(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6101824号
(P6101824)

(45)発行日　平成29年3月22日(2017.3.22)　(24)登録日　平成29年3月3日(2017.3.3)

(51)Int.Cl.　F I
G06Q 20/38 (2012.01)　G06Q 20/38 ZIT
G06Q 20/38 312
G06Q 20/38 318
G06Q 20/38 322

請求項の数 20　(全 31 頁)

(21)出願番号　特願2015-557060 (P2015-557060)
(86)(22)出願日　平成26年2月6日(2014.2.6)
(65)公表番号　特表2016-513317 (P2016-513317A)
(43)公表日　平成28年5月12日(2016.5.12)
(86)国際出願番号　PCT/US2014/015050
(87)国際公開番号　WO2014/124108
(87)国際公開日　平成26年8月14日(2014.8.14)
審査請求日　平成27年9月29日(2015.9.29)
(31)優先権主張番号　61/761,654
(32)優先日　平成25年2月6日(2013.2.6)
(33)優先権主張国　米国(US)

(73)特許権者　503260918
アップル　インコーポレイテッド
アメリカ合衆国　９５０１４　カリフォルニア州　クパチーノ　インフィニット　ループ　1
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】セキュアエレメントのトランザクション及びアセットの管理のための装置及び方法

(57)【特許請求の範囲】
【請求項１】
セキュアエレメントを含むクライアント装置へアセットを分配するための、１つ以上のアカウントサーバを含む、アセットブローカのための方法であって、前記方法は、前記アセットブローカが、少なくとも、
前記クライアント装置から、（ｉ）前記アセットをアカウントへ提供する要求と、（ｉｉ）前記クライアント装置を一意的に識別する装置識別子と、を受信することと、
前記アセットを前記アカウントへ提供する前記要求を認証することと、
前記クライアント装置に割り当てられている前記アセットを一意的に識別するアセット識別子をアセットロッカーから受信することと、
前記アセット識別子を前記クライアント装置へ送信することと、
前記割り当てられたアセットに対する要求を前記クライアント装置から受信することと、
前記アセット識別子を前記クライアント装置から受信することと、
前記割り当てられたアセットを前記クライアント装置へ送信することと、
を含むことを特徴とする方法。
【請求項２】
前記方法は、前記アセットブローカが、
前記アセット識別子を前記アセットロッカーから受信することの前に、
前記装置識別子に関連付けられている電子署名を前記クライアント装置から受信する

こと、
　前記電子署名をアセットエージェントへ送信することと、
を更に含み、前記送信された電子署名が前記アセットエージェントにより検証されていることを特徴とする、請求項１に記載の方法。
【請求項３】
前記方法は、前記アセットブローカが、
前記電子署名を前記アセットエージェントへ送信することに続き、
　前記セキュアエレメントにより生成されたチャレンジを前記クライアント装置から受信することと、
　前記チャレンジを前記アセットエージェントへ送信することと、
を更に含み、前記送信されたチャレンジが前記アセットエージェントにより検証されていることを特徴とする、請求項２に記載の方法。
【請求項４】
前記アセットを前記アカウントへ提供する前記要求を認証することが、前記装置識別子が前記アカウントに関連付けられていることを検証することを含むことを特徴とする、請求項１に記載の方法。
【請求項５】
前記方法は、前記アセットブローカが、
前記割り当てられたアセットを、前記クライアント装置又は前記装置識別子と関連付けることを更に含むことを特徴とする、請求項１に記載の方法。
【請求項６】
前記方法は、前記アセットブローカが、
前記割り当てられたアセットを前記クライアント装置へ送信することに続き、前記割り当てられたアセットの値に基づいて前記アカウントを借方記入することを更に含むことを特徴とする、請求項１に記載の方法。
【請求項７】
前記割り当てられたアセットが、前記クライアント装置からの前記受信したチャレンジに基づくチャレンジデータを含むことを特徴とする、請求項３に記載の方法。
【請求項８】
前記方法は、前記アセットブローカが、
前記アセットを前記アカウントへ提供する前記要求を受信することの前に、ユーザアカウントを識別するアカウント情報を前記クライアント装置から受信することを更に含むことを特徴とする、請求項１に記載の方法。
【請求項９】
前記方法は、前記アセットブローカが、
前記割り当てられたアセットを、第１の地理的位置と、前記第１の地理的位置とは別の第２の地理的位置と、に記憶することを更に含み、
前記割り当てられたアセットを前記クライアント装置へ送信することが、前記割り当てられたアセットを前記第１の地理的位置から、又は前記第２の地理的位置から送信することを含み、前記クライアント装置が、前記送信された、割り当てられたアセットを、前記送信された、割り当てられたアセット内に埋め込まれたチャレンジデータに基づいて検証するよう構成されていることを特徴とする、請求項１に記載の方法。
【請求項１０】
セキュアエレメントを含むクライアント装置へアセットを分配する１つ以上の装置のための方法であって、それぞれの装置が、メモリと、プロセッサと、を含み、少なくとも、
前記クライアント装置を一意的に識別する装置識別子に基づいて、ユニークキーとともに前記アセットを暗号化することと、チャレンジデータを前記アセット内に埋め込むことと、により、前記アセットを予め構成することと、
前記予め構成されたアセットをアセット識別子と関連付けることと、
前記アセット識別子を含む要求を前記クライアント装置から受信することと、

前記要求を受信したことに応じて、前記予め構成されたアセットを前記クライアント装置へ配信することと、
を含むことを特徴とする方法。
【請求項１１】
前記方法は、前記１つ以上の装置が、
前記アセットを予め構成することの前に、ユーザアカウントを識別するアカウント情報を前記クライアント装置のユーザから受領することを更に含むことを特徴とする、請求項１０に記載の方法。
【請求項１２】
前記アセットを予め構成することが、前記アセットをユーザアカウントと関連付けることを更に含むことを特徴とする、請求項１０に記載の方法。
【請求項１３】
前記方法は、前記１つ以上の装置が、
前記アセットを予め構成することの前に、前記アセット識別子を前記クライアント装置へ提供することを更に含むことを特徴とする、請求項１０に記載の方法。
【請求項１４】
前記方法は、前記１つ以上の装置が、
前記予め構成されたアセットを、第１の地理的位置と、前記第１の地理的位置とは別の第２の地理的位置と、に記憶することを更に含み、
前記予め構成されたアセットを前記クライアント装置へ配信することが、前記予め構成されたアセットを前記第１の地理的位置から、又は前記第２の地理的位置から配信することを含み、前記クライアント装置が、前記配信された、予め構成されたアセットを、前記配信された、予め構成されたアセット内に埋め込まれた前記チャレンジデータに基づいて検証するよう構成されていることを特徴とする、請求項１０に記載の方法。
【請求項１５】
前記方法は、前記１つ以上の装置が、
前記アセットを予め構成することの前に、前記装置識別子を、前記クライアント装置に関連付けられている箱上に配設されたラベル又は証印から取得することを更に含むことを特徴とする、請求項１０に記載の方法。
【請求項１６】
前記要求が、前記アセット識別子に関連付けられている電子署名を含むことを特徴とする、請求項１０に記載の方法。
【請求項１７】
アセットをリモートサーバから要求するよう構成されたクライアント装置であって、前記クライアント装置が、
アプリケーションプロセッサと、
記憶装置であって、前記アプリケーションプロセッサにより実行されると、前記クライアント装置に、
アセットをアカウントへ提供する要求を前記リモートサーバへ送信させ、
前記クライアント装置を一意的に識別する装置識別子を前記リモートサーバへ送信させ、前記送信された装置識別子は、前記アセットを提供する前記要求を認証するために使用されており、
前記クライアント装置のセキュアエレメントからチャレンジを取得させ、
前記チャレンジを前記リモートサーバへ送信させる
命令を記憶するよう構成された記憶装置と、
前記セキュアエレメントであって、
セキュアプロセッサと、
セキュアメモリであって、前記セキュアプロセッサにより実行されると、前記セキュアエレメントに、
前記アセットを前記リモートサーバから受信させ、前記受信したアセットは、前記リ

モートサーバへ送信された前記チャレンジに基づくチャレンジデータを含み、
　前記受信したアセットを、前記チャレンジデータに基づいて検証させる
命令を記憶するよう構成されたセキュアメモリと、
を含む前記セキュアエレメントと、
を備えることを特徴とするクライアント装置。
【請求項１８】
前記セキュアプロセッサにより実行されると、前記受信したアセットを検証することに続き、前記セキュアエレメントに、前記チャレンジを前記セキュアエレメントから削除させる命令を記憶するよう、前記セキュアメモリが更に構成されていることを特徴とする、請求項１７に記載のクライアント装置。
【請求項１９】
前記セキュアプロセッサにより実行されると、前記セキュアエレメントに、
新たなチャレンジを生成させ、
前記新たなチャレンジを前記セキュアエレメント上に記憶させる
命令を記憶するよう、前記セキュアメモリが、更に構成されていることを特徴とする、請求項１８に記載のクライアント装置。
【請求項２０】
前記アプリケーションプロセッサにより実行されると、前記装置識別子を前記リモートサーバへ送信することの前に、前記クライアント装置に、前記装置識別子を前記セキュアエレメントから取得させる命令を記憶するよう、前記記憶装置が更に構成されていることを特徴とする、請求項１７に記載のクライアント装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は全般的にセキュア機器のトランザクションの分野に関し、より詳細には、例示的な一実施形態における、金融商品及び他のアセットの展開に関する。
【背景技術】
【０００２】
顧客及び小売商は一般に、金融及び他の関連するトランザクションを行うための便利でセキュアな手段を望む。クレジットカード、デビットカード、プリペイドカード、ギフトカード、クーポン、等、といったアセットはすべて、大きく「仮想化」された性質の通貨の例である。具体的には、商品及び／又はサービスに対して物理的な通貨又は物理的なクーポンを実際に交換するのではなく、トランザクションは、例えば、口座番号又は「プロキシ」口座番号（例えば、店頭でのトランザクションの処理を目的に作成されたものであり、実際の貸方（credit）口座番号でも借方（debit）口座番号でもない）とともに行われており、資金は電子的に貸方記入／借方記入されている。
【０００３】
残念ながら、本明細書に詳述する理由により、それらのアセットを分配するための既存のソリューションは非効率であり、上手くいかない傾向にある。例えば、バーチャルウォレットパラダイムは、先存するアカウントに基づくことができ、金融取引を行うため、クライアント装置のユーザは、ウォレットサービスを伴う先存するアカウントを有する必要がある、（例えば、ウォレットに関連付けられているアカウンティングデータベースを提供する信頼されたエンティティ）、又はウォレットサービスに先払いしておく必要がある。加えて、既存のアセットは「代替可能」でなく、作成されると特定の用途専用となる。
【０００４】
顧客及び小売商は、トランザクション上の複雑さ及び／又は利便性（更に広がるモバイルデバイスの使用を含む）において着実に進化しているため、アセットを分配するための新規及び改善されたスキームが必要となっている。理想的には、そのようなソリューションは、顧客、小売商、及び振り出しエンティティに対して、アセットのフレキシビリティを損なうことなく、合理的で便利な管理機能を提示すべきである。

【発明の概要】
【０００５】
本開示は、特に、セキュアエレメントのトランザクション及びアセットの管理のための装置及び方法を提供することで、先のニーズに対処する。
【０００６】
一実施形態では、アセットをクライアント装置へ分配するための方法が開示されている。この方法は、アセットをアカウントへ提供する要求をクライアント装置から受信することにより実行され得る。アセットを提供する要求は、クライアント装置を一意的に識別する装置識別子が伴われ得る。次に、アセットを提供する要求は認証される。ある場合には、アセットを提供する要求は、装置識別子を使用して、クライアント装置がアカウントに関連付けられているか検証することにて認証されている。要求を認証すると、アセットはアカウントに提供され、このアセットはクライアント装置に割り当てられる。次に、割り当てられたアセットを一意的に識別するアセット識別子が、アセットロッカーなどのリモート装置から受信される。アセット識別子は続いて、クライアント装置に送信される。その後、クライアント装置は、アセット識別子を使用して、割り当てられたアセットを要求し得る。割り当てられたアセット及びアセット識別子に対する要求をクライアント装置から受信すると、割り当てられたアセットは、クライアント装置に配信される。
【０００７】
別の実施形態では、アセットをクライアント装置へ分配するための方法が開示されている。クライアント装置は、クライアント装置を一意的に識別する装置識別子に関連付けられている。この方法は、クライアント装置に対するアセットを予め構成することにより実行されている。予め構成するプロセスは、（ｉ）装置識別子に基づいてユニークキーとともにアセットを暗号化すること、（ｉｉ）アセットにチャレンジデータを埋め込むこと、及び／又は（ｉｉｉ）アセットをユーザアカウントと関連付けること、を含み得る。それに応じて、アセットは、クライアント装置に対して構成される又は「パーソナライズ」される。次に、予め構成されたアセットが、アセット識別子に関連付けられる。実施形態の一態様では、アセット識別子は、アセットを予め構成することの前に、クライアント装置に提供されている。クライアント装置は続いて、予め構成されたアセットを要求し得る。この要求は、アセット識別子を含み得る。要求を受信すると、予め構成されたアセットは、クライアント装置に配信され得る。
【０００８】
更に別の実施形態では、コンピュータ可読記憶媒体が開示されている。コンピュータ可読記憶媒体は、クライアント装置のプロセッサにより実行されると、クライアント装置に、アセットをアカウントへ提供する要求を送らせる命令を記憶する。要求は、リモート装置へ送信され得る。アカウントは、クライアント装置のユーザに関連付けられ得る。要求と併せて、クライアント装置は、クライアント装置を一意的に識別する装置識別子を送り得る。実施形態の一態様では、装置識別子は、クライアント装置内に配設されたセキュアエレメント上に記憶されている。更に、１つ以上のチャレンジも、セキュアエレメント上に記憶され得る。命令は更に、クライアント装置に、チャレンジをリモート装置へ送信させる。クライアント装置は続いて、リモート装置からアセットを受信し得る。受信したアセットは、受信したアセットが有効であるか検証するためにセキュアエレメントが使用し得るチャレンジデータを含み得る。チャレンジデータは、送信されたチャレンジに基づくことができる。
【０００９】
この説明される実施形態の概要は、本明細書で説明する主題のいくつかの態様の基本的理解を提供するように、いくつかの例示的実施形態を要約することを目的として提供されるものにすぎない。したがって、上述した特徴が例にすぎず、いかなる方法でも本明細書で説明する主題の範囲又は趣旨を狭めるように解釈すべきではないことが了解されよう。本明細書で説明する主題の他の特徴、態様及び利点は、後続の詳細な説明、図及び請求の範囲から明らかになるであろう。

