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

特許第4334531号
(P4334531)

(45)発行日　平成21年9月30日(2009.9.30)　(24)登録日　平成21年7月3日(2009.7.3)

(51)Int.Cl.		F I		
H04L 12/56	(2006.01)	H04L	12/56	A
H04W 12/00	(2009.01)	H04Q	7/00	180
H04W 92/10	(2009.01)	H04Q	7/00	686
H04M 3/00	(2006.01)	H04M	3/00	A
H04L 12/22	(2006.01)	H04L	12/22	

請求項の数 13　(全 27 頁)　最終頁に続く

(21)出願番号　特願2005-318917(P2005-318917)
(22)出願日　平成17年11月1日(2005.11.1)
(65)公開番号　特開2007-129371(P2007-129371A)
(43)公開日　平成19年5月24日(2007.5.24)
審査請求日　平成20年10月24日(2008.10.24)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100083806
弁理士　三好　秀和
(74)代理人　100100712
弁理士　岩▲崎▼　幸邦
(74)代理人　100095500
弁理士　伊藤　正和
(74)代理人　100101247
弁理士　高橋　俊一
(74)代理人　100117064
弁理士　伊藤　市太郎

最終頁に続く

(54)【発明の名称】通信システム、移動局、交換機及び通信方法

(57)【特許請求の範囲】

【請求項１】

移動局と無線アクセスシステムに配置されたアクセスポイントとの間でセキュリティが確保された第１のコネクションを確立する通信システムであって、

前記移動局と、前記無線アクセスシステムに接続された交換機との間に、セキュリティが確保された第２のコネクションを確立するか否かを、前記無線アクセスシステムを管理する装置を一意に識別する無線アクセスシステム側識別子と、前記交換機を管理する装置を一意に識別する交換機側識別子とを用いて判断する判断部を備えることを特徴とする通信システム。

【請求項２】

前記判断部は、前記アクセスポイントから受信した前記無線アクセスシステム側識別子と、前記交換機から受信した前記交換機側識別子とを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする請求項１に記載の通信システム。

【請求項３】

前記アクセスポイントから受信した前記無線アクセスシステム側識別子と、前記交換機側識別子との組み合わせである識別子リストを保持する識別子リスト保持部を更に備え、

前記判断部は、前記アクセスポイントから受信した前記無線アクセスシステム側識別子と、前記交換機から受信した前記交換機側識別子と、前記識別子リストとを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする請求項１に記載の通信システム。

【請求項４】
前記移動局内に、前記交換機側識別子を予め保持する識別子保持部を更に備え、
前記判断部は、前記識別子保持部に保持された前記交換機側識別子と、前記アクセスポイントから受信した前記無線アクセスシステム側識別子とを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする請求項１に記載の通信システム。
【請求項５】
前記無線アクセスシステムにおいて用いる、セキュリティが確保されている、あるいは、セキュリティが確保されていないアルゴリズムを、アルゴリズムリストとして保持するアルゴリズムリスト保持部を更に備え、
前記判断部は、前記アクセスポイントから受信した前記無線アクセスシステム側識別子と、前記交換機から受信した前記交換機側識別子とを比較し、かつ、前記無線アクセスシステムにおいて用いるアルゴリズムと前記アルゴリズムリストとを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする請求項１に記載の通信システム。
【請求項６】
前記交換機から受信した前記交換機側識別子と、前記交換機側識別子との組み合わせである識別子リストを保持する識別子リスト保持部と、
前記無線アクセスシステムにおいて用いる、セキュリティが確保されている、あるいは、セキュリティが確保されていないアルゴリズムを、アルゴリズムリストとして保持するアルゴリズムリスト保持部とを更に備え、
前記判断部は、前記アクセスポイントから受信した前記無線アクセスシステム側識別子と、前記交換機から受信した前記交換機側識別子と、前記識別子リストとを比較し、かつ、前記無線アクセスシステムにおいて用いるアルゴリズムと前記アルゴリズムリストとを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする請求項１に記載の通信システム。
【請求項７】
前記移動局内に、前記交換機側識別子を予め保持する識別子保持部と、
前記無線アクセスシステムにおいて用いる、セキュリティが確保されている、あるいは、セキュリティが確保されていないアルゴリズムを、アルゴリズムリストとして保持するアルゴリズムリスト保持部とを更に備え、
前記判断部は、前記識別子保持部に保持された前記交換機側識別子と、前記アクセスポイントから受信した前記無線アクセスシステム側識別子とを比較し、かつ、前記無線アクセスシステムにおいて用いるアルゴリズムと前記アルゴリズムリストとを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする請求項１に記載の通信システム。
【請求項８】
移動局と無線アクセスシステムに配置されたアクセスポイントとの間でセキュリティが確保された第１のコネクションを確立する通信システムであって、
前記移動局と、前記無線アクセスシステムに接続された交換機との間に、セキュリティが確保された第２のコネクションを確立するか否か判断する判断部と、
前記無線アクセスシステムが払い出すアドレスの範囲を示すアドレスリストを保持するアドレスリスト保持部とを備え、
前記判断部は、前記移動局から送信された前記移動局のアドレスと、前記アドレスリストとを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする通信システム。
【請求項９】
前記アクセスポイントが配置された無線アクセスシステムにおいて用いる、セキュリティが確保されている、あるいは、セキュリティが確保されていないアルゴリズムを、アルゴリズムリストとして保持するアルゴリズムリスト保持部を更に備え、

前記判断部は、前記移動局から送信された前記移動局のアドレスと、前記アドレスリストとを比較し、かつ、前記アクセスポイントが配置された無線アクセスシステムにおいて用いるアルゴリズムと前記アルゴリズムリストとを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする請求項８に記載の通信システム。

【請求項１０】

無線アクセスシステムに配置されたアクセスポイントとの間でセキュリティが確保された第１のコネクションを確立する移動局であって、

前記移動局と、前記無線アクセスシステムに接続された交換機との間に、セキュリティが確保された第２のコネクションを確立するか否かを、前記無線アクセスシステムを管理する装置を一意に識別する無線アクセスシステム側識別子と、前記交換機を管理する装置を一意に識別する交換機側識別子とを用いて判断する判断部を備えることを特徴とする移動局。

【請求項１１】

移動局と無線アクセスシステムに配置されたアクセスポイントとの間でセキュリティが確保された第１のコネクションを確立する通信システムにおいて、前記無線アクセスシステムに接続された交換機であって、

前記移動局と、前記交換機との間に、セキュリティが確保された第２のコネクションを確立するか否か判断する判断部と、

前記無線アクセスシステムが払い出すアドレスの範囲を示すアドレスリストを保持するアドレスリスト保持部とを備え、

前記判断部は、前記移動局から送信された前記移動局のアドレスと、前記アドレスリストとを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする交換機。

【請求項１２】

移動局と、無線アクセスシステムに配置されたアクセスポイントと、前記無線アクセスシステムに接続された交換機とを備える通信システムにおける通信方法であって、

前記移動局と前記アクセスポイントとの間でセキュリティが確保された第１のコネクションを確立するステップと、

前記移動局と、前記交換機との間に、セキュリティが確保された第２のコネクションを確立するか否かを、前記無線アクセスシステムを管理する装置を一意に識別する無線アクセスシステム側識別子と、前記交換機を管理する装置を一意に識別する交換機側識別子とを用いて判断するステップと

を含むことを特徴とする通信方法。

【請求項１３】

移動局と、無線アクセスシステムに配置されたアクセスポイントと、前記無線アクセスシステムに接続された交換機とを備える通信システムにおける通信方法であって、

前記移動局と前記アクセスポイントとの間でセキュリティが確保された第１のコネクションを確立するステップと、

前記移動局と、前記交換機との間に、セキュリティが確保された第２のコネクションを確立するか否か判断するステップと

を含み、

前記判断するステップでは、前記移動局から送信された前記移動局のアドレスと、前記無線アクセスシステムが払い出すアドレスの範囲を示すアドレスリストとを比較することにより、前記第２のコネクションを確立するか否か判断することを特徴とする通信方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、セキュリティが確保されたコネクションを確立する通信システム、移動局、交換機及び通信方法に関する。

【背景技術】

【０００２】
最近、無線ネットワークシステムにおいて、IMS(Internet Protocol Multimedia Subsystem)が注目されている。IMSとは、これまで固定網や移動体通信、放送などで行なわれていたサービスをIP化し、融合したマルチメディアサービスなどを実現するための規格である。
【０００３】
IMSは、モバイルオペレータ以外の事業者が運営することを可能とするため、アクセスネットワークとは完全に独立した基盤として設計されている。そのため、移動局と、IMS装置間で独自に暗号化機能を持たせることで、セキュアな通信を実現している。例えば、図２０に示すように、移動局１０と、無線アクセスシステムに配置されたアクセスポイント２０との間で、秘匿・Integrityを確保したコネクションが確立されている場合に、更に、移動局１０と、無線アクセスシステムに接続された交換機３０（ここでは、IMS装置）との間に、セキュアなコネクションを確立している。
【０００４】
このようなコネクションの張るための手順を、図２１を参照しながら説明する（例えば、非特許文献１参照。）。尚、図２１は、3GPPに則った手順である。
【０００５】
まず、移動局１０は、無線アクセスシステムに配置されたアクセスポイント２０と認証を行い、秘匿鍵、Integrity鍵を交換する（Ｓ９０１）。そして、無線区間で使う秘匿やIntegrityのアルゴリズムを保持する（Ｓ９０２）。ここで、移動局１０と無線アクセスシステムに配置されたアクセスポイント２０間で、セキュリティが確保されたコネクションが確立される。
【０００６】
次に、移動局１０は、交換機３０（ここでは、P-CSCF（Proxy Call Session Control Function）３０ａ）へ、ユーザＩＤ、認証要求、IPsecセキュリティアソシエーション等を送信し、ＳＩＰ登録を行う（Ｓ９０３）。次に、P-CSCF３０ａは、S-CSCF（Serving Call Session Control Function）３０ｂへ、ユーザＩＤ、認証要求等を送信し、ＳＩＰ登録を行い（Ｓ９０４）、S-CSCF３０ｂは、P-CSCF３０ａへ、乱数、秘匿鍵、Integrity鍵等を送信し、認証チャレンジを行う（Ｓ９０５）。次に、P-CSCF３０ａは、秘密鍵及びIntegrity鍵を保持する（Ｓ９０６）。次に、P-CSCF３０ａは、移動局１０へ、乱数、秘匿鍵、Integrity鍵等を送信し、認証チャレンジを行う（Ｓ９０７）。ここで、無線アクセスシステムに配置されたアクセスポイント２０と交換機３０間で、セキュリティが確保されたコネクションが確立される。
【０００７】
そして、移動局１０は、P-CSCF３０ａへ、ユーザＩＤ、チャレンジレスポンス、IPsec使用アルゴリズム等を送信し、ＳＩＰ登録を行い（Ｓ９０８）、P-CSCF３０ａは、S-CSCF３０ｂへ、ユーザＩＤ、チャレンジレスポンス、IPsec秘匿とIntegrityとが正当であること等を送信し、ＳＩＰ登録を行う（Ｓ９０９）。次に、S-CSCF３０ｂは、P-CSCF３０ａへ、認証が正当であることを送信し（Ｓ９１０）、P-CSCF３０ａは、移動局１０へ認証が正当であることを送信する（Ｓ９１１）。
【非特許文献１】3GPP TS33.203 V6.8.0
【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかしながら、モバイルオペレータは無線アクセスネットワーク上を暗号化することで、移動局と、無線アクセスシステム間のセキュリティを既に確保しているのが普通であり、又、無線アクセスシステムからIMS装置までの区間についても、物理的にセキュリティを確保しているのが普通である。そのため、無線アクセスシステムとアクセス先のIMS装置が同一オペレータ内で運営されている場合は、IMS装置が持つ暗号化機能は冗長となってしまうことになる。

