【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成24年1月19日(2012.1.19)

【公開番号】特開2006-107453(P2006-107453A)
【公開日】平成18年4月20日(2006.4.20)
【年通号数】公開・登録公報2006-016
【出願番号】特願2005-223307(P2005-223307)
【国際特許分類】
Ｇ０６Ｆ　21/20　(2006.01)
Ｈ０４Ｌ　12/66　(2006.01)
Ｈ０４Ｌ　12/56　(2006.01)
Ｈ０４Ｗ　24/00　(2009.01)
Ｈ０４Ｗ　84/12　(2009.01)
【ＦＩ】
Ｇ０６Ｆ　15/00　３３０Ａ
Ｈ０４Ｌ　12/66　Ｂ
Ｈ０４Ｌ　12/56　４００Ｚ
Ｈ０４Ｌ　12/28　３００Ｍ

【誤訳訂正書】
【提出日】平成23年11月29日(2011.11.29)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【特許請求の範囲】
【請求項１】
安全なネットワークアクセスを提供するためのコンピュータに実装された方法であって、
安全ネットワークプロビジョニングデバイスを、ワイヤレスネットワークからリモートネットワークへのゲートウェイとして働くコンピュータに接続することと、
前記安全ネットワークプロビジョニングデバイスが通信できるネットワークのタイプに関する情報に基づいて、前記コンピュータにおいて既知のネットワークプロファイルのリストをグラフィカルユーザインターフェースで提示することと、
前記コンピュータから、前記グラフィカルユーザインラーフェースを介して選択または作成された少なくとも１つのネットワークプロファイルを獲得することと、
前記少なくとも１つのネットワークプロファイルを解析して、前記安全ネットワークプロビジョニングデバイスの少なくとも１つのネットワークインターフェースに関連する構成ブロックを作成することと、
前記安全ネットワークプロビジョニングデバイスを獲得モードからゲートウェイモードに切り換えることと、
前記安全ネットワークプロビジョニングデバイスを、前記ワイヤレスネットワークに関連するワイヤレスネットワークポイントと通信するクライアントデバイスに接続することと、
前記少なくとも１つのネットワークプロファイルのそれぞれにつき、前記ネットワークプロファイルに関連する安全ネットワークへのアクセスを前記クライアントデバイスに提供することと
を備えることを特徴とする方法。

【請求項２】
リセットコマンドに応答して、
前記少なくとも１つのネットワークプロファイルを前記安全ネットワークプロビジョニングデバイスから消去することと、
前記安全ネットワークプロビジョニングデバイスを前記ゲートウェイモードから前記獲得モードに切り換えることと
をさらに備えることを特徴とする請求項１に記載の方法。
【請求項３】
前記少なくとも１つのネットワークインターフェースの少なくとも１つは、ワイヤレスネットワークインターフェースであることを特徴とする請求項１に記載の方法。
【請求項４】
前記安全ネットワークプロビジョニングデバイスを前記コンピュータに接続することは、前記安全ネットワークプロビジョニングデバイスおよび前記コンピュータの物理的な近接を要することを特徴とする請求項１に記載の方法。
【請求項５】
前記安全ネットワークプロビジョニングデバイスを前記クライアントデバイスに接続することは、前記安全ネットワークプロビジョニングデバイスおよび前記クライアントデバイスの物理的な近接を要することを特徴とする請求項１に記載の方法。
【請求項６】
前記安全ネットワークプロビジョニングデバイスは、前記少なくとも１つのネットワークインターフェースから独立したネットワークインターフェースを介して前記コンピュータに接続されることを特徴とする請求項１に記載の方法。
【請求項７】
前記安全ネットワークプロビジョニングデバイスは、前記少なくとも１つのネットワークインターフェースから独立した前記ネットワークインターフェースを介して前記クライアントデバイスに接続されることを特徴とする請求項６に記載の方法。
【請求項８】
前記少なくとも１つのネットワークインターフェースから独立した前記ネットワークインターフェースは、ワイヤラインネットワークインターフェースであることを特徴とする請求項７に記載の方法。
【請求項９】
前記安全ネットワークプロビジョニングデバイスは、
前記獲得モードのとき、ネットワークプロファイルを獲得し、
前記ゲートウェイモードのとき、前記ネットワークプロファイルに関連する安全ネットワークへのアクセスを前記クライアントデバイスに提供することを特徴とする請求項７に記載の方法。
【請求項１０】
前記少なくとも１つのネットワークインターフェースから独立した前記ネットワークインターフェースは、ユニバーサルシリアルバス（ＵＳＢ）インターフェースであり、異なるモードにおいて異なるユニバーサルシリアルバス（ＵＳＢ）列挙クラス識別子を列挙することを特徴とする請求項９に記載の方法。
【請求項１１】
ワイヤレスネットワークからリモートネットワークへのゲートウェイとして働くコンピュータと、
安全ネットワークプロビジョニングデバイスと
を備えたコンピュータ化されたシステムであって、
前記コンピュータは、
前記安全ネットワークプロビジョニングデバイスの接続に応答して前記安全ネットワークプロビジョニングデバイスが通信できるネットワークのタイプに関する情報に基づいて、前記コンピュータにおいて既知のネットワークプロファイルのリストをグラフィカルユ

ーザインターフェースで提示し、前記グラフィカルユーザインラーフェースを介して選択または作成された少なくとも１つのネットワークプロファイルを受信し、
前記安全ネットワークプロビジョニングデバイスは、
第１のセットのネットワーク通信インターフェースであって、前記第１のセットのネットワーク通信インターフェースの少なくとも１つは、関連するネットワークへのアクセスを可能にするために構成ブロックを要求する第１のセットのネットワーク通信インターフェースと、
第２のセットのネットワーク通信インターフェースであって、前記第２のセットのネットワーク通信インターフェースの少なくとも１つは、ネットワークアクセスの前に構成の必要がない第２のセットのネットワーク通信インターフェースと、
前記第１および第２のセットのネットワーク通信インターフェース中のネットワーク通信インターフェース間のネットワークトラフィックをゲートするように構成された通信インターフェースゲートウェイモジュールと、
ネットワークプロファイル獲得モジュールであって、少なくとも、
前記コンピュータから少なくとも１つのネットワークプロファイルを獲得し、
前記少なくとも１つのネットワークプロファイルを解析して、前記第１のセットのネットワーク通信インターフェースの前記少なくとも１つのそれぞれによって要求される各構成ブロックを提供するように構成されたネットワークプロファイル獲得モジュールと
を備えたことを特徴とするシステム。
【請求項１２】
前記安全ネットワークプロビジョニングデバイスは複数の動作モードを有し、前記複数の動作モードは獲得モードおよびゲートウェイモードを備え、
前記第１のセットのネットワーク通信インターフェースの少なくとも１つは、前記安全ネットワークプロビジョニングデバイスが前記ゲートウェイモードのときにイネーブルされ、
前記第２のセットのネットワーク通信インターフェースの少なくとも１つは、前記安全ネットワークプロビジョニングデバイスが前記獲得モードのときおよび前記安全ネットワークプロビジョニングデバイスが前記ゲートウェイモードのときにイネーブルされ、
前記通信インターフェースゲートウェイモジュールは、前記安全ネットワークプロビジョニングデバイスが前記ゲートウェイモードのときにイネーブルされ、
前記ネットワークプロファイル獲得モジュールは、前記安全ネットワークプロビジョニングデバイスが前記獲得モードのときにイネーブルされることを特徴とする請求項１１に記載のシステム。
【請求項１３】
前記安全ネットワークプロビジョニングデバイスは、前記ネットワークプロファイル獲得モジュールが前記第１のセットのネットワーク通信インターフェースの前記少なくとも１つのそれぞれによって要求される各構成ブロックを提供した後、前記獲得モードから前記ゲートウェイモードに切り換わることを特徴とする請求項１２に記載のシステム。
【請求項１４】
リセットコマンドに応答して、前記安全ネットワークプロビジョニングデバイスは、
前記少なくとも１つのネットワークプロファイルを消去し、
前記ゲートウェイモードから前記獲得モードに切り換えることを特徴とする請求項１３に記載のシステム。
【請求項１５】
前記コンピュータから前記少なくとも１つのネットワークプロファイルを獲得することは、前記第２のセットのネットワーク通信インターフェースの１つを介して前記安全ネットワークプロビジョニングデバイスを前記コンピュータに接続する結果として生じることを特徴とする請求項１１に記載のシステム。
【請求項１６】
前記ワイヤレスネットワークに関連するワイヤレスネットワークポイントと通信するク

