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

特許第6101088号
(P6101088)

(45)発行日　平成29年3月22日(2017.3.22)　(24)登録日　平成29年3月3日(2017.3.3)

(51)Int.Cl.		F I		
H04M 1/66	(2006.01)	H04M	1/66	
H04M 3/00	(2006.01)	H04M	3/00	E
H04W 12/06	(2009.01)	H04W	12/06	

請求項の数 11　(全 28 頁)

(21)出願番号	特願2013-10630(P2013-10630)
(22)出願日	平成25年1月23日(2013.1.23)
(65)公開番号	特開2014-112813(P2014-112813A)
(43)公開日	平成26年6月19日(2014.6.19)
審査請求日	平成27年8月24日(2015.8.24)
(31)優先権主張番号	特願2012-241276(P2012-241276)
(32)優先日	平成24年10月31日(2012.10.31)
(33)優先権主張国	日本国(JP)

(73)特許権者　392026693
株式会社ＮＴＴドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100121083
弁理士　青木　宏義
(74)代理人　100138391
弁理士　天田　昌行
(74)代理人　100158528
弁理士　守屋　芳隆
(72)発明者　石川　秀俊
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　杉山　久人
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
最終頁に続く

(54)【発明の名称】状態変化通知方法、加入者認証装置、状態変化検出装置及び移動通信システム

(57)【特許請求の範囲】
【請求項１】
ユーザ端末に備えられる加入者認証モジュールを用いた状態変化通知方法であって、
前記ユーザ端末が接続するネットワーク装置から送信された認証トークンを受信する工程と、
前記ユーザ端末内の状態に基づいて前記ユーザ端末、前記加入者認証モジュール又はこれらと連携する付帯デバイスの状態変化を検出する工程と、
前記状態変化が検出されている場合、前記ネットワーク装置に対して認証トークンに対する認証応答を送信する際に、当該認証応答に代えて、再同期トークンを送信する工程と、
を有することを特徴とする状態変化通知方法。
【請求項２】
前記状態の変化を検出する工程は、前記ユーザ端末内のシステム領域の状態に基づいて検出することを特徴とする請求項１記載の状態変化通知方法。
【請求項３】
前記再同期トークンは、前記ユーザ端末、加入者認証モジュール又は付帯デバイスにおける権限状態の変化の通知に用いられる通知情報を含むことを特徴とする請求項２に記載の状態変化通知方法。
【請求項４】
前記状態変化は、前記ユーザ端末、加入者認証モジュール若しくは付帯デバイスにおけ

る、権限状態の変化又は問題についての検出結果であることを特徴とする請求項１に記載の状態変化通知方法。
【請求項５】
前記再同期トークンは、前記加入者認証モジュールによる再同期手順に使用される場合と同一のデータ長を有することを特徴とする請求項２に記載の状態変化通知方法。
【請求項６】
前記システム領域の状態は、スーパーユーザ（ｓｕ）ファイルの有無、又は、前記システム領域の書き込み可能状態であることを特徴とする請求項２、請求項３及び請求項５のいずれかに記載の状態変化通知方法。
【請求項７】
ユーザ端末に備えられる加入者認証モジュールを用いた加入者認証装置であって、
前記ユーザ端末が接続するネットワーク装置から送信された認証トークンを受信する受信部と、
前記認証トークンに基づいて、前記ネットワーク装置に対する認証応答を送信する送信部と、
前記ユーザ端末内の状態に基づいて前記ユーザ端末、前記加入者認証モジュール又はこれらと連携する付帯デバイスの状態変化を検出する検出部と、を具備し、
前記送信部は、前記状態変化が検出されている場合、前記ネットワーク装置に対して認証応答を送信する際に、当該認証応答に代えて、再同期トークンを送信することを特徴とする加入者認証装置。
【請求項８】
加入者認証モジュールを備えたユーザ端末とネットワーク経由で接続され、前記ユーザ端末、前記加入者認証モジュール又はこれらと連携する付帯デバイスに状態変化が発生していることを検出する状態変化検出装置であって、
ネットワーク装置から送信された認証トークンに応じて前記ユーザ端末が送出する認証応答を受信すると共に、前記状態変化が発生している場合に前記認証応答に代えて送信された再同期トークンを前記ユーザ端末から受信する受信部と、
前記再同期トークンに基づいて、前記状態変化の発生を検出する検出部と、を具備することを特徴とする状態変化検出装置。
【請求項９】
前記検出部は、前記再同期トークンに前記ユーザ端末、加入者認証モジュール又は付帯デバイスにおける状態の変化の通知に用いられる通知情報が含まれる場合、その通知情報に基づき前記ユーザ端末、加入者認証モジュール又は付帯デバイスにおける権限状態の変化或いは問題があるかを検出することを特徴とする請求項８に記載の状態変化検出装置。
【請求項１０】
前記検出部は、前記再同期トークンが前記加入者認証モジュールによる再同期手順に使用される場合と同一のデータ長を有する場合、該再同期トークンに含まれるシーケンス番号（ＳＱＮ）が正常範囲内であるか否かに基づいて、前記ユーザ端末における権限状態の変化を検出することを特徴とする請求項８に記載の状態変化検出装置。
【請求項１１】
ユーザ端末に備えられる加入者認証モジュール又は付帯デバイスを用いた加入者認証装置と、前記ユーザ端末、加入者認証モジュール又は付帯デバイスにおける状態の変化を検出する状態変化検出装置と、を含む移動通信システムであって、
前記加入者認証装置は、前記ユーザ端末が接続するネットワーク装置から送信された認証トークンを受信する受信部と、前記認証トークンに基づいて、前記ネットワーク装置に対する認証応答を送信する送信部と、を具備し、
前記状態変化検出装置は、前記ユーザ端末内の状態に基づいて前記ユーザ端末、前記加入者認証モジュール又はこれらと連携する付帯デバイスの状態変化を検出する検出部と、を具備し、
前記検出部によって前記状態の変化が検出された場合、前記認証応答に代えて、再同期

トークンを送信することを特徴とする移動通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザ端末又は加入者認証モジュールにおける権限状態等の変化を通知するための状態変化通知方法、加入者認証装置、状態変化検出装置及び移動通信システムに関する。
【背景技術】
【０００２】
IMT-2000（3G）、LTEといった、3GPP標準仕様による移動通信では、加入者認証モジュール（3GPP TS 33.102の3G security contextにおけるクインテットを用いるUSIM（Universal Subscriber Identity Module））と物理的かつ地理的に離れているネットワークノード（ネットワーク機器）との間で相互認証が行われる。
【０００３】
ユーザ端末、加入者認証モジュール及び付帯デバイス（ユーザ端末又は加入者認証モジュールと連携可能なもの）（以下、これらを総称して「ユーザ設備」という）は、通常、加入者認証モジュールを発行したホームネットワーク事業者の事業場とは物理的かつ地理的に離れた地点において、無線通信を介して接続された電気通信設備を経由する形態を通じて、正当ユーザにより当該ユーザ設備の使用がなされる。正当ユーザとは、ホームネットワーク事業者と電気通信役務に関する契約締結を行ったユーザのことである。
【０００４】
従来、日本においてユーザ設備における各種機能実装（デジタルコンテンツ著作権管理機能の実装など）は、専らユーザ端末上で動作するソフトウエアによって機能が実現されている。これはユーザ端末のアーキテクチュアが俗に言うフィーチャーフォンと呼ばれるような、原則としてユーザがユーザ端末のプラットフォームには手を加えることが極めて困難なクローズドなプラットフォームアーキテクチュアであったことに起因している。
【０００５】
近年、市場で急速に普及を遂げているスマートフォンのような、いわゆるオープンプラットフォームに注目した場合に、少なくともホームネットワーク事業者の電気通信設備の観点からは、オープンプラットフォームのユーザ端末は必ずしも信頼されたノードと言い切れない。ユーザ設備においてホームネットワーク事業者から信頼されているノードは唯一、加入者認証モジュールが該当するということもできる。
【０００６】
実際、GSM（登録商標）よりIMT-2000、LTEへと移行してきた、主として欧州のネットワーク事業者にしてみれば、当該ネットワーク事業者の発行した加入者認証モジュールのみがユーザ設備において信頼できるノードとして位置づけられている。このため、Sim Application Toolkit（SAT）、あるいはUniversal Sim Application Toolkit（USAT）が非常に発達する形で当該ネットワーク事業者の提供する独自サービス（例：SMSではない、Emailと接続されたメールサービスなど）が発展してきていた。
【０００７】
従来、オープンプラットフォームでは、ユーザ端末内の機能の利用や設定の変更に係る権限として最高権限であるｒｏｏｔ権限（スーパーユーザ権限）を不正に取得したり、ユーザ端末におけるユーザ権限の制限を不正に取り除いたりする（ジェイルブレイク）などの特権奪取が悪意のユーザによって不正に行なわれる恐れがある。このため、悪意のユーザによる特権奪取によるユーザ端末の不正利用を防止する種々の方策が検討されている（例えば、特許文献１）。
【先行技術文献】
【特許文献】
【０００８】
【特許文献１】特開２０１２－００３４８８号公報

【発明の概要】
【発明が解決しようとする課題】
【０００９】
しかしながら、上記のいずれの形態にあっても、例えば、ユーザ設備が正当な権原を有するユーザ又はその他の者によって当該ネットワーク事業者の意図しない状態に遷移していることを、当該ネットワーク事業者に対して確実に伝達することができる手段は無かった。
【００１０】
その理由としては、例えば、オープンプラットフォームのユーザ端末にあっては、ｒｏｏｔ権限の取得、あるいは、ジェイルブレイクなどという言葉により表現されるように、オープンプラットフォームで実行されている基本システムの特権奪取をすることにより（換言すれば、通常、ユーザが利用可能であり、当該ネットワーク事業者によって当該ユーザに対して許容されている、いわゆるユーザ権限から、特権昇格をすることにより）、概念上、当該オープンプラットフォームの全ファイルシステムへのアクセス及びプロセス制御が可能となる。このため、仮に特権奪取されたことをシステム上で検知をした場合に、当該ネットワーク事業者へ何らかの通報を行うとしても、その特権奪取の通報機構そのものが正常に作動しない（当該通報を抑止する、あるいは改竄した情報を送出する）ことが技術的には可能であった。
【００１１】
本発明は、かかる点に鑑みてなされたものであり、ユーザ端末、加入者認証モジュール又は付帯デバイスにおける権限状態等の状態変化をネットワーク事業者に確実に通知可能な状態変化通知方法、加入者認証装置、状態変化検出装置及び移動通信システム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】
【００１２】
本発明の第１側面に係る状態変化通知方法は、ユーザ端末に備えられる加入者認証モジュールを用いた状態変化通知方法であって、前記ユーザ端末が接続するネットワーク装置から送信された認証トークンを受信する工程と、前記ユーザ端末内の状態に基づいて前記ユーザ端末、前記加入者認証モジュール又はこれらと連携する付帯デバイスの状態変化を検出する工程と、前記状態変化が検出されている場合、前記ネットワーク装置に対して認証トークンに対する認証応答を送信する際に、当該認証応答に代えて、再同期トークンを送信する工程と、を有することを特徴とする。
【００１３】
また、本発明の状態変化通知方法は、ユーザ端末に備えられる加入者認証モジュールを用いた状態変化通知方法であって、前記ユーザ端末が接続するネットワーク装置から送信された認証トークンを受信する工程と、前記ユーザ端末内のシステム領域の状態に基づいて、前記ユーザ端末に関する権限状態の変化（その端末内に備えられる加入者認証モジュールに対する権限を含む）を検出する工程と、前記権限状態の変化が検出された場合、前記認証トークンに応じて、前記ネットワーク装置に対する認証応答に代えて、再同期トークンを送信する工程と、を有することを特徴とする。
【００１４】
本発明の第２側面に係る加入者認証装置は、ユーザ端末に備えられる加入者認証モジュールを用いた加入者認証装置であって、前記ユーザ端末が接続するネットワーク装置から送信された認証トークンを受信する受信部と、前記認証トークンに基づいて、前記ネットワーク装置に対する認証応答を送信する送信部と、前記ユーザ端末内の状態に基づいて前記ユーザ端末、前記加入者認証モジュール又はこれらと連携する付帯デバイスの状態変化を検出する検出部と、を具備し、前記送信部は、前記状態変化が検出されている場合、前記ネットワーク装置に対して認証応答を送信する際に、当該認証応答に代えて、再同期トークンを送信することを特徴とする。
【００１５】

また、本発明の加入者認証装置は、ユーザ端末に備えられる加入者認証モジュールを用いた加入者認証装置であって、前記ユーザ端末が接続するネットワーク装置から送信された認証トークンを受信する受信部と、前記認証トークンに基づいて、前記ネットワーク装置に対する認証応答を送信する送信部と、前記ユーザ端末内のシステム領域の状態に基づいて、前記ユーザ端末における権限状態の変化を検出する検出部と、を具備し、前記送信部は、前記検出部によって前記権限状態の変化が検出された場合、前記認証応答に代えて、再同期トークンを送信することを特徴とする。