【００１０】
本発明の他の態様及び利点は、例として、説明される実施形態の原理を例示する添付図とともに考慮される、下記の「発明を実施するための形態」から明らかとなるであろう。
【図面の簡単な説明】
【００１１】
記載の実施形態は、以下の記載及び添付の図面を参照することによって一層良好に理解することができる。加えて、以下の記載及び添付の図面を参照することにより、記載の実施形態の利点を一層良好に理解することができる。
【００１２】
【図１】本開示による、トランザクショナルネットワークの１つの例示的な構成の図形表現である。
【００１３】
【図２】本開示による、プロビジョニングシステムの１つの例示的な構成の図形表現である。
【００１４】
【図３Ａ】本開示による、クライアント装置の例示的な一実施形態の論理ブロック図である。
【００１５】
【図３Ｂ】本開示による、小売商装置の例示的な一実施形態の論理ブロック図である。
【００１６】
【図４】本開示による、アセットエージェントの例示的な一実施形態の論理ブロック図である。
【００１７】
【図５】本開示による、アセットブローカのアカウントサーバの例示的な一実施形態の論理ブロック図である。
【００１８】
【図６】本開示による、アセットロッカーの例示的な一実施形態の論理ブロック図である。
【００１９】
【図７】本開示による、アセットを分配するための一般化された方法の一実施形態の論理フローダイアグラムである。
【００２０】
【図８】本開示による、例示的なプロビジョニングトランザクションを表す論理ラダーダイアグラムである。
【００２１】
【図９Ａ】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。
【図９Ｂ】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。
【００２２】
【図１０Ａ】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。
【図１０Ｂ】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。
【００２３】
【図１１】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。
【００２４】
【図１２】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。

【００２５】
【図１３Ａ】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。
【図１３Ｂ】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。
【図１３Ｃ】本開示による、アセットを分配するための一般化された方法の別の実施形態の論理フローダイアグラムである。
【発明を実施するための形態】
【００２６】
本出願による方法及び装置の代表的な適用を、本セクションで説明する。これらの実施例は、説明する実施形態を理解する上での文脈と手助けを加えることのみを目的として提供される。それゆえ、説明される実施形態は、これらの具体的な詳細の一部又はすべてを伴わずに実践することができる点が、当業者には明白となるであろう。他の場合、説明される実施形態を不必要に不明瞭化することを回避するために、周知のプロセスステップは、詳細には説明されていない。他の適用が可能であり、以下の例は限定的なものと解釈されるべきでない。
【００２７】
以下の発明を実施するための形態では、その説明の一部を形成し、説明される実施形態による具体的な実施形態が実例として示される、添付図面が参照される。これらの実施形態は、当業者が説明される実施形態を実施できるように十分詳細に説明されるが、これらの例は限定的なものでなく、他の実施形態が使用されてもよく、説明される実施形態の趣旨又は範囲から逸脱せずに変更が行われてもよいということが理解されよう。
【００２８】
仮想化された「ウォレット」は、顧客、小売商、及び金融機関に対して大きな利点を提供し得る。仮想化されたウォレットのバーチャル「コンテンツ」は、１つ以上のアセット含み得る。いずれのエンティティ（例えば、ユーザ、小売商、金融機関、等）も、適切に有効にされたセキュア機器との間でそれらのアセットを自由に転送し得、そのうえ、それらのアセットはフレキシブルに記憶、バックアップ、等、され得る。既存のソリューションは、例えば、分配、アップデート、パッチング、等、特定の基本トランザクションを、インターネットプロトコル（ＩＰ）ネットワークを介して提供する。しかし、金融トランザクション及び情報の機密性により、窃盗、悪用、悪意のある行為、等を防止するために有意のセキュリティ対策が必要である。
【００２９】
本説明の文脈について、本開示を通しての実施形態は、仮想化交換媒体（ＶＭＥ）の形式をとるアセットを説明することに注意すべきである。仮想化交換媒体の一般例は、クレジット「カード」番号、デビット「カード」番号、プリペイド「カード」番号、アカウント情報、及び仮想通貨、等、を含むがこれらに限定しない。より一般的には、仮想化交換媒体はまた、例えば、電子クーポン、電子商品券、電子チケット、電子パス、等、実際の価値を伴わない手段も包含する。この説明は限定するものでなく、説明された実施形態は、有用なもの及び／又は価値のあるものすべての分配に使用され得ることが理解されるべきである。更に、ＶＭＥは、複雑さにおいて多岐に渡る、多種多様なデータ構造（例えば、ストリング、アレイ、オブジェクト、暗号エレメント、等）内に実装され得、例えば、シンプルな実装は、シンプルな口座番号とされ得、より複雑な実装は、アカウント情報、及び／又はチェック値を組み込み得る。いくつかの場合では、ＶＭＥは、例えば、暗号保護、アカウンタビリティ（つまり、トランザクション履歴）、匿名性、不正検知、等、といった、更なる機能を提供し得る。
【００３０】
説明された実施形態は、セキュアトランザクション及びＶＭＥの管理のための方法及び装置に関する。一実施形態では、プロビジョニングシステムは、ＶＭＥをクライアント装置へ分配する。プロビジョニングシステムは、Ｌ１、Ｌ２、及びＬ３として参照され得る

、３つのレベルを有するセキュリティプロトコルにしたがってＶＭＥを管理し、クライアント装置へ分配する１つ以上のエンティティを含む。Ｌ１では、ＶＭＥは安全に生成され、記憶され、及び暗号化されている。Ｌ１は、１つ以上のアセットロッカーにより促進され得る。Ｌ２は、ＶＭＥの有効なコピー数を制御及び管理する。Ｌ２は、ＶＭＥの不注意な複製及び／又は悪意のある複製を防ぎ得る。実施形態の一態様では、Ｌ２は、１つ以上のチャレンジを使用し得、ＶＭＥの第１のコピーが分配された後での、ＶＭＥの二重のコピーを無効にする。Ｌ２は、１つ以上のアセットエージェントにより促進され得る。Ｌ３は、意図されたクライアント装置へのアセットの分配を認証及び認可する。実施形態の一態様では、Ｌ３は、認証プロセス中に、クライアント装置内に配設されたセキュアエレメントから取得した識別子を使用し得る。Ｌ３はまた、認証プロセス中に、ユーザのアカウントに関連付けられている情報を使用し得る。Ｌ３は、１つ以上のアセットブローカにより促進され得る。

【００３１】

一実施形態では、クライアント装置とプロビジョニングシステムとの間のプロビジョニングトランザクションが開示されている。プロビジョニングシステムは、アセットブローカと、アセットエージェントと、アセットロッカーと、を含む。クライアント装置は、クライアント装置に関連付けられている装置識別子を含む。識別子は、クライアント装置内に配設されたセキュアエレメント内に記憶され、暗号化され得る。ユーザアカウントは、クライアント装置がユーザ（つまり、顧客）により購入されると作成され得る。あるいは、ユーザアカウントは、クライアント装置が購入されると、ユーザにより識別される、先存するアカウントとされ得る。クライアント装置は、アセットブローカからＶＭＥを要求し、例えば、装置識別子などの識別情報を提供する。アセットブローカは、識別情報を認証し、ＳＥ／クライアント装置がユーザアカウントに関連付けられていることを判定する。認証されると、アセットブローカは、ＳＥの署名をアセットエージェントに転送し得る。アセットエージェントは、セキュアエレメントの識別を検証し、セキュアエレメントに対するＶＭＥを識別する。次に、セキュアエレメントは、チャレンジをプロビジョニングシステムへ提供する。提供されたチャレンジに基づくチャレンジデータは、アセットエージェントにより、ＶＭＥ内に埋め込まれ得る。それに応じて、チャレンジデータは、ＶＭＥのコピーが二重に発行されることの防止に使用され得る。アセットロッカーは続いて、クライアント装置のセキュアエレメントに対して、ＶＭＥに関連付けられている識別子、例えば、ＶＭＥ識別子を提供し得る。ＶＭＥ識別子を受信すると、クライアント装置はその後、ＶＭＥ識別子を使用して、アセットブローカからＶＭＥの配信を要求し得る。

【００３２】

別の実施形態では、ＶＭＥの構成及び配信は、セキュアエレメントを有するクライアント装置をユーザが購入するまで延期され得る。このようにして、クライアント装置は、ＶＭＥを伴って製造又は予めプログラムされない。むしろ、クライアント装置は、クライアント装置をユーザへ配信することの前に、ＶＭＥに予め割り当てられているよう、「予めパーソナライズ」されている。「予めのパーソナライゼーション」プロセスは、プロビジョニングシステム内に記憶されたＶＭＥを、クライアント装置に関連付けられている識別子と関連付けることを含み得る。購入時には、認証情報がユーザにより提供される。移送期間中（例えば、ユーザがクライアント装置を購入した時と、ユーザがＶＭＥを要求した時との間の時間、及び／又は、クライアント装置をユーザへ出荷するために要する時間との間）は、ＶＭＥは、クライアント装置に対して予め構成され得る。ＶＭＥを予め構成することは、（ｉ）セキュアエレメントに特有のキーを伴ってＶＭＥを暗号化することと、（ｉｉ）ＶＭＥ内にチャレンジデータを埋め込むことと、（ｉｉｉ）ＶＭＥを認証情報と関連付けること、を含み得る。ＶＭＥは続いて、ＶＭＥ識別子に関連付けられる。次に、クライアント装置は、ＶＭＥ識別子を使用してＶＭＥを要求し得る。同様に、プロビジョニングシステムは、予め構成されたクライアント装置へＶＭＥを配信し得る。このようにして、ＶＭＥは、リアルタイムでのトラフィックを必要とすることなく、ＶＭＥが要求されると、クライアント装置に途切れなくロードされ得る。

【００３３】
更に別の実施形態では、ＶＭＥのプールからのＶＭＥは、ＶＭＥに対する要求をクライアント装置から受信する前に、クライアント装置に対して割り当てられている（例えば、ＶＭＥのプール内のそれぞれのＶＭＥは、最初は、特定のクライアント装置に関連付けられていない）。クライアント装置が購入されると、認証情報がユーザにより提供される。クライアント装置はユーザへ提供され得る。クライアント装置に加えて、クライアント装置を認証するために使用され得る識別情報、例えば、クライアント装置を一意的に識別する装置識別子も、ユーザへ提供される。例えば、装置識別子は、クライアント装置が梱包されている箱上に配設されたステッカから収集され得る。クライアント装置は続いて、ユーザの命令にて、ＶＭＥのアクティベーションを要求する際に、装置識別子をプロビジョニングシステムへ提供し得る。

【００３４】
それら及び他の実施形態が、図１～図１３Ｃを参照して以下に説明されている。しかしながら、これらの図に関して本明細書に記載される「発明を実施するための形態」は、説明を目的とするものにすぎず、限定するものとして解釈するべきではないことが、当業者には容易に理解されるであろう。

【００３５】
ここで図１を参照すると、１つの例示的トランザクショナルネットワーク１００が示される。例示的トランザクショナルネットワーク１００は、１つ以上のクライアント装置１０２と、１つ以上の小売商装置（「販売時点情報管理システム」（ＰＯＳ）とも呼ばれる）１０４と、１つ以上のバックエンドサーバ１０６と、を含む。先のトランザクショナルネットワーク１００は、広範に可能なネットワークトポロジ及び機能を単に示していることが、当業者には容易に理解されるであろう。そのうえ、様々な実装は、図１に示す様々なエンティティを組み合わせてもよく、及び／又は更に分割してもよいことが認識されるべきである。

【００３６】
トランザクションは、クライアント装置１０２がトランザクション情報を暗号により符号化し、小売商装置１０４へ送信すると行われる。一例では、クライアント装置１０２は、例えば、（近距離無線通信（ＮＦＣ）、等といった）適切なリーダー上でスワイプすること、グラフィカルユーザインタフェース（ＧＵＩ）からトランザクション識別子（例えば、バーコード、数字、等）を目視確認することに、等により、トランザクションを小売商装置１０４とともに実行するよう構成されたバーチャル「ウォレット」を含み得る。別の例では、クライアント装置１０２は、クライアント装置１０２の存在を小売商装置１０４（例えば、レジスター、モバイルタブレット、等）にアラートするために使用されている、全地球測位システム（ＧＰＳ）受信機又は他の位置情報（例えば、Ｗｉ－Ｆｉ（登録商標）の存在、等）を含み得、既知のユーザアカウントの課金を認可するため、それに続くクライアント装置１０２のユーザの妥当性検証（例えば、顔写真などの生体認証）が行われる。トランザクション情報は、（ｉ）エイリアス、（ｉｉ）増分カウンタ、（ｉｉｉ）乱数、（ｉｖ）小売商識別子、（ｖ）他のトランザクションエラッタ（例えば、取引金額、タイムスタンプ、ロケーションスタンプ、等）、の組み合わせを含み得る。

【００３７】
小売商装置１０４は、保護されたトランザクション情報をバックエンドサーバ１０６へ提供する。その後は、バックエンドサーバ１０６は、保護されたトランザクション情報を復号し、トランザクションを検証し、トランザクションを適切に処理し得る。例えば、エイリアス値がクレジットカード番号にマップされており、暗号化された情報が正しいと、続いてバックエンドサーバ１０６が、エイリアス値にマップされているクレジットカード番号とともにトランザクションを処理する。あるいは、トランザクション情報が破損している、又は不正であることが判明すると、トランザクションは拒否される。

