(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-140563
(P2004-140563A)
(43)公開日　平成16年5月13日(2004.5.13)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04Q	7/38	H04B	7/26	109R	5J104
H04B	7/26	H04Q	7/04	Z	5K067
H04Q	7/20	H04B	7/26	E	
// H04L	9/32	H04L	9/00	673B	

審査請求 未請求　請求項の数 10　ＯＬ　（全 17 頁）

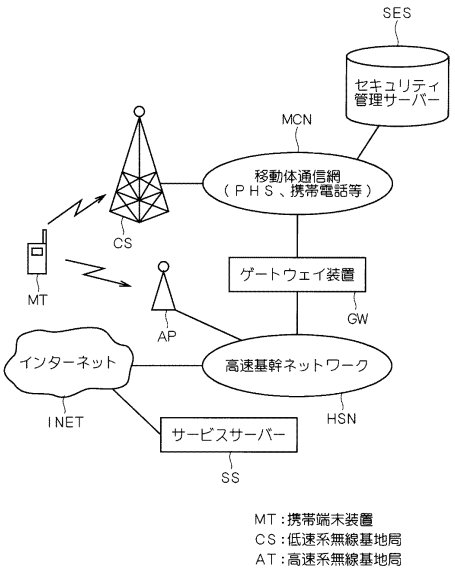
(21)出願番号　特願2002-302909(P2002-302909)
(22)出願日　平成14年10月17日(2002.10.17)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(74)代理人　100089233
弁理士　吉田　茂明
(74)代理人　100088672
弁理士　吉竹　英俊
(74)代理人　100088845
弁理士　有田　貴弘
(72)発明者　前田　尚利
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　湯川　純
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】通信システムおよび通信端末装置

(57)【要約】
【課題】高速系と低速系の両方の通信システムを利用する無線通信システムにおいて、セキュリティー性の確保を図る。
【解決手段】無線通信システムは、低速系無線基地局ＣＳおよび移動体通信網ＭＣＮから成る低速系通信システムと、高速系無線基地局ＡＰ、高速基幹ネットワークＨＳＮから成る高速系通信システムとを有する。移動体通信網ＭＣＮには、セキュリティ情報の認証等のセキュリティ処理を行うセキュリティ管理サーバーＳＥＳが専用回線により直接接続されており、セキュリティ管理サーバーＳＥＳへのセキュリティ情報の送信は、比較的セキュリティ性の高い低速系通信システムを介して行われる。
【選択図】　図１



【特許請求の範囲】
【請求項１】
互いに接続可能な第１の通信網および第２の通信網と、
前記第１の通信網および前記第２の通信網の両方に接続可能な通信端末と、
前記第１の通信網および前記第２の通信網を介して前記通信端末にコンテンツを提供するサービスサーバーと、
前記第１の通信網に直接接続され、前記通信端末から送信される個人情報等のセキュリティ情報に基づき、前記サービスサーバーが提供する特定のコンテンツにアクセスするために必要なセキュリティ処理を行うセキュリティ管理サーバーとを備える無線通信システムであって、
前記通信端末からの前記セキュリティサーバーへの前記セキュリティ情報の送信は、前記第１の通信網のみを介して行なわれる
ことを特徴とする通信システム。
【請求項２】
請求項１に記載の通信システムであって、
前記通信端末は、携帯電話の端末としての機能および無線ＬＡＮの端末としての機能を有する携帯通信端末であり、
前記第１の通信網は、前記携帯電話のサービスを提供する移動体通信網であり、
前記第２の通信網は、前記無線ＬＡＮを介して接続可能な前記移動体通信網よりも通信速度が高速な高速基幹ネットワークであり、
前記通信端末は、前記サービスサーバーに対する通信を、前記第２の通信網を優先的に使用して行う
ことを特徴とする通信システム。
【請求項３】
請求項１または請求項２に記載の通信システムであって、
前記サービスサーバーは、前記通信端末に前記セキュリティ情報の入力を促すコンテンツ（以下「セキュリティ処理専用コンテンツ」）をさらに提供し、
前記通信端末は、前記セキュリティ処理専用コンテンツを受信すると、使用する通信網を前記第１の通信網に切り替える
ことを特徴とする通信システム。
【請求項４】
請求項１または請求項２に記載の通信システムであって、
前記セキュリティ管理サーバーは、前記通信端末に前記セキュリティ処理専用コンテンツの位置情報をさらに提供し、
前記サービスサーバーはさらに、前記セキュリティ管理サーバーが提供する前記セキュリティ処理専用コンテンツの位置情報を提供し、
前記通信端末は、前記位置情報を受信すると、使用する通信網を前記第１の通信網に切り替えると共に、前記セキュリティ管理サーバーに対し前記位置情報に対応した前記セキュリティ処理専用コンテンツを要求する
ことを特徴とする通信システム。
【請求項５】
請求項３または請求項４に記載の通信システムにおける通信制御方法であって、
前記セキュリティ処理専用コンテンツはそれぞれ、前記セキュリティ処理専用コンテンツの種類あるいは前記セキュリティ処理専用コンテンツを提供するサーバーの種類に応じて異なる識別子を有する
ことを特徴とする通信システム。
【請求項６】
請求項１から請求項５のいずれかに記載の通信システムにおける通信制御方法であって、
前記セキュリティ管理サーバーにおける単一の前記セキュリティ処理によって、複数個の前記特定のコンテンツへのアクセスが可能となる

ことを特徴とする通信システム。
【請求項７】
特定のコンテンツにアクセスするために必要な処理を個人情報等のセキュリティ情報に基づいて行うセキュリティ管理サーバーが直接接続された第１の通信網、並びに、前記第１の通信網と互いに接続可能な第２の通信網の両方に接続可能であり、且つ、前記第１の通信網および前記第２の通信網を介して前記コンテンツを提供するサービスサーバーに接続可能な通信端末装置であって、
前記セキュリティサーバーへの前記セキュリティ情報の送信は、前記第１の通信網のみを介して行う
ことを特徴とする通信端末装置。
【請求項８】
請求項７に記載の通信端末装置であって、
前記第１の通信網は、携帯電話のサービスを提供する移動体通信網であり、
前記第２の通信網は、無線ＬＡＮを介して接続可能な前記移動体通信網よりも通信速度が高速な高速基幹ネットワークであり、
前記通信端末装置は、前記携帯電話の端末としての機能および前記無線ＬＡＮの端末としての機能を有する携帯通信端末であり、前記サービスサーバーに対する通信を、前記第２の通信網を優先的に使用して行う
ことを特徴とする通信端末装置。
【請求項９】
請求項７または請求項８に記載の通信端末装置であって、
セキュリティ処理専用コンテンツを受信すると、使用する通信網を前記第１の通信網に切り替える
ことを特徴とする通信端末装置。
【請求項１０】
請求項７または請求項８に記載の通信端末装置であって、
セキュリティ処理専用コンテンツの位置情報を受信すると使用する通信網を前記第１の通信網に切り替えると共に、前記位置情報に対応した前記セキュリティ処理専用コンテンツを要求する
ことを特徴とする通信端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、高速通信装置におけるデータ通信方法に関し、特に、ＰＨＳを含む携帯電話のような低速の無線通信システムと無線ＬＡＮのような高速な無線通信システムと相互に接続したシステムを用いる場合の無線通信網の通信制御に関する。
【０００２】
【従来の技術】
近年、移動局との間で高速な無線通信を可能にするシステムとして、無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）システムの普及が加速している。しかし現時点では、無線ＬＡＮなどの高速系無線通信システムが提供する無線サービスが受けられるエリアは、構内等の限られた場所となっている。よって、高速系のサービスを使用する場合には、高速系無線通信サービスに対応した端末を使用し、高速系無線通信システムのアクセスポイント（無線基地局等）を経由して、目的の通信相手（サーバー等）にアクセスすることになる。
【０００３】
それに対し、低速系の無線通信サービスを提供する携帯電話の移動体通信網は、現在でも全国規模で実現されている。よって、高速系無線通信サービスが使えない場所でも、低速系無線通信サービスに対応した端末を使って、低速系無線通信システムから目的の通信相手にアクセスすることが可能である。

