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

特許第4866862号
(P4866862)

(45)発行日　平成24年2月1日(2012.2.1)　(24)登録日　平成23年11月18日(2011.11.18)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	530E
G06F 21/20	(2006.01)	G06F	15/00	330A
H04L 9/10	(2006.01)	G06F	12/14	520D
		H04L	9/00	621A

請求項の数 15　(全 25 頁)

(21)出願番号	特願2007-550484 (P2007-550484)
(86)(22)出願日	平成18年1月6日 (2006.1.6)
(65)公表番号	特表2008-527543 (P2008-527543A)
(43)公表日	平成20年7月24日 (2008.7.24)
(86)国際出願番号	PCT/US2006/000411
(87)国際公開番号	WO2006/074338
(87)国際公開日	平成18年7月13日 (2006.7.13)
審査請求日	平成20年12月8日 (2008.12.8)
(31)優先権主張番号	11/032,764
(32)優先日	平成17年1月7日 (2005.1.7)
(33)優先権主張国	米国(US)
(31)優先権主張番号	11/075,197
(32)優先日	平成17年3月7日 (2005.3.7)
(33)優先権主張国	米国(US)

(73)特許権者　508041127
シスコ　テクノロジー，インコーポレイテッド
アメリカ合衆国，カリフォルニア州　９５１３４－１７０６，サンノゼ，ウェスト・タスマン・ドライヴ　１７０
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　バウアー，マーク，ジョン
アメリカ合衆国，オレゴン州　９７２１９，ポートランド，サウスウェスト・オーキッド・ストリート　５５１０

最終頁に続く

(54)【発明の名称】データ及び装置をローカライズするシステム及び方法

(57)【特許請求の範囲】

【請求項１】

ネットワーク上の中継装置を介したサービスへのアクセスを制御する方法であって、

前記サービスのプロバイダにより発行され、装置が前記ネットワーク上の前記中継装置に登録されていることを示す値を含む、ライセンス機関により署名されたネットワークサービスクレデンシャルを前記装置が受信するステップと、

前記装置の不揮発性メモリに格納され、前記装置のメーカーを特定する装置メーカークレデンシャルを特定するステップと、

前記装置メーカークレデンシャルを置換するため、前記ネットワークサービスクレデンシャルを前記装置上の不揮発性メモリに格納するステップと、

前記装置によって前記ネットワークサービスクレデンシャルを前記サービスのプロバイダに提示するステップと、

を有し、

前記値は、前記サービスのプロバイダの名前とインターネットプロトコル（ＩＰ）アドレストとを含む群から選ばれ、

前記不揮発性メモリにおける前記ネットワークサービスクレデンシャルの存在によって、前記中継装置は、前記装置が前記ネットワークに登録されていると判断し、前記装置を前記ネットワークに拘束し、前記装置が前記中継装置を介し前記ネットワーク以外のネットワークにアクセスすることを禁止し、

前記プロバイダは、前記ネットワークサービスクレデンシャルを使用して前記装置を認

証及び許可し、認証されると、前記装置に前記サービスへのアクセスが付与される方法。
【請求項２】
前記ネットワークサービスクレデンシャルは、ＤＴＬＡ（Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｌｉｃｅｎｓｅ Ａｕｔｈｏｒｉｔｙ）クレデンシャルである、請求項１記載の方法。
【請求項３】
前記ネットワークサービスクレデンシャルは、前記装置と前記プロバイダとの暗号化アイデンティティを有する、請求項１記載の方法。
【請求項４】
前記ネットワークは、前記プロバイダのためのリモートサーバにインターネットを介し接続可能なローカルサーバに接続される複数の装置を有し、
前記ローカルサーバは、前記リモートサーバにより登録され、
前記装置は、前記ローカルサーバにより登録される、請求項１記載の方法。
【請求項５】
前記装置は、複数のパブリックアドレスを有するマルチホーム化された装置であり、
前記装置には、前記アドレスのそれぞれのネットワークサービスクレデンシャルが割り当てられる、請求項１記載の方法。
【請求項６】
バスと、
前記バスに接続される１以上のプロセッサと、
前記バスに接続され、前記プロセッサにより実行可能な命令を有するメモリ部と、
を有する装置であって、
前記プロセッサは、前記命令実行時、
ネットワーク上の中継装置を介したサービスへのアクセスを制御するサービスプロバイダにより実行される発行元装置から送信され、当該装置が前記ネットワーク上の前記中継装置に登録されていることを示す値を含む、ライセンス機関により署名されたネットワークサービスクレデンシャルを受信し、
当該装置の不揮発性メモリに、当該装置のメーカーを特定する装置メーカークレデンシャルに対応する位置を特定し、
前記不揮発性メモリにおける前記特定された位置に前記ネットワークサービスクレデンシャルを格納し、
前記サービスプロバイダが前記ネットワークサービスクレデンシャルに基づき当該装置が前記サービスにアクセスすることを認証及び許可することを可能にするため、前記ネットワークサービスクレデンシャルを前記サービスプロバイダに提示する、
よう動作可能であり、
前記ネットワークサービスクレデンシャルは、前記サービスプロバイダの名前又はアドレスが前記ネットワークサービスクレデンシャルに含まれていることを介して、前記ネットワークサービスクレデンシャルと前記サービスプロバイダとを論理的に関連付け、
前記不揮発性メモリにおける前記ネットワークサービスクレデンシャルの存在によって、前記中継装置は、前記装置が前記ネットワークに登録されていると判断し、当該装置を前記ネットワークに拘束し、当該装置が前記中継装置を介し前記ネットワーク以外のネットワークにアクセスすることを禁止する装置。
【請求項７】
前記ネットワークサービスクレデンシャルは、前記ネットワークサービスクレデンシャルに係るネットワークに対応するインターネットプロトコル（ＩＰ）アドレスを含むことによって、当該装置と前記サービスプロバイダとを論理的に関連付ける、請求項６記載の装置。
【請求項８】
前記ネットワークサービスクレデンシャルは、前記サービスプロバイダの１６バイトの名前を含むことによって、当該装置と前記サービスプロバイダとを論理的に関連付ける、

請求項６記載の装置。
【請求項９】
前記ネットワークサービスクレデンシャルは、前記サービスプロバイダにより規定され、ホームネットワークからインターネットへのアクセスを当該装置に提供するブロードバンドモデムのＭＡＣアドレスを含む加入者識別子を含むことによって、当該装置を含む前記ホームネットワークと前記サービスプロバイダとを論理的に関連付ける、請求項６記載の装置。
【請求項１０】
当該装置は、前記プロバイダのリモートサーバにインターネットを介し接続可能なローカルゲートウェイに接続される複数のネットワーク装置を有するホームネットワークにおいて動作し、
当該装置は、前記リモートサーバに登録されている前記ローカルゲートウェイに登録される、請求項６記載の装置。
【請求項１１】
当該装置はまた、インターネットプロトコル（ＩＰ）アドレスに関連付けされ、
当該装置のＩＰアドレスは、前記サービスへのアクセスが許可されているか判断するため、前記ネットワークサービスクレデンシャルと共に使用される、請求項６記載の装置。
【請求項１２】
前記ネットワークサービスクレデンシャルは、メーカー装置証明書を格納するため初期的に使用される前記不揮発性メモリの一部に格納される、請求項６記載の装置。
【請求項１３】
１以上のプロセッサと、
バスに接続され、前記プロセッサにより実行可能な命令を有するメモリ部と、
を有する装置であって、
前記プロセッサは、前記命令実行時、
ネットワーク上の中継装置を介したサービスへのアクセスを制御するサービスプロバイダにより実行される発行元装置から送信され、当該装置が前記ネットワーク上の前記中継装置に登録されていることを示す値を含む、ライセンス機関により署名されたネットワークサービスクレデンシャルを受信し、
当該装置のメーカーを特定する装置メーカークレデンシャルを格納するための当該装置の不揮発性メモリにおける位置を特定し、
前記装置メーカークレデンシャルを置換するため、前記不揮発性メモリの前記特定された位置に前記受信したネットワークサービスクレデンシャルを格納する、
よう動作可能であり、
前記ネットワークサービスクレデンシャルは、前記サービスプロバイダの名前又はアドレスが前記ネットワークサービスクレデンシャルに含まれていることを介して、前記ネットワークサービスクレデンシャルと前記サービスプロバイダとを論理的に関連付け、
前記不揮発性メモリにおける前記ネットワークサービスクレデンシャルの存在によって、前記中継装置は、前記装置が前記ネットワークに登録されていると判断し、当該装置をネットワークに拘束し、当該装置が前記中継装置を介し前記ネットワーク以外のネットワークにアクセスすることを禁止する装置。
【請求項１４】
前記ネットワークサービスクレデンシャルは、前記ネットワークサービスクレデンシャルに係るネットワークに対応するインターネットプロトコル（ＩＰ）アドレスを含むことによって、当該装置と前記サービスプロバイダとを論理的に関連付ける、請求項１３記載の装置。
【請求項１５】
前記ネットワークサービスクレデンシャルは、前記サービスプロバイダの１６バイトの名前を含むことによって、当該装置と前記サービスプロバイダとを論理的に関連付ける、請求項１３記載の装置。