【００３８】
例示的トランザクショナルネットワーク１００内では、トランザクション情報に適用さ

れた暗号保護は、ユーザの価値のある情報をいずれの悪意のある他者及び／又は小売商から保護する。具体的には、悪意のある他者がトランザクション情報を奪おうとしても、又は、小売商装置１０４が（例えば、ウイルス、等に）感染していても、暗号保護は、トランザクションが後に不正に再生されることを防止するよう援助し得る。それに応じて、ユーザ保護を最大化するため、暗号エレメントは、セキュアプロセッサ、セキュアファイルシステム、及びオペレーショナルメモリを含んでもよい、クライアント装置１０２内に配設されたセキュアエレメント内に物理的に保護されている。しかし、クライアントの機器内に記憶された暗号マテリアルのセキュリティを保つことが難しいことを当業者は認識するであろう。例えば、１つのそのような問題は、初期構成、展開、及び保守である。クライアント装置は、（信頼されていない場合もある）機器製造業者により製造されている。また、特定のビジネスモデルは、（信頼されていない場合もある）第三者としての参加者の市場に依存することもある。

【００３９】

理想的には、暗号マテリアルを分配するためのソリューションは、大規模分配ネットワークに渡ってスケーラブルであるべきである。そのうえ、分配スキームは、暗号マテリアル（証明書）を、いずれの仲介エンティティ（例えば、機器製造業者、第三者ブローカ、等）から保護しなければならない。いくつかの実施形態では、暗号マテリアルは固有であるべきである（つまり、単一のアセットインスタンスが単一のセキュアエレメントのみの内で一度に使用可能である）。最後に、ソリューションは、リアルタイムでの双方向作用に対する要件を最小化すべきである。

【００４０】

ここで図２を参照すると、１つの例示的プロビジョニングシステム２００が示される。示すように、プロビジョニングシステム２００は、クライアント装置３００と、アセットエージェント４００と、アセットブローカ５００と、アセットロッカー６００と、を含む。前述するように、ＶＭＥ動作の文脈内では、ＶＭＥセキュリティは更に、レベル１（Ｌ１）、レベル２（Ｌ２）、及びレベル３（Ｌ３）を含むレベルに下位分割され得る。それぞれのレベルは、プロビジョニングシステム２００のエレメントにより促進され得る。

【００４１】

アセットロッカー６００は、レベル１（Ｌ１）のセキュリティにしたがってＶＭＥセキュリティを行うために使用され得る。本明細書にて使用されるように、レベル１のセキュリティは一般的に、ＶＭＥ内に含まれる秘密及び／又は暗号マテリアル（例えば、セキュアキー、暗号マテリアル、ユーザ履歴、等）を保護するよう構成されたセキュリティメカニズムを指すが、これらに限定しない。更に、用語「セキュリティ」とは、概して、データ及び／又はソフトウェアの保護を指す。例えば、暗号セキュリティは、ＶＭＥに関連付けられたデータ及び／又はソフトウェアを、無認可のアクティビティ及び／又は悪意の第三者による、窃盗、悪用、破壊、公開、及び／又は改竄から保護する。

【００４２】

アセットエージェント４００は、レベル２（Ｌ２）のセキュリティにしたがってＶＭＥセキュリティを行うために使用され得る。本明細書にて使用されるように、レベル２のセキュリティは一般的に、ＶＭＥの予期しない複製及び／又は悪意のある複製を防止するためのセキュリティメカニズムを指すが、これらに限定しない（保存エンフォースメント）。更に、用語「保存性」、「保存する」、及び「保存された」とは、本明細書で使用する時、簡単に増加又は減少させることができない、（物理的又は仮想的のいずれかの）要素を指す。例えば、保存されたＶＭＥは、通常動作の間にコピー又は複製することができない。更には、本明細書で使用する時、（物理的又は仮想的のいずれかの）要素に適用される用語「固有性」とは、その要素が、特定の特性及び／又は特質を有する唯一無二の要素であるという特性を指す。例えば、固有のＶＭＥは、複製のＶＭＥを有し得ない。

【００４３】

アセットブローカ５００は、レベル３（Ｌ３）のセキュリティにしたがってＶＭＥセキュリティを行うために使用され得る。本明細書にて使用されるように、レベル３のセキュ

リティは一般的に、意図されたユーザ（例えば、個人、企業、マシンクライアント、等）に関連付けられている機器（例えば、クライアント装置、ＰＯＳ、等）へＶＭＥを安全に配信するセキュリティメカニズムと呼ばれるが、これらに限定しない。その上に、本明細書で使用するように、用語「ユーザ認可」とは、概して、リソースに対するユーザのアクセスを指定することを指す。一般的な交換媒体（クレジットカード、デビットカード、現金）では、トランザクションは、媒体の物理的な所有を要求し得、物理的なカードは、ユーザにより保護されている。例えば、物理的なクレジットカードが使用される場合、カードはユーザの所有にある（及び、ユーザにより暗黙に認可されている）ことが想定されている。ＶＭＥ動作の文脈の範囲内では、ＶＭＥ移動のユーザ認可に対する類似の機能が必要である。特に、ＶＭＥの「所有者」（及び、プロビジョニングシステム２００も）は、ＶＭＥが１つ以上の正当な機器にのみ移されたことを保証する必要がある。

【００４４】

以降に明確にされる理由として、セキュリティのそれぞれのレベルは、限定された機能／責任一式に関連付けられており、したがって、レベル２のセキュリティを提供する機器は、レベル２に関連付けられているアクションを自由に行い得るが、ＶＭＥのレベル１のエレメントに影響を与えることが可能なレベル１のセキュリティでもある必要がある。例えば、（以下に詳述される）アセットエージェントは、ＶＭＥが複製されることを防止するが、しかし、このアセットエージェントは、ＶＭＥ内に含まれる暗号マテリアルを変更する機能を有する必要はなく、破損した暗号マテリアルを検出する義務を負うアセットエージェントである必要もない。

【００４５】

ＶＭＥセキュリティレベルの先の定義は純粋に例示的なものであり、本明細書の説明を限定する意図はない。事実、先の専門用語は当業者の間での「業界用語」とみなされるべきであり、関連産業及び／又は技術の初期の進化の点から変更されるであろうことが理解されよう。

【００４６】

ソフトウェアは一般的に、ハードウェアよりも柔軟であり、例えば、ソフトウェアは、コピー、修正、及び配布が容易であることが理解されよう。更には、ソフトウェアは、多くの場合、ハードウェアの均等物よりも安価に、電力効率的に、物理的に小さく作製することができる。しかし、ＶＭＥデータの機密性（例えば、顧客財務情報、アセットブローカの暗号の秘密、等）は特別な配慮が必要とされる。ユーザ保護のために、ＶＭＥの意図されない複製、及び／又は破損が防止されなければならないことが予期される。それに応じて、ＶＭＥ動作は、（ｉ）セキュリティ、（ｉｉ）固有性、及び（ｉｉｉ）保存の特性を満たすべきである。

【００４７】

例示的な一実施形態では、セキュアエレメントへのＶＭＥの配信を有効にする分配インフラストラクチャが開示されている。セキュアエレメントは、クライアント装置及び／又は小売商装置内に配設され得る。そのうえ、開示されているインフラストラクチャの様々な機能は、個人（例えば、機器製造業者、第三者小売商、顧客、等）が、インフラストラクチャの各部をホストし得るよう、フレキシブルに仕切られ得及び／又は適合され得、そのような断片的なソリューションは、それぞれ個々の当事者のニーズに最適化され得る。依然として更に、例示的な実施形態は、動作における冗長性を提供し得る。

【００４８】

ここで図３Ａを参照すると、１つの例示的なクライアント装置３００が提示されている。例示的なクライアント装置３００は、クライアントと小売商との間のインタフェース３０２と、プロセッササブシステム３０４と、非一時的コンピュータ可読媒体（メモリサブシステム）３０６と、セキュアエレメント３０８と、を含む。いくつかの変形例では、セキュアエレメント３０８は、セキュアプロセッサ３０８Ａと、セキュアな非一時的コンピュータ可読媒体（セキュアメモリ）３０８Ｂと、を更に含む。本明細書にて使用されるように、用語「クライアント装置」は、ユーザのＶＭＥのうちの１つ以上と取引及び／又は

管理するよう構成されている機器を含むがこられに限定しない。クライアント装置の一般例は、特に、無線対応セルラー電話、（例えば、ｉＰｈｏｎｅ（登録商標）などの）スマートホン、無線対応パーソナルコンピュータ（ＰＣ）、ハンドヘルドコンピュータなどのモバイルデバイス、携帯情報端末（ＰＤＡ）、パーソナルメディア機器（ＰＭＤ）、（例えば、ｉＰａｄ（登録商標）などの）ワイヤレスタブレット、いわゆる「ファブレット」、又は先のいずれの組み合わせである。

【００４９】

プロセッササブシステム３０４は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、１つ以上の基板上に実装された複数の処理構成要素のうちの１つ以上を含み得る。プロセッササブシステム３０４はまた、内部キャッシュメモリも含み得る。プロセッササブシステム３０４は、メモリサブシステム３０６と通信し、後者は、例えば、スタティックランダムアクセスメモリ（ＳＲＡＭ）、フラッシュ、及び／又はシンクロナスダイナミックランダムアクセスメモリ（ＳＤＲＡＭ）構成要素を含み得るメモリを含む。メモリサブシステム３０６は、当該技術分野において周知であるように、データアクセスを容易にするために、ダイレクトメモリアクセス（ＤＭＡ）タイプのハードウェアのうちの１つ以上を実装し得る。例示的な実施形態のメモリサブシステム３０６は、プロセッササブシステム３０４により実行可能なコンピュータ実行可能命令を含む。

【００５０】

例示的な一実施形態では、クライアント装置３００は、１つ以上のインタフェース、例えば、小売商装置へ接続するよう適合された、クライアントと小売商との間のインタフェース３０２を含む。クライアントと小売商との間のインタフェース３０２は、無線インタフェース又は代替的に物理的インタフェース（有線）とすることができる。無線インタフェースは、最大で数センチメートルの操作範囲を有する（例えば、国際標準化機構（ＩＳＯ）規格１４４４３Ａ／Ｂに準拠し、その全体において参照により本明細書に組み込まれているそれらなどの、例えば、無線周波数識別（ＲＦＩＤ）、ＮＦＣ、等）「タッチ」又は「バンプ」タイプのインタフェースから、例えば、移動通信用のグローバルシステム（ＧＳＭ）（登録商標）、符号分割多元接続（ＣＤＭＡ）、ユニバーサル移動体通信システム（ＵＭＴＳ）、ロングタームエボリューション（ＬＴＥ）／ＬＴＥアドバンスト、ワールドワイドインターオペラビリティフォーマイクロウェーブアクセス（ＷｉＭＡＸ）（登録商標）、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ワイヤレスユニバーサルシリアルバス（ＵＳＢ）（登録商標）、等といった、より強力な無線インタフェースを含み得る。物理的インタフェースの一般例は、例えば、ＵＳＢ（登録商標）（例えば、ＵＳＢ　２．０、ＵＳＢ　３．０）、ＦｉｒｅＷｉｒｅ（登録商標）、Ｔｈｕｎｄｅｒｂｏｌｔ（登録商標）、等、を含む。そのうえ、特定の機器が、例えば、加入者識別モジュール（ＳＩＭ）カード又はクレジットカード、等、といった、「カード」タイプのフォームファクターを有し得ることが更に理解されよう。それら「カード」機器は、支払いリーダーの既存のエコシステムとの後方互換性を提供し得、一方で本明細書に説明する向上機能を依然としてサポートする。

【００５１】

いくつかの実施形態では、クライアント装置３００は、例えば、キーパッド、タッチスクリーン（例えば、マルチタッチインタフェース）、液晶ディスプレイ（ＬＣＤ）、バックライト、スピーカ、及び／又はマイクロホンが挙げられるがこれらに限定されない任意の数の周知のＩ／Ｏを含むユーザインタフェースサブシステムなどの、他の構成要素を更に含み得る。特定のアプリケーションでは、ユーザインタフェースは不要とされてもよいことが認識される。例えば、カードタイプクライアントの実施形態は、ユーザインタフェースを欠くことができる。

【００５２】

図示した実施形態では、クライアント装置３００は、セキュアエレメント３０８を含む。セキュアエレメント３０８は、この実施形態では、セキュアメモリ３０８Ｂ内に記憶さ

れたソフトウェアを実行する、セキュアプロセッサ３０８Ａを含む。セキュアメモリ３０８Ｂは、他の構成要素（セキュアプロセッサ３０８Ａ以外）に対してはアクセス不可である。更には、セキュアエレメント３０８は、改竄を防止するために、更に硬質にする（例えば、樹脂内に包み込む）ことができる。

【００５３】

セキュアエレメント３０８は、１つ以上のＶＭＥを受信し、転送し、そして記憶することが可能である。一実施形態では、セキュアエレメント３０８は、ユーザに関連付けられているＶＭＥの単一のアレイ又は複数のＶＭＥを記憶する（例えば、クレジット「カード」、デビット「カード」、プリペイドアカウント又はカード番号、バスの定期券、映画チケットの商品券、クーポン、「ロイヤリティ」プログラムエレメント、等）。いくつかの変形例では、それぞれのＶＭＥは、コンピュータ可読命令、及び関連データ（例えば、暗号キー、完全性キー、等）を含む、小型ファイルシステムに更に関連付けられ得る。

【００５４】

ファイルシステムは、更なる機能をサポートし得る。例えば、ファイルシステムは、例えば、セキュリティ（例えば、他のエンティティとの通信を保護するための認証プログラム、認可プログラム、及び暗号マテリアル）、ユーザ管理（例えば、勘定残高情報、最新のトランザクション履歴、等）、等のためのプログラム及びデータを含み得る。その関連ファイルシステムを伴うＶＭＥは、固有であり、保存されたデータアセットであることが、当業者には容易に理解されるであろう。

