(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-516126
(P2024-516126A)
(43)公表日　令和6年4月12日(2024.4.12)

(51)国際特許分類		FI		
H04L 9/08 (2006.01)		H04L	9/08	B
H04L 9/10 (2006.01)		H04L	9/10	Z
H04L 9/32 (2006.01)		H04L	9/32	２００Ｄ
G06F 21/64 (2013.01)		G06F	21/64	
G06F 21/73 (2013.01)		G06F	21/64	３５０

審査請求　未請求　予備審査請求　未請求　（全44頁）　最終頁に続く

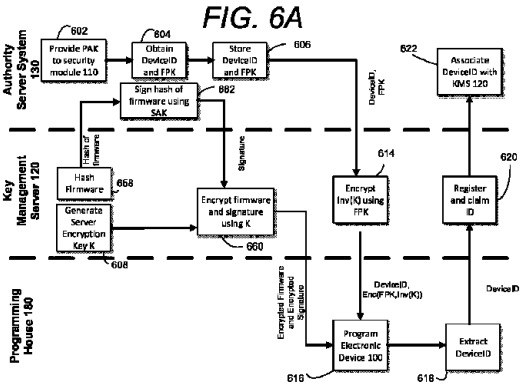
(21)出願番号　特願2023-562296(P2023-562296)
(86)(22)出願日　令和4年4月12日(2022.4.12)
(85)翻訳文提出日　令和5年12月11日(2023.12.11)
(86)国際出願番号　PCT/GB2022/050910
(87)国際公開番号　WO2022/219319
(87)国際公開日　令和4年10月20日(2022.10.20)
(31)優先権主張番号　2105203.0
(32)優先日　令和3年4月12日(2021.4.12)
(33)優先権主張国・地域又は機関
英国(GB)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　521452588
クリプト・クオンティーク・リミテッド
Ｃｒｙｐｔｏ Ｑｕａｎｔｉｑｕｅ Ｌｉｍｉｔｅｄ
英国エスイー１・０エルエイチ、ロンドン、ユニオン・ストリート１６４－１８０、ザ・プリント・ルームズ、ユニット３０４－５
(74)代理人　100145403
弁理士　山尾 憲人
(74)代理人　100135703
弁理士　岡部 英隆
(72)発明者　アーマー，マルセル
英国エスイー１・０エルエイチ、ロンドン、ユニオン・ストリート１６４－１８
最終頁に続く

(54)【発明の名称】　信頼の起点に基づくセキュリティを備えた暗号化及び認証されたファームウェアプロビジョニング

(57)【要約】
電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対するチャレンジ及びレスポンスに基づき、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含むファームウェア鍵ペアを確立する。本方法は、鍵ペアの秘密鍵を用いてファームウェアのハッシュに署名させてハッシュ上の署名を取得することを含む。公開鍵は電子装置に安全に組み込まれる。本方法は、サーバ暗号鍵を用いて、ファームウェアと、ハッシュ上の署名とを暗号化することを含む。本方法は、暗号化されたファームウェア及び暗号化された署名を復号するためのサーバ復号鍵を、ＦＰＫを用いて暗号化することを含む。本方法は、暗号化されたファームウェア、暗号化された署名、及び暗号化されたサーバ復号鍵を、電子装置へのインストールのために、サードパーティーに伝送することを含む。

FIG. 6A



10

20

【特許請求の範囲】
【請求項１】
電子装置にファームウェアを提供する方法であって、
上記電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備え、
上記セキュリティモジュールは、上記ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成され、
上記ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含み、
上記方法は、認証局鍵ペアの秘密鍵を用いて上記ファームウェアのハッシュに署名させて署名を取得することを含み、
上記認証局鍵ペアは公開鍵及び上記秘密鍵を含み、
上記公開鍵は上記電子装置に安全に組み込まれ、
上記方法は、
サーバ暗号鍵を用いて上記ファームウェア及び上記署名を暗号化することと、
上記暗号化されたファームウェア及び上記暗号化された署名を復号するためのサーバ復号鍵を、ＦＰＫを用いて暗号化することと、
上記暗号化されたファームウェア、上記暗号化された署名、及び上記暗号化されたサーバ復号鍵を、上記電子装置へのインストールのために、サードパーティーに伝送することとを含む、
方法。
【請求項２】
上記ファームウェアを受信することと、
上記ファームウェアに対してハッシュ関数を実行して上記ファームウェアのハッシュを生成することとをさらに含む、
請求項１記載の方法。
【請求項３】
上記ファームウェアのハッシュを受信することをさらに含む、
請求項１記載の方法。
【請求項４】
上記ファームウェアのハッシュに署名させることは、上記ファームウェアのハッシュに署名することを含む、
請求項１～３のうちの１つに記載の方法。
【請求項５】
上記ファームウェアのハッシュに署名させることは、上記ファームウェアのハッシュを信頼された認証局に送信することと、上記信頼された認証局から上記署名を受信することとを含む、
請求項１～３のうちの１つに記載の方法。
【請求項６】
上記ＦＰＫを信頼された認証局から受信することをさらに含む、
請求項１～５のうちの１つに記載の方法。
【請求項７】
上記サーバ暗号鍵は上記サーバ復号鍵と同じである、
請求項１～６のうちの１つに記載の方法。
【請求項８】
上記セキュリティモジュールは、上記ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて登録鍵ペア（ＥＰＫ，ＥＳＫ）を確立するようにさらに構成され、
上記登録鍵ペアは、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含み、
上記方法は、上記ＥＰＫの関数を含む装置識別子を上記サードパーティーに伝送することをさらに含む、

請求項１～７のうちの１つに記載の方法。
【請求項９】
上記装置識別子は、信頼された認証局から受信される、
請求項８記載の方法。
【請求項１０】
上記ファームウェアが上記電子装置にインストールされた後、上記装置識別子を受信することと、上記装置識別子を上記信頼された認証局に対して登録することとをさらに含む、
請求項１～９のうちの１つに記載の方法。
【請求項１１】
１つ又は複数のプロセッサによって実行されたとき、上記１つ又は複数のプロセッサに請求項１～１０のうちの１つに記載の方法を実行させる命令を格納したコンピュータ可読媒体。
【請求項１２】
１つ又は複数のプロセッサと、
上記１つ又は複数のプロセッサによって実行されたとき、上記１つ又は複数のプロセッサに請求項１～１０のうちの１つに記載の方法を実行させる命令を格納した１つ又は複数のメモリとを備える、
計算装置。
【請求項１３】
電子装置のためのファームウェアを認証する方法であって、
上記電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備え、
上記セキュリティモジュールは、上記ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいてファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立し、上記ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて登録鍵ペア（ＥＰＫ，ＥＳＫ）を確立するように構成され、
上記ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含み、
上記登録鍵ペア（ＥＰＫ，ＥＳＫ）は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含み、
上記方法は、
サーバから、安全な通信チャネルを介して、上記電子装置にインストールされるファームウェアのハッシュを受信することと、
公開認証局鍵（ＰＡＫ）及び秘密認証局鍵（ＳＡＫ）を含む認証局鍵ペアの上記秘密認証局鍵を用いて、上記ファームウェアのハッシュに署名することとを含み、
上記公開認証局鍵は、上記電子装置に安全に組み込まれ、
上記方法は、
上記電子装置へのインストールのために、サードパーティーへの上記ハッシュ上の署名の伝送を開始することと、
上記ＦＰＫと、上記電子装置を識別するための、上記ＥＰＫの関数を含む関連付けられた装置識別子とを、上記サーバへの安全な通信チャネルを介して送信することとを含む、
方法。
【請求項１４】
上記セキュリティモジュールから上記装置識別子を抽出することをさらに含む、
請求項１３記載の方法。
【請求項１５】
上記セキュリティモジュールから上記ＦＰＫを抽出することをさらに含む、
請求項１３又は１４記載の方法。
【請求項１６】

上記装置識別子及び上記ＦＰＫを受信することをさらに含む、
請求項１３又は１４記載の方法。
【請求項１７】
上記装置識別子を上記サーバに登録する要求を受信することをさらに含む、
請求項１３～１６のうちの１つに記載の方法。
【請求項１８】
上記装置識別子及び上記ＦＰＫをルックアップテーブルに入力することをさらに含む、
請求項１３～１７のうちの１つに記載の方法。
【請求項１９】
１つ又は複数のプロセッサによって実行されたとき、上記１つ又は複数のプロセッサに請求項１３～１８のうちの１つに記載の方法を実行させる命令を格納したコンピュータ可読媒体。
【請求項２０】
１つ又は複数のプロセッサと、
上記１つ又は複数のプロセッサによって実行されたとき、上記１つ又は複数のプロセッサに請求項１３～１８のうちの１つに記載の方法を実行させる命令を格納した１つ又は複数のメモリとを備える、
計算装置。
【請求項２１】
電子装置により実行する方法であって、
上記電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備え、
上記セキュリティモジュールは、上記ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成され、
上記ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含み、
上記方法は、
上記ＦＰＫを用いて暗号化されたサーバ復号鍵を、上記ＦＳＫを用いて復号することと、
上記復号されたサーバ復号鍵を用いて、ファームウェアと、上記ファームウェアのハッシュ上の署名とを復号することと、
上記電子装置に安全に組み込まれていた公開認証局鍵を用いて、上記ファームウェアのハッシュが、信頼された認証局によって署名されていることを検証することと、
上記検証に基づいて、上記復号されたファームウェアを上記電子装置にインストールすることとを含む、
方法。
【請求項２２】
ブート中に、上記ファームウェアが、信頼された当事者によって署名されていることを検証することをさらに含む、
請求項２１記載の方法。
【請求項２３】
セキュリティモジュール及び１つ又は複数のプロセッサを備える電子装置であって、
上記セキュリティモジュールは物理的複製困難関数（ＰＵＦ）を有し、
上記セキュリティモジュールは、上記ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成され、
上記ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含み、
１つ又は複数のプロセッサは、上記セキュリティモジュールを備えるか、又は、上記セキュリティモジュールに通信可能に接続され、
上記１つ又は複数のプロセッサは、

上記ＦＰＫを用いて暗号化されたサーバ復号鍵を、上記ＦＳＫを用いて復号し、
上記復号されたサーバ復号鍵を用いて、ファームウェアと、上記ファームウェアのハッシュ上の署名とを復号し、
上記電子装置に安全に組み込まれていた公開認証局鍵を用いて、上記ファームウェアのハッシュが、信頼された認証局によって署名されていることを検証し、
上記検証に基づいて、上記復号されたファームウェアを上記電子装置にインストールするように構成された、
電子装置。
【請求項２４】
電子装置にファームウェアを提供するためのシステムであって、
上記電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備え、
上記セキュリティモジュールは、上記ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成され、
上記ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含み、
上記システムは、信頼された認証局及びサーバを備え、
上記信頼された認証局は、
上記サーバからファームウェアのハッシュを受信し、
公開認証局鍵及び秘密認証局鍵を含む認証局鍵ペアの上記秘密認証局鍵を用いて、上記ファームウェアのハッシュに署名し、
上記公開認証局鍵は上記電子装置に安全に組み込まれ、
上記ファームウェアのハッシュ上の署名を上記サーバに送信し、
上記ＦＰＫを上記サーバに送信するように構成され、
上記サーバは、
上記信頼された認証局から上記署名を受信し、
上記信頼された認証局から上記ＦＰＫを受信し、
サーバ暗号鍵を用いて上記ファームウェア及び上記署名を暗号化し、
上記暗号化されたファームウェア及び上記暗号化された署名を復号するためのサーバ復号鍵を、ＦＰＫを用いて暗号化し、
上記暗号化されたファームウェア、上記暗号化された署名、及び上記暗号化されたサーバ復号鍵を、上記電子装置へのインストールのために、サードパーティーに伝送するように構成された、
システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、概して、当事者間の信頼を確立するための方法及びシステムに関する。特に、本開示は、電子装置にファームウェアを安全に提供する方法と、そのような方法を実行するように構成された計算装置とに関する。本開示は、多数の装置及びネットワークに適用可能であるが、特に、インターネット接続を有する装置に適用可能である。
【背景技術】
【０００２】
インターネットのようなネットワークは、日常のタスクが行われる方法を変更し、このことは、情報セキュリティにとって主要な意味合いを有するものであった。多数の日常のタスクが、安全に認証しまた他の当事者によって安全に認証されるために、及び／又は、プライベートな情報を安全に取り扱うために、ディジタル装置を必要とする。モノのインターネット（Internet of Things：ＩｏＴ）の開発によって、暖房及び照明のようなシステムがインターネット接続を有する装置によって制御されることがより一般的になり、年々、ますます多くの装置がインターネットに接続される。

【先行技術文献】
【特許文献】
【０００３】
【特許文献１】国際公開ＷＯ２０２０／２１２６８９Ａ１号（２０２０年４月８日に出願され、「Device Identification With Quantum Tunnelling Currents」のタイトルを有する国際特許出願番号第ＰＣＴ／ＧＢ２０２０／０５０９１８号）
【特許文献２】英国特許出願番号第２１０５１８５．９号明細書（２０２１年４月１２日に出願され、「Interim Root-Of-Trust Enrolment And Device-Bound Public Key Registration」のタイトルを有する）
【特許文献３】英国特許出願番号第２１０５１８３．４号明細書（２０２１年４月１２日に出願され、「Secure Root-Of-Trust Enrolment And Identity Management Of Embedded Devices」のタイトルを有する）
【発明の概要】
【発明が解決しようとする課題】
【０００４】
ＩｏＴ装置のような電子装置に秘密情報を安全に提供することの固有の困難は、装置の登録、すなわち、相互接続された装置のグリッドへのその加入のような、さらなる後段の処理に影響する可能性がある。しばしば、予め共有された鍵又は非対称鍵ペアの秘密鍵、及び／又は装置証明書のような秘密情報が、サービスに登録するために使用する何らかの基礎的なクレデンシャルを装置に提供するために、製造時に装置に安全に提供されなければならない。再び、このことが安全に実行されうる程度に関する制限が存在する。
【０００５】
典型的なシナリオにおいて、ＯＥＭ（Original Equipment Manufacturer）は、製造した装置に、ＩｏＴサービスへの登録を可能にするための身元情報を提供することと、装置にファームウェアを安全にインストールすることとを達成しようとすることがある。装置は、例えば、鍵を格納するための安全な領域を有するマイクロコントローラを含んでもよく、マイクロコントローラは、サードパーティーの製造業者によって製造されていてもよい。ＯＥＭ又は製造業者は、例えば、秘密鍵及び装置証明書を安全な領域に投入することがあり、安全な設備を必要とする。装置にファームウェア／証明書をインストールするために、ＯＥＭは、装置を構成するプログラミング会社のサービスを使用してもよく、このことは、さらなる信頼を必要とする。プログラミング会社は、安全な設備を運用し、正しい情報を投入し、ＯＥＭに代わって証明書に安全に署名すると信頼されなければならない。いくつかの状況では、装置を提供することは、互いに異なる複数の当事者が電子装置と相互動作することを必要とする可能性がある。しかしながら、これらの異なる当事者は、電子装置にインストールされる情報、例えば、ファームウェア又は証明書にアクセスしている可能性があり、従って、電子装置にそれがインストールされる前に、これらの当事者のいずれかが情報を改竄するリスクが存在する。
【０００６】
本発明の実施形態の目的は、当該技術において既知の１つ又は複数の問題を少なくとも緩和することにある。
【課題を解決するための手段】
【０００７】
本発明の態様によれば、電子装置にファームウェアを提供する方法が提供される。電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成される。ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含む。本方法は、認証局鍵ペアの秘密鍵を用いてファームウェアのハッシュに署名させて署名を取得することを含む。認証局鍵ペアは公開鍵及び秘密鍵を含み、公開鍵は電子装置に安全に組み込まれる。本方法は、サーバ暗号鍵を用いてファームウェア及び署名を暗号化する

ことをさらに含む。本方法は、暗号化されたファームウェア及び暗号化された署名を復号するためのサーバ復号鍵を、ＦＰＫを用いて暗号化することをさらに含む。本方法は、暗号化されたファームウェア、暗号化された署名、及び暗号化されたサーバ復号鍵を、電子装置へのインストールのために、サードパーティーに伝送することをさらに含む。

【０００８】

優位点として、本方法は、電子装置のみがファームウェアを復号できるように、暗号化された形式でファームウェアが電子装置に提供されることを可能にする。このことは、プロプライエタリなファームウェアが機密のままであると、ファームウェアの作成者、例えばＯＥＭ（original equipment manufacturer）が信頼しうることを保証する。電子装置の製造及びプログラミングに関与する他の当事者、例えば、サードパーティーのプログラミング会社は、改竄を検出可能にすることなく、ファームウェアを改竄することができない。

【０００９】

優位点として、ファームウェア鍵ペアは、ＰＵＦに対するチャレンジ及びレスポンスに基づき、このことは、秘密情報が製造中に装置に投入されることを必要とせず、また、装置のメモリに秘密鍵が格納されることを必要としない、ということを意味する。

【００１０】

本方法は、ファームウェアを受信することと、ファームウェアに対してハッシュ関数を実行してファームウェアのハッシュを生成することとをさらに含んでもよい。

【００１１】

本方法は、ファームウェアのハッシュを受信することをさらに含んでもよい。

【００１２】

ファームウェアのハッシュに署名させることは、ファームウェアのハッシュに署名することを含んでもよい。

【００１３】

ファームウェアのハッシュに署名させることは、ファームウェアのハッシュを信頼された認証局に送信することと、信頼された認証局から署名を受信することとを含んでもよい。

【００１４】

本方法は、ＦＰＫを信頼された認証局から受信することをさらに含んでもよい。

【００１５】

サーバ暗号鍵はサーバ復号鍵と同じであってもよい。代替として、非対称なサーバ暗号鍵及びサーバ復号鍵が使用されてもよい。

【００１６】

セキュリティモジュールは、ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含む登録鍵ペア（ＥＰＫ，ＥＳＫ）を確立するようにさらに構成されてもよく、本方法は、ＥＰＫの関数を含む装置識別子をサードパーティーに伝送することをさらに含んでもよい。従って、優位点として、装置識別子は、ＰＵＦに対するチャレンジ及びレスポンスに基づくＥＰＫ及びＥＳＫにリンクされ、従って、装置に身元情報を提供するために、製造中に、装置に秘密情報を投入することを必要としない。

