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

特許第5002830号
(P5002830)

(45)発行日　平成24年8月15日(2012.8.15)　(24)登録日　平成24年6月1日(2012.6.1)

(51)Int.Cl.　　F I
H04L 29/06 (2006.01)　　H04L 13/00　305C
H04L 29/08 (2006.01)　　H04L 13/00　307A
H04L 12/66 (2006.01)　　H04L 12/66　B

請求項の数 14　(全 30 頁)

(21)出願番号　特願2007-200107(P2007-200107)
(22)出願日　平成19年7月31日(2007.7.31)
(65)公開番号　特開2009-38536(P2009-38536A)
(43)公開日　平成21年2月19日(2009.2.19)
審査請求日　平成22年5月14日(2010.5.14)

(73)特許権者　501440684
ソフトバンクモバイル株式会社
東京都港区東新橋一丁目９番１号
(74)代理人　100104156
弁理士　龍華　明裕
(72)発明者　瀬田　直也
東京都港区東新橋一丁目９番１号　ソフトバンクモバイル株式会社内
(72)発明者　宮島　春弥
東京都港区東新橋一丁目９番１号　ソフトバンクモバイル株式会社内
(72)発明者　張　亮
東京都港区東新橋一丁目９番１号　ソフトバンクモバイル株式会社内

最終頁に続く

(54)【発明の名称】通信モジュール、通信方法、通信プログラム、通信端末、および通信制御装置

(57)【特許請求の範囲】
【請求項１】
通信データを送受信する通信端末の通信モジュールであって、
シグナリングメッセージを生成するシグナリング制御部と、
前記シグナリング制御部が生成したシグナリングメッセージを、前記通信端末と通信相手端末とのセッションを管理する通信制御装置に送信するシグナリング送受信部と、
第１通信方式で通信する第１通信部と、
第２通信方式で通信する第２通信部と、
を備え、
前記シグナリング制御部は、
前記通信モジュールが起動された場合に、第１セキュリティプロトコルに基づく第１シグナリング用セッションを、前記通信制御装置との間に確立し、
前記第１シグナリング用セッションが確立された場合に、第２セキュリティプロトコルに基づく第２シグナリング用セッションを、前記通信制御装置との間に確立し、
前記シグナリング送受信部は、前記シグナリング制御部が生成したシグナリングメッセージを、前記第２シグナリング用セッションを介して前記通信制御装置に送信し、
前記シグナリング送受信部は、前記通信端末が、前記第１通信部が通信可能な第１エリアから前記第２通信部が通信可能な第２エリアに移動する場合に、前記第２エリアにおいて前記第２通信方式で確立される第３シグナリング用セッションを確立するためのシグナリングメッセージを、前記第１エリアにおいて前記第１通信方式で確立された前記第２シ

グナリング用セッションを介して前記通信制御装置に送信する、通信モジュール。
【請求項２】
前記シグナリング送受信部は、前記第２シグナリング用セッションを確立するためのシグナリングメッセージを、前記第１シグナリング用セッションを介して前記通信制御装置に送信する、請求項１に記載の通信モジュール。
【請求項３】
通信データを生成するアプリケーション部、
をさらに備え、
前記シグナリング送受信部は、前記アプリケーション部が生成した通信データを前記通信相手端末に送信するために用いる第１通信データ用セッションを確立するためのシグナリングメッセージを、前記第２シグナリング用セッションを介して前記通信制御装置に送信する、請求項２に記載の通信モジュール。
【請求項４】
前記シグナリング制御部は、
前記第１セキュリティプロトコルを用いて前記通信端末と前記通信制御装置との相互の認証を得ることによって、前記第１シグナリング用セッションを確立し、
前記第１セキュリティプロトコルを用いて得られた認証の結果を使って、前記第２シグナリング用セッションを確立する、請求項３に記載の通信モジュール。
【請求項５】
前記シグナリング制御部は、
前記第１セキュリティプロトコルであるＴＬＳを用いて、前記第１シグナリング用セッションであるＴＬＳセッションを確立し、
前記第２セキュリティプロトコルであるＳＲＴＰを用いて、前記第２シグナリング用セッションであるＳＲＴＰセッションを確立する、請求項４に記載の通信モジュール。
【請求項６】
前記シグナリング制御部が生成したシグナリングメッセージを、前記第１セキュリティプロトコルに基づいて暗号化する第１暗号化部と、
前記シグナリング制御部が生成したシグナリングメッセージを、前記第２セキュリティプロトコルに基づいて暗号化する第２暗号化部と、
をさらに備える、請求項１に記載の通信モジュール。
【請求項７】
前記シグナリング制御部が生成したシグナリングメッセージを、前記第２セキュリティプロトコルに基づいて暗号化できるデータ形式に変換するデータ形式変換部、
をさらに備え、
前記第２暗号化部は、前記データ形式変換部によってデータ形式が変換されたシグナリングメッセージを、前記第２セキュリティプロトコルに基づいて暗号化する、請求項６に記載の通信モジュール。
【請求項８】
前記データ形式変換部は、前記シグナリング制御部が生成したシグナリングメッセージを、前記第２セキュリティプロトコルであるＳＲＴＰに基づいて暗号化できるデータ形式に変換し、
前記第２暗号化部は、前記データ形式変換部によって変換されたシグナリングメッセージを、ＳＲＴＰに基づいて暗号化する、請求項７に記載の通信モジュール。
【請求項９】
前記通信端末が、前記第１通信部が通信可能な第１エリアから前記第２通信部が通信可能な第２エリアに移動する場合に、
前記シグナリング送受信部は、前記第２エリアにおいて前記第２通信方式で確立される第２通信データ用セッションを確立するためのシグナリングメッセージを、前記第１エリアにおいて前記第１通信方式で確立された前記第２シグナリング用セッションを介して前記通信制御装置に送信する、請求項１から８のいずれか１項に記載の通信モジュール。

【請求項１０】
コンピュータを、請求項１から９のいずれか１項に記載の通信モジュールとして機能させるためのプログラム。
【請求項１１】
通信データを送受信する通信端末により実行される通信方法であって、
前記通信端末が起動された場合に、第１セキュリティプロトコルに基づく第１シグナリング用セッションを、前記通信端末と通信相手端末とのセッションを管理する通信制御装置との間に確立する段階と、
前記第１シグナリング用セッションが確立された場合に、第２セキュリティプロトコルに基づく第２シグナリング用セッションを、前記通信制御装置との間に確立する段階と、
シグナリングメッセージを、前記第２シグナリング用セッションを介して前記通信制御装置に送信する段階と、
前記通信端末が、第１通信方式で通信可能な第１エリアから第２通信方式で通信可能な第２エリアに移動する場合に、前記第２エリアにおいて前記第２通信方式で確立される第３シグナリング用セッションを確立するためのシグナリングメッセージを、前記第１エリアにおいて前記第１通信方式で確立された前記第２シグナリング用セッションを介して前記通信制御装置に送信する段階と、を備える通信方法。
【請求項１２】
通信データを送受信する通信端末であって、
シグナリングメッセージを生成するシグナリング制御部と、
前記シグナリング制御部が生成したシグナリングメッセージを、前記通信端末と通信相手端末とのセッションを管理する通信制御装置に送信するシグナリング送受信部と、
第１通信方式で通信する第１通信部と、
第２通信方式で通信する第２通信部と、
を備え、
前記シグナリング制御部は、
前記通信端末が起動された場合に、第１セキュリティプロトコルに基づく第１シグナリング用セッションを、前記通信制御装置との間に確立し、
前記第１シグナリング用セッションが確立された場合に、第２セキュリティプロトコルに基づく第２シグナリング用セッションを、前記通信制御装置との間に確立し、
前記シグナリング送受信部は、前記シグナリング制御部が生成したシグナリングメッセージを、前記第２シグナリング用セッションを介して前記通信制御装置に送信し、
前記シグナリング送受信部は、前記通信端末が、前記第１通信部が通信可能な第１エリアから前記第２通信部が通信可能な第２エリアに移動する場合に、前記第２エリアにおいて前記第２通信方式で確立される第３シグナリング用セッションを確立するためのシグナリングメッセージを、前記第１エリアにおいて前記第１通信方式で確立された前記第２シグナリング用セッションを介して前記通信制御装置に送信する、通信端末。
【請求項１３】
通信相手端末との間で通信データを送受信する通信端末と、前記通信端末と前記通信相手端末とのセッションを管理する通信制御装置とを備える通信システムであって、
前記通信端末は、
シグナリングメッセージを生成するシグナリング制御部と、
前記シグナリング制御部が生成したシグナリングメッセージを、前記通信端末と通信相手端末とのセッションを管理する通信制御装置に送信するシグナリング送受信部と、
第１通信方式で通信する第１通信部と、
第２通信方式で通信する第２通信部と、
を備え、
前記シグナリング制御部は、
前記通信端末が起動された場合に、第１セキュリティプロトコルに基づく第１シグナリング用セッションを、前記通信制御装置との間に確立し、

前記第１シグナリング用セッションが確立された場合に、第２セキュリティプロトコルに基づく第２シグナリング用セッションを、前記通信制御装置との間に確立し、
前記シグナリング送受信部は、前記シグナリング制御部が生成したシグナリングメッセージを、前記第２シグナリング用セッションを介して前記通信制御装置に送信し、
前記シグナリング送受信部は、前記通信端末が、前記第１通信部が通信可能な第１エリアから前記第２通信部が通信可能な第２エリアに移動する場合に、前記第２エリアにおいて前記第２通信方式で確立される第３シグナリング用セッションを確立するためのシグナリングメッセージを、前記第１エリアにおいて前記第１通信方式で確立された前記第２シグナリング用セッションを介して前記通信制御装置に送信する、通信システム。
【請求項１４】
通信端末と通信相手端末とのセッションを管理する通信制御装置であって、
シグナリングメッセージを生成するシグナリング制御部と、
前記シグナリング制御部が生成したシグナリングメッセージを、前記通信端末に送信するシグナリング送受信部と、
を備え、
前記シグナリング制御部は、
前記通信端末から要求があった場合に、第１セキュリティプロトコルに基づく第１シグナリング用セッションを、前記通信端末との間に確立し、
前記第１シグナリング用セッションが確立された場合に、第２セキュリティプロトコルに基づく第２シグナリング用セッションを、前記通信端末との間に確立し、
前記シグナリング送受信部は、前記シグナリング制御部が生成したシグナリングメッセージを、前記第２シグナリング用セッションを介して前記通信端末に送信し、
前記シグナリング送受信部は、前記通信端末が、前記通信端末が備える第１通信方式で通信する第１通信部が通信可能な第１エリアから、前記通信端末が備える第２通信方式で通信する第２通信部が通信可能な第２エリアに移動する場合に、前記第２エリアにおいて前記第２通信方式で確立される第３シグナリング用セッションを確立するためのシグナリングメッセージを、前記第１エリアにおいて前記第１通信方式で確立された前記第２シグナリング用セッションを介して前記通信端末から受信する、通信制御装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信モジュール、通信方法、通信プログラム、通信端末、および通信制御装置に関する。特に、本発明は、通信データを送受信する通信モジュール、通信方法、通信プログラム、通信端末、および通信制御装置に関する。
【背景技術】
【０００２】
特許文献１には、通信中の通信端末が通信方式を変更して通信が中断した場合に、通信端末のアドレスと未送信の通信データとを自動的に記録して、通信が再開したときに未送信のデータを継続して送信する通信システムについて提案されている。
【特許文献１】特開２００１－２３７８６９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、特許文献１に記載の発明においては、通信端末が通信方式を変更する場合、および通信方式を変更する前後において、通信端末が送受信する通信データについて、適切なセキュリティを確保していない。したがって、特許文献１に記載の発明においては、通信端末のシグナリング、および通信端末が通信相手端末と送受信する通信データの秘匿性を確保できない場合がある。
【０００４】
そこで本発明は、上記課題を解決することができる通信モジュール、通信方法、通信プ

ログラム、および通信端末を提供することを目的とする。この目的は特許請求の範囲における独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

【課題を解決するための手段】

【０００５】

上記課題を解決するために、本発明の第１の形態によれば、通信データを送受信する通信端末通信端末の通信モジュールであって、シグナリングメッセージを生成するシグナリング制御部と、シグナリング制御部が生成したシグナリングメッセージを、通信端末と通信相手端末とのセッションを管理する通信制御装置に送信するシグナリング送受信部と、を備え、シグナリング制御部は、通信モジュールが起動された場合に、第１セキュリティプロトコルに基づく第１シグナリング用セッションを、通信制御装置との間に確立し、第１シグナリング用セッションが確立された場合に、第２セキュリティプロトコルに基づく第２シグナリング用セッションを、通信制御装置との間に確立し、シグナリング送受信部は、シグナリング制御部が生成したシグナリングメッセージを、第２シグナリング用セッションを介して通信制御装置に送信する。

【０００６】

また、本発明の第２の形態によれば、通信端末と通信相手端末とのセッションを管理する通信制御装置であって、シグナリングメッセージを生成するシグナリング制御部と、シグナリング制御部が生成したシグナリングメッセージを、通信端末に送信するシグナリング送受信部と、を備え、シグナリング制御部は、通信端末から要求があった場合に、第１セキュリティプロトコルに基づく第１シグナリング用セッションを、通信端末との間に確立し、第１シグナリング用セッションが確立された場合に、第２セキュリティプロトコルに基づく第２シグナリング用セッションを、通信端末との間に確立し、シグナリング送受信部は、シグナリング制御部が生成したシグナリングメッセージを、第２シグナリング用セッションを介して通信端末に送信する。

【０００７】

なお、上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではない。また、これらの特徴群のサブコンビネーションもまた、発明となりうる。

【発明を実施するための最良の形態】

【０００８】

以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は特許請求の範囲に係る発明を限定するものではない。また、また実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【０００９】