【０００４】
このような双方の利点を生かすシステムとして、両システムの使い分けに関する利用者の操作を介することなく、高速系と低速系の両方の無線通信システムを利用ことができる無線通信システムが提案されている（例えば、特許文献１）。
【０００５】
【特許文献１】
特開２００１－１４４８１５号公報（第４－９頁、第１－６図）
【０００６】
【発明が解決しようとする課題】
そのような無線通信システムにおいては、携帯端末は一旦高速系通信システムの回線を確保した後は、通信を終了するまで、あるいは高速系無線通信のエリア外に当該携帯端末が移動するまでは高速系通信システムを利用した通信（高速系通信）を継続する。この場合、通信相手との間でセキュリティ上の安全性（セキュリティ性）を確保する必要がある情報（例えば、個人の電話番号や携帯端末装置の暗証番号、クレジットカード番号などの個人情報等）（本明細書においては「セキュリティ情報」と定義する）の通信を行う場合も、移動局－高速系無線基地局間通信や、インターネットを使用することになる。
【０００７】
一般に、ＰＨＳを含む携帯電話の移動体通信網は、それぞれの携帯電話事業者独自の専用回線および通信装置により構成された上で、それら限られた事業者により管理され、携帯電話以外からのアクセスは困難であるのでセキュリティ上の安全性は比較的高い。それに対し、無線ＬＡＮ等を介して接続される高速基幹ネットワークのような高速系通信システムはインターネットと同様に、パソコン等のあらゆる通信機器により公衆回線を介して容易にアクセス可能であり、比較的セキュリティ性が低いと考えられる。
【０００８】
つまり、上記したような高速系と低速系の両方の無線通信システムを使用する従来の無線通信通信システムでは、個人情報等のセキュリティ性の確保が必要な情報（セキュリティ情報）が、使用者の意図に関係なく比較的セキュリティ性の低い移動端末－高速系無線基地局間の通信やインターネット通信を介して行なわれる可能性がある。つまり、個人の重要なデータやサービス提供者の重要なデータが不正アクセスやハッキング等によって漏洩してしまう危険性がある。
【０００９】
この発明は、以上のような課題を解決するためになされたものであり、高速系と低速系の両方のシステムを利用する無線通信システムにおいて、セキュリティー性の確保を図ることができる通信システムを提供することを目的とする。
【００１０】
【課題を解決するための手段】
請求項１に係る通信システムは、互いに接続可能な第１の通信網および第２の通信網と、前記第１の通信網および前記第２の通信網の両方に接続可能な通信端末と、前記第１の通信網および前記第２の通信網を介して前記通信端末にコンテンツを提供するサービスサーバーと、前記第１の通信網に直接接続され、前記通信端末から送信される個人情報等のセキュリティ情報に基づき、前記サービスサーバーが提供する特定のコンテンツにアクセスするために必要なセキュリティ処理を行うセキュリティ管理サーバーとを備える無線通信システムであって、前記通信端末からの前記セキュリティサーバーへの前記セキュリティ情報の送信は、前記第１の通信網のみを介して行なわれることを特徴とする。
【００１１】
【発明の実施の形態】
＜実施の形態１＞
図１は本発明の実施の形態１に係る無線通信システムの構成を示す図である。携帯端末装置ＭＴは、低速系の通信網と高速系の通信網とに相互に接続可能である。ここでは、低速系の通信システムとして、ＰＨＳを含む携帯電話などのサービスを提供する移動体通信網

ＭＣＮを想定している。携帯端末装置ＭＴと移動体通信網ＭＣＮとの間の通信は、移動体通信網ＭＣＮに有線で接続された低速系無線基地局ＣＳを介して行なわれる。また、移動体通信網ＭＣＮには、携帯端末装置ＭＴから送信される個人情報等のセキュリティ情報に基づき認証等のセキュリティ処理を行うセキュリティ管理サーバーＳＥＳが専用回線で直接接続されている。図１においては、低速系無線基地局ＣＳは１つのみ図示しているが、実際には複数の無線基地局ＣＳが移動体通信網ＭＣＮに接続されており、それぞれが移動体通信網のエリアを提供している。

【００１２】

また、高速系の通信システムとして、無線ＬＡＮシステムを想定している。携帯端末装置ＭＴは、無線ＬＡＮのエリアを提供する高速系無線基地局ＡＰを介して高速基幹ネットワークＨＳＮと接続可能である。図１においては、高速系無線基地局ＡＰは１つのみ図示しているが、実際には複数の高速系無線基地局ＡＰが様々な場所に分散して設置されている。

【００１３】

高速基幹ネットワークＨＳＮは、インターネット網ＩＮＥＴを介して、携帯端末装置ＭＴにコンテンツを提供するサービスサーバーＳＳに接続される。サービスサーバーＳＳが提供するコンテンツには、通常のコンテンツの他、アクセスするためにセキュリティ情報による認証処理等のセキュリティ処理の結果得られる特定のアクセス権が必要なコンテンツ、そのセキュリティ処理に使用するセキュリティ情報の入力を促すコンテンツ（以下「セキュリティ処理専用コンテンツ」）等が含まれている。セキュリティ情報としては、例えば個人の電話番号や携帯端末装置の暗証番号、クレジットカード番号等が挙げられる。セキュリティ処理専用コンテンツは、例えば、所定の規則に従ってコンテンツ情報のデータの中にセキュリティ情報の入力を要求することを示す識別子（即ち、自身がセキュリティ処理専用コンテンツであることを示す識別子）および、セキュリティ管理サーバーＳＥＳへのアクセス方法が付加された信号である。

【００１４】

セキュリティ管理サーバーＳＥＳは、セキュリティ情報の認証等のセキュリティ処理を行うサーバーであり、移動体通信網ＭＣＮと専用回線で直接接続され、セキュリティ管理サーバーＳＥＳへのアクセスは、必ず、低速系無線基地局ＣＳおよび移動体通信網ＭＣＮから成る低速系通信システムを介して行なわれる。セキュリティ管理サーバーＳＥＳには、サービスサーバーＳＳに存在するアクセス権が必要なコンテンツの位置を示すＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）などのコンテンツ位置情報が予め格納されている。

【００１５】

また、移動体通信網ＭＣＮは高速基幹ネットワークＨＳＮに、ゲートウェイ装置ＧＷを介して接続されている。ゲートウェイ装置ＧＷは、互いに通信速度が異なる低速系の通信システムと高速系の通信システムとの間で、通信チャネルの信号の中継を行うことで、移動体通信網ＭＣＮと高速基幹ネットワークＨＳＮとの間の通信が可能になる。

【００１６】

本実施の形態に係る無線通信システムの動作について説明する。なお、ここでは携帯端末装置ＭＴが、既に高速系の通信が確立されている状態を仮定し、その状態からセキュリティ処理によるアクセス権が必要なコンテンツにアクセスしようとする場合の動作を説明する。図２、図３及び図４はそれぞれ、その場合における無線通信システム全体の通信制御動作を示すシーケンス図、携帯端末装置ＭＴの動作を示すフローチャート、サービスサーバーＳＳの動作を示すフローチャートである。なお、図２において、細線の矢印は低速系の通信システムを介して送受信される信号（低速通信用信号）を表しており、太線の矢印は高速系の通信システムを介して送受信される信号（高速通信用信号）を表している。以下の説明は、基本的に図２のシーケンス図に基づいて行うが、以下の説明中にカッコ書きで示したＳ１０１～Ｓ１１３は図３のフローチャートにおけるステップに対応しており、Ｓ１２１～Ｓ１２６は図４のフローチャートにおけるステップに対応している。

