(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2011-192129
(P2011-192129A)
(43)公開日　平成23年9月29日(2011.9.29)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330C	5B285
H04L 9/32	(2006.01)	H04L	9/00	673B	5J104

審査請求 未請求　請求項の数 2　ＯＬ　（全 10 頁）

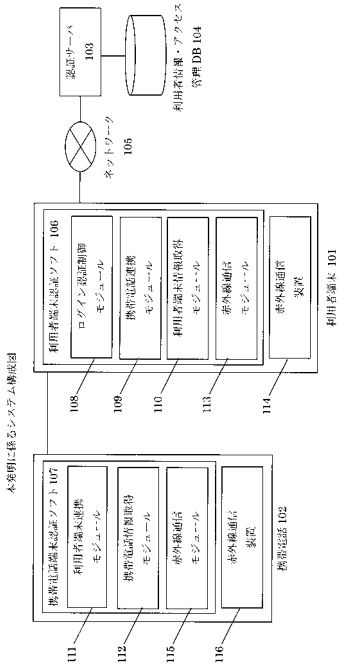
(21)出願番号　特願2010-58907(P2010-58907)
(22)出願日　平成22年3月16日(2010.3.16)

(71)出願人　000233055
株式会社日立ソリューションズ
東京都品川区東品川四丁目１２番７号
(74)代理人　100088720
弁理士　小川　眞一
(72)発明者　松浦　靖和
東京都品川区東品川四丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内

Ｆターム(参考)　5B285 AA01 BA02 CB42 CB62 CB73
CB85 DA04 DA10
5J104 AA07 AA16 EA01 EA16 KA02
NA06 NA36 PA01

(54)【発明の名称】携帯電話端末を用いたログイン認証システム

(57)【要約】
【課題】　なりすましログインによりコンピュータ内にある機密情報、認証機器の紛失による機器に登録された機密情報の第三者に漏洩されることを防ぐことができるログイン認証システムを提供すること。
【解決手段】　利用者端末と携帯電話端末と認証サーバ及び利用者情報管理ＤＢを備えた認証システムであって前記利用者端末が、自端末に接続された携帯電話端末のＩＭＳＩ情報を取得する手段と、自利用者端末のＭＡＣアドレス情報を取得する手段と、前記認証サーバに対して前記ＩＭＳＩとＭＡＣアドレス情報を送信し、ログイン認証を受ける手段とを備え、
前記携帯電話端末が前記利用者端末からのＩＭＳＩ情報取得要求に対し、自携帯電話端末のＩＭＳＩ情報を前記利用者端末に送信する手段を備え、
前記認証サーバが、前記利用者端末からのログイン認証要求のＩＭＳＩ情報とＭＡＣアドレス情報を受信し、前記利用者管理情報ＤＢに同一の情報が登録されているか否かを問い合わせることによりログイン認証を行う手段を備えることを特徴とする。



【特許請求の範囲】
【請求項１】
利用者端末と携帯電話端末と認証サーバ及び利用者情報管理ＤＢを備えた認証システムであって
前記利用者端末が、
前記認証サーバへログイン認証要求する際に、前記利用者端末に接続された前記携帯電話端末のＩＭＳＩ情報を取得する手段と、自利用者端末のＭＡＣアドレス情報を取得する手段と、前記認証サーバに対して前記ＩＭＳＩとＭＡＣアドレス情報を送信し、ログイン認証を受ける手段と、認証結果によって前記利用者端末へのログインを不可とする手段を備え、
前記携帯電話端末が、
前記利用者端末からのＩＭＳＩ情報取得要求に対し、自携帯電話端末のＩＭＳＩ情報を前記利用者端末に送信する手段を備え、
前記認証サーバが、
前記利用者端末からのログイン認証要求のＩＭＳＩ情報とＭＡＣアドレス情報を受信し、前記利用者管理情報ＤＢに同一の情報が登録されているか否かを問い合わせることによりログイン認証を行う手段を備えることを特徴とするログイン認証システム。
【請求項２】
前記利用者端末及び携帯電話端末は、両者が接続されていない場合、携帯電話端末のＩＭＳＩ情報を取得するための赤外線通信手段を互に備えることを特徴とする請求項１に記載の携帯電話端末を用いたログイン認証システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、パーソナルコンピュータなどの利用者端末にインストールされているオペレーションシステム（ＯＳ）へのログインを、携帯電話端末とコンピュータの固有情報を使用して認証を行い、端末の利用者を限定することで情報漏えいを防ぐようにした携帯電話端末を用いたログイン認証システムに関するものである。
【背景技術】
【０００２】
従来、パーソナルコンピュータなどの利用者端末へのログイン認証は、オペレーションシステム（ＯＳ）に登録しているユーザ名とパスワードを利用者が入力し、登録したユーザ名とパスワードが入力した内容と一致していれば、利用者端末へログインでき、利用者端末のすべての資源が利用可能となる。
また、ＯＳに登録したユーザ名とパスワード以外のログイン認証として、ＩＣカードとカードリーダーを使用して行うことも可能となっている。このＩＣカードでのログイン認証は、コンピュータに接続したカードリーダーにＩＣカードの記録データを読ませたり、ＩＣカードを常時カードリーダーに挿入しておくことで、利用者端末へのログインを行っている。
【０００３】
この種の先行技術文献として下記の特許文献に開示されたものがある。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特表２００３－５０３８０３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ＯＳに登録したユーザ名とパスワードによるログイン認証の場合、パスワードがユーザ名と同じといった推測し易くなっている場合があり、悪意のある利用者によりなりすまし