図１は、本発明の一実施形態に係る通信システムのネットワーク接続構成を示す。本実施形態に係る通信システムは、通信端末１０、通信端末１２、プロキシサーバ２０、ＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）サーバ２２、ロケーションサーバ２４、公開サーバ２６、基地局３０、アクセスポイント３１、アクセスポイント３２、セルラー網４０、コアネットワーク４２、インターネット４４、および無線ＬＡＮ網４６を備える。

【００１０】

本実施形態に係る通信端末１０は、セルラー網４０と無線ＬＡＮ網４６との双方を介して通信可能な通信端末１０のモビリティ性を確保することを目的とする。また、通信端末１０とＳＩＰサーバ２２との間で送受信されるシグナリングメッセージの秘匿性を確保するとともに、通信端末１０と通信端末１２との間で送受信される通信データの秘匿性を確保することを目的とする。

【００１１】

なお、ＳＩＰとは、複数の通信端末がネットワークを介して、音声、テキスト、および映像等の様々なメディアの送受信を実行すべく、複数の通信端末間における通信の開始および通信の切断等におけるシグナリングに用いられるプロトコルである。また、ここでの

シグナリングには、通信端末１０のＳＩＰサーバ２２への位置登録の他、ＳＩＰ Ｒｅｇｉｓｔｅｒ、ＳＩＰ Ｉｎｖｉｔｅ、ＳＩＰ Ｂｙｅ、２００ＯＫ等のすべてのシグナリングが含まれる。

【００１２】

ＳＩＰサーバ２２は、通信制御装置の一例である。通信制御装置は、通信端末１０のシグナリングを制御するシグナリング制御サーバであればよく、ＳＩＰサーバ２２に限られるものではない。また、基地局３０、無線アクセスポイント３１、および無線アクセスポイント３２は、通信端末１０と通信端末１２との通信を中継する通信中継装置の一例である。通信中継装置は、通信端末１０に実ＩＰアドレスを割り当てて通信端末１０の通信を中継するゲートウェイであればよく、基地局３０、無線アクセスポイント３１、および無線アクセスポイント３２に限られるものではない。

【００１３】

通信端末１０は、複数の異なる通信方式、例えば、３Ｇ方式、ＧＳＭ方式、またはＰＨＳ方式等の通信方式のそれぞれで通信する機能を有する。さらに、通信端末１０は、無線ＬＡＮを用いて通信する機能を有する。なお、通信端末１０は、例えば、電話通信機能および無線ＬＡＮ通信機能を有するノートパソコンである。また、通信端末１０は、無線ＬＡＮ機能を有する携帯電話端末、電話通信機能および無線ＬＡＮ通信機能を有するＰＤＡ、および電話通信機能および無線ＬＡＮ通信機能を有するデジタルカメラ等の携帯通信端末であってもよい。

【００１４】

通信端末１０が通信相手端末である通信端末１２と通信する場合、通信端末１０は、まず、通信端末１０が存在する位置において利用可能な通信方式を用いて、ＳＩＰサーバ２２に対してシグナリングする。例えば、通信端末１０がアクセスポイント３２を介して無線ＬＡＮ通信方式を利用できる場合、通信端末１０は、無線ＬＡＮ通信方式を用いて、ＳＩＰサーバ２２に対してシグナリングする。すなわち、通信端末１０は、アクセスポイント３２、無線ＬＡＮ網４６、およびコアネットワーク４２を介して、ＳＩＰサーバ２２に対してシグナリングする。一方、通信端末１０が電話通信機能を利用できる場合、通信端末１０は、電話通信の通信方式を用いてＳＩＰサーバ２２に対してシグナリングする。すなわち、通信端末１０は、基地局３０、セルラー網４０、およびコアネットワーク４２を介して、ＳＩＰサーバ２２に対してシグナリングする。

【００１５】

ＳＩＰサーバ２２は、通信端末１０がネットワーク上に存在する位置に関する情報である位置情報をロケーションサーバ２４に蓄積させる。ロケーションサーバ２４は、ＳＩＰサーバ２２に制御され、通信端末１０の位置情報を格納する。また、ＳＩＰサーバ２２は、通信端末１２がシグナリングした場合も、通信端末１２の位置情報をロケーションサーバ２４に蓄積させる。

【００１６】

通信端末１０は、基地局３０またはアクセスポイント３２を介して、ＳＩＰサーバ２２との間にシグナリング用のＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）セッションを確立する。続いて、通信端末１０は、ＴＬＳセッションを確立した後、ＴＬＳセッションを用いてＳＩＰサーバ２２との間でシグナリングメッセージをやりとりすることで、ＳＩＰサーバ２２との間にシグナリング用のＳＲＴＰ（Ｓｅｃｕｒｅ Ｒｅａｌ－Ｔｉｍｅ Ｐｒｏｔｏｃｏｌ）セッションを確立する。ここで、通信端末１０は、ＴＬＳセッションを確立したときに得られたＳＩＰサーバ２２との間の認証の結果を使って、ＳＲＴＰセッションを確立するときのＳＩＰサーバ２２との認証を得ることで、ＳＲＴＰセッションを確立する。他の例においては、通信端末１０は、ＴＬＳセッションを確立したときに得られたＳＩＰサーバ２２との間の認証の結果を使わず、ＳＲＩＰサーバ２２との間で改めて認証情報をやりとりして認証を得ることで、ＳＲＴＰセッションを確立してもよい。

【００１７】

その後、通信端末１０は、ＳＲＴＰプロトコルを用いてシグナリングメッセージを暗号化した上で、ＳＲＴＰセッションを介して、コネクションレス型のプロトコルであるＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）でＳＩＰサーバ２２へ送信する。これにより、通信端末１０とＳＩＰサーバ２２とのシグナリングは、ＳＲＴＰプロトコルによってセキュアに実現される。

【００１８】

通信端末１０は、利用している通信方式が無線ＬＡＮ通信方式である場合には、通信端末１２に送信すべき通信データを、アクセスポイント３２および無線ＬＡＮ網４６を介して送信する。また、通信端末１０は、利用している通信方式が電話通信機能である場合には、通信端末１２に送信すべき通信データを、基地局３０およびセルラー網４０を介して送信する。係る場合において、通信端末１０は、通信端末１２に送信すべき通信データを、ＳＲＴＰを用いて暗号化する。そして、通信端末１０は、ＳＲＴＰで暗号化した通信データを、ＵＤＰを用いて通信端末１２に送信する。

【００１９】

ここで、通信端末１０が現在存在している位置とは異なる位置に移動して、通信端末１０において利用可能な通信方式が変化した場合を考える。例えば、通信端末１０において利用可能な通信方式が、無線ＬＡＮ通信方式から電話通信方式に変化した場合、または利用可能な通信方式が、電話通信方式から無線ＬＡＮ通信方式に変化した場合を考える。係る場合において、通信端末１０が実ＩＰアドレスを用いて確立したＴＬＳセッションは、基地局３０またはアクセスポイント３２によって割り当てられた実ＩＰアドレスが変更された場合に切断される。そして、通信端末１０が新たに割り当てられた実ＩＰアドレスを用いて再度ＴＬＳセッションを確立する場合には、ＳＩＰサーバ２２と相互の認証を再度得なければならない。したがって、ＳＩＰサーバ２２とのシグナリングメッセージのやりとりに遅延が生じてしまい、モビリティ性を確保できない。

【００２０】

このような状況において、通信端末が再接続処理を実行する場合、通信端末は、インターネット等のネットワークにおいて暗号化通信する規格の１つであるＩＰｓｅｃを用いて、ＳＩＰサーバにシグナリングメッセージを送信することがある。ＩＰｓｅｃを用いる場合、通信端末は、通信端末とＩＰｓｅｃ Ｓｅｃｕｒｉｔｙ Ｇａｔｅｗａｙとの間でＩＰｓｅｃ Ｔｕｎｎｅｌを構築した後に、ＳＩＰサーバにシグナリングメッセージを送信する必要がある。したがって、通信端末とＳＩＰサーバとの間の接続が切断された場合、ＩＰｓｅｃ Ｔｕｎｎｅｌを初めから再構築しなければならず、迅速なハンドオーバに対応することが困難である。

【００２１】

また、ＳＩＰサーバに送信すべき通信データは、全てＩＰｓｅｃ Ｓｅｃｕｒｉｔｙ Ｇａｔｅｗａｙを介して送信しなければならず、ＩＰｓｅｃ Ｓｅｃｕｒｉｔｙ Ｇａｔｅｗａｙにトラフィックが集中して通信速度が低下して、通信端末のモビリティを確保することが困難な場合がある。例えば、通信端末が、インターネットまたはイントラネット等のＴＣＰ／ＩＰネットワークを用いて音声データを送受信する技術である、Ｖｏｉｃｅ ｏｖｅｒ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ（ＶｏＩＰ）を用いた通信をする場合、通信端末は、音声を示す音声データを複数のショートパケットに分割して送信する。例えば、パケットのデータサイズが２０から４０バイトのショートパケットに分割する。

【００２２】

係る場合において、通信端末は、通信相手端末に送信すべき通信データがＩＰｓｅｃ Ｔｕｎｎｅｌを通過することを可能とすべく、通信データに含まれる複数のショートパケットのそれぞれに対してヘッダを付加する処理を実行する。通信端末は、複数のショートパケットの全てに対して係る処理を実行するので、データ処理量が多大となる。したがって、ＩＰｓｅｃを用いた通信は、ＶｏＩＰ等のリアルタイム性を要求する通信に対して不向きである。

【００２３】

さらに、ＩＰｓｅｃは、サーバクライアント方式のセキュリティを実現する。よって、ＩＰｓｅｃ　Ｓｅｃｕｒｉｔｙ　Ｇａｔｅｗａｙの後段では、セキュリティが何ら提供されておらず、通信データの秘匿性を確保することができない。したがって、Ｅｎｄ－ｔｏ－Ｅｎｄ（Ｅ２Ｅ）のセキュリティの実現が困難である。

【００２４】

一方、本実施形態の通信端末１０は、ＴＬＳセッションを確立した後、すぐに、ＴＬＳセッションを用いてＳＲＴＰセッションを確立する。そして、通信端末１０は、ＳＲＴＰセッションを確立した後では、ＴＬＳセッションを用いることなくＳＲＴＰセッションを用いてシグナリングメッセージを送受信する。

【００２５】

さらに、通信端末１０が現在存在している位置とは異なる位置に移動して、通信端末１０において利用可能な通信方式が変化した場合には、新たな通信方式で利用するためのＳＲＴＰセッションを予め確立しておく。つまり、通信端末１０は、通信端末１０が移動する前の位置で利用していたＳＲＴＰセッションを介して、ＳＩＰサーバ２２との間でシグナリングメッセージを送受信することで、通信端末１０が移動した後の位置で利用するためのＳＲＴＰセッションを確立する。このように、通信端末１０は、ＳＲＴＰを用いてＳＩＰサーバ２２とシグナリングメッセージを送受信することによって、シームレスで迅速なハンドオーバに対応できる。

【００２６】

また、本実施形態の通信端末１０が用いるＳＲＴＰは、ＩＰｓｅｃとは異なり、通信端末間（Ｅ２Ｅ）のセキュリティを実現する。したがって、通信端末１０がＳＩＰサーバ２２に送信すべきシグナリングメッセージを、ＳＲＴＰで暗号化して送信することにより、Ｅ２Ｅの通信データの秘匿性を確保することができる。

【００２７】

通信端末１０が公開サーバ２６に対して通信データを送信する場合には、通信端末１０は、現在、当該通信端末１０が存在する位置において利用可能な通信方式を用いて、プロキシサーバ２０に対してセッション接続要求を送信する。例えば、通信端末１０がアクセスポイント３２を介して無線ＬＡＮ通信方式を利用できる場合、通信端末１０は、無線ＬＡＮ通信方式を用いてプロキシサーバ２０に対してセッション接続要求を送信する。すなわち、通信端末１０は、アクセスポイント３２、無線ＬＡＮ網４６、およびコアネットワーク４２を介してプロキシサーバ２０に対してセッション接続を要求する。一方、通信端末１０が電話通信機能を利用できる場合、通信端末１０は、電話通信の通信方式を用いてプロキシサーバ２０に対してセッション接続要求を送信する。すなわち、通信端末１０は、基地局３０、セルラー網４０、およびコアネットワーク４２を介してプロキシサーバ２０に対してセッション接続を要求する。

【００２８】

そして、通信端末１０とプロキシサーバ２０とのセッションが確立されることにより、通信端末１０は、公開サーバ２６に対して通信データを送信することが可能となる。通信端末１０は、基地局３０またはアクセスポイント３２、セルラー網４０または無線ＬＡＮ網４６、およびコアネットワーク４２を介して、公開サーバ２６に送信すべき通信データを、プロキシサーバ２０に送信する。通信端末１０は、通信データをＳＲＰＴで暗号化して、ＵＤＰを用いて送信する。当該通信データを受信したプロキシサーバ２０は、当該通信データを、公開サーバ２６が受信可能なデータ形式に変換する。そして、プロキシサーバ２０は、公開サーバ２６が受信可能なデータ形式に変換した通信データを、インターネット等のインターネット４４を介して公開サーバ２６に送信する。

【００２９】

本実施形態に係る通信端末１０によれば、音声データ通信のセキュリティプロトコルであるＳＲＴＰをシグナリングメッセージの送受信に適用できる。したがって、シグナリング用のセッションの確立に要する処理時間を短くすることができる。また、音声データ通信と同様にシグナリングに対しても、通信端末１０のモビリティ性を確保することができ

