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

特許第6788752号
(P6788752)

(45)発行日　令和2年11月25日(2020.11.25)　(24)登録日　令和2年11月4日(2020.11.4)

(51)Int.Cl.		F I		
G06F 21/57	(2013.01)	G06F	21/57	320
G06F 21/60	(2013.01)	G06F	21/60	360
H04L 9/08	(2006.01)	H04L	9/00	601B
G06F 21/31	(2013.01)	G06F	21/31	
G06F 21/44	(2013.01)	G06F	21/44	

請求項の数 15　(全 26 頁)

(21)出願番号　特願2019-547216(P2019-547216)
(86)(22)出願日　平成29年11月14日(2017.11.14)
(65)公表番号　特表2019-537179(P2019-537179A)
(43)公表日　令和1年12月19日(2019.12.19)
(86)国際出願番号　PCT/US2017/061511
(87)国際公開番号　WO2018/089990
(87)国際公開日　平成30年5月17日(2018.5.17)
審査請求日　令和2年7月15日(2020.7.15)
(31)優先権主張番号　62/421,878
(32)優先日　平成28年11月14日(2016.11.14)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/421,852
(32)優先日　平成28年11月14日(2016.11.14)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　519170209
インテグリティ　セキュリティ　サービシーズ　エルエルシー
アメリカ合衆国　９３１０１　カリフォルニア　サンタ　バーバラ　ウエスト　ソラ　ストリート　３００
(74)代理人　110000796
特許業務法人三枝国際特許事務所
(72)発明者　ラティン　ウィリアム　エル.
アメリカ合衆国　９２６１８　カリフォルニア　アーバイン　アーバイン　センター　ドライブ　７５８５　スイート　２５０　シー／オー　インテグリティ　セキュリティ　サービシーズ　エルエルシー

最終頁に続く

(54)【発明の名称】機器の安全なプロビジョニングと管理

(57)【特許請求の範囲】
【請求項１】
コンピュータ化された機器を安全にプロビジョニングするためのシステムであって、
前記コンピュータ化された機器に通信可能に接続され、第１のデジタル資産を受信し、前記第１のデジタル資産を前記コンピュータ化された機器内にロードするように動作可能な第１の安全な配信機器と、
第１の安全な通信チャネルを介して前記第１の安全な配信機器に接続され、前記第１のデジタル資産を生成して条件付きで前記第１の安全な配信機器に送信するように動作可能なデジタル資産管理サーバと、
第２の安全な通信チャネルを介して前記第１の安全な配信機器に接続され、第３の安全な通信チャネルを介して前記デジタル資産管理サーバに接続され、前記第１のデジタル資産を前記第１の安全な配信機器に送信するように前記デジタル資産管理サーバに指示するように動作可能なプロビジョニングコントローラと、
第４の安全な通信チャネルを介して前記デジタル資産管理サーバに接続され、第１の安全な配信機器が切断された後に前記コンピュータ化された機器に通信可能に接続され、第２のデジタル資産を受信し、前記第２のデジタル資産を前記コンピュータ化された機器内にロードするように動作可能な第２の安全な配信機器と、
を含み、
前記プロビジョニングコントローラはさらに、前記第２のデジタル資産を前記第２の安全な配信機器に送信するように前記デジタル資産管理サーバに指示するように動作可能で

あり、
前記第２のデジタル資産が前記コンピュータ化された機器内にロードされた後、前記コンピュータ化された機器は完全に機能し、
前記第２のデジタル資産が前記コンピュータ化された機器にロードされる前に、前記コンピュータ化された機器は機能しないシステム。
【請求項２】
前記システムはさらに、
登録局アプリケーションを実行し、前記登録局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンと、
登録認証局アプリケーションを実行し、前記登録認証局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンと、
偽名認証局アプリケーションを実行し、前記偽名認証局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンと、
第１の連携局アプリケーションを実行し、前記第１の連携局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンと、
第２の連携局アプリケーションを実行し、前記第２の連携局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンとを含む、請求項１に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項３】
前記システムは、
前記登録局アプリケーションを実行する前記１つ以上の仮想マシンと、前記登録認証局を実行する前記１つ以上の仮想マシンと、前記偽名認証局アプリケーションを実行する前記１つ以上の仮想マシンと、前記第１の連携局アプリケーションを実行する前記１つ以上の仮想マシンと、前記第２の連携局アプリケーションを実行する前記１つ以上の仮想マシンとに動作可能に接続されたデータベースをさらに含む、請求項２に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項４】
前記プロビジョニングコントローラに動作可能に接続され、前記コンピュータ化された機器の製造業者を認証し、前記製造業者が前記コンピュータ化された機器のプロビジョニングを管理することを可能にする第１のポータルをさらに含む、請求項１に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項５】
前記プロビジョニングコントローラに動作可能に接続され、前記コンピュータ化された機器の設置業者を認証し、前記設置業者が前記コンピュータ化された機器のプロビジョニングを管理することを可能にする第２のポータルをさらに含む、請求項４に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項６】
前記プロビジョニングコントローラに動作可能に接続され、前記コンピュータ化された機器のレギュレータを認証し、前記レギュレータが前記コンピュータ化された機器のプロビジョニングを管理することを可能にする第３のポータルをさらに含む、請求項１に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項７】
前記プロビジョニングコントローラは、前記コンピュータ化された機器にロードするために前記第１のデジタル資産を前記第１の安全な配信機器に送信するようにさらに動作可能である、請求項１に記載のコンピュータ化された機器を安全にプロビジョニングするた

めのシステム。
【請求項８】
前記第１のデジタル資産は、前記コンピュータ化された機器によって実行される実行可能コードである、請求項７に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項９】
前記第２のデジタル資産は、デジタル証明書、暗号鍵、および実行可能なソフトウェアのうちの少なくとも１つである、請求項１に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項１０】
前記プロビジョニングコントローラは、前記コンピュータ化された機器に関連し、前記コンピュータ化された機器のプロビジョニング活動に関する情報を格納するログを作成し維持するようにさらに動作可能である、請求項１に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項１１】
前記デジタル資産管理サーバは、前記コンピュータ化された機器に関連するプロビジョニング活動に関する情報を前記ログに格納するために前記プロビジョニングコントローラに送信するようにさらに動作可能である、請求項１０に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項１２】
前記第１の安全な配信機器は、前記ログに格納するために前記コンピュータ化された機器に関連するプロビジョニング活動に関する情報を前記プロビジョニングコントローラに送信するようにさらに動作可能である、請求項１０に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項１３】
前記プロビジョニングコントローラは、前記デジタル資産管理サーバに前記第１のデジタル資産を送信するように指示する前に、前記コンピュータ化された機器を認証するようにさらに動作可能である、請求項１に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項１４】
前記コンピュータ化された機器は、埋め込み型ユニバーサル集積回路カード（ｅＵＩＣＣ）である、請求項１に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【請求項１５】
前記デジタル資産管理サーバは複数のサーバを含む、請求項１に記載のコンピュータ化された機器を安全にプロビジョニングするためのシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の相互参照）
本出願は、２０１６年１１月１４日に出願された米国仮特許出願第６２／４２１，８７８号、２０１６年１１月１４日に出願された米国仮特許出願第６２／４２１，８５２号、および２０１７年４月２０日に出願された米国仮特許出願第６２／４８７，９０９号の利益を主張し、それらの全ては、それらの全体が参照により本明細書に組み込まれる。
【０００２】
本発明は、コンピュータ化された機器を安全にプロビジョニングするためのシステム、機器、および方法に関する。
【背景技術】
【０００３】
コンピュータがますます小型化および商品化されるにつれて、製造業者は、１つ以上の

組み込み型コンピュータまたはプロセッサを含む、ますます多様な機器を製造している。コンピュータ化された機器内のコンピュータは、とりわけ、機器の動作を制御し、データを収集、保存、共有し、他のコンピュータや他のコンピュータ化された機器と通信し、それ自身のソフトウェアを更新することができる。

【０００４】

モノのインターネット（ＩｏＴ）は、プロセッサ、電子機器、ソフトウェア、データ、センサ、アクチュエータ、および／またはネットワーク接続を内蔵したコンピュータ化された物理機器のネットワークであり、インターネット、携帯電話ネットワーク、およびその他のワイヤレスネットワークを含むデジタルネットワークを介してこれらの機器にデータを接続および交換可能にする。通常、それぞれの「モノ」は、その組み込みコンピューティングシステムを通じて一意に識別可能であり、既存のインターネットインフラストラクチャ内で相互運用することができる。

【０００５】

ＩｏＴの意味での「モノ」とは、とりわけ、家電製品、ビジネスや企業の環境で使用される企業向け機器、製造機械、農業用機器、家庭や建物内のエネルギー消費型機器（スイッチ、コンセント、電球、テレビなど）、医療およびヘルスケア機器、インフラストラクチャ管理機器、ロボット、ドローン、および輸送機器および車両などの多様なコンピュータ化された機器を指すことができる。

【０００６】

例えば、全部ではないにしても大部分の現代の乗り物（例えば、自動車、トラック、航空機、列車、船舶など）は、それらのサブシステム内にいくつかの組み込みプロセッサまたは組み込みコンピュータを含み、少なくともいくつかの態様でコンピュータ制御される。同様に、ますます多くの現代の交通インフラ機器（例えば、信号機、交通カメラ、交通センサ、ブリッジモニタ、ブリッジ制御システムなど）は、少なくとも１つ、そしてしばしば多くの、組み込みプロセッサまたは組み込みコンピュータシステムを含み、少なくともいくつかの態様でコンピュータ制御される。交通ネットワークのこれらのコンピュータ制御要素は、通常、相互に通信して様々な種類の情報をやり取りし、安全で、正しく、効率的で、信頼できる動作のために、それらは車両間（Ｖ２Ｖ、Ｃ２Ｃ、車間とも呼ばれる）通信における他の車両との間でおよび／または車両とインフラストラクチャ間（Ｖ２Ｉ、Ｃ２Ｉ、車インフラストラクチャ間とも呼ばれる）通信におけるインフラストラクチャ要素との間で受信／送信される情報に反応し、応答し、動作を変更し、あるいは依存することができる。

【０００７】

コンピュータ化された機器内のコンピュータは、それらのソフトウェアおよび／またはファームウェアおよびデータに従って動作する。安全で適切な動作を確実にするために、コンピュータ化された機器は、製造業者によって意図されたように、適切なソフトウェア、ファームウェア、実行可能命令、デジタル証明書（例えば、公開鍵証明書）、および暗号鍵など（以下において、集合的に「デジタル資産」または「ソフトウェア」と呼ぶものとする）で適切に初期化および更新されなければならないので、ＩｏＴは、認可された、動作確認済みのソフトウェアとデータを実行している機器のみからなる。しかしながら、認可されていない人または組織（例えば、ハッカー）がコンピュータ化された機器内のソフトウェアを交換または変更するときに問題が生じる。また、古いソフトウェア、テストされていないソフトウェア、認可されていないソフトウェア、および／または既知のバグを有するソフトウェアがコンピュータ化された機器内に設置されている場合にも問題が生じる。

【０００８】

従って、エラーに敏感な、誤って機能する、テストされていない、悪意を持って改変された、またはさもなければ望ましくないソフトウェアおよびデータを使用してコンピュータ化された機器が動作するのを防ぐように、コンピュータ化された機器内のデジタル資産を安全にプロビジョニングするための改良されたシステム、方法、および技術を提供する

