(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年9 月8 日 (08.09.2006)

PCT

(10) 国際公開番号
WO 2006/093148 A1

(51) 国際特許分類:
H04Q 7/38 (2006.01) *H04L 9/32* (2006.01)
H04B 7/26 (2006.01)

(21) 国際出願番号: PCT/JP2006/303749

(22) 国際出願日: 2006 年2 月28 日 (28.02.2006)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2005-058868 2005 年3 月3 日 (03.03.2005) JP

(71) 出願人 (米国を除く全ての指定国について): フェリカネットワークス株式会社 (FELICA NETWORKS, INC.) [JP/JP]; 〒1410032 東京都品川区大崎１－１１－１ ゲートシティー大崎 ウェストタワー Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 徳野 行太 (TOKUNO, Kota). 疋田 智治 (HIKITA, Tomoharu).

(74) 代理人: 中村 友之 (NAKAMURA, Tomoyuki); 〒1050001 東京都港区虎ノ門１丁目２番８号 虎ノ門琴平タワー 三好内外国特許事務所内 Tokyo (JP).

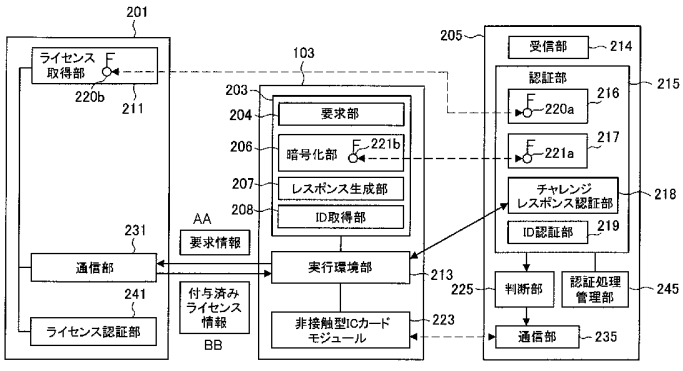
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR),

[続葉有]

(54) Title: DATA COMMUNICATION SYSTEM, ALTERNATE SYSTEM SERVER, COMPUTER PROGRAM, AND DATA COMMUNICATION METHOD

(54) 発明の名称: データ通信システム，代行システムサーバ，コンピュータプログラム，およびデータ通信方法



211 LICENSE ACQUIRING PART
231 COMMUNICATING PART
241 LICENSE AUTHENTICATING PART
AA REQUESTED INFORMATION
BB GIVEN LICENSE INFORMATION
204 REQUESTING PART
206 ENCRYPTING PART
207 RESPONSE GENERATING PART
208 ID ACQUIRING PART
213 EXECUTION ENVIRONMENT PART
223 NONCONTACT IC CARD MODULE
214 RECEIVING PART
215 AUTHENTICATING PART
218 CHALLENGE RESPONSE AUTHENTICATING PART
219 ID AUTHENTICATING PART
225 DETERMINING PART
245 AUTHENTICATION PROCESS MANAGING PART
235 COMMUNICATING PART

(57) Abstract: A data communication system wherein one or two types of authenticating means are combined to authenticate a mobile communication terminal or the like and a communication process is executed for a noncontact IC card module, and wherein an alternate system (105) comprises an authenticating part (215) for executing, based on given license information received from the mobile communication terminal (103), at least one of a process in which to authenticate a service providing system (101) by use of a system authentication key, a process in which to authenticate the mobile communication terminal by use of a client authentication key, and a process in which to authenticate the mobile communication terminal by use of identification information for identifying the mobile communication terminal; a determining part (225) for determining, based on the given license information, whether communication is to be permitted or not; and a communicating part (235) for performing a communication with the noncontact IC card module when it is determined by the determining part that the communication is to be permitted.

[続葉有]

WO 2006/093148 A1

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 代行システム（１０５）は，システム認証鍵を用いることでサービス提供システム（１０１）を認証する処理，クライアント認証鍵を用いることで携帯通信端末（１０３）を認証する処理，または携帯通信端末を識別する識別情報を用いることで携帯通信端末を認証する処理のうち少なくとも一つの認証処理を携帯通信端末からの付与済みライセンス情報を基にして実行する認証部（２１５）と；付与済みライセンス情報に基づいて通信許可／通信不許可を判断する判断部（２２５）と；上記判断部によって通信許可されると，非接触型ＩＣカードモジュールと通信処理を行う通信部（２３５）とを備え、１又は２種類の認証手段を組み合わせて携帯通信端末等を認証し，非接触型ＩＣカードモジュールに対して通信処理を実行するデータ通信システムを提供する。

明 細 書

データ通信システム，代行システムサーバ，コンピュータプログラム，およびデータ通信方法

技術分野

[0001] 本発明はデータ通信システム，代行システムサーバ，コンピュータプログラム，およびデータ通信方法に関する。

背景技術

[0002] 現在では，情報処理技術の発展，ネットワーク技術の多様化により，PC（パーソナルコンピュータ）等の情報処理装置からネットワークを介してサーバ等の装置が保有する数多くの情報に手軽にアクセスできることが一般的となっている。

[0003] また，例えば，従来では通話機能に限定されていた携帯電話についても現在ではプロトコル変換等によってインターネット等のネットワークを介して数多くの情報に手軽にアクセスでき情報処理装置と同等の機能を備えつつある。

[0004] 一方で，リーダライタ（R／W）を介して他のサーバ等の情報処理装置と通信をすることが可能な非接触型ICカードが実用化されている。さらに，かかる非接触型ICカード又は非接触型ICカード機能を具備した装置（以下，非接触型ICカードモジュール）を携帯電話等の小型軽量な携帯通信端末に搭載し，例えば外部のシステムと非接触型ICカードとの間で通信する技術が開示されている（例えば文献1（特開2002－133373号公報）参照）。

[0005] かかる先行文献1においては，非接触型ICカードモジュールには，複数のアプリケーションを登録することが可能である。上記アプリケーションは，サービス提供者側に属するサービス提供管理システムなどによって作成される。

[0006] 利用者は，例えば利用者の用途に応じて複数種類のアプリケーションを登録し，リーダライタにかざして非接触型ICカードモジュールに情報処理させることで，利用者はサービス提供システムが提供するサービスを享受することができる。

[0007] なお，非接触型ICカードモジュールに記憶された情報を読み込んだり，書き込んだりする等の情報処理を実行する場合，その非接触型ICカードを発行及び／又は運

用する事業者側に属す管理システムから非接触型ICカードに対する通信処理によって行われる。

発明の開示

[0008] しかしながら，携帯通信端末に備わる非接触型ICカードモジュールと通信処理を行う場合，管理システム側で，セキュリティ上の点から当該携帯通信端末を認証する必要があるが，携帯通信端末を管理するキャリア（通信事業者など）ごとに認証方式が異なったり又は認証する手段が存在しなかったりと認証に関して統一されず又は不十分であった。

[0009] したがって，利用者側では認証方式の異なるサービス提供システムからはサービスを享受することができない等，非接触型ICカードモジュールに対して効率よく情報処理を実行させることができず，また提供者側では管理システムが対応可能な認証手段の選択が限定されている等，認証処理に柔軟性が図られていなかった。

[0010] 本発明は，上記問題点に鑑みてなされたものであり，本発明の目的は，1又は2種類の認証手段を組み合わせて，携帯通信端末を認証し，当該携帯通信端末に備わる非接触型ICカードモジュールに対して通信処理を実行することが可能な，新規かつ改良されたデータ通信システム，代行システムサーバ，コンピュータプログラム，およびデータ通信方法を提供することである。

[0011] 上記課題を解決するため，本発明の第1の観点によれば，それぞれが外部からの要求に応じて情報処理する非接触型ICカードモジュールを備える一つ以上の携帯通信端末と，その非接触型ICカードモジュールの情報処理によってサービスを提供するサービス提供システムと，該サービス提供システムを代行して非接触型ICカードモジュールと通信処理する代行システムとを備えたデータ通信システムが提供される。上記データ通信システムにおける携帯通信端末は，非接触型ICカードモジュールと代行システムとが通信処理を行うために，サービス提供システムが保有する情報であって携帯通信端末に付与された該通信処理に関するライセンスを示す付与済みライセンス情報を要求する要求部を備え，サービス提供システムは，携帯通信端末の1つから要求されると，該要求元の携帯通信端末に係る付与済みライセンス情報を取得する取得部とを備えており，その取得した付与済みライセンス情報は，代行システ

ム及びサービス提供システムの双方が保持し該双方との間で情報を暗号化／復号可能なシステム認証鍵で上記サービス提供システムによって暗号化され，携帯通信端末及び代行システムの双方が保持し該双方との間で情報を暗号化／復号可能なクライアント認証鍵で携帯通信端末によってさらに暗号化されて代行システムに送信され，代行システムは，(1)システム認証鍵を用いることでサービス提供システムを認証するシステム認証処理，(2)クライアント認証鍵を用いることで携帯通信端末を認証する第1のクライアント認証処理，および(3)携帯通信端末を識別する識別情報を用いることで携帯通信端末を認証する第2のクライアント認証処理を含む複数の認証処理うち少なくとも一つの認証処理を携帯通信端末からの付与済みライセンス情報を基にして実行する認証部と；認証部による認証処理後，付与済みライセンス情報に設定されたライセンスに基づいて通信許可／通信不許可を判断する判断部と；上記判断部によって通信が許可されると，非接触型ICカードモジュールと通信処理を行う通信部とを備える。なお，上記識別情報は携帯通信端末を識別する場合を例に挙げて説明したが，かかる例に限定されず，例えば，識別情報は携帯通信端末に格納されるクライアントアプリケーションを識別する場合等でもよく，またシステム認証鍵又はクライアント認証鍵は，所定間隔ごとに別のシステム認証鍵又はクライアント認証鍵に更新されてもよい。

[0012] 本発明によれば，データ通信システムでは，携帯通信端末がサービス提供システムから付与済みライセンス情報を受け取り，その付与済みライセンス情報を代行システムに送信することで，代行システムは，1又は2種以上の認証処理から少なくとも一つを選択し組み合わせた認証処理を実行することで，その付与済みライセンス情報からサービス提供システム，携帯通信端末の真正性を検証する。検証の結果，通信処理が許可されると，携帯通信端末に備わる非接触型ICカードモジュールと通信部とが通信処理をする。かかる構成により，サービス提供システムのセキュリティレベル等に応じて代行システムにおける認証処理を選択し，組み合わせて認証することができるため，汎用性の高い認証処理を可能とし，その結果，携帯通信端末の機種等に依存せずに非接触型ICカードモジュールに対する情報処理の実行が可能となり，汎用性の高いデータ通信システムを実現できる。

[0013] 認証部は，1又は2種以上の認証処理のうち一つあるいは二つ以上選択され組み合わされた認証処理の選択指示を受信し，受信した前記選択指示に従って認証処理を実行するように構成してもよい。かかる構成により，サービス提供システム又は代行システムからの要求を選択指示として受付けて認証処理を実行することで，より柔軟性，汎用性の高い認証処理を可能とする。

[0014] 上記通信部が行う通信処理は，非接触型ICカードモジュールに書き込み処理又は読み込み処理を実行させる処理であるように構成してもよい。

[0015] 上記読み込み処理の対象となるデータについて，そのデータを暗号化する処理又はデータを基にして作成される電子署名を該データに付加する処理のうち一方あるいは両方の処理の選択指示を受け付け，上記認証部は，受け付けた選択指示に従って処理するように構成してもよい。

[0016] 上記書き込み処理の対象となるデータについて，暗号化されたデータを復号する処理および予め電子署名が付加されたデータを基にしてそのデータの真正性を検証する処理のうち一方あるいは両方の処理の選択指示が受け付け，上記認証部は，その選択指示に従って処理するように構成してもよい。

[0017] 上記サービス提供システムと上記代行システムとの通信は，携帯通信端末を介して行われるように構成してもよい。

[0018] 上記第1のクライアント認証処理は，携帯通信端末に対してチャレンジコードを送信し，そのチャレンジコードと付与済みライセンス情報とを基にして作成されるレスポンスを受けることによって認証するチャレンジレスポンス方式の認証処理であるように構成してもよい。なお，かかる例に限定されず，例えば，本発明は係る第1のクライアント認証処理は，チャレンジコードと付与済みライセンス情報とクライアント認証鍵とを基にして作成されるレスポンスを受けることによって認証する等の場合でもよい。

[0019] 上記携帯通信端末は，携帯電話であるように構成してもよい。かかる構成により，携帯電話のキャリアや，機種などの相違に因らず代行システム側で認証処理を可能とし，非接触型ICカードモジュールに対して情報処理を実行させることができる。

[0020] 上記課題を解決するために，本発明の別の観点によれば，携帯通信端末に備わる非接触型ICカードモジュールが情報処理することでサービスを提供するサービス提

供サーバを代行して，該非接触型ICカードモジュールと通信処理する代行システムサーバが提供される。上記代行システムサーバは，非接触型ICカードモジュールと代行システムサーバとの通信処理に関するライセンスを示した付与済みライセンス情報は代行システムサーバ及びサービス提供サーバの双方が保持し該双方との間で情報を暗号化／復号可能なシステム認証鍵で前記サービス提供サーバによって暗号化されて，さらに該携帯通信端末及び前記代行システムサーバの双方が保持し該双方との間で情報を暗号化／復号可能なクライアント認証鍵で携帯通信端末によって暗号化され，その暗号化された付与済みライセンス情報を該携帯通信端末から受信する受信部と；システム認証鍵を用いることでサービス提供システムを認証するシステム認証処理，クライアント認証鍵を用いることで携帯通信端末を認証する第1のクライアント認証処理，および携帯通信端末を識別する識別情報を用いることで携帯通信端末を認証する第2のクライアント認証処理を含む複数の認証処理のうち少なくとも一つの認証処理を携帯通信端末からの付与済みライセンス情報を基にして実行する認証部と；上記認証部による認証処理後，付与済みライセンス情報に基づき通信許可／通信不許可を判断する判断部と；上記判断部によって通信許可されると，非接触型ICカードモジュールと通信処理を行う通信部とを備える。

[0021] 本発明によれば，代行システムサーバは，携帯通信端末から送信される付与済みライセンス情報を上記受信部が受け取り，その付与済みライセンス情報を基にして，1又は2種以上の認証処理から少なくとも一つを選択し組み合わせた認証処理を実行することで，サービス提供システム，携帯通信端末の真正性を検証する。検証の結果，通信処理を許可すると，携帯通信端末に備わる非接触型ICカードモジュールと通信部とが通信処理をする。かかる構成により，サービス提供サーバ側のセキュリティレベル等に応じて実行可能な1又は2種以上の認証処理のうちから適切な認証処理を選択し，組み合わせて代行システムサーバが実行することができるため，汎用性の高い認証処理を可能とし，その結果，携帯通信端末の機種等に依存せずに非接触型ICカードモジュールに対して情報処理を実行させることができる。

