(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4477494号
(P4477494)
(45)発行日　平成22年6月9日(2010.6.9)　(24)登録日　平成22年3月19日(2010.3.19)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　A

請求項の数 38　(全 21 頁)

(21)出願番号	特願2004-519672 (P2004-519672)
(86)(22)出願日	平成15年6月30日 (2003.6.30)
(65)公表番号	特表2005-537701 (P2005-537701A)
(43)公表日	平成17年12月8日 (2005.12.8)
(86)国際出願番号	PCT/US2003/020417
(87)国際公開番号	WO2004/006521
(87)国際公開日	平成16年1月15日 (2004.1.15)
審査請求日	平成18年6月21日 (2006.6.21)
(31)優先権主張番号	10/190,849
(32)優先日	平成14年7月9日 (2002.7.9)
(33)優先権主張国	米国(US)

前置審査

(73)特許権者　502377350
ベリサイン・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　９４０４３　マウンテン・ビュー、イースト・ミドルフィールド・ロード　４８７
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉

最終頁に続く

(54)【発明の名称】インターネットプロトコル（ＶＯＩＰ）通信において音声のデジタル証明書を登録し自動的に検索する方法およびシステム

(57)【特許請求の範囲】
【請求項１】
ネットワークにおける通信方法において、
呼者から呼者証明書に関連するデジタル音声呼設定リクエストを受信し、
前記デジタル音声呼設定リクエスト中で識別される呼出されるパーティの位置を、
呼出されるパーティの識別子と呼者の署名とを含む前記位置に対するリクエストを位置サーバへ送信し、
前記位置サーバから前記呼出されるパーティに対する前記位置と呼出されるパーティの証明書と、前記呼者証明書とを含む位置応答を受信することによって決定し、
前記呼者証明書と共に前記デジタル音声呼設定リクエストを前記呼出されるパーティへ送信し、
呼出されたパーティの受取りメッセージを受信し、
前記呼出されたパーティの受取りメッセージを確認し、
前記呼出されたパーティの受取りメッセージと前記呼出されたパーティの証明書を前記呼者へ送信するステップを含んでおり、
さらに、前記デジタル音声呼設定リクエストが受信される前に、呼者および呼出されるパーティを登録するステップを含んでおり、
呼者についての登録は、呼者証明書の受信を含んでおり、
呼出されるパーティについての登録は、呼出されるパーティの位置および証明書の受信を含んでいる方法。

【請求項２】
前記デジタル音声呼設定リクエストの受信は、
前記呼者証明書に関連するインターネットプロトコル（ＶＯＩＰ）呼設定リクエストで前記呼者から音声を受信するステップを含んでいる請求項１記載の方法。
【請求項３】
前記デジタル音声呼設定リクエストは、
呼者インターネットプロトコル（ＩＰ）アドレスと、
前記呼出されるパーティのＩＰアドレスとを含んでいる請求項１記載の方法。
【請求項４】
前記デジタル音声呼設定は呼者の署名に関連している請求項１記載の方法。
【請求項５】
前記位置応答は前記位置サーバの署名を含んでいる請求項１記載の方法。
【請求項６】
前記デジタル音声呼設定リクエストはさらに前記呼者の署名を含んでいる請求項１記載の方法。
【請求項７】
前記呼出されるパーティの受取りメッセージは呼出されるパーティの署名を含んでいる請求項１記載の方法。
【請求項８】
前記呼出されるパーティの受取りメッセージの前記確認は、
前記受取りメッセージに付けられた前記呼出されるパーティの証明書を確認するステップと、
先に受信された呼出されるパーティの証明書を確認するステップとの少なくとも一方を含んでいる請求項１記載の方法。
【請求項９】
先に受信された呼出されるパーティの証明書は前記呼出されるパーティの前記位置と共に受信された請求項８記載の方法。
【請求項１０】
さらに、呼出されるパーティの署名を前記呼者へ送信するステップを含んでいる請求項１記載の方法。
【請求項１１】
前記呼者および前記呼出されるパーティの登録は、
ユーザ名と、
ユーザのＩＰアドレスと、
ユーザの公共キー証明書と、
ユーザのデジタル署名との受信を含んでいる請求項１記載の方法。
【請求項１２】
さらに、前記ユーザ名が前記ユーザ公共キー証明書中のユーザ名と同一であることを確認し、
前記ユーザのデジタル署名を確認し、
前記ユーザの公共キー証明書が正当であることを確認するステップを含んでいる請求項１１記載の方法。
【請求項１３】
さらに、前記ユーザ名を前記ユーザのＩＰアドレスへ結合し、
前記確認されたユーザの公共キー証明書を前記結合されたユーザ名およびユーザのＩＰアドレスへ結合するステップを含んでいる請求項１２記載の方法。
【請求項１４】
呼者の登録に成功した場合に、ＯＫメッセージを返送するステップを含んでいる請求項１３記載の方法。
【請求項１５】

前記登録は前記デジタル呼設定リクエストが受信される前に行われる請求項１記載の方法。

【請求項１６】

前記登録は、

前記呼者証明書と共に別々のデジタル音声呼設定リクエストを前記呼出されるパーティへ送信し、

前記呼出されたパーティから別々の受取りメッセージを受信し、

前記別々の呼出されたパーティの受取りメッセージを確認し、

前記別々の呼出されたパーティの受取りメッセージおよび別々の呼出されるパーティの証明書を前記呼者へ送信するステップを含んでいる請求項１５記載の方法。

【請求項１７】

前記登録は前記デジタル呼設定リクエストが受信された後に行われる請求項１記載の方法。

【請求項１８】

実行されるとき、プロセッサにより実行されるように構成されている命令を記憶する媒体において、プロセッサを構成するための命令は、

呼者証明書に関連しているデジタル音声呼設定リクエストを呼者から受信し、

前記デジタル音声呼設定リクエスト中で識別される呼出されるパーティの位置を決定し、

前記呼者証明書と共に前記デジタル音声呼設定リクエストを前記呼出されるパーティへ送信し、

呼出されたパーティの受取りメッセージを受信し、

前記呼出されたパーティの受取りメッセージを確認し、

前記呼出されたパーティの受取りメッセージと呼出されたパーティの証明書とを前記呼者へ送信する動作を行わせ、

前記呼出されるパーティの位置の決定は、

前記位置に対する位置サーバへリクエストを送信し、前記位置サーバから位置応答を受信するステップを含み、

前記リクエストは呼出されるパーティの識別子と署名とを含んでおり、

前記位置サーバから受信される位置応答は前記呼出されるパーティの前記位置と、呼出されるパーティの証明書と、前記呼者の証明書とを含んでおり、

プロセッサを構成するための前記命令は、さらに、前記デジタル音声呼設定リクエストが受信される前に、呼者および呼出されるパーティを登録し、

呼者についての登録は、呼者証明書の受信を含んでおり、

呼出されるパーティについての登録は、呼出されるパーティの位置および証明書の受信を含んでいる媒体。

【請求項１９】

デジタル音声呼設定リクエストの前記受信はプロセッサを構成し、そのプロセッサは、

前記呼者証明書に関連するインターネットプロトコル（ＶＯＩＰ）呼設定リクエストにより前記呼者から音声を受信する請求項１８記載の媒体。

【請求項２０】

デジタル音声呼設定リクエストの前記受信はプロセッサを構成し、そのプロセッサは、

前記デジタル音声呼設定リクエストを呼者インターネットプロトコル（ＩＰ）アドレスから受信し、前記デジタル音声呼設定リクエストはそれに関連する前記呼者証明書を有し、呼出されるパーティのＩＰアドレスに導かれる請求項１８記載の媒体。

【請求項２１】

デジタル音声呼設定リクエストの前記受信はさらにプロセッサを構成し、そのプロセッサは、

呼者署名を有する前記デジタル音声呼設定リクエストを受信する請求項１８記載の媒体。

【請求項２２】
前記位置応答の前記受信はさらに、前記位置サーバの署名を受信するようにプロセッサを構成する請求項１８記載の媒体。
【請求項２３】
前記デジタル音声呼設定リクエストの前記送信はプロセッサを構成し、そのプロセッサは、
署名と共に前記デジタル音声呼設定リクエストを送信する請求項１８記載の媒体。
【請求項２４】
前記呼出されたパーティの受取りメッセージの前記受信動作は、前記呼出されたパーティの受信メッセージと共に呼出されたパーティの署名を受信するようにプロセッサを構成する請求項１８記載の媒体。
【請求項２５】
前記呼出されたパーティの受取りメッセージの前記確認は、
前記受取りメッセージに付けられた前記呼出されたパーティの証明書と、
先に受信された呼出されたパーティの証明書の一方を使用して、前記呼出されたパーティの受取りメッセージで受信される呼出されたパーティの署名を確認するようにプロセッサを構成する請求項１８記載の媒体。
【請求項２６】
前記先に受信された呼出されたパーティの証明書は前記呼出されたパーティの前記位置と共に受信された請求項２５記載の媒体。
【請求項２７】
プロセッサはさらに、呼出されたパーティの署名を前記呼者へ送信するように構成されている請求項１８記載の媒体。
【請求項２８】
前記呼者および前記呼出されるパーティの前記登録動作はプロセッサを構成し、そのプロセッサは、
ユーザ名を受信し、
ユーザのＩＰアドレスを受信し、
ユーザの公共キー証明書を受信し、
ユーザのデジタル署名を受信する請求項１８記載の媒体。
【請求項２９】
前記プロセッサはさらに、
前記ユーザ名が前記ユーザ公共キー証明書中のユーザ名と同一であることを確認し、
前記ユーザのデジタル署名を確認し、
前記ユーザの公共キー証明書が正当であることを確認するように構成されている請求項２８記載の媒体。
【請求項３０】
前記プロセッサはさらに、
前記受信されたユーザ名を前記ユーザのＩＰアドレスと結合し、
前記確認されたユーザの公共キー証明書を前記結合されたユーザ名およびユーザのＩＰアドレスと結合するように構成されている請求項２９記載の媒体。
【請求項３１】
前記プロセッサはさらに、
呼者登録に成功した場合には、ＯＫメッセージを返送するように構成されている請求項３０記載の媒体。
【請求項３２】
インターネットプロトコル（ＶＯＩＰ）通信システムにより音声でデジタル証明書登録および自動証明書検索を行うシステムにおいて、
ＶＯＩＰゲートウェイを具備し、前記ＶＯＩＰゲートウェイは、
呼者証明書に関連するデジタル音声呼設定リクエストを呼者から受信し、