る。

【００３０】

図２は、本実施形態に係る通信セキュリティの概要を示す。通信端末１０は、起動するとまず、ＳＩＰサーバ２２との間に、ＴＬＳセッションを確立する。続いて、通信端末１０は、確立したＴＬＳセッションを介してシグナリングメッセージを送受信することにより、ＳＩＰサーバ２２との間に、ＳＲＴＰセッションを確立する。その後、通信端末１０は、確立されたＳＲＴＰセッションを介してシグナリングを送受信する。したがって、通信端末１０は、継続的かつ迅速にＳＲＴＰセッションでシグナリングメッセージをＳＩＰサーバ２２とやりとりすることができる。さらに、通信端末１０は、セルラー網４０および無線ＬＡＮ網４６のようなオープンネットワークにおけるシグナリングメッセージのセキュリティを確保できる。

【００３１】

また、通信端末１０は、通信端末１２およびプロキシサーバ２０との間で、通信データをＳＲＴＰで暗号化して送受信する。通信端末１０は、通信端末１２およびプロキシサーバ２０に送信すべき通信データを、ＴＬＳセッションが確立された場合にＳＩＰサーバ２２によって割り当てられた仮想ＩＰアドレスを送信元アドレスとする通信データから実ＩＰアドレスを送信元アドレスとする通信データにカプセル化する。

【００３２】

そして、通信端末１０は、カプセル化された通信データを、ＳＲＴＰで暗号化してＵＤＰで通信端末１２およびプロキシサーバ２０へ送信する。したがって、通信端末１０は、ＳＲＴＰによる通信を常に実現することができ、セルラー網４０、無線ＬＡＮ網４６、およびインターネット４４のようなオープンネットワークにおける通信データのセキュリティを確保できる。

【００３３】

例えば、通信端末１０は、通信データの暗号化方式の１つであるＡｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（ＡＥＳ）で通信データを暗号化でき、また、高速に暗号鍵の交換ができる。また、通信端末１０は、暗号鍵の交換に、例えば、鍵交換プロトコルの１つであるＭｕｌｔｉｍｅｄｉａ Ｉｎｔｅｒｎｅｔ ＫＥＹｉｎｇ（ＭＩＫＥＹ）を用いてもよい。通信端末１０は、ＭＩＫＥＹを用いることにより、１Ｒｏｕｎｄ－Ｔｒｉｐで鍵の交換を実行できる。

【００３４】

図３は、本実施形態に係る通信端末１０の通信モジュール１４の機能構成の一例を示す。通信モジュール１４は、一般アプリケーション部１００、リアルタイムアプリケーション部１０５、仮想インターフェース部１１０、通信ユニット１２０、通信制御ユニット１３０、およびセッションモビリティ制御ユニット１６０を備える。なお、プロキシサーバ２０およびＳＩＰサーバ２２は、通信モジュール１４の機能および構成の一部、または全部を備えていてよい。

【００３５】

通信ユニット１２０は、第１通信部１２２、第２通信部１２４、および第ｎ通信部１２６を含む複数の通信部を有する。また、通信制御ユニット１３０は、通信ＩＦ選択部１４０およびアドレス取得部１５０を有する。また、セッションモビリティ制御ユニット１６０は、データ形式変換部１６００、シグナリング制御部１６０５、（デ）カプセル化部１６１０、第２暗号化部１６２０、シグナリング送受信部１６２５、変換テーブル記憶部１６４０、およびデータ送受信部１６４５を有する。

【００３６】

通信ユニット１２０は、通信モジュール１４が通信可能な複数の通信方式ごとに異なる複数の通信部を有する。例えば、通信ユニット１２０は、第１の通信方式（例えば、無線ＬＡＮ通信方式）で通信する第１通信部１２２、第２の通信方式（例えば、電話通信方式）で通信する第２通信部１２４、および第ｎの通信方式（例えば、無線ＬＡＮおよび電話通信方式を除く他の通信方式）で通信する第ｎ通信部１２６を有する。なお、通信ユニッ

ト１２０は、複数の通信方式で通信可能な通信部を有していてもよい。例えば、通信ユニット１２０は、第１の通信方式と第２の通信方式とのいずれかで通信可能な通信部、すなわち、上述した第１通信部および第２通信部の機能を併せ持った通信部を有していてもよい。これにより、通信モジュール１４の構成の簡略化、および小型化に資することができる。

【００３７】

また、複数の通信部のそれぞれは、セルラー網４０、無線ＬＡＮ網４６等の複数の通信網のそれぞれに対応する複数の通信中継装置のそれぞれを介して、シグナリング送受信部１６２５が生成したシグナリングメッセージを、ＳＩＰサーバ２２との間で送信する。また、通信ユニット１２０が有する複数の通信部のそれぞれは、一般アプリケーション部１００またはリアルタイムアプリケーション部１０５が生成した通信データを、通信端末１２またはプロキシサーバ２０との間で送信する。

【００３８】

また、複数の通信部のそれぞれは、ＳＩＰサーバ２２から受信したシグナリングメッセージを、通信制御ユニット１３０を介してシグナリング制御部１６０５に供給する。また、複数の通信部のそれぞれは、通信端末１２またはプロキシサーバ２０から受信した通信データを、通信制御ユニット１３０を介して一般アプリケーション部１００またはリアルタイムアプリケーション部１０５に供給する。

【００３９】

通信ユニット１２０が有する複数の通信部のそれぞれは、それぞれに割り当てられた通信方式で通信することができるか否かを通信ＩＦ選択部１４０が判断するために用いられる情報を、通信制御ユニット１３０に供給する。さらに、複数の通信部は、それぞれが通信可能な通信中継装置から動的な実ＩＰアドレスを割り当てられた場合、割り当てられた実アドレスを通信制御ユニット１３０に供給する。

【００４０】

通信ＩＦ選択部１４０は、複数の通信部から供給された情報に基づいて、複数の通信部のうち通信可能な通信部を選択する。例えば、通信ＩＦ選択部１４０は、通信中継装置が発する通信方式を識別する情報を含む電波の電波強度を示す情報を、複数の通信部から受け取り、電荷強度の大きさに基づいて通信可能な通信部を判断する。他の例において、通信ＩＦ選択部１４０は、複数の通信部に対して予め設定された利用優先順位等のポリシーに基づいて、複数の通信部から１つの通信部を選択してもよい。そして、通信ＩＦ選択部１４０は、選択した通信部を識別する情報を変換テーブル記憶部１６４０に供給する。

【００４１】

アドレス取得部１５０は、通信中継装置によって通信端末１０に対して動的に割り当てられる実アドレスを取得する。すなわち、アドレス取得部１５０は、通信ＩＦ選択部１４０が選択した通信部に割り当てられた実アドレスを取得する。実アドレスは、例えば、通信中継装置が管理しているプライベートＩＰアドレスまたはグローバルＩＰアドレスであり、以下において、実ＩＰアドレスと称する。そして、アドレス取得部１５０は、取得した実ＩＰアドレスを変換テーブル記憶部１６４０に供給する。

【００４２】

変換テーブル記憶部１６４０は、通信ＩＦ選択部１４０が選択した通信部を識別する情報、およびアドレス取得部１５０が取得した実ＩＰアドレスを記憶する。そして、変換テーブル記憶部１６４０は、記憶している実ＩＰアドレスをデータ形式変換部１６００および（デ）カプセル化部１６１０に通知する。

【００４３】

一般アプリケーション部１００は、所定の目的の処理を実行する。具体的には、一般アプリケーション部１００は、データ処理を実行するアプリケーションプログラムに所定の目的のデータ処理を実行させる。アプリケーションプログラムは、例えば、Ｗｅｂブラウザプログラム、電子メール送受信プログラム、およびマルチメディアデータの送受信プログラム等であってよい。一般アプリケーション部１００は、アプリケーションプログラム

が処理したデータであって、通信端末１２またはプロキシサーバ２０に送信すべき通信データを、仮想インターフェース部１１０に供給する。

【００４４】

係る場合において、一般アプリケーション部１００は、仮想インターフェース部１１０を一意に識別する識別番号を通信データに付加して仮想インターフェース部１１０に供給する。識別番号は、例えば、仮想インターフェース部１１０に割り当てられた仮想アドレスである。仮想アドレスは、シグナリング制御部１６０５の起動段階においてＳＩＰサーバ２２によって動的または静的に割り当てられる。仮想アドレスは、例えば、ＩＰアドレスの構成を有しており、以下において、仮想ＩＰアドレスと称する。なお、仮想ＩＰアドレスは、一般アプリケーション部１００に対して固定的に設定されてよい。

【００４５】

リアルタイムアプリケーション部１０５は、所定の目的の処理を実行する。具体的には、リアルタイムアプリケーション部１０５は、データ処理を実行するＳＩＰアプリケーションプログラムに所定の目的のデータ処理を実行させる。例えば、ＳＩＰアプリケーションプログラムは、リアルタイムのマルチメディア通信を提供するＩＰ電話等のアプリケーションプログラムであってよい。

【００４６】

仮想インターフェース部１１０は、仮想ＩＰアドレスが割り当てられており、通信端末１２またはプロキシサーバ２０に送信する通信データを一般アプリケーション部１００から受け取る。仮想インターフェース部１１０は、受け取った通信データをデータ形式変換部１６００に供給する。

【００４７】

シグナリング制御部１６０５は、シグナリングメッセージを生成して、通信端末１０のシグナリングを制御する。シグナリング制御部１６０５は、例えばＳＩＰによるシグナリングを制御する。具体的には、シグナリング制御部１６０５は、アドレス取得部１５０が取得した実ＩＰアドレスを用いて、ＳＩＰサーバ２２とのセッションを確立する。より具体的には、シグナリング制御部１６０５は、第１セキュリティプロトコルに基づく第１シグナリング用セッションをＳＩＰサーバ２２との間に確立する。そして、第１シグナリング用セッションを確立した後、第２セキュリティプロトコルに基づく第２シグナリング用セッションをＳＩＰサーバ２２との間に確立する。

【００４８】

シグナリング制御部１６０５は、まず、第１暗号化部１６１５を介してシグナリングメッセージをシグナリング送受信部１６２５に供給する。これにより、シグナリング制御部１６０５は、第１セキュリティプロトコルに基づく第１シグナリング用セッションを、ＳＩＰサーバ２２との間に確立する。このとき、シグナリング制御部１６０５は、第１セキュリティプロトコルを用いて、通信端末１０とＳＩＰサーバ２２との間の相互の認証を得ることによって、第１シグナリング用セッションを確立する。

【００４９】

シグナリング制御部１６０５は、第１シグナリング用セッションが確立すると、第１暗号化部１６１５を介してシグナリングメッセージをシグナリング送受信部１６２５に供給して、第１シグナリング用セッションを介してＳＩＰサーバ２２とやりとりする。これにより、シグナリング制御部１６０５は、第２セキュリティプロトコルに基づく第２シグナリング用セッションを、ＳＩＰサーバ２２との間に確立する。このとき、シグナリング制御部１６０５は、第１シグナリング用セッションを確立する場合に第１セキュリティプロトコルを用いて得られた認証の結果を使って、第２シグナリング用セッションを確立する。

【００５０】

シグナリング制御部１６０５は、第２シグナリング用セッションが確立された後は、データ形式変換部１６００および第２暗号化部１６２０を介して、シグナリングメッセージをシグナリング送受信部１６２５に供給して、第２シグナリング用セッションを介してＳ

ＩＰサーバ２２とやりとりする。なお、シグナリング制御部１６０５は、通信端末１０への電源投入、通信モジュール１４の起動または再起動、通信端末１０のＨＯ、通話中のコーデック変更、定期的なＳＩＰ登録更新等の様々な動作を契機として、シグナリングメッセージを生成して位置登録等のシグナリングを処理する。

【００５１】

第１暗号化部１６１５は、シグナリング制御部１６０５がＳＩＰサーバ２２に対してシグナリングすべく生成したシグナリングメッセージを、通信のセキュリティを確保する第１セキュリティプロトコルを用いて暗号化する。具体的には、第１暗号化部１６１５は、コネクション型の通信プロトコルとともに利用可能な第１セキュリティプロトコルを用いて暗号化する。より具体的には、第１暗号化部１６１５は、ＯＳＩ参照モデルにおけるトランスポート層（レイヤー４）で用いられるコネクション型の通信プロトコルとともに利用可能な第１セキュリティプロトコルを用いて暗号化する。第１セキュリティプロトコルは、公開鍵暗号または秘密鍵暗号、デジタル証明書、およびハッシュ関数等のセキュリティ技術の少なくとも１つを用いて通信データの盗聴および改ざん等を防止するプロトコルであってよい。例えば、第１暗号化部１６１５は、シグナリングメッセージを、第１セキュリティプロトコルとしてＴＬＳプロトコルを用いて暗号化する。

【００５２】

また、第１暗号化部１６１５は、ＳＩＰサーバ２２から送信されたシグナリングメッセージを復号化してシグナリング制御部１６０５に供給する。この場合、第１暗号化部１６１５は、シグナリングメッセージを直接シグナリング送受信部１６２５から受け取る。

【００５３】

データ形式変換部１６００は、シグナリング制御部１６０５が生成したシグナリングメッセージを、第２セキュリティプロトコルに基づいて暗号化できるデータ形式に変換する。具体的には、データ形式変換部１６００は、ＲＴＰ（Ｒｅａｌ－Ｔｉｍｅ　Ｐｒｏｔｏｃｏｌ）ヘッダを付加することによって、シグナリング制御部１６０５が生成したシグナリングメッセージを、ＳＲＴＰに基づいて暗号化できるＲＴＰのデータ形式に変換する。そして、データ形式変換部１６００は、データ形式を変換したシグナリングメッセージを、第２暗号化部１６２０に供給する。