【００１７】

装置識別子は、信頼された認証局から受信されてもよい。

【００１８】

本方法は、ファームウェアが電子装置にインストールされた後、装置識別子を受信することと、装置識別子を信頼された認証局に対して登録することとをさらに含んでもよい、信頼された認証局に対して装置識別子を登録することによって、装置識別子が登録されていない他の当事者が電子装置と通信することを禁止しうるので、セキュリティは向上する。具体的には、装置識別子は、特定のサーバに関連付けられ、したがって、他のサードパーティーは、サーバの認可なしに、装置と相互動作できない。

【００１９】
本発明の態様によれば、コンピュータ可読媒体が提供される。コンピュータ可読媒体は、１つ又は複数のプロセッサによって実行されたとき、上述した電子装置にファームウェアを提供する方法を１つ又は複数のプロセッサに実行させる命令を格納している。
【００２０】
本発明の態様によれば、計算装置が提供される。計算装置は１つ又は複数のプロセッサを備える。計算装置はさらに１つ又は複数のメモリを備え、１つ又は複数のメモリは、１つ又は複数のプロセッサによって実行されたとき、上述した電子装置にファームウェアを提供する方法を１つ又は複数のプロセッサに実行させる命令を格納している。
【００２１】
本発明の態様によれば、電子装置のためのファームウェアを認証する方法が提供される。電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいてファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立し、ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて登録鍵ペア（ＥＰＫ，ＥＳＫ）を確立するように構成される。ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含む。登録鍵ペア（ＥＰＫ，ＥＳＫ）は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含む。本方法は、サーバから、安全な通信チャネルを介して、電子装置にインストールされるファームウェアのハッシュを受信することを含む。本方法は、公開認証局鍵（ＰＡＫ）及び秘密認証局鍵（ＳＡＫ）を含む認証局鍵ペアの秘密認証局鍵を用いて、ファームウェアのハッシュに署名することを含む。公開認証局鍵は電子装置に安全に組み込まれる。本方法は、電子装置へのインストールのために、サードパーティーへの署名の伝送を開始することを含む。本方法は、ＦＰＫと、電子装置を識別するための、ＥＰＫの関数を含む関連付けられた装置識別子とを、サーバへの安全な通信チャネルを介して送信することを含む。
【００２２】
優位点として、そのような方法は、信頼された認証局がファームウェアにアクセスすることなく、電子装置が、その信頼された認証局によって認可されているファームウェアを受信することを可能にする。さらに、暗号化されていない形式で秘密情報を電子装置に投入することを必要としない。
【００２３】
本方法は、セキュリティモジュールから装置識別子を抽出することをさらに含んでもよい。
【００２４】
本方法は、セキュリティモジュールからＦＰＫを抽出することをさらに含んでもよい。
【００２５】
本方法は、装置識別子及びＦＰＫを受信することをさらに含んでもよい。
【００２６】
本方法は、装置識別子をサーバに登録する要求を受信することをさらに含んでもよい。
【００２７】
本方法は、装置識別子及びＦＰＫをルックアップテーブルに入力することをさらに含んでもよい。
【００２８】
本発明の態様によれば、コンピュータ可読媒体が提供される。コンピュータ可読媒体は、１つ又は複数のプロセッサによって実行されたとき、上述した電子装置のためのファームウェアを認証する方法を１つ又は複数のプロセッサに実行させる命令を格納している。
【００２９】
本発明の態様によれば、計算装置が提供される。コンピュータ装置は１つ又は複数のプロセッサを備える。計算装置はさらに１つ又は複数のメモリを備え、１つ又は複数のメモリは、１つ又は複数のプロセッサによって実行されたとき、上述した電子装置のためのフ

ファームウェアを認証する方法を１つ又は複数のプロセッサに実行させる命令を格納している。

【００３０】

本発明の態様によれば、電子装置により実行される方法が提供される、電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備え、セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成され、ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含む。本方法は、ＦＰＫを用いて暗号化されたサーバ復号鍵を、ＦＳＫを用いて復号することを含む。と、本方法は、復号されたサーバ復号鍵を用いて、ファームウェアと、ファームウェアのハッシュ上の署名とを復号することをさらに含む。本方法は、電子装置に安全に組み込まれていた公開認証局鍵を用いて、ファームウェアのハッシュが、信頼された認証局によって署名されていることを検証することをさらに含む。本方法は、検証に基づいて、復号されたファームウェアを電子装置にインストールすることとをさらに含む。

【００３１】

本方法は、電子装置のブート中に、ファームウェアが、信頼された当事者によって署名されていることを検証することをさらに含んでもよい。

【００３２】

本発明の態様によれば、電子装置が提供される。電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成される。ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含む。電子装置は１つ又は複数のプロセッサをさらに備える。１つ又は複数のプロセッサは、セキュリティモジュールを備えるか、又は、セキュリティモジュールに通信可能に接続される。１つ又は複数のプロセッサはＦＰＫを用いて暗号化されたサーバ復号鍵を、ＦＳＫを用いて復号するように構成される。１つ又は複数のプロセッサは、復号されたサーバ復号鍵を用いて、ファームウェアと、ファームウェアのハッシュ上の署名とを復号するように構成される。１つ又は複数のプロセッサは、電子装置に安全に組み込まれていた公開認証局鍵を用いて、ファームウェアのハッシュが、信頼された認証局によって署名されていることを検証するように構成される。１つ又は複数のプロセッサは、検証に基づいて、復号されたファームウェアを電子装置にインストールするように構成される。

【００３３】

優位点として、電子装置にファームウェアが安全に提供される。電子装置上に、製造中、秘密情報が格納されない。さらに、セキュリティの一部が、電子装置にインストールされたＰＵＦに対するチャレンジ及びレスポンスに基づくので、関連する秘密鍵は、電子装置上に格納されることをいっさい必要とせず、代わりに、必要とされたときに動的に再生成されてもよい。

【００３４】

本発明の態様によれば、電子装置にファームウェアを提供するためのシステムが提供される。電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成される。ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含む。本システムは、信頼された認証局と、サーバとを備える。信頼された認証局は、サーバからファームウェアのハッシュを受信するように構成される。信頼された認証局は、公開認証局鍵及び秘密認証局鍵を含む認証局鍵ペアの秘密認証局鍵を用いて、ファームウェアのハッシュに署名するように構成される。公開認証局鍵は電子装置に安全に組み込まれる。信頼された認証局は、ファームウェアのハッシュ上の署名をサーバに送信するように構成される。信頼された認証局は、ＦＰＫをサーバに送信するように構成される。

サーバは、信頼された認証局からファームウェア上の署名を受信するように構成される。サーバは、信頼された認証局からＦＰＫを受信するように構成される。サーバは、サーバ暗号鍵を用いてファームウェア及び署名を暗号化するように構成される。サーバは、暗号化されたファームウェア及び暗号化された署名を復号するためのサーバ復号鍵を、ＦＰＫを用いて暗号化するように構成される。サーバは、暗号化されたファームウェア、暗号化された署名、及び暗号化されたサーバ復号鍵を、電子装置へのインストールのために、サードパーティーに伝送するように構成される。

【００３５】

本発明の態様によれば、電子装置にファームウェアを提供する方法が提供される。電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成される。ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含む。本方法は、公開鍵及び秘密鍵を含む認証局／署名鍵ペアの秘密鍵を用いて、暗号化された形式のファームウェアに署名させることを含む。公開鍵は電子装置に安全に組み込まれる。ファームウェアは、サーバ暗号鍵を用いて暗号化される。本方法は、電子装置へのインストールのために、暗号化及び署名された形式のファームウェアをサードパーティーに伝送することをさらに含む。本方法は、電子装置へのインストールのために、暗号化された形式のサーバ複合鍵をサードパーティーに伝送することをさらに含む。サーバ復号鍵は、暗号化された形式のファームウェアの復号用である。サーバ復号鍵は、ＦＰＫを用いて暗号化される。

【００３６】

優位点として、本方法は、電子装置のみがファームウェアを復号できるように、暗号化された形式でファームウェアが電子装置に提供されることを可能にする。このことは、プロプライエタリなファームウェアが機密のままであると、ファームウェアの作成者、例えばＯＥＭ（original equipment manufacturer）が信頼しうることを保証する。電子装置の製造及びプログラミングに関与する他の当事者は、ファームウェアを改竄することができない。

【００３７】

優位点として、ファームウェア鍵ペアは、ＰＵＦに対するチャレンジ及びレスポンスに基づき、このことは、秘密情報が製造中に装置に投入されることを必要とせず、また、装置のメモリに秘密鍵が格納されることを必要としない、ということを意味する。

【００３８】

本方法は、ファームウェアを受信することと、ファームウェアを暗号化して、暗号化された形式のファームウェアを生成することとをさらに含んでもよい。本方法は、暗号化された形式のファームウェアを受信することをさらに含んでもよい。

【００３９】

暗号化された形式のファームウェアに署名させることは、暗号化された形式のファームウェアに署名することを含んでもよい、暗号化された形式のファームウェアに署名させることは、暗号化された形式のファームウェアを信頼された認証局に送信することと、信頼された認証局から暗号化及び署名された形式のファームウェアを受信することとを含んでもよい。暗号化された形式のファームウェアに署名することは、装置にインストールする前におけるファームウェアのいかなる改竄も検出可能になることを保証し、ダウンストリームのセキュリティ対策の信頼性をもたらす。

【００４０】

本方法は、ＦＰＫを信頼された認証局から受信することをさらに含んでもよい。

【００４１】

本方法は、ＦＰＫを用いてサーバ暗号鍵を暗号化することをさらに含んでもよい。

【００４２】

サーバ暗号鍵はサーバ復号鍵と同じであってもよい。

【００４３】
セキュリティモジュールは、ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含む登録鍵ペア（ＥＰＫ，ＥＳＫ）を確立するようにさらに構成されてもよい。本方法は、ＥＰＫの関数を含む装置識別子をサードパーティーに伝送することをさらに含んでもよい。関数は暗号ハッシュ関数を含んでもよい。優位点として、装置識別子は、ＰＵＦに対するチャレンジ及びレスポンスに基づくＥＰＫ及びＥＳＫにリンクされ、従って、製造中に、装置に秘密情報を投入することを必要としない。
【００４４】
装置識別子は、信頼された認証局から受信されてもよい。
【００４５】
本方法は、ファームウェアが電子装置にインストールされた後、装置識別子を受信することと、装置識別子を信頼された認証局に対して登録することとをさらに含んでもよい、信頼された認証局に対して装置識別子を登録することによって、装置識別子が登録されていない他の当事者が電子装置と通信できないので、セキュリティは向上する。具体的には、装置識別子はそのサーバに関連付けられ、したがって、他のサードパーティーは、サーバの認可なしに、装置と相互動作できない。
【００４６】
本発明の態様によれば、コンピュータ可読媒体が提供される。コンピュータ可読媒体は、１つ又は複数のプロセッサによって実行されたとき、上述した電子装置にファームウェアを提供する方法を１つ又は複数のプロセッサに実行させる命令を格納している。
【００４７】
本発明の態様によれば、計算装置が提供される。計算装置は１つ又は複数のプロセッサを備える。計算装置はさらに１つ又は複数のメモリを備え、１つ又は複数のメモリは、１つ又は複数のプロセッサによって実行されたとき、上述した電子装置にファームウェアを提供する方法を１つ又は複数のプロセッサに実行させる命令を格納している。
【００４８】
本発明の態様によれば、電子装置のためのファームウェアを認証する方法が提供される。電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいてファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立し、ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて登録鍵ペア（ＥＰＫ，ＥＳＫ）を確立するように構成される。ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含む。登録鍵ペア（ＥＰＫ，ＥＳＫ）は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含む。本方法は、サーバから、安全な通信チャネルを介して、電子装置にインストールされるファームウェアであって、暗号化ファームウェアを受信することを含む。本方法は、公開認証局鍵及び秘密認証局鍵を含む認証局鍵ペアの秘密認証局鍵を用いて、暗号化されたファームウェアに署名することをさらに含む。公開認証局鍵は電子装置に安全に組み込まれる。本方法は、電子装置へのインストールのために、サードパーティーへの暗号化及び署名されたファームウェアの伝送を開始することをさらに含む。本方法は、安全な通信チャネルを介して、ルックアップテーブルをサーバに送信することをさらに含む。ルックアップテーブルは、ＦＰＫと、電子装置を識別するための、ＥＰＫの関数を含む関連付けられた装置識別子とを示す。関数は暗号ハッシュ関数を含んでもよい。
【００４９】
優位点として、そのような方法は、信頼された認証局が暗号化されていない形式でファームウェアにアクセスすることなく、電子装置が、その信頼された認証局によって認可されているファームウェアを受信することを可能にする。さらに、暗号化されていない形式で秘密情報を電子装置に投入することを必要としない。
【００５０】
本方法は、セキュリティモジュールから装置識別子を抽出することをさらに含んでもよ

い。本方法は、セキュリティモジュールからＦＰＫを抽出することをさらに含んでもよい。本方法は、装置識別子及びＦＰＫを受信することを含んでもよい。

【００５１】

本方法は、装置識別子をサーバに登録する要求を受信することをさらに含んでもよい。サーバに対して装置識別子を登録することによって、装置識別子が登録されていない他の当事者が電子装置と通信できないので、セキュリティは向上する。本方法は、装置識別子及びＦＰＫをルックアップテーブルに入力することをさらに含んでもよい。

【００５２】

本発明の態様によれば、コンピュータ可読媒体が提供される。コンピュータ可読媒体は、１つ又は複数のプロセッサによって実行されたとき、上述した電子装置のためのファームウェアを認証する方法を１つ又は複数のプロセッサに実行させる命令を格納している。

【００５３】

本発明の態様によれば、計算装置が提供される。計算装置は１つ又は複数のプロセッサを備える。計算装置はさらに１つ又は複数のメモリを備え、１つ又は複数のメモリは、１つ又は複数のプロセッサによって実行されたとき、上述した電子装置のためのファームウェアを認証する方法を１つ又は複数のプロセッサに実行させる命令を格納している。

【００５４】

本発明の態様によれば、電子装置により実行される方法が提供される。電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含むファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成される。本方法は、ＦＰＫを用いて暗号化されたサーバ復号鍵を、ＦＳＫを用いて復号することを含む。本方法は、電子装置に安全に組み込まれていた公開認証局鍵を用いて、暗号化された形式のファームウェアが、信頼された認証局によって認証されていることを検証することをさらに含む。本方法は、復号されたサーバ復号鍵を用いて、電子装置にインストールされるファームウェアを復号することをさらに含む。

【００５５】

優位点として、電子装置にファームウェアが安全に提供される。電子装置上に、製造中、秘密情報が格納されない。さらに、セキュリティの一部が、電子装置にインストールされたＰＵＦに対するチャレンジ及びレスポンスに基づくので、関連する秘密鍵は、電子装置上に格納されることをいっさい必要とせず、代わりに、必要とされたときに動的に再生成されてもよい。

【００５６】

本発明の態様によれば、コンピュータ可読媒体が提供される。コンピュータ可読媒体は、１つ又は複数のプロセッサによって実行されたとき、１つ又は複数のプロセッサに下記の方法を実行させる命令を格納する。本方法は、ＦＰＫを用いて暗号化されたサーバ復号鍵を、ＦＳＫを用いて復号することと、電子装置に安全に組み込まれていた公開認証局鍵を用いて、暗号化された形式のファームウェアが、信頼された認証局によって認証されていることを検証することと、復号されたサーバ復号鍵を用いて、電子装置にインストールされるファームウェアを復号することとを含む。

【００５７】

本発明の態様によれば、電子装置が提供される。電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含むファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成される。電子装置は１つ又は複数のプロセッサをさらに備える。１つ又は複数のプロセッサは、セキュリティモジュールを備えるか、又は、セキュリティモジュールに通信可能に接続される。１つ又は複数のプロセッサは、ＦＰＫを用いて暗号化されたサーバ復号鍵を、ＦＳＫを用いて復号し、電子装置に安全に組み込まれていた公開認証

局鍵を用いて、暗号化された形式のファームウェアが、信頼された認証局によって認証されていることを検証し、復号されたサーバ復号鍵を用いて、電子装置にインストールされるファームウェアを復号するように構成される。

【００５８】

本発明の態様によれば、電子装置にファームウェアを提供するためのシステムが提供される。電子装置は、物理的複製困難関数（ＰＵＦ）を有するセキュリティモジュールを備える。セキュリティモジュールは、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいてファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立し、ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて登録鍵ペア（ＥＰＫ，ＥＳＫ）を確立するように構成される。ファームウェア鍵ペアは、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含む。登録鍵ペア（ＥＰＫ，ＥＳＫ）は、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含む。本システムは、信頼された認証局と、サーバとを備える。信頼された認証局は、サーバから、暗号化されたファームウェアを受信するように構成される。信頼された認証局は、公開認証局鍵及び秘密認証局鍵を含む認証局鍵ペアの秘密認証局鍵を用いて、暗号化されたファームウェアに署名するようにさらに構成される。公開認証局鍵は電子装置に安全に組み込まれる。信頼された認証局は、暗号化及び署名されたファームウェアをサーバに送信するようにさらに構成される。信頼された認証局は、電子装置を識別するための装置識別子であって、ＥＰＫの関数を含む装置識別子を、サーバに送信するようにさらに構成される。信頼された認証局は、ＦＰＫをサーバに送信するようにさらに構成される。サーバは、サーバ暗号鍵を用いて暗号化された形式ファームウェアを、署名のために、信頼された認証局に送信するように構成される。サーバは、信頼された認証局から暗号化及び署名されたファームウェアを受信するようにさらに構成される。サーバは、信頼された認証局から装置識別子及びＦＰＫを受信するようにさらに構成される。サーバは、暗号化されたファームウェアを復号するためのサーバ復号鍵を、ＦＰＫを用いて暗号化するようにさらに構成される。サーバは、装置識別子、暗号化されたサーバ復号鍵、及び暗号化及び署名されたファームウェアを、電子装置へのインストールのために、サードパーティーに伝送するようにさらに構成される。