【００１６】

本発明の第３側面に係る状態変化検出装置は、加入者認証モジュールを備えたユーザ端末とネットワーク経由で接続され、前記ユーザ端末、前記加入者認証モジュール又はこれらと連携する付帯デバイスに状態変化が発生していることを検出する状態変化検出装置であって、ネットワーク装置から送信された認証トークンに応じて前記ユーザ端末が送出する認証応答を受信すると共に、前記状態変化が発生している場合に前記認証応答に代えて送信された再同期トークンを前記ユーザ端末から受信する受信部と、前記再同期トークンに基づいて、前記状態変化の発生を検出する検出部と、を具備することを特徴とする。

【００１７】

また、本発明の状態変化検出装置は、加入者認証モジュールを備えるユーザ端末における権限状態の変化を検出する状態変化検出装置であって、前記ユーザ端末が接続するネットワーク装置から送信された認証トークンに応じて、該ネットワーク装置に対する認証応答に代えて前記加入者認モジュールから送信された再同期トークンを、前記ネットワーク装置から受信する受信部と、前記再同期トークンに基づいて、前記ユーザ端末における権限状態の変化を検出する検出部と、を具備することを特徴とする。

【００１８】

本発明の第４側面に係る移動通信システムは、ユーザ端末に備えられる加入者認証モジュール又は付帯デバイスを用いた加入者認証装置と、前記ユーザ端末、加入者認証モジュール又は付帯デバイスにおける状態の変化を検出する状態変化検出装置と、を含む移動通信システムであって、前記加入者認証装置は、前記ユーザ端末が接続するネットワーク装置から送信された認証トークンを受信する受信部と、前記認証トークンに基づいて、前記ネットワーク装置に対する認証応答を送信する送信部と、を具備し、前記状態変化検出装置は、前記ユーザ端末内の状態に基づいて前記ユーザ端末、前記加入者認証モジュール又はこれらと連携する付帯デバイスの状態変化を検出する検出部と、を具備し、前記検出部によって前記状態の変化が検出された場合、前記認証応答に代えて、再同期トークンを送信することを特徴とする。

【発明の効果】

【００１９】

本発明によれば、ユーザ端末、加入者認証モジュール又は付帯デバイスにおける権限状態等の状態変化をネットワーク事業者により確実に通知可能な状態変化通知方法、加入者認証装置、状態変化検出装置及び移動通信システムを提供できる。

【図面の簡単な説明】

【００２０】

【図１】相互認証プロセスの一例を示す図である。

【図２Ａ】第１の実施の形態に係る移動通信システムの概略構成図である。

【図２Ｂ】ネットワーク構成にＭＶＮＯの加入者管理サーバまで含んだ移動通信システムの概略構成図である。

【図３】第１の実施の形態に係るユーザ端末及び加入者認証モジュールの機能構成図である。

【図４】第１の実施の形態に係る認証トークン及び認証ベクトルの一例を示す図である。

【図５】第１の実施の形態に係るＨＬＲの機能構成図である。

【図６】第１の実施の形態に係る状態変化検出動作の一例を示すシーケンス図である。

【図７】第１の実施の形態に係る状態変化検出動作の一例を示すシーケンス図である。
【図８】第２の実施の形態に係るユーザ端末及び加入者認証モジュールの機能構成図である。
【図９】第２の実施の形態に係る状態変化検出動作の一例を示すシーケンス図である。
【図１０】第２の実施の形態に係る状態変化検出動作の一例を示すシーケンス図である。
【図１１】携帯電話端末の構成例を示す図である。
【図１２】第３の実施の形態における加入者認証モジュールの機能ブロックの構成図である。
【図１３】第４の実施の形態におけるユーザ端末、加入者認証モジュール及び非接触ＩＣカード機能部の構成を示す図である。
【図１４】第５の実施の形態におけるユーザ端末、加入者認証モジュール及び非接触ＩＣカード機能部の構成を示す図である。
【図１５】ユーザ端末が接触型ＩＣカード決済端末に組み込まれた構成を示す図である。
【発明を実施するための形態】
【００２１】
ユーザ端末がネットワーク事業者の意図しない権限状態に変化している場合に、ユーザ端末の権限状態の変化をネットワーク事業者に確実に通知できない要因は、ｒｏｏｔ権限（スーパーユーザ権限）の不正取得やジェイルブレイクなどの特権奪取や、不正に操作権限が格上げされる特権昇格が行なわれることにより、ネットワーク事業者に対する権限状態の変化の通知機能そのものが正常に動作しない点にあると考えられる。
【００２２】
例えば、ネットワーク事業者に対する権限状態の変化の通知機能としては、端末状態監視アプリケーションを用いて、ＳＭＳ（Short Message Service）あるいはパケット通信上におけるＨＴＴＰ／ＨＴＴＰＳ通信によるネットワーク事業者からの要求に応じて、ユーザ端末において検出された権限状態の変化を、前記監視アプリケーションの機能によりＳＭＳあるいはパケット通信上におけるＨＴＴＰ／ＨＴＴＰＳ通信を介してネットワーク事業者に通知することが考えられる。しかしながら、ユーザ端末において、ｒｏｏｔ権限（スーパーユーザ権限）の不正取得やジェイルブレイクなどの特権奪取や、不正に操作権限が格上げされる特権昇格が行われている場合、ＳＭＳによるネットワーク事業者からの要求に応じた通知機能が不正に抑止されたり、ネットワーク事業者においてユーザ端末における特権奪取や特権昇格などの権限状態の変化を検知できないようにＳＭＳあるいはパケット通信上におけるＨＴＴＰ／ＨＴＴＰＳ通信による通知情報が改竄されたりする恐れがある。また、ローミング時にネットワーク事業者とローミング事業者との間にＳＭＳローミングあるいはパケット通信が許可されていない可能性もある。
【００２３】
このように、ユーザ端末の位置登録後に利用可能となる各種ネットワークサービス（例えば、上記ＳＭＳあるいはパケット通信上におけるＨＴＴＰ／ＨＴＴＰＳ通信）を利用した権限状態の変化の通知機能では、通知機能の不正抑止や通知情報の改竄により、ネットワーク事業者に対する権限状態の変化の通知機能そのものが正常に動作しないという問題点がある。そこで、本発明者らは、各種ネットワークサービスが利用可能となる位置登録前の加入者認証モジュールとネットワークノードとの間の相互認証プロセスにおいて、ユーザ端末における権限状態の変化をネットワーク事業者に通知するという着想を得た。
【００２４】
また、ユーザ設備が正当ユーザ又はその他の者によって当該ネットワーク事業者の意図しない状態に遷移していることを、ネットワーク事業者へ伝達するという観点からは、ユーザ端末における権限状態の変化のみならず、加入者認証モジュール及び付帯デバイス（例えば、非接触ＩＣチップ、外部記憶媒体）、さらには周辺デバイス（例えば、近距離無線通信による接続、非接触ＩＣ技術を用いた接続、充電器などを含む電磁誘導による接続、赤外線接続、ＵＳＢ接続、Ｂｌｕｅｔｏｏｔｈ（登録商標）接続、無線ＬＡＮ接続及びＨＤＭＩ接続など、ユーザ端末と有線又は無線によって接続可能であるような装置類及び

当該装置類に搭載されているソフトウェア）に対する攻撃（例えば、記憶情報の漏洩、改竄及びその他の異常状態）に関する情報（以下、状態変化情報ともいう）についても、ネットワーク事業者へ伝達することが望まれる。

【００２５】

本発明の骨子は、ユーザ端末に備えられる加入者認証モジュールを用いたネットワークノードとの相互認証プロセスにおいて、ユーザ設備が正当ユーザ又はその他の者によって当該ネットワーク事業者の意図しない状態に遷移していることを、ネットワークノードに対して再同期トークン（ＡＵＴＳ）によって伝達することである。

【００２６】

ユーザ端末の権限状態の変化をネットワークノードに通知する状態通知変化方法の場合、前記ユーザ端末が接続するネットワーク装置から送信された認証トークンを受信する工程と、前記ユーザ端末内のシステム領域の状態に基づいて、前記ユーザ端末における権限状態の変化を検出する工程と、前記権限状態の変化が検出された場合、前記認証トークンに応じて、前記ネットワーク装置に対する認証応答に代えて、再同期トークンを送信する工程と、を有することになる。

【００２７】

ユーザ端末の位置登録前の加入者認証モジュールとネットワークノードとの間の相互認証プロセスでは、図１に示すように、ネットワーク側装置（例えば、ＶＬＲやＳＧＳＮ）からの認証トークン（ＡＵＴＮ）に応じて、加入者認証モジュール（ＵＳＩＭ）から認証応答（ＲＥＳ）が送信される。本発明では、相互認証プロセスの中で端末側（加入者認証モジュール）からネットワーク側装置へ返されるこの認証応答（ＲＥＳ）に代えて、再同期トークン（ＡＵＴＳ）を送信することで、ユーザ設備がネットワーク事業者の意図しない状態に遷移していること（ユーザ端末における権限状態の変化を含む）がネットワーク事業者に通知されるようにしている。

【００２８】

これにより、各種ネットワークサービスが利用可能となる位置登録前の加入者認証モジュールとネットワークノードとの間の相互認証プロセスにおいて、ユーザ端末における権限状態の変化等のユーザ設備の状態遷移を、ＭＡＣの付いたＡＵＴＳによりネットワーク事業者に対して通知できるので、通知機能の不正抑止や通知情報の改竄などにより通知機能が正常に動作しなくなるのを回避でき、ユーザ端末における権限状態の変化等のユーザ設備の状態遷移をより確実にネットワーク事業者に通知できる。なお、当然のことながらユーザ端末に電源投入を行って間も無く行う位置登録における相互認証プロセスにおいては、当該ＡＵＴＳがネットワーク側から受理されない限り加入者認証モジュールがユーザ設備の状態遷移を通知し続け、その後、ネットワーク側装置（例えば、ＶＬＲやＳＧＳＮ）から改めて再発行される認証トークン（ＡＵＴＮ）において、前記ユーザ設備の状態遷移を通知に対する受理を意味する情報を受信したことにより、通常の相互認証プロセスの演算結果をネットワークノードに通知する、という手順にすることにより、ユーザ端末操作者に明示することなく、前記ユーザ設備の状態遷移通知を確実にネットワーク側装置（例えば、ＶＬＲやＳＧＳＮ）に対して通知することができ、逆に前記通知が完了するまではユーザ端末の位置登録が完了しないため、ユーザ端末操作者やユーザ端末の各種アプリケーションが実行しようとする通話又はパケット通信が実行できない、という特徴を有することとなる。

【００２９】

以下、本発明の実施の形態について図面を参照して詳細に説明する。なお、本発明の実施の形態では、加入者認証装置が、ユーザ端末の権限状態の変化が検出された場合に、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。この加入者認証装置は、ユーザ端末であってもよいし、ユーザ端末に備えられる加入者認証モジュールであってもよい。以下、第１の実施の形態では、加入者認証装置がユーザ端末である場合を説明し、第２の実施の形態では、加入者認証装置が加入者認証モジュールである場合を説明する。また、第３の実施の形態から第６の実施の形態においては第１の実施の形態又は第２

の実施の形態のいずれかの方法でネットワークノードに対して再同期トークン（ＡＵＴＳ）が送信される。

【００３０】

（第１の実施の形態）

図２Ａは、第１の実施の形態に係る移動通信システムの概略構成図である。図２Ａに示すように、移動通信システム１は、ユーザ端末１０と、ユーザ端末１０に備えられる加入者認証モジュール２０と、ユーザ端末１０が接続する移動通信ネットワーク３０と、移動通信ネットワーク３０に設けられるＶＬＲ（Visitor Location Register）４０と、ＶＬＲ４０に接続されるＨＬＲ（Home Location Register）５０と、ＨＬＲ５０に接続される端末管理サーバ６０と、を含んで構成される。

【００３１】

ユーザ端末（User Equipment）１０は、例えば、携帯電話端末、ノートパソコンなどの端末装置である。ユーザ端末は移動機と呼ばれても良い。ユーザ端末１０は、ＵＭＴＳ（Universal Mobile Telecommunications System）、ＬＴＥ（Long Term Evolution）、ＬＴＥ－Ａ（Long Term Evolution－Advanced）などの各種の通信方式をサポートしている。

【００３２】

加入者認証モジュール２０は、ユーザ端末１０が移動通信ネットワーク３０に接続する場合、ユーザ端末１０の位置登録前に行われる相互認証に用いられるモジュールである。加入者認証モジュール２０は、例えば、ユーザ端末１０に装着可能な接触型ＩＣカードによって構成される。なお、加入者認証モジュール２０は、ＵＳＩＭ（User Subscriber Identity Module）等と呼ばれてもよい。また、加入者認証モジュール２０がユーザ端末１０に備えられる形態は、ユーザ端末１０に装着される形態（例えば、挿入など）であってもよいし、ユーザ端末１０に固定的に埋め込まれる形態であってもよいし、場合によってはＤＩＰなどの樹脂等パッケージに収容されている形状となっているＩＣチップなど、種々の形態を適用可能である。

【００３３】

移動通信ネットワーク３０は、無線基地局（不図示）などを介してユーザ端末１０が接続するネットワークである。ユーザ端末１０間の通信は、移動通信ネットワーク３０を介して行われる。

