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

特許第5312722号
(P5312722)

(45)発行日　平成25年10月9日(2013.10.9)　(24)登録日　平成25年7月12日(2013.7.12)

(51)Int.Cl.		F I		
H04L 29/08	(2006.01)	H04L	13/00	307Z
G08C 17/00	(2006.01)	G08C	17/00	Z
H04L 9/08	(2006.01)	H04L	9/00	601B

請求項の数 6　(全 22 頁)

(21)出願番号	特願2004-248198 (P2004-248198)
(22)出願日	平成16年8月27日 (2004.8.27)
(65)公開番号	特開2005-86808 (P2005-86808A)
(43)公開日	平成17年3月31日 (2005.3.31)
審査請求日	平成19年8月23日 (2007.8.23)
審判番号	不服2011-15104 (P2011-15104/J1)
審判請求日	平成23年7月13日 (2011.7.13)
(31)優先権主張番号	10/656551
(32)優先日	平成15年9月5日 (2003.9.5)
(33)優先権主張国	米国 (US)

(73)特許権者　596170170
ゼロックス　コーポレイション
ＸＥＲＯＸ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国、コネチカット州　０６８５６、ノーウォーク、ピーオーボックス　４５０５、グローバー・アヴェニュー　４５
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜
(74)代理人　100139712
弁理士　那須　威夫

最終頁に続く

(54)【発明の名称】安全なワイヤレス・センサを供給する方法、装置、およびプログラム・プロダクト

(57)【特許請求の範囲】

【請求項１】

ワイヤレス・センサと提供装置(provisioning device)の間に、好ましいチャンネル(preferred channel)を介して通信を確立し、

ワイヤレス・センサと提供装置の間で、前記好ましいチャンネルを介してコミットメントを交換し、

前記提供装置においてワイヤレス・センサから前記ワイヤレス・センサの公開鍵を受信し、

前記提供装置において前記ワイヤレス・センサの公開鍵のハッシュを計算して公開鍵が前記好ましいチャンネルを介して提供されたコミットメントと一致することを照合し、

前記提供装置において一致することが照合された場合、前記ワイヤレス・センサは、前記提供装置から、前記好ましいチャンネルを介して提供情報(provisioning information)を受け取り、そして、

前記ワイヤレス・センサは、前記提供情報に応じて、センサ情報を、前記提供情報により安全化された通信チャンネルを介して送出するために、前記ワイヤレス・センサを自動的に構成する(configuring)

ステップを含む、コンピュータ制御された方法。

【請求項２】

ワイヤレス・センサ内のコンピュータによって実行された時に、コンピュータに、

ワイヤレス・センサと提供装置(provisioning device)の間に、好ましいチャンネル(pr

eferred channel)を介して通信を確立し、
ワイヤレス・センサと提供装置の間で、前記好ましいチャンネルを介してコミットメントを交換し、
前記提供装置において前記ワイヤレス・センサの公開鍵のハッシュを計算して公開鍵が前記好ましいチャンネルを介して提供されたコミットメントと一致することを照合するために前記ワイヤレス・センサの公開鍵を提供装置へ送信し、
前記提供装置において一致することが照合された場合、前記ワイヤレス・センサは、前記提供装置から、前記好ましいチャンネルを介して提供情報(provisioning information)を受け取り、そして、
前記ワイヤレス・センサは、前記提供情報に応じて、センサ情報を、前記提供情報により安全化された通信チャンネルを介して送出するために、前記ワイヤレス・センサを自動的に構成する(configuring)、
ステップを含む方法を実行させる命令を記憶するコンピュータ読取可能な記憶媒体。
【請求項３】
好ましいチャンネルを確立(establish)するために構成された少なくとも１つのポート、
提供装置との、前記好ましいチャンネルを介した通信を確立するための好ましいチャンネル通信手段、
ワイヤレス・センサと提供装置の間で、前記好ましいチャンネルを介してコミットメントを交換するための交換メカニズム手段、
提供装置において前記ワイヤレス・センサの公開鍵のハッシュを計算して公開鍵が前記好ましいチャンネルを介して提供されたコミットメントと一致することを照合するために前記ワイヤレス・センサの公開鍵を提供装置へ送信するための送信メカニズム手段、
前記提供装置において一致することが照合された場合、前記提供装置からの提供情報を、前記好ましいチャンネルを介して受信するための受信メカニズム手段、および、
ワイヤレス・センサが、前記提供情報に応じて、前記提供情報により安全化された通信チャンネルを介して、センサ情報を送出することを可能とするための自動構成メカニズム手段、
を備えるワイヤレス装置。
【請求項４】
前記安全化された通信チャンネルを介して前記センサ情報を送出するステップを更に含む、請求項１，または２に記載の発明。
【請求項５】
前記ワイヤレス・センサが、一つあるいはそれ以上の、医療情報、位置情報、近似情報(proximity information)、環境情報、または、乗物情報、を検知する、
請求項１，２、または３に記載の発明。
【請求項６】
前記安全化された通信チャンネルを介して前記センサ情報を送出するために構成された送出メカニズムを更に含む、請求項３に記載の発明。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施例は、暗号方法の分野に関連する。
【背景技術】
【０００２】
公開鍵暗号の採用は、「鍵管理問題」、即ち、ユーザが信頼して、彼らの意図する通信相手の公開鍵を識別することを可能とするという問題によって非常に制限されてきた。
【０００３】
ＰＫＩ(Public Key Infrastructure)(公開鍵インフラストラクチャ)によって提起された主要な困難さは、鍵管理および分配の問題である。即ち、いかにして、鍵に依存する必

要のある個人および装置に対する、特定の個人の、または装置の公開鍵の、認証された(authenticated)複製物を得るか、の判断の問題である。ＰＫＩは、良く知られ、信頼された、おそらく階層的に編成された(organized)公開鍵のシステムである。

【０００４】

そのようなＰＫＩは、アプリオリ(a priori)を交換されねばならぬいくつかの鍵が、多くの信頼された公開鍵だけから渡るようにして、鍵管理問題を単純化する。

不幸にも、証明書の分配に加えて、ＰＫＩの生成および管理は、信じられない程の困難さおよび複雑さをもたらした。一つの組織内の一つのアプリケーションのための公開鍵暗号作成の使用をサポートするための、小さな特別目的のＰＫＩの確立でさえ、一般的に、余りにも高価で困難と考えられる。

更に、ＰＫＩの文脈における上述の鍵管理および分配の問題は、信用証明書の発行のための信用保証発行権限を持つ、いかなる安全な信用保証インフラストラクチャにおいても存在する。

【０００５】

ワイヤレス・ネットワークに対して、派生的な問題が存在する。これらのネットワークは、知識を持つ企業ＩＴ部門においてさえも、安全に構成することが、悪名高く困難であることが証明された。

医療分野において、他の問題が存在する。病院環境における、患者データに対するセキュリティーは、常に重要であったが、新たなＨＩＰＡＡガイドラインの出現に伴って、それはより法的に義務的となってきた。同時に、患者データを収集するセンサまたは装置は、コンピュータ技術に必ずしも精通していないかもしれない医師および看護士のコミュニティーによって高度に利用可能でなければならない。

今日、看護士の援助者が、体温および血圧を人手で測定し、記録する。これらの測定は、物理的チャートを通じて利用可能であるが、これは、データを時間軸上グラフ化する機能等を有さない。ナース・ステーションの警報装置に接続され得る、患者を自動的に監視するためのいくつかの設備(例えばＥＫＧ機器)が存在するが、これらの設備は、高価で、任意のセンサーの組み込みを可能とせず、それらは全て、センサおよび患者の間に、ケーブル、ワイヤ、またはチューブの使用を必要とする。これらのケーブル、ワイヤ、およびチューブは、室内を大きく散らかし、患者および医療スタッフが引っかかって転ぶ危険を引き起こす。

【０００６】

いくつかの会社が、ワイヤレス・センサを、患者に付加することによる患者監視の自動化を一般化することを開めている。本特許のデータは、802.11、他のワイヤレス・ネットワーク、または、ワイヤド・ネットワーク、を介して、患者データベースに送信され得る。しかし、そのようなシステムは、センサと患者データベースの間のリンクを確保することを必要とする。このセキュリティーは、不特定の攻撃者による盗聴を避けるだけでなく、ＨＩＰＡＡを遵守するために、病院コミュニティーの真正なメンバーの間のアクセス制御を実行しなければならない。この問題のための市場についての旨い解決法は存在せず、パスワードのような従来のアプローチは、センサのような埋め込まれた素子に対して、旨く機能しない。

更に別の状況では、家庭でセンサを用いる患者は、彼らの医師へのデータ送信を保護する際に(或いは、監視装置が、彼らの医師に適切にデータを通信するように構成する際にさえ)類似の問題に直面する。いくつかのセンサ素子は、データを適切な場所に確保することと、送出中のデータへのアクセスを制限すること、の双方を取り扱うために、電話ベースのデータ送出を用いる。しかし、データを保護するためのニーズの増大と同様に、そのようなデータを送出するための、ワイヤレス・センサの使用、およびインターネットまたは携帯電話ネットワークの使用が増大されることが予想される。

【０００７】

ＰＫＩのような安全な信用保証インフラストラクチャを生成するための、より単純な方法を提供することが有利であろう。ワイヤド・ネットワークに対しての場合さえ含むネッ

トワークを構成する工程の単純化に加えて、ワイヤレス・アクセス・ポイント(ＷＡＰ)の構成(セキュリティー面を含む)を単純化することもまた有利であろう。更に、保護される(secured)必要があるデータを提供するセンサの供給(provisioning)を単純化することが有利であろう。