【００５５】

そのうえ、一実施形態では、セキュアエレメント３０８は、記憶されたＶＭＥ及びそれらの関連ファイルシステムのリスト又はマニフェストを維持する。マニフェストは、記憶されたＶＭＥの現在の状態についての情報を含み得、そのような情報は、例えば、可用性、妥当性、アカウント情報（例えば、経常勘定、等）、及び／又は以前に発生したエラーを含み得る。マニフェストは、利用可能なＶＭＥのユーザセレクションを有効にするよう、ユーザインタフェースに更にリンク又は連結され得る。いくつかの場合では、ユーザは、例えば、すべてのトランザクション、小売商とのすべてのトランザクション、期間内のすべてのトランザクション、等に対して、１つのＶＭＥをデフォルト（例えば、デフォルトクレジットカード）として選択し得る。

【００５６】

いくつかの変形例では、セキュアエレメント３０８は、１つ以上の関連機器の暗号キーを有し得る。それらの機器キーは、交換をセキュア化するために使用される。１つのそのような変形例では、暗号キーは、メッセージングトランザクションを暗号化するための一組の非対称パブリックキー／プライベートキーである。パブリックキーは、プライベートキーの完全性を損なうことなく自由に分配され得る。例えば、クライアント装置３００は、リベスト、シャミル及びアドルマン（ＲＳＡ）アルゴリズムに基づいて、パブリックキー／プライベートキーが割り当て（又は、内部生成）されてもよく、パブリックキーは、クライアント装置３００と安全に通信しようとするいずれの機器にも利用可能となる。クライアント装置３００のパブリックキーを用いて暗号化されたメッセージは、（クライアント装置３００内に安全に記憶された）クライアント装置自身のプライベートキーのみにより復号され得る。他の変形例では、暗号キーは対称である（つまり、暗号装置及び復号装置は同じキーを有する）。対称の変形例は、暗号論的に低減した複雑性を提供してもよいが、暗号装置及び復号装置の双方は、共用キーを強固に保護することを必要とする。

【００５７】

他の変形例では、セキュアエレメント３０８は、デジタル証明書を検証及び／又は発行するための暗号キーを有し得る。デジタル証明書は、例えば、（証明書の）発行者の識別の検証に使用され得る。例えば、セキュアエレメント３０８は、小売商装置が後に、（クライアント装置の署名付き証明書を回収することで）トランザクションが発生したことを証明できるよう、デジタル証明書を小売商装置へ発行し得る。同様に、セキュアエレメント３０８は、小売商装置が信頼され得ることを証明する、小売商装置から提供されたデジ

タル証明書を検証し得る。

【００５８】

クライアントと小売商との間のトランザクション（又は、クライアント／第三者の仲介トランザクション）中、セキュアエレメント３０８は、関連する１つ以上のＶＭＥとトランザクションを行う。簡易的な実施形態は、口座番号、「プロキシ」番号、又はそれらのサブセットの送信とされ得る。より複雑な変形例では、送信は、例えば、取引金額、暗号保護、証明情報（例えば、トランザクションの時刻／日付及び場所）、小売商ＩＤ情報、等、を組み込み得る。

【００５９】

本明細書に説明する多くの実施形態が、金融トランザクションの文脈において説明されている一方で、非金融トランザクションも等しく適している。例えば、商品券、チケット、等は、使用にしたがって、クレジット数を増分及び／又は減分され得る。他の例では、トランザクションは、妥当性チェック、例えば、バスの定期券が一定期間に有効であり（例えば、日数、週数、月数、年数、等）、したがって、その一定期間の任意の回数の使用は有効である、とされ得る。同様に、特定の種類のパスは、パスがそのブラックアウト期間に無効である、例えば、「ブラックアウト」日の対象とされてもよい。

【００６０】

いくつかの実施形態では、クライアントと小売商（又は、他）との間のトランザクションは、クライアント装置３００と小売商装置との間で共通の時間に行われ（つまり、クライアント装置３００及び小売商装置の双方に、同時にトランザクションが生じる）、例えば、ＮＦＣトランザクションでは、クライアント装置のＮＦＣインタフェースは、クライアント装置３００上の少なくとも一部のパッシブなＮＦＣ　ＩＣに信号を送信するインテロゲータなどの、小売商装置のＮＦＣインタフェースに近接して（「バンプして」）配設される。

【００６１】

しかし、代替のシナリオでは、クライアントと小売商との間のトランザクションは、時間シフト方式で行われ得ることが理解されよう。例えば、クライアント装置又は小売商装置が、トランザクションを最初に開始し、対応する機器が、後にトランザクションを認めてもよい。双方の機器がトランザクションを認めると、続いてトランザクションが完了され得る（例えば、適切な資金を送金すること、等）。例えば、クライアント及び小売商は、例えば、接続性のない農産物市場にて、トランザクションを行う。後に小売商装置がアセットブローカに接続すると、トランザクションが開始される。続いてその後は、クライアント装置がそのトランザクション記録と同期し、トランザクションが完了する。いくつかの場合では、アセットブローカは、未決済の課金が発生している場合に、クライアント装置に更に通知し得る。

【００６２】

ここで図３Ｂを参照すると、１つの例示的な小売商装置３５０が提示されている。例示的な小売商装置３５０は、小売商とクライアントとの間のインタフェース３５２と、プロセッササブシステム３５４と、非一時的コンピュータ可読媒体（メモリサブシステム）３５６と、ネットワークインタフェース３５８と、を含む。本明細書にて使用されるように、用語「小売商装置」は、ＶＭＥに対応するサーバ（例えば、バックエンドサーバ１０６）と取引する、及び／又は、（例えば、トランザクションを許可すべきか判定するため、等）サーバにクエリするよう構成されている機器を含むがこれに限定しない。用語「小売商」の使用は決して、何かを買う又は売るエンティティにより所有又は操作される機器に対するこの定義を制限することを意図するものではないことが理解されよう。むしろ、この用語は、トランザクションが商品、サービス、仮想の報酬、であってもトランザクション処理すること、資金又はクレジット、クーポンの償還を取得すること又は預金すること、等、のために構成された又は有効にされた装置を含むがこれらに限定しない装置のためにより広範に意図されている。小売商装置の一般例は、キオスク、自動預金受け払い機（例えば、ＡＴＭ）、「キャッシュ」レジスター、（例えば、ＲＦＩＤ又はバーコードベー

スの）モバイルチェックアウトリーダー、モバイルワイヤレスタブレット、及びスマートホンまでも含むがこれらに限定しない。そのうえ、小売商装置は歴史的に特殊用途タイプの機器である一方で、顧客向け電子機器の現在での急速な増加により、例えば、第三者、又は機器ユーザ自身による、製作時、又は以降の提供時であっても、スモールビジネス事業が促進できることが理解されよう（例えば、無線対応携帯電話、スマートホン、パーソナルコンピュータ（ＰＣ）、ハンドヘルドコンピュータ、ＰＤＡ、パーソナルメディア機器（ＰＭＤ）、ワイヤレスタブレット、「ファブレット」、等）。

【００６３】

プロセッササブシステム３５４は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、１つ以上の基板上に実装された複数の処理構成要素のうちの１つ以上を含み得る。プロセッササブシステム３５４はまた、内部キャッシュメモリも含み得る。プロセッササブシステム３５４は、メモリサブシステム３５６と通信し、後者は、例えば、ＳＲＡＭ、フラッシュ、及び／又はＳＤＲＡＭ構成要素を含み得るメモリを含む。メモリサブシステム３５６は、当該技術分野において周知のようにデータアクセスを円滑にするために、ＤＭＡタイプのハードウェアのうちの１つ以上を実装し得る。例示的な実施形態のメモリサブシステム３５６は、プロセッササブシステム３５４により実行可能なコンピュータ実行可能命令を含む。

【００６４】

例示的な一実施形態では、小売商装置３５０は、１つ以上のインタフェース、例えば、クライアント装置へ接続するよう適合された、小売商とクライアントとの間のインタフェース３５２、を含む。小売商とクライアントとの間のインタフェース３５２は、無線インタフェース又は代替的に物理的インタフェース（有線）とすることができる。無線インタフェースは、最大で数センチメートルの操作範囲を有する（例えば、ＲＦＩＤ、ＮＦＣ、等）「タッチ」タイプのインタフェースから、例えば、ＧＳＭ（登録商標）、ＣＤＭＡ、ＵＭＴＳ、ＬＴＥ／ＬＴＥ－Ａ、ＷｉＭＡＸ（登録商標）、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ワイヤレスＵＳＢ（登録商標）、等、又は先のいずれの組み合わせなどのより強力な無線インタフェースを含み得る。例えば、小売商装置３５０は、近距離ＮＦＣインタフェース、同様に長距離Ｗｉ－Ｆｉ（登録商標）インタフェース、更にはＷｉＭＡＸ（登録商標）インタフェース、衛星インタフェース、又はセルラーインタフェースを含み得る。物理的インタフェースの一般例は、例えば、ＵＳＢ（登録商標）、ＦｉｒｅＷｉｒｅ（登録商標）、Ｔｈｕｎｄｅｒｂｏｌｔ（登録商標）、等、を含む。いくつかの変形例では、小売商とクライアントとの間のインタフェース３５２は、（例えば、既存のレガシーカードとの適合性を維持するため、等）カードリーダー又はスマートカードレセプタクルとして実装され得る。

【００６５】

いくつかの実施形態では、小売商装置３５０はまた、例えば、キーパッド、タッチスクリーン（例えば、マルチタッチインタフェース）、ＬＣＤ、バックライト、スピーカ、及び／又はマイクロホンが挙げられるがこれらに限定されない任意の数の周知のＩ／Ｏを含むユーザインタフェースサブシステムなどの、他の構成要素も含み得る。特定のアプリケーションでは、ユーザインタフェースは不要とされてもよいことが認識される。例えば、簡易的なカードリーダー式の小売商装置は、ユーザインタフェースを欠いてもよい。

【００６６】

図示した実施形態では、小売商装置３５０は、１つ以上のＶＭＥとのトランザクションを、アセットブローカへ安全に報告するよう構成されたネットワークインタフェース３５８を含む。いくつかの変形例では、それぞれのトランザクションは、将来の参照／簿記のために、セキュアファイルシステム内に更に記憶されてもよい。ネットワークインタフェースの一般例は、Ｅｔｈｅｒｎｅｔ（登録商標）、デジタル加入者回線（ＤＳＬ）、ケーブル、ハイブリッドファイバーコアキシャル（Hybrid Fiber Coaxial）、無線ローカルエリアネットワーク（ＷＬＡＮ）、セルラーデータ接続、等、を含むがこれらに限定しない。

【００６７】
いくつかの実施形態では、小売商装置３５０は、高度暗号化標準（ＡＥＳ）／データ暗号化標準（ＤＥＳ）での暗号化、インターネットプロトコルセキュリティ（ＩＰＳｅｃ）、マルチメディアインターネットキーイング（ＭＩＫＥＹ）、セキュアソケットレイヤー（ＳＳＬ）／トランスポートレイヤーセキュリティ（ＴＬＳ）、などの、関連機器の暗号キー又は他の暗号機能を有し得るがこれらに限定しない。それらの機器キー（及び／又は他の機能）は、交換をセキュア化するために使用され得る。１つのそのような変形例では、暗号キーは、一組の非対称パブリックキー／プライベートキーである。更に他の変形例では、暗号キーは、一組の対称キーである。他の変形例では、小売商装置３５０は、デジタル証明書を検証及び／又は発行するための暗号キーを有し得る。そのうえ、ＮＦＣインタフェース（使用されている場合）は、機密のユーザ情報又は支払い情報を送信中に暗号化するためなどの、適用された暗号を有し得る。
【００６８】
例示的なクライアントと小売商との間のトランザクション中、小売商装置３５０は、関連する１つ以上のＶＭＥとトランザクションを行う。例えば、小売商装置３５０は、商品／サービスとの引き換えに、クライアント装置のバーチャルクレジットカードを受信（又は、要求）し得る。受信した情報は、例えば、取引される金額、妥当性チェック情報、暗号保護、証明情報（例えば、トランザクションの時刻／日付及び場所）、小売商ＩＤ、等、を更に組み込むことができる。他の実施形態では、小売商装置３５０は、例えば、トランザクションが正常に行われた場合に取引された金額、使用された支払いソース、小売商ＩＤ、等の報告を、クライアント装置へ報告を返し得る。
【００６９】
例示的な小売商装置とアセットブローカとの間のトランザクション中、小売商装置３５０は、トランザクションをアセットブローカへ報告する。これは、クライアント装置のＶＭＥ、貸方記入／借方記入対象の小売商アカウント、等、及び取引金額に関連付けられている情報を報告することを含み得る。これに応じて、アセットブローカは、クライアント装置の対応するアカウントから小売商装置のアカウントへ金額が正常に送金されたこと（又は、送金が失敗したこと）を認める。
【００７０】
ここで図４を参照すると、１つの例示的なアセットエージェント４００が提示されている。例示的なアセットエージェント４００は、クライアント装置インタフェース４０２と、プロセッササブシステム４０４と、非一時的コンピュータ可読媒体（メモリサブシステム）４０６と、ネットワークインタフェース４０８と、を含む。本明細書にて使用されるように、用語「アセットエージェント」は、ＶＭＥを分配するよう構成されているエンティティを含むがこれに限定しない。ＶＭＥの一般例は、機器製造業者、第三者の再販業者、等、を含むがこれらに限定しない。
【００７１】
プロセッササブシステム４０４は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、１つ以上の基板上に実装された複数の処理構成要素のうちの１つ以上を含み得る。プロセッササブシステム４０４はまた、内部キャッシュメモリも含み得る。プロセッササブシステム４０４は、メモリサブシステム４０６と通信し、後者は、例えば、ＳＲＡＭ、フラッシュ、及び／又はＳＤＲＡＭ構成要素を含み得るメモリを含む。メモリサブシステム４０６は、当該技術分野において周知のようにデータアクセスを円滑にするために、ＤＭＡタイプのハードウェアのうちの１つ以上を実装し得る。例示的な実施形態のメモリサブシステム４０６は、プロセッササブシステム４０４により実行可能なコンピュータ実行可能命令を含む。
【００７２】
例示的な一実施形態では、アセットエージェント４００は、１つ以上のインタフェース、例えば、クライアント装置へ接続するよう適合されたクライアント装置インタフェース４０２を含む。クライアント装置インタフェース４０２は、無線インタフェース又は代替

