(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5927681号
(P5927681)
(45)発行日　平成28年6月1日(2016.6.1)　(24)登録日　平成28年5月13日(2016.5.13)

(51)Int.Cl.		F I		
G06F 21/33	(2013.01)	G06F	21/33	
G06F 21/34	(2013.01)	G06F	21/34	
H04L 9/32	(2006.01)	H04L	9/00	675B

請求項の数 28　(全 16 頁)

(21)出願番号	特願2014-550249 (P2014-550249)
(86)(22)出願日	平成23年12月28日 (2011.12.28)
(65)公表番号	特表2015-509234 (P2015-509234A)
(43)公表日	平成27年3月26日 (2015.3.26)
(86)国際出願番号	PCT/US2011/067532
(87)国際公開番号	WO2013/100954
(87)国際公開日	平成25年7月4日 (2013.7.4)
審査請求日	平成26年7月3日 (2014.7.3)

(73)特許権者　591003943
インテル・コーポレーション
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　バクシ、サンジェイ
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内

最終頁に続く

(54)【発明の名称】ネットワークアクセスに関連したアプリケーションのための認証

(57)【特許請求の範囲】
【請求項１】
コントローラであって、
当該コントローラのユーザによる操作に応じて認証要求のための入力信号を受け、
前記認証要求のための入力信号に応じて、リモート認証プロバイダによって生成された識別パケットを、近接場通信リンクを介して受信し、
当該コントローラに結合された電子デバイス上に安全なウィンドウを表示させ、
前記ウィンドウ内での前記ユーザの操作に応じてログイン許可のための入力信号を受け、
前記ログイン許可のための入力信号に応じて前記識別パケットに電子署名を関連づけ、
前記リモート認証プロバイダに前記識別パケットを送信し、
前記リモート認証プロバイダから許可を受信し、
前記識別パケットに関連づけられたログイン情報を受信し、
前記ログイン情報を使用してログイン手順を開始する
ための論理を備えるコントローラ。
【請求項２】
前記論理は、リモートデバイスと通信するための近接場ワイヤレス通信インターフェースを備える、請求項１に記載のコントローラ。
【請求項３】
開始入力信号を検出するための論理をさらに備える、請求項１または２に記載のコント

ローラ。
【請求項４】
前記識別パケットは、前記リモート認証プロバイダによって発行されたカードに関連づけられたデータを備え、
前記開始入力信号は、前記カードが当該コントローラの所定の物理的近傍内にあることに応答して生成される、
請求項３に記載のコントローラ。
【請求項５】
当該コントローラと前記リモート認証プロバイダとの間に安全な通信チャネルを作成するための論理をさらに備える、請求項１から４のいずれか１項に記載のコントローラ。
【請求項６】
前記ユーザからトランザクション許可を得るための論理をさらに備える、請求項１から５のいずれか１項に記載のコントローラ。
【請求項７】
前記電子デバイスにログインクレデンシャルを提供するための論理をさらに備える、請求項１から６のいずれか１項に記載のコントローラ。
【請求項８】
電子デバイスであって、
信頼できないコンピューティング環境を実現するオペレーティングシステムを実行するプロセッサと、
コントローラと
を備え、前記コントローラは、
メモリと、
論理と
を備え、前記論理は、
当該電子デバイスのユーザによる操作に応じて認証要求のための入力信号を受け、
前記認証要求のための入力信号に応じて、リモート認証プロバイダによって生成された識別パケットを、近接場通信リンクを介して受信し、
当該電子デバイス上に安全なウィンドウを表示させ、
前記ウィンドウ内での前記ユーザの操作に応じてログイン許可のための入力信号を受け、
前記ログイン許可のための入力信号に応じて前記識別パケットに電子署名を関連づけ、
前記リモート認証プロバイダに前記識別パケットを送信し、
前記リモート認証プロバイダから許可を受信し、
前記識別パケットに関連づけられたログイン情報を受信し、
前記ログイン情報を使用してログイン手順を開始する
ためのものである、電子デバイス。
【請求項９】
前記論理は、リモートデバイスと通信するための近接場ワイヤレス通信インターフェースを備える、請求項８に記載の電子デバイス。
【請求項１０】
開始入力信号を検出するための論理をさらに備える、請求項８または９に記載の電子デバイス。
【請求項１１】
前記識別パケットは、前記リモート認証プロバイダによって発行されたカードに関連づけられたデータを備え、
前記開始入力信号は、前記カードが前記コントローラの所定の物理的近傍内にあることに応答して生成される、
請求項１０に記載の電子デバイス。
【請求項１２】

前記コントローラと前記リモート認証プロバイダとの間に安全な通信チャネルを作成するための論理をさらに備える、請求項８から１１のいずれか１項に記載の電子デバイス。
【請求項１３】
前記ユーザからトランザクション許可を得るための論理をさらに備える、請求項８から１２のいずれか１項に記載の電子デバイス。
【請求項１４】
当該電子デバイスにログインクレデンシャルを提供するための論理をさらに備える、請求項８から１３のいずれか１項に記載の電子デバイス。
【請求項１５】
方法であって、
コントローラが、前記コントローラのユーザによる操作に応じて認証要求のための入力信号を受けることと、
前記認証要求のための入力信号に応じて、リモート認証プロバイダによって生成された識別パケットを、近接場通信リンクを介して前記コントローラが受信することと、
前記コントローラが、前記コントローラに結合された電子デバイス上に安全なウィンドウを表示させることと、
前記コントローラが前記ウィンドウ内での前記ユーザの操作に応じてログイン許可のための入力信号を受けることと、
前記ログイン許可のための入力信号に応じて前記コントローラが前記識別パケットに電子署名を関連づけることと、
前記コントローラが前記リモート認証プロバイダに前記識別パケットを送信することと、
前記コントローラが前記リモート認証プロバイダから許可を受信することと、
前記コントローラが、前記識別パケットに関連づけられたログイン情報を受信することと、
前記コントローラが前記ログイン情報を使用してログイン手順を開始することと
を備える方法。
【請求項１６】
前記コントローラが開始入力信号を検出することをさらに備える、請求項１５に記載の方法。
【請求項１７】
前記識別パケットは、前記リモート認証プロバイダによって発行されたカードに関連づけられたデータを備え、
前記開始入力信号は、前記カードが前記コントローラの所定の物理的近傍内にあることに応答して生成される、
請求項１６に記載の方法。
【請求項１８】
前記コントローラが前記コントローラと前記リモート認証プロバイダとの間に安全な通信チャネルを作成することをさらに備える、請求項１５から１７のいずれか１項に記載の方法。
【請求項１９】
前記コントローラが前記ユーザからトランザクション許可を得ることをさらに備える、請求項１５から１８のいずれか１項に記載の方法。
【請求項２０】
前記コントローラが前記電子デバイスにログインクレデンシャルを提供することをさらに備える、請求項１５から１９のいずれか１項に記載の方法。
【請求項２１】
非一時的なコンピュータ可読媒体に記憶された論理命令を備えるコンピュータプログラムであって、前記論理命令は、コントローラのプロセッサによって実行された場合に前記プロセッサを、