【発明の詳細な説明】
【発明の詳細な説明】
【０００１】
［関連出願］
本出願は、参照することによりその全体がここに含まれる、２００５年３月７日にＡ．Ｈｕｏｔａｒｉ及びＭ．Ｂａｕｇｈｅｒにより出願された同時係属中の共願の米国特許出願第１１／０７５，１９７号（代理人整理番号ＣＳＣＯ－１０７８４．ＣＩＰ）“Ｒｅｍｏｔｅ Ａｃｃｅｓｓ ｔｏ Ｌｏｃａｌ Ｃｏｎｔｅｎｔ Ｕｓｉｎｇ Ｔｒａｎｓｃｒｙｐｔｉｏｎ ｏｆ Ｄｉｇｉｔａｌ Ｒｉｇｈｔｓ Ｍａｎａｇｅｍｅｎｔ Ｓｃｅｍｅｓ”の一部継続出願であり、さらにそれは、２００５年１月７日にＭ．Ｂａｕｇｈｅｒにより出願された同時係属中の共願の米国特許出願第１１／０３２，７６４号（代理人整理番号ＣＳＣＯ－１０１９８）“Ｕｓｉｎｇ ａ Ｎｅｔｗｏｒｋ－Ｓｅｒｖｉｃｅ Ｃｒｅｄｅｎｔｉａｌ ｆｏｒ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ”の一部継続出願である。
【０００２】
［技術分野］
本発明の実施例は、ネットワーク上に存在するコンテンツへのアクセスの制御に関する。
【０００３】
［背景技術］
コンテンツプロテクションシステムは、典型的には、仕様書により規定される。企業コンソーシアムが仕様書を開発し、独立したライセンス機関が仕様書を他の企業にライセンスする。例えば、Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ（ＤＴＣＰ）が企業コンソーシアムにより作成されたが、仕様書はＤｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｌｉｃｅｎｓｉｎｇ Ａｕｔｈｏｒｉｔｙ（ＤＴＬＡ）によりライセンスされている。
【０００４】
著作物の権利者は、特定タイプの装置に著作物をライセンスするが、他のタイプの装置にはライセンスしないよう選択するかもしれない。例えば、映画の著作物は、ＤＶＤ Ｃｏｐｙ Ｃｏｎｔｒｏｌ Ａｓｓｏｃｉａｔｉｏｎ（ＤＶＤ ＣＣＡ）によりライセンスされたデジタルビデオディスク（ＤＶＤ）プレーヤー装置上でのみ再生することが許されているかもしれない。
【０００５】
このような装置のメーカーは、ハードウェアコンフィギュレーション、ソフトウェアコンフィギュレーション及びライセンスされたデータの処理に関するライセンス機関のポリシーに従っている。準拠した装置は、当該ライセンス機関のプロトコル及びアルゴリズムを使用する。
【０００６】
各種ライセンス機関から多数のプロトコル及びアルゴリズムが提供されている。例えば、ライセンスされた装置は、Ｈｉｇｈ Ｄｅｆｉｎｉｔｉｏｎ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ（ＨＤＣＰ）規格によりプロテクトされるデジタルビデオ出力を有することが要求されているかもしれない。Ｄｉｇｉｔａｌ Ｖｉｄｅｏ Ｉｎｔｅｒｆａｃｅ（ＤＶＩ）及びＨｉｇｈ Ｄｅｆｉｎｉｔｉｏｎ Ｍｕｌｔｉ－Ｍｅｄｉａ Ｉｎｔｅｒｆａｃｅ（ＨＤＭＩ）装置は、ＨＤＣＰを利用する。ＤＶＤ技術の場合、例えば、準拠した装置のメーカーは、ＤＶＤ ＣＣＡのＣｏｎｔｅｎｔ Ｓｃｒａｍｂｌｅ Ｓｙｓｔｅｍ（ＣＳＳ）を利用し、ライセンス機関からＣＳＳキーを受け取る。上述されるように、ＤＴＬＡ管理者は、ＤＴＣＰ規格に従ってコンテンツを処理する準拠したＩＥＥＥ１３９４及びＵＳＢ２．０装置にライセンスを与える。ＤＴＬＡはまた、ＩＰネットワーク上で動作する装置にＤＴＣＰ／ＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）技術をライセンスする。Ｌｉｃｅｎｓｅ Ｍａｎａｇｅｍｅｎｔ Ｉｎｔｅｒｎａｔｉｏｎａｌ（ＬＭＩ）

管理者は、準拠したＤＶＤ記録装置にライセンスし、当該装置がＣｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｒｅｃｏｒｄａｂｌｅ　Ｍｅｄｉａ（ＣＰＲＭ）プロトコル及びアルゴリズムを実行することができるように、暗号キーを発行する。Ｃｏｎｔｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｌｉｃｅｎｓｉｎｇ　Ａｄｍｉｎｉｓｔｒａｔｏｒ（ＣＭＬＡ）は、Ｏｐｅｎ　Ｍｏｂｉｌｅ　Ａｌｌｉａｎｃｅ’ｓ　Ｄｉｇｉｔａｌ　Ｒｉｇｈｔｓ　Ｍａｎａｇｅｍｅｎｔ　ｖｅｒｓｉｏｎ　２（ＯＭＡ　ＤＲＭ２）規格に準拠した装置をライセンスする。

【０００７】

著作物についてライセンスされる装置のタイプを制御することに加えて、権利者はまた当該装置がどこにあるかに関心がある。例えば、テレビコンテンツは、典型的には、家計にライセンスされるが、音楽は個人にライセンスされるかもしれない。この制約は、通常は“ローカリゼーション（ｌｏｃａｌｉｚａｔｉｏｎ）”と呼ばれる。

【０００８】

ＤＴＣＰ／ＩＰ及びＯＭＡ　ＤＲＭ２と異なり、多数のライセンスされた装置が、コンピュータバスや着脱可能なディスクなどの特定タイプの伝送媒体を介し動作している。しかしながら、ＩＰネットワーキングによると、このような装置は自宅内の全てだけでなく、実際的には至る所でネットワークアクセス可能とすることができる。ＩＰネットワーキングのこの現実は、装置及びデータにローカリゼーション制約を課そうとするビジネスモデル及びセキュリティポリシーについて問題を提起する。各種ライセンス機関により利用される多くのプロトコル及びアルゴリズムを考慮すると、このタイプの問題を解決することが可能な装置及び／又は方法が効果的である。

【０００９】

［発明の詳細な説明］

本発明の以下の詳細な説明では、本発明の完全な理解を提供するため、多数の具体的詳細が提供される。しかしながら、本発明がこれらの具体的詳細なしに、又はその均等物により実現可能であるということが当業者に認識されるであろう。他の例では、本発明の特徴を不必要に不明りょうにしないように、周知の方法、手順、コンポーネント及び回路は説明されない。

【００１０】

以下の詳細な説明の一部は、コンピュータメモリ上で実行可能なデータビットに対する手順、ステップ、ロジックブロック、処理及び他の記号表現に関して提供される。これらの記述及び表現は、他の当業者に自らの作業の本質を最も効果的に伝えるため、データ処理技術の当業者により使用される手段である。ここでは、手順、コンピュータにより実行されるステップ、ロジックブロック、プロセスなどは、一般には所望の結果をもたらす自己矛盾のないステップ又は命令シーケンスであると考えられる。これらのステップは、物理量の物理的操作を必要とするものである。通常、必ずしも必要ではないが、これらの物理量は、コンピュータシステムにおいて格納、転送、合成、比較及び操作可能な電気若しくは磁気信号の形態をとる。原則的に通常の利用のため、これらの信号をビット、値、要素、シンボル、文字、項、数などと呼ぶことがときどき便利であるとわかる。

【００１１】

しかしながら、上記及び類似する用語のすべてが、当該量に適用される単に便利なラベルである適切な物理量と関連付けされることに留意すべきである。以下の説明から明らかなように、特段の記載がない場合、本発明を通じて、“受信”、“変換”、“認証”、“許可”、“識別”、“転送”などの用語を使用した記載は、コンピュータシステムのレジスタ及びメモリ内の物理（電子）量として表現されるデータを、コンピュータシステムのメモリ若しくはレジスタ又は他の同様の情報ストレージ、伝送若しくは表示装置内の物理量として同様に表現される他のデータに操作及び変換するコンピュータシステム又は同様の電子計算システムのアクション及びプロセスを参照していることが理解される。

【００１２】

［ハブによるデータ又はネットワーク装置のローカリゼーション］

図１は、本発明の実施例によるネットワーク１００のブロック図である。一実施例では、ネットワーク１００は、ネットワーク上に装置を有する家計又はホームネットワークを示す。他の実施例では、ネットワーク１００は、ネットワーク上に装置を有する企業ネットワークを示す。

【００１３】

図１の例では、ネットワーク１００は、その上で本発明の実施例が実現可能なシンク装置１１０と、ソース装置１２０と、第１ローカリゼーションハブ１３０と、第２ローカリゼーションハブ１４０とを有する。ハブ１３０は、ＤＴＣＰ／ＩＰ装置のネットワークなどのローカライズされたネットワークにおいてソースとシンクの両方のサービスを提供することができる。本発明の効果は、ソースがＤＴＣＰ／ＩＰの３ホップローカリゼーション及び７ミリ秒の制約を超えてシンクにリモートとなることを可能にする。リモートのケースでは、家計又は家族により装置をローカライズする２つのハブが存在するかもしれない。図１の例では、すべての装置は少なくともプライベートネットワーク（家計又は企業ネットワークなど）に接続され、さらにパブリックネットワーク（インターネットサービスプロバイダにより運営されるプレゼンスのインターネットポイントなど）に接続されてもよい。プライベートネットワークは、図示される具体例より多くの要素を有することが可能である。また、プライベートネットワーク上にはさらなるハブ、ソース又はシンク装置を設けることが可能である。さらに、ホームネットワークは、複数のネットワーク（複数のローカルエリアネットワークなど）から構成されてもよい。

【００１４】

図１から続けて、一実施例では、シンク装置１１０は矢印Ａに沿ってソース装置１２０からデータを受信しようとする。データは暗号化され、シンク装置１１０は、矢印Ｂに沿ってソース装置１２０又は第３の装置から解読キーを要求する。要求元がそれを使用してアクセスを許可する応答者に秘密を提示するこのようなキー確立アルゴリズムは、周知である。図１では、要求元はシンク装置１１０であり、その許可クレデンシャル（ａｕｔｈｏｒｉｚｉｎｇ　ｃｒｅｄｅｎｔｉａｌ）は、矢印Ｃの交換により登録プロセスの初期に取得されたネットワークサービス秘密である。本実施例では、シンク装置１１０は、ＩＰ　Ｓｅｃｕｒｉｔｙ（ＩＰｓｅｃ）プロトコルにより矢印Ｃの交換をセキュアにする。ある機関により署名されたデジタル証明書を利用して、各当事者が自らの権限を証明するとき、Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ（ＩＫＥ）を使用してセキュア接続を確立することは、ネットワークセキュリティ技術において周知である。本発明の実施例は、この目的のためＤｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｌｉｃｅｎｓｅ　Ａｕｔｈｏｒｉｔｙ（ＤＴＬＡ）クレデンシャルを利用する。クレデンシャルは、シンク装置１１０のメモリにおいて初期化される。（例えば、装置アイデンティティのクレデンシャルは、ＤＴＬＡ許可のためルートパブリックキーと共にメモリにある。）一実施例では、ソース装置１２０とシンク装置１１０は、それら各自のキーとＤＴＬＡクレデンシャルを使用して互いに認証する。本発明の一実施例では、シンク装置１１０はさらに、それが特定のネットワークサービス上のローカリゼーションハブにより登録されたことを証明するため、それのネットワークサービスクレデンシャルをわたし、ソース装置１２０は、認証プロセスのため当該クレデンシャルを利用する（例えば、あるネットワーク上で登録されている装置に制限されるコンテンツへのアクセスを条件付きで許可するためなど）。一実施例では、ネットワーク装置又はハブは、インターネットサービスプロバイダからネットワークサービスクレデンシャルを取得する。これがネットワークサービスインタフェースに対しハブ又は装置をローカライズし、ハブがケーブルＤＯＣＳＩＳ（Ｄａｔａ　Ｏｖｅｒ　Ｃａｂｌｅ　Ｓｅｒｖｉｃｅ　Ｉｎｔｅｒｆａｃｅ　Ｓｐｅｃｉｆｉｃａｔｉｏｎ）モデムなどのモデムと共存するとき、物理的インタフェースを利用する。

【００１５】

ある実施例では、ハブ装置１３０とシンク装置１１０は、シンク装置がネットワークサービスクレデンシャルを有しないとき、ＤＴＬＡクレデンシャルを使用して相互に認証する。各装置は、第１ネットワークサービスの登録後に、ＤＴＬＡとネットワークサービス