【発明の開示】

【課題を解決するための手段】

【０００８】

ここに開示された実施例の一つの特徴は、単純に使用ができる、安全な(secure)、信用保証(credential)インフラストラクチャを生成するための技術である。そのようなインフラストラクチャは、例えば、「インスタントＰＫＩ」であり得る。即ち、ＰＫＩによって提供されるセキュリティを減ずることなく、構築、構成、および使用が容易なＰＫＩである。

他の特徴は、位置が限定されるチャンネルを用いた、自動的に提供する(automatically provisioning)装置のための技術であり、例えば、医療センサおよび家庭警報のような模範的システムでこの技術を用いる装置である。

開示された実施例の、更に他の特徴には、センサ・データを、目的地に安全に送ることが可能な、容易に提供されるセンサが含まれる。そのようなセンサは、広い種類のアプリケーションで使用され得る。

開示された実施例の更に別の特徴には、特定の受信機に向けられた情報を安全に受信し、それを提供するために使用され得る、安全状態通知装置が含まれる。

【発明を実施するための最良の形態】

【０００９】

図１は、本発明の一つの実施例を含む、ネットワーク化されたコンピュータ・システム100を示す。ネットワーク化されたコンピュータ・システム100は、ＣＰＵ103、メモリ105、および、ネットワーク・インターフェース107、記憶システム115、および、リムーバブルな媒体データ装置117を含むコンピュータ101を含む。リムーバブルな媒体データ装置117は、プログラム・プロダクト121を一般的に含むコンピュータ読み取り可能なメディア119を読むことが出来る。コンピュータ読取可能な媒体119上のプログラム・プロダクト121は一般的に、メモリ105に、プログラムとして読み込まれる。更に、プログラム・プロダクト121、またはその更新版は、ネットワークから、ネットワーク・インターフェース107を通じて送信媒体中で実体化されたコンピュータ命令信号として提供され得る。

メンバ装置(member device)125は、ネットワーク接続127を介して、ネットワーク109を通じても通信可能である。メンバ装置125は、ネットワーク・インターフェース107またはＩ／Ｏインターフェース111(不図示)を介して、好ましいチャンネル129を通じて、コンピュータ101とも通信可能である。

【００１０】

一つの実施例は、安全な(secure)信用保証(credential)インフラストラクチャーの構築に向けられる。そのような安全な信用保証インフラストラクチャーには、(１)暗号化された情報を表すデータが、意味(meaning)だけを、正しい鍵を持つコンピュータに運ぶように，または，(２)信用保証インフラストラクチャーが、他のメンバーへの認証を行うために装置が信用保証を使用することを可能とするように，または，(３) 信用保証インフラストラクチャーが、他のメンバーまたはサービス・プロバイダに対して認証を行うために装置が信用保証を使用することを可能とするように，ネットワークを介して送られた情報を暗号化するための、鍵(例えば、秘密鍵、または公開・秘密鍵の組)を用いる、有線の(wired)の、および、ワイヤレスのネットワークが含まれる。この実施例は、公開鍵インフラストラクチャーのような、安全な信用保証インフラストラクチャー、ワイヤレス・ネットワーク、有線ネットワーク、および、ハイブリッド・ネットワークに適用される。本発明の一つの実施例は、ターゲット装置を、公開鍵インフラストラクチャー(ＰＫＩ)に加えるために使用され得、これによって、メンバー装置を有するＰＫＩを構築する。以下のものの多くは、安全な信用保証インフラストラクチャーに向けられるが、本発明の特徴は、

ＰＫＩにも適用される。

【００１１】

図２は、パワーが最初に信用保証発行装置に印加された時に呼び出される、または、信用保証発行装置がリセットされた時に呼び出される、「安全な信用保証インフラストラクチャー構築」の工程200を説明する。「安全な信用保証インフラストラクチャー構築(secure credential infrastructure construction)」の工程200は、開始され、信用保証発行権限を構成する「信用保証発行権限構成(credential issuing authority configuration)」の工程203に続く。

一旦、証明権限(certification authority)が構成されると、「安全な信用保証インフラストラクチャー構築」の工程200は、予想されるメンバー装置が、信用保証発行装置に、好ましいチャンネルを介して通信するために利用可能な時を検知すると、予想されるメンバー装置が、好ましいチャンネル以外のいくつかのネットワークを介して信用保証発行装置と通信することを可能とするために、ネットワーク構成情報を、予想されるメンバー装置に任意に提供し、予想される(prospective)メンバー装置を事前に認証(pre-authenticates)する、「予想されるメンバー装置の事前認証(prospective member device pre-authentication)」工程205に続く。

一旦、予想されるメンバー装置が事前に認証されると、「予想されるメンバー装置に信用保証を自動的に提供する(automatically provision prospective member device with credential)」手順207が、予想されるメンバー装置に、予想されるメンバー装置のための信用保証(ＰＫＩの場合には公開鍵証明)、および、信用保証装置の公開鍵証明、および、予想されるメンバー装置によって要求される何らかの他の情報、または、登録(enrollment)ステーションによって自動的に提供される何らかの他の情報、を提供することによって、予想されるメンバー装置を提供する(provisions)。

【００１２】

「安全な信用保証インフラストラクチャー構築」の工程200は反復して、各予想されるメンバー装置が、安全信用保証インフラストラクチャーに追加されるための、「予想されるメンバー装置の事前認証」工程205に戻る。

一旦予想されるメンバー装置が提供されると、それはメンバー装置になり、その信用保証を使用出来る。これは、ネットワークに亘った安全な通信を可能とするため信用保証を用いること、および、装置，ネットワーク，サービス，コンテイナ(containers)，オフィス空間，または他の装置，エリア，または、認証及び／又は授権、または、アクセスへの信用保証を要求するサービス、へのアクセスを提供するために信用保証を使用することを含む。

他の安全なネットワークのための供給サービス(provisioning service)を実行するいかなる装置にも加えて、「安全な信用保証インフラストラクチャー構築」の工程200を実行するいかなる装置も、信用保証発行装置として考慮の対象とされる。しばしば、信用保証発行装置には、信用保証発行権限(authority)(ＰＫＩの文脈においては、証明権限(ＣＡ：certificate authority))が含まれる。公開鍵インフラストラクチャは、信用保証発行装置を通じた、予想される数の装置へ(公開鍵証明のような)信用保証を提供する、(証明権限のような)信用保証発行権限を含む安全信用保証インフラストラクチャの一つの場合に過ぎない。予想されるメンバー装置による信用保証の保持は、装置を、安全信用保証インフラストラクチャのメンバー装置にする。信用保証の保持は、メンバー装置に、認証(authenticate)及び／又は権限付け(authorize)する、またはアクセスする能力を提供する。

【００１３】

好ましいチャンネルは、位置が限定されたチャンネル(location-limited channel)、または、例証識別プロパティ(demonstrative identification property)および認証プロパティ(authentication property)の双方を持つ何らかの他のチャンネルであり得る。

例証識別プロパティは、識別が、物理的コンテキスト(physical context)(例えば、「私の前のプリンタ」、「部屋の中の全てのＰＤＡ」であるがこれに限定されない)に基づ

くことを要求する。好ましいチャンネルは、それらの送信についての固有の物理的制限を持つ通信技術を用いる。そのような技術の例(これには限定されない)には、可視的な、または不可視的な、赤外線通信、短い経路の電線を通じた通信、音声(可聴および不可聴(例えば超音波)の双方)、物理的なコンピュータ読取可能な媒体[リムーバルな媒体またはドライブ{例えばフレキシブル・ディスク、リムーバブル・ディスク、ＵＳＢ記憶装置(フラッシュ・メモリ・ペンまたはディスク・ドライブのような)或いは他の有形のデータ・キャリア)}のような]、物理的な電子接触、本体を横断する近似電界信号(near-field signaling across the body)、および短距離ＲＦ、および、オペレータがコードを入力することを要求する実施例(他の例は、図８を参照した議論の中に発見できる)、を用いて一つの装置から他の装置に情報を渡すことによる通信、のような電磁的放射通信が含まれる。好ましいチャンネルの例証識別プロパティは、人間のオペレータが、どの装置が、好ましいチャンネルを通じて互いに通信しているかを認知していること、および、人間のオペレータが、いつ、好ましいチャンネルに対して攻撃(attack)が為されているかを容易に検知できることを意味する。

【００１４】

好ましいチャンネルの確実性プロパティ(authenticity property)は、攻撃者にとって、正当な通信の当事者によって検知されること無しに、好ましいチャンネルを通じて送信すること、または、好ましいチャンネルを通じて送られたメッセージにいたずらをする(tamper)ことが不可能または困難であることを意味する。

攻撃者が、検知されずに好ましいチャンネル上で送信出来ない限り、好ましいチャンネルは、セキュリティを要求しない。好ましいチャンネルの、位置が制限された性質に起因して、攻撃者がチャンネルをモニタすることは困難であるし、検知されずにチャンネルの上で送信することは尚更困難である。

参加者の鍵を事前認証(pre-authenticate)するための、好ましいチャンネルの使用は、安全な信用保証インフラストラクチャのアドミニストレータが、鍵が、好ましいチャンネルへのアクセスを持つ、予想されるメンバー装置のみに提供されることを確信することを可能とする。予想されるメンバー装置のユーザは、好ましいチャンネルへの物理的アクセスを持っていたはずなので、このようにして、「信頼」を確立することになる。

