(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7181914号
(P7181914)

(45)発行日　令和4年12月1日(2022.12.1)

(24)登録日　令和4年11月22日(2022.11.22)

(51)国際特許分類
*Ｇ０６Ｑ　20/38　(2012.01)*

ＦＩ
Ｇ０６Ｑ　20/38　３１０

請求項の数　18　外国語出願　（全91頁）

(21)出願番号　特願2020-170396(P2020-170396)
(22)出願日　令和2年10月8日(2020.10.8)
(62)分割の表示　特願2018-558106(P2018-558106)の分割
原出願日　平成29年1月25日(2017.1.25)
(65)公開番号　特開2021-7049(P2021-7049A)
(43)公開日　令和3年1月21日(2021.1.21)
審査請求日　令和2年11月9日(2020.11.9)
(31)優先権主張番号　62/286,938
(32)優先日　平成28年1月25日(2016.1.25)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/384,059
(32)優先日　平成28年9月6日(2016.9.6)
(33)優先権主張国・地域又は機関
最終頁に続く

(73)特許権者　503260918
アップル インコーポレイテッド
Ａｐｐｌｅ Ｉｎｃ．
アメリカ合衆国 ９５０１４ カリフォルニア州 クパチーノ アップル パーク ウェイ ワン
One Apple Park Way, Cupertino, California 95014, U. S. A.
(74)代理人　100094569
弁理士　田中 伸一郎
(74)代理人　100067013
弁理士　大塚 文昭
(74)代理人　100086771
弁理士　西島 孝喜
最終頁に続く

(54)【発明の名称】　非ネーティブクレデンシャルを有する電子デバイスを使用したトランザクションの実行

(57)【特許請求の範囲】
【請求項１】
第１のユーザデバイスの少なくとも１つのプロセッサが、小売商サブシステムから、前記第１のユーザデバイスと前記小売商サブシステムとの間の金融トランザクションを示す潜在的トランザクションデータを受信することと、
前記受信に応答して、前記第１のユーザデバイスの少なくとも１つのプロセッサがホスト利用可能性要求を第２のユーザデバイスへ送信することと、
前記第１のユーザデバイスの少なくとも１つのプロセッサが、前記第２のユーザデバイスから、前記第２のユーザデバイス上で利用可能な少なくとも１つのホストクレデンシャルアプリケーションを識別するホストクレデンシャルアプリケーション識別情報を含むホスト利用可能性応答を受信することと、
前記第１のユーザデバイスの少なくとも１つのプロセッサが、前記第２のユーザデバイス上で利用可能な少なくとも１つのホストクレデンシャルアプリケーションの識別を、選択のために表示することと、
前記表示に応答して、前記第１のユーザデバイスの少なくとも１つのプロセッサが、前記少なくとも１つのホストクレデンシャルアプリケーションからの１つの選択を受信することと、
前記第１のユーザデバイスの少なくとも１つのプロセッサが、受信した前記潜在的トランザクションデータに基づき、前記小売商サブシステム及び前記少なくとも１つのホストクレデンシャルアプリケーションから選択された１つを識別するホストクレデンシャルア

プリケーション識別子に対応する小売商識別子を含む決済要求データを前記第２のユーザデバイスへ送信することと、
前記第１のユーザデバイスの少なくとも１つのプロセッサが、送信された前記決済要求データに基づき、前記第２のユーザデバイスにより生成された暗号化決済クレデンシャルデータであって、前記小売商サブシステムの公開鍵及び前記少なくとも１つのホストクレデンシャルアプリケーションから選択された１つに対応する暗号化決済クレデンシャルデータを用いて暗号化した当該暗号化決済クレデンシャルデータを受信することと、
前記第１のユーザデバイスの少なくとも１つのプロセッサが、前記第１のユーザデバイスと前記小売商サブシステムとの間の前記金融トランザクションの少なくとも一部に資金供給するため、前記第２のユーザデバイスから受信した前記暗号化決済クレデンシャルデータを前記小売商サブシステムへ送信することと、
を含む方法。
【請求項２】
前記決済要求データを送信する前に、受信した前記潜在的トランザクションデータに基づき、固有の決済要求識別子を前記第１のユーザデバイスの少なくとも１つのプロセッサにより生成することを更に含む請求項１に記載の方法。
【請求項３】
前記決済要求データは、前記固有の決済要求識別子を含む、請求項２に記載の方法。
【請求項４】
前記暗号化決済クレデンシャルデータは、前記固有の決済要求識別子を更に含む、請求項３に記載の方法。
【請求項５】
前記第１のユーザデバイスの少なくとも１つのプロセッサが、前記金融トランザクションに資金供給するために前記小売商サブシステムにアクセス可能な少なくとも１つの決済タイプを識別することを更に含む、請求項１に記載の方法。
【請求項６】
前記ホスト利用可能性要求が、識別された前記少なくとも１つの決済タイプを識別する、請求項５に記載の方法。
【請求項７】
前記小売商サブシステムの公開鍵に対応する秘密鍵は、前記第１のユーザデバイスにアクセス可能ではない、請求項１に記載の方法。
【請求項８】
前記小売商サブシステムの公開鍵に対応する秘密鍵は、前記第２のユーザデバイスにアクセス可能ではない、請求項１に記載の方法。
【請求項９】
前記第１のユーザデバイス及び前記第２のユーザデバイスは、同一のユーザアカウントに関連する、請求項１に記載の方法。
【請求項１０】
メモリと、少なくとも１つのプロセッサとを含む第１のユーザデバイスであって、
前記プロセッサが、
小売商サブシステムから、前記第１のユーザデバイスと前記小売商サブシステムとの間の金融トランザクションを示す潜在的トランザクションデータを受信し、
前記受信に応答して、ホスト利用可能性要求を第２のユーザデバイスへ送信し、
前記第２のユーザデバイスから、前記第２のユーザデバイス上で利用可能な少なくとも１つのホストクレデンシャルアプリケーションを識別するホストクレデンシャルアプリケーション識別情報を含むホスト利用可能性応答を受信し、
前記第２のユーザデバイス上で利用可能な少なくとも１つのホストクレデンシャルアプリケーションの識別を、選択のために表示し、
前記表示に応答して、前記少なくとも１つのホストクレデンシャルアプリケーションからの１つの選択を受信し、

受信した前記潜在的トランザクションデータに基づき、前記小売商サブシステム及び前記少なくとも１つのホストクレデンシャルアプリケーションから選択された１つを識別するホストクレデンシャルアプリケーション識別子に対応する小売商識別子を含む決済要求データを前記第２のユーザデバイスへ送信し、
送信された前記決済要求データに基づき、前記第２のユーザデバイスにより生成された暗号化決済クレデンシャルデータであって、前記小売商サブシステムの公開鍵及び前記少なくとも１つのホストクレデンシャルアプリケーションから選択された１つに対応する暗号化決済クレデンシャルデータを用いて暗号化した当該暗号化決済クレデンシャルデータを受信し、
前記第１のユーザデバイスと前記小売商サブシステムとの間の前記金融トランザクションの少なくとも一部に資金供給するため、前記第２のユーザデバイスから受信した前記暗号化決済クレデンシャルデータを前記小売商サブシステムへ送信する、
ように構成されている、第１のユーザデバイス。
【請求項１１】
前記少なくとも１つのプロセッサは、更に、
前記決済要求データを送信する前に、受信した前記潜在的トランザクションデータに基づき、固有の決済要求識別子を生成することを更に含む請求項１０に記載の第１のユーザデバイス。
【請求項１２】
前記決済要求データは、前記固有の決済要求識別子を含む、請求項１１に記載の第１のユーザデバイス。
【請求項１３】
前記暗号化決済クレデンシャルデータは、前記固有の決済要求識別子を更に含む、請求項１２に記載の第１のユーザデバイス。
【請求項１４】
前記少なくとも１つのプロセッサは、更に、前記金融トランザクションに資金供給するために前記小売商サブシステムにアクセス可能な少なくとも１つの決済タイプから識別する、請求項１０に記載の第１のユーザデバイス。
【請求項１５】
前記ホスト利用可能性要求が、識別された前記少なくとも１つの決済タイプを識別する、請求項１４に記載の第１のユーザデバイス。
【請求項１６】
前記小売商サブシステムの公開鍵に対応する秘密鍵は、前記第１のユーザデバイスにアクセス可能ではない、請求項１０に記載の第１のユーザデバイス。
【請求項１７】
前記小売商サブシステムの公開鍵に対応する秘密鍵は、前記第２のユーザデバイスにアクセス可能ではない、請求項１０に記載の第１のユーザデバイス。
【請求項１８】
前記第１のユーザデバイス及び前記第２のユーザデバイスは、同一のユーザアカウントに関連する、請求項１０に記載の第１のユーザデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、先に出願された、２０１６年１月２５日に出願された米国仮特許出願公開第６２／２８６，９３８号、２０１６年６月１２日に出願された米国仮特許出願公開第６２／３４８，９５８号、及び２０１６年９月６日に出願された米国仮特許出願公開第６２／３８４，０５９号の利益を主張するものであり、これらのそれぞれは、本明細書により、参照によりその全体が本明細書に組み込まれる。
本開示は、非ネーティブクレデンシャルを有する電子デバイスを用いてトランザクショ

ンを実行すること、より具体的には、ホスト電子デバイスからのクレデンシャルを有するクライアント電子デバイスを用いてトランザクションを実行することに関する。

【背景技術】

【０００２】

ポータブル電子デバイス（例えば、携帯電話）には、別のエンティティ（例えば、小売商）との非接触近接ベース通信を有効化する近距離通信（「ＮＦＣ」）コンポーネントを設けることができる。多くの場合、これらの通信は、非接触近接ベース通信における他のエンティティと、クレジットカードクレデンシャルなどのネーティブ決済クレデンシャルを生成、アクセス、及び／若しくは共有することを電子デバイスに必要とする金融トランザクション又は他のセキュアデータトランザクションに関連付けられる。しかし、他のタイプの通信（例えば、オンライン金融トランザクション）における電子デバイスによるネーティブ決済クレデンシャルの効率的な使用は非効率的であることが多かった。

【発明の概要】

【０００３】

非ネーティブクレデンシャルを有する電子デバイスを用いてトランザクションを実行するためのシステム、方法、及びコンピュータ可読媒体が記載される。

【０００４】

一実施例として、商業エンティティサブシステム、クライアント電子デバイス、並びにセキュアエレメント及び、セキュアエレメント上にプロビジョニングされたホストクレデンシャルアプリケーションを含むホスト電子デバイスを使用して、小売商サブシステムと金融トランザクションを実行する方法は、ホスト電子デバイスにおいて、クライアント電子デバイスから、決済要求データであって、小売商サブシステムを識別する小売商サブシステム識別子情報と、ホストクレデンシャルアプリケーションを識別するホストクレデンシャルアプリケーション識別子情報と、を含む、決済要求データを受信することと、受信された決済要求データによって識別されるホストクレデンシャルアプリケーションを使用してセキュアエレメント上にホスト決済クレデンシャルデータを含む第１のデータを生成することと、セキュアエレメント上に、第１のデータ及び受信された決済要求データの小売商サブシステム識別子情報を第１の鍵で暗号化することによって第２のデータを生成することと、商業エンティティサブシステムに、第２のデータを送信することと、小売商サブシステム識別子情報に関連付けられた第２の鍵で暗号化された第１のデータを含む第３のデータを受信することと、受信された第３のデータを送信して金融トランザクションの少なくとも一部に資金を供給することと、を含むことができる。

【０００５】

別の実施例として、クライアント電子デバイス及びホスト電子デバイスを使用して小売商サブシステムと金融トランザクションを実行する方法は、クライアント電子デバイスにおいて、小売商サブシステムから、金融トランザクションを示す潜在的トランザクションデータを受信することと、ホスト電子デバイスに、受信された潜在的トランザクションデータに基づいて決済要求データを送信することと、送信された決済要求データに基づいてホスト電子デバイスによって生成されたホスト決済クレデンシャルデータを含むホストトランザクションデータを受信することと、小売商サブシステムに、受信されたホストトランザクションデータのホスト決済クレデンシャルデータを送信して、金融トランザクションの少なくとも一部に資金を供給することと、を含むことができる。

【０００６】

別の実施例として、商業エンティティサブシステム、クライアント電子デバイス、並びにセキュアエレメント及び、セキュアエレメント上にプロビジョニングされたホストクレデンシャルアプリケーションを含むホスト電子デバイスを使用して、小売商サブシステムと金融トランザクションを実行する方法は、商業エンティティサブシステムにおいて、クライアント電子デバイスから、金融トランザクションに資金を供給するために小売商サブシステムに受け入れ可能な少なくとも１つの決済タイプを識別するホスト可用性要求を受信することと、ホスト電子デバイスがクライアント電子デバイスに関連付けられていると

判定することと、ホスト電子デバイスがクライアント電子デバイスに関連付けられているという判定に基づいて、ホスト電子デバイスのセキュアエレメントにプロビジョニングされたホストクレデンシャルアプリケーションが、受信されたホスト可用性要求の識別された少なくとも１つの決済タイプを満たすと判定することと、ホストクレデンシャルアプリケーションが識別された少なくとも１つの決済タイプを満たすという判定に基づいて、クライアント電子デバイスに、ホスト電子デバイスを識別するホスト可用性応答を送信することと、を含むことができる。

【０００７】

更に別の実施例として、金融機関サブシステム、小売商サブシステム、及びホスト電子デバイスを含むシステム内のクライアント電子デバイスは、オンライン通信コンポーネントと、プロセッサであって、オンライン通信コンポーネントを使用して小売商サブシステムから、金融トランザクションを示す潜在的なトランザクションデータにアクセスし、オンライン通信コンポーネントを使用してホスト電子デバイスに、潜在的トランザクションデータに基づいて決済要求データを通信し、オンライン通信コンポーネントを使用してホスト電子デバイスから、決済要求データに基づいてホスト決済クレデンシャルデータを受信し、オンライン通信コンポーネントを使用して小売商サブシステムに、ホスト決済クレデンシャルデータを通信する、プロセッサと、を含むことができ、ホスト決済クレデンシャルデータは、金融トランザクションの少なくとも一部に資金を供給するために、金融機関サブシステムから資金にアクセスするように動作する。

【０００８】

更に別の実施例として、少なくとも１つのプログラムを記憶する非一時的コンピュータ可読記憶媒体を提供することができ、少なくとも１つのプログラムは、命令を含み、命令は、ユーザインターフェース出力コンポーネントを含む電子デバイスによって実行されるとき、電子デバイスに、潜在的なトランザクションに資金を供給するために、小売商サブシステムに受け入れ可能な少なくとも１つの決済タイプを識別させ、識別された少なくとも１つの決済タイプを示すホスト可用性要求データを送信させ、ホスト可用性要求データに基づいて別の電子デバイスからのホスト可用性応答データを処理させ、処理に応じて、ユーザインターフェース出力コンポーネントを使用して、他の電子デバイスへの決済要求データの送信を開始するように動作するユーザ選択可能な任意選択を提供させる。

【０００９】

更に別の実施例として、クライアント電子デバイス及びホスト電子デバイスを使用してサービスプロバイダサブシステムとトランザクションを実行する方法を提供することができる。その方法は、クライアント電子デバイスにおいて、サービスプロバイダサブシステムと通信して、サービスプロバイダサブシステムの製品へのアクセスを購入するためのトランザクションの少なくとも一部を定義することと、ホスト電子デバイスを関与させてトランザクションに資金を供給するためのトランザクションクレデンシャルを生成することと、を含むことができる。

【００１０】

本発明の概要は、本明細書に記載される主題のいくつかの態様の基本的な理解を提供するように、いくつかの例示的な実施形態を要約するためにのみ提供される。したがって、本発明の概要に記載された特徴は単なる例であり、本明細書に記載された主題の範囲又は精神を多少でも限定するものと解釈されるべきではないことが理解されよう。特に明記しない限り、一例の文脈で記載された特徴は、１つ以上の他の例の文脈で記載された特徴と組み合わせられるか又はそれとともに使用され得る。本明細書に記載された主題の他の特徴、態様、及び利点は、以下の発明を実施するための形態、図、及び特許請求の範囲から明らかとなるであろう。

【図面の簡単な説明】

【００１１】

以下の議論は以下の図面を参照しており、同様の参照符号は全体を通して同様の部分を指す。

【図１】トランザクションを実行するための例示的なシステムの概略図である。
【図１Ａ】図１のシステムのより詳細な概略図である。
【図１Ｂ】図１及び図１Ａのシステムの別のより詳細な概略図である。
【図２】図１、図１Ｂのシステムの電子デバイスのより詳細な概略図である。
【図２Ａ】図１及び図２の電子デバイスの別のより詳細な概略図である。
【図３】図１及び図２Ａの電子デバイスの正面図である。
【図３Ａ】図１～図３の１つ以上の電子デバイスのグラフィカルユーザインターフェースの画面の正面図であり、トランザクションを実行するプロセスを示す。
【図３Ｂ】図１～図３の１つ以上の電子デバイスのグラフィカルユーザインターフェースの画面の正面図であり、トランザクションを実行するプロセスを示す。
【図３Ｃ】図１～図３の１つ以上の電子デバイスのグラフィカルユーザインターフェースの画面の正面図であり、トランザクションを実行するプロセスを示す。
【図３Ｄ】図１～図３の１つ以上の電子デバイスのグラフィカルユーザインターフェースの画面の正面図であり、トランザクションを実行するプロセスを示す。
【図３Ｅ】図１～図３の１つ以上の電子デバイスのグラフィカルユーザインターフェースの画面の正面図であり、トランザクションを実行するプロセスを示す。
【図３Ｆ】図１～図３の１つ以上の電子デバイスのグラフィカルユーザインターフェースの画面の正面図であり、トランザクションを実行するプロセスを示す。
【図３Ｇ】図１～図３の１つ以上の電子デバイスのグラフィカルユーザインターフェースの画面の正面図であり、トランザクションを実行するプロセスを示す。
【図３Ｈ】図１～図３の１つ以上の電子デバイスのグラフィカルユーザインターフェースの画面の正面図であり、トランザクションを実行するプロセスを示す。
【図４】図１～図１Ｂのシステムの商業エンティティサブシステムのより詳細な概略図である。
【図５】トランザクションを実行するための例示的なプロセスのフローチャートである。
【図６】トランザクションを実行するための例示的なプロセスのフローチャートである。
【図７】トランザクションを実行するための例示的なプロセスのフローチャートである。
【図８】トランザクションを実行するための例示的なプロセスのフローチャートである。
【図９】トランザクションを実行するための例示的なプロセスのフローチャートである。
【図１０】トランザクションを実行するための例示的なプロセスのフローチャートである。
【発明を実施するための形態】
【００１２】
クレデンシャル対応（又は決済可能）ホスト電子デバイスのセキュアエレメントにプロビジョニングされたクレデンシャル（例えば、決済クレデンシャル又は任意の他の適切なトランザクションクレデンシャル）は、セキュアに資金を供給するか、又はトランザクション（例えば、金融トランザクション又は任意の他の適切なクレデンシャルトランザクション）を、小売商（又はサービスプロバイダ又は処理）サブシステムと、小売商サブシステムとインターフェースされ得るクライアント電子デバイスを介して、実行するために、使用されてもよい。小売商製品にアクセスする（例えば、購入する）ために、小売商サブシステム（例えば、オンラインリソース（例えば、オンラインアプリケーション又はウェブブラウザ）を介して、又は非接触近接ベース通信媒体を介して）とインターフェースする間、クライアントデバイスは、ホストデバイスを、資金を供給するために、又は他の方法でトランザクションを進めて小売商製品にアクセスするために使用されるクレデンシャルの所望のソースとして、識別することができる。次いで、クライアントデバイスは、識別されたホストデバイスに、資金を供給されるトランザクションを示すクレデンシャル（又は決済）要求（例えば、小売商、購入される製品、トランザクションのコスト、トランザクションの出荷住所、など、を示すデータ）を送信することができる。ホストデバイスが決済要求を受信するのに応じて、ホストデバイスのユーザが要求を承認した後、ホストデバイス上にプロビジョニングされたクレデンシャル（例えば、決済クレデンシャル）の特定のクレデンシャルデータ（例えば、トークンデータ及び関連付けられた暗号データ）

は、ホストデバイスのセキュアエレメントによって提供され、任意の他の適切なトランザクション情報（例えば、小売商、購入される製品、トランザクションのコスト、トランザクションの通貨、トランザクションの出荷アドレス、などを示すデータ）とともに、トランザクションに資金を供給するために、ホストデバイスからクライアントデバイスに、又は小売商サブシステムに、又は金融機関（又は発行又はクレデンシャル）サブシステムに、セキュアに通信される。そのようなクレデンシャルデータは、ホスト電子デバイスと小売商サブシステムの間で直接的に共有されなくてもよい。代わりに、クライアントデバイスは、ホストデバイスからクレデンシャルデータを受信し、次いで、クライアントデバイスは、クレデンシャルデータを小売商サブシステムと共有することができる。クライアントデバイスは、クライアントデバイスと関連付けられても関連付けられなくてもよい様々なホストデバイスの様々なクレデンシャルの状態を監視するように動作することができる、商業（又は運用又は信頼された）エンティティサブシステムの識別管理サービスを利用することを含む任意の適切な技術を使用して、ホストデバイスを識別しそれと通信することができる。

【００１３】

図１はシステム１を示し、そこでは、おそらく運用（又は商業又は信頼された）エンティティサブシステム４００と関連して、ホスト電子デバイス１００にプロビジョニングされたクレデンシャルが、ホスト電子デバイス１００によって使用されて、サービスプロバイダ（又は小売商又は処理）サブシステム２００と、クライアント電子デバイス１００’を介して、又はクライアント電子デバイス１００’の要求で、トランザクションを実行することができる。図１Ａ及び図１Ｂはシステム１のより詳細を示し、そこでは、商業（又は運用又は信頼された）エンティティサブシステム４００とともに金融機関（又は発行又はクレデンシャル）サブシステム３５０から１つ以上のクレデンシャルをホスト電子デバイス１００にプロビジョニングすることができ、及びそこでは、そのようなクレデンシャルは、ホスト電子デバイス１００によって使用されて、小売商（又はサービスプロバイダ又は処理）サブシステム２００及び関連付けられた取得サブシステム３００（例えば、取得銀行サブシステム）と、クライアント電子デバイス１００’の要求で、トランザクションを実行することができる。一方、図２、図３は、システム１の１つ以上の電子デバイスの特定の実施形態に関する更なる詳細を示す。図３Ａ～図３Ｈは例示的な画面１９０ａ～１９０ｈを示し、そのようなトランザクション中のシステム１の１つ以上の電子デバイスのグラフィカルユーザインターフェースを表すことができる。図４は、システム１の商業エンティティサブシステム４００の特定の実施形態に関する更なる詳細を示す。図５～図１０は、そのようなトランザクションを実行する例示的なプロセスのフローチャートである。

図１の説明

【００１４】

図１は例示的なシステム１の概略図であり、それは、サービスプロバイダ（又は小売商又はプロセッサ）との、クライアント電子デバイスを介しての又はその要求での、トランザクション（例えば、オンライン決済又は非接触近接ベース決済）におけるホスト電子デバイス上のクレデンシャルのセキュアな使用を可能にすることができる。例えば、図１に示すように、システム１は、そこに（例えば、ホスト電子デバイス１００のセキュアエレメント上に）プロビジョニングされた少なくとも１つのクレデンシャルを有するエンドユーザホスト電子デバイス１００、そこにプロビジョニングされた少なくとも１つのクレデンシャルを有しても有さなくてもよいエンドユーザクライアント電子デバイス１００’、運用（又は商業又は信頼された）エンティティサブシステム４００及びサービスプロバイダ（又は小売商又は処理）サブシステム２００を含むことができる。ホスト電子デバイス１００、クライアント電子デバイス１００’、サービスプロバイダサブシステム２００、及び運用エンティティサブシステム４００の任意の２つの間の任意の適切なデータの通信を、任意の適切な通信設定９を介して有効化することができ、それは、任意の適切な通信プロトコル及び／又は任意の適切なネットワーク及び／又はクラウドアーキテクチャを使用して、任意の適切な有線通信経路、無線通信経路、２つ以上の有線及び／又は無線通信経路

の組み合わせを含むことができる。

【００１５】

クレデンシャル（例えば、決済クレデンシャル又は任意の他の適切なトランザクションクレデンシャル）を、ホスト電子デバイス１００上に（例えば、ホスト電子デバイス１００のセキュアエレメント又は他の記憶コンポーネント上に）、任意の適切なクレデンシャル発行サブシステム（例えば、金融機関サブシステム）から、クレデンシャル発行サブシステムから直接的に、又は運用エンティティサブシステム４００を介してのいずれかで、プロビジョニングすることができ、それは、クレデンシャルデータをホストデバイス１００にセキュアに通信し、そのようなクレデンシャルデータを管理するように動作することができる。一旦、ホストデバイス１００にプロビジョニングされると、次いで、トランザクションクレデンシャルはホストデバイス１００によって使用されて、セキュアに資金を供給するか、又は、他の方法で、サービスプロバイダサブシステム２００（例えば、任意の適切な良好なサブシステムへのアクセスを提供するか又はトランザクションの一部として機能するように動作することができる任意の適切なサブシステム）と、サービスプロバイダサブシステム２００とインターフェースするクライアントデバイス１００’を介して、又はサービスプロバイダサブシステム２００トランザクションを開始し得たクライアントデバイス１００’に代わってのいずれかで、トランザクション（例えば、金融トランザクション又は任意の他の適切なクレデンシャルトランザクション）を実行することができる。

【００１６】

例えば、サービスプロバイダ製品にアクセスする（例えば、購入する）ために、サービスプロバイダサブシステム２００と（例えば、オンラインリソース（例えば、オンラインアプリケーション又はウェブブラウザ）を介して又は非接触近接ベース通信媒体を介して）インターフェースする間、クライアントデバイス１００’は、ホストデバイス１００を、資金を供給するか又は他の方法でトランザクションを進めてサービスプロバイダ製品にアクセスするために使用されるトランザクションクレデンシャルの所望のソースとして識別することができる。クライアントデバイス１００’は、トランザクションに資金を供給する際に使用するためのトランザクションクレデンシャルを記憶するか若しくはそこにプロビジョニングするように構成されなくてもよいタイプのデバイスであるか（例えば、クライアントデバイス１００’は、決済クレデンシャルをセキュアに利用するように動作するセキュアエレメントを含まなくてもよい）、又はトランザクションクレデンシャルを記憶するように構成されているが、クライアントデバイス１００’によって開始された特定のトランザクションで使用されることを望まれる特定のクレデンシャルをそこに現在記憶していないタイプのデバイスのいずれかであることができる。例えば、サービスプロバイダサブシステム２００の製品にアクセスするためのトランザクションを定義するためのクライアントデバイス１００’とサービスプロバイダサブシステム２００の間の任意の適切な通信中の任意の適切な時点で、クライアントデバイス１００’は、その代わりに（例えば、運用エンティティサブシステム４００によって）トランザクションに資金を供給する際に使用するために利用可能であり得るホストデバイス１００に記憶された少なくとも１つのトランザクションクレデンシャルの可用性を識別するか又は識別していてもよい。次いで、クライアントデバイス１００’は、ホストデバイス１００と任意の適切なデータを共有して、クライアントデバイス１００’の代わりにトランザクションに資金を供給するために、ホストデバイス１００上のそのようなトランザクションクレデンシャルがサービスプロバイダサブシステム２００と共有されることを要求することができる。そのような要求に応じて、ホストデバイス１００は、トランザクションに資金供給するように動作することができる任意の適切なトランザクションクレデンシャルデータを生成することができる。次いで、いくつかの実施形態では、ホストデバイス１００は、そのようなトランザクションクレデンシャルデータを任意の他の適切なトランザクションデータ（例えば、クライアントデバイス１００’からの要求に含まれるトランザクションデータ）とともに、サービスプロバイダサブシステム２００に通信して、クライアントデバイス１００’がトランザクションクレデンシャルデータを処理することなく（例えば、クライアントデバイス１００’は、トランザ

クションの制御をホストデバイス１００へハンドオフすることができる（例えば、トランザクションクレデンシャルの要求とともに通信中に））トランザクションの資金供給を完了することができる。あるいは、他の実施形態では、ホストデバイス１００は、そのようなトランザクションクレデンシャルデータをクライアントデバイス１００’に返信してもよく、クライアントデバイス１００’は、トランザクションクレデンシャルデータをサービスプロバイダサブシステム２００に通信してトランザクションの資金供給を完了することができる（例えば、サービスプロバイダサブシステム２００が、ホストデバイス１００と通信するか、又はそれを認識することも必要なく（例えば、トランザクションクレデンシャルデータがクライアントデバイス１００’上でローカルに生成されたかのように））。いずれのシナリオにおいても、運用エンティティサブシステム４００は、サービスプロバイダサブシステム２００と、トランザクションクレデンシャルデータを通信することができるいずれかのデバイスの間のコンジットとして利用され得る（例えば、任意の適切な共有された秘密又は運用プロバイダサブシステム２００の他のセキュリティ機能を使用してセキュアな通信経路を有効化するために）。更に、クライアントデバイス１００’は、ピアツーピア若しくは他の直接リンクを介して直接的に、を含む、任意の適切な技術を使用して、又はクライアントデバイス１００’と関連付けられても関連付けられなくてもよい様々なホストデバイスの様々なクレデンシャルの状態を監視するように動作することができる、識別管理サービス若しくは任意の他の適切な運用エンティティサービス２００を使用することにより、ホストデバイス１００を識別し、及び／又は他の方法でそれと通信することができる。（例えば、ホストデバイス１００とクライアントデバイス１００’は、運用エンティティサブシステム２００によって管理される共通のユーザアカウントに基づいて互いに対になるか、又は互いに関連付けられ、トランザクションプロセスの任意の適切な部分を容易にすることができる）。

図１Ａの説明

【００１７】

ここで図１Ａを参照して、図１Ａは、図１に関して上述したシステム１の拡大図を示し、それは、クライアント電子デバイスを介しての小売商とのトランザクション（例えば、オンライン決済又は非接触近接ベース決済）においてホスト電子デバイスでクレデンシャルをセキュアに使用することを可能にする。例えば、図１Ａに示すように、システム１は、ホスト電子デバイス１００に１つ以上のクレデンシャルをセキュアにプロビジョニングするためのエンドユーザホスト電子デバイス１００並びに商業エンティティサブシステム４００及び金融機関（又はクレデンシャル又は発行）サブシステム３５０を含むことができる。更に、図１Ａに示すように、システム１は、エンドユーザクライアント電子デバイス１００’及び小売商（又はサービスプロバイダ又は処理）サブシステム２００を含むことができ、そのようなプロビジョニングされたクレデンシャルは、ホストデバイス１００によって使用されて、クライアントデバイス１００’を介して小売商サブシステム２００と金融トランザクションを実行することができる。例えば、小売商サブシステム２００との特定の金融トランザクションのためのクライアントデバイス１００’からのクライアント決済要求の受信に応じて、ホストデバイス１００は、プロビジョニングされたクレデンシャルのホストトランザクションデータ又はホスト決済クレデンシャルデータをクライアントデバイス１００’と共有することができ（例えば、セキュアなホストトランザクションデータ６８４として）、クライアントデバイス１００’は、次いで、そのホスト決済クレデンシャルデータを、非接触近接ベース通信５（例えば、近距離通信又はＢｌｕｅＴｏｏｔｈ（登録商標）通信）及び／又はオンラインベース通信６８６（例えば、ネットワーク電気通信又は他の方法）として、小売商サブシステム２００と共有し、小売商サブシステム２００との特定の金融トランザクションに資金を供給することができる。システム１は、金融機関サブシステム３５０との金融トランザクションを完了するために、非接触近接ベース通信５及び／又はそのようなオンラインベースの通信６８６を利用することができる取得銀行サブシステム３００も含むことができる。

【００１８】

システム１は、クライアントデバイス１００’と小売商サブシステム２００の間の通信を有効化する通信経路１５、小売商サブシステム２００と取得銀行サブシステム３００の間の通信を有効化する通信経路２５、取得銀行サブシステム３００と金融機関サブシステム３５０の間の通信を有効化する通信経路３５、金融機関サブシステム３５０の決済ネットワークサブシステム３６０と金融機関サブシステム３５０の発行銀行サブシステム３７０の間の通信を有効化する通信経路４５、金融機関サブシステム３５０と商業エンティティサブシステム４００の間の通信を有効化する通信経路５５、商業エンティティサブシステム４００とホスト電子デバイス１００の間の通信を有効化する通信経路６５、金融機関サブシステム３５０とホスト電子デバイス１００の間の通信を有効化する通信経路７５、商業エンティティサブシステム４００と小売商サブシステム２００の間の通信を有効化する通信経路８５、商業エンティティサブシステム４００とクライアントデバイス１００’の間の通信を有効化する通信経路９５、及びホストデバイス１００とクライアントデバイス１００’の間の通信を有効化する通信経路９９、を含むことができる。経路１５、２５、３５、４５、５５、６５、７５、８５、９５及び９９の１つ以上は、１つ以上の信頼されたサービスマネージャ（「ＴＳＭ」）によって少なくとも部分的に管理されてもよい。通信ネットワークを生成するように動作することができる任意の適切な回路、デバイス、システム、又はこれらの組み合わせ（例えば、１つ以上の通信タワー、電気通信サーバ、などを含み得る無線通信インフラストラクチャ）を使用して、任意の適切な有線通信プロトコル又は無線通信プロトコルを使用して通信を提供することができる、経路１５、２５、３５、４５、５５、６５、７５、８５、９５及び９９の１つ以上を提供することができる。例えば、経路１５、２５、３５、４５、５５、６５、７５、８５、９５及び９９のうちの１つ以上は、Ｗｉ－Ｆｉ（例えば、８０２．１１プロトコル）、ＺｉｇＢｅｅ（例えば、８０２．１５．４プロトコル）、ＷｉＤｉ（商標）、イーサネット（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＢＬＥ、（例えば、９００ＭＨｚ、２．４ＧＨｚ、及び５．６ＧＨｚの通信システム）、赤外線、ＴＣＰ／ＩＰ、ＳＣＴＰ、ＤＨＣＰ、ＨＴＴＰ、ＢｉｔＴｏｒｒｅｎｔ（商標）、ＦＴＰ、ＲＴＰ、ＲＴＳＰ、ＲＴＣＰ、ＲＡＯＰ、ＲＤＴＰ、ＵＤＰ、ＳＳＨ、ＷＤＳブリッジング、無線及び携帯電話及び個人用電子メールデバイスによって使用され得る任意の通信プロトコル（例えば、ＧＳＭ（登録商標）、ＧＳＭ（登録商標）プラスＥＤＧＥ、ＣＤＭＡ、ＯＦＤＭＡ、ＨＳＰＡ、マルチバンドなど）、低電力無線パーソナルエリアネットワーク（「６ＬｏＷＰＡＮ」）モジュール、その他の通信プロトコルによって使用され得る任意の通信プロトコル、又はそれらの任意の組み合わせ、をサポートすることができる。経路１５、２５、３５、４５、５５、６５、７５、８５、９５及び９９のうちの１つ以上は、任意の適切な通信設定（例えば、図１の通信設定９）によって有効化され得る。

図１Ｂの説明

【００１９】

ここで図１Ｂを参照して、図１Ｂは、図１Ａに関して上述したシステム１のより詳細な図を示す。図１Ｂに示すように、例えば、ホスト電子デバイス１００は、プロセッサ１０２、通信コンポーネント１０６、及び／又は近距離通信（ＮＦＣ）コンポーネント１２０を含むことができる。ＮＦＣコンポーネント１２０は、耐改ざん性プラットフォーム（例えば、単一チップ又は複数チップのセキュアマイクロコントローラ）を提供するように構成され得るセキュアエレメント１４５を含むか又は他の方法で提供することができ、それは、よく識別された信頼された権限者（例えば、金融機関サブシステム及び／又はＧｌｏｂａｌＰｌａｔｆｏｒｍなどの業界標準の権限者）の集合によって設定され得るルール及びセキュリティ要件に従って、アプリケーション並びにそれらの機密及び暗号データ（例えば、図１Ｂに示すように、クレデンシャル鍵１５５ａ’、及びアクセス鍵１５５ａ、及び／又は発行者セキュリティドメイン（「ＩＳＤ」）鍵１５６ｋなどの、クレデンシャルアプレット及び関連付けられたクレデンシャル鍵）をセキュアにホスティングすることを可能にし得る。以下により詳細に説明するように、ホストデバイス１００のセキュアエレメント１４５（例えば、ＮＦＣコンポーネント１２０）上のクレデンシャルアプレット又は

決済アプリケーション、ホスト決済クレデンシャルデータを、ホストトランザクションデータとして十分詳細に提供するように構成されて、資金供給アカウント又は他の金融商品又はクレジットソース（例えば、金融機関サブシステム３５０における）を識別することができ、ここで、そのようなホスト決済クレデンシャルデータは、クライアントデバイス１００’及び／又は小売商サブシステム２００及び／又は商業エンティティサブシステム４００との１つ以上の通信においてホストデバイス１００によって使用され、金融トランザクションを容易にすることができる。ＮＦＣコンポーネント１２０は、小売商サブシステム２００との（例えば、レンガ及びモルタルの店舗、又はホストデバイス１００のユーザがホストデバイス１００に記憶されたクレデンシャルを使用して非接触近接ベース通信を介して近位に位置する小売商端末２２０と金融トランザクションを実行することができる、レンガ及びモルタルの店舗又は任意の物理的な場所に配置され得る、小売商サブシステム２００の小売商端末２２０との通信経路（図示せず）を介しての）及び／又はクライアントデバイス１００’のＮＦＣコンポーネント１２０’との、非接触近接ベース通信（例えば、近距離通信）として、そのようなホスト決済クレデンシャルデータを通信するように構成されてもよい。代替で、又は追加で、通信コンポーネント１０６は、ホストデバイス１００が任意の適切なホスト決済データを、１つ以上の他の電子デバイス又はサーバ又はサブシステム（例えば、システム１の１つ以上のサブシステム又は他のコンポーネント）と、任意の適切な有線又は無線プロトコルを使用して（例えば、通信経路６５、７５、及び／又は９９のうちの１つ以上を介して）通信することを可能にするように提供され得る。ホストデバイス１００のプロセッサ１０２は、ホストデバイス１００の１つ以上のコンポーネントの動作及び性能を制御するように動作することができる任意の処理回路を含むことができる。例えば、プロセッサ１０２は、デバイス１００上の１つ以上のアプリケーション（例えば、アプリケーション１０３及び／又はオンラインリソース又は小売商アプリケーション１１３）を実行するように構成されてもよく、それは、データ（例えば、ホストトランザクションデータのホスト決済クレデンシャルデータ）が、ホストデバイス１００によって通信されて、クライアントデバイス１００’を介してなどの小売商サブシステム２００との金融トランザクションに資金を供給する方法（例えば、データがホストデバイス１００とクライアントデバイス１００’の間で（例えば、通信経路９９を介して）通信される方法、及び／又は通信経路９５を介して商業エンティティサブシステム４００からクライアントデバイス１００’に最終的に通信され得る、ホストデバイス１００と商業エンティティサブシステム４００の間で（例えば、通信経路６５を介して）データを通信する方法、を少なくとも部分的に指示することができる。更に、図１Ｂに示すように、ホストデバイス１００は、プロセッサ１０２又はデバイス１００の任意の他の適切な部分にアクセス可能な任意の適切なホストデバイス識別情報１１９を含むことができる。ホストデバイス識別情報１１９は、クライアントデバイス１００’及び／又は商業エンティティサブシステム４００及び／又は小売商サブシステム２００及び／又は金融機関サブシステム３５０のユーザによって、ホストデバイス１００を一意的に識別するために利用されて、小売商サブシステム２００との金融トランザクションを容易にすることができ、及び／又はホストデバイス１００との任意の適切なセキュア通信を有効化することができる。単なる一例として、ホストデバイス識別情報１１９は、電話番号又は電子メールアドレス、又はデバイス１００に関連付けられ得る任意の一意の識別子であってもよい。

【００２０】

クライアントデバイス１００’は、ホストデバイス１００と同じコンポーネントの１つ、いくつか、若しくは全て、又はホストデバイス１００によって提供されない任意のコンポーネントを含むことができる。例えば、図１Ｂに示すように、クライアントデバイス１００’は、ホストデバイス１００と（例えば、通信経路９９を介して）、及び／又は商業エンティティサブシステム４００と（例えば、通信経路９５を介して）、及び／又は小売商サブシステム２００と（例えば、通信経路１５を介して）、任意の適切な通信を通信し得る任意の適切な通信コンポーネント１０６’を含むことができる。追加で、又は代替で、図１Ｂに示すように、クライアントデバイス１００’は、小売商サブシステム２００の端末２２

０と非接触近接ベース通信５を通信するように動作することができる任意の適切な非接触近接ベース又はＮＦＣコンポーネント１２０’を含むことができる。追加で、又は代替で、図１Ｂに示すように、クライアントデバイス１００’は任意の適切なプロセッサ１０２’を含むことができ、それは、ホストデバイス１００からの決済クレデンシャルデータが、クライアントデバイス１００’によって通信されて、小売商サブシステム２００との金融トランザクションに資金を供給することができる方法を少なくとも部分的に指定し得る１つ以上の適切なアプリケーション（例えば、オンラインリソース又は小売商アプリケーション１１３’）をデバイス１００’上で実行するように動作することができる。更に、図１Ｂに示すように、クライアントデバイス１００’は任意の適切なクライアントデバイス識別情報１１９’を含むことができ、それは、プロセッサ１０２’又はデバイス１００’の任意の他の適切な部分にアクセス可能であり得る。クライアントデバイス識別情報１１９’は、クライアントデバイス１００’を一意的に識別するために、ホストデバイス１００及び／又は商業エンティティサブシステム４００及び／又は小売商サブシステム２００及び／又は金融機関サブシステム３５０のユーザによって利用されて、小売商サブシステム２００との金融トランザクションを容易にすることができ、及び／又はクライアントデバイス１００’との任意の適切なセキュア通信を有効化することができる。単なる一例として、クライアントデバイス識別情報１１９’は、電話番号又は電子メールアドレス、又はデバイス１００’に関連付けられ得る任意の一意の識別子であってもよい。図示されていないが、クライアント電子デバイス１００’は、図２の電子デバイス１００のＩ／Ｏインターフェース１１４と同じか又は類似のＩ／Ｏインターフェース、図２の電子デバイス１００のバス１１８と同じか又は類似のバス、図２の電子デバイス１００のメモリコンポーネント１０４と同じか又は類似のメモリコンポーネント、及び／又は図２の電子デバイス１００の電源コンポーネント１０８と同じか又は類似の電源コンポーネントも含むことができる。

【００２１】

小売商サブシステム２００は、図１Ｂに示すように、任意の適切な小売商サーバ２１０を含むことができ、それには、任意の適切な通信プロトコル（例えば、Ｗｉ－Ｆｉ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、携帯電話、有線ネットワークプロトコル、など）を介して、商業エンティティサブシステム４００の通信コンポーネントと（例えば、通信経路８５を介して）、及び／又は取得銀行３００の通信コンポーネントと（例えば、通信経路２５を介して）、及び／又はクライアントデバイス１００’の通信コンポーネントと（例えば、通信パス１５を介して）、通信するように構成された任意の適切なコンポーネント又はサブシステムが含まれ得る。例えば、小売商サーバ２１０は、潜在的なトランザクションデータ６６０及び／又は更新された潜在的なトランザクションデータ６７２を、小売商サーバ２１０によって管理され得るクライアントデバイス１００’上で動作するサードパーティ小売商アプリケーション１１３’、又はターゲット又はウェブリソースが小売商サーバ２１０によって管理され得るユニフォームリソースロケータ（「ＵＲＬ」）を示され得るクライアントデバイス１００’上で動作するインターネットアプリケーション１１３’（例えば、Ａｐｐｌｅ　Ｉｎｃ．によるＳａｆａｒｉ（商標））、などの、クライアントデバイス１００’のユーザが、小売商サーバ２１０と通信して、クライアントデバイス１００’上で実行中であり得る任意の適切な小売商オンラインリソース１１３’を介して金融トランザクションを実行する場合など、任意の適切なオンラインコンテキスト内でクライアントデバイス１００’の通信コンポーネント１０６’と、通信するように動作することができる。したがって、小売商サーバ２１０とクライアントデバイス１００’の間の通信は、（例えば、インターネットを介して）無線で及び／又は有線経路を介して行われ得ることに留意されたい。小売商サーバ２１０は、小売商サブシステム２００の小売商によって提供されてもよい（例えば、ウェブサイトデータをホストし、及び／又はサードパーティのアプリケーションデータを管理するためのウェブサーバとして）。追加で、又は代替で、図１Ｂに示すように、小売商サブシステム２００は任意の適切な小売商端末２２０（例えば、小売商決済端末）を含むことができ、それは、任意の適切なデータをホストデバイス１００の及び／又はクライアントデバイス１００’の非接触近接ベース通信コンポーネント（例えば、

クライアントデバイス１００’のＮＦＣコンポーネント１２０’との非接触近接ベース通信５）と通信するように構成された任意の適切なコンポーネント又はサブシステムを含むことができる。更に、図１Ｂに示すように、小売商サブシステム２００は、小売商鍵１５７を含むことができる。図示されていないが、小売商サブシステム２００は、図１Ｂ及び図２の電子デバイス１００のプロセッサコンポーネント１０２と同じか又は類似であり得る小売商プロセッサコンポーネント、図１Ｂ及び図２の電子デバイス１００の通信コンポーネント１０６と同じか又は類似であり得る小売商通信コンポーネント（例えば、サーバ２１０の一部として）、図２の電子デバイス１００のＩ／Ｏインターフェース１１４と同じか又は類似であり得る小売商Ｉ／Ｏインターフェース、図２の電子デバイス１００のバス１１８と同じか又は類似であり得る小売商バス、図２の電子デバイス１００のメモリコンポーネント１０４と同じか又は類似であり得る小売商メモリコンポーネント、及び／又は図２の電子デバイス１００の電源コンポーネント１０８と同じか又は類似であり得る小売商電源コンポーネント、も含むことができる。

【００２２】

金融機関サブシステム３５０は、決済ネットワークサブシステム３６０（例えば、決済カードアソシエーション又はクレジットカードアソシエーション）及び／又は発行銀行サブシステム３７０を含むことができる。例えば、発行銀行サブシステム３７０は、特定のクレデンシャルによって負い得る債務を償還するための消費者の能力に対して主たる責任を負うことができる金融機関であってもよい。ホストデバイス１００のＮＦＣコンポーネント１２０の各特定のクレデンシャルアプレットは、特定のユーザのアカウント（単数又は複数）に電子的にリンクされ得る特定の決済カードに関連付けられ得る。クレジットカード、デビットカード、チャージカード、ストアドバリューカード、フリートカード、ギフトカード、などを含む様々なタイプの決済カードが適切であり得る。特定の決済カードの商取引クレデンシャルは、小売商サブシステム２００との（例えば、直接的に、又は商業エンティティサブシステム４００を介して、及び／又はクライアントデバイス１００’を介して）商取引クレデンシャルデータ通信（例えば、非接触近接ベース通信及び／又はオンラインベース通信）で使用するために発行銀行サブシステム３７０によって、ホストデバイス１００上にプロビジョニングされ得る（例えば、後述するように、ＮＦＣコンポーネント１２０のクレデンシャル追加セキュリティドメインのクレデンシャルとして）。各クレデンシャルは、決済ネットワークサブシステム３６０によってブランド化され得る特定のブランドの決済カードであり得る。決済ネットワークサブシステム３６０は、特定のブランドの決済カード（例えば商取引クレデンシャル）の使用を処理することができる様々な発行銀行３７０及び／又は様々な取得銀行３００のネットワークであってもよい。