的に物理的インタフェース（有線）とされ得る。無線インタフェースは、例えば、ＧＳＭ（登録商標）、ＣＤＭＡ、ＵＭＴＳ、ＬＴＥ／ＬＴＥ－Ａ、ＷｉＭＡＸ（登録商標）、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ワイヤレスＵＳＢ（登録商標）、等、を含み得る。物理的インタフェースの一般例は、例えば、ＵＳＢ（登録商標）、ＦｉｒｅＷｉｒｅ（登録商標）、Ｔｈｕｎｄｅｒｂｏｌｔ（登録商標）、等、を含む。

【００７３】

図示した実施形態では、アセットエージェント４００は、１つ以上のＶＭＥの分配を、アセットブローカへ安全に報告するよう構成されたネットワークインタフェース４０８を含む。ネットワークインタフェースの一般例は、Ｅｔｈｅｒｎｅｔ（登録商標）、ＤＳＬ、ケーブル、ハイブリッドファイバーコアキシャル（Hybrid Fiber Coaxial）、ＷＬＡＮ、セルラーデータ接続、等、を含むがこれらに限定しない。

【００７４】

いくつかの実施形態では、アセットエージェント４００は、関連機器の暗号キーを有し得る。それらの機器キーは、交換をセキュア化するために使用され得る。１つのそのような変形例では、暗号キーは、一組の非対称パブリックキー／プライベートキーである。更に他の変形例では、暗号キーは、一組の対称キーである。他の変形例では、アセットエージェント４００は、デジタル証明書を検証及び／又は発行するための暗号キーを有し得る。

【００７５】

例示的な一実施形態では、アセットエージェント４００は、先天的にはセキュアエレメントに関連付けられていない（つまり、セキュアエレメントを有するクライアント装置に関連していない）ＶＭＥのデータベース、等、を有する。以降に詳述されるように、ＶＭＥは、Ｌ２セキュリティレイヤーにしたがって、アセットエージェントにより、セキュアエレメントに関連付けられ得る。Ｌ２セキュリティレイヤーは、ＶＭＥが配信された際に「複製」されることを防ぐ。

【００７６】

例えば、１つの実装では、クライアント装置は、数々の「チャレンジ」を要求し、予めロードされており、それぞれのチャレンジは、要求が有効であり、現在のものである（例えば、以前の要求により再生されていない）か、検証するために使用されている。より具体的には、それぞれのチャレンジは、クライアント装置のセキュアエレメントに対して唯一有効なチャレンジである、一回限りのチャレンジであり、つまり、チャレンジが一度使用されると、次のチャレンジのみがセキュアエレメントに対して有効である。ユーザが様々なアカウントにサインアップするにしたがい、アセットエージェント４００によりＶＭＥが提供される。クライアント装置がチャレンジの残りを使い果たすと、ユーザは、新たなチャレンジ一式を要求するようクライアント装置に指示し得る。いくつかの変形例では、ＶＭＥの転送は、例えば、サービスキオスクを介して、バーチャルプライベートネットワーク（ＶＰＮ）接続上のパーソナルコンピュータ（ＰＣ）を介して、等、セキュアリンクを介して行われている。

【００７７】

ここで図５を参照すると、アセットブローカ５００の１つの例示的なアカウントサーバ５０１が提示されている。例示的なアカウントサーバ５０１は、ネットワークインタフェース５０２と、プロセッササブシステム５０４と、非一時的コンピュータ可読媒体（メモリサブシステム）５０６と、アカウントデータベース５０８と、を含む。本明細書にて使用されるように、用語「アセットブローカ」は、ＶＭＥに関連付けられているアカウントへ適切に借方記入する、貸方記入する、及び／又はＶＭＥに関連付けられているアカウントを有効にするよう構成されているシステム及びネットワークを含むがこれらに限定しない。そのようなシステムは、１つ以上のアカウントサーバ、例えば、アカウントサーバ５０１を含み得る。したがって、「アセットブローカ」への参照はまた、アセットブローカの１つ以上のアカウントサーバ及びその逆も呼べることが理解される。

【００７８】

プロセッササブシステム５０４は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、１つ以上の基板上に実装された複数の処理構成要素のうちの１つ以上を含み得る。プロセッササブシステム５０４はまた、内部キャッシュメモリも含み得る。プロセッササブシステム５０４は、メモリサブシステム５０６と通信し、後者は、例えば、ＳＲＡＭ、フラッシュ、及び／又はＳＤＲＡＭ構成要素を含み得るメモリを含む。メモリサブシステム５０６は、当該技術分野において周知のようにデータアクセスを円滑にするために、ＤＭＡタイプのハードウェアのうちの１つ以上を実装し得る。例示的な実施形態のメモリサブシステム５０６は、プロセッササブシステム５０４により実行可能なコンピュータ実行可能命令を含む。

【００７９】

例示的な一実施形態では、アカウントサーバ５０１は、クライアント装置及び小売商装置へのネットワーク接続を確立するよう適合されたネットワークインタフェース５０２を含む。ネットワークインタフェースの一般例は、Ｅｔｈｅｒｎｅｔ（登録商標）、ＤＳＬ、ケーブル／ハイブリッドファイバーコアキシャル（Hybrid Fiber Coaxial）、ＷＬＡＮ、ワイヤレス大都市圏ネットワーク（ＷＭＡＮ）、セルラーデータ接続、ミリ波、等、を含むがこれらに限定しない。

【００８０】

いくつかの実施形態では、アカウントサーバ５０１は、関連する暗号キーを有し得る。それらのキーは、メッセージ交換をセキュア化するために使用され得る。１つのそのような変形例では、暗号キーは、一組の非対称パブリックキー／プライベートキーである。更に他の変形例では、暗号キーは、一組の対称キーである。他の変形例では、アカウントサーバ５０１は、例えば、デジタル証明書を検証及び／又は発行するための暗号キーを有し得る。

【００８１】

例示的な一実施形態では、アカウントサーバ５０１は、顧客アカウントに対してＶＭＥを認証及び認可するよう構成されている。ＶＭＥは、Ｌ３セキュリティレイヤーにしたがって、アカウントサーバ５０１により関連付けられている。Ｌ３セキュリティレイヤーは、顧客アカウントのＶＭＥの組み合わせが信頼でき、認可されている（つまり、不正でも悪用でもない）か、検証する。

【００８２】

ここで図６を参照すると、１つの例示的なアセットロッカー６００が提示されている。例示的なアセットロッカーは、ネットワークインタフェース６０２と、プロセッササブシステム６０４と、非一時的コンピュータ可読媒体（メモリサブシステム）６０６と、セキュアデータベース６０８と、を含み得る。本明細書にて使用されるように、用語「アセットロッカー」は、ＶＭＥを記憶し、暗号化し、及び生成するよう構成されている機器を含むがこれに限定しない。例えば、アセットロッカー６００は、信頼されたセキュリティモジュール（ＴＳＭ）とされ得る。

【００８３】

プロセッササブシステム６０４は、デジタル信号プロセッサ、マイクロプロセッサ、フィールドプログラマブルゲートアレイ、又は、１つ以上の基板上に実装された複数の処理構成要素のうちの１つ以上を含み得る。プロセッササブシステム６０４はまた、内部キャッシュメモリも含み得る。プロセッササブシステム６０４は、メモリサブシステム６０６と通信し、後者は、例えば、ＳＲＡＭ、フラッシュ、及び／又はＳＤＲＡＭ構成要素を含み得るメモリを含む。メモリサブシステム６０６は、当該技術分野において周知のようにデータアクセスを円滑にするために、ＤＭＡタイプのハードウェアのうちの１つ以上を実装し得る。メモリサブシステム６０６は、プロセッササブシステム６０４により実行可能であるコンピュータ実行可能命令を含むが、他の種類のコンピュータ化されたロジック（例えば、ハードウェア及びソフトウェア／ファームウェアの組み合わせ）が同様に使用されてもよい。

【００８４】

例示的な一実施形態では、アセットロッカー６００は、１つ以上のアカウントサーバへのネットワーク接続を確立するよう適合されたネットワークインタフェース６０２を含む。ネットワークインタフェースの一般例は、Ｅｔｈｅｒｎｅｔ（登録商標）、ＤＳＬ、ケーブル、ハイブリッドファイバーコアキシャル（Hybrid Fiber Coaxial）、ＷＬＡＮ、セルラーデータ接続、等、を含むがこれらに限定しない。

【００８５】

いくつかの実施形態では、アセットロッカー６００は、関連する暗号キーを有し得る。それらのキーは、メッセージ交換をセキュア化するために使用され得る。１つのそのような変形例では、暗号キーは、一組の非対称パブリックキー／プライベートキーである。更に他の変形例では、暗号キーは、一組の対称キーである。他の変形例では、アセットロッカー６００は、デジタル証明書を検証及び／又は発行するための暗号キーを有し得る。

【００８６】

アセットロッカー６００は、１つ以上のＶＭＥを提供及び／又は生成するよう更に構成されている。例示的な一実施形態では、ＶＭＥは、特定の規格（例えば、米国規格協会（ＡＮＳＩ）の規格Ｘ４．１３－１９８３（その全体において参照により本明細書に組み込まれている））にしたがって生成され、セキュアデータベース６０８内に記憶されている。代替的に、ＶＭＥは、例えば、専用フォーマット又は特定使用フォーマットにしたがって構築され得る。本開示の内容を所与として、非常に多くの可能なフォーマットが、関連の当業者に容易に理解されるであろう。

【００８７】

例示的な一実施形態では、アセットロッカー６００は、クライアント装置のセキュアエレメントに対してＶＭＥを暗号化するよう構成されている。アセットロッカー６００は、それぞれのアセットが、Ｌ１セキュリティレイヤーにしたがって、暗号化されている間にのみ転送されることを促進する。Ｌ１セキュリティレイヤーは、ＶＭＥが、アセットロッカー６００又はクライアント装置のセキュアエレメントのいずれかの内の、（暗号化されていない）プレーンテキスト内にのみ存在することを促進する。

【００８８】

ここで図７を参照すると、ＶＭＥをシステム内に分配するための一般化された方法７００の一実施形態が開示されている。ステップ７０２では、１つ以上のＶＭＥのコンテンツは、第１の標準的な、信頼された関係にしたがって保護されている。例示的な一実施形態では、第１の信頼された関係は、ＶＭＥ内に含まれる秘密及び／又は暗号マテリアル（例えば、セキュアキー、暗号マテリアル、ユーザ履歴、等）を保護するよう構成されている。例えば、第１の信頼された関係は、ＶＭＥを、固有の機器キー及び承認証明書にしたがって、暗号化する又は復号するよう構成されている、（ハードウェア又はソフトウェア内に実装された）セキュリティモジュールに基づいている。特に、セキュリティモジュールは、第１の信頼された関係にしたがっている、所望する行先装置（例えば、クライアント装置又は小売商装置）へ配信するために、ＶＭＥを暗号化するよう、又は第１の信頼された関係にしたがっているソース機器から受信したアクセス制御クライアントを復号するよう構成されている。例示的な一実施形態では、すべてのＶＭＥは、各機器との間に転送されている際には、暗号化されなければならない（つまり、ＶＭＥは、暗号化されていない形態では、いずれの他の機器へ転送され得ない）。第１の信頼された関係レベルにあるそれぞれの機器には、ＶＭＥを安全に転送するために使用され得る固有の機器キー及び承認証明書が所与される。

【００８９】

第１の標準的な、信頼された関係の様々な実装はまた、物理的及び／又は論理的に保護もされ得る。例えば、第１の標準的な、信頼された関係は、強制的に開放される／アクセスされると自身を破壊するよう構成されたハードウェアセキュリティモジュール（ＨＳＭ）内の保護を含み得る。より一般的には、第１の標準的な、信頼された関係の例示的な実施形態は、信頼された境界を最小限保護する。信頼された境界の一般例は、物理的境界（例えば、物理的隔離、等）、及び／又は論理的境界（例えば、暗号化された通信、等）の

双方を含む。

【００９０】

ステップ７０４では、ＶＭＥのコピー数は、第２の標準的な、信頼された関係にしたがって制御されている。例示的な一実施形態では、第２の信頼された関係は、ＶＭＥの予期しない複製及び／又は悪意のある複製を防ぐよう構成されている（保存エンフォースメント）。例えば、第２の標準的な、信頼された関係は、それ自体又は別の機器に対してＶＭＥを暗号化するよう構成されたセキュリティモジュールにより管理され得る。同様に、セキュリティモジュールは、（例えば、非対称暗号キーに基づいて）別の特定の機器によってのみ復号されてもよいＶＭＥを暗号化し得る。いくつかの実施形態では、セキュリティモジュールの暗号化スキームは、一組の非対称キーに基づくことができるか、又は、代替的に、セキュリティモジュールの暗号化スキームは、一組の対称キーを使用し得る。

【００９１】

先に説明するように、一組のパブリックキー／プライベートキーは、秘密のプライベートキー、及び公表可能なパブリックキーに基づいている。パブリックキー／プライベートキースキームは、暗号化及び復号に使用されるキーが異なり、したがって、エンクリプタ及びデクリプタは、同じキーを共有しないため、「非対称」とみなされる。対照的に、「対称」キースキームは、暗号化及び復号の両方に同じキー（又は、自明に変換したキー）を使用する。ＲＳＡアルゴリズムは、関連技術の範囲内で広く使用されている公開／秘密キーペア暗号法の種類の１つだが、本明細書に説明する実施形態は、ＲＳＡアルゴリズムに（又は、一組の非対称キー又は対称キーが重要であることに対して）全く制限されないものと認識されよう。

