(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2018-32149
(P2018-32149A)
(43)公開日　平成30年3月1日(2018.3.1)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 17/30	(2006.01)	G06F	17/30	120A	5J104
H04L 9/14	(2006.01)	H04L	9/00	641	
		G06F	17/30	110F	

審査請求 未請求　請求項の数 9　ＯＬ　（全 17 頁）

(21)出願番号　特願2016-162889 (P2016-162889)
(22)出願日　平成28年8月23日 (2016.8.23)

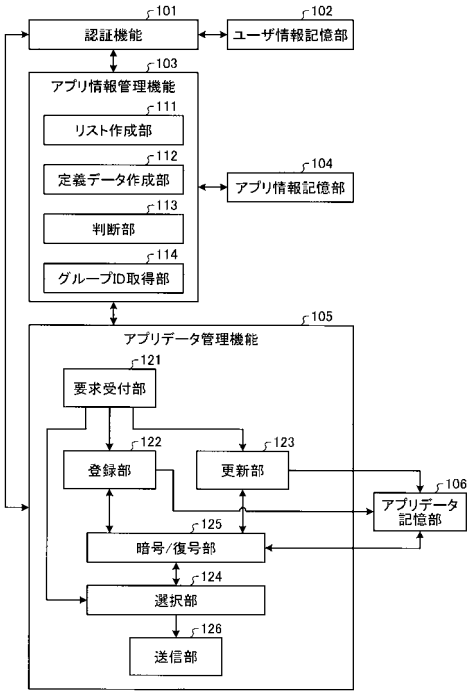
(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100089118
弁理士　酒井　宏明
(72)発明者　竹原　健
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考)　5J104 AA16　AA35　EA04　NA02　NA37
PA07

(54)【発明の名称】情報処理装置、情報処理システム、情報処理方法およびプログラム

(57)【要約】

【課題】情報の漏洩リスクを低減可能な情報処理装置、情報処理システム、情報処理方法およびプログラムを提供する。
【解決手段】本発明の情報処理装置は、第１の記憶部と選択部と復号部と送信部とを備える。第１の記憶部は、グループ識別情報と、アプリケーション識別情報と、暗号化されていない第１のデータと、グループ識別情報に基づく暗号鍵で第１のデータを暗号化した第２のデータと、を対応付けた第１の対応情報を記憶する。選択部は、検索要求を受け付けた場合、検索要求に含まれるアプリケーション識別情報と、検索要求に含まれる検索文字列と一致する第１のデータとの組み合わせに対応する第２のデータを選択する。復号部は、選択部により選択された第２のデータを、対応するグループ識別情報に基づく暗号鍵で復号する。送信部は、検索要求に対する応答として、復号部で復号されたデータを送信する。
【選択図】図３



【特許請求の範囲】
【請求項１】
グループを識別するグループ識別情報と、アプリケーションを識別するアプリケーション識別情報と、暗号化されていない第１のデータと、前記グループ識別情報に基づく暗号鍵で前記第１のデータを暗号化した第２のデータと、を対応付けた第１の対応情報を記憶する第１の記憶部と、
検索用の文字列を示す検索文字列と、前記アプリケーション識別情報とを含む検索要求を受け付けた場合、前記検索要求に含まれる前記アプリケーション識別情報と、前記検索要求に含まれる前記検索文字列と一致する前記第１のデータとの組み合わせに対応する前記第２のデータを選択する選択部と、
前記選択部により選択された前記第２のデータを、対応する前記グループ識別情報に基づく前記暗号鍵で復号する復号部と、
前記検索要求に対する応答として、前記復号部で復号されたデータを送信する送信部と、を備える、
情報処理装置。
【請求項２】
前記第１の対応情報は、
前記グループ識別情報と、前記アプリケーション識別情報とを対応付けた第２の対応情報と、
記録する情報の単位を示すレコードを識別するレコード識別情報ごとに、前記アプリケーション識別情報と、前記第１のデータと、前記第２のデータと、を対応付けた第３の対応情報と、から構成される、
請求項１に記載の情報処理装置。
【請求項３】
前記検索要求に含まれる前記アプリケーション識別情報に対応付けられた前記グループ識別情報を取得するグループ識別情報取得部をさらに備え、
前記選択部は、前記検索要求に含まれる前記アプリケーション識別情報と、前記検索要求に含まれる前記検索文字列と一致する前記第１のデータと、を含む１以上の前記レコードを選択し、該選択した１以上の前記レコードに含まれる前記第２のデータを選択し、
前記復号部は、前記選択部により選択された前記第２のデータを、前記グループ識別情報取得部により取得された前記グループ識別情報に基づく暗号鍵で復号する、
請求項２に記載の情報処理装置。
【請求項４】
前記グループ識別情報と、ユーザを識別するユーザ識別情報とを対応付けた第４の対応情報を記憶する第２の記憶部をさらに備え、
前記検索要求は前記ユーザ識別情報をさらに含み、
前記選択部は、
前記検索要求に含まれる前記ユーザ識別情報に対応付けられた前記グループ識別情報と、前記検索要求に含まれる前記アプリケーション識別情報に対応付けられた前記グループ識別情報とが一致する場合に、前記第２のデータの選択を行う、
請求項２または３に記載の情報処理装置。
【請求項５】
前記第１のデータと、前記ユーザ識別情報と、前記アプリケーション識別情報と、を含み、かつ、新規のデータ登録を要求する新規登録要求を受け付けた場合、前記新規登録要求に含まれる前記第１のデータと、前記新規登録要求に含まれる前記アプリケーション識別情報に対応付けられた前記グループ識別情報に基づく暗号鍵で該第１のデータを暗号化した前記第２のデータと、前記レコード識別情報とを対応付けた新たな前記レコードを前記第３の対応情報に登録する登録部をさらに備える、
請求項４に記載の情報処理装置。
【請求項６】

前記第１のデータと、前記ユーザ識別情報と、前記アプリケーション識別情報と、前記レコード識別情報とを含み、かつ、前記レコードの更新を要求する更新要求を受け付けた場合、前記更新要求に含まれる前記レコード識別情報で識別される前記レコードに含まれる前記第１のデータを、前記更新要求に含まれる前記第１のデータに更新するとともに、該レコードに含まれる前記第２のデータを、前記更新要求に含まれる前記アプリケーション識別情報に対応付けられた前記グループ識別情報に基づく暗号鍵で該更新後の前記第１のデータを暗号化した前記第２のデータに更新する更新部をさらに備える、

請求項４または５に記載の情報処理装置。

【請求項７】

複数の情報処理装置群から構成される情報処理システムであって、

グループを識別するグループ識別情報と、アプリケーションを識別するアプリケーション識別情報と、暗号化されていない第１のデータと、前記グループ識別情報に基づく暗号鍵で前記第１のデータを暗号化した第２のデータと、を対応付けた第１の対応情報を記憶する第１の記憶部と、

検索用の文字列を示す検索文字列と、前記アプリケーション識別情報とを含む検索要求を端末から受け付けた場合、前記検索要求に含まれる前記アプリケーション識別情報と、前記検索要求に含まれる前記検索文字列と一致する前記第１のデータとの組み合わせに対応する１以上の前記第２のデータを選択する選択部と、