【００５９】

本願において説明する方法を実行するためのコンピュータプログラム及び／又はコード／命令は、コンピュータ可読媒体又はコンピュータプログラム製品において、コンピュータのような装置に提供されてもよい。コンピュータ可読媒体は、例えば、電子的、磁気的、光学的、電磁的、赤外線、半導体システム、又はデータ送信のための、例えばインターネットを介してコードをダウンロードするための伝搬媒体であってもよい。代替として、コンピュータ可読媒体は、半導体又はソリッドステートメモリ、磁気テープ、取り外し可能なコンピュータディスケット、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、剛体磁気ディスク、及びＣＤ－ＲＯＭ、ＣＤ－Ｒ／Ｗ、又はＤＶＤなどの光ディスクのような、物理的コンピュータ可読媒体の形式を有してもよい。

【００６０】

本願において説明された発明の多数の変形例及び他の実施形態は、本願において提示した開示内容に照らして、これらの発明が関連する技術分野の当業者に理解される。従って、本開示は、本願において開示した特定の実施形態に限定されないことが理解されるであろう。また、本願において提供した説明は、構成要素の所定の組み合わせのコンテキストにおける例示的な実施形態を提供するが、ステップ及び／又は機能は、本発明の範囲から離れることなく、代替の実施形態によって提供されてもよい。

【図面の簡単な説明】

【００６１】

【図１】発明の詳細な説明の全体にわたって例示の目的でのみ参照される、様々な当事者の図を示す。

【図２】通信システムを示す。

【図３Ａ】電子装置のブロック図を示す。

【図３Ｂ】マイクロコントローラの図を示す。
【図４Ａ】セキュリティモジュールのブロック図を示す。
【図４Ｂ】ＰＵＦモジュールのブロック図を示す。
【図５】計算装置のブロック図を示す。
【図６Ａ】電子装置にファームウェアを提供する方法を示す。
【図６Ｂ】電子装置にファームウェアを提供する他の方法を示す。
【図７Ａ】フローチャートを示す。
【図７Ｂ】フローチャートを示す。
【図８Ａ】フローチャートを示す。
【図８Ｂ】フローチャートを示す。
【図９Ａ】フローチャートを示す。
【図９Ｂ】フローチャートを示す。
【図１０】コンピュータ可読媒体のブロック図を示す。
【発明を実施するための形態】
【００６２】
本発明の実施形態は、添付図面を参照して、例示としてのみ、さらに説明される。
【００６３】
説明及び図面の全体にわたって、同様の参照符号は同様の部分を参照する。
【００６４】
様々な実施形態が下記に説明されているが、本発明はこれらの実施形態に限定されず、また、これらの実施形態の変形例は本発明の範囲内に含まれ、本発明の範囲は、添付された特許請求の範囲によってのみ限定されるであろう。
【００６５】
下記では、ＩｏＴ装置のセキュリティ及び登録を参照する。しかしながら、当業者は、本願において説明した方法、システム、及び装置が、さらにずっと広く適用可能であることを認識するであろう。
【００６６】
下記では、電子装置にファームウェアを安全に提供する方法を説明する。本願において説明する方法は、関連する様々な当事者が特に電子装置のセキュリティを互いにゆだねることを必要とすることなく、電子装置にファームウェアをインストールすることを可能にする。説明の簡単化のために、いくつかの利害関係者（例えば、ＯＥＭ及びＩｏＴハブ）を含む例示的なシナリオを図１に示し、発明の詳細な説明の全体にわたって参照する。しかしながら、本願において説明する方法は、当業者によって認識されるように、より一般的に適用可能である。
【００６７】
発明の詳細な説明を読むことで認識されるように、電子装置には物理的複製困難関数が提供されてもよい。物理的複製困難関数（物理的に複製困難な関数又はＰＵＦ（physical unclonable function）としても知られる）は、安全なＥＥＰＲＯＭ及び他の高価なハードウェアの要件なしに、認証及び秘密鍵格納のために使用される暗号プリミティブである。ディジタルメモリに秘密を格納する代わりに、ＰＵＦは、通常は製造中に導入される、１つ又は複数の構成要素の一意的な物理的特性から秘密を導出する。既知のＰＵＦは、小さなシリカ球を含む懸濁物である硬化エポキシ樹脂のシートを介するレーザ光の散乱、又は、何らか回路のゲート遅延における製造時の変動のような現象に基づく。
【００６８】
下記では、物理的に複製困難な関数、物理的複製困難関数、及びＰＵＦという用語は、交換可能に使用される。ＰＵＦは、機能的動作を実行するという目的を有する、すなわち、所定の入力により問い合わせを受けたとき、ＰＵＦは測定可能な出力を生成する。ＰＵＦに対する１つの入力が、１つよりも多くの可能な出力を有してもよいので、ＰＵＦは、数学的な意味において、真の関数ではない。典型的には、ＰＵＦに対する入力は「チャレンジ」と呼ばれ、ＰＵＦの結果として得られる出力は「レスポンス」と呼ばれる。印加さ

れたチャレンジと、その測定されたレスポンスとは、「チャレンジ・レスポンスペア」（challenge-response pair：ＣＲＰ）として知られる。本願で使用される用語「チャレンジ」は、ＰＵＦに提供される、選択された入力（例えば、アレイの特定のセルの選択、特定の電圧の適用、など）を意味すると理解され、また、用語「レスポンス」は、ＰＵＦの対応する出力を参照するように本願において使用される。

【００６９】

電子装置での使用に適しているならば、任意の適切なＰＵＦが、本願において説明したシステム及び方法とともに使用されてもよい。例えば、ＰＵＦは、ＳＲＡＭ　ＰＵＦであってもよい。ＳＲＡＭ　ＰＵＦは、ＳＲＡＭのしきい値電圧におけるランダムな差分を使用して、一意のチャレンジ・レスポンスペアを生成する。

【００７０】

適切なＰＵＦの他の実施例は遅延ＰＵＦであり、これは、チップにおける導線又はゲートにおける遅延のランダムな変動を利用する。入力チャレンジが与えられると、回路において競合条件がセットアップされ、異なる経路に沿って伝搬する２つの遷移が比較されて、どちらが先に到来するか（レスポンス）を確かめる。

【００７１】

ＰＵＦの他の実施例において、量子閉じ込めを利用してもよい。例えば、ＰＵＦは、いくつかの共振トンネルダイオードから形成されてもよい。

【００７２】

ＰＵＦの他の実施例において、量子トンネルバリアを介する量子トンネルを利用してもよい。ＰＵＦの一例は、特許文献１において説明される。実施例によれば、ＰＵＦは、個々にアドレス指定可能な複数のセルを有するアレイを備えてもよい。各セルは、量子トンネルバリアを有する基本回路を備えてもよい。セルは、トランジスタの形式を有する第１の電子部品と、第２の電子的トランジスタの形式を有する第２の電子部品とを備えてもよい。第１のトランジスタのソース、ドレイン、及びボディは、同じ電位（例えば接地）に保持されてもよい。第２のトランジスタのソース、ドレイン、及びボディもまた、すべて同じ電位に保持されてもよい。第１のトランジスタは、トランジスタのチャネルとゲート端子との間に第１の量子トンネルバリアを有する。第２のトランジスタは、トランジスタのチャネルとゲート端子との間に第２の量子トンネルバリアを有する。製造中に導入されたトランジスタの固有差に起因して、第１の量子トンネルバリアは第１のトランジスタを一意的に特徴づけ、第２の量子トンネルバリアは第２のトランジスタを一意的に特徴づける。セルは、第１の量子トンネルバリア及び第２の量子トンネルバリアにわたって電位差を印加するために、行デコーダ及び列デコーダを用いて選択されてもよい。電位差は、第１の量子トンネルバリア及び第２の量子トンネルバリアのいずれかを電流が古典的に通過できるしきい値電圧未満であってもよい。従って、いったんセルが選択されると、第１のトランジスタの第１の量子トンネルバリアを介して量子トンネル電流が流れてもよく、第２のトランジスタの第２の量子トンネルバリアを介し量子トンネル電流が流れてもよい。古典的電流は流れなくてもよい。量子トンネル電流は、比較及び増幅されてもよい。セル及び印加電圧の組み合わせはチャレンジとみなされてもよく、出力される量子トンネル電流はレスポンスとみなされてもよい。

【００７３】

他の実施例では、ＰＵＦは、それが電子的に相互動作できる限り、電子部品に基づくことを必要としない。

【００７４】

下記では、非対称鍵ペアとしても知られる、いくつかの公開鍵ペアを参照する。公開鍵ペアは、他の当事者と共有されてもよい公開鍵と、共有されない対応する秘密鍵とを含む。公開鍵は、秘匿される必要はない公開値であるが、改竄できないように格納されるべきである。実施例では、公開鍵は、いかなる方法でも書きかえも変更も不可能であることを保証するために、電子装置のＲＯＭに格納されてもよい。本願において説明する公開鍵ペアは、多くの場合、名前を有する。例えば、１つの公開鍵ペアは、「ファームウェア公開

鍵」（firmware public key：ＦＰＫ）及び対応する「ファームウェア秘密鍵」（firmware secret key：ＦＳＫ）を含む「ファームウェア公開鍵ペア」として記述される。もう１つの公開鍵ペアは、「登録公開鍵」（enrolment public key：ＥＰＫ）及び対応する「登録秘密鍵」（enrolment secret key：ＥＳＫ）を含む「登録公開鍵ペア」として記述される。もう１つの公開鍵ペアは、「公開認証局鍵」（public authority key：ＰＡＫ）及び対応する「秘密認証局鍵」（secret authority key：ＳＡＫ）を含む「認証局鍵ペア」として記述される。読者は、これらの公開鍵ペアの名前が、公開鍵ペアを区別することのみを意図していることを認識であろう。

【００７５】

本願において説明する公開鍵ペアは、例えば、ＲＳＡ又は楕円曲線に基づく暗号システムのような、任意の適切な公開鍵暗号システムに関連して使用されてもよい。本願において説明する公開鍵ペアの多くは、ディジタル署名用である。ディジタル署名は、ディジタルメッセージ又は文書の真正性を検証するための数学的方式である。例えば本願の例では、ＲＳＡ、ＥｌＧａｍａｌ署名方式、又はＥＣＤＳＡのような、任意の適切なディジタル署名方式が使用されてもよい。

【００７６】

本願において説明するサーバ／サーバシステム／計算装置のうちのいくつかには、「認証局サーバシステム」又は「鍵管理サーバ」のような名前が与えられている。読者は、そのような名前が異なる計算装置を区別することのみを意図していることを認識するであろう。

【００７７】

図１は、電子装置１００の安全な生成、提供、及び配備に関与しうる商業上の（又は他の）当事者を示す図を示す。当業者は、他のセットアップが企図され、この図が例示目的のためにのみ提供されることを認識するであろう。上位概念では、セキュリティモジュールが製造され、次いで、電子装置１００へのインストールのために、ＯＥＭ（original equipment manufacturer）１６０に（典型的にはマイクロコントローラの一部として、ただし必ずしもそうでなくてもよい）提供される。次いで、ＯＥＭ１６０は、プログラミング会社１８０の支援を受けて、電子装置１００にファームウェアをインストールし、最終的に、電子装置に１００を配備のために準備するステップを実行してもよい。いったん配備されると、電子装置１００は、ＩｏＴハブ１７０を介して提供されるサービスと通信してもよい。

【００７８】

図を参照すると、認証局１４０は、電子装置１００にインストールされるセキュリティモジュール１１０を製造する製造能力１５０を有してもよい（又は、信頼された製造業者と密接に協働してもよい）。セキュリティモジュール及び電子装置の実施例をさらに後述する。

【００７９】

本願の説明のために、セキュリティモジュール１１０は、図１には図示しない、公開鍵ペアを確立するように動作可能である物理的複製困難関数（ＰＵＦ）を含む。公開鍵ペアは、他の当事者と共有されてもよい公開鍵と、共有されない対応する秘密鍵とを含む。公開鍵ペアは、非対称鍵ペアとしても知られているかもしれない。公開鍵及び秘密鍵は、ＰＵＦに対するチャレンジ及びレスポンスに基づいてもよい。従って、セキュリティモジュール１１０は、製造業者１５０及び任意の後段の当事者のいずれかによって、いかなる秘密鍵がそこに投入されることを必要することなく、公開鍵ペアを確立することができる。

【００８０】

本願の説明のために、セキュリティモジュール１１０は、対応する少なくとも２つのチャレンジ・レスポンスペアに基づいて、少なくとも２つの鍵ペアを確立するように構成される。優位点として、ＰＵにＦ基づく公開鍵ペアを用いると、秘密鍵は、電子装置上に格納されることを必要としないが、セキュリティモジュールによって提供される安全な周囲／信頼ゾーン内のＰＵＦから動的に再生成可能である。従って、電子装置がハックされて

も、そこに格納されて盗まれる秘密鍵は存在しない。

【００８１】

ファームウェア公開鍵（ＦＰＫ）及び対応するファームウェア秘密鍵（ＦＳＫ）は、第１のＣＲＰに基づき、後述するように、電子装置にファームウェアを安全に提供するために使用される。ファームウェア鍵ペアは、サードパーティープログラミング会社１８０のセキュリティが何らかの方法で損なわれている場合であっても、ＯＥＭ１６０が電子装置１００のファームウェアを準備することを可能にするために使用される。

【００８２】

登録公開鍵（ＥＰＫ）及び対応する登録秘密鍵（ＥＳＫ）は、第２のＣＲＰに基づく。ＥＰＫは、電子装置の識別子を提供するために使用される。装置識別子はＥＰＫの関数に基づく。本願において説明する実施例の多くでは、関数は暗号ハッシュ関数であるが、そうでなくてもよく、他の関数が使用されてもよい。ＳＨＡ－１又はＭＤ５のような暗号ハッシュ関数が、暗号学では広く使用される。ハッシュ関数によって擬似乱数のビット列が生成される。ハッシュ関数Ｈは、任意長のビット列ｍを入力として取得し、固定長のビット列ｎを出力する一方向関数である。ハッシュ関数についての１つの基礎的な要件は、ハッシュ値Ｈ（ｍ）を簡単に計算できることであり、これにより、ハードウェア及びソフトウェア実装の両方を実用的にする。ハッシュ関数Ｈは、衝突耐性を有する場合、すなわち、Ｈ（ｍ）＝Ｈ（ｍ’）を満たす２つの異なるビット列ｍ及びｍ’を発見することが計算上不可能である場合、暗号ハッシュ関数である。暗号ハッシュ関数の例は、ＭＤ５、ＳＨＡ－１、ＳＨＡ－２、ＳＨＡ－３、ＲＩＰＥＭＤ－１６０、ＢＬＡＫＥ２、及びＢＬＡＫＥ３を含む。

【００８３】

ＰＵＦを用いて装置にファームウェアを安全に提供して電子装置の識別子を提供することによって、電子装置は、公開鍵インフラストラクチャを構築することと、ＩｏＴサービスに安全に接続することとの要件のすべてを有する。そのような登録処理は、同時係属中の特許文献２及び３に説明される。これらの関連出願の各々の内容全体は、すべての目的で、本願に援用される。

【００８４】

本開示の目的で、電子装置１００は、マイクロコントローラ（ＭＣＵ）のような低レベルの回路からなると理解されてもよい。電子装置１００は、代替として、より高レベルの回路、例えば、湿度又は温度を検出するための回路を備えると理解されてもよく、又は、スマートフォン又はコンピュータのような、より大規模な電子装置であると理解されてもよい。製造業者１５０は、単にセキュリティモジュール１１０を製造してもよく、又は、セキュリティモジュール１１０がインストールされたマイクロコントローラを製造してもよい。

【００８５】

詳細後述するように、認証局１４０は、公開鍵ペアに関連付けられてもよい。すなわち、認証局１４０は、公開鍵（以下、公開認証局鍵、ＰＡＫと呼ぶ）及び対応する秘密鍵（以下、秘密認証局鍵、ＳＡＫと呼ぶ）に関連付けられてもよい。ＳＡＫは他のいかなる当事者とも共有されず、一方、ＰＡＫはより広く共有されてもよい。例えば、ＰＡＫは、セキュリティモジュール１１０に、例えば安全なメモリに書き込まれていてもよい。代替として、製造業者１５０が、セキュリティモジュールを備えるマイクロコントローラ（又は他の電子装置）を製造する場合、ＰＡＫは、セキュリティモジュールの外部における、電子装置の他の読み出し専用メモリ（ＲＯＭ）にインストールされてもよい。セキュリティの目的で、セキュリティモジュール／電子装置に格納されたＰＡＫは、その完全性を保つために、書きかえ又は変更不可能であることが重要である。受信された情報がＳＡＫを用いて署名され、したがって、認証局１４０によって承認されていることを検証するために、ＰＡＫは、後の段階において、セキュリティモジュール１１０によって使用されてもよい。また、他の非秘密情報、例えば、ＳＡＫを用いて認証局１４０によって署名され、ＰＡＫが認証局１４０に関連付けられていることを示すルート証明書が、セキュリティモジ

ュール／電子装置に書き込まれていてもよい。秘密情報が認証局１４０によってセキュリティモジュール１１０に提供されることはない。秘密情報が認証局１４０又は製造業者１５０によってセキュリティモジュール１１０から抽出されることはない。