【００３４】

ＶＬＲ４０は、加入者認証モジュール２０と移動通信ネットワーク３０との間の相互認証に用いられるネットワーク装置の一つである。ＶＬＲ４０を介して、ユーザ端末１０の移動通信ネットワーク３０に対する接続処理（アタッチ処理）や、位置登録処理などが行なわれる。なお、ＶＬＲ４０は、ＭＭＥ（Mobile Management Entity）などと呼ばれても良い。

【００３５】

ＨＬＲ５０は、加入者認証モジュール２０と移動通信ネットワーク３０との間の相互認証の際に、ユーザ端末１０における権限状態の変化を検出する状態変化検出装置である。ＨＬＲ５０を介して、ユーザ端末１０の位置登録処理などが行われる。ＨＬＲ５０は、ＨＳＳ（Home Subscriber Server）などと呼ばれてもよい。

【００３６】

端末管理サーバ６０は、ユーザ端末１０の状態を管理する状態管理装置である。端末管理サーバ６０は、ＨＬＲ５０からの状態変化通知に基づいて、ユーザ端末１０の状態を更新する。端末管理サーバ６０は、ネットワーク事業者によって管理されている。

【００３７】

なお、図２Ａでは、移動通信ネットワーク３０は、単一の通信事業者のネットワークで構成されているが、複数のネットワーク（例えば、ローミング網、ホーム網）を含んでいてもよい。また、無線通信インフラを他社から借り受けて通信サービスを提供している事業者（ＭＶＮＯ：Mobile Virtual Network Operator）の場合、ＨＬＲを独自に保有する

あるいはＨＬＲを有しないなど、様々な形態が想定可能であるが、独自の加入者管理サーバを運用している。

【００３８】

図２Ｂに、ローミング網、ホーム網及びＭＶＮＯの加入者管理サーバまで含んだネットワーク構成を例示する。移動通信ネットワーク３０は、通信インフラまで提供する事業者Ａが運用していて、加入者管理サーバ７０は事業者Ａから通信インフラを借り受けて通信サービスを提供している事業者Ｂによって運用されている。また、ＶＬＲ４１は、海外ローミング網に配置されたネットワーク装置であり、加入者認証モジュール２０と移動通信ネットワーク３０との間の相互認証に用いられる。

【００３９】

次に、図３－図５を参照し、第１の実施の形態に係る移動通信システムの詳細構成を説明する。なお、移動通信システム１を構成する各装置（例えば、ユーザ端末１０、加入者認証モジュール２０、ＶＬＲ４０、ＨＬＲ５０など）は、通信インターフェース、プロセッサ、メモリ、送受信回路などを含むハードウェアを有しており、メモリには、プロセッサによって実行されるソフトウェアモジュールが記憶されている。後述する各装置の機能構成は、上述のハードウェアによって実現されてもよいし、プロセッサによって実行されるソフトウェアモジュールによって実現されてもよいし、両者の組み合わせによって実現されてもよい。

【００４０】

図３は、第１の実施の形態に係るユーザ端末及び加入者認証モジュールの機能構成図である。図３に示すように、ユーザ端末１０は、無線基地局（不図示）を介してネットワークノードと通信を行う通信部１１と、権限状態の変化を検出する検出部１２と、加入者認証モジュール２０とのインターフェース部１３と、判定部１４と、を具備する。

【００４１】

通信部１１は、ＵＭＴＳ、ＬＴＥ、ＬＴＥ－Ａなどの各種方式の移動通信機能を有する。具体的には、通信部１１は、認証プロセスに関する処理として、ＶＬＲ４０からの認証メッセージ（例えば、ユーザ認証要求など）を受信し、当該認証メッセージに含まれる認証パラメータを、インターフェース部１３を介して加入者認証モジュールに対する認証演算コマンドに変換した後、加入者認証モジュール２０に送信する。また、通信部１１は、加入者認証モジュール２０からインターフェース部１３を介して前記認証演算コマンドへの応答受信内容から認証パラメータを抽出し、当該認証パラメータを含む認証メッセージ（例えば、ユーザ認証応答など）を送信する。

【００４２】

ここで、認証パラメータには、例えば、後述する乱数（ＲＡＮＤ：RANDom challenge）、認証トークン（ＡＵＴＮ：Authentication TokeN）、認証応答（ＲＥＳ：authentication RESponse）、再同期トークン（再同期トークン（ＡＵＴＳ）：Re-synchronization Token）などが含まれる。

【００４３】

検出部１２は、ユーザ端末１０における権限状態の変化を検出する。ここで、ユーザ端末１０における権限状態の変化とは、例えば、ユーザ端末１０に実装されたオペレーティングシステムの最高操作権限（例えば、ｒｏｏｔ権限、スーパーユーザ（ｓｕ）権限など）が取得されたこと（特権奪取）や、ユーザ端末１０のユーザ権限がより多くの操作を可能な権限に格上げされたこと（特権昇格）などをいう。なお、検出部１２は、権限状態の変化に限らず、ユーザ端末１０にアプリケーションがダウンロードされた、画像がダウンロードされた、一定の操作を実行した、アプリケーションが実行された、一定の場所に移動した、決済行為を行った、一定の外部機器等との通信が発生した、一定の機器異常状態（例えば、機器故障を検出）に遷移したことなど、ユーザ端末１０の各種状態の変化を検出してもよい。

【００４４】

例えば、検出部１２は、スーパーユーザ（ＳＵ）ファイルがユーザ端末１０内の所定領

域（例えば、システム領域）に生成されているか否かによって、上述の特権奪取や特権昇格を検出してもよい。また、検出部１２は、読み取り専用であるシステム領域が書き込み可能に変更されているかによって、上述の特権奪取や特権昇格を検出してもよい。なお、ユーザ端末１０における権限状態の変化の検出手法は、これに限られるものではない。

【００４５】

検出部１２は、ユーザ端末１０における権限状態の変化を検出すると、判定部１４に検出情報を入力する。ここで、検出情報とは、特権奪取や特権昇格などの上記権限状態の変化が検出されたことを示す情報である。

【００４６】

判定部１４は、検出部１２においてユーザ端末１０における権限状態の変化が検出されているか否かを判定する。具体的には、判定部１４は、検出部１２から検出情報が入力されている場合、インターフェース部１３を介して加入者認証モジュール２０から受信した認証応答（ＲＥＳ）に代えて、再同期トークン（ＡＵＴＳ）を送信するよう、通信部１１に指示する。

【００４７】

ここで、再同期トークン（ＡＵＴＳ）とは、通常、後述する加入者認証モジュール２０における演算処理においてシーケンス番号（ＳＱＮ）が正常範囲でない場合に、加入者認証モジュール２０とＨＬＲ５０との間の再同期手順に使用される。一方、第１の実施の形態に係る再同期トークン（ＡＵＴＳ）は、この再同期手順だけでなく、ユーザ端末１０における権限状態の変化を通知するためにも使用される。

【００４８】

ユーザ端末１０における権限状態の変化を通知するための再同期トークン（ＡＵＴＳ）は、権限状態の変化を通知するための通知情報、例えば、特権奪取や特権昇格などを示すデータ列を含んでもよい。なお、当該再同期トークンは、再同期手順に用いられる場合と同一のデータ長であってもよいし、異なってもよい。

【００４９】

加入者認証モジュール２０は、送受信部２１（受信部、送信部）と、記憶部２２と、演算部２３と、を具備する。

【００５０】

送受信部２１は、ユーザ端末１０のインターフェース部１３と信号を送受信する。具体的には、送受信部２１は、インターフェース部１３から認証パラメータ（例えば、乱数（ＲＡＮＤ）及び認証トークン（ＡＵＴＮ））を受信し、演算部２３に出力する。また、送受信部２１は、演算部２３から入力された認証パラメータ（例えば、認証応答（ＲＥＳ）又は再同期トークン（ＡＵＴＳ））をインターフェース部１３に送信する。

【００５１】

記憶部２２は、ＩＭＳＩ（International Mobile Subscriber Identity）などの加入者識別子や、認証用アルゴリズム及び秘密鍵などを記憶する。

【００５２】

演算部２３は、加入者認証モジュール２０と移動通信ネットワーク３０との間の相互認証のための演算を行う。具体的には、演算部２３は、送受信部２１で受信された乱数（ＲＡＮＤ）及び認証トークン（ＡＵＴＮ）に基づいて、所定の演算を行う。図４Ａを参照し、認証トークン（ＡＵＴＮ）及び認証ベクトル（ＡＶ：Authentication Vector）について説明する。

【００５３】

図４Ａに示すように、認証トークン（ＡＵＴＮ）は、シーケンス番号（ＳＱＮ：SeQuence Number）と匿名キー（ＡＫ：Anonymity Key）との演算結果、認証管理フィールド（ＡＭＦ：Authentication and key Management Field）、メッセージ認証コード（ＭＡＣ：Message Authentication Code）で構成される。

【００５４】

また、図４Ａに示すように、認証ベクトル（ＡＶ）は、クインテットと呼ばれる５つの

認証パラメータ、すなわち、乱数（ＲＡＮＤ）、期待認証応答（ＸＲＥＳ：eXpected authentication RESponse）、秘匿キー（ＣＫ：Cypher Key）、インテグリティキー（ＩＫ：Integrity Key）及び上述の認証トークン（ＡＵＴＮ）で構成される。認証ベクトル（ＡＶ）は、後述するＨＬＲ５０で生成され、ＶＬＲ４０に送信される。また、認証ベクトル（ＡＶ）を構成する認証パラメータのうち、乱数（ＲＡＮＤ）及び認証トークン（ＡＵＴＮ）が、ＶＬＲ４０からユーザ端末１０を介して送受信部２１で受信される。

【００５５】

図４Ｂに示すように、演算部２３は、送受信部２１で受信された乱数（ＲＡＮＤ）に基づいて匿名キー（ＡＫ）を演算し、演算した匿名キー（ＡＫ）に基づいて、送受信部２１で受信された認証トークン（ＡＵＴＮ）からシーケンス番号（ＳＱＮ）を抽出する。

【００５６】

また、図４Ｂに示すように、演算部２３は、送受信部２１で受信された認証トークン（ＡＵＴＮ）から、認証管理フィールド（ＡＭＦ）及びメッセージ認証コード（ＭＡＣ）を抽出する。一方、演算部２３は、抽出されたシーケンス番号（ＳＱＮ）及び認証管理フィールド（ＡＭＦ）と受信された乱数（ＲＡＮＤ）とに基づいて、期待メッセージ認証コード（ＸＭＡＣ：eXpected Message Authentication Code）を演算する。演算された期待メッセージ認証コード（ＸＭＡＣ）と、抽出されたメッセージ認証コード（ＭＡＣ）とが一致するか否かによって、移動通信ネットワーク３０の認証が行なわれる。

【００５７】

また、図４Ｂに示すように、演算部２３は、以上の演算結果に基づいて、ＶＬＲ４０（ネットワーク装置）に対する認証応答（ＲＥＳ）を演算する。具体的には、演算部２３は、期待メッセージ認証コード（ＸＭＡＣ）とメッセージ認証コード（ＭＡＣ）とが一致し、シーケンス番号（ＳＱＮ）が正常範囲内である場合、乱数（ＲＡＮＤ）に基づいて認証応答（ＲＥＳ）を演算する。ここで、認証応答（ＲＥＳ）は、乱数（ＲＡＮＤ）に基づいて演算される所定値である。認証応答（ＲＥＳ）とＨＬＲ５０で生成される期待認証応答（ＸＲＥＳ）とは、後述するように、ＶＬＲ４０などのネットワーク側装置において照合される。認証応答（ＲＥＳ）と期待認証応答（ＸＲＥＳ）とが一致する場合、認証に成功する。

【００５８】

また、演算部２３は、シーケンス番号（ＳＱＮ）が正常範囲でない場合に、加入者認証モジュール２０とＨＬＲ５０との間の再同期手順に用いる再同期トークン（ＡＵＴＳ）を演算する。当該再同期トークン（ＡＵＴＳ）は、シーケンス番号（ＳＱＮ）を含む。

【００５９】

図５は、第１の実施の形態に係るＨＬＲの機能構成図である。図５に示すように、ＨＬＲ５０（状態変化検出装置）は、送受信部５１（受信部）と、認証ベクトル生成部５２と、検出部５３と、を具備する。

【００６０】

送受信部５１は、ＶＬＲ４０や端末管理サーバ６０との間で信号を送受信する。具体的には、送受信部５１は、ＶＬＲ４０からの認証データ要求を受信し、後述する認証ベクトル（ＡＶ）を含む認証データ応答をＶＬＲ４０に送信する。認証データ要求には、加入者識別子又は再同期トークン（ＡＵＴＳ）が含まれてもよい。また、送受信部５１は、後述する検出部５３の指示に基づいて、状態変化通知を端末管理サーバ６０に送信する。

【００６１】

認証ベクトル生成部５２は、送受信部５１で受信された認証データ要求に応じて、加入者認証モジュール２０と移動通信ネットワーク３０との相互認証に用いられる認証ベクトル（ＡＶ）を生成する。具体的には、認証ベクトル生成部５２は、図４Ａに示す認証ベクトル（ＡＶ）を生成し、送受信部５１に出力する。

