(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4533935号
(P4533935)
(45)発行日　平成22年9月1日(2010.9.1)　(24)登録日　平成22年6月18日(2010.6.18)

(51)Int.Cl.　F I
G06F 21/22 (2006.01)　G06F 9/06 660C

請求項の数 3　(全 21 頁)

(21)出願番号　特願2008-11572(P2008-11572)
(22)出願日　平成20年1月22日(2008.1.22)
(65)公開番号　特開2009-175853(P2009-175853A)
(43)公開日　平成21年8月6日(2009.8.6)
審査請求日　平成22年1月20日(2010.1.20)

早期審査対象出願

(73)特許権者　000233055
日立ソフトウエアエンジニアリング株式会社
東京都品川区東品川四丁目１２番７号
(74)代理人　110000442
特許業務法人　武和国際特許事務所
(72)発明者　堤　俊之
東京都品川区東品川４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

審査官　岸野　徹

最終頁に続く

(54)【発明の名称】ライセンス認証システム及び認証方法

(57)【特許請求の範囲】
【請求項１】
クライアントＰＣにアプリケーションをインストールする際のライセンス認証システムにおいて、
前記クライアントＰＣと接続して通信可能であり、かつ、無線回線を介してサーバと接続して通信可能な携帯端末を有し、
前述サーバは、前記クライアントＰＣにインストールするアプリケーションに対する仮使用権を発行する仮使用権発行手段と、正規使用権を発行する正規使用権発行手段とを備え、
前述携帯端末は、前記サーバが発行する仮使用権と正規使用権とをサーバから取得、保持する手段と、前記サーバから取得した仮使用権と正規使用権とを前記クライアントＰＣへ提供する手段とを備え、
前記クライアントＰＣは、使用権の種類に応じてアプリケーションの使用を制限するライセンス認証手段と、仮使用権により認証された状態で、正規使用権を要求する手段とを備え、
前記携帯端末は、前記クライアントＰＣにインストールするアプリケーションの入手時に、前記サーバが発行する仮使用権を取得、保持し、前記クライアントＰＣがアプリケーションをインストールする際、前記保持している仮使用権により一時的なライセンス認証を行ってアプリケーションのクライアントＰＣでの利用を可能にし、
前記携帯端末は、その後、サーバと通信可能なエリアに移動して、サーバから正規使用

権を取得、保持し、前記クライアントＰＣから正規使用権によるライセンス認証要求があった場合に、前記保持した正規使用権により正式なライセンス認証を行うことを特徴とするライセンス認証システム。

【請求項２】

前記携帯端末は、正規使用権により正式なライセンス認証を行ってアプリケーションの使用を続ける際の定期的に行われる当該アプリケーションに対する継続使用の認証を、サーバと通信可能なエリアで、サーバから継続使用権を取得、保持し、前記クライアントＰＣから継続使用権によるライセンス認証要求があった場合に、前記保持した継続使用権によりライセンス認証を行うことを特徴とする請求項１記載のライセンス認証システム。

【請求項３】

クライアントＰＣにアプリケーションをインストールする際のライセンス認証方法において、

前記クライアントＰＣと接続して通信可能であり、かつ、無線回線を介してサーバと接続して通信可能な携帯端末を有し、

前述サーバは、前記クライアントＰＣにインストールするアプリケーションに対する仮使用権を発行する仮使用権発行手段と、正規使用権を発行する正規使用権発行手段とを備え、

前述携帯端末は、前記サーバが発行する仮使用権と正規使用権とをサーバから取得、保持する手段と、前記サーバから取得した仮使用権と正規使用権とを前記クライアントＰＣへ提供する手段とを備え、

前記クライアントＰＣは、使用権の種類に応じてアプリケーションの使用を制限するライセンス認証手段と、仮使用権により認証された状態で、正規使用権を要求する手段とを備え、

前記携帯端末は、前記クライアントＰＣにインストールするアプリケーションの入手時に、前記サーバが発行する仮使用権を取得、保持し、前記クライアントＰＣがアプリケーションをインストールする際、前記保持している仮使用権により一時的なライセンス認証を行ってアプリケーションのクライアントＰＣでの利用を可能にし、

前記携帯端末は、その後、サーバと通信可能なエリアに移動して、サーバから正規使用権を取得、保持し、前記クライアントＰＣから正規使用権によるライセンス認証要求があった場合に、前記保持した正規使用権により正式なライセンス認証を行うことを特徴とするライセンス認証方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ライセンス認証システム及び認証方法に係り、特に、事前に使用権が付与されている数だけのアプリケーションだけを利用できるようにするライセンス認証システム及び認証方法に関する。

【背景技術】

【０００２】

アプリケーションの使用権は、従来、ライセンス付与者により、使用者毎にシリアル番号を発行し、アプリケーションのインストール時やアプリケーション起動時に発行されたシリアル番号を入力させて、認証を行うことにより付与されてきた。この場合のアプリケーションには、入力されたシリアル番号がライセンス付与者により発行されたものであることを確認するロジックが組み込まれており、これにより、アプリケーションの不正利用を防止している。

【０００３】

前述したようなシリアル番号による使用権の付与は、同一のシリアル番号を使いまわして複数の人がアプリケーションを使用したり、不正者にシリアル番号を盗み見られて使用されてしまうなどの問題点を有している。

【０００４】

このような問題点を解決する技術として、インターネットを利用したアプリケーションの使用状況確認方法を利用する方法が知られている。この方法は、利用者のＰＣとライセンス付与者のサーバとをインターネットを介して接続し、相互に通信を行うことができることが前提の方法である。この方法は、シリアル番号を用いて利用可能となったアプリケーションが、定期的にユーザ情報とシリアル番号と利用環境情報（ＯＳ、ＩＰアドレス、機器構成情報など）をサーバに送信し、サーバが、利用者毎の使用権数が管理されていて、定期的に送られてくる使用情報との整合性をチェックするというものである。これにより、アプリケーションの不正な利用を発見し、必要に応じて利用制限や使用停止を行うことができる。

【０００５】

前述した方法は、利用者のＰＣがインターネットに接続されてなければ、不正利用の発見を行うことができず、また、正規使用権を持つ利用者による使用を行うことができないものである。そのため、携帯電話を利用してアプリケーションの使用権及び使用状況の確認を行う技術が、例えば、特許文献１等に記載された提案されている。この特許文献１に記載された従来技術は、インターネットに接続されていないＰＣに対して、使用者の持つ携帯電話を中継器のように利用し、携帯電話を介してＰＣとサーバとを接続することにより、アプリケーションの使用権の付与や使用状況の確認をサーバから行うことができるようにしたものである。

【特許文献１】特開２００６－３０９７２０号公報

【発明の開示】

【発明が解決しようとする課題】

【０００６】

前述した携帯電話を中継器として利用しアプリケーションの使用権の付与や使用状況の確認をサーバから行う従来技術は、携帯電話が中継を行う際に、携帯電話の無線通信を利用してインターネットに接続している。しかし、利用者のＰＣが置かれている場所が、携帯電話が通信可能エリア外であったり、海外等での利用の場合には、インターネットに接続することができないため、利用することができないという問題点有している。

【０００７】

本発明の目的は、前述した従来技術の問題点を解決し、アプリケーションの認証を行うサーバとの通信ができない状況にあるクライアントＰＣにインストールするアプリケーションの認証を行うことを可能にしたライセンス認証システム及び認証方法を提供することにある。

【課題を解決するための手段】

【０００８】

本発明によれば前記目的は、クライアントＰＣにアプリケーションをインストールする際のライセンス認証システムにおいて、前記クライアントＰＣと接続して通信可能であり、かつ、無線回線を介してサーバと接続して通信可能な携帯端末を有し、前述サーバは、前記クライアントＰＣにインストールするアプリケーションに対する仮使用権を発行する仮使用権発行手段と、正規使用権を発行する正規使用権発行手段とを備え、前述携帯端末は、前記サーバが発行する仮使用権と正規使用権とをサーバから取得、保持する手段と、前記サーバから取得した仮使用権と正規使用権とを前記クライアントＰＣへ提供する手段とを備え、前記クライアントＰＣは、使用権の種類に応じてアプリケーションの使用を制限するライセンス認証手段と、仮使用権により認証された状態で、正規使用権を要求する手段とを備え、前記携帯端末は、前記クライアントＰＣにインストールするアプリケーションの入手時に、前記サーバが発行する仮使用権を取得、保持し、前記クライアントＰＣがアプリケーションをインストールする際、前記保持している仮使用権により一時的なライセンス認証を行ってアプリケーションのクライアントＰＣでの利用を可能にし、前記携帯端末は、その後、サーバと通信可能なエリアに移動して、サーバから正規使用権を取得、保持し、前記クライアントＰＣから正規使用権によるライセンス認証要求があった場合に、前記保持した正規使用権により正式なライセンス認証を行うことにより達成される。