前記コントローラのユーザによる操作に応じて認証要求のための入力信号を受け、
前記認証要求のための入力信号に応じて、リモート認証プロバイダによって生成された識別パケットを、近接場通信リンクを介して受信し、
前記コントローラに結合された電子デバイス上に安全なウィンドウを表示させ、
前記ウィンドウ内での前記ユーザの操作に応じてログイン許可のための入力信号を受け
ン
前記ログイン許可のための入力信号に応じて前記識別パケットに電子署名を関連づけ、
前記リモート認証プロバイダに前記識別パケットを送信し、
前記リモート認証プロバイダから許可を受信し、
前記識別パケットに関連づけられたログイン情報を受信し、
前記ログイン情報を使用してログイン手順を開始する
ように構成する、コンピュータプログラム。

【請求項２２】

リモートデバイスと通信するための近接場ワイヤレス通信インターフェースを実現するための、非一時的なコンピュータ可読媒体に記憶された論理命令をさらに備える、請求項２１に記載のコンピュータプログラム。

【請求項２３】

開始入力信号を検出するための、非一時的なコンピュータ可読媒体に記憶された論理命令をさらに備える、請求項２１または２２に記載のコンピュータプログラム。

【請求項２４】

前記識別パケットは、前記リモート認証プロバイダによって発行されたカードに関連づけられたデータを備え、
前記開始入力信号は、前記カードが前記コントローラの所定の物理的近傍内にあることに応答して生成される、
請求項２３に記載のコンピュータプログラム。

【請求項２５】

前記コントローラと前記リモート認証プロバイダとの間に安全な通信チャネルを作成するための、非一時的なコンピュータ可読媒体に記憶された論理命令をさらに備える、請求項２１から２４のいずれか１項に記載のコンピュータプログラム。

【請求項２６】

前記ユーザからトランザクション許可を得るための、非一時的なコンピュータ可読媒体に記憶された論理命令をさらに備える、請求項２１から２５のいずれか１項に記載のコンピュータプログラム。

【請求項２７】

前記電子デバイスにログインクレデンシャルを提供するための、非一時的なコンピュータ可読媒体に記憶された論理命令をさらに備える、請求項２１から２６のいずれか１項に記載のコンピュータプログラム。

【請求項２８】

請求項２１から２７の何れか１項に記載のコンピュータプログラムを格納した、コンピュータ可読媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本明細書に説明される主題は、一般的に、ネットワークアクセスの分野に関し、より詳細には、ネットワークアクセスのための認証プロトロコルを実現するためにリモート認証プロバイダが動作させる第三者認証システムを利用することを電子デバイスに可能にさせるシステムおよび方法に関する。

【背景技術】

【０００２】

大企業のネットワークは多くの場合、許可されたユーザによるネットワークへのアクセ

スを可能にする一方で無許可の従業員によるネットワークへのアクセスを禁止または防止する認証技術により、保護されている。中小企業環境は、企業ネットワークの安全化における、より困難な問題に直面する。ビジネスクラスの認証技術は、高価かつ複雑であり、中小企業の経済力および技術力を超えることが多い。

【０００３】

したがって、コンピューティング環境を安全にするための認証手法を提供するためのシステムおよび手法は、特に中小企業環境において、有用性を見出し得る。

【０００４】

詳細な説明が、添付図面を参照して説明される。

【図面の簡単な説明】

【０００５】

【図１】いくつかの実施形態に係る、ネットワークアクセスのための認証を実現するためのインフラストラクチャを含むように適合し得る例示的な電子デバイスの模式図である。

【図２】いくつかの実施形態に係る、ネットワークアクセスのための認証のための例示的なアーキテクチャのハイレベルな模式図である。

【図３】いくつかの実施形態に係る、ネットワークアクセスのための認証のための例示的なアーキテクチャの模式図である。

【図４】いくつかの実施形態に係る、ネットワークアクセスのための認証のための例示的なシステムの模式図である。

【図５】いくつかの実施形態に係る、ネットワークアクセスのための認証を実現するための方法における動作を示すフローチャートである。

【発明を実施するための形態】

【０００６】

本明細書に説明されるのは、電子デバイスにおいてネットワークアクセスのための認証を実現するための例示的なシステムおよび方法である。本明細書に説明されるシステムおよび方法のいくつかの実施形態は、ネットワークセキュリティのコンテキストで、また、特に中小企業環境において、有用性を見出し得る。本明細書に説明されるいくつかの実施形態は、第三者によって提供されるさまざまな認証プラットフォームの活用を中小企業に可能にさせることができるので、第三者がリモート認証プロバイダとして機能する。例として、システムのユーザは、第三者または当事者によって発行されたクレデンシャルを含み得る識別パケットを割り当てられ得る。識別パケットは、適切な記憶場所、例えば、磁気ストリップカード、スマートカード、または、電子デバイスに関連づけられたメモリモジュールに記憶され得る。

【０００７】

ネットワークへのアクセスを望むユーザが、電子デバイスを介してログイン手順を開始し得る。ログイン手順中、識別パケットは、電子デバイスからリモート認証プロバイダに、安全な通信チャネルを通じて送信され得る。リモート認証プロバイダは、識別パケット中のデータを使用して１つ又は複数の認証ルーチンを実現することができ、ユーザがネットワークアクセスを許可されることを確定する、または、拒否する、のいずれかである応答を戻し得る。応答に基づいて、電子デバイスは次に、ネットワークへのログイン手順を、完了する、または、中止する、のいずれかである。

【０００８】

本明細書は、ネットワークアクセスのための認証が実現され得るハードウェアおよびソフトウェア環境の説明、およびネットワークアクセスのための認証を実現するための例示的な動作の説明を提供する。以下の説明では、多数の特定の詳細が、さまざまな実施形態の完全な理解を提供するために説明される。しかしながら、さまざまな実施形態が特定の詳細なしに実現され得ることが、当業者によって理解されるだろう。他の例では、周知の方法、手順、コンポーネント、および回路は、特定の実施形態を曖昧にしないように、詳細に例示または説明されない。

【０００９】

図１は、いくつかの実施形態に係る、ネットワークアクセスのための認証を実現するように適合し得る例示的な電子デバイス１１０の模式図である。図１に示すように、電子デバイス１１０は、携帯電話、タブレットコンピュータ、ポータブルコンピュータ、または携帯情報端末（ＰＤＡ）といった、従来のモバイルデバイスとして具体化され得る。

