(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7204705号
(P7204705)

(45)発行日　令和5年1月16日(2023.1.16)

(24)登録日　令和5年1月5日(2023.1.5)

(51)国際特許分類

Ｈ０４Ｌ	*9/32*	*(2006.01)*	Ｈ０４Ｌ	9/32　２００Ａ
Ｇ０６Ｆ	*21/64*	*(2013.01)*	Ｈ０４Ｌ	9/32　２００Ｅ
Ｇ０６Ｑ	*20/38*	*(2012.01)*	Ｇ０６Ｆ	21/64
			Ｇ０６Ｑ	20/38　３１０

請求項の数　17　外国語出願　（全100頁）

(21)出願番号　特願2020-94513(P2020-94513)
(22)出願日　令和2年5月29日(2020.5.29)
(62)分割の表示　特願2018-559670(P2018-559670)の分割
原出願日　平成29年1月3日(2017.1.3)
(65)公開番号　特開2020-145752(P2020-145752A)
(43)公開日　令和2年9月10日(2020.9.10)
審査請求日　令和2年6月5日(2020.6.5)
(31)優先権主張番号　62/289,656
(32)優先日　平成28年2月1日(2016.2.1)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/297,923
(32)優先日　平成28年2月21日(2016.2.21)
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　100103610
弁理士　▲吉▼田 和彦
(74)代理人　100067013
弁理士　大塚 文昭
最終頁に続く

(54)【発明の名称】　セキュアデバイス機能へのオンラインアクセスの妥当性検査

(57)【特許請求の範囲】
【請求項１】
販売事業者サブシステムとコンピュータデバイスとの間のトランザクションを容易にする方法であって、
前記コンピュータデバイスが、
前記販売事業者サブシステムと相互作用して前記トランザクションをイニシャライズすること、
第１の妥当性データが商業エンティティサブシステムから受信されたかを判定すること、　前記第１の妥当性データが前記商業エンティティサブシステムから受信されたかの判定に応答して、
第２の妥当性データ及び機密データを前記商業エンティティサブシステムに提供すること、
前記商業エンティティサブシステムが前記第２の妥当性データを認証することに応じて、暗号化した機密データが前記商業エンティティサブシステムから受信されたかを判定すること、
前記暗号化した機密データが前記商業エンティティサブシステムから受信されたかの判定に応答して、前記暗号化した機密データを前記販売事業者サブシステムに提供して前記トランザクションを完了すること、
を実行し、及び
前記第１の妥当性データが提供される前に、前記商業エンティティサブシステムは、

販売事業者識別子を含むチャレンジ要求を前記販売事業者サブシステムから受信し、前記販売事業者識別子は(1)前記販売事業者サブシステム及び(2)前記コンピュータデバイスの販売事業者オンラインリソースに関連し、前記チャレンジ要求は前記販売事業者サブシステムに関連する販売事業者キーを用いて定められた署名を含み、
前記販売事業者識別子に基づき前記販売事業者キーを取得し、
前記販売事業者キーを用いて前記署名を検証する、
ことを含む、方法。
【請求項２】
前記チャレンジ要求を受信する前に、前記商業エンティティサブシステムは、前記販売事業者サブシステムによる登録処理の間に、(1)前記販売事業者識別子及び(2)前記販売事業者キーを受信する、請求項１に記載の方法。
【請求項３】
前記第２の妥当性データは、妥当性検査セッション識別子を含み、
前記妥当性検査セッション識別子は、
前記トランザクションのイニシャライズとあわせて前記前記コンピュータデバイスと前記販売事業者サブシステムとの間で定められ、
前記販売事業者サブシステムによって前記商業エンティティサブシステムへ前記チャレンジ要求において提供される、
請求項１に記載の方法。
【請求項４】
前記妥当性検査セッション識別子は、時間の閾値に関して前記販売事業者キーと関連づけられている、請求項３に記載の方法。
【請求項５】
前記機密データは、
金融トランザクションに用いられる決済クレデンシャルデータ、又は
健康トランザクションに用いられる健康データ、
を含む、請求項１に記載の方法。
【請求項６】
前記暗号化した機密データは、前記販売事業者サブシステムに関連する販売事業者キーにより暗号化される、請求項１に記載の方法。
【請求項７】
前記第２の妥当性データは、前記商業エンティティサブシステムが前記コンピュータデバイスを検証できるようにする妥当性データである、請求項１に記載の方法。
【請求項８】
販売事業者サブシステムと、商業エンティティサブシステムと、前記販売事業者サブシステムとトランザクションを実行するためのコンピュータデバイスとを含むシステムであって、
前記販売事業者サブシステムと相互作用して前記トランザクションをイニシャライズし、
第１の妥当性データが前記商業エンティティサブシステムから受信されたかを判定し、
前記第１の妥当性データが前記商業エンティティサブシステムから受信されたかの判定に応答して、
第２の妥当性データ及び機密データを前記商業エンティティサブシステムに提供し、
前記商業エンティティサブシステムが前記第２の妥当性データを認証することに応じて、暗号化した機密データが前記商業エンティティサブシステムから受信されたかを判定し、
前記暗号化した機密データが前記商業エンティティサブシステムから受信されたかの判定に応答して、前記暗号化した機密データを前記販売事業者サブシステムに提供して前記トランザクションを完了し、及び
前記第１の妥当性データが提供される前に、前記商業エンティティサブシステムは、
販売事業者識別子を含むチャレンジ要求を前記販売事業者サブシステムから受信し、前記

販売事業者識別子は(1)前記販売事業者サブシステム及び(2)前記コンピュータデバイスの販売事業者オンラインリソースに関連し、前記チャレンジ要求は前記販売事業者サブシステムに関連する販売事業者キーを用いて定められた署名を含み、
前記販売事業者識別子に基づき前記販売事業者キーを取得し、
前記販売事業者キーを用いて前記署名を検証する、
ことを含む処理を実行するシステム。
【請求項９】
前記チャレンジ要求を受信する前に、前記商業エンティティサブシステムは、前記販売事業者サブシステムによる登録処理の間に、(1)前記販売事業者識別子及び(2)前記販売事業者キーを受信する、請求項８に記載のシステム。
【請求項１０】
前記第２の妥当性データは、妥当性検査セッション識別子を含み、
前記妥当性検査セッション識別子は、
前記トランザクションのイニシャライズとあわせて前記前記コンピュータデバイスと前記販売事業者サブシステムとの間で定められ、
前記販売事業者サブシステムによって前記商業エンティティサブシステムへ前記チャレンジ要求において提供される、
請求項８に記載のシステム。
【請求項１１】
前記妥当性検査セッション識別子は、時間の閾値に関して前記販売事業者キーと関連づけられている、請求項１０に記載のシステム。
【請求項１２】
前記機密データは、
金融トランザクションに用いられる決済クレデンシャルデータ、又は
健康トランザクションに用いられる健康データ、
を含む、請求項８に記載のシステム。
【請求項１３】
販売事業者サブシステムとトランザクションを実行するコンピュータデバイスであって、前記コンピュータデバイスのプロセッサにより、
前記販売事業者サブシステムと相互作用して前記トランザクションをイニシャライズすること、
第１の妥当性データが商業エンティティサブシステムから受信されたかを判定すること、
前記第１の妥当性データが前記商業エンティティサブシステムから受信されたかの判定に応答して、
第２の妥当性データ及び機密データを前記商業エンティティサブシステムに提供すること、
前記商業エンティティサブシステムが前記第２の妥当性データを認証することに応じて、暗号化した機密データが前記商業エンティティサブシステムから受信されたかを判定すること、
前記暗号化した機密データが前記商業エンティティサブシステムから受信されたかの判定に応答して、前記暗号化した機密データを前記販売事業者サブシステムに提供して前記トランザクションを完了すること、及び
前記第１の妥当性データが提供される前に、前記商業エンティティサブシステムは、
販売事業者識別子を含むチャレンジ要求を前記販売事業者サブシステムから受信し、前記販売事業者識別子は(1)前記販売事業者サブシステム及び(2)前記コンピュータデバイスの販売事業者オンラインリソースに関連し、前記チャレンジ要求は前記販売事業者サブシステムに関連する販売事業者キーを用いて定められた署名を含み、
前記販売事業者識別子に基づき前記販売事業者キーを取得し、
前記販売事業者キーを用いて前記署名を検証する、
ことが実行される、コンピュータデバイス。

【請求項１４】
前記チャレンジ要求を受信する前に、前記商業エンティティサブシステムは、前記販売事業者サブシステムによる登録処理の間に、(1)前記販売事業者識別子及び(2)前記販売事業者キーを受信する、請求項１３に記載のコンピュータデバイス。
【請求項１５】
前記第２の妥当性データは、妥当性検査セッション識別子を含み、
前記妥当性検査セッション識別子は、
前記トランザクションのイニシャライズとあわせて前記前記コンピュータデバイスと前記販売事業者サブシステムとの間で定められ、
前記販売事業者サブシステムによって前記商業エンティティサブシステムへ前記チャレンジ要求において提供される、
請求項１３に記載のコンピュータデバイス。
【請求項１６】
前記妥当性検査セッション識別子は、時間の閾値に関して前記販売事業者キーと関連づけられている、請求項１５に記載のコンピュータデバイス。
【請求項１７】
前記機密データは、
金融トランザクションに用いられる決済クレデンシャルデータ、又は
健康トランザクションに用いられる健康データ、
を含む、請求項１３に記載のコンピュータデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願（単数又は複数）の相互参照）
本出願は、２０１６年２月１日に出願された先出願の米国特許仮出願第６２／２８９，６５６号、２０１６年２月２１日に出願された先出願の米国特許仮出願第６２／２９７，９２３号、２０１６年６月１２日に出願された先出願の米国特許仮出願第６２／３４８，９６０号、及び２０１６年６月１２日に出願された先出願の米国特許仮出願第６２／３４８，９７９号の利益を主張するものであり、それらの各出願は、その全体が参照により本明細書に組み込まれる。
本開示は、セキュアデバイス機能へのオンラインアクセスを妥当性検査することに関し、より具体的には、サードパーティサブシステムによる電子デバイスのセキュア機能へのオンラインアクセスを可能とするための、サードパーティサブシステムの妥当性検査に関する。
【０００２】
（開示の背景）
ポータブル電子デバイス（例えば、携帯電話）は、他のエンティティ（例えば販売事業者）との機密データの非接触近接型通信を可能とする近距離無線通信（「ＮＦＣ」）構成要素を備えることがある。こうしたデータのトランザクションにおいては、電子デバイスは、クレジットカードクレデンシャルなどのネイティブ決済クレデンシャルを生成し、アクセスし、及び／又は他のエンティティとの間で共有することが必要となる。しかし、他のタイプの通信（例えば、オンライントランザクション）における電子デバイスによってそのようなネイティブ決済クレデンシャルをセキュアに使用することは、非効率的であることが多い。
【発明の概要】
【０００３】
本明細書では、セキュアデバイス機能へのオンラインアクセスを妥当性検査するためのシステム、方法、及びコンピュータ可読媒体を記載する。
【０００４】
例として、販売事業者オンラインリソースを介した販売事業者サブシステムと、販売事

業者サブシステムに通信可能に結合された電子デバイスとの間でセキュアなトランザクションを行う商業エンティティサブシステムを使用する方法が提供される。本方法は、商業エンティティサブシステムにおいて、販売事業者サブシステムから、販売事業者オンラインリソースに対する妥当性検査要求を受信することと、妥当性検査要求及びその受信前に最初に商業エンティティサブシステムに利用可能にされた登録データを用いてオンライン販売事業者リソースを妥当性検査することと、妥当性検査した後に、妥当性検査要求の少なくとも一部分に関連付けた妥当性検査データを生成することと、電子デバイスに妥当性検査データを通信することと、電子デバイスからデバイストランザクションデータを受信することと、デバイストランザクションデータが妥当性検査データを含むことを判定することと、判定した後、販売事業者サブシステムが使用するためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することと、を含むことができる。

【０００５】

別の例として、管理エンティティサブシステムを使用して、処理サブシステムと、処理サブシステムと通信可能に結合された電子デバイスとの間のセキュアなトランザクションを、電子デバイス上で実行されるオンラインリソースを介して行う方法を提供することができる。本方法は、管理エンティティサブシステムにおいて、オンラインリソースに対する妥当性検査要求を受信することであって、妥当性検査要求は妥当性検査要求データを含むことと、妥当性検査要求データ及び登録データを用いてオンラインリソースを妥当性検査することであって、登録データは妥当性検査要求の受信前に最初に管理エンティティサブシステムに利用可能とされていることと、オンラインリソースが妥当性検査された後、妥当性検査レスポンスデータを妥当性検査要求データの少なくとも一部分と関連付けることと、妥当性検査レスポンスデータを電子デバイスに通信することと、妥当性検査レスポンスデータを電子デバイスに通信した後、デバイストランザクションデータを電子デバイスから受信することと、妥当性検査レスポンスデータを用いてデバイストランザクションデータを妥当性検査することと、デバイストランザクションデータが妥当性検査された後、処理サブシステムが使用するためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することと、を含むことができる。

【０００６】

更に別の例として、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介して処理サブシステムに通信可能に結合されている電子デバイスとの間のセキュアなトランザクションを可能とする管理エンティティサブシステムを使用する方法を提供することができる。本方法は、管理エンティティサブシステムにおいて、オンラインリソースを登録することであって、管理エンティティサブシステムと処理サブシステムとの間で処理共有秘密を確立することを含むことと、オンラインリソースに対する妥当性検査要求を受信することであって、妥当性検査要求はオンラインリソースを示す処理識別子を含み、また妥当性検査要求は、オンラインリソースを介した、電子デバイスと処理サブシステムとの間の潜在的トランザクションに一意である妥当性検査セッション識別子を更に含むことと、妥当性検査セッション識別子と処理共有秘密を用いて処理識別子が示すオンラインリソースを妥当性検査することと、を含むことができる。

【０００７】

更に別の例として、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介して処理サブシステムに通信可能に結合された電子デバイスとの間でセキュアなトランザクションを行うために管理エンティティサブシステムを使用する方法を提供することができる。本方法は、管理エンティティサブシステムにおいて、オンラインリソースに対する妥当性検査要求を受信することであって、この妥当性検査要求は妥当性検査要求データを含み、また妥当性検査要求データは、オンラインリソースを介した、電子デバイスと処理サブシステムとの間の潜在的トランザクションを示す潜在的トランザクション識別情報を含むことと、妥当性検査要求データの少なくとも一部分を用いてオンラインリソースを妥当性検査することと、妥当性検査レスポンスデータを少なくとも潜在的トランザ

クション識別情報と関連付けることと、オンラインリソースが妥当性検査された後、妥当性検査レスポンスデータを電子デバイスに通信することと、妥当性検査レスポンスデータを電子デバイスに通信した後、デバイストランザクションデータを電子デバイスから受信することと、妥当性検査レスポンスデータ及び潜在的トランザクション識別情報を用いてデバイストランザクションデータを妥当性検査することと、デバイストランザクションデータが妥当性検査された後、処理サブシステムが使用するためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することと、を含むことができる。

【０００８】

この「発明の概要」は、本明細書で説明する主題のいくつかの態様の基本的理解を提供するように、いくつかの例示的実施形態を要約することのみを目的として提供されるものに過ぎない。したがって、この「発明の概要」に説明した特徴は、単なる例であって、いかなる方式でも、本明細書で説明される主題の範囲又は趣旨を狭めるものとして解釈すべきではないことを理解されたい。特に明記しない限り、一実施例のコンテキストで説明される特徴は、１つ以上の他の実施例のコンテキストで説明される特徴と組合せてもよいし、それとともに使用されてもよい。本明細書で説明される主題の、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】

【０００９】

以下の説明では以下の図面を参照し、同様の参照文字は全体にわたって同様の部分を参照する。

【００１０】

【図１】セキュアデバイス機能へのオンラインアクセスを妥当性検査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別の概略図である。

【図２】図１及び図１Ａのシステムの例示の電子デバイスのより詳細な概略図である。

【図２Ａ】図１～図２の例示の電子デバイスのより詳細な別の概略図である。

【図３】図１～図２Ａの例示の電子デバイスの正面図である。

【図３Ａ】セキュアデバイス機能へのオンラインアクセスを妥当性検査するプロセスを図示する図１～図３のうちの１つ以上の例示の電子デバイスのグラフィカルユーザインタフェースの画面の正面図である。

【図３Ｂ】セキュアデバイス機能へのオンラインアクセスを妥当性検査するプロセスを図示する図１～図３のうちの１つ以上の例示の電子デバイスのグラフィカルユーザインタフェースの画面の正面図である。

【図３Ｃ】セキュアデバイス機能へのオンラインアクセスを妥当性検査するプロセスを図示する図１～図３のうちの１つ以上の例示の電子デバイスのグラフィカルユーザインタフェースの画面の正面図である。

【図３Ｄ】セキュアデバイス機能へのオンラインアクセスを妥当性検査するプロセスを図示する図１～図３のうちの１つ以上の例示の電子デバイスのグラフィカルユーザインタフェースの画面の正面図である。

【図４】図１及び図１Ａのシステムの例示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】セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセスのフローチャートである。

【図６】セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセスのフローチャートである。

【図７】セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセスのフローチャートである。

【図８】セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセ

スのフローチャートである。
【図９】セキュアデバイス機能へのオンラインアクセスを妥当性検査する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】
【００１１】
処理（又は販売事業者）サブシステムは、パートナ・ペイメント・サービス・プロバイダ（ＰＳＰ）の有無にかかわらず、処理サブシステムのオンラインリソース（例えば、ネイティブアプリケーション又はウェブサイト）が、ＰＳＰに組み込まれた決済フォームの有無にかかわらず、機密データ（例えば、セキュアエレメント決済クレデンシャルデータ）をユーザ電子デバイスからセキュアに受信するために使用される前に、信頼された管理（又は商業）エンティティサブシステムによって妥当性検査され得る。更に、オンラインリソースの妥当性検査に加えて、オンラインリソースが機能して、処理サブシステムとのトランザクションにおいて機密データを共有するオプションをユーザデバイスに提示する前に、特定のトランザクションを可能とするためのオンラインリソース使用を再許可するために、このようなオプションの選択に応じた追加的なセッション妥当性検査プロセスが実行され得る。
【００１２】
図１及び図１Ａでは、１つ以上のクレデンシャルが、金融機関（又はトランザクション若しくは発行者）サブシステム３５０から、商業（又は管理）エンティティサブシステム４００と連携して、電子デバイス１００に供給され、電子デバイス１００はこのようなクレデンシャルを使用して販売事業者（又は処理）サブシステム２００及び関連付けられた取得銀行（又は取得者）サブシステム３００とのトランザクション（例えば、財務トランザクション又は任意の他の好適なセキュアなデータトランザクション）を行うことができる（例えば、電子デバイス１００のセキュアデバイス機能）、システム１を示す。一方、図２～図３はシステム１の電子デバイス１００の特定の実施形態に関する更なる詳細を示し、図３Ａ～図３Ｄは、このようなトランザクション実行中のシステム１の電子デバイス１００のグラフィカルユーザインタフェースとして代表的な例示画面１９０ａ～１９０ｄを示しており、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とともに、図５～図９は、（例えば、このような財務トランザクションを行う）セキュアデバイス機能へのオンラインアクセスを妥当性検査する例示的なプロセスのフローチャートである。
【００１３】
図１の説明
図１は、販売事業者サブシステム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型決済）における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とする販売事業者（又は処理）サブシステムの妥当性検査など、サードパーティサブシステムによる電子デバイスのセキュア機能へのオンラインアクセスを可能とするサードパーティサブシステムの妥当性検査を可能にし得る例示的なシステム１の概略図である。例えば、図１に示すように、システム１は、電子デバイス１００、ならびに電子デバイス１００に１つ以上のクレデンシャルをセキュアに供給するための、商業（又は管理）エンティティサブシステム４００及び金融機関（又はトランザクション若しくは発行者）サブシステム３５０を含むことができる。また、図１に示すように、システム１は販売事業者（又は処理）サブシステム２００を含んでもよく、それによって、このように供給されたクレデンシャルは、販売事業者サブシステム２００とのトランザクション（例えば、財務トランザクション又は任意の他の公的なセキュアなデータトランザクション）を行うために電子デバイス１００によって使用され得る。例えば、販売事業者サブシステム２００からの潜在的トランザクションデータの受信に応じて、電子デバイス１００は、販売事業者サブシステム２００との特定の財務トランザクションに資金供給するため、非接触近接型通信５（例えば、近距離無線通信又はＢｌｕｅｔｏｏｔｈ（登録商標）通信）として、及び／又はオンライン型通信６８４（例えば、ネットワーク電気通信など）として、供給されたク

レデンシャルのセキュアデバイスデータを、販売事業者サブシステム２００と共有することができる。システム１はまた、金融機関サブシステム３５０とのトランザクションを完了するために、このような非接触近接型通信５及び／又はこのようなオンライン型通信６８４を利用し得る取得銀行（又は取得者）サブシステム３００も含むことができる。

【００１４】

システム１は、電子デバイス１００と販売事業者サブシステム２００との間の通信を可能とする通信経路１５と、販売事業者サブシステム２００と取得銀行サブシステム３００との間の通信を可能とする通信経路２５と、取得銀行サブシステム３００と金融機関サブシステム３５０との間の通信を可能とする通信経路３５と、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との間の通信を可能とする通信経路４５と、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との間の通信を可能とする通信経路５５と、商業エンティティサブシステム４００と電子デバイス１００との間の通信を可能とする通信経路６５と、金融機関サブシステム３５０と電子デバイス１００との間の通信を可能とする通信経路７５と、商業エンティティサブシステム４００と販売事業者サブシステム２００との間の通信を可能とする通信経路８５と、を含むことができる。経路１５、２５、３５、４５、５５、６５、７５、８５のうち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得る。任意の好適な回路、デバイス、システム、又は、通信ネットワークを作成するように機能し得るこれらの組合せ（例えば、１つ以上の通信タワー、電気通信サーバ等を含み得る有線通信インフラ及び／又は無線通信インフラ）は、任意の好適な有線又は無線通信プロトコルを用いて通信を提供可能にし得る経路１５、２５、３５、４５、５５、６５、７５、８５のうち１つ以上を提供するのに使用することができる。例えば、経路１５、２５、３５、４５、５５、６５、７５、８５のうち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（登録商標）、イーサネット（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＢＬＥ、高周波数システム（例えば、９００ＭＨｚ、２．４ＧＨｚ及び５．６ＧＨｚ通信システム）、赤外線、ＴＣＰ／ＩＰ、ＳＣＴＰ、ＤＨＣＰ、ＨＴＴＰ、ＢｉｔＴｏｒｒｅｎｔ（登録商標）、ＦＴＰ、ＲＴＰ、ＲＴＳＰ、ＲＴＣＰ、ＲＡＯＰ、ＲＤＴＰ、ＵＤＰ、ＳＳＨ、ＷＤＳブリッジング、無線及び携帯電話ならびに個人用電子メールデバイス（例えば、ＧＳＭ(登録商標)、ＧＳＭ(登録商標)＋ＥＤＧＥ、ＣＤＭＡ、ＯＦＤＭＡ、ＨＳＰＡ、ｍｕｌｔｉ－ｂａｎｄ等）により使用され得る任意の通信プロトコル、低出力のＷｉｒｅｌｅｓｓ　Ｐｅｒｓｏｎａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ（６ＬｏＷＰＡＮ）モジュールにより使用され得る任意の通信プロトコル、あらゆる他の通信プロトコル、又はこれらのあらゆる組合せをサポートすることができる。

【００１５】

図１Ａの説明

ここで図１Ａを参照すると、図１Ａは、上記したシステム１の、図１のより詳細な図を示している。図１Ａに示すように、例えば、電子デバイス１００は、プロセッサ１０２、通信構成要素１０６及び／又は近距離無線通信（「ＮＦＣ」）構成要素１２０を含むことができる。ＮＦＣ構成要素１２０は、耐タンパ性プラットフォームを（例えば、単一チップ又は複数チップセキュアマイクロコントローラとして）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、このプラットフォームは、認証され信頼された権限者の集合（例えば、金融機関サブシステム及び／又はＧｌｏｂａｌＰｌａｔｆｏｒｍのような業界標準の権限者）によって定められ得る規則及びセキュリティ要件に従って、アプリケーションならびにそれらの機密データ及び暗号化データ（例えば、クレデンシャルアプレット及び、図１Ａに示すような、クレデンシャル鍵１５５ａ’及びアクセス鍵１５５ａ、ならびに／又は発行者のセキュリティドメイン（ＩＳＤ）鍵１５６ｋなどの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し得る。以下により詳細に説明するように、デバイス１００の（例えば、ＮＦＣ構成要素１

２０の）セキュアエレメント１４５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は、資金供給口座又は他の金融商品若しくは信用元（例えば、金融機関サブシステム３５０における）を識別するための十分な詳細を含むトランザクションデータとして決済クレデンシャルデータを提供するように構成することができ、このような決済クレデンシャルデータは、財務トランザクションを促進するために、販売事業者サブシステム２００及び／又は商業エンティティサブシステム４００との１つ以上の通信の中でデバイス１００によって使用され得る。ＮＦＣ構成要素１２０は、このようなホスト決済クレデンシャルデータを、販売事業者サブシステム２００との非接触近接型通信５（例えば、近距離無線通信）として（例えば、デバイス１００のユーザがデバイス１００に記憶されたクレデンシャルを使用して、近接して配置された販売事業者端末２２０と非接触近接型通信を介して財務トランザクションを行い得る、実在の店舗又は任意の物理的所在地に配置され得る販売事業者サブシステム２００の販売事業者端末２２０との通信）、通信するように構成され得る。代替的に、又は追加的に、任意の好適な有線又は無線プロトコル（例えば、通信経路１５、６５及び／又は７５のうちの１つ以上を介して）を用いて、任意の好適な決済クレデンシャルデータを（例えば、オンライン型通信６８４として）１つ以上の他の電子デバイス又はサーバ若しくはサブシステム（例えば、任意の好適なオンライン通信を介する販売事業者サブシステム２００の販売事業者サーバ２１０のような、システム１の１つ以上のサブシステム又は他の構成要素）と通信することを可能とするように、通信構成要素１０６がデバイス１００に設けられてもよい。デバイス１００のプロセッサ１０２は、デバイス１００の１つ以上の構成要素の動作及び性能を制御するように機能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、販売事業者サブシステム２００との財務トランザクションに資金供給するためにデバイス１００によりデータ（例えば、トランザクションデータの決済クレデンシャルデータ）が通信され得る方法を、少なくとも部分的に決定し得る、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若しくは販売事業者アプリケーション１１３）をデバイス１００上で実行するように構成され得る。また、図１Ａに示すように、デバイス１００は、プロセッサ１０２又はデバイス１００の任意の他の好適な部分にとってアクセス可能となり得る任意の好適なデバイス識別情報又はデバイス識別子１１９を含むことができる。デバイス識別情報１１９は、デバイス１００を一意に識別し、販売事業者サブシステム２００とのトランザクションを促進し、かつ／又はデバイス１００との好適なセキュアな通信を可能とするため、商業エンティティサブシステム４００及び／又は販売事業者サブシステム２００及び／又は金融機関サブシステム３５０によって利用され得る。一例として、デバイス識別情報１１９は、電話番号若しく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とすることができる。

【００１６】

販売事業者サブシステム２００は、図１Ａに示すような、任意の好適な販売事業者サーバ２１０を含むことができ、それは、任意の好適な通信プロトコル（例えば、Ｗｉ－Ｆｉ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、セルラ、有線ネットワークプロトコル等）を介して、（例えば、通信経路８５を介して）商業エンティティサブシステム４００の通信構成要素と、及び／又は、（例えば、通信経路２５を介して）取得銀行３００の通信構成要素と、及び／又は（例えば、通信経路１５を介して）デバイス１００の通信構成要素と、あらゆる好適なデータを通信するように構成され得る任意の好適な構成要素又はサブシステムを含むことができる。例えば、販売事業者サーバ２１０は、デバイス１００の通信構成要素１０６と,潜在的トランザクションデータ６６０を、次のような任意の好適なオンラインコンテキスト内で通信するように機能することができ、これには、デバイス１００のユーザが、デバイス１００上で実行中であり得る任意の好適な販売事業者オンラインリソース１１３を介するトランザクションを行うために販売事業者サーバ２１０と通信している場合の、次のオンラインリソースが含まれる。

販売事業者サーバ２１０によって管理され得るデバイス１００上で動作中のサードパーティ販売事業者アプリケーション１１３（例えば、ネイティブアプリケーション）、又

はデバイス１００上で動作中であって、ターゲット又はウェブリソースが販売事業者サーバ２１０（例えば販売事業者のウェブサイト）によって管理され得るユニフォームリソースロケーター（「ＵＲＬ」）に向けられ得るインターネットアプリケーション１１３（例えば、アップル　インコーポレイテッドによるＳａｆａｒｉ（登録商標））

販売事業者ウェブサイトに向けられたウェブ表示を用いた販売事業者アプリケーション（例えば、販売事業者アプリケーション内にバンドルされたインターネットブラウザであって、それによってハイブリッドアプリと呼ばれ得るものを生成することでウェブ技術（例えば、ＨＴＭＬ、ＪａｖａＳｃｒｉｐｔ(登録商標)、ＣＳＳ等）を用いて構築できるアプリをネイティブアプリとしてパッケージング可能なもの、及び／又は

販売事業者のウェブサイトに向けられたウェブ表示を用いた非販売事業者アプリケーション。

したがって、販売事業者サーバ２１０とデバイス１００との間の通信は、無線で、及び／又は有線経路を介して（例えば、インターネット上で）生じ得ることに留意されたい。販売事業者サーバ２１０は、販売事業者サブシステム２００の販売事業者によって（例えば、ウェブサイトデータをホストする、かつ／又はサードパーティアプリケーションデータを管理するウェブサーバとして）提供されてもよい。追加的に、又は代替的に、図１Ａに示すように、販売事業者サブシステム２００は、任意の販売事業者端末２２０（例えば、販売事業者決済端末）を含むことができ、それは、デバイス１００の非接触近接型通信構成要素（例えば、デバイス１００のＮＦＣ構成要素１２０との非接触近接型通信５）と任意の好適なデータを通信するように構成され得る好適な構成要素又はサブシステムを含むことができる。また、図１Ａに示すように、販売事業者サブシステム２００は、販売事業者鍵１５７及び／又は販売事業者識別子（「ＩＤ」）１６７を含むことができる。図示していないが、販売事業者サブシステム２００はまた、図１Ａ及び図２の電子デバイス１００のプロセッサ構成要素１０２と同一又は同様であり得る販売事業者プロセッサ構成要素、（例えば、サーバ２１０の一部分として）図１Ａ及び図２の電子デバイス１００の通信構成要素１０６と同一又は同様であり得る販売事業者通信構成要素、図２の電子デバイス１００のＩ／Ｏインタフェース１１４と同一又は同様であり得る販売事業者Ｉ／Ｏインタフェース、図２の電子デバイス１００のバス１１８と同一又は同様であり得る販売事業者バス、図２の電子デバイス１００のメモリ構成要素１０４と同一又は同様であり得る販売事業者メモリ構成要素、及び／又は図２の電子デバイス１００の電源構成要素１０８と同一又は同様であり得る販売事業者電源構成要素、も含むことができる。

【００１７】

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、決済カード組合又はクレジットカード組合）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り負担し得る債務を完済する消費者の能力に対する主たる責任を引き受け得る金融機関とすることができる。デバイス１００のＮＦＣ構成要素１２０の特定のクレデンシャルアプレットをそれぞれ、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ることができる。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（fleet card）、ギフトカード等を含む様々なタイプの決済カードが好適であり得る。特定の決済カードの商業クレデンシャルは、（例えば、直接的又は商業エンティティサブシステム４００を介した）販売事業者サブシステム２００との商業クレデンシャルデータ通信（例えば、非接触近接型通信及び／又はオンライン型通信）に使用するために発行銀行サブシステム３７０によってデバイス１００上に（例えば、後述のＮＦＣ構成要素１２０のクレデンシャル補足的セキュリティドメインのクレデンシャルとして）供給され得る。各クレデンシャルは、決済ネットワークサブシステム３６０によってブランド付けされ得る特定の決済カードのブランドであってよい。決済ネットワークサブシステム３６０は、種々の発行銀行３７０及び／又は、特定のブランドの決済カードの使用（例えば、商業クレデンシャル）を処理することができる種々の取得銀行３００のネットワークであってもよい。

【００１８】
財務トランザクションがシステム１内で生じるために、少なくとも１つの商業クレデンシャルが電子デバイス１００のセキュアエレメント上にセキュアに供給されなければならない。例えば、このような商業クレデンシャルを、（例えば、金融機関サブシステム３５０とデバイス１００との間の通信経路７５を介するクレデンシャルデータ６５４として、そして通信構成要素１０６を介してセキュアエレメント１４５に渡されることにより）金融機関サブシステム３５０から直接デバイス１００のセキュアエレメント１４５に少なくとも部分的に直接供給することができる。追加的に、又は代替的に、このような商業クレデンシャルを、金融機関サブシステム３５０からデバイス１００のセキュアエレメント１４５に，商業エンティティサブシステム４００を介して、少なくとも部分的に直接供給することができる（例えば、このような商業クレデンシャルを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との間の通信経路５５を介するクレデンシャルデータ６５４として供給し、それを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の通信構成要素１０６との間の通信経路６５を介してクレデンシャルデータ６５４としてデバイス１００に渡し、そして、通信構成要素１０６からセキュアエレメント１４５に渡すことができる）。経路７５を介した、かつ／又は経路５５／６５を介したクレデンシャルデータ６５４は、セキュアエレメントのクレデンシャル補足的セキュリティドメインの少なくとも一部分又は全部として、デバイス１００のセキュアエレメント１４５に供給することができ、またそれは、決済アプリケーション又は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１Ａに示すように、例えば、金融機関サブシステム３５０はまた、（例えば、クレデンシャル鍵１５５ａ’を用いてデバイス１００により暗号化されたデータを解読するために）クレデンシャル鍵１５５ａ’へアクセスすることもできる。金融機関サブシステム３５０は、クレデンシャル鍵１５５ａ’の管理を担当することができ、管理は、そのような鍵の生成、交換、記憶、使用、及び置換を含んでもよい。金融機関サブシステム３５０は、金融機関サブシステム３５０のセキュアエレメントにクレデンシャル鍵１５５ａ’のバージョンを記憶することができる。デバイス１００のクレデンシャル鍵１５５ａ’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及び金融機関サブシステム３５０の両方が利用可能な任意の好適な共有秘密（例えば、パスワード、パスフレーズ、ランダムに選ばれたバイトのアレイ、１つ以上の対称鍵、公開／秘密鍵（例えば、非対称鍵）等）とすることができ、（例えば、財務トランザクションの決済データを妥当性検査するため）電子デバイス１００と金融機関サブシステム３５０が独立して任意の好適な暗号データ（例えば、暗号文）又は任意の他の好適なデータを生成することを可能とする機能を持つ。これは、関数の出力が少なくとも部分的に共有秘密によって決定され得る任意の好適な暗号アルゴリズム又は暗号を用い、共有秘密は金融機関サブシステム３５０によってデバイス１００に供給され得ることによっていることを理解されたい。共有秘密は、事前に（例えば、金融機関サブシステム３５０によるデバイス１００へのクレデンシャルの提供の際に）金融機関サブシステム３５０とデバイス１００との間で共有されてもよく（この場合には、このような共有秘密は事前共有鍵と呼ばれる場合がある）、又は、共有秘密は、特定の財務トランザクションに使用する前に、鍵合意プロトコルを用いて（例えば、ディフィー・ヘルマンのような公開鍵暗号法を用いて、又はケルベロスのような対称鍵暗号法を用いて）作成されてもよい。共有秘密及び、関数の出力が共有秘密によって少なくとも部分的に決定され得る好適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とってアクセス可能とすることができる。

【００１９】
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とデバイス１００との間の媒介として提供されてもよく、その場合、商業エンティティサブシステム４００は、クレデンシャルがデバイス１００のセキュアエレメントに供給される際、及び／又

はそのような供給されたクレデンシャルがデバイス１００と販売事業者サブシステム２００との間の商業クレデンシャルデータ通信の一部として使用される際に、新たなセキュリティ層を提供、かつ／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い。商業エンティティサブシステム４００は、特定の商業エンティティによって提供されてもよく、デバイス１００のユーザに、ユーザ固有アカウントのユーザ固有のログイン情報を通じて（例えば、ユーザ固有識別及びパスワードの組合せを通じて）種々のサービスを提供し得る。一例として、商業エンティティサブシステム４００は、アップル　インコーポレイテッド（カリフォルニア州クパチーノ）によって提供されてもよい。同社はまた、デバイス１００のユーザへの様々なサービスの提供者（例えば、デバイス１００で再生されるメディアを販売／レンタルするｉＴｕｎｅｓ（登録商標）ストア、デバイス１００上で使用されるアプリケーションを販売／レンタルするアップルのＡｐｐ　Ｓｔｏｒｅ（登録商標）、デバイス１００からデータを記憶する、かつ／又は複数のユーザデバイス及び／又は複数のユーザプロファイルを互いに関連付けるアップルのｉＣｌｏｕｄ（登録商標）サービス、様々なアップル製品をオンラインで購入するためのアップルのオンラインストア、デバイス間でメディアメッセージを通信するためのアップルのｉＭｅｓｓａｇｅ（登録商標）サービス等）であってもよく、また、（例えば、デバイス１００がｉＰｏｄ（登録商標）、ｉＰａｄ（登録商標）、ｉＰｈｏｎｅ（登録商標）等である場合）デバイス１００自身及び／又はデバイス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）の提供者、製造業者及び／又は開発者であってもよい。商業エンティティサブシステム４００を提供し得る商業エンティティ（例えば、アップル　インコーポレイテッド）は、金融機関サブシステム３５０のいずれの金融エンティティとも別個で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を提供し得る商業エンティティは、エンドユーザデバイス１００上で提供されるクレジットカード又は他の商業クレデンシャルを供給及び／又は管理し得る、いずれ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とも別個かつ／又はそれから独立したものであってもよい。追加的に、又は代替的に、商業エンティティサブシステム４００を提供し得る商業エンティティ（例えば、アップル　インコーポレイテッド）は、販売事業者サブシステム２００のいずれの販売事業者とも別個で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を提供し得る商業エンティティは、非接触近接型通信用の販売事業者端末、オンライン通信用のサードパーティアプリケーション又はオンラインリソース１１３、及び／又は販売事業者サブシステム２００の任意の他の態様を提供し得る販売事業者サブシステム２００のいずれの販売事業者とも別個かつ／又はそれから独立したものであってもよい。このような商業エンティティは、自身がデバイス１００上で金融機関サブシステム３５０によって提供されたクレデンシャルを供給したいと望む場合、及び／又は、このような供給されたクレデンシャルが財務トランザクションに資金供給する販売事業者サブシステム２００との商業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場合、デバイス１００のユーザに対してよりシームレスなユーザエクスペリエンスを提供するために、デバイス１００の種々の構成要素（例えば、商業エンティティが少なくとも部分的にデバイス１００を製造又は管理することができる場合、例えば、デバイス１００のソフトウェア構成要素及び／又はハードウェア構成要素）を構成又は制御する潜在的能力を活用することができる。例えば、いくつかの実施形態では、デバイス１００は、（例えば、デバイス１００と販売事業者サブシステム２００との間のオンライン型セキュアデータ通信の間）より高いレベルのセキュリティを可能にし得る特定のデータの共有及び／又は受信を、デバイス１００のユーザにはシームレスで透過的に、商業エンティティサブシステム４００と（例えば、通信経路６５を介して）通信するように構成されてもよい。図示していないが、商業エンティティサブシステム４００はまた、図１Ａ及び図２の電子デバイス１００のプロセッサ構成要素１０２と同一又は同様であり得るプロセッサ構成要素、図１Ａ及び図２の電子デバイス１００の通信構成要素１０６と同一又は同様であり得る通信構成要素、図２の電子デバイス１００のＩ／Ｏインタフェース１１４と同一又は同様であり得るＩ／Ｏインタフェース、図２の電子デバ

イス１００のバス１１８と同一又は同様であり得るバス、図２の電子デバイス１００のメモリ構成要素１０４と同一又は同様であり得るメモリ構成要素、及び／又は、図２の電子デバイス１００の電源構成要素１０８と同一又は同様であり得る電源構成要素も含むことができ、そのうち１つ、一部又は全部が少なくとも部分的にサーバ４１０によって提供されてもよい。

【００２０】

少なくとも１つの商業クレデンシャルが（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の一部分として）デバイス１００のセキュアエレメント上に供給されることに加えて、デバイス１００が販売事業者サブシステム２００と財務トランザクションをよりセキュアに行うことができるように、アクセス鍵１５５ｂを有する少なくとも１つのアクセスＳＳＤがデバイス１００のセキュアエレメント上に供給されてもよい。例えば、アクセスＳＳＤを少なくとも部分的に、商業エンティティサブシステム４００から直接デバイス１００のセキュアエレメントに供給することができる（例えば、商業エンティティサブシステム４００のサーバ４１０とデバイス１００の通信構成要素１０６との間の通信経路６５を介してアクセスデータ６５２として供給でき、そして、通信構成要素１０６からセキュアエレメント１４５に渡すことができる）。経路６５２を介したアクセスデータ６５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供給されることができ、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１Ａに示すように、商業エンティティサブシステム４００はまた、（例えば、アクセス鍵１５５ｂを用いてデバイス１００によって暗号化されたデータを解読するために）アクセス鍵１５５ｂにアクセスすることもできる。商業エンティティサブシステム４００は、アクセス鍵１５５ｂの管理を担当することができ、管理は、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。商業エンティティサブシステム４００は、アクセス鍵１５５ｂのそのバージョン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内に記憶することができる。アクセス鍵１５５ｂを有するデバイス１００のアクセスＳＳＤは、（例えば、バイオメトリック入力構成要素などのデバイス１００の１つ以上の入力構成要素１１０を介して）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、また、このような判定に応じて、（例えば、デバイス１００のクレデンシャルＳＳＤのクレデンシャルを用いて）決済トランザクションを行うための別の特定のＳＳＤを可能とするように構成されてもよい。このようなアクセス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、財務トランザクションに対するユーザの意図及び財務トランザクションの認証を確実に判定する能力を向上させることができる。また、デバイス１００のこのようなアクセスＳＳＤのアクセス鍵１５５ｂは、デバイス１００のセキュアエレメントの外部に通信され得るトランザクションデータの暗号化を高めるために活用されてもよい。追加的に又は代替的に、以下に説明するように、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発行者セキュリティドメイン（「ＩＳＤ」）に対するＩＳＤ鍵１５６ｋを含むことができ、そのＩＤＳ鍵はまた商業エンティティサブシステム４００によって維持されてもよく、以下に説明するようにアクセス鍵１５５ｂに加えて、又はその代わりに使用されてもよい。

【００２１】

販売事業者アプリケーション又はオンラインリソース１１３は、デバイス１００と販売事業者サブシステム２００との間でオンライン財務トランザクションを促進することを可能とするために、又は販売事業者サブシステム２００によるデバイス１００の任意の他の好適なセキュアデバイス機能性へのオンラインアクセスを可能とするために、デバイス１００によりアクセスすることができる。最初に、このようなアプリケーション１１３は、アプリケーション１１３がデバイス１００によって有効に利用される前に、商業エンティティサブシステム４００によって承認若しくは登録されてもよいし、又は別の方法で可能にされてもよい。例えば、商業エンティティサブシステム４００のアプリケーションストア４２０（例えば、Ａｐｐｌｅ　Ａｐｐ　Ｓｔｏｒｅ（登録商標））は、通信経路８５を介

して販売事業者サブシステム２００からアプリケーション１１３を表す少なくとも一部のデータを受信することができる。また、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のための販売事業者鍵１５７を生成するか、他の方法で割り当てることができ、また、このような販売事業者鍵１５７を販売事業者サブシステム２００に（例えば、経路８５を介して）提供することができる。代替的に、販売事業者サブシステム２００は、アプリケーション１１３のために販売事業者鍵１５７を生成するか、又は他の方法により割り当てることができ、またこのような販売事業者鍵１５７を、商業エンティティサブシステム４００に（例えば、経路８５を介して）提供することができる。販売事業者サブシステム２００又は商業エンティティサブシステム４００のいずれも、販売事業者鍵１５７の管理を担当することができ、管理は、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。このような販売事業者鍵１５７がどのように、又はどこで生成及び／又は管理され得るかにかかわらず、販売事業者サブシステム２００及び商業エンティティサブシステム４００はともに、販売事業者鍵１５７のバージョンを記憶することができる（例えば、販売事業者サブシステム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、その場合、いくつかの実施形態では、（例えば、非対称鍵暗号化／解読プロセスに使用するために）販売事業者サブシステム２００によって記憶された販売事業者鍵１５７は秘密鍵とすることができ、商業エンティティサブシステム４００によって記憶された販売事業者鍵１５７は対応する公開鍵とすることができる）。いくつかの実施形態では、このような販売事業者鍵１５７を販売事業者アプリケーション１１３に特に関連付けることができ、他の実施形態では、販売事業者鍵１５７を販売事業者サブシステム２００の販売事業者に特に関連付けることで、販売事業者鍵１５７は、販売事業者サブシステム２００の同じ販売事業者が稼働させる複数のサードパーティアプリケーション又はウェブリソースに関連付けることができる。一意の販売事業者識別子１６７が、商業エンティティサブシステム４００によって、かつ／又は販売事業者サブシステム２００によって、生成され、かつ／又は、他の方法でアプリケーション１１３に割り当てられ、若しくはアプリケーションに関連付けられてもよい。例えば、販売事業者識別子１６７は、英数字列、ドメイン（例えば、ＵＲＬ、又は、ウェブリソースタイプのオンラインリソースアプリケーション１１３のための）、又は、販売事業者及び／又は特定の販売事業者オンラインリソースを一意に識別する（例えば、それらを商業エンティティサブシステム４００に対して一意に識別する）ことができる他の好適な識別子とすることができる。販売事業者アプリケーション１１３又は販売事業者エンティティの特定の販売事業者識別子１６７と販売事業者鍵１５７を関連付けるために、表４３０又は商業エンティティサブシステム４００にとってアクセス可能であり得る他の好適なデータ構造若しくは情報源が提供され得る。販売事業者オンラインリソースを、特定の販売事業者識別子１６７及び特定の販売事業者鍵１５７と関連付けることができ、それらのそれぞれを、販売事業者サブシステム２００と商業エンティティサブシステム４００との間でセキュアに共有することができる。表４３０は、デバイス１００が鍵１５７及び販売事業者識別子１６７と関連付けられた販売事業者アプリケーション１１３を介して販売事業者サブシステム２００とインタフェースすることを伴い得るトランザクションのために、セキュリティ層を販売事業者サブシステム２００に通信される任意のセキュアデバイスデータ（例えば、デバイス１００にとってネイティブな決済クレデンシャルデータを含み得る商業クレデンシャルデータ）に提供するために、商業エンティティサブシステム４００が適切な販売事業者鍵１５７を決定及び利用することを可能とすることができる。デバイス１００は、アプリケーション１１３に（例えば、アプリケーションストア４２０から通信経路６５を介して）アクセスし、アプリケーション１１３を（例えば、プロセッサ１０２を用いて）実行するように構成することができる。代替的に、又は追加的に、販売事業者鍵１５７及び販売事業者の識別子１６７は、販売事業者のサードパーティネイティブアプリではなく、又はそれに加えて、販売事業者のウェブサイト（例えば、いくつかの実施形態において本明細書において販売事業者オンラインリソース又は販売事業者アプリケーションと呼ぶ場合がある、１つ以上のＵＲＬ又はドメイン）又は販売事業