前記デジタル音声呼設定リクエスト中で識別された呼出されたパーティの位置を決定し、
前記呼者証明書と共に前記デジタル音声呼設定リクエストを前記呼出されるパーティへ送信し、
呼出されたパーティの受取りメッセージを受信し、
前記呼出されたパーティの受取りメッセージを確認し、
前記呼出されたパーティの受取りメッセージと呼出されたパーティの証明書とを前記呼者へ送信するステップを含んでおり、
前記呼出されるパーティの位置の決定は、
前記位置に対する位置サーバへリクエストを送信し、前記位置サーバから位置応答を受信することによって行われ、
前記位置サーバへ送信されるリクエストは呼出されるパーティの識別子と署名とを含んでおり、
前記位置サーバから受信される位置応答は前記呼出されるパーティの前記位置と、呼出されるパーティの証明書と、前記呼者の証明書とを含んでおり、
前記ＶＯＩＰゲートウェイは、さらに、前記デジタル音声呼設定リクエストが受信される前に、呼者および呼出されるパーティを登録するステップを含んでおり、
呼者についての登録は、呼者証明書の受信を含んでおり、
呼出されるパーティについての登録は、呼出されるパーティの位置および証明書の受信を含んでいるシステム。

【請求項３３】
前記ＶＯＩＰゲートウェイは、
前記ＶＯＩＰ通信システムと通信するセッション初期プロトコル（ＳＩＰ）代理サーバを具備し、このＳＩＰ代理サーバは前記呼者と前記呼出されるパーティ間の通信を可能にするように構成されている請求項３２記載のシステム。

【請求項３４】
前記ＶＯＩＰゲートウェイはさらに、
前記ＳＩＰ代理サーバと通信する位置サーバと、
前記ＳＩＰ代理サーバと通信する少なくとも１つの別の代理サーバと、
前記ＳＩＰ代理サーバと通信する証明書観察装置と、
前記ＳＩＰ代理サーバと通信するオンライン証明書状態プロトコル（ＯＣＳＰ）応答装置とのうちの少なくとも１つを具備している請求項３３記載のシステム。

【請求項３５】
前記ＶＯＩＰゲートウェイはさらに、
前記ＳＩＰ代理サーバと通信する位置サーバと、
前記位置サーバと通信し、前記呼出されるパーティの現在位置と、呼出されるパーティの証明書と、前記呼者証明書とを含んでいる位置データベースと、
前記位置サーバおよび前記ＳＩＰ代理サーバと通信する証明機関とを具備している請求項３３記載のシステム。

【請求項３６】
ネットワーク上で通信を設定する装置において、
プロセッサと、
前記プロセッサに結合され、以下のステップを行うように前記プロセッサにより実行される呼設定命令を記憶するメモリとを具備し、前記命令の実行するステップは、
呼者証明書に関連するデジタル音声呼設定リクエストを呼者から受信し、
前記デジタル音声呼設定リクエスト中で識別される呼出されるパーティの位置を決定し、
前記呼者証明書と共に前記デジタル音声呼設定リクエストを前記呼出されるパーティへ送信し、
呼出されたパーティの受取りメッセージを受信し、

前記呼出されたパーティの受取りメッセージを確認し、
前記呼出されたパーティの受取りメッセージと前記呼出されたパーティの証明書とを前記呼者へ送信するステップを含んでおり、
__前記呼出されるパーティの位置の決定は、
__前記位置に対する位置サーバへリクエストを送信し、前記位置サーバから位置応答を受信するステップを含み、
__前記位置サーバへ送信されるリクエストは呼出されるパーティの識別子と呼者の署名とを含んでおり、
__前記位置サーバから受信される位置応答は前記呼出されるパーティの前記位置と、呼出されるパーティの証明書と、前記呼者の証明書とを含んでおり、
さらに、前記デジタル音声呼設定リクエストが受信される前に、呼者および呼出されるパーティを登録するステップを含んでおり、
呼者についての登録は、呼者証明書の受信を含んでおり、
呼出されるパーティについての登録は、呼出されるパーティの位置および証明書の受信を含んでいる装置。

【請求項３７】
インターネットプロトコル（ＶＯＩＰ）通信システムにより音声でデジタル証明書登録および自動証明書検索を行うシステムにおいて、
ＶＯＩＰゲートウェイを具備し、そのＶＯＩＰゲートウェイは、
呼者証明書に関連しているデジタル音声呼設定リクエストを呼者から受信する手段と、
前記デジタル音声呼設定リクエスト中で識別される呼出されるパーティの位置を決定する手段と、
前記呼者証明書と共に前記デジタル音声呼設定リクエストを前記呼出されたパーティへ送信する手段と、
呼出されたパーティの受取りメッセージを受信する手段と、
前記呼出されたパーティの受取りメッセージを確認する手段と、
前記呼出されたパーティの受取りメッセージと前記呼出されたパーティの証明書を前記呼者へ送信する手段とを具備しており、
前記決定する手段は、
前記位置に対する位置サーバへリクエストを送信する手段と、前記位置サーバから位置応答を受信する手段とを具備し、
前記位置サーバへ送信するリクエストは呼出されるパーティの識別子と署名とを含んでおり、
前記位置サーバからの位置応答は前記呼出されるパーティの前記位置と、呼出されるパーティの証明書と、前記呼者の証明書とを含んでおり、
前記ＶＯＩＰゲートウェイは、さらに、前記デジタル音声呼設定リクエストが受信される前に、呼者および呼出されるパーティを登録する手段を含んでおり、
呼者についての登録は、呼者証明書の受信を含んでおり、
呼出されるパーティについての登録は、呼出されるパーティの位置および証明書の受信を含んでいるシステム。

【請求項３８】
ネットワーク上で通信を設定する装置において、
処理手段と、
前記処理手段に結合され、以下のステップを前記処理手段により実行させるための呼設定命令を記憶する記憶手段とを具備し、前記ステップは、
呼者証明書に関連するデジタル音声呼設定リクエストを呼者から受信し、
前記デジタル音声呼設定リクエスト中で識別される呼出されるパーティの位置を決定し、
前記呼者証明書と共に前記デジタル音声呼設定リクエストを前記呼出されたパーティへ送信し、

呼出されたパーティの受取りメッセージを受信し、
前記呼出されたパーティの受取りメッセージを確認し、
前記呼出されたパーティの受取りメッセージと前記呼出されたパーティの証明書とを前記呼者へ送信するステップを含んでおり、
__前記呼出されるパーティの位置の決定は、
__前記位置に対する位置サーバへリクエストを送信し、前記位置サーバから位置応答を受信するステップを含み、
__前記リクエストは位置サーバへ送信される呼出されるパーティの識別子と署名とを含んでおり、
__前記位置サーバから受信される位置応答は前記呼出されるパーティの前記位置と、呼出されるパーティの証明書と、前記呼者の証明書とを含んでおり、
さらに、前記デジタル音声呼設定リクエストが受信される前に、呼者および呼出されるパーティを登録するステップを含んでおり、
呼者についての登録は、呼者証明書の受信を含んでおり、
呼出されるパーティについての登録は、呼出されるパーティの位置および証明書の受信を含んでいる装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明はコンピュータ通信システム、特にインターネットプロトコル（ＶＯＩＰ）通信において音声のデジタル証明書を登録し自動的に検索する方法およびシステムに関する。
【背景技術】
【０００２】
図１は、本発明の１実施形態による証明書登録および自動証明書検索を有するインターネットプロトコル（ＶＯＩＰ）による音声の通信システム100におけるシステムブロック図である。通常、このような通信システム100はネットワーク120（例えばインターネット、構内網（ＬＡＮ）、広域網（ＷＡＮ）、イントラネット等）へ結合されている呼出しているＩＰ通信装置110と、ネットワーク120に結合されている呼出されるＩＰ電気通信装置130と、ネットワーク120に結合された自動証明書検索システム140とを含むことができる。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
本発明はインターネットプロトコル（ＶＯＩＰ）通信において音声のデジタル証明書を登録し自動的に検索する方法およびシステムを提供する。
【課題を解決するための手段】
【０００４】
本発明の１実施形態によれば、ネットワーク上における通信方法は呼者証明書に関連されるデジタル音声呼設定リクエストを呼者から受信し、デジタル音声呼設定リクエスト中で識別される呼出されるパーティの位置を決定するステップを含んでいる。この方法はさらに呼者証明書と共にデジタル音声呼設定リクエストを呼出されるパーティへ送信し、呼出されたパーティの受取りメッセージを受信し、呼出されたパーティの受取りメッセージを受信し、呼出されたパーティの受取りメッセージを確認し、呼出されたパーティの受取りメッセージおよび呼出されたパーティの証明書を呼者へ送信するステップを含んでいる。
【０００５】
本発明の１実施形態によれば、プロセッサにより実行されるように構成された媒体が記憶する命令は、それが実行されるならば、命令は、呼者証明書に関連しているデジタル音声呼設定リクエストを呼者から受信し、デジタル音声呼設定リクエスト中で識別される呼出されるパーティの位置を決定し、呼者証明書と共にデジタル音声呼設定リクエストを呼