前記選択部により選択された前記第２のデータを、対応する前記グループ識別情報に基づく暗号鍵で復号する復号部と、

前記検索要求に対する応答として、前記復号部で復号されたデータを前記端末へ送信する送信部と、を備える、

情報処理システム。

【請求項８】

検索用の文字列を示す検索文字列と、アプリケーションを識別するアプリケーション識別情報とを含む検索要求を受け付けた場合、組織の単位を識別するグループ識別情報と、前記アプリケーション識別情報と、暗号化されていない第１のデータと、前記グループ識別情報に基づく暗号鍵で前記第１のデータを暗号化した第２のデータと、を対応付けた第１の対応情報を参照して、前記検索要求に含まれる前記アプリケーション識別情報と、前記検索要求に含まれる前記検索文字列と一致する前記第１のデータとの組み合わせに対応する１以上の前記第２のデータを選択する第２のデータ選択ステップと、

前記第２のデータ選択ステップにより選択された前記第２のデータを、対応する前記グループ識別情報に基づく前記暗号鍵で復号する復号ステップと、

前記検索要求に対する応答として、前記復号ステップで復号されたデータを送信する送信ステップと、を含む、

情報処理方法。

【請求項９】

コンピュータに、

検索用の文字列を示す検索文字列と、アプリケーションを識別するアプリケーション識別情報とを含む検索要求を受け付けた場合、グループを識別するグループ識別情報と、前記アプリケーション識別情報と、暗号化されていない第１のデータと、前記グループ識別情報に基づく暗号鍵で前記第１のデータを暗号化した第２のデータと、を対応付けた第１の対応情報を参照して、前記検索要求に含まれる前記アプリケーション識別情報と、前記検索要求に含まれる前記検索文字列と一致する前記第１のデータとの組み合わせに対応する１以上の前記第２のデータを選択する第２のデータ選択ステップと、

前記第２のデータ選択ステップにより選択された前記第２のデータを、対応する前記グループ識別情報に基づく前記暗号鍵で復号する復号ステップと、

前記検索要求に対する応答として、前記復号ステップで復号されたデータを送信する送信ステップと、を実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、情報処理装置、情報処理システム、情報処理方法およびプログラムに関する。
【背景技術】
【０００２】
従来、クラウドコンピューティングによるサービスを提供するクラウドシステムから、クラウドコンピューティングを可能とする機能を有する装置（例えば画像処理装置等）に対してサービスを提供する技術が知られている。
【０００３】
例えば特許文献１などに開示されたクラウドシステムにおいては、サービスを提供するサーバは、サービスを提供する単位となるグループ（テナント）ごとに、該グループでの使用が許可されるアプリケーションで利用されるデータを保持するためのデータベースを構築することが一般的であるが、このような形態ではデータの管理が煩雑となる。そこで、例えばグループごとのデータを１つのデータベース上でまとめて管理するといった方法が考えられる。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、上述したようにグループごとのデータを１つのデータベース上でまとめて管理する形態においては、ＳＱＬ（Structured Query Language）などを利用してデータの検索を実行するときの不正な操作などに起因して、検索文字列を含むデータだけでなく全てのグループにまたがる全データが外部に漏洩するリスクがある。
【０００５】
本発明は、上記に鑑みてなされたものであって、情報の漏洩リスクを低減可能な情報処理装置、情報処理システム、情報処理方法およびプログラムを提供することを目的とする。
【課題を解決するための手段】
【０００６】
上述した課題を解決し、目的を達成するために、本発明は、グループを識別するグループ識別情報と、アプリケーションを識別するアプリケーション識別情報と、暗号化されていない第１のデータと、前記グループ識別情報に基づく暗号鍵で前記第１のデータを暗号化した第２のデータと、を対応付けた第１の対応情報を記憶する第１の記憶部と、検索用の文字列を示す検索文字列と、前記アプリケーション識別情報とを含む検索要求を受け付けた場合、前記検索要求に含まれる前記アプリケーション識別情報と、前記検索要求に含まれる前記検索文字列と一致する前記第１のデータとの組み合わせに対応する前記第２のデータを選択する選択部と、前記選択部により選択された前記第２のデータを、対応する前記グループ識別情報に基づく前記暗号鍵で復号する復号部と、前記検索要求に対する応答として、前記復号部で復号されたデータを送信する送信部と、を備える情報処理装置である。
【発明の効果】
【０００７】
本発明によれば、情報の漏洩リスクを低減可能な情報処理装置、情報処理システム、情報処理方法およびプログラムを提供することができる。
【図面の簡単な説明】
【０００８】
【図１】図１は、実施形態のシステムの構成の一例を示す図である。
【図２】図２は、サーバのハードウェア構成の一例を示す図である。
【図３】図３は、サーバが有する機能の一例を示す図である。
【図４】図４は、ユーザ対応情報の一例を示す図である。

【図５】図５は、アプリケーション対応情報の一例を示す図である。
【図６】図６は、アプリデータの一例を示す図である。
【図７】図７は、システムの動作手順の一例を示すシーケンス図である。
【図８】図８は、ログイン画面の一例を示す図である。
【図９】図９は、初期画面の一例を示す図である。
【図１０】図１０は、システムの動作手順の一例を示すシーケンス図である。
【図１１】図１１は、レコード追加画面の一例を示す図である。
【図１２】図１２は、システムの動作手順の一例を示すシーケンス図である。
【図１３】図１３は、変更画面の一例を示す図である。
【図１４】図１４は、システムの動作手順の一例を示すシーケンス図である。
【図１５】図１５は、データ検索画面の一例を示す図である。
【発明を実施するための形態】
【０００９】
以下、添付図面を参照しながら、本発明に係る情報処理装置、情報処理システム、情報処理方法およびプログラムの実施形態を詳細に説明する。
【００１０】
図１は、本実施形態のシステム１００の構成の一例を示す図である。図１に示すように、システム１００は、クラウドコンピューティングによるサービスを提供するサーバ１０と、複数の端末２０と、を備え、これらは、インターネットなどのネットワーク３０を介して相互に接続される。この例では、サーバ１０によるクラウドサービスは、例えば企業などの経済活動を行う単位で区分されるグループごとに提供される。図１の例では、それぞれが何れかのグループに属する各端末２０は、サーバ１０と通信してデータを取得し、取得したデータを表示する機能（Ｗｅｂ－ＵＩ機能）を有している。端末２０は、例えばＰＣ（Personal Computer）であってもよいし、スマートデバイスやタブレットなどの可搬型の情報処理端末であってもよい。
【００１１】
次に、「情報処理装置」の一例であるサーバ１０の構成について説明する。説明の便宜上、図１の例では、システム１００に含まれるサーバ１０は１台であるが、これに限らず、システム１００に含まれるサーバ１０の台数は任意である（複数台であってもよい）。
【００１２】
図２は、サーバ１０のハードウェア構成の一例を示す図である。図２に示すように、サーバ１０は、ＣＰＵ１１、ＲＯＭ１２、ＨＤＤ１３、ＲＡＭ１４、入力部１５、表示部１６、通信Ｉ／Ｆ１７などを備え、それぞれがバスＢで相互に接続されている。
【００１３】
ＣＰＵ１１は、ＲＯＭ１２やＨＤＤ１３などの記憶装置からプログラムやデータをＲＡＭ１４上に読み出し、処理を実行することで、サーバ１０全体の制御や各種の機能を実現する演算装置である。
【００１４】
ＲＯＭ１２は、電源を切っても（サーバ１０に対する電力供給が遮断されても）プログラムやデータを保持することができる不揮発性の半導体メモリ（記憶装置）の一例である。ＲＯＭ１２には、サーバ１０の起動時に実行されるＢＩＯＳ、ＯＳ設定、及びネットワーク設定などのプログラムやデータが格納されている。
【００１５】
ＨＤＤ１３は、プログラムやデータを格納する不揮発性の記憶装置の一例である。ＲＡＭ１４は、プログラムやデータを一時保存する揮発性の記憶装置の一例であり、ＣＰＵ１１が実行する処理の作業領域（ワークエリア）として機能する。
【００１６】
入力部１５は、ユーザが各種の操作信号を入力するのに用いられるデバイスであり、例えばキーボードやマウス、タッチパネルなどで構成され得る。表示部１６は、各種の情報（例えばサーバ１０による処理の結果等）を表示するデバイスであり、例えば液晶型のデ