者と一般に関連付けられてもよい。例えば、販売事業者サブシステム２００の販売事業者は商業エンティティサブシステム４００と協働し、特定の販売事業者ウェブサイト又は販売事業者を一般に表４３０内の特定の販売事業者鍵１５７及び販売事業者識別子１６７と関連付けることができ、それにより、ターゲット又はウェブリソースが販売事業者鍵１５７及び販売事業者識別子１６７に関連付けられ得るＵＲＬ又はドメイン（例えば、そのウェブリソースの一意のドメイン（例えば、store.merchant.com））に向けられ得る、デバイス１００上で実行中の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トランザクションを行うように、デバイス１００が販売事業者サーバ２１０とインタフェースすることを伴い得るトランザクションのため、セキュリティ層を、販売事業者サブシステム２００（例えば、デバイス１００にネイティブな決済クレデンシャルデータを含み得る商業クレデンシャルデータ）に通信された任意のセキュアデバイスデータに提供するために、商業エンティティサブシステム４００が適切な販売事業者鍵１５７を決定及び利用することを可能とすることができる。デバイス１００は、例えば、販売事業者サーバ２１０から通信経路１５を介して、このようなＵＲＬに（例えば、このような販売事業者ウェブリソースをターゲットにする際に販売事業者オンラインリソースとみなすことができるデバイス１００上のインターネットアプリケーション１１３を用いて）アクセスするように構成することができる。他の実施形態では、アプリケーション１１３を、特定の販売事業者、販売事業者サブシステム２００、販売事業者鍵１５７及び／又は販売事業者識別子１６７と関連付けられず、代わりに、そのような販売事業者ウェブリソースをターゲットとするウェブ表示によりデバイス１００が利用可能であり、それにより販売事業者オンラインリソースの役割を果たす独立したアプリケーションとすることができる。商業エンティティサブシステム４００による販売事業者オンラインリソースのこのような登録（例えば、（例えば、表４３０に記憶するための）販売事業者サブシステム２００と商業エンティティサブシステム４００との間での販売事業者鍵１５７及び販売事業者識別子１６７の、セキュアかつ妥当性検査された共有）を、販売事業者サブシステム２００がオンラインリソースの正当な所有者であることを商業エンティティサブシステム４００に対し確実とする任意の好適な方法で実行することができる。上述のように、販売事業者オンラインリソース（例えば、ネイティブアプリ、ドメイン／ＵＲＬ、又は任意の他の好適なウェブリソース、又はおそらく販売事業者端末でも）を、（例えば、図５のステップ５０１及び／又は図６のステップ６０６での登録の間）特定の販売事業者識別子１６７及び特定の販売事業者鍵１５７と関連付けることができ、それらのそれぞれを、任意の好適な方法で販売事業者サブシステム２００と商業エンティティサブシステム４００との間でセキュアに共有することができ、そのような関連付けを、（例えば、表４３０で）商業エンティティサブシステム４００にとってアクセス可能にすることができる。

【００２２】

図２の説明

ここで図２を参照すると、図２は図１及び図１Ａに関して上記したシステム１の電子デバイス１００のより詳細な図を示している。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、通信構成要素１０６、電源１０８、入力構成要素１１０、出力構成要素１１２、アンテナ１１６、近距離無線通信（「ＮＦＣ」）構成要素１２０を含むことができる。電子デバイス１００はまた、デバイス１００の他の種々の構成要素に、それらから、又はそれらの間で、データ及び／又は電力を転送するための１つ以上の有線若しくは無線通信リンク又は経路を提供し得るバス１１８を含むことができる。電子デバイス１００は、デバイス１００の外部のゴミ又は他の劣化力から保護するためにデバイス１００の構成要素のうち１つ以上を少なくとも部分的に囲み得る筐体１０１を備えることもできる。いくつかの実施形態では、電子デバイス１００の１つ以上の構成要素を組合せてもよいし、又は省略してもよい。また、電子デバイス１００は、図２に組み合わされていない、又は含まれていない他の構成要素を含んでもよい。例えば、電子デバイス１００は、図２に示す構成要素の任意の他の好適な構成要素又はいくつかの実例を含むことができる。簡潔にするために、図２では、それぞれの構成要素のうち１つだけ

を示している。１つ以上の入力構成要素１１０を、ユーザに、デバイス１００と相互作用（interact）又はインタフェースさせるように設けてもよいし、及び／又は、１つ以上の出力構成要素１１２を、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／又は触覚情報）を提示するように設けてもよい。ここで、１つ以上の入力構成要素及び１つ以上の出力構成要素を、本明細書では、入出力（「Ｉ／Ｏ」）構成要素又はＩ／Ｏインタフェース１１４と総称する（例えば、入力構成要素１１０及び出力構成要素１１２をＩ／Ｏ構成要素又はＩ／Ｏインタフェース１１４と総称する）場合があることを留意されたい。例えば、入力構成要素１１０及び出力構成要素１１２は、表示画面へのユーザのタッチにより入力情報を受信でき、また同一の表示画面を介してユーザに視覚情報を提供し得るタッチスクリーンなど、単一のＩ／Ｏ構成要素１１４である場合がある。電子デバイス１００のプロセッサ１０２は、電子デバイス１００の１つ以上の構成要素の動作及び性能を制御するように機能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、入力構成要素１１０から入力信号を受信することができ、かつ／又は出力構成要素１１２を通して出力信号を駆動することができる。図２に示すように、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ためにプロセッサ１０２を使用することができる。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ってもよく、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であってもよいし、他の好適なオンラインリソース（例えば、販売事業者サブシステム２００の販売事業者に関連付けられたアプリケーション）であってもよい。また、図示するように、プロセッサ１０２は、デバイス１００を識別するためにデバイス１００のユーザ及び／又は商業エンティティサブシステム４００によって利用され得るデバイス識別情報１１９にアクセスすることができる。

【００２３】

ＮＦＣ構成要素１２０は、電子デバイス１００と販売事業者サブシステム２００の販売事業者端末（例えば、販売事業者決済端末２２０）との間の非接触近接型トランザクション又は通信を可能にし得る任意の好適な近接型通信メカニズムとすることができる。ＮＦＣ構成要素１２０は、電子デバイス１００とそのような販売事業者端末との間の非接触近接型通信を可能とする任意の好適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構成要素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、ＮＦＣブースタ１３６を含むことができる。ＮＦＣデータモジュール１３２は、非接触近接型通信又はＮＦＣ通信の一部としてＮＦＣ構成要素１２０により販売事業者端末に送信され得る好適なデータを収容し、経路設定し、又はその他機能により提供するように構成されてもよい。追加的に、又は代替的に、ＮＦＣデータモジュール１３２は、非接触近接型通信の一部として販売事業者端末からＮＦＣ構成要素１２０により受信され得る好適なデータを収容し、経路設定し、又はその他機能により受信す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、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、電子デバイス１００と販売事業者端末との間でＮＦＣ通信を通信するためにＮＦＣ構成要素１２０を可能とする、アクティブにする、許可する、及び／又は、その他機能により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構成要素１２０の働きを決定づけるのを助ける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のに使用され得る、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とともに動作し、電子デバイス１００と販売事業者サブシステム２００との間の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、耐タンパ性であってもよく、セキュアエレメント１４５の少なくとも一部分（例えば、図２Ａ参照）を提供してもよい。例えば、このようなセキュアエレメントは、耐タン

パ性プラットフォームを提供するように構成されてよく（例えば、単一チップ又は複数チップセキュアマイクロコントローラとして）、認証され信頼された権限者の集合（例えば、金融機関サブシステム及び／又はＧｌｏｂａｌＰｌａｔｆｏｒｍのような業界標準の権限者）によって定められ得る規則及びセキュリティ要件に従って、アプリケーションならびにそれらの機密データ及び暗号データ（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し得る。

【００２４】

図２に示すように、例えば、ＮＦＣメモリモジュール１５０は、ＮＦＣ仕様標準（例えば、ＧｌｏｂａｌＰｌａｔｆｏｒｍ）によって定義及び管理され得る、発行者セキュリティドメイン（「ＩＳＤ」）１５２及び補足的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」）等）のうちの１つ以上を含むことができる。例えば、ＩＳＤ１５２は、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）が、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、（例えば、通信構成要素１０６を介して）電子デバイス１００上に、１つ以上のクレデンシャル（例えば、各種クレジットカード、銀行カード、ギフトカード、アクセスカード、交通パスなどに関連付けられたクレデンシャル）を形成し、又は他の方法で供給するための鍵及び／又は他の好適な情報を記憶することができる、ＮＦＣメモリモジュール１５０の一部分であり得る。クレデンシャルは、ユーザ／消費者に割り当てられ、かつ電子デバイス１００上にセキュアに記憶され得る、クレジットカード決済番号（例えば、デバイス主アカウント番号（「ＤＰＡＮ」）、ＤＰＡＮ有効期限、ＣＶＶ等（例えば、トークン又はその他として））などの、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）を、特定の特典又は決済権を電子デバイス１００に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により供給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衆交通カードクレデンシャル）と関連付けることができる。一方、第２のＳＳＤ１５４ｂ（例えば、アクセスＳＳＤ１５４ｂ）を、別のＳＳＤ（例えば、第１のＳＳＤ１５４ａ）の特定のクレデンシャルに対するデバイス１００のアクセスを制御して、例えば、特定の特典又は決済権を電子デバイス１００に提供し得る商業エンティティ（例えば、デバイス１００用の制御エンティティと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）と関連付けることができる。代替的に、第１のＳＳＤ１５４ａ及び第２のＳＳＤ１５４ｂのうちのそれぞれを、電子デバイス１００に特定の特典又は決済権を提供し得る各特定のクレデンシャル（例えば、金融機関サブシステム３５０によって供給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衆交通カードクレデンシャル）と関連付けることができる。各ＳＳＤ１５４は、少なくとも１つのアプレット１５３を含むことができ、かつ／又はそのアプレットと（例えば、ＳＳＤ１５４ａはアプレット１５３ａと、ＳＳＤ１５４ｂはアプレット１５３ｂと）関連付けられてもよい。例えば、ＳＳＤ１５４のアプレット１５３を、（例えば、ＧｌｏｂａｌＰｌａｔｆｏｒｍ環境で）ＮＦＣ構成要素１２０のセキュアエレメント上で実行され得るアプリケーションとすることができる。クレデンシャルアプレット１５３は、クレデンシャル情報１６１を含むことができ、又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）と関連付けられることができる。各ＳＳＤ１５４及び／又はアプレット１５３は、自身の鍵１５５のうち少なくとも１つを含むこともでき、かつ／又はそれ自身の鍵のうち少なくとも１つと（例えば、アプレット１５３ａは少なくとも１つの鍵１５５ａと、アプレット１５３ｂは少なくとも１つの鍵１５５ｂと）に関連付けられてもよい。

【００２５】

ＳＳＤ１５４の鍵１５５は、暗号アルゴリズム又は暗号の関数出力を決定し得る情報とすることができる。例えば、暗号化では、鍵は、平文から暗号文への特定の変換を指定することができ、又は解読中はその逆とすることができる。鍵はまた、デジタル署名方式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使用されてもよい。ＳＳＤの鍵は、好適な共有秘密を別のエンティティに提供することができる。鍵及びアプレットのそれぞれを、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上にロードしてもよいし、デバイス１００上に初めて提供されるときに、セキュアエレメント上に事前ロードしてもよい。一例として、クレデンシャルＳＳＤ１５４ａを特定のクレジットカードクレデンシャルと関連付けることができる一方、その特定のクレデンシャルは、デバイス１００のセキュアエレメントから（例えば、ＮＦＣ構成要素１２０から）販売事業者サブシステム２００に対する商業クレデンシャルデータ通信として、クレデンシャルＳＳＤ１５４ａのアプレット１５３ａがかかる使用に対して可能にされている、又は他の方法でアクティブにされている、又はロック解除されている場合に行う財務トランザクションのためにのみ、通信可能である。

【００２６】

ＮＦＣ構成要素１２０の使用を可能とするため、クレデンシャルのクレジットカード情報又は銀行アカウント情報などの機密決済情報を、電子デバイス１００から販売事業者サブシステム２００に送信する際に特に有用であり得るセキュリティ特徴を提供してもよい。このようなセキュリティ特徴はまた、アクセスが制限され得るセキュア記憶領域を含むことができる。セキュア記憶領域にアクセスするために、例えば、個人識別番号（「ＰＩＮ」）の入力を介した、又はバイオメトリックセンサとのユーザ相互作用を介したユーザ認証を提供することが必要とされ得る。例として、アクセスＳＳＤ１５４ｂは、他のＳＳＤ１５４（例えば、クレデンシャルＳＳＤ１５４ａ）をそのクレデンシャル情報１６１ａを通信するために使用することを可能とする前に、このような認証が生じているかどうかを判定するためにアプレット１５３ｂを活用することができる。特定の実施形態では、セキュリティ特徴の一部又は全部がＮＦＣメモリモジュール１５０内に記憶されてもよい。更に、商業クレデンシャルデータを販売事業者サブシステム２００と通信するための認証鍵のようなセキュリティ情報を、ＮＦＣメモリモジュール１５０内に記憶してもよい。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内に埋め込まれたマイクロコントローラを含むことができる。一例としては、アクセスＳＳＤ１５４ｂのアプレット１５３ｂは、（例えばバイオメトリック入力構成要素などの１つ以上の入力構成要素１１０を介して）のデバイス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することができ、そのような判定に応じて、（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行うために別の特定のＳＳＤを可能とするように構成することができる。

【００２７】

図２Ａの説明

ここで図２Ａを参照すると、図２Ａは、図１～図２に関して上記したシステム１の電子デバイス１００の一部分の別の詳細図を示している。図２Ａに示すように、例えば、デバイス１００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１６１ａ、アクセス鍵１５５ａ、及び／若しくはクレデンシャル鍵１５５ａ’を含み得る、又は、アプレット１５３ａ、クレデンシャル１６１ａ、アクセス鍵１５５ａ、及び／若しくはクレデンシャル鍵１５５ａ’に関係付けられ得るＳＳＤ１５４ａと、アプレット１５３ｂ、クレデンシャル１６１ｂ、アクセス鍵１５５ｂ、及び／若しくはクレデンシャル鍵１５５ｂ’を含み得る、又は、アプレット１５３ｂ、クレデンシャル１６１ｂ、アクセス鍵１５５ｂ、及び／若しくはクレデンシャル鍵１５５ｂ’に関係付けられ得るＳＳＤ１５４ｂとを含むことができる。いくつかの実施形態において、特定の補足的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）を、特定のＴＳＭ及び、電子デバイス１００に特定の特典又は決済権を提供し得る少なくとも１つの特定の商業クレデンシャル（例えば、特定のクレジットカードクレデンシャル又は特定の公衆交

通カードクレデンシャル）と関連付けることができる。各ＳＳＤ１５４は、ＮＦＣデバイスモジュール１３０によって使用されるＳＳＤ１５４の機能を可能とするために、アクティブ化を必要とすることがある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る。追加的に又は代替的に、各ＳＳＤ１５４は、特定の商業クレデンシャルと関連付けられ得る、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）（例えば、ＳＳＤ１５４ａのクレデンシャルアプレット１５３ａを第１の商業クレデンシャルと関連付けることができ、かつ／又は、ＳＳＤ１５４ｂのクレデンシャルアプレット１５３ｂを第２の商業クレデンシャルと関連付けることができる）のうち少なくとも１つを含むことができ、かつ／又はそれと関連付けられることができ、クレデンシャルアプレットは自身のアクセス鍵（例えば、クレデンシャルアプレット１５３ａ用のアクセス鍵１５５ａ及び／又はクレデンシャルアプレット１５３ｂ用のアクセス鍵１５５ｂ）、及び／又は、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用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用のクレデンシャル鍵１５５ｂ’）を有することができ、クレデンシャルアプレットは、（例えば、販売事業者端末２２０による）ＮＦＣ通信として、かつ／又は（例えば、商業エンティティサブシステム４００を介した）電子デバイス１００と販売事業者サブシステム２００との間のオンライン型通信として、ＮＦＣデバイスモジュール１３０によって使用される、その関連付けられた商業クレデンシャルを可能とするためにアクティブ化を必要とすることがある。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用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用のクレデンシャル鍵１５５ｂ’）は、（例えば、販売事業者サブシステム２００を介した）セキュアエレメント１４５と金融機関サブシステム３５０との間の当該アプレットの当該クレデンシャル情報のセキュアな送信を可能とするため、そのようなクレデンシャルを担当することができ、かつ（例えば、図１Ａに示すように）金融機関サブシステム３５０によってアクセス可能とすることができる金融機関サブシステム３５０によって生成されてもよい。追加的に、又は代替的に、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用のアクセス鍵１５５ａ及び／又はクレデンシャルアプレット１５３ｂ用のアクセス鍵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、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との間で当該アプレットの当該クレデンシャル情報のセキュアな送信を可能とするため、（例えば、図１Ａに示すように）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とすることができる。追加的に、又は代替的に、図示するように、各アプレットは、それ自体の一意のアプリケーション識別子（「ＡＩＤ」）、例えば、アプレット１５３ａのＡＩＤ１５５ａａ及び／又はアプレット１５３ｂのＡＩＤ１５５ｂａを含むことができる。例えば、ＡＩＤは、特定のカード方式及び製品、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、ＡＩＤは、ＡＩＤに関連付けられたクレデンシャルの決済システム（例えば、カード方式）又はネットワーク（例えば、ＭａｓｔｅｒＣａｒｄ、Ｖｉｓａ、Ｉｎｔｅｒａｃなど）を識別するのに使用され得る登録されたアプリケーションプロバイダ識別子（「ＲＩＤ」）だけでなく、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間を区別するのに使用され得る専用アプリケーション識別子拡張（「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統括するように機能し得る任意の好適な仕様（例えば、Ｊａｖａ(登録商標)カード仕様）は、セキュアエレメント１４５上の各ＡＩＤの一意性を確実とするか、又は他の方法で強制するように機能することができる（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をそれ自体の一意のＡＩＤと関連付けることができる）。

【００２８】

追加的に、又は代替的に、図２Ａに示すように、セキュアエレメント１４５はＩＳＤ１

５２を含むことができ、それは、そのセキュリティドメイン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１Ａに示す、商業エンティティサブシステム４００）にも知られた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と電子デバイス１００のセキュアエレメント１４５との間のセキュアな送信を可能とするために、アクセス鍵１５５ａ及び／又はアクセス鍵１５５ｂと同様に、かつ／又はその代わりに、商業エンティティサブシステム４００及び電子デバイス１００によって活用されることがある。また、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との間で各種データを通信してもよい。例えば、デバイス１００のプロセッサ１０２は、プロセッサ１０２の販売事業者アプリケーション１１３、ならびに、セキュアエレメント１４５、（例えば、Ｉ／Ｏ入力データ１１５ｉを受信するための、かつ／又は、Ｉ／Ｏ出力データ１１５ｏを送信するための）Ｉ／Ｏインタフェース構成要素１１４ａ及び／又は通信構成要素１０６と、情報を通信することができるデバイスアプリケーション１０３を実行するように構成することができる。また、図示するように、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との間のセキュアな通信を可能とするために利用され得る。

【００２９】

追加的に、又は代替的に、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、サードパーティオンエレメントの信頼のルート（ｔｈｉｒｄ－ｐａｒｔｙ　ｏｎ－ｅｌｅｍｅｎｔ　ｒｏｏｔ　ｏｆ　ｔｒｕｓｔ）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とすることができる。ＣＡＳＤ１５８に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／又は特定の管理層（例えば、ＧｌｏｂａｌＰｌａｔｆｏｒｍ管理層）へのグローバルサービスとして、オンエレメント機密鍵生成を提供するように構成されてもよい。ＣＡＳＤ１５８内で使用され得る機密鍵素材は、セキュアエレメント１４５の発行者を含むいかなるエンティティによっても検査又は修正されないように構成されてもよい。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／又はＣＡＳＤ署名モジュール）を含むように構成されてもよく、かつ／又はそれを生成し、かつ／又は他の方法で、それを含むように構成されてもよい。例えば、ＣＡＳＤ１５８は、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構成要素１０６）に特定のデータを提供する前に、セキュアエレメント１４５上で特定のデータに（例えば、ＣＡＳＤアクセスキット１５８ｋを用いて）署名するように構成することができる。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し、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（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を用いて）確認することができるように構成され得る。

【００３０】

追加的に、又は代替的に、図２Ａに示すように、セキュアエレメント１４５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、アクティブ化され、非アクティブ化された、ロックされた、など）を修正し、特定のライフサイクル状態での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インタフェース１１４ａを介して）共有するための電子デバイス１００にローカル機能性を提供するように構成され得る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を維持し得るＣＲＳリスト１５１ｔ（例えば、ＳＳＤ１５４ａのクレデンシャルアプレット１５３ａ及び／又はＳＳＤ１

５４ｂのクレデンシャルアプレット１５３ｂの１つ、一部又は全部のライフサイクル状態を含み得るリスト）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、（例えば、オペレーティングシステムアプリケーション１０３内のバックグラウンドプロセスとして実行し得るカード管理デーモン（「ＣＭＤ」）アプリケーション１０３ａ及び／又はカード管理アプリケーション１０３ｂ（例えば、アップル　インコーポレイテッドによるＰａｓｓｂｏｏｋ（登録商標）又はＷａｌｌｅｔ（登録商標）アプリケーション）及び／又は販売事業者アプリケーション１１３（例えば、販売事業者鍵１５７及び販売事業者識別子１６７と関連付けられ得る販売事業者オンラインリソース）及び／又は識別サービス（「ＩＤＳ」）アプリケーション１０３ｃなどのデーモンのような任意の好適なアプリケーションタイプであって、必ずしもデバイス１００のインタラクティブなユーザの制御下にある必要はない）デバイス１００のアプリケーションと共有するように構成され得、また、それは、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インタフェース１１４ａ及びユーザインタフェース（「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１０３ｂのＵＩ）を介して提供することができ、それにより、（例えば、特定のクレデンシャルアプレットの商業クレデンシャルを財務トランザクションに使用可能とするよう、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）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可能とすることができる。追加的に、又は代替的に、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１Ａに示すような、商業エンティティサブシステム４００）にも知られ得るＣＲＳアクセス鍵１５１ｋを含むことができる。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との間のセキュアな送信を可能とするため、アクセス鍵１５５ａ及び／又はアクセス鍵１５５ｂと同様に、かつ／又はそれの代わりに、ＣＲＳアクセス鍵１５１ｋを商業エンティティサブシステム４００及び電子デバイス１００により活用することができる。

【００３１】

ＩＤＳアプリケーション１０３ｃは、オペレーティングシステムアプリケーション１０３及び／又はカード管理アプリケーション１０３ｂの内部でバックグラウンドプロセスとして実行し得る、かつ／又はＣＭＤアプリケーション１０３ａによって提供され得るデーモンのような任意の好適なアプリケーションタイプとすることができ、また、それは、任意の好適なＩＤＳサービ上で送信され得るＩＤＳメッセージをリスニングし、それに応答するＩＤＳマネージャとして動作することができ、ＩＤＳマネージャは、アップル　インコーポレイテッドによるｉＭｅｓｓａｇｅ（登録商標）など（例えば、アップル　インコーポレイテッドによるＦａｃｅＴｉｍｅ（登録商標）又はＣｏｎｔｉｎｕｉｔｙ（登録商標））のような任意の好適なメッセージングサービスと同様とすることができ、これにより、ホストデバイス１００のＩＤＳアプリケーション１０３ｃと別のデバイス（例えば、クライアントデバイス）同様のＩＤＳアプリケーションとの間のメッセージの一意のエンドツーエンド暗号化を可能とすることができる。そのようなメッセージを、通信デバイスの一方又は両方の、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用いて暗号化することもできる。このようなメッセージを、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）通信として通信してもよいし、商業エンティティサブシステム４００を介して（例えば、識別管理システム構成要素４７０を介して）通信してもよい。このようなメッセージングを、構造化されたフォーマット（例えば、プロトコルバッファ）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し得る低遅延ソリューションとして可能とすることができる。ＩＤＳアプリケーション１０３ｃは、ＩＤＳメッセージが受信されたとき、実行されていない場合は、自動的に起動され得る。ＩＤＳアプリケーション１０３ｃは、受信したＩＤＳ通信に関するユーザインタフェース表示及び要求されたデータに関する要求デバイスへの応答を見張るよう機能し得る。ホストデバイスのＩＳＤアプリケーション１０３ｃは、初期要求をクライアント

デバイスから検出し得るときに、カード管理アプリケーション１０３ｂのカード管理デーモンアプリケーション１０３ａを稼働状態に復帰させるように機能することができ、これにより、ホストデバイスが低電力「スリープ」モードで動作することを可能とすることができる。ＩＤＳアプリケーション１０３ｃは、追加的に又は代替的に、このような要求の「タイムアウト」を管理するように機能することができ、それにより、クライアントデバイスからの決済の要求がホストデバイス上で一定期間（例えば、そのような要求に応答するホストデバイスの能動的なユーザ対応がない場合、６０秒）アクションがない場合、ＩＤＳアプリケーション１０３ｃは、要求を終了させてホストデバイスが「キャンセル」状態を生成しクライアントデバイスに配信する結果となり得る判定を行うように機能することができ、それにより、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対する「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３Ｄの説明

【００３２】

図３に示すように、また以下により詳細に説明するように、電子デバイス１００の特定の例としてはｉＰｈｏｎｅ（登録商標）のようなハンドヘルド型電子デバイスとすることができ、筐体１０１は、デバイス１００とユーザならびに／又は周辺環境とが互いにインタフェースし得る種々の入力構成要素１１０ａ～１１０ｉ、種々の出力構成要素１１２ａ～１１２ｃ、及び種々のＩ／Ｏ構成要素１１４ａ～１１４ｄへのアクセスを可能とすることができる。例えば、タッチスクリーンＩ／Ｏ構成要素１１４ａは、表示出力構成要素１１２ａ及び関連タッチ入力構成要素１１０ｆを含むことができ、表示出力構成要素１１２ａは、ユーザが電子デバイス１００と相互作用することを可能にし得る視覚又はグラフィックユーザインタフェース（「ＧＵＩ」）１８０を表示するために使用されてもよい。ＧＵＩ１８０は、表示出力構成要素１１２ａの領域の全部又は一部に表示され得る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）の種々の層、ウィンドウ、画面、テンプレート、要素、メニュー、及び／又は他の構成要素を含むことができる。例えば、図３に示すように、ＧＵＩ１８０は、ＧＵＩ１８０の１つ以上のグラフィック要素又はアイコン１８２を有する第１の画面１９０を表示するように構成することができる。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、販売事業者オンラインリソースアプリケーションなどの、当該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することができる。例えば、「Ｍｅｒｃｈａｎｔ　Ａｐｐ」テキストインジケータ１８１（すなわち、特定のアイコン１８３）がラベル付けされた特定のアイコン１８２がデバイス１００のユーザにより選択されると、デバイス１００は、特定のサードパーティ販売事業者アプリケーション（例えば、ネイティブアプリケーション又はハイブリッドアプリケーション）を起動し、又は他の方法で、それにアクセスすることができる。別の例として、「Ｉｎｔｅｒｎｅｔ」テキストインジケータ（すなわち、特定のアイコン１８４）がラベル付けされた特定のアイコン１８２がデバイス１００のユーザにより選択されると、デバイス１００は、別のタイプの販売事業者オンラインリソースをデバイス１００に提供するための特定のサードパーティ販売事業者のウェブリソースのＵＲＬに向けられ得るインターネットブラウザアプリケーションを起動し、又は他の方法でそれにアクセスすることができる。任意の好適な販売事業者オンラインリソースがアクセスされると、デバイス１００は、特定の方法（例えば、デバイス１００の任意のセキュア機能を実行するために（例えば、デバイス１００のＮＦＣ構成要素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）を用いて販売事業者サブシステム２００に決済を行うために）、デバイスユーザにより使用され得る任意の好適なアプリケーション（例えば、販売事業者オンラインリソース１１３）の使用中の、ＧＵＩ１８０のこのような表示の特定の例のための図３Ａ～図３Ｄ参照）でデバイス１００を用いて当該販売事業者オンラインリソースと相互作用するための１つ以上のツール又は特徴を含み得る特定のユーザインタフェースの画面を表示するように機能することができる。各アプリケーションに対して、

画面は表示出力構成要素１１２ａ上に表示されてもよく、種々のユーザインタフェース要素を含んでもよい。追加的に、又は代替的に、各アプリケーションに対して、他の種々のタイプの非視覚情報を、デバイス１００の種々の他の出力構成要素１１２を介してユーザに提供してもよい。例えば、いくつかの実施形態では、デバイス１００は、ＧＵＩを提供するように機能するユーザインタフェース構成要素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供給するために決済クレデンシャルの使用を選択及び認証するための、又はデバイスの他の好適なセキュアな任意の機能を行うための、オーディオ出力構成要素及び機械的又は他の好適なユーザ入力構成要素を提供してもよい。

【００３３】

図４の説明

ここで図４を参照すると、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している。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とすることができ、セキュアモバイルプラットフォーム（「ＳＭＰ」）ブローカ構成要素４４０、ＳＭＰ信頼サービスマネージャ（「ＴＳＭ」）構成要素４５０、ＳＭＰ暗号サービス構成要素４６０、識別管理システム（「ＩＤＭＳ」）構成要素４７０、不正システム構成要素４８０、ハードウェアセキュリティモジュール（ＨＳＭ）構成要素４９０、ストア構成要素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、一部、又は全部の構成要素を、デバイス１００のプロセッサ構成要素１０２と同一又は類似であり得る１つ以上のプロセッサ構成要素、デバイス１００のメモリ構成要素１０４と同一又は類似であり得る１つ以上のメモリ構成要素、及び／又は、デバイス１００の通信構成要素１０６と同一又は類似であり得る、１つ以上の通信構成要素を使用して実施することができる。商業エンティティサブシステム４００の１つ、一部又は全部の構成要素は、金融機関サブシステム３５０及び／又は販売事業者サブシステム２００とは別個の独立したものであり得る単一の商業エンティティ（例えば、アップル　インコーポレイテッド）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の構成要素は、新しいセキュリティ層を提供するために、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ために、互いに相互作用することができ、また、任意の好適な金融機関サブシステム３５０及び／又は電子デバイス１００及び／又は販売事業者サブシステム２００と集合的に相互作用することができる。

【００３４】

商業エンティティサブシステム４００のＳＭＰブローカ構成要素４４０は、商業エンティティユーザアカウントを用いたユーザ認証を管理するように構成することができる。ＳＭＰブローカ構成要素４４０はまた、デバイス１００上のクレデンシャルのライフサイクル及び供給を管理するように構成することができる。ＳＭＰブローカ構成要素４４０は、デバイス１００上のユーザインタフェース要素（例えば、ＧＵＩ１８０の要素）を制御し得る主エンドポイントとすることができる。オペレーティングシステム又はエンドユーザデバイスの他のアプリケーション（例えば、デバイス１００のアプリケーション１０３、アプリケーション１１３、及び／又はアプリケーション１４３）は、特定のアプリケーションプログラムインタフェース（「ＡＰＩ」）を呼び出すように構成することができ、またＳＭＰブローカ４４０は、これらのＡＰＩの要求を処理し、デバイス１００のユーザインタフェースを導き出し得るデータで応答するように、及び／又は、セキュアエレメント１４５と（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との間の通信経路６５を介して）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」）で応答するように構成することができる。このようなＡＰＤＵは、金融機関サブシステム３５０から、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との間の通信経路５５のＴＳＭ）を介して商業エンティティサブシステム４００により受信され得る。商業エンティティサブシステム４００のＳＭＰ　ＴＳＭ構成要素４５０は、金融機関サブシ

ステム３５０からのデバイス１００へのクレデンシャル供給動作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好適なサービスを提供するように構成することができる。ＧｌｏｂａｌＰｌａｔｆｏｒｍ、又は任意の他の好適なセキュアなチャネルプロトコルは、ＳＭＰ　ＴＳＭ構成要素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との間のセキュアな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との間で、機密なアカウントデータを適正に通信及び／又は供給することを可能とすることができる。

【００３５】

ＳＭＰ　ＴＳＭ構成要素４５０は、ＨＳＭ構成要素４９０を使用してその鍵を保護し、新しい鍵を生成するように構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暗号サービス構成要素４６０は、システム１の種々の構成要素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動作を提供するように構成することができる。ＳＭＰ暗号サービス構成要素４６０は、セキュアな鍵記憶及び／又は不透明な暗号動作のためにＨＳＭ構成要素４９０を利用することができる。ＳＭＰ暗号サービス構成要素４６０の決済暗号サービスは、ＩＤＭＳ構成要素４７０と相互作用し、ファイル上のクレジットカードに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（登録商標）アカウント）と関連付けられた他のタイプの商業クレデンシャルを取り出すように構成することができる。このような決済暗号サービスは、メモリ内のそのユーザアカウントの商業クレデンシャル（例えば、クレジットカード番号）を記述する平文（例えば、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の唯一の構成要素となるように構成することができる。ＩＤＭＳ構成要素４７０は、（例えば、商業エンティティ固有サービス（例えば、アップル　インコーポレイテッドによるｉＭｅｓｓａｇｅ（登録商標））を用いた）識別サービス（「ＩＤＳ」）転送のような、デバイス１００と別のデバイスとの間の好適な通信を可能とする、かつ／又は管理するように構成することができる。例えば、特定のデバイスを、そのようなサービスに対して自動で又は手動で登録することができる（例えば、商業エンティティ４００のエコシステム内のすべてのデバイスを、そのサービスに対して自動で登録することができる）。サービスを使用して（例えば、デバイス１００のＩＳＤアプリケーション１０３ｃを使用して）メッセージが送信可能となる前に、このようなサービスは、アクティブな登録を要求し得るエンドツーエンド暗号化メカニズムを提供することができる。商業エンティティサブシステム４００が、特定のユーザアカウントと関連付けられた特定のクライアントデバイス（例えば、商業エンティティサブシステム４００とのファミリーアカウントの複数のデバイス）にとって利用可能であり得る１つ以上の非ネイティブ決済クレデンシャルを効率的かつ効果的に識別するように機能することができるように、ＩＤＭＳ構成要素４７０及び／又は他の好適な任意のサーバ若しくは運用エンティティサブシステム４００の一部分は、所与のユーザアカウント又は他のものと関連付けられた任意の電子デバイス上に供給された任意のクレデンシャルの状況を識別するように、又は他の方法で検索するように機能することができる。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構成要素４８０は、商業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既知のデータ（例えば、商業エンティティによりユーザアカウントと関連付けられたデータに基づいて（例えば、商業クレデンシャル情報）、及び／又は商業エンティティの制御下にあり得る他の好適な任意のデータ、及び／又は金融機関サブシステム３５０の制御下にないかも知れない他の好適な任意のデータに基づいて）、商業クレデンシャルに関する商業エンティティ不正検査を実行するように構成することができる。商業エンティティ不正システム構成要素４８０は、種々の要因又は閾値に基づいて、クレデンシャルに対する商業エンティティ不正スコアを決定するように構成されてもよい。追加的に、又は代替的に、商業エンティティサブシステム４００は、デバイス１００のユーザへの種々のサービスのプロバイダでありうるストア４２０（例えば、デバイス１００により再生されるメディアを販売／レンタルするｉＴｕｎｅｓ（登録商標）Ｓｔｏｒｅ、デバイス１００上で使用するアプリケーションを販売／レンタルするＡ

ｐｐｌｅ　Ａｐｐ　Ｓｔｏｒｅ（登録商標）、デバイス１００からのデータを記憶しかつ／又は複数のユーザデバイス及び／又は複数のユーザプロファイルを互いに関連付けるＡｐｐｌｅ　ｉＣｌｏｕｄ（登録商標）Ｓｅｒｖｉｃｅ、種々のＡｐｐｌｅ製品をオンラインで購入するＡｐｐｌｅ　Ｏｎｌｉｎｅ　Ｓｔｏｒｅなど）を含んでもよい。一例として、ストア４２０は、アプリケーション１１３を管理し、デバイス１００に（例えば、通信経路６５を介して）提供するように構成することができ、アプリケーション１１３は、銀行業務アプリケーション、商業販売事業者アプリケーション、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、又は他の好適な任意の通信アプリケーションなどの好適な任意のアプリケーションとすることができる。（例えば、図４の少なくとも１つの通信経路４９５を介して）商業エンティティサブシステム４００の種々の構成要素間でデータを通信するために、及び／又は商業エンティティサブシステム４００とシステム１の他の構成要素（例えば、図１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１の通信経路６５を介した電子デバイス１００）の間でデータを通信するために、好適な任意の通信プロトコル又は通信プロトコルの組合せを商業エンティティサブシステム４００により使用することができる。

【００３６】

図５の説明

図５は、セキュアデバイス機能へのオンラインアクセスを妥当性検査するための例示的なプロセス５００のフローチャートである。プロセス５００は、電子デバイス１００、商業エンティティサブシステム４００、及び販売事業者サブシステム２００によって実施するように示されている。しかし、プロセス５００は、他の任意の好適な構成要素又はサブシステムを用いて実施され得ることを理解されたい。プロセス５００は、販売事業者サブシステム２００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型決済）における電子デバイス１００でのクレデンシャルのセキュアな使用を可能とするための、又は電子デバイス１００の任意の他の好適なデータ（例えば、位置データ、健康データ、又は任意の他のプライベートデータ又は有効に妥当性検査されていないサードパーティサブシステムと共有されるべきではないもの）の販売事業者サブシステム２００によるセキュアなアクセスを可能とするための、商業エンティティサブシステム４００による販売事業者サブシステム２００の妥当性検査などの、販売事業者サブシステム２００による電子デバイス１００のセキュア機能へのオンラインアクセスを可能とするために、サードパーティ販売事業者サブシステム２００をセキュアにかつ効率的に妥当性検査する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。販売事業者オンラインリソース又は鍵若しくはサーバ若しくは端末若しくは識別子などの販売事業者サブシステム２００及び／又はそのいずれかの特徴を記述するために用語「販売事業者（merchant）」を利用することができるが、サブシステム２００は、電子デバイス１００の所有者又はユーザとは、及び／又は商業（又は運用）エンティティサブシステム４００とは別個であり得る、任意の好適なサードパーティエンティティによって動作される任意の好適なサブシステム（例えば、処理サブシステム（例えば、データ処理サブシステム））とすることができることを理解されたい。例えば、販売事業者サブシステム２００は、電子デバイス１００のセキュアデバイス機能へのアクセス又は他の方法による、受信若しくは相互作用（例えば、販売事業者オンラインリソースを用いた、デバイス１００へのデータのロード（例えば、デバイス１００への決済クレデンシャルの供給）、デバイス１００からのデータの受信（例えば、デバイス１００の決済クレデンシャルデータ若しくはヘルスケアデータ若しくは位置データ若しくは連絡先データ若しくはプライベートメディアデータへのアクセス）など）を試み得る任意の好適なサードパーティサブシステムとすることができる。プロセス５００は、デバイス１００と任意の好適な販売事業者サブシステムの任意の好適なウェブリソースとの間でよりセキュアで信頼された任意の好適なデータの通信を可能とするように機能することができる。プロセス５００は、そのようなデータ通信を可能とする前に、商業エンティティサブシステム４００と信頼関係があることを確実とするために、好適な

ウェブリソース又は他のオンラインリソースを妥当性検査するように機能することができる。

【００３７】

プロセス５００のステップ５０１では、販売事業者サブシステム２００を商業エンティティサブシステム４００に登録することができる。上述のように、販売事業者サブシステム２００の販売事業者オンラインリソース１１３（例えば、ネイティブアプリ、ドメイン／ＵＲＬ、又は任意の他の好適なウェブリソース、又はおそらく販売事業者端末でも）を特定の販売事業者識別子１６７及び特定の販売事業者鍵１５７と関連付けることができ、それらのそれぞれを、任意の好適な方法で、販売事業者サブシステム２００と商業エンティティサブシステム４００の間でセキュアに共有することができ、そのような関連付けは、（例えば、表４３０内で）商業エンティティサブシステム４００にとってアクセス可能とすることができる。いくつかの実施形態では、ネイティブアプリケーション（例えば、ネイティブアプリケーション販売事業者オンラインリソース１１３）の開発者は、権利付与のシステムを使用して、アプリケーションを実行する電子デバイス１００のセキュアデバイス機能（例えば、プッシュメッセージング、クラウドストレージ、セキュアエレメントクレデンシャル決済等）へのアクセスを可能とすることができ、その権利付与は、（例えば、アプリケーションストア４２０への配置のため、及び／又は表４３０内でアプリケーションの販売事業者鍵１５７及び販売事業者識別子１６７をセキュアに関連付けるために）アプリケーションが商業エンティティサブシステム４００により登録されるのを可能とするのに必要とされ得るコード署名プロセスの一部としてアプリケーションのバイナリに署名されてもよく、例えば、販売事業者識別子１６７はアプリケーションの権利付与の一部を形成することができる。このようなネイティブアプリケーションとは異なり、ウェブリソース（例えば、ウェブサイト販売事業者オンラインリソース１１３）は、電子デバイス１００上で実行され得るように機能するネイティブアプリケーションに（例えば、商業エンティティサブシステム４００によって）提供され得るコード署名又は同様の保護を有し得ない。代わりに、ウェブリソースのドメインの所有権を、当該ウェブリソースを登録し得る前に証明してもよい。販売事業者サブシステム２００によって所有、又は、又は他の方法で制御されたウェブサイト販売事業者オンラインリソース１１３を登録するためには、このような所有権を、商業エンティティサブシステム４００による販売事業者オンラインリソース１１３の登録前に（例えば、特定の販売事業者識別子１６７及び特定の販売事業者鍵１５７を当該販売事業者オンラインリソース１１３に関連付けて、（例えば、表４３０内の）商業エンティティサブシステム４００による将来のアクセスのために販売事業者サブシステム２００と商業エンティティサブシステム４００との間で共有する前に）、商業エンティティサブシステム４００に証明しなければならない。例えば、商業エンティティサブシステム４００に登録される販売事業者オンラインリソース１１３のドメインの所有権を証明するためには、ドメインの識別情報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、商業エンティティサブシステム４００は任意の好適なファイル（例えば、ＪＳＯＮファイルなどの静的ファイル）を販売事業者サブシステム２００に提供し、販売事業者サブシステム２００は（例えば、共有された販売事業者鍵１５７によって）当該ファイルに署名し、登録されるドメイン上の周知のパスに当該ファイルをホストすることができ、そして、商業エンティティサブシステム４００は、ドメインから当該署名されたファイルにアクセスし、（例えば、共有された販売事業者鍵１５７によって）ファイルの署名を削除し、アクセスしたファイルが販売事業者サブシステム２００と共有したファイルと一致することを確認することができる。ウェブリソースを登録するためのいくつかの例示的なプロセスは、「Ｓｈａｒｉｎｇ Ａｃｃｏｕｎｔ Ｄａｔａ Ｂｅｔｗｅｅｎ Ｄｉｆｆｅｒｅｎｔ Ｉｎｔｅｒｆａｃｅｓ Ｔｏ Ａ Ｓｅｒｖｉｃｅ」と題された米国特許出願公開第２０１５／０３５０１０６号に記載され、その全体が参照により本明細書に組み込まれる。ステップ５０２では、商業エンティティサブシステム４００に、販売事業者サブシステム２００の任意の好適なタイプの販売事業者オンラインリソース１１３（例えば、デバイス上でローカルに実行しているか、サーバ上でリモートでホスト

されているか、それとも、デバイスに近接して配置されるかにかかわらず、ネイティブアプリ、ハイブリッドアプリ、ウェブリソース、又は電子デバイスにより利用される販売事業者の販売事業者端末も）の妥当性をセキュアに登録する任意の好適なプロセス又はプロセス（複数可）を利用することができ、それによって、販売事業者オンラインリソース１１３に関連付けられた少なくとも１つの販売事業者識別子１６７及び少なくとも１つの販売事業者鍵１５７（例えば、対称又は非対称鍵ペア）を、販売事業者オンラインリソース１１３と関連付けることができ、将来の使用のために（例えば、表４３０内で）販売事業者サブシステム２００及び商業エンティティサブシステム４００の両方にとってアクセス可能にさせることができ、また任意の好適なデータを、任意の好適な方法（例えば、アプリケーション１１３、鍵１５７、識別子１６７及び／又は任意の好適な通信プロトコル（単数又は複数）を用いた通信経路８５を介した任意の他の好適なデータ）でそのようなプロセスの間、販売事業者サブシステム２００と商業エンティティサブシステム４００との間で通信することができる。１つ以上の販売事業者識別子を特定の販売事業者オンラインリソース１１３と関連付けることができ、例えば、第１の販売事業者識別子１６７を特定の販売事業者オンラインリソース１１３と一意に関連付けて、及び／又は、第２の販売事業者識別子１６７を特定の販売事業者サブシステム２００のそれぞれの販売事業者オンラインリソース１１３と関連付けることができる。追加的に、又は代替的に、１つ以上の販売事業者鍵を、特定の販売事業者識別子又は特定の販売事業者オンラインリソース１１３と関連付けてもよい。このような販売事業者鍵及び販売事業者識別子のすべての関連付けを、ステップ５０１の１つ以上のインスタンスにおいて、商業エンティティサブシステム４００（例えば、１つ以上の表４３０内に）に記憶してもよいし、又は他の方法で、商業エンティティサブシステムにとってアクセス可能としてもよい。