【００１０】

いくつかの実施形態において、電子デバイスは、信頼できる実行環境を含むことができ、それはまた、信頼できる実行エンジン、または時に、安全なエレメントまたは管理容易性エンジンとも呼ばれ得る。信頼できる実行環境は、信頼できない実行環境と時に呼ばれる一次実行環境から分離された、１つ又は複数のコントローラを備え得る。分離は、信頼できる実行環境が信頼できない実行環境から物理的に分離され得るという意味で、物理的であり得る。あるいは、信頼できる実行環境は、信頼できる実行環境が、信頼できない実行環境をホストする同一のチップまたはチップセット上でホストされ得るが、信頼できる実行環境が安全であるようにシリコンレベルで分離され得る、という意味で、論理的であり得る。

【００１１】

さまざまな実施形態において、電子デバイス１１０は、ディスプレイ、１つ又は複数のスピーカー、キーボード、１つ又は複数の他のＩ／Ｏデバイス、マウス、等を含む１つ又は複数の付属の入力／出力デバイスを含むことができ、または、これらに結合されることができる。例示的なＩ／Ｏデバイスは、タッチスクリーン、音声起動入力デバイス、トラックボール、ジオロケーションデバイス、加速度計／ジャイロスコープ、バイオメトリックフィーチャー入力デバイス、および、ユーザからの入力を受信することを電子デバイス１１０に可能にさせる任意の他のデバイスを含み得る。

【００１２】

電子デバイス１１０は、システムハードウェア１２０と、ランダムアクセスメモリおよび／または読み出し専用メモリとして実現され得るメモリ１４０と、を含む。ファイルストアが、コンピューティングデバイス１１０に通信可能に結合され得る。ファイルストアは、例えば、ｅＭＭＣ、ＳＳＤ、１つ又は複数のハードドライブ、または他のタイプのストレージデバイスのように、コンピューティングデバイス１１０の内部にあり得る。ファイルストア１８０はまた、例えば、１つ又は複数の外部のハードドライブ、ネットワーク接続ストレージ、または分離したストレージネットワークのように、コンピュータ１１０の外部にあり得る。

【００１３】

システムハードウェア１２０は、１つ又は複数のプロセッサ１２２、グラフィックスプロセッサ１２４、ネットワークインターフェース１２６、およびバス構造１２８を含み得る。一実施形態において、プロセッサ１２２は、Ｉｎｔｅｌ　Ｃｏｒｐｏｒａｔｉｏｎ，Ｓａｎｔａ　Ｃｌａｒａ，Ｃａｌｉｆｏｒｎｉａ，ＵＳＡから入手可能な、Ｉｎｔｅｌ（登録商標）Ａｔｏｍ（登録商標）プロセッサ、Ｉｎｔｅｌ（登録商標）Ａｔｏｍ（登録商標）ベースのシステムオンチップ（ＳＯＣ）、またはＩｎｔｅｌ（登録商標）Ｃｏｒｅ２Ｄｕｏ（登録商標）プロセッサとして、具体化され得る。本明細書において使用される場合、「プロセッサ」という用語は、マイクロプロセッサ、マイクロコントローラ、複数命令セットコンピューティング（ＣＩＳＣ）マイクロプロセッサ、縮小命令セットコンピュータ（ＲＩＳＣ）マイクロプロセッサ、超長命令語（ＶＬＩＷ）マイクロプロセッサ、または任意の他のタイプのプロセッサまたは処理回路といった、しかしこれらに限定されない、任意のタイプの計算エレメントを意味する。

【００１４】

グラフィックスプロセッサ１２４は、グラフィックスおよび／またはビデオ動作を管理する付加的なプロセッサとして機能し得る。グラフィックスプロセッサ１２４は、電子デバイス１１０のマザーボード上に組み込まれることができ、または、マザーボード上に拡張スロットを介して結合され得る。

【００１５】

一実施形態において、ネットワークインターフェース１２６は、イーサネット（登録商標）インターフェースのような有線インターフェース（例えば、Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ／ＩＥＥＥ ８０２．３－２００２を参照）、または、ＩＥＥＥ８０２．１１ａ、ｂ、またはｇに準拠したインターフェースのようなワイヤレスインターフェース（例えば、ＩＥＥＥ Ｓｔａｎｄａｒｄ ｆｏｒ ＩＴ－Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ ａｎｄ ｉｎｆｏｒｍａｔｉｏｎ ｅｘｃｈａｎｇｅ ｂｅｔｗｅｅｎ ｓｙｓｔｅｍｓ ＬＡＮ／ＭＡＮ－－Ｐａｒｔ ＩＩ：Ｗｉｒｅｌｅｓｓ ＬＡＮ Ｍｅｄｉｕｍ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ（ＭＡＣ）ａｎｄ Ｐｈｙｓｉｃａｌ Ｌａｙｅｒ（ＰＨＹ）ｓｐｅｃｉｆｉｃａｔｉｏｎｓ Ａｍｅｎｄｍｅｎｔ ４：Ｆｕｒｔｈｅｒ Ｈｉｇｈｅｒ Ｄａｔａ Ｒａｔｅ Ｅｘｔｅｎｓｉｏｎ ｉｎ ｔｈｅ ２．４ＧＨｚ Ｂａｎｄ，８０２．１１Ｇ－２００３を参照）であり得る。ワイヤレスインターフェースの別の例は、汎用パケット無線サービス（ＧＰＲＳ）インターフェース（例えば、Ｇｕｉｄｅｌｉｎｅｓ ｏｎ ＧＰＲＳ Ｈａｎｄｓｅｔ Ｒｅｑｕｉｒｅｍｅｎｔｓ，Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ／ＧＳＭ（登録商標） Ａｓｓｏｃｉａｔｉｏｎ，Ｖｅｒ．３．０．１，Ｄｅｃｅｍｂｅｒ ２００２を参照）であろう。

【００１６】

バス構造１２８は、システムハードウェア１２０のさまざまなコンポーネントを接続する。一実施形態において、バス構造１２８は、１１ビットバス、業界標準アーキテクチャ（ＩＳＡ）、マイクロチャネルアーキテクチャ（ＭＳＡ）、拡張ＩＳＡ（ＥＩＳＡ）、インテリジェントドライブエレクトロニクス（ＩＤＥ）、ＶＥＳＡローカルバス（ＶＬＢ）、ペリフェラルコンポーネントインターコネクト（ＰＣＩ）、ユニバーサルシリアルバス（ＵＳＢ）、アドバンストグラフィックスポート（ＡＧＰ）、パーソナルコンピュータメモリカード国際協会バス（ＰＣＭＣＩＡ）、および小型コンピュータシステムインターフェース（ＳＣＳＩ）、高速同期シリアルインターフェース（ＨＳＩ）、シリアル低電力チップ間メディアバス（ＳＬＩＭｂｕｓ（登録商標））、等を含むがこれらに限定されない、任意のさまざまな利用可能なバスアーキテクチャを使用する、メモリバス、ペリフェラルバス、または外部バス、および／または、ローカルバスを含む、いくつかのタイプのバス構造の１つ又は複数であり得る。

