(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2012-531111
(P2012-531111A)
(43)公表日　平成24年12月6日(2012.12.6)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 64/00	(2009.01)	H04Q	7/00	509	5K067
H04W 48/16	(2009.01)	H04Q	7/00	502	
		H04Q	7/00	506	
		H04Q	7/00	406	

審査請求 未請求　予備審査請求 未請求　（全 46 頁）

(21)出願番号　特願2012-516320 (P2012-516320)
(86)(22)出願日　平成22年6月17日 (2010.6.17)
(85)翻訳文提出日　平成24年1月25日 (2012.1.25)
(86)国際出願番号　PCT/US2010/039092
(87)国際公開番号　WO2010/148260
(87)国際公開日　平成22年12月23日 (2010.12.23)
(31)優先権主張番号　61/218,888
(32)優先日　平成21年6月19日 (2009.6.19)
(33)優先権主張国　米国 (US)

(71)出願人　509065964
デバイススケープ・ソフトウェア・インコーポレーテッド
アメリカ合衆国・９４０６６・カリフォルニア州・サンブルーノ・ベイヒル　ドライブ・１００１・スウイート　１８５
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100098394
弁理士　山川　茂樹
(72)発明者　ウィン，サイモン
アメリカ合衆国・９４０６５・カリフォルニア州・レッドウッド　シティ・ボードウォーク　プレイス・８０７

最終頁に続く

(54)【発明の名称】ネットワークを介して位置を特定するためのシステム及び方法

(57)【要約】
ネットワークを介して位置を特定するためのシステム及び方法を開示する。いくつかの実施形態では、方法が、デジタル装置によって１又はそれ以上の無線ネットワークを求めて領域を走査するステップと、この１又はそれ以上の無線ネットワークに関連する１又はそれ以上のＢＳＳＩＤを受け取るステップと、この１又はそれ以上のＢＳＳＩＤを含む位置要求を、ＤＮＳプロトコルフォーマットのメッセージで生成するステップと、位置要求を提供するステップと、この位置要求に基づく位置応答を受け取るステップと、この位置応答から少なくとも１つの位置識別子を取り出すステップとを含む。
【選択図】　図１０

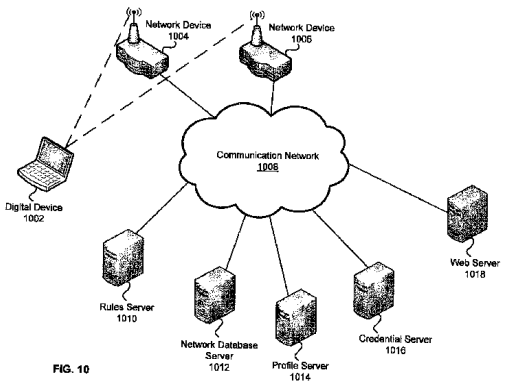

FIG. 10

【特許請求の範囲】
【請求項１】
デジタル装置によって１又はそれ以上の無線ネットワークを求めて領域を走査するステップと、
前記１又はそれ以上の無線ネットワークに関連する１又はそれ以上のＢＳＳＩＤを受け取るステップと、
前記１又はそれ以上のＢＳＳＩＤを含む位置要求を、ＤＮＳプロトコルフォーマットのメッセージで生成するステップと、
前記位置要求を提供するステップと、
前記位置要求に基づく位置応答を受け取るステップと、
前記位置応答から少なくとも１つの位置識別子を取り出すステップと、
を含むことを特徴とするネットワークを介して位置を特定するための方法。
【請求項２】
前記位置応答は、ＤＮＳプロトコルとしてフォーマットされる、
ことを特徴とする請求項１に記載の方法。
【請求項３】
前記位置要求の中の前記１又はそれ以上のＢＳＳＩＤを符号化するステップをさらに含む、
ことを特徴とする請求項１に記載の方法。
【請求項４】
前記位置応答から取り出した少なくとも１つの位置識別子を復号するステップをさらに含む、
ことを特徴とする請求項１に記載の方法。
【請求項５】
前記位置要求は、ネットワークアクセス装置のオープンポートを使用してネットワーク上の位置サーバに提供される、
ことを特徴とする請求項１に記載の方法。
【請求項６】
前記オープンポートは、ポート５３である、
ことを特徴とする請求項５に記載の方法。
【請求項７】
前記少なくとも１つの位置識別子は、緯度及び経度を含む、
ことを特徴とする請求項１に記載の方法。
【請求項８】
前記少なくとも１つの位置識別子を、前記デジタル装置のアプリケーションに提供するステップをさらに含む、
ことを特徴とする請求項１に記載の方法。
【請求項９】
ＧＰＳ座標及び１又はそれ以上のネットワーク装置識別子をサーバに提供するステップをさらに含む、
ことを特徴とする請求項１に記載の方法。
【請求項１０】
１又はそれ以上の無線ネットワークを求めて領域を走査し、前記１又はそれ以上の無線ネットワークに関連する１又はそれ以上のＢＳＳＩＤを受け取るように構成された走査モジュールと、
前記１又はそれ以上のＢＳＳＩＤを含む位置要求を、ＤＮＳプロトコルフォーマットのメッセージで生成し、前記位置要求を提供するように構成されたＤＮＳモジュールと、
前記位置要求に基づく位置応答を受け取り、前記位置応答から少なくとも１つの位置識別子を取り出すように構成された位置モジュールと、
を備えることを特徴とするネットワークを介して位置を特定するためのシステム。

【請求項１１】
前記位置応答は、ＤＮＳプロトコルとしてフォーマットされる、
ことを特徴とする請求項１０に記載のシステム。
【請求項１２】
前記ＤＮＳモジュールは、前記位置要求の中の前記１又はそれ以上のＢＳＳＩＤを符号化するようにさらに構成される、
ことを特徴とする請求項１０に記載のシステム。
【請求項１３】
前記位置モジュールは、前記位置応答から取り出した前記少なくとも１つの位置識別子を復号するようにさらに構成される、
ことを特徴とする請求項１０に記載のシステム。
【請求項１４】
前記ＤＮＳモジュールは、ネットワークアクセス装置のオープンポートを使用してネットワーク上の位置サーバに前記位置要求を提供するように構成される、
ことを特徴とする請求項１０に記載のシステム。
【請求項１５】
前記オープンポートは、ポート５３である、
ことを特徴とする請求項１４に記載のシステム。
【請求項１６】
前記少なくとも１つの位置識別子は、緯度及び経度を含む、
ことを特徴とする請求項１０に記載のシステム。
【請求項１７】
前記位置モジュールは、前記デジタル装置のアプリケーションに前記少なくとも１つ位置識別子を提供するようにさらに構成される、
ことを特徴とする請求項１０に記載のシステム。
【請求項１８】
前記ＤＮＳモジュールは、ＧＰＳ座標及び１又はそれ以上のネットワーク装置識別子をサーバに提供するようにさらに構成される、
ことを特徴とする請求項１０に記載のシステム。
【請求項１９】
デジタル装置によって１又はそれ以上の無線ネットワークを求めて領域を走査するステップと、
前記１又はそれ以上の無線ネットワークに関連する１又はそれ以上のＢＳＳＩＤを受け取るステップと、
前記１又はそれ以上のＢＳＳＩＤを含む位置要求を、ＤＮＳプロトコルフォーマットのメッセージで生成するステップと、
前記位置要求を提供するステップと、
前記位置要求に基づく位置応答を受け取るステップと、
前記位置応答から少なくとも１つの位置識別子を取り出すステップと、
からなる方法を実行する命令を記憶したことを特徴とするコンピュータ可読記憶媒体。
【請求項２０】
前記位置応答は、ＤＮＳプロトコルとしてフォーマットされる、
ことを特徴とする請求項１９に記載のコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に通信ネットワークへのアクセスに関する。より詳細には、本発明は、ネットワークを介して位置を特定することに関する。
【背景技術】
【０００２】

ネットワークを使用して情報にアクセスすることが増えることにより、様々な活動に関してネットワーク通信への依存度が高まってきた。この依存度とともに、ネットワークアクセスが至る所で可能になるという期待が高まっている。無線技術の向上により、モバイルユーザのネットワークアクセスは特に強化されてきた。様々なセルラ（ＧＳＭ、ＣＤＭＡなど）、Ｗｉ－Ｆｉ（すなわちＩＥＥＥ　８０２．１１）、ＷｉＭａｘ（すなわちＩＥＥＥ　８０２．１６）及びその他の技術により、潜在的ネットワークユーザに対して広範囲にわたるアクセスオプションが可能になってきた。多くの無線アクセスポイントすなわち「ホットスポット」は、局所的な地理的領域でしかアクセスすることができず、特定の会社又はその他の住所と同じぐらい狭いこともある。また、戦略的に配置されたホットスポットは、全ての人々に公的又は私的ネットワークアクセスを提供することができる。

【先行技術文献】
【特許文献】
【０００３】
【特許文献１】米国特許出願第１１／８９９，６９７号明細書
【特許文献２】米国特許出願第１１／８９９，６３８号明細書
【発明の概要】
【発明が解決しようとする課題】
【０００４】
ホットスポットの所有者又は管理者は、ユーザアクセスを可能にするために、多くの場合パスワードなどを要求する。この結果、複数のホットポットのユーザは、数多くのパスワードを記憶し、覚え、又は別様に管理する必要が生じ得る。多くのユーザは、ホットスポットへのアクセスに使用するラップトップコンピュータ上に自身のパスワードを記憶することができる。しかしながら、ホットスポットにアクセスできる装置は、全てがラップトップコンピュータであるとは限らず、現在では携帯電話、携帯情報端末（ＰＤＡ）、及びその他の多くの装置が無線アクセス可能である。残念ながら、ユーザは、装置上に容易にパスワードを入力したり、或いは装置内にパスワードを記憶させることができないことが多い。例えば、無線アクセス可能な装置には、キーボードを有していないものもある。たとえ装置がキーボードを含んでいても、このキーボードは小さいことが多く、特に指先が器用でないユーザにとっては機能が限られることがある。
【０００５】
ユーザがラップトップコンピュータ上にパスワードを記憶する場合、ユーザはまず、ラップトップコンピュータにアクセスしてコンピュータに正しいパスワードを記憶させなければならない。パスワードが変わると、ユーザは、コンピュータ内のパスワードを更新する必要がある。また、装置内にユーザ名及びパスワードを記憶させると、装置が紛失又は盗難にあった場合にセキュリティ上の問題を生じる。
【０００６】
さらに、通常、ユーザは、パスワード、ユーザ名を入力し、ウェブサイトを渡り歩いてネットワークアクセスを得る必要がある。この過程には時間がかかり、またユーザが誤った情報を入力して、データを再入力せざるを得なくなる場合もある。
【０００７】
ユーザは、パスワードを手動入力する場合、難しいパスワードを覚えようとはしない。この結果、単純なパスワードでのアクセスは、ハッキングを受けやすく、ユーザのネットワークアクセス、ホットスポット及び／又はユーザの個人情報を危険にさらすことがある。さらに、ユーザの単純なパスワードがハッキングされたり、又は単純に推測される場合、ユーザのネットワークアクセスが盗まれることがある。
【０００８】
これまで、無線ネットワークに接続することは、無線装置のユーザにとって他の理由で複雑な処理であった。通常、ユーザは、２又はそれ以上のＷｉ－Ｆｉネットワークが存在する領域に入り、自身のラップトップ上でＷｉ－Ｆｉ機能を選択し、利用可能なＷｉ－Ｆｉネットワークを一覧にした一連の「走査結果」を見る。１つの例では、利用可能なＷｉ

－Ｆｉネットワークのリストが、Ｗｉ－Ｆｉネットワークのリストを含む。多くの場合、ユーザは、暗号化又は（ログインページなどの）その他のセキュリティメカニズムが存在しないＷｉ－Ｆｉネットワークを識別しなければならない。機能的な無線ネットワークもいくつか存在する一方で、ネットワークが使用できなくなるように誤設定された無線ネットワークも存在することが、ユーザの不満を増大させる。

【０００９】

通常、ユーザは、どのＷｉ－Ｆｉネットワークに接続すべきかを一覧に基づいて任意に判断する。通常、ユーザは、どのＷｉ－Ｆｉネットワークに接続すべきかを判断する際に、選択したＷｉ－Ｆｉネットワークが十分なサービス品質を提供するかどうか、或いはネットワークが動的ホスト構成プロトコル（ＤＨＣＰ）を介してＩＰアドレスを提供できるかどうかが分からない。

【００１０】

多くのアプリケーションでは位置情報を利用することが増えているが、全ての装置が全地球測位システム（ＧＰＳ）又は同様のハードウェアを含んでいるわけではない。さらに、装置がＧＰＳを有していても、位置を特定するのに十分な数の衛星を利用又は視認できないことがある。例えば、ユーザが屋内にいたり、１又はそれ以上の衛星にアクセスできなかったり、又は装置からのＧＰＳ信号が遮られたりすることがある。さらに、装置が小型化して安価になるにつれ、ＧＰＳハードウェアの能力、柔軟性及び通信機能が限られて、ＧＰＳ座標の検索を阻むこともある。

【課題を解決するための手段】

【００１１】

ネットワークアクセスのためのネットワーク信用証明書を提供する例示的な方法及びシステムについて説明する。この例示的な方法は、ネットワーク装置を介してデジタル装置から信用証明書要求を受け取るステップと、この信用証明書要求の中の少なくとも一部の情報に基づいてネットワーク記録を識別するステップと、このネットワーク記録に基づいて、複数のネットワーク信用証明書から１つのネットワーク信用証明書を取り出すステップと、複数のネットワーク信用証明書から取り出したネットワーク信用証明書を含む信用証明書要求応答をデジタル装置へ送信するステップとを含む。

【００１２】

この方法は、信用証明書要求を解読し、信用証明書要求を認証し、信用証明書要求応答を暗号化するステップをさらに含むことができる。さらに、この方法は、デジタル装置に基づいて暗号鍵を取り出すステップを含むこともできる。信用証明書要求は、ネットワーク装置の標準プロトコルを介して受け取ることができる。この標準プロトコルはＤＮＳとすることができる。

【００１３】

信用証明書要求は、位置識別子を含むことができる。方法は、デジタル装置から確認済みアクセス応答を受け取るステップをさらに含むことができる。

【００１４】

ネットワーク信用証明書を提供するための例示的なシステムは、信用証明書要求モジュール及び信用証明書要求応答モジュールを含むことができる。信用証明書要求モジュールは、デジタル装置からネットワーク装置を介して信用証明書要求を受け取るように構成することができる。信用証明書要求応答モジュールは、この信用証明書要求の中の少なくとも一部の情報に基づいてネットワーク記録を識別し、このネットワーク記録に基づいて複数のネットワーク信用証明書から１つのネットワーク信用証明書を取り出し、このネットワークを含む信用証明書要求応答をデジタル装置へ送信するように構成することができる。

【００１５】

例示的なコンピュータ可読媒体は、プログラムを含むことができる。このプログラムは、ネットワーク信用証明書を提供する方法を実施するためのプロセッサによって実行することができる。この方法は、ネットワーク装置を介してデジタル装置から信用証明書要求

を受け取るステップと、この信用証明書要求の中の少なくとも一部の情報に基づいてネットワーク記録を識別するステップと、このネットワーク記録に基づいて複数のネットワーク信用証明書から１つのネットワーク信用証明書を取り出すステップと、複数のネットワーク信用証明書から取り出したネットワーク信用証明書を含む信用証明書要求応答をデジタル装置へ送信するステップとを含むことができる。

【００１６】

無線ネットワークを選択するためのシステム及び方法を開示する。いくつかの実施形態では、方法が、第１のネットワーク装置のための第１のネットワーク装置識別子及び第２のネットワーク装置のための第２のネットワーク装置識別子を受け取るステップと、第１の属性を含む、第１のネットワーク装置識別子に基づく第１のネットワークプロファイルを取得するステップと、第２の属性を含む、第２のネットワーク装置識別子に基づく第２のネットワークプロファイルを取得するステップと、第１の属性及び第２の属性の属性分析に基づいて第１のネットワーク装置識別子又は第２のネットワーク装置識別子を選択するステップとを含む。

【００１７】

様々な実施形態では、第１のネットワーク装置識別子及び第２のネットワーク装置識別子が、デジタル装置からサーバによって受け取られる。この方法は、選択に基づいて無線ネットワーク選択を行うステップをさらに含むことができる。この方法は、選択に基づいて信用証明書要求応答を提供するステップをさらに含むこともできる。

【００１８】

いくつかの実施形態では、ネットワーク選択識別子が第１のネットワーク装置識別子を含む。ネットワーク選択識別子はまた、第１のネットワーク装置識別子及び第２のネットワーク装置識別子を含むソート済みリストを含むこともでき、このリストは第１の属性及び第２の属性の属性分析に基づいてソートされる。属性は、性能測定基準、共有インジケータ、及びサービス識別子を含むことができる。

【００１９】

方法は、第１の属性及び第２の属性を最低要件と比較するステップをさらに含むことができ、第１のネットワーク識別子又は第２のネットワーク装置識別子を選択するステップは、この属性と最低要件の比較にも少なくとも部分的に基づく。方法はまた、第１の属性及び第２の属性を個別設定と比較するステップをさらに含むこともでき、第１のネットワーク識別子又は第２のネットワーク装置識別子を選択するステップは、この属性と個別設定の比較にも少なくとも部分的に基づく。方法はまた、ユーザ識別子を受け取り、このユーザ識別子に基づいてユーザアカウントから個別設定を取り出すステップをさらに含むこともできる。

【００２０】

様々な実施形態では、システムがデジタル装置及びサーバを含む。デジタル装置は、通信ネットワークに結合することができ、この通信ネットワークを介して第１のネットワーク装置のための第１のネットワーク装置識別子及び第２のネットワーク装置のための第２のネットワーク装置識別子を受け取るように構成することができる。サーバも通信ネットワークに結合するとができ、第１のネットワーク装置識別子及び第２のネットワーク装置識別子をデジタル装置から受け取って、第１の属性を含む、第１のネットワーク装置識別子に基づく第１のネットワークプロファイルを取得し、第２の属性を含む、第２のネットワーク装置識別子に基づく第２のネットワークプロファイルを取得し、第１の属性及び第２の属性の属性分析に基づいて第１のネットワーク装置識別子又は第２のネットワーク装置識別子を選択するように構成することができる。

【００２１】

コンピュータ可読記憶媒体は、方法を含む命令を記憶するように構成することができ、この方法は、第１のネットワーク装置のための第１のネットワーク装置識別子及び第２のネットワーク装置のための第２のネットワーク装置識別子を受け取るステップと、第１の属性を含む、第１のネットワーク装置識別子に基づく第１のネットワークプロファイルを

取得するステップと、第２の属性を含む、第２のネットワーク装置識別子に基づく第２のネットワークプロファイルを取得するステップと、第１の属性及び第２の属性の属性分析に基づいて第１のネットワーク装置識別子又は第２のネットワーク装置識別子を選択するステップとを含む。

【００２２】

様々な実施形態では、方法が、デジタル装置によって１又はそれ以上の無線ネットワークを求めて領域を走査するステップと、この１又はそれ以上の無線ネットワークに関連する１又はそれ以上のＢＳＳＩＤを受け取るステップと、この１又はそれ以上のＢＳＳＩＤを含む位置要求を、ＤＮＳプロトコルフォーマットのメッセージで生成するステップと、位置要求を提供するステップと、この位置要求に基づく位置応答を受け取るステップと、この位置応答から少なくとも１つの位置識別子を取り出すステップとを含む。

【００２３】

位置応答は、ＤＮＳプロトコルとしてフォーマットすることができる。この方法は、位置要求の中の１又はそれ以上のＢＳＳＩＤを符号化するステップ、及び／又は位置応答から取り出した少なくとも１つの位置識別子を復号するステップをさらに含むことができる。位置要求は、ネットワークアクセス装置のオープンポートを使用してネットワーク上の位置サーバに提供することができる。さらに、オープンポートは、ポート５３とすることができる。少なくとも１つの位置識別子は、緯度及び経度を含むことができる。