【００６２】

検出部５３は、送受信部５１で受信された再同期トークン（ＡＵＴＳ）に基づいて、ユーザ端末１０における権限状態の変化を検出する。検出部５３は、ユーザ端末１０におけ

る権限状態の変化を検出すると、送受信部５１を介して端末管理サーバ６０に状態変化通知を送信する。

【００６３】

例えば、検出部５３は、再同期トークン（ＡＵＴＳ）に上述の通知情報が含まれる場合、ユーザ端末１０における権限状態の変化を検出してもよい。上述の通知情報は、ユーザ端末１０における権限状態の変化の通知に用いられる再同期トークン（ＡＵＴＳ）に含まれるが、再同期手順に使用される再同期トークン（ＡＵＴＳ）には、含まれないためである。

【００６４】

また、検出部５３は、再同期トークン（ＡＵＴＳ）に含まれるシーケンス番号（ＳＱＮ）が正常範囲内である場合、ユーザ端末１０における権限状態の変化を検出してもよい。シーケンス番号（ＳＱＮ）が正常範囲内であれば、再同期手順に使用される再同期トークン（ＡＵＴＳ）は送信されないためである。この場合、再同期トークン（ＡＵＴＳ）のデータ長が、再同期手順に用いる場合と同一であっても、ユーザ端末１０における権限状態の変化を検出可能である。

【００６５】

次に、図６及び図７を参照し、第１の実施の形態に係る状態変化通知方法を説明する。なお、第１の実施の形態に係る状態通知方法は、図２に示す移動通信システム１で用いられる。

【００６６】

図６に示すように、ユーザ端末１０は、自端末における権限状態の変化を検出する（ステップＳ１０１）。ここで、ユーザ端末１０における権限状態の変化とは、上述の特権奪取や特権昇格などである。

【００６７】

ユーザ端末１０がネットワーク事業者で利用可能となるためには、所定の時期に加入者認証モジュール２０を用いて、加入者認証モジュール２０に格納されている固有番号（例えば、ＩＭＳＩ、ＴＭＳＩ）によりネットワークノード（ＨＬＲ５０）に対して位置登録に付随した認証演算（電源ON時、圏内復旧時、一定期間経過後の周期的位置登録）又は認証演算（発着信時）を行わなければならない。ユーザ端末１０は、所定タイミングで、ＶＬＲ４０に対して接続要求（アタッチ）又は発着信処理を行う（ステップＳ１０２）。ここで、所定タイミングとは、例えば、移動通信ネットワーク３０に対する位置登録に付随した認証演算に関するネットワーク接続要求、電話又はパケット通信等を発信するユーザ操作、あるいはネットワーク側からの着信要求が受け付けられた場合である。接続要求には、加入者認証モジュール２０の記憶部２２で記憶される加入者識別子（例えば、ＩＭＳＩ、ＴＭＳＩ）が含まれてもよい。

【００６８】

ＶＬＲ４０は、ユーザ端末１０からの接続要求に応じて、ＨＬＲ５０に対して、認証データ要求を送信する（ステップＳ１０３）。ここで、認証データ要求とは、加入者認証モジュール２０を認証するための認証ベクトルを要求するものであり、加入者識別子（例えば、ＩＭＳＩ）を含む。

【００６９】

ＨＬＲ５０は、ＶＬＲ４０からの認証データ要求に応じて、認証ベクトル（ＡＶ）を生成する（ステップＳ１０４）。具体的には、ＨＬＲ５０は、認証データ要求に含まれる加入者識別子（例えば、ＩＭＳＩ）に基づいて、認証ベクトル（ＡＶ）を生成する。図４Ａに示すように、各認証ベクトル（ＡＶ）は、乱数（ＲＡＮＤ）、期待認証応答（ＸＲＥＳ）、秘匿キー（ＣＫ）、インテグリティキー（ＩＫ）及び認証トークン（ＡＵＴＮ）で構成される。

【００７０】

ＨＬＲ５０は、生成された認証ベクトル（ＡＶ）を含む認証データ応答を、ＶＬＲ４０に送信する（ステップＳ１０５）。ＶＬＲ４０は、ＨＬＲ５０で生成された認証ベクトル

（ＡＶ）を構成する５つの認証パラメータのうち、乱数（ＲＡＮＤ）及び認証トークン（ＡＵＴＮ）をユーザ認証要求に含めて、ユーザ端末１０に送信する（ステップＳ１０６）。ユーザ端末１０は、ＶＬＲ４０からの認証要求に含まれる乱数（ＲＡＮＤ）及び認証トークン（ＡＵＴＮ）を加入者認証モジュール２０に送信する（ステップＳ１０７）。

【００７１】

加入者認証モジュール２０は、ユーザ端末１０からの認証トークン（ＡＵＴＮ）に基づいて、所定の演算を行い、演算結果に基づいて、ＶＬＲ４０に対する認証応答（ＲＥＳ）を演算する（ステップＳ１０８）。

【００７２】

具体的には、加入者認証モジュール２０は、図４Ｂに示すように、乱数（ＲＡＮＤ）に基づいて匿名キー（ＡＫ）を演算し、演算された匿名キー（ＡＫ）に基づいて認証トークン（ＡＵＴＮ）からシーケンス番号（ＳＱＮ）を抽出する。また、加入者認証モジュール２０は、認証トークン（ＡＴＵＮ）から認証管理フィールド（ＡＭＦ）及びメッセージ認証コード（ＭＡＣ）を抽出する。一方、加入者認証モジュール２０は、認証トークン（ＡＵＴＮ）から抽出されたシーケンス番号（ＳＱＮ）及び認証管理フィールド（ＡＭＦ）と乱数（ＲＡＮＤ）とに基づいて期待メッセージ認証コード（ＸＭＡＣ）を演算する。

【００７３】

また、加入者認証モジュール２０は、演算された期待メッセージ認証コード（ＸＭＡＣ）が、抽出されたメッセージ認証コード（ＭＡＣ）と一致するか否かを検証する。両者が一致しない場合、移動通信ネットワーク３０の認証に失敗したことを示す認証失敗メッセージ（不図示）が送信され、本動作は終了する。ここでは、両者が一致するので、本動作は継続する。

【００７４】

また、加入者認証モジュール２０は、メッセージ認証コード（ＭＡＣ）の検証に成功すると、抽出されたシーケンス番号（ＳＱＮ）が正常範囲内であるか否かを検証する。シーケンス番号（ＳＱＮ）が正常範囲内でない場合、このシーケンス番号（ＳＱＮ）を含む再同期トークン（ＡＵＴＳ）が送信され、本動作は終了する。この再同期トークン（ＡＵＴＳ）は、加入者認証モジュール２０とＨＬＲ５０との間の再同期手順に使用される。ここでは、シーケンス番号（ＳＱＮ）は正常範囲内であるので、本動作は継続する。

【００７５】

また、加入者認証モジュール２０は、シーケンス番号（ＳＱＮ）の検証に成功すると、ＶＬＲ４０に対する認証応答（ＲＥＳ）を演算する。

【００７６】

図７に示すように、加入者認証モジュール２０は、ステップＳ１０８におけるメッセージ認証コード（ＭＡＣ）及びシーケンス番号（ＳＱＮ）の検証に成功すると、ステップＳ１０８で演算された認証応答（ＲＥＳ）をユーザ端末１０に送信する（ステップＳ１０９）。

【００７７】

ユーザ端末１０は、加入者認証モジュール２０からの認証応答（ＲＥＳ）に応じて、自端末における権限状態の変化が検出されているか否かを判定する（ステップＳ１１０）。

【００７８】

ユーザ端末１０における権限状態の変化が検出されていない場合（ステップＳ１１０；ＮＯ）、ユーザ端末１０は、加入者認証モジュール２０から受信した認証応答（ＲＥＳ）をユーザ認証応答に含めて、ＶＬＲ４０に送信する（ステップＳ１１１）。

【００７９】

ＶＬＲ４０は、ユーザ端末１０からのユーザ認証応答に含まれる認証応答（ＲＥＳ）が、ＨＬＲ５０から受信した認証ベクトル（ＡＶ）を構成する期待認証応答（ＸＲＥＳ）と一致するか否かを検証する（ステップＳ１１２）。両者が一致しない場合、加入者認証モジュール２０の認証が失敗し、本動作は終了する。一方、両者が一致する場合、加入者認証モジュール２０の認証が成功し、ＶＬＲ４０とＨＬＲ５０との間で位置登録処理が行な

われる（ステップＳ１１３）。位置登録処理が完了すると、ユーザ端末１０が、種々のネットワークサービスを利用可能となる。

【００８０】

一方、ユーザ端末１０における権限状態の変化が検出されている場合（ステップＳ１１０；ＹＥＳ）、ユーザ端末１０は、加入者認証モジュール２０から受信した認証応答（ＲＥＳ）に代えて、再同期トークン（ＡＵＴＳ）をＶＬＲ４０に送信する（ステップＳ１１４）。ここでは、再同期トークン（ＡＵＴＳ）は、ユーザ端末１０における権限状態の変化を通知するために使用される。この再同期トークン（ＡＵＴＳ）には、権限状態の変化の通知に用いられることを明示する通知情報、例えば、特権奪取や特権昇格などを示すデータ列が含まれてもよい。

【００８１】

ＶＬＲ４０は、ユーザ端末１０からの再同期トークン（ＡＵＴＳ）を認証データ要求に含めて、ＨＬＲ５０に送信する（ステップＳ１１５）。

【００８２】

ＨＬＲ５０は、ＶＬＲ４０からの認証データ要求に含まれる再同期トークン（ＡＵＴＳ）に基づいて、ユーザ端末１０における権限状態の変化を検出する（ステップＳ１１６）。例えば、ＨＬＲ５０は、再同期トークン（ＡＵＴＳ）に上述の通知情報が含まれる場合、ユーザ端末１０における権限状態の変化を検出してもよい。或いは、ＨＬＲ５０は、再同期トークン（ＡＵＴＳ）に含まれるシーケンス番号（ＳＱＮ）が正常範囲内である場合、ユーザ端末１０における権限状態の変化を検出してもよい。

【００８３】

ＨＬＲ５０は、ユーザ端末１０における権限状態の変化を検出すると、その旨を示す状態変化通知を端末管理サーバ６０に送信する（ステップＳ１１７）。端末管理サーバ６０は、ＨＬＲ５０からの状態変化通知に応じて、ユーザ端末１０についての端末管理情報を更新する（ステップＳ１１８）。

【００８４】

また、図２Ｂに示すネットワーク構成において、ユーザ端末１０における権限状態が変化しており、かつ、例えばローミング網のＶＬＲ４１を経由して相互認証手順が実行されているものとする。この場合、権限状態の変化を検出したユーザ端末１０は、ＶＬＲ４０に対する認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。正常な認証応答（ＲＥＳ）はローミング網のＶＬＲ４１で認証処理されてＨＬＲ５０まで伝達されないが、再同期トークン（ＡＵＴＳ）はＨＬＲ５０まで伝達される。したがって、再同期トークン（ＡＵＴＳ）を使ってユーザ端末１０における権限状態の変化を伝達する仕組みは、確実にＨＬＲ５０まで伝達する点で極めて有効である。

【００８５】

また、ホームネットワーク事業者Ａから通信インフラを借り受けている事業者Ｂが運営する加入者管理サーバ７０では権限状態の変化を通知する再同期トークン（ＡＵＴＳ）を検出して、ユーザ端末１０の状態変化を状態管理サーバ（特権奪取状況を管理するサーバであって、ホームネットワーク事業者Ｂ内の設備として設置されるか又は通信回線等を介して何らかの管理主体（例えば、当該ユーザ設備を所有又は管理する企業など））が設置している設備に伝達する。

【００８６】

第１の実施の形態に係る移動通信システムによれば、ユーザ端末１０が、ＶＬＲ４０に対する認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信することで、ユーザ端末１０における権限状態の変化をＨＬＲ５０に通知する。これにより、各種ネットワークサービスが利用可能となる位置登録前の加入者認証モジュール２０と移動通信ネットワーク３０との間の相互認証の際に、ユーザ端末１０における権限状態の変化をＨＬＲ５０に対して通知できるので、通知機能の不正抑止や通知情報の改竄などにより通知機能が正常に動作しなくなるのを回避でき、ユーザ端末における権限状態の変化をより確実にネットワーク事業者に通知できる。

【００８７】
すなわち、仮にネットワークノードからは信頼のないユーザ端末（例えば、特権奪取状態であり、当該特権奪取状態であることをネットワーク事業者等のユーザ端末管理者へ通報する機能が抑止されている可能性のあるユーザ端末、を含む）であったとしても、ネットワークノード（ＨＬＲ５０）に位置登録をしない限りは、あらゆる通話及び通信（ＳＭＳの他に、いわゆるパケット通信も含む）の実行は当該ユーザ端末においては不可能である。本実施の形態は、この位置登録の段階で特権奪取の通報を実施してしまうことに加えて、当該再同期トークン（ＡＵＴＳ）の検知が仮に可能であったとしても改竄又は阻止はＭＡＣに基づくＨＬＲ５０における検出が機能するためユーザ端末側では事実上不可能であることから、加入者認証モジュール２０で生成された当該再同期トークン（ＡＵＴＳ）は中継ノードの有無や数に関わらず透過的に確実に伝達される。仮に、当該再同期トークン（ＡＵＴＳ）を改竄した場合は、単純に当該加入者認証モジュール２０を含むユーザ端末１０の位置登録が結果的に不可能になる。このため、ユーザにとってはネットワーク接続以外での利用を前提としなければならず、もし当該再同期トークン（ＡＵＴＳ）の発行を阻止した場合であっても同様に位置登録が単純に不可能になるので、当該再同期トークン（ＡＵＴＳ）に関して、何らユーザ端末側では手を加えるべき有利な要因があるということは判断できないと考えられる。

