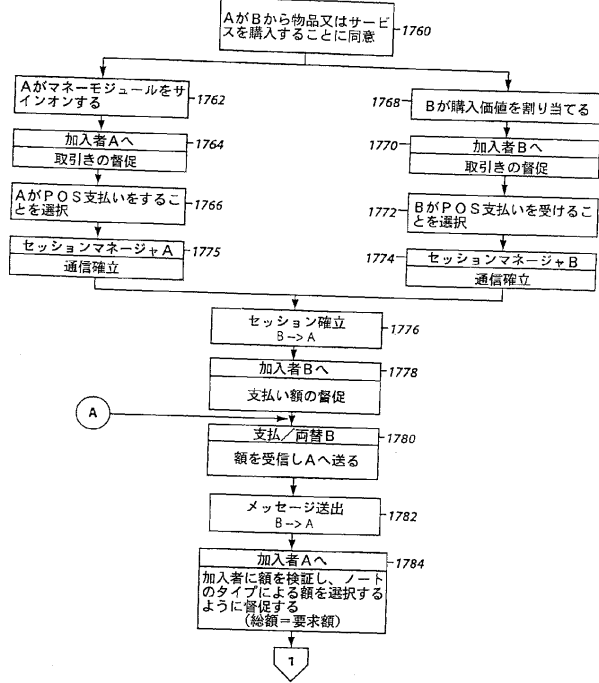


Figure 12A

【図 12 B】

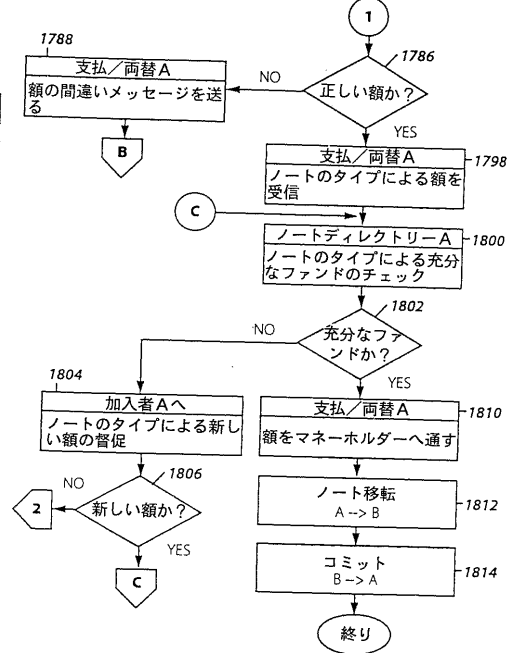


Figure 12B

【図 12 C】

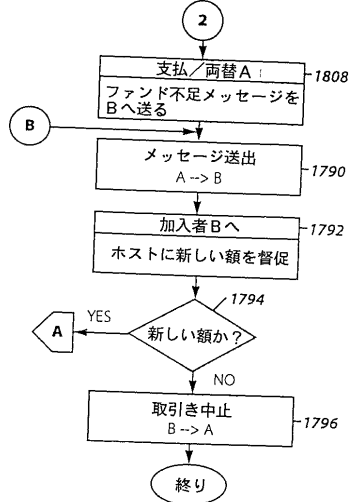


Figure 12C

【図 21 A】

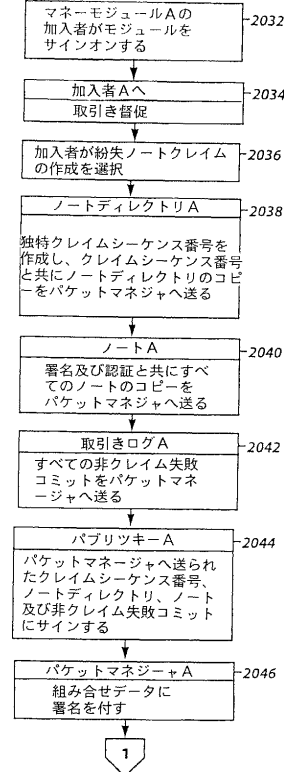


Figure 21A

【図 13 A】

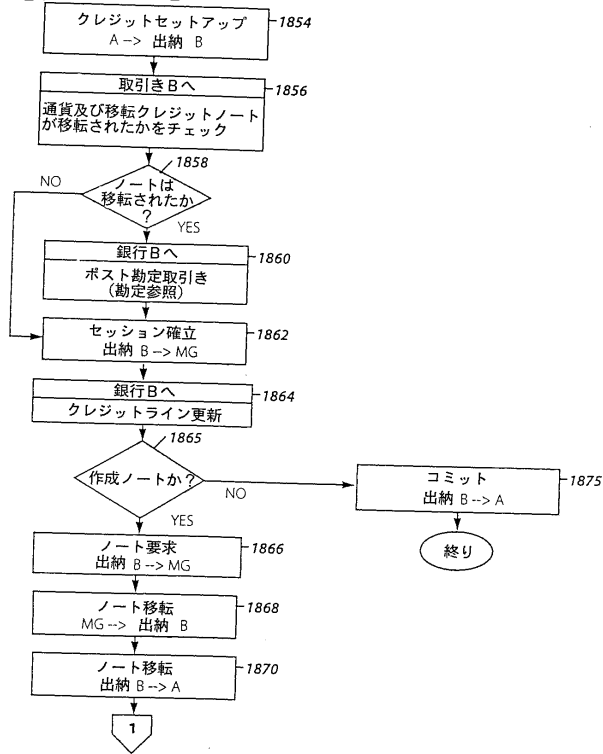


