(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2009 年2 月5 日 (05.02.2009)

PCT

(10) 国際公開番号
WO 2009/017097 A1

(51) 国際特許分類:
H04Q 7/38 (2006.01) *H04L 29/08* (2006.01)
H04L 12/66 (2006.01) *H04Q 7/32* (2006.01)
H04L 29/06 (2006.01)

(21) 国際出願番号: PCT/JP2008/063538

(22) 国際出願日: 2008 年7 月28 日 (28.07.2008)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2007-200107 2007 年7 月31 日 (31.07.2007) JP

(71) 出願人 (米国を除く全ての指定国について): ソフトバンクモバイル株式会社 (SOFTBANK MOBILE CORP.) [JP/JP]; 〒1057317 東京都港区東新橋一丁目９番１号 Tokyo (JP).

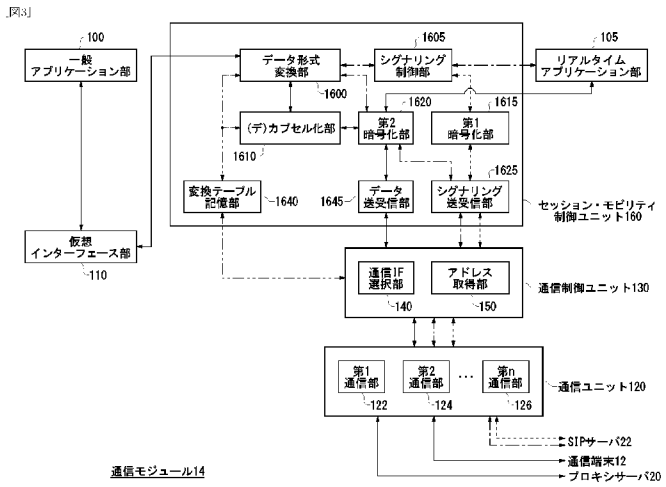
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 瀬田 直也 (SETA, Naoya) [JP/JP]; 〒1057317 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 Tokyo (JP). 宮島 春弥 (MIYAJIMA, Haruya) [JP/JP]; 〒1057317 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 Tokyo (JP). 張 亮 (ZHANG, Liang) [JP/JP]; 〒1057317 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 Tokyo (JP). 林 秀樹 (HAYASHI, Hideki) [JP/JP]; 〒1057317 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 Tokyo (JP). 藤井 輝也 (FUJII, Teruya) [JP/JP]; 〒1057317 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 Tokyo (JP).

[続葉有]

(54) **Title:** COMMUNICATION MODULE, COMMUNICATION METHOD, COMMUNICATION PROGRAM, COMMUNICATION TERMINAL, AND COMMUNICATION CONTROL DEVICE

(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



100 GENERAL APPLICATION UNIT
110 VIRTUAL INTERFACE UNIT
160 SESSION MOBILITY CONTROL UNIT
1600 DATA FORMAT CONVERSION BLOCK
1605 SIGNALING CONTROL BLOCK
1610 DE-CAPSULATION BLOCK
1620 SECOND ENCRYPTION BLOCK
1615 FIRST ENCRYPTION BLOCK
1640 CONVERSION TABLE STORAGE BLOCK
1645 DATA TRANSMISSION RECEPTION BLOCK
1625 SIGNALING TRANSMISSION RECEPTION BLOCK
105 REAL TIME APPLICATION UNIT
130 COMMUNICATION CONTROL UNIT
140 COMMUNICATION IF SELECTION BLOCK
150 ADDRESS ACQUISITION BLOCK
120 COMMUNICATION UNIT
122 FIRST COMMUNICATION BLOCK
124 SECOND COMMUNICATION BLOCK
126 N-TH COMMUNICATION BLOCK
22 SIP SERVER
12 COMMUNICATION TERMINAL
20 PROXY SERVER
14 COMMUNICATION MODULE

(57) Abstract: To ensure mobility of a communication terminal and confidentiality of communication data and signaling. A communication module according to the present invention comprises a signaling control block for generating a signaling message and a signaling transmission reception block for transmitting the signaling message generated by the signaling control block to a communication control device which manages the session between the communication terminal and a communication destination terminal. The signaling control block establishes a session for first signaling according to a first security protocol with the communication control device when the communication module is activated and establishes a session for second signaling according to a second security protocol with the communication control device when the session for first signaling has been established. The signaling transmission reception block transmits the signaling message generated by the signaling control block to the communication control device via the session for second signaling.

[続葉有]

WO 2009/017097 A1

(74) 代理人: 龍華 明裕 (RYUKA, Akihiro); 〒1631105 東京都新宿区西新宿６－２２－１ 新宿スクエアタワー５階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

(57) 要約: 通信端末のモビリティを確保するとともに、通信データおよびシグナリングの秘匿性を確保することを目的とする。 本発明に係る通信モジュールは、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、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。

明 細 書

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

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。なお、本出願は、下記の日本出願に関連する。文献の参照による組み込みが認められる指定国については、下記の出願に記載された内容を参照により本出願に組み込み、本出願の一部とする。

特願2007－200107 出願日 2007年7月31日

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。

発明の効果

[0008] 本発明によれば、通信端末のモビリティを確保するとともに、通信データおよびシグナリングの秘匿性を確保することができる。

図面の簡単な説明

[0009] [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

[0010] 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

発明を実施するための最良の形態

[0011] 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。

[0012] 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。

[0013] 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。

[0014] 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 Re

gister、SIP Invite、SIP Bye、200OK等のすべてのシグナリングが含まれる。

[0015] 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。

[0016] 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。

[0017] 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。

[0018] 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。

[0019] 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。

[0020] 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。

[0021] 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。

[0022] 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。

[0023] 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。

[0024] 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。

[0025] 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。

[0026] 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。

[0027] 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。

[0028] 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。

[0029] 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。

[0030] 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。

[0031] 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。

[0032] 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。

[0033] 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。

[0034] 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。

[0035] 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。

[0036] 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。

[0037] 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。

[0038] 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。

[0039] 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。

[0040] 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。

[0041] 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。

[0042] 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。

[0043] 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。

[0044] 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。

[0045] 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。

[0046] 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。

[0047] 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。

[0048] 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。

[0049] 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。

[0050] 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。

[0051] 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。

[0052] 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。

[0053] 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SIP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。