【０００９】
更に、今後の無線ネットワークにおいては、IMSをベースにVoIP、Push to Talkなど多様なサービスを実現していくことが想定される。よって、可能な限りIMS装置へ接続する際の接続遅延短縮、及び移動局とネットワークの処理負荷を削減することは、サービス品質向上、リソース有効活用のためには重要な要素となる。
【００１０】
そこで、本発明は、上記の課題に鑑み、移動局とネットワークを接続する際の遅延短縮、及び移動局とネットワークの処理負荷削減を実現する、通信システム、移動局、交換機及び通信方法を提供することを目的とする。
【課題を解決するための手段】
【００１１】
上記目的を達成するため、本発明の第１の特徴は、移動局と無線アクセスシステムに配置されたアクセスポイントとの間でセキュリティが確保された第１のコネクションを確立する通信システムであって、移動局と、無線アクセスシステムに接続された交換機との間に、セキュリティが確保された第２のコネクションを確立するか否か判断する判断部を備える通信システムであること要旨とする。
【００１２】
第１の特徴に係る通信システムによると、移動局とネットワークを接続する際の遅延短縮、及び移動局とネットワークの処理負荷削減を実現することができる。
【００１３】
又、第１の特徴に係る通信システムにおける判断部は、アクセスポイントから受信した無線アクセスシステムを管理する装置を一意に識別する識別子と、交換機から受信した交換機を管理する装置を一意に識別する識別子とを比較することにより、第２のコネクションを確立するか否か判断してもよい。
【００１４】
又、第１の特徴に係る通信システムは、アクセスポイントから受信した無線アクセスシステムを管理する装置を一意に識別する識別子と、交換機を管理する装置を一意に識別する識別子との組み合わせである識別子リストを保持する識別子リスト保持部を更に備え、判断部は、アクセスポイントから受信した無線アクセスシステムを管理する装置を一意に識別する識別子と、交換機から受信した交換機を管理する装置を一意に識別する識別子と、識別子リストとを比較することにより、第２のコネクションを確立するか否か判断してもよい。
【００１５】
又、第１の特徴に係る通信システムは、移動局内に、交換機を管理する装置を一意に識別する識別子を保持する識別子保持部を更に備え、判断部は、識別子保持部に保持された識別子と、アクセスポイントから受信した無線アクセスシステムを管理する装置を一意に識別する識別子とを比較することにより、第２のコネクションを確立するか否か判断してもよい。
【００１６】
又、第１の特徴に係る通信システムは、無線アクセスシステムにおいて用いる、セキュリティが確保されている、あるいは、セキュリティが確保されていないアルゴリズムを、アルゴリズムリストとして保持するアルゴリズムリスト保持部を更に備え、判断部は、アクセスポイントから受信した無線アクセスシステムを管理する装置を一意に識別する識別子と、交換機から受信した交換機を管理する装置を一意に識別する識別子とを比較し、かつ、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、第２のコネクションを確立するか否か判断してもよい。
【００１７】
又、第１の特徴に係る通信システムは、交換機から受信した交換機を管理する装置を一意に識別する識別子と、交換機を管理する装置を一意に識別する識別子との組み合わせである識別子リストを保持する識別子リスト保持部と、無線アクセスシステムにおいて用い

る、セキュリティが確保されている、あるいは、セキュリティが確保されていないアルゴリズムを、アルゴリズムリストとして保持するアルゴリズムリスト保持部とを更に備え、判断部は、アクセスポイントから受信した無線アクセスシステムを管理する装置を一意に識別する識別子と、交換機から受信した交換機を管理する装置を一意に識別する識別子と、識別子リストとを比較し、かつ、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、第２のコネクションを確立するか否か判断してもよい。

【００１８】

又、第１の特徴に係る通信システムは、移動局内に、交換機を管理する装置を一意に識別する識別子を保持する識別子保持部と、無線アクセスシステムにおいて用いる、セキュリティが確保されている、あるいは、セキュリティが確保されていないアルゴリズムを、アルゴリズムリストとして保持するアルゴリズムリスト保持部とを更に備え、判断部は、識別子保持部に保持された識別子と、アクセスポイントから受信した無線アクセスシステムを管理する装置を一意に識別する識別子とを比較し、かつ、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、第２のコネクションを確立するか否か判断してもよい。

【００１９】

又、第１の特徴に係る通信システムは、交換機が配置された無線アクセスシステムが払い出すアドレスの範囲を示すアドレスリストを保持するアドレスリスト保持部を更に備え、判断部は、移動局から送信された移動局のアドレスと、アドレスリストとを比較することにより、第２のコネクションを確立するか否か判断してもよい。

【００２０】

又、第１の特徴に係る通信システムは、交換機が配置された無線アクセスシステムが払い出すアドレスの範囲を示すアドレスリストを保持するアドレスリスト保持部と、アクセスポイントが配置された無線アクセスシステムにおいて用いる、セキュリティが確保されている、あるいは、セキュリティが確保されていないアルゴリズムを、アルゴリズムリストとして保持するアルゴリズムリスト保持部とを更に備え、判断部は、移動局から送信された移動局のアドレスと、アドレスリストとを比較し、かつ、アクセスポイントが配置された無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、第２のコネクションを確立するか否か判断してもよい。

【００２１】

本発明の第２の特徴は、無線アクセスシステムに配置されたアクセスポイントとの間でセキュリティが確保された第１のコネクションを確立する移動局であって、移動局と、無線アクセスシステムに接続された交換機との間に、セキュリティが確保された第２のコネクションを確立するか否か判断する判断部を備える移動局であることを要旨とする。

【００２２】

第２の特徴に係る移動局によると、移動局とネットワークを接続する際の遅延短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【００２３】

本発明の第３の特徴は、移動局と無線アクセスシステムに配置されたアクセスポイントとの間でセキュリティが確保された第１のコネクションを確立する通信システムにおいて、無線アクセスシステムに接続された交換機であって、移動局と、交換機との間に、セキュリティが確保された第２のコネクションを確立するか否か判断する判断部を備える交換機であることを要旨とする。

【００２４】

第３の特徴に係る交換機によると、移動局とネットワークを接続する際の遅延短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【００２５】

本発明の第４の特徴は、移動局と、無線アクセスシステムに配置されたアクセスポイントと、無線アクセスシステムに接続された交換機とを備える通信システムにおける通信方

法であって、移動局とアクセスポイントとの間でセキュリティが確保された第１のコネクションを確立するステップと、移動局と、交換機との間に、セキュリティが確保された第２のコネクションを確立するか否か判断するステップとを含む通信方法であることを要旨とする。

【００２６】

第４の特徴に係る通信方法によると、移動局とネットワークを接続する際の遅延短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【発明の効果】

【００２７】

本発明によると、移動局とネットワークを接続する際の遅延短縮、及び移動局とネットワークの処理負荷削減を実現する、通信システム、移動局、交換機及び通信方法を提供することができる。

【発明を実施するための最良の形態】

【００２８】

次に、図面を参照して、本発明の実施の形態を説明する。以下の図面の記載において、同一又は類似の部分には、同一又は類似の符号を付している。ただし、図面は模式的なものであることに留意すべきである。

【００２９】

本発明の実施の形態では、移動局もしくは交換機（IMS装置）が、既に移動局と交換機（IMS装置）間の通信路で、セキュリティが確保されていることを検知し、IMSの暗号化処理をスキップすることについて説明する。

【００３０】

＜第１の実施の形態＞

第１の実施の形態では、移動局が利用する無線アクセスシステムのオペレータ装置とIMS装置のオペレータ装置とが同一であることを、移動局が検知する場合について説明する。

【００３１】

（通信システム）

第１の実施の形態に係る通信システムは、図１に示すように、移動局１０と、無線アクセスシステムに配置されたアクセスポイント２０（例えば、基地局）と、無線アクセスシステムに接続された交換機３０（例えば、IMS装置）とを備える。この通信システムでは、移動局１０とアクセスポイント２０との間でセキュリティ（秘匿・Integrity）が確保されたコネクションが確立されているとする。

【００３２】

アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持する。又、交換機３０は、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）を保持する。

【００３３】

移動局は、図１に示すように、通信部１１と、認証部１２と、判断部１３と、登録部１４と、データ保持部１５とを備える。

【００３４】

通信部１１は、アクセスポイント２０や交換機３０との通信を行い、秘匿鍵や各種信号の送受信を行う。

【００３５】

認証部１２は、移動局１０と、アクセスポイント２０や交換機３０間の認証を行う。

【００３６】

判断部１３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。具体的には、判断部１３は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）と、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）とを比較することによ