【００３８】

プロセス５００のステップ５０２では、登録された販売事業者オンラインリソースを用いて、販売事業者サブシステム２００と電子デバイス１００との間で潜在的トランザクションデータを通信することができる。例えば、販売事業者オンラインリソースアプリケーション１１３を実行中の、又は他の方法でそれにアクセス中のデバイス１００とユーザが相互作用している間（例えば、ユーザが販売事業者の商品又はサービスをオンラインショッピングしている間、又はユーザがヘルスケアプロフェッショナルと通信している間）のある時点では、潜在的トランザクションデータが、デバイス１００に、販売事業者サブシステム２００、又は、デバイス１００と販売事業者（又は処理）サブシステム２００の販売事業者（又はプロセッサ）との間で生じ得る、潜在的なセキュアなデータトランザクションに関する任意の好適なデータを示し得る任意の他の好適なエンティティから通信されることがある。潜在的トランザクションデータは、以下を含むがこれに限られない。（ｉ）販売事業者オンラインリソースアプリケーション１１３の少なくとも１つの又はそれぞれの販売事業者識別子１６７などの特定の販売事業者情報、（ii）デバイス１００と販売事業者サブシステム２００との間で共有される特定のタイプのセキュアなデータの識別情報などの特定のトランザクション情報（例えば、財務トランザクションの通貨及び金額ならびに決済タイプ（例えば、デバイス１００上に供給されたＶｉｓａ決済クレデンシャルを用いた５米ドル）、健康トランザクションのヘルスケアデータのタイプ及び量（例えば、デバイス１００により検出された、又は他の方法で取得された過去３日間にわたる特定のユーザの心拍数データ）など）、及び／又は（iii）一意の販売事業者ベースのトランザクション識別子（例えば、行われているトランザクションと関連付けるための販売事業者サブシステム２００によりランダムに又は一意に生成され得る複数文字英数字列などの任意の好適なデータ要素）が挙げられるが、これらに限定されない。このような潜在的トランザクションデータは、関連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、送り先住所）などの、セキュアなデータトランザクションを完了するのに必要とされ得る、又は少なくとも使用され得る任意の好適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、そのような潜在的トランザクションデータの一部として取り込まれ、挿入されてもよく、

及び／又はいくつかのフィールドは、そのような潜在的トランザクションデータの一部としては取り込まれないが、空になっており、プロセス５００の後半部分の間に取り込まれるのを待ち受けてもよい。ステップ５０２のこのような潜在的トランザクションデータは、本明細書では、（例えば、財務トランザクションのための）ＰＫＤａｔａＲｅｑｕｅｓｔ又はＰＫＰａｙｍｅｎｔＲｅｑｕｅｓｔと呼ばれる場合がある。いくつかの実施形態では、販売事業者サブシステム２００と関連付けられた潜在的トランザクションデータをステップ５０２でデバイス１００にとって利用できるようにさせるために、ユーザはデバイス１００とアクティブに相互作用しなくてもよい。代わりに、例として、デバイス１００は、すべて自動で、デバイス１００のユーザによるいかなるアクティブな相互作用もなしに、特定の製品を購入すべきことを判定し、当該特定の製品の少なくとも１つの特定の販売事業者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つ以上の販売事業者と相互作用するように構成することができる（例えば、デバイス１００は、家電製品を購入しなければならないことを判定する（例えば、洗濯機がより多くの洗濯洗剤を必要とすることを検出する、又は特定の日付により多くの洗剤を購入するように、ユーザが事前に設定したカレンダ行事を検出する）ように構成され得る家電であって、自動で、当該製品の最良の商談を提供する特定の販売事業者を識別することができ、自動で、販売事業者オンラインリソースを用いて当該販売事業者と相互作用し、当該製品を当該販売事業者から購入するために、トランザクションデータを取得し得る家電とすることができる）。ステップ５０２の潜在的トランザクションデータは、潜在的トランザクションデータと関連付けられたセキュアなデータトランザクションを完了する（例えば、財務トランザクションに資金供給する）ために、デバイス１００がセキュアにセキュアデバイスデータ（例えば、適切な決済クレデンシャルデータ）を生成し、かつ／又は、それを販売事業者サブシステム２００に提供するのに必要なすべてのデータを含むことができる。このような潜在的トランザクションデータは、ステップ５０２において、任意の好適な方法で販売事業者サブシステム２００によってデバイス１００に通信することができる（例えば、このような潜在的トランザクションデータは、任意の好適な通信プロトコルを用いた通信経路１５を介して、又は任意の好適な通信プロトコルを用いた端末２２０とＮＦＣ構成要素１２０との間の非接触近接型通信チャネルを介して、販売事業者サブシステム２００のサーバ２１０からデバイス１００の通信構成要素１０６に送信することができる）。

【００３９】

プロセス５００のステップ５０４では、販売事業者オンラインリソース妥当性検査セッションを開始することができる。このことは、電子デバイス１００がセキュアなデータトランザクション（例えば、ステップ５０２の潜在的トランザクションデータによって識別されたセキュアなデータトランザクション）が生じることを示すことに応じて（例えば、デバイス１００のユーザが、ステップ５０２の販売事業者オンラインリソースの潜在的トランザクションデータにより識別されたセキュアなデータトランザクションを行うユーザの願望を伝えるために、販売事業者オンラインリソースのＧＵＩエレメント（例えば、無線ボタン）を選択することに応じて、又は任意の好適な要件が満たされたことに自動的に基づいて（例えば、ステップ５０２の潜在的トランザクションデータがデバイス１００に通信されることに単に応じて））生じ得る。販売事業者オンラインリソースと特定のセキュアなデータトランザクションを実行するような意図が判定されると、デバイス１００上の販売事業者オンラインリソース１１３は、データトランザクション要求を生成してカード管理アプリケーション１０３ｂ又はデバイス１００上の他の好適なデバイスアプリケーションを送信するように機能することができ、当該デバイスアプリケーション１０３ｂは、ステップ５０４において販売事業者妥当性検査セッション開始データを生成し販売事業者サブシステム２００に通信するように機能することができる。ステップ５０４では、実行される特定のセキュアなデータトランザクションに対する販売事業者オンラインリソース妥当性検査セッションを開始するための販売事業者妥当性検査セッション開始データとして、任意の好適なデータが、電子デバイス１００により生成され、かつ／又は販売事業者サブシステム２００に通信され得る。例えば、ステップ５０４では、妥当性検査セッシ

ョン識別子がデバイス１００によって生成され、それを販売事業者妥当性検査セッション開始データの少なくとも一部分として販売事業者サブシステム２００に通信することができ、そのような妥当性検査セッション識別子は任意の好適な英数字列又は任意の他の好適な識別子とすることができ、それらは、開始されている現在の販売事業者オンラインリソース妥当性検査セッションを一意に識別する（例えば、少なくとも一定期間、セッションが販売事業者サブシステム２００及び／又は商業エンティティサブシステム４００に対するものであることを一意に識別する）ことができる。デバイス１００によって生成されると、妥当性検査セッション識別子は、妥当性検査セッション識別子の生成を助けるように、デバイス１００の一意の識別子（例えば、デバイス識別子１１９又はデバイス１００に対して（例えば、商業エンティティサブシステム４００に対して）一意となり得るデバイス１００のセキュアエレメント１４５の一意のセキュアエレメント識別子）を利用することで商業エンティティサブシステム４００に対して一意とされることができる。追加的に、又は代替的に、ステップ５０４では、販売事業者妥当性検査セッション開始データの少なくとも一部分として、チャレンジ要求ターゲット識別子（例えば、チャレンジ要求ＵＲＬ）を、デバイス１００から販売事業者サブシステム２００に通信することができ、このようなチャレンジ要求ターゲット識別子は、販売事業者サブシステム２００が、販売事業者を妥当性検査するために通信することとなるエンティティを識別することができる（例えば、実行される特定のセキュアなデータトランザクションの販売事業者オンラインリソースを妥当性検査するために、販売事業者サブシステム２００と協働し得る商業エンティティサブシステム４００のサーバ４１０を識別するＵＲＬ）。デバイスアプリケーション（例えば、カード管理アプリケーション１０３ｂ（例えば、ウォレットアプリケーション））は、商業エンティティサブシステム４００によって制御され得る任意の好適なオペレーティングシステム又はアプリケーション更新の一部としてプログラミングされたこのようなチャレンジ要求ターゲット識別子を有することができるので、チャレンジ要求ターゲット識別子を、デバイス１００上で、任意の好適な時間に商業エンティティサブシステム４００により更新することができる。追加的に、又は代替的に、このような販売事業者妥当性検査セッション開始データは、自身を妥当性検査するよう販売事業者への要求を示す任意の好適なデータ、デバイス１００を示す任意の好適なデータ（例えば、デバイス識別子１１９）及び／又は実行される特定のセキュアなデータトランザクションを示す任意の好適なデータ（例えば、特定の販売事業者情報（例えば、販売事業者識別子１６７）、特定のトランザクション情報（例えば、財務トランザクションの通貨及び金額ならびに決済タイプ又は健康トランザクションのヘルスケアデータのタイプ又は量）などのステップ５０２の潜在的トランザクションデータからの任意の好適なデータ）、及び／又は一意の販売事業者ベースのトランザクション識別子などの、他の任意の好適なデータを含むことができる。ステップ５０４では、任意の好適な販売事業者妥当性検査セッション開始データを、任意の好適な方法で、デバイス１００によって販売事業者サブシステム２００に通信することができる（例えば、このような販売事業者妥当性検査セッション開始データを、任意の好適な通信プロトコルを用いた通信経路１５を介して、又は任意の好適な通信プロトコルを用いたＮＦＣ構成要素１２０と端末２２０との間の非接触近接型通信チャネルを介してデバイス１００の通信構成要素１０６から販売事業者サブシステム２００のサーバ２１０に送信することができる）。

【００４０】

プロセス５００のステップ５０６では、販売事業者サブシステム２００が妥当性検査セッションを開始するためにステップ５０４でデバイス１００から任意の好適な販売事業者妥当性検査セッション開始データを受信したことに応じて、販売事業者サブシステム２００は、販売事業者オンラインリソースを妥当性検査するために商業エンティティサブシステム４００と通信するように機能することができる。いくつかの実施形態では、ステップ５０４の販売事業者妥当性検査セッション開始データが妥当性検査セッション識別子を含まない場合、販売事業者サブシステム２００は、開始されている現在の販売事業者オンラインリソース妥当性検査セッションを一意に識別し得るような妥当性検査セッション識別

子を生成するように機能することができる。販売事業者サブシステム２００により生成されると、販売事業者サブシステム２００が同一の妥当性検査セッション識別子を、少なくとも、同一の商業エンティティサブシステムに対して、かつ／又は同一の販売事業者識別子に対して、かつ／又はセッション識別子が商業エンティティサブシステムにおいて任意の特定のプロセスに保留されていないことを確実とするのに十分な一定期間内に、２回使用しないことを確実とすることによって、妥当性検査セッション識別子は商業エンティティサブシステム４００に対して一意となり得る。ステップ５０６は、商業エンティティサブシステム４００が、（例えば、ステップ５０２及び５０４で識別されるように）実行される特定のセキュアなデータトランザクションのために販売事業者オンラインリソースを妥当性検査することを可能にし得る適切な数のサブプロセスを含むことができる。図６のプロセス６００のステップ６１４～ステップ６２２に関して詳細に記載するように、ステップ５０６の妥当性検査は、販売事業者サブシステム２００が妥当性検査される販売事業者オンラインリソースと関連付けられた販売事業者識別子（例えば、販売事業者オンラインウェブリソースのドメインであり得るステップ５０１で登録された販売事業者識別子１６７）、（例えば、ステップ５０４でデバイス１００により、又はステップ５０６で販売事業者サブシステム２００により生成された）妥当性検査セッション識別子、及び任意の他の好適なデータ（例えば、デバイス１００を識別するデータ及び／又は実行される特定のセキュアなデータトランザクションを識別するデータ）を含み得るチャレンジ要求を、（例えば、ステップ５０４でデバイス１００から販売事業者妥当性検査セッション開始データにより識別され得るような）商業エンティティサブシステム４００に通信することを含むことができる。このようなチャレンジ要求は、（例えば、ＨＴＴＰヘッダ又は別の方法で）販売事業者サブシステム２００によって、チャレンジ要求の販売事業者識別子と関連付けられた販売事業者鍵（例えば、（例えば、妥当性検査される販売事業者オンラインリソース１１３のための）ステップ５０１で販売事業者識別子１６７に登録された販売事業者鍵１５７）で署名することができる。商業エンティティサブシステム４００は、このようなチャレンジ要求を受信し、（例えば、（例えば、表４３０内で販売事業者識別子１６７を識別することによって）販売事業者オンラインリソース１１３がステップ５０１で登録されていたこと、かつまだ妥当であることを確認するために）チャレンジ要求の販売事業者識別子１６７により識別された販売事業者オンラインリソース１１３を妥当性検査するように機能することができ、そして、（例えば、表４３０内の当該識別された販売事業者識別子１６７と関連付けられた販売事業者鍵１５７を用いて）チャレンジ要求の署名を妥当性検査することができる。チャレンジ要求のエレメントの妥当性検査に応じて、商業エンティティサブシステム４００は、チャレンジデータ（例えば、エントロピーを介して任意の好適なランダムデータ）を生成し、任意の好適なデータ構造で（例えば、表４３０等で）識別子データに対してチャレンジデータ（例えば、チャレンジ要求の妥当性検査セッション識別子及び販売事業者の販売事業者識別子の一方又は両方）を記憶し、商業エンティティサブシステム４００によりアクセス可能な販売事業者鍵１５７（例えば、チャレンジ要求の署名を妥当性検査するのに使用される表４３０からの販売事業者鍵）を用いてチャレンジデータを暗号化し、そして、チャレンジデータを暗号化するのに使用される販売事業者鍵のハッシュ（例えば、複数の登録された販売事業者オンラインリソース及び／又は複数の販売事業者鍵を有し得る販売事業者を支援するために提供され得る、適正な販売事業者鍵１５７（例えば、チャレンジデータを解読するための販売事業者サブシステム２００の秘密鍵１５７）を識別するために販売事業者サブシステム２００によって使用され得る表４３０の公開販売事業者鍵１５７のハッシュバージョン）、チャレンジ要求の妥当性検査セッション識別子、などの、任意の他の好適なデータとともに暗号化されたチャレンジデータを含み得るチャレンジングデータを、販売事業者サブシステム２００に通信することができる。このようなチャレンジングデータの受信に応じて、販売事業者サブシステム２００は、適切な販売事業者鍵１５７（例えば、ステップ５０１で登録されている販売事業者サブシステム２００での秘密販売事業者鍵１５７）を用いて、暗号化されたチャレンジデータを解読して、そして、チャレンジ要求の妥当性検査セッション識別子及

び適切な販売事業者識別子などの任意の他の好適なデータとともに、解読されたチャレンジデータを含むチャレンジレスポンスデータを商業エンティティサブシステム４００に通信するように機能することができ、当該チャレンジレスポンスは、チャレンジ要求の販売事業者識別子と関連付けられた販売事業者鍵（例えば、（例えば、妥当性検査される販売事業者オンラインリソース１１３のための）販売事業者識別子１６７でステップ５０１で登録された販売事業者鍵１５７）で（例えば、ＨＴＴＰヘッダ内に、又は別の方法で）販売事業者サブシステム２００によって署名され得る。そのようなチャレンジレスポンスデータの受信に応答して、商業エンティティサブシステム４００は、（表４３０内の識別された販売事業者識別子１６７と関連付けられた販売事業者鍵１５７を用いて）チャレンジレスポンスの署名を妥当性検査し、チャレンジレスポンスの解読されたチャレンジデータが、チャレンジレスポンスの妥当性検査セッション識別子に対して、及び／又は（表４３０内の）販売事業者の識別子に対して記憶されていることを確認するように機能することができる。いくつかの実施形態では、チャレンジデータと妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクを、リンクが自動で削除される前の限られた時間しか維持できないので、販売事業者サブシステム２００は、チャレンジングデータを受信し、そして、特定の妥当性検査セッションのための販売事業者オンラインリソースを妥当性検査するために、適切なチャレンジレスポンスデータを商業エンティティサブシステム４００に送信しなければならない特定の持続時間に限定されることがあり（例えば、商業エンティティサブシステム４００は、特定時間後に商業エンティティサブシステム４００で、チャレンジデータと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、リンクが作成された後１０分（又は任意の他の好適な時間）以内に表４３０からのリンクを除去する）ように機能することができる）、それにより、トランザクションのセキュリティを向上させることができる。したがって、（例えば、ステップ５０１で登録された）商業エンティティサブシステム４００における販売事業者鍵と販売事業者識別子との関連付けを用いて、（例えば、ステップ５０２及びステップ５０４で識別された）実行される特定のセキュアなデータトランザクションのステップ５０６における販売事業者オンラインリソースの妥当性検査を完了することができる。ステップ５０６では、任意の好適なデータを、適切な方法で販売事業者サブシステムと商業エンティティサブシステム４００との間で通信することができる（例えば、このようなデータを、好適な通信プロトコルを用いた通信経路８５を介して販売事業者サブシステム２００のサーバ２１０と商業エンティティサブシステム４００のサーバ４１０との間で送信することができる）。

【００４１】

ステップ５０８では、ステップ５０４で開始された妥当性検査セッションに基づいたステップ５０６での販売事業者オンラインリソースの妥当性検査に応じて、商業エンティティサブシステム４００は、妥当性検査データを生成し、妥当性検査セッションの妥当性検査セッション識別子及び／又は販売事業者識別子などの、識別子データに対してそれを記憶することができる。例えば、チャレンジレスポンスの署名の妥当性検査に応じて、かつ、チャレンジレスポンスの当該チャレンジデータ及び妥当性検査セッション識別子及び／又は販売事業者識別子も商業エンティティサブシステム４００において（例えば、表４３０内で）適正にリンクされたことを確認したことに応じて、商業エンティティサブシステム４００は、当該リンクを消費し（例えば、商業エンティティサブシステム４００においてチャレンジデータと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去し（例えば、表４３０からリンクを除去し））、妥当性検査データ（例えば、任意の好適なランダムデータ（例えば、暗号ナンス（例えば、エントロピーを介する任意の好適なランダムデータ））））を生成し、そして、ステップ５０８で、妥当性検査データを、チャレンジ要求及び／又はチャレンジレスポンスの妥当性検査セッション識別子に対して、又は他の方法によりそれに関連付けて、及び／又は販売事業者の販売事業者識別子に対して、又は他の方法によりそれに関連付けて、（例えば、表４３０又は別の方法などの任意の好適なデータ構造で）記憶することができる。

【００４２】
ステップ５１０では、ステップ５０６で販売事業者オンラインリソースを妥当性検査し、そして、ステップ５０８で妥当性検査セッション識別子及び／又は販売事業者識別子に対する任意の好適な妥当性検査データを記憶したことに応じて、商業エンティティサブシステム４００は、妥当性検査レスポンスデータを電子デバイス１００に通信することができ、このような妥当性検査レスポンスデータは、限定されることなく、ステップ５０８での妥当性検査データ、ステップ５０８での妥当性検査セッション識別子、ステップ５０６で妥当性検査された販売事業者オンラインリソースを識別するデータ（例えば、販売事業者識別子１６７）及び／又は任意の他の好適なデータを含む、任意の好適なデータを含むことができる。いくつかの実施形態において、図５に示すように、このような妥当性検査レスポンスデータを、商業エンティティサブシステム４００から直接電子デバイス１００に（例えば、任意の好適な通信プロトコルを用いた通信経路６５を介して）通信することができ、商業エンティティサブシステム４００が妥当性検査レスポンスデータを適正な電子デバイス１００に通信することができるように、電子デバイス１００を識別するデータ（例えば、デバイス識別子１１９）を（例えば、ステップ５０２等で）妥当性検査セッション識別子と関連付け、またステップ５０６の妥当性検査と関連付けることができる。代替的に、いくつかの実施形態では、このような妥当性検査レスポンスデータを、商業エンティティサブシステム４００から販売事業者サブシステム２００を介して電子デバイス１００に通信することができ、それによって、販売事業者サブシステム２００は、妥当性検査レスポンスデータを商業エンティティサブシステム４００から（例えば、任意の好適な通信プロトコルを用いた通信経路８５を介して）受信し、そして、妥当性検査レスポンスデータの少なくとも一部分を電子デバイス１００に（例えば、任意の好適な通信プロトコルを用いた通信経路１５を介して、又は非接触近接型通信として）渡すことができる。このような妥当性検査データは、（例えば、ＨＴＴＰヘッダ内で、又は別の方法で）商業エンティティサブシステム４００により、電子デバイス１００にとってアクセス可能であり得る、商業エンティティサブシステム４００に関連付けられたアクセス鍵（例えば、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／若しくはＩＳＤ鍵１５６ｋ又は、デバイスアプリケーション（例えば、カード管理アプリケーション１０３ｂ）に知られ得る任意の鍵）で署名され得るので、デバイス１００は、署名された妥当性検査データを受信するとすぐに署名を妥当性検査し、電子デバイス１００によって信頼されていない別のエンティティサブシステムではなく、商業エンティティサブシステム４００が妥当性検査データを生成したことを確認することができる。

【００４３】
プロセス５００のステップ５１２では、セキュアデバイスデータは、少なくとも部分的にデバイス１００により生成され、アクセスされ得る。そして、ステップ５１４では、このようなセキュアデバイスデータは、ステップ５１０で受信された妥当性検査レスポンスデータの少なくとも一部分及びステップ５０２の潜在的トランザクションデータの少なくとも一部分とともに、デバイストランザクションデータとしてデバイス１００により商業エンティティサブシステム４００に通信され得る。例えば、ステップ５０２の潜在的トランザクションデータに使用されている販売事業者オンラインリソースの妥当性を示し得るステップ５１０での妥当性検査レスポンスデータの受信に応じて、デバイス１００は、特定のセキュアなデータトランザクションを実行するため、ステップ５１２では、販売事業者サブシステム２００と共有されるセキュアなデータを取得するか、他の方法により識別する（例えば、財務トランザクションに使用される決済クレデンシャルデータを生成するか、健康トランザクションで共有される特定の健康データを収集する）ように機能することができる。そして、ステップ５１４では、デバイス１００は、ステップ５１０の妥当性検査レスポンスデータの妥当性検査データ及び妥当性検査セッション識別子及び販売事業者識別子とともに、及び／又は、（例えば、特定の販売事業者情報（例えば、販売事業者識別子１６７）、特定のトランザクション情報（例えば、財務トランザクションの通貨及び金額ならびに決済タイプ、又は健康トランザクションのヘルスケアデータのタイプ若し

くは量）、及び／又は一意の販売事業者ベースのトランザクション識別子など、ステップ５０２の潜在的トランザクションデータによってデバイス１００に提供され得る）実行される潜在的セキュアなデータトランザクションに関する任意の好適なデータとともに、ステップ５１２のセキュアなデータを、デバイストランザクションデータとして商業エンティティサブシステム４００に通信することができる。したがって、ステップ５１４でデバイス１００から商業エンティティサブシステム４００に通信されるデバイス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、ならびにステップ５１２のセキュアデバイスデータ、ならびにステップ５１０の妥当性検査レスポンスデータを含むことができる。

【００４４】

デバイス１００は、ステップ５１４においてデバイス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、ステップ５１４のデバイストランザクションデータ（例えば、ステップ５１２のセキュアデバイスデータ）の全部又は少なくとも一部分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、デバイス１００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、ＣＡＳＤ１５８ｋ、及び／若しくはＩＳＤ鍵１５６ｋ又は、デバイス１００にとって（例えば、デバイスアプリケーション１０３からプロセッサ１０２にとって等）アクセス可能な任意の他の鍵であって、また商業エンティティサブシステム４００にとってもアクセス可能であり得る鍵（例えば、デバイス１００と商業エンティティサブシステム４００との間の共有秘密）で、デバイストランザクションデータの少なくとも一部分を暗号化することができる。いくつかの実施形態では、こ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の方式に関連付けられた商業エンティティ公開鍵とすることができ、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し得る。商業エンティティサブシステム４００は、このような商業エンティティ公開鍵を任意の好適な方法で、デバイス１００に提供することができる。デバイストランザクションデータは、任意の好適な商業エンティティ鍵によっる少なくとも部分的な暗号化、及び／又は署名がなされているか否かにかかわらず、ステップ５４０において、任意の好適な方法で、デバイス１００により商業エンティティサブシステム４００に通信され得る（例えば、このようなデバイストランザクションデータは、任意の好適な通信プロトコルを用いた通信経路６５を介してデバイス１００の通信構成要素１０６から商業エンティティサブシステム４００のサーバ４１０に送信され得る）。

【００４５】

次に、ステップ５１４で通信されたデバイストランザクションデータを受信した後、プロセス５００のステップ５１６は、商業エンティティサブシステム４００がステップ５１４で受信した受信デバイストランザクションデータの妥当性検査データを妥当性検査することを含むことができる。例えば、このようなデバイストランザクションデータの受信に応じて、商業エンティティサブシステム４００は、当該デバイストランザクションデータから妥当性検査レスポンスデータを識別し、ステップ５１６では、当該受信した妥当性検査レスポンスデータの当該妥当性検査データが、受信したデバイストランザクションデータ（例えば、妥当性検査レスポンスデータ）の妥当性検査セッション識別子に対して、及び／又は受信したデバイストランザクションデータ（例えば、妥当性検査レスポンスデータ）の販売事業者識別子に対して（例えば、表４３０で）記憶されていることを確認するように機能することができる。いくつかの実施形態においては、妥当性検査データと、妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクは、リンクが自動的に削除される前の限られた時間しか維持できないので、電子デバイス１００は、妥当性検査された販売事業者オンラインリソースとの特定のセキュアなデータトランザクションを実行するために、当該デバイストランザクションデータのセキュアデバイスデータを商業エンティティサブシステム４００によりセキュアされるようにするため、ステップ５１０で妥当性検査レスポンスデータを受信し、そして、ステップ５１４でデバイス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

送信しなければならない、特定の持続時間を限定されてもよく（例えば、商業エンティティサブシステム４００は、特定の時間後に、商業エンティティサブシステム４００において妥当性検査データと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、リンクが作成された後１０分（又は任意の他の好適な時間）以内に表４３０からのリンクを除去する）ように機能することができる）、それにより、トランザクションのセキュリティを向上させることができる。追加的に、又は代替的に、ステップ５０８では、妥当性検査データと、妥当性検査セッション識別子及び販売事業者識別子のうち一方又は両方との間の記憶されたリンクとの関連付けも行われることができ、ステップ５０６中に（例えば、チャレンジ要求の一部分として）販売事業者サブシステム２００により商業エンティティサブシステム４００に利用可能とされ得る、特定のタイプのセキュアなデータの識別情報などの任意の好適な特定トランザクション情報は、デバイス１００と販売事業者サブシステム２００との間で共有される（例えば、財務トランザクションの通貨及び金額ならびに決済タイプ（例えば、デバイス１００上に供給されたＶｉｓａ決済クレデンシャルを用いた５米ドル）、健康トランザクションのヘルスケアデータのタイプ及び量（例えば、デバイス１００により検出されるか、他の方法により取得された過去３日間にわたる特定のユーザの心拍数データ）など）。また、同様の特定のトランザクション情報もまた、ステップ５１４のデバイストランザクションデータの一部分として、電子デバイス１００により商業エンティティサブシステム４００にとって利用可能とさせることができ、それにより、ステップ５１６は、商業エンティティサブシステム４００がステップ５１４で受信した（例えば、ステップ５０８で表４３０に記憶した）妥当性検査データに対して現在記憶されている特定のトランザクション情報が、ステップ５１４で受信した特定のトランザクション情報に少なくとも特定の程度類似していることの確認も含むことができ、それによりトランザクションのセキュリティを向上させることができる。例えば、ステップ５０８では、特定の妥当性検査データが、５米ドルの財務トランザクションを示す潜在的トランザクションと関連付けられた特定のトランザクション情報に対して記憶されるが、ステップ５１４で特定の妥当性検査データとともに商業エンティティサブシステム４００により受信した特定のトランザクション情報が２，０００米ドルの財務トランザクションを示している場合、商業エンティティサブシステム４００は、＄５と＄２，０００との間のずれの大きさが特定の閾値より大きい（例えば、５％超の相違）ことにより、デバイストランザクションデータの妥当性検査データを妥当性検査しないように機能することができる。したがって、たとえ妥当性検査データと、ステップ５１４で受信したデバイストランザクションデータの妥当性検査セッション識別子及び／又は販売事業者識別子とが、商業エンティティサブシステム４００で（例えば、表４３０で）アクティブにリンクされていることが確認されても、そのリンクと関連付けられ得る他のデータにデバイストランザクションデータが適合しない場合（例えば、妥当性検査ステップ５０６中に識別されたセキュアなデータトランザクションの任意の好適な特徴が、ステップ５１４のデバイストランザクションデータで識別されたものと適切な量（例えば、財務トランザクション通貨価値の１０％超、健康データの概算時間の１０％超、健康データのタイプが異なるなど）異なる場合）、妥当性検査データは妥当性検査されなくてもよい。

【００４６】

ステップ５００のステップ５１８では、ステップ５１６でのデバイストランザクションデータの妥当性検査データの妥当性検査に応じて、商業エンティティサブシステム４００は更に、セキュアデバイスデータが販売事業者サブシステム２００以外の任意の他のエンティティにより受信及び利用され得ないように、販売事業者サブシステム２００との共有秘密を用いてデバイストランザクションデータの少なくともセキュアデバイスデータを暗号化することによって、ステップ５１４で受信したデバイストランザクションデータのセキュアデバイスデータをセキュアとすることができる。例えば、妥当性検査データ及びデバイストランザクションデータの妥当性検査セッション識別子ならびに／又は販売事業者識別子もステップ５１６で商業エンティティサブシステム４００で（例えば、表４３０で

）適正にリンクされていたことを確認することで、デバイストランザクションデータの妥当性検査データの妥当性検査に応じて、商業エンティティサブシステム４００は当該リンクを消費する（例えば、商業エンティティサブシステム４００で妥当性検査データと妥当性検査セッション識別子及び／又は販売事業者識別子との間のそのような関連付けを除去する（例えば、表４３０からリンクを除去する））ことができ、そして、デバイストランザクションデータのセキュアデバイスデータを更にセキュアとするためにステップ５１８に進むことができる。ステップ５１４のデバイストランザクションデータがいずれかの商業エンティティ鍵で暗号化される場合、商業エンティティサブシステム４００は、ステップ５１８でそのようなデータを解読するように機能することができる（例えば、商業エンティティサブシステム４００のサーバ４１０は、デバイストランザクションデータを受信し、そして、（例えば、商業エンティティサブシステム４００のアクセス鍵１５５ａ、アクセス鍵１５５ｂ、ＣＲＳ１５１ｋ、ＣＡＳＤ１５８ｋ及び／又はＩＳＤ鍵１５６ｋで）当該デバイストランザクションデータを解読する／その署名を削除することができる）。デバイス１００と商業エンティティサブシステム４００の両方に既知の商業エンティティ鍵を用いて暗号化／署名された形式でデバイス１００と商業エンティティサブシステム４００との間でデバイストランザクションデータを通信することによって、プロセス５００は、当該デバイストランザクションデータの通信が、商業エンティティ鍵にアクセスできないエンティティにより傍受され使用されるのを禁止することができる。また、ステップ５１８では、商業エンティティサブシステム４００は、デバイストランザクションデータの少なくとも一部分を、販売事業者鍵（例えば、特定のトランザクションへの資金供給が行われている販売事業者サブシステム２００に関連付けられ得る販売事業者鍵１５７）で暗号化する、又は他の方法により再フォーマットするように機能することができる。このような販売事業者鍵は、（例えば、ステップ５１４のデバイストランザクションデータの販売事業者識別子に関連付けられた販売事業者鍵を識別することによって）、商業エンティティサブシステム４３０により表４００を介して決定されてもよく、商業エンティティサブシステム４００にとって表４３０を介してアクセス可能であり得る。販売事業者識別子は、ステップ５１８では、商業エンティティサブシステム４００により受信及び利用され、商業エンティティサブシステム４００によりアクセス可能な、多くの販売事業者鍵のうち特定の１つを（例えば、商業エンティティサブシステム４００の表４３０を活用することによって販売事業者鍵１５７を）識別することができ、そして、商業エンティティサブシステム４００は、デバイストランザクションデータの少なくとも一部分（例えば、デバイストランザクションデータの少なくともセキュアデバイスデータ）を暗号化するための当該識別された販売事業者鍵を使用することができる。このようなセキュアデバイスデータをこのような販売事業者鍵（例えば、商業エンティティサブシステム４００及び販売事業者サブシステム２００に知られ得るが、電子デバイス１００又はシステム１の他のサブシステムには知られ得ない鍵）で暗号化することで、このようなセキュアデバイスデータを、別のエンティティに傍受されず、かつ意図しない目的で使用されずに商業エンティティサブシステム４００から販売事業者サブシステム２００にセキュアに通信できるようにセキュアとすることができる。デバイストランザクションデータの少なくともセキュアデバイスデータを暗号化するために、ステップ５１８で商業エンティティサブシステム４００により利用された販売事業者鍵は、ステップ５０６での販売事業者オンラインリソースの妥当性検査中にチャレンジデータを暗号化するために商業エンティティサブシステム４００により使用された販売事業者鍵（例えば、デバイス１００又は商業エンティティサブシステム４００及び販売事業者サブシステム２００以外の任意のサブシステムによる使用に利用することができない鍵）と同一とすることができる。したがって、商業エンティティサブシステム４００は、セキュアなデータトランザクションに特有の販売事業者妥当性検査セッション中に商業エンティティサブシステム４００によって最近妥当性検査された販売事業者オンラインリソースを用いたデバイス１００と販売事業者サブシステム２００との間のセキュアなデータトランザクションを促進するように機能することができる（例えば、ステップ５０４及びステップ５０６の妥当性検査セッションとステップ５１６及

びステップ５１８のセキュアなデータトランザクションは、同一の妥当性検査セッション識別子を使用することができ、それは、アクティブであるか、他の方法により限られた時間可能とすることができ（例えば、妥当性検査セッション識別子とチャレンジデータとの間のリンク及び／又は妥当性検査セッション識別子と妥当性検査データとの間のリンクは、限られた時間（例えば、３０秒と１０分の間のような、任意の好適な時間の量）、商業エンティティサブシステム４００で妥当であり得る））、それによりトランザクションのセキュリティを向上させることができる）。

【００４７】

次に、ステップ５２０では、プロセス５００は、商業エンティティサブシステム４００がステップ５１８のセキュアなセキュアデバイスデータをセキュアなトランザクションデータとしてデバイス１００に通信することを含むことができる。例えば、デバイストランザクションデータのこのような販売事業者鍵で暗号化されたセキュアデバイスデータを、ステップ５２０で、セキュアなトランザクションデータの少なくとも一部分として、適切な通信プロトコルを用いた通信経路６５を介して商業エンティティサブシステム４００からデバイス１００に送信してもよい。このようなセキュアなトランザクションデータは、販売事業者鍵で暗号化されたセキュアデバイスデータに加え、トランザクションに関連付けられたステップ５０２の任意の好適なデータなど、任意の好適なデータを含むことができ、それは、（ｉ）ステップ５０２の潜在的トランザクションデータを提供した特定の販売事業者サブシステム２００を識別し得る販売事業者識別子の識別などの特定の販売事業者情報、（ii）財務トランザクションの支払いをするのに使用される特定の通貨又は価値の識別などの特定のトランザクション情報、（iii）（例えば、行われているトランザクションと関連付けるために販売事業者サブシステム２００により生成された）一意の販売事業者ベースのトランザクション識別子、（iv）（例えば、行われているトランザクションと関連付けるためにデバイス１００により生成された）一意のデバイスベーストランザクション識別子、（v）妥当性検査セッション識別子などを含むが、これらに限定されるものではない。したがって、ステップ５２０において商業エンティティサブシステム４００からデバイス１００に通信されたセキュアな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、ならびにセキュアなセキュアデバイスデータを含むことができる。

【００４８】

次に、プロセス５００のステップ５２２では、デバイス１００は、ステップ５２０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トランザクションデータを受信でき、好適な方法でそのセキュアなトランザクションデータを販売事業者サブシステム２００と共有することができる。例えば、このようなセキュアなトランザクションデータは、任意の好適な通信プロトコルを用いた通信経路１５を介して、及び／又はＮＦＣ構成要素１２０と販売事業者端末２２０との間の非接触近接型通信として、デバイス１００の通信構成要素１０６から販売事業者サブシステム２００のサーバ２１０に送信されてもよい。ステップ５２２でデバイス１００により販売事業者サブシステム２００に（例えば、販売事業者オンラインリソース１１３（例えば、ステップ５０２で使用される同一のリソース）を用いて）通信され得るセキュアなトランザクションデータは、ステップ５２０の販売事業者鍵で暗号化されたセキュアデバイスデータに加えて、トランザクションに関連付けられた任意の好適なデータなどの任意の好適なデータを含むことができ、それは、（ｉ）ステップ５０２の潜在的トランザクションデータを提供した特定の販売事業者サブシステム２００を識別し得る販売事業者識別子の識別などの特定の販売事業者情報、（ii）財務トランザクションの支払いをするのに使用される特定の通貨又は価値の識別などの特定のトランザクション情報、（iii）（例えば、行われているトランザクションと関連付けるために販売事業者サブシステム２００により生成された）一意の販売事業者ベースのトランザクション識別子、（iv）（例えば、行われているトランザクションと関連付けるためにデバイス１００により生成された）一意のデバイスベーストランザクション識別子、（v）妥当性検査セッション識別子などを含むが、これらに限定されるものではない。し

たがって、ステップ５２２で販売事業者サブシステム２００と共有されたセキュアな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、ならびにステップ５１８の少なくとも販売事業者鍵で暗号化されたセキュアデバイスデータを含むことができる。ステップ５２２で、セキュアなトランザクションデータの、販売事業者鍵で暗号化されたセキュアデバイスデータを通信することにより、プロセス５００は、ステップ５１２でデバイス１００により生成された、又は他の方法により識別されたセキュアデバイスデータが販売事業者鍵へのアクセスを有しない販売事業者（又はプロセッサ）エンティティ（例えば、販売事業者サブシステム２００以外の販売事業者サブシステム又はシステム１の任意の他のサブシステム）により使用されるのを防止しつつ、特定のセキュアなデータトランザクションを促進するため、このような販売事業者鍵で暗号化されたセキュアデバイスデータの販売事業者サブシステム２００への通信を可能とすることができる。代替的に、図示されていないが、このようなセキュアなトランザクションデータは、任意の好適な方法（例えば、任意の好適な通信プロトコルを用いた通信経路８５を介して）で、ステップ５２０及びステップ５２２デバイス１００を介せずに、商業エンティティサブシステム４００から販売事業者サブシステム２００に直接通信することができ、商業エンティティサブシステム４００は、ステップ５１４のデバイストランザクションデータの任意の販売事業者識別子を活用し、ターゲット販売事業者サブシステム２００を識別することができる。セキュアなトランザクションデータの、販売事業者鍵で暗号化されたセキュアデバイスデータが販売事業者サブシステム２００により受信された後、プロセス５００は、販売事業者サブシステム２００がその販売事業者鍵で暗号化されたセキュアデバイスデータを好適な目的（例えば、任意の好適なセキュアデバイスデータの処理又は取扱い）で利用することを含むことができる。

【００４９】

図５のプロセス５００で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。プロセス５００の妥当性検査ステップが失敗した場合、そのような失敗は１つ以上の適切なエンティティに通信され得ることを理解されたい。例えば、ステップ５０６で販売事業者オンラインリソースの妥当性検査が失敗した場合、及び／又はステップ５１６で妥当性検査データの妥当性検査が失敗した場合、このような失敗は、デバイス１００が販売事業者サブシステム２００との潜在的トランザクションを解除し、デバイス１００から販売事業者オンラインリソースを潜在的に除去することができるように、商業エンティティサブシステム４００により電子デバイス１００と共有されてもよい。デバイス１００のユーザがステップ５１２でセキュアなデータトランザクションに使用するために特定のセキュアなデータを選択した後、プロセス５００の残りのステップは、そのユーザにとって透過的に発生することがある（例えば、ステップ５１４～５２２は、デバイス１００に対するユーザによる更なる相互作用なしに発生することがあり、デバイス１００のユーザにとって瞬時に行われるもののように見えることがある）。プロセス５００は、あたかも、ステップ５１２の後、セキュアデバイスデータが自動でかつ瞬時に販売事業者サブシステム２００に送信されるように、デバイス１００のユーザに見えることがあり、トランザクションの状況は（例えば、販売事業者サブシステム２００及び／又は商業エンティティサブシステム４００により）デバイス１００に確認されることができる。追加的に、又は代替的に、販売事業者オンラインリソースの妥当性検査は、デバイス１００に対して透過的に発生することができる（例えば、ステップ５０６～５１０は、また、場合によりステップ５０４も、デバイス１００に対するユーザによる相互作用なしに発生することができ、ステップ５０２の後デバイス１００のユーザに対して瞬時に行われているように見えることがある）。代替的に、いくつかの実施形態では、プロセス５００は、デバイス１００のユーザにとって全く透過的に発生することができる（例えば、デバイス１００は、セキュアなデバイストランザクションがいつ発生すべきかを判定し、妥当性検査レスポンスデータを自動で受信し、かつ／又はデバイストランザクションデータを自動で送信するように、かつ／又は、デバイス１００に対するユーザによるア

クティブな相互作用なしにセキュアなデバイストランザクションのセキュアなトランザクションデータを自動で受信及び／又は送信するように構成されてもよい。

【００５０】

図６の説明

図６は、財務トランザクションを行うためのセキュアデバイス機能へのオンラインアクセスを妥当性検査に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、電子デバイス１００、販売事業者サブシステム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によって実施されているように示されている。しかし、プロセス６００は、他の任意の好適な構成要素又はサブシステムを用いて実施され得ることを理解されたい。プロセス６００は、デバイス１００からの決済クレデンシャルを用いて販売事業者サブシステム２００との間で財務トランザクションを安全かつ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。図６のプロセス６００に従って財務トランザクションを行うためのシステム１の動作に関する以下の議論を容易にするため、図１～図４の解釈図のシステム１の種々の構成要素、及び、そのようなトランザクション中のデバイス１００のグラフィカルユーザインタフェース（例えば、販売事業者オンラインリソース１１３又はデバイス１００の任意の好適なアプリケーションによって提供され得るようなＧＵＩ）を表し得る図３～図３Ｄの画面１９０～１９０ｄの正面図が参照される。説明する動作は、幅広い種類のグラフィカル要素及び視覚的方式により実現されてもよい。したがって、図３～図３Ｄの実施形態は、本明細書で採用するユーザインタフェース規則に厳密に限定されることを意図していない。むしろ、実施形態は、幅広い種類のユーザインタフェーススタイルを含んでもよい。プロセス６００は、販売事業者サブシステム２００による電子デバイス１００のセキュアな決済機能へのアクセスを可能とするため販売事業者サブシステム２００を妥当性検査するコンテキストにおいて少なくとも部分的に記載されているが、プロセス６００のすべてではないにしても多くが、任意の好適なサードパーティサブシステムによるデバイス１００の任意のセキュア機能（例えば、位置データ、健康データ、他の任意のプライベートデータ、又は、他の有効に妥当性検査されていないサードパーティサブシステムと共有若しくはそのサードパーティサブシステムから受信されるべきではない機能）へのアクセスを可能とするために当該サードパーティサブシステムを妥当性検査するために利用され得ることを理解されたい。

【００５１】

プロセス６００は、ステップ６０２で開始することができ、アクセスデータ６５２（例えば、図１Ａのアクセスデータ６５２）は、商業エンティティサブシステム４００によってデバイス１００上に供給され得る。例えば、デバイス１００が販売事業者サブシステム２００とのトランザクションをよりセキュアに行うことを可能とするために、アクセスＳＳＤ（例えば、ＳＳＤ１５４ｂ）を、アクセスデータ６５２として、デバイス１００のセキュアエレメント１４５に商業エンティティサブシステム４００のサーバ４１０から供給することができる。上述のように、アクセスＳＳＤ１５４ｂを、商業エンティティサブシステム４００から直接デバイス１００のセキュアエレメント１４５上に少なくとも部分的に供給することができる（例えば、商業エンティティサブシステム４００のサーバ４１０とデバイス１００の通信構成要素１０６との間の通信経路６５を介してアクセスデータ６５２として供給でき、それは、そして、（例えば、バス１１８を介して）通信構成要素１０６からセキュアエレメント１４５に渡すことができる）。経路６５を介したアクセスデータ６５２は、アクセスＳＳＤ１５４ｂ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１４５上に供給することができ、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、デバイス１００が（例えば、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）最初に構成されているとき、少なくとも部分的に実行されてもよい。追加的に、又は代替的に、ステップ６０２は、デバイス１００のユーザがＮＦＣ構成要素１２０のセキュアエレメント１４５を最初にセットアップするのに応じて、少なくとも部分的に実

行されてもよい。追加的に、又は代替的に、アクセスデータ６５２は、セキュアエレメント１４５のＩＳＤ　１５２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とデバイス１００との間のセキュアな送信を可能とするために、アクセス鍵１５５ｂに加えて、又はその代替的に使用することができる。追加的に、又は代替的に、アクセスデータ６５２は、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、それは、商業エンティティサブシステム４００とデバイス１００との間のセキュアな送信を可能とするために（例えば、任意の好適な商業エンティティ鍵として、又は商業エンティティサブシステム４００とデバイス１００との間の共有秘密として使用されるための）アクセス鍵１５５ｂ及び／又はアクセス鍵１５５ａ及び／又はＩＳＤ１５６ｋに加えて、又はその代替的に使用されてもよい。追加的に、又は代替的に、アクセスデータ６５２は、デバイス１００のセキュアエレメントには記憶されなくてよく、プロセッサ１０２など、デバイス１００の他の部分にとって、メモリ１０４を介してアクセス可能であり得る、任意の他の好適な商業エンティティ鍵又は商業エンティティサブシステム４００とデバイス１００との間の共有秘密を含むことができる。