[0054] 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。

[0055] 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。

[0056] 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。

[0057] 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。

[0058] 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。

[0059] (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。

[0060] 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。

[0061] 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。

[0062] 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。

[0063] 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。

[0064] 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。

[0065] 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。

[0066] 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。

[0067] 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。

[0068] 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。

[0069] 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。

[0070] 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。

[0071] 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 I

F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。

[0072] 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。

[0073] 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。

[0074] 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。

[0075] 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。

[0076] 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I

F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。

[0077] 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。

[0078] 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。

[0079] 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。

[0080] 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。

[0081] 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。

[0082] 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。

[0083] 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22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。

[0084] 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。

[0085] 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。

[0086] 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。

[0087] 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。

[0088] 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。

[0089] 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。

[0090] (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。

[0091] 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。

[0092] 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。

[0093] 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。

[0094] 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。

[0095] 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。

[0096] 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。

[0097] 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。

[0098] 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。

[0099] 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。

[0100] 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。

[0101] 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。

[0102] 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。

[0103] 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。

[0104] 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。

[0105] 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。

[0106] 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。

[0107] 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。

[0108] 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3

625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。

[0109] 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。

[0110] 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。

[0111] 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。

[0112] 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。

[0113] 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。

[0114] 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。

[0115] 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)。

[0116] 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。

[0117] 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)。

[0118] 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)。

[0119] 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。

[0120] 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。

[0121] 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。

[0122] 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)。

[0123] 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2600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。