【００２３】

金融トランザクションをシステム１内で行うためには、ホスト電子デバイス１００のＮＦＣコンポーネント１２０のセキュアエレメントに少なくとも１つの商取引クレデンシャルをセキュアにプロビジョニングしなければならない。例えば、そのような商取引クレデンシャルは、金融機関サブシステム３５０から直接的にホストデバイス１００のＮＦＣコンポーネント１２０のセキュアエレメントに少なくとも部分的にプロビジョニングされ得る（例えば、金融機関サブシステム３５０とデバイス１００の間の通信経路７５を介してのクレデンシャルデータ６５４として、それは、通信コンポーネント１０６を介してＮＦＣコンポーネント１２０に渡され得る）。追加で、又は代替で、そのような商取引クレデンシャルは、商業エンティティサブシステム４００を介して金融機関サブシステム３５０からホストデバイス１００のＮＦＣコンポーネント１２０のセキュアエレメントに少なくとも部分的にプロビジョニングされ得る（例えば、金融機関サブシステム３５０と商業エンティティサブシステム４００の間の通信経路５５を介してクレデンシャルデータ６５４として、それは、商業エンティティサブシステム４００のサーバ４１０とデバイス１００の通信コンポーネント１０６の間の通信経路６５を介してクレデンシャルデータ６５４としてデバイス１００に渡されてもよく、それは、次いで、通信コンポーネント１０６からＮＦＣコンポーネント１２０に渡されてもよい）。経路７５を介した及び／又は経路５５

／６５を介したクレデンシャルデータ６５４は、ＮＦＣコンポーネント１２０のクレデンシャル追加セキュリティドメインの少なくとも一部又は全てとしてデバイス１００のセキュアエレメントにプロビジョニングされ、クレデンシャル情報１６１ａ及びクレデンシャル鍵１５５ａ’を有する決済アプリケーション又はクレデンシャルアプレット１５３ａなどの、クレデンシャル情報及び／又はクレデンシャル鍵を有するクレデンシャルアプレットを含むことができる。図１Ｂに示すように、例えば、金融機関サブシステム３５０は、クレデンシャル鍵１５５ａ’にアクセスすることもできる（例えば、クレデンシャル鍵１５５ａ’を使用してデバイス１００によって暗号化されたデータを復号するために）。金融機関サブシステム３５０は、そのような鍵の生成、交換、記憶、使用、及び置換を含むことができるクレデンシャル鍵１５５ａ’の管理に対して責任を負うことができる。金融機関サブシステム３５０は、クレデンシャル鍵１５５ａ’のそのバージョンを金融機関サブシステム３５０のセキュアエレメントに記憶することができる。ＮＦＣコンポーネント１２０及び金融機関サブシステム３５０のクレデンシャル鍵１５５ａ’は、電子デバイス１００のセキュアエレメントと金融機関サブシステム３５０の両方に利用可能な、任意の適切な共有秘密（例えば、パスワード、パスフレーズ、ランダムに選択されたバイトの配列、１つ以上の対称鍵、公開－秘密鍵（例えば、非対称鍵）、など）であることができ、それは、そのような共有秘密が金融機関サブシステム３５０によってデバイス１００にプロビジョニングされ得る共有秘密によって機能的な出力が少なくとも部分的に判定され得る任意の適切な暗号アルゴリズム又は暗号を使用することによってなど、電子デバイス１００及び金融機関サブシステム３５０によって（例えば、金融トランザクションの決済データを検証するために）任意の適切な暗号データ（例えば、暗号文）又は任意の他の適切なデータが独立して生成されることを有効化するように動作することができることが、理解されるべきである。共有秘密は、金融機関サブシステム３５０とホストデバイス１００の間で（例えば、金融機関サブシステム３５０によるデバイス１００上にクレデンシャルのプロビジョニング中に）予め共有されて、その場合そのような共有秘密は、事前共有鍵と呼ばれ得るか、又は共有秘密は、鍵共有プロトコルを使用することによって（例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎなどの公開鍵暗号を使用して、又はＫｅｒｂｅｒｏｓなどの対称鍵暗号を使用して）特定の金融トランザクションのために使用される前に作成され得るか、のいずれかであってもよい。共有秘密及び共有秘密情報によって機能的出力が少なくとも部分的に判定され得る任意の適切な暗号アルゴリズム又は暗号は、デバイス１００のセキュアエレメントにアクセス可能であることができる。

【００２４】

商業エンティティサブシステム４００は、金融機関サブシステム３５０とホストデバイス１００の間の仲介として提供されてもよく、商業エンティティサブシステム４００は、新しいセキュリティレイヤーを提供し、及び／又はよりシームレスなユーザエクスペリエンスを提供するように構成されてもよく、このときクレデンシャルはデバイス１００のセキュアエレメント上にプロビジョニングされており、及び／又はこのときそのようなプロビジョニングされたクレデンシャルは、デバイス１００と小売商サブシステム２００の間の商取引クレデンシャルデータ通信の一部として使用されている。商業エンティティサブシステム４００は、デバイス１００のユーザ及び／又はデバイス１００’のユーザに様々なサービスを提供することができる特定の商業エンティティによって、その商業エンティティを有するユーザ固有のアカウント（例えば、ユーザ固有の識別及びパスワードの組み合わせを介して）へのユーザ固有のログイン情報を介して、提供されてもよい。単なる一例として、商業エンティティサブシステム４００は、Ａｐｐｌｅ　Ｉｎｃ．ｏｆ　Ｃｕｐｅｒｔｉｎｏ，ＣＡによって提供されてもよく、それは、デバイス１００及び／若しくはデバイス１００’のユーザへの様々なサービス（例えば、デバイス１００によって再生されるメディアを販売／レンタルするためのｉＴｕｎｅｓ（商標）Ｓｔｏｒｅ、アプリケーションを販売／レンタルするためのＡｐｐｌｅ　Ａｐｐ　Ｓｔｏｒｅ（商標）、デバイス１００に使用するために、デバイス１００からのデータを記憶し、並びに／又は複数のユーザデバイス及び／若しくは複数のユーザプロファイルを相互に関連付けるためのＡｐｐｌｅ　ｉ

Ｃｌｏｕｄ（商標）Ｓｅｒｖｉｃｅ、様々なＡｐｐｌｅ製品をオンラインで購入するためのＡｐｐｌｅ　Ｏｎｌｉｎｅ　Ｓｔｏｒｅ、デバイス間でメディアメッセージを通信するためのＡｐｐｌｅ　ｉＭｅｓｓａｇｅ（商標）Ｓｅｒｖｉｃｅ、など）、のプロバイダであることもでき、並びに、それは、デバイス１００自体及び／若しくはデバイス１００’自体の（例えば、デバイス１００がｉＰｏｄ（登録商標）、ｉＰａｄ（登録商標）、ｉＰｈｏｎｅ（登録商標）、などである場合）、並びに／又はデバイス１００及び／若しくはデバイス１００’のオペレーティングシステム（例えば、デバイスアプリケーション１０３）のプロバイダ、製造者並びに／又は開発者であることもできる。商業エンティティサブシステム４００（例えば、Ａｐｐｌｅ　Ｉｎｃ．）を提供することができる商業エンティティは、金融機関サブシステム３５０の任意の金融エンティティとは異なる独立したものであってもよい。例えば、商業エンティティサブシステム４００を提供することができる商業エンティティは、エンドユーザホストデバイス１００にプロビジョニングされる任意のクレジットカード又は他の商取引クレデンシャルを提供及び／又は管理することができる任意の決済ネットワークサブシステム３６０又は発行銀行サブシステム３７０とは異なる、及び／又は独立したものであってもよい。追加で、又は代替で、商業エンティティサブシステム４００（例えば、Ａｐｐｌｅ　Ｉｎｃ．）を提供することができる商業エンティティは、小売商サブシステム２００の任意の小売商とは異なる独立したものであってもよい。例えば、商業エンティティサブシステム４００を提供することができる商業エンティティは、ＮＦＣ通信用の小売商端末、サードパーティアプリケーション１１３、及び／又は小売商サブシステム２００の任意の他の態様を提供し得る小売商サブシステム２００の任意の小売商とは異なる及び／又は独立したものであってもよい。そのような商業エンティティは、デバイス１００の様々なコンポーネント（例えば、その商業エンティティが、デバイス１００を少なくとも部分的に製造又は管理し得る場合などの、デバイス１００のソフトウェア及び／又はハードウェアコンポーネント）を構成又は制御するための潜在的能力を利用して、ユーザがホストデバイス１００上で金融機関サブシステム３５０によって提供されるクレデンシャルをプロビジョニングすることを望むとき、及び／又はそのようなプロビジョニングされたクレデンシャルが、小売商サブシステム２００との商取引クレデンシャルデータ通信の一部として使用されて、金融トランザクションに資金供給するとき、デバイス１００のユーザに対してシームレスなユーザエクスペリエンスを提供することができる。例えば、いくつかの実施形態では、デバイス１００は、商業エンティティサブシステム４００と、デバイス１００のユーザに（例えば、通信経路６５を介して）シームレスかつ透過的に通信して、より高いレベルの安全性を有効化し得る特定のデータを共有及び／又は受信する（例えば、デバイス１００と小売商サブシステム２００の間のオンラインベースの商取引クレデンシャルデータ通信中に）ように、構成され得る。図示されていないが、商業エンティティサブシステム４００は、図１Ｂ及び図２の電子デバイス１００のプロセッサコンポーネント１０２と同じか又は類似であり得るプロセッサコンポーネント、図１Ｂ及び図２の電子デバイス１００の通信コンポーネント１０６と同じか又は類似であり得る通信コンポーネント、図２の電子デバイス１００のＩ／Ｏインターフェース１１４と同じか又は類似であり得るＩ／Ｏインターフェース、図２の電子デバイス１００のバス１１８と同じか又は類似であり得るバス、図２の電子デバイス１００のメモリコンポーネント１０４と同じか又は類似であり得るメモリコンポーネント、及び／又は図２の電子デバイス１００の電源コンポーネント１０８と同じか又は類似であり得る電源コンポーネント、も含むことができ、それらの１つ、いくつか又は全部は、サーバ４１０によって少なくとも部分的に提供されてもよい。

【００２５】

ホストデバイス１００のＮＦＣコンポーネント１２０のセキュアエレメント上に（例えば、クレデンシャル鍵１５５ａ’及びクレデンシャル情報１６１ａを有するクレデンシャルＳＳＤの一部として）プロビジョニングされる少なくとも１つの商取引クレデンシャルに加えて、アクセス鍵１５５ｂを有する少なくとも１つのアクセスＳＳＤは、デバイス１００のＮＦＣコンポーネント１２０のセキュアエレメント上でプロビジョニングされて、デ

バイス１００が小売商サブシステム２００との金融トランザクションをよりセキュアに実行することを有効化することもできる。例えば、アクセスＳＳＤは、商業エンティティサブシステム４００から直接的にホストデバイス１００のＮＦＣコンポーネント１２０のセキュアエレメント上に少なくとも部分的にプロビジョニングされ得る（例えば、商業エンティティサブシステム４００のサーバ４１０とデバイス１００の通信コンポーネント１０６の間の通信経路６５を介してのアクセスデータ６５２として、それは、次いで、通信コンポーネント１０６からＮＦＣコンポーネント１２０に渡され得る）。パス６５を介したアクセスデータ６５２は、アクセスＳＳＤの少なくとも一部又は全部としてデバイス１００のセキュアエレメント上にプロビジョニングされてもよく、アクセス鍵１５５ｂを有するアクセスアプレット１５３ｂを含むことができる。図１Ｂに示すように、商業エンティティサブシステム４００は、アクセス鍵１５５ｂにアクセスすることもできる（例えば、アクセス鍵１５５ｂを使用してデバイス１００によって暗号化されたデータを復号するために）。商業エンティティサブシステム４００は、そのような鍵の生成、交換、記憶、使用、及び置換を含むことができるアクセス鍵１５５ｂの管理の責任を負うことができる。商業エンティティサブシステム４００は、そのバージョンのアクセス鍵１５５ｂを商業エンティティサブシステム４００のセキュアエレメントに記憶することができる。アクセス鍵１５５ｂを有するＮＦＣコンポーネント１２０のアクセスＳＳＤはデバイス１００のユーザの意図及びローカル認証を判定する（例えば、バイオメトリック入力コンポーネントなどの、デバイス１００の１つ以上の入力コンポーネント１１０を介して）ように構成されてもよく、そのような判定に対する応答において、別の特定のＳＳＤが決済トランザクションを実行する（例えば、ＮＦＣコンポーネント１２０のクレデンシャルＳＳＤのクレデンシャルを用いて）ことを有効化するように構成され得る。そのようなアクセスＳＳＤをデバイス１００のセキュアエレメント内に記憶することにより、金融トランザクションのユーザ意図及び認証を確実に判定するその能力を高めることができる。更に、ＮＦＣコンポーネント１２０のそのようなアクセスＳＳＤのアクセス鍵１５５ｂを利用して、デバイス１００のセキュアエレメントの外部で通信され得る金融トランザクションデータに増加された暗号化を提供することができる。追加で、又は代替で、以下に記載するように、アクセスデータ６５２は、電子デバイス１００のセキュアエレメントのＩＳＤのための発行者セキュリティドメイン（「ＩＳＤ」）鍵１５６ｋを含むことができ、それは、以下に記載するように、商業エンティティサブシステム４００によって維持されることも可能であり、アクセス鍵１５５ｂに加えて、又はその代わりとして使用され得る。

【００２６】

明示的に図示又は記載されていないが、商業エンティティサブシステム４００は、商業エンティティサブシステム４００が、ホストデバイス１００と相互作用するか又は関連付けられるように動作することができるのと任意の又は全ての同じ方法で、クライアントデバイス１００’と相互作用するか又は関連付けられるように動作することができる（例えば、クライアントデバイス１００’がホストデバイスとして動作することができるように、クレデンシャルがクライアントデバイス１００’上にプロビジョニングされ得る場合）ことが、理解されるべきである。

【００２７】

小売商アプリケーション又はオンラインリソース１１３’がクライアントデバイス１００’によってアクセスされて、オンライン金融トランザクションがデバイス１００’と小売商サブシステム２００の間で容易にされることを有効化することができる。第一に、そのようなアプリケーション１１３’は、アプリケーション１１３’がクライアントデバイス１００’によってアクセス可能であり得る前に、商業エンティティサブシステム４００によって承認されるか、又は他の方法で使用有効化されてもよい。例えば、商業エンティティサブシステム４００（例えば、Ａｐｐｌｅ　Ａｐｐ　Ｓｔｏｒｅ（商標））のアプリケーションストア４２０は、通信経路８５を介して、小売商サブシステム２００からアプリケーション１１３’を表す少なくともいくつかのデータを受信することができる。更に、いくつかの実施形態では、商業エンティティサブシステム４００は、アプリケーション１１３’用の小

売商鍵１５７’を生成するか、又は他の方法で割り当てることができ、小売商サブシステム２００にそのような小売商鍵１５７’を（例えば、経路８５を介して）提供することができる。あるいは、小売商サブシステム２００は、アプリケーション１１３’用の小売商鍵１５７’を生成するか、又は他の方法で割り当てることができ、商業エンティティサブシステム４００にそのような小売商鍵１５７’を（例えば、経路８５を介して）提供することができる。小売商サブシステム２００又は商業エンティティサブシステム４００のいずれかが、そのような鍵の生成、交換、保管、使用、及び置換を含む小売商鍵１５７’の責任を負うことができる。そのような小売商鍵１５７’がどのように又はどこで生成及び／又は管理されることが可能であっても、小売商サブシステム２００及び商業エンティティサブシステム４００の両方は、小売商鍵１５７’のバージョンを記憶することができる（例えば、それぞれの小売商サブシステム２００及び商業エンティティサブシステム４００のセキュアエレメントに）。いくつかの実施形態では、そのような小売商鍵１５７’は、小売商アプリケーション１１３’と具体的に関連付けられてもよく、他の実施形態では、小売商鍵１５７’は、小売商鍵１５７’が小売商サブシステム２００の同じ小売商によって操作される複数のサードパーティアプリケーションに関連付けられ得るように、小売商サブシステム２００の小売商と具体的に関連付けられてもよい。商業エンティティサブシステム４００にアクセス可能であり得るテーブル４３０又は他の適切なデータ構造又は情報源が、特定の小売商鍵１５７’を特定の小売商アプリケーション１１３’又は小売商エンティティと関連付けるために、提供され得る。表４３０は、商業エンティティサブシステム４００が適切な小売商鍵１５７’を判定して利用することを有効化し、鍵１５７’と関連付けられた小売商アプリケーション１１３’を介して、小売商サブシステム２００とインターフェースするクライアントデバイス１００’を含み得る金融トランザクションのために、小売商サブシステム２００に通信された任意の商取引クレデンシャルデータ（例えば、ホストデバイス１００にネーティブ決済クレデンシャルデータを含み得る商取引クレデンシャルデータ）にセキュリティのレイヤーを提供することができる。デバイス１００’は、アプリケーション１１３’にアクセスし（例えば、通信経路９５を介してアプリケーションストア４２０から）、アプリケーション１１３’を実行する（例えば、プロセッサ１０２’を用いて）ように構成され得る。追加で、又は代替で、小売商鍵１５７’は、小売商のウェブサイト（例えば、１つ以上のＵＲＬ）と、又は、小売商のサードパーティアプリケーション（例えば、アプリケーション１１３’）ではなく若しくはそれに加えて、小売商と一般に、関連付けられ得る。例えば、小売商サブシステム２００の小売商は、商業エンティティサブシステム４００と協働して、特定の小売商ウェブサイト又は小売商を、一般に、テーブル４３０内の特定の小売商鍵１５７’と関連付けることができ、それは、クライアントデバイス１００’が小売商サーバ２１０とインターフェースして、ターゲット又はウェブリソースがその小売商鍵１５７’に関連付けられ得るＵＲＬを示され得るデバイス１００’上で動作するインターネットアプリケーション又はウェブブラウザを介して金融トランザクションを行うことができる金融トランザクションのために、商業エンティティサブシステム４００が、適切な小売商鍵１５７’を判定して利用することを有効化して、小売商サブシステム２００に通信された任意の商取引クレデンシャルデータ（例えば、ホストデバイス１００にネーティブ決済クレデンシャルデータを含む商取引クレデンシャルデータ）にセキュリティのレイヤーを提供することができる。デバイス１００’は、例えば、通信経路１５を介して（例えば、デバイス１００’上のインターネットアプリケーション１１３’を使用して）小売商サーバ２１０からそのようなＵＲＬにアクセスするように構成され得る。他の実施形態では、アプリケーション１１３’は、特定の小売商、小売商サブシステム２００、及び／又は小売商鍵１５７’に関連付けられていなくてもよく、代わりに、デバイス１００’に利用可能な独立したアプリケーションであってもよい。いくつかの実施形態では、図示のように、小売商鍵１５７を有する同様のアプリケーション１１３は、ホストデバイス１００に提供されてもよく、アプリケーション１１３は、アプリケーション１１３’と同じであるか若しくは異なっていてもよく、及び／又は鍵１５７は、鍵１５７’とは異なっていてもよい。

図２の説明

【００２８】
ここで図２を参照して、図２は、図１～図１Ｂに関して上述したシステム１の電子デバイス１００のより詳細な図を示す。図２に示すように、例えば、電子デバイス１００は、プロセッサ１０２、メモリ１０４、通信コンポーネント１０６、電源１０８、入力コンポーネント１１０、出力コンポーネント１１２、アンテナ１１６、及び近距離通信（「ＮＦＣ」）コンポーネント１２０を含むことができる。電子デバイス１００は、デバイス１００の様々な他のコンポーネントから、又はそれらの間で、データ及び／若しくは電力の伝送のための１つ以上の有線若しくは無線の通信リンク又は経路を提供し得る、バス１１８も含むことができる。電子デバイス１００は、デバイス１００の外部の破片及び他の劣化させる力からの保護のために、デバイス１００の１つ以上のコンポーネントを少なくとも部分的に囲み得る筐体１０１も設けられてもよい。いくつかの実施形態では、電子デバイス１００の１つ以上のコンポーネントを組み合わせるか又は省略してもよい。更に、電子デバイス１００は、図２には組み合わされていないか又は含まれていない他のコンポーネントを含むことができる。例えば、電子デバイス１００は、図２に示すコンポーネントの任意の他の適切なコンポーネント又はいくつかのインスタンスを含むことができる。簡略化のために、各コンポーネントのうちの１つのみが図２に示されている。１つ以上の入力コンポーネント１１０が、ユーザがデバイス１００と対話するか、若しくはインターフェースすることを可能にするために提供されてもよく、並びに／又は１つ以上の出力コンポーネント１１２が、デバイス１００のユーザに情報（例えば、グラフィカル、可聴及び／若しくは触知情報）を提示するために、提供されてもよい。１つ以上の入力コンポーネント及び１つ以上の出力コンポーネントは、本明細書では、集合的に入出力（「Ｉ／Ｏ」）コンポーネント又はＩ／Ｏインターフェース１１４（例えば、Ｉ／Ｏコンポーネント又はＩ／Ｏインターフェース１１４としての入力コンポーネント１１０及び出力コンポーネント１１２）と呼ばれることもあり得ることに留意されたい。例えば、入力コンポーネント１１０及び出力コンポーネント１１２は、ユーザが表示画面をタッチして入力情報を受信することができ、その同じ表示画面を介してユーザに視覚情報を提供することができる、タッチ画面などの単一のＩ／Ｏコンポーネント１１４であることもあり得る。電子デバイス１００のプロセッサ１０２は、電子デバイス１００の１つ以上のコンポーネントの動作及び性能を制御するように動作することができる任意の処理回路を含むことができる。例えば、プロセッサ１０２は、入力コンポーネント１１０からの入力信号及び／又は出力コンポーネント１１２を介した駆動出力信号を受信することができる。図２に示すように、プロセッサ１０２を使用して、アプリケーション１０３及び／又はアプリケーション１１３などの１つ以上のアプリケーションを実行することができる。一例として、アプリケーション１０３は、オペレーティングシステムアプリケーションであり、アプリケーション１１３は、サードパーティアプリケーション又は他の適切なオンラインリソース（例えば、小売商サブシステム２００の小売商に関連付けられたアプリケーション）であってもよい。更に、図示のように、プロセッサ１０２は、ホストデバイス識別情報１１９にアクセスすることができ、それは、デバイス１００及び／又は商業エンティティサブシステム４００のユーザによって使用されて、デバイス１００の識別を、小売商サブシステム２００に（例えば、金融トランザクションを容易にするために）及び／又はクライアントデバイス１００’に（例えば、デバイス１００と１００’の間のセキュア通信を容易にするために）、提供することができる。

【００２９】
ＮＦＣコンポーネント１２０は、任意の適切な近接型の通信メカニズムであってもよく、それは、小売商サブシステム２００の電子デバイス１００と小売商端末（例えば、小売商決済端末２２０）の間の非接触近接ベースのトランザクション又は通信を有効化することができる。ＮＦＣコンポーネント１２０は、電子デバイス１００とそのような小売商端末の間の非接触近接ベース通信を有効化するための任意の適切なモジュールを含むことができる。図２に示すように、例えば、ＮＦＣコンポーネント１２０は、ＮＦＣデバイスモジュール１３０、ＮＦＣコントローラモジュール１４０、及び／又はＮＦＣメモリモジュ

ール１５０を含むことができる。ＮＦＣデバイスモジュール１３０は、ＮＦＣデータモジュール１３２、ＮＦＣアンテナ１３４、及びＮＦＣブースター１３６を含むことができる。ＮＦＣデータモジュール１３２は、非接触近接ベース又はＮＦＣ通信の一部として、小売商端末にＮＦＣコンポーネント１２０によって送信され得る任意の適切なデータを含ませるか、送信するか、又は他の方法で提供するように構成され得る。追加で、又は代替で、ＮＦＣデータモジュール１３２は、非接触近接ベース通信の一部として小売商端末からＮＦＣコンポーネント１２０によって受信され得る任意の適切なデータを含む、送信するか、又は他の方法で受信するように構成され得る。ＮＦＣコントローラモジュール１４０は、少なくとも１つのＮＦＣプロセッサモジュール１４２を含むことができる。ＮＦＣプロセッサモジュール１４２は、電子デバイス１００と小売商端末の間でＮＦＣ通信を通信するために、ＮＦＣデバイスモジュール１３０と連携して動作して、ＮＦＣコンポーネント１２０を有効化、起動、許可、及び／又は制御することができる。ＮＦＣコントローラモジュール１４０は、ＮＦＣコンポーネント１２０の機能を指示するのに役立ち得るＮＦＣ低電力モード又はウォレットアプリケーション１４３などの１つ以上のアプリケーションを実行するために使用され得る少なくとも１つのＮＦＣプロセッサモジュール１４２を含むことができる。ＮＦＣメモリモジュール１５０は、ＮＦＣデバイスモジュール１３０及び／又はＮＦＣコントローラモジュール１４０と連携して動作して、電子デバイス１００と小売商サブシステム２００の間のＮＦＣ通信を可能とすることができる。ＮＦＣメモリモジュール１５０は、耐改ざん性であってもよく、セキュアエレメント１４５の少なくとも一部を提供してもよい（例えば、図２Ａ参照）。例えば、そのようなセキュアエレメントは、耐改ざん性のプラットフォーム（例えば、単一チップ又は複数チップのセキュアマイクロコントローラ）を提供するように構成されてもよく、それは、よく識別された信頼された権限者（例えば、金融機関サブシステム及び／又はＧｌｏｂａｌＰｌａｔｆｏｒｍなどの業界標準の権限者）の集合によって設定され得るルール及びセキュリティ要件に従って、アプリケーション並びにそれらの機密及び暗号データ（例えば、アプレット１５３及び鍵１５５）をセキュアにホスティングすることを可能にし得る。

【００３０】

図２に示すように、例えば、ＮＦＣメモリモジュール１５０は、１つ以上の発行者セキュリティドメイン（「ＩＳＤ」）１５２及び追加セキュリティドメイン（「ＳＳＤ」）１５４（例えば、サービスプロバイダセキュリティドメイン（「ＳＰＳＤ」）、信頼されたサービスマネージャセキュリティドメイン（「ＴＳＭＳＤ」）、など）を含むことができ、それらは、ＮＦＣ仕様標準（例えば、ＧｌｏｂａｌＰｌａｔｆｏｒｍ）によって定義され管理され得る。例えば、ＩＳＤ１５２は、ＮＦＣメモリモジュール１５０の一部であってもよく、そこにおいて、信頼されたサービスマネージャ（「ＴＳＭ」）又は発行金融機関（例えば、金融機関サブシステム３５０）は、クレデンシャルコンテンツ管理、及び／又はセキュリティドメイン管理のために、鍵及び／又は他の適切な情報を記憶して、電子デバイス１００上で（例えば、通信コンポーネント１０６を介して）、１つ以上のクレデンシャル（例えば、様々なクレジットカード、銀行カード、ギフトカード、アクセスカード、トランジットパス、などと関連付けられたクレデンシャル）を生成するか又は他の方法でプロビジョニングすることができる。クレデンシャルは、クレジットカード決済番号（例えば、デバイスプライマリアカウント番号（「ＤＰＡＮ」）、ＤＰＡＮ有効期限、ＣＶＶ、など（例えば、トークン又はそれ以外のものとして））などの、／消費者に割り当てられ得る、電子デバイス１００にセキュアに記憶され得るクレデンシャルデータ（例えば、クレデンシャル情報１６１ａ）を含むことができる。ＮＦＣメモリモジュール１５０は、少なくとも２つのＳＳＤ１５４（例えば、少なくとも第１のＳＳＤ１５４ａ及び第２のＳＳＤ１５４ｂ）を含むことができる。例えば、第１のＳＳＤ１５４ａ（例えば、クレデンシャルＳＳＤ１５４ａ）は、電子デバイス１００に対して特定の特権又は決済権利を提供し得る特定のクレデンシャル（例えば、金融機関サブシステム３５０によってプロビジョニングされた特定のクレジットカードクレデンシャル又は特定の公共トランジットカードクレデンシャル）と関連付けられてもよく、一方、第２のＳＳＤ１５４ｂ（例えば、

アクセスＳＳＤ１５４ｂ）は、例えば、特定の特権又は決済権利を電子デバイス１００に提供するために、別のＳＳＤ（例えば、第１のＳＳＤ１５４ａ）の特定のクレデンシャルへのデバイス１００のアクセスを制御し得る商業エンティティ（例えば、デバイス１００に対する制御エンティティであり得る、商業エンティティサブシステム４００の商業エンティティ）と関連付けられてもよい。あるいは、第１のＳＳＤ１５４ａ及び第２のＳＳＤ１５４ｂの各１つは、電子デバイス１００に対して特定の特権又は決済権利を提供し得るそれぞれの特定のクレデンシャル（例えば、金融機関サブシステム３５０によってプロビジョニングされた特定のクレジットカードクレデンシャル又は特定の公共トランジットカードクレデンシャル）と関連付けられてもよい。各ＳＳＤ１５４は、少なくとも１つのアプレット１５３（例えば、アプレット１５３ａを有するＳＳＤ１５４ａ及びアプレット１５３ｂを有するＳＳＤ１５４ｂ）を含み、及び／又はそれに関連付けられてもよい。例えば、ＳＳＤ１５４のアプレット１５３は、（例えば、ＧｌｏｂａｌＰｌａｔｆｏｒｍ環境において）ＮＦＣコンポーネント１２０のセキュアエレメント上で動作し得るアプリケーションであってもよい。クレデンシャルアプレット１５３は、クレデンシャル情報１６１（例えば、アプレット１５３ａの情報１６１ａ及び／又はアプレット１５３ｂの情報１６１ｂ）を含むか、又はそれと関連付けられてもよい。各ＳＳＤ１５４及び／又はアプレット１５３は、それ自身の鍵１５５（例えば、少なくとも１つの鍵１５５ａを有するアプレット１５３ａ及び少なくとも１つの鍵１５５ｂを有するアプレット１５３ｂ）のうちの少なくとも１つを含み、及び／又はそれと関連付けられてもよい。

【００３１】

ＳＳＤ１５４の鍵１５５は、暗号アルゴリズム又は暗号の機能的な出力を判定することができる１つの情報であってもよい。例えば、暗号化において、鍵は、復号中に、暗号文への平文の特定の変換、又はその逆を指定することができる。鍵は、デジタル署名スキーム及びメッセージ認証コードなどの他の暗号アルゴリズムでも使用され得る。ＳＳＤの鍵は、任意の適切な共有秘密を他のエンティティに提供することができる。各鍵及びアプレットは、ＴＳＭ又は許可されたエージェントによってデバイス１００のセキュアエレメントに組み込まれてもよく、又はデバイス１００に最初に提供されるときにセキュアエレメントに予め組み込まれてもよい。一例として、クレデンシャルＳＳＤ１５４ａは特定のクレジットカードクレデンシャルと関連付けられ得るが、その特定のクレデンシャルは、そのクレデンシャルＳＳＤ１５４ａのアプレット１５３ａが有効化されているか、又は他の方法でそのような使用のためにアクティブ化又はロック解除されている場合、金融トランザクションのために、デバイス１００のセキュアエレメントから（例えば、ＮＦＣコンポーネント１２０から）小売商サブシステム２００への商取引クレデンシャルデータ通信として通信されるだけであり得る。

【００３２】

ＮＦＣコンポーネント１２０の使用を有効化するためにセキュリティ機能を設けることができ、それは、クレジットカード情報又はクレデンシャルの銀行口座情報などの機密決済情報を、電子デバイス１００から小売商サブシステム２００に（例えば、商業エンティティサブシステム４００を介して及び／又はデバイス１００’を介して）送信するときに、特に有用であり得る。そのようなセキュリティ機能は、制限されたアクセスを有し得るセキュア記憶領域も含むことができる。例えば、個人識別番号（「ＰＩＮ」）入力を介しての、又はバイオメトリックセンサーとのユーザ対話を介してのユーザ認証は、セキュア記憶領域にアクセスするために提供される必要があり得る。一例として、アクセスＳＳＤ１５４ｂは、アプレット１５３ｂを利用して、クレデンシャル情報１６１ａを通信するために他のＳＳＤ１５４（例えば、クレデンシャルＳＳＤ１５４ａ）を使用することを許可する前に、そのような認証を行ったかどうかを判定することができる。特定の実施形態では、セキュリティ機能の一部又は全部をＮＦＣメモリモジュール１５０内に記憶することができる。更に、小売商サブシステム２００と商取引クレデンシャルデータを通信するための、認証鍵などのセキュリティ情報は、ＮＦＣメモリモジュール１５０内に記憶され得る。特定の実施形態では、ＮＦＣメモリモジュール１５０は、電子デバイス１００内に組み

込まれたマイクロコントローラを含むことができる。単なる一例として、アクセスＳＳＤ１５４ｂのアプレット１５３ｂは、デバイス１００のユーザの意図及びローカル認証を判定するように（例えば、バイオメトリック入力コンポーネントなどの１つ以上の入力コンポーネント１１０を介して）構成されてもよく、そのような判定に応じて、別の特定のＳＳＤを有効化するように構成されて（例えば、クレデンシャルＳＳＤ１５４ａのクレデンシャルを用いて）決済トランザクションを実行することができる。

図２Ａの説明

【００３３】

ここで図２Ａを参照して、図２Ａは、図１、図２に関して上述したシステム１の電子デバイス１００の一部の別の詳細図を示す。図２Ａに示すように、例えば、ＮＦＣコンポーネント１２０のセキュアエレメント１４５は、アプレット１５３ａ、クレデンシャル情報１６１ａ、アクセス鍵１５５ａ、及び／又はクレデンシャル鍵１５５ａ’を含むか、又はそれらに関連付けられ得るＳＳＤ１５４ａ、並びにアプレット１５３ｂ、クレデンシャル情報１６１ｂ、アクセス鍵１５５ｂ、及び／又はクレデンシャル鍵１５５ｂ’を含むか、又はそれらに関連付けられ得るＳＳＤ１５４ｂ、を含むことができる。いくつかの実施形態では、特定の追加セキュリティドメイン（「ＳＳＤ」）１５４（例えば、ＳＳＤ１５４ａ及び１５４ｂのうちの１つ）は、特定のＴＳＭ及び少なくとも１つの特定の商取引クレデンシャル（例えば、特定のクレジットカードクレデンシャル又は公衆トランジットカードクレデンシャル）と関連付けられてもよく、それは、電子デバイス１００に特定の特権又は決済権利を提供することができる。各ＳＳＤ１５４は、それ自身のマネージャ鍵１５５（例えば、鍵１５５ａｋ及び１５５ｂｋのそれぞれ１つ）を有することができ、それは、ＮＦＣデバイスモジュール１３０による使用のためにそのＳＳＤ１５４の機能を有効化するようにアクティブ化される必要があり得る。追加で、又は代替で、各ＳＳＤ１５４は、特定の商取引クレデンシャルと関連付けられた少なくとも１つのそれ自身のクレデンシャルアプリケーション又はクレデンシャルアプレット（例えば、Ｊａｖａ（登録商標）カードアプレットインスタンス）を含み、及び／又はそれと関連付けられてもよく（例えば、ＳＳＤ１５４ａのクレデンシャルアプレット１５３ａは第１の商取引クレデンシャルに関連付けられてもよく、及び／又はＳＳＤ１５４ｂのクレデンシャルアプレット１５３ｂは第２の商取引クレデンシャルと関連付けられてもよい）。ここで、クレデンシャルアプレットはそれ自身のアクセス鍵例えば、クレデンシャルアプレット１５３ａに対するアクセス鍵１５５ａ及び／又はクレデンシャルアプレット１５３ｂに対するアクセス鍵１５５ｂ）及び／又はそれ自身のクレデンシャル鍵（例えば、クレデンシャルアプレット１５３ａに対するクレデンシャル鍵１５５ａ’及び／又はクレデンシャルアプレット１５３ｂに対するクレデンシャル鍵１５５ｂ’）を有することができ、ここで、クレデンシャルアプレットは、ＮＦＣ通信（例えば、小売商端末２２０との）として及び／又は電子デバイス１００と小売商サブシステム２００の間のオンラインベース通信（例えば、商業エンティティサブシステム４００及び／又はクライアントデバイス１００’を介して）として、ＮＦＣデバイスモジュール１３０によって使用するために、その関連付けられた商取引クレデンシャルを有効化するようにアクティブ化される必要があり得る。いくつかの実施形態では、クレデンシャルアプレットのクレデンシャル鍵（例えば、クレデンシャルアプレット１５３ａのクレデンシャル鍵１５５ａ’及び／又はクレデンシャルアプレット１５３ｂのクレデンシャル鍵１５５ｂ’）は、そのようなクレデンシャルに対して責任があり得る金融機関サブシステム３５０によって生成されてもよく、それらは金融機関サブシステム３５０によってアクセス可能であり（例えば、図１Ｂに示すように）、セキュアエレメント１４５と金融機関サブシステム３５０との間で（例えば、小売商サブシステム２００を介して）そのアプレットのクレデンシャル情報のセキュア送信を有効化することができる。追加で、又は代替で、クレデンシャルアプレットのアクセス鍵（例えば、クレデンシャルアプレット１５３ａのアクセス鍵１５５ａ及び／又はクレデンシャルアプレット１５３ｂのアクセス鍵１５５ｂ）は、商業エンティティサブシステム４００によって生成されてもよく、それは、商業エンティティサブシステム４００によってアクセス可能であり（例えば、図１Ｂに

示すように）、セキュアエレメント１４５と商業エンティティサブシステム４００の間でそのアプレットのそのクレデンシャル情報のセキュア送信を有効化することができる。追加で、又は代替で、図示のように、各アプレットは、アプレット１５３ａのＡＩＤ１５５ａａ及び／又はアプレット１５３ｂのＡＩＤ１５５ｂａなどのそれ自身の一意のアプリケーション識別子（「ＡＩＤ」）を含むことができる。例えば、ＡＩＤは、特定のカードスキーム及び製品、プログラム、又はネットワーク（例えば、ＭａｓｔｅｒＣａｒｄ　Ｃｉｒｒｕｓ、Ｖｉｓａ　ＰＬＵＳ、Ｉｎｔｅｒａｃ、など）を識別することができ、ここで、ＡＩＤは、ＡＩＤと関連付けられたクレデンシャルの決済システム（例えば、カードスキーム）又はネットワーク（例えば、ＭａｓｔｅｒＣａｒｄ、Ｖｉｓａ、Ｉｎｔｅｒａｃ、など）を識別するために使用され得る登録済みアプリケーションプロバイダ識別子（「ＲＩＤ」）ばかりでなく、ＡＩＤに関連付けられたクレデンシャルのプロバイダ又は決済システムによって提供される製品、プログラム、又はアプリケーションを区別するために使用され得る独自のアプリケーション識別子拡張子（「ＰＩＸ」）も含むことができる。セキュアエレメント１４５のファームウェアを管理するように動作することができる任意の適切な仕様（例えば、Ｊａｖａ（登録商標）　Ｃａｒｄ仕様）は、セキュアエレメント１４５上の各ＡＩＤの一意性を保証するか、又は他の方法で実施するように動作することができる（例えば、セキュアエレメント１４５上の各クレデンシャルインスタンスはそれ自身の一意のＡＩＤと関連付けられ得る）。

【００３４】

追加で、又は代替で、図２Ａに示すように、セキュアエレメント１４５はＩＳＤ１５２を含むことができ、それは、そのセキュリティドメイン（例えば、図１Ｂに示すように商業エンティティサブシステム４００）に関連付けられた信頼されたサービスマネージャにも既知であり得るＩＳＤ鍵１５６ｋを含むことができる。ＩＳＤ鍵１５６ｋは、商業エンティティサブシステム４００及び電子デバイス１００によって、アクセス鍵１５５ａ及び／若しくはアクセス鍵１５５ｂと同様に並びに／又はそれらの代わりに利用されて、商業エンティティサブシステム４００と電子デバイス１００のセキュアエレメント１４５の間のセキュア送信を有効化することができる。更に、図２Ａに示すように、プロセッサ１０２とセキュアエレメント１４５の間で、様々なデータを通信することができる。例えば、デバイス１００のプロセッサ１０２は、デバイスアプリケーション１０３を実行するように構成されてもよく、それは、プロセッサ１０２の小売商アプリケーション１１３並びに、セキュアエレメント１４５、Ｉ／Ｏインターフェースコンポーネント１１４ａ（例えば、Ｉ／Ｏ入力データ１１５ｉを受信するための、及び／又はＩ／Ｏ出力データ１１５ｏを送信するための）、及び／又は通信コンポーネント１０６と情報を通信することができる。更に、図示のように、プロセッサ１０２はデバイス識別情報１１９にアクセスすることができ、それは、デバイス１００とリモートエンティティの間のセキュア通信を有効化するために利用され得る。

【００３５】

追加で、又は代替で、図２Ａに示すように、セキュアエレメント１４５は制御権限セキュリティドメイン（「ＣＡＳＤ」）１５８を含むことができ、それは、サードパーティのオンエレメントの信頼のルートとして機能するように構成され得る特定の目的のセキュリティドメインであることができる。ＣＡＳＤ１５８の関連付けられたアプリケーションは、他のアプリケーション及び／又は特定の管理レイヤー（例えば、ＧｌｏｂａｌＰｌａｔｆｏｒｍ管理レイヤー）へのグローバルサービスとしてオンエレメントの機密鍵生成を提供するように構成され得る。ＣＡＳＤ１５８内で使用され得る機密鍵材料は、セキュアエレメント１４５の発行者を含む任意のエンティティによって検査又は変更されないように構成され得る。ＣＡＳＤ１５８は、ＣＡＳＤアクセスキット１５８ｋ（例えば、ＣＡＳＤ秘密鍵（「ＣＡＳＤ－ＳＫ」）、ＣＡＳＤ公開鍵（「ＣＡＳＤ－ＰＫ」）、ＣＡＳＤ証明書（「ＣＡＳＤ－Ｃｅｒｔ。」）、及び／若しくはＣＡＳＤ署名モジュール）を含むように構成されてもよく並びに／又はそれらを生成し、及び／若しくは他の方法で含むように構成されてもよい。例えば、ＣＡＳＤ１５８は、そのようなデータをデバイス１００の別

の部分（例えば、システム１の他のサブシステムと共有するための通信コンポーネント１０６）に提供する前に、（例えば、ＣＡＳＤアクセスキット１５８ｋを使用して）セキュアエレメント１４５上の特定のデータに署名するように構成されてもよい。一例として、ＣＡＳＤ１５８は、セキュアエレメント１４５によって提供される任意のデータに署名するように構成されて、他のサブシステム（例えば、商業エンティティサブシステム４００）が、そのような署名されたデータがセキュアエレメント１４５によって署名されたことを確認することができる（例えば、商業エンティティサブシステム４００において関連付けられたＣＡＳＤキット１５８ｋを使用して）。

【００３６】

追加で、又は代替で、図２Ａに示すように、セキュアエレメント１４５は、非接触レジストリサービス（「ＣＲＳ」）アプレット又はアプリケーション１５１を含むことができ、それは、特定のセキュリティドメインエレメントのライフサイクル状態（例えば、アクティブ化、非アクティブ化、ロック、など）を変更するために、及び特定のセキュリティドメインエレメントについての特定の出力情報１１５ｏをデバイス１００のユーザと（例えば、ユーザＩ／Ｏインターフェース１１４ａを介して）共有するために、電子デバイス１００にローカル機能を提供するように構成され得る。例えば、ＣＲＳアプリケーション１５１は、セキュアエレメント１４５上の各セキュリティドメインエレメントの現在のライフサイクル状態のリスト（例えば、リストＳＳＤ１５４ａのクレデンシャルアプレット１５３ａ及び／又はＳＳＤ１５４ｂのクレデンシャルアプレット１５３ｂの１つ、いくつか、又は全てを含み得るリスト）を保持し得るＣＲＳリスト１５１ｔを含むことができ、ＣＲＳアプリケーション１５１は、セキュアエレメント１４５の１つ以上のセキュリティドメインエレメントのライフサイクル状態を、デバイス１００のアプリケーションと（例えば、デーモンなどの任意の適切なアプリケーションタイプは、オペレーティングシステムアプリケーション１０３内でバックグラウンドプロセスとして実行され得るカード管理デーモン（「ＣＭＤ」）アプリケーション１１３ａ、及び／又はカード管理アプリケーション１１３ｂ（例えば、Ａｐｐｌｅ　Ｉｎｃ．によるＰａｓｓｂｏｏｋ（商標）又はＷａｌｌｅｔ（商標）アプリケーション）、及び／又は小売商アプリケーション１１３ｃ（例えば、小売商鍵１５７と関連付けられた小売商アプリケーション）、及び／又は識別サービス（「ＩＤＳ」）アプリケーション１１３ｄなどの、デーモンなどの任意の適切なアプリケーションタイプと、しかし必ずしもデバイス１００の対話型ユーザの制御下にある必要はない）と共有するように構成されてもよく、それは、順に、特定のライフサイクル状態情報をデバイス１００のユーザに出力情報１１５ｏとしてＩ／Ｏインターフェース１１４ａ及びユーザインターフェース（「ＵＩ」）アプリケーション（例えば、カード管理アプリケーション１１３ｂのＵＩ）を介して、提供することができ、ユーザがセキュリティドメインエレメントのライフサイクル状態を変更することを有効化する（例えば、金融トランザクションにおいて使用するために特定のクレデンシャルアプレットの商取引クレデンシャルを有効化するためなど、ＣＲＳリスト１５１ｔ及びセキュリティドメインエレメントのライフサイクル状態を更新するために）。追加で、又は代替で、ＣＲＳ１５１は、ＣＲＳ１５１に関連付けられた信頼されたサービスマネージャ（例えば、図１Ｂに示すように、商業エンティティサブシステム４００）にも既知であり得るＣＲＳアクセス鍵１５１ｋを含むことができる。ＣＲＳアクセス鍵１５１ｋは、アクセス鍵１５５ａ及び／若しくはアクセス鍵１５５ｂと同様に並びに／又は代わりに、商業エンティティサブシステム４００及び電子デバイス１００によって利用されて、商業エンティティサブシステム４００と電子デバイス１００のセキュアエレメント１４５間のセキュア送信を有効化することができる。

【００３７】

ＩＤＳアプリケーション１１３ｄは、オペレーティングシステムアプリケーション１０３及び／若しくはカード管理アプリケーション１１３ｂ内のバックグラウンドプロセスとして実行中であり得る、並びに／又はＣＭＤアプリケーション１１３ａによって提供され得る、デーモンなどの、任意の適切なアプリケーションタイプであってもよく、並びに、