【００５２】

プロセス６００のステップ６０４では、金融（又は発行者又はトランザクション）機関サブシステム３５０は、商業エンティティサブシステム４００を介して、いくつかの実施形態におけるデバイス１００上にクレデンシャルデータ６５４（例えば、図１Ａのクレデンシャルデータ６５４）を供給することができる。例えば、このようなクレデンシャルデータ６５４を、少なくとも部分的に、金融機関サブシステム３５０から直接デバイス１００のセキュアエレメント１４５上に供給することができる（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１Ａの通信経路７５を介して供給することができ、それを通信構成要素１０６を介してセキュアエレメント１４５に渡すことができる）。追加的に、又は代替的に、このようなクレデンシャルデータ６５４を、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供給することができる（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との間の図１Ａの通信経路５５を介して供給でき、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の通信構成要素１０６との間の図１Ａ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に渡すことができ、そして、（例えば、バス１１８を介して）通信構成要素１０６からセキュアエレメント１４５に渡すことができる）。経路７５及び／又は経路６５を介したクレデンシャルデータ６５４は、クレデンシャルＳＳＤ１５４ａの少なくとも一部分又は全部としてデバイス１００のセキュアエレメント１４５上に供給でき、クレデンシャル情報１６１ａを有するクレデンシャルアプレット１５３ａ及び／又はクレデンシャル鍵１５５ａ’及び／又は鍵１５５ａｋを含むことができる。ステップ６０４は、デバイス１００のユーザがデバイス１００に供給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、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から金融機関サブシステム３５０へ最初に提供され得る、及び／又は、商業エンティティサブシステム４００によって追加され得る、アクセス鍵１５５ａも含むことができる。いくつかの実施形態では、このようなクレデンシャルデータ６５４は、供給されている決済クレデンシャルのクレデンシャル情報の少なくとも一部分として主アカウント番号（例えば、アプレット１５３ａのクレデンシャル情報１６１ａ）、ＡＩＤ（例えば、ＳＳＤ１５４ａで供給されている決済クレデンシャルのデータのアプレット１５３ａ用のＡＩＤ１５５ａａ）、ＳＳＤ識別子、及び／又はＳＳＤカウンタを含むことができる。

【００５３】

デバイス１００に供給されるクレデンシャルデータは、金融又は決済クレデンシャルである場合、そのクレデンシャルで決済を行うのに必要なすべてのデータ、例えば、主アカウント番号（「ＰＡＮ」）、カードセキュリティコード（例えば、カード妥当性検査コー

ド（「ＣＶＶ」））、ＰＡＮ有効期限、クレデンシャルと関連付けられた名称、ならびに、デバイス１００が適切な暗号データ（例えば、任意の好適な共有秘密及び関数出力が少なくとも部分的に共有秘密によって決定され得る任意の好適な暗号アルゴリズム又は暗号）を生成するように動作し得る、その他のデータを含むことができる。「仮想」クレデンシャル又は仮想ＰＡＮ又はデバイスＰＡＮ（「Ｄ－ＰＡＮ」）を、ユーザの「実際の」クレデンシャル又は実際ＰＡＮ又は資金供給ＰＡＮ（「Ｆ－ＰＡＮ」）ではなく、デバイス１００上に供給することができる。例えば、クレデンシャルがデバイス１００に提供されることが決定されると、実際のクレデンシャルの代わりに仮想クレデンシャルが生成され、実際のクレデンシャルにリンクされ、デバイス１００に供給されることが（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と実際のクレデンシャルとのこのような作成及びリンク付けは、金融機関サブシステム３５０の任意の好適な構成要素によって実行され得る。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と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、（例えば、図１Ａに示すように）実際のクレデンシャルと仮想クレデンシャルとの間の関連付けを作成し得る仮想リンク付けテーブル３１２を規定して記憶することができるので、仮想クレデンシャルが（例えば、デバイス１００に供給された後の）販売事業者サブシステム２００との財務トランザクションのためにデバイス１００により利用されるときはいつでも、決済ネットワークサブシステム３６０は、許可又は妥当性検査要求を受信し、又は他の方法により、（例えば、ステップ６３８でのデータ６８８の受信に応じてステップ６４０で）その仮想クレデンシャルを示す任意の受信したデータを妥当性検査するように試みることができ、表３１２によって決定される仮想クレデンシャルと関連付けられた実際のクレデンシャルに照らして、この妥当性検査試行要求の分析を行うことができる。代替的に、このような表は、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任意の他の好適なサブシステムによってアクセス可能及び／又は同様に活用されてもよい。デバイス１００に実際のクレデンシャルではなく、仮想のクレデンシャルを供給することにより、金融機関サブシステム３５０を仮想のクレデンシャルが無許可のユーザにより傍受された場合に生じ得る不正活動を制限するように構成することができる。これは、決済ネットワークサブシステム３６０は、特定のトランザクション中に、表３１２を利用して仮想クレデンシャルを実際のクレデンシャルにリンク付ける構成のみ可能とされることによる。

【００５４】

プロセス６００のステップ６０６では、商業エンティティサブシステム４００は、販売事業者サブシステム２００を登録することができる。例えば、プロセス５００のステップ５０１に関して説明するように、ステップ６０６では、販売事業者サブシステム２００の販売事業者オンラインリソース１１３（例えば、ネイティブアプリ、ドメイン／ＵＲＬ、又は任意の他の好適なウェブリソース、又はおそらく販売事業者端末でも）を、少なくとも１つの特定の販売事業者識別子１６７及び少なくとも１つの特定の販売事業者鍵１５７と関連付けることができ、それらのそれぞれを、任意の好適な方法で、販売事業者サブシステム２００と商業エンティティサブシステム４００の間でセキュアに共有することができ、また、そのような関連付けは、販売事業者オンラインリソース１１３を商業エンティティサブシステム４００に登録できるように（例えば、表４３０内で）商業エンティティサブシステム４００にとってアクセス可能とすることができる。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、販売事業者は、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すること、及び／又は販売事業者証明書を取得することが必要とされ得る。販売事業者は、証明書又は他の好適な登録証拠なしに決済データを受け取ることができない。このような販売事業者鍵（単数又は複数）及び／又は販売事業者識別子（単数又は複数）がどのように又はどこで生成され、かつ／又は管理されても、販売事業者サブシステム２００及び／又は商業エンティティサブシステム４００はともに、販売事業者鍵ペアの販売事

業者鍵のバージョンを（例えば、販売事業者サブシステム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の中で）記憶することができる。これにより、商業エンティティサブシステム４００と販売事業者サブシステム２００との間でデータをセキュアに通信するための共有秘密を可能とすることができる。いくつかの実施形態において、デバイス１００は、デバイス１００上の鍵で決済データをセキュアに暗号化するための販売事業者鍵を備えることができる。

【００５５】

プロセス６００のステップ６０８では、デバイス１００は、販売事業者のオンラインリソース６５８（例えば、（例えば、ステップ６０６で登録される）図１Ａの販売事業者オンラインリソース１１３）にアクセスすることができる。図１Ａに示すように、販売事業者のリソースアプリケーション１１３を、商業エンティティサブシステム４００（例えば、アプリケーションストア４２０）からデバイス１００にロードすることができる。例えば、図３に示すように、デバイス１００のユーザは、Ｉ／Ｏ構成要素１１４ａのタッチスクリーン入力構成要素１１０ｆを用いてＧＵＩ１８０の特定の画面１９０の「Ｍｅｒｃｈａｎｔ　Ａｐｐ」アイコン１８３を選択することができ、この選択を、デバイス１００により、販売事業者のサードパーティアプリケーション１１３（例えば、（例えば、アプリケーションストア４２０の登録された販売事業者オンラインリソースアプリケーションとして）商業エンティティサブシステム４００を介してデバイス１００によりアクセスされ得るデバイス１００上で少なくとも部分的に実行中のネイティブアプリケーション）と相互作用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することができる。追加的に、又は代替的に、このような販売事業者のリソース６５８は、（例えば、サーバ２１０又は端末２２０を介して）販売事業者サブシステム２００から直接デバイス１００によってアクセスされ得る。このような販売事業者アプリケーションアイコンの選択に応じて、ＧＵＩは、デバイス１００により、ユーザがアプリケーション１１３と相互作用する（例えば、購入のために販売事業者から商業的に入手可能なアイテムを閲覧するか、販売事業者又は他の人と共有する特定の健康データ又は位置データを判定する）ことを可能にし得る相互作用型スクリーンを提供することができる。代替的に、ステップ６０８は、デバイス１００が、「Ｉｎｔｅｒｎｅｔ」アイコン（例えば、図３のＧＵＩ１８０の特定の画面１９０のアイコン１８４）により選択可能とすることができる、デバイス１００のインターネットアプリケーション、又は販売事業者のサードパーティネイティブアプリケーションではなく、販売事業者のウェブページ又は他のウェブリソースと相互作用する能力をユーザに提供するウェブ表示を有するハイブリッドアプリケーションを用いて、（例えば、販売事業者サーバ２１０又は販売事業者エンティティにより少なくとも部分的に制御される任意のサーバを介して）販売事業者サブシステム２００から販売事業者のウェブリソースとして販売事業者のリソース６５８にアクセスすることを含むことができる。代替的に、ステップ６０８は、アクティブなユーザ入力なしに販売事業者オンラインリソース１１３としてのリソース６５８の任意の好適な自動アクセスを含むことができる（例えば、特定の供給を切らしていることを検出する自律型家電製品デバイス１００（例えば、洗剤の供給が少ないことを検出したことに応じる洗濯機デバイス１００）のように、デバイス１００は、任意の好適なイベントの検出に応じてリソース６５８と自動で相互作用するように機能することができる）。

【００５６】

次に、ステップ６１０では、デバイス１００は、（例えば、プロセス５００のステップ５０２に関して説明するように）アクセスされた販売事業者リソースから潜在的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１Ａに示すように、デバイス１００が販売事業者のリソース１１３（例えば、販売事業者のサードパーティアプリケーション若しくはウェブサイト又は任意の他の好適なオンラインリソース（例えば、リソース６５８））と相互作用しているときに、潜在的トランザクションデータ６６０を、販売事業者サブシステム２００（例えば、販売事業者サーバ２１０）からデバイス１００に提供してもよい。追加的に、又は代替的に、潜在的トランザクションデータ６６０の少なく

とも一部分は、ステップ６１０でデータが販売事業者サーバ２１０からデバイス１００にアクティブに送信されるのではなく、（例えば、アプリケーション１１３がメモリ構成要素に記憶されている、又はデバイス１００のプロセッサ１０２によって実行されている場合）デバイス１００に対してローカルなアプリケーション１１３を介してデバイス１００によってローカルにアクセス可能とすることができる。例えば、アプリケーション１１３をデバイス１００に最初に記憶することができると（例えば、販売事業者のリソース６５８としてステップ６０８で（例えば、アプリケーションストア４２０からロードすることができると））、追加情報が販売事業者サブシステム２００によりデバイス１００に提供されることなく、潜在的トランザクションデータ６６０の少なくとも一部は、当該最初に記憶されたアプリケーション１１３により生成されることができる。潜在的トランザクションデータ６６０は、デバイス１００のユーザと販売事業者サブシステム２００の販売事業者との間で生じる潜在的財務トランザクションの任意の好適な特性を示す任意の好適なデータを含むことができ、それは、（ｉ）一意の販売事業者識別子（例えば、取得銀行販売事業者識別子及び／又は商業エンティティ販売事業者識別子（例えば、ステップ６１０で登録され得る販売事業者識別子１６７））及び／又は使用されている特定の販売事業者リソース（例えば、特定の販売事業者アプリケーション１１３）の識別情報）など、特定の販売事業者情報、（ii）トランザクションの支払いをするの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、トランザクションに支払われる通貨の特定の量の識別、及び／又は、購入もしくレンタルされる、他の方法により支払いをされる特定の製品又はサービスの識別、及び／又は、使用される既定若しくは初期の配送先住所の識別など、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の販売事業者にアクセス可能な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、Ｖｉｓａではなく、ＭａｓｔｅｒＣａｒｄ））、及び／又は（iv）一意の販売事業者ベースのトランザクション識別子（例えば、行われているトランザクションと関連付けるために販売事業者サブシステム２００によりランダムにかつ一意に生成され得る、３文字又は４文字英数字列など、任意の好適なデータ要素）を含むが、これらに限定されない。このような潜在的トランザクションデータ６６０は、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、送り先住所）など、関連付けられたデータにかかわらず、財務トランザクションを完了するのに必要とされ、又は少なくとも使用され得る任意の好適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、このような潜在的トランザクションデータ６６０として取り込まれ挿入されることがあり、及び／又はいくつかのフィールドは、このような潜在的トランザクションデータ６６０の一部としては取り込まれないが、空とされ、プロセス６００の間に取り込みを待ち受けてもよい。ステップ６１０のこのような潜在的トランザクションデータ６６０は、本明細書では、（例えば、財務トランザクションのための）ＰＫＤａｔａＲｅｑｕｅｓｔ又はＰＫＰａｙｍｅｎｔＲｅｑｕｅｓｔと呼ばれる場合がある。代替的に、上述のように、販売事業者サブシステム２００と関連付けられた潜在的トランザクションデータ６６０をステップ６１０でデバイス１００にとって利用できるようにさせるために、ユーザはデバイス１００とアクティブに相互作用しなくてもよい。

【００５７】

セキュアな決済データの通信のために、潜在的トランザクションデータ６６０は、商品及び／又はサービスの購入のための決済トークンを生成するためのデバイス１００に対する販売事業者リソースの要求を含むことができ、例えば、販売事業者の決済処理能力、支払い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好適な情報をカプセル化することができる。潜在的トランザクションデータ６６０はまた、販売事業者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（単数又は複数）３６０）のリストも含むことができることで、デバイス１００は、このようなリスト化された１つ以上の決済ネットワークのいずれかがデバイス１００又はクライアントとしてデバイス１００にとって利用可能な任意の好適なホストデバイスに対す

る許可された決済クレデンシャルを有するかを判定するように構成することができる。いくつかの実施形態では、例えば図３Ａに示すように、このような潜在的トランザクションデータ６６０がデバイス１００によりアクセスされると、デバイス１００のＧＵＩは、画面１９０ａを提供することができ、販売事業者のリソースはトランザクションデータ６６０を使用してデバイス１００のユーザに、潜在的トランザクションと関連付けられた任意の好適な情報、例えば、情報３０７ａで販売事業者の名称（例えば、「販売事業者Ａ」）、情報３０７ｂで製品の名称（例えば、「商品Ｂ」）、情報３０７ｃで価格（例えば、「価格Ｃ」）、及び／又は情報３０７ｄで初期の配送先データ（例えば、「住所Ｄ」）を示すことができる。販売事業者サブシステム２００によりデバイス１００に提供され得る潜在的トランザクションデータ６６０は、このような情報３０７ａ、３０７ｂ、３０７ｃ及び／又は３０７ｄを示すことができる。デバイス１００のユーザは、デバイス１００及び画面１９０ａと相互作用して、そのような情報（例えば、配送先住所など）の特定の部分を調整することができ、それは、（例えば、ステップ６１０の別のインスタンスで）更新された潜在的トランザクションデータが販売事業者サブシステム２００により生成又は共有されることを必要とし得る。図３Ａに示すように、かつ以下により詳細に説明するように、画面１９０ａには、セキュアな支払いプロンプト３０９も含まれていてもよい。潜在的トランザクションデータ６６０の少なくとも一部分を、図１Ａの通信経路１５を介して販売事業者サブシステム２００からデバイス１００に提供することができ、デバイス１００の通信構成要素１０６により受信することができる。通信構成要素１０６は、この潜在的トランザクションデータ６６０を、（例えば、（例えば、情報３０７ａ～３０７ｄ及び３０９のために）デバイス１００上のユーザインタフェースの一部としての画面１９０ａ上に表示するための）プロセッサ１０２及び／又はセキュアエレメント１４５に渡すことができる。例えば、セキュアエレメント１４５は、デバイス１００と販売事業者サブシステム２００との間の財務トランザクションをセキュアに可能とするために、そのような潜在的トランザクションデータ６６０の少なくとも一部分を利用することができる。いくつかの実施形態では、潜在的トランザクションデータ６６０は、販売事業者決済要求データ及び／又はユニフォームリソースロケータ（「ＵＲＬ」）又は任意の他の好適な参照文字列及び／又はクエリ文字列と呼ばれる場合がある。

【００５８】

プロセス６００のステップ６１２では、販売事業者オンラインリソース妥当性検査セッションを開始することができる。プロセス５００のステップ５０４に関して上述したように、ステップ６１２は、電子デバイス１００がセキュアなデータトランザクション（例えば、ステップ６１０の潜在的トランザクションデータ６６０により識別されたセキュアなデータトランザクション（例えば、財務トランザクション））が発生すべきことを示したことに応じて生じることがある。このような指示は、ステップ６１０の販売事業者オンラインリソースの潜在的トランザクションデータ６６０によって識別されるセキュアなデータトランザクションを行うユーザの意図を伝えるために、デバイス１００のユーザが図３Ａのセキュアな支払いプロンプト３０９などの販売事業者オンラインリソースのＧＵＩ要素（例えば無線ボタン）を選択することに応じて生じ得る。代替的に、このような指示は、好適な要件が満たされていることに基づいて（例えば、ステップ６１０の潜在的トランザクションデータ６６０がデバイス１００に通信されていることに単純に応じて）自動的に生じてもよい。例えば、この指示が発生したとき、販売事業者オンラインリソース１１３（例えば、ウェブリソース用のウェブキット）は、カード管理アプリケーション１０３ｂ（例えば、決済用のセキュアなデータトランザクションのパスキット）にセキュアなデータトランザクション要求を送信するように動作するようにしてもよいし、デバイス１００（例えば、カード管理アプリケーション１０３ｂ又はデバイス１００の他の好適なアプリケーション）は、このようなセキュアなデータトランザクション要求を受信かつ処理するように動作し、そして、ステップ６１２で販売事業者オンラインリソース妥当性検査セッション開始データ６６２を生成し、販売事業者サブシステム２００に通信するように動作するようにしてもよい。

【００５９】
ステップ６１２では、実行される特定のセキュアなデータトランザクション（例えば、図３Ａのデータ６６０及び／又は画面１９０ａにより識別された財務トランザクション）に対する販売事業者オンラインリソース妥当性検査セッションを開始するための販売事業者オンラインリソース妥当性検査セッション開始データ６６２として、任意の好適なデータを、電子デバイス１００により生成し、かつ／又は販売事業者サブシステム２００に通信することができる。例えば、妥当性検査セッション識別子はデバイス１００により生成され、ステップ６１２で販売事業者オンラインリソース妥当性検査セッション開始データ６６２の一部分として販売事業者サブシステム２００に通信されてもよく、このような妥当性検査セッション識別子は、任意の好適な英数字列又は、開始されている現在の販売事業者オンラインリソース妥当性検査セッションを一意に識別し得る（例えば、少なくとも特定の期間に、販売事業者サブシステム２００及び／又は商業エンティティサブシステム４００に対してそのようなセッションを一意に識別する）任意の他の好適な識別子とすることができる。追加的に、又は代替的に、ステップ６１２では、販売事業者オンラインリソース妥当性検査セッション開始データ６６２の少なくとも一部分として、チャレンジ要求ターゲット識別子（例えば、チャレンジ要求ＵＲＬ）を、デバイス１００から販売事業者サブシステム２００に通信することができ、このようなチャレンジ要求ターゲット識別子は、販売事業者サブシステム２００が、販売事業者を妥当性検査するために通信することとなるエンティティを識別することができる（例えば、実行される特定のセキュアなデータトランザクションの販売事業者オンラインリソースを妥当性検査するために、販売事業者サブシステム２００と協働することとなる商業エンティティサブシステム４００のサーバ４１０を識別するＵＲＬ）。デバイスアプリケーション（例えば、カード管理アプリケーション１０３ｂ）は、商業エンティティサブシステム４００により制御され得る任意の好適なオペレーティングシステム又はアプリケーション更新の一部としてプログラミングされたこのようなチャレンジ要求ターゲット識別子を有することができるので、チャレンジ要求ターゲット識別子は、デバイス１００上で、任意の好適な時間に商業エンティティサブシステム４００により更新することができる。追加的に、又は代替的に、このような販売事業者オンラインリソース妥当性検査セッション開始データ６６２は、自身を妥当性検査する販売事業者及び／又はステップ６０８でアクセスされ、ステップ６１０で潜在的トランザクションデータ６６０を受信するために利用された特定の販売事業者オンラインリソースへの要求を示す任意の好適なデータ、デバイス１００を示す任意の好適なデータ（例えば、デバイス識別子１１９）、及び／又は実行される特定のセキュアなデータトランザクションを示す任意の好適なデータ（例えば、特定の販売事業者情報（例えば、販売事業者オンラインリソースの販売事業者識別子１６７）、特定のトランザクション情報（例えば、財務トランザクションの通貨及び金額ならびに決済タイプ）などのステップ６１０の潜在的トランザクションデータ６６０からの任意の好適なデータ）、及び／又は一意の販売事業者ベースのトランザクション識別子などの、他の任意の好適なデータを含むことができる。任意の好適な販売事業者オンラインリソース妥当性検査セッション開始データ６６２を、ステップ６１２で、任意の好適な方法で、デバイス１００によって販売事業者サブシステム２００に通信することができる（例えば、このような販売事業者オンラインリソース妥当性検査セッション開始データ６６２を、任意の好適な通信プロトコルを用いた通信経路１５を介して、又は任意の好適な通信プロトコルを用いた、端末２２０とＮＦＣ構成要素１２０との間の非接触近接型通信チャネルを介してデバイス１００の通信構成要素１０６から販売事業者サブシステム２００のサーバ２１０に送信することができる）。

【００６０】
ステップ６００でプロセス６１４では、販売事業者サブシステム２００が、販売事業者オンラインリソース１１３の妥当性検査セッションを開始するため、ステップ６１２でデバイス１００からいずれかの好適な販売事業者オンラインリソース妥当性検査セッション開始データ６６２を受信したことに応じて、販売事業者サブシステム２００は、実行され

る特定のセキュアなデータトランザクション（例えば、ステップ６１０及び／又はステップ６１２で識別された金融決済トランザクション）のための販売事業者オンラインリソースを妥当性検査するために、任意の好適なチャレンジ要求データ６６４を商業エンティティサブシステム４００に通信するように機能することができる。ステップ６１４で販売事業者サブシステム２００から商業エンティティサブシステム４００に通信されるチャレンジ要求データ６６４は、販売事業者サブシステム２００（例えば、販売事業者リソース１１３）の妥当性を商業エンティティサブシステム４００に証明しようとするための任意の好適なデータを含むことができ、それは、妥当性検査される販売事業者オンラインリソースと関連付けられた販売事業者識別子（例えば、販売事業者オンラインウェブリソースのドメインであり得るステップ６０６で登録された少なくとも１つの販売事業者識別子１６７）、（例えば、ステップ５０４でデバイス１００により、又はステップ５０６で販売事業者サブシステム２００により生成された）妥当性検査セッション識別子及び／又は任意の他の好適なデータ（例えば、デバイス１００を識別するデータ及び／又は実行される特定のセキュアなデータトランザクションを識別するデータ）を含むことができるが、これらに限定されない。例えば、チャレンジ要求データ６６４の販売事業者識別子は、現在の販売事業者オンラインリソース妥当性検査セッションを開始したステップ６１０で使用される販売事業者オンラインリソースに関連付けられた任意の好適な販売事業者識別子１６７とすることができる。ステップ６１２の販売事業者オンラインリソース妥当性検査セッション開始データ６６２が、（例えばデバイス１００によって生成される）妥当性検査セッション識別子を含む場合、当該妥当性検査セッション識別子を、ステップ６１４でチャレンジ要求データ６６４の少なくとも一部分として販売事業者サブシステムにより提供することができる。しかし、ステップ６１２の販売事業者オンラインリソース妥当性検査セッション開始データ６６２が妥当性検査セッション識別子を含んでいない場合、又は販売事業者オンラインリソース妥当性検査セッションを、販売事業者サブシステム２００により自動で（例えば、ステップ６１０の潜在的トランザクションデータ６６０の通信に応じて）、かつステップ６１２の販売事業者オンラインリソース妥当性検査セッション開始データ６６２に応じずに開始することができる場合、販売事業者サブシステム２００は、開始されている現在の販売事業者オンラインリソース妥当性検査セッションを一意に識別し得るそのような妥当性検査セッション識別子を生成するように機能することができ、そして、ステップ６１４でチャレンジ要求データ６６４の少なくとも一部分としてその妥当性検査セッション識別子を含むように動作することができる。いくつかの実施形態では、実行される特定のセキュアなデータトランザクション（例えば、ステップ６１０及び／又はステップ６１２で識別される金融決済トランザクション）に特有であり得る任意の好適な追加情報が、ステップ６１４でチャレンジ要求データ６６４の少なくとも一部分として提供され得、それは、潜在的トランザクションデータの情報３０７ｂの「製品Ｂ」、潜在的トランザクションデータの情報３０７ｃの「価格Ｃ」、潜在的トランザクションデータの情報３０７ｄの配送先データ「宛先Ｄ」、潜在的トランザクションデータの決済クレデンシャル識別「クレデンシャルＸ」情報３１３を示す情報及び／又は、（例えば、データのいずれかについての任意のプライバシーに対する懸念に照らして）実行されるセキュアなデータトランザクションが健康データトランザクションである場合、実際の心拍数情報ではなく、「過去３日間の心拍数情報」のような、商業エンティティサブシステム４００と共有するのに適切であり得る実行されるセキュアなデータトランザクションに関連付けられた任意の他の好適な情報を含むが、これらに限定されない。本明細書では潜在的トランザクション識別情報と呼ばれ得るセキュアなデータトランザクションに特定のもので特有であり得るこのような情報は、セキュリティの追加層（単数又は複数）を現在のデータトランザクションプロセスに提供し、及び／又は将来のデータトランザクションに対する追加のセキュリティ（例えば、不正検出）サービスを提供するためのプロセス６００の好適な部分の間に使用され得る。チャレンジ要求データ６６４は、販売事業者サブシステム２００により（例えば、ＨＴＴＰヘッダにおいて、又は別の方法で）販売事業者サブシステム２００にとって利用可能で、かつチャレンジ要求の販売事業者識別子に関連付けられた

販売事業者鍵（例えば、（例えば、販売事業者オンラインリソース１１３を妥当性検査するために）ステップ６０６において販売事業者識別子１６７で登録された販売事業者鍵１５７）で署名することができ、それにより、チャレンジ要求データ６６４を、販売事業者オンラインリソース１１３を妥当性検査するために商業エンティティサブシステム４００により効率的に利用することができる。ステップ６１４では、任意の好適なチャレンジ要求データ６６４を、適切な方法で販売事業者サブシステム２００により商業エンティティサブシステム４００に通信することができる（例えば、このようなチャレンジ要求データ６６４を、好適な通信プロトコルを用いた通信経路８５を介して販売事業者サブシステム２００のサーバ２１０から商業エンティティサブシステム４００のサーバ４１０に送信することができる）。このようなチャレンジ要求データ６６４の通信は、販売事業者オンラインリソース妥当性検査セッション開始データ６６２の少なくとも一部分として、ステップ６１２でデバイス１００から販売事業者サブシステム２００に通信され得るチャレンジ要求ターゲット識別子（例えば、チャレンジ要求ＵＲＬ）に基づいて商業エンティティサブシステム４００に適切にアドレス指定され得る。追加的に、又は代替的に、このようなチャレンジ要求データ６６４の通信は、販売事業者サブシステム２００にとって利用可能とすることができ、かつステップ６１０の潜在的トランザクションデータ６６０と関連付けられ得るチャレンジ要求ターゲット識別子（例えば、チャレンジ要求ＵＲＬ）に基づいて商業エンティティサブシステム４００に適切にアドレス指定され得る（例えば、商業エンティティサブシステム４００を識別する識別子を、任意のコード（例えば、ウェブリソース用のＪａｖａ(登録商標)スクリプトコード）と関連付けることができ、又は他の方法により、販売事業者オンラインリソース内に任意の好適な「セキュアなトランザクション」プロンプト（例えば、図３Ａのセキュアな支払いプロンプト３０９）を提供するために、販売事業者サブシステム２００にとって利用可能とさせることができる）。

【００６１】

プロセス６００のステップ６１６では、商業エンティティサブシステム４００がステップ６１４で販売事業者サブシステム２００から好適なチャレンジ要求データ６６４を受信したことに応じて、商業エンティティサブシステム４００は、チャレンジ要求の販売事業者識別子１６７によって識別される販売事業者オンラインリソース１１３を妥当性検査するように機能することができる。例えば、ステップ６１６では、商業エンティティサブシステム４００は、受信したチャレンジ要求データ６６４の販売事業者識別子１６７により識別された販売事業者オンラインリソース１１３が商業エンティティサブシステム４００において妥当で、かつ登録された販売事業者オンラインリソースであることの確認を試みるように機能することができ、それは、（例えば、（例えば、ステップ６０６で）販売事業者識別子１６７が商業エンティティサブシステム４００に登録されており、かつそのような登録が依然として妥当であること（例えば、商業エンティティサブシステム４００が表４３０から販売事業者識別子１６７を除去しておらず、又は疑わしいか、又は他の理由で、もはや信頼されていないとして表４３０内のその販売事業者識別子１６７にフラグをたてていないこと、及び／又は（例えば、表４３０内の）販売事業者識別子１６７と関連付けられた証明書が依然として妥当であること）を判定するため）表４３０内のその販売事業者識別子１６７を識別することによって、及び／又は、その販売事業者識別子１６７と関連付けられ、又はそれにより識別されたドメインを識別し、（例えば、ステップ５０１及び／又はステップ６０６に関して説明するように）そのドメイン上にホストされ得るファイルを再検証することでそのドメインを再検証することによって、確認することができ、そのような再検証を、代替的に又は追加的に、必ずしもデータ６６４の受信に応じたステップ６１６ではなく、任意の好適な時（例えば、定期的に又は別の方法で）に商業エンティティサブシステム４００により実行することができる。追加的に、又は代替的に、ステップ６１６では、商業エンティティサブシステム４００は、受信したチャレンジ要求データ６６４の署名の妥当性検査を試みるよう動作することができ、それは、表４３０内、又はその他商業エンティティサブシステム４００内における受信したチャレンジ要求データ６６４の販売事業者識別子１６７と関連付けられ得る販売事業者鍵１５７（例えば、

ステップ６０６の登録の間に行われていることがある関連付け）を識別し、そして、受信したチャレンジ要求データ６６４の署名を妥当性検査するために（例えば、商業エンティティサブシステム４００にとってアクセス可能な販売事業者鍵１５７が、ステップ６１４でチャレンジ要求データ６６４を商業エンティティサブシステム４００に通信する前にチャレンジ要求データ６６４に署名するために販売事業者サブシステム２００により使用されていた、販売事業者サブシステム２００にとってアクセス可能な販売事業者鍵１５７とともに設定されたペアの鍵（例えば、鍵のうち一方を公開鍵とすることができ、他方をペアの鍵セットの秘密鍵とすることができる）のうちの１つであることを確認するため）、その識別された販売事業者鍵１５７を利用することによって行うことができ、それは、プロセス６００の後半部（単数又は複数）で（例えば、販売事業者サブシステム２００が商業エンティティサブシステム４００により事前に暗号化されたデータを解読し得るステップ６３６で）販売事業者サブシステム２００の使用に必要とされ得る販売事業者サブシステム２００による販売事業者鍵１５７の所持を確実とすることができる。商業エンティティサブシステム４００による受信したチャレンジ要求データ６６４の好適な妥当性検査後（例えば、受信したチャレンジ要求データ６６４の販売事業者識別子及び／又は署名の妥当性検査後）、商業エンティティサブシステム４００はまた、ステップ６１６で、好適なチャレンジデータを生成し、受信したチャレンジ要求データ６６４の好適な識別子データに対してそのチャレンジデータを記憶するように機能することができる。例えば、受信したチャレンジ要求データ６６４の好適な妥当性検査後、商業エンティティサブシステム４００は、好適なチャレンジデータ（例えば、エントロピーを介した好適なランダムデータ）を生成し、そして、商業エンティティサブシステム４００にとってアクセス可能な任意のデータ構造で（例えば、表４３０で、又は別の方法で）、チャレンジ要求データ６６４の妥当性検査セッション識別子及びチャレンジ要求データ６６４の販売事業者識別子の一方又は両方に対してそのチャレンジデータを記憶するように機能することができる。妥当性検査セッションのこのようなチャレンジデータと識別子データ（例えば、妥当性検査セッション識別子及び／又はチャレンジ要求データ６６４の販売事業者識別子）との間の記憶されたリンク又は関連付けは、（例えば、ステップ６２２で）妥当性検査セッションの販売事業者オンラインリソースを更に妥当性検査するために、かつ／又は（例えば、ステップ６３０で）実行されるセキュアなデータトランザクションを更にセキュアとするために、商業エンティティサブシステム４００により、後で使用され得る。また、いくつかの実施形態では、チャレンジ要求データ６６４の潜在的トランザクション識別情報のいずれか又はすべてが、チャレンジデータ及び識別子データに対して記憶され、又は他の方法によりそれらと関連付けられてもよい。

【００６２】

プロセス６００のステップ６１８では、商業エンティティサブシステム４００が受信したチャレンジ要求データ６６４を妥当性検査し、ステップ６１６で妥当性検査セッションの識別子データに対してチャレンジデータを生成したことに応じて、商業エンティティサブシステム４００は、任意の好適な鍵又は別の方法を用いてステップ６１６のチャレンジデータを暗号化するように機能することができ、そして、任意の他の好適なデータとともにその暗号化されたチャレンジデータを、チャレンジングデータ６６８として販売事業者サブシステム２００に通信するように機能することができる。例えば、商業エンティティサブシステム４００は、商業エンティティサブシステム４００にとってアクセス可能で、（例えば、表４３０内の、又は、その他商業エンティティサブシステム４００内における（例えば、ステップ６０６の登録の間に行われた関連付け））受信したチャレンジ要求データ６６４の販売事業者識別子１６７に関連付けられ得る任意の好適な販売事業者鍵１５７を用いてチャレンジデータを暗号化することができ、ステップ６１８でのチャレンジデータの暗号化のため商業エンティティサブシステム４００により使用されるそのような販売事業者鍵１５７は、ステップ６１６でチャレンジ要求データ６６４を妥当性検査するために、商業エンティティサブシステム４００により使用された販売事業者鍵１５７と同一であってもよいし、又は販売事業者鍵１５７とは異なる販売事業者鍵１５７であってもよ

い。このような暗号化されたチャレンジデータに加えて、任意の他の好適なデータを、ステップ６１８で商業エンティティサブシステム４００により販売事業者サブシステム２００に通信されるチチャレンジングデータ６６８の一部分として含むことができ、それは、複数の登録された販売事業者オンラインリソース及び／又は複数の販売事業者鍵を有し得る販売事業者を支援するために提供され得る、チャレンジデータを暗号化するために商業エンティティサブシステム４００により使用される販売事業者鍵１５７のハッシュ（例えば、適当な販売事業者鍵１５７（例えば、チャレンジデータを解読するための販売事業者サブシステム２００の秘密鍵１５７）を識別するために販売事業者サブシステム２００により受信及び使用され得る表４３０の公開販売事業者鍵１５７のハッシュバージョン）、チャレンジ要求データ６６４の妥当性検査セッション識別子、チャレンジ要求データ６６４の販売事業者識別子、チャレンジデータの暗号化のために商業エンティティサブシステム４００により使用される販売事業者鍵１５７と商業エンティティサブシステム４００において（例えば、表４３０で）関連付けられた販売事業者識別子などを含むが、これらに限定されない。好適なチャレンジングデータ６６８を、ステップ６１８で任意の好適な方法で商業エンティティサブシステム４００により販売事業者サブシステム２００に通信することができる（例えば、このようなチャレンジングデータ６６８を、好適な通信プロトコルを用いた通信経路８５を介して商業エンティティサブシステム４００のサーバ４１０から販売事業者サブシステム２００のサーバ２１０に送信することができる）。

【００６３】

プロセス６００のステップ６２０では、販売事業者サブシステム２００がステップ６１８でそのようなチャレンジングデータ６６８を受信したことに応じて、販売事業者サブシステム２００は、受信したチャレンジングデータ６６８を処理し、そして、現在の妥当性検査セッション中に販売事業者サブシステム２００を更に妥当性検査するためにチャレンジレスポンスデータ６７０を生成し、商業エンティティサブシステム４００に通信するように機能することができる。例えば、ステップ６２０では、販売事業者サブシステム２００は、販売事業者サブシステム２００にとって利用可能な任意の好適な販売事業者鍵１５７（例えば、（例えば、現在の妥当性検査セッション中に妥当性検査されている販売事業者オンラインリソース１１３のための）ステップ６０６で販売事業者識別子１６７に登録された販売事業者鍵１５７）を用いて、受信したチャレンジングデータ６６８の暗号化されたチャレンジデータを解読するように機能することができる。ステップ６２０での暗号化されたチャレンジデータの解読のために販売事業者サブシステム２００により使用されるこのような販売事業者鍵１５７は、（例えば、データ６６４及びデータ６６８の共通のセッション識別子と関連付けられ得るように）チャレンジングデータ６６８の任意のハッシュ鍵情報を用いて、及び／又は、チャレンジングデータ６６８の販売事業者識別子を用いて、及び／又は、チャレンジ要求データ６６４の販売事業者識別子を用いて販売事業者サブシステム２００により識別され得る。ステップ６２０での暗号化されたチャレンジデータの解読のために販売事業者サブシステム２００により使用されるこのような販売事業者鍵１５７は、ステップ６１４でチャレンジ要求データ６６４に署名するのに販売事業者サブシステム２００により使用された販売事業者鍵１５７と同一であってもよいし、又は販売事業者鍵１５７とは異なる販売事業者鍵１５７であってもよい。受信したチャレンジングデータ６６８の暗号化されたチャレンジデータを解読した後、販売事業者サブシステム２００はまた、ステップ６２０でチャレンジレスポンスデータ６７０を生成し、それを販売事業者サブシステム２００から商業エンティティサブシステム４００に通信するように機能することができ、チャレンジレスポンスデータ６７０は、他の任意の好適なデータとともに商業エンティティサブシステム４００に対して販売事業者サブシステム２００（例えば、販売事業者リソース１１３）の妥当性を更に証明しようとするために販売事業者サブシステム２００により解読されるチャレンジデータを含むことができ、この他の任意の好適なデータは、現在の妥当性検査セッションの妥当性検査セッション識別子（例えば、チャレンジ要求データ６６４及び／又は受信したチャレンジングデータ６６８の妥当性セッション識別子）、現在の妥当性検査セッションによって妥当性検査されている販売事

業者オンラインリソースと関連付けられた販売事業者識別子（例えば、チャレンジ要求データ６６４の販売事業者識別子、チャレンジデータの暗号化のために商業エンティティサブシステム４００により使用される販売事業者鍵１５７と商業エンティティサブシステム４００で（例えば、表４３０で）関連付けられた販売事業者識別子など）、ステップ６１４のチャレンジ要求データ６６４に含まれてもよいし、含まれなくてもよいセキュアなデータトランザクションが実行されるための任意の好適な潜在的トランザクション識別情報のいずれか、又はすべてを含むが、これらに限定されない。チャレンジレスポンスデータ６７０を、販売事業者サブシステム２００により（例えば、ＨＴＴＰヘッダで、又は別の方法で）、販売事業者サブシステム２００にとって利用可能な販売事業者鍵（例えば、（例えば、現在妥当性検査されている販売事業者オンラインリソース１１３のための）販売事業者識別子１６７にステップ６０６で登録される販売事業者鍵１５７）で署名することができ、それにより、販売事業者オンラインリソース１１３を更に妥当性検査するために、チャレンジレスポンスデータ６７０を、商業エンティティサブシステム４００により効率的に利用することができる。ステップ６２０でチャレンジレスポンスデータ６７０に署名するために販売事業者サブシステム２００によって使用され得るこのような販売事業者鍵１５７は、ステップ６１４でチャレンジ要求データ６６４に署名するために販売事業者サブシステム２００によって使用され得る販売事業者鍵１５７と同一の販売事業者鍵１５７であってもよいし、又は異なる販売事業者鍵１５７であってもよい。追加的に、又は代替的に、ステップ６２０でチャレンジレスポンスデータ６７０に署名するために販売事業者サブシステム２００によって使用され得るこのような販売事業者鍵１５７は、ステップ６２０で暗号化されたチャレンジデータを解読するために販売事業者サブシステム２００によって使用され得る販売事業者鍵１５７と同一の販売事業者鍵１５７であってもよいし、又は異なる販売事業者鍵１５７であってもよい。ステップ６２０では、任意の好適なチャレンジレスポンスデータ６７０を、適切な方法で販売事業者サブシステム２００により商業エンティティサブシステム４００に通信することができる（例えば、このようなチャレンジレスポンスデータ６７０を、好適な通信プロトコルを用いた通信経路８５を介して販売事業者サブシステム２００のサーバ２１０から商業エンティティサブシステム４００のサーバ４１０に送信することができる）。

【００６４】

プロセス６００のステップ６２２では、商業エンティティサブシステム４００がステップ６２０で販売事業者サブシステム２００から好適なチャレンジレスポンスデータ６７０を受信したことに応じて、商業エンティティサブシステム４００は、現在の妥当性検査セッションで更なる販売事業者サブシステム２００及び対象となるその販売事業者オンラインリソースを妥当性検査するように機能することができる。例えば、ステップ６２２では、商業エンティティサブシステム４００は、受信したチャレンジレスポンスデータ６７０の署名の妥当性検査を試みようと動作することができ、それは、表４３０内の受信したチャレンジレスポンスデータ６７０の妥当性検査セッション識別子と関連付けられ得る、かつ表４３０内の、又は商業エンティティサブシステム４００における別の方法（例えば、ステップ６０６の登録の間に行われていることがある関連付け）の、受信したチャレンジレスポンスデータ６７０の販売事業者識別子１６７と関連付けられ得る販売事業者鍵１５７を識別し、そして、受信したチャレンジ要求データ６７０の署名を妥当性検査するために（例えば、商業エンティティサブシステム４００にとってアクセス可能な販売事業者鍵１５７が、ステップ６２０でチャレンジレスポンスデータ６７０を商業エンティティサブシステム４００に通信する前にチャレンジレスポンスデータ６７０に署名するために販売事業者サブシステム２００により使用されていた、販売事業者サブシステム２００にとってアクセス可能な販売事業者鍵１５７とともに設定されたペアの鍵（例えば、鍵のうち一方を公開鍵とすることができ、他方をペアの鍵セットの秘密鍵とすることができる）のうちの１つであることを確認するため）、その識別された販売事業者鍵１５７を利用することによって行うことができる。ステップ６２２でチャレンジレスポンスデータ６７０の署名を妥当性検査するために商業エンティティサブシステム４００により使用され得る、そ

のような販売事業者鍵１５７は、ステップ６１６でチャレンジレスポンスデータ６６４の署名を妥当性検査するために商業エンティティサブシステム４００によって使用され得る販売事業者鍵１５７と同一の販売事業者鍵１５７であってもよいし、又はそれとは異なる販売事業者鍵１５７であってもよく、及び／又は、ステップ６２２でチャレンジレスポンスデータ６７０の署名を妥当性検査するために商業エンティティサブシステム４００によって使用され得る、そのような販売事業者鍵１５７は、ステップ６１８でチャレンジデータを暗号化するために商業エンティティサブシステム４００によって使用され得る販売事業者鍵１５７と同一の販売事業者鍵１５７であってもよいし、又はそれとは異なる販売事業者鍵１５７であってもよい。追加的に、又は代替的に、ステップ６２２では、商業エンティティサブシステム４００は、受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータが妥当なチャレンジデータであることの確認を試みるように機能することができる。例えば、商業エンティティサブシステム４００は、受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータが現在記憶されているか、又は他の方法により、商業エンティティサブシステム４００にとって独立して（例えば、表４３０で）アクセス可能であることを確認しようとするように機能することができる。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、同一のチャレンジデータが表４３０に現在記憶されていることを識別することによって、受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータの妥当性を判定することができる。代替的に、商業エンティティサブシステム４００は、ステップ６１６で表４３０に記憶されているような、受信したチャレンジレスポンスデータ６７０の任意の好適な識別子データに対して（例えば、妥当性検査セッション識別子又は販売事業者識別子に対して）同一のチャレンジデータが現在表４３０に記憶されていることを識別することによって、受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータの妥当性を判定することができる。いくつかの実施形態において、チャレンジデータと妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクを、又はこのような記憶されたチャレンジデータ自体を、商業エンティティサブシステム４００は、リンク又は記憶されたデータが自動で削除される前の限られた時間量の間だけしか維持できないので、販売事業者サブシステム２００は、チャレンジングデータ６６８を受信し、その後、特定の妥当性検査セッションのための販売事業者オンラインリソースを妥当性検査するために、適切なチャレンジレスポンスデータ６７０を商業エンティティサブシステム４００に送信しなければならない特定の持続時間に限定されることがある（例えば、商業エンティティサブシステム４００は、特定時間後の商業エンティティサブシステム４００におけるチャレンジデータと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、リンク又はチャレンジデータが作成された後１０分以内に表４３０からリンク又はチャレンジデータを除去する）ように動作することができ、それにより、トランザクションのセキュリティを向上させることができる）。したがって、（例えば、ステップ６０８で登録するように）商業エンティティサブシステム４００における販売事業者鍵と販売事業者識別子との１つ以上の関連付けを用いて、（例えば、ステップ６１０及び／又はステップ６１２で識別されるように）実行される特定のセキュアなデータトランザクションのステップ６１４～ステップ６２２のいずれか又はすべてにおける販売事業者オンラインリソースの妥当性検査を完了することができる。

【００６５】

商業エンティティサブシステム４００による受信したチャレンジレスポンスデータ６７０の好適な妥当性検査後（例えば、受信したチャレンジレスポンスデータ６７０の署名の妥当性検査後及び／又は受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータの妥当性検査後）、商業エンティティサブシステム４００はまた、ステップ６２２で、好適な妥当性検査データを生成し、受信したチャレンジ要求データ６６４及び／又は受信したチャレンジレスポンスデータ６７０の好適な識別子データに対してその妥当性検査データを記憶するように機能することができる。例えば、受信したチャレンジ要求データ６６４及び／又は受信したチャレンジレスポンスデータ６７０の好適な妥当性検査後

、商業エンティティサブシステム４００は、好適な妥当性検査データ（例えば、エントロピーを介した任意の好適なランダムデータ及び／又は任意の好適な暗号ナンス）を生成し、そして、商業エンティティサブシステム４００にとってアクセス可能な任意のデータ構造で（例えば、表４３０で、又は別の方法で）、チャレンジ要求データ６６４及びチャレンジレスポンスデータ６７０の妥当性検査セッション識別子及び販売事業者識別子の一方又は両方に対してその妥当性検査データを記憶するように機能することができる。妥当性検査セッションのこのような妥当性検査データと識別子データ（例えば、妥当性検査セッション識別子ならびに／又はチャレンジ要求データ６６４及び／若しくはチャレンジレスポンスデータ６７０の販売事業者識別子）との間の記憶されたリンク又は関連付けは、（例えば、ステップ６３０で）実行されるセキュアなデータトランザクションを更にセキュアとするために、商業エンティティサブシステム４００により、後で使用され得る。また、いくつかの実施形態では、チャレンジ要求データ６６４及び／又はチャレンジレスポンスデータ６７０の潜在的トランザクション識別情報のいずれか又はすべてが、妥当性検査データ及び識別子データに対して記憶され、又は他の方法によりそれらと関連付けられてもよい。

