(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-192597
(P2014-192597A)
(43)公開日　平成26年10月6日(2014.10.6)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/66	(2006.01)	H04L	12/66	B	5K030
H04L 12/46	(2006.01)	H04L	12/46	E	5K033

審査請求 有　請求項の数 10　ＯＬ　（全 16 頁）

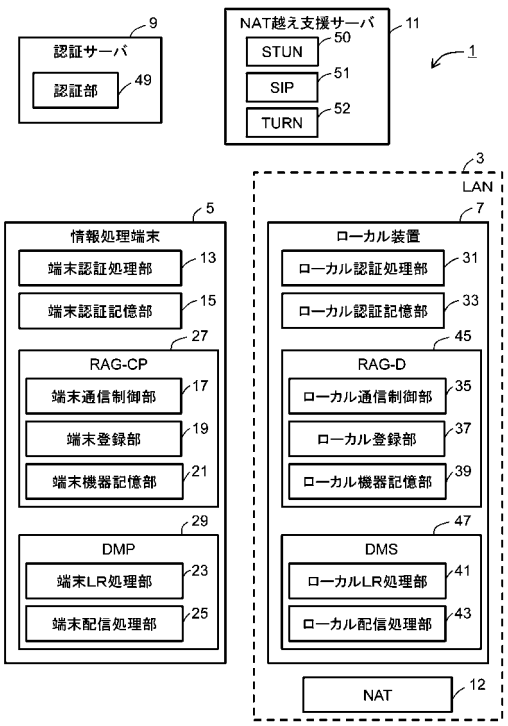
(21)出願番号　特願2013-64565(P2013-64565)
(22)出願日　平成25年3月26日(2013.3.26)

(71)出願人　300036578
株式会社デジオン
福岡県福岡市早良区百道浜２丁目３番８号
(74)代理人　100116573
弁理士　羽立　幸司
(74)代理人　100136180
弁理士　羽立　章二
(72)発明者　脇　浩一
福岡県福岡市早良区百道浜二丁目３番８号
株式会社デジオン内
(72)発明者　久留　吉伸
福岡県福岡市早良区百道浜二丁目３番８号
株式会社デジオン内

Ｆターム(参考)　5K030 GA15 HD03 KA06 LC16 LD17
5K033 AA08 CB01 CB08 DA06 DB18
EC03

(54)【発明の名称】通信制御方法、ローカル装置、情報処理端末、通信経路確立支援装置及びプログラム

(57)【要約】
【課題】　管理者に高度な知識や経験を要求することなく、セキュリティを確保して、ＬＡＮ外の情報処理端末が、ＬＡＮ内のローカル装置に接続することを可能とすることに適した通信制御方法等を提案する。
【解決手段】　情報処理端末５は、ＬＡＮ３外のローカル装置７に対して、接続要求をする。このとき、ローカル装置７は、情報処理端末５が、ＬＡＮ３外の認証サーバ９により認証されており、かつ、ローカル装置７の管理者が、情報処理端末５が接続可能な機器として登録している（ローカルレジストレーション）場合に、情報処理端末５との間で接続経路を構築する。ＬＡＮ３外の認証サーバ９により認証されているため、専門家による信頼性が保護される。さらに、ローカル装置７の管理者が、ローカルレジストレーションをすることにより、直観的に接続可否を管理でき、この点でも、さらに信頼性を確保することができる。
【選択図】　図２



【特許請求の範囲】
【請求項１】
情報処理端末と、ローカルエリアネットワークに接続されたローカル装置との間の通信経路を確立するか否かを制御する通信制御方法であって、
前記ローカルエリアネットワークとは異なるネットワークに接続する認証サーバが備える認証手段が、一つ又は複数の情報処理端末を認証する認証ステップと、
前記ローカル装置が備えるローカル登録手段が、前記ローカル装置が備えるローカル機器記憶手段に、前記認証サーバによって認証された一つ又は複数の情報処理端末を登録するローカルレジストレーションステップと、
前記ローカルエリアネットワークとは異なるネットワークに接続する情報処理端末が備える端末通信制御手段が、前記ローカル装置に対して通信経路確立要求をした場合に、前記ローカル装置が備えるローカル通信制御手段が、
前記ローカル機器記憶手段に当該情報処理端末が登録されているときに、当該情報処理端末と前記ローカル装置との間の通信経路を確立することを許可し、
前記ローカル機器記憶手段に当該情報処理端末が登録されていないときに、当該情報処理端末と前記ローカル装置との間の通信経路を確立することを拒否する通信経路確立制御ステップを含むことを特徴とする通信制御方法。
【請求項２】
前記ローカルレジストレーションステップにおいて、
前記情報処理端末は、前記ローカルエリアネットワークに接続するものであり、
前記ローカル装置が備えるローカル登録手段は、前記ローカルエリアネットワークに接続する前記情報処理端末から当該情報処理端末の識別情報を得て、前記ローカル機器記憶手段に登録する、請求項１記載の通信制御方法。
【請求項３】
前記認証ステップにおいて、前記認証手段は、前記情報処理端末のそれぞれに対して、デバイス識別情報を付与し、
前記ローカルレジストレーションステップにおいて、前記ローカル登録手段は、前記情報処理端末から、当該情報処理端末の識別情報として、前記認証手段から付与されたデバイス識別情報を登録する、請求項２記載の通信制御方法。
【請求項４】
前記通信経路確立制御ステップにおいて、前記ローカルエリアネットワークとは異なるネットワークに接続する支援手段は、前記情報処理端末が前記ローカルエリアネットワークとは異なるネットワークに接続する状態で前記通信経路確立要求をした場合に、前記情報処理端末が前記認証サーバにより認証されているときに、前記情報処理端末と前記ローカル装置との間で通信経路を確立するためのＮＡＴ越えを支援する、請求項１から３のいずれかに記載の通信制御方法。
【請求項５】
前記認証ステップにおいて、前記認証手段は、前記ローカル装置に対して、当該ローカル装置を識別するためのデバイス識別情報を付与して認証し、
前記ローカルレジストレーションステップにおいて、前記情報処理端末が備える端末登録手段は、前記ローカル装置のデバイス識別情報を登録し、
前記通信経路確立制御ステップにおいて、
前記情報処理端末は、前記支援手段に対して、前記ローカル装置のデバイス識別情報を通知し、
前記支援手段は、前記ローカル装置のデバイス識別情報を用いて前記ローカル装置へアクセスするための情報を得て、端末通信制御手段に対して、前記ローカル装置を接続先として伝え、前記情報処理端末と前記ローカル装置との間で通信経路を確立するためのＮＡＴ越えを支援する、請求項４記載の通信制御方法。
【請求項６】
ローカルエリアネットワークに接続するローカル装置であって、