クレデンシャルのペアを使用する。

【００１６】

他の実施例は、ＤＴＬＡの代わりに又はそれに加えて、Ｏｐｅｎ　Ｍｏｂｉｌｅ　Ａｌｌｉａｎｃｅ（ＰＭＡ）のＣｏｎｔｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｌｉｃｅｎｓｅ　Ａｄｍｉｎｉｓｔｒａｔｉｏｎ（ＣＭＬＡ）などの他の機関や、本発明のローカリゼーション機能を搭載したＭｉｃｒｏｓｏｆｔ　ＤＲＭ１０などの専用システムを利用するようにしてもよい。

【００１７】

一実施例では、矢印Ｃの交換は、シンク装置とハブ装置との間の家計ネットワーク内ですべて行われ、また、管理対象とされるＩＰアドレスのＤｙｎａｍｉｃ　Ｈｏｓｔ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ（ＤＨＣＰ）サーバが実行される。他の実施例では、ハブは、Ｕｎｉｖｅｒｓａｌ　Ｐｌｕｇ　ａｎｄ　Ｐｌａｙ（ＵＰｎＰ）プロトコルを利用して、検出又は他の目的のためホームネットワーク装置と通信する。他の実施例では、矢印Ｃの交換が、それのハブからサービスプロバイダのネットワークサービスクレデンシャルを取得するため、ホームネットワーク装置とサービスプロバイダの装置との間で行われる。これは、ケーブルのブロードバンドネットワークインタフェースやデジタル加入者線（ＤＳＬ）モデムなどのネットワークサービスインタフェースに対しクレデンシャルをローカライズする。さらなる他の実施例では、サービスがマルチホーム化（ｍｕｌｔｉ－ｈｏｍｅｄ）されるとき、装置がさらなるクレデンシャルを取得又はクエリすることが可能な矢印Ｃ’の交換が行われる。（マルチホーム化された装置は、各々が自らのネットワークサービスクレデンシャルを有する複数のネットワークサービスインタフェースを有する。）

【００１８】

図１を参照するに、各矢印のトランザクションは秘密とされ、インテグリティがプロテクトされる。一実施例では、ソース、シンク及びハブの各装置は、パブリック／プライベートキーペアを有する。ライセンス機関が装置のパブリックキーを含むクレデンシャルを署名し、装置ライセンス又はセキュリティポリシーの準拠を証明することは知られている。ある実施例は、ライセンス機関としてＤＴＬＡを利用する。

【００１９】

図２は、本発明の実施例による異なる登録状態を示す装置状態遷移図２００である。この図は、ネットワークサービスクレデンシャルがどのように不揮発性の装置メモリにおいて初期化、維持、削除及び他のクレデンシャルと置換されるか規定する。図２は、ある装置が１つのネットワークサービスに登録することが許可されている実施例を示す。異なる実施例は、複数の登録又はカウントのみの登録又は単なるトラック状態を許容するかもしれない。

【００２０】

本発明の実施例によると、不揮発性装置メモリは、装置メーカーのＤＴＬＡ証明書のコピーにより初期化される。この状態は、状態遷移図２００において“ＨＡＳ　ＭＡＮＵＦＡＣＴＵＲＥＳ’Ｓ　ＣＲＥＤＥＮＴＩＡＬ”２１０として参照される。この状態は、状態遷移図２００において“ＥＭＰＴＹ”２３０として参照される。ＥＮＲＯＬＬトランザクション（図１の矢印Ｃ内）は、装置の装置メーカーのクレデンシャルをネットワークサービスクレデンシャルと置換する。この状態は、状態遷移図２００において“ＨＡＳ　ＮＥＴＷＯＲＫ－ＳＥＲＶＩＣＥ　ＣＲＥＤＥＮＴＩＡＬ”２２０として参照される。以降のＲＥ－ＥＮＲＯＬＬトランザクション（図１の矢印Ｃ内）は、現在のネットワークサービスクレデンシャルの使用を認証する。ネットワークサービス装置及びオペレータは、一実施例では、装置がまず自宅や職場に設置されるとき、又は新たな若しくは異なる家計若しくは企業ネットワークに移るとき、ユーザにより実行される頻繁でない手順であるＥＮＲＯＬＬ又はＲＥ－ＥＮＲＯＬＬをすべての装置が自動的に実行することを必ずしも可能にする必要はない。モバイルのケースは特別である。なぜなら、ソース装置は、ホームゲートウェイの外部に検出されるものなど、非ローカルＩＰアドレスによりローカルクレデ

ンシャルを受け付ける可能性があるためである。他の実施例では、ネットワーク登録は、完全にユーザの制御下にあり、装置は完全にユーザ制御下で登録及び再登録されるかもしれない。

【００２１】

図２を参照するに、本発明の実施例によるＥＮＲＯＬＬトランザクションがさらに説明される。物理的な近接性よりも、本発明は、データ処理（ネットワーク）装置とネットワークサービス（ローカリゼーションハブ）装置との間の論理的関連付けを利用し、ネットワーク（ソース又はシンク）装置がそれのネットワーク上に登録すると、署名されたクレデンシャルが発行される。クレデンシャルは、典型的には、アクセスについてそれのシグネチャが黙示的な認証を提供するある機関を識別するものである。ネットワークサービスクレデンシャルは、ネットワークサービスを識別し、サービスプロバイダの名前又はアドレスと任意的な加入者情報とを含む。ある実施例では、名前は大きな（１６バイトなど）の乱数であり、アドレスはＩＰｖ４又はＩＰｖ６アドレスである。

【００２２】

ネットワークサービスプロバイダは、ブロードバンドモデムのＭＡＣ（Ｍｅｄｉｕｍ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）アドレスを含むネットワークとのインタフェースと加入者とを関連付ける各種手段を有する。一実施例では、“加入者識別子（ＩＤ）”として参照されるかもしれないネットワーク加入者の明示的識別子が規定される。加入者ＩＤは、ネットワークサービスが加入者のホームネットワークを識別するのに使用する情報を伝達するものである。ＤＨＣＰ規格によると、ネットワークアドレスが加入者の装置にわたされる前に、加入者ＩＤオプションが物理ネットワーク情報と共に分離される。本発明の一実施例では、登録されると、ネットワークサービス識別子が、デジタル署名されたネットワークサービスクレデンシャルの形式により装置に返される。

【００２３】

ある実施例では、機関がネットワークサービスクレデンシャルを発行するか、又はこの役割をネットワークオペレータ又は装置ベンダーに委託する。当該機関は、装置に関する１以上の事項について証明する証明書を発行する。マルチメディア装置では、ライセンス機関は、当該装置があるデータクラスを処理することが許可されていることを証明するデジタル署名されたクレデンシャルを発行する。このようなライセンス機関が、ＤＶＤ、ＩＥＥＥ１３９４、ＯＭＡ及びデジタルビデオ装置について存在する。ＤＴＬＡは、ＩＥＥＥ１３９４バス、ＩＰネットワーク及び他の通信メディア上のＤＴＣＰ装置にライセンスを付与する。

【００２４】

一実施例では、装置はネットワークサービスクレデンシャルのための署名機関として、ＤＴＬＡ又は他の装置ライセンス機関を利用する。他の実施例では、装置はネットワークサービスの証明書機関を利用する。さらなる他の実施例では、装置は装置ベンダーのクレデンシャルを受け付ける。これらの実施例では、クレデンシャルは、装置及びネットワークサービスプロバイダの暗号アイデンティティ（Ｘ．５０９証明書による公開鍵など）を含む。ネットワーク（シンク）及びハブ装置は、ＤＴＣＰやＩＫＥ手順などの認証されたキー確立においてこれらのクレデンシャルを利用する。クレデンシャルを装置に発行する機関は、ネットワークサービスとの関連付け（登録）、ネットワークとの関連付け解除（失効）、及び新たなネットワークとの関連付け（再登録）のための方法を指示する。

【００２５】

図３を参照するに、ある実施例では、真理テーブル３００に示されるように、モバイル及び家計トランザクションなどの各事項が列記される。一実施例では、非ローカルアドレスを有する装置がローカルクレデンシャルにより認証するモバイル処理が規定される。本実施例は、インターネット上のリモート装置に拡張されるホーム及び企業ネットワークのローカリゼーションの物理的でなく論理的概念を利用する。さらに、本発明は、インターネットとの接続を有さないネットワークと、複数のインターネットサービスプロバイダ（ＩＳＰ）の接続（“マルチホーム化”されるなど）を有するネットワークとに適用される

。ホームネットワークは、典型的には、インターネット接続が一時的に又は永久的に利用可能でないときでさえ、家計装置間で動作する。

【００２６】

図３を参照するに、真理テーブル３００は、何れのタイプの装置（ここでは、家計、モバイル、ビジター又はフォーリン（ｆｏｒｅｉｇｎ）装置として示される）がネットワークサービス（ムービー又は他のメディアのサーバなど）へのアクセスを取得しようとしているか決定するのに利用可能である。一実施例では、真理テーブル３００は、シンク装置と同じネットワーク上のサーバ又はソース装置の認証ロジックに配置される。ソース装置上のデータへのアクセスを取得しようとする装置のタイプは、それのＩＰアドレス及びネットワークサービスクレデンシャルに基づき決定することが可能である。家計装置がアクセスを取得しようとする場合、それはネットワークサービス装置と同一のＩＰアドレス範囲（サブネットなど）及び同一のネットワークサービスクレデンシャルとを有するであろう。モバイル装置である場合、それはネットワークサービス装置と同一のネットワークサービスクレデンシャルと異なるＩＰアドレスとを有するであろう。ビジター装置である場合、それは、ネットワークサービス装置と同一のＩＰアドレス範囲（サブネットなど）と異なるネットワークサービスクレデンシャルとを有するであろう。それがフォーリン装置である場合、それは、ネットワーク装置と異なるＩＰアドレスと異なるネットワークサービスクレデンシャルとを有するであろう。

【００２７】

コンテンツのアイテムは、例えば、特定タイプの装置のみに利用可能であるとラベル付けすることが可能である。一実施例では、家計装置のみに利用可能であると識別されたコンテンツのアイテムのみが、真理テーブル３００に従って家計装置として識別されたシンク装置に提供されるであろう。

【００２８】

図４は、家計ネットワークモデル４００の実施例を示すブロック図である。家計ネットワークモデル４００上で、各ソース及びシンク装置（４３０，４４０及び４５０）は、一実施例では、モデム及び／又はＤＨＣＰサーバと共存するローカルハブ４２０により登録され、さらにＩＳＰネットワークのＩＳＰローカリゼーションハブ４１０により登録される。ローカルハブ４２０は、一実施例では、ネットワーク装置にネットワーククレデンシャルを発行するためのそれの機関としてメーカーのクレデンシャルを利用する。一実施例では、ローカルハブ４２０は、ＩＳＰローカリゼーションハブ４１０に登録し、その後にネットワークサービスクレデンシャルをホームネットワークハブに通知する。これにより、ハブ機能が自宅にではなくＩＳＰにのみ存在する場合でなければ（ローカリゼーションハブを所有及び運営する家計を解放する実施例）、ホームネットワークの存在及びアイデンティティは、ＩＳＰネットワークサービスに開示されない。本実施例では、ハブ４２０は存在せず、各装置は直接ハブ４１０に登録する。しかしながら、２つのハブ４１０と４２０の両方が動作中であるとき、ネットワーク装置は、ローカルネットワークサービス用とＩＳＰのネットワークサービス用のクレデンシャルのペアを受け取るかもしれない。従って、ホームネットワーク上のデータ処理装置は、ネットワークサービスのためのクレデンシャル（署名されたデジタル証明書など）の形式によりネットワークサービスに関連付けされる。これは、ＤＨＣＰと共にネットワークサービスをＤＨＣＰサーバ又はリレイと共存したものから独立した実施例において真である。