によるログインが行われると、コンピュータ内にある資源が利用となり、機密情報が外部に漏洩されてしまう脅威がある。
また、ＩＣカードを使用したログイン認証の場合、ＩＣカードの紛失、盗難によりＩＣカードに格納されている会社名、個人情報、パスワードなどの情報が悪意のある利用者により読み取られ、機密情報が外部に漏洩されてしまう脅威がある。
【０００６】
本発明の目的は、携帯電話端末を使用し、ログイン認証で使用する機器に新たに情報登録を行わず、携帯電話端末の一意な認識番号として付与されているＩＭＳＩ（International Mobile Subscriber Identity）とコンピュータに一意に割り当てられているのＭＡＣアドレス（Media Access Control address）を使用してＯＳへのログイン認証を可能とするシステムを提供することにある。
【課題を解決するための手段】
【０００７】
上記課題を解決するために本発明は、利用者端末と携帯電話端末と認証サーバ及び利用者情報管理ＤＢを備えた認証システムであって
前記利用者端末が、
前記認証サーバへログイン認証要求する際に、前記利用者端末に接続された前記携帯電話端末のＩＭＳＩ情報を取得する手段と、自利用者端末のＭＡＣアドレス情報を取得する手段と、前記認証サーバに対して前記ＩＭＳＩとＭＡＣアドレス情報を送信し、ログイン認証を受ける手段と、認証結果によって前記利用者端末へのログインを不可とする手段を備え、
前記携帯電話端末が、
前記利用者端末からのＩＭＳＩ情報取得要求に対し、自携帯電話端末のＩＭＳＩ情報を前記利用者端末に送信する手段を備え、
前記認証サーバが、
前記利用者端末からのログイン認証要求のＩＭＳＩ情報とＭＡＣアドレス情報を受信し、前記利用者管理情報ＤＢに同一の情報が登録されているか否かを問い合わせることによりログイン認証を行う手段を備えることを特徴とする。
また、前記利用者端末及び携帯電話端末は、両者が接続されていない場合、携帯電話端末のＩＭＳＩ情報を取得するための赤外線通信手段を互に備えることを特徴とする。
【発明の効果】
【０００８】
本発明によれば、携帯電話端末に一意に設定されているＩＭＳＩ情報と利用者端末のＭＡＣアドレス情報とを用いて利用者端末の利用者任認証を行うため、利用者はログイン認証を行うためのパスワード設定、ログイン認証するための利用者端末、携帯電話端末にログイン認証情報の登録、パスワードを覚えるといったことが必要なくなり、認証が容易となる。
また、利用者端末を紛失した場合でも、紛失した利用者端末のＭＡＣアドレスと携帯電話端末端末のＩＭＳＩが認証サーバで一致しなければログイン認証が成立しないため、不正ログインによる情報漏えいを防ぐことが可能となる。
【図面の簡単な説明】
【０００９】
【図１】本発明に係るシステム構成図である。
【図２】利用者情報・アクセス管理ＤＢ１０４の保持するテーブル図である。
【図３】ログイン認証する際の利用者端末１０１と認証サーバ１０３間の処理のフローチャートである。
【図４】携帯電話端末１０２が利用者端末１０１に接続されている場合の利用者端末１０１と携帯電話端末１０２間の処理のフローチャートである。
【図５】赤外線通信による利用者端末１０１と携帯電話端末１０２間の処理のフローチャートである。