【００９２】

パブリック／プライベート暗号化方式は、メッセージを暗号化し、及び／又は署名を生成する目的で使用することができる。具体的には、メッセージを、秘密キーで暗号化し、パブリックキーで復号することができ、それによって、そのメッセージが送信中に変更されていないことを保証する。同様に、秘密キーで生成された署名は、パブリックキーで検証することができ、その署名を生成したエンティティが正当なものであることを保証する。どちらの用途においても、秘密キーは秘匿されており、自由に配布される。

【００９３】

ステップ７０６では、ＶＭＥは、第３の信頼された関係にしたがって、行先装置へ使用のために分配されている。第３の信頼された関係は、エンティティ認証及び認可を必要とする。より直接的には、第３の信頼された関係は、ＶＭＥが、それらの識別を認証し得るエンティティ、及びＶＭＥに対して認可されているエンティティのみに送信されることを保証する。

【００９４】

分配モデルのフレキシビリティにより、多くの異なるスキームが想定されており、及び、本開示の提供により当業者は認識するであろう。本発明の様々な態様にしたがう動作に適した幅広いスキームを例示する、種々のＶＭＥ分配スキームが以降に詳しく開示されている。

【００９５】

ここで図８を参照すると、プロビジョニングトランザクションの例示的な一実施形態を表す論理ラダーダイアグラムが示されている。プロビジョニングトランザクションは、クライアント装置、アセットブローカ、アセットエージェント、及びアセットロッカーにより実行され得る。クライアント装置は、セキュアエレメント（ＳＥ）と、アプリケーションプロセッサ（ＡＰ）（例えば、プロセッササブシステム３０４）と、を含む。ＳＥは、本開示にしたがうトランザクションを促進する、ソフトウェアレイヤーのいわゆる「スタック」を含むソフトウェアを記憶し得る。それぞれのソフトウェアレイヤーは、その対応するピアソフトウェアレイヤーとネゴシエートされる階層的な機能一式に対して責任を負う。いくつかの場合では、ＡＰは、危険（例えば、「脱獄」、等）にさらされ得ることが更に理解され、その結果、信頼関係は、ＳＥと、対応する論理的レイヤーエンティティと

の間にのみある、つまり、ＡＰは信頼されていない。

【００９６】

セキュリティソフトウェアプロトコルは、Ｌ１レイヤーと、Ｌ２レイヤーと、Ｌ３レイヤーと、を含む。Ｌ１セキュリティは、ＶＭＥデータの暗号化及び復号を行う。Ｌ１の動作は、セキュアな実行環境（例えば、ＳＥ又はＴＳＭ）に限定されている。Ｌ１内では、ＶＭＥデータは、論理的Ｌ１境界内のプレーンテキスト（つまり、暗号化されていない）にて記憶され得、論理的Ｌ１境界外では、ＶＭＥデータは安全に暗号化されている。Ｌ２セキュリティは、ＶＭＥデータが複製されることを防ぐ。Ｌ２境界は、ＶＭＥのコピーが１つのみ、Ｌ２境界外に存在することを保証する。Ｌ２境界内では複数のコピーが存在し得る。そのうえ、Ｌ２セキュリティは、暗号化されたＶＭＥデータ内にチャレンジを更に埋め込み得る。ＶＭＥをインストールする前に、クライアント装置は、ＶＭＥ内に埋め込まれたチャレンジを、クライアント装置上に記憶されたチャレンジと比較し得、ＶＭＥが古くなっていないか検証する（つまり、ＶＭＥは、現在の唯一のＶＭＥである）。Ｌ３セキュリティは、ＶＭＥを所有する顧客の信用、所有権、及び証明を確立する責任を負う。それぞれのＶＭＥについて、ＳＥは情報を記憶し得、ＶＭＥに関連付けられている所有権を示す。

【００９７】

例示的な一実施形態では、アセットロッカーは、ＶＭＥのデータ構成要素を生成し、バルクロットにてＶＭＥを記憶するよう構成されているＴＳＭである。アセットロッカーは、Ｌ１セキュリティにしたがってＶＭＥ動作を行い、暗号化されたＶＭＥのみが送信されることを保証する（つまり、ＶＭＥは、暗号化されていない形態では、アセットロッカー外に送信されない）。ＶＭＥを顧客に提供するため、アセットエージェントは、暗号化されたＶＭＥをアセットロッカーから受信し、ＶＭＥを記憶し、クライアント装置へ必要に応じて提供する。アセットエージェントは、Ｌ２セキュリティにしたがってＶＭＥ動作を行い、暗号化されたＶＭＥのコピーが１つのみクライアント装置へ提供されることを保証する。最後に、アセットブローカの例示的な実施形態は、Ｌ３セキュリティにしたがってＶＭＥ動作を行い、暗号化されたＶＭＥの送信が、認証され、認可されているＳＥを伴うクライアント装置へのみ生じることを促進する。ＶＭＥがクライアント装置へ配信されると、アセットブローカは、ＶＭＥを、クライアント装置と関連付けられているアカウントと、及び／又は、クライアント装置のユーザと関連付けられているアカウントと関連付け得る。

【００９８】

一実施形態では、クライアント装置内に記憶されたソフトウェアアプリケーションは、新たなバーチャルクレジットカード（ＶＣＣ）が、ユーザのアカウントへ使用のために提供されることを要求する。ソフトウェアアプリケーションは、ＡＰとともに実行されている。８０２では、ＡＰは、クライアント装置又はＳＥを一意的に識別するＳＥからの情報を要求する。例えば、情報は、装置識別子を含み得る。ＡＰは、装置識別子を、新たなＶＣＣに対する要求にて、８０４にてアセットブローカへ送信する。アセットブローカは要求を認証し、ＶＣＣをユーザのアカウントへ提供する。認証は、装置識別子に基づいている。実施形態の一態様では、アセットブローカは、ＳＥ／クライアント装置がユーザアカウントに関連付けられていることを判定することで、要求を認証する。

【００９９】

ＳＥは、装置識別子が、クライアント装置からアセットブローカへ安全に送信されるよう、装置識別子を電子署名とともに暗号化し得る。アセットブローカが新たなＶＣＣを認証／認可すると、アセットブローカは、ＳＥの電子署名をアセットエージェントへ転送する。アセットエージェントはＳＥの電子署名を検証し、したがって、ＶＣＣに対する行先のＳＥを８０６にて一意的に識別する。８０７では、いずれの更なるＶＣＣオプションが、クライアント装置へ提供されている。

【０１００】

余談として、いわゆる「チャレンジ」は、特定のＶＭＥをＳＥと関連付けるために使用

される重要なリソースである。具体的には、それぞれのＳＥは、特定数のチャレンジを保持し、Ｌ２セキュリティを維持する。チャレンジが有効であることを検証することで、ＳＥは、ＶＭＥが「古い」ＶＭＥ（つまり、無効、又は、さもなければ使用できない複製）でないか確かめ得る。ＳＥは、照合チャレンジデータを伴うＶＭＥを受信すると、チャレンジを削除する。以下の実装を考慮すると、ＳＥは、アセットエージェントと共有される数多くのチャレンジを作成する（又は、与えられる）。続いてその後は、アセットエージェントは、ＳＥに対して提供されているＶＭＥ内に現在のチャレンジを埋め込み得る。ＳＥがＶＭＥを受信すると、ＳＥは、受信したＶＭＥが適切なチャレンジを含み、古いものでないか検証し得る。

【０１０１】

先のスキームの１つの潜在的な欠点は、固定数のチャレンジは、サービスの妨害（ＤＯＳ）攻撃とともに容易に危険にさらされ得ることである。ＤＯＳ攻撃では、ＳＥは、すべてのそのチャレンジリソースを使い尽くすまでチャレンジを生成するよう、継続してトリガされる。それらの最後まで、ＳＥの例示的な実施形態は、チャレンジを消費するようＳＥをトリガするであろう要求を処理する前に、アセットブローカ／アセットエージェントとのセッションハンドシェイクを更に行う。加えて、リソースが使い果たされ、ＳＥが新たなチャレンジを作成できない、思いもよらない場合では、ＳＥは、別の一式のチャレンジを活用するために特別に割り当てられた、個別の一式の保存されたチャレンジを記憶し得る。いくつかの場合では、ＳＥはまた、相手先商標製造会社（ＯＥＭ）クレデンシャルを含み得、これは、ＯＥＭがチャレンジ動作を更に制御するために使用し得る。

【０１０２】

８０８では、ＡＰは、ＶＣＣと関連付けるためのチャレンジをＳＥが提供することを要求する。ＳＥにより提供されると、チャレンジがアセットブローカへ８１０にて送信され、続いて、アセットエージェントへ８１２にて転送される。アセットエージェントはチャレンジを検証し、続いて、パーソナライゼーション情報をアセットロッカーへ８１４にて提供する。アセットロッカーは、ＳＥに対する新たなＶＣＣをパーソナライズし、関連付けられたＶＣＣ識別子をアセットブローカへ８１６にて提供する。次に、アセットブローカは、ＶＣＣ識別子をＡＰへ８１７にて提供する。ＡＰがＶＣＣ識別子を受信すると、ＡＰは、ＶＣＣの配信を８１８にて要求し得る。その後は、アセットブローカは、クライアント装置のＳＥへ８２０にてＶＣＣを提供し得る。

【０１０３】

大規模分配ネットワークの動作中は、複数の現実的な問題が生じることを、関連ネットワークの当業者は認識するであろう。具体的には、大規模分配ネットワークは、大型のトラフィックバーストを扱うよう、スケーラブルでなければならない（クライアント装置のいわゆる「開設日」に生じ得るなどの）。ネットワークトラフィック全体を削減するための１つのスキームは、ＶＭＥの配信の延期を必要とする（可能な場合）。

【０１０４】

図９Ａ及び図９Ｂを参照すると、ＶＭＥをシステム内に分配するための一般化された方法９００の一実施形態が開示されている。予めパーソナライズされた動作中、ＳＥを有するいわゆる「予めパーソナライズされた」クライアント装置は、出荷前にＶＭＥが予め割り当てられている（つまり、ユーザが店頭にて機器を購入する際、オンラインで機器を発注する際、等）。９０２では、クライアント装置がユーザへ配送される前に、クライアント装置に関連付けられている箱上に配設されたステッカ、ラベル、又は他の証印がスキャンされる。例えば、箱は、クライアント装置が包まれている小売梱包とすることができる。このステッカは、クライアント装置を一意的に識別し、ＶＭＥに関連付けられ得る情報（例えば、装置識別子）を含む。ＶＭＥは、クライアント装置に対して、例えば、（ｉ）ＶＭＥを、（ステッカから判定された）ＳＥ（Ｌ１）に特有のキーとともに９０４にて暗号化し、（ｉｉ）割り当てられた初期チャレンジをＶＭＥ（Ｌ２）内に９０６にて埋め込み、及び、（ｉｉｉ）ＶＭＥを、（購入時に判定された）ユーザの認証／認可情報（Ｌ３）と９０８にて関連付けることにより、予め構成され得る。ＶＭＥは続いて、ＶＭＥを一

意的に識別する識別子、例えば、ＶＭＥ識別子に、９１０にて割り当てられる。その後は、クライアント装置は、ＶＭＥ識別子を使用して、９１２にてＶＭＥを要求し得る。９１４では、要求及びＶＭＥ識別子を受信すると、ＶＭＥは、クライアント装置へ、その完全に構成された状態にて配信され得る。

【０１０５】

先のスキームは、クライアント装置（及び／又は、クライアント装置に関連付けられている箱）から収集した情報、及び購入時のユーザからの情報に基づいて、ＶＭＥを効率的に予め構成する。ＶＭＥは、機器が移送（例えば、出荷時、自宅へ持ち帰る際、等）にある間に、ベストエフォートベースにしたがって構成されている（つまり、構成は、リソースが利用可能となると生じる）。その後は、ＶＭＥは、キャッシュされた位置から、リアルタイムでのトラフィックを必要とすることなく、クライアント装置内に途切れなくロードされ得る。システムの信頼性を最大にするため、予め構成されたＶＭＥはまた、複数の地理的位置にて冗長にキャッシュされ得る、つまり、異なる地理的位置に渡る複数のデータセンターが、ＶＭＥの複製を有する（ＶＭＥの第１のコピーが回収されると複製は古くなるよう、Ｌ２セキュリティが初期チャレンジスキームを提供する）。

【０１０６】

より直接的には、従来の製造スキームとは異なり、クライアント装置の例示的な実施形態は、ＶＭＥを伴って製造されておらず、予めプログラムされてもいない。ＶＭＥの構成及び配信は、クライアント装置が製造及び／又は展開されるまで「延期」され得る。例えば、複数のＶＭＥがクライアント装置によりサポートされ得ると、続いて、クライアント装置は、ユーザがアカウントを有効にする際に、選択されたＶＭＥとともに後に構成され得る、包括的なソフトウェアを有し得る。いくつかの実装では、包括的なソフトウェアは、包括的なＶＭＥ、又はデフォルトのＶＭＥを含み得る。この実装では、ユーザがクライアント装置を購入すると、ユーザは、デフォルトのＶＭＥとともに使用するためのクレジットカードアカウント（又は同様のもの）の提供を許可されてもよい（又は必要とされてもよい）。その後は、クライアント装置が有効にされると、アクティベーションシーケンスの一部として、デフォルトのＶＭＥが自動でロードされる。