[0124] 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。

[0125] 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)。

[0126] 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。

[0127] 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。

[0128] 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。

[0129] 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。

[0130] 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。

[0131] 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。

[0132] 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。

[0133] 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、請求の範囲の記載から明らかである。

産業上の利用可能性

[0134] 本発明によれば、通信端末のモビリティを確保するとともに、通信データおよびシグナリングの秘匿性を確保することができる。

請求の範囲

[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、

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する、通信モジュール。

[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。

[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。

[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。

[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。

[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。

[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。

[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。

[9] 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、

をさらに備え、

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、請求項1に記載の通信モジュール。

[10] 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9に記載の通信モジュール。

[11] 通信データを送受信する通信端末の通信方法であって、

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、

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する、通信方法。

[12] 通信データを送受信する通信端末の通信モジュール用の通信プログラムであって、前記通信モジュールを、

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、および

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、

として機能させ、

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する、プログラム。

[13] 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、

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する、通信端末。

[14] 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、

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する、通信システム。

[15] 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、

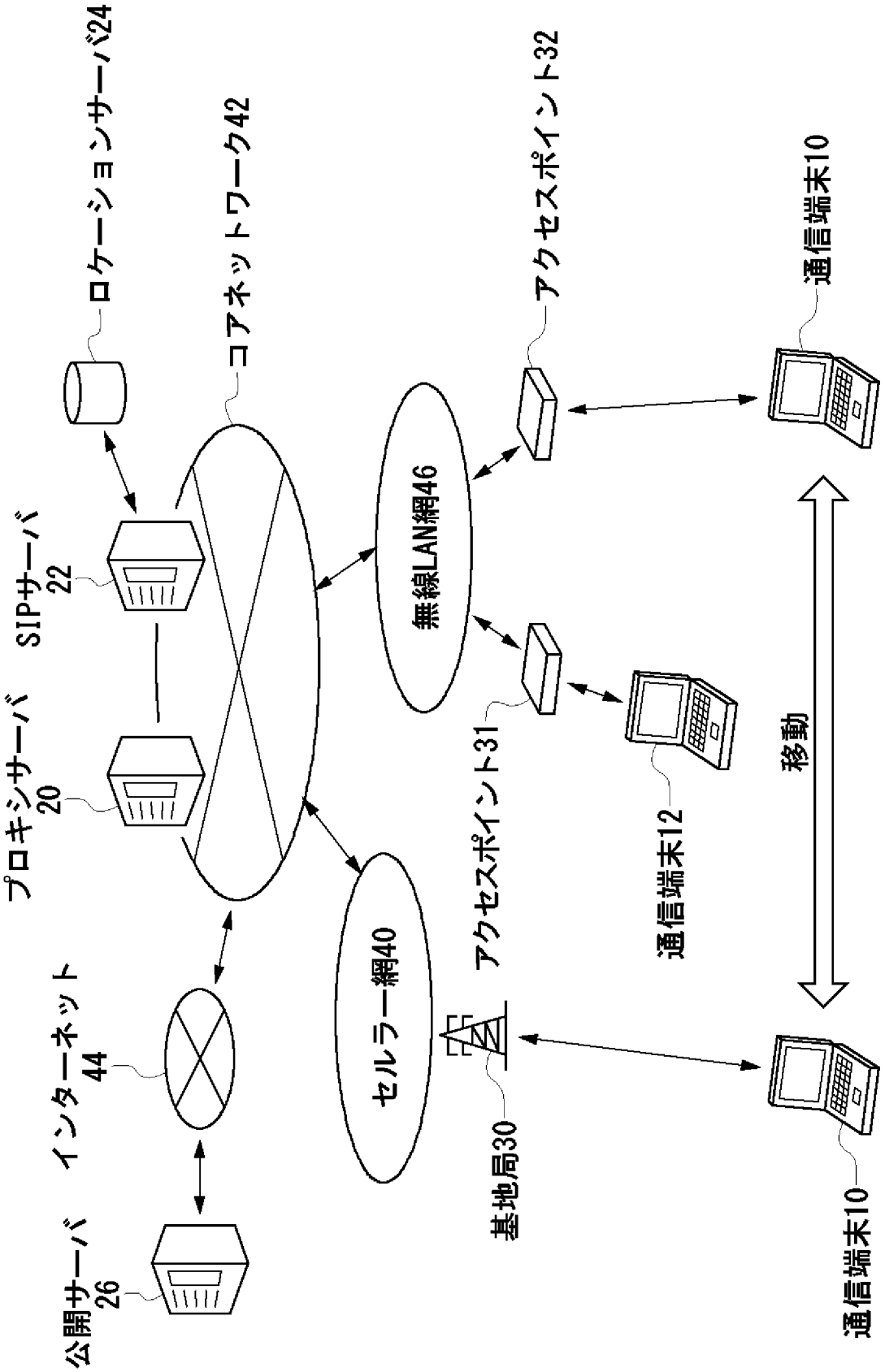
前記シグナリング制御部は、

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、

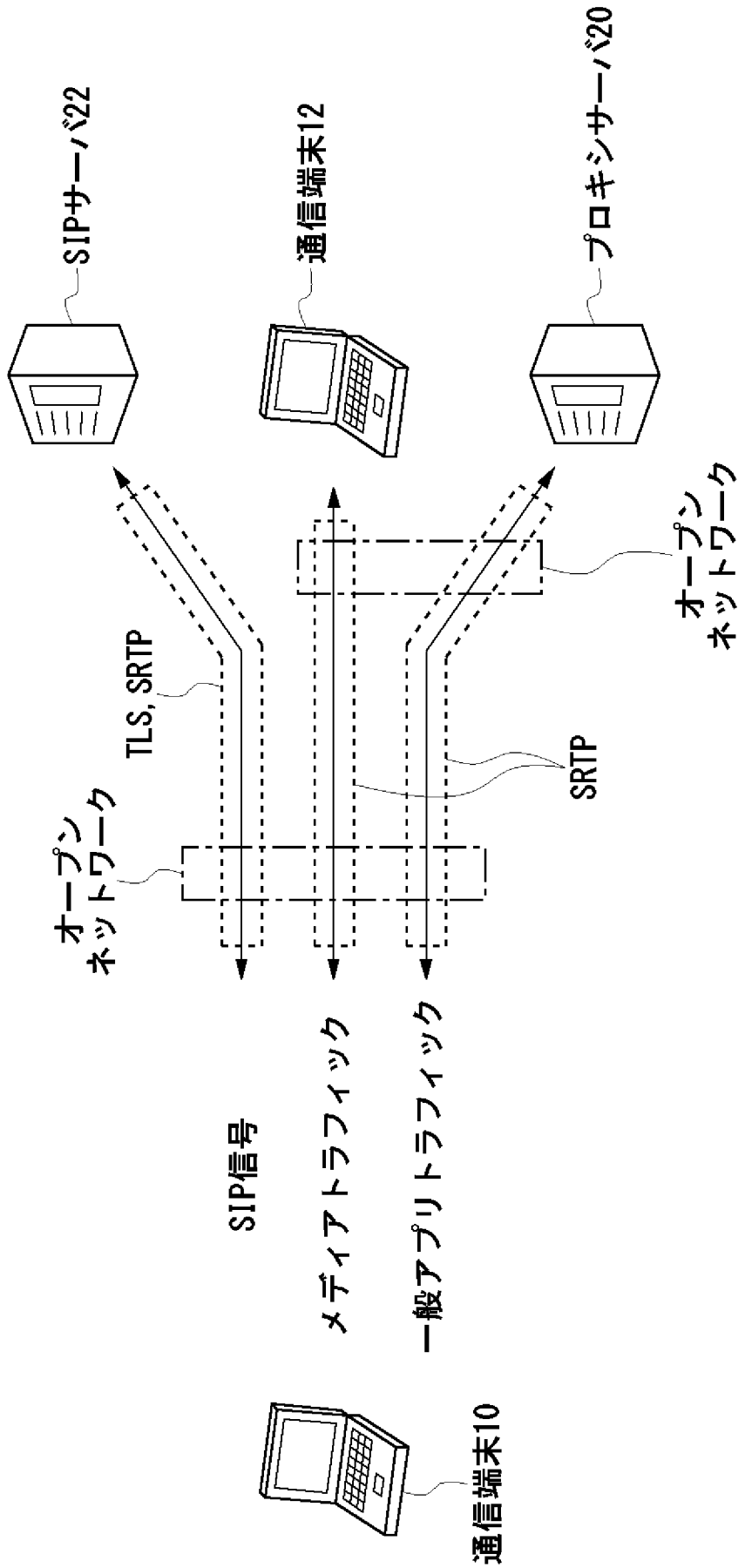
前記第1シグナリング用セッションが確立された場合に、第2セキュリティプロトコルに基づく第2シグナリング用セッションを、前記通信端末との間に確立し、

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する、通信制御装置。

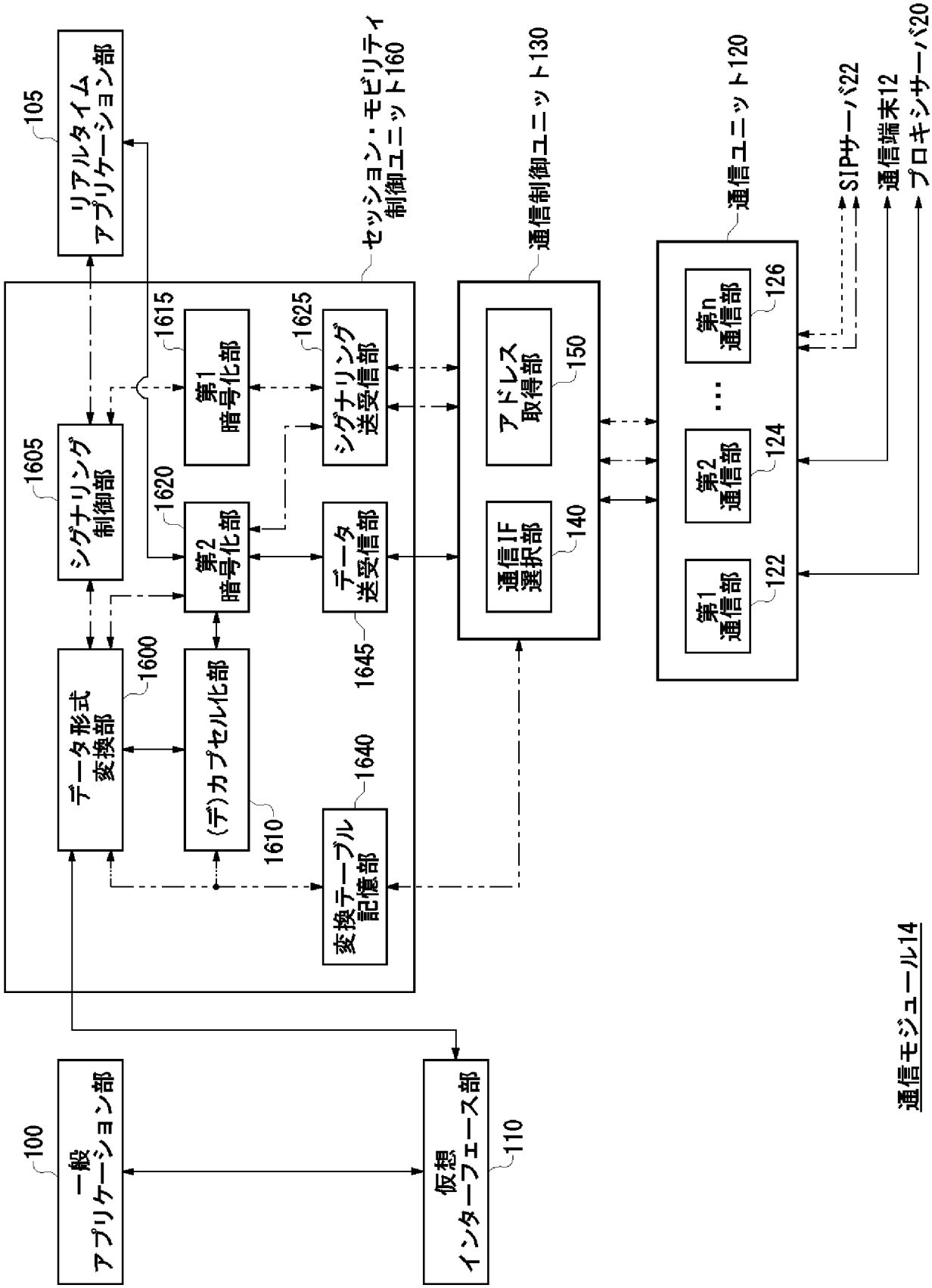
[図1]