り、コネクションを確立するか否か判断する。

【００３７】

登録部１４は、交換機３０に対してＳＩＰ登録を行う。

【００３８】

データ保持部１５は、受信した、秘匿鍵やIntegrity鍵、オペレータ識別子、通信途中のデータなどを保持する。

【００３９】

（通信方法）

次に、第１の実施の形態に係る通信方法について、図２を用いて説明する。

【００４０】

まず、アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持し（Ｓ１０１）、交換機３０（例えば、P-CSCF３０ａ）は、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）を保持する（Ｓ１０２）。

【００４１】

次に、移動局１０は、無線アクセスシステムに配置されたアクセスポイント２０と認証を行い、秘匿鍵、Integrity鍵を交換する（Ｓ１０３）。このとき、アクセスポイント２０は、移動局１０へオペレータ識別子Ａを送信し、移動局１０は、オペレータ識別子Ａを保持する。

【００４２】

次に、移動局１０は、無線区間で使う秘匿やIntegrityのアルゴリズムを保持する（Ｓ１０４）。ここで、移動局１０と無線アクセスシステムに配置されたアクセスポイント２０間で、セキュリティが確保されたコネクションが確立される。

【００４３】

次に、移動局１０は、P-CSCF３０ａへ、オペレータ識別子要求を送信し（Ｓ１０５）、P-CSCF３０ａは、移動局１０へオペレータ識別子Ｂを含むオペレータ識別子応答を送信する（Ｓ１０６）。そして、移動局１０は、オペレータ識別子Ａと、オペレータ識別子Ｂとを比較することにより、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する（Ｓ１０７）。ここで、オペレータ識別子Ａとオペレータ識別子Ｂとが同一である場合は、移動局１０は、無線アクセスシステムを管理する装置と、交換機３０を管理する装置が同一であると判断し、セキュリティが確保されたコネクションを確立する必要が無いと判断する。尚、以下の処理は、コネクションが不要であると判断した場合の処理であり、コネクションが必要である場合は、従来の手順と同様に、コネクションが確立される。

【００４４】

そして、移動局１０は、P-CSCF３０ａへ、ユーザＩＤ、認証要求、IPsec不要通知等を送信し、ＳＩＰ登録を行う（Ｓ１０８）。次に、P-CSCF３０ａは、S-CSCF３０ｂへ、ユーザＩＤ、認証要求等を送信し、ＳＩＰ登録を行い（Ｓ１０９）、S-CSCF３０ｂは、P-CSCF３０ａへ、乱数、秘匿鍵、Integrity鍵等を送信し、認証チャレンジを行う（Ｓ１１０）。次に、P-CSCF３０ａは、秘密鍵及びIntegrity鍵を保持する（Ｓ１１１）。

【００４５】

次に、P-CSCF３０ａは、移動局１０へ、乱数、IPsec不要受付応答等を送信し、認証チャレンジを行う（Ｓ１１２）。そして、移動局１０は、P-CSCF３０ａへ、ユーザＩＤ、チャレンジレスポンス等を送信し、ＳＩＰ登録を行い（Ｓ１１３）、P-CSCF３０ａは、S-CSCF３０ｂへ、ユーザＩＤ、チャレンジレスポンス、IPsec秘匿とIntegrityとが正当であること等を送信し、ＳＩＰ登録を行う（Ｓ１１４）。次に、S-CSCF３０ｂは、P-CSCF３０ａへ、認証が正当であることを送信し（Ｓ１１５）、P-CSCF３０ａは、移動局１０へ認証が正当であることを送信する（Ｓ１１６）。

【００４６】

（作用及び効果）

第１の実施の形態に係る通信システム、移動局１０及び通信方法によると、移動局１０が、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）と、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）とを比較することにより、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。オペレータ識別子Ａとオペレータ識別子Ｂが同一である場合は、既に無線アクセスシステムに配置されたアクセスポイント２０と交換機３０間で、セキュリティが確保されたコネクションが確立されているため、新たにコネクションを確立することは不要であると判断する。

【００４７】

このため、第１の実施の形態に係る通信システム、移動局１０及び通信方法によると、IMSの暗号化処理をスキップすることができ、無駄な暗号化処理を行わないことによる接続遅延の短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【００４８】

＜第２の実施の形態＞

第１の実施の形態では、移動局１０が、アクセスポイント２０が保持するオペレータ識別子と、交換機３０が保持するオペレータ識別子とを比較したが、第２の実施の形態では、移動局１０が保持するオペレータ識別子リストを用いて比較することにより、コネクションの確立の有無を判断する場合について説明する。

【００４９】

（通信システム）

第２の実施の形態に係る通信システムは、図３に示すように、移動局１０と、無線アクセスシステムに配置されたアクセスポイント２０（例えば、基地局）と、無線アクセスシステムに接続された交換機３０（例えば、IMS装置）とを備える。この通信システムでは、移動局１０とアクセスポイント２０との間でセキュリティ（秘匿・Integrity）が確保されたコネクションが確立されているとする。

【００５０】

アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持する。又、交換機３０は、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）を保持する。

【００５１】

移動局は、図１に示すように、通信部１１と、認証部１２と、判断部１３と、登録部１４と、データ保持部１５と、識別子リスト保持部１６とを備える。

【００５２】

識別子リスト保持部１６は、図４に示すように、セキュリティが確保されている、あるいは、セキュリティが確保されていない、無線アクセスシステムを管理する装置を一意に識別する識別子と、交換機３０を管理する装置を一意に識別する識別子との組み合わせである識別子リストを保持する。ここで、セキュリティが確保されているとは、通信を行う両方の装置（アクセスポイント２０、交換機３０）及び、両方の装置を結ぶ伝送路が物理的にセキュアであることを指す。

【００５３】

又、オペレータ識別子リストは、図４に示すように、無線アクセスシステム（アクセスポイント２０）のオペレータ識別子（例えば、operatorY）と、交換機３０のオペレータ識別子（例えば、operatorX）とが同一でなくても、セキュリティが確保されており、新たなセキュリティコネクション（IPsec）が不要であると設定することもできる。

【００５４】

判断部１３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。具体的には、判断部１３は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）と、交換機３０を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）と、識別子リストとを比較することにより、コネクションを確立するか否か判断する。

【００５５】
通信部１１、認証部１２、登録部１４、データ保持部１５については、第１の実施の形態と同様であるので、ここでは説明を省略する。
【００５６】
（通信方法）
次に、第２の実施の形態に係る通信方法について、図５を用いて説明する。
【００５７】
まず、移動局１０は、オペレータ識別子リストを保持し（Ｓ２０１）、アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持し（Ｓ２０２）、交換機３０（例えば、P-CSCF３０ａ）は、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）を保持する（Ｓ２０３）。
【００５８】
次に、移動局１０は、無線アクセスシステムに配置されたアクセスポイント２０と認証を行い、秘匿鍵、Integrity鍵を交換する（Ｓ２０４）。このとき、アクセスポイント２０は、移動局１０へオペレータ識別子Ａを送信し、移動局１０は、オペレータ識別子Ａを保持する。
【００５９】
次に、移動局１０は、無線区間で使う秘匿やIntegrityのアルゴリズムを保持する（Ｓ２０５）。ここで、移動局１０と無線アクセスシステムに配置されたアクセスポイント２０間で、セキュリティが確保されたコネクションが確立される。
【００６０】
次に、移動局１０は、P-CSCF３０ａへ、オペレータ識別子要求を送信し（Ｓ２０６）、P-CSCF３０ａは、移動局１０へオペレータ識別子Ｂを含むオペレータ識別子応答を送信する（Ｓ２０７）。そして、移動局１０は、オペレータ識別子Ａと、オペレータ識別子Ｂと、オペレータ識別子リストを比較することにより、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する（Ｓ２０８）。ここで、例えば、図４に示す識別子リストを参照し、オペレータ識別子Ａが、operatorYであり、とオペレータ識別子Ｂが、operatorXである場合は、セキュリティが確保されており、新たなセキュリティコネクション（IPsec）が不要であると判断する。尚、以下の処理は、コネクションが不要であると判断した場合の処理であり、コネクションが必要である場合は、従来の手順と同様に、コネクションが確立される。
【００６１】
又、ステップＳ２０９～Ｓ２１７の処理は、図２に示すステップＳ１０８～Ｓ１１６の処理と同様であるので、ここでは説明を省略する。
【００６２】
（作用及び効果）
第２の実施の形態に係る通信システム、移動局１０及び通信方法によると、移動局１０が、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）と、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）と、オペレータ識別子リスト（例えば、図４参照）を比較することにより、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。
【００６３】
このため、第２の実施の形態に係る通信システム、移動局１０及び通信方法によると、IMSの暗号化処理をスキップすることができ、無駄な暗号化処理を行わないことによる接続遅延の短縮、及び移動局とネットワークの処理負荷削減を実現することができる。
【００６４】
又、第２の実施の形態では、オペレータ識別子リストを任意に書き換えることが可能であり、コネクションの確立の有無を柔軟に判断することができる。
【００６５】

＜第３の実施の形態＞

第１の実施の形態では、移動局１０が、アクセスポイント２０が保持するオペレータ識別子と、交換機３０が保持するオペレータ識別子とを比較したが、第３の実施の形態では、移動局１０が交換機３０を管理する装置を一意に識別する識別子を保持し、この識別子とアクセスポイント２０が保持するオペレータ識別子とを比較することにより、コネクションの確立の有無を判断する場合について説明する。

【００６６】

（通信システム）

第３の実施の形態に係る通信システムは、図６に示すように、移動局１０と、無線アクセスシステムに配置されたアクセスポイント２０（例えば、基地局）と、無線アクセスシステムに接続された交換機３０（例えば、IMS装置）とを備える。この通信システムでは、移動局１０とアクセスポイント２０との間でセキュリティ（秘匿・Integrity）が確保されたコネクションが確立されているとする。

