(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7551080号
(P7551080)

(45)発行日　令和6年9月17日(2024.9.17)

(24)登録日　令和6年9月6日(2024.9.6)

(51)国際特許分類

H04L 9/32 (2006.01)		H04L	9/32	200B
H04L 9/08 (2006.01)		H04L	9/08	F

請求項の数　18　（全28頁）

(21)出願番号　特願2021-526464(P2021-526464)
(86)(22)出願日　令和1年7月31日(2019.7.31)
(65)公表番号　特表2022-507488(P2022-507488A)
(43)公表日　令和4年1月18日(2022.1.18)
(86)国際出願番号　PCT/SG2019/050382
(87)国際公開番号　WO2020/101567
(87)国際公開日　令和2年5月22日(2020.5.22)
審査請求日　令和4年7月28日(2022.7.28)
(31)優先権主張番号　10201810250P
(32)優先日　平成30年11月16日(2018.11.16)
(33)優先権主張国・地域又は機関
シンガポール(SG)

(73)特許権者　521207106
マイクロセック プライベート リミテッド
シンガポール国 ３４９５８５ シンガポール ＃０６－０７，ゲンティン レーン ２８
(74)代理人　100129654
弁理士　大池 達也
(72)発明者　ミシュラ，ビシュラム
シンガポール国 ５３０４４６ シンガポール ＃１０－１６２３，ホウガン アベニュー ８，４４６
(72)発明者　イクラム，マグジャン
シンガポール国 ５２０２７１ シンガポール ＃１１－１０７，タンピネス ストリート ２１，２７１

最終頁に続く

(54)【発明の名称】　最適化された公開鍵基盤を備える組み込みシステムのネットワークを保護および管理するための方法ならびにアーキテクチャ

(57)【特許請求の範囲】

【請求項１】

データを通信するための通信方法であって、

トランスポート層またはアプリケーション層のセキュリティを提供するマイクロ公開鍵基盤内のマイクロ証明書を使用してデータ通信セッションの当事者を、データ通信のための装置によって認証するステップと、

前記マイクロ証明書を使用して前記データ通信セッションを、データ通信のための装置によって確立するステップと、

前記データ通信セッションを通じて安全なデータ通信を、データ通信のための装置によって実行するステップと、を含み、

前記マイクロ公開鍵基盤は、通信プロトコル、前記マイクロ証明書、および管理プラットフォームの組み合わせよりなり、

前記データ通信セッションの少なくとも１の当事者がリソースおよび帯域幅に制約のあるデバイスであり、

前記認証するステップにおいて、

前記当事者によりマイクロ証明書署名要求を生成するステップと、

前記マイクロ公開鍵基盤のサーバにおいてマイクロ証明書署名要求を前記当事者から受信するステップと、

前記マイクロ証明書署名要求を、前記マイクロ公開鍵基盤のサーバによって認証局に送信するステップと、

前記マイクロ公開鍵基盤のサーバにおいて、前記マイクロ証明書署名要求に対する署名された情報を含む応答を前記認証局から受信するステップと、
前記マイクロ公開鍵基盤のサーバからの前記応答を該当事者に送信し、当該当事者が前記署名された情報に基づいてマイクロ証明書を再作成し、該マイクロ証明書をインストールするか、あるいは前記署名された情報により以前のマイクロ証明書を更新するステップと、を実行し、
前記マイクロ証明書署名要求は、前記認証局によって提供されるマイクロ証明書のフィールドのセットを含むことなく構成され、
該マイクロ証明書のフィールドのセットは、発行者、日付、期間のうちの１または複数を含み、
前記マイクロ証明書は、マイクロテーブルベースあるいはルックアップテーブルベースのスキームを使用して前記マイクロ証明書のサイズを縮小し、前記マイクロテーブルベースあるいはルックアップテーブルベースのスキームは、前記マイクロ証明書のタイプおよび前記マイクロ証明書が保持するさまざまなパラメータに関する情報を提供するために、前記マイクロ証明書の異なるフィールドを利用する、データ通信方法。

【請求項２】
請求項１において、前記マイクロ公開鍵基盤が、アプリケーションコードとネットワーク通信コードとの間に位置するソフトウェア開発キットを通じて統合されるデータ通信方法。

【請求項３】
請求項１において、前記マイクロ公開鍵基盤に関連するアクティビティが、マイクロ公開鍵基盤通信プロトコルを介して実行され、
前記アクティビティには、証明書交換、セッション鍵交換、証明書署名、および関連メッセージの制御が含まれるデータ通信方法。

【請求項４】
請求項３において、前記マイクロ公開鍵基盤通信プロトコルが、１バイトの識別子フィールドと、任意の長さのメッセージと、を含むパケットを定義するデータ通信方法。

【請求項５】
請求項１において、前記マイクロ証明書の複数の識別子が数値であり、前記複数の識別子のそれぞれは、識別子の目的に合わせてサイズが調整されるデータ通信方法。

【請求項６】
請求項１において、前記マイクロ証明書が公開鍵を含み、
前記公開鍵は、楕円曲線暗号に基づいており、前記マイクロ証明書において、該公開鍵の楕円曲線上の点に対する圧縮を実行する点圧縮技術を使用して表されるデータ通信方法。

【請求項７】
請求項１において、前記マイクロ証明書のサイズが、Ｘ．５０９証明書を含む従来のデジタル証明書よりも小さいデータ通信方法。

【請求項８】
請求項１において、自動証明書管理環境およびシステムが、前記マイクロ証明書のコミッショニング、更新、および失効を遠隔管理するデータ通信方法。

【請求項９】
請求項１において、さらに、
コンピューティングデバイスにおいて、前記マイクロ証明書署名要求に対する応答を前記認証局から受信するステップと、
前記応答に基づいて、前記認証局によって署名されており楕円曲線暗号を利用するマイクロ証明書を前記コンピューティングデバイスによって再作成するステップと、
を含む、データ通信方法。

【請求項１０】
請求項９において、前記応答は、前記コンピューティングデバイスが所有する前記マイクロ証明書のフィールドのセットを含むことなく構成されているデータ通信方法。

【請求項１１】
請求項９において、前記マイクロ証明書における複数の識別子が数値であり、
前記数値の意味は前記マイクロ証明書の外部に格納され、
前記複数の識別子のそれぞれは、識別子の目的に合わせてサイズが調整されるデータ通信方法。
【請求項１２】
請求項９において、前記マイクロ証明書が公開鍵を含み、該公開鍵が、前記マイクロ証明書において点圧縮技術を使用して表されているデータ通信方法。
【請求項１３】
請求項９において、前記マイクロ証明書署名要求は、マイクロ公開鍵基盤通信プロトコルを介して前記認証局に送信され、
前記マイクロ公開鍵基盤通信プロトコルは、１バイトの識別子フィールドと、任意の長さのメッセージと、を含むパケットを定義し、
前記１バイトの識別子フィールドは、前記メッセージの長さを定義しないデータ通信方法。
【請求項１４】
請求項１において、さらに、
前記認証局において前記マイクロ証明書署名要求を受信するステップと、
前記マイクロ証明書署名要求に対する応答を前記認証局によって生成するステップと、
前記認証局によって前記応答を送信するステップと、
を含み、
前記認証局によって署名されており、楕円曲線暗号を利用するマイクロ証明書は、前記応答に基づいて再作成される、データ通信方法。
【請求項１５】
請求項１４において、前記応答は、コンピューティングデバイスが所有する前記マイクロ証明書のフィールドのセットを含むことなく構成されているデータ通信方法。
【請求項１６】
請求項１４において、前記マイクロ証明書の複数の識別子が数値であり、
前記複数の識別子のそれぞれは、識別子の目的に合わせてサイズが調整され、
各数値識別子は、それ自体を前記マイクロ証明書に格納する必要のない、より詳細な情報に関連付けられるデータ通信方法。
【請求項１７】
請求項１４において、前記マイクロ証明書が公開鍵を含み、前記公開鍵は、ポイント圧縮技術を使用して前記マイクロ証明書に表されるデータ通信方法。
【請求項１８】
請求項１４において、前記応答の生成は、
前記マイクロ証明書署名要求の検証、
前記マイクロ証明書への署名、および
署名された前記マイクロ証明書に基づく前記応答の作成、を含むデータ通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願へのクロスリファレンス
本出願は、２０１８年１１月１６日出願の「Method and Architecture for Securing and Managing Networks of Embedded Systems with Optimised Public Key Infrastructure」と題するシンガポール特許出願第１０２０１８１０２５０Ｐ号に基づく優先権を主張しており、このシンガポール出願の全体が参照されて本明細書に明示的に組み込まれる。
【０００２】
本開示の様々な態様は、一般に、コンピュータセキュリティ、より具体的には、組み込

みシステムのネットワークのための公開鍵基盤に関するものである。
【背景技術】
【０００３】
モノのインターネット（ＩｏＴ）は、電子機器、ソフトウェア、アクチュエータ、およびこれらを接続、連携、データ交換させる接続性を有する車両や家電製品などのデバイスのネットワークである。ＩｏＴには、デスクトップ、ラップトップ、スマートフォン、およびタブレットなどの標準的なデバイスを超えて、従来はインターネットまたはネットワークに対応していなかった物理デバイスや日用品にまで、インターネットやその他のネットワークとの接続性を拡張することが含まれる。テクノロジーが組み込まれたこれらのデバイスは、インターネットまたはその他のネットワーク接続を通じて通信および連携でき、遠隔から監視、制御できる。
【０００４】
システムあるいはネットワークのセキュリティは、例えば、弱い管理パスワード、十分な暗号化の欠如、または不十分な物理的セキュリティといった最も弱いリンクに律則される。ネットワークとの接続性を有する小型でローパワーの組み込みエンドポイント、いわゆるモノのインターネット（ＩｏＴ）のキーエレメントが大量に出現した場合には、これらのデバイスが弱いリンクとなる。これらのデバイスの演算能力および帯域幅には制約があるため、従来の暗号化ソリューションを直接、適用することが不可能である。このため、これらのデバイスの使用が制限されるか、この弱点のためにシステム全体のセキュリティが危殆化する結果となる。
【０００５】
コンピューティングシステムでは、デバイスおよび／またはデバイスを動作させる人々（簡潔に「当事者」とする）のＩＤを検証し、当事者間で安全なデータ交換を実現するためのメカニズムが必要である。その目的は、２以上の当事者がデータ交換の予定された参加者であることを保証すること、外部の第三者が交換されたデータを判別できず検出しない限りデータを破壊できなくすること、にある。これは、様々な暗号化技術を応用することにより実現できる。埋め込み型センサノード、個人用監視デバイス、およびモノのインターネットを構成するその他のデバイスなどのテクノロジーにおいては、ユーザに信頼されると共にプライバシーやセキュリティに悪影響を与えることなく使用できる暗号化技術を利用する必要がある。
【０００６】
セキュリティを提供する従来の方法としては、例えば、事前共有鍵（ＰＳＫ）、鍵管理システム（ＫＭＳ）、および公開鍵暗号化がある。それぞれの方法は、暗号化データ交換の手段を提供するために使用され、認証されていない第三者にメッセージの内容が漏洩することを防いでいる。公開鍵基盤（ＰＫＩ）は、公開鍵管理を提供するインフラストラクチャである。ＰＫＩは、公開鍵暗号の管理を提供する。
【０００７】
ＰＳＫでは、適切な暗号化アルゴリズムを用いる暗号化の基礎として使用される共有秘密鍵または共有鍵について、当事者間で合意しておく必要がある。秘密鍵を所有している当事者は、他の当事者が送受信するメッセージを復号化／暗号化できるため、暗に参加が許可され、ＩＤ確認がさらに実施されることもない。未認証の当事者によって共有鍵が推測、盗難、またはその他の方法で作成された場合、データ交換のセキュリティが危殆化する。
【０００８】
ＫＭＳは、鍵を生成および共有するための、より洗練された方法をＰＳＫに導入することにより構築されている。この管理システムは、通信に使用される鍵の整合をとる。各当事者が一意の鍵（unique key）を持っている場合には、当事者を一意に識別できる。少数の当事者によって管理対象の鍵が使用されている場合であれば、危殆化した鍵の影響はＰＳＫよりも小さくなる。しかしながら、鍵が危殆化した場合には、ＫＭＳは、壊滅的な被害の中心座標（central coordination point）を提供してしまい、ＫＭＳを制御可能

な悪意のインサイダーの攻撃対象となるおそれがある。

【０００９】

ＰＫＩは、鍵ペアを使用することにより、ＰＳＫおよびＫＭＳを大幅に強化する。鍵ペアは、公開部分と秘密部分とで構成される。公開部分は、当事者間でオープンに交換でき、鍵ペアの秘密部分を所有する当事者を対象としたデータの暗号化、およびＩＤ確認のために使用できる。秘密部分を所有する当事者により、秘密部分の秘密が保たれる。公開鍵および関連するデジタル証明書を交換することにより、２の当事者は互いを特定でき、セキュア通信を確立できる。