[0022] 上記認証部は，1又は2種以上の認証処理のうち一つあるいは二つ以上選択され組み合わされた認証処理の選択指示を受信し、受信した選択指示に従って認証処

理を実行するように構成してもよい。

[0023] 上記課題を解決するために，本発明の別の観点によれば，コンピュータをして，携帯通信端末に備わる非接触型ICカードモジュールが情報処理することでサービスを提供するサービス提供サーバを代行して，該非接触型ICカードモジュールと通信処理する代行システムサーバとして機能させるコンピュータプログラムが提供される。上記コンピュータプログラムは，非接触型ICカードモジュールと代行システムサーバとの通信処理に関するライセンスを示した付与済みライセンス情報は代行システムサーバ及びサービス提供サーバの双方が保持し該双方との間で情報を暗号化／復号可能なシステム認証鍵で前記サービス提供サーバによって暗号化されて，さらに該携帯通信端末及び前記代行システムサーバの双方が保持し該双方との間で情報を暗号化／復号可能なクライアント認証鍵で携帯通信端末によって暗号化され，その暗号化された付与済みライセンス情報を該携帯通信端末から受信する受信手段と；システム認証鍵を用いることでサービス提供サーバを認証するシステム認証処理，クライアント認証鍵を用いることで携帯通信端末を認証する第1のクライアント認証処理，または携帯通信端末を識別する識別情報を用いることで携帯通信端末を認証する第2のクライアント認証処理を含む複数の認証処理のうち少なくとも一つの認証処理を携帯通信端末からの付与済みライセンス情報を基にして実行する認証手段と；上記認証処理した後，付与済みライセンス情報に基づき通信許可／通信不許可を判断する判断手段と；上記判断した結果，通信処理が許可された場合，非接触型ICカードモジュールと通信処理を行う通信手段とを備える。

[0024] 上記課題を解決するために，本発明の別の観点によれば，携帯通信端末に備わる非接触型ICカードモジュールが情報処理することでサービスを提供するサービス提供サーバを代行して，該非接触型ICカードモジュールと通信処理する代行システムサーバのデータ通信方法が提供される。上記データ通信方法は，非接触型ICカードモジュールと代行システムサーバとの通信処理に関するライセンスを示した付与済みライセンス情報は代行システムサーバ及びサービス提供サーバの双方が保持し該双方との間で情報を暗号化／復号可能なシステム認証鍵で前記サービス提供サーバによって暗号化されて，さらに該携帯通信端末及び前記代行システムサーバの双方

が保持し該双方との間で情報を暗号化／復号可能なクライアント認証鍵で携帯通信端末によって暗号化され，その暗号化された付与済みライセンス情報を該携帯通信端末から受信する受信ステップと；上記システム認証鍵を用いることでサービス提供サーバを認証するシステム認証処理，クライアント認証鍵を用いることで携帯通信端末を認証する第1のクライアント認証処理，および携帯通信端末を識別する識別情報を用いることで携帯通信端末を認証する第2のクライアント認証処理を含む複数の認証処理のうち少なくとも一つの認証処理を携帯通信端末からの付与済みライセンス情報を基にして実行する認証ステップと；認証ステップを実行した後，付与済みライセンス情報に基づき通信許可／通信不許可を判断する判断ステップと；判断ステップにおける判断結果が通信許可の場合，非接触型ICカードモジュールと通信処理を行う通信ステップとを含む。

図面の簡単な説明

[0025] [図1]図1は、本実施の形態にかかるデータ通信システムの概略の一例を示す説明図である。

[図2]図2は、本実施の形態にかかるデータ通信システムに備わるサービス提供システムの概略を示す説明図である。

[図3]図3は、本実施の形態に係るライセンス取得部の付与済みライセンス情報生成処理の概略を示す説明図である。

[図4]図4は、本実施の形態にかかる携帯通信端末の概略的な構成の一例を示すブロック図である。

[図5]図5は、本実施の形態にかかるレスポンス生成部による暗号化処理の概略的な一例を示す説明図である。

[図6]図6は、本実施の形態にかかる認証処理を選択するための選択画面の概略を示す説明図である。

[図7]図7は、本実施の形態にかかるシステム認証部，携帯通信端末認証部，およびID認証部が認証する場合の認証処理と，非接触型ICカードモジュールへの通信処理とを概略的に示すシーケンス図である。

[図8]図8は、本実施の形態にかかるチャレンジレスポンス認証部及びID認証部が認

証する場合の認証処理と，非接触型ICカードモジュールへの通信処理とを概略的に示すシーケンス図である。

[図9]図9は、本実施の形態にかかる非接触型ICカードモジュールに対する書き込み処理の概略を示すシーケンス図である。

[図10]図10は、本実施の形態にかかる非接触型ICカードモジュールに対する読み込み処理の概略を示すシーケンス図である。

発明を実施するための最良の形態

[0026] 以下，本発明の好適な実施の形態について，添付図面を参照しながら詳細に説明する。なお，以下の説明及び添付図面において，略同一の機能及び構成を有する構成要素については，同一符号を付することにより，重複説明を省略する。

[0027] (データ通信システムについて)

まず，図1を参照しながら，本実施の形態にかかるデータ通信システム100について説明する。図1は，本実施の形態にかかるデータ通信システムの概略の一例を示す説明図である。

[0028] 図1に示すように，データ通信システム100は，サービス提供システム101と，代行システム105と，携帯通信端末103(103a，103b，…103n)と，通信網104と，通信網106と，通信網108と，情報処理装置109(109a，109b，…109n)と，リーダ／ライタ装置(R／W)111(111a，111b，…111n)と，基地局113と，パケット通信網115と，ゲートウェイ117とを備えている。

[0029] 上記サービス提供システム101は，携帯通信端末103の要求に応じて付与済みライセンス情報を生成するシステムである。またサービス提供システム101は，携帯通信端末103が実行するクライアントアプリケーション(クライアントアプリ)等を作成する。

[0030] 上記非接触型ICカードモジュールに対してデータの書き込み又は読込みなどの情報処理を実行させることで，サービス提供システム101は，携帯通信端末103を使用する利用者にサービスを提供するシステムである。

[0031] 例えば，サービス提供システム101の提供するサービスが商品購入金額に応じて付与するポイントである場合，携帯通信端末103に格納されたクライアントアプリがネ

ット上のオンラインで商品を購入する商品購入情報を送信することで，その商品購入が成立すると，クライアントアプリはその商品購入代金に応じて発生するポイント情報を非接触型ICカードモジュールに格納するよう代行システム105に要求する。

[0032] なお，詳細は後述するが代行システム105に通信処理を依頼するには携帯通信端末103を認証する必要があるため，その前にサービス提供システム101から付与済みライセンス情報の一部（例えば，利用条件）又は全部をクライアントアプリは取得する。その後，代行システム105が非接触型ICカードモジュールにデータを記憶させる。

[0033] また，非接触型ICカードモジュールが記憶するデータは，例えば，上記ポイント情報，電子マネー等を例示することができる。また，そのデータのことを，ネット上で取引される情報であって貨幣価値など所定の価値を有する情報を示した電子的価値情報と総称する場合もある。さらに，貨幣の入金によって，非接触型ICカードモジュールに電子マネーの残高を加算することをチャージと記載する場合もある。

[0034] ここで，サービス提供者は，サービス提供システム101を操作し，携帯通信端末103上に搭載されるクライアントアプリケーションの作成と提供等の業務を行う事業主体者のことである。

[0035] 次に，上記代行システム105は，非接触型ICカードモジュール（非接触型ICカード）の発行又は管理や，クライアントアプリに関する環境設定情報などを非接触型ICカードモジュール内の記憶領域に登録する，その環境設定情報を削除する，非接触型ICカードモジュール内の記憶領域に格納された電子的価値情報を読み込む，または非接触型ICカードモジュールに電子的価値情報を書き込む等の処理を，サービス提供システムを代理して行うシステムである。

[0036] 代行システム105は，上記サービス提供システム101の代わりに，非接触型ICカードモジュールに対してデータの読み／書き等の情報処理を実行させる。つまり，サービス提供システム101は非接触型ICカードモジュールに対して直接実行させることはできず，非接触型ICカードモジュールに対する一切の処理権限は代行システム105に委譲されている。

[0037] なお，本実施の形態では，非接触型ICカードモジュールが携帯通信端末103に備

わる場合を例に挙げて説明するが，その非接触型ICカードモジュールは，非接触型ICカードを含み，非接触型ICカードの機能を有する装置の総称である。

[0038] また，代行システム105は，サービス提供システム101ごとに，代行システム105とサービス提供システム101との間をセキュアにするシステム認証鍵を作成する。作成されたシステム認証鍵は代行システム105とサービス提供システム101内に各々格納される。なお，かかるシステム認証鍵の作成は，サービス提供システム101側で行っても良い。

[0039] なお，本実施の形態にかかるシステム認証鍵は，サービス提供システム101ごとに1つ作成される場合を例に挙げて説明するが，かかる場合に限定されず，例えば，サービス提供システム101が提供しているクライアントアプリの種類の分だけシステム認証鍵を作成する場合等でも実施可能である。

[0040] システム認証鍵は，機密性が極めて高い秘密情報であるため，耐タンパ性等を具備する記憶手段等に格納される。また，システム認証鍵は，例えば，代行システム105とサービス提供システム101との相互認証等に用いられる。

[0041] また，かかるシステム認証鍵は，RSA等の非対称鍵や，DES又はAES等の対称鍵などの如何なる鍵の場合であっても実施可能である。なお，対称鍵の場合，秘密裏に鍵を相手方に配布する必要があるため通信網から直接配布するのではなく内容証明付き郵送等別の手段で配布される。

[0042] 上記代行システム105にサービス提供システム101に関する情報が登録され，システム認証鍵が格納されると，携帯通信端末103がクライアントアプリを実行し，代行システム105が認証すると，代行システム105は，サービス提供システム101の代わりにその携帯通信端末103に備わる非接触型ICカードモジュールにアクセスする。

[0043] なお，アクセスは，例えば，システムの利用，システム又はサーバへの接続，ファイルの参照，ファイルの保存，ファイルの削除，またはファイルの変更など，通信網を介して情報を処理する情報処理の総称である。

[0044] 次に，携帯通信端末103（103a，103b，…，103n）は，1又は2以上の通信可能な端末であって，基地局113を介した通話機能や，基地局113とパケット通信網115とゲートウェイ117によってサービス提供システム101にアクセスすることができる。

[0045] つまり，携帯通信端末103はブラウジング機能を有するクライアントアプリを実行し，URLなどの指定を利用者から受付けて，Webサーバから HTMLに準ずるWebデータを受信し，画面に表示することができる。

[0046] また，携帯通信端末103は，上記通話機能，ブラウジング機能の他にも，R／W111を介して無線でデータをやりとりすることが可能な非接触型ICカードモジュール（非接触型ICカード等を含む）を備えている。

[0047] 非接触型ICカードモジュールは，携帯通信端末103をR／W111等に近接距離でかざすと，無線でR／W111を介して非接触型ICカードモジュール内に記憶するデータを，例えば代行システム105に送信等することができる。

[0048] また，携帯通信端末103は，代行システム105にアクセスする際に，代行システム105と相互認証するための認証鍵（クライアント認証鍵）を保有している。なお，かかるクライアント認証鍵は，機密性が極めて高い秘密情報であるため，耐タンパ性等を具備する記憶手段等に格納されるが，必ずしも必須ではない。

[0049] また，かかるクライアント認証鍵は，RSA等の非対称鍵や，DES又はAES等の対称鍵などの如何なる鍵の場合であっても実施可能である。なお，対称鍵の場合，秘密裏に鍵を相手方に配布する必要があるため通信網から直接配布するのではなく郵送等別の手段で配布される。

[0050] また，詳細は後述するが，携帯通信端末103は，携帯通信端末103内に格納したクライアントアプリを識別するクライアントアプリ識別情報を保有する。かかるクライアントアプリ識別情報を基に代行システム105は携帯通信端末103を認証してもよい。なお，携帯通信端末103は必ずクライアントアプリ識別情報を保有するとは限らず，当該クライアントアプリ識別情報を保有しなくともよい。

[0051] なお，図1に示すように，本実施の形態にかかるデータ通信システム100では，サービス提供システム101と携帯通信端末103とは通信網108等によって接続され，携帯通信端末103と代行システム105とは通信網106等によって接続されている。つまり，代行システム105とサービス提供システム101とは直接接続するネットワークが存在しないため，直接，通信することができず，上記携帯通信端末103を介さないと代行システム105とサービス提供システム101とはデータのやりとりができない。

[0052] したがって，携帯通信端末103のクライアントアプリによる通信処理を間接的に介在することでサービス提供システム101からの情報を代行システム105に送信することができる。

[0053] なお，本実施の形態にかかる携帯通信端末103とサービス提供システム101との間の通信網104等では，HTTP又はHTTPSなどのTCP／IP通信に限定されず，携帯通信端末103が具備する通信機能であれば如何なる場合でも実施可能であり，例えば，非接触型ICカード，接触型ICカード，赤外線（Ir），QRコード等の2次元バーコード，または電子メール（SMTP等）を例示することができる。かかる通信は，サービス提供システム101から携帯通信端末103のクライアントアプリに付与済みライセンス情報等を送信する際の通信手段に特に有効である。

[0054] また，本実施の形態にかかる携帯通信端末103と代行システム105との間の通信網106では，HTTP又はHTTPSなどのTCP／IP通信で行われることを例示することができる。

[0055] （サービス提供システム101）

次に，図2を参照しながら，本実施の形態にかかるサービス提供システム101について説明する。なお，図2は，本実施の形態にかかるデータ通信システムに備わるサービス提供システムの概略を示す説明図である。

[0056] 図2に示すように，サービス提供システム101はサービス提供サーバ201を備えている。上記説明したように，サービス提供サーバ201は携帯通信端末103と通信網108等を介してデータをやりとりすることができる。

[0057] また，サービス提供サーバ201は，図2に示すように，ライセンス取得部211と，通信部231と，ライセンス認証部241とを備えている。

[0058] ライセンス取得部211は，携帯通信端末103から要求情報を受け取ると，その要求情報に基づいて該当するライセンスをライセンスデータベース（図示せず。）から取得し，付与済みライセンス情報を生成する。

[0059] ライセンス取得部211は，上記説明したように，代行システム105側が保有するシステム認証鍵220aに対応するシステム認証鍵220bを保有している。

[0060] 上記要求情報には，自己の携帯通信端末103を特定する情報が含まれている。な

お，詳細は後述する。ライセンス取得部211は，上記要求情報に含まれる情報に基づいて該当のライセンスを取得し，上記システム認証鍵220bを用いて付与済みライセンス情報を生成する。

[0061] 通信部231は，通信網108，ゲートウェイ117，パケット通信網115，基地局113を介して携帯通信端末103と通信可能であり，通信部231は携帯通信端末103から要求情報等のデータを受信し，又は携帯通信端末103に付与済みライセンス情報等のデータを送信する。

[0062] （ライセンス取得部211）

次に，図3を参照しながら，本実施の形態に係るライセンス取得部の付与済みライセンス情報の生成処理について説明する。図3は，本実施の形態に係るライセンス取得部の付与済みライセンス情報生成処理の概略を示す説明図である。

[0063] 図3に示すように，ライセンス取得部211は，利用条件情報（又は，単に「利用条件」という。）と個別情報の入力を受付けて，利用条件情報と個別情報とを一組とする付与済みライセンス情報を生成する。さらに，ライセンス取得部211は，予め代行システム105とサービス提供システム101との間で作成したシステム認証鍵220bを用いて付与済みライセンス情報を暗号化する。

[0064] なお，ライセンス取得部211は，システム認証鍵220bで付与済みライセンス情報を暗号化する他にも，例えば，生成した付与済みライセンス情報のハッシュ値を求めてそれをシステム認証鍵220bで暗号化することで作成される署名データを付与済みライセンス情報に付加する場合でもよい。

[0065] 上記個別情報は，携帯通信端末103から送信されてくる要求情報に含まれている。個別情報には，例えば，非接触型ICカードモジュールを識別するための「ICカードID」や，携帯通信端末103に格納されるクライアントアプリを識別するための「クライアントアプリID」などが含まれている。

[0066] また，上記利用条件情報は，携帯通信端末103からの要求情報に含まれる個別情報に対応した情報であり，サービス提供の許可／不許可をするための判断材料となるライセンス情報である。