【００５４】

また、データ形式変換部１６００は、通信端末１２またはプロキシサーバ２０に送信する通信データを、ＳＲＴＰを用いて暗号化できるデータ形式に変換する。データ形式変換部１６００は、通信データのデータ構成およびヘッダの形式を変換することにより、ＳＲＴＰを用いて暗号化できるデータ形式に変換する。例えば、データ形式変換部１６００は、仮想インターフェース部１１０から受け取ったＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）で送信可能な通信データを、ＵＤＰで送信可能な通信データに変換すべく、予め定められた付加情報を仮想インターフェース部１１０から受け取った通信データに付加する。但し、データ形式変換部１６００は、通信データがＲＴＰのパケットである場合には、データ形式の変換を実行せず、通信データがＲＴＰ以外のパケットである場合には、ＲＴＰヘッダを付加することにより、ＲＴＰのパケットへのデータ形式の変換を実行する。そして、データ形式変換部１６００は、データ形式を変換した後の通信データを（デ）カプセル化部１６１０に供給する。

【００５５】

また、データ形式変換部１６００は、通信端末１２またはプロキシサーバ２０から送信された通信データのデータ形式を逆変換する。例えば、データ形式変換部１６００は、仮想インターフェース部１１０から受け取ったＵＤＰによる通信データを、ＴＣＰによる通信データに変換する。そして、データ形式変換部１６００は、データ形式を逆変換した後の通信データを仮想インターフェース部１１０に供給する。

【００５６】

（デ）カプセル化部１６１０は、データ形式変換部１６００から受け取った通信データに、予め定められた付加情報を付加することによりカプセル化する。具体的には、（デ）

カプセル化部１６１０は、仮想インターフェース部１１０から供給される、仮想ＩＰアドレスが送信元アドレスとして付加された通信データに、アドレス取得部１５０が取得して変換テーブル記憶部１６４０に記憶されている実ＩＰアドレスを送信元アドレスとして付加してカプセル化する。そして、（デ）カプセル化部１６１０は、カプセル化した通信データを、データ送受信部１６４５に供給する。

【００５７】

また、（デ）カプセル化部１６１０は、通信端末１２またはプロキシサーバ２０から送信された、カプセル化された通信データを受け取る。そして、（デ）カプセル化部１６１０は、受け取った通信データをデカプセル化してデータ形式変換部１６００に供給する。

【００５８】

第２暗号化部１６２０は、データ形式変換部１６００によってデータ形式が変換されたシグナリングメッセージまたは通信データを、第１セキュリティプロトコルとは異なる第２セキュリティプロトコルに基づいて暗号化する。具体的には、第２暗号化部１６２０は、コネクションレス型の通信プロトコルとともに利用可能な第２セキュリティプロトコルを用いて暗号化する。より具体的には、第２暗号化部１６２０は、ＯＳＩ参照モデルにおけるトランスポート層（レイヤー４）で用いられるコネクションレス型の通信プロトコルとともに利用可能な第２セキュリティプロトコルを用いて暗号化する。例えば、第２暗号化部１６２０は、シグナリングメッセージまたは通信データを、第２セキュリティプロトコルとしてＳＲＴＰを用いて暗号化する。

【００５９】

そして、第２暗号化部１６２０は、暗号化したシグナリングメッセージを、シグナリング送受信部１６２５に供給する。第２暗号化部１６２０は、暗号化した通信データを、データ送受信部１６４５に供給する。また、第２暗号化部１６２０は、ＳＩＰサーバ２２から送信されたシグナリングメッセージを復号化して（デ）カプセル化部１６１０に供給する。第２暗号化部１６２０は、通信端末１２またはプロキシサーバ２０から送信された通信データを復号化して（デ）カプセル化部１６１０に供給する。

【００６０】

シグナリング送受信部１６２５は、第１シグナリング用セッションを確立する場合、シグナリング制御部１６０５が生成して第１暗号化部１６１５が暗号化したシグナリングメッセージを、ＳＩＰサーバ２２に送信する。また、シグナリング送受信部１６２５は、第２シグナリング用セッションを確立する場合、シグナリング制御部１６０５が生成して第１暗号化部１６１５が暗号化したシグナリングメッセージを、第１シグナリング用セッションを介してＳＩＰサーバ２２に送信する。このとき、シグナリング送受信部１６２５は、コネクション型の通信プロトコルを用いてシグナリングメッセージを送信する。具体的には、シグナリング送受信部１６２５は、第１暗号化部１６１５から供給されたシグナリングメッセージを、通信ＩＦ選択部１４０が選択した通信部に通信制御ユニット１３０を介して供給してＴＣＰを用いて送信させる。

【００６１】

シグナリング送受信部１６２５は、第２シグナリング用セッションが確立された後、第２暗号化部１６２０が暗号化したシグナリングメッセージを、第２シグナリング用セッションを介してＳＩＰサーバ２２に送信する。このとき、シグナリング送受信部１６２５は、コネクションレス型の通信プロトコルを用いてシグナリングメッセージを送信する。具体的には、シグナリング送受信部１６２５は、第２暗号化部１６２０から供給されたシグナリングメッセージを、通信ＩＦ選択部１４０が選択した通信部に通信制御ユニット１３０を介して供給してＵＤＰを用いて送信させる。

【００６２】

通信端末１０が、第１通信部１２２が通信可能な第１エリアから第２通信部１２４が通信可能な第２エリアに移動する場合に、シグナリング送受信部１６２５は、第２エリアにおいて第２通信方式で確立される第３シグナリング用セッションであるＳＲＴＰセッションを確立するためのシグナリングメッセージを、第１エリアにおいて第１通信方式で確立

された第２シグナリング用セッションを介して、第１通信方式の通信中継装置経由でＳＩＰサーバ２２に送信する。つまり、第２通信部１２４に通信中継装置から実ＩＰアドレスが割り当てられると、通信ＩＦ選択部１４０が第２通信部１２４を選択する以前に、第２通信方式によるＳＲＴＰセッションを予め確立する。これにより、通信ＩＦ選択部１４０によって、第１通信部１２２から第２通信部１２４に切り換えられた場合に、即座に第２通信方式によるシグナリングが可能となり、シグナリングに遅延を生じさせることがない。

【００６３】

同様に、通信端末１０が、第１通信部１２２が通信可能な第１エリアから第２通信部１２４が通信可能な第２エリアに移動する場合に、シグナリング送受信部１６２５は、第２エリアにおいて第２通信方式で確立される第２通信データ用セッションを確立するためのシグナリングメッセージを、第１エリアにおいて第１通信方式で確立された第２シグナリング用セッションを介して、第１通信方式の通信中継装置経由でＳＩＰサーバ２２に送信する。つまり、第２通信部１２４に通信中継装置から実ＩＰアドレスが割り当てられると、通信ＩＦ選択部１４０が第２通信部１２４を選択する以前に、第２通信方式によるＳＲＴＰセッションを予め確立する。これにより、通信ＩＦ選択部１４０によって、第１通信部１２２から第２通信部１２４に切り換えられた場合に、即座に第２通信方式によるデータ通信が可能となり、データ通信に遅延を生じさせることがない。

【００６４】

また、シグナリング送受信部１６２５は、ＳＩＰサーバ２２から送信されたシグナリングメッセージをシグナリング制御部１６０５に供給する。この場合も、シグナリング送受信部１６２５は、第１シグナリング用セッションおよび第２シグナリング用セッションを確立する場合、シグナリングメッセージを第１暗号化部１６１５に供給する。一方で、シグナリング送受信部１６２５は、第２シグナリング用セッションが確立された後において、シグナリングメッセージを、第２暗号化部１６２０およびデータ形式変換部１６００を介してシグナリング制御部１６０５に供給する。

【００６５】

また、シグナリング送受信部１６２５は、一般アプリケーション部１００およびリアルタイムアプリケーション部１０５が生成した通信データを通信端末１０に送信するために用いる通信データ用セッションを確立するためのシグナリングメッセージを、第２シグナリング用セッションを介してＳＩＰサーバ２２に送信する。

【００６６】

データ送受信部１６４５は、通信端末１２またはプロキシサーバ２０に送信すべき通信データを、通信ＩＦ選択部１４０が選択した通信部に通信制御ユニット１３０を介して供給して通信端末１２またはプロキシサーバ２０に送信する。具体的には、データ送受信部１６４５は、第２暗号化部１６２０が暗号化した通信データを、コネクションレス型の通信プロトコルを用いて送信する。例えば、データ送受信部１６４５は、第２暗号化部１６２０がＳＰＴＰによって暗号化した通信データを、ＵＤＰを用いて送信する。また、データ送受信部１６４５は、通信端末１２またはプロキシサーバ２０から受信するデータを、通信ＩＦ選択部１４０が選択した通信部から通信制御ユニット１３０を介して受け取り、送信する。第２暗号化部１６２０に供給する。

【００６７】

本実施形態に係る通信端末１０によれば、ＳＩＰサーバ２２とのシグナリングを実行する場合に、ＳＩＰサーバ２２に送信するシグナリングメッセージのセキュリティを、ＳＲＴＰを用いて確保できる。また、通信端末がデータ通信を実行する場合に、通信端末１２またはプロキシサーバ２０に送信する通信データのセキュリティを、ＳＲＴＰを用いて確保できる。これにより、通信端末１０は、通信端末１２、プロキシサーバ２０、およびＳＩＰサーバ２２との通信接続が途切れることなく通信を継続することができるだけでなく、シグナリングメッセージおよび通信データのセキュリティを確実に確保できる。

【００６８】

図４は、本実施形態に係る通信端末１０のモジュール構成の一例を示す。なお、一般クライアントアプリケーションモジュール２００は、例えば、Ｗｅｂブラウザ等のアプリケーションであり、図３の上記説明における一般アプリケーション部１００の一例である。Ｍｏｂｉｌｅ　ＳＩＰ　ＡＰｓモジュール２０５は、図３の上記説明におけるリアルタイムアプリケーション部１０５の一例であり、例えば、ＶｏＩＰアプリケーションである。また、Ｖｉｒｔｕａｌ　ＩＦモジュール２１０は、図３の上記説明における仮想インターフェース部１１０の一例である。また、複数の通信ＩＦモジュールを有する通信インターフェースユニット２２０および複数のＮＩＣは、図３の上記説明における通信ユニット１２０の一例である。

【００６９】

シグナリング制御モジュール２６０５は、図３の上記説明におけるシグナリング制御部１６０５の一例である。また、ＩＡＣモジュール２６１０は、図３の上記説明における通信ＩＦ選択部１４０およびアドレス取得部１５０の一例である。また、（デ）カプセル化モジュール２６００は、図３の上記説明における（デ）カプセル化部１６１０の一例である。また、ＲＴＰモジュール２６１５およびＲＴＰモジュール２６２０は、図３の上記説明におけるデータ形式変換部１６００の一例であり、ＲＴＰモジュール２６１５とＲＴＰモジュール２６２０とは、物理的に１つのモジュールであってもよい。

【００７０】

ＴＬＳモジュール２５８は、図３の上記説明における第１暗号化部１６１５の一例である。また、ＳＲＴＰモジュール２５６は、図３の上記説明における第２暗号化部１６２０の一例である。また、ＵＤＰモジュール２４０は、図３の上記説明におけるシグナリング送受信部１６２５およびデータ送受信部１６４５の一例である。また、ＴＣＰモジュール２４２は、図３の上記説明におけるシグナリング送受信部１６２５の一例である。

【００７１】

複数のネットワークインターフェースカード（ＮＩＣ）は、それぞれに対応する通信方式を用いて通信端末１２、プロキシサーバ２０、およびＳＩＰサーバ２２と通信する。複数のＮＩＣはそれぞれに対応する通信ＩＦモジュールに制御されて、通信データを送受信する。複数の通信ＩＦモジュールは、それぞれに対応するＮＩＣを介して通信データを送受信する。

【００７２】

例えば、通信ＩＦモジュールａ２２２はＮＩＣａ２３２を介して通信データを送受信する。同様にして、通信ＩＦモジュールｂ２２４はＮＩＣｂ２３４を介して、そして、通信ＩＦモジュールｎ２２６はＮＩＣｎ２３６を介して通信データを送受信する。具体的には、ＮＩＣａ２３２は、無線ＬＡＮインターフェースカードであってよく、ＮＩＣｂ２３４は、携帯電話通信方式のインターフェースカードであってよい。そして、ＮＩＣｎ２３６は、無線ＬＡＮ通信方式および携帯電話通信方式を除く、他の通信方式のインターフェースカードであってよい。

【００７３】

ＩＡＣモジュール２６１０は、通信インターフェースユニット２２０が有する複数の通信ＩＦモジュール（例えば、通信ＩＦモジュールａ２２２、通信ＩＦモジュールｂ２２４、および通信ＩＦモジュールｎ２２６等）のうち、いずれが利用可能かを判断して選択する。すなわち、ＩＡＣモジュール２６１０は、通信中継装置と通信可能な通信ＩＦモジュールがいずれであるかを判断して、通信可能な通信ＩＦモジュールを選択する。ＩＡＣモジュール２６１０が、通信可能な通信ＩＦモジュールがいずれであるかを判断する方法は、図３の上記説明における通信ＩＦ選択部１４０と略同様であるので詳細な説明は省略する。

【００７４】

ＩＡＣモジュール２６１０は、通信可能な通信ＩＦモジュールを介して、通信中継装置が通信端末１０に対して動的に割り当てたＩＰアドレスを取得する。そして、ＩＡＣモジュール２６１０は、通信可能な通信ＩＦモジュールを識別する情報と取得したＩＰアドレ

スとをシグナリング制御モジュール２６０５、（デ）カプセル化モジュール２６００、ＲＴＰモジュール２６１５、ＲＴＰモジュール２６２０、およびＭｏｂｉｌｅ ＳＩＰ ＡＰｓモジュール２０５に通知する。