任意の適切なＩＤＳサービスを介して送信され得るＩＤＳメッセージを受信し応答するためのＩＤＳマネージャとして動作することができる。それは、Ａｐｐｌｅ　Ｉｎｃ．によるｉＭｅｓｓａｇｅ（商標）、など（例えば、Ａｐｐｌｅ　Ｉｎｃ．のＦａｃｅＴｉｍｅ（商標）又はＣｏｎｔｉｎｕｉｔｙ（商標））などの、任意の適切なメッセージングサービスに類似していてもよい。それは、ホストデバイス１００のＩＤＳアプリケーション１１３ｄと、別のデバイスの同様のＩＤＳアプリケーション（例えば、クライアントデバイス１００’のＩＤＳアプリケーション）の間のメッセージの一意のエンドツーエンドの暗号化を有効化することができる。そのようなメッセージは、通信デバイスの一方又は両方の一意の識別子（例えば、ホストデバイスの一意の識別子１１９及び／又はクライアントデバイスの一意の識別子１１９’）及び／又は通信デバイスの特定のユーザの一方又は両方の一意の識別子を使用して暗号化されてもよい。そのようなメッセージは、ローカルリンク又は真のデバイスツーデバイス（例えば、ピアツーピア）通信として通信されてもよく、又は商業エンティティサブシステム４００を介して（例えば、識別管理システムコンポーネント４７０を介して）通信されてもよい。そのようなメッセージングは、構造化フォーマット（例えば、プロトコルバッファー）及び／又は非構造化フォーマットでデータを交換することを可能にする短待ち時間の解決策として有効化され得る。ＩＤＳアプリケーション１１３ｄは、ＩＤＳメッセージが受信されたときに実行されていなければ、自動的に起動され得る。ＩＤＳアプリケーション１１３ｄは、適切なユーザインターフェースを提示し、受信したＩＤＳ通信の要求されたデータを案内して、要求デバイスに返送するように動作することができる。ホストデバイスのＩＤＳアプリケーション１１３ｄは、最初の要求がクライアントデバイスから検出された場合に、カード管理アプリケーション１１３ｂのカード管理デーモンアプリケーション１１３ａを起動させるように動作することができ、ホストデバイスを低電力「スリープ」モードで動作させることができる。ＩＤＳアプリケーション１１３ｄは、追加で、又は代替的で、そのような要求に対する「タイムアウト」を管理するように動作し、クライアントデバイスからの決済の要求が、ある時間期間（例えば、そのような要求に応答するアクティブなホストデバイスのユーザの対話がないために、６０秒間）ホストデバイス上で作用しなくなると、ＩＤＳアプリケーション１１３ｄはその要求を終了する判定をするように動作することができ、ホストデバイスが「キャンセル」状態を生成してクライアントデバイスに返送することをもたらすことができ、適切なメッセージ（例えば、クライアントデバイスのユーザに「タイムアウトエラー」）を表示することができる。

図３及び図３Ａ～図３Ｈの説明

【００３８】

図３に示すように、及びより詳細にいかに記載するように、ホスト電子デバイス１００の特定の例は、ｉＰｈｏｎｅ（登録商標）などのハンドヘルド電子デバイスであってもよく、筐体１０１は、様々な入力コンポーネント１１０ａ～１１０ｉ、様々な出力コンポーネント１１２ａ～１１２ｃ、及び様々なＩ／Ｏコンポーネント１１４ａ～１１４ｄへのアクセスを許容することができ、それらを介してデバイス１００及びユーザ及び／又は周囲環境が相互にインターフェースすることができる。例えば、タッチ画面Ｉ／Ｏコンポーネント１１４ａは、ディスプレイ出力コンポーネント１１２ａ及び関連付けられたタッチ入力コンポーネント１１０ｆを含むことができ、ディスプレイ出力コンポーネント１１２ａは、視覚又はグラフィックユーザインターフェース（「ＧＵＩ」）１８０を表示するために使用されてもよく、ユーザが電子デバイス１００と対話することを可能にし得る。ＧＵＩ１８０は、現在実行中のアプリケーション（例えば、アプリケーション１０３及び／又はアプリケーション１１３及び／又はアプリケーション１４３）の様々なレイヤー、ウィンドウ、画面、テンプレート、エレメント、メニュー、及び／又は他のコンポーネントを含むことができ、それらは、ディスプレイ出力コンポーネント１１２ａのエリアの全て又はいくつかに表示され得る。例えば、図３に示すように、ＧＵＩ１８０は、ＧＵＩ１８０の１つ以上のグラフィカルエレメント又はアイコン１８２を有する第１の画面１９０を表示するように構成されてもよい。特定のアイコン１８２が選択されると、デバイス１００

は、そのアイコン１８２に関連付けられた新しいアプリケーションを開き、そのアプリケーションに関連付けられたＧＵＩ１８０の対応する画面を表示するように構成され得る。例えば、「小売商アプリケーション」テキスト表示１８１（すなわち、特定のアイコン１８３）でラベル付けされた特定のアイコン１８２が、デバイス１００のユーザによって選択されると、デバイス１００は、特定のサードパーティの小売商アプリケーションを起動するか又は他の方法でそれにアクセスすることができ、特定の方法でデバイス１００と対話するための１つ以上のツール又は機能を含み得る特定のユーザインターフェースの画面を表示することができる（ホストデバイス１００のＮＦＣコンポーネント１２０のクレデンシャル（例えば、クレデンシャルＳＳＤ１５４ａのクレデンシャル）で決済を行うためにデバイスユーザによって使用され得る、任意の適切なアプリケーション（例えば、ホストデバイス１００上のカード管理アプリケーション１１３ｂ及び／又はクライアントデバイス１００’上の小売商アプリケーション１１３’）の使用中のＧＵＩ１８０のそのようなディスプレイの具体例については、図３Ａ～図３Ｈを参照）。各アプリケーションでは、画面はディスプレイ出力コンポーネント１１２ａ上に表示されることが可能であり、様々なユーザインターフェースエレメントを含むことができる。追加で、又は代替で、各アプリケーションに対して、様々な他のタイプの非可視情報を、デバイス１００の様々な他の出力コンポーネント１１２を介してユーザに提供することができる。

【００３９】

また、図２、図３はホストデバイス１００に関して記載され得るが、図２、図３の任意の１つ以上のデバイス１００のコンポーネントの１つ、いくつか、又は全ては、クライアントデバイス１００’によって同様に提供され得ることを理解されたい。いくつかの実施形態では、ホストデバイス１００の１つ以上のコンポーネントは、クライアントデバイス１００’によって提供されなくてもよい（例えば、クライアントデバイス１００’は、その上に１つ以上のクレデンシャルがプロビジョニングされたセキュアエレメントを含むことはできないが、クライアントデバイス１００’は、その上に１つ以上のネーティブクレデンシャルがプロビジョニングされたセキュアエレメントも含むことができ、それにもかかわらずクライアントデバイス１００’は、非ネーティブクレデンシャル（例えば、ホストデバイス１００にネーティブクレデンシャル）を使用して金融トランザクションを更に容易にすることができる）。いくつかの実施形態では、クライアントデバイス１００’は、ＧＵＩを提供するように動作するユーザインターフェースコンポーネントを含まなくてもよいが、代わりにより自動化されたデバイスと見なされ得る。追加で、又は代替で、ホストデバイス１００は、ＧＵＩを提供するように動作するユーザインターフェースコンポーネントを含まなくてもよいが、代わりに、トランザクションに資金を供給するための決済クレデンシャルの使用を選択及び認証するためのオーディオ出力コンポーネント及び機械的又は他の適切なユーザ入力コンポーネントを提供することができる。

図４の説明

【００４０】

ここで図４を参照して、図４は、システム１の商業エンティティサブシステム４００の特定の実施形態に関する更なる詳細を示す。図４に示すように、商業エンティティサブシステム４００は、セキュアプラットフォームシステムであってもよく、セキュアモバイルプラットフォーム（「ＳＭＰ」）ブローカーコンポーネント４４０、ＳＭＰ信頼されたサービスマネージャ（「ＴＳＭ」）コンポーネント４５０、ＳＭＰ暗号化サービスコンポーネント４６０、（「ＩＤＭＳ」）コンポーネント４７０、不正システムコンポーネント４８０、ハードウェアセキュリティモジュール（「ＨＳＭ」）コンポーネント４９０、記憶コンポーネント４２０、及び／又は１つ以上のサーバ４１０を含むことができる。商業エンティティサブシステム４００の１つ、いくつか、又は全てのコンポーネントは、デバイス１００のプロセッサコンポーネント１０２と同じか又は類似であり得る１つ以上のプロセッサコンポーネント、デバイス１００のメモリコンポーネント１０４と同じか又は類似であり得る１つ以上のメモリコンポーネント、及び／又はデバイス１００の通信コンポーネント１０６と同じか又は類似であり得る１つ以上の通信コンポーネント、を使用して実

装されてもよい。商業エンティティサブシステム４００の１つ、いくつか、又は全てのコンポーネントは、金融機関サブシステム３５０とは区別され、独立していてもよい単一の商業エンティティ（例えば、Ａｐｐｌｅ　Ｉｎｃ．）によって管理され、所有され、少なくとも部分的に制御され、及び／又は他の方法で提供されてもよい。商業エンティティサブシステム４００のコンポーネントは、互いに並びに金融機関サブシステム３５０及び／又はホスト電子デバイス１００及び／又はクライアント電子デバイス１００’及び／又は小売商サブシステム２００と集合的に対話して、セキュリティの新しいレイヤーを提供し、及び／又はよりシームレスなユーザ体験を提供することができる。

【００４１】

商業エンティティサブシステム４００のＳＭＰブローカーコンポーネント４４０は、商業エンティティユーザアカウントを用いてユーザ認証を管理するように構成され得る。ＳＭＰブローカーコンポーネント４４０は、デバイス１００上のクレデンシャルのライフサイクル及びプロビジョニングを管理するようにも構成され得る。ＳＭＰブローカーコンポーネント４４０は、デバイス１００及び／又はデバイス１００’上のユーザインターフェースエレメント（例えば、ＧＵＩ１８０のエレメント）を制御することができる主エンドポイントであることができる。エンドユーザデバイスのオペレーティングシステム又は他のアプリケーション（例えば、アプリケーション１０３、アプリケーション１１３、及び／又はホストデバイス１００のアプリケーション１４３）は、特定のアプリケーションプログラミングインターフェース（「ＡＰＩ」）を呼び出すように構成されてもよく、ＳＭＰブローカー４４０は、それらのＡＰＩの要求を処理し、デバイス１００のユーザインターフェースを導出し得るデータで応答し、及び／又はＮＦＣコンポーネント１２０のセキュアエレメントと通信し得るアプリケーションプロトコルデータユニット（「ＡＰＤＵ」）で応答する（例えば、商業エンティティサブシステム４００と電子デバイス１００の間の通信経路６５を介して）ように構成され得る。そのようなＡＰＤＵは、システム１の信頼されたサービスマネージャ（「ＴＳＭ」）（例えば、商業エンティティサブシステム４００と金融機関サブシステム３５０の間の通信経路５５のＴＳＭ）を介して、金融機関サブシステム３５０から商業エンティティサブシステム４００によって受信され得る。商業エンティティサブシステム４００のＳＭＰ　ＴＳＭコンポーネント４５０は、金融機関サブシステム３５０からデバイス１００上でクレデンシャルプロビジョニングオペレーションを実行するために使用され得る、ＧｌｏｂａｌＰｌａｔｆｏｒｍベースのサービス又は他の適切なサービスを提供するように構成され得る。ＧｌｏｂａｌＰｌａｔｆｏｒｍ、又は任意の他の適切なセキュアチャネルプロトコルは、ＳＭＰ　ＴＳＭコンポーネント４５０が、商業エンティティサブシステム４００と金融機関サブシステム３５０の間のセキュアデータ通信のために、デバイス１００のセキュアエレメント１４５とＴＳＭの間で機密アカウントデータを適切に通信し及び／又はプロビジョニングすることを有効化することができる。

【００４２】

ＳＭＰ　ＴＳＭコンポーネント４５０は、ＨＳＭコンポーネント４９０を使用するように構成されて、その鍵を保護し、新しい鍵を生成することができる。商業エンティティサブシステム４００のＳＭＰ暗号化サービスコンポーネント４６０は、システム１の様々なコンポーネント間のユーザ認証及び／又は機密データ送信のために提供され得る鍵管理及び暗号化オペレーションを提供するように構成され得る。ＳＭＰ暗号化サービスコンポーネント４６０は、セキュア鍵記憶及び／又は不透明な暗号化オペレーションのためにＨＳＭコンポーネント４９０を利用することができる。ＳＭＰ暗号化サービスコンポーネント４６０の決済暗号化サービスは、ＩＤＭＳコンポーネント４７０と対話するように構成されて、ファイル上のクレジットカードと関連付けられた情報又は商業エンティティのユーザアカウント（例えば、Ａｐｐｌｅ　ｉＣｌｏｕｄ（商標）アカウント）に関連付けられた他のタイプの商取引クレデンシャルを取得することができる。そのような決済暗号化サービスは、メモリ内のそのユーザアカウントの商取引クレデンシャル（例えば、クレジットカード番号）を記載するクリアーテキスト（すなわち、ハッシュされていない）情報を

有し得る商業エンティティサブシステム４００の唯一のコンポーネントであるように構成され得る。ＩＤＭＳコンポーネント４７０は、識別サービス（「ＩＤＳ」）トランスポート（例えば、商業エンティティ固有のサービス（例えば、Ａｐｐｌｅ　Ｉｎｃ．によるｉＭｅｓｓａｇｅ（Ｒ））を使用して、などのホストデバイス１００とクライアントデバイス１００’の間の任意の適切な通信を有効化し、及び／又は管理するように構成され得る。例えば、特定のデバイスは、そのようなサービスに対して自動的に又は手動で登録されてもよい（例えば、商業エンティティ４００のエコシステム内の全てのデバイスは、サービスに対して自動的に登録され得る）。そのようなサービスは、メッセージをそのサービスを使用して（例えば、ホストデバイス１００のＩＤＳアプリケーション１１３ｄを使用して）送信することができる前にアクティブな登録を必要とし得るエンドツーエンドの暗号化メカニズムを提供することができる。ＩＤＭＳコンポーネント４７０及び／又は商業エンティティサブシステム４００の任意の他のサーバ若しくは一部は、所与のユーザアカウント又は他のものに関連付けられた任意の電子デバイス上にプロビジョニングされた任意のクレデンシャルの状態を識別するか又は他の方法でルックアップするように動作することができ、特定のユーザアカウント（例えば、商業エンティティサブシステム４００を有するファミリーアカウントの商業エンティティサブシステム４００は、複数のホストデバイス）に関連付けられた特定のクライアントデバイスに利用可能であり得る１つ以上の非ネーティブ決済クレデンシャルを効率的かつ有効に識別するように動作することができる。商業エンティティサブシステム４００の商業エンティティ不正システムコンポーネント４８０は、商取引クレデンシャル及び／又はユーザについて商業エンティティに知られているデータに基づいて（例えば、商業エンティティのユーザアカウント、及び／又は商業エンティティの制御下にあり得るその他の適切なデータ、及び／又は金融機関サブシステム３５０の制御下にはあり得ない任意の他の適切なデータと関連付けられたデータ（例えば、商取引クレデンシャル情報）に基づいて）、商取引クレデンシャルに関する商業エンティティ不正チェックを実行するように構成されてもよい。商業エンティティ不正システムコンポーネント４８０は、様々な要因又は閾値に基づいてクレデンシャルの商業不正スコアを判定するように構成され得る。追加で、又は代替で、商業エンティティサブシステム４００は、店舗４２０を含むことができ、それは、デバイス１００のユーザに対する様々なサービスのプロバイダ（デバイス１００／１００’によって再生されるメディアを販売／レンタルするためのｉＴｕｎｅｓ（商標）Ｓｔｏｒｅ）、１００／１００’デバイスで使用するためのアプリケーションを販売／レンタルするＡｐｐｌｅ　Ａｐｐ　Ｓｔｏｒｅ（商標）、デバイス１００／１００’からのデータを記憶し、並びに／又は複数のユーザデバイス及び／若しくは複数のユーザプロファイルを互いに関連付ける、Ａｐｐｌｅ　ｉＣｌｏｕｄ（商標）Ｓｅｒｖｉｃｅ、様々なＡｐｐｌｅ製品をオンラインで購入するためのＡｐｐｌｅ　Ｏｎｌｉｎｅ　Ｓｔｏｒｅ、など）であることができる。単なる一例として、店舗４２０は、アプリケーション１１３を管理してデバイス１００に提供する（例えば、通信経路６５を介して）ように構成されてもよく、アプリケーション１１３は、銀行アプリケーション、商業アプリケーション、電子メールアプリケーション、テキストメッセージングアプリケーション、インターネットアプリケーション、カード管理アプリケーション、又は任意の他の適切な通信アプリケーションなどの、任意の適切なアプリケーションであってもよい。任意の適切な通信プロトコル又は通信プロトコルの組み合わせが、商業エンティティサブシステム４００によって使用されて商業エンティティサブシステム４００の様々なコンポーネント間でデータを通信し（例えば、図４の少なくとも１つの通信経路４９５を介して）、及び／又はシステム１の商業エンティティサブシステム４００と他のコンポーネントの間でデータを通信することができる（例えば、図１Ａの通信経路５５を介した金融エンティティサブシステム３５０及び／又は図１Ａの通信経路６５を介したホスト電子デバイス１００及び／又は図１Ａの通信経路９５を介したクライアント電子デバイス１００’）。

図５の説明

【００４３】

図５は、非ネーティブ決済クレデンシャルを有する電子デバイスを使用して金融トランザクションを行う例示的なプロセス５００のフローチャートである。プロセス５００は、ホスト電子デバイス１００、クライアント電子デバイス１００’、小売商サブシステム２００、取得銀行サブシステム３００、商業エンティティサブシステム４００、及び金融機関サブシステム３５０によって実施されるように示されている。しかしながら、プロセス５００は、任意の他の適切なコンポーネント又はサブシステムを使用して実施され得ることが理解されるべきである。プロセス５００は、ホストデバイス１００からの決済クレデンシャルを使用しながら、クライアントデバイス１００’を介して小売商サブシステム２００との金融トランザクションをセキュアに効率的に行うためのシームレスなユーザエクスペリエンスを提供することができる。

【００４４】

プロセス５００のステップ５０２において、潜在的なトランザクションデータは、小売商サブシステム２００からクライアントデバイス１００’に通信されてもよい。例えば、（例えば、ユーザが小売商の商品又はサービスについてオンラインでショッピングしている間に）小売商アプリケーション１１３’を実行しているクライアントデバイス１００’とのユーザ対話中のある時点で、潜在的なトランザクションデータは、クライアントデバイス１００’のユーザと小売商サブシステム２００の小売商の間で行う潜在的な金融トランザクションに関連する任意の適切なデータを示すことができる、小売商サブシステム２００から又は任意の他の適切なエンティティからクライアントデバイス１００’に通信され得る。それは、（ｉ）一意の小売商識別子などの特定の小売商情報、（ｉｉ）トランザクションの決済に使用される特定の通貨（例えば、円、ポンド、ドルなど）の識別、及び／又はトランザクションのために決済される特定の通貨量の識別、及び／又は購入されるか若しくはレンタルされるか若しくは別途決済される特定の商品又はサービスの識別、及び／又は使用されるデフォルト又は最初の出荷住所の識別などの、特定のトランザクション情報、（ｉｉｉ）トランザクションのために小売商に受け入れ可能な１つ以上のタイプの決済方法を示す情報（例えば、購入に使用され得る決済カードのリスト（例えば、ＭａｓｔｅｒＣａｒｄであるがＶｉｓａではない））、ｉｖ）一意の小売商ベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのために小売商サブシステム２００によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、を含むが、これらに限定されない。そのような潜在的なトランザクションデータは、関連付けられたデータの有無に関わらず、購入する顧客の連絡先情報フィールド（例えば、電話番号、電子メールアドレス、郵送先住所）などの金融トランザクションを完了するために要求されるか、又は少なくとも使用され得る、任意の適切な数とタイプのデータフィールドを含むことができ、いくつかのフィールドはそのような潜在的なトランザクションデータの一部として取り込まれ、含められてもよく、及び／又はいくつかのフィールドはそのような潜在的なトランザクションデータの一部として取り込まれずに、プロセス５００中にオープンになって取り込みを待ってもよい。そのようなステップ５０２の潜在的トランザクションデータは、本明細書ではＰＫＰａｙｍｅｎｔＲｅｑｕｅｓｔと呼ばれ得る。あるいは、いくつかの実施形態では、ステップ５０２において、小売商サブシステム２００に関連付けられた潜在的なトランザクションデータをクライアントデバイス１００’に利用可能にするために、ユーザはクライアントデバイス１００’とアクティブに対話していなくてもよい。代わりに、一例として、クライアントデバイス１００’は、特定の製品が購入されるべきであると判定して、その特定の製品の少なくとも１つの特定の小売商から関連付けられたトランザクションデータを取得するために１つ以上の小売商と対話するように（例えば、クライアントデバイス１００’は、家電製品であってもよく、家電製品を購入しなければならない（例えば、洗濯機により多くの洗濯洗剤が必要とされていることを検出するか、又は特定の日により多くの洗剤を購入するようにユーザよって予め設定されたカレンダーイベントを検出する）と判定するように構成されることが可能であり、その製品のための最良の取引を提供する特定の商人を自動的に識別することができ、その小売商と自動的に対話してその商人から製品を購入す

るためのトランザクションデータを取得することができる）、全て自動的に、クライアントデバイス１００’のユーザによる任意のアクティブな対話なしに、構成され得る。ステップ５０２の潜在的なトランザクションデータは、クライアントデバイス１００’、又はクライアントデバイス１００’に関連する利用可能なホストデバイス１００に必要な全てのデータを含んで、潜在的なトランザクションデータに関連付けられた金融トランザクションに資金を供給するために、決済済クレデンシャルデータを小売商サブシステム２００にセキュアに生成し提供することができる。そのような潜在的なトランザクションデータは、小売商サブシステム２００によって、クライアントデバイス１００’に、ステップ５０２において任意の適切な方法で通信され得る（例えば、そのような潜在的なトランザクションデータは、小売商サブシステム２００のサーバ２１０からクライアントデバイス１００’の通信コンポーネント１０６’に、任意の適切な通信プロトコルを使用して通信経路１５を介して、又は任意の適切な通信プロトコルを使用して、端末２２０とＮＦＣコンポーネント１２０’の間の非接触近接ベース通信チャネルを介して、送信されてもよい）。

【００４５】

プロセス５００のステップ５０４において、ステップ５０２のトランザクションデータに関連付けられたトランザクションなどの金融トランザクションに潜在的に資金を供給するために、少なくとも１つの利用可能な非ネーティブ決済ソースを識別することができる。これは、ステップ５０２でトランザクションデータを受信することに応じてクライアントデバイス１００’によって自動的に行われてもよく、又はトランザクションデータの受信とは独立して定期的に行われてもよく、又はクライアントデバイス１００’のユーザによってなされた要求に応じて、任意の適切なときに行われてもよい。例えば、ステップ５０２においてクライアントデバイス１００’によって受信されているトランザクションデータに応じて、クライアントデバイス１００’は、少なくとも１つのホスト電子デバイス（例えば、ホストデバイス１００などの、セキュアエレメント上に決済クレデンシャルデータを生成するように構成され得る、任意の電子デバイス）を識別することを試みるように動作することができ、それは、ステップ５０２のトランザクションデータと関連付けられた金融トランザクションに少なくとも部分的に資金供給するために利用可能であり得る。任意の適切な技術を使用して、任意の利用可能な非ネーティブ決済ソースを識別することができる。例えば、ビーコン信号は、ビーコンを受信し得る任意のホストデバイスからの応答を要求することができるディスカバリ要求としてクライアントデバイス１００’によって送信されてもよい（例えば、そのビーコン又はあるビーコンの特定の通信プロトコルを使用して通信するように動作するクライアントデバイス１００’の特定の距離内の任意のホストデバイスは、クライアントデバイス１００’によって提示され、１つ以上のホストデバイスのスキャナーによって読み取られ得る、クイックレスポンス（「ＱＲ」）コード又は任意の他の適切なコードであってもよい）。追加で、又は代替で、クライアントデバイス１００’は、任意の適切な通信経路及びプロトコルを使用して１つ以上の特定のホストデバイスにディスカバリ要求を送信することができる（例えば、デバイス１００’の連絡先アプリケーションで識別され、及び／又はデバイス１００’のユーザによって手動で識別される１つ以上のデバイスに（例えば、電話番号又は電子メールアドレス又は任意の適切な一意的なデバイス識別子（例えば、ホストデバイス１００のデバイス識別子１１９）によって））。そのようなディスカバリ要求は、クライアントデバイス１００’を識別する情報（例えば、クライアントデバイス１００’のデバイス識別子１１９’）及び／又は潜在的な金融トランザクションに資金を供給するために（例えば、小売商によって）受け入れ可能であり得る１つ以上の特定の決済タイプを識別する情報（例えば、ステップ５０２の潜在的なトランザクションデータによって識別され得る決済タイプ）を識別する情報などの、任意の適切な情報を含んでもよく、それに応じて、応答するホストデバイスを識別する任意の適切な情報（例えば、ホストデバイス１００のデバイス識別子１１９）、及び／又はそのホストデバイスに利用可能であり得る１つ以上の決済タイプを識別する任意の適切な情報（例えば、ホストデバイス１００のＡＩＤ１５５ａａ及び／又はＡＩＤ１５５ｂａ）であり、応答のそのような決済タイプの識別は、ディスカバリ要求のタイプに一致する各タイプのみ

を含むことができるか、又はその応答ホストに利用可能な全ての決済タイプを含むことができる）及び／又は応答するホストデバイスの場所を識別する任意の適切な情報及び／又はホストデバイスの状態を識別する任意の適切な情報（例えば、動作、休止、切断、など）を識別する任意の適切な情報、などの、任意の適切な情報を要求してもよい。

【００４６】

商業エンティティサブシステム４００又は任意の他のエンティティは、ステップ５０４で、クライアントデバイス１００’によるホストデバイス１００の識別に参加することができる。例えば、上述のように、商業エンティティサブシステム４００は、ｉＣｌｏｕｄ（商標）及び／若しくはｉＭｅｓｓａｇｅ（商標）などの、クライアントデバイス１００’及び／若しくはホストデバイス１００に利用可能にされた任意の適切なサービス又は任意の他の識別サービストランスポートを管理するように動作することができ、異なるデバイス間の関連付けを行い、並びに／又は様々なデバイスの状態及び／若しくは能力を自動的に判定するように動作することができる（例えば、ファミリは、クライアントデバイス１００’及びホストデバイス１００を含む複数の他のデバイスと関連付けられ得る商業エンティティサブシステム４００とのアカウントを有することができる）。一例として、ステップ５０４は、クライアントデバイス１００’が、ディスカバリ要求をクライアントデバイス１００’のアカウントに関連付けられた全ての他のデバイスの状態について商業エンティティサブシステム４００に送信し、商業エンティティサブシステム４００が、そのようなデバイスの１つ、いくつか、又は各１つの状態を取得して（例えば、識別サービストランスポートを用いて又は他の方法で）、これらの状態の各１つをクライアントデバイス１００’と共有することを含むことができ、状態は、ホストデバイス１００の可用性及びホストデバイス１００に利用可能な少なくとも１つの決済タイプの識別を示しもよい（例えば、ホストデバイス識別子、ＡＩＤ及び各決済アプリケーションの状態（例えば、ビザ／アプリ内使用可能及びディスカバー／アプリ内使用不可）及び／又はデバイス自体の状態）。各ホストデバイスは、そのような要求及び潜在的な応答に関して独自の設定を有することができる（例えば、特定のホストデバイスは、特定のクライアントデバイスからの状態要求にのみ応答するように構成されてもよい（例えば、商業エンティティサブシステム４００の同じアカウントに関連付けられたデバイスのみ、その特定のホストデバイスの連絡先アプリケーション内の連絡先に関連付けられたデバイスのみ、など））。ステップ５０４において１つ以上の利用可能な決済ソースの識別を有効化するためのそのようなディスカバリ要求及び／又はディスカバリ応答は、クライアントデバイス１００’とホストデバイス１００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路９９を介して）直接的に（例えば、ピアツーピア）、又はクライアントデバイス１００’と商業エンティティサブシステム４００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路９５を介して）及び商業エンティティサブシステム４００とホストデバイス１００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路６５を介して）など、任意の適切な方法で通信されてもよい（例えば、識別サービストランスポート又は商業エンティティサブシステム４００の任意の他の適切な通信サービスを使用して）。

【００４７】

プロセス５００のステップ５０６において、クライアントデバイス１００’は、決済要求データを少なくとも１つの特定のホスト電子デバイス１００に通信することができる。そのような決済要求データは、資金を供給される潜在的トランザクションの１つ以上の特定の機能を識別するためにクライアントデバイス１００’によって提供され得る任意の適切な情報を含むことができる。例えば、ステップ５０２の潜在的なトランザクションデータと同様に、ステップ５０６の決済要求データは、資金を供給される潜在的な金融トランザクションに関連する任意の適切なデータを含むことができる。それは、（ｉ）ステップ５０２の潜在的なトランザクションデータの少なくとも一部を提供した特定の小売商サブシステム２００を識別することができる小売商識別子の識別などの特定の小売商情報、（ｉｉ）トランザクションの決済に使用される特定の通貨（例えば、円、ポンド、ドルなど）の識別、及び／又はトランザクションのために決済される特定の通貨量の識別、及び／又は

購入されるか若しくはレンタルされるか若しくは別途決済される特定の商品又はサービスの識別、及び／又は使用されるデフォルト又は最初の出荷住所の識別などの、特定のトランザクション情報、（ｉｉｉ）トランザクションのために小売商に受け入れ可能な１つ以上のタイプの決済方法を示す情報（例えば、購入に使用され得る決済カードのリスト（例えば、ＭａｓｔｅｒＣａｒｄであるがＶｉｓａではない））、（ｉｖ）一意の小売商ベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのために小売商サブシステム２００によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、（ｖ）一意のクライアントベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのためにクライアントデバイス１００’によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、及び／又は（ｖｉ）一意のクライアントベースの決済要求識別子（例えば、行われている決済要求との関連付けのためにクライアントデバイス１００’によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、を含むが、これらに限定されない。いくつかの実施形態では、そのような決済要求データは、目標ホストデバイス１００と通信する前に、商業エンティティサブシステム４００によって暗号化されるか、又は他の方法でフォーマット若しくは処理されてもよい。ステップ５０６の決済要求データの目標ホストデバイス１００は、ステップ５０４で任意の利用可能な決済ソースの識別に基づいて（例えば、ステップ５０４の任意の適切なディスカバリ応答に基づいて）選択されてもよく、又はステップ５０４でなされた任意の識別とは独立して選択されてもよい。ステップ５０６の決済要求データは、目標ホストデバイスが利用可能であることをクライアントデバイス１００’が知ることができる特定の決済タイプの識別子を含むことができる（例えば、ステップ５０４でクライアントデバイス１００’によって又は他の方法で得られた任意の識別データ（例えば、ホストデバイスＡＩＤデータ）に基づいて）。クライアントデバイス１００’のユーザは、ステップ５０４で１つ以上の決済ソースの識別に基づいて提供され得る潜在的な目標ホストデバイスのリストから、ステップ５０６の決済要求データのための目標ホストデバイス１００を選択することができ、又はクライアントデバイス１００’は、任意の適切な特定の目標ホストデバイスを、任意の適切な方法で識別するができる（例えば、デバイス１００’の連絡先アプリケーション内の、及び／又はデバイス１００’のユーザによって（例えば、電話番号又はＥメールアドレス又は任意の適切な一意のデバイス識別子によって）手動で識別される、デバイス）。あるいは、ステップ５０６の決済要求データの目標ホストデバイス１００は、ステップ５０４でクライアントデバイス１００’によって取得された任意の識別データに、クライアントデバイス１００’によって自動的に選択されてもよい（例えば、デバイス１００’は、任意の適切な特性に基づいて利用可能なホストデバイスの群から１つのホストデバイスを選択するようにカスタマイズされるか又は他の方法で構成されてもよい。例えば、クライアントデバイス１００’への最短距離を有するホストデバイス、又は利用可能なホストデバイスの最高の優先順位を有するホストデバイス（例えば、デバイス１００’のアプリケーションのデフォルト又はカスタマイズされた設定によって判定され得るような）、など）。そのようなステップ５０６の決済要求データは、本明細書ではＰＫＲｅｍｏｔｅＰａｙｍｅｎｔＲｅｑｕｅｓｔと呼ばれてもよく、任意の適切なデータを含むことができる。それは、（１）ステップ５０２のＰＫＰａｙｍｅｎｔＲｅｑｕｅｓｔ（例えば、ＰＫＲｅｍｏｔｅＰａｙｍｅｎｔＲｅｑｕｅｓｔ内にラップされてもよい）、（２）本明細書ではＰＫＲｅｍｏｔｅＤｅｖｉｃｅと呼ばれ得る、選択された目標ホストデバイスを識別する任意の適切なデータ（例えば、ステップ５０４のディスカバリ応答に含まれてもよい、ホストデバイス１００のホストデバイス識別子１１９、）、（３）本明細書ではＳｅｌｅｃｔｅｄＡｐｐｌｉｃａｔｉｏｎＩｄｅｎｔｉｆｉｅｒと呼ばれ得る、目標ホストデバイスの選択された又はデフォルトの特定の決済を識別する任意の適切なデータ（例えば、ステップ５０４のディスカバリ応答に含まれてもよく、クライアントデバイス１００’において自動的に又はユーザによって選択されてもよい、目標ホストデバイス１００のセキュアエレメント１４５の

ＡＩＤ１５５ａａなど）、及び／又は（４）本明細書ではＲｅｍｏｔｅＰａｙｍｅｎｔＩｄｅｎｔｉｆｉｅｒと呼ばれ得る、決済要求と関連付けられる一意の識別子を識別する任意の適切なデータ（例えば、システムのクライアント及びホストデバイスを介して決済要求を識別するために使用され得る、及びクライアントデバイス１００又はその他のものによって生成され得る、一意の値）、を含むが、これらに限定されない。そのような決済要求データは、クライアントデバイス１００’とホストデバイス１００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路９９を介して）直接的に（例えば、ピアツーピア）、又はクライアントデバイス１００’と商業エンティティサブシステム４００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路９５を介して）及び商業エンティティサブシステム４００とホストデバイス１００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路６５を介して）など、ステップ５０６において任意の適切な方法で通信されてもよい（例えば、識別サービストランスポート又は商業エンティティサブシステム４００の任意の他の適切な通信サービスを使用して）。

【００４８】

プロセス５００のステップ５０８において、ホスト決済クレデンシャルデータは、ホストデバイス１００によって少なくとも部分的に生成されてもよく、次いで、ステップ５１０において、ホスト決済クレデンシャルデータは、ホストトランザクションデータとしてホストデバイス１００によって商業エンティティサブシステム４００に通信されてもよい。例えば、ステップ５０６で決済要求データを受信したことに応じて、ホストデバイス１００は、トランザクションに資金を供給することを試みるために使用されるセキュアエレメント１４５の特定のクレデンシャルを識別するように動作することができ（例えば、ステップ５０６の決済要求データのＳｅｌｅｃｔｅｄＡｐｐｌｉｃａｔｉｏｎＩｄｅｎｔｉｆｉｅｒに基づいて）、その特定のクレデンシャルに関連付けられたホスト決済クレデンシャルデータが、ステップ５０８で生成され、次いでステップ５０６の決済要求データ（例えば、ＰＫＰａｙｍｅｎｔＲｅｑｕｅｓｔの小売商の識別情報）の少なくとも一部とともに、ステップ５１０においてホストトランザクションデータとして通信されてもよい。そのようなホスト決済クレデンシャルデータは、ホストデバイス１００の特定のセキュアエレメントクレデンシャル（例えば、ＳＳＤ１５４ａのクレデンシャル）の適切な所有権をセキュアに証明するように動作することができる任意の適切なデータを含むことができる。それは、（ｉ）トークンデータ（例えば、ＤＰＡＮ、ＤＰＡＮ有効期限、及び／又はＳＳＤ１５４ａのクレデンシャル情報１６１ａのＣＶＶ）、（ｉｉ）暗号データ（例えば、ＳＳＤ１５４ａ及び金融機関サブシステム３５０の共有秘密（例えば、鍵１５５ａ’）並びに他の任意の適切な情報（例えば、トークンデータの一部又は全部、ホストデバイス１００を識別する情報、コスト及び／又は通貨、任意の適切なカウンター値、ノンス、などの、ステップ５０２の潜在的なトランザクションデータの一部又は全部を識別する情報）を使用してセキュアエレメント１４５によって生成され得る暗号文であって、それは、共有秘密を使用して暗号データを独立して生成するために、ホストデバイス１００に利用可能にされてもよく、金融機関サブシステム３５０（例えば、ステップ５２０又はその他において）に利用可能にされてもよい）、を含むが、これらに限定されない。次いで、ステップ５１０において、ホストトランザクションデータは、ホストデバイス１００から商業エンティティサブシステム４００に通信されてもよく、そのようなホストトランザクションデータは、ステップ５０８で生成された特定のホスト決済クレデンシャルデータ及び資金を供給される潜在的な金融トランザクションに関連する任意の他の適切なデータを含むことができる（例えば、ステップ５０６の決済要求データによってホストデバイス１００に提供され得るように）。それは、（ｉ）ステップ５０２の潜在的なトランザクションデータを提供した特定の小売商サブシステム２００を識別することができる小売商識別子の識別などの特定の小売商情報、（ｉｉ）トランザクションの決済に使用される特定の通貨（例えば、円、ポンド、ドルなど）の識別、及び／又はトランザクションのために決済される特定の通貨量の識別、及び／又は購入されるか若しくはレンタルされるか若しくは別途決済される特定の商品又はサービスの識別、及び／又は使用されるデフォルト又は最初

の出荷住所の識別などの、特定のトランザクション情報、（ｉｉｉ）一意の小売商ベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのために小売商サブシステム２００によって生成された）、（ｉｖ）一意のクライアントベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのためにクライアントデバイス１００’によって生成された）、（ｖ）一意のクライアントベースの決済要求識別子（例えば、決済要求との関連付けのためにクライアントデバイス１００’によって生成された）、及び／又は（ｖｉ）一意のホストベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのためにホストデバイス１００によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、を含むが、これらに限定されない。したがって、ホストデバイス１００から商業エンティティサブシステム４００に通信されたホストトランザクションデータは、ステップ５１０において、ステップ５０２の潜在的なトランザクションデータの、及び／又はステップ５０６の決済要求データ（例えば、小売商の識別子）の一部又は全部、並びにデバイス１００の特定のクレデンシャルに基づいたデータの少なくとも２つのタイプ及び又は分割可能な部分を含み得るステップ５０８のホスト決済クレデンシャルデータ（例えば、金融機関サブシステム３５０によって受信されたときに、ともによりセキュアな金融トランザクション（例えば、暗号文検証）を有効化し得る任意の適切なトークンデータ及び任意の適切な暗号データ）を、含むことができる。

【００４９】

ホストデバイス１００は、ステップ５１０においてトランザクションデータを商業エンティティサブシステム４００に通信する前に、ホストトランザクションデータのホスト決済クレデンシャルデータの全部又は少なくとも一部（例えば、ホスト決済クレデンシャルデータのトークンデータ及び／又は暗号データ）を金融機関鍵で暗号化することができる。例えば、セキュアエレメント１４５は、金融機関サブシステム３５０にも利用可能なセキュアエレメント１４５（例えば、クレデンシャル鍵１５５ａ’）に利用可能な任意の適切なクレデンシャル鍵又はエレメントを用いて、任意の適切な方法でホストトランザクションデータの少なくとも一部を暗号化又は署名することができる。追加で、又は代替で、ホストデバイス１００は、ステップ５１０においてトランザクションデータを商業エンティティサブシステム４００に通信する前に、ホストトランザクションデータの全部又はホストトランザクションデータの少なくとも一部（例えば、ホスト決済クレデンシャルデータ）を商業エンティティ鍵で暗号化することができる（例えば、ホストトランザクションデータの任意の部分が最初に金融機関鍵で最初に暗号化されているか否かによらず）。例えば、セキュアエレメント１４５は、セキュアエレメント１４５のアクセス鍵１５５ａ、アクセス鍵１５５ｂ、ＣＲＳ１５１ｋ、及び／又はＩＳＤ鍵１５６ｋを用いてホストトランザクションデータの少なくとも一部を暗号化することができ、それは、商業エンティティサブシステム４００（例えば、ホストデバイス１００と商業エンティティサブシステム４００の間の任意の共有秘密）にもアクセス可能であり得る。追加で、又は代替で、セキュアエレメント１４５は、商業エンティティサブシステム４００にアクセス可能なＣＡＳＤ１５８ｋを用いてホストトランザクションデータの少なくとも一部に署名することができる。いくつかの実施形態では、そのような商業エンティティ鍵又はアクセス鍵は、商業エンティティサブシステム４００のスキームに関連付けられた商業エンティティ公開鍵であり、商業エンティティサブシステム４００は、関連付けられた商業エンティティ秘密鍵にアクセスすることができる。商業エンティティサブシステム４００は、そのような商業エンティティ公開鍵を金融機関サブシステム３５０に提供することができ、金融機関サブシステム３５０は、その商業エンティティ公開鍵をホストデバイス１００と共有することができる（例えば、ホストデバイス１００上のクレデンシャルデータをプロビジョニングするとき（例えば、プロセス６００のステップ６０４において））。任意の適切な金融機関鍵及び／又は任意の商業エンティティ鍵によって少なくとも部分的に暗号化及び／又は署名されているか否かにかかわらず、ホストトランザクションデータは、ホストデバイス１００によって、商業エンティティサブシステム４００に、ステップ５１０において任意の

適切な方法で、通信されてもよい（例えば、そのようなホストトランザクションデータは、ホストデバイス１００の通信コンポーネント１０６から、商業エンティティサブシステム４００のサーバ４１０に、通信経路６５を介して任意の適切な通信プロトコルを使用して送信され得る）。

【００５０】

次に、ステップ５１２において、プロセス５００は、商業エンティティサブシステム４００を含んで、ステップ５１０で受信されたホストトランザクションデータを小売商サブシステム２００との共有秘密を使用してホストトランザクションデータの少なくともホスト決済クレデンシャルデータを暗号化することによって、更にセキュリティ保護することができ、ホスト決済クレデンシャルデータは、小売商サブシステム２００以外のエンティティとのトランザクションに資金を供給するために利用されなくてもよい。例えば、ステップ５１０のホストトランザクションデータが任意の商業エンティティ鍵で暗号化されている場合、商業エンティティサブシステム４００は、ステップ５１２でそのデータを復号するように動作することができる（例えば、商業エンティティサブシステム４００のサーバ４１０はホストトランザクションデータを受信し、次いで、そのホストトランザクションデータを復号／署名削除することができる（例えば、アクセス鍵１５５ａ、アクセス鍵１５５ｂ、ＣＲＳ１５１ｋ、ＣＡＳＤ１５８ｋ、及び／又は商業エンティティサブシステム４００のＩＳＤ鍵１５６ｋを用いて））。ホストデバイス１００と商業エンティティサブシステム４００の間でホストトランザクションデータを、ホストデバイス１００と商業エンティティサブシステム４００の両方に知られている商業エンティティ鍵を使用して、暗号化／署名された形式で通信することによって、プロセス５００は、商業エンティティ鍵にアクセスを有さないエンティティによってホストトランザクションデータが傍受され使用されることを防止することができる。更に、ステップ５１２において、商業エンティティサブシステム４００は、ホストトランザクションデータの少なくとも一部を、小売商鍵（例えば、特定のトランザクションが資金を供給されている小売商サブシステム２００と関連付けられ得る小売商鍵１５７及び／又は小売商鍵１５７’）で暗号化又は他の方法で再フォーマットするように動作することができる。そのような小売商鍵は、テーブル４３０を介して商業エンティティサブシステム４００によって判定され、それにアクセス可能であり得る（例えば、ステップ５１０のホストトランザクションデータの小売商識別子に関連付けられた小売商鍵を識別することによって、それは、ステップ５０６の決済要求データによってクライアントデバイス１００’からホストデバイス１００に提供されていてもよく、それは、ステップ５０２の潜在的トランザクションデータによって小売商サブシステム２００からクライアントデバイス１００’に提供されていてもよい）。例えば、上述のように、いくつかの実施形態では、ステップ５０２で小売商サブシステム２００からクライアントデバイス１００’に通信された潜在的トランザクション要求データは、小売商サブシステム２００を示す小売商識別子を含むことができる。例えば、小売商識別子は、ステップ５０２で潜在的なトランザクションデータを受信したときに、クライアントデバイス１００’によって利用されるオンラインリソース１１３’に関連付けられてもよい。小売商識別子は、ステップ５１２において商業エンティティサブシステム４００によって受信され、利用されて、商業エンティティサブシステム４００によってアクセス可能な多くの小売商鍵のうちの特定の１つを識別することができ（例えば、商業エンティティサブシステム４００の活用テーブル４３０を介した小売商鍵１５７’）、次いで商業エンティティサブシステム４００は、するためにその識別された小売商鍵を使用して、ホストトランザクションデータの少なくとも一部を暗号化することができる（例えば、少なくともホストトランザクションデータのホスト決済クレデンシャルデータ）。そのような小売商鍵（例えば、商業エンティティサブシステム４００及び小売商サブシステム２００のみが知ることができる鍵）を用いてそのようなホスト決済クレデンシャルデータを暗号化することによって、そのようなホスト決済クレデンシャルデータを、他のエンティティによって傍受されて別の小売商とのトランザクションに資金を供給するために使用されることなく、商業エンティティサブシステム４００から小売商サブシステム２００にセキュアに通信され得る

