(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2006-270431
(P2006-270431A)
(43)公開日　平成18年10月5日(2006.10.5)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	A	5J104
H04M 3/00	(2006.01)	H04M	3/00	E	5K030
H04L 29/08	(2006.01)	H04L	13/00	307A	5K034
H04L 9/32	(2006.01)	H04L	9/00	675A	5K201

審査請求 未請求　請求項の数 10　ＯＬ　（全 15 頁）

(21)出願番号　特願2005-84699(P2005-84699)
(22)出願日　平成17年3月23日(2005.3.23)

(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　齊藤　允
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(72)発明者　アハメッド　アシル
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

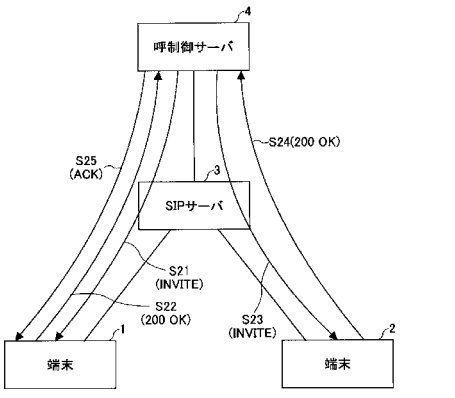
Ｆターム(参考)　5J104 AA07　KA04　PA07

最終頁に続く

(54)【発明の名称】呼制御装置、端末、これらのプログラム、及び通信チャネル確立方法

(57)【要約】
【課題】　アクセス制御に係るセッション管理サーバの負荷を低減させる。
【解決手段】　セッション管理装置とそれぞれ相互認証され、セッション管理装置とそれぞれ暗号化シグナリングチャネルを介して接続された２つの端末間に、第三者呼制御を用いて通信チャネルを確立するための呼制御装置において、セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立する暗号化シグナリングチャネル確立手段と、前記第三者呼制御に基づく接続要求メッセージを、前記暗号化シグナリングチャネルを介して前記２つの端末のそれぞれに送信する呼制御手段とを備える。
【選択図】　図５

本発明の実施の形態における通信システムの構成とシーケンス概要を示す図



【特許請求の範囲】
【請求項１】
セッション管理装置と相互認証され、暗号化シグナリングチャネルを介して接続された呼制御装置による第三者呼制御に基づき、他の端末との間で通信チャネルを確立する端末であって、
セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立する暗号化シグナリングチャネル確立手段と、
前記第三者呼制御に基づき、前記他の端末のセッション情報を含む接続要求メッセージを呼制御装置から受信し、自端末のセッション情報を含む応答メッセージを呼制御装置に送信する呼制御情報処理手段と
を有することを特徴とする端末。
【請求項２】
前記端末は、前記呼制御装置の識別情報を信頼できる装置の識別情報として記録する記録手段を有し、
前記呼制御情報処理手段は、前記記録手段に前記呼制御装置の識別情報が記録されている場合に、前記接続要求メッセージのヘッダ部に含まれる当該接続要求メッセージの送信元アドレスと、前記他の端末のセッション情報に含まれる前記他の端末のアドレスとの比較を行わない請求項１に記載の端末。
【請求項３】
セッション管理装置と相互認証され、暗号化シグナリングチャネルを介して接続された呼制御装置による第三者呼制御に基づき、他の端末との間で通信チャネルを確立する端末であって、
セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立する暗号化シグナリングチャネル確立手段と、
前記第三者呼制御に基づき、呼制御装置からセッション情報を含まない接続要求メッセージを受信し、自端末のセッション情報を含む応答メッセージを呼制御装置に送信する呼制御情報処理手段と
を有することを特徴とする端末。
【請求項４】
前記端末は、前記呼制御装置の識別情報を信頼できる装置の識別情報として記録する記録手段を有し、
前記呼制御情報処理手段は、前記記録手段に前記呼制御装置の識別情報が記録されている場合に、呼制御情報から受信した第三者呼制御に基づく受信確認メッセージのヘッダ部に含まれる送信元アドレスと、前記受信確認メッセージに含まれる前記他の端末のセッション情報内の前記他の端末のアドレスとの比較を行わない請求項３に記載の端末。
【請求項５】
セッション管理装置とそれぞれ相互認証され、セッション管理装置とそれぞれ暗号化シグナリングチャネルを介して接続された２つの端末間に、第三者呼制御を用いて通信チャネルを確立するための呼制御装置であって、
セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立する暗号化シグナリングチャネル確立手段と、
前記第三者呼制御に基づく接続要求メッセージを、前記暗号化シグナリングチャネルを介して前記２つの端末のそれぞれに送信する呼制御手段と
を有することを特徴とする呼制御装置。
【請求項６】
前記接続要求メッセージに対する応答メッセージのヘッダ部に含まれる当該応答メッセージの送信元アドレスと、当該応答メッセージに含まれるセッション情報内の送信元アド