【０１０７】

図１０Ａ及び図１０Ｂを参照すると、ＶＭＥをシステム内に分配するための一般化された方法１０００の別の実施形態が開示されている。この変形例では、ＳＥを有するクライアント装置は、出荷時（つまり、ユーザが店頭にて機器を購入する際、オンラインで機器を発注する際、等）に、ＶＭＥのプールから１００２にてＶＭＥが割り当てられており、つまり、特定のＶＭＥはクライアント装置に関連付けられていない。この時、ユーザは、認証／認可情報を１００４にて提供し得る。クライアント装置がユーザへ１００６にて配信されると、クライアント装置を一意的に識別する情報が、例えば、小売商の販売時点情報管理システム、自宅にいるユーザ、等、により入力される。情報は、クライアント装置に関連付けられている箱上に配設されたステッカ、ラベル、又は他の証印から収集され得る。情報はまた、ＶＭＥがクライアント装置に対して割り当てられるべきであるが、まだ割り当てられていないことも示し得る。情報を１００８にて受信したことに応じて、アセットブローカ、アセットエージェント、及びアセットブローカは協調し、（ステッカから判定される）ＳＥ（Ｌ１）に特有のキーとともにＶＭＥを１０１０にて暗号化し、チャレンジデータをＶＭＥ（Ｌ２）内に１０１２にて埋め込み、及び、ＶＭＥを（購入時に判定される）ユーザの認証／認可情報（Ｌ３）と１０１４にて関連付けることにより、利用可能なＶＭＥを割り当てる。１０１６では、新規に作成され、暗号化されたＶＭＥが、クライアント装置へ、その完全に構成された状態にて配信される。

【０１０８】

先のスキームは、必要に応じて効率的にＶＭＥを構成する。そのような実装は、アセットブローカ及び／又はアセットエージェントが、ＶＭＥのプールを知的に管理可能にする。ＶＭＥのプール内のそれぞれのＶＭＥは特定のクライアント装置（つまり、特定の用途専用）に割り当てられておらず、必要に応じて割り当てられているため、アセットブロー

カ及び／又はアセットエージェントは、まだ有効でない在庫を追跡する必要はない（例えば、機器によっては購入されて、有効にされる前に返却されてもよく、これは不要なＶＭＥの「撹拌」を削減する）。これは、ＶＭＥが有限リソースである場合に有効となり得る。口座番号は有限リソース（及び、したがって、その不足において貴重）であることが、当業者には容易に理解されるであろう。例えば、ＡＮＳＩ規格Ｘ４．１３－１９８３（その全体において参照により本明細書に以前に組み込まれている）は、多くの国内クレジットカードシステムにより使用されるアカウントナンバリングシステムである。ＡＮＳＩ規格Ｘ４．１３－１９８３の１６桁のクレジットカード番号によると、それらのサブセットのみが実際の口座番号を表し（例えば、最大で１０００万の固有の口座番号を表すためには８桁のみ使用され得）、他の桁は他の用途に与えられている（例えば、カード発行者の識別、「チェック」値の提供、カード番号の識別、等）。

【０１０９】

ここで図１１を参照すると、ＶＭＥをシステム内に分配するための一般化された方法１１００の別の実施形態が開示されている。この実施形態では、ＶＭＥの構成は、最初のトランザクションが発生するまで完全に延期され得る。この実施形態は、システムとクライアント装置との間に複数のトランザクション（例えば、定期トランザクション）が発生する場合に有用とされ得る。例えば、ユーザは、例えば、複数の映画パス、月間バス定期券、等を購入するよう選択してもよい。１１０２では、ユーザは、支払い情報、例えば、クレジットカード情報をシステムへ提供する。１１０４では、クライアント装置を識別する情報、例えば、装置識別子がシステムへ提供される。装置識別子は、いずれの前述の実施形態にしたがって提供され得る（例えば、「予めのパーソナライゼーション」プロセス、ユーザによる入力、ＡＰによる提供、等）。最初のトランザクションは、１１０６にて正常に行われ得る。その間、ＶＭＥが装置識別子を使用してクライアント装置に対して構成され、支払い情報及び／又はチャレンジデータが提供され、ＶＭＥが１１０８にて構成されると、以降の使用のために１１１０にてクライアント装置へ配信される。いくつかの場合では、配信は、準備完了時のプッシュ通知、自動ダウンロード、又は手動ダウンロードに基づくことができる。

【０１１０】

ここで図１２を参照すると、ＶＭＥをシステム内に分配するための一般化された方法１２００の別の実施形態が開示されている。方法１２００は、アセットブローカとともに、ＳＥを有するクライアント装置、アセットエージェント、及びアセットロッカーと通信して実行され得る。１２０２では、アセットブローカは、ＶＭＥをユーザのアカウントへ使用のために提供する要求をクライアント装置から受信する。アカウントは、クライアント装置のユーザと関連付けられ得る（つまり、アカウントはユーザにより所有されている）。要求は、クライアント装置、例えば、装置識別子に一意的に関連付けられている識別情報を含み得る。実施形態の一態様では、要求はまた、アカウントを識別する情報を送信することを含み得る。次に、アセットブローカは、１２０４にて要求を認証する。アセットブローカは、装置識別子により識別されたクライアント装置がアカウントに関連付けられていることを検証することで、要求を認証し得る。アセットブローカは続いて、アセットエージェント及びアセットロッカーと協調し、本明細書に説明する実施形態にしたがって、アカウントに対してＶＭＥを提供し、クライアント装置に対してＶＭＥを構成する。１２０６では、アセットブローカは、アセットロッカーからＶＭＥ識別子を受信する。ＶＭＥ識別子は、クライアント装置に対して構成されているＶＭＥを識別する。アセットブローカは続いて、ＶＭＥ識別子をクライアント装置へ１２０８にて送信し得る。クライアント装置は、ＶＭＥ識別子を記憶し得、その後、構成されたＶＭＥをアセットブローカから要求する際にＶＭＥ識別子を使用する。ＶＭＥに対する要求をクライアント装置から１２１０にて受信すると、アセットブローカは、構成されたＶＭＥをクライアント装置へ１２１２にて送信し得る。

【０１１１】

ここで図１３Ａ～図１３Ｃを参照すると、ＶＭＥをシステム内に分配するための一般化

された方法１３００の別の実施形態が開示されている。方法１３００は、アセットエージェント、アセットブローカ、及び／又はアセットロッカーを含み得るプロビジョニングシステムと通信するクライアント装置により実行され得る。クライアント装置は、ＳＥ及びＡＰを含み得る。明確化及び簡略化を目的として、クライアント装置とアセットブローカとの間で実行される方法１３００が以下に説明されることに注意すべきである。方法１３００の各ステップはまた、クライアント装置と、プロビジョニングシステムの１つ以上のエンティティ（例えば、アセットエージェント、アセットブローカ）との間で実行され得ることが理解されるべきである。

【０１１２】

１３０２では、クライアント装置は、使用のためにＶＭＥのユーザのアカウントへの提供を希望することを示す入力を受信する。入力は、クライアント装置でのＩ／Ｏインタフェース（例えば、ボタン、キーパッド、タッチスクリーン、音声コマンド、等）を使用してユーザにより入力され得る。１３０４では、クライアント装置は、識別情報をＳＥから要求し得る。識別情報は、クライアント装置、例えば、装置識別子に一意的に関連付けられている。識別情報は、ＳＥから取得され得る。代替の実施形態では、識別情報は、クライアント装置外部のソースから取得され得る。例えば、ユーザは、クライアント装置の箱上のステッカから識別情報を取得し得、クライアント装置のＩ／Ｏ機器を使用して識別情報を入力し得る。

【０１１３】

ＳＥから装置識別子を受信すると、クライアント装置は、ＶＭＥを提供する要求をアセットブローカへ１３０６にて送信し得る。要求に加えて、クライアント装置はまた、装置識別子もアセットブローカへ１３０８にて送信する。１３１０では、クライアント装置は、チャレンジに対する要求をアセットブローカから受信する。チャレンジは、本明細書に説明するように、Ｌ２セキュリティにしたがって、ＶＭＥの検証に使用され得る。アセットブローカから要求を受信したことに応じて、ＡＰは、チャレンジをＳＥから１３１２にて要求し得る。チャレンジをＳＥから受信すると、クライアント装置は、チャレンジをアセットブローカへ１３１４にて送信する。プロビジョニングシステムは、要求を認証し、クライアント装置に対してＶＭＥを構成し得る。次に、クライアント装置は、ＶＭＥ識別子をアセットブローカから１３１６にて受信し得る。ＶＭＥ識別子は、クライアント装置に対して構成されているＶＭＥを一意的に識別し得る。その後、クライアント装置は、構成されたＶＭＥに対する要求をアセットブローカへ１３１８にて送信し得る。要求に加えて、クライアント装置は、ＶＭＥ識別子を１３２０にて送信する。要求及びＶＭＥ識別子を受信したことに応じて、アセットブローカは、構成されたＶＭＥをクライアント装置へ１３２２にて配信し得る。ＳＥは、受信したＶＭＥが、有効なチャレンジデータとともに埋め込まれていることを検証することで、受信したＶＭＥが有効である（つまり、受信したＶＭＥが古くない）か、１３２４にて検証し得る。

【０１１４】

特定の機構が、特定の方法の具体的なステップのシーケンスの観点から説明されているが、これらの説明は、本明細書で開示される、より広範な方法の例示にすぎないものであり、具体的な適用によって、必要に応じて修正することができる点が、認識されるであろう。あるステップは、ある状況下では、不必要又は任意選択とすることができる。更には、特定のステップ又は機能性を、開示される実施形態に追加してもよく、あるいは２つ以上のステップの実行の順序を、置き換えることもできる。すべてのこのような変更形態は、本開示の範囲内に包含され、本明細書において特許請求されるとみなされる。

【０１１５】

更に、説明される実施形態の様々な態様、実施形態、実装、又は特徴は、個別に若しくは任意の組み合わせで使用できる。記載される実施形態の様々な態様は、ソフトウェア、ハードウェア、又はハードウェアとソフトウェアとの組み合わせによって実施できる。更に、説明した実施形態は、コンピュータ可読媒体上のコンピュータ可読コードとして実施できる。コンピュータ可読媒体は、後にコンピュータシステムによって読み出すことが可

能なデータを記憶することができる、任意のデータ記憶装置である。コンピュータ可読媒体の例としては、読み出し専用メモリ、ランダムアクセスメモリ、ＣＤ－ＲＯＭ、ＨＤＤ、ＤＶＤ、磁気テープ、及び光学的データ記憶装置が挙げられる。コンピュータ可読媒体はまた、ネットワーク結合されたコンピュータシステム上に分散させることもでき、コンピュータ可読コードが分散方式で記憶及び実行される。

【０１１６】

上述の説明は、説明の目的上、説明される実施形態の完全な理解を提供するために、具体的な専門用語を使用した。しかしながら、それらの具体的詳細は、記載される実施形態を実践するために必須のものではないことが、当業者には明らかとなるであろう。それゆえ、上述の具体的な実施形態の説明は、例示及び説明の目的のために提示される。それらの説明は、網羅的であることも、又は説明される実施形態を開示される厳密な形態に限定することも意図してはいない。上記の教示を考慮して、多くの修正形態及び変更形態が可能であることが、当業者には明らかとなるであろう。