ことが望まれている。

【発明の概要】

【０００９】

１つ以上のコンピュータ化された機器を安全にプロビジョニングするためのシステム、方法、および機器システムが本明細書で開示される。様々な実施形態において、システムは、コンピュータ化された機器に通信可能に接続され、デジタル資産を受信し、デジタル資産をコンピュータ化された機器内にロードするように動作可能な第１の配信機器と、第１の安全な通信チャネルを介して配信機器に接続され、デジタル資産を生成して条件付きで配信機器に送信するように動作可能なデジタル資産管理システムと、第２の安全な通信チャネルを介して配信機器に接続され、第３の安全な通信チャネルを介してデジタル資産管理システムに接続され、デジタル資産を配信機器に送信するようにデジタル資産管理システムに指示するように動作可能なプロビジョニングコントローラとを含む。デジタル資産が存在しないために、コンピュータ化された機器は、デジタル資産がコンピュータ化された機器にロードされる前には機能しない、または部分的にしか機能しない可能性がある。デジタル資産は、デジタル証明書、暗号鍵、および実行可能なソフトウェアのうちの少なくとも１つとすることができる。

【００１０】

様々な実施形態では、システムは、第４の安全な通信チャネルを介してデジタル資産管理システムに接続され、第１の配信機器が切断された後にコンピュータ化された機器に通信可能に接続され、第２のデジタル資産を受信し、第２のデジタル資産をコンピュータ化された機器内にロードするように動作可能な第２の配信機器をさらに含み、プロビジョニングコントローラはさらに、第２のデジタル資産を配信機器に送信するようにデジタル資産管理システムに指示するように動作可能である。コンピュータ化された機器は、第２のデジタル資産がコンピュータ化された機器にロードされた後に完全に機能的になることができる。

【００１１】

様々な実施形態では、デジタル資産管理システムは、登録局アプリケーションを実行し、登録局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンと、登録認証局アプリケーションを実行し、登録認証局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンと、偽名認証局アプリケーションを実行し、偽名認証局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンと、第１の連携局アプリケーションを実行し、第１の連携局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンと、第２の連携局アプリケーションを実行し、第２の連携局アプリケーションによって必要とされる暗号計算を実行する１つ以上の計算エンジンに通信可能に接続された１つ以上の仮想マシンとをさらに含むことができる。

【００１２】

他の実施形態では、デジタル資産管理システムは、登録局アプリケーションを実行する１つ以上の仮想マシンと、登録認証局を実行する１つ以上の仮想マシンと、偽名認証局アプリケーションを実行する１つ以上の仮想マシンと、第１の連携局アプリケーションを実行する１つ以上の仮想マシンと、第２の連携局アプリケーションを実行する１つ以上の仮想マシンとに動作可能に接続されたデータベースをさらに含むことができる。

【００１３】

さらに他の実施形態では、システムは、プロビジョニングコントローラに動作可能に接続され、コンピュータ化された機器の製造業者を認証し、製造業者がコンピュータ化された機器のプロビジョニングを管理することを可能にするポータル、および／またはプロビジョニングコントローラに動作可能に接続され、コンピュータ化された機器の設置業者を認証し、設置業者がコンピュータ化された機器のプロビジョニングを管理することを可能

にするポータル、および／またはプロビジョニングコントローラに動作可能に接続され、コンピュータ化された機器のレギュレータを認証し、レギュレータがコンピュータ化された機器のプロビジョニングを管理することを可能にするポータルをさらに含むことができる。

【００１４】

さらに他の実施形態では、プロビジョニングコントローラは、コンピュータ化された機器にロードするためにデジタル資産（例えば、実行可能ソフトウェアイメージ）を配信機器に送信するようにさらに動作可能とすることができる。さらに他の実施形態では、プロビジョニングコントローラは、デジタル機器に関連付けられ、デジタル機器のプロビジョニングアクティビティに関する情報を格納するログを作成し維持するようにさらに動作可能とすることができ、配信機器は、ログに格納するためのプロビジョニングコントローラへのデジタル機器に関連するプロビジョニングアクティビティに関する情報を送信するようにさらに動作可能とすることができる。

【００１５】

さらに他の実施形態では、プロビジョニングコントローラは、デジタル資産管理システムにデジタル資産を送信するように指示する前にデジタル機器を認証するようにさらに動作可能とすることができる。

【図面の簡単な説明】

【００１６】

本明細書に組み込まれてその一部を構成する添付の図面は、本発明の実施形態を例示し、その説明と共に、本発明の原理を説明するのに役立つ。

【００１７】

【図１】本発明の実施形態と一致する、安全なプロビジョニングのためのシステムの一例を示すブロック図である。

【００１８】

【図２】本発明の実施形態と一致する、コンピュータ化された機器を安全にプロビジョニングするためのプロセスの一例を示すスイムレーン図である。

【００１９】

【図３】本発明の実施形態と一致する、コンピュータ化された機器を安全にプロビジョニングするためのプロセスの別の一例を示すスイムレーン図である。

【００２０】

【図４Ａ】本発明の実施形態と一致する、スケーラブルで安全なデジタル資産管理システムを実装するためのシステムの一例のブロック図の第１の部分である。

【００２１】

【図４Ｂ】本発明の実施形態と一致する、スケーラブルで安全なデジタル資産管理システムを実装するためのシステムの一例のブロック図の第２の部分である。

【００２２】

【図５】本発明の実施形態と一致するシステムおよび方法をホスティングするために使用することができるコンピューティングシステムの一例のブロック図である。

【発明を実施するための形態】

【００２３】

ここで、本発明の様々な実施形態について詳細に言及するが、それらの例は添付の図面に示されている。都合のよい場合にはいつでも、同じまたは同様の部分を指すために、図面全体を通して同じ符号を使用する。

【００２４】

現場での安全で適切な動作を保証するために、組込み機器（例えば、車両に使用される電子制御ユニット（ＥＣＵ））は、セキュリティ資産などのデジタル資産をプロビジョニングすることによって製造中に適切に初期化される必要がある。デジタル資産には、様々な暗号化キー、一意の識別子、デジタル証明書、およびソフトウェアを含めることができる。ほとんどの場合、これらのデジタル資産の起源と製造工場は、地理的に異なる場所に

あり、これらの場所は、従来、安全でないインターネット通信を介して相互接続されている。したがって、デジタル資産が悪意のある者によってまたは偶然にアクセスまたは変更されることがないように、これらのデジタル資産の起点から機器へのエンドツーエンドの安全なチャネルを作成することが望ましい。

【００２５】

ＴＬＳ／ＳＳＬなどのエンドツーエンド保護のための従来のネットワークセキュリティプロトコルには、両方の通信側に事前共有キーまたは特定の秘密セキュリティ資料が予め存在することが必要であるという欠点がある。これは、デジタル資産をプロビジョニングするために、いくつかの初期の秘密資料が事前に存在しなければならないという点で、周期的な技術的問題を引き起こす。この問題には、いかに最初の秘密資料を保護するか、という事が含まれている。物流を単純化するために、通常、初期ソフトウェアの単一バージョンが製造中にコンピュータ化された機器にロードされるので、この問題はコンピュータ化された機器にとって特に深刻である。この初期ソフトウェアに初期セキュリティ資料を含める必要がある場合、これにはグローバルシークレットが存在する必要がある。結果として、初期のセキュリティ資料を危険にさらすことは、それらがすべて同じグローバルシークレットを共有するので、すべての機器上にプロビジョニングされるすべてのデジタル資産の漏洩につながるであろう。本開示と一致するシステム、方法、および機器は、従来のプロビジョニングシステムのこれらのおよび他の問題に対処する。

【００２６】

プロビジョニングとは一般的に、適切なデータとソフトウェアを使ってコンピュータ化された機器を準備するためにとられる一連のアクションを指す。それはまた、機器をその運用環境に適切に設置して運用準備を整えるためにとられる一連のアクションも含むことができる。アクションは、適切なデジタル資産（例えば、オペレーティングシステム、機器ドライバ、ミドルウェア、アプリケーション、デジタル証明書など）を機器のデジタルストレージ（例えば、メモリ）にロードすること、および（必要な場合）各々の特定の機器に固有であり得る特定のデジタル資産を機器上で適切にカスタマイズし構成することを含む。アクションはまた、コンピュータ化された機器が正当な機器製造業者によって作成された正当な機器であり、コピーまたは偽造の機器ではないことを検証することを含むことができる。

【００２７】

アクションはまた、機器をその動作環境に正しく設置すること、および機器が正しく動作していることを検証するためにそれをテストすることを含むことができる。機器が１つの製造業者によって構築され、後で別の業者によってより大きなシステムまたは機器に設置される可能性がある（例えば、部品メーカーにより作られたオンボードユニット（ＯＢＵ）が、自動車メーカーによって作られた自動車に取り付けられる可能性がある）という事実によって、安全性が確認されている機器のみを安全にプロビジョニングする機能は複雑である。不適切に設置された機器は、正しく機能しない可能性がある。

【００２８】

本発明と一致した様々な実施形態は、ＩｏＴ機器を含むコンピュータ化された機器の安全なプロビジョニングを提供する。そのような実施形態は、コンピュータ化された機器によって使用されるデジタル資産の悪意のある、過失の、または誤った改ざん、改変、更新、またはリリースを防止または禁止し、コンピュータ化された機器およびそれらのソフトウェアの不適切な設置を防止または禁止するのに役立つ。

【００２９】

本発明と一致した様々な実施形態はまた、安全なプロビジョニングプロセスの監査ログ、記録、報告などを生成することができ、それは後で発見された問題を分析し解決するために使用することができる。