事前認証工程の最中に、各参加者の公開鍵へのコミットメント(commitments)(後述)は、好ましいチャンネルを通じて交換される。一旦、コミットメントが交換されると、装置は、鍵交換プロトコルまたは手順を実行でき、更なる安全な通信を達成する。説明のために、一旦鍵が受け取られると、それは、受け取った鍵が、好ましいチャンネルを介して提供されたコミットメントに一致することをチェックすることによって照合される。一旦、鍵が照合されると、良く知られた技術が使用されて、鍵を用いて通信が開始される。一旦公開鍵が照合され、公開鍵の提供者が、公開鍵に対応する秘密鍵の保持を証明すると、信用保証発行権限は、その使用のために、予想されるメンバー装置が、ＰＫＩの実際のメンバー装置となるように、信用保証を予想されるメンバー装置に提供できる。

【００１５】

一つの情報Ｘ(a piece of information X)へのコミットメントは、Ｘと一致するために認証され得る一つの情報Ｃである。コミットメントは、それが、ＸおよびＣを知っている攻撃者にとってさえ、Ｃがやはり一致する、異なった情報(piece of information)Ｙを生成することが暗号的に困難であるときには、「バインディング(binding)」である。

コミットメントは、Ｃを知っている攻撃者にとって、Ｘについての部分的情報さえも抽出することが暗号的に困難である時には「ハイディング(hiding)」である。

Ｘに対するバインディング・コミットメントおよびハイディング・コミットメントの例は、Ｈが暗号的に安全なハッシュ関数であり得るときにＨ(Ｘ)であり得る。当業者は、コンテキスト(context)から、使用されたコミットメントが、バインディング、ハイディング、または、その双方、である必要があるか否かを理解するであろう。

コミットメントは、もしそれが、好ましいチャンネルを介して受信されたならば、或いは、受信人が信頼する当事者からデジタル署名を与えられたならば、信用を確立するため

に使用され得る。信頼されたコミットメントは、(恐らく、信頼されないチャンネルを介して受信された、或いは、署名がされていない)情報の一致部分(matching piece of information)の信頼のレベルが、コミットメントと同じ信用のレベルまで評価されることを可能とする。

【００１６】

図３は、「信用保証発行権限構成」工程203によって使用され得る「信用保証発行権限構成」工程300を示す。この工程は、信用保証発行装置が信用された(trusted)信用保証(credential)を持つように、信用保証発行装置を初期化するために使用され得る。「信用保証発行権限構成」工程300が開始され、良く知られた技術を用いて公開鍵および秘密鍵を生成する「信用された鍵の組の生成(create trusted key pair)」の工程303に継続する。「信用された鍵の組の記憶(store trusted key pair)」工程305は、信用される鍵の組を、記憶装置に記憶する。一旦、信用された鍵の組が生成されると、「信用保証発行権限構成」工程300が、「発行権限信用保証の生成(create issuing authority credential)」工程307に続く。

「発行権限信用保証の生成」工程307は、自己署名された(self-signed)信用保証(「ルート」信用保証(a "root" credential))を生成できる。「発行権限信用保証の生成」工程307は、連鎖的信用保証(chained credential)を得て、連鎖的信用保証を、信用保証発行装置にインポート(import)して戻すために、親証明権限へのアクセスも行う。一旦、信用保証が生成され、或いは得られると、「発行権限信用保証の記憶(store issuing authority credential)」工程309が、いくらかの利用可能な記憶部に、後の利用のために、信用保証を記憶する。

他のサービスまたは特徴が、「他の初期化(other initialization)」工程311によって初期化され得る。これらのサービス及び／又は特徴は、ディレクトリ・サービス、認証取消リスト(ＣＲＬｓ：certificate revocation lists)の生成、または、信用保証状態処理、および他のサービスを含み得る。更に、これらのサービスは、例えば、鍵の組の生成サービス、802.11ａ/ｂ/ｇ提供サービス(provisioning services)、ネットワーク・アドレス提供サービス、等、を含み得る。「信用保証発行権限構成」工程300は、「終了」ターミナル313を通じて完了する。

【００１７】

図４は、「予想されるメンバー装置の事前認証」工程205によって用いられる、信用保証発行装置400のための事前認証工程を説明する。

信用保証発行装置400のための事前認証工程は、予想されるメンバー装置に、信用保証が提供され得、安全信用保証インフラストラクチャのメンバー装置となるように、信用保証発行装置と予想されるメンバー装置の間の信頼を確立するために使用され得る。

信用保証発行装置400のための事前認証工程は、開始されて、予想されるメンバー装置について、好ましいチャンネルを確立するために用いられることになる、一つあるいはそれ以上の、信用保証発行装置のＩ／Ｏポートを起動する「位置限定のポートの初期化(initialize location-limited ports)」工程403に続く。

好ましいチャンネルは、図８を参照して記載されるもののような、何らかの位置限定(location-limited)通信メカニズムを用いて確立され得る。一旦好ましいチャンネル・ポートが初期化されると、信用保証発行装置のための事前認証工程400は、「位置限定ポートの初期化」工程403によって初期化された位置限定ポートの一つを用いて、信用保証発行装置と予想されるメンバー装置の間の好ましいチャンネルを通じた通信を確立する「好ましいチャンネルを通じた通信の確立(establish communication over preferred channel)」工程405に続く。一旦、(例えば、装置上のＩＲポートをアライニング(aligning)させることによって)予想されるメンバー装置と信用保証発行装置の間に通信が確立されると、信用保証発行装置のための事前認証工程400は、公開鍵のためのコミットメントを生成する「コミットメント情報の交換(exchange commitment information)」工程407に続く。コミットメントは、好ましいチャンネルを通じて予想されるメンバー装置に送られる。信用保証発行装置は、鍵に対する予想されるメンバー装置からのコミットメント、または、予

想されるメンバー装置が信用保証発行装置に送る秘密、をも受信する。

【００１８】

次に、「通信可能化情報の提供(provide communication enablement information)」工程409が、予想されるメンバー装置に、信用保証発行装置が、予想されるメンバー装置と、(好ましいチャンネルと比較して)所望の通信メディアを介して通信するために要求されるネットワーク構成情報を提供できる。例えば、信用保証発行装置がＷＡＰである場合には、それは、ＳＳＩＤ、および恐らくワイヤレス・チャンネル選択、及び／又はＷＥＰ鍵を指定出来る。そして、有線ネットワークのためには、信用保証発行装置は、ＭＡＣアドレス及び／又は静的なＩＰアドレスを指定出来る。「通信可能化情報を提供」工程409は、多くの実施例においてオプションであり、予想されるメンバー装置は、ネットワーク通信のために事前に構成されたもので有り得る。しかし、「通信可能化情報を提供」工程409の一つの利点は、それが、予想されるメンバー装置のためのネットワーク構成工程を単純化することである。例えば、しかしこれに限定されることなく、信用保証発行装置は、(ＤＨＣＰアドレスに比較して)固定ネットワークアドレスを、予想されるメンバー装置に自動的に割り当てること、ＳＳＩＤを指定すること、ＷＥＰ鍵，ドメイン名，ＩＰアドレス，ＶＰＮアドレス，ゲートウェイ・アドレス，ブルートゥース・アドレス，セキュリティ設定，セキュリティ・ポリシー，ビット長，または、信用保証発行装置と予想されるメンバー装置の間の、好ましいチャンネル以外のチャンネルを介した通信を確立するために必要な他の情報、を指定すること、が可能である。更に、ただのネットワーク構成情報を越えた、他の情報が提供され得る。更に、通信可能化情報は、予想されるメンバー装置を更に提供するために使用され得る、安全通信チャンネルをブート・ストラップするために使用され得る。

一旦コミットメントが交換されると、信用保証発行装置および予想されるメンバー装置が、好ましいチャンネルではないネットワークを介しての通信を実行可能となるように、「鍵交換」手順411が鍵を交換する。「鍵交換」手順411は、公開鍵を交換するために、好ましいチャンネルまたは暗号化されたデータ・パスを使用する必要は無い。しかし、もし秘密鍵が交換されているならば、安全な通信(secure communication)が要求される。更に、何らかの秘密データが暗号化されている限り、好ましいチャンネル(preferred channel)が、「鍵交換」手順とともに使用され得る。これは、好ましいチャンネルが、時宜を得たタイミングでプロトコルを運ぶ(carry)ために十分な帯域幅を持つ場合には有用であり得る。

一旦鍵が交換されると、「鍵のコミットメントとの照合(verify keys with commitment)」手順413が、受信された鍵が、コミットメントと一致することを照合する。例えば、受信された鍵が、コミットメントと一致することを照合することは、鍵の暗号のハッシュを計算して、このハッシュがコミットメントと等しいことを照合することによって実行され得る。一旦公開鍵が、コミットメント情報によって照合されると、「秘密鍵の保持の照合(verify possession of private key)」手順414が、照合された公開鍵を提供している装置が、対応する秘密鍵をも保持する、というプルーフ(proof)を確立する。信用保証発行装置400のための事前の認証工程は、終了する。

本発明の実施例において、実際の鍵は、コミットメントとして提供され得る。次に、鍵が交換された時に、受信された鍵が、以前受信したコミットメントと一致することを照合することは、単に、それらが等しいことを確かめることによって為され得る。

【００１９】

図５は、図４の信用保証発行装置400に対する事前認証工程に非常に類似する、予想されるメンバー装置500に対する事前の認証工程を説明する。予想されるメンバー装置500のための事前認証工程には、「開始」ターミナル501、「位置制限されたポートの初期化(initialize location-limited ports)」工程503、「好ましいチャンネルを介した通信の確立(establish communication over a preferred channel)」工程505、「コミットメント情報の交換(exchange commitment information)」工程507、「通信可能化情報の受信(receive communication enablement information)」工程509、「鍵交換(key exchange)」工

