(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6707717号
(P6707717)
(45)発行日　令和2年6月10日(2020.6.10)　(24)登録日　令和2年5月22日(2020.5.22)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601A
H04W 12/04	(2009.01)	H04L	9/00	601F
H04W 84/10	(2009.01)	H04W	12/04	
		H04W	84/10	110

請求項の数 27　(全 34 頁)

(21)出願番号　特願2019-520681 (P2019-520681)
(86)(22)出願日　平成29年8月25日 (2017.8.25)
(65)公表番号　特表2019-537871 (P2019-537871A)
(43)公表日　令和1年12月26日 (2019.12.26)
(86)国際出願番号　PCT/US2017/048560
(87)国際公開番号　WO2018/075135
(87)国際公開日　平成30年4月26日 (2018.4.26)
審査請求日　令和2年2月19日 (2020.2.19)
(31)優先権主張番号　62/410,309
(32)優先日　平成28年10月19日 (2016.10.19)
(33)優先権主張国・地域又は機関
米国 (US)
(31)優先権主張番号　15/648,437
(32)優先日　平成29年7月12日 (2017.7.12)
(33)優先権主張国・地域又は機関
米国 (US)

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100158805
弁理士　井関　守三
(74)代理人　100112807
弁理士　岡田　貴志

最終頁に続く

(54)【発明の名称】デバイスプロビジョニングプロトコル（ＤＰＰ）のためのコンフィギュレータ鍵パッケージ

(57)【特許請求の範囲】
【請求項１】
ネットワークの第１のコンフィギュレータデバイスによって実行される方法であって、
前記第１のコンフィギュレータデバイスによって、前記ネットワークでエンローリデバイスを登録するために前記第１のコンフィギュレータデバイスがコンフィギュレータ秘密署名鍵を使用するように構成されたデバイスプロビジョニングプロトコルを実装することと、
前記第１のコンフィギュレータデバイスに関連付けられた少なくとも前記コンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成することと、
前記コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することと、
第２のコンフィギュレータデバイスによる後のリストアのためのバックアップとして、ストレージロケーションに前記コンフィギュレータ鍵パッケージを記憶することと、
を備え、同じコンフィギュレータ秘密署名鍵および同じコンフィギュレータ公開検証鍵は、前記デバイスプロビジョニングプロトコルに従って前記ネットワークで異なるエンローリデバイスを登録するために、前記第２のコンフィギュレータデバイスを含む複数のコンフィギュレータ間で共有される、方法。
【請求項２】
前記コンフィギュレータ鍵パッケージは、前記コンフィギュレータ秘密署名鍵に関連付けられるコンフィギュレータ公開検証鍵をさらに含む、請求項１に記載の方法。
【請求項３】

前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を暗号化することは、前記コンフィギュレータ秘密署名鍵とは異なる暗号鍵を使用して前記コンフィギュレータ鍵パッケージを暗号化することを含む、請求項１に記載の方法。

【請求項４】

前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を暗号化することは、秘密鍵暗号化技法を使用して前記コンフィギュレータ秘密署名鍵を暗号化することと、前記コンフィギュレータ鍵パッケージのヘッダ中に前記秘密鍵暗号化技法のインジケーションを含めることと、を含む、請求項１に記載の方法。

【請求項５】

前記コンフィギュレータ鍵パッケージを記憶することは、

前記コンフィギュレータ鍵パッケージと復号情報とを含むデジタルエンベロープを生成することを含み、前記復号情報は、前記第２のコンフィギュレータデバイスが前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することを可能にする、

請求項１に記載の方法。

【請求項６】

前記ストレージロケーションは、前記第１のコンフィギュレータデバイスのメモリ、ネットワーク共有ロケーション、パーソナルコンピュータ、ホームサーバ、クラウドベースのストレージサービス、およびワイヤレスネットワークのアクセスポイント（ＡＰ）、からなるグループから選択される少なくとも１つのメンバである、請求項１に記載の方法。

【請求項７】

前記第１のコンフィギュレータデバイスによって、前記ストレージロケーションから前記コンフィギュレータ鍵パッケージの前記バックアップを検索することと、

前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することと、

前記コンフィギュレータ鍵パッケージから前記コンフィギュレータ秘密署名鍵を取得することと、

をさらに備える、請求項１に記載の方法。

【請求項８】

前記コンフィギュレータ鍵パッケージから取得された前記コンフィギュレータ秘密署名鍵に少なくとも部分的に基づいて、コンフィギュレータ公開検証鍵を決定すること、

をさらに備える、請求項７に記載の方法。

【請求項９】

前記ストレージロケーションにおける前記コンフィギュレータ鍵パッケージのロケーションアドレスを決定することと、

前記第２のコンフィギュレータデバイスに前記ロケーションアドレスを提供することと、

をさらに備える、請求項１に記載の方法。

【請求項１０】

前記第２のコンフィギュレータデバイスに復号情報を提供することをさらに備え、前記復号情報は、前記第２のコンフィギュレータデバイスが、前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することと、前記コンフィギュレータ秘密署名鍵を取得することと、を可能にする、

請求項１に記載の方法。

【請求項１１】

前記復号情報は、前記ストレージロケーションにおける前記コンフィギュレータ鍵パッケージのロケーションアドレスと、前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号するために使用可能な暗号鍵と、からなるグループから選択される少なくとも１つのメンバを含む、請求項１０に記載の方法。

【請求項１２】

前記復号情報を提供することは、前記第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェ

ース、からなるグループから選択される少なくとも１つのメンバからの信号中で前記復号情報を通信することを含む、請求項１０に記載の方法。
【請求項１３】
前記復号情報を提供することは、前記復号情報が符号化されているイメージを表示することを含む、請求項１０に記載の方法。
【請求項１４】
前記イメージは、バーコードまたはクイックレスポンス（ＱＲ）コードイメージである、請求項１３に記載の方法。
【請求項１５】
第１のコンフィギュレータデバイスで使用するための装置であって、
少なくとも１つのプロセッサと、前記少なくとも1つのプロセッサは、
前記ネットワークでエンローリデバイスを登録するために前記第１のコンフィギュレータデバイスがコンフィギュレータ秘密署名鍵を使用するように構成されたデバイスプロビジョニングプロトコルを実装することと、
前記第１のコンフィギュレータデバイスに関連付けられた少なくとも前記コンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成することと、
前記コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することと、
を行うように構成され、
第２のコンフィギュレータデバイスによる後のリストアのためのバックアップとして、ストレージロケーションに前記コンフィギュレータ鍵パッケージを出力するように構成された第１のインターフェースと、
を備え、同じコンフィギュレータ秘密署名鍵および同じコンフィギュレータ公開検証鍵は、前記デバイスプロビジョニングプロトコルに従って前記ネットワークで異なるエンローリデバイスを登録するために、前記第２のコンフィギュレータデバイスを含む複数のコンフィギュレータ間で共有される、装置。
【請求項１６】
前記プロセッサは、前記コンフィギュレータ秘密署名鍵とは異なる暗号鍵を使用して前記コンフィギュレータ鍵パッケージを暗号化する
ようにさらに構成される、請求項１５に記載の装置。
【請求項１７】
前記プロセッサは、
秘密鍵暗号化技法を使用して前記コンフィギュレータ秘密署名鍵を暗号化することと、
前記コンフィギュレータ鍵パッケージのヘッダ中に前記秘密鍵暗号化技法のインジケーションを含めることと、
を行うようにさらに構成される、請求項１５に記載の装置。
【請求項１８】
前記プロセッサは、前記コンフィギュレータ鍵パッケージと復号情報とを含むデジタルエンベロープを生成するようにさらに構成され、前記復号情報は、前記第２のコンフィギュレータデバイスが前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することを可能にする、請求項１５に記載の装置。
【請求項１９】
前記プロセッサは、
前記ストレージロケーションから前記コンフィギュレータ鍵パッケージの前記バックアップを検索することと、
前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することと、
前記コンフィギュレータ鍵パッケージから前記コンフィギュレータ秘密署名鍵を取得することと、
を行うようにさらに構成される、請求項１５に記載の装置。
【請求項２０】
プロセッサは、

前記ストレージロケーションにおけるコンフィギュレータ鍵パッケージのロケーションアドレスを決定することと、
前記第２のコンフィギュレータデバイスに前記ロケーションアドレスを提供することと、
を行うようにさらに構成される、請求項１５に記載の装置。
【請求項２１】
プロセッサは、前記第２のコンフィギュレータデバイスに復号情報を提供するようにさらに構成され、前記復号情報は、前記第２のコンフィギュレータデバイスが、前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することと、前記コンフィギュレータ秘密署名鍵を取得することと、を可能にする、請求項１５に記載の装置。
【請求項２２】
前記復号情報は、前記ストレージロケーションにおける前記コンフィギュレータ鍵パッケージのロケーションアドレスと、前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号するために使用可能な暗号鍵と、からなるグループから選択される少なくとも１つのメンバを含む、請求項２１に記載の装置。
【請求項２３】
前記プロセッサは、前記第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェース、からなるグループから選択される少なくとも１つのメンバを使用して前記復号情報を提供するようにさらに構成される、請求項２１に記載の装置。
【請求項２４】
ネットワークの第１のコンフィギュレータデバイスで使用するためのワイヤレス通信デバイスであって、
少なくとも１つのモデムと、
前記少なくとも１つのモデムと通信可能に結合された少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサと通信可能に結合され、プロセッサ可読コードを記憶する少なくとも１つのメモリと、を備え、
前記プロセッサ可読コードは、前記少なくとも１つのモデムと連携して前記少なくとも１つのプロセッサによって実行されたとき、
前記ネットワークでエンローリデバイスを登録するために前記第１のコンフィギュレータデバイスがコンフィギュレータ秘密署名鍵を使用するように構成されたデバイスプロビジョニングプロトコルを実装することと、
前記第１のコンフィギュレータデバイスに関連付けられた少なくとも前記コンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成することと、
前記コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することと、
第２のコンフィギュレータデバイスによる後のリストアのためのバックアップとして、ストレージロケーションに前記コンフィギュレータ鍵パッケージを記憶することと、ここにおいて、同じコンフィギュレータ秘密署名鍵および同じコンフィギュレータ公開検証鍵は、前記デバイスプロビジョニングプロトコルに従って前記ネットワークで異なるエンローリデバイスを登録するために、前記第２のコンフィギュレータデバイスを含む複数のコンフィギュレータ間で共有される、
を行うように構成される、ワイヤレス通信デバイス。
【請求項２５】
前記プロセッサ可読コードは、前記少なくとも１つのプロセッサによって実行されたとき、
秘密鍵暗号化技法を使用して前記コンフィギュレータ秘密署名鍵を暗号化することと、
前記コンフィギュレータ鍵パッケージのヘッダ中に前記秘密鍵暗号化技法のインジケーションを含めることと、
を行うように構成される、請求項２４に記載のワイヤレス通信デバイス。
【請求項２６】

前記プロセッサ可読コードは、前記少なくとも１つのプロセッサによって実行されたとき、
前記ストレージロケーションから前記コンフィギュレータ鍵パッケージの前記バックアップを検索することと、
前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することと、
前記コンフィギュレータ鍵パッケージから前記コンフィギュレータ秘密署名鍵を取得することと、
を行うように構成される、請求項２４に記載のワイヤレス通信デバイス。
【請求項２７】
モバイル局であって、
ネットワークの第１のコンフィグレータデバイスにおいて使用するためのワイヤレス通信デバイスを備え、前記ワイヤレス通信デバイスは、
少なくとも１つのモデムと、
前記少なくとも１つのモデムと通信可能に結合された少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサと通信可能に結合され、プロセッサ可読コードを記憶する少なくとも１つのメモリと、
前記プロセッサ可読コードは、前記少なくとも１つのモデムと連携して前記少なくとも１つのプロセッサによって実行されたとき、
ネットワークでエンローリデバイスを登録するために第１のコンフィギュレータデバイスがコンフィギュレータ秘密署名鍵を使用するように構成されたデバイスプロビジョニングプロトコルを実装することと、
前記第１のコンフィギュレータデバイスに関連付けられた少なくとも前記コンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成することと、
前記コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することと、
第２のコンフィギュレータデバイスによる後のリストアのためのバックアップとして、ストレージロケーションに前記コンフィギュレータ鍵パッケージを記憶することと、ここにおいて、同じコンフィギュレータ秘密署名鍵および同じコンフィギュレータ公開検証鍵は、前記デバイスプロビジョニングプロトコルに従って前記ネットワークで異なるエンローリデバイスを登録するために、前記第２のコンフィギュレータデバイスを含む複数のコンフィギュレータ間で共有される、
を行うように構成され、
前記少なくとも１つのモデムに結合された少なくとも１つのトランシーバと、
前記少なくとも１つのトランシーバから出力された信号をワイヤレスに送信するために、および前記少なくとも１つのトランシーバへの入力のための信号をワイヤレスに受信するために、前記少なくとも１つのトランシーバに結合された少なくとも１つのアンテナと、
前記少なくとも１つのモデム、前記少なくとも１つのプロセッサ、前記少なくとも１つのメモリ、前記少なくとも１つのトランシーバ、および前記少なくとも１つのアンテナの少なくとも一部分、を包含するハウジングと、
を備える、モバイル局。
【発明の詳細な説明】
【関連出願】
【０００１】
[0001] 本特許出願は、「DEVICE PROVISIONING PROTOCOL (DPP) WITH MULTIPLE CONFIGURATORS」と題され、本願の譲受人に譲渡された、２０１６年１０月１９日付で出願された、米国仮特許出願第６２／４１０，３０９号の優先権を主張する、２０１７年７月１２日付で出願された、米国特許出願第１５／６４８，４３７号の優先権を主張する。これら先行出願の開示は、本特許出願の一部と見なされ、かつ参照により本特許出願に組み込まれている。
【技術分野】