【００８８】
また、第１の実施の形態に係る移動通信システムでは、ＶＬＲ４０までしか到達しない認証応答（ＲＥＳ）ではなく、ＨＬＲ５０まで到達する再同期トークン（ＡＵＴＳ）を用いて、ユーザ端末１０における権限状態の変化をＨＬＲ５０に対して通知するので、例えば、海外ローミングによる接続を行う場合であっても、より確実にネットワーク事業者にユーザ端末１０における権限状態の変化を通知できる。

【００８９】
すなわち、再同期トークン（ＡＵＴＳ）の返却は加入者認証モジュール２０の所属するホーム網だけでなくローミング網（ただし、3GPP TS 33.102のクインテットによる認証を実施しているネットワークノードに限る）おいても再同期トークン（ＡＵＴＳ）の発行及び受付が可能であり、当該再同期トークン（ＡＵＴＳ）はホーム網に対して確実に伝達されることが保証されている。仮に、ホーム網に対して再同期トークン（ＡＵＴＳ）を伝達しないローミング網については、当該ユーザ端末１０からの呼接続が達成不可能ということとなる。事業者間精算による通話料収入が当該ローミング網においては見込めないこととなるため、通常は再同期トークン（ＡＵＴＳ）を確実に伝達する設計運用となるであろうことがローミング網の設計として期待される。

【００９０】
（第２の実施の形態）
第１の実施の形態では、ユーザ端末１０における権限状態の変化が検出されている場合、ユーザ端末１０が、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。一方、第２の実施の形態では、同様の場合、加入者認証モジュール２０が、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する点で、第１の実施の形態と異なる。以下では、第２の実施の形態について、第１の実施の形態との相違点を中心に説明する。

【００９１】
図８は、第２の実施の形態に係るユーザ端末及び加入者認証モジュールの機能構成図である。図８に示すように、第２の実施の形態に係るユーザ端末１０は、通信部１１と、検出部１２と、インターフェース部１３とを具備する。すなわち、第２の実施の形態に係るユーザ端末１０は、判定部１４を具備しなくともよい。

【００９２】
第２の実施の形態において、検出部１２は、ユーザ端末１０における権限状態の変化を検出すると、インターフェース部１３を介して加入者認証モジュール２０に検出情報を送信する。上述のように、検出情報とは、特権奪取や特権昇格などの上記権限状態の変化が

検出されたことを示す状態変化情報である。例えば、検出情報は、加入者認証モジュール２０によって発行されるプロアクティブコマンドを用いて送信されてもよい。

【００９３】

第２の実施の形態に係る加入者認証モジュール２０は、送受信部２１と、記憶部２２と、演算部２３とに加えて、判定部２５を具備する。第２の実施の形態では、ユーザ端末１０における権限状態の変化が発生したか否かの判定、すなわち、認証応答（ＲＥＳ）に代えて、再同期トークン（ＡＵＴＳ）を送信するかの判定は、加入者認証モジュール２０で行われる。このため、送受信部２１は、ユーザ端末１０の検出部１２からの検出情報を、インターフェース部１３を介して受信し、記憶部２２に出力する。記憶部２２は、送受信部２１から入力された検出情報を記憶する。

【００９４】

判定部２５は、記憶部２２を参照して、ユーザ端末１０における権限状態の変化が検出されているか否かを判定する。具体的には、判定部２５は、上述の検出情報が記憶部２２に記憶されている場合、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信するよう、演算部２３に指示する。

【００９５】

なお、認証応答（ＲＥＳ）に代えて送信される再同期トークン（ＡＵＴＳ）は、権限状態の変化を通知するために使用される通知情報、例えば、特権奪取や特権昇格などを示すデータ列を含んでもよい。なお、当該再同期トークンは、再同期手順に用いられる場合と同一のデータ長であってもよいし、異なってもよい。

【００９６】

次に、図９及び図１０を参照し、第２の実施の形態に係る状態変化通知方法を説明する。図９に示すように、第２の実施の形態では、ステップＳ２０１においてユーザ端末１０における権限状態の変化が検出された場合、ユーザ端末１０は、権限状態の変化が検出されたことを示す検出情報を加入者認証モジュール２０に送信する（ステップＳ２０２）。加入者認証モジュール２０は、ユーザ端末１０から送信された検出情報を記憶部２２に記憶させる。なお、図９のステップＳ２０３－Ｓ２０９は、図６のステップＳ１０２－Ｓ１０８と同様であるため説明を省略する。

【００９７】

図１０に示すように、加入者認証モジュール２０は、ステップＳ２０９におけるメッセージ認証コード（ＭＡＣ）及びシーケンス番号（ＳＱＮ）の検証に成功すると、ユーザ端末１０における権限状態の変化が検出されているか否かを判定する（ステップＳ２１０）。具体的には、加入者認証モジュール２０は、ユーザ端末１０から送信された検出情報が記憶部２２に記憶されているか否かを判定する。

【００９８】

ユーザ端末１０における権限状態の変化が検出されていない場合（ステップＳ２１０；ＮＯ）、加入者認証モジュール２０は、ステップＳ２０９で演算された認証応答（ＲＥＳ）をユーザ端末１０に送信する（ステップＳ２１１）。なお、図１０のステップＳ２１２－Ｓ２１４は、図７のステップＳ１１１－Ｓ１１３と同様であるため、説明を省略する。

【００９９】

一方、ユーザ端末１０における権限状態の変化が検出されている場合（ステップＳ２１０；ＹＥＳ）、加入者認証モジュール２０は、ステップＳ２０９で演算された認証応答（ＲＥＳ）に代えて、再同期トークン（ＡＵＴＳ）をユーザ端末１０に送信する（ステップＳ２１５）。なお、ステップＳ２１６－Ｓ２２０は、図７のステップＳ１１４－Ｓ１１８と同様であるため、説明を省略する。

【０１００】

第２の実施の形態に係る移動通信システムによれば、加入者認証モジュール２０が、ＶＬＲ４０に対する認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信することで、自端末における権限状態の変化をＨＬＲ５０に通知する。これにより、各種ネットワークサービスが利用可能となる位置登録前の加入者認証モジュール２０と移動通信ネッ

トワーク３０との間の相互認証の際に、ユーザ端末１０における権限状態の変化をＨＬＲ５０に対して通知できるので、通知機能の不正抑止や通知情報の改竄などにより通知機能が正常に動作しなくなるのを回避でき、ユーザ端末における権限状態の変化をより確実にネットワーク事業者に通知できる。

【０１０１】

次に、ユーザ設備である加入者認証モジュール又は付帯デバイスがネットワーク事業者の意図しない状態に遷移している場合の通知方法について、第３の実施の形態から第６の実施の形態として説明する。

【０１０２】

(第３の実施の形態)

第３の実施の形態は、加入者認証モジュール２０における状態変化（ネットワーク事業者の意図しない状態に遷移）が検出されている場合、加入者認証モジュール２０が、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。

【０１０３】

加入者認証モジュールは、ホーム網（あるいはＭＶＮＯ）を運営する事業者とユーザとの回線契約に付帯して発行され、加入者認証モジュールの所有権をホーム網事業者が有しているのが一般的である。このことに鑑みると、加入者認証モジュールへの不正アクセス（認証アルゴリズムの解析、秘密鍵の解析、その他加入者認証モジュールが有する各種セキュリティ機能）あるいは不正改造防止（加入者認証モジュールが保有するデータの所定の権限を伴わない状態での読み出し、改竄、盗用を含む）を担保するために、加入者認証モジュールであるＩＣカード内部の情報漏洩、改竄及びその他異常動作に関連したリスク（問題）を検出してＨＬＲ等へ通報することは非常に有意義である。そこで、ＩＣカードに対する攻撃を検知した場合は、加入者認証モジュール内部で状態変化を変化させておき、次に再同期トークン（ＡＵＴＳ）を発行可能なタイミングで状態変化を示す再同期トークン（ＡＵＴＳ）を送出することが有効である。

【０１０４】

本例ではユーザ端末１０として携帯電話端末を例に説明する。図１１は携帯電話端末１００の構成例を示している。携帯電話端末１００は、無線部１０１、表示操作部１０２、通信制御部１０３、メモリ部１０４、加入者認証モジュール通信制御部１０５を備えている。無線部１０１は、無線基地局などの無線通信設備との間で無線通信を行う機能部分であり、通信制御部１０５はＵＭＴＳ、ＬＴＥ又はＬＴＥ－Ａなどの移動通信方式に基づいてネットワークノード（不図示の無線基地局）、ＶＬＲ４０、ＨＬＲ５０との間の通信を制御する機能部分である。無線部１０１及び通信制御部１０３が、図８に示す通信部１１に相当する。表示操作部１０２はユーザが操作する操作画面を制御する機能部分であり、メモリ部１０４は各種のプログラムの他に、特に認証に関する情報が記憶される。加入者認証モジュール通信制御部１０５は、携帯電話端末１００に備えられる加入者認証モジュール２００との間のデータ伝送を制御するインターフェース部であり、図８に示すインターフェース部１３に相当する。本例では携帯電話端末１００は、端末側の権限状態の変化を検出する検出部は備えていないので、携帯電話端末１００から加入者認証モジュール２００に対して権限状態に関する検出結果は通知されない。

【０１０５】

図１２は加入者認証モジュール２００の機能ブロックの構成図である。図８に示す加入者認証モジュール２０と同一機能を有する部分には同一符号を付している。加入者認証モジュール２００は、送受信部２１、記憶部２２、演算部２３、判定部２５及び検出部２４を備えている。送受信部２１は、移動通信ネットワーク３０と加入者認証モジュール２００との間の相互認証プロセスにおいて携帯電話端末１００のインターフェース部１３との間で認証パラメータを送受信する。記憶部２２は、ＩＭＳＩなどの加入者識別子、認証用アルゴリズムなどを記憶し、演算部２３は、加入者認証モジュール２００と移動通信ネットワーク３０との間の相互認証のための演算を行う。検出部２４は、加入者認証モジュール２００に対する物理的攻撃又はソフト的な攻撃を検知する。物理的攻撃としては異常ク

ロック、異常電圧及び異常電流の印加、光又は電磁気の照射による故障動作誘発、情報改変又はソフトウェア破壊、ファイルシステム破壊のほかに、切断、研削等による物理的な攻撃が挙げられる。また、ソフト的な攻撃としてはコンピュータからのVerify PINコマンド、Authenticate コマンド等の各種コマンドの数次にわたる繰り返し実行、その他コマンドインタフェースの通信規約に抵触又は逸脱するようなコマンド実行が挙げられる。検出部２４は、これらの攻撃を検出すると、判定部２５が状態変化を示す状態変化情報を記憶部２２に書き込むようにしている。送受信部２１は、認証応答（ＲＥＳ）を発行する際に、記憶部２２に状態変化を示す状態変化情報が記憶されていれば、認証応答（ＲＥＳ）に代えて、再同期トークン（ＡＵＴＳ）を送信する。図１１に示すように、携帯電話端末１００の加入者認証モジュール通信制御部１０５が加入者認証モジュール２００から再同期トークン（ＡＵＴＳ）を受け取る。無線部１０１及び通信制御部１０３によって、再同期トークン（ＡＵＴＳ）が移動通信ネットワーク３０へ伝達される。以降の処理は、第２の実施の形態と同じである。

【０１０６】

このように、加入者認証モジュール２００に対する攻撃を検知した場合は、加入者認証モジュール内部で状態変化を記憶しておき、次に認証応答（ＲＥＳ）を発行する際に、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を発行することで、加入者認証モジュール２００に対する攻撃をＨＬＲ４０（４１）まで確実に伝達することができる。

【０１０７】

なお、再同期トークン（ＡＵＴＳ）であることを表示した上で、その内部データに状態が変化していること（例えば、攻撃を受けた履歴がある旨）を表示するデータ列を挿入して、再同期トークン（ＡＵＴＳ）として規定されている所定データ長のデータ列の形式で、当該ネットワーク事業者のネットワークノード（ＨＬＲ４０，４１）に返却をするようにしても良い。また、ＨＬＲ４０，４１において当該加入者認証モジュールの機能の一部又は全部を停止させる必要があると判断した場合は、次回のＡＶ生成時にＡＵＴＳにおいて所定の情報を含めることにより、再発行したＡＶを受信した加入者認証モジュールの機能の一部又は全部を停止させることにつなげてもよい。

【０１０８】

（第４の実施の形態）

ユーザ端末１０に、例えば、交通乗車券等にも使用することのできる非接触ＩＣカード（例えば、FeliCa（登録商標））機能を備えることができる。この非接触ＩＣカードはユーザ端末１０又は加入者認証モジュール２０と連携して決済サービス等をユーザに提供する付帯デバイスである。