【００２４】

様々な実施形態では、この方法が、この少なくとも１つの位置識別子をデジタル装置のアプリケーションに提供するステップをさらに含むことができる。さらに、この方法は、ＧＰＳ座標及び１又はそれ以上のネットワーク装置識別子をサーバに提供するステップをさらに含むことができる。

【００２５】

いくつかの実施形態では、例示的なシステムが、走査モジュール、ＤＮＳモジュール、及び位置モジュールを備える。走査モジュールは、１又はそれ以上の無線ネットワークを求めて領域を走査するように構成できるとともに、この１又はそれ以上の無線ネットワークに関連する１又はそれ以上のＢＳＳＩＤを受け取るように構成することができる。ＤＮＳモジュールは、１又はそれ以上のＢＳＳＩＤを含む位置要求を、ＤＮＳプロトコルフォーマットのメッセージで生成するように構成することができる。位置モジュールは、位置要求に基づく位置応答を受け取るとともに、この位置応答から少なくとも１つの位置識別子を取り出すように構成することができる。

【００２６】

例示的なコンピュータ可読記憶媒体は、命令を記憶するように構成することができる。この命令は方法を含むことができる。この方法は、デジタル装置によって１又はそれ以上の無線ネットワークを求めて領域を走査するステップと、この１又はそれ以上の無線ネットワークに関連する１又はそれ以上のＢＳＳＩＤを受け取るステップと、この１又はそれ以上のＢＳＳＩＤを含む位置要求を、ＤＮＳプロトコルフォーマットのメッセージで生成するステップと、位置要求を提供するステップと、この位置要求に基づく位置応答を受け取るステップと、この位置応答から少なくとも１つの位置識別子を取り出すステップとを含む。

【図面の簡単な説明】

【００２７】

【図１】本発明の実施形態を実施できる環境を示す図である。

【図２】例示的な信用証明書サーバのブロック図である。

【図３】デジタル装置にネットワークアクセスを提供する例示的な処理のフロー図である。

【図４】例示的な信用証明書要求のブロック図である。

【図５】例示的な信用証明書要求応答のブロック図である。

【図６】ネットワーク信用証明書を提供する例示的な方法のフロー図である。

【図７】ネットワーク信用証明書を提供する例示的な方法の別のフロー図である。
【図８】ネットワーク信用証明書を受け取って記憶する例示的な方法のフロー図である。
【図９】例示的な信用証明書サーバのブロック図である。
【図１０】本発明の実施形態を実施できる別の環境を示す図である。
【図１１】無線ネットワークの選択を提供する例示的な処理のフロー図である。
【図１２】無線ネットワークを選択する例示的な処理のフロー図である。
【図１３】無線ネットワークを選択し、この選択した無線ネットワークにアクセスするための略図である。
【図１４】例示的なデジタル装置のブロック図である。
【図１５】ＤＮＳプロトコルフォーマットのメッセージを通じ、無線ネットワークを介して位置情報を受け取る例示的な方法のフロー図である。
【図１６】例示的な位置サーバのブロック図である。
【図１７】ＤＮＳプロトコルフォーマットのメッセージを通じ、無線ネットワークを介して位置情報を提供する例示的な方法のフロー図である。
【図１８】ネットワークを介して位置情報を収集する例示的な方法のフロー図である。
【発明を実施するための形態】
【００２８】
本発明の実施形態は、ネットワーク信用証明書を提供するためのシステム及び方法を提供する。例示的な実施形態では、信用証明書サーバが、ホットスポットにおけるデジタル装置からネットワーク信用証明書の要求を受け取る。この要求は、ホットスポットから信用証明書サーバへ中継される標準プロトコルとしてフォーマットすることができる。信用証明書サーバは、要求の中に含まれる少なくとも一部の情報に基づいてネットワーク記録を識別し、このネットワーク記録に関連する送信ネットワーク信用証明書をデジタル装置へ送信することができる。デジタル装置は、ネットワーク信用証明書を受け取り、ネットワークアクセスを取得するためにこれをネットワーク装置に提供することができる。
【００２９】
様々な実施形態では、ルールサーバが、様々なネットワーク属性に基づいてデジタル装置が接続できる複数の利用可能なネットワークから好ましいネットワークを識別することができる。１つの例では、デジタル装置が、利用可能なネットワークを求めて物理的領域を走査し、利用可能な無線ネットワークのリストを生成することができる。このリストをルールサーバに提供し、このルールサーバが、リスト上の個々の無線ネットワークのネットワークプロファイルを識別して取り出すことができる。次に、ルールサーバは（個々のプロファイルに含まれる属性などを通じて）個々のネットワークプロファイルを比較して、リストから好ましいネットワークを選択することができる。その後、ルールサーバは、この時点でネットワークにアクセスできるデジタル装置へ無線ネットワーク選択を送信することができる。
【００３０】
いくつかの実施形態では、デジタル装置が、信用証明書サーバにより提供された信用証明書を使用して、選択した無線ネットワークにアクセスする。１つの例では、ルールサーバが好ましい無線ネットワークを選択すると、ルールサーバ（又は、ルールサーバと通信している別のサーバ）は、選択した無線ネットワークに関連するネットワーク信用証明書を含む信用証明書要求応答を同時に（又はほぼ同時に）提供することができる。
【００３１】
図１は、本発明の実施形態を実施できる環境１００の図を示している。例示的な実施形態では、デジタル装置１０２を有するユーザがホットスポットに入る。デジタル装置１０２は、標準プロトコルとしての信用証明書要求を、ネットワーク装置１０４の向こうへ自動的に送信することができる。この信用証明書要求が信用証明書サーバ１１６へ転送され、この信用証明書サーバ１１６が、信用証明書要求の中に含まれる情報に基づいてデジタル装置１０２へ信用証明書要求応答を送信することができる。信用証明書要求応答はネットワーク信用証明書を含み、デジタル装置１０２は、これをネットワーク装置１０４、認

証サーバ１０８又はアクセスコントローラ１１２に提供して通信ネットワーク１１４へのアクセスを取得することができる。

【００３２】

様々な実施形態では、ホットスポットが、（「ウォールド・ガーデン（ｗａｌｌｅｄ ｇａｒｄｅｎ）」などの）ローカルエリアネットワーク１０６に結合されたネットワーク装置１０４、認証サーバ１０８、ＤＮＳサーバ１１０及びアクセスコントローラ１１２を含む。ネットワーク装置１０４は、デジタル装置１０２がローカルエリアネットワーク１０６を介して認証サーバ１０８、ＤＮＳサーバ１１０及びアクセスコントローラ１１２と通信できるようにするアクセスポイントを含むことができる。デジタル装置１０２は、ラップトップ、携帯電話、カメラ、携帯情報端末又はその他のあらゆるコンピュータ装置を含むことができる。認証サーバ１０８は、デジタル装置１０２を通信ネットワーク１１４にアクセスできるようにする前に、デジタル装置１０２にネットワーク信用証明書を要求するサーバである。ＤＮＳサーバ１１０は、ローカルエリアネットワーク１０６を介してＤＮＳサービスを提供するとともに、通信ネットワーク１１４を横切って他のＤＮＳサーバ（図示せず）へ要求を中継することができる。アクセスコントローラ１１２は、ネットワーク装置１０４に機能上結合された装置と、通信ネットワーク１１４に結合された装置との間の通信を可能にすることができるルータ又はブリッジなどのアクセス装置である。

【００３３】

図１のホットスポットは、ローカルエリアネットワーク１０６に結合された別個のサーバを示しているが、当業者であれば、ローカルエリアネットワーク１０６に結合された装置（サーバ、デジタル装置、アクセスコントローラ及びネットワーク装置など）はいくつ存在してもよいことを理解するであろう。いくつかの実施形態では、ローカルエリアネットワーク１０６が任意である。１つの例では、認証サーバ１０８、ＤＮＳサーバ１１０、及びアクセスコントローラ１１２が、ネットワーク装置１０４に直接結合される。様々な実施形態では、認証サーバ１０８、ＤＮＳサーバ１１０、及びアクセスコントローラ１１２を、１又はそれ以上のサーバ、或いは１又はそれ以上のデジタル装置内で組み合わせることができる。さらに、図１は無線アクセスを示しているが、デジタル装置１０２は、無線で又は（１０ｂａｓｅＴなどの）有線を介してネットワーク装置１０４に結合することができる。

【００３４】

通信ネットワーク１１４にアクセスするために、認証サーバ１０８は、デジタル装置１０２に、ホットスポットにアクセスするための１又はそれ以上のネットワーク信用証明書を提供するように求めることができる。ネットワーク信用証明書は、例えばホットスポットに関連するアカウント用のユーザ名及びパスワードを含むことができる。代替の実施形態では、ユーザ名及びパスワード以外のネットワーク信用証明書を利用することができる。

【００３５】

例示的な実施形態によれば、デジタル装置１０２は、ネットワーク信用証明書を信用証明書サーバ１１６から動的に取得することができる。デジタル装置１０２は、デジタル装置１０２（又はデジタル装置１０２のユーザ）のアイデンティティ及び（ネットワーク装置１０４又はＷｉ－Ｆｉサービス提供者名などの）ネットワーク装置１０４に関する詳細を含む信用証明書要求を信用証明書サーバ１１６へ送信することができる。

【００３６】

１つの例では、デジタル装置１０２がホットスポットに入る際に、ネットワーク装置１０４は、ＤＮＳクエリを提出できる相手先のＩＰアドレスを、例えばＤＨＣＰ（動的ホスト構成プロトコル）を介して提供することができる。信用証明書要求は、標準プロトコルとしてフォーマットすることができる。一例では、信用証明書要求をＤＮＳ要求としてフォーマットすることができる。信用証明書要求は、（アクセスコントローラ１１２などの）ネットワークインフラが要求を阻止しないように、（ＴＸＴなどの）標準記録形式を含むテキスト記録要求とすることができる。ネットワーク信用証明書を取得する処理に関す

るさらなる詳細が、２００７年９月６日に出願された「ネットワーク信用証明書を取得するためのシステム及び方法」という名称の同時係属中米国特許出願第１１／８９９，６９７号に記載されており、該特許出願は引用により本明細書に組み入れられる。

【００３７】

いくつかの実施形態では、信用証明書要求がＤＮＳサーバ１１０によって受け取られ、このＤＮＳサーバ１１０が、ネットワーク信用証明書を求めて信用証明書要求を信用証明書サーバ１１６へ転送することができる。例示的な実施形態では、信用証明書サーバ１１６が検索を実行して（単複の）適切なネットワーク信用証明書を決定してＤＮＳサーバ１１０へ返送し、このＤＮＳサーバ１１０が、要求元のデジタル装置１０２へネットワーク信用証明書を返送することができる。様々な実施形態では、（単複の）適切なネットワーク信用証明書が、信用証明書サーバ１１６から信用証明書要求の送信と同じ経路を介してデジタル装置１０２へ送信される。

【００３８】

図１には１つのＤＮＳサーバ１１０しか示していないが、信用証明書要求が信用証明書サーバ１１６によって受け取られる前に、限定するわけではないが、ＤＮＳサーバを含むあらゆる数のサーバを介して信用証明書要求を転送することができる。他の実施形態では、信用証明書要求が、ネットワーク装置１０４から信用証明書サーバ１１６へ直接転送される。

【００３９】

いくつかの実施形態では、信用証明書サーバ１１６からの信用証明書要求応答が、ユーザ名、パスワード及び／又はログイン手順情報を含むことができる。ログイン手順情報は、例えばＨＴＭＬ形式要素名、提出ＵＲＬ又は提出プロトコルを含むことができる。いくつかの実施形態では、信用証明書サーバ１１６が、ネットワーク信用証明書応答をデジタル装置１０２へ送信する前に、デジタル装置１０２に関連する暗号鍵を使用して暗号化することができる。

【００４０】

デジタル装置１０２がネットワーク信用証明書応答を受け取ると、デジタル装置１０２は、ネットワーク装置１０４に（ネットワーク信用証明書応答から取り出した）ネットワーク信用証明書を認証応答の形で提出することができる。例示的な実施形態では、検証のために認証応答を認証サーバ１０８へ転送することができる。いくつかの実施形態では、認証サーバ１０８が、ＡＡＡサーバ又はＲＡＤＩＵＳサーバを含むことができる。２００７年９月６日に出願された「ネットワークアクセスを取得するシステム及び方法」という名称の同時係属中米国特許出願第１１／８９９，６３８号に、ネットワークアクセスを取得する処理に関するさらなる詳細が記載されており、該特許出願は引用により本明細書に組み入れられる。

【００４１】

なお、図１は例示的なものである。代替の実施形態は、より多くの、より少ない、又は機能的に同等の構成要素を含むことができるが、これもまた本実施形態の範囲内にある。例えば、前述したように、（ＤＮＳサーバ１１０、信用証明書サーバ１１６及び認証サーバ１０８などの）様々なサーバの機能を組み合わせて１つ又は２つのサーバにすることができる。すなわち、例えば認証サーバ１０８及びＤＮＳサーバ１１０を同じサーバで構成できる場合、認証サーバ１０８、ＤＮＳサーバ１１０及びアクセスコントローラ１１２の機能を組み合わせて単一の装置にすることができる。

【００４２】

図２は、例示的な信用証明書サーバ１１６のブロック図である。信用証明書サーバ１１６は、認証モジュール２００、ネットワークモジュール２０２、信用証明書要求モジュール２０４、信用証明書要求応答モジュール２０６、暗号化／解読モジュール２０８、ネットワーク記録ストレージ２１０、及び暗号鍵ストレージ２１２を含む。モジュールは、ソフトウェア、ハードウェア、ファームウェア又は回路を個別に又は組み合わせて含むことができる。

【００４３】
認証モジュール２００は、信用証明書要求を認証して信用証明書要求応答にセキュリティを与えるように構成することができる。様々な実施形態では、デジタル装置１０２が、（共有暗号鍵又は鍵対の一部である暗号鍵などの）暗号鍵を使用して信用証明書要求を暗号化し、又は信用証明書要求にデジタル署名することができる。認証モジュール２００は、暗号鍵ストレージ２１２から取り出した適切な暗号鍵で信用証明書要求を解読することにより、信用証明書要求を認証することができる。１つの例では、デジタル装置１０２が信用証明書要求のハッシュを生成し、信用証明書要求の暗号化部分の中にハッシュを記憶する。認証モジュール２００は、信用証明書要求を解読し、信用証明書要求応答のハッシュを生成し、生成したハッシュを信用証明書要求の中に含まれるハッシュと比較して認証を行うことができる。

【００４４】
他の実施形態では、デジタル装置１０２がナンス（すなわちランダム値）を生成し、デジタル署名された信用証明書要求の一部の中にナンスを記憶することができる。認証モジュール２００は、デジタル署名を解読して信用証明書要求を認証し、ナンスを取り出すことができる。様々な実施形態では、信用証明書要求応答モジュール２０６が信用証明書要求応答を生成する（後述）際に、認証モジュール２００が信用証明書要求応答にナンスを含めることができる。その後、認証モジュール２００又は暗号化／解読モジュール２０８は、信用証明書要求応答を暗号化することができる。デジタル装置１０２が信用証明書要求応答を解読する場合、デジタル装置１０２は、信用証明書要求応答からナンスを取り出し、このナンスを、信用証明書要求に含めて送信したナンスと比較してさらなる認証を行うことができる。

【００４５】
ネットワークモジュール２０２は、信用証明書要求を受け取り、通信ネットワーク１１４を介して信用証明書要求応答を送信するように構成することができる。

【００４６】
信用証明書要求モジュール２０４は、ネットワークモジュール２０２から信用証明書要求を受け取ることができる。信用証明書要求は標準プロトコルとすることができる。１つの例では、信用証明書要求が（ＤＮＳなどの）ＵＤＰプロトコルである。

【００４７】
例示的な実施形態では、信用証明書要求モジュール２０４が、信用証明書要求からＤＤＩＤ及びＳＳＩＤを取り出すことができる。ＤＤＩＤは、デジタル装置１０２、デジタル装置１０２のユーザ、及び／又はネットワーク記録に関連するユーザを識別することができる。ＳＳＩＤは、ホットスポット又はホットスポットのサービスプロバイダ（すなわち運営会社）を識別することができる。

【００４８】
信用証明書要求モジュール２０４又は信用証明書要求応答モジュール２０６は、ＤＤＩＤ及びＳＳＩＤに基づいてネットワーク記録を識別することができる。ネットワーク記録とは、ＤＤＩＤ及びＳＳＩＤに（（リレーショナルデータベースのように）直接的に又は間接的に）関連する記録のことである。１つの例では、ネットワーク記録が、ＳＳＩＤに関連するホットスポットにおいてＤＤＩＤに関連するデジタル装置１０２にネットワークアクセスを提供するのに必要なネットワーク信用証明書を含む。ネットワーク記録は、ネットワーク記録ストレージ２１０内に記憶することができる。

【００４９】
信用証明書要求応答モジュール２０６は信用証明書要求応答を生成することができる。様々な実施形態では、信用証明書要求応答モジュール２０６が、ネットワーク記録からＤＤＩＤ及びＳＳＩＤに関連するネットワーク信用証明書を受け取る。いくつかの実施形態では、ネットワーク信用証明書が、クレジットカード番号を含むことができる。１つの例では、デジタル装置１０２が、ネットワーク信用証明書を受け取り、クレジットカード番号を取り出して、このクレジットカード番号を認証サーバ１０８に提供する。いくつかの

例では、その後、認証サーバ１０８が、クレジットカード番号に関連するクレジットカードに料金を請求し、或いはこの情報を使用して、ネットワークアクセスを認める前にユーザのアイデンティティを確認することができる。

【００５０】

さらに、様々な実施形態では、ネットワーク信用証明書がログイン手順情報を含むことができる。１つの例では、信用証明書がユーザ名及びパスワードを含み、これらがデジタル装置１０２によって認証サーバ１０８から取り出された（認証フォームなどの）フォームで提供されることになる。いくつかの実施形態では、ログイン手順情報によってデジタル装置１０２に、フォーム内の特定のフィールドにネットワーク信用証明書を読み込んだ後で、完成したフォームを認証サーバ１０８に提出するように指示することができる。当業者であれば、信用証明書を認証サーバ１０８に提供するための方法は数多く存在することを理解するであろう。認証サーバに信用証明書を提供する処理は、２００７年９月６日に出願された「ネットワークアクセスを取得するシステム及び方法」という名称の同時係属中米国特許出願第１１／８９９，６３８号にさらに記載されている。

【００５１】

信用証明書要求応答モジュール２０６又は暗号化／解読モジュール２０８は、ＤＤＩＤ又は信用証明書要求に関連する暗号鍵で信用証明書要求応答を暗号化することができる。１つの例では、信用証明書サーバ１１６が１又はそれ以上の共有暗号鍵を記憶する。少なくとも１つのデジタル装置１０２により、個々の共有暗号鍵を共有することができる。信用証明書要求応答モジュール２０６は、デジタル装置１０２に関連する共有暗号鍵で信用証明書要求応答を暗号化することができる（例えば、共有暗号鍵をＤＤＩＤに関連付けることができる）。信用証明書要求応答モジュール２０６又は暗号化／解読モジュール２０８は、鍵対の一部である暗号鍵で信用証明書要求を暗号化することもできる。暗号化／解読モジュール２０８が信用証明書要求を暗号化する方法は、数多く存在し得る。

【００５２】

暗号化／解読モジュール２０８は、信用証明書要求を解読して信用証明書要求応答を暗号化することができる。上述したように、暗号化／解読モジュール２０８は、信用証明書要求のデジタル署名を解読することができる。１つの例では、暗号化／解読モジュール２０８が、信用証明書要求の中に含まれるＤＤＩＤに関連する暗号鍵に基づいてデジタル署名を解読する。暗号化／解読モジュール２０８は、信用証明書要求応答を暗号化することもできる。１つの例では、暗号化／解読モジュール２０８が、（共有暗号鍵又は鍵対の一部である暗号鍵などの）ＤＤＩＤに関連する暗号鍵に基づいて信用証明書要求応答を暗号化する。