[0067] 利用条件情報は，例えば，携帯通信端末103にクライアントアプリを格納し，クライ

アントアプリを代行システム105に登録すると，サービス提供システム101にサービス利用可能とするための利用条件情報が作成される。

[0068] 利用条件情報は，そのサービス提供システム101が提供するサービスを利用可能とする条件が設定されており，例えば，利用条件情報には，「有効期間開始日時」及び「有効期間終了日時」が設定され，それらの日時によってサービス利用可能期間が定められる。また，「利用回数」が設定されることで，サービス利用可能期間中に利用できる回数が定められる。

[0069] なお，上記利用条件情報は，必ずしも個別情報ごとに異なる内容の情報が作成されるわけではなく，例えば，個別情報の「ICカードID」に全て“＊”からなるIDが設定された場合，「有効期間開始日時」と「有効期間終了日時」が一律所定日時に設定された全て同じ内容の利用条件情報が作成される場合でもよい。かかる場合では，例えば，サービス内容次第で，全ての利用者が保有する非接触型ICカードモジュールについてサービス利用可能な対象とすることができる。

[0070] また，個別情報に含まれる非接触型ICカードモジュールに書き込まれるデータ（書き込みデータ）又は非接触型ICカードモジュール内の記憶領域から読み込まれたデータ（読み込みデータ）は，携帯通信端末103がサービス利用可能か否かを含めて認証する認証処理の場合，不要である。なお，上記書き込みデータ又は読み込みデータは，非接触型ICカードモジュールに対する代行システム105からの書き込み／読み込み処理時には必要なデータである。

[0071] なお，本実施の形態にかかるライセンス取得部211は，利用条件と個別情報とを入力として付与済みライセンス情報を生成する場合を例に挙げて説明したが，かかる例に限定されず，例えば，利用条件を入力として付与済みライセンス情報を生成する場合等でも実施可能である。つまり，付与済みライセンス情報には，一部（利用条件など）又は全部（利用条件，個別情報など）が含まれる。なお，特に明記されていない場合，付与済みライセンス情報は一部（利用条件など）又は全部（利用条件，個別情報など）を含んだ情報を意味する。

[0072] （携帯通信端末103）

次に，図4を参照しながら，本実施の形態にかかる携帯通信端末103について説

明する。図4は，本実施の形態にかかる携帯通信端末103の概略的な構成の一例を示すブロック図である。

[0073] 図4に示すように，携帯通信端末103は，メモリ又はHDD等に格納されアプリケーションとして機能するアプリケーション部203と，アプリケーション部203からの要求に応じて処理を実行する実行部213と，非接触型ICカードモジュール223とを備えている。

[0074] アプリケーション部203は，上記説明した通り，サービス提供システム101によって作成されるクライアントアプリである。したがって，携帯通信端末103は，サービス提供サーバ201から通信網等を介してクライアントアプリを受け取ると，例えばEEPROM等のメモリ又はHDDに実行可能なように格納する。

[0075] 本実施の形態にかかるアプリケーション部は，1又は2以上のモジュール又はコンポーネントから構成されたソフトウェアである場合を例に挙げて説明するが，かかる例に限定されず，例えば1又は2以上の素子から形成された回路等のハードウェアである場合でも実施可能である。上記の場合，サービス提供システム101からは通信網以外の郵送手段によってアプリケーション部203が提供され，利用者自らハードウェアを組み込む等によって実施できる。

[0076] なお，クライアントアプリ格納時に例えばサービス提供サーバ201から渡されるクライアントアプリを識別するクライアントアプリIDも同じく記憶手段に格納されてもよい。かかるクライアントアプリIDは，代行システム101にアクセスする際の認証に用いられる。

[0077] 実行部213は，携帯通信端末103に予め組み込まれた1又は2以上のモジュールからなるソフトウェアである。実行部213は，アプリケーション部203から通信処理等の要求があると，通信網を介してサーバにアクセスしたり，通信相手から送られてきたデータをアプリケーション部203にフィードバックしたりする。

[0078] 非接触型ICカードモジュール223は，非接触型ICカード，非接触型ICカードの機能を有する装置又は半導体素子などを例示することができる。さらに非接触型ICカードは，アンテナを備えて変復調し近接距離で無線通信可能なICカードである。上記無線通信によって非接触型ICカードに備わる記憶手段からデータを読み出したり

，記憶手段にデータを書き込むことができる。

[0079] 携帯通信端末103とサーバ（サービス提供サーバ201，代行システムサーバ205）とで通信を行う場合は，まず携帯通信端末103のアプリケーション部203から実行部213に通信要求が行われる。

[0080] なお，上述したように，本実施形態に係るデータ通信システム100における携帯通信端末103とサーバとの通信では，携帯通信端末103から通信開始のトリガがあるものとするが，かかる例に限定されない。

[0081] 実行部213は，アプリケーション部203からサーバに対する通信要求があるとサーバに通信網を介してアクセスを試みる。なお，その際にセキュリティ上，直接の通信相手によって認証が行われるため暗号化又は電子署名を付加する等の処理が施される。詳細は後述する。

[0082] サーバで認証が行われると，実行部213とサーバとの間でコネクションが確立し，さらに上記通信要求が非接触型ICカードモジュール223に関する情報処理の場合，サーバ（代行システムサーバ205）と非接触型ICカードモジュール223との間で相互認証が行われ，当該双方との間で通信処理が開始する。

[0083] 次に，図2を参照しながら，携帯通信端末103に備わるアプリケーション部203についてより具体的に説明する。

[0084] 図2に示すように，アプリケーション部203には，要求部204と，暗号化部206と，レスポンス生成部207と，ID取得部208とが備わっている。

[0085] 要求部204は，代行システムサーバ205又はサービス提供サーバ201と通信を行うために要求情報を生成し，実行部213に要求情報を伝送することで通信要求する機能を有する。

[0086] 要求部204は，上記要求情報を生成する際，個別情報をHDD等の記憶手段（図示せず。）から取得し，要求情報に設定する。

[0087] 暗号化部206は，代行システムサーバ205が保有するクライアント認証鍵221aと対応するクライアント認証鍵221bを用いて，データを暗号化する。かかる暗号化によって，代行システムサーバ205側の携帯通信端末認証部217が当該クライアント認証鍵221bに対応するクライアント認証鍵221aで復号できた場合，携帯通信端末103

の真正性を正当化できることとなる。

[0088] レスポンス生成部207は，チャレンジレスポンス方式によるレスポンスを生成する機能を少なくとも有する。レスポンス生成部207は，代行システムサーバ205からのチャレンジコードを取得しそのチャレンジコード（又は，シード等）に基づいてレスポンスを生成する。なお，レスポンスは，チャレンジコードのハッシュ値を求めることによって生成されるが，かかる例に限定されず，例えば，チャレンジコードと利用者からの入力で受け付けたパスワードとを付加した上でハッシュ値を求めてレスポンスを生成しても良い。

[0089] また，レスポンス生成部207は，詳細は後述するが，上記暗号化部206が保有するクライアント認証鍵221bを用いて，付与済みライセンス情報とレスポンスとを一組とし暗号化する。

[0090] ID取得部208は，アプリケーション部203を識別するクライアントアプリIDを記憶手段から取得する。なお，クライアントアプリIDが記憶手段に格納されていない場合，ID取得部208は，表示画面にクライアントアプリIDを未取得である旨のメッセージを表示するための画面情報を生成しても良い。

[0091] （レスポンス生成部207）

次に，図5を参照しながら，本実施の形態にかかるレスポンス生成部207の暗号化処理について説明する。図5は，本実施の形態にかかるレスポンス生成部207による暗号化処理の概略的な一例を示す説明図である。

[0092] 図5に示すように，レスポンス生成部207は，入力としてチャレンジ（チャレンジコード）と付与済みライセンス情報とクライアント認証鍵221bを受け付けると，ハッシュ関数を利用してそれらの情報のハッシュ値（HMAC：Hashing for Message Authentication Code）を求める。

[0093] 求められたハッシュ値（レスポンス）は上記付与済みライセンス情報に含む利用条件情報（図5に示す「利用条件」）とともに，実行部213により通信網106を介して代行システム105に送信される。かかる送信処理では付与済みライセンス情報のうち利用条件情報のみが通信網106を介して送信される。なお，個別情報は，携帯通信端末103の記憶手段（図示せず。）等に格納されており，予め又は別途に当該携帯通

信端末103から代行システム105に送信される。また，一度携帯通信端末103から送信された個別情報のうち一部（クライアントアプリID等）又は全部を代行システム105側で保有しても良い。

[0094] なお，本実施の形態にかかるデータ通信システム100ではレスポンス生成部207によるHMAC演算が行われる場合を例に挙げて説明したが，かかる例に限定されず，例えば，レスポンス生成部207はチャレンジと付与済みライセンス情報とを入力してハッシュ値を求める場合でも実施可能である。なお，求められたハッシュ値は，さらにレスポンス生成部207によって，クライアント認証鍵221bを用いることで暗号化されることで，レスポンスが生成される。生成されたレスポンスは付与済みライセンス情報に含む利用条件情報（図5に示す「利用条件」）とともに，実行部213により通信網106を介して代行システム105に送信され，代行システム105側で，チャレンジと付与済みライセンス情報に含む利用条件情報と，個別情報とから上記と同様にハッシュ値（レスポンス）を求めて，送信元のクライアント認証鍵221aで受信したレスポンスを復号し，双方のレスポンスを比較して一致不一致を検証してもよい。

[0095] 上記入力情報であるチャンレンジは，上記説明したようにチャレンジレスポンス方式を利用したチャレンジコードであって，代行システムサーバ205によって生成される。

[0096] また，レスポンス生成部207への入力情報である付与済みライセンス情報のうち一部の情報（図5に示す「利用条件」）は，レスポンスが送信されるとともに，または別の任意のタイミングで，そのまま通信網106を介して実行部213により代行システム105に送信される。認証する際の判断材料にするためである。

[0097] （代行システム105）

次に，図2を参照しながら，本実施の形態にかかる代行システム105について説明する。なお，図2は，本実施の形態にかかるデータ通信システムの概略を示す説明図である。

[0098] 図2に示すように，代行システム105は代行システムサーバ205を備えている。上記説明したように，代行システムサーバ205は携帯通信端末103と通信網106等を介してデータをやりとりすることができ，さらに携帯通信端末103に備わる非接触型ICカードモジュールと通信網104，R／W111を介して通信できる。

[0099] 代行システムサーバ205は，図2に示すように，受信部214，認証部215と，判断部225と，通信部235と，認証処理管理部245とを備えている。通信部235は，判断部225から指示があると携帯通信端末103の実行部213を介して非接触型ICカードモジュール223と通信を行う。

[0100] なお，非接触型ICカードモジュール223に備わる記憶手段の記憶領域の所定アドレスにデータを書き込む処理や，非接触型ICカードモジュール223に備わる記憶手段の記憶領域の所定アドレスに格納されたデータを読み込む処理など具体的な通信処理の内容は携帯通信端末103から送信される。

[0101] 認証部215は，さらにシステム認証鍵220aを用いてサービス提供システム101を認証するシステム認証部216と，クライアント（携帯通信端末103）を認証する携帯通信端末認証部217と，チャレンジレスポンス方式で携帯通信端末103を認証するチャレンジレスポンス認証部218と，クライアントアプリIDで携帯通信端末103を認証するID認証部219とを備えている。

[0102] システム認証部216は，サービス提供サーバ201で暗号化されたデータをシステム認証鍵220aを用いて復号できた場合，送信元であるサービス提供サーバ201の真正性について検証することができる。

[0103] 携帯通信端末認証部217も，上記と同様に携帯通信端末103で暗号化されたデータをクライアント認証鍵221aを用いて復号できた場合，送信元である携帯通信端末103の真正性について検証できる。

[0104] チャレンジレスポンス認証部218は，携帯通信端末103からチャレンジの要求があるとチャレンジコードを生成して，携帯通信端末103に送信するとともに，チャレンジと，別途に受信する付与済みライセンス情報とからハッシュ値を求め比較対照用のレスポンスを作成する。そして，携帯通信端末103からレスポンスを受けると，そのレスポンスと比較対照用のレスポンスとを比較し，一致／不一致を確認する。双方が一致していれば，真正性を有すると判断し，携帯通信端末103を認証することができる。

[0105] ID認証部219は，携帯通信端末103から送られてくるクライアントアプリIDを受信すると，予めクライアントアプリIDデータベース（図示せず。）から該当するクライアントアプリIDを検索する。

[0106] 検索結果，該当するクライアントアプリIDが存在した場合，通信元の携帯通信端末103は真正であると判断する。なお，クライアントアプリIDデータベースには，登録されたクライアントアプリIDが全て格納されている。クライアントアプリIDは，暗号化されて例えばサービス提供システム101から携帯通信端末103を介して代行システム105に送信される場合でもよい。

[0107] 判断部225は，上記認証部215による認証結果を受けて，さらに付与済みライセンス情報に含まれる上記説明の「利用回数」，「有効期間開始日時」，及び「有効期間終了日時」を参照して，サービス提供可能であるか否かを判断する。

[0108] 認証処理管理部245は，例えば，代行システムサーバ205に内部接続されたコンソール，又はサービス提供システムを管理する管理者が使用する情報処理装置から1又は2種以上の認証処理を選択した選択情報を受けると，認証部216に対して，選択情報に記載された認証処理で，認証処理を実行するよう指示（認証処理の選択指示）する。

[0109] より具体的に説明すると，認証部215は，認証処理を実行する際に，どの方式又は種類の認証処理で実行するか，認証処理管理部245に問合せ処理を行ってから認証処理を実行している。

[0110] したがって，認証部215からの問合せがあると認証処理管理部245は，選択情報に記載された1又は2種以上の認証処理で実行するよう認証部215に指示する。なお，上記選択情報は，該当するサービス提供システム101又は代行システム105に接続されたコンソール等から送られてくる。

[0111] その指示内容に応じて，認証部215に備わるシステム認証部216，携帯通信端末認証部217，チャレンジレスポンス認証部218，またはID認証部219のうち少なくとも一つによる認証処理が実行される。

[0112] 認証処理管理部245は，認証部215に認証処理を指示するために，例えば，サービス提供システム101を識別するサービス提供システムIDと選択情報とをひも付けて認証処理データベース（図示せず。）を保有している。

[0113] 認証処理管理部245は，選択情報をコンソールから受けると，選択情報に設定されたサービス提供システムIDを参照し，認証処理データベースに格納された該当する

選択情報を更新する。

[0114] なお，本実施の形態にかかる認証部215に備わる各認証部（216，217，218）は，暗号化されたデータを復号できるか否かで認証する場合を例に挙げて説明したが，かかる例に限定されず，例えば，データに電子署名が付加されていた場合，各認証部（216，217，218）は，そのデータを基にして電子署名を作成し，データに添付された電子署名と作成後の電子署名との一致／不一致を判断することによって認証してもよい。

[0115] （認証処理の組み合わせ）

選択情報に設定された認証処理の組み合わせを必要に応じて変更することができる。認証処理には，複数種類の認証処理が存在している。代行システム105が提供する複数種類の認証処理から適切な認証処理を組み合わせて選択することができる。

[0116] ここで，図6を参照しながら，認証処理管理部245がコンソール等から受け付ける認証処理の選択画面について説明する。図6は，本実施の形態にかかる認証処理を選択するための選択画面の概略を示す説明図である。

[0117] 図6に示す選択画面は，例えば，代行システムサーバ205にLAN等で内部接続するコンソール等に表示される認証処理を選択するための画面である。なお，かかる例に限定されず，例えば，選択画面は，サービス提供システム101を運用する管理者が使用する情報処理装置に表示されても良い。かかる場合，管理者が使用する情報処理装置であることを認証するためログインパスワードなどを情報処理装置は受け付け，代行システムサーバ205が認証する必要がある。