前記ローカルエリアネットワークとは異なるネットワークに接続する認証サーバが認証した一つ又は複数の情報処理端末を記憶するローカル機器記憶手段と、
通信経路確立要求をした情報処理端末との間で通信経路を確立するか否かを制御するローカル通信制御手段を備え、
前記ローカル通信制御手段は、前記ローカルエリアネットワークとは異なるネットワークに接続する情報処理端末が備える端末通信制御手段が、当該ローカル装置に対して通信経路確立要求をした場合に、前記ローカル機器記憶手段に当該情報処理端末が登録されていないときに、当該情報処理端末との間で通信経路を確立することを拒否することを特徴とするローカル装置。
【請求項７】
ローカルエリアネットワークに接続するローカル装置に対して通信経路確立要求をする情報処理端末であって、
前記ローカルエリアネットワークとは異なるネットワークに接続する認証サーバに対して、当該情報処理端末の認証要求をする端末認証処理手段と、
前記ローカル装置が備えるローカル登録手段に対して、当該情報処理端末の登録要求をする端末ＬＲ処理手段と、
前記ローカルエリアネットワークとは異なるネットワークに接続する状態で、前記ローカル装置に対して通信経路確立要求をする端末通信制御手段を備える情報処理端末。
【請求項８】
情報処理端末が、ローカルエリアネットワークに接続するローカル装置との間で通信経路を確立することを支援する通信経路確立支援装置であって、
前記情報処理端末が前記ローカルエリアネットワークとは異なるネットワークに接続する状態で前記ローカル装置に対して接続要求をした場合に、前記情報処理端末が、前記ローカルエリアネットワークとは異なるネットワークに接続する認証サーバによって認証されているときに、前記情報処理端末が前記ローカル装置との間で通信経路を確立するためのＮＡＴ越えを支援する支援手段を備える通信経路確立支援装置。
【請求項９】
ローカルエリアネットワークに接続するコンピュータを、
ローカル機器記憶手段に対して、前記ローカルエリアネットワークとは異なるネットワークに接続する認証サーバが認証した一つ又は複数の情報処理端末を、前記ローカルエリアネットワークとは異なるネットワークに接続する状態で当該コンピュータとの間で通信経路を確立することが可能な情報処理端末として記憶させるローカル登録手段として機能させるためのプログラム。
【請求項１０】
コンピュータを、
ローカル装置が接続するローカルエリアネットワークとは異なるネットワークに接続する認証サーバに対して、当該コンピュータの認証要求をする端末認証処理手段と、
前記ローカル装置が備えるローカル登録手段に対して、当該コンピュータの登録要求をする端末ＬＲ処理手段と、
前記ローカルエリアネットワークとは異なるネットワークに接続する状態で、前記ローカル装置に対して通信経路確立要求をする端末通信制御手段として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信制御方法、ローカル装置、情報処理端末、通信経路確立支援装置及びプログラムに関し、特に、ローカルエリアネットワークに接続されたローカル装置と、前記ローカルエリアネットワークとは異なるネットワークに接続する情報処理端末との間の通信経路を確立する通信制御方法等に関する。
【背景技術】

【０００２】
特許文献１には、送信側端末から受信側端末にデータを転送する際に、送信者及び受信者は、通信支援装置へユーザ登録を行っておき、データは、中継サーバを経由して、送信側端末から受信側端末へと転送されるものが記載されている。
【０００３】
特許文献２には、ユーザ端末が、動画利用管理サーバに対してユーザ認証を行い、動画利用管理サーバが動画提供サーバにユーザ登録させておき、ユーザ端末は、動画提供サーバからサービスの提供を受けるものが記載されている。
【０００４】
特許文献３には、アクセス端末とユーザ宅内装置との間の通信路を、プロキシサーバが中継して確立するものが記載されている。アクセス端末とプロキシサーバ間の通信は、認証機関からのプロキシ証明書により客観的に証明される。プロキシサーバとユーザ宅内装置との間の通信は、ユーザ宅内装置の自己署名によるユーザ証明書により証明する。
【０００５】
特許文献４には、端末の個別ＩＤをサーバに登録しておき、その登録の有無によって、サーバへのアクセスを管理するものが記載されている。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００５－８０２４９号公報
【特許文献２】特開２０１２－１０８７３９号公報
【特許文献３】特開２００７－３３４７５３号公報
【特許文献４】特開２００３－３４５７５４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
情報処理端末からサーバへのアクセスを認めるか否かは、特に、ローカルエリアネットワーク（以下、「ＬＡＮ」ともいう。）におけるサーバ（以下、「ローカルサーバ」という。例えばホームサーバのように、家庭内で構築されたネットワークで用いられ、映像等のコンテンツを情報処理端末に配信するサーバなどである。）において重要である。ローカルサーバは、ＬＡＮとは異なるネットワークにおける端末（例えば、グローバルネットワークに接続して当該ＬＡＮとの間で通信経路を確立することが可能な端末や、他のＬＡＮに接続し、グローバルエリアネットワークを経由して当該ＬＡＮとの間で通信経路を確立することが可能な端末など）との間で通信経路を確立してしまうと、当該ローカルサーバそのもののセキュリティが問題となるだけでなく、当該ローカルサーバを経由して当該ＬＡＮにおける情報処理装置に対してアクセスすることが可能となりうる。そのため、ローカルサーバがＬＡＮ外の情報処理端末からのアクセスを認めることは、ＬＡＮにおける情報処理装置全体にとって、セキュリティ上の問題が生じうることとなる。
【０００８】
例えばホームサーバ等では、家庭内などにおける使用が想定されている。サーバ管理者は、素人が想定されており、高度な技能や知識を期待することはできない。そのため、ローカルサーバを管理するためには、ローカルサーバや情報処理端末についての高度な技能や知識が必要なく、かつ、サーバ管理者や情報処理端末の利用者からの指示は簡易にとどめることが望ましい。
【０００９】
特許文献１記載の技術では、通信支援装置によってセキュリティが確保されており、かつ、データのアクセスは、中継サーバを経由するため、ＬＡＮ全体のセキュリティも確保されている。しかしながら、送信側端末及び受信側端末が、ユーザ登録をする必要がある。このようなユーザ登録は、一般に、パスワード等を利用する。ユーザは、パスワード等を無くしたり忘れたりすることが多い。そのため、日々の使用において、サーバ管理者及

び情報処理端末の利用者に対する負担が大きい。また、中継サーバを経由してデータの送受信が行われるため、中継サーバの負荷が高くなる。さらに、送信側端末は、中継サーバに同じデータが存在する状態にし、かつ、その状態を維持する必要がある。

【００１０】

特許文献２記載の技術は、動画利用管理サーバが、動画提供サーバに代わってユーザの認証を行う点では、家庭内等の動画提供サーバの管理者に高度な知識・技能を求めるものではない。しかしながら、特許文献２記載の技術も、特許文献１記載の技術と同様に、人に着目したものであり、日々の運用において、情報処理端末の利用者等に対する負担が大きい。さらに、動画提供サーバにおいて、情報処理端末による個々のアクセスの管理ができない。そのため、サーバ管理者による管理の自由度が低くなる。

【００１１】

特許文献３記載の技術は、ハードウエアに着目しており、日々の運用におけるサーバ管理者や情報処理端末の利用者の負担は軽減されている。しかしながら、ＬＡＮ内のセキュリティは、ユーザ宅内装置の自己署名によって確保されている。そのため、サーバ管理者に対して、高度な知識・技能を要求するものとなる。

【００１２】

特許文献４記載の技術も、特許文献３記載の技術と同様に、ハードウエアに着目するものである。しかしながら、ローカルサーバに登録すれば端末のアクセスが認められてしまうため、ローカルサーバの安全性を確保するためには、サーバ管理者が、ローカルサーバ及び端末に関して一定の知識を有することを前提とする。そのため、サーバ管理者に対して、高度な知識・技能を期待するものとなる。

【００１３】

そこで、本願発明は、例えばローカルサーバなどのＬＡＮ内のローカル装置について、管理者に高度な知識や技能を必要とせずにセキュリティを確保して、このＬＡＮとは異なるネットワークに接続する情報処理端末が、ＬＡＮ内のローカル装置に接続することを可能とすることに適した通信制御方法等を提案することを目的とする。