Figure 13A

【図 14】

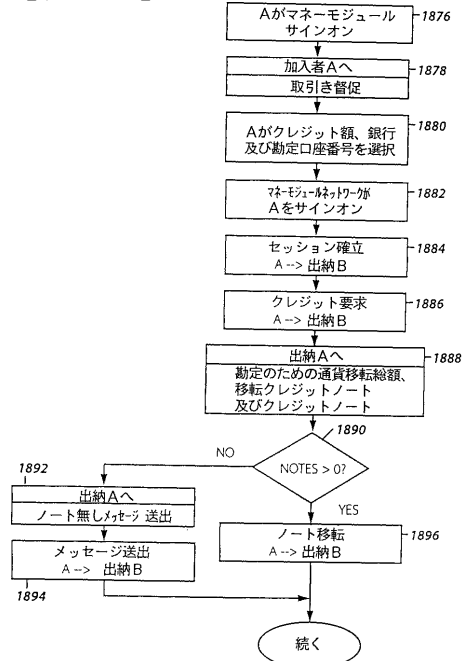


Figure 14

【図 15 A】

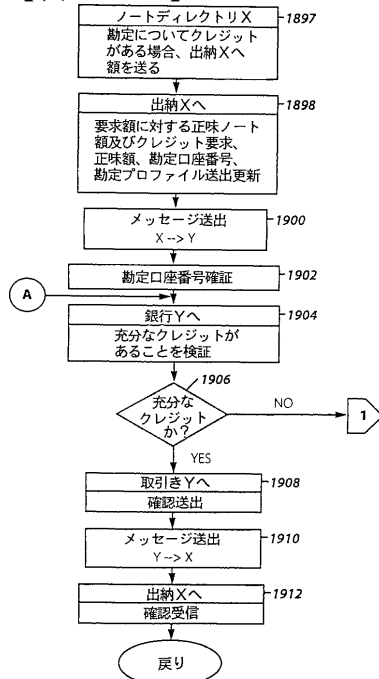


Figure 15A

【図 22 C】

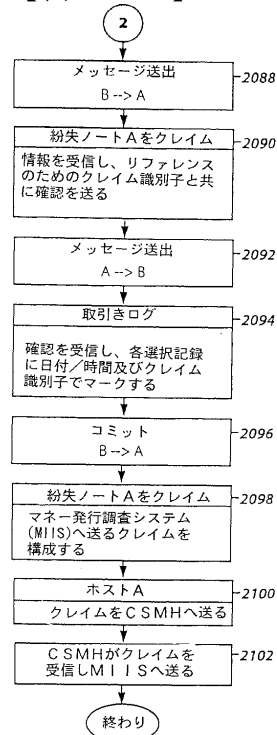


Figure 22C

【図 15 B】

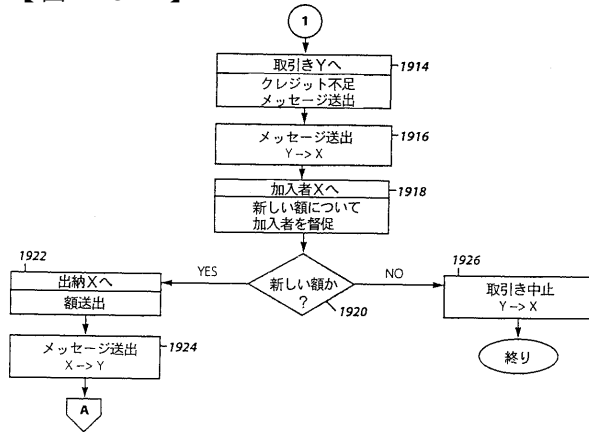


Figure 15B

【図 16】