【００６６】

商業エンティティサブシステム４００において（例えば、表４３０内で）、受領したチャレンジレスポンスデータ６７０が復号されたチャレンジデータを、チャレンジデータが識別子情報（妥当性検査セッション識別子及び／又は販売事業者識別子）にリンクされていることの確認によって妥当性検査したことに応じて、商業エンティティサブシステム４００は、ステップ６２２においてそのリンクを消費し（例えば、チャレンジデータと商業エンティティサブシステム４００での妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、表４３０からリンクを除去する））、妥当性検査データ（例えば、任意の好適なランダムデータ（例えば、暗号ナンス（例えば、エントロピーを介した任意の好適なランダムデータ））を生成し、そして、妥当性検査データを任意の好適な識別子情報(例えば、例えば、チャレンジ要求及び／若しくはチャレンジレスポンスの妥当性検査セッション識別子、かつ／又はチャレンジ要求及び／若しくはチャレンジレスポンスの販売事業者識別子に対する)に対し、又は他の方法によりそれに関連付けて、商業エンティティサブシステム４００において（例えば、表４３０又は別の方法などの任意の好適なデータ構造で）記憶することができる。代替的に、商業エンティティサブシステム４００（例えば、表４３０内）において、チャレンジデータが識別子情報（例えば、妥当性検査セッション識別子及び／又は販売事業者識別子情報）にリンクされていることを確認することによって、受信したチャレンジレスポンスデータ６７０の解読済のチャレンジデータの妥当性検査に応じて、商業エンティティサブシステム４００は、ステップ６２２で、そのリンクを維持するか、又は他の方法により商業エンティティサブシステム４００（例えば、表４３０内）でそのリンクを更新し（例えば、そのリンクと関連付けられ得るタイマーをリセットするか、又はそのリンクと関連付けるために任意の追加潜在的トランザクション識別情報を追加する）、そして、（例えば、ステップ６１６で生成された）そのリンクのチャレンジデータを、ステップ６２２で本来生成され得る妥当性検査データとして利用するように機能することができる。いくつかの実施形態では、ステップ６１８～ステップ６２２でのチャレンジデータの使用は、ステップ６２４～ステップ６３０での妥当性検査データの使用とは異なり得るため、チャレンジデータと妥当性検査データはサイズ又は任意の他の好適なプロパティ（単数又は複数）に関して、異なっていてもよい。

【００６７】

プロセス６００のステップ６２４では、商業エンティティサブシステム４００が受信したチャレンジ要求データ６６４を妥当性検査し、及び／又は受信したチャレンジレスポンスデータ６７０を妥当性検査し、ステップ６２２で妥当性検査セッションの識別子データに対して妥当性検査データを生成し、又は他の方法によりそれを定義することに応じて、商業エンティティサブシステム４００は、任意の好適な妥当性検査レスポンスデータ６７

４を生成し通信するように機能することができる。例えば、妥当性検査レスポンスデータ６７４は、任意の他の好適なデータとともにステップ６２２の妥当性検査データを含むことができ、この任意の他の好適なデータは、妥当性検査セッション識別子（例えば、チャレンジ要求データ６６４及び／又はチャレンジレスポンスデータ６７０の、及び／又は、妥当性検査セッションと関連付けられ得る、妥当性検査セッション識別子）、販売事業者識別子（例えば、チャレンジ要求データ６６４及び／又はチャレンジレスポンスデータ６７０の、及び／又は、商業エンティティサブシステム４００（例えば、表４３０内）において妥当性検査セッション中に妥当性検査されている販売事業者オンラインリソースと関連付けられ得る販売事業者識別子）などを含むが、これらに限定されない。いくつかの実施形態において、図６に示すように、このような妥当性検査レスポンスデータ６７４を、商業エンティティサブシステム４００から直接電子デバイス１００に（例えば、任意の好適な通信プロトコルを用いた通信経路６５を介して）通信することができ、商業エンティティサブシステム４００が妥当性検査レスポンスデータ６７４を適正な電子デバイス１００に通信することができるように、電子デバイス１００を識別するデータ（例えば、デバイス識別子１１９）は、妥当性検査セッション開始データ６６２及び／又はチャレンジ要求データ６６４及び／又はチャレンジレスポンスデータ６７０などと関連付けられてもよいし、又は他の方法により、それに含まれてもよい。代替的に、いくつかの実施形態では、このような妥当性検査レスポンスデータ６７４を、商業エンティティサブシステム４００から販売事業者サブシステム２００を介して電子デバイス１００に通信することができ、それによって、販売事業者サブシステム２００は、妥当性検査レスポンスデータ６７４を商業エンティティサブシステム４００から（例えば、任意の好適な通信プロトコルを用いた通信経路８５を介して）受信し、そして、妥当性検査レスポンスデータ６７４の少なくとも一部分を電子デバイス１００に（例えば、任意の好適な通信プロトコルを用いた通信経路１５を介して、又は非接触近接型通信として）渡すことができるので、妥当性検査レスポンスデータ４００は、ステップ６２４で直接デバイス１００とのセキュアな通信チャネルを確立する必要はなくてもよい。妥当性検査レスポンスデータ６７４は、（例えば、ＨＴＴＰヘッダ内で、又は別の方法で）商業エンティティサブシステム４００により、電子デバイス１００にとってもアクセス可能であり得る商業エンティティサブシステム４００に関連付けられたアクセス鍵（例えば、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／若しくはＩＳＤ鍵１５６ｋ又は、デバイスアプリケーション（例えば、カード管理アプリケーション１０３ｂ）に知られ得る任意の鍵）で署名されることがあるので、デバイス１００は、署名された妥当性検査データを受信するとすぐに署名を妥当性検査し、電子デバイス１００によって信頼され得ない別のエンティティサブシステムではなく、商業エンティティサブシステム４００が妥当性検査レスポンスデータ６７４を生成したことを確認することができ、及び／又は、署名された妥当性検査データは、そのようなアクセス鍵へのアクセスを有し得ないエンティティ（例えば、署名された妥当性検査データを商業エンティティサブシステム４００からデバイス１００に渡すのに使用され得る販売事業者サブシステム２００）により利用され得る。

【００６８】

上述のように、ステップ６１０の販売事業者オンラインリソースの潜在的トランザクションデータ６６０によって識別されるセキュアなデータトランザクションを行うユーザの意図を伝えるために、デバイス１００のユーザは図３Ａのセキュアな支払いプロンプト３０９などの販売事業者オンラインリソースのＧＵＩ要素（例えば無線ボタン）を選択することができる。

図３Ｂに示すように、デバイス１００及び／又は販売事業者オンラインリソース１１３は、以下の場合に応じて画面１９０ｂを提供するように構成され得る。

図３Ａの画面１９０ａにおいて、セキュアな支払いプロンプト３０９の選択を単体で、又は、デバイス１００がステップ６２４で、妥当性検査セッションエラーがなかったことを示す、妥当性検査レスポンスデータ６７４を受信したことに加えて受けた場合、及び／又は、

デバイス１００が（例えば、ステップ６２５で）、ステップ６１２における妥当性検査セッション開始データ６６２の一部分としてデバイス１００により生成されたかも知れないセッション識別子と、受信した妥当性検査レスポンスデータ６７４の一部分として提供され得るセッション識別子との一致を検証した場合。

これにより、デバイス１００は、レスポンスデータ６７４が、プロセス６００の同一の妥当性検査セッションの一部として、妥当性検査セッション開始データ６６２と関連付けられていることを確認できる（例えば、デバイス１００は（例えば、ステップ６１２で）販売事業者サブシステム２００の販売事業者識別子と組合せて妥当性検査セッション開始データ６６２のセッション識別子を記憶することができ、そして、記憶されたデータの組合せをセッション識別子及び妥当性検査レスポンスデータ６７４の販売事業者識別子と比較し（例えば、ステップ６２５で）、プロセス６００の残りの部分を可能とする前に適切な一致を確認することができ、デバイス１００は、ステップ６１２でデバイス１００により生成された任意のセッション識別子がステップ６１２で開始されたセッション中、妥当性検査される特定の販売事業者サブシステム又は販売事業者オンラインリソースに対して一意であることを確実とするように機能することができる）。いずれの場合も、図３Ｂに示すように、画面１９０ｂは、購入を行うためデバイス１００にとって利用可能であり得る特定の決済元又はクレデンシャルを選択するために１つ以上の方法でユーザにデバイス１００と相互作用するようプロンプトを表示することができる。例えば、画面１９０ｂは、ユーザがデバイス１００にとって利用可能であり得る複数の決済元のうちの１つを選択することを可能とする決済元選択プロンプト３１１を含むことができる。決済元選択プロンプト３１１は、（例えば、上述したように、潜在的トランザクションデータ６６０により決定され得る）販売事業者によってサポートされた決済ネットワークに関連付けられたクレデンシャルを有する決済元のみ含めることもできず、又は、デバイス１００にとって利用可能なすべての決済元を表示するが、許容される決済ネットワークと関連付けられたもののみ選択可能とすることもできる。決済元選択プロンプト３１１は、任意の好適な決済元（例えば、プロンプト３１１の決済オプション識別子３１１ａに示され得る「クレデンシャルＸ」を用いた決済方法、プロンプト３１１の決済オプション識別子３１１ｂに示され得る「クレデンシャルＹ」を用いた決済方法など）を含むことができ、それは、デバイス１００のセキュアエレメントにとってネイティブな任意の好適な決済クレデンシャル及び／又は、デバイス１００にとってアクセス可能な任意の利用可能な決済元の任意の好適な非ネイティブ決済クレデンシャル（例えば、クライアントデバイスとしてのデバイス１００に対してホストデバイスの役割を果たし得る別のデバイス）を含むが、これらに限定されない。一特定実施例では、図３Ｃに示すように、デバイス１００は、図３Ｂの決済元選択プロンプト３１１の識別子３１１ａの「クレデンシャルＸ」のユーザ選択の受信に応じて、画面１９０ｃを提供するように構成されてもよい。図３Ｃの画面１９０ｃは、選択された又は自動的に識別されたデフォルトのクレデンシャルをクレデンシャル識別子情報３１３で識別することができ、また、選択されたクレデンシャルを利用するユーザ及びその意図を認証するため、１つ以上の方法でデバイス１００と相互作用するようデバイス１００のユーザにプロンプトを表示することができる。これは、デバイス１００のセキュアエレメントに、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、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によるユーザの相互作用を介してユーザ認証を入力するよう（例えば、図３Ｃの認証プロンプト３１５で）ユーザにプロンプトを表示することを含むことができる。販売事業者オンラインリソース妥当性検査セッションは、潜在的トランザクションデータ６６０が通信されることに応じて、及び／又は画面１９０ａが提示されることに応じて、及び／又は図３Ａの画面１９０ａのセキュアな支払いプロンプト３０９のユーザ選択に応じて、図３Ｂの決済元選択プロンプト３１１の特定のクレデンシャルのユーザ選択に応じて、及び／又は、図３Ｃの画面１９０ｃの提示に応じて、などの任意の好適なイベントに基づいて（例えば、ステップ６１２及び／又はステップ６１４で）開始され得る。図３Ｂの決済元選択プロンプト３１１は、ステップ６１２～ステップ６２４（例えば、ステップ６１２～ステップ６１４のい

ずれか１つの前又はその間）で発生し得る妥当性検査セッションの状況にかかわらず、図３Ａの画面１９０ａのセキュアな支払いプロンプト３０９のユーザ選択に応じて、及び／又は図３Ａの画面１９０ａのセキュアな支払いプロンプト３０９のユーザ選択だけでなく、妥当性検査セッションの失敗を示すものではないステップ６２４での妥当性検査レスポンスデータ６７４の受け入れにも応じて、などの、任意の好適な瞬間に提示されてもよい。図３Ｃの認証プロンプト３１５は、ステップ６１２～ステップ６２４（例えば、ステップ６１２～ステップ６１４の前、その間、又はいずれかのステップ）で発生し得る妥当性検査セッションの状況にかかわらず、決済元選択プロンプト３１１の決済識別子のユーザ選択の受信に応じて、及び／又は、決済元選択プロンプト３１１の決済識別子のユーザ選択の受信だけでなく、妥当性検査セッションの失敗を示すものではないステップ６２４での妥当性検査レスポンスデータ６７４の受け入れにも応じてなどの、任意の好適な瞬間に提示されてもよく、及び／又は画面１９０ｃは、ステップ６２４での妥当性検査レスポンスデータ６７４の受け入れ前に提示されてもよいが、図３Ｃの認証プロンプト３１５は、ステップ６２４での妥当性検査レスポンスデータ６７４の受け入れ後までは使用を可能にされることができない。

【００６９】

デバイス１００のユーザが、ステップ６１０で受信した潜在的トランザクションデータ６６０（例えば、決済要求データ）に応じて、潜在的トランザクションへの資金供給に使用する特定の決済クレデンシャルを選択又は確認する意思及び能力があり、かつ、妥当性検査レスポンスデータ６７４がステップ６２４で電子デバイス１００によって受信されている（例えば、ステップ６１２～ステップ６２２の販売事業者オンラインリソース妥当性検査セッションの成功を示し得るデータ）場合、プロセス６００は、ステップ６２５に進むことができ、プロセス６００は、いずれのセッション識別子も一致が（例えば、上述のステップ６２５で）識別された後、（例えば、図３Ｃの認証プロンプト３１５のユーザの選択により）潜在的トランザクションデータ６６０に基づいて特定の販売事業者、製品、価格又は配送先に対して潜在的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デバイス１００のユーザによる意図及び許可を受信することを含むことができる。アクセスＳＳＤ１５４ｂは、デバイス１００のアプレット１５３ｂを活用して、そのクレデンシャル情報を商業クレデンシャルデータ通信内で可能とするために他のＳＳＤ１５４（例えば、クレデンシャルＳＳＤ１５４ａ）を使用することが可能になる前にそのような認証が発生したかどうかを判定することができる。ステップ６２５の一例としては、アクセスＳＳＤ１５４ｂのアプレット１５３ｂは、（例えば、ユーザがデバイス１００の任意のアプリケーション（例えば、デバイス１００の販売事業者リソース１１３及び／又はカード管理アプリケーション１０３ｂ）と相互作用することで使用され得る、図３のバイオメトリック入力構成要素１１０ｉなどの１つ以上の入力構成要素１１０を介して）デバイス１００のユーザの意図又はローカル認証を判定するように構成することができ、また、そのような判定に応じて、（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行うために別の特定のＳＳＤを可能とするように構成することができる。いくつかの実施形態では、このような判定の後でこのように可能とする前に、デバイス１００のＧＵＩは、選択及び認証されたクレデンシャルを用いて最終的に決済を開始するよう、１つ以上の方法でデバイス１００と相互作用するように（例えば、図３Ｃのプロンプト３１５と同様のプロンプトで）デバイス１００のユーザにプロンプトを表示することができる別の画面（図示せず）を提供するように構成することができる。デバイス１００のユーザは、（例えば、画面１９０ａ～１９０ｃの「販売事業者Ａ」及び「製品Ｂ」及び「価格Ｃ」及び「配送先Ｄ」に対する）ステップ６１０の潜在的トランザクションデータ６６０により識別された潜在的トランザクションに資金供給するために、デバイス１００にとってネイティブな特定の決済クレデンシャルの使用のためのステップ６２５で意図及び認証を提供することができる。しかし、代替的に、プロセス６００は、ステップ６２５で意図及び認証が提供され得る前に、デバイス１００のユーザが潜在的トランザクションの１つ以上の特性を調整するのを可能とすることができる（例えば、

配送先住所情報は、画面１９０ａ及び／又は画面１９０ｂ上で、又は他の方法により、販売事業者サブシステム２００とデバイス１００との間で通信される追加の更新された潜在的トランザクションデータ６６０を通して更新され得る）。

【００７０】

次に、潜在的トランザクションデータ６６０の特定の決済要求データの受信に応じて、ステップ６２５で特定の決済クレデンシャルのために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、デバイス１００が、（例えば、プロセス５００のステップ５１２及びステップ５１４に関して説明したように）商業エンティティサブシステム４００による使用のためのデバイストランザクションデータ６７８を生成し、暗号化し、かつ送信することを含むことができる。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、財務トランザクション（例えば、ステップ６２５）での使用のために選択され、認証され、及び／又は可能にされると、デバイス１００のセキュアエレメント１４５（例えば、ＮＦＣ構成要素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によって使用される、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及び暗号化することができる。例えばトークンデータ及び暗号データなどの、クレデンシャルＳＳＤ１５４ａ（例えば、（例えば、選択された「クレデンシャルＸ」と関連付けられ得る）ＳＳＤ１５４ａの決済カードデータ）のデバイス決済クレデンシャルデータ６７５は、ステップ６２６で少なくともトークンデータ及び暗号データを含むデバイス決済クレデンシャルデータ６７６として生成され、及び／又はクレデンシャル鍵１５５ａ’で少なくとも部分的に暗号化され得ることで、このような暗号化されたデバイス決済クレデンシャルデータ６７６は、デバイス決済クレデンシャルデータ６７５にアクセスするためのそのクレデンシャル鍵１５５ａ’へのアクセスを有するエンティティ（例えば、金融機関サブシステム３５０）により解読されてもよい。このような決済クレデンシャルデータ６７５は、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）の適切な所有をセキュアに証明するように動作し得る任意の好適なデータを含むことができ、この好適なデータは、（ｉ）トークンデータ（例えば、ＳＳＤ１５４ａのクレデンシャル情報１６１ａのＤＰＡＮ、ＤＰＡＮ満了日、及び／又はＣＶＶ）及び（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’）ならびに、デバイス１００にとって利用可能とすることができ、共有秘密を用いて暗号データを独立して生成する金融機関サブシステム３５０にとって利用可能とさせ得る任意の他の好適な情報（例えば、トークンデータの一部又は全部、デバイス１００を識別する情報、コスト及び／又は通貨などのステップ６１０の潜在的トランザクションデータ６６０の一部又は全部を識別する情報、任意の好適なカウンタ値、ナンス（例えば、妥当性検査レスポンスデータ６７４の妥当性検査データのナンス）など）を用いてセキュアエレメント１４５により生成され得る暗号）を含むが、これらに限定されない。したがって、決済クレデンシャルデータ６７５は、例えば、主アカウント番号（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、カード妥当性検査コード（「ＣＶＶ」））、有効期限、クレデンシャルに関連付けられた名称、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との間の共有秘密及び任意の他の好適な情報を用いて生成される暗号）などの、そのクレデンシャルで決済を行うのに必要なすべてのデータを含むことができる。いくつかの実施形態では、クレデンシャルＳＳＤ１５４ａの決済クレデンシャルデータ６７５の一部又は全部がステップ６２６で暗号化された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、その暗号化された決済クレデンシャルデータ６７６は、単独で、又は適用できる潜在的トランザクションデータ６６０の全部ではないが少なくとも第１の部分（例えば、販売事業者の識別、代金額の識別、通貨及び／又は配送先及び／又は製品の識別、及び一意の販売事業者型トランザクション識別子及び／又は一意のユーザデバイスベースのトランザクション識別子などを含み得る潜在的トランザクションデータ６６０の一部分又は全部）、妥当性検査レスポンスデータ６７４の一部又は全部、及び

／又は任意の他の好適な情報（例えば、デバイス１００自体を識別する情報（例えば、デバイス識別子１１９）、任意の特有のデバイスベーストランザクション識別子及び／又は同様のもの）とともに、セキュアデバイスデータ６７７としてステップ６２７でアクセス情報によって暗号化されてもよい（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によって暗号化されてもよく、及び／又はＣＡＳＤ１５８ｋによって署名されてもよい）。例えば、デバイス１００のセキュアエレメント１４５（例えば、ＮＦＣ構成要素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及び／又はデータ６７４からの販売事業者の識別（例えば、販売事業者又は、アプリケーション１１３などの購入に使用されるそのリソースの識別）だけでなく、データ６６０、ならびに、ＳＳＤ１５４ａの暗号化された決済クレデンシャルデータ６７５（例えば、暗号化された決済クレデンシャルデータ６７６）からの購入額及び／又は通貨コードの識別を、セキュアデバイスデータ６７７に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などのＳＳＤ１５４ａの決済カードデータ）を生成することができるが、（例えば、ステップ６２７でデータ６７７として）商業エンティティ鍵又はアクセス鍵で暗号化する前に、（例えば、ステップ６２６でデータ６７６として）クレデンシャル鍵で暗号化することはできない。その代わりに、このような決済クレデンシャルデータ６７５を（例えば、ステップ６２７でデータ６７７として）商業エンティティ鍵又はアクセス鍵で暗号化することができ、それによって、このような実施形態では、今後のデータ６７６に対する言及はまた、クレデンシャル鍵で暗号化されていないデータ６７５に対する言及とすることもできる。いくつかの実施形態では、こ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の方式に関連付けられた商業エンティティ公開鍵とすることができ、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し得る。商業エンティティサブシステム４００は、こ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、そして、（例えば、（例えば、プロセス６００のステップ６５４で）クレデンシャルデータをデバイス１００に供給するときに）その商業エンティティ公開鍵をデバイス１００と共有することができる。

【００７１】

次に、潜在的トランザクションデータ６６０又は潜在的トランザクション識別情報（例えば、販売事業者の識別、代金額の識別、通貨の識別、一意の販売事業者ベースのトランザクション識別子、製品／サービスの識別及び／又は同様のもの）の少なくとも一部及び／又は、妥当性検査レスポンスデータ６７４の少なくとも一部分又は全部及び／又は任意の他の好適な情報（例えば、デバイス１００自体を識別する情報、一意のデバイスベースのトランザクション識別子及び／又は同様のもの）などの、任意の追加情報とともに、セキュアデバイスデータ６７７を、（例えば、プロセス５００のステップ５１４に関して説明するように）ステップ６２８でデバイストランザクションデータ６７８としてデバイス１００から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。したがって、デバイストランザクションデータ６７８（例えば、妥当性検査レスポンスデータ６７４を有する又は有しないセキュアデバイスデータ６７７）の少なくとも一部を、デバイストランザクションデータ６７８のセキュアデバイスデータ６７７を生成した暗号化に使用されるそのアクセス情報（例えば、アクセス鍵１５５ａ、アクセス鍵１５５ｂ、ＩＳＤ鍵１５６ｋ、ＣＲＳ１５１ｋ及び／又はＣＡＳＤ１５８ｋ）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）により解読することができる。このようなデバイストランザクションデータ６７８を、ステップ６２６～ステップ６２８で生成し、そして、ステップ６２８で（例えば、セキュアエレメント１４５から、又は他の方法により通信構成要素１０６及び通信経路６５を介して）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。ステップ６２６、６２７、及び６２８は、デバイストランザクションデータ６７８の一部としてデバイス１００のセキュアエレメント１４５から生

成され送信されるクレデンシャルデータが最初に、デバイス１００の別の部分（例えばプロセッサ１０２）により解読できないように暗号化されていることを確実とすることができる。すなわち、デバイストランザクションデータ６７８の決済クレデンシャルデータ６７５を、そのセキュアエレメントの外部のデバイス１００のどの部分にも露出され得ない、又はそれによりアクセスできないクレデンシャル鍵１５５ａ’で、暗号化されたデバイス決済クレデンシャルデータ６７６として暗号化することができる。また、このようなトランザクションデータ６７８のデバイス決済クレデンシャルデータ６７６を、そのセキュアエレメントの外部のデバイス１００のどの部分にも露出され得ない、又はそれによりアクセスできないアクセス鍵（例えば、アクセス鍵１５５ａ、１５５ｂ、１５６ｋ、１５１ｋ、及び／又は１５８ｋ（例えば、本明細書では「アクセス情報」とも呼ばれる））でセキュアデバイスデータ６７７として暗号化することができる。

【００７２】

次に、ステップ６２９では、プロセス６００は、商業エンティティサブシステム４００がデバイストランザクションデータ６７８の少なくとも一部分を受信及び復号す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、デバイストランザクションデータ６７８を受信することができ、そして、商業エンティティサブシステム４００で利用可能なアクセス情報（例えば、１５５ａ、１５５ｂ、１５６ｋ、１５１ｋ、及び／又は１５８ｋ）を用いて、デバイストランザクションデータ６７８のセキュアデバイスデータ６７７を解読することができる。これにより、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データ６７５を暗号化状態に（例えば、暗号さされたデバイス決済クレデンシャルデータ６７６として）維持しつつ、（例えば、解読済のセキュアデバイスデータ６７７から）販売事業者の暗号化されていない識別を判定できるようになる。これは、商業エンティティサブシステム４００は、ステップ６２６で暗号化されたデバイス決済クレデンシャルデータ６７６として、そのようなデバイス決済クレデンシャルデータ６７５をデバイス１００のセキュアエレメント１４５により暗号化し得るクレデンシャル鍵１５５ａ’へアクセスできないからである。追加的に、又は代替的に、販売事業者は、セキュアデバイスデータ６７７とともにデバイストランザクションデータ６７８に含まれ得る追加データによって識別されてもよい。デバイストランザクションデータ６７８は、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るので、デバイス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により受信されると、商業エンティティサブシステム４００はステップ６２９で使用すべきアクセス情報はどれかを（例えば、アクセス情報１５５ａ、１５５ｂ、１５６ｋ、１５１ｋ及び／又は１５８ｋのどれを）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、それぞれの鍵は、特定のデバイス１００又は特定のセキュアエレメントに特有とすることができる。

【００７３】

また、ステップ６２９の前又は後に、ステップ６２８で通信されたデバイストランザクションデータ６７８を受信した後、プロセス６００のステップ６２９は、商業エンティティサブシステム４００が、デバイストランザクションデータ６７８に含まれるデバイス１００が有し得る妥当性検査レスポンスデータ６７４の妥当性検査データを妥当性検査することを含むことができる。例えば、このようなデバイストランザクションデータ６７８の受信に応じて、商業エンティティサブシステム４００は、そのデバイストランザクションデータ６７８から妥当性検査レスポンスデータ６７４の少なくとも一部分又は全部を識別し、かつ受信したデバイストランザクションデータ６７８の妥当性検査データが商業エンティティサブシステム４００に現在記憶されていることを確認する、又は、より具体的には、一部の実施形態では、受信したデバイストランザクションデータ６７８の妥当性検査データが、（例えば、プロセス５００のステップ５１６と同様に）ステップ６３０で（例えば、表４３０内の）受信したデバイストランザクションデータ６７８の妥当性検査セッション識別子に対して、及び／又は受信したデバイストランザクションデータ６７８の販

売事業者識別子に対して商業エンティティサブシステム４００に現在記憶されていることを確認するように機能することができる。いくつかの実施形態において、妥当性検査データと妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクを、リンクが自動的に削除される前の限られた時間量の間だけしか維持できないので、電子デバイス１００は、妥当性検査された販売事業者オンラインリソースとの特定のセキュアデータトランザクションを実行するため、そのデバイストランザクションデータ６７８のセキュアデバイスデータ６７７を商業エンティティサブシステム４００によりセキュアとできるようにするために、ステップ６２４で妥当性検査レスポンスデータ６７４を受信し、そして、ステップ６２８でデバイストランザクションデータ６７８を、商業エンティティサブシステム４００に送信しなければならない特定の持続時間に限定されることがある（例えば、商業エンティティサブシステム４００は、特定時間後の商業エンティティサブシステム４００におけるチャレンジデータと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、リンクが作成された後１０分以内に表４３０からのリンクを除去する）ように動作することができ、それにより、トランザクションのセキュリティを向上させることができる）。追加的に、又は代替的に、妥当性検査データと、妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間の記憶されたリンクも、ステップ６２２で、ステップ６１４及びステップ６２０の１つ以上の間に販売事業者サブシステム２００により商業エンティティサブシステム４００にとって利用できるようにした、デバイス１００と販売事業者サブシステム２００との間で共有される特定のタイプのセキュアなデータ（例えば、財務トランザクション用の通貨及び金額ならびに決済タイプ）の識別などの、好適な特定の潜在的トランザクション識別情報と（例えば、チャレンジ要求データ６６４及び／又はチャレンジレスポンスデータ６７０の一部分として）関連付けることができ、また、同様の特定の潜在的トランザクション識別情報も、ステップ６２８のデバイストランザクションデータ６７８の一部分として電子デバイス１００により商業エンティティサブシステム４００にとって利用できるようにすることができるので、ステップ６３０はまた、商業エンティティサブシステム４００が（例えば、ステップ６１６及び／又はステップ６２２で表４３０に記憶されているように）ステップ６１４及び／又はステップ６２０で受信した妥当性検査データに対して現在記憶されている特定の潜在的トランザクション識別情報がステップ６２８で受信された特定の潜在的トランザクション識別情報少なくとも同様であることを確認することも含むことができる。例えば、ステップ６２２では、特定の妥当性検査データが、５米ドルの財務トランザクションを示す潜在的トランザクションと関連付けられた特定の潜在的トランザクション識別情報に対して記憶されるが、ステップ６２８で特定の妥当性検査データとともに商業エンティティサブシステム４００により受信された特定の潜在的トランザクション識別情報が２，０００米ドルの財務トランザクションを示している場合、商業エンティティサブシステム４００は、＄５と＄２，０００との間のずれの大きさにより、デバイストランザクションデータ６７８の妥当性検査データを妥当性検査しないように動作することができる。したがって、妥当性検査データとステップ６２８で受信したデバイストランザクションデータ６７８の妥当性検査セッション識別子及び／又は販売事業者識別子とが、商業エンティティサブシステム４００で（例えば、表４３０で）アクティブにリンクされていると確認できる場合、そのリンクと関連付けられ得る他のデータがデバイストランザクションデータ６７８により満たされていない場合、妥当性検査データを妥当性検査しなくてもよい（例えば、ステップ６１６～ステップ６２２中に識別されたセキュアなデータトランザクションのいずれの好適な特性が、好適な量だけ（例えば、財務トランザクション通貨値の１０％超だけ、又は健康データのタイムフレームの１０％超などの、特定のデータタイプのパーセンテージ偏差）又は、特定のタイプだけ異なる（例えば、健康データのタイプは識別されたデータの２つのインスタンス間（例えば、心拍数データ対マイルウォークデータ、又はバイオメトリックデータ対決済データなど）で異なる、及び／又はトランザクションに使用される通貨タイプは識別されたデータの２つのインスタンス間（例えば、ドル対円など）で異なるといった識別されたデータの

異なるタイプ及び／又は商品の配送のための決済トランザクションの配送先住所の場所）ステップ６２８のデバイストランザクションデータ６７８とは異なる）。データ比較は、特定のトランザクションのために実際に受信されたデータと、特定の販売事業者が予想基準からずれた特定のインスタンスを検出する（例えば、そのときまでに決済クレデンシャルデータ等を処理しただけの販売事業者によるバイオデータの第１のトランザクションを検出する）ための過去の集計データとの間で行うことができ、潜在的トランザクション識別情報は、妥当性検査又は販売事業者によるかつ必ずしもユーザデバイスに関しない不正を検出するのに使用されてもよい（例えば、エンドユーザのプライバシー問題を尊重する特定のインスタンスにおいてデバイスのためではなく販売事業者のために集計データをトラックしてもよい）。

【００７４】

次に、ステップ６３１では、プロセス６００は、商業エンティティサブシステム４００が決済要求データ６１０及び／又は妥当性検査セッションにより、したがって、デバイストランザクションデータ６７８により識別され得る販売事業者と関連付けられた販売事業者鍵（例えば、販売事業者鍵１５７）を識別し、そして、その販売事業者鍵を用いてデバイストランザクションデータ６７８の少なくとも一部分を再暗号化することを含むことができる。すなわち、ステップ６２９で好適なアクセス情報を用いてデバイストランザクションデータ６７８の少なくとも一部分を解読した後（例えば、セキュアデバイスデータ６７７を解読し、デバイス決済クレデンシャルデータ６７６及び、セキュアデバイスデータ６７７内に暗号化され得る任意の他の情報（例えば、妥当性検査レスポンスデータ６７４）を達成した後）、商業エンティティサブシステム４００は、ステップ６３１で、デバイストランザクションデータ６７８の少なくとも一部分（例えば、デバイス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）を、デバイストランザクションデータ６７８内で識別された販売事業者情報と関連付けられ得る、又はステップ６３０で妥当性検査されたリンクされた妥当性検査データと関連付けられる表４３０で識別され得る適切な販売事業者鍵で再暗号化することができる。例えば、このような販売事業者鍵（例えば、販売事業者鍵１５７）を、デバイストランザクションデータ６７８を用いて識別された商業エンティティ販売事業者情報と、図１Ａの表４３０でのデータとを比較することによって決定することができる。この決定された適切な販売事業者鍵により、商業エンティティサブシステム４００は、その販売事業者鍵（例えば、販売事業者鍵１５７）で、デバイストランザクションデータ６７８の少なくとも一部分（例えば、デバイス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）を暗号化された販売事業者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、暗号化された販売事業者クレデンシャルデータ６８１は、デバイス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デバイス決済クレデンシャルデータ６７６、ならびに、デバイストランザクションデータ６７８及び／又は潜在的トランザクションデータ６６０からの、又はそれに基づいた購入額データ又は他の好適なトランザクションデータなどの好適なトランザクションデータを含むことができる。デバイストランザクションデータ６７８からの販売事業者識別情報は、その販売事業者識別が既に、暗号化された販売事業者クレデンシャルデータ６８１がステップ６３１で暗号化され得る販売事業者鍵を決定するのに使用されているので、暗号化された販売事業者クレデンシャルデータ６８１の中に含まれる必要はない。暗号化された販売事業者クレデンシャルデータ６８１は、販売事業者サブシステム２００により受信されると、販売事業者サブシステム２００がこのような暗号化された販売事業者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を確立できるように、及び／又は販売事業者サブシステム２００がこのような暗号化された販売事業者クレデンシャルデータ６８１が署名後修正されていないことを確実とすることができるように商業エンティティサブシステム４００により署名され得る。このような暗号化された販売事業者クレデンシャルデータ６８１は、ステップ６３１で生成され、そして、ステップ６３２で、セキュアなトランザクションデータ６８２として他の好適なデータとともにデバイス１００に（例えば、図１Ａの経路６５を介して商業エ

ンティティサブシステム４００のサーバ４１０からデバイス１００の通信構成要素１０６に）送信されてもよい。

【００７５】

ステップ６３１及びステップ６３２は、図１Ａのセキュアなトランザクションデータ６８２の一部として商業エンティティサブシステム４００から送信されたクレデンシャルデータ（例えば、暗号化された販売事業者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）が、セキュアエレメント１４５以外のデバイス１００の一部分により解読できないように暗号化されてもよいことを確実とするように機能することができる。すなわち、セキュアな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、暗号化された販売事業者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）を、いくつかの実施形態では、セキュアエレメント１４５を含む、デバイス１００のいかなる部分にも露出されていない、又は他の方法により、それによりアクセスできない販売事業者鍵（例えば、販売事業者鍵１５７）で暗号化することができる。また、セキュアな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、暗号化された販売事業者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）を、（例えば、ステップ６２６で）セキュアエレメント１４５の外部のデバイス１００のいかなる部分にも露出していない、又はアクセスできないクレデンシャル鍵１５５ａ’で暗号化することができる。

【００７６】

そして、ステップ６３４で、セキュアなトランザクションデータ６８２を、セキュアなトランザクションデータ６８４として（例えば、通信経路１５を介して、又は非接触近接型通信５として）販売事業者サブシステム２００に転送することができる。代替的に、販売事業者クレデンシャルデータ６８１を、デバイス１００（図示せず）を介して通信することなく、商業エンティティサブシステム４００から販売事業者サブシステム２００に通信することができる。潜在的トランザクションデータ６６０の１つ、一部、又はすべての部分を、デバイス１００及び／又は商業エンティティサブシステム４００を通してセキュアなトランザクションデータ６８２及び／又はセキュアなトランザクションデータ６８４に運ぶことができるので、潜在的トランザクションの特定の識別子を、プロセス６００の間、エンティティのそれぞれにより識別することができ、その識別子は、（ｉ）販売事業者（例えば、「販売事業者Ａ」）の一意の販売事業者識別子及び／又は使用されている特定の販売事業者リソース（例えば、特定の販売事業者アプリケーション１１３’）の識別などの特定の販売事業者情報、（ii）トランザクションに支払うの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に支払われる特定の通貨額（例えば、「価格Ｃ」）の識別及び／又は購入され、又はレンタルされ、又は他の方法により、支払われる特定の製品又はサービス（すなわち、「製品Ｂ」）の識別及び／又は使用されるデフォルトの又は初期の配送先住所（すなわち、「配送Ｄ」）の識別などの特定のトランザクション情報、（iii）トランザクションに対する販売事業者にとって許容できる１つ以上のタイプの決済方法（例えば、購入に使用され得る決済カードのリスト（例えば、ＶｉｓａではなくＭａｓｔｅｒＣａｒｄ））又はデバイス１００により選択され得る決済方法（すなわち、「クレデンシャルＸ」）を示す情報、（iv）一意の販売事業者ベースのトランザクション識別子（例えば、行われているトランザクションと関連付けるための販売事業者サブシステム２００によりランダムに又は一意に生成され得る３又は４文字の英数字列などの任意の好適なデータ要素）、（v）一意のユーザデバイスベースのトランザクション識別子（例えば、行われるトランザクションと関連付けるためのデバイス１００によりランダムに又は一意に生成され得る３又は４文字の英数字列などの任意の好適なデータ要素）、（vi）一意の販売事業者オンラインリソース妥当性検査セッション識別子などを含むが、これらに限定されない。

【００７７】

決済クレデンシャルデータ６７５／６７６を含む販売事業者クレデンシャルデータ６８１が販売事業者サブシステム２００により（例えば、ステップ６３４でセキュアなトラン

ザクションデータ６８４として）受信されると、プロセス６００はまた、販売事業者サブシステム２００が決済データ６８６を生成し、取得銀行サブシステム３００に（例えば、図１Ａの販売事業者サブシステム２００と取得銀行サブシステム３００との間の通信経路２５を介して）送信するように構成され得るステップ６３６も含むことができ、データ６８６は、（例えば、セキュアなトランザクションデータ６８４に含まれ得る、又は他の方法により、それに関連付けられ得るように、又は他の方法により、販売事業者サブシステム２００により（例えば、（例えば、一意のトランザクション識別子に基づいた）潜在的トランザクションデータ６６０により）既知のトランザクションと関連付けられ得るように）デバイス１００のセキュアなデバイス決済クレデンシャルデータ及び製品又はサービスに対する販売事業者の購入価格を示し得る、決済情報と許可要求とを含むことができる。例えば、ステップ６３６では、販売事業者サブシステム２００は、その既知の販売事業者鍵１５７を活用して、セキュアなトランザクションデータ６８４の販売事業者クレデンシャルデータ６８１を少なくとも部分的に解読することができるので、決済データ６８６は、金融機関サブシステム３５０にとって利用可能ではない鍵ではなく、そのクレデンシャル鍵１５５ａ’（例えば、データ６７６）で暗号化されたクレデンシャルＳＳＤ１５４ａのセキュアな決済クレデンシャルデータを含むことができる。

【００７８】

ステップ６３６で決済データ６８６が取得銀行サブシステム３００に送信されると、ステップ６３８では、取得銀行サブシステム３００は、許可要求データ６８８として決済データ６８６からの許可要求情報を金融機関サブシステム３５０に（例えば、図１Ａの取得銀行サブシステム３００と金融機関サブシステム３５０との間の通信経路３５を介して）転送することができる。次に、ステップ６４０では、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（例えば、ステップ６４０でデータ６８８として取得銀行サブシステム３００から直接に、又はデータ４０５として決済ネットワークサブシステム３６０を介して間接に）受信するとき、決済情報（例えば、デバイス１００のセキュアエレメント１４５によるクレデンシャル鍵１５５ａ’によって暗号化されたデバイス１００の決済クレデンシャルデータ６７５（例えば、データ６７６））及び決済額は、そのそれぞれは許可要求データ６８８ならびにデータ６８２、６８４、及び／又は６８６に含まれ得るが、（例えば、金融機関サブシステム３５０でクレデンシャル鍵１５５ａ’を用いて）解読され、商業クレデンシャルと関連付けられたアカウントは、購入額をカバーするには十分なクレジットを有するかを判定するように分析され得る。十分な資金が存在しない場合、発行銀行サブシステム３７０は、取得銀行サブシステム３００に否定的許可レスポンスを送信することにより、要求されたトランザクションを断ることができる。しかし、十分な資金が存在する場合、発行銀行サブシステム３７０は、取得銀行サブシステム３００に肯定的許可レスポンスを送信することにより、要求されたトランザクションを承認することができ、財務トランザクションを完了することができる。いずれかのタイプの許可レスポンスを、プロセス６００のステップ６４０で許可レスポンストランザクション状況データ６９０としてユーザ金融サブシステム３５０により取得銀行サブシステム３００に（例えば、図１Ａ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に提供され得る許可レスポンスデータ４１５に基づいて通信経路３５を介して発行銀行サブシステム３７０から直接取得銀行サブシステム３００に、又は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に）提供することができる。次に、ステップ６４０で、許可レスポンストランザクション状況データ６９０の受信に応じて、プロセス６００はまた、取得銀行サブシステム３００又は任意の他の好適なサブシステムがステップ６４２で許可レスポンストランザクション状況データ６９２として、このような許可レスポンストランザクション状況データを販売事業者サブシステム２００と共有することも含むことができ、そして、許可レスポンストランザクション状況データを、ステップ６４４で確認されたトランザクション状況データ６９４として（例えば、販売事業者リソースを用いて、又は別の方法で）デバイス１００と共有することができる。このような確認されたトランザクション状況データは、図３Ｄの画面１９０ｄ

の確認データ３１７などの好適な確認データをデバイス１００に提供するように構成されてもよい。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況データは、ステップ６４４でデバイス１００でトランザクションを終了するように機能することができる。追加的に、又は代替的に、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況データは、トランザクションを終了する（例えば、有効な資金が利用可能でなければ、又は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終了するが、有効でない配送先住所が判定された場合は、トランザクションを継続し更新を可能とする）ように動作してもよいし、動作しなくしてもよい。トランザクションを終了させないあらゆるトランザクション状況データは、その処理がアプリケーションによりキャンセルされる、その処理がユーザによりキャンセルされる、又は処理が完了するまで決済処理を継続させることができる。

【００７９】

したがって、販売事業者サブシステム２００は、セキュアなトランザクションデータ６８４又は販売事業者クレデンシャルデータ６８１の他のキャリアを好適な方法で処理するように構成することができる。例えば、販売事業者クレデンシャルデータ６８１からデバイス決済クレデンシャルデータを得るために、販売事業者サブシステム２００は、受信した販売事業者クレデンシャルデータ６８１の署名性が有効であり、その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。販売事業者サブシステム２００は、商業エンティティサブシステム４００がどの販売事業者鍵（例えば、どの販売事業者公開鍵１５７）を使用してもよいかを決定して販売事業者クレデンシャルデータ６８１を構築する任意の好適な技法を使用することができる。そして、販売事業者サブシステム２００は、対応する販売事業者秘密鍵（例えば、販売事業者サブシステム２００での販売事業者秘密鍵１５７）を検索し、その検索された鍵を用いて暗号化された販売事業者クレデンシャルデータ６８１をカプセル化解除及び／又は解読して暗号化データ６７６を復元することができる。そして、このようなデータ６７６を、適切な決済ネットワーク３６０に提供することができ、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’を活用して暗号化されたデバイス決済クレデンシャルデータ６７６をカプセル化解除及び／又は解読し、デバイス決済クレデンシャルデータ６７５を復元する（例えば、デバイス決済クレデンシャルデータ６７５を妥当性検査するためデバイス決済クレデンシャルデータ６７５のトークンデータ及び／又は暗号データを復元する（例えば、受信したデバイス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、生成された暗号データを、受信したデバイス決済クレデンシャルデータ６７５の暗号データを比較し、その比較に基づいてトランザクションを妥当性検査するか、又は拒絶する））ことができる。

【００８０】

図６のプロセス６００で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。図示しないが、セキュアな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から直接販売事業者サブシステム２００に（例えば、ステップ６３２及びステップ６３４でデバイス１００を介さず、通信経路８５を介して）通信してもよいし、又は（例えば、ステップ６３２～ステップ６３８でデバイス１００を介さず、及び／又は販売事業者サブシステム２００を介さず、及び／又は取得銀行３００を介さず、通信経路５５を介して）直接金融機関サブシステム３５０に通信してもよい。追加的に、又は代替的に、図示しないが、セキュアなトランザクションデータを、デバイス１００から直接金融機関サブシステム３５０に（例えば、販売事業者サブシステム２００を介さずに）通信してもよい。プロセス６００の妥当性検査ステップが失敗した場合は、そのような失敗を１つ以上の好適なエンティティに通信することができることを理解されたい。例えば、ステップ６１６でチャレンジ要求データ６６４の妥当性検査が失敗した場合、及び／又はステップ６２２でチャレンジレスポンスデータ６７０の妥当性検査が失敗した場合、及び／又はステップ６３０でデバイストランザクションデータ６７

８の妥当性検査レスポンスデータ６７４の妥当性検査データの妥当性検査が失敗した場合、このような失敗は、デバイス１００が販売事業者サブシステム２００との潜在的トランザクションを解除し、デバイス１００から販売事業者オンラインリソースを潜在的に除去することができるように、商業エンティティサブシステム４００により、販売事業者サブシステム２００及び／又は電子デバイス１００と共有されてもよい。デバイス１００のユーザがステップ６２５でセキュアなデータトランザクションに使用するために特定のセキュアなデータ（例えば、特定の決済クレデンシャルの特定の決済クレデンシャルデータ）を選択した後、プロセス６００の残りのステップは、そのユーザにとって透過的に発生することがある（例えば、ステップ６２６～６４４は、デバイス１００に対するユーザによる更なる相互作用なしに発生することがあり、デバイス１００のユーザにとって瞬時に行われるもののように見えることがある）。プロセス６００は、あたかも、ステップ６２５の後、セキュアデバイスデータが自動でかつ瞬時に販売事業者サブシステム２００に送信されるように、デバイス１００のユーザに見えることがあり、トランザクションの状況は（例えば、販売事業者サブシステム２００及び／又は商業エンティティサブシステム４００により）デバイス１００に確認されることができる。追加的に、又は代替的に、販売事業者オンラインリソースの妥当性検査は、デバイス１００に対して透過的に発生することができる（例えば、ステップ６１４～６２４は、もしステップ６１２でなければ、デバイス１００に対するユーザによる相互作用なしに発生することができ、ステップ６１０の後デバイス１００のユーザに対して瞬時に行われているように見えることがある）。代替的に、いくつかの実施形態では、プロセス６００は、デバイス１００のユーザにとって透過的に一緒に発生することができる（例えば、デバイス１００は、セキュアなデバイストランザクションがいつ発生すべきかを判定し、妥当性検査レスポンスデータを自動で受信し、かつ／又はデバイストランザクションデータを自動で送信するように、かつ／又は、デバイス１００に対するユーザによるアクティブな相互作用なしにセキュアなデバイストランザクションのセキュアなトランザクションデータを自動で受信及び／又は送信するように構成されてもよく、販売事業者オンラインリソースは、その特定のセキュアなデバイストランザクションのために開始され、実行される妥当性検査セッションの間、依然として妥当性検査されてもよい）。例えば、上述のように、デバイス１００は、すべて自動で、デバイス１００のユーザによるアクティブな相互作用なしで、特定の製品を購入すべきことを決定し、その特定の製品の少なくとも１つの特定の販売事業者から関連付けられた潜在的トランザクションデータを取得するために１つ以上の販売事業者と相互作用するように構成することができる（例えば、デバイス１００は、家電製品を購入しなければならないことを決定する（例えば、洗濯機がより多くの洗濯洗剤を必要とすることを検出する、又は特定の日により多くの洗剤を購入するための、ユーザが事前に設定したカレンダ行事を検出する）ように構成され得る家電製品であって、自動で、その製品の最良の商談を提供する特定の販売事業者を識別でき、自動で、その販売事業者と相互作用し、その製品をその販売事業者から購入するためにトランザクションデータを取得し得る家電製品とすることができる）。そして、デバイス１００及び／又は特定の販売事業者は、ステップ６１２の妥当性検査セッションを自動的に開始するように機能することができる。