【課題を解決するための手段】

【００１４】

本願発明の第１の観点は、情報処理端末と、ローカルエリアネットワークに接続されたローカル装置との間の通信経路を確立するか否かを制御する通信制御方法であって、前記ローカルエリアネットワークとは異なるネットワークに接続する認証サーバが備える認証手段が、一つ又は複数の情報処理端末を認証する認証ステップと、前記ローカル装置が備えるローカル登録手段が、前記ローカル装置が備えるローカル機器記憶手段に、前記認証サーバによって認証された一つ又は複数の情報処理端末を登録するローカルレジストレーションステップと、前記ローカルエリアネットワークとは異なるネットワークに接続する情報処理端末が備える端末通信制御手段が、前記ローカル装置に対して通信経路確立要求をした場合に、前記ローカル装置が備えるローカル通信制御手段が、前記ローカル機器記憶手段に当該情報処理端末が登録されているときに、当該情報処理端末と前記ローカル装置との間の通信経路を確立することを許可し、前記ローカル機器記憶手段に当該情報処理端末が登録されていないときに、当該情報処理端末と前記ローカル装置との間の通信経路を確立することを拒否する通信経路確立制御ステップを含むことを特徴とするものである。

【００１５】

本願発明の第２の観点は、第１の観点の通信制御方法であって、前記ローカルレジストレーションステップにおいて、前記情報処理端末は、前記ローカルエリアネットワークに接続するものであり、前記ローカル装置が備えるローカル登録手段は、前記ローカルエリアネットワークに接続する前記情報処理端末から当該情報処理端末の識別情報を得て、前記ローカル機器記憶手段に登録するものである。

【００１６】

本願発明の第３の観点は、第２の観点の通信制御方法であって、前記認証ステップにお

いて、前記認証手段は、前記情報処理端末のそれぞれに対して、デバイス識別情報を付与し、前記ローカルレジストレーションステップにおいて、前記ローカル登録手段は、前記情報処理端末から、当該情報処理端末の識別情報として、前記認証手段から付与されたデバイス識別情報を登録するものである。

【００１７】

本願発明の第４の観点は、第１から第３のいずれかの観点の通信制御方法であって、前記通信経路確立制御ステップにおいて、前記ローカルエリアネットワークとは異なるネットワークに接続する支援手段は、前記情報処理端末が前記ローカルエリアネットワークとは異なるネットワークに接続する状態で前記通信経路確立要求をした場合に、前記情報処理端末が前記認証サーバにより認証されているときに、前記情報処理端末と前記ローカル装置との間で通信経路を確立するためのＮＡＴ越えを支援するものである。

【００１８】

本願発明の第５の観点は、第４の観点の通信制御方法であって、前記認証ステップにおいて、前記認証手段は、前記ローカル装置に対して、当該ローカル装置を識別するためのデバイス識別情報を付与して認証し、前記ローカルレジストレーションステップにおいて、前記情報処理端末が備える端末登録手段は、前記ローカル装置のデバイス識別情報を登録し、前記通信経路確立制御ステップにおいて、前記情報処理端末は、前記支援手段に対して、前記ローカル装置のデバイス識別情報を通知し、前記支援手段は、前記ローカル装置のデバイス識別情報を用いて前記ローカル装置へアクセスするための情報を得て、端末通信制御手段に対して、前記ローカル装置を接続先として伝え、前記情報処理端末と前記ローカル装置との間で通信経路を確立するためのＮＡＴ越えを支援するものである。

【００１９】

本願発明の第６の観点は、ローカルエリアネットワークに接続するローカル装置であって、前記ローカルエリアネットワークとは異なるネットワークに接続する認証サーバが認証した一つ又は複数の情報処理端末を記憶するローカル機器記憶手段と、通信経路確立要求をした情報処理端末との間で通信経路を確立するか否かを制御するローカル通信制御手段を備え、前記ローカル通信制御手段は、前記ローカルエリアネットワークとは異なるネットワークに接続する情報処理端末が備える端末通信制御手段が、当該ローカル装置に対して通信経路確立要求をした場合に、前記ローカル機器記憶手段に当該情報処理端末が登録されていないときに、当該情報処理端末との間で通信経路を確立することを拒否することを特徴とするものである。

【００２０】

本願発明の第７の観点は、ローカルエリアネットワークに接続するローカル装置に対して通信経路確立要求をする情報処理端末であって、前記ローカルエリアネットワークとは異なるネットワークに接続する認証サーバに対して、当該情報処理端末の認証要求をする端末認証処理手段と、前記ローカル装置が備えるローカル登録手段に対して、当該情報処理端末の登録要求をする端末ローカルレジストレーション（ＬＲ）処理手段と、前記ローカルエリアネットワークとは異なるネットワークに接続する状態で、前記ローカル装置に対して通信経路確立要求をする端末通信制御手段を備えるものである。

【００２１】

本願発明の第８の観点は、情報処理端末が、ローカルエリアネットワークに接続するローカル装置との間で通信経路を確立することを支援する通信経路確立支援装置であって、前記情報処理端末が前記ローカルエリアネットワークとは異なるネットワークに接続する状態で前記ローカル装置に対して接続要求をした場合に、前記情報処理端末が、前記ローカルエリアネットワークとは異なるネットワークに接続する認証サーバによって認証されているときに、前記情報処理端末が前記ローカル装置との間で通信経路を確立するためのＮＡＴ越えを支援する支援手段を備えるものである。

【００２２】

本願発明の第９の観点は、ローカルエリアネットワークに接続するコンピュータを、ローカル機器記憶手段に対して、前記ローカルエリアネットワークとは異なるネットワーク

に接続する認証サーバが認証した一つ又は複数の情報処理端末を、前記ローカルエリアネットワークとは異なるネットワークに接続する状態で当該コンピュータとの間で通信経路を確立することが可能な情報処理端末として記憶させるローカル登録手段として機能させるためのプログラムである。

【００２３】

本願発明の第１０の観点は、コンピュータを、ローカル装置が接続するローカルエリアネットワークとは異なるネットワークに接続する認証サーバに対して、当該コンピュータの認証要求をする端末認証処理手段と、前記ローカル装置が備えるローカル登録手段に対して、当該コンピュータの登録要求をする端末ＬＲ処理手段と、前記ローカルエリアネットワークとは異なるネットワークに接続する状態で、前記ローカル装置に対して通信経路確立要求をする端末通信制御手段として機能させるためのプログラムである。

【００２４】

なお、本願発明を、コンピュータを、第８の観点に記載の通信経路確立支援装置として機能させるためのプログラムとして捉えてもよい。また、本願発明を、第９又は第１０の観点等に記載のプログラムを定常的に記録するコンピュータ読み取り可能な記録媒体として捉えてもよい。

【発明の効果】

【００２５】

本願発明の各観点によれば、ローカル装置と情報処理端末との間の通信経路を、機器に対する認証サーバによる認証を前提として確立する。よって、人に着目せずに機器に着目することから、人に対する負担は軽減される。さらに、機器の安全性は、認証サーバにより、専門家によって管理することが可能である。ローカル装置の管理者は、格別の知識や技能を必要としない。さらに、ローカルレジストレーションとして、ローカル装置の管理者は、情報処理端末ごとに、ＬＡＮ外からの通信を許可するものを登録する。管理者は、情報処理端末という機器に着目した直観的な操作によって、個々の情報処理端末に対するＬＡＮ外からのアクセスの可否を制御することが可能になる。このように、使用者の負担を軽減しつつ、専門家が機器を管理する信頼性だけなく、使用者が直感的に接続の可否を判断することによる信頼性をも確保して、ＬＡＮ外からのアクセスを管理することが可能になる。

【００２６】

さらに、本願発明の第２の観点によれば、ローカルレジストレーションは、ＬＡＮに情報処理端末が接続した状態で行う。ローカル装置は、情報処理端末が同じＬＡＮ内にあれば、情報処理端末のアドレスを知ることができ、アクセスすることができる。さらに、情報処理端末が、認証サーバによる認証だけでなく、ローカル装置と同じＬＡＮ内に接続する必要があり、安全性を確保することが可能になる。

【００２７】

さらに、本願発明の第３の観点によれば、認証サーバによる認証において各情報処理端末に与えられた識別情報を用いることにより、認証サーバによる認証が確実に行われたもののみを登録することが可能となる。