【００５３】

様々な実施形態では、暗号化／解読モジュール２０８が、ネットワーク記録ストレージ２１０に含まれるネットワーク記録を暗号化して、暗号鍵ストレージ２１２を管理することができる。暗号化／解読モジュール２０８はまた、ネットワーク信用証明書を記憶する際に、（ＳＳＬ及びＨＴＴＰなどを介して）デジタル装置と安全な通信を確立することもできる。この処理については図７でさらに説明する。いくつかの実施形態によれば、暗号化／解読モジュール２０８を任意とすることができる。

【００５４】

ネットワーク記録ストレージ２１０及び暗号鍵ストレージ２１２は、ネットワーク記録及び暗号鍵をそれぞれ記憶することができる。ネットワーク記録ストレージ２１０及び暗号鍵ストレージ２１２は、１又はそれ以上のデータベースを含むことができる。１つの例では、ネットワーク記録ストレージ２１０がネットワーク記録を記憶することができる。ネットワーク記録は、ＤＤＩＤ、ＳＳＩＤ及びネットワーク信用証明書を含むことができる。ネットワーク記録はまた、ユーザがネットワーク記録にアクセスし、これらを変更、更新し、又は信用証明書サーバ１１６に記憶するためのユーザ名及びパスワードを含むこともできる。

【００５５】

様々な実施形態では、ネットワーク記録により、複数のデジタル装置１０２が同じネットワーク信用証明書を使用できるようにすることもできる。１つの例では、ユーザが複数のデジタル装置１０２を所有することができる。各々が異なるデジタル装置１０２に関連する複数のＤＤＩＤを、同じネットワーク記録に含めることができる。いくつかの実施形態では、複数の装置を１又はそれ以上のネットワーク記録に関連付けることができ、この１又はそれ以上のネットワーク記録がユーザに関連する。この結果、ユーザは、あらゆる数のデジタル装置１０２を使用して、ホットスポットに対してネットワーク信用証明書を取り出すことができる。当業者であれば、ネットワーク記録及び／又はこれに含まれる情報を記憶して体系化することができる方法（例えば、異なるデータ構造、データベース、記録、体系化方式及び／又は方法）は数多く存在することを理解するであろう。

【００５６】

図３は、デジタル装置１０２にネットワークアクセスを提供する例示的な処理のフロー図である。ステップ３００において、デジタル装置１０２は、最初にホットスポットに入る際に、ローカルエリアネットワーク１０６を求めて走査を行うことができる。走査の結果、ステップ３０２において、ネットワーク装置１０４がネットワーク構成情報を提供することができる。このネットワーク構成情報は、ＤＮＳサーバ１１０にアクセスするための１又はそれ以上のＩＰアドレスを含むことができる。

【００５７】

ステップ３０４において、デジタル装置１０２が信用証明書要求を生成する。その後、ステップ３０６において、先程ネットワーク装置１０４から受け取ったＩＰアドレスの１つを使用して、信用証明書要求をＤＮＳサーバ１１０へ送信することができる。

【００５８】

ステップ３０８において、信用証明書要求に基づいて、ＤＮＳサーバ１１０が信用証明書サーバ１１６を識別する。他の実施形態では、ＤＮＳサーバ１１０が、信用証明書要求を信用証明書サーバ１１６へ転送する。ＤＮＳサーバ１１０がＤＮＳ要求をローカルに解析できない場合、信用証明書要求は（ポート５３などを介して）通信ネットワーク１１４上の別のＤＮＳサーバに転送され、その後、このＤＮＳサーバが、信用証明書要求を信用証明書サーバ１１６へ転送することができる。ステップ３１０において、信用証明書要求が、信用証明書サーバ１１６へ直接、又は通信ネットワーク１１４上の１又はそれ以上のＤＮＳサーバを介して間接的に転送される。

【００５９】

ステップ３１２において、信用証明書サーバ１１６が、信用証明書要求に基づいて必要とされるネットワーク信用証明書を識別する。例えば、信用証明書要求は、デジタル装置１０２の識別子（すなわちＤＤＩＤ）、並びにホットスポットＳＳＩＤ（例えば、運営会社などのサービスプロバイダ）の識別子を含むことができる。信用証明書要求モジュール２０４又は信用証明書要求応答モジュール２０６により、これらの識別子を（ネットワーク記録などの）このような識別子の表と比較して、適切なネットワーク信用証明書を決定することができる。その後、ステップ３１４において、信用証明書要求応答モジュール２０６が信用証明書要求応答を生成し、ステップ３１６において、これがＤＮＳサーバ１１０へ中継して戻される。ステップ３１８において、ＤＮＳサーバ１１０が、信用証明書要求応答をデジタル装置へ転送する。

【００６０】

その後、ステップ３２０において、デジタル装置１０２が、信用証明書要求応答からネットワーク信用証明書を取り出すことができる。その後、ステップ３２２において、このネットワーク信用証明書をネットワーク装置１０４に提供することができる。ステップ３２４において、ネットワーク装置１０４が、ネットワーク信用証明書を確認した上でデジタル装置１０２にネットワークアクセスを提供する。

【００６１】

ここで図４を参照すると、例示的な信用証明書要求４００をより詳細に示している。例示的な実施形態によれば、信用証明書要求応答モジュール２０４が信用証明書要求応答４

００を生成することができる。１つの実施形態では、信用証明書要求４００を、位置識別子４０２、シーケンス識別子４０４、署名４０６、ＤＤＩＤ４０８、サービスセット識別子（ＳＳＩＤ）４１０、及びバージョン識別子４１２を含む構造を有するＤＮＳ文字列とすることができる。

【００６２】

任意の位置識別子４０２は、デジタル装置１０２、ネットワーク装置１０４、認証サーバ１０８又はアクセスコントローラ１１２の物理的又は地理的位置を示すことができる。様々な実施形態では、信用証明書サーバ１１６が位置識別子４０２を使用して、ホットスポットの使用状況、デジタル装置１０２のユーザ、及びデジタル装置１０２を追跡することができる。

【００６３】

シーケンス識別子４０４は、その後の信用証明書サーバ１１６への要求に対応してログインが成功したかどうかを判定するために使用されるあらゆる数字又数字の組を含むことができる。すなわち、シーケンス識別子４０４は相関機構を提供し、この相関機構により信用証明書サーバ１１６がログイン処理を確認することができる。

【００６４】

例示的な実施形態では、署名４０６が、なりすましを防ぐために利用される暗号署名（すなわちデジタル署名）を含む。デジタル装置１０２からの要求の署名４０６は、信用証明書サーバ１１６により検証される。署名４０６が有効でなければ、この要求は信用証明書サーバ１１６により拒絶される。

【００６５】

ＤＤＩＤ４０８は、デジタル装置１０２の識別子を含む。例えば、ＤＤＩＤ４０８は、デジタル装置１０２のＭＡＣアドレス又はその他のいずれかの識別子を含むことができる。

【００６６】

ＳＳＩＤ４１０は、ネットワークアクセスポイント又はＷｉ－Ｆｉサービスプロバイダの識別子を含む。例えば、ＳＳＩＤ４１０は、サービスプロバイダ名、又はネットワーク装置１０４が動作している場所の名前を含むことができる。

【００６７】

バージョン識別子４１２は、信用証明書要求４００のプロトコル又はフォーマットを識別することができる。例えば、デジタル装置１０２は、信用証明書要求４００を生成し、データをいくつかの異なるフォーマットで体系化することができる。個々の異なるフォーマットを異なるバージョン識別子に関連付けることができる。いくつかの実施形態では、信用証明書要求応答モジュール２０６の構成要素を更新し、再構成し、又は徐々に変更することができ、これが信用証明書要求４００の構造に影響を与え得る。この結果、信用証明書サーバ１１６は、別様にフォーマットされた複数の信用証明書要求４００を受け取ることができる。信用証明書サーバ１１６は、それぞれのバージョン識別子に基づいて、個々の信用証明書要求が必要とする情報にアクセスすることができる。

【００６８】

図５は、例示的な信用証明書要求応答のブロック図である。例示的な実施形態によれば、信用証明書要求応答モジュール２０６が、信用証明書要求応答５００を生成することができる。１つの実施形態では、信用証明書要求応答５００が暗号化テキスト５０２を含むことができる。暗号化テキストは、任意のナンス５０４及び信用証明書情報５０６を含むことができる。信用証明書情報は、鍵／値の対５０８～５１０を含むことができる。

【００６９】

上述したように、信用証明書要求応答を、暗号化テキスト５０２を含むＤＮＳ応答としてフォーマットすることができる。暗号化テキスト５０２は、（ユーザ名、パスワード及びログイン手順情報などの）ネットワーク信用証明書を含む。信用証明書要求応答５００を、暗号化テキスト５０２を含むように示しているが、信用証明書要求応答５００内のテキストを暗号化する必要はない。

【００７０】
暗号化テキスト５０２は、ナンスを含むことができる。上述したように、このナンスは、信用証明書要求から取り出すことができる。デジタル装置１０２は、信用証明書要求応答５００を受け取ると、信用証明書要求応答５００内のナンスを、信用証明書要求に含めて送信したナンスと比較して認証を行うことができる。図５では、ナンスを信用証明書要求応答５００に含まれた形で示しているが、ナンスは任意である。
【００７１】
信用証明書情報５０６は、ユーザ名、パスワード、ログイン手順情報、又はこれらの組み合わせを含むことができる。信用証明書情報５０６は鍵／値の対５０８～５１０を含むことができる。信用証明書情報５０６内にはあらゆる数の鍵／値の対が存在することができる。鍵／値の対は、デジタル装置１０２が受け取って解釈する信用証明書情報を表すことができる。信用証明書情報５０６を鍵／値の対として示すのは例示目的にすぎず、信用証明書情報は、必ずしも鍵／値の対に限定されないあらゆるフォーマットとすることができる。
【００７２】
図６は、ネットワーク信用証明書を提供する例示的な方法のフロー図である。ステップ６０２において、信用証明書サーバ１１６が、デジタル装置１０２から信用証明書要求を受け取る。
【００７３】
様々な実施形態では、信用証明書サーバ１１６が、デジタル署名を暗号鍵で解読して認証する。その後、ステップ６０４において、信用証明書サーバ１１６が、ネットワーク記録に含まれるＤＤＩＤ及びＳＳＩＤに基づいてネットワーク記録を識別することができる。１つの例では、信用証明書要求応答モジュール２０６が、信用証明書要求の中のＤＤＩＤに関連する１又はそれ以上のネットワーク記録を取り出す。その後、信用証明書要求応答モジュール２０６は、取り出した（単複の）ネットワーク記録内のＳＳＩＤに関連する少なくとも１つのネットワーク信用証明書を識別する。
【００７４】
ステップ６０６において、信用証明書要求応答モジュール２０６が、選択したネットワーク記録から、識別した（単複の）ネットワーク信用証明書を取り出す。１つの例では、信用証明書要求応答モジュール２０６が、デジタル装置１０２のユーザがネットワークアクセスを取得するために認証サーバ１０８に提供しなければならないユーザ名及びパスワードを識別する。ステップ６０８において、信用証明書要求応答モジュール２０６が、（ユーザ名、パスワードなどの）ネットワーク信用証明書を含む信用証明書要求応答をデジタル装置１０２に対して生成する。
【００７５】
いくつかの実施形態では、信用証明書要求応答モジュール２０６が、ネットワーク信用証明書の一部としてログイン手順情報を識別することができる。信用証明書要求応答モジュール２０６は、（ＳＳＩＤに関連するパスワードを含む同じネットワーク記録などの）ネットワーク記録からログイン手順情報を取り出すことができる。ログイン手順情報は、ネットワークアクセスを取得するためにデジタル装置１０２が従うためのフォーム識別子及び（パラメータなどの）命令を含むことができる。１つの例では、デジタル装置１０２が、信用証明書要求応答の中のネットワーク信用証明書からフォーム識別子及び命令を取り出す。デジタル装置１０２は、このフォーム識別子及び命令に基づいて、認証サーバ１０８及び入力データから受け取ったフォームを識別することができる。別の例では、デジタル装置１０２が、信用証明書要求応答に含まれるログイン手順情報に基づいて、ネットワークアクセスを取得するための情報を認証サーバ１０８に提供する。認証サーバ１０８に情報を提供する処理は、２００７年９月６日に出願された「ネットワークアクセスを取得するシステム及び方法」という名称の米国特許出願第１１／８９９，６３８号にさらに記載されている。
【００７６】

図７は、ネットワーク信用証明書を提供するための例示的な方法の別のフロー図である。デジタル装置１０２は、ネットワーク装置１０４を介して利用可能な無線ネットワークを検索し、これを発見することができる。ステップ７０２において、デジタル装置１０２は、ホットスポットに接続している間にネットワーク構成情報を受け取ることができる。ネットワーク構成情報は、ネットワーク装置１０４又はＤＮＳサーバ１１０の識別子を含むことができる。１つの例では、デジタル装置１０２が、接続処理中に（ＤＮＳサーバ１１０などの）ＤＮＳサーバのＩＰアドレスを受け取る。

【００７７】

ステップ７０４において、デジタル装置１０２が信用証明書要求を生成する。この信用証明書要求は、シーケンス識別子、ＤＤＩＤ及びＳＳＩＤを含むことができる。ステップ７０６において、デジタル装置１０２が任意にナンスを生成し、暗号鍵を使用して信用証明書要求にデジタル署名する。ステップ７０８において、デジタル装置１０２が、信用証明書要求を標準プロトコルとして送信する。ネットワーク装置１０４は、信用証明書要求を受け取って通信ネットワーク１１４へ転送することができる。様々な実施形態では、ネットワーク装置１０４が、信用証明書要求をＤＮＳサーバ１１０に提供し、このＤＮＳサーバ１１０が、信用証明書要求を信用証明書サーバ１１６へ転送することができる。

【００７８】

例示的な実施形態では、信用証明書サーバ１１６の信用証明書要求モジュール２０４が信用証明書要求を受け取る。信用証明書要求モジュール２０４は、信用証明書サーバ内のＤＤＩＤに関連する暗号鍵を暗号鍵ストレージ２１２から取り出すことができる。その後、信用証明書要求モジュール２０４は、信用証明書要求のデジタル署名を解読して認証を行うことができる。信用証明書要求モジュール２０４は、信用証明書要求からナンス及びシーケンス識別子をさらに取り出すことができる。

【００７９】

その後、信用証明書サーバ１１６の信用証明書要求応答モジュール２０６は、ネットワーク記録ストレージ２１０からＤＤＩＤ及びＳＳＩＤに関連するネットワーク記録を取り出すことができる。信用証明書要求応答モジュール２０６は、ネットワーク記録からネットワーク信用証明書を取り出して信用証明書要求応答を生成する。信用証明書要求応答は、ネットワーク信用証明書及びナンスを含むことができる。暗号化／解読モジュール２０８は、暗号鍵ストレージ２１２から取り出したＤＤＩＤに関連する暗号鍵を使用して、信用証明書要求応答を暗号化することができる。いくつかの実施形態では、信用証明書要求応答が（ＤＮＳなどの）標準プロトコルとしてフォーマットされる。

【００８０】

ステップ７１０において、デジタル装置１０２が信用証明書要求応答を受け取る。その後、ステップ７１２において、デジタル装置１０２が信用証明書要求応答を認証する。１つの例では、デジタル装置１０２が、信用証明書要求にデジタル署名するために使用するものと同じ暗号鍵を使用して信用証明書要求応答を解読する。デジタル装置１０２は、信用証明書要求応答内のナンスをさらに取り出し、このナンスを、信用証明書要求に含めて送信したナンスと比較してさらに認証を行うことができる。信用証明書要求応答が本物であると判明した場合、ステップ７１４において、デジタル装置１０２が、信用証明書要求応答からネットワーク信用証明書を取り出す。

【００８１】

ステップ７１６において、デジタル装置１０２が、ネットワークアクセスに関連する認証要件を識別する。様々な実施形態では、デジタル装置１０２が、認証サーバ１０８に提供するのに適した情報及びネットワーク信用証明書を決定する。１つの例では、デジタル装置１０２が、認証サーバ１０８から１又はそれ以上のネットワークアクセスページを取り出す。デジタル装置１０２は、認証サーバからの正しいネットワークアクセスページにアクセスして自動的に選択を行うことができる。１つの例では、デジタル装置１０２が、選択を自動的に起動する（例えば、ネットワークアクセスページ内のボタンを起動する、ボックスをチェックする、及びラジオボタンを選択する）ことができる。

【００８２】
例えば、信用証明書要求応答モジュール２０６は、ネットワークアクセスページ内の自動選択のための命令をデジタル装置１０２に提供することができる。本明細書で説明したように、ネットワークアクセスページは、認証サーバ１０８から取り出した１又はそれ以上のウェブページ、１又はそれ以上のタグ、又はこれらの両方の組み合わせを含むことができる。１つの例では、デジタル装置１０２内のソフトウェアが、ネットワークアクセスページ内の全ての選択ボックスに自動的にチェックを入れることができる。その後、デジタル装置１０２は、ログイン手順情報に基づいて選択ボックスのチェックを外すことができる。当業者であれば、自動的に選択を行えるようにする方法は数多く存在できることを理解するであろう。他の実施形態では、デジタル装置１０２が、認証サーバ１０８からＸＭＬタグを受け取る。デジタル装置１０２は、ログイン手順情報の中のＸＭＬタグ及び命令に基づく情報を認証サーバ１０８に提供してネットワークアクセスを取得することができる。

【００８３】
ステップ７１８において、デジタル装置１０２が、ネットワーク装置１０４にネットワーク信用証明書を提供して通信ネットワーク１１４へのネットワークアクセスを取得する。１つの例では、信用証明書要求応答モジュール２０６が、認証サーバ１０８から１又はそれ以上のフォームを取り出し、フォームに１又はそれ以上のネットワーク信用証明書を読み込んで、完成したフォームを認証サーバ１０８に提供する。別の例では、信用証明書要求応答モジュール２０６が、必要に応じて認証サーバ１０８にネットワーク信用証明書を提供する。認証サーバ１０８は、ネットワーク信用証明書を受け取ると、デジタル装置１０２と通信ネットワーク１１４の間の通信を可能にすることができる。１つの例では、認証サーバ１０８が、アクセスコントローラ１１２に、デジタル装置１０２の通信ネットワーク１１４へのアクセスを許可するように命令する。

【００８４】
その後、デジタル装置１０２は、ネットワーク接続性をテストしてネットワークアクセスを確認することができる。１つの例では、デジタル装置１０２が、通信ネットワーク１１４を利用できるかどうかを判定するための要求を信用証明書サーバ１１６へ送信する。いくつかの実施形態では、クエリ又はコマンドが、以前に信用証明書要求に含めて提出したシーケンス識別子を含む。ネットワークアクセスが成功した場合、信用証明書サーバ１１６は、この要求を受け取ってシーケンス識別子を取り出すことができる。この結果、信用証明書サーバ１１６は、ネットワークアクセスが成功したことを確認することができる。

【００８５】
図８は、ネットワーク信用証明書を受け取って記憶するための例示的な方法のフロー図である。様々な実施形態では、ユーザが、ネットワーク記録を作成して信用証明書サーバ１１６に記憶することができる。例えば、信用証明書サーバ１１６は、ユーザがネットワーク記録を作成、記憶、更新、削除、及び修正できるようにするグラフィカルユーザインターフェイス（ＧＵＩ）を提供する信用証明書記憶モジュール（図示せず）を含むことができる。