【００２９】

図５は、本発明の実施例による装置を秘匿化する方法５００のフローチャートである。フローチャート５００には具体的なステップが開示されているが、このようなステップは例示的なものである。すなわち、本発明の実施例は、フローチャート５００に記載されるステップの変形又は他の（追加的な）各種ステップを実行するのに適している。フローチャート５００の各ステップは、提供されたものと異なる順序により実行されてもよく、フローチャート５００のステップのすべてが実行される必要がないということが理解される。

【００３０】
ステップ５１０において、クレデンシャルが自宅のネットワーク装置において受信される。当該クレデンシャルは、装置がネットワーク又はサービスに登録されていることを示す。
【００３１】
ステップ５２０において、クレデンシャルは、装置の不揮発性メモリに格納される。クレデンシャルは、装置をネットワークに接続し、他のネットワークのポリシーに従ってこれらのネットワークへの装置アクセスを制御する。
【００３２】
ステップ５３０において、ネットワーク装置は、コンテンツ又はサービスに対するリクエストの一部としてクレデンシャルを提供する。当該リクエストは、ハブ自体にされてもよく、又はハブクレデンシャルを受け付けるファイアウォール、ムービーなどのライセンスされたデータのプロバイダにされてもよい。ハブ、ゲートウェイ、サーバなどは、このクレデンシャルを利用して装置を認証し、認証されると、許可された装置にサービスへのアクセスが提供される。装置が許可されているか否かは、実施例では真理テーブル３００及び／又は他のコンテンツに対するライセンス制限によって決定される。装置が家計のＩＰアドレスを有し、家計ネットワーク上に登録される場合、例えば、それは家計コンテンツにアクセスすることが許可され、モバイル又はフォーリン装置は許可されないかもしれない。クレデンシャルの提供及び認証プロセスは、装置のユーザに透過である。
【００３３】
すなわち、署名されたクレデンシャル（ネットワークサービスクレデンシャル）は、当該データがプライベートであるか、又は特定の家計又はホームネットワークにローカライズされることがライセンスされているとき、ネットワークを介したデータアクセスを可能及び制御するのに利用される。一般に、特定の位置にあるブロードバンドサービスへの加入者などネットワークへのローカリゼーションを提供するため、ネットワーク装置とハブ装置との間の論理的関連付けが利用可能である。例えば、クレデンシャルは、ある都市のホームネットワーク上の装置を、他の都市のケーブル企業又は電話企業の加入者と関連付けることができる。このローカリゼーション機能は、ＤＲＭローカリゼーションスキームのプロキシー機能とトランスクリプションを提供するハブにとって有用である。
【００３４】
ネットワークサービスクレデンシャルは、装置上に格納し、装置が属するネットワーク又はサービスを特定するのに利用可能である。装置は、他のネットワークサービスが再登録を許可するまで、特定のネットワークサービスに接続され続け（ネットワークサービスクレデンシャルを用いた論理的関連付けを介し）、特定のライセンス機関又はセキュリティポリシーの条件に従って実行される。ネットワークサービスクレデンシャルを利用して、複数のネットワークサービスの関連付けが可能とされるが、装置は一度に１つのみのネットワークサービス関連付けしか許可されない。しかしながら、ネットワーク装置が１つのネットワークサービスに不正に接続される場合、当該ポリシーが登録を１つのネットワークサービスのみに制限するものであるとき、他の何れのネットワークサービスへの不正に接続することを防ぐことができる。ホーム又は企業ネットワークに対するデータ伝送制御などの上記要求は、これらのネットワーク上及びネットワークに対するデータ転送を制御することが可能である。
【００３５】
［ハブに対しデータ及び装置をローカライズするシステム及び方法］
図６は、本発明の実施例が実現可能なシステム６００のブロック図である。一般に、システム６００は、情報及び命令を処理するプロセッサ６０１と、プロセッサ６０１のため情報及び命令を格納するランダムアクセス（揮発性）メモリ６０２と、プロセッサ６０１のため静的な情報及び命令を格納する読み出し専用（不揮発性）メモリ６０３と、コンテンツを格納するための磁気若しくは光ディスク及びディスクドライブなどのデータ記憶装置６０４とを有する。システム６００は、情報及びコマンド選択を通信するため、任意的

なユーザ出力装置と任意的なユーザ入力装置とを有するかもしれない。

【００３６】

上述されたように、著作物についてライセンス付与される装置のタイプを制御することに加えて、権利者は装置の設置場所であり、“ローカリゼーション”と通常呼ばれる制約に関心がある。本発明の実施例によると、システム６００は、１以上のライセンスされたインタフェースを統合し、ネットワーク装置、特にＤＶＤ　ＣＣＡ、ＤＴＬＡ、ＣＭＬＡ、ＬＭＩ及びＨＤＣＰなどの著作物の配信を制御することを担当する機関によってライセンスされた装置にネットワークローカリゼーションサービスを提供する“ローカリゼーションハブ”として利用される。このハブは、ライセンスされたインタフェースと従来のネットワークインタフェースを統合したものであり、上述したライセンス機関のローカリゼーションポリシーとの準拠性を維持しながら、ローカリゼーションのレイヤを追加する。図７と共に、付加情報が以下で与えられる。一般に、ハブは、ネットワーク装置（ここでは、娯楽装置、クライアント装置、又はシンク若しくはソース装置とも呼ばれる）をネットワークの場所と関連付ける。特に、加入者により所有されるホームネットワークは、ケーブル、通信企業（ｔｅｌｃｏ）又は他のブロードバンドサービスと関連付けすることが可能である。ハブは、以下で詳述されるように、ホームネットワーク内又はネットワークサービスプロバイダに配置されるかもしれない。ハブは、家計によって所有され、又はホームネットワークと関連付け、ホームネットワークをネットワークサービスの加入と関連付けることによって家計にライセンスされた装置及びデータを“ローカライズ”するのに利用可能である。

【００３７】

図７は、各種ライセンス機関からの論理インタフェースの具体例を示す本発明の一実施例によるローカリゼーションは部７０２の“外部”の表示を示す。図７の例では、ハブ７０２はまた、イーサネット（登録商標）やＷｉＦｉ（Ｗｉｒｅｌｅｓｓ　Ｆｉｄｅｌｉｔｙ）ネットワークなどのいくつかのタイプのネットワークを介しＩＰサービスを実行する少なくとも１つのインタフェース７０４を有する。ＤＴＣＰ／ＩＰ及びＯＭＡ　ＤＲＭ２インタフェース７０６及び７０８はまたＩＰネットワーク上で実行され、インタフェース７０６及び７０８は共有ＩＰインタフェース上で多重化されるかもしれない。

【００３８】

一実施例では、クライアント装置（図７には図示せず）が、図１～５に関して上述されたように、ネットワークを介しハブ７０２に登録される。他の実施例では、ハブ７０２は、クライアント装置自体の内部に埋め込まれてもよく、この場合、図２（及び以降の図９）によって上述されたものなどの明示的な登録交換は必要でないかもしれない。クライアント装置は、ハブ７０２から証明書を取得するため、Ｓｉｍｐｌｅ　Ｃｅｒｔｉｆｉｃａｔｅ　Ｅｎｒｏｌｌｍｅｎｔ　Ｐｒｏｔｏｃｏｌなどの標準的なプロトコルを使用してもよい。一般に、上述されたような機構を利用して、ハブ７０２は、各種装置を加入者のホームネットワークなどと関連付けすることが可能であり、これにより当該装置は、ホームネットワーク害の装置だけでなく、互いに各自のネットワーク関連付けを証明することが可能である。

【００３９】

ここで使用される“ハブ”という用語は、一般に動作のローカリゼーションポイントを表している。ハブのスポークは、スポークはまた他のハブと接続されるかもしれないが、上述したインタフェースとすることが可能である。“ハブ”という用語は、リピーター（ｒｅｐｅａｔｅｒ）や他の同様の装置などに限定されると解釈されるべきでない。

【００４０】

基本的に、本発明の実施例によると、ハブ７０２がホームネットワーク（家計）を規定する。家計毎に複数のハブが存在するかもしれない。例えば、ルータやファイアウォールがホームネットワークの装置に対する個別のアドレス割当てを利用してホームネットワークをセグメント化するときなど、家計に複数のアドレススペースが存在するとき、家計毎に複数のハブが存在するかもしれない。一実施例では、個別のアドレスセグメント上にあ

るハブは、ホームネットワークに対する“ルートハブ”に登録することが可能である。（ルートハブは、複数のハブの１つであってもよい。）他の実施例は、ドングル（ｄｏｎｇｌｅ）、トークン装置又はスマートカードなどの装置を利用して、ハブを関連付け又は装置をハブに関連付ける。さらなる他の実施例では、ユーザは、インタラクティブ音声応答システムの認証された電話をハブに配置する。コンピュータセキュリティの当業者は、人間の物理的アクションを利用して関連付けを行い、これにより、インターネットを介したなりすましにより動作する装置がハブと不正な関連付けを行うことを回避する効果を理解するであろう。

【００４１】

図８は、本発明の実施例によるローカリゼーションハブ７０２（家計ネットワーク８１６上）とローカリゼーションハブ８１０（ＩＳＰネットワーク８１２上）とを有するネットワーク８００のブロック図である。ネットワーク８１６は、ローカルエリアネットワーク（ＬＡＮ）と呼ばれ、ネットワーク８１２は、ワイドエリアネットワーク（ＷＡＮ）と呼ばれるかもしれない。

【００４２】

家計ネットワーク８１６と通信するＩＳＰネットワークは複数存在するかもしれない。本実施例では、ゲートウェイ８１４は、家計ネットワーク８１６と１以上のＩＳＰネットワークとの間の通信インタフェースを提供する。クライアント装置８０４、８０５及び８０６は、あるタイプのネットワーク装置（ネットワークＤＶＤプレーヤーなど）とすることが可能である。一実施例では、家計ネットワーク８１６はＩＥＥＥ８０２に互換したローカルエリアネットワークである。

【００４３】

他の実施例では、ハブ７０２はゲートウェイ８１４に埋め込まれている。さらなる他の実施例では、ハブ７０２はクライアント装置８０４、８０５及び８０６の１つに埋め込まれている。さらなる他の実施例では、ハブ７０２は独立した装置である。

【００４４】

本実施例では、家計ハブ７０２はＩＳＰハブ８１０と関連付け（登録）されている。一実施例では、図１～５に関して上述されるように、ハブ７０２はハブ８１０に登録されている。他の実施例では、セキュアなバーチャル・プライベート・ネットワーク（ＶＰＮ）が、ＩＰｓｅｃ接続などを利用してハブ７０２と８１０を接続する。