【００８１】

いくつかの実施形態では、ステップ６１８～ステップ６２２を、ステップ６１６でチャレンジ要求が妥当性検査された後にスキップしてもよく、代わりに、ステップ６１６で、チャレンジデータではなく妥当性検査データを生成して記憶してもよい。したがって、いくつかの実施形態では、ステップ６１４及びステップ６１６は、特定の妥当性検査セッションのための販売事業者オンラインリソースを妥当性検査するのに適切であり得る。いくつかの実施形態では、ステップ６１６で生成されたチャレンジデータは、ステップ６２２で生成された妥当性検査データとは異なってもよい。例えば、チャレンジデータは、著しく堅牢なチャレンジを可能とする十分なランダム性を、チャレンジングデータ６６８とともに販売事業者サブシステム２００に提供するのに十分な長さ（例えば、１０文字以上などの好適な長さのデータ列）とすることができるが、妥当性検査データは、セッション妥

当性検査の証拠を可能とする十分なランダム性を提供するために、及び／又は妥当性検査レスポンスデータデータ６７４で任意の好適な規格を満たすために（例えば、ＥＭＶ（Ｅｕｒｏｐａｙ　ＭａｓｔｅｒＣａｒｄ　Ｖｉｓａ）規格のデータ長要件を満たすために）、チャレンジングデータより短くてもよい（例えば、妥当性検査データは、６文字などの、チャレンジデータのデータ列より短い長さのデータ列としてもよい）。代替的に、チャレンジデータと妥当性検査データは同じであってもよく、ステップ６１６とステップ６２２の両方で再利用されてもよい。妥当性検査レスポンスデータ６７４の妥当性検査データ（例えば、ナンス）は、決済トランザクションがデバイス１００と販売事業者との間で発生するという判定に基づくだけではなく、ステップ６２４で販売事業者サブシステム２００のチャレンジの成功した妥当性検査に基づいて、商業エンティティサブシステム４００によって生成され、デバイス１００に提供されてもよい。デバイス１００が販売事業者に特有であり得るデバイス１００上のネイティブアプリケーションを介して販売事業者サブシステム２００と通信することができる場合、販売事業者アプリケーション１１３はそのようなアプリケーションによって提供されてもよい。しかし、デバイス１００が、販売事業者に特有であってもよいし、特有でなくてもよいが、（例えば、販売事業者の制御下にあるサーバ上の）販売事業者によって管理されたウェブサイトに向けられ得るインターネットブラウザアプリケーション又はハイブリッドアプリケーションを介して販売事業者サブシステム２００と通信することができる場合、販売事業者アプリケーション１１３は、通信を販売事業者のウェブサイトに（例えば、通信構成要素１０６を介して）転送し得るレイアウトエンジンソフトウェア構成要素（例えば、ＷｅｂＫｉｔ）とすることができる。例えば、デバイス１００のこのようなアプリケーション１１３は、任意のデバイストランザクションデータを販売事業者サブシステム２００に提供するためのコンジットとすることができる。

【００８２】

ここで、プロセス６００の特定の部分の代替的な実施形態を、異なる販売事業者構成に関して記載してもよい。販売事業者サブシステム２００は、制御の程度がさまざまであるプロセス６００のセキュアなトランザクションに対応するように装備されてもよい。販売事業者サブシステム２００がプロセス全体の制御を保持し得る第１の販売事業者構成では、販売事業者サブシステム２００は、販売事業者オンラインリソースの妥当性検査（例えば、ステップ６１４及びステップ６１６で、及び／又はステップ６１８及びステップ６２０で、販売事業者サブシステム２００自体が、販売事業者オンラインリソースを妥当性検査するために商業エンティティサブシステム４００と通信することができる）だけでなく、商業エンティティサブシステム４００により暗号化されたセキュアなデータの解読（例えば、ステップ６３６で、販売事業者サブシステム２００は、販売事業者鍵１５７を活用して、少なくとも部分的に、セキュアなトランザクションデータ６８４の販売事業者クレデンシャルデータ６８１を解読することができる）に対応するように機能することができる。このような第１の販売事業者構成では、販売事業者サブシステム２００は、それ自身の決済サービスプロバイダ（「ＰＳＰ」）の役割を果たすことができ、大容量をもつ巨大販売事業者（例えば、Ａｍａｚｏｎ．ｃｏｍ）が典型であり得るような、プロセス６００においてオンラインリソースを登録及び妥当性検査するための商業エンティティサブシステム４００と通信する唯一のサブシステムとすることができる。代替的に、第２の販売事業者構成では、販売事業者サブシステム２００は、図１Ａ及び図６に取得銀行３００の一部分として示され得る、ＰＳＰサブシステム３１０のような好適な販売事業者パートナサブシステムに対する決済に関する暗号解読責任を放棄してもよい。このような第２の販売事業者構成では、販売事業者サブシステム２００は、販売事業者オンラインリソースの妥当性検査に対応する（例えば、ステップ６１４で、及び／又はステップ６１８及びステップ６２０で、販売事業者サブシステム２００自体が、販売事業者オンラインリソースを妥当性検査するために商業エンティティサブシステム４００と通信することができる）ように動作することができるが、ＰＳＰサブシステム３１０は、商業エンティティサブシステム４００により暗号化されたセキュアなデータの解読に対応する（例えば、ステップ６３

８で、ＰＳＰサブシステム３１０は、販売事業者鍵１５７を活用して、少なくとも部分的に、決済データ６８６の販売事業者クレデンシャルデータ６８１を解読することができる）ように動作することができる。このような第２の販売事業者構成では、販売事業者サブシステム２００は、その決済解読のために別個のサードパーティバックエンドＰＳＰを使用することができるので、販売事業者サブシステム２００とＰＳＰサブシステム３１０はともに、プロセス６００でオンラインリソースを登録するために商業エンティティサブシステム４００と通信することができ、これは、決済サービスプロバイダを活用しうる、より小規模な販売事業者（例えば、取得銀行（例えば、Ｃｈａｓｅ　Ｐａｙｍｅｎｔｅｃｈ）又は小規模ＰＳＰ（例えば、Ｓｔｒｉｐｅ、Ｂｒａｉｎｔｒｅｅ、Ｆｉｒｓｔ　Ｄａｔａ）であり、複数の取得銀行、カード及び決済ネットワークと通信し、及び／又は、販売事業者サブシステム２００に代わって外部ネットワーク及び銀行口座との技術的接続及び関係を管理し、それによって、販売事業者サブシステム２００の金融機関への依存を少なくするように動作し得る）に典型的である。このような第２の販売事業者構成のＰＳＰサブシステム３１０はデバイス１００のユーザから隠されることができ、ユーザは、（例えば、図３Ａ～図３Ｄの画面１９０ａ～１９０ｄにより）販売事業者サブシステム２００のオンラインリソースとのインタフェースのみ行ってよい。代替的に、第３の販売事業者構成では、販売事業者サブシステム２００は、ＰＳＰサブシステム３１０などの、任意の好適な販売事業者パートナサブシステムに対するオンラインリソース妥当性検査責任及び決済解読責任を委ねることができる。このような第３の販売事業者構成では、ＰＳＰサブシステム３１０は、販売事業者オンラインリソースの妥当性検査（例えば、ステップ６１４で、ＰＳＰサブシステム３１０自体が、（例えば、ＰＳＰサブシステム３１０が販売事業者サブシステム２００からセッション開始データ６６２を受信することに応じて）販売事業者オンラインリソースを妥当性検査するために商業エンティティサブシステム４００とチャレンジ要求データ６６４を通信することができる）だけでなく、商業エンティティサブシステム４００により暗号化されたセキュアなデータの解読にも対応する（例えば、ステップ６３８で、ＰＳＰサブシステム３１０は、販売事業者鍵１５７を活用して、少なくとも部分的に決済データ６８６の販売事業者クレデンシャルデータ６８１を解読することができる）ように動作することができる。このような第３の販売事業者構成では、販売事業者サブシステム２００は、妥当性検査及び決済解読のために別個のサードパーティフロントエンドＰＳＰを使用することができる。そのため、販売事業者サブシステム２００とＰＳＰサブシステム３１０はともに、プロセス６００でオンラインリソースを登録し妥当性検査するために商業エンティティサブシステム４００と通信することができる。これは、勘定精算（checkout）及び決済プロセス全体のプロセスをサードパーティ決済サービスマークプロバイダによる代行に依存し得る「ロングテール」販売事業者に典型（例えば、ＳｔｒｉｐｅのレジはＳｔｒｉｐｅインコーポレイテッドのＰＳＰによって提供され得る）であり得る。別個のサードパーティフロントエンドＰＳＰサブシステム３１０は、（例えば、販売事業者サブシステム２００の販売事業者リソースに埋め込まれたＰＳＰサブシステム３１０のＪａｖａ　ｓｃｒｉｐｔ(登録商標)などのＰＳＰサブシステム３１０のサーバ上でホストされ得る）埋め込み可能な決済フォームをデスクトップ、タブレット及びモバイルデバイスに提供でき、これが販売事業者サブシステム２００のウェブリソース内で働くことにより、顧客は（例えばデバイス１００のユーザ）トランザクションを完了するのに販売事業者サブシステム２００のウェブリソースから離れてリダイレクトされることなく決済を行うこともでき、又は、顧客は販売事業者サブシステム２００のウェブリソースから離れてＰＳＰサブシステム３１０のウェブリソースにリダイレクトされて、ＰＳＰサブシステム３１０のウェブリソース内で決済を完了することもできる（例えば、ＰａｙＰａｌ．ｃｏｍ）。このような第３の販売事業者構成のＰＳＰサブシステム３１０は、ＰＳＰオンラインリソースを管理し動作させるように動作することができ、これは販売事業者オンラインリソースと同様であり得るが、例えば、決済自体を処理するように備えられていない販売事業者オンラインリソースによって利用され得る。これにより、例えば、ウェブサイト販売事業者オンラインリソース１１３は、そのウェブサイト販売事業者オンラ

インリソース１１３とインタフェースするデバイス１００のユーザを、ウェブサイト販売事業者オンラインリソース１１３の任意の部分に埋め込まれ得る、ウェブサイトＰＳＰオンラインリソース１１３のインタフェースにリダイレクトするか、又はユーザは、ウェブサイト販売事業者オンラインリソース１１３の任意の好適な部分からリダイレクトされ得る（例えば、図３Ａ～図３Ｄの画面１９０ａ～１９０ｄの１つ以上の任意の好適な部分は、ウェブサイト販売事業者オンラインリソースではなく、ウェブサイトＰＳＰオンラインリソースによって提供され得る）。したがって、販売事業者サブシステム２００及びＰＳＰサブシステム３１０（例えば、取得者サブシステム３００）は、合わせて、システム１の単一で堅牢な処理サブシステム２９９を提供してもよいし、又はシステム１の構成及び販売事業者サブシステム２００の能力に応じてシステム１の別個のエンティティとして使用されてもよい。

【００８３】

販売事業者オンラインリソースを商業エンティティサブシステム４００に登録することは、販売事業者サブシステム２００が、（例えば、３つの販売事業者構成のうちいずれが採用されるかに応じて）単独で又はＰＳＰサブシステム３１０と組合せて、商業エンティティサブシステム４００でオンラインリソースを妥当性検査し、また商業エンティティサブシステム４００により暗号化されるクレデンシャルデータを解読するように動作するように商業エンティティサブシステム４００に加入登録することを含むことができる。例えば、ステップ６０６は、オンラインリソースと関連付けられた１つ以上の販売事業者識別子１６７に対して商業エンティティサブシステム４００と販売事業者サブシステム２００又はＰＳＰサブシステム３１０との間で共有されている販売事業者鍵１５７であって、（例えば、ステップ６３１で）商業エンティティサブシステム４００でデータを暗号化するとともに、（例えば、ステップ６３６又はステップ６３８で）販売事業者サブシステム２００又はＰＳＰサブシステム３１０でそのデータを解読するために使用され得るこのような鍵１５７を含むことができるだけでなく、オンラインリソースと関連付けられた１つ以上の販売事業者識別子１６７に対して商業エンティティサブシステム４００と販売事業者サブシステム２００又はＰＳＰサブシステム３１０との間で共有されている証明書１７７であって、（例えば、ステップ６１４及びステップ６１６で）オンラインリソースを妥当性検査するのに使用され得る証明書１７７も含むことができる。

【００８４】

一例として、ステップ６０６では、オンラインリソース（例えば、ウェブサイト販売事業者オンラインリソース１１３）の共有鍵用の第１の証明書署名要求（「ＣＳＲ」）を生成し、商業エンティティサブシステム４００に通信することができる。共有鍵用のこの第１のＣＳＲは、オンラインリソースのＦＱＤＮ（ｆｕｌｌｙ　ｑｕａｌｉｆｉｅｄ　ｄｏｍａｉｎ　ｎａｍｅ：完全修飾ドメイン名）（例えば、ルート及びサブドメイン（例えば、ＤＮＳホスト名）及び／又は、オンラインリソースのドメインにリンクされ得る任意の好適な販売事業者識別子、及び／又は、オンラインリソースと関連付けられ得る任意の好適な販売事業者パートナの任意の他の好適な識別子（例えば、販売事業者サブシステム２００が商業エンティティサブシステム４００により暗号化されたクレデンシャルデータを解読するためにＰＳＰを使用することができる場合、ＰＳＰ識別子）を含む、その正確な位置を特定し得るウェブドメイン）などの、オンラインリソースに関連付けられた少なくとも１つの販売事業者識別子１６７を含むことができる。商業エンティティサブシステム４００は、第１のＣＳＲの１つ以上の販売事業者識別子１６７と関連付けられ得る商業エンティティサブシステム４００と販売事業者サブシステム２００又はＰＳＰサブシステム３１０との間で鍵ペア（例えば、公開販売事業者鍵及び秘密販売事業者鍵１５７）の共有秘密化を促進することによって、ステップ６０６で共有鍵用の第１のＣＳＲに応答することができる。例えば、鍵ペアのうち第１の販売事業者鍵１５７を、販売事業者オンラインリソース用の第１のＣＳＲの販売事業者識別子の１つ、一部又はそれぞれに対して、又は他の方法によりそれに関連付けて商業エンティティサブシステム４００の表４３０に記憶することができ、鍵ペアのうち第２の販売事業者鍵１５７を、販売事業者オンラインリソー

ス用の第１のＣＳＲの販売事業者識別子の１つ、一部又はそれぞれに対して、又は他の方法によりそれに関連付けて、販売事業者サブシステム２００及び／又はＰＳＰサブシステム３１０に記憶することができる。１つ以上の販売事業者識別子を、特定の販売事業者オンラインリソース１１３と一意に関連付けられた第１の販売事業者識別子１６７（例えば、ウェブリソース販売事業者オンラインリソース１１３の場合、ＦＱＤＢ）及び／又は特定の販売事業者サブシステム２００の各販売事業者オンラインリソース１１３と関連付けられた第２の販売事業者識別子１６７などの、特定の販売事業者オンラインリソース１１３と関連付けることができる。追加的に、又は代替的に、１つ以上の販売事業者鍵を、特定の販売事業者識別子又は特定の販売事業者オンラインリソース１１３と関連付けることができる。このような販売事業者鍵及び販売事業者識別子のすべての関連付けを、ステップ６０６の１つ以上のインスタンスにおいて、商業エンティティサブシステム４００（例えば、１つ以上の表４３０内に）に記憶してもよいし、又は他の方法により、それにとってアクセス可能としてもよい。第１の販売事業者構成では、販売事業者サブシステム２００は、このような第１のＣＳＲを生成し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、また販売事業者サブシステム２００は、オンラインリソース用の第１のＣＳＲの販売事業者識別子１６７の１つ、一部又はそれぞれに対して、又は他の方法により、それと関連付けて販売事業者鍵１５７を記憶することができる。第２及び第３の販売事業者構成では、ＰＳＰサブシステム３１０又は販売事業者サブシステム２００は、このような第１のＣＳＲを生成し、ＰＳＰサブシステム３１０又は販売事業者サブシステム２００のいずれかは、このような第１のＣＳＲ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、またＰＳＰサブシステム３１０は、商業エンティティサブシステム４００から（例えば、直接又は販売事業者サブシステム２００を介して）販売事業者鍵１５７を受信し、オンラインリソース用の第１のＣＳＲの販売事業者識別子１６７の１つ、一部又はそれぞれに対して、又は他の方法により、それと関連付けて、販売事業者鍵１５７を記憶することができる。

【００８５】

更に、ステップ６０６では、オンラインリソース（例えば、ウェブサイト販売事業者オンラインリソース１１３）用の証明書の第２のＣＳＲを生成し、商業エンティティサブシステム４００に通信することができる。証明書用のこの第２のＣＳＲは、第１のＣＳＲ等の少なくとも１つの販売事業者識別子１６７（例えば、オンラインリソースのＦＱＤＮ又は、オンラインリソースのドメインとリンクされ得る任意の他の好適な販売事業者識別子）、及び／又は、オンラインリソースと関連付けられ得る任意の好適な販売事業者パートナの任意の他の好適な識別子（例えば、販売事業者サブシステム２００がオンラインリソースを妥当性検査するためにＰＳＰサブシステムを使用することができる場合、ＰＳＰ識別子）などの、オンラインリソースに関連付けられた少なくとも１つの販売事業者識別子１６７を含むことができる。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と販売事業者サブシステム２００又はＰＳＰサブシステム３１０との間で生成され、共有されている証明書１７７を促進することによって、ステップ６０６で証明書用の第２のＣＳＲに応答することができ、証明書１７７は、第２のＣＳＲの販売事業者識別子１６７の１つ、一部又は全部を含むことができ、（例えば、第２のＣＳＲの販売事業者識別子のうち１つ以上によって識別され得る）販売事業者オンラインリソース用の第１のＣＳＲの販売事業者鍵を用いて（例えば、商業エンティティサブシステム４００により）生成され得る。例えば、第２のＣＳＲのオンラインリソース用の証明書１７７を、オンラインリソース用の第２のＣＳＲの販売事業者識別子の１つ、一部、又はそれぞれに対して、又は他の方法により、それと関連付けて、商業エンティティサブシステム４００の表４３０に記憶することができ、証明書１７７も、オンラインリソース用の第２のＣＳＲの販売事業者識別子の１つ、一部、又はそれぞれに対して、又は他の方法により、それと関連付けて、販売事業者サブシステム２００及び／又はそれのＰＳＰサブシステム３１０にも記憶することができる。証明書１７７は、ＴＬＳ（ｔｒａｎｓｐｏｒｔ　ｌａｙｅｒ　ｓｅｃｕｒｉｔｙ）証明書又はＳＳＬ（ｓｅｃｕｒｅ　ｓｏｃｋｅｔｓ　ｌａｙｅｒ

）証明書などの好適なデジタル証明書とすることができる。第１の販売事業者構成及び第２の販売事業者構成の両方では、販売事業者サブシステム２００は、このような第２のＣＳＲを生成し、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、また販売事業者サブシステム２００は、オンラインリソース用の第２のＣＳＲの販売事業者識別子１６７の１つ、一部又はそれぞれに対して、又は他の方法によりそれと関連付けて証明書１７７を記憶することができる。第３の販売事業者構成では、ＰＳＰサブシステム３１０及び／又は販売事業者サブシステム２００は、そのような第２のＣＳＲを生成することができるとともに、このような第２のＣＳＲ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、またＰＳＰサブシステム３１０は、オンラインリソース用の第２のＣＳＲの販売事業者識別子１６７の１つ、一部又はそれぞれに対して、又は他の方法により、それと関連付けて証明書１７７を記憶することができ、ＰＳＰサブシステム３１０に証明書１７７を提供するこのプロセスは、販売事業者サブシステム２００に関わりなく行われてもよく、販売事業者サブシステム２００がＰＳＰサブシステム３１０とパートナシップを形成する前に行われてもよい（例えば、ＰＳＰサブシステム３１０は商業エンティティサブシステム４００の信頼されたＰＳＰとすることができ、決済がＰＳＰサブシステム３１０及びＰＳＰサブシステム３１０のドメインを介して発生しているフロントエンドＰＳＰモデルを提供するため販売事業者サブシステム２００がＰＳＰサブシステム３１０とパートナシップを形成する前に証明書１７７を備えてもよい）。販売事業者サブシステム２００は、ＰＳＰが提供したドメインと、ＰＳＰサブシステム３１０が信頼しており、そのドメインに対する証明書１７７を有する商業エンティティサブシステム４００からの要求確認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。

【００８６】

更に、ステップ６０６では、第１のＣＳＲ及び第２のＣＳＲのいずれか又は両方に対応する前、対応中又は対応した後に、販売事業者サブシステム２００による又は販売事業者パートナＰＳＰサブシステム３１０によるウェブサイトオンラインリソースのドメイン（例えばＦＱＤＮ）の所有権を検証する、又は他の方法により、（例えば、ステップ５０１に関して説明するように）商業エンティティサブシステム４００に証明することができる。鍵用の第１のＣＳＲ、証明書用の第２のＣＳＲ、及びドメイン妥当性検査のいずれか１つは、鍵用の第１のＣＳＲ、証明書用の第２のＣＳＲ、及びオンラインリソースの登録時のドメイン妥当性検査のいずれか１つの前又は後に生じてもよい。しかし、いくつかの実施形態では、証明書用の第２のＣＳＲを処理する前にドメインを検証することは、より容易かつ／又はより効率的な登録プロセスを可能とすることができる。第１の販売事業者構成及び第２の販売事業者構成の両方では、販売事業者サブシステム２００は、商業エンティティサブシステム４００に加入・登録されているウェブサイト販売事業者オンラインリソースのＦＱＤＮを共有することができ、商業エンティティサブシステム４００は、（例えば、ＪＳＯＮファイルなどの）好適なファイルを販売事業者サブシステム２００に提供することができ、販売事業者サブシステム２００は、（例えば、共有販売事業者鍵１５７で）そのファイルに署名し、そのファイルをＦＱＤＮ上にホストすることができ、そして、商業エンティティサブシステム４００は、ＦＱＤＮからその署名されたファイルにアクセスし、（例えば、共有販売事業者鍵１５７で）そのファイルの署名を削除し、アクセスされたファイルが販売事業者サブシステム２００と共有されたファイルと一致すること、及び任意の関連付けられた閾値が満たされていること（例えば、持続時間など）を確認することができる。第３の販売事業者構成では、ＰＳＰサブシステム３１０は、商業エンティティサブシステム４００に加入・登録されているウェブサイトオンラインリソースのＦＱＤＮを共有することができ、商業エンティティサブシステム４００は、（例えば、ＪＳＯＮファイルなどの）好適なファイルをＰＳＰサブシステム３１０に提供することができ、ＰＳＰサブシステム３１０は、（例えば、共有販売事業者鍵１５７で）そのファイルに署名し、そのファイルをＦＱＤＮ上にホストすることができ、そして、商業エンティティサブシステム４００は、ＦＱＤＮからその署名されたファイルにアクセスし、（例えば、共有販売事業者鍵１５７で）そのファイルの署名を削除し、アクセスされたファイルがＰ

ＳＰサブシステム３１０と共有されたファイルと一致すること、及び任意の関連付けられた閾値が満たされていること（例えば、持続時間など）を確認することができる。第３の販売事業者構成では、販売事業者サブシステム２００は、販売事業者サブシステム２００とＰＳＰサブシステム３１０との間のパートナシップを示す商業エンティティサブシステム４００にデータを通信するように機能することができるので、商業エンティティサブシステム４００は、ＰＳＰサブシステム３１０の妥当性検査を販売事業者サブシステム２００に確認し、プロセス６００の他の部分の間における任意の好適な使用のために（例えば、表４３０で）販売事業者サブシステム２００の販売事業者識別子１６７とＰＳＰサブシステム３１０のＦＱＤＮ及び／又は証明書１７７との間の関連付けを記憶するように機能することができる。いくつかの実施形態では、第２及び第３の販売事業者構成のＰＳＰサブシステム３１０に提供される販売事業者鍵（単数又は複数）１５７は、いずれかのパートナ販売事業者サブシステム２００に対してデータを解読するためにＰＳＰサブシステム３１０によってグローバルに使用されてもよい。代替的に、第２及び第３の販売事業者構成のＰＳＰサブシステム３１０に提供される販売事業者鍵（単数又は複数）１５７は、特定のパートナ販売事業者サブシステム２００に特有とすることができ、それによって、販売事業者サブシステム２００は、（例えば、鍵用の第１のＣＳＲで）商業エンティティサブシステム４００と通信することができ、そして、ＰＳＰサブシステム３１０がその販売事業者サブシステム２００に特有のそのような販売事業者鍵（単数又は複数）１５７を（例えば、商業エンティティサブシステム４００から直接、又は販売事業者サブシステム２００から）受信できるようにすることができ、このような販売事業者鍵（単数又は複数）１５７を、商業エンティティサブシステム４００（例えば、表４３０で）及び／又はＰＳＰサブシステム３１０において記憶する、又は他の方法により、販売事業者サブシステム２００の好適な販売事業者識別子１６７と関連付けることができる。これにより、ＰＳＰサブシステム３１０の他の販売事業者特有の鍵を他の販売事業者サブシステムに対して使用できるようにしながら、特定の販売事業者サブシステムがもはや商業エンティティサブシステム４００により信頼されない場合、販売事業者特有の販売事業者鍵１５７を商業エンティティサブシステム４００で無効化することができる。いくつかの実施形態では、（例えば、ＰＳＰサブシステム３１０が商業エンティティサブシステム４００を販売事業者のプロキシとして販売事業者に実装されるように）販売事業者サブシステム２００が直接そのプロセスに関わることなく、ＰＳＰサブシステム３１０が商業エンティティサブシステム４００と、ＰＳＰサブシステム３１０の特定のパートナ販売事業者サブシステム２００に特有であり得る任意の販売事業者鍵１５７及び証明書１７７を共有することを可能とするため、ＰＳＰサブシステム３１０が直接商業エンティティサブシステム４００とインタフェースできるようにするための１つ以上のＡＰＩを提供することができる。証明書１７７はまた、ＰＳＰサブシステム３１０にとってグローバルであってもよいし、又は特定のパートナ販売事業者サブシステム２００に特有であってもよい。

【００８７】

したがって、ステップ６０６及び／又はステップ５０１は、商業エンティティサブシステム４００によって検証されるオンラインリソースのドメインだけでなく、商業エンティティサブシステム４００でオンラインリソースを加入・登録させるために、商業エンティティサブシステム４００ならびに、販売事業者サブシステム２００及び／又は販売事業者パートナＰＳＰサブシステム３１０で販売事業者鍵１５７及び証明書１７７の両方に対して記憶されるオンラインリソースのドメインと関連付けられるか、又は同じである販売事業者識別子１６７も含むことができる。これにより、オンラインリソースの検証されたＦＱＤＮ及び／又は任意の他の好適な販売事業者識別子１６７を、販売事業者鍵１５７及び証明書１７７に対して、（例えば、プロセス６００のステップ６１４、６１６及び／又はプロセス５００のステップ５０６における）妥当性検査セッション中のオンラインリソースのＦＱＤＮの妥当性検査を可能とするためだけでなく、（例えば、プロセス６００のステップ６３１及び／又はプロセス５００のステップ５１８における）商業エンティティサブシステム４００によるセキュアなデータの暗号化、及び、（例えば、プロセス６００の

ステップ６３６又は６３８及び／又はプロセス５００のステップ５２２における）販売事業者サブシステム２００又はＰＳＰサブシステム３１０による当該暗号化されたセキュアなデータのカウンターパート復号を可能とするためにも、商業エンティティサブシステム４００及び販売事業者サブシステム２００及び／又はＰＳＰサブシステム３１０（例えば、プロセス６００のステップ６０６及び／又はプロセス５００のステップ５０１における）において記憶することができる。例えば、第１の販売事業者構成及び第２の販売事業者構成の両方では、販売事業者オンラインリソース１１３の妥当性検査セッションを開始するため、販売事業者サブシステム２００がステップ６１２で任意の好適な販売事業者オンラインリソース妥当性検査セッション開始データ６６２をデバイス１００から受信することに応じて、このような妥当性検査セッション開始データ６６２がオンラインリソースの識別子（例えば、デバイス１００によりアクセスされる販売事業者オンラインリソースのＦＱＤＮ）を含むことができる場合、販売事業者サブシステム２００は、実行される特定のセキュアなデータトランザクション（例えば、ステップ６１０及び／又はステップ６１２での金融決済トランザクション）のための販売事業者オンラインリソースを妥当性検査するため、販売事業者サブシステム２００がステップ６０６で受信し、妥当性検査セッション開始データ６６２のＦＱＤＮに対して記憶された証明書１７７を含む任意の好適なチャレンジ要求データ６６４を、ステップ６１４で商業エンティティサブシステム４００に通信するように機能することができる。代替的に、第３の販売事業者構成では、ＰＳＰオンラインリソース１１３の妥当性検査セッションを開始するため、ＰＳＰサブシステム３１０がステップ６１２で任意の好適なオンラインリソース妥当性検査セッション開始データ６６２をデバイス１００から受信することに応じて、このような妥当性検査セッション開始データ６６２がオンラインリソースの識別子（例えば、デバイス１００によりアクセスされるＰＳＰオンラインリソースのＦＱＤＮ）を含むことができる場合、ＰＳＰサブシステム３１０は、実行される特定のセキュアなデータトランザクション（例えば、ステップ６１０及び／又はステップ６１２での金融決済トランザクション）のためのＰＳＰオンラインリソースを妥当性検査するため、ＰＳＰサブシステム３１０がステップ６０６で受信し、妥当性検査セッション開始データ６６２のＦＱＤＮに対して記憶された証明書１７７を含む任意の好適なチャレンジ要求データ６６４を、ステップ６１４で商業エンティティサブシステム４００に通信するように機能することができる。ステップ６１４で販売事業者サブシステム２００又はＰＳＰサブシステム３１０から商業エンティティサブシステム４００に通信された、このようなチャレンジ要求データ６６４は、商業エンティティサブシステム４００に対してオンラインリソースの妥当性を証明しようとするための任意の好適なデータを含むことができ、これには、限定されることなく、証明書１７７が含まれ、この証明書は、ＦＱＤＮ及び／又は、ステップ６０６で商業エンティティサブシステム４００により生成されるオンラインリソースと関連付けられた任意の他の好適な識別子、及び、任意の他の好適なデータ（例えば、デバイス１００を識別するデータ及び／又は、実行される特定のセキュアなデータトランザクションを識別するデータ（例えば、本明細書では、潜在的トランザクション識別情報と呼ばれる場合もあるステップ６１０及び／又はステップ６１２で識別される金融決済トランザクションであって、それは、追加のセキュリティ層（単数又は複数）を現在のデータトランザクションプロセスに提供するための、及び／又は将来のデータトランザクションのための追加のセキュリティ（例えば、不正検出）サービスを提供するためのプロセス６００の任意の好適な部分の間に使用され得る））を含むことができる。

【００８８】

プロセス６００のステップ６１６では、商業エンティティサブシステム４００がステップ６１４で証明書１７７を有する任意の好適なチャレンジ要求データ６６４を販売事業者サブシステム２００又はＰＳＰサブシステム３１０から受信することに応じて、商業エンティティサブシステム４００は、チャレンジ要求の販売事業者識別子１６７により識別されるオンラインリソース１１３を妥当性検査するように機能することができる。例えば、第１の販売事業者構成及び第２の販売事業者構成の両方では、商業エンティティサブシス

テム４００がステップ６１４で証明書１７７を有する任意の好適なチャレンジ要求データ６６４を販売事業者サブシステム２００から受信することに応じて、商業エンティティサブシステム４００は、受信したチャレンジ要求データ６６４の証明書１７７を検証及びチェックし、その信頼が依然として妥当であり、任意の好適なプロセス（単数又は複数）を通じて満了していないことを確実とするように機能することができる（例えば、証明書１７７は、データ６６４中で商業エンティティサブシステム４００により受信され得、そして、商業エンティティサブシステム４００は、その証明書１７７が商業エンティティサブシステム４００に知られている（例えば、表４３０に記憶されている）か否か、及びその証明書１７７が依然として信頼されるものか、及び／又はその証明書１７７が満了していないかを判定するように機能することができる）。次に、受信した証明書１７７が検証されると、受信した証明書１７７からＦＱＤＮ及び／又は別の販売事業者識別子１６７を抽出し、商業エンティティサブシステム４００の表４３０に記憶されているＦＱＤＮ及び証明書１７７の関連付けと照合して、受信した証明書１７７のＦＱＤＮが登録されることを確実とすることができる。例えば、ステップ６１６では、商業エンティティサブシステム４００は受信したチャレンジ要求データ６６４の販売事業者識別子１６７によって識別されたオンラインリソース１１３が商業エンティティサブシステム４００において妥当でかつ登録されたオンラインリソースであることを確認しようとするように機能することができ、そのことは、（例えば、（例えば、ステップ６０６で）販売事業者識別子１６７が商業エンティティサブシステム４００に登録されていること、及びそのような登録が依然として妥当であること（例えば、商業エンティティサブシステム４００が販売事業者識別子１６７を表４３０から除去していないか、又は疑わしいもの又は他の方法により、もはや信頼されていないものとして、表４３０で販売事業者識別子１６７にフラグを立てていないこと）を判定するために）表４３０のその販売事業者識別子１６７を識別することによって確認することができる。同様に、第３の販売事業者構成では、商業エンティティサブシステム４００がステップ６１４で証明書１７７を有する任意の好適なチャレンジ要求データ６６４をＰＳＰサブシステム３１０から受信したことに応じて、商業エンティティサブシステム４００は、受信したチャレンジ要求データ６６４の証明書１７７を検証及びチェックし、その信頼が依然として妥当であり、満了していないことを確実とするように機能することができ、受信した証明書１７７が検証されると、ＦＱＤＮ及び別の販売事業者識別子１６７及びＰＳＰ識別子を、受信した証明書１７７から抽出できるので、そして、識別されたＰＳＰが識別された販売事業者に代わってトランザクションを行うように許可されているか、ならびに、抽出されたＦＱＤＮがステップ６１４の要求を完全に妥当性検査するために商業エンティティサブシステム４００における他の抽出された販売事業者識別子に登録されているかを判定することができる。販売事業者識別子１６７は、特定の販売事業者サブシステム２００のグローバル販売事業者識別子とすることができる（例えば、単一の販売事業者識別子１６７を、ネイティブアプリの販売事業者オンラインリソース及び販売事業者サブシステム２００のウェブサイト販売事業者オンラインリソースを識別するのに使用することができ、及び／又は単一のＦＱＤＮを、複数の販売事業者サブシステムと関連付けることができる（例えば、ＰＳＰのＦＱＤＮは複数の販売事業者サブシステムにより使用され得る））。ＦＱＤＮ及び、特定の販売事業者サブシステム２００及び特定のＰＳＰサブシステム３１０の一意の識別子などの少なくとも１つの他の識別子はともに、証明書１７７から抽出され、ステップ６０６で行われ得たように、これらの２つが商業エンティティサブシステム４００において（例えば、表４３０で）既に互いに関連付けられていることが確認できる。商業エンティティサブシステム４００による受信したチャレンジ要求データ６６４の好適な妥当性検査後（例えば、受信した証明書１７７の妥当性検査後及び／又は受信した証明書１７７のＦＱＤＮの妥当性検査後及び識別されたＰＳＰと受信した証明書１７７の識別された販売事業者との間の許可された関係を確認後）、商業エンティティサブシステム４００はまた、ステップ６１６で、好適な妥当性検査データを生成し、受信したチャレンジ要求データ６６４の好適な識別子データに対してその妥当性検査データを記憶するように機能することができる。例えば、ステップ６１６での受

信したチャレンジ要求データ６６４の好適な妥当性検査後、商業エンティティサブシステム４００はまた、ステップ６１６で、好適な妥当性検査データ（例えば、（例えば、上述のステップ６２２の妥当性検査データと同様の）エントロピーを介した好適なランダムデータ及び／又は好適な暗号ナンス）及び妥当性検査セッション識別子（例えば、好適な英数字列又は（例えば、ステップ６１２でデバイス１００によって、又はステップ６１４で販売事業者サブシステム２００若しくはＰＳＰサブシステム３１０によって、又はステップ６１６で商業エンティティサブシステム４００によって生成され得る）商業エンティティサブシステム４００に対して現在のオンラインリソースを一意に識別し得る他の好適な識別子）を生成するように機能することができ、そして、商業エンティティサブシステム４００は、ステップ６１６で、商業エンティティサブシステム４００にとってアクセス可能な好適なデータ構造で（例えば、表４３０で、又は別の方法で）その妥当性検査データを、妥当性検査セッション識別子及びチャレンジ要求データ６６４の販売事業者識別子の一方又は両方に対して記憶することができる。したがって、特定の実施形態では、妥当性検査セッション識別子が、少なくとも特定の販売事業者識別子に対して、商業エンティティサブシステム４００により実行されている特定の妥当性検査プロセスに対して一意であることを商業エンティティサブシステム４００が確実とすることができるように、妥当性検査セッション識別子は商業エンティティサブシステム４００により生成されてもよい。しかし、妥当性検査セッション識別子が販売事業者サブシステム２００又はＰＳＰサブシステム３１０によって生成されると、商業エンティティサブシステム４００は、そのような妥当性検査セッション識別子が、その妥当性検査セッション識別子をその特定の妥当性検査セッションに使用できるようにする前の妥当性検査セッションの販売事業者識別子に一意であることを確認することができる。そうでなければ、商業エンティティサブシステム４００は、妥当性検査セッション識別子を拒絶し、新しい識別子が販売事業者サブシステム２００又はＰＳＰサブシステム３１０によって生成されることを要求することができる。そのような妥当性検査データと妥当性検査セッションの識別子データ（例えば、妥当性検査セッション識別子及び／又はチャレンジ要求データ６６４の販売事業者識別子）とのこのような記憶されたリンク又は関連付けは、（例えば、ステップ６３０で）実行されるセキュアなデータトランザクションを更にセキュアとするために、後に商業エンティティサブシステム４００によって使用され得る。また、いくつかの実施形態では、チャレンジ要求データ６６４の潜在的トランザクション識別情報のいずれか又はすべてが、ステップ６１６で妥当性検査データ及び識別子データに対して記憶され、又は他の方法によりそれらと関連付けられてもよい。

【００８９】

第１、第２及び第３の販売事業者構成のうちいずれか１つの構成では、このようなステップ６１６の後、オンラインリソースをステップ６１４及び６１６の単一のセットで妥当性検査することができるので、ステップ６１８、６２０及び６２２をスキップすることができ、そして、プロセス６００は、商業エンティティサブシステム４００が好適な妥当性検査レスポンスデータ６７４を生成かつ通信するように機能し得るステップ６２４を含むことができる。例えば、妥当性検査レスポンスデータ６７４は、限定されることなく、妥当性検査セッション識別子（例えば、ステップ６１６で生成された妥当性検査セッション識別子）、１つ以上の販売事業者識別子（例えば、チャレンジ要求データ６６４（例えば、ＦＱＤＮ、他の販売事業者識別子、ＰＳＰ識別子など）のいずれかの、若しくはそれぞれの販売事業者識別子、及び／又は、他の方法により、商業エンティティサブシステム４００で（例えば、表４３０で）妥当性検査セッション中に妥当性検査されているオンラインリソースと関連付けられ得るいずれかの、若しくはそれぞれの販売事業者識別子）、チャレンジ要求データ６６４の証明書１７７、又は同様のものを含み得る他の好適なデータとともにステップ６１６の妥当性検査データを含み得るセッションオブジェクトとすることができる。いくつかの実施形態において、図６に示すように、このような妥当性検査レスポンスデータ６７４を、商業エンティティサブシステム４００から直接電子デバイス１００に（例えば、任意の好適な通信プロトコルを用いた通信経路６５を介して）通信する

ことができ、商業エンティティサブシステム４００が妥当性検査レスポンスデータ６７４を適正な電子デバイス１００に通信することができるように、電子デバイス１００を識別するデータ（例えば、デバイス識別子１１９）は、妥当性検査セッション開始データ６６２及び／又はチャレンジ要求データ６６４などと関連付けられてもよいし、又は他の方法により、それに含まれてもよい。代替的に、いくつかの実施形態（図示せず）では、妥当性検査レスポンスデータ６７４を、（例えば、第１又は第２の販売事業者構成の）販売事業者サブシステム２００を介して、及び／又は、（例えば、第３の販売事業者構成の）ＰＳＰサブシステム３１０を介して商業エンティティサブシステム４００から電子デバイス１００に通信することができることによって、販売事業者サブシステム２００及び／又はＰＳＰサブシステム３１０は妥当性検査レスポンスデータ６７４を商業エンティティサブシステム４００から受信し、そして、妥当性検査レスポンスデータ６７４の少なくとも一部分を電子デバイス１００に渡すことができる。妥当性検査レスポンスデータ６７４のセッションオブジェクトは、（例えば、ＨＴＴＰヘッダ内で、又は別の方法で）商業エンティティサブシステム４００により、電子デバイス１００がアクセス可能であり得る商業エンティティサブシステム４００に関連付けられたアクセス鍵（例えば、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／若しくはＩＳＤ鍵１５６ｋ又は、デバイスアプリケーション（例えば、カード管理アプリケーション１０３ｂ）に知られ得る任意の鍵）で署名されることがあるので、デバイス１００は、署名された妥当性検査データを受信するとすぐに署名を妥当性検査し、電子デバイス１００により信頼され得ない別のエンティティサブシステムではなく、商業エンティティサブシステム４００が妥当性検査レスポンスデータ６７４を生成したことを確認する、及び／又はそのようなアクセス鍵へのアクセスを有しない別のエンティティ（例えば、販売事業者サブシステム２００及び／又はＰＳＰサブシステム３１０）が、その他のエンティティがそのような署名された妥当性検査データを受信し、それをデバイス１００に転送することを依然として可能にしながら、署名された妥当性検査データを使用するのを防止することができる。

【００９０】

第１、第２及び第３の販売事業者構成のいずれか１つの構成では、デバイス１００のユーザが、ステップ６１０で受信した潜在的トランザクションデータ６６０（例えば、決済要求データ）に応じて、潜在的トランザクションに資金供給するのに使用される特定の決済クレデンシャルを選択又は確認する意思と能力があり、また、妥当性検査レスポンスデータ６７４がステップ６２４で電子デバイス１００によって受信されている（例えば、ステップ６１２～ステップ６１６の販売事業者オンラインリソース妥当性検査セッションの成功を示し得るデータ）場合、プロセス６００は、ステップ６２５に進むことができ、この場合、プロセス６００は、セッション識別子の一致が（例えば、上述のステップ６２５で）識別された後、（例えば、図３Ｃの認証プロンプト３１５のユーザの選択により）潜在的トランザクションデータ６６０に基づいて特定の販売事業者、製品、価格又は配送先に対して潜在的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むことができる。いくつかの実施形態では、セッション識別子整合性がこのような意図及び認証に先立って検証されることを含むステップ６２５に加えて、又は代替的に、ステップ６２５は、ドメイン整合性がこのような意図及び認証に先立って検証されることを含むことができる。例えば、ステップ６２４でデバイス１００が妥当性検査レスポンスデータ６７４を受信したことに応答して、デバイス１００は、そのような妥当性検査レスポンスデータ６７４のドメイン識別子（例えば、妥当性検査レスポンスデータ６７４のＦＱＤＮ）を現在デバイス１００のオンラインリソースのアドレスバー内にあるドメイン識別子と比較するように機能することができる。例えば、デバイス１００のウェブキット（例えば、オンラインリソースアプリケーション１１３）は、妥当性検査レスポンスデータ６７４を受信し、その妥当性検査レスポンスデータ６７４を、そのウェブキットが現在ターゲットとしているドメイン識別子（例えば、ＦＱＤＮ）とともにデバイス１００のパスキット（例えば、カード管理アプリ

ケーション１０３ｂ）に中継することができる。そして、パスキットは、（もしあれば）受信した妥当性検査レスポンスデータ６７４の署名を（例えば、デバイス１００のアクセス鍵を用いて）妥当性検査し、ドメイン識別子（例えば、ＦＱＤＮ）を妥当性検査レスポンスデータ６７４から抽出し、そして、その抽出されたドメイン識別子をウェブキット（例えば、デバイス１００のウェブキットによって現在ホストされているＪａｖａ ｓｃｒｉｐｔ(登録商標)のＦＱＤＮ（例えば、第１及び第２の販売事業者構成の販売事業者オンラインリソースのＦＱＤＮ及び第３の販売事業者構成のＰＳＰオンラインリソースのＦＱＤＮ））によって識別され、かつ提供されたドメイン識別子と比較することができ、それにより、（例えば、リプレイ攻撃を回避するため）デバイス１００がレスポンスデータ６７４がデバイス１００により現在アクセスされている同一のオンラインリソースに関連付けられていることを確認するのを可能とすることができる。ステップ６２５で好適なセッション識別子整合性及び／又は好適なドメイン識別子整合性が検証された後、ステップ６２５で特定の決済クレデンシャルのための意図及び認証を受信することができる。そして、第１、第２及び第３の販売事業者構成のそれぞれの構成について、ステップ６２６～６２９が上述のように発生することができ、妥当性検査レスポンスデータ６７４のいずれかの又はすべての好適な部分（例えば、セッション識別子、妥当性検査データ（例えば、ナンス）、ＦＱＤＮ及び／又は任意の他の好適な販売事業者識別子又はＰＳＰ識別子、及び／又は他のデータ（例えば、証明書１７７の少なくとも一部分））は、デバイストランザクションデータ６７８として、セキュアデバイスデータ６７７及びトランザクションデータ６６０とともに含まれ得る。