[0118] 図6に示すように，選択画面には，携帯通信端末認証部217が行う携帯通信端末103を認証する認証処理を選択するチェックボックス601aや，チャレンジレスポンス認証部218が行う認証処理を選択するチェックボックス601b等が表示されている。上記チェックボックス601をセキュリティレベルに合わせて選択することで，様々な認証処理の組み合わせを実現することができる。

[0119] かかるチェックボックス601をクリックし，代行システム105にて行う認証処理の方式を選択する。図6に示す選択例では，チェックボックス601a，チェックボックス601b，

チェックボックス601d，チェックボックス601eが選択されている。

[0120] 「更新」ボタンをクリックすると，コンソール側で選択情報を生成し，認証処理管理部245に選択情報を送信する。以上より，サービス提供システム101側の所望とする認証処理に対して柔軟に代行システム105は対応することができる。また，認証処理を組み合わせることで，セキュリティレベルをサービス提供システム101によって自由に選択し，変更することができる。

[0121] なお，チェックボックス601dに示す読み込み処理時の署名付加は，主に非接触型ICカードモジュール223から読み込んだデータの改ざんを防止するため代行システム105側で電子署名を付加する機能である。この機能は，例えば，認証部215に備わる各部とも備えている。

[0122] また，チェックボックス601eに示す書き込み処理時の署名付加は，主にサービス提供システム101側から非接触型ICカードモジュール223に書き込むデータの改ざん防止のため，サービス提供システム101側で電子署名が付加される機能である。したがって，かかる機能が選択された場合，代行システム105側では，受け取ったデータを基に作成した電子署名と，送られてきた電子署名との一致／不一致を確認する必要がある。なお，この非接触型ICカードモジュール223に書き込むデータの改ざんを検出する機能は，例えば，認証部215に備わる各部とも備えている。

[0123] 同じく，チェックボックス601fに示す読み込み処理時の暗号化は，主に非接触型ICカードモジュール223から読み込んだデータが盗聴されるリスクを予め想定し，代行システム105側でデータを暗号化する機能である。この機能は，例えば，認証部215に備わる各部とも備えている。したがって，かかる機能が選択された場合，代行システム105側で暗号化されたデータは，サービス提供システム101側で復号する必要がある。

[0124] チェックボックス601gに示す書き込み処理時の暗号化は，主にサービス提供システム101側から非接触型ICカードモジュール223に書き込むデータが盗聴されるリスクを想定し，上記データをサービス提供システム101側で暗号化する機能である。したがって，かかる機能が選択された場合，代行システム105側では，受け取ったデータを所定のシステム認証鍵等の鍵を用いて復号する必要がある。なお，この非接触

型ICカードモジュール223に書き込むデータを復号する機能は，例えば，認証部215に備わる各部とも備えている。

[0125] （非接触型ICカードモジュールとの通信処理）

次に，図7を参照しながら，本実施の形態にかかる認証部215による認証処理を含め，非接触型ICカードモジュールとの通信処理について説明する。図7は，本実施の形態にかかるシステム認証部216，携帯通信端末認証部217，およびID認証部219が認証する場合の認証処理と，非接触型ICカードモジュールへの通信処理とを概略的に示すシーケンス図である。

[0126] 図7に示すように，携帯通信端末103についての認証処理を実行する場合，アプリケーション部203は，まずサービス提供サーバ201にアクセスする（S701）。なお，アプリケーション部203は，既に付与済みライセンス情報を保持しており，その付与済みライセンス情報が有効である場合，サービス提供サーバ201にはアクセスしない。

[0127] また，サービス提供サーバ201に対してアクセスするためのサービス提供サーバ201のアドレスは，例えば，サービス提供サーバ201のURL等に基づいてアプリケーション部203は実行部213を通じてアクセスする。

[0128] サービス提供サーバ201は，アプリケーション部203から個別情報を受け取ると，上記説明したように，付与済みライセンス情報を生成（S702）し，要求元の携帯通信端末103のアプリケーション部203に当該付与済みライセンス情報を送信する（S703）

次に，アプリケーション部203は，受け取った付与済みライセンス情報を代行システムサーバ205に実行部213を通じて送信する（S705）。サービス提供システム101から直接，代行システムサーバ205に付与済みライセンス情報を送信しないため，両サーバのセキュリティの独立性を向上させることができる。

[0129] ここで，送信処理（S705）では，ID取得部208が取得したクライアントアプリIDも一緒に送信する場合を例に挙げて説明するが，かかる例に限定されず，例えば，クライアントアプリIDによるID認証処理を選択しない場合，クライアントアプリIDを送信しなくてもよい。

[0130] 次に，代行システムサーバ205は，携帯通信端末103から付与済みライセンス情報とクライアントアプリIDを受け取ると，まず当該クライアントアプリIDを基にしてID認証

部219によるID認証処理が実行される(S707)。

[0131] ID認証部219によるID認証処理は，予めクライアントアプリがアプリケーション部203として登録される際に代行システムサーバ205のデータベース(クライアントアプリデータベース)に格納されたクライアントアプリIDと一致するか確認する。

[0132] ID認証処理(S707)が終了すると，次に，携帯通信端末認証部217による携帯通信端末103の認証処理が実行される(S709)。この認証処理は，携帯通信端末103が付与済みライセンス情報を暗号化する際に用いたクライアント認証鍵221bと対応するクライアント認証鍵221aを用いて復号することができるか否かによって認証する。携帯通信端末認証部217が復号することができれば，真正性を有する携帯通信端末103と認証することができる。

[0133] なお，本実施の形態にかかるデータ通信システム100では携帯通信端末103の認証処理(S709)が行われる場合を例に挙げて説明したが，かかる例に限定されず，データ通信システム100では，例えば，後述するチャレンジレスポンスによる認証処理を行わないときに，携帯通信端末103の認証処理(S709)を実行する場合等でもよい。かかる場合，認証処理を簡略化することができ処理の効率化を図ることができる。

[0134] また、本実施の形態にかかるデータ通信システム100では，携帯通信端末103の認証処理(S709)が行われる場合を例に挙げて説明したが，かかる例に限定されず，例えば，データ通信システム100では、携帯通信端末103の認証処理(S709)を実行しない場合等でも実施可能である。

[0135] 次に，携帯通信端末認証部217による携帯通信端末103の認証処理(S709)が終了すると，その復号された付与済みライセンス情報を基にして，システム認証部216によるサービス提供システム101の認証処理が実行される(S711)。

[0136] システム認証部216は，携帯通信端末認証部217による認証処理(S709)で復号された付与済みライセンス情報を，サービス提供システム101側で暗号化する際に用いたシステム認証鍵220bに対応するシステム認証鍵220aを用いて復号することができるか否かによって認証する。システム認証部216が復号することができれば，真正性を有するサービス提供サーバ201であると認証することができる。

[0137] なお，本実施の形態にかかる認証部215に備わるシステム認証部216，携帯通信端末認証部217は，暗号化されたデータを復号できるか否かで認証する場合を例に挙げて説明したが，かかる例に限定されず，例えば，データに電子署名が付加されていた場合，システム認証部216，携帯通信端末認証部217は，そのデータを基にして電子署名を作成し，データに添付された電子署名と作成後の電子署名との一致／不一致を判断することによって認証してもよい。

[0138] 以上，ID認証部219，携帯通信端末認証部217，システム認証部216による各々の認証処理が終了すると，判断部225は，認証部215からの認証結果と付与済みライセンス情報に含まれるライセンス「利用条件」とを基にして要求元の携帯通信端末103の非接触型ICカードモジュール223に対して通信可能であるか否かを判断し，通信処理の決定をする（S713）。

[0139] 判断部225による非接触型ICカードモジュール223との通信処理が決定すると（S713），通信部235は通信網106とゲートウェイ117とパケット通信網115と基地局113を経由し，さらに携帯通信端末103に備わる実行部213を経由することで，非接触型ICカードモジュール223と相互認証する（S715）。なお，相互認証の際，通信部235は，通信相手の「ICカードID」が付与済みライセンス情報に含む「ICカードID」と一致するか確認する。

[0140] なお，本実施の形態にかかる通信部235は，ゲートウェイ117及びパケット通信網115等を経由し，さらに携帯通信端末103に備わる実行部213を経由して非接触型ICカードモジュール223と相互認証する場合に限定されず，例えば，通信部235は，R／W（リーダ／ライタ）111を介して非接触型ICカードモジュール223と相互認証する（S715）場合でも実施可能である。

[0141] 通信部235と非接触型ICカードモジュール223との相互認証が完了すると（S715），通信部235は，携帯通信端末103の認証処理の際にリクエスト要求で受信する（S705），又は認証処理後に別途受信する通信処理の内容が記載された通信処理情報を非接触型ICカードモジュール223に送信することで非接触型ICカードモジュール223との通信処理を実行する（S717）。なお，当該通信処理（S717）は相互に有する暗号化鍵／復号鍵を用いたセキュア通信であるが，かかる例に限定されない

。

[0142] 非接触型ICカードモジュール223は，例えば，通信部235から記憶手段の記憶領域（例えば，アドレス“A”）にポイント情報“80”を書き込む処理を通信処理内容とする通信処理情報を受け取ると，その通信処理内容に従ってポイント情報“80”をアドレス“A”に書き込む。さらに当該書き込み処理が終了すると通信部235に処理結果としてレスポンス情報を送信する。まだ後続の通信処理があれば継続して通信処理が実行される。

[0143] 続けて，図8を参照しながら，本実施の形態にかかる認証部215による認証処理を含め，非接触型ICカードモジュールとの通信処理について説明する。図8は，本実施の形態にかかるチャレンジレスポンス認証部218及びID認証部219が認証する場合の認証処理と，非接触型ICカードモジュールへの通信処理とを概略的に示すシーケンス図である。

[0144] 図8に示すように，携帯通信端末103についての認証処理を実行する場合，アプリケーション部203は，まずサービス提供サーバ201にアクセスする（S801）。なお，上記説明したように，アプリケーション部203は，既に付与済みライセンス情報を保持しており，その付与済みライセンス情報が有効である場合，サービス提供サーバ201にはアクセスしない。

[0145] サービス提供サーバ201は，アプリケーション部203から個別情報を受け取ると，上記説明したように，付与済みライセンス情報を生成（S802）し，要求元の携帯通信端末103のアプリケーション部203に当該付与済みライセンス情報を送信する（S803）。

[0146] 次に，アプリケーション部203は，代行システムサーバ205に実行部213を通じてアクセスし，認証処理をリクエストする（S805）。なお，かかるリクエスト処理（S805）では，ID取得部208が取得したクライアントアプリIDも一緒に送信する場合を例に挙げて説明するが，かかる例に限定されず，例えば，クライアントアプリIDによるID認証処理を選択しない場合，クライアントアプリIDを送信しなくてもよい。

[0147] 次に，携帯通信端末103からクライアントアプリIDを受け取ると，ID認証部219は，当該クライアントアプリIDを基にしてID認証処理を実行する（S807）。

[0148] 上記ID認証部219によるID認証処理が完了すると，次に，チャレンジレスポンス認証部218は，チャレンジコードを生成して，通信網を介して携帯通信端末103に送信する(S809)。

[0149] アプリケーション部203が代行システムサーバ205からチャレンジコードを受け取ると，そのチャレンジコードと付与済みライセンス情報とを基にして，レスポンスを生成する(S811)。なお，レスポンスについては，既に説明したので，詳細な説明は省略する。

[0150] 次に，アプリケーション部203は，上記レスポンスを代行システムサーバ205に実行部213を通じて送信する(S813)。また，レスポンスを代行システムサーバ205に送信するタイミングと同じくして，付与済みライセンス情報も送信する(S813)。なお，上記付与済みライセンス情報を別途に送信する場合等でも実施可能である。

[0151] 次に，レスポンスを受け取ったチャレンジレスポンス認証部218は，既に生成したチャレンジコードと携帯通信端末103から送信された付与済みライセンス情報とからレスポンス生成部207とほぼ同様な処理によってレスポンスを生成する。

[0152] なお，携帯通信端末103から送信された付与済みライセンス情報が携帯通信端末103によって暗号化されていた場合，チャレンジレスポンス認証部218は，クライアント認証鍵221aを用いて復号してからレスポンスを生成する。

[0153] また，携帯通信端末103から送信された付与済みライセンス情報がサービス提供サーバ201によって暗号化されていた場合，チャレンジレスポンス認証部218は，システム認証鍵220aを用いて復号してからレスポンスを生成する。

[0154] チャレンジレスポンス認証部218は，レスポンスを生成すると，携帯通信端末103からのレスポンスと，生成したレスポンスとを比較し，一致／不一致を検証する。チャレンジレスポンス認証部218は，レスポンスの一致を確認すると送信元の携帯通信端末103とサービス提供サーバ201との真正性が確認できたとして，認証を完了する。

[0155] 以上，チャレンジレスポンス認証部218，ID認証部219による各々の認証処理が終了すると，判断部225は，認証部215からの認証結果と付与済みライセンス情報に含まれるライセンス「利用条件」とを基にして要求元の携帯通信端末103の非接触型ICカードモジュール223に対して通信可能であるか否かを判断し，通信処理の決定

をする(S817)。

[0156] なお，判断部225は，例えば，付与済みライセンス情報に含む個別情報を携帯通信端末103から送信するように，通信部235を介して携帯通信端末103に要求しても良い。携帯通信端末103に備わる実行部213は，個人情報の要求があると，個人情報を取得し，代行システムサーバ205に送信する。

[0157] また，かかる例に限定されず，判断部225は，必要に応じて付与済みライセンス情報に含まれた携帯通信端末103を識別する「携帯機器ハードウェアID」もクライアントアプリIDデータベースから検索し確認しても良い。なお，クライアントアプリIDデータベースのデータ構造は，「クライアントアプリID」，「携帯機器ハードウェアID」，その携帯機器の所有者を識別する「所有者ID」，非接触型ICカードモジュール等を識別する「ICカードID」などの項目から構成されている。

[0158] 判断部225による非接触型ICカードモジュール223との通信処理が決定すると(S817)，通信部235は通信網106とゲートウェイ117とパケット通信網115と基地局113を経由し，さらに携帯通信端末103に備わる実行部213を経由することで，非接触型ICカードモジュール223と相互認証する(S819)。なお，相互認証の際，通信部235は，通信相手の「ICカードID」が付与済みライセンス情報に含む「ICカードID」と一致するか確認する。

[0159] なお，本実施の形態にかかる通信部235は，ゲートウェイ117及びパケット通信網115等を経由し，さらに携帯通信端末103に備わる実行部213を経由して非接触型ICカードモジュール223と相互認証する場合に限定されず，例えば，通信部235は，R／W(リーダ／ライタ)111を介して非接触型ICカードモジュール223と相互認証する(S819)場合でも良い。

[0160] 通信部235と非接触型ICカードモジュール223との相互認証が完了すると(S819)，通信部235は，携帯通信端末103の認証処理の際に，又は認証処理後に別途受信する通信処理の内容が記載された通信処理情報を非接触型ICカードモジュール223に送信することで非接触型ICカードモジュール223との通信処理を実行する(S821)。通信処理(S821)については，上記説明した通信処理(S717)と実質的に同一であるため詳細な説明は省略する。

[0161] ここで，図7又は図8に示す認証処理の変形例としてID認証部219によるID認証処理だけの場合を例に挙げて，本実施の形態にかかる認証処理を説明する。なお，図7又は図8に示す認証処理と実質的に同様な処理については説明を省略する。