【００３０】

本発明と一致した様々な実施形態は、機器およびシステム製造業者へのサービスとして提供され得る安全なプロビジョニングおよび管理プラットフォームも提供することができ

る。
【００３１】
図１は、本発明の実施形態と一致する、コンピュータ化された機器の安全なプロビジョニングのためのシステム１００の一例を示すブロック図である。図１の例に示すように、システム１００はプロビジョニングコントローラ１２０を含む。プロビジョニングコントローラ１２０は、デジタルセキュリティ資産を安全に生成および格納し、様々な暗号化および機密計算を安全に実行する組み込みハードウェアセキュリティモジュール（ＨＳＭ）を有する（例えば、少なくとも１つのプロセッサおよび関連メモリを有する）サーバコンピュータとして実装することができる。ＨＳＭは、暗号キーなどのデジタルセキュリティ資産やその他の機密データを起こり得る攻撃者によるアクセスから保護する。様々な実施形態では、プロビジョニングコントローラ１２０は、システム１００のユーザを認証し、それらと安全に通信するように機能し、１つ以上の配信機器１０８、１３１と安全に通信し、それらを管理するように機能し、デジタル資産管理システム（ＤＡＭＳ）１１０と安全に通信し、その動作を指示するように機能し、プロビジョニングレコードを作成して保存するように機能し、プロビジョニングレコードを作成、保存、配信するように機能し、監査ログを作成、保存、配信するように機能し、ＤＡＭＳ１１０と配信機器１０８、１３１の要素を暗号的に結び付けるために証明書を作成し配信するように機能し、ユーザと管理対象機器が信頼されなくなった場合は、必要に応じてそれらを無効にするように機能し、ビジネス継続性と災害復旧のための、オフサイトストレージ用の重要なキーとデータの安全な暗号化バックアップを作成し配信するように機能する。
【００３２】
図１の例に示すように、プロビジョニングコントローラ１２０は、データベース１２５に通信可能に接続され、データベース１２５は、機器１０６ａ、１０６ｂ（まとめて１０６と呼ぶことがある）の安全なプロビジョニングに関連するデータ、情報、およびデジタル資産を格納することができる。
【００３３】
プロビジョニングコントローラ１２０はまた、製造業者のユーザポータル１１５に安全に通信可能に接続され、ユーザポータル１１５は、例えば、サーバとして、またはプロビジョニングコントローラ１２０へのインターフェースとして実装することができる。様々な実施形態では、機器製造業者１０５のスタッフ１０９は、製造業者のユーザポータル１１５を使用して、プロビジョニングコントローラ１２０（およびしたがってＤＡＭＳ１１０）とインターフェース接続し、それらの機器プロビジョニングアクティビティを管理することができる。様々な実施形態では、製造業者のユーザポータル１１５は、ユーザ名、パスワード、２ファクタ識別データ、顔認識画像、指紋などの識別情報をスタッフユーザ１０９から収集し、識別情報をプロビジョニングコントローラ１２０に提供することができる。プロビジョニングコントローラ１２０は、スタッフ１０９に安全なプロビジョニングシステム１００へのアクセスを可能にする前に、スタッフ１０９を認証することができる。例えば、プロビジョニングコントローラ１２０は、スタッフユーザ１０９に関連付けられ、以前に検証されてそのデータベース１２５に格納された識別情報を検索し、格納された識別情報を製造業者のユーザポータル１１５によって収集された識別情報と比較することができる。あるいはまた、プロビジョニングコントローラ１２０またはＤＡＭＳユーザポータル１１５は、スタッフ１０９がシステム１００を使用することを認可されているかどうかを判断する、ユーザの企業識別および認証システムと統合されてもよい。様々な実施形態では、プロビジョニングコントローラ１２０またはＤＡＭＳユーザポータル１１５は、認証に成功したスタッフ１０９に役割を与え、システム１００内での彼らのアクションを制限することができる。いくつかの実施形態では、プロビジョニングコントローラ１２０は、２セットの識別情報が一致する場合にのみアクセスを可能にすることができる。
【００３４】
同様に、プロビジョニングコントローラ１２０はまた、例えばサーバとして、またはプ

ロビジョニングコントローラ１２０へのインターフェースとして実装され得る設置業者ユーザポータル１１６に通信可能に接続される。様々な実施形態では、機器設置業者のスタッフ１３２は、設置業者ユーザポータル１１６を使用して、プロビジョニングコントローラ１２０（およびしたがってＤＡＭＳ１１０）とインターフェース接続し、それらの機器設置およびプロビジョニングアクティビティを管理することができる。プロビジョニングコントローラ１２０は、スタッフ１３２を認可する前にスタッフ１３２を認証し、スタッフ１３２が安全なプロビジョニングシステム１００にアクセスしてシステム上で認可された機能を実行することを可能にする前にそれらに役割を割り当てることができる。

【００３５】

また同様に、プロビジョニングコントローラ１２０はまた、例えばサーバとして、またはプロビジョニングコントローラ１２０へのインターフェースとして実装することができるレギュレータポータル１１７に通信可能に接続される。様々な実施形態では、プロビジョニングコントローラ１２０によって認証されると、レギュレータ１４０は、レギュレータポータル１１７を使用してプロビジョニングコントローラ１２０とインターフェース接続し、製造業者１０４、設置業者１３０、機器１０６、および／または機器１０６に設置されているソフトウェア／デジタル資産のレビューおよび認可を管理することができる。プロビジョニングコントローラ１２０は、レギュレータ１４０が安全なプロビジョニングシステム１００にアクセスすることを可能にする前に、レギュレータ１４０を認証することができる。システム１００のいくつかの実施形態では、レギュレータ１４０およびレギュレータポータル１１７はオプションである。

【００３６】

プロビジョニングコントローラ１２０はさらに、ＤＡＭＳ１１０と通信可能に接続されている。様々な実施形態では、ＤＡＭＳ１１０は、サーバ、機器、または安全な機器および／またはサーバのシステムとして実装することができる。ＤＡＭＳ１１０は、配信機器１０８、１３１、または他の安全で認証された接続を介して、プロビジョニングされるエンドエンティティ機器から公開鍵を安全に検索し、機器１０６に設置されているデジタル証明書および関連データを安全に供給する。また、ＤＡＭＳ１１０は、製造業者１０５および設置業者１３０から、コンピュータ化された機器１０６のプロビジョニング、設置、機能性などに関するステータス情報を、配信機器１０８、１３１を介して安全に受信する。さらに、ＤＡＭＳ１１０は、図１に示されるように単一のサイトまたは複数のサイトでこのプロビジョニングを実行することができる。図４に関してより詳細に説明されるように、ＤＡＭＳ１１０は、以下の主な要素を含むことができる：ルート認証局（ＣＡ）、ポリシージェネレータ、ＣＲＬジェネレータ、不正行為局、中間ＣＡ、登録ＣＡ、連携局、偽名ＣＡ、および登録局。

【００３７】

ＤＡＭＳ１１０は、新しい機能性を追加し、Ｗｉｌｌｉａｍ Ｗｈｙｔｅらによる２０１３年１２月の２０１３ ＩＥＥＥ Ｖｅｈｉｃｕｌａｒ Ｎｅｔｗｏｒｋｉｎｇ Ｃｏｎｆｅｒｅｎｃｅによる論文「Ｖ２Ｖ通信のための安全な信用証明書管理システム」に記載されているコンポーネントおよび機能性を改善する。様々な実施形態では、ＤＡＭＳ１１０は、多段階プログラミングおよび柔軟な管理を含む（例えば、レギュレータ１４０を含めることを可能にする）。ＤＡＭＳ１１０の様々な実施形態はまた、単一のＤＡＭＳ１１０が異なる加入者に異なるレベルのプロビジョニングを提供することを可能にする機能を可能にする。ＤＡＭＳ１１０の様々な実施形態はまた、加入者がある期間中（例えば、１週間あたり）に異なるデジタル証明書の使用ならびに異なる証明書のロード（従来のシステムのような３年の代わりに１週間など）を割り当てることを可能にする機能を可能にする。特定の製造業者のコンピュータ化された機器１０６（例えば、ＯＥＭの自動車）が製造業者の範囲内に留まる（例えば、それらのＵＲＬがそれらの名前を示す）ことができるように、ＤＡＭＳ１１０の様々な実施形態は加入者固有のＵＲＬも提供し得る。

【００３８】

図示されるように、プロビジョニングコントローラ１２０はまた、配信機器１０８、１

３１に通信可能に接続される。様々な実施形態において、配信機器１０８、１３１は、とりわけ（図示のように）会社の敷地に設置されたスタンドアロンの安全な機器として、またはウェブサービスまたはクラウドサービスとして実装することができる。様々な実施形態では、配信機器１０８、１３１は、好ましくは専用の非インターネット通信チャネルを介してＤＡＭＳ１１０およびプロビジョニングコントローラ１２０との間でデジタル資産および他の情報を安全に送受信する信頼できるエンドポイント機器として実現される。図示されるように、配信機器１０８、１３１はまた、デジタル資産を機器１０６ａ、１０６ｂにダウンロードし、そこからデータを受信するために、機器１０６ａ、１０６ｂと直接的または間接的のいずれかで接続する。様々な実施形態では、配信機器１０８、１３１は、ハードウェアセキュリティモジュール、強化オペレーティングシステム（ＯＳ）、内部ファイアウォール、および内部ホスト侵入検知／防御システムを備えた（例えば、少なくとも１つのプロセッサおよび関連メモリを有する）サーバコンピュータを含むボックスとして実装できる。配信機器は、信頼できない環境で動作するように特に設計されてもよく、それでもなお信頼され信頼できる動作を提供する。配信機器は、それ自体と安全なプロビジョニングコントローラ１２０およびＤＡＭＳ１１０との間に安全な通信チャネルを有する。このチャネルは、配信機器を制御し、プロビジョニング関連のデータとログ情報を送受信するために使用される。配信機器はまた、機器１０６をプログラムまたはプロビジョニングするために使用されるテスタ１０７への安全な通信チャネルを有することができる。このチャネルは、製造場所の通信ネットワーク上でプロビジョニングデータとログデータが漏洩されたり変更されたりすることから保護する。配信機器１０８はまた、プロビジョニングデータが（不正テスタ１０７を含む）第三者によって危険にさらされたり変更されたりすることができないように、プログラムされる機器１０６と直接的に安全な通信チャネルを確立することができる。様々な実施形態では、配信機器は、それがプロビジョニングしようとしている機器１０６から、公開鍵およびマイクロプロセッサのシリアル番号などの他のデータを収集することができる。配信機器は、この情報をプロビジョニングコントローラ１２０および／またはＤＡＭＳ１１０に送信することができる。配信機器はまた、機器１０６内にプログラムするために、プロビジョニングコントローラ１２０および／またはＤＡＭＳ１１０からデータおよびコマンドおよび他の情報を受け取ることができる。配信機器はそれ自身のログデータを返すことができ、そして配信機器はテスタ１０７からプロビジョニングコントローラ１２０および／またはＤＡＭＳ１１０へデータを返すことができる。

【００３９】

機器製造業者１０５に関して図示されているように、配信機器１０８はテスタ１０７（例えば、コンピュータ化された製造装置、製品検査機器など）に通信可能に接続することができ、テスタ１０７は次いで、ＯＢＵ機器などの製造業者１０５によって製造された機器１０６ａに接続される。製造業者１０５は、コンピュータ化された機器１０６ａを製造するおよび／または市場に供給する工場を含むか、またはそのような工場とすることができる。多くの可能な例のうちの１つとして、コンピュータ化された機器１０６ａは、自動車と交通インフラ機器間の通信用に後で自動車に設置されるオンボードユニット（ＯＢＵ）の一部として組み込まれる、電気通信用のセルラーモデムで使用される組み込み型ユニバーサル集積回路カード（ｅＵＩＣＣ）とすることができる。それは、他の車両や路側機（ＲＳＵ）と通信するためにＯＢＵに搭載されたＶ２Ｖセキュアマイクロプロセッサとすることもできる。これらの新しく製造された機器１０６ａは、適切に動作するために、デジタル資産（例えば、ＤＡＭＳ１１０からのデジタル証明書）によって適切にプロビジョニングされなければならない。製造業者１０５のスタッフ１０９は、ユーザポータル１１５を使用して、プロビジョニングコントローラ１２０と対話し、ＤＡＭＳ１１０による製品プロビジョニングアクティビティを管理することができる。

【００４０】

設置業者１３０に関して示されるように、機器１０６ｂがその動作環境に設置されている間または設置された後に、配信機器１３１は代替的に機器１０６ｂに直接通信可能に接

続されてもよい。設置業者１３０は、コンピュータ化された機器１０６ｂをそれらの動作環境内に設置する（例えば、ＯＢＵを自動車内に設置する）工場または店舗を含むか、またはそれらであり得る。設置時に、コンピュータ化された機器１０６ｂは、適切に動作するために、デジタル資産（例えば、ＤＡＭＳ１１０からの追加のデジタル証明書）をさらに適切にプロビジョニングされなければならない。設置業者１３０のスタッフ１３２は、設置業者ユーザポータル１１６を使用して、プロビジョニングコントローラ１２０と対話し、ＤＡＭＳ１１０による製品プロビジョニングアクティビティを管理することができる。

