(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2011-19129
(P2011-19129A)
(43)公開日　平成23年1月27日(2011.1.27)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601A	5B017
H04L 9/14	(2006.01)	H04L	9/00	641	5B285
G06F 21/20	(2006.01)	G06F	15/00	330A	5J104
G06F 21/24	(2006.01)	G06F	12/14	520A	
		G06F	12/14	540P	

審査請求 未請求　請求項の数 20　ＯＬ　（全 23 頁）　最終頁に続く

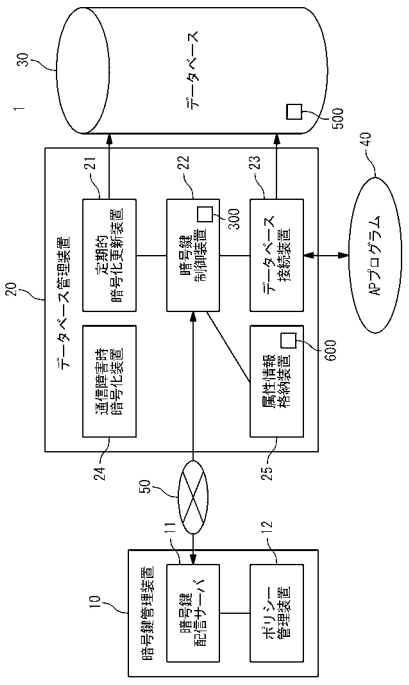
(21)出願番号　特願2009-163031 (P2009-163031)
(22)出願日　平成21年7月9日 (2009.7.9)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100102864
弁理士　工藤　実
(72)発明者　藤尾　秀洋
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B017 AA03 BA06 BA07 CA16
5B285 AA04 BA07 CA06 CA17 CA42
5J104 AA16 AA32 AA34 EA04 EA15
EA16 JA03 NA02 NA27 NA37
PA14

(54)【発明の名称】データ管理システム及びデータ管理方法

(57)【要約】
【課題】預託された秘密情報を二次利用するＳａａＳ事業者等に対し、預託側のポリシーで設定されるアクセス制御を実現し、秘匿制御を預託側で行う。
【解決手段】データ管理システムは、データベース３０とデータベース管理装置２０と暗号鍵管理装置１０とを具備する。データベース３０は、預託者が預託し、第１暗号鍵で暗号化された秘密情報を保持する。データベース管理装置２０は、第１暗号鍵を保持しているとき、アプリケーションプログラム４０の要求に応答し、データベース３０の秘密情報を第１暗号鍵で復号化して提供する。暗号鍵管理装置１０は、預託者のポリシーに基づき、第２暗号鍵を生成してデータベース管理装置２０に配信する。データベース管理装置２０は、秘密情報を第１暗号鍵で復号化し、第２暗号鍵で再暗号化してデータベース３０に格納する。データベース管理装置２０は、第１暗号鍵を削除し、第２暗号鍵を保持しないか又は秘匿する。
【選択図】図１