程511、「鍵のコミットメントとの照合(verify keys with commitment)」工程513、「秘密鍵の保持の照合(verify possession of private key)」工程514、および、「終了」ターミナル515が含まれる。これらの工程は、「通信可能化情報の受信(receive communication enablement information)」工程509を除いて、実質的に図４に示される対応する工程と同じである。

「通信可能化情報の受信」工程509は、信用保証発行装置によって提供された情報を、「通信可能化情報の提供」工程409で受信し、予想されるメンバー装置が一つあるいはそれ以上のネットワークを介して通信するように、予想されるメンバー装置を調節するか、さもなければ、適切に、通信可能化特有の情報(communication enablement-specific information)を処理する。

「好ましいチャンネルを介した通信の確立」工程405、および、「好ましいチャンネルを介した通信の確立」工程505に関しては、好ましいチャンネルを介した通信を確立するための、少なくとも２つのモードが存在する。これらのモードは、如何にして通信が確立されるか、において異なる。第１のモードにおいては、予想されるメンバー装置は明白に、好ましいチャンネルを介して信用保証発行装置への接続を開始出来、信用保証を要求出来る。これは、予想されるメンバー装置に、指定された信用保証発行装置との信用保証の交換を開始させることによって実現できる。好ましいチャンネルの確立の一つの例は、予想されるメンバー装置と、信用保証発行装置の、赤外線または可視光の光ポートのアライニング(aligning)によるものである。接続例の、更なる例は、図８を参照して以下に説明される。

【００２０】

信用保証発行装置の指定は明示的(explicit)(例えば、「私が電子的接続を確立したこの装置」、「私が触るこの装置」、「特定のＩＲポートとアラインされているこの装置」)、または、黙示的(implicit)(例えば、「私が、私の装置から発行された可聴信号を受信できる何らかの装置」)で有り得る。

第２のモードにおいて、好ましいチャンネルを介した通信は、ユーザが、予想されるメンバー装置を、シリアル・ポートによって、またはＵＳＢポートによって、または、予想されるメンバー装置に安全信用保証インフラストラクチャ(secure credential infrastructure)に対応付けられた信用保証授与トークン(credential-granting token)に応答させることによって、信用保証発行装置に付着されたクレードル(cradle)、の中に置くことのようなアクションに応じて、信用保証発行装置によって開始され得る。このアプローチを用いて、予想されるメンバー装置は一般的に、信用保証発行装置からの、事前認証要求の受領が可能なように構成され得る。この構成における予想されるメンバー装置は、例えば、信用保証を受け取るアプリケーションを実行でき、受信した信用保証を判断し処理することができる。他の例において、予想されるメンバー装置は、信用保証を受け取るバックグラウンド・プログラムをサポートでき、(オプションのユーザ確認又は他のフィードバックを伴って)それを、他の登録されたアプリケーションに利用可能とできる。

信用保証授与トークンは、(ＪＡＶＡ（登録商標）カードのような)ポータブルな信用保証発行装置、信用保証を生成可能で、予想されるメンバー装置を直接提供可能なスマート・カード、を含み得る。他の装置は、たとえば、安全信用保証インフラストラクチャに所属すべき、予想されるメンバー装置のグループの間の通信を蓄積し、記憶するための記憶装置として機能する。最後に、信用保証発行装置は、信用保証発行装置の信用保証発行ファンクションを可能とするために、鍵の身元識別(identification)を要求できる(例えば、そのような鍵は、信用保証発行装置が信用保証を提供する前にアクセスされねばならない、ＵＳＢ記憶、または、生物測定のセンサーで有り得る。)。

好ましいチャンネルは、検知されないアクティブな攻撃に対して耐性を持つはずであり、それ故、それを通じて輸送されたデータに、真正特性(authenticity property)を与えるはずなので、鍵は、好ましいチャンネルを介して輸送される。公開情報(例えば、公開鍵、または、公開鍵へのコミットメント)だけが、そのチャンネルを介して送られるので、好ましいチャンネルとして用いられるチャンネルは、盗聴者に対して耐性を持つ必要が

無い。そして、そのような鍵またはコミットメント情報を、好ましいチャンネルを介して送ることによって、互いに一組の装置自身を認証する一組の装置が、互いとの安全な通信をセット・アップすることが可能である。何故なら、それらは、好ましいチャンネルを介してコミットされたまたは交換された公開鍵に対応する秘密鍵の保持を立証出来るからである。好ましいチャンネルを介して送られたコミットメントまたは鍵を検知する盗聴は、対応する秘密鍵の保持を立証できず、それ故、正当な当事者の間の通信に影響を与えることが不可能である。更に、鍵コミットメント(そして恐らく、ＬＡＮまたはインターネットのような、好ましくないチャンネルに対する重要な通信パラメータ)を運ぶに際して、好ましいチャンネルは、非常に狭い(low)帯域のチャンネルであり得る。信用保証および他の情報の、予想されるメンバー装置への提供は、好ましくない(non-preferred)、一つあるいはそれ以上のチャンネルを用いて実現され得る。

【００２１】

コミットメントを交換するための例示のプロトコルは、以下のようなものである。

２つの鍵のための事前認証は、好ましいチャンネルを介して為される。

１．Ａ→Ｂ：$addr_A$，$h(PK_A)$

２．Ｂ→Ａ：$addr_B$，$h(PK_B)$

認証は、PK_AおよびPK_Bを交換して安全な通信を確立するための、何らかの標準鍵交換プロトコルを伴った、好ましいものでない(non-preferred)(ワイヤレス)チャンネルを介して続く。例えば、

１．Ａ→Ｂ：TLS CLIENT HELLO

２．...等々。

種々のシンボルは：

$addr_B$，$addr_B$：便利さのためだけに、ワイヤレス空間でのＡの(およびＢの)アドレスを意味する。

PK_A，PK_B：Ａ(またはＢ)に属する公開鍵で、長寿命鍵か、この交換でのみ使用される短命な鍵かのいずれか；

$h(PK_A)$：PK_Aへの通信。例えば、鍵の符号化の一方方向のハッシュ。

好ましいチャンネルを介して行われる、一つの鍵のための事前認証：

１．Ａ→Ｂ：$addr_A$，$h(PK_A)$

２．Ｂ→Ａ：$addr_B$，$h(S_B)$

認証は、PK_Aおよび秘密を交換するための、何らかの標準鍵交換プロトコルを伴う、好ましいものではない(non-preferred)(ワイヤレス)チャンネルを介して継続する。例えば、

１．Ａ→Ｂ：PK_A

２．Ｂ→Ａ：$E_{PKA}(S_B)$

【００２２】

種々のシンボルは、

$addr_A$，$addr_B$：便利さのためだけのための、ワイヤレス空間でのＡ(或いはＢの)アドレス；

PK_A：長寿命鍵か、この交換だけのために使用される短寿命鍵かのいずれかの、Ａに属する公開鍵；

S_B：Ｂに属する秘密(secret)；

$h(PK_A)$：PK_Aへのコミットメント。例えば、鍵の符号化の一方方向のハッシュ；

$h(S_B)$：S_Bへのコミットメント；

$E_{PKA}(S_B)$：PK_Aの下でのS_Bの暗号；

を表す。

【００２３】

図６は、「予測されるメンバー装置への信用保証の自動的な提供(automatically provision prospective member device with credential)」工程207によって使用され得る、自

動予測されるメンバー装置の信用保証提供工程600を示す。自動的な予測されるメンバー装置の信用保証提供工程600は、予測されるメンバー装置に、信用保証を提供する。それはまた、予想されるメンバー装置に、他の提供情報(provisioning information）をも送る。

自動的な予測されるメンバー装置の信用保証提供工程600は開始されて、「提供情報要求の獲得(acquire provisioning information request)」工程603に続く。この「提供情報要求の獲得(acquire provisioning information request)」工程603は、予測されるメンバー装置からの情報を提供するための要求を受信できる。更に、この「提供情報要求の獲得」工程603は、事前に決定された、または、ユーザが選択した、提供情報を提供するために信用保証発行装置をトリガする状態を検知できる。この要求には、単に信用保証を提供すること、を越えた情報またはサービスのための要求(request)が含まれ得る。

一旦信用保証発行装置が、その要求を獲得すると、「提供情報の生成(generate provisioning information)」工程605が、信用保証、および、何らかの他の要求された提供情報を生成する。「提供情報の生成」工程605は、登録エージェントからの信用保証のための権限を要求することを含み得る。

「信用保証の発送(send credential)」工程607は、信用保証発行装置が、一つあるいはそれ以上の信用保証を、予想されるメンバー装置に送ることを引き起こす。一旦予想されるメンバー装置が、信用保証を受信すると、それは、安全な信用保証インフラストラクチャのメンバー装置となる。更に、「提供情報の発送(send provisioning information)」工程609は、信用保証発行装置からの提供情報Bを、予想されるメンバー装置に送る。

予想されるメンバー装置は、それに、信用保証発行装置または利用可能であり得る何らかの他の情報によって生成された鍵の組が提供されることを要求することもできる。

いくつかの実施例では、予想されるメンバー装置によって要求されない提供情報を送ることが可能である。

更に、予想されるメンバー装置は、いくつかの他のメンバー装置、セキュリティ・ゲートウェイ、等とのバーチャル・プライベート・ネットワーク(ＶＰＮ)を確立するために予想されるメンバー装置によって使用され得る情報を提供され得る。