【００１７】
まず、携帯端末装置ＭＴは、高速系無線基地局ＡＰを介して高速系の通信システムに接続していると仮定する。そして、携帯端末装置ＭＴは、高速系無線基地局ＡＰに対して所定のコンテンツへのアクセスするためのコンテンツ要求１００を送信する（Ｓ１０１）。ここでは携帯端末装置ＭＴは、特定のコンテンツへのアクセス権を獲得するために、セキュリティ処理専用コンテンツに接続しようとしており、即ち、コンテンツ要求１００はセキュリティ処理専用コンテンツを要求するためのものである。
【００１８】
高速系無線基地局ＡＰはコンテンツ要求１００を受信すると、それをコンテンツ要求１０１として高速基幹ネットワークＨＳＮへ送信する。高速基幹ネットワークＨＳＮは受信したコンテンツ要求１０１を、コンテンツ要求１０２としてインターネット網ＩＮＥＴを介してサービスサーバーＳＳに送信する。そして、サービスサーバーＳＳはコンテンツ要求１０２を受信する（Ｓ１２１）。
【００１９】
コンテンツ要求１０２を受信したサービスサーバーＳＳは、その要求に対応したコンテンツ情報を返送する（Ｓ１２２）。ここではコンテンツ要求１０２はセキュリティ処理専用コンテンツを要求しているので、サービスサーバーＳＳが返送するコンテンツ情報１０３は、セキュリティ処理専用コンテンツ情報である。上述したように、セキュリティ処理専用コンテンツは、それを受信した端末に対して、セキュリティ情報の入力を促すコンテンツである。
【００２０】
サービスサーバーＳＳから送信されたコンテンツ情報１０３は、インターネット網ＩＮＥＴを介して高速基幹ネットワークＨＳＮに受信され、コンテンツ情報１０４として高速系無線基地局ＡＰへ送信される。高速系無線基地局ＡＰはそれをコンテンツ情報１０５として携帯端末装置ＭＴに送信し、携帯端末装置ＭＴがそれを受信する（Ｓ１０２）。コンテンツ情報１０５を受信した携帯端末装置ＭＴは、それがセキュリティ処理専用コンテンツであるかどうか確認する（Ｓ１０３）。
【００２１】
このときコンテンツ情報１０５がセキュリティ処理専用コンテンツでない通常のコンテンツの情報のような場合には、そのコンテンツに適応した再生処理を行い（Ｓ１１２）、ユーザー操作待ち状態になる（Ｓ１１３）。ここでは、コンテンツ情報１０５はセキュリティ処理専用コンテンツの情報であり、その場合、携帯端末ＭＴは使用する通信システム（通信回線）を低速系の回線に切り替える処理を行う（Ｓ１０４）。そして、携帯端末装置ＭＴは、使用者にセキュリティ情報の入力を促し、入力されたセキュリティ情報をセキュリティ情報１０６として低速系通信システムを使用してサービスサーバーＳＳ宛てに送信する（Ｓ１０５）。低速系無線基地局ＣＳはセキュリティ情報１０６を受信し、それをセキュリティ情報１０７として移動体通信網ＭＣＮへ送信する。セキュリティ情報１０７を受信した移動体通信網ＭＣＮは、それをセキュリティ情報１０８としてセキュリティ管理サーバーＳＥＳへと送信する。
【００２２】
セキュリティ管理サーバーＳＥＳは、セキュリティ情報１０８を受信すると、それに基づき個人認証やクレジット番号などの取得、照合あるいは課金といったセキュリティ処理を行う。セキュリティ処理の結果、正規の処理が正常に完了した場合には、特定のコンテンツに対するアクセス権を内包するアクセス許可信号１０９を生成し、移動体通信網ＭＣＮへ送信する。なお、アクセス許可信号１０９には、携帯端末装置ＭＴから送信されたセキュリティ情報の内容は含まれていない。アクセス許可信号１０９を受信した移動体通信網ＭＣＮは、それをアクセス許可信号１１０として低速系無線基地局ＣＳへ送信される。アクセス許可信号１１０を受信した低速系無線基地局ＣＳは、それをアクセス許可信号１１１として携帯端末装置ＭＴに送信する。そして携帯端末装置ＭＴは、アクセス許可信号１１１を受信する（Ｓ１０６）。

【００２３】
携帯端末装置ＭＴは、アクセス許可信号１１１を受信すると、そのアクセス許可信号を利用するコンテンツ（そのアクセス権が必要なコンテンツ）の位置を示す情報を要求するコンテンツ位置情報要求１１２をセキュリティ管理サーバーＳＥＳ宛てに送信する（Ｓ１０７）。
【００２４】
コンテンツ位置情報要求１１２は低速系無線基地局ＣＳに受信され、コンテンツ位置情報要求１１３として移動体通信網ＭＣＮへ送信される。コンテンツ位置情報要求１１３を受信した移動体通信網ＭＣＮは、それをコンテンツ位置情報要求１１４としてセキュリティ管理サーバーＳＥＳに送信する。セキュリティ管理サーバーＳＥＳは、コンテンツ位置情報要求１１４を受け取ると、当該アクセス権が必要なコンテンツの位置情報として、例えばそのＵＲＬ等をコンテンツ位置情報１１５として移動体通信網ＭＣＮへ送信する。移動体通信網ＭＣＮは、それをコンテンツ位置情報１１６として低速系無線基地局ＣＳへ送信する。コンテンツ位置情報１１６を受信した低速系無線基地局ＣＳは、それをコンテンツ位置情報１１７として携帯端末装置ＭＴに送信する。そして携帯端末装置ＭＴは、コンテンツ位置情報１１７を受信する（Ｓ１０８）。
【００２５】
携帯端末装置ＭＴは、コンテンツ位置情報１１７を受信すると、使用する通信システム（通信回線）を高速系の回線に切り替える（Ｓ１０９）。そして、コンテンツ位置情報１１７が示すコンテンツの位置および先にアクセス許可信号１１１で獲得した入手したアクセス権の情報を含むコンテンツ要求１１８を生成し、高速系の通信システムを使用してサービスサーバーＳＳ宛てに送信する（Ｓ１１０）。ここでも、コンテンツ要求１１８に含まれるアクセス権情報には、携帯端末装置ＭＴから送信されたセキュリティ情報の内容は含まれておらず、コンテンツ要求１１８全体としてもセキュリティ情報は含んでいない。
【００２６】
コンテンツ要求１１８は高速系無線基地局ＡＰで受信され、コンテンツ要求１１９として高速基幹ネットワークＨＳＮに送信される。コンテンツ要求１１９を受信した高速基幹ネットワークＨＳＮは、それをコンテンツ要求１２０としてインターネット網ＩＮＥＴを介してサービスサーバーＳＳに送信する。そして、サービスサーバーＳＳはコンテンツ要求１２０を受信する（Ｓ１２３）。
【００２７】
サービスサーバーＳＳはコンテンツ要求１２０を受信すると、コンテンツ要求１２０に含まれているアクセス権情報およびコンテンツ位置情報を抽出し、その対象となるコンテンツにアクセス権があるかどうか調べる（Ｓ１２４）。アクセス権があると判断された場合には、そのコンテンツへのアクセスを許可し、当該コンテンツ位置情報に対応したコンテンツ情報１２１を携帯端末装置ＭＴ宛に送信し（Ｓ１２５）、その後は要求待ち状態になる（Ｓ１２６）。また、アクセス権が無いと判断された場合には、アクセス不許可であることを示すエラー信号を携帯端末装置ＭＴ宛てに送信（Ｓ１２７）した後、要求待ち状態になる（Ｓ１２６）。ここでは、アクセス権があると判断されたと仮定する。
【００２８】
コンテンツへのアクセスが許可され、サービスサーバーＳＳから送信されたコンテンツ情報１２１は、インターネット網ＩＮＥＴを介して、高速基幹ネットワークＨＳＮに受信される。高速基幹ネットワークＨＳＮは、それをコンテンツ情報１２２として高速系無線基地局ＡＰへ送信する。高速系無線基地局ＡＰに受信されたコンテンツ情報１２２は、コンテンツ情報１２３として送信され、携帯端末装置ＭＴに受信される（Ｓ１１１）。それにより、携帯端末装置ＭＴによる、アクセス権が必要なコンテンツへのアクセスが完了する。
【００２９】
携帯端末装置ＭＴは、コンテンツ情報１２３を受信するとその内容に適応した再生、表示処理あるいは保存処理を行う（Ｓ１１２）。携帯端末装置ＭＴはコンテンツの処理後、要