レスとが一致するか否かの確認を行う確認手段を有する請求項５に記載の呼制御装置。
【請求項７】
ネットワークに接続された第１の端末、第２の端末、呼制御装置、及びセッション管理装置を有する通信システムにおいて、呼制御装置による第三者呼制御に基づき第１の端末と第２の端末間で通信チャネルを確立するための方法であって、
セッション管理装置と第１の端末との間で暗号化シグナリングチャネルを確立し、相互認証を行い、セッション管理装置と第２の端末との間で暗号化シグナリングチャネルを確立し、相互認証を行い、セッション管理装置と呼制御装置との間で暗号化シグナリングチャネルを確立し、相互認証を行うステップと、
呼制御装置が、前記第三者呼制御に基づく接続要求メッセージを前記暗号化シグナリングチャネルを介して第１の端末に送信し、この接続要求メッセージを受信した第１の端末が、自身のセッション情報を含む応答メッセージを前記暗号化シグナリングチャネルを介して呼制御サーバに送信するステップと、
前記応答メッセージを受信した呼制御サーバが、前記暗号化シグナリングチャネルを介して、受信したセッション情報を含む接続要求メッセージを第２の端末に送信し、この接続要求メッセージを受信した第２の端末が、自身のセッション情報を含む応答メッセージを前記暗号化シグナリングチャネルを介して呼制御装置に送信するステップと、
前記応答メッセージを受信した呼制御サーバが、前記暗号化シグナリングチャネルを介して、受信したセッション情報を含む受信確認メッセージを第１の端末に送信するステップと
を有することを特徴とする方法。
【請求項８】
セッション管理装置と相互認証され、暗号化シグナリングチャネルを介して接続された呼制御装置による第三者呼制御に基づき、他の端末との間で通信チャネルを確立するための処理をコンピュータに実行させるプログラムであって、コンピュータを、
セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立する暗号化シグナリングチャネル確立手段、
前記第三者呼制御に基づき、前記他の端末のセッション情報を含む接続要求メッセージを呼制御装置から受信し、自身のセッション情報を含む応答メッセージを呼制御装置に送信する呼制御情報処理手段、
として機能させるプログラム。
【請求項９】
セッション管理装置と相互認証され、暗号化シグナリングチャネルを介して接続された呼制御装置による第三者呼制御に基づき、他の端末との間で通信チャネルを確立するための処理をコンピュータに実行させるプログラムであって、コンピュータを、
セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立する暗号化シグナリングチャネル確立手段、
前記第三者呼制御に基づき、呼制御装置からセッション情報を含まない接続要求メッセージを受信し、自身のセッション情報を含む応答メッセージを呼制御装置に送信する呼制御情報処理手段、
として機能させるプログラム。
【請求項１０】
セッション管理装置とそれぞれ相互認証され、セッション管理装置とそれぞれ暗号化シグナリングチャネルを介して接続された２つの端末間に、第三者呼制御を用いて通信チャネルを確立するための処理をコンピュータに実行させるプログラムであって、コンピュータを、
セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立す

る暗号化シグナリングチャネル確立手段、
前記第三者呼制御に基づく接続要求メッセージを、前記暗号化シグナリングチャネルを介して前記２つの端末のそれぞれに送信する呼制御手段、
として機能させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セッション管理サーバを用いて端末間でデータチャネルを構築するシステムにおけるアクセス制御を効率的に行う技術に関する。
【背景技術】
【０００２】
セッション管理サーバを介して端末間でチャネルを構築するシステムの例を図１に示す。図１に示すシステムでは、端末１と端末２との間にセッション管理サーバ３を設置し、端末１－セッション管理サーバ３－端末２間で、端末１－端末２間のデータチャネル構築のためのシグナリング（信号手順）を実行し、データチャネル構築後はセッション管理サーバ３を介さずに端末間のみでデータ通信を行うというものである。
【０００３】
まず、端末１－セッション管理サーバ３間、セッション管理サーバ３－端末２間の各々で、ＩＰｓｅｃ等の暗号化通信を行うためのセキュアシグナリングチャネルが確立される。そして、端末１－セッション管理サーバ３間、セッション管理サーバ３－端末２間の各々で確立されたセキュアシグナリングチャネルを介して、端末１、２からセッション管理サーバ３へのアクセスがなされ、端末１－端末２間のデータチャネル確立のためのシグナリングが実行される。上記のシグナリングのための手段として例えばＳＩＰプロトコルが用いられる。
【０００４】
図１に示すシステムでは、セッション管理サーバ３は特定の端末に対してのみアクセスを許容するためのアクセス制御を行う。そのために、セッション管理サーバ３は、端末毎にその端末がどの端末と通信できるかを登録した図２に示すようなアクセス制御リストを有している。ある端末が他の端末に対する接続要求をセッション管理サーバ３に送信すると、セッション管理サーバ３は図２のリストを参照し、その通信が許可されているか否かをチェックし、許可されている場合にこの接続要求を他の端末に転送する。
【特許文献１】特開２００２－２０８９２１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、アクセス制御のために上記の技術を用いた場合、アクセス制御の対象となる端末の数が膨大になるとセッション管理サーバ３の負荷が増大し、ユーザ収容率あるいは処理速度等の性能が低下する恐れがある。
【０００６】
セッション管理サーバ３に接続される端末として１０００台のカメラと１００台のモニタを有するビル管理システムを例にとると、図３に示すリストが必要となる。この場合、モニタ１００台の各々に対してカメラ１～１０００（１０００台分）の許可エントリー（１０万エントリー）が管理され、更に、カメラ１０００台の各々に対してモニタ１～１００（１００台分）の許可エントリー（１０万エントリー）が管理され、合計２０万エントリーのリストが管理されることになる。モニタもしくはカメラから接続要求を受ける度にこのリストを検索することになるので、セッション管理サーバ３の負荷が増大する。
【０００７】
更に、例えば上記の構成にモニタが１台追加されると、１０００台のカメラの許可エントリーの各々にこのモニタを追加する必要があり、管理が煩雑であるという問題もある。
【０００８】

本発明は上記の点に鑑みてなされたものであり、アクセス制御に係るセッション管理サーバの負荷を低減させる技術を提供することを目的とする。

【課題を解決するための手段】

【０００９】

上記の課題は、セッション管理装置と相互認証され、暗号化シグナリングチャネルを介して接続された呼制御装置による第三者呼制御に基づき、他の端末との間で通信チャネルを確立する端末であって、セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立する暗号化シグナリングチャネル確立手段と、前記第三者呼制御に基づき、前記他の端末のセッション情報を含む接続要求メッセージを呼制御装置から受信し、自端末のセッション情報を含む応答メッセージを呼制御装置に送信する呼制御情報処理手段とを有することを特徴とする端末により解決できる。

【００１０】

前記端末は、前記呼制御装置の識別情報を信頼できる装置の識別情報として記録する記録手段を有し、前記呼制御情報処理手段は、前記記録手段に前記呼制御装置の識別情報が記録されている場合に、前記接続要求メッセージのヘッダ部に含まれる当該接続要求メッセージの送信元アドレスと、前記他の端末のセッション情報に含まれる前記他の端末のアドレスとの比較を行わないこととしてもよい。