[0162] 図7又は図8に示すように，ID認証部219によるID認証処理のみの場合，携帯通信端末103は，付与済みライセンス情報を代行システムサーバ205に送信せずに，クライアントアプリIDのみを送信すればよい。したがって，サービス提供システム101にアクセスする必要はないが，その分，セキュリティレベルが下がり，携帯通信端末103のなりすましが行われる可能性が高くなる。

[0163] 上記携帯通信端末103がクライアントアプリIDを代行システムサーバ205に送信した後は，図7又は図8に示す一連の認証処理と実質的に同一であるため，詳細な説明を省略する。

[0164] (書き込み処理)

次に，図9を参照しながら，本実施の形態にかかる非接触型ICカードモジュール223に対する書き込み処理について説明する。なお，図9は，本実施の形態にかかる非接触型ICカードモジュールに対する書き込み処理の概略を示すシーケンス図である。

[0165] なお，図9に示す書き込み処理では，既に説明したため図7又は図8に示す認証処理を省略して説明するが，かかる例に限定されず，書き込み処理についても予め認証処理が実行されるものとする。

[0166] 図9に示すように，非接触型ICカードモジュール223に対してデータの書き込み処理を実行する場合，アプリケーション部203は，まずサービス提供サーバ201にアクセスして，個別情報が含まれる要求情報を送信する(S901)。

[0167] サービス提供サーバ201は，アプリケーション部203から個別情報を受け取ると，上記説明したように，書き込み用の付与済みライセンス情報を生成し(S902)，要求元の携帯通信端末103のアプリケーション部203に当該付与済みライセンス情報を送信する(S903)。

[0168] 次に，アプリケーション部203は，書き込み処理を依頼したい旨を代行システムサーバ205に実行部213を通じてリクエストする(S905)。なお，詳細な説明は省略す

るが，代行システムサーバ205では，携帯通信端末103の認証処理が行われる。

[0169] 代行システムサーバ205内の判断部225が通信処理を許可すると，通信部235と非接触型ICカードモジュール223とが相互認証する（S907）。なお，既に説明したのとほぼ同様であるため詳細な説明は省略する。

[0170] 相互認証（S907）が完了すると，次に，代行システムサーバ205内の通信部235は，アプリケーション部203に対し，非接触型ICカードモジュール223内の記憶手段に書き込むデータを要求する（S909）。

[0171] アプリケーション部203は，受け取った書き込み用の付与済みライセンス情報と，書き込み対象となるデータを実行部213を通じて代行システムサーバ205に送信する（S911）。

[0172] なお，かかる送信処理（S911）の際の書き込み対象となるデータは，アプリケーション部203が作成する場合や，サービス提供サーバ201から直接送信される場合等を例示することができる。

[0173] また，かかる送信処理（S911）の際に，書き込み対象となるデータ及び書き込み用の付与済みライセンス情報とは，図3に示すように，クライアント認証鍵221bで暗号化される。

[0174] 認証部215は，上記書き込み対象データ及び書き込み用の付与済みライセンス情報を受け取ると，システム認証部216又は携帯通信端末認証部217等によって，暗号化された書き込み対象データ及び書き込み用の付与済みライセンス情報を復号する。当該復号により，認証部215は，データ送信元であるサービス提供サーバ201又は携帯通信端末103の真正性について検証することができる（S913）。

[0175] 判断部225は，受け取った付与済みライセンス情報に設定された「利用回数」等の利用条件が適切であるか否かを確認（S915）し，適切であると確認すると通信部235に書き込み処理の実行を指示する。なお，「利用回数」等の利用条件のほかに，判断部225は，上記説明したが携帯機器のハードウェアIDなどを確認してもよい。

[0176] 通信部235は，上記書き込み対象のデータと書き込み用のコマンド等を非接触型ICカードモジュール223に送信することによって，当該非接触型ICカードモジュール223に対して記憶領域の指定個所にデータを書き込ませる（S917）。以上で，本実

施の形態にかかる書き込み処理の一連の動作が終了する。

[0177] なお，図9に示す書き込み処理では書き込み対象のデータや書き込み用のライセンス情報を暗号化する場合を例に挙げたが，かかる例に限定されず，例えば，書き込み処理では，一切暗号化しない場合，暗号化の代わりに電子署名を付加する場合，電子署名を付加した上でその電子署名付きデータを暗号化する場合などでもよい。つまり，上記説明したように暗号化又は電子署名などのセキュリティ環境を組み合わせて実行できる。

[0178] (読み込み処理)

次に，図10を参照しながら，本実施の形態にかかる非接触型ICカードモジュール223に対する読み込み処理について説明する。なお，図10は，本実施の形態にかかる非接触型ICカードモジュールに対する読み込み処理の概略を示すシーケンス図である。

[0179] なお，図10に示す読み込み処理では，既に説明したため図7又は図8に示す認証処理を省略して説明するが，かかる例に限定されず，本実施の形態に係る読み込み処理についても予め認証処理が実行されるものとする。

[0180] 図10に示すように，アプリケーション部203は，読み込み処理を依頼したい旨を代行システムサーバ205に実行部213を通じてリクエストする(S1005)。なお，詳細な説明は省略するが，代行システムサーバ205では，携帯通信端末103の認証処理が行われる。

[0181] 代行システムサーバ205内の判断部225が通信処理を許可すると，通信部235と非接触型ICカードモジュール223とが相互認証する(S1007)。なお，既に説明したのとほぼ同様であるため詳細な説明は省略する。

[0182] 相互認証(S1007)が完了すると，次に，代行システムサーバ205内の通信部235は，非接触型ICカードモジュール223に対して，読み込み用のコマンド等を送信することで，記憶領域の指定個所に格納されたデータを読み込ませる(S1009)。非接触型ICカードモジュール223は，データを読み込むと当該データをリプライとして通信部235に送信する。なお，読み込ませる記憶領域の指定個所(指定アドレス)は，例えば，アプリケーション部203からのリクエスト時(S1005)等の処理で受信してい

るものとする。

[0183] 代行システムサーバ205は，非接触型ICカードモジュール223からデータを受信すると，システム認証部216等によって，そのデータをシステム認証鍵220aで暗号化する(S1011)。

[0184] 次に，代行システムサーバ205は，通信網106等を介して携帯通信端末103に暗号化された読み込みデータを送信する(S1013)。

[0185] アプリケーション部203は，暗号化された読み込み対象のデータを受信すると，その暗号化されたデータと個別情報とが含まれる読み込み用の要求情報をサービス提供サーバ201に送信する(S1015)。

[0186] ライセンス認証部241は，上記要求情報を取得すると，サービス提供サーバ201にてデータ暗号化処理の際に用いられたシステム認証鍵220aに対応するシステム認証鍵220bで，復号する。当該復号により，ライセンス認証部241は，データ送信元であるサービス提供サーバ201の真正性について検証することができる(S1017)。

[0187] また，ライセンス認証部241は，受け取った要求情報に設定された「クライアントアプリID」などを基に該当するライセンスをライセンスデータベース(図示せず。)から検索し，そのライセンスに設定された「利用回数」等の利用条件が適切であるか否かを確認する(S1017)する。なお，「利用回数」等の利用条件のほかに，判断部225は，上記説明したが携帯機器のハードウェアIDなどを確認してもよい。

[0188] ライセンス認証部241による検証処理(S1017)が終了すると，非接触型ICカードモジュール223の読み込みデータを携帯通信端末103に送信する(S1019)。アプリケーション部203は，上記データを画面上に表示等する。

[0189] 例えば，サービス提供システム101が提供するサービスとしてポイントを付与するサービスが存在する場合，非接触型ICカードモジュール223に格納されたポイント残高がどの程度なのかを画面上に表示することによって，利用者は確認することができる。以上で，本実施の形態にかかる読み込み処理の一連の動作が終了する。

[0190] なお，図10に示す読み込み処理では読み込み対象のデータを暗号化する場合を例に挙げたが，かかる例に限定されず，例えば，読み込み処理では，一切暗号化しない場合，暗号化の代わりに電子署名を付加する場合，電子署名を付加した上でそ

の電子署名付き読み込みデータを暗号化する場合などでもよい。つまり，上記説明したように暗号化又は電子署名などのセキュリティ環境を組み合わせて実行できる。

[0191] なお，図7～図10に示す一連の処理は，専用のハードウェアにより行うこともできるし，ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には，そのソフトウェアを構成するプログラムが汎用のコンピュータやマイクロコンピュータ等の情報処理装置にインストールされ，上記情報処理装置を代行システムサーバ205，サービス提供サーバ201，携帯通信端末103として機能させる。

[0192] プログラムは，コンピュータに内蔵されている記録媒体としてのハードディスクやROM等に予め記録しておくことができる。あるいはまた，プログラムは，ハードディスクドライブに限らず，フレキシブルディスク，CD－ROM（Compact Disc Read Only Memory），MO（Magneto Optical）ディスク，DVD（Digital Versatile Disc）などに，一時的あるいは永続的に格納（記録）しておくことができる。

[0193] また，プログラムを人工衛星等を介して，コンピュータに無線で転送したり，LAN（Local Area Network），インターネットといったネットワークを介して，コンピュータに有線で転送する場合でもよい。

[0194] ここで，本明細書において，コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは，必ずしもシーケンス図として記載された順序に沿って時系列に処理する必要はなく，並列的あるいは個別に実行される処理（例えば，並列処理あるいはオブジェクトによる処理）も含むものである。

[0195] また，プログラムは，1のコンピュータにより処理されるものであっても良いし，複数のコンピュータによって分散処理されるものであっても良い。

[0196] 以上で，本実施の形態にかかるデータ通信システム100の説明を終了するが，かかるデータ通信システム100によって以下に示すような効果がある。

（1）複数の認証機能を提供し，それらを各サービス提供システム101のセキュリティレベルに応じて自由に組み合わせることができる。さらにサービス提供者がセキュリティとシステム構築のコスト等を考慮して，容易に設定／変更が可能である。例えば，サービス提供システム101のセキュリティレベルを上げた場合，ワンタイムのライセンスを適用し，セキュリティレベルを下げた場合，クライアントアプリID認証のみを適用す

るように認証処理を組み合わせることができる。

(2)ライセンス認証機能を利用した場合，例えば，無期限とするライセンスや，ワンタイムなライセンスなど，サービス提供者がセキュリティポリシーに応じライセンスの期限を定めることで柔軟な運用ができる。

(3)ライセンスの発行単位を携帯通信端末103としてサービス利用可能な機器を制限しているため第三者による不正利用を困難にすることができる。

(4)アプリケーション部203が，サーバ等との通信ステータスを一元管理できるため，例えば，通信網の接続不能時に容易にリトライすることができる。

(5)アプリケーション部203による通信量を削減することができる。

(6)代行システム105側でカスタマイズ可能な認証機能を提供することで，代行システムとサービス提供システムとの間のシステム構築工数を削減することができる。

(7)非接触型ICカードモジュール223と代行システム105との相互認証を利用しているため，サービス提供システム101が代行システム105を認証する手順を省略できる。

(8)携帯通信端末103を識別する識別情報を作成しなくても，システム認証鍵等を用いた認証手段によって，データ通信システムを実行することが可能であるため，汎用性のあるデータ通信システムを実現することができ，携帯通信端末103のキャリアや，機種等に依存せずに非接触型ICカードモジュールに通信処理を実行させて，サービスを提供することができる。

[0197] 以上，添付図面を参照しながら本発明の好適な実施形態について説明したが，本発明はかかる例に限定されない。当業者であれば，特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例を想定し得ることは明らかであり，それらについても当然に本発明の技術的範囲に属するものと了解される。

[0198] 上記実施形態においては，データ通信システム100には，サービス提供システム101と，代行システム105とがそれぞれ1つ備わる場合を例に挙げて説明したが，本発明は係る場合に限定されない。例えば，データ通信システム100には，サービス提供システム101が各サービス提供者単位に複数備わる場合でも実施可能である。また，データ通信システム100には，代行システム105が複数備わる場合でも実施可能

である。

[0199] 上記実施形態においては，サービス提供システム101に備わる各部はハードウェアからなる場合を例にあげて説明したが，本発明はかかる例に限定されない。例えば，上記各部は，1又は2以上のモジュールまたはコンポーネントから構成されるプログラムの場合であってもよい。

[0200] 上記実施形態においては，代行システム105に備わる各部はハードウェアからなる場合を例にあげて説明したが，本発明はかかる例に限定されない。例えば，上記各部は，1又は2以上のモジュールまたはコンポーネントから構成されるプログラムの場合であってもよい。

[0201] 上記実施形態においては，携帯通信端末103に備わるアプリケーション部203及び実行部213は1又は2以上のモジュールまたはコンポーネントから構成されるプログラムの場合を例に挙げて説明したが，かかる例に限定されず，例えば，1又は2以上の素子から構成された回路等のハードウェアの場合でもよい。

[0202] また，上記実施形態においては，携帯通信端末103は，非接触型ICカードモジュール223を備えた携帯電話である場合を例に挙げて説明したが，外部と通信網を介して通信可能であり，非接触型ICカードモジュール223を備えていれば，本発明はかかる例に限定されない。例えば，携帯通信端末103は，ノート型PC，PDA（Personal Digital Assistant）などの場合でもよい。

[0203] また，上記実施携帯では，通信部235は，通信網106，ゲートウェイ117，パケット通信網115，および基地局113を介し，さらに携帯通信端末103に備わる実行部213を介して非接触型ICカードモジュール223と相互認証などの一連の通信を行う場合を例に挙げて説明したが，本発明は，かかる例に限定されない。例えば，通信部235は，通信網104と情報処理装置109に備わるR／W111を介して，さらに携帯通信端末103に備わる実行部213を介して非接触型ICカードモジュール223と通信する場合でもよい。

[0204] 以上説明したように，本発明によれば，データ通信システムにおいて通信相手を認証する際，1又は2種以上の認証処理のうちセキュリティレベルに応じて選択された認証処理を組み合わせて実行することが可能であるため，サービスを提供する側の要

求に対して柔軟に対応することができる。

産業上の利用可能性

[0205] 本発明は，データ通信システム，代行システムサーバ，コンピュータプログラム，およびデータ通信方法に適用可能である。

請求の範囲

[1] それぞれが外部からの要求に応じて情報処理する非接触型ICカードモジュールを備える一つ以上の携帯通信端末と，その非接触型ICカードモジュールの情報処理によってサービスを提供するサービス提供システムと，該サービス提供システムを代行して前記非接触型ICカードモジュールと通信処理する代行システムとを備えたデータ通信システムであって：

前記携帯通信端末は，前記非接触型ICカードモジュールと前記代行システムとが通信処理を行うために，前記サービス提供システムが保有する情報であって前記携帯通信端末に付与した該通信処理に関するライセンスを示す付与済みライセンス情報を要求する要求部を備え，

前記サービス提供システムは，前記携帯通信端末の1つから要求されると，該要求元の携帯通信端末に係る付与済みライセンス情報を取得する取得部とを備えており，

前記取得した付与済みライセンス情報は，前記代行システム及び前記サービス提供システムの双方が保持し該双方との間で情報を暗号化／復号可能なシステム認証鍵で前記サービス提供システムによって暗号化され，さらに前記携帯通信端末及び前記代行システムの双方が保持し該双方との間で情報を暗号化／復号可能なクライアント認証鍵で前記携帯通信端末によって暗号化されて前記代行システムに送信され，

前記代行システムは，前記システム認証鍵を用いることで前記サービス提供システムを認証するシステム認証処理，前記クライアント認証鍵を用いることで前記携帯通信端末を認証する第1のクライアント認証処理，および前記携帯通信端末を識別する識別情報を用いることで前記携帯通信端末を認証する第2のクライアント認証処理を含む複数の認証処理のうち少なくとも一つの認証処理を前記携帯通信端末からの付与済みライセンス情報を基にして実行する認証部と；