出されるパーティへ送信するようにプロセッサを構成する。命令はさらに、呼出されたパーティの受取りメッセージを受信し、呼出されたパーティの受取りメッセージを確認し、呼出されたパーティの受取りメッセージと呼出されたパーティの証明書を呼者へ送信するようにプロセッサを構成する。

【０００６】

本発明の１実施形態によれば、インターネットプロトコル（ＶＯＩＰ）通信システムによって音声でデジタル証明書登録と自動証明書検索を行うシステムは、呼者証明書に関連するデジタル音声呼設定リクエストを呼者から受信し、デジタル音声呼設定リクエスト中で識別される呼出されるパーティの位置を決定し、呼者証明書と共にデジタル音声呼設定リクエストを呼出されるパーティへ送信し、呼出されたパーティの受取りメッセージを受信し、呼出されたパーティの受取りメッセージを確認し、呼出されたパーティの受取りメッセージと呼出されたパーティの証明書を呼者へ送信するように構成されたＶＯＩＰゲートウェイを含んでいる。

【０００７】

本発明の１実施形態によれば、ネットワーク上で通信を設定する装置はプロセッサと、プロセッサに結合されたメモリを含み、そのメモリは本発明の１実施形態にしたがった方法を行うようにプロセッサにより実行されるように構成された呼設定命令を記憶している。

【発明を実施するための最良の形態】

【０００８】

図１は、本発明の１実施形態による証明書登録および自動証明書検索を有するインターネットプロトコル（ＶＯＩＰ）による音声の通信システム100におけるシステムブロック図である。通常、このような通信システム100はネットワーク120（例えばインターネット、構内網（ＬＡＮ）、広域網（ＷＡＮ）、イントラネット等）へ結合されている呼出しているＩＰ通信装置110と、ネットワーク120に結合されている呼出されるＩＰ電気通信装置130と、ネットワーク120に結合された自動証明書検索システム140とを含むことができる。例えば呼出しているＩＰ電気通信装置110と呼出されるＩＰ電気通信装置130はそれぞれインターネットエネーブル陸線および／または無線電話機、ヘッドセット／電話機インターフェースが取付けられているパーソナルコンピュータ、パーソナルデジタルアシスタント（ＰＤＡ）、および／または他の携帯装置であってもよい。両者はオペレーティングシステム（ＯＳ）を含み、必要ならば別々のＶＯＩＰ通信アプリケーションプログラムを含むことができる。例えばＶＯＩＰエネーブル電話機は１つのＯＳだけを有し、ハンドセット／電話機インターフェースを有するＰＣは別々のＯＳと別々のＶＯＩＰ通信アプリケーションプログラムを有することができる。同様に、呼出し装置としてのＩＰ電気通信装置110と、呼出される装置としてのＩＰ電気通信装置130の名称は本発明の１実施形態の単なる例示であり、ＩＰ電気通信装置130は容易にＩＰ電気通信装置110を呼ぶことができることを理解すべきである。自動証明書検索システム140は呼者から、デジタル音声呼をネットワーク120にわたって設定するために呼者の証明書を有する定期的なリクエストを受信できる。各リクエストに応答して、自動証明書検索システム140は呼出されるパーティの位置、例えばデジタル音声呼設定リクエストで識別される呼出されるパーティのＩＰアドレスのような電子アドレスを決定し、呼者証明書を有するデジタル音声呼設定リクエストを呼出されるパーティへ送信してもよい。自動証明書検索システム140はまた呼出されたパーティから受取りメッセージを受信し、呼出されたパーティの受取りメッセージを確認し、呼出されたパーティの証明書と共に呼出されたパーティの受取りメッセージを呼者へ送信することができる。

【０００９】

本発明の実施形態によれば、自動証明書検索システム140は種々の構造を使用して構成され、例えば自動証明書検索システム140は集積されたおよび／または分散されたシステムとして構成されることができる。

【００１０】

図２のＡ乃至Ｅは本発明の１実施形態による証明書登録および検索機能の一方または両方を行うことのできる自動証明書検索システム140の別の構造を示すブロック図である。図２のＡでは、自動証明書検索システム140は単一の代理サーバ210として構成されてもよく、これは通常、呼者および呼出されるパーティの証明書を呼設定中に検索し転送するのに必要な幾つかまたは全ての機能を行うことができる。例えば、図２のＡの実施形態では、代理サーバ210は高速の検索のため局部的に証明書を記憶するかおよび／または１以上の遠隔位置から証明書および／または位置情報を検索するように構成されてもよい。同様に図２のＢでは、自動証明書検索システム140は代理サーバ210-1、210-2、…210-nのグループとして構成されることができ、ここでｎ≧２であり、通常、代理サーバ210-1、210-2、…210-nは呼の設定中に証明書を検索し転送するのに必要な幾つかまたは全ての機能を実行できる。図２のＡに関して前述したように、代理サーバ210-1、210-2、…210-nはまた高速の検索のため局部的に証明書を記憶するかおよび／または１以上の遠隔位置、例えばグループにはない他の代理サーバから証明書および／または位置情報を検索するように構成されてもよい。

【００１１】

図２のＣでは、自動証明書検索システム140は位置サーバ220と通信している代理サーバ210で構成されることもでき、これは本発明の実施形態にしたがってローカルまたは代理サーバ210から遠隔であってもよい。通常、代理サーバ210と位置サーバ220は個々にまたは組み合わせて呼設定中に呼者および呼出されるパーティの証明書を検索し転送するのに必要な幾つかまたは全ての機能を実行できる。例えば位置サーバ220は呼者および呼出されるパーティのＩＰアドレスを記憶し、そのＩＰアドレスを代理サーバ210へ提供できる。図２のＡとＢの実施形態に関してと同様に、図２のＣの本発明の実施形態は高速の検索のために証明書を局部的に記憶するかおよび／または１以上の遠隔位置、例えば他の代理サーバおよび／または位置サーバから証明書および／または位置情報を検索するように構成されてもよい。

【００１２】

図２のＤでは、自動証明書検索システム140は証明機関230と通信している代理サーバ210で構成され、これは本発明の実施形態にしたがってローカルまたは代理サーバ210から遠隔であってもよい。証明機関230はメッセージの暗号化のためセキュリティ信用証明書と公共キーを発行および管理する。セキュリティ信用証明書発行の一部として、証明機関230は呼者と呼出されるパーティの両者に対して、必要なセキュリティ信用証明書、公共キーおよびその他の情報と共に個人のデジタル署名されたデジタル証明書を発行することができる。通常、代理サーバ210と証明機関230は個々にまたは組合わせて、呼者および呼出されるパーティの証明書を呼設定中に検索し転送するのに必要な幾つかまたは全ての機能を行うことができる。図２のＡ乃至図２のＣと同様に、図２のＤの本発明の実施形態は証明機関230および／または代理サーバ210で証明書を記憶し、および／または１以上の遠隔位置、例えば他の代理サーバ、証明機関および／または位置サーバから証明書および／または位置情報を検索するように構成されている。

【００１３】

図２のＥでは、自動証明書検索システム140は代理サーバ210、位置サーバ220、証明機関230で構成され、これらは全て相互に通信している。前述したように、位置サーバ220と証明機関230はそれぞれ本発明の１実施形態にしたがってローカルまたは代理サーバ210から遠隔である。通常、代理サーバ210、位置サーバ220、証明機関230は個々にまたは組合わせて、呼者および呼出されるパーティの証明書を呼設定中に検索し転送するのに必要な幾つかまたは全ての機能を行うことができる。図２のＡ乃至図２のＤと同様に、図２のＥの本発明の実施形態は証明機関230および／または代理サーバ210で証明書を記憶し、および／または１以上の遠隔位置、例えば他の代理サーバ、証明機関および／または位置サーバから証明書および／または位置情報を検索するように構成されている。

【００１４】

図３は、本発明の１実施形態によるＶＯＩＰ通信システムにおけるデジタル証明書登録

および自動証明書検索を行う通信システム100のシステムブロック図である。図３では、図２のＥに示されている実施形態として構成されている自動証明書検索システム140が示されており、ここでは代理サーバ342は関連する位置データベース346を有する位置サーバ344および証明機関348と通信している。同様に、位置サーバ344と証明機関348は相互に通信できる。代理サーバ342は呼出しているＩＰ電気通信装置110と呼出されるＩＰ電気通信装置130とも通信でき、呼出しているＩＰ電気通信装置110と呼出されるＩＰ電気通信装置130は相互に直接通信できる。通常、自動証明書検索システム140のコンポーネント間の全ての通信は２方向である。