求待ち状態になる（Ｓ１１３）。

【００３０】

以上の動作を、携帯端末装置ＭＴ、セキュリティ管理サーバーＳＥＳ、サービスサーバーＳＳに注目し、使用する通信システムが高速系か低速系かを分けてまとめると、図５のシーケンス図のようになる。この図からも分かるように、本実施の形態に係る無線通信システムによれば、携帯端末装置ＭＴが高速系通信システムを使用中であっても、セキュリティ処理に関係する情報の通信は自動的に低速系通信システムを介して行われる。つまり、低速系と高速系の通信システムの両方を利用する従来の無線通信システムと異なり、セキュリティの高い安全性を確保する必要があるセキュリティ情報（１０６～１０８）の通信は、必ず低速系通信システムのみによって行われる。

【００３１】

上述したように、低速系通信システムである移動体通信網ＭＣＮは比較的セキュリティ性が高く、高速系通信システムである高速基幹ネットワークＨＳＮおよびインターネットは、比較的セキュリティ性が低い。つまり、本実施の形態によれば、セキュリティ情報の通信は、２つある通信システムのうち、必ずセキュリティ性の高い方の通信システムのみによって行われることとなり、不正アクセスやハッキング等によるセキュリティ情報の漏洩や改ざんを防止することができる。また、セキュリティ処理完了後は高速系通信に戻り、高速な通信が可能であるという高速系通信システムの利点が生かされる。

【００３２】

なお、本実施の形態において、コンテンツ情報１０３～１０５が有する、セキュリティ処理専用コンテンツであることを示す識別子は、アクセスの対象となるサービスサーバーＳＳ（即ち、当該セキュリティ処理専用コンテンツを提供するサーバー）が異なる場合や、あるいは同じサービスサーバーＳＳ内でも異なるセキュリティ処理専用コンテンツである場合には、それぞれが異なる識別子を有する構成であってもよい。それにより、それらのサービスサーバーＳＳあるいはセキュリティ処理専用コンテンツのそれぞれに対応した適当なセキュリティ情報の入力を促すことができ、あらゆるセキュリティ情報に対して柔軟に対応できる。

【００３３】

また、サービスサーバーＳＳに同一のアクセス権でアクセス可能なコンテンツが複数個ある場合は、１つのアクセス許可信号で獲得したアクセス権で、それら複数のコンテンツにアクセスできるようにサービスサーバーＳＳを制御してもよい。それにより、携帯端末装置ＭＴの使用者がセキュリティ情報をくり返し入力する手間を省くことができ、また、セキュリティ情報が通信システムに送信される回数を少なくすることができるため、セキュリティ情報の漏洩の危険性をさらに抑えることができる。

【００３４】

さらに、上の例ではアクセス許可信号１０９～１１１とコンテンツ位置情報１１２～１１４とは別々に送信されているが、それら両方の情報を含む信号を、アクセス許可信号としてセキュリティ管理サーバーＳＥＳから送信する構成であってもよい。それにより、低速系通信を使用する通信の回数が減るため、携帯端末装置ＭＴは、アクセス権およびコンテンツ位置をより迅速に獲得することができる。

【００３５】

また、本実施の形態においては、本発明に係るセキュリティ管理サーバーＳＥＳを移動体通信網ＭＣＮに接続される特別なサーバーとして新たに設けた構成としたが、従来の低速系通信網に既存のサーバー（例えば、特許文献１における管理装置ＤＢ）がそれと同様の機能を担う構成であってもよく、システム構成の簡略化に寄与できる。

【００３６】

なお、以上の説明は、携帯端末装置ＭＴが予め高速系通信システムに接続した状態を仮定しているが、上記したように、現時点では無線ＬＡＮ等の高速系無線通信システムが提供する無線サービスが受けられるエリア（即ち、高速系無線基地局ＡＰのエリア）は、構内等の限られた場所である。高速系無線通信サービスが使えない場所の場合は、広範囲に提

供されている低速系の無線通信システムのみを使って、以上説明した動作を行えばよい。その場合も、セキュリティ情報の通信は比較的セキュリティ性の高い低速系の無線通信システムのみによって行われることとなり、不正アクセスやハッキング等によるセキュリティ情報の漏洩や改ざんは防止される。そして、例えば、携帯端末装置ＭＴが高速系無線基地局ＡＰのエリア内に移動した場合などに、高速系通信システムを優先的に使用すれば、高速な通信が可能であるという高速系通信システムの利点が生かされる。

【００３７】

＜実施の形態２＞

実施の形態２においては、セキュリティ処理専用コンテンツ情報が、サービスサーバーＳＳではなくセキュリティ管理サーバーＳＥＳから携帯端末装置ＭＴに送信される構成例を示す。即ち、本実施の形態においては、セキュリティ処理専用コンテンツは、セキュリティ管理サーバーＳＥＳにより提供される。また、サービスサーバーＳＳは、受信したコンテンツ要求がセキュリティ処理専用コンテンツを要求するものである場合、セキュリティ管理サーバーＳＥＳ上のセキュリティ処理専用コンテンツの位置を示すＵＲＬ等の位置情報を返送し、それ以外の場合は通常のコンテンツ情報を返送する。セキュリティ処理専用コンテンツ位置情報とは、例えば、所定の規則に従ってコンテンツの中に自身がセキュリティ処理専用コンテンツ位置情報であることを示す識別子を付加したものである。

【００３８】

なお、本実施の形態においても、全体のシステム構成としては、図１に示したシステム構成と同様であるので、ここでの詳細な説明は省略する。

【００３９】

以下、本実施の形態に係る無線通信システムの動作について説明する。ここでも、携帯端末装置ＭＴは低速系の通信網と高速系の通信網とに相互に接続可能であり、当該携帯端末装置ＭＴが、既に高速系の通信が確立されている状態を仮定し、その状態からセキュリティ処理によるアクセス権が必要なコンテンツにアクセスしようとする場合の動作を説明する。図６、図７及び図８はそれぞれ、その場合における無線通信システム全体の通信制御動作を示すシーケンス図、携帯端末装置ＭＴの動作を示すフローチャート、サービスサーバーＳＳの動作を示すフローチャートである。なお、図６において、細線の矢印は低速系の通信システムを介して送受信される信号（低速通信用信号）を表しており、太線の矢印は高速系の通信システムを介して送受信される信号（高速通信用信号）を表している。以下の説明は、基本的に図６のシーケンス図に基づいて行うが、以下の説明中にカッコ書きで示したＳ２０１～Ｓ２１５は図７のフローチャートにおけるステップに対応しており、Ｓ２２１～Ｓ２２６は図８のフローチャートにおけるステップに対応している。