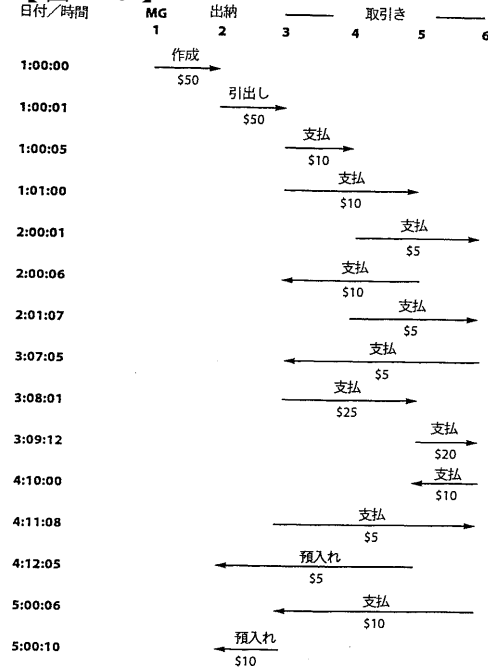


Figure 16

【図 17】

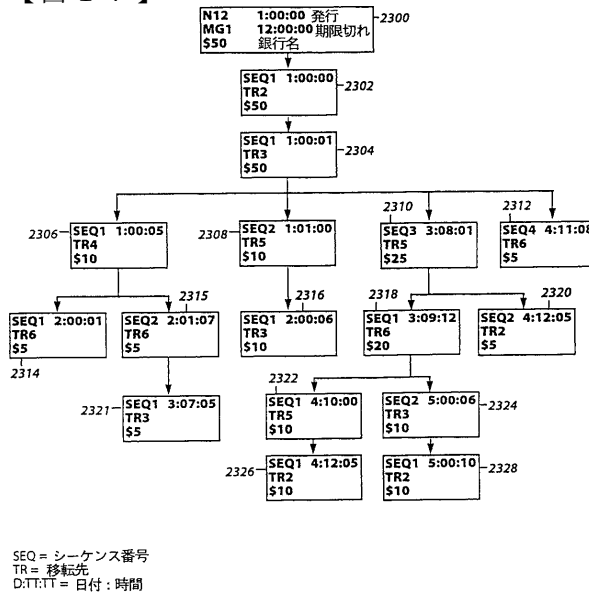


Figure 17

【図 18 A】

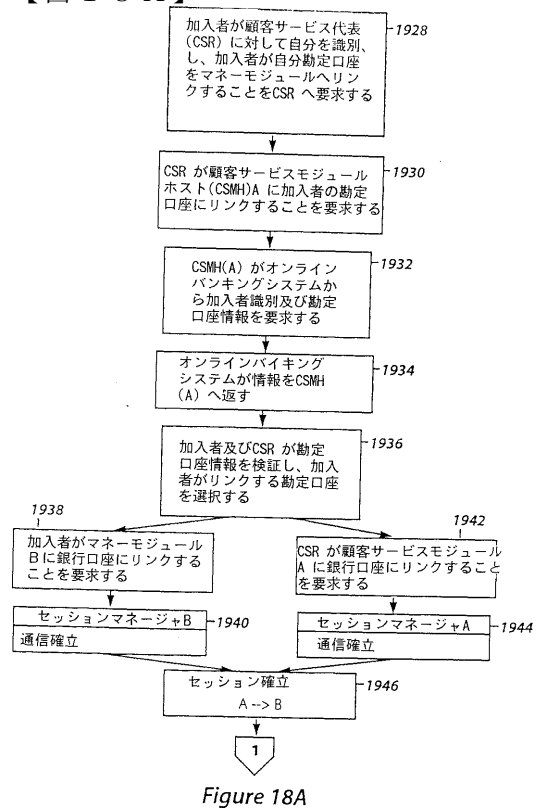


Figure 18A

【図 18 C】

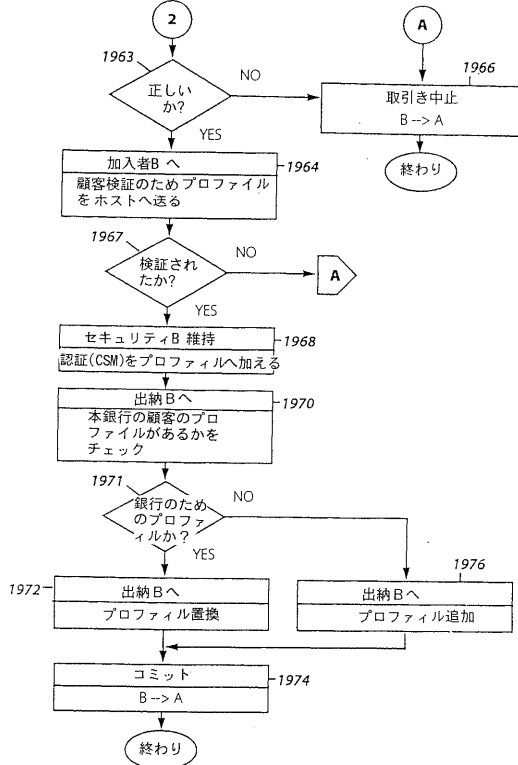


Figure 18C

【図 19 A】

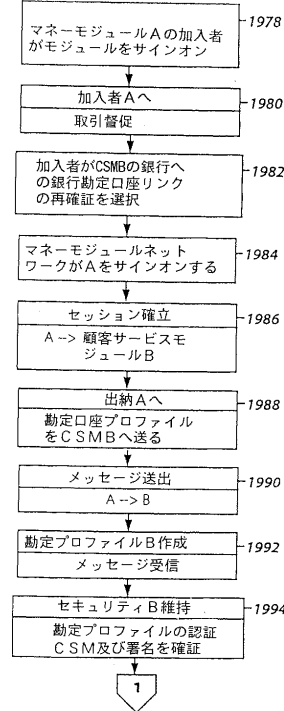