【００１１】

また、本発明は、セッション管理装置と相互認証され、暗号化シグナリングチャネルを介して接続された呼制御装置による第三者呼制御に基づき、他の端末との間で通信チャネルを確立する端末であって、セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立する暗号化シグナリングチャネル確立手段と、前記第三者呼制御に基づき、呼制御装置からセッション情報を含まない接続要求メッセージを受信し、自端末のセッション情報を含む応答メッセージを呼制御装置に送信する呼制御情報処理手段とを有することを特徴とする端末として構成することもできる。

【００１２】

上記端末は、前記呼制御装置の識別情報を信頼できる装置の識別情報として記録する記録手段を有し、前記呼制御情報処理手段は、前記記録手段に前記呼制御装置の識別情報が記録されている場合に、呼制御情報から受信した第三者呼制御に基づく受信確認メッセージのヘッダ部に含まれる送信元アドレスと、前記受信確認メッセージに含まれる前記他の端末のセッション情報内の前記他の端末のアドレスとの比較を行わないこととしてもよい。

【００１３】

また、本発明は、セッション管理装置とそれぞれ相互認証され、セッション管理装置とそれぞれ暗号化シグナリングチャネルを介して接続された２つの端末間に、第三者呼制御を用いて通信チャネルを確立するための呼制御装置であって、セッション管理装置との間で暗号化通信のための鍵情報を交換し、セッション管理装置と相互に認証を行い、セッション管理装置との間で暗号化シグナリングチャネルを確立する暗号化シグナリングチャネル確立手段と、前記第三者呼制御に基づく接続要求メッセージを、前記暗号化シグナリングチャネルを介して前記２つの端末のそれぞれに送信する呼制御手段とを有することを特徴とする呼制御装置として構成することもできる。

【００１４】

前記呼制御装置において、前記接続要求メッセージに対する応答メッセージのヘッダ部に含まれる当該応答メッセージの送信元アドレスと、当該応答メッセージに含まれるセッション情報内の送信元アドレスとが一致するか否かの確認を行う確認手段を有することとしてもよい。

【００１５】

また、本発明は、上記の端末、呼制御装置の各手段をコンピュータに実現させるプログ

ラムとして構成することもできる。

【００１６】

また、本発明は、ネットワークに接続された第１の端末、第２の端末、呼制御装置、及びセッション管理装置を有する通信システムにおいて、呼制御装置による第三者呼制御に基づき第１の端末と第２の端末間で通信チャネルを確立するための方法であって、セッション管理装置と第１の端末との間で暗号化シグナリングチャネルを確立し、相互認証を行い、セッション管理装置と第２の端末との間で暗号化シグナリングチャネルを確立し、相互認証を行い、セッション管理装置と呼制御装置との間で暗号化シグナリングチャネルを確立し、相互認証を行うステップと、呼制御装置が、前記第三者呼制御に基づく接続要求メッセージを前記暗号化シグナリングチャネルを介して第１の端末に送信し、この接続要求メッセージを受信した第１の端末が、自身のセッション情報を含む応答メッセージを前記暗号化シグナリングチャネルを介して呼制御サーバに送信するステップと、前記応答メッセージを受信した呼制御サーバが、前記暗号化シグナリングチャネルを介して、受信したセッション情報を含む接続要求メッセージを第２の端末に送信し、この接続要求メッセージを受信した第２の端末が、自身のセッション情報を含む応答メッセージを前記暗号化シグナリングチャネルを介して呼制御装置に送信するステップと、前記応答メッセージを受信した呼制御サーバが、前記暗号化シグナリングチャネルを介して、受信したセッション情報を含む受信確認メッセージを第１の端末に送信するステップとを有することを特徴とする方法として構成してもよい。

【発明の効果】

【００１７】

本発明によれば、セッション管理装置と相互認証され、暗号化シグナリングチャネルで接続された呼制御装置が端末に対する第三者呼制御を行うことにより端末間の通信チャネルを構築することとしたため、セッション管理装置は、端末間毎のアクセス制御リストを持つ必要はなく、呼制御装置と端末間の通信を許可するアクセス制御リストを持つだけで端末間の通信チャネル構築をセキュアに行うことができる。従って、端末数が多くてもセッション管理装置の負荷を増大させることなくアクセス制御をセキュアに行うことが可能となる。

【発明を実施するための最良の形態】

【００１８】

以下、本発明の実施の形態について説明するが、その前に本発明の実施の形態の前提となる端末間でセキュアデータチャネル構築を行う技術について説明する。

【００１９】

図４にそのシーケンスを示す。図４に示すシーケンスは、図１に示した通りの端末１、セッション管理サーバ３、端末２がＩＰネットワークに接続されたシステム構成に基づくものである。

【００２０】

各端末は、セッション管理サーバ３との間でシグナリングを実行するシグナリング機能、セキュアデータチャネルを介してデータ通信を行うための機能、及びデータ通信を利用して所望のサービスを提供するアプリケーションを備えている。

【００２１】

また、セッション管理サーバ３は、シグナリングを各端末との間で実行するシグナリング機能、端末間の接続許可等を制御する接続ポリシー制御機能、各端末を認証するための認証機能、端末の名前からＩＰアドレスを取得する名前解決機能、及び、認証のために用いるＩＤ、パスワードを格納するデータベースや、名前とＩＰアドレス等を対応付けて格納するデータベース等を備えている。また、名前解決機能として一般のＤＮＳと同等の機能を持たせることもできる。