【発明の効果】
【０００９】
本発明によれば、新たなサーバなどを必要とせずＷｅｂブラウザプログラムとＷｅｂサーバプログラムに機能を追加するだけで、アプリケーションの認証を行うサーバとの通信ができない状況にあるクライアントＰＣにインストールするアプリケーションの認証を行うことが可能となる。
【発明を実施するための最良の形態】
【００１０】
以下、本発明によるライセンス認証システムの実施形態を図面により詳細に説明する。以下に説明する本発明の実施形態によるライセンス認証システムは、アプリケーションを利用するクライアントＰＣがライセンス認証のためのサーバとの通信を行うことができない環境に設置されており、このようなクライアントＰＣに記録媒体等に格納されたアプリケーションをインストールする際に、クライアントＰＣを利用するユーザが所持する携帯電話、ＰＨＳ等の携帯端末を使用して、クライアントＰＣにインストールするアプリケーションに対する認証を行うことを可能とするものである。
【００１１】
図１は本発明の一実施形態によるライセンス認証システムの構成を示すブロック図である。
【００１２】
本発明の実施形態によるライセンス認証システムは、図１に示すように、利用者が使用するデスクトップＰＣやノートＰＣ等の情報処理機器であるクライアントＰＣ１０１と、携帯電話やＰＨＳ等の利用者本人が所持する情報処理機器である携帯端末１０２と、デスクトップＰＣやブレードＰＣ等の情報処理機器であるサーバ１０３と、インターネット１０４とにより構成される。クライアントＰＣ１０１は、会社内部や自宅内等だけで利用するＰＣのためインターネット１０４には接続せずに利用されるものとする。携帯端末１０２やサーバ１０３は、公衆回線網や無線通信網等で構成されるインターネット１０４を介してデータ通信を行うことができる。インターネット１０４には、携帯端末１０２やサーバ１０３と同様の機器が複数接続されている。携帯端末１０２は、インターネット１０４と電波で接続しているため、電波状態の悪い場所では、インターネット１０４にアクセスすることができない。
【００１３】
図２はクライアントＰＣ１０１の構成を示すブロック図である。図２に示すクライアントＰＣ１０１は、プログラムの実行を行うＣＰＵ２０１と、プログラムやデータをロードするメモリ２０２と、他の情報処理機器とデータ交換を行う通信部２０３と、命令やデータの入力を行う入力部２０４と、システムの状態等を出力する出力部２０５と、ＨＤＤ等の記憶部２０８とがバス２０７により接続されて構成されている。記憶部２０８には、共有機密情報Ｂ２０９、アプリＩＤ２１０、キー２１１、乱数２１２等を保持するアプリケーションインストールプログラム２０６と、暗号モジュール２１３とハッシュ関数２１４とが記憶されている。
【００１４】
前述において、通信部２０３は、無線ＬＡＮ、Bluetooth、 赤外線等を利用して携帯端末１０２との間のデータ通信を行う機能を持つ。入力部２０４は、キーボード、マウス、ペン入力、音声入力、ボタン、ジョグダイヤル、十字キー等の入力手段である。出力部２０５は、ディスプレイ、プリンター、音声等の出力手段である。アプリケーションインストールプログラム２０６は、サーバ１０３により生成された新規のアプリケーションをインストールするプログラムである。共有機密情報Ｂ２０９、アプリＩＤ２１０、キー２１１、乱数２１２は、処理の過程でアプリケーションインストールプログラム２０６が保持するデータである。暗号モジュール２１３は、ＤＥＳやＡＥＳ等の共通鍵暗号による暗号処理や復号処理を行うモジュールである。ハッシュ関数モジュール２１４は、ＭＤ５やＳＨＡ１等の一方向性関数の計算処理を行うモジュールである。暗号モジュール２１３やハ

ッシュ関数モジュール２１４は、クライアントＰＣ１０１と携帯端末１０２とサーバ１０３との間で、予め決めた同一の方式のものが記憶されている。

【００１５】

図３は携帯端末１０２の構成を示すブロック図である。携帯端末１０２は、プログラムの実行を行うＣＰＵ３０１と、プログラムやデータをロードするメモリ３０２と、他の情報処理機器とデータ交換を行う通信部３０３と、命令やデータの入力を行う入力部３０４と、システムの状態等を出力する出力部３０５と、ＲＯＭとうによる記憶部３１０とがバス３１１により接続されて接続されている。

【００１６】

前述において、記憶部３１０には、ライセンス管理プログラム３０６、ライセンス取得プログラム３０７、ライセンスリスト３０８、キーリスト３０９、ユーザＩＤ３１２、暗号モジュール３１３、ハッシュ関数モジュール３１４、共有機密シード３１５等を記憶している。

【００１７】

通信部３０３は、無線ＬＡＮ、Bluetooth、 赤外線等を利用してクライアントＰＣ１０１との間でのデータ通信を行う機能やインターネット１０４を介してサーバ１０３との間でのデータ通信を行う機能を持つ。ライセンス管理プログラム３０６は、クライアントＰＣ１０１にインストールされるアプリケーションのライセンス認証をサーバ１０３に代わって行うプログラムである。ライセンス取得プログラム３０７は、クライアントＰＣ１０１にインストールされるアプリケーションのライセンス認証情報をサーバ１０３から取得するプログラムである。ライセンスリスト３０８には、ライセンス認証情報が納されている。キーリスト３０９は、ライセンス管理プログラム３０６がライセンスを供与するに利用できるキー関連情報を格納している。ユーザＩＤ３１２は、処理の過程で携帯端末１０２が保持するデータである。共有機密シード３１５は、サーバ１０３との間だけで、予め共有している秘密データである。

【００１８】

図４は携帯端末１０２が持つライセンスリスト３０８の構成を示す図である。ライセンスリスト３０８は、項番４０１、アプリ種別４０２、利用アプリＩＤ４０３、キー４０４、共有機密情報Ａ４０５の組を１つのレコードとして複数のレコードが格納されて構成される。項番４０１は、リスト内のレコードを一意に決定する識別子である。アプリ種別４０２は、ライセンスを供与することができるアプリケーションの種類を識別する識別子である。利用アプリＩＤ４０３は、ライセンスを供与したアプリケーションを識別する識別子である。キー４０４は、ライセンス供与時に利用したキー情報である。共有機密情報Ａ４０５は、サーバ１０３とだけで共有する秘密情報である。

【００１９】

図５は携帯端末１０２が持つキーリスト３０９の構成を示す図である。キーリスト３０９は、項番５０１、キー５０２、暗号キーシード５０３、利用フラグ５０４の組を１つのレコードとして複数のレコードが格納されて構成される。項番５０１は、リスト内のレコードを一意に決定する識別子である。キー５０２は、ライセンス供与時に利用されるキー情報である。暗号キーシード５０３は、キー５０２に関連した暗号情報である。利用フラグ５０４は、対応するレコードのキー情報の使用状態を表している。「０」は未使用、「１」は使用である。

【００２０】

図６はサーバ１０３の構成を示すブロック図である。サーバ１０３は、プログラムの実行を行うＣＰＵ６０１と、プログラムやデータをロードするメモリ６０２と、他の情報処理機器との間でデータ交換を行う通信部６０３と、命令やデータの入力を行う入力部６０４と、システムの状態等を出力する出力部６０５と、記憶部６１２とがバス６１３により接続されて構成される。

【００２１】

前述において、記憶部６１２には、ライセンス発行プログラム６０６、インストール作

成プログラム６０７、ライセンス登録プログラム６０８、共有機密情報Ｂ６０９、アプリケーションリスト６１０、ライセンス管理テーブル６１１、アプリケーションインストールモジュール６１４、暗号モジュール６１５、ハッシュ関数モジュール６１６、共有機密シード６１７が記憶されている。