【００８６】

また、セキュリティモジュール１１０から装置識別子及び１つ又は複数の公開鍵が抽出されることを可能にするために、初期登録ファームウェア（initial enrolment firmware：ＩＥＦ）がセキュリティモジュール／電子装置に提供される。

【００８７】

認証局１４０は、１つ又は複数のサーバを備えるサーバシステム１３０を所有し、及び／又は、動作させてもよい。図１の認証局サーバシステム１３０は、３つのサーバにより示されているが、当業者は、サーバシステム１３０がより多数又はより少数のサーバを備えてもよいことを認識するであろう。

【００８８】

認証局システムのサーバのうちの少なくとも１つは、ＳＡＫを用いて証明書に署名するように構成される（このことについてのより多くの情報をさらに下記に提供する）。ＳＡＫは、ファームウェアに署名するためにも使用されてもよい。

【００８９】

認証局サーバシステム１３０のサーバのうちの少なくとも１つは、装置識別子のような、セキュリティモジュール１１０についての情報を有するデータベースを保持するように構成される。

【００９０】

認証局サーバシステム１３０のサーバのうちの少なくとも１つは、ＯＥＭ（original equipment manufacturer）１６０によって動作される計算装置１２０と安全に通信するように構成される。

【００９１】

サーバのうちの少なくとも１つは、ＩｏＴハブ１７０と通信するように構成される。ＩｏＴハブは、クラウドにおいてホスティングされた、管理されたサービスであり、それは、ＩｏＴアプリケーションと、それが管理する電子装置との間における双方向通信のためのメッセージハブとして動作する。本願の説明のために、本願において説明する方法は、ＩｏＴハブ１７０と通信する準備ができた状態で配備されうるように、電子装置を提供することに適している。

【００９２】

明確性のみを目的として、サーバシステム１３０のサーバを、本願では、時々、「認証局サーバ」と呼ぶ。

【００９３】

当業者は、サーバシステム１３０の機能の少なくとも一部がクラウドサービスとして提供されてもよいことを認識するであろう。サーバのうちの１つ又は複数は、物理的に、認証局１４０の外部に設けられてもよい。サーバシステム１３０の認証局サーバは、特定のセキュリティモジュール１１０を識別するための装置識別子であって、登録秘密鍵（ＥＳＫ）及び登録公開鍵（ＥＰＫ）を含む登録鍵ペアのＥＰＫの関数に基づく装置識別子を受信してもよい。サーバシステム１３０は、装置識別子をデータベースに格納するように構成される。いくつかの実施例では、サーバシステム１３０は、特定のセキュリティモジュール１１０のＥＰＫを受信してもよいが、このことは必須ではない。

【００９４】

サーバシステム１３０はまた、いくつかの実施形態によれば、ファームウェア秘密鍵（ＦＳＫ）及びファームウェア公開鍵（ＦＰＫ）を含むファームウェア鍵ペアのＦＰＫを受信してもよい。サーバシステム１３０は、装置識別子及び対応するＦＰＫをデータベースに格納してもよい。

【００９５】

いったんサーバシステム１３０がセキュリティモジュール１１０の装置識別子を受信及

び格納すると、セキュリティモジュール１１０（おそらくは既にマイクロコントローラにインストールされている）はＯＥＭ１６０に提供される。ＯＥＭは、典型的には、ＯＥＭ１６０によって製造されているいくつかの電子装置１００にインストールするために、そのようなセキュリティモジュールをまとめて購入してもよい。

【００９６】

ＯＥＭ１６０はまた、認証局１４０のサーバシステム１３０と安全に通信できる計算装置１２０にアクセスする。参照の都合上、ＯＥＭによって動作される計算装置１２０を、下記では「鍵管理サーバ」と呼ぶ。用語「鍵管理サーバ」を単数形で使用しているが、当業者は、計算装置１２０の機能が複数の計算装置にわたって共有されてもよいことを認識するであろう。したがって、「鍵管理サーバ」はまた、所望の機能を有する複数の計算装置（１つ又は複数のサーバ／計算装置を備える鍵管理サーバシステム）を参照すると理解されているべきである。

【００９７】

下記ではＫＭＳ１２０と呼ばれる鍵管理サーバ１２０は、いくつかの状況では、ＯＥＭ１６０が直接的に相互動作できるサーバであるが、認証局サーバシステム１３０の他の認証局サーバとみなされてもよい。特に、ＫＭＳ１２０は、認証局サーバシステム１３０との安全に通信することができ、従って、認証局１４０によるＯＥＭの使用のために証明されてもよい。

【００９８】

鍵管理サーバ１２０は、オンプレミス動作のためにＯＥＭ１６０に提供された物理サーバを備えてもよい。例えば、ＯＥＭ１６０は、認証局１４０から物理的ＫＭＳ１２０を取得するように構成されてもよい。認証局１４０は、ＯＥＭ１６０に提供される特定のＫＭＳインスタンス１２０を識別するためのＫＭＳ識別子を生成及び記録してもよい。認証局１４０は、ＫＭＳ１２０の内部のハードウェアセキュリティモジュール（hardware security module：ＨＳＭ）においてＫＭＳ公開鍵ペアを生成し、ＫＭＳ公開鍵ペアのＫＭＳ公開鍵を抽出し、ＳＡＫを用いて証明書に署名することでＫＭＳ公開鍵及びＫＭＳソフトウェアにおける証明書に対してＫＭＳ識別子を関連付けてもよい。認証局１４０はまた、ＰＡＫを認証局１４０に関連付けるルート証明書と、ＫＭＳが認証局サーバシステム１３０の認証局サーバに接続することを可能にするＵＲＬとを、ＫＭＳ１２０に組み込んでもよい。次いで、ＫＭＳ１２０は、ＯＥＭ１６０に物理的に転送されてもよい。続いて、ＫＭＳ１２０は、サーバシステム１３０との安全な通信（例えばＴＬＳ通信）を開始してもよい。サーバシステム１３０は、ＳＡＫによって署名されたＴＬＳ証明書及びチェーンを提示し、ＴＬＳサーバ認証を実行することによって認証してもよい。次いで、ＫＭＳ１２０は、ＰＡＫを認証局１４０に関連付ける、ハードコーディングされたルート証明書を用いて、証明書を検証してもよい。ＫＭＳ１２０は、その証明書（認証局１４０によってＳＡＫを用いて署名されている）を提示し、ＴＬＳクライアント認証を実行することで、認証局サーバに対して認証してもよい。認証局１４０は、ＫＭＳにインストールされた証明書を署名することに使用されたＳＡＫに対応するルート公開鍵（ＰＡＫ）を用いて、証明書上の署名を検証してもよい。当業者は、ＫＭＳ１２０を証明することに使用される公開認証局鍵が、セキュリティモジュール１１０へインストールされた公開認証局鍵と同じであっても、異なっていてもよいことを認識するであろう。

【００９９】

オンプレミス動作のためにＯＥＭ１６０に提供される専用の物理サーバとは対照的に、鍵管理サーバ１２０は、ＯＥＭ１６０によって動作される計算装置１２０であって、認証局１４０のサーバシステム１３０と通信するために提供される安全なゲートウェイのための専用のソフトウェアを有する計算装置１２０を備えてもよい。専用のソフトウェアは、配備しやすいか否かについては何ともいえないが、ＯＥＭ１６０によって容易にインストール及び動作されうる。専用のソフトウェアは、サーバシステム１３０に対して認証する際に使用可能であるメカニズム（公開鍵）を含む。

【０１００】

ＯＥＭ１６０は、ＫＭＳ１２０を用い、１つ又は複数の受けとったセキュリティモジュールを登録してもよい。具体的には、ＫＭＳ１２０は、電子装置のセキュリティモジュール１１０と通信することで、ＥＰＫの関数を含む装置識別子を抽出してもよい。ＫＭＳ１２０は、認証局サーバシステム１３０に対する安全な通信チャネルを開き、ＫＭＳインスタンス１２０及び装置識別子の間の関連付けを、信頼された認証局１４０に対して登録してもよい。認証局１４０は、ローカルデータベースを更新し、装置識別子の登録に成功したことをＫＭＳ１２０に通知してもよく、また、その装置識別子に関連付けられた電子装置と通信する所定の許可をＫＭＳ１２０に与えてもよい。

【０１０１】

ＯＥＭ１６０は、ＫＭＳ１２０を用いて、本願において説明する方法に従って電子装置にファームウェアを安全に提供してもよい。ファームウェアは、電子装置のハードウェアを制御するための低レベルの命令を含んでもよい。ファームウェアは、同時係属中の特許文献２及び３に説明されるような方法により装置を登録するための１つ又は複数のルート証明書を含んでもよい。ファームウェアは、電子装置の装置識別子が登録されるＫＭＳ１２０の識別子を含んでもよい。例えば、識別子は、電子装置がＫＭＳ１２０と通信して接触する際に使用されるＵＲＬ（Uniform Resource Locator ）を含んでもよい。ファームウェアは、ＵＲＬによって識別される計算装置／サーバとのＴＬＳ接続のような、安全な接続を開始するための命令を含んでもよい。ファームウェアは、電子装置が受信された証明書を解釈できるように、証明書命名構造の詳細事項を含んでもよい。ファームウェアは、証明書署名要求（certificate signing request：ＣＳＲ）を確立するための詳細事項をさらに含んでもよい。証明書署名要求は、通常、証明書が発行されるべき対象である公開鍵と、識別情報（装置識別子など）と、完全性保護（例えばディジタル署名）とを含む。

【０１０２】

鍵管理サーバ１２０はまた、さらにもう１つの電子装置１００と通信することができる。このように、１つ又は複数の電子装置１００がＯＥＭ１６０に登録されてもよい。本願において説明するように、ＫＭＳ１２０は、電子装置１００へのファームウェアの安全なインストールを容易にするために使用されてもよい。ＫＭＳ１２０は、特定の電子装置１００に対して装置識別子を関連付けるために使用されてもよい。ＫＭＳ１２０は、証明書に署名するために使用されてもよい。いったん電子装置にファームウェアがインストールされると、装置をＯＥＭに登録し、最終的に、ＩｏＴハブ用の安全な使用のために装置を配備するように準備するために、信頼のチェーンを構築することができる。

【０１０３】

ＫＭＳ１２０はまた、ＩｏＴハブ１７０に接続するために必要な情報を電子装置に安全に提供するために使用されてもよい。例えば、ＫＭＳ１２０は、ＩｏＴハブと直接的に又はサーバシステム１３０を介して通信することで、各登録された電子装置１００の装置証明書をＩｏＴハブに提供するように構成されてもよい。ＫＭＳ１２０は、ＩｏＴルート証明書及びＩｏＴエンドポイントを１つ又は複数の電子装置１００に提供することで、装置がＩｏＴハブ１７０と通信することを可能にするように構成されてもよい。

【０１０４】

電子装置１００には、ＩｏＴハブ１７０と通信するためにそれらが必要とする情報のすべてが配備されてもよい。

【０１０５】

図２は、図１に存在するハードウェア装置の多くを含む通信システムを、より概略的に示す。図２は、特に、通信ネットワーク２００と、セキュリティモジュール１１０を有する例示的な電子装置１００と、例えばＯＥＭ１６０によって動作されうる鍵管理サーバ１２０と、認証局サーバシステム１３０と、例えばＩｏＴハブ１７０によって動作されうる計算装置２２０とを示す。通信ネットワーク２００は、インターネットのような、任意の適切な通信ネットワークであってもよい。いくつかの実施例では、ネットワーク２００はワイドエリアネットワーク（ＷＡＮ）を含んでもよい。

【０１０６】
電子装置１００は、本願において説明する方法を実行するための、任意の適切な形式を有してもよく、任意の適切な計算装置を備えてもよい。例えば、電子装置は、パーソナルコンピュータ、サーバ、ラップトップコンピュータ、又は他のそのようなマシンのような、処理及び格納可能である任意の計算装置であってもよい。電子装置１００はＩｏＴ装置を備えてもよい。電子装置は、より大きな装置にインストールされるマイクロコントローラ装置（ＭＣＵ）を備えてもよい。電子装置１００は、他の装置と直接的に又はネットワーク２００を介して通信してもよい。例えば、電子装置１００は、物理接続及びネットワーク２００のいずれかを介してＫＭＳ１２０と通信してもよい。いったん電子装置１００が配備されると、装置１００は、ネットワーク２００を介して計算装置２２０と通信してもよい。電子装置は、ＫＭＳ１２０と通信してもよく、及び／又は、安全な接続、例えばＴＬＳ接続を介して計算装置２２０と通信してもよい。
【０１０７】
ＫＭＳ１２０は、詳細後述する計算装置５００のような、任意の適切な計算装置を備えてもよい。ＫＭＳ１２０は、サーバのクラスタ又は単一の装置を備えてもよい。ＫＭＳ１２０の機能は、分散データ処理環境、単一のデータ処理装置、などを含む、多数の異なるタイプのデータ処理環境において利用されてもよい。
【０１０８】
ＫＭＳ１２０は、ネットワーク２００を介して認証局サーバシステム１３０との安全な接続を確立することができ、また、ネットワーク２００を介して、又はいくつかの状況では、有線接続のような直接接続を介して、電子装置１００と通信することができる。ＫＭＳ１２０は、電子装置１００のセキュリティモジュール１１０を識別する装置識別子のような、電子装置１００に関する情報と、電子装置１００のＥＰＫのような、１つ又は複数の公開鍵とを格納するように構成される。追加的又は代替的に、ＫＭＳ１２０は、認証局サーバシステム１３０のデータベース２１０と通信することで、そのような情報を取得するように構成されてもよい。ＫＭＳ１２０は、証明書に署名するようにさらに構成される。
【０１０９】
認証局サーバシステム１３０は、１つ又は複数のサーバを備え、データベース２１０を含む。認証局サーバシステム１３０の１つ又は複数の認証局サーバは、認証局１４０に代わって証明書に署名し、例えば、ＫＭＳ１２０が認証局１４０によって信頼されることを証明するか、又は、電子装置１００にインストールされるファームウェアに署名するように構成される。データベース２１０は、電子装置１００を識別する装置識別子のような、電子装置１００に関する情報を格納し、いくつかの実施例では、電子装置１００のファームウェア公開鍵ＦＰＫを格納するように構成される。データベース２１０は、ＫＭＳ１２０に関する情報を格納するようにさらに構成されてもよい。例えば、データベース２１０は、一群の装置識別子を特定のＫＭＳ１２０に関連付ける情報を含んでもよく、ＫＭＳ１２０が、関連付けられた装置識別子のみと相互動作することを認可するように使用されてもよい。
【０１１０】
計算装置２２０は、（例えば、分散計算環境における）多数の接続された装置を備えてもよく、又は、単一の計算装置を備えてもよい。
【０１１１】
図３Ａは、実施例に係る電子装置１００のブロック図を示す。例えば、電子装置１００はＩｏＴ装置であってもよい。当業者によって認識されるように、図３Ａに示すものとは別のアーキテクチャが使用されてもよい。
【０１１２】
図を参照すると、電子装置１００は、セキュリティモジュール１１０、１つ又は複数のＣＰＵ／プロセッサ３０２、１つ又は複数のメモリ３０４、センサモジュール３０６、通信モジュール３０８、ポート３１０、及び電源３１２を含む。構成要素３０２、３０４、

３０６、３０８、３１０、３１２のそれぞれは、様々なバスを用いて相互接続される。ＣＰＵ３０２は、電子装置１００内において実行するように命令を処理してもよい。命令は、メモリ３０４に格納された命令、通信モジュール３０８又はポート３１０を介して受信された命令を含む。

【０１１３】

メモリ３０４は、電子装置１００内におけるデータの格納用である。１つ又は複数のメモリ３０４は、１つ又は複数の揮発性メモリ装置を含んでもよい。１つ又は複数のメモリは、１つ又は複数の不揮発性メモリ装置を含んでもよい。１つ又は複数のメモリ３０４は、磁気又は光ディスクのような、他の形式のコンピュータ可読媒体であってもよい。１つ又は複数のメモリ３０４は、電子装置１００のための大規模記憶装置を提供してもよい。本願において説明する方法を実行するための命令が、１つ又は複数のメモリ３０４内に格納されてもよい。

【０１１４】

通信モジュール３０８は、プロセッサ３０２及び他のシステムの間において通信を送信及び受信することに適している。例えば、通信モジュール３０８は、インターネットのような通信ネットワーク２００を介して通信を送信及び受信するために使用されてもよい。通信モジュール３０８は、ＷｉＦｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＮＦＣなどのような多数のプロトコルのうちのいずれかによって、電子装置１００が他の装置／サーバと通信することを可能にしてもよい。

【０１１５】

ポート３１０は、例えば、プロセッサ３０２によって処理される命令を含んでいる非一時的なコンピュータ可読媒体を受けることに適している。ポート３１０は、例えば、電子装置１００及び鍵管理サーバ１２０の間における有線通信に使用されてもよい。

【０１１６】

センサモジュール３０６は、温度、湿度、又は他の任意のパラメータのような、検出パラメータのための１つ又は複数のセンサを備えてもよい。

【０１１７】

プロセッサ３０２は、例えば、センサモジュール３０６、セキュリティモジュール１１０、又は通信モジュール３０８から、データを受信するように構成される。プロセッサ３０２は、メモリ３０４にアクセスし、上記メモリ３０４と、通信モジュール３０８と、ポート３１０に接続されたコンピュータ可読記憶媒体とのいずれかから受信された命令及び／又は情報に対して動作するようにさらに構成される。

【０１１８】

図３Ｂは、他の例示的な電子装置１００のアーキテクチャ、すなわちマイクロコントローラ装置（ＭＣＵ）３１５を示し、それは、より大きな電子装置内にインストールされてもよい。当業者は、他のＭＣＵアーキテクチャが使用されてもよいことを認識するであろう。