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

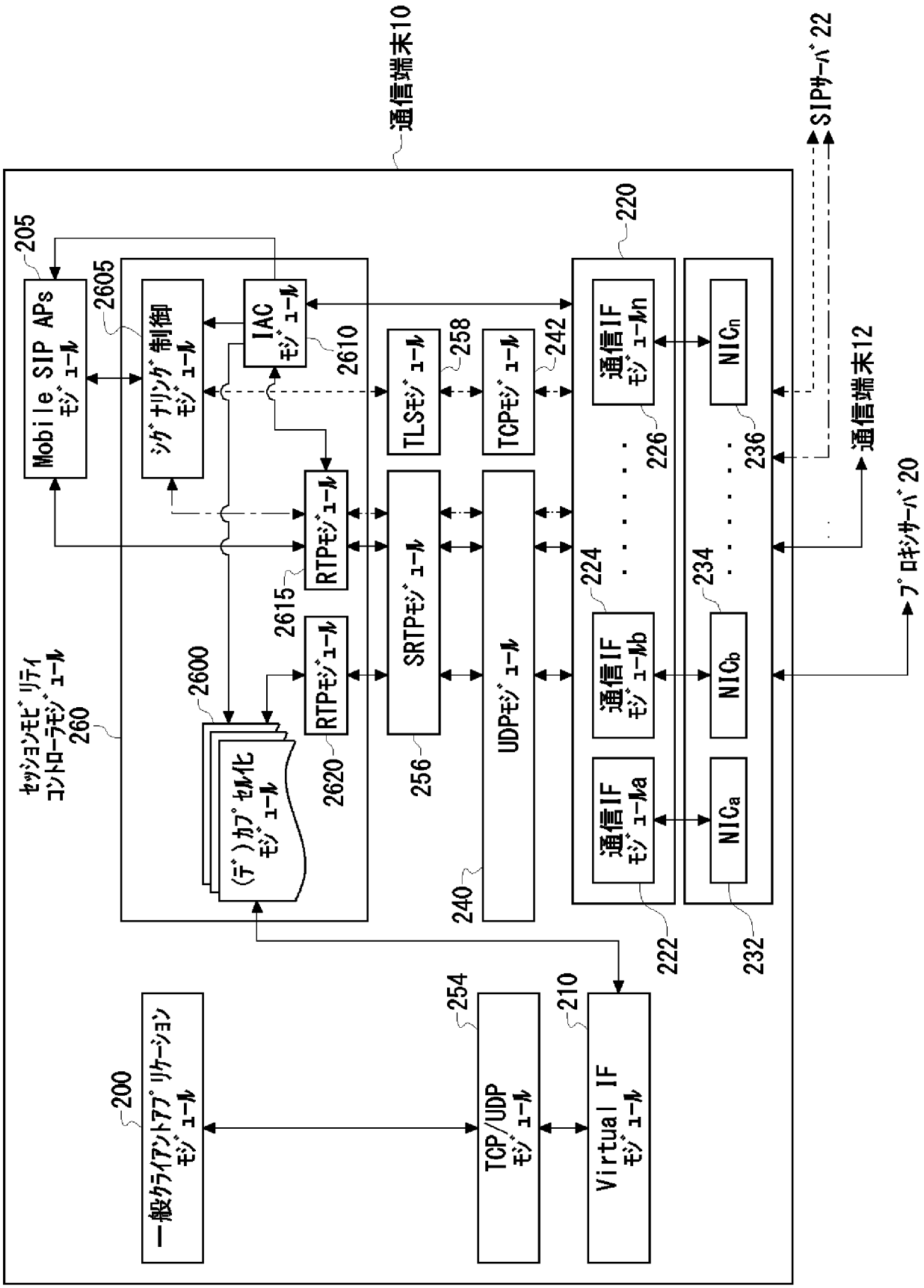
[図2]