方法で、セキュアにされ得る。

【００５１】

次に、ステップ５１４において、プロセス５００は、ステップ５１２のセキュアホストトランザクションデータをホストデバイス１００に通信する商業エンティティサブシステム４００を含むことができる。例えば、そのような小売商鍵暗号化ホスト決済クレデンシャルデータは、任意の適切な通信プロトコルを使用して、通信路６５を介して、商業エンティティサブシステム４００からホストデバイス１００へ、ステップ５１４でセキュアホストトランザクションデータの少なくとも一部として送信されてもよい。そのようなセキュアホストトランザクションデータは、資金を供給されるトランザクションに関連付けられたステップ５０２及び／又はステップ５０６の任意の適切なデータなどの、小売商鍵暗号化ホスト決済クレデンシャルデータに加えて、任意の適切なデータを含むことができる。それは、（ｉ）ステップ５０２の潜在的なトランザクションデータを提供した特定の小売商サブシステム２００を識別することができる小売商識別子の識別などの特定の小売商情報、（ｉｉ）トランザクションの決済に使用される特定の通貨（例えば、円、ポンド、ドルなど）の識別、及び／又はトランザクションのために決済される特定の通貨量の識別、及び／又は購入されるか若しくはレンタルされるか若しくは別途決済される特定の商品又はサービスの識別、及び／又は使用されるデフォルト又は最初の出荷住所の識別などの、特定のトランザクション情報、（ｉｉｉ）一意の小売商ベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのために小売商サブシステム２００によって生成された）、（ｉｖ）一意のクライアントベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのためにクライアントデバイス１００’によって生成された）、（ｖ）一意のクライアントベースの決済要求識別子（例えば、決済要求との関連付けのためにクライアントデバイス１００’によって生成された）、及び／又は（ｖｉ）一意のホストベースのトランザクション識別子（例えば、ホストデバイストランザクションデータのためにホストデバイス１００によって生成された）、を含むが、これらに限定されない。したがって、ステップ５１４で商業エンティティサブシステム４００からホストデバイス１００に通信されるセキュアホストトランザクションデータは、ステップ５０２の潜在的なトランザクションデータの一部若しくは全部、及び／又はステップ５０６の決済のデータ一部又は全部、並びにセキュアホスト決済クレデンシャルデータを含むことができる。

【００５２】

次に、プロセス５００のステップ５１６において、ホストデバイス１００は、ステップ５１４で商業エンティティサブシステム４００から通信されたセキュアなホストトランザクションデータを受信し、そのセキュアホストトランザクションデータを任意の適切な方法でクライアントデバイス１００’と共有することができる。例えば、セキュアなホストトランザクションデータは、ホストデバイス１００及び／又はクライアントデバイス１００’に一意の共有秘密又は鍵でデータの一部を暗号化又は他の方法で再フォーマットすることを含み得る任意の適切な通信プロトコル（例えば、セキュアトランスポートプロトコル（例えば、Ａｐｐｌｅ　Ｉｎｃ．のｉＭｅｓｓａｇｅ（商標））又は電子メール又は任意の他の適切な方法）を使用して、通信経路９９を介して、ホストデバイス１００とクライアントデバイス１００’の間で共有されてもよい。いくつかの実施形態では、そのようなセキュアなホストトランザクションデータは、ＮＦＣコンポーネント１２０とＮＦＣコンポーネント１２０’の間の非接触近接ベース通信を介して、ホストデバイス１００とクライアントデバイス１００’の間で通信されてもよい。あるいは、図示されていないが、そのようなセキュアなホストトランザクションデータは、商業エンティティサブシステム４００からクライアントデバイス１００’に、ホストデバイス１００及びステップ５１４を介することなく、任意の適切な方法で（例えば、任意の適切な通信プロトコルを用いて通信経路９５を介して）、直接通信されてもよく、商業エンティティサブシステム４００は、ステップ５１０のホストトランザクションデータの任意のクライアントデバイス識別子を利用して、目標クライアントデバイス１００’を識別することができる。あるいは、図示されていな

いが、そのようなセキュアなホストトランザクションデータは、商業エンティティサブシステム４００から小売商サブシステム２００に、ホストデバイス１００並びに／又はクライアントデバイス１００’及びステップ５１４及び５１６を介することなく、任意の適切な方法で（例えば、任意の適切な通信プロトコルを用いて通信経路８５を介して）、直接的に通信されてもよく、商業エンティティサブシステム４００は、ステップ５１０のホストトランザクションデータの任意の小売商識別子を利用して、目標小売商サブシステム２００を識別することができる。あるいは、図示されていないが、そのようなセキュアなホストトランザクションデータは、商業エンティティサブシステム４００から金融機関サブシステム３５０に、ホストデバイス１００並びに／又はクライアントデバイス１００’並びに／又は小売商サブシステム２００及びステップ５１４～５１８を介することなく、任意の適切な方法で（例えば、任意の適切な通信プロトコルを用いて通信経路５５を介して）、直接的に通信されてもよい。ステップ５１６でクライアントデバイス１００’によって受信され得るセキュアなホストトランザクションデータは、資金を供給されるトランザクションと関連付けられた任意の適切なデータなどの小売商鍵暗号化ホスト決済クレデンシャルデータに加えて、任意の適切なデータを含むことができる。それは、（ｉ）ステップ５０２の潜在的なトランザクションデータを提供した特定の小売商サブシステム２００を識別することができる小売商識別子の識別などの特定の小売商情報、（ｉｉ）トランザクションの決済に使用される特定の通貨（例えば、円、ポンド、ドルなど）の識別、及び／又はトランザクションのために決済される特定の通貨量の識別、及び／又は購入されるか若しくはレンタルされるか若しくは別途決済される特定の商品又はサービスの識別、及び／又は使用されるデフォルト又は最初の出荷住所の識別などの、特定のトランザクション情報、（ｉｉｉ）一意の小売商ベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのために小売商サブシステム２００によって生成された）、（ｉｖ）一意のクライアントベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのためにクライアントデバイス１００’によって生成された）、（ｖ）一意のクライアントベースの決済要求識別子（例えば、決済要求との関連付けのためにクライアントデバイス１００’によって生成された）、及び／又は（ｖｉ）一意のホストベースのトランザクション識別子（例えば、ホストデバイストランザクションデータのためにホストデバイス１００によって生成された）、を含むが、これらに限定されない。したがって、クライアントデバイス１００’と共有されたセキュアなホストトランザクションデータは、ステップ５０２の潜在的なトランザクションデータの一部又は全部、及び／又はステップ５０６の決済要求データの一部又は全部、並びにセキュアなホスト決済クレデンシャルデータを含むことができる。

【００５３】

次に、プロセス５００のステップ５１８において、クライアントデバイス１００’は、ステップ５１６で共有されたセキュアなホストトランザクションデータを使用して、セキュアなホストトランザクションデータの小売商鍵暗号化ホスト決済クレデンシャルを含み得る小売商サブシステム２００にクライアントトランザクションデータを送信することによって、小売商サブシステム２００とのトランザクションに資金を供給することができる。例えば、そのようなクライアントトランザクションデータは、任意の適切な通信プロトコルを使用して、及び／又はＮＦＣコンポーネント１２０’と小売商端末２２０の間の非接触近接ベース通信として、通信経路１５を介して、クライアントデバイス１００’の通信コンポーネント１０６’から小売商サブシステム２００のサーバ２１０に送信されてもよい。クライアントデバイス１００’によって（例えば、小売商リソース１１３’を使用して）小売商サブシステム２００に通信され得るクライアントトランザクションデータは、資金を供給されるトランザクションに関連付けられた任意の適切なデータなどの、セキュアなホストトランザクションデータの小売商鍵暗号化ホスト決済クレデンシャルデータに加えて、任意の適切なデータを含むことができる。それは、（ｉ）ステップ５０２の潜在的なトランザクションデータを提供した特定の小売商サブシステム２００を識別することができる小売商識別子の識別などの特定の小売商情報、（ｉｉ）トランザクションの決済に使用さ

れる特定の通貨（例えば、円、ポンド、ドルなど）の識別、及び／又はトランザクションのために決済される特定の通貨量の識別、及び／又は購入されるか若しくはレンタルされるか若しくは別途決済される特定の商品又はサービスの識別、及び／又は使用されるデフォルト又は最初の出荷住所の識別などの、特定のトランザクション情報、（ｉｉｉ）一意の小売商ベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのために小売商サブシステム２００によって生成された）、（ｉｖ）一意のクライアントベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのためにクライアントデバイス１００’によって生成された）、（ｖ）一意のクライアントベースの決済要求識別子（例えば、決済要求との関連付けのためにクライアントデバイス１００’によって生成された）、及び／又は（ｖｉ）一意のホストベースのトランザクション識別子（例えば、ホストデバイストランザクションデータのためにホストデバイス１００によって生成された）、を含むが、これらに限定されない。したがって、小売商サブシステム２００と共有されたクライアントトランザクションデータは、ステップ５０２の潜在的トランザクションデータの一部又は全部、及び／又はステップ５０６の決済要求データの一部又は全部、並びに少なくともステップ５１２のセキュアなホストトランザクションデータの小売商鍵暗号化ホスト決済クレデンシャルデータ、を含むことができる。セキュアなホストトランザクションデータの小売商鍵暗号化されたホスト決済クレデンシャルデータをクライアントトランザクションデータの少なくとも一部として通信することにより、プロセス５００は、そのような小売商鍵暗号化ホスト決済クレデンシャルデータの小売商サブシステム２００への通信を有効化し、小売商サブシステム２００がホストデバイス１００と通信する必要なく、金融トランザクションに資金を供給することができ、及び／又は商業エンティティサブシステム４００は、更に、ステップ５０８でホストデバイス１００によって生成されたホスト決済クレデンシャルデータが、小売商鍵（例えば、ホストデバイス１００及び／又はクライアントデバイス１００’））へのアクセスを有さない小売商エンティティのためにトランザクションに資金を供給するのに使用されることを防止することもできる。あるいは、図示されていないが、ステップ５１４のセキュアなホストトランザクションデータの少なくとも小売商鍵暗号化ホスト決済クレデンシャルデータは、クライアントデバイス１００’及び追加のステップ５１８を介することなく、任意の適切な方法で、ホストデバイス１００から小売商サブシステム２００に直接的に通信されてもよく、ホストデバイス１００は、ステップ５０６の決済要求データの任意の小売商識別子を利用して、目標小売商サブシステム２００を識別することができる。追加で、又は代替で、図示されていないが、ホストデバイス１００は、ステップ５０８のホスト決済クレデンシャルデータを、商業エンティティサブシステム４００においてではなく、ホストデバイス１００上で適切な小売商鍵で暗号化するように動作することができる（例えば、そのような小売商鍵がホストデバイス１００にアクセス可能にされている場合）。あるいは、図示されていないが、ステップ５１２のセキュアなホストトランザクションデータの少なくとも小売商鍵暗号化ホスト決済クレデンシャルデータは、ホストデバイス１００及び／又はクライアントデバイス１００’及び、したがって、追加のステップ５１６及び５１８を介することなく、任意の適切な方法で（例えば、任意の適切な通信プロトコルを用いて通信経路８５を介して）、商業エンティティサブシステム４００から小売商サブシステム２００に直接的に通信されてもよく、商業エンティティサブシステム４００は、ステップ５１０のホストトランザクションデータの任意の小売商識別子を利用して、目標小売商サブシステム２００を識別することができる。あるいは、図示されていないが、ステップ５１２のセキュアなホストトランザクションデータの少なくとも小売商鍵暗号化ホスト決済クレデンシャルデータは、ホストデバイス１００及び／又はクライアントデバイス１００’及び／又は小売商サブシステム２００及びステップ５１４～５１８を介してではなく、任意の適切な方法で（例えば、任意の適切な通信プロトコルを使用する通信パス５５を介して）、商業エンティティサブシステム４００から金融機関サブシステム３５０に直接的に通信されてもよい。他の実施形態では、ホストデバイス１００は、クライアントデバイス１００’を介するのではなく、ステップ５１６で、セキュアなホストトランザク

ションデータを直接的に小売商サブシステム２００に通信することができる。更に他の実施形態では、商業エンティティサブシステム４００は、ホストデバイス１００を介するのではなく、ステップ５１４で、セキュアなホストトランザクションデータをクライアントデバイス１００’に直接的に通信することができる。更に他の実施形態では、商業エンティティサブシステム４００は、ホストデバイス１００及び／又はクライアントデバイス１００’を介するのではなく、ステップ５１４で、セキュアなホストトランザクションデータを直接的に小売商サブシステム２００に通信することができる。

【００５４】

ステップ５１２のセキュアなホストトランザクションデータの小売商鍵暗号化ホスト決済クレデンシャルデータが小売商サブシステム２００によって受信された後、プロセス５００は、小売商鍵暗号化ホスト決済クレデンシャルデータを利用する小売商サブシステム２００を含んで、ステップ５２０で取得銀行３００及び／又は金融機関サブシステム３５０と金融トランザクションを実行することができる。例えば、小売商サブシステム２００は、小売商鍵暗号化ホスト決済クレデンシャルデータを小売商サブシステム２００にアクセス可能な小売商鍵（例えば、小売商鍵１５７及び／又は小売商鍵１５７’）で復号することができ、次いでそのホスト決済クレデンシャルデータを、取得銀行３００及び／又は金融機関サブシステム３５０に転送することができ（例えば、通信経路２５及び／又は通信経路３５を介して）、そのホスト決済クレデンシャルデータに関連付けられた資金供給アカウントが取得銀行３００及び／又は金融機関サブシステム３５０によって識別され使用されて、金融トランザクションに資金を供給することができる。次に、そのようなトランザクションがステップ５２０で実行された後、プロセス５００は、ステップ５２２で、任意の適切な確認情報を使用して、クライアントデバイス１００’に対してトランザクションの状態（例えば、トランザクションの実行又は拒否）を確認する小売商サブシステム２００を含むことができる（例えば、任意の適切な決済レシートデータ及び／又は任意の適切な不十分な資金供給メッセージデータとして）。次いで、クライアントデバイス１００’は、ステップ５２４でそのような確認されたトランザクション状態（例えば、任意の適切な決済レシートデータ及び／又は任意の適切な不十分な資金供給メッセージデータとして）をホストデバイス１００と共有するように動作することができる。トランザクションが成功した場合、確認情報は、ステップ５２２のクライアントデバイス１００’で、及び／又はステップ５２４のホストデバイス１００で、トランザクション（例えば、決済要求データの一意のＲｅｍｏｔｅＰａｙｍｅｎｔＩｄｅｎｔｉｆｉｅｒによって識別されるトランザクション）を閉じるように動作することができる。追加で、又は代替で、トランザクションが成功しなかった場合、確認情報は、トランザクションを閉じるために動作してもしなくてもよい（例えば、有効な資金供給が利用できないか又はホストデバイスが不正であると識別された場合は、トランザクションを閉じるが、無効な出荷住所が判定された場合は、開いたままにして更新を許可する）。

【００５５】

図５のプロセス５００に示されるステップは単なる例示であり、既存のステップが変更又は省略されてもよく、追加のステップが追加されてもよく、特定のステップの順序が変更されてもよいことが理解される。例えば、いくつかの実施形態では、商業エンティティサブシステム４００なしで、プロセス５００と同様のプロセスを実行することができる。代わりに、ホストデバイス１００は、小売商サブシステム２００と関連付けられた小売商鍵にアクセスし、小売商鍵暗号化ホスト決済クレデンシャルデータを導出し（例えば、ステップ５０８で、ホストデバイス１００がステップ５１２の動作を実行し得るように）、次いでトランザクションをホスト決済クレデンシャルデータでセキュアに資金を供給することを有効化するために、そのような小売商鍵暗号化ホスト決済クレデンシャルデータをクライアントデバイス１００’及び／又は小売商サブシステム２００と通信するように、動作することができる。小売商鍵暗号化ホスト決済クレデンシャルデータを小売商サブシステム２００と通信することによって、プロセス５００は、クライアントデバイス１００’と小売商サブシステム２００との間で開始される金融トランザクションが、クライアントデ

バイス１００’には非ネーティブ決済クレデンシャルによるよりはホストデバイス１００にネーティブ決済クレデンシャルによって、少なくとも部分的に資金を供給されることを有効化することができる。プロセス５００は、小売商サブシステム２００へのそのような小売商鍵暗号化ホスト決済クレデンシャルデータの通信を有効化し、小売商サブシステム２００がホストデバイス１００及び／又は商業エンティティサブシステム４００のいずれかの存在と通信するか、又はそれを認識することも必要なく、金融トランザクションに資金を供給することができ、更に、ステップ５０８でホストデバイス１００によって生成されたホスト決済クレデンシャルデータが、そのような小売商鍵へのアクセスを有さないエンティティによって使用されるのを防止することもできる。いくつかの実施形態では、ホストデバイス１００は、商業エンティティサブシステム４００と、ホストデバイス１００のユーザにシームレスかつ透過的に、通信するように（例えば、ステップ５１０～５１４において）構成され、より高いレベルのセキュリティ又は効率を有効化し得る特定のデータを共有及び／又は受信することができる。ホストデバイス１００のユーザが、ステップ５０８で決済要求データに基づいて金融トランザクションを実行するために特定のクレデンシャルを利用することを選択した後、プロセス５００の残りのステップはそのユーザに対して透過的に行われてもよい（例えば、ステップ５１０～５２４は、ホストデバイス１００との任意の更なるユーザ対話なしに行われてもよく、ホストデバイス１００のユーザに瞬間的に見える可能性がある）。プロセス５００は、ステップ５０８の後、セキュアホスト決済クレデンシャルデータが自動的及び瞬間的に小売商サブシステム２００に送信されて、金融トランザクションの状態が確認されたかのように、ホストデバイス１００のユーザに見える可能性がある。追加で、又は代替で、クライアントデバイス１００’のユーザが、ステップ５０６で決済要求データが通信される特定の決済ソースを識別した後、プロセス５００の残りのステップはそのユーザに対して透過的に行われてもよい（例えば、ステップ５０８～５２４は、クライアントデバイス１００’との任意の更なるユーザ対話なしに行われてもよく、クライアントデバイス１００’のユーザに瞬間的に見える可能性がある）。プロセス５００は、ステップ５０６の後（例えば、ホストデバイスを選択した後）、セキュアホスト決済クレデンシャルデータが自動的及び瞬間的に小売商サブシステム２００に送信されて、金融トランザクションの状態が確認されたかのように、クライアントデバイス１００’のユーザに見える可能性がある。あるいは、いくつかの実施形態では、プロセス５００は、クライアントデバイス１００’のユーザに対して完全に透過的に行われてもよい（例えば、クライアントデバイス１００’は、金融トランザクションが行われて、アクティブなクライアントデバイスユーザのクライアントデバイス１００’との対話なしに、１つ以上の利用可能な決済ソースへのそのような金融トランザクションの決済要求データを自動的に送信すべきときを、自動的に判定するように構成され得る）。

図６の説明

【００５６】

図６は、非ネーティブ決済クレデンシャルを有する電子デバイスを使用して金融トランザクションを実行するための例示的なプロセス６００のフローチャートである。プロセス６００は、ホスト電子デバイス１００、クライアント電子デバイス１００’、小売商サブシステム２００、取得銀行サブシステム３００、商業エンティティサブシステム４００、及び金融機関サブシステム３５０によって実施されるように示されている。しかしながら、プロセス６００は、任意の他の適切なコンポーネント又はサブシステムを使用して実施されてもよいことが理解されるべきである。プロセス６００は、ホストデバイス１００からの決済クレデンシャルを使用しながら、クライアントデバイス１００’を介して小売商サブシステム２００との金融トランザクションをセキュアに及び効率的に実行するためのシームレスなユーザエクスペリエンスを提供することができる。図６のプロセス６００による金融トランザクションを実行するためのシステム１の動作に関する以下の議論を容易にするために、図１～図４の概略図のシステム１の様々なコンポーネントに、及び図３～図３Ｈの画面１９０～１９０ｈの正面図に参照がなされ、それらは、そのようなトランザクション中に、ホストデバイス（ＨＤ）１００のグラフィカルユーザインターフェース（例え

ば、カード管理アプリケーション１１３ｂ又はホストデバイス１００の任意の適切な決済アプリケーションによって提供され得るＧＵＩ）を表すことができ、及び／又はクライアントデバイス（ＣＤ）１００’のグラフィカルユーザインターフェース（例えば、クライアントデバイス１００’の小売商アプリケーション１１３’若しくはクライアントデバイス１００’の任意の適切な決済アプリケーションによって提供され得るＧＵＩ）を表すことができる。記載された動作は、多種多様なグラフィカルエレメント及び視覚スキームによって達成され得る。したがって、図３～図３Ｈの実施形態は、本明細書で採用されている正確なユーザインターフェースの取り決めに限定されることを意図されない。むしろ、実施形態は、多種多様なユーザインターフェーススタイルを含むことができる。

【００５７】

プロセス６００はステップ６０２で開始することができ、ホストアクセスデータ６５２（例えば、図１Ｂのホストアクセスデータ６５２）は、商業エンティティサブシステム４００によってホストデバイス１００のセキュアエレメント上にプロビジョニングされ得る。例えば、アクセスＳＳＤ（例えば、ＳＳＤ１５４ｂ）は、ホストデバイス１００のセキュアエレメント１４５上に商業エンティティサブシステム４００のサーバ４１０からのアクセスデータ６５２としてプロビジョニングされて、ホストデバイス１００が、小売商サブシステム２００との金融トランザクションを実行することをよりセキュアに有効化することができる。上述のように、アクセスＳＳＤ１５４ｂは、商業エンティティサブシステム４００から直接的にホストデバイス１００のセキュアエレメント１４５に少なくとも部分的にプロビジョニングされてもよい（例えば、商業エンティティサブシステム４００のサーバ４１０とホストデバイス１００の通信コンポーネント１０６の間の通信経路６５を介したホストアクセスデータ６５２として、それは、次いで、通信コンポーネント１０６からセキュアエレメント１４５に渡され得る（例えば、バス１１８を介して））。経路６５を介したホストアクセスデータ６５２は、アクセスＳＳＤ１５４ｂの少なくとも一部及び全部としてホストデバイス１００のセキュアエレメント１４５上にプロビジョニングされてもよく、アクセスアプレット１５３ｂ及び／又はアクセス鍵１５５ｂを含むことができる。ステップ６０２は、ホストデバイス１００が最初に構成されたときに少なくとも部分的に実行されてもよい（例えば、ホストデバイス１００がユーザに販売される前に商業エンティティサブシステム４００によって）。代替で、又は追加で、ステップ６０２は、ＮＦＣコンポーネント１２０のセキュアエレメント１４５を初期設定するホストデバイス１００のユーザに応じて、少なくとも部分的に実行されてもよい。追加で、又は代替で、ホストアクセスデータ６５２は、セキュアエレメント１４５のＩＳＤ１５２用のＩＳＤ鍵１５６ｋを含むことができ、商業エンティティサブシステム４００とホストデバイス１００の間のセキュア送信を有効化するためのアクセス鍵１５５ｂに加えて、又はその代わりに使用されてもよい。追加で、又は代替で、ホストアクセスデータ６５２は、ホストデバイス１００のセキュアエレメント１４５のＣＲＳ１５１のＣＲＳ１５１ｋ及び／又はＣＡＳＤ１５８のＣＡＳＤ１５８ｋを含むことができ、コマーシャルエンティティサブシステム４００とホストデバイス１００の間のセキュアな送信を有効化するためのアクセス鍵１５５ｂ及び／若しくはアクセス鍵１５５ａ及び／若しくはＩＳＤ鍵１５６ｋに加えて、又はその代わりに使用されてもよい（例えば、商業エンティティサブシステム４００とホストデバイス１００の間の任意の適切な商業エンティティ鍵又は共有秘密として使用するために）。

【００５８】

ステップ６０４において、プロセス６００は、いくつかの実施形態では、商業エンティティサブシステム４００を介して、金融機関サブシステム３５０によってホストデバイス１００のセキュアエレメント上でホストクレデンシャルデータ６５４（例えば、図１Ｂのクレデンシャルデータ６５４）をプロビジョニングすることを含むことができる。例えば、そのようなホストクレデンシャルデータ６５４は、金融機関サブシステム３５０から直接的にホストデバイス１００のセキュアエレメント１４５に少なくとも部分的にプロビジョニングされてもよい（例えば、金融機関サブシステム３５０とデバイス１００との間の

図１Ｂの通信経路７５を介して、それは、通信コンポーネント１０６を介してセキュアエレメント１４５に渡され得る）。追加で、又は代替で、そのようなホストクレデンシャルデータ６５４は、商業エンティティサブシステム４００を介して金融機関サブシステム３５０からホストデバイス１００のセキュアエレメント１４５に少なくとも部分的にプロビジョニングされてもよい（例えば、金融機関サブシステム３５０と商業エンティティサブシステム４００の間の図１Ｂの通信経路５５を介して、それは、商業エンティティサブシステム４００サーバ４１０とホストデバイス１００の通信コンポーネント１０６の間の図１Ｂの通信経路６５を介したホストクレデンシャルデータ６５４としてホストデバイス１００に渡されてもよく、それは、次いで、通信コンポーネント１０６からセキュアエレメント１４５に（例えば、バス１１８を介して）渡されてもよい）。経路７５及び／又は経路６５を介したホストクレデンシャルデータ６５４は、クレデンシャルＳＳＤ１５４ａの少なくとも一部又は全部としてホストデバイス１００のセキュアエレメント１４５上にプロビジョニングされ、クレデンシャル情報１６１ａ及び／又はクレデンシャル鍵１５５ａ’及び／又は鍵１５５ａｋを有するクレデンシャルアプレット１５３ａを含むことができる。ステップ６０４は、ホストデバイス１００のユーザがホストデバイス１００上にプロビジョニングされる特定のクレデンシャルを選択するときに、少なくとも部分的に実行されてもよい。いくつかの実施形態では、ホストクレデンシャルデータ６５４はアクセス鍵１５５ａも含むことができ、商業エンティティサブシステム４００から金融機関サブシステム３５０に最初に提供されてもよく、及び／又は商業エンティティサブシステム４００によって追加されてもよい。いくつかの実施形態では、そのようなホストクレデンシャルデータ６５４は、プロビジョニングされた決済クレデンシャルのクレデンシャル情報（例えば、アプレットアプレット１５３ａのクレデンシャル情報１６１ａ）、ＡＩＤ（例えば、ＳＳＤ１５４ａにプロビジョニングされた決済クレデンシャルのデータのアプレット１５３ａのＡＩＤ１５５ａａ）、ＳＳＤ識別子、及び／又はＳＳＤカウンターの少なくとも一部として、プライマリアカウント番号を含むことができる。

【００５９】

ホストデバイス１００上にプロビジョニングされたクレデンシャルデータは、例えば、プライマリアカウント番号（「ＰＡＮ」）、カードセキュリティコード（例えば、カード認証コード（「ＣＶＶ」））、ＰＡＮ有効期限、クレデンシャルに関連付けられた名前、など、及びホストデバイス１００が適切な暗号データを生成するために動作することができる他のデータ（例えば、任意の適切な共有秘密、及び機能的出力が共有秘密によって少なくとも部分的に判定され得る任意の適切な暗号アルゴリズム又は暗号）、などのそのクレデンシャルと決済を行うのに必要な全てのデータを含むことができる。ユーザの「実際の」クレデンシャル又は実際のＰＡＮ又は資金供給ＰＡＮ（「Ｆ－ＰＡＮ」）ではなく、「仮想」クレデンシャル又は仮想ＰＡＮ又はデバイスＰＡＮ（「Ｄ－ＰＡＮ」）をホストデバイス１００上にプロビジョニングすることができる。例えば、クレデンシャルがホストデバイス１００上にプロビジョニングされると判定されると、仮想クレデンシャルを生成し、実際のクレデンシャルにリンクし、実際のクレデンシャルの代わりにホストデバイス１００上にプロビジョニングすることが、（例えば、金融機関サブシステム３５０によって、商業エンティティサブシステム４００によって、及び／又はホストデバイス１００のユーザによって）要求されてもよい。仮想クレデンシャルの実際のクレデンシャルとのそのような生成及びリンク付けは、金融機関サブシステム３５０の任意の適切なコンポーネントによって実行されてもよい。例えば、決済ネットワークサブシステム３６０（例えば、実際のクレデンシャルのブランドに関連付けられ得る特定の決済ネットワークサブシステム３６０）は、実際のクレデンシャルと仮想クレデンシャルの間の関連付けを生成し得る仮想リンクテーブル３１２を定義して記憶することができ（例えば、図１Ｂに示すように）、いつでも、仮想クレデンシャルが、小売商サブシステム２００との金融トランザクションのためにホストデバイス１００によって利用され（例えば、ホストデバイス１００にプロビジョニングされた後に）、決済ネットワークサブシステム３６０は、認可又は検証要求又は他の方法で、その仮想クレデンシャルを示す任意の受信データを検証する試

み（例えば、ステップ６４０での受信データ６９０に応じてステップ６４２において）を受信することができ、テーブル３１２によって判定された仮想クレデンシャルに関連付けられた実際のクレデンシャルに照らしてその検証試行要求の分析を実行することができる。あるいは、そのようなテーブルは、適切な発行銀行サブシステム３７０又は金融機関サブシステム３５０によってアクセス可能な他の適切なサブシステムによってアクセス可能であるか及び／又は同様に利用されてもよい。実際のクレデンシャルではなくホストデバイス１００上に仮想クレデンシャルをプロビジョニングすることによって、金融機関サブシステム３５０は、決済ネットワークサブシステム３６０をテーブル３１２を利用するためにのみ構成して、特定のトランザクション中に仮想クレデンシャルを実際のクレデンシャルにリンクすることができるので、仮想クレデンシャルが不正ユーザによって傍受された場合に生じ得る不正行為を制限するように構成され得る。

【００６０】

ステップ６０６において、プロセス６００は、小売商アプリケーション１１３又は小売商ウェブサイトなどの小売商のオンラインリソースを小売商鍵１５７と関連付けることを含むことができる。例えば、商業エンティティサブシステム４００は、小売商鍵を小売商のリソースと関連付けるために（例えば、小売商鍵１５７をホストデバイス１００のリソース１１３と、及び／又は小売商鍵１５７’をクライアントデバイス１００’のリソース１１３’と）テーブル４３０を取り込んで商業エンティティサブシステム４００と小売商サブシステム２００の間のセキュア商取引クレデンシャルデータ通信（例えば、ホストデバイス１００及び／又はクライアントデバイス１００’を介して）をその小売商リソースを用いて有効化することができる。小売商サブシステム２００及び商業エンティティサブシステム４００の両方は、そのような小売商鍵のバージョンを（例えば、図１Ｂに示すように、小売商サブシステム２００及び商業エンティティサブシステム４００のそれぞれのセキュアエレメントに）記憶することができる。いくつかの実施形態では、オンラインリソース決済プログラムに参加するために、小売商は、商業エンティティサブシステム４００の商業エンティティによって実行されるプログラムのメンバーとして登録し、及び／又は小売商証明を取得することを要求され得る。小売商はクレデンシャルなしで決済データを受け取ることができない場合がある。各クレデンシャルは、小売商をその小売商の公開鍵（例えば、公開小売商鍵１５７／１５７’）に結び付けることができる一意の商業エンティティ小売商識別子を含むことができる。小売商は複数のクレデンシャルを取得することができ、したがって複数の識別を保持することができる。そのような一意の商業エンティティ小売商識別子は、小売商サブシステム２００によってクライアントデバイス１００’に提供されてもよく（例えば、ステップ６１０において、潜在的なトランザクションデータ６６０の一部として、及び／又はクライアントデバイス１００’（例えば、小売商アプリケーション１１３’）上で実行されている小売商オンラインリソースの固有エレメントとして）、そのような商業エンティティ小売商識別子は、試行されたトランザクション中に、クライアントデバイス１００’から商業エンティティサブシステム４００にホストデバイス１００を介して提供されてもよい（例えば、決済要求データ６６６及び／又は決済要求データ６７４を介して、ステップ６２８においてホストトランザクションデータ６７８の少なくとも一部として）。いくつかの実施形態では、商業エンティティサブシステム４００は、小売商オンラインリソース（例えば、アプリケーション１１３の鍵１５７及び／又はアプリケーション１１３’の鍵１５７’）の小売商鍵を生成するか又は他の方法で割り当てて、小売商サブシステム２００にそのような小売商鍵を提供することができる（例えば、経路８５を介して）。あるいは、小売商サブシステム２００は、小売商オンラインリソース用の小売商鍵を生成するか又は他の方法で割り当てて、そのような小売商鍵を商業エンティティサブシステム４００に提供することができる（例えば、経路８５を介して）。小売商サブシステム２００又は商業エンティティサブシステム４００のいずれかが、そのような鍵の生成、交換、保管、使用、及び置換を含み得る任意の小売商鍵の管理に責任があり得る。どのように又はどこでそのような小売商鍵が生成されるか及び／又は管理されようとも、小売商サブシステム２００及び商業エンティティサブシステム４００の両方は、小売商鍵

のバージョンを記憶することができる（例えば、小売商サブシステム２００及び商業エンティティサブシステム４００のそれぞれのセキュアエレメント内に）。これは、商業エンティティサブシステム４００と小売商サブシステム２００の間の共有秘密を有効化し、それらの間でデータをセキュアに通信することができる。いくつかの実施形態では、ホストデバイス１００は、そのような小売商鍵を提供されて、ホストデバイス１００上のその鍵で決済データをセキュアに暗号化することができる。

【００６１】

ステップ６０８において、プロセス６００は、クライアントデバイス１００’によってアクセスされた小売商のリソース６５８（例えば、図１Ｂの小売商のサードパーティリソース１１３’）を含むことができる。図１Ｂに示すように、小売商のリソースアプリケーション１１３’は、商業エンティティサブシステム４００から（例えば、アプリケーションストア４２０から）クライアントデバイス１００’上にロードされてもよい。例えば、ホストデバイス１００に関して図３に示すように、クライアントデバイス１００’のユーザは、Ｉ／Ｏコンポーネント１１４ａのタッチ画面入力コンポーネント１１０ｆを使用して、ＧＵＩ１８０の特定の画面１９０の「小売商アプリケーション」アイコン１８３を選択することができ、この選択は、クライアントデバイス１００’によって、小売商のサードパーティアプリケーション１１３’と対話する能力をユーザに提供するための開始イベントとして認識され得る。代替で、又は追加で、そのような小売商のリソース６５８は、小売商サブシステム２００から直接的にクライアントデバイス１００’によってアクセスされてもよい。そのような小売商アプリケーションアイコンの選択に応じて、ＧＵＩは、クライアントデバイス１００’が、ユーザがアプリケーション１１３’と対話して購入のために小売商から商業的に入手可能なアイテムを精査することを有効化する対話型画面を提供することができる。あるいは、ステップ６０８は、クライアントデバイス１００’のインターネットアプリケーションを使用して、（例えば、小売商サーバ２１０を介して）小売商サブシステム２００から小売商のウェブページとしての小売商のリソース６５８にアクセスするクライアントデバイス１００’を含むことができ、それは、「インターネット」アイコン（例えば、図３のＧＵＩ１８０の特定の画面１９０のアイコン１８２）によっても選択可能であって、ユーザに小売商の第３の部分アプリケーションではなく小売商のウェブページと対話する能力を提供することができる。あるいは、ステップ６０８は、アクティブなユーザ入力なしでリソース６５８の任意の適切な自動アクセスを含むことができる（例えば、特定の供給が欠乏していることを検出する自律型家電クライアントデバイス１００’などの、クライアントデバイス１００’は、任意の適切なイベントの検出に応じてリソース６５８と自動的に対話するように動作することができる（例えば、洗濯洗剤の低供給の検出に応答する洗濯機クライアントデバイス１００’））。

【００６２】

次に、ステップ６１０において、クライアントデバイス１００’は、（例えば、プロセス５００のステップ５０２に関して説明したように）アクセスされた小売商リソースから潜在的なトランザクションデータ６６０を受信することができる。例えば、図１Ｂに示すように、潜在的なトランザクションデータ６６０は、クライアントデバイス１００’が小売商のリソース１１３’（例えば、小売商のサードパーティアプリケーション又はウェブサイト又は任意の他の適切なオンラインリソース（例えば、リソース６５８））と対話しているときに、小売商サブシステム２００から（例えば、小売商サーバ２１０から）クライアントデバイス１００’に提供され得る。代替で、又は追加で、潜在的なトランザクションデータ６６０の少なくとも一部は、ステップ６１０において、小売商サーバ２１０からクライアントデバイス１００’にアクティブに送信されるデータではなく、クライアントデバイス１００’にローカルであるアプリケーション１１３’を介して（例えば、アプリケーション１１３’がメモリコンポーネントに記憶されるか、又はクライアントデバイス１００’のプロセッサ１０２’によって実行されているとき）、クライアントデバイス１００’によってローカルにアクセス可能であり得る。例えば、アプリケーション１１３’がクライアントデバイス１００’に最初に記憶されている場合（例えば、ステップ６０８において小売商のリ

ソース６５８として）、潜在的なトランザクションデータ６６０の少なくとも一部は、小売商サブシステム２００によってクライアントデバイス１００’に追加の情報は何ら提供されていない、その最初に記憶されたアプリケーション１１３’によって、生成され得る。潜在的なトランザクションデータ６６０は、クライアントデバイス１００’のユーザと小売商サブシステム２００の小売商の間で行われる潜在的な金融トランザクションの任意の適切な特性を示す任意の適切なデータを含むことができる。それは、（ｉ）一意の小売商識別子（例えば、取得銀行小売商識別子及び／又は商業エンティティ小売商識別子）及び／又は使用されている特定の小売商リソース（例えば、特定の小売商アプリケーション１１３’）の識別などの、特定の小売商情報、（ｉｉ）トランザクションの決済に使用される特定の通貨（例えば、円、ポンド、ドルなど）の識別、及び／又はトランザクションのために決済される特定の通貨量の識別、及び／又は購入されるか若しくはレンタルされるか若しくは別途決済される特定の商品又はサービスの識別、及び／又は使用されるデフォルト又は最初の出荷住所の識別などの、特定のトランザクション情報、（ｉｉｉ）トランザクションのために小売商に受け入れ可能な１つ以上のタイプの決済方法を示す情報（例えば、購入に使用され得る決済カードのリスト（例えば、ＭａｓｔｅｒＣａｒｄであるがＶｉｓａではない））、ｉｖ）一意の小売商ベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのために小売商サブシステム２００によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、を含むが、これらに限定されない。そのような潜在的なトランザクションデータ６６０は、関連受けられたデータの有無にかかわらず、購入を行う顧客の連絡先情報フィールド（例えば、電話番号、電子メールアドレス、郵送先住所）などの、金融トランザクションを完了するために必要とされるか、又は少なくとも使用され得る、任意の適切な数及びタイプのデータフィールドを含むことができ、いくつかのフィールドはそのような潜在的なトランザクションデータ６６０の一部として取り込まれ、含められてもよく、及び／又はいくつかのフィールドはそのような潜在的なトランザクションデータ６６０の一部として取り込まれずに、プロセス６００中にオープンになって、取り込みを待ってもよい。ステップ６１０のそのような潜在的なトランザクションデータ６６０は、本明細書ではＰＫＰａｙｍｅｎｔＲｅｑｕｅｓｔと呼ばれ得る。あるいは、上述のように、ステップ６１０において、小売商サブシステム２００に関連付けられた潜在的なトランザクションデータ６６０をクライアントデバイス１００’に利用可能にするために、ユーザはクライアントデバイス１００’とアクティブに対話していなくてもよい。

【００６３】

潜在的トランザクションデータ６６０は、クライアントデバイス１００’に対する小売商リソースの要求を定義して、製品及び／又はサービスの購入のために決済トークンを生成することができ、例えば、小売商の決済処理能力、決済額、及び通貨コードに関する情報を含む、潜在的トランザクションに関する任意の適切な情報をカプセル化することができる。潜在的なトランザクションデータ６６０は、小売商によってサポートされ得る１つ以上の決済ネットワーク（例えば、決済ネットワーク３６０）のリストも含むことができ、クライアントデバイス１００’は、１つ以上の決済ネットワークが、クライアントデバイス１００’上に又はクライアントデバイス１００’に利用可能な任意の適切なホストデバイス上に、許可された決済クレデンシャルを有するかどうか、を判定するように構成され得る。いくつかの実施形態では、例えば、図３Ａに示すように、一旦、そのような潜在的なトランザクションデータ６６０が、クライアントデバイス１００’によってアクセスされ得ると、クライアントデバイス１００’のＧＵＩは画面１９０ａを提供することができ、ここで、小売商のリソースは、トランザクションデータ６６０を使用して、情報３０７ａを有する小売商（例えば、「小売商Ａ」）の名前、情報３０７ｂを有する製品（例えば、「製品Ｂ」）の名前、情報３０７ｃを有する価格（例えば、「価格Ｃ」）、及び／又は情報３０７ｄを有する初期出荷データ（例えば、「住所Ｄ」）などの、潜在的なトランザクションに関連付けられた任意の適切な情報を、クライアントデバイス１００’のユーザに示すことができる。小売商サブシステム２００によってクライアントデバイス１００’に提供され得

る潜在的なトランザクションデータ６６０は、そのような情報３０７ａ、３０７ｂ、３０７ｃ及び／又は３０７ｄを示すことができる。クライアントデバイス１００’のユーザはデバイス１００’及び画面１９０ａと対話して、小売商サブシステム２００によって、更新された潜在的なトランザクションデータが生成され、共有される（例えば、ステップ６２２において）ことを必要とし得るそのような情報（例えば、出荷住所、など）の特定の部分を調整することができる。図３Ａに示され以下により詳細に記載されてもいるように、画面１９０ａは、セキュア決済プロンプト３０９を含むこともできる。潜在的なトランザクションデータ６６０の少なくとも一部は、図１Ｂの通信経路１５を介して、小売商サブシステム２００からクライアントデバイス１００’に提供されてもよく、クライアントデバイス１００’の通信コンポーネント１０６’によって受信されてもよい。通信コンポーネント１０６’は、この潜在的なトランザクションデータ６６０を、プロセッサ１０２’に（例えば、クライアントデバイス１００’上のユーザインターフェースの一部として画面１９０ａに表示するために（例えば、情報３０７ａ～３０７ｄのために））及び／又はＮＦＣコンポーネント１２０’に、渡すことができる。例えば、ＮＦＣコンポーネント１２０’は、そのような潜在的なトランザクションデータ６６０を利用して、クライアントデバイス１００’と小売商サブシステム２００の間の金融トランザクションをセキュアに有効化することができる。いくつかの実施形態では、潜在的なトランザクションデータ６６０は、小売商決済要求データ及び／若しくはユニフォームリソースロケータ（「ＵＲＬ」）又は任意の他の適切な参照文字列及び／若しくはクエリ文字列と呼ばれ得る。

【００６４】

次に、プロセス６００のステップ６１２において、クライアントデバイス１００’は、ステップ６１０の潜在的なトランザクションデータ６６０に関連付けられたトランザクションなどの、金融トランザクションに潜在的に資金を供給するために、任意の適切なホスト可用性要求データ６６２（例えば、ディスカバリ要求）を任意の適切なリモートソースに送信することによって少なくとも１つの非ネーティブ決済ソース、（例えば、少なくとも１つのホストデバイスの）を識別しようと試みることができ、次いで、プロセス６００のステップ６１４において、任意の送信されたホスト可用性要求データ６６２に応じて、クライアントデバイス１００’は、任意の適切なソース（例えば、プロセス５００のステップ５０４に関して記載したような）から、任意の適切なホスト可用性応答データ６６４（例えば、任意の適切なディスカバリ応答）を受信することができる。任意の適切な技術を使用して、任意の利用可能な非ネーティブ決済ソースを識別することができる。例えば、ビーコン信号は、ビーコンを受信し得る任意のホストデバイスからの応答を要求することができるホスト可用性要求データ６６２としてクライアントデバイス１００’によって送信されてもよい（例えば、そのビーコン又はあるビーコンの特定の通信プロトコルを使用して通信するように動作することができるクライアントデバイス１００’の特定の距離内の任意のホストデバイスは、クライアントデバイス１００’によって提示され、１つ以上のホストデバイスのスキャナーによって読み取られ得る、クイックレスポンス（「ＱＲ」）コード又は任意の他の適切なコードであってもよい）。代替で、又は追加で、クライアントデバイス１００’は、任意の適切な通信経路及びプロトコルを使用して、１つ以上の特定のホストデバイスにホスト可用性要求データ６６２を送信することができる（例えば、デバイス１００’の連絡先アプリケーションにおいて識別され、及び／又はデバイス１００’のユーザによって（例えば、電話番号又は電子メールアドレス又は任意の適切な一意のデバイス識別子（例えば、ホストデバイス１００のデバイス識別子１１９）によって）手動で識別された１つ以上のデバイスに）。

【００６５】

そのようなホスト可用性要求データ６６２は、クライアントデバイス１００’を識別する情報（例えば、クライアントデバイス１００’のデバイス識別子１１９’）及び／又は潜在的な金融トランザクションに資金を供給するために（例えば、小売商によって）受け入れ可能であり得る１つ以上の特定の決済タイプを識別する情報（例えば、ステップ６１０の潜在的なトランザクションデータ６６０によって識別され得る決済タイプ）を識別する情

報などの、任意の適切な情報を含んでもよく、それに応じて、応答するホストデバイスを識別する任意の適切な情報（例えば、ホストデバイス１００のデバイス識別子１１９）、及び／又はそのホストデバイスに利用可能であり得る１つ以上の決済タイプを識別する任意の適切な情報（例えば、ホストデバイス１００のＡＩＤ１５５ａａ及び／又はＡＩＤ１５５ｂａ）であり、ホスト可用性応答データ６６４のそのような決済タイプの識別は、ホスト可用性要求データ６６２のディスカバリ要求のタイプに一致する各タイプのみを含むことができるか、又はその応答ホストに利用可能な全ての決済タイプを含むことができる）及び／又は応答するホストデバイスの場所を識別する任意の適切な情報及び／又はホストデバイスの状態を識別する任意の適切な情報（例えば、動作、休止、切断、など）を識別し得る任意の適切な情報、などの、任意の適切なホスト可用性応答データ６６４を要求してもよい。ホストデバイスによって共有されたホスト可用性応答データ６６４は、プロトコルバッファーを使用するなど、ホストディスカバリに必要な最小限の最小データ量であってもよい。商業エンティティサブシステム４００又は任意の他のエンティティは、ステップ６１２及び／又はステップ６１４において、クライアントデバイス１００’によってホストデバイス１００の識別に参加することができる。例えば、上述のように、商業エンティティサブシステム４００は、ｉＣｌｏｕｄ（商標）及び／若しくはｉＭｅｓｓａｇｅ（商標）などの、クライアントデバイス１００’及び／若しくはホストデバイス１００に利用可能にされた任意の適切なサービス又は任意の他の識別サービストランスポートを管理するように動作することができ、異なるデバイス間の関連付けを行い、並びに／又は様々なデバイスの状態及び／若しくは能力を自動的に判定するように動作することができる（例えば、ファミリは、クライアントデバイス１００’及びホストデバイス１００を含む複数の他のデバイスと関連付けられ得る商業エンティティサブシステム４００とのアカウントを有することができる）。一例として、クライアントデバイス１００’は、ホスト可用性要求データ６６２を商業エンティティサブシステム４００に送信して、クライアントデバイス１００’のアカウントに関連付けられた全ての他のデバイスの状態を要求することができ、商業エンティティサブシステム４００は、そのようなデバイスの１つ、いくつか、又は各１つの状態を取得し、それらの状態の各１つをホスト可用性応答データ６６４としてクライアントデバイス１００’と共有することによって、応答することができ、ここで、状態は、ホストデバイス１００の可用性及びホストデバイス１００に利用可能な少なくとも１つの決済タイプの識別を示すことができる。各ホストデバイスは、そのような要求及び潜在的な応答に関して独自の設定を有することができる（例えば、特定のホストデバイスは、特定のクライアントデバイスから受信されたホスト可用性要求データ６６２にのみ（例えば、商業エンティティサブシステム４００の同じアカウントに関連付けられたデバイスのみ、その特定のホストデバイスの連絡先アプリケーション内の連絡先と関連付けられたデバイスのみ、など）、応答するように構成され得る）。ステップ６１２及び６１４で１以上の利用可能な決済ソースの識別を有効化するためのそのような要求及び／又は応答は、クライアントデバイス１００’とホストデバイス１００の間で（例えば、任意の適切な通信プロトコルを使用している通信経路９９を介して）、又はクライアントデバイス１００’と商業エンティティサブシステム４００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路９５を介して）、及び商業エンティティサブシステム４００とホストデバイス１００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路６５を介して）直接的になどの、任意の適切な方法で、通信され得る。例えば、図１Ｂに示すように、ホスト可用性要求データ６６２は、クライアントデバイス１００’から、ホストデバイス１００に（例えば、任意の適切な通信プロトコルを使用して通信経路９９を介して又は商業エンティティサブシステム４００を介して（例えば、任意の適切な通信プロトコルを使用して通信経路９５及び通信経路６５を介して））、又は商業エンティティサブシステム４００に（例えば、任意の適切な通信プロトコルを使用して通信パス９５を介して）、送信されてもよく、ホスト可用性応答データ６６４は、クライアントデバイス１００’に、ホストデバイス１００から（例えば、任意の適切な通信プロトコルを使用して通信経路９９を介して又は商業エンティティサブシステム４００を介して（例えば、任意の適切な