【００４０】

まず、携帯端末装置ＭＴは、高速系無線基地局ＡＰを介して高速系の通信システムに接続していると仮定する。そして、携帯端末装置ＭＴはサービスサーバーＳＳ宛てに、高速系通信システムを介して所定のコンテンツへのアクセスするためのコンテンツ要求２００を送信する（Ｓ２０１）。ここでも携帯端末装置ＭＴは、特定のコンテンツへのアクセス権を獲得するために、セキュリティ処理専用コンテンツに接続しようとしており、即ち、コンテンツ要求２００はセキュリティ処理専用コンテンツを要求するものである。

【００４１】

携帯端末装置ＭＴがコンテンツ要求２００を送信すると（Ｓ２０１）、当該コンテンツ要求２００は高速系無線基地局ＡＰを介してコンテンツ要求２０１として高速基幹ネットワークＨＳＮに送信され、さらに高速基幹ネットワークＨＳＮを介してコンテンツ要求２０２としてサービスサーバーＳＳに受信される（Ｓ２２１）。

【００４２】

上述したように、本実施の形態に係るサービスサーバーＳＳは、受信したコンテンツ要求がセキュリティ処理専用コンテンツを要求するものである場合はセキュリティ管理サーバーＳＥＳ上のセキュリティ処理専用コンテンツの位置を示すＵＲＬ等の位置情報を返送し、それ以外の場合は通常のコンテンツ情報を返送する。ここではコンテンツ要求２０２は

セキュリティ処理専用コンテンツを要求しているので、サービスサーバーＳＳはその応答として、セキュリティ処理専用コンテンツの位置を示すセキュリティ処理専用コンテンツ位置情報２０３を送信する（Ｓ２２２）。

【００４３】

サービスサーバーＳＳから送信されセキュリティ処理専用コンテンツ位置情報２０３は、インターネット網ＩＮＥＴを介して高速基幹ネットワークＨＳＮに受信され、セキュリティ処理専用コンテンツ位置情報２０４として高速系無線基地局ＡＰへ送信される。高速系無線基地局ＡＰはそれをセキュリティ処理専用コンテンツ位置情報２０５として携帯端末装置ＭＴに送信し、携帯端末装置ＭＴがそれを受信する（Ｓ２０２）。コンテンツ情報１０５を受信した携帯端末装置ＭＴは、その応答がセキュリティ処理専用コンテンツ位置情報であるかどうか確認する（Ｓ２０３）。

【００４４】

そして、その応答がセキュリティ処理専用コンテンツ位置情報でない通常のコンテンツ情報のような場合には、そのコンテンツに適応した再生処理を行い（Ｓ２１４）、ユーザー操作待ち状態になる（Ｓ２１５）。ここでは、その応答はセキュリティ処理専用コンテンツ位置情報２０５であり、その場合、携帯端末ＭＴは使用する通信システム（通信回線）を低速系の回線に切り替える処理を行う（Ｓ２０４）。そして、携帯端末装置ＭＴは、受信したセキュリティ処理専用コンテンツ位置情報２０５に対応したセキュリティ処理専用コンテンツを要求するためのセキュリティ処理専用コンテンツ要求２０６を、低速系通信システムを使用して低速系無線基地局ＣＳ宛てに送信する（Ｓ２０５）。即ち、セキュリティ処理専用コンテンツ情報要求２０６は、低速系無線基地局ＣＳを介して、セキュリティ処理専用コンテンツ情報要求２０７として移動体通信網ＭＣＮへ送信され、さらに移動体通信網ＭＣＮを介して、セキュリティ処理専用コンテンツ情報要求２０８としてセキュリティ管理サーバーＳＥＳに受信される。

【００４５】

セキュリティ管理サーバーＳＥＳは、セキュリティ処理専用コンテンツ情報要求２０８を受信すると、それに対応したセキュリティ処理専用コンテンツ情報２０９を生成し、移動体通信網ＭＣＮへ送信する。セキュリティ処理専用コンテンツ情報２０９は、移動体通信網ＭＣＮを介し、セキュリティ処理専用コンテンツ情報２１０として低速系無線基地局ＣＳへ送信され、さらに低速系無線基地局ＣＳを介してセキュリティ処理専用コンテンツ情報２１１として送信され、携帯端末装置ＭＴに受信される（Ｓ２０６）。

【００４６】

セキュリティ処理専用コンテンツ情報２１１を受信した携帯端末装置ＭＴは、使用者にセキュリティ情報の入力を促し、入力されたセキュリティ情報をセキュリティ情報２１２として低速系通信システムを使用してサービスサーバーＳＳ宛てに送信する（Ｓ２０７）。セキュリティ情報２１２は、低速系無線基地局ＣＳを介し、セキュリティ情報２１３として移動体通信網ＭＣＮへと送信され、さらに移動体通信網ＭＣＮを介してセキュリティ情報２１４としてセキュリティ管理サーバーＳＥＳへと送信される。

【００４７】

セキュリティ管理サーバーＳＥＳは、セキュリティ情報２１４を受信すると、それに基づき個人認証やクレジット番号などの取得、照合あるいは課金といったセキュリティ処理を行う。セキュリティ処理の結果、正規の処理が正常に完了した場合には、特定のコンテンツに対するアクセス権を内包するアクセス許可信号２１５を生成し、移動体通信網ＭＣＮへ送信する。なお、アクセス許可信号２１５には、携帯端末装置ＭＴから送信されたセキュリティ情報の内容は含まれていない。アクセス許可信号２１５は、移動体通信網ＭＣＮを介し、アクセス許可信号２１６として低速系無線基地局ＣＳへ送信され、さらに低速系無線基地局ＣＳを介してアクセス許可信号２１７として携帯端末装置ＭＴに送信される。そして携帯端末装置ＭＴは、アクセス許可信号２１７を受信する（Ｓ２０８）。

【００４８】

携帯端末装置ＭＴは、アクセス許可信号２１７を受信すると、そのアクセス許可信号を利

用するコンテンツ（そのアクセス権が必要なコンテンツ）の位置を示す情報を要求するコンテンツ位置情報要求２１８をセキュリティ管理サーバーＳＥＳ宛てに送信する（Ｓ２０９）。

【００４９】

コンテンツ位置情報要求２１８は、低速系無線基地局ＣＳを介して、コンテンツ位置情報要求２１９として移動体通信網ＭＣＮへ送信され、さらに移動体通信網ＭＣＮを介して、コンテンツ位置情報要求２２０としてセキュリティ管理サーバーＳＥＳに送信される。セキュリティ管理サーバーＳＥＳは、コンテンツ位置情報要求２２０を受け取ると、当該アクセス権が必要なコンテンツの位置情報として、例えばそのＵＲＬ等をコンテンツ位置情報２２１として移動体通信網ＭＣＮへ送信する。コンテンツ位置情報２２１は、移動体通信網ＭＣＮを介して、コンテンツ位置情報２２２として低速系無線基地局ＣＳへ送信され、さらの低速系無線基地局ＣＳを介して、コンテンツ位置情報２２３として携帯端末装置ＭＴに送信され、携帯端末装置ＭＴはそれを受信する（Ｓ２１０）。

【００５０】

携帯端末装置ＭＴは、コンテンツコンテンツ位置情報２２３を受信すると、使用する通信システム（通信回線）を高速系の回線に切り替える（Ｓ２１１）。そして、コンテンツ位置情報２２３が示すコンテンツの位置および先にアクセス許可信号２１７で獲得した入手したアクセス権の情報を含むコンテンツ要求２２４を生成し、高速系の通信システムを使用してサービスサーバーＳＳ宛てに送信する（Ｓ２１２）。ここでも、コンテンツ要求２２４に含まれるアクセス権情報には、携帯端末装置ＭＴから送信されたセキュリティ情報の内容は含まれておらず、コンテンツ要求２２４全体としてもセキュリティ情報は含んでいない。