【００２２】

通信部６０３は、有線、無線ＬＡＮ、Bluetooth 等を利用してインターネット１０４を介してクライアント１０１との間でのデータを通信を行う機能を持つ。ライセンス発行プログラム６０６は、サーバ１０３の生成するアプリケーションインストールプログラムのライセンス認証情報等を携帯端末１０２に提供するプログラムである。インストール作成ログラム６０７は、クライアントＰＣ１０１に導入するアプリケーションのインストールプログラムを生成するプログラムである。ライセンス登録プログラム６０８は、クライアントＰＣ１０１にインストールされたアプリケーションのライセンス認証やライセンスインストール状況の登録等を行うプログラムである。共有機密情報Ｂ６０９は、クライアントＰＣ１０１との間で共有する秘密データである。アプリケーションリスト６１０は、サーバ１０３がライセンス認証できるアプリケーションの種類を格納している。ライセンス管理テーブル６１１は、ライセンス供与しているユーザやアプリケーション、ライセンス認証状況等の情報を格納している。アプリケーションインストールモジュール６１４は、アプリケーションインストールプログラムのライセンス認証の処理を実行するモジュールである。暗号モジュール６１５、ハッシュ関数モジュール６１６は、すでに説明したように、クライアントＰＣ１０１と携帯端末１０２とサーバ１０３との間で、予め決めた同一の方式のものが記憶されている。共有機密シード６１７は、携帯端末１０２との間だけで、予め共有している秘密データである。

【００２３】

図７はサーバ１０３が持つアプリケーションリスト６１０の構成を示す図である。アプリケーションリスト６１０は、項番７０１、アプリ種別７０２、モジュール格納場所７０３の組を１つのレコードとして複数のレコードが格納されて構成される。項番７０１は、リスト内のレコードを一意に決定する識別子である。アプリ種別７０２は、ライセンス認証が可能なアプリケーションの種類を識別する識別子である。モジュール格納場所７０３は、アプリ種別毎のアプリケーションプログラムの実行モジュールを格納している場所（ディレクトリ名やＵＲＬ等）を示している。なお、各実行モジュールは、予め用意されている。

【００２４】

図８はサーバ１０３が持つライセンス管理テーブル６１１の構成を示す図である。ライセンス管理テーブル６１１は、項番８０１、ユーザＩＤ８０２、ライセンスアプリ８０３、アプリＩＤ８０４、キー８０５、共有機密情報Ａ８０６の組を１つのレコードとして複数のレコードが格納されて構成される。項番８０１は、テーブル内のレコードを一意に決定する識別子である。ユーザＩＤ８０２は、ライセンスを供与しているユーザの識別子である。ライセンスアプリ８０３は、ライセンス供与するアプリケーションの種類である。アプリＩＤ８０４は、ライセンスを供与したアプリケーションを一意に識別する識別子である。キー８０５は、ライセンスを認証する際に利用する情報である。共有機密情報Ａ８０６は、携帯端末１０２との間で共有する秘密データである。

【００２５】

図９は本発明の実施形態によるライセンス認証システム全体の処理動作を説明するフローチャートであり、次に、これについて説明する。

【００２６】

（１）ライセンス管理者は、利用者にアプリケーションに対するライセンスを提供、認証するために必要なアプリケーションのインストールプログラムを作成する。このため、はじめに、ライセンス管理者は、サーバ１０３のインストール作成プログラム６０７を起動して、クライアントＰＣ１０１上に導入することができるアプリケーションインストールプログラムを作成する。作成されたアプリケーションインストールプログラムは、アプリ

ケーションそのものをも含み、記録媒体等に格納されて、あるいは、顧客の携帯端末１０２にダウンロードする等により配布される。なお、この処理の詳細については、図１２に示すフローを参照して後述する（ステップ９０１）。

【００２７】

（２）クライアントＰＣを使用する利用者は、記録媒体等に格納されて配布されるアプリケーションインストールプログラムを購入する際、そのアプリケーションをクライアントＰＣ１０１にインストールする際、あるいは、アプリケーションをインストールした後、アプリケーションに対するライセンスの認証を受けるため、自身が所持する携帯端末１０２とサーバ１０３との間で通信を行うことが可能な場所に移動する。そして、利用者は、携帯端末１０２をサーバ１０３に接続し、携帯端末上のライセンス取得プログラム３０４を起動して、サーバ１０３から必要なアプリケーションの仮ライセンス情報を取得する。なお、この処理の詳細については、図１０に示すフローを参照して後述する（ステップ９０２）。

【００２８】

（３）その後、利用者は、インストールするアプリケーションインストールプログラムに含まれるアプリケーションをクライアントＰＣ１０１で利用可能にするために、携帯端末１０２とクライアントＰＣ１０１とを接続する。これにより、クライアントＰＣ１０１は、アプリケーションのライセンスの取得を行う。この場合のライセンスは、仮のものである。なお、この処理の詳細については、図１１に示すフローを参照して後述する（ステップ９０３）。

【００２９】

（４）その後、利用者は、アプリケーションをクライアントＰＣ１０１に導入するために、ステップ９０１で作成されて提供されたアプリケーションインストールプログラムを起動し、アプリケーションインストールプログラムが携帯端末１０２を利用してライセンス認証を行う。なお、この処理の詳細については、図１１に示すフローを参照して後述する（ステップ９０４）。

【００３０】

図１２は図９のステップ９０１での処理であるサーバ１０３のインストール作成プログラム６０７の処理動作の詳細を説明するフローチャートであり、次に、これについて説明する。

【００３１】

（１）インストール作成プログラム６０７は、まず、図７により説明したアプリケーションリスト６１０のアプリ種別７０２を出力部６０５に表示し、ライセンス管理者により指定されたアプリ種別を取得する。ここでは、ライセンス管理者によって、インストールプログラムを作成するアプリケーションのアプリ種別が指定されるものとしている（ステップ１２０１、１２０２）。

【００３２】

（２）次に、インストール作成プログラム６０７は、アプリケーションリスト６１０から、ステップ１２０２の処理で取得したアプリ種別に対応したモジュール格納場所７０３の項目を検索し、その場所のモジュールであるアプリケーションプログラムを取得する（ステップ１２０３）。

【００３３】

（３）ステップ１２０３の処理で取得したモジュールとアプリケーションインストールモジュール６１４と共有機密情報Ｂ６０９とからアプリケーションインストールプログラムを生成する（ステップ１２０４）。

【００３４】

図１０は図９のステップ９０２の処理での仮ライセンス取得のための携帯端末１０２のライセンス取得プログラム３０７とサーバ１０３のライセンス発行プログラム６０６とによる処理動作を説明するフローチャートであり、次に、これについて説明する。

【００３５】

（１）処理が開始されると、携帯端末１０２のライセンス取得プログラム３０７がサーバ１０３のライセンス発行プログラム６０６にアプリケーションリスト要求を送信する。このアプリケーションリスト要求を受け取ったライセンス発行プログラム６０６は、アプリケーションリスト６１０のアプリ種別７０２の全項目を返送する（ステップ１００１、１００２）。

【００３６】

（２）ライセンス取得プログラム３０７は、ステップ１００２で返送されたアプリ種別７０２の項目を受け取り、それらの項目を出力部３０５に表示して、利用者に選択させ、利用者により指定されたアプリ種別を取得する（ステップ１００３、１００９）。

【００３７】

（３）ライセンス取得プログラム３０７は、ユーザＩＤ３１２にデータが登録されているか否かを確認し、ユーザＩＤ３１２の登録がなかった場合、新規にユーザＩＤを作成する（ステップ１０１０、１０１１）。

【００３８】

（４）ステップ１０１０の確認で、ユーザＩＤ３１２の登録があった場合、そのユーザＩＤを、ステップ１０１１で新たにユーザＩＤを作成した場合、そのユーザＩＤを、ユーザＩＤ３１２として、ステップ１００９で取得したアプリ種別とユーザＩＤ３１２とをライセンス取得要求として、サーバ１０３のライセンス発行プログラム６０６に送信する（ステップ１００４）。

【００３９】

（５）サーバ１０３のライセンス発行プログラム６０６は、ライセンス取得要求を受け取ると、ライセンス管理テーブル６１１に新しいレコードを作成し、受信したライセンス取得要求のアプリ種別とユーザＩＤとを作成したレコードのユーザＩＤ８０２とライセンスアプリ８０３との項目に登録する（ステップ１００５）。