【特許請求の範囲】
【請求項１】
預託者が預託し、第１暗号鍵で暗号化された秘密情報を保持するデータベースと、
前記第１暗号鍵を保持しているとき、アプリケーションプログラムの要求に応答して、前記データベースの前記秘密情報を前記第１暗号鍵で復号化して提供するデータベース管理装置と、
前記預託者による前記秘密情報の開示に関するポリシーに基づいて、第２暗号鍵を生成して前記データベース管理装置に配信する暗号鍵管理装置と
を具備し、
前記データベース管理装置は、前記データベースの前記秘密情報を前記第１暗号鍵で復号化し、前記第２暗号鍵で再暗号化して前記データベースに格納し、
前記データベース管理装置は、前記第２暗号鍵で前記秘密情報が再暗号化された後、前記第１暗号鍵を削除し、前記第２暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記第２暗号鍵を秘匿する
データ管理システム。
【請求項２】
請求項１に記載のデータ管理システムにおいて、
前記データベース管理装置は、前記アプリケーションプログラムの要求に応答して前記秘密情報を前記第２暗号鍵で復号化するとき、前記第２暗号鍵を保持していないか、又は前記第２暗号鍵を秘匿している場合、前記暗号鍵管理装置へ前記第２暗号鍵を要求し、
前記暗号鍵管理装置は、前記要求に応答して、前記ポリシーが許可する場合、前記第２暗号鍵を抽出して、当該許可の条件と共に前記データベース管理装置へ出力し、
前記データベース管理装置は、前記データベースの前記秘密情報を前記第２暗号鍵で復号化して提供し、前記許可の条件の範囲で前記第２暗号鍵を保持する
データ管理システム。
【請求項３】
請求項１に記載のデータ管理システムにおいて、
前記暗号鍵管理装置は、前記ポリシーで設定された更新時期が来たとき、新たな暗号鍵を生成して前記データベース管理装置に配信し、
前記データベース管理装置は、前記データベースの前記秘密情報を前記第２暗号鍵で復号化し、前記新たな暗号鍵で再暗号化して前記データベースに格納し、
前記データベース管理装置は、前記新たな暗号鍵で前記秘密情報が再暗号化された後、前記第２暗号鍵を削除し、前記新たな暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記新たな暗号鍵を秘匿する
データ管理システム。
【請求項４】
請求項１記載のデータ管理システムにおいて、
前記データベース管理装置は、前記秘密情報を暗号化するときに使用した暗号鍵を保持するとき、複数の預託者の各々毎に暗号鍵を保持する
データ管理システム。
【請求項５】
請求項１乃至４のいずれか一項に記載のデータ管理システムにおいて、
前記秘密情報の開示が中断されるとき、
前記暗号鍵管理装置は、第３暗号鍵を生成し、前記第２暗号鍵と共に出力し、
前記データベース管理装置は、前記データベースの前記秘密情報を前記第２暗号鍵で復号化し、前記第３暗号鍵で再暗号化して前記データベースに格納し、前記第３暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記第３暗号鍵を秘匿する
データ管理システム。
【請求項６】

請求項１記載のデータ管理システムにおいて、
前記データベース管理装置と前記暗号鍵管理装置との通信が途絶した場合、予め配備された前記預託者の公開鍵に基づいて前記秘密情報を暗号化することにより、前記秘密情報の漏洩を防ぐ
データ管理システム。
【請求項７】
預託者が預託し、暗号鍵で暗号化された秘密情報を保持するデータベースを管理するデータベース管理装置であって、
秘密情報の暗号化に用いた第１暗号鍵を保持する暗号鍵制御装置と、
アプリケーションプログラムの要求に応答して、前記データベースの前記秘密情報を前記第１暗号鍵で復号化して提供するデータベース接続装置と、
前記データベースの前記秘密情報を前記第１暗号鍵で復号化し、その後、前記預託者による前記秘密情報の開示に関するポリシーに基づいて暗号鍵管理装置が生成した第２暗号鍵で、復号化された前記秘密情報を再暗号化して、前記データベースに格納する定期的暗号化更新装置と
を備え、
前記暗号鍵制御装置は、前記第２暗号鍵で前記秘密情報が再暗号化された後、前記第１暗号鍵を削除し、前記第２暗号鍵を保持しないか、又は、前記データベース接続装置に対して前記第２暗号鍵を秘匿する
データベース管理装置。
【請求項８】
請求項７に記載のデータベース管理装置において、
前記暗号鍵制御装置は、
前記アプリケーションプログラムの要求に応答して前記秘密情報を前記第２暗号鍵で復号化するとき、前記第２暗号鍵を保持していないか、又は前記第２暗号鍵を秘匿している場合、前記暗号鍵管理装置へ前記第２暗号鍵を要求し、
前記暗号鍵管理装置が前記要求に応答して前記ポリシーが許可する場合に抽出し前記第２暗号鍵を、当該許可の条件と共に受信し、
前記データベース接続装置は、前記データベースの前記秘密情報を前記第２暗号鍵で復号化して提供し、
前記暗号鍵制御装置は、前記許可の条件の範囲で前記第２暗号鍵を保持する
データベース管理装置。
【請求項９】
請求項７に記載のデータ管理装置において、
前記暗号鍵制御装置は、前記暗号鍵管理装置が前記ポリシーで設定された更新時期が来たとき、生成して配信してきた新たな暗号鍵を受信し、
前記定期的暗号化更新装置は、前記データベースの前記秘密情報を前記第２暗号鍵で復号化し、前記新たな暗号鍵で再暗号化して前記データベースに格納し、
前記暗号鍵制御装置は、前記新たな暗号鍵で前記秘密情報が再暗号化された後、前記第２暗号鍵を削除し、前記新たな暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記新たな暗号鍵を秘匿する
データ管理装置。
【請求項１０】
請求項７乃至９のいずれか一項に記載のデータベース管理装置において、
前記秘密情報の開示が中断されるとき、
前記暗号鍵制御装置は、前記暗号鍵管理装置が生成した第３暗号鍵を前記第２暗号鍵と共に受信し、
前記定期的暗号化更新装置は、前記データベースの前記秘密情報を前記第２暗号鍵で復号化し、前記第３暗号鍵で再暗号化して前記データベースに格納し、
前記暗号鍵制御装置は、前記第３暗号鍵を保持しないか、又は、前記アプリケーショ