通信プロトコルを使用して通信経路６５及び通信経路９５を介して））、又は商業エンティティサブシステム４００から（例えば、任意の適切な通信プロトコルを使用して通信経路９５を介して）、通信されてもよい。

【００６６】

ホスト可用性要求データ６１２は、潜在的なトランザクションデータ６６０の受信に応じて、又はそのようなトランザクションデータ６６０の受信とは定期的に独立して、又は、クライアントデバイス１００’のユーザが図３Ａの画面１９０ａのＧＵＩと対話することに応じてなど、任意の適切な時点でクライアントデバイス１００’のユーザによってなされた要求に応じて、クライアントデバイス１００’によって、自動的に送信されてもよい。例えば、潜在的なトランザクションデータ６６０の詳細によって小売商から購入を行うために、クライアントデバイス１００’の画面１９０ａのセキュア決済プロンプト３０９のユーザの選択に応じて、クライアントデバイス１００’は、ホスト可用性要求データ６６２を生成して送信することができる。また、図３Ｂに示すように、クライアントデバイス１００’は、図３Ａの画面１９０ａのセキュア決済プロンプト３０９の受信選択に応じて、及び任意の適切なホスト可用性応答データ６６４の受信に応じて、画面１９０ｂを提供するように構成されてもよく、それは、ユーザが、クライアントデバイス１００’と１つ以上の方法で対話して、購入を行うためにクライアントデバイス１００’が利用可能な特定の決済ソース又はクレデンシャルを選択するように促すことができる。例えば、図示のように、画面１９０ｂは、ユーザが、クライアントデバイス１００’に利用可能であり得る潜在的に複数の決済ソースの１つを選択することを有効化し得る決済ソース選択プロンプト３１１を含むことができる。決済ソース選択プロンプト３１１は、小売商によってサポートされた決済ネットワークと関連付けられるクレデンシャルを有する決済ソースのみを含むことができ（例えば、上述の潜在的なトランザクションデータ６６０によって判定されるように）、又はクライアントデバイス１００’に利用可能な全ての決済ソース（例えば、ホスト可用性応答データ６６４として受信された全てのＡＩＤに関連付けられた全てのソース）を示すことができ、更に許容可能な決済ネットワークと関連付けられるものだけをユーザによって選択可能にすることができるようにすることができる。決済ソース選択プロンプト３１１は、クライアントデバイス１００’のセキュアエレメントにネーティブな任意の適切な決済クレデンシャル（図示せず）、任意の受信されたホスト可用性応答データ６６４によって識別され得る、任意の利用可能な決済ソースの任意の適切な非ネーティブ決済クレデンシャル（例えば、プロンプト３１１の決済オプション識別子３１１ａによって示され得るホストデバイス１の決済方法Ｘ、プロンプト３１１の決済オプション識別子３１１ｂによって示され得るホストデバイス１の決済方法Ｙ、など）、及び／又はクライアントデバイス１００’によって識別され得る任意の適切な他の決済ソース（例えば、クライアントデバイス１００’のユーザが決済を要求するための任意の適切なリモートホストデバイスを手動で入力するか又は選択することを有効化するプロンプト３１１の決済オプション識別子３１１ｃ（例えば、クライアントデバイス１００’によって使用されてそのリモートホストと通信することができる、ホストデバイスの電話番号又はｅメールアドレスなどの、任意の適切な一意のホストデバイス識別子を入力することによって、又はクライアントデバイス１００’の連絡先アプリケーションにおいて識別され得るか、若しくは最後の選択されたホストデバイス又はその他のものとして識別され得る、ホストデバイスを選択することによって））、を含む、任意の適切な決済ソースを含むことができるが、これらに限定されない。いくつかの実施形態では、決済ソース選択プロンプト３１１は、クライアントデバイス１００’のユーザが特定の決済ソースの特定の決済タイプ（例えば、識別子３１１ａのホストデバイス１の決済方法（ＰＭ）Ｘ（例えば、「００９６で終わるアカウント番号を有するＡｍｅｒｉｃａｎ　Ｅｘｐｒｅｓｓ　Ｃａｒｄ」）、又は識別子３１１ｂのホストデバイス１の決済方法（ＰＭ）Ｙ（例えば、「００３５で終わるアカウント番号を有するＭａｓｔｅｒＣａｒｄ　Ｃａｒｄ」）を選択することを有効化するように動作することができ、及び／又は決済ソース選択プロンプト３１１は、ソースクライアントデバイス１００’のユーザが特定決済タイプのその決済ソースではない特定の決済ソース（例えば、ホスト

デバイス１又はホストデバイス２）を単に選択することを有効化するように単に動作することができる（例えば、クライアントデバイス１００’によって受信されたホスト可用性応答データ６６４の特定性に応じて、又はクライアントデバイス１００’に利用可能な他の適切なデータに応じて）。いくつかの実施形態では、ホスト可用性応答データ６６４は、商業エンティティサブシステム４００によって、及び／又は現在日応答であり得る特定のホストデバイス１００のクライアントデバイス１００’によって知られているキャッシュされた決済可用性データに基づくことができ（例えば、オフにされてステップ６１２のディスカバリ要求に応答しないことがあるが、適切な決済クレデンシャルを含むことがわかっている可能性があるホストデバイス１００）、ここで、プロンプト３１１の識別子（図示せず）は、そのホストデバイス及びその既知の決済クレデンシャル並びにそのようなホストデバイスが現在オフになっていることをクライアントデバイス１００’のユーザに警告する情報の識別（例えば、「ＨＤ２はＨＤ２’ｓ　ＰＭ　Ｚを使用有効化するためにオンにされなければならない」）を含むことができる。

【００６７】

次に、プロセス６００のステップ６１６において、クライアントデバイス１００’は、決済要求データ６６６を少なくとも１つの特定のホストデバイス１００に通信することができる（例えば、プロセス５００のステップ５０６に関して説明したように）。決済要求データ６６６のターゲットホストデバイス１００は、図３Ｂの決済ソース選択プロンプト３１１に対して自動的に又はユーザの選択に応じてなど、クライアントデバイス１００’によって任意の適切な方法で判定されてもよく、並びに／又はそのような判定は、潜在的なトランザクションデータ６６０及び／若しくはホスト可用性応答データ６６４などの任意の適切な情報に基づいて行われてもよい。例えば、クライアントデバイス１００’のユーザは、ホスト可用性応答データ６６４（例えば、識別子３１１ａの「ＨＤ１’ｓ　ＰＭ　Ｘ」及び識別子３１１ｂの「ＨＤ１のＰＭ　Ｙ」）を使用して１つ以上の決済ソースの識別に基づいて提供され得る、図３Ｂの決済ソース選択プロンプト３１１の潜在的なターゲットホストデバイスのリストから、ステップ６１６の決済要求データ６６６のためのターゲットホストデバイス１００を選択することができ、又はクライアントデバイス１００’は、任意の適切な方法で任意の適切な特定のターゲットホストデバイス（例えば、クライアントデバイス１００’の連絡先アプリケーション内のホストデバイス及び／又はデバイス１００’のユーザによって手動で識別される（例えば、電話番号又は電子メールアドレス又はホストデバイスの任意の適切な一意のデバイス識別子によって（例えば、図３Ｂの識別子３１１ｃのオプションを使用して））ホストデバイス）を識別することができる。単なる１つの特定の例として、図３Ｃに示すように、クライアントデバイス１００’は、図３Ｂの決済ソース選択プロンプト３１１の識別子３１１ａの「ＨＤ１’ｓ　ＰＭ　Ｘ」のユーザの選択の受信に応じて画面１９０ｃを提供するように構成され得る。図３Ｃの画面１９０ｃは、ユーザが１つ以上の方法でクライアントデバイス１００’と対話するように促して、図３Ｃの要求ホストデバイス（ＨＤ）決済プロンプト３１５のユーザの選択によってなどの、図３Ｃの決済方法識別子３１３によって示されるように、図３Ｂの決済ソース選択プロンプト３１１の選択された決済ソースに対して非ネーティブホストデバイス決済を要求することができる。あるいは、ステップ６１６の決済要求データ６６６のターゲットホストデバイス１００は、ステップ６１４でクライアントデバイス１００’によって取得された任意の識別データに応じて、クライアントデバイス１００’によって自動的に選択されてもよい（例えば、クライアントデバイス１００’は、任意の適切な特性に基づいて利用可能なホストデバイスの群から１つのホストデバイス（例えば、クライアントデバイス１００’へ最短距離を有するホストデバイス、又は利用可能なホストデバイスの最高の優先順位を有するホストデバイス（例えば、ホスト可用性応答データ６６４又は他のものと組み合わせてクライアントデバイス１００’のアプリケーションのデフォルト又はカスタマイズされた設定によって判定され得るような）、など）を選択するようにカスタマイズされるか又は他の方法で構成されてもよい。したがって、ステップ６１６の決済要求データ６６６は、クライアントデバイス１００’との任意のユーザ対話なしに、クライアントデバイス１００’によ

って自動的に生成され送信され得る（例えば、トランザクションデータ６６０及び／又は任意のホスト可用性応答データ６６４及び／又は任意のアプリケーションパラメータ（例えば、クライアントデバイス１００’上で動作する任意のアプリケーションの）に基づいて）。ステップ６１６のそのような決済要求データ６６６は、図１Ｂに示すように、クライアントデバイス１００’とホストデバイス１００の間で（例えば、任意の適切な通信プロトコルを使用している通信経路９９を介して）、又はクライアントデバイス１００’と商業エンティティサブシステム４００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路９５を介して）、及び次いで商業エンティティサブシステム４００とホストデバイス１００の間で（例えば、任意の適切な通信プロトコルを使用して通信経路６５を介して）直接的になどの、ステップ６１６の任意の適切な方法で、通信され得る。クライアントデバイス１００’は、クライアントデバイス１００’に関連付けられた様々なホストデバイスに利用可能な様々な決済タイプのローカルキャッシュを維持する（例えば、クライアントデバイス１００’にローカルなメモリで）ように動作することができ（例えば、商業エンティティサブシステム４００によって定期的に収集され、任意の適切な時間にクライアントデバイス１００’と共有され得るデータに基づいて）、決済要求がなされるべきときに、特定の専用のディスカバリ要求及び応答サイクルは必要とされない。ネーティブクレデンシャル（例えば、クライアントデバイス１００’上の）及び／又は非ネーティブクレデンシャル（例えば、１つ以上のホストデバイス１００上の）１つ以上の利用可能な決済タイプがクライアントデバイス１００’によって判定されるとき、クライアントデバイス１００’のユーザによる選択のための様々な決済ソースの中の特定の決済ソース及び／又は優先順位付けの自動選択を有効化することができる。例えば、クライアントデバイス１００’は、クライアントデバイス１００’と選択された決済ソースを含み得るホストデバイスの間の距離に基づいて、決済要求において目標とされ識別される少なくとも１つの利用可能な決済ソースの１つを自動的に選択するか又は優先順位付けするように動作することができる（例えば、クライアントデバイスに最も近い利用可能な決済ソースを有するホストデバイス（例えば、ディスカバリ応答内の距離データから、又は他の適切な通信関連データ（例えば、検出された通信信号強度ＢｌｕｅＴｏｏｔｈ（登録商標）、など）を介して判定され得るような）が、自動的に選択されてクライアントデバイスのユーザへの使い易さを容易にすることができる）。代替で、又は追加で、クライアントデバイス１００’は、小売商によってサポートされる決済ソースに基づいて決済要求において目標とされ識別される少なくとも１つの利用可能な決済ソースの１つを自動的に選択するか又は優先順位付けするように動作することができる（例えば、企業ブランドの決済クレデンシャルは、その企業とのトランザクションで使用するために優先順位を付けられ得る（例えば、ディズニーブランドのビザカードは、ディズニー小売商とのトランザクションで使用するために優先順位をつけられるか又は選択されることが可能であり、その様な優先性は小売商によって表現され、クライアントデバイス１００’に利用可能にされ得る））。

【００６８】

決済要求データ６６６は、資金を供給される潜在的トランザクションの１つ以上の特定の特徴を識別するために、クライアントデバイス１００’によって目標ホストデバイス１００に提供され得る任意の適切な情報を含むことができる。例えば、ステップ６１０の潜在的なトランザクションデータ６６０と同様に、ステップ６１６の決済要求データ６６６は、資金を供給される潜在的な金融トランザクションに関連する任意の適切なデータを含むことができる。それは、（ｉ）一意の小売商（すなわち、「小売商Ａ」）の小売商識別子及び／又は使用されている特定の小売商リソース（例えば、特定の小売商アプリケーション１１３’）の識別などの、特定の小売商情報、（ｉｉ）トランザクションの決済に使用される特定の通貨（例えば、円、ポンド、ドルなど）の識別、及び／又はトランザクションのために決済される特定の通貨量（すなわち、「価格Ｃ」）の識別、及び／又は購入されるか若しくはレンタルされるか若しくは別途決済される特定の商品又はサービス（すなわち、「製品Ｂ」）の識別、及び／又は使用されるデフォルト又は最初の出荷住所（すなわち、「出荷Ｄ」）の識別などの、特定のトランザクション情報、（ｉｉｉ）トランザクシ

ョンのために小売商に受け入れ可能な、又はクライアントデバイス１００’（すなわち、「ＨＤ１’ｓ　ＰＭ　Ｘ」）によって選択された１つ以上のタイプの決済方法を示す情報（例えば、購入に使用され得る決済カードのリスト（例えば、ＭａｓｔｅｒＣａｒｄであるがＶｉｓａではない））、ｉｖ）一意の小売商ベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのために小売商サブシステム２００によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、（ｖ）一意のクライアントベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのためにクライアントデバイス１００’によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、及び／又は（ｖｉ）一意のクライアントベースの決済要求識別子（例えば、決済要求データ６６６によって行われている決済要求との関連付けのためにクライアントデバイス１００’によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、を含むが、これらに限定されない。いくつかの実施形態では、決済要求データ６６６は、目標ホストデバイス１００と通信する前に、商業エンティティサブシステム４００によって暗号化されるか、又は他の方法でフォーマットされるか若しくは処理されてもよい。そのような決済要求データ６６６は、本明細書ではＰＫＲｅｍｏｔｅＰａｙｍｅｎｔＲｅｑｕｅｓｔと呼ばれてもよく、任意の適切なデータを含むことができる。それは、（１）ステップ６１０の潜在的トランザクションデータ６６０のＰＫＰａｙｍｅｎｔＲｅｑｕｅｓｔ（例えば、ＰＫＲｅｍｏｔｅＰａｙｍｅｎｔＲｅｑｕｅｓｔ内にラップされてもよい）、（２）本明細書ではＰＫＲｅｍｏｔｅＤｅｖｉｃｅと呼ばれ得る、選択された目標ホストデバイスを識別する任意の適切なデータ（例えば、ステップ６１４のホスト可用性応答データ６６４に含まれてもよい、ホストデバイス１００のホストデバイス識別子１１９、）、（３）本明細書ではＳｅｌｅｃｔｅｄＡｐｐｌｉｃａｔｉｏｎＩｄｅｎｔｉｆｉｅｒと呼ばれ得る、目標ホストデバイスの選択された又はデフォルトの特定の決済を識別する任意の適切なデータ（例えば、ステップ６１４のホスト可用性応答データ６６４に含まれてもよく、及び／又はクライアントデバイス１００’において自動的に又はユーザによって選択されてもよい、目標ホストデバイス１００のセキュアエレメント１４５のＡＩＤ１５５ａａなど）、及び／又は（４）本明細書ではＲｅｍｏｔｅＰａｙｍｅｎｔＩｄｅｎｔｉｆｉｅｒと呼ばれ得る、決済要求と関連付けられる一意の識別子を識別する任意の適切なデータ（例えば、システムのクライアント及びホストデバイスを介して決済要求を識別するために使用され得る、及びクライアントデバイス１００又はその他のものによって生成され得る、一意の値）、を含むが、これらに限定されない。

【００６９】

ステップ６１６でクライアントデバイス１００’から決済要求データ６６６を受信することに応じて、ターゲットホストデバイス１００は、決済要求に作用するためにホストデバイス１００のユーザに任意の適切な情報を提供するように動作可能であることができる。例えば、図３Ｄに示すように、プッシュ通知画面１９０ｄは、ホストデバイス１００のユーザにクライアント決済要求が識別子３１７とともに受信されたことを示すように動作することができる、ホストデバイス１００のＧＵＩによって提供されてもよく、通知を隠すように選択可能であり得るオプション３２１及び／又は通知に関する更なる詳細を表示するように選択可能であり得るオプション３１９を含むことができる。例えば、ユーザのより詳細なビューのオプション３１９の選択に応じて、又は画面１９０ｄの代わりに、ホストデバイス１００のＧＵＩは、ホストデバイス１００のユーザが１つ以上の適切な方法でクライアント決済要求に応答することを有効化し得る、図３Ｅの画面１９０ｅに進むことができる。図３Ｅの画面１９０ｅは、購入を行うために、ホストデバイス１００のユーザにホストデバイス１００と１つ以上の方法で対話するように指示して、ホストデバイス１００にネーティブであるか、又はデバイス１００に非ネーティブであるがプロセス６００と同様のプロセスを介してデバイス１００にアクセス可能な特定のクレデンシャルを選択することができる。図３Ｅに示すように、図３Ｃの画面１９０ｃ上でクライアントデバイ

ス１００’のユーザに識別されたのと同じ潜在的なトランザクションに関する小売商、製品、価格、及び出荷情報を、ステップ６１６の前に及び／又はステップ６１６において、ホストデバイス１００のユーザに識別させ得る識別子３０７ａ～３０７ｄに加えて、画面１９０ｅは、ユーザが、潜在的なトランザクションに資金を供給するのに使用するために、ホストデバイス１００上にプロビジョニングされ得る潜在的に複数のクレデンシャルのうちの１つ（例えば、クレデンシャルＳＳＤ１５４ａのクレデンシャル）を選択することを有効化し得るクレデンシャル選択プロンプト３２３を、含むことができる。プロンプト３２３は小売商によってサポートされる決済ネットワークに関連付けられたホストデバイス１００にネーティブなクレデンシャルのみを含むことができる（例えば、上記のように決済要求データ６６６によって判定され得るように）。図示のように、プロンプト３２３は、ホストデバイス１００の「クレデンシャルＸ」に関連付けられた第１のネーティブ決済クレデンシャルオプション３２５及びホストデバイス１００の「クレデンシャルＹ」に関連付けられた第２のネーティブ決済クレデンシャルオプション３２７を含むことができ、その各々は潜在的トランザクションの小売商サブシステム２００によって使用されるために受け入れ可能であってもよく（例えば、決済要求データ６６６の任意の適切な部分に基づいて）、及び／又は、ここで、適用可能であれば、任意の適切な技術を使用して、クライアントデバイス１００’によって選択されたクレデンシャルを識別することができる（例えば、「ＰＭ　Ｘ」がクライアントデバイス１００’によって選択され（例えば、図３Ｂの画面１９０ｂで）、決済要求データ６６６で特定的に識別され得た場合、「クレデンシャルＸ」に関連付けられた第１のネーティブ決済クレデンシャルオプション３２５の次に「*」を設けてもよい）。図３Ｆに示すように、ホストデバイス１００のＧＵＩは、図３Ｅの画面１９０ｅのクレデンシャル選択プロンプト３２３からの特定のクレデンシャル（例えば、「クレデンシャルＸ」）のホストデバイスユーザの選択の受信に応じて、画面１９０ｆを提供するように構成されてもよい。図３Ｆの画面１９０ｆは、クレデンシャル識別情報３２９を用いて、その選択された又は自動的に識別されたデフォルトクレデンシャルを識別することができ、ホストデバイス１００のユーザに１つ以上の方法でホストデバイス１００と対話するように指示して、ユーザ及びその意図が選択されたクレデンシャルを利用することを認証することができる。これは、ホストデバイス１００のセキュアエレメント、したがって購入に使用されるクレデンシャルにアクセスするために、ユーザに（例えば、認証プロンプト３３１を用いて）、個人識別番号（「ＰＩＮ」）入力を介して、又はバイオメトリックセンサーとのユーザ対話を介して、ユーザ認証を入力するように指示することを含むことができる。

【００７０】

決済要求データ６６６の異なるインスタンスは、ステップ６１６において、異なるターゲットホストデバイスに送信されてもよい（例えば、高速応答の機会を増すために、利用可能なホストデバイスの群に（例えば、子供のクライアントデバイスからその父親のホストデバイスに及びその母親のホストデバイスに））。休止しているホストデバイスが目標ホストデバイスである場合、次いで、そのホストデバイスの決済要求データ６６６は、オンラインになったときその目標ホストデバイスと共有するために待ち行列に入れられてもよく（例えば、商業エンティティサブシステム４００によって、又はクライアントデバイス１００’自体によって）、ここでそのような待ち行列は、特定の時間期間のみ有効化されている場合がある（例えば、そのような決済要求データ６６６の生成後２時間、その後そのような決済要求データは期限切れとみなされ得ず、その目標ホストデバイスに提供され得ない）。上述のように、プロンプト３１１は、特定のホストデバイスがオンラインではないか、又は特定のホストデバイスが決済要求データに応じていないことを示す通知が提供され得る、クライアントデバイス１００’への通知を含むことができ、クライアントデバイスのユーザのために、そのホストデバイスを有効化するためにステップを実行する要求を生成することができる。商業エンティティサブシステム４００は、特定のクライアントデバイスからの特定のディスカバリ要求及び／若しくは特定の決済要求を、特定のホストデバイスへ行くことからブロックするように動作することができる設定を管理するように

動作することができ、又は、特定のホストデバイスは、任意の適切な任意選択を設定してそのような要求を特定のクライアントデバイスからブロックするように動作することができる。

【００７１】

ホストデバイス１００のユーザが、ステップ６１６で受信された決済要求データ６６６に応じて潜在的なトランザクションに資金を供給する際に使用する特定の決済クレデンシャルを選択するか又は確認することの用意があってそれをできる場合、プロセス６００はステップ６２５に進み、プロセス６００は、ホストデバイス１００のユーザによる意図及び認証を受信することを含んで、潜在的なトランザクションデータ６６６に基づいて（例えば、図３Ｆの認証プロンプト３３１のユーザの選択を介して）特定の小売商、製品、価格、及び出荷先のための潜在的なトランザクションを実行するための特定のクレデンシャルを利用することができる。アクセスＳＳＤ１５４ｂは、ホストデバイス１００のアプレット１５３ｂを利用して、他のＳＳＤ１５４（例えば、クレデンシャルＳＳＤ１５４ａ）が商取引クレデンシャルデータ通信においてそのクレデンシャル情報を有効化するために使用されることを許容する前に、そのような認証が行われたかどうかを判定することができる。ステップ６２５の単なる一例として、アクセスＳＳＤ１５４ｂのアプレット１５３ｂは、ホストデバイス１００のユーザの意図及びローカル認証を判定するように構成されてもよく（例えば、図３のバイオメトリック入力コンポーネント１１０ｉなどの、デバイス１００の任意のアプリケーション（例えば、ホストデバイス１００のカード管理アプリケーション１１３ｂ）と対話するユーザによって使用され得る、１つ以上の入力コンポーネント１１０を介して）、決済トランザクションを実行するために（例えば、クレデンシャルＳＳＤ１５４ａのクレデンシャルを用いて）別の特定のＳＳＤを有効化するように構成されてもよい。いくつかの実施形態では、そのような判定の後、しかしそのような有効化の前に、ホストデバイス１００のＧＵＩは、ホストデバイス１００のユーザに、（例えば、図３Ｇのプロンプト３３３と同様のプロンプトを用いて）１つ以上の方法でホストデバイス１００と対話するように指示して、選択され認証されたクレデンシャルを使用して決済を最終的に開始することができる、別の画面（例えば、図３Ｇの画面１９０ｇと同様の）を提供するように構成され得る。

【００７２】

ホストデバイス１００のユーザは、ステップ６２５において、ステップ６１６の決済要求データ６６６（例えば、画面１９０ｃ及び１９０ｅの「小売商Ａ」及び「製品Ｂ」及び「価格Ｃ」及び「出荷Ｄ」）によって識別される潜在的なトランザクションに資金を供給するためにホストデバイス１００にネーティブの特定の決済クレデンシャルを使用するための意図及び認証を提供することができ、ステップ６２５はステップ６１６の直後に行われてもよい。しかし、あるいは、プロセス６００は、ホストデバイス１００のユーザが、任意の意図及び認証がステップ６２５で提供される前に、潜在的なトランザクションの１つ以上の特性を調整することを有効化することができる。例えば、ステップ６１６で決済要求データ６６６を受信した後、ホストデバイス１００は、トランザクションの出荷住所、トランザクションの出荷方法、及び／又はトランザクションの決済方法などの、潜在的トランザクションの任意の適切な特性を、自動的に、又はホストデバイス１００との（例えば、画面１９０ｅとの）任意の適切なユーザ対話に応じてのいずれかで、調整するように動作することができる。ステップ６１６からステップ６２５に進むのではなく、プロセス６００はステップ６１８を含むことができ、それによって、ホストデバイス１００は、決済要求データ６６６に応じてホスト応答データ６６８をクライアントデバイス１００’に返送することができる。そのようなホスト応答データ６６８は、ホストデバイス１００によって少なくとも部分的に定義され得る任意の適切な潜在的トランザクションデータを示す任意の適切なデータを含むことができる。例えば、図３Ｅの画面１９０ｅとの対話を介して、ホストデバイス１００のユーザは、第１のネーティブ決済クレデンシャルオプション３２５の「クレデンシャルＸ」（例えば、決済要求データ６６６によって識別される同じ又は異なる決済方法）を選択し得るだけでなく、潜在的なトランザクションに、「商品

Ｂ」を、クライアントデバイス１００’の画面１９０ｃ及び決済要求データ６６６によって識別され得る最初の「出荷住所Ｄ」ではなく新しい「出荷住所Ｅ」に発送させるように、選択することができる。したがって、プロセス６００がトランザクションの資金供給を有効化し得る前に、クライアントデバイス１００’及び／又は小売商サブシステム２００によって処理される必要があり得る出荷住所情報の又は決済要求データの他の適切な部分の、ホストデバイスの更新に応じて、ホストデバイス１００は、ステップ６１８において、更新された出荷情報を示すホスト応答データ６６８を生成してクライアントデバイス１００’に送信する（例えば、商業エンティティサブシステム４００を介して、又は他の方法で、プロセス６００中にホストデバイス１００クライアントデバイス１００’の間で通信される任意の他の情報と同様に）ように動作することができる。そのようなホスト応答データ６６８は、決済要求データ６６６と実質的に類似しているが、ホストデバイス１００によって識別された変更は何でも（例えば、「出荷アドレスＤ」から「出荷アドレスＥ」への変更）示すものであってもよい。次に、クライアントデバイス１００’は、ステップ６１８においてそのようなホスト応答データ６６８を受信し、そのようなホスト応答データ６６８の少なくとも一部を小売商サブシステム２００に、ステップ６２０での更新されたトランザクション要求データ６７０として通信してもよく、更新されたトランザクション要求データ６７０は、小売商サブシステム２００に対して、潜在的トランザクションデータ６６０に対する任意の１以上の所望の更新（例えば、ホストデバイス１００によって識別された「出荷住所Ｄ」から「出荷住所Ｅ」への変更、又はステップ６１０後に及び／又はステップ６１８の後であるがステップ６２０の前にクライアントデバイス１００’によってローカルに行われた任意の変更（例えば、クライアントデバイス１００’のユーザによる画面１９０ｂにおける特定の決済方法３１１ａの選択は、更新されたトランザクション要求データ６７０を生成することができる）を識別することができる。

【００７３】

そのような更新されたトランザクション要求データ６７０の受信及び処理に応じて、小売商サブシステム２００は、ステップ６２２において、任意の適切な更新された潜在的トランザクションデータ６７２を生成してクライアントデバイス１００’に送信するように動作することができ、それは、潜在的なトランザクションデータ６６０と実質的に類似しているが、クライアントデバイス１００’及び／又はホストデバイス１００によって行われた任意の更新（例えば、「出荷住所Ｄ」から「出荷住所Ｅ」への変更）及び結果として小売商サブシステム２００によって変更され得る追加の潜在的なトランザクション情報を示すことができる（例えば、価格は、潜在的トランザクションデータ６６０の「価格Ｃ」から「価格Ｃ*」に変更されてもよく、それは、「出荷住所Ｄ」から「出荷住所Ｅ」への変更に関連付けられた異なる出荷費用に起因し得る）。別の例として、クライアントデバイス１００’が決済方法オプション３１１ａを選択（例えば、要求決済プロンプト３１５を選択する前に画面１９０ｃで）した後に決済方法オプション３１１ｂを選択して、適切な更新されたトランザクション要求データ６７０を送信することに応じて、小売商サブシステム２００は、ステップ６２２において、任意の適切な更新された潜在的トランザクションデータ６７２を生成してクライアントデバイス１００’に送信するように動作することができ、それは、潜在的なトランザクションデータ６６０と実質的に類似しているが、クライアントデバイス１００’によって行われたその更新（例えば、オプション３１１ａの「決済方法Ｘ」からオプション３１１ｂの「決済方法Ｙ」）及び結果として小売商サブシステム２００によって変更され得る追加の潜在的なトランザクション情報を示すことができる（例えば、価格は、潜在的トランザクションデータ６６０の「価格Ｃ」から「価格Ｃ*」に変更されてもよく、それは、選択された異なる決済方法（例えば小売商ブランドの決済方法の選択は、小売商によってブランド化されていない決済方法の選択よりも価格の節約を実現することができる）に起因し得る）。そのような更新された潜在的トランザクションデータ６７２は、クライアントデバイス１００’によって（例えば、更新された画面１９０ｃを提供することによって）受信及び処理されてもよく、及び／又はクライアントデバイス１００’は、ステップ６２４において更新された決済要求データ６７４を生成してホストデバイ

ス１００に送信してもよい。決済要求データ６６６、ホスト応答データ６６８、及び更新された決済要求データ６７４の各１つは、そのようなデータ間で変化する特定の他の情報（例えば、出荷住所情報及び／若しくは決済方法情報及び／又は価格情報）にかかわらず、同じ一意の小売商ベースのトランザクション識別子及び／若しくは同じ一意のクライアントベースのトランザクション識別子及び／若しくは同じ一意のクライアントベースの決済要求識別子（例えば、ＲｅｍｏｔｅＰａｙｍｅｎｔＩｄｅｎｔｉｆｉｅｒ）と関連付けられてもよく、又はそれらを含んでもよい。したがって、決済方法の変更（例えば、第１の決済クレデンシャルから第２の決済クレデンシャルへの）、及び／若しくは出荷方法の変更（例えば、地上配送方法から２日間の航空配送方法へ）、及び／若しくは出荷住所の変更（第１の出荷住所から第２の出荷住所へ）、及び／若しくは任意の他の適切なデータタイプの変更などの、クライアントデバイス１００’による潜在的トランザクションデータ６６０の任意の適切な部分の任意の変更に応じて、並びに／又はストデバイス１００による決済要求データ６６６の任意の適切な部分への任意の変更に応じて、更新されたトランザクション要求は、一貫したトランザクション識別子を維持しながら、ステップ６２４でホストデバイス１００に送信され得る更新された決済要求データ６７４をもたらし得る更新された潜在的なトランザクションデータ６７２をもたらすことができる。各デバイスのユーザインターフェースの能力に応じて、トランザクション情報（例えば、発送方法、発送住所、決済方法、など）の少なくとも一部を変更するように、クライアントデバイス１００’とホストデバイス１００のいずれも動作することができないか、いずれか、又は両方が、動作することができる。任意の適切な要求／応答モデルを使用して、いずれかのデバイスによる任意の適切な変更に基づく更新要求及び応答の適切な生成を有効化することができる。例えば、更新された潜在的なトランザクションデータ６７２及び／又は更新された決済要求データ６７４は、更新を確認することができ、決済概要項目、出荷方法、決済状態、などを含む更新情報を提供することができる。例えば、更新トランザクション要求データ６７０に応じて、更新された全体及び出荷の方法、又は「無効な出荷住所」の決済状態を含む、更新された潜在的なトランザクションデータ６７２を得ることができる。デバイス間の任意の適切な基本通信プロトコル（例えば、クライアントデバイス１００’とホストデバイス１００の間の識別サービストランスポートレイヤー）は、各デバイスが、他のデバイスが更新を受信して処理した（例えば、ｉＭｅｓｓａｇｅ（商標）又は他の適切なメディアメッセージングプロトコルの「読み取りレシート」と同様に）ときを知ったことを保証するように動作し得る完了ハンドラを提供するように動作することができる。例えば、決済継続サービスが提供されて（例えば、商業エンティティサブシステム４００のＩＤＭＳコンポーネント４７０などによって）、クライアントデバイスとホストデバイスの間の決済要求及び決済応答のセキュア通信を有効化することができ、クライアントデバイスとホストデバイスの各々は、そのサービスのメッセージングトランスポート（例えば、ホストデバイス１００のＩＤＳアプリケーション１１３ｄを用いてなどのＩＤＳトランスポート）を使用することができる。Ａｐｐｌｅ　Ｉｎｃ．によるＨａｎｄｏｆｆ（商標）（例えば、デバイス間のアプリケーションデータのシームレスな共有）、又はＡｐｐｌｅ　Ｉｎｃ．によるＡｉｒＤｒｏｐ（商標）（例えば、セキュアアドホック転送プロトコル）、又はＡｐｐｌｅ　Ｉｎｃ．によるＣｏｎｔｉｎｕｉｔｙ（商標）ＳＭＳ／ＭＭＳなどの、そのようなデータを通信するための任意の適切なメカニズムを使用することができる。更に、いずれかのデバイスは、要求をキャンセルするように動作することができ（例えば、クライアントデバイス１００’は、ステップ６１２の後に及び／若しくはステップ６２４の後に送信された要求をキャンセルすることができ、並びに／又はホストデバイス１００は、ステップ６１２の後に及び／若しくはステップ６２４の後に受信された要求をキャンセルすることができる）、各デバイス（例えば、更新画面１９０ｃ及び１９０ｅ）上のデータの提示を更新するように動作することができる。特定のトランザクションに対する全ての要求／応答の共通のＲｅｍｏｔｅＰａｙｍｅｎｔＩｄｅｎｔｉｆｉｅｒを各デバイスが使用して、各デバイスが同じ特定のトランザクションに関して通信していることを確認することができる。例えば、特定のＲｅｍｏｔｅＰａｙｍｅｎｔＩｄｅｎｔｉｆｉｅ

ｒを用いて最も最近受信された決済要求は、その同じ特定のＲｅｍｏｔｅＰａｙｍｅｎｔＩｄｅｎｔｉｆｉｅｒを用いて任意の以前受信された決済要求を介してホストデバイスによって使用されてもよい。

【００７４】

次に、特定の決済要求データ（例えば、ステップ６１６における決済要求データ６６６又はステップ６２４における更新された決済要求データ６７４）を受信することに応じて、特定の決済クレデンシャルに対してステップ６２５において意図及び認証が受信されると、プロセス６００のステップ６２６～６２８は、ホストデバイス１００が商業エンティティサブシステム４００によって使用されるホストトランザクションデータ６７８を生成、暗号化及び送信することを含むことができる（例えば、プロセス５００のステップ５０８及び５１０に関して記載したように）。ホストデバイス１００のセキュアエレメント１４５上のクレデンシャルＳＳＤ１５４ａのクレデンシャルが、金融トランザクションで使用するために選択され、認証され、及び／又は使用有効化される（例えば、ステップ６２５）と、ホストデバイス１００のセキュアエレメント１４５（例えば、ＮＦＣコンポーネント１２０のプロセッサモジュール１４２）は、商業エンティティサブシステム４００によって使用するためにその選択されたクレデンシャルの特定のクレデンシャルデータを生成し、暗号化することができる。例えば、クレデンシャルＳＳＤ１５４ａのホスト決済クレデンシャルデータ６７５（例えば、トークンデータ及び暗号データ（例えば、プロセス５００のステップ５０８に関して上述したような）などの、ＳＳＤ１５４ａの決済カードデータ（例えば、選択された「クレデンシャルＸ」に関連付けられ得る））が生成され及び／又はホスト決済クレデンシャルデータ６７６としてステップ６２６においてクレデンシャル鍵１５５ａ’で少なくとも部分的に暗号化されて、少なくともトークンデータ及び暗号データを含むことができ、そのような暗号化されたホスト決済クレデンシャルデータ６７６は、ホスト決済クレデンシャルデータ６７５にアクセスするためにそのクレデンシャル鍵１５５ａ’（例えば、金融機関サブシステム３５０）へのアクセスを有するエンティティによってのみ復号され得る。そのホスト決済クレデンシャルデータ６７５は、例えば、クレジットカード番号などのクレデンシャルを用いて決済を行うために必要な全てのデータ、例えば、プライマリアカウント番号（例えば、実際のＦ－ＰＡＮ又は仮想Ｄ－－ＰＡＮ）、カードセキュリティコード（例えば、カード検証コード（「ＣＶＶ」））、有効期限、クレデンシャル鍵に関連付けられた名前、関連付けられた暗号データ（例えば、セキュアエレメント１４５と金融機関サブシステム３５０の間の共有秘密を使用して生成された暗号及び任意の他の適切な情報）、などを含むことができる。いくつかの実施形態では、ステップ６２６で、クレデンシャルＳＳＤ１５４ａのホスト決済クレデンシャルデータ６７５の一部又は全てが、暗号化ホスト決済クレデンシャルデータ６７６としてクレデンシャル鍵１５５ａ’で暗号化されると、その暗号化されたホスト決済クレデンシャルデータ６７６は、単独で、又は適用可能な決済要求データ６６６／６７４（例えば、小売商の識別、価格額の識別、通貨及び／若しくは出荷及び／若しくは製品の識別、及び／若しくは一意の小売商ベースのトランザクション識別子及び／若しくは一意のクライアントベースのトランザクション識別子及び／若しくは一意のクライアントベースの決済要求など、を含み得る潜在的トランザクションデータ６６０／６７２の一部又は全部）の全てではないにしても少なくとも第１の部分とともにのいずれかで、及び／又は任意の他の適切な情報（例えば、ホストデバイス１００自体を識別する任意の情報（例えば、ホストデバイス識別子１１９）、任意の特定のホストデバイスベースのトランザクション識別子、など）は、ステップ６２７で、暗号化されたホスト決済データ６７７として、アクセス情報（例えば、ＳＳＤ１５４ａのアクセス鍵１５５ａ、アクセスＳＳＤ１５４ｂのアクセス鍵１５５ｂ、ＩＳＤ鍵１５６ｋ、及び／又はＣＲＳ１５１ｋ及び／又はＣＡＳＤ１５８ｋによって署名された）によって暗号化され得る。例えば、ホストデバイス１００のセキュアエレメント１４５（例えば、ＮＦＣコンポーネント１２０のプロセッサモジュール１４２）は、アクセス情報を使用して、データ６６０／６６６／６７２／６７４からの小売商の識別（例えば、アプリケーション１１３’などの、購入に使用される小売商又はそのリソースの識

別）だけでなく、データ６６０／６６６／６７２／６７４からの購入及び／又は通貨コードの識別、並びに暗号化されたホスト決済データ６７７へＳＳＤ１５４ａの暗号化されたホスト決済クレデンシャルデータ６７５（例えば、暗号化されたホスト決済クレデンシャルデータ６７６）を、暗号化することができる。いくつかの実施形態では、クレデンシャルＳＳＤ１５４ａのホスト決済クレデンシャルデータ６７５（例えば、トークンデータ及び暗号データ（例えば、プロセス５００のステップ５０８に関して上述したような）などの、ＳＳＤ１５４ａの決済カードデータ））が生成され得るが商業エンティティ鍵又はアクセス鍵で（例えば、ステップ６２７でデータ６７７として）暗号化される前に、クレデンシャル鍵で（例えば、ステップ６２６でデータ６７６として）暗号化され得ず、代わりに、そのようなホスト決済クレデンシャルデータ６７５は商業エンティティ鍵又はアクセス鍵で（例えば、ステップ６２７でデータ６７７として）暗号化されてもよく、それによって、そのような実施形態では、データ６７６への任意の将来の参照は、任意のクレデンシャル鍵で暗号化されていないデータ６７５への参照であってもよい。いくつかの実施形態では、そのような商業エンティティ鍵又はアクセス鍵は、商業エンティティサブシステム４００のスキームに関連付けられた商業エンティティ公開鍵であり、商業エンティティサブシステム４００は、関連付けられた商業エンティティ秘密鍵にアクセスすることができる。商業エンティティサブシステム４００は、そのような商業エンティティ公開鍵を金融機関サブシステム３５０に提供することができ、金融機関サブシステム３５０は、その商業エンティティ公開鍵をホストデバイス１００と共有することができる（例えば、ホストデバイス１００上にクレデンシャルデータをプロビジョニングするとき（例えば、プロセス６００のステップ６５４で））。

【００７５】

次に、決済要求データ６６６／６７４の少なくともいくつか（例えば、小売商の識別、価格額の識別、通貨の識別、一意の小売商ベースのトランザクション識別子、製品／サービスの識別、など）などの任意の追加情報とともに、暗号化されたホスト決済データ６７７、及び／又は任意の他の適切な情報（例えば、ホストデバイス１００自体を識別する任意の情報、一意のホストデバイスベースのトランザクション識別子、など）が、ホストトランザクションデータ６７８として、ステップ６２８においてホストデバイス１００から商業エンティティサブシステム４００に一緒に送信されてもよい（例えば、プロセス５００のステップ５１０に関して記載したように）。したがって、ホストトランザクションデータ６７８の少なくとも一部（例えば、暗号化されたホスト決済データ６７７）は、ホストトランザクションデータ６７８の暗号化されたホスト決済データ６７７を生成した暗号化（例えば、アクセス鍵１５５ａ、アクセス鍵１５５ｂ、ＩＳＤ鍵１５６ｋ、ＣＲＳ１５１ｋ、及び／又はＣＡＳＤ１５８ｋ）に使用されたそのアクセス情報へのアクセスを有するエンティティ（例えば、商業エンティティサブシステム４００）によってのみ復号され得る。そのようなホストトランザクションデータ６７８は、ステップ６２６～６２８で生成され、次いで、ステップ６２８で（例えば、ＮＦＣコンポーネント１２０のセキュアエレメント１４５から、通信コンポーネント１０６及び通信パス６５を介して）商業エンティティサブシステム４００に送信され得る。ステップ６２６、６２７及び６２８は、ホストトランザクションデータ６７８の一部としてホストデバイス１００のセキュアエレメント１４５から生成され、送信されたクレデンシャルデータが、ホストデバイス１００の別の部分によって復号され得ない方法で最初に暗号化されていることを保証することができる（例えば、プロセッサ１０２によって）。すなわち、ホストトランザクションデータ６７８のホスト決済クレデンシャルデータ６７５は、そのセキュアエレメントの外部のホストデバイス１００の任意の部分に公開され得ないか、又はそれによってアクセスし得ないクレデンシャル鍵１５５ａ’を用いて暗号化ホスト決済クレデンシャルデータ６７６として暗号化されてもよい。更に、ホストトランザクションデータ６７８のそのような暗号化されたホスト決済クレデンシャルデータ６７６は、そのセキュアエレメントの外部のホストデバイス１００の任意の部分に公開され得ないか、又はそれによってアクセスし得ないアクセス鍵（例えば、アクセス鍵１５５ａ、１５５ｂ、１５６ｋ、１５１ｋ、及び／又は１

５８ｋ（例えば、本明細書では、「アクセス情報」と呼ばれる））を用いて暗号化ホスト決済クレデンシャルデータ６７７として暗号化されてもよい。

【００７６】

次に、ステップ６３０において、プロセス６００は、ホストトランザクションデータ６７８の少なくとも一部を受信し復号する商業エンティティサブシステム４００を含むことができる。例えば、商業エンティティサブシステム４００は、ホストトランザクションデータ６７８を受信してもよく、次いで、エンティティサブシステム４００で入手可能なアクセス情報（例えば、１５５ａ、１５５ｂ、１５６ｋ、１５１ｋ、及び／又は１５８ｋ）を使用して、ホストトランザクションデータ６７８の暗号化ホスト決済データ６７７を復号することができる。コマーシャルエンティティサブシステム４００は、ステップ６２６において、ホスト決済クレデンシャルデータ６７５がホストデバイス１００のセキュアエレメント１４５によって暗号化ホスト決済クレデンシャルデータ６７６として暗号化され得るクレデンシャル鍵１５５ａ’へのアクセスを有していない可能性があるので、これは、商業エンティティサブシステム４００が小売商の暗号化されていない識別を判定する（例えば、復号されたホスト決済データ６７７から）ことを有効化することができ、一方暗号化された状態でホスト決済クレデンシャルデータ６７５も維持する（例えば、暗号化されたホスト決済クレデンシャルデータ６７６として）。追加で、又は代替で、小売商は、暗号化されたホスト決済データ６７７と共にホストトランザクションデータ６７８に含まれ得る潜在的な追加のデータによって識別されてもよい。ホストトランザクションデータ６７８は、ホストデバイス１００又は少なくともそのセキュアエレメントを識別する情報を含むことができ、ホストトランザクションデータ６７８が商業エンティティサブシステム４００によって受信されたとき、商業サブシステム４００は、どのアクセス情報（例えば、アクセス情報１５５ａ、１５５ｂ、１５６ｋ、１５１ｋ、及び／又は１５８ｋのうちのどれか）をステップ６３０で使用するべきかを知ることができる。例えば、商業エンティティサブシステム４００は、複数のアクセス鍵１５５ａ／１５５ｂ及び／又は複数のＩＳＤ鍵１５６ｋにアクセスすることができ、その各１つは、特定のホストデバイス１００又は特定のセキュアエレメントに特定のものであり得る。