【００２８】

さらに、本願発明の第４及び第８の観点によれば、通信経路確立支援手段等は、情報処理端末が、認証サーバによって認証されていることを前提に、ＬＡＮ外からＮＡＴ越えを支援する。一般に、ＮＡＴ越えを実現するためには、ＬＡＮ外のサーバによることが必要である。認証の有無によりＮＡＴ越えを支援するか否かを制御することができ、安全性をさらに確保することが可能になる。

【００２９】

さらに、本願発明の第５の観点によれば、ローカル装置も認証サーバによって認証されており、安全性が高まる。さらに、情報処理端末は、認証サーバがローカル装置に対して与えたデバイス識別情報を用いてローカル装置へ接続し、さらに、情報処理端末もローカル装置も共に認証されていることを前提とするため、仮にローカル装置に接続するための

情報（エンドポイント）が漏洩した場合でも、ＬＡＮ内への侵入が困難になる。さらに、サーバ側とクライアント側のアプリケーションソフトを、同様のシステムとして実現することが可能になる。

【図面の簡単な説明】

【００３０】

【図１】本願発明に係るコンテンツ配信システム１の構成について、ローカルレジストレーションが行われる状態の一例を示すブロック図である。

【図２】本願発明に係るコンテンツ配信システム１の構成について、コンテンツを配信する状態の一例を示すブロック図である。

【図３】図１及び図２のコンテンツ配信システム１において、全体的な処理を示すフロー図である。

【図４】図３のステップＳＴ２のローカルレジストレーションにおける処理の例を示すシーケンス図である。

【図５】図３のステップＳＴ４のローカルレジストレーションされたデバイスを削除する処理の一例を示す図である。

【図６】図３のステップＳＴ４のローカルレジストレーションされたデバイスを削除する処理の他の一例を示す図である。

【図７】図３のステップＳＴ６～９のコンテンツの配信サービスを実現するための処理の例を示すシーケンス図である。

【発明を実施するための形態】

【００３１】

以下では、図面を参照して、本願発明の実施例について説明する。なお、本願発明は、この実施例に限定されるものではない。

【実施例】

【００３２】

図１は、ローカルレジストレーションが行われる状態のコンテンツ配信システム１の構成の一例を示すブロック図である。図２は、コンテンツを配信する状態のコンテンツ配信システム１の構成の一例を示すブロック図である。

【００３３】

図１及び図２のコンテンツ配信システム１は、情報処理端末５（本願請求項の「情報処理端末」の一例）と、ローカル装置７（本願請求項の「ローカル装置」の一例）と、認証サーバ９（本願請求項の「認証サーバ」の一例）と、ＮＡＴ越え支援サーバ１１（本願請求項の「通信経路確立支援装置」の一例）と、ＮＡＴ１２を備える。

【００３４】

情報処理端末５は、端末認証処理部１３（本願請求項の「端末認証処理手段」の一例）と、端末認証記憶部１５と、端末通信制御部１７（本願請求項の「端末通信制御手段」の一例）と、端末登録部１９（本願請求項の「端末登録手段」の一例）と、端末機器記憶部２１（本願請求項の「端末機器記憶手段」の一例）と、端末ＬＲ処理部２３（本願請求項の「端末ＬＲ処理手段」の一例）と、端末配信処理部２５を備える。端末通信制御部１７、端末登録部１９及び端末機器記憶部２１を併せたものが、ＲＡＧ－ＣＰ２７である。端末ＬＲ処理部２３及び端末配信処理部２５を併せたものが、ＤＭＰ２９である。

【００３５】

ローカル装置７は、ローカル認証処理部３１と、ローカル認証記憶部３３と、ローカル通信制御部３５（本願請求項の「ローカル通信制御手段」の一例）と、ローカル登録部３７（本願請求項の「ローカル登録手段」の一例）と、ローカル機器記憶部３９（本願請求項の「ローカル機器記憶手段」の一例）と、ローカルＬＲ処理部４１と、ローカル配信処理部４３を備える。ローカル通信制御部３５、ローカル登録部３７及びローカル機器記憶部３９を併せたものが、ＲＡＧ－Ｄ４５である。ローカルＬＲ処理部４１及びローカル配信処理部４３を併せたものが、ＤＭＳ４７である。

【００３６】

認証サーバ９は、認証部４９（本願請求項の「認証手段」の一例）を備える。ＮＡＴ越え支援サーバ１１は、ＳＴＵＮ５０、ＳＩＰ５１（ＳＴＵＮ５０及びＳＩＰ５１を併せたものが、本願請求項の「支援手段」の一例）、ＴＵＲＮ５２を備える。ＳＴＵＮ５０は、デバイスが位置するＮＡＴのタイプと接続可能なグローバルＩＰアドレス及びマッピングポートの検出を行うものである。ＳＩＰ５１は、ＲＡＧ間でＰ２Ｐトンネルを構築するためのＩＣＥメッセージをリレーするものである。ＴＵＲＮ５２は、Ｐ２Ｐ通信路が確立不可能な場合に、リレーするものである。

【００３７】

図１では、情報処理端末５とローカル装置７は、共に、ＬＡＮ３（本願請求項の「ローカルエリアネットワーク」の一例）の中に存在する。ここで、ある情報処理装置がＬＡＮ３の中に存在するとは、当該情報処理装置が、ＬＡＮ３の中に存在する他の情報処理装置との間で通信をする際に、ネットワーク上の識別情報を変換する必要がないこと（すなわち、例えばインターネットプロトコルでは、ＮＡＴ１２が、ＩＰアドレスのネットワークアドレス変換をする必要がないこと）を意味し、ある情報処理装置がＬＡＮ３の中に存在しないとは、当該情報処理装置が、ＬＡＮ３の中に存在する他の情報処理装置との間で通信をする際に、ネットワーク上の識別情報を変換する必要があること（すなわち、例えばインターネットプロトコルでは、ＮＡＴ１２が、ＬＡＮ３内のＩＰアドレスを、外部ＩＰアドレスに変換する必要があること）を意味するとする。情報処理装置がＬＡＮ３に接続するとは、ＬＡＮ３の中に存在する場合を意味し、ある情報処理装置がＬＡＮ３以外の他のネットワークに接続するとは、この情報処理装置がＬＡＮ３に存在せず、グローバルネットワーク等の他のネットワークに接続して、ＬＡＮ３の中の情報処理装置にアクセスできる状態を意味するとする。

【００３８】

他方、図２では、ローカル装置７は、ＬＡＮ３の中に存在し、情報処理端末５は、ＬＡＮの中には存在しない。情報処理端末５及びローカル装置７は、ＮＡＴ越え支援サーバ１１の支援により、ＮＡＴ越えの技術を用いてセキュアトンネルを構築する。ローカル装置７は、ローカルサーバとして、情報処理端末５に対してコンテンツを配信する。なお、情報処理端末５及びローカル装置７が共にＬＡＮ３内に存在する場合には、ローカル装置７及び情報処理端末５は、ＮＡＴ等を行うことなく互いに通信可能である。ローカル装置７は、情報処理端末５に対して、その状態を利用してコンテンツを配信すればよい。

【００３９】

図１及び図２において、認証サーバ９は、ＬＡＮ３の中に存在しない。認証サーバ９をＬＡＮ３の管理とは独立させることにより、認証サーバ９による認証の信頼性を確保するためである。

【００４０】

端末認証処理部１３及びローカル認証処理部３１は、認証サーバ９による認証を行うためのものである。端末認証記憶部１５及びローカル認証記憶部３３は、認証サーバ９により発行されたデバイス証明書及びサービス証明書を記憶する。