【００４０】

（６）ライセンス発行プログラム６０６は、乱数Ａと乱数Ｂを生成し、生成した乱数Ａを暗号モジュール６１５と共有機密情報Ｂ６０９とにより暗号化すると共に、生成した乱数Ａとハッシュ関数モジュール６１６とからハッシュ値を計算する（ステップ１０１２～１０１４）。

【００４１】

（７）その後、ライセンス発行プログラム６０６は、共有機密シード６１７とステップ１０１２で生成した乱数Ｂとを連結し、ハッシュ関数モジュール６１６で計算した結果を、ステップ１００５の処理で作成した新規レコードの共有機密情報Ａ８０６の項目に登録する（ステップ１０１５）。

【００４２】

（８）そして、ライセンス発行プログラム６０６は、ステップ１０１２の処理で生成した乱数Ｂとステップ１０１３の処理で暗号化した暗号データとステップ１０１４の処理で算出したハッシュ値とステップ１００５の処理で受信したアプリ種別とをライセンス情報として、携帯端末１０２のライセンス取得プログラム３０７に返送する（ステップ１００６）。

【００４３】

（９）携帯端末１０２のライセンス取得プログラム３０７は、共通機密シード３１５と受信したライセンス情報の乱数Ｂとを連携させ、ハッシュ関数モジュール３１４でハッシュ値を計算する（ステップ１０１６）。

【００４４】

(10) その後、ライセンス取得プログラム３０７は、ライセンスリスト３０８に新たなレコードを追加して、ライセンス情報のアプリ種別とステップ１０１６の処理で算出したハッシュ値とを、アプリ種別４０２と共有機密情報Ａ４０５との項目に登録する（ステップ１００７）。

【００４５】

（11）さらに、ライセンス取得プログラム３０７は、キーリスト３０９に、新たなレコードを追加して、ライセンス情報のハッシュ値と暗号データとを、キー５０２と暗号キーシード５０３との項目に登録する。また、利用フラグ５０４の項目に「０」を設定する（ステップ１０１７）。

【００４６】

（12）ライセンス取得プログラム３０７は、利用者からのライセンスの追加要求がないか否かを確認し、追加要求があれば、ステップ１００３からの処理に戻って処理を続け、追加要求がなければ、ここでの処理を終了する（ステップ１００８）。

【００４７】

図１１は図９のステップ９０３、９０４の処理におけるクライアントＰＣ１０１のアプリケーションインストールプログラム２０６と携帯端末１０２のライセンス管理プログラム３０６とサーバ１０３のライセンス登録プログラム６０８とによる処理動作を説明するフローチャートであり、次に、これについて説明する。

【００４８】

（１）利用者により、クライアントＰＣ１０１のアプリケーションインストールプログラム２０６が起動させられると、アプリケーションインストールプログラム２０６は、アプリＩＤと乱数とを生成し、それらをアプリＩＤ２１０と乱数２１２とに登録する。ここで、アプリＩＤは、日時やクライアントＰＣ１０１に固有の情報等を利用して生成される（ステップ１１０１、１１１７）。

【００４９】

（２）一方、携帯端末１０２のライセンス管理プログラム３０６が起動されて、クライアントＰＣ１０１のアプリケーションインストールプログラム２０６に接続する（ステップ１１０２）。

【００５０】

（３）クライアントＰＣ１０１のアプリケーションインストールプログラム２０６は、ステップ１１１７でした登録したアプリＩＤ２１０と乱数２１２とを、携帯端末１０２のライセンス管理プログラム３０６に送信する（ステップ１１０３）。

【００５１】

（４）ライセンス管理プログラム３０６は、クライアントＰＣ１０１から受信したアプリＩＤと乱数とをライセンスリスト３０８に登録する。なお、ここでの処理の詳細については、図１３に示すフローにより後述する（ステップ１１０４）。

【００５２】

（５）次に、ライセンス管理プログラム３０６は、レスポンスデータを作成する。なお、ここでの処理の詳細については、図１４に示すフローにより後述する（ステップ１１０５）。

【００５３】

（６）サーバのライセンス管理プログラム３０６は、ステップ１１０５の処理で作成したレスポンスデータとキーリスト３０９内の暗号キーシードとをクライアントＰＣ１０１に返送する（ステップ１１０６）。

【００５４】

（７）クライアントＰＣ１０１のアプリケーションインストールプログラム２０６は、レスポンスデータを受信し、受信したレスポンスデータの確認を行い、アプリケーションをインストールし、利用者にアプリケーションモジュールの利用を一時的に許可する。なお、レスポンスデータの確認の処理の詳細については、図１５に示すフローにより後述する（ステップ１１０７、１１０８）。

【００５５】

図１１により説明した前述までの処理が図９に示すフローのステップ９０３での処理の詳細である。

【００５６】

（８）ここで、利用者は、携帯端末１０２を持って携帯電話の通信可能エリアに移動して

、携帯端末１０２とサーバ１０３とを接続する。携帯端末１０２のライセンス管理プログラム３０６は、サーバ１０３との間での通信が可能となるので、ライセンス認証に必要な登録データをサーバ１０３のライセンス登録プログラム６０８に送信する。なお、ここでの処理の詳細については、図１６に示すフローにより後述する（ステップ１１０９）。

【００５７】

（９）サーバ１０３のライセンス登録プログラム６０８は、携帯端末１０２からの登録データを受信し、受信した登録データをライセンス管理テーブル６１１に登録する。なお、ここでの処理の詳細については、図１７に示すフローにより後述する（ステップ１１１０）。

【００５８】

（10）次に、ライセンス登録プログラム６０８は、後述する図１７のフローのステップ１７０５の処理で復号したキーデータを、共有機密情報Ｂ６０９と暗号モジュール６１５とにより暗号化し、さらに、ステップ１７０２で検索した対象レコードの共有機密情報Ａ８０６の項目と暗号モジュール６１５とにより暗号化し、これを暗号キーとする（ステップ１１１１）。

【００５９】

（11）次に、ライセンス登録プログラム６０８は、ステップ１１１０の処理で受信した登録データのアプリＩＤとステップ１１１１の処理で暗号化した暗号キーを携帯端末１０２のライセンス管理プログラム３０６に送信する（ステップ１１１８）。

【００６０】

（12）携帯端末１０２のライセンス管理プログラム３０６は、暗号キーを受信すると、ライセンスリスト３０８のキー４０４に受信した暗号キーを登録する。なお、ここでの処理の詳細については、図１８に示すフローにより後述する（ステップ１１１２）。

【００６１】

（13）前述したステップ１１０８の処理で、利用が一時的に許可されているアプリケーションモジュールが、一時的な許可の時点から一定時間経過した、あるいは、一定の起動回数となったことを、アプリケーションインストールプログラム２０６が検知したものとする。この場合、一般には、アプリケーションの使用が不可能になる。このような状態で、クライアントＰＣ１０１と携帯端末１０２とが接続されると、携帯端末１０２のライセンス管理プログラム３０６が起動して、アプリケーションインストールプログラム２０６に接続する（ステップ１１１９）。

【００６２】

（14）クライアントＰＣ１０１のアプリケーションインストールプログラム２０６は、携帯端末１０２との接続が行われると、ライセンスの再認証要求として、アプリＩＤ２１０をライセンス管理プログラム３０６に送信する（ステップ１１１３）。

【００６３】

（15）携帯端末のライセンス管理プログラム３０６は、受信した再認証要求に対して暗号キーを返信する。なお、ここでの処理の詳細については、図１９に示すフローにより後述する（ステップ１１１４）。

【００６４】

（16）アプリケーションインストールプログラム２０６は、携帯端末１０２から受信した暗号キーの確認を行い、確認ができたら利用者にアプリケーションモジュールの利用を許可する。なお、ここでの暗号キーの確認の処理の詳細については、図１９に示すフローにより後述する（ステップ１１１５、１１１６）。

【００６５】

図１１により説明したステップ１１０９以降の処理が図９に示すフローのステップ９０４での処理の詳細である。

【００６６】

図１１により説明した処理において、ステップ１１１９以降の処理は、アプリケーションに対するライセンスが正式に認証された後に、定期的行われる当該アプリケーションに

対する継続使用の認証を行う場合にも利用される。

【００６７】

図１３は図１１に示すフローにおけるステップ１１０４での携帯端末１０２のライセンスリストへの登録処理の詳細を説明するフローチャートであり、次に、これについて説明する。