【００６７】

アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持する。

【００６８】

移動局は、図１に示すように、通信部１１と、認証部１２と、判断部１３と、登録部１４と、データ保持部１５と、識別子保持部１７とを備える。

【００６９】

識別子保持部１７は、交換機３０を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｃ）を保持する。

【００７０】

判断部１３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。具体的には、判断部１３は、識別子保持部１７に保持された識別子（例えば、オペレータ識別子Ｃ）と、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）とを比較することにより、コネクションを確立するか否か判断する。

【００７１】

通信部１１、認証部１２、登録部１４、データ保持部１５については、第１の実施の形態と同様であるので、ここでは説明を省略する。

【００７２】

（通信方法）

次に、第３の実施の形態に係る通信方法について、図７を用いて説明する。

【００７３】

まず、移動局１０は、交換機３０を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｃ）を保持し（Ｓ３０１）、アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持する（Ｓ３０２）。

【００７４】

次に、移動局１０は、無線アクセスシステムに配置されたアクセスポイント２０と認証を行い、秘匿鍵、Integrity鍵を交換する（Ｓ３０３）。このとき、アクセスポイント２０は、移動局１０へオペレータ識別子Ａを送信し、移動局１０は、オペレータ識別子Ａを保持する。

【００７５】

次に、移動局１０は、無線区間で使う秘匿やIntegrityのアルゴリズムを保持する（Ｓ３０４）。ここで、移動局１０と無線アクセスシステムに配置されたアクセスポイント２０間で、セキュリティが確保されたコネクションが確立される。

【００７６】

次に、移動局１０は、オペレータ識別子Ｃと、オペレータ識別子Ａとを比較することに

より、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する（Ｓ３０５）。ここで、オペレータ識別子Ｃとオペレータ識別子Ａとが同一である場合は、移動局１０は、無線アクセスシステムを管理する装置と、交換機３０を管理する装置が同一であると判断し、セキュリティが確保されたコネクションを確立する必要が無いと判断する。尚、以下の処理は、コネクションが不要であると判断した場合の処理であり、コネクションが必要である場合は、従来の手順と同様に、コネクションが確立される。

【００７７】

又、ステップＳ３０６～Ｓ３１４の処理は、図２に示すステップＳ１０８～Ｓ１１６の処理と同様であるので、ここでは説明を省略する。

【００７８】

（作用及び効果）

第３の実施の形態に係る通信システム、移動局１０及び通信方法によると、移動局１０が、移動局内に保持された交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｃ）と、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）とを比較することにより、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。

【００７９】

このため、第３の実施の形態に係る通信システム、移動局１０及び通信方法によると、IMSの暗号化処理をスキップすることができ、無駄な暗号化処理を行わないことによる接続遅延の短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【００８０】

又、第１の実施の形態に比較すると、第３の実施の形態では、交換機３０からオペレータ識別子を受信する必要がないため、更に、接続遅延の短縮や、移動局及び交換機の処理負荷軽減を実現することができる。

【００８１】

＜第４の実施の形態＞

第１の実施の形態では、移動局１０が、アクセスポイント２０が保持するオペレータ識別子と、交換機３０が保持するオペレータ識別子とを比較したが、第４の実施の形態では、これに加え、アルゴリズムリストを比較することにより、コネクションの確立の有無を判断する場合について説明する。

【００８２】

（通信システム）

第４の実施の形態に係る通信システムは、図８に示すように、移動局１０と、無線アクセスシステムに配置されたアクセスポイント２０（例えば、基地局）と、無線アクセスシステムに接続された交換機３０（例えば、IMS装置）とを備える。この通信システムでは、移動局１０とアクセスポイント２０との間でセキュリティ（秘匿・Integrity）が確保されたコネクションが確立されているとする。

【００８３】

アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持する。又、交換機３０は、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）を保持する。

【００８４】

移動局は、図１に示すように、通信部１１と、認証部１２と、判断部１３と、登録部１４と、データ保持部１５と、アルゴリズムリスト保持部１８とを備える。

【００８５】

アルゴリズムリスト保持部１８は、図９に示すように、無線アクセスシステムにおいて用いる、セキュリティが確保されている、あるいは、セキュリティが確保されていないアルゴリズムを、無線区間アルゴリズムリストとして保持する。図９では、例えば、無線区間において、秘匿アルゴリズムがAESであり、IntegrityアルゴリズムがSHA-1であると、

セキュリティが確保されており、新たなセキュリティコネクション（IPsec）が不要であると設定されている。

【００８６】

判断部１３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。具体的には、判断部１３は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）と、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）とを比較し、かつ、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、コネクションを確立するか否か判断する。

【００８７】

通信部１１、認証部１２、登録部１４、データ保持部１５については、第１の実施の形態と同様であるので、ここでは説明を省略する。

【００８８】

（通信方法）

次に、第４の実施の形態に係る通信方法について、図１０を用いて説明する。

【００８９】

まず、移動局１０は、無線区間アルゴリズムリストを保持し（Ｓ４０１）、アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持し（Ｓ４０２）、交換機３０は、交換機３０を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持する（Ｓ４０３）。

【００９０】

次に、移動局１０は、無線アクセスシステムに配置されたアクセスポイント２０と認証を行い、秘匿鍵、Integrity鍵を交換する（Ｓ４０４）。このとき、アクセスポイント２０は、移動局１０へオペレータ識別子Ａを送信し、移動局１０は、オペレータ識別子Ａを保持する。

【００９１】

次に、移動局１０は、無線区間で使う秘匿やIntegrityのアルゴリズムを保持する（Ｓ４０５）。ここで、移動局１０と無線アクセスシステムに配置されたアクセスポイント２０間で、セキュリティが確保されたコネクションが確立される。

【００９２】

次に、移動局１０は、P-CSCF３０ａへ、オペレータ識別子要求を送信し（Ｓ４０６）、P-CSCF３０ａは、移動局１０へオペレータ識別子Ｂを含むオペレータ識別子応答を送信する（Ｓ４０７）。そして、移動局１０は、オペレータ識別子Ａと、オペレータ識別子Ｂとを比較する（Ｓ４０８）。次に、移動局１０は、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較する（Ｓ４０９）。ここで、オペレータ識別子Ａとオペレータ識別子Ｂとが同一であり、かつ、アルゴリズムリストにおいて、無線アクセスシステムにおいて用いるアルゴリズムがIPsec不要であると設定されている場合は、移動局１０は、セキュリティが確保されたコネクションを確立する必要が無いと判断する。尚、以下の処理は、コネクションが不要であると判断した場合の処理であり、コネクションが必要である場合は、従来の手順と同様に、コネクションが確立される。

【００９３】

又、ステップＳ４１０～Ｓ４１８の処理は、図２に示すステップＳ１０８～Ｓ１１６の処理と同様であるので、ここでは説明を省略する。

【００９４】

（作用及び効果）

第４の実施の形態に係る通信システム、移動局１０及び通信方法によると、移動局１０が、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）と、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）とを比較することに加え、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、交換機３０との間に、セキュリティが確保さ

れたコネクションを確立するか否か判断する。

【００９５】

このため、第４の実施の形態に係る通信システム、移動局１０及び通信方法によると、IMSの暗号化処理をスキップすることができ、無駄な暗号化処理を行わないことによる接続遅延の短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【００９６】

又、第４の実施の形態では、無線区間におけるアルゴリズムを比較するため、強いセキュリティコネクションが張られている場合は、移動局１０と交換機３０間に新たなコネクションを張らないなど、より細かな制御が可能となる。

【００９７】

＜第５の実施の形態＞

第２の実施の形態では、移動局１０が、アクセスポイント２０が保持するオペレータ識別子と、交換機３０が保持するオペレータ識別子と、オペレータ識別子リストを比較したが、第５の実施の形態では、これに加え、アルゴリズムリストを比較することにより、コネクションの確立の有無を判断する場合について説明する。

【００９８】

（通信システム）

第５の実施の形態に係る通信システムは、図１１に示すように、移動局１０と、無線アクセスシステムに配置されたアクセスポイント２０（例えば、基地局）と、無線アクセスシステムに接続された交換機３０（例えば、IMS装置）とを備える。この通信システムでは、移動局１０とアクセスポイント２０との間でセキュリティ（秘匿・Integrity）が確保されたコネクションが確立されているとする。

【００９９】

アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持する。又、交換機３０は、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）を保持する。

【０１００】

移動局は、図１に示すように、通信部１１と、認証部１２と、判断部１３と、登録部１４と、データ保持部１５と、識別子リスト保持部１６と、アルゴリズムリスト保持部１８とを備える。

【０１０１】

判断部１３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。具体的には、判断部１３は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）と、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）と、識別子リストとを比較し、かつ、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、コネクションを確立するか否か判断する。

【０１０２】

識別子リスト保持部１６は、第２の実施の形態と同様であるので、ここでは説明を省略する。又、アルゴリズムリスト保持部１８は、第４の実施の形態と同様であるので、ここでは説明を省略する。

【０１０３】

通信部１１、認証部１２、登録部１４、データ保持部１５については、第１の実施の形態と同様であるので、ここでは説明を省略する。

【０１０４】

（通信方法）

次に、第５の実施の形態に係る通信方法について、図１２を用いて説明する。

【０１０５】

まず、移動局１０は、無線区間アルゴリズムリストを保持し（Ｓ５０１）、オペレータ識別子リスト（Ｓ５０２）を保持する。又、アクセスポイント２０は、無線アクセスシス

テムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持し（Ｓ５０３）、交換機３０は、交換機３０を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）を保持する（Ｓ５０４）。

【０１０６】

次に、移動局１０は、無線アクセスシステムに配置されたアクセスポイント２０と認証を行い、秘匿鍵、Integrity鍵を交換する（Ｓ５０５）。このとき、アクセスポイント２０は、移動局１０へオペレータ識別子Ａを送信し、移動局１０は、オペレータ識別子Ａを保持する。

【０１０７】

次に、移動局１０は、無線区間で使う秘匿やIntegrityのアルゴリズムを保持する（Ｓ５０６）。ここで、移動局１０と無線アクセスシステムに配置されたアクセスポイント２０間で、セキュリティが確保されたコネクションが確立される。