【００４１】

端末登録部１９及び端末ＬＲ処理部２３並びにローカル登録部３７及びローカルＬＲ処理部４１は、ローカルレジストレーションの処理を行うものである。ローカルレジストレーションの具体的な処理の一例に関しては、図４を参照して説明する。端末機器記憶部２１は、ローカルレジストレーションされたローカル装置を記憶する。ローカル機器記憶部３９は、ローカルレジストレーションされた情報処理端末を記憶する。端末機器記憶部２１及びローカル機器記憶部３９に記憶された機器を削除する処理の例については、図５及び図６を参照して説明する。

【００４２】

端末通信制御部１７及びローカル通信制御部３５は、情報処理端末５とローカル装置７との間の通信を実現するためのものである。端末配信処理部２５及びローカル配信処理部４３は、ローカル装置７が、情報処理端末５に対して、コンテンツを配信する処理を実現

するためのものである。この処理の一例については、図７を参照して説明する。ＮＡＴ越え支援サーバ１１は、ＬＡＮ３の外の情報処理端末５とＬＡＮ３の中のローカル装置７との間のＮＡＴ越えを支援するため、ＬＡＮ３の中に存在しない。

【００４３】

図１及び図２を参照して、本実施例によれば、情報処理端末５とローカル装置７は、同様の構成により実現することが可能である。そのため、認証処理部、認証記憶部、通信制御部、登録部、機器記憶部、ＬＲ処理部、及び、配信処理部を実現するための１つのプログラムを配信し、これが、情報処理端末５及び／又はローカル装置７の利用者の指示によって、情報処理端末５の各部及び／又はローカル装置７の各部を実現するものとしてもよい。なお、情報処理端末５とローカル装置７を実現するためのプログラムを別々のものとしてもよい。このプログラムは、アプリケーションソフトとして実現でき、管理者権限を必要としないものである。そのため、仮に、情報処理端末５が、スマートフォンやタブレット等であっても、容易に、アプリケーションプログラムを配布して実現することが可能である。

【００４４】

続いて、図３を参照して、コンテンツ配信システム１の動作の概要を説明する。図３は、コンテンツ配信システム１における処理の概要を示すフロー図である。

【００４５】

認証サーバ９は、情報処理端末５及びローカル装置７を認証する（図３のステップＳＴ１）。なお、ローカルレジストレーション（ステップＳＴ２）の前に、情報処理端末５及びローカル装置７の認証処理が行われていればよく、情報処理端末５及びローカル装置７の認証の順番は、問われない。

【００４６】

図３のステップＳＴ１の処理の一例について、具体的に説明する。

【００４７】

情報処理端末５の端末認証処理部１３は、認証サーバ９の認証部４９に対して、デバイス証明書の発行を要求する。認証部４９は、情報処理端末５の認証処理を行い、デバイス証明書を発行する。このデバイス証明書には、情報処理端末５を、他に認証した情報処理装置とは区別するためのデバイス識別情報（例えば、シリアルナンバーなど。本願請求項の「情報処理端末のデバイス識別情報」の一例。）が含まれている。また、デバイス証明書と同時に、サービス証明書も発行される。端末認証処理部１３は、発行されたデバイス証明書及びサービス証明書を端末認証記憶部１５に記憶する。

【００４８】

同様に、ローカル装置７のローカル認証処理部３１は、認証サーバ９の認証部４９に対して、デバイス証明書の発行を要求する。認証サーバ９の認証部４９は、ローカル装置７の認証処理を行い、デバイス証明書を発行する。デバイス証明書には、ローカル装置７を、他に認証した情報処理装置（例えば情報処理端末５）とは区別するためのデバイス識別情報が含まれている。また、デバイス証明書と同時に、サービス証明書も発行される。ローカル認証処理部３１は、発行されたデバイス証明書及びサービス証明書をローカル認証記憶部３３に記憶する。

【００４９】

また、認証部４９は、ローカル認証処理部３１との間で、ＬＡＮ３の外からローカル装置７へＮＡＴ越えによりアクセスするためのＮＡＴ越え支援情報を得る。これは、セキュアトンネルの構築（ステップＳＴ６）の前までに行われれば足りる。そのため、例えば、認証時に一度収集し、ローカル装置７のローカルのＩＰアドレスが変更されたときに修正する等により、ＮＡＴ越え支援情報を更新するようにしてもよい。

【００５０】

続いて、ローカルレジストレーションの処理（図３のステップＳＴ２。本願請求項の「ローカルレジストレーションステップ」の一例。）が、図１にあるように、情報処理端末５及びローカル装置７が同じＬＡＮ３の中に存在する状態で行われる。

【００５１】
図４を参照して、ローカルレジストレーションの処理の例について、具体的に説明する。図４は、図３のステップＳＴ２のローカルレジストレーションにおける処理の例を示すシーケンス図である。
【００５２】
ローカルレジストレーションは、図１にあるように、情報処理端末５及びローカル装置７が同じＬＡＮ３の中に存在する状態で行われる。情報処理端末５及びローカル装置７が同じＬＡＮ３の中に存在する場合、端末通信制御部１７及びローカル通信制御部３５は、互いに、アドレスを検出することができる。そのため、情報処理端末５とローカル装置７との間で通信をすることが可能である。
【００５３】
情報処理端末５の端末ＬＲ処理部２３は、情報処理端末５の使用者の指示によって、ローカル装置７のローカルＬＲ処理部４１に対して、デバイス証明書を提示して、ローカルレジストレーションの要求をする（図４のステップＳＴＬＲ１）。
【００５４】
ローカルＬＲ処理部４１は、端末ＬＲ処理部２３からローカルレジストレーションの要求があると、ローカル装置７の使用者が情報処理端末５のローカルレジストレーションを許可する場合、ＲＡＧ－Ｄ４５に対して、ＤＭＰ２９及びＤＭＳ４７の登録を指示する（ステップＳＴＬＲ２）。ローカル通信制御部３５は、端末通信制御部１７に対して、ローカル装置７のデバイス識別情報を通知し、ＤＭＳ４７のローカルレジストレーションを指示する（ステップＳＴＬＲ３）。端末登録部１９は、端末機器記憶部２１にローカル装置７のデバイス識別情報を記憶することにより、ＤＭＳ４７を登録する。端末通信制御部１７は、ローカル通信制御部３５に対して、ＤＭＳ４７を登録したことを通知する（ステップＳＴＬＲ４）。ローカル通信制御部３５が通知を受信すると、ローカル登録部３７は、ローカル機器記憶部３９に情報処理端末５のデバイス識別情報を記憶することにより、ＤＭＰ２９を登録する。ＲＡＧ－Ｄ４５は、ローカルＬＲ処理部４１に対して、ＤＭＰ２９及びＤＭＳ４７が登録されたことを通知する（ステップＳＴＬＲ５）。ローカルＬＲ処理部４１は、端末ＬＲ処理部２３に対して、ローカルレジストレーションが終了したことを通知する（ステップＳＴＬＲ６）。
【００５５】
他方、図２にあるように、ローカル装置７がＬＡＮ３の中に存在し、情報処理端末５がＬＡＮ３の外に存在する場合、端末通信制御部１７及びローカル通信制御部３５は、互いに、アドレスを検出することができない。そのため、本実施例では、図１のような場合にのみローカルレジストレーションができる状態にし、図２のような場合には、ローカルレジストレーションはできない状態とされている。
【００５６】
続いて、ローカルレジストレーションされた機器を削除するか否かが判断される（図３のステップＳＴ３）。削除する場合、削除処理が行われる（図３のステップＳＴ４）。
【００５７】
図５及び図６を参照して、削除処理の例を説明する。
【００５８】
図５は、ＬＡＮ３内にあるローカルレジストレーションした情報処理端末から削除要求がなされた場合の処理である。これは、図４とほぼ同様の処理となる。すなわち、端末ＬＲ処理部２３は、ローカルＬＲ処理部４１に対して、削除要求をする（ステップＳＴＤ１）。ローカルＬＲ処理部４１は、削除要求を受けると、ＲＡＧ－Ｄ４５に対して、ＤＭＰ２９及びＤＭＳ４７の登録削除を指示する（ステップＳＴＤ２）。ローカル通信制御部３５は、端末通信制御部１７に対して、ＤＭＳ４７の登録削除を指示する（ステップＳＴＤ３）。端末通信制御部１７が登録削除指示を受信すると、端末登録部１９は、端末機器記憶部２１からローカル装置７のデバイス識別情報を削除することにより、ＤＭＳ４７を登録削除する。端末通信制御部１７は、ローカル通信制御部３５に対して、ＤＭＳ４７を登