いくつかの実施例での「予想されるメンバー装置への信用保証の自動的な提供(automatically provision prospective member device with credential)」工程207は、予想されるメンバー装置に、信用保証だけを提供する一方、他の実施例は、予想されるメンバー装置に、信用保証と他の要求された(またはデフォールトの)提供情報の双方を提供する(そして、いくつかの実施例では、信用保証を全く提供しない---図１０およびそれについての説明を参照)。

【００２４】

提供情報は、予想されるメンバー装置によって使用され得る何らかの情報であり得る。この情報は、アプリケーション特有の情報、サイト特有の情報、ネットワーク特有の情報、または、他の情報を含み得る。この情報は例えば、アプリケーションに依存する情報、装置特有の割り当て情報(例えば、病院の環境において、患者の名称、案件の番号、または、装置からデータを獲得するため、または、装置が動作するようにするために要求されるデータ獲得情報)、データベース・アクセス情報、(携帯電話番号のような)携帯電話(cell phone)提供情報、何らかの種類の所有者情報、車両情報、位置情報、安全な通信リンクを確立するために要求される情報(例えば、ＶＰＮ関連の情報)、協動的作業空間情報、無線チャンネル、何らかの種類のアプリケーション特有の情報、および、データベースにアクセスするために要求される情報、のような情報をも含み得るが、これに限定されない。従って、用語「提供(provisioning)」は、信用保証の提供に加えて、メンバー装置によって使用され得る他の情報の提供に適用される。いくつかの実施例において、提供情報は、複数の(multiple)通信チャンネルを用いて提供され得る。特に、提供情報(例えば、好ましいものでないチャンネルを介して一時的な通信を確立するために必要な情報)を、好ましいか、或いは好ましいものではない(non-preferred)チャンネルを介してブートス・トラップ後続通信(subsequent communication)(安全化されているか、いないかの、いず

れか)に送るために、好ましいチャンネルが使用され得る。上述の「鍵交換手順(key exchange procedure)」および「鍵照合手順(key verification procedure)」に引き続いて、２つの当事者は次に、その好ましいものではないチャンネルを介した、追加の提供情報の交換(これは、好ましいものではないチャンネルを介した、当事者間の、安全で認証された通信を確立するために使用され得る)に進むことが出来る。この追加の提供情報は、新たなメンバー装置が、他の、好ましいものではない、提供(provisioning)中に使用されないネットワーク接続で通信することを可能とするために十分な通信可能化情報を含む、上述の何らかの提供情報タイプを含み得る。他の実施例において、予想されるメンバー装置を提供するために、恐らく、追加的にその通信のいくつかを安全化(secure)するための鍵交換プロトコルの使用を伴って、好ましいチャンネル(preferred channel)のみが使用され得る。より一般的な実施例は、第１の提供情報の組が、好ましいチャンネルを介して提供され、他の提供情報が、第２の(一般的に安全な)通信チャンネルを用いて提供される場合である。

【００２５】

図７は、信用保証発行装置から、信用保証および他の提供情報を自動的に受信するために、予想されるメンバー装置によって使用され得る「予想されるメンバー装置サイドの提供(prospective member device-side provisioning)」工程700を示す。「予想されるメンバー装置サイドの提供」工程700は一般的に、事象(event)に応答して開始され、(予想されるメンバー装置500のための事前認証工程を呼び出す)「事前認証(pre-authentication)」工程703に続く。一旦「事前認証」工程703が完了すると、予想されるメンバー装置は、ネットワークを介して通信出来る。「要求提供情報(request provisioning information)」工程705において、予想されるメンバー装置は、信用保証および他の所望で利用可能な提供情報のための要求を送る。「信用保証の受信(receive credential)」工程707は、信用保証を受信し、「提供情報の受信」工程709において、自動予想メンバー装置信用保証提供工程(automatic prospective member device credential provisioning process)600によって送られた他の要求(request)提供情報を受信する。受信された信用保証および、あり得る他の提供情報は次に、使用のために利用可能とされ得る(予想されるメンバー装置内のアプリケーションか、予想されるメンバー装置のリーダ(readers)か、信用保証を使用するための従来技術で既知の他の方法か、のいずれかによって)。「予想されるメンバー装置サイドの提供」工程700は、「エンド」ターミナル711を通じて完了する。

いくつかの実施例は、ワイヤレス・ネットワーク上の(或いは有線ネットワークのための)802.1XおよびＥＡＰ－ＴＬＳプロトコルの代わりに(または、それに加えて)ＩＰＳＥＣ　ＶＰＮを提供する。更に、ファイヤー・ウォールを含み、システム／ユーザに対して信用保証を自動的に提供し、システム／ユーザがファイヤー・ウォールを通じて通信することを可能とする他の実施例が構想される。これは、システムが、インターネットまたは有線のまたはワイヤレスのＬＡＮから、ＶＰＮを通じて、ファイヤー・ウォールによって保護されたネットワークに接続することを可能とすることを含み得る。当業者は、キード・ホッピング・パターン等のような技術を用いてワイヤレスＬＡＮsを安全化するために、いくつかの実施例が使用され得ることを理解するであろう。

【００２６】

図８は、アンテナ803を通じて電子信号を提供するための、これもまたワイヤレス・アクセス・ポイント(ＷＡＰ)として構成された、提供装置801を用いる、ワイヤレス・アクセス・ポイントの安全化信用保証インフラストラクチャ・システム(secure credential infrastructure system)800を説明する。ＷＡＰｓは、良く知られた技術であり、一般的に802.11(ａ)、(ｂ)、又は(ｇ)に適合するが、それらは、現存するか、或いはこれから開発される他のスタンダードにも適合する。提供装置801は、信用保証発行装置及び／又は提供装置の一つの実施例である。

提供装置801は、スイッチ、ルータ、ＤＳＬまたはケーブル・モデム、ファイヤー・ウォール、ＶＰＮクライアントまたはターミネータ、および、信用保証発行権限(credential issuing authority)のような追加の機能を持ちうる。これらの機能は、図８には示され

ない。提供装置801は、好ましいチャンネルを確立するために使用され得る一つあるいはそれ以上のポートをも持つ。提供装置801は、色々なやり方で、ポートの一つを用いて、予想されるメンバー装置821について好ましいチャンネルを確立出来る。提供装置801によってサポートされた好ましいチャンネルは、赤外線、可聴または非可聴の音声、音声または他の信号の電子表現、予想されるメンバー装置821と提供装置801の間を、ＵＳＢ　Ｂレセプタクルに付着されたＵＳＢケーブルを通じて、ＵＳＢ－Ａリセプタクル815にプラグ・インされ得、適切に装備された予想メンバー装置に渡され得る、除去可能なトークンを介して送られた情報、或いは、予想されるメンバー装置821上の検知エリアへ接触している間の、人間の、提供装置801上の近似フィールド検知エリア817への接触、による近似フィールドシグナリング(near field signaling)によって送られた情報、を含み得る。更に、好ましいチャンネルは、受話器を介したシグナリング・トーンを用いた、電話または携帯電話のスイッチング・システムを用いて確立された通信、または、電話ジャックを通じた直接接続によって確立された通信を含み得る。

他のあり得るポートは、(テキスト、データ・グリフ、または、変化するパターンのような)情報を表示するコンピュータ・スクリーンの画像を捕獲(capture)するために用いられるカメラでありうる。好ましいチャンネルのための、他のあり得る技術は、短距離無線周波数技術で有り得る。更に、ユーザがマニュアルで、情報を入力出来るための、キーボード、キーパッド、タッチ・スクリーン、等を用いて、情報が、予想されるメンバー装置821、および、提供装置801に提供され得る。

予想されるメンバー装置821は、好ましいチャンネル(この場合には、提供装置801の間の音声接続ケーブル825を用いた)、および、予想されるメンバー装置821を通じた通信を可能とする、アンテナ823、および一つあるいはそれ以上のポート(不図示)、を含む。

【００２７】

提供装置801は、アプリケーション特有の情報を提供(provision or provide)するために、或いは、信用保証を提供するために、ＩＰアドレス、プロキシ情報、ドメイン情報等のようなネットワーク構成情報を提供することによって、ワイヤレスまたは有線のネットワーク装置を提供するために、ＳＳＩＤコードおよびＷＥＰキーを提供することによって、ワイヤレス・ネットワーク化された装置を提供するために使用され得る。

例えば、コンピュータ、ワイヤレス・アクセス・ポート(ＷＡＰ)、または、好ましいチャンネルを持ち、「信用保証インフラストラクチャ構築の安全化(secure credential infrastructure construction)」工程200を実行するように構成された他の提供装置が、公開鍵インフラストラクチャを構築するために使用され得る。

信用保証発行装置が、ワイヤレス・アクセス・ポイント(ＷＡＰ)内に取り込まれたときに、ネットワーク構成情報を持つＷＡＰにアクセスするネットワーク装置を提供するために、本発明の一つの実施例が使用され得る。この提供は、ネットワーク装置が、予想されるよメンバー装置であるように、安全化信用保証インフラストラクチャにネットワーク装置を追加することで有り得る。更に、信用保証発行装置は、ＷＡＰによって認識された鍵(例えば、ＳＳＩＤ、および、ＷＡＰ内のワイヤド・イクイバレント・プライバシー(ＷＥＰ：Wired Equivalent Privacy)機能によって使用されるための鍵)を、好ましいチャンネルを介して、ネットワーク装置に提供出来、これによって、現在の技術によって要求されるような、エラーが発生しがちで、混乱しがちな、鍵を表す長いストリングの文字の入力を自動化出来る(いくつかのＷＡＰｓは、実際の鍵を直接提供する代わりにパス・フレーズ(passphrase)の使用を可能とするが、パスフレーズの使用は、ＷＥＰセキュリティーを減少する。更に、長い、任意の文字のストリングを入力する時に言語障害を起こす誰かの困難さを考慮する。)。更に、鍵が魔法の基礎にある(is in hex base)ことを理解しないために、鍵のテキストを数文字(numeric characters)に限定することによって、潜在的な鍵の組み合わせの数を減少させる、初心なユーザの成り行き(consequences)を考慮する。