【００４５】

ハブ７０２とハブ８１０との関連付けは、ハブ７０２がネットワークサービス加入者の場所に設置されているという事実を証明する。一実施例では、“場所（ｌｏｃａｔｉｏｎ）”は、ネットワークのアドレススペース（ネットワークに割り当てられたＩＰアドレスの範囲など）に従って規定され、ＤＨＣＰサーバなどにより割り当てられ、ネットワークの物理的な位置でないネットワーク位置である。他の実施例では、“場所”は、特定のアドレスなどブロードバンドネットワークサービスとのサービスインタフェースを特定する。これらの実施例では、ハブが登録されているとき、場所はハブの位置に限定されない。しかしながら、“場所”という用語の使用は、モバイル又はマルチホーム化された装置などが家計からコンテンツにアクセスすることを可能にするよう拡張することができる。一実施例では、装置は、各装置間のセキュアな関連付けを確立するため、予め共有された又は公開されたキーを搬送する“クーリエイントロデューサ（ｃｏｕｒｉｅｒ ｉｎｔｒｏｄｕｃｅｒ）”方法を利用して、ハブと関連付けすることが可能である。Ｅａｓｙ Ｓｅｃｕｒｅ Ｄｅｖｉｃｅ Ｐｏｓｉｔｉｏｎｉｎｇ（ＥＺＳＤＰ）（Ｅａｓｙ Ｓｅｃｕｒｅ Ｄｅｖｉｃｅ Ｄｅｐｌｏｙｍｅｎｔとも呼ばれる）は、各装置間のセキュアな関連付けを可能にする。ＥＺＳＤＰは、ユーザが２つの装置の間のセキュアな関連付けを確立することを可能にするウェブブラウザインタフェースとして実現可能な信頼されたイントロデューサモデルを利用する。あるいは、ウェブブラウザの代わりに、ウェブブラウザ又はパーソナルコンピュータが導入又は関連付けを行うのに利用可能でない環境に適応するため、電話が利用可能である。スマートカードやセキュリティドングルなどの他の方法

がまた、ハブと装置との間のセキュアな関連付けを確立するのに利用可能である。

【００４６】

ハブ７０２とハブ８１０との関連付けはまた、家計ネットワーク８１６にある他の装置（クライアント装置８０４～８０６など）を登録する権限がハブ７０２に委託可能であることを意味する。ハブ７０２とこれらの他の装置との関連付けは、これら他の装置が加入者の家計ネットワークに関連付けされているという事実を証明する。一実施例では、家計ネットワーク８１６上のクライアント装置の個数とタイプがネットワークサービスプロバイダには見えない可能性があることに留意されたい。しかしながら、他の実施例では、ハブ７０２の機能は代わりにハブ８１０により提供され、この場合、家計ネットワーク上のクライアント装置は、ネットワークサービスプロバイダに可視化されるであろう。

【００４７】

図８の例では、クライアント装置８０６はハブ７０２に直接接続され、クライアント装置８０４及び８０５は家計ネットワーク８１６のファブリックを介しハブ７０２と通信する。図８において、ハブ７０２はクライアント装置８０４～８０６の間のパス上にあると示されていない。なぜなら、ハブ７０２はクライアント装置８０４～８０６にアクセス可能であり、それらにサービスを提供するが、コンテンツ（著作物など）は必ずしもクライアント装置を通過する必要がないためである。

【００４８】

クライアント装置８０４～８０６は、上述されるように、ライセンス機関に従ってライセンスされてもよい。また、ハブ７０２は複数のＩＰ又はライセンスされた装置インタフェースを有してもよい。

【００４９】

図９は、本発明の実施例によるネットワーク登録プロセスを示す。本実施例では、ハブ７０２は、ＩＳＰインタフェース９２０を介しネットワークサービスプロバイダのハブ９１０と関連付けされる。ネットワーク登録プロセスの一部として、ハブ７０２は、それが要求元のクライアント装置を登録することがライセンス機関又はメーカーに許可されていることを示すため、適切なクレデンシャル（証明書ストア）をフェッチしてもよい。

【００５０】

クライアント（シンク）装置９０１及び９０２からのネットワーク登録に対するリクエストが、ハブ７０２に対する各自のインタフェース９３０又は９３１を通過する。インタフェース９２０、９３０及び９３１は、図７の例に関して上述されたように、ホームネットワークにおいて使用される各種タイプのインタフェースに対応する。従って、インタフェース９２０、９３０及び９３１は、一般に有線又は無線インタフェースとすることが可能であり、より詳細にはイーサネット（登録商標）、ＷｉＦｉなどのインタフェースとすることが可能である。

【００５１】

図１０は、本発明の一実施例によるローカリゼーションハブにより装置（クライアント装置など）を登録するプロセスを示すフローチャート１０００である。図９を参照するに、ステップ１００１において、ローカリゼーションハブ７０２はクライアント装置（クライアント装置９０１など）から登録リクエストを受け取る。

【００５２】

ステップ１００２において、ハブ７０２は、“クーリエイントロデューサ”による予めの関連付けなどの上述した各種方法を利用して、要求元のクライアント装置９０１がハブ７０２により管理される家計ネットワークのメンバーであると確認する。一実施例では、クライアント装置９０１が予め共有される同一の秘密を有し、またハブ７０２と同一のアドレススペースを共有する場合、クライアント装置９０１が家計ネットワークのメンバーであるということが示され、フローチャート１０００がステップ１００３に移行する。そうでない場合、フローチャート１０００はステップ１００４に移行する。

【００５３】

ステップ１００３において、ハブ７０２は、それが要求元のクライアント装置９０１を

登録するための機関を有していることを確認する。一実施例では、ハブ７０２は、装置９０１がライセンス機関又はメーカーにより発行された適切なクレデンシャルを有することを確認し、要求元のクライアント装置９０１を登録することができる。一実施例では、ハブ７０２は、それが要求元のクライアント装置９０１と同一のライセンス機関により発行されたクレデンシャルを有していることを確認する。他の実施例では、ハブ７０２は、クーリエイントロデューサ又は同様の技術によって許可される自己署名された証明書などのクレデンシャルを有する装置を登録することが可能である。

【００５４】

ハブ７０２は、サーバ、ファイアウォール、ビデオレコーダ、カメラ、ジュークボックスなどのホームネットワーク装置におけるアクセスを許可及び制御するため、クレデンシャルが利用可能となるように、登録された装置にクレデンシャル（限定されるものではないが、Ｘ．５０９証明書及び対称秘密クレデンシャルなど）を発行する。本発明の実施例によると、ハブ７０２に登録された装置は、同様にハブ７０２に登録された他の装置により制御されるリソースにアクセスすることができる。これは、ホームネットワークとの密接な関係を確立することが（ネットワーク所有者又はライセンス機関の何れかによって）明示的に許可されていない場合、ホームネットワークへの外部者（ネットワークサービスプロバイダを含む）によるアクセスを効果的に制限する。このような密接な関係は、外部者が制御されたコンテンツを共有することを可能にするであろう（コンテンツのライセンス条項によって許可される場合）。

【００５５】

ステップ１００４において、クライアント装置９０１がハブ７０２により管理される家計ネットワークのメンバーであることが示されていない場合（上記ステップ１００２を参照されたい）、あるいはハブ７０２が要求元のクライアント装置を登録することが許可されていない場合（上記ステップ１００３を参照されたい）、登録リクエストは拒絶される。

【００５６】

図１１は、本発明の一実施例によるハブ（チャイルドハブ）を他のハブ（ペアレントハブ）により登録するプロセスを示すフローチャート１１００である。一般に、フローチャート１１００のプロセスは、複数のハブを特定の家計ネットワークに関連付けるため実行される。チャイルドハブは、家計ネットワークの複数のハブの１つであってもよく、ペアレントハブは、ルートハブとして指定される家計ネットワークのハブであってもよい。あるいは、ペアレントハブは、図８のＩＳＰローカリゼーションハブ８１０であってもよい。

【００５７】

図１１のステップ１１０１において、ペアレントハブは、チャイルドハブから登録リクエストを受け取る。ステップ１１０２において、ペアレントハブは、要求元のチャイルドハブがペアレントハブにより管理される家計ネットワークのメンバーであることを確認する。一実施例では、ペアレントハブとチャイルドハブが同一のＤＯＣＳＩＳケーブルインタフェース又はＤＳＬインタフェースを介し接続されている場合、チャイルドハブは、ペアレントにより登録許可される。他の実施例では、チャイルドハブは、それが適切な認証（クーリエイントロデューサからの予め共有された秘密、パス段階など）を利用してＩＰｓｅｃ接続などのペアレントハブとの許可されたセキュアな接続を確立する場合、登録可能である。チャイルドハブが登録可能である場合、フローチャート１１００はステップ１１０３に移行する。そうでない場合、フローチャート１１００はステップ１１０４に移行する。

【００５８】

ステップ１１０３において、ペアレントハブは、それが要求元のチャイルドハブを登録する権限を有することを確認する。例えば、ペアレントハブは、それがライセンス機関又はメーカーにより発行される適切なクレデンシャルを有しているか判断し、要求元のチャイルドハブを登録することが可能である。

【００５９】
ステップ１１０４において、要求元のチャイルドハブがペアレントハブにより管理される家計ネットワークのメンバーであることが示されていない場合（上記ステップ１１０２を参照されたい）、あるいはペアレントハブが要求元のチャイルドハブを登録することが許可されていない場合（上記ステップ１１０３を参照されたい）、登録リクエストは拒絶される。
【００６０】
上記プロセスの完了後、ホームネットワークがインターネットから切断される場合、例えば、ホームネットワーク（クライアント）装置はサービスプロバイダのハブ（図８のハブ８１０など）に従属しない。なぜなら、ハブ８１０は家計ハブ（図８のハブ７０２など）に権限を委任しているためである。従って、装置は、当該サービスプロバイダのインタフェースがダウンし、装置がサービスプロバイダに関連付けされていない他のリンクを介しインターネットにアクセスしているときでさえ、それがサービスプロバイダにより登録されていることを示す証明書を提供することが可能である。これは、ホームネットワーク上にハブを有するための１つの利点である。
【００６１】
フローチャート１０００及び１１００において具体的なステップが記載されているが（それぞれ図１０及び１１）、このようなステップは一例である。すなわち、本発明の実施例は、フローチャート１０００及び１１００に記載されたステップの変形又は他の（追加的な）各種ステップを実行するのに適している。フローチャート１０００及び１１００の各ステップが提供されるものと異なる順序により実行されてもよく、フローチャート１０００及び１１００のステップの必ずしもすべてが実行されなくてもよいということは理解されるであろう。
【００６２】
すなわち、本発明の実施例によると、ハブは装置（又は他のハブ）とネットワーク（具体的には、家計又はホームネットワーク）とを関連付ける。ハブはホームネットワークに付属されてもよく、又はネットワークサービスプロバイダ装置に実現されてもよい。すなわち、クライアント装置（メディアプレーヤーなど）は、家計ネットワーク上のハブにより登録可能であり、又は装置はサービスプロバイダにより操作されるハブにより直接登録されてもよい。
【００６３】
ネットワークとの関連付け（登録）は、ハブ又はネットワーク装置（ネットワーク娯楽装置など）がライセンスされたコンテンツ（映画の著作物など）を受信することが許可されている加入者のネットワークに属するものとして特定されることを可能にする。装置に固有のアクセス制御又はコンテンツに固有のアクセス制御に着目した従来技術と対照的に、本発明による実施例は、ライセンスされたデータへのアクセスを受け付けるための条件としてネットワーク位置又はネットワーク関連付けを利用する。これが各種ライセンス機関により使用される多くのプロトコル及びアルゴリズムに関して実現されることは重要である。
【００６４】
［ハブにおけるＤＲＭローカリゼーションスキームのプロキシートランスクリプション］
図７を参照するに、本発明は、図７の１つのインタフェースの他に対するＤＲＭローカリゼーションを“トランスクライブ（ｔｒａｎｓｃｒｉｂｅ）”するためのプロキシーとして動作可能である。例えば、ＤＴＣＰ／ＩＰインタフェース６０６を介したやりとりは、ＷＡＮ　ＩＰインタフェース７０４との間でトランスクライブすることができる。このようなトランスクリプションは、ＤＴＣＰなどを管理するライセンス機関（ＤＴＬＡ）が、ＩＰインタフェースを介しＤＴＣＰ／ＩＰコンテンツをハブが出力することを許可している場合に限って正当に実行可能であり、それは、往復時間及びホップカウントを制限するＤＴＣＰ／ＩＰ方法と異なってローカライズされる。ＤＴＣＰ／ＩＰは、それのソース及びシンクのためのローカリゼーションスキームを有し、出力プロトコルは適切なローカ