【００１７】

電子デバイス１１０は、ＲＦ信号を送受信するためのＲＦトランシーバ１３０と、近接場通信（ＮＦＣ）ラジオ１３４と、ＲＦトランシーバ１３０によって受信された信号を処理するためのシグナルプロセッシングモジュール１３２と、を含み得る。ＲＦトランシーバは、例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）または８０２．１１Ｘ、ＩＥＥＥ８０２．１１ａ、ｂ、またはｇに準拠したインターフェース（例えば、ＩＥＥＥ Ｓｔａｎｄａｒｄ ｆｏｒ ＩＴ－Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ ａｎｄ ｉｎｆｏｒｍａｔｉｏｎ ｅｘｃｈａｎｇｅ ｂｅｔｗｅｅｎ ｓｙｓｔｅｍｓ ＬＡＮ／ＭＡＮ－－Ｐａｒｔ ＩＩ：Ｗｉｒｅｌｅｓｓ ＬＡＮ Ｍｅｄｉｕｍ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ（ＭＡＣ）ａｎｄ Ｐｈｙｉｓｃａｌ Ｌａｙｅｒ（ＰＨＹ）ｓｐｅｃｉｆｉｃａｔｉｏｎｓ Ａｍｅｎｄｍｅｎｔ ４：Ｆｕｒｔｈｅｒ Ｈｉｇｈｅｒ Ｄａｔａ Ｒａｔｅ Ｅｘｔｅｎｓｉｏｎ ｉｎ ｔｈｅ ２．４ＧＨｚ Ｂａｎｄ，８０２．１１Ｇ－２００３を参照）といったプロトコルを介したローカルワイヤレス接続を実現し得る。ワイヤレスインターフェースの別の例は、ＷＣＤＭＡ、ＬＴＥ、汎用パケット無線サービス（ＧＰＲＳ）インターフェース（例えば、Ｇｕｉｄｅｌｉｎｅｓ ｏｎ ＧＰＲＳ Ｈａｎｄｓｅｔ Ｒｅｑｕｉｒｅｍｅｎｔｓ，Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ／ＧＳＭ（登録商標） Ａｓｓｏｃｉａｔｉｏｎ，Ｖｅｒ．３．０．１，Ｄｅｃｅｍｂｅｒ ２００２を参照）であろう。

【００１８】

電子デバイス１１０はさらに、例えばキーパッド１３６およびディスプレイ１３８のよ

うな、１つ又は複数の入力／出力インターフェースを含み得る。いくつかの実施形態において、電子デバイス１１０は入力のために、キーパッドを有さずにタッチパネルを使用し得る。

【００１９】

メモリ１４０は、コンピューティングデバイス１１０の動作を管理するためのオペレーティングシステム１４２を含み得る。一実施形態において、オペレーティングシステム１４２は、システムハードウェア１２０へのインターフェースを提供するハードウェアインターフェースモジュール１５４を含む。加えて、オペレーティングシステム１４２は、コンピューティングデバイス１１０の動作において使用されるファイルを管理するファイルシステム１５０と、コンピューティングデバイス１１０上で実行する処理を管理する処理制御サブシステム１５２と、を含み得る。

【００２０】

オペレーティングシステム１４２は、リモートソースからのデータパケットおよび／またはデータストリームを送受信するためにシステムハードウェア１２０と共に動作し得る１つ又は複数の通信インターフェース１４６を含み（または管理し）得る。オペレーティングシステム１４２はさらに、オペレーティングシステム１４２とメモリ１４０に常駐している１つ又は複数のアプリケーションモジュールとの間のインターフェースを提供する、システム呼び出しインターフェースモジュール１４４を含み得る。オペレーティングシステム１４２は、ＵＮＩＸ（登録商標）オペレーティングシステムまたはその任意の派生物（例えば、Ｌｉｎｕｘ（登録商標）、Ａｎｄｒｏｉｄ、等）として、または、Ｗｉｎｄｏｗｓ（登録商標）ブランドのオペレーティングシステムまたは他のオペレーティングシステムとして、具体化され得る。

【００２１】

電子デバイス１１０は、信頼できる実行エンジン１７０を備え得る。いくつかの実施形態では、信頼できる実行エンジン１７０は、電子デバイス１１０のマザーボード上に存在する独立した集積回路として実装されることができ、その一方で他の実施形態では、信頼できる実行エンジン１７０は、同一のＳＯＣチップ上の専用プロセッサブロックとして実装されることができ、その一方で他の実施形態では、信頼できる実行エンジンは、HW強制メカニズムを使用してプロセッサの他の部分から隔離されたプロセッサ１２２の一部分に実装されることができる。

【００２２】

図１に示す実施形態において、信頼できる実行エンジン１７０は、プロセッサ１７２、メモリモジュール１７４、１つ又は複数の認証モジュール１７６、およびＩ／Ｏモジュール１７８、近接場通信（ＮＦＣ）モジュール、ｗｈａｔ　ｙｏｕ　ｓｅｅ　ｉｓ　ｗｈａｔ　ｙｏｕ　ｓｉｇｎ（ＷＹＳＩＷＹＳ）モジュール１８２、エンハンストプライバシー識別（ＥＰＩＤ）モジュール１８４、および１つ又は複数のアプリケーションプロキシ１８６を備える。いくつかの実施形態において、メモリモジュール１７４は、永続的なフラッシュメモリモジュールを備えることができ、さまざまな機能モジュールが、永続的なメモリモジュールにおいて符号化された論理命令、例えばファームウェアまたはソフトウェア、として実現されることができる。Ｉ／Ｏモジュール１７８は、シリアルＩ／ＯモジュールまたはパラレルＩ／Ｏモジュールを備え得る。信頼できる実行エンジン１７０はメインプロセッサ１２２およびオペレーティングシステム１４２から分離されているので、信頼できる実行エンジン１７０は、安全にされることができ、すなわち、典型的にホストプロセッサ１２２からＳＷ攻撃を展開するハッカーにアクセス不可能にされることができる。

【００２３】

いくつかの実施形態において、信頼できる実行エンジンは、ネットワークアクセス手順のための認証が実現され得るホスト電子デバイスにおいて、信頼できる実行環境を定義し得る。図２は、いくつかの実施形態に係る、ネットワークアクセスのための認証のための例示的なアーキテクチャのハイレベルな模式図である。図２を参照すると、ホストデバイ