【０１０９】

非接触ＩＣカード機能を実現している非接触ＩＣチップは、ＩＣカードに対する攻撃を検知する機能を備えており、当該機能を用いて攻撃を検知した場合に、ユーザ端末１０経由で加入者認証モジュール２０に対して当該非接触ＩＣカードにおける状態変化を伝達して、ユーザ端末１０の状態変化の例に準じて、加入者認証モジュール２０より状態変化伝達のための再同期トークン（ＡＵＴＳ）を送出する。

【０１１０】

図１３は第４の実施の形態に係るユーザ端末、加入者認証モジュール及び非接触ＩＣカード機能部の構成を示している。

【０１１１】

第４の実施の形態は、付帯デバイスにおける状態変化（ネットワーク事業者の意図しない状態に遷移）が検出されている場合、ユーザ端末１０又は加入者認証モジュール２０が、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。

【０１１２】

第４の実施の形態に係るユーザ端末１０は、ユーザ端末１０に非接触ＩＣカード機能部８０を備えている。ユーザ端末１０は、移動通信ネットワーク３０と通信するために通信部１１と、加入者認証モジュール２０、非接触ＩＣカード機能部８０との間でデータ伝送

するためのインターフェース部１３とを備える。なお、本実施の形態はユーザ端末１０における権限状態の変化は検出しない例を示しているため、図３に示されていた検出部１２、判定部１４は備えていない。

【０１１３】

加入者認証モジュール２０は、送受信部２１と、記憶部２２と、演算部２３とを備えている。第４の実施の形態では、主に非接触ＩＣカード機能部８０における状態変化を検出してネットワークノードへ伝達することについて説明する。そのため、加入者認証モジュール２０は、図１２に示す構成と同様であっても良いが、ここでは説明を省略する。

【０１１４】

非接触ＩＣカード機能部８０は、無線・有線送受信部８１、記憶部８２、演算部８３、検出部８４及び判定部８５を備える。無線・有線送受信部８１は、リーダ・ライタから送信されるキャリアの変調によりリーダ・ライタとの間で通信を行い、非接触ＩＣカード機能部８０（記憶部８２）に対してバリューの書き込み等が行なわれる。記憶部８２は、バリュー情報の他に、認証に必要な情報が記憶されると共に、非接触ＩＣカード機能部８０における状態変化（ネットワーク事業者の意図しない状態に遷移）が検出された場合には状態変化情報が記憶される。演算部８３は、非接触ＩＣカード機能部８０と非接触通信するリーダ・ライタとの間の相互認証やデータの暗号化及びＭＡＣ付加のための演算を行う。検出部８４は、第３の実施の形態で説明した加入者認証モジュール２０と同様に、非接触ＩＣカード機能部８０に対する物理的攻撃又はソフト的な攻撃を検知する。判定部８５は、検出部８４によって攻撃が検出された場合に状態変化を示す状態変化情報を記憶部８２に書き込むようにしている。無線・有線送受信部８１は、所定の契機（例えば、非接触ＩＣ機能部８０に対するインタフェース部１３からの情報アクセスであって、ユーザ端末１０にあるアプリケーションからの要求に基づく）で状態変化を示す状態変化情報をユーザ端末１０へ通知する。ユーザ端末１０の通信部１１は、加入者認証モジュール２０が認証応答（ＲＥＳ）を発行する際に非接触ＩＣカード機能部８０から状態変化を示す状態変化情報が通知されていれば、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。又は、第２の実施の形態と同様の通知方法を適用することもできる。すなわち、加入者認証モジュール２０が非接触ＩＣカード機能部８０の状態変化情報をユーザ端末１０経由で受け取り、位置登録時等の相互認証プロセスにおいて認証応答（ＲＥＳ）を発行する際に、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。これにより、加入者認証モジュールへの不正アクセスあるいは不正改造防止と同様にＩＣカード内部の情報漏洩、改竄及びその他異常動作に関連したリスク（問題）を検出してＨＬＲ等へ通報することは非常に有意義である。そこで、ＩＣカードに対する問題を検知した場合は、加入者認証モジュール内部で状態変化を変化させておき、次に再同期トークン（ＡＵＴＳ）を発行可能なタイミングで状態変化を示す再同期トークン（ＡＵＴＳ）を送出することが有効である。

【０１１５】

また、再同期トークン（ＡＵＴＳ）であることを表示した上で、その内部データに状態が変化していることを表示するデータ列を挿入して、再同期トークン（ＡＵＴＳ）として規定されている所定データ長のデータ列の形式で、当該ネットワーク事業者のネットワークノード（ＨＬＲ４０，４１）に返却をするようにしても良い。

【０１１６】

なお、判定部８５はユーザ端末１０側に備えても良い。この場合、検出部８４が検出した状態変化を示す状態変化情報は記憶部８２に一旦書き込まれ、ユーザ端末１０の判定部８５から読みだされて判定するようにすることができる。

【０１１７】

（第５の実施の形態）

ユーザ端末１０に備えられた非接触ＩＣカード機能部８０は、他の非接触ＩＣカードと非接触通信可能である。他の非接触ＩＣカードにおける状態変化（ネットワーク事業者の意図しない状態に遷移）が検出されている場合、非接触ＩＣカード機能部８０が他の非接

触ＩＣカードと通信した際に状態変化を示す変化情報を受け取り、受け取った他の非接触ＩＣカードの変化情報をユーザ端末１０又は加入者認証モジュール２０に渡し、加入者認証モジュール２０による相互認証プロセスの過程で認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。

【０１１８】

図１４は第５の実施の形態に係るユーザ端末、加入者認証モジュール及び非接触ＩＣカード機能部の構成を示している。第５の実施の形態に係るユーザ端末１０は、ユーザ端末１０に非接触ＩＣカード機能部８０を備えている。非接触ＩＣカード機能部８０は、第４の実施の形態と同様にリーダ・ライタと非接触通信すると共に、他の非接触ＩＣカード９０との間で非接触のデータ通信を行うことができる。非接触ＩＣカード機能部８０は、無線・有線送受信部８１、記憶部８２及び演算部８３で構成でき、非接触ＩＣカード機能部８０に対する攻撃を移動通信ネットワーク３０へ通知しないのであれば、図１４に示すように判定部８５は不要である。

【０１１９】

他の非接触ＩＣカード９０は、無線送受信部９１、記憶部９２、演算部９３、検出部９４及び判定部９５を備える。無線送受信部９１は、リーダ・ライタと非接触通信して非接触ＩＣカード９０（記憶部９２）に対してバリューの書き込み等が行なわれる。無線送受信部９１は、さらに非接触ＩＣカード機能部８０との間で非接触通信する。記憶部９２は、バリュー情報が書き込まれる他に、認証に必要な情報が記憶されると共に、非接触ＩＣカード９０における状態変化（ネットワーク事業者の意図しない状態に遷移）が検出された場合には状態変化情報が記憶される。演算部９３は、非接触ＩＣカード９０と非接触通信するリーダ・ライタ等との間の相互認証やデータの暗号化及びＭＡＣ付加のための演算を行う。検出部９４は、第３の実施の形態で説明した加入者認証モジュール２０と同様に、非接触ＩＣカード９０に対する物理的攻撃又はソフト的な攻撃を検知する。判定部９５は、検出部９４によって攻撃が検出された場合に状態変化を示す状態変化情報を記憶部９２に書き込むようにしている。無線送受信部９１は、所定の契機（例えば、非接触ＩＣカード機能部８０との間のバリューの授受を伴うような無線通信発生、記憶部９２に格納されているデータ（例えば、会員情報など）の読み出しに伴う無線通信の発生）で状態変化を示す状態変化情報を非接触ＩＣカード機能部８０へ通知する。非接触ＩＣカード機能部８０は、所定の契機（例えば、非接触ＩＣ機能部８０に対するインタフェース部１３からの情報アクセスであって、ユーザ端末１０にあるアプリケーションからの要求に基づく）で状態変化を示す状態変化情報をユーザ端末１０へ通知する。

【０１２０】

ユーザ端末１０の通信部１１は、加入者認証モジュール２０が認証応答（ＲＥＳ）を発行する際に非接触ＩＣカード機能部８０から状態変化を示す状態変化情報が通知されていれば、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。又は、第２の実施の形態と同様の通知方法を適用することもできる。すなわち、加入者認証モジュール２０が非接触ＩＣカード９０の状態変化情報をユーザ端末１０経由で受け取り、位置登録時等の相互認証プロセスにおいて認証応答（ＲＥＳ）を発行する際に、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。

【０１２１】

また、再同期トークン（ＡＵＴＳ）であることを表示した上で、その内部データに状態が変化していることを表示するデータ列を挿入して、再同期トークン（ＡＵＴＳ）として規定されている所定データ長のデータ列の形式で、当該ネットワーク事業者のネットワークノード（ＨＬＲ４０，４１）に返却をするようにしても良い。

【０１２２】

（第６の実施の形態）

次に、ユーザ端末（形状に関わらず、第６の実施の形態を実現するに足りる機能のみが含まれている場合を含む）が接触型ＩＣカード決済端末に組み込まれている場合を想定する。接触型ＩＣカード決済端末は、小売店等において専ら接触型ＩＣカードを用いてクレ

ジットカード決済する場合に、ユーザ端末によるネットワーク接続機能を有する一体型端末（あるいは有線又は無線によりネットワーク接続機能が別機器となっている場合も含む）とするが、これらに限られない。

【０１２３】

接触型ＩＣカード決済端末に接続された接触型ＩＣカードについて、当該接触型ＩＣカード内部で異常があったことを検知していた場合に、当該状態変化を接触型ＩＣカード決済端末及びユーザ端末を経由して移動通信ネットワーク３０（ＨＬＲ５０）に通知する。このとき、上述の各実施の形態と同様に、加入者認証モジュール２０が認証応答（ＲＥＳ）を発行するタイミングで、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。

【０１２４】

図１５はユーザ端末が接触型ＩＣカード決済端末に組み込まれた構成を示している。ユーザ端末１０に相当する移動機本体１００が、接触型ＩＣカード決済機能部１１０に組み込まれている。移動機本体１００は、加入者認証モジュール２０が備えられている。接触型ＩＣカード決済機能部１１０は、接触型ＩＣカード１２０と通信して決済サービスを提供する。

【０１２５】

移動機本体１００は、通信部１１０１及びインターフェース部１１０２を備える。通信部１１０１は、前述した通信部１１と同等の機能を備える。すなわち、移動通信ネットワーク３０と通信して、接触型ＩＣカード１２０で検出された状態変化をＨＬＲ５０に通知する。インターフェース部１１０２は、加入者認証モジュール２０との間で認証パラメータを送受信すると共に、接触型ＩＣカード決済機能部１１０との間でデータを送受信する。

【０１２６】

接触型ＩＣカード決済機能部１１０は、移動機本体１００及び接触型ＩＣカード１２０と有線接続してデータを送受信する。記憶部１１２は、カード決済に必要な情報が記憶され、演算部１１３はカード決済に必要な演算が実行される機能部分である。

【０１２７】

接触型ＩＣカード１２０は、有線送受信部１２１、記憶部１２２、演算部１２３、検出部１２４、判定部１２５を備える。有線送受信部１２１は、接触型ＩＣカード決済機能部１１０と有線接続されて決済情報を送受信する。また、有線送受信部１２１は、記憶部１２２に記憶された状態変化情報を所定の契機（例えば、決済時におけるVerify PINコード交換に基づくような接触型ＩＣカード決済機能部１１０との通信発生）で接触型ＩＣカード決済機能部１１０へ通知する。記憶部１２２は、ＩＣカード決済に必要な情報が書き込まれると共に、接触型ＩＣカード１２０に対する攻撃で改竄等されたことを示す状態変化情報が書き込まれる。演算部１２３は、カード決済に必要な演算が実行される機能部分である。検出部１２４は、第３の実施の形態で説明した加入者認証モジュール２０と同様に、接触型ＩＣカード１２０に対する物理的攻撃又はソフト的な攻撃を検知する。判定部１２５は、検出部１２４によって攻撃が検出された場合に状態変化を示す状態変化情報を記憶部１２２に書き込むようにしている。有線送受信部１２１が、上記所定の契機で状態変化情報を接触型ＩＣカード決済機能部１１０へ通知する。接触型ＩＣカード決済機能部１１０は、所定の契機（例えば、接触型ＩＣカード決済機能部１１０に対するインタフェース部１１０２からの情報アクセスであって、移動機本体１００にあるアプリケーションからの要求に基づく）で状態変化を示す状態変化情報を移動機本体１００へ通知する。

【０１２８】

移動機本体１００の通信部１１０１は、加入者認証モジュール２０が認証応答（ＲＥＳ）を発行する際に接触型ＩＣカード決済機能部１１０から状態変化を示す状態変化情報が通知されていれば、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。又は、第２の実施の形態と同様の通知方法を適用することもできる。すなわち、加入者認証モジュール２０が接触型ＩＣカード１２０の状態変化情報をユーザ端末１０経由で受