【００７７】

次に、ステップ６３１において、プロセス６００は、決済要求データ６６６／６７４によって、したがってホストタランザクションデータ６７８によって識別され得る小売商に関連付けられた小売商鍵（例えば、小売商鍵１５７’）を識別し、次いでその小売商鍵を使用してホストトランザクションデータ６７８の少なくとも一部を再暗号化する、商業エンティティサブシステム４００を含むことができる。すなわち、ステップ６３０で適切なアクセス情報を使用して、ホストトランザクションデータ６７８の少なくとも一部を復号した後（例えば、暗号化ホスト決済データ６７７で暗号化され得る暗号化ホスト決済クレデンシャルデータ６７６及び任意の他の情報を実現するために暗号化ホスト決済データ６７７を復号した後）、商業エンティティサブシステム４００は、次いで、ステップ６３１において、ホストトランザクションデータ６７８で識別された小売商情報に関連付けられ得る適切な小売商鍵を用いて、ホストトランザクションデータ６７８（例えば、暗号化ホスト決済クレデンシャルデータ６７６のトークンデータ及び／又は暗号データ）の少なくとも一部を再暗号化することができる。例えば、そのような小売商鍵（例えば、小売商鍵１５７’）は、ホストトランザクションデータ６７８で識別される商業エンティティの小売商情報を、図１Ｂのテーブル４３０のデータと比較することによって判定されてもよい。この判定された適切な小売商鍵に関しては、商業エンティティサブシステム４００は、その小売商鍵（例えば、小売商鍵１５７’）を用いて、ホストトランザクションデータ６７８の少なくとも一部（例えば、トークンデータ及び／又は暗号化されたホスト決済クレデンシャルデータ６７６の暗号データ）を暗号化された小売商クレデンシャルデータ６８１として再暗号化することができる。例えば、暗号化された小売商クレデンシャルデータ６８１は、ホストトランザクションデータ６７８からの少なくとも暗号化されたホスト決済クレデンシャルデータ６７６、並びにホストトランザクションデータ６７８及び／又は決済要

求データ６６６／６７４（例えば、潜在的なトランザクションデータ６６０／６７２によって最初に識別され得たデータ）からの又はそれに基づく購入金額データ又は他の適切なトランザクションデータなどの任意の適切なトランザクションデータ、を含むことができる。ホストトランザクションデータ６７８からの小売商識別情報は、ステップ６３１において暗号化された小売商クレデンシャルデータ６８１を暗号化し得る小売商鍵を判定するために、その小売商識別が既に使用されていてもよいので、暗号化小売商クレデンシャルデータ６８１に含まれる必要はなくてもよい。暗号化された小売商クレデンシャルデータ６８１は、小売商サブシステム２００によって受信されたときに、そのような暗号化された小売商クレデンシャルデータ６８１の作成者として商業エンティティサブシステム４００を確立することができ、及び／又は小売商サブシステム２００がそのような暗号化された小売商クレデンシャルデータ６８１が署名された後に変更されていないことを保証することを有効化し得るような方法で、商業サブシステム４００によって署名されてもよい。そのような暗号化された小売商クレデンシャルデータ６８１は、ステップ６３１において生成され、次いで、ステップ６３２において、セキュアなホストトランザクションデータ６８２として任意の他の適切なデータとともにホストデバイス１００に送信されてもよい（例えば、商業エンティティサブシステム４００のサーバ４１０からホストデバイス１００の通信コンポーネント１０６へ図１Ｂの経路６５を介して）。

【００７８】

ステップ６３１及び６３２は、商業エンティティサブシステム４００から図１Ｂのセキュアなホストトランザクションデータ６８２（暗号化された小売商クレデンシャルデータ６８１のトークンデータ及び／又は暗号データ）の一部として送信されたクレデンシャルデータが、セキュアエレメント１４５以外のホストデバイス１００の一部によって復号され得ないような方法で暗号化され得ることを確実にするように動作することができる。すなわち、セキュアなホストトランザクションデータ６８２のクレデンシャルデータ（例えば、暗号化された小売商クレデンシャルデータ６８１のトークンデータ及び／又は暗号データ）は、いくつかの実施形態では、セキュアエレメント１４５を含む、ホストデバイス１００の任意の部分に公開され得ないか、又は他の方法でそれによってアクセスし得ない小売商鍵（例えば、小売商鍵１５７’）を用いて、暗号化されてもよい。更に、セキュアなホストトランザクションデータ６８２のクレデンシャルデータ（例えば、暗号化された小売商クレデンシャルデータ６８１のトークンデータ及び／又は暗号データ）は、セキュアエレメント１４５の外部のホストデバイス１００の任意の部分に公開され得ないか、又は他の方法でそれによってアクセスし得ないクレデンシャル鍵１５５ａ’を用いて、暗号化されてもよい。

【００７９】

セキュアなホストトランザクションデータ６８２は、次いで、ステップ６３４において、セキュアホストトランザクションデータ６８４として（例えば、任意の適切なプロトコルを使用して通信経路９９を介して及び／又は商業エンティティサブシステム４００を介して）クライアントデバイス１００’に転送されてもよい（例えば、プロセス５００のステップ５１６に関して記載したように）。次いで、クライアントデバイス１００’は、ステップ６３６において、クライアントトランザクションデータ６８６として（通信経路１５を介して、又は非接触近接ベース通信５として）、セキュアホストトランザクションデータ６８４の少なくとも暗号化された小売商クレデンシャルデータ６８１を小売商サブシステム２００に転送するように動作することができる（例えば、プロセス５００のステップ５１８に関して記載したように）。いくつかの実施形態では、ステップ６３４とステップ６３６との間に、クライアントデバイス１００’のＧＵＩは、図３Ｇの別の画面１９０ｇを提供するように構成されてもよく、それは、ホストデバイス１００からの、選択され認証されたクレデンシャルを使用して（例えば、セキュアなホストトランザクションデータ６８２／６８４の暗号化された小売商クレデンシャルデータ６８１内で暗号化された、暗号化されたホスト決済クレデンシャルデータ６７６として）、クライアントデバイス１００’のユーザに、プロンプト３３３を用いて、１つ以上の方法でクライアントデバイス１００’と

対話して、決済を審査して拒否し、及び／又は最終的に開始するように指示することができる。あるいは、ステップ６３６は、クライアントデバイス１００’のユーザに対して透過的に行われてもよい。あるいは、小売商クレデンシャルデータ６８１は、ホストデバイス１００を介して及び／又はクライアントデバイス１００’を介して通信されることなく商業エンティティサブシステム４００から小売商サブシステム２００に通信されてもよい。潜在的トランザクションデータ６６０／６７２の１つ、いくつか、又は全ての部分は、クライアントデバイス１００’及び／又はホストデバイス１００及び／又は商業的エンティティサブシステム４００を介して、決済要求データ６６６／６７４からホストトランザクションデータ６７８及び／又はセキュアなホストトランザクションデータ６８２及び／又はセキュアなホストトランザクションデータ６８４及び／又はクライアントトランザクションデータ６８６へ運ばれて、潜在的なトランザクションの特定の識別子がプロセス６００中に各エンティティによって識別され得る。それは、（ｉ）一意の小売商（すなわち、「小売商Ａ」）の小売商識別子及び／又は使用されている特定の小売商リソース（例えば、特定の小売商アプリケーション１１３’）の識別などの、特定の小売商情報、（ｉｉ）トランザクションの決済に使用される特定の通貨（例えば、円、ポンド、ドルなど）の識別、及び／又はトランザクションのために決済される特定の通貨量（すなわち、「価格Ｃ」及び／又は「価格Ｃ*」）の識別、及び／又は購入されるか若しくはレンタルされるか若しくは別途決済される特定の商品又はサービス（すなわち、「製品Ｂ」）の識別、及び／又は使用されるデフォルト又は最初の出荷住所（すなわち、「出荷Ｄ」及び／又は「出荷Ｅ」）の識別などの、特定のトランザクション情報、（ｉｉｉ）トランザクションのために小売商に受け入れ可能な、又はクライアントデバイス１００’（すなわち、「ＨＤ１’ｓ　ＰＭＸ」）によって選択された１つ以上のタイプの決済方法を示す情報（例えば、購入に使用され得る決済カードのリスト（例えば、ＭａｓｔｅｒＣａｒｄであるがＶｉｓａではない））、ｉｖ）一意の小売商ベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのために小売商サブシステム２００によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、（ｖ）一意のクライアントベースのトランザクション識別子（例えば、実行されているトランザクションとの関連付けのためにクライアントデバイス１００’によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、（ｖｉ）一意のクライアントベースの決済要求識別子（例えば、決済要求データ６６６／６７４によって行われている決済要求との関連付けのためにクライアントデバイス１００’によってランダムに又は一意的に生成され得る、３又は４文字の英数字文字列などの、任意の適切なデータエレメント）、及び／又は（ｖｉｉ）一意のホストベース決済要求識別子（例えば、３又は４文字の英数字文字列などの、ホストデバイス１００によって資金を供給される決済要求との関連付けのためにホストデバイス１００によってランダムに又は一意的に生成され得る、任意の適切なデータエレメント）、を含むが、これらに限定されない。そのような運ばれたデータは、本明細書ではＰＫＲｅｍｏｔｅＰａｙｍｅｎｔＲｅｑｕｅｓｔの少なくとも一部を含むことができ、任意の適切なデータを含むことができる。それは、（１）ステップ６１０及び／又はステップ６２２のＰＫＰａｙｍｅｎｔＲｅｑｕｅｓｔ（例えば、ＰＫＲｅｍｏｔｅＰａｙｍｅｎｔＲｅｑｕｅｓｔ内にラップされてもよい）、（２）本明細書ではＰＫＲｅｍｏｔｅＤｅｖｉｃｅと呼ばれ得る、選択された目標ホストデバイスを識別する任意の適切なデータ（例えば、ステップ６１４のディスカバリ応答に含まれてもよい、ホストデバイス１００のホストデバイス識別子１１９、）、（３）本明細書ではＳｅｌｅｃｔｅｄＡｐｐｌｉｃａｔｉｏｎＩｄｅｎｔｉｆｉｅｒと呼ばれ得る、目標ホストデバイスの選択された又はデフォルトの特定の決済を識別する任意の適切なデータ（例えば、ステップ６１４のディスカバリ応答に含まれてもよく、クライアントデバイス１００’において自動的に又はユーザによって選択されてもよい、目標ホストデバイス１００のセキュアエレメント１４５のＡＩＤ１５５ａａなど）、及び／又は（４）本明細書ではＲｅｍｏｔｅＰａｙｍｅｎｔＩｄｅｎｔｉｆｉｅｒと呼ばれ得る、決済要求と関連付けられる一意の識別子を識別する任意の適切なデータ（例

えば、システムのクライアント及びホストデバイスを介して決済要求を識別するために使用され得る、及びクライアントデバイス１００又はその他のものによって生成され得る、一意の値）、を含むが、これらに限定されない。他の実施形態では、ホストデバイス１００は、クライアントデバイス１００’を介してではなく、ステップ６３４において、セキュアなホストトランザクションデータ６８４を小売商サブシステム２００に直接的に通信することができる。更に他の実施形態では、商業エンティティサブシステム４００は、ホストデバイス１００を介してではなく、ステップ６３２において、セキュアなホストトランザクションデータ６８２をクライアントデバイス１００’に直接的に通信することができる。更に他の実施形態では、商業エンティティサブシステム４００は、ホストデバイス１００及び／又はクライアントデバイス１００’を経由するのではなく、ステップ６２１において、セキュアなホストトランザクションデータ６３２を小売商サブシステム２００に直接的に通信することができる。

【００８０】

セキュアなホスト決済クレデンシャルデータ６７５／６７６を含む小売商クレデンシャルデータ６８１が小売商サブシステム２００によって受信されると（例えば、ステップ６３６においてクライアントトランザクションデータ６８６として）、プロセス６００は、小売商サブシステム２００が、決済６８８を生成して取得銀行サブシステム３００に送信するように（例えば、図１Ｂの小売商サブシステム２００と取得銀行サブシステム３００の間の通信経路２５を介して）構成され得るステップ６３８も含むことができ、ここで、データ６８８は、ホストデバイス１００のセキュアなホスト決済クレデンシャルデータ及び製品又はサービスの小売商の購入価格を示し得る決済情報及び許可要求を含むことができる（例えば、クライアントトランザクションデータ６８６に含まれるか、若しくは他の方法でそれと関連付けられ得るように、又は他の方法で小売商サブシステム２００によって（例えば、潜在的なトランザクションデータ６６０／６７２によって（例えば、一意のトランザクション識別子に基づいて）知られているトランザクションと関連付けられるように））。例えば、ステップ６３８において、小売商サブシステム２００は、その既知の小売商鍵１５７’を利用して、クライアントトランザクションデータ６８６の小売商クレデンシャルデータ６８１を少なくとも部分的に復号することができ、決済データ６８８は、金融機関サブシステム３５０には利用できない鍵を用いてではなく、そのクレデンシャル鍵１５５ａ’を用いて暗号化されたクレデンシャルＳＳＤ１５４ａのセキュアなホスト決済クレデンシャルデータ（例えば、暗号化された決済クレデンシャルデータ６７６）を含むことができる。

【００８１】

ステップ６３８において、決済データ６８８が取得銀行サブシステム３００に送信された場合、次いで、ステップ６４０において、取得銀行サブシステム３００は、許可要求情報を決済データ６８８から金融機関サブシステム３５０に許可要求データ６９０として転送することができる（例えば、図１Ｂの取得銀行サブシステム３００と金融機関サブシステム３５０の間の通信経路３５を介して）。次に、ステップ６４２において、金融機関サブシステム３５０の発行銀行サブシステム３７０が許可要求を受信すると（例えば、ステップ６４０においてデータ６９０として取得銀行サブシステム３００から直接的に、又は間接的にデータ４０５として決済ネットワークサブシステム３６０を介して間接的に）、各々が、許可要求データ６９０に、並びにデータ６８４、６８６及び／又は６８８に含まれ得る、決済情報（例えば、ホストデバイス１００のセキュアエレメント１４５によってクレデンシャル鍵１５５ａ’によって暗号化されたホストデバイス１００のホスト決済クレデンシャルデータ６７５（例えば、暗号化されたホスト決済クレデンシャルデータ６７６））並びに購入金額が、復号され（例えば、金融機関サブシステム３５０でクレデンシャル鍵１５５ａ’を使用して）分析されて、その商取引クレデンシャルと関連付けられたアカウントが購入額をカバーするのに十分なクレジットを有するかどうかを判定することができる。十分な資金供給が存在しない場合、発行銀行サブシステム３７０は、否定的な許可応答を取得銀行サブシステム３００に送信することによって、要求されたトランザクショ

ンを拒否することができる。しかし、十分な資金供給が存在する場合、発行銀行サブシステム３７０は、肯定的な許可応答を取得銀行サブシステム３００に送信することによって要求されたトランザクションを承認することができ、金融トランザクションは完了され得る。いずれかのタイプの許可応答は、プロセス６００のステップ６４２において許可応答トランザクション状態データ６９２として、ユーザ金融サブシステム３５０によって取得銀行サブシステム３００に提供されてもよい（例えば、発行銀行サブシステム３７０から取得銀行サブシステム３００へ通信経路３５を介して直接的に、又は図１Ｂの通信経路４５を介して発行銀行サブシステム３７０から決済ネットワークサブシステム３６０に提供され得る認可応答データ４１５に基づいて、決済ネットワークサブシステム３６０から取得銀行サブシステム３００へ）。次に、ステップ６４２において許可応答トランザクション状態データ６９２を受信したことに応じて、プロセス６００は、取得銀行サブシステム３００又は任意の他の適切なサブシステムが、ステップ６４４において、そのような許可応答トランザクション状態データを許可応答トランザクション状態データ６９４として小売商サブシステム２００と共有することも含むことができ、それは、次いで、ステップ６４６において確認されたトランザクション状態データ６９６として（例えば、プロセス５００のステップ５２２に関して説明したように）クライアントデバイス１００’と（例えば、小売商リソース又は他の方法で）、及び／又はステップ６４８において確認されたトランザクション状態データ６９８として（例えば、プロセス５００のステップ５２４に関して説明したように）ホストデバイス１００と、共有されてもよい。そのような確認されたトランザクション状態データは、図３Ｈの画面１９０ｈの確認データ３３５などの、任意の適切な確認データをデバイス１００及び／又は１００’に提供するように構成され得る。トランザクションが成功した場合、確認されたトランザクション状態データは、ステップ６４６のクライアントデバイス１００’で、及び／又はステップ６４８のホストデバイス１００で、トランザクション（例えば、決済要求データの一意のＲｅｍｏｔｅＰａｙｍｅｎｔＩｄｅｎｔｉｆｉｅｒによって識別されたトランザクション）を閉じるように動作することができる。追加で、又は代替で、トランザクションが成功しなかった場合、確認されたトランザクション状態データは、トランザクションを閉じるために動作しても動作しなくてもよい（例えば、有効な資金供給が利用できないか、又はホストデバイスが不正であると識別された場合、トランザクションを閉じるが、無効な出荷住所が判定された場合、開いたままにしておいて更新を許容する）。任意の非トランザクション終了トランザクション状況データによって、プロセスがアプリケーションによってキャンセルされるか、プロセスがユーザによってキャンセルされるか、又はプロセスが完了するまで、決済プロセスを継続することが可能になり得る。

【００８２】

したがって、小売商サブシステム２００は、任意の適切な方法で、クライアントトランザクションデータ６８６又は小売商クレデンシャルデータ６８１の任意の他のキャリヤを処理するように構成され得る。例えば、小売商サブクレデンシャルデータ６８１からホスト決済クレデンシャルデータを得るために、小売商サブシステム２００は、受信した小売商クレデンシャルデータ６８１の署名特性が有効であり、商業エンティティサブシステム４００がその署名の署名者であることを検証することができる。小売商サブシステム２００は、任意の適切な技術を使用して、どの小売商鍵（例えば、小売商公開鍵１５７’）が商業エンティティサブシステム４００によって小売商クレデンシャルデータ６８１を構築するために使用されたかを判定することができる。次いで、小売商サブシステム２００は、対応するクレデンシャル秘密鍵（例えば、小売商サブシステム２００の小売商秘密鍵１５７’）を取得し、その取得された鍵を使用して、暗号化された小売商クレデンシャルデータ６８１をカプセル化解除及び／又は復号して暗号化されたホスト決済クレデンシャルデータ６７６を回復することができる。次いで、そのようなデータ６７６は、適切な決済ネットワーク３６０に提供されてもよく、それは、金融機関サブシステム３５０の適切なクレデンシャル鍵１５５ａ’を利用して、暗号化されたホスト決済クレデンシャルデータ６７６をカプセル化解除及び／又は復号してホスト決済クレデンシャルデータ６７５を回復する

ことができる（ホスト決済クレデンシャルデータ６７５を有効にするためにホスト決済クレデンシャルデータ６７５のトークンデータ及び／又は暗号データを回復することができる（例えば、受信したホスト決済クレデンシャルデータ６７５のトークンデータに基づいて暗号データを独立して生成し、その生成された暗号データを受信されたホスト決済クレデンシャルデータ６７５の暗号データと比較し、その比較に基づいてトランザクションを有効にするか又は拒否するかのいずれかを行うことができる）。

【００８３】

図６のプロセス６００で示されるステップは、単に例示されたものに過ぎず、その既存のステップは修正又は省略されてもよく、更なるステップが追加されてもよく、特定のステップの順序が変更されてもよいことが理解される。いくつかの実施形態では、潜在的なトランザクション（例えば、潜在的なトランザクションデータ６６０又は潜在的なトランザクションデータ６７２によって識別されるような）は、２つの異なる決済クレデンシャルによって少なくとも部分的に資金を供給されてもよい。例えば、クライアントデバイス１００’は、トランザクションの第１の部分に資金を供給するように動作することができる第１のホストトランザクションデータ（例えば、第１のホストトランザクションデータ６８４）の生成を開始するための第１のホストデバイスへの第１の決済要求（例えば、第１の決済要求データ６６６）だけでなく、トランザクションの第２の部分に資金を供給するように動作することができる第２のホストトランザクションデータ（例えば、第２のホストトランザクションデータ６８４）の生成を開始するための第２のホストデバイスへの第２の決済要求（例えば、第２の決済要求データ６６６）、も生成して送信するように動作することができ、ホストトランザクションデータの各インスタンスは、トランザクションに資金を供給するためにクライアントデバイス１００’によって共有されてもよい。あるいは、トランザクションの第２の部分は、クライアントデバイス１００’にネーティブクレデンシャルデータによって資金を供給されてもよい。図示されていないが、セキュアなホストトランザクションデータは、商業エンティティサブシステム４００から、クライアントデバイス１００’に直接的に（例えば、通信経路９５を介して及びホストデバイス１００を介さずに）、又は小売商サブシステム２００に直接的に（例えば、通信経路８５を介して及びホストデバイス１００を介さずに及び／又はクライアントデバイス１００’を介さずに）、又は金融機関サブシステム３５０に直接的に（例えば、通信経路５５を介して及びホストデバイス１００を介さずに及び／又はクライアントデバイス１００’を介さずに及び／又は小売商サブシステム２００を介さずに）、通信されてもよい。追加で、又は代替で、図示されていないが、セキュアなホストトランザクションデータは、ホストデバイス１００から、小売商サブシステム２００に直接的に（例えば、クライアントデバイス１００’を介さずに）、又は金融機関サブシステム３５０に直接的に（例えば、通信経路７５を介して及びクライアントデバイス１００’を介さずに及び／又は小売商サブシステム２００を介さずに）送信されてもよい。追加で、又は代替で、図示されていないが、クライアントトランザクションデータは、クライアントデバイス１００’から金融機関サブシステム３５０に直接的に（例えば、小売商サブシステム２００を介さずに）通信されてもよい。上述のように、クライアントデバイス１００’は、特定の製品を購入すべきであると判断して、その特定の製品の少なくとも１つの特定の小売商から関連付けられた潜在的なトランザクションデータを取得するために、全て自動的に及びクライアントデバイス１００’のユーザによる任意のアクティブな対話なしに、１つ以上の小売商と対話するように構成されてもよい（例えば、クライアントデバイス１００’は、家電製品であり、家電製品が購入されなければならないと判定するように構成され得る家庭電化製品であることができ（例えば、より多くの洗濯洗剤が洗濯機によって必要とされていることを検出するか、又は特定の日により多くの洗剤を購入するようにユーザによって予め設定されたカレンダーイベントを検出する）、その製品に対して最良の取引を提供する特定の小売商を自動的に識別することができ、その小売商と自動的に対話してその小売商からその製品を購入するための潜在的なトランザクションデータを得ることができる）。その後、クライアントデバイス１００’は、決済要求（例えば、決済要求データ６６６）を１つ以上の特定の目標ホストデバイス

に、自動的に生成してプッシュするように動作することができる。例えば、そのようなクライアントデバイス１００’は、エコシステム内の１つ以上のホストデバイス１００（例えば、Ａｐｐｌｅ　Ｉｎｃ．によるＨｏｍｅＫｉｔ（商標）などのホームオートメーションプラットフォームを使用して）と対にされ得る自動化デバイスであってもよく、そのような決済要求は、予め決められた設定に従って少なくとも部分的に取り込まれるか、又は他の方法で取り込まれてもよい（例えば、ホストデバイスＸからの新しい洗濯洗剤の決済を要求し、ホストデバイスＹからの新しい乾燥機シートの決済を要求するか、又はホストデバイスＸからの＄Ｇ超の及びホストデバイスＹからの＄Ｇ未満の任意の購入の決済を要求する、など）。

【００８４】

プロセス６００のホストデバイス１００とクライアントデバイス１００’の間の１つ、いくつか、又は各々のデータ通信（例えば、データ６６２、６６４、６６６、６６８、６７４、６８４、及び／又は６９８の１つ、いくつか、又は各々の通信）は、ピアツーピア配置で直接的に、又は商業エンティティサブシステム４００若しくは任意の他の適切なエンティティを介して、などの任意の適切な通信プロトコルを使用して、任意の適切な方法で暗号化されてもまったく暗号化されなくてもよい任意の適切なトランスポート機構を使用して、任意の適切な通信経路を介して行われてもよい。そのようなデータ通信は、任意の適切なオンラインメッセージング、インスタントメッセージング、電子メールメッセージング、テキストメッセージ、任意の適切な近接型メッセージング、ＮＦＣ、ＢｌｕｅＴｏｏｔｈ（登録商標）、などを介して行われてもよく、電話番号、電子メールアドレス、一意のデバイス識別子、位置ベースのビーコン、などの任意の適切なデバイスアドレッシングスキームを使用して、有効化することができる。各ホストデバイス及び各クライアントデバイスは、ラップトップ、携帯電話、家庭電化製品、小売商アクセサリデバイス（例えば、ガソリン小売商によってガスポンプで提供されるデバイス）、ユーザアクセサリ（例えば、スマートウォッチなどのウェアラブルデバイス）、などの、ユーザに対して任意の適切なＵＩ及びＩ／Ｏ能力を有する任意の適切なデバイスであってもよい。ネーティブ決済クレデンシャルを有する任意のホストデバイスが、それ自体ネーティブ決済クレデンシャルを有しても有さなくてもよい、任意の他の適切なデバイス（例えば、それ自体のネーティブ決済を有するか、又は有さないクライアントデバイス）から決済要求を受信し応答する（例えば公衆インターネットを介して又は他の適切な方法で）ことを可能にすることによって、システム１及びプロセス６００は、多くのセキュアで効果的な使用事例及びユーザエクスペリエンスを有効化することができる。

【００８５】

例えば、ユーザは、クライアントデバイス１００’（例えば、セキュアエレメント又は任意のネーティブ決済クレデンシャルを有さなくてもよいラップトップコンピュータ）上の小売商サブシステム２００のオンライン小売商リソース（例えば、アプリケーション１１３’）を使用してオンラインショッピングを行い、オンラインリソースと対話して購入する特定の製品（例えば、「製品Ｂ」）を識別する。その製品の識別に応じて（例えば、ユーザが「セキュアクレデンシャル決済で購入する（Ｂｕｙ　ｗｉｔｈ　Ｓｅｃｕｒｅ　Ｃｒｅｄｅｎｔｉａｌ　Ｐａｙｍｅｎｔ）」（例えば、Ａｐｐｌｅ　Ｉｎｃ．によるＡｐｐｌｅ　Ｐａｙ（商標））を選択することに応じて、オンラインリソースは、クライアントデバイス１００’上に決済シート又は任意の適切なＵＩを提示して、ユーザが特定の出荷住所又は他の可変データを入力することを有効化し得るように動作することができる（例えば、画面１９０ａによって示されるように、及び他の情報を更新し得るステップ６２０及び６２２の１回以上の反復を介してクライアントデバイス１００’のユーザによって更新され得るように（例えば、クライアントデバイス１００’のユーザが情報３０７ｄの出荷アドレスを変更することに応じて、情報３０７ｃの価格が更新され得る））。ある時点で、クライアントデバイス１００’のユーザは、画面１９０ａの「セキュア決済（Ｓｅｃｕｒｅ　Ｐａｙ）」オプション３０９を選択することができ、それは、クライアントデバイス１００’が画面１９０ａの決済シートの購入に資金を供給する（例えば、潜在的なトランザクションデ

ータ６６０によって示された許容可能な決済オプションに基づいて）のに適したネーティブ決済クレデンシャルを有さないこと、及び「ＨＤ１’ｓ　ＰＭ　Ｘ」（例えば、ホストデバイス１の決済方法Ｘ）が、使用に適した唯一の利用可能又は好ましい非ネーティブ決済クレデンシャルであること、を自動的に識別することができる（例えば、クライアントデバイス１００’のユーザによる任意の更なる対話なしで）ディスカバリプロセス（例えば、ステップ６６２及び６６４）をもたらすことができる（例えば、各利用可能な使用可能なホストデバイスのクライアントデバイスへの近接性、又はディスカバリプロセスを介してクライアントデバイス１００’にアクセス可能であり得る任意の他の適切な特性に基づいて、優先度が自動的に判定されてもよい）。そのような識別の後、クライアントデバイス１００’は、図３Ｃの画面１９０ｃをクライアントデバイス１００’のユーザに自動的に提示して、適切な決済要求をそのホストデバイスに送信するためにユーザが図３Ｃのオプション３１５を選択することを有効化するように動作することができ、又は、プロセス６００は、ユーザに代わってその選択を自動的に行うことができ（例えば、ディスカバリプロセスの識別に応じて、利用可能な目標ホストデバイス１（すなわち、ホストデバイス１００）に適切な決済要求データ６６６／６７４を自動的に送信することによって）、それは、そのホストデバイス１００によって自動的に提示される、図３Ｄの画面１９０ｄ又は図３Ｅの画面１９０ｅをもたらすことができる（例えば、クライアントデバイス１００’に提示された決済シートに類似してもよいホストデバイス１００上の決済シートを提示する）。ホストデバイス１００は、クライアントデバイス１００’によって開始されたトランザクションに資金を供給するのに適した少なくとも１つのネーティブ決済クレデンシャルを有するセキュアエレメントを含み得る、携帯電話又は他の任意のデバイスであってもよい。クライアントデバイス１００’のユーザは、クライアントデバイス１００’だけでなくホストデバイス１００にも近接していてもよく、ホストデバイス１００の画面１９０ｄ～１９０ｆのうちの１つのＧＵＩと対話してクライアントデバイス１００’及び小売商サブシステム２００によって開始されたか、又は他の方法で実行されている（例えば、図３Ｆの画面１９０ｆの認証オプション３３１を選択することによって）トランザクションに資金を供給するためにホストデバイス１００にネーティブな特定の決済クレデンシャルの使用を許可することができる。ホストデバイス１００上のそのような認証に応じて、ホストデバイス１００にネーティブクレデンシャルのホスト決済クレデンシャルデータがトランザクションに資金を供給することを試みるために金融機関サブシステム３５０に提供されてもよく（例えば、プロセス６００のステップ６２５～６４０において）、次いで、トランザクションの確認状態は、クライアントデバイス１００’及び／又はホストデバイス１００のユーザと共有され得る（例えば、図３Ｈの画面１９０ｈによって）。代替の実施形態では、複数のホストデバイスが利用可能であると識別され、決済要求が、クライアントデバイス１００’から利用可能なホストデバイスの各１つに送信されてもよく、ホスト決済クレデンシャルデータで応答する第１のホストデバイスが、トランザクションに資金を供給することができるか、又は各ホストデバイスが、トランザクションの特定の部分に資金を供給し得るホスト決済クレデンシャルデータで応答することができる。

【００８６】

別の例として、ホームオートメーションプラットフォーム（例えば、Ａｐｐｌｅ　Ｉｎｃ．のＨｏｍｅＫｉｔ（商標））を使用して通信ネットワークに通信結合されたユーザの家庭電化製品クライアントデバイス１００’（例えば、洗濯機）は、適切に動作するのに必要とされるリソースがほとんどなくなっていると判定するように動作することができる（例えば、洗濯機クライアントデバイス１００’は、その洗濯洗剤の貯蔵量が２０％の容量にあることを自動的に判定するように動作することができる）。そのような判定に応じて、家庭電化製品クライアントデバイス１００’は、より多くのそのリソースを購入する機会を自動的に識別するように動作することができる（例えば、家庭電化製品クライアントデバイス１００’は、１つ以上の小売商サブシステムと１つ以上のオンラインリソースを介して対話して、最良の価格又は他の適切な指標で販売している必要な洗濯洗剤を識別するように動作することができる）。その購入機会のための潜在的トランザクションデータ６６０

／６７２は、それによってクライアントデバイス１００’によって取得されてもよく、クライアントデバイス１００’は、そのトランザクションに資金を供給するために利用可能な少なくとも１つのホストデバイスを自動的に発見するように動作することができ（例えば、ステップ６６２／６６４のディスカバリプロセスを介して）、家庭電化製品クライアントデバイス１００’を含むホームオートメーションプラットフォームエコシステムに関連付けられた少なくとも１人のユーザのホストデバイスなどの、少なくとも１つの発見されたホストデバイスの各々と適切な決済要求データ６６６／６７４を自動的に共有することができる。ホストデバイス１００は、そのような決済要求データを受信することができ、家庭電化製品クライアントデバイス１００’によって識別された（例えば、クライアントデバイス１００’において何らアクティブなユーザ対話なしに識別された）トランザクションに資金を供給するのに使用するためにそのホストデバイスにネーティブ決済クレデンシャルを選択し、認証する能力を有するホストデバイス１００のユーザを提示することができる。これは、家庭電化製品クライアントデバイス１００’に関する任意の適切な場所のユーザ及びホストデバイス１００が、家庭電化製品クライアントデバイス１００’からの一意の決済要求を受信し、家庭電化製品クライアントデバイス１００’に、一意の決済要求に関連付けられたトランザクションに資金を供給するのに使用するためのホストデバイスにネーティブ決済クレデンシャルのホストトランザクションデータを提供することを有効化することができる（例えば、ホストデバイス１００及びそのユーザは、家庭電化製品クライアントデバイス１００’から人の他方の側に配置され得るが、まだ家庭電化製品クライアントデバイス１００’から決済要求を受信し、ホスト決済クレデンシャルデータで応答するように（例えば、任意の適切なインターネット通信経路又は任意の他の適切な通信経路を介して）動作することができる）。あるいは、インターネットを介して遠距離通信するのではなく、家電機器クライアントデバイス１００’は、近接ホストデバイス１００のセンサーによってスキャンされ、特定の決済要求データを識別するように処理され得るクライアントデバイス１００’のディスプレイ上にＱＲコード（登録商標）を提示することができ、又はクライアントデバイス１００’とホストデバイス１００は、ＢｌｕｅＴｏｏｔｈ（登録商標）又は任意の他の適切なローカル通信プロトコルを介して通信することができる。

【００８７】

いくつかの実施形態では、プロセス５００及び／又は６００の少なくとも一部及び／又は本開示の任意の他のプロセスは、ホストデバイス１００のユーザとクライアントデバイス１００’のユーザの間で送金するように動作することができる（例えば、クライアントデバイス１００’は、クライアントデバイス１００’と小売商サブシステムの間のトランザクションとは独立して、ホストデバイス１００からの資金供給を要求することができる）。いくつかの実施形態では、これは、取得銀行及び／又は金融機関サブシステム３５０の１つ以上のエンティティによって、小売商サブシステムを何ら必要とせず、ホストトランザクションデータが、ホストデバイス上のクレデンシャルと関連付けられたアカウントとクライアントデバイスのユーザと関連付けられたアカウントの間の資金の移転を容易にすることを有効化することを有効化され得る。あるいは、ホストデバイス上のストアドバリューカード及び／又はクライアントデバイス上のストアドバリューカードを利用して、ホストとクライアントの間で資金を移転することができる（例えば、ホストデバイスにネーティブなストアドバリュークレデンシャル（例えば、ホストデバイス１００のセキュアエレメント１４５上のクレデンシャル）から、クライアントデバイスにネーティブなストアドバリュークレデンシャル（例えば、クライアントデバイス１００’のセキュアエレメント上のクレデンシャル）に資金を移転する）。例えば、クライアントデバイス１００’は、決済要求を、ホストデバイス１００がホストデバイス１００上のストアドバリュークレデンシャルからある量の通貨を差し引くことを要求するように動作し得るホストデバイス１００に通信し、任意の適切なＡＰＤＵコマンドを、クライアントデバイス１００’のストアドバリュークレデンシャルに適切な量の通貨を追加するように動作し得るクライアントデバイス１００’に送信することができる（例えば、クライアントデバイス１００’と共有されたホストトランザクションデータがそのようなＡＰＤＵコマンドを含むことができ、及び／

又は実際の暗号通貨を含むことができるように）。

【００８８】

クライアントデバイス１００’が、小売商に固有であり得るクライアントデバイス１００’上のネーティブアプリケーションを介して、小売商サブシステム２００と通信し得る場合、次いで小売商アプリケーション１１３ｃは、そのようなアプリケーションによって提供され得る。しかし、クライアントデバイス１００’が、小売商に特有ではないが、小売商によって管理されるウェブサイト（例えば、小売商の制御下にあるサーバ上）に示され得るインターネットブラウザを介して、小売商サブシステム２００と通信し得る場合、小売商アプリケーション１１３ｃは小売商のウェブサイトに通信を転送することができる、（例えば、通信コンポーネント１０６を介して）レイアウトエンジンソフトウェアコンポーネント（例えば、ＷｅｂＫｉｔ）であってもよい。例えば、クライアントデバイス１００’のそのようなアプリケーション１１３ｃは、小売商サブシステム２００に提供される任意のホストトランザクションデータのためのコンジットであることができる。あるいは、そのようなホストトランザクションデータは、クライアントデバイス１００’を経由せず、代わりにホストデバイス１００又は商業エンティティサブシステム４００から直接的に、小売商サブシステム２００に通信されてもよい（例えば、潜在的なトランザクションデータ及びクライアントデバイスの決済要求データにおいて小売商によって提供される小売商識別子又は住所を使用して）。

図７の説明

【００８９】

図７は、商業エンティティサブシステム、クライアント電子デバイス、並びにセキュアエレメント及びセキュアエレメント上にプロビジョニングされたホストクレデンシャルアプリケーションを含むホスト電子デバイスを使用して小売商サブシステムと金融トランザクションを実行するための例示的なプロセス７００のフローチャートである。プロセス７００のステップ７０２において、ホスト電子デバイスは、小売商サブシステムを識別する小売商サブシステム識別子情報及びホストクレデンシャルアプリケーションを識別するホストクレデンシャルアプリケーション識別子情報を含む決済要求データを、クライアント電子デバイスから受信することができる。例えば、ホスト電子デバイス１００は、小売商サブシステム２００の識別子及びホスト電子デバイス１００のクレデンシャル決済アプレット１５３ａの識別子を含む決済要求データ６６２を受信することができる。プロセス７００のステップ７０４において、ホスト電子デバイスは、受信された決済要求データによって識別されるホストクレデンシャルアプリケーションを使用してセキュアエレメント上に、ホスト決済クレデンシャルデータを含む第１のデータを生成することができる。例えば、決済要求データ６６６によって識別されるクレデンシャル決済アプレット１５３ａは、ホスト決済クレデンシャルデータ６７５を生成することができる。プロセス７００のステップ７０６において、ホスト電子デバイスは、ホスト電子デバイスのセキュアエレメント上に、第１の鍵を用いて第１のデータ及び受信された決済要求データの小売商サブシステム識別子情報を暗号化することによって、第２のデータを生成することができる。例えば、ホスト電子デバイス１００は、ホスト決済データ６７７として、アクセス鍵を用いて、小売商サブシステム２００の識別子を含むホスト決済クレデンシャルデータ６７５及び決済要求データを暗号化することができる。プロセス７００のステップ７０８において、ホスト電子デバイスは、ホスト電子デバイスから商業エンティティサブシステムに第２のデータを送信することができる。例えば、ホスト電子デバイス１００は、ホスト決済データ６７８を商業エンティティサブシステム４００に送信することができる。プロセス７００のステップ７１０において、ホスト電子デバイスは、小売商サブシステム識別子情報に関連付けられた第２の鍵で暗号化された第１のデータを含む第３のデータを受信することができる。例えば、ホスト電子デバイス１００は、小売商サブシステム２００に関連付けられた小売商鍵で暗号化されたホスト決済クレデンシャルデータ６７５／６７６を含み得るセキュアなホストトランザクション６８２を受信することができる。プロセス７００のステップ７１２において、ホスト電子デバイスは、受信された第３のデータを送信して、

金融トランザクションの少なくとも一部に資金を供給することができる。例えば、ホスト電子デバイス１００は、金融トランザクションの少なくとも一部に資金を供給するために（例えば、小売商サブシステム２００のために）セキュアなホストトランザクションデータ６８４を送信することができる。

【００９０】

図７のプロセス７００に示されたステップは、例示的なものに過ぎず、既存のステップは変更又は省略されてもよく、追加のステップが追加されてもよく、特定のステップの順序が変更されてもよいことが理解される。

図８の説明

【００９１】

図８は、クライアント電子デバイス及びホスト電子デバイスを使用して、小売商サブシステムと金融トランザクションを実行するための例示的プロセス８００のフローチャートである。プロセス８００のステップ８０２において、クライアント電子デバイスは、小売商サブシステムから、金融トランザクションを示す潜在的なトランザクションデータを受信することができる。例えば、クライアント電子デバイス１００’は、小売商サブシステム２００から金融トランザクションを示す潜在的なトランザクションデータ６６０を受信することができる。プロセス８００のステップ８０４において、クライアント電子デバイスは、受信された潜在的なトランザクションデータに基づいて決済要求データをクライアント電子デバイスからホスト電子デバイスに送信することができる。例えば、クライアント電子デバイス１００’は、潜在的なトランザクションデータ６６０／６７２に基づいて、決済要求データ６６６／６７４をホスト電子デバイス１００に送信することができる。プロセス８００のステップ８０６において、クライアント電子デバイスは、クライアント電子デバイスにおいて、送信された決済要求データに基づいてホスト電子デバイスによって生成されたホスト決済クレデンシャルデータを含むホストトランザクションデータを受信することができる。例えば、ホスト電子デバイス１００によって生成されたホスト決済クレデンシャルデータ６７５を含むセキュアなホストトランザクションデータ６８４は、クライアント電子デバイス１００’によって受信されてもよい。プロセス８００のステップ８０８において、クライアント電子デバイスは、クライアント電子デバイスから小売商サブシステムに、受信されたホストトランザクションデータのホスト決済クレデンシャルデータを送信して、金融トランザクションの少なくとも一部に資金を供給することができる。例えば、クライアント電子デバイス１００’は、金融トランザクションの少なくとも一部に資金を供給するために（例えば、小売商サブシステム２００のために）、ホスト決済クレデンシャルデータ６７５を含むクライアントトランザクションデータ６８６を小売商サブシステム２００に送信することができる。

【００９２】

図８のプロセス８００に示されたステップは、例示的なものに過ぎず、既存のステップは変更又は省略されてもよく、追加のステップが追加されてもよく、特定のステップの順序が変更されてもよいことが理解される。

図９の説明

【００９３】

図９は、商業エンティティサブシステム、クライアント電子デバイス、並びにセキュアエレメント及びセキュアエレメント上にプロビジョニングされたホストクレデンシャルアプリケーションを含むホスト電子デバイスを使用して小売商サブシステムと金融トランザクションを実行するための例示的なプロセス９００のフローチャートである。プロセス９００のステップ９０２において、商業エンティティサブシステムは、金融トランザクションに資金を供給するために、小売商サブシステムに受け入れ可能な少なくとも１つの決済タイプを識別するホスト可用性要求を、クライアント電子デバイスから受信することができる。例えば、商業エンティティサブシステム４００は、（例えば、潜在的なトランザクションデータ６６０に基づいて）金融トランザクションに資金を供給するために、小売商サブシステム２００に受け入れ可能な少なくとも１つの決済タイプを識別する、クライア

ントデバイス１００’からのホスト可用性要求データ６６２を受信することができる。プロセス９００のステップ９０４において、商業エンティティサブシステムは、商業エンティティサブシステムにおいて、ホスト電子デバイスがクライアント電子デバイスに関連付けられていると判定することができる。例えば、商業エンティティサブシステム４００は、ホスト電子デバイス１００がクライアント電子デバイス１００’に関連付けられていること（例えば、両方のデバイスが商業エンティティサブシステムの同じ特定のユーザアカウントに関連付けられていること）を判定するように動作することができる。プロセス９００のステップ９０６において、商業エンティティサブシステムは、ホスト電子デバイスがクライアント電子デバイスに関連付けられているという判定に基づいて、ホスト電子デバイスのセキュアエレメント上にプロビジョニングされたホストクレデンシャルアプリケーションが、受信されたホスト可用性要求の識別された少なくとも１つの決済タイプを満たすと、判定することができる。例えば、商業エンティティサブシステム４００は、決済クレデンシャルアプレット１５３ａが小売商サブシステム２００に受け入れ可能な決済方法（例えば、Ｖｉｓａクレジットカード）に関連付けられていると判定するように動作することができる。プロセス９００のステップ９０８において、商業エンティティサブシステムは、ホストクレデンシャルアプリケーションが識別された少なくとも１つの決済タイプを満たすという判定に基づいて、商業エンティティサブシステムからクライアント電子デバイスに、ホスト電子デバイスを識別するホスト可用性応答を送信することができる。例えば、商業エンティティサブシステム４００は、ホスト電子デバイス１００を（例えば、利用可能な非ネーティブ決済ソースとして）識別することができるクライアント電子デバイス１００’にホスト可用性応答データ６６４を送信するように動作することができる。

【００９４】

図９のプロセス９００に示されたステップは、例示的なものに過ぎず、既存のステップは変更又は省略されてもよく、追加のステップが追加されてもよく、特定のステップの順序が変更されてもよいことが理解される。

図１０の説明

【００９５】

図１０は、クライアント電子デバイス及びホスト電子デバイスを使用してサービスプロバイダサブシステムとのトランザクションを実行するための例示的プロセス１０００のフローチャートである。プロセス１０００のステップ１００２において、クライアント電子デバイスは、サービスプロバイダサブシステムと通信して、サービスプロバイダサブシステムの製品へのアクセスを購入するためのトランザクションの少なくとも一部を定義することができる。例えば、クライアント電子デバイス１００’は、小売商サブシステム２００から金融トランザクションを示す潜在的なトランザクションデータ６６０を受信することができる。プロセス１０００のステップ１００４において、クライアント電子デバイスは、ホスト電子デバイスを関与させて、トランザクションに資金を供給するためのトランザクションクレデンシャルを生成することができる。例えば、クライアント電子デバイス１００’は、潜在的なトランザクションデータ６６０／６７２に基づいて、決済要求データ６６６／６７４をホスト電子デバイス１００に送信することができる。

【００９６】

図１０のプロセス１０００に示されたステップは、例示的なものに過ぎず、既存のステップは変更又は省略されてもよく、追加のステップが追加されてもよく、特定のステップの順序が変更されてもよいことが理解される。

図１、図１Ａ、図１Ｂ、図２、図２Ａ、及び図３の更なる説明

【００９７】

ホストデバイス１００のセキュアエレメントのクレデンシャルが、適切にホストトランザクションデータのホスト決済クレデンシャルデータとして（例えば、小売商端末２２０への非接触近接ベース通信として、及び／又は小売商サーバ２１０へのオンラインベース通信として）提供されるように、有効化されると（例えば、ＮＦＣコンポーネント１２０のクレデンシャルＳＳＤ１５４ａの有効化されたアプレット１５３ａに関連付けられた商