【００５１】

コンテンツ要求２２４は高速系無線基地局ＡＰを介し、コンテンツ要求２２５として高速基幹ネットワークＨＳＮに送信される。コンテンツ要求２２５を受信した高速基幹ネットワークＨＳＮは、それをコンテンツ要求２２６としてインターネット網ＩＮＥＴを介してサービスサーバーＳＳに送信する。そして、サービスサーバーＳＳはコンテンツ要求２２６を受信する（Ｓ２１３）。

【００５２】

サービスサーバーＳＳはコンテンツ要求２２６を受信すると、コンテンツ要求２２６に含まれているアクセス権情報およびコンテンツ位置情報を抽出し、その対象となるコンテンツにアクセス権があるかどうか調べる（Ｓ２２４）。アクセス権があると判断された場合には、そのコンテンツへのアクセスを許可し、当該コンテンツ位置情報に対応したコンテンツ情報２２７を携帯端末装置ＭＴ宛てに送信し（Ｓ２２５）、その後は要求待ち状態になる（Ｓ２２６）。また、アクセス権が無いと判断された場合には、アクセス不許可であることを示すエラー信号を携帯端末装置ＭＴ宛てに送信（Ｓ２２７）した後、要求待ち状態になる（Ｓ２２６）。ここでは、アクセス権があると判断されたと仮定する。

【００５３】

コンテンツへのアクセスが許可され、サービスサーバーＳＳから送信されたコンテンツ情報２２７は、インターネット網ＩＮＥＴを介して、高速基幹ネットワークＨＳＮに受信される。高速基幹ネットワークＨＳＮは、それをコンテンツ情報２２８として高速系無線基地局ＡＰへ送信する。高速系無線基地局ＡＰに受信されたコンテンツ情報２２８は、コンテンツ情報２２９として送信され、携帯端末装置ＭＴにより受信される（Ｓ２１３）。それにより、携帯端末装置ＭＴによる、アクセス権が必要なコンテンツへのアクセスが完了する。

【００５４】

携帯端末装置ＭＴは、コンテンツ情報１２３を受信するとその内容に適応した再生、表示処理あるいは保存処理を行う（Ｓ２１４）。携帯端末装置ＭＴはコンテンツの処理後、要求待ち状態になる（Ｓ２１５）。

【００５５】

以上の動作を、携帯端末装置ＭＴ、セキュリティ管理サーバーＳＥＳ、サービスサーバーＳＳに注目し、使用する通信システムが高速系か低速系かを分けてまとめると、図９のシーケンス図のようになる。この図からも分かるように、本実施の形態に係る無線通信システムによれば、携帯端末装置ＭＴが高速系通信システムを使用中であっても、セキュリティ処理に関係する情報の通信は自動的に低速系通信システムを介して行われる。つまり、低速系と高速系の通信システムの両方を利用する従来の無線通信システムと異なり、セキュリティの高い安全性を確保する必要があるセキュリティ情報（２１３～２１４）の通信は、必ず低速系通信システムのみによって行われる。

【００５６】

つまり、本実施の形態においても、セキュリティ情報の通信は、２つある通信システムのうち、必ずセキュリティ性の高い方の通信システムによって行われることとなり、不正アクセスやハッキング等によるセキュリティ情報の漏洩や改ざんを防止することができる。また、セキュリティ処理完了後は高速系通信に戻り、高速な通信が可能であるという高速系通信システムの利点が生かされる。

【００５７】

なお、本実施の形態においても、セキュリティ処理専用コンテンツ情報２０９，２１０，２１１が有する、セキュリティ処理専用コンテンツ情報であることを示す識別子は、セキュリティ管理サーバーＳＥＳが提供するセキュリティ処理専用コンテンツが異なる場合には、それぞれが異なる識別子を有する構成であってもよい。それにより、それらのセキュリティ処理専用コンテンツのそれぞれに対応した適当なセキュリティ情報の入力を促すことができ、あらゆるセキュリティ情報に対して柔軟に対応できる。

【００５８】

また、サービスサーバーＳＳに同一のアクセス権でアクセス可能なコンテンツが複数個ある場合は、１つのアクセス許可信号で獲得したアクセス権で、それら複数のコンテンツにアクセスできるようにサービスサーバーＳＳを制御してもよい。それにより、携帯端末装置ＭＴの使用者がセキュリティ情報をくり返し入力する手間を省くことができ、また、セキュリティ情報が通信システムに送信される回数を少なくすることができるため、セキュリティ情報の漏洩の危険性をさらに抑えることができる。

【００５９】

さらに、上の例でもアクセス許可信号２１５～２１７とコンテンツ位置情報２２１～２２３とは別々に送信されているが、それら両方の情報を含む信号を、アクセス許可信号としてセキュリティ管理サーバーＳＥＳから送信する構成であってもよい。それにより、低速系通信を使用する通信の回数が減るため、携帯端末装置ＭＴは、アクセス権およびコンテンツ位置をより迅速に獲得することができる。

【００６０】

また、本実施の形態においても、本発明に係るセキュリティ管理サーバーＳＥＳを移動体通信網ＭＣＮに接続される特別なサーバーとして新たに設けた構成としたが、従来の低速系通信網に既存のサーバー（例えば、特許文献１における管理装置ＤＢ）がそれと同様の機能を担う構成であってもよく、システム構成の簡略化に寄与できる。

【００６１】

また、本実施の形態においても、携帯端末装置ＭＴが予め高速系通信システムに接続した状態を仮定しているが、高速系無線通信サービスが使えない場所の場合は、広範囲に提供されている低速系の無線通信システムのみを使って、以上説明した動作を行えばよい。そして、例えば、携帯端末装置ＭＴが高速系無線基地局ＡＰのエリア内に移動した場合などに、高速系通信システムを優先的に使用すれば、高速な通信が可能であるという高速系通信システムの利点が生かされる。

【００６２】

【発明の効果】

以上説明したように、請求項１に係る通信システムによれば、セキュリティ情報の通信は、必ず第１の通信網のみによって行われる。よって、第１および第２の通信網のうち、第

１の通信網に比較的セキュリティ性の高い通信網を使用すれば、不正アクセスやハッキング等によるセキュリティ情報の漏洩や改ざんを防止することができる。例えば、現存する通信システムにおいて、携帯電話のサービスを提供する移動体通信網は比較的セキュリティ性が高く、無線ＬＡＮを介して接続可能な高速基幹ネットワークは比較的セキュリティ性が低い。その場合、第１の通信網として移動体通信網、第２の通信網として高速基幹ネットワークを使用すればよい。さらに、現存の無線ＬＡＮのサービスを受けることができるエリアは狭いが、そのエリア内では通常のサービスサーバーとの通信を無線ＬＡＮを介して行うことで、高速な通信が可能であるという高速系通信システムの利点も生かされる。

【図面の簡単な説明】

【図１】実施の形態１に係る無線通信システムの構成を示す図である。

【図２】実施の形態１に係る無線通信システムにおける通信制御動作を示すシーケンス図である。

【図３】実施の形態１に係る無線通信システムにおける携帯端末装置ＭＴの動作を示すフローチャートである。

【図４】実施の形態１に係る無線通信システムにおけるサービスサーバーＳＳの動作を示すフローチャートである。

【図５】実施の形態１に係る無線通信システムにおける効果を説明するためのシーケンス図である。

【図６】実施の形態２に係る無線通信システムにおける通信制御動作を示すシーケンス図である。

【図７】実施の形態２に係る無線通信システムにおける携帯端末装置ＭＴの動作を示すフローチャートである。

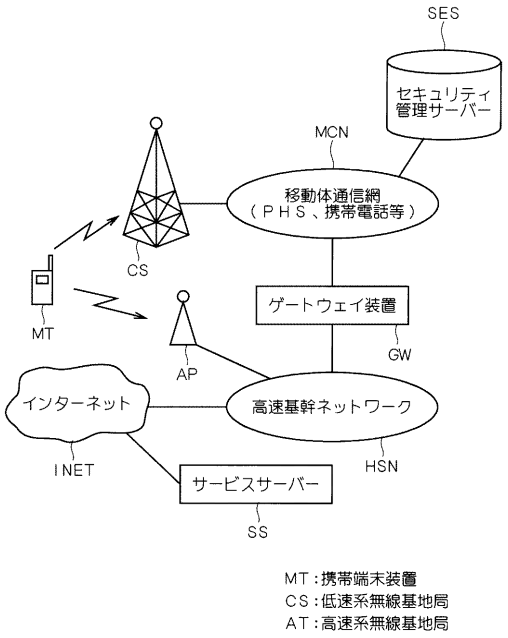
【図８】実施の形態２に係る無線通信システムにおけるサービスサーバーＳＳの動作を示すフローチャートである。