リゼーション方法を有する必要がある。本発明は、ネットワークサービスクレデンシャルを利用してホームネットワークをネットワークサービスにローカライズする。一実施例では、プロトコルは、ネットワークサービスクレデンシャルを利用したＩＰｓｅｃ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｈｅａｄｅｒ（ＡＨ）プロトコルである。ＤＴＣＰ／ＩＰ及びＡＨフローをトランスクライブするため、ハブはキー管理に参加し、ライセンスされているデータのための解読キーへのアクセスを制御する。

【００６５】

ＤＴＣＰ／ＩＰやＯＭＡ　ＤＲＭ２などのライセンスされたシステムは、ライセンスされたデータを当該データへのアクセスを制限する手段として暗号化する。これらのライセンスされたシステムは、データに対する解読キーを管理及び確立するためのキー管理プロトコルを有する。エンドポイント装置は、あるアイデンティティを認証し、それがキーを受け取ることが許可されていることを証明する。それは“認証キー確立（ＡＫＥ）”と通常呼ばれている。

【００６６】

ＤＴＣＰ／ＩＰ及び他のライセンスされたシステムは、ライセンス機関が許可された装置に発行するクレデンシャルを使用してＡＫＥを実行する。他の何れかの証明機関（ＣＡ）又は公開鍵インフラストラクチャ（ＰＫＩ）について、ライセンス機関は、装置の公開鍵又は名前により装置を特定するクレデンシャルを署名する。装置は、ライセンスされたデータのソースをクレデンシャルに提示する。このソースは、平文キーへのアクセスを付与する条件として有効なクレデンシャルを要求する。装置は、ライセンスされたデータ（娯楽コンテンツなど）を受け付け、解読キーへのアクセスを取得するためのそれの認証を証明するため、クレデンシャルを提供する。一部のケースでは、認証判定は、関連する機関がクレデンシャルを発行し、その後当該クレデンシャルを失効していないことを保証するため、デジタル署名の単一のチェックから構成される。他のケースでは、ライセンスされたシステムは、Ｍｉｃｒｏｓｏｆｔ　ＤＲＭ１０及びＯＭＡ　ＤＲＭ２と同様に、権利の詳細への準拠に基づき複雑な認証を使用する。本発明は、上述されたように、コンテンツ及び装置をローカライズすることを所望するＭｉｃｒｏｓｏｆｔ及びＯＭＡ　ＤＲＭなどの複雑な認証ＤＲＭシステムに有用である。

【００６７】

ＤＴＣＰ／ＩＰシステムはまた、ネットワークローカリゼーションがＤＴＣＰ／ＩＰ処理をワイドエリアに拡張する効果的な手段であるため、本発明の利用から恩恵を受けることが可能である。本発明の実施例は、モバイル装置がホームネットワーク上のその他のＤＴＣＰ／ＩＰ装置に対しローカルであることを保証しながら、ハブを使用してワイドエリアにＤＴＣＰ／ＩＰ処理を拡張する。これは、モバイル装置がＤＴＣＰ／ＩＰプロキシーのＸ．５０９レジスタなどホームネットワークにより以前に登録されているという事実から生じるものである（例えば、図２と同様に）。

【００６８】

図１２及び１３は、本発明の実施例によるソース１２１０からシンク１２４０へのライセンスされたコンテンツの配信パスを示す。キー管理メッセージが、パスのすべて又は一部を介し送信される。１以上のハブ装置（ゲートウェイ１２２０）は、ソース１２１０とシンク１２４０とを分離してもよい。ローカリゼーションゲートウェイとして動作するハブは、２つのローカリゼーションスキームの間の接続を代理する。図１２の例では、プロキシー１２３０は、シンクゲートウェイの後方にあり、一実施例ではプライベートなホームネットワークであるシンクのネットワーク上にある。ゲートウェイ１２２０及びプロキシー１２３０は、同一の物理装置に一緒に配置可能な論理機能である。（例えば、プロキシー１２３０は、シンクのゲートウェイ１２２０に統合されてもよい。）

図１３の例では、プロキシー１２３５は、ソースのゲートウェイの後方にあり、ソースのネットワーク上にある。ゲートウェイ１２２５とプロキシー１２３５は、同一の物理装置に一緒に配置可能な論理機能である。（例えば、プロキシー１２３５は、シンクのゲートウェイ１２２５に統合されてもよい。）

図１３を参照するに、シンク１２４０は、ソース１２１０とのやりとりを開始し、シンク１２４０がアクセスすることを求めているライセンスされているコンテンツ（データ）を有する。シンク１２４０が認証リクエストを発行する前のある時点に、又はシンク１２４０からの第１メッセージに続いて、プロキシー１２３５はソース１２１０とのやりとりを実行する。認証やりとりの期間中、プロキシー１２３５はネットワークサービスクレデンシャルを利用して自らを明らかにする。ソース１２１０がプロキシー１２３５を認証することが可能である場合、それはプロキシー１２３５のアクセス権限をチェックする。一実施例では、アクセス制御リストが署名を有効にするため使用される。（例えば、ソース１２１０は、プロキシー１２３５にキーをダウンロードする前に、１又はいくつかの署名検証を実行する。）しかしながら、このやりとりは、ＯＭＡ　ＤＲＭ２．０について説明されたように、より多くの情報のより多くのチェックを含むことが可能である。

【００６９】

上述されたやりとりの目的は、解読キーを取得することであるが、プロキシー１２３５とシンク１２４０との間のプロトコル交換は、プロキシー１２３５とソース１２１０との間のものとは異なる可能性がある。一実施例では、プロキシー１２３５は、シンク１２４０に対しＤＴＣＰ／ＩＰを実行し、ソース１２１０に対しＩＰｓｅｃ　ＡＨによるＩＫＥなどの他のプロトコルを実行する。他の実施例では、ソース１２１０及びプロキシー１２３５は、ＲＦＣ３３９４キーラップ（ＯＭＡ　ＤＲＭ２．０により使用されるような）などのファイル暗号化及び認証プロトコルを使用するが、プロキシー１２３５は、シンク１２４０に対しＤＴＣＰ／ＩＰを実行する。プロキシーがキーを取得すると、ライセンス機関又はローカル管理によって強制されるポリシーに応じて、適切なクレデンシャルを有する他のシンクにキーを配布することが許可されるかもしれない。

【００７０】

ライセンス機関はプロキシー１２３５に対しキーアクセス制御機能のオフロード（ｏｆｆｌｏａｄ）を認めないケースがあるかもしれない。他の実施例では、図１３を参照するに、プロキシー１２３５は、プロキシー１２３５によりプロキシーされる装置に対しＡＫＥメッセージを単に中継する。プロキシーは、それのネットワークサービスクレデンシャルに基づき、装置及びコンテンツをローカライズするサービスを提供する。このような実施例では、プロキシーはまたシンクのネットワーク（それがシンク１２４０を代理するとき）又はソースのネットワーク（それがソース１２１０を代理するとき）からのリモートアクセスを維持するのに有用である。従って、プロキシー１２３５は、それがキーへのアクセスを有しないときでさえ有用である。すなわち、それは依然としてプライバシーを保護し、ネットワークアクセスを制限することが可能である。

【００７１】

他の実施例では、図１３をさらに参照するに、プロキシー１２３５は、プロキシー１２３５が特定のライセンス機関によってそうすることが許可されているとき、キーを受動的に取得する。このような“マン・イン・ザ・ミドル（ｍａｎ－ｉｎ－ｔｈｅ－ｍｉｄｄｌｅ）”の実施例では、プロキシー１２３５は、平文キーを取得するための方法としてソース１２１０とシンク１２４０との間でメッセージを変更する。“マン・イン・ザ・ミドル”攻撃と対照的に、ここでの“マン・イン・ザ・ミドル”は正当なものである（プロキシー１２３５が関連する機関によってマン・イン・ザ・ミドルとして機能することが許可されているとき）。従って、本発明の実施例によると、プロキシーは他の装置（代理されている装置など）のために認証されたキー交換を完了させることが可能である。

【００７２】

図１４は、本発明の一実施例によるローカルエリアネットワーク（ＬＡＮ）又は複数のＬＡＮから構成されるネットワーク１４００（プライベート、ホームネットワークなど）のブロック図である。図１４の例では、ＬＡＮ１４００は、メディアサーバ（ソース）１４１０と、メディアレンダラ（シンク）１４２０と、ゲートウェイ１４３０（レジデンシャルゲートウェイであってもよい）とを有する。シンク１４２０は、例えば、セットトップボックス又はデジタルメディアアダプタ（ＤＭＡ）であってもよい。