ライアントデバイスをさらに備え、
前記少なくとも１つのネットワークプロファイルのそれぞれにつき、前記安全ネットワークプロビジョニングデバイスは、前記ネットワークプロファイルに関連する安全ネットワークへのアクセスを前記クライアントデバイスに提供することを特徴とする請求項１１に記載のシステム。
【請求項１７】
前記アクセスを提供する間、前記安全ネットワークプロビジョニングデバイスは、前記第２のセットのネットワーク通信インターフェースの１つを介して前記クライアントデバイスに接続されることを特徴とする請求項１６に記載のシステム。
【請求項１８】
前記第１のセットのネットワーク通信インターフェースのそれぞれは、ワイヤレス通信インターフェースであり、
前記第２のセットのネットワーク通信インターフェースのそれぞれは、ワイヤライン通信インターフェースであることを特徴とする請求項１１に記載のシステム。
【請求項１９】
前記コンピュータから前記少なくとも１つのネットワークプロファイルを獲得することは、前記安全ネットワークプロビジョニングデバイスおよび前記コンピュータの物理的な近接を要することを特徴とする請求項１１に記載のシステム。
【請求項２０】
前記安全ネットワークプロビジョニングデバイスは複数の動作モードを有し、前記複数の動作モードは獲得モードおよびゲートウェイモードを備え、
前記第２のセットのネットワーク通信インターフェースの前記少なくとも１つはユニバーサルシリアルバス（ＵＳＢ）通信インターフェースであり、
新しい通信接続を確立する間に前記安全ネットワークプロビジョニングデバイスについて列挙されるユニバーサルシリアルバス（ＵＳＢ）列挙クラス識別子は、その時の前記安全ネットワークプロビジョニングデバイスの動作モードに依存することを特徴とする請求項１１に記載のシステム。
【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【発明の詳細な説明】
【発明の名称】安全なネットワークアクセスを提供するためのシステムおよび方法
【技術分野】
【０００１】
本発明は、一般にコンピュータネットワークに関し、より詳細には、安全なネットワークのプロビジョニング（ｐｒｏｖｉｓｉｏｎｉｎｇ）に関する。
【背景技術】
【０００２】
コンピュータネットワークおよびインターネットワークは、ますます多くの人が仕事および遊びのために使用するにつれて一般的になってきた。電子メール、インスタントメッセージ、ストリーミングオーディオおよびビデオ、共同フォーラム、対話式ゲーム、これらは、絶えず増加し続けるコンピュータネットワーク応用分野のほんの数例である。コンピュータネットワークが日常生活に組み込まれるようになるにつれて、気軽で直感的なネットワーキングへの需要が生まれている。例えば、コンピュータネットワーキング専門家の助けに頼ることなくコンピュータネットワークリソースにアクセスできることへの需要である。
【０００３】
しかし同時に、相互に関連する理由で、気軽なコンピュータネットワーキングに対する

少なくとも１つの障壁が生じている。コンピュータネットワークが日常生活に組み込まれるようになるにつれて、ますます多くの機密データが、これらのネットワークを介して渡され、またこれらのネットワークからアクセス可能になる。安全でないコンピュータネットワークの使用が適切である環境の数は急速に減少しており、特に、物理的なアクセスポイントが必ずしも明白ではないワイヤレスコンピュータネットワークの普及を考えるとそうである。住居用ネットワークにおいてさえ、複雑なセキュリティ機構を目にすることは珍しくない。セキュリティは、すでに複雑なネットワークアクセス手順にさらに複雑化の層を追加することによって、気軽なネットワーキングを損なう。ネットワークアクセスを提供することに伴うフラストレーションは、セキュリティ機構が機能しなくなる結果をもたらすことがあるか、または単純に完全なアクセス禁止をもたらすことがある。

【０００４】

例示的なシナリオとして、ラップトップまたはその他のネットワーク対応デバイスを持った人が、家または仕事から離れて移動し、新しいネットワークのある場所を訪ねる。手の込んだ安全ネットワーク登録手順を回避するために、ローカルがそれ自体のネットワークアクセスクリデンシャル（例えばユーザ名、パスワード、および／または暗号鍵）を訪問者に提供することがある。これは、有効なセキュリティポリシーにいくつかの形で違反する。例えば、訪問者はネットワーク上でローカルになることができ（場合によってローカルは過度に広いネットワークアクセスを訪問者に与え）、ネットワークアクセスクリデンシャルを消去する労力が費やされない場合、そのコピーが訪問者のデバイス上に残る。これは、ネットワークがそのリソースへのアクセスに課金する場合には特に問題である。

【０００５】

構成の利便性からみた問題の一面は、ネットワークアクセスクリデンシャルが「帯域外で」、すなわちアクセスが求められている安全なネットワーク以外の何らかの方法によって提供されることが最良である。安全でないネットワークサービスが安全なネットワークサービスの前に利用可能であることは多いが、安全でないネットワークを介してネットワークアクセスクリデンシャルを渡すのは、セキュリティ上のリスクである。別の複雑さは、特定の安全なネットワークにアクセスできるようにデバイスを構成することが通常、ネットワークアクセスクリデンシャルだけでなくそれ以上のものを要求することである。例えば、最適な機能のためにネットワーク対応デバイス（ｎｅｔｗｏｒｋ－ｒｅａｄｙ　ｄｅｖｉｃｅ）によって要求される完全な関連ネットワーク「プロファイル」がある場合がある。このようなネットワークプロファイルの例として、非特許文献１に記載されたワイヤレスプロファイルがある。伴うデータの量は、例えばヘルプデスクへの電話による構成を、厄介でエラーを起こしやすいものにすることがある。