【図９】実施の形態２に係る無線通信システムの効果を説明するためのシーケンス図である。

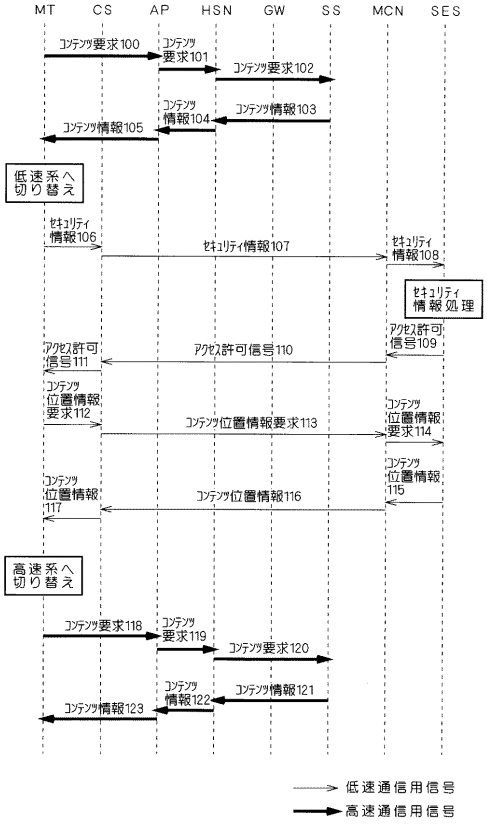
【符号の説明】

ＭＴ　携帯端末装置、ＣＳ　低速系無線基地局、ＭＣＮ　移動体通信網、ＳＥＳ　セキュリティ管理サーバー、ＡＰ　高速系無線基地局、ＨＳＮ　高速基幹ネットワーク、ＧＷ　ゲートウェイ装置、ＩＮＥＴ　インターネット網、ＳＳ　サービスサーバー。

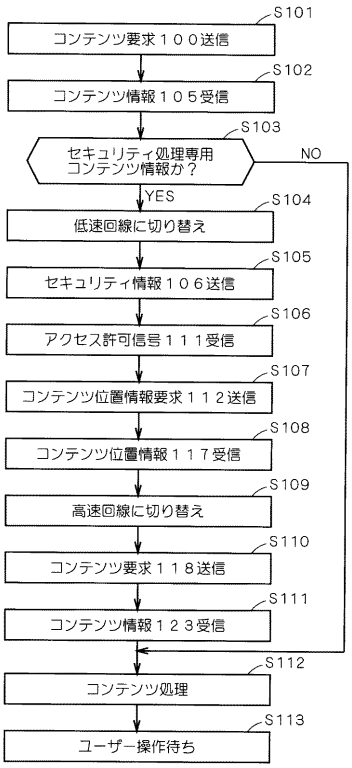
【図１】


SES
セキュリティ管理サーバー
MCN
移動体通信網（ＰＨＳ、携帯電話等）
CS
MT
AP
ゲートウェイ装置
GW
インターネット
高速基幹ネットワーク
INET
HSN
サービスサーバー
SS
MT：携帯端末装置
CS：低速系無線基地局
AT：高速系無線基地局

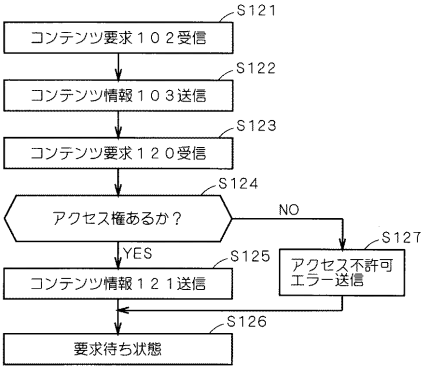
【図２】


MT
CS
AP
HSN
GW
SS
MCN
SES
コンテンツ要求100
コンテンツ要求101
コンテンツ要求102
コンテンツ情報104
コンテンツ情報103
コンテンツ情報105
低速系へ切り替え
セキュリティ情報106
セキュリティ情報107
セキュリティ情報108
セキュリティ情報処理
アクセス許可信号109
アクセス許可信号111
アクセス許可信号110
コンテンツ位置情報要求112
コンテンツ位置情報要求113
コンテンツ位置情報要求114
コンテンツ位置情報115
コンテンツ位置情報116
コンテンツ位置情報117
高速系へ切り替え
コンテンツ要求118
コンテンツ要求119
コンテンツ要求120
コンテンツ情報122
コンテンツ情報121
コンテンツ情報123
低速通信用信号
高速通信用信号

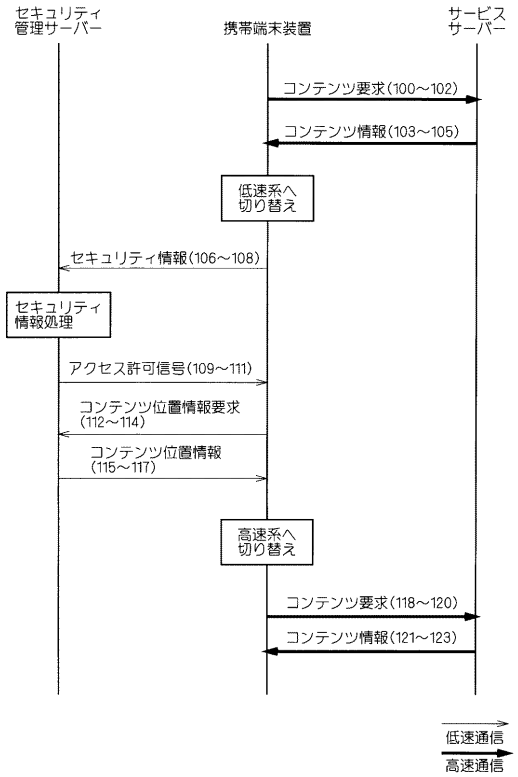
【図３】


S101
コンテンツ要求１００送信
S102
コンテンツ情報１０５受信
S103
セキュリティ処理専用コンテンツ情報か？
NO
YES
S104
低速回線に切り替え
S105
セキュリティ情報１０６送信
S106
アクセス許可信号１１１受信
S107
コンテンツ位置情報要求１１２送信
S108
コンテンツ位置情報１１７受信
S109
高速回線に切り替え
S110
コンテンツ要求１１８送信
S111
コンテンツ情報１２３受信
S112
コンテンツ処理
S113
ユーザー操作待ち