【０００２】
[0002] 本開示は、概して、通信システムの分野に関し、より具体的には、通信ネットワーク中のデバイスプロビジョニングプロトコル（ＤＰＰ）に関する。
【背景技術】
【０００３】
[0003] ネットワークは、通信媒体を介して互いに通信するデバイスを含んでいる。デバイスは、そのデバイスがネットワークの他のデバイスと通信する前に通信媒体にアクセスするためのパラメータを用いて構成される。デバイスを構成するプロセスは、デバイスプロビジョニングと呼ばれ得、アソシエーション、登録、認証に関するオペレーション、または他のオペレーションを含み得る。ネットワーク用にまだ構成されていない新規のデバイスは、エンローリデバイス（enrollee device）と呼ばれる。デバイスプロビジョニングプロトコル（ＤＰＰ：device provisioning protocol）は、ネットワークに取り込まれるエンローリデバイスの構成を容易にし得る。コンフィギュレータデバイスは、デバイスプロビジョニングプロトコルにしたがって、ネットワークに関するエンローリデバイスを構成するための能力を有するデバイスである。
【発明の概要】
【０００４】
[0004] 本開示のシステム、方法、およびデバイスはそれぞれ、いくつかの革新的な様態を有し、これらのうちの何れも、本明細書に開示される所望の属性を単独で担うものではない。
【０００５】
[0005] 本開示で説明される主題の１つの革新的な態様は、ネットワークの第１のコンフィギュレータデバイスに実装されることができる。第１のコンフィギュレータデバイスは、第１のコンフィギュレータデバイスに関連付けられた少なくともコンフィギュレータ秘密署名鍵（private signing key）を含む、コンフィギュレータ鍵パッケージを生成し得る。第１のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化する。第１のコンフィギュレータデバイスは、第１のコンフィギュレータデバイスまたは第２のコンフィギュレータデバイスによる後のリストア（restore）のためのバックアップとして、ストレージロケーションにコンフィギュレータ鍵パッケージを記憶する。
【０００６】
[0006] いくつかの実装では、コンフィギュレータ鍵パッケージは、コンフィギュレータ秘密署名鍵に関連付けられるコンフィギュレータ公開検証鍵（public verification key）をさらに含む。
【０００７】
[0007] いくつかの実装では、第１のコンフィギュレータデバイスは、コンフィギュレータ秘密署名鍵とは異なる暗号鍵（encryption key）を使用してコンフィギュレータ鍵パッケージを暗号化し得る。
【０００８】
[0008] いくつかの実装では、第１のコンフィギュレータデバイスは、秘密鍵暗号化技法を使用してコンフィギュレータ秘密署名鍵を暗号化し、コンフィギュレータ鍵パッケージのヘッダ中に秘密鍵暗号化技法のインジケーションを含め得る。
【０００９】
[0009] いくつかの実装では、第１のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージと復号（decrypt）情報とを含むデジタルエンベロープ（digital envelope）を生成し得る。復号情報は、第２のコンフィギュレータデバイスがコンフィギュレータ鍵パッケージの少なくとも一部分を復号することを可能にし得る。
[0010] いくつかの実装では、ストレージロケーションは、第１のコンフィギュレータデバイスのメモリ、ネットワーク共有ロケーション、パーソナルコンピュータ、ホームサーバ、クラウドベースのストレージサービス、およびワイヤレスネットワークのアクセス

ポイント（ＡＰ）、からなるグループから選択される少なくとも１つのメンバである。
【００１０】
[0011] いくつかの実装では、コンフィギュレータ鍵パッケージを記憶することは、コンフィギュレータ鍵パッケージのバックアップを記憶することを含む。第１のコンフィギュレータデバイスは、ストレージロケーションからコンフィギュレータ鍵パッケージのバックアップを検索し得る。第１のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージの少なくとも一部分を復号し得、コンフィギュレータ鍵パッケージからコンフィギュレータ秘密署名鍵を取得し得る。
【００１１】
[0012] いくつかの実装では、第１のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージから取得されたコンフィギュレータ秘密署名鍵に少なくとも部分的に基づいて、コンフィギュレータ公開検証鍵を決定し得る。
【００１２】
[0013] いくつかの実装では、第１のコンフィギュレータデバイスは、ストレージロケーションにおいてコンフィギュレータ鍵パッケージのロケーションアドレスを決定し得、第２のコンフィギュレータデバイスにロケーションアドレスを提供し得る。
【００１３】
[0014] いくつかの実装では、第１のコンフィギュレータデバイスは、デバイスプロビジョニングプロトコルに関連付けられたブートストラッピング技法を使用して、復号情報を提供し得る。
【００１４】
[0015] いくつかの実装では、第１のコンフィギュレータデバイスは、第２のコンフィギュレータデバイスに復号情報を提供し得る。復号情報は、第２のコンフィギュレータデバイスが少なくともコンフィギュレータ鍵パッケージの一部分を復号することを可能にし得、コンフィギュレータ秘密署名鍵およびコンフィギュレータ公開検証鍵を取得し得る。
【００１５】
[0016] いくつかの実装では、復号情報は、ストレージロケーションにおけるコンフィギュレータ鍵パッケージのロケーションアドレス、パスフレーズ（passphrase）、およびコンフィギュレータ鍵パッケージの少なくとも一部分を復号するために使用可能な暗号鍵からなるグループ構成から選択される少なくとも１つのメンバを含む。
【００１６】
[0017] いくつかの実装では、復号情報を提供することは、第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェース、からなるグループから選択される少なくとも１つのメンバを使用して復号情報を提供することを含む。
【００１７】
[0018] いくつかの実装では、第１のコンフィギュレータデバイスは、復号情報が符号化されているイメージを表示することによって、復号情報を提供し得る。
【００１８】
[0019] いくつかの実装では、イメージは、バーコードまたはクイックレスポンス（ＱＲ）コードイメージである。
【００１９】
[0020] いくつかの実装では、コンフィギュレータ秘密署名鍵およびコンフィギュレータ公開検証鍵は、第１のネットワークの複数のコンフィギュレータ間で共有される。複数のコンフィギュレータの各々は、第１のネットワーク用のエンローリデバイスを構成するために、デバイスプロビジョニングプロトコルに従ってコンフィギュレータ秘密署名鍵およびコンフィギュレータ公開検証鍵を使用することが可能であり得る。
【００２０】
[0021] 本開示で説明される主題の別の革新的な態様は、第２のコンフィギュレータデバイスに実装され得る。第２のコンフィギュレータデバイスは、ストレージロケーション

から、コンフィギュレータ鍵パッケージを取得し得る。コンフィギュレータ鍵パッケージの少なくとも一部分は暗号化され得、コンフィギュレータ鍵パッケージは、第１のコンフィギュレータデバイスに関連付けられた、少なくともコンフィギュレータ秘密署名鍵およびコンフィギュレータ公開検証鍵を含み得る。第２のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージの少なくとも一部分を復号し得る。第２のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージからコンフィギュレータ秘密署名鍵を取得し得る。第２のコンフィギュレータデバイスは、デバイスプロビジョニングプロトコルに従って、コンフィギュレータ秘密署名鍵を利用して、ネットワーク用にエンローリデバイスをプロビジョニングし得る。

【００２１】

[0022] いくつかの実装では、第２のコンフィギュレータデバイスは、第１のコンフィギュレータデバイスから復号情報を取得し得る。復号情報は、第２のコンフィギュレータデバイスがコンフィギュレータ鍵パッケージの少なくとも一部分を復号することを可能にし得る。

【００２２】

[0023] いくつかの実装では、第２のコンフィギュレータデバイスは、第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェース、からなるグループから選択される少なくとも１つのメンバを使用して復号情報を取得し得る。

【００２３】

[0024] いくつかの実装では、第２のコンフィギュレータデバイスは、第２のコンフィギュレータデバイスに関連付けられたカメラを介して、復号情報が符号化されているイメージを取得し得る。第２のコンフィギュレータデバイスは、復号情報を検索するためにイメージを復号し得る。

【００２４】

[0025] 本開示で説明されている主題の別の革新的な態様が、方法に実装され得る。方法は、ネットワークの第１のコンフィギュレータデバイスによって行われ得、第１のコンフィギュレータデバイスに関連付けられた少なくともコンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成することを含み得る。方法は、コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することを含み得る。方法は、第１のコンフィギュレータデバイスは、第１のコンフィギュレータデバイスまたは第２のコンフィギュレータデバイスによる後のリストアのためのバックアップとして、ストレージロケーションにコンフィギュレータ鍵パッケージを記憶することを含み得る。

【００２５】

[0026] いくつかの実装では、コンフィギュレータ鍵パッケージは、コンフィギュレータ秘密署名鍵に関連付けられるコンフィギュレータ公開検証鍵をさらに含み得る。

【００２６】

[0027] いくつかの実装では、コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することは、コンフィギュレータ秘密署名鍵とは異なる暗号鍵を使用してコンフィギュレータ鍵パッケージを暗号化することを含み得る。

【００２７】

[0028] いくつかの実装では、コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することは、秘密鍵暗号化技法を使用してコンフィギュレータ秘密署名鍵を暗号化することを含み得、コンフィギュレータ鍵パッケージのヘッダ中に秘密鍵暗号化技法のインジケーションを含める。

【００２８】

[0029] いくつかの実装では、コンフィギュレータ鍵パッケージを記憶することは、コンフィギュレータ鍵パッケージと復号情報とを含むデジタルエンベロープを生成することを含み得、復号情報は、第２のコンフィギュレータデバイスがコンフィギュレータ鍵パッケージの少なくとも一部分を復号することを可能にする。

【００２９】
[0030] いくつかの実装では、ストレージロケーションは、第１のコンフィギュレータデバイスのメモリ、ネットワーク共有ロケーション、パーソナルコンピュータ、ホームサーバ、クラウドベースのストレージサービス、およびワイヤレスネットワークのアクセスポイント（ＡＰ）、からなるグループから選択される少なくとも１つのメンバであり得る。
【００３０】
[0031] いくつかの実装では、コンフィギュレータ鍵パッケージを記憶することは、コンフィギュレータ鍵パッケージのバックアップを記憶することを含み得る。方法は、第１のコンフィギュレータデバイスによって、ストレージロケーションからコンフィギュレータ鍵パッケージのバックアップを検索することを含み得る。方法は、コンフィギュレータ鍵パッケージの少なくとも一部分を復号することを含み得る。方法は、コンフィギュレータ鍵パッケージからコンフィギュレータ秘密署名鍵を取得することを含み得る。
【００３１】
[0032] いくつかの実装では、方法は、コンフィギュレータ鍵パッケージから取得されたコンフィギュレータ秘密署名鍵に少なくとも部分的に基づいて、コンフィギュレータ公開検証鍵を決定することを含み得る。
【００３２】
[0033] いくつかの実装では、方法は、ストレージロケーションにおけるコンフィギュレータ鍵パッケージのロケーションアドレスを決定することを含み得る。方法は、第２のコンフィギュレータデバイスにロケーションアドレスを提供することを含み得る。
【００３３】
[0034] いくつかの実装では、方法は、第２のコンフィギュレータデバイスに復号情報を提供することを含み得、復号情報は、第２のコンフィギュレータデバイスがコンフィギュレータ鍵パッケージの少なくとも一部分を復号することと、コンフィギュレータ秘密署名鍵を取得することとを可能にする。
【００３４】
[0035] いくつかの実装では、復号情報は、ストレージロケーションにおけるコンフィギュレータ鍵パッケージのロケーションアドレスと、コンフィギュレータ鍵パッケージの少なくとも一部分を復号するために使用可能な暗号鍵と、からなるグループから選択される少なくとも１つのメンバを含み得る。
【００３５】
[0036] いくつかの実装では、復号情報を提供することは、第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェース、からなるグループから選択される少なくとも１つのメンバを使用して復号情報を提供することを含み得る。
【００３６】
[0037] いくつかの実装では、復号情報を提供することは、復号情報が符号化されているイメージを表示することを含み得る。
【００３７】
[0038] いくつかの実装では、イメージは、バーコードまたはクイックレスポンス（ＱＲ）コードイメージであり得る。
【００３８】
[0039] いくつかの実装では、コンフィギュレータ公開検証鍵は、コンフィギュレータ秘密署名鍵から導出されるか、またはコンフィギュレータ鍵パッケージから取得され得る。コンフィギュレータ秘密署名鍵およびコンフィギュレータ公開検証鍵は、第１のネットワークの複数のコンフィギュレータ間で共有され得る。複数のコンフィギュレータの各々は、第１のネットワーク用にエンローリデバイスを構成するために、デバイスプロビジョニングプロトコルに従ってコンフィギュレータ秘密署名鍵およびコンフィギュレータ公開検証鍵を使用することが可能であり得る。

【００３９】
[0040] 本開示で説明されている主題の別の革新的な態様が、プロセッサと、命令を記憶したメモリとを含む、第１のコンフィギュレータデバイスに実装されることができる。命令は、プロセッサによって実行されると、第１のコンフィギュレータデバイスに、第１のコンフィギュレータデバイスに関連付けられた少なくともコンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成させ得る。命令は、プロセッサによって実行されると、第１のコンフィギュレータデバイスに、コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することと、第１のコンフィギュレータデバイスまたは第２のコンフィギュレータデバイスによる後のリストアのためのバックアップとして、ストレージロケーションにコンフィギュレータ鍵パッケージを記憶することと、を行わせ得る。

【００４０】
[0041] いくつかの実装では、命令は、プロセッサによって実行されると、第１のコンフィギュレータデバイスに、コンフィギュレータ秘密署名鍵とは異なる暗号化を使用してコンフィギュレータ鍵パッケージを暗号化することを行わせ得る。

【００４１】
[0042] いくつかの実装では、命令は、プロセッサによって実行されると、第１のコンフィギュレータデバイスに、秘密鍵暗号化技法を使用してコンフィギュレータ秘密署名鍵を暗号化することと、コンフィギュレータ鍵パッケージのヘッダ中に秘密鍵暗号化技法のインジケーションを含めることと、を行わせ得る。

【００４２】
[0043] いくつかの実装では、命令は、プロセッサによって実行されると、第１のコンフィギュレータデバイスに、コンフィギュレータ鍵パッケージと復号情報とを含むデジタルエンベロープを生成することを行わせ、復号情報は、第２のコンフィギュレータデバイスがコンフィギュレータ鍵パッケージの少なくとも一部分を復号することを可能にする。

【００４３】
[0044] いくつかの実装では、コンフィギュレータ鍵パッケージを記憶するための命令は、コンフィギュレータ鍵パッケージのバックアップを記憶するための命令を含む。命令は、プロセッサによって実行されると、第１のコンフィギュレータデバイスに、ストレージロケーションからコンフィギュレータ鍵パッケージのバックアップを検索することと、コンフィギュレータ鍵パッケージの少なくとも一部分を復号することと、コンフィギュレータ鍵パッケージからコンフィギュレータ秘密署名鍵を取得することと、を行わせる。

【００４４】
[0045] いくつかの実装では、命令は、プロセッサによって実行されると、第１のコンフィギュレータデバイスに、ストレージロケーションにおけるコンフィギュレータ鍵パッケージのロケーションアドレスを決定することと、第２のコンフィギュレータデバイスにロケーションアドレスを提供することと、を行わせ得る。

【００４５】
[0046] いくつかの実装では、命令は、プロセッサによって実行されると、第１のコンフィギュレータデバイスに、第２のコンフィギュレータデバイスに復号情報を提供することを行わせ得、復号情報は、第２のコンフィギュレータデバイスがコンフィギュレータ鍵パッケージの少なくとも一部分を復号することと、コンフィギュレータ秘密署名鍵を取得することとを可能にする。