【発明を実施するための形態】
【００１０】
以下、本発明を実施する場合の実施形態を、図面を用いて詳細に説明する。
図１は、携帯電話端末が利用者端末に接続されている場合のシステム構成図である。
図１において、ネットワーク１０５には、利用者端末１０１、及び認証サーバ１０３が接続されている。利用者端末１０１には、携帯電話端末１０２が接続されている。
利用者端末１０１内には、利用者端末認証ソフト１０６がインストールされ、赤外線装置１１４が装備されている。
利用者端末認証ソフト１０６は、ログイン認証制御モジュール１０８、携帯電話連携モジュール１０９、利用者端末情報取得モジュール１１０、赤外線通信モジュール１１３で構成されている。
携帯電話端末１０２内には、携帯電話端末認証ソフト１０７がインストールされ、赤外線装置１１６が装備されている。
携帯電話端末認証ソフト１０７は、利用者端末連携モジュール１１１、携帯電話端末情報取得モジュール１１２、赤外線通信モジュール１１５で構成されている。
【００１１】
利用者端末認証ソフト１０６は、利用者からのログイン認証要求があった場合、ログイン認証制御モジュール１０８が利用者端末１０１のＭＡＣアドレス及び携帯電話端末１０２のＩＭＳＩ情報を取得し、これらの情報で認証サーバ１０３にログイン認証を行う。
ログイン認証制御モジュール１０８は、携帯電話連携モジュール１０９から携帯電話端末のＩＭＳＩ情報を、利用者端末情報取得モジュール１１０から利用者端末のＭＡＣアドレス情報をそれぞれ受信する。受信したＩＭＳＩ情報とＭＡＣアドレス情報で認証サーバ１０３にログイン認証を行う。
【００１２】
携帯電話連携モジュール１０９は、利用者端末１０１に接続された携帯電話端末１０２の携帯電話端末認証ソフト１０７の利用者端末連携モジュール１１１にアクセスする。
利用者端末連携モジュール１１１が送信した内容をログイン認証制御モジュール１０８へ送信する。
利用者端末情報取得モジュール１１０は、利用者端末のＭＡＣアドレス情報を取得し、ログイン認証制御モジュール１０８へ送信する。
赤外線通信モジュール１１３は、赤外線通信装置１１４経由で携帯電話端末１０２の携帯電話端末認証ソフト１０７の赤外線通信モジュール１１５からのデータ受信を受信する。受信したデータをログイン認証モジュール１０８へ送信する。
【００１３】
携帯電話認証ソフト１０７は、携帯電話連携モジュール１０９からアクセス要求があった場合、利用者端末連携モジュール１１１が、携帯電話情報取得モジュール１１２から受信したデータを、携帯電話連携モジュール１０９へ送信する。
携帯電話認証ソフト１０７は、利用者から起動された場合、赤外線通信モジュール１１５が、携帯電話情報取得モジュール１１２から受信したデータを、赤外線通信装置１１６経由で赤外線通信モジュール１１３へ送信する。
【００１４】
携帯電話情報取得モジュール１１２は、携帯電話端末１０２のＩＭＳＩ情報を取得し、利用者端末連携モジュール１１１もしくは赤外線通信連携モジュール１１５へ送信する。
認証サーバ１０３は、ログイン認証制御モジュール１０８からアクセスがあった場合、ログイン認証制御モジュール１０８からのＩＭＣＩ情報とＭＡＣドレス情報で、利用者情報・アクセス管理ＤＢ１０４に問い合わせてログイン認証を行い、同一の情報が登録されていればログイン認証ＯＫとし、ログイン認証モジュール１０８に認証結果を送信し、アクセスログを収集する。
【００１５】
ログイン認証が成立すれば、利用者は利用者端末１０１にログインでき、利用者端末１