【０１１９】

図３ＢのＭＣＵ３１５は、ＣＰＵ３２０、ユーザメモリ３２２、及びブートランダムアクセスメモリ３２８を備える。ＣＰＵ３２０、ブートＲＯＭ３２８、及びユーザメモリ３２２は、コードバス３２４を介して通信してもよい。ＣＰＵ３２０、ブートＲＯＭ３２８、及びユーザメモリ３２２は、システムバス３２６に接続されてもよく、それは、複数の周辺装置Ａ、Ｂ、及びＣ（３３０、３３２、及び３３４）及びセキュリティモジュール１１０に接続されてもよい。セキュリティに関連する構成要素のみをＭＣＵ３１５に示す。当業者は、ＭＣＵ３１５がより多数又はより少数の構成要素を有してもよいことを認識するであろう。例えば、ＭＣＵ３１５は、より多数の周辺装置及びシステム構成要素を有してもよい。

【０１２０】

図４Ａは、実施例に係るセキュリティモジュール１１０のブロック図を示す。セキュリティモジュール１１０は、電子装置１００の他の構成要素から安全な構成要素を分離する

信頼ゾーンとみなされてもよい。セキュリティモジュール１１０は、ＰＵＦモジュール４０２、暗号アクセラレータ４０４、及びセキュアメモリ４０６を備える。当業者は、他のアーキテクチャもまた可能であることを認識するであろう。セキュリティモジュール１１０は、電子装置１００のシステムバスに接続される。

【０１２１】

ＰＵＦモジュール４１０は、ＰＵＦと、ＰＵＦに対して相互動作することに必要な任意の回路とを備える。特に、ＰＵＦモジュールは、暗号アクセラレータ４０４から信号を受信し、適切なレスポンスを提供してもよい。暗号アクセラレータ４０４は、暗号演算を実行するために、また、ＰＵＦモジュール４０２及びセキュアメモリ４０６に対する相互動作のために、専用処理装置を備える。

【０１２２】

セキュアメモリは、ＰＵＦモジュール４０２によって生成された鍵、及び／又は、ルート証明書のような、秘密情報を格納するように構成される。ＰＵＦモジュール４０２と、セキュリティモジュール１１０内のセキュリティ周辺装置と、セキュアメモリとを制御するためにＣＰＵ３２０によって必要とされる命令は、ブートＲＯＭ３２８内に含まれ、それはシステムの変更不可のブート処理の一部である。

【０１２３】

図４Ｂは、実施例に係るＰＵＦモジュール４０２の機能的構成要素を示す。ＰＵＦモジュール４０２は、ＰＵＦ４５０、アナログフロントエンド（ＡＦＥ）４５２、後処理エンジン４５４、及びＲＩＳＣ－Ｖコア４５６を備える。

【０１２４】

当業者は、ＰＵＦ４５０が任意の適切なＰＵＦであってもよいことを認識するであろう。

【０１２５】

アナログフロントエンド（ＡＦＥ）４５２は、ＰＵＦとの相互動作のためにアナログ信号調節回路を備える。例えば、ＡＦＥは、ＰＵＦ４５０と相互動作することで、未処理の「指紋」を確立してもよい。後処理エンジン４５４は、ＡＦＥ４５２の出力を補正し、ＡＦＥの出力をさらに処理することでさらなるプライバシー向上を提供するように構成される。ＲＩＳＣ－Ｖコア４５６は、ＰＵＦ４５０からのデータの後処理、例えばデータの誤り訂正を実行するＣＰＵコアである。他のＣＰＵコアが利用されてもよいが、ＲＩＳＣ－Ｖコアは、外部マイクロコントローラに対するＰＵＦモジュール４０２の容易な接続を可能にするインターフェースを提供する。

【０１２６】

図５は、計算装置５００のブロック図である。例えば、計算装置５００は、計算装置、サーバ、モバイル又はポータブルコンピュータ又は電話機、などを備えてもよい。計算装置５００は、複数の接続された装置にわたって分散されてもよい。計算装置５００は、鍵管理サーバ１２０、認証局サーバシステム１３０の認証局サーバ、又は例えばＩｏＴハブ用のサーバ２２０としての使用に適していてもよい。

当業者によって認識されるように、図５に示すものとは別のアーキテクチャが使用されてもよい。

【０１２７】

図を参照すると、計算装置５００は、１つ又は複数のプロセッサ５１０と、１つ又は複数のメモリ５２０と、視覚ディスプレイ５３０及び仮想又は物理キーボード５４０のような多数のオプションのユーザインターフェースと、通信モジュール５５０と、オプションのポート５６０と、オプションの電源５７０とを含む。構成要素５１０、５２０、５３０、５４０、５５０、５６０、及び５７０のそれぞれは、様々なバスを用いて相互接続される。プロセッサ５１０は、計算装置５００内において実行するように命令を処理してもよい。命令は、メモリ５２０に格納された命令、通信モジュール５５０又はポート５６０を介して受信された命令を含む。

【０１２８】

メモリ５２０は、計算装置５００内におけるデータの格納用である。１つ又は複数のメモリ５２０は、１つ又は複数の揮発性メモリ装置を含んでもよい。１つ又は複数のメモリは、１つ又は複数の不揮発性メモリ装置を含んでもよい。１つ又は複数のメモリ５２０は、磁気又は光ディスクのような、他の形式のコンピュータ可読媒体であってもよい。１つ又は複数のメモリ５２０は、計算装置５００のための大規模記憶装置を提供してもよい。本願において説明する方法を実行するための命令が、１つ又は複数のメモリ５２０内に格納されてもよい。

【０１２９】

装置５００は、視覚ディスプレイ５３０のような視覚化手段と、キーボード５４０のような仮想又は専用だったユーザ入力装置とを含む、多数のユーザインターフェースを含む。

【０１３０】

通信モジュール５５０は、プロセッサ５１０及び遠隔のシステムの間において通信を送信及び受信することに適している。例えば、通信モジュール５５０は、インターネットのような通信ネットワーク２００を介して通信を送信及び受信するために使用されてもよい。

【０１３１】

ポート５６０は、例えば、プロセッサ５１０によって処理される命令を含んでいる非一時的なコンピュータ可読媒体を受けることに適している。

【０１３２】

プロセッサ５１０は、データを受信し、メモリ５２０にアクセスし、上記メモリ５２０又はポート５６０に接続されたコンピュータ可読記憶媒体から、通信モジュール５５０から、又はユーザ入力装置５４０から受信された命令に対して動作するように構成される。

【０１３３】

計算装置５００は、暗号鍵を安全に格納するための、図５には図示しないハードウェアセキュリティモジュール（ＨＳＭ）をさらに備えてもよい。例えば、鍵管理サーバ１２０として使用される計算装置５００の場合、ＨＳＭは、証明書に署名するために１つ又は複数の秘密鍵を格納するか、又は、ファームウェアを暗号化／復号するためにサーバ暗号鍵及びサーバ復号鍵を格納するように要求されてもよい。例えば、認証局サーバシステム１３０の認証局サーバとして使用される計算装置５００の場合、ＨＳＭは、認証局鍵ペアの秘密認証局鍵（ＳＡＫ）のような、１つ又は複数の秘密鍵を格納するように要求されてもよい。当業者は、ＨＳＭが秘密鍵を格納するように要求されず、他のセキュリティ構成が適用可能されてもよいことを認識するであろう。例えば、計算装置は、クラウドに基づくＨＳＭにアクセスしてもよい。

【０１３４】

図６Ａは、実施例に係る電子装置１００にファームウェアを安全に提供する方法を示す。この実施例では、図１を参照して、ＯＥＭ１６０は、電子装置１００にファームウェアをインストールしようとし、この目的のために、サードパーティーのプログラミング会社１８０を使用する。ＯＥＭ１６０は、認証局サーバシステム１３０と安全に通信できる鍵管理サーバ１２０にアクセスする。

【０１３５】

認証局１４０／製造業者１５０は、セキュリティモジュール１１０を製造する（オプションで、それをＭＣＵ３１５内にインストールする）ように構成される。

【０１３６】

セキュリティモジュール１１０はＰＵＦ４５０を備える。セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘密鍵（ＦＳＫ）を含むファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を生成するように構成される。セキュリティモジュール１１０は、ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて、登録公開鍵（ＥＰＫ）及び登録秘密鍵（ＥＳＫ）を含む登録鍵ペア（ＥＰＫ，ＥＳＫ）を生成するようにさらに構成されてもよ

い。秘密鍵ＦＳＫ及びＥＳＫは、セキュリティモジュール１１０から離れない。実際に、これらの秘密鍵はＰＵＦ４５０からの応答に基づくので、それらは、メモリに格納される必要がなく、適切な入力とともにＰＵＦ４５０から動的に再生成可能である。

【０１３７】

セキュリティモジュール１１０は、セキュリティモジュール１１０が最終的にインストールされる電子装置１００を識別するために使用される装置識別子（図６Ａの「ＤｅｖｉｃｅＩＤ」）を生成するように構成される。装置識別子は、登録公開鍵ＥＰＫの関数に基づいて、好ましくは非線形関数に基づいて決定される。装置識別子がＥＰＫの関数に基づくことにより、セキュリティモジュール１１０の身元情報は、セキュリティモジュール１１０の物理的性質に基づき、従って、偽ることはできない。

【０１３８】

実施例によれば、装置識別子は、ＥＰＫに暗号ハッシュ関数を適用することで決定されてもよい。

【０１３９】

図６Ａの実施例によれば、装置識別子は、登録公開鍵に暗号ハッシュ関数を適用することで生成される。

【０１４０】

図６Ａを参照すうと、ステップ６０２において、公開認証局鍵ＰＡＫが、製造中に、セキュリティモジュールに提供される。例えば、ＰＡＫは、セキュリティモジュール１１０のセキュアメモリ４０６に格納されてもよい。実施例では、セキュアメモリ４０６は、読み出し専用メモリ（ＲＯＭ）であってもよい。ＲＯＭは、いかなる方法でも書きかえ又は変更が不可能であり、従って、ＰＡＫをＲＯＭに格納することは、それが改竄不可能であることを保証する。公開認証局鍵ＰＡＫは、秘密認証局鍵ＳＡＫ及びＰＡＫを含む認証局鍵ペアの公開鍵である。秘密認証局鍵ＳＡＫは認証局１４０（又は認証局サーバシステム１３０のサーバ）にのみ知られている一方、ＰＡＫは広く共有されてもよい。当業者は、図６Ａにおいて、ＰＡＫがサーバシステム１３０によってセキュリティモジュール１１０に提供されているが、ＰＡＫは他の何らかのエンティティによってセキュリティモジュールに提供されてもよいこと、例えば、ＰＡＫは信頼された製造業者１５０によってセキュリティモジュールに組み込まれてもよいことを認識するであろう。セキュリティモジュール１１０には、装置識別子及び１つ又は複数の公開鍵の抽出を可能にすることと、ローカルに格納されたエンドポイントとの安全な接続を開始すること（例えばＵＲＬ）とのような、必要なセキュリティ機能を実行するための基本ソフトウェアを含む初期登録ファームウェアが提供されてもよい。また、当業者は、図６Ａのステップ６０２では公開認証局鍵ＰＡＫがセキュリティモジュール１１０に提供されているが、ＰＡＫが、電子装置１００の他の部品に提供され、電子装置１００に安全に組み込まれてもよいことを認識するであろう。

【０１４１】

６０４において、認証局サーバシステム１３０は、セキュリティモジュール１１０の装置識別子及びファームウェア公開鍵ＦＰＫを取得する。装置識別子は、登録公開鍵ＥＰＫのハッシュを含む。サーバシステム１３０は、装置識別子及びＦＰＫを装置から抽出してもよく、又は、それらを例えば製造業者１５０から受信してもよい。

【０１４２】

セキュリティモジュール１１０は、一群のセキュリティモジュールのうちの１つのセキュリティモジュールであってもよい。従って、サーバシステム１３０は、多数の装置識別子及び対応するＦＰＫを取得してもよい。６０６において、サーバシステム１３０は、後の参照のために、装置ＩＤ及び対応するＦＰＫをデータベース２１０に格納する。

【０１４３】

いったん装置識別子及び対応するＦＰＫがサーバシステム１３０によって取得及び格納されると、セキュリティモジュール１１０（又はセキュリティモジュールを含むＭＣＵ３１５）は、電子装置１００へのインストールのためにＯＥＭ１６０に輸送されてもよい。

【０１４４】
図６Ａを参照して説明するシナリオにおいて、ＯＥＭ１６０は、電子装置１００にインストールされるファームウェアを設計する。ファームウェアは、ＯＥＭによって自己署名された１つ又は複数のルート証明書をさらに含むことで、電子装置の登録中に信頼のチェーンを構築することを可能にしてもよい。ファームウェアは、電子装置１００のハードウェアを制御するための低レベルの命令を含んでもよい。ファームウェアは鍵管理サーバ１２０に提供され、鍵管理サーバ１２０は、ステップ６０８において、ファームウェアを暗号化するためのサーバ暗号鍵Ｋを生成する。サーバ暗号鍵Ｋは、対称暗号関数の鍵であってもよく、又は、非対称暗号関数の鍵であってもよい。すなわち、サーバ復号鍵（図６Ａの「Ｉｎｖ（Ｋ）」）は、サーバ暗号鍵Ｋと同じであってもよく、又は、異なっていてもよい。６５８において、ＫＭＳ１２０は、ファームウェアに暗号ハッシュ関数を適用する。このことは、サーバ暗号鍵が生成６０８される前、中、又は後に行われてもよい。

【０１４５】
ＫＭＳ１２０は、認証局サーバシステム１３０と安全に通信可能であり、ファームウェアのハッシュがサーバシステム１３０に送信される。ＫＭＳ１２０からサーバシステム１３０にファームウェアのハッシュを送信することによって、ファームウェア自体が送信される必要はなく、サーバシステム１３０自体はファームウェアを変更できない。６６２において、認証局サーバシステム１３０は、秘密認証局鍵ＳＡＫを用いてファームウェアのハッシュに署名する。従って、ファームウェアのハッシュ上の署名とともに公開認証局鍵ＰＡＫを用いる任意のエンティティは、ファームウェアのハッシュがサーバシステム１３０によって署名されていることを検証できるであろう。

【０１４６】
次いで、ファームウェアのハッシュ上の署名は、ＫＭＳ１２０に返送される。６６０において、ＫＭＳ１２０は、サーバ暗号鍵Ｋを用いてファームウェア及び署名を暗号化する。

【０１４７】
ファームウェアを暗号化するために使用されるサーバ暗号鍵は、異なるファームウェアに対して同じであってもよく、又は、異なっていてもよい。例えば、ＯＥＭ１６０は、第１の一群の電子装置のための第１のファームウェアを生成してもよく、第２の一群の電子装置のための第２のファームウェアを生成してもよく、同じサーバ暗号鍵Ｋを用いて第１のファームウェア及び第２のファームウェアの両方を暗号化してもよく、又は、ファームウェア固有の暗号鍵を使用してもよい。さらに、いくつかの実施例では、ＯＥＭが製造する各一群の電子装置１００に対して、互いに異なる複数のサーバ暗号鍵が存在してもよい。

【０１４８】
認証局サーバシステム１３０はまた、装置識別子（「ＤｅｖｉｃｅＩＤ」）及び対応するＦＰＫを鍵管理サーバ１２０に安全に伝送する。複数のセキュリティモジュール１１０の装置識別子及びＦＰＫは、個々に又はまとめて、例えばルックアップテーブルの形式で、ＫＭＳ１２０に伝送されてもよい。

【０１４９】
６１４において、ＫＭＳは、ＦＰＫを用いてサーバ復号鍵Ｉｎｖ（Ｋ）を暗号化する。暗号化されたサーバ復号鍵（図６Ａにおいて符号「Ｅｎｃ（ＦＰＫ，Ｉｎｖ（Ｋ））」により示す）及び対応する装置識別子は、プログラミング会社１８０に伝送される。例えば、複数の装置識別子及び対応する暗号化されたサーバ復号鍵を含むルックアップテーブルが、プログラミング会社１８０に提供されてもよい。サーバ復号鍵は、ファームウェア及び署名されたハッシュの復号用である。

【０１５０】
次いで、暗号化されたファームウェア、暗号化された署名、及び暗号化されたサーバ復号鍵は、電子装置１００へのインストールのためにプログラミング会社１８０に送信される。