【００８６】
ステップ８０２において、信用証明書サーバ１１６が、ユーザにネットワーク信用証明書要求フォームを提供する。１つの例では、信用証明書サーバ１１６が、ネットワーク信用証明書要求フォームを、インターネットを介して１又はそれ以上のウェブページとしてユーザに提供する。ネットワーク信用証明書要求フォームは、（運営会社名などの）サービスプロバイダ名及び／又はＳＳＩＤ及びネットワーク信用証明書を受け取るように構成される。

【００８７】
サービスプロバイダ名は、ホットスポット、ホットスポットに関する１又はそれ以上の構成要素（例えばネットワーク装置１０４）、又はローカルエリアネットワーク１０６の

インフラを運営するエンティティ名を含むことができる。いくつかの実施形態では、サービスプロバイダ名が、別のサービスプロバイダの１又はそれ以上のホットスポットを管理する組織名を含む。１つの例では、たとえホットスポットに異なるサービスプロバイダが存在していても、コーヒーショップ及び書店は、両方とも第三の管理者を使用してホットスポットを管理することができる。いくつかの実施形態では、ネットワーク信用証明書要求フォームを、第三の管理者名を受け取るように構成することができる。いくつかの実施形態では、サービスプロバイダ名が、ホットスポットネットワークへのアクセスを再販する組織（アグリゲータなど）の名前を含む。

【００８８】

ネットワーク信用証明書要求フォームは、ネットワークサービス選択としてＳＳＩＤを受け取ることもできる。１つの例では、ネットワーク信用証明書要求フォームが、異なるサービスプロバイダのプルダウンメニュー及び／又はユーザが選択できるホットスポットを含む。例えば、ユーザは、ホットスポットとして「スターバックス」又は「サンフランシスコ国際空港」を選択することができる。ユーザには、ホットスポットの地理的位置などに対するさらなる選択肢を与えることができる。ユーザは、サービスプロバイダを選択することもできる。例えば、ユーザは、サービスプロバイダとして「Ｔ－Ｍｏｂｉｌｅ」を選択することができる。この結果、ネットワーク信用証明書要求フォームは、ユーザがＴ－ｍｏｂｉｌｅに関連する１又はそれ以上の様々なホットスポットの中から選択を行えるようにすることができる。その後、これらの（単複の）選択をネットワーク記録として記憶することができる。或いは、（単複の）選択に関連するネットワークサービス識別子がＳＳＩＤとして生成される。

【００８９】

さらに、ネットワーク信用証明書要求フォームは、ユーザからネットワーク信用証明書を受け取ることができる。例えば、ユーザは、ネットワーク信用証明書要求フォームの中に、ネットワーク信用証明書としてユーザ名、パスワード、パスコードを入力することができる。いくつかの実施形態では、ネットワーク信用証明書要求フォームが、ＳＳＩＤを受け取った後で、必要なネットワーク信用証明書の種類を決定する。例えば、ネットワーク信用証明書要求フォームは、ユーザが先程選択したサンフランシスコ国際空港のホットスポットにおいてネットワークにアクセスするために必要な情報を識別する。その後、ネットワーク信用証明書要求フォームは、ユーザがこのホットスポットにおいてネットワークアクセスを取得するために必要な（ユーザ名、パスワードなどの）情報のみを入力できるようにするフィールド又は選択肢を生成する。

【００９０】

信用証明書サーバ１１６はまた、ネットワーク信用証明書要求フォームを受け取る前に登録を行うことをユーザに求めることもできる。登録中、ユーザは、サービス条件に同意して顧客情報を入力する必要がある。顧客情報は、信用証明書サーバ１１６にアクセスしてネットワーク信用証明書を記憶するためのユーザ名及びパスワードを含む。任意に、顧客情報は、ユーザの住所、連絡先情報、及び信用証明書サーバ１１６により提供されるサービスをユーザが使用するための支払い選択肢を含むことができる。

【００９１】

ステップ８０４において、信用証明書サーバ１１６が、ネットワーク信用証明書要求フォームを介して顧客情報及びネットワークサービスの選択を受け取る。ステップ８０６において、信用証明書サーバが、ネットワーク信用証明書を取り出すことができる。ステップ８０８において、信用証明書サーバ１１６が顧客情報を受け取る。ステップ８１０において、信用証明書サーバ１１６が、ネットワーク信用証明書を顧客情報、ネットワークサービスの選択、及び（単複の）ネットワーク信用証明書と関連付けてネットワーク記録を作成する。その後、ステップ８１２において、ネットワーク記録が記憶される。

【００９２】

いくつかの実施形態では、ユーザが、インターネットを介して信用証明書サーバ１１６に手動でアクセスすることができる。他の実施形態では、ユーザが、ネットワーク信用証

明書ソフトウェアをダウンロードしてデジタル装置１０２上にインストールすることができる。このネットワーク信用証明書ソフトウェアは、デジタル装置１０２のＤＤＩＤを識別して信用証明書サーバ１１６へ送ることができる。他の実施形態では、デジタル装置１０２上にネットワーク信用証明書ソフトウェアをプリインストールすることができる。デジタル装置１０２がネットワーク信用証明書ソフトウェアを最初に起動する際に、ネットワーク信用証明書ソフトウェアが、デジタル装置１０２のＤＤＩＤ識別して信用証明書サーバへ送ることができる。

【００９３】

ユーザは、ネットワーク信用証明書ソフトウェアにＳＳＩＤを入力する（例えば、サービスプロバイダ又はホットスポットを識別する）ことができる。ユーザは、ネットワーク信用証明書ソフトウェアにネットワーク信用証明書を入力することもできる。ネットワーク信用証明書ソフトウェアは、ＤＤＩＤ、ＳＳＩＤ及びネットワーク信用証明書を取得した後で、この情報を信用証明書サーバ１１６にアップロードし、信用証明書サーバ１１６は、この情報をネットワーク記録に記憶することができる。様々な実施形態では、ネットワーク信用証明書ソフトウェアを信用証明書サーバ１１６からダウンロードすることができる。

【００９４】

図９は、例示的なデジタル装置のブロック図である。信用証明書サーバ１１６は、プロセッサ９００、メモリシステム９０２、記憶システム９０４、入出力インターフェイス９０６、通信ネットワークインターフェイス９０８、及びディスプレイインターフェイス９１０を含む。プロセッサ９００は、（プログラムなどの）実行可能命令を実行するように構成される。いくつかの実施形態では、プロセッサ９００が、実行可能命令を処理できる回路又はいずれかのプロセッサを含む。

【００９５】

メモリシステム９０２は、データを記憶するように構成されたいずれかのメモリである。メモリシステム９０２のいくつかの例として、ＲＡＭ又はＲＯＭなどの記憶装置がある。メモリシステム９０２は、ラムキャッシュを含むことができる。様々な実施形態では、メモリシステム９０２にデータが記憶される。メモリシステム９０２内のデータは、クリア又は最終的に記憶システム９０４に伝送することができる。

【００９６】

記憶システム９０４は、データを取り出して記憶するように構成されたいずれかのストレージである。記憶システム９０４のいくつかの例として、フラッシュドライブ、ハードドライブ、光ドライブ及び／又は磁気テープがある。いくつかの実施形態では、信用証明書サーバ１１６が、ＲＡＭの形のメモリシステム９０２及びフラッシュデータの形の記憶システム９０４を含む。メモリシステム９０２及び記憶システム９０４はいずれも、プロセッサ９００などのコンピュータプロセッサにより実行可能な命令又はプログラムを記憶できるコンピュータ可読媒体を含む。

【００９７】

任意の入出力（Ｉ／Ｏ）インターフェイス９０６は、ユーザから入力を受け取ってデータを出力するいずれかの装置である。任意のディスプレイインターフェイス９１０は、グラフィクス及びデータをディスプレイに出力するように構成されたいずれかの装置である。１つの例では、ディスプレイインターフェイス９１０がグラフィックアダプタである。全てのデジタル装置１０２が、入出力インターフェイス９０６又はディスプレイインターフェイス９１０を含むとは限らないと理解されたい。

【００９８】

通信ネットワークインターフェイス（ｃｏｍ．　ｎｅｔｗｏｒｋ　ｉｎｔｅｒｆａｃｅ）９０８は、リンク９１２を介して（ローカルエリアネットワーク１０６及び通信ネットワーク１１４などの）ネットワークに結合することができる。通信ネットワークインターフェイス９０８は、例えば、イーサネット（登録商標）接続、シリアル接続、パラレル接続又はＡＴＡ接続を介して通信をサポートすることができる。通信ネットワークインター

フェイス９０８は、（８０２．１１／ｂ／ｇ／ｎ、ＷｉＭａｘなどの）無線通信をサポートすることもできる。当業者には、通信ネットワークインターフェイス９０８が多くの有線及び無線標準をサポートできることが明らかであろう。

【００９９】

様々な実施形態では、満足のいくサービス品質を実現するために、デジタル装置が様々なルールに基づいて複数の利用可能な無線ネットワークから利用可能な無線ネットワークを自動的に選択してアクセスできるようにするシステム及び方法について説明する。このようなルールを、デジタル装置自体の中で、デジタル装置と通信しているサーバ上で、又はこれらの両方の組み合わせで実施することができる。様々な実施形態では、無線ネットワークは、デジタル装置とインターネットなどの通信ネットワークとの間の無線アクセスを可能にするネットワークである。

【０１００】

いくつかの実施形態によれば、（Ｗｉ－Ｆｉ通信が可能なデジタル装置などの）無線デジタル装置のユーザが、ウェブサーバ上にアカウントを作成し、このアカウントを使用して１又はそれ以上の（コンピュータ、ラップトップ、携帯情報端末及び携帯電話などの）デジタル装置を登録する。登録されたデジタル装置を管理して、ＨＴＴＰなどのネットワーク通信メカニズムを介して（プロファイルサーバ又は信用証明書サーバなどの）中央サーバによりネットワーク記録が提供されるようにすることができる。

【０１０１】

図１０は、本発明の実施形態を実施できる別の環境を示す図である。様々な実施形態では、デジタル装置１００２を有するユーザが、ネットワーク装置１００４及び１００６の近くに存在する領域に入る。１つの例では、ネットワーク装置１００４及び１００６が別個のアクセスポイントであり、これらの各々を使用して、デジタル装置１００２と通信ネットワーク１００８の間の通信を確立することができる。

【０１０２】

デジタル装置１００２は、デジタル装置１００２を取り巻く領域を走査し、２つのネットワーク装置１００４及び１００６を検出し、デジタル装置１００２が通信を確立できる利用可能な無線ネットワークのリストを生成することができる。いくつかの実施形態では、利用可能な無線ネットワークのリストが、ネットワーク装置１００４及び１００６のＤＤＩＤ識別子、ＳＳＩＤ識別子及び／又はＢＢＳＩＤ識別子を含む。

【０１０３】

その後、デジタル装置１００２は、この利用可能な無線ネットワークのリストをルールサーバ１０１０に提供する。１つの例では、デジタル装置１００２が、利用可能な無線ネットワークのリストを、ネットワーク装置１００４又はネットワーク装置１００６のオープンポートに対する標準プロトコルとして通信ネットワーク１００８に提供し、最終的にはルールサーバ１０１０に提供する。別の例では、デジタル装置１００２が、図示していないセルラ通信ネットワークなどの別のネットワークを介して（ＣＤＭＡ、ＧＳＭ（登録商標）、３Ｇ、又はＥＶＤＯなどを介して）利用できる無線ネットワーク、又は（Ｗｉ－Ｆｉ、Ｗｉｍａｘ又はＬＴＥネットワークなどの）その他の無線ネットワークをのリストを提供する。

【０１０４】

ルールサーバ１０１０は、利用可能な無線ネットワークのリストを受け取り、リスト内で識別された個々の無線ネットワークのネットワークプロファイルを取り出すことができる。ネットワークプロファイルとは、無線ネットワークに関連するとともに、この関連するネットワークにより提供される性能及び／又はサービス品質に関する属性を含む記録のことである。１つの例では、ルールサーバ１０１０が、リスト内の個々のネットワークを識別して個々のネットワークのＳＳＩＤ及び／又はＢＢＳＩＤをプロファイルサーバ１０１４に提供する。その後、プロファイルサーバ１０１４は、個々のネットワークの（ＳＳＩＤ及び／又はＢＢＳＩＤに基づく）ネットワークプロファイルをルールサーバ１０１０に提供することができる。いくつかの実施形態では、プロファイルサーバ１０１４が、デ

ータベース又は（ネットワークデータベースサーバ１０１２などの）その他のサーバからネットワークプロファイルを取り出す。

【０１０５】

ルールサーバ１０１０は、ネットワークプロファイル内の属性、及び／又はデジタル装置１００２から受け取ったあらゆる属性に基づいて、利用可能な無線ネットワークのリストから好ましい無線ネットワークを選択することができる。属性とは、無線ネットワークの特性のことである。様々な実施形態では、属性が、性能測定基準、共有インジケータ、又はサービス識別子を含む。無線ネットワークの性能測定基準とは、ネットワーク性能のいずれかの尺度のことである。いくつかの例では、性能測定基準が、待ち時間測定基準、帯域幅測定基準、又はサービス品質（ＱＯＳ）測定基準を含むことができる。当業者であれば、性能測定基準が、無線ネットワークの性能を表すあらゆる種類の測定基準を含むことができると理解するであろう。

【０１０６】

待ち時間測定基準とは、ネットワーク上でデジタル装置からサーバへデータパケットを送信するための時間を表す尺度のことである。いくつかの実施形態では、デジタル装置１００２がサーバへＩＣＭＰ「エコー要求」パケットを送信し、ＩＣＭＰ「エコー反応」応答に耳を傾けることができる。待ち時間測定基準は、往復時間（一般的にはミリ秒単位）の推定値を含み、及び／又はいずれかのパケット損失を含むことができる。別の例では、待ち時間測定基準が、推定される往復時間の半分である。

【０１０７】

帯域幅測定基準とは、無線ネットワークの利用可能な帯域幅の尺度のことである。１つの例では、デジタル装置が、無線ネットワークを介してサーバへデータブロックを送信して応答のタイミングを計ることにより、利用可能な帯域幅をテストすることができる。

【０１０８】

ＱＯＳ測定基準は、無線ネットワーク、アクセス装置１００４、アクセス装置１００６、及び／又は通信ネットワーク１００８のサービス品質を測定するいずれかの尺度である。１つの例では、ＱＯＳ測定基準が、ＩＰアドレスを得るために必要な時間の長さを計ることにより判定されるＤＨＣＰの信頼度を表す。ＤＨＣＰの信頼度は、統計的測定、ＩＰアドレスを多少なりとも受け取る確率、及び／又は時間の配分を含むことができる。

【０１０９】

共有インジケータは、無線ネットワークが共有されているかどうかを示す。いくつかの実施形態では、共有インジケータを、「共有」、「非共有」、「不明」を含む３つの状態のうちの１つとすることができる。共有インジケータは、（「非共有」などの）１つの状態しか含むことができないが、当業者であれば、共有インジケータがあらゆる数の状態を有することができると理解するであろう。ネットワークが「共有」されていることを示す共有インジケータを含む無線ネットワークは、無線ネットワークの所有者が、他の誰かがネットワークの使用を意図していることを示すことができる。「共有」ネットワークの一例として、他の誰かが使用するために意図的に「オープン」になっている（例えば、暗号化されていない）無線ネットワークを挙げることができる。

【０１１０】

ネットワークが「非共有」であることを示す共有インジケータを含む無線ネットワークは、無線ネットワークの所有者が、ネットワークにアクセスするための明確な許可を持たない者を望まないことを示すことができる。１つの例では、非共有の無線ネットワークは、無許可のユーザに対してアクセスを制限するために（ＷＥＰ又はＷＰＡなどを介して）意図的に暗号化されていることが多い。しかしながら、全ての「非共有」のネットワークが暗号化されているとは限らない。例えば、たとえネットワークが共有を意図されていなくても、ネットワークの所有者がネットワーク装置を誤って設定したり、或いはエラーを通じてネットワークがオープン（すなわち非暗号化に）になったりする可能性がある。

【０１１１】

ネットワークが「不明」であることを示す共有インジケータを含む無線ネットワークは

、無線ネットワークが「共有」又は「非共有」のいずれの可能性もあることを示すことができる。例えば、オープンネットワークの所有者の意図が不明な場合がある。

【０１１２】

サービス識別子は、無線ネットワークがサポートする１又はそれ以上のサービスを識別することができる。１つの例では、１又はそれ以上のサービス識別子が、無線ネットワークがＶｏＩＰ、テレビ会議及び／又はビデオ会議をサポートしていることを示す。サービス識別子は、無線ネットワークがサポートするあらゆる種類のサービスを識別することができる。いくつかの実施形態では、サービス識別子が、無線ネットワークがサポートしていないサービスを識別することができる。

【０１１３】

当業者であれば、ネットワークプロファイルがあらゆる数の属性を含むことができると理解するであろう。さらに、当業者であれば、ネットワークプロファイルが１つのみ又はそれ以上の性能測定基準、１つのみの共有インジケータ又は１つのみ又はそれ以上のサービス識別子を含むことができることを理解するであろう。

【０１１４】

様々な実施形態では、ルールサーバ１０１０が、属性分析に基づいて、利用可能な無線ネットワークのリストから１又はそれ以上の無線ネットワークを選択する。１つの例では、ルールサーバ１０１０が属性に様々なルールを適用する。これらのルールとして、最低要件、個別設定、及び属性比較を挙げることができる。１つの例では、ルールサーバ１０１０により適用されるルールが、１又はそれ以上の無線ネットワークの属性を１又はそれ以上の最低要件と比較することができる。無線ネットワークの属性が最低要件を下回る場合、この無線ネットワークを選択することができず、又は利用可能な無線ネットワークのリストから削除することができる。

【０１１５】

いくつかの実施形態では、ルールサーバ１０１０により適用されるルールが、ユーザによる個別設定に基づくことができる。例えば、デジタル装置１００２のユーザは、デジタル装置１００２を、「共有」と指定された無線ネットワークを介してのみ接続すべきであることを示す個別設定を示すことができる。この例では、ルールサーバ１０１０は、無線ネットワークを「共有」であると識別する共有インジケータを含む属性の無線ネットワークのみを選択することができる。

【０１１６】

様々な実施形態では、ルールサーバ１０１０により適用されるルールが、１つの無線ネットワークの属性と別のネットワークの属性との比較に基づくことができる。１つの例では、属性が、１つの無線ネットワークが別の無線ネットワークよりも帯域幅が大きく、待ち時間が短いことを示すことができる。この例では、ルールサーバ１０１０は、別の無線ネットワークとの比較においてより性能が良く、又はサービスの価値が高い１つの無線ネットワークを選択することができる。当業者であれば、利用可能な無線ネットワークのリストから無線ネットワークを選択する際に、選択又は支援のために使用するルールにはあらゆる種類があり得ることを理解するであろう。

【０１１７】

無線ネットワーク選択を行う際には、ルールサーバ１０１０が２以上のルールを適用することができる。１つの例では、ルールサーバ１０１０が、異なる無線ネットワークからの属性を比較して選択を行う前に、ユーザの個別設定を適用することができる。別の例では、ルールサーバ１０１０が、属性を比較する前に、属性に最低要件を適用することができる。

【０１１８】

ルールサーバ１０１０は、ネットワークプロファイルからの属性の比較に基づいて無線ネットワークを選択したら、この無線ネットワーク選択をデジタル装置１００２に提供することができる。無線ネットワーク選択は、少なくとも１つの無線ネットワークを識別する（ネットワーク識別子などの）１又はそれ以上の識別子を含む。この無線ネットワーク

選択は、単一の無線ネットワークを識別すること、又は優先度順にソートされた無線ネットワークのソート済みリストを含むことができる。

【０１１９】

いくつかの実施形態では、ルールサーバ１０１０が、無線ネットワーク選択に加え、選択された無線ネットワークの（信用証明書要求応答などの）信用証明書もデジタル装置１００２に提供する。１つの例では、ルールサーバ１０１０が、選択された無線ネットワークを信用証明書サーバ１０１６に提供し、次にこの信用証明書サーバ１０１６が、（たとえ信用証明書要求が行われなかったとしても）選択された無線ネットワークの信用証明書要求応答をデジタル装置１００２に提供する。他の実施形態では、デジタル装置１００２が無線ネットワーク選択を受け取り、その後、本明細書で説明したように、信用証明書サーバ１０１６に信用証明書要求を送信するステップに進んで信用証明書を受け取る。