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

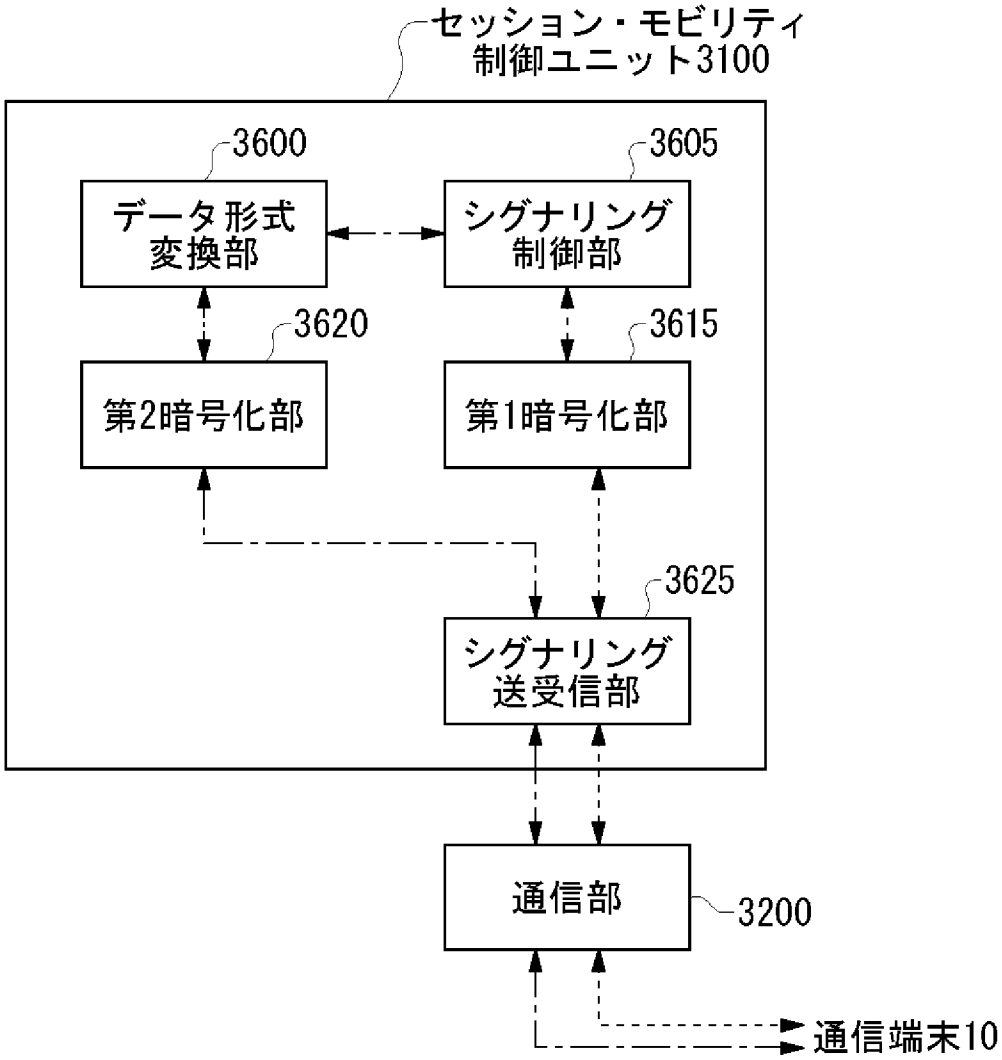
[図3]


通信モジュール14
一般アプリケーション部
100
仮想インターフェース部
110
リアルタイムアプリケーション部
105
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
1605
データ形式変換部
1600
(デ)カプセル化部
1610
変換テーブル記憶部
1640
第1暗号化部
1615
第2暗号化部
1620
シグナリング送受信部
1625
データ送受信部
1645
アドレス取得部
150
通信IF選択部
140
第1通信部
122
第2通信部
124
第n通信部
126

[図4]

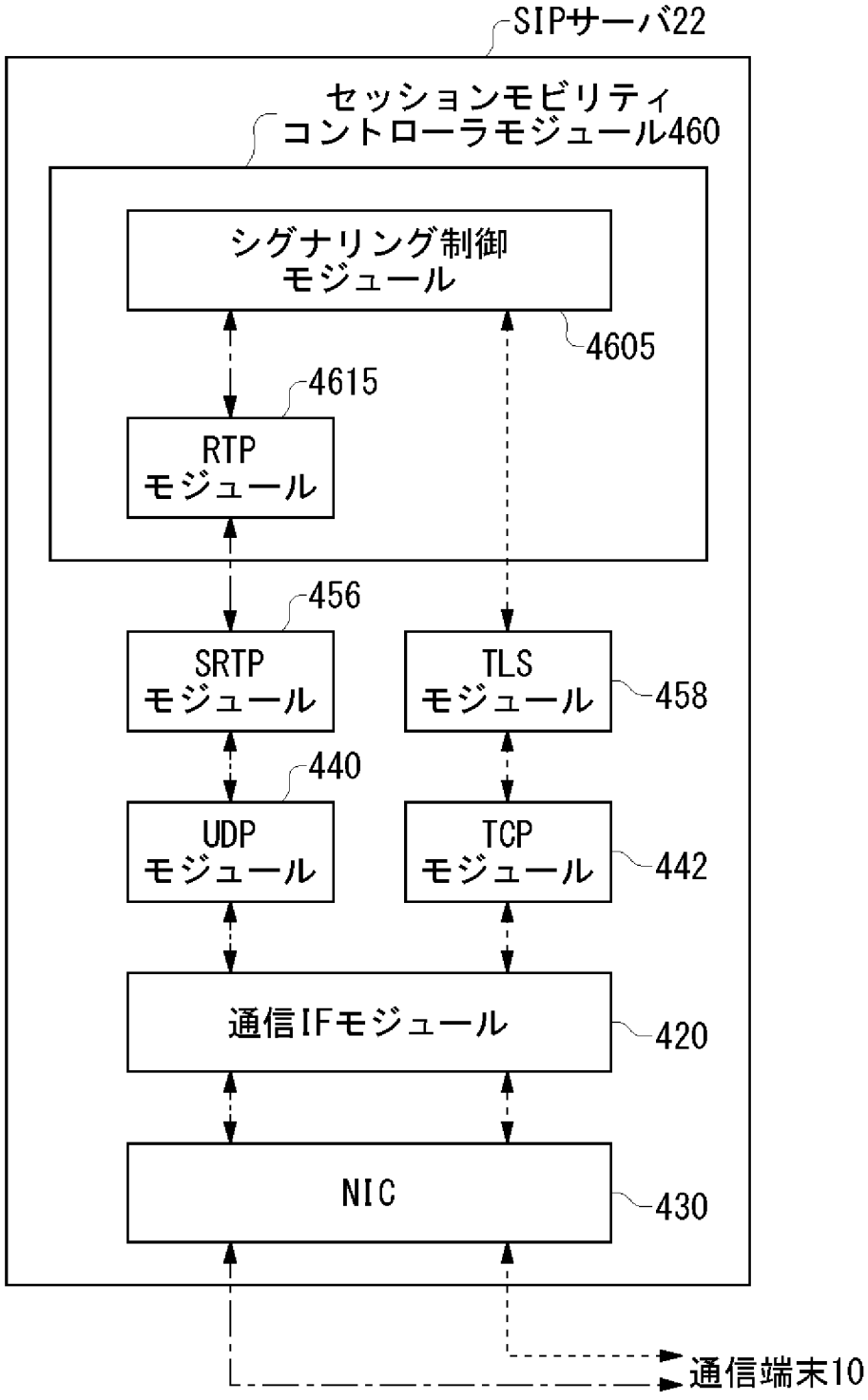

通信端末10
SIPサーバ22
プロキシサーバ20
通信端末12
205
Mobile SIP APs モジュール
2605
シグナリング制御 モジュール
IAC モジュール
2610
TLSモジュール
258
TCPモジュール
242
220
通信IF モジュールn
NICn
226
236
RTPモジュール
2615
RTPモジュール
2620
SRTPモジュール
256
UDPモジュール
240
224
234
通信IF モジュールb
NICb
通信IF モジュールa
NICa
222
232
セッションモビリティ コントローラモジュール 260
2600
(デ)カプセル化 モジュール
200
一般クライアントアプリケーション モジュール
254
TCP/UDP モジュール
210
Virtual IF モジュール