取引クレデンシャルデータ）、取得銀行サブシステム３００は、金融機関サブシステム３５０との金融トランザクションを完了するためにそのようなホスト決済クレデンシャルデータを利用することができる。例えば、クライアントデバイス１００’のユーザが購入のための製品を選択し、ホストデバイス１００のユーザが、デバイス１００の特定のクレデンシャルを決済に使用することを適切に有効化した後、小売商サブシステム２００は、特定のクレデンシャルの決済クレデンシャルデータを示すホスト決済クレデンシャルデータを受信することができる。小売商サーバ２１０及び／又は小売商端末２２０は、（例えば、クライアントデバイス１００’を介して）デバイス１００がホスト決済クレデンシャルデータを提供することに応じてエンドユーザ電子デバイスのユーザに製品又はサービスを提供し得る、小売商サブシステム２００の任意の適切な小売商又は小売商エージェントによって提供されてもよい。そのような受信されたホスト決済クレデンシャルデータ（例えば、データ６８６として）に基づいて、小売商サブシステム２００は、（例えば、小売商サブシステム２００と取得銀行サブシステム３００の間の通信経路２５を介して）取得銀行サブシステム３００へのデータ６８８を生成して送信するように構成されてもよく、データ６８８は、ホスト決済クレデンシャルデータ並びにホストデバイス決済クレデンシャル及び製品又はサービスの小売商の購入価格を示し得る許可要求を含むことができる。決済プロセッサ又は取得者としても知られる取得銀行サブシステム３００は、小売商サブシステム２００に関連付けられた小売商の銀行パートナーであってもよく、取得銀行サブシステム３００は、金融機関サブシステム３５０と協働して、ホスト決済クレデンシャルデータを用いてホストデバイス１００によって資金を供給されることを試みたクレデンシャルトランザクションを承認し決済するように構成されてもよい。取得銀行サブシステム３００は、次いで許可データ６９０として決済データ６８８から金融機関サブシステム３５０に許可要求を転送することができる（例えば、取得銀行サブシステム３００と金融機関サブシステム３５０の間の通信経路３５を介して）。

【００９８】

決済ネットワークサブシステム３６０及び発行銀行サブシステム３７０は、単一のエンティティ又は別個のエンティティであってもよい。例えば、Ａｍｅｒｉｃａｎ　Ｅｘｐｒｅｓｓは、決済ネットワークサブシステム３６０と発行銀行サブシステム３７０の両方であってもよい。一方、Ｖｉｓａ及びＭａｓｔｅｒＣａｒｄは、決済ネットワーク３６０であってもよく、Ｃｈａｓｅ、Ｗｅｌｌｓ　Ｆａｒｇｏ、Ｂａｎｋ　ｏｆ　Ａｍｅｒｉｃａなどの発行銀行３７０と協力して動作してもよい。金融機関サブシステム３５０は、取得銀行サブシステム３００などの１つ以上の取得銀行も含むことができる。例えば、取得銀行サブシステム３００は、発行銀行システム３７０と同じエンティティであってもよい。取得銀行サブシステム３００の１つ、いくつか、又は全てのコンポーネントは、デバイス１００のプロセッサコンポーネント１０２と同じか又は類似であり得る１つ以上のプロセッサコンポーネント、デバイス１００のメモリコンポーネント１０４と同じか又は類似であり得る１つ以上のメモリコンポーネント、及び／又はデバイス１００の通信コンポーネント１０６と同じか又は類似であり得る１つ以上の通信コンポーネントを使用して実装されてもよい。決済ネットワークサブシステム３６０の１つ、いくつか、又は全てのコンポーネントは、デバイス１００のプロセッサコンポーネント１０２と同じか又は類似であり得る１つ以上のプロセッサコンポーネント、デバイス１００のメモリコンポーネント１０４と同じか又は類似であり得る１つ以上のメモリコンポーネント、及び／又はデバイス１００の通信コンポーネント１０６と同じか又は類似であり得る１つ以上の通信コンポーネントを使用して実装されてもよい。発行銀行サブシステム３７０の１つ、いくつか、又は全てのコンポーネントは、デバイス１００のプロセッサコンポーネント１０２と同じか又は類似であり得る１つ以上のプロセッサコンポーネント、デバイス１００のメモリコンポーネント１０４と同じか又は類似であり得る１つ以上のメモリコンポーネント、及び／又はデバイス１００の通信コンポーネント１０６と同じか又は類似であり得る１つ以上の通信コンポーネントを使用して実装されてもよい。決済ネットワークサブシステム３６０及び発行銀行サブシステム３７０が別々のエンティティである場合、決済ネットワークサブシ

ステム３６０は、取得銀行サブシステム３００を取得することからデータ６９０を受信することができ、次いで、要求を発行銀行サブシステム３７０にデータ４０５として転送することができる（例えば、決済ネットワークサブシステム３６０と発行銀行サブシステム３７０の間の通信経路４５を介して）。決済ネットワークサブシステム３６０及び発行銀行サブシステム３７０が同じエンティティである場合、取得銀行サブシステム３００は、発行銀行サブシステム３７０に直接的にデータ６９０を提出することができる。更に、決済ネットワークサブシステム３６０は、発行銀行サブシステム３７０に代わって取得銀行サブシステム３００に応答することができる（例えば、決済ネットワークサブシステム３６０と発行銀行サブシステム３７０の間で合意された条件に従って）。取得銀行サブシステム３００と発行銀行サブシステム３７０の間でインターフェースすることによって、決済ネットワークサブシステム３６０は、取得銀行サブシステム３００と各発行銀行サブシステム３７０が直接的に対話しなければならないエンティティの数を減らすことができる。すなわち、金融機関サブシステム３５０の直接的な統合ポイントを最小にするために、決済ネットワークサブシステム３６０は、様々な発行銀行３７０及び／又は様々な取得銀行３００のためのアグリゲータとして機能することができる。金融機関サブシステム３５０は、取得銀行サブシステム３００などの１つ以上の取得銀行も含むことができる。例えば、取得銀行サブシステム３００は、発行銀行サブシステム３７０と同じエンティティであってもよい。

【００９９】

発行銀行サブシステム３７０が許可要求を受信すると（例えば、取得銀行サブシステム３００からデータ６９０として直接的に、又は決済ネットワークサブシステム３６０を介してデータ４０５として間接的に）、決済情報（例えば、デバイス１００の商取引クレデンシャル情報）及び許可要求に含まれる購入量が分析されて、商取引クレデンシャルに関連付けられたアカウントが購入量をカバーするのに十分なクレジットを有するかどうかを判定することができる。十分な資金供給が存在しない場合、発行銀行サブシステム３７０は、否定的な許可応答を取得銀行サブシステム３００に送信することによって、要求されたトランザクションを拒否することができる。しかし、十分な資金供給が存在する場合、発行銀行サブシステム３７０は、肯定的な許可応答を取得銀行サブシステム３００に送信することによって要求されたトランザクションを承認することができ、金融トランザクションは完了され得る。いずれかのタイプの許可応答は、許可応答データ又はトランザクション状態データ６９２として、ユーザ金融サブシステム３５０によって取得銀行サブシステム３００に提供されてもよい（例えば、トランザクション状態データ６９２は、発行銀行サブシステム３７０から取得銀行サブシステム３００へ通信経路３５を介して直接的に提供されてもよく、又はトランザクション状態データ６９２は、通信経路４５を介して発行銀行サブシステム３７０から決済ネットワークサブシステム３６０に提供され得る認可応答データ若しくはトランザクション状態データ４１５に基づいて、決済ネットワークサブシステム３６０から取得銀行サブシステム３００へ、提供されてもよい）。

【０１００】

上述のように、及び図２に示すように、ホスト電子デバイス１００は、音楽プレーヤ（例えば、Ａｐｐｌｅ Ｉｎｃ．ｏｆ Ｃｕｐｅｒｔｉｎｏ，Ｃａｌｉｆｏｒｎｉａによって入手可能なｉＰｏｄ（登録商標））、ビデオプレーヤ、静止画像プレーヤ、ゲームプレーヤ、他のメディアプレーヤ、音楽レコーダ、映画若しくはビデオカメラ若しくはレコーダ、静止カメラ、他のメディアレコーダ、無線、医療機器、家庭用若しくは商業用電気機器、輸送車両計器、楽器、電卓、携帯電話（例えば、Ａｐｐｌｅ Ｉｎｃ．によって入手可能なｉＰｈｏｎｅ（登録商標））、他の無線通信デバイス、携帯端末、リモコン、ページャ、コンピュータ（例えば、デスクトップ、ラップトップ、タブレット（例えば、Ａｐｐｌｅ Ｉｎｃ．によって入手可能なｉＰａｄ（登録商標））、サーバ、など）モニター、テレビ、ステレオ機器、セットアップボックス、セットトップボックス、ブームボックス、モデム、ルーター、プリンター、又はそれらの任意の組み合わせ、を含むことができるが、これらに限定されない。いくつかの実施形態では、電子デバイス１００は、単一の機

能（例えば、金融トランザクションを実行する専用デバイス）を実行することができ、他の実施形態では、電子デバイス１００は、複数の機能を実行することができる（例えば、金融トランザクションを実行し、音楽を演奏し、電話を受け取って送信するデバイス）。電子デバイス１００は、ユーザがどこに移動しても金融トランザクションを実行するように構成され得る、任意のポータブル、モバイル、ハンドヘルド又は小型の電子デバイスであることができる。いくつかの小型電子デバイスは、ｉＰｏｄ（登録商標）などのハンドヘルド電子デバイスのそれよりも小さい形状因子を有することができる。例示的な小型電子デバイスは、時計（例えば、Ａｐｐｌｅ　Ｉｎｃ．によるＡｐｐｌｅ　Ｗａｔｃｈ（商標））、リング、ネックレス、ベルト、ベルト用アクセサリ、ヘッドセット、靴用アクセサリ、バーチャルリアリティデバイス、眼鏡、他のウェアラブル電子機器、スポーツ用具のアクセサリ、フィットネス器具のアクセサリ、鍵チェーン、又はそれらの任意の組み合わせを含むが、これらに限定されない、様々な物体に一体化され得る。あるいは、ホスト電子デバイス１００は携帯可能でなくてもよく、代わりに、概して静止していてもよい。

【０１０１】

図２に示すように、例えば、電子デバイス１００は、プロセッサ１０２、メモリ１０４、通信コンポーネント１０６、電源１０８、入力コンポーネント１１０、出力コンポーネント１１２、アンテナ１１６、及び近距離通信（「ＮＦＣ」）コンポーネント１２０を含むことができる。電子デバイス１００は、デバイス１００の様々な他のコンポーネントから、又はそれらの間で、データ及び／若しくは電力の伝送のための１つ以上の有線若しくは無線の通信リンク又は経路を提供し得る、バス１１８も含むことができる。いくつかの実施形態では、電子デバイス１００の１つ以上のコンポーネントを組み合わせるか又は省略してもよい。更に、電子デバイス１００は、図２には組み合わされていないか又は含まれていない他のコンポーネントを含むことができる。例えば、電子デバイス１００は、図２に示すコンポーネントの任意の他の適切なコンポーネント又はいくつかのインスタンスを含むことができる。簡略化のために、各コンポーネントのうちの１つのみが図２に示されている。

【０１０２】

メモリ１０４は、例えば、ハードドライブ、フラッシュメモリ、読み出し専用メモリ（「ＲＯＭ」）などの永久メモリ、ランダムアクセスメモリ（「ＲＡＭ」）などの半永久的メモリ、任意の他の適切なタイプの記憶コンポーネント、又はそれらの任意の組み合わせを含む１つ以上の記憶媒体を含むことができる。メモリ１０４はキャッシュメモリを含むことができ、それは、電子デバイスアプリケーション用のデータを一時的に記憶するために使用される１つ以上の異なるタイプのメモリであってもよい。メモリ１０４は、電子デバイス１００内に固定的に組込まれてもよく、又は繰り返し、電子デバイス１００に挿入されてそれから取り出され得る１つ以上の適切なタイプのカード（例えば、加入者識別モジュール（「ＳＩＭ」）カード又はセキュアデジタル（「ＳＤ」）メモリカード）に組み込まれてもよい。メモリ１０４は、メディアデータ（例えば、音楽及び画像ファイル）、ソフトウェア（例えば、デバイス１００に機能を実装するためのソフトウェア）、ファームウェア、嗜好情報（例えば、メディア再生嗜好）、ライフスタイル情報（例えば、食品嗜好）、（例えば、運動監視装置によって得られた情報）、トランザクション情報（例えば、クレジットカード情報などの情報）、無線接続情報（例えば、デバイス１００が無線接続を確立することを有効化する情報）、サブスクリプション情報（例えば、ユーザが加入しているポッドキャスト又はテレビ番組又は他のメディアを追跡する情報）、連絡先情報（例えば、電話番号及び電子メールアドレス）、カレンダ情報、任意の他の適切なデータ、又はそれらの任意の組み合わせ、を記憶することができる。

【０１０３】

通信コンポーネント１０６は、任意の適切な通信プロトコルを使用して、デバイス１００が１つ以上の他の電子デバイス又はサーバ又はサブシステム（例えば、１つ以上のサブシステム又はシステム１の他のコンポーネント）と通信できるように提供されてもよい。例えば、通信コンポーネント１０６は、Ｗｉ－Ｆｉ（例えば、８０２．１１プロトコル）

、ＺｉｇＢｅｅ（例えば８０２．１５．４プロトコル）、ＷｉＤｉ（登録商標）、イーサネット（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）低エネルギ（「ＢＬＥ」）（例えば、９００ＭＨｚ、２．４ＧＨｚ及び５．６ＧＨｚ通信システム）、赤外線、伝送制御プロトコル／インターネットプロトコル（「ＴＣＰ／ＩＰ」）（例えば、各ＴＣＰ／ＩＰレイヤーで使用されるプロトコルの任意のもの）、Ｓｔｒｅａｍ Ｃｏｎｔｒｏｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｐｒｏｔｏｃｏｌ（「ＳＣＴＰ」）、Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ（「ＤＨＣＰ」）、ハイパーテキスト伝送プロトコル（「ＨＴＴＰ」）ＢｉｔＴｏｒｒｅｎｔ（商標）、ファイル伝送プロトコル（「ＦＴＰ」）、リアルタイム伝送プロトコル（「ＲＴＰ」）、リアルタイムストリーミングプロトコル（「ＲＴＳＰ」）、リアルタイム制御プロトコル（「ＲＴＣＰ」）、Ｒｅｍｏｔｅ Ａｕｄｉｏ Ｏｕｔｐｕｔ Ｐｒｏｔｏｃｏｌ（「ＲＡＯＰ」）、Ｒｅａｌ Ｄａｔａ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ（商標（「ＲＤＴＰ」）、Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ（「ＵＤＰ」）、セキュアシェルプロトコル（ＳＳＨ）、無線配信システム（「ＷＤＳ」）ブリッジング、無線及び携帯電話及び個人用電子メールデバイス（例えば、ＧＳＭ（登録商標）（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ））によって使用され得る任意の通信プロトコル、ＧＳＭ（登録商標） Ｅｖｏｌｕｔｉｏｎ用のＧＳＭ（登録商標） ｐｌｕｓ Ｅｎｈａｎｃｅｄ Ｄａｔａレート（「ＥＤＧＥ」）、Ｃｏｄｅ Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ（「ＣＤＭＡ」）、Ｏｒｔｈｏｇｏｎａｌ Ｆｒｅｑｕｅｎｃｙ－Ｄｉｖｉｓｉｏｎ Ｍｕｌｔｉｐｌｅ Ａｃｃｅｓｓ（「ＯＦＤＭＡ」）、高速パケットアクセス（「ＨＳＰＡ」）、マルチバンドなど）、低電力Ｗｉｒｅｌｅｓｓ Ｐｅｒｓｏｎａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ（「６ＬｏＷＰＡＮ」）モジュールによって使用され得る任意の通信プロトコル、任意の他の通信プロトコル、又はそれらの任意の組み合わせ、をサポートすることができる。通信コンポーネント１０６は、デバイス１００が別のデバイス（例えば、ホストコンピュータ又はアクセサリデバイス）に通信結合されることを有効化し得る、任意の適切な送受信機回路（例えば、送受信機回路又はバス１１８を介したアンテナ１１６）も含むか、又はそれと電気的に結合されてもよく、それの他のデバイスと無線で、又は（例えば、コネクタポートを使用して）有線接続を介して通信することができる。通信コンポーネント１０６は、任意の適切なデータを任意のリモートサーバ又は他の適切なエンティティに（例えば、任意の適切なインターネット接続に）通信するように動作する場合、オンライン通信コンポーネントと呼ばれてもよい。通信コンポーネント１０６は、電子デバイス１００の地理的位置を判定するように構成され得る。例えば、通信コンポーネント１０６は、地球測位システム（「ＧＰＳ」）、又はセルタワー位置決め技術又はＷｉ－Ｆｉ技術を使用し得る地域の若しくはサイト全体の測位システムを利用することができる。

【０１０４】

電源１０８は、電力を受信及び／又は生成するための、並びにそのような電力を電子デバイス１００の１つ以上のコンポーネントに供給するための、任意の適切な回路を含むことができる。例えば、電源１０８は、電力網に結合され得る（例えば、デバイス１００がポータブルデバイスとして動作していないとき、又はデバイスのバッテリが電気コンセントにおいて発電所によって生成された電力で充電されているとき）。別の例として、電源１０８は、自然のソース（例えば、太陽電池を使用した太陽光発電）から電力を生成するように構成され得る。別の例として、電源１０８は電力を供給するための１つ以上のバッテリを含むことができる、（例えば、デバイス１００がポータブルデバイスとして動作しているとき）。例えば、電源１０８は、電池（例えば、ゲル、ニッケル金属水素化物、ニッケルカドミウム、ニッケル水素、鉛酸、又はリチウムイオン電池）、無停電電源又は連続電源（ＵＰＳ）、及び発電ソースから受信された電力（例えば、発電プラントによって生成され、電気ソケットなどを介してユーザに供給された）電力を処理するための回路、の１つ以上を含むことができる。電力は、交流又は直流として電源１０８によって供給されることが可能であり、特定の特性に電力を変換するか、又は受信電力をそれに限定する

ように処理され得る。例えば、電力は、直流に又は直流から変換されて、平均電力、有効電力、ピーク電力、パルス当たりのエネルギ、電圧、電流（例えば、アンペアで測定された）、又は受信電力の任意の他の特性の１つ以上の値に制約され得る。電源１０８は、例えば、電子デバイス１００又は電子デバイス１００に結合され得る周辺デバイスの必要性又は要求に基づいて、異なる時刻に特定の電力量を要求又は提供するように動作することができる（例えば、バッテリが既に充電されたときではなくバッテリを充電するときにより多くの電力を要求するように）。

【０１０５】

１つ以上の入力コンポーネント１１０は、ユーザがデバイス１００と対話するか又はインターフェースすることを可能にするために提供されてもよい。例えば、入力コンポーネント１１０は、タッチパッド、ダイヤル、クリックホイール、スクロールホイール、タッチ画面、１つ以上のボタン（例えば、キーボード）、マウス、ジョイスティック、トラックボール、マイクロフォン、カメラ、スキャナー（例えば、バーコードスキャナー又はバーコード、ＱＲコード（登録商標）などのコードから製品識別情報を得ることができる任意の他の適切なスキャナー）、近接センサー、光検出器、動きセンサー、バイオメトリックセンサー（例えば、ユーザを認証するために電子デバイス１００にアクセス可能な特徴処理アプリケーションとともに動作する指紋リーダー又は他の特徴認識センサー）及びそれらの組み合わせを含む、様々な形態をとることができる。各入力コンポーネント１１０は、操作デバイス１００に関連付けられた選択を行うか又はコマンドを発行するための１つ以上の専用の制御機能を提供するように構成され得る。

【０１０６】

電子デバイス１００は、デバイス１００のユーザに情報（例えば、グラフィカル、可聴及び／又は触知情報）を提示得る１つ以上の出力コンポーネント１１２も含むことができる。例えば、電子デバイス１００の出力コンポーネント１１２は、オーディオスピーカ、ヘッドフォン、オーディオラインアウト、ビジュアルディスプレイ、アンテナ、赤外線ポート、触覚出力コンポーネント（例えば、タンブラー、バイブレータ、など）、又はそれらの組み合わせを含むが、これらに限定されない、様々な形態をとることができる。

【０１０７】

特定の例として、電子デバイス１００は、出力コンポーネント１１２としてディスプレイ出力コンポーネントを含むことができる。そのようなディスプレイ出力コンポーネントは、ユーザに視覚データを提示するための任意の適切なタイプのディスプレイ又はインターフェースを含むことができる。ディスプレイ出力コンポーネントは、デバイス１００に組込まれたディスプレイ、又はデバイス１００に結合されたディスプレイ（例えば、取り外し可能ディスプレイ）を含むことができる。ディスプレイ出力コンポーネントは、例えば、液晶ディスプレイ（ＬＣＤ）、発光ダイオード（「ＬＥＤ」）ディスプレイ、有機発光ダイオード（「ＯＬＥＤ」）ディスプレイ、表面伝導電子放出ディスプレイディスプレイ（「ＳＥＤ」）、カーボンナノチューブディスプレイ、ナノ結晶ディスプレイ、任意の他の適切なタイプのディスプレイ、又はそれらの組み合わせを含むことができる。あるいは、ディスプレイ出力コンポーネントは、例えば、ビデオプロジェクタ、ヘッドアップディスプレイ、又は３次元（例えば、ホログラフィック）ディスプレイなどの、電子デバイス１００から離れた表面上にコンテンツの表示を提供するための可動ディスプレイ又は投影システムを含むことができる。別の例として、ディスプレイ出力コンポーネントは、コンパクトデジタルカメラ、リフレックスカメラ、又は任意の他の適切な静止又はビデオカメラに見られるタイプのビューファインダなどの、デジタル又は機械的ビューファインダを含むことができる。ディスプレイ出力コンポーネントは、ディスプレイドライバ回路、ディスプレイドライバを駆動する回路、又はその両方を含むことができ、そのようなディスプレイ出力コンポーネントは、プロセッサ１０２の指示下にあり得るコンテンツ（例えば、メディア再生情報、電子デバイス１００に実装されるアプリケーションのアプリケーション画面、進行中の通信動作に関する情報、入ってくる通信要求に関する情報、デバイス動作画面、など）、を表示するように動作することができる。

【０１０８】
１つ以上の入力コンポーネント及び１以上の出力コンポーネントは、本明細書では集合的に入出力（「Ｉ／Ｏ」）コンポーネント又はＩ／Ｏインターフェース（例えば、入力コンポーネント１１０及び出力コンポーネント１１２をＩ／Ｏコンポーネント又はＩ／Ｏインターフェース１１４として）と呼ばれることがあることに留意されたい。例えば、入力コンポーネント１１０及び出力コンポーネント１１２は、ユーザが表示画面をタッチして入力情報を受信することができ、その同じ表示画面を介してユーザに視覚情報を提供することができる、タッチ画面などの単一のＩ／Ｏコンポーネント１１４であることもあり得る。
【０１０９】
電子デバイス１００のプロセッサ１０２は、電子デバイス１００の１つ以上のコンポーネントの動作及び性能を制御するように動作し得る任意の処理回路を含むことができる。例えば、プロセッサ１０２は、入力コンポーネント１１０からの入力信号及び／又は出力コンポーネント１１２を介した駆動出力信号を受信することができる。図２に示すように、プロセッサ１０２は、アプリケーション１０３、アプリケーション１１３、及び／又はアプリケーション１４３などの１つ以上のアプリケーションを実行するために使用されてもよい。各アプリケーション１０３／１１３／１４３は、１つ以上のオペレーティングシステムアプリケーション、ファームウェアアプリケーション、メディア再生アプリケーション、メディア編集アプリケーション、ＮＦＣ低電力モードアプリケーション、バイオメトリック特徴処理アプリケーション、又は任意の他の適切なアプリケーションを含むことができるが、これらに限定されない。例えば、プロセッサ１０２は、アプリケーションコンポーネント１０３／１１３／１４３をユーザインターフェースプログラムとしてロードして、入力コンポーネント１１０又はデバイス１００の他のコンポーネントを介して受信された命令又はデータが、情報が記憶され及び／又は出力コンポーネント１１２を介してユーザに提供され得る方法をどのように操作することができるかを判定することができる。アプリケーション１０３／１１３／１４３は、（例えば、バス１１８を介して）メモリ１０４から、又は（例えば、通信コンポーネント１０６を介して）別のデバイス又はサーバからなど、任意の適切なソースからプロセッサ１０２によってアクセスされてもよい。プロセッサ１０２は、単一のプロセッサ又は複数のプロセッサを含むことができる。例えば、プロセッサ１０２は、少なくとも１つの「汎用」マイクロプロセッサ、汎用と専用のマイクロプロセッサの組み合わせ、命令セットプロセッサ、グラフィックスプロセッサ、ビデオプロセッサ、及び／又は関連チップセット、及び／又は専用マイクロプロセッサ、を含むことができる。プロセッサ１０２は、キャッシュ目的のためにオンボードメモリも含むことができる。
【０１１０】
電子デバイス１００は、近距離通信（「ＮＦＣ」）コンポーネント１２０も含むことができる。ＮＦＣコンポーネント１２０は、電子デバイス１００と小売商サブシステム２００（例えば、小売商決済端末２２０）の間の非接触近接ベースのトランザクション又は通信を有効化する、任意の適切な近接ベース通信メカニズムであってもよい。ＮＦＣコンポーネント１２０は、比較的低いデータレート（例えば、４２４ｋｂｐｓ）で近接距離通信を可能にすることができ、ＩＳＯ／ＩＥＣ７８１６、ＩＳＯ／ＩＥＣ１８０９２、ＥＣＭＡ－３４０、ＩＳＯ／ＩＥＣ２１４８１、ＥＣＭＡ－３５２、ＩＳＯ　１４４４３、及び／又はＩＳＯ　１５６９３などの、任意の適切な標準に準拠することができる。代替で、又は追加で、ＮＦＣコンポーネント１２０は、比較的高いデータレート（例えば、３７０Ｍｂｐｓ）で近接距離通信を可能にすることができ、ＴｒａｎｓｆｅｒＪｅｔ（商標）プロトコルなどの任意の適切な標準に準拠することができる。ＮＦＣコンポーネント１２０又はＮＦＣコンポーネント１２０’と小売商サブシステム２００の間の通信は、ＮＦＣコンポーネントと小売商サブシステム２００の間の、約２～４センチメートルの範囲などの、任意の適切な近接距離の距離内で行われてもよい（例えば、ＮＦＣコンポーネント１２０’と小売商決済端末２２０の間の図１Ａ及び図１Ｂの距離Ｄ参照）、任意の適切な周波数（

例えば、１３．５６ＭＨｚ）で動作することができる。例えば、ＮＦＣコンポーネントのそのような近接距離通信は、ＮＦＣコンポーネントが他のＮＦＣデバイスと通信し、及び／又は無線周波数識別（「ＲＦＩＤ」）回路を有するタグから情報を取得することを可能にし得る磁界誘導を介して行うことができる。そのようなＮＦＣコンポーネントは、商品情報を取得し、決済情報を転送し、他の方法で外部デバイスと通信する方法を提供することができる（例えば、ＮＦＣコンポーネント１２０’と小売商端末２２０の間、及び／又はＮＦＣコンポーネント１２０’とＮＦＣコンポーネント１２０の間で通信する）。

【０１１１】

ＮＦＣコンポーネント１２０は、電子デバイス１００と小売商サブシステム２００の間の非接触近接ベース通信を有効化するための任意の適切なモジュールを含むことができる。図２に示すように、例えば、ＮＦＣコンポーネント１２０は、ＮＦＣデバイスモジュール１３０、ＮＦＣコントローラモジュール１４０、及びＮＦＣメモリモジュール１５０を含むことができる。

【０１１２】

ＮＦＣデバイスモジュール１３０は、ＮＦＣデータモジュール１３２、ＮＦＣアンテナ１３４、及びＮＦＣブースター１３６を含むことができる。ＮＦＣデータモジュール１３２は、非接触近接ベースの又はＮＦＣ通信５の一部として、ＮＦＣコンポーネント１２０によって小売商サブシステム２００に送信され得る任意の適切なデータを含む、ルーティングする、又は他の方法で提供するように構成されてもよい。追加で、又は代替で、ＮＦＣデータモジュール１３２は、非接触近接ベース通信の一部として小売商サブシステム２００からＮＦＣコンポーネント１２０によって受信され得る任意の適切なデータを含む、ルーティングする、又は他の方法で受信するように構成されてもよい（例えば、ＮＦＣコンポーネント１２０’と小売商端末２２０の間の通信５）。

【０１１３】

ＮＦＣ送受信機又はＮＦＣアンテナ１３４は、ＮＦＣデータモジュール１３２から小売商サブシステム２００への及び／又はサブシステム２００からのＮＦＣデータモジュール１３２への通信の通信を一般に有効化する任意の適切なアンテナ又は他の適切な送受信機回路であってもよい。したがって、ＮＦＣアンテナ１３４（例えば、ループアンテナ）は、ＮＦＣコンポーネント１２０の非接触近接ベース通信能力を有効化するために特に設けられてもよい。

【０１１４】

代替で、又は追加で、ＮＦＣコンポーネント１２０は、電子デバイス１００の別の通信コンポーネント（例えば、通信コンポーネント１０６）が利用し得る同じ送受信機回路又はアンテナ（例えば、アンテナ１１６）を利用することができる。例えば、通信コンポーネント１０６は、アンテナ１１６を利用して、電子デバイス１００と別の遠隔エンティティとの間のＷｉ－Ｆｉ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、セルラー、又はＧＰＳ通信を有効化することができ、一方、ＮＦＣコンポーネント１２０は、アンテナ１１６を利用して、ＮＦＣデバイスモジュール１３０のＮＦＣデータモジュール１３２と別のエンティティ（例えば、小売商サブシステム２００）の間の非接触近接ベース又はＮＦＣ通信を有効化することができる。そのような実施形態では、ＮＦＣデバイスモジュール１３０は、ＮＦＣコンポーネント１２０のデータ（例えば、ＮＦＣデータモジュール１３２内のデータ）に適切な信号増幅を提供するように構成され得るＮＦＣブースター１３６を含むことができ、そのようなデータは、共有アンテナ１１６によってサブシステム２００への通信として適切に送信され得る。例えば、共有アンテナ１１６は、電子デバイス１００と小売商サブシステム２００の間の非接触近接ベース又はＮＦＣ通信を通信するためにアンテナ１１６（例えば、非ループアンテナ）が適切に有効化され得る前に、ブースター１３６からの増幅を必要とする場合がある（例えば、より多くの電力が、アンテナ１１６を使用して他のタイプのデータを送信するために必要とされ得るのではなく、アンテナ１１６を使用してＮＦＣデータを送信するために、必要とされ得る）。

【０１１５】

ＮＦＣコントローラモジュール１４０は、少なくとも１つのＮＦＣプロセッサモジュール１４２を含むことができる。ＮＦＣプロセッサモジュール１４２は、ＮＦＣデバイスモジュール１３０とともに動作して、電子デバイス１００と小売商サブシステム２００の間のＮＦＣ通信を通信するためにＮＦＣコンポーネント１２０を有効化、起動、許可、及び／又は他の方法で制御することができる。ＮＦＣプロセッサモジュール１４２は、別個のコンポーネントとして存在してもよく、別のチップセットに一体化されてもよく、又は例えばチップ上のシステム（「ＳｏＣ」）の一部としてプロセッサ１０２と一体化されてもよい。図２に示すように、ＮＦＣコントローラモジュール１４０のＮＦＣプロセッサモジュール１４２は、ＮＦＣコンポーネント１２０の機能を指示するのに役立ち得るＮＦＣ低電力モード又はウォレットアプリケーション１４３などの、１つ以上のアプリケーションを実行するために使用されてもよい。アプリケーション１４３は、１つ以上のオペレーティングシステムアプリケーション、ファームウェアアプリケーション、ＮＦＣ低電力アプリケーション、又はＮＦＣコンポーネント１２０（例えば、アプリケーション１０３／１１３）にアクセス可能であり得る任意の他の適切なアプリケーションを含むことができるが、これらに限定されない。ＮＦＣコントローラモジュール１４０は、別のＮＦＣデバイス（例えば、小売商サブシステム２００）と通信するために、Ｎｅａｒ Ｆｉｅｌｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｉｎｔｅｒｆａｃｅ ａｎｄ Ｐｒｏｔｏｃｏｌｓ（「ＮＦＣＩＰ－１」）などの１つ以上のプロトコルを含むことができる。プロトコルは、通信速度を適応させ、近距離通信を制御するイニシエータデバイスとして接続されたデバイスの１つを指定するために使用されてもよい。

【０１１６】

ＮＦＣコントローラモジュール１４０は、ＮＦＣコンポーネント１２０の近距離通信モードを制御することができる。例えば、ＮＦＣプロセッサモジュール１４２は、別のＮＦＣ対応デバイス（例えば、小売商サブシステム２００）とデータを交換するためのピアツーピアモード（例えば、通信５）である、ＮＦＣタグから（例えば、小売商サブシステム２００から）ＮＦＣデータモジュール１３２への情報を読み取るためのリーダー／ライターモード（例えば、通信５）と、別のＮＦＣ有効化デバイス（例えば、小売商サブシステム２００）がＮＦＣデータモジュール１３２から情報を読み取る（例えば、通信５）ことを有効化するためのカードエミュレーションモードの間で、ＮＦＣデバイスモジュール１３０を切り替えるように構成されてもよい。ＮＦＣコントローラモジュール１４０は、ＮＦＣコンポーネント１２０をアクティブとパッシブモードの間で切り替えるようにも構成され得る。例えば、ＮＦＣプロセッサモジュール１４２は、ＮＦＣデバイスモジュール１３０が自身のＲＦフィールドを生成し得るアクティブモードと、ＮＦＣデバイスモジュール１３０が負荷変調を使用してデータをＲＦフィールドを生成する別のデバイス（例えば、小売商サブシステム２００）に転送することができるパッシブモードの間で、ＮＦＣデバイスモジュール１３０を（例えば、ＮＦＣアンテナ１３４又は共用アンテナ１１６とともに）切り替えるように構成されてもよい。そのようなパッシブモードでの動作は、そのようなアクティブモードでの動作と比較して、電子デバイス１００のバッテリ寿命を延ばすことができる。ＮＦＣデバイスモジュール１３０のモードは、ユーザの好みに基づいて、及び／又はデバイス１００上で動作するアプリケーション（例えば、アプリケーション１０３及び／又はアプリケーション１４３）によって定義されるか、又は指示され得るデバイス１００の製造者の好みに基づいて、制御されてもよい。

【０１１７】

ＮＦＣメモリモジュール１５０は、ＮＦＣデバイスモジュール１３０及び／又はＮＦＣコントローラモジュール１４０とともに動作して、電子デバイス１００と小売商サブシステム２００間のＮＦＣ通信を可能にすることとができる。ＮＦＣメモリモジュール１５０は、ＮＦＣデバイスハードウェア内に、又はＮＦＣ集積回路（「ＩＣ」）内に組込まれてもよい。ＮＦＣメモリモジュール１５０は、耐改ざん性であってもよく、セキュアエレメントの少なくとも一部を提供してもよい。例えば、ＮＦＣメモリモジュール１５０は、ＮＦＣコントローラモジュール１４０によってアクセスされ得るＮＦＣ通信（例えば、アプ

リケーション１４３）に関する１つ以上のアプリケーションを記憶することができる。例えば、そのようなアプリケーションは、金融決済アプリケーション、セキュアアクセスシステムアプリケーション、ポイントカードアプリケーション、及び暗号化され得る他のアプリケーションを含むことができる。いくつかの実施形態では、ＮＦＣコントローラモジュール１４０及びＮＦＣメモリモジュール１５０は、独立して又は組み合わせて、電子デバイス１００上で機密アプリケーションを記憶及び実行するために使用されるように意図されたオペレーティングシステム、メモリ、アプリケーション環境、及びセキュリティプロトコルを含み得る専用マイクロプロセッサシステムを提供することができる。ＮＦＣコントローラモジュール１４０及びＮＦＣメモリモジュール１５０は、独立して又は組み合わせて、耐改ざん性であり得るセキュアエレメント１４５の少なくとも一部を提供することができる。例えば、そのようなセキュアエレメント１４５は、十分に識別された信頼された権限（例えば、金融機関サブシステムの権限及び／又はＧｌｏｂａｌＰｌａｔｆｏｒｍなどの業界標準）によって設定され得る規則及びセキュリティ要件に従って、アプリケーション及びそれらの機密及び暗号データ（例えば、アプレット１５３及び１５５）をセキュアにホスティングすることができる耐改ざん性のプラットフォーム（例えば、単一又は複数のチップセキュアマイクロコントローラとして）を提供するように構成されてもよい。ＮＦＣメモリモジュール１５０は、メモリ１０４の一部、又はＮＦＣコンポーネント１２０に固有の少なくとも１つの専用チップであってもよい。ＮＦＣメモリモジュール１５０は、ＳＩＭ、電子デバイス１００のマザーボード上の専用チップ、又はメモリカード内の外部プラグとして存在することができる。ＮＦＣメモリモジュール１５０は、ＮＦＣコントローラモジュール１４０から完全に独立していてもよく、デバイス１００の異なるコンポーネントによって提供されてもよく、及び／又は異なる取り外し可能なサブシステムによって電子デバイス１００に提供されてもよい。セキュアエレメント１４５は、機密データ又はアプリケーションを電子デバイス１００に記憶するために使用され得る、チップ内の非常にセキュアな耐改ざん性のハードウェアコンポーネントであってもよい。セキュアエレメント１４５の少なくとも一部は、ユニバーサル集積回路カード（「ＵＩＣＣ」）又は加入者識別モジュール（「ＳＩＭ」）カードなどの取り外し可能な回路カード内に設けられてもよく、それは、移動体通信用グローバルシステム（「ＧＳＭ（登録商標）」）ネットワーク、ユニバーサル移動体通信システム（「ＵＭＴＳ」）及び／又はロングタームエボリューション（「ＬＴＥ」）標準ネットワーク内で互換性のある電子デバイス１００において使用され得る。代替で、又は追加で、セキュアエレメント１４５の少なくとも一部は、デバイス１００の製造中に電子デバイス１００に組込まれ得る集積回路内に設けられてもよい。代替で、又は追加で、セキュアエレメント１４５の少なくとも一部は、マイクロセキュアデジタル（「ＳＤ」）メモリカードなどの電子デバイス１００に差し込まれ、挿入され、又は他の方法で結合され得る周辺デバイス内に設けられてもよい。

【０１１８】

図２に示すように、ＮＦＣメモリモジュール１５０は、ＮＦＣ仕様規格（例えば、ＧｌｏｂａｌＰｌａｔｆｏｒｍ）によって定義され管理され得る、発行者セキュリティドメイン（「ＩＳＤ」）１５２及び追加セキュリティドメイン（「ＳＳＤ」）１５４（例えば、サービスプロバイダセキュリティドメイン（「ＳＰＳＤ」）、信頼されたサービスマネージャセキュリティドメイン（「ＴＳＭＳＤ」）、など）の１つ以上を含むことができる。例えば、ＩＳＤ１５２は、ＮＦＣメモリモジュール１５０の一部であってもよく、そこにおいて、信頼されたサービスマネージャ（「ＴＳＭ」）又は発行金融機関（例えば、商業エンティティサブシステム４００及び／又は金融機関サブシステム３５０）は、クレデンシャルコンテンツ管理、及び／又はセキュリティドメイン管理のために、鍵及び／又は他の適切な情報を記憶して、電子デバイス１００上で（例えば、通信コンポーネント１０６を介して）、１つ以上のクレデンシャル（例えば、様々なクレジットカード、銀行カード、ギフトカード、アクセスカード、トランジットパス、デジタル通貨（例えば、ビットコイン及び関連付けられた決済ネットワーク）、などと関連付けられた商取引クレデンシャル）を生成するか又は他の方法でプロビジョニングすることができる。特定の追加セキュ

リティドメイン（「ＳＳＤ」）１５４（例えば、ＳＳＤ１５４ａ）は、特定のＴＳＭ及び少なくとも１つの特定の商取引クレデンシャル（例えば、特定のクレジットカードクレデンシャル又は公衆トランジットカードクレデンシャル）と関連付けられてもよく、それは、電子デバイス１００に特定の特権又は決済権利を提供することができる。例えば、第１の決済ネットワークサブシステム３６０（例えば、Ｖｉｓａ）は、第１のＳＳＤ１５４ａのＴＳＭであり、第１のＳＳＤ１５４ａのアプレット１５３ａは、その第１の決済ネットワークサブシステム３６０によって管理される商取引クレデンシャルと関連付けられ得るが、第２の決済ネットワークサブシステム３６０（例えば、マスターカード）は、別のＳＳＤ１５４のＴＳＭであってもよい。

【０１１９】

ＮＦＣコンポーネント１２０の使用を有効化するために（例えば、デバイス１００にプロビジョニングされた商取引クレデンシャルのアクティブ化を有効化するために）セキュリティ機能を設けることができ、それは、クレジットカード情報又はクレデンシャルの銀行口座情報などの機密決済情報を、電子デバイス１００から小売商サブシステム２００に送信するときに、特に有用であり得る。そのようなセキュリティ機能は、制限されたアクセスを有し得るセキュア記憶領域も含むことができる。例えば、個人識別番号（「ＰＩＮ」）入力を介した、又はバイオメトリックセンサーとのユーザ対話を介したユーザ認証が、セキュア記憶領域にアクセスするために（例えば、ユーザがセキュアエレメントのセキュリティドメインエレメントのライフサイクル状態を変更するために）提供される必要があり得る。特定の実施形態では、セキュリティ機能の一部又は全部をＮＦＣメモリモジュール１５０内に記憶することができる。更に、サブシステム２００と通信するための、認証鍵などのセキュリティ情報は、ＮＦＣメモリモジュール１５０内に記憶されてもよい。特定の実施形態では、ＮＦＣメモリモジュール１５０は、電子デバイス１００内に組込まれたマイクロコントローラを含むことができる。

【０１２０】

図１Ｂの小売商サブシステム２００の小売商端末２２０は、電子デバイス１００又は電子デバイス１００’（例えば、クライアントデバイス１００’が小売商端末２２０の特定の距離又は近傍内に来たときの通信５）から、ＮＦＣ通信を検出、読み取り、又は受信するためのリーダーを含むことができる。したがって、そのような小売商端末と電子デバイス１００／１００’の間のＮＦＣ通信は無線で行われてもよく、したがって、それぞれのデバイス間に明確な「見通し線」を必要としなくてもよいことに留意されたい。上述のように、ＮＦＣデバイスモジュール１３０はパッシブ又はアクティブであってもよい。パッシブである場合、ＮＦＣデバイスモジュール１３０は、そのような小売商端末の適切なリーダーの応答範囲内にあるときにのみ起動され得る。例えば、そのような小売商端末のリーダーは、ＮＦＣデバイスモジュール１３０（例えば、共用アンテナ１１６又はＮＦＣ特有のアンテナ１３４）によって利用されるアンテナに電力を供給するために使用され得る比較的低電力の電波フィールドを放出し、それによって、そのアンテナが、適切なＮＦＣ通信情報（例えば、クレジットカードクレデンシャル情報）を、ＮＦＣデータモジュール１３２から、アンテナ１１６又はアンテナ１３４を介して、ＮＦＣ通信などの小売商端末に、送信することを有効化することができる。アクティブである場合、ＮＦＣデバイスモジュール１３０は、電子デバイス１００（例えば、電源１０８）にローカルな電源を組み込むか又はそれにアクセスすることができ、それは、共用アンテナ１１６又はＮＦＣ特有のアンテナ１３４が、パッシブＮＦＣデバイスモジュール１３０の場合のように、無線周波数信号を反射するのではなく、ＮＦＣ通信情報（例えば、クレジットカードクレデンシャル情報）を、ＮＦＣデータモジュール１３２からアンテナ１１６又はアンテナ１３４を介して、ＮＦＣ通信として小売商端末２２０にアクティブに送信することを有効化することができる。小売商端末２２０は、（例えば店舗でデバイス１００’のユーザに製品又はサービスを直接的に販売するために小売商の店内にある）小売商サブシステム２００の小売商によって提供されてもよい。近距離通信に関してＮＦＣコンポーネント１２０を記載してきたが、コンポーネント１２０は、電子デバイス１００とそのような小売商端末の間の任意

の適切な非接触近接ベースのモバイル決済又は任意の他の適切なタイプの非接触近接ベース通信を提供するように構成されてもよいことが理解されるべきである。例えば、ＮＦＣコンポーネント１２０は、電磁気／静電結合技術を含むものなどの、適切な短距離通信を提供するように構成されてもよい。

【０１２１】

近距離通信に関してＮＦＣコンポーネント１２０を記載してきたが、コンポーネント１２０は、電子デバイス１００と小売商サブシステム２００の間の任意の適切な非接触近接ベースのモバイル決済又は任意の他の適切なタイプの非接触近接ベース通信を提供するように構成されてもよいことが理解されるべきである。例えば、ＮＦＣコンポーネント１２０は、電磁気／静電結合技術を含むものなどの、適切な短距離通信を提供するように構成されてもよい。更に、いくつかの実施形態では、クライアントデバイス１００’のＮＦＣコンポーネント１２０’は、ホストデバイス１００のＮＦＣコンポーネント１２０と同じか又は実質的に同じであってもよい。あるいは、いくつかの実施形態では、クライアントデバイス１００’のＮＦＣコンポーネント１２０’は、プロセッサ１０２’又はデバイス１００’の任意の他の部分に利用有効化し得る任意の適切なコンポーネントを含むように構成されて、クライアントデバイス１００’のＮＦＣコンポーネント１２０’と小売商サブシステム２００の小売商端末２２０の間で、任意の適切な非接触近接ベース通信として通信され得るが、ＮＦＣコンポーネント１２０’は、ホストデバイス１００にネーティブクレデンシャルデータなどの金融トランザクションにセキュアに資金を供給するために、クライアントデバイス１００’上にセキュアクレデンシャルデータを生成するためのクレデンシャルアプレットをセキュアに記憶するように動作するセキュアエレメントを含んでも含まなくてもよい。

【０１２２】

電子デバイス１００は、デバイス１００の外部の破片及び他の劣化させる力からの保護のために、デバイス１００の１つ以上のコンポーネントを少なくとも部分的に囲み得る筐体１０１も設けられてもよい。いくつかの実施形態では、１つ以上のコンポーネントは、それ自体の筐体内に設けられてもよい（例えば、入力コンポーネント１１０は、無線で又は有線を介して、それ自身の筐体内に設けられ得るプロセッサ１０２と通信することができる独立したキーボード又はマウスであってもよい）。任意のクライアントデバイス１００’は、電子デバイス１００に関して記載された特徴の１つ、いくつか、若しくは全てを含むことができ、及び／又は電子デバイス１００に関して記載されていない追加の特徴を含むことができることが理解されるべきである。任意のホストデバイス１００又は任意のクライアントデバイス１００’は、互いにともに動作する２つ以上のデバイス（例えば、任意の適切な近接通信プロトコル（例えば、ＢｌｕｅＴｏｏｔｈ（登録商標）を介して通信結合された携帯電話及びスマート時計）の組み合わせとして提供されてもよいことも理解されるべきである。