【０００６】

【非特許文献１】Wireless Provisioning Service section of the Microsoft Developer Network (MSDN (登録商標)) Library dated may 2004

【非特許文献２】Plug and Play section of the Kernel－Mode Driver Architecture Design Guide in the Microsoft Developer Network (MSDN (登録商標)) Library dated June 14, 2004

【非特許文献３】Authentication section of the Microsoft (登録商標) Windows (登録商標) Platform Software Development Kit (SDK) in the Microsoft Developer Network (MSDN (登録商標)) Library dated June, 2004

【発明の開示】

【発明が解決しようとする課題】

【０００７】

これらの困難を克服するために新しい種類のネットワークを設計することも可能だが、このような解決法は、既存のネットワークの広大な基盤への安全なアクセスを提供できないことになる。互換性を最大限にするためには、構成の困難を、可能な限り既存のネットワーキング標準の制約内で解決すべきである。同様に、最適な解決法は、例えばカスタムインターフェースを要求することによって既存の広範なネットワーク対応デバイスを除外

すべきではなく、加えて、「プラグアンドプレイ」機能など、デバイスによって保持される自動構成機能のどんな追加層にも対応すべきである。デバイスの自動構成機能に関する例示的な詳細およびコンテキストが非特許文献２に記述されている。

【課題を解決するための手段】

【０００８】

このセクションでは、本発明のいくつかの実施形態を単純化した概要を提示する。この概要は、本発明の広範な概観ではない。この概要は、本発明の鍵となる／クリティカルな要素を特定するものではなく、本発明の範囲を画定するものでもない。この唯一の目的は、本発明のいくつかの実施形態を、後で提示するより詳細な記述への前置きとして、単純化した形で提示することである。

【０００９】

本発明の一実施形態では、安全なネットワークアクセスを提供することは、安全ネットワークプロビジョニングデバイス（ｓｅｃｕｒｅ　ｎｅｔｗｏｒｋ　ｐｒｏｖｉｓｉｏｎｉｎｇ　ｄｅｖｉｃｅ）をセキュリティ権限に接続することを含む。セキュリティ権限から、１つまたは複数のネットワークプロファイルを獲得することができる。獲得したネットワークプロファイルの属性に対応するデータで、安全ネットワークプロビジョニングデバイスの１つまたは複数のネットワークインターフェースを構成することができる。安全ネットワークプロビジョニングデバイスは、獲得モードからゲートウェイモードに切り換えることができる。安全ネットワークプロビジョニングデバイスは、クライアントデバイスに接続することができる。クライアントデバイスには、獲得された各ネットワークプロファイルに関連する安全ネットワークへのアクセスを提供することができる。

【００１０】

本発明の一実施形態では、安全なネットワークアクセスを提供することは、安全ネットワークに関連する１つまたは複数のネットワークプロファイルを管理することを含む。安全ネットワークプロビジョニングデバイスが獲得モードのとき、安全ネットワークプロビジョニングデバイスからの接続を受け入れることができ、管理下にあるネットワークプロファイルをこのデバイスに提供することができる。提供された各ネットワークプロファイルにより、安全ネットワークプロビジョニングデバイスは、ゲートウェイモードに切り換わったときに、そのネットワークプロファイルに関連する安全ネットワークへのアクセスをクライアントデバイスに提供することができる。

【００１１】

本発明の一実施形態では、安全なネットワークアクセスを提供することは、安全ネットワークプロビジョニングデバイスがゲートウェイモードのときに、安全ネットワークプロビジョニングデバイスからの接続を受け入れることを含む。安全ネットワークプロビジョニングデバイスを介して安全ネットワークにアクセスするために、各安全ネットワークはアクセスのための認証クリデンシャルを要求することができる。安全ネットワークプロビジョニングデバイスは、獲得モードにある間に、要求される認証クリデンシャルで構成することができる。

【００１２】

本発明の一実施形態では、安全ネットワークプロビジョニングデバイスは、第１のセットのネットワーク通信インターフェースと、第２のセットのネットワーク通信インターフェースと、通信インターフェースゲートウェイモジュールと、ネットワークプロファイル獲得モジュールとを備える。第１のセットのネットワーク通信インターフェースは、１つまたは複数のネットワーク通信インターフェースを含むことができ、これらのネットワーク通信インターフェースは、関連するネットワークへのアクセスを可能にするために構成ブロックを必要とする。第２のセットのネットワーク通信インターフェースは、ネットワークアクセスの前に構成する必要のない１つまたは複数のネットワーク通信インターフェースを含むことができる点で異なる。通信インターフェースゲートウェイモジュールは、第１および第２のセット中のネットワーク通信インターフェース間のネットワークトラフィックをゲートするように構成することができる。ネットワークプロファイル獲得モジュ

ールは、セキュリティ権限からネットワークプロファイルを獲得し、第１のセットの通信インターフェースによって要求される構成ブロックを提供することができる。各構成ブロックは、獲得されたネットワークプロファイルの１つまたは複数に対応する。

【００１３】

本発明の特徴を添付の特許請求の範囲に特に開陳するが、本発明およびその利点は、添付の図面と共に以下の詳細な記述を読めば最もよく理解される。

【発明を実施するための最良の形態】

【００１４】

本発明の様々な実施形態の記述に進む前に、本発明の様々な実施形態を実施することのできるコンピュータに関する記述を以下に提供する。必須ではないが、本発明については、プログラムモジュールなど、コンピュータによって実行されるコンピュータ実行可能命令の一般的なコンテキストで述べる。一般にプログラムは、特定のタスクを実行するか特定の抽象データ型を実装するルーチン、オブジェクト、コンポーネント、データ構造などを含む。本明細書で使用される用語「プログラム」は、単一のプログラムモジュール、または協調して動作する複数のプログラムモジュールを意味することができる。本明細書で使用される用語「コンピュータ」および「コンピューティングデバイス」には、パーソナルコンピュータ（ＰＣ）、ハンドヘルドデバイス、マルチプロセッサシステム、マイクロプロセッサベースのプログラム可能な民生用電子機器、ネットワークＰＣ、ミニコンピュータ、タブレットＰＣ、ラップトップコンピュータ、マイクロプロセッサまたはマイクロコントローラを有する民生用機器、ルータ、ゲートウェイ、ハブなど、１つまたは複数のプログラムを電子的に実行する任意のデバイスが含まれる。本発明は分散コンピューティング環境で利用することもでき、その場合、タスクは通信ネットワークでリンクされたリモート処理デバイスによって実行される。分散コンピューティング環境では、プログラムはローカルとリモートの両方のメモリ記憶デバイスに位置することができる。