０１のすべての資源が利用可能となる。ログイン認証が成立しなければ、利用者端末１０１にログインは行えず、利用者端末１０１は利用不可となる。

悪意ある利用者が利用者情報・アクセス管理ＤＢ１０４に登録されていないＩＭＳＩ情報とＭＡＣアドレス情報の組み合わせでログイン認証を行おうとしても、ログイン認証が成立せず、利用者端末１０１からの情報漏えいを防ぐことができる。

例えば、悪意ある利用者の携帯電話端末１０２と拾得した利用者端末１０１でログイン認証を行おうとしても、悪意ある利用者の携帯電話端末１０２のＩＭＳＩ情報と拾得した利用者端末のＭＡＣアドレスが利用者情報・アクセス管理ＤＢ１０４で一致しなければ、ログイン認証が成立しない。

また、アクセスログの収集は、ログイン認証の履歴を保管することによって、いつ、だれが、どの携帯電話端末１０２と利用者端末１０１で、ログイン認証をおこなったかの証跡となる。

【００１６】

図２は、利用者情報・アクセス管理ＤＢ１０４が保持するテーブル図である。

この利用者情報・アクセス管理ＤＢ１０４は、利用者情報管理テーブル２００とログイン履歴テーブル２０３の２つのテーブルを保持している。

利用者情報管理テーブル２００には、ＩＭＳＩ情報２０１とＭＡＣアドレス情報２０２の情報が保管されている。

アクセス管理テーブル２０３には、ＩＭＳＩ情報２０４とＭＡＣアドレス情報２０５ごとにいつアクセスしたかといった履歴情報と、ログイン認証が成立したか不成立したかといった情報が格納されている。認証を行った日時を日時２０６に、認証結果をログイン認証結果２０７に格納する。

アクセスログを保管しておくことにより利用者端末１０１の不正利用を検知する。

【００１７】

図３は、ログイン認証する際の利用者端末１０１と認証サーバ１０３間の処理のフローチャートである。

利用者が利用者端末１０１からログイン認を要求したとき、利用者端末認証ソフト１０６は、利用者端末１０１のＭＡＣアドレス情報と利用者端末１０１に接続された携帯電話端末１０２のＩＭＳＩ情報をＳＳＬ等によって認証サーバ１０３に暗号化して送信する（ステップ３０１）。

これに対し、そのデータを受信した認証サーバ１０３は、ＭＡＣアドレス情報とＩＭＳＩ情報をもとに利用者情報・アクセス管理ＤＢ１０４に問い合わせ（ステップ３０２）、ユーザ認証を行う（ステップ３０３）。

ユーザ認証に失敗した場合、その旨を利用者端末認証ソフト１０６に通知し、利用者端末認証ソフト１０６がアクセス拒否ダイアログを表示して利用者による利用者端末１０１へのログインを拒否する（ステップ３０４）。

【００１８】

一方、ログイン認証に成功した場合は、ログイン処理を行う。（ステップ３０５）

図４は、携帯電話端末端末１０２が利用者端末１０１に接続されている場合の利用者端末１０１と携帯電話端末端末１０２間の処理のフローチャートである。

利用者が利用者端末１０１からログイン認証を要求したとき、利用者端末認証ソフト１０６は、ログイン認証モジュール１０８を起動する（ステップ４０１）。

ログイン認証モジュール１０８は、ダイアログを表示し、携帯電話端末１０２のＩＭＳＩ取得方法の選択を促し、利用者が利用者端末１０１に接続した携帯電話端末からの取得方法を選択すると、携帯電話端末連携モジュール１０９を起動する（ステップ４０２）。

携帯電話端末連携モジュール１０９は、利用者端末１０１に携帯電話端末が接続されているかチェックを行う（ステップ４０３）。

【００１９】

携帯電話端末が接続されていない場合は、その旨をログイン認証モジュールへ通知し、ログイン認証モジュール１０８が、接続エラーダイアログを表示して利用者による利用者

端末１０１へのログインを拒否する（ステップ４０４）。
携帯電話端末１０２が接続されている場合は、携帯電話端末認証ソフト１０７を起動する（ステップ４０５）。
携帯電話端末認証ソフト１０７がインストールされていない携帯電話端末１０２が接続されている可能性があるので携帯電話端末認証ソフト１０７からの応答のタイムアウトチェックを行う（ステップ４０６）。