【００１０】

一般に、公開鍵は、名前、組織、証明書の有効期間などの当事者に関する付加情報が含まれる証明書に統合されている。この証明書には、暗号化により生成された署名も含まれている。証明書の一部を変更するには、署名の変更が必要となる。ルートＣＡが証明書への署名を許可した中間認証局に対する証明書にルートＣＡが署名する、という署名チェーンを形成できる。ＣＡの公開鍵を所有し中間公開鍵および証明書を受信できる当事者は、提示された全ての証明書の整合性を検証できる。

【００１１】

公開鍵／秘密鍵、証明書、署名、ＣＡ、チェーン、および暗号検証の組み合わせにより、ＩＤ確認および安全なデータ交換を提供するためのより堅牢なメカニズムを提供できる。いずれの２の当事者も、一意のデータ交換を常に安全に行うことができる。秘密鍵が危殆化しない限り、他の当事者が別の当事者になりすますことは不可能である。

【００１２】

ＰＫＩの提供に関連する暗号化方式には、リベスト・シャミア・エーデルマン（Rivest-Shamir-Adleman、ＲＳＡ）、楕円曲線暗号（ＥＣＣ）、Ｘ．５０９形式の証明書、デジタル署名アルゴリズム（ＤＳＡ）、楕円曲線ＤＳＡ（ＥＣＤＳＡ）、ＳＳＬ／ＴＬＳプロトコル群が含まれる。

【００１３】

上記に加えて、一旦、ＰＫＩを使用してＩＤやセキュア通信が確立すると、ディフィー・ヘルマン鍵共有（ＤＨＥ）やＥＣＣベースの楕円曲線ディフィー・ヘルマン鍵共有（ＥＣＤＨＥ）などの対称鍵暗号メカニズムを通じて、さらに安全なセッションを確立できる。これらの対称セッションは、セッションを保護するために使用される鍵がＰＫＩ鍵に基づいていないという点で一時的なものとなる可能性がある。例えば、前方秘匿性（perfect forward secrecyに基づく短期鍵は、元のＰＫＩ鍵とは直接の関係がない。

【００１４】

従来の暗号化ソリューションは、インターネットプロトコル（ＩＰｖ４／ＩＰｖ６など）ネットワークを対象とする傾向がある。このようなネットワークは、フレームサイズの大きなデータ（例えば、１５００バイト以上）に対応でき、参加デバイスは、大容量のデータ転送および暗号化アルゴリズムを処理するための十分な処理能力を備えている。ＩｏＴネットワークのエンドポイントは、通常、これらの両面において、より制約されている。一例としては、ＬｏＲａ（長距離）トランシーバを備えた８ビットマイクロコントローラに基づくセンサノードがある。このデバイスには、実用的な公開鍵暗号化セキュリティを提供するために十分な演算能力がない。また、長距離ワイドエリアネットワーク（ＬｏＲａＷＡＮ）のフレームサイズ（例えば、５１－２２２バイト）では、たとえ最もコンパクトな識別符号化規則（ＤＥＲ）のバイナリ形式であっても、使用される典型的なＸ．５０９証明書（平均１．５キロバイトだが潜在的にはさらに大きい）の送信が制限される。

【００１５】

これらの制約のため、従来のＩｏＴデバイスは、ネットワーク全体で単一の鍵が使用される事前共有鍵（ＰＳＫ）ベースのセキュリティを実装している。単一のデバイス／鍵が危殆化すると、ネットワーク全体が危殆化してしまう。この危殆化を軽減するために、ネットワーク内のすべてのデバイス毎に一意の鍵が割り当てられる鍵管理システム（ＫＭＳ）を使用し得るが、ＫＭＳにはスケーラビリティの問題、インサイダー攻撃、静的な鍵攻

撃（static key attack）などの欠点がある。ハッキングや内部犯行により、これらの鍵が盗まれる場合もある。

【００１６】

したがって、相互認証、エンドツーエンドセキュリティ、動的セッション鍵、セキュリティポリシーの更新（証明書の更新など）、およびネットワーク内の危殆化した他のデバイスからの保護を提供する新しいセキュリティメカニズムが必要である。

【００１７】

ローパワーのコンピューティングリソース（ＡＶＲ、ＡＲＭ Ｃｏｒｔｅｘ Ｍ０／Ｍ３／Ｍ４、ＴＩ ＭＳＰ４３０、およびその他同様のデバイスなど）上で稼働し、Ｂｌｕｅｔｏｏｔｈ、Ｚｉｇｂｅｅ、ＬｏＲａＷＡＮ、ＬｏＲａ、ＮＢＩｏＴ、ＺＷａｖｅなどの制約付きプロトコルを通じて通信する制約付きＩｏＴデバイスでは、セッション鍵を証明書と交換することによるアプリケーション層／トランスポート層／ネットワーク層を実現できず、前方秘匿性を効果的な方法で実現できない。主要な懸念事項の１つは、異種のアプリケーションおよび環境では単一のセキュリティプロトコルを容易に統合できないことに起因してソリューションのサイロ化が発生し、その結果、管理が困難になりセキュリティの脆弱性が誘発されることである。このようなシステムには、遠隔からの無線による証明書のコミッショニング、プロビジョニング、更新、および失効が、遠隔システムでは面倒である、という他の問題がある。

【００１８】

制約のあるデバイスだけがスケーラビリティの問題を有するわけではない。膨大な数のデバイスが展開されたネットワークでは、従来のセキュリティスキームが適応できずにネットワークを占有し、スループットのボトルネックとなるおそれがある。さらに、デバイスの数が増えるにつれて、デバイスのライフサイクル管理および証明書管理が大きな問題となる。

【発明の概要】

【００１９】

１または複数の態様の基本的な理解を提供するために、簡略化された概要を提示する。この概要は、考えられる全ての態様の包括的な概要ではなく、また、全ての態様の主要な要素または重要な要素を特定したり、一部または全ての態様の範囲を定めたりすることを意図するものではない。その唯一の目的は、後述のより詳細な説明の前置きとして、１または複数の態様のいくつかの概念を簡略化された形式で提示することにある。

【００２０】

本開示の一態様では、Ｍｉｃｒｏ－ＰＫＩ技術が提供される。Ｍｉｃｒｏ－ＰＫＩ技術は、リソースおよび帯域幅に制約のあるＩｏＴデバイスにおいて公開鍵基盤を有効にし得る可能性がある。従来のＸ．５０９証明書よりも実質的に小さいサイズの証明書（例えば、従来のＸ．５０９証明書のサイズの１０％未満）を利用して、公開鍵基盤をＩｏＴネットワークプラットフォームに展開できる。この証明書は、マイクロ証明書と呼ばれることもある。マイクロ証明書のサイズを縮小するために、点圧縮方法（point compression method）やルックアップテーブルベースのスキームを策定することも良い。このスキームでは、マイクロ証明書の別のフィールドを利用して証明書のタイプおよび証明書が保持するさまざまなパラメータに関する情報を提供できる。このため、マイクロ証明書は、Ｘ．５０９標準とは直接の互換性がないが、例えば、従来のＩＴシステムとＩｏＴエンドポイントのセグメントとを組み合わせた基盤においてＸ．５０９と共存できる柔軟性を具備し得る。プロトコルコンバータを使用すれば、Ｘ．５０９証明書からマイクロ証明書への変換、またはその逆の変換が可能である。同様に、プロトコルコンバータを使用して、Ｍｉｃｒｏ－ＰＫＩと従来のＰＫＩネットワークとの間でディフィー・ヘルマン（Diffie-Hellman）セッションを維持することもできる。マイクロ証明書は、Ｘ．５０９と同様の暗号化スキーム（同様の公開鍵サイズ、同様のＥＣＣ曲線、および同様のハッシュアルゴリズム）を利用するため、Ｘ．５０９証明書で可能なレベルと同等のセキュリティレベルを提供し得る。

【００２１】
本開示の別の態様では、方法、コンピュータ可読媒体、およびデータ通信のための装置が提供される。装置は、トランスポート層またはアプリケーション層のセキュリティを提供するマイクロ公開鍵基盤内のマイクロ証明書を使用して、データ通信セッションの当事者を認証できる。マイクロ公開鍵基盤は、通信プロトコル、マイクロ証明書、および管理プラットフォームの組み合わせであっても良い。データ通信セッションの少なくとも１の当事者は、リソースおよび／または帯域幅に制約のあるデバイスであり得る。いくつかの実施形態では、証明書交換、鍵交換、暗号化データなどのセキュリティ機能が基盤（underlying）のデータペイロードおよびペイロードの送信速度に対して多大な負荷を追加するネットワーク技術に、帯域幅の制約が関連し得る。装置は、マイクロ証明書を使用してデータ通信セッションを確立できる。装置は、データ通信セッションを介して安全なデータ通信を実行できる。
【００２２】
本開示のさらに別の態様では、安全な通信のための方法、コンピュータ可読媒体、および装置が提供される。装置は、コンピューティングデバイスであっても良い。装置は、マイクロ証明書署名要求を生成できる。装置は、マイクロ証明書署名要求を認証局に送信できる。装置は、マイクロ証明書署名要求に対する認証局からの応答を受信できる。装置は、応答に基づいて、認証局によって署名されたマイクロ証明書を再作成できる。マイクロ証明書は、楕円曲線暗号を利用できる。
【００２３】
本開示のさらに別の態様では、安全な通信のための方法、コンピュータ可読媒体、および装置が提供される。装置は認証局であっても良い。装置は、コンピューティングデバイスからマイクロ証明書署名要求を受信できる。装置は、マイクロ証明書署名要求に対する応答を生成できる。応答を生成するために、装置は、マイクロ証明書署名要求を検証し、マイクロ証明書に署名し、署名されたマイクロ証明書に基づいて応答を作成できる。装置は、コンピューティングデバイスに応答を送信できる。装置によって署名されたマイクロ証明書は、応答に基づいて再作成され得る。マイクロ証明書は、楕円曲線暗号を利用できる。
【００２４】
前述および関連する目的を達成するために、１または複数の態様は、以下で十分に説明され個別に特許請求の範囲で示される特徴を含んでいる。以下の詳細な説明および添付の図面は、１または複数の態様の特定の例示的な特徴を詳細に説明している。しかしながら、これらの特徴は、様々な態様の原理が採用され得る様々な方法のうちのいくつかを示しているに過ぎず、この詳細な説明は、そのような全ての態様およびそれらの均等物を含むことを意図している。
【図面の簡単な説明】
【００２５】
【図１】図１は、多層セキュリティアーキテクチャの例を示す図である。
【００２６】
【図２】図２は、エンドツーエンドセキュリティアーキテクチャの例を示す図である。
【００２７】
【図３】図３は、Ｍｉｃｒｏ－ＰＫＩソフトウェア開発キットの統合の例を示す図である。
【００２８】
【図４】図４は、Ｍｉｃｒｏ－ＰＫＩとネットワーク技術との統合の例の拡張図である。
【００２９】
【図５】図５は、Ｍｉｃｒｏ－ＰＫＩ通信プロトコルの例示的なメッセージフォーマットを示す図である。
【００３０】
【図６】図６は、Ｍｉｃｒｏ－ＰＫＩで保護されたセッションをセットアップするための情報フローの例を示す図である。