【００１５】

図１を参照すると、本明細書に述べる本発明の態様を実施することのできるコンピュータ１０２の基本的な構成の例が示されている。コンピュータ１０２は通常、その最も基本的な構成では、少なくとも１つの処理ユニット１０４およびメモリ１０６を備える。処理ユニット１０４は、本発明の様々な実施形態に従ってタスクを実施するための命令を実行する。このようなタスクを実施する際、処理ユニット１０４は、コンピュータ１０２の他の部分およびコンピュータ１０２の外部のデバイスに電子信号を送って、何らかの結果を引き起こすことができる。コンピュータ１０２の厳密な構成およびタイプに応じて、メモリ１０６は揮発性（ＲＡＭなど）、不揮発性（ＲＯＭやフラッシュメモリなど）、またはこの２つの何らかの組合せとすることができる。この最も基本的な構成は、図１では破線１０８で示されている。

【００１６】

コンピュータ１０２は、追加の機構／機能を有することもできる。例えば、コンピュータ１０２は追加のストレージ（リムーバブル１１０および／または非リムーバブル１１２）を備えることもでき、これらには、限定しないが磁気ディスクまたは光ディスクあるいはテープが含まれる。コンピュータ記憶媒体には、コンピュータ実行可能命令、データ構造、プログラムモジュール、その他のデータを含む情報を格納するための任意の方法または技術で実装された揮発性および不揮発性、リムーバブルおよび非リムーバブルの媒体が含まれる。コンピュータ記憶媒体には、限定しないがＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリ、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）またはその他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージまたはその他の磁気記憶デバイスが含まれ、あるいは、所望の情報を記憶するのに使用できコンピュータ１０２からアクセスできるその他の任意の媒体が含まれる。このような任意のコンピュータ記憶媒体をコンピュータ１０２の一部とすることができる。

【００１７】

コンピュータ１０２はまた、デバイスがリモートコンピュータ１１６など他のデバイス

と通信できるようにする通信接続１１４も備えることが好ましい。通信接続は、通信媒体の一例である。通信媒体は通常、コンピュータ可読命令、データ構造、プログラムモジュール、またはその他のデータを、搬送波やその他のトランスポート機構などの変調データ信号に具体化し、任意の情報送達媒体がこれに含まれる。限定ではなく例として、用語「通信媒体」には、音響、無線周波数、赤外線などのワイヤレス媒体、およびその他のワイヤレス媒体が含まれる。本明細書で使用される用語「コンピュータ可読媒体」には、コンピュータ記憶媒体と通信媒体の両方が含まれる。

【００１８】

コンピュータ１０２は、キーボード／キーパッド、マウス、ペン、音声入力デバイス、タッチ入力デバイスなどの入力デバイス１１８も有することができる。また、表示装置、スピーカ、プリンタなどの出力デバイス１２０を備えることもできる。これらのデバイスはすべて当技術分野で周知であり、ここで詳細に述べる必要はない。

【００１９】

以下の記述では、特に指示がない限り、１つまたは複数のコンピューティングデバイスによって実行されるオペレーションのシンボル表現およびアクトを参照しながら本発明を述べる。このように、コンピュータによって実行されるものとして言及されることがあるこのようなアクトおよびオペレーションは、構造化された形でデータを表す電子信号をコンピュータの処理ユニットによって操作することを含むことが理解されるであろう。この操作は、データを変換するか、またはデータをコンピュータのメモリシステム中のロケーションで維持し、それにより、コンピュータのオペレーションは、当業者にはよく理解されるようにして再構成されるかまたは他の方法で変更される。データが維持されるデータ構造は、データのフォーマットによって定義される特定のプロパティを有する物理的なメモリロケーションである。しかし、本発明を前述のコンテキストで述べるが、これは限定を意味するのではなく、以下に述べるアクトおよびオペレーションの多くをハードウェア中で実施してもよいことを当業者は理解するであろう。

【００２０】

図２に、本発明の態様を組み込むのに適したネットワーキング環境２００の例示的な詳細を示す。ネットワーキング環境２００は、第１のワイヤレスネットワークに関連する第１のワイヤレスネットワークアクセスポイント（ＡＰ）２０２と、第２のワイヤレスネットワークに関連する第２のワイヤレスネットワークアクセスポイント２０４とを含む。例えば、第１および第２のワイヤレスネットワークは、ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃ Ｅｎｇｉｎｅｅｒｓ）８０２．１ｘシリーズの標準などの標準に準拠するワイヤレスローカルエリアネットワーク（ＷＬＡＮ）技術や、Ｂｌｕｅｔｏｏｔｈ（ＢＴ）シリーズの標準などの標準に準拠するワイヤレスパーソナルエリアネットワーク（ＷＰＡＮ）技術などを使用することができる。この例では、プリンタ２０６、ラップトップコンピュータ（ラップトップ）２０８、パーソナルデジタルアシスタント（ＰＤＡ）２１０、携帯電話機２１２はそれぞれ、安全ネットワークプロビジョニングデバイス２１４を介して１つまたは複数のワイヤレスネットワークへのアクセスを有する。各安全ネットワークプロビジョニングデバイス２１４は、ワイヤレスアクセスポイント２０２および２０４のうちの１つまたは複数と通信して、ワイヤレスネットワークへのアクセスを提供する。

【００２１】

この例では、パーソナルコンピュータ（ＰＣ）２１６は、パーソナルコンピュータ２１６が第１のワイヤレスネットワークに参加するのを可能にする、安全ネットワークプロビジョニングデバイス２１４から独立したワイヤレスネットワークアクセス機構（例えばワイヤレスネットワークインターフェースカードすなわちＮＩＣ）を備える。パーソナルコンピュータ２１６はまた、パーソナルコンピュータ２１６がリモートネットワーク２１８にアクセスするのを可能にする第２のネットワークアクセス機構も備える。リモートネットワーク２１８および第２のワイヤレスアクセスポイント２０４はそれぞれ、インターネット２２０（すなわち、「インターネット」を含めた複数の相互接続ネットワーク）への

アクセスを提供する。パーソナルコンピュータ２１６は、第１のワイヤレスネットワークからリモートネットワーク２１８へのゲートウェイとして働くことができる。インターネット２２０へは、第１および第２の両方のワイヤレスネットワークからの経路が存在するが、第１のワイヤレスネットワークからのインターネットアクセスはリモートネットワーク２１８を通る。リモートネットワーク２１８は追加のセキュリティ（例えばファイアウォール化やウイルススキャン）を提供することができ、したがって、２つの経路によって提供されるサービスの品質は異なる場合がある。

【００２２】

前述のように、プリンタ２０６、ラップトップ２０８、ＰＤＡ２１０、携帯電話機２１２などのコンピューティングデバイスを安全なネットワークアクセスのために従来のように構成するのは、厄介でエラーが起こりやすいことがある。本発明の一実施形態では、このようなデバイスを構成する必要はなく、安全ネットワークプロビジョニングデバイス２１４が適切に構成され、次いで安全ネットワークプロビジョニングデバイス２１４は、デバイス２０６、２０８、２１０、２１２と、１つまたは複数の安全なネットワーク、すなわちこの例では第１および第２のワイヤレスアクセスポイント２０２および２０４に関連するワイヤレスネットワークとの間で、ゲートウェイとして働く。本発明の一実施形態では、安全ネットワークプロビジョニングデバイス２１４は、パーソナルコンピュータ２１６またはその他の適したネットワークセキュリティ権限エージェントによって、ネットワークアクセスクリデンシャルを含めた安全ネットワークプロファイルに対応するデータで構成される。セキュリティ権限およびそれらのエージェントに関する例示的な詳細およびコンテキストが記述されている（非特許文献３参照）。安全ネットワークプロビジョニングデバイス２１４は、構成されると、モードを切り換えて安全ネットワークゲートウェイになる。