Figure 19A

【図 21 B】

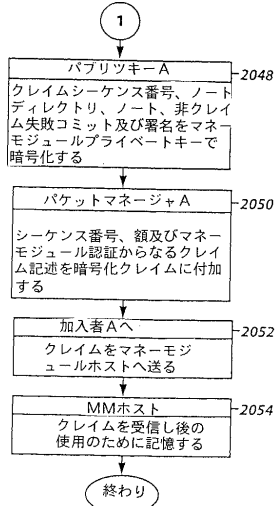


Figure 21B

【図 19 B】

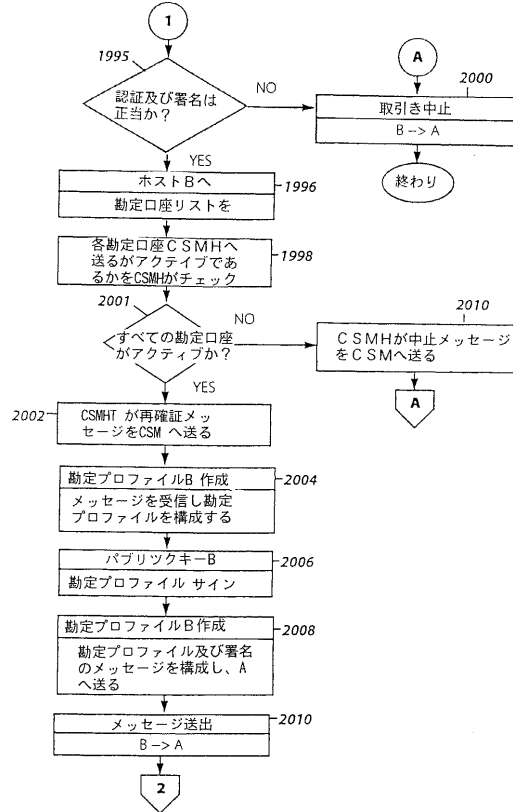


Figure 19B

【図 19 C】

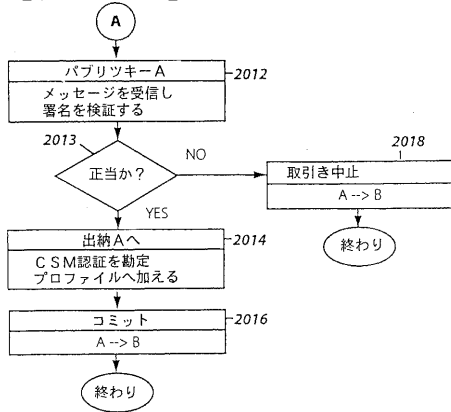


Figure 19C

【図 20】

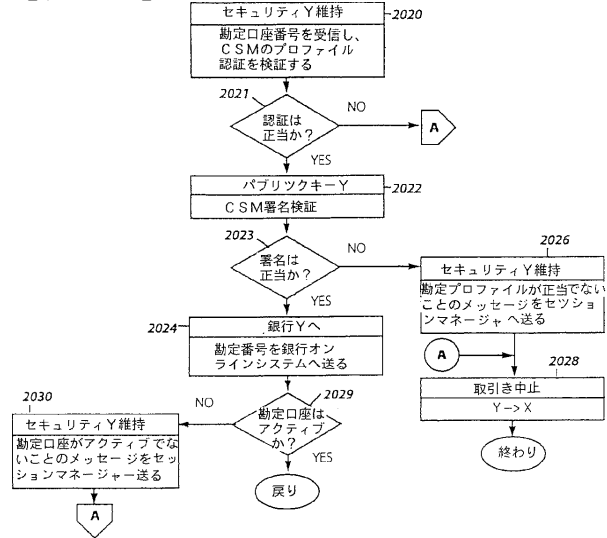


Figure 20

【図 22 A】