【０１５１】
６１６において、所与の電子装置１００に関して、プログラミング会社１８０は、対応する暗号化されたサーバ復号鍵を電子装置１００にインストールする。プログラミング会社はさらに、暗号化されたファームウェアを、インストールのために、電子装置１００に提供する。
【０１５２】
セキュリティモジュール１１０を含む電子装置１００は、ファームウェアを復号及びインストールするために必要な情報のすべてを含む。暗号化されたサーバ復号鍵Ｅｎｃ（ＦＰＫ，Ｉｎｖ（Ｋ））は、ＦＰＫを用いて暗号化されたので、電子装置１００は、ＦＳＫを用いてサーバ復号鍵を復号することができる。ファームウェアのハッシュ上の署名はＳＡＫを用いて署名されたので、電子装置は、ＰＡＫを用いて署名を検証することができる。電子装置はさらに、暗号化されたファームウェアを、サーバ復号鍵Ｉｎｖ（Ｋ）を用いて復号することができる。電子装置１００はさらに、例えば、復号されたファームウェアにハッシュ関数を適用し、認証局サーバシステム１３０によって署名されたそれに対して比較することによって、署名が受信されたファームウェアに対応することをチェックすることができる。検証に基づいて、電子装置１００は、復号されたファームウェアを電子装置１００にインストールしてもよい。
【０１５３】
オプションで、ブート中に、電子装置は、ファームウェアのハッシュを計算し、署名を用いてハッシュをチェックすることで、ファームウェアを検証してもよい。このように、ファームウェアは、電子装置がブートするごとに検証されてもよい。
【０１５４】
従って、図６Ａの方法は、秘密情報が、どの段階においても、暗号化されていない形式で、電子装置１００（又は、電子装置１００にインストールされる前のセキュリティモジュール１１０）に投入されることを必要としないことを保証する。ＯＥＭ１６０は、電子装置１００に提供されるファームウェアが、電子装置１００にインストールされる前に、検出なしに変更できると信じてもよく、このことは、例えばサードパーティープログラミング会社１８０を、完全に信頼する必要性を低減する。認証局サーバシステム１３０は、ファームウェアのハッシュのみを受信するので、ファームウェアを確認しない、又は、ファームウェアを変更する機会をもたない。
【０１５５】
オプションで、プログラミング会社１８０は、電子装置１００から（６１８において）装置識別子を抽出し、これをＫＭＳ１２０に伝送してもよく、ＫＭＳ１２０は、装置識別子を認証局サーバシステムに（６２０において）登録するステップを引き受けてもよい。次いで、認証局サーバシステム１３０は、装置識別子をＫＭＳに関連付けることを、例えば、この情報をデータベース２１０に格納することで行ってもよい。他の実施例では、装置識別子は、サーバシステム１３０からそれらを受信した後で（６０６及び６１４の間の矢印）、ＫＭＳ１２０によって登録されてもよい。装置識別子の登録は、いかなる意味でも、電子装置にファームウェアを提供する方法にリンクされることを必要としない。例えば、ＯＥＭ１６０は、セキュリティモジュール１１０／マイクロコントローラ３１５の製造元である製造業者１５０によって装置識別子のファイルの提供を受けてもよく、登録のために装置識別子をＫＭＳ１２０に手動でアップロードしてもよい。
【０１５６】
装置識別子を認証局サーバシステム１３０に登録することは、ＫＭＳ１２０が主張された装置識別子に関連付けられていることを保証し、さらなるセキュリティチェックとして動作する。認証局サーバシステム１３０は、多数の鍵管理サーバと通信してもよく、したがって、装置識別子をＫＭＳ１２０にリンクすることは、特定のセキュリティモジュール１１０を有する装置を正しいＯＥＭ１６０が供給及び配備していることを保証する。
【０１５７】
装置識別子を登録及び主張する処理は、下記のように動作してもよい。装置識別子につ

いての知識を有するＫＭＳ１２０は、認証局サーバシステム１３０の認証局サーバに対して安全な接続、例えばＴＬＳ接続を確立してもよい。次いで、ＫＭＳ１２０は、ＴＬＳ接続を介して、１つ又は複数の装置識別子を認証局サーバに送信してもよい。サーバシステム１３０は、データベース２１０に格納された情報を用いて、１つ又は複数の装置識別子を検証してもよい。特に、サーバシステム１３０は、装置識別子のすべてが実際の装置に対応すること（すなわち、それらがデータベース２１０において対応するエントリを有すること）と、受信された装置識別子のどれも以前に第２のＫＭＳによって主張されていないこととをチェックしてもよい。チェックに成功した場合、サーバシステム１３０は、装置識別子を主張したＫＭＳ１２０が装置識別子に関連付けられていること、すなわち、ＫＭＳ１２０がそれらの装置識別子を「所有する」ことを示すように、データベース２１０を更新してもよい。いったんこの登録が完了すると、成功を示す情報がＫＭＳ１２０に送信されてもよい。成功を示す情報は、例えば、ＫＭＳ１２０が電子装置との安全なＴＬＳ接続を確立することを可能にしてもよく、及び／又は、ＫＭＳ１２０のユーザインターフェースに装置識別子（又は別のアイコン）を出現させてもよい。次いで、ＫＭＳ１２０及び認証局サーバシステム１３０の間の安全な接続が閉じられてもよい。

【０１５８】

図６Ｂは、実施例に係る電子装置１００にファームウェアを安全に提供するもう１つの方法を示す。この実施例では、図１を参照して、ＯＥＭ１６０は、電子装置１００にファームウェアをインストールしようとし、この目的のために、サードパーティーのプログラミング会社１８０を使用する。ＯＥＭ１６０は、認証局サーバシステム１３０と安全に通信できる鍵管理サーバ１２０にアクセスする。

【０１５９】

セキュリティモジュール１１０は、セキュリティモジュール１１０が最終的にインストールされる電子装置１００を識別するために使用される装置識別子（図６Ｂの「ＤｅｖｉｃｅＩＤ」）を生成するように構成される。装置識別子は、登録公開鍵ＥＰＫの関数に基づいて、好ましくは非線形関数に基づいて決定される。装置識別子がＥＰＫの関数に基づくことにより、セキュリティモジュール１１０の身元情報は、セキュリティモジュール１１０の物理的性質に基づき、従って、偽ることはできない。

【０１６０】

図６Ａの場合のように、ステップ６０２において、公開認証局鍵ＰＡＫが、製造中に、セキュリティモジュール（又はマイクロコントローラの他のセキュアメモリ）に提供される。

【０１６１】

６０４において、サーバシステム１３０は、セキュリティモジュール１１０の装置識別子及びファームウェア公開鍵ＦＰＫを取得する。装置識別子は、登録公開鍵ＥＰＫのハッシュを含む。サーバシステム１３０は、装置識別子及びＦＰＫを装置から抽出してもよく、又は、それらを例えば製造業者１５０から受信してもよい。

【０１６２】

セキュリティモジュール１１０は、一群のセキュリティモジュールのうちの１つのセキュリティモジュールであってもよい。従って、サーバシステム１３０は、多数の装置識別子及び対応するＦＰＫを取得してもよい。６０６において、サーバシステム１３０は、後の参照のために、装置ＩＤ及び対応するＦＰＫをデータベース２１０に格納する。

【０１６３】

いったん装置識別子及び対応するＦＰＫがサーバシステム１３０によって取得及び格納されると、セキュリティモジュール１１０（又はセキュリティモジュールを含むＭＣＵ３１５）は、電子装置１００へのインストールのためにＯＥＭ１６０に輸送されてもよい。

【０１６４】

図６Ａにおいて説明したシナリオのように、図８Ｂのシナリオにおいて、ＯＥＭ１６０は、電子装置１００にインストールされるファームウェアを設計する。ファームウェアは鍵管理サーバ１２０に提供され、鍵管理サーバ１２０は、ステップ６０８において、ファ

ームウェアを暗号化するためのサーバ暗号鍵Ｋを生成する。６１０において、ＫＭＳ１２０は、サーバ暗号鍵Ｋを用いてファームウェアを暗号化する。

【０１６５】

ＫＭＳ１２０はサーバシステム１３０と安全に通信でき、暗号化されたファームウェアはサーバシステム１３０に送信され、サーバシステム１３０は、６１２において、秘密認証局鍵ＳＡＫを用いて、暗号化されたファームウェアに署名する。従って、暗号化及び署名されたファームウェアとともに公開認証局鍵ＰＡＫを用いる任意のエンティティは、暗号化されたファームウェアがサーバシステム１３０によって署名されていることを検証できるであろう。暗号化及び署名されたファームウェアは、オプションでＫＭＳ１２０を介して、プログラミング会社１８０に送信される。

【０１６６】

認証局サーバシステム１３０はまた、装置識別子（「ＤｅｖｉｃｅＩＤ」）及び対応するＦＰＫを鍵管理サーバ１２０に安全に伝送する。複数のセキュリティモジュール１１０の装置識別子及びＦＰＫは、個々に又はまとめて、例えばルックアップテーブルの形式で、ＫＭＳ１２０に伝送されてもよい。

【０１６７】

６１４において、ＫＭＳは、ＦＰＫを用いてサーバ復号鍵Ｉｎｖ（Ｋ）を暗号化する。暗号化されたサーバ復号鍵（図６Ｂにおいて符号「Ｅｎｃ（ＦＰＫ，Ｉｎｖ（Ｋ））」により示す）及び対応する装置識別子は、プログラミング会社１８０に伝送される。例えば、複数の装置識別子及び対応する暗号化されたサーバ復号鍵を含むルックアップテーブルが、プログラミング会社１８０に提供されてもよい。

【０１６８】

６１６において、所与の電子装置１００に関して、プログラミング会社１８０は、対応する暗号化されたサーバ復号鍵を電子装置１００に提供する。プログラミング会社はさらに、暗号化及び署名されたファームウェアを電子装置１００に提供する。

【０１６９】

セキュリティモジュール１１０を含む電子装置１００は、ファームウェアを復号及びインストールするために必要な情報のすべてを含む。暗号化されたサーバ復号鍵Ｅｎｃ（ＦＰＫ，Ｉｎｖ（Ｋ））は、ＦＰＫを用いて暗号化されたので、電子装置１００は、ＦＳＫを用いてサーバ復号鍵を復号することができる。暗号化及び署名されたファームウェアはＳＡＫを用いて署名されたので、電子装置は、ＰＡＫを用いて、暗号化及び署名されたファームウェアを検証することができる。電子装置１００はさらに、暗号化及び署名されたファームウェアを、サーバ復号鍵Ｉｎｖ（Ｋ）を用いて復号することができる。

【０１７０】

オプションで、プログラミング会社１８０は、電子装置１００から（６１８において）装置識別子を抽出し、これをＫＭＳ１２０に伝送してもよく、ＫＭＳ１２０は、装置識別子を認証局サーバシステムに（６２０において）登録するステップを引き受けてもよい次いで、認証局サーバシステム１３０は、装置識別子をＫＭＳに関連付けることを、例えば、この情報をデータベース２１０に格納することで行ってもよい。他の実施例では、装置識別子は、サーバシステム１３０からそれらを受信した後で（６０６及び６１４の間の矢印）、ＫＭＳ１２０によって登録されてもよい。装置識別子の登録は、いかなる意味でも、電子装置にファームウェアを提供する方法にリンクされることを必要としない。例えば、ＯＥＭ１６０は、セキュリティモジュール１１０／マイクロコントローラ３１５の製造元である製造業者１５０によって装置識別子のファイルの提供を受けてもよく、登録のために装置識別子をＫＭＳ１２０に手動でアップロードしてもよい。

【０１７１】

図７Ａは、電子装置１００にファームウェアを提供する概略的な方法７００のフローチャートを示す。電子装置１００は、ＰＵＦ４５０を有するセキュリティモジュール１１０を備えると仮定される。セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア公開鍵（ＦＰＫ）及びファームウェア秘

密鍵（ＦＳＫ）を含むファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成される。公開鍵が電子装置１００に、例えば、電子装置１００のセキュリティモジュール１１０に、安全に組み込まれているとさらに仮定される。公開鍵は、公開鍵及び対応する秘密鍵を含む公開鍵ペアの一部である。署名鍵ペアは、公開認証局鍵と、認証局１４０にのみ知られた秘密認証局鍵とを含む認証局鍵ペアであってもよい。方法７００は、例えば、鍵管理サーバ１２０によって実行されてもよい。

【０１７２】

７１０において、方法７００は、公開鍵及び秘密鍵を含む署名鍵ペアの秘密鍵を用いて、ファームウェアのハッシュに署名させることを含む。公開鍵は電子装置に安全に組み込まれている。

【０１７３】

いくつかの実施形態では、鍵管理サーバ１２０は、署名鍵のペアの秘密鍵を用いてファームウェアのハッシュに署名するように構成されてもよい。しかしながら、（図６Ａに示すような）他の実施形態では、鍵管理サーバ１２０は、認証局サーバシステム１３０の認証局サーバとの安全な接続を確立するように構成されてもよい。次いで、ＫＭＳ１２０は、ファームウェアのハッシュを認証局サーバに伝送し、ファームウェアの署名されたハッシュの署名を受信してもよい。ファームウェアのハッシュは、署名鍵ペアの秘密鍵を用いて署名されている。すなわち、署名鍵ペアは、公開認証局鍵ＰＡＫ及び秘密認証局鍵ＳＡＫを含んでもよく、サーバシステム１３０は、ＳＡＫを用いてファームウェアのハッシュに署名してもよい。

【０１７４】

７２０において、方法７００は、サーバ暗号鍵１００を用いてファームウェア及び署名を暗号化することを含む。サーバ暗号鍵は、ユーザクレデンシャル、例えばユーザのパスワード（例えばＯＥＭのパスワード）に少なくとも部分的に基づいてもよい。

【０１７５】

７２５において、方法７００は、ＦＰＫを用いてサーバ復号鍵を暗号化することを含む。サーバ復号鍵は、暗号化されたファームウェア及び暗号化された署名の復号用である。

【０１７６】

７３０において、方法７００は、暗号化されたファームウェア、暗号化された署名、及び暗号化されたサーバ復号鍵を、電子装置へのインストールのために、サードパーティーに伝送することを含む。サードパーティーは、例えば、プログラミング会社１８０のサーバ、又は、ＫＭＳ及び認証局サーバシステム１３０の外部における他の任意の計算装置を備えてもよい。

【０１７７】

ＦＰＫは、（図６Ａの場合のように）認証局サーバ１３０から安全な接続を介して受信されてもよく、又は、他の何らかの方法で受信されてもよい。例えば、ＦＰＫは、ＫＭＳ１２０に直接的にアップロードされてもよく、又は、他の何らかの情報源から受信されてもよい。

【０１７８】

図７Ｂは、電子装置１００にファームウェアを提供する概略的な方法７５０のフローチャートを示す。電子装置１００は、ＰＵＦ４５０を有するセキュリティモジュール１１０を備えると仮定される。セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成される。公開鍵が電子装置１００に、例えば、電子装置１００のセキュリティモジュール１１０に、安全に組み込まれているとさらに仮定される。公開鍵は、公開鍵及び対応する秘密鍵を含む署名鍵ペアの一部である。署名鍵ペアは、公開認証局鍵と、認証局１４０にのみ知られた秘密認証局鍵とを含む認証局鍵ペアであってもよい。方法７５０は、例えば、鍵管理サーバ１２０によって実行されてもよい。

【０１７９】

７６０において、方法７５０は、署名鍵ペアの秘密鍵を用いて、暗号化された形式のフ

ァームウェアに署名させることを含む。ファームウェアは、サーバ暗号鍵Ｋを用いて暗号化される。サーバ暗号鍵は、ユーザクレデンシャル、例えばユーザのパスワード（例えばＯＥＭのパスワード）に少なくとも部分的に基づいてもよい。

【０１８０】

例えば、鍵管理サーバ１２０は、暗号化されていない形式でファームウェアを受信し、次いで、（図６Ｂの場合のように）サーバ暗号鍵Ｋを用いてファームウェアを暗号化してもよく、又は、暗号化された形式のファームウェアを直接的に受信してもよい。いくつかの実施形態では、鍵管理サーバ１２０は、署名鍵のペアの秘密鍵を用いて、暗号化された形式のファームウェアに署名するように構成されてもよい。しかしながら、（図６Ｂに示すような）他の実施形態では、鍵管理サーバ１２０は、認証局サーバシステム１３０の認証局サーバとの安全な接続を確立するように構成されてもよい。次いで、ＫＭＳ１２０は、暗号化された形式のファームウェアを認証局サーバに伝送し、暗号化及び署名された形式のファームウェアを受信してもよい。暗号化及び署名された形式のファームウェアは、認証局鍵ペアの秘密認証局鍵を用いて署名されている。

【０１８１】

７７０において、方法７５０は、電子装置１００へのインストールのために、暗号化及び署名された形式のファームウェアをサードパーティーに伝送することを含む。サードパーティーは、例えば、プログラミング会社１８０のサーバ、又は、ＫＭＳ及び認証局サーバシステム１３０の外部における他の任意の計算装置を備えてもよい。

【０１８２】

７８０において、方法７５０は、電子装置へのインストールのために、暗号化された形式のサーバ複合鍵をサードパーティーに伝送することを含む。サーバ復号鍵は、ＦＰＫを用いて暗号化される。当然ながら、暗号化された形式のサーバ復号鍵は、暗号化及び署名された形式のファームウェアがサードパーティーに伝送される前、同時、又は後に、サードパーティーに伝送されてもよい。

【０１８３】

ＦＰＫは、（図６Ａの場合のように）認証局サーバ１３０から安全な接続を介して受信されてもよく、又は、他の何らかの方法で受信されてもよい。例えば、ＦＰＫは、ＫＭＳ１２０に直接的にアップロードされてもよく、又は、他の何らかの情報源から受信されてもよい。

【０１８４】

図８Ａは、電子装置１００のファームウェアを認証する概略的な方法８００のフローチャートを示す。電子装置１００は、ＰＵＦ４５０を有するセキュリティモジュール１１０を備えると仮定される。セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいてファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立し、ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて登録鍵ペア（ＥＰＫ，ＥＳＫ）を確立するように構成される。認証局鍵ペアの公開認証局鍵ＰＡＫが、電子装置１００に、例えば、電子装置１００のセキュリティモジュール１１０に、すでに安全に組み込まれているとさらに仮定される。認証局鍵ペアは、ＰＡＫ及び対応する秘密認証局鍵ＳＡＫを含む。本方法は、例えば、認証局サーバシステム１３０の１つ又は複数のサーバによって実行されてもよい。

【０１８５】

８１０において、方法８００は、サーバから、安全な通信チャネルを介して、電子装置１００にインストールされるファームウェアのハッシュを受信することを含む。例えば、認証局サーバは、図６Ａの場合のように、ＴＬＳ接続を介してＫＭＳ１２０から暗号化されたファームウェアを受信してもよい。

【０１８６】

８２０において、方法８００は、公開認証局鍵（ＰＡＫ）及び秘密認証局鍵（ＳＡＫ）を含む認証局鍵ペアの秘密認証局鍵を用いて、ファームウェアのハッシュに署名することを含む。公開認証局鍵は電子装置に安全に組み込まれている。任意の適切なディジタル署