ンプログラムに対して前記第３暗号鍵を秘匿する
データベース管理装置。
【請求項１１】
請求項７記載のデータベース管理装置において、
前記暗号鍵制御装置と前記暗号鍵管理装置との通信が途絶した場合、予め配備された前記預託者の公開鍵に基づいて前記秘密情報を暗号化することにより、前記秘密情報の漏洩を防ぐ
データベース管理装置。
【請求項１２】
預託者が預託し、第１暗号鍵で暗号化された秘密情報をデータベースに保持するステップと、
アプリケーションプログラムの要求に応答して、前記データベースの前記秘密情報を前記第１暗号鍵で復号化するステップと、
前記預託者による前記秘密情報の開示に関するポリシーに基づいて、第２暗号鍵を生成するステップと、
前記データベースの前記秘密情報を前記第１暗号鍵で復号化し、前記第２暗号鍵で再暗号化するステップと、
再暗号化された前記秘密情報を前記データベースに格納するステップと、
前記第２暗号鍵で前記秘密情報が再暗号化された後、前記第１暗号鍵を削除し、前記第２暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記第２暗号鍵を秘匿するステップと
を具備する
データ管理方法。
【請求項１３】
請求項１２に記載のデータ管理方法において、
前記アプリケーションプログラムの要求に応答して前記秘密情報を前記第２暗号鍵で復号化するとき、前記第２暗号鍵を保持していないか、又は前記第２暗号鍵を秘匿している場合、前記第２暗号鍵を要求するステップと、
前記要求に応答して、前記ポリシーが許可する場合、前記第２暗号鍵を抽出して、当該許可の条件と共に出力するステップと
を更に具備する
データ管理方法。
【請求項１４】
請求項１２に記載のデータ管理方法において、
前記ポリシーで設定された更新時期が来たとき、新たな暗号鍵を生成するステップと、
前記データベースの前記秘密情報を前記第２暗号鍵で復号化し、前記新たな暗号鍵で再暗号化するステップと、
再暗号化された前記秘密情報を前記データベースに格納するステップと、
前記新たな暗号鍵で前記秘密情報が再暗号化された後、前記第２暗号鍵を削除し、前記新たな暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記新たな暗号鍵を秘匿するステップと
を更に具備する
データ管理方法。
【請求項１５】
請求項１２乃至１４のいずれか一項に記載のデータ管理方法において、
前記秘密情報の開示が中断されるとき、第３暗号鍵を生成し、前記第２暗号鍵と共に出力するステップと、
前記データベースの前記秘密情報を前記第２暗号鍵で復号化し、前記第３暗号鍵で再暗号化するステップと、
再暗号化された前記秘密情報を前記データベースに格納するステップと、