け取り、位置登録時等の相互認証プロセスにおいて認証応答（ＲＥＳ）を発行する際に、認証応答（ＲＥＳ）に代えて再同期トークン（ＡＵＴＳ）を送信する。

【０１２９】

また、再同期トークン（ＡＵＴＳ）であることを表示した上で、その内部データに状態が変化していることを表示するデータ列を挿入して、再同期トークン（ＡＵＴＳ）として規定されている所定データ長のデータ列の形式で、当該ネットワーク事業者のネットワークノード（ＨＬＲ４０，４１）に返却をするようにしても良い。

【０１３０】

また、上述の実施の形態では、再同期トークン（ＡＵＴＳ）に基づくユーザ端末１０における権限状態の変化の検出は、ＨＬＲ５０で行われるものとしたが、ＶＬＲ４０やＶＳＲやＳＧＳＮなど、他のネットワーク側装置で行われてもよい。また、上述の実施の形態では、認証応答（ＲＥＳ）と期待認証応答（ＸＲＥＳ）との照合は、ＶＬＲ４０で行われるものとしたが、ＭＭＥなどの他のネットワーク側装置で行われてもよい。ＶＳＲ又はＳＧＳＮなど他のネットワーク側装置において、権限状態の変化の検出をする通信システムであれば、特権奪取情報を再同期トークン（ＡＵＴＳ）フォーマット長と同じデータ列で送信した場合、ＲＥＳとＸＲＥＳとの比較前に、ＲＥＳフォーマットか否かを判断し、ＲＥＳフォーマットであれば、従来通りの認証処理を実行し、再同期トークン（ＡＵＴＳ）フォーマットであればデータ列の内の通知情報、例えば特権奪取情報を示すパラメータを抽出し、ＶＬＲ及びＨＬＲへ登録するようにしてもよい。また、上述の実施の形態では、状態変化検出装置が、ＨＬＲ５０であるものとして説明したが、ＨＬＲ５０と端末管理サーバ６０は、別々のハードウェア上に構成することもできる（さらに、近接して設置してもよいし、通信回線等により物理的に離れている場所に設置することもできるし、他のネットワーク（例えば、ＭＶＮＯ）を構成する装置として存在していてもよい）し、同一のハードウェア上で機能するソフトウェアにより構成することもできる。また、ＨＬＲ５０は前記ユーザ端末１０における権限状態の変化を検出したことに関して、加入者認証モジュール２０に対して再発行するＡＶにおけるＡＵＴＮにおいて、その旨の情報を含めてもよい。

【０１３１】

上述の実施形態を用いて本発明について詳細に説明したが、当業者にとっては、本発明が本明細書中に説明した実施形態に限定されるものではないということは明らかである。本発明は、特許請求の範囲の記載により定まる本発明の趣旨及び範囲を逸脱することなく修正及び変更態様として実施することができる。従って、本明細書の記載は、例示説明を目的とするものであり、本発明に対して何ら制限的な意味を有するものではない。

【０１３２】

なお、本実施形態で記載の非接触ＩＣカードはＦｅｌｉＣａ（登録商標）を例示しているが、ＮＦＣ（Ｎｅａｒ　Ｆｉｅｌｄ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ）など、その他の短距離無線通信規格であるＴｙｐｅ　Ａ、Ｂであっても良い。また非接触に限らず、接触式ＩＣカードであっても、図示又は説明しない、リーダを介しての通信可能な形態で本発明が適用できることは言うまでも無い。

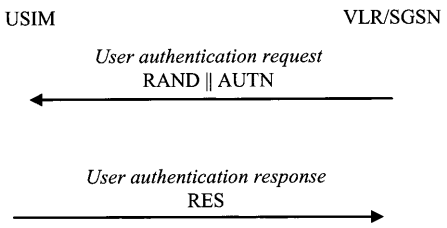
【符号の説明】

【０１３３】

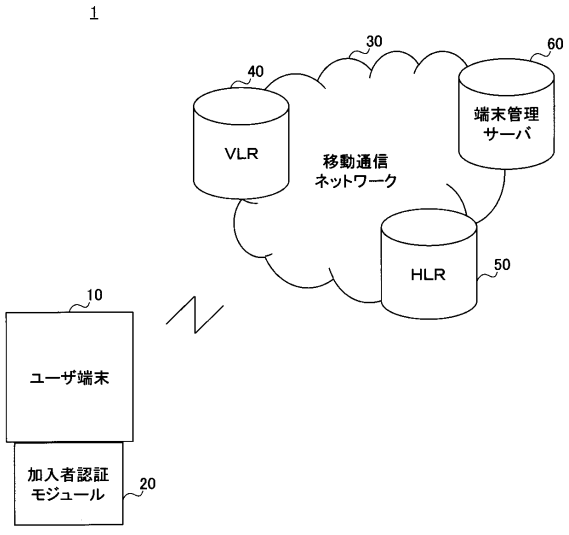
１…移動通信システム
１０…ユーザ端末
２０…加入者認証モジュール
３０…移動通信ネットワーク
４０…ＶＬＲ
５０、５１…ＨＬＲ
６０…端末管理サーバ
１１、１０１…通信部
１２、２４、８４、９４、１２４…検出部

１３、１０２…インターフェース部
２１…送受信部
２２、８２、９２、１１２、１２２…記憶部
２３、８３、９３、１１３、１２３…演算部
２５、８５、９５、１２５…判定部
５１…送受信部
５２…認証ベクトル生成部
５３…検出部

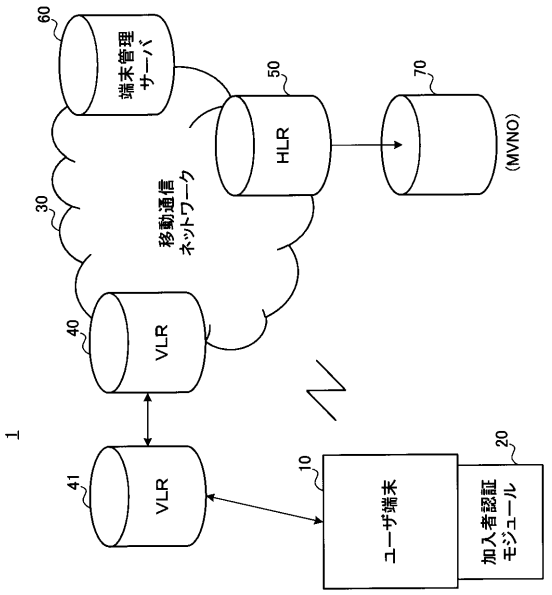
【図１】



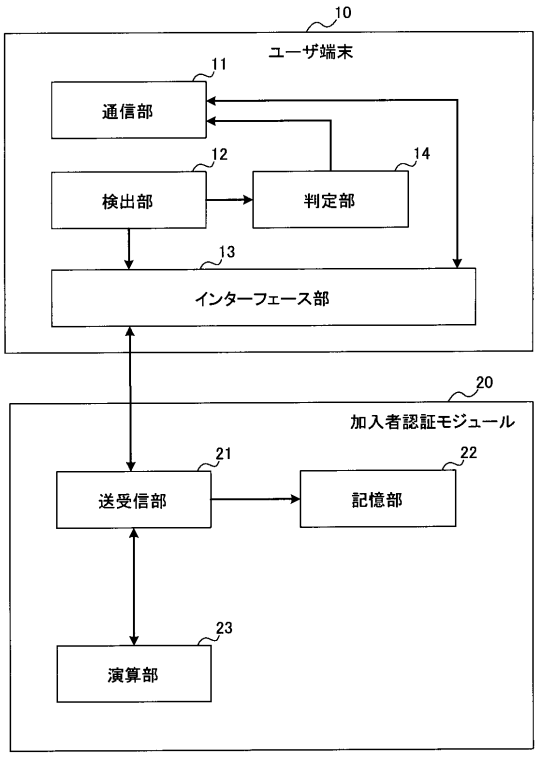
【図２Ａ】



【図２Ｂ】



【図３】



【図４】

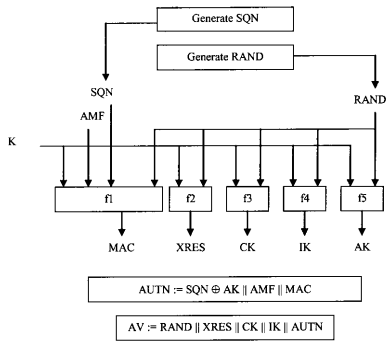


図 4A

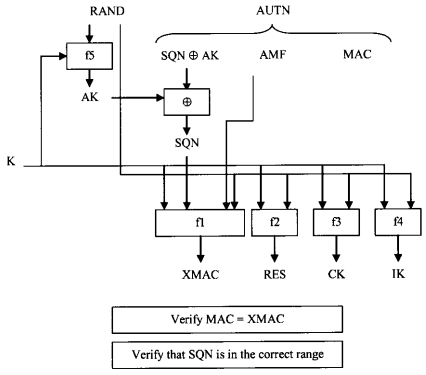
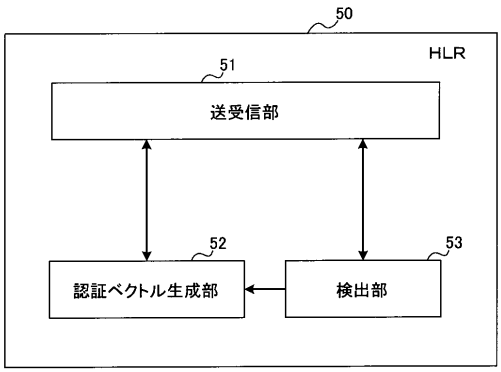
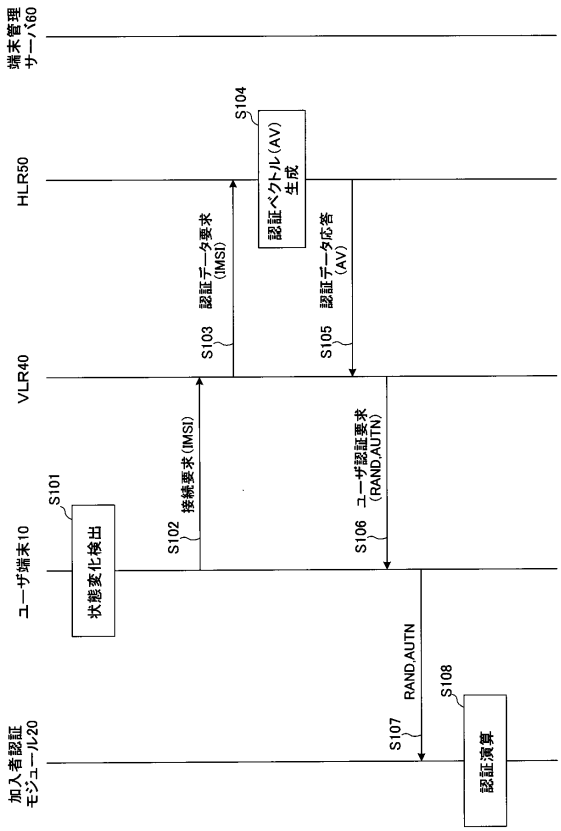


図 4B

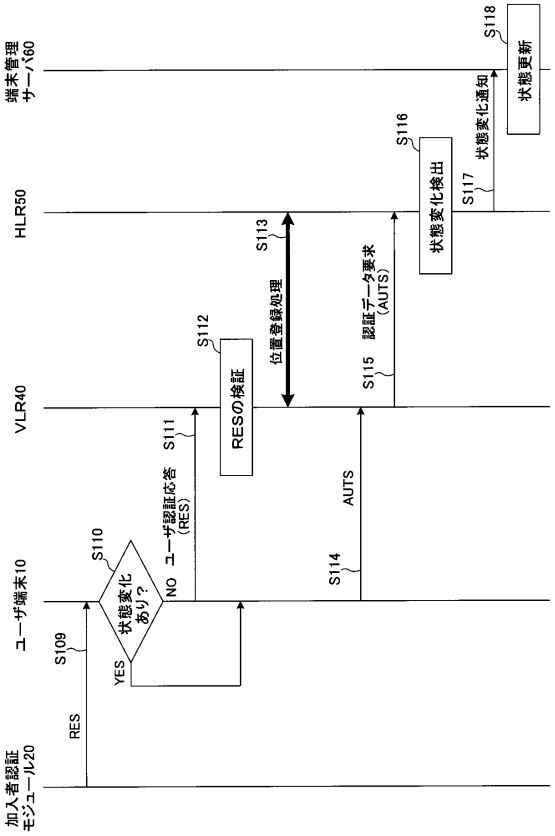
【図５】



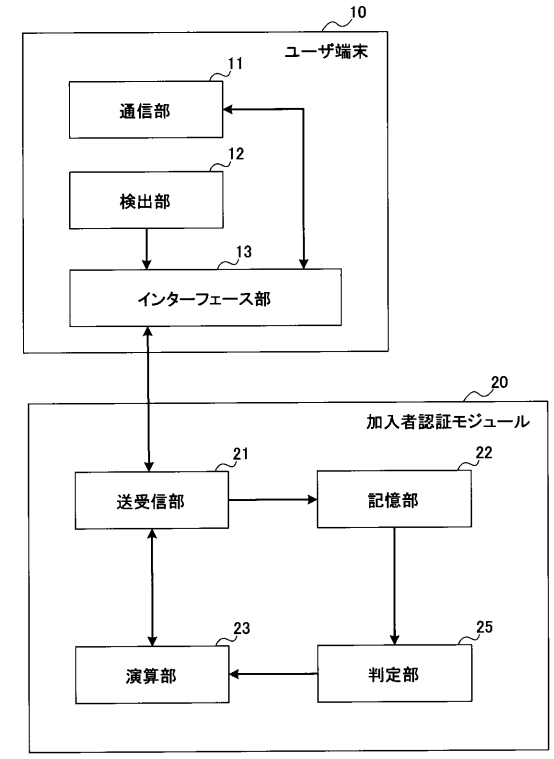
【図６】


端末管理サーバ60
HLR50
VLR40
ユーザ端末10
加入者認証モジュール20
S101
状態変化検出
S102
接続要求(IMSI)
S103
認証データ要求(IMSI)
S104
認証ベクトル(AV)生成
S105
認証データ応答(AV)
S106
ユーザ認証要求(RAND,AUTN)
S107
RAND,AUTN
S108
認証演算