【０１２０】

さらに、様々な実施形態では、デジタル装置１００２が、選択された無線ネットワークに基づいて接続を確立しようと試みる。接続が失敗した場合、デジタル装置１００２は、本明細書で説明したように、信用証明書要求を信用証明書サーバ１０１６へ送信して、ネットワークアクセスのための信用証明書を取り出すことができる。デジタル装置１００２は、ネットワーク装置１００４のオープンポートを介して信用証明書サーバ１０１６に信用証明書要求を提供することができる。別の例では、デジタル装置１００２が、異なるネットワーク装置との接続を含む他のいずれかのネットワークを介して、又は携帯電話接続を介して信用証明書要求を提供することができる。

【０１２１】

図１では、ルールサーバ１０１０、ネットワークデータベースサーバ１０１２、プロファイルサーバ１０１４、信用証明書サーバ１０１６及びウェブサーバ１０１８を別個のサーバとして示しているが、これらのサーバは全て、１又はそれ以上のサーバとして組み合わせることができる。同様に、サーバのいずれかの機能を、図示している他のサーバの１つ又はその他のいずれかのサーバが実行することもできる。

【０１２２】

図１０には、複数の利用可能な無線ネットワークから無線ネットワーク選択を行うための複数のサーバ（ルールサーバ、ネットワークデータベースサーバ、プロファイルサーバ、信用証明書サーバ、及びウェブサーバなど）を示しているが、当業者であれば、無線ネットワーク選択をデジタル装置１００２内で行うこともできると理解するであろう。１つの例では、デジタル装置１００２が、利用可能な無線ネットワークを一覧にした走査結果を取り出して、設定優先度に基づいて無線ネットワークを選択する。この設定優先度は、１又はそれ以上のローカルに実行されるルール、好ましい信号強度、又はその他のいずれか１つの又は複数の属性に基づくことができる。別の例では、デジタル装置１００２が、（ＶｏＩＰなどの）所望のサービスをサポートし、最小待ち時間標準を満たし、最小ＱＯＳ標準を満たす無線ネットワークを選択する。別の例では、プロファイルサーバ１０１４が、所望のネットワークプロファイルをデジタル装置１００２に提供し、このデジタル装置１００２が分析を行って好ましい無線ネットワークを決定する。

【０１２３】

図１１は、無線ネットワーク選択を提供する例示的な処理のフロー図である。ステップ１１０２において、（ルールサーバ１０１０、ネットワークデータベースサーバ１０１２、プロファイルサーバ１０１４、信用証明書サーバ１０１６又はウェブサーバ１０１８などの）サーバが、デジタル装置１００２から利用可能な無線ネットワークのリストを受け取る。いくつかの例では、このリストは、（ネットワーク装置１００４及びネットワーク装置１００６などの）１又はそれ以上のネットワーク装置のＳＳＩＤ又はＢＢＳＩＤを含む。リストは、ネットワーク及び／又はネットワーク装置を識別するあらゆる情報を含むことができる。

【０１２４】

いくつかの実施形態では、サーバが、ネットワーク及び／又はネットワーク装置に関連

する１又はそれ以上の属性も受け取る。様々な実施形態では、デジタル装置１００２が、信号強度を測定し、利用可能なサービスを判別し、又は利用可能な無線ネットワークのリスト上で識別される１又はそれ以上のネットワーク及び／又はネットワーク装置の性能測定基準を取り上げる。

【０１２５】

ステップ１１０４において、サーバが、ネットワークデータベースに記憶された複数のネットワークプロファイルから、利用可能な無線ネットワークのリスト上の個々の利用可能な無線ネットワークのネットワークプロファイルを取り出す。個々のネットワークプロファイルは、少なくとも１つの属性を含むことができる。いくつかの実施形態では、リスト上の全ての無線ネットワークがネットワークプロファイルを有するとは限らない。リスト上の無線ネットワークのネットワークプロファイルが見つからない場合、この無線ネットワークに関連するネットワークプロファイルを作成することができる。デジタル装置１００２から属性を受け取った場合、サーバは、デジタル装置１００２から受け取ったいずれの属性がいずれのネットワーク、ネットワーク装置及び／又はネットワークプロファイルに関連するかを判定することができる。

【０１２６】

ステップ１１０６において、サーバが、個々のネットワークプロファイルからの属性を最低要件と比較する。１つの例では、サーバが、（利用可能な場合）リスト内の全てのネットワークプロファイルからの待ち時間測定基準を最小待ち時間測定基準と比較する。サーバは、デジタル装置１００２から受け取った属性を最低要件と比較することもできる。ステップ１１０８において、サーバが、（単複の）比較に基づいて、利用可能な無線ネットワーク及び／又は無線ネットワークプロファイルのリストから１又はそれ以上の無線ネットワークを削除する。例えば、待ち時間測定基準が最小待ち時間測定基準を下回る無線ネットワークは選択しなくてもよい。他の実施形態では、待ち時間測定基準が最小待ち時間測定基準を下回る無線ネットワークが重み値を受け取り、これを他の無線ネットワークと比較して選択処理を支援することができる。

【０１２７】

いくつかの実施形態では、デジタル装置１０１０のユーザが最低要件を決定する。他の実施形態では、（管理者などが）ユーザのために最低要件を選択することができる。

【０１２８】

ステップ１１１０において、サーバがユーザのための個別設定を取り出す。ユーザは、この個別設定をサーバへ送ることができる。いくつかの実施形態では、ユーザが、個別設定を含むウェブサーバ１０１８とのアカウントを有する。１つの例では、サーバが、利用可能な無線ネットワークのリストとともにユーザ識別子を受け取る。次に、サーバは、ユーザのアカウントにアクセスして個別設定を受け取り、その後、この個別設定が、リスト上の無線ネットワークに関連するネットワークプロファイルの属性に適用される。様々な実施形態では、ユーザが（「攻撃性」などの）個別設定を設定することができ、デジタル装置１００２は、この設定で無線ネットワークに接続することができる。このような設定は以下を含むことができる。

（ａ）　共有インジケータに関係なくオープンなものに接続する。

（ｂ）　所有者が混乱してアクセスポイントを単純にオープンのままにしてセキュリティ機能の設定方法を知らないと思われる旨を（「ｌｉｎｋｓｙｓ」などの）デフォルトのメーカＳＳＩＤが示すもの以外はオープンなものに接続する。

（ｃ）　プロファイルサーバ１０８が認めた（又はＷｉ－Ｆｉネットワークに関する情報を既に記憶している）オープンなものに接続する。或いは、

（ｄ）　「共有」という共有インジケータを含み、又は他の何らかの手段により共有と示されるオープンなものに接続する。当業者であれば、個別設定が数多く存在できることを理解するであろう。

【０１２９】

ステップ１１１２において、サーバが、個別設定に基づいてリスト又はネットワークプ

ロファイルから１又はそれ以上の無線ネットワークを削除する。例えば、個別設定は、ビデオ会議をサポートし、ユーザが定義したＱｏＳ要件を保持する無線ネットワークへの接続のみをユーザが望んでいることを示すことができる。その後、サーバは、ネットワークプロファイルから得られた、又はユーザの個別設定を満たさないデジタル装置１００２から最近受け取った属性に基づいて、利用可能な無線ネットワークのリストからいずれかの無線ネットワークを削除することができる。

【０１３０】

いくつかの実施形態では、その後、ネットワークプロファイルから得られた属性の比較前、又は比較後に個別設定を考慮することができる。１つの例では、個別設定が、「共有」と指定されていない、又は特定のサービスを提供していない無線ネットワークへの接続をユーザが望まないことを示す。１つの例では、ルールサーバ１０１０が、必要なサービスを提供しないネットワークに関連するネットワークプロファイルを取り出さず、及び／又はこれらのネットワークに関連する属性を比較しない。他の実施形態では、デジタル装置１００２が、ルールサーバ１０１０から受け取った結果（無線ネットワーク選択など）に個別設定を適用した後で好ましい無線ネットワークにアクセスする。

【０１３１】

ステップ１１１４において、サーバが、リスト上の残りの無線ネットワークの属性を比較する。様々な実施形態では、サーバが重みを適用して、ネットワークプロファイル内から得られた（測定基準などの）属性の１又はそれ以上を標準化する。いくつかの実施形態では、古い属性を削除し、又はより新しい他の属性よりも低く重み付けすることができる。１つの例では、１週間よりも以前のあらゆる測定基準に同様のより新しい測定基準よりも低い重みを付けることができる。別の例では、１ヵ月よりも以前の測定基準をネットワークプロファイルから削除し、又は比較において検討対象外とすることができる。当業者であれば、ネットワークプロファイル内から得られる全ての属性又は情報を比較において考慮できるわけではないことを理解するであろう。

【０１３２】

個々のネットワークプロファイルは、あらゆる数の属性を含むことができる。１つの例では、ルールサーバ１０１０が、２つの異なるネットワークプロファイルからの測定基準の比較に基づいて無線ネットワーク選択を行う。いくつかの実施形態では、ルールサーバ１０１０が、２つの類似する測定基準間の比較に基づいて無線ネットワークを選択する（すなわち、第１のネットワークプロファイルからの待ち時間測定基準が、第２のネットワークプロファイルからの待ち時間測定基準と比較される）。当業者であれば、ルールサーバ１０１０が、２つの類似する最近受け取った測定基準間の比較又はネットワークプロファイル内の最近受け取った測定基準及び別の測定基準に基づいて無線ネットワークを選択できることを理解するであろう。

【０１３３】

他の実施形態では、ルールサーバ１０１０が、２つの異なる測定基準間の比較に基づいて無線ネットワークを選択する（すなわち、第１のネットワークプロファイルからの待ち時間測定基準が、第２のネットワークプロファイルからの帯域幅測定基準と比較される）。ルールサーバ１０１０は、適当な無線ネットワークを選択するための比較を行うために、類似する及び／又は異なる測定基準又は属性に重み付けして標準化するアルゴリズムを実行することができる。１つの例では、ルールサーバ１０１０が、第１のネットワークプロファイル内の待ち時間測定基準を第２のネットワークプロファイル内の帯域幅測定基準と比較する。ルールサーバ１０１０は、測定基準に重み付けして標準化するアルゴリズムを実行することができる。待ち時間の方がネットワーク性能に及ぼす影響が大きいと考えられるので、このアルゴリズムは、待ち時間測定基準に帯域幅測定基準よりも大きく重み付けすることができる。

【０１３４】

属性又は測定基準は、あらゆる数の要素に依存して異なる重みを受け取ることができる。例えば、待ち時間測定基準は、この測定基準が許容範囲内にあるときには所定の重みを

受け取ることができ、そうでない場合には、大幅に下回る重みとなり得る。デジタル装置１００２から最近受け取った測定基準は、ネットワークプロファイル内の類似する種類の測定基準よりも大きな重みを受け取ることができる。当業者であれば、類似する及び／又は異なる性能及び／又は質的な測定基準を比較するための方法は数多く存在することを理解するであろう。

【０１３５】

ステップ１１１６において、サーバが、属性の比較に基づいて無線ネットワークを選択する。無線ネットワーク選択は、単一の好ましい無線ネットワーク、又は優先度順にソートされた無線ネットワークのリストを含むことができる。１つの例では、ルールサーバ１０１０が、最も好ましいネットワーク、２番目に好ましいネットワークなどを識別する。その後、ステップ１１１８において、ルールサーバ１０１０は、無線ネットワーク選択をデジタル装置１００２へ送信することができる。

【０１３６】

様々な実施形態では、ルールサーバ１０１０が、デジタル装置１００２から最近受け取った測定基準のみを比較する。１つの例では、デジタル装置１００２から２つの待ち時間測定基準が受け取られる。個々の待ち時間測定基準は、利用可能なネットワークのリスト上で識別された別個の無線ネットワークに関連する。この例では、ルールサーバ１０１０が、２つの属性の比較に基づいて無線ネットワークを選択することができる。

【０１３７】

図１２は、無線ネットワークを選択するための例示的な処理のフロー図である。１００２ステップにおいて、デジタル装置１００２が、２つの無線ネットワークを含む領域内に入り、デジタル装置１２０２が、アクセスするネットワークを求めて走査する。ステップ１２０４において、デジタル装置１００２が、第１及び第２の利用可能な無線ネットワークのネットワーク識別子を受け取る。本明細書で説明したように、第１及び第２のネットワーク識別子は、ＢＢＳＩＤ、ＳＳＩＤ、又はその他のいずれかのネットワーク識別子を含むことができる。例えば、第１のネットワーク識別子はＢＢＳＩＤを含むことができ、第２のネットワーク識別子はＳＳＩＤ識別子を含むことができる。別の例では、第１のネットワークが、ＢＢＳＩＤ及びＳＳＩＤを含む複数の識別子を提供できるのに対し、第２のネットワークはＳＳＩＤのみを提供する。この例では、第１のネットワーク識別子が、第１のネットワーク装置のＢＢＳＩＤ及びＳＳＩＤの両方を含むことができるのに対し、第２のネットワーク識別子は、第２のネットワーク装置のＳＳＩＤしか含まない。

【０１３８】

ステップ１２０６において、デジタル装置１００２が、利用可能な無線ネットワークのリストを生成する。例えば、デジタル装置１００２は、第１のネットワーク識別子及び第２のネットワーク識別子を含むリストを生成することができる。その後、ステップ１２０８において、リストがサーバに提供される。

【０１３９】

ステップ１２１０において、デジタル装置１００２が、無線ネットワーク選択をサーバから受け取る。無線ネットワーク選択は、選択された無線ネットワークを識別し、又は選択された無線ネットワークに関連するネットワーク装置を識別する識別子（ネットワーク装置のＢＢＳＩＤ及び／又はＳＳＩＤなど）を含むことができる。様々な実施形態では、無線ネットワーク選択が、優先度によってソートされた無線ネットワークのリストを含むことができる。リストは、選択された無線ネットワーク又はネットワーク装置を識別する２又はそれ以上の識別子を含むことができる。

【０１４０】

ステップ１２１２において、デジタル装置１００２が、無線ネットワーク選択のための信用証明書をサーバから受け取る。いくつかの実施形態では、信用証明書が、利用可能な無線ネットワークのリストをデジタル装置１００２から受け取ったサーバと同じサーバから受け取られる。

【０１４１】

様々な実施形態では、デジタル装置１００２が無線ネットワーク選択をサーバから受け取り、その後信用証明書要求を提供して所望のネットワークの信用証明書を受け取る。１つの例では、デジタル装置１００２が、利用可能な無線ネットワークのリストを提供する方法と同じ方法で（例えば、ネットワークのオープンポートを介して）信用証明書要求を提供する。いくつかの実施形態では、好ましいネットワークが信用証明書を必要とせず、又は信用証明書がデジタル装置１００２上にローカルに記憶される。

【０１４２】

ステップ１２１４において、デジタル装置１００２が信用証明書を使用して、選択された無線ネットワークにアクセスする。本明細書では、ログインページなどに信用証明書を適用する処理について説明する。

【０１４３】

様々な実施形態では、デジタル装置１００２が、本明細書で説明する信用証明書要求の提供と同様の方法で、利用可能な無線ネットワークのリストをネットワーク装置のオープンポートを介してサーバに提供することができる。他の実施形態では、デジタル装置１００２が、別のネットワークを介してサーバにリストを提供することができる。１つの例では、デジタル装置１００２が、利用可能なＷｉ－Ｆｉネットワークのリストを生成し、（ＥＶＤＯ又はＨＳＤＰＡネットワークなどの）携帯電話ネットワークを介してリストを提供する。この例では、無線ネットワーク選択を携帯電話ネットワークを介してデジタル装置へ戻し、その後デジタル装置１００２が、好ましいＷｉ－Ｆｉネットワークにアクセスしようと試みることができる。

【０１４４】

別の例では、デジタル装置１００２が１つの無線ネットワークにアクセスする。その後、デジタル装置１００２は、利用可能な無線ネットワークのリストをサーバに提供することができる。サーバは、無線ネットワーク選択をデジタル装置１００２へ戻すことができる。この好ましい無線ネットワークが、デジタル装置１００２が最初にアクセスしたネットワークでない場合、デジタル装置１００２は、接続を中断して好ましい無線ネットワークにアクセスすることができる。

【０１４５】

図１０～図１２は、利用可能な無線ネットワークのリストを受け取り、無線ネットワーク選択を決定し、この選択をデジタル装置１００２に提供するサーバを想定したものであるが、当業者であれば、サーバが必須ではないことを理解するであろう。１つの例では、デジタル装置１００２が、利用可能な無線ネットワークのリストを生成し、その後（例えば、ローカルに記憶されたネットワークプロファイルから、１又はそれ以上のネットワーク装置から、ローカルデータベース又は遠隔データベースから、及び／又はインターネットなどの別のネットワークから情報を取り出して）、リスト上のネットワークに関するいずれかの利用可能な情報を取り出す。次に、デジタル装置１００２は、選択を行うために、又は優先順位リストを生成するために、ネットワークに関連するどのような属性が利用可能であるかに基づいて比較を行うことができる。その後、デジタル装置１００２は、選択した無線ネットワークにアクセスすることができる。

【０１４６】

様々な実施形態では、デジタル装置１００２が、１又はそれ以上のネットワークに関する属性を生成して提供し、ネットワークプロファイルを更新することができる。１つの例では、デジタル装置１００２が、信号の品質、帯域幅、又はその他のあらゆる測定基準を判定して、利用可能な無線ネットワークのリストとともにこれらの測定基準をサーバに提供する。別の例では、デジタル装置１００２が、選択した無線ネットワークにアクセスし、属性を測定し、ネットワークプロファイル内に属性更新測定基準を提供する。デジタル装置１００２は、いつでも（待ち時間測定基準、帯域幅測定基準及びＱＯＳ測定基準などの）属性を取り込み、これらを使用してネットワークプロファイルを更新することができる。

【０１４７】

図１３は、無線ネットワークを選択し、選択した無線ネットワークにアクセスするための略図である。様々な実施形態では、ステップ１３０２及び１３０４において、ネットワーク装置１００４及びネットワーク装置１００６が、第１及び第２のネットワーク識別子をデジタル装置１００２に提供する。ステップ１３０６において、デジタル装置１００２が、ネットワーク装置１００４及びネットワーク装置１００６に関連する無線ネットワークに関する測定を行うことにより、測定基準（すなわち属性）を生成する。いくつかの例では、測定基準として、待ち時間、信号強度、又はＱＯＳ測定基準を挙げることができる。

【０１４８】

ステップ１３０８において、デジタル装置１００２が、ネットワーク装置１００４からのネットワーク識別子及びネットワーク装置１００６からのネットワーク識別子を含むことができる利用可能な無線ネットワークのリストを生成する。いくつかの実施形態では、デジタル装置１００２が、２つのネットワーク識別子間の優先度を示すこと、又はネットワーク識別子の一方又は両方を削除することができる個別設定を含むこともできる。１つの例では、個別設定が、（「ｌｉｎｋｓｙｓ」などの）デフォルトのメーカＳＳＩＤを有していないオープンネットワークにのみアクセスできることを示す。この例では、ネットワーク装置１００４からのネットワーク識別子がデフォルトのメーカＳＳＩＤを示す場合、デジタル装置１００２は、このネットワーク装置１００４のネットワーク識別子を利用可能な無線ネットワークのリスト内に含めることができない。