【００２０】
一定時間経過しても携帯電話端末認証ソフト１０７から応答がない場合は、タイムアウトエラーとし、その旨をログイン認証モジュール１０８へ通知し、ログイン認証モジュール１０８が、タイムアウトエラーダイアログを表示して利用者による利用者端末１０１へのログインを拒否する（ステップ４０７）。

【００２１】
次に、携帯電話端末認証ソフト１０７は、携帯電話連携モジュール１０９からアクセスがあった場合、利用者端末連携モジュール１１１を起動する（ステップ４０８）。
利用者端末連携モジュール１１１は、携帯電話端末１０２のＩＭＳＩ情報を取得するため、携帯電話情報取得モジュール１１２を起動する（ステップ４０９）。
携帯電話情報取得モジュール１１２は、携帯電話端末１０２に登録されたＩＭＳＩ情報を取得し、利用者端末連携モジュール１１１へ取得したＩＭＳＩ情報を送信する（ステップ４１０）。

【００２２】
利用者端末連携モジュール１１１は、携帯電話情報取得モジュール１１２から送信された情報を携帯電話端末連携モジュール１０９へ送信する（ステップ４１１）。
携帯電話連携モジュール１０９は、受信した情報をログイン認証制御モジュール１０８へ送信する（ステップ４１２）。
携帯電話端末認証ソフト１０７が処理している間に、携帯電話端末１０２が利用者端末１０１から切り離される可能性があるので、送信完了のタイムアウトチェックを行う（ステップ４１３）。

【００２３】
一定期間経過しても利用者端末１０１に送信できない場合は、タイムアウトエラーとして、その旨を携帯電話端末認証ソフト１０７へ通知し、携帯電話端末認証ソフト１０７が、タイムアウトエラーダイアログを表示する（ステップ４１４）。
次に、ログイン認証制御モジュール１０６は、ＭＡＣアドレス情報を取得するため、利用者端末情報取得モジュール１１０を起動する（ステップ４１５）。
利用者端末情報取得モジュール１１０は、利用者端末１０１のＭＡＣアドレス情報を取得し、ログイン認証モジュール１０８へ送信する。（ステップ４１６）
ログイン認証制御モジュールは、受信したＩＭＳＩ情報とＭＡＣアドレス情報で認証サーバ１０３にログイン認証を行う（ステップ４１７）。

【００２４】
図５は、赤外線通信による利用者端末１０１と携帯電話端末１０２間の処理のフローチャートである。
利用者が利用者端末１０１からログイン認証を要求したとき、利用者端末認証ソフト１０６は、ログイン認証制御モジュール１０８を起動する（ステップ５０１）。
ログイン認証制御モジュール１０８は、ダイアログを表示し、携帯電話端末１０２のＩＭＳＩ情報取得方法の選択を促し、利用者が赤外線通信による取得方法を選択すると、赤外線通信モジュール１１３を起動する（ステップ５０２）。
ここで、利用者端末１０１の赤外線通信装置１１４は、データ受信待ちの状態となる（ステップ５０３）。

【００２５】
携帯電話端末１０１と赤外線通信が行われない可能性があるので、データ受信待ちのタイムアウトチェックを行う（ステップ５０４）。

一定時間経過しても携帯電話端末１０１と赤外線通信が行われないと、タイムアウトエラーとし、その旨をログイン認証制御モジュール１０８へ通知し、ログイン認証制御モジュール１０８が、タイムアウトエラーダイアログを表示して利用者による利用者端末１０１へのログインを拒否する（ステップ５０５）。

次に、利用者が携帯電話端末認証ソフト１０７を起動すると、携帯電話端末認証ソフト１０７が赤外線通信モジュール１１５を起動する（ステップ５０６）。

赤外線通信モジュール１１５は、携帯電話端末１０２のＩＭＳＩ情報を取得するため、携帯電話情報取得モジュール１１２を起動する（ステップ５０７）。

携帯電話情報取得モジュール１１２は、携帯電話端末１０２に登録されたＩＭＳＩ情報を取得し、赤外線通信モジュール１１１へ取得したＩＭＳＩ情報を送信する（ステップ５０８）。

【００２６】

赤外線通信モジュール１１５は、携帯電話情報取得モジュール１１２から送信された情報を携帯電話端末１０２の赤外線通信装置１１６経由で利用者端末１０１の赤外線通信モジュール１１３へ送信する（ステップ５０９）。