【００２２】

図４に示すように、端末１－端末２間でのセキュアデータチャネル構築にあたり、まず、端末１－セッション管理サーバ３間、端末２－セッション管理サーバ３間の各々でセキ

ュアシグナリングチャネルを構築して、名前の登録を行う。詳細は下記の通りである。

【００２３】

予め端末１、端末２の各々のＩＤとパスワードがセッション管理サーバ３に配布され、セッション管理サーバ３のＩＤ、パスワードが端末１、端末２に配布されている。まず、端末１－セッション管理サーバ３間でＩＰｓｅｃ等の暗号通信で用いる鍵情報の交換を行う（ステップ１）。その後、自分のＩＤ、パスワードを含む情報を暗号化して相手側に送信することにより、相互に認証を行う（ステップ２）。認証後は、セキュアシグナリングチャネル（暗号化シグナリングチャネル）が確立された状態となり、そのチャネルを用いて、端末１は名前とＩＰアドレスの登録をセッション管理サーバ３に対して行う（ステップ３）。端末１の通信相手となる端末２とセッション管理サーバ３間でも同様のシーケンスが実行され、端末２の名前とＩＰアドレスがセッション管理サーバ３に登録される（ステップ４、５、６）。

【００２４】

その後、端末１から端末２への接続要求が、セキュアシグナリングチャネルを介して送信される（ステップ７）。接続要求には、端末２の名前とセッション情報（端末１のアドレス、暗号通信用の鍵情報（暗号鍵生成用の情報）等）が含まれる。接続要求を受信したセッション管理サーバ３は、端末１からの接続要求に関して、端末１が嘘をついていないことをチェックし（発信者詐称チェック）、更に、アクセス許可リストを用いて端末１と端末２の通信が許可されているかをチェックし（ステップ８）、許可されていれば、名前解決機能を用いてデータベースを参照することにより端末２の名前から端末２のＩＰアドレスを取得し（ステップ９）、セキュアシグナリングチャネルを介して端末２へ接続要求を転送する（ステップ１０）。端末１と端末２の通信が許可されていなければ、端末１の接続要求は拒否される。このとき、端末２に関する情報は端末１には全く送信されない。

【００２５】

接続要求を受信した端末２は、接続要求に対する応答として、自分のセッション情報（暗号通信用の鍵情報等）を含む応答メッセージをセキュアシグナリングチャネルを介してセッション管理サーバ３に送信し（ステップ１１）、セッション管理サーバ３が、ステップ８と同様のポリシー制御等を行って、その応答メッセージを端末１に送る（ステップ１２）。

【００２６】

この手順により、端末１と端末２との間での暗号化通信が可能となる。すなわち、セキュアデータチャネルが確立され、所望のデータ通信が行われる。

【００２７】

上記のシーケンスを実現する手段として、ＳＩＰ（session initiation protocol）に基づくプロトコルを用いることが可能である。この場合、セキュアシグナリングチャネルの確立及び名前登録のためにＲＥＧＩＳＴＥＲリクエストメッセージを用い、端末１－端末２間のセキュアデータチャネル確立のためにＩＮＶＩＴＥリクエストメッセージを用いることができる。また、ステップ７の後の発信者詐称チェックは次のようにして行うことができる。

【００２８】

セッション管理サーバ３は、端末１の名前、ＩＰアドレス、ポート番号、端末１とセッション管理サーバ３間のセキュアシグナリングチャネルのコネクションを識別する情報（例えばＩＰｓｅｃＳＡ）を対応付けて保持している。従って、セッション管理サーバ３は、ＩＮＶＩＴＥリクエストメッセージを受信したコネクション情報から、端末１の名前と端末１のＩＰアドレスとを把握でき、それらと、ＩＮＶＩＴＥリクエストメッセージの中のＦｒｏｍ行（メッセージの送信元の名前が記述される行）に記述された名前と、Ｃｏｎｔａｃｔ行（メッセージの送信元のＩＰアドレスが記述される行）に記述されるＩＰアドレスとを比較することにより、名前やＩＰアドレスに詐称がないことを判断できる。

【００２９】

図４のシーケンスのように、ステップ１、２及び４、５を経てセキュアシグナリングチ

ャネルが確立されているということは、端末－セッション管理サーバ間で相互に認証が成功しており、信頼関係が成立しているということである。端末１－セッション管理サーバ３間、及び端末２－セッション管理サーバ３間の各々でこのような関係が成立しているので、端末１と端末２との間も相互に信頼できる関係となることから、ステップ７以降は、一般の暗号化通信で用いられる鍵交換手順より簡略化した手順を用いることが可能となっている。

【００３０】

従って上記のシーケンスでは、ＳＤＰ（セッション情報）に証明書の配布が面倒な電子署名を付けること等はしない。その代わり、ＳＤＰの正当性をチェックするために、ステップ１０でＩＮＶＩＴＥリクエストメッセージを受信した端末２は、ＩＮＶＩＴＥリクエストメッセージのヘッダ部におけるＣｏｎｔａｃｔ行と、ＳＤＰ内のｃ行（セッションの通信相手のＩＰアドレス、すなわち端末１のＩＰアドレスが記述される）とを比較してこれらが一致している場合にＳＤＰは正当であると判定し、セッションを継続する。２００ＯＫレスポンスメッセージを受信する端末２側でも同様のチェックを行う。ＩＮＶＩＴＥリクエストメッセージのヘッダ部のＣｏｎｔａｃｔ行の正当性（詐称がないこと）がシステム側（セッション管理サーバ側）で保障されているので、上記のような簡易なチェックによりＳＤＰが正常であることを確認できる。

【００３１】

（本発明の実施の形態の説明）

図５に、本発明の実施の形態における通信システムの構成を示す。この通信システムは、セッション管理サーバ３としてのＳＩＰサーバ３、呼制御サーバ４、及び、データチャネルを介してデータ通信を行う端末１と端末２を有している。また、各装置はインターネット等のＩＰネットワークに接続されている。実際には多数の端末が接続可能であるが、図５では端末１及び端末２のみを示している。

【００３２】

図５に示す通信システムでは、まず、端末１、端末２及び呼制御サーバ４の各々が、図４のステップ１～３の手順と同様にしてＳＩＰサーバ３との間にセキュアシグナリングチャネルを確立し、名前とＩＰアドレスをＳＩＰサーバ３に登録する。この状態において、各端末－ＳＩＰサーバ３間、及び呼制御サーバ４－ＳＩＰサーバ３間で相互に認証が成功しており、信頼関係が成立している。