【００６８】

（１）携帯端末１０２のライセンス管理プログラム３０６は、まず、ライセンスリスト３０８の先頭レコードを検索開始位置として、アプリ種別４０２の項目とクライアントＰＣ１０１から受信したアプリ種別とが同じレコードを検索し、同一のレコードがあるか否かを判定し、同一のレコードがなかった場合、ライセンス付与が行われていない等のエラーを意味するので、ここでの処理を終了する（ステップ１３０１、１３０２）。

【００６９】

（２）ステップ１３０２の検索、判定の処理で、同一のレコードが見つかった場合、検索した対象レコードのアプリＩＤの項目に既にデータが登録されているか否かを確認し、既にデータが登録されていた場合、既にアプリＩＤが登録されているので、そのレコードの次のレコードである残りのレコードの先頭を検索開始位置に設定して、ステップ１３０２からの処理に戻って処理を続ける（ステップ１３０３、１３０４）。

【００７０】

（３）ステップ１３０３の確認で、ライセンスリスト３０８の対象レコードのアプリＩＤの項目にデータが登録されていなかった場合、検索した対象レコードのアプリＩＤの項目に受信したアプリＩＤを登録して、図１１のステップ１１０５の処理に進む（ステップ１３０５）。

【００７１】

図１４は図１１に示すフローにおけるステップ１１０５でのレスポンスデータの作成処理の詳細を説明するフローチャートであり、次に、これについて説明する。

【００７２】

（１）携帯端末１０２のライセンス管理プログラム３０６は、まず、キーリスト３０９から利用フラグ５０４の項目が「０」のレコードを検索し、利用フラグ５０４の項目が「０」のレコードがなかった場合、認証作業を続けることができないので、出力部３０５にエラーメッセージを出力して処理を終了する（ステップ１４０１、１４０６）。

【００７３】

（２）ステップ１４０１の検索で、利用フラグ５０４の項目が「０」のレコードがあった場合、検索された対象レコードの暗号キーシード５０３の項目を取得し、ステップ１１０４の処理で受信した乱数とステップ１４０１で検索した対象レコードのキー５０２の項目の値とを連結したデータを入力として、ハッシュ関数モジュール３１４により計算した結果を、認証ハッシュ値として算出する（ステップ１４０２、１４０３）。

【００７４】

（３）次に、携帯端末１０２のライセンス管理プログラム３０６は、ステップ１４０１の処理で検索した対象レコードの利用フラグ５０４の項目に「１」を設定し、ステップ１４０１の処理で検索した対象レコードの暗号キーシード５０３の項目とステップ１４０３で計算した認証ハッシュ値とからレスポンスデータを作成し、図１１のステップ１１０６の処理に進む（ステップ１４０４、１４０５）。

【００７５】

図１５は図１１に示すフローにおけるステップ１１０７での受信したレスポンスデータの確認処理の詳細を説明するフローチャートであり、次に、これについて説明する。

【００７６】

（１）クライアントＰＣ１０１のアプリケーションインストールプログラム２０６は、携帯端末１０２から受信したレスポンスデータの暗号キーシードを、共有機密情報Ｂ２０９と暗号モジュール２１３とにより復号する（ステップ１５０１）。

【００７７】

（２）次に、アプリケーションインストールプログラム２０６は、ハッシュ関数モジュール２１４に、ステップ１５０１の処理で復号したデータを入力して、ハッシュ値を計算すると共に、乱数２１２と計算したハッシュ値とを連結し、これをハッシュ関数モジュール２１４に入力して確認用認証ハッシュ値を計算する（ステップ１５０２、１５０３）。

【００７８】

（３）そして、ステップ１５０２の処理で算出した受信したレスポンスデータの認証ハッシュ値とステップ１５０３の処理で算出した確認用認証ハッシュ値とを比較し、それらの値が同一か否かを判定する（ステップ１５０４）。

【００７９】

（４）ステップ１５０４の判定で２つのハッシュ値が同一であった場合、ステップ１５０２で算出したハッシュ値をキー２１１に登録し、図１１のステップ１１０８の処理に進み、２つのハッシュ値が同一でなかった場合、認証作業を続けることができないので、出力部２０５にエラーメッセージを出力して処理を終了する（ステップ１５０５、１５０６）。

【００８０】

図１６は図１１に示すフローにおけるステップ１１０９での携帯端末１０２のライセンス管理プログラム３０６がライセンス認証に必要な登録データをサーバ１０３に送信する処理の詳細を説明するフローチャートであり、次に、これについて説明する。

【００８１】

（１）携帯端末１０２のライセンス管理プログラム３０６は、まず、キーリスト３０９の先頭レコードを検索開始位置とし、キーリスト３０９の利用フラグ５０４の項目が「０」のレコードを検索して、対応するレコードがあるか否かを判定する（ステップ１６０１、１６０２）。

【００８２】

（２）ステップ１６０２の検索、判定の処理で、利用フラグ５０４の項目が「０」のレコードが見つかった場合、ステップ１６０２の処理で検索した対象レコードのキー５０２の項目を取得する（ステップ１６０３）。

【００８３】

（４）ライセンスリスト３０８のキー４０４の項目が、ステップ１６０３の処理で取得したキーと同一のレコードを検索して、対応するレコードがあるか否かを判定し、対応するレコードがなかった場合、認証作業を続けることができないので、出力部３０５にエラーメッセージを出力して処理を終了するする（ステップ１６０４、１６１０）。

【００８４】

（５）ステップ１６０４の検索、判定で対応するレコードがあった場合、ステップ１６０４の処理で検索した対象レコードのアプリ種別４０２と利用アプリＩＤ４０３と共有機密情報Ａ４０５との項目を取得する（ステップ１６０５）。

【００８５】

（６）次に、ステップ１６０３の処理で取得したキーをステップ１６０５の処理で取得した共有機密情報Ａ４０５と暗号モジュール３１３とにより暗号化する（ステップ１６０６）。

【００８６】

（７）ステップ１６０５の処理で取得したアプリＩＤとアプリ種別、ステップ１６０６の処理で暗号化したキー、ユーザＩＤ３１２を登録データとしてまとめて、サーバ１０３のライセンス登録プログラム６０８に送信する（ステップ１６０７）。

【００８７】

（８）その後、前述までの処理を行ったキーリスト３０９のレコードの次のレコードである残りのレコードの先頭を検索開始位置に設定して、ステップ１６０２からの処理に戻って処理を続ける（ステップ１６０８）。

【００８８】

（９）ステップ１６０２での検索、判定で、キーリスト３０９の利用フラグ５０４の項目

が「０」のレコードがなかった場合、ステップ１６０２での検索結果として検索された対象レコードが１つ以上あったか否かを判定する。なお、検索された対象レコード（利用フラグ５０４の項目が「０」のレコード）の数は、前述した処理を行う途中で、図示しない処理によりカウントされているものとする（ステップ１６０９）。

【００８９】

（10）ステップ１６０９の判定で、対象レコードがなかった場合、処理を終了し、対象レコードが合った場合、図１１のステップ１１１０の処理に進む。

【００９０】

図１７は図１１に示すフローにおけるステップ１１１０でのサーバ１０３のライセンス登録プログラム６０８が登録データをライセンス管理テーブル６１１に登録する処理の詳細説明するフローチャートであり、次に、これについて説明する。

【００９１】

（１）サーバ１０３のライセンス登録プログラム６０８は、まず、ライセンス管理テーブル６１１の先頭レコードを検索開始位置として、ライセンス管理テーブル６１１のユーザＩＤ８０２の項目と携帯端末１０２から受信した登録データのユーザＩＤとが同一のレコードを検索し、同一のレコードが見つからなかった場合、ライセンス認証に失敗したことになるので、処理を終了する（ステップ１７０１、１７０２、１７０７）。

【００９２】

（２）ステップ１７０２の検索で、ユーザＩＤが一致するレコードが見つかった場合、ステップ１７０２の処理で検索した対象レコードのライセンスアプリ８０３の項目が、受信した登録データのアプリ種別と同一か否かを確認する（ステップ１７０３）。