【００４６】
[0047] いくつかの実装では、復号情報は、ストレージロケーションにおけるコンフィギュレータ鍵パッケージのロケーションアドレスと、コンフィギュレータ鍵パッケージの少なくとも一部分を復号するために使用可能な暗号鍵と、からなるグループから選択される少なくとも１つのメンバを含み得る。

【００４７】
[0048] いくつかの実装では、命令は、プロセッサによって実行されると、第１のコン

フィギュレータデバイスに、第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェース、からなるグループから選択される少なくとも１つのメンバを使用して復号情報を提供することを行わせ得る。

【００４８】

[0049]本開示で説明されている主題の別の革新的な態様は、命令を記憶するコンピュータ可読媒体に実装され得、命令は、第１のコンフィギュレータデバイスのプロセッサによって実行されると、第１のコンフィギュレータデバイスに、第１のコンフィギュレータデバイスに関連付けられた少なくともコンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成させ得る。命令は、第１のコンフィギュレータデバイスのプロセッサによって実行されると、コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することと、第１のコンフィギュレータデバイスまたは第２のコンフィギュレータデバイスによる後の検索のために、ストレージロケーションにおいてコンフィギュレータ鍵パッケージを記憶することと、を行わせ得る。

【００４９】

[0050] 本開示で説明される主題の別の革新的な態様は、第２のコンフィギュレータデバイスによって行われる方法に実装され得る。方法は、第２のコンフィギュレータデバイスにおいて、ストレージロケーションからコンフィギュレータ鍵パッケージを取得することと、ここにおいて、コンフィギュレータ鍵パッケージの少なくとも一部分は暗号化され、コンフィギュレータ鍵パッケージは、第１のコンフィギュレータデバイスに関連付けられた少なくともコンフィギュレータ秘密署名鍵を含み得る。方法は、コンフィギュレータ鍵パッケージの少なくとも部分を復号することと、コンフィギュレータ鍵パッケージからコンフィギュレータ秘密署名鍵を取得することと、デバイスプロビジョニングプロトコルに従って、コンフィギュレータ秘密署名鍵を利用して、ネットワーク用にエンローリデバイスをプロビジョニングすることと、を含み得る。

【００５０】

[0051] いくつかの実装では、方法は、第１のコンフィギュレータデバイスから復号情報を取得することを含み得、復号情報は、第２のコンフィギュレータデバイスがコンフィギュレータ鍵パッケージの少なくとも一部分を復号することを可能にする。

【００５１】

[0052] いくつかの実装では、復号情報は、ストレージロケーションにおけるコンフィギュレータ鍵パッケージのロケーションアドレスと、コンフィギュレータ鍵パッケージの少なくとも一部分を復号するために使用可能な暗号鍵と、からなるグループから選択される少なくとも１つのメンバを含み得る。

【００５２】

[0053] いくつかの実装では、復号情報を取得することは、第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェース、からなるグループから選択される少なくとも１つのメンバを使用して復号情報を取得することを含み得る。

【００５３】

[0054] いくつかの実装では、復号情報を取得することは、第２のコンフィギュレータデバイスに関連付けられたカメラを介して、復号情報が符号化されているイメージを取得することと、復号情報を検索するためにイメージを復号することと、を含み得る。

【００５４】

[0055] 本開示で説明される主題の１つまたは複数の実装の詳細が、添付の図面および以下の説明に記載されている。他の特徴、様態、および利点が、説明、図面、および特許請求の範囲から明らかになるだろう。下記の図面の相対的な寸法は、原寸通りに描かれていない可能性があることに留意されたい。

【図面の簡単な説明】

【００５５】

【図１】図１は、複数のコンフィギュレータを有するデバイスプロビジョニングプロトコルの概念を紹介するための例示的なシステム図を示す。
【図２】図２は、デバイスプロビジョニングプロトコルの例示的なメッセージフロー図を示す。
【図３】図３は、コンフィギュレータ鍵を記憶する第１のコンフィギュレータデバイスに関する例示的なフローチャートを示す。
【図４】図４は、第１のコンフィギュレータデバイスによるコンフィギュレータ鍵のリストアおよびバックアップを説明するための、例示的なシステム図を示す。
【図５】図５は、第１のコンフィギュレータデバイスから第２のコンフィギュレータデバイスへのコンフィギュレータ鍵を共有することを説明するための例示的なシステム図を示す。
【図６】図６は、複数のコンフィギュレータを有するデバイスプロビジョニングプロトコルの例示的なメッセージフロー図を示す。
【図７】図７は、第１のコンフィギュレータデバイスを動作させるための例示的なフローチャートを示す。
【図８】図８は、第２のコンフィギュレータデバイスを動作させるための例示的なフローチャートを示す。
【図９】図９は、コンフィギュレータ鍵をバックアップおよびリストアするためにコンフィギュレータデバイスを動作させるための例示的なフローチャートを示す。
【図１０】図１０は、本開示の態様を実装するための例示的な電子デバイスのブロック図を示す。
【発明の詳細な説明】
【００５６】
[0066] 様々な図面における同様の参照番号および呼称は、同様の要素を示す。
【００５７】
[0067] 下記の説明は、本開示の革新的な態様を説明することを目的として、ある特定の実装を対象としている。しかしながら、当業者は、本明細書における教示が多数の異なる方法で適用される得ることを容易に認識するだろう。説明される実装は、米国電気電子学会（ＩＥＥＥ）１６．１１規格のうちの任意のもの、またはＩＥＥＥ８０２．１１規格のうちの任意のもの、Ｂｌｕｅｔｏｏｔｈ（登録商標）規格、符号分割多元接続（ＣＤＭＡ）、周波数分割多元接続（ＦＤＭＡ）、時分割多元接続（ＴＤＭＡ）、モバイル通信のためのグローバルシステム（ＧＳＭ（登録商標））、ＧＳＭ／汎用パケット無線サービス（ＧＰＲＳ）、エンハンストデータＧＳＭ環境（ＥＤＧＥ）、地上基盤無線（ＴＥＴＲＡ）、ワイドバンドＣＤＭＡ（Ｗ－ＣＤＭＡ（登録商標））、エボリューションデータオプティマイズド（ＥＶ－ＤＯ）、１ｘＥＶ－ＤＯ、ＥＶ－ＤＯ Ｒｅｖ Ａ、ＥＶ－ＤＯ Ｒｅｖ Ｂ、高速パケットアクセス（ＨＳＰＡ）、高速ダウンリンクパケットアクセス（ＨＳＤＰＡ）、高速アップリンクパケットアクセス（ＨＳＵＰＡ）、発展型高速パケットアクセス（ＨＳＰＡ＋）、ロングタームエボリューション（ＬＴＥ（登録商標））、ＡＭＰＳにしたがう無線周波数（ＲＦ）信号、あるいは、３Ｇ、４Ｇ、または５Ｇ、もしくはそれらのさらなる実装の技術を利用するシステムのようなワイヤレス、セルラまたはモノのインターネット（ＩＯＴ）ネットワーク内で通信するために使用される他の知られている信号を送信および受信することが可能な任意のデバイス、システムまたはネットワークにおいて実装され得る。
【００５８】
[0068] 上述されたように、デバイスプロビジョニングプロトコル（Ｗｉ－ＦｉデバイスプロビジョニングプロトコルなどのＤＰＰ）は、ネットワークに導入されるエンローリデバイスの構成を容易にし得る。例えば、ＤＰＰは、エンローリデバイスとコンフィギュレータデバイスとの間の認証および認証キー確立を提供し得る。いくつかの実装では、ＤＰＰは、認証プロトコルに通常使用されるよりも少ないメッセージを使用する。例えば、ＤＰＰ認証プロトコルは、第１の認証のために、およびさらなるプロビジョニングの前に

エフェメラルプロトコル鍵（ephemeral protocol key）を生成するために、「ブートストラップされた（bootstrapped）」公開鍵を使用し得る。ブートストラッピング（bootstrapping）は、公開鍵を取得するための信頼された帯域外技法の使用を指す。帯域外技法は、（複数の）デバイスの近接性に基づいた信頼の度合いを提供する。例えば、ブートストラッピングは、第２のデバイスに表示される（または、第２のデバイスに付加される）イメージをスキャンおよび復号（decode）するために、第１のデバイス上のカメラの使用を含む。

【００５９】

[0069] ＤＰＰでは、コンフィギュレータデバイスは、エンローリのセットアップをサポートすることを担う。通常、ブートストラッピング鍵は、コンフィギュレータデバイスと新規のエンローリとの間の第１の認証のために使用され得る。その認証が完了した後、コンフィギュレータデバイスは、ネットワークを介して通信するためにエンローリをプロビジョニングし得る。プロビジョニングの一部として、コンフィギュレータデバイスは、エンローリがネットワーク中の他のピアとセキュアなアソシエーションを確立することを可能にする。コンフィギュレータ鍵は、「コネクタ」（「構成オブジェクト」とも呼ばれ得る）を生成するために、コンフィギュレータデバイスによって使用される。コネクタは、エンローリの構成を搬送し、かつエンローリデバイスとピアデバイス（アクセスポイントまたはピア・ツー・ピアの隣接機器など）との間の接続を許可する（authorize）。コンフィギュレータ鍵は、コンフィギュレータ秘密署名鍵（「ｃ－ｓｉｇｎ－ｋｅｙ」とも呼ばれ得る）と、コンフィギュレータ公開検証鍵（「Ｃ－ｓｉｇｎ－ｋｅｙ」とも呼ばれ得る）とで構成されている署名鍵ペアを含む。コンフィギュレータ秘密署名鍵（ｃ－ｓｉｇｎ－ｋｅｙ）は、コネクタに署名するコンフィギュレータによって使用され、一方コンフィギュレータ公開検証鍵（Ｃ－ｓｉｇｎ－ｋｅｙ）は、同じコンフィギュレータによって署名される他のデバイスのコネクタを検証するプロビジョニングされたデバイスによって使用される。以下でさらに説明されるように、コンフィギュレータ鍵は、数学的に対応しており、コンフィギュレータデバイスによって署名されたメッセージの信頼性を検証するために使用され得る。各コネクタは、コンフィギュレータデバイスのコンフィギュレータ秘密署名鍵を使用して署名され得る。コンフィギュレータデバイスは、コンフィギュレータデバイスが構成する各エンローリに対し１つまたは複数のコネクタを作成し得る。コネクタがコンフィギュレータデバイスのコンフィギュレータ秘密署名鍵を使用して署名された後、コネクタは、ネットワーク中の任意のピアによって検証され得る。例えば、コンフィギュレータ公開検証鍵は、コンフィギュレータ秘密署名鍵を使用して署名されたコネクタの信頼性を検証するために使用され得る。コンフィギュレータ鍵はデバイスプロビジョニングプロトコルの基本的態様であり得るため、コンフィギュレータ鍵がバックアップとしてセキュアに記憶され得るか、別のコンフィギュレータデバイスと共有され得る状況が存在し得る。

【００６０】

[0070] 一態様では、コンフィギュレータデバイスは、コンフィギュレータ鍵のセキュアなバックアップとしてコンフィギュレータ鍵パッケージを準備し得る。コンフィギュレータ鍵パッケージは、後のリストアのためのバックアップとして記憶され得る。例えば、コンフィギュレータ鍵パッケージは、コンフィギュレータデバイスおよびもしかすると他のコンフィグレーションデバイスによってアクセス可能なロケーションにエクスポートされ得る。別の態様では、複数のコンフィギュレータデバイスは、同じ（複数の）コンフィギュレータ鍵を共有することができる。例えば、コンフィギュレータ鍵は、第２のコンフィギュレータデバイスが当該コンフィギュレータ鍵を使用することができるように、第２のコンフィギュレータデバイスと共有され得る。仮説的シナリオとして、二人のルームメイトが住居を共有しており、ゲストエンローリデバイスを構成するように各ルームメイトがコンフィギュレータデバイス（彼ら個人の携帯電話など）を動作する例が考えられる。本開示で説明される実装は、（複数の）コンフィギュレータ鍵が複数のコンフィギュレータデバイスによって使用されることができるように、デバイスプロビジョニングプロトコ

ルを拡張する。

【００６１】

[0071] 第１のコンフィギュレータデバイスは、当該第１のコンフィギュレータデバイスに関連付けられた少なくとも１つのコンフィギュレータ秘密署名鍵を含む、１つのコンフィギュレータ鍵パッケージを生成し得る。コンフィギュレータ鍵パッケージはまた、コンフィギュレータ秘密署名鍵に関連付けられたコンフィギュレータ公開検証鍵を含み得る。第１のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化し、そして第１のコンフィギュレータデバイスまたは第２のコンフィギュレータデバイスによる後の検索のために、ストレージロケーションにコンフィギュレータ鍵パッケージを記憶することができる。コンフィギュレータ鍵パッケージは、第１のコンフィギュレータデバイスから第２のコンフィギュレータデバイスに共有されることができる暗号鍵を使用して暗号化され得る。いくつかの実装では、デバイスプロビジョニングプロトコルは、エンローリデバイスの公開ブートストラップ鍵を取得するためにブートストラッピングを使用する。同様のブートストラッピング技法は、コンフィギュレータデバイス間の暗号鍵を共有するために使用され得る。ブートストラッピングは、帯域外技法がピアデバイスとの近接性または物理的アソシエーションを伴うため、暗号鍵における信頼を提供する。

【００６２】

[0072] 本開示で説明される主題の特定の実装は、下記の潜在的な利点のうちの１つまたは複数を実現するように実装され得る。本開示における実装を使用して、デバイスプロビジョニングプロトコルは、コンフィギュレータ鍵のバックアップ／リストアまたはエクスポート／インポートをサポートし得る。いくつかの実装では、デバイスプロビジョニングプロトコルは、１つのネットワークのために複数のコンフィギュレータデバイスを有することで恩恵を受け得る。複数のコンフィギュレータデバイスは、同じ共有された（複数の）コンフィギュレータ鍵を使用することができ、それらはネットワークのために構成されたピア間の互換性を改善し得る。例えば、どのコンフィギュレータデバイスが当該ネットワーク用にエンローリデバイスを構成したかにかかわらず、コネクタは、同じコンフィギュレータ鍵を使用して署名および検証され得る。本開示におけるコンフィギュレータ鍵を共有するための技法は、各コンフィギュレータデバイスに対する異なるコンフィギュレータ鍵に依存するアプローチと比較すると、より多くのコンフィギュレータデバイスをデバイスプロビジョニングプロトコルに追加するためのスケーラブルかつ複雑性の低いアプローチを提供し得る。コンフィギュレータ鍵を記憶または共有するためのセキュアなストレージフォーマットを定義することによって、デバイスプロビジョニングプロトコルは、コンフィギュレータデバイス間で高まる相互運用性からの恩恵を受ける。