録削除したことを通知する（ステップＳＴＤ４）。ローカル通信制御部３５が通知を受信すると、ローカル登録部３７は、ローカル機器記憶部３９から情報処理端末５のデバイス識別情報を削除することにより、ＤＭＰ２９を登録削除する。ＲＡＧ－Ｄ４５は、ローカルＬＲ処理部４１に対して、ＤＭＰ２９及びＤＭＳ４７が登録削除されたことを通知する（ステップＳＴＤ５）。ローカルＬＲ処理部４１は、端末ＬＲ処理部２３に対して、登録削除が終了したことを通知する（ステップＳＴＤ６）。

【００５９】

図６は、ローカル装置７の使用者が削除する場合の処理の一例である。例えば、情報処理端末５の使用者が、悪意で、ＬＡＮ３に接続して、ローカル装置７にローカルレジストレーションをする可能性がある。そのため、ローカル装置７の使用者は、外部サーバ５３から登録削除できる。外部サーバ５３は、ローカルＬＲ処理部４１に対して、所定の情報処理端末の削除要求をする（ステップＳＴＳＤ１）。ローカルＬＲ処理部４１は、削除要求を受けると、ＲＡＧ－Ｄ４５に対して、当該情報処理端末のＤＭＰの登録削除を指示する（ステップＳＴＳＤ２）。ローカル登録部３７は、ローカル機器記憶部３９から当該情報処理端末のデバイス識別情報を削除することにより、ＤＭＰを登録削除する。ローカル登録部３７は、ローカルＬＲ処理部４１に対して、ＤＭＰが登録削除されたことを通知する（ステップＳＴＳＤ３）。ローカルＬＲ処理部４１は、外部サーバ５３に対して、登録削除が終了したことを通知する（ステップＳＴＳＤ４）。

【００６０】

このように、本実施例では、情報処理端末５の端末機器記憶部２１にローカル装置７が登録されていても、ローカル装置７のローカル機器記憶部３９からは情報処理端末５は削除されている可能性がある。

【００６１】

続いて、情報処理端末５において、サービス証明書の有無が判断される（図３のステップＳＴ５）。サービス証明書が無ければ、情報処理端末５の端末認証処理部１３は、認証サーバ９の認証部４９に対して、サービス証明書の発行を要求する（ステップＳＴ６）。これにより、認証サーバ９では、例えば、情報処理端末５でのコンテンツ利用の状況を把握することができ、その頻度等により、違法な利用等の可能性を検出することが可能になり、認証サーバ９による認証の信頼性が、さらに高まることとなる。認証サーバ９の認証部４９は、問題が認められない場合には、新たなサービス証明書を発行する。情報処理端末５にサービス証明書がある状態であれば、サービス証明書が有効であるかが判断される（ステップＳＴ７）。サービス証明書が、例えば期限が切れた状態などのために無効であれば、ステップＳＴ３に戻り、削除後に、改めてローカルレジストレーションがなされることが必要な状態とする。

【００６２】

有効なサービス証明書が存在する場合、情報処理端末５がローカル装置７に対して、接続要求をしたか否かが判断される（図３のステップＳＴ８）。接続要求は、情報処理端末５の使用者の指示によって行われる。情報処理端末５の使用者は、例えば、情報処理端末５のアプリケーションソフトにおいて、接続可能な装置として提示されたデバイスリストの中からローカル装置７を接続先として指示したり、以前にローカル装置７から配信されたコンテンツの再視聴を指示したりすることにより、ローカル装置７への接続を指示する。接続要求がなければ、ステップＳＴ３に戻る。

【００６３】

情報処理端末５が接続要求をした場合、情報処理端末５が、図１のようにＬＡＮ３内に存在するのであれば、端末通信制御部１７及びローカル通信制御部３５は、互いに、アドレスを検出することができる。

【００６４】

情報処理端末５が、ＬＡＮ３に存在せず、図２にあるように、ＬＡＮ３とは異なるネットワークに接続する状態で接続要求をした場合、端末通信制御部１７及びローカル通信制御部３５は、互いに、アドレスを検出することができない。そのため、端末通信制御部１

７は、ＮＡＴ越え支援サーバ１１の支援により、ローカル通信制御部３５との間でセキュアトンネルを構築して、コネクションを成立する。なお、以下では、ＮＡＴ越えについて、ＩＣＥを利用したＮＡＴ越えの場合を例に説明するが、その他の手法であってもよい。この処理の例について、図３及び図７を参照して、具体的に説明する。

【００６５】

まず、グローバルＩＰアドレスの検出について説明する。グローバルＩＰアドレスの検出は、ＮＡＴ越え支援サーバ１１のＳＴＵＮ５０のリクエスト／レスポンスを利用して、ＮＡＴ１２の外側に割り当てられているＩＰアドレスとポートを検出する。ＳＴＵＮ５０は、クライアント／サーバ型のプロトコルで、端末通信制御部１７及びローカル通信制御部３５からＳＴＵＮ５０へリクエストを送信し、そのレスポンスにＮＡＴの外側のＩＰアドレスとマップされたポート番号が格納される。また、ＳＴＵＮ５０は、ＮＡＴ１２のＮＡＴタイプの検出を行う。例えば、ＮＡＴ１２のＮＡＴタイプが多段であった場合には、一番制約の厳しいＮＡＴのタイプとなる。最終的に得られるものは、ローカルＩＰアドレスとポート番号、グローバルＩＰアドレスとポート番号、ＮＡＴタイプとなる。ここで得られた情報をＳＩＰ５１に送信して、ＮＡＴ越えサーバ１１においてデータベースに格納する。

【００６６】

まず、ローカル通信制御部３５は、ＳＴＵＮ５０との間で通信を行い、エンドポイントを取得する（ステップＳＴＤＥ１）。続いて、ローカル通信制御部３５は、ＳＩＰ５１に、エンドポイントを登録する（ステップＳＴＤＥ２）。

【００６７】

情報処理端末５の利用者が接続要求をすると、端末配信処理部２５は、端末通信制御部１７に対して、デバイスリストの取得要求を行う（ステップＳＴＤＥ３）。端末通信制御部１７は、端末配信処理部２５に対して、デバイスリストを送信する（ステップＳＴＤＥ４）。端末配信処理部２５は、端末通信制御部１７に対して、ローカル装置７に対する接続要求を行う（ステップＳＴＤＥ５）。

【００６８】

端末通信制御部１７は、ローカル通信制御部３５のアドレスを取得できない。そのため、端末通信制御部１７は、ＳＴＵＮ５０との間で通信を行い、エンドポイントを取得する（ステップＳＴＤＥ６）。続いて、端末通信制御部１７は、ＳＩＰ５１に、エンドポイントを登録する（ステップＳＴＤＥ７）。