ス２１０は、信頼できない実行環境と信頼できる実行環境とを有するものとして特徴づけられ得る。ホストデバイス２１０が電子デバイス１１０として具体化される場合、信頼できる実行環境が、信頼できる実行エンジン１７０によって実現され得る一方で、信頼できない実行環境は、システム１００のメインプロセッサ１２２およびオペレーティングシステム１４２によって実現され得る。図２に示すように、図２において発行者２３０として識別されているクレデンシャルを発行するリモートエンティティが、クレデンシャルを供給し、それは、ホストデバイス２１０の信頼できる実行環境において記憶される。使用において、発行されたクレデンシャルおよび１つ又は複数のユーザクレデンシャル２２４が、１つ又は複数の認証アルゴリズム２２２に入力として提供されることができ、１つ又は複数の認証アルゴリズム２２２は、クレデンシャルを処理してトークンを生成し、トークンが、１つ又は複数の信用できる当事者２４０に提供されることができる。信頼できる実行環境の完全性は、信頼できる実行環境とクレデンシャルを２２０に発行することが可能なエンティティとの間の、または、コンテンツのライフサイクル管理２３５と信頼できる実行環境のアルゴリズム２２２との間の、排他的かつ暗号で保護された関係を通して、維持されることができる。

【００２４】

図３は、いくつかの実施形態に係る販売トランザクションの仮想ポイントのための例示的なアーキテクチャのより詳細な模式図である。図３に示す実施形態では、信頼できる実行レイヤは、プロビジョニングおよびライフサイクル管理モジュール３１０、プラットフォームセンサクレデンシャルモジュール３２０、およびクレデンシャルリポジトリ３４０のセット、を備える。トークンアクセス管理モジュール３５２は、信頼できる実行レイヤにおいて記憶された１つ又は複数のトークンアクセス方法および規則３５０を入力として受理する。

【００２５】

図３に示す実施形態において、プラットフォームセンサクレデンシャルは、安全にされたキーボード入力経路クレデンシャル３２２、ＧＰＳロケーションクレデンシャル、バイオメトリッククレデンシャル３２６、加速度計またはジャイロスコープクレデンシャル３２８、またはマルウェアの傍受に耐性のある安全な画面入力メカニズムクレデンシャル３３０、の１つ又は複数を備え得る。クレデンシャルリポジトリ３４０は、ＮＦＣ入力デバイス３４２、１つ又は複数の安全なエレメント３４４、およびクラウドクレデンシャルストアアクセスメカニズム３４６、を備え得る。

【００２６】

信頼できない実行レイヤ（すなわち、ホストオペレーティングシステムレイヤ）は、信頼できる実行レイヤのコンポーネントとの通信を容易にするために、１つ又は複数のプロキシを実現する。したがって、信頼できない実行レイヤは、プロビジョニングおよびライフサイクル管理モジュール３１０と、クレデンシャルのリモート発行者２３０と、信頼できる実行レイヤを安全に管理することを任せられたエンティティ２３５と、の間の通信を容易にするために、ライフサイクル管理プロキシ３６０を維持する。同様に、ホストプロキシ３６２が、信頼できない実行レイヤにおいて実行する１つ又は複数のクライアントアプリケーション３８０とトークンアクセス管理３５２との間の通信を容易にする。永続性プロキシ３６４が、トークンアクセス管理３５２とプラットフォームデータストア３６６との間の通信リンクを提供する。クラウドプロキシ３７０が、クラウドクレデンシャルストア２５０とクラウドストアアクセスメカニズム３４６との間の通信リンクを提供する。

【００２７】

使用において、システムは、さまざまなソースからクレデンシャルを得ることができる。例えば、発行者２３０は、ＬＣＭプロキシ３６０を介してシステムにクレデンシャルを発行することができる。発行されたクレデンシャルは、動的なワンタイムパスワード（ＯＴＰ）生成シード、ユーザ証明書（例えば、公開／秘密鍵のペアを有するｘ５０９証明書）、金融情報（例えば、クレジットカード情報）、銀行カード情報、等を含み得る。発行されたクレデンシャルは、クレデンシャルリポジトリ３４０の１つ又は複数において記憶

され得る。対照的に、プラットフォームセンサクレデンシャル３２０は、信用できる当事者からの要求に応答して、認証処理中にリアルタイムでまたは前もってのいずれかで、ユーザから得られることができる。当業者は、プラットフォームセンサクレデンシャルが、以下に説明するように、信用できる当事者が他のクレデンシャルを求めた結果として間接的に、または、信用できる当事者によって直接的にも、要求され得ることを認識するだろう。例として、バイオメトリック署名が、ユーザのためにカタログに登録されることができ、集中実行型の認証確認システムを可能にする。本明細書に説明される実施形態を使用して、信用できる当事者は、指紋クレデンシャルをプラットフォームに求め得る。プラットフォームは、その指紋収集ハードウェアを使用してこのクレデンシャルを得て、要求している／信用できる当事者にこの情報を戻すだろう。

【００２８】

図４は、いくつかの実施形態に係るネットワークアクセスのための認証のためのシステムの模式図である。図４を参照すると、電子デバイス１１０は、ネットワーク４４０を介して、１つ又は複数のネットワークリソース４２０に、および１つ又は複数の認証サーバ４３０に、結合され得る。電子デバイス１１０は、リモートデバイス、例えば、デビット／クレジットまたはＩＤカード４１０とのワイヤレス通信を可能にする、近接場通信（ＮＦＣ）インターフェースを備え得る。いくつかの実施形態において、電子デバイス１１０は、電子デバイス１１０に関連して上述したように、携帯電話、タブレット、ＰＤＡ、または他のモバイルコンピューティングデバイスとして具体化され得る。ネットワーク４４０は、例えばインターネットのような公衆通信ネットワークとして、またはプライベートな通信ネットワークとして、またはその組み合わせで、具体化され得る。デビット／クレジットまたはＩＤカード４１０は、ユーザを識別する磁気ストリップデータを備え得る。いくつかの実施形態において、磁気ストライプデータは、暗号鍵を使用してラッピングされ得る。

【００２９】

認証サーバ４３０は、コンピュータシステムとして具体化され得る。いくつかの実施形態において、サーバ４３０は、認証サーバとして具体化されることができ、ベンダーによって、または、安全なプラットフォームを動作させる第三者によって、管理され得る。認証サーバ４３０は、ベンダーによって、または、例えばトランザクション手形交換サービスまたはクレジットカードサービスといった、第三者支払いシステムによって、動作させられ得る。