【００２３】

図２では、安全ネットワークプロビジョニングデバイス２１４はクライアントデバイス２０６、２０８、２１０、２１２から物理的に離れているように示されているが、当業者には明らかなように、安全ネットワークプロビジョニングデバイス２１４は、クライアントデバイス２０６、２０８、２１０、２１２および同様のコンピューティングデバイスにモジュラー方式で組み込まれつつ実質的な効用を維持することができる。

【００２４】

安全ネットワークプロビジョニングデバイス２１４の動作をより詳細に述べる前に、安全ネットワークプロビジョニングデバイス２１４の例示的なアーキテクチャを述べるのが役立つであろう。図３に、本発明の一実施形態による、安全ネットワークプロビジョニングデバイスを実現するのに適した例示的なアーキテクチャを示す。この例示的なアーキテクチャでは、安全ネットワークプロビジョニングデバイス３０２が、１つまたは複数のワイヤライン通信インターフェース３０４と、１つまたは複数のワイヤレス通信インターフェース３０６と、通信インターフェースゲートウェイモジュール３０８と、ネットワークプロファイル獲得モジュール３１０とを備えている。

【００２５】

ワイヤライン通信インターフェース３０４には、ユニバーサルシリアルバス（ＵＳＢ）インターフェースと、Ｅｔｈｅｒｎｅｔ（登録商標）インターフェース（例えば標準的なＮＥ２０００Ｅｔｈｅｒｎｅｔ（登録商標）インターフェースや、ＩＥＥＥ８０２．３ｘシリーズの標準に準拠するその他の通信インターフェース）と、任意の適したワイヤライン通信インターフェース（例えばメタリックまたはノンメタリックワイヤを組み込んだ通信媒体への通信インターフェース）とを含むことができる。ワイヤレス通信インターフェース３０６には、ＩＥＥＥ８０２．１ｘシリーズの標準（例えばＷｉ－Ｆｉ）に準拠する通信インターフェースと、Ｂｌｕｅｔｏｏｔｈ（ＢＴ）シリーズの標準に準拠する通信インターフェースと、ウルトラワイドバンド（ＵＷＢ）ワイヤレス通信インターフェースと、ワイヤレスＵＳＢ通信インターフェースと、任意の適したワイヤレス通信インターフェース（例えばメタリックまたはノンメタリックワイヤから独立した通信媒体への通信イン

ターフェース）とを含むことができる。
【００２６】
ネットワークプロファイル獲得モジュール３１０は、図２のパーソナルコンピュータ２１６などのネットワークセキュリティ権限エージェントから、ワイヤライン通信インターフェース３０４の１つを介して、１つまたは複数のネットワークプロファイル３１２を獲得することができる。ネットワークプロファイル獲得モジュール３１０は、ワイヤレス通信インターフェース３０６に１つまたは複数の構成ブロック３１４を提供することができる。本発明の一実施形態では、各ワイヤレス通信インターフェース３０６は、１つまたは複数の構成ブロック３１４に関連付けられている。特定のワイヤレス通信インターフェースに関連する構成ブロック３１４が提供されたとき、このワイヤレス通信インターフェースは、関連するワイヤレスネットワークを介して通信することができる。本発明の一実施形態では、ワイヤレス通信インターフェースが関連のワイヤレスネットワークを介して安全に通信できるようになる前に、関連する構成ブロック３１４が必要である。
【００２７】
構成ブロック３１４中のデータは、ネットワークプロファイル３１２の１つまたは複数の属性に対応する。１つまたは複数の構成ブロック３１４は、ネットワークプロファイル３１２のうちの関連する１つと同一であってもよい。構成ブロック３１４の内容の詳細は当技術分野で知られており、ここで詳しく述べる必要はない。このような詳細は、例えば上で参照したＩＥＥＥ標準文書など、構成されるネットワークインターフェースに関連する１つまたは複数の標準文書に大部分が記述されている。
【００２８】
ネットワークプロファイル獲得モジュール３１０が構成ブロック３１４をワイヤレス通信インターフェース３０６に提供すると、ネットワークプロファイル獲得モジュール３１０はディセーブルされ、通信インターフェースゲートウェイモジュール３０８がイネーブルされる。通信インターフェースゲートウェイモジュール３０８は、ワイヤライン通信インターフェース３０４と構成済みのワイヤレス通信インターフェース３０６との間の通信トラフィックのための、ブリッジ／ルータとして働く。このようなゲートウェイモジュールは当技術分野で知られており、ここでさらに述べる必要はない。
【００２９】
この例では、ネットワークプロファイル獲得モジュール３１０がワイヤライン通信インターフェース３０４の１つを利用してネットワークプロファイルを獲得し、次いでこれらのネットワークプロファイルを利用して１つまたは複数のワイヤレス通信インターフェース３０６を構成するが、本発明の実施形態はこのように限定されるわけではない。例えば、通信インターフェースのセット３０４と３０６は両方ともワイヤレス通信インターフェースであってもよく、あるいは両方ともワイヤライン通信インターフェースであってもよく、あるいは、ネットワークプロファイル獲得モジュール３１０が介する通信インターフェースはワイヤレス通信インターフェースとし、ネットワークプロファイル獲得モジュール３１０が構成する通信インターフェースはワイヤライン通信インターフェースとしてもよい。
【００３０】
図４に、本発明の一実施形態による、安全ネットワークプロビジョニングデバイス２１４（図２）によって安全なネットワークアクセスを提供するために実行することのできる例示的なステップを示す。この初期状態４０２では、安全ネットワークプロビジョニングデバイス２１４は獲得モードとすることができる。図５に、獲得モードでアクティブになることのできる安全ネットワークプロビジョニングデバイス３０２（図３）のコンポーネントを破線５０２で示す。獲得モードでは、ワイヤレス通信インターフェース３０６および通信インターフェースゲートウェイモジュール３０８は非アクティブであり、ワイヤライン通信インターフェース３０４およびネットワークプロファイル獲得モジュール３１０はアクティブである。
【００３１】

ステップ４０４で、安全ネットワークプロビジョニングデバイス２１４（図２）を、セキュリティ権限（またはパーソナルコンピュータ２１６などのセキュリティ権限エージェント）に、ワイヤライン通信インターフェース３０４（図５）によって接続する。安全ネットワークプロビジョニングデバイス２１４は、セキュリティ権限に接続されると、従来のプラグアンドプレイ（ＰｎＰ）技法によって安全ネットワークプロビジョニングデバイスとして認識される。ワイヤライン通信インターフェース３０４によってセキュリティ権限に接続するには、通常、セキュリティ権限との、またはセキュリティ権限に接続されたケーブルとの物理的接触が必要である。本発明の一実施形態では、ネットワークプロビジョニングデバイス２１４がセキュリティ権限と物理的に接触する必要があることが、安全なネットワークアクセス認証の一要素である。