【００７５】

まず、シグナリング制御モジュール２６０５は、例えば通信端末１０の起動時に、ＴＬＳを用いてＳＩＰサーバ２２に対してシグナリングする。すなわち、シグナリング制御モジュール２６０５は、シグナリング処理を実行するシグナリングメッセージをＴＬＳモジュール２５８においてＴＬＳを用いて暗号化させる。そして、シグナリング制御モジュール２６０５は、暗号化されたシグナリングメッセージをＴＣＰモジュール２４２においてＴＣＰで送信可能な形式にして、ＳＩＰサーバ２２に送信させる。具体的には、シグナリング制御モジュール２６０５は、通信インターフェースユニット２２０が有する複数の通信ＩＦモジュールのうち、通信中継装置と通信可能な通信ＩＦモジュールを介して、ＴＬＳで暗号化されたシグナリングメッセージをＳＩＰサーバ２２に送信する。

【００７６】

例えば、シグナリング制御モジュール２６０５は、通信端末１０が起動されたことを契機として、ＳＩＰサーバ２２との間に第１シグナリング用セッションであるＴＬＳセッションを確立する。その後、シグナリング制御モジュール２６０５は、ＳＩＰサーバ２２に、シグナリングメッセージとしてＲＥＧＩＳＴＥＲリクエストメッセージを送信する。ＲＥＧＩＳＴＥＲリクエストメッセージは、シグナリング処理をするＳＩＰサーバ２２のＳＩＰ ＵＲＩ、登録を要求する通信端末１０のＳＩＰ ＵＲＩ、および登録の有効期限を示す情報等を含む。そして、ＲＥＧＩＳＴＥＲリクエストメッセージを受信したＳＩＰサーバ２２は、通信端末１０のシグナリング処理を実行する。ＳＩＰサーバ２２は、シグナリング処理が完了した場合、シグナリングが完了したことを、例えば、２００ＯＫメッセージを返信することで通信端末１０のシグナリング制御モジュール２６０５に通知する。

【００７７】

次に、シグナリング制御モジュール２６０５は、第２シグナリング用セッションであるＳＲＴＰセッションを確立するためのシグナリングメッセージを、ＴＬＳセッションを介してＳＩＰサーバ２２に送信する。このとき、シグナリング制御モジュール２６０５は、ＴＬＳセッションを確立する場合にＳＩＰサーバ２２との間で認証された認証結果をＳＩＰサーバ２２との間でやりとりすることで、再度ＳＩＰサーバ２２との間で認証処理を実行することなく、ＳＲＴＰセッションを確立する。

【００７８】

次に、通信中継装置との通信が可能な通信ＩＦモジュールが変更した場合、すなわち、通信端末１０が移動することによってハンドオーバ制御を要する場合について説明する。係る場合に、シグナリング制御モジュール２６０５は、通信端末１０から見て通信端末１２およびＳＩＰサーバ２２との通信が切断されていないように見せるべく、通信端末１０のシグナリングを以下に示すべく実行する。

【００７９】

ＩＡＣモジュール２６１０は、新たに通信可能となった通信ＩＦモジュールが検出された場合に、通信中継装置が通信ＩＦモジュールに割り当てたＩＰアドレスを取得する。そして、ＩＡＣモジュール２６１０は、通信可能な通信ＩＦモジュールを識別する情報と取得したＩＰアドレスとをシグナリング制御モジュール２６０５に通知する。

【００８０】

シグナリング制御モジュール２６０５は、新たに通信可能となった通信ＩＦモジュールを識別する情報が通知されると、通信端末１０とＳＩＰサーバ２２との間に第３シグナリング用セッションであるＳＲＴＰセッションを確立すべく、シグナリングメッセージを生成する。シグナリング制御モジュール２６０５は、シグナリングメッセージをＲＴＰモジュール２６１５に供給してＲＴＰのデータ形式に変換させ、ＳＲＴＰモジュール２５６にＳＲＴＰを用いて暗号化させる。そして、シグナリング制御モジュール２６０５は、既に確立されているＳＲＴＰセッションを介して、シグナリングメッセージをＳＩＰサーバ２

２に送信することによって、新たなＳＲＴＰセッションをＳＩＰサーバ２２との間に確立する。

【００８１】

以上のように、通信端末１０は、現在選択されている通信ＩＦモジュールを介して確立されているシグナリング用のＳＲＴＰセッションを用いて、次に選択される通信ＩＦモジュールからのシグナリング用のＳＲＴＰセッションを確立する。これにより、通信端末１０がネットワーク間をハンドオーバする前に、移動先のネットワークで利用できるＳＲＴＰセッションを予め用意することができるので、モビリティ性を確保することができる。

【００８２】

次に、一般クライアントアプリケーションモジュール２００が通信端末１２と所定の通信データの送受信を実行する場合を説明する。一般クライアントアプリケーションモジュール２００は、通信端末１２に送信すべき通信データを、ＴＣＰ／ＵＤＰモジュール２５４においてＴＣＰで送信可能な形式にして、Ｖｉｒｔｕａｌ　ＩＦモジュールに供給する。

【００８３】

係る場合において、一般クライアントアプリケーションモジュール２００は、ＴＬＳセッションの確立時にＶｉｒｔｕａｌ　ＩＦモジュール２１０に割り当てられた仮想ＩＰアドレスを通信データに付加する。そして、一般クライアントアプリケーションモジュール２００は、仮想ＩＰアドレスを付加した通信アドレスをＶｉｒｔｕｌａ　ＩＦモジュール２１０に供給する。これにより、一般クライアントアプリケーションモジュール２００にとっては、常に同一の通信相手と通信していると擬制できる。

【００８４】

Ｖｉｒｔｕａｌ　ＩＦモジュール２１０は、一般クライアントアプリケーションモジュール２００から受け取った通信データを、（デ）カプセル化モジュール２６００に供給する。（デ）カプセル化モジュール２６００は、Ｖｉｒｔｕａｌ　ＩＦモジュール２１０から受け取った通信データをカプセル化する。具体的には、（デ）カプセル化モジュール２６００は、ＩＡＣモジュール２６１０から通知された実ＩＰアドレスを通信データに付加して、ＲＴＰモジュール２６２０に供給する。

【００８５】

ＲＴＰモジュール２６２０は、（デ）カプセル化モジュール２６００がカプセル化した通信データを、ＳＲＴＰを用いて暗号化できるデータ形式に変換する。そして、ＳＲＴＰモジュール２５６は、ＲＴＰモジュール２６２０がデータ形式を変換した通信データを、ＳＲＴＰを用いて暗号化する。ＳＲＴＰモジュール２５６は、ＳＲＴＰを用いて暗号化した通信データを、ＵＤＰモジュール２４０から通信ＩＦモジュールを介して通信端末１２に送信する。

【００８６】

一方、通信端末１２が通信端末１０にあてて送信した通信データは、ＮＩＣ、当該ＮＩＣに対応する通信ＩＦモジュールを介して受信する。なお、通信端末１２が送信した通信データは、ＴＣＰで通信可能な通信データをＵＤＰで通信可能な形式にカプセル化した上で、ＳＲＴＰで暗号化されている。ＵＤＰモジュール２４０は、受信した通信データをＳＲＴＰモジュール２５６に供給する。ＳＲＴＰモジュール２５６は、ＳＲＴＰで暗号化された通信データを復号化する。そして、ＲＴＰモジュール２６２０は、復号かされた通信データの形式を逆変換して（デ）カプセル化モジュール２６００に供給する。

【００８７】

（デ）カプセル化モジュール２６００は、ＳＲＴＰモジュール２５６が復号化した通信データを、デカプセル化する。すなわち、（デ）カプセル化モジュール２６００は、ＵＤＰで送信可能な形式にカプセル化された通信データをデカプセル化する。（デ）カプセル化モジュール２６００は、デカプセル化した通信データをＶｉｒｔｕａｌ　ＩＦモジュール２１０に供給する。

【００８８】

Ｖｉｒｔｕａｌ　ＩＦモジュール２１０は、ＴＣＰ／ＵＤＰモジュール２５４を介して受け取った通信データを一般クライアントアプリケーションモジュール２００に供給する。一般クライアントアプリケーションモジュール２００は、Ｖｉｒｔｕａｌ　ＩＦモジュール２１０から受け取った通信データを、所定のアプリケーションに渡すことにより処理する。

【００８９】

これにより、一般クライアントアプリケーションモジュール２００から見ると、一般クライアントアプリケーションモジュール２００が通信する通信相手は常にＶｉｒｔｕａｌ　ＩＦモジュール２１０である。したがって、一般クライアントアプリケーションモジュール２００がＴＣＰで通信可能な通信データをＵＤＰで通信可能な通信データに変換すること、および通信端末１２と送受信する通信データを暗号化／復号化することがなくなる。すなわち、本実施形態に係る通信端末１０によれば、一般クライアントアプリケーションモジュール２００が特別な機能を有さなくても、Ｅ２Ｅのセキュリティを提供することができる。

【００９０】

次に、Ｍｏｂｉｌｅ　ＳＩＰ　ＡＰｓモジュール２０５が通信データを送信する場合について説明する。Ｍｏｂｉｌｅ　ＳＩＰ　ＡＰｓモジュール２０５は、ＩＡＣモジュール２６１０から通知された、利用可能な通信ＩＦモジュールを介して、通信端末１２に送信すべき通信データを送信する。

【００９１】

具体的には、Ｍｏｂｉｌｅ　ＳＩＰ　ＡＰｓモジュール２０５は、通信端末１２に送信すべき通信データをＲＴＰモジュール２６１５に送信する。ＲＴＰモジュール２６１５は、Ｍｏｂｉｌｅ　ＳＩＰ　ＡＰｓモジュール２０５から受け取った通信データを、ＲＴＰで送信可能な形式に変換する。

【００９２】

そして、ＲＴＰモジュール２６１５は、ＲＴＰで送信可能な形式に変換した通信データを、ＳＲＴＰモジュール２５６に供給する。ＳＲＴＰモジュール２５６は、ＲＴＰモジュール２６１５から受け取った通信データを、ＳＲＴＰを用いて暗号化する。そして、ＳＲＴＰモジュール２５６は、暗号化した通信データを、通信モジュールを介して通信端末１２に送信する。また、通信端末１２から通信ＩＦモジュールが受信したＳＩＰ　ＡＰの通信データは、ＳＲＴＰモジュール２５６が復号化する。そして、ＳＲＴＰモジュール２５６は、ＲＴＰモジュール２６１５を介して、復号化した通信データをＭｏｂｉｌｅ　ＳＩＰ　ＡＰｓモジュール２０５に供給する。

【００９３】

なお、上記説明における通信端末１２に送信する通信データは、プロキシサーバ２０を介して公開サーバ２６等の他のサーバ、または通信端末に送信してもよい。係る場合に、通信端末１０が送信した通信データのデカプセル化および復号化、並びに公開サーバ２６等が送信した通信データのカプセル化および暗号化は、プロキシサーバ２０が実行する。

【００９４】

これにより、通信端末１０は、通信端末１２と送受信する通信データのセキュリティを、ＳＲＴＰを用いて確保できる。さらに、ＩＰｓｅｃを用いることがないので、ＩＰｓｅｃ　Ｓｅｃｕｒｉｔｙ　Ｇａｔｅｗａｙを介して通信データを送受信することがなくなる。これにより、通信トラフィックが一点集中することを回避できる。

【００９５】

図５は、本実施形態に係るＳＩＰサーバ２２の通信モジュール３００の機能構成の一例を示す。通信モジュール３００は、セッションモビリティ制御ユニット３１００、および通信部３２００を備える。セッションモビリティ制御ユニット３１００は、データ形式変換部３６００、シグナリング制御部３６０５、第１暗号化部３６１５、第２暗号化部３６２０、およびシグナリング送受信部３６２５を有する。

【００９６】

通信部３２００は、予め割り当てられた実ＩＰアドレスを有しており、通信端末１０と通信する。シグナリング制御部３６０５は、通信端末１０からのセッション確立要求に対して、シグナリング用のセッションを確立する。そして、シグナリング制御部３６０５は、通信端末１０との間のシグナリングを処理する。シグナリング制御部３６０５は、通信部３２００に割り当てられた実ＩＰアドレスを用いて、通信端末１０との間に第１シグナリング用セッションであるＴＳＬセッションを確立する。そして、ＴＬＳセッションを確立した後、通信端末１０との間に第２シグナリング用セッションであるＳＲＴＰセッションを確立する。さらに、シグナリング制御部３６０５は、通信端末１０が移動することによってハンドオーバ処理をする場合に、第３シグナリング用セッションであるＳＲＴＰセッションを確立する。

【００９７】

シグナリング制御部３６０５は、通信端末１０とのＴＬＳセッションおよび第２シグナリング用セッションであるＳＲＴＰセッションを確立する場合、第１暗号化部３６１５を介して、シグナリングメッセージをシグナリング送受信部３６２５に供給して、ＴＬＳセッションを介して通信端末１０とやりとりする。一方で、シグナリング制御部３６０５は、第２シグナリング用セッションであるＳＲＴＰセッションが確立された後は、データ形式変換部３６００および第２暗号化部３６２０を介して、シグナリングメッセージをシグナリング送受信部３６２５に供給して、第２シグナリング用セッションであるＳＲＴＰセッションを介して通信端末１０とやりとりする。

【００９８】

第１暗号化部３６１５は、シグナリング制御部３６０５が生成したシグナリングメッセージを、通信のセキュリティを確保する第１セキュリティプロトコルを用いて暗号化する。具体的には、第１暗号化部３６１５は、コネクション型の通信プロトコルとともに利用可能な第１セキュリティプロトコルを用いて暗号化する。例えば、第１暗号化部３６１５は、シグナリングメッセージを、第１セキュリティプロトコルとしてＴＬＳプロトコルを用いて暗号化する。

【００９９】

そして、第１暗号化部３６１５は、暗号化したシグナリングメッセージを、シグナリング送受信部３６２５に供給する。また、第１暗号化部３６１５は、通信端末１０から送信されたシグナリングメッセージを復号化してシグナリング制御部３６０５に供給する。