【００３０】

ネットワークアクセスのための認証のためのシステムのさまざまな構造を説明してきたが、そのようなシステムの動作態様が、いくつかの実施形態に係るネットワークアクセスのための認証を実現するための方法における動作を示すフローチャートである、図５を参照して説明される。いくつかの実施形態において、図５のフローチャートに示す動作は、図１に示した信頼できる実行エンジン１７０のさまざまなモジュール１７６により、単独で、または、電子デバイスのオペレーティングシステム上で実行し得るソフトウェアモジュールとの組み合わせで、実現され得る。

【００３１】

図５を参照すると、いくつかの実施形態において、図５に示す動作は、ユーザに、認証サーバ４３０によって提供される第三者認証能力を活用することによってネットワークアクセスのための認証を実現することを可能にさせる。いくつかの実施形態において、電子デバイスは、図１～５に示す信頼できる実行エンジンを備えるハンドヘルドコンピューティングデバイスとして具体化されることができる。同様に、認証サーバは、図１～５に示す信頼できる実行エンジンを備えるコンピューティングデバイスとして具体化されることができる。図５を参照すると、動作５１０で、認証要求が電子デバイスによって受信される。例として、いくつかの実施形態において、認証要求は、ユーザが、例えば、電子デバイス１１０上で磁気ストライプデータカードをタップすること、またはそうでなければ、認証アプリケーションを起動することによって、ログインシーケンスを開始することによ

り、開始され得る。認証要求に応答して、信頼できる実行エンジン１７０のプロセッサ１７２は、認証モジュール１７６を起動する。

【００３２】

動作５１５で、電子デバイスは、近接場通信（ＮＦＣ）通信リンクを介して第三者識別パケットを受信する。例として、いくつかの実施形態において、認証モジュール１７６は、ＮＦＣモジュール１８０を呼び出して安全な通信リンクを開始し、信頼できる実行エンジン上のＩ／Ｏインターフェースを介して、磁気ストライプデータカード上の磁気ストライプデータ上に符号化された識別パケットを検索する。Ｉ／Ｏ動作が信頼できる実行エンジンから実行されるため、磁気ストライプカードから検索されたデータは、決して電子デバイスのオペレーティングシステムにさらされず、したがって、悪意のあるアクセスから安全である。

【００３３】

動作５２０で、電子デバイスは、ログイン許可を受信する。例として、いくつかの実施形態において、ＷＹＳＩＷＹＳモジュール１８２が、電子デバイスのディスプレイ上に安全なウィンドウを開き、そのウィンドウ上に許可要求を提示する。電子デバイスのユーザは、安全なウィンドウ中に入力を入力することによって許可要求に応答し、それは、ログイン要求を許可する。ＷＹＳＩＷＹＳモジュール１８２は、入力に関連づけられたピンを生成する。

【００３４】

動作５２５で、識別パケットは、リモート認証プロバイダへのトランスポートのために、署名およびラッピングされる。例として、いくつかの実施形態において、認証モジュール１７６は、ＥＰＩＤモジュールを呼び出し、ＥＰＩＤモジュールは、識別パケットをラッピングし、パケットがＮＦＣ通信リンクによって安全に得られたこと、ＷＹＳピンがＷＹＳＩＷＹＳモジュールを使用して安全に得られたこと、を証明する署名を適用する。

【００３５】

動作５３０で、電子デバイス１１０は、ラッピングされた識別パケットをリモート認証サーバ４３０に転送し、リモート認証サーバ４３０が動作５３５でパケットを受信する。例として、いくつかの実施形態において、認証モジュール１７６は、識別パケット中のデータを使用してリモート認証サーバ４３０との安全なエンドツーエンドセッションを確立し、リモート認証プロバイダ４３０によってユーザのアカウント情報を得る。

【００３６】

動作５４０で、リモート認証プロバイダ４３０は、識別パケットによって提供されたデータを使用して、ユーザを認証および許可する。例として、いくつかの実施形態において、リモート認証プロバイダ４３０は、ユーザが認証であることを確認し、識別パケット中のデータの不正使用を検出および／または禁止するための１つ又は複数のアンチ不正処理を実行し得る。リモート認証サーバ４３０は、電子デバイス１１０に許可応答を戻す。

【００３７】

動作５４５で、電子デバイス１１０は、許可応答を受信する。例として、いくつかの実施形態において、応答は、信頼できる実行エンジン１７０におけるＩ／Ｏインターフェース１７８を介して受信されるので、電子デバイス１１０の信頼できない動作環境にとってアクセス可能ではない。

【００３８】

動作５５０で、認証モジュール１７６は、リモート認証プロバイダからの応答を綿密に調べる。動作５５０で、リモート認証サーバ４３０からの応答が、ログインが許可されなかったことを示す場合には、制御は動作５５５に進み、ログイン手順は中止され、アクセスは拒否される。対照的に、動作５５０で、リモート認証サーバ４３０からの応答が、ログインが許可されたことを示す場合には、制御は動作５６０に進み、ユーザのためのログイン情報が検索される。例として、いくつかの実施形態において、認証モジュール１７６は、識別パケット中のデータに関連づけられたアカウント情報へのネットワークユーザおよびドメインからのマッピングを含むローカルデータベースを探索する。

【００３９】
動作５６５で、ログイン情報は、認証モジュール１７６からホストプロキシに送られる。ログイン情報の特定の形態は、要求されたログインのタイプに応じたものであり得る。例として、ローカルログインが要求された場合には、ローカルログインクレデンシャルが戻される。対照的に、ドメインログインが要求された場合には、ドメインログインクレデンシャルが戻される。同様に、ウェブログインが要求された場合には、ウェブクレデンシャルが戻される。ホストプロキシは、適切なバックエンドサービスへの接続を確立してクレデンシャルを供給し、動作５７０で、ノーマルログイン手順が実現され得る。

【００４０】
いくつかの実施形態において、サービスプロバイダ４３０は、認証サービスを提供する第三者サービスプロバイダによって管理され得る。例として、いくつかの実施形態において、クレジットカード４１０は、ＶＩＳＡによって発行されることができ、ＶＩＳＡネットワークが、認証および不正検出サービスを提供するために利用され得る。当業者は、代替のサービスプロバイダが利用され得ることを認識するだろう。

【００４１】
このように、本明細書には、電子デバイスにおいてネットワークアクセスのための認証を実現するためのアーキテクチャおよび関連づけられた方法が説明されている。いくつかの実施形態において、アーキテクチャは、トランザクションが許可された個人によって行われているという保証を、トランザクションを許可する当事者に提供するために、電子デバイスのプラットフォームに組み込まれたハードウェア能力を使用する。本明細書に説明された実施形態において、認証および永続性は、ホストオペレーティングシステムから分離された、信頼できる環境内で行われる処理に基づいている。実行環境は、信頼できる実行エンジンにおいて実現されることができ、信頼できる実行エンジンは、ユーザ識別を得て確認し、次に識別確認のプルーフを提供し、トランザクション要件を満足するために要求される他のエレメントを提供し得る。結果は、信用できる当事者に対し、要求されたこれらのエレメントの履行を表す、プラットフォーム発行のトークンである。いくつかの実施形態において、信頼できる実行エンジンは、リモートまたは取り付け可能なデバイス、例えばドングル、に実装されることができる。