ィスプレイ装置で構成され得る。なお、例えばタッチパネルなどのように、入力部１５と表示部１６と、が一体で構成される形態であってもよい。また、入力部１５および表示部１６は必要なときに接続して利用する形態であってもよい。

【００１７】

通信Ｉ／Ｆ１７は、各端末２０と通信するためのインタフェースである。この例では、通信Ｉ／Ｆ１７は、サーバ１０をネットワーク３０に接続するためのインタフェースである。

【００１８】

図３は、サーバ１０が有する機能の一例を示す図である。図３に示すように、サーバ１０は、認証機能１０１と、ユーザ情報記憶部１０２と、アプリ情報管理機能１０３と、アプリ情報記憶部１０４と、アプリデータ管理機能１０５と、アプリデータ記憶部１０６と、を有する。

【００１９】

認証機能１０１は、ユーザ情報記憶部１０２に記憶されたユーザ情報を用いて、ユーザの認証を行う。つまり、ユーザ（アクセスしてきた端末１０）が、クラウドサービスを利用する権限を有するか否かを判断する機能を有する。この例では、サーバ１０が提供するクラウドサービスとしては、複数のデータ（アプリケーションで利用されるデータ）を端末２０上で設定または更新して、簡単にアプリケーションを作るというサービスを想定しているが、これに限られるものではない。認証機能１０１の詳細な動作については後述する。

【００２０】

ユーザ情報記憶部１０２は、クラウドサービスを利用する権限を有するユーザごとに、ユーザ情報を記憶する。この例ではユーザ情報は、ユーザＩＤとパスワードの組み合わせであるが、これに限られるものではない。

【００２１】

アプリ情報管理機能１０３は、アプリ情報記憶部１０４に記憶されたアプリ情報を管理し、アプリ情報を利用した各種の処理を行う。アプリ情報記憶部１０４は、複数のアプリケーションごとに、該アプリケーションに関する情報を示すアプリ情報（後述のリストの元になる情報や後述の定義データなど）を記憶する。図３に示すように、アプリ情報管理機能１０３は、リスト作成部１１１と、定義データ作成部１１２と、判断部１１３と、グループＩＤ取得部１１４とを有する。

【００２２】

リスト作成部１１１は、認証されたユーザが利用可能なアプリケーションのリストを作成する。この例では、リストは、アプリケーションを識別するアプリＩＤ（アプリケーション識別情報の一例）と、アプリケーションの名前（画面に表示するアプリ名）と、を含む。この例では、アプリ情報記憶部１０４は、複数のアプリケーションごとのアプリ情報に加えて、ユーザ対応情報とグループ対応情報とを記憶している。ユーザ対応情報は、「第４の対応情報」の一例であり、ユーザＩＤと、該ユーザＩＤで識別されるユーザが属するグループを識別するグループＩＤ（グループ識別情報の一例）とを対応付けた情報である。図４はユーザ対応情報の一例を示す図である。アプリケーション対応情報は、「第２の対応情報」の一例であり、アプリＩＤと、該アプリＩＤで識別されるアプリケーションを利用可能なグループを識別するグループＩＤとを対応付けた情報である。図５はアプリケーション対応情報の一例を示す図である。リスト生成部１１１の詳細な動作については後述する。この例では、アプリ情報記憶部１０４は、「第２の記憶部」として機能すると考えることもできる。

【００２３】

定義データ作成部１１２は、端末２０の画面上で選択されたアプリケーションの定義データを作成する。アプリケーションの定義データとは、該アプリケーションに対応する画面を生成するためのデータであり、アプリＩＤ、アプリの名前の他、項目リスト、画面のレイアウト情報などを含む。項目リストに含まれる要素としては、項目を識別する項目Ｉ

Ｄ（項目識別情報）、項目の名称、項目のタイプなどが挙げられる。定義データ作成部１１２の詳細な動作については後述する。

【００２４】

判断部１１３は、後述の各種の要求をしてきたユーザが、要求対象のアプリケーションを利用することができるか否かを判断する。判断部１１３の詳細な動作については後述する。グループＩＤ取得部１１４は、後述の各種の要求の対象となるアプリケーションに対応するグループＩＤを取得する。グループＩＤ取得部１１４の詳細な動作については後述する。

【００２５】

アプリデータ管理機能１０５は、アプリデータ記憶部１０６に記憶されたアプリデータを管理し、アプリデータを利用した各種の処理を行う。この例では、アプリデータは、「第３の対応情報」の一例であり、記録する情報の単位を示すレコードを識別するレコードＩＤ（レコード識別情報の一例）ごとに、アプリＩＤと、暗号化されていない第１のデータと、該アプリＩＤに対応するグループＩＤに基づく暗号鍵で第１のデータを暗号化した第２のデータと、を対応付けた情報である。

【００２６】

この例では、第１のデータは、項目とバリュー（暗号化されていないデータの実体）との組であると考えてもよいし、暗号化されていないバリューそのものであると考えてもよい。同様に、第２のデータは、項目とバリュー（暗号化されたデータの実体）との組であると考えてもよいし、暗号化されたバリューそのものであると考えてもよい。ここでは、第１のデータを暗号化するための暗号鍵は、上述のアプリケーション対応情報（図５参照）において、該第１のデータを利用するアプリケーションのアプリＩＤに対応付けられたグループＩＤに基づいて生成される。

【００２７】

図６は、アプリデータの一例を示す図である。ここでは、アプリデータは、レコードＩＤごとに、アプリＩＤと、暗号化されていないデータと、暗号化されたデータと、を対応付けた情報である。図６の例では、行単位の情報の集合である「レコード」は、レコードＩＤと、アプリＩＤと、暗号化されていないデータの項目を識別する項目ＩＤ（Ｄ＿ＩＤと表記）のバリューと、暗号化されたデータの項目を識別する項目ＩＤ（Ｅ＿ＩＤと表記）のバリューと、を含む情報である。なお、Ｄ＿ＩＤおよびＥ＿ＩＤの数は、各アプリケーションで利用されるデータの数に応じて決まり、任意に変更可能である。図６の例では、Ｄ＿ＩＤおよびＥ＿ＩＤは２つずつ設けられているが、これに限られるものではない。また、Ｄ＿ＩＤおよびＥ＿ＩＤの末尾に付された数字は対応関係を表し、Ｄ＿ＩＤ＿１とＥ＿ＩＤ＿１とは互いに対応し、Ｄ＿ＩＤ＿２とＥ＿ＩＤ＿２とは互いに対応するといった具合である。なお、例えばＤ＿ＩＤ＿１とＥ＿ＩＤ＿１とが互いに対応するとは、Ｅ＿ＩＤ＿１のバリューは、Ｄ＿ＩＤ＿１のバリューを、対応するアプリＩＤに対応付けられたグループＩＤに基づく暗号鍵で暗号化して得られた値であることを意味する。