前記第３暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記第３暗号鍵を秘匿するステップと
を更に具備する
データ管理方法。
【請求項１６】
預託者が預託し、暗号鍵で暗号化された秘密情報を保持するデータベースを管理するデータベース管理方法をコンピュータに実行させるプログラムであって、
秘密情報の暗号化に用いた第１前記暗号鍵を保持するステップと、
アプリケーションプログラムの要求に応答して、前記データベースの前記秘密情報を前記第１暗号鍵で復号化して提供するステップと、
前記データベースの前記秘密情報を前記第１暗号鍵で復号化し、その後、前記預託者による前記秘密情報の開示に関するポリシーに基づいて暗号鍵管理装置が生成した第２暗号鍵で、復号化された前記秘密情報を再暗号化するステップと、
再暗号化された前記秘密情報を前記データベースに格納するステップと、
前記第２暗号鍵で前記秘密情報が再暗号化された後、前記第１暗号鍵を削除し、前記第２暗号鍵を保持しないか、又は、前記データベース接続装置に対して前記第２暗号鍵を秘匿するステップと
を具備するデータベース管理方法をコンピュータに実行させるプログラム。
【請求項１７】
請求項１６記載のプログラムにおいて、
前記アプリケーションプログラムの要求に応答して前記秘密情報を前記第２暗号鍵で復号化するとき、前記第２暗号鍵を保持していないか、又は前記第２暗号鍵を秘匿している場合、前記暗号鍵管理装置へ前記第２暗号鍵を要求するステップと、
前記暗号鍵管理装置が前記要求に応答して前記ポリシーが許可する場合に抽出した前記第２暗号鍵を、当該許可の条件と共に受信するステップと、
前記データベースの前記秘密情報を前記第２暗号鍵で復号化して提供するステップと、
前記許可の条件の範囲で前記第２暗号鍵を保持するステップと
を更に具備する
プログラム。
【請求項１８】
請求項１６に記載のプログラムにおいて、
前記暗号鍵管理装置が前記ポリシーで設定された更新時期が来たとき、生成して配信してきた新たな暗号鍵を受信するステップと、
前記データベースの前記秘密情報を前記第２暗号鍵で復号化し、前記新たな暗号鍵で再暗号化して前記データベースに格納するステップと、
前記新たな暗号鍵で前記秘密情報が再暗号化された後、前記第２暗号鍵を削除し、前記新たな暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記新たな暗号鍵を秘匿する
プログラム。
【請求項１９】
請求項１６乃至１８のいずれか一項に記載のプログラムにおいて、
前記秘密情報の開示が中断されるとき、前記暗号鍵管理装置が生成した第３暗号鍵を前記第２暗号鍵と共に受信するステップと、
前記データベースの前記秘密情報を前記第２暗号鍵で復号化し、前記第３暗号鍵で再暗号化して前記データベースに格納するステップと、
前記第３暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記第３暗号鍵を秘匿するステップと
を更に具備する
プログラム。
【請求項２０】

請求項１６記載のプログラムにおいて、
前記暗号鍵管理装置との通信が途絶した場合、予め配備された前記預託者の公開鍵に基づいて前記秘密情報を暗号化することにより、前記秘密情報の漏洩を防ぐステップを更に具備する
プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データ管理システム及びデータ管理方法に関し、特に、秘密情報の漏洩の防止を行うデータ管理システム及びデータ管理方法に関する。
【背景技術】
【０００２】
近年、ソフトウェアをネットワーク上に配備されたサービスとして利用する形態、いわゆるＳａａＳ（ソフトウェア・アズ・ア・サービス）の利用が広がっている。ＳａａＳは、サービス間を連携させるという点で、従来のネットワーク上のホスティングサービスであるＡＳＰ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）の進化型となっている。
【０００３】
ＳａａＳを利用する企業をテナントと呼ぶ。テナントがＳａａＳを利用する場合、自社の顧客情報など、企業秘密などの秘密情報をＳａａＳ事業者に預託する必要がある。ただし、情報の預託とは、情報処理を委託するなどの目的で他者に自らが保有する情報を預けることである。テナントが契約したＳａａＳ事業者に秘密情報を預託する場合、秘密情報