【００６３】

[0073] 図１は、複数のコンフィギュレータを有するデバイスプロビジョニングプロトコルの概念を紹介するための例示的なシステム図を示す。例示的なシステム１００は、第１のコンフィギュレータデバイス１１０、第２のコンフィギュレータデバイス１２０、およびエンローリデバイス１５０Ａおよび１５０Ｂを含む。エンローリデバイスは、第１のコンフィギュレータデバイス１１０または第２のコンフィギュレータデバイス１２０のいずれかによって管理されるネットワーク中で使用するために未だ構成されていないデバイスの任意のタイプであり得る。第１のコンフィギュレータデバイス１１０は、コンフィギュレータ秘密署名鍵およびコンフィギュレータ公開検証鍵を含む一対のコンフィギュレータ鍵を有し得る。コンフィギュレータ秘密署名鍵は、デジタルで署名されたメッセージを作成するために使用され得る。コンフィギュレータ公開検証鍵は、デジタルで署名されたメッセージがコンフィギュレータ秘密署名鍵を使用して署名されたことを検証するために使用され得る。

【００６４】

[0074] 図１で示されるように、第１のコンフィギュレータデバイス１１０は、ネットワーク中での使用のためにエンローリデバイス１５０Ａを構成するようにデバイスプロビ

ジョニングプロトコルを実施し得る（矢印１５８として示される）。複数のコンフィギュレータデバイスとともにデバイスプロビジョニングプロトコルを使用するために、第１のコンフィギュレータデバイス１１０は、その一対のコンフィギュレータ鍵を、第２のコンフィギュレータデバイス１２０と共有する（矢印１５２として示される）。以下でさらに説明されるように、コンフィギュレータ鍵は、第２のコンフィギュレータデバイス１２０に直接送信され得ない。むしろ、第１のコンフィギュレータデバイス１１０がコンフィギュレータ鍵パッケージを生成し得る。コンフィギュレータ鍵パッケージのいくつかまたは全てのコンテンツは、暗号鍵を使用して暗号化され得る。コンフィギュレータ鍵パッケージは、第２のコンフィギュレータデバイス１２０によってアクセス可能なネットワーク中のロケーションにエクスポートされ得る。いくつかの実装では、第１のコンフィギュレータデバイス１１０は、第２のコンフィギュレータデバイス１２０がコンフィギュレータ鍵パッケージを取得および復号することができるように、第２のコンフィギュレータデバイス１２０に復号情報を提供し得る。例えば、復号情報は、コンフィギュレータ鍵パッケージが記憶されるロケーションアドレスを含み得る。いくつかの実装では、復号情報は、暗号鍵を含み得る。復号情報は、エンローリデバイスの公開ブートストラップ鍵を取得するためにコンフィギュレータデバイスによって使用される同様のブートストラッピング技法を使用して提供され得る。ブートストラッピング技法は、図２の説明においてより詳細に説明される。いくつかの他の実装では、復号情報は、コンフィギュレータ鍵パッケージを復号するために、第２のコンフィギュレータデバイス１２０にマニュアルで入力され得るパスフレーズまたは他の情報を含み得る。

【００６５】

[0075] 一旦第２のコンフィギュレータデバイス１２０が復号情報およびコンフィギュレータ鍵パッケージを取得すると、第２のコンフィギュレータデバイス１２０は、（暗号鍵などを使用して）コンフィギュレータ鍵パッケージを復号し、コンフィギュレータ鍵を検索することができる。第２のコンフィギュレータデバイス１２０は、コンフィギュレータ鍵を記憶し、他のエンローリデバイスを構成するとき、共有されたコンフィギュレータ鍵を使用することができる。例えば、第２のコンフィギュレータデバイス１２０は、エンローリデバイス１５０Ｂを構成するために、デバイスプロビジョニングプロトコルを実施し得る（矢印１５４として示される）。エンローリデバイス１５０Ａおよび１５０Ｂが異なるコンフィギュレータデバイスで構成されたとしても、エンローリデバイス１５０Ａおよび１５０Ｂの各々は、（これらがネットワークを介して通信することを許可する）署名されたコネクタを、同じコンフィギュレータ公開検証鍵を使用して検証し得る。

【００６６】

[0076] 図２は、デバイスプロビジョニングプロトコルの例示的なメッセージフロー図を示す。図２のＤＰＰ２００は、一対のデバイス、エンローリデバイス２５０とコンフィギュレータデバイス２１０との間のものである。ＤＰＰ２００は、ブートストラッピング技法、ＤＰＰ認証、およびＤＰＰ構成の３つのオペレーションを含む。ＤＰＰ認証は、（下記でさらに説明されるもののような）ブートストラッピング技法を通じて取得されている認証パーティのブートストラッピング鍵（authenticating party’s bootstrapping key）に依存する。

【００６７】

[0077] ブートストラッピングは、別のデバイスから共有鍵を取得するための帯域外技法を指す。エンローリデバイス２５０およびコンフィギュレータデバイス２１０の各々は、初期認証に関しておよび一時的プロビジョニング鍵（temporary provisioning key）を生成することに関して信頼された公開ブートストラップ鍵（「公開アイデンティティ鍵」と呼ばれることもある）を有し得る。ブートストラッピングは、公開ブートストラップ鍵を共有するために使用され得る様々な技法のうちの１つである。例えば、ブートストラッピングは、公開ブートストラップ鍵を符号化するクイックレスポンス（登録商標）（ＱＲ）コードをスキャンすることを含み得る。認証のこの形式に関するサポートは、ユーザインターフェースを欠いているある特定のデバイス（ＩＯＴデバイス、ウェアラブルアクセ

サリ、ホームオートメーションデバイスなど）が、コンフィギュレータデバイスを用いて認証されることを可能にする。

【００６８】

[0078] ２０５において、コンフィギュレータデバイス２１０は、エンローリデバイス２５０からエンローリブートストラッピングデータを取得し得る。例えば、エンローリデバイス２５０は、それにプリントされた（またはパッケージング上にプリントされた、またはパッケージングに挿入された）ビジュアルタグを有し得る。そのビジュアルタグは、バーコード、マトリックスコード、二次元コードなどであり得る。バーコードの一般的な例は、ＱＲコード（登録商標）であり得る。コンフィギュレータデバイス２１０は、カメラおよび対応するソフトウェアを使用してバーコード（または同様のビジュアルタグ）を検出し得る。コンフィギュレータデバイス２１０は、そのバーコードを復号することによって、エンローリブートストラッピングデータを取得し得る。１つの実施形態では、エンローリブートストラッピングデータは、エンローリデバイス２５０のための公開ブートストラップ鍵を含み得る。公開ブートストラップ鍵に加えて、他の情報もまた、エンローリブートストラッピングデータに含まれ得る。例えば、エンローリブートストラッピングデータは、公開ブートストラップ鍵、並びに、グローバルオペレーティングクラス（Global Operating Class）およびチャネルナンバリスト（Channel Number list）を含み得る。グローバルオペレーティングクラスおよびチャネルナンバリストは、どの無線パラメータまたはどの（1つまたは複数の）ワイヤレスチャネルを、エンローリデバイス２５０がＤＰＰ認証のために使用するかを決定するために使用され得る。例えば、グローバルオペレーティングクラスおよびチャネルナンバリストは、共に（together）、エンローリデバイス２５０がＤＰＰ認証リクエストメッセージをリッスンする（または送る）ワイヤレスチャネルはどれであるかを示し得る。２０７において、いくつかの実装では、エンローリデバイス２５０はまた、コンフィギュレータデバイス２１０からコンフィギュレータブートストラッピングデータを取得し得る。両方のパーティが互いのブートストラッピングデータを取得したとき、ＤＰＰ認証は、相互の双方向性認証を利用することができる。

【００６９】

[0079] 図２で示されるブートストラッピングデータ技法に加えて、様々な他のブートストラッピング技法が使用され得る。ブートストラッピング技法は、ブートストラッピングデータが特定のデバイスに属することを受信側が信頼することを可能にする。図１で説明されるように、（ＱＲコードなどの）２次元マトリックスコードをスキャンすることは、ブートストラッピングデータを取得するための１つの技法である。バーコードをスキャンすることの代替として、コンフィギュレータデバイス２１０が近隣認識ネットワーキング（ＮＡＮ：Neighbor-Aware Networking）（図示せず）を使用し得る。ＮＡＮは、デバイス間のアソシエーションを用いることなく、ワイヤレス媒体上で発見能力およびサービス情報交換を提供する。別のブートストラッピング技法は、転送されたコンテンツのインテグリティのためにある一定の信頼性を提供することができる他の媒体上でブートストラッピングデータを転送するものである。例えば、いくつかの実装では、ブートストラッピングは、ユニバーサルシリアルバス（ＵＳＢ）、近距離通信（ＮＦＣ）、または短距離無線通信（Ｂｌｕｅｔｏｏｔｈ（登録商標）通信など）の使用を含み得る。さらに別のブートストラッピング技法は、共有されたコード／キー／フレーズ／ワード（以下、「コード」）を用いてブートストラッピングデータをマスクするものであり、ブートストラッピング鍵をアンマスクするための共有されたコードの知識に依存する。ピアが、共有されたコードを知っておりかつそれを使用することができると証明することが可能な場合、そのピアのブートストラッピングデータは信頼され得る。

【００７０】

[0080] ＤＰＰ認証段階は、コンフィギュレータおよびエンローリを強固に認証するために、ブートストラッピング技法を使用して取得されたブートストラッピングデータを使用する。ＤＰＰ認証段階は、３つのメッセージ交換からなり、共有秘密鍵および認証鍵を生成する。２１５において、コンフィギュレータデバイス２１０は、第１のナンス（nonc

e）を生成し、プロトコル鍵ペアを生成し、エンローリ公開ブートストラップ鍵のハッシュ関数を実行し、ハッシュされたブートストラップデータから導出される共有秘密に基づいて第１の対称鍵（symmetric key）を生成する。コンフィギュレータデバイス２１０は、チャネルリスト中の1つまたは複数のチャネルを介して、ＤＰＰ認証リクエストメッセージ２１７を送る。ＤＰＰ認証リクエストメッセージ２１７は、共有秘密、および第１の対称鍵によって暗号化された第１のノンスを含み得る。

【００７１】

[0081] エンローリデバイス２５０は、ＤＰＰ認証リクエストメッセージ２１７を受信する。２２５において、エンローリデバイス２５０は、その公開ブートストラップ鍵のハッシュがメッセージ中にあるかどうかをチェックする。その公開ブートストラップ鍵のハッシュがメッセージ中にある場合、エンローリデバイス２５０は、共有秘密を生成し、第１の対称鍵を導出する。エンローリデバイス２５０は、第１の対称鍵を使用して第１のノンスをアンラップ（unwrap）しようと試みる。次に、エンローリデバイス２５０は、第２のノンス、共有秘密、および第２の対称鍵を生成する。エンローリデバイス２５０は、２つのノンスとその能力を第１の対称鍵中にラップ(wrap)し、認証タグを第２の対称鍵にラップする。エンローリデバイス２５０は次いで、そのパブリックブートストラッピング鍵のハッシュ（および、オプションで、それが相互認証を行う場合、コンフィギュレータ公開ブートストラッピング鍵のハッシュを含む）、その公開プロトコル鍵、ラップされたノンスおよびそのラップされたネットワーク公開鍵、およびラップされた認証タグを、ＤＰＰ認証応答メッセージ２２７に置く。ＤＰＰ認証応答メッセージ２２７は、コンフィギュレータデバイス２１０に送信される。

【００７２】

[0082] 応答を成功裏に受信した後、コンフィギュレータデバイス２１０は、２３５において、結果を確証し（validate）、ＤＰＰ認証段階を完了させるために、ＤＰＰ認証確認メッセージ２３７を送信する。これらのフレーム交換が成功裏に完了した後、イニシエータ／コンフィギュレータとレスポンダ／エンローリとの間のセキュアチャネルが、２４５において確立される。

【００７３】

[0083] ＤＰＰ認証が完了した後、コンフィギュレータデバイス２１０は、デバイス・ツー・デバイス通信またはインフラストラクチャ通信のために、エンローリデバイス２５０をプロビジョニングする。プロビジョニングの一部として、コンフィギュレータデバイス２１０は、エンローリデバイス２５０がネットワーク中の他のピアとセキュアなアソシエーションを確立することを可能にする。

エンローリデバイス２５０は、ＤＰＰ構成リクエストメッセージ２６３を送信することによって構成段階を開始し、ＤＰＰ構成応答メッセージ２６７中の構成情報を用いてプロビジョニングされる。ＤＰＰ構成応答メッセージ２６７を成功裏に受信した後、エンローリデバイス２５０は、ネットワークへのセキュアアクセスを確立するために使用可能な構成情報を用いてプロビジョニングされる。

【００７４】

[0084] いくつかの実装では、コンフィギュレータデバイス２１０はまた、ワイヤレスローカルエリアネットワーク（ＷＬＡＮ）のアクセスポイントであり得る。代替的に、コンフィギュレータデバイス２１０は、アクセスポイントから離されていることがある。例えば、コンフィギュレータデバイス２１０によって提供された構成情報は、アクセスポイント２８０とのセキュアなワイヤレス接続を確立するために、エンローリデバイス２５０によって使用され得る。別の態様では、コンフィギュレータデバイス２１０は、ピア・ツー・ピア（Ｐ２Ｐ）グループオーナーまたはＰ２Ｐグループメンバであり得る。

【００７５】

[0085] ＤＰＰ構成段階の終わりに、コンフィギュレータデバイス２１０は、コネクタを形成し得る（矢印２７７によって表される）。コネクタは、ネットワーク上の他のデバイスがエンローリデバイス２５０と通信するために許可されたという、信頼されたステー

トメントを、エンローリデバイス２５０が獲得することを可能にする、署名された導入部（introduction）である。各コネクタは、グループ識別子、ネットワークロール、およびネットワークアクセスプロビジョニングキーのタプル(tuple)を含み得、全てがコンフィギュレータデバイスのコンフィギュレータ秘密署名鍵を使用して署名される。識別子は、特定のピア、あるいは、全てのピアを示すワイルドカードを示すことができる。上述されるように、コネクタは、コンフィギュレータデバイス２１０のコンフィギュレータ秘密署名鍵（ｃ－ｓｉｇｎ－ｋｅｙ）によって署名され、コンフィギュレータデバイス２１０のコンフィギュレータ公開検証鍵（Ｃ－ｓｉｇｎ－ｋｅｙ）を使用して検証され得る。