【００２８】

図６の例では、アプリＩＤ「８５２」で識別されるアプリケーションは、顧客の名簿を管理するアプリケーションであり、Ｄ＿ＩＤ＿１は、暗号化されていない名前に対応する項目を表し、Ｅ＿ＩＤ＿１は、暗号化された名前に対応する項目を表す。つまり、Ｄ＿ＩＤ＿１のバリューは暗号化されていない名前を表し、Ｅ＿ＩＤ＿１のバリューは暗号化された名前を表す。また、Ｄ＿ＩＤ＿２は、暗号化されていない住所に対応する項目を表し、Ｅ＿ＩＤ＿２は、暗号化された住所に対応する項目を表す。つまり、Ｄ＿ＩＤ＿２のバリューは暗号化されていない住所を表し、Ｅ＿ＩＤ＿２のバリューは暗号化された住所を表す。なお、アプリデータに登録されるアプリＩＤ、Ｄ＿ＩＤ、および、Ｅ＿ＩＤの種類や数は任意であり、レコードごとに固有の形態を取り得る。本実施形態では、グループごとに、該グループで利用可能なアプリケーションで利用されるデータを管理するためのデータベースを個別に構築することは行わずに、各グループで利用可能な複数のアプリケーションの各々で利用されるデータをアプリデータ上で一括管理している。

【００２９】
なお、本実施形態のサーバ１０は、上述のアプリケーション対応情報と、上述のアプリデータとを個別に管理しているが、これに限らず、例えば上述のアプリケーション対応情報と上述のアプリデータとを統合した情報を管理する形態であってもよい。要するに、サーバ１０は、グループＩＤと、アプリＩＤと、暗号化されていない第１のデータと、グループＩＤに基づく暗号鍵で第１のデータを暗号化した第２のデータと、を対応付けた第１の対応情報を記憶する第１の記憶部を有する形態であればよい。本実施形態では、上述のアプリケーション対応情報を記憶するアプリ情報記憶部１０４と、上述のアプリデータを記憶するアプリデータ記憶部１０６との組み合わせが「第１の記憶部」として機能する。
【００３０】
図３に戻って説明を続ける。アプリデータ管理機能１０５は、要求受付部１２１と、登録部１２２と、更新部１２３と、選択部１２４と、暗号／復号部１２５と、送信部１２６と、を有する。
【００３１】
要求受付部１２１は、端末２０から各種の要求を受け付ける。詳しくは後述するが、要求受付部１２１は、第１のデータと、認証トークン（ユーザＩＤ）と、アプリＩＤと、を含み、かつ、新規のデータ登録を要求する新規登録要求を受け付けることもできる。また、要求受付部１２１は、１以上の第１のデータと、認証トークン（ユーザＩＤ）と、アプリＩＤと、レコードＩＤとを含み、かつ、レコードの更新を要求する更新要求を受け付けることもできる。さらに、要求受付部１２１は、検索用の文字列を示す検索文字列と、アプリＩＤとを少なくとも含む検索要求を受け付けることもできる。後述するように、ここでは、検索要求は認証トークン（ユーザＩＤ）をさらに含む。
【００３２】
なお、要求受付部１２１で各種の要求を受け付けた場合におけるアプリデータ管理機能１０５と認証機能１０１との間のやり取りや、アプリデータ管理機能１０５とアプリ情報管理機能１０３との間のやり取りについては後述する。
【００３３】
登録部１２２は、要求受付部１２１で上述の新規登録要求を受け付けた場合、該新規登録要求に含まれる第１のデータと、該新規登録要求に含まれるアプリＩＤに対応付けられたグループＩＤに基づく暗号鍵で該第１のデータを暗号化した第２のデータと、新たに発行するレコードＩＤとを対応付けた情報を、新たなレコードとしてアプリデータ（第３の対応情報）に登録する。登録部１２２の詳細な動作については後述する。
【００３４】
更新部１２３は、要求受付部１２１で上述の更新要求を受け付けた場合、該更新要求に含まれるレコードＩＤで識別されるレコードに含まれる第１のデータを、該更新要求に含まれる第１のデータに更新するとともに、該レコードに含まれる第２のデータを、更新要求に含まれるアプリＩＤに対応付けられたグループＩＤに基づく暗号鍵で該更新後の第１のデータを暗号化した第２のデータに更新する。更新部１２３の詳細な動作については後述する。
【００３５】
選択部１２４は、要求受付部１２１で上述の検索要求を受け付けた場合、該検索要求に含まれるアプリＩＤと、該検索要求に含まれる検索文字列と一致する第１のデータとの組み合わせに対応する第２のデータを選択する。より具体的には、選択部１２４は、アプリデータの中から、検索要求に含まれるアプリＩＤと、該検索要求に含まれる検索文字列と一致する第１のデータとを含む１以上のレコードを選択し、該選択した１以上のレコードに含まれる第２のデータ（全ての第２のデータ）を選択する。選択部１２４の詳細な動作については後述する。
【００３６】
暗号／復号部１２５は、登録部１２２、更新部１２３、および、選択部１２４の各々の要求に応じて、データの暗号化または復号を行う。ここでは、暗号／復号部１２５は、「

復号部」の一例であり、選択部１２４により選択された第２のデータを、対応するグループ識別情報に基づく暗号鍵で復号する機能を有している。詳しくは後述するが、アプリデータ管理機能１０５は、アプリ情報管理機能１０３のグループＩＤ取得部１１４に対して、要求受付部１２１で受け付けた上述の検索要求に含まれるアプリＩＤに対応付けられたグループＩＤを取得させる。そして、暗号／復号部１２５は、選択部１２４により選択された第２のデータを、グループＩＤ取得部１１４により取得されたグループＩＤに基づく暗号鍵で復号する。暗号／復号部１２５の詳細な動作については後述する。

【００３７】

送信部１２６は、検索要求に対する応答として、暗号／復号部１２５で復号されたデータを送信する。

【００３８】

次に、図７を用いて、ユーザが認証されてから該ユーザが選択したアプリケーションに対応する画面が端末２０に表示されるまでのシステム１００の動作手順の一例を説明する。端末２０は、ユーザの操作に応じて、クラウドサービスの提供を受ける権限を有する者として認証を受けるためのログイン画面を表示する（ステップＳ１）。図８は、ログイン画面の一例を示す図である。図８の例では、認証処理に用いられるユーザＩＤとパスワードを入力するための領域と、認証処理の開始を要求するためのログインボタンとが表示されているが、これに限られるものではない。

【００３９】

図７の説明を続ける。ログイン画面上でのユーザＩＤとパスワードの入力後、ログインボタンの押下を受け付けると、端末２０は、その入力されたユーザＩＤとパスワードを含み、かつ、ユーザの認証を要求する認証要求をサーバ１０へ送信する（ステップＳ２）。認証要求を受信したサーバ１０の認証機能１０１は、ユーザ情報記憶部１０２に記憶された複数のユーザ情報（ユーザＩＤとパスワードの組み合わせ）の中に、認証要求に含まれるユーザＩＤとパスワードの組み合わせと一致するユーザ情報が存在するか否かを判断する認証処理を行う（ステップＳ３）。説明の便宜上、以下では、ステップＳ３の認証処理の結果が肯定であった場合（ユーザが認証された場合）を例に挙げて説明する。ステップＳ３の認証処理の結果が肯定の場合、認証機能１０１は、認証トークンを発行（生成）する。この例では、認証トークンは、認証するたびに発行される一意なキーを示すワンタイムキーと、認証されたユーザのユーザＩＤとを含む情報を暗号化した情報である。認証機能１０１は、発行済みの認証トークンの管理も行う。