【００３２】

ステップ４０６で、安全ネットワークプロビジョニングデバイス２１４は、セキュリティ権限によって認識された後、１つまたは複数のネットワークプロファイル３１２をセキュリティ権限から獲得する。本発明の一実施形態では、セキュリティ権限から獲得される特定のネットワークプロファイルは、ネットワークプロファイル獲得プロトコルによって決定される。例示的なネットワークプロファイル交渉プロトコルを含めて、ステップ４０４および４０６の態様については、後で図７を参照しながらより詳細に述べる。

【００３３】

ステップ４０８で、ネットワークプロファイル獲得モジュール３１０から１つまたは複数のワイヤレス通信インターフェース３０６（図５）に構成ブロック３１４を提供する。特定のワイヤレス通信インターフェース３０６に関連の通信ブロック３１４を提供すると、ワイヤレス通信インターフェース３０６がアクティブになるものとすることもでき、あるいは、ワイヤレス通信インターフェース３０６は例えばステップ４１０で、明示的なアクティブ化を必要とすることもできる。

【００３４】

ステップ４１０で、安全ネットワークプロビジョニングデバイス２１４（図２）は、ゲートウェイモードに切り換える。図６に、ゲートウェイモードでアクティブになることのできる安全ネットワークプロビジョニングデバイス３０２（図３）のコンポーネントを破線６０２で示す。ゲートウェイモードでは、ネットワークプロファイル獲得モジュール３１０は非アクティブであり、ワイヤライン通信インターフェース３０４、ワイヤレス通信インターフェース３０６、通信インターフェースゲートウェイモジュール３０８はアクティブである。

【００３５】

ステップ４１２で、安全ネットワークプロビジョニングデバイス２１４（図２）をクライアントデバイス、例えばクライアントデバイス２０６、２０８、２１０、または２１２に接続する。ゲートウェイモードに切り換えた後、本発明の一実施形態では、安全ネットワークプロビジョニングデバイス２１４は、例えばセキュリティ権限に接続されたときと同じワイヤライン通信接続でクライアント２０６、２０８、２１０、または２１２デバイスに接続されている場合でも、構成を要求する安全ネットワークプロビジョニングデバイスとしてもはや現れることはない。そうではなく、安全ネットワークプロビジョニングデバイス２１４は、クライアントデバイス２０６、２０８、２１０、または２１２に対して、例えばＵＳＢやＥｔｈｅｒｎｅｔ（登録商標）などの標準的なワイヤライン通信インターフェースとして現れる。すなわち、ゲートウェイモードでは、安全ネットワークプロビジョニングデバイス２１４は、セキュリティ権限またはパーソナルコンピュータ２１６などのセキュリティ権限エージェントへの、またはその他の適した安全ネットワークアクセスポイントへの、直接の（例えばＵＳＢやＥｔｈｅｒｎｅｔ（登録商標）による）ワイヤライン接続をシミュレートすることができる。

【００３６】

この場合もやはり、安全ネットワークプロビジョニングデバイス２１４（図２）をクライアントデバイス２０６、２０８、２１０、または２１２に接続するには、通常、安全ネ

ットワークプロビジョニングデバイス２１４がクライアントデバイス２０６、２０８、２１０、または２１２と物理的に接触している（例えばクライアントデバイスのＵＳＢまたはＥｔｈｅｒｎｅｔ（登録商標）ポートに挿入されている）か、少なくとも近接している（例えば赤外線ベースの通信インターフェースの場合）必要があり、本発明の一実施形態では、このことは安全なネットワークアクセス認証の一要素である。ラップトップを持った訪問者のシナリオでは、構成済み（すなわち獲得モード後）の安全ネットワークプロビジョニングデバイス２１４を単に訪問者に手渡して、ラップトップのＵＳＢポートに挿入されるようにすればよい。

【００３７】

ゲートウェイモードの安全ネットワークプロビジョニングデバイス２１４（図２）が、標準的なワイヤライン通信インターフェースとしてクライアントデバイス２０６、２０８、２１０、または２１２によって認識されると、クライアントデバイス２０６、２０８、２１０、または２１２は、獲得モードの間に安全ネットワークプロビジョニングデバイス２１４によって獲得された１つまたは複数の安全ネットワークにアクセスすることができる。クライアントデバイス２０６、２０８、２１０、２１２とワイヤレスアクセスポイント２０２および２０４との間の通信トラフィックは、通信インターフェースゲートウェイモジュール３０８（図６）によってゲートされる（例えばブリッジ、ルート、プロキシ、および／またはフィルタリングされる）。

【００３８】

重要なことに、クライアントデバイス２０６、２０８、２１０、または２１２は、安全ネットワークプロビジョニングデバイス２１４のネットワークプロファイル３１２（図３）へのアクセスも構成ブロック３１４へのアクセスも得ない。その結果、安全ネットワークプロビジョニングデバイス２１４がクライアントデバイス２０６、２０８、２１０、または２１２から取り外されると、１つまたは複数の関連する安全ネットワークへのアクセスも除去される。すなわち、安全ネットワークプロビジョニングデバイス２１４は、物理的な安全ネットワーク「ゲストキー」として働くことができる。

【００３９】

ステップ４１４で、安全ネットワークプロビジョニングデバイス２１４（図２）は、リセットされるまで通信ゲートウェイとして動作し続ける。リセットはプログラムによって開始することができるが、本発明の一実施形態では、リセットは、安全ネットワークプロビジョニングデバイス２１４に組み込まれた物理的なリセットボタンまたはスイッチによって開始される。リセットされると、手順はステップ４１６に進む。

【００４０】

ステップ４１６で、安全ネットワークプロビジョニングデバイス２１４の構成ブロック３１４（図３）を消去し、関連するワイヤレス通信インターフェース３０６をディセーブルする。ステップ４１８で、ネットワークプロファイル３１２を消去し、セキュリティ権限またはパーソナルコンピュータ２１６（図２）などのセキュリティ権限エージェントから１つまたは複数のネットワークプロファイル３１２が再獲得されることなくワイヤレス通信インターフェース３０６が再アクティブ化されることがないようにする。ステップ４２０で、安全ネットワークプロビジョニングデバイス２１４は、獲得モードに戻り、セキュリティ権限に接続されるのを待機する。リセットされない場合は、安全ネットワークプロビジョニングデバイス２１４は、セキュリティ権限に対して、標準的なワイヤライン通信インターフェースとして現れる。すなわち、セキュリティ権限に対して、安全なネットワークアクセスを要求するクライアントデバイスであるかのように現れる。リセット後、獲得モードで、安全ネットワークプロビジョニングデバイス２１４は、セキュリティ権限に対して、１つまたは複数のネットワークプロファイルに関連付けられる（すなわち獲得する）準備のできた安全ネットワークプロビジョニングデバイスとして現れる。