赤外線通信モジュール１１５は、利用者端末１０１の赤外線通信モジュール１１４へ送信完了のタイムアウトチェックを行う（ステップ５１０）。

一定期間経過しても利用者端末１０１に送信できない場合は、タイムアウトエラーとして、その旨を携帯電話端末認証ソフト１０７へ通知する。すると、携帯電話端末認証ソフト１０７が、タイムアウトエラーダイアログを表示する（ステップ５１１）。

【００２７】

利用者端末１０１の赤外線通信モジュール１１３は、赤外線装置１１４経由で受信したデータをログイン認証モジュールに送信する（ステップ５１２）。

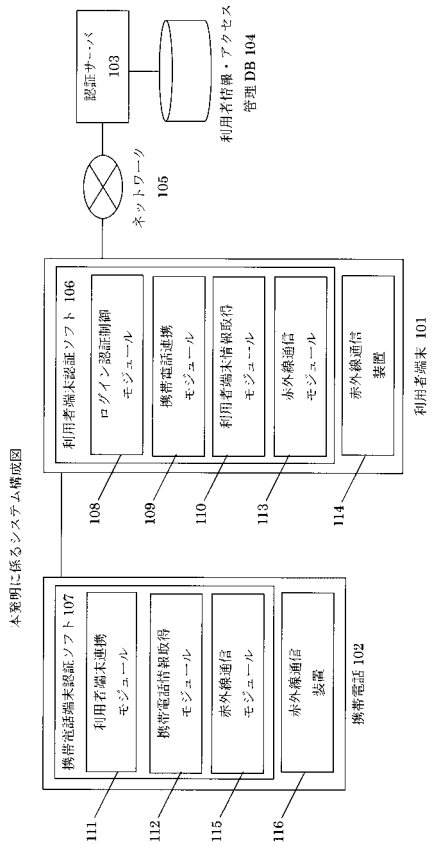
この後は、図４のステップ４１５以降のフローチャートと同じとなる。

【符号の説明】

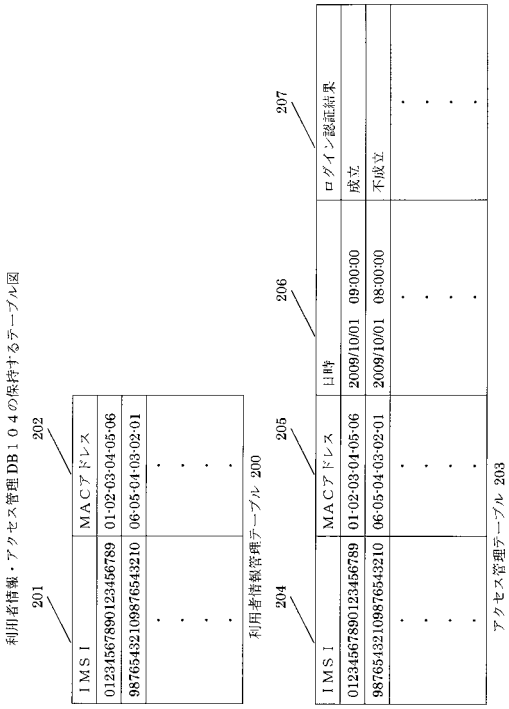
【００２８】

１０１…利用者端末
１０２…携帯電話端末
１０３…認証サーバ
１０４…利用者情報・アクセス管理ＤＢ
１０５…ネットワーク
１０６…利用者端末認証ソフト
１０７…携帯電話端末認証ソフト
１０８…ログイン認証制御モジュール
１０９…携帯電話端末連携モジュール
１１０…利用者端末情報取得モジュール
１１１…利用者端末連携モジュール
１１２…携帯電話端末情報取得モジュール
１１３…赤外線通信モジュール
１１４…赤外線通信装置
１１５…赤外線通信モジュール
１１６…赤外線通信装置
２００…利用者情報管理テーブル
２０１…ＩＭＳＩ情報
２０２…ＭＡＣアドレス情報
２０３…アクセス管理テーブル