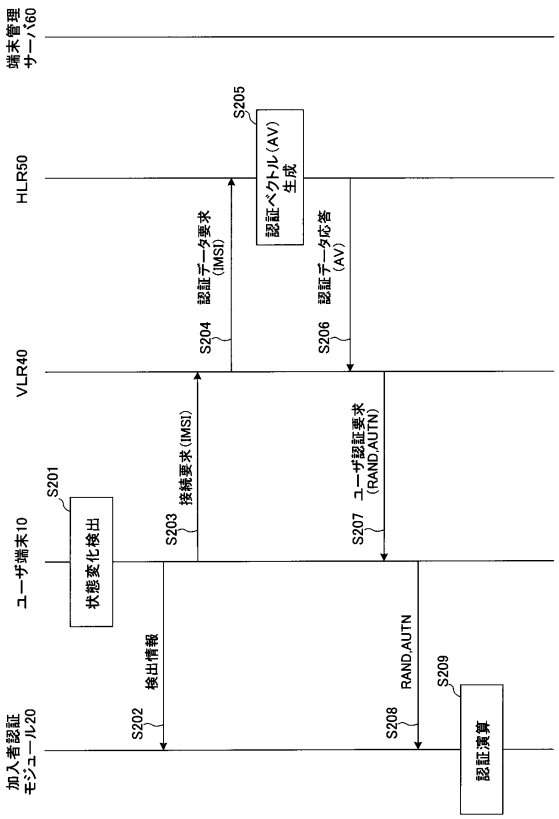
【図７】


端末管理サーバ60
HLR50
VLR40
ユーザ端末10
加入者認証モジュール20
S109
RES
S110
状態変化あり?
YES
NO
S111
ユーザ認証応答(RES)
S112
RESの検証
S113
位置登録処理
S114
AUTS
S115
認証データ要求(AUTS)
S116
状態変化検出
S117
状態変化通知
S118
状態更新

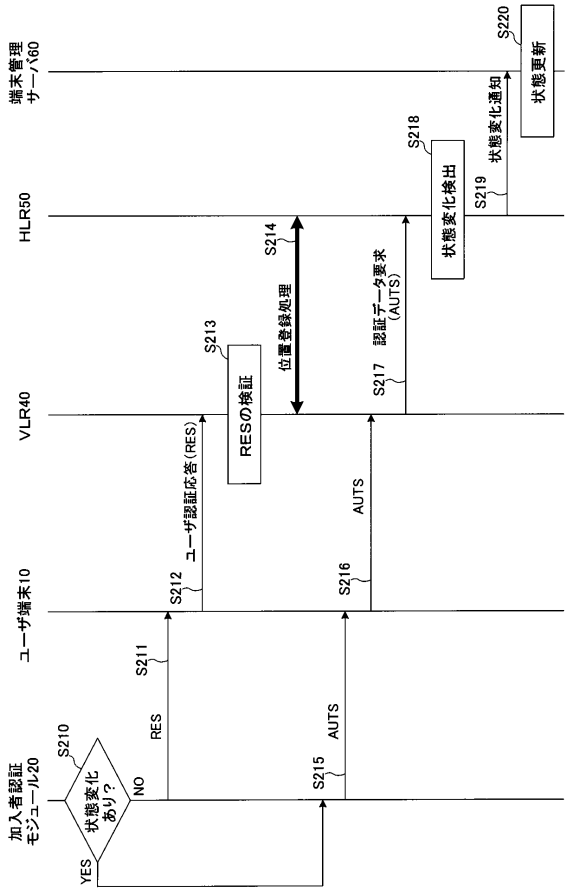
【図８】


10
ユーザ端末
11
通信部
12
検出部
13
インターフェース部
20
加入者認証モジュール
21
送受信部
22
記憶部
23
演算部
25
判定部

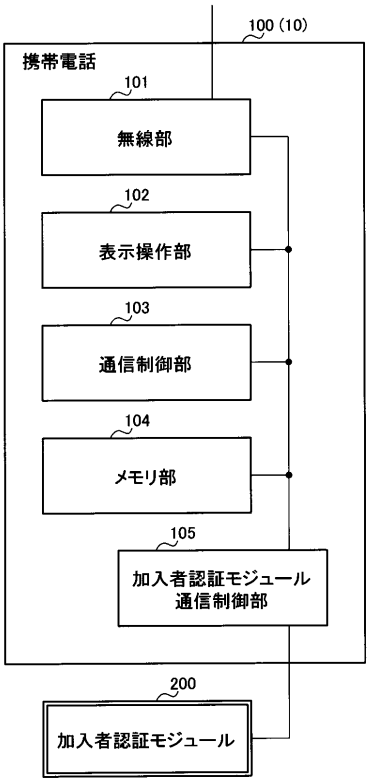
【図９】


端末管理サーバ60
HLR50
VLR40
ユーザ端末10
加入者認証モジュール20
S201
状態変化検出
S202
検出情報
S203
接続要求(IMSI)
S204
認証データ要求(IMSI)
S205
認証ベクトル(AV)生成
S206
認証データ応答(AV)
S207
ユーザ認証要求(RAND,AUTN)
S208
RAND,AUTN
S209
認証演算

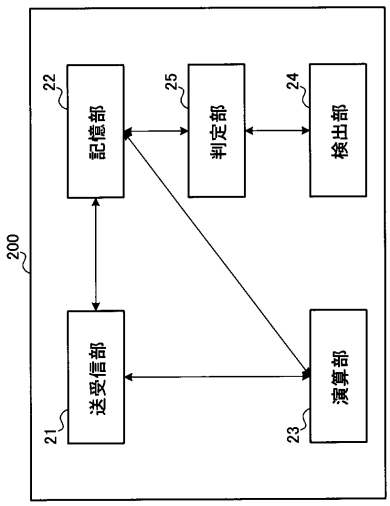
【図１０】



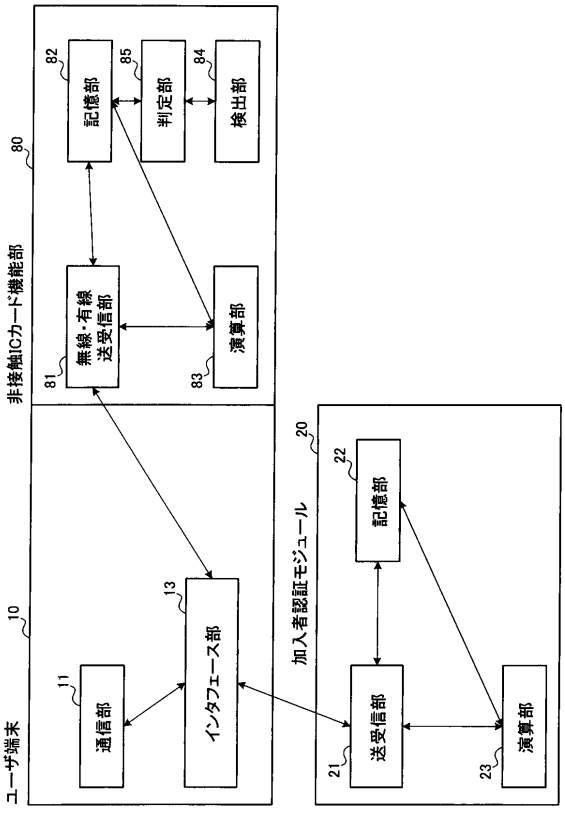
【図１１】



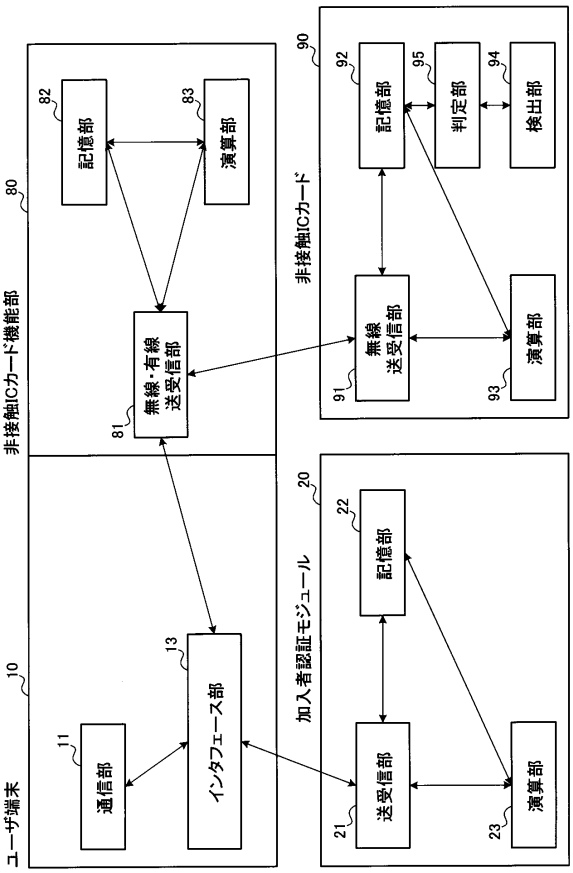
【図１２】



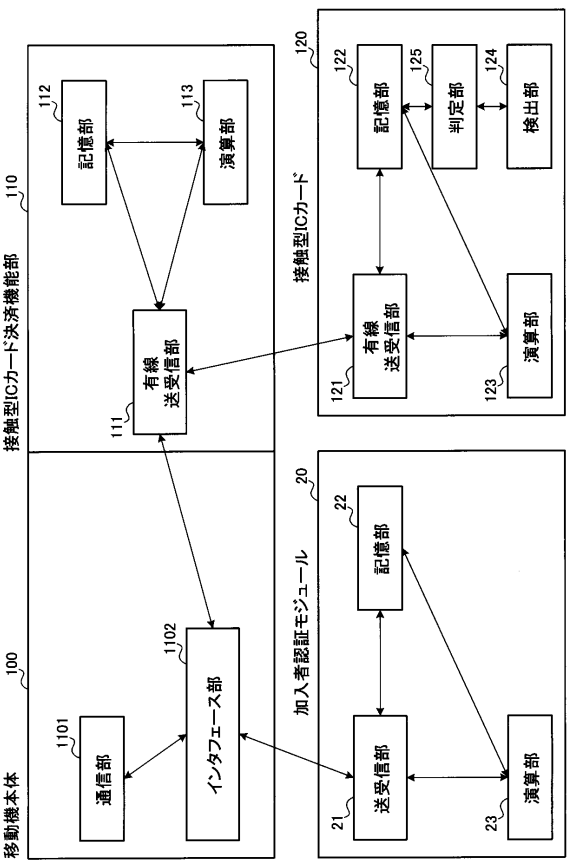
【図１３】



【図１４】


ユーザ端末
10
通信部
11
インタフェース部
13
非接触ICカード機能部
80
記憶部
82
演算部
83
無線・有線
送受信部
81
加入者認証モジュール
20
送受信部
21
記憶部
22
演算部
23
非接触ICカード
90
無線
送受信部
91
記憶部
92
演算部
93
検出部
94
判定部
95

【図１５】


移動機本体
100
通信部
1101
インタフェース部
1102
接触型ICカード決済機能部
110
記憶部
112
演算部
113
有線
送受信部
111
加入者認証モジュール
20
送受/信部
21
記憶部
22
演算部
23
接触型ICカード
120
有線
送受/信部
121
記憶部
122
演算部
123
検出部
124
判定部
125

フロントページの続き

審査官　山田　倍司

(56)参考文献　特表２００９－５３６８０３（ＪＰ，Ａ）
特開２００８－０６１２００（ＪＰ，Ａ）
特開２０１２－００３４８８（ＪＰ，Ａ）
特開２０１０－２６３４２６（ＪＰ，Ａ）
特表２０１２－５２４４６９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)

Ｇ０６Ｆ	２１／００
	２１／１２－２１／５７
Ｈ０４Ｂ	７／２４－ ７／２６
Ｈ０４Ｍ	１／００
	１／２４－ ３／００
	３／１６－ ３／２０
	３／３８－ ３／５８
	７／００－ ７／１６
	１１／００－１１／１０
	９９／００
Ｈ０４Ｗ	４／００－９９／００