【００３３】

ＳＩＰサーバ３は、図６に示すように、呼制御サーバと各端末間の通信のみを許可する内容のアクセス制御リストを備えており、そのアクセス制御リストを参照したアクセス制御に基づき、呼制御サーバが端末１と端末２間のデータチャネル構築に必要な呼制御（第三者呼制御：３ｒｄ Ｐａｒｔｙ Ｃａｌｌ Ｃｏｎｔｒｏｌ、略して３ＰＣＣと呼ばれる）を行い、セキュアシグナリングチャネルを介したシグナリングシーケンスが実行され、端末１と端末２との間のデータチャネルが構築される。なお、図３で示した例と同じ端末数であったとしても、図６のアクセス制御リストの許可エントリー数（２２００）は、図３の例の許可エントリー数（２０万）と比較して桁違いに少なくなる。

【００３４】

（動作概要）

図５を参照して端末１と端末２の間のデータチャネル構築のための動作概要を説明する。まず、呼制御サーバ４が、ＳＤＰを含まないＩＮＶＩＴＥリクエストメッセージを送信することにより端末１を呼び出し（ステップ２１）、端末１は自分のセッション情報を含むＳＤＰを付加した応答メッセージを呼制御サーバ４に返す（ステップ２２）。呼制御サーバ４はそのＳＤＰを含むＩＮＶＩＴＥリクエストメッセージを端末２に送信し（ステップ２３）、端末２は自分のセッション情報を含むＳＤＰを付加した応答メッセージを呼制御サーバ４に返し（ステップ２４）、呼制御サーバ４がそのＳＤＰを含む確認メッセージを端末１に送る（ステップ２５）。これにより、端末１と端末２は互い他のセッション情報を取得し、セッション情報の基づくデータ通信を開始することが可能となる。

【００３５】
上記の手順では、ＳＤＰを含むメッセージを受信する端末１、端末２において、当該メッセージはいずれも呼制御サーバ４から受信することになるので、Ｃｏｎｔａｃｔ行とＳＤＰ内のｃ行とが異なることになる。図４で説明した例では、Ｃｏｎｔａｃｔ行とＳＤＰ内のｃ行とが異なればセッションを中止することとしているが、本実施の形態では、各端末は呼制御サーバ４を信頼するものとし（具体的には、信頼するサーバとして呼制御サーバ４を端末内に記録しておく）、信頼するサーバとして記録されている呼制御サーバ４から送られたＳＤＰはそのまま信頼するものとし、Ｃｏｎｔａｃｔ行とＳＤＰ内のｃ行との比較チェックを行わないこととしている。従って、Ｃｏｎｔａｃｔ行とＳＤＰ内のｃ行とが異なっていてもセッションが継続される。

【００３６】
（動作詳細）
次に、図７のシーケンスチャートを参照して本実施の形態のシステムの動作を詳細に説明する。

【００３７】
図７の例では、呼制御サーバ４のＩＰアドレスが１７２．１６．０．１、名前が３ＰＣＣ@ａｂｃ．ｃｏｍであり、端末１のＩＰアドレスが１９２．１６８．０．１、名前がＵＡ１@ａｂｃ．ｃｏｍであり、端末２のＩＰアドレスが１０．０．０．１、名前がＵＡ２@ａｂｃ．ｃｏｍであるものとする。

【００３８】
ステップ３１）まず、呼制御サーバ４は、ヘッダ部にＦｒｏｍ：　３ＰＣＣ@ａｂｃ．ｃｏｍ（呼制御サーバ４の名前）、Ｔｏ：　ＵＡ１@ａｂｃ．ｃｏｍ（端末１の名前）、Ｃｏｎｔａｃｔ：　１７２．１６．０．１（呼制御サーバ４のＩＰアドレス）を含み、ＳＤＰの記述を含まないＩＮＶＩＴＥリクエストメッセージを端末１に向けて送信する。

【００３９】
ＩＮＶＩＴＥリクエストメッセージを受信したＳＩＰサーバ３は、図４で示した発信者詐称チェックにおける処理と同様にして、Ｆｒｏｍ行の内容、Ｃｏｎｔａｃｔ行の内容が確かに呼制御サーバ４のものであることを確認する。Ｆｒｏｍ行の内容、もしくはＣｏｎｔａｃｔ行の内容が呼制御サーバ４のものと異なる場合にはセッションを中止する。

【００４０】
また、ＳＩＰサーバ３は、図６に示したアクセス制御リストを参照し、呼制御サーバ４から端末１への通信が許可されていることを確認し、ＩＮＶＩＴＥリクエストメッセージを端末１に転送する。

【００４１】
ステップ３２）ＩＮＶＩＴＥリクエストメッセージを受信した端末１は、ヘッダ部にＦｒｏｍ：　３ＰＣＣ@ａｂｃ．ｃｏｍ（呼制御サーバ４の名前）、Ｔｏ：　ＵＡ１@ａｂｃ．ｃｏｍ（端末１の名前）、Ｃｏｎｔａｃｔ：　１９２．１６８．０．１（端末１のＩＰアドレス）を含み、自分のセッション情報を含むＳＤＰ（ｃ＝１９２．１６８．０．１（端末１のＩＰアドレス）を含む）を有する２００　ＯＫレスポンスメッセージを呼制御サーバ４に向けて送信する。

【００４２】
レスポンスメッセージに関しては、ＳＩＰサーバ３は、図４で示した発信者詐称チェックにおける処理と同様にして、Ｔｏ行の内容とＣｏｎｔａｃｔ行の内容が確かに端末１のものであることをチェックする。ｃ行を含むＳＤＰの中身については暗号化されることがあるので確認しない。

【００４３】
ステップ３３）２００　ＯＫレスポンスメッセージを受信した呼制御サーバ４は、Ｃｏｎｔａｃｔ行の内容とｃ行の内容とが同一（１９２．１６８．０．１：端末１のＩＰアドレス）であることを確認し、端末１がＳＤＰの中身についても嘘をついていないことを確認する。