【００７６】

[0086]コンフィギュレータデバイス２１０がアクセスポイント２８０から離れている場合、エンローリデバイス２５０は、アクセスポイント２８０とのワイヤレスアソシエーション２８７のための信用証明（credentials）として、コネクタおよび構成情報を使用することができる。エンローリデバイス２５０は、アクセスポイント２８０を発見し、ピア発見リクエストフレーム（図示せず）を送信し、次いで、ピア発見リクエストフレーム（図示せず）を待ち得る。ピア発見フレームの成功裏の検証(validation)の際に、エンローリデバイス２５０およびアクセスポイント２８０は、ＰＭＫ（pairwise master key）を相互に導出し、通常のＩＥＥＥ８０２．１１プロシージャにしたがう。例えば、４－ｗａｙハンドシェイクプロシージャは、アクセスポイント２８０とのエンローリデバイス２５０の認証およびワイヤレスアソシエーションを完了させるために、エンローリデバイス２５０とアクセスポイント２８０との間で行われ得る。ＰＭＫ（pairwise master key）は、後続のＷＰＡ（Wi-Fi（登録商標） Protected Access）ハンドシェイクおよび構成メッセージのために使用され得る。代替的に、アクセスポイント２８０がレガシアクセスポイントである場合、構成情報は、エンローリデバイス２５０がアクセスポイント２８０に接続することを可能にするために、ＰＳＫ（pre-shared key）またはＰＳＫパスフレーズ信用情報（passphrase credential）を含み得る。この実装では、エンローリデバイス２５０は、ＩＥＥＥ８０２．１１およびＷＰＡ２パーソナルネットワークアクセスプロシージャを使用してＡＰを発見しかつＡＰとアソシエートするために、構成情報を使用するだろう。

【００７７】

[0087] 図３は、コンフィギュレータ鍵を記憶する第１のコンフィギュレータデバイスに関する例示的なフローチャートを示す。フローチャート３００は、ブロック３１０において開始する。ブロック３１０において、第１のコンフィギュレータデバイスは、少なくとも、第１のコンフィギュレータデバイスに関連付けられたコンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成し得る。いくつかの実装では、コンフィギュレータ鍵パッケージはコンフィギュレータ秘密署名鍵およびコンフィギュレータ公開検証鍵の両方を含み得る。

【００７８】

[0088] ブロック３２０において、第１のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化し得る。例えば、コンフィギュレータ鍵パッケージは、コンフィギュレータ秘密署名鍵とは異なる暗号鍵を使用して暗号化され得る。いくつかの実装では、第１のコンフィギュレータデバイスは、秘密鍵暗号化技法を使用してコンフィギュレータ秘密署名鍵（および、オプションで、コンフィギュレータ公開検証鍵）を暗号化し得る。いくつかの実装では、コンフィギュレータ鍵パッケージは、コンフィギュレータ鍵パッケージを準備するために使用されるストラクチャ、コンテンツ、または暗号化技法を記述するヘッダを含み得る。

【００７９】

[0089] ブロック３３０において、第１のコンフィギュレータデバイスは、第１のコンフィギュレータデバイスまたは第２のコンフィギュレータデバイスによる後のリストアのために、バックアップとして、ストレージロケーションにコンフィギュレータ鍵パッケージを記憶し得る。例えば、ストレージロケーションは、第１のコンフィギュレータデバイ

スのメモリ、ネットワーク共有ロケーション、パーソナルコンピュータ、ホームサーバ、クラウドベースのストレージサービス、およびワイヤレスネットワークのアクセスポイント（ＡＰ）であり得る。

【００８０】

[0090] コンフィギュレータ鍵パッケージが記憶された後、記憶されたコンフィギュレータ鍵パッケージを使用するための異なる方法が存在する。例えば、ブロック３４０において、第１のコンフィギュレータデバイスは、ストレージロケーションからコンフィギュレータ鍵パッケージのバックアップを検索し得る。第１のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージを復号し、コンフィギュレータ鍵パッケージからコンフィギュレータ秘密署名鍵を取得し得る。別の例では、ブロック３５０において、第１のコンフィギュレータデバイスは、第２のコンフィギュレータデバイスに復号情報を提供し得る。復号情報は、第１のコンフィギュレータデバイスによって暗号化されたコンフィギュレータ鍵パッケージの少なくとも一部分を、第２のコンフィギュレータデバイスが復号することを可能にし得る。第２のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージからコンフィギュレータ秘密署名鍵を取得し得る。コンフィギュレータ鍵パッケージが、コンフィギュレータ公開検証鍵を含む場合、第２のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージからコンフィギュレータ公開検証鍵をリストアすることができる。コンフィギュレータ鍵パッケージがコンフィギュレータ公開検証鍵を含まない場合、第２のコンフィギュレータデバイスは、コンフィギュレータ秘密署名鍵に少なくとも部分的に基づいて、コンフィギュレータ公開検証鍵を決定し得る。

【００８１】

[0091] 図４は、第１のコンフィギュレータデバイスによるコンフィギュレータ鍵のリストアおよびバックアップを説明するための、例示的なシステム図を示す。例示的なシステム４００は、第１のコンフィギュレータデバイス１１０およびストレージロケーション４１０を含む。第１のコンフィギュレータデバイス１１０は、コンフィギュレータ鍵４１２を有し、暗号化技法４１６を使用して、コンフィギュレータ鍵４１２の少なくとも一部分を暗号化することを可能にする。本開示の実装に容易に適合し得る様々な暗号化技法が存在し得る。異なる暗号化技法の例が、以下にさらに説明される。

【００８２】

[0092] 第１のコンフィギュレータデバイス１１０は、コンフィギュレータ鍵４１２を含むコンフィギュレータ鍵パッケージ４２７を生成し、暗号化技法４１６を使用して少なくとも部分的に暗号化されている（中括弧で示される）。第１のコンフィギュレータデバイス１１０はまた、バックアップ／リストアモジュール４５５を有する。バックアップ／リストアモジュール４５５は、コンフィギュレータ鍵パッケージ４２７が、ストレージロケーション４１０に記憶されることを行わせ得る（矢印４６７で示される）。例えば、コンフィギュレータ鍵パッケージ４２７を記憶するための動作は、バックアップと呼ばれ得る。

【００８３】

[0093] コンフィギュレータ鍵パッケージ４２７が記憶された後、バックアップ／リストアモジュール４５５は、コンフィギュレータ鍵をリストアすることを可能にし得る。バックアップ／リストアモジュール４５５は、ストレージロケーション４１０からコンフィギュレータ鍵パッケージ４２７を検索し得る（矢印４７７で示される）。例えば、バックアップ／リストアモジュール４５５は、ストレージロケーション４１０からコンフィギュレータ鍵パッケージ４２７にアクセスし得るか、またはそれをダウンロードし得る。バックアップ／リストアモジュール４５５は、暗号化技法を逆にし（reversing）、コンフィギュレータ鍵パッケージ４２７からコンフィギュレータ鍵を取得することによって、コンフィギュレータ鍵をリストアし得る。

【００８４】

[0094] 図５は、第１のコンフィギュレータデバイスから第２のコンフィギュレータデバイスへのコンフィギュレータ鍵を共有することを説明するための例示的なシステム図を

示す。例示的なシステム５００は、第１のコンフィギュレータデバイス１１０、第２のコンフィギュレータデバイス１２０、およびストレージロケーション４１０を含み得る。ストレージロケーション４１０は、ネットワーク共有メモリ、ネットワークドライブ、アクセスポイントのリソース、クラウドベースのストレージロケーション、または通信ネットワークを介して第２のコンフィギュレータデバイス１２０によってアクセス可能な任意の他のリソースであり得る。上述されるように、第１のコンフィギュレータデバイス１１０は、コンフィギュレータ鍵４１２を有し、それは、コンフィギュレータ秘密署名鍵およびコンフィギュレータ公開検証鍵を含み得る。第２のコンフィギュレータデバイス１２０にコンフィギュレータ鍵を提供するために、第１のコンフィギュレータデバイス１１０は、コンフィギュレータ鍵パッケージ４２７中にコンフィギュレータ鍵をエクスポートし得る。５１７で表されるように、第１のコンフィギュレータデバイス１１０は、コンフィギュレータ鍵を（暗号鍵を使用して）暗号化し、コンフィギュレータ鍵パッケージ４２７を作成し得る。

【００８５】

[0095] いくつかの実装では、第１のコンフィギュレータデバイス１１０は、公開鍵暗号法規格（ＰＫＣＳ：Public-Key Cryptography Standards）と呼ばれる規格のファミリに従って、コンフィギュレータ鍵パッケージを生成し得る。例えば、ＰＫＣＳ＃８は、規格のうちの１つであり、秘密鍵情報を記憶するために標準シンタックス（standard syntax）を定義する。ＰＣＫＳ＃８における暗号化は、デジタルエンベロープを特定し、それは（構成についての情報を有する）非対称鍵パッケージ（Asymmetric Key Package）および暗号鍵からなる。暗号鍵は、鍵管理、鍵アグリーメント（Key agreement）、共有されたパスワードを用いて導出される対称鍵、または共有された情報を通じた対称鍵暗号化のいずれかを使用して保護されることができる。よって、暗号鍵を導出することができるデバイスのみがコンフィギュレータ鍵パッケージを復号することができる。１つの実装では、第１のコンフィギュレータデバイス１１０は、任意のコンフィギュレータデバイスが（ＰＫＣＳ＃８ ｂｌｏｂの形式で）ストレージロケーション４１０からコンフィギュレータ鍵パッケージ４２７を取得することができるように、ネットワークにおける公開コネクタプロファイル（public connector profile）を作成し得る。

【００８６】

[0096] 公開コネクタプロファイルは、例えば、コンフィギュレータ鍵パッケージがダウンロードされ得るストレージロケーション４１０のための、ユニフォームリソースロケータ（ＵＲＬ）またはユニフォームリソース識別子（ＵＲＩ）などのロケーションアドレスを含み得る。コンフィギュレータ鍵パッケージは複数のデバイスによってアクセス可能であり得るが、許可されたコンフィギュレータデバイスのみ（第２のコンフィギュレータデバイス１２０など）がコンフィギュレータ鍵パッケージを復号するのに必要とされる復号情報を有しているだろう。例えば、復号情報は、コンフィギュレータ鍵パッケージに関連付けられたデジタルエンベロープから暗号鍵を導出するための共有されたパスワードであり得る。代替的に、復号情報は、コンフィギュレータ鍵パッケージを暗号化するために使用される暗号鍵をデバイスが取得するための任意の他の手段であり得る。別の実装では、ロケーションアドレスは、許可されたコンフィギュレータにのみ提供される秘密として維持される。５４７において、コンフィギュレータ鍵パッケージ４２７は、後の検索のためにストレージロケーション４１０に記憶される。いくつかの実装では、第１のコンフィギュレータデバイス１１０は、ネットワークを介して、コンフィギュレータ鍵パッケージ４２７を第２のコンフィギュレータデバイス１２０に送り、コンフィギュレータ鍵パッケージ４２７が、第２のコンフィギュレータデバイス１２０においてコロケートされたストレージロケーションに記憶されるようにし得る。

【００８７】

[0097] 第２のコンフィギュレータデバイス１２０は、第１のコンフィギュレータデバイス１１０から復号情報を取得し得る（矢印５３７によって表される）。いくつかの実装では、復号情報は、コンフィギュレータ鍵パッケージを復号するのに必要とされる暗号鍵

を含み得る。いくつかの実装では、復号情報は、コンフィギュレータ鍵パッケージがストレージロケーション４１０中のどこに記憶されるかを示すロケーションアドレスを含み得る。第１のコンフィギュレータデバイス１１０が第２のコンフィギュレータデバイス１２０に復号情報を提供するための様々な方法―ブートストラッピングを含む―が存在し得る。例えば、暗号鍵は、第２のコンフィギュレータデバイス１２０によってスキャンされることができるバーコードイメージに符号化され得る。いくつかの実装では、そのバーコードイメージは、静的またはエフェメラル（ephemeral）であり得る。例えば、第１のコンフィギュレータデバイス１１０は、ディスプレイを装備し得、暗号鍵を用いて符号化されているバーコードイメージ（または他のコーディングされたイメージ）を作成し得る。暗号鍵は、機械可読イメージ（ＱＲコードなど）を、カメラ、スマートフォン、スキャナ、または第２のコンフィギュレータデバイス１２０の別の機械可読コードを用いてスキャンおよび復号することによって決定され得る。暗号鍵に加えて、バーコードイメージはまた、第２のコンフィギュレータデバイス１２０がコンフィギュレータ鍵パッケージ４２７をダウンロードすることができるロケーションアドレスを用いて符号化され得る。

【００８８】

[0098] 第２のコンフィギュレータデバイス１２０は、ネットワークロケーションからコンフィギュレータ鍵パッケージ４２７をダウンロードすることができる（矢印５５７によって表される）。一旦、第２のコンフィギュレータデバイス１２０がコンフィギュレータ鍵パッケージ５４２７および暗号鍵を取得すると、第２のコンフィギュレータデバイス１２０は、暗号化された秘密鍵パッケージを復号することができ、それにより、コンフィギュレータ鍵を取得し、デバイスプロビジョニングプロトコルを用いた使用のための第２のコンフィギュレータデバイス１２０のメモリにコンフィギュレータ鍵を記憶する。

【００８９】

[0099] 図６は、複数のコンフィギュレータを有するデバイスプロビジョニングプロトコルの例示的なメッセージフロー図を示す。メッセージフロー図６００は、第１のコンフィギュレータデバイス１１０、第２のコンフィギュレータデバイス１２０、およびストレージロケーション４１０の間のメッセージを含む。６０５において、第１のコンフィギュレータデバイス１１０は、第１のコンフィギュレータデバイス１１０のコンフィギュレータ鍵（ｃ－ｓｉｇｎ－ｋｅｙおよび Ｃ－ｓｉｇｎ－ｋｅｙ）を含むコンフィギュレータ鍵パッケージを生成し得る。コンフィギュレータ鍵パッケージは、暗号鍵を使用して暗号化される。６１１において、第１のコンフィギュレータデバイス１１０は、ストレージロケーション４１０においてコンフィギュレータ鍵パッケージをエクスポートおよび記憶する。第１のコンフィギュレータデバイス１１０はまた、コンフィギュレータ鍵パッケージがどこに記憶されるかを示すロケーションアドレスを決定し得る。暗号鍵およびロケーションアドレスは、バーコードイメージまたは他のタイプのデータストラクチャとして符号化され得る。

【００９０】

[00100] ６１３において、第２のコンフィギュレータデバイス１２０は、コンフィギュレータ鍵パッケージ（および、オプションでロケーションアドレス）を取得し得る。例えば、第２のコンフィギュレータデバイス１２０は、バーコードイメージまたは他のデータストラクチャを取得および復号し得る。６１９において、第２のコンフィギュレータデバイス１２０は、コンフィギュレータ鍵パッケージのロケーションアドレスを決定し得る。第２のコンフィギュレータデバイス１２０は、バーコードイメージから、第１のコンフィギュレータデバイス１１０から別のメッセージ（図示せず）を介して、公開コネクタプロファイルを使用して、またはロケーションアドレスを共有するための任意の他のメカニズムによって、ロケーションアドレスを決定し得る。ロケーションアドレスに基づいて、第２のコンフィギュレータデバイス１２０は、ストレージロケーション４１０へのコンフィギュレータ鍵パッケージのリクエストを（６２１において）送り得る。６２３において、第２のコンフィギュレータデバイス１２０は、ストレージロケーション４１０からコンフィギュレータ鍵パッケージを受信し得る。６２５において、第２のコンフィギュレータ