【００４１】

様々な実施形態では、プロビジョニングコントローラ１２０、配信機器１０８、１３１、およびＤＡＭＳ１１０は、それらの間に安全で公的にアクセスできない通信リンクまたはチャネルを有することができ、様々な実施形態では、図１に示される通信リンクのすべてが、安全で公的にアクセスできない通信チャネルであり得る。様々な実施形態では、これらの安全なチャネルは、この安全なインフラストラクチャ内で未認可のエンドポイントが通信するのを防ぐために暗号化され、相互に認証されている。外層が何らかの形で危険にさらされても、内層は安全なままとなるように、これらの通信チャネルを保護するために複数のセキュリティ機構を使用することができる。一例として、相互認証ＴＬＳトンネルは、独自の安全な通信プロトコルなどの別のプロトコルを使用して、内層と共に外層として使用することができる。システム１００を含むインフラストラクチャコンポーネント間のこれらの安全な接続は、コンポーネント間の機密通信を保護し、それらの正しい動作を保証するために使用される。これらの安全な経路を使用して、プロビジョニングコントローラ１２０およびＤＡＭＳ１１０は、転送中に漏洩または変更されることを懸念することなく、コンポーネント間でデジタルデータを送信することができる。コマンドおよび制御情報もこれらのチャネルを介して渡すことができる。例えば、プロビジョニングコントローラ１２０は、どの配信機器１０８、１３１に、特定のデジタル資産およびデータを送信するかを制御することができる。それはまた、それがプロビジョニングされている製造ライン上の機器１０６にこのデータをどのように計量するかを配信機器１０８、１３１に指示することができる。さらに、配信機器１０８、１３１は、情報が送信中に漏洩または変更されることを心配することなく、情報をプロビジョニングコントローラ１２０に報告して戻すことができる。例えば、安全なプロビジョニングコントローラ１２０は、任意の種類のデジタル資産（例えば、証明書、ソフトウェア、ヒューズコンテンツなど）を用いて最大１０，０００個の機器をプロビジョニングするように配信機器１０８、１３１をプログラムすることができる。配信機器１０８、１３１は、それがプロビジョニングしている機器をカウントすることができ、それがその限界に達すると、それをプロビジョニングコントローラ１２０に報告する。様々な実施形態では、プロビジョニングコントローラ１２０によって管理される機器（例えば、１０８、１１０、１３１、１１５、１１６、１１７）は、それらがプロビジョニングコントローラ１２０と定期的に通信しない場合に、したがって、それらが盗まれて役に立たなくなった場合に、それらを動作させなくする機能を含む。この機能は、紛失／盗難にあった機器が動作し続け、あたかもそれらがまだ適切な製造環境に置かれているかのように機器１０６をプロビジョニングすることを防止する。

【００４２】

引き続き図１に示す例を参照すると、動作時に、製造業者１０５に配置された配信機器１０８は、ＤＡＭＳ１１０からデジタル資産を安全に受け取り、それらを機器１０６ａ用のテスタ１０７に供給する。各機器１０６ａが製造業者１０５によって製造されると、テスタ１０７は機器１０６ａと通信して、機器１０６ａからその固有の識別番号およびステータスなどの情報を取得し、デジタル資産（例えば、デジタル証明書）を機器内にダウンロードまたはさもなければ設置する。テスタ１０７はまた、機器１０６ａから配信機器１０８に情報（例えば、プロビジョニングステータス）を供給することができ、配信機器１０８は、その情報をＤＡＭＳ１１０および／またはプロビジョニングコントローラ１２０

に安全に通信する。いくつかの実施形態では、テスタ１０７は、配信機器１０８と機器１０６ａとの間でデータを安全にトランスポートするソフトウェアトランスポートレイヤセキュリティ（ＴＬＳ）エージェントを含むことができ、これは実際には、各機器１０６ａに関連付けられた一時鍵を使用して、配信機器１０８およびテスタ１０７を介してＤＡＭＳ１１０と機器１０６ａとの間に安全な暗号化通信経路を作成する。

【００４３】

それが最初にプロビジョニングされた後、製造業者１０５は機器１０６ａを設置業者１３０に出荷し、設置業者１３０は機器１０６ｂを設置する。様々な実施形態では、最初のプロビジョニングの前に、機器１０６ａは機能しておらず、製造業者１０５による最初のプロビジョニングの後に、機器１０６ａは、部分的に機能することはできるが、まだ完全には機能していない。そのような実施形態では、最初のプロビジョニングは、設置およびさらなる最後のプロビジョニングのために必要とされる程度までだけ機器を機能的にし、それは完全に動作可能にするために必要とされる。

【００４４】

設置業者１３０は、機器１０６ｂをその動作環境内に設置し、設置業者１３０のスタッフメンバー１３２は、設置業者ポータル１１６を介してその事実をプロビジョニングコントローラ１２０に通知する。この通知は、設置が正しく完了したことを証明するものであり、プロビジョニングコントローラ１２０に対して機器１０６ｂを一意に識別する情報を含むことが好ましい。いくつかの実施形態では、配信機器１３１は、ステータスおよび識別情報について機器１０６ｂに照会した後に、プロビジョニングコントローラ１２０に自動的に通知することができる。設置業者１３０が設置業者ポータル１１６を介して自分が機器１０６ｂを適切に設置したことを証明する様々な実施形態では、この証明はプロビジョニングコントローラ１２０によってデータベース１２５に記録／保存されてもよい。証明は、無線送信電力測定またはＧＰＳアンテナ位置の検証などの、各々の特定の設置された機器１０６ｂに関連する特定の試験データを含み得る。

【００４５】

設置通知に応答して、プロビジョニングコントローラ１２０は、（ｉ）製造業者１０５によって合法的に製造された機器として機器１０６ｂがそのデータベース１２５内にリストされていること、（ｉｉ）製造業者１０５によって最初に首尾よくプロビジョニングされたとして機器１０６ｂがそのデータベース１２５内にリストされていること、および（ｉｉｉ）設置業者１３０がそのデータベース１２５内に認可された設置業者としてリストされていることを検証する。この検証が成功した場合、コントローラ１２０は、機器１０６ｂがその動作環境内に設置されたとき適切に機能することができるように、ＤＡＭＳ１１０にデジタル資産（例えば、偽名証明書（ＰＣ））および／または機器１０６ｂを動作可能にプロビジョニングするのに必要な他の情報を送信するように指示する。

【００４６】

様々な実施形態では、レギュレータポータル１１７を介してレギュレータ１４０はプロビジョニングコントローラ１２０と対話して、設置業者１３０および／または製造業者１０５を識別、検証、および管理し、無認可の設置業者（例えば、ハッカー）がシステム１００からの本物のデジタル資産を取得できないようにする。レギュレータ１４０のスタッフメンバーは、プロビジョニングコントローラ１２０によって認証されることができ、システム１００との一意のＩＤを有することができるので、それらのアクションは一意に記録することができる。様々な実施形態では、レギュレータ１４０は、レギュレータポータル１１７を使用してプロビジョニングコントローラ１２０に問い合わせて、検証レポート、設置業者のアクション、製造された機器１０６ａの数および識別情報、設置済みの完全にプロビジョニングされた機器１０６ｂの数および識別情報などのコントローラ１２０によって記録された情報のコピーおよびレポートを取得することができる。

【００４７】

様々な実施形態では、設置業者１３０は、システム１００と対話するために、プロビジョニングコントローラ１２０によって認可されたものとして認証されなければならない。

認可されるために、設置業者１３０は、例えば、ターゲット環境（例えば、ターゲット車両またはサイトなど）に機器１０６ｂを適切に設置することを記載した適切な契約文書を締結しなければならない場合がある。設置業者１３０は、例えば、レギュレータ１４０による他の契約上の要素を証明することを要求されてもよい。好ましくは、各設置業者１３０は、そのアクションがプロビジョニングコントローラ１２０によって一意に記録され得るように、システム１００内に一意のＩＤを有する。

【００４８】

システム１００およびその機能の記載された実施形態は、製造業者１０５によって製造され、認可された設置業者１３０によって適切に設置および試験された機器１０６のみが、機器１０６を動作可能にするために必要なデジタル資産で完全にプロビジョニングされることを保証する。プロビジョニングコントローラ１２０は、プロビジョニングプロセスの各段階で誰がどのような行動を取ったかについての広範なログおよびレポートを生成し、従来のシステムには存在しなかった重要な監査機能を提供する。

【００４９】

当業者であれば、図１に示すコンポーネント、プロセス、データ、動作、および実施形態の詳細は、説明の簡潔さおよび明瞭さのために提示された例であることを理解するであろう。この例は限定を意図するものではなく、多くの変形が可能であるので、本発明の原理から逸脱することなく他のコンポーネント、プロセス、実施形態の詳細、および変形を使用することができる。例えば、図１には１つの製造業者１０５だけ、１つの設置業者１３０だけ、および１つのレギュレータ１４０だけが示されているが、他の実施形態はこれらのエンティティのそれぞれをいくつでも有することができる。別の一例では、ＤＡＭＳ１１０およびプロビジョニングコントローラ１２０は別々の機器として示されているが、他の実施形態はそれらの機能を単一の機器（例えば、単一のサーバ）に組み合わせてもよい。さらに別の一例として、ポータル１１５～１１７についても同じことが行われ得る。さらに別の一例では、システム１００は、２０１６年１１月１４日に出願された参照として援用される米国特許仮出願第６２／４２１，８５２号に記載されているように、資産管理機器（ＡＭＡ、図示せず）をさらに含むことができる。そのような一実施形態では、ＡＭＡは、プロビジョニングコントローラ１２０および／または配信機器１０８、１３１および／またはＤＡＭＳ１１０に通信可能に接続され得る。様々な実施形態において、ＡＭＡは、生産コーディネータが製品（例えば、機器１０６）の構成および構築を容易かつ効率的に管理することを可能にし、資産所有者がデジタル資産の在庫を容易かつ効率的に管理することを可能にするユーザフレンドリーなＧＵＩおよび機能を含むことができる。

【００５０】

図２は、本発明の実施形態と一致する、コンピュータ化された機器を安全にプロビジョニングするためのプロセス２００の一例を示すスイムレーン図である。様々な実施形態では、図示のプロセス２００または動作の一部または全部は、（１つ以上のプロセッサまたは１つ以上のコンピューティングサブシステムを含み得る）汎用コンピューティングシステム上で実行するコードによって、ハードウェアのみのシステムによって、またはそれら２つのハイブリッドであるシステムによって、実行され得る。図２の上を横切って示されるように、プロセス２００に関与するエンティティは、コンピュータ化された機器１０６の製造業者１０５、製造業者１０５に配置されている配信機器１０８、プロビジョニングコントローラ１２０、およびＤＡＭＳ１１０を含む。様々な実施形態では、これらのエンティティは、図１に関しておよび本開示を通して説明されるようなものであることができ、そのように互いに通信することができる。

【００５１】

図２の例に示すように、プロセス２００は、製造業者１０５（例えば、スタッフメンバー１０９）が、プロビジョニングコントローラ１３０からデジタル資産プロビジョニングサービスを要求する２０５において開始し、ここでデジタル資産は機器１０６ａにプロビジョニングされ（例えば、機器１０６ａによって使用され）、要求はデジタル資産の宛先である機器１０６ａを識別することができる。要求は、例えば、製造業者１０５が新しい