【００９３】

（３）ステップ１７０３の確認で、ライセンスアプリ８０３の項目が、受信した登録データのアプリ種別と同一であった場合、ステップ１７０２の処理で検索した対象レコードのキー８０５の項目に、データが登録されていないことを確認する（ステップ１７０４）。

【００９４】

（４）ステップ１７０４の確認で、対象レコードのキー８０５の項目に、データが登録されていなかった場合、携帯端末１０２から受信した登録データのキーをステップ１７０２の処理で検索した対象レコードの共有機密情報Ａ８０６の項目と暗号モジュール６１５とにより復号する（ステップ１７０５）。

【００９５】

（５）その後、ステップ１７０２の処理で検索した対象レコードのキー８０５とアプリＩＤ８０４との項目に、ステップ１７０５で復号したデータと受信した登録データのアプリＩＤとを登録して、図１１のステップ１１１１の処理に進む（ステップ１７０６）。

【００９６】

（６）ステップ１７０３の確認で、ライセンスアプリ８０３の項目が、受信した登録データのアプリ種別と同一でなかった場合、あるいは、ステップ１７０４の確認で、対象レコードのキー８０５の項目にデータが登録されていた場合、ライセンス管理テーブル６１１の前述までの処理を行った次のレコードを検索の先頭レコードを検索開始位置とし、ステップ１７０２からの処理に戻って処理を続ける（ステップ１７０８）。

【００９７】

図１８は図１１に示すフローにおけるステップ１１１２での携帯端末１０２のライセンス管理プログラム３０６がサーバ１０３から受信した暗号キーをライセンスリスト３０８に登録する処理の詳細を説明するフローチャートであり、次に、これについて説明する。

【００９８】

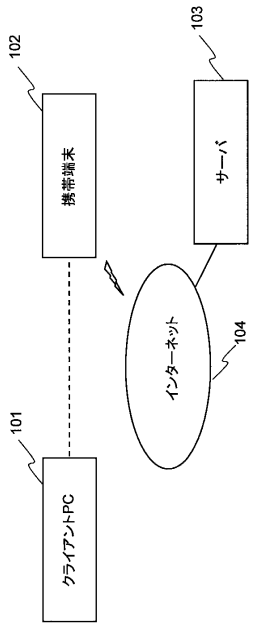
（１）携帯端末１０２のライセンス管理プログラム３０６は、ライセンスリスト３０８の利用アプリＩＤ４０３の項目と受信したアプリＩＤとが同一のレコードを検索し、同一のレコードがあったか否かを判定し、同一のレコードがなかった場合、ライセンス認証に失敗したので、認証失敗メッセージを出力部３０５に表示して、処理を終了する。（ステップ１８０１、１８０６）。

【００９９】
（２）ステップ１８０１の検索、判定で、ライセンスリスト３０８に受信したアプリＩＤとが同一のレコードがあった場合、ステップ１８０１の処理で検索した対象レコードのキー４０４の項目を取得し、キーリスト３０９のキー５０２の項目とライセンスリスト３０８から取得したキーが同一のレコードをキーリスト３０９から削除するする（ステップ１８０２、１８０３）。
【０１００】
（３）サーバ１０３から受信した暗号キーを、ステップ１８０１で検索した対象レコードの共有機密情報Ａ４０５と暗号モジュール３１３とにより復号し、ステップ１８０１の処理で検索した対象レコードのキー４０４の項目を前述で復号したデータに置き換える（ステップ１８０４、１８０５）。
【０１０１】
図１９は図１１に示すフローにおけるステップ１１１４での携帯端末１０２のライセンス管理プログラム３０６が、クライアントＰＣ１０１から受信した再認証要求に対して暗号キーを返信する処理の詳細を説明するフローチャートであり、次に、これについて説明する。
【０１０２】
（１）携帯端末１０２のライセンス管理プログラム３０６は、ライセンスリスト３０８の利用アプリＩＤ４０３の項目とクライアントＰＣから受信したアプリＩＤとが同一のレコードを検索し、対象レコードがあるか否か判定する。この判定で、対象レコードがなかった場合、ライセンス認証に失敗したことになるので、処理を終了する（ステップ１９０１、１９０３）。
【０１０３】
（２）ステップ１９０１の検索、判定で、クライアントＰＣから受信したアプリＩＤとが同一のレコードがライセンスリスト３０８にあった場合、ステップ１９０１の処理で検索した対象レコードのキー４０４の項目を、クライアントＰＣ１０１のアプリケーションインストールプログラム２０６に返信して、図１１のステップ１１１５の処理へ進む（ステップ１９０２）。
【０１０４】
図２０は図１１に示すフローにおけるステップ１１１５でのクライアントＰＣ１０１のアプリケーションインストールプログラム２０６が携帯端末１０２から受信した暗号キーの確認を行う処理の詳細を説明するフローチャートであり、次に、これについて説明する。
【０１０５】
（１）クライアントＰＣ１０１のアプリケーションインストールプログラム２０６は、携帯端末１０２から受信した暗号キーを共有機密情報Ｂ２０９と暗号モジュール２１３とにより復号する（ステップ２００１）。
【０１０６】
（２）次に、ステップ２００１の処理で復号した暗号キーと自ＰＣ内のキー２１１とを比較し、異なっていた場合、ライセンス認証に失敗したことになるので、処理を終了し、キーが一致していた場合、図１１のステップ１１１６の処理に進む（ステップ２００２、２００３）。
【図面の簡単な説明】
【０１０７】
【図１】本発明の一実施形態によるライセンス認証システムの構成を示すブロック図である。
【図２】クライアントＰＣの構成を示すブロック図である。
【図３】携帯端末の構成を示すブロック図である。
【図４】携帯端末が持つライセンスリストの構成を示す図である。
【図５】携帯端末が持つキーリストの構成を示す図である。

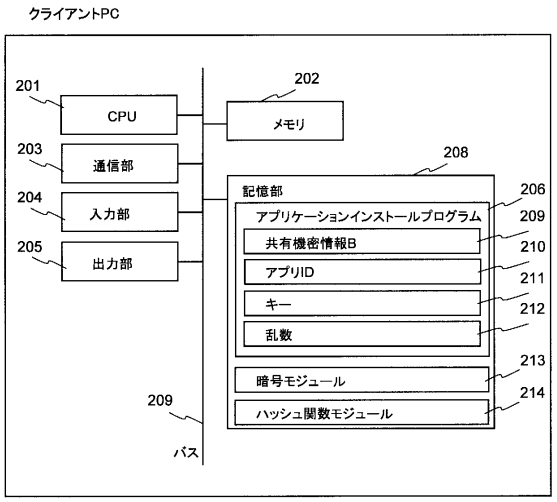
【図６】サーバの構成を示すブロック図である。
【図７】サーバが持つアプリケーションリストの構成を示す図である。
【図８】サーバが持つライセンス管理テーブルの構成を示す図である。
【図９】本発明の実施形態によるライセンス認証システム全体の処理動作を説明するフローチャートである。
【図１０】図９のステップ９０２の処理での仮ライセンス取得のための携帯端末のライセンス取得プログラムとサーバのライセンス発行プログラムとによる処理動作を説明するフローチャートである。
【図１１】図９のステップ９０３、９０４の処理でのクライアントＰＣのアプリケーションインストールプログラムと携帯端末のライセンス管理プログラムとサーバのライセンス登録プログラムとによる処理動作を説明するフローチャートである。
【図１２】図９のステップ９０１での処理でのサーバのインストール作成プログラム６０７処理動作の詳細を説明するフローチャートである。
【図１３】図１１に示すフローのステップ１１０４での携帯端末のライセンスリストへの登録処理の詳細を説明するフローチャートである。
【図１４】図１１に示すフローのステップ１１０５でのレスポンスデータの作成処理の詳細を説明するフローチャートである。
【図１５】図１１に示すフローにおけるステップ１１０７での受信したレスポンスデータの確認処理の詳細を説明するフローチャートである。
【図１６】図１１に示すフローのステップ１１０９での携帯端末のライセンス管理プログラムがライセンス認証に必要な登録データをサーバに送信する処理の詳細を説明するフローチャートである。
【図１７】図１１に示すフローのステップ１１１０でのサーバのライセンス登録プログラムが登録データをライセンス管理テーブルに登録する処理の詳細説明するフローチャートである。
【図１８】図１１に示すフローのステップ１１１２での携帯端末のライセンス管理プログラムがサーバから受信した暗号キーをライセンスリストに登録する処理の詳細を説明するフローチャートである。
【図１９】図１１に示すフローのステップ１１１４での携帯端末のライセンス管理プログラムが、クライアントＰＣから受信した再認証要求に対して暗号キーを返信する処理の詳細を説明するフローチャートである。
【図２０】図１１に示すフローのステップ１１１５でのクライアントＰＣのアプリケーションインストールプログラムが携帯端末から受信した暗号キーの確認を行う処理の詳細を説明するフローチャートである。
【符号の説明】
【０１０８】
１０１　クライアントＰＣ
１０２　携帯端末、
１０３　サーバ
１０４　インターネット
２０１、３０１、６０１　ＣＰＵ
２０２、３０２、６０２　メモリ
２０３、３０３、６０３　通信部
２０４、３０４、６０４　入力部
２０５、３０５、６０５　出力部
２０６　アプリケーションインストールプログラム
２０７、３１１　バス
２０８、３１０、６１２　記憶部
２０９、６０９　共有機密情報Ｂ
２１０　アプリＩＤ