デバイス１２０は、（暗号鍵を使用して）コンフィギュレータ鍵パッケージを復号し、コンフィギュレータ鍵を検索し得る。一旦第２のコンフィギュレータデバイス１２０がコンフィギュレータ鍵をもつと、第２のコンフィギュレータデバイス１２０は、第１のコンフィギュレータデバイス１１０が使用するであろう同じコンフィギュレータ鍵を使用して、エンローリデバイス２５０を構成し得る。

【００９１】

[00101] （ブートストラップ、認証、および構成を含む）デバイスプロビジョニングは、先に説明されたように続けることができる（図２のメッセージ２０５、２０７、２１７、２２７、２３７、２６３、２６７、および２７７の対応する説明を参照）。

【００９２】

[00102] 図７は、第１のコンフィギュレータデバイスを動作させるための例示的なフローチャートを示す。フローチャート７００は、ブロック７１０において開始する。ブロック７１０において、第１のコンフィギュレータデバイスは、暗号鍵を使用して少なくとも一部分を暗号化されたコンフィギュレータ鍵パッケージを生成し得る。コンフィギュレータ鍵パッケージは、第１のコンフィギュレータデバイスのための少なくともコンフィギュレータ秘密署名鍵を含み得る。ブロック７２０において、第１のコンフィギュレータデバイスは、第２のコンフィギュレータデバイスによってアクセス可能なストレージロケーションにおいてコンフィギュレータ鍵パッケージを記憶し得る。ブロック７３０において、第１のコンフィギュレータデバイスは、第２のコンフィギュレータデバイスがストレージロケーションからのコンフィギュレータ鍵パッケージを復号することを可能にするために、暗号鍵を提供する。ブロック７４０において、第１のコンフィギュレータデバイスは、オプションで、第２のコンフィギュレータデバイスにロケーションアドレスを提供し得る。ロケーションアドレスは、コンフィギュレータ鍵パッケージがストレージロケーションにおいてどこに記憶されるかを示し得る。

【００９３】

[00103] 図８は、第２のコンフィギュレータデバイスを動作させるための例示的なフローチャートを示す。フローチャート８００は、ブロック８１０において開始する。ブロック８１０において、第２のコンフィギュレータデバイスは、第２のコンフィギュレータデバイスにおいて、第１のコンフィギュレータデバイスから復号情報を取得し得る。例えば、復号情報は、コンフィギュレータ鍵パッケージを暗号化するために前に使用された暗号鍵であり得る。ブロック８２０において、第２のコンフィギュレータデバイスは、第２のコンフィギュレータデバイスにおいて、ストレージロケーションからコンフィギュレータ鍵パッケージを取得し得る。コンフィギュレータ鍵パッケージは、第１のコンフィギュレータデバイスのための少なくともコンフィギュレータ秘密署名鍵を含み得る。ブロック８３０において、第２のコンフィギュレータデバイスは、コンフィギュレータ秘密署名鍵を検索するために、復号情報を使用してコンフィギュレータ鍵パッケージを復号し得る。コンフィギュレータ鍵パッケージがコンフィギュレータ公開検証鍵を含み得る場合、第２のコンフィギュレータデバイスは、コンフィギュレータ鍵パッケージからコンフィギュレータ公開検証鍵をリストアすることができる。コンフィギュレータ鍵パッケージがコンフィギュレータ公開検証鍵を含まない場合、第２のコンフィギュレータデバイスは、コンフィギュレータ秘密署名鍵に少なくとも部分的に基づいて、コンフィギュレータ公開検証鍵を決定し得る。ブロック８４０において、第２のコンフィギュレータデバイスは、デバイスプロビジョニングプロトコルにしたがってコンフィギュレータ公開検証鍵およびコンフィギュレータ秘密署名鍵を使用して、ネットワーク用にエンローリデバイスを構成し得る。

【００９４】

[00104] 図９は、コンフィギュレータ鍵をバックアップおよびリストアするためにコンフィギュレータデバイスを動作させるための例示的なフローチャートを示す。フローチャート９００は、ブロック９１０において開始する。ブロック９１０において、コンフィギュレータデバイスは、コンフィギュレータ秘密署名鍵の暗号化されたコピーを少なくと

も含むコンフィギュレータ鍵パッケージを生成し得る。暗号化されたコピーは、秘密鍵暗号化技法を使用して暗号化され得る。例えば、秘密鍵暗号化技法は、インターネット・エンジニアリング・タスクフォース（ＩＥＴＦ）のＲＦＣ（Request for Comments）５９５８およびＲＦＣ５２０８のうちの少なくとも１つにおいて定義され得る。いくつかの実装では、秘密鍵暗号化技法は、コンフィギュレータ鍵パッケージのヘッダにおいて識別され得る。

【００９５】

[00105] ブロック９２０において、コンフィギュレータデバイスは、コンフィギュレータデバイスによってアクセス可能なストレージロケーションに、コンフィギュレータ鍵パッケージをバックアップとして記憶し得る。ストレージロケーションは、コンフィギュレータデバイスに利用可能な任意のストレージデバイスであり得る。ストレージロケーションの例は、コンフィギュレータデバイスのメモリ、ストレージロケーション、パーソナルコンピュータ、ホームサーバ、クラウドベースのストレージサービスなどを含む。いくつかの実装では、ストレージロケーションは、異なるコンフィギュレータ鍵を使用して、異なるコンフィギュレータデバイスからのバックアップを記憶するために使用され得る。

【００９６】

[00106] ブロック９３０において、コンフィギュレータデバイスは、コンフィギュレータ鍵パッケージを取得し、秘密鍵暗号化技法を使用してコンフィギュレータ鍵パッケージを復号することによって、バックアップを後にリストアし得る。

【００９７】

[00107] 以下は、本明細書で説明された任意の実装を用いて使用され得るコンフィギュレータ鍵パッケージの一例である。例示的なコンフィギュレータ鍵パッケージは、（ＰＫＣＳ＃８を使用して）ＲＦＣ５９５８において定義された１つの非対称鍵のＡＳＮ．１シーケンスである非対称鍵パッケージである。

【００９８】

【数１】

```
AsymmetricKeyPackage ::= SEQUENCE SIZE (1) OF OneAsymmetricKey
OneAsymmetricKey ::= SEQUENCE {
    version                 Version,
    privateKeyAlgorithm     PrivateKeyAlgorithmIdentifier,
    privateKey PrivateKey,
    [[publicKey             PublicKey OPTIONAL,]]

    [必要あればオプションの情報]
    }
PrivateKey ::= SEQUENCE {
        encryptionAlgorithm  EncryptionAlgorithmIdentifier,
        encryptedData        EncryptedData }
EncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
        { CONTENT-ENCRYPTION,
        { KeyEncryptionAlgorithms } }
EncryptedData ::= コンフィギュレータ秘密署名鍵の暗号化バージョンを含むOCTET STRING
```

【００９９】

[00108] 図１０は、本開示の態様を実装するための例示的な電子デバイス１０００のブロック図を示す。いくつかの実装では、電子デバイス１０００は、第１のコンフィギュレータデバイス１１０または第２のコンフィギュレータデバイス１２０に類似し得る。電

子デバイス１０００は、ラップトップコンピュータ、タブレットコンピュータ、モバイルフォン、ゲーミングコンソール、スマートウォッチ、仮想または拡張現実デバイス、ドローン、あるいは別の電子システムであり得る。電子デバイス１０００は、（場合により、複数のプロセッサ、複数のコア、複数のノードを含む、またはマルチスレッドを実行するなどの）プロセッサ１００２を含む。電子デバイス１０００は、プロセッサ１００６を含む。メモリ１００６は、システムメモリ、あるいは、機械可読媒体またはコンピュータ可読媒体の下記に説明されるあり得る現実（realizations）のうちの任意の１つまたは複数であり得る。電子デバイス１０００はまた、（ＰＣＩ、ＩＳＡ、ＰＣＩ－Ｅｘｐｒｅｓｓ、ＨｙｐｅｒＴｒａｎｓｐｏｒｔ（登録商標）、ＩｎｆｉｎｉＢａｎｄ（登録商標）、ＮｕＢｕｓ、ＡＨＢ、ＡＸＩなどの）バス１００１を含み得る。電子デバイスは、１つまたは複数のネットワークインターフェース１００４を含み得、それは、（ＷＬＡＮインターフェース、Ｂｌｕｅｔｏｏｔｈ（登録商標）インターフェース、ＷｉＭＡＸインターフェース、ＺｉｇＢｅｅ（登録商標）インターフェース、ワイヤレスＵＳＢインターフェースなどのような）ワイヤレスネットワークインターフェースまたは（電力線通信インターフェース、イーサネット（登録商標）インターフェースなどのような）ワイヤードネットワークインターフェースであり得る。いくつかの実装では、電子デバイス１０００は、複数のネットワークインターフェース１００４をサポートし得る、その各々は、電子デバイス１０００を異なる通信ネットワークに結合するように構成され得る。

【０１００】

[00109] メモリ１００６は、上述された様々な実装をサポートするための機能を含む。メモリ１００６は、デバイスプロビジョニングプロトコルの実装を容易にする１つまたは複数の機能を含み得る。例えば、メモリ１００６は、上述されるように第１のコンフィギュレータデバイス１１０または第２のコンフィギュレータデバイス１２０のうちの１つまたは複数の態様を実装し得る。メモリ１００６は、上記の図１～図９に説明される実装を利用可能にするための機能を具現化し得る。いくつかの実装では、メモリ１００６は、コンフィギュレータ鍵パッケージを生成、記憶、または検索することを容易にする１つまたは複数の機能を含み得る。電子デバイス１０００は、暗号化／復号モジュール１０１６またはバックアップ／リストアモジュール１０５５を含み得る。例えば、暗号化／復号モジュール１０１６は、コンフィギュレータ鍵パッケージの少なくとも一部分の暗号化、またはコンフィギュレータ鍵パッケージの復号を容易にし得る。バックアップ／リストアモジュール１０５５は、コンフィギュレータ鍵パッケージのストレージ、およびストレージロケーションからのコンフィギュレータ鍵パッケージの検索を容易にし得る。電子デバイス１０００はまた、センサユニット、ユーザインターフェースコンポーネント、または別の入力／出力コンポーネントなどの他のコンポーネント１０２０を含み得る。いくつかの他の実装では、電子デバイス１０００は、ブートストラッピング技法を使用して、復号情報を取得するために使用される（カメラ、マイクロフォン、ＮＦＣ検出器、バーコードスキャナなどのような）他の適切なセンサを有し得る。

【０１０１】

[00110] これらの機能のうちの任意の１つが、プロセッサ１００２上などのハードウェア中で部分的に（または全体的に）実装され得る。例えば、機能は、特定用途向け集積回路を用いて、プロセッサ１００２中で実施されるロジックにおいて、周辺デバイスのコプロセッサ（co-processor）において、またはカードなどで、実施され得る。さらに、それらの実現は、図１０において例示されていない、より少ないまたは追加のコンポーネント（例えば、映像カード、音声カード、追加のネットワークインターフェース、周辺デバイスなど）を含み得る。プロセッサ１００２およびプロセッサ１００６は、バス１００１に結合され得る。バス１００１に結合されているように図示されるが、メモリ１００６は、プロセッサ１００２に直接結合されてもよい。

【０１０２】

[00111] 本明細書で使用されるとき、項目のリスト「のうちの少なくとも１つ」を示すフレーズは、単一の要素を含む、それらの項目の任意の組み合わせを指す。例として、

「ａ、ｂ、またはｃのうちの少なくとも１つ」は、ａ、ｂ、ｃ、ａ－ｂ、ａ－ｃ、ｂ－ｃ、およびａ－ｂ－ｃをカバーすることを意図される。

【０１０３】

[00112] 本明細書で開示された実施形態に関連して説明される様々な例示的なロジック、論理ブロック、モジュール、回路、およびアルゴリズムプロセスは、電子ハードウェア、コンピュータソフトウェア、または両方の組み合わせとして実施され得る。ハードウェアとソフトウェアとの互換性は概して、機能の観点から説明されており、上述された様々な例示的なコンポーネント、ブロック、モジュール、回路、およびプロセスにおいて例示されている。そのような機能をハードウェアにおいて実装されるか、ソフトウェアにおいて実装されるかは、特定の適用例および全体的なシステムに課される設計制約に依存する。

【０１０４】

[00113] 本明細書に開示された態様に関連して説明された例示的な様々な論理、論理ブロック、モジュール、および回路を実装するために使用されるハードウェアおよびデータ処理装置は、汎用のシングルチップまたはマルチチッププロセッサ、デジタルシグナルプロセッサ（ＤＳＰ）、－特定用途向け集積回路（ＡＳＩＣ）、フィールド－プログラマブルゲートアレイ（ＦＰＧＡ）または他のプログラマブル論理デバイス、ディスクリートゲートまたはトランジスタ論理回路、ディスクリートハードウェア構成要素、もしくは、本明細書で説明された機能を行うように設計されたそれらの任意の組合せで実装され得るかまたは行われ得る。汎用プロセッサは、マイクロプロセッサ、または、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、あるいはステートマシンであり得る。プロセッサはまた、ＤＳＰとマイクロプロセッサの組み合わせ、複数のマイクロプロセッサ、ＤＳＰコアと連携した１つまたは複数のマイクロプロセッサ、あるいはあらゆる他のこのような構成などの、コンピューティングデバイスの組み合わせとして実装され得る。いくつかの実施形態では、特定のプロセスおよび方法が、所与の機能に特有である回路によって行われ得る。

【０１０５】

[00114] １つまたは複数の様態では、説明された機能は、この明細書中に開示された構造およびそれらの構造的同等物を含む、ハードウェア、デジタル電子回路、コンピュータソフトウェア、ファームウェアまたはそれらの任意の組み合わせにおいて実装され得る。本明細書で説明された主題の実装はまた、データ処理装置による実行のための、またはデータ処理装置の動作を制御するために、コンピュータ記憶媒体上で符号化される、１つまたは複数のコンピュータプログラム、すなわち、コンピュータプログラムの命令の１つまたは複数のモジュールとして実装されることができる。