【００３１】
【図７】図７は、Ｍｉｃｒｏ－ＰＫＩおよび自動証明書管理環境（Automated Certificate Management Environment）のアーキテクチャの概要を示す図である。
【００３２】
【図８】図８は、マイクロ証明書要求および署名フローの例を示す図である。
【００３３】
【図９】図９は、データ通信方法のフローチャートである。
【００３４】
【図１０】図１０は、マイクロ証明書の更新方法のフローチャートである。
【００３５】
【図１１】図１１は、例示的な装置における異なる手段／コンポーネント間のデータフローを示す概念的なデータフロー図である。
【００３６】
【図１２】図１２は、処理システムを採用する装置へのハードウェア実装例を示す図である。
【００３７】
【図１３】図１３は、証明書の生成および処理方法のフローチャートである。
【００３８】
【図１４】図１４は、例示的な装置における異なる手段／コンポーネント間のデータフローを示す概念的なデータフロー図である。
【００３９】
【図１５】図１５は、処理システムを採用する装置へのハードウェア実装例を示す図である。
【発明を実施するための形態】
【００４０】
添付の図面に関連して以下に記載される詳細な説明は、様々な構成の説明として意図されており、本明細書に記載の概念が実施され得る唯一の構成を表すことを意図するものではない。詳細な説明には、さまざまな概念を完全に理解するための具体的な詳細が含まれている。しかしながら、当業者には、これらの概念が具体的な詳細が無くても実施され得ることが明らかである。いくつかの場合には、これらの概念が不明瞭になることを避けるために、公知の構造およびコンポーネントがブロック図の形で示されている。
【００４１】
組み込みシステムのネットワークのための公開鍵基盤のいくつかの態様が、さまざまな装置および方法を参照して提示される。これらの装置および方法は、以下の詳細な説明で説明され、様々なブロック、コンポーネント、回路、プロセス、アルゴリズムなど（総称して「要素」と呼ぶ）、によって添付の図面に示される。これらの要素は、電子的なハードウェア、コンピュータソフトウェア、またはそれらの任意の組み合わせとして実装されていても良い。これらの要素がハードウェアとして実装されるかソフトウェアとして実装されるかは、個別のアプリケーションおよびシステム全体に課せられた設計上の制約によって決まる。
【００４２】
一例として、要素、要素の任意の部分、または要素の任意の組み合わせは、１または複数のプロセッサを含む「処理システム」として実装され得る。プロセッサの例としては、マイクロプロセッサ、マイクロコントローラ、グラフィックス処理装置（ＧＰＵｓ）、中央処理装置（ＣＰＵｓ）、アプリケーションプロセッサ、デジタルシグナルプロセッサ（ＤＳＰｓ）、縮小命令セットコンピューティング（ＲＩＳＣ）プロセッサ、システムオンチップ（ＳｏＣ）、ベースバンドプロセッサ、フィールドプログラマブルゲートアレイ（ＦＰＧＡｓ）、プログラマブルロジックデバイス（ＰＬＤｓ）、ステートマシン、論理ゲート、ディスクリートハードウェア回路、および本開示の全体を通して説明される様々な機能を実行するように構成された他の適切なハードウェアが含まれる。処理システムの１

または複数のプロセッサがソフトウェアを実行する場合がある。ソフトウェアは、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、ハードウェア記述言語などと呼ばれるか否かに関わらず、命令、命令セット、コード、コードセグメント、プログラムコード、プログラム、サブプログラム、ソフトウェアコンポーネント、アプリケーション、ソフトウェアアプリケーション、ソフトウェアパッケージ、ルーチン、サブルーチン、オブジェクト、実行可能ファイル、実行スレッド、プロシージャ、関数などを意味するもの、と広く解釈できる。

【００４３】

したがって、１または複数の例示的な実施形態では、説明された各機能が、ハードウェア、ソフトウェア、またはそれらの任意の組み合わせにより実装され得る。ソフトウェアにより実装される場合、各機能は、１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格納またはエンコードされ得る。コンピュータ可読媒体には、コンピュータ記憶媒体が含まれる。記憶媒体は、コンピュータがアクセスできる任意の利用可能な媒体であれば良い。限定ではなく例示を目的として、このようなコンピュータ可読媒体は、ランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、フラッシュメモリ、光ディスク記憶装置、磁気ディスクストレージ、他の磁気ストレージデバイス、前述のタイプのコンピュータ可読媒体の組み合わせ、または、コンピュータがアクセスできる命令またはデータ構造の形式のコンピュータ実行可能コードを格納するために使用できる他の媒体を含んでいても良い。

【００４４】

この開示の目的は、認証、安全なセッション、およびセキュリティ管理機能を、リモートデバイスに提供することである。小さなデジタルマイクロ証明書は、相互認証または一方向認証のいずれかに使用でき、暗号化および復号化機能用の一意の鍵を使用してセッションを開始するために使用される。セッションは、層状またはエンドツーエンドで保護されたアーキテクチャにおいて提供される場合がある。セキュリティ管理コンポーネントは、デバイス上のマイクロ証明書のコミッショニング、管理、更新、および失効を実現する場合もある。セキュリティ管理コンポーネントは、セキュリティの管理を担当する場合もある。

【００４５】

本開示のいくつかの実施形態は、制約された演算能力を有すると共に帯域幅および／または通信時間が制限されたネットワークを通じて通信する深く組み込まれたデバイスのための公開鍵基盤を提供する。これにより、ＩＤ確認、暗号化通信、およびデバイスのライフサイクル管理に関するデバイスのセキュリティ機能が、従来の方法と比較して大幅に向上する。

【００４６】

この開示の主な目的は、マイクロ証明書の設計を通じて、ＰＡＮ（パーソナルエリアネットワーク）、ＬＰ－ＷＡＮ（低消費電力ワイドエリアネットワーク）、ボディエリアネットワーク（ＢＡＮ）タイプのネットワークあるいは同様のネットワークで容易に使用できるサイズに、証明書の長さを短縮することである。いくつかの実施形態では、ＥＣＣを使用して主な目的を達成できる。本開示の別の包括的な目的は、ＩｏＴデバイス上で実行できる効率的なＰＫＩ（Ｍｉｃｒｏ－ＰＫＩと呼ばれる場合がある）の基礎としてマイクロ証明書およびＥＣＣを使用することである。さらに、証明書の交換、安全なセッションの作成、およびその他のＰＫＩ関連のアクティビティ用のプロトコルが提供される。このプロトコルは、低帯域幅のＰＡＮ／ＬＰ－ＷＡＮ／ＢＡＮネットワークまたは同様のネットワークにおいて低消費電力のＩｏＴデバイスまたは同様のデバイスを使用して効率的に稼働するように設計されている。このプロトコルと、サーバ側のアーキテクチャおよび登録プロトコルと、を組み合わせれば、サイズ効率の高い証明書更新方法を有するＩｏＴデバイス向けの証明書およびライフサイクル管理、という本開示の別の目的を達成できる。

【００４７】

Ｍｉｃｒｏ－ＰＫＩ技術は、リソースおよび帯域幅に制約のあるＩｏＴデバイスにおい

て公開鍵基盤を有効にする可能性がある。従来のＸ．５０９証明書よりも実質的に小さいサイズの証明書（例えば、従来のＸ．５０９証明書のサイズの１０％未満）を利用して、ＩｏＴネットワークプラットフォームに公開鍵基盤を展開できる。この証明書は、マイクロ証明書と呼ばれることもある。証明書のサイズを縮小するために、点圧縮方法およびルックアップテーブルベースのスキームを策定することも良い。このスキームは、マイクロ証明書の別のフィールドを利用して証明書のタイプ、および証明書が保持するさまざまなパラメータに関する情報を提供する場合がある。このため、マイクロ証明書は、Ｘ．５０９標準との互換性がないが、例えば従来のＩＴシステムとＩｏＴエンドポイントのセグメントとを組み合わせた基盤においてＸ．５０９と共存できる柔軟性を備えていても良い。プロトコルコンバータを使用して、Ｘ．５０９証明書からマイクロ証明書への変換、およびその逆の変換が可能である。同様に、プロトコルコンバータを使用すれば、Ｍｉｃｒｏ－ＰＫＩと従来のＰＫＩネットワークとの間でディフィー・ヘルマンセッションを維持できる。マイクロ証明書は、Ｘ．５０９と同様の暗号化スキーム（例えば、同様の公開鍵サイズ、同様のＥＣＣ曲線、および同様のハッシュアルゴリズム）を利用する。このため、マイクロ証明書は、Ｘ．５０９証明書で可能なレベルと同等のセキュリティレベルを提供し得る。

【００４８】

セキュリティ基盤を調整するために、ネットワーク内のセキュリティメカニズム全体の動作を取り扱う管理スキームを提供することも良い。これには、ネットワーク内の認証済みノードに関する情報、それらの証明書、およびルート証明書情報の提供が含まれる。管理機能には、証明書の失効（ブラックリスト）および証明書の更新が含まれることもある。証明書登録プロトコル（ＣＥＰ）を使用してデバイス内の最初の証明書をプロビジョニングすることができる一方、自動証明書管理環境およびシステム（Automated Certificate Management Environment & System、ＡＣＭＳ）を使用して更新や失効を含む証明書の管理が可能となる。

【００４９】

Ｍｉｃｒｏ－ＰＫＩは、最適化された公開鍵基盤を利用することで、制約のあるＩｏＴデバイスで多く使用されるＰＳＫや同様のアプローチよりも優れたセキュリティを提供できる。各デバイスには、一意のマイクロ証明書が発行される場合がある。事前共有鍵を使用する代わりに、デバイスは、データ送信において一意の短期セッション鍵を使用する。セッション鍵は、全てのセッションについてセッションごとに動的に生成される場合やデバイスごとに異なる場合がある。したがって、セッション鍵が危殆化したとしても、その特定のデバイスの特定のセッションが危殆化するだけである。同様に、デバイスの秘密鍵の危殆化は、単一のデバイスのトラフィックにのみ影響する。Ｍｉｃｒｏ－ＰＫＩは、無線コマンドによるマイクロ証明書の遠隔更新が可能となる自動証明書管理環境を利用する。これにより、マイクロ証明書のプロビジョニング、失効、および更新が可能になる。現時点において安全なインターネット全体がＰＫＩに基づいていることから、ＰＫＩが成功することは証明されている。したがって、Ｍｉｃｒｏ－ＰＫＩによれば、制約のあるＩｏＴデバイスが容易に適応でき、対処できるようになる。

【００５０】

Ｍｉｃｒｏ－ＰＫＩは、多層セキュリティアーキテクチャおよびエンドツーエンドセキュリティアーキテクチャの２つの異なるアーキテクチャをサポートし得る。多層セキュリティアーキテクチャにおけるセキュリティは、センサと中間装置との間に存在し、次に中間装置とデータ／オペレーションセンタとの間に存在する。図１は、多層セキュリティアーキテクチャの一例を示すダイアグラム１００である。同図の例示では、多層セキュリティアーキテクチャは、センサ１０２とゲートウェイ１０４との間の第１のセキュリティ層、および、ゲートウェイ１０４とデータセンタ１０６との間の第２のセキュリティ層、の２つの層を含み得る。各通信ペアは、異なる方法を使用して保護される。例えば、センサ１０２とゲートウェイ１０４との間の通信はＭｉｃｒｏ－ＰＫＩ基盤を利用して保護される一方、ゲートウェイ１０４とデータセンタ１０６との間の通信はＸ．５０９証明書ベー

スの基盤を利用して保護される。この通信セキュリティの形式は、センサ１０２およびゲートウェイ１０４がプライベートネットワーク上に配置されているか、あるいは安全な実行環境を有する場合に利用できる。センサ１０２はまた、Ｍｉｃｒｏ－ＰＫＩ基盤の使用を通じて他のセンサ１０２との安全な接続を開始できる。これにより、機器間通信またはピアツーピア通信において、マイクロ証明書の使用を通じたＭｉｃｒｏ－ＰＫＩを介してエッジデバイスを保護できる。ゲートウェイ１０４の物理セキュリティおよびソフトウェアセキュリティは、Ｍｉｃｒｏ－ＰＫＩおよびＸ．５０９基盤の両方に実装されたセキュリティの完全性にとって極めて重要である。

【００５１】

上記の例および本開示全体を通してセンサが図示され説明されているが、当業者であれば、他の任意のＩｏＴデバイス（例えば、アクチュエータなど）が開示の目標または目的から逸脱することなく代わりに使用できることを認識できる。

【００５２】

図２は、エンドツーエンドセキュリティアーキテクチャの一例を示すダイアグラム２００である。同図の例示では、センサ２０４とデータセンタ２０６との間でＭｉｃｒｏ－ＰＫＩが利用される。これは、センサ２０４からデータセンタ２０６までに亘ってデータが保護されていることを意味する。この通信セキュリティの形式は、センサ２０４あるいはゲートウェイ２０８が共有ネットワーク上に配置されている場合、またはエンドポイント（例えば、センサ２０４）とデータセンタ２０６との間のメッセージの転送を担当するゲートウェイ２０８などの中間装置にセキュリティ上の不安がある場合、に利用される。

【００５３】

いくつかの実施形態では、Ｍｉｃｒｏ－ＰＫＩは、既存のシステムのソフトウェアおよびハードウェアアーキテクチャに組み込み可能に設計でき、実装時の最小限の労力でそのセキュリティ上の利点を提供できる。Ｍｉｃｒｏ－ＰＫＩは、ソフトウェア開発キット（ＳＤＫ）を通じて組み込みＩｏＴデバイスに統合できる。ＳＤＫは、アプリケーションコード（センサデータ収集など）とネットワーク通信コード（無線送信など）との間に位置していることも良い。そうすることで、ＳＤＫは、さまざまな無線技術およびＩｏＴアプリケーションを直ちにサポートできる。したがって、ＳＤＫは、既存のどんなアプリケーションとでも簡単に統合できるだけでなく、新しいアプリケーションのソフトウェアアーキテクチャに組み込むことができる。ソフトウェアアーキテクチャ内におけるこのような位置づけにより、Ｍｉｃｒｏ－ＰＫＩは、適用されるネットワークレベルのセキュリティに依存しなくなる。したがって、Ｍｉｃｒｏ－ＰＫＩは、ローレベルの方法と並行して追加セキュリティを提供し得る。Ｍｉｃｒｏ－ＰＫＩは、これらのローレベルのセキュリティ実装で発生する欠陥の影響を受けず、他には共通のセキュリティ実装を共有していない複数のネットワーク技術間で動作し得る。