【００１５】

通信システム100の動作を説明するため、個者が呼出されるパーティを呼ぶ場合に生じることについての説明を図３に関して行う。本発明の１実施形態によれば、図３では代理サーバ342は呼出しているＩＰ電気通信装置110から呼出されるＩＰ電気通信装置130への呼を仲介するエンティティとしてセッション開始プロトコル（ＳＩＰ）代理サーバ342として構成されることができる。ＳＩＰは草案のインターネットエンジニアリングタスクフォース（ＩＥＴＦ）ワーキングドキュメントに現在規定されており、参照番号はrfc2543bis-08.psであり、2002年２月21日付けで発表された“１人以上の参加者によるセッションの生成、変更および終了のためのアプリケーション層制御（通報）プロトコル”である。ＳＩＰ代理サーバ342は呼の通報を処理するので、これはまた呼者と呼出されるパーティに対応する証明書の検索を仲介するための適切なエンティティを表している。しかしながら、前述したように他のエンティティも証明書の検索に使用されることができる。

【００１６】

図３では、呼リクエストは呼出しているＩＰ電気通信装置110からＳＩＰ代理サーバ342へ、第１の通信路305に沿って例えばＳＩＰコンテキストでＳＩＰインバイト－メッセージとして送信されることができる。しかしながら、通常のＳＩＰインバイト－メッセージとは異なって、この実施形態のＳＩＰインバイト－メッセージは呼出しているＩＰ電気通信装置110からの証明書を含んでおり、ＳＩＰインバイト－メッセージは呼出しているＩＰ電気通信装置110によりデジタル署名されることができる。ＳＩＰインバイト－メッセージはＳＩＰ代理サーバ342により受信／中断されることができ、ＳＩＰ代理サーバ342は呼出されるＩＰ電気通信装置130の現在の位置、即ちＩＰアドレスを第２の通信路310に沿って位置サーバ344に問い合わせる。同様に、位置サーバ344への問い合わせは位置サーバ344に対するサービスの攻撃の否認を防止するためにＳＩＰ代理サーバ342によりデジタル署名されることができる。位置サーバ344はＳＩＰサーバ342からの証明書を所有していると仮定され、問い合わせられたＳＩＰ代理サーバ342の署名を随意選択的に確認してもよい。

【００１７】

ＳＩＰ代理サーバ342からの問い合わせに応答して、位置サーバ344は呼出される位置、例えば呼出されるＩＰ電気通信装置130のＩＰアドレスを第３の通信路315に沿って返送する。同様に、位置サーバ344もまた位置サーバ344により知られるとき、呼出される電気通信装置130の証明書と、呼出しているＩＰ電気通信装置110の証明書を返送するようにしてもよい。メッセージ全体はメッセージに含まれる証明書が応答メッセージの署名時に有効であったことを示すために位置サーバ344によりデジタル署名されることができる。通常、位置サーバ344は呼出しているＩＰ電気通信装置110と呼出されるＩＰ電気通信装置130の有効な証明書を戻す。位置サーバ344は呼出しているＩＰ電気通信装置110と呼出されるＩＰ電気通信装置130の証明書の固有のコピーをオンライン証明書状態プロトコル（ＯＣＳＰ）応答装置／証明機関または他の証明書状態サービス（図示せず）に対して確認し、または単に証明機関348から現在の証明書を獲得する。ＯＣＳＰはネットワークリソース、例えば代理サーバ210のセキュリティを維持するためのさらに最近の方式である。図３の位置サーバ344が呼出しているＩＰ電気通信装置110と呼出されるＩＰ電気通信装置130の現在の有効な証明書を得ることができないならば、位置サーバ344は第３の通信路315に沿って何もＳＩＰ代理サーバ342へ戻さない。この位置サーバによる証明書の観察は呼者

および呼出されるパーティに関する１以上の属性、例えば位置サーバ344により知られているｅメールアドレスに基づくことができる。

【００１８】

本発明の別の実施形態によれば、位置サーバ344自体は実際にＯＣＳＰ応答装置／証明機関および／またはある種の証明書取消しリスト（ＣＲＬ）貯蔵所であってもよい。ＣＲＬはネットワークリソースのセキュリティを維持するための古い方法であり、ユーザのデジタル証明書の状態で識別されるユーザリストを維持し、ユーザのデジタル証明書の状態に基づいてアクセスを許可または否認することによりそれを行う。

【００１９】

ＶＯＩＰ呼についてのＳＩＰ実施形態の説明を続けると、図３でＳＩＰ代理サーバ342はオリジナルＳＩＰ－インバイトと共にメッセージを、呼出しているＩＰ電気通信装置110から呼出されるＩＰ電気通信装置130へ転送し、第４の通信路320に沿って位置サーバ344により戻された呼出しているＩＰ電気通信装置110に対する有効な証明書を転送する。ＳＩＰ代理サーバ342は呼出されるＩＰ電気通信装置130が既にその自分の証明書を有しているので、呼出されるＩＰ電気通信装置130のその自分の証明書のコピーを送信する必要はない。メッセージ全体はＳＩＰ代理サーバ342により署名されることができる。

【００２０】

一度、呼出されるＩＰ電気通信装置130が呼を受ける意思があることを示すと、呼出されるＩＰ電気通信装置130はそれがデジタル署名するＯＫメッセージに応答する。呼出されるＩＰ電気通信装置130のＯＫ応答を中断するとき、ＳＩＰ代理サーバ342は呼出されるＩＰ電気通信装置130によりＯＫメッセージに取付けられた証明書を使用するか、または証明書が取付けられていないならば、ＳＩＰ代理サーバ342が先に位置サーバ344から獲得した呼出されるＩＰ電気通信装置130の証明書のコピーを使用して、メッセージの署名を確認する。

【００２１】

ＳＩＰ代理サーバ342により呼出されているＩＰ電気通信装置130の署名の確認中に次の２つのことが行われる。第１に、呼出されるＩＰ電気通信装置130が証明書をＯＫメッセージに取付け、署名がその証明書を使用して適切に確認されたならば、ＳＩＰ代理サーバ342はＳＩＰ代理サーバ342がその証明書を最近位置サーバ344から獲得したコピーと比較する。証明書が同一ならば、ＳＩＰ代理サーバ342は呼出されるＩＰ電気通信装置130の証明書を呼出しているＩＰ電気通信装置110へ転送できる。しかしながら、証明書が同一ではないならば、ＳＩＰ代理サーバ342はＯＫメッセージ中の呼出されるＩＰ電気通信装置130により供給される証明書の状態を例えばＯＣＳＰ応答装置に対して確認する。状態確認が肯定として戻される（即ち証明書が有効）ならば、全ては良好であり、ＳＩＰ代理サーバ342は呼出されるＩＰ電気通信装置130の証明書を呼出しているＩＰ電気通信装置110へ転送できる。例えば、ＯＣＳＰ応答装置が否定の結果、即ち証明書が無効である結果を戻すならば、ＳＩＰ代理サーバ342はエラーメッセージ、例えばValid-Certificate-Not-Presentを呼出しているＩＰ電気通信装置110へ戻し、呼出されるＩＰ電気通信装置130が有効な証明書にＯＫメッセージを署名しなければならないか、または有効な証明書がＯＫメッセージに取付けられなければならないことを示す。

【００２２】

第２に、呼出されるＩＰ電気通信装置130がＯＫメッセージに証明書を取付けず、署名がＳＩＰ代理サーバ342で、呼出されるＩＰ電気通信装置130の証明書のコピー、即ち位置サーバ344から先に得られた証明書を使用して適切に確認されたならば、ＳＩＰ代理サーバは呼出されているＩＰ電気通信装置130に対して発行されたこの証明書を呼出しているＩＰ電気通信装置110へ転送する。これは呼出されるＩＰ電気通信装置130が偽りがなく、その証明書が現在／有効であることを示している。

【００２３】

一度、ＳＩＰ代理サーバ342が有効な呼出されているＩＰ電気通信装置130の証明書を所有すると、ＳＩＰ代理サーバ342は呼出されているＩＰ電気通信装置130の証明書を呼出し

ているＩＰ電気通信装置110へ戻す。

【００２４】

呼出されるＩＰ電気通信装置130の証明書のコピーを受信するとき、呼出しているＩＰ電気通信装置110は呼が進行できることを示す肯定応答（ＡＣＫ）メッセージを呼出されるＩＰ電気通信装置130へ送信する。呼出しているＩＰ電気通信装置110はその後の会話の他のキーとなるマテリアルを交渉するために呼出されるＩＰ電気通信装置130の公共キーも使用することができる。

【００２５】

図４は、本発明の１実施形態によるＶＯＩＰ通信における証明書登録および自動検索／転送および取消しを示す証明書登録および自動証明書検索システムのシステムブロック図である。図４で、呼出しているＩＰ電気通信装置110は代理登録装置442へ結合され、これは位置サーバ444と証明機関448へ結合されることができる。位置サーバ444は位置データベース446へ結合されることができる。図３に説明されているＳＩＰシステムの実施形態について継続すると、図４のシステムは証明書の登録と自動検索／転送および取消しがどのようにしてＶＯＩＰ呼のコンテキストで行われるかの１実施形態を示している。特に代理登録装置442はＳＩＰ代理登録装置442であってもよい。

【００２６】

図４で、本発明の１実施形態によれば、ユーザは第１の通信路405に沿って登録メッセージをＳＩＰ代理サーバとしても動作するＳＩＰ代理登録装置442へ送信することにより呼出しているＩＰ電気通信装置110から登録する。通常、通信路は同一または異なる物理的パスを横切る所定のソースと目的地との間の論理的接続として規定される。登録メッセージは通常ユーザ番号および位置、即ちＩＰアドレス、情報とユーザの公共キー証明書を含んでいる。全体的な登録メッセージはまたユーザにより署名されることができる。通常、ユーザによって署名された登録メッセージを有するとき、ユーザが自己であることを主張する通りの人であるという信用度が高くなる。