【００４０】

次に、認証機能１０１は、アプリ情報管理機能１０３に対して、認証したユーザのユーザＩＤを渡し、該ユーザＩＤで識別されるユーザが利用可能なアプリケーションのリストを要求する（ステップＳ４）。この要求を受けたリスト作成部１１１は、リストを作成する（ステップＳ５）。より具体的には、リスト作成部１１１は、上述のユーザ対応情報（図４）を参照して、認証されたユーザのユーザＩＤに対応するグループＩＤを特定する。そして、リスト作成部１１１は、上述のアプリケーション対応情報（図５）を参照して、特定したグループＩＤに対応する全てのアプリＩＤを特定する。このようにして特定したアプリＩＤで識別されるアプリケーションが、認証されたユーザが利用可能なアプリケーションとなる。リスト作成部１１１は、アプリ情報記憶部１０４に記憶されたアプリ情報を用いて、認証されたユーザが利用可能なアプリケーションごとに、アプリＩＤと該アプリケーションの名前とを少なくとも含むリストを作成する。

【００４１】

リスト作成部１１１は、ステップＳ５で作成したリストを認証機能１０１へ返信する（ステップＳ６）。認証機能１０１は、ステップＳ３で発行した認証トークンと、リスト作成部１１１から受信したリストと、を端末２０へ送信する（ステップＳ７）。そして、端末２０は、サーバ１０から受信したリストに基づき、図９に示すような初期画面を表示する（ステップＳ８）。図９の例では、初期画面は、アプリケーションの作成等を行うための第１の画面と、リストに基づくアプリケーションの一覧を表示する第２の画面とを含む

が、これに限られるものではない。

【００４２】

図７の説明を続ける。初期画面（この例では第２の画面）から何れかのアプリケーションを選択する入力を受け付けると、端末２０は、その選択されたアプリケーションのアプリＩＤと、サーバ１０から受信済みの認証トークンとを含み、かつ、該アプリケーションの定義データを要求する定義データ要求を、サーバ１０へ送信する（ステップＳ９）。

【００４３】

定義データ要求を受け付けた定義データ作成部１１２は、認証機能１０１に対して、その定義データ要求に含まれる認証トークンを渡し、該認証トークンの確認を依頼する（ステップＳ１０）。認証機能１０１は、定義データ作成部１１２から受け取った認証トークンを復号し、復号したワンタイムキーとユーザＩＤとの組み合わせが発行済みのものであるか否かを確認する（ステップＳ１１）。説明の便宜上、以下では、ステップＳ１１の確認の結果が肯定であった場合を例に挙げて説明する。認証機能１０１は、復号した認証トークンの中からユーザＩＤを取り出し、その取り出したユーザＩＤを定義データ作成部１１２へ送信する（ステップＳ１２）。

【００４４】

次に、定義データ作成部１１２は、判断部１１３に対して、認証機能１０１から受信したユーザＩＤと、定義データ要求に含まれるアプリＩＤとを渡し、該ユーザＩＤで識別されるユーザは該アプリＩＤで識別されるアプリケーションを利用することができるか否かの判断を要求する（ステップＳ１３）。この要求を受けた判断部１１３は、定義データ作成部１１２から渡されたユーザＩＤとアプリＩＤを用いて、該ユーザＩＤで識別されるユーザは該アプリＩＤで識別されるアプリケーションを利用することができるか否かを判断する（ステップＳ１４）。より具体的には、判断部１１３は、ユーザ対応情報（図４）を参照して、定義データ作成部１１２から渡されたユーザＩＤに対応するグループＩＤを特定する。そして、アプリケーション対応情報（図５）を参照して、特定したグループＩＤに対応する１以上のアプリＩＤを特定し、その特定したアプリＩＤの中に、定義データ作成部１１２から渡されたアプリＩＤが存在するか否かを判断する。この判断結果が肯定の場合、定義データ作成部１１２から渡されたユーザＩＤで識別されるユーザは、定義データ作成部１１２から渡されたアプリＩＤで識別されるアプリケーションを利用することができると判断されることになる。

【００４５】

説明の便宜上、以下では、ステップＳ１４の判断結果が肯定であった場合を例に挙げて説明する。判断部１１３は、ステップＳ１４の判断結果を定義データ作成部１１２へ送信する（ステップＳ１５）。この判断結果（ここでは肯定の判断結果）を受け取った定義データ作成部１１２は、アプリ情報記憶部１０４に記憶されたアプリ情報を用いて、定義データ要求に含まれるアプリＩＤで識別されるアプリケーションの定義データを作成し（ステップＳ１６）、作成した定義データを端末２０へ送信する（ステップＳ１７）。この定義データを受信した端末２０は、その受信した定義データに基づく画面（アプリケーションに対応する画面）を作成し、作成した画面を表示する（ステップＳ１８）。

【００４６】

次に、図１０を用いて、認証済みのユーザ（ログイン中のユーザ）が、何れかのアプリケーションで利用されるデータとして新たなデータ（この例ではレコード単位のデータ）を登録する操作を行った場合におけるシステム１００の動作手順の一例を説明する。

【００４７】

まず、認証済みのユーザは、何れかのアプリケーションに対応する画面から、新たなレコードを追加するためのレコード追加画面を呼び出す操作を行い、該レコード追加画面から、各項目に対応するバリューを新たに追加する操作を行った後、データの新規登録を要求する操作を行う。例えば顧客の名簿を管理するアプリケーションの場合、ユーザは、図１１のようなレコード追加画面から、「名前」および「住所」の各々の項目に対応するバリューを入力する操作を行った後、登録ボタンを押下する操作を行うこともできる。この

操作を受け付けた端末１０は、入力されたデータ（それぞれが項目とバリューの組からなる１以上の第１のデータ）と、サーバ１０から取得済みの認証トークン（ユーザＩＤを含む）と、アプリＩＤ（上記何れかのアプリケーションのアプリＩＤ）と、を含む上述の新規登録要求をサーバ１０へ送信する（ステップＳ２１）。

【００４８】

上述の新規登録要求を受け付けたサーバ１０の要求受付部１２１は、認証機能１０１に対して、その新規登録要求に含まれる認証トークンを渡し、該認証トークンの確認を依頼する（ステップＳ２２）。認証機能１０１は、要求受付部１２１から受け取った認証トークンを復号し、復号したワンタイムキーとユーザＩＤとの組み合わせが発行済みのものであるか否かを確認する（ステップＳ２３）。説明の便宜上、以下では、ステップＳ２３の確認の結果が肯定であった場合を例に挙げて説明する。認証機能１０１は、復号した認証トークンの中からユーザＩＤを取り出し、その取り出したユーザＩＤを要求受付部１２１へ送信する（ステップＳ２４）。

【００４９】

次に、要求受付部１２１は、判断部１１３に対して、認証機能１０１から受信したユーザＩＤと、新規登録要求に含まれるアプリＩＤとを渡し、該ユーザＩＤで識別されるユーザは該アプリＩＤで識別されるアプリケーションを利用することができるか否かの判断を要求する（ステップＳ２５）。この要求を受けた判断部１１３は、要求受付部１２１から渡されたユーザＩＤとアプリＩＤを用いて、該ユーザＩＤで識別されるユーザは該アプリＩＤで識別されるアプリケーションを利用することができるか否かを判断する（ステップＳ２６）。この処理内容は図７に示すステップＳ１４の処理内容と同様である。

【００５０】

説明の便宜上、以下では、ステップＳ２６の判断結果が肯定であった場合を例に挙げて説明する。判断部１１３は、ステップＳ２６の判断結果を要求受付部１２１へ送信する（ステップＳ２７）。この判断結果（ここでは肯定の判断結果）を受け取った要求受付部１２１は、グループＩＤ取得部１１４に対して、ステップＳ２１で受け付けた新規登録要求に含まれるアプリＩＤを渡し、該アプリＩＤに対応するグループＩＤを要求する（ステップＳ２８）。この要求を受けたグループＩＤ取得部１１４は、アプリケーション対応情報を参照して、要求受付部１２１から受け取ったアプリＩＤに対応するグループＩＤを取得する（ステップＳ２９）。そして、グループＩＤ取得部１１４は、その取得したグループＩＤを要求受付部１２１へ送信する（ステップＳ３０）。