[図5]

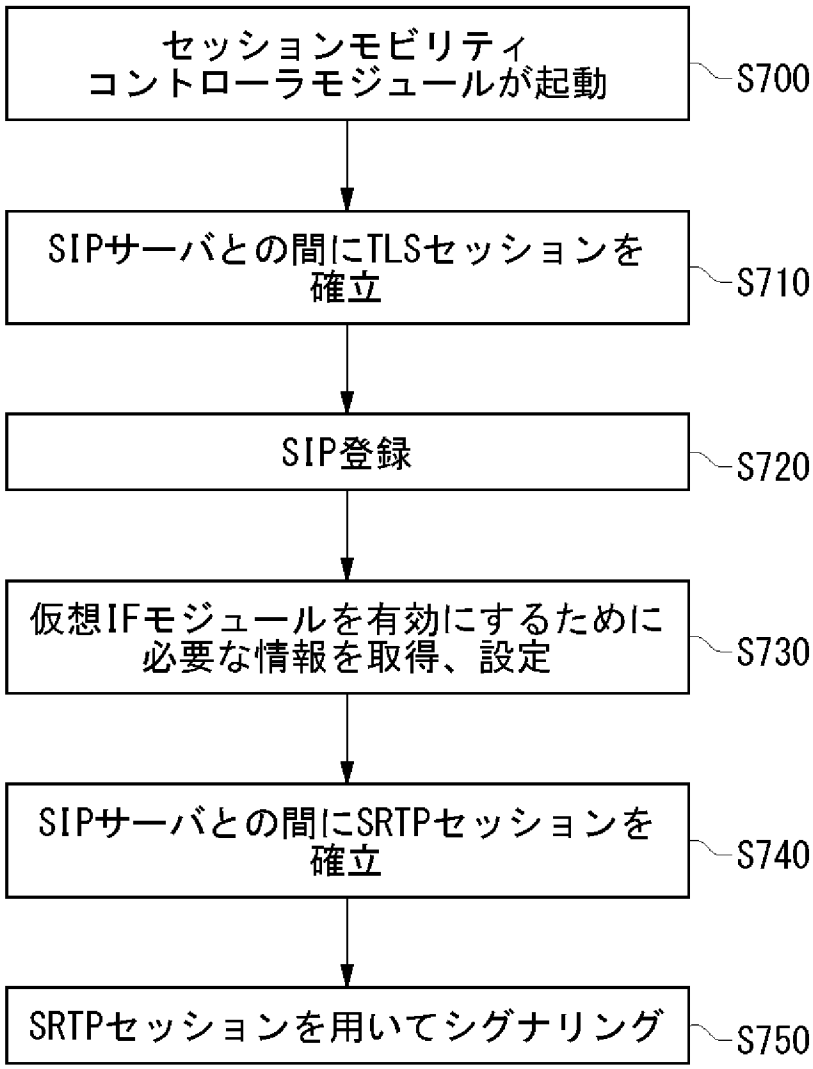


通信モジュール300

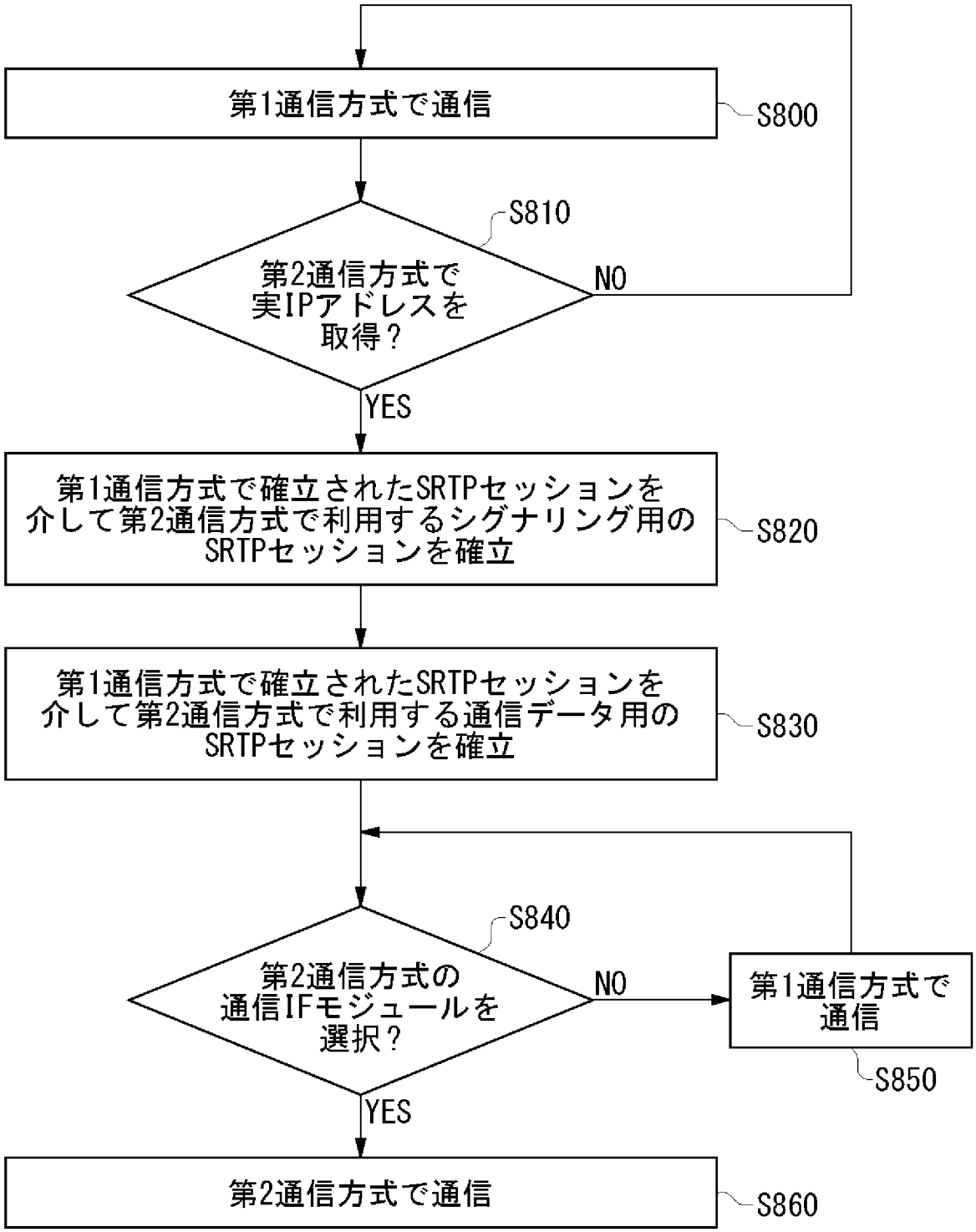
[図6]