【００２７】

図４で、ＳＩＰ代理登録装置442は証明書で与えられたアイデンティティがユーザが主張しているアイデンティティと一致することを確認する。ＳＩＰ代理登録装置442はまた登録メッセージのデジタル署名を確認することができる。ＳＩＰ代理登録装置442はさらに例えば第２の通信路410に沿って証明機関448へ、それを証明書の状態サービスにより確認することにより証明書の有効性を確認してもよい。

【００２８】

ＳＩＰ代理登録装置442はユーザの存在／位置およびユーザの公共キー証明書を位置サーバ444へ通知するため第３の通信パス415に沿ってメッセージを送信する。ＳＩＰ代理登録装置442からのメッセージはまたその固有のデジタル証明書を使用してＳＩＰ代理登録装置442により署名されてもよい。ＳＩＰ代理登録装置442はユーザの名称／アイデンティティ、例えばｅメールアドレスをユーザの位置（例えばＩＰアドレス）に結合するだけでなく、ユーザの確認された証明書にも結合する。

【００２９】

図４では、ＳＩＰ代理登録装置442は登録プロセスが成功して完了したことを示すために第４の通信パス420に沿って呼出しているＩＰ電気通信装置110のユーザへＯＫメッセージを返送することができる。同様に、登録プロセスが不成功であるならば、ＳＩＰ代理登録装置442は登録プロセスが失敗したことを示すために第４の通信パス420に沿って呼出しているＩＰ電気通信装置110のユーザへエラーメッセージを返送してもよい。登録プロセスが失敗したならば、ユーザは全体的な登録プロセスに再度トライする。同一の登録プロセスがシステムに結合されている任意のＩＰ電気通信装置、例えば呼出されるＩＰ電気通信装置130間で行われる。別々のパスとしての第１の通信パス405と第４の通信パス420の説明は単なる本発明の実施形態の方法の説明を補助するだけである。このようにして、単一の２方向通信パスもまた使用され、例えば第１の通信パス405および第４の通信パス420は単一の２方向通信パスとして構成されてもよいことが明白に理解されるべきである。

【００３０】
図５は、本発明の１実施形態によるユーザが信用証明書をダウンロードするための２つの可能な方法を説明するために示されているＶＯＩＰ通信システムのブロック図である。通常、図５では呼出しているＩＰ電気通信装置110はその信用証明書を呼出されるＩＰ電気通信装置130への呼を開始の一部分としてダウンロードする。これは呼出しているＩＰ電気通信装置110が、図４に関連して前述したように、呼者の暗号化された信用証明書の検索をトリガーする呼者によって随意選択的なエントリを受信することを可能にすることにより実現される。図５では、呼者の暗号化された信用証明書の検索を完了するために、呼者は呼者の秘密のＰＩＮ番号またはパスワードを入力するか、或いは呼出しているＩＰ電気通信装置110でトークンをプリセットし、それは呼者の信用証明書を解読し、呼出しているＩＰ電気通信装置110の揮発性記憶装置（図示せず）例えばメモリへロードする。トークンはハードウェア装置、例えばスマートカードであってもよく、その持ち主を認証するのに便利である。本発明の実施形態によれば、ＶｏＩＰ呼の完了時に、呼出しているＩＰ電気通信装置110はその揮発性記憶装置（メモリ）から信用証明書を自動的に消去することができる。
【００３１】
本発明の実施形態によれば、呼者の信用証明書のダウンロードは第１の通信パス505に沿ってリクエストされたユーザの信用証明書を信用証明書サーバ550から得るための仲介として代理サーバ542、例えばＳＩＰ代理サーバ542を使用して実現されることができる。このＳＩＰ代理サーバ542は次に第２の通信パス510に沿って信用証明書サーバ550から信用証明書の暗号化されたピースを得ることができる。信用証明書サーバ550は次に関連する信用証明書記憶装置560-1…560-nから暗号化されたピースを獲得し、ここで各関連される信用証明書記憶装置560-1…560-nはそれぞれ位置データベース562-1…562-nへ結合されることができる。信用証明書サーバ550は第３の通信パス515に沿って獲得された信用証明書の暗号化されたピースをＳＩＰ代理サーバ542へ送信でき、これは次に通信パス520に沿って信用証明書の暗号化されたピースを呼出しているＩＰ電気通信装置110へ送信できる。別々のパスとしての通信パス505、510、515、520は単にこの実施形態の方法の説明を助けるためのものである。このようにして、単一の２方向通信パスも使用され、例えば第１の通信パス505および第４の通信パス520は単一の２方向通信パスとして構成されてもよく、第２の通信パス510および第３の通信パス515は別の単一の２方向通信パスとして構成されてもよいことが明白に理解されるべきである。
【００３２】
本発明の別の実施形態によれば、図５では、信用証明書のダウンロードは第５の通信パス530に沿って信用証明書を信用証明書サーバ550からダウンロードするため呼出しているＳＩＰ電気通信装置110を使用して直接実現されることができる。前述の実施形態のように、信用証明書サーバ550は次に関連する信用証明書記憶装置560-1…560-nと位置データベース562-1…562-nからそれぞれ信用証明書の暗号化されたピースを獲得することができる。信用証明書サーバ550は第６の通信パス535に沿って獲得された信用証明書の暗号化されたピースを呼出しているＳＩＰ電気通信装置110へ送信できる。先の実施形態のように、別々のパスとして通信パス530と535が例示されたがこれは単に本発明の実施形態の方法の説明を助けるためである。このようにして、単一の２方向通信パスもまた使用され、例えば第５の通信パス530および第６の通信パス535は単一の２方向通信パスとして構成されてもよいことが明白に理解されるべきである。
【００３３】
本発明のさらに別の実施形態によれば、図１に説明されている証明書登録システムはまたＳＩＰ代理サーバ342を介して信用証明書を記憶するために使用されてもよい。
【００３４】
図６は、本発明の１実施形態によるＶＯＩＰ通信における自動証明書検索／転送および取消し方法を示す詳細なプロセスフロー図である。図６では、本発明の１実施形態にしたがって、呼出されるパーティへのＶＯＩＰ呼リクエストは呼者によりデジタル署名される

メッセージ中の呼者の証明書と共にＳＩＰ－インバイトメッセージとしてＳＩＰ代理サーバで受信されることができる（605）。ＳＩＰ代理サーバは呼出されたパーティの現在位置についての代理サーバ（ＰＳ）が署名したデジタルリクエストを送信できる（610）。呼出されたパーティの現在の位置についてのリクエストは位置サーバへ送信されることができる。代理サーバは位置サーバ（ＬＳ）が署名したデジタルメッセージ中で、呼出されたパーティの証明書と呼出しているパーティの証明書との確認コピーと共に呼出されるパーティの位置を位置サーバから受信する（615）。証明書の確認コピーはＯＣＳＰ応答装置またはその他の証明書状態サービスに対する位置サーバで証明書のコピーを確認することによって得られる。同様に、証明書の確認コピーは証明書のコピーを有する証明機関から得られてもよく、実際に位置サーバはＯＣＳＰ応答装置および／またはＯＲＬ貯蔵所として動作する。

【００３５】

図６では、本発明の１実施形態にしたがって、ＳＩＰインバイト－メッセージはデジタルメッセージ中の呼者の証明書の確認コピーと共にＳＩＰ代理サーバから呼出されたパーティの現在の位置へ転送される（620）。デジタルメッセージはＳＩＰ代理サーバにより署名されることができる。それに応答して、呼出されたパーティからのデジタルＯＫメッセージは呼出されたパーティの証明書を有してまたはそれなしでＳＩＰ代理サーバにより受信されることができる（625）。デジタルＯＫメッセージは呼出されたパーティにより署名されてもよい。ＯＫメッセージにおける呼出されたパーティの署名はＳＩＰ代理サーバにより受信されるときに確認されることができる（630）。ＯＫメッセージ、呼出されたパーティの証明書、およびデジタル署名はＳＩＰ代理サーバから呼出しているパーティへ転送されることができる（635）。

【００３６】

図６では、ＳＩＰ代理サーバからのＯＫメッセージ、呼出されたパーティの証明書およびデジタル署名が受信されるとき、呼出したパーティは呼を完了するために臨時およびセッションキーと共に承諾メッセージ（ＡＣＫメッセージ）を呼出されたパーティへ送信できる（650）。呼は呼出したパーティと呼出されたパーティの一方または両者が呼の接続を断つまでそれらの間で継続する。

【００３７】

図７は、本発明の１実施形態によるＶＯＩＰ通信における証明書登録方法を示す詳細なプロセスフロー図である。図７では、ユーザの番号、位置、証明書を有するユーザからのデジタル署名されたＶＯＩＰ登録メッセージはＳＩＰ代理サーバにより受信される（705）。ＳＩＰ代理サーバは証明書中のユーザのアイデンティティがユーザが主張するアイデンティティと一致することを確認する（710）。ＳＩＰ代理サーバはまた登録メッセージ中のユーザの署名を確認する（715）。ＳＩＰ代理サーバはユーザの証明書の妥当性の確認をリクエストし（720）、リクエストされたユーザ証明書の妥当性の確認を位置サーバから受信する（725）。ユーザの存在／位置情報および公共キー証明書はＯＣＳＰへ送信される（730）。ＯＣＳＰは証明機関および／またはＣＲＬであってもよく送信はその固有の証明書を有するＳＩＰ代理サーバにより署名されることができる。代理サーバはユーザ名／アイデンティティ（例えばｅメールアドレス）、ユーザ位置（例えばＩＰアドレス）、および確認された証明書を一緒に結合する（735）。登録完了メッセージ、例えばＯＫメッセージは登録プロセスが成功した場合に、ＳＩＰ代理サーバからユーザへ送信されることができる（740）。