【００５４】

図３は、Ｍｉｃｒｏ－ＰＫＩ　ＳＤＫ統合の一例を示すダイアグラム３００である。同図の例示では、Ｍｉｃｒｏ－ＰＫＩを有しないデバイス３０２は、ネットワークソフトウェア層３０６およびアプリケーションソフトウェア層３０８を含み得る。Ｍｉｃｒｏ－ＰＫＩは、ＳＤＫ（例えば、Ｍｉｃｒｏ－ＰＫＩ層３１０）を介してデバイス３０２に統合され得る。Ｍｉｃｒｏ－ＰＫＩ層３１０は、ネットワークソフトウェア層３０６とアプリケーションソフトウェア層３０８との間に位置し得る。

【００５５】

図４は、Ｍｉｃｒｏ－ＰＫＩとネットワーク技術との統合例の拡張図である。同図の例示では、Ｍｉｃｒｏ－ＰＫＩは、ＳＤＫ（例えば、Ｍｉｃｒｏ－ＰＫＩ層４１０）を介してデバイスに統合され得る。Ｍｉｃｒｏ－ＰＫＩ層４１０は、ネットワークソフトウェア層４０６とアプリケーションソフトウェア層４０８との間に位置し得る。

【００５６】

サーバ側では、Ｍｉｃｒｏ－ＰＫＩがサービスを介して統合される。メッセージがサービスに対して送信され、それによって応答が生成および送信されたり、データが暗号化／

復号化されたりする場合がある。このサービスは、データの利用ポイントと緊密に統合するように設計され得る。データの利用ポイントは、例えば、データが格納、分析、または変換されるポイントであり、ユーザのデータセンタ、プライベートクラウドサービス、または同等の主権（sovereignty）およびセキュリティを備えたＩＴシステム内に存在し得る。

【００５７】

Ｍｉｃｒｏ－ＰＫＩ通信プロトコルは、安全なセッションを確立し、そのセッションを通じてデータ送信するために２の当事者間でのメッセージ交換を目的として設計されており、ネットワークに依存しないものである。Ｍｉｃｒｏ－ＰＫＩの他のすべての目的と同様に、Ｍｉｃｒｏ－ＰＫＩ通信プロトコルは、処理およびネットワークのオーバーヘッドを最小限に抑えるように設計されている。

【００５８】

図５は、Ｍｉｃｒｏ－ＰＫＩ通信プロトコルの例示的なメッセージフォーマットを示すダイアグラム５００である。同図の例示では、Ｍｉｃｒｏ－ＰＫＩ通信プロトコルのパケットは、メッセージタイプ識別子フィールド５０４およびメッセージフィールド５１０を含み得る。メッセージフィールド５１０は、任意の長さのペイロードを有し得る。このパケットは、暗号化表示フィールド５０２、識別子拡張フィールド５０６、およびカウンタフィールド５０８を任意に含み得る。

【００５９】

いくつかの実施形態では、Ｍｉｃｒｏ－ＰＫＩ通信プロトコルは、メッセージタイプ識別子フィールド５０４を介して他の情報を推測できるため、１バイトのメッセージタイプ識別子フィールド５０４を利用して効率化を達成でき、ヘッダサイズを最小化できる。メッセージタイプ識別子フィールド５０４は各パケットの内容が何であるかを示すことができ、その用途は２の当事者間のセッションの状態に依存し得る。メッセージタイプには、証明書交換、セッション鍵交換、証明書への署名、およびその他の制御関連メッセージが含まれるが、これらに限定されない。メッセージタイプ識別子フィールド５０４は、メッセージ長を定義しなくても良い。証明書などのメッセージの内容自体が、メッセージ固有の追加の識別子、または明示的な長さの符号化のいずれかを通じて、メッセージの長さを決定するのに十分な情報を提供する場合がある。基盤となるネットワークのパケット形式はヘッダを含むメッセージ全体の長さも記述できるので、冗長な長さの符号化を最小限に抑えることができる。将来の拡張を可能にするために、メッセージタイプ識別子フィールド５０４は、識別子拡張フィールド５０６を通じて拡張可能である。

【００６０】

暗号化表示フィールド５０２およびカウンタフィールド５０８の２つのオプションフィールドを規定することができる。暗号化表示フィールド５０２は、安全なセッションのセットアップにおけるプライバシーを高めるためにメッセージの内容を暗号化することが可能である。カウンタフィールド５０８は、再送信およびメッセージの順序付けを支援できる。

【００６１】

いくつかの実施形態では、Ｍｉｃｒｏ－ＰＫＩは配信保証を必要としない。Ｍｉｃｒｏ－ＰＫＩへのソフトウェアインターフェイスでは、例えばアプリケーションおよびネットワークの適切な遅延の後などに、受信パケットがゼロである旨が報知される。そして、データの再送信または状態の変更が必要かどうかが内部で決定される。基盤（underlying）となるネットワークが配信保証をサポートしている場合、Ｍｉｃｒｏ－ＰＫＩはその恩恵を受け得る。したがって、Ｍｉｃｒｏ－ＰＫＩが稼働する抽象化レベルにより、Ｍｉｃｒｏ－ＰＫＩは損失のあるシナリオおよび損失のないシナリオの両方で機能し得る。

【００６２】

いくつかの実施形態では、Ｍｉｃｒｏ－ＰＫＩは、必要に応じて前方秘匿性（ＰＦＳ）をサポートし得る。ＰＦＳは、２つの通信当事者の証明書と保護されたセッションとを切り離す。一意の短期鍵ペアが各当事者によって生成されてその公開部分が共有され、秘密

部分自体を送信することなく共通の共有秘密鍵を導出するために公開部分が使用される場合がある。当事者の証明書は、交換された情報に署名してその出所や有効性を保証するためにのみ使用される。共有秘密鍵は、どちらの当事者の秘密鍵にもまったく関係がない。

【００６３】

共有秘密鍵は、例えば、高度暗号化標準（ＡＥＳ）ブロック暗号およびストリーム暗号アルゴリズム、または同等のアルゴリズムによって提供されるセッションなど、対称的に暗号化されたセッションの鍵として使用できる。データ送信の時間およびデータ量の両方の観点から、攻撃者が共有秘密鍵を推測または取得する機会を最小限に抑えるためにセッション期間が制限される場合がある。ＩｏＴデバイスの消費電力を最小限に抑えるように、手動または自動によりセッション期間を構成することも良い。共有秘密鍵を危殆化するために要する労力を非常に高くできると共に、たとえ危殆化が発生したとしても、そのセッションのみに危殆化を抑えることができるようになる。過去または将来の全てのセッションは、独自の短期鍵および共有秘密鍵を有しているため、保護された状態に維持でき、これにより、前方秘匿性を獲得できる。

【００６４】

共有秘密鍵は、２の通信当事者間で維持される場合がある。したがって、鍵管理におけるスケーリングの問題はなく、ＰＫＩモデルを通じた通信の検証が引き続き提供される。ＥＣＣは、マイクロ証明書と同様に、鍵サイズを小さく保ちつつ、ＰＡＮ／ＢＡＮ／ＬＰ－ＷＡＮまたはその他の制約のあるネットワークとの互換性を保ちながら、短期鍵の交換において使用され得る。

【００６５】

ＰＦＳが要求されない場合には、他の方法を使用して安全なセッションを確立できる。ランダムに生成された共有秘密鍵が、受信者の公開鍵により暗号化され転送中に当事者間で通信される場合がある。この秘密鍵は、対称暗号化された安全なセッションのための鍵として使用される。

【００６６】

双方向通信では、各当事者が共有秘密鍵の半分を提供し、相手方から受け取った共有秘密鍵から全体の秘密鍵を作成できる。一方向通信（メッセージを送信できるが受信できないセンサなど）では、前述のように、送信者が、秘密鍵を提供し、受信者の公開鍵を使用して秘密鍵を安全に共有する。このような場合、エンドポイントの証明書は、受信者の証明書と同様に静的である。受信サーバのセキュリティが維持されていれば、当事者間の信頼が保護される。証明書を信頼することを止めてデバイスからの通信を無視することにより、そのデバイスを退役させる、といったデバイスのライフサイクル管理が引き続き可能である。

【００６７】

図６は、Ｍｉｃｒｏ－ＰＫＩで保護されたセッションをセットアップするための情報フローの例を示すダイアグラム６００である。同図の例示では、６１０および６１２において、エンドポイントデバイス６０２およびＭｉｃｒｏ－ＰＫＩサービス６０４は、証明書を交換および検証できる。６１４および６１６において、エンドポイントデバイス６０２およびＭｉｃｒｏ－ＰＫＩサービス６０４は、セッション秘密鍵またはＰＦＳ短期鍵を交換できる。６１８において、エンドポイントデバイス６０２は、暗号化されたデータをＭｉｃｒｏ－ＰＫＩサービス６０４に対して任意に送信できる。６２０において、Ｍｉｃｒｏ－ＰＫＩサービス６０４は、暗号化されたデータをエンドポイントデバイス６０２に対して任意に送信できる。上記のように列挙された各方法では、Ｍｉｃｒｏ－ＰＫＩのさまざまな動作態様を通じて、両当事者の信頼を保護しつつ、可能な場合には前方秘匿性を使用して、双方向および一方向の通信シナリオに対応できることが示されている。

【００６８】

いくつかの実施形態では、Ｍｉｃｒｏ－ＰＫＩの使用を開始するために、デバイスを管理システムに登録する必要がある。デバイスのコミッショナ（commissioner）は、プログラムされる時点で（現場（field）あるいは出荷前に）、デバイスに証明書をインストー

ルする。コミッショニング証明書は、安全なセッションを確立して新しいＣＳＲを実行するためにのみ使用されるようにその使用が制限される場合がある。この「最初に使用される」ＣＳＲの受け入れを自動化することもできるし、管理システムを介して手動で行うこともできる。

【００６９】

いくつかの実施形態では、自動証明書管理環境が、証明書の更新のトリガ、および古い証明書の失効の取り扱いを担当する。Ｍｉｃｒｏ－ＰＫＩの場合、ＡＣＭＳと交換されるメッセージは、ローパワー、低帯域幅の要求に合わせて小さいままにする必要がある。

【００７０】

データセンタ側では、デバイスの証明書が有効であるが期限切れ（out of date）であると考えられる場合に、更新命令がデバイスに送信され得る。次に、デバイスは、新しい鍵ペアを生成してＣＳＲを作成し、データセンタサーバに返すことができる。次に、サーバは、署名された情報を検証してデバイスに返すために、ＣＡとの間でＣＳＲを通信し得る。同様に、サーバ自体の証明書の有効期限が切れた場合、ＣＡとの間で同じ更新メカニズムにしたがっても良い。有効期限に基づく更新に加えて、例えば組織によるセキュリティポリシーの変更などに対応する恣意的な更新や、特定のデバイスに関する懸念のための更新を、トリガーするため、管理フレームワークを利用可能である。

【００７１】

特定のＩｏＴデバイスのセキュリティを更新するために、無線（ＯＴＡ）による安全な方法で遠隔からマイクロ証明書が送信される場合がある。各デバイスは、次に証明書署名要求（ＣＳＲ）として渡される独自の秘密鍵－公開鍵ペアを生成する機能を有している。次に、ＣＳＲに基づいてマイクロ証明書を発行する認証局（ＣＡ）サーバに対してＣＳＲが渡される。次に、新しいマイクロ証明書が元のデバイスにインストールされる。ＣＡは、アプリケーションプログラミングインターフェイス（ＡＰＩ）を介してアクセス可能であり、アクセス制御メカニズムによって保護されている。暗号化手順において使用される鍵は、ハードウェアセキュリティモジュールまたは安全な要素内のストレージによってさらに保護される。