共有された秘密およびＷＥＰ鍵が提供されうる。特に、何らかの「ネットワーク・パスワード」または、何らかのタイプの対称鍵(symmetric key)は、装置をワイヤレス・ネットワークに認証する(authenticate)ためにワイヤレス・ネットワークのためのデータを直

接暗号化することか、有線またはワイヤレス・ネットワークの上でＶＰＮを確立するために要求される情報を直接暗号化することか、更なる鍵交換を保護する、ことのいずれかが意図されている。

【００２８】

提供装置801が、ルータ、モデム、または、ＷＡＰとして動作する場合には、提供装置801は、トラフィックが、メンバー装置(即ち、安全なチャンネルを使用するために権限授与された装置)からのものか、いくつかの他の権限授与されていない装置からのものか、かを判断するために、提供装置801を通過するトラフィックをモニター出来る。提供装置801が、装置がメンバーであると決定する場合には、許可されない(unauthorized)装置をソースとすパケットがオープン・チャンネル(open channel)を通じてルーティングされる間に、メンバー装置をソースとするパケットは、自動的に安全化されたチャンネルを通じてルーティングされ得る。

これらの技術は、ルータ、ブリッジ、ハブ、ファイヤー・ウォール、ＶＰＮs、および、ＷＡＰ以外の装置に応用され得る。

【００２９】

図９は、異なった位置における複数のエンロールメント・ステーション(各々が、位置が限定されたチャンネルを持つ)にアクセスするための、信用保証発行装置901(または、証明権限(certification authority))を可能とする、エンロールメント・ステーション・ベースの構成(enrollment station based configuration)900を示す。これは、位置限定されたチャンネルが、(会社の各遠隔オフィスにおける、ような)複数の位置において配備されることを可能とする。エンロールメント・ステーションを、複数の位置に配備することによって、装置を、安全な信用保証インフラストラクチャに登録(enroll)することを求める人は、単に、エンロールメント・ステーションの一つに移動することによってそれを行うことが出来る。エンロールメント・ステーションの使用は、付加的な情報を追加し、予想されるメンバー装置の、安全な信用保証インフラストラクチャへの登録(enrollment)に権限付与するために、(登録エージェントまたは他のエージェントのような)証明工程に人間を含ませる一つの方法であり得る。エンロールメント・ステーションの使用の他の利点は、それが、(信用保証発行権限付与サービスを提供する)信用保証発行装置901が、事前の認証の知識、または、好ましいチャンネルの知識を持たない、棚から降ろした(off-the-shelf)ソフトウェアを使用することを可能とすることである。

登録エージェント(registration agent)または、他のエージェントもまた、例えば、事前の権限付与を承認するために特定のトークンを用いることによって、しかしこれに限定されずに、(これまで説明されてきたように、予想されるメンバー装置が、好ましいチャンネルへのアクセスを持つという要求を越えた)予想されるメンバー装置の付加を限定し得る。また、付加を承認するために、他の装置を用いる。

信用保証発行装置901は、ネットワーク903を介して、ネットワーク接続907によって、メンバー装置905に通信出来る。更に、信用保証発行装置901は、(ＶＰＮのような)安全なネットワーク接続911を介して、エンロールメント・ステーション909に通信出来る。エンロールメント・ステーション909は、好ましいチャンネル913を介して、メンバー装置905を登録(enroll)出来、安全なネットワーク接続911を介して信用保証発行装置901と通信出来る。信用保証発行装置901およびエンロールメント・ステーション909は、当該技術分野で既知の技術、およびここに記載される技術を用いて、相互に、互いに、認証出来る。

先に説明されたように、ネットワーク装置の構成を単純化することに伴う問題が存在する。この問題は、本発明の他の実施例、即ちネットワーク提供装置(network provisioning device)、によって言及される。ネットワーク提供装置は、ネットワーク装置が通信することを可能とするために、ネットワーク装置にネットワーク構成情報を提供するために使用され得る、好ましいチャンネルを持つ。この機能の詳細の多くは、これまでに説明されてきた。

【００３０】

図１０は、ネットワーク提供装置によって使用され得る、自動ネットワーク装置構成工

程1000を説明する。自動ネットワーク装置構成工程1000は、パワー・オン、または、リセットの状態で開始し、ネットワーク提供装置を初期化して、ユーザまたは初期化システムが、要求されるネットワーク情報を指定することを可能とする「構成提供装置」工程1003に続く。「好ましいチャンネルを介したネットワーク装置との通信の確立」工程1005は、これまでに説明されたのと類似のやり方での、チャンネルを介したネットワーク装置との通信を確立する。一旦、通信が確立されると、「ネットワーク構成情報のネットワーク装置への送信」工程1007が、ネットワーク構成情報をネットワーク装置に送る。

これまでに説明したように、ケーブル接続されたセンサを引きまわす(work around)ことが困難であるが、現時点では、患者のプライナシーを保護するために十分に安全なワイヤレス・センサを提供することが余りにも困難であるような、医療環境での問題が存在する。しかし、これまでに述べたように、単に、信用保証を発行し、管理する能力を持つことによって、この問題に対する新規の解決策が可能となる。

本発明の他の実施例は、ワイヤレス・センサによってデータが集められ、データがプライベートなものか法的に保護されているような環境での、情報の管理および分配に応用できる。そのような環境の１つの例は、病院である。現在の労働集約的で面倒な、患者の生命力の測定方法(即ち、人間が測定を行い、記録することを要求することによるもの)の代わりに、自動化されたセンサを用いて、患者のデータを捕捉し、正確に、そのデータをデータベースまたは他のリポジトリに送出するものである。しかし、導線がセンサに付着した状態は、病院の部屋を酷く散らかし、しばしば、患者、医者、看護士、および他の病院スタッフに迷惑をかける。したがって、ワイヤレスのセンサが望まれる。しかし、このアプローチが成功する前に、ワイヤレスセンサは、簡単に、セット・アップされねばならず、権限付与されない個人が、センサによって測定された患者データにアクセスできないように安全化されねばならない。

【００３１】

病院或いは医療機関によって新しい装置が得られるにつれて、それらの新しい装置は、病院または医療機関の安全インフラストラクチャの一部としての信用保証発行権限によって提供された、信用保証を持つエンロールメント・ステーションで構成され得る。更に、その装置が、その使用環境で作動することを可能とするために、他の構成可能な情報が、装置に提供され得る(この情報は、新規の装置がアクセスすることとなるデータ・サーバへのコミットメントを含み得、したがって、装置が、それが、正当なデータ・リポジトリと通信しているということを知り、患者のデータを、非合法的なやり方で集めるように設計された悪党(rogue)の装置、の使用を避けることを可能とする)。

特定のセンサは次に(一時的に)、その患者と対応付けられたベッド・サイド・エンロールメント・ステーション(これは単に、その患者のための権限付与された装置のリスト内のその装置の公開鍵についての情報を記憶する)との類似の事前認証交換、または、看護士のステーションまたは医者のデスクにおける構成インターフェースとの類似の事前認証交換を使用することによって、特定の患者と対応付けられ得る。センサとバック・エンド(back-end)の病院インフラストラクチャの間の通信、または、センサと遠隔のデータ収集サイトの間の通信は次に、標準的技術を用いて安全化される。そして、データは、装置によって、および、特定の患者と対応付けられたシステムの装置の記録によって、提供された情報の組み合わせによって、適切な患者と対応付けられる。

遠隔監視の場合には、病院または診療所のファイヤー・ウォールは、自己構成ＶＰＮにしたがって、何れかの装置から入って来るデータの、病院／診療所の信用保証(瞬時ＰＫＩの一部)との接続を可能とするように構成され得る。

図１１は、家庭および病院の設定でのワイヤレス・センサーの使用を示した、安全なワイヤレス・センサ・システム1100を示す。上述のように、患者は、信用保証(および他のデータ)を提供されたセンサー1101と対応付けられ、患者識別情報(identification)が提供される。センサ1101は、患者に関連する情報を集め、ワイヤレス通信チャンネル1105を介して、ワイヤレス・アクセス・ポイント1103を通じて、その情報を安全に、患者データ記憶部1107に送る。センサは、患者が動きくにつれて、センサが情報を患者データ記憶部

1107に送信するための連続的な能力を維持しながら、医療設備内のいかなるＷＡＰへも、安全に通信できる。更に、ワイヤレス・センサは、いくつかの実施例によってエネーブルされているので、追加のセンサは、利用可能に、患者に付着され得る。一つのそのような例は、病院管理部が、何時でも、移動する患者がどこに存在するかを常に知ることができるようにして、患者の位置を認識するセンサである。そのようなセンサは、病院スタッフが、他のセンサが、患者での問題を示した場合、より迅速に応答すること、（および、どこに患者が存在し、医療管理を行う時刻が何時なのか、を検知すること）を可能とする。複数のＷＡＰｓのワイヤレス受信の強度に基づいて、三角測量法を用いることによって、患者を追跡するために、他の技術が使用され得る。