【０１０６】

[00115] ソフトウェアで実施する場合、機能は、１つまたは複数の命令またはコードとしてコンピュータ可読媒体上に記憶するか、あるいはコンピュータ可読媒体を介して送信することができる。本明細書で開示された方法またはアルゴリズムのプロセスは、コンピュータ可読媒体上に存在し得るプロセッサ実行可能ソフトウェアモジュールにおいて実装され得る。コンピュータ可読媒体は、ある場所から別の場所にコンピュータプログラムを転送することを可能にされることができる任意の媒体を含む通信媒体およびコンピュータ記憶媒体の両方を含む。記憶媒体は、コンピュータによってアクセスされ得る任意の利用可能な媒体であり得る。限定はされないが、例として、このようなコンピュータ可読媒体は、ＲＡＭ（ＳＲＡＭ、ＤＲＡＭ、ゼロキャパシタＲＡＭ、ツイントランジスタＲＡＭ、ｅＤＲＡＭ、ＥＤＯ ＲＡＭ、ＤＤＲ ＲＡＭ、ＥＥＰＲＯＭ（登録商標）、ＮＲＡＭ、ＲＲＡＭ（登録商標），ＳＯＮＯＳ、ＰＲＡＭなどを含む）、ＲＯＭ、ＥＥＰＲＯＭ（登録商標）、ＣＤ－ＲＯＭあるいは他の光ディスク記憶装置、磁気ディスク記憶デバイスあるいは他の磁気記憶デバイス、または命令あるいはデータ構造の形態で所望のプログラムコードを記憶するために使用され、コンピュータによってアクセスされ得る任意の他の媒体を含み得る。また、任意の接続は、コンピュータ可読媒体と適切に呼ばれ得る。本明細

書で使用するディスク（disk）およびディスク（disc）は、コンパクトディスク（ＣＤ）、レーザーディスク（登録商標）、光ディスク、デジタル多用途ディスク（ＤＶＤ）、フロッピー（登録商標）ディスクおよびブルーレイディスクを含み、ディスク（disk）は、通常、データを磁気的に再生し、ディスク（disc）は、データをレーザで光学的に再生する。上記の組合せもコンピュータ可読媒体の範囲内に含まれることができる。加えて、方法またはアルゴリズムの動作は、機械－可読媒体およびコンピュータ可読媒体上で、コードおよび命令のうちの１つ、またはそれらの任意の組み合わせ、またはそれらのセットとして存在し得、それは、コンピュータプログラム製品に組み込まれ得る。

【０１０７】

[00116] 本開示で説明される実装への様々な変更は、当業者にとって容易に明らかであり、および、ここで定義される一般的な原理は、本開示の精神または範囲から逸脱することなく他の実装に適用され得る。よって、特許請求の範囲は、本明細書に示される実施形態に限定されることを意図されてはいないが、本明細書に開示されたこの開示、原理および新規の特徴と一致する最も広い範囲が付与されるべきである。

【０１０８】

[00117] 加えて、当業者は、「上方」および「下方」という用語が、図を説明しやすくするために使用されることがあり、適正に方向付けられた頁上で図の向きに対応する相対位置を示し、実施されたときの任意のデバイスの適正な向きを反映しないことがあり得ることを容易に認識するであろう。

【０１０９】

[00118] 別個の実装に照らして本明細書で説明される、ある特徴もまた、単一の実装で組み合わせて実施されることができる。反対に、単一の実装のコンテキストにおいて説明されている様々な特徴もまた、別個に複数の実装において、または任意の適したサブコンビネーションにおいて実装されることができる。さらに、特徴は、ある特定の組み合わせで機能するとして上述され、特許請求の範囲にさえ最初はそのように記載され得るが、特許請求の範囲に記載されている組み合わせからの１つまたは複数の特徴は、いくつかのケースでは、その組み合わせから削除され、特許請求の範囲に記載されている組み合わせは、サブコンビネーションまたはサブコンビネーションの変形を対象とし得る。

【０１１０】

[00119] 同様に、動作が特定の順序で図面に図示されているが、このことは、そのような動作が、望ましい結果を達成するために、示された特定の順序または連続した順序で行われること、または全ての例示された動作が行われることを必要とするものと理解されるべきではない。さらに、図面は、フロー図の形式でもう１つの実例的なプロセスを概略的に図示し得る。しかしながら、図示されていない他の動作は、概略的に例示されている実例的なプロセス中に組み込まれることができる。例えば、１つまたは複数の追加の動作は、例示されている動作のいずれかの前に、後で、同時に、または間に行われ得る。ある特定の状況では、マルチタスクおよび平行処理が有利であり得る。さらに、上述された実装における様々なシステムコンポーネントの分離は、すべての実装においてそのような分離を必要とするものと理解されるべきではなく、説明されたプログラムコンポーネントおよびシステムが、概して、単一のソフトウェア製品に一体化されるか、または複数のソフトウェア製品にパッケージ化される得ることが理解されるべきである。加えて、他の実施形態は、下記の特許請求の範囲内にある。いくつかのケースでは、特許請求の範囲に記載されるアクションは、異なる順序で行われ、それでもなお望ましい結果を達成することができる。

以下に本願の出願当初の特許請求の範囲に記載された発明を付記する。

［Ｃ１］

ネットワークの第１のコンフィギュレータデバイスによって実行される方法であって、

前記第１のコンフィギュレータデバイスに関連付けられた少なくともコンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成することと、

前記コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することと、

前記第１のコンフィギュレータデバイスまたは第２のコンフィギュレータデバイスによる後のリストアのためのバックアップとして、ストレージロケーションに前記コンフィギュレータ鍵パッケージを記憶することと、
を備える、方法。
［Ｃ２］
前記コンフィギュレータ鍵パッケージは、前記コンフィギュレータ秘密署名鍵に関連付けられるコンフィギュレータ公開検証鍵をさらに含む、Ｃ１に記載の方法。
［Ｃ３］
前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を暗号化することは、前記コンフィギュレータ秘密署名鍵とは異なる暗号鍵を使用して前記コンフィギュレータ鍵パッケージを暗号化することを含む、Ｃ１に記載の方法。
［Ｃ４］
少なくとも前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を暗号化することは、秘密鍵暗号化技法を使用して前記コンフィギュレータ秘密署名鍵を暗号化することと、前記コンフィギュレータ鍵パッケージのヘッダ中に前記秘密鍵暗号化技法のインジケーションを含めることと、を含む、Ｃ１に記載の方法。
［Ｃ５］
前記コンフィギュレータ鍵パッケージを記憶することは、
前記コンフィギュレータ鍵パッケージと復号情報とを含むデジタルエンベロープを生成することを含み、前記復号情報は、前記第２のコンフィギュレータデバイスが前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することを可能にする、
Ｃ１に記載の方法。
［Ｃ６］
前記ストレージロケーションは、前記第１のコンフィギュレータデバイスのメモリ、ネットワーク共有ロケーション、パーソナルコンピュータ、ホームサーバ、クラウドベースのストレージサービス、およびワイヤレスネットワークのアクセスポイント（ＡＰ）、からなるグループから選択される少なくとも１つのメンバである、Ｃ１に記載の方法。
［Ｃ７］
前記コンフィギュレータ鍵パッケージを記憶することは、前記コンフィギュレータ鍵パッケージのバックアップを記憶することを含み、前記方法は、
前記第１のコンフィギュレータデバイスによって、前記ストレージロケーションから、前記コンフィギュレータ鍵パッケージの前記バックアップを検索することと、
前記コンフィギュレータ鍵パッケージのすくなくとも前記一部分を復号することと、
前記コンフィギュレータ鍵パッケージから前記コンフィギュレータ秘密署名鍵を取得することと、
をさらに備える、Ｃ１に記載の方法。
［Ｃ８］
前記コンフィギュレータ鍵パッケージから取得された前記コンフィギュレータ秘密署名鍵に少なくとも部分的に基づいて、コンフィギュレータ公開検証鍵を決定すること、
をさらに備える、Ｃ７に記載の方法。
［Ｃ９］
前記ストレージロケーションにおける前記コンフィギュレータ鍵パッケージのロケーションアドレスを決定することと、
前記第２のコンフィギュレータデバイスに前記ロケーションアドレスを提供することと、
をさらに備える、Ｃ１に記載の方法。
［Ｃ１０］
前記第２のコンフィギュレータデバイスに復号情報を提供することをさらに備え、前記復号情報は、前記第２のコンフィギュレータデバイスが、前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することと、前記コンフィギュレータ秘密署名鍵を

取得することと、を可能にする、
Ｃ１に記載の方法。
［Ｃ１１］
前記復号情報は、前記ストレージロケーションにおける前記コンフィギュレータ鍵パッケージのロケーションアドレスと、前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号するために使用可能な暗号鍵と、からなるグループから選択される少なくとも１つのメンバを含む、Ｃ１０に記載の方法。
［Ｃ１２］
前記復号情報を提供することは、前記第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェース、からなるグループから選択される少なくとも１つのメンバを使用して前記復号情報を提供することを含む、Ｃ１０に記載の方法。
［Ｃ１３］
前記復号情報を提供することは、前記復号情報が符号化されているイメージを表示することを含む、Ｃ１０に記載の方法。
［Ｃ１４］
前記イメージは、バーコードまたはクイックレスポンス（ＱＲ）コードイメージである、Ｃ１３に記載の方法。
［Ｃ１５］
コンフィギュレータ公開検証鍵は、前記コンフィギュレータ秘密署名鍵から導出されるか、または前記コンフィギュレータ鍵パッケージから取得され、
前記コンフィギュレータ秘密署名鍵および前記コンフィギュレータ公開検証鍵は、第１のネットワークの複数のコンフィギュレータ間で共有され、
前記複数のコンフィギュレータの各々は、前記第１のネットワーク用にエンローリデバイスを構成するために、デバイスプロビジョニングプロトコルに従って前記コンフィギュレータ秘密署名鍵および前記コンフィギュレータ公開検証鍵を使用することが可能である、
Ｃ１に記載の方法。
［Ｃ１６］
第１のコンフィギュレータデバイスであって、
プロセッサと、
命令を記憶したメモリと、
を備え、前記命令は、前記プロセッサによって実行されると、前記第１のコンフィギュレータデバイスに、
前記第１のコンフィギュレータデバイスに関連付けられた少なくともコンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成することと、
前記コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することと、
前記第１のコンフィギュレータデバイスまたは第２のコンフィギュレータデバイスによる後のリストアのためのバックアップとして、ストレージロケーションに前記コンフィギュレータ鍵パッケージを記憶することと、
を行わせる、第１のコンフィギュレータデバイス。
［Ｃ１７］
前記命令は、前記プロセッサによって実行されると、前記第１のコンフィギュレータデバイスに、
前記コンフィギュレータ秘密署名鍵とは異なる暗号鍵を使用して、前記コンフィギュレータ鍵パッケージを暗号化すること、
をさらに行わせる、Ｃ１６に記載の第１のコンフィギュレータデバイス。
［Ｃ１８］
前記命令は、前記プロセッサによって実行されると、前記第１のコンフィギュレータデバイスに、

秘密鍵暗号化技法を使用して前記コンフィギュレータ秘密署名鍵を暗号化することと、
前記コンフィギュレータ鍵パッケージのヘッダ中に前記秘密鍵暗号化技法のインジケーションを含めることと、
をさらに行わせる、Ｃ１６に記載の第１のコンフィギュレータデバイス。
［Ｃ１９］
前記命令は、前記プロセッサによって実行されると、前記第１のコンフィギュレータデバイスに、
前記コンフィギュレータ鍵パッケージと復号情報とを含むデジタルエンベロープを生成することをさらに行わせ、前記復号情報は、前記第２のコンフィギュレータデバイスが前記コンフィギュレータ鍵パッケージの少なくとも前記部分を復号することを可能にする、
Ｃ１６に記載の第１のコンフィギュレータデバイス。
［Ｃ２０］
前記コンフィギュレータ鍵パッケージを記憶するための前記命令は、前記コンフィギュレータ鍵パッケージのバックアップを記憶するための命令を含み、前記命令は、前記プロセッサによって実行されると、前記第１のコンフィギュレータデバイスに、
前記ストレージロケーションから前記コンフィギュレータ鍵パッケージの前記バックアップを検索することと、
前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することと、
前記コンフィギュレータ鍵パッケージから前記コンフィギュレータ秘密署名鍵を取得することと、
をさらに行わせる、Ｃ１６に記載の第１のコンフィギュレータデバイス。
［Ｃ２１］
前記命令は、前記プロセッサによって実行されると、前記第１のコンフィギュレータデバイスに、
前記ストレージロケーションにおけるコンフィギュレータ鍵パッケージのロケーションアドレスを決定することと、
前記第２のコンフィギュレータデバイスに前記ロケーションアドレスを提供することと、
をさらに行わせる、Ｃ１６に記載の第１のコンフィギュレータデバイス。
［Ｃ２２］
前記命令は、前記プロセッサによって実行されると、前記第１のコンフィギュレータデバイスに、
前記第２のコンフィギュレータデバイスに復号情報を提供することをさらに行わせ、前記復号情報は、前記第２のコンフィギュレータデバイスが前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することと、前記コンフィギュレータ秘密署名鍵を取得することと、を可能にする、
Ｃ１６に記載の第１のコンフィギュレータデバイス。
［Ｃ２３］
前記復号情報は、前記ストレージロケーションにおける前記コンフィギュレータ鍵パッケージのロケーションアドレスと、前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号するために使用可能な暗号鍵と、からなるグループから選択される少なくとも１つのメンバを含む、Ｃ２２に記載の第１のコンフィギュレータデバイス。
［Ｃ２４］
前記命令は、前記プロセッサによって実行されると、前記第１のコンフィギュレータデバイスに、
前記第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェース、からなるグループから選択される少なくとも１つのメンバを使用して前記復号情報を提供すること、
をさらに行わせる、Ｃ２２に記載の第１のコンフィギュレータデバイス。
［Ｃ２５］

命令を記憶したコンピュータ可読媒体であって、前記命令は、第１のコンフィギュレータデバイスのプロセッサによって実行されると、前記第１のコンフィギュレータデバイスに、
前記第１のコンフィギュレータデバイスに関連付けられた少なくともコンフィギュレータ秘密署名鍵を含む、コンフィギュレータ鍵パッケージを生成することと、
前記コンフィギュレータ鍵パッケージの少なくとも一部分を暗号化することと、
前記第１のコンフィギュレータデバイスまたは第２のコンフィギュレータデバイスによる後の検索のために、ストレージロケーションに前記コンフィギュレータ鍵パッケージを記憶することと、
を行わせる、第１のコンフィギュレータデバイス。

［Ｃ２６］
第２のコンフィギュレータデバイスによって行われる方法であって、
前記第２のコンフィギュレータデバイスにおいて、ストレージロケーションからコンフィギュレータ鍵パッケージを取得することと、ここにおいて、前記コンフィギュレータ鍵パッケージの少なくとも一部分は暗号化され、前記コンフィギュレータ鍵パッケージは、第１のコンフィギュレータデバイスに関連付けられたコンフィギュレータ秘密署名鍵を少なくとも含み、
前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することと、
前記コンフィギュレータ鍵パッケージから前記コンフィギュレータ秘密署名鍵を取得することと、
デバイスプロビジョニングプロトコルに従って、前記コンフィギュレータ秘密署名鍵を利用して、ネットワーク用にエンローリデバイスをプロビジョニングすることと、
を備える、方法。