製品１０６に対するプロビジョニングサービスを要求しているか、または既存の製品１６に対する新しいプロビジョニングサービス要求を行っている可能性がある。様々な実施形態では、この動作は、認可されたユーザが、例えばユーザポータル１１５を介してプロビジョニングコントローラ１３０にログオンすることを含み得る。場合によっては、要求されたデジタル資産は、例えば、登録証明書、機器１０６が実行する実行可能コード、デジタル動作パラメータなどの安全な資格情報である場合がある。登録証明書は、すべての参加者が有効な登録証明書を共有する必要があり（例えば、ＵＳＤＯＴのＶ２Ｘエコシステム）、認可された参加者も（例えば、ＵＳＤＯＴのＶ２Ｘエコシステムの例では、車両と路側インフラストラクチャとの間の通信および動作を可能にするために）エコシステム内の機器１０６の通信および動作を可能にする偽名証明書を受け取ることができるエコシステム内の認可された参加者としてその所有者を識別する公開鍵証明書である。

【００５２】

２１０において、プロビジョニングコントローラ１２０は、製造業者１０９からのユーザが認可されたユーザであるかどうかを判定する。いくつかの実施形態では、プロビジョニングコントローラ１２０はまた、２１０において、プロビジョニングされるべき機器１０６ａ（例えば、製品）がシステム１００と共に使用することを認可されているかどうかを判定することができる。場合によっては、認可された機器のリストが図１のレギュレータ１４０によって提供され、この決定を行うためにプロビジョニングコントローラ１２０によって使用されてもよい。

【００５３】

ユーザ（および／または製品）が認可されていない場合、プロビジョニングコントローラ１２０はデジタル資産プロビジョニングサービス（図２には図示せず）に対する要求を拒否する。一方、認可されたユーザが（例えば、認可された製品に対する）要求を行っている場合（２１０、はい）、プロビジョニングコントローラ１２０は、（例えば、（２１５で）サービス要求命令をＤＡＭＳ１１０に送信することによって）サービス要求を満たすようにＤＡＭＳ１１０に指示、命令し、または他の方法でＤＡＭＳ１１０を制御する。

【００５４】

２２０において、２１５からの要求を受信したことに応答して、およびそれを条件として、ＤＡＭＳ１１０は、その要求に基づいて機器１０６ａへのサービスを開始するように自身を設定する。いくつかの実施形態では、ＤＡＭＳ１１０はまた、機器１０６ａにサービスを提供するように配信機器１０８を設定するように、配信機器１０８に命令を送信することができる（図示せず）。

【００５５】

２２２において、ＤＡＭＳ１１０は、２０５において要求されたように、機器１０６ａのためのデジタル資産を生成、作成、計算、および／または検索する。様々な実施形態では、ＤＡＭＳ１１０は、公開鍵と秘密鍵のペア、ならびに機器１０６ａのための登録証明書と偽名証明書などの要求されたデジタルセキュリティ資産を作成または生成することができる。

【００５６】

動作２２２の代替の実施形態（図２には図示されない）では、ＤＡＭＳ１１０は、機器１０６ａに関連するデジタル資産生成情報（例えば、機器１０６ａによって生成されたか、または機器１０６ａから検索された登録および偽名公開鍵ならびに機器１０６ａを一意に識別するデータ（例えば、マイクロプロセッサのシリアル番号））を配信機器１０８から要求し、受信する。そのような実施形態では、ＤＡＭＳ１１０は次に、登録および偽名公開鍵を使用して、デジタル資産（例えば、機器１０６ａのための登録証明書および適切な数の偽名証明書）を生成する。

【００５７】

２２５において、ＤＡＭＳ１１０は、２０５でデジタル資産サービスを要求した製造業者１０５の配信機器１０８にデジタル資産を送信する。例えば、ＤＡＭＳ１１０は、公開鍵と秘密鍵のペア、登録証明書、および偽名証明書を製造業者１０５の配信機器１０８に

安全に送信することができる。

【００５８】

２２６において、ＤＡＭＳ１１０は、デジタル資産に関するログ情報をプロビジョニングコントローラ１２０に送信する。様々な実施形態では、ログ情報は、例えば、要求者のＩＤ、デジタル資産のＩＤ、配信機器のＩＤ、要求および送信アクションのタイムスタンプ、受信したマイクロプロセッサのシリアル番号などのデジタル資産の要求および転送を記述する情報を含み得る。いくつかの実施形態では、ログ情報はデジタル資産のコピーを含み得る。２２７において、プロビジョニングコントローラ１２０はログ情報を受信し、例えばデータベース１２５に格納する。実際には、プロビジョニングコントローラ１２０は、システム１００内で発生するすべてのアクティビティの監査跡を維持し、これにより、機器１０６ａが製造業者１０５によってどのようにそしていつ構築およびプロビジョニングされ得るかに関するデータなど、多くの種類のデータを組み立てることができる。そのようなデータおよびログ情報は、請求および監査目的で使用される場合がある。

【００５９】

２３０において、配信機器１０８は、ＤＡＭＳ１１０によって送信されたデジタル資産（例えば、公開鍵と秘密鍵のペア、登録証明書と偽名証明書）を受信して記憶する。

【００６０】

２３５において、配信機器１０８は、デジタル資産を配信機器１０８から機器１０６ａに安全に転送するために使用することができる公開鍵などのデジタルセキュリティ資産を機器１０６ａに要求して受信する。様々なタイプの機器１０６ａは、おそらく機器１０６に内蔵された安全なプロセッサを使用して一時鍵ペアを生成する能力を有し、公開鍵は一時鍵ペアの一部であり得る。２４０において、配信機器１０８は、デジタルセキュリティ資産（例えば、公開鍵）を使用してデジタル資産（例えば、登録証明書）を安全に機器１０６ａに送信する。様々な実施形態では、配信機器１０８は、例えば、機器１０６ａとの仮想プライベートネットワーク（ＶＰＮ）を形成し、その中でデジタル資産を安全に送信するために、機器１０６ａの公開鍵を使用することができる。

【００６１】

様々な実施形態では、配信機器１０８は、それとテスタ１０７との間でトランスポートレイヤーセキュリティ（ＴＬＳ）を使用して、機器１０６ａに接続され得るテスタ１０７との通信を保護することができる。機器１０６ａへの安全な通信を直接行うことが望ましい実施形態では、システムは、機器１０６ａ上で一時公開鍵ペアを作成し、その公開鍵を配信機器１０８の公開鍵を含む配信機器１０８からの証明書と共に使用して、機器１０６ａへの安全なトンネルを作成することができる。そのような実施形態では、機器１０６ａは、その中でシステム１００のルート公開鍵を用いて特別なコードを実行し、配信機器１０８がそれに送信する証明書を検証する。

【００６２】

安全なパスが機器１０６ａまたはテスタ１０７と配信機器１０８との間に確立されると、機器１０６ａは、（例えば、Ｖ２Ｘエコシステムのための）登録および偽名公開鍵ペアを作成し、公開鍵および他のデータを配信機器１０８にエクスポートし、配信機器１０８はその後、このデータをＤＡＭＳ１１０およびプロビジョニングコントローラ１２０に送信することができる。動作２２２の代替実施形態に関して上述したように、ＤＡＭＳ１１０は、受信した公開鍵を使用して登録証明書および偽名証明書を作成することができ、いくつかの実施形態では、多数（例えば３，０００）の偽名証明書があり得る。一実施形態のこの代替例では、ＤＡＭＳ１１０は、前述のように、動作２２５でこれらの証明書を配信機器１０８に返す。いくつかの他の実施形態では、ＤＡＭＳ１１０は、プロビジョニングが実行されている場所に応じて、１０８の代わりにこれらの証明書を配信機器１３１に送信することができる。

【００６３】

いくつかの実施形態では、例えば、機器１０６がそれ自体のワイヤレスまたは有線通信機能を有し、少なくとも部分的に動作可能である場合、配信機器１０８は機器１０６と直

接通信することができる。他の実施形態では、配信機器１０８は、テスタ１０７などの中間機器を介して機器１０６と間接的に通信することができる。

【００６４】

機器１０６ａはデジタル資産を受信し、動作中に使用するためにそれを格納する。例えば、機器１０６ａが自動車搭載ユニット（ＯＢＵ）または電子制御ユニット（ＥＣＵ）であり、デジタル資産が無線ネットワークに参加するために必要なセキュリティ資産（例えば、公開鍵証明書）である場合、デジタルセキュリティ資産はＯＢＵによって保管される。ＯＢＵが後で車に取り付けられて作動すると、ワイヤレスネットワークへの接続を試みる。ＯＢＵがネットワークに接続することを可能にする前に、ネットワークはＯＢＵの認証を試みる。ＯＢＵは、それが製造業者１０５において配信機器１０８によって提供されたデジタルセキュリティ資産を有する場合にのみ、ネットワークを認証し参加することができる。

【００６５】

２４５において、配信機器１０８は、２４０で送信されたデジタル資産を機器１０６ａが正常に受信および設置（例えば、格納）したかどうかを示すステータス情報を機器１０６ａから受信またはアクセスする。

【００６６】

２５０において、配信機器１０８はステータス情報をプロビジョニングコントローラ１２０に送信する。そして、２５５において、プロビジョニングコントローラ１２０は、動作２２７で格納されたログ情報に関連してステータス情報を受信して格納する。したがって、プロビジョニングコントローラ１２０は、各々の特定の機器１０６に関連付けられたシステム１００の活動のすべてについて監査跡または監査ログを継続する。様々な実施形態では、監査ログは、各々の機器１０６に対して、製造業者のプロビジョニングの失敗の成功（例えば、動作２３５～２４５）、デジタル資産の識別情報（および／またはデジタル資産自体のコピー）、暗号の種類などを示す情報を含むことができる。

【００６７】

２７０において、機器１０６ａがデジタル資産を首尾よくプロビジョニングされた場合、製造業者１０５は機器を市場にリリースする。例えば、製造業者１０５は、機器をその動作環境に設置する会社（例えば、図１の設置業者の会社１３０）に機器１０６ａを物理的に出荷することができる。いくつかの実施形態では、機器１０６ａは、この時点で完全にプログラムまたはプロビジョニングされ、完全な機能で動作することが可能であり得る。一方、他の実施形態では、機器１０６ａはこの時点で部分的にのみプログラムまたはプロビジョニングされてもよく、完全な機能で動作することができないか、または機能しない。

【００６８】

図２に示す例は、例示の目的のためだけであり、限定することを意図しない。さらに、図示されたプロセス２００は、特定の開示された実施形態と一致する特定の新規かつ革新的な構成の説明を明確にするために幾分単純化された一例であるが、この例は限定的であることを意図せず、多くの変形が可能である。例えば、機能および動作は特定の順序で実行されるように示されているが、説明された順序は単なる一例であり、開示された特定の実施形態と矛盾しない様々な異なる動作シーケンスを実行することができる。さらに、動作は、単に説明の目的のために別々のステップとして説明され、いくつかの実施形態では、複数の動作が、同時に、および／または単一の計算もしくはより大きな動作の一部として、実行され得る。説明された動作は、網羅的、限定的、または絶対的であることを意図されておらず、様々な動作は修正、挿入、または削除することができる。変形の一例として、図２は概して単一のデジタル資産（例えば、単一のデジタル証明書）の文脈で説明されているが、システムおよびプロセスは複数のデジタル資産（例えば、２つ以上のデジタル証明書）を処理するために同様に機能する。別の一例として、機器１０６ａが安全な通信機能を有さない場合、動作２３５および２４０を削除することができ、配信機器１０８は暗号化されていない通信を使用して機器１０６ｂと通信することができる。