【０１０８】

次に、移動局１０は、P-CSCF３０ａへ、オペレータ識別子要求を送信し（Ｓ５０７）、P-CSCF３０ａは、移動局１０へオペレータ識別子Ｂを含むオペレータ識別子応答を送信する（Ｓ５０８）。そして、移動局１０は、オペレータ識別子Ａと、オペレータ識別子Ｂと、オペレータ識別子リストを比較する（Ｓ５０９）。次に、移動局１０は、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較する（Ｓ５１０）。ここで、オペレータ識別子Ａとオペレータ識別子Ｂとの組み合わせがオペレータ識別子リストにおいてIPsec不要であると設定されており、かつ、アルゴリズムリストにおいて、無線アクセスシステムにおいて用いるアルゴリズムがIPsec不要であると設定されている場合は、移動局１０は、セキュリティが確保されたコネクションを確立する必要が無いと判断する。尚、以下の処理は、コネクションが不要であると判断した場合の処理であり、コネクションが必要である場合は、従来の手順と同様に、コネクションが確立される。

【０１０９】

又、ステップＳ５１１～Ｓ５１９の処理は、図２に示すステップＳ１０８～Ｓ１１６の処理と同様であるので、ここでは説明を省略する。

【０１１０】

（作用及び効果）

第５の実施の形態に係る通信システム、移動局１０及び通信方法によると、移動局１０が、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）と、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｂ）と、オペレータ識別子リストを比較することに加え、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。

【０１１１】

このため、第５の実施の形態に係る通信システム、移動局１０及び通信方法によると、IMSの暗号化処理をスキップすることができ、無駄な暗号化処理を行わないことによる接続遅延の短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【０１１２】

又、第５の実施の形態では、オペレータ識別子リストを任意に書き換えることが可能であり、コネクションの確立の有無を柔軟に判断することができる。更に、無線区間におけるアルゴリズムを比較するため、強いセキュリティコネクションが張られている場合は、移動局１０と交換機３０間に新たなコネクションを張らないなど、より細かな制御が可能となる。

【０１１３】

＜第６の実施の形態＞

第３の実施の形態では、移動局１０が、交換機３０を管理する装置を一意に識別する識別子を保持し、この識別子と、交換機３０が保持するオペレータ識別子とを比較したが、第６の実施の形態では、これに加え、アルゴリズムリストを比較することにより、コネク

ションの確立の有無を判断する場合について説明する。

【０１１４】

（通信システム）

第６の実施の形態に係る通信システムは、図１３に示すように、移動局１０と、無線アクセスシステムに配置されたアクセスポイント２０（例えば、基地局）と、無線アクセスシステムに接続された交換機３０（例えば、IMS装置）とを備える。この通信システムでは、移動局１０とアクセスポイント２０との間でセキュリティ（秘匿・Integrity）が確保されたコネクションが確立されているとする。

【０１１５】

アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持する。

【０１１６】

移動局は、図１に示すように、通信部１１と、認証部１２と、判断部１３と、登録部１４と、データ保持部１５と、識別子保持部１７と、アルゴリズムリスト保持部１８とを備える。

【０１１７】

判断部１３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。具体的には、判断部１３は、識別子保持部１７に保持された識別子（例えば、オペレータ識別子Ｃ）と、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）とを比較し、かつ、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、コネクションを確立するか否か判断する。

【０１１８】

識別子保持部１７は、第３の実施の形態と同様であるので、ここでは説明を省略する。又、アルゴリズムリスト保持部１８は、第４の実施の形態と同様であるので、ここでは説明を省略する。

【０１１９】

通信部１１、認証部１２、登録部１４、データ保持部１５については、第１の実施の形態と同様であるので、ここでは説明を省略する。

【０１２０】

（通信方法）

次に、第６の実施の形態に係る通信方法について、図１４を用いて説明する。

【０１２１】

まず、移動局１０は、無線区間アルゴリズムリストを保持し（Ｓ６０１）、交換機３０を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｃ）を保持する（Ｓ６０２）。又、アクセスポイント２０は、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）を保持する（Ｓ６０３）。

【０１２２】

次に、移動局１０は、無線アクセスシステムに配置されたアクセスポイント２０と認証を行い、秘匿鍵、Integrity鍵を交換する（Ｓ６０４）。このとき、アクセスポイント２０は、移動局１０へオペレータ識別子Ａを送信し、移動局１０は、オペレータ識別子Ａを保持する。

【０１２３】

次に、移動局１０は、無線区間で使う秘匿やIntegrityのアルゴリズムを保持する（Ｓ６０５）。ここで、移動局１０と無線アクセスシステムに配置されたアクセスポイント２０間で、セキュリティが確保されたコネクションが確立される。

【０１２４】

次に、移動局１０は、オペレータ識別子Ｃと、オペレータ識別子Ａとを比較する（Ｓ６０６）。次に、移動局１０は、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較する（Ｓ６０７）。ここで、オペレータ識別子Ｃとオペレータ識

別子Ａとが同一であり、かつ、アルゴリズムリストにおいて、無線アクセスシステムにおいて用いるアルゴリズムがIPsec不要であると設定されている場合は、移動局１０は、セキュリティが確保されたコネクションを確立する必要が無いと判断する。尚、以下の処理は、コネクションが不要であると判断した場合の処理であり、コネクションが必要である場合は、従来の手順と同様に、コネクションが確立される。

【０１２５】

又、ステップＳ６０８～Ｓ６１６の処理は、図２に示すステップＳ１０８～Ｓ１１６の処理と同様であるので、ここでは説明を省略する。

【０１２６】

（作用及び効果）

第６の実施の形態に係る通信システム、移動局１０及び通信方法によると、移動局１０が、交換機を管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ｃ）と、無線アクセスシステムを管理する装置を一意に識別する識別子（例えば、オペレータ識別子Ａ）とを比較することに加え、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。

【０１２７】

このため、第６の実施の形態に係る通信システム、移動局１０及び通信方法によると、IMSの暗号化処理をスキップすることができ、無駄な暗号化処理を行わないことによる接続遅延の短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【０１２８】

又、第６の実施の形態では、交換機３０からオペレータ識別子を受信する必要がないため、更に、接続遅延の短縮や、移動局及び交換機の処理負荷軽減を実現することができる。更に、第６の実施の形態では、無線区間におけるアルゴリズムを比較するため、強いセキュリティコネクションが張られている場合は、移動局１０と交換機３０間に新たなコネクションを張らないなど、より細かな制御が可能となる。

【０１２９】

＜第７の実施の形態＞

第７の実施の形態では、交換機が、自網無線アクセスシステムが払い出すＩＰアドレスの範囲を保持しておき、移動局のＩＰアドレスと比較することにより、コネクションの確立の有無を判断する場合について説明する。

【０１３０】

（通信システム）

第７の実施の形態に係る通信システムは、図１５に示すように、移動局１０と、無線アクセスシステムに配置されたアクセスポイント２０（例えば、基地局）と、無線アクセスシステムに接続された交換機３０（例えば、IMS装置）とを備える。この通信システムでは、移動局１０とアクセスポイント２０との間でセキュリティ（秘匿・Integrity）が確保されたコネクションが確立されているとする。

【０１３１】

交換機３０は、図１５に示すように、通信部３１と、認証部３２と、判断部３３と、登録部３４と、データ保持部３５と、アドレスリスト保持部３６とを備える。

【０１３２】

通信部３１は、移動局１０との通信を行い、ＩＰアドレス、ユーザＩＤ、認証要求や各種信号の送受信を行う。

【０１３３】

認証部３２は、移動局１０と交換機３０間の認証を行う。

【０１３４】

判断部３３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。具体的には、移動局１０から送信された移動局１０のアドレスと、アドレスリスト保持部３６に保持されたアドレスリストとを比較することに

より、コネクションを確立するか否か判断する。

【０１３５】

登録部３４は、移動局１０に対してＳＩＰ登録を行う。

【０１３６】

データ保持部３５は、受信した、ＩＰアドレス、通信途中のデータなどを保持する。

【０１３７】

アドレスリスト保持部３６は、図１６に示すように、交換機３０が配置された無線アクセスシステムが払い出すＩＰアドレスの範囲を示すアドレスリストを保持する。

【０１３８】

（通信方法）

次に、第７の実施の形態に係る通信方法について、図１７を用いて説明する。交換機３０は、ＩＰアドレスリストを保持していることを前提とする。

【０１３９】

まず、移動局１０は、無線アクセスシステムに配置されたアクセスポイント２０と認証を行い、秘匿鍵、Integrity鍵を交換する（Ｓ７０１）。

【０１４０】

次に、移動局１０は、無線区間で使う秘匿やIntegrityのアルゴリズムを保持する（Ｓ７０２）。ここで、移動局１０と無線アクセスシステムに配置されたアクセスポイント２０間で、セキュリティが確保されたコネクションが確立される。

【０１４１】

そして、移動局１０は、P-CSCF３０ａへ、ユーザＩＤ、認証要求、IPsecセキュリティアソシエーション等を送信し、ＳＩＰ登録を行う（Ｓ７０３）。次に、P-CSCF３０ａは、判断部３３へ、移動局１０のＩＰアドレスを含むIPsec要否確認要求を送信する（Ｓ７０４）。

【０１４２】

次に、判断部３３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する（Ｓ７０５）。具体的には、判断部３３は、移動局１０から送信された移動局１０のアドレスと、アドレスリスト保持部３６に保持されたＩＰアドレスリストとを比較することにより、コネクションを確立するか否か判断する。例えば、判断部３３は、移動局１０から送信された移動局のＩＰアドレスは、図１６に示すＩＰアドレス範囲に該当する場合、自網無線アクセスシステムが払い出したＩＰアドレスであると判断し、セキュリティが確保されたコネクションを確立する必要が無いと判断する。

【０１４３】

そして、判断部３３は、P-CSCF３０ａへIPsec不要であることを通知する応答を送信する（Ｓ７０６）。尚、以下の処理は、コネクションが不要であると判断した場合の処理であり、コネクションが必要である場合は、従来の手順と同様に、コネクションが確立される。