前記認証部による認証処理後，前記付与済みライセンス情報に設定されたライセンスに基づいて通信許可／通信不許可を判断する判断部と；

前記判断部によって通信が許可されると，前記非接触型ICカードモジュールと通

信処理を行う通信部とを備えるデータ通信システム。

[2] 前記認証部は，前記1又は2種以上の認証処理のうち一つあるいは二つ以上選択され組み合わされた認証処理の選択指示を受信し，受信した前記選択指示に従って認証処理を実行する請求項1に記載のデータ通信システム。

[3] 前記通信部が行う通信処理は，前記非接触型ICカードモジュールに書き込み処理又は読み込み処理を実行させる処理である請求項1に記載のデータ通信システム。

[4] 前記読み込み処理の対象となるデータについて，そのデータを暗号化する処理，又はデータを基にして作成される電子署名を該データに付加する処理のうち一方あるいは両方の処理の選択指示を受け付け，前記認証部は，受け付けた前記選択指示に従って処理する請求項3に記載のデータ通信システム。

[5] 前記書き込み処理の対象となるデータについて，暗号化されたデータを復号する処理，および予め電子署名が付加されたデータを基にしてそのデータの真正性を検証する処理のうち一方あるいは両方の処理の選択指示が受け付け，前記認証部は，その選択指示に従って処理する請求項3に記載のデータ通信システム。

[6] 前記サービス提供システムと前記代行システムとの通信は，前記携帯通信端末を介して行われる請求項1に記載のデータ通信システム。

[7] 前記第1のクライアント認証処理は，前記携帯通信端末に対してチャレンジコードを送信し，そのチャレンジコードと前記付与済みライセンス情報とを基にして作成されるレスポンスを受けることによって認証するチャレンジレスポンス方式の認証処理である請求項1に記載のデータ通信システム。

[8] 前記携帯通信端末は，携帯電話である請求項1に記載のデータ通信システム。

[9] 携帯通信端末に備わる非接触型ICカードモジュールが情報処理することでサービスを提供するサービス提供サーバを代行して，該非接触型ICカードモジュールと通信処理する代行システムサーバであって：

前記非接触型ICカードモジュールと代行システムサーバとの通信処理に関するライセンスを示した付与済みライセンス情報は前記代行システムサーバ及び前記サービス提供サーバの双方が保持し該双方との間で情報を暗号化／復号可能なシステム認証鍵で前記サービス提供サーバによって暗号化されて，さらに該携帯通信端末

及び前記代行システムサーバの双方が保持し該双方との間で情報を暗号化／復号可能なクライアント認証鍵で前記携帯通信端末によって暗号化され，その暗号化された付与済みライセンス情報を該携帯通信端末から受信する受信部と；

前記システム認証鍵を用いることで前記サービス提供システムを認証するシステム認証処理，前記クライアント認証鍵を用いることで前記携帯通信端末を認証する第1のクライアント認証処理，および前記携帯通信端末を識別する識別情報を用いることで前記携帯通信端末を認証する第2のクライアント認証処理を含む複数の認証処理のうち少なくとも一つの認証処理を前記携帯通信端末からの付与済みライセンス情報を基にして実行する認証部と；

前記認証部による認証処理後，前記付与済みライセンス情報に設定されたライセンスに基づき通信許可／通信不許可を判断する判断部と；

前記判断部によって通信許可されると，前記非接触型ICカードモジュールと通信処理を行う通信部とを備える代行システムサーバ。

[10] 前記認証部は，前記1又は2種以上の認証処理のうち一つあるいは二つ以上選択され組み合わされた認証処理の選択指示を受信し、受信した前記選択指示に従って認証処理を実行する請求項9に記載の代行システムサーバ。

[11] 前記通信部が行う通信処理は，前記非接触型ICカードモジュールに書き込み処理又は読み込み処理を実行させる処理である請求項9に記載の代行システムサーバ。

[12] 前記読み込み処理の対象となるデータについて，そのデータを暗号化する処理，又はデータを基にして作成される電子署名を該データに付加する処理のうち一方あるいは両方の処理の選択指示を受け付け，前記認証部は，受け付けた前記選択指示に従って処理する請求項11に記載の代行システムサーバ。

[13] 前記書き込み処理の対象となるデータについて，暗号化されたデータを復号する処理，又は予め電子署名が付加されたデータを基にしてそのデータの真正性を検証する処理のうち少なくとも一方の処理の選択指示が受け付け，前記認証部は，その選択指示に従って処理する請求項11に記載の代行システムサーバ。

[14] コンピュータをして，携帯通信端末に備わる非接触型ICカードモジュールが情報処理することでサービスを提供するサービス提供サーバを代行して，該非接触型ICカ

ードモジュールと通信処理する代行システムサーバとして機能させるコンピュータプログラムであって:

前記非接触型ICカードモジュールと代行システムサーバとの通信処理に関するライセンスを示した付与済みライセンス情報は前記代行システムサーバ及び前記サービス提供サーバの双方が保持し該双方との間で情報を暗号化／復号可能なシステム認証鍵で前記サービス提供サーバによって暗号化されて，さらに該携帯通信端末及び前記代行システムサーバの双方が保持し該双方との間で情報を暗号化／復号可能なクライアント認証鍵で前記携帯通信端末によって暗号化され，その暗号化された付与済みライセンス情報を該携帯通信端末から受信する受信手段と;

前記システム認証鍵を用いることで前記サービス提供サーバを認証するシステム認証処理，前記クライアント認証鍵を用いることで前記携帯通信端末を認証する第1のクライアント認証処理，および前記携帯通信端末を識別する識別情報を用いることで前記携帯通信端末を認証する第2のクライアント認証処理を含む複数の認証処理のうち少なくとも一つの認証処理を前記携帯通信端末からの付与済みライセンス情報を基にして実行する認証手段と;

前記認証処理後，前記付与済みライセンス情報に基づき通信許可／通信不許可を判断する判断手段と;

前記判断した結果，通信処理が許可された場合，前記非接触型ICカードモジュールと通信処理を行う通信手段とを備えるコンピュータプログラム。

[15] 携帯通信端末に備わる非接触型ICカードモジュールが情報処理することでサービスを提供するサービス提供サーバを代行して，該非接触型ICカードモジュールとして通信処理する代行システムサーバのデータ通信方法であって:

前記非接触型ICカードモジュールと代行システムサーバとの通信処理に関するライセンスを示した付与済みライセンス情報は前記代行システムサーバ及び前記サービス提供サーバの双方が保持し該双方との間で情報を暗号化／復号可能なシステム認証鍵で前記サービス提供サーバによって暗号化されて，さらに該携帯通信端末及び前記代行システムサーバの双方が保持し該双方との間で情報を暗号化／復号可能なクライアント認証鍵で前記携帯通信端末によって暗号化され，その暗号化さ

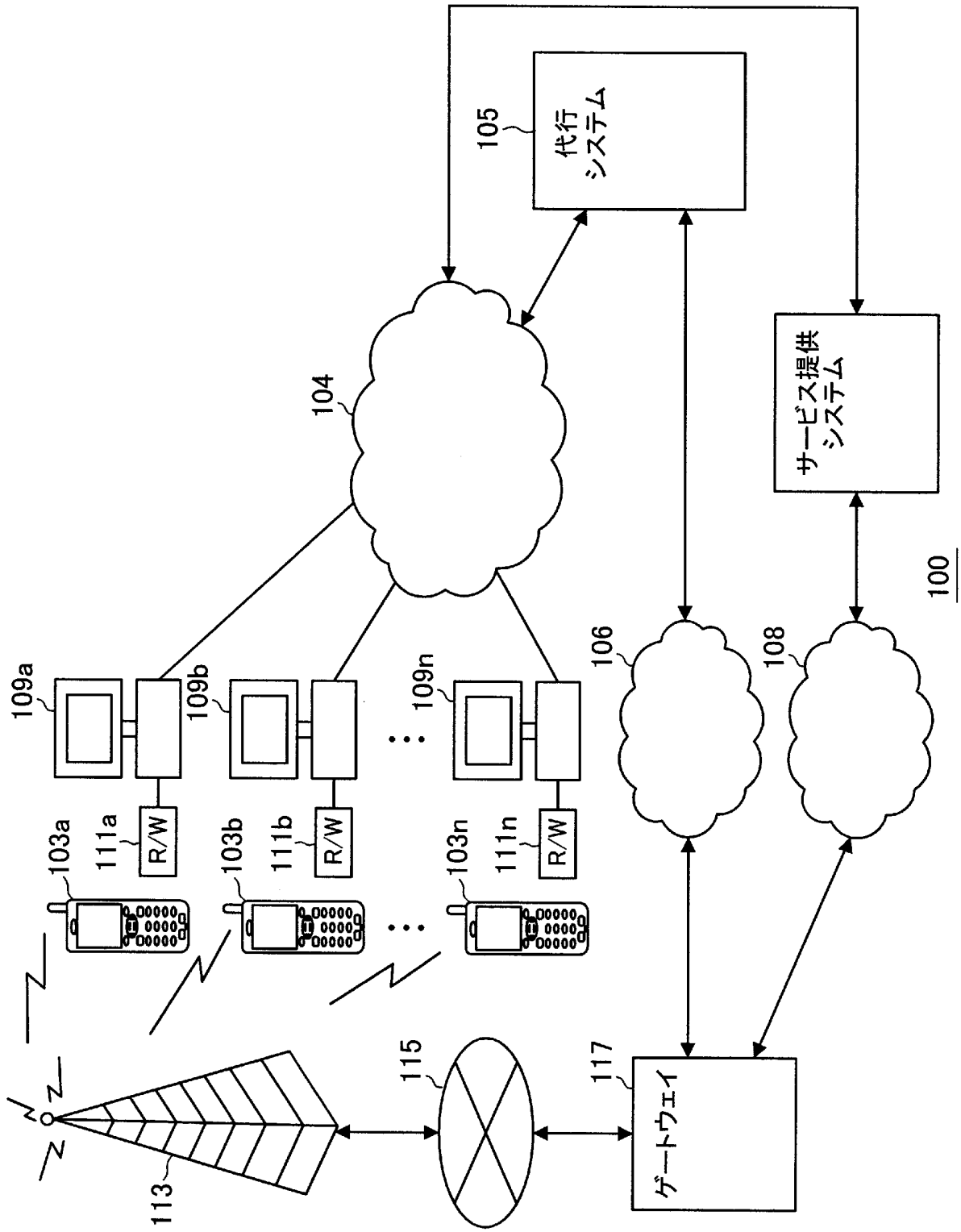
れた付与済みライセンス情報を該携帯通信端末から受信する受信ステップと;

前記システム認証鍵を用いることで前記サービス提供サーバを認証するシステム認証処理，前記クライアント認証鍵を用いることで前記携帯通信端末を認証する第1のクライアント認証処理，および前記携帯通信端末を識別する識別情報を用いることで前記携帯通信端末を認証する第2のクライアント認証処理を含む複数の認証処理のうち少なくとも一つの認証処理を前記携帯通信端末からの付与済みライセンス情報を基にして実行する認証ステップと;

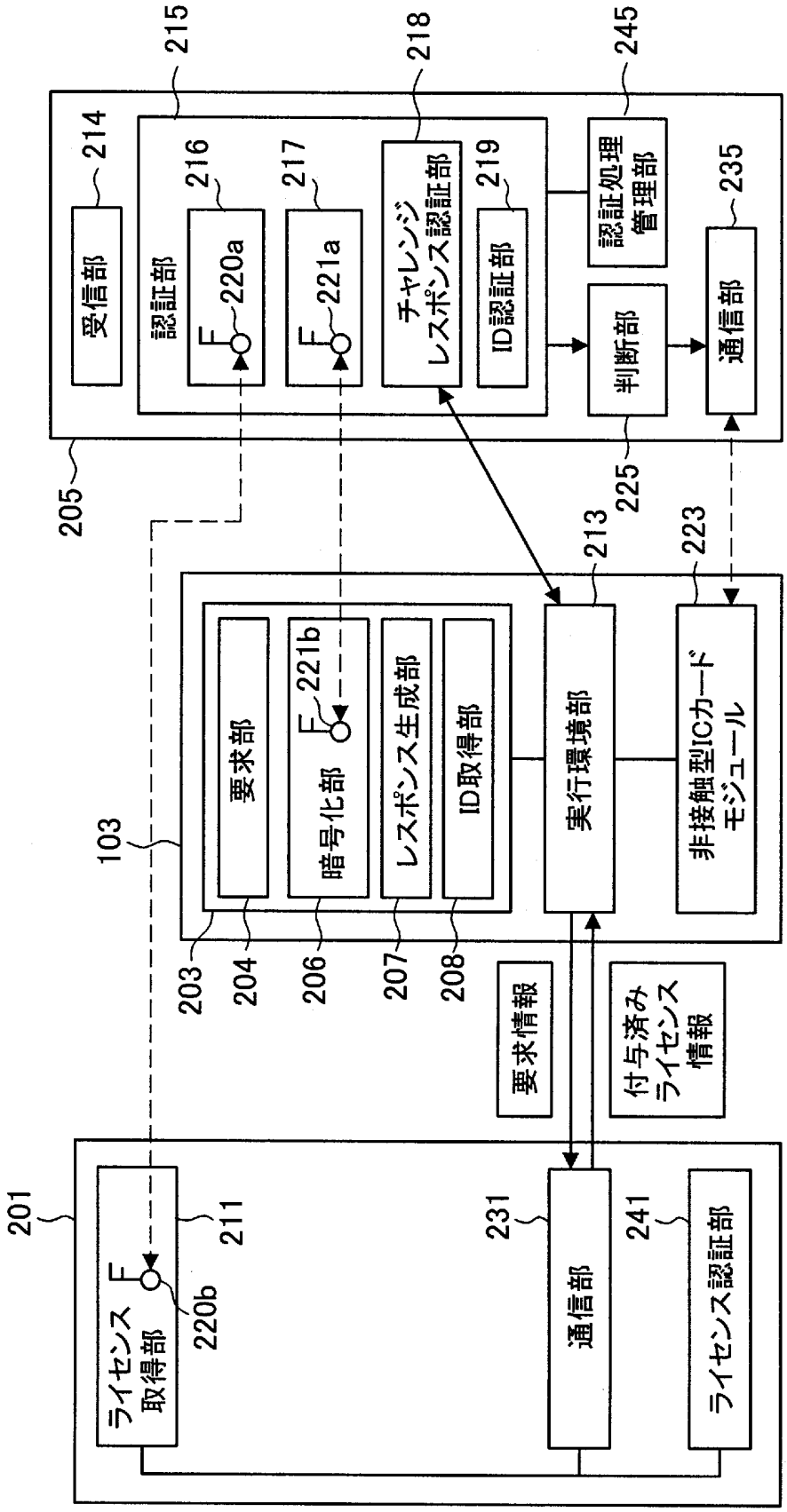
前記認証ステップを実行した後，前記付与済みライセンス情報に基づき通信許可／通信不許可を判断する判断ステップと;