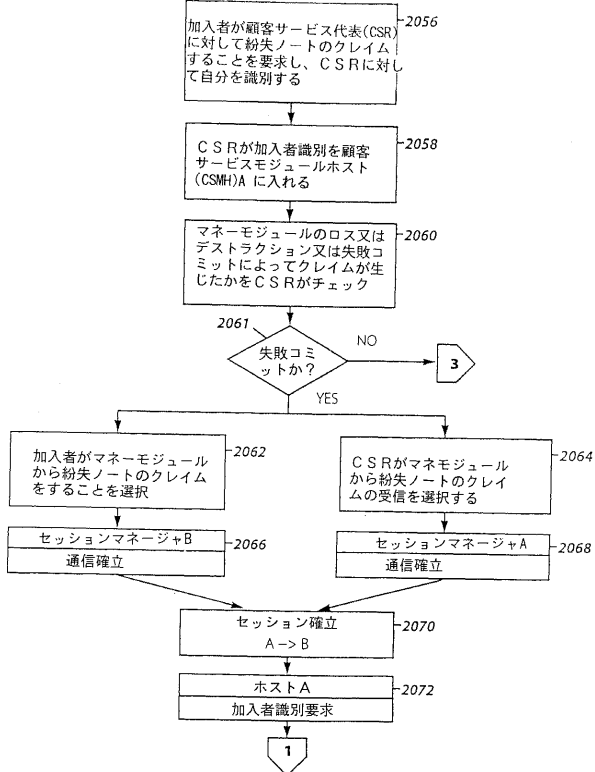


Figure 22A

【図 22 B】

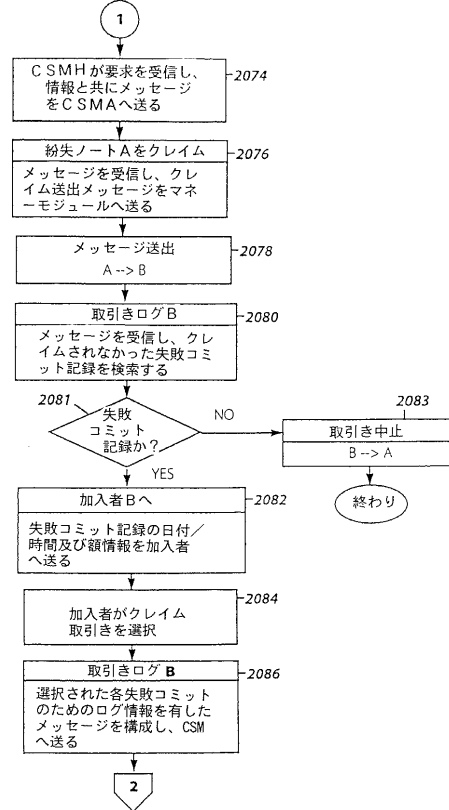


Figure 22B

【図 2 2 D】

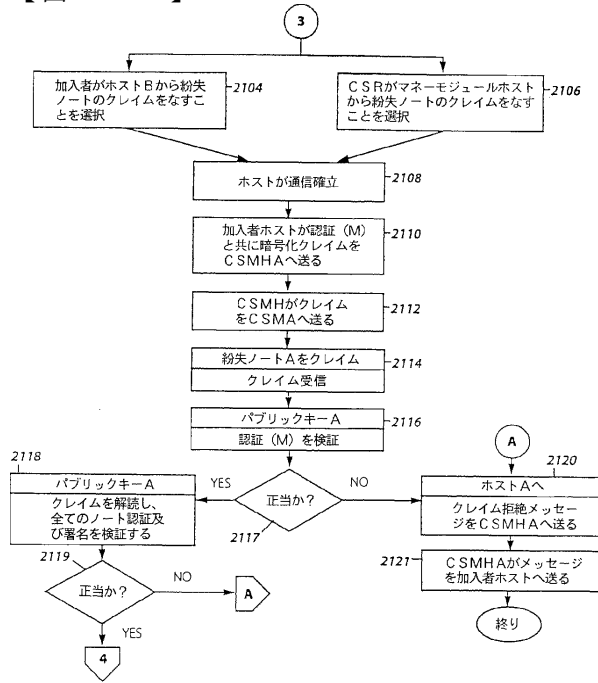


Figure 22D

【図 2 2 E】

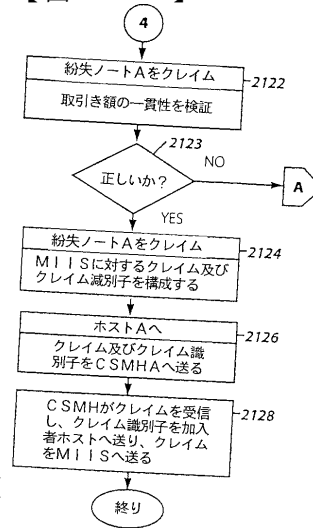


Figure 22E

フロントページの続き

(74)代理人 100084009

弁理士 小川 信夫

(74)代理人 100082821

弁理士 村社 厚夫

(72)発明者 ローゼン ショーラム エス

アメリカ合衆国 ニューヨーク州 10024 ニューヨーク ウェスト エイティシックス
ストリート 10 アpartment 7エイ

審査官 関 博文

(56)参考文献 特開平06-162059 (JP, A)

特開平06-020117 (JP, A)

特開平07-046323 (JP, A)

特開平06-035947 (JP, A)

(58)調査した分野(Int.Cl.⁷, DB名)

G06F 17/60

JICSTファイル(JOIS)