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

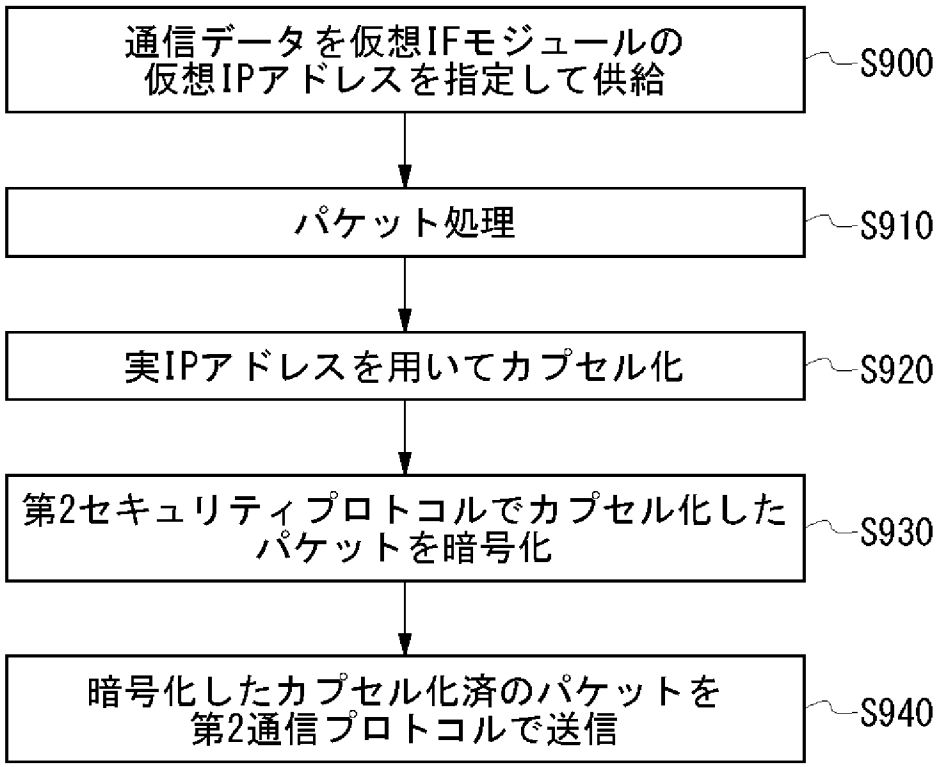
[図7]


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

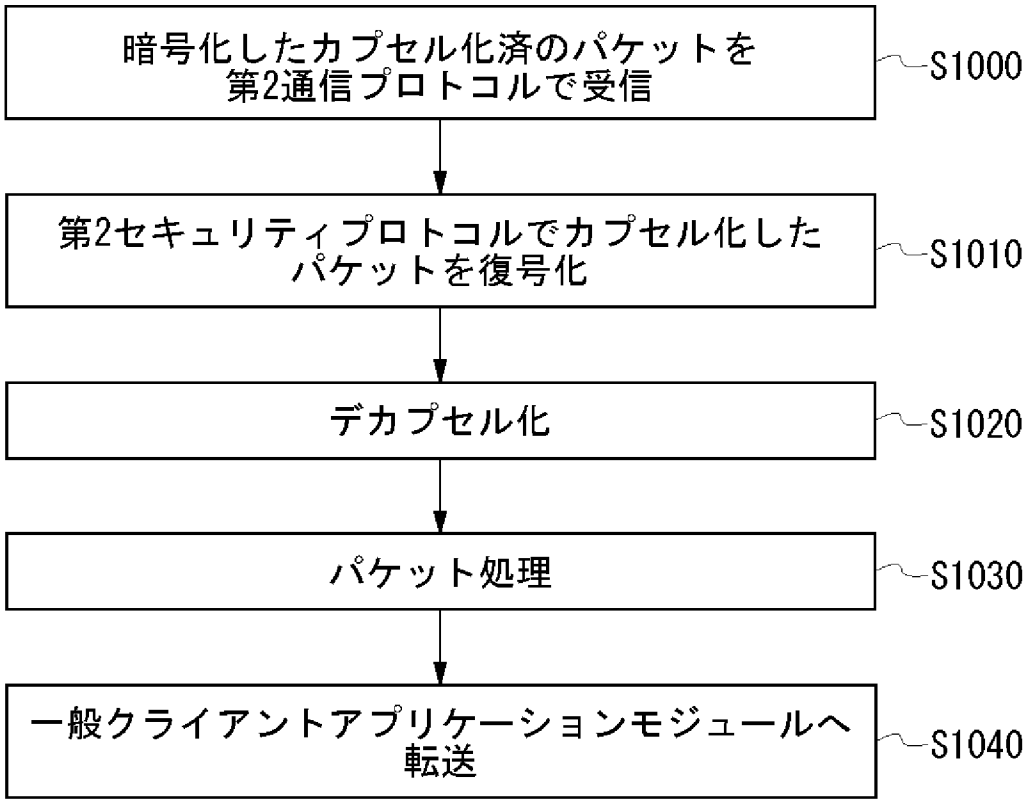
[図8]