【０１４９】

いくつかの実施形態では、デジタル装置１００２が少なくとも２又はそれ以上のネットワークを識別するリストを生成できない場合、デジタル装置１００２はリストを送らない。１つの例では、デジタル装置１００２が、ユーザ要件を満たす利用可能な無線ネットワークを１つしか識別できない場合、デジタル装置１００２は、無線ネットワークに直接アクセスしようと試みるか、或いは信用証明書要求をサーバへ送信して、アクセスに必要ないずれかの信用証明書を取り出すことができる。

【０１５０】

ステップ１３１０において、デジタル装置１００２が、利用可能なネットワークの属性及びリストをルールサーバ１０１０に提供する際にプロキシのように振る舞うネットワーク装置１００６の（ポート５３などの）オープンポートを介して、属性及び利用可能な無線ネットワークのリストを提供する。他の実施形態では、デジタル装置１００２が、ネットワーク装置１００４のオープンポートを介して属性及びリストを提供する。或いは、デジタル装置１００２は、別個のネットワークを介して属性及びリストを（例えば、ネットワーク装置のうちの１つのオープンポートを介して属性を、及びセルラネットワークを介してリストを）提供することもできる。ステップ１３１２において、ＤＮＳを介して属性及びリストをルールサーバ１０１０に提供することにより、ネットワーク装置１００６がプロキシの役割を果たす。

【０１５１】

ステップ１３１４において、ルールサーバ１０１０がネットワークプロファイルを取り出す。１つの例では、ルールサーバ１０１０がリストからネットワーク識別子を取り出し、このネットワーク識別子に関連するネットワークプロファイルを取り出す。

【０１５２】

ステップ１３１６において、ルールサーバ１０１０（又はプロファイルサーバ１０１４）が、ネットワークプロファイル内の属性をデジタル装置１００２から受け取った属性に更新する。１つの例では、デジタル装置１００２からの新たな待ち時間測定基準を使用して、ネットワーク装置１００４からのネットワーク識別子に関連するネットワークプロファイルを更新する。新たな待ち時間測定基準が最近のものであることを示すために、属性に関連する有効期間値を更新することもできる。

【０１５３】

ステップ１３１８において、ルールサーバ１０１０が、ネットワークプロファイル内か

ら得た属性の比較に基づいてネットワーク装置を選択する。いくつかの実施形態では、ルールサーバ１０１０が、（ウェブサーバ１０１８などを介して）デジタル装置１００２から、又はデジタル装置１００２に関連するアカウントから得た個別設定も適用した後で選択を行う。ルールサーバ１０１０は、デジタル装置１００２により提供されたリストから、２つのネットワーク装置の優先順位リストを作成することができる。リストには、２つのネットワーク装置のうちのいずれの方がネットワークプロファイルからの測定基準に基づいて最も望ましいサービスを提供するかに基づいて優先順位が付けられる。

【０１５４】

ステップ１３２０において、ルールサーバ１０１０が、デジタル装置１００２へ情報を送るためのプロキシとして機能するために、ＤＮＳを介してネットワーク装置１００６へ無線ネットワーク選択及び信用証明書を提供する。１つの例では、ルールサーバ１０１０がネットワーク装置１００４を選択する。ルールサーバ１０１０は、ネットワーク装置１００４のネットワーク識別子に基づいてネットワーク装置１００４の信用証明書を取り出すことができる。例えば、ルールサーバ１０１０は、信用証明書サーバ１０１６に信用証明書要求を提供することができる。信用証明書サーバ１０１６は、必要な信用証明書を含む信用証明書要求応答をルールサーバ１０１０に提供することができ、その後このルールサーバ１０１０が、信用証明書サーバ１０１６から受け取った信用証明書及び無線ネットワーク選択をデジタル装置１００２へ送信する。

【０１５５】

その後、ステップ１３２２において、ネットワーク装置１００６が、オープンポートを介してネットワーク選択及び信用証明書をデジタル装置１００２に提供する。ステップ１３２４において、デジタル装置１００２が、信用証明書を提供してネットワーク装置１００４にアクセスし、ネットワークに関する追加の属性を生成する（すなわち追加測定を行う）。接続が確立されると、ステップ１３２６において、ルールサーバ１０１０又はプロファイルサーバ１０１４に新しい属性が提供されて、ネットワーク装置１００４に関連するネットワークプロファイルが更新される。１つの例では、デジタル装置１００２が、ネットワーク装置１００４との接続を確立するのに必要な時間を測定することができる。その後、この接続を確立するのに必要な時間を使用して、ネットワークプロファイル内の属性を更新することができる。接続が確立されなかったり、又は失敗した場合、この情報を提供して関連するネットワークプロファイルを更新することもできる。

【０１５６】

いくつかの実施形態では、選択したネットワークとのネットワーク接続が失敗した場合、デジタル装置１００２は接続を再試行することができる。接続をしようとする複数の試みが失敗した場合、この失敗に関する情報が送られて、関連するネットワークプロファイルが更新される。その後、デジタル装置１００２は、（ネットワーク装置１００６などの）別のネットワーク装置との接続を試みることができる。いくつかの実施形態では、デジタル装置１００２が領域を再走査して、利用可能なネットワークの新しいリストを生成し、このリストに、デジタル装置１００２が接続を失敗したネットワークを含めないようにすることができる。この新しいリストをルールサーバ１０１０へ送って新しい無線ネットワーク選択を受け取り、この処理を繰り返すことができる。

【０１５７】

いくつかの実施形態では、ルールサーバ１０１０が、優先度によりソートされた利用可能な無線ネットワークの優先順位リストを提供する。１つの例では、ルールサーバ１０１０が、３つのネットワークの優先順位リストをデジタル装置１００２に提供する。その後、デジタル装置１００２は、この優先順位リストに基づいて第１の無線ネットワークにアクセスしようと試みることができる。デジタル装置１００２は、第１の無線ネットワークに接続できなかった場合、リスト上の次のネットワークへの接続を試行することができる。当業者であれば、この優先順位リストが、利用可能な無線ネットワークのリスト内で識別された無線ネットワークの全て、１つ、又はいくつかを含むことができると理解するであろう。例えば、ルールサーバ１０１０は、性能が劣ると分かっていたり、（ＶｏＩＰサ

ービスなどの）所望のサービスを提供しなかったり、及び／又は別様にブラックリストに載っている無線ネットワークを識別することはできない。

【０１５８】

様々な実施形態では、デジタル装置１００２のユーザが、無線ネットワーク選択を無効にしていずれかの無線ネットワークにアクセスすることができる。１つの例では、ユーザが、利用可能な無線ネットワークの優先順位を選択する。いくつかの実施形態では、ユーザが、デジタル装置１００２、又はウェブサーバ１０１８とのアカウントを、ルールサーバ１０１０から得た無線ネットワークの優先順位リストを並べ替え、又は別様に変更することができる個人的な優先度を含むように構成することができる。例えば、利用可能な無線ネットワークのリストをルールサーバ１０１０に提供する前に、デジタル装置１００２又はウェブサーバ１０１８が、このリストをユーザの優先度に基づいて変更することができる。

【０１５９】

いくつかの実施形態では、１又はそれ以上のオープンなＷｉ－Ｆｉネットワークに加え、所定の位置に１又はそれ以上の暗号化されたＷｉ－Ｆｉネットワークが存在することもある。デジタル装置１００２は、オープンなＷｉ－Ｆｉネットワークに接続して、暗号化されたＷｉ－Ｆｉネットワークを含む他のＷｉ－ＦｉネットワークのＳＳＩＤをＨＴＴＰなどのネットワーク通信プロトコルを介してルールサーバ１０１０へ送信することができる。

【０１６０】

その後、ルールサーバ１０１０は、個別設定又はその他のルールに基づいて、利用可能な暗号化されたＷｉ－Ｆｉネットワークがネットワーク接続にとって好ましい選択であると判定することができる。ルールサーバ１０１０は、現在のオープンなＷｉ－Ｆｉネットワーク接続を介してデジタル装置１００２へ必要な暗号鍵を送信するとともに、暗号化されたＷｉ－Ｆｉネットワークに切り替えるための命令をデジタル装置１００２へ送ることができる。

【０１６１】

ユーザ、アプリケーション、及びオペレーティングシステムは、たとえＧＰＳハードウェアが利用できず又は機能しない（例えば、衛星が視認できない）としても、位置情報を所望又は要求する。いくつかの実施形態では、ＧＰＳハードウェアに代わる方法として、ユーザ、アプリケーション、及びオペレーティングシステムが、デジタル装置の近くに位置するネットワークの存在に基づいて位置情報を検索することができる。この位置情報を、アシスト型ＧＰＳ（すなわち、ＡＧＰＳ）として使用することを含むあらゆる数の方法で使用することができる。例えば、位置情報を使用して、速度及び／又は精度を向上させるようにＧＰＳハードウェアを「準備する」ことができる。

【０１６２】

ネットワークの位置は、ほとんど安定する傾向にある。従って、（ルータ、ホットスポット又はその他のネットワーク装置などの）ネットワークの物理的位置の場所を識別して使用し、ユーザの位置を識別することができる。１つの例では、デジタル装置を有するユーザが、無線ネットワークを求めて領域を走査することができる。１又はそれ以上の無線ネットワークを識別することができる。この識別された（単複の）無線ネットワークに関する情報を、識別された（単複の）無線ネットワークの位置（ＧＰＳ座標など）を識別するデータ構造（表又はデータベースなど）を有することができるサーバに提供することができる。サーバは、この位置をユーザのデジタル装置に提供することができる。その後、デジタル装置は、この情報を表示することができ、及び／又は（地図アプリケーションなどの）１又はそれ以上のアプリケーション又はデジタル装置のオペレーティングシステムにこの情報を提供することができる。

【０１６３】

図１４は、例示的なデジタル装置１０２のブロック図である。デジタル装置１０２は、コントローラ１４０２、走査モジュール１４０４、ＤＮＳモジュール１４０６、位置モジ

ュール１４０６、及びウェブモジュール１４１０を備えることができる。いくつかの実施形態では、デジタル装置１０２上に、位置情報を特定するための（クライアントなどの）アプリケーションがインストールされる。このアプリケーションは、図１４に示すモジュールの１又はそれ以上を含むことができる。例えば、このアプリケーションは、識別された無線ネットワークと、位置応答から位置情報を取り出すための位置モジュール１４０８とに基づいて位置要求を生成して送信するＤＮＳモジュール１４０６を含むことができる。

【０１６４】

コントローラ１４０２は、走査モジュール１４０４、ＤＮＳモジュール１４０６、位置モジュール１４０６、及び／又はウェブモジュール１４１０を制御するように構成することができる。１つの例では、コントローラ１４０２が、走査モジュール１４０２による走査を引き起こし、ＤＮＳモジュール１４０６でＤＮＳプロトコルフォーマットの位置要求を生成し、位置要求を提供し、位置応答を受け取り、位置応答から位置情報を取り出すことができる。いくつかの実施形態では、コントローラ１４０２が、（応答を表示するような）ユーザ、デジタル装置１０２上のアプリケーション（図示せず）又はオペレーティングシステム（図示せず）に位置情報を提供することができる。

【０１６５】

様々な実施形態では、走査モジュール１４０２を、無線ネットワークを求めてデジタル装置１０２の近くの領域を走査するように構成することができる。当業者であれば、利用可能な無線ネットワークを求めて走査を行うことは、ネットワークアクセスのために利用できるネットワークを識別するためのかなり一般的な処理であることを理解するであろう。走査モジュール１４０２は、無線ネットワークを求めて領域を走査すると、１又はそれ以上の無線ネットワークを識別することができる。例えば、無線ネットワーク及び／又はネットワーク装置に関連する、ＳＳＩＤ及び／又はＢＳＳＩＤなどのネットワーク識別子のリストを検出することができる。リスト化される無線ネットワークの１又はそれ以上は、（パスワード、ユーザ名、パスコード又は記録を必要とするような）安全なものの場合もあれば、或いは安全でないものの場合もある。リストは、（１又はそれ以上などの）あらゆる数のネットワーク識別子を含むことができる。

【０１６６】

ＤＮＳモジュール１４０６は、走査されたネットワークの１又はそれ以上に基づいて位置要求を生成するように構成することができる。位置要求は、ネットワークを介して（サーバなどの）第２のデジタル装置へ送られる、位置情報を要求するためのメッセージである。位置要求は、あらゆる数の方法でフォーマットできるメッセージである。１つの例では、位置要求が、ＤＮＳプロトコルメッセージ（ＲＦＣ１８７６で定義されるようなＤＮＳ　ＬＯＣ記録としてフォーマットされるメッセージなど）としてフォーマットされる。位置要求は、ＵＤＰプロトコルでフォーマットすることもできる。１つの例では、位置要求に、（ＢＳＳＩＤなどの）走査したネットワーク識別子の１つを含めることができる。位置要求には、あらゆる数のネットワーク識別子を含めることができる。

【０１６７】

いくつかの実施形態では、この位置検索にＤＮＳを使用することにより、本明細書で説明する位置要求及び関連する位置応答を、インターネットを介して例外なく又はほぼ例外なくサポートできるコネクションレス型分散プロトコルを介して搬送することができる。位置要求及び位置応答は、標準フォーマットとすることができる。従って、デジタル装置１０２は、位置を検索するために、Ｗｉ－Ｆｉ層におけるオープンなホットスポット又はネットワーク装置を認証する必要はない。

【０１６８】

例えば、ネットワーク装置は、ネットワークへのアクセスを許可する前に、（ユーザ名、パスワード又はその他の情報などの）アクセス情報を必要とすることがある。しかしながら、ネットワーク装置は、アクセス情報を必要とせずにサービスを提供するために、（ポート５３などの）１又はそれ以上のオープンポートを含むこともできる。１つの例では

、ネットワーク装置が、ポート５３を通じてＤＮＳサービスを可能にすることができる。デジタル装置１０２は、本明細書で説明したようなＤＮＳプロトコルでフォーマットされた位置要求を生成し、アクセス情報を提供することなくネットワーク装置のオープンポートを介してネットワークに位置要求を提供することができる。その後、デジタル装置１０２は、位置情報を含む位置応答をオープンポートから受け取ることができる。

【０１６９】

位置要求は、以下に限定されるわけではないが、走査されたネットワークの１又はそれ以上の信号強度、（ライセンスキーなどの）ライセンス識別子、及びデジタル装置１０２の識別子などのあらゆる種類の情報を含むことができる。信号強度は、デジタル装置１０２によって検出された無線ネットワークに関連する信号の強度指標とすることができる。１つの例では、走査モジュール１４０４が領域を走査し、検出された無線ネットワークのリストを提供することができる。この無線ネットワークの１又はそれ以上は、デジタル装置１０２と無線ネットワークの１つとの潜在的接続の強度を示す関連信号強度指標を有することができる。いくつかの実施形態では、領域を所定の時間にわたって定期的に又は連続的に走査することにより、信号強度を求めることができる。検出された無線ネットワークに関連する信号の強度を平均化（例えば、幾何学的に平均化）し、又は統計的に測定して関連信号強度指標を作成することができる。

【０１７０】

ライセンス識別子は、デジタル装置１０２上のアプリケーション又はクライアントに関連する識別子とすることができる。様々な実施形態では、ユーザが、本明細書で説明した手段及び方法によってデジタル装置の位置を特定し、本明細書で説明したような信用証明書を検索し、又はあらゆる数の動作を行うアプリケーションをインストールする。このアプリケーションをライセンス識別子に関連付け、位置要求に含めて提供することができる。

【０１７１】

装置識別子は、装置を識別するために使用できるいずれの識別子であってもよい。いくつかの実施形態では、装置識別子が一意のものである。いくつかの例では、装置識別子が、ＭＡＣアドレス、シリアル番号、ＩＰアドレス、デジタル装置１０２にインストールされたソフトウェアのバージョン番号、ＩＰアドレス及び／又はその他のいずれかの識別子である。

【０１７２】

位置情報は、ネットワーク及び／又はネットワークに関連するネットワーク装置（アクセスポイントなど）の物理的位置を識別するいずれの情報であってもよい。１つの例では、位置情報が、緯度及び経度座標を含むことができる。位置情報は、（海面よりも上又は下などの）高度を含むこともできる。当業者であれば、位置情報は、ユーザ、デジタル装置、ネットワーク装置、アプリケーション、オペレーティングシステムなどに位置又は位置の近似を提供するために使用できるあらゆる情報を含むことができると理解するであろう。

【０１７３】

いくつかの実施形態では、ＤＮＳモジュール１４０６が、位置要求の中の１又はそれ以上のネットワーク識別子及び／又はその他の情報を符号化することができる。例えば、ＤＮＳモジュール１４０６は、位置要求の中の情報の一部又は全部を１６進符号化することができる。位置要求を暗号化することもできる。位置要求の全部又は一部をハッシュ化することもできる。例えば、ＤＮＳモジュール１４０６は、サービスの悪用を防ぐために、ＢＳＳＩＤを共用秘密値でハッシュ化して新たな名前を生成することができる。位置要求に装置識別子（ＵＵＩＤ）を追加することもできる。例えば、最終結果は以下のようになる。

＜ｕｕｉｄ＞＜ｂｓｓｉｄ　ｈａｓｈ＞．＜ｓｅｒｖｅｒ　ｄｏｍａｉｎ＞

【０１７４】

位置要求は、コントローラ１４０２又はＤＮＳモジュール１４０６によって提供するこ

とができる。いくつかの実施形態では、コントローラ１４０２又はＤＮＳモジュール１４０６が、ネットワークを介して位置要求を送信することができる。１つの例では、ＤＮＳモジュール１４０６が、ネットワーク装置を介して位置サーバにＤＮＳプロトコルフォーマットの位置要求を提供する。ＤＮＳモジュール１４０６は、ネットワーク装置のオープンポートを介して位置要求を提供することができる。オープンポートは、ポート５３とすることができる。この位置要求は、本明細書で説明した信用証明書要求を提供する方法と同様の方法でネットワーク装置を介して提供することができる。

【０１７５】

位置モジュール１４０８は、ネットワーク上から位置応答を受け取るように構成することができる。この位置応答を、位置要求に関連付けることができる。位置応答は、位置情報を含むことができる。いくつかの実施形態では、位置モジュール１４０８が、位置応答から位置情報を取り出す。いくつかの例では、位置モジュール１４０８が、位置の全部又は一部を（ユーザにＧＰＳ座標などを表示して）ユーザに、デジタル装置１０２上のアプリケーションに、デジタル装置１０２上のオペレーティングシステムに、又は別のデジタル装置に提供する。

【０１７６】

いくつかの実施形態では、位置モジュール１４０８が、位置応答から情報を復号及び／又は解読する。位置要求は、ＤＮＳプロトコル又はいずれかのプロトコルとしてフォーマットすることができる。いくつかの実施形態では、位置モジュール１４０８が、位置応答から位置情報を復号する。１つの例では、位置情報の全部又は一部を１６進符号化することができる。

【０１７７】

位置応答を、インターネットを介して受け取ることもできる。いくつかの実施形態では、位置モジュール１４０８が、（暗号鍵などで）位置応答の全部又は一部を解読し、及び／又は位置応答を認証する。その後、この認証に基づいて、位置モジュール１４０８が、位置応答から取り出した位置情報を提供することができる。

【０１７８】

ウェブモジュール１４１０は、位置要求を提供し、及び／又はインターネット又はその他のアクセス可能なネットワーク上から位置応答を受け取るように構成することができる。いくつかの実施形態では、ウェブモジュール１４１０が、ウェブブラウザとして機能することができる。ウェブモジュール１４１０は、ネットワーク識別子を含む位置要求を（ＨＴＴＰ、ＨＴＴＰＳ、又はＸＭＰＰなどを通じて）生成し、アクセスされたネットワークを介して別のデジタル装置に位置要求を提供することができる。ウェブモジュール１４１０は、（ＨＴＴＰ、ＨＴＴＰＳ、又はＸＭＰＰなどを通じて）位置応答を受け取り、位置情報を取り出すこともできる。