【０１４４】

又、ステップＳ７０７～Ｓ７１４の処理は、図２に示すステップＳ１０９～Ｓ１１６の処理と同様であるので、ここでは説明を省略する。

【０１４５】

（作用及び効果）

第７の実施の形態に係る通信システム、交換機３０及び通信方法によると、交換機３０が、移動局１０のアドレスとアドレスリスト保持部３６に保持されたＩＰアドレスリストとを比較することにより、移動局１０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。移動局１０のアドレスが、アドレスリストに含まれている場合、既に移動局１０と交換機３０間で、セキュリティが確保されたコネクションが確立されているため、新たにコネクションを確立することは不要であると判断する。

【０１４６】

このため、第７の実施の形態に係る通信システム、交換機３０及び通信方法によると、IMSの暗号化処理をスキップすることができ、無駄な暗号化処理を行わないことによる接続遅延の短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【０１４７】

＜第８の実施の形態＞

第７の実施の形態では、交換機３０が、移動局１０のアドレスと、アドレスリストとを比較したが、第８の実施の形態では、これに加え、アルゴリズムリストを比較することにより、コネクションの確立の有無を判断する場合について説明する。

【０１４８】

（通信システム）

第８の実施の形態に係る通信システムは、図１８に示すように、移動局１０と、無線アクセスシステムに配置されたアクセスポイント２０（例えば、基地局）と、無線アクセスシステムに接続された交換機３０（例えば、IMS装置）とを備える。この通信システムでは、移動局１０とアクセスポイント２０との間でセキュリティ（秘匿・Integrity）が確保されたコネクションが確立されているとする。

【０１４９】

交換機３０は、図１８に示すように、通信部３１と、認証部３２と、判断部３３と、登録部３４と、データ保持部３５と、アドレスリスト保持部３６と、アルゴリズムリスト保持部３７とを備える。

【０１５０】

判断部３３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。具体的には、判断部３３は、移動局１０から送信された移動局１０のアドレスと、アドレスリストとを比較し、かつ、無線アクセスシステムにおいて用いるアルゴリズムとアルゴリズムリストとを比較することにより、コネクションを確立するか否か判断する。

【０１５１】

通信部３１、認証部３２、登録部３４、データ保持部３５、アドレスリスト保持部３６は、第７の実施の形態と同様であるので、ここでは説明を省略する。又、アルゴリズムリスト保持部３７は、第４の実施の形態と同様であるので、ここでは説明を省略する。

【０１５２】

（通信方法）

次に、第８の実施の形態に係る通信方法について、図１９を用いて説明する。交換機３０は、ＩＰアドレスリスト及び無線区間アルゴリズムリストを保持していることを前提とする。

【０１５３】

まず、ステップＳ８０１～８０４の処理は、図１７に示すステップＳ７０１～Ｓ７０４の処理と同様であるので、ここでは説明を省略する。

【０１５４】

判断部３３は、移動局１０と、交換機３０との間に、セキュリティが確保されたコネクションを確立するか否か判断する（Ｓ８０５及びＳ８０６）。具体的には、判断部３３は、移動局１０から送信された移動局１０のアドレスと、アドレスリスト保持部３６に保持されたＩＰアドレスリストとを比較する（Ｓ８０５）。次に、判断部３３は、無線アクセスシステムにおいて用いるアルゴリズムと無線区間アルゴリズムリストとを比較する（Ｓ８０６）。ここで、移動局１０のＩＰアドレスが、ＩＰアドレスリストに該当し、かつ、無線区間アルゴリズムリストにおいて、無線アクセスシステムにおいて用いるアルゴリズムがIPsec不要であると設定されている場合は、判断部３３は、セキュリティが確保されたコネクションを確立する必要が無いと判断する。尚、以下の処理は、コネクションが不要であると判断した場合の処理であり、コネクションが必要である場合は、従来の手順と同様に、コネクションが確立される。

【０１５５】

又、ステップＳ８０７～Ｓ８１５の処理は、図１７に示すステップＳ７０６～Ｓ７１４の処理と同様であるので、ここでは説明を省略する。

【０１５６】

（作用及び効果）

第８の実施の形態に係る通信システム、交換機３０及び通信方法によると、交換機３０が、移動局１０のアドレスと、ＩＰアドレスリストとを比較することに加え、無線アクセスシステムにおいて用いるアルゴリズムと無線区間アルゴリズムリストとを比較することにより、移動局１０との間に、セキュリティが確保されたコネクションを確立するか否か判断する。

【０１５７】

このため、第８の実施の形態に係る通信システム、交換機３０及び通信方法によると、IMSの暗号化処理をスキップすることができ、無駄な暗号化処理を行わないことによる接続遅延の短縮、及び移動局とネットワークの処理負荷削減を実現することができる。

【０１５８】

又、第８の実施の形態では、無線区間におけるアルゴリズムを比較するため、強いセキュリティコネクションが張られている場合は、移動局１０と交換機３０間に新たなコネクションを張らないなど、より細かな制御が可能となる。

【０１５９】

＜その他の実施形態＞

本発明は上記の実施形態によって記載したが、この開示の一部をなす論述及び図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施形態、実施例及び運用技術が明らかとなろう。

【０１６０】

例えば、第１～第６の実施の形態において、無線アクセスシステムを管理する装置を一意に識別する識別子と、交換機を管理する装置を一意に識別する識別子とを比較すると説明したが、無線アクセスシステムを一意に識別する識別子と、交換機を一意に識別する識別子とを比較しても構わない。

【０１６１】

又、第７及び第８の実施の形態において、図１５及び図１８では、判断部３３、アドレスリスト保持部３５、アルゴリズムリスト保持部３７等を１の交換機３０内に配置すると説明したが、これら各部を交換機以外の装置に配置しても構わない。

【０１６２】

このように、本発明はここでは記載していない様々な実施形態等を含むことは勿論である。従って、本発明の技術的範囲は上記の説明から妥当な特許請求の範囲に係る発明特定事項によってのみ定められるものである。

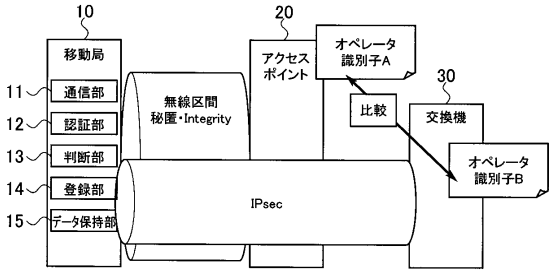
【図面の簡単な説明】

【０１６３】

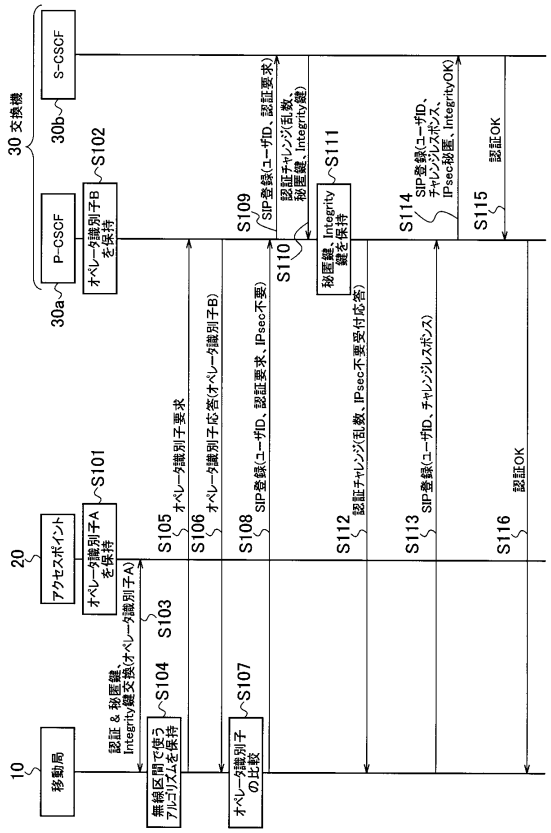
【図１】第１の実施の形態に係る通信システムの構成ブロック図である。
【図２】第１の実施の形態に係る通信方法を示すシーケンス図である。
【図３】第２の実施の形態に係る通信システムの構成ブロック図である。
【図４】第２の実施の形態に係るオペレータ識別子リストの一例である。
【図５】第２の実施の形態に係る通信方法を示すシーケンス図である。
【図６】第３の実施の形態に係る通信システムの構成ブロック図である。
【図７】第３の実施の形態に係る通信方法を示すシーケンス図である。
【図８】第４の実施の形態に係る通信システムの構成ブロック図である。
【図９】第４の実施の形態に係る無線区間アルゴリズムリストの一例である。
【図１０】第４の実施の形態に係る通信方法を示すシーケンス図である。
【図１１】第５の実施の形態に係る通信システムの構成ブロック図である。
【図１２】第５の実施の形態に係る通信方法を示すシーケンス図である。
【図１３】第６の実施の形態に係る通信システムの構成ブロック図である。

【図１４】第６の実施の形態に係る通信方法を示すシーケンス図である。
【図１５】第７の実施の形態に係る通信システムの構成ブロック図である。
【図１６】第７の実施の形態に係るＩＰアドレスリストの一例である。
【図１７】第７の実施の形態に係る通信方法を示すシーケンス図である。
【図１８】第８の実施の形態に係る通信システムの構成ブロック図である。
【図１９】第８の実施の形態に係る通信方法を示すシーケンス図である。
【図２０】従来の通信システムの構成ブロック図である。
【図２１】従来の通信方法を示すシーケンス図である。
【符号の説明】
【０１６４】
１０…移動局
１１…通信部
１２…認証部
１３…判断部
１４…登録部
１５…データ保持部
１６…識別子リスト保持部
１７…識別子保持部
１８…アルゴリズムリスト保持部
２０…アクセスポイント
３０…交換機
３０ａ…CSCF
３０ｂ…CSCF
３１…通信部
３２…認証部
３３…判断部
３４…登録部
３５…データ保持部
３６…アドレスリスト保持部
３７…アルゴリズムリスト保持部