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

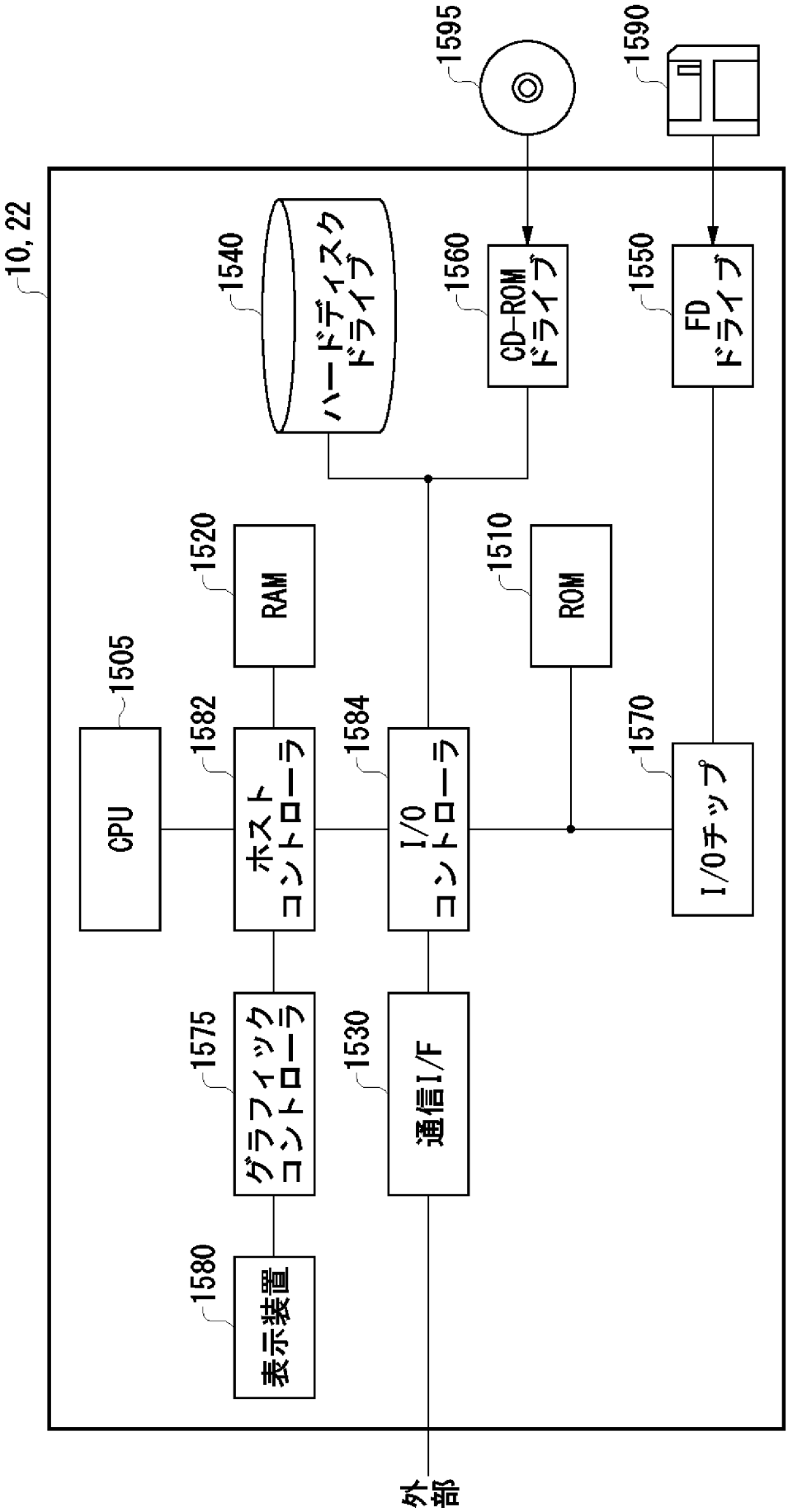
[図9]


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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/063538

A. CLASSIFICATION OF SUBJECT MATTER
H04Q7/38(2006.01)i, *H04L12/66*(2006.01)i, *H04L29/06*(2006.01)i, *H04L29/08*(2006.01)i, *H04Q7/32*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04B7/24-7/26, H04Q7/00-7/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2008
Kokai Jitsuyo Shinan Koho 1971-2008 Toroku Jitsuyo Shinan Koho 1994-2008

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	Cisco CallManager Version 4.0, 2004, full text, [retrieval date:08 September, 2008 (08.09.08)], Internet <URL:http://www.cisco.com/web/JP/product/hs/iptel/callmgr/prodlit/cm4ds_ds.html>	1-8,11-15 9,10
X	Ken'ichi TAKEBE, "IP Denwa no Tocho Boshi Kino, Jitsuyo Dankai e", Nikkei Communications, 01 December, 2004 (01.12.04), No.427, pages 88 to 89	1-8,11-15
Y A	JP 2003-9224 A (Toshiba Corp.), 10 January, 2003 (10.01.03), Fig. 4 (Family: none)	9,10 1-8,11-15

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 September, 2008 (08.09.08)	16 September, 2008 (16.09.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/063538

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-514337 A (Citrix Systems, Inc.), 31 May, 2007 (31.05.07), Full text & WO 2005/036857 A1	1-15

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０６３５３８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04Q7/38(2006.01)i, H04L12/66(2006.01)i, H04L29/06(2006.01)i, H04L29/08(2006.01)i, H04Q7/32(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04B7/24-7/26, H04Q7/00-7/38

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００８年
日本国実用新案登録公報	１９９６－２００８年
日本国登録実用新案公報	１９９４－２００８年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	Cisco CallManager バージョン４．０，2004，全文，［検索日：２００８．０９．０８］、インターネット<URL:http://www.cisco.com/web/JP/product/hs/iptel/callmgr/prodlit/cm4ds_ds.html>	1-8，11-15 9，10
X	武部健一，ＩＰ電話の盗聴防止機能、実用段階へ，日経コミュニケーションズ，2004.12.01，第４２７号，８８－８９頁	1-8，11-15

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０８．０９．２００８	１６．０９．２００８

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｊ	４０５７
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	倉本　敦史 電話番号　０３－３５８１－１１０１　内線　３５３４		

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2003-9224 A (株式会社東芝) 2003.01.10, 図４	9, 10
A	(ファミリーなし)	1-8, 11-15
A	JP 2007-514337 A (サイトリックス　システムズ, インコーポレイテッド) 2007.05.31, 全文 & WO 2005/036857 A1	1-15