名方式が利用されてもよい。
【０１８７】
認証局サーバシステム１３０が方法８００を実行する場合、暗号化されたファームウェアに署名する認証局サーバは、ステップ８１０を実行した認証局サーバと同じであってもよく、又は、異なっていてもよい。
【０１８８】
８３０において、方法８００は、電子装置へのインストールのために、サードパーティーへのファームウェアのハッシュ上の署名の伝送を開始することを含む。例えば、サードパーティーは、プログラミング会社１８０を含んでもよく、又は、認証局サーバシステム１３０及び暗号化されたファームウェアの発信元であるサーバ（例えばＫＭＳ１２０）以外の任意のエンティティも含んでもよい。例えば、サーバシステム１３０は、（図６Ｂの場合のように）暗号化及びサードパーティーへの転送のためにＫＭＳ１２０に署名を伝送してもよく、又は、暗号化されていない形式で署名をサードパーティーに直接的に伝送してもよい。
【０１８９】
８４０において、方法８００は、ＦＰＫと、電子装置１００を識別するための、ＥＰＫの関数を含む関連付けられた装置識別子とを、安全な通信チャネルを介して、サーバ（例えばＫＭＳ１２０）に送信することを含む。ＦＰＫ及び装置識別子は、ルックアップテーブルとしてサーバに提供されてもよい。装置識別子及びＦＰＫは、任意の適切な方法で取得されてもよく、例えば、ＯＥＭ１６０に出荷される前にセキュリティモジュール１１０からそれらを抽出することで、又は、他のソースから情報を受信することで取得されてもよい。ステップ８３０は、ステップ８４０の前、同時、又は後に実行されてもよい。
【０１９０】
本方法は、電子装置がプログラミングされた後、装置識別子を登録する要求をサーバから受信することと、サーバを装置識別子に関連付けることとをさらに含んでもよい。
【０１９１】
図８Ｂは、電子装置１００のファームウェアを認証する概略的な方法８５０のフローチャートを示す。電子装置１００は、ＰＵＦ４５０を有するセキュリティモジュール１１０を備えると仮定される。セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいてファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立し、ＰＵＦに対する第２のチャレンジ及びレスポンスに基づいて登録鍵ペア（ＥＰＫ，ＥＳＫ）を確立するように構成される。認証局鍵ペアの公開認証局鍵ＰＡＫが、電子装置１００に、例えば、電子装置１００のセキュリティモジュール１１０に、すでに安全に組み込まれているとさらに仮定される。認証局鍵ペアは、ＰＡＫ及び対応する秘密認証局鍵ＳＡＫを含む。本方法は、例えば、認証局サーバシステム１３０の１つ又は複数のサーバによって実行されてもよい。
【０１９２】
８６０において、方法８５０は、サーバから、安全な通信チャネルを介して、電子装置１００にインストールされる暗号化されたファームウェアを受信することを含む。例えば、認証局サーバは、図６Ｂの場合のように、ＴＬＳ接続を介してＫＭＳ１２０から暗号化されたファームウェアを受信してもよい。
【０１９３】
８７０において、方法８５０は、認証局鍵ペアの秘密認証局鍵ＳＡＫを用いて、暗号化されたファームウェアに署名することを含む。任意の適切なディジタル署名方式が利用されてもよい。
【０１９４】
認証局サーバシステム１３０が方法８５０を実行する場合、暗号化されたファームウェアに署名する認証局サーバは、ステップ８６０を実行した認証局サーバと同じであってもよく、又は、異なっていてもよい。
【０１９５】

８８０において、方法８５０は、電子装置へのインストールのために、サードパーティーへの暗号化及び署名されたファームウェアの伝送を開始することを含む。例えば、サードパーティーは、プログラミング会社１８０を含んでもよく、又は、認証局サーバシステム１３０及び暗号化されたファームウェアの発信元であるサーバ（例えばＫＭＳ１２０）以外の任意のエンティティも含んでもよい。例えば、サーバシステム１３０は、サードパーティーへの転送のために、暗号化及び署名されたファームウェアをＫＭＳ１２０に伝送してもよく、又は、暗号化及び署名されたファームウェアをサードパーティーに直接的に伝送してもよい。

【０１９６】

８９０において、方法８５０は、ＦＰＫと、電子装置１００を識別するための、ＥＰＫの関数を含む関連付けられた装置識別子とを、安全な通信チャネルを介して、サーバ（例えばＫＭＳ１２０）に送信することを含む。ＦＰＫ及び装置識別子は、ルックアップテーブルとしてサーバに提供されてもよい。装置識別子及びＦＰＫは、任意の適切な方法で取得されてもよく、例えば、ＯＥＭ１６０に出荷される前にセキュリティモジュール１１０からそれらを抽出することで、又は、他のソースから情報を受信することで取得されてもよい。ステップ８８０は、ステップ８９０の前、同時、又は後に実行されてもよい。

【０１９７】

本方法は、電子装置がプログラミングされた後、装置識別子を登録する要求をサーバから受信することと、サーバを装置識別子に関連付けることとをさらに含んでもよい。

【０１９８】

図９Ａは、電子装置１００により実行する概略的な方法９００のフローチャートを示す。電子装置１００は、物理的複製困難関数（ＰＵＦ）４５０を有するセキュリティモジュール１１０を備える。セキュリティモジュール１１０は、ＰＵＦに対する第１のチャレンジ及びレスポンスに基づいて、ファームウェア鍵ペア（ＦＰＫ，ＦＳＫ）を確立するように構成される。

【０１９９】

９１０において、方法９００は、ＦＰＫを用いて暗号化されたサーバ復号鍵を、ＦＳＫを用いて復号することを含む。

【０２００】

９１５において、方法９００は、復号されたサーバ復号鍵を用いて、ファームウェアと、ファームウェアのハッシュ上の署名とを復号することを含む。

【０２０１】

９２０において、方法９００は、電子装置に安全に組み込まれていた公開認証局鍵を用いて、ファームウェアのハッシュが、認証局１４０のような信頼された認証局によって署名されていることを検証することを含む。公開認証局鍵は、公開認証局鍵と、信頼された認証局に所有された対応する秘密認証局鍵とを含む認証局鍵ペアの一部である。
ステップ９１０は、ステップ９２０の前、同時、又は後に実行されてもよい。

【０２０２】

９３０において、方法９００は、検証に基づいて、復号されたファームウェアを電子装置１００にインストールすることを含む。

【０２０３】

図９Ｂは、電子装置１００により実行するもう１つの概略的な方法９５０のフローチャートを示す。

【０２０４】

９６０において、方法９５０は、ＦＰＫを用いて暗号化されたサーバ復号鍵を、ＦＳＫを用いて復号することを含む。

【０２０５】

９７０において、方法９５０は、電子装置１００に安全に組み込まれていた公開認証局鍵を用いて、暗号化された形式のファームウェアが、認証局１４０のような信頼された認証局によって認証されていることを検証することを含む。公開認証局鍵は、公開認証局鍵

と、信頼された認証局に所有された対応する秘密認証局鍵とを含む認証局鍵ペアの一部である。ステップ９６０は、ステップ９７０の前、同時、又は後に実行されてもよい。

【０２０６】

９８０において、方法９５０は、復号されたサーバ復号鍵を用いて、電子装置１００にインストールされるファームウェアを復号することを含む。

【０２０７】

図６Ａ～図９Ｂに関して上述した方法は、ファームウェアが電子装置に安全に提供されることを可能にする。優位点として、ファームウェアは、認証局１４０及びプログラミング会社１８０のいずれにも、暗号化されていない形式で提供されることはない。いったん電子装置１００にファームウェアが提供されると、電子装置は登録を開始することができる。

【０２０８】

１つ又は複数のルート証明書は、製造時に電子装置１００にインストールされてもよく、又は、追加セキュリティのために、図６～図９に関して上述した方法を用いて、ファームウェアとともに、又はその一部として、電子装置１００に提供されてもよい。

【０２０９】

図１０は、いくつかの実施例に係るコンピュータ可読媒体１７００を示す。

【０２１０】

コンピュータ可読媒体１７００は、実行されたとき、プロセッサ１７２０又は他の処理／計算デバイス又は装置に特定の動作を実行させる命令１７１０をそれぞれ含む複数のユニットを格納する。

【０２１１】

例えば、命令１７１０は、公開鍵及び秘密鍵を含む鍵ペアの秘密鍵を用いて、ファームウェアのハッシュに署名させることをプロセッサ１７２０に実行させてもよい。公開鍵は電子装置に安全に組み込まれている。命令１７１０はさらに、サーバ暗号鍵を用いて、ファームウェアと、ハッシュ上の署名とを暗号化することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、暗号化されたファームウェア及び暗号化された署名を復号するためのサーバ復号鍵を、ＦＰＫを用いて暗号化することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、暗号化されたファームウェア、暗号化された署名、及び暗号化されたサーバ復号鍵を、電子装置へのインストールのために、サードパーティーに伝送することをプロセッサ１７２０に実行させてもよい。

【０２１２】

もう１つの実施例では、命令１７１０は、公開鍵及び秘密鍵を含む暗号鍵ペアの秘密鍵を用いて、暗号化された形式のファームウェアに署名させることをプロセッサ１７２０に実行させてもよい。公開鍵は電子装置に安全に組み込まれている。ファームウェアは、サーバ暗号鍵を用いて暗号化されている。命令１７１０はさらに、電子装置へのインストールのために、暗号化及び署名された形式のファームウェアをサードパーティーに伝送することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、電子装置へのインストールのために、暗号化された形式のサーバ複合鍵をサードパーティーに伝送することをプロセッサ１７２０に実行させてもよい。サーバ復号鍵は、暗号化された形式のファームウェアの復号用である。サーバ復号鍵は、ＦＰＫを用いて暗号化されている。

【０２１３】

例えば、命令１７１０は、公開認証局鍵及び秘密認証局鍵を含む認証局鍵ペアの秘密認証局鍵を用いて、上記ファームウェアのハッシュに署名することをプロセッサ１７２０に実行させてもよい。公開認証局鍵は、電子装置のセキュリティモジュールに安全に組み込まれている。ファームウェアのハッシュは、サーバから安全な通信チャネルを介して受信される。命令１７１０はさらに、電子装置へのインストールのために、サードパーティーへのファームウェアのハッシュ上の署名の伝送を開始することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、ファームウェア公開鍵ＦＰＫと、電子装置を識別するための、登録公開鍵ＥＰＫの関数を含む関連付けられた装置識別子とを示すルック

アップテーブルを、安全な通信チャネルを介してサーバに送信することをプロセッサ１７２０に実行させてもよい。

【０２１４】

もう１つの実施例では、命令１７１０は、公開認証局鍵及び秘密認証局鍵を含む認証局鍵ペアの秘密認証局鍵を用いて、暗号化されたファームウェアに署名することをプロセッサ１７２０に実行させてもよい。公開認証局鍵は、電子装置のセキュリティモジュールに安全に組み込まれている。暗号化されたファームウェアは、サーバから安全な通信チャネルを介して受信される。命令１７１０はさらに、電子装置へのインストールのために、サードパーティーへの暗号化及び署名されたファームウェアの伝送を開始することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、ファームウェア公開鍵ＦＰＫと、電子装置を識別するための、登録公開鍵ＥＰＫの関数を含む関連付けられた装置識別子とを示すルックアップテーブルを、安全な通信チャネルを介してサーバに送信することをプロセッサ１７２０に実行させてもよい。

【０２１５】

例えば、命令１７１０は、ファームウェア公開鍵ＦＰＫを用いて暗号化されたサーバ復号鍵を、ファームウェア秘密鍵ＦＳＫを用いて復号することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、暗号化されたファームウェアと、ファームウェアのハッシュ上の署名とを、復号されたサーバ復号鍵を用いて復号することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、電子装置に安全に組み込まれていた公開認証局鍵を用いて、ファームウェアのハッシュが、信頼された認証局によって署名されていることを検証することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、検証に基づいて、復号されたファームウェアを電子装置にインストールすることをプロセッサ１７２０に実行させてもよい。

【０２１６】

例えば、命令１７１０は、ＦＳＫとともにファームウェア鍵ペアを形成するファームウェア公開鍵ＦＰＫを用いて暗号化されたサーバ復号鍵を、ファームウェア秘密鍵ＦＳＫを用いて復号することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、公開認証局鍵を用いて、暗号化された形式のファームウェアが、信頼された認証局によって認証されていることを検証することをプロセッサ１７２０に実行させてもよい。命令１７１０はさらに、復号されたサーバ復号鍵を用いて、電子装置にインストールされるファームウェアを復号することをプロセッサ１７２０に実行させてもよい。

【０２１７】

１つ又は複数のコンピュータ可読媒体の任意の組み合わせが利用されてもよい。コンピュータ可読媒体は、コンピュータ可読信号媒体又はコンピュータ可読記憶媒体であってもよい。コンピュータ可読記憶媒体は、例えば、電子的、磁気的、光学的、電磁的、赤外線、または半導体システム、装置、デバイス、又は上述のものの任意の適切な組み合わせであってもよいが、これらに限定されない。コンピュータ可読媒体のより特定の例（非網羅的なリスト）は、１つ又は複数の導線を有する電気的接続、ポータブルコンピュータディスケット、ハードディスク、ランダムアクセスメモリ（ＲＡＭ）、読み出し専用メモリ（ＲＯＭ）、消去及びプログラム可能な読み出し専用メモリ（ＥＰＲＯＭ又はフラッシュメモリ）、光ファイバ、携帯型のコンパクトディスク読み出し専用メモリ（ＣＤＲＯＭ）、光記憶装置、磁気記憶装置、又は上述のものの任意の適切な組み合わせを含む。本願のコンテキストにおいて、コンピュータ可読記憶媒体は、命令実行システム、装置、又はデバイスにより使用するための、又は、それらに関連するプログラムを含む又は格納することができる任意の有形媒体であってもよい。

【０２１８】

コンピュータ可読信号媒体は、例えば、ベースバンド又は搬送波の一部として、そこに具体化されたコンピュータ可読プログラムコードを含む、伝搬されるデータ信号を含んでもよい。そのような伝搬される信号は、電磁的、光学的、又はそれらの任意の適切な組み合わせを含むが、これらに限定されない、さまざまな形式のうちの何かを有してもよい。

コンピュータ可読信号媒体は、コンピュータ可読記憶媒体でなく、命令実行システム、装置、又はデバイスによる使用のための、又はそれらに関連するプログラムを伝送、伝搬、又は輸送することができる、任意のコンピュータ可読媒体であってもよい。

【０２１９】

コンピュータ可読媒体に具体化されたコンピュータコードは、無線、有線、光ファイバケーブル、無線周波数（ＲＦ）など、又はそれらの任意の適切な組み合わせを含むが、これらに限定されない、任意の適切な媒体を用いて送信されてもよい。

【０２２０】

本発明の態様のための動作を実行するためのコンピュータプログラムコードは、Ｊａｖａ（登録商標）、Ｓｍａｌｌｔａｌｋ（登録商標）、Ｃ＋＋などのようなオブジェクト指向プログラミング言語、「Ｃ」プログラミング言語のような従来の手続き的なプログラミング言語、又は同様のプログラミング言語を含む、１つ又は複数のプログラミング言語の任意の組み合わせとして記述されてもよい。プログラムコードは、完全にユーザのコンピュータにおいて実行されてもよく、スタンドアロン型ソフトウェアパッケージとして、部分的にユーザのコンピュータにおいて実行されてもよく、部分的にユーザのコンピュータにおいて、かつ、部分的に遠隔のコンピュータにおいて実行されてもよく、又は完全に遠隔のコンピュータ又はサーバにおいて実行されてもよい。後者のシナリオにおいて、遠隔のコンピュータは、ローカルエリアネットワーク（ＬＡＮ）又はワイドエリアネットワーク（ＷＡＮ）を含む任意のタイプのネットワークを介してユーザのコンピュータに接続されてもよく、又は、接続は、（例えば、インターネットサービスプロバイダーを用いてインターネットを介して）外部コンピュータに対して行われてもよい。

【０２２１】

本願において説明した方法の多数の変形例が当業者には明らかになるであろう。

【０２２２】

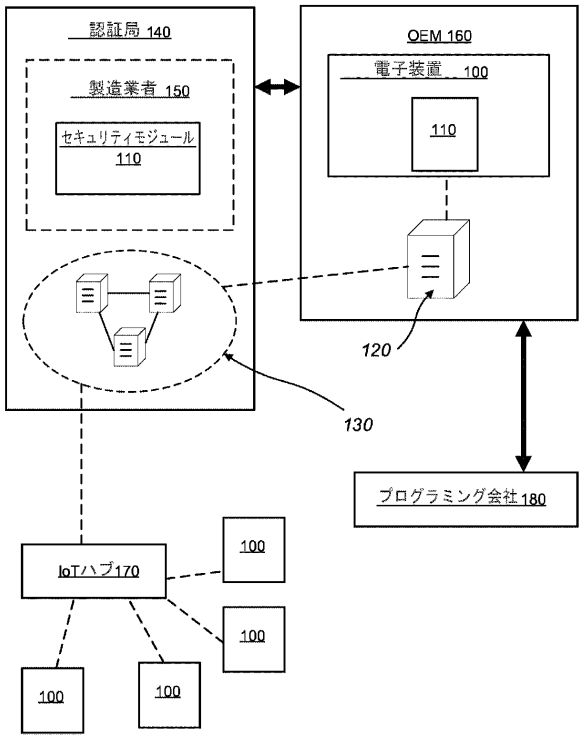
本明細書（任意の添付の特許請求の範囲、要約書、及び図面も含む）において開示された各特徴は、明示的にそうでないと述べていない限り、同じ、同等、又は類似した目的をはたす代替の特徴で置き換えられてもよい。したがって、明示的にそうでないと述べていない限り、開示された各特徴は、一般的な一連の同等又は同様の特徴の単なる一例である。