【００３８】

前述したように、図７に示されている登録プロセスはユーザからの呼開始リクエストの前、またはそれと同時に行われることができる。

【００３９】

図８は本発明の１実施形態によるＶＯＩＰ通信における自動証明書検索／転送および取消しのためのプロセスを示す詳細なプロセスフロー図である。図８では本発明の１実施形態にしたがって、ユーザは呼リクエスト、例えばＳＩＰインバイト－メッセージを呼出さ

れるパーティへ送信する（805）ことによりＶＯＩＰ呼を開始する。ＳＩＰインバイトーメッセージはまた呼者によりデジタル署名され呼者の証明書と共に送信されるメッセージ中に含まれていてもよい。ＳＩＰインバイトーメッセージはＳＩＰ代理サーバで受取られ／受信され、それによりＳＩＰ代理サーバは呼出されるパーティの現在位置に対するデジタル署名されたリクエストを送信することができる（810）。現在位置についてのリクエストは位置サーバへ送信され、その位置サーバはＯＣＳＰ応答装置またはその他の証明書状態サービスへリクエストを送信し、位置サーバに記憶されている呼者および呼出されるパーティの証明書を確認する（815）。位置サーバはまた本発明の実施形態ではＯＣＳＰ応答装置および／またはＣＲＬレポジトリとしても動作する。ＯＣＳＰは呼者および呼出されるパーティの証明書の確認／非確認認証を位置サーバへ返送する（820）。証明書が確認されるならば、位置サーバはＳＩＰ代理サーバへ呼出されたパーティの現在の位置と呼出されるパーティおよび呼者の証明書の確認コピーを返送する（825）。証明書の確認コピーはＬＳ署名されたデジタルメッセージで返送されることができる。証明書が確認されないならば、位置サーバは代理サーバへ何も返送しない（830）。

【００４０】

図８では、証明書の確認コピーを受信／受信しないとき、代理サーバはＳＩＰインバイトーメッセージを、呼者の証明書の確認コピーを有するかそれをもたない呼出されるパーティの現在位置の呼出されるパーティへ転送する（835）。呼出されるパーティは通常、既に固有の証明書を有するので、受信された呼出されるパーティの証明書の確認コピーは代理サーバによって呼出されるパーティへ送信される必要はない。呼出されるパーティは呼出されるパーティの証明書を有するかそれをもたないＯＫメッセージを代理サーバへ返送し（840）、呼出されるパーティが呼を受けることを所望していることを示す。ＯＫメッセージは呼出されるパーティにより署名されることができる。呼出されるパーティの署名はＳＩＰ代理サーバによりＯＫメッセージが受信されたときに確認される（845）。呼出されるパーティの署名が確認されるならば、ＳＩＰ代理サーバは呼出されるパーティの確認された証明書およびデジタル署名と共に、呼者にＯＫメッセージを転送する（850）。ＳＩＰ代理サーバからＯＫメッセージ、呼出されるパーティの証明書およびデジタル署名を受信するとき、呼者は呼を完了するため臨時およびセッションキーを有する受取りメッセージ（ＡＣＫメッセージ）を呼出されるパーティへ送信できる。臨時は一片の情報、例えば一度のみ使用可能な番号であってもよい。臨時は時間で変化するパラメータ、例えばタイムスタンプまたは特別なマーカであってもよい。呼は呼出すパーティと呼出されるパーティの一方または両者が呼の接続を断つまでそれらの間で継続する。

【００４１】

図８では、呼出されるパーティの署名が確認されないならば（845）、ＳＩＰ代理サーバは呼出されるパーティの証明書を再確認するためにＯＣＳＰへリクエストを送信する（860）。リクエストを受信するとき、ＯＣＳＰは証明書が妥当であるか否かを示すために状態確認メッセージを返送する（865）。状態確認メッセージ証明書が妥当であることを示すならば、ＳＩＰ代理サーバは呼出されるパーティの証明書とデジタル署名と共にＯＫメッセージを呼者へ転送し（850）、呼は前述したように完了されることができる。しかしながら、状態確認メッセージは証明書が妥当ではないことを示すならば、ＳＩＰ代理サーバはエラーメッセージを呼出されるパーティに返送し、呼出されるパーティに妥当な証明書を有する署名されたＯＫメッセージまたは妥当な証明書が取付けられているＯＫメッセージの一方を返送するようにリクエストする（870）。呼出されるパーティはＳＩＰ代理サーバに、呼出されるパーティの妥当な証明書を有するＯＫメッセージまたは呼出されるパーティの妥当な証明書が取付けられているＯＫメッセージを再度送信する（840）。プロセスは呼出されるパーティの署名を確認することにより継続し（845）、呼は前述したように完了されることができる。

【００４２】

図９は、本発明の１実施形態によるＶＯＩＰ通信における証明書登録および自動検索／転送および取消し方法を示すトップレベルのフロー図である。図９では、デジタル音声ユ

ーザおよびそれらの関連するユーザ証明書はＶＯＩＰ通信を行うシステムを使用するために登録される（905）。登録は例えば図１の自動証明書検索システム140に位置される登録サーバ／代理登録装置により通信システム中で行われることができる。図９では、デジタル音声呼設定リクエストは例えば図１の自動証明書検索システム140中に位置されるゲートウェイで受信されることができ（910）、そのゲートウェイはシステムのユーザ間の呼を仲介する。図９に戻ると、デジタル音声呼のための呼設定情報および証明書は例えばゲートウェイにより得られる（915）。証明書はデジタル音声呼設定中に識別される呼者と呼出されるパーティに対するものである。デジタル音声呼は呼者と呼出されるパーティとの間で設定され実行され（920）、デジタル音声呼の終了で完了する。前述したように、この方法は図１乃至５に示され前述されている構造のような広範囲のシステム構造を使用して実現されることができる。それ故、前述の特別な例の方法およびシステム構造は広い範囲の方法の一般的動作を単に示しているだけで、この方法の応用を説明した特別なシステムに限定するものと解釈されるべきではない。

【００４３】

図１０は、本発明の１実施形態によるＶＯＩＰ通信における証明書登録方法を示す詳細なフロー図である。図１０では、ユーザにより署名される公共キー証明書と共にユーザ登録メッセージは例えば図１の自動証明書検索システム140中に位置されている登録サーバ／代理登録装置により受信されることができる（1005）。図１０では、登録メッセージで主張されるアイデンティティが公共キー証明書のアイデンティティと一致するか否かが例えば登録サーバにより確認されることができる（1010）。ユーザ登録メッセージ中のユーザの署名もまた例えば登録サーバにより確認される（1015）。公共キー証明書の妥当性の確認は例えば登録サーバによりリクエストされることができる（1020）。公共キー証明書の妥当性の確認は例えば登録サーバにより受信される（1025）。ユーザの存在／位置情報および公共キー証明書は例えば図１の自動証明書検索システム中に位置される位置サーバに記憶されることができる。図１０では、ユーザの名称／アイデンティティ、例えばｅメールアドレスはユーザのＩＰアドレス（位置）へ結合され（1035）、同様に、ユーザの名称／アイデンティティおよびＩＰアドレスはまたユーザの確認された証明書に結合される（1035）。この方法はさらに登録が成功したことを示すため登録完了メッセージをユーザへ送信して終了する（1040）。前述したように、この方法は例えば図１乃至５に示され前述したように広範囲のシステム構造を使用して実現されることができる。それ故、前述の特別な例の方法およびシステム構造は広範囲の方法の一般的な動作を単に示しているだけで、この方法の応用を説明した特別なシステムに限定するものと解釈されるべきではない。

【００４４】

図１１は、本発明の１実施形態によるＶＯＩＰ通信における自動証明書検索／転送および取消し方法を示す詳細なフロー図である。図１１では関連する呼者証明書を有するデジタル音声呼設定リクエストは例えば図３の自動証明書検索システム140の代理サーバ342のようなゲートウェイにより受信されることができる（1105）。図１１では、デジタル音声呼設定リクエスト中で識別される呼出されるパーティの位置は例えば代理サーバ342により決定されることができる（1110）。関連する呼者証明書と共にデジタル音声呼設定リクエストは例えば代理サーバ342から呼出されるパーティへ送信されることができる（1115）。さらに、代理サーバ342はデジタル呼設定リクエストおよび関連する呼者証明書と共にその署名を送信することもできる。呼出されるパーティの受取りメッセージは例えば呼出されるパーティから代理サーバ342により受信される（1120）。通常、呼出されるパーティの受取りメッセージは、呼出されるパーティの呼者からデジタル音声呼を受信する能力および／または要望を示している。同様に、呼出されるパーティの受取りメッセージは、呼出されるパーティの証明書を伴い、呼出されるパーティにより署名されることができる。受信された呼出されるパーティの受取りメッセージは例えば代理サーバ342により確認される（1125）。前述したように、呼出されるパーティの受取りメッセージが確認されることができないならば、例えば呼出されるパーティの証明書は確認されることができな

いならば、代理サーバ342は呼出されるパーティがその受取りメッセージおよび呼出されるパーティの証明書を再度提出することをリクエストする。呼出されるパーティの受取りメッセージおよび呼出されるパーティの証明書は例えば代理サーバ342から呼者へ送信され（1130）、その方法は終了する。前述したように、この方法は広範囲のシステム構造、例えば図１乃至５に示され前述した構造を使用して実施されることができる。それ故、前述の特別な例の方法およびシステム構造は広範囲の方法の一般的な動作を単に示しているだけで、この方法の適用を説明した特別なシステムに限定するものと解釈されるべきではない。