【００４４】
そして、呼制御サーバ４は、ヘッダ部にＦｒｏｍ：　３ＰＣＣ@ａｂｃ．ｃｏｍ（呼制御サーバ４の名前）、Ｔｏ：　ＵＡ２@ａｂｃ．ｃｏｍ（端末２の名前）、Ｃｏｎｔａｃｔ：　１７２．１６．０．１（呼制御サーバ４のＩＰアドレス）を含み、端末１から受信したＳＤＰ（ｃ＝１９２．１６８．０．１（端末１のＩＰアドレス）を含む）を有するＩＮＶＩＴＥリクエストメッセージを端末２に向けて送信する。
【００４５】
ＩＮＶＩＴＥリクエストメッセージを受信したＳＩＰサーバ３は、Ｆｒｏｍ行の内容とＣｏｎｔａｃｔ行の内容が確かに呼制御サーバ４のものであることを確認する。ｃ行を含むＳＤＰの中身については暗号化されることがあるので確認しない。また、ＳＩＰサーバ３は、アクセス制御リストを参照し、呼制御サーバ４から端末２への通信が許可されていることを確認し、ＩＮＶＩＴＥリクエストメッセージを端末２に転送する。
【００４６】
ステップ３４）端末２はＩＮＶＩＴＥリクエストメッセージを受信する。このＩＮＶＩＴＥリクエストメッセージのＣｏｎｔａｃｔ行のＩＰアドレス（１７２．１６．０．１：呼制御サーバ４のＩＰアドレス）とｃ行のＩＰアドレス（１９２．１６８．０．１：端末１のＩＰアドレス）とは異なる。このような場合、図４に示したシーケンスでは端末はこれを検出し、セッションを中止していた。
【００４７】
一方、本実施の形態においては、ｃ行のＩＰアドレスが確かに端末１のものであることは呼制御サーバ４が確認しており、また、端末２と呼制御サーバ４間では相互認証によって相互信頼関係が築かれており、端末２は呼制御サーバ４を信頼できるので、端末２はＣｏｎｔａｃｔ行のＩＰアドレスとｃ行のＩＰアドレスとの比較チェックを行わずにセッションを継続する。より具体的には、端末２に予め信頼できるサーバとして呼制御サーバ４の名前等を記録しておき、記録されたサーバから受信したメッセージに含まれるＳＤＰについてはＣｏｎｔａｃｔ行とｃ行との比較チェックを行わないこととする。
【００４８】
続いて、端末２は、ヘッダ部にＦｒｏｍ：　３ＰＣＣ@ａｂｃ．ｃｏｍ（呼制御サーバ４の名前）、Ｔｏ：　ＵＡ２@ａｂｃ．ｃｏｍ（端末２の名前）、Ｃｏｎｔａｃｔ：　１０．０．０．１（端末２のＩＰアドレス）を含み、ｃ＝１０．０．０．１（端末２のＩＰアドレス）を含むＳＤＰを有する２００　ＯＫレスポンスメッセージを呼制御サーバ４に向けて送信する。
【００４９】
２００　ＯＫレスポンスメッセージを受信したＳＩＰサーバ３は、Ｔｏ行の内容とＣｏｎｔａｃｔ行の内容が確かに端末２のものであることを確認し、メッセージを転送する。ｃ行を含むＳＤＰの中身については暗号化されることがあるので確認しない。
【００５０】
ステップ３５）２００　ＯＫレスポンスメッセージを受信した呼制御サーバ４は、Ｃｏｎｔａｃｔ行の内容とｃ行の内容とが同一（１０．０．０．１：端末２のＩＰアドレス）であることを確認し、端末２がＳＤＰの中身についても嘘をついていないことを確認する。
【００５１】
そして、呼制御サーバ４は、ヘッダ部にＦｒｏｍ：　３ＰＣＣ@ａｂｃ．ｃｏｍ（呼制御サーバ４の名前）、Ｔｏ：　ＵＡ１@ａｂｃ．ｃｏｍ（端末１の名前）、Ｃｏｎｔａｃｔ：　１７２．１６．０．１（呼制御サーバ４のＩＰアドレス）を含み、端末２から受信したＳＤＰ（ｃ＝１０．０．０．１（端末２のＩＰアドレス）を含む）を有するＡＣＫリクエストメッセージを端末１に向けて送信する。また、端末２にもＡＣＫリクエストメッセージが送信される。
【００５２】
端末１に向けて送信されたＡＣＫリクエストメッセージを受信したＳＩＰサーバ３は、

Ｆｒｏｍ行の内容とＣｏｎｔａｃｔ行の内容が確かに呼制御サーバ４のものであることを確認し、メッセージを転送する。ＳＤＰの中身に関しては暗号化されることがあるので確認しない。従って、Ｃｏｎｔａｃｔ行の内容とｃ行の内容とが異なっていてもメッセージを破棄することなくセッションが継続される。

【００５３】

このＡＣＫリクエストメッセージを受け取った端末１は信頼できるサーバとして呼制御サーバ４を予め記録しており、ＩＮＶＩＴＥリクエストメッセージを受信した端末２の場合と同様に、Ｃｏｎｔａｃｔ行とｃ行との比較チェックを行わない。そして、ｃ行に記載されたＩＰアドレスに対してセッションを張ることにより、端末１と端末２の間でデータ通信が開始される。

【００５４】

（各装置の機能構成）

次に、本実施の形態における各装置の機能構成を図８を参照して説明する。

【００５５】

ＳＩＰサーバ３は、呼（メッセージ）の転送のための処理を行うＳＩＰプロキシ３１、名前登録を行うＳＩＰレジストラ３２、ＩＤ、パスワード、もしくは証明書等を用いて各端末や呼制御サーバの認証を行う認証モジュール３３、ＩＰｓｅｃ等の暗号化通信を行うための暗号化モジュール３４を有している。