前記判断ステップにおける判断結果が通信許可の場合，前記非接触型ICカードモジュールと通信処理を行う通信ステップとを含むデータ通信方法。

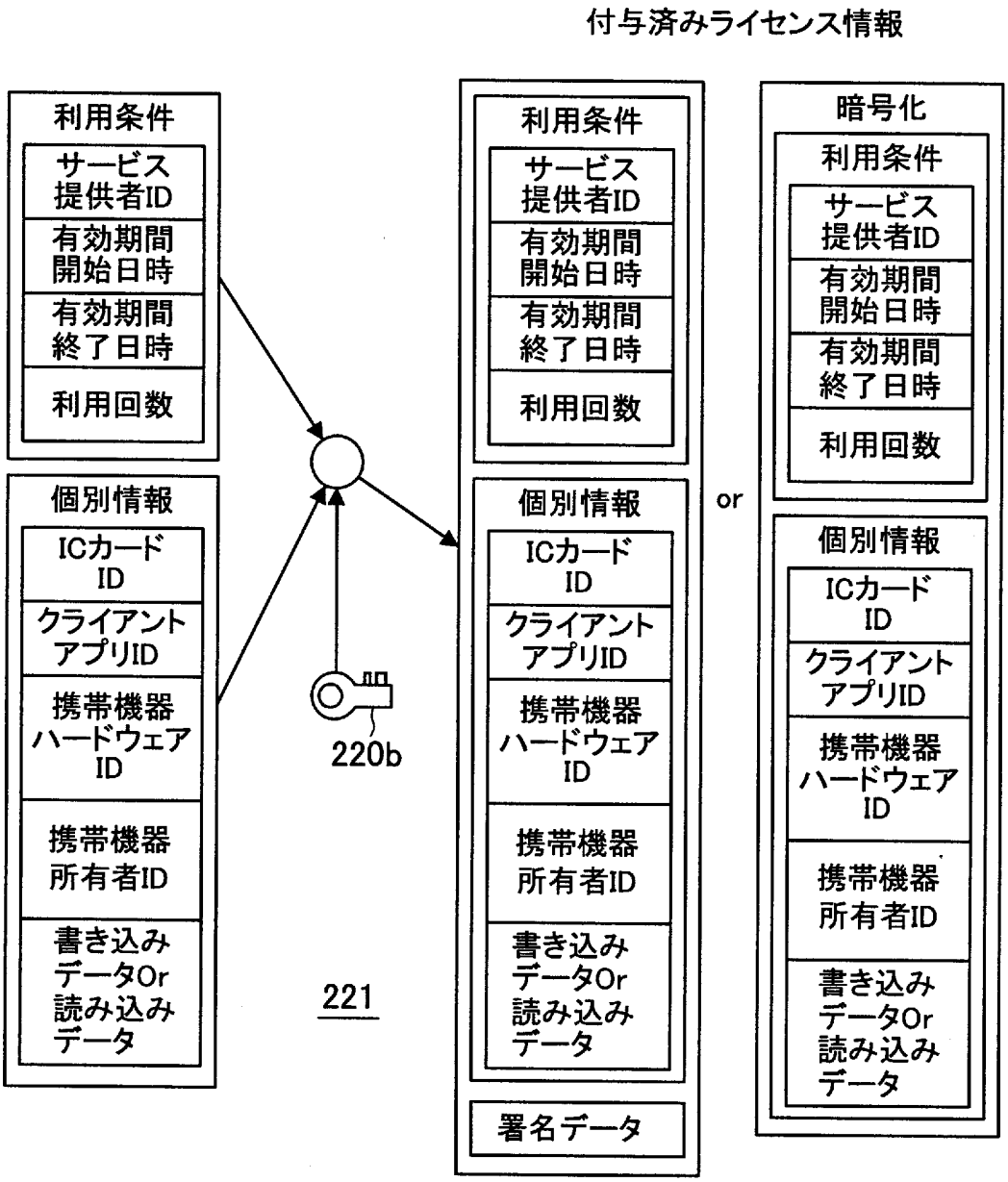
[図1]


105
代行システム
104
サービス提供システム
100
106
108
109a
109b
109n
103a
111a
R/W
103b
111b
R/W
103n
111n
R/W
115
117
ゲートウェイ
113

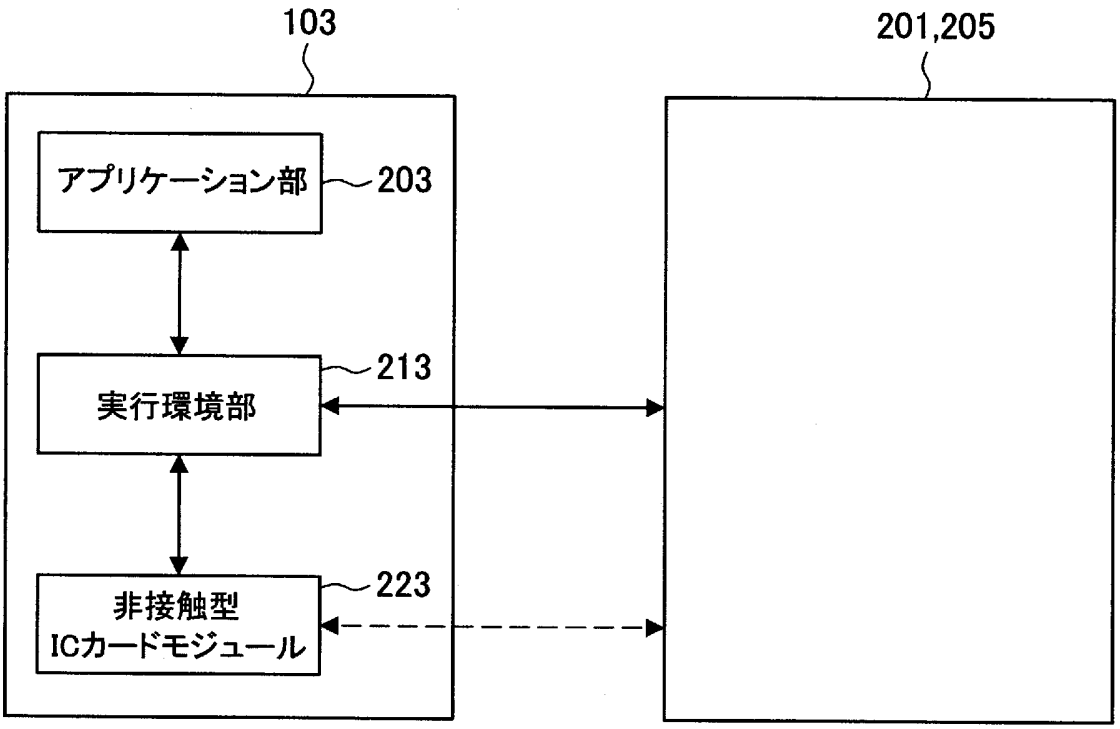
[図2]


受信部
214
認証部
215
220a
216
221a
217
チャレンジ
レスポンス認証部
218
ID認証部
219
認証処理
管理部
245
判断部
通信部
235
205
225
213
223
要求部
暗号化部
221b
レスポンス生成部
ID取得部
実行環境部
非接触型ICカード
モジュール
103
203
204
206
207
208
要求情報
付与済み
ライセンス
情報
201
ライセンス
取得部
220b
211
231
通信部
241
ライセンス認証部

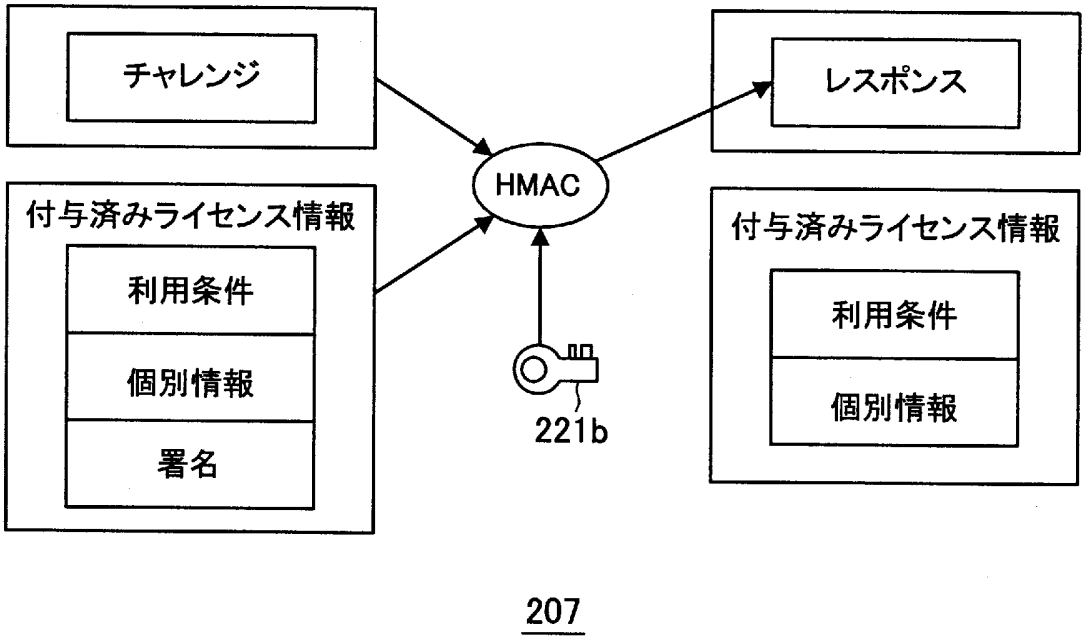
[図3]


付与済みライセンス情報
利用条件
サービス提供者ID
有効期間開始日時
有効期間終了日時
利用回数
個別情報
ICカードID
クライアントアプリID
携帯機器ハードウェアID
携帯機器所有者ID
書き込みデータOr読み込みデータ
署名データ
or
暗号化
220b
221

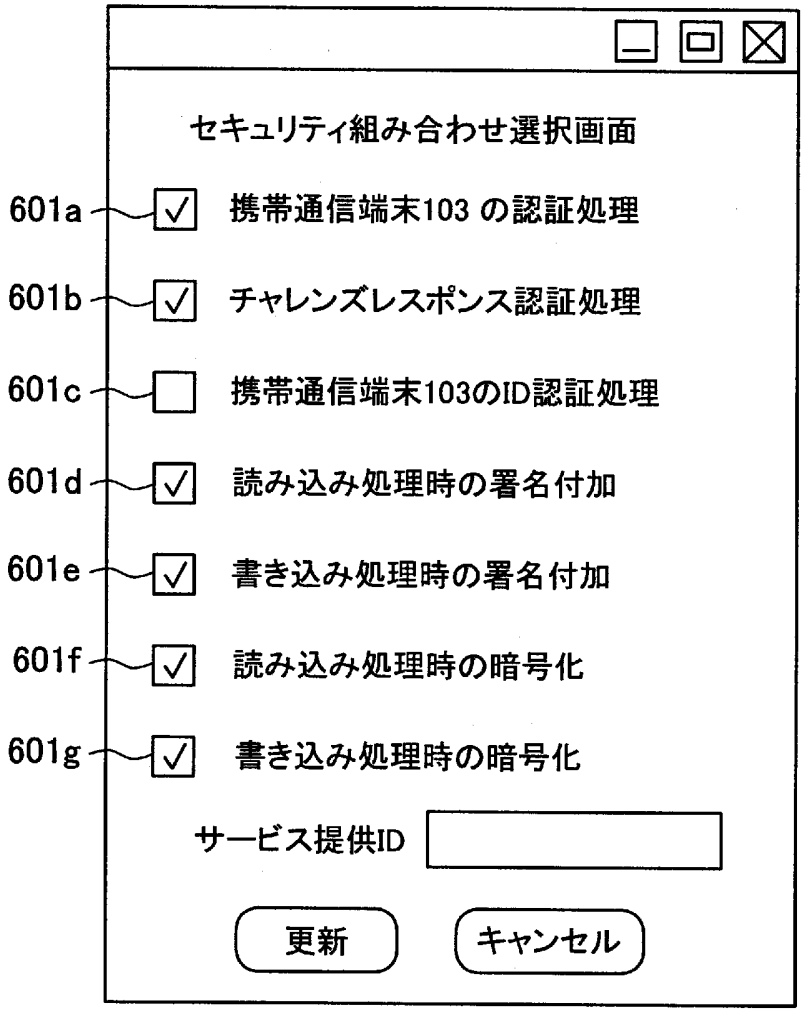
[図4]


103
201,205
アプリケーション部
203
実行環境部
213
非接触型
ICカードモジュール
223

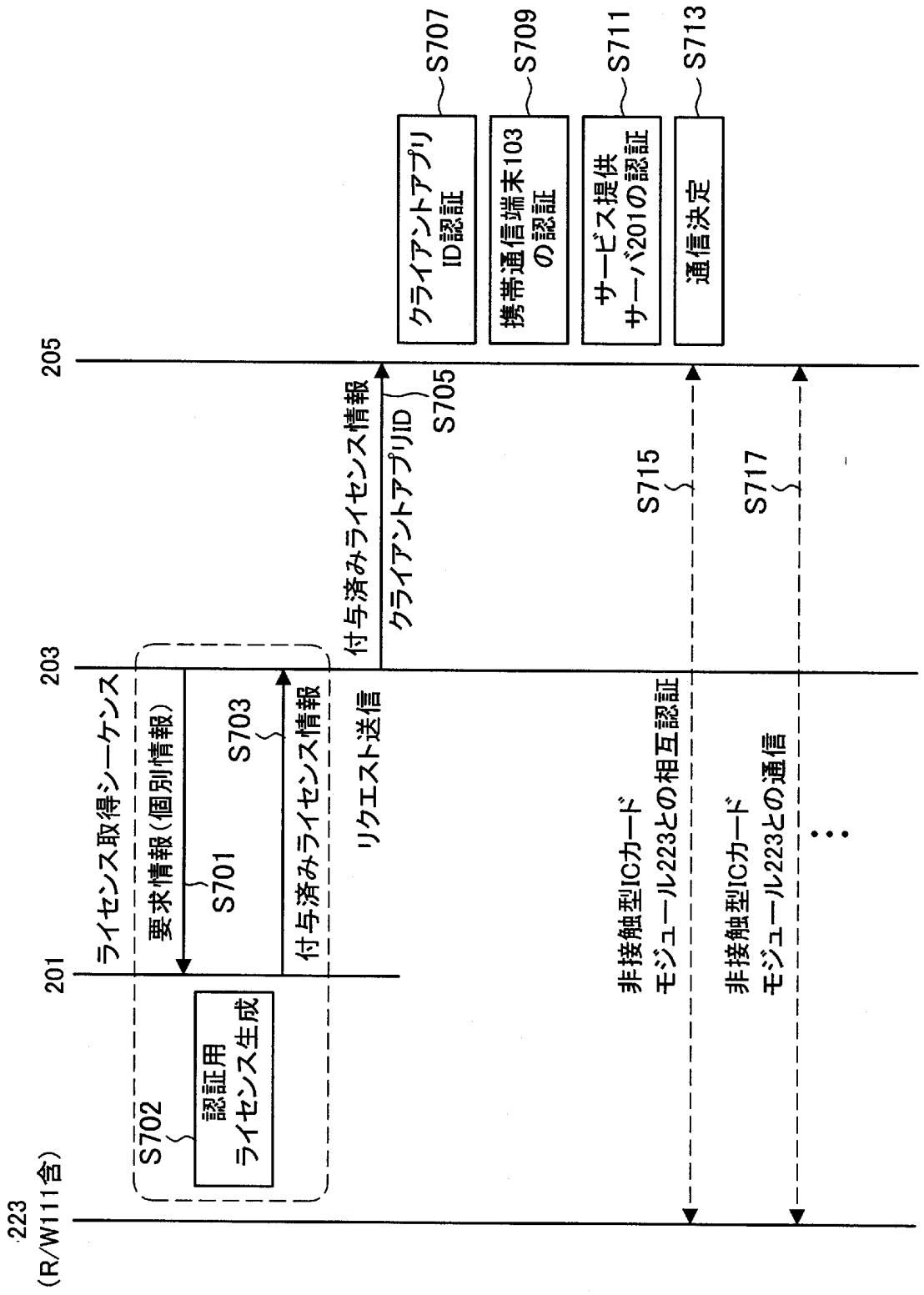
[図5]