【００６９】
さらに別の一例として、様々な実施形態では、プロビジョニングコントローラ１２０、または専用の署名機器などの委任局が、同様に配信機器１０８に送信し、ソフトウェア、ファームウェア、ヒューズＢＬＯＢ、マニフェストファイルなどのデジタル資産を含む別のまたは追加のデジタル資産を機器１０６ｂにロードさせることができる。そのような実施形態では、プロビジョニングコントローラ１２０は、追加的にまたは代替的に、要求されたデジタル資産をストレージから検索、取得、または他の方法でアクセス、またはアクセスを指示することができる。例えば（図２には図示せず）、プロビジョニングコントローラ１２０またはその認可された委任先は、機器１０６ａにロードされて実行される実行可能ソフトウェアイメージ（例えば、データベース１２５に格納されたコンパイル済みコンピュータプログラム）を検索し、実行可能ソフトウェアイメージを機器内へプログラミングするために配信機器１０に送信することができる。様々な実施形態では、プロビジョニングコントローラ１２０によってアクセスされるデジタル資産は、不正なソフトウェアを機器１０６ａ内にロードすることができないように、機器１０６ａの製造業者１０５によって安全に供給、リリース、および／または認可されたソフトウェアなどのみからなることができる。いくつかの実施形態では、プロビジョニングコントローラ１２０によって検索されたデジタル資産は、図１のデータベース１２５など、プロビジョニングコントローラ１２０に関連付けられているストレージ機器またはデータベース内に格納することができる。

【００７０】
図３は、本発明の実施形態と一致する、コンピュータ化された機器を安全にプロビジョニングするためのプロセス２００の一例を示すスイムレーン図である。様々な実施形態では、（１つ以上のプロセッサまたは１つ以上のコンピューティングサブシステムを含むことができる）汎用コンピューティングシステム上で実行するコードによって、ハードウェアのみのシステムによって、またはそれら２つのハイブリッドであるシステムによって、プロセス３００または図示の動作の一部またはすべてを実行することができる。図３の上を横切って示されるように、プロセス３００に関与するエンティティは、コンピュータ化された機器１０６の設置業者１３０、設置業者１３０に配置されている配信機器１３１、プロビジョニングコントローラ１２０、およびＤＡＭＳ１１０を含む。様々な実施形態では、これらのエンティティは、図１に関しておよび本開示を通して説明されるようなものであることができ、そのように互いに通信することができる。

【００７１】
図３の例に示すように、プロセス３００は、製造業者１０５によって製造およびリリースまたは出荷された機器１０６ｂ（例えば、ＯＢＵまたはＥＣＵ）を設置業者１３０が受け取る３０５で始まる（図２の動作２７０を参照）。３１０において、設置業者１３０は、より大きなシステムなど、その動作環境に機器１０６ｂを設置することができる。例えば、設置業者１３０は、製造業者１０５からＯＢＵを購入する自動車メーカーとすることができ、設置業者１３０は、自動車にＯＢＵを設置することができる。様々な実施形態では、機器１０６ｂを設置することは、設置後に機器１０６ｂの動作、機能などをテストすること、および関連するステータスデータを収集することを含むことができる。

【００７２】
いくつかの実施形態では、機器１０６ｂは、部分的にのみプロビジョニングされ、完全に機能的ではない場合がある。例えば、機器１０６ｂの製造業者１０５は、機器１０６ｂが完全な機能性（例えば、別の完全にプログラムされた機器１０６と通信する機能性）を得るために別のデジタル証明書（例えば、偽名証明書）を用いてさらにプロビジョニングされる必要があるように、機器１０６ｂを登録証明書のみによってプロビジョニングしてもよい。

【００７３】
３１５において、設置業者１３０（例えば、スタッフメンバー１３２）は、設置ステータスデータをプロビジョニングコントローラ１２０に送信する。様々な実施形態では、設

置ステータスデータは、設置された機器の不変の識別子（例えば、一度生成されて消去されることがない鍵ペアからの公開鍵などのシリアル番号または他の固定の一意の識別情報）を含む。設置ステータスデータはまた、設置業者１３０の一意の識別子、機器１０６ｂがいつどのように設置されたかを示す情報、設置された機器１０６ｂで行われたテストの結果に関する情報、設置業者１３０が適用可能な仕様、契約上の要件、および／または指示、および／または他の同様の情報に従って、機器１０６ｂを設置したことを証明する情報などの他の情報を含むことができる。

【００７４】

３２０において、プロビジョニングコントローラ１２０は、設置業者１３０からのユーザが認可されたユーザであるかどうかを判定する。そうでない場合、プロビジョニングコントローラ１２０は、設置ステータス通信を拒絶する（図３には図示せず）。一方、認可されたユーザが要求を出している場合（３２０、はい）、プロビジョニングコントローラ１２０は、設置ステータスデータで識別された機器１０６ｂが認可された機器であるかどうかを判定する（３２５）。いくつかの実施形態では、プロビジョニングコントローラ１２０は、１）機器１０６ｂに対する記録がそのデータベース１２５内に存在し、２）その記録は、機器１０６ｂが製造業者１０５にうまくプロビジョニングされたことを示し、３）その記録は、機器１０６ｂが（３２０において認可された設置業者であると検証された）設置業者１３０に送信されたことを示す、以前に格納された情報に対してそのデータベース１２５を検証することによって、機器１０６ｂが認可されていると判断することができる。

【００７５】

設置ステータスデータで識別された機器が認可されていない場合、プロビジョニングコントローラ１２０は設置ステータス通信を拒否する（図３には図示されない）。一方、設置ステータスデータで識別された機器１０６ｂが認可されている場合（３２５、はい）、プロビジョニングコントローラ１２０は、３３０において、設置ステータスデータを機器１０６ｂに関連付けられたログ情報と共に格納する。例えば、機器１０６ｂに関連付けられたログ情報は、図２の動作２２７に関して説明したようにデータベース１２５に以前に格納されていてもよい。

【００７６】

３３５において、プロビジョニングコントローラ１２０は、（例えば、設置業者１３０にある機器１０６ｂをプロビジョニングする要求をＤＡＭＳ１１０に送信することによって）プロビジョニング要求を満たすようにＤＡＭＳ１１０に指示、命令し、または他の方法でＤＡＭＳ１１０を制御する。３４０において、３３５からの要求を受信したことに応答して、およびそれを条件として、ＤＡＭＳ１１０は、３３５において要求されたデジタル資産を生成および／または検索する。様々な実施形態では、ＤＡＭＳ１１０は、図２に関して説明したように、偽名証明書または他の公開鍵証明書などの要求されたデジタル資産を作成または生成することができる。様々な実施形態では、ＤＡＭＳ１１０、またはＤＡＭ１１０の代わりにプロビジョニングコントローラ１２０は、追加または代替として、機器１０６ｂの種類の機器での使用のためにデータベース１２５に以前に格納された実行可能イメージなどのストレージから要求されたデジタル資産を検索、取得、またはさもなければアクセスすることができる。

【００７７】

３４５において、ＤＡＭＳ１１０は、３１５において設置ステータスを送信した設置業者１３０の配信機器１３１にデジタル資産を送信する。例えば、ＤＡＭＳ１１０は、偽名証明書を設置業者１３０の配信機器１３１に安全に送信することができる。

【００７８】

３５０において、配信機器１３１は、図２に関して説明したように、動作２３０～２４５と同じまたは類似の動作を実行する。３５５において、配信機器１３１は、ステータス情報をプロビジョニングコントローラ１２０に送信する。そして、３６０において、プロビジョニングコントローラ１２０は、動作２２７で格納されたステータス情報などの機器

１０６ｂに関連して以前に格納された情報に関連したステータス情報を受信して格納する。したがって、プロビジョニングコントローラ１２０は、各々の特定の機器１０６に関連付けられたシステム１００の活動のすべてについて監査跡または監査ログを継続する。

【００７９】

図３に示されるプロセス３００は、例示の目的のための一例であり、限定することを意図しない。さらに、図示のプロセス３００は、開示された特定の実施形態と一致する特定の新規かつ革新的な構成の説明を明確にするために幾分単純化された一例であるが、多くの変形が可能である。例えば、機能および動作は特定の順序で実行されるように示されているが、説明された順序は単なる一例であり、開示された特定の実施形態と矛盾しない様々な異なる動作シーケンスを実行することができる。さらに、動作は、単に説明の目的のために別々のステップとして説明され、いくつかの実施形態では、複数の動作が、同時に、および／または単一の計算もしくはより大きな動作の一部として、実行され得る。説明された動作は、網羅的、限定的、または絶対的であることを意図されておらず、様々な動作は修正、挿入、または削除することができる。

【００８０】

図４Ａおよび図４Ｂは共に、本発明の実施形態に係る、スケーラブルで安全なデジタル資産管理システムを実装するためのシステム４００の一例のブロック図である。システム４００の様々な実施形態は、極めて大量の機器トランザクションおよび証明書生成処理に使用することができる。様々な実施形態では、システム４００は、複数のサーバ、ハードウェアセキュリティモジュール、複数の計算エンジンまたはコンピューティングエンジン、および複数の仮想マシン（ＶＭ）を使用して実装することができる。システム４００の例は、プライベートデータセンター、クラウドデータセンター（例えば、ＡＷＳ）、またはプライベートデータセンターとクラウドデータセンターとのハイブリッドで実装することができる。

【００８１】

様々な実施形態では、システム４００は、図１および本開示の他のセクションに関して説明したように機能し得るデジタル資産管理システム（ＤＡＭＳ）１１０とすることができるか、その一部とすることができるか、またはそれと対話することができる。

【００８２】

図４の例に示すように、このアーキテクチャは、（好ましくは別々のサーバに実装される）２つのプロビジョニングコントローラ１２０（すなわち、プライマリおよびスタンバイ）を含むことができる。２つのプロビジョニングコントローラ１２０は、プライマリプロビジョニングコントローラに含まれるオブジェクト、データなどがコピーされるか、さもなればスタンバイ（セカンダリ）プロビジョニングコントローラに含まれるような機能を含む。プライマリプロビジョニングコントローラが何らかの理由でオフラインになった場合は、スタンバイプロビジョニングコントローラをオンラインにしてプライマリプロビジョニングコントローラに取って代わることができる。これは、プロビジョニングコントローラ１２０の連続的な（または非常に高い）可用性を提供する。様々な実施形態では、プライマリプロビジョニングコントローラおよびスタンバイプロビジョニングコントローラは、図１および本開示の他のセクションに関して説明した通りとすることができる。様々な実施形態では、プロビジョニングコントローラ１２０は、図１のプロビジョニングコントローラ１２０とＤＡＭＳ１１０との間の接続および通信に関して本明細書で説明したのと同じまたは類似の方法でシステム４００に接続することができる。一般的に、プロビジョニングコントローラ１２０は、明示的に認可された要素だけが参加してシステム４００と対話できるように、インフラストラクチャを構成するシステム要素を管理する。様々な実施形態では、プロビジョニングコントローラ１２０は、ユーザ（例えば、製造業者１０５または設置業者１３０）の従業員識別および認可システムと統合することができ、あるいは認可されたユーザのみがシステム４００を使用できるように識別および認可のための独自の機能を提供することができる。