【００９１】

第１、第２及び第３の販売事業者構成のうちいずれか１つの構成では、商業エンティティサブシステム４００は、ステップ６３０で、デバイス１００がデバイストランザクションデータ６７８の中に含み得た妥当性検査レスポンスデータ６７４の妥当性検査データを妥当性検査するように機能することができる。例えば、このようなデバイストランザクションデータ６７８の受信に応じて、商業エンティティサブシステム４００は、そのデバイストランザクションデータ６７８から妥当性検査レスポンスデータ６７４の少なくとも一部分又は全部を識別し、かつ受信したデバイストランザクションデータ６７８の妥当性検査データが商業エンティティサブシステム４００に現在記憶されていることを確認する、又は、より具体的には、一部の実施形態では、受信したデバイストランザクションデータ６７８の妥当性検査データが、（例えば、プロセス５００のステップ５１６と同様に）ステップ６３０で（例えば、表４３０内の）受信したデバイストランザクションデータ６７８の妥当性検査セッション識別子に対して、及び／又は受信したデバイストランザクションデータ６７８の販売事業者識別子（例えば、ＦＱＤＮ）に対して商業エンティティサブシステム４００に現在記憶されていることを確認するように機能することができる。妥当性検査データと妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間のこのような記憶されたリンクを、リンクが自動的に削除される前の限られた時間量の間だけしか維持できないので、電子デバイス１００は、妥当性検査された販売事業者オンラインリソースとの特定のセキュアなデータトランザクションを実行するため、そのデバイストランザクションデータ６７８のセキュアデバイスデータ６７７を商業エンティティサブシステム４００によりセキュアとできるようにするために、ステップ６２４で妥当性検査レスポンスデータ６７４を受信し、そして、ステップ６２８でデバイストランザクションデータ６７８を、商業エンティティサブシステム４００に送信しなければならない特定の持続時間を限定することがある（例えば、商業エンティティサブシステム４００は、特定時間後に商業エンティティサブシステム４００におけるチャレンジデータと妥当性検査セッション識別子及び／又は販売事業者識別子との間のこのような関連付けを除去する（例えば、リンクが作成された後１０分以内に表４３０からのリンクを除去する）ように機能することができ、それにより、トランザクションのセキュリティを向上させることができる）。追加的に、又は代替的に、妥当性検査データと、妥当性検査セッション識別子及び販売事業者識別子の一方又は両方との間の記憶されたリンクも、ステップ６２２で、ス

テップ６１４で販売事業者サブシステム２００又はＰＳＰサブシステム３１０により商業エンティティサブシステム４００にとって利用できるようにした、デバイス１００と販売事業者サブシステム２００又はＰＳＰサブシステム３１０との間で共有される特定のタイプのセキュアなデータ（例えば、財務トランザクション用の通貨及び金額ならびに決済タイプ）の識別などの、好適な特定の潜在的トランザクション識別情報と（例えば、チャレンジ要求データ６６４の一部分として）関連付けることができ、また、同様の特定の潜在的トランザクション識別情報も、ステップ６２８のデバイストランザクションデータ６７８の一部分として電子デバイス１００により商業エンティティサブシステム４００にとって利用できるようにすることができるので、ステップ６３０はまた、商業エンティティサブシステム４００が（例えば、ステップ６１６で表４３０に記憶されているように）ステップ６１４で受信した妥当性検査データに対して現在記憶されている特定の潜在的トランザクション識別情報がステップ６２８で受信された特定の潜在的トランザクション識別情報少なくとも同様であることを確認することも含むことができる。

【００９２】

次に、ステップ６３１では、プロセス６００は、商業エンティティサブシステム４００が販売事業者サブシステム２００又はＰＳＰサブシステム３１０（例えば、妥当性検査セッションのオンラインリソースのステップ６０６で鍵用の第１のＣＳＲを生成し得たサブシステム）に関連付けられた販売事業者鍵（例えば、販売事業者鍵１５７）を識別することを含むことができる。すなわち、ステップ６２９で好適なアクセス情報を用いてデバイストランザクションデータ６７８の少なくとも一部分を解読した後（例えば、セキュアデバイスデータ６７７を解読し、デバイス決済クレデンシャルデータ６７６及びセキュアデバイスデータ６７７内に暗号化され得た任意の他の情報を達成した後）、商業エンティティサブシステム４００は、そして、ステップ６３１で、デバイストランザクションデータ６７８の少なくとも一部分（例えば、デバイス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）を、（例えば、第１の販売事業者構成のための）販売事業者サブシステム２００の好適な販売事業者鍵１５７で、又は（例えば、第２及び第３の販売事業者構成のための）ＰＳＰサブシステム３１０の好適な販売事業者鍵１５７で、暗号化された販売事業者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、この好適な販売事業者鍵１５７は、データ６７８内に含まれ得る妥当性検査データの任意の好適な識別子データを用いて、かつ（例えば、ステップ６０６の間に規定され得るように、テーブル４３０内の）その識別子データに関連付けられた事前に記憶された関連付けを用いて、商業エンティティサブシステム４００により識別され得る。例えば、暗号化された販売事業者クレデンシャルデータ６８１は、デバイス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デバイス決済クレデンシャルデータ６７６、ならびに、デバイストランザクションデータ６７８及び／又は潜在的トランザクションデータ６６０からの、又はそれに基づいた購入額データ又は他の好適なトランザクションデータなどの好適なトランザクションデータを含むことができる。暗号化された販売事業者クレデンシャルデータ６８１は、販売事業者サブシステム２００又はＰＳＰサブシステム３１０により受信されると、そのサブシステムがこのような暗号化された販売事業者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を確立できるように、及び／又はそのサブシステムがこのような暗号化された販売事業者クレデンシャルデータ６８１が署名された後修正されていないことを確実とすることを可能とすることができるように商業エンティティサブシステム４００により署名され得る。このような暗号化された販売事業者クレデンシャルデータ６８１は、ステップ６３１で生成され、そして、ステップ６３２で、セキュアなトランザクションデータ６８２として他の好適なデータとともにデバイス１００に（例えば、図１Ａの経路６５を介して商業エンティティサブシステム４００のサーバ４１０からデバイス１００の通信構成要素１０６に）送信されてもよい。

【００９３】

ステップ６３１及びステップ６３２は、図１Ａのセキュアなトランザクションデータ６８２の一部として商業エンティティサブシステム４００から送信されたクレデンシャルデ

ータ（例えば、暗号化された販売事業者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）が、セキュアエレメント１４５以外のデバイス１００の一部分により解読できないように暗号化されてもよいことを確実とするように機能することができる。すなわち、セキュアな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、暗号化された販売事業者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）を、いくつかの実施形態では、セキュアエレメント１４５を含む、デバイス１００のいかなる部分にも露出されていない、又は他の方法により、それによりアクセスできない販売事業者鍵（例えば、販売事業者鍵１５７）で暗号化することができる。また、セキュアな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、暗号化された販売事業者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）を、セキュアエレメント１４５の外部のデバイス１００のいかなる部分にも露出していない、又はアクセスできないクレデンシャル鍵１５５ａ’で暗号化することができる。

【００９４】

第１及び第２の販売事業者構成では、セキュアなトランザクションデータ６８２は、ステップ６３４で、セキュアなトランザクションデータ６８４として、デバイス１００によって販売事業者サブシステム２００に（例えば、通信経路１５を介して、又は非接触近接型通信５として）転送されてもよいし、代替的に、販売事業者クレデンシャルデータ６８１は、デバイス１００を介して通信されずに商業エンティティサブシステム４００から販売事業者サブシステム２００に通信されてもよい（図示せず）。潜在的トランザクションデータ６６０の１つ、一部又は全部を、デバイス１００及び／又は商業エンティティサブシステム４００を通して、セキュアなトランザクションデータ６８２及び／又はセキュアなトランザクションデータ６８４に搬送することができるので、潜在的トランザクションの特定の識別子は、プロセス６００中にエンティティのそれぞれによって識別され得る。

【００９５】

決済クレデンシャルデータ６７５／６７６を含む販売事業者クレデンシャルデータ６８１が販売事業者サブシステム２００によって（例えば、ステップ６３４でセキュアなトランザクションデータ６８４として）受信されると、プロセス６００はまた、販売事業者サブシステム２００が決済データ６８６を生成し送信するように構成され得るステップ６３６も含むことができる。第１の販売事業者構成では、例えば、ステップ６３６では、販売事業者サブシステム２００は、その既知の販売事業者鍵１５７を活用して、セキュアなトランザクションデータ６８４の販売事業者クレデンシャルデータ６８１を少なくとも部分的に解読することができるので、決済データ６８６は、金融機関サブシステム３５０にとって利用可能ではない鍵ではなく、そのクレデンシャル鍵１５５ａ’（例えば、データ６７６）で暗号化されたクレデンシャルＳＳＤ１５４ａのセキュアな決済クレデンシャルデータを含むことができ、そして、そのようなデータ６８６を、販売事業者サブシステム２００によって任意の好適なサブシステム（例えば、取得銀行サブシステム３００及び／又はＰＳＰサブシステム３１０）に通信することができる。代替的に、第２の販売事業者構成では、例えば、ステップ６３６で、販売事業者サブシステム２００は、決済データ６８６として、セキュアなトランザクションデータ６８４の再暗号化された販売事業者クレデンシャルデータ６８１をＰＳＰサブシステム３１０に転送することができ、そして、ＰＳＰサブシステム３１０は、その既知の販売事業者鍵１５７を活用して、少なくとも部分的に、決済データ６８６のその再暗号化された販売事業者クレデンシャルデータ６８１を解読することができる。代替的に、第３の販売事業者構成では、セキュアなトランザクションデータ６８２はデバイス１００によってＰＳＰサブシステム３１０に（例えば、デバイス１００によって現在アクセスされ得るＰＳＰオンラインリソースを使用して）転送されてもよく、そして、ＰＳＰサブシステム３１０はその既知の販売事業者鍵１５７を活用して、少なくとも部分的に、その転送されたセキュアなトランザクションデータの再暗号化された販売事業者クレデンシャルデータ６８１を解読することができる。プロセス６００の残りの部分は、販売事業者サブシステム２００及びＰＳＰサブシステム３１０のうち適切なサブシステム（単数又は複数）が適切な販売事業者構成に従ってデータをデバイス１０

０と通信しながら、ステップ６３８～ステップ６４４に関して上記したように進行することができる。

【００９６】

図７の説明

図７は、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介した処理サブシステムに通信可能に結合された電子デバイスとの間のセキュアなトランザクションを行うために、管理エンティティサブシステムを使用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では、管理エンティティサブシステムは、オンラインリソースに対する妥当性検査要求を受信することができ、妥当性検査要求は、妥当性検査要求データ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、ステップ６１４でチャレンジ要求データ６６４を、及び／又はプロセス６００のステップ６２０でチャレンジレスポンスデータ６７０を受信することができる）。プロセス７００のステップ７０４では、管理エンティティサブシステムは、妥当性検査要求データ及び登録データを用いてオンラインリソースを妥当性検査することができ、登録データは、妥当性検査要求を受信する前に管理エンティティサブシステムにとって最初に利用できるようにすることができる（例えば、商業エンティティサブシステム４００は、プロセス６００のステップ６１６で、チャレンジ要求データ６６４及びステップ６０６からの登録データを用いて、ならびに／又はプロセス６００のステップ６２２で、チャレンジレスポンスデータ６７０及びステップ６０６からの登録データを用いて、オンラインリソース１１３を妥当性検査することができる）。プロセス７００のステップ７０６では、管理エンティティサブシステムは、妥当性検査レスポンスデータを、妥当性検査要求データの少なくとも一部分と関連付けることができる（例えば、商業エンティティサブシステム４００は、プロセス６００のステップ６１６及び／又はステップ６２２で識別子データに対して、妥当性検査データを関連付けることができる）。プロセス７００のステップ７０８では、管理エンティティサブシステムは、妥当性検査レスポンスデータを電子デバイスに通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はプロセス６００のステップ６２４で妥当性検査レスポンスデータ６７４の一部分としての妥当性検査データを電子デバイス１００に通信することができる）。プロセス７００のステップ７１０では、管理エンティティサブシステムは、電子デバイスからデバイス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、商業エンティティサブシステム４００は、プロセス６００のステップ６２８で電子デバイス１００からデバイストランザクションデータ６７８を受信することができる）。プロセス７００のステップ７１２では、管理エンティティサブシステムは、妥当性検査レスポンスデータを用いてデバイストランザクションデータを妥当性検査することができる（例えば、商業エンティティサブシステム４００は、妥当性検査レスポンスデータ６７４を用いて、プロセス６００のステップ６３０でデバイストランザクションデータ６７８の妥当性検査データを妥当性検査することができる）。プロセス７００のステップ７１４では、デバイストランザクションデータが妥当性検査された後、管理エンティティサブシステムは、処理サブシステムに使用されるためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することができる（例えば、商業エンティティサブシステム４００は、プロセス６００のステップ６３１でデバイストランザクションデータ６７８に基づいて販売事業者クレデンシャルデータ６８１を生成することができる）。

【００９７】

図７のプロセス７００で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。

【００９８】

図８の説明

図８は、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介して処理サブシステムに通信可能に結合された電子デバイスとの間で、セキュアなトランザ

クションを可能とするために、管理エンティティサブシステムを使用するための例示的なプロセス８００のフローチャートである。プロセス８００のステップ８０２では、管理エンティティサブシステムは、管理エンティティサブシステムと処理サブシステムとの間で処理する共有秘密を確立することによってオンラインリソースを登録することができる（例えば、商業エンティティサブシステム４００は、プロセス６００のステップ６０６で販売事業者サブシステム２００と共有秘密を確立することによってオンラインリソース１１３を登録することができる）。プロセス８００のステップ８０４では、管理エンティティサブシステムはオンラインリソースに対する妥当性検査要求を受信することができ、妥当性検査要求はオンラインリソースを示す処理識別子を含むことができ、妥当性検査要求は、オンラインリソースを介した電子デバイスと処理サブシステムとの間の潜在的トランザクションに一意である妥当性検査セッション識別子を更に含むことができる（例えば、商業エンティティサブシステム４００は、ステップ６１４で、販売事業者識別子及びセッション識別子を有するチャレンジ要求データ６６４を、ならびに／又はプロセス６００のステップ６２０で、販売事業者識別子及びセッション識別子を有するチャレンジレスポンスデータ６７０を受信することができる）。プロセス８００のステップ８０６では、管理エンティティサブシステムは、妥当性検査セッション識別子及び処理共有秘密を用いて、処理識別子が示すオンラインリソースを妥当性検査することができる（例えば、商業エンティティサブシステム４００は、プロセス６００のステップ６１６でチャレンジ要求データ６６４及びステップ６０６からの登録データを用いて、及び／又は、プロセス６００のステップ６２２で、チャレンジレスポンスデータ６７０及びステップ６０６から登録データを用いて、オンラインリソース１１３を妥当性検査することができる）。

【００９９】

図８のプロセス８００で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。

【０１００】

図９の説明

図９は、処理サブシステムと、電子デバイス上で実行されるオンラインリソースを介した処理サブシステムに通信可能に結合された電子デバイスとの間のセキュアなトランザクションを行うために、管理エンティティサブシステムを使用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では、管理エンティティサブシステムはオンラインリソースに対する妥当性検査要求を受信することができ、妥当性検査要求は妥当性検査要求データを含むことができ、妥当性検査要求データは、オンラインリソースを介した電子装置と処理サブシステムとの間の潜在的トランザクションを示す潜在的トランザクション識別情報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、ステップ６１４で、チャレンジ要求データ６６４を、及びに／又はプロセス６００のステップ６２０で、チャレンジレスポンスデータ６７０を受信することができる）。プロセス９００のステップ９０４では、管理エンティティサブシステムは、妥当性検査要求データの少なくとも一部分を用いて、オンラインリソースを妥当性検査することができる（例えば、商業エンティティサブシステム４００は、プロセス６００のステップ６１６でチャレンジ要求データ６６４を用いて、及び／又は、プロセス６００のステップ６２２で、チャレンジレスポンスデータ６７０を用いて、オンラインリソース１１３を妥当性検査することができる）。プロセス９００のステップ９０６では、管理エンティティサブシステムは、妥当性検査レスポンスデータを、少なくとも潜在的トランザクション識別情報と関連付けることができる（例えば、商業エンティティサブシステム４００は、プロセス６００のステップ６１６及び／又はステップ６２２で潜在的トランザクション識別情報に対して、妥当性検査データを関連付けることができる）。プロセス９００のステップ９０８では、管理エンティティサブシステムは、妥当性検査レスポンスデータを電子デバイスに通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はプロセス６００のステップ６２４で妥当性検査レスポンスデータ６７４の一部分としての

妥当性検査データを電子デバイス１００に通信することができる）。プロセス９００のステップ９１０では、管理エンティティサブシステムは、電子デバイスからデバイス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、商業エンティティサブシステム４００は、プロセス６００のステップ６２８で電子デバイス１００からデバイストランザクションデータ６７８を受信することができる）。プロセス９００のステップ９１２では、管理エンティティサブシステムは、妥当性検査レスポンスデータ及び潜在的トランザクション識別情報を用いてデバイストランザクションデータを妥当性検査することができる（例えば、商業エンティティサブシステム４００は、妥当性検査レスポンスデータ６７４及び潜在的トランザクション識別情報を用いて、プロセス６００のステップ６３０でデバイストランザクションデータ６７８の妥当性検査データを妥当性検査することができる）。プロセス９００のステップ９１４では、デバイストランザクションデータが妥当性検査された後、管理エンティティサブシステムは、処理サブシステムに使用されるためのデバイストランザクションデータに基づいてセキュアトランザクションデータを生成することができる（例えば、商業エンティティサブシステム４００は、プロセス６００のステップ６３１でデバイストランザクションデータ６７８に基づいて販売事業者クレデンシャルデータ６８１を生成することができる）。

【０１０１】

図９のプロセス９００で示されるステップは、単に例示したものに過ぎず、既存のステップを修正又は省略し、更なるステップを追加し、そして、特定のステップの順序を変更することができることを理解されたい。

【０１０２】

実施形態の更なる説明

デバイス１００のセキュアエレメントのクレデンシャルが、トランザクションデータの決済クレデンシャルデータとして（例えば、非接触近接型通信として、販売事業者端末２２０に、及び／又はオンライン型の通信として、販売事業者サーバ２１０に）提供されるよう、適切にイネーブルされる（例えば、クレデンシャルＳＳＤ１５４ａの可能にされたアプレット１５３ａと関連付けられた商業クレデンシャルデータ）と、取得銀行サブシステム３００は、金融機関サブシステム３５０との財務トランザクションを完了するために、このような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、デバイス１００のユーザが購入する製品を選択し、決済に使用するデバイス１００の特定のクレデンシャルを適切にイネーブルした後、販売事業者サブシステム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決済クレデンシャルデータを受信することができる。販売事業者サーバ２１０及び／又は販売事業者端末２２０は、デバイス１００が決済クレデンシャルデータを提供することに応じて、製品又はサービスをエンドユーザ用の電子デバイスのユーザに提供し得る好適な販売事業者又は販売事業者サブシステム２００の販売事業者エージェントにより提供され得る。このような受信された決済クレデンシャルデータ（例えば、データ６８４として）に基づいて、販売事業者サブシステム２００は、データ６８６を生成し、（例えば、販売事業者サブシステム２００と取得銀行サブシステム３００との間の通信経路２５を介して）取得銀行サブシステム３００に送信するように構成され得、データ６８６は、決済クレデンシャルデータと、デバイス決済クレデンシャル及び製品又はサービスの販売事業者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、販売事業者サブシステム２００に関連付けられた販売事業者の銀行パートナであることができ、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、デバイス１００が資金供給を試みたクレデンシャルトランザクションを、決済クレデンシャルデータによって承認及び決済するように構成され得る。そして、取得銀行サブシステム３００は、（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との間の通信経路３５を介して）許可要求データ６８８として決済データ６８６からの許可要求を金融機関サブシステム３５０に転送することができる。

【０１０３】

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であってもよいし、又は別個のエンティティであってよい。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の両方であってよい。対照的に、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と連携して機能してもよい。金融機関サブシステム３５０はまた、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と同一の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、一部、又は全部の構成要素を、デバイス１００のプロセッサ構成要素１０２と同一又は類似であり得る１つ以上のプロセッサ構成要素、デバイス１００のメモリ構成要素１０４と同一又は類似であり得る１つ以上のメモリ構成要素、及び／又はデバイス１００の通信構成要素１０６と同一又は類似であり得る１つ以上の通信構成要素を使用して実施することができる。決済ネットワークサブシステム３６０の１つ、一部、又は全部の構成要素を、デバイス１００のプロセッサ構成要素１０２と同一又は類似であり得る１つ以上のプロセッサ構成要素、デバイス１００のメモリ構成要素１０４と同一又は類似であり得る１つ以上のメモリ構成要素、及び／又はデバイス１００の通信構成要素１０６と同一又は類似であり得る１つ以上の通信構成要素を使用して実施することができる。発行銀行サブシステム３７０の１つ、一部、又は全部の構成要素を、デバイス１００のプロセッサ構成要素１０２と同一又は類似であり得る１つ以上のプロセッサ構成要素、デバイス１００のメモリ構成要素１０４と同一又は類似であり得る１つ以上のメモリ構成要素、及び／又はデバイス１００の通信構成要素１０６と同一又は類似であり得る１つ以上の通信構成要素を使用して実施することができる。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からデータ６９０を受信することができ、そして、（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との間の通信経路４５を介して）データ４０５として要求を発行銀行サブシステム３７０に転送することができる。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が同一のエンティティである場合、取得銀行サブシステム３００は、データ６９０を直接発行銀行サブシステム３７０に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、（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との間に合意された条件に応じて）発行銀行サブシステム３７０の代わりに、取得銀行サブシステム３００に応答することができる。取得銀行サブシステム３００と発行銀行サブシステム３７０との間をインタフェースすることにより、決済ネットワークサブシステム３６０は、各取得銀行サブシステム３００と各発行銀行サブシステム３７０とが直接相互作用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の直接統合点を最小化するために、決済ネットワークサブシステム３６０は、種々の発行銀行３７０及び／又は種々の取得銀行３００のためのアグリゲータの役割を果たすことができる。金融機関サブシステム３５０はまた、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と同一のエンティティであってもよい。

【０１０４】

発行銀行サブシステム３７０が（例えば、データ６８８として直接取得銀行サブシステム３００から、又はデータ４０５として間接的に決済ネットワークサブシステム３６０を介して）許可要求を受信すると、許可要求に含まれる決済情報（例えば、デバイス１００の商業クレデンシャル情報）及び購入額は、商業クレデンシャルに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を判定するように分析され得る。十分な資金が存在しない場合、発行銀行サブシステム３７０は、取得銀行サブシステム３００に否定的許可レスポンスを送信することにより、要求されたトランザクションを断ることができる。しかし、十分な資金が存在する場合、発行銀行サブシステム３７０は

、取得銀行サブシステム３００に肯定的許可レスポンスを送信することにより、要求されたトランザクションを承認することができ、財務トランザクションを完了することができる。いずれかのタイプの許可レスポンスを、許可レスポンスデータ又はトランザクション状況データ６９０としてユーザ金融サブシステム３５０により取得銀行サブシステム３００に提供することができる（例えば、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に提供され得る許可レスポンスデータ又はトランザクション状況データ４１５に基づいて、トランザクション状況データ６９０を、通信経路３５を介して発行銀行サブシステム３７０から取得銀行サブシステム３００に提供することができ、又はトランザクション状況データ６９０を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に提供することができる）。

【０１０５】

上述のように、図２に示すように、電子デバイス１００には、非限定的に、音楽プレイヤ（例えば、カリフォルニア州クパチーノのアップル インコーポレイテッドにより供給可能なｉＰｏｄ（登録商標））、ビデオプレイヤ、静止画プレイヤ、ゲームプレイヤ、他のメディアプレイヤ、音楽レコーダ、ムービー若しくはビデオカメラ又はレコーダ、静止画カメラ、他のメディアレコーダ、ラジオ、医療用機器、家庭用若しくは商業用機器、輸送車両用計器、楽器、計算機、セルラ電話（例えば、アップル インコーポレイテッドにより供給可能なｉＰｈｏｎｅ（登録商標））、他の無線通信デバイス、携帯情報端末、リモートコントローラ、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、アップル インコーポレイテッドにより供給可能なｉＰａｄ（登録商標））、サーバなど）、モニタ、テレビ、ステレオ装置、セットアップボックス、セットトップボックス、モデム、ルータ、プリンタ、又はそれらの任意の組合せを含むことができる。いくつかの実施形態では、電子デバイス１００は、単一の機能を実行することができ（例えば、セキュアなデータトランザクションを行うために専小型電子デバイス用のデバイス）、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、セキュアなデータトランザクションを行い、音楽を再生し、電話呼出しを受信し、送信する）。電子デバイス１００は、ユーザがどこを移動していても、財務トランザクションを行う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、又は小型電子デバイスとすることができる。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よりも小さなフォームファクタを有することができる。例示する小型電子デバイスを、非限定的に、腕時計（例えば、アップル インコーポレイテッドによるＡｐｐｌｅＷａｔｃｈ（登録商標））、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、仮想現実デバイス、眼鏡、他のウェアラブル電子機器、スポーツ用品用アクセサリ、フィットネス機器用アクセサリ、キーホルダ、又はそれらの任意の組合せを含みうる、種々の対象物に組み込むことができる。代替的に、電子デバイス１００は、全くポータブルでなくてもよく、代わりに概ね据え置き型でもよい。

【０１０６】

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、通信構成要素１０６、電源１０８、入力構成要素１１０、出力構成要素１１２、アンテナ１１６、近距離無線通信（「ＮＦＣ」）構成要素１２０を含むことができる。電子デバイス１００はまた、デバイス１００の他の種々の構成要素に、それらから、又はそれらの間に、データ及び／又は電力を転送するための１つ以上の有線若しくは無線通信リンク又は経路を提供し得るバス１１８を含むことができる。いくつかの実施形態では、電子デバイス１００の１つ以上の構成要素を組合せてもよいし、又は省略してもよい。また、電子デバイス１００は、図２に組み合わされていない、又は含まれていない他の構成要素を含んでもよい。例えば、電子デバイス１００は、図２に示す構成要素の任意の他の好適な構成要素又はいくつかのインスタンスを含むことができる。簡潔にするために、図２には、それぞれの構成要素を１つだけ示している。

【０１０７】

メモリ１０４は、例えば、ハードドライブ、フラッシュメモリ、リードオンリーメモリ（「ＲＯＭ」）などの永続的メモリ、ランダムアクセスメモリ（「ＲＡＭ」）などの半永続的メモリ、他の好適な任意のタイプの記憶構成要素、又はそれらの任意の組合せを含む、１つ以上の記憶媒体を含むことができる。メモリ１０４は、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り得るキャッシュメモリを含むことができる。メモリ１０４は、電子デバイス１００内に固定して埋め込まれてもよいし、又は、電子デバイス１００の中に反復的に挿入し、そこから取り出し得る１つ以上の好適なタイプのカード（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には、メディアデータ（例えば、音楽及び画像ファイル）、（例えば、デバイス１００上で機能を実施するための）ソフトウェア、ファームウェア、基本設定情報（例えば、メディア再生基本設定）、ライフスタイル情報（例えば、食の好み）、運動情報（例えば、運動監視機器により取得された情報）、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のを可能にし得る情報）、定期購読情報（例えば、ユーザが定期購読を受けているポットキャスト又はテレビ番組又は他のメディアを追跡記録する情報）、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、任意の他の好適なデータ、又はそれらの組合せが含まれることができる。

【０１０８】

デバイス１００が、任意の好適な通信プロトコルを用いて、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の他の構成要素）と通信することができるように通信構成要素１０６を設けることができる。例えば、通信構成要素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）、Ｅｔｈｅｒｎｅｔ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＢＬＥ（Ｂｌｕｅｔｏｏｔｈ（登録商標）Ｌｏｗ　Ｅｎｅｒｇｙ）、高周波数システム（例えば、９００　ＭＨｚ、２．４　ＧＨｚ、及び５．６　ＧＨｚ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、ＴＣＰ／ＩＰ層のそれぞれで使用されるプロトコルのいずれか）、ストリーム制御伝送プロトコル（「ＳＣＴＰ」）、動的ホスト構成プロトコル（「ＤＨＣＰ」）、ハイパーテキスト転送プロトコル（「ＨＴＴＰ」）、ＢｉｔＴｏｒｒｅｎｔ（登録商標）、ファイル転送プロトコル（「ＦＴＰ」）、リアルタイム転送プロトコル（「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」）、リモートオーディオ出力プロトコル（「ＲＡＯＰ」）、リアルデータ転送プロトコル（登録商標）（「ＲＤＴＰ」）、ユーザデータグラムプロトコル（「ＵＤＰ」）、セキュアシェルプロトコル（「ＳＳＨ」）、ワイヤレスディストリビューションシステム（「ＷＤＳ」）ブリッジング、無線及び携帯電話ならびに個人用電子メールデバイス（例えば、移動通信用のグローバルシステム（「ＧＳＭ(登録商標)」）、ＧＳＭ(登録商標)プラスＧＳＭ(登録商標)進化型高速データレート（「ＥＤＧＥ」）、符号分割多元接続（「ＣＤＭＡ」）、直交周波数分割多元接続（「ＯＦＤＭＡ」）、高速パケットアクセス（「ＨＳＰＡ」）、マルチバンドなど）が使用し得る任意の通信プロトコル、低電力無線パーソナルエリアネットワーク（「６ＬｏＷＰＡＮ」）モジュールが使用し得る任意の通信プロトコル、任意の他の通信プロトコル、又はそれらの組合せをサポートすることができる。通信構成要素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）に通信可能に結合され、他のデバイスと無線又は有線接続（例えば、コネクタポートを用いて）通信するのを可能とする任意の好適な送受信機回路（例えば、送受信機回路又はバス１１８を介してアンテナ１１６）を含んでもよいし、又はそれに電気的に結合されてもよい。通信構成要素１０６は、任意のリモートサーバ又は他の好適なエンティティ（例えば、好適なインターネット接続）に好適なデータを通信するように機能するときに、オンライン通信構成要素と呼ばれる場合がある。通信構成要素１０６は、電子デバイス１００の地理的位置を決定するように

構成されてもよい。例えば、通信構成要素１０６は、全地球測位システム（「ＧＰＳ」）又はセルタワー測位技術又はＷｉ　Ｆｉ技術を使用し得る地域内若しくはサイト内測位システムを利用することができる。

【０１０９】

電源１０８は、電力を受信及び／又は生成し、電子デバイス１００の１つ以上の他の構成要素にそのような電力を供給するために適切な回路を含むことができる。例えば、電源１０８を、（例えば、デバイス１００がポータブルデバイスの役割を果たしていない場合、又はデバイスのバッテリが電力プラントが発電した電力で電気コンセントに充電されているとき）電力グリッドに結合することができる。別の例として、電源１０８は、自然源（例えば、太陽電池を用いた太陽光）から電力を生成するように構成することができる。別の例として、電源１０８は、（例えば、デバイス１００がポータブルデバイスの役割を果たすとき）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、電源１０８は、バッテリ（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バッテリ）、無停電又は連続電源（「ＵＰＳ」又は「ＣＰＳ」）、及び発電源から受電した電力（例えば、電力プラントによって発電され、電気ソケット等を介してユーザに配電される電力）を処理する回路のうち１つ以上を含むことができる。電力は、電源１０８によって、交流又は直流として供給することができ、電力を変換し、又は受信した電力を特定の特性に制限するように処理することができる。例えば、電力を直流に、又は直流から変換することができ、平均電力、有効電力、ピーク電力、パルス当たりのエネルギー、電圧、（例えば、アンペアで測定された）電流、又は受信電力の他の特性の１つ以上の値に制約することができる。電源１０８は、（例えば、バッテリが既に充電されているときよりもバッテリ充電中により多くの電力を要求するため）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周辺デバイスのニーズ又は要件に基づいて、異なる時間に特定の量の電力を要求又は提供するように機能することができる。

【０１１０】

１つ以上の入力構成要素１１０を、ユーザにデバイス１００と相互作用させる又はインタフェースさせるために設けることができる。例えば、入力構成要素１１０は、限定されることなく、タッチパッド、ダイアル、クリックホイール、スクロールホイール、タッチスクリーン、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（例えば、バーコードスキャナ又は、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好適なスキャナ）、接近センサ、光検出器、動きセンサ、バイオメトリックセンサ（例えば、ユーザを認証するために電子デバイス１００にとって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又は他の特徴認識センサ）及びそれらの組合せを含む種々の形態をとることができる。各入力構成要素１１０を、操作デバイス１００に関連付けられた選択を行う、又はコマンドを発行するための１つ以上の専用制御機能を提供するように構成することができる。

【０１１１】

電子デバイス１００はまた、デバイス１００のユーザに情報（例えば、グラフィカル、聴覚、及び／又は触覚情報）を提示し得る１つ以上の出力構成要素１１２も含むことができる。例えば、電子デバイス１００の出力構成要素１１２は、限定されることなく、オーディオスピーカ、ヘッドホン、オーディオラインアウト、視覚ディスプレイ、アンテナ、赤外線ポート、触覚出力構成要素（例えば、ランブラー、バイブレータなど）、又はそれらの組合せを含む様々な形態をとることができる。

【０１１２】

具体例として、電子デバイス１００は、出力構成要素１１２として表示出力構成要素を含むことができる。このような表示出力構成要素は、ユーザに視覚データを提示するための好適なタイプのディスプレイ又はインタフェースを含むことができる。表示出力構成要素は、デバイス１００に埋め込まれるか、又はデバイス１００（例えば、リムーバブルデ

ィスプレイ）に結合されたディスプレイを含むことができる。表示出力構成要素は、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、表面伝導型電子放出素子ディスプレイ（「ＳＥＤ」）、カーボンナノチューブディスプレイ、ナノクリスタルディスプレイ、任意の他の適切なタイプのディスプレイ、又はそれらの組合せを含むことができる。代替的に、表示出力構成要素は、例えば、ビデオプロジェクタ、ヘッドアップディスプレイ、又は三次元（例えば、ホログラフィック）ディスプレイのような、電子デバイス１００から離れた表面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、表示出力構成要素は、コンパクトデジタルカメラ、レフカメラ、又は他の好適な静止又はビデオカメラで求められるタイプのビューファインダのようなデジタル又は機械式ビューファインダを含むことができる。表示出力構成要素は、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、又は両者を含むことができ、また、このような表示出力構成要素は、プロセッサ１０２の指示の下で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に実装されたアプリケーションのアプリケーション画面、通信中の動作に関する情報、入ってくる通信要求に関する情報、デバイス操作画面等）を表示するように機能することができる。

【０１１３】

ここで、１つ以上の入力構成要素及び１つ以上の出力構成要素を、入出力（「Ｉ／Ｏ」）構成要素又はＩ／Ｏインタフェースと総称する（例えば、入力構成要素１１０及び出力構成要素１１２をＩ／Ｏ構成要素又はＩ／Ｏインタフェース１１４と総称する）場合があることを留意されたい。例えば、入力構成要素１１０及び出力構成要素１１２は、表示画面へのユーザのタッチにより入力情報を受信でき、また同一の表示画面を介してユーザに視覚情報を提供し得るタッチスクリーンのような単一のＩ／Ｏ構成要素１１４である場合がある。

【０１１４】

電子デバイス１００のプロセッサ１０２は、電子デバイス１００の１つ以上の構成要素の動作及び性能を制御するように機能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、入力構成要素１１０から入力信号を受信することができ、かつ／又は出力構成要素１１２を介して出力信号を駆動することができる。図２に示すように、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のような１つ以上のアプリケーションを実行するためにプロセッサ１０２を使用することができる。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、又は他の好適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、ユーザインタフェースプログラムとしてアプリケーション１０３／１１３／１４３をロードし、情報が記憶され、及び／又は出力構成要素１１２を介してユーザに提供され得る方法を、入力構成要素１１０又はデバイス１００の他の構成要素を介して受信された命令又はデータがどのように、操作し得るかを決定することができる。アプリケーション１０３／１１３／１４３は、プロセッサ１０２によって、メモリ１０４（例えば、バス１１８を介して）から、又は（例えば、通信構成要素１０６を介して）別のデバイス又はサーバからなどの、任意の適切なソースからアクセスされ得る。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、汎用及び特定目的用マイクロプロセッサ、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の組合せ、及び／又は特定目的マイクロプロセッサを含むことができる。プロセッサ１０２はまた、キャッシュ目的のオンボードメモリを含むことができる。

【０１１５】

電子デバイス１００はまた、近距離無線通信（「ＮＦＣ」）構成要素１２０も含むこと

ができる。ＮＦＣ構成要素１２０は、電子デバイス１００と販売事業者サブシステム２００（例えば、販売事業者決済端末２２０）との間の非接触近接型トランザクション又は通信を可能とする任意の好適な近接型通信メカニズムとすることができる。ＮＦＣ構成要素１２０は、比較的低いデータ速度（例えば、４２４ｋｂｐｓ）での近接範囲通信を可能とすることができ、ＩＳＯ／ＩＥＣ７８１６、ＩＳＯ／ＩＥＣ１８０９２、ＥＣＭＡ－３４０、ＩＳＯ／ＩＥＣ２１４８１、ＥＣＭＡ－３５２、ＩＳＯ１４４４３、及び／又はＩＳＯ１５６９３などの好適な任意の規格に準拠することができる。追加的に、又は代替的に、ＮＦＣ構成要素１２０は、比較的高いデータ速度（例えば、３７０Ｍｂｐｓ）での近接範囲通信を可能にしてもよく、ＴｒａｎｓｆｅｒＪｅｔ（登録商標）プロトコルなどの好適な任意の規格に準拠してもよい。ＮＦＣ構成要素１２０販売事業者サブシステム２００の間の通信は、おおよそ２～４センチメートルの範囲など、ＮＦＣ構成要素と販売事業者サブシステム２００の間における好適な任意の近接範囲距離（例えば、図１及び図１ＡにおけるＮＦＣ構成要素１２０と販売事業者決済端末２２０の間の距離Ｄを参照）内で生じることができ、好適な任意の周波数（例えば、１３．５６ＭＨｚ）で動作することができる。例えば、ＮＦＣ構成要素のこのような近接範囲通信は、ＮＦＣ構成要素が他のＮＦＣデバイスと通信し得ること及び／又は無線周波数識別（「ＲＦＩＤ」）回路を有するタグから情報を取り出すことを可能にし得る、磁界誘導により生じることができる。このようなＮＦＣ構成要素は、製品情報を取得し、決済情報を移転し、又は他の方法により外部デバイスと通信する（例えば、ＮＦＣ構成要素１２０と販売事業者端末２２０の間で通信する）方法を提供することができる。

【０１１６】

ＮＦＣ構成要素１２０は、電子デバイス１００と販売事業者サブシステム２００との間の非接触近接型通信を可能とする好適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構成要素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。

【０１１７】

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、非接触近接型又はＮＦＣ通信５の一部としてＮＦＣ構成要素１２０によって販売事業者サブシステム２００に送信され得る好適なデータを収容し、経路設定し、又は他の方法により提供するように構成されてもよい。追加的に、又は代替的に、ＮＦＣデータモジュール１３２は、非接触近接型通信（例えば、ＮＦＣ構成要素１２０と販売事業者端末２２０との間の通信５）の一部として販売事業者サブシステム２００からＮＦＣ構成要素１２０によって受信され得る好適なデータを収容し、経路設定し、又は他の方法により受信するように構成されてもよい。

【０１１８】

ＮＦＣ送受信機又はＮＦＣアンテナ１３４は、ＮＦＣデータモジュール１３２から販売事業者サブシステム２００への通信及び／又はサブシステム２００からＮＦＣデータモジュール１３２への通信の通信を一般的に可能にし得る任意の好適なアンテナ又は他の好適な送受信機回路とすることができる。したがって、特にＮＦＣ構成要素１２０の非接触近接型通信能力を可能とするために、ＮＦＣアンテナ１３４（例えば、ループアンテナ）を設けることができる。

【０１１９】

追加的に、又は代替的に、ＮＦＣ構成要素１２０は、電子デバイス１００の別の通信構成要素（例えば、通信構成要素１０６）が利用し得る、同一の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、通信構成要素１０６は、アンテナ１１６を活用して、電子デバイス１００と他のリモートエンティティとの間のＷｉ Ｆｉ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、セルラ、又はＧＰＳ通信を可能とすることができ、ＮＦＣ構成要素１２０は、アンテナ１１６を活用して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、販売事業者サブシ

ステム２００）との間の非接触近接型又はＮＦＣ通信を可能とすることができる。このような実施形態では、ＮＦＣデバイスモジュール１３０はＮＦＣブースタ１３６を含むことができ、それは、ＮＦＣ構成要素１２０のデータ（例えば、ＮＦＣデータモジュール１３２内のデータ）に対して適切な信号増幅を行うことで、そのようなデータが共有アンテナ１１６によってサブシステム２００に通信として適切に送信され得るように構成され得る。例えば、電子デバイス１００と販売事業者サブシステム２００との間で非接触近接型又は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）が正しくイネーブルされ得る前に、共有アンテナ１１６はブースタ１３６からの増幅を必要とする場合がある（例えば、アンテナ１１６を用いて他のタイプのデータを送信するのに必要とされるよりも、アンテナ１１６を用いてＮＦＣデータを送信するのにより多くの電力が必要となる場合がある）。

【０１２０】

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、電子デバイス１００と販売事業者サブシステム２００との間でＮＦＣ通信を通信するためのＮＦＣ構成要素１２０を可能とする、アクティブにする、許可する、及び／又は、他の方法により制御することができる。ＮＦＣプロセッサモジュール１４２は別個の構成要素として存在してもよいし、別のチップセットに統合されてもよいし、あるいは、例えば、システムオンチップ（「ＳｏＣ」）の一部としてプロセッサ１０２と統合されてもよい。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構成要素１２０の機能を命令するのに役立ちうる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のに使用され得る。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構成要素１２０（例えばアプリケーション１０３／１１３）にとってアクセス可能となり得る任意の他の好適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、販売事業者サブシステム２００）と通信するための、近接場通信インタフェース及びプロトコル（「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るとともに、接続されたデバイスのうち１つを近距離無線通信を制御するイニシエータデバイスに指定するのに使用され得る。

【０１２１】

ＮＦＣコントローラモジュール１４０はＮＦＣ構成要素１２０の近距離無線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、ＮＦＣタグから（例えば、販売事業者サブシステム２００から）ＮＦＣデータモジュール１３２に情報（例えば、通信５）を読み出すためのリーダ／ライタモード、データ（例えば、通信５）を別のＮＦＣ可能化デバイス（例えば、販売事業者サブシステム２００）と交換するためのピアツーピアモード、及び、別のＮＦＣ可能化デバイス（例えば、販売事業者サブシステム２００）がＮＦＣデータモジュール１３２から情報（例えば、通信５）を読み出すのを可能とするためのカードエミュレーションモード間で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構成要素１２０をアクティブモードと受動モードとの間で切り替えるように構成されてもよい。例えば、ＮＦＣプロセッサモジュール１４２は、ＲＦフィールドを生成する別のデバイス（例えば、販売事業者サブシステム２００）にデータを転送するために、ＮＦＣデバイスモジュール１３０が自身のＲＦフィールドを生成することができるアクティブモードと、ＮＦＣデバイスモジュール１３０が負荷変調を用いることができる受動モードとの間で（例えば、ＮＦＣアンテナ１３４又は共有アンテナ１１６とともに）ＮＦＣデバイスモジュール１３０を切り替えるように構成され得る。このような受動モードでの動作は、このようなアクティブモードでの動作に比べて、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、デバイス１００（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）上で実行されるアプリケーションによって定義され得るか、又は他の方法により命令され得る、ユーザの好みに基づいて、及び／又はデバイス１００の製造業者の好みに基づいて、制御されてもよい。

【０１２２】

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、電子デバイス１００と販売事業者サブシステム２００との間の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、ＮＦＣデバイスハードウェア内又はＮＦＣ集積回路（「ＩＣ」）内に埋め込まれてもよい。ＮＦＣメモリモジュール１５０は、耐タンパ性であってもよく、セキュアエレメントの少なくとも一部分を提供してもよい。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通信に関連付けられた１つ以上のアプリケーション（例えば、アプリケーション１４３）を記憶してもよい。例えば、こ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、ロイヤリティカードアプリケーション、及び他のアプリケーションを含むことができ、それは暗号化されてもよい。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、電子デバイス１００上で感応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ことを目的とする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独立して、又は組合せて、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、独立に又は組合せて、耐タンパ性であり得るセキュアエレメント１４５の少なくとも一部分を提供することができる。例えば、このようなセキュアエレメント１４５は、識別され信頼された権限者の集合（例えば、金融機関サブシステム、及び／又は、ＧｌｏｂａｌＰｌａｔｆｏｒｍのような業界標準の権限者）によって定めら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が可能である耐タンパ性プラットフォームを（例えば、単一又は複数チップのセキュアマイクロコントローラとして）提供するように構成され得る。ＮＦＣメモリモジュール１５０は、メモリ１０４の一部分であってもよいし、又はＮＦＣ構成要素１２０に特有の少なくとも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上に、電子デバイス１００のマザーボード上の専用チップ上に、又はメモリカード内の外部プラグとして常駐してもよい。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の種々の構成要素によって提供されてもよく、及び／又は様々なリムーバブル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、機密データ又は電子デバイス１００上のアプリケーションを記憶するために使用され得る、チップ内の高度にセキュアな、耐タンパ性ハードウェア構成要素とすることができる。汎欧州デジタル移動通信（「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」）規格ネットワークに適合した電子デバイス１００に使用され得る、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」）カードなどのリムーバブル回路カード内にセキュアエレメント１４５の少なくとも一部分を設けることができる。追加的に、又は代替的に、デバイス１００の製造中に電子デバイス１００に埋め込まれ得る集積回路内にセキュアエレメント１４５の少なくとも一部分を設けてもよい。追加的に、又は代替的に、電子デバイス１００にプラグイン、挿入、又は他の方法により結合され得る、マイクロセキュアデジタル（「ＳＤ」）メモリカードなどの周辺デバイス内にセキュアエレメント１４５の少なくとも一部分を設けてもよい。