チャレンジ
付与済みライセンス情報
利用条件
個別情報
署名
HMAC
221b
レスポンス
付与済みライセンス情報
利用条件
個別情報
207

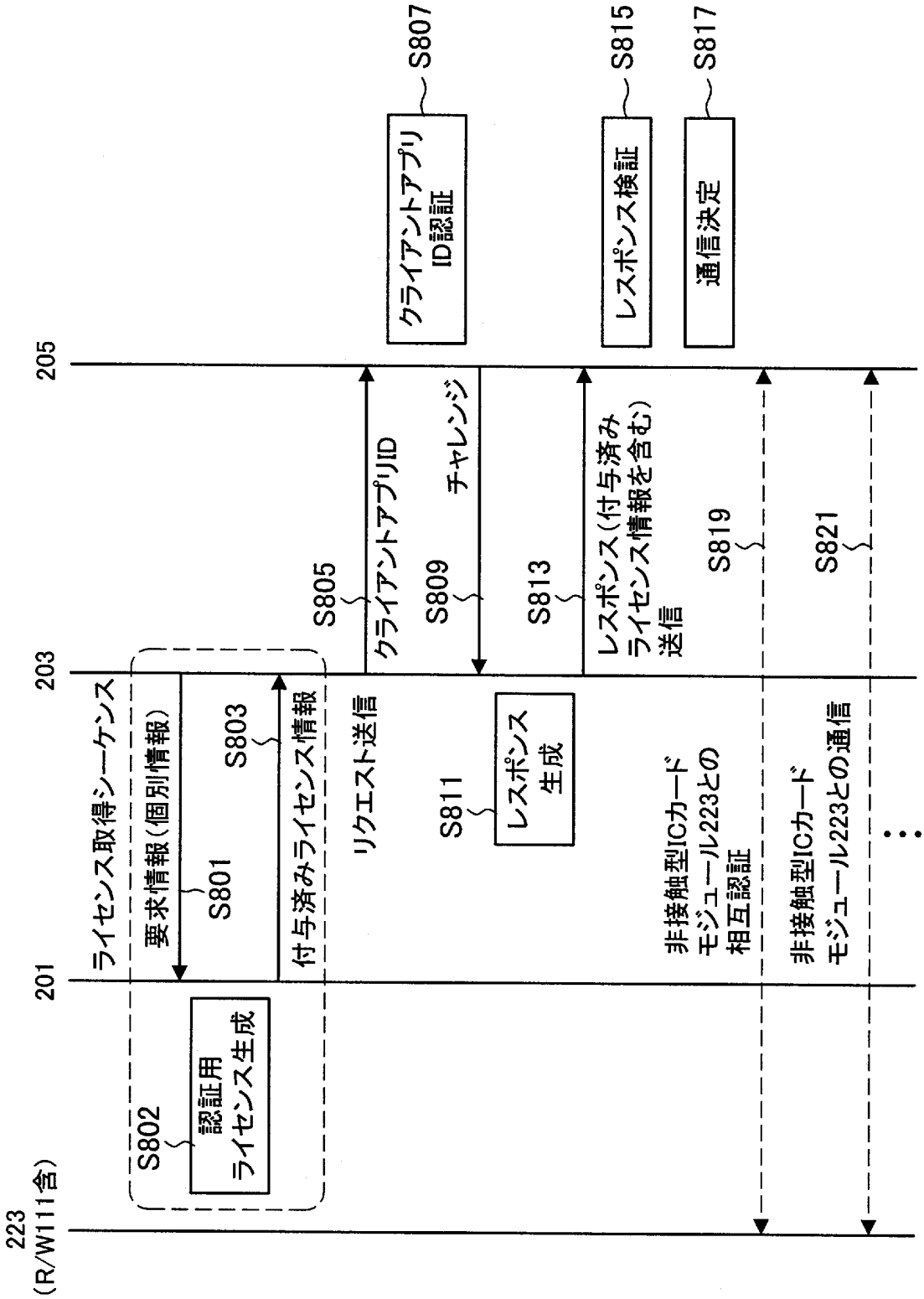
[図6]


セキュリティ組み合わせ選択画面
601a
携帯通信端末103 の認証処理
601b
チャレンズレスポンス認証処理
601c
携帯通信端末103のID認証処理
601d
読み込み処理時の署名付加
601e
書き込み処理時の署名付加
601f
読み込み処理時の暗号化
601g
書き込み処理時の暗号化
サービス提供ID
更新
キャンセル

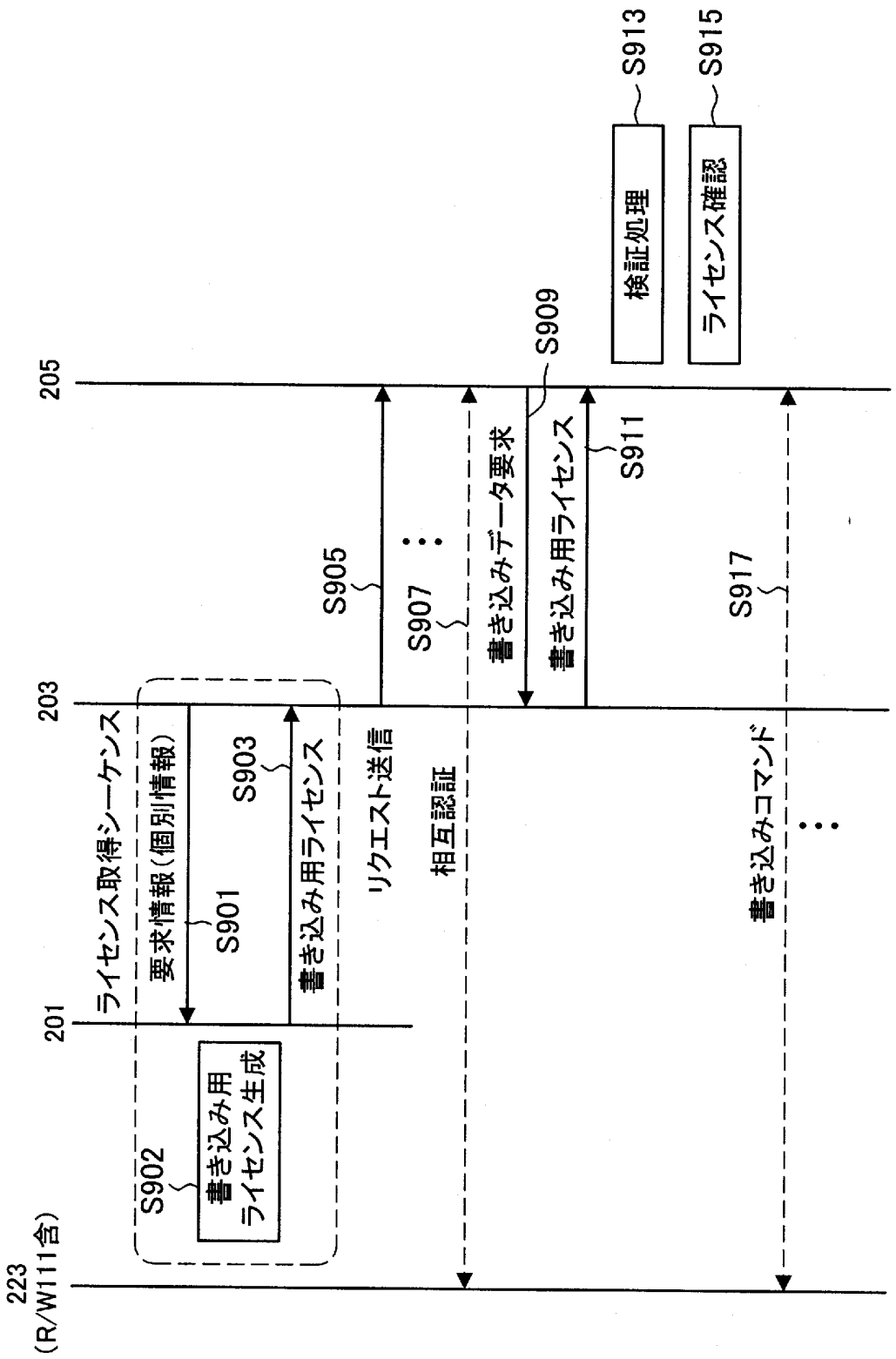
[図7]


223
(R/W111含)
201
203
205
ライセンス取得シーケンス
要求情報(個別情報)
S701
S703
S702
認証用
ライセンス生成
付与済みライセンス情報
リクエスト送信
付与済みライセンス情報
クライアントアプリID
S705
クライアントアプリ
ID認証
S707
携帯通信端末103
の認証
S709
サービス提供
サーバ201の認証
S711
通信決定
S713
S715
非接触型ICカード
モジュール223との相互認証
S717
非接触型ICカード
モジュール223との通信

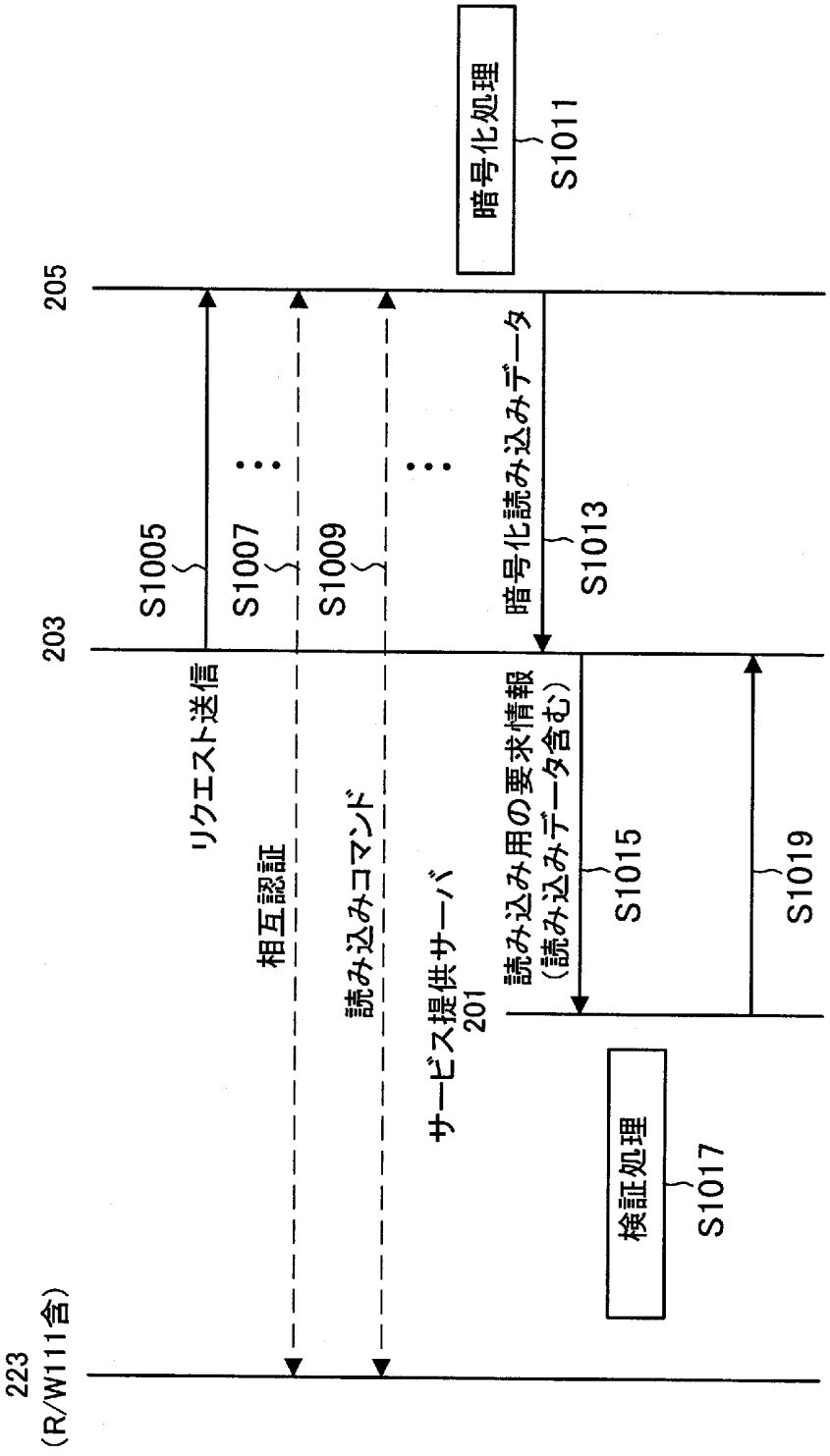
[図8]


223
(R/W111含)
201
203
205
ライセンス取得シーケンス
要求情報(個別情報)
S801
S802
認証用
ライセンス生成
S803
付与済みライセンス情報
リクエスト送信
S805
クライアントアプリID
S807
クライアントアプリ
ID認証
S809
チャレンジ
S811
レスポンス
生成
S813
レスポンス(付与済み
ライセンス情報を含む)
送信
S815
レスポンス検証
S817
通信決定
S819
非接触型ICカード
モジュール223との
相互認証
S821
非接触型ICカード
モジュール223との通信

[図9]


223
(R/W111含)
201
203
205
ライセンス取得シーケンス
要求情報(個別情報)
S901
S902
書き込み用
ライセンス生成
S903
書き込み用ライセンス
リクエスト送信
相互認証
S905
S907
書き込みデータ要求
S909
書き込み用ライセンス
S911
検証処理
S913
ライセンス確認
S915
S917
書き込みコマンド

[図10]


223
(R/W111含)
203
205
リクエスト送信
S1005
相互認証
S1007
読み込みコマンド
S1009
サービス提供サーバ
201
暗号化処理
S1011
暗号化読み込みデータ
S1013
読み込み用の要求情報
(読み込みデータ含む)
S1015
検証処理
S1017
S1019

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/303749

A. CLASSIFICATION OF SUBJECT MATTER
H04Q7/38(2006.01), ***H04B7/26***(2006.01), ***H04L9/32***(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04Q7/38, H04B7/26, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-162680 A (JCB Co., Ltd.), 06 June, 2003 (06.06.03), Full text; Figs. 1 to 12 (Family: none)	1-15
A	JP 2003-203178 A (Mitsubishi Electric Corp.), 18 July, 2003 (18.07.03), Full text; Figs. 1 to 13 (Family: none)	1-15
A	JP 2004-258739 A (Omron Corp.), 16 September, 2004 (16.09.04), Full text; Figs. 1 to 12 (Family: none)	1-15

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 March, 2006 (22.03.06)	28 March, 2006 (28.03.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/303749

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-175545 A (Toshiba Corp.), 21 June, 2002 (21.06.02), Full text; Figs. 1 to 25 (Family: none)	1-15

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３０３７４９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　*H04Q7/38(2006.01), H04B7/26(2006.01), H04L9/32(2006.01)*

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04Q7/38, H04B7/26, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２００３－１６２６８０　Ａ（株式会社ジェーシービー） ２００３．０６．０６，全文，第１－１２図（ファミリーなし）	１－１５
Ａ	ＪＰ　２００３－２０３１７８　Ａ（三菱電機株式会社） ２００３．０７．１８，全文，第１－１３図（ファミリーなし）	１－１５
Ａ	ＪＰ　２００４－２５８７３９　Ａ（オムロン株式会社） ２００４．０９．１６，全文，第１－１２図（ファミリーなし）	１－１５

☑ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２２．０３．２００６	２８．０３．２００６

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｊ　９３７４
高橋　宣博
電話番号　０３－３５８１－１１０１　内線　３５３４

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３０３７４９

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２００２－１７５５４５　Ａ（株式会社東芝） ２００２．０６．２１，全文，第１－２５図（ファミリーなし）	１－１５