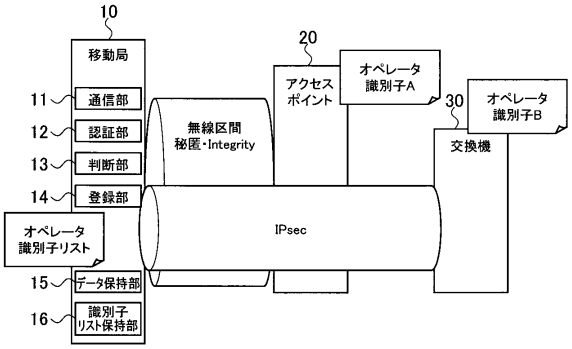
【図１】



【図２】



【図３】

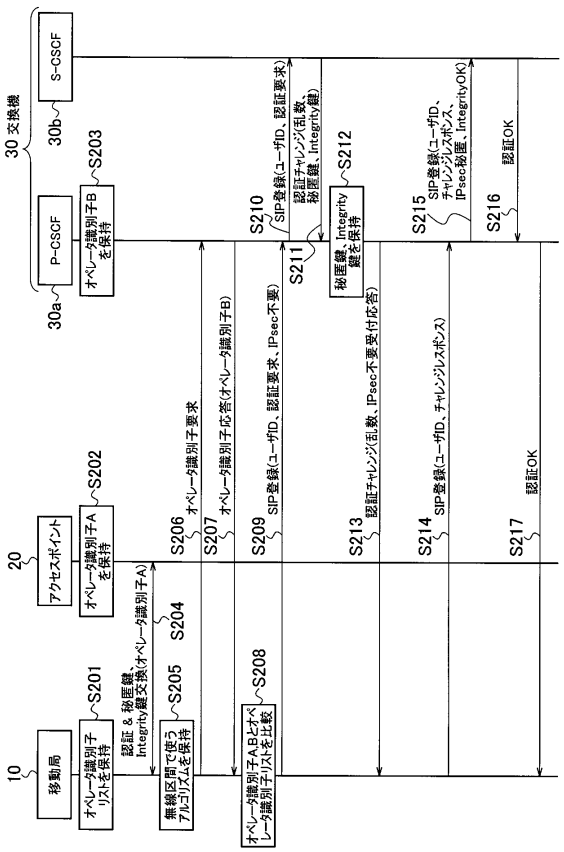


【図４】

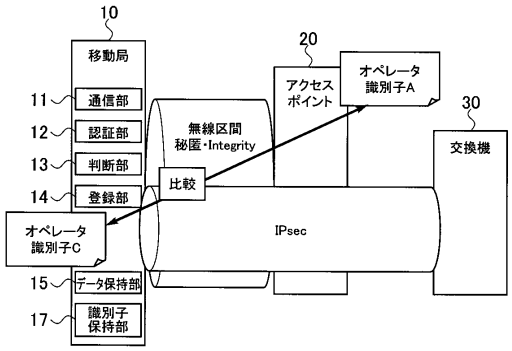
オペレータ識別子リストの例

アクセスポイント	交換機	IPsec
operatorX	operatorX	不要
operatorX	operatorZ	必要
operatorY	operatorX	不要