【００５６】

各端末は、セキュアデータチャネル上での通信を行うアプリケーション、第三者呼制御に基づくシグナリングを行う機能やＲＥＧＩＳＴＥＲメッセージの発行等の機能を含むＳＩＰ機能部１２、ＩＤ、パスワード、もしくは証明書等を用いてＳＩＰサーバ３の認証を行う認証モジュール１３、ＩＰｓｅｃ等の暗号化通信を行うための暗号化モジュール１４を有している。

【００５７】

また、呼制御サーバ４は、第三者呼制御の開始の制御等を行うアプリケーション４１、第三者呼制御に基づくシグナリングを行う機能やＲＥＧＩＳＴＥＲメッセージの発行等の機能を含むＳＩＰ機能部４２、ＩＤ、パスワード、もしくは証明書等を用いてＳＩＰサーバ３の認証を行う認証モジュール４３、ＩＰｓｅｃ等の暗号化通信を行うための暗号化モジュール４４を有している。

【００５８】

上記のＳＩＰサーバ３、各端末１、２、呼制御サーバ４の各機能は、プログラムにより実現されるものであり、本発明における各装置の各手段は、プログラムとコンピュータのハードウェア資源とで実現されているものである。また、端末１、２は、ＣＰＵ、メモリ、ハードディスク等の記憶装置を含む一般的なＰＣ等のコンピュータ、モバイル機器、カメラ等であり、当該コンピュータ等にプログラムをインストールすることにより本実施の形態の端末の機能を実現できる。端末はディジタル家電等でもよい。また、ＳＩＰサーバ３、呼制御サーバ４のそれぞれも、記憶装置等を有するコンピュータにプログラムを搭載することにより実現されるものである。

【００５９】

（応用例）

図９に第１の応用例を示す。図９に示す例は、図５の構成における端末を家電製品とし、呼制御サーバ４を携帯電話機としたものである。このようなシステムでは、ＳＩＰサーバに対して、全ての家電製品と携帯電話機との通信を許容するという設定だけを行うことにより、家電製品間の様々な通信を安全に制御することが可能になる。この場合、携帯電話機にマスターキーとしての役割を持たせていると考えることができる。携帯電話機のアプリケーションとしては、例えば利用者の操作により選択した家電製品間での通信を開始させるものや、予め設定した時刻になると所定の家電製品間での通信を開始させるもの等がある。

【００６０】

このような第三者呼制御機能を用いない場合には、カメラとテレビの間の通信を許可する等の設定を利用者がＳＩＰサーバに一つずつ設定することになり非常に煩雑であるが、第三者呼制御機能を導入したことにより簡易な設定で安全な制御を行うことができる。

【００６１】

図１０に第２の応用例を示す。図１０に示す例は、信頼されたグループ内での匿名通信を実現する例である。本実施の形態のシステムでは、信頼される呼制御サーバ４が利用者の端末に代わって発呼を行う。従って、各利用者の端末に送信される呼制御メッセージの中のＦｒｏｍ行には呼制御サーバ４の名前が入るだけであり、他の利用者の名前が入ることはなく、また、Ｔｏ行には呼制御メッセージを受信する端末自身の名前が入るだけなので、図１０に示すような利用者間での安全な匿名通信を実現することが可能となる。

【００６２】

なお、本発明は、上記の実施の形態に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。また、本発明の実施の形態ではＳＩＰを用いているが、本発明はＳＩＰに限定されるものではない。例えば、ＳＩＰに代えてＨＴＴＰを用いることができる。

【図面の簡単な説明】

【００６３】

【図１】セッション管理サーバを介して端末間でチャネルを構築するシステムの例を示す図である。

【図２】アクセス制御リストの例を示す図である。

【図３】アクセス制御リストの例を示す図である。

【図４】端末間でセキュアデータチャネル構築を行う技術について説明するための図である。

【図５】本発明の実施の形態における通信システムの構成とシーケンス概要を示す図である。

【図６】アクセス制御リストの例を示す図である。

【図７】本発明の実施の形態のシステムにおける処理シーケンスを示す図である。

【図８】本発明の実施の形態における各装置の機能構成を示す図である。

【図９】第１の応用例を示す図である。

【図１０】第２の応用例を示す図である。

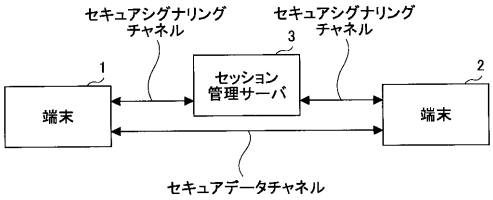
【符号の説明】

【００６４】

１、２　端末
３　セッション管理サーバ、ＳＩＰサーバ
４　呼制御サーバ
１１、４１　アプリケーション
１２、４２　ＳＩＰ機能部
１３、３３、４３　認証モジュール
１４、３４、４４　暗号化モジュール
３１　ＳＩＰプロキシ
３２　ＳＩＰレジストラ