【０２２３】

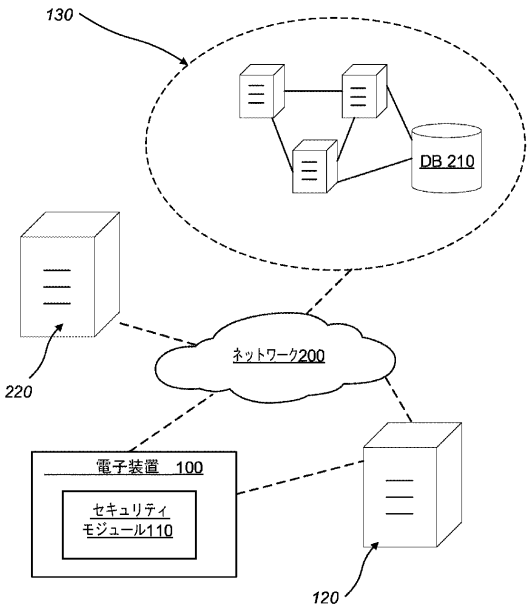
本発明は、上述した実施形態のいずれの詳細事項にも限定されない。本発明は、本明細書（任意の添付の特許請求の範囲、要約書、及び図面も含む）において開示された特徴のうちの任意の新規なもの又は任意の新規な組み合わせに拡張され、又は、そのように開示された任意の方法又は処理のステップのうちの任意の新規なもの又は任意の新規な組み合わせに拡張される。特許請求の範囲は、単に上述した実施形態をカバーするように解釈されるべきでなく、特許請求の範囲内にある任意の実施形態をカバーするように解釈されるべきである。

【図面】

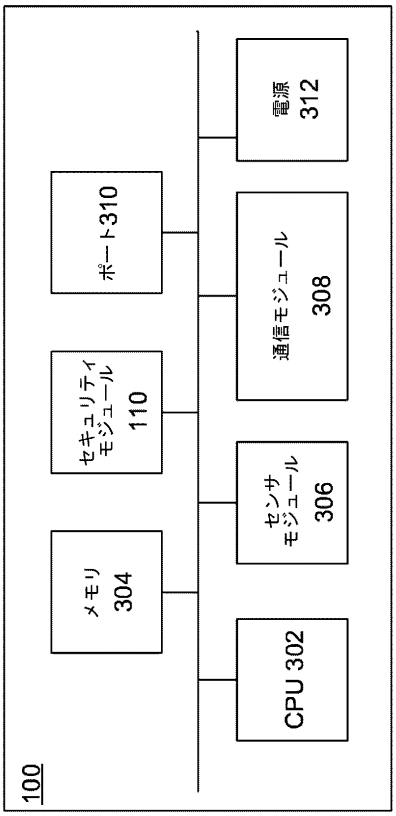
【図１】



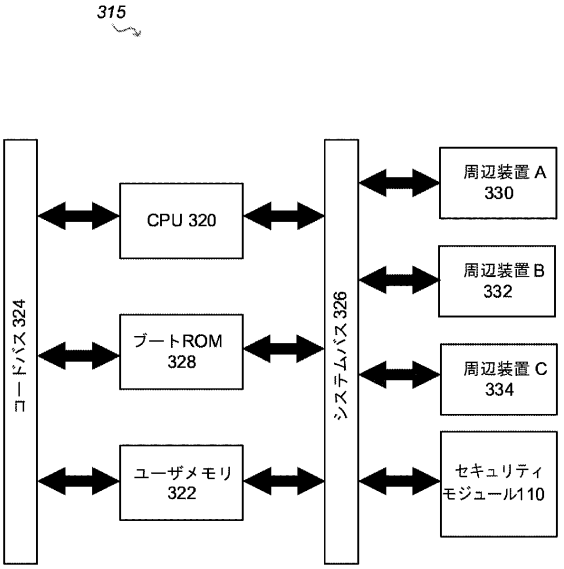
【図２】



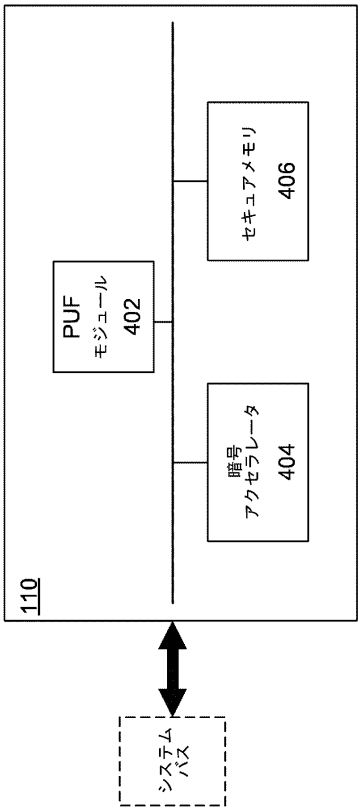
【図３Ａ】



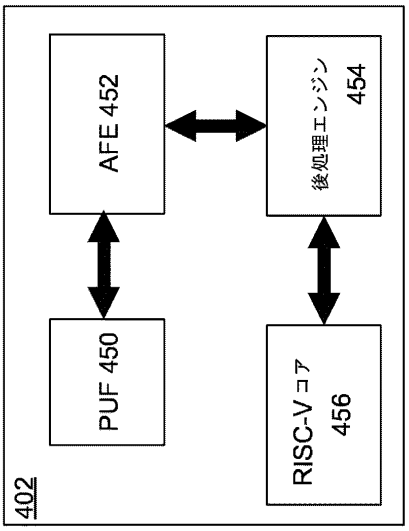
【図３Ｂ】



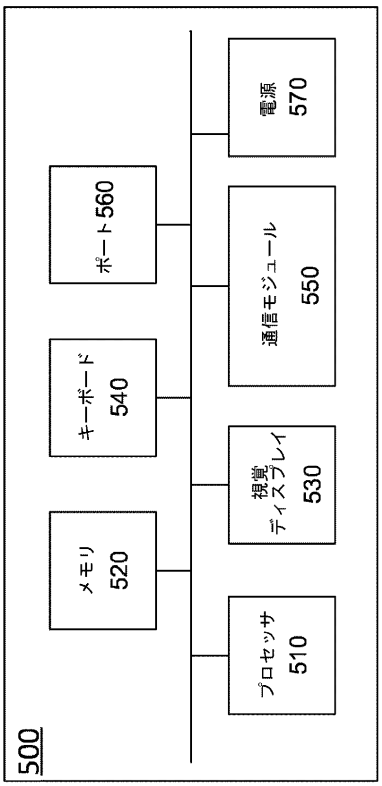
【図４Ａ】



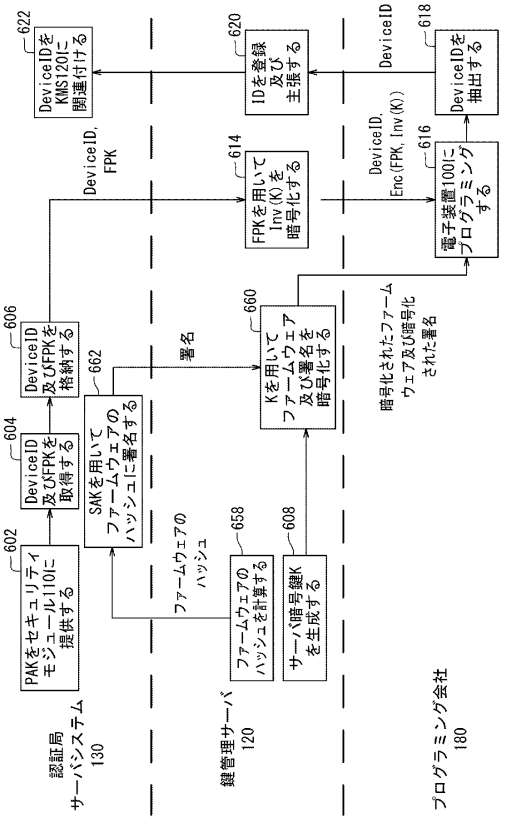
【図４Ｂ】



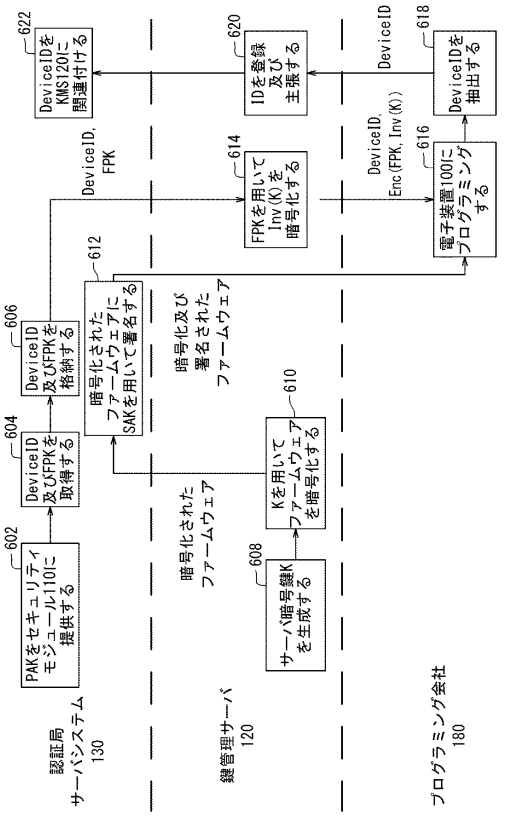
【図５】



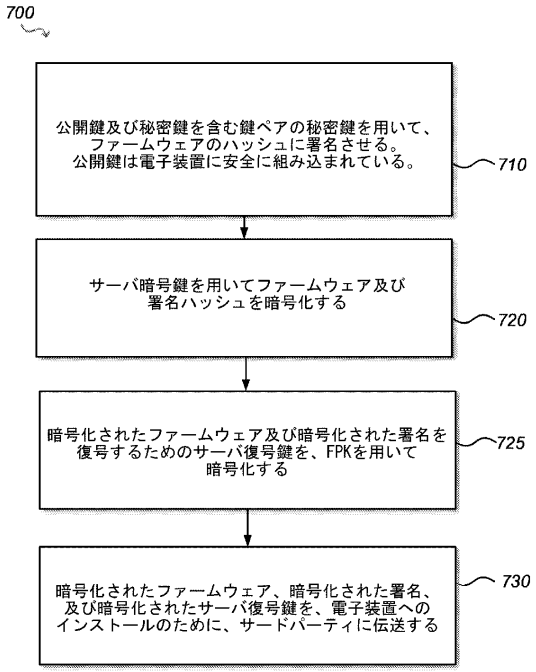
【図６Ａ】



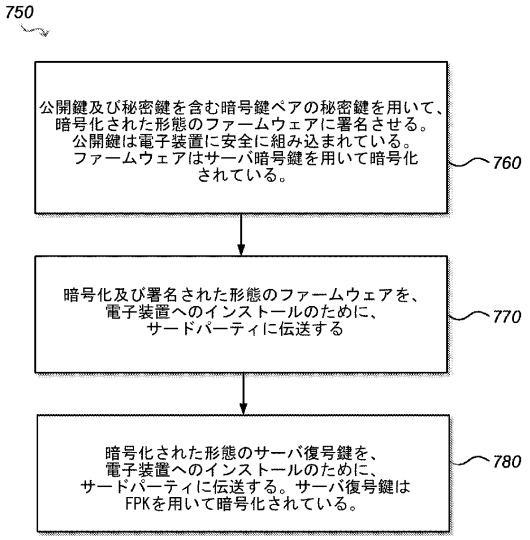
【図６Ｂ】



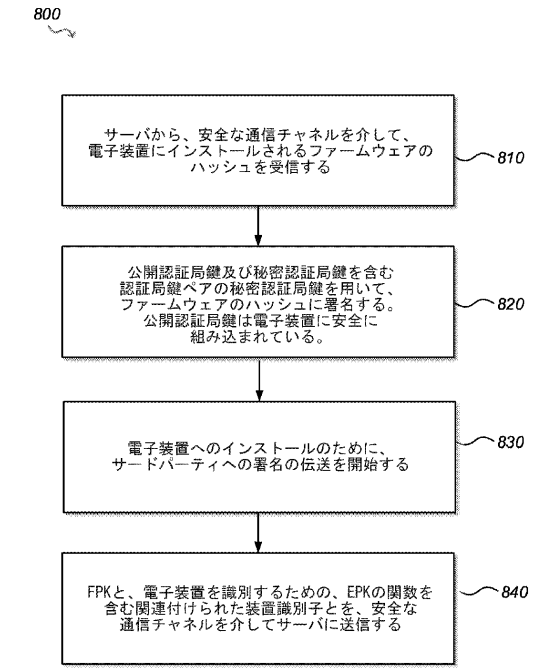
【図７Ａ】



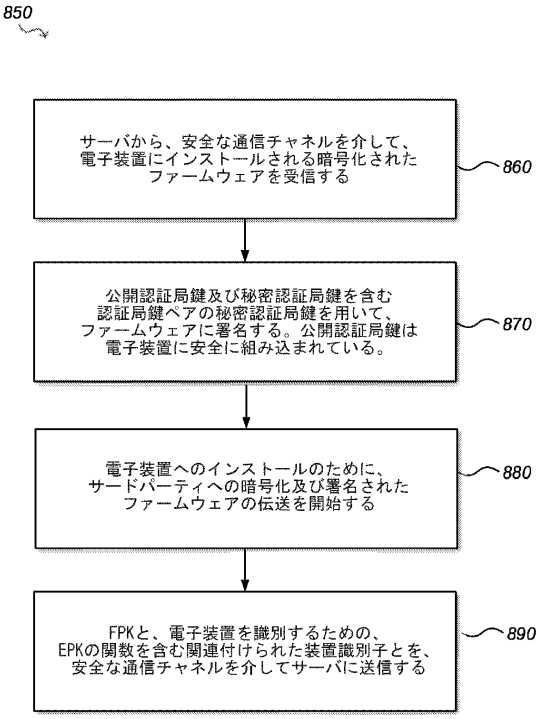
【図７Ｂ】



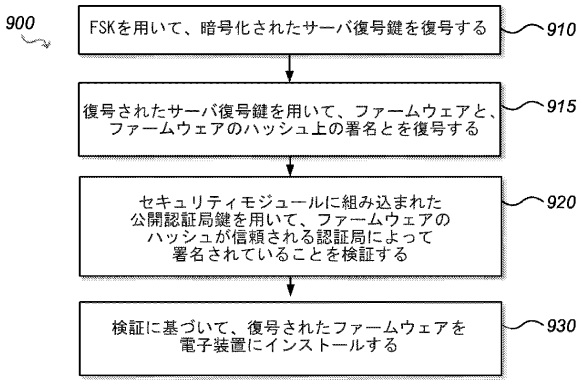
【図８Ａ】



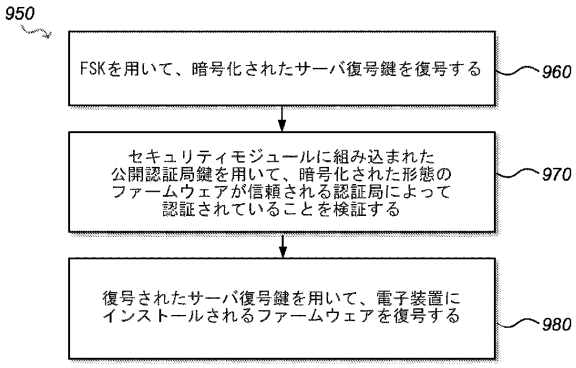
【図８Ｂ】



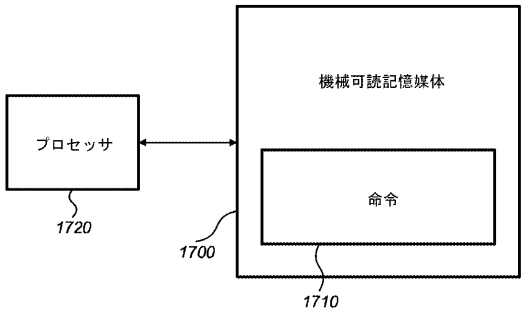
【図９Ａ】



【図９Ｂ】



【図１０】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2022/050910

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/06 H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2020/159965 A1 (NOREM JOSHUA JAY [US]) 21 May 2020 (2020-05-21) paragraph [0006] - paragraph [0009] paragraph [0017] - paragraph [0058]; figures 1-6 claims 1-15	1-24
A	MANSOR HAFIZAH ET AL: "Don't Brick Your Car: Firmware Confidentiality and Rollback for Vehicles", 2015 10TH INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY, IEEE, 24 August 2015 (2015-08-24), pages 139-148, XP032795237, DOI: 10.1109/ARES.2015.58 sections II, III; figures 1, 2; tables III, IV	1-24

-/--

[x] Further documents are listed in the continuation of Box C.
[x] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 June 2022	24/06/2022

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Spranger, Stephanie

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2022/050910

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Schrijen Geert-Jan, Selimis Georgios, Treurniet Jan Jaap: "Secure Device Management for the Internet of Things", Intrinsic id, 1 April 2019 (2019-04-01), pages 1-10, XP055865750, sections II, III; figures 1-5 -----	1-24

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2022/050910

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2020159965 A1	21-05-2020	CN 111199058 A	26-05-2020
		US 2020159965 A1	21-05-2020

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(51)国際特許分類　　ＦＩ
　　Ｇ０６Ｆ　　21/73

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JM,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

０、ザ・プリント・ルームズ、ユニット３０４－５

(72)発明者　グローバー，チャールズ
英国エスイー１・０エルエイチ、ロンドン、ユニオン・ストリート１６４－１８０、ザ・プリント・ルームズ、ユニット３０４－５

(72)発明者　モサエビ，シャフラム
英国エスイー１・０エルエイチ、ロンドン、ユニオン・ストリート１６４－１８０、ザ・プリント・ルームズ、ユニット３０４－５