【０１００】

データ形式変換部３６００は、シグナリング制御部３６０５が生成したシグナリングメッセージを、第２セキュリティプロトコルに基づいて暗号化できるデータ形式に変換する。具体的には、データ形式変換部３６００は、ＲＴＰ（Ｒｅａｌ－Ｔｉｍｅ　Ｐｒｏｔｏｃｏｌ）ヘッダを付加することによって、シグナリング制御部３６０５が生成したシグナリングメッセージを、ＳＲＴＰに基づいて暗号化できるＲＴＰのデータ形式に変換する。そして、データ形式変換部３６００は、データ形式を変換したシグナリングメッセージを、第２暗号化部３６２０に供給する。

【０１０１】

第２暗号化部３６２０は、データ形式変換部３６００によってデータ形式が変換されたシグナリングメッセージを、第１セキュリティプロトコルとは異なる第２セキュリティプロトコルに基づいて暗号化する。具体的には、第２暗号化部３６２０は、コネクションレス型の通信プロトコルとともに利用可能な第２セキュリティプロトコルを用いて暗号化する。より具体的には、第２暗号化部３６２０は、ＯＳＩ参照モデルにおけるトランスポート層（レイヤー４）で用いられるコネクションレス型の通信プロトコルとともに利用可能な第２セキュリティプロトコルを用いて暗号化する。例えば、第２暗号化部３６２０は、シグナリングメッセージを、第２セキュリティプロトコルとしてＳＲＴＰを用いて暗号化する。

【０１０２】

そして、第２暗号化部３６２０は、暗号化したシグナリングメッセージを、シグナリン

グ送受信部３６２５に供給する。また、第２暗号化部３６２０は、通信端末１０から送信されたシグナリングメッセージを復号化してデータ形式変換部３６００に供給する。

【０１０３】

シグナリング送受信部３６２５は、第１シグナリング用セッションを確立する場合、シグナリング制御部３６０５が生成して第１暗号化部３６１５が暗号化したシグナリングメッセージを、通信端末１０に送信する。また、シグナリング送受信部３６２５は、第２シグナリング用セッションを確立する場合、シグナリング制御部３６０５が生成して第１暗号化部３６１５が暗号化したシグナリングメッセージを、第１シグナリング用セッションを介して通信端末１０に送信する。このとき、シグナリング送受信部３６２５は、コネクション型の通信プロトコルを用いてシグナリングメッセージを送信する。具体的には、シグナリング送受信部３６２５は、第１暗号化部３６１５から供給されたシグナリングメッセージを通信部３２００に供給してＴＣＰを用いて送信させる。

【０１０４】

シグナリング送受信部３６２５は、第２シグナリング用セッションが確立された後、第２暗号化部３６２０が暗号化したシグナリングメッセージを、第２シグナリング用セッションを介して通信端末１０に送信する。このとき、シグナリング送受信部３６２５は、コネクションレス型の通信プロトコルを用いてシグナリングメッセージを送信する。具体的には、シグナリング送受信部３６２５は、第２暗号化部３６２０から供給されたシグナリングメッセージを、通信部３２００に供給してＵＤＰを用いて送信させる。

【０１０５】

また、シグナリング送受信部１６２５は、通信端末１０から送信されたシグナリングメッセージをシグナリング制御部３６０５に供給する。この場合も、シグナリング送受信部３６２５は、第１シグナリング用セッションおよび第２シグナリング用セッションを確立する場合、シグナリングメッセージを第１暗号化部３６１５に供給する。一方で、シグナリング送受信部３６２５は、第２シグナリング用セッションが確立された後において、シグナリングメッセージを、第２暗号化部３６２０およびデータ形式変換部３６００を介してシグナリング制御部３６０５に供給する。

【０１０６】

本実施形態に係るＳＩＰサーバ２２によれば、通信端末１０とのシグナリングを実行する場合に、通信端末１０に送信するシグナリングメッセージのセキュリティを、ＳＲＴＰを用いて確保できる。これにより、移動先のネットワークで利用できるＳＲＴＰセッションを予め用意することで通信の遅延を防止することができるだけでなく、シグナリングメッセージのセキュリティを確実に確保できる。

【０１０７】

図６は、本実施形態に係るＳＩＰサーバ２２のモジュール構成の一例を示す。なお、通信ＩＦモジュール４２０およびＮＩＣ４３０は、図５の上記説明における通信部３２００の一例である。また、シグナリング制御モジュール４６０５は、図５の上記説明におけるシグナリング制御部３６０５の一例である。また、ＲＴＰモジュール４６１５は、図５の上記説明におけるデータ形式変換部３６００の一例である。また、ＴＬＳモジュール４５８は、図５の上記説明における第１暗号化部３６１５の一例である。また、ＳＲＴＰモジュール４５６は、図５の上記説明における第２暗号化部３６２０の一例である。また、ＵＤＰモジュール４４０およびＴＣＰモジュール４４２は、図５の上記説明におけるシグナリング送受信部３６２５の一例である。

【０１０８】

まず、シグナリング制御モジュール４６０５は、通信端末１０からセッション確立要求が送信されたことを契機として、シグナリングメッセージとして２００ＯＫメッセージを通信端末１０に送信する。すなわち、シグナリング制御モジュール４６０５は、２００ＯＫメッセージをＴＬＳモジュール４５８においてＴＬＳを用いて暗号化させる。そして、シグナリング制御モジュール４６０５は、ＴＬＳで暗号化された２００ＯＫメッセージを、ＴＣＰモジュール４４２から通信ＩＦモジュール４２０を介して通信端末１０に送信す

る。これにより、通信端末１０とＳＩＰサーバ２２との間に第１シグナリング用セッションであるＴＬＳセッションが確立される。

【０１０９】

通信端末１０とＳＩＰサーバ２２との間にＴＬＳセッションが確立すると、シグナリング制御モジュール４６０５は、さらに、通信端末１０からＳＲＴＰセッションのセッション確立要求を受信する。係る場合において、シグナリング制御モジュール４６０５は、さらに２００ＯＫメッセージを生成した後、ＴＬＳモジュール４５８に供給してＴＬＳを用いて暗号化させる。そして、シグナリング制御モジュール４６０５は、ＴＬＳで暗号化された２００ＯＫをＴＣＰモジュール４４２においてＴＣＰで送信可能な形式にする。続いて、シグナリング制御モジュール４６０５は、ＴＬＳで暗号化した上でＴＣＰで送信可能な形式にした２００ＯＫメッセージを、通信ＩＦモジュール４２０を介して通信端末１０に送信する。これにより、通信端末１０とＳＩＰサーバ２２との間に第２シグナリング用セッションであるＳＲＴＰセッションが確立される。

【０１１０】

通信端末１０とＳＩＰサーバ２２との間に第２シグナリング用セッションであるＳＲＴＰセッションが確立すると、その後、シグナリング制御モジュール４６０５は、ＳＲＴＰセッションを介して通信端末１０とシグナリングメッセージをやりとりする。係る場合において、シグナリング制御モジュール４６０５は、生成したシグナリングメッセージをＲＴＰモジュール４６１５に供給する。そして、ＲＴＰモジュール４６１５は、シグナリングメッセージを、ＳＲＴＰに基づいて暗号化できるＲＴＰのデータ形式に変換して、ＳＲＴＰモジュールに供給する。ＳＲＴＰモジュール４５６は、ＲＴＰのデータ形式に変換されたシグナリングメッセージを、ＳＲＴＰで暗号化して通信ＩＦモジュール４２０を介して通信端末１０に送信する。

【０１１１】

以上のように、ＳＩＰサーバ２２は、通信端末１０との間でＳＲＴＰセッションを確立できる。通信端末１０に動的に割り当てられる実ＩＰアドレスが変化した場合でも、移動先のネットワークで利用できるＳＲＴＰセッションが予め用意されるので、通信端末１０とのシグナリングのためのセッションが途切れることなく、継続的に通信端末１０とのシグナリングを実行することができる。

【０１１２】

図７は、本実施形態に係る通信端末１０の起動処理の流れの一例を示す。セッションモビリティコントローラモジュール２６０が起動すると（Ｓ７００）、シグナリング制御モジュール２６０５は、ＳＩＰサーバ２２との間にＴＬＳセッションを確立する（Ｓ７１０）。ＴＳＬセッションが確立されると、ＳＩＰサーバ２２は、通信端末１０をＳＩＰ登録する（Ｓ７２０）。

【０１１３】

次に、シグナリング制御モジュール２６０５は、Ｖｉｒｔｕａｌ　ＩＦモジュール２１０を有効にするために必要な情報を取得して設定する（Ｓ７３０）。具体的には、仮想ＩＰアドレス、プロキシサーバのＩＰアドレス、デフォルトゲートウェイのＩＰアドレス、ＤＮＳサーバのＩＰアドレス等のコアネットワーク４２に関する情報を取得する。

【０１１４】

次に、シグナリング制御モジュール２６０５は、ＳＩＰサーバ２２との間にＳＲＴＰセッションを確立する（Ｓ７４０）。このとき、シグナリング制御モジュール２６０５は、ＴＬＳセッションを用いて、ＳＲＴＰセッションを確立するためのシグナリングメッセージをＳＩＰサーバ２２との間でやりとりする。係る場合において、シグナリング制御モジュール２６０５は、ＴＬＳセッションを確立したときに得られた、ＳＩＰサーバ２２との相互の認証情報を使って、ＳＲＴＰセッションを確立する。その後、シグナリング制御モジュール２６０５は、ＴＬＳセッションを用いることなく、ＳＲＴＰセッションを用いて、音声データ通信を確立する場合のシグナリングメッセージをやりとりする（Ｓ７５０）。

【０１１５】
図８は、本実施形態に係る通信端末１０のハンドオーバ処理の流れを示す。通信端末１０が第１通信ＩＦモジュールを用いて第１通信方式で通信している状態において（Ｓ８００）、ＩＡＣモジュール２６１０は、第１通信方式とは異なる第２通信方式で通信する第２通信ＩＦモジュールが実ＩＰアドレスを取得したか否かを検出する（Ｓ８１０）。第２通信ＩＦモジュールが実ＩＰアドレスを取得していない場合には（Ｓ８１０－Ｎ）、通信端末１０は、引き続き第１通信方式で通信する（Ｓ８００）。
【０１１６】
第２通信ＩＦモジュールが実ＩＰアドレスを取得した場合には（Ｓ８１０－Ｙ）、シグナリング制御モジュール２６０５は、第１通信方式で確立されているＳＲＴＰセッションを介して、第２通信方式で利用するシグナリング用のＳＲＴＰセッションを確立する（Ｓ８２０）。さらに、シグナリング制御モジュール２６０５は、第１通信方式で確立されているＳＲＴＰセッションを介して、第２通信方式で利用する通信データ用のＳＲＴＰセッションを確立する（Ｓ８３０）。係る場合において、シグナリング制御モジュール２６０５は、第１通信方式のＳＲＴＰセッションを確立したときに得られた、ＳＩＰサーバ２２との相互の認証情報を使って、第２通信方式のＳＲＴＰセッションを確立する。
【０１１７】
その後、ＩＡＣモジュール２６１０は、複数の通信ＩＦモジュールが通信中継装置から受信する電波の強度、複数の通信ＩＦモジュールに対して予め設定された利用優先順位等のポリシー等に基づいて、第１通信ＩＦモジュールと第２通信ＩＦモジュールとのいずれを選択するかを判断する（Ｓ８４０）。そして、第１通信方式の第１通信ＩＦモジュールが選択された場合には（Ｓ８４０－Ｎ）、通信端末１０は、引き続き第１通信方式で通信する（Ｓ８５０）。一方で、第２通信方式の第２通信ＩＦモジュールが選択された場合には、通信端末１０は、第１通信ＩＦモジュールから第２通信ＩＦモジュールに切り換え、第２通信ＩＦモジュールを用いて第２通信方式で通信する（Ｓ８６０）。そして、通信端末１０は、ＳＩＰサーバ２２との間で、Ｓ８２０で確立されたＳＲＴＰセッションを介してシグナリングメッセージをやりとりする。また、通信端末１０は、通信端末１２との間で、Ｓ８３０で確立されたＳＲＴＰセッションを介して通信データをやりとりする。
【０１１８】
図９は、通信データの送信処理の流れの一例を示す。まず、一般クライアントアプリケーションモジュール２００は、通信端末１２に送信すべき通信データを、Ｖｉｒｔｕａｌ　ＩＦモジュール２１０に割り当てられた仮想ＩＰアドレスを指定して送信する（Ｓ６００）。仮想ＩＰアドレスは、Ｖｉｒｔｕａｌ　ＩＦモジュール２１０に固定的に割り当てられるので、一般クライアントアプリケーションモジュール２００は、通信中継装置が通信端末１０に動的に割り当てたＩＰアドレスがいかなるＩＰアドレスであっても、常に仮想ＩＰアドレスを指定して、通信データを送信する。なお、一般クライアントアプリケーションモジュール２００は、ＴＣＰを用いて送信可能な形式で通信データをＶｉｒｔｕａｌ　ＩＦモジュール２１０に送信する。
【０１１９】
Ｖｉｒｔｕａｌ　ＩＦモジュール２１０は、一般クライアントアプリケーションモジュール２００から受け取った通信データに関してパケット処理を実行する（Ｓ６１０）。すなわち、Ｖｉｒｔｕａｌ　ＩＦモジュール２１０は、一般クライアントアプリケーションモジュール２００から受け取った、複数の通信パケットを含む通信データを（デ）カプセル化モジュール２６００に供給する。（デ）カプセル化モジュール２６００は、Ｖｉｒｔｕａｌ　ＩＦモジュール２１０から受け取った通信データを、ＵＤＰを用いて通信できる形式にカプセル化する（Ｓ６２０）。
【０１２０】
例えば、（デ）カプセル化モジュール２６００は、ＩＡＣモジュール２６１０が取得した実ＩＰアドレスをＴＣＰで通信可能な形式の通信データに付加してカプセル化することにより、ＵＤＰで通信可能な形式にカプセル化する。（デ）カプセル化モジュール２６０