【図１】

セッション管理サーバを介して端末間でチャネルを構築するシステムの例を示す図



【図２】

アクセス制御リストの例を示す図

端末	通信許可端末
端末1	端末2、端末3、・・・
端末2	端末1、・・・・・
端末3	・・・・・・・・・・
・・・・・・	・・・・・・

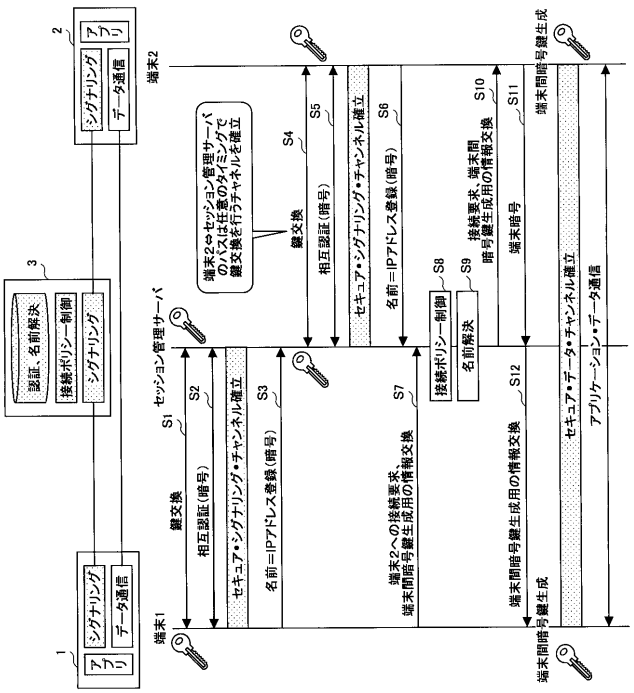
【図３】

アクセス制御リストの例を示す図

端末	通信許可端末
カメラ1	モニタ1、モニタ2、・・・・、モニタ100
カメラ2	モニタ1、モニタ2、・・・・、モニタ100
・・・・・・	・・・・・・
カメラ1000	モニタ1、・・・・・・・・・・・・、モニタ100
モニタ1	カメラ1、カメラ2、・・・・・・、カメラ1000
モニタ2	・・・・・
・・・・・・	・・・・・・
モニタ100	カメラ1、カメラ2、・・・・・・、カメラ1000

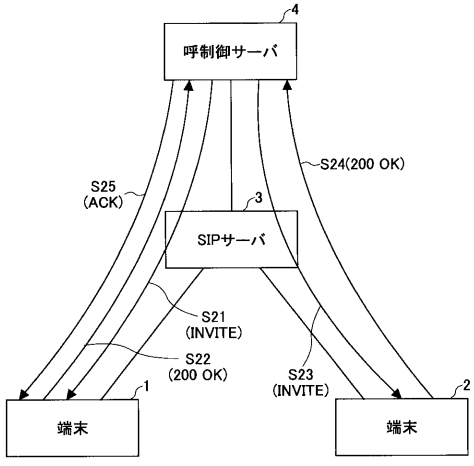
【図４】

端末間でセキュアデータチャネル構築を行う技術について説明するための図



【図５】

本発明の実施の形態における通信システムの構成とシーケンス概要を示す図



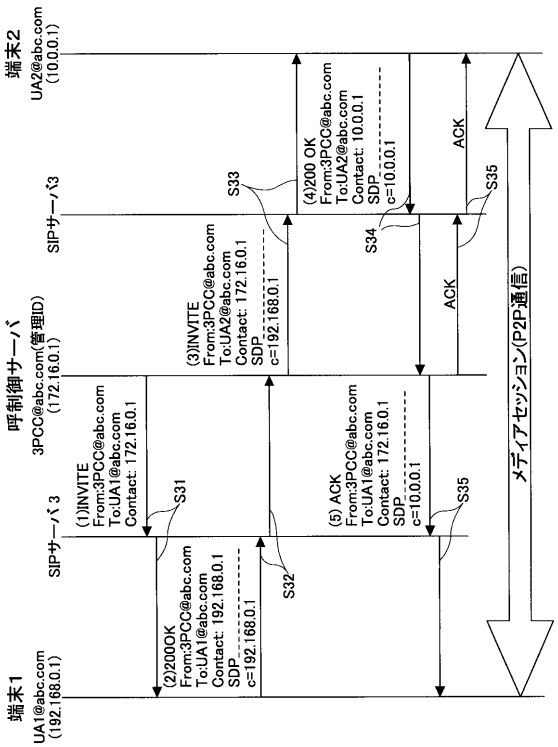
【図６】

アクセス制御リストの例を示す図

	通信許可端末
呼制御サーバ	端末1、端末2、・・・
端末1	呼制御サーバ
端末2	呼制御サーバ
……	……

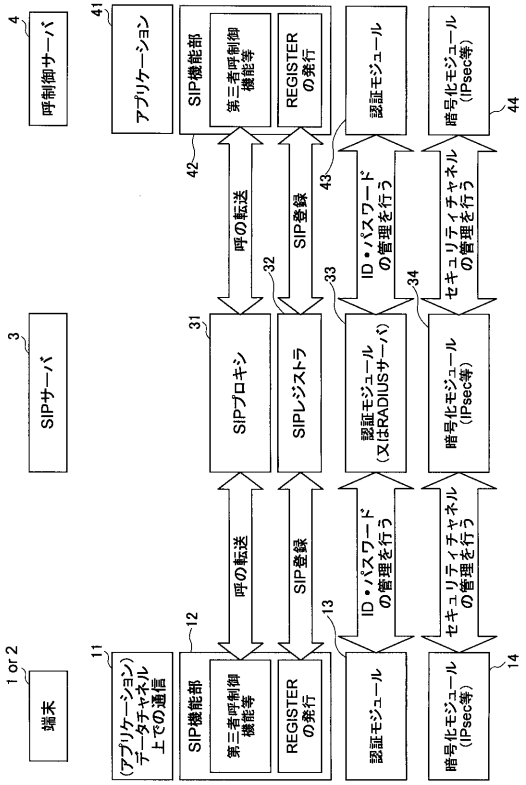
【図７】

本発明の実施の形態のシステムにおける処理シーケンスを示す図



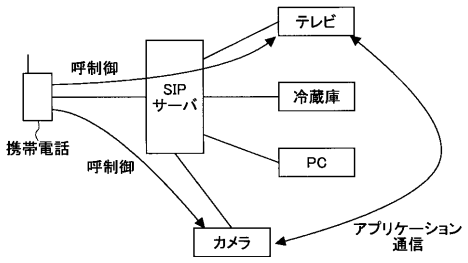
【図８】

本発明の実施の形態における各装置の機能構成を示す図



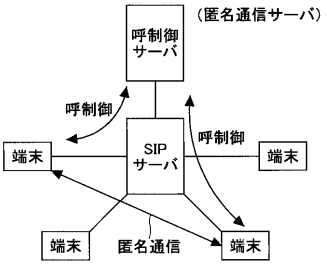
【図９】

第1の応用例を示す図



【図１０】

第2の応用例を示す図



フロントページの続き

Ｆターム(参考) 5K030 LB02 LD19
5K034 AA05 EE11 HH06 HH11 LL01 LL02 NN11
5K201 AA08 AA09 CB06 CD09 EC06