【００６９】

端末通信制御部１７は、ＳＩＰ５１に対して、ローカル通信制御部３５に対する接続するための提案メッセージを送信する（ステップＳＴＤＥ８）。このとき、ローカル装置７に与えられたデバイス識別情報は、接続先を特定するための情報として使用される。ＳＩＰ５１は、ローカル通信制御部３５に対して、この提案メッセージを送信する（ステップＳＴＤＥ９）。ローカル通信制御部３５は、ＳＩＰ５１に対して、端末通信制御部１７に対しての応答メッセージを送信する（ステップＳＴＤＥ１０）。ＳＩＰ５１は、端末通信制御部１７に対して、この応答メッセージを送信する（ステップＳＴＤＥ１１）。

【００７０】

そして、端末通信制御部１７は、ＮＡＴ越えを利用して、ローカル通信制御部３５との間でセキュアトンネルを構築する（図３のステップＳＴ９、図７のステップＳＴＤＥ１２。）。ＮＡＴ越えは、必要であればＮＡＴ越え支援サーバ１１の支援のもとに行われる。

【００７１】

ＮＡＴ越えの技術には、いくつかの技法が提案されている。例えば、UDPホールパンチングや、TCPホールパンチングなどが提案されている。NATタイプは、ＲＦＣ３４８９では、Full Cone、Restricted Cone、Port Restricted Cone, Symmetricが規定されている。Open Internetであれば、なにもせずに接続可能である。Full Coneであれば、STUNによるアドレス解決を利用して接続することができる。Restricted ConeやPort Restricted Cone、Symmetricであれば、STUN／TURN並びにConnection Reversal及び／又はホ

ールパンチング、TURNによるリレーを利用して接続が可能である。このように、ＮＡＴタイプによって、ＮＡＴ越えの可否が異なる。

【００７２】

ローカル通信制御部３５は、情報処理端末５が、ローカル機器記憶部３９に記憶されている場合、端末通信制御部１７との間でコネクションの成立を許可する。ローカル通信制御部３５は、情報処理端末５が、ローカル機器記憶部３９に記憶されていない場合、端末通信制御部１７との間でコネクションの成立を拒否する。

【００７３】

情報処理端末５は、ローカル機器記憶部３９に記憶されていることから、ローカルレジストレーションの前提として認証サーバ９による認証処理により一定の信頼性が確保されている。さらに、ローカルレジストレーションによりローカル装置７の使用者により許可がされ、その後、削除されていないことから、ローカル装置７の使用者によっても信頼されていることが確保されている。そのため、これらの信頼性を前提とした、ＮＡＴ越えによるセキュアトンネルの構築が実現されている。

【００７４】

端末通信制御部１７は、端末配信処理部２５に対して、セキュアトンネルが構築されたことを通知する（ステップＳＴＤＥ１３）。

【００７５】

続いて、コンテンツの配信処理が行われる（図３のステップＳＴ１０）。すなわち、端末配信処理部２５は、端末通信制御部１７に対して、サービス証明書を提示して、コンテンツの配信要求をする（図７のステップＳＴＤＥ１４）。端末通信制御部１７は、セキュアトンネルでリレーする（図７のステップＳＴＤＥ１５）。ローカル通信制御部３５は、ローカル配信処理部４３に対して、配信要求を伝える（図７のステップＳＴＤＥ１６）。ローカル配信処理部４３は、ローカル通信制御部３５に対して、コンテンツ記憶部（図示を省略）に記憶されたコンテンツの配信処理を行う（図７のステップＳＴＤＥ１７）。ローカル通信制御部３５は、セキュアトンネルでリレーする（図７のステップＳＴＤＥ１８）。端末通信制御部１７は、端末配信処理部２５に対して、配信処理を伝える（図７のステップＳＴＤＥ１９）。

【００７６】

そして、情報処理端末５又はローカル装置７の使用者から切断が指示されたか否かを判断する（図３のステップＳＴ１１）。切断しない場合には、ステップＳＴ１０の処理に戻る。切断が指示された場合、情報処理端末５とローカル装置７の通信経路を切断する（図３のステップＳＴ１２）。

【００７７】

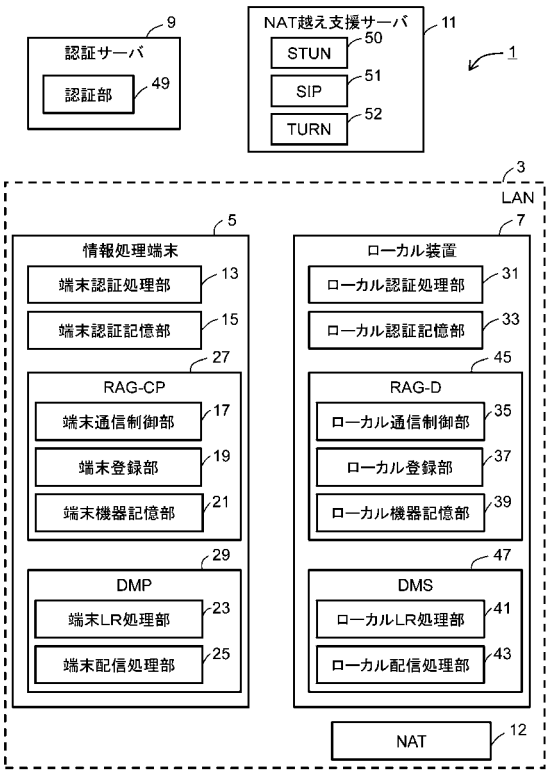
なお、ローカル装置７の安全性を確保する観点からは、少なくとも情報処理端末５が認証サーバ９により認証されていれば足りる。この場合、ＬＡＮ３の外からローカル装置７へＮＡＴ越えをするための情報は、認証処理とは別に、ＮＡＴ越え支援サーバ１１に与えられる。

【符号の説明】

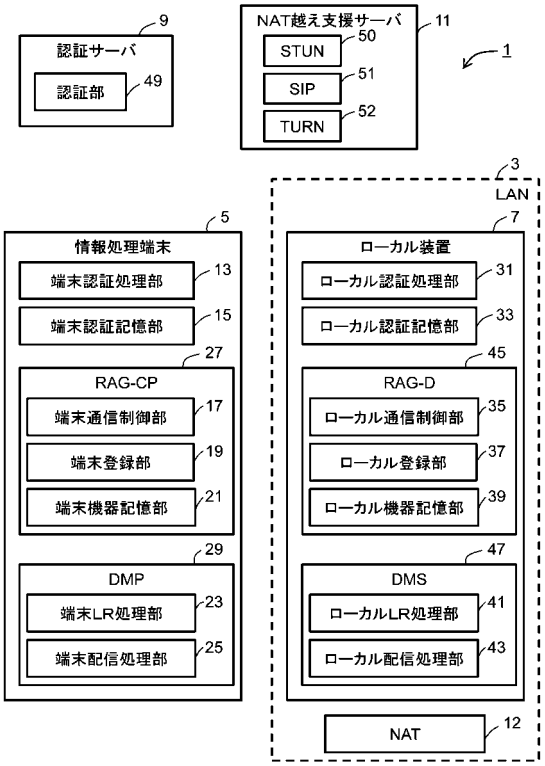
【００７８】

１　コンテンツ配信システム、３　ＬＡＮ、５　情報処理端末、７　ローカル装置、９　認証サーバ、１１　ＮＡＴ越え支援サーバ、１２　ＮＡＴ、１３　端末認証処理部、１５　端末認証記憶部、１７　端末通信制御部、１９　端末登録部、２１　端末機器記憶部、２３　端末ＬＲ処理部、２５　端末配信処理部、２７　ＲＡＧ－ＣＰ、２９　ＤＭＰ、３１　ローカル認証処理部、３３　ローカル認証記憶部、３５　ローカル通信制御部、３７　ローカル登録部、３９　ローカル機器記憶部、４１　ローカルＬＲ処理部、４３　ローカル配信処理部、４５　ＲＡＧ－Ｄ、４７　ＤＭＳ、４９　認証部、５０　ＳＴＵＮ、５１　ＳＩＰ、５２　ＴＵＲＮ、５３　外部サーバ