【００４１】

図７に、図４を参照しながら上述した手順のステップ４０４および４０６に組み込むのに適した例示的なネットワークプロファイル獲得プロトコルを示す。図７の破線間の各矢

印は、モジュール間で送られるプロトコルメッセージを表す。プロトコルメッセージの順番は、図を上から下に読むことによって決定することができる。

【００４２】

安全ネットワークプロビジョニングデバイス７０２が、この例ではユニバーサルシリアルバスによってセキュリティ権限７０４に接続するとき、安全ネットワークプロビジョニングデバイス７０２は、ユニバーサルシリアルバス（ＵＳＢ）列挙クラス識別子（ＩＤ）を含むメッセージを送る。このＵＳＢ列挙クラスＩＤは、安全ネットワークプロビジョニングデバイス７０２を、ネットワークプロファイルを獲得する準備のできた安全ネットワークプロビジョニングデバイスとして識別する。この例では、ＵＳＢ列挙クラスＩＤは、例えば、安全ネットワークプロビジョニングデバイス７０２がセキュリティ権限のＵＳＢポートに挿入されたときに、セキュリティ権限７０４のユニバーサルシリアルバス（ＵＳＢ）ＰＯＮＧマネージャ７０６によって、標準的なＵＳＢ新規デバイス列挙の一部として受け取られる。ＵＳＢ　ＰＯＮＧマネージャ７０６は、ネットワークプロファイルとネットワークタイプとの間を調停し、各ネットワークプロファイルを様々なネットワークタイプにインテリジェントに関連付けることによって特定のネットワークプロファイルの適用性を拡張する。ここでは、ＵＳＢ　ＰＯＮＧマネージャ７０６のいくつかの機能だけを述べる。追加の詳細およびコンテキストは２００３年８月２１日に出願された「PHYSICAL DEVICE BONDING」という名称の同時係属の米国特許第１０／６４５００８号明細書に見ることができる。

【００４３】

ＵＳＢ列挙クラスＩＤは、安全ネットワークプロビジョニングデバイスに特有であってもよく、さらにはその特定バージョンに特有であってもよい。あるいは、安全ネットワークプロビジョニングデバイスは、ＵＳＢフラッシュドライブなど標準的なデバイスクラスとして列挙することもできる。安全ネットワークプロビジョニングデバイス７０２がモジュラー方式でクライアントデバイスに組み込まれている場合、安全ネットワークプロビジョニングデバイス７０２とクライアントデバイスとはＵＳＢ複合デバイスとして列挙することができ、安全ネットワークプロビジョニングデバイスとクライアントデバイスとが単一のＵＳＢ通信インターフェースを共用していても、列挙クラス識別子は別々とすることができる。ＵＳＢ列挙クラスＩＤメッセージに応答して、ＵＳＢ　ＰＯＮＧマネージャ７０６は、クエリｐｏｎｇ／デバイスヘッダメッセージを安全ネットワークプロビジョニングデバイス７０２に送り、安全ネットワークプロビジョニングデバイス７０２が通信できるネットワークのタイプに関する情報を要求する。クエリｐｏｎｇ／デバイスヘッダメッセージに応答して、安全ネットワークプロビジョニングデバイス７０２は、要求された情報を含むリターンｐｏｎｇ／デバイスヘッダメッセージを送る。

【００４４】

この例では、ＵＳＢ　ＰＯＮＧマネージャ７０６は、安全ネットワークプロビジョニングデバイス７０２がＩＥＥＥ８０２．１１シリーズの標準に準拠するワイヤレスネットワークと通信できると判定する。その結果、ＵＳＢ　ＰＯＮＧマネージャ７０６は、安全ネットワークプロビジョニングデバイス７０２から送られたｐｏｎｇ／デバイスヘッダメッセージを、ＰＯＮＧ８０２．１１プラグインモジュール７０８に中継する。安全ネットワークプロビジョニングデバイスから返された情報が異なる場合は、ＵＳＢ　ＰＯＮＧマネージャ７０６は、ｐｏｎｇ／デバイスヘッダメッセージの中継先として異なるプラグインモジュールを選択することができる。

【００４５】

ＰＯＮＧ８０２．１１プラグインモジュールは、ｐｏｎｇ／デバイスヘッダメッセージを解析し、ワイヤレスネットワーク（ＷＳＮＫ）ウィザード７１０を呼び出して、安全ネットワークプロビジョニングデバイス７０２が関連付けられることになる１つまたは複数のワイヤレスネットワークを安全ネットワークプロビジョニングデバイスのユーザ７１２に照会する。ワイヤレスネットワークウィザード７１０の呼出しは、呼出しを引き起こしたデバイスタイプの指示、この場合は安全ネットワークプロビジョニングデバイス７０２

の指示を含み、それにより、ワイヤレスネットワークウィザード７１０は、ユーザ７１２に求められる質問と回答の数を最適化（例えば最小限に）することができる。ワイヤレスネットワークウィザード７１０は、まず既知のワイヤレスネットワークプロファイルのリストをワイヤレス自動構成モジュール７１４に照会し、次いで、このリストをグラフィカルフォーマットでユーザ７１２に提示する。本発明の一実施形態に組み込むのに適した例示的なグラフィカルユーザインターフェースについては、後で図８を参照しながらより詳細に述べる。

【００４６】

ユーザ７１２は、既知のワイヤレスネットワークプロファイルの１つまたは複数を選択し（あるいは新しいワイヤレスネットワークプロファイルを作成し）、ワイヤレスネットワークウィザード７１０は、この選択を呼出し元のＰＯＮＧ８０２．１１プラグインモジュール７０８に返す。この例では、ＰＯＮＧ８０２．１１プラグインモジュール７０８は、選択されたワイヤレスネットワークプロファイルを解析して、この安全ネットワークプロビジョニングデバイスタイプに特化したワイヤレスネットワーク構成データ構造（例えばワイヤレスネットワークインターフェース構成ブロック）を作成する。例えば、ワイヤレスネットワーク構成データ構造は、ワイヤレスネットワークに対するサービスセット識別子（ＳＳＩＤ）と、接続タイプ指示子（例えば拡張サービスセット「ＥＳＳ」や独立基本サービスセット「ＩＢＳＳ」）と、認証タイプ指示子（例えば「ＯＰＥＮ」や「ＷＰＡＰＳＫ」（Ｗｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ　ｗｉｔｈ　Ｐｒｅ－ｓｈａｒｅｄ　Ｋｅｙ））と、暗号化タイプ指示子（例えば「ＷＥＰ」（Ｗｉｒｅｌｅｓｓ　Ｅｎｃｒｙｐｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）や「ＴＫＩＰ」（Ｔｅｍｐｏｒａｌ　Ｋｅｙ　Ｉｎｔｅｇｒｉｔｙ　Ｐｒｏｔｏｃｏｌ））と、ネットワーク鍵（例えばＡＳＣＩＩまたはＨＥＸの４０／１０４ビットＷＥＰ鍵や２５６ビットＷＰＡＰＳＫ鍵）を含むことができる。