【００７２】

図７は、Ｍｉｃｒｏ－ＰＫＩおよびＡＣＭＳのアーキテクチャの概要を示すダイアグラム７００である。図７では、ＣＳＲ要求および応答全体のバックグラウンドで生ずる動作の例が示されている。同図の例示では、デバイス（例えば、組み込みデバイス７０２）は、秘密鍵－公開鍵ペアを生成し、対応するＣＳＲをゲートウェイ７０４に渡すことができる。ゲートウェイ７０４は、Ｍｉｃｒｏ－ＰＫＩサービスを提供できるデータセンタ７０６にＣＳＲを渡すことができる。データセンタ７０６は、ステータスおよび制御情報をＡＣＭＳ７０８と交換できる。

【００７３】

データセンタ７０６は、ＣＡサーバＡＰＩ７１０にＣＳＲを渡すことができる。次に、ＣＡサーバＡＰＩ７１０は、アクセス制御モジュール７１２にＣＳＲを渡して認証させることができる。認証されたＣＳＲは、ＣＡサーバ７１４に渡される。ＣＡサーバ７１４は、ＣＳＲに署名して証明書を生成できる。生成された証明書は、署名された証明書を検証するためにアクセス制御モジュール７１２に渡される。次に、アクセス制御モジュール７１２は、署名された証明書をＣＡサーバＡＰＩ７１０を介してデータセンタ７０６に渡すことができる。データセンタ７０６は、署名された証明書をゲートウェイ７０４に渡すことができ、ゲートウェイ７０４は、次に、署名された証明書をデバイス（例えば、組み込みデバイス７０２）に渡すことができる。デバイスは、新しい証明書をインストールするか、あるいは以前の証明書を更新できる。

【００７４】

マイクロ証明書は、Ｍｉｃｒｏ－ＰＫＩの効率化に不可欠である。マイクロ証明書の形式は、従来の証明書形式と比較して非常に小さいサイズを維持する一方で、複数の楕円曲線および署名タイプをサポートできる。マイクロ証明書には、証明書識別子、発行者識別

子、発行日、有効期間、デバイス識別子、組織識別子、ネットワーク識別子、ＥＣＣ曲線識別子、署名識別子、公開鍵、および署名が含まれていても良い。マイクロ証明書には、中間ＣＡサーバの署名チェーンをサポートするための追加パラメータが含まれていても良い。

【００７５】

いくつかの実施形態では、マイクロ証明書の様々な識別子は、それらのサイズを最小化するために、テキストベースではなく数値であり得る。いくつかの実施形態では、すべての識別子は、それらの目的に適切なサイズに調整され得る。これは、多くのフィールドのサイズがオープンエンドであるためにＩｏＴや同様のユースケースには適していない通常の証明書とは対照的である。これらの識別子は、管理や従来のＰＫＩとの共存を容易にするために、他のシステムのテキストベースの識別子または同等物にマッピングされる場合がある。このマッピングはデータセンタで維持されるので、デバイスやその低帯域幅ネットワークに負担をかけないようにできる。いくつかの実施形態では、楕円曲線上の点（elliptic curve data points）に対して圧縮を実行する点圧縮技術（point compression technique）によって、さらなるサイズ縮小が実現され得る。この技術は、マイクロ証明書において公開鍵を表すために任意に使用できる。

【００７６】

いくつかの実施形態では、マイクロ証明書署名要求（Ｍｉｃｒｏ－ＣＳＲ）は、マイクロ証明書と同じアプローチに従うことができるが、ＣＡによって提供される部分、すなわち、発行者、日付、および期間を含むことなく構成できる。Ｍｉｃｒｏ－ＣＳＲは、Ｍｉｃｒｏ－ＣＳＲの作成者が鍵ペアを生成したことを検証するために署名を保持しても良い。ＣＡにより署名がされると、ＣＡは、デバイスが署名された証明書を再構築するために必要な部分のみを含むさらに最適化された応答を任意に返すことができる。これにより、デバイスがすでに所有している部分の再送信を回避できる。

【００７７】

図８は、マイクロ証明書要求および署名フローの例を示すダイアグラム８００である。同図の例示では、デバイス８０２は、新しいマイクロ証明書の検証および署名をＣＡ８０４に要求する。

【００７８】

デバイス８０２は、新しい証明書の必要性を検出したときに、マイクロ証明書要求および署名手順を開始できる。８０８において、デバイス８０２は、ＣＳＲ８１０を生成できる。デバイス８０２は、Ｍｉｃｒｏ－ＰＫＩおよびネットワーク基盤を介してＣＡ８０４にＣＳＲ８１０を送信できる。８１２において、ＣＡ８０４は、ＣＳＲを検証および署名してＣＳＲに対する応答８１４を生成できる。応答８１４は、署名および追加フィールドを含んでいても良い。ＣＡ８０４は、Ｍｉｃｒｏ－ＰＫＩおよびネットワーク基盤を介してデバイス８０２に応答８１４を送信できる。８２０において、デバイス８０２は、応答に基づいて、署名された完全な証明書８２０を再作成できる。８２２において、デバイス８０２は、新しい証明書８２０を使用してセキュア通信を確保できる。

【００７９】

Ｍｉｃｒｏ－ＰＫＩを使用することにより、デバイスは、セッション鍵を証明書と交換することによるアプリケーション層／トランスポート層／ネットワーク層のセキュリティを実現でき、ＡＶＲ、ＡＲＭ Ｃｏｒｔｅｘ Ｍ０／Ｍ３／Ｍ４、ＴＩ ＭＳＰ４３０、その他の同様のデバイスなどの制限された計算能力を有する制約付きデバイスにおいて実行される制約付き通信プロトコル（Ｂｌｕｅｔｏｏｔｈ、Ｚｉｇｂｅｅ、ＬｏＲａＷＡＮ、ＬｏＲａ、ＮＢＩｏＴ、ＺＷａｖｅなど。）における前方秘匿性を実現できる。ＳＤＫは非依存的に設計されているため、あらゆる種類の組み込みデバイスと簡単に統合でき、あらゆる種類のネットワークを介して通信できる。ＡＣＭＳを使用すれば、デバイスは、遠隔から新しい証明書をコミッショニング、プロビジョニング、および更新できると共に、必要に応じて既存の証明書を失効させることができる。

【００８０】

いくつかの実施形態では、Ｍｉｃｒｏ－ＰＫＩのアプリケーションは、制約されたデバイスおよびプロトコルに限定されない。代わりに、システム全体のパフォーマンスおよびスループットを向上させるために最適化が必要な全てのデバイスにも拡張し得る。この技術は、証明書管理システムおよびライフサイクル管理システムが必要な場所にも適用できる。この技術には、証明書および鍵のコミッショニングおよび管理も含まれる。

【００８１】

図９は、データ通信方法のフローチャート９００である。同図の方法は、装置（例えば、図１１または図１２を参照して以下に説明する装置１１０２／１１０２’）によって実行され得る。いくつかの実施形態では、装置は、Ｍｉｃｒｏ－ＰＫＩプロトコルを実装するコンピューティングデバイス（例えば、センサ１０２、２０４、デバイス３０２、エンドポイントデバイス６０２、組み込みデバイス７０２、デバイス８０２）であっても良い。

【００８２】

９０２において、装置は、トランスポート層またはアプリケーション層のセキュリティを提供するマイクロ公開鍵基盤内のマイクロ証明書を使用して、データ通信セッションにおける他の当事者を認証できる。マイクロ公開鍵基盤は、通信プロトコル、マイクロ証明書、および管理プラットフォームの組み合わせであっても良い。データ通信セッションの少なくとも一方の当事者は、リソースおよび帯域幅に制約のあるデバイスであっても良い。

【００８３】

いくつかの実施形態では、帯域幅が制約された、とは、証明書交換、鍵交換、および暗号化されたデータなどのセキュリティ機能が基盤のデータペイロードおよびペイロードが送信される速度に対して多大な負荷を追加するネットワーク技術を意味し得る。いくつかの実施形態では、データ通信は、有線または無線通信であり得る。いくつかの実施形態では、マイクロ公開鍵基盤は、アプリケーションコードとネットワーク通信コードとの間に位置するソフトウェア開発キットを通じて統合できる。

【００８４】

９０４において、装置は、マイクロ証明書を使用してデータ通信セッションを確立できる。いくつかの実施形態では、マイクロ公開鍵基盤に関連するアクティビティは、マイクロ公開鍵基盤通信プロトコルを通じて実行され得る。これらのアクティビティには、証明書交換、セッション鍵交換、証明書署名、および制御関連メッセージが含まれ得る。いくつかの実施形態では、マイクロ公開鍵基盤通信プロトコルは、１バイトの識別子フィールドと任意の長さのメッセージとを含むパケットを定義できる。

【００８５】

９０６において、装置は、データ通信セッションを通じて安全なデータ通信を実行できる。いくつかの実施形態では、マイクロ証明書の複数の識別子は数値であり得る。複数の識別子のそれぞれは、識別子の目的に合わせてサイズを調整できる。いくつかの実施形態では、マイクロ証明書は公開鍵を含み得る。公開鍵は、楕円曲線暗号に基づくものであっても良い。公開鍵は、公開鍵の楕円曲線上の点に対して圧縮を実行する点圧縮技術を使用して、マイクロ証明書中に表すことができる。いくつかの実施形態では、マイクロ証明書のサイズは、Ｘ．５０９証明書などの従来のデジタル証明書よりも実質的に小さくても良い。いくつかの実施形態では、マイクロテーブルベースのスキームを使用してマイクロ証明書のサイズを縮小できる。マイクロテーブルベースのスキームは、マイクロ証明書の異なるフィールドを利用してマイクロ証明書のタイプおよびマイクロ証明書が保持する様々なパラメータに関する情報を提供し得る。

【００８６】

図１０は、マイクロ証明書の更新方法のフローチャート１０００である。同図の方法は、装置（例えば、図１１または１２を参照して以下に説明する装置１１０２／１１０２’）によって実行され得る。いくつかの実施形態では、装置は、Ｍｉｃｒｏ－ＰＫＩプロトコルを実装するコンピューティングデバイス（例えば、センサ１０２、２０４、デバイス３０２、エンドポイントデバイス６０２、組み込みデバイス７０２、デバイス８０２）であっても良い。いくつかの実施形態では、この方法の動作は、図６から図８までを参照して

説明した動作に対応し得る。

【００８７】

１００２において、装置は、マイクロ証明書署名要求を生成し得る。いくつかの実施形態では、マイクロ証明書の複数の識別子は数値であっても良い。複数の識別子のそれぞれは、その識別子の目的に合わせてサイズを調整できる。各数値識別子は、それ自体を証明書に格納する必要のない、より詳細な情報に関連付けられる。

【００８８】

１００４において、装置は、マイクロ証明書署名要求を認証局に送信し得る。いくつかの実施形態では、マイクロ証明書署名要求は、認証局によって提供されるマイクロ証明書のフィールドのセットを含むことなく構成されている。いくつかの実施形態では、このマイクロ証明書のフィールドのセットは、発行者、日付、期間のうちの１または複数を含み得る。

【００８９】

１００６において、装置は、マイクロ証明書署名要求に対する認証局からの応答を受信し得る。いくつかの実施形態では、応答は、装置が所有しているマイクロ証明書のフィールドのセットを含むことなく構成できる。

【００９０】

１００８において、装置は、この応答に基づいて、認証局によって署名されたマイクロ証明書を再作成し得る。マイクロ証明書は、楕円曲線暗号を利用し得る。いくつかの実施形態では、マイクロ証明書は公開鍵を含み得る。公開鍵は、楕円曲線上の点に対して圧縮を実行する点圧縮技術を使用してマイクロ証明書に表すことができる。

【００９１】

図１１は、例示的な装置１１０２における異なる手段／コンポーネント間のデータフローを示す概念的なデータフローダイアグラム１１００である。装置１１０２は、コンピューティングデバイス（例えば、センサ１０２、２０４、デバイス３０２、エンドポイントデバイス６０２、組み込みデバイス７０２、デバイス８０２）であり得る。装置１１０２は、ＣＳＲに対する応答をＣＡ１１５０から受信する受信コンポーネント１１０４を含み得る。一実施形態では、受信コンポーネント１１０４は、図１０の１００６を参照して説明した動作を実行し得る。

【００９２】

装置１１０２は、ＣＡ１１５０にＣＳＲを送信する送信コンポーネント１１１０を含み得る。一実施形態では、送信コンポーネント１１１０は、図１０の１００４を参照して説明した動作を実行し得る。受信コンポーネント１１０４および送信コンポーネント１１１０は、協働して装置１１０２の通信を調整し得る。

【００９３】

装置１１０２は、証明書再作成コンポーネント１１０６を含み得る。証明書再作成コンポーネント１１０６は、受信コンポーネント１１０４が受信したＣＳＲに対する応答に基づいてマイクロ証明書を再作成するように構成されている。一実施形態では、証明書再構成コンポーネント１１０６は、図１０の１００８を参照して説明した動作を実行できる。