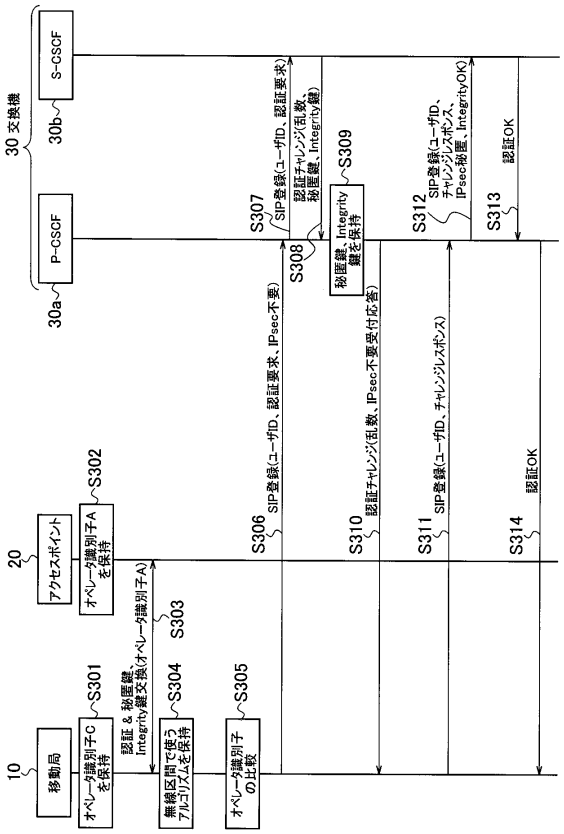
【図５】



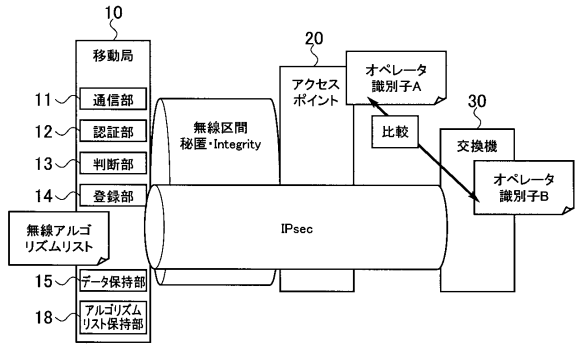
【図６】



【図７】



【図８】

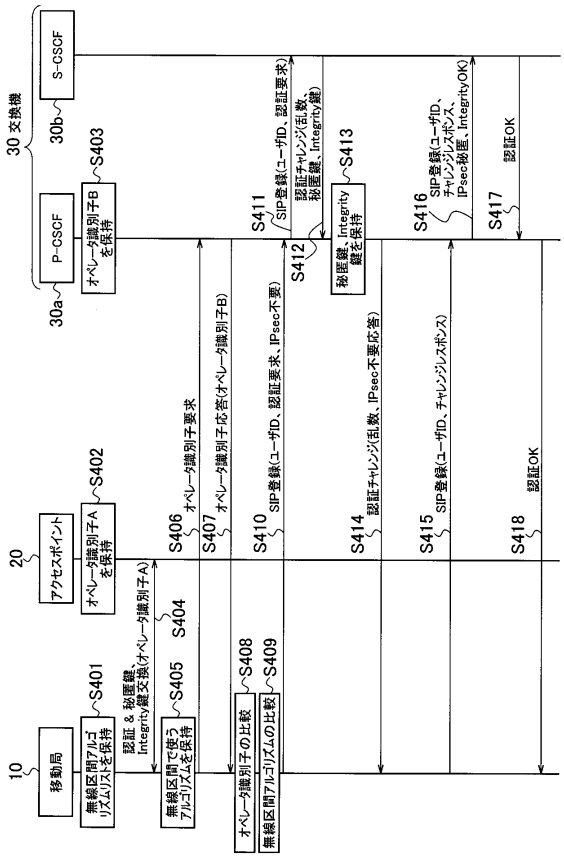


【図９】

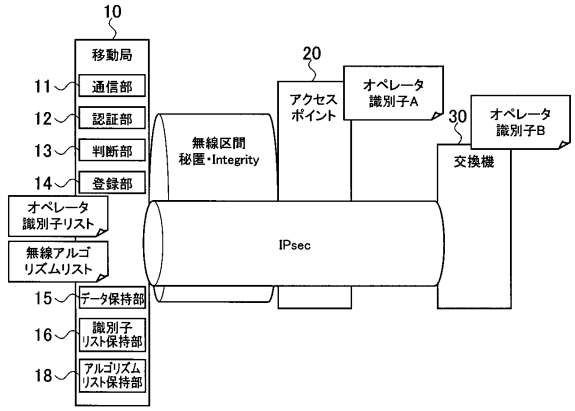
無線区間アルゴリズムリストの例

秘匿	Integrity	IPsec
AES	SHA-1	不要
3DES	SHA-1	不要
DES	MD5	必要

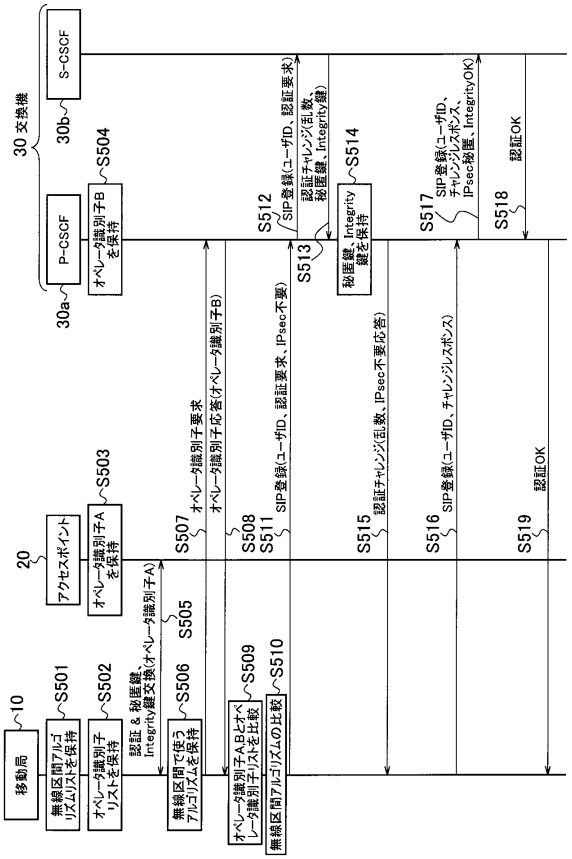
【図１０】



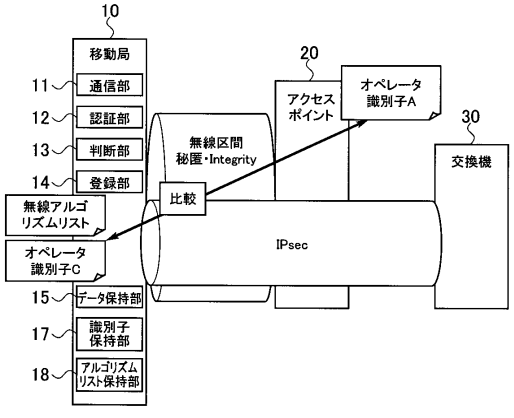
【図１１】



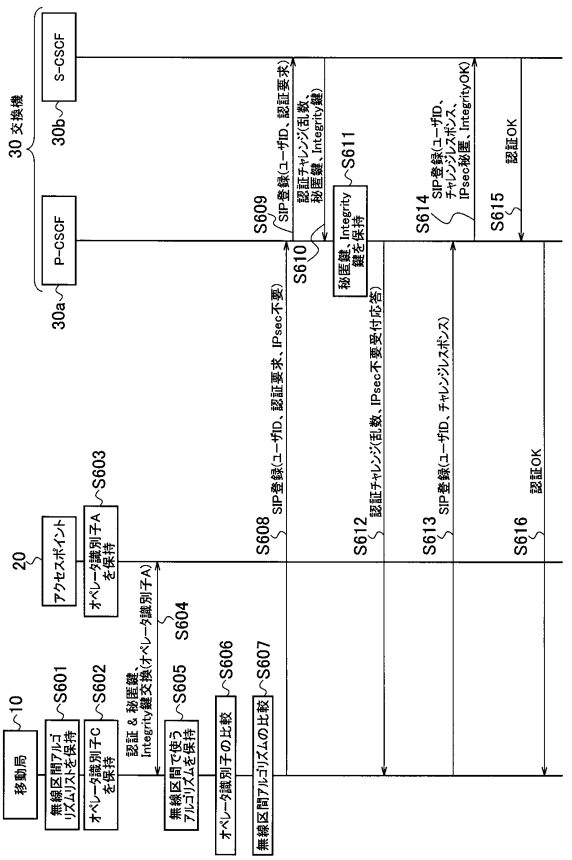
【図１２】



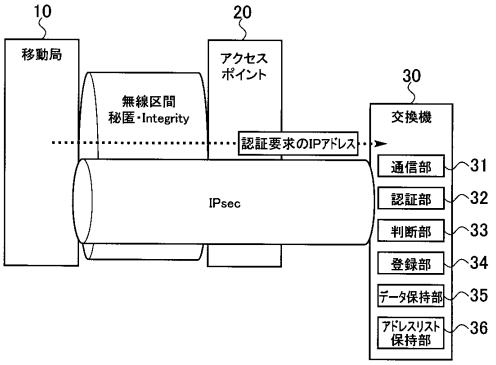
【図１３】



【図１４】



【図１５】

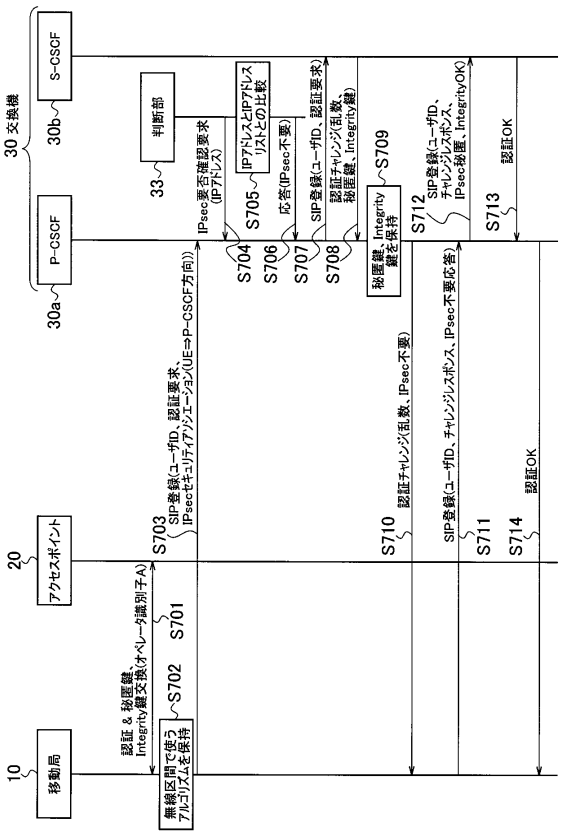


【図１６】

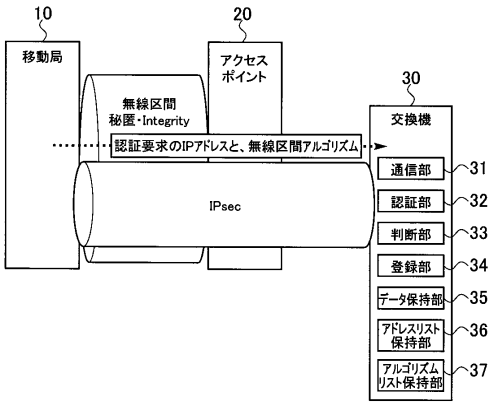
IPアドレスリストの例

	IPアドレス範囲
無線アクセスシステムA	10.0.0.0～10.1.1.1
無線アクセスシステムB	10.1.1.1～10.2.2.2

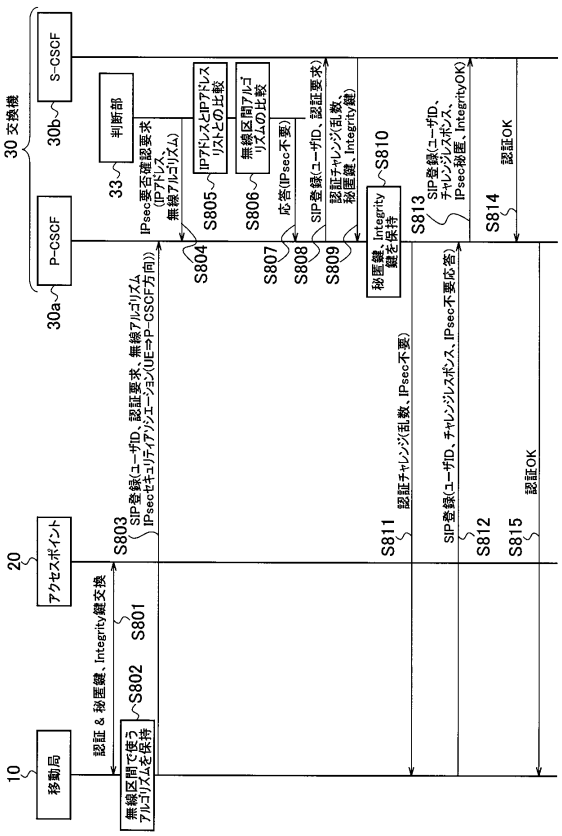
【図１７】



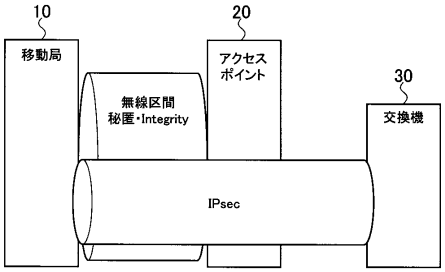
【図１８】



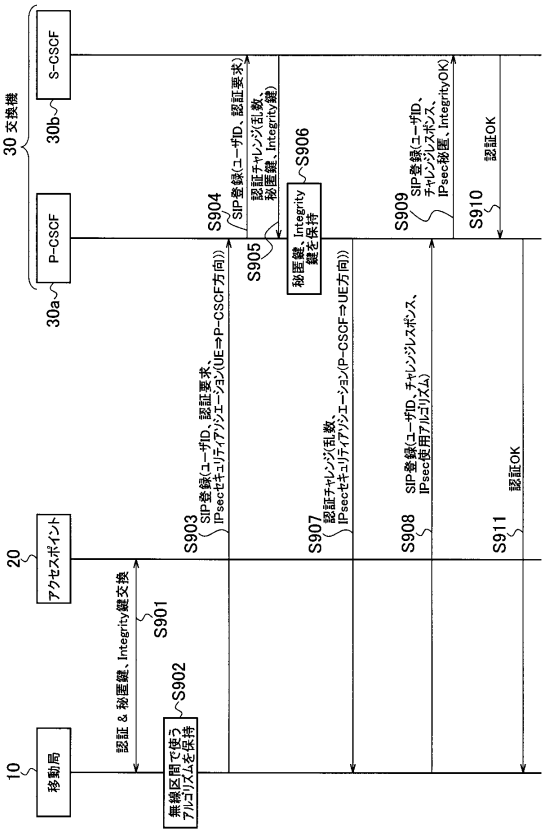
【図１９】



【図２０】


10
移動局
20
アクセス
ポイント
30
交換機
無線区間
秘匿・Integrity
IPsec

【図２１】


30 交換機
S-CSCF
30b
P-CSCF
30a
20
アクセスポイント
10
移動局
S901
認証 & 秘匿鍵、Integrity鍵交換
S902
無線区間で使うアルゴリズムを保持
S903
SIP登録(ユーザID、認証要求、IPsecセキュリティアソシエーション(UE⇒P-CSCF方向))
S904
SIP登録(ユーザID、認証要求)
S905
認証チャレンジ(乱数、秘匿鍵、Integrity鍵)
S906
秘匿鍵、Integrity鍵を保持
S907
認証チャレンジ(乱数、IPsecセキュリティアソシエーション(P-CSCF⇒UE方向))
S908
SIP登録(ユーザID、チャレンジレスポンス、IPsec使用アルゴリズム)
S909
SIP登録(ユーザID、チャレンジレスポンス、IPsec秘匿、IntegrityOK)
S910
認証OK
S911
認証OK

フロントページの続き

(51)Int.Cl. F I
H04L 9/32 (2006.01) H04L 9/00 673B

(72)発明者 田原 拓永
東京都千代田区永田町二丁目１１番１号 株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者 田辺 哲通
東京都千代田区永田町二丁目１１番１号 株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者 野口 勝広
東京都千代田区永田町二丁目１１番１号 株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者 川勝 慎平
東京都港区赤坂二丁目４番５号 ドコモ・テクノロジ株式会社内

審査官 菊地 陽一

(56)参考文献 特表２００５－５１０９４９（ＪＰ，Ａ）
3GPP TS 33.203 V6.8.0, ２００５年 9月

(58)調査した分野(Int.Cl., ＤＢ名)
H04L １２／５６
H04L ９／３２
H04L １２／２２
H04M ３／００
H04W １２／００
H04W ９２／１０