【０１２３】

上述のように、及び図３に示すように、電子デバイス１００の１つの特定の例は、ｉＰｈｏｎｅ（登録商標）などのハンドヘルド電子デバイスであってもよく、筐体１０１が、様々な入力コンポーネント１１０ａ～１１０ｉ、様々な出力コンポーネント１１２ａ～１１２ｃ、及び様々なＩ／Ｏコンポーネント１１４ａ～１１４ｄへのアクセスを可能にすることができ、それらを介して、デバイス１００及びユーザ及び／又は周囲環境が相互にインターフェースすることができる。入力コンポーネント１１０ａは、押圧されると、現在実行中のアプリケーションの「ホーム」画面又はメニューをデバイス１００によって表示させるボタンを含むことができる。入力コンポーネント１１０ｂは、電子デバイス１００をスリープモードとウェークモードの間で、又は任意の他の適切なモードの間でトグルするためのボタンであってもよい。入力コンポーネント１１０ｃは、電子デバイス１００の特定のモードで１つ以上の出力コンポーネント１１２を無効にし得る２位置スライダーを含むことができる。入力コンポーネント１１０ｄ及び１１０ｅは、電子デバイス１００の出力コンポーネント１１２のボリューム出力又は他の特性出力を増減するためのボタンを

含むことができる。入力コンポーネント１１０ａ～１１０ｅの各１つは、ドームスイッチ、スライドスイッチ、制御パッド、鍵、ノブ、スクロールホイール、又は任意の他の適切な形態によって支持されたボタンなどの機械式入力コンポーネントであってもよい。

【０１２４】

出力コンポーネント１１２ａは、ユーザが電子デバイス１００と対話することを可能にする視覚的又はグラフィックのユーザインターフェース（「ＧＵＩ」）１８０を表示するのに使用され得るディスプレイであってもよい。ＧＵＩ１８０は、現在実行中のアプリケーション（例えば、アプリケーション１０３及び／又はアプリケーション１１３及び／又はアプリケーション１４３）の様々なレイヤー、ウィンドウ、画面、テンプレート、エレメント、メニュー、及び／又は他のコンポーネントを含むことができ、それらは、ディスプレイ出力コンポーネント１１２ａのエリアの全て又はいくつかに表示され得る。例えば、図３に示すように、ＧＵＩ１８０は、第１の画面１９０を表示するように構成されてもよい。１つ以上のユーザ入力コンポーネント１１０ａ～１１０ｉが、ＧＵＩ１８０を介してナビゲートするのに使用されてもよい。例えば、１つのユーザ入力コンポーネント１１０は、ユーザがＧＵＩ１８０の１つ以上のグラフィカルエレメント又はアイコン１８２を選択することを可能にし得るスクロールホイールを含むことができる。アイコン１８２は、ディスプレイ出力コンポーネント１１２ａ及び関連付けられたタッチ入力コンポーネント１１０ｆを含み得るタッチ画面Ｉ／Ｏコンポーネント１１４ａを介して選択されてもよい。そのようなタッチ画面Ｉ／Ｏコンポーネント１１４ａは、抵抗性、容量性、赤外線、表面弾性波、電磁気、又は近接場撮像などの任意の適切なタイプのタッチ画面入力技術を用いることができる。更に、タッチ画面Ｉ／Ｏコンポーネント１１４ａは、シングルポイント又はマルチポイント（例えば、マルチタッチ）入力感知を使用することができる。

【０１２５】

アイコン１８２は、ユーザによる選択の際にディスプレイコンポーネント１１２ａの一部又は全てのエリアに表示され得る様々なレイヤー、ウィンドウ、画面、テンプレート、エレメント、及び／又は他のコンポーネントを表すことができる。更に、特定のアイコン１８２の選択は、階層ナビゲーションプロセスに導くことができる。例えば、特定のアイコン１８２の選択は、同じアプリケーション又はそのアイコン１８２に関連付けられた新しいアプリケーションの１つ以上の追加のアイコン又は他のＧＵＩエレメントを含むＧＵＩ１８０の新しい画面に導くことができる。各アイコン１８２の上又は近傍にテキストインジケータ１８１を表示して、各グラフィカルエレメントアイコン１８２のユーザの解釈を容易にすることができる。ＧＵＩ１８０は、階層レイヤー構造及び／又は非階層レイヤー構造に配置された様々なコンポーネントを含み得ることが理解されるべきである。特定のアイコン１８２が選択されると、デバイス１００は、そのアイコン１８２に関連付けられた新しいアプリケーションを開き、そのアプリケーションに関連付けられたＧＵＩ１８０の対応する画面を表示するように構成され得る。例えば、「小売商アプリケーション」テキストインジケータ１８１（すなわち、特定のアイコン１８３）で標識された特定のアイコン１８２が選択された場合、デバイス１００は、特定の小売商アプリケーションを起動するか又は他の方法でそれにアクセスすることができ、デバイス１００と特定の方法で対話するための１つ以上のツール又は機能を含み得る特定のユーザインターフェースの画面を表示することができる。各アプリケーションに対して、画面は、ディスプレイ出力コンポーネント１１２ａ上に表示されることが可能であり、様々なユーザインターフェースエレメント（例えば、図３Ａ～図３Ｈの画面１９０ａ～１９０ｈ）を含むことができる。追加で、又は代替で、各アプリケーションに対して、様々な他のタイプの非可視情報を、デバイス１００の様々な他の出力コンポーネント１１２を介してユーザに提供することができる。様々なＧＵＩ１８０に関して記載された動作は、多種多様なグラフィカルエレメント及び視覚的スキームを用いて実現され得る。したがって、記載された実施形態は、本明細書で採用された正確なユーザインターフェース協定に限定されることを意図されない。むしろ、実施形態は、多種多様なユーザインターフェーススタイルを含むことができる。

【０１２６】

電子デバイス１００は、デバイス１００と他のデバイスの間の通信を可能にし得る様々な他のＩ／Ｏコンポーネント１１４も含むことができる。Ｉ／Ｏコンポーネント１１４ｂは、リモートデータソース及び／又は外部電源からの電力から、メディアファイル又は顧客注文ファイルなどのデータファイルを送受信するように構成され得る接続ポートであってもよい。例えば、Ｉ／Ｏコンポーネント１１４ｂは、Ａｐｐｌｅ Ｉｎｃ．ｏｆ Ｃｕｐｅｒｔｉｎｏ，ＣａｌｉｆｏｒｎｉａからのＬｉｇｈｔｎｉｎｇ（商標）コネクタ又は３０ピンドックコネクタなどの専用ポートであってもよい。Ｉ／Ｏコンポーネント１１４ｃは、ＳＩＭカード又は任意の他のタイプの取り外し可能なコンポーネントを受けるための接続スロットであってもよい。Ｉ／Ｏコンポーネント１１４ｄは、マイクコンポーネントを含んでも含まなくてもよいオーディオヘッドフォンを接続するためのヘッドフォンジャックであってもよい。電子デバイス１００は、マイクロフォンなどの少なくとも１つのオーディオ入力コンポーネント１１０ｇ、及びオーディオスピーカなどの少なくとも１つのオーディオ出力コンポーネント１１２ｂも含むことができる。

【０１２７】

電子デバイス１００は、少なくとも１つの触覚又は触知出力コンポーネント１１２ｃ（例えば、タンブラー）、カメラ及び／又はスキャナー入力コンポーネント１１０ｈ（例えば、ビデオ又は静止カメラ、及び／又はバーコードスキャナー又はバーコード、ＱＲコード（登録商標）、などのコードから製品識別情報を取得し得る任意の他の適切なスキャナー）、及びバイオメトリック入力コンポーネント１１０ｉ（例えば、ユーザを認証するために電子デバイス１００にアクセス可能であり得る特徴処理アプリケーションとともに動作し得る、指紋リーダー又は他の特徴認識センサー）も含むことができる。図３に示すように、バイオメトリック入力コンポーネント１１０ｉの少なくとも一部は、デバイス１００の入力コンポーネント１１０ａ又は任意の他の適切な入力コンポーネント１１０に組み込まれるか、又は他の方法で結合され得る。例えば、バイオメトリック入力コンポーネント１１０ｉは、ユーザが、その指で入力コンポーネント１１０ａを押圧することによって、機械式入力コンポーネント１１０ａと対話するときに、ユーザの指の指紋をスキャンするように構成され得る指紋リーダーであってもよい。別の例として、バイオメトリック入力コンポーネント１１０ｉは、タッチ画面Ｉ／Ｏコンポーネント１１４ａのタッチ入力コンポーネント１１０ｆと組み合わせられ得る指紋リーダーであってもよく、バイオメトリック入力コンポーネント１１０ｉは、ユーザが、その指でタッチ画面入力コンポーネント１１０ｆを押圧するか又はそれに沿ってスライドさせることによって、タッチ画面入力コンポーネント１１０ｆと対話するときに、ユーザの指の指紋をスキャンするように構成され得る。更に、上述のように、電子デバイス１００は、アンテナ１１６及び／又はアンテナ１３４（図３には図示せず）を介してサブシステム２００に通信アクセス可能であり得るＮＦＣコンポーネント１２０を更に含むことができる。ＮＦＣコンポーネント１２０は、筐体１０１内に少なくとも部分的に配置されてもよく、ＮＦＣコンポーネント１２０と関連付けられた１つ以上のアンテナの全体的な位置（例えば、アンテナ１１６及び／又はアンテナ１３４の全体的な位置）を識別し得るマーク又はシンボル１２１を、筐体１０１の外部に設けることができる。

【０１２８】

図１～図１０に関して記載されたプロセスの１つ、いくつか、又は全ては、各々ソフトウェアによって実施され得るが、ハードウェア、ファームウェア、又はソフトウェア、ハードウェア、及びファームウェアの任意の組み合わせでも実施され得る。これらの処理を実行するための命令は、機械又はコンピュータ可読媒体に記録された機械又はコンピュータ可読コードとしても具現化され得る。いくつかの実施形態では、コンピュータ可読媒体は、非一時的コンピュータ可読媒体であってもよい。そのような非一時的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、フラッシュメモリ、ＣＤ－ＲＯＭ、ＤＶＤ、磁気テープ、取り外し可能メモリカード、及びデータ記憶デバイス（例えば、図２のメモリ１０４及び／又はメモリモジュール１５０）が挙げられるが、これらに限定されない。他の実施形態では、コンピュータ可読媒体は、一時的コンピュ

ータ可読媒体であってもよい。そのような実施形態では、一時的コンピュータ可読媒体はネットワーク結合されたコンピュータシステムを介して分散されることが可能であり、コンピュータ可読コードは分散形式で記憶され実行される。例えば、そのような一時的コンピュータ可読媒体は、任意の適切な通信プロトコルを使用して、１つの電子デバイスから別の電子デバイスに通信されてもよい（例えば、コンピュータ可読媒体は、通信コンポーネント１０６を介して電子デバイス１００に通信されてもよい（例えば、アプリケーション１０３の少なくとも一部として、及び／又はアプリケーション１１３の少なくとも一部として、及び／又はアプリケーション１４３の少なくとも一部として））。そのような一時的コンピュータ可読媒体は、コンピュータ可読コード、命令、データ構造、プログラムモジュール、又は搬送波又は他のトランスポート機構などの変調データ信号内の他のデータを具現化することができ、任意の情報配信メディアを含むことができる。変調されたデータ信号は、信号内の情報を符号化するように設定又は変更された１つ以上の特性を有する信号であってもよい。

【０１２９】

システム１の任意の、各、又は少なくとも１つのモジュール又はコンポーネント又はサブシステムは、ソフトウェア構築物、ファームウェア構築物、１つ以上のハードウェアコンポーネント、又はそれらの組み合わせとして提供され得ることが理解されるべきである。例えば、システム１の任意の、各、又は少なくとも１つのモジュール又はコンポーネント又はサブシステムは、１つ以上のコンピュータ又は他のデバイスによって実行され得る、プログラムモジュールなどのコンピュータ実行可能命令の一般的な文脈で、記載されてもよい。一般に、プログラムモジュールは、１つ以上の特定のタスクを実行し得るか、又は１つ以上の特定の抽象データタイプを実装し得る１つ以上のルーチン、プログラム、オブジェクト、コンポーネント、及び／又はデータ構造を含むことができる。システム１のモジュール及びコンポーネント及びサブシステムの数、構成、機能、及び相互接続は単なる例示であり、既存のモジュール、コンポーネント、及び／又はモジュールの数、構成、機能、及び相互接続、及び／又はサブシステムは変更又は省略されてもよく、追加のモジュール、コンポーネント、及び／又はサブシステムが追加されてもよく、特定のモジュール、コンポーネント、及び／又はサブシステムの相互接続が変更されてもよいことも理解されるべきである。

【０１３０】

システム１の１つ以上のモジュール又はコンポーネント又はサブシステムの少なくとも一部は、任意の適切な方法で、システム１のエンティティに記憶されるか、又は他の方法でアクセス可能であってもよい（例えば、デバイス１００のメモリ１０４に（例えば、アプリケーション１０３の少なくとも一部として、及び／又はアプリケーション１１３の少なくとも一部として、及び／又はアプリケーション１４３の少なくとも一部として））。例えば、ＮＦＣコンポーネント１２０の任意の又は各モジュールは、任意の適切な技術（例えば、１つ以上の集積回路デバイス）を使用して実装されてもよく、異なるモジュールは、構造、機能、及び動作が同一であってもなくてもよい。システム１のモジュール又は他のコンポーネント任意のもの又は全ては、拡張カードに搭載されてもよく、システムマザーボードに直接的に搭載されてもよく、又はシステムチップセットコンポーネント（例えば、「ノースブリッジ」チップ）に一体化されてもよい。

【０１３１】

システム１の任意のモジュール又はコンポーネント（例えば、ＮＦＣコンポーネント１２０の任意のモジュール又は各モジュール）は、様々なバス規格に適合された１つ以上の拡張カードを使用して実装される専用システムであってもよい。例えば、全てのモジュールを相互に接続された異なる拡張カードに搭載してもよく、又は全てのモジュールを１つの拡張カードに搭載してもよい。ＮＦＣコンポーネント１２０に関して、単に例として、ＮＦＣコンポーネント１２０のモジュールは、拡張スロット（例えば、周辺コンポーネント相互接続（ＰＣＩ）スロット又はＰＣＩ　ｅｘｐｒｅｓｓスロット）を介してデバイス１００のマザーボード又はプロセッサ１０２とインターフェースすることができる。ある

いは、ＮＦＣコンポーネント１２０は取り外し可能である必要はなく、モジュールの利用に専用のメモリ（例えば、ＲＡＭ）を含み得る１つ以上の専用モジュールを含むことができる。他の実施形態では、ＮＦＣコンポーネント１２０はデバイス１００に一体化されてもよい。例えば、ＮＦＣコンポーネント１２０のモジュールは、デバイス１００のデバイスメモリ１０４の一部を利用することができる。システム１の任意のモジュール又はコンポーネント（例えば、ＮＦＣコンポーネント１２０の任意のモジュール又は各モジュール）は、それ自体の処理回路及び／又はメモリを含むことができる。あるいは、システム１の任意のモジュール又はコンポーネント（例えば、ＮＦＣコンポーネント１２０の任意の又は各モジュール）は、処理回路及び／又はメモリを、ＮＦＣコンポーネント１２０並びに／又はデバイス１００のプロセッサ１０２及び／若しくはメモリ１０４の任意の他のモジュールと共有することができる。

【０１３２】

上述のように、デバイス１００の入力コンポーネント１１０（例えば、入力コンポーネント１１０ｆ）は、有線又は無線バス１１８を介してデバイス１００の他のコンポーネントと対話するためのタッチ入力を受信し得るタッチ入力コンポーネントを含むことができる。そのようなタッチ入力コンポーネント１１０は、キーボード、マウス、などの他の入力コンポーネントの代わりに、又はそれらと組み合わせて、デバイス１００にユーザ入力を提供するために使用されてもよい。

【０１３３】

タッチ入力コンポーネント１１０は、全体的又は部分的に透明、半透明、非透明、不透明、又はそれらの任意の組み合わせであり得るタッチ感知パネルを含むことができる。タッチ入力コンポーネント１１０は、タッチ画面、タッチパッド、タッチパッドとして機能するタッチ画面（例えば、ラップトップのタッチパッドに置き代わるタッチ画面）、任意の他の入力デバイスと組み合わされた若しくはそれに組み込まれたタッチパッド又はタッチパッド（例えば、キーボード上に配置されたタッチ画面又はタッチパッド）、又はタッチ入力を受信するためのタッチ感知面を有する任意の多次元オブジェクト、として具現化されてもよい。いくつかの実施形態では、タッチ感知面及びタッチパッドという用語は互換的に使用されてもよい。

【０１３４】

いくつかの実施形態では、タッチ画面として具現化されたタッチ入力コンポーネント１１０は、ディスプレイの少なくとも一部（例えば、ディスプレイ出力コンポーネント１１２ａ）の上、下、及び／又は中に部分的に又は全体的に配置された透明及び／又は半透明のタッチ感知パネルを含むことができる。他の実施形態では、タッチ入力コンポーネント１１０は、タッチ感知コンポーネント／デバイスがディスプレイコンポーネント／デバイスと一体である一体型タッチ画面として具現化されてもよい。更に他の実施形態では、タッチ入力コンポーネント１１０は、主ディスプレイの追加又はそれと同じグラフィカルデータを表示するために、及びタッチ入力を受信するために、追加又は更なるディスプレイ画面として使用されてもよい。

【０１３５】

タッチ入力コンポーネント１１０は、容量性、抵抗性、光学的、音響的、誘導的、機械的、化学的測定値、又は入力コンポーネント１１０に近接して１つ以上のタッチ又はニアタッチの発生に対して測定され得る任意の現象に基づいて、１つ以上のタッチ又はニアタッチの位置を検出するように構成されてもよい。ソフトウェア、ハードウェア、ファームウェア、又はそれらの任意の組み合わせを使用して、検出されたタッチの測定値を処理して、１つ以上のジェスチャーを識別及び追跡することができる。ジェスチャーは、タッチ入力コンポーネント１１０上の定常の若しくは非定常の、単一の若しくは複数のタッチ又はニアタッチに対応することができる。ジェスチャーは、タッピング、押圧、揺動、スクラビング、回転、ねじり、向きの変更、圧力の変化を伴う押圧などの、タッチ入力コンポーネント１１０上の特定の方法で、１つ以上の指又は他の物体を、本質的に同時に、継続的に、又は連続的に、動かすことによって実行され得る。ジェスチャーは、任意の他の指

（単数又は複数）の間の又はそれを用いた、挟み込み、引っ張り、摺動、スワイプ、回転、屈曲、引きずり、若しくはタッピングの動作によって特徴付けられ得るが、これらに限定されない。単一のジェスチャーは、１人以上のユーザによる１つ以上の手を用いて、又はその任意の組み合わせによって、実行されてもよい。

【０１３６】

上述のように、電子デバイス１００は、グラフィカルユーザインターフェース（「ＧＵＩ」）１８０を表示するために、グラフィカルデータを用いてディスプレイ（例えば、ディスプレイ出力コンポーネント１１２ａ）を駆動することができる。ＧＵＩ１８０は、タッチ入力コンポーネント１１０ｆを介してタッチ入力を受信するように構成されてもよい。タッチ画面として（例えば、Ｉ／Ｏコンポーネント１１４ａとしてディスプレイ出力コンポーネント１１２ａと共に）具現化された、タッチＩ／Ｏコンポーネント１１０ｆは、ＧＵＩ１８０を表示することができる。あるいは、ＧＵＩ１８０は、タッチ入力コンポーネント１１０ｆとは別個のディスプレイ（例えば、ディスプレイ出力コンポーネント１１２ａ）上に表示されてもよい。ＧＵＩ１８０は、インターフェース内の特定の場所に表示されたグラフィカルエレメントを含むことができる。グラフィカルエレメントは、仮想スクロールホイール、仮想キーボード、仮想ノブ、仮想ボタン、任意の仮想ユーザインターフェース（「ＵＩ」）、などを含む、様々な表示された仮想入力デバイスを含むことができるが、これらに限定されない。ユーザは、ＧＵＩ１８０のグラフィカルエレメントに関連付けられた、タッチ入力コンポーネント１１０ｆ上の１つ以上の特定の場所で、ジェスチャーを実行することができる。他の実施形態では、ユーザは、ＧＵＩ１８０のグラフィカルエレメントの場所に依存しない１つ以上の場所で、ジェスチャーを実行することができる。タッチ入力コンポーネント１１０上で実行されるジェスチャーは、ＧＵＩ内の、カーソル、アイコン、メディアファイル、リスト、テキスト、画像の全部又は一部などのグラフィカルエレメントを、直接的又は間接的に操作し、制御し、修正し、移動させ、起動し、開始させるか、又はそれらに全般的に影響を及ぼすことができる。例えば、タッチ画面の場合、ユーザは、タッチ画面上のグラフィカルエレメントの上でジェスチャーを実行することによって、グラフィカルエレメントと直接的に対話することができる。あるいは、タッチパッドは、一般に、間接的な対話を提供することができる。ジェスチャーは、表示されていないＧＵＩエレメントにも影響を及ぼす（例えば、ユーザインターフェースを表示させる）ことができ、又はデバイス１００の他の動作に影響を及ぼす（例えば、ＧＵＩ、アプリケーション、又はオペレーティングシステムの状態又はモードに影響を及ぼす）ことができる。ジェスチャーは、表示されたカーソルとともに、タッチ入力コンポーネント１１０上で実行されてもされなくてもよい。例えば、タッチパッド上でジェスチャーが実行される場合、ディスプレイ画面又はタッチ画面上に、カーソル又はポインタを表示することができ、タッチパッド上のタッチ入力を介してカーソル又はポインタを制御して、ディスプレイ画面上のグラフィカルオブジェクトと対話することができる。あるいは、ジェスチャーがタッチ画面上で直接的に実行される場合、ユーザは、タッチ画面上に表示されているカーソル又はポインタの有無にかかわらず、タッチ画面上のオブジェクトと直接的に対話することができる。フィードバックは、タッチ入力コンポーネント１１０上のタッチ又はニアタッチに応じて、又はそれに基づいて、バス１１８を介してユーザに提供されてもよい。フィードバックは、光学的に、機械的に、電気的に、嗅覚的に、音響的に、又はこれらの任意の組み合わせで、可変の又は非可変の方式で、送信され得る。

記載された概念の更なるアプリケーション

【０１３７】

非ネーティブクレデンシャルを有する電子デバイスを使用してトランザクションを実行するためのシステム、方法、及びコンピュータ可読媒体が記載されてきたが、本明細書に任意の方法で記載された主題事項の精神及び範囲から逸脱することなく多くの変更を行うことができることが理解されるべきである。現在既知であるか又は後に考案される、当業者から見て、特許請求された主題事項からの本質的でない変更は、特許請求の範囲内と均等であると明示的に考えられる。したがって、当業者に、今後既知となる明白な置換は、

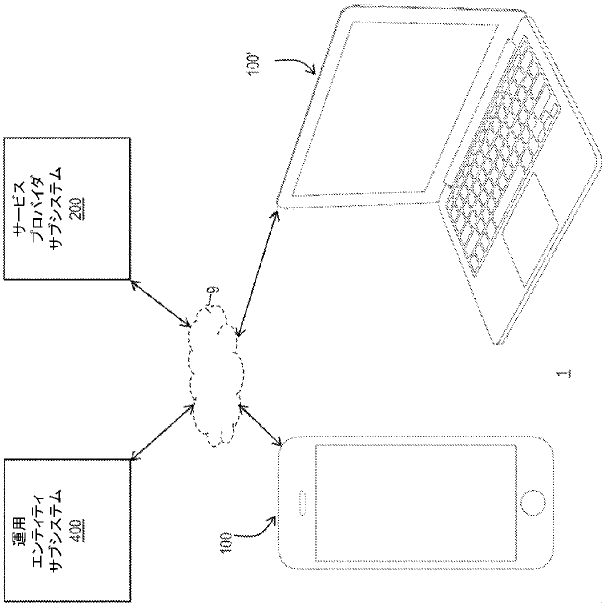
定義されたエレメントの範囲内にあるものと定義される。

【０１３８】

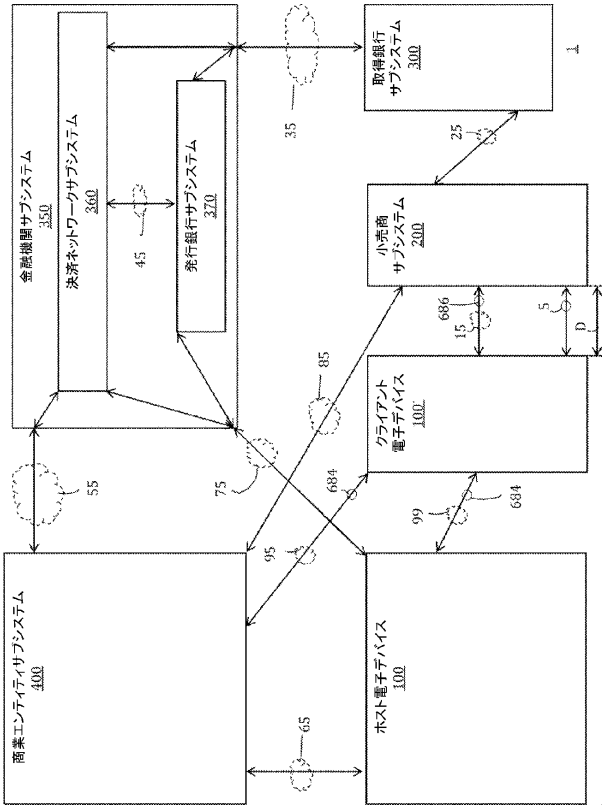
したがって、当業者は、限定ではなく例示のために提示された記載された実施形態以外のものによって、本発明を実施できることを、理解するであろう。

【図面】

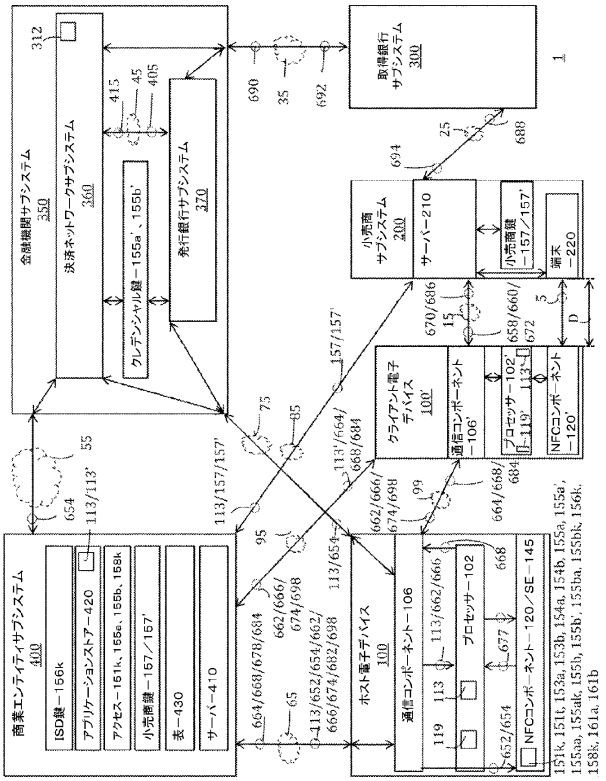
【図１】



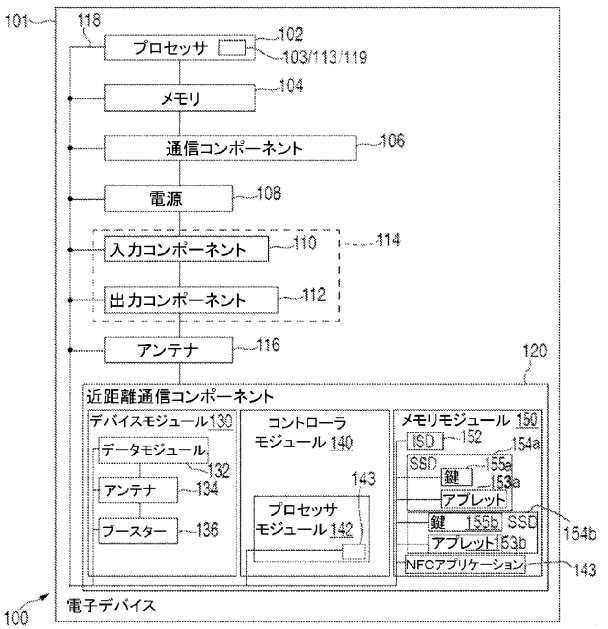

【図１Ａ】



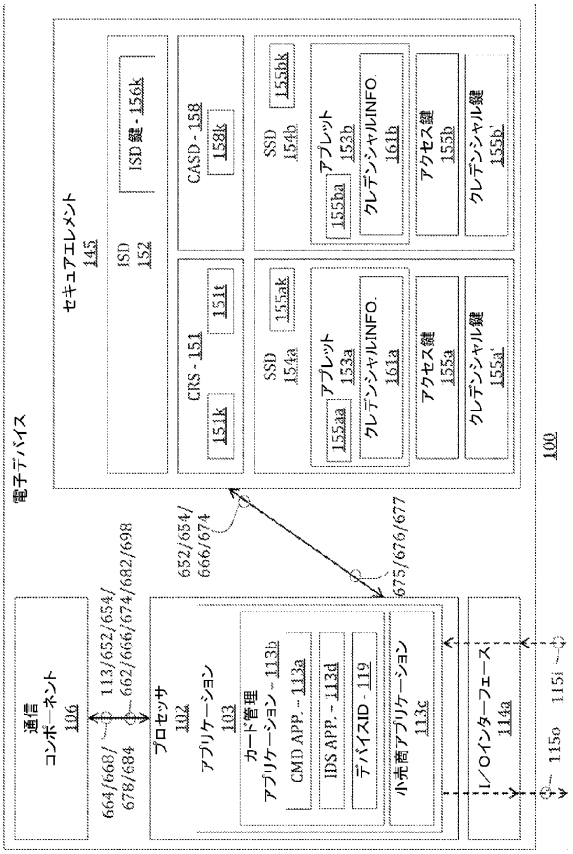

【図１Ｂ】



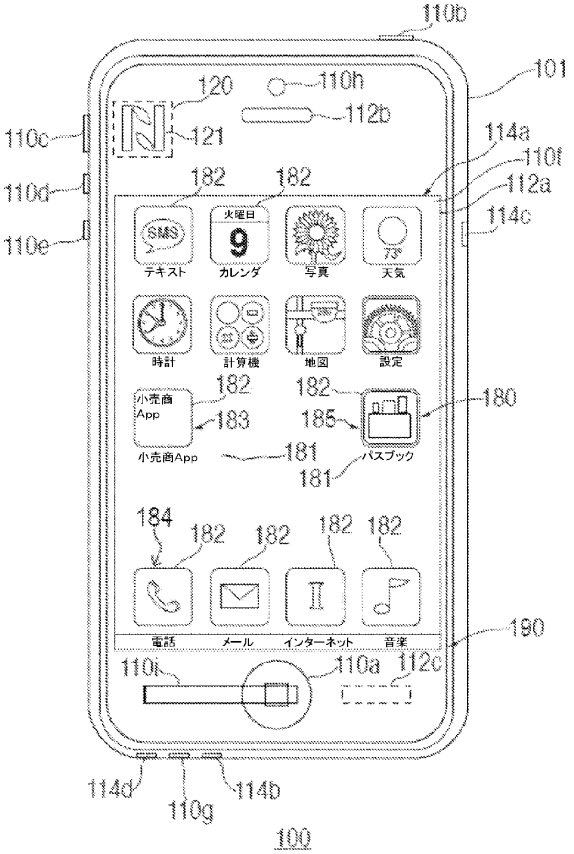

【図２】



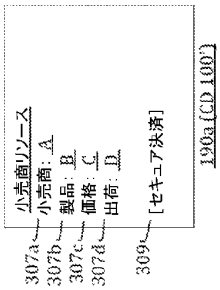
【図２Ａ】



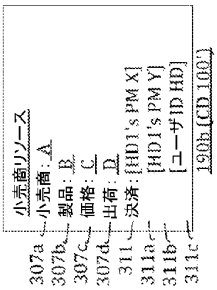

【図３】



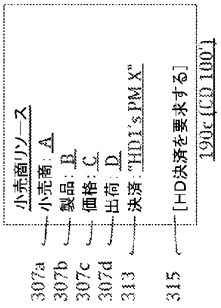

【図３Ａ】



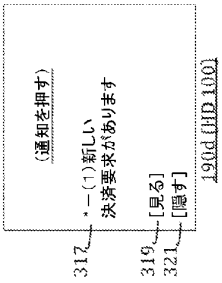

【図３Ｂ】



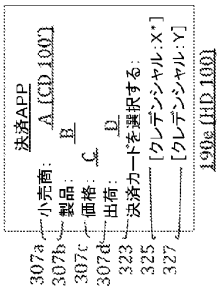
【図３Ｃ】



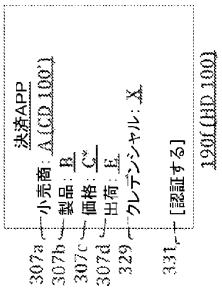

【図３Ｄ】



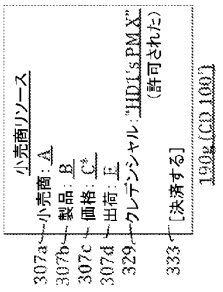

【図３Ｅ】



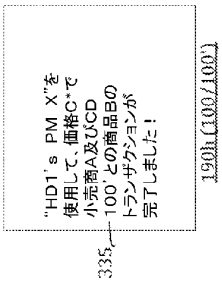

【図３Ｆ】



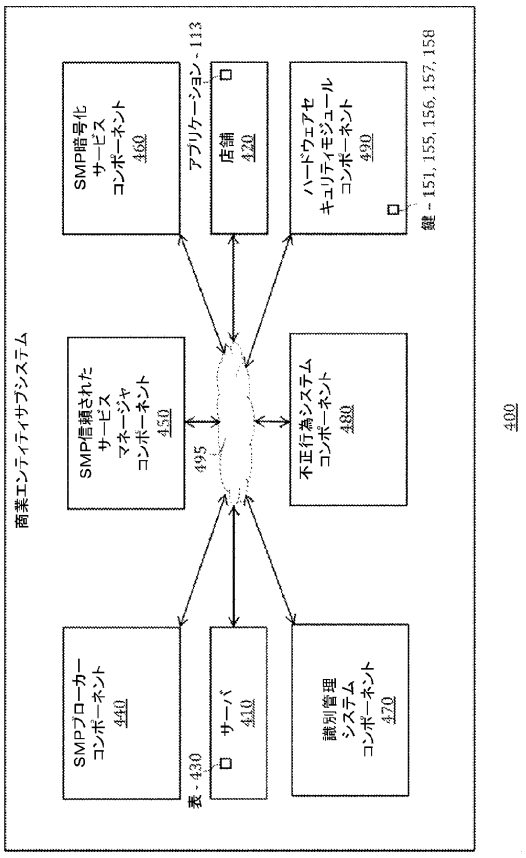

【図３Ｇ】



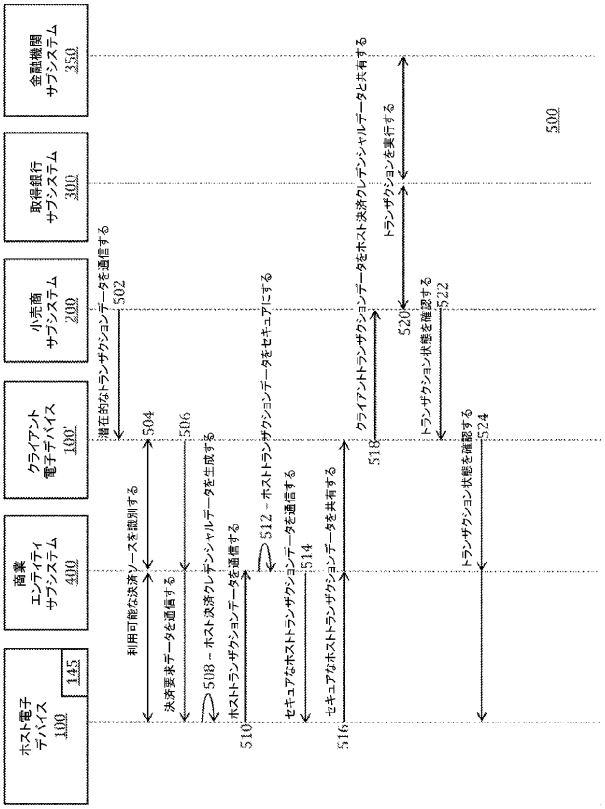

【図３Ｈ】



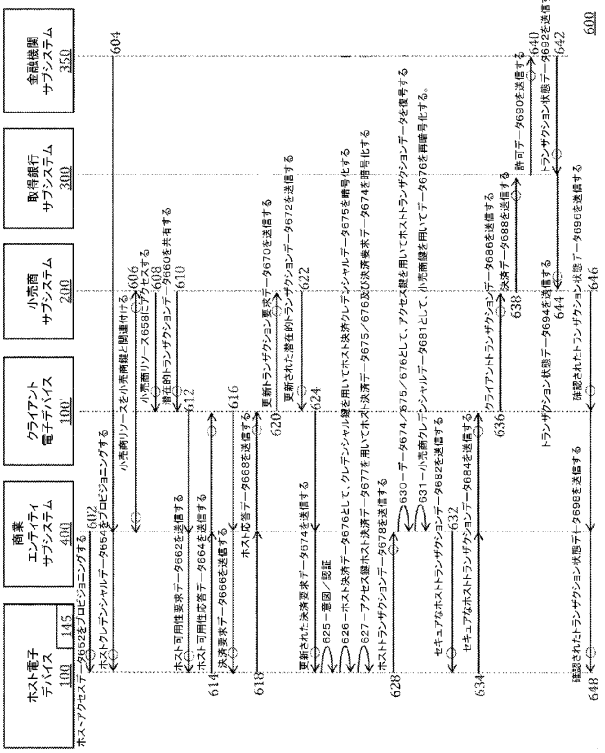
【図４】


商業エンティティサブシステム
SMPブローカーコンポーネント 440
サーバ 410
識別管理システムコンポーネント 420
SMP信頼されたサービスマネージャコンポーネント 450
不正行為システムコンポーネント 480
SMP暗号化サービスコンポーネント 460
アプリケーション、113
店舗 420
ハードウェアセキュリティモジュールコンポーネント 490
鍵 - 151, 155, 156, 157, 158
裏 - 430
495
400

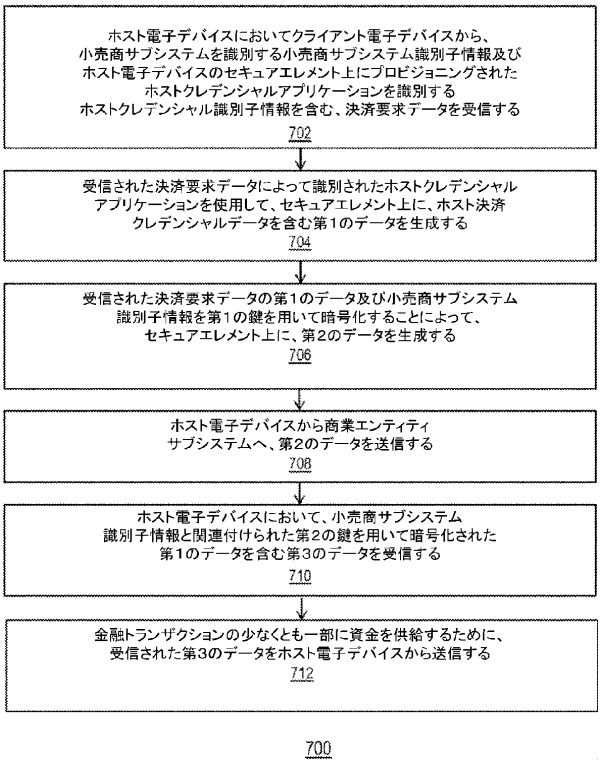
【図５】


ホスト電子デバイス 100
145
商業エンティティサブシステム 400
クライアント電子デバイス 100'
小売商サブシステム 200
取得銀行サブシステム 300
金融機関サブシステム 350
潜在的なトランザクションデータを通信する 502
利用可能な決済ソースを識別する 504
決済要求データを通信する 506
508 - ホスト決済クレデンシャルデータを生成する
ホストトランザクションデータを通信する 510
512 - ホストトランザクションデータをセキュアにする
セキュアなホストトランザクションデータを通信する 514
セキュアなホストトランザクションデータを共有する 516
クライアントトランザクションデータをホスト決済クレデンシャルデータと共有する 518
トランザクションを実行する 520
トランザクション状態を確認する 522
トランザクション状態を確認する 524
500

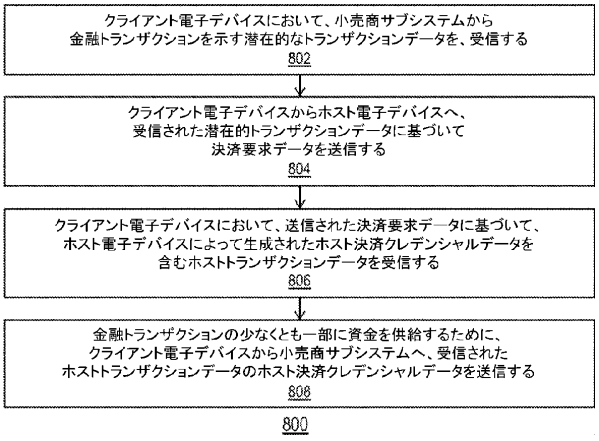
【図６】


ホスト電子デバイス 100
145
商業エンティティサブシステム 400
クライアント電子デバイス 100
小売商サブシステム 200
取得銀行サブシステム 300
金融機関サブシステム 350
600

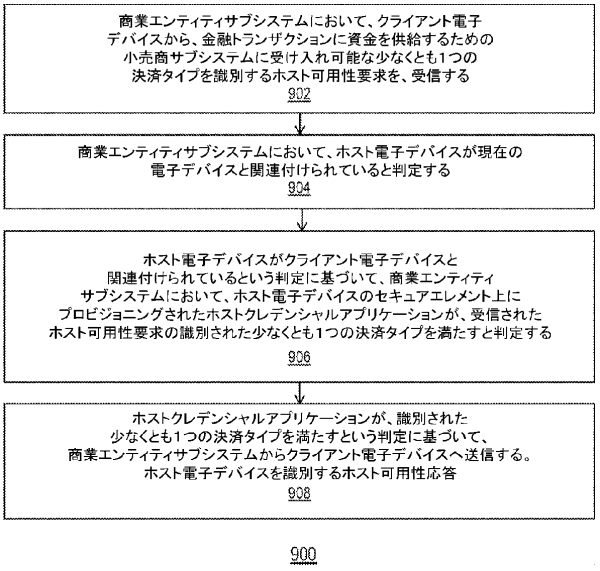
【図７】


ホスト電子デバイスにおいてクライアント電子デバイスから、小売商サブシステムを識別する小売商サブシステム識別子情報及びホスト電子デバイスのセキュアエレメント上にプロビジョニングされたホストクレデンシャルアプリケーションを識別するホストクレデンシャル識別子情報を含む、決済要求データを受信する 702
受信された決済要求データによって識別されたホストクレデンシャルアプリケーションを使用して、セキュアエレメント上に、ホスト決済クレデンシャルデータを含む第1のデータを生成する 704
受信された決済要求データの第1のデータ及び小売商サブシステム識別子情報を第1の鍵を用いて暗号化することによって、セキュアエレメント上に、第2のデータを生成する 706
ホスト電子デバイスから商業エンティティサブシステムへ、第2のデータを送信する 708
ホスト電子デバイスにおいて、小売商サブシステム識別子情報と関連付けられた第2の鍵を用いて暗号化された第1のデータを含む第3のデータを受信する 710
金融トランザクションの少なくとも一部に資金を供給するために、受信された第3のデータをホスト電子デバイスから送信する 712
700

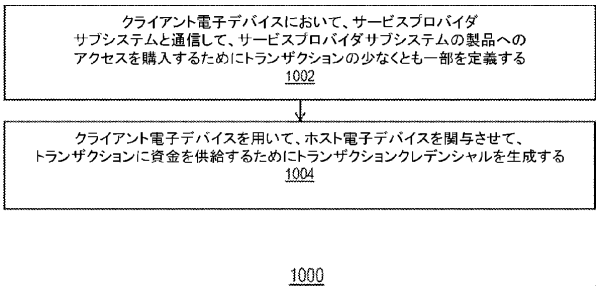
【図８】


クライアント電子デバイスにおいて、小売商サブシステムから
金融トランザクションを示す潜在的なトランザクションデータを、受信する
802
クライアント電子デバイスからホスト電子デバイスへ、
受信された潜在的トランザクションデータに基づいて
決済要求データを送信する
804
クライアント電子デバイスにおいて、送信された決済要求データに基づいて、
ホスト電子デバイスによって生成されたホスト決済クレデンシャルデータを
含むホストトランザクションデータを受信する
806
金融トランザクションの少なくとも一部に資金を供給するために、
クライアント電子デバイスから小売商サブシステムへ、受信された
ホストトランザクションデータのホスト決済クレデンシャルデータを送信する
808
800

【図９】


商業エンティティサブシステムにおいて、クライアント電子
デバイスから、金融トランザクションに資金を供給するための
小売商サブシステムに受け入れ可能な少なくとも1つの
決済タイプを識別するホスト可用性要求を、受信する
902
商業エンティティサブシステムにおいて、ホスト電子デバイスが現在の
電子デバイスと関連付けられていると判定する
904
ホスト電子デバイスがクライアント電子デバイスと
関連付けられているという判定に基づいて、商業エンティティ
サブシステムにおいて、ホスト電子デバイスのセキュアエレメント上に
プロビジョニングされたホストクレデンシャルアプリケーションが、受信された
ホスト可用性要求の識別された少なくとも1つの決済タイプを満たすと判定する
906
ホストクレデンシャルアプリケーションが、識別された
少なくとも1つの決済タイプを満たすという判定に基づいて、
商業エンティティサブシステムからクライアント電子デバイスへ送信する。
ホスト電子デバイスを識別するホスト可用性応答
908
900

【図１０】


クライアント電子デバイスにおいて、サービスプロバイダ
サブシステムと通信して、サービスプロバイダサブシステムの製品への
アクセスを購入するためにトランザクションの少なくとも一部を定義する
1002
クライアント電子デバイスを用いて、ホスト電子デバイスを関与させて、
トランザクションに資金を供給するためにトランザクションクレデンシャルを生成する
1004
1000

フロントページの続き

米国(US)
(31)優先権主張番号　62/348,958
(32)優先日　平成28年6月12日(2016.6.12)
(33)優先権主張国・地域又は機関
米国(US)
(74)代理人　100139712
弁理士　那須 威夫
(74)代理人　100122563
弁理士　越柴 絵里
(72)発明者　ディッカー ジョージ アール
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
(72)発明者　シアラー ニコラス ジェイ
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
審査官　小山 和俊
(56)参考文献　特開２０１１－２４８８８０（ＪＰ，Ａ）
米国特許出願公開第２０１２／０３３０７６４（ＵＳ，Ａ１）
特開２００３－１４１４３２（ＪＰ，Ａ）
特表２０１５－５２９８６３（ＪＰ，Ａ）
米国特許出願公開第２０１０／００５１６８５（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００