【００９４】

装置１１０２は、ＣＳＲ生成コンポーネント１１０８を含み得る。ＣＳＲ生成コンポーネント１１０８は、ＣＳＲを生成し、ＣＡ１１５０に送信するためにＣＳＲを送信コンポーネント１１１０に提供するように構成されている。一実施形態では、ＣＳＲ生成コンポーネント１１０８は、図１０の１００２を参照して説明した動作を実行できる。

【００９５】

装置１１０２は、前述した図９および図１０のフローチャートにおけるアルゴリズムの各ブロックを実行する追加コンポーネントを含み得る。したがって、前述した図９および図１０のフローチャートの各ブロックはコンポーネントによって実行でき、装置はそれらのコンポーネントのうちの１または複数を含み得る。コンポーネントは、記載されたプロセス／アルゴリズムを実行するように具体的に構成された１または複数のハードウェアコ

ンポーネントであっても良いし、記載されたプロセス／アルゴリズムを実行するように構成されたプロセッサによって実装されていても良いし、プロセッサによる実装のためにコンピュータ可読媒体内に格納されていても良いし、これらのいくつかの組み合わせであっても良い。

【００９６】

図１２は、処理システム１２１４を採用する装置１１０２’のハードウェア実装の例を示すダイアグラム１２００である。一実施形態では、装置１１０２’は、図１１を参照して説明した装置１１０２であり得る。処理システム１２１４では、一般にバス１２２４によって表されるバスアーキテクチャが実装され得る。バス１２２４は、処理システム１２１４の具体的な用途および全体的な設計上の制約に応じて、任意の数の相互接続バスおよびブリッジを含み得る。バス１２２４は、プロセッサ１２０４、コンポーネント１１０４、１１０６、１１０８、１１１０、およびコンピュータ可読媒体／メモリ１２０６によって表される１または複数のプロセッサおよび／またはハードウェアコンポーネント、を含む様々な回路を互いにリンクする。バス１２２４はまた、タイミングソース、周辺機器、電圧レギュレータ、および電力管理回路などの様々な他の回路をリンクできるが、これらは当技術分野で周知であり、したがって、これ以上の説明を行わない。

【００９７】

いくつかの実施形態では、処理システム１２１４は、トランシーバ１２１０に接続され得る。トランシーバ１２１０は、１または複数のアンテナ１２２０に接続される。トランシーバ１２１０は、伝送媒体を通じて他の様々な装置と通信するための手段を提供する。トランシーバ１２１０は、１または複数のアンテナ１２２０から信号を受信し、受信した信号から情報を抽出し、抽出された情報を処理システム１２１４、具体的には受信コンポーネント１１０４に提供する。さらに、トランシーバ１２１０は、処理システム１２１４、具体的には送信コンポーネント１１１０から情報を受信し、受信した情報に基づいて、１または複数のアンテナ１２２０に供給する信号を生成する。他の実施形態では、装置１１０２’は、有線インターフェースを介して接続可能である。このような実施形態では、装置１１０２’は、トランシーバまたはアンテナを全く含まない。

【００９８】

処理システム１２１４は、コンピュータ可読媒体／メモリ１２０６に接続されたプロセッサ１２０４を含む。プロセッサ１２０４は、装置自体のセンサを通じて装置自体によって収集されたデータの分析、およびコンピュータ可読媒体／メモリ１２０６に格納されたソフトウェアの実行、を含む一般的な処理を担当する。ソフトウェアは、プロセッサ１２０４によって実行されることにより、各装置について上述した様々な機能を処理システム１２１４に実行させる。コンピュータ可読媒体／メモリ１２０６は、ソフトウェアを実行するときにプロセッサ１２０４によって扱われるデータを格納するために使用され得る。処理システム１２１４は、コンポーネント１１０４、１１０６、１１０８、１１１０のうちの少なくとも１つをさらに含む。コンポーネントは、プロセッサ１２０４で実行されるソフトウェアコンポーネント、コンピュータ可読媒体／メモリ１２０６に常駐／格納されるソフトウェアコンポーネント、プロセッサ１２０４に接続された１または複数のハードウェアコンポーネント、またはそれらのいくつかの組み合わせであり得る。

【００９９】

図１３は、証明書の生成および処理方法のフローチャート１３００である。同図の方法は、上述した図１０に記載された方法と対になる方法であり得る。この方法は、装置（例えば、図１４または図１５を参照して以下に説明する装置１４０２／１４０２’）によって実行され得る。いくつかの実施形態では、装置は、１または複数のコンピューティングデバイスを含むサーバであっても良い。いくつかの実施形態では、装置は、Ｍｉｃｒｏ－ＰＫＩプロトコルを実装するＣＡ（例えば、デバイス３０２、Ｍｉｃｒｏ－ＰＫＩサービス６０４、ＣＡサーバ７１４、ＣＡ８０４）であり得る。いくつかの実施形態では、この方法の動作は、図６から図８を参照して説明した動作に対応し得る。

【０１００】

１３０２において、装置は、コンピューティングデバイスからマイクロ証明書署名要求を受信し得る。いくつかの実施形態では、マイクロ証明書署名要求は、装置によって提供されるマイクロ証明書のフィールドのセットを含むことなく構成できる。いくつかの実施形態では、このマイクロ証明書のフィールドのセットは、発行者、日付、期間のうちの１または複数を含んでいても良い。

【０１０１】

いくつかの実施形態では、マイクロ証明書署名要求は、マイクロ公開鍵基盤通信プロトコルを介して受信され得る。マイクロ公開鍵基盤通信プロトコルは、１バイトの識別子フィールドと任意の長さのメッセージとを含むパケットを定義できる。１バイトの識別子フィールドは、メッセージの長さを定義しない。

【０１０２】

１３０３において、装置は、マイクロ証明書署名要求を認証し得る。いくつかの実施形態では、１３０３での動作は、図７を参照して説明したアクセス制御モジュール７１２によって実行され得る。

【０１０３】

１３０４において、装置は、マイクロ証明書署名要求に対する応答を生成し得る。いくつかの実施形態では、応答は、コンピューティングデバイスが所有しているマイクロ証明書のフィールドのセットを含むことなく構成できる。いくつかの実施形態では、応答を生成するために、装置は、マイクロ証明書署名要求を検証してマイクロ証明書に署名し、署名されたマイクロ証明書に基づいて応答を作成し得る。

【０１０４】

１３０５において、装置は、マイクロ証明書署名要求に対する応答を検証できる。いくつかの実施形態では、１３０５での動作は、図７を参照して説明したアクセス制御モジュール７１２によって実行され得る。

【０１０５】

１３０６において、装置は、コンピューティングデバイスに対して応答を送信し得る。認証局によって署名されたマイクロ証明書は、応答に基づいて再作成され得る。マイクロ証明書は、楕円曲線暗号を利用し得る。いくつかの実施形態では、マイクロ証明書の複数の識別子は数値であり得る。複数の識別子のそれぞれは、その識別子の目的に合わせてサイズが調整され得る。いくつかの実施形態では、マイクロ証明書は公開鍵を含み得る。公開鍵は、楕円曲線上の点に対して圧縮を実行する点圧縮技術を使用してマイクロ証明書に表すことができる。

【０１０６】

図１４は、例示的な装置１４０２における異なる手段／コンポーネント間のデータフローを示す概念的なデータフローダイアグラム１４００である。装置１４０２は、Ｍｉｃｒｏ－ＰＫＩプロトコルを実装するＣＡ（例えば、ＣＡサーバ７１４、デバイス３０２、Ｍｉｃｒｏ－ＰＫＩサービス６０４、ＣＡ８０４）であり得る。装置１４０２は、１または複数のコンピューティングデバイスを含み得る。装置１４０２は、コンピューティングデバイス１４５０からＣＳＲを受信する受信コンポーネント１４０４を含み得る。いくつかの実施形態では、コンピューティングデバイス１４５０は、図１１または図１２において説明した装置１１０２／１１０２’であり得る。一実施形態では、受信コンポーネント１４０４は、図１３の１３０２を参照して説明した動作を実行し得る。

【０１０７】

装置１４０２は、コンピューティングデバイス１４５０にＣＳＲに対する応答を送信する送信コンポーネント１４１０を含み得る。一実施形態では、送信コンポーネント１４１０は、図１３の１３０６を参照して説明した動作を実行し得る。受信コンポーネント１４０４および送信コンポーネント１４１０は、協働して装置１４０２の通信を調整し得る。

【０１０８】

装置１４０２は、ＣＳＲに対する応答を生成するように構成された応答生成コンポーネント１４０６を含み得る。一実施形態では、応答生成コンポーネント１４０６は、図１３

の１３０４を参照して説明した動作を実行し得る。
【０１０９】
装置１４０２は、受信コンポーネント１４０４が受信したＣＳＲを、応答生成コンポーネント１４０６に転送する前に認証するように構成されたアクセス制御コンポーネント１４０８を含み得る。アクセス制御コンポーネント１４０８は、さらに、応答生成コンポーネント１４０６によって生成されたＣＳＲに対する応答を検証し、検証された応答を送信コンポーネント１４１０に転送するように構成され得る。一実施形態では、アクセス制御コンポーネント１４０８は、図１３の１３０３または１３０５を参照して説明した動作を実行し得る。
【０１１０】
装置１４０２は、前述した図１３のフローチャートにおけるアルゴリズムの各ブロックを実行する追加コンポーネントを含み得る。したがって、前述した図１３のフローチャートの各ブロックはコンポーネントによって実行でき、装置は、それらのコンポーネントのうちの１または複数を含み得る。コンポーネントは、記載されたプロセス／アルゴリズムを実行するように具体的に構成された１または複数のハードウェアコンポーネントであっても良いし、記載されたプロセス／アルゴリズムを実行するように構成されたプロセッサに実装されても良いし、プロセッサによる実装のためにコンピュータ可読媒体内に格納されても良いし、これらのいくつかの組み合わせであっても良い。
【０１１１】
図１５は、処理システム１５１４を採用する装置１４０２’のハードウェアの実装例を示すダイアグラム１５００である。一実施形態では、装置１４０２’は、図１４を参照して説明した装置１４０２であっても良い。処理システム１５１４では、一般にバス１５２４によって表されるバスアーキテクチャが実装され得る。バス１５２４は、処理システム１５１４の具体的な用途および全体的な設計上の制約に応じて、任意の数の相互接続バスおよびブリッジを含むと良い。バス１５２４は、プロセッサ１５０４、コンポーネント１４０４、１４０６、１４０８、１４１０、およびコンピュータ可読媒体／メモリ１５０６によって表される１または複数のプロセッサおよび／またはハードウェアコンポーネント、を含む様々な回路を互いにリンクする。バス１５２４はまた、タイミングソース、周辺機器、電圧レギュレータ、および電力管理回路などの様々な他の回路をリンクできるが、これらは当技術分野で周知であり、したがって、これ以上の説明を行わない。
【０１１２】
処理システム１５１４は、コンピュータ可読媒体／メモリ１５０６に接続されたプロセッサ１５０４を含む。プロセッサ１５０４は、装置自体のセンサを介して装置自体によって収集されたデータの分析、およびコンピュータ可読媒体／メモリ１５０６に格納されたソフトウェアの実行、を含む一般的な処理を担当する。ソフトウェアは、プロセッサ１５０４によって実行されることにより、各装置について上述した様々な機能を処理システム１５１４に実行させる。コンピュータ可読媒体／メモリ１５０６は、ソフトウェアを実行するときにプロセッサ１５０４によって扱われるデータを格納するために使用され得る。処理システム１５１４は、コンポーネント１４０４、１４０６、１４０８、１４１０のうちの少なくとも１つをさらに含む。コンポーネントは、プロセッサ１５０４で実行されるソフトウェアコンポーネント、コンピュータ可読媒体／メモリ１５０６に常駐／格納されるソフトウェアコンポーネント、プロセッサ１５０４に接続された１または複数のハードウェアコンポーネント、またはそれらのいくつかの組み合わせであっても良い。
【０１１３】
以下、本開示の様々な態様を説明する。
【０１１４】
実施例１は、安全な通信のための方法または装置である。装置は、コンピューティングデバイスであり得る。装置は、マイクロ証明書署名要求を生成し得る。装置は、マイクロ証明書署名要求を認証局に送信し得る。装置は、マイクロ証明書署名要求に対する応答を認証局から受信し得る。装置は、応答に基づいて、認証局によって署名されたマイクロ証