【０１２３】

図２に示すように、ＮＦＣメモリモジュール１５０は、ＮＦＣ仕様標準（例えば、ＧｌｏｂａｌＰｌａｔｆｏｒｍ）によって定義及び管理され得る、発行者セキュリティドメイン（「ＩＳＤ」）１５２及び補足的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」）等）のうちの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の一部分とすることができ、その部分には、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）が、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、例えば、通信構成要素１０６を介して）電子デバイス１００上に、１つ以上のクレデンシャル（例えば、各種クレジットカード、銀行カード、ギフトカード、アクセスカード、交通パス、デジタル通貨（例えば、ビットコイン及び関連決済ネットワーク）などに関連付けられた商業クレデンシャル）を形成し、又は他の方法により、供給するための鍵及び／又は他の好適な情報を記憶することができる。特定の補足的セキュリティドメイン（「ＳＳＤ」）１５４（例えば、ＳＳＤ１５４ａ）を、特定のＴＳＭ及び、電子デバイス１００に特定の特典又は決済権を提供し得る少なくとも１つの特定の商業クレデンシャル（例えば、特定のクレジットカードクレデンシャル又は特定の公衆交通カードクレデンシャル）と関連付けることができる。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用のＴＳＭとすることができ、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によって管理された商業クレデンシャルと関連付けられてもよく、第２の決済ネットワークサブシステム３６０（例えば、ＭａｓｔｅｒＣａｒｄ）は、別のＳＳＤ１５４用のＴＳＭとすることができる。

【０１２４】

ＮＦＣ構成要素１２０の使用を可能とするため（例えば、デバイス１００上に供給された商業クレデンシャルのアクティブ化を可能とするため）、クレデンシャルのクレジットカード情報又は銀行アカウント情報などの機密決済情報を電子デバイス１００から販売事業者サブシステム２００に送信する際に特に有用であり得るセキュリティ特徴を設けることができる。このようなセキュリティ特徴はまた、アクセスが制限され得るセキュアな記憶領域を含むことができる。（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）セキュアな記憶領域にアクセスするために、例えば、個人識別番号（「ＰＩＮ」）の入力を介した、又はバイオメトリックセンサとのユーザ相互作用を介したユーザ認証を設けることが必要とされ得る。特定の実施形態では、セキュリティ特徴の一部又は全部がＮＦＣメモリモジュール１５０内に記憶されてもよい。更に、サブシステム２００と通信するための認証鍵のようなセキュリティ情報を、ＮＦＣメモリモジュール１５０内に記憶してもよい。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内に埋め込まれたマイクロコントローラを含むことができる。

【０１２５】

図１Ａの販売事業者サブシステム２００の販売事業者端末２２０は、電子デバイス１００からＮＦＣ通信（例えば、デバイス１００が販売事業者端末２２０の特定の距離内に、又はその近傍に来たときの通信５）を検出し、読み取り、又は他の方法により受信するリーダを含むことができる。したがって、このような販売事業者端末と電子デバイス１００との間のＮＦＣ通信が無線で生じ得ること、よって、各デバイスの間に明瞭な「見通し線」を必要としな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は受動的であってもよいし、又はアクティブであってもよい。受動的であるとき、ＮＦＣデバイスモジュール１３０は、このような販売事業者端末の好適なリーダの応答範囲内にある場合にのみアクティブ化することができる。例えば、このような販売事業者端末のリーダは、比較的低電力の電波を発することができ、電波は、ＮＦＣデバイスモジュール１３０により利用されるアンテナ（例えば、共有アンテナ１１６又はＮＦＣ特有のアンテナ１３４）に電力供給し、それにより、そのアンテナが好適な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を介してそのような販売事業者端末にＮＦＣ通信として送信するこ

とを可能とするために使用することができる。アクティブであるとき、ＮＦＣデバイスモジュール１３０は、電子デバイス１００にとってローカルな電力ソース（例えば、電源１０８）を取り込み、又は他の方法により電力ソースにアクセスすることができ、電力ソースは、共有アンテナ１１６又はＮＦＣ特有のアンテナ１３４が、受動的な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を介して販売事業者端末２２０にＮＦＣ通信としてアクティブに送信することを可能とすることができる。販売事業者端末２２０は、販売事業者サブシステム２００の販売事業者により（例えば、ストアにて製品又はサービスをデバイス１００のユーザに直接販売するための販売事業者のストアにて）提供され得る。ＮＦＣ構成要素１２０について近距離無線通信に関して説明してきたが、好適な非接触近接型の任意のモバイル決済又は電子デバイス１００とこのような販売事業者端末の間の他の好適な任意のタイプの非接触近接型通信を提供するように構成要素１２０を構成してもよいことを理解されたい。例えば、電磁／静電結合技術を伴う通信などの好適な任意の近距離無線通信を提供するようにＮＦＣ構成要素１２０を構成することができる。

【０１２６】

ＮＦＣ構成要素１２０について近距離無線通信に関して説明してきたが、好適な非接触近接型の任意のモバイル決済又は電子デバイス１００と販売事業者サブシステム２００の間の他の好適な任意のタイプの非接触近接型通信を提供するように構成要素１２０を構成してもよいことを理解されたい。例えば、電磁／静電結合技術を伴う通信などの好適な任意の近距離無線通信を提供するようにＮＦＣ構成要素１２０を構成することができる。代替的に、いくつかの実施形態では、プロセッサ１０２又はデバイス１００の任意の他の部分にとって利用可能なデータを、デバイス１００のＮＦＣ構成要素１２０と、販売事業者サブシステム２００の販売事業者端末２２０との間の任意の好適な非接触近接型通信として通信することを可能とする任意の好適な構成要素を含むようにデバイス１００のＮＦＣ構成要素１２０を構成することができるが、ＮＦＣ構成要素１２０は、プロセス６００のクレデンシャルデータのような、財務トランザクションにセキュアに資金供給するためにデバイス１００上にセキュアなクレデンシャルデータを生成する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機能するセキュアエレメントを含んでもよいし、含まなくてもよい。

【０１２７】

電子デバイス１００は、デバイス１００の外部のゴミ又は他の劣化力から保護するためデバイス１００の構成要素のうち１つ以上を少なくとも部分的に囲み得る筐体１０１を備えることもできる。いくつかの実施形態では、構成要素の１つ以上を、自身の筐体内に設けることができる（例えば、入力構成要素１１０は、自身の筐体内に設けられ得るプロセッサ１０２と無線で、又は有線を通じて通信し得る、自身の筐体内の独立したキーボード又はマウスとすることができる）。互いに関連して動作する２つ以上のデバイス（例えば、好適な近接通信プロトコル（例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標））を介して通信可能に結合された携帯電話及びスマートウォッチ）の組合せとしていずれかのデバイス１００を設けてもよいことを理解されたい。

【０１２８】

上述のように、かつ図３に示すように、電子デバイス１００の特定の一例はｉＰｈｏｎｅ（登録商標）のようなハンドヘルド型電子デバイスとすることができ、筐体１０１は、デバイス１００とユーザならびに／又は周辺環境とが互いにインタフェースし得る種々の入力構成要素１１０ａ～１１０ｉ、種々の出力構成要素１１２ａ～１１２ｃ、及び種々のＩ／Ｏ構成要素１１４ａ～１１４ｄへのアクセスを可能とすることができる。入力構成要素１１０ａは、押下されると、デバイス１００によって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表示させることができるボタンを含むことができる。入力構成要素１１０ｂは、スリープモードとウェークモードとの間で、又は他の好適なモード間で電子デバイス１００をトグルするためのボタンとすることができる。入力構成要素１

１０ｃは、電子デバイス１００の特定の態様で１つ以上の出力構成要素１１２を不能にし得る２つの位置のスライダを含むことができる。入力構成要素１１０ｄ、１１０ｅは、電子デバイス１００の出力構成要素１１２のボリューム出力又は他の特性出力を増減させるためのボタンを含むことができる。入力構成要素１１０ａ～１１０ｅのそれぞれは、ドームスイッチ、スライドスイッチ、制御パッド、キー、ノブ、スクロールホイール、又は任意の好適な形態でサポートされたボタンなどの機械式入力構成要素とすることができる。

【０１２９】

出力構成要素１１２ａは、ユーザが電子デバイス１００と相互作用することを可能にし得る視覚的又はグラフィックユーザインタフェース（「ＧＵＩ」）１８０を表示するために使用され得るディスプレイとすることができる。ＧＵＩ１８０は、表示出力構成要素１１２ａの領域の全部又は一部に表示され得る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）の種々の層、ウィンドウ、画面、テンプレート、要素、メニュー、及び／又は他の構成要素を含むことができる。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いてもよい。ユーザ入力構成要素１１０ａ～１１０ｉのうち１つ以上は、ＧＵＩ１８０を介してナビゲートするのに使用され得る。例えば、１つのユーザ入力構成要素１１０は、ユーザがＧＵＩ１８０の１つ以上のグラフィック要素又はアイコン１８２を選択するのを可能とす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、表示出力構成要素１１２ａ及び関連付けられたタッチ入力構成要素１１０ｆを含み得るタッチスクリーンＩ／Ｏ構成要素１１４ａを介して選択されてもよい。このようなタッチスクリーンＩ／Ｏ構成要素１１４ａは、限定されることなく、抵抗性、容量性、赤外線、弾性表面波、電磁、又は近接場撮像などの、任意の好適なタイプのタッチスクリーン入力技術を採用することができる。更に、タッチスクリーンＩ／Ｏ構成要素１１４ａは、単一ポイント又はマルチポイント（例えば、マルチタッチ）入力感知を採用することができる。

【０１３０】

アイコン１８２は、種々の層、ウィンドウ、スクリーン、テンプレート、要素、及び／又はユーザによる選択の際に、表示構成要素１１２ａの一部又は全部に表示され得る他の構成要素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の、又はそのアイコン１８２と関連付けられた新しいアプリケーションの、１つ以上の追加アイコン又は他のＧＵＩ要素を含み得るＧＵＩ１８０の新しい画面に導くことができる。各グラフィカル要素アイコン１８１のユーザ解釈を容易にするために、各アイコン１８２上又はその近くにテキストインジケータ１８２を表示してもよい。ＧＵＩ１８０は階層構造及び／又は非階層構造に配置された種々の構成要素を含んでもよいことを理解されたい。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たな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することができる。例えば、「Ｍｅｒｃｈａｎｔ　Ａｐｐ」テキストインジケータ１８１がラベル付けされた特定のアイコン１８２（すなわち、特定のアイコン１８３）が選択されると、デバイス１００は、特定の販売事業者アプリケーションを起動し、又は他の方法によりそのアプリケーションにアクセスしてもよく、特定の方法でデバイス１００と相互作用する１つ以上のツール又は特徴を含み得る特定のユーザインタ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のために、画面は表示出力構成要素１１２ａ上に表示されてもよく、種々のユーザインタフェース要素（例えば、図３Ａ～図３Ｄの画面１９０ａ～１９０ｄ）を含むことができる。追加的に、又は代替的に、各アプリケーションに対して、他の種々のタイプの非視覚情報を、デバイス１００の種々の他の出力構成要素１１２を介してユーザに提供してもよい。種々のＧＵＩ１８０に関して説明する動作は、幅広い種類のグラフィカル要素及び視覚的方式により実現されてもよい。したがって、説明する実施形態は、本明細書で採用するユーザインタフェース規則に厳密に限定されることを意図していない。むしろ、

実施形態は、幅広い種類のユーザインタフェーススタイルを含んでもよい。
【０１３１】
電子デバイス１００はまた、デバイス１００と他のデバイスとの間の通信を可能にし得る種々の他のＩ／Ｏ構成要素１１４も含むことができる。Ｉ／Ｏ構成要素１１４ｂは、リモートデータソース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、及び／又は外部電源から電力を送受信するように構成され得る接続ポートとすることができる。例えば、Ｉ／Ｏ構成要素１１４ｂは、カリフォルニア州クパチーノのアップルインコーポレイテッドからのライトニング（登録商標）コネクタ又は３０ピンドックコネクタなど、専用のポートとすることができる。Ｉ／Ｏ構成要素１１４ｃは、ＳＩＭカード又は任意の他のタイプのリムーバブル構成要素を受け入れるための接続スロットとすることができる。Ｉ／Ｏ構成要素１１４ｄは、マイクロフォン構成要素を含んでもよいし、あるいは含まなくてもよいオーディオヘッドホンを接続するためのヘッドホンジャックとすることができる。電子デバイス１００はまた、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構成要素１１０ｇと、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構成要素１１２ｂとを含むことができる。
【０１３２】
＋子デバイス１００はまた、少なくとも１つの触知又は触覚出力構成要素１１２ｃ（例えば、回転機）と、カメラ及び／又はスキャナ入力構成要素１１０ｈ（例えば、ビデオ又はスチルカメラ、及び／又はバーコードスキャナ、又はバーコード、ＱＲコード(登録商標)又は同様のものなどのコードから製品識別情報を取得し得る任意の好適なスキャナ）と、バイオメトリック入力構成要素１１０ｉ（例えば、ユーザを認証するための電子デバイス１００にとってアクセス可能とな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又は他の特徴認識センサ）と、を含むこともできる。図３に示すように、バイオメトリック入力構成要素１１０ｉの少なくとも一部分を、入力構成要素１１０ａ又はデバイス１００の任意の他の好適な入力構成要素１１０に組み込んでもよいし、又は他の方法により、それと組合せてもよい。例えば、バイオメトリック入力構成要素１１０ｉは、ユーザが、入力構成要素１１０ａをユーザの指で押すことによって機械式入力構成要素１１０ａと相互作用する際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とすることができる。別の例として、バイオメトリック入力構成要素１１０ｉは、タッチスクリーンＩ／Ｏ構成要素１１４ａのタッチ入力構成要素１１０ｆと組み合わされ得る指紋リーダとすることができるので、バイオメトリック入力構成要素１１０ｉは、ユーザがユーザの指でタッチスクリーン入力構成要素１１０ｆを押圧するか、又は、それに沿ってスライドすることによってタッチスクリーン入力構成要素１１０ｆと相互作用する際、ユーザの指の指紋をスキャンするように構成することができる。また、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には示されない）を介してサブシステム２００にとって通信可能にアクセス可能であり得るＮＦＣ構成要素１２０を更に含むことができる。ＮＦＣ構成要素１２０を、少なくとも部分的に筐体１０１内に配置してもよく、また、ＮＦＣ構成要素１２０と関連付けられたアンテナの１つ以上の一般的な位置（例えば、アンテナ１１６及び／又はアンテナ１３４の一般的位置）を識別し得るマーク又はシンボル１２１を、筐体１０１の外面に設けることができる。
【０１３３】
図１～図９に関して記載のプロセスの１つ、いくつか、又はすべてはそれぞれ、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いずれかの組合せで実施されてもよい。これらのプロセスを実行する命令は、機械又はコンピュータ可読媒体上に記録された機械又はコンピュータ可読コードとして具現化されてもよい。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とすることができる。こ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、リムーバブルメモリカード、及びデータ記憶装置（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非一時的コンピュータ可読媒体とすることができる。このような実施形態では、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が分散形式で記憶及び実行されるように、ネットワークに結合されたコンピュータシステムにわたって分散させることができる。例えば、一時的コンピュータ可読媒体を、任意の好適な通信プロトコルを用いて１つの電子デバイスから別の電子デバイスに通信することができる（例えば、コンピュータ可読媒体を、（例えば、アプリケーション１０３の少なくとも一部分として、及び／又は、アプリケーション１１３の少なくとも一部分として、及び／又はアプリケーション１４３の少なくとも一部分として）通信構成要素１０６を介して電子デバイス１００に通信することができる）。このような一時的コンピュータ可読媒体は、搬送波又は他のトランスポート機構などの、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、又は変調されたデータ信号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とすることができる。

【０１３４】

システム１のモジュール又は構成要素又はサブシステムのいずれか、それぞれ又は少なくとも１つを、ソフトウェア構成、ファームウェア構成、１つ以上のハードウェア構成要素、又はそれらの組合せとして提供してもよいことを理解されたい。例えば、システム１のモジュール又は構成要素又はサブシステムのいずれか、それぞれ又は少なくとも１つを、１つ以上のコンピュータ又は他のデバイスにより実行されうる、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説明することができる。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若しくは１つ以上の具体的な概要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のモジュール及び構成要素及びサブシステムの数、構成、機能、及び相互接続が例示にすぎないこと、及び存在するモジュール、構成要素、及び／又はサブシステムの数、構成、機能、及び相互接続を修正又は省略してもよく、追加のモジュール、構成要素、及び／又はサブシステムを追加してもよく、いくつかのモジュール、構成要素、及び／又はサブシステムの相互接続を改変してもよいことも理解されたい。

【０１３５】

システム１のモジュール又は構成要素又はサブシステムの１つ以上の少なくとも一部分は、好適な任意の方法でシステム１のエンティティ（（例えば、アプリケーション１０３の少なくとも一部分及び／又はアプリケーション１１３の少なくとも一部分及び／又はアプリケーション１４３の少なくとも一部分として）例えば、デバイス１００のメモリ１０４）に記憶されることができ、又は他の方法によりシステム１のエンティティにとってアクセス可能とすることができる。例えば、ＮＦＣ構成要素１２０のモジュールのいずれか又はそれぞれを、好適な任意の技術を使用して（例えば、１つ以上の集積回路デバイスとして）実装してもよく、様々なモジュールが、構造、性能、及び動作において同一でもよいし、同一でなくてもよい。システム１のモジュール又は他の構成要素のいずれか又はそれぞれを、拡張カード上に搭載してもよく、システムマザーボード上に直接搭載してもよく、システムチップセット構成要素（例えば、「ノースブリッジ」チップ）に組み込んでもよい。

【０１３６】

システム１のモジュール又は構成要素のいずれか又はそれぞれ（例えば、ＮＦＣ構成要素１２０のモジュールのいずれか又はそれぞれ）は、種々の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た専用システムとすることができる。例えば、モジュールのすべてを相互接続された様々な拡張カード上に搭載してもよく、１つの拡張カード上に搭載してもよい。ＮＦＣ構成要素１２０に関して、例のみとして、ＮＦＣ構成要素１２０のモジュールは、拡張スロット（例えば、ペリフェラルコンポーネントインターコネクト（「ＰＣＩ」）スロット又はＰＣＩエクスプレススロット）を通じてデバイス１００

のマザーボード又はプロセッサ１０２とインタフェースすることができる。代わりに、ＮＦＣ構成要素１２０は、リムーバブルである必要はないが、モジュールの利用に専用のメモリ（例えば、ＲＡＭ）を含みうる１つ以上の専用モジュールを含んでもよい。他の実施形態では、ＮＦＣ構成要素１２０をデバイス１００に組み込むことができる。例えば、ＮＦＣ構成要素１２０のモジュールが、デバイス１００のデバイスメモリ１０４の一部分を利用することができる。システム１のモジュール又は構成要素のいずれか又はそれぞれ（例えば、ＮＦＣ構成要素１２０のモジュールのいずれか又はそれぞれ）は、それ自体の処理回路構成及び／又はメモリを含むことができる。代わりに、システム１のモジュール又は構成要素のいずれか又はそれぞれ（例えば、ＮＦＣ構成要素１２０のモジュールのいずれか又はそれぞれ）は、処理回路構成及び／又はメモリを、ＮＦＣ構成要素１２０の他の任意のモジュール及び／又はデバイス１００のプロセッサ１０２及び／又はメモリ１０４と共有してもよい。

【０１３７】

本開示は、この技術のそのような個人情報データを使用してユーザを利することができることを理解する。例えば、個人情報データは、ユーザがより興味がある的を絞ったコンテンツを配信するために使用することができる。したがって、そのような個人情報データの使用は、配信されるコンテンツの計算された制御を可能とする。更に、ユーザを利する個人情報データに関するその他の使用もまた、本開示により意図されている。

【０１３８】

本開示は、そのような個人情報データの収集、分析、開示、伝送、記憶、又はその他の使用に応答するエンティティは、確固たるプライバシーのポリシー及び／又はプライバシー慣行に従うであろうことを更に意図している。具体的には、そのようなエンティティは、個人情報データを秘密として厳重に保守するための業界又は政府の要件を満たすか又は上回るものとして一般に認識されている、プライバシーのポリシー及び慣行を実施し常に使用すべきである。例えば、ユーザからの個人情報は、そのエンティティの合法的かつ正当な使用のために収集されるべきであり、それらの合法的使用を除いて、共有又は販売されるべきではない。更には、そのような収集は、ユーザに告知して同意を得た後にのみ実施するべきである。更には、そのようなエンティティは、そのような個人情報データへのアクセスを保護して安全化し、その個人情報データへのアクセスを有する他者が、それらのプライバシーのポリシー及び手順を遵守することを確実とするための、あらゆる必要な措置を講じるであろう。更には、そのようなエンティティは、広く受け入れられているプライバシーのポリシー及び慣行に対する自身の遵守を証明するために、第三者による評価を自らが受けることができる。

【０１３９】

前述のことがらにもかかわらず、本開示はまた、ユーザが、個人情報データの使用又は個人情報データへのアクセスを選択的に阻止する実施形態も企図している。すなわち、本開示は、そのような個人情報データへのアクセスを防止又は阻止するために、ハードウェア要素及び／又はソフトウェア要素を提供することができると想到する。例えば、広告配信サービスの場合において、本技術は、ユーザが、サービスの登録の間、個人情報データの収集への参加の「オプトイン」又は「オプトアウト」を選択することを可能とするように構成することができる。別の実施例では、ユーザは、ターゲットコンテンツ配信サービスに位置情報を提供しないように選択することができる。更に別の例では、ユーザは正確な位置情報を提供しないが、位置領域情報の転送を許可することを選択することができる。

【０１４０】

説明するコンセプトの更なる用途

セキュアデバイス機能へのオンラインアクセスを妥当性検査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いるが、本明細書に記載されている主題の趣旨及び範囲をいかなる方法でも逸脱せずに多くの変更を行うことができることを理解されたい。当業者から見て、特許請求された主題からの本質的でなく、現在既知であるか、又は今後で考案された変更は、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

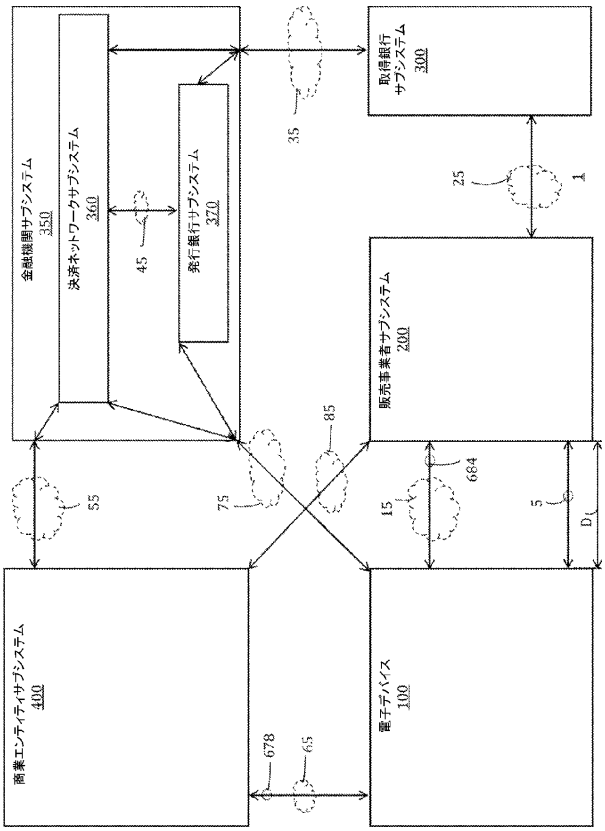
って、当業者に、現在既知であるか、又は今後既知となる明白な置換は、定義された要素の範囲内にあるものと定義される。

【０１４１】

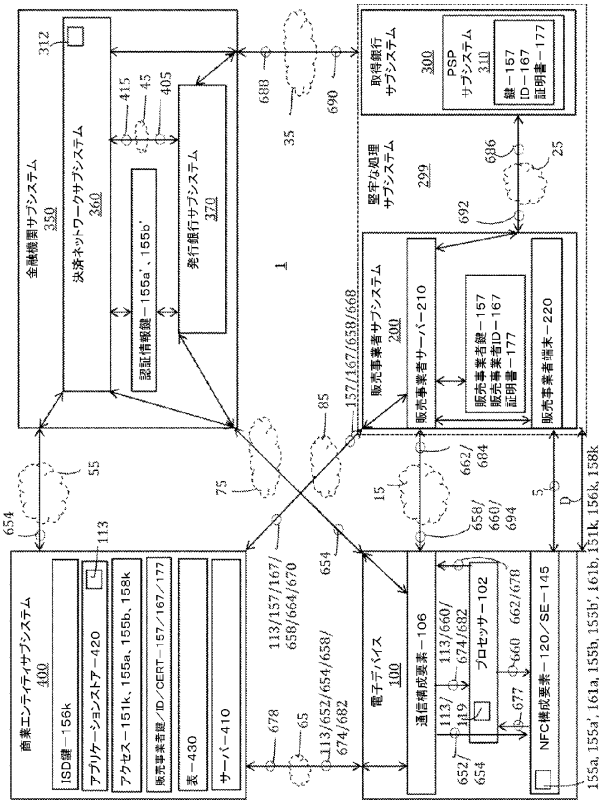
したがって、当業者は、限定ではなく例示を目的として提示される説明した実施形態とは異なる方法で本発明を実践できることを理解するであろう。

【図面】

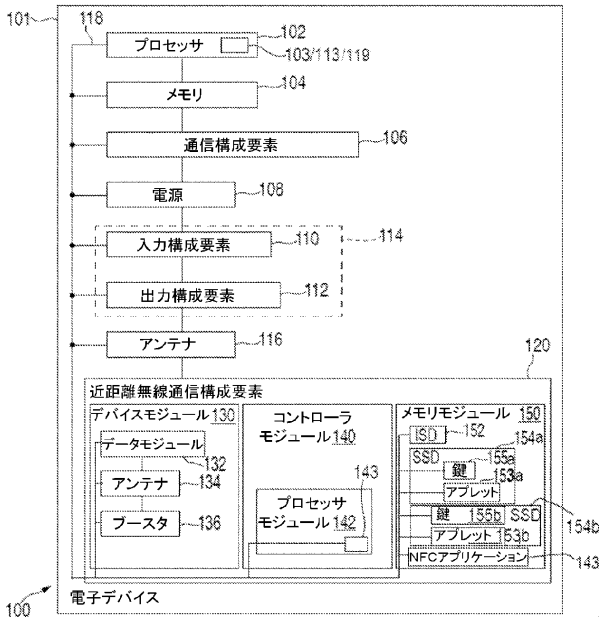
【図１】



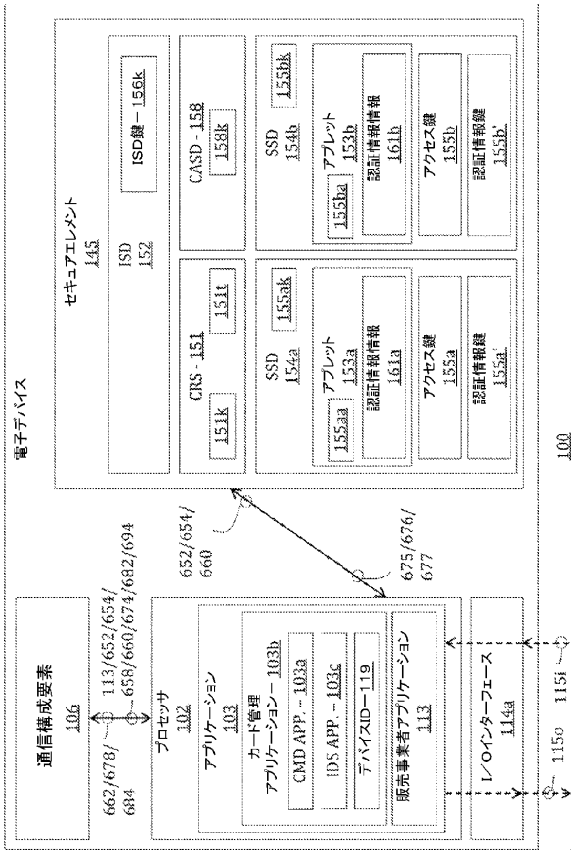
【図１Ａ】



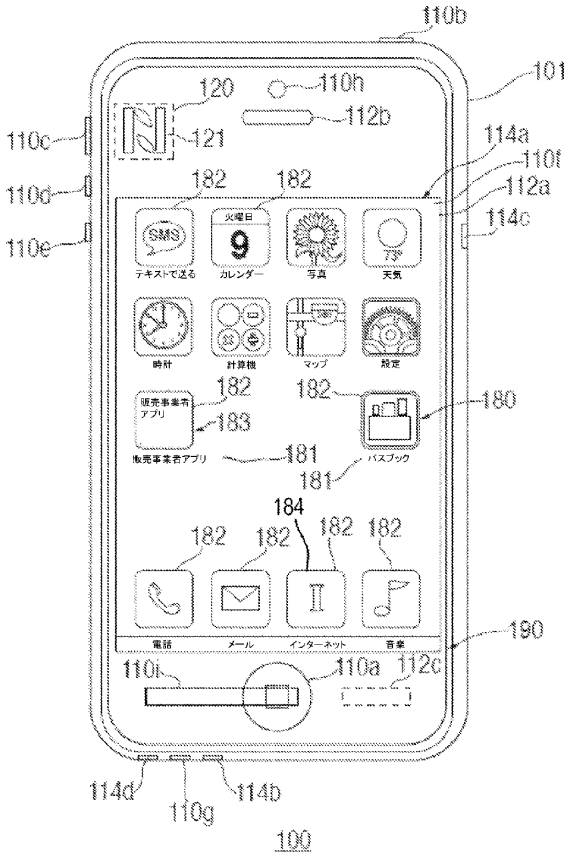
【図２】



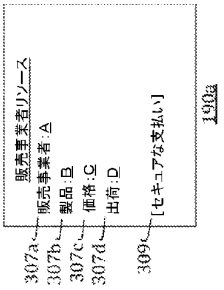
【図２Ａ】



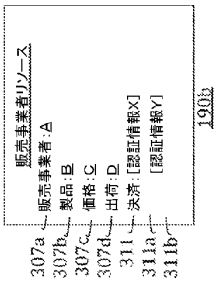
【図３】



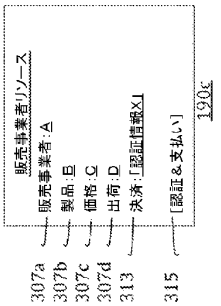
【図３Ａ】



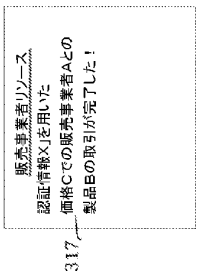
【図３Ｂ】



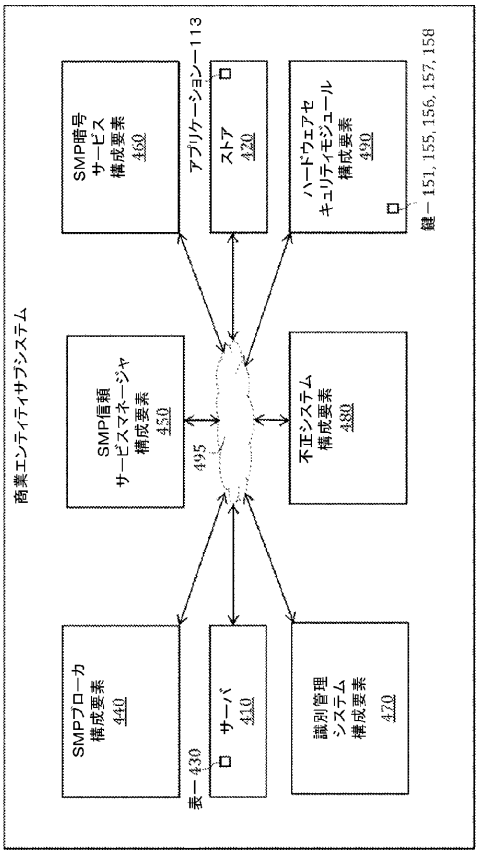
【図３Ｃ】



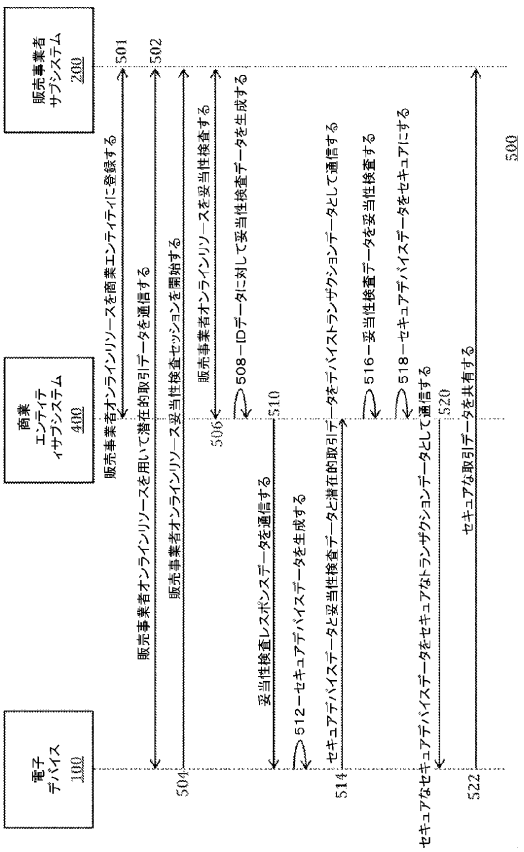
【図３Ｄ】


販売事業者リソース
認証情報X」を用いた
価格Cでの販売事業者Aとの
製品Bの取引が完了した！
317
1904

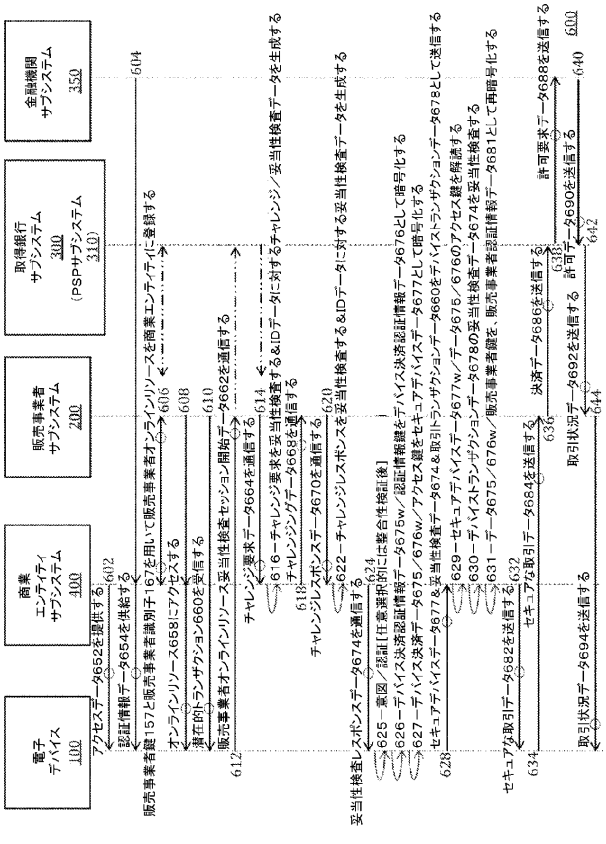
【図４】


商業エンティティサブシステム
SMP暗号
サービス
構成要素
460
アプリケーション113
ストア
420
ハードウェアセキュリティモジュール
構成要素
490
鍵－151, 155, 156, 157, 158
SMP信頼
サービスマネージャ
構成要素
450
495
不正システム
構成要素
480
SMPブローカ
構成要素
440
サーバ
410
識別管理
システム
構成要素
470
表－430
400

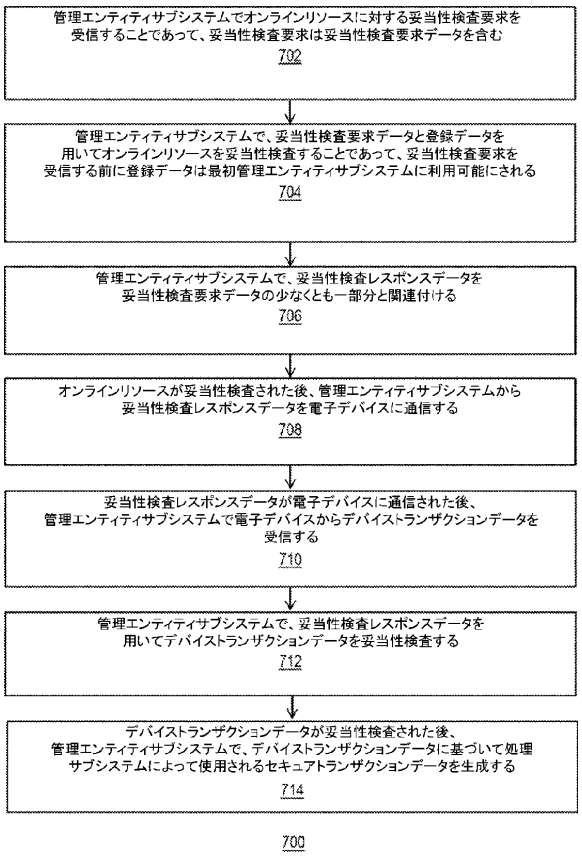
【図５】


電子
デバイス
100
商業
エンティティ
サブシステム
400
販売事業者
サブシステム
200
販売事業者オンラインリソースを商業エンティティに登録する
501
販売事業者オンラインリソースを用いて潜在的取引データを通信する
502
販売事業者オンラインリソース妥当性検査セッションを開始する
504
販売事業者オンラインリソースを妥当性検査する
506
508－IDデータに対して妥当性検査データを生成する
510
妥当性検査レスポンスデータを通信する
512－セキュアデバイスデータを生成する
514
セキュアデバイスデータと妥当性検査データと潜在的取引データをデバイストランザクションデータとして通信する
516－妥当性検査データを妥当性検査する
518－セキュアデバイスデータをセキュアにする
520
セキュアなセキュアデバイスデータをセキュアなトランザクションデータとして通信する
522
セキュアな取引データを共有する
500

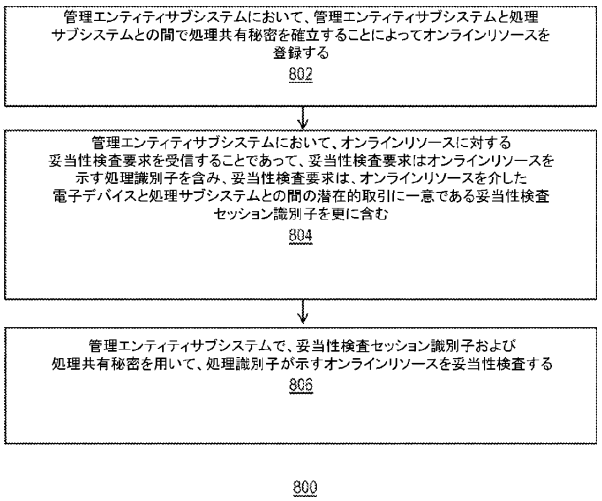
【図６】


電子
デバイス
100
商業
エンティティ
サブシステム
400
販売事業者
サブシステム
200
取得銀行
サブシステム
300
(PSPサブシステム
310)
金融機関
サブシステム
350
604
606
608
610
612
614
616－チャレンジ要求を妥当性検査する&IDデータに対するチャレンジ／妥当性検査データを生成する
618
620
622－チャレンジレスポンスを妥当性検査する&IDデータに対する妥当性検査データを生成する
624
625－裏図／認証[任意選択的には整合性検証後]
626－デバイス決済認証情報データ675w／認証情報鍵をデバイス決済認証情報データ676として暗号化する
627－デバイス決済データ675／676w／アクセス鍵をセキュアデバイスデータ677として暗号化する
628
629－セキュアデバイスデータ677w／データ675／676Oのアクセス鍵を解読する
630－デバイストランザクションデータ678の妥当性検査データ674を妥当性検査する
631－データ675／676w／販売事業者認証、販売事業者鍵情報データ681として再暗号化する
632
634
636
638
640
642
644
600
アクセスデータ652を提供する
認証情報データ654を供給する
販売事業者鍵157と販売事業者識別子167を用いて販売事業者オンラインリソースを商業エンティティに登録する
オンラインリソースA658にアクセスする
潜在的トランザクション660を実行する
販売事業者オンラインリソース妥当性検査セッション開始データ662を通信する
チャレンジ要求データ664を通信する
チャレンジングデータ666を通信する
チャレンジレスポンスデータ670Eを通信する
妥当性検査レスポンスデータ674を通信する
セキュアデバイスデータ674&取引トランザクションデータ660をデバイストランザクションデータ678として送信する
セキュアな取引データ682を送信する
決済データ686を送信する
許可要求データ688を送信する
取引状況データ694を送信する
許可データ690を送信する
セキュアな取引データ684を送信する
取引状況データ692を送信する

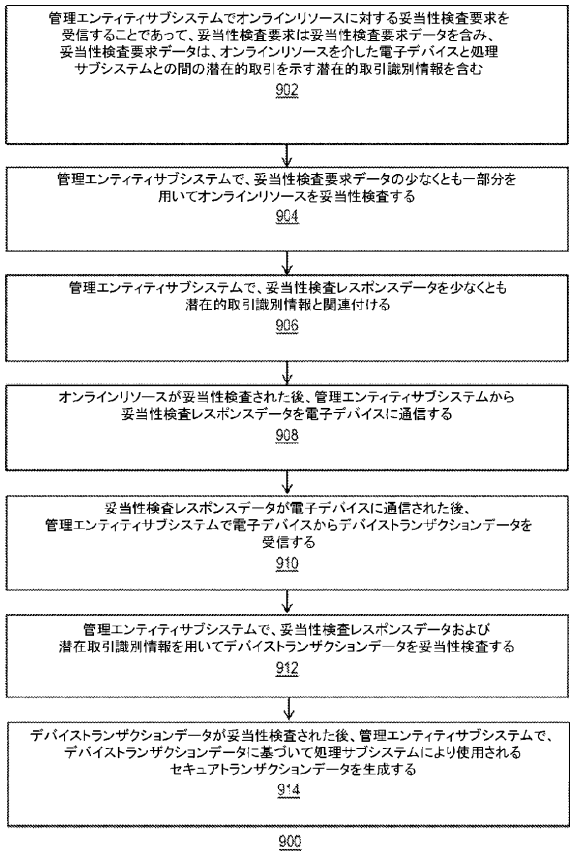
【図７】


管理エンティティサブシステムでオンラインリソースに対する妥当性検査要求を受信することであって、妥当性検査要求は妥当性検査要求データを含む
702
管理エンティティサブシステムで、妥当性検査要求データと登録データを用いてオンラインリソースを妥当性検査することであって、妥当性検査要求を受信する前に登録データは最初管理エンティティサブシステムに利用可能にされる
704
管理エンティティサブシステムで、妥当性検査レスポンスデータを妥当性検査要求データの少なくとも一部分と関連付ける
706
オンラインリソースが妥当性検査された後、管理エンティティサブシステムから妥当性検査レスポンスデータを電子デバイスに通信する
708
妥当性検査レスポンスデータが電子デバイスに通信された後、管理エンティティサブシステムで電子デバイスからデバイストランザクションデータを受信する
710
管理エンティティサブシステムで、妥当性検査レスポンスデータを用いてデバイストランザクションデータを妥当性検査する
712
デバイストランザクションデータが妥当性検査された後、管理エンティティサブシステムで、デバイストランザクションデータに基づいて処理サブシステムによって使用されるセキュアトランザクションデータを生成する
714
700

【図８】


管理エンティティサブシステムにおいて、管理エンティティサブシステムと処理サブシステムとの間で処理共有秘密を確立することによってオンラインリソースを登録する
802
管理エンティティサブシステムにおいて、オンラインリソースに対する妥当性検査要求を受信することであって、妥当性検査要求はオンラインリソースを示す処理識別子を含み、妥当性検査要求は、オンラインリソースを介した電子デバイスと処理サブシステムとの間の潜在的取引に一意である妥当性検査セッション識別子を更に含む
804
管理エンティティサブシステムで、妥当性検査セッション識別子および処理共有秘密を用いて、処理識別子が示すオンラインリソースを妥当性検査する
806
800

【図９】


管理エンティティサブシステムでオンラインリソースに対する妥当性検査要求を受信することであって、妥当性検査要求は妥当性検査要求データを含み、妥当性検査要求データは、オンラインリソースを介した電子デバイスと処理サブシステムとの間の潜在的取引を示す潜在的取引識別情報を含む
902
管理エンティティサブシステムで、妥当性検査要求データの少なくとも一部分を用いてオンラインリソースを妥当性検査する
904
管理エンティティサブシステムで、妥当性検査レスポンスデータを少なくとも潜在的取引識別情報と関連付ける
906
オンラインリソースが妥当性検査された後、管理エンティティサブシステムから妥当性検査レスポンスデータを電子デバイスに通信する
908
妥当性検査レスポンスデータが電子デバイスに通信された後、管理エンティティサブシステムで電子デバイスからデバイストランザクションデータを受信する
910
管理エンティティサブシステムで、妥当性検査レスポンスデータおよび潜在取引識別情報を用いてデバイストランザクションデータを妥当性検査する
912
デバイストランザクションデータが妥当性検査された後、管理エンティティサブシステムで、デバイストランザクションデータに基づいて処理サブシステムにより使用されるセキュアトランザクションデータを生成する
914
900

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 62/348,960
(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)
(31)優先権主張番号 15/275,122
(32)優先日 平成28年9月23日(2016.9.23)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 62/348,979
(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 100086771
弁理士 西島 孝喜
(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 カールソン カール アンダース
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 ディードリッヒ アントン ケイ
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
(72)発明者 シャープ クリストファー
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 ファソリ ジャンパオロ
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 スタチョウィアク マチェイ
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
(72)発明者 バイイントン マシュー シー
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
(72)発明者 ウェイニグ サミュエル エム
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 金沢 史明
(56)参考文献 米国特許出願公開第２０１５／００１９４４３（ＵＳ，Ａ１）
特表２０１３－５３９５６７（ＪＰ，Ａ）
特表２０１６－５０２３７３（ＪＰ，Ａ）
特開２００３－０１６０４１（ＪＰ，Ａ）
米国特許出願公開第２０１５／００９５２１９（ＵＳ，Ａ１）
米国特許出願公開第２０１５／００８８７５６（ＵＳ，Ａ１）
米国特許出願公開第２０１５／０３７１２２６（ＵＳ，Ａ１）
米国特許出願公開第２０１４／０２８９８３３（ＵＳ，Ａ１）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／４４
Ｇ０６Ｆ ２１／６０－２１／６４

G06Q 20/38