【００５１】

次に、要求受付部１２１は、ステップＳ２１で受け付けた新規登録要求に含まれるアプリＩＤおよび第１のデータと、ステップＳ３０で取得したグループＩＤとを登録部１２２へ渡し、データの登録を要求する（ステップＳ３１）。この要求を受けた登録部１２２は、暗号／復号部１２５に対して、要求受付部１２１から受け取ったグループＩＤと第１のデータとを渡し、該第１のデータの暗号化を要求する（ステップＳ３２）。この要求を受けた暗号／復号部１２５は、登録部１２２から受け取ったグループＩＤに基づく暗号鍵で第１のデータを暗号化して第２のデータを生成する（ステップＳ３３）。新規登録要求に含まれる第１のデータが複数存在する場合は、複数の第１のデータと１対１に対応する複数の第２のデータが生成されることになる。

【００５２】

ステップＳ３３の後、暗号／復号部１２５は、ステップＳ３３で生成した第２のデータを登録部１２２へ送信する（ステップＳ３４）。次に、登録部１２２は、新たなレコードＩＤを発行し、該発行したレコードＩＤに対して、要求受付部１２１から渡されたアプリＩＤおよび第１のデータと、暗号／復号部１２５から渡された第２のデータとを対応付けたレコードを、新たなレコードとしてアプリデータに登録する（ステップＳ３５）。

【００５３】

次に、図１２を用いて、認証済みのユーザ（ログイン中のユーザ）が、何れかのアプリケーションで利用されるデータとして登録済みのデータ（この例ではレコード単位のデー

タ）を更新する場合のシステム１００の動作手順の一例を説明する。
【００５４】
まず、認証済みのユーザは、何れかのアプリケーションに対応する画面から、所望のレコードに対応する各項目のバリュー（登録済みのバリュー）を変更（修正）するための変更画面を呼び出す操作を行い、該変更画面から、各項目のバリューを変更する操作を行った後、データの更新を要求する操作を行う。例えば顧客の名簿を管理するアプリケーションの場合、ユーザは、図１３のような変更画面から、「名前」および「住所」の各々の項目に対応するバリューを変更する操作を行った後、更新ボタンを押下する操作を行うこともできる。この操作を受け付けた端末１０は、入力されたデータ（第１のデータ）と、変更対象のレコードを識別するレコードＩＤと、サーバ１０から取得済みの認証トークン（ユーザＩＤを含む）と、アプリＩＤ（上記何れかのアプリケーションのアプリＩＤ）と、を含む上述の更新要求をサーバ１０へ送信する（ステップＳ４１）。
【００５５】
ステップＳ４２～ステップＳ５０の処理内容は、図１０に示すステップＳ２２～ステップＳ３０の処理内容と同様であるので、詳細な説明は省略する。ステップＳ５０の後、要求受付部１２１は、ステップＳ４１で受け付けた更新要求に含まれるレコードＩＤ、アプリＩＤおよび第１のデータと、ステップＳ５０で取得したグループＩＤとを更新部１２３へ渡し、データの更新を要求する（ステップＳ５１）。ステップＳ５２～ステップＳ５４の処理内容は、図１０に示すステップＳ３２～ステップＳ３４の処理内容と同様であるので詳細な説明は省略する。ステップＳ５４の後、更新部１２３は、アプリデータに含まれるレコードのうち、要求受付部１２１から渡されたレコードＩＤに対応するレコードを選択し、該選択したレコードを、要求受付部１２１から渡されたレコードＩＤ、アプリＩＤおよび第１のデータと、暗号／復号部１２５から渡された第２のデータとを対応付けたレコードに更新する（ステップＳ５５）。具体的には、既存のレコード内の各バリューを、要求受付部１２１から渡された第１のデータ内の対応するバリュー、または、暗号／復号部１２５から渡された第２のデータ内の対応するバリューに更新するという具合である。
【００５６】
次に、図１４を用いて、認証済みのユーザ（ログイン中のユーザ）が、何れかのアプリケーションで利用されるデータを検索する操作を行った場合におけるシステム１００の動作手順の一例を説明する。
【００５７】
まず、認証済みのユーザは、何れかのアプリケーションに対応する画面から、データを検索するためのデータ検索画面を呼び出す操作を行い、該データ検索画面から、検索文字列を入力する操作を行った後、データの検索を要求する操作を行う。例えばユーザは、図１５のようなデータ検索画面から、検索文字列を入力する操作を行った後、検索ボタンを押下する操作を行うこともできる。この操作を受け付けた端末１０は、入力された検索文字列と、サーバ１０から取得済みの認証トークン（ユーザＩＤを含む）と、アプリＩＤ（上記何れかのアプリケーションのアプリＩＤ）と、を含む上述の検索要求をサーバ１０へ送信する（ステップＳ６１）。
【００５８】
ステップＳ６２～ステップＳ７０の処理内容は、図１０に示すステップＳ２２～ステップＳ３０の処理内容と同様であるので、詳細な説明は省略する。ステップＳ７０の後、要求受付部１２１は、ステップＳ６１で受け付けた検索要求に含まれる検索文字列およびアプリＩＤと、ステップＳ７０で取得したグループＩＤとを選択部１２４へ渡し、データの検索を要求する（ステップＳ７１）。この要求を受けた選択部１２４は、アプリデータの中から、ステップＳ７１で受け取ったアプリＩＤと、ステップＳ７１で受け取った検索文字列と一致する第１のデータとの組み合わせに対応する第２のデータを選択する（ステップＳ７２）。より具体的には、選択部１２４は、アプリデータの中から、ステップＳ７１で受け取ったアプリＩＤと、ステップＳ７１で受け取った検索文字列と一致するバリュー（暗号化されていないバリュー）と、を含む全てのレコードを選択し、該選択したレコー

ドに含まれる第２のデータ（ここでは、暗号化されたバリューが第２のデータに相当）を選択する。

【００５９】

次に、選択部１２４は、暗号／復号部１２５に対して、ステップＳ７１で受け取ったグループＩＤと、ステップＳ７２で選択した第２のデータ（１つとは限らず、複数の場合も当然にあり得る）とを渡し、該第２のデータの復号を要求する（ステップＳ７３）。この要求を受けた暗号／復号部１２５は、選択部１２４から受け取ったグループＩＤに基づく暗号鍵で、選択部１２４から受け取った第２のデータを復号する（ステップＳ７４）。そして、暗号／復号部１２５は、復号したデータを選択部１２４へ渡す（ステップＳ７５）。次に、選択部１２４は、復号したデータを送信部１２６へ渡し、端末２０への送信を依頼する（ステップＳ７６）。この依頼を受けた送信部１２６は、復号したデータを端末２０へ送信する（ステップＳ７７）。検索要求の応答として、復号したデータを受信した端末２０は、その受信したデータを検索結果として表示する（ステップＳ７８）。

【００６０】

以上に説明したように、本実施形態のサーバ１０は、グループごとにデータベースを個別に構築することなく、グループＩＤと、アプリＩＤと、第１のデータと、グループＩＤに基づく暗号鍵で第１のデータを暗号化した第２のデータと、を対応付けて一括管理（上述の実施形態では、アプリケーション対応情報とアプリデータとの組み合わせにより一括管理）する。これにより、データ管理が容易になる。また、本実施形態のサーバ１０は、検索文字列と、アプリＩＤとを含む上述の検索要求を受け付けた場合、該検索要求に含まれるアプリＩＤと、該検索要求に含まれる検索文字列と一致する第１のデータと、の組み合わせに対応する第２のデータを選択する。そして、サーバ１０は、その選択した第２のデータを、対応するグループＩＤに基づく暗号鍵で復号し、その復号したデータのみを検索結果として端末２０へ返す。すなわち、本実施形態では、復号したデータのみを検索結果として返すので、正常に復号されない限り、暗号化されていないデータが外部に漏洩することはない。以上より、本実施形態によれば、データ管理を容易にしつつ情報の漏洩リスクを低減することができる。