明書を再作成し得る。マイクロ証明書は、楕円曲線暗号を利用しても良い。
【０１１５】
実施例２では、マイクロ証明書署名要求が、認証局によって提供されるマイクロ証明書のフィールドのセットを含むことなく構成できること、を実施例１の内容に任意に含めることができる。
【０１１６】
実施例３では、このマイクロ証明書のフィールドのセットが、発行者、日付、または期間のうち１または複数を含み得ること、を実施例２の内容に任意に含めることができる。
【０１１７】
実施例４では、応答が、コンピューティングデバイスが所有するマイクロ証明書のフィールドのセットを含むことなく構成できること、を実施例１から実施例３までのいずれか１つの内容に任意に含めることができる。
【０１１８】
実施例５では、マイクロ証明書の複数の識別子が数値であっても良く、複数の識別子のそれぞれは、識別子の目的に合わせてサイズを調整でき、各数値識別子は、それ自体を証明書に格納する必要のない、より詳細な情報に関連付けできること、を実施例１から実施例４までのいずれか１つの内容に任意に含めることができる。
【０１１９】
実施例６では、マイクロ証明書が公開鍵を含むことができ、公開鍵は、マイクロ証明書において点圧縮技術を使用してマイクロ証明書に表され得ること、を実施例１から実施例５までのいずれか１つの内容に任意に含めることができる。
【０１２０】
実施例７では、マイクロ公開鍵基盤通信プロトコルを介して認証局にマイクロ証明書署名要求を送信でき、マイクロ公開鍵基盤通信プロトコルは、１バイトの識別子フィールドと任意の長さのメッセージとを含むパケットを定義でき、１バイトの識別子フィールドはメッセージの長さを定義しないこと、を実施例１から実施例６までのいずれか１つの内容に任意に含めることができる。
【０１２１】
実施例８は、安全な通信のための方法または装置である。装置は、ＣＡであり得る。装置は、コンピューティングデバイスからマイクロ証明書署名要求を受信できる。装置は、マイクロ証明書署名要求に対する応答を生成できる。装置は、コンピューティングデバイスに対して応答を送信できる。装置によって署名されたマイクロ証明書は、応答に基づいて再作成され得る。マイクロ証明書は、楕円曲線暗号を利用しても良い。
【０１２２】
実施例９では、マイクロ証明書署名要求が、装置によって提供されるマイクロ証明書のフィールドのセットを含むことなく構成できること、を実施例８の内容に任意に含めることができる。
【０１２３】
実施例１０では、このマイクロ証明書のフィールドのセットが、発行者、日付、または期間のうち１または複数を含み得ること、を実施例９の内容に任意に含めることができる。
【０１２４】
実施例１１では、応答が、コンピューティングデバイスが所有するマイクロ証明書のフィールドのセットを含むことなく構成できること、を実施例８から実施例１０までのいずれか１つの内容に任意に含めることができる。
【０１２５】
実施例１２では、マイクロ証明書の複数の識別子が数値であっても良く、複数の識別子のそれぞれは、識別子の目的に合わせてサイズを調整でき、各数値識別子は、それ自体を証明書に格納する必要のない、より詳細な情報に関連付けできること、を実施例８から実施例１１までのいずれか１つの内容に任意に含めることができる。
【０１２６】

実施例１３では、マイクロ証明書が公開鍵を含むことができ、公開鍵は、点圧縮技術を使用してマイクロ証明書に表され得ること、を実施例８から実施例１２までのいずれか１つの内容に任意に含めることができる。

【０１２７】

実施例１４では、マイクロ公開鍵基盤通信プロトコルを介してマイクロ証明書署名要求を受信でき、マイクロ公開鍵基盤通信プロトコルは、１バイトの識別子フィールドと任意の長さのメッセージとを含むパケットを定義でき、１バイトの識別子フィールドはメッセージの長さを定義しないこと、を実施例８から実施例１３までのいずれか１つの内容に任意に含めることができる。

【０１２８】

実施例１５では、応答を生成するために、装置が、マイクロ証明書署名要求を検証し得ること、マイクロ証明書に署名し得ること、および署名されたマイクロ証明書に基づいて応答を作成し得ること、を実施例８から実施例１４までのいずれか１つの内容に任意に含めることができる。

【０１２９】

実施例１６は、データ通信のための方法または装置である。装置は、コンピューティングデバイスであっても良い。装置は、トランスポート層またはアプリケーション層のセキュリティを提供するマイクロ公開鍵基盤内のマイクロ証明書を使用してデータ通信セッションの当事者を認証できる。マイクロ公開鍵基盤は、通信プロトコル、マイクロ証明書、および管理プラットフォームの組み合わせである。データ通信セッションの少なくとも１の当事者は、リソースおよび帯域幅に制約のあるデバイスである。装置は、マイクロ証明書を使用してデータ通信セッションを確立できる。装置は、データ通信セッションを通じて安全なデータ通信を実行できる。

【０１３０】

実施例１７では、マイクロ公開鍵基盤が、アプリケーションコードとネットワーク通信コードとの間に位置するソフトウェア開発キットを通じて統合され得ること、を実施例１６の内容に任意に含めることができる。

【０１３１】

実施例１８では、マイクロ公開鍵基盤に関連するアクティビティがマイクロ公開鍵基盤通信プロトコルを通じて実行でき、アクティビティは、証明書交換、セッション鍵交換、証明書署名、および関連するメッセージの制御を含むこと、を実施例１６または実施例１７の内容に任意に含めることができる。

【０１３２】

実施例１９では、マイクロ公開鍵基盤通信プロトコルが、１バイトの識別子フィールドと任意の長さのメッセージとを含むパケットを定義し得ること、を実施例１８の内容に任意に含めることができる。

【０１３３】

実施例２０では、マイクロ証明書の複数の識別子が数値であっても良く、複数の識別子のそれぞれは、識別子の目的に合わせてサイズが調整されること、を実施例１６から実施例１９までのいずれか１つの内容に任意に含めることができる。

【０１３４】

実施例２１では、マイクロ証明書が公開鍵を含んでいても良く、公開鍵は楕円曲線暗号に基づくものであっても良く、公開鍵は、公開鍵の楕円曲線上の点に対して圧縮を実行する点圧縮技術を使用してマイクロ証明書に表すことができること、を実施例１６から実施例２０までのいずれか１つの内容に任意に含めることができる。

【０１３５】

実施例２２では、マイクロ証明書のサイズは、Ｘ．５０９証明書を含む従来のデジタル証明書よりも実質的に小さいものであり得ること、を実施例１６から実施例２１までのいずれか１つの内容に任意に含めることができる。

【０１３６】

実施例２３では、マイクロ証明書がマイクロテーブルベースのスキームを使用してマイクロ証明書のサイズを縮小でき、マイクロテーブルベースのスキームは、マイクロ証明書の異なるフィールド利用してマイクロ証明書のタイプと、マイクロ証明書が保持するさまざまなパラメータと、に関する情報を提供し得ること、を実施例１６から実施例２２までのいずれか１つの内容に任意に含めることができる。

【０１３７】

実施例２４では、マイクロ公開鍵基盤が前方秘匿性をサポートできること、を実施例１６から実施例２３までのいずれか１つの内容に任意に含めることができる。

【０１３８】

実施例２５では、自動証明書管理環境およびシステム（Automated Certificate Management Environment and System）を使用して、マイクロ証明書を遠隔管理（例えば、マイクロ証明書のコミッショニング、更新、および失効）できること、を実施例１６から実施例２４までのいずれか１つの内容に任意に含めることができる。

【０１３９】

例示したプロセス／フローチャートにおけるブロックの具体的な順序または階層は、例示的なアプローチでの説明であることが理解される。設計時の選択に基づいて、プロセス／フローチャート内におけるブロックの具体的な順序または階層を再配置できると理解できる。また、一部のブロックを組み合わせたり省略できる。付随する方法クレームは、様々なブロックの要素の順序を一例として示すものであり、クレームに示された具体的な順序または階層に限定されることを意味するものではない。

【０１４０】

先の説明は、本明細書で説明される様々な態様を当業者が実施できるようにするために提供されている。これらの態様に対する様々な修正は、当業者には直ちに明らかであり、本明細書で定義される包括的な原理は、他の態様に適用されても良い。したがって、特許請求の範囲は、本明細書に示される態様に限定されるものではなく、特許請求の範囲の文言に整合する全範囲が与えられるべきであり、単数形での要素への言及は、特にそのように述べられていない限り、「１つだけ」を意味することを意図せず、むしろ「１または複数」を意味する。「例示的」という単語は、本明細書では、「例、事例、または例証としての役割を果たす」ことを意味するために使用される。本明細書で「例示的」として説明される任意の態様は、必ずしも、他の態様よりも好ましいあるいは有利であると解釈されるべきではない。特に明記しない限り、「いくつか」という用語は１または複数を意味している。「Ａ、Ｂ、Ｃの少なくとも１つ」、「Ａ、Ｂ、Ｃの１または複数」、「Ａ、Ｂ、およびＣの少なくとも１つ」、「Ａ、Ｂ、およびＣの１または複数」および「Ａ、Ｂ、Ｃ、またはそれらの任意の組み合わせ」は、Ａ、Ｂ、および／またはＣの任意の組み合わせを含み、複数のＡ、複数のＢ、または複数のＣを含むことができる。具体的には、「Ａ、Ｂ、Ｃの少なくとも１つ」、「Ａ、Ｂ、Ｃの１または複数」、「Ａ、Ｂ、およびＣの少なくとも１つ」、「Ａ、Ｂ、およびＣの１または複数」および「Ａ、Ｂ、Ｃ、またはそれらの任意の組み合わせ」の組合せは、Ａのみ、Ｂのみ、Ｃのみ、ＡとＢ、ＡとＣ、ＢとＣ、またはＡとＢとＣの場合があり、このような組み合わせは、いずれも、Ａ、Ｂ、Ｃの１または複数の要素を含むことができる。本出願全体に亘って説明される様々な態様の要素に対し、既に当業者に知られているか或いは後に当業者に知られるようになる構造的および機能的な均等物は、すべて、参照により本明細書に明示的に組み込まれ、特許請求の範囲に含まれることが意図されている。さらに、本明細書に開示されている事項は、そのような開示が特許請求の範囲に明示的に記載されているか否かに関係なく、公衆に解放することを意図したものではない。「モジュール」、「メカニズム」、「要素」、「装置（デバイス）」などの単語は、「手段」という単語の代わりにはならない場合がある。したがって、「～のための手段」という句を使用して要素が明示的に列挙されていない限り、請求の範囲の要素はミーンズ・プラス・ファンクションとして解釈されるべきではない。