【００４５】

本発明の幾つかの実施形態をここで特別に示し説明した。しかしながら、本発明の変更および変形は本発明の技術的範囲内を逸脱せずに先の教示により特許請求の範囲内でカバーされることが認識されるであろう。

【図面の簡単な説明】

【００４６】

【図１】本発明の１実施形態による証明書登録および自動証明書検索を有するインターネットプロトコル（ＶＯＩＰ）通信システムにおける音声のシステムブロック図。

【図２】本発明の１実施形態による証明書登録および検索の一方または両者を行うことのできる別の構成の自動証明書検索システムを示すブロック図。

【図３】本発明の１実施形態によるインターネットプロトコル（ＶＯＩＰ）通信システムにおける音声のデジタル証明書登録および自動証明書検索のシステムブロック図。

【図４】本発明の１実施形態によるＶＯＩＰ通信における証明書登録および自動証明書検索／転送および取消しを示す証明書登録および自動証明書検索システムのシステムブロック図。

【図５】本発明の１実施形態によるユーザが信用証明書をダウンロードするための２つの可能な方法を説明するために示されているＶＯＩＰ通信システムのブロック図。

【図６】本発明の１実施形態によるＶＯＩＰ通信におけるデジタル証明書登録および自動証明書検索を行う方法を示す詳細なプロセスフロー図。

【図７】本発明の１実施形態によるＶＯＩＰ通信においてデジタル証明書登録を行う方法を示す詳細なプロセスフロー図。

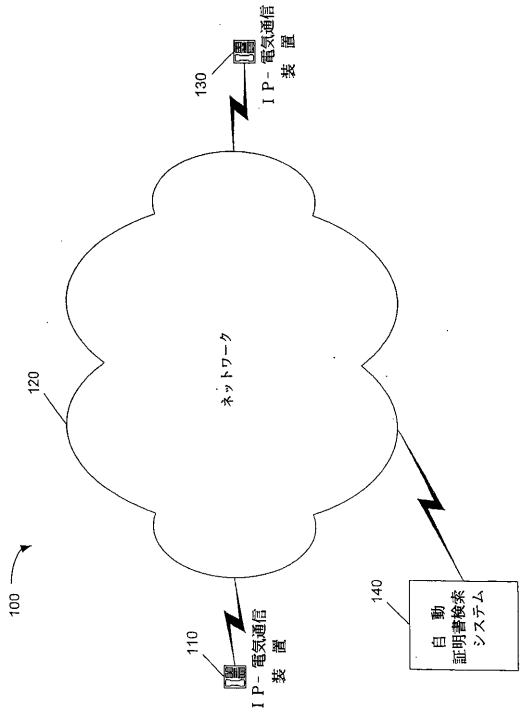
【図８】本発明の１実施形態によるＶＯＩＰ通信における自動証明書検索／転送および取消しのためのプロセスを示す詳細なプロセスフロー図。

【図９】本発明の１実施形態によるＶＯＩＰ通信における証明書登録および自動検索／転送および取消し方法を示すトップレベルのフロー図。

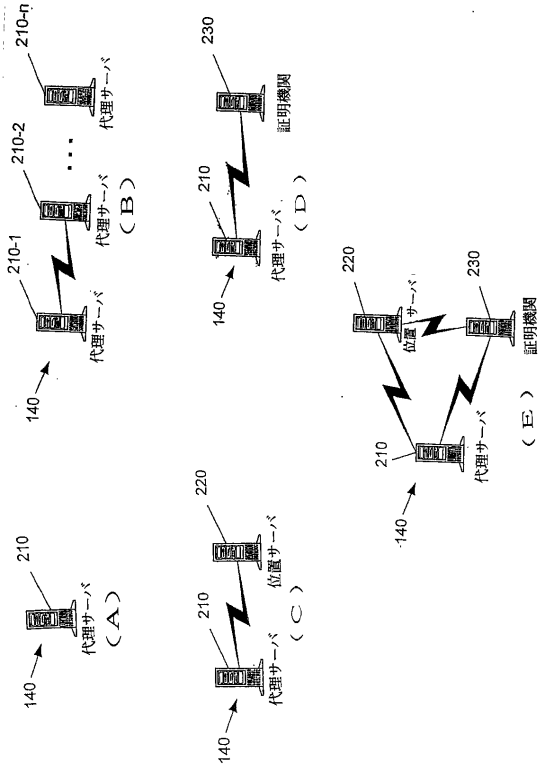
【図１０】本発明の１実施形態によるＶＯＩＰ通信における証明書登録方法を示す詳細なフロー図。

【図１１】本発明の１実施形態によるＶＯＩＰ通信における自動証明書検索／転送および取消し方法を示す詳細なフロー図。

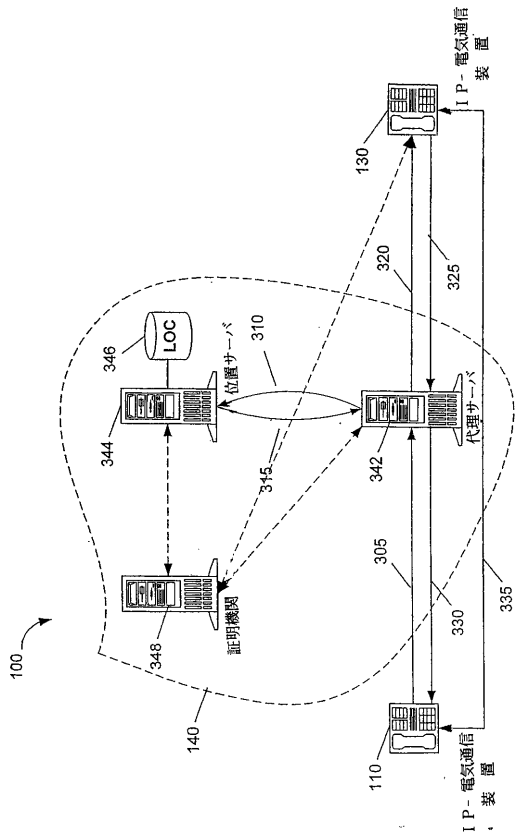
【図１】


100
120
ネットワーク
130
IP-電気通信装置
110
IP-電気通信装置
140
自動証明書検索システム

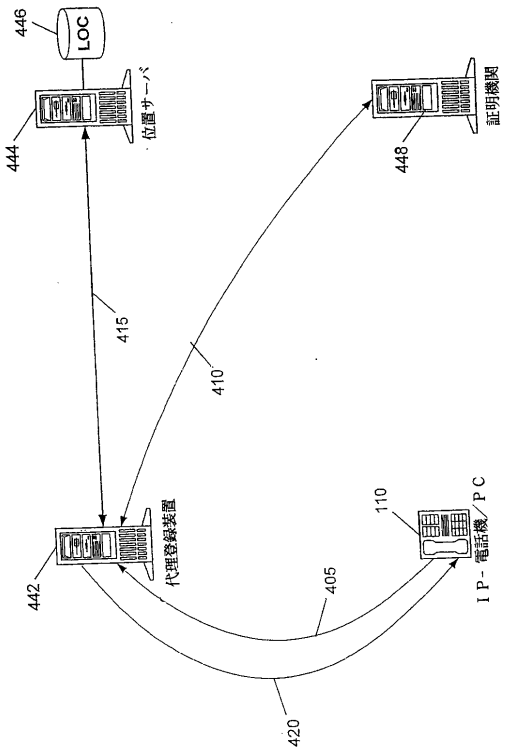
【図２】


210-n
210-2
210-1
210
代理サーバ
140
(A)
(B)
230
証明機関
(D)
220
位置サーバ
(C)
(E)

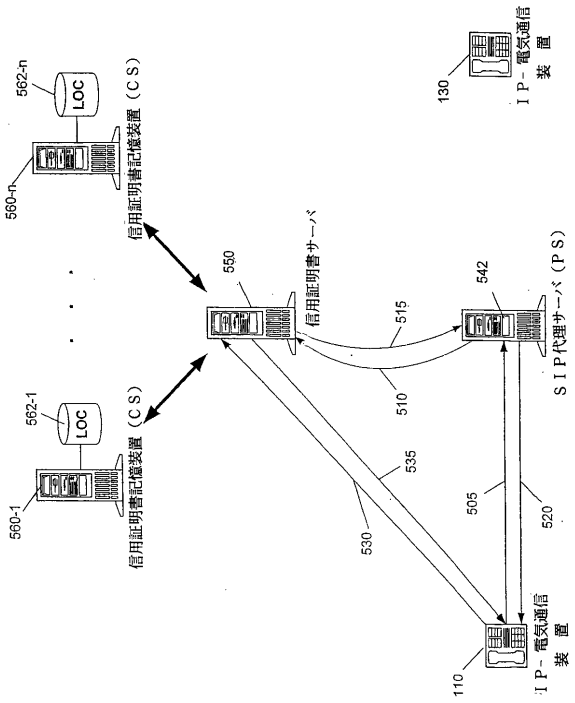
【図３】


100
130
IP-電気通信装置
320
325
346
LOC
位置サーバ
310
344
代理サーバ
342
345
証明機関
348
305
330
335
140
110
IP-電気通信装置