０は、カプセル化した通信データをＳＲＴＰモジュール２５６に供給する。ＳＲＴＰモジュール２５６は、（デ）カプセル化モジュール２６００から受け取った通信データを、第２セキュリティプロトコルであるＳＲＴＰで暗号化する（Ｓ６３０）。そして、ＵＤＰモジュール２４０は、ＳＲＴＰモジュール２５６が暗号化した通信データを、第２通信プロトコルであるＵＤＰを用いて、通信ＩＦモジュールから通信端末１２に送信する。

【０１２１】

図１０は、通信データの受信処理の流れの一例を示す。まず、ＵＤＰモジュール２４０は、通信端末１２が通信端末１０にあてて送信した通信データを、通信ＩＦモジュールを介して受信する（Ｓ７００）。通信端末１２が通信端末１０にあてて送信した通信データは、ＴＣＰで通信可能な通信データをＵＤＰで通信可能な形式にカプセル化した上で、第２セキュリティプロトコルであるＳＲＴＰを用いて暗号化されている。

【０１２２】

ＵＤＰモジュール２４０は、受信した通信データをＳＲＴＰモジュール２５６に供給する。ＳＲＴＰモジュール２５６は、ＳＲＴＰを用いて暗号化されている通信データを復号化する（Ｓ７１０）。ＳＲＴＰモジュール２５６は、復号化した通信データを（デ）カプセル化モジュール２６００に供給する。（デ）カプセル化モジュール２６００は、ＳＲＴＰモジュール２５６から受け取った通信データをデカプセル化する（Ｓ７２０）。（デ）カプセル化モジュール２６００は、でカプセル化した後の通信データをＶｉｒｔｕａｌ　ＩＦモジュール２１０に供給する。Ｖｉｒｔｕａｌ　ＩＦモジュール２１０は、（デ）カプセル化モジュール２６００から受け取った通信データをパケット処理して（Ｓ７３０）、一般クライアントアプリケーションモジュール２００に転送する（Ｓ７４０）。

【０１２３】

図１１は、本実施形態に係る通信端末１０またはＳＩＰサーバ２２のハードウェア構成の一例を示す。なお、本実施形態に係るプロキシサーバ２０は、以下に述べるハードウェア構成の一部または全部を備えていてもよい。本実施形態に係る通信端末１０およびＳＩＰサーバ２２は、ホスト・コントローラ１５８２により相互に接続されるＣＰＵ１５０５、ＲＡＭ１５２０、グラフィック・コントローラ１５７５、および表示装置１５８０を有するＣＰＵ周辺部と、入出力コントローラ１５８４によりホスト・コントローラ１５８２に接続される通信インターフェース１５３０、ハードディスクドライブ１５４０、およびＣＤ－ＲＯＭドライブ１５６０を有する入出力部と、入出力コントローラ１５８４に接続されるＲＯＭ１５１０、フレキシブルディスク・ドライブ１５５０、および入出力チップ１５７０を有するレガシー入出力部とを備える。

【０１２４】

ホスト・コントローラ１５８２は、ＲＡＭ１５２０と、高い転送レートでＲＡＭ１５２０をアクセスするＣＰＵ１５０５およびグラフィック・コントローラ１５７５とを接続する。ＣＰＵ１５０５は、ＲＯＭ１５１０およびＲＡＭ１５２０に格納されたプログラムに基づいて動作して、各部を制御する。グラフィック・コントローラ１５７５は、ＣＰＵ１５０５等がＲＡＭ１５２０内に設けたフレーム・バッファ上に生成する画像データを取得して、表示装置１５８０上に表示させる。これに代えて、グラフィック・コントローラ１５７５は、ＣＰＵ１５０５等が生成する画像データを格納するフレーム・バッファを、内部に含んでもよい。

【０１２５】

入出力コントローラ１５８４は、ホスト・コントローラ１５８２と、比較的高速な入出力装置である通信インターフェース１５３０、ハードディスクドライブ１５４０、ＣＤ－ＲＯＭドライブ１５６０を接続する。通信インターフェース１５３０は、ネットワークを介して他の装置と通信する。ハードディスクドライブ１５４０は、通信端末１０またはＳＩＰサーバ２２内のＣＰＵ１５０５が使用するプログラムおよびデータを格納する。ＣＤ－ＲＯＭドライブ１５６０は、ＣＤ－ＲＯＭ１５９５からプログラムまたはデータを読み取り、ＲＡＭ１５２０を介してハードディスクドライブ１５４０に提供する。

【０１２６】

また、入出力コントローラ１５８４には、ＲＯＭ１５１０と、フレキシブルディスク・ドライブ１５５０、および入出力チップ１５７０の比較的低速な入出力装置とが接続される。ＲＯＭ１５１０は、通信端末１０またはＳＩＰサーバ２２が起動時に実行するブート・プログラム、通信端末１０またはＳＩＰサーバ２２のハードウェアに依存するプログラム等を格納する。フレキシブルディスク・ドライブ１５５０は、フレキシブルディスク１５９０からプログラムまたはデータを読み取り、ＲＡＭ１５２０を介してハードディスクドライブ１５４０に提供する。入出力チップ１５７０は、フレキシブルディスク・ドライブ１５５０、例えばパラレル・ポート、シリアル・ポート、キーボード・ポート、マウス・ポート等を介して各種の入出力装置を接続する。

【０１２７】

ＲＡＭ１５２０を介してハードディスクドライブ１５４０に提供される通信プログラムは、フレキシブルディスク１５９０、ＣＤ－ＲＯＭ１５９５、またはＩＣカード等の記録媒体に格納されて利用者によって提供される。通信プログラムは、記録媒体から読み出され、ＲＡＭ１５２０を介して通信端末１０またはＳＩＰサーバ２２内のハードディスクドライブ１５４０にインストールされ、ＣＰＵ１５０５において実行される。

【０１２８】

通信端末１０にインストールされて実行される通信プログラムは、ＣＰＵ１５０５等に働きかけて、通信端末１０を、図１から図１０にかけて説明した一般アプリケーション部１００、リアルタイムアプリケーション部１０５、仮想インターフェース部１１０、複数の通信部、通信ＩＦ選択部１４０、アドレス取得部１５０、データ形式変換部１６００、シグナリング制御部１６０５、（デ）カプセル化部１６１０、第２暗号化部１６２０、シグナリング送受信部１６２５、変換テーブル記憶部１６４０、およびデータ送受信部１６４５として機能させる。

【０１２９】

また、ＳＩＰサーバ２２にインストールされて実行される通信プログラムは、ＣＰＵ１５０５等に働きかけて、ＳＩＰサーバ２２を、図１から図１０にかけて説明したセッションモビリティ制御ユニット３１００および通信部３２００として機能させる。

【０１３０】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更または改良を加え得ることが当業者に明らかである。そのような変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【図面の簡単な説明】

【０１３１】

【図１】通信システムのネットワーク接続構成を示す。
【図２】通信セキュリティの概要を示す。
【図３】通信端末１０の通信モジュール１４の機能構成を示す。
【図４】通信端末１０のモジュール構成を示す。
【図５】ＳＩＰサーバ２２の通信モジュール３００の機能構成を示す。
【図６】ＳＩＰサーバ２２のモジュール構成を示す。
【図７】通信端末１０の起動処理の流れの一例を示す。
【図８】通信端末１０のハンドオーバ処理の流れを示す。
【図９】通信データの送信処理の流れを示すフローチャートである。
【図１０】通信データの受信処理の流れを示すフローチャートである。
【図１１】通信端末１０またはＳＩＰサーバ２２のハードウェア構成を示す。

【符号の説明】

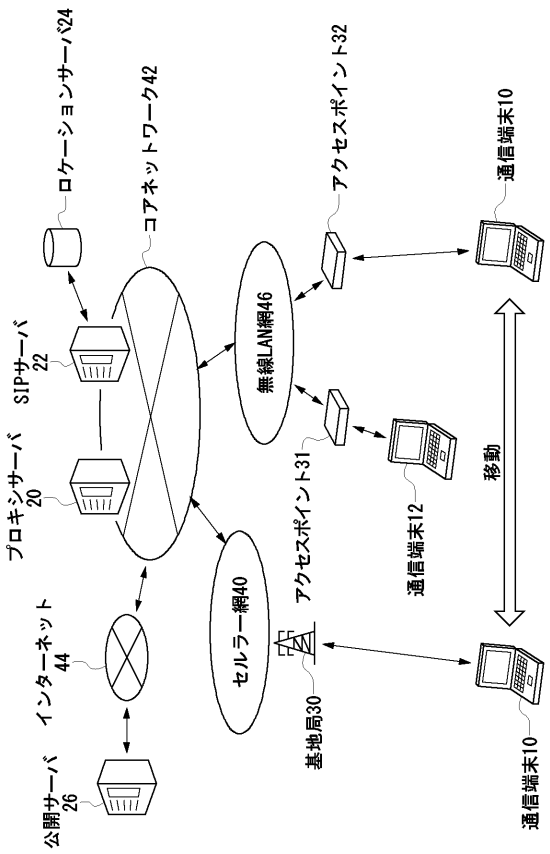
【０１３２】

１０、１２　通信端末
１４　通信モジュール
２０　プロキシサーバ

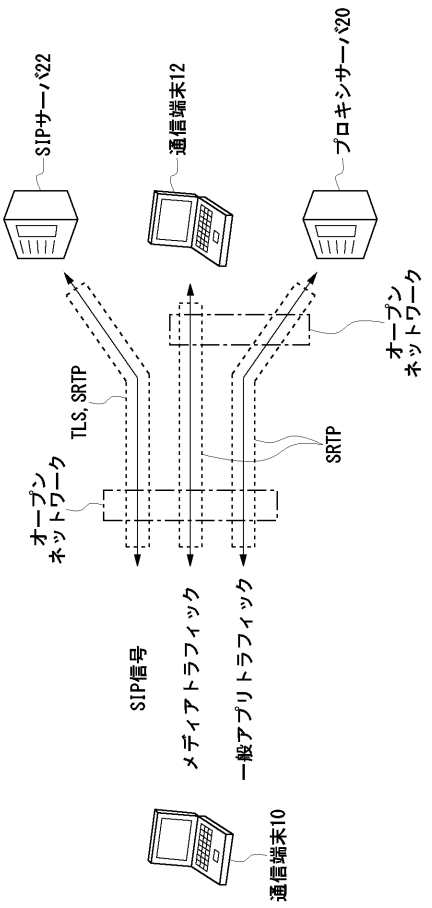
２２　ＳＩＰサーバ
２４　ロケーションサーバ
２６　公開サーバ
３０　基地局
３１　アクセスポイント
３２　アクセスポイント
４０　セルラー網
４２　コアネットワーク
４４　インターネット
４６　無線ＬＡＮ網
１００　一般アプリケーション部
１０５　リアルタイムアプリケーション部
１１０　仮想インターフェース部
１２０　通信ユニット
１２２　第１通信部
１２４　第２通信部
１２６　第ｎ通信部
１３０　通信制御ユニット
１４０　通信ＩＦ選択部
１５０　アドレス取得部
１６０　セッションモビリティ制御ユニット
２００　一般クライアントアプリケーションモジュール
２０５　Ｍｏｂｉｌｅ　ＳＩＰ　ＡＰｓモジュール
２１０　Ｖｉｒｔｕａｌ　ＩＦモジュール
２２０　通信インターフェースユニット
２２２　通信ＩＦモジュールａ
２２４　通信ＩＦモジュールｂ
２２６　通信ＩＦモジュールｎ
２３２　ＮＩＣａ
２３４　ＮＩＣｂ
２３６　ＮＩＣｎ
２４０　ＵＤＰモジュール
２４２　ＴＣＰモジュール
２５４　ＴＣＰ／ＵＤＰモジュール
２５６　ＳＲＴＰモジュール
２５８　ＴＬＳモジュール
２６０　セッションモビリティコントローラモジュール
３００　通信モジュール
４２０　通信ＩＦモジュール
４３０　ＮＩＣ
４４０　ＵＤＰモジュール
４４２　ＴＣＰモジュール
４５６　ＳＲＴＰモジュール
４５８　ＴＬＳモジュール
４６０　セッションモビリティコントローラモジュール
１５０５　ＣＰＵ
１５１０　ＲＯＭ
１５２０　ＲＡＭ
１５３０　通信インターフェース
１５４０　ハードディスクドライブ

１５５０　フレキシブルディスク・ドライブ
１５６０　ＣＤ－ＲＯＭドライブ
１５７０　入出力チップ
１５７５　グラフィック・コントローラ
１５８０　表示装置
１５８２　ホスト・コントローラ
１５８４　入出力コントローラ
１５９０　フレキシブルディスク
１５９５　ＣＤ－ＲＯＭ
１６００　データ形式変換部
１６０５　シグナリング制御部
１６１０　（デ）カプセル化部
１６１５　第１暗号化部
１６２０　第２暗号化部
１６２５　シグナリング送受信部
１６４０　変換テーブル記憶部
１６４５　データ送受信部
２６００　（デ）カプセル化モジュール
２６０５　シグナリング制御モジュール
２６１０　ＩＡＣモジュール
２６１５　ＲＴＰモジュール
２６２０　ＲＴＰモジュール
３１００　セッションモビリティ制御ユニット
３２００　通信部
３６００　データ形式変換部
３６０５　シグナリング制御部
３６１５　第１暗号化部
３６２０　第２暗号化部
３６２５　シグナリング送受信部
４６０５　シグナリング制御モジュール
４６１５　ＲＴＰモジュール