【００７３】
一実施例では、ソース１４１０、シンク１４２０及びゲートウェイ１４３０は、ホームネットワークに登録され、上述されるように、クレデンシャルが発行される（上記図１～５に関する説明を参照されたい）。ホームネットワークの何れかの装置が登録を管理することが可能であり、一実施例では、登録はゲートウェイ１４３０により実行され、それはネットワークサービスクレデンシャルの登録機関として機能し、ドングル、パスフレーズ又は他の手段に関する予め共有されている秘密を利用するなど、ある物理世界のアクションを介し装置の登録をローカライズする。
【００７４】
一実施例では、ゲートウェイ１４３０は、上述したようなＬＡＮ若しくは複数のＬＡＮから構成されるホームネットワークとワイドエリアネットワーク（ＷＡＮ）との間の境界とインタフェースとの両方として機能することに加えて、ＱｏＳ（Ｑｕａｌｉｔｙ－ｏｆ－Ｓｅｒｖｉｃｅ）スキーム及びコンテンツの転送のためのインタフェースとしてサービス提供する。各種実施例では、ゲートウェイ１４３０は、ルータ及びブロードバンドモデムを搭載し、複数のタイプのホームネットワークメディア（ＩＥＥＥ１４０２．１１、１０／１００イーサネット（登録商標）など）の使用をサポートすることができる。ある実施例では、ネットワークサービスプロバイダは、ゲートウェイ１４３０をリモート管理する。すなわち、ゲートウェイ１４３０のローカリゼーション及びプロキシー機能がサービスプロバイダに可視化され、サービスプロバイダは、コンフィギュレーションファイルをインストールすることが可能であるか、又はゲートウェイ１４３０のパラメータを変更することが可能である。ゲートウェイ１４３０が特定の特徴及び機能を有するものとして説明されてきたが、本発明はそのような特徴及び機能を有する装置に限定されるものではない。
【００７５】
一般に、ゲートウェイ１４３０は、ＬＡＮ１４００とワイドエリアネットワーク（インターネットなど）とを接続する。ゲートウェイ１４３０は、一方のサイドではＷＡＮとのブロードバンド接続を提供し、ＬＡＮサイドではホームネットワーク装置へのアクセスを提供する。ゲートウェイ１４３０におけるネットワークアドレス変換（ＮＡＴ）の存在は、パブリックＩＰアドレス（ＷＡＮサイド）とプライベートＩＰアドレススペース（ＬＡＮサイド）との間の境界を提供する。
【００７６】
図１４の例では、シンク１４２０は、シンク１４２０がソース１４１０からコンテンツ（データ）アイテムを受信することが許可されることを確立するため、自らをソース１４１０に対して認証する。異なる機能が認証及び許可のために利用可能である。上述されるように、一実施例では、シンク１４２０が登録され、シンク１４２０を認証及び許可するのに使用されるクレデンシャルが発行される。一実施例では、コンテンツはＤＴＣＰ／ＩＰを利用してＬＡＮ１４００内に送信される。
【００７７】
図１５及び１６は、本発明の実施例によるＬＡＮ１４００（ホームネットワークなど）とＷＡＮ１５００（インターネットなどのブロードバンドネットワークなど）のブロック図である。図１５及び１６のネットワークは、上述された図１２及び１３のシステムと類似している。
【００７８】
まず図１５を参照するに、ゲートウェイ１４３０は、ＬＡＮ１４００の外部にあるＷＡＮベースメディアサーバ（ソース）１５４０をソースとするコンテンツのプロキシーシンクとして機能するハブ７０２を有する。また、ゲートウェイ１４３０は、ＬＡＮ１４００内にあるシンク１４２０のプロキシーソースとして機能する。ＷＡＮベースソース１５４０からのコンテンツは、ＤＲＭスキーム（Ｍｉｃｒｏｓｏｆｔ　ＤＲＭ１０など）に従って転送されてもよい。これにより、ゲートウェイ１４３０は、ＷＡＮベースローカリゼーションスキームからＬＡＮ１４００により使用されているローカリゼーション方法（ＤＴ

ＣＰ／ＩＰなど）に変換するため、ローカリゼーション方法のＤＲＭ“トランスクリプション”を実行する。ある実施例では、ＷＡＮベースローカリゼーションは、ネットワークサービスクレデンシャルを利用し、ゲートウェイ／ハブは、ＷＡＮ　ＩＰインタフェース上でこのクレデンシャルを維持し、ＤＴＣＰ／ＩＰ装置とのＬＡＮインタフェースがＤＴＣＰ／ＩＰローカリゼーション（例えば、最大で７ミリ秒及び３以下のホップのパケット“Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ”など）に準拠していることを保証する。その後、シンク１４２０は、ＤＴＣＰ／ＩＰからコンテンツを解読し、当該コンテンツを再生する（視覚的又は聴覚的）。一実施例では、ゲートウェイ１４３０は、コンテンツを解読しない。

【００７９】

図１５の例では、シンク１４２０は、ゲートウェイ１４３０に対し自らを認証し、ゲートウェイ１４３０は、ＷＡＮベースソース１５４０に対し自らを認証する。認証及び許可について、異なる機構が利用可能である。一実施例では、シンク１４２０及びゲートウェイ１４３０は、上述されるように秘匿化される。ＷＡＮベースソース１５４０はまた、ＬＡＮ１４００により登録されてもよく、適切に秘匿化されてもよい。例えば、ソース１５４０は、ホームネットワークのメンバーであるモバイル装置であってもよいが、ホームの外部に一時的に転送されている。

【００８０】

次に図１６を参照するに、ゲートウェイ１４３０は、ＬＡＮ１４００内から（ソース１４１０などから）のコンテンツのためのプロキシーシンクとして機能する。ゲートウェイ１４３０はまた、ＬＡＮ１４００の外部にあるメディアレンダラ（シンク）１６４０のプロキシーソースとして機能する。

【００８１】

図１６の例では、ゲートウェイ１４３０は、ソース１４１０に対し自らを認証し、シンク１６４０は、ゲートウェイ１４３０に対し自らを認証する。一実施例では、ソース１４１０とゲートウェイ１４３０は、上述されたように秘匿化される。シンク１６４０はまたＬＡＮ１４００により登録されてもよく、適切に秘匿化されてもよい。例えば、シンク１６４０は、ホームネットワークのメンバーであるモバイル装置であってよいが、ホームの外部に一時的に転送されている。

【００８２】

しかしながら、ＬＡＮ１４００内のコンテンツは、ＷＡＮ１５００上で機能しないＤＴＣＰ／ＩＰに従って転送される。このため、ゲートウェイ１４３０は、ＤＴＣＰ／ＩＰローカリゼーションから、シンク１６４０により使用され、ＷＡＮ１５００上のアクセスを許可するのに利用可能なローカリゼーションスキームに変換するため、ローカリゼーションスキームを実行する。従って、本発明の実施例によると、ＤＴＣＰ／ＩＰによりコピープロテクトされたコンテンツアイテムのみが、ゲートウェイ１４３０まで到達する。その後、ゲートウェイ１４３０は、コンテンツアイテムをＷＡＮ１５００を介しシンク１６４０に転送するのに適したフォーマットにコンテンツをトランスクリプト（ｔｒａｎｓｃｒｉｐｔ）する。一実施例では、当該フォーマットはＩＰｓｅｃ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｈｅａｄｅｒ（ＡＨ）プロトコルによるＤＴＣＰ／ＩＰメッセージのシンプルなカプセル化である。

【００８３】

一般に、ＬＡＮ１４００上のコンテンツアイテムは、ＤＴＣＰ／ＩＰスキームを利用して“ラップ”される。一実施例では、ゲートウェイ１４３０は、コンテンツアイテムを“ラップ解除”し、その後、それをＬＡＮ１４００の外部で利用可能なフォーマット（ＤＴＣＰ／ＩＰ以外のスキーム）に“再ラップ”する。他の実施例では、ゲートウェイ１４３０は、ＬＡＮ１４００を介し受信したメッセージをＩＰｓｅｃ　AHなどの他のプロトコルに“カプセル化”し、ＷＡＮ９００に転送される。ＷＡＮ１５００からのメッセージは、“カプセル解除”され、ＬＡＮ１４００に転送される。これらのスキームは、ネットワークセキュリティ技術の知識のある人には周知である。後者のスキームは、ゲートウェイ１４３０がコンテンツキーにアクセスすることを要しないが、前者のスキームはそれを要

する。両方の実施例が、異なる２つのローカリゼーションドメイン上の装置を代理するローカリゼーションハブにおいて本発明によりサポートされる。

【００８４】

ゲートウェイ１４３０はＬＡＮ１４００の他の装置（シンク及びソースなど）から独立した要素として記載されているが、ゲートウェイ１４３０により提供される機能は、ＬＡＮ１４００の何れかの装置上で実現可能である。すなわち、例えば、ＬＡＮ１４００上のソース又はシンク装置は、ソース又はシンクとして機能し、またゲートウェイ装置として機能する二重の機能を提供することが可能である。

【００８５】

図１７は、本発明の一実施例によるコンテンツの配信を管理する方法のフローチャート１７００である。フローチャート１７００に具体的なステップが開示されているが、このようなステップは一例である。すなわち、本発明の実施例はフローチャート１７００に記載されたステップの変形又は他の（追加的な）各種ステップを実行するのに適している。フローチャート１７００の各ステップは提示されている順序とは異なる順序により実行可能であり、フローチャート１７００のすべてのステップが必ずしも実行される必要はないということが理解される。一実施例では、フローチャート１７００はゲートウェイ（図１５及び１６のゲートウェイ１４３０など）上で実現される。

【００８６】

図１７のステップ１７１０では、一実施例では、コンテンツアイテムに対するリクエストがシンク装置から受信される。当該リクエストは、ＷＡＮ（インターネットなど）を介し送信される。コンテンツアイテムは、ＬＡＮ上に配置される。ＬＡＮ内のコンテンツアイテムの配信は、コンテンツアイテムがＬＡＮの外部に配信されることを防ぐ第１のローカリゼーション方法及びプロトコル（ＤＴＣＰ／ＩＰなど）を利用する。

【００８７】

ステップ１７２０において、要求されたコンテンツアイテムに対して、ゲートウェイは第１のローカリゼーション方法及びプロトコルを第２のローカリゼーション方法及びプロトコルに変換する。このローカリゼーション方法は、装置をネットワーク装置に関連付ける登録のための手順とネットワークサービスクレデンシャルである。ローカリゼーションプロトコルは、ＷＡＮ又はＬＡＮを介した転送を最適化するため、コンテンツをカプセル化、ラップ又はラップ解除する。その後、コンテンツアイテムは、第２ローカリゼーション方法及びプロトコルに従ってシンク装置に転送可能である。一実施例では、シンク装置は、シンク装置をＬＡＮに拘束又はバインド（ｂｉｎｄ）するクレデンシャルを利用し、ネットワークにローカライズされるコンテンツを受信することが許可されていることを示すことにより、自らを認証する。

【００８８】

従って、本発明の実施例は、“モビリティ（ｍｏｂｉｌｉｔｙ）”（すなわち、個人が各自の自宅から自らが所有するホームベースコンテンツにアクセスする能力）と、“アフィニティ（ａｆｆｉｎｉｔｙ）”（友人、家族又は他人に家計にライセンスされているコンテンツへのアクセスを可能にすること）と呼ばれる問題についての消費者及び産業の懸念を解消することに役立ちうる。本発明の利用を通じて、ホームネットワーク内からのローカルコンテンツが、家計ベースローカリゼーション制約に違反することなく、ホームネットワーク外の許可された装置に許可及び転送することができる（例えば、データが家計装置に厳格にライセンスされているときなど）。

【００８９】

本発明の利用を通じて、ホームネットワーク外からのリモートコンテンツは、ホームネットワークにより登録されている装置に許可及び転送することが可能である。本発明は、装置が家計に関連付けされ、他の何れにも（又は他のいくつかなど）関連付けされていないというローカリゼーション保証を提供する。レジデンシャルゲートウェイなどの装置が、このローカリゼーション保証を提供する。