【００６１】

以上、本発明に係る実施形態について説明したが、本発明は、上述の実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上述の実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態および変形例にわたる構成要素を適宜組み合わせてもよい。

【００６２】

上述の実施形態では、図３に示す各機能を有するサーバ１０は１台で構成されているが、これに限らず、例えば図３に示す各機能が複数の情報処理装置に分散して搭載される形態であってもよい。要するに、複数の情報処理装置群から構成される情報処理システムが、図３に示す各機能を有する形態であってもよい。

【００６３】

また、上述の情報処理システム１００で実行されるプログラム（ＣＰＵ１１が実行するプログラム）は、インストール可能な形式または実行可能な形式のファイルでＣＤ－ＲＯＭ、フレキシブルディスク（ＦＤ）、ＣＤ－Ｒ、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｋ）、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）等のコンピュータで読み取り可能な記録媒体に記録して提供するように構成してもよいし、インターネット等のネットワーク経由で提供または配布するように構成してもよい。また、各種プログラムを、ＲＯＭ等に予め組み込んで提供するように構成してもよい。

【符号の説明】

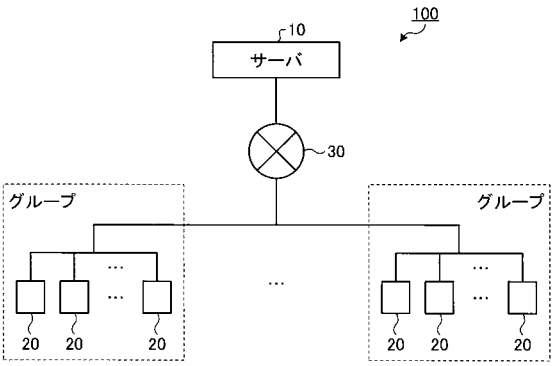
【００６４】

１０　サーバ

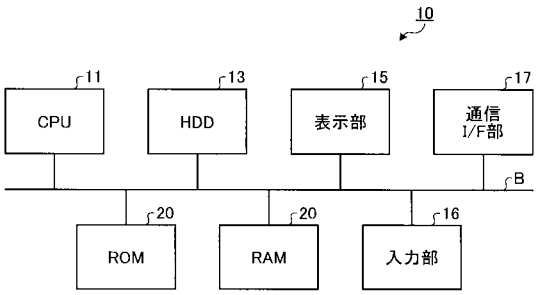
２０　端末
３０　ネットワーク
１００　システム
１０１　認証機能
１０２　ユーザ情報記憶部
１０３　アプリ情報管理機能
１０４　アプリ情報記憶部
１０５　アプリデータ管理機能
１０６　アプリデータ記憶部
１１１　リスト作成部
１１２　定義データ作成部
１１３　判断部
１１４　グループＩＤ取得部
１２１　要求受付部
１２２　登録部
１２３　更新部
１２４　選択部
１２５　暗号／復号部
１２６　送信部

【先行技術文献】
【特許文献】
【００６５】
【特許文献１】特開２０１４－２７４９２号公報

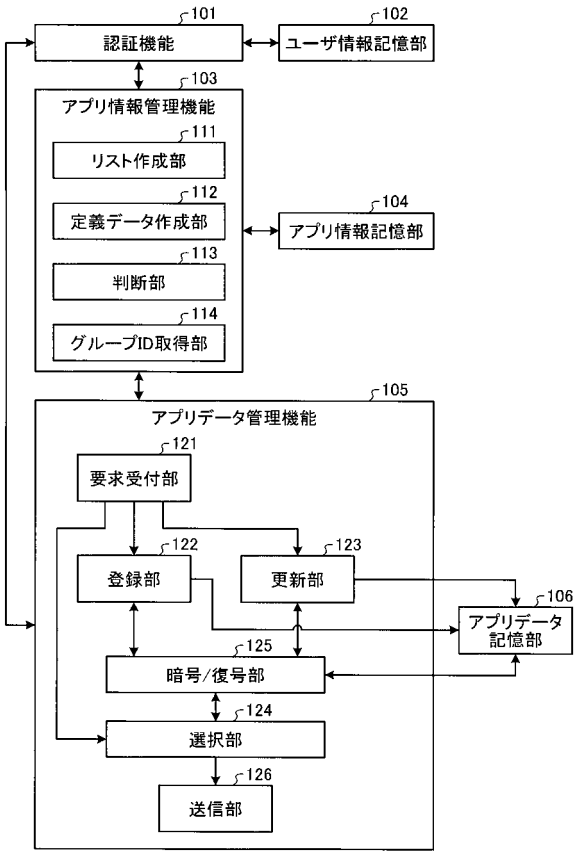
【図１】



【図２】



【図３】



【図４】

ユーザID	グループID
X12	AAA
X13	AAA
X15	AAA
Z12	BBB
Z13	BBB
Y11	CCC
⋮	⋮

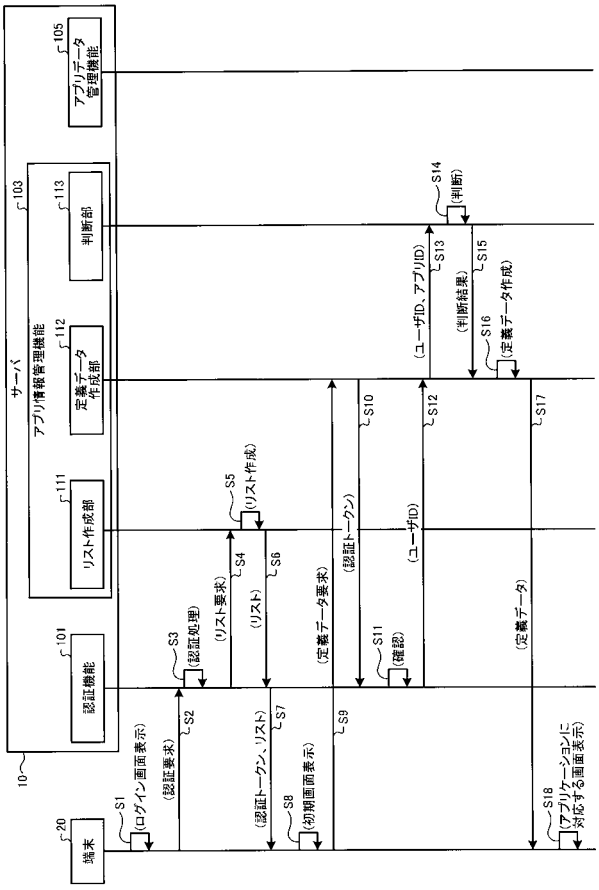
【図５】

アプリID	グループID
852	AAA
159	BBB
357	CCC
⋮	⋮

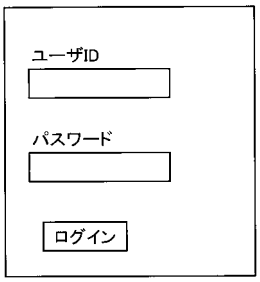
【図６】

	レコードID	アプリID	D_ID_1	E_ID_1	D_ID_2	E_ID_2
レコード	001	852	鈴木	xxxxx	東京	yyyyy
レコード	002	852	加藤	aaaaa	神奈川	bbbbb
レコード	003	852	山田	wwwww	埼玉	kkkkk