【００８３】

システム４００のアーキテクチャは、セキュリティ関連ではないアプリケーションをセキュリティ機能から分離する。この例に示すように、登録局４２０、認証局４３０、４４０、および連携局４５０、４６０は、それら自身の専用計算エンジン４２５、４３５、４４５、５５５、４６５上で実行されるそれら自身の仮想マシン上のアプリケーションとして実装され、これらはすべて、セキュリティ関連以外のアプリケーションおよび機能とは分離している。これは、ハードウェアセキュリティモジュールの性能が遅い、またはクラウドサービスプロバイダがＨＳＭを供給することができない、またはＨＳＭの適切な管理が不確実である、従来のシステムに対する技術的およびセキュリティ上の利点および改善の両方を提供する。図４に示すように、重要なセキュリティ機能を互いに、別々の計算エンジンに分離することによって、例えば、登録局４２０、認証局４３０、４４０、および連携局４５０、４６０によって実行されるような、計算集約型の暗号およびセキュリティ機能（例えば、楕円曲線バタフライ拡張演算または楕円曲線デジタル署名）が、既存の登録局システムよりもかなり速く実行される。この設計により、「ボトルネック」アプリケーションを必要に応じて拡張できるため、トランザクション処理を大幅に改善できる。例えば、４０５および４２０で実行されている登録局アプリケーションを拡張する必要がある場合は、４２５の安全な計算機能に変更を加えることなく、追加のＶＭを追加できる。あるいはまた、セキュリティ計算が性能を制限している場合、追加の安全な計算エンジン４２５を追加することができる。これと同じ多次元スケーリングは、４００の他のコンポーネントにも当てはまる。この機能により、他の既存のＳＣＭＳシステムよりも大幅にパフォーマンスが向上する。

【００８４】

様々な実施形態では、登録局４０５は、デジタル証明書または他の種類のデジタルセキュリティ資産に対するユーザ要求を検証するプロビジョニングネットワーク内の局とすることができ、認証局（例えば、認証局４３０、４４０）がデジタル証明書を発行することを可能にし得る。様々な実施形態では、登録局４０５は、公開鍵インフラストラクチャ（ＰＫＩ）システムで知られている登録局と同様とすることができる。様々な実施形態では、登録局４０５は、Ｒｅｐｒｅｓｅｎｔａｔｉｏｎａｌ　Ｓｔａｔｅ　Ｔｒａｎｓｆｅｒ（ＲＥＳＴ）ウェブサービスとして実装することができる。登録局４０５に関して図４に示される３つの「積み重ねられた」長方形によって表されるように、様々な実施形態において、同時に実行する登録局４０５の複数のインスタンスが存在してもよい。これは、図４の他の「積み重ねられた」要素についても同様に表される。

【００８５】

矩形の左下に現れる「ＤＢ」矢印によって表されるように、登録局４０５（および「ＤＢ」矢印で示される図４の他のコンポーネント）は、データベース４７０に接続することができる。好ましい実施形態では、データベース４７０は高速アクセス、低待ち時間データベースである。いくつかの実施形態では、データベース４７０は、ＮｏＳＱＬデータベースまたはデータベースサービス（例えば、Ａｍａｚｏｎウェブサービスによって提供されるＤｙｎａｍｏＤＢデータサービス）とすることができる。様々な実施形態では、データベース４１０に格納されたデータはアプリケーションに依存するが、過去に発行された証明書、様々な連携局値、証明書が発行された機器に関するデータ、オペレータアクションなどを含み得る。データは、暗号化されていないか、暗号化されているか、またはそれらの何らかの組み合わせで格納されてもよいことに留意されたい。

【００８６】

図４に示す例では、登録局４０５は他のコンポーネントに接続され、他のコンポーネントはボックス４１０によって表されるメッセージングサブシステムまたはサービスによって互いに接続される。いくつかの実施形態では、メッセージングサービス４１０は、Ａｍａｚｏｎウェブサービスによって提供されるＡｍａｚｏｎ単純キューサービス（ＳＱＳ）などの高速メッセージキューイングサービスとすることができる。

【００８７】

様々な実施形態では、システム４００は、登録局４０５によって生成されたデジタル証

明書が異なるセグメント（例えば、登録デジタル証明書と偽名デジタル証明書）に分割されるので、登録認証局４３０と偽名認証局４４０を含む。

【００８８】

様々な実施形態では、連携局４５０、４６０は、失効の目的で、証明書要求者の識別情報（すなわち、証明書要求者の機器の一意の識別子）を発行された偽名証明書にリンクさせる。

【００８９】

様々な実施形態では、計算エンジン４２５、４３５、４４５、４５５、および４６５ならびにプロビジョニングコントローラ１２０は、ハッカーから過度に脅かされることなくこれらのコンポーネントが安全な計算を実行することを可能にするＨＳＭを含む。いくつかの実施形態では、計算エンジン４２５、４３５、４４５、４５５、および４６５は、組込み型ＨＳＭを必要とせずに安全な計算自体を実行するように設計することができ、そのような実施形態では、それらはＨＳＭを具現化する。

【００９０】

当業者であれば、図４に示すコンポーネント、プロセス、データ、動作、および実装の詳細は、説明を簡潔かつ明確にするために提示された例であることを理解するであろう。この例は限定を意図するものではなく、多くの変形が可能であるので、本発明の原理から逸脱することなく他のコンポーネント、プロセス、実施形態の詳細、および変形を使用することができる。

【００９１】

図５は、本発明の実施形態と一致するシステムおよび方法を実装するために使用することができるコンピューティングシステム５００を含む、コンピューティング環境５０１の一例のブロック図である。他のコンポーネントおよび／または配置もまた使用することができる。いくつかの実施形態では、コンピューティングシステム５００を使用して、少なくとも部分的に図１～図３の様々なコンポーネント（例えば、とりわけ、プロビジョニングコントローラ１２０およびＤＡＭＳ１１０）を実装することができる。いくつかの実施形態では、コンピューティングシステム５００と同様の一連のコンピューティングシステムは、それぞれ、専用ハードウェアでカスタマイズされ、および／または図１～図３のコンポーネントのうちの１つを実装するための専用サーバとしてプログラムすることができ、ネットワーク５３５を介して互いに通信することができる。

【００９２】

図５に示す例では、コンピューティングシステム５００は、中央処理装置（ＣＰＵ）５０５、メモリ５１０、入出力（Ｉ／Ｏ）機器５２５、ハードウェアセキュリティモジュール（ＨＳＭ）５４０、および不揮発性ストレージデバイス５２０などの多くのコンポーネントを含む。システム５００は様々な方法で実施することができる。例えば、（サーバ、ワークステーション、パーソナルコンピュータ、ラップトップなどの）統合プラットフォームとしての実装は、ＣＰＵ５０５、メモリ５１０、不揮発性ストレージ５２０、およびＩ／Ｏ機器５２５を含むことができる。そのような構成では、コンポーネント５０５、５１０、５２０、および５２５は、ローカルデータバスを介して接続および通信することができ、外部Ｉ／Ｏ接続を介して（例えば、別個のデータベースシステムとして実装される）データリポジトリ５３０にアクセスすることができる。Ｉ／Ｏコンポーネント５２５は、ローカルエリアネットワーク（ＬＡＮ）またはワイドエリアネットワーク（ＷＡＮ、例えば、携帯電話ネットワークまたはインターネット）などのネットワークを介して、および／または他の適切な接続を介して、直接通信リンク（例えば、有線またはローカルのＷｉＦｉ接続）を介して外部機器に接続することができる。システム５００はスタンドアロンでもよいし、またはより大きなシステムのサブシステムでもよい。

【００９３】

ＣＰＵ５０５は、カリフォルニア州サンタクララのインテル（登録商標）コーポレーションによって製造されたＣｏｒｅ（登録商標）ファミリーのマイクロプロセッサ、またはカリフォルニア州サニーベールのＡＭＤ（登録商標）コーポレーションによって製造され

たＡｔｈｌｏｎ（登録商標）ファミリーのマイクロプロセッサなどの１つ以上の既知のプロセッサまたは処理デバイスとすることができる。メモリ５１０は、本発明の実施形態に関連する特定の機能、方法、およびプロセスを実行するためにＣＰＵ５０５によって実行または使用される命令および情報を格納するように構成された１つ以上の高速記憶デバイスとすることができる。ストレージ５２０は、揮発性または不揮発性、磁気、半導体、テープ、光学、または他の種類のストレージデバイス、またはＣＤおよびＤＶＤなどのデバイスを含むコンピュータ可読媒体、および長期記憶を意図したソリッドステートデバイスとすることができる。

【００９４】

図示の実施形態では、メモリ５１０は、ＣＰＵ５０５によって実行されたときに、本発明と一致する様々な動作、手順、プロセス、または方法を実行する、ストレージ５２０からまたはリモートシステム（図示せず）からロードされた１つ以上のプログラムまたはアプリケーション５１５を含む。あるいはまた、ＣＰＵ５０５は、システム５００から遠隔に位置する１つ以上のプログラムを実行することができる。例えば、システム５００は、実行時に本発明の実施形態に関連する機能およびプロセスを実行する、ネットワーク５３５を介して１つ以上のリモートプログラムにアクセスすることができる。

【００９５】

一実施形態では、メモリ５１０は、プロビジョニングコントローラ１２０、ＤＡＭＳ１１０、および／または配信機器１０８、１３１について本明細書で説明されている特殊な機能および動作を実行するためのプログラム５１５を含むことができる。いくつかの実施形態では、メモリ５１０は、本発明に補助機能を提供する他の方法およびプロセスを実装する他のプログラムまたはアプリケーションも含むことができる。

【００９６】

メモリ５１０はまた、本発明とは無関係の他のプログラム（図示せず）および／またはＣＰＵ５０５によって実行されると当該技術分野で周知のいくつかの機能を実行するオペレーティングシステム（図示せず）で構成することもできる。例として、オペレーティングシステムは、Ｍｉｃｒｏｓｏｆｔ Ｗｉｎｄｏｗｓ（登録商標）、Ｕｎｉｘ（登録商標）、Ｌｉｎｕｘ（登録商標）、Ａｐｐｌｅ Ｃｏｍｐｕｔｅｒｓ（登録商標）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することができる。オペレーティングシステムの選択、さらにはオペレーティングシステムの使用にとっても、本発明にとって重要ではない。

【００９７】

ＨＳＭ５４０は、デジタルセキュリティ資産を安全に生成および格納し、および／または様々な暗号および機密計算を安全に実行する、それ自身のプロセッサを有する機器とすることができる。ＨＳＭ５４０は、暗号鍵などのデジタルセキュリティ資産とその他の機密データを可能性のある攻撃者によるアクセスから保護する。いくつかの実施形態では、ＨＳＭは、コンピューティングシステム５００に直接取り付けられたプラグインカードまたはボードとすることができる。

【００９８】

Ｉ／Ｏ機器５２５は、システム５００によってデータを受信および／または送信することを可能にする１つ以上の入出力機器を含むことができる。例えば、Ｉ／Ｏ機器５２５は、データがユーザから入力されることを可能にする（例えば、キーボード、タッチスクリーン、マウスなどの）１つ以上の入力機器を含むことができる。さらに、Ｉ／Ｏ機器５２５は、データを出力するまたはユーザに提示することを可能にする（例えば、ディスプレイスクリーン、ＣＲＴモニタ、ＬＣＤモニタ、プラズマディスプレイ、プリンタ、スピーカ装置などの）１つ以上の出力装置を含むことができる。Ｉ／Ｏ機器５２５はまた、コンピューティングシステム５００が他のマシンおよび機器と（例えば、デジタルで）通信することを可能にする１つ以上のデジタルおよび／またはアナログ通信入出力機器を含むことができる。他の構成および／またはいくつかの入力機器および／または出力機器をＩ／Ｏ機器５２５に組み込むことができる。