更に、適切な信用保証を持つ看護士または他の医療専門家が、センサに、患者識別情報、警報限界、服用量スケジュール、等、のような患者特有の情報を提供できる。

【００３２】

遠隔の患者の上のセンサ、例えば遠隔センサ1109は、ワイヤレス通信チャンネル1113を介してワイヤレス・アクセス・ポイント1111に安全に通信する。ワイヤレス・アクセス・ポイント1111は、ネットワーク1115および病院ファイヤー・ウォール1117を通じて、患者のデータ記憶部1107に情報を送る。遠隔のセンサ1109は、病院，患者の医師のオフィスのエンロールメント・ステーション，或いは他の場所、で提供され得る。医療監視へのこのアプローチは、患者の部屋の酷い散らかり状態を無くす一方、依然として、患者データの安全な通信を提供する。

ワイヤレス・アクセス・ポイント1103およびワイヤレス・アクセス・ポイント1111もまた、病院において、信用保証発行装置との通信状態で、エンロールメント・ステーションとして使用され得、信用保証発行装置として使用され得、センサに特定の患者関連の、患者データ，制限データ，警報データ，服用量データ，インターバル・データ(interval data)，アクセスデータ，医者のデータ、看護者データ，看護士データ，保険データ，および部屋割り当てデータ，のようなデータを提供するためにも使用され得る。

いくつかの実施例が、いかなるセンサーにも応用され得る。特に、いくつかの実施例は、監視、家庭またはオフィスのセキュリティ，または、安全化されるべき他の装置(位置および近接度センサ(proximity sensor)を含む)，のためのセンサー・ネットワークの要素に応用され得る。更に、センサは、医療情報，位置情報，近接度情報，(粒子放射への露出，化学的気体，音声レベル，煙レベル，環境熱，高度，風速，振動，動作への近接(proximity to motion)，湿度，および生物的エージェント(biological agents)のような)環境情報，および、乗物または乗物のグループ内のセンサ(乗物の速度，乗物の方向，乗物のサブ・コンポーネント(翼、エンジンまたはモータ測定，ブレーキ，のようなもの)の状態のようなもの)、または、ロボットを検知し、及び／又は、測定できる。位置，物体，人，およびターゲット，の画像を認識するために、および、特徴的なノイズを認識するために、更なるセンサが、使用され得る。そのようなセンサは、提供情報内のデータ(例えば、服用量データ、インターバル・データ(interval data)、起動データ(activation data)等)によって制御される起動要素(activation components)をも持ち得る。

【００３３】

ネットワークは、(以前に説明されたデータおよび、コンピュータ・プログラムを定義するデータのような)情報を送信する。プログラムおよびデータは、(コンパクト・ディスク、フレキシブル・ディスク、磁気ディスクのような)有形の物理的メディアおよび、ネットワークの双方から共通に読まれる。したがって、有形の物理メディアのようなネットワークは、コンピュータによって利用可能なデータ・キャリア(data carrier)である。

更に、ここに提供されるフローチャートは、説明目的のためのものであり、本発明の実施例を教示するために用いられる。基本となるアイデア(またはその修正)を取りこむ他のフローチャートは、均等物として考慮されるためのものである。

当業者は、本発明の実施例が、安全な信用保証インフラストラクチャの生成、管理、および維持、を非常に単純化していることを理解するであろう。したがって、ＰＫＩは、安価で効率的に、生成され、管理され得る。更に、いくつかの実施例の特徴は、今、伝統的

な安全な信用保証インフラストラクチャに関連する支出および必要経費が禁止された場合の、応用および環境における、安全な信用保証インフラストラクチャの使用を可能とする。

【００３４】

以上の説明から、本発明の実施例が、(限定無しに)一つあるいはそれ以上の以下の利点を持つことが理解されるであろう。

１）非セキュリティ・エクスポート(non-security exports)によって、迅速に、そして単純に、安全な信用保証インフラストラクチャを生成し、維持し、そして管理する能力。

２）コストの削減、および、安全な信用保証インフラストラクチャの生成における努力による、公衆に利用可能な、動的に(dynamically)改善されたセキュリティが、今、コンピュータの門外漢(layperson)が、彼らの通信を安全に維持することを可能とする。

３）情報が傍受される、または、プライバシー法令に違反する、という危惧無しに、人に関する感度の高い個人データを提供するワイヤレス・センサの使用を可能とする。

４）安全なワイヤレス・アクセス・ポイントの単純なセット・アップを可能とする。

５）ネットワーク装置の単純な提供(信用保証、ネットワーク特有の情報、アプリケーション特有の情報、または、これらのの組み合わせ、を伴ったもののいずれか)を可能とする。

６）厄介な信用証明工程(trust verification process)を要求されずにＰＫＩに参加する能力を可能とする。

【図面の簡単な説明】

【００３５】

【図１】一つの実施例によるネットワーク化されたコンピュータ・システムを説明する。

【図２】一つの実施例による、安全な信用保証インフラストラクチャ構築工程を説明する。

【図３】一つの実施例による、信用保証発行権限(credential issuing authority)の構成工程を説明する。

【図４】一つの実施例による、好ましいチャンネルを介して、予想されるメンバ装置(prospective member device)を事前に認証するための、信用保証発行装置によって使用され得る工程を説明する。

【図５】一つの実施例による、好ましいチャンネルを介して、信用保証発行装置を事前に認証するための、予想されるメンバ装置によって使用され得る工程を説明する。

【図６】一つの実施例による、自動的な、予想されるメンバ装置の信用保証提供工程(credential provisioning process)を説明する。

【図７】一つの実施例による、予想されるメンバ装置の提供工程を説明する。

【図８】一つの実施例による、ワイヤレス・アクセス・ポイントの安全な信用保証インフラストラクチャ・システムを説明する。

【図９】一つの実施例による、登録ステーション(enrollment station)ベースの構成システムを説明する。

【図１０】一つの実施例による、自動ネットワーク装置の構成工程を説明する。

【図１１】一つの実施例による、医療環境に配備された安全な(secure)ワイヤレス・センサ・システムを説明する。

【図１２】安全な通信警報システムの実施例を説明する。

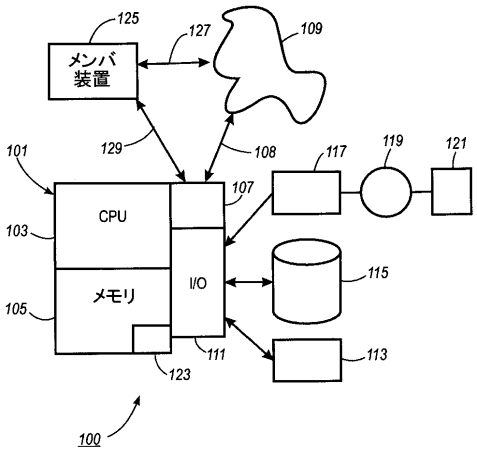
【符号の説明】

【００３６】

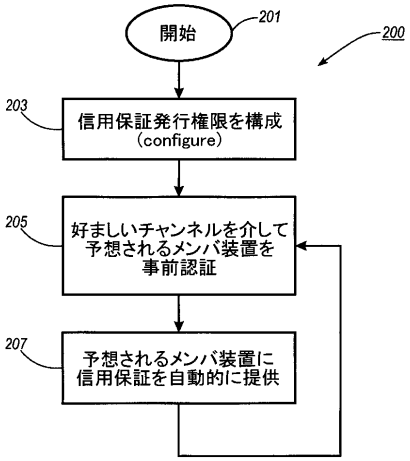
100　ネットワーク化されたコンピュータ・システム
101　コンピュータ
103　ＣＰＵ
105　メモリ
107　ネットワーク・インターフェース
109　ネットワーク

111　Ｉ／Ｏインターフェース
115　記憶システム
117　媒体データ装置
119　コンピュータ読み取り可能なメディア
121　プログラム・プロダクト
125　メンバ装置(member device)
127　ネットワーク接続
129　好ましいチャンネル

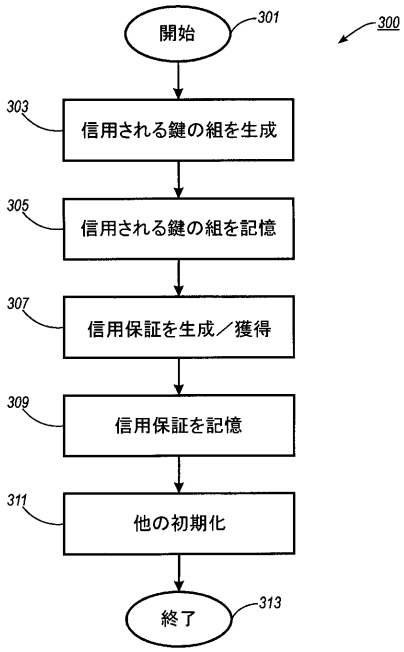
【図１】



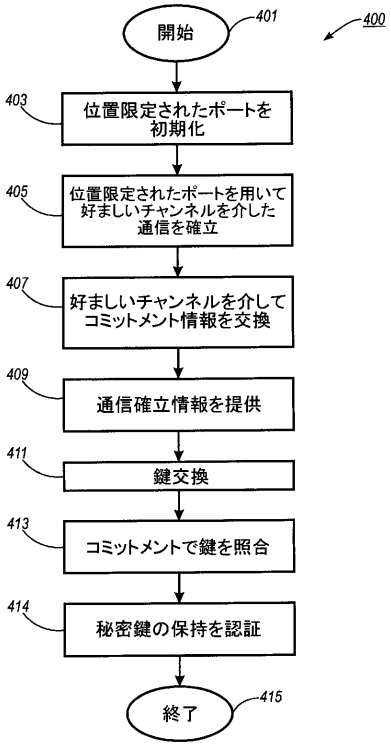
【図２】



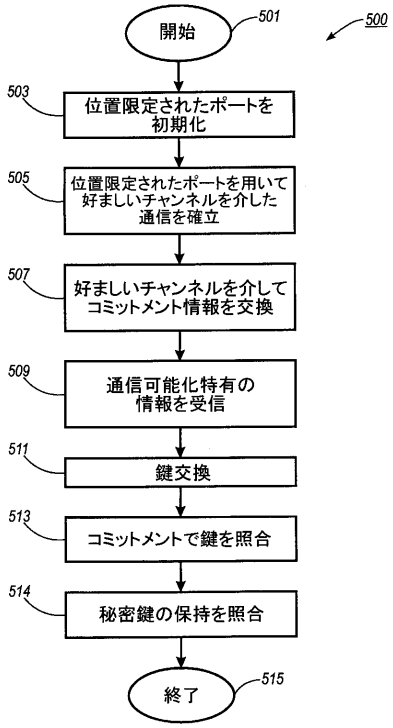
【図３】


300
開始
301
303
信用される鍵の組を生成
305
信用される鍵の組を記憶
307
信用保証を生成／獲得
309
信用保証を記憶
311
他の初期化
終了
313