【０１７９】

当業者であれば、いくつかの実施形態は、無線ネットワークを求めて走査を行うことを想定するものであるが、有線ネットワークを使用してユーザの位置を特定することもできると理解するであろう。例えば、デジタル装置が（イーサネットケーブルなどを介して）有線ネットワークに結合されている場合、このデジタル装置は、ＩＰアドレス、ホスト名アドレスなどのネットワーク識別子を受け取ることができる。１つの例では、ネットワーク識別子が、アクセスを提供するネットワーク装置の識別子である。このネットワーク識別子を位置サーバに提供し、その後この位置サーバが、ネットワーク及び／又はアクセスを提供するネットワーク装置の物理的位置を提供することができる。いくつかの実施形態では、（ＨＴＴＰなどを介して）アクセスが確立されると、デジタル装置１０２が、ネットワークを介して位置要求を送信することができる。様々な実施形態では、デジタル装置１０２が、異なるネットワークを介して位置要求を送信することができる。１つの例では、デジタル装置１０２が、ＤＮＳプロトコルを通じ、無線ネットワークを介して位置要求を送信することができる。

【０１８０】

図１５は、ＤＮＳプロトコルフォーマットのメッセージを通じ、無線ネットワークを介して位置情報を受け取る例示的な方法のフロー図である。ステップ１５０２において、走査モジュール１４０４が、無線ネットワーク（ネットワークのＢＳＳＩＤ及び／又はＳＳＩＤをブロードキャストするネットワーク装置など）を求めて領域を走査する。例えば、走査モジュール１４０４は、オペレーティングシステム、別のアプリケーション、プラグイン、又はクライアントの一部とすることができる。ステップ１５０４において、走査モジュール１４０４が、走査を通じて無線ネットワークのネットワーク識別子を検出する。ネットワーク識別子は、例えばＢＳＳＩＤ及び／又はＳＳＩＤなどの、無線ネットワーク又はネットワーク装置を識別するいずれかの情報とすることができる。走査を通じて、あらゆる数の無線ネットワークに関連するあらゆる数のネットワーク識別子を受け取ることができる。

【０１８１】

ステップ１５０６において、ＤＮＳモジュール１４０６が、ＤＮＳプロトコル用にフォーマットされた位置要求を生成する。この位置要求は、ネットワーク識別子を含むことができる。いくつかの実施形態では、走査モジュール１４０４による走査により２以上のネットワーク識別子が見つかったとしても、位置要求は１つのネットワーク識別子しか含まない。他の実施形態では、位置要求が、走査モジュール１４０４による走査で見つかったネットワーク識別子の一部又は全部を含む。

【０１８２】

ステップ１５０８において、コントローラ１４０２又は走査モジュール１４０４が、ＤＮＳプロトコルを通じ、ネットワークを介してサーバなどのデジタル装置に位置要求を提供する。例えば、デジタル装置１００２は、ネットワーク装置のオープンポートを介して位置サーバに位置要求を提供することができる。位置要求を提供する処理は、本明細書で説明したようなネットワーク装置のオープンポートを介して（信用証明書要求などの）メッセージを提供する処理と同様のものとすることができる。オープンポートは、いずれのオープンポートであってもよい。１つの例では、オープンポートがポート５３である。

【０１８３】

ステップ１５１０において、位置モジュール１４０８が、位置要求を受け取ったデジタル装置から位置応答を受け取る。位置応答は、ネットワーク識別子により識別されるネットワーク又はネットワーク装置の近似位置を識別する位置情報を含むことができる。

【０１８４】

ステップ１５１２において、位置モジュール１４０８が、位置応答から位置情報を取り出す。位置モジュール１４０８は、この位置情報をユーザ、ハードウェア装置、又はソフトウェアプログラムに提供することができる。位置モジュール１５０８は、位置情報を復号することができる。

【０１８５】

いくつかの実施形態では、位置応答が、追加情報の要求を含むことができる。例えば、位置要求は、符号化されたＢＳＳＩＤなどの、無線ネットワークに関連するネットワーク識別子を含むことができる。位置要求を受け取るデジタル装置は、ネットワーク識別子に関する情報又は不十分な情報を有することができない。この結果、位置要求を受け取ったデジタル装置は、追加情報の要求を含む位置応答を提供することができる。その後、ＤＮＳモジュール１４０４は、前の位置要求とは異なる１又はそれ以上のネットワーク識別子を含む新たな位置要求を生成することができる。その後、この新たな位置要求を提供して、位置を特定できるかどうかを判定することができる。この処理は、例えば、位置が識別されるまで、走査モジュール１４０４によって走査されたネットワーク識別子が、全て１又はそれ以上の位置要求に含まれるまで、所定の時間が経過するまで、及び／又は位置を識別するための試行が所定の回数に達するまで継続することができる。

【０１８６】

当業者であれば、いつ何時でも位置要求を生成及び／又は送信できることを理解するであろう。例えば、ユーザが、ＧＰＳ装置を有していないデジタルカメラで撮った写真にタ

グを付けたいと望むことがある。ユーザは、無線ネットワーク識別子を求めて領域を走査することもできるデジタルカメラで写真を撮ることもある。走査した無線ネットワーク識別子に写真の１又はそれ以上を関連付けることができる。デジタルカメラが（例えば無線で、又は有線ネットワークを介して）ネットワークに接続されている場合、ＤＮＳモジュール１４０４又はウェブモジュール１４０８は、位置要求を生成することができる。位置要求は、走査したネットワーク識別子の１又はそれ以上を含むことができる。次に、コントローラ１４０２が、受け取った位置応答から受け取った位置情報に基づいて、個々の写真に適宜タグを付けることができる。いくつかの実施形態では、写真に関連する１又はそれ以上のネットワーク識別子を含む個別の位置要求が写真ごとに存在してもよい。他の実施形態では、複数の写真の位置要求が存在してもよい。タグを付けた位置情報を写真に関連付ける方法はいくつも存在し、以下に限定されるわけではないが、写真をプリントする際に位置情報をプリントしたり、又は写真に関連するメタデータ内に位置情報を表示したりすることができる。

【０１８７】

図１６は、例示的な位置サーバ１６０２のブロック図である。位置サーバ１６０２は、限定するわけではないが、信用証明書サーバ１１６（図１を参照）を含むいずれかのデジタル装置とすることができる。位置サーバ１６０２は、異なるネットワーク識別子に関連する位置情報を収集し、及び／又は位置要求に基づいてデジタル装置に位置情報を提供するように構成することができる。位置サーバ１６０２は、ＤＮＳ位置モジュール１６０４、ウェブモジュール１６０６、位置分析モジュール１６０８、及び位置データベース１６１０を含むことができる。

【０１８８】

ＤＮＳ位置モジュール１６０４は、位置要求を受け取るように構成することができる。１つの例では、ＤＮＳ位置モジュール１６０４が、デジタル装置１０２から位置要求を受け取る。ＤＮＳ位置モジュール１６０４は、１又はそれ以上のネットワーク識別子、位置要求を送信したデジタル装置、バージョン識別子、又はその他のいずれかの情報を位置要求から取り出すことができる。ＤＮＳ位置モジュール１６０４を、位置要求から情報を復号する（例えば、１６進符号化された情報を復号する）ように構成することもできる。１つの例では、ＤＮＳ位置モジュール１６０４が、ハッシュ化されたネットワーク識別子を共有鍵で復号する。いくつかの実施形態では、ＤＮＳ位置モジュール１６０４が、位置要求を認証及び／又は解読することができる。

【０１８９】

いくつかの実施形態では、ＤＮＳ位置モジュール１６０４が、１又はそれ以上のデジタル装置から位置識別メッセージを受け取ることもできる。例えば、１又はそれ以上のデジタル装置は、ＧＰＳ装置を有することができ、又はデジタル装置の近似位置を知ることができる。デジタル装置は、領域を走査してネットワーク識別子を検出し、検出したネットワーク識別子及び（ＧＰＳ装置又は位置サーバ１６０２などからの）いずれかの位置情報を位置サーバ１６０２へ送信することができる。

【０１９０】

位置識別メッセージは、１又はそれ以上のネットワーク識別子を含むことができる。位置識別メッセージは、位置識別メッセージ及び／又はネットワーク識別子の１又はそれ以上を送信するデジタル装置に関連付けることができる位置情報を含むこともできる。いくつかの実施形態では、ＤＮＳ位置モジュール１６０４又は位置分析モジュール１６０８が、位置情報をネットワーク識別子の１又はそれ以上に関連付け、この関連性を位置データベース１６１０に記憶することができる。様々な実施形態では、ＤＮＳ位置モジュール１６０４又は位置分析モジュール１６０８が、位置情報及び／又はネットワーク識別子の全部又は一部を位置データベース１６１０に記憶することができる。

【０１９１】

ウェブモジュール１６０６は、（ＨＴＴＰ又はＨＴＴＰＳなどを介して）位置要求を受け取るように構成することもできる。いくつかの実施形態では、位置サーバ１６０２がウ

ェブサーバである。１つの例では、ＤＮＳ位置モジュール１６０４と同様に、ウェブモジュール１６０６も、デジタル装置１０２から位置要求を受け取る。ウェブモジュール１６０６は、１又はそれ以上のネットワーク識別子、位置要求を送信したデジタル装置、バージョン識別子、又はその他のいずれかの情報を位置要求から取り出すことができる。ウェブモジュール１６０６は、位置要求からの情報を復号するように構成することができる。いくつかの実施形態では、ウェブモジュール１６０６が、位置要求を認証及び／又は解読することができる。

【０１９２】

いくつかの実施形態では、ウェブモジュール１６０６も、ＤＮＳ位置モジュール１６０４の場合と同様の方法で１又はそれ以上のデジタル装置から位置識別メッセージを受け取ることができる。

【０１９３】

位置分析モジュール１６０８は、利用可能な位置情報に基づいて、ネットワーク装置の位置又は近似位置を特定して記憶するように構成することができる。様々な実施形態では、位置分析モジュール１６０８が、デジタル装置から（例えば、ネットワーク収集メッセージから）ネットワーク識別子及び位置情報を受け取る。ネットワーク識別子は、ネットワーク装置を識別することができる。位置情報は、検出されたネットワーク装置を走査したスマートフォンなどのデジタル装置の位置を識別することができる。位置分析モジュール１６０８は、（デジタル装置のＧＰＳ座標などの）位置情報をネットワーク識別子に関連付け、この関連性を位置データベース１６１０に記憶することができる。

【０１９４】

位置情報は、座標に加え、座標の信頼度又信頼レベルを含むことができる。例えば、多くの異なる種類のＧＰＳハードウェアが、緯度座標、経度座標、及び信頼度を識別する。信頼度は、生じ得る誤差を示す範囲とすることができる。例えば、特定の座標の組の信頼度（精度又は誤差範囲など）を、＋／－２０フィートとすることができる。換言すれば、ＧＰＳハードウェアは、特定の座標の組から２０フィート以内に位置すると考えることができる。この信頼度を、関連する座標とともに位置データベース１６１０に記憶することができる。

【０１９５】

様々な実施形態では、位置分析モジュール１６０８が、所定の時間後に、及び／又は特定のネットワーク識別子を識別する所定の数のネットワーク識別メッセージを受け取った後にネットワーク装置の位置を特定する。例えば、位置分析モジュール１６０８は、ネットワーク装置を識別する設定数のメッセージ及び位置情報を受け取った（例えば、ネットワーク装置に関するいくつかのネットワーク収集メッセージを受け取った）後にしかネットワーク装置の位置を特定することができない。当業者であれば、単一のネットワーク収集メッセージでは、誤った位置情報が含まていれる可能性があることを理解するであろう。いくつかの異なるデジタル装置が同じネットワーク識別子を検出して位置情報を提供するので、ネットワーク識別子の位置の信頼性が高まると考えられる。従って、例えば、位置分析モジュール１６０８は、同じネットワーク識別子を含む１０個の位置識別メッセージを受け取った後に、このネットワーク識別子に関連するネットワークの位置を特定することができる。

【０１９６】

位置分析モジュール１６０８は、位置に関する全体的信頼度を判定することもできる。１つの例では、位置分析モジュール１６０８が、位置を特定するために使用した位置情報に関連する利用可能な信頼度を統計的に測定し、重み付けし、及び／又は平均化することができる。全体的信頼度は、デジタル装置１０２に提供できる位置の誤差範囲を示すことができる。いくつかの実施形態では、位置応答が、位置情報及び全体的信頼度を含む。

【０１９７】

いくつかの実施形態では、位置分析モジュール１６０８が、ネットワーク識別子に関連する位置情報（例えば、所定の時間にわたって受け取られた位置情報、又は位置サーバ１

６０２及び／又はその他のデジタル装置によって受け取られた全てのネットワーク識別メッセージ）を取り出すことにより、このネットワークの位置を特定する。その後、位置分析モジュール１６０８は、（ネットワーク装置を検出した全てのデジタル装置のＧＰＳ座標を平均化することなどの）いずれかの統計的手段を通じて、ネットワーク装置の位置を特定することができる。

【０１９８】

いくつかの実施形態では、位置分析モジュール１６０８が、ＧＰＳ座標の１又はそれ以上に関する信頼度を取り出し、この情報を使用してネットワーク装置の位置を特定する。例えば、統計処理では、位置分析モジュール１６０８が、信頼度に少なくとも部分的に基づいてＧＰＳ座標に重み付けすることができる。１つの例では、位置分析モジュールが、（＋／－５フィートの信頼度などの）誤差範囲の低いＧＰＳ座標に高く重み付けすることができる。同様に、位置分析モジュールは、（＋／－５００フィートの信頼度などの）誤差範囲の高いＧＰＳ座標の衝突を低減又は除去することができる。当業者であれば、信頼度に部分的に基づいてあらゆる数の方法でＧＰＳ座標に重み付けできることを理解するであろう。

【０１９９】

いくつかの実施形態では、位置分析モジュール１６０８が、データを閾値化する。例えば、位置分析モジュール１６０８は、位置を特定する前に（ＧＰＳ座標の大部分が集まっているのに対し、１つ又は２つのＧＰＳ座標がこの集まりから何マイルも離れて位置するような）異常値を除去することができる。さらに、位置分析モジュール１６０８は、信頼性の欠如を示唆する位置情報を除去することができる。例えば、位置分析モジュール１６０８は、検出中のデジタル装置が移動中であったこと、又は他の位置情報に対して高高度にあったことを示す位置情報を除去することができる。同様に、位置分析モジュール１６０８は、ＧＰＳ座標の誤差範囲が広すぎることを示す位置情報も除去することができる。

【０２００】

当業者であれば、位置分析モジュール１６０８が、所定の時間後、所定数のネットワーク識別メッセージを受け取った後、又はネットワークが移動した可能性があることを示唆するいくつかのネットワーク識別メッセージを受け取った後に位置を特定し直すことによってネットワーク識別子の位置を定期的に確認できることを理解するであろう。例えば、会社が閉鎖して物的資産を売却することは珍しくない。この結果、ネットワーク装置が売却され、異なる位置で使用されている可能性がある。１つの例では、位置分析モジュール１６０８が、あるネットワーク識別子に関してすでに収集した位置情報と異なる位置情報を有するネットワーク識別子を含むいくつかのネットワーク識別メッセージを受け取ることができる。所定の時間後、又は所定数のネットワーク識別メッセージを受け取った後に、位置分析モジュール１６０８は、新たな情報に基づいてネットワーク識別子の位置を特定し、以前に記憶した位置と新たに特定した位置を比較することができる。これらの位置が大幅に異なる場合、位置分析モジュール１６０８は、位置データベース１６１０を新たな位置で更新し、又はさらなる情報を受け取るのを待ってから変更を行うことができる。

【０２０１】

位置分析モジュール１６０８は、信号強度又はＧＰＳ位置の品質に基づいてネットワーク識別子の位置に重み付けすることもできる。いくつかの実施形態では、位置情報が、ネットワーク識別子の信号強度及び／又は（ネットワーク識別子を走査したデジタル装置から２０メートル以内などの）ＧＰＳ位置の信頼度の指標を含む。このＧＰＳ位置の信号強度及び／又は信頼度を、あらゆる数の関連するネットワーク識別メッセージを介して位置を特定する上での因子とすることができる。

【０２０２】

位置データベース１６１０は、複数のネットワーク識別子及び関連する位置（位置情報など）を含むいずれかのデータ構造（表など）である。位置データベース１６１０は、位置識別メッセージ、デジタル装置識別子、ライセンス識別子などを記憶することもできる。

【０２０３】
図１７は、ＤＮＳプロトコルフォーマットのメッセージを通じ、無線ネットワークを介して位置情報を提供する例示的な方法のフロー図である。ステップ１７０２において、ＤＮＳ位置モジュール１６０４が、ＤＮＳプロトコル用にフォーマットされた位置要求を受け取る。位置要求は、（ＢＳＳＩＤ又はＳＳＩＤなどの）１又はそれ以上のネットワーク識別子を含むことができる。次にＤＮＳ位置モジュール１６０４は、ステップ１７０４において、位置要求から（単複の）ネットワーク識別子を取り出すことができる。
【０２０４】
ステップ１７０６において、位置分析モジュール１６０８が、位置データベース１６１０から（単複の）ネットワーク識別子に関連する位置情報を取り出すことができる。この（単複の）ネットワーク識別子に関連する位置情報が存在しない場合、位置分析モジュール１６０８は、位置要求を提供したデジタル装置に追加情報を要求することができる。
【０２０５】
ステップ１７０８において、ＤＮＳ位置モジュール１６０４が、位置情報を含む位置応答をＤＮＳプロトコルでフォーマットすることができる。当業者であれば、いくつかの実施形態では、ウェブモジュール１６０６がＨＴＴＰフォーマットのメッセージとして位置応答を受け取ることができると理解するであろう。ウェブモジュール１６０６は、ＨＴＴＰフォーマットのメッセージとして位置応答を提供することもできる。
【０２０６】
ステップ１７１０において、位置要求を提供したデジタル装置に位置応答を提供する。様々な実施形態では、位置サーバ１６０２が、位置要求と同じ形で位置応答を戻す。例えば、位置要求がＤＮＳプロトコルでフォーマットされていた場合、位置応答もＤＮＳプロトコルフォーマットのメッセージとして戻される。
【０２０７】
いくつかの実施形態では、デジタル装置１０２が、複数の異なるネットワークの位置情報を含む位置応答を位置サーバ１６０２から受け取ることができる。例えば、デジタル装置１０２による領域の走査が、３つの異なるＢＳＳＩＤを含むことがある。この３つのＢＳＳＩＤを（ＨＴＴＰなどを介して）位置要求に含め、デジタル装置１０２は、この３つのＢＳＳＩＤの全ての位置情報を含む位置応答を受け取ることができる。様々な実施形態では、デジタル装置１０２が、３つのＢＳＳＩＤのうちの１つの位置情報を選択し、位置情報を平均化し、或いはＢＳＳＩＤの各々の信号強度に基づいてデジタル装置１０２の位置を三角測量することができる。当業者であれば、あらゆる数の方法でデジタル装置１０２の位置を特定できることを理解するであろう。
【０２０８】
様々な実施形態では、デジタル装置１０２が、１つの位置要求、又は複数のネットワーク識別子を含む複数の位置要求を提供することができる。位置サーバ１６０２は、この（単複の）位置要求からネットワーク識別子を取り出し、ネットワーク識別子の２又はそれ以上に関連する位置情報を識別して、デジタル装置１０２の位置を三角測量することができる。この三角測量は、位置サーバ１６０２が記憶する位置情報の信頼度に部分的に基づくことができる。その後、位置サーバ１６０２は、三角測量した情報を含む位置応答をデジタル装置１０２に戻すことができる。
【０２０９】
図１８は、ネットワークを介して位置情報を収集する例示的な方法のフロー図である。ステップ１８０２において、ＤＮＳ位置モジュール１６０４が、無線ネットワークに関する（１又はそれ以上のネットワーク識別子などに関連する）複数のネットワーク収集メッセージを受け取る。
【０２１０】
ステップ１８０４において、ＤＮＳ位置モジュール１６０４が、この複数のネットワーク収集メッセージから位置識別子を取り出す。この複数のネットワーク収集メッセージからのネットワーク識別子及び位置情報などの情報を、位置データベース１６１０に記憶す