２１１　キー
２１２　乱数
２１３、３１３、６１５　暗号モジュール
２１４、３１４、６１６　ハッシュ関数モジュール
３０６　ライセンス管理プログラム
３０７　ライセンス取得プログラム
３０８　ライセンスリスト
３０９　キーリスト
３１２　ユーザＩＤ
３１５、６１７　共有機密シード
６０６　ライセンス発行プログラム
６０７　インストール作成プログラム
６０８　ライセンス登録プログラム
６１０　アプリケーションリスト
６１１　ライセンス管理テーブル
６１４　アプリケーションインストールモジュール

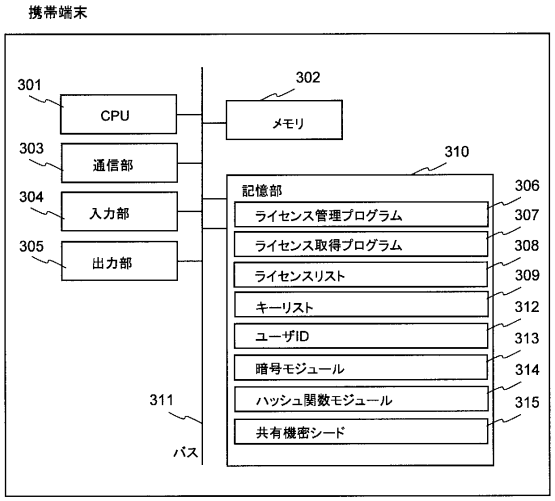
【図１】



【図２】



【図３】



【図４】

ライセンスリスト

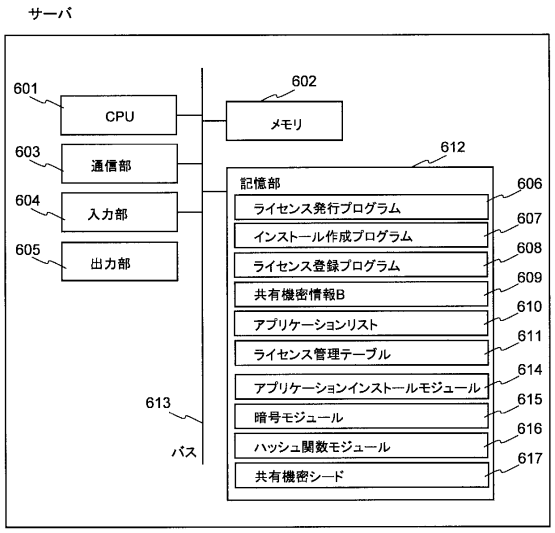
401 項番	402 アプリ種別	403 利用アプリID	404 キー	405 共有機密情報A
1	Document	App02-123	ab123efg	daiojw3kda9
2	Encrypt	App01-124	Za8t3YsI	D)jda9a49id
3	. . .	. . .	. . .	. . .

【図５】

キーリスト

501 項番	502 キー	503 暗号キーシード	504 利用フラグ
1	ab123efg	j9jo4q8:]-^k:ipaoP	1
2	Za8t3YsI	9thP23ieaoUZjzAi	0
3	. . .	. . .	. . .

【図６】



【図７】

アプリケーションリスト

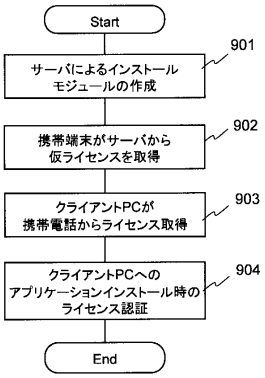
701 項番	702 アプリ種別	703 モジュール格納場所
1	Document	¥App01.dll
2	Encrypt	¥App02.dll
3	. . .	. . .

【図８】

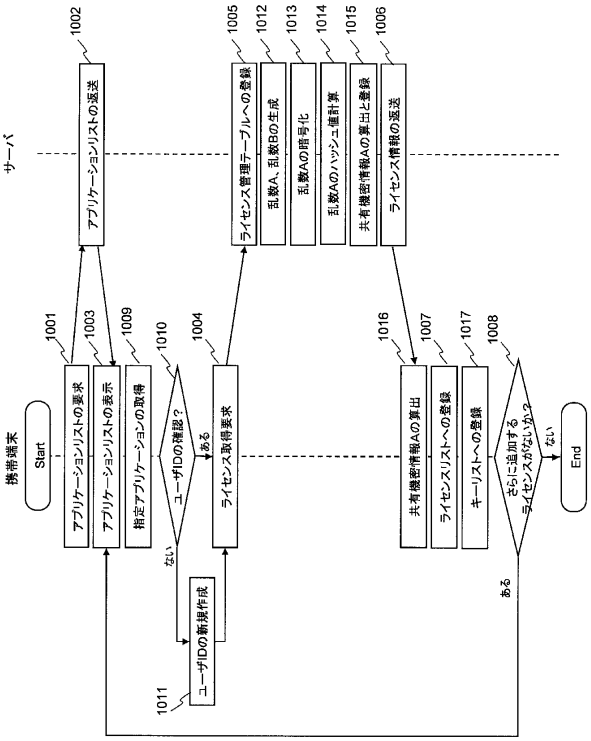
ライセンス管理テーブル

801 項番	802 ユーザID	803 ライセンスアプリ	804 アプリID	805 キー	806 共有機密情報A
1	User11	Document	App02-123	ab123efg	daiojw3kda9
2	User12	Encrypt	App01-124	Za8t3YsI	D)jda9a49id
3	. . .	. . .	. . .	. . .	. . .