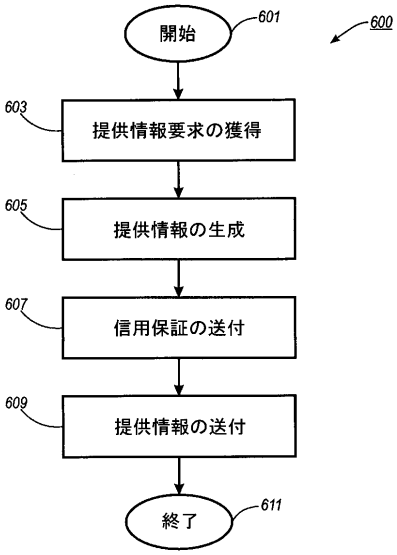
【図４】


400
開始
401
403
位置限定されたポートを初期化
405
位置限定されたポートを用いて好ましいチャンネルを介した通信を確立
407
好ましいチャンネルを介してコミットメント情報を交換
409
通信確立情報を提供
411
鍵交換
413
コミットメントで鍵を照合
414
秘密鍵の保持を認証
終了
415

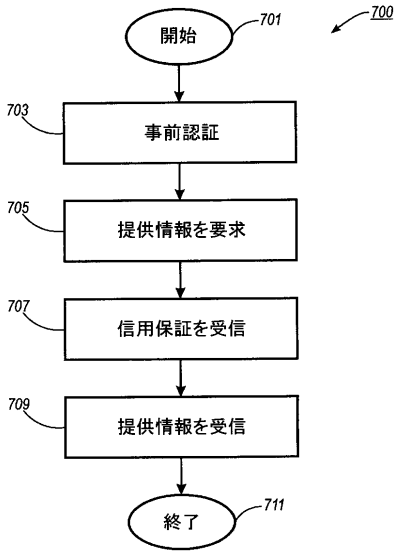
【図５】


500
開始
501
503
位置限定されたポートを初期化
505
位置限定されたポートを用いて好ましいチャンネルを介した通信を確立
507
好ましいチャンネルを介してコミットメント情報を交換
509
通信可能化特有の情報を受信
511
鍵交換
513
コミットメントで鍵を照合
514
秘密鍵の保持を照合
終了
515

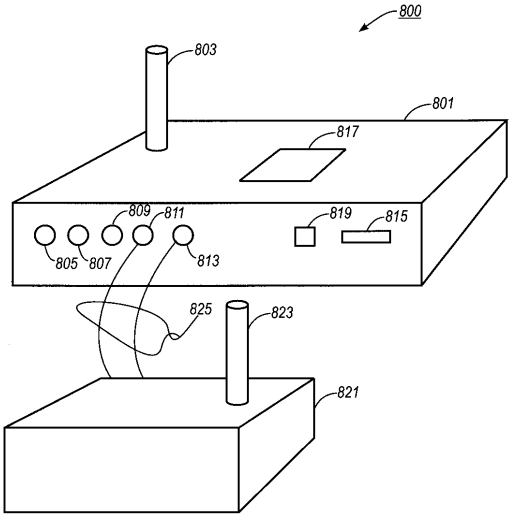
【図６】


600
開始
601
603
提供情報要求の獲得
605
提供情報の生成
607
信用保証の送付
609
提供情報の送付
終了
611

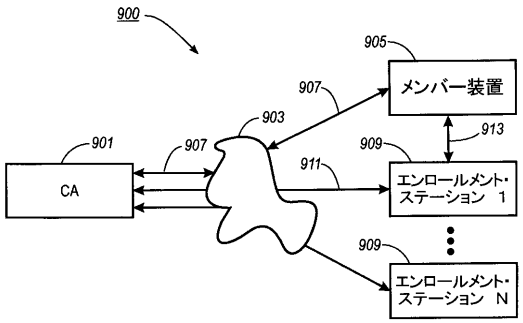
【図７】


700
開始
701
703
事前認証
705
提供情報を要求
707
信用保証を受信
709
提供情報を受信
終了
711

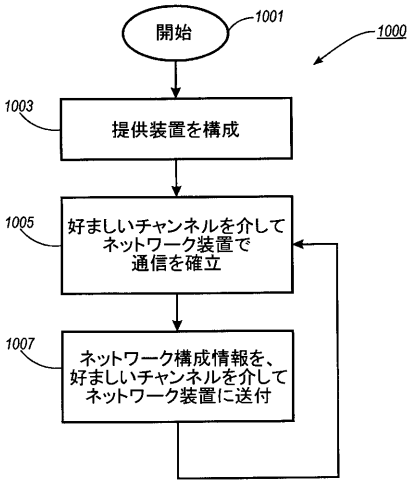
【図８】


800
803
801
817
809
811
819
815
805
807
813
825
823
821

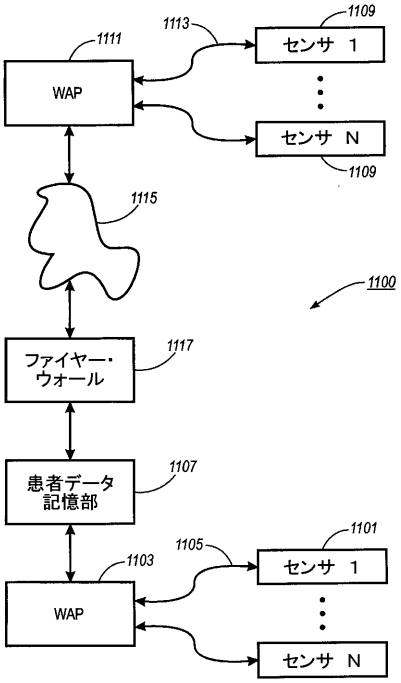
【図９】


900
905
メンバー装置
907
903
913
901
907
909
911
CA
エンロールメント・ステーション 1
909
エンロールメント・ステーション N

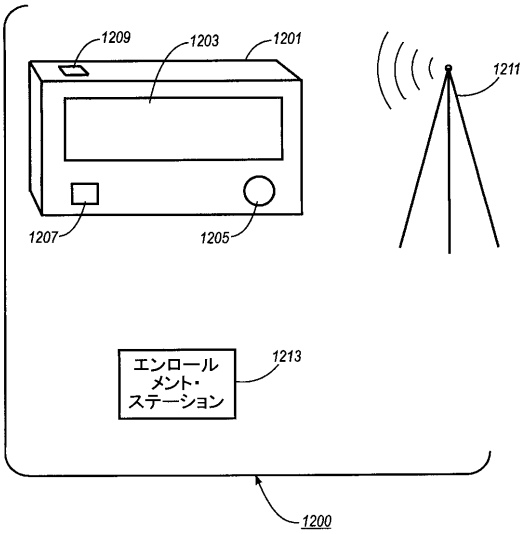
【図１０】


開始
1001
1000
1003
提供装置を構成
1005
好ましいチャンネルを介してネットワーク装置で通信を確立
1007
ネットワーク構成情報を、好ましいチャンネルを介してネットワーク装置に送付

【図１１】


1111
1113
1109
センサ 1
WAP
センサ N
1109
1115
1100
ファイヤー・
ウォール
1117
患者データ
記憶部
1107
1105
1101
1103
センサ 1
WAP
センサ N

【図１２】


1209
1203
1201
1211
1207
1205
エンロール
メント・
ステーション
1213
1200

フロントページの続き

(72)発明者 ダイアナ ケイ スメッターズ
アメリカ合衆国 カリフォルニア州 ９４１３１ サン フランシスコ シザー チャヴェッツ ストリート １／２ ４３１９
(72)発明者 ディルク バルファンツ
アメリカ合衆国 カリフォルニア州 ９４０２５ メンロ パーク シャロン パーク ドライヴ ３５０ アパートメント ディー１
(72)発明者 グレン イー ダーフィー
アメリカ合衆国 カリフォルニア州 ９４１１７ サン フランシスコ ＃４ ハイト ストリート ７０７
(72)発明者 レベッカ イー グリンター
アメリカ合衆国 カリフォルニア州 ９４１１０ サン フランシスコ ウィンフィールド ストリート ８３
(72)発明者 ポール ジェイ スチュアート
アメリカ合衆国 カリフォルニア州 ９４０２２ ロス アルトス ファースト ストリート １０１ ＃４６７
(72)発明者 ハオーチ ウォン
アメリカ合衆国 カリフォルニア州 ９４０７０ サン カルロス シダー ストリート ３６８

合議体
審判長 藤井 浩
審判官 矢島 伸一
審判官 山本 章裕

(56)参考文献 特開２００３－３０９５５８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/08
H04L 29/08
G08C 17/00