［Ｃ２７］
前記第１のコンフィギュレータデバイスから復号情報を取得することをさらに備え、前記復号情報は、前記第２のコンフィギュレータデバイスが前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号することを可能にする、
Ｃ２６に記載の方法。

［Ｃ２８］
前記復号情報は、前記ストレージロケーションにおける前記コンフィギュレータ鍵パッケージのロケーションアドレスと、前記コンフィギュレータ鍵パッケージの少なくとも前記一部分を復号するために使用可能な暗号鍵と、からなるグループから選択される少なくとも１つのメンバを含む、Ｃ２７に記載の方法。

［Ｃ２９］
前記復号情報を取得することは、前記第１のコンフィギュレータデバイスのディスプレイ、スピーカ、光信号、センサインターフェース、および短距離無線周波数インターフェース、からなるグループから選択される少なくとも１つのメンバを使用して前記復号情報を取得することを含む、Ｃ２７に記載の方法。

［Ｃ３０］
前記復号情報を取得することは、前記第２のコンフィギュレータデバイスに関連付けられたカメラを介して、前記復号情報が符号化されているイメージを取得することと、
前記復号情報を検索するために前記イメージを復号することと、
を含む、Ｃ２７に記載の方法。

【図１】

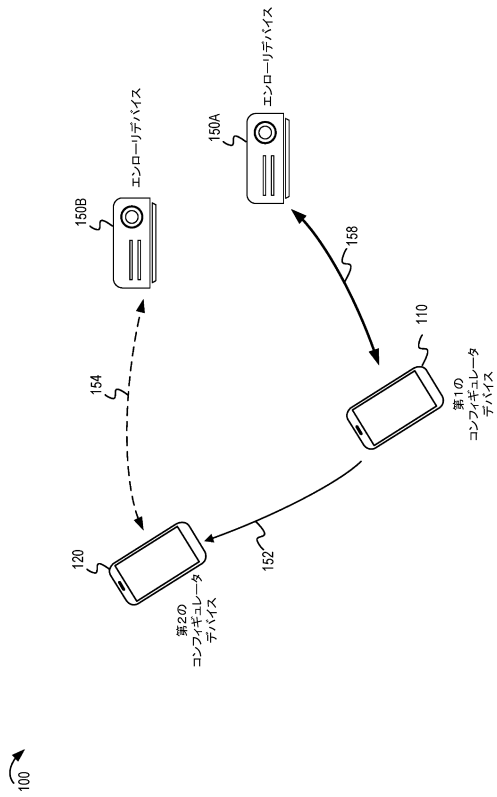

FIG. 1

【図２】

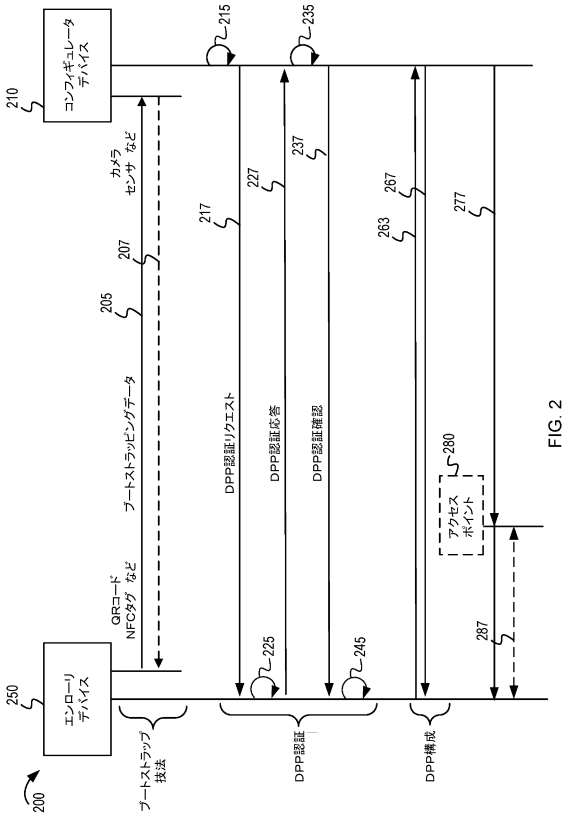

FIG. 2

【図３】

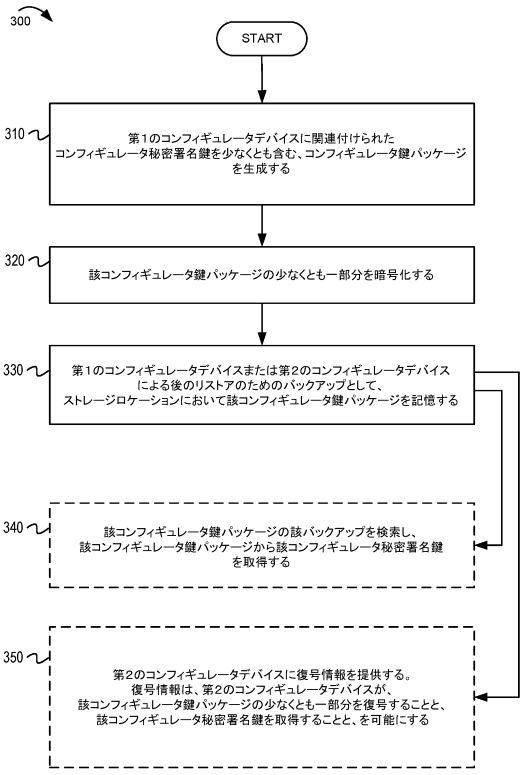

FIG. 3

【図４】

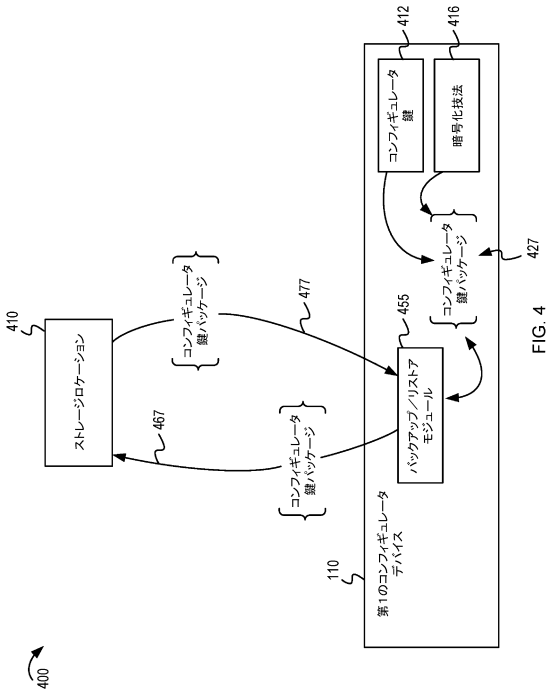

FIG. 4

【図５】

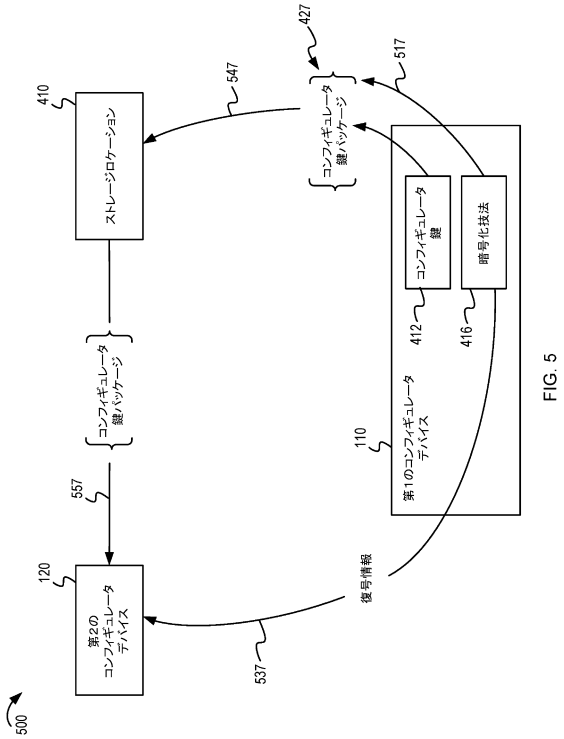

FIG. 5

【図６】

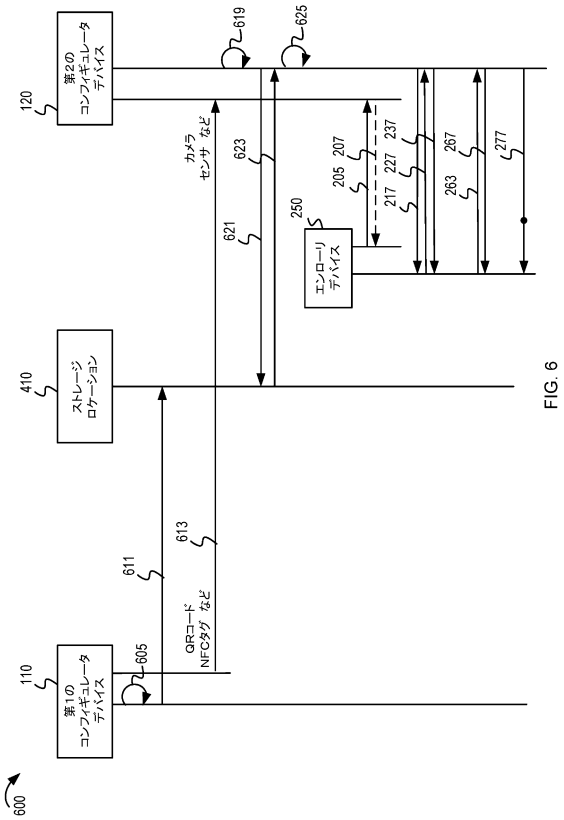

FIG. 6

【図７】

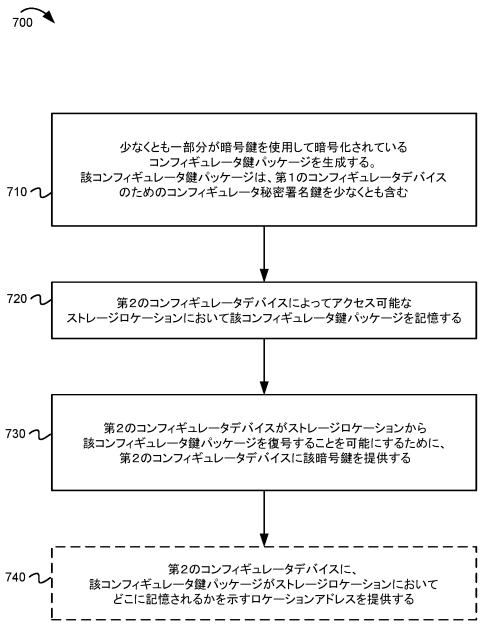

FIG. 7

【図８】

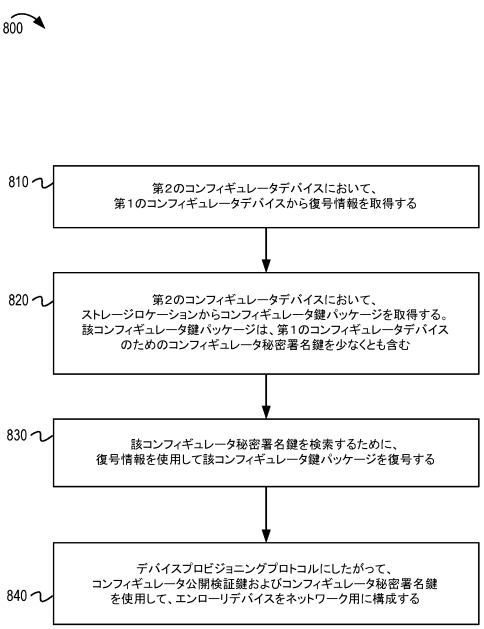

FIG. 8

【図９】

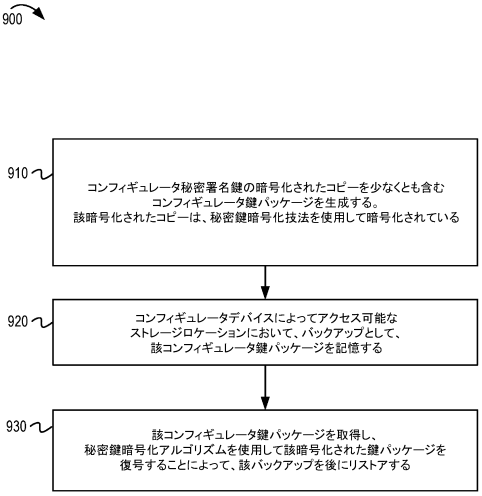

FIG. 9

【図１０】

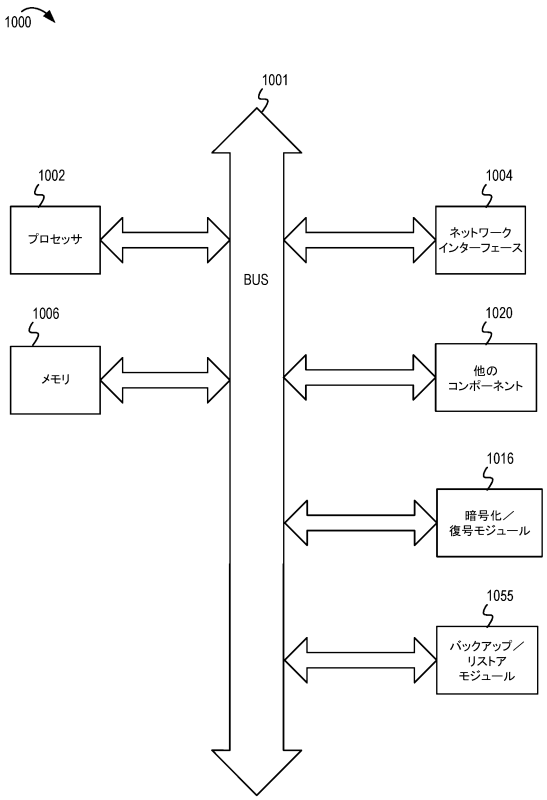

FIG. 10

フロントページの続き

早期審査対象出願

(72)発明者　カマロタ、ロサリオ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(72)発明者　マリネン、ジョウニ・カレビ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(72)発明者　ティナゴーンスリスパップ、ピーラポン
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５

審査官　中里　裕正

(56)参考文献　特開平９－６２３６（ＪＰ，Ａ）
特開２００６－３５２５６０（ＪＰ，Ａ）
特開２０１３－２３５４６５（ＪＰ，Ａ）
国際公開第２０１５／０９４３２６（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｗ　１２／０４
Ｈ０４Ｗ　８４／１０