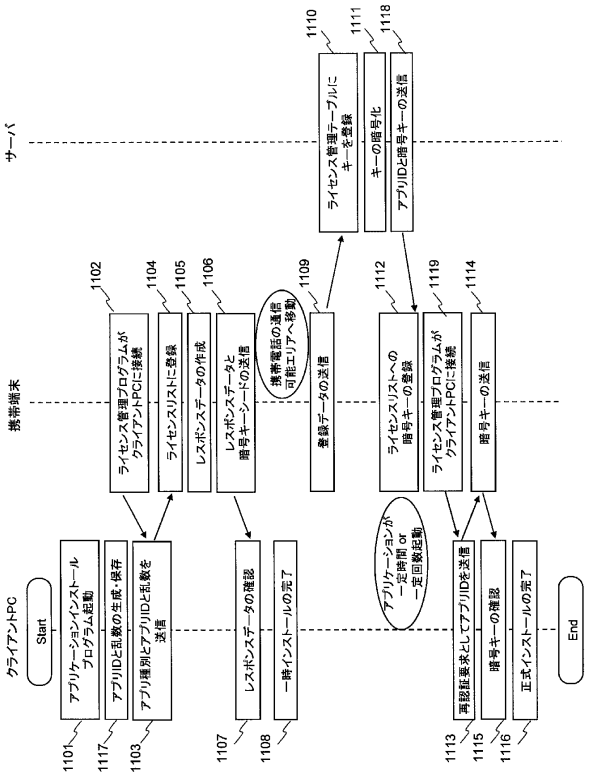
【図９】



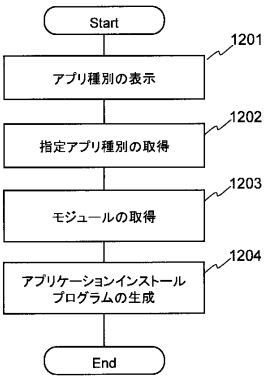
【図１０】



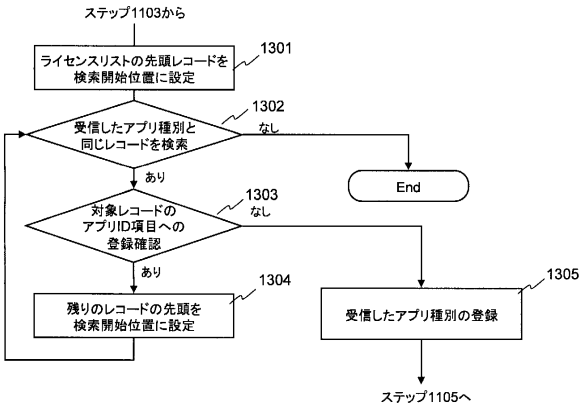
【図１１】



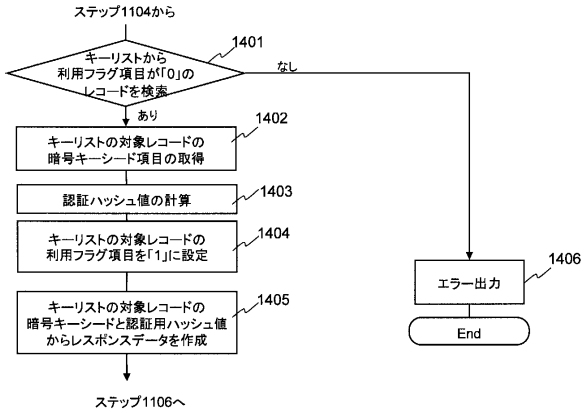
【図１２】



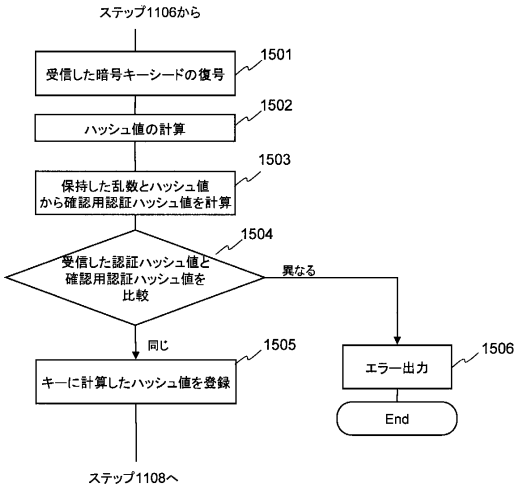
【図１３】



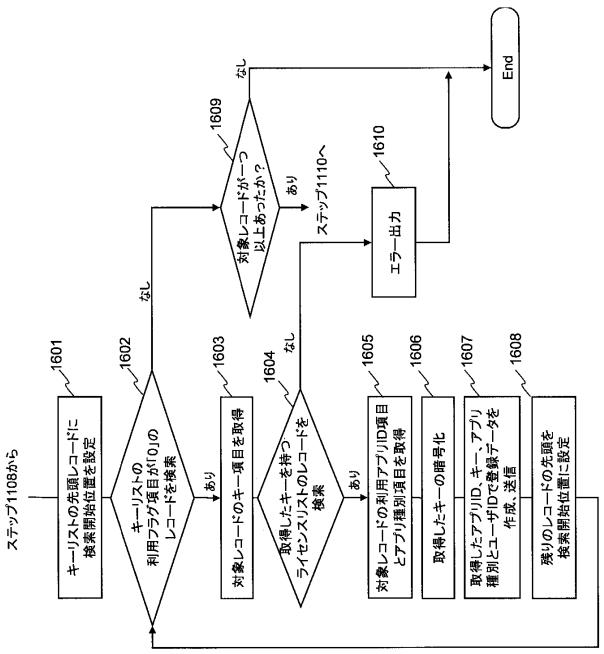
【図１４】



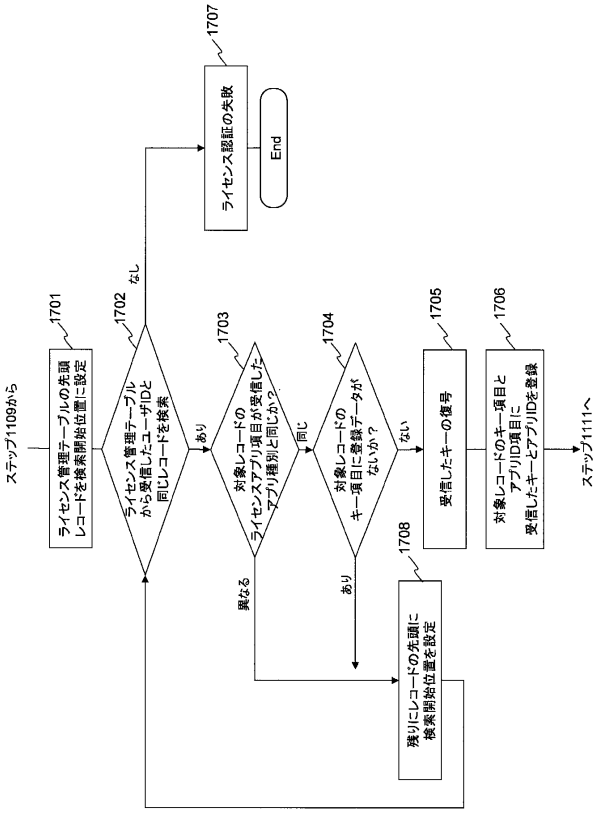
【図１５】



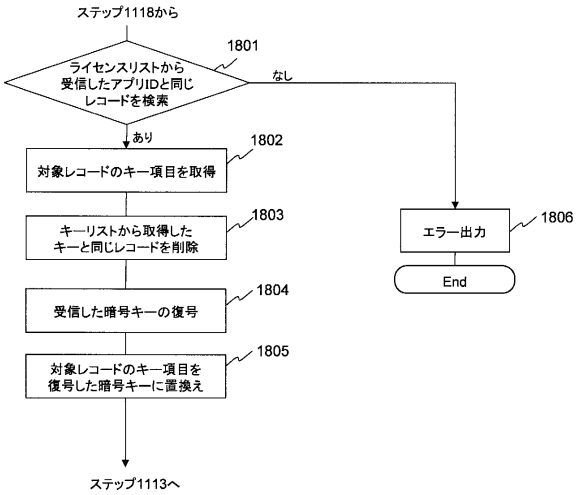
【図１６】



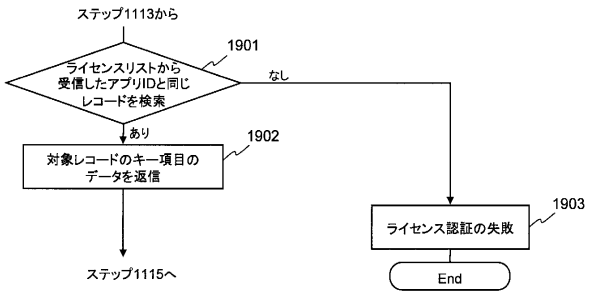
【図１７】



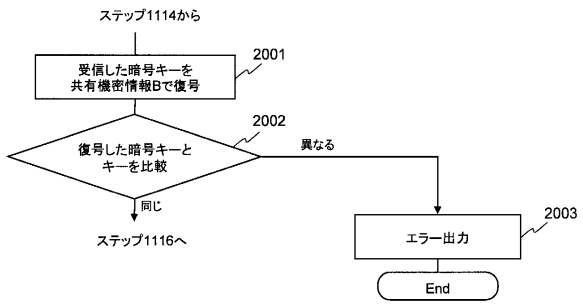
【図１８】



【図１９】



【図２０】



フロントページの続き

(56)参考文献 特開２００５－１６５６３１（ＪＰ，Ａ）
特開２００４－１７８１２１（ＪＰ，Ａ）
特開２００５－１２２２８３（ＪＰ，Ａ）
特開２００１－３２５４５５（ＪＰ，Ａ）
特開２０００－２９３３６８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２２