【００４２】
本明細書で言及される「論理命令」という用語は、１つ又は複数の論理演算を実行するための１つ又は複数の機械によって理解され得る式に関する。例えば、論理命令は、１つ又は複数のデータオブジェクトに対し１つ又は複数の演算を実行するためのプロセッサコンパイラによって解釈可能な命令を備え得る。しかしながら、これは単に機械可読命令の例にすぎず、実施形態はこの点について限定されない。

【００４３】
本明細書で言及される「コンピュータ可読媒体」という用語は、１つ又は複数の機械によって認知可能な式を維持することができる媒体に関する。例えば、コンピュータ可読媒体は、コンピュータ可読命令またはデータを記憶するための１つ又は複数のストレージデバイスを備え得る。そのようなストレージデバイスは、例えば、光学、磁気、または半導体記憶媒体といった、記憶媒体を備え得る。しかしながら、これは単にコンピュータ可読媒体の例にすぎず、実施形態はこの点について限定されない。

【００４４】
本明細書で言及される「論理」という用語は、１つ以上の論理演算を実行するための構造に関する。例えば、論理は、１つ又は複数の入力信号に基づいて１つ又は複数の出力信号を提供する回路を備え得る。そのような回路は、デジタル入力を受信してデジタル出力を提供する有限状態機械、または、１つ又は複数のアナログ入力信号に応答して１つ又は複数のアナログ出力信号を提供する回路、を備え得る。そのような回路は、特定用途向け集積回路（ＡＳＩＣ）またはフィールドプログラマブルゲートアレイ（ＦＰＧＡ）において提供され得る。また、論理は、機械可読命令を備えることができ、機械可読命令は、そのような機械可読命令を実行するための処理回路との組み合わせでメモリに記憶される。

しかしながら、これらは単に論理を提供し得る構造の例にすぎず、実施形態はこの点について限定されない。

【００４５】

本明細書に説明された方法のいくつかは、コンピュータ可読媒体上の論理命令として具体化され得る。プロセッサ上で実行された場合、論理命令は、プロセッサが、説明された方法を実現する専用機械としてプログラムされるようにする。プロセッサは、本明細書に説明された方法を実行するように論理命令によって構成された場合、説明された方法を実行するための構造を構成する。あるいは、本明細書に説明された方法は、例えば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、特定用途向け集積回路（ＡＳＩＣ）、等での論理に縮小されることができる。

【００４６】

説明および請求項において、「結合された」および「接続された」という用語が、それらの派生物と共に使用され得る。特定の実施形態において、「接続された」は、２つ以上のエレメントが互いに、直接的に物理的に接触しているか、または電気的に接触していることを示すために使用され得る。「結合された」は、２つ以上のエレメントが直接的に物理的に接触しているか、または電気的に接触していることを意味し得る。しかしながら、「結合された」もまた、２つ以上のエレメントが、互いに直接的に接触していないが、それでも互いに協調またはインタラクトし得ることを意味し得る。

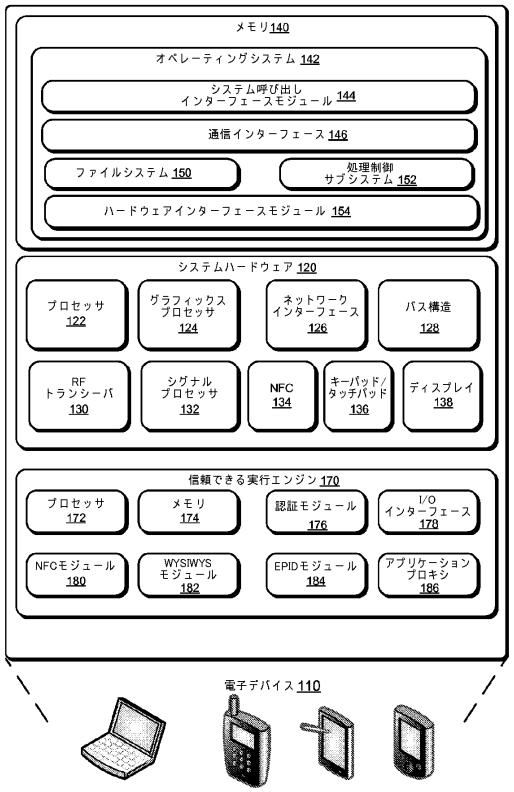
【００４７】

本明細書における「一実施形態」または「いくつかの実施形態」への言及は、実施形態に関連して説明された特定の特徴、構造、または特色が、少なくとも実現に含まれることを意味する。本明細書におけるさまざまな箇所での「一実施形態において」というフレーズの登場は、すべてが同一の実施形態への言及であることもできるし、またはそうでないこともできる。

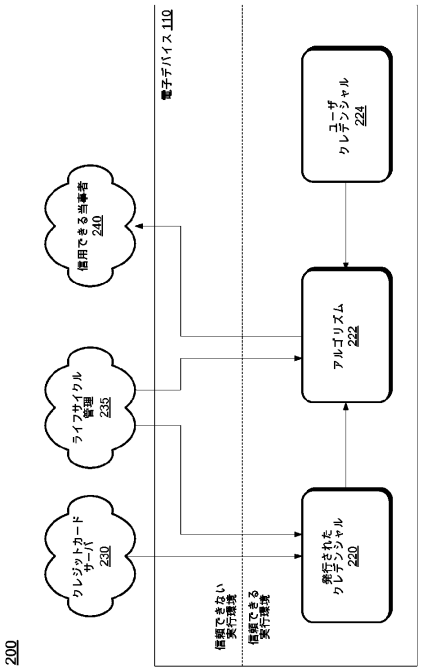
【００４８】

実施形態が構造的な特徴および／または方法の動作に固有の表現で説明されたが、特許請求される主題が説明された特定の特徴または動作に限定され得ないことが理解されるべきである。むしろ、特定の特徴および動作は、特許請求される主題を実現する例示的な形態として開示されている。