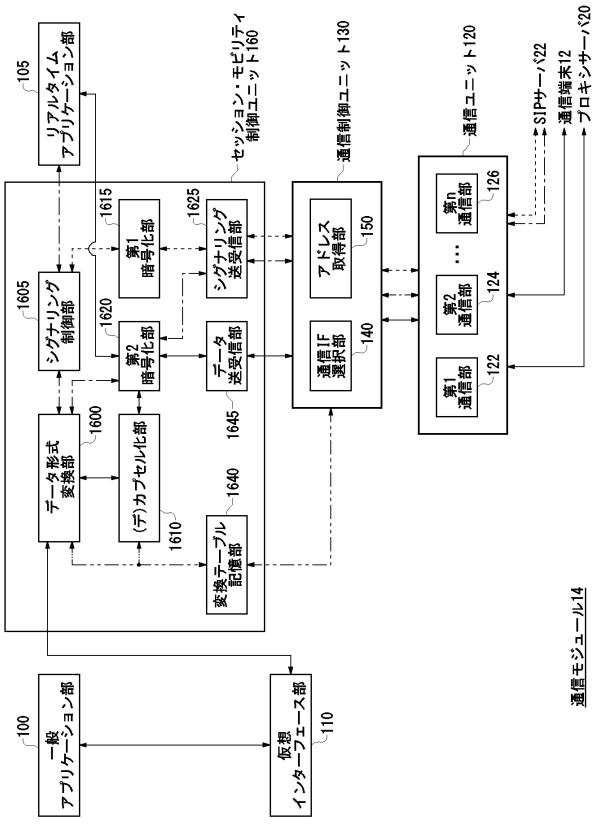
【図１】


ロケーションサーバ24
コアネットワーク42
SIPサーバ 22
プロキシサーバ 20
無線LAN網46
アクセスポイント32
通信端末10
インターネット 44
セルラー網40
アクセスポイント31
通信端末12
移動
公開サーバ 26
基地局30
通信端末10

【図２】


SIPサーバ22
通信端末12
プロキシサーバ20
オープン ネットワーク
TLS, SRTP
SRTP
オープン ネットワーク
SIP信号
メディアトラフィック
一般アプリトラフィック
通信端末10

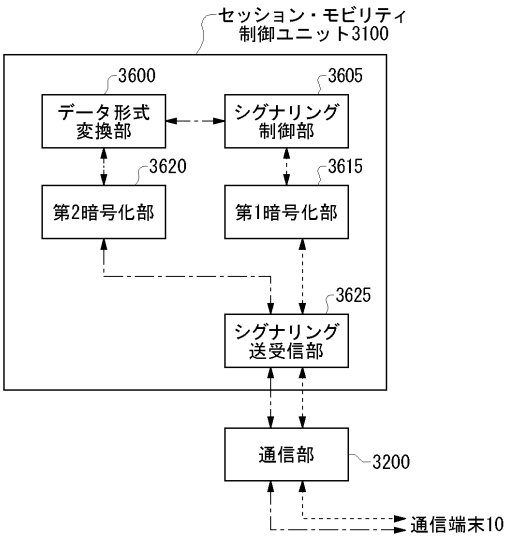
【図３】


リアルタイム アプリケーション部
セッション・モビリティ 制御ユニット160
通信制御ユニット130
通信ユニット120
SIPサーバ22
通信端末12
プロキシサーバ20
シグナリング 制御部
第2 暗号化部
データ 送受信部
アドレス 取得部
通信IF 選択部
第1 通信部
第2 通信部
第n 通信部
データ形式 変換部
(デ)カプセル化部
変換テーブル 記憶部
一般 アプリケーション部
仮想 インターフェース部
通信モジュール14

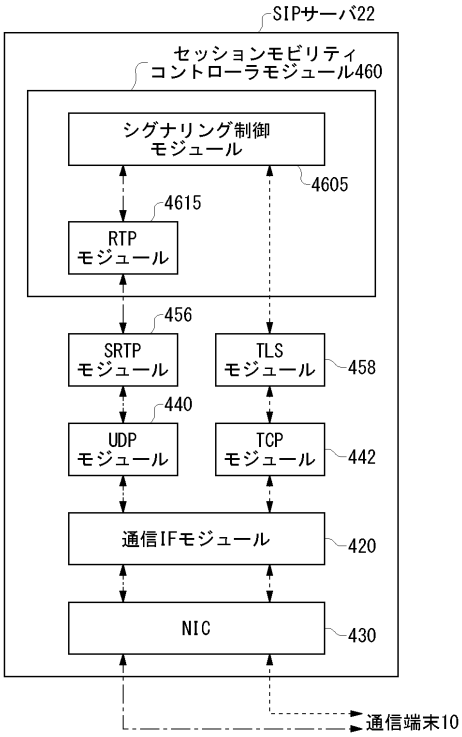
【図４】

通信端末10
SIPサーバ22
プロキシサーバ20
通信端末12
Mobile SIP APs モジュール
シグナリング制御 モジュール
IAC モジュール
TLSモジュール
TCPモジュール
通信IF モジュールn
NICn
RTPモジュール
SRTPモジュール
UDPモジュール
通信IF モジュールb
NICb
通信IF モジュールa
NICa
(デ)カプセル化 モジュール
セッションモビリティ コントローラモジュール
一般クライアントアプリケーション モジュール
TCP/UDP モジュール
Virtual IF モジュール

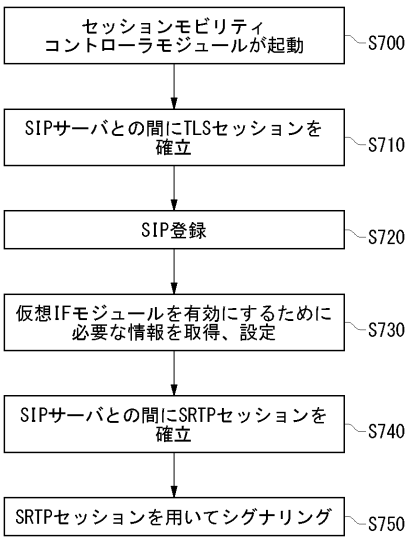
【図５】


セッション・モビリティ
制御ユニット3100
3600
データ形式
変換部
3605
シグナリング
制御部
3620
第2暗号化部
3615
第1暗号化部
3625
シグナリング
送受信部
通信部
3200
通信端末10
通信モジュール300

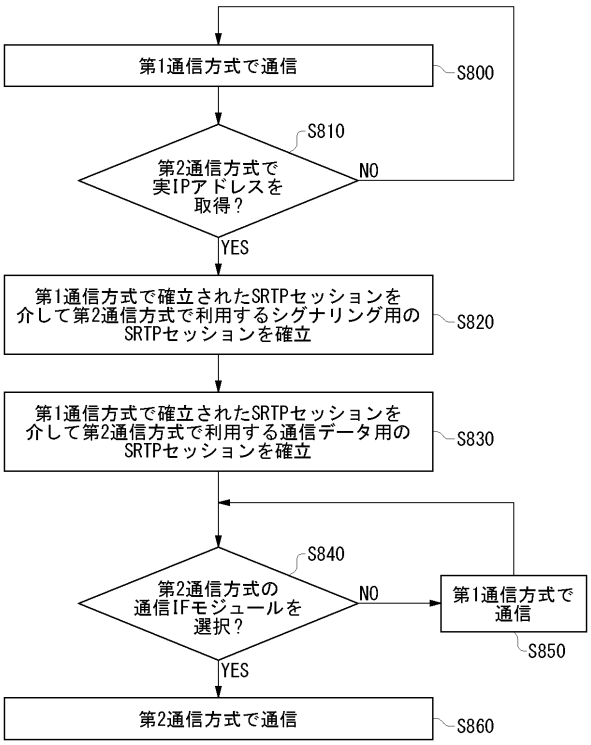
【図６】


SIPサーバ22
セッションモビリティ
コントローラモジュール460
シグナリング制御
モジュール
4605
4615
RTP
モジュール
456
SRTP
モジュール
TLS
モジュール
458
440
UDP
モジュール
TCP
モジュール
442
通信IFモジュール
420
NIC
430
通信端末10

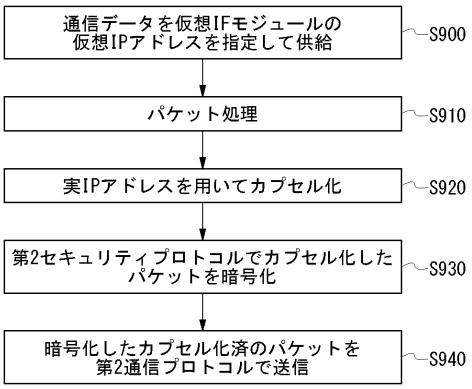
【図７】


セッションモビリティ
コントローラモジュールが起動
S700
SIPサーバとの間にTLSセッションを
確立
S710
SIP登録
S720
仮想IFモジュールを有効にするために
必要な情報を取得、設定
S730
SIPサーバとの間にSRTPセッションを
確立
S740
SRTPセッションを用いてシグナリング
S750

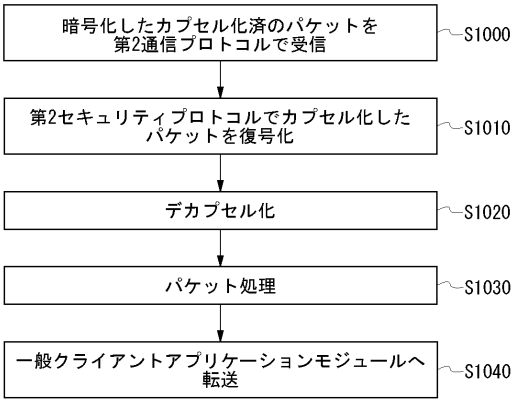
【図８】


第1通信方式で通信
S800
S810
第2通信方式で
実IPアドレスを
取得？
NO
YES
第1通信方式で確立されたSRTPセッションを
介して第2通信方式で利用するシグナリング用の
SRTPセッションを確立
S820
第1通信方式で確立されたSRTPセッションを
介して第2通信方式で利用する通信データ用の
SRTPセッションを確立
S830
S840
第2通信方式の
通信IFモジュールを
選択？
NO
第1通信方式で
通信
S850
YES
第2通信方式で通信
S860

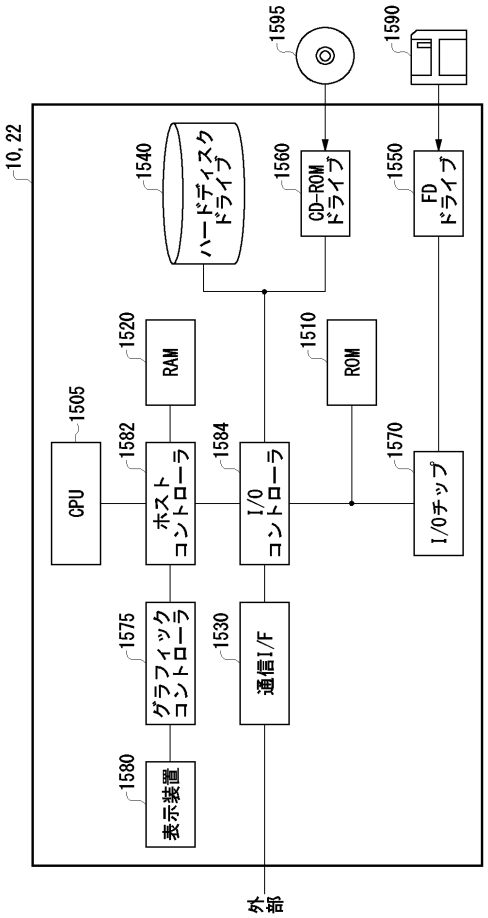
【図９】


通信データを仮想IFモジュールの仮想IPアドレスを指定して供給
S900
パケット処理
S910
実IPアドレスを用いてカプセル化
S920
第2セキュリティプロトコルでカプセル化したパケットを暗号化
S930
暗号化したカプセル化済のパケットを第2通信プロトコルで送信
S940

【図１０】


暗号化したカプセル化済のパケットを第2通信プロトコルで受信
S1000
第2セキュリティプロトコルでカプセル化したパケットを復号化
S1010
デカプセル化
S1020
パケット処理
S1030
一般クライアントアプリケーションモジュールへ転送
S1040

【図１１】


10, 22
1595
1590
1540
ハードディスクドライブ
1560
CD-ROMドライブ
1550
FDドライブ
1520
RAM
1510
ROM
1505
CPU
1582
ホストコントローラ
1584
I/Oコントローラ
1570
I/Oチップ
1575
グラフィックコントローラ
1530
通信I/F
1580
表示装置
外部

フロントページの続き

(72)発明者　林　秀樹
東京都港区東新橋一丁目９番１号　ソフトバンクモバイル株式会社内
(72)発明者　藤井　輝也
東京都港区東新橋一丁目９番１号　ソフトバンクモバイル株式会社内

審査官　森谷　哲朗

(56)参考文献　J. Bilien, E. Eliasson, J. Orrblad, J-O. Vatn, Secure VoIP: call establishment and media protection, ２００５年　６月, pp.1-19, ＵＲＬ, http://www.minisip.org/publications/secvoip-minisip-camera.pdf
Tzvetkov, V. Zuleger, H., Service Provider Implementation of SIP Regarding Security, Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference on, ２００７年　５月２１日, pp.30-35, ＵＲＬ, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4221031
Naoya SETA;et al., All-SIP Mobility: Session Continuity on Handover in Heterogeneous Access Environment, Vehicular Technology Conference, 2007.VTC2007-Spring.IEEE 65th, ２００７年　４月２２日, p.1121-1126
張　亮　他, アクセス網非依存Ａｌｌ－ＳＩＰモビリティ技術のセキュリティ方式の提案, 電子情報通信学会技術研究報告, ２００７年　９月１３日, 第107巻,第222号, pp.19-24

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　２９／０６
Ｈ０４Ｌ　１２／６６
Ｈ０４Ｌ　２９／０８