【００９０】

要約すると、本記載はローカルエリアネットワーク（ＬＡＮ）上のソース装置にあるコンテンツの配信を可能にする方法及び装置を開示した。ＬＡＮとワイドエリアネットワーク（ＷＡＮ）との間のゲートウェイは、シンク装置からコンテンツのインスタンスに対するリクエストを受信する。当該リクエストは、ＷＡＮを介し送信される。ＬＡＮ内のコンテンツアイテムの配信は、当該コンテンツアイテムがＬＡＮ外に配信されることを防ぐ第１のデジタル著作権管理（ＤＲＭ）プロトコルを利用する。当該コンテンツアイテムについて、ゲートウェイは、第１ＤＲＭプロトコルをＷＡＮを介しコンテンツを送信するのに利用可能な第２ＤＲＭプロトコルに変換する。その後、コンテンツアイテムは、第２ＤＲＭプロトコルに従ってシンク装置に転送することが可能である。

【００９１】

要約すると、本記載はネットワーク上のサービスへのアクセスを制御するための方法及び装置を開示した。クレデンシャルが、装置に提供される。このクレデンシャルは、装置がネットワークに登録されていることを示す。クレデンシャルは、装置上の不揮発性メモリに格納される。クレデンシャルは、装置をネットワークに拘束又はバインド（ｂｉｎｄ）し、装置が他のネットワークにアクセスすることを防ぐ。装置はクレデンシャルをプロバイダに提示し、プロバイダはクレデンシャルを用いて当該装置を認証及び許可する。許可されると、装置にはサービスへのアクセスが与えられる。

【００９２】

本発明の実施例が説明された。本発明は特定の実施例により説明されたが、本発明はこのような実施例により限定されると解釈されるべきではなく、以下の請求項に従って解釈されるべきであるということが理解されるべきである。

【図面の簡単な説明】

【００９３】

【図１】図１は、本発明の実施例によるネットワークのブロック図である。

【図２】図２は、本発明の実施例によるローカリゼーションハブにより登録されるネットワーク装置の状態遷移図である。

【図３】図３は、本発明の実施例によるネットワークを介しデータへのアクセスをリクエストするネットワーク装置のタイプ（家計、モバイル、ビジター又はフォーリンなど）を決定するのに利用可能な論理テーブルである。

【図４】図４は、本発明の実施例によるローカリゼーションハブにより登録されるネットワーク装置（ソース及びシンク）、家計ネットワーク上のハブ及びサービスプロバイダにおけるハブを示すブロック図である。

【図５】図５は、本発明の実施例によるネットワーク装置を秘匿化する方法のフローチャートである。

【図６】図６は、本発明の実施例が実現可能な装置のブロック図である。

【図７】図７は、本発明の一実施例によるローカリゼーションハブの概略図である。

【図８】図８は、本発明の実施例によるローカリゼーションハブの階層的ネットワークのブロック図である。

【図９】図９は、本発明の実施例によるエンドシステム装置とローカリゼーションハブとの間の物理的及び論理的インタフェースを介したネットワーク登録プロセスのデータフロー図である。

【図１０】図１０は、本発明の一実施例によるローカリゼーションハブにより装置を登録するプロセスを示すフローチャートである。

【図１１】図１１は、本発明の一実施例による第２ローカリゼーションハブによりローカリゼーションハブを登録するプロセスを示すフローチャートである。

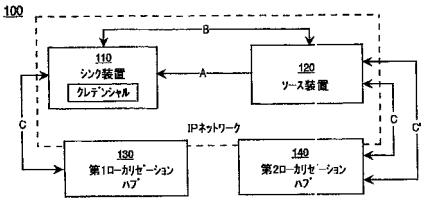
【図１２】図１２は、本発明の実施例によるローカリゼーションプロキシーコンフィギュレーションにおけるローカリゼーションハブを示すブロック図である。

【図１３】図１３は、本発明の実施例によるローカリゼーションプロキシーコンフィギュレーションにおけるローカリゼーションハブを示すブロック図である。

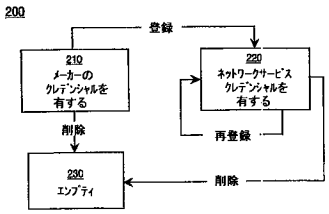
【図１４】図１４は、本発明の一実施例によるローカライズされたネットワークのブロッ

ク図である。
【図１５】図１５は、本発明の実施例によるシンク装置及びソース装置に対するローカライズされた制御フローを示すブロック図である。
【図１６】図１６は、本発明の実施例によるシンク装置及びソース装置に対するローカライズされた制御フローを示すブロック図である。
【図１７】図１７は、本発明の一実施例によるコンテンツの配信を管理する方法のフローチャートである。

【図１】



【図２】

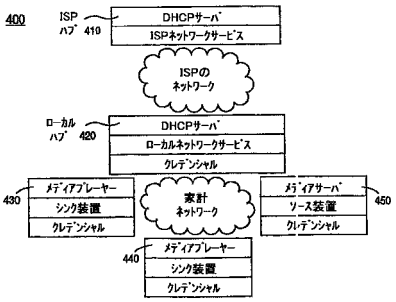


【図３】

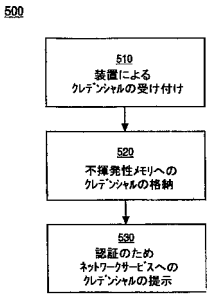
300

	DHCPベースネットワークサービス	
	装置と同一の サブネット	装置と同一の クレデンシャル
家計装置	TRUE	TRUE
モバイル装置	FALSE	TRUE
ビジター装置	TRUE	FALSE
フォーリン装置	FALSE	FALSE

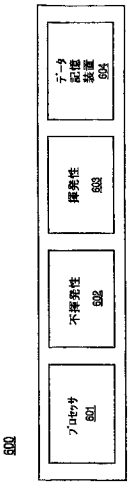
【図４】



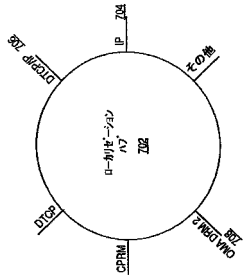
【図５】



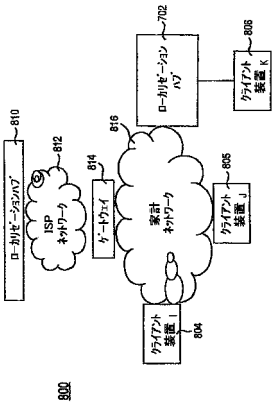
【図６】



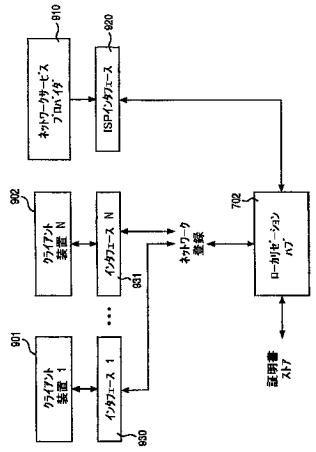
【図７】



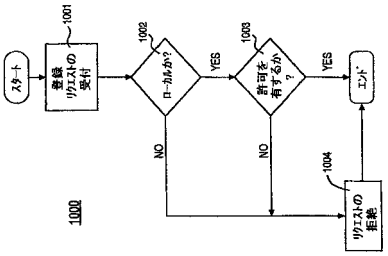
【図８】



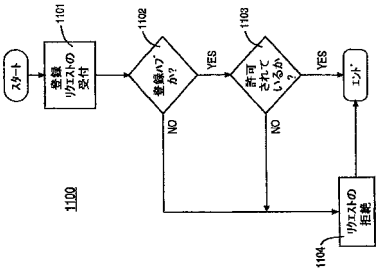
【図９】



【図１０】



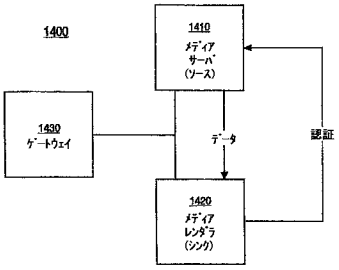
【図１１】



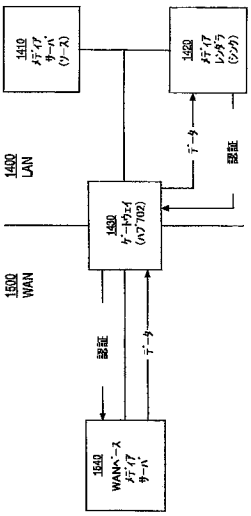
【図１２】

【図１３】

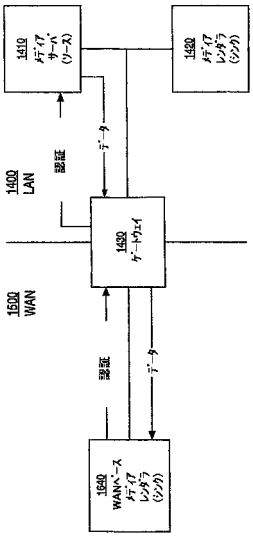
【図１４】



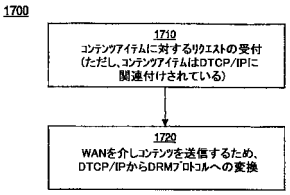
【図１５】



【図１６】



【図１７】



フロントページの続き

(31)優先権主張番号 11/260,531
(32)優先日 平成17年10月26日(2005.10.26)
(33)優先権主張国 米国(US)

前置審査

(72)発明者 フオタリ，アレン，ジェイ
アメリカ合衆国，カリフォルニア州 ９２８４１－１６３１，ガーデン・グローヴ，ヴィシリア・ストリート １１２４５

審査官 戸島 弘詩

(56)参考文献 特開２００４－０１５４９５（ＪＰ，Ａ）
特開２００２－２７８９３５（ＪＰ，Ａ）
特開２００３－２１８８５２（ＪＰ，Ａ）
特表２００３－５１８２８３（ＪＰ，Ａ）
米国特許出願公開第２００５／０２２８８７４（ＵＳ，Ａ１）
米国特許第０７５３３２５８（ＵＳ，Ｂ１）
米国特許第０７１１４０７０（ＵＳ，Ｂ１）
特開２００４－１８００２０（ＪＰ，Ａ）
国際公開第０３／０９２２６４（ＷＯ，Ａ１）
特開２００４－２０６１５８（ＪＰ，Ａ）
特開平１１－０８８４０３（ＪＰ，Ａ）
特表２００５－５２４１６３（ＪＰ，Ａ）
特開２００３－２７１４８７（ＪＰ，Ａ）
米国特許出願公開第２００４／０１６８０６２（ＵＳ，Ａ１）
米国特許第０６６７５２０８（ＵＳ，Ｂ１）
米国特許第０６０６５１２０（ＵＳ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F21/00-21/24
G09C1/00-5/00
H04K1/00
H04L9/00
H04N7/10,7/14-7/173,7/20-7/22
H04L12/46
H04K12/28