【００４７】

次いで、ＰＯＮＧ８０２．１１プラグインモジュール７０８は、メッセージ中のワイヤレスネットワーク構成データ構造をＵＳＢ　ＰＯＮＧマネージャ７０６に送り、ＵＳＢ　ＰＯＮＧマネージャは、このデータ構造を安全ネットワークプロビジョニングデバイス７０２に渡す。ワイヤレスネットワーク構成データ構造を含むメッセージがうまく受け取られたことが、ＵＳＢ　ＰＯＮＧマネージャ７０６への確認メッセージで確認され、ＵＳＢ　ＰＯＮＧマネージャ７０６は、ユーザ７１２で終了する一連の確認メッセージをトリガする。

【００４８】

セキュリティ権限７０４は、どの安全ネットワークプロビジョニングデバイスが特定のネットワークプロファイルで構成されたかを追跡することができ、いくつかのネットワークタイプでは、セキュリティ権限７０４は、例えば盗まれた安全ネットワークプロビジョニングデバイスを使用した無許可ネットワークアクセスから保護するために、特定の安全ネットワークプロビジョニングデバイスに関連するネットワークアクセスを取り消すことができる。セキュリティ権限７０４は、追加のネットワークアクセスレベルを施行することもできる。例えば、すでに安全ネットワークプロビジョニングデバイスを利用して接続されているユーザが特定のネットワークリソースにアクセスするには、追加の承認が必要であるようにすることができる。さらに、セキュリティ権限７０４は、接続性診断情報を提供して、安全ネットワークプロビジョニングデバイスのユーザが技術的困難を解決するのを補助することもできる。

【００４９】

図８に、本発明の一実施形態による、安全ネットワークプロファイルを選択するのに適した例示的なグラフィカルユーザインターフェース要素を示す。意図的に簡素なユーザインターフェース８００は、安全ネットワークプロビジョニングデバイスがアクセスを提供することになるワイヤレスネットワークを選択するよう、安全ネットワークプロビジョニングデバイスのユーザを促す。例示的なリスト選択領域８０２は、各ワイヤレスネットワ

ークの「フレンドリ名」、ならびにワイヤレスネットワークのタイプの指示、具体的には各ネットワークに関連するセキュリティレベルを含む。ユーザは、ワイヤレスネットワークを選択してから「次へ」ボタン８０４を選択することもでき、あるいは、最初に「新規作成」ボタン８０６を選択し、新しいワイヤレスネットワーク（および関連するワイヤレスネットワークプロファイル）を作成して選択領域８０２に追加することもできる。

【００５０】

刊行物、特許出願、特許を含めて、本明細書で引用したすべての参考文献は、各参考文献が参照により組み込まれるよう個別かつ具体的に指示されておりその全体が本明細書に記載されているかのように、参照により本明細書に組み込まれる。

【００５１】

本発明を記述するコンテキスト（特に添付の特許請求の範囲のコンテキスト）における冠詞や不定冠詞および同様の指示物の使用は、本明細書に特に指示がない限り、またはコンテキストにより明らかに矛盾しない限り、単数と複数の両方をカバーするものと解釈すべきである。用語「備える」「有する」「含む」「入る」は、特に注記がない限り、オープンエンドの用語（すなわち「含むが限定されない」という意味）として解釈すべきである。本明細書における値の範囲の引用は、本明細書に特に指示がない限り、その範囲に入る各個々の値を個別に参照する略記方法として働くだけであり、各個々の値は、それが本明細書で個別に引用されたかのように本明細書に組み込まれる。本明細書で述べたすべての方法は、本明細書に特に指示がない限り、またはコンテキストにより明らかに矛盾しない限り、任意の適した順番で実行することができる。本明細書で提供したあらゆる例または例示的な言葉（例えば「など」）の使用は、本発明をよりはっきりさせるものに過ぎず、特に特許請求の範囲に記載されない限り、本発明の範囲を限定するものではない。本明細書中のどの言葉も、特許請求の範囲に記載されていない要素を本発明の実施に不可欠なものとして示すものと解釈すべきではない。

【００５２】

本明細書では、本発明者らにとって本発明を実施するための最良の形態を含め、本発明の好ましい実施形態を述べた。これらの好ましい実施形態の変形も、以上の記述を読めば当業者には明らかになるであろう。本発明者らは、当業者がこのような変形を適切に利用することを予想し、また本発明が、本明細書に具体的に記載されているのとは別の方式で実施されることも意図している。したがって本発明は、準拠法によって許可される本明細書に添付の特許請求の範囲に記載された主題の修正および均等すべてを含む。さらに、本明細書に特に指示がない限り、またはコンテキストにより明らかに矛盾しない限り、前述の要素のいかなる組合せも、その可能なすべての変形が本発明に含まれる。

【図面の簡単な説明】

【００５３】

【図１】本発明の一実施形態を実施するのに使用可能な例示的なコンピュータシステムを一般的に示す概略図である。

【図２】本発明の態様を組み込むのに適した例示的なネットワーキング環境を示す概略図である。

【図３】本発明の一実施形態による例示的な安全ネットワークプロビジョニングデバイスアーキテクチャを示す概略図である。

【図４】本発明の一実施形態による、安全ネットワークプロビジョニングデバイスによって安全なネットワークアクセスを提供するための例示的なステップを示すフローチャートである。

【図５】本発明の一実施形態による、獲得モードにおける安全ネットワークプロビジョニングデバイスを示す概略図である。

【図６】本発明の一実施形態による、ゲートウェイモードにおける安全ネットワークプロビジョニングデバイスを示す概略図である。

【図７】本発明の一実施形態による、例示的なネットワークプロファイル獲得プロトコルを示すプロトコル図である。

【図８】本発明の一実施形態による、安全ネットワークプロファイルを選択するのに適した例示的なグラフィカルユーザインターフェース要素を示す概略図である。
【符号の説明】
【００５４】
１０２　コンピュータ
１０４　処理ユニット
１０６　システムメモリ
１０８　基本構成
１１０　リムーバブルストレージ
１１２　非リムーバブルストレージ
１１４　通信接続
１１６　リモートコンピュータ
１１８　入力デバイス
１２０　出力デバイス
２００　ネットワーキング環境
２０２　ワイヤレスＡＰ
２０４　ワイヤレスＡＰ
２０６　プリンタ
２０８　ラップトップ
２１２　携帯電話機
２１４　安全ネットワークプロビジョニングデバイス
２１６　パーソナルコンピュータ
２１８　リモートネットワーク
２２０　インターネット
３０２　安全ネットワークプロビジョニングデバイス
３０４　ワイヤライン通信インターフェース
３０６　ワイヤレス通信インターフェース
３０８　通信インターフェースゲートウェイモジュール
３１０　ネットワークプロファイル獲得モジュール
３１２　ネットワークプロファイル
３１４　構成ブロック
５０２　コンポーネント
６０２　コンポーネント
７０２　デバイス
７０６　ＵＳＢ　Ｐｏｎｇマネージャ
７０８　８０２．１１プラグイン
７１０　ＷＳＮＫ
７１４　ワイヤレス自動構成
７１２　ユーザ