ることができる。

【０２１１】

ステップ１８０６において、位置分析モジュール１６０８が、位置データベース１６１０に記憶された位置情報に少なくとも部分的に基づいてネットワーク識別子の位置を特定する。位置は、ＧＰＳ座標、高度、又はその他のいずれかの特定を含むことができる。位置は、信頼基準を含むこともできる（例えば、この信頼基準は、位置が近似であり、２０メートル以内に存在し得ることを示すことができる。）

【０２１２】

いくつかの実施形態では、位置分析モジュール１６０８が、ネットワーク識別子に関連する位置情報を統計的に分析することによってネットワークの位置を特定する。例えば、特定のネットワーク識別子に関連する位置情報を含むあらゆる数のネットワーク収集メッセージが時間とともに受け取られると考えられる。位置分析モジュール１６０８は、所定の時間後、及び／又はそのネットワーク識別子に関する所定数のメッセージを受け取った後に、ネットワークの位置を特定することができる。１つの例では、位置分析モジュール１６０８が、あらゆる異常値を除去した後に、複数の異なるネットワーク収集メッセージからの位置情報を平均化することにより、ネットワークの近似位置を特定する。その後、結果として得られる位置をネットワークのネットワーク識別子に関連付け、位置データベース１６１０に記憶することができる。

【０２１３】

上述の機能及び構成要素は、コンピュータ可読媒体などの記憶媒体上に記憶された命令で構成することができる。この命令をプロセッサが取り出して実行することができる。命令のいくつかの例として、ソフトウェア、プログラムコード及びファームウェアがある。記憶媒体のいくつかの例としては、記憶装置、テープ、ディスク、集積回路及びサーバがある。この命令は、プロセッサにより実行された場合、プロセッサが本発明の実施形態に従って動作するように導く。当業者は、命令、（単複の）プロセッサ及び記憶媒体に精通している。

【０２１４】

以上、例示的な実施形態を参照しながら本発明について説明した。当業者には、本発明のより広い範囲から逸脱することなく、様々な修正を行うとともに他の実施形態を使用できることが明らかであろう。従って、例示的な実施形態に対するこれらの及びその他の変形も本発明に含まれることが意図されている。

【符号の説明】

【０２１５】

１００２：デジタル装置
１００４：ネットワーク装置
１００６：ネットワーク装置
１００８：通信ネットワーク
１０１０：ルールサーバ
１０１２：ネットワークデータベース
１０１４：プロファイルサーバ
１０１６：信用証明書サーバ
１０１８：ウェブサーバ

【図１】

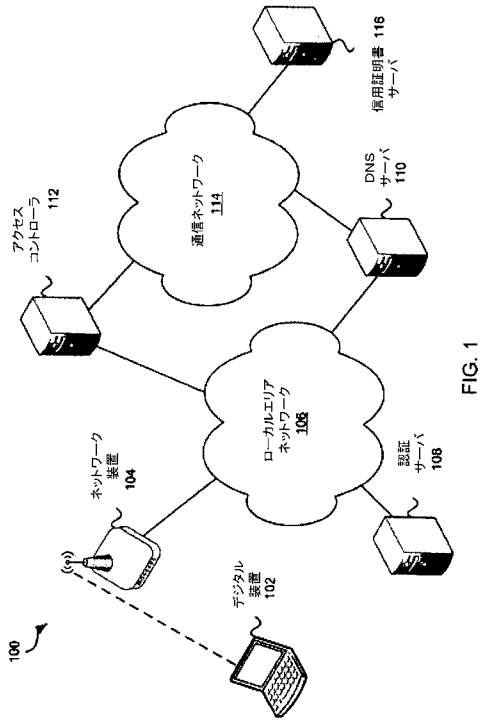

FIG. 1

【図２】

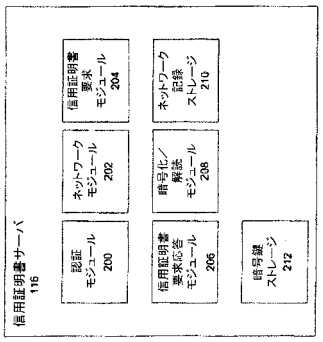

FIG. 2

【図３】

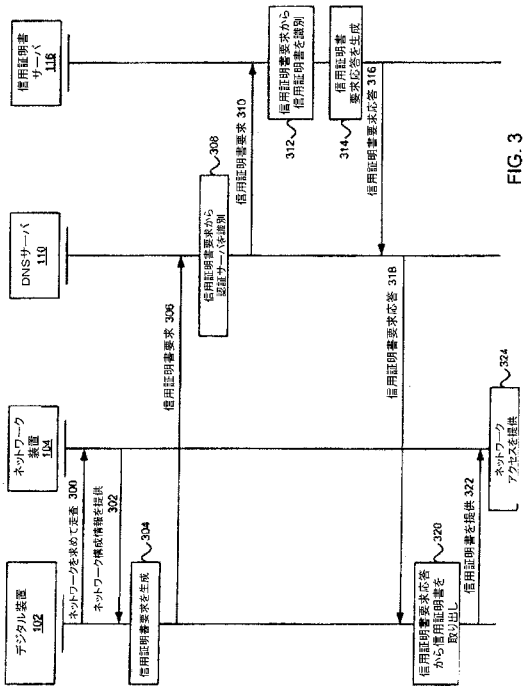

FIG. 3

【図４】

FIG. 4

【図５】

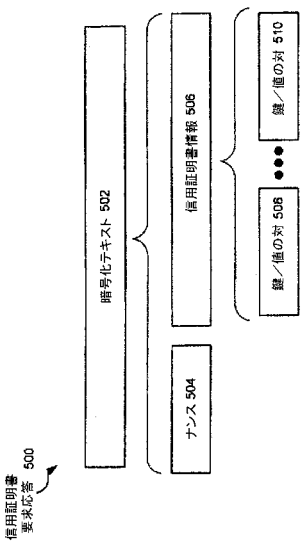

FIG. 5

【図６】

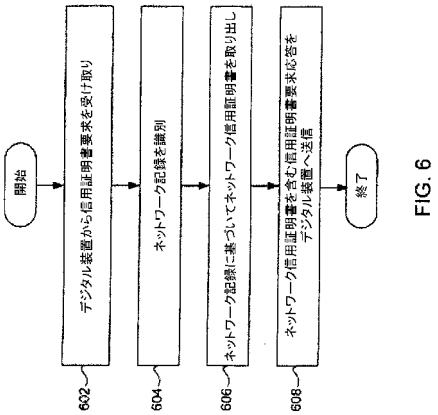

FIG. 6

【図７】

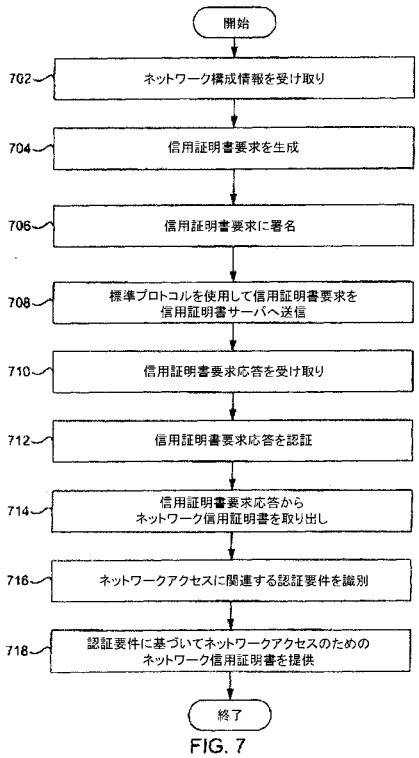

FIG. 7

【図８】

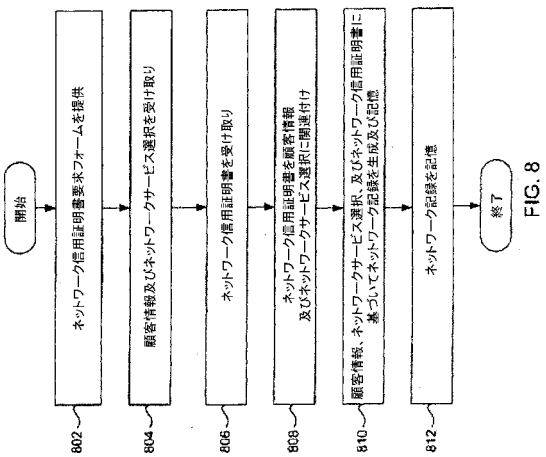

FIG. 8

【図９】

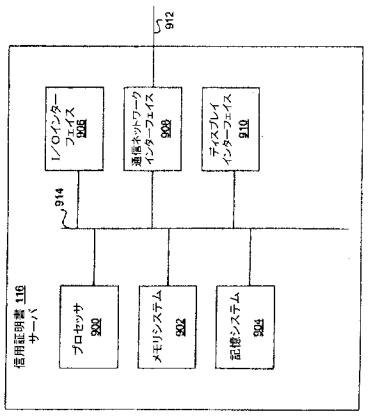

FIG. 9

【図１０】

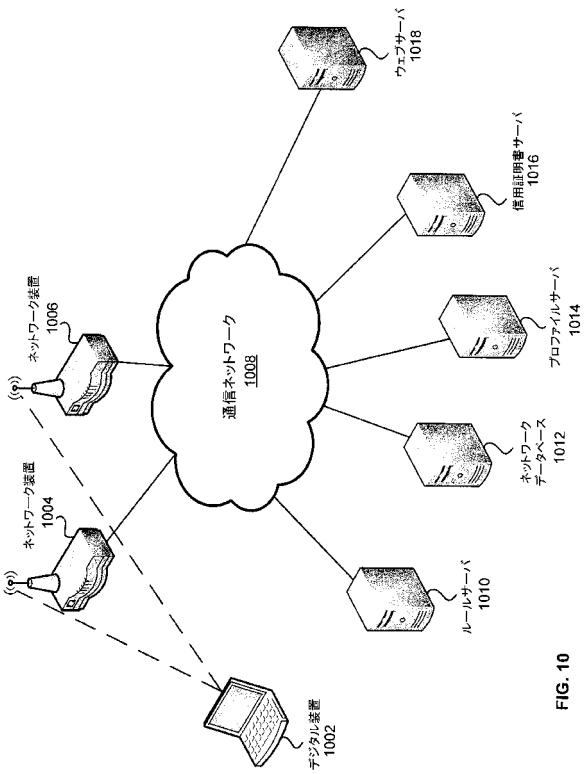

FIG. 10

【図１１】

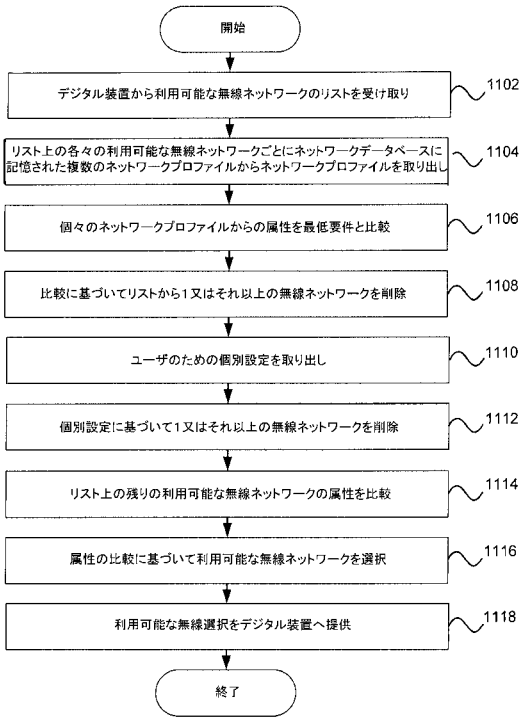

FIG. 11

【図１２】

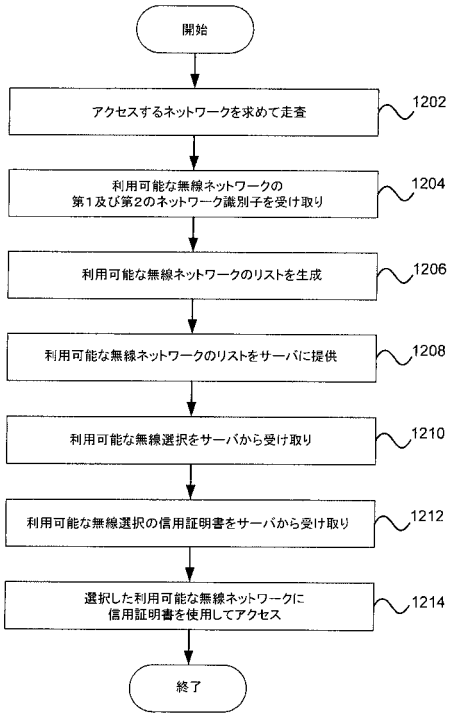

FIG. 12

【図１３】

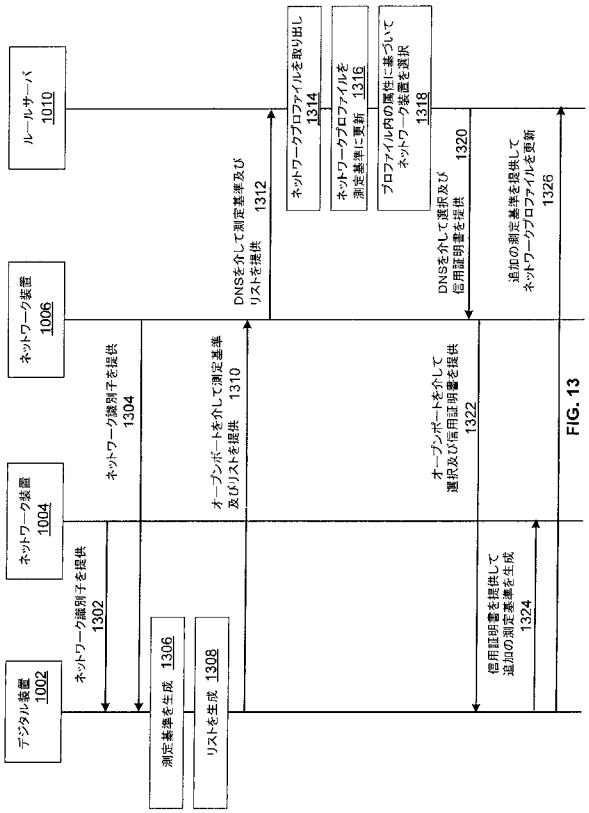

FIG. 13

【図１４】

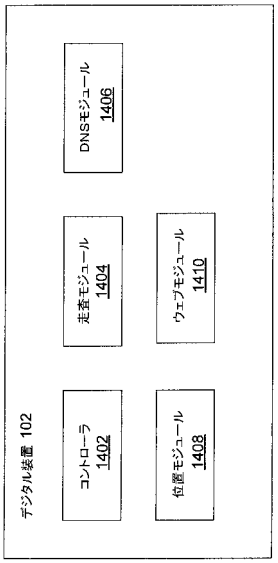

FIG. 14

【図１５】

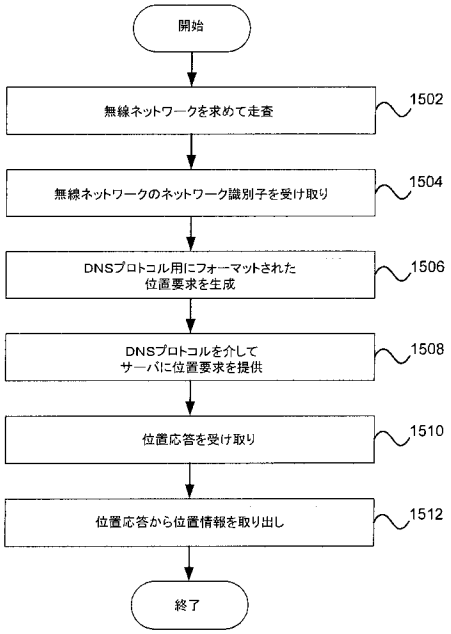

FIG. 15

【図１６】

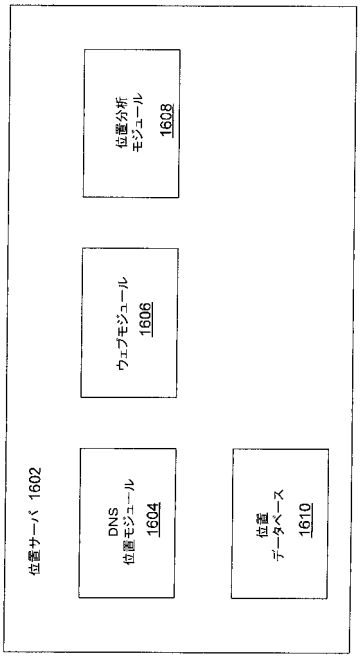

FIG. 16

【図１７】

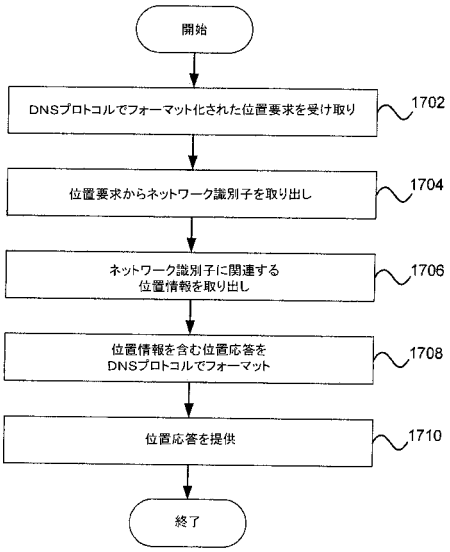

FIG. 17

【図１８】

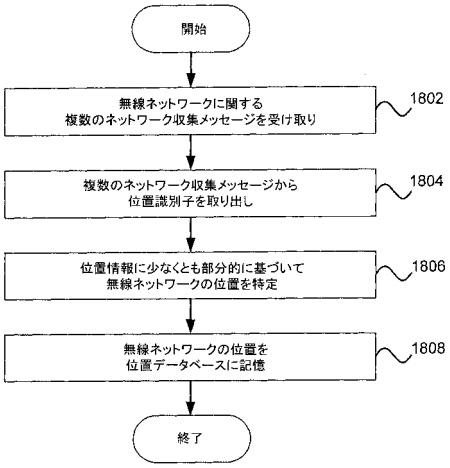

FIG. 18

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 10/39092

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 15/173 (2010.01)
USPC - 709/223
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC: 709/223

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 709/223-224; 701/207, 213 (keyword limited - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST (PGPB, USPT, USOC, EPAB, JPAB); GOOGLE WEB
Search Terms: DNS, wireless, network, BSS, BSSID, identifier, MAC, address, Basic Service Set, message, GPS, scanning, port, port 53, locating

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2006/0187858 A1 (Kenichi et al.) 24 August 2006 (24.08.2006), entire document, especially; abstract, para. [0007], [0097], [0105], [0119], [0139], [0190], [0194], [0242], [0308], [0542]	1 - 20
Y	US 2006/0215622 A1 (Abdel-Kader et al.) 28 September 2006 (28.09.2006), entire document, especially; abstract, para. [0036], [0042], [0044]	1 - 20

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 July 2010 (23.07.2010)	11 AUG 2010
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

フロントページの続き

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

(72)発明者 ゴードン, ジョン
アメリカ合衆国・９４５０１・カリフォルニア州・アラメダ・リナ アヴェニュ・３３１
(72)発明者 キムドン, デイヴィッド, ホィードン
アメリカ合衆国・９４０６６・サン ブルーノ・ベイヒル ドライブ・１００１・スイート・１８５

Ｆターム(参考) 5K067 AA21 BB21 DD19 DD20 EE02 EE10 EE16 JJ53 JJ56