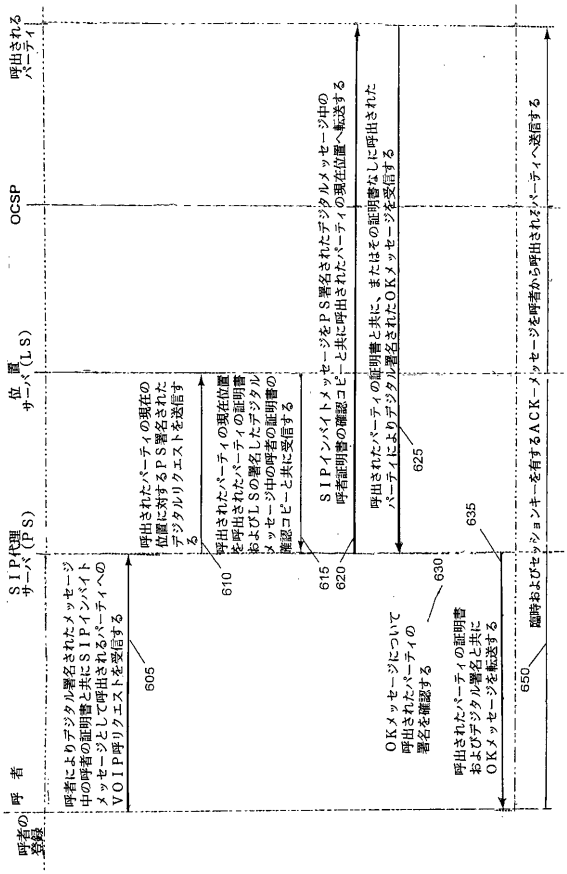
【図４】


446
LOC
位置サーバ
444
415
410
448
証明機関
442
代理登録装置
405
110
IP-電話機/PC
420

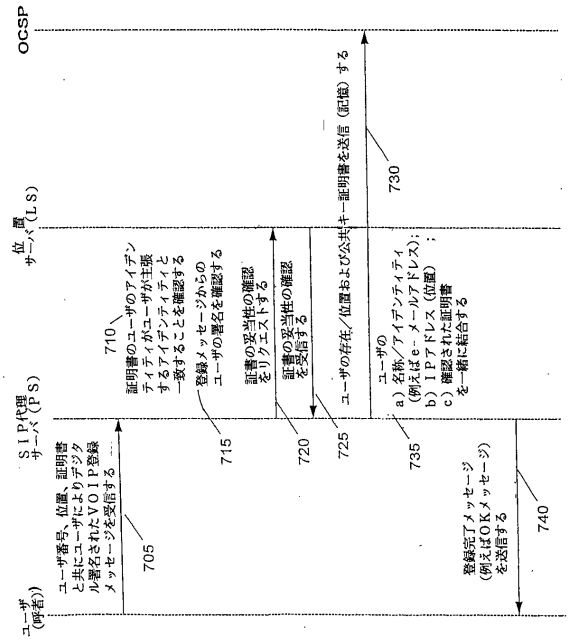
【図５】


560-n
562-n
LOC
信用証明書記憶装置（ＣＳ）
560-1
562-1
LOC
信用証明書記憶装置（ＣＳ）
550
信用証明書サーバ
515
510
542
ＳＩＰ代理サーバ（ＰＳ）
130
ＩＰ－電気通信装置
535
530
505
520
110
ＩＰ－電気通信装置

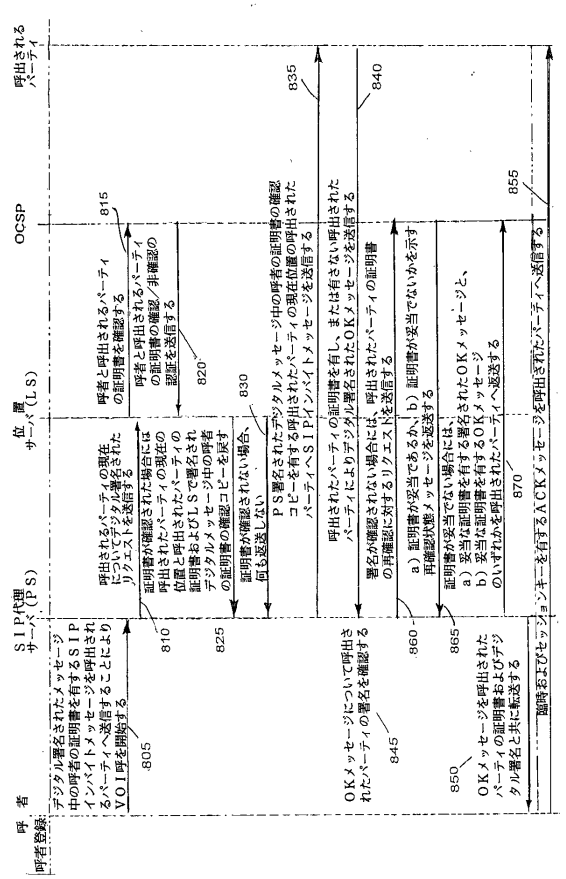
【図６】


呼者
ＳＩＰ代理サーバ（ＰＳ）
位置サーバ（ＬＳ）
OCSP
呼出されるパーティ
呼者の登録
605
610
615
620
625
630
635
650

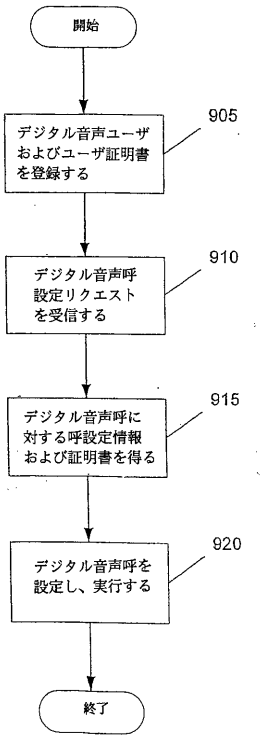
【図７】


ユーザ（呼者）
ＳＩＰ代理サーバ（ＰＳ）
位置サーバ（ＬＳ）
OCSP
705
710
715
720
725
730
735
740

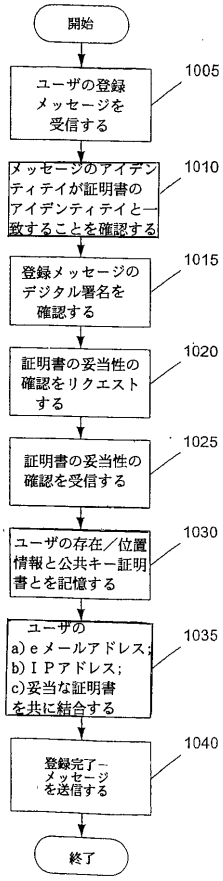
【図８】


呼者
呼者登録
ＳＩＰ代理サーバ（ＰＳ）
位置サーバ（ＬＳ）
OCSP
呼出されるパーティ
805
810
815
820
825
830
835
840
845
850
855
860
865
870

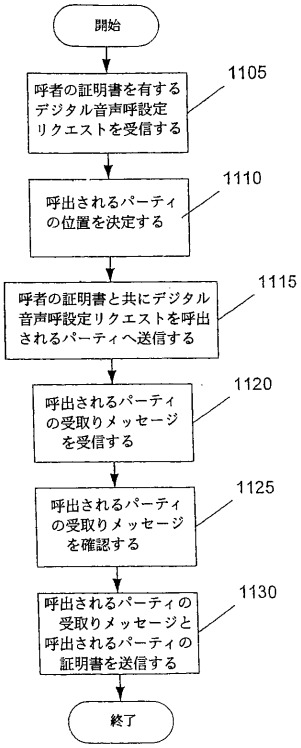
【図９】


開始
デジタル音声ユーザおよびユーザ証明書を登録する
905
デジタル音声呼設定リクエストを受信する
910
デジタル音声呼に対する呼設定情報および証明書を得る
915
デジタル音声呼を設定し、実行する
920
終了

【図１０】


開始
ユーザの登録メッセージを受信する
1005
メッセージのアイデンティティテイが証明書のアイデンティティテイと一致することを確認する
1010
登録メッセージのデジタル署名を確認する
1015
証明書の妥当性の確認をリクエストする
1020
証明書の妥当性の確認を受信する
1025
ユーザの存在／位置情報と公共キー証明書とを記憶する
1030
ユーザの
a) ｅメールアドレス;
b) ＩＰアドレス;
c) 妥当な証明書
を共に結合する
1035
登録完了メッセージを送信する
1040
終了

【図１１】


開始
呼者の証明書を有するデジタル音声呼設定リクエストを受信する
1105
呼出されるパーティの位置を決定する
1110
呼者の証明書と共にデジタル音声呼設定リクエストを呼出されるパーティへ送信する
1115
呼出されるパーティの受取りメッセージを受信する
1120
呼出されるパーティの受取りメッセージを確認する
1125
呼出されるパーティの受取りメッセージと呼出されるパーティの証明書を送信する
1130
終了

フロントページの続き

(72)発明者　ハードジョーノ，トーマス　ピー.
アメリカ合衆国，マサチューセッツ　０１８９０，ウィンチェスター，ハイランド　アベニュ　４３０

審査官　吉田　隆之

(56)参考文献　特表２００３－５２６２７６（ＪＰ，Ａ）
国際公開第０１／６７６７５（WO，Ａ１）
Internet-Draft draft-ietf-mmusic-sip-sec-00.txt
Internet-Draft draft-garcia-sip-called-party-id-04.txt
Internet-Draft draft-sparks-sip-multiproxy-auth-00.txt

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12