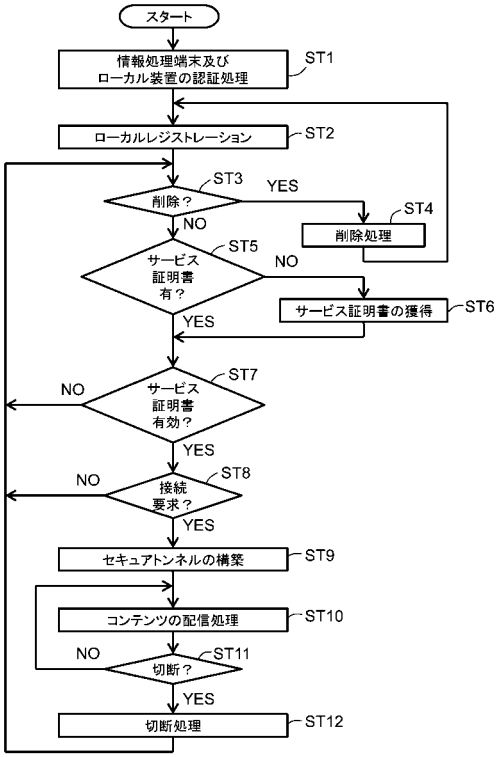
【図１】


認証サーバ
9
認証部
49
NAT越え支援サーバ
11
STUN
50
SIP
51
TURN
52
1
LAN
3
情報処理端末
5
端末認証処理部
13
端末認証記憶部
15
RAG-CP
27
端末通信制御部
17
端末登録部
19
端末機器記憶部
21
DMP
29
端末LR処理部
23
端末配信処理部
25
ローカル装置
7
ローカル認証処理部
31
ローカル認証記憶部
33
RAG-D
45
ローカル通信制御部
35
ローカル登録部
37
ローカル機器記憶部
39
DMS
47
ローカルLR処理部
41
ローカル配信処理部
43
NAT
12

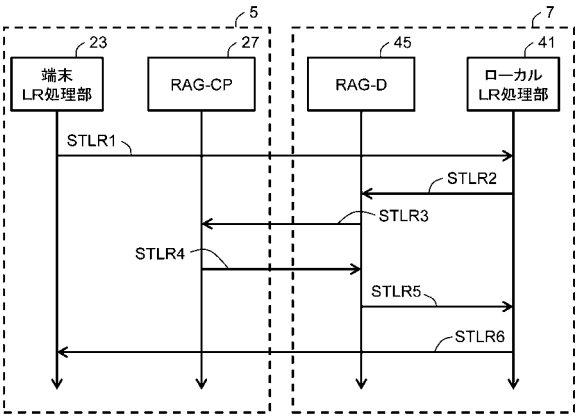
【図２】


認証サーバ
9
認証部
49
NAT越え支援サーバ
11
STUN
50
SIP
51
TURN
52
1
LAN
3
情報処理端末
5
端末認証処理部
13
端末認証記憶部
15
RAG-CP
27
端末通信制御部
17
端末登録部
19
端末機器記憶部
21
DMP
29
端末LR処理部
23
端末配信処理部
25
ローカル装置
7
ローカル認証処理部
31
ローカル認証記憶部
33
RAG-D
45
ローカル通信制御部
35
ローカル登録部
37
ローカル機器記憶部
39
DMS
47
ローカルLR処理部
41
ローカル配信処理部
43
NAT
12

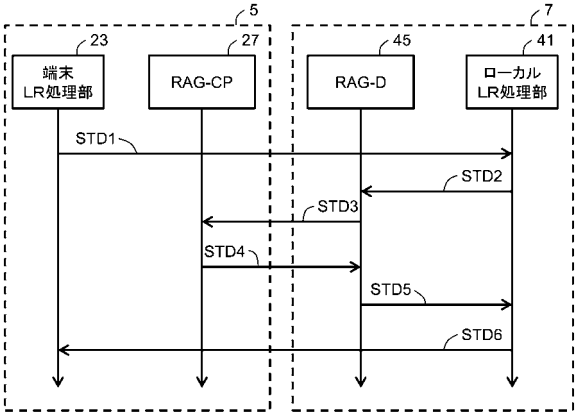
【図３】


スタート
情報処理端末及び
ローカル装置の認証処理
ST1
ローカルレジストレーション
ST2
削除？
ST3
YES
NO
削除処理
ST4
サービス
証明書
有？
ST5
NO
サービス証明書の獲得
ST6
YES
サービス
証明書
有効？
ST7
NO
YES
接続
要求？
ST8
NO
YES
セキュアトンネルの構築
ST9
コンテンツの配信処理
ST10
切断？
ST11
NO
YES
切断処理
ST12

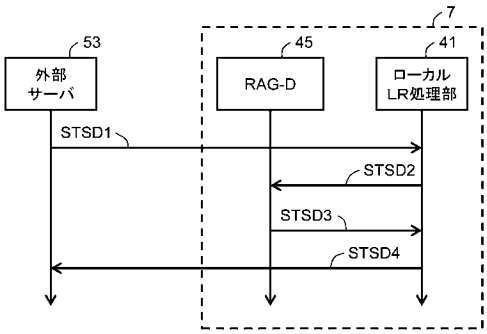
【図４】


5
7
23
27
45
41
端末
LR処理部
RAG-CP
RAG-D
ローカル
LR処理部
STLR1
STLR2
STLR3
STLR4
STLR5
STLR6

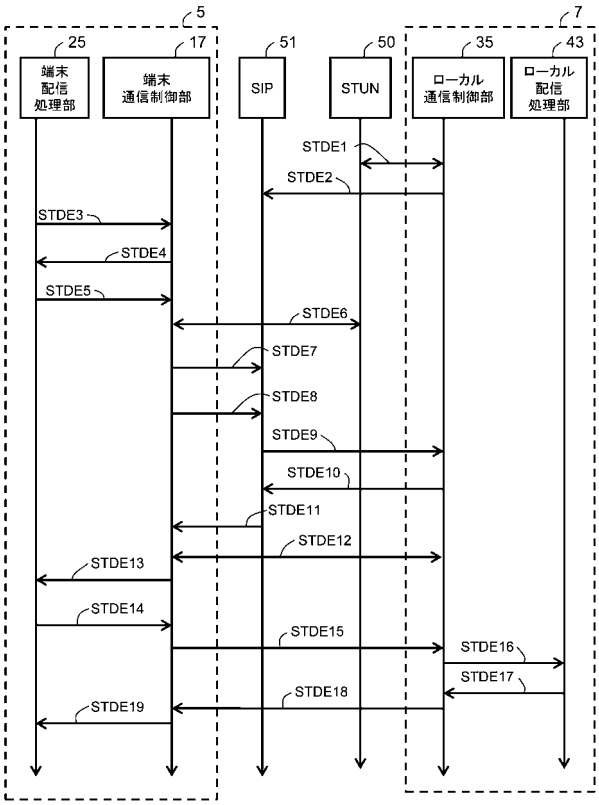
【図５】


5
7
23
27
45
41
端末
LR処理部
RAG-CP
RAG-D
ローカル
LR処理部
STD1
STD2
STD3
STD4
STD5
STD6

【図６】


7
53
外部
サーバ
45
RAG-D
41
ローカル
LR処理部
STSD1
STSD2
STSD3
STSD4

【図７】


5
7
25
端末
配信
処理部
17
端末
通信制御部
51
SIP
50
STUN
35
ローカル
通信制御部
43
ローカル
配信
処理部
STDE1
STDE2
STDE3
STDE4
STDE5
STDE6
STDE7
STDE8
STDE9
STDE10
STDE11
STDE12
STDE13
STDE14
STDE15
STDE16
STDE17
STDE18
STDE19