【図１】

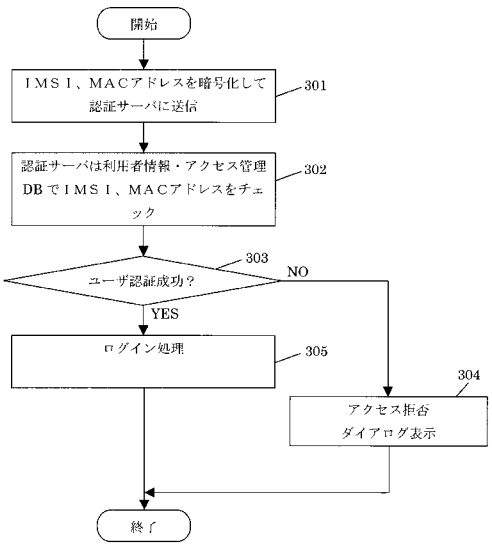


【図２】

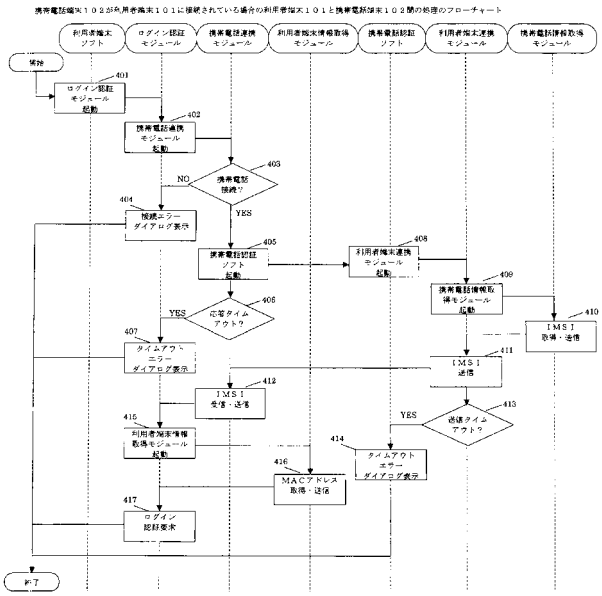


【図３】

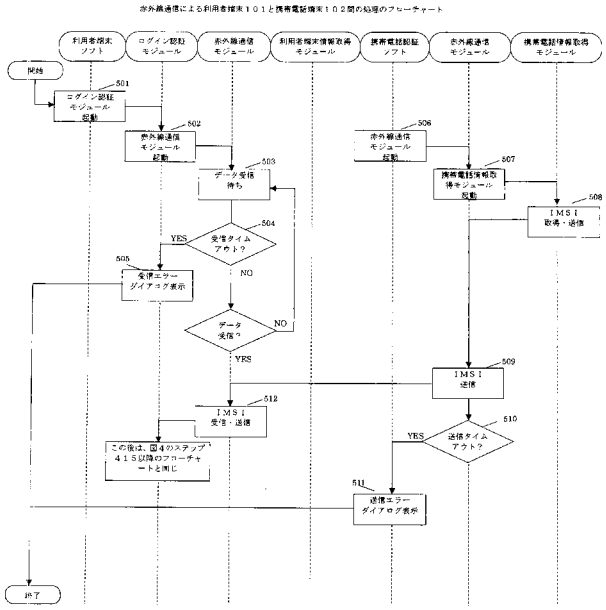
ログイン認証する際の利用者端末１０１と認証サーバ１０３間の処理のフローチャート



【図４】



【図５】


赤外線通信による利用者端末１０１と携帯電話端末１０２間の処理のフローチャート
利用者端末ソフト
ログイン認証モジュール
赤外線通信モジュール
利用者端末情報取得モジュール
携帯電話起動ソフト
赤外線通信モジュール
携帯電話情報取得モジュール
開始
501
ログイン認証モジュール起動
502
赤外線通信モジュール起動
503
データ受信待ち
504
受信タイムアウト？
YES
NO
505
受信エラーダイアログ表示
データ受信？
NO
YES
506
赤外線通信モジュール起動
507
携帯電話情報取得モジュール起動
508
ＩＭＳＩ取得・送信
509
ＩＭＳＩ送信
510
送信タイムアウト？
YES
511
送信エラーダイアログ表示
512
ＩＭＳＩ受信・送信
この後は、図４のステップ４１５以降のフローチャートと同じ
終了

フロントページの続き

【要約の続き】
【選択図】　図１