【図１】

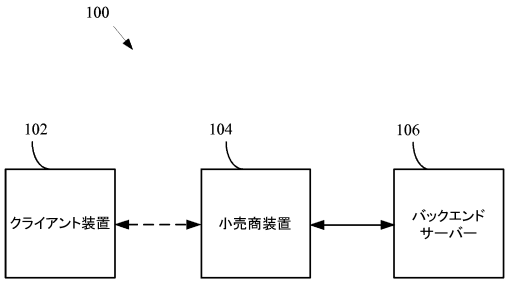

FIG. 1

【図２】

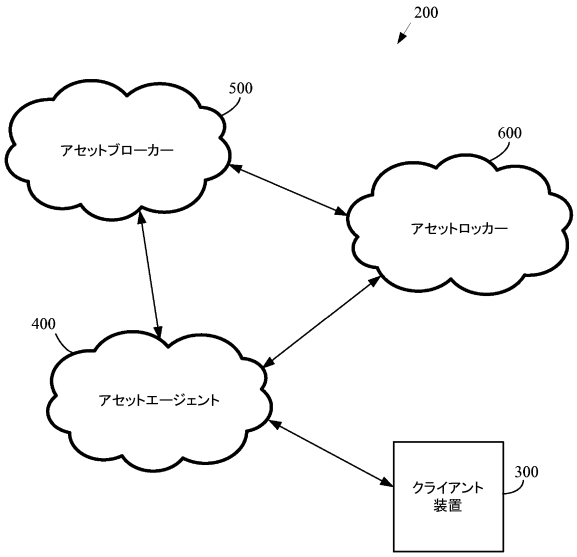

FIG. 2

【図３Ａ】

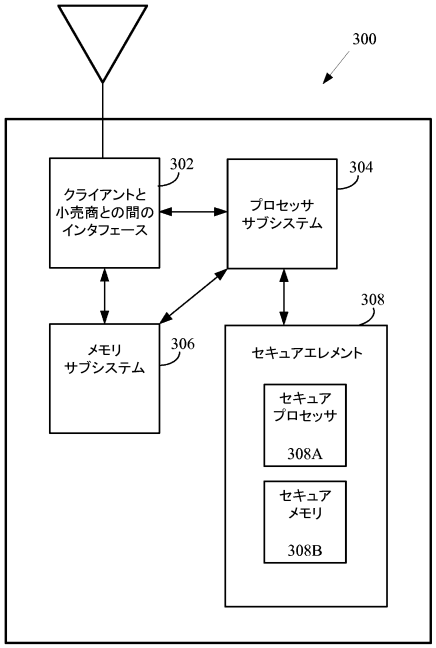

FIG. 3A

【図３Ｂ】

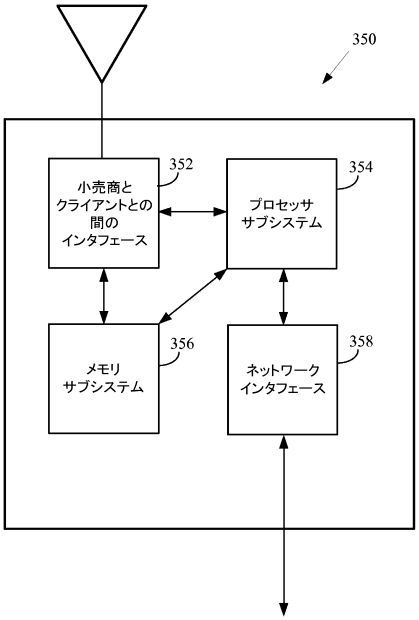

FIG. 3B

【図４】

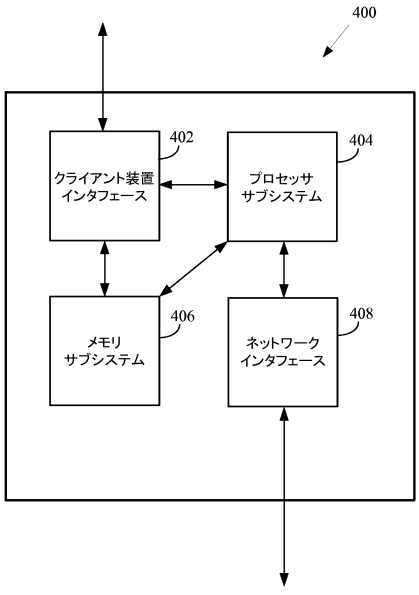

FIG. 4

【図５】

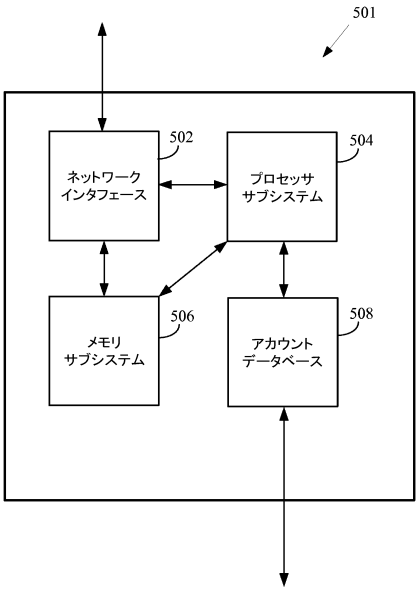

FIG. 5

【図６】

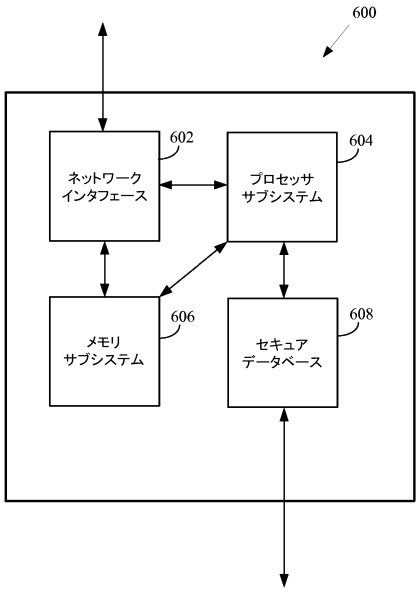

FIG. 6

【図７】

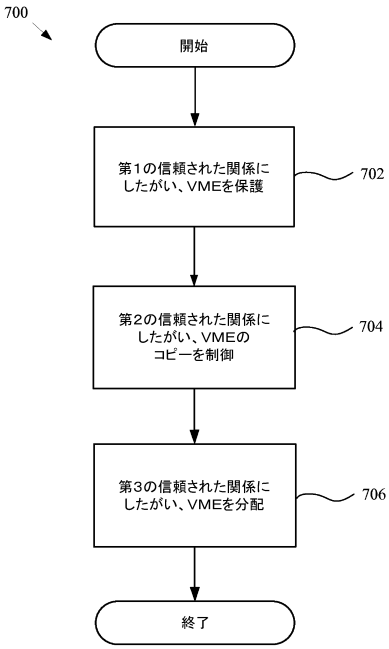

FIG. 7

【図８】

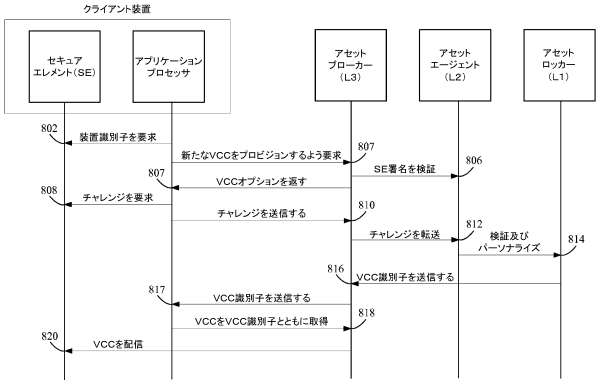

FIG. 8

【図９Ａ】

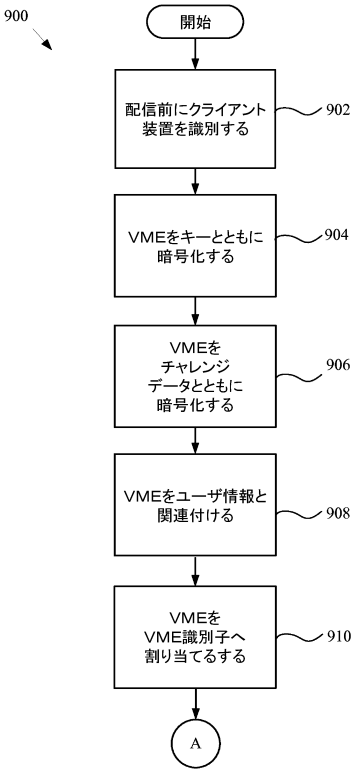

FIG. 9A

【図９Ｂ】

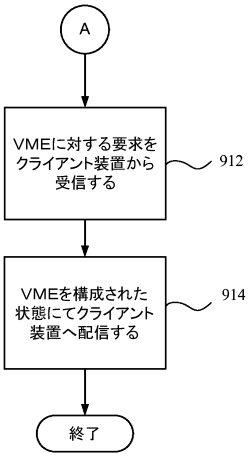

FIG. 9B

【図１０Ａ】

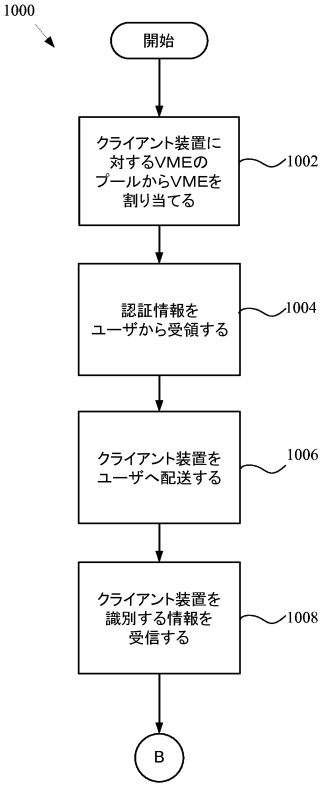

FIG. 10A

【図１０Ｂ】

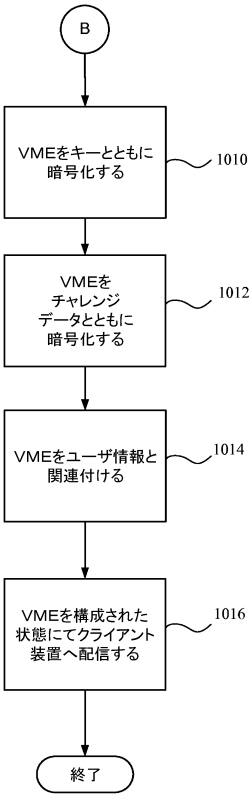

FIG. 10B

【図１１】

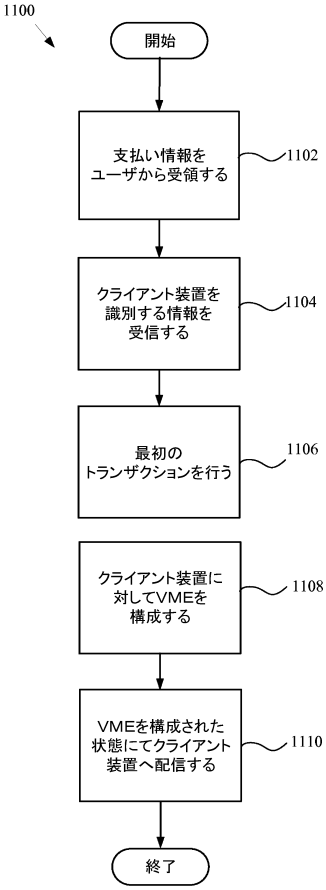

FIG. 11

【図１２】

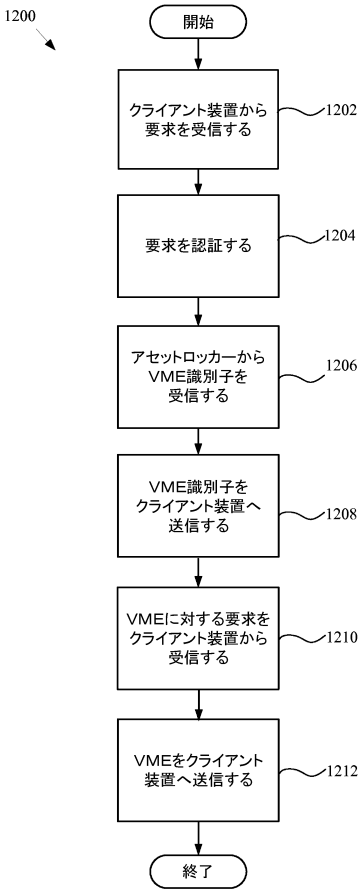

FIG. 12

【図１３Ａ】

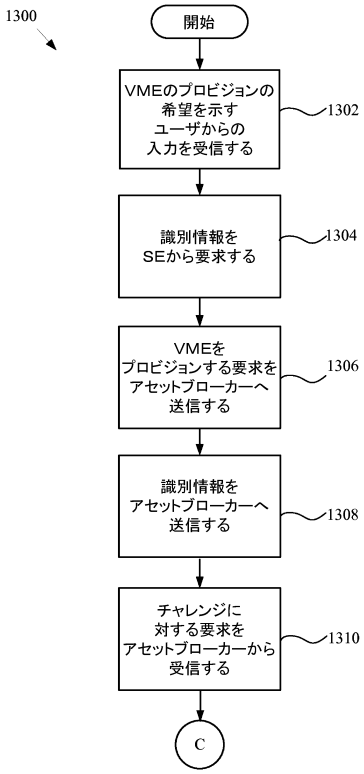

FIG. 13A

【図１３Ｂ】

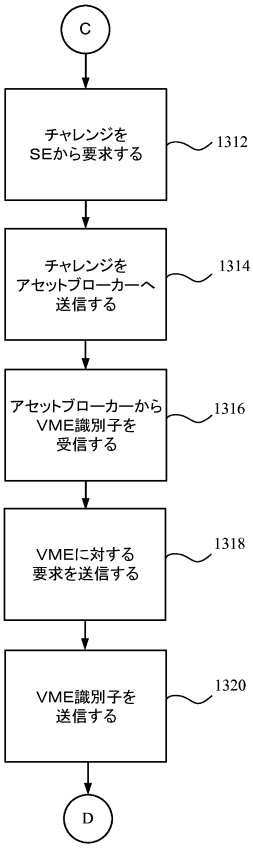

FIG. 13B

【図１３Ｃ】

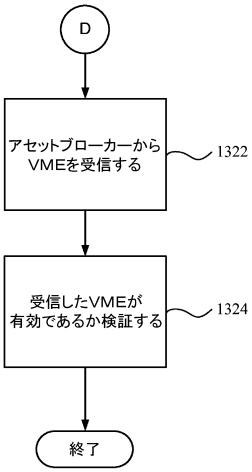

FIG. 13C

フロントページの続き

(74)代理人 100134175
弁理士 永川 行光
(72)発明者 ハガティ, デイビット ティー.
アメリカ合衆国 カリフォルニア州 ９５０１４, クパチーノ, インフィニット ループ 1
(72)発明者 カーン, アーメル エー.
アメリカ合衆国 カリフォルニア州 ９５０１４, クパチーノ, インフィニット ループ 1
(72)発明者 シャープ, クリストファー
アメリカ合衆国 カリフォルニア州 ９５０１４, クパチーノ, インフィニット ループ 1
(72)発明者 ホーク, ジェラルド ファン
アメリカ合衆国 カリフォルニア州 ９５０１４, クパチーノ, インフィニット ループ 1
(72)発明者 リンデ, ヨアキム
アメリカ合衆国 カリフォルニア州 ９５０１４, クパチーノ, インフィニット ループ 1
(72)発明者 マクラウリン, ケヴィン ピー.
アメリカ合衆国 カリフォルニア州 ９５０１４, クパチーノ, インフィニット ループ 1
(72)発明者 ジアト, メヘディ
アメリカ合衆国 カリフォルニア州 ９５０１４, クパチーノ, インフィニット ループ 1
(72)発明者 ヴァイド, ユーセフ エイチ.
アメリカ合衆国 カリフォルニア州 ９５０１４, クパチーノ, インフィニット ループ 1

審査官 山下 剛史

(56)参考文献 国際公開第２０１１／１５９５４９（WO, Ａ1）
特表２０１１－５０９５７５（ＪＰ, Ａ）
特表２０１２－５０５４７５（ＪＰ, Ａ）
特開２０１０－４５５４２（ＪＰ, Ａ）
米国特許第８１９６１３１（ＵＳ, Ｂ1）
米国特許出願公開第２００８／００８２４４９（ＵＳ, Ａ1）
中道理, ＮＦＣは“おサイフ”を超えて 第２部<海外動向>セキュア・エレメントの争奪へＡｐｐｌｅ, Ｇｏｏｇｌｅも参戦, 日経エレクトロニクス, 日経ＢＰ社, ２０１１年 3月２１日, 第1052号, p.66-71

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｑ １０／００－９９／００
Ｇ０６Ｆ ２１／００