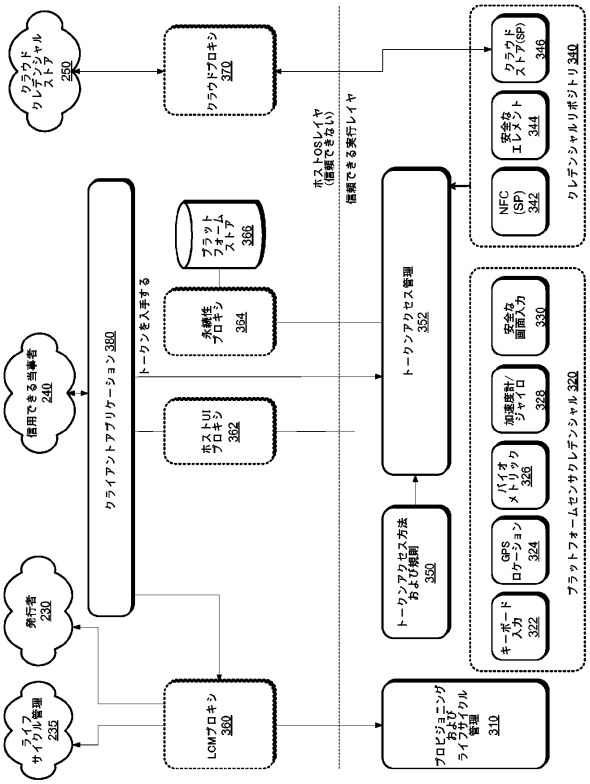
【図１】


メモリ140
オペレーティングシステム 142
システム呼び出し
インターフェースモジュール 144
通信インターフェース 146
ファイルシステム 150
処理制御
サブシステム 152
ハードウェアインターフェースモジュール 154
システムハードウェア 120
プロセッサ 122
グラフィックス プロセッサ 124
ネットワーク インターフェース 126
バス構造 128
RF トランシーバ 130
シグナル プロセッサ 132
NFC 134
キーパッド/ タッチパッド 136
ディスプレイ 138
信頼できる実行エンジン 170
プロセッサ 172
メモリ 174
認証モジュール 176
I/O インターフェース 178
NFCモジュール 180
WYSIWYS モジュール 182
EPIDモジュール 184
アプリケーション プロキシ 186
電子デバイス 110

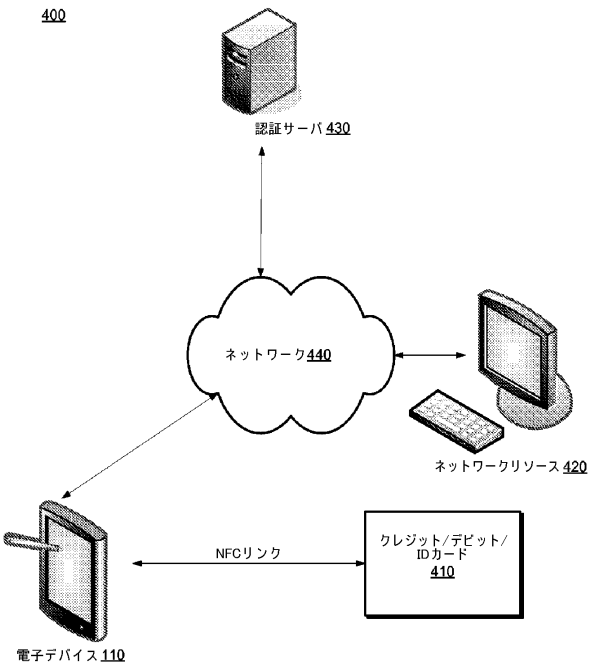
【図２】


電子デバイス 110
ユーザ クレデンシャル 224
信用できる当事者 240
アルゴリズム 222
ライフサイクル 管理 235
クレジットカード サーバ 230
発行された クレデンシャル 220
信頼できない 実行環境
信頼できる 実行環境
200

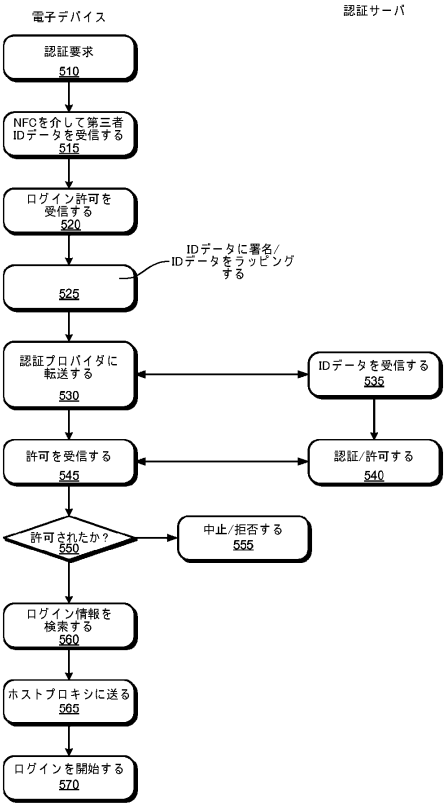
【図３】


クラウド クレデンシャル ストア 250
クラウドプロキシ 370
ホストOSレイヤ (信頼できない)
信頼できる実行レイヤ
クラウド ストア(SP) 346
安全な エレメント 344
NFC (SP) 342
クレデンシャルリポジトリ 340
プラットフォーム ストア 366
永続性 プロキシ 364
トークンを入手する
トークンアクセス管理 352
信用できる当事者 240
クライアントアプリケーション 380
ホストUI プロキシ 362
安全な 画面入力 330
加速度計/ ジャイロ 328
バイオ メトリック 326
GPS ロケーション 324
キーボード 入力 322
プラットフォームセンサクレデンシャル 320
発行者 230
トークンアクセス方法 および規則 350
ライフ サイクル管理 235
LCMプロキシ 360
プロビジョニング クライアント ライフサイクル 管理 310

【図４】


400
認証サーバ 430
ネットワーク 440
ネットワークリソース 420
NFCリンク
クレジット/デビット/ IDカード 410
電子デバイス 110

【図５】


電子デバイス
認証サーバ
認証要求
510
NFCを介して第三者IDデータを受信する
515
ログイン許可を受信する
520
IDデータに署名/IDデータをラッピングする
525
認証プロバイダに転送する
530
IDデータを受信する
535
許可を受信する
545
認証/許可する
540
許可されたか?
550
中止/拒否する
555
ログイン情報を検索する
560
ホストプロキシに送る
565
ログインを開始する
570

フロントページの続き

(72)発明者　スミス、ネッド
アメリカ合衆国　９５０５４　カリフォルニア州・サンタクララ・ミッション　カレッジ　ブーレバード・２２００　インテル・コーポレーション内

審査官　岸野　徹

(56)参考文献　特開２０１０－２３８０９０（ＪＰ，Ａ）
特開２００６－２７７１９９（ＪＰ，Ａ）
特表２０１１－５１１３５５（ＪＰ，Ａ）
特開２００７－２４１５９０（ＪＰ，Ａ）
特開２００８－２１７６２６（ＪＰ，Ａ）
特開２０１０－１９８３４１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３３
Ｇ０６Ｆ　２１／３４
Ｈ０４Ｌ　９／３２