【図面】

【図１】

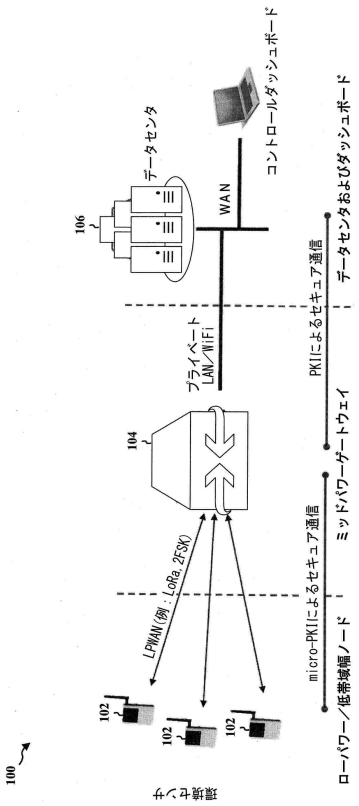

FIG. 1

【図２】

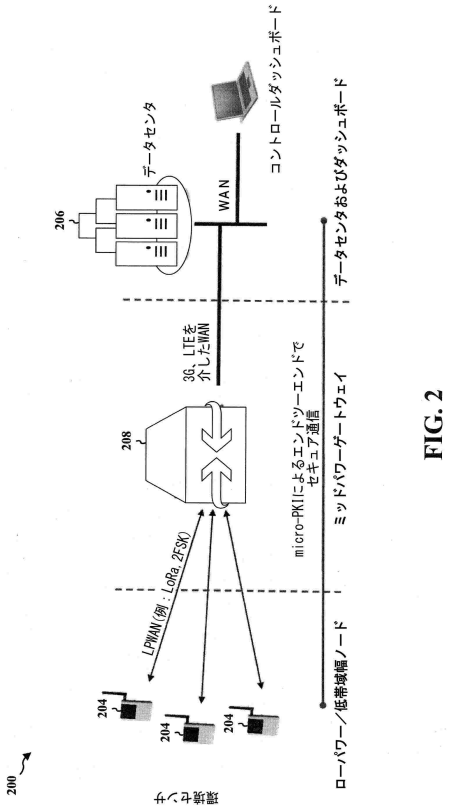

FIG. 2

【図３】

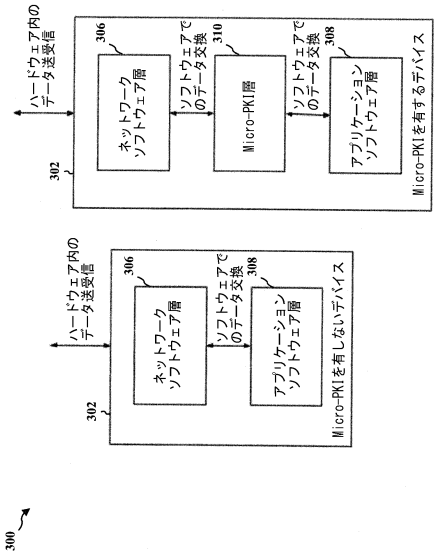

FIG. 3

【図４】

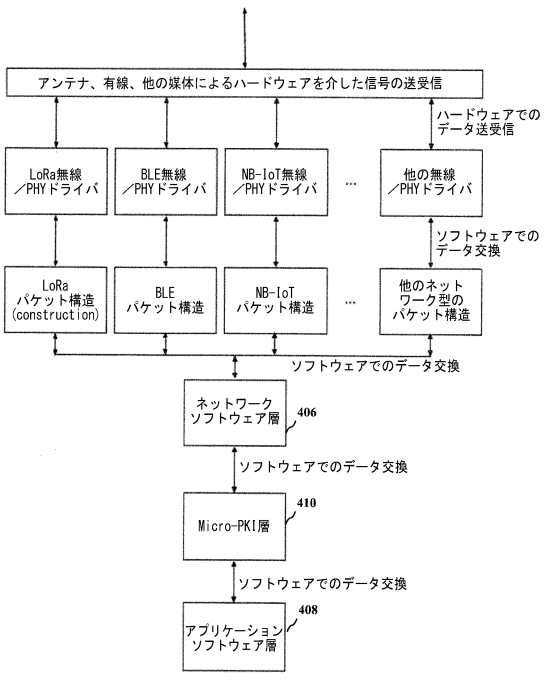

FIG. 4

【図５】

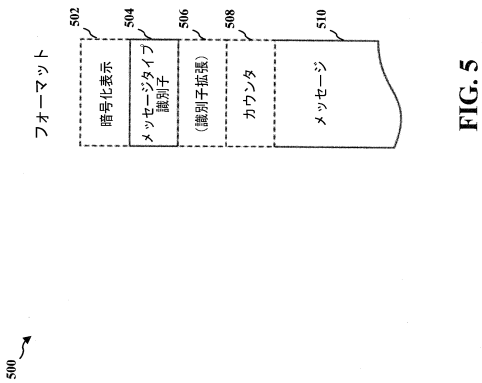

FIG. 5

【図６】

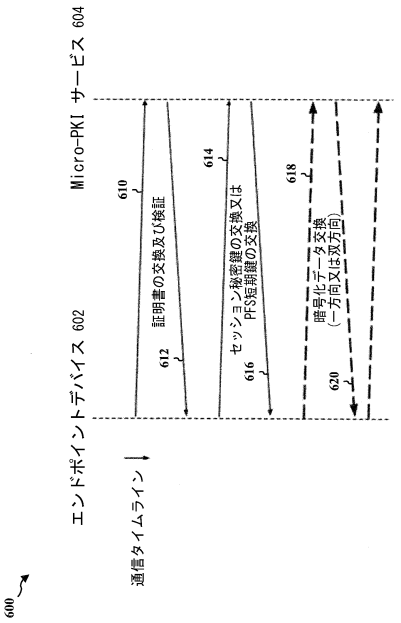

FIG. 6

【図７】

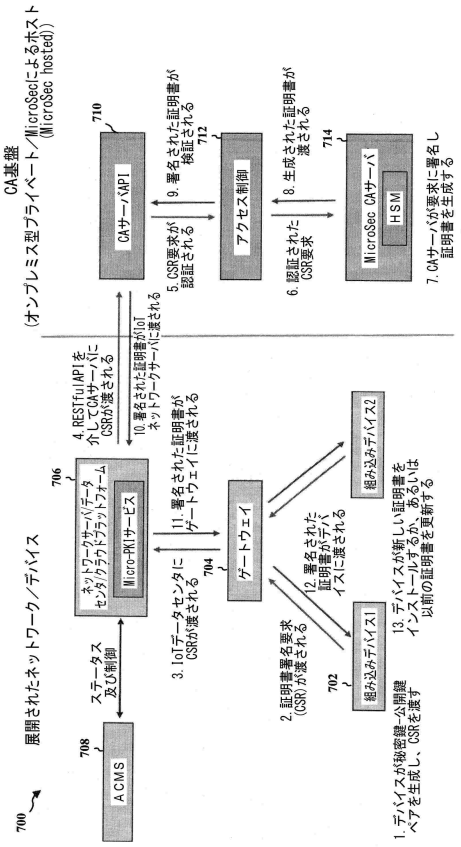

FIG. 7

【図８】

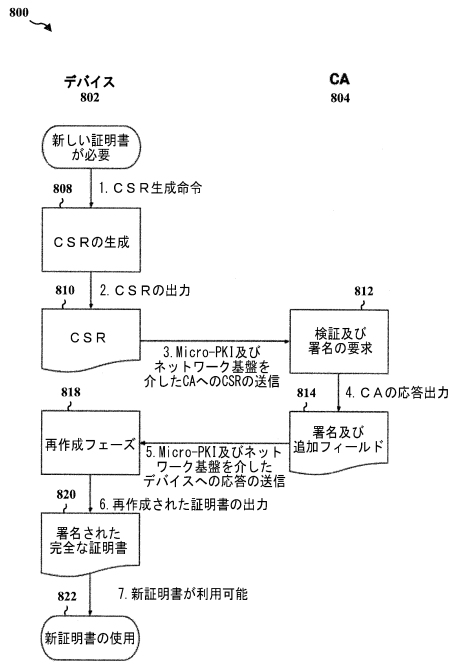

FIG. 8

【図９】

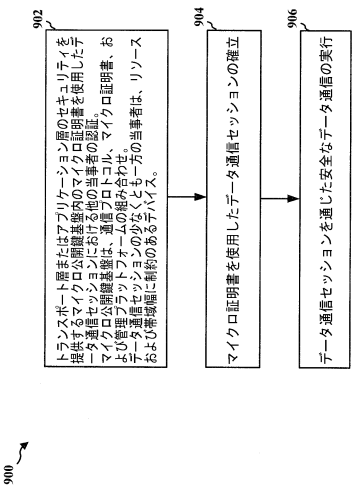

FIG. 9

【図１０】

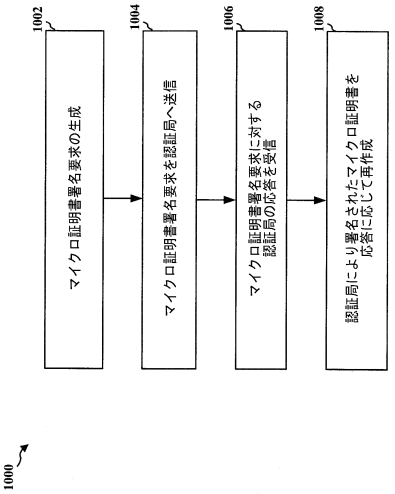

FIG. 10

【図１１】

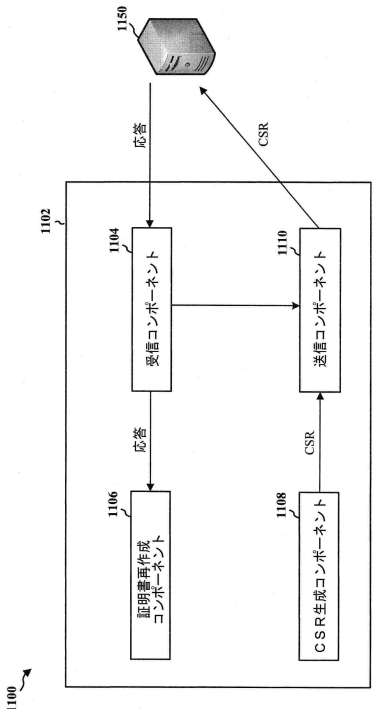

FIG. 11

【図１２】

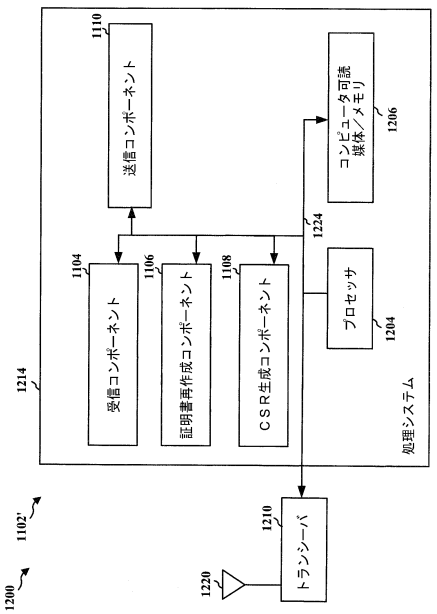

FIG. 12

【図１３】

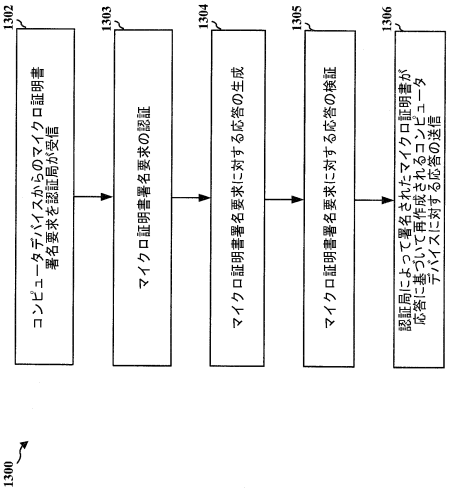

FIG. 13

【図１４】

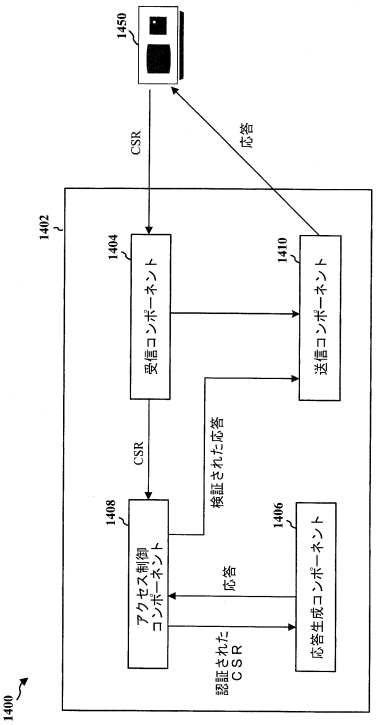

FIG. 14

【図１５】

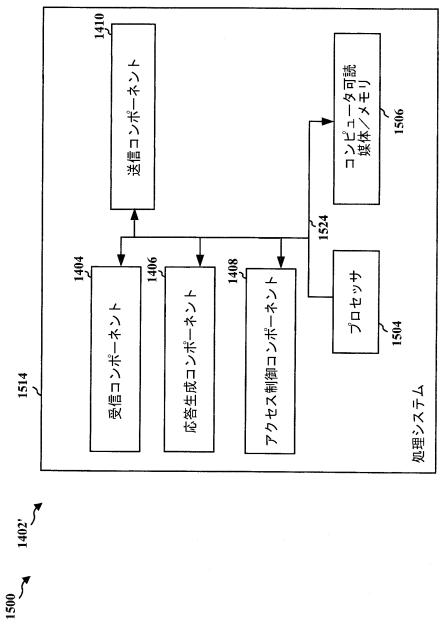

FIG. 15

フロントページの続き

(72)発明者　ケリソン，スティーブン ポール
シンガポール国 １４００８３ シンガポール ＃１１－１６３，コモンウェルス クローズ ８３
(72)発明者　ザイーニ，シャジナ ビンティ
シンガポール国 ０６９４１５ シンガポール ＃１０－１８，クラブ ストリート ３３
(72)発明者　シディキ，アーナフ アフ
シンガポール国 ４７０７７０ シンガポール ＃１５－１７９，ベドック リザーバー ビュー ７７０

審査官　金沢 史明
(56)参考文献　米国特許出願公開第２０１０／０２０２６１６（ＵＳ，Ａ１）
特開２０１８－０３８０３６（ＪＰ，Ａ）
特開２００９－１６９１７１（ＪＰ，Ａ）
米国特許出願公開第２０１６／０１０５２８９（ＵＳ，Ａ１）
特開２００４－１７３２８６（ＪＰ，Ａ）
特開２００１－０６９１３７（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｈ０４Ｌ　９／０８
Ｈ０４Ｗ　１２／０６