【００９９】
図示の実施形態では、システム５００はネットワーク５３５（例えば、インターネット、プライベートネットワーク、仮想プライベートネットワーク、携帯電話ネットワーク、または他のネットワーク、あるいはこれらの組み合わせ）に接続され、ネットワーク５３５は次いで、様々なシステムおよびコンピューティングマシン（例えば、サーバ、パーソナルコンピュータ、ラップトップコンピュータ、クライアント機器など）に接続することができる。一般的に、システム５００は、ネットワーク５３５を介して外部のマシンおよび機器からデータを入力し、外部のマシンおよび機器にデータを出力することができる。
【０１００】
図５に示す例示的な実施形態では、データソース５３０は、システム５００の外部にあるスタンドアロンデータベース（例えば、データベース１２５）である。他の実施形態では、データソース５３０は、システム５００によってホストされ得る。様々な実施形態では、データソース５３０は、本発明と一致したシステムおよび方法を実施するために使用されるデータを管理および格納することができる。例えば、データソース５３０は、システム１００によってプロビジョニングされた各々の機器１０６のステータスおよびログ情報などを含むデータ構造を管理および格納することができる。
【０１０１】
データソース５３０は、情報を記憶し、システム５００を通じてアクセスおよび／または管理される１つ以上のデータベースを含むことができる。例として、データベース５３０は、Ｏｒａｃｌｅ（登録商標）データベース、Ｓｙｂａｓｅ（登録商標）データベース、または他のリレーショナルデータベースとすることができる。しかしながら、本発明によるシステムおよび方法は、別々のデータ構造またはデータベースに、あるいはデータベースまたはデータ構造の使用にさえ限定されない。
【０１０２】
当業者であれば、図５のシステムのコンポーネントおよび実施形態の詳細は、説明を簡潔かつ明確にするために提示された例であることを理解するであろう。他のコンポーネントおよび実施形態の詳細が使用されてもよい。
【０１０３】
前述の例は、説明を明確にするために、ＯＢＵ、ＥＣＵ、およびＲＳＵなどのコンピュータ化された機器の特定の例を使用しているが、本発明はそれらの特定の例に限定されない。本発明と一致する様々な実施形態は、とりわけ、医療機器（例えば、透析機、注入ポンプなど）、ロボット、ドローン、自律走行車、無線通信モジュール（例えば、埋め込み型ユニバーサル集積回路カード（ｅＵＩＣＣ））などの多種多様なコンピュータ化された機器と共に、およびそれらのために使用することができる。
【０１０４】
本発明の他の実施形態は、本明細書の考察および本明細書に開示された本発明の実施から当業者には明らかであろう。明細書および実施例は例示としてのみ考慮されることを意図しており、本発明の真の範囲は以下の特許請求の範囲によって示される。

【図１】

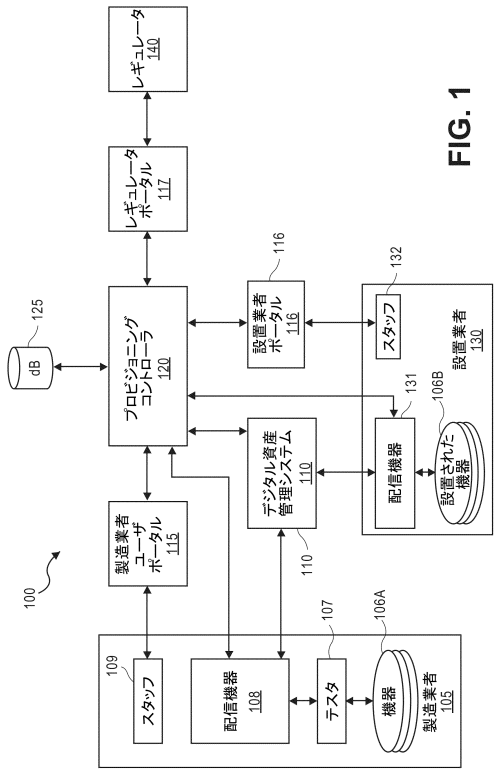

FIG. 1

【図２】

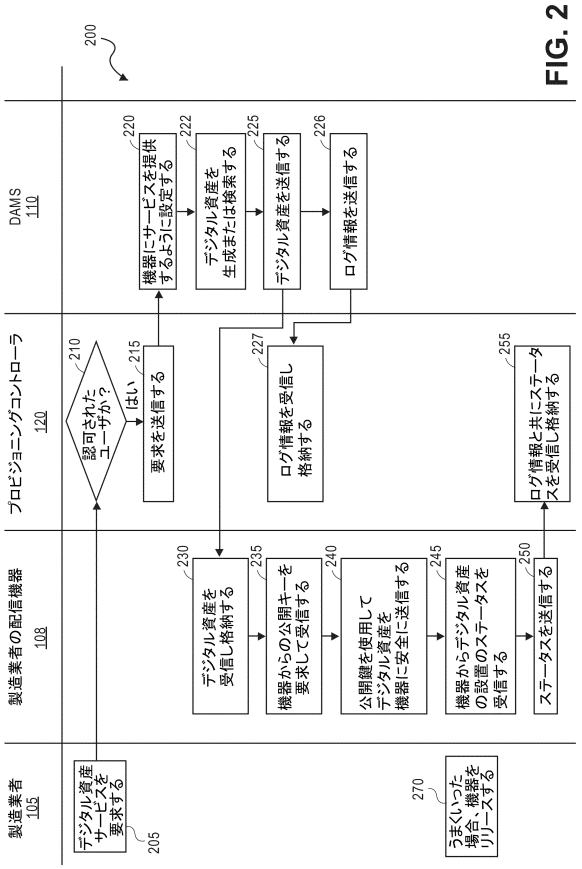

FIG. 2

【図３】

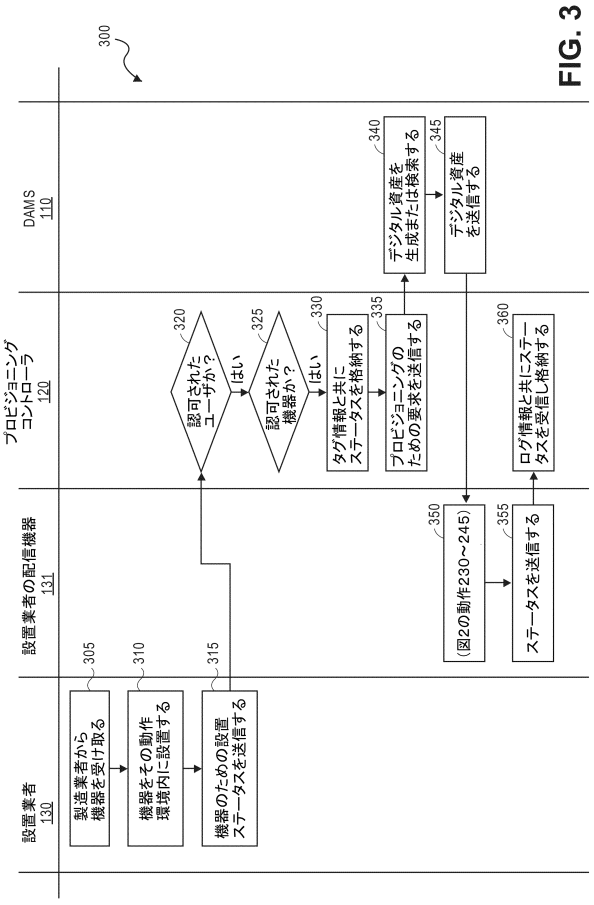

FIG. 3

【図４Ａ】

FIG. 4A

【図４Ｂ】

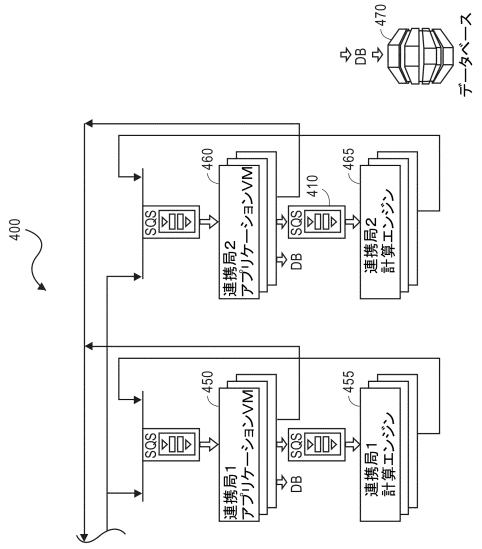

FIG. 4B

【図５】

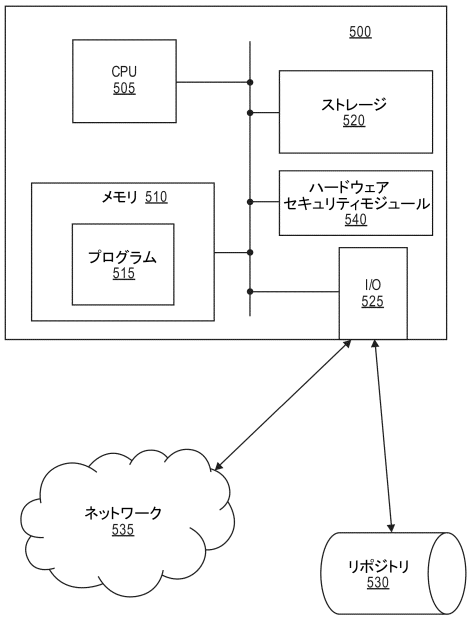

FIG. 5

フロントページの続き

(31)優先権主張番号 62/487,909
(32)優先日 平成29年4月20日(2017.4.20)
(33)優先権主張国・地域又は機関
米国(US)

早期審査対象出願

(72)発明者 セキーノ デイビッド アール.
アメリカ合衆国 ９２６１８ カリフォルニア アーバイン アーバイン センター ドライブ ７５８５ スイート ２５０ シー／オー インテグリティ セキュリティ サービシーズ エルエルシー
(72)発明者 メイヤー アラン ティー.
アメリカ合衆国 ９２６１８ カリフォルニア アーバイン アーバイン センター ドライブ ７５８５ スイート ２５０ シー／オー インテグリティ セキュリティ サービシーズ エルエルシー
(72)発明者 パウエル グレゴリー エー.
アメリカ合衆国 ９２６１８ カリフォルニア アーバイン アーバイン センター ドライブ ７５８５ スイート ２５０ シー／オー インテグリティ セキュリティ サービシーズ エルエルシー

審査官 宮司 卓佳

(56)参考文献 特表２０１７－５１３２６５（ＪＰ，Ａ）
特表２００７－５１１１６７（ＪＰ，Ａ）
特表２０１４－５０１９６６（ＪＰ，Ａ）
特開２０１３－２３５５０４（ＪＰ，Ａ）
特開２０１６－１２６７６０（ＪＰ，Ａ）
特開２０１２－８５２７２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／００－２１／８８
Ｈ０４Ｌ ９／０８