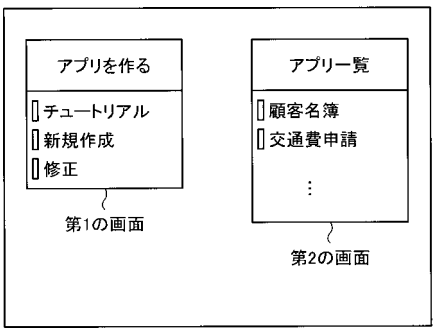
【図７】



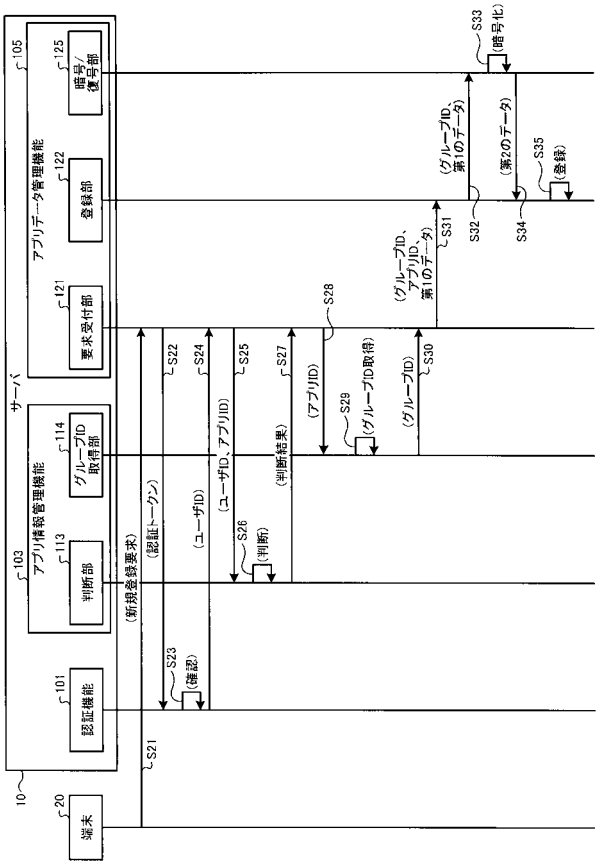
【図８】



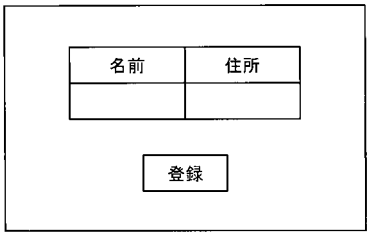
【図９】



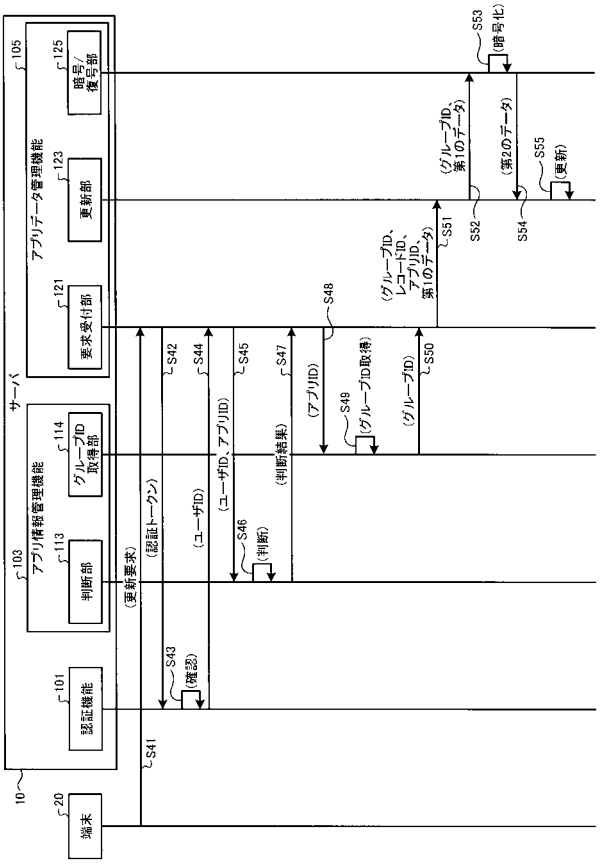
【図１０】



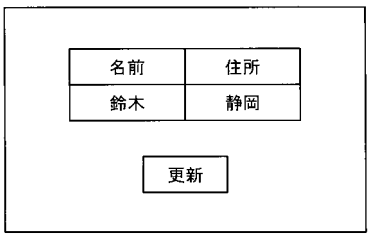
【図１１】



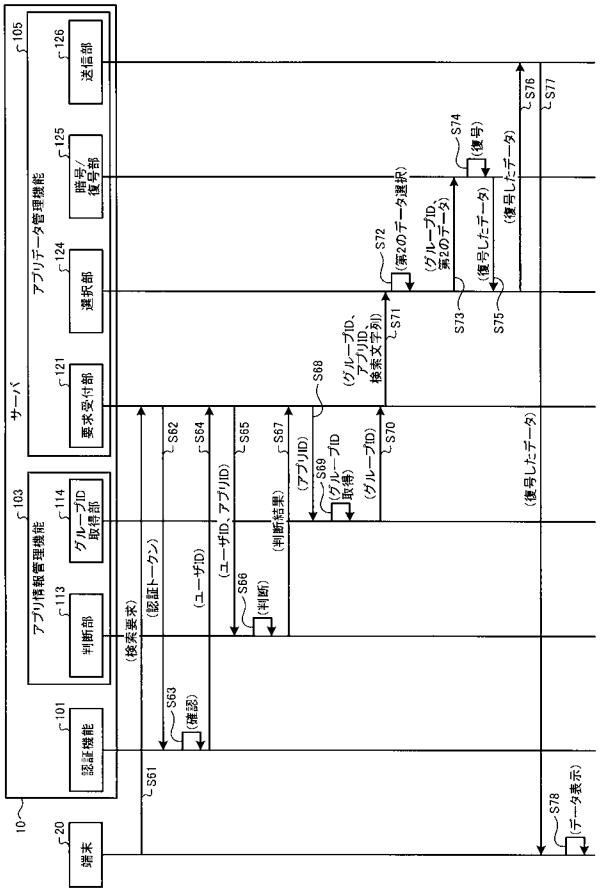
【図１２】



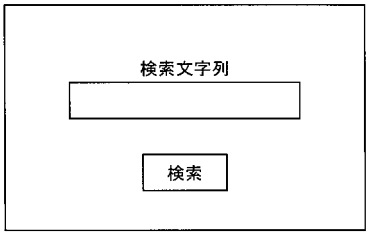
【図１３】



【図１４】


サーバ
10
端末
20
認証機能
101
アプリ情報管理機能
103
判断部
113
グループID取得部
114
アプリデータ管理機能
105
要求受付部
121
選択部
124
暗号/復号部
125
送信部
126
(検索要求)
(認証トークン)
(確認)
(ユーザID)
(ユーザID、アプリID)
(判断結果)
(判断)
(アプリID)
(グループID取得)
(グループID)
(グループID、アプリID、検索文字列)
(第2のデータ選択)
(グループID、第2のデータ)
(復号)
(復号したデータ)
(復号したデータ)
(データ表示)
S61
S62
S63
S64
S65
S66
S67
S68
S69
S70
S71
S72
S73
S74
S75
S76
S77
S78

【図１５】


検索文字列
検索