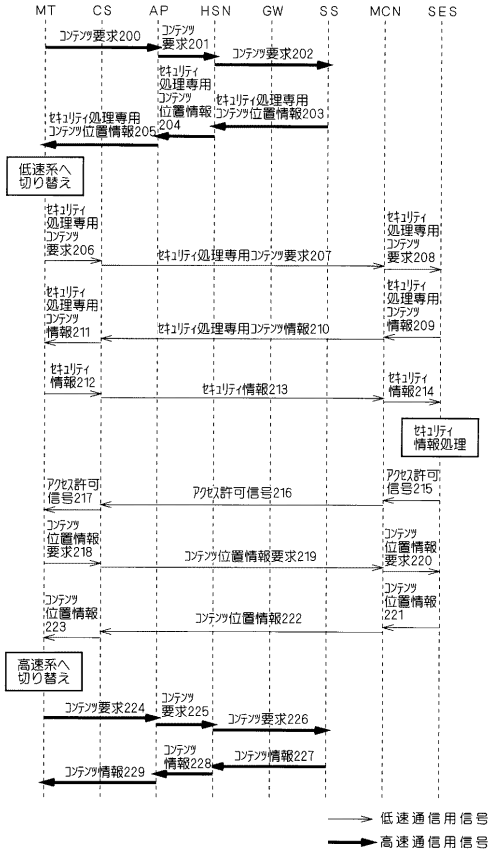
【図４】


S121
コンテンツ要求１０２受信
S122
コンテンツ情報１０３送信
S123
コンテンツ要求１２０受信
S124
アクセス権あるか？
NO
YES
S127
アクセス不許可エラー送信
S125
コンテンツ情報１２１送信
S126
要求待ち状態

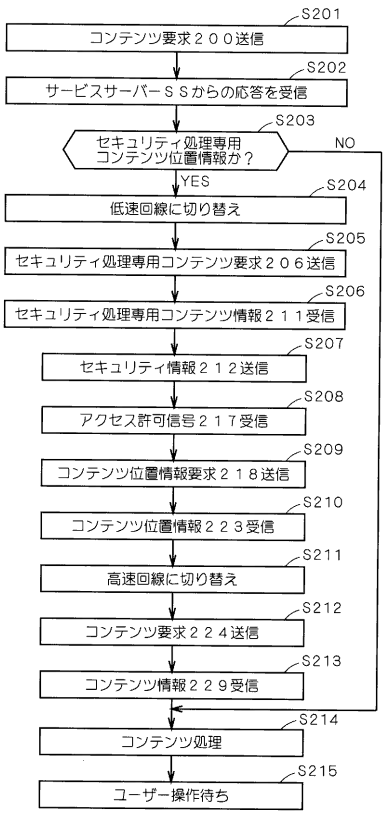
【図５】


セキュリティ管理サーバー
携帯端末装置
サービスサーバー
コンテンツ要求(100～102)
コンテンツ情報(103～105)
低速系へ切り替え
セキュリティ情報(106～108)
セキュリティ情報処理
アクセス許可信号(109～111)
コンテンツ位置情報要求(112～114)
コンテンツ位置情報(115～117)
高速系へ切り替え
コンテンツ要求(118～120)
コンテンツ情報(121～123)
低速通信
高速通信

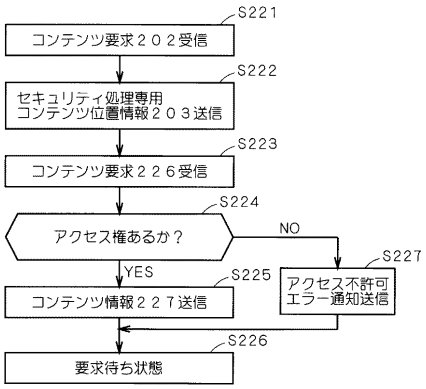
【図６】


MT
CS
AP
HSN
GW
SS
MCN
SES
コンテンツ要求200
コンテンツ要求201
コンテンツ要求202
セキュリティ処理専用コンテンツ位置情報203
セキュリティ処理専用コンテンツ位置情報204
セキュリティ処理専用コンテンツ位置情報205
低速系へ切り替え
セキュリティ処理専用コンテンツ要求206
セキュリティ処理専用コンテンツ要求207
セキュリティ処理専用コンテンツ要求208
セキュリティ処理専用コンテンツ情報209
セキュリティ処理専用コンテンツ情報210
セキュリティ処理専用コンテンツ情報211
セキュリティ情報212
セキュリティ情報213
セキュリティ情報214
セキュリティ情報処理
アクセス許可信号215
アクセス許可信号216
アクセス許可信号217
コンテンツ位置情報要求218
コンテンツ位置情報要求219
コンテンツ位置情報要求220
コンテンツ位置情報221
コンテンツ位置情報222
コンテンツ位置情報223
高速系へ切り替え
コンテンツ要求224
コンテンツ要求225
コンテンツ要求226
コンテンツ情報227
コンテンツ情報228
コンテンツ情報229
低速通信用信号
高速通信用信号

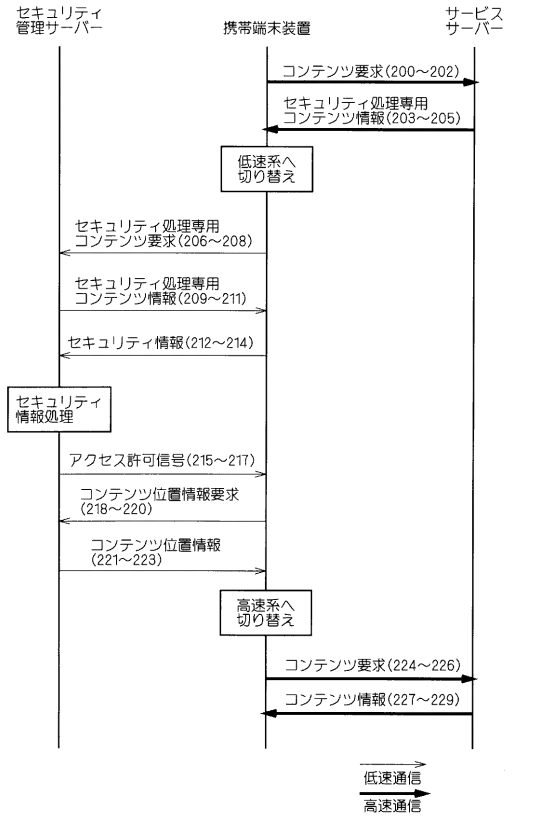
【図７】


S201
コンテンツ要求２００送信
S202
サービスサーバーＳＳからの応答を受信
S203
セキュリティ処理専用コンテンツ位置情報か？
NO
YES
S204
低速回線に切り替え
S205
セキュリティ処理専用コンテンツ要求２０６送信
S206
セキュリティ処理専用コンテンツ情報２１１受信
S207
セキュリティ情報２１２送信
S208
アクセス許可信号２１７受信
S209
コンテンツ位置情報要求２１８送信
S210
コンテンツ位置情報２２３受信
S211
高速回線に切り替え
S212
コンテンツ要求２２４送信
S213
コンテンツ情報２２９受信
S214
コンテンツ処理
S215
ユーザー操作待ち

【図８】


S221
コンテンツ要求２０２受信
S222
セキュリティ処理専用コンテンツ位置情報２０３送信
S223
コンテンツ要求２２６受信
S224
アクセス権あるか？
NO
YES
S225
コンテンツ情報２２７送信
S227
アクセス不許可エラー通知送信
S226
要求待ち状態

【図９】


セキュリティ
管理サーバー
携帯端末装置
サービス
サーバー
コンテンツ要求(200～202)
セキュリティ処理専用
コンテンツ情報(203～205)
低速系へ
切り替え
セキュリティ処理専用
コンテンツ要求(206～208)
セキュリティ処理専用
コンテンツ情報(209～211)
セキュリティ情報(212～214)
セキュリティ
情報処理
アクセス許可信号(215～217)
コンテンツ位置情報要求
(218～220)
コンテンツ位置情報
(221～223)
高速系へ
切り替え
コンテンツ要求(224～226)
コンテンツ情報(227～229)
低速通信
高速通信

フロントページの続き

Ｆターム(参考) 5J104 AA03 AA12 PA02
5K067 AA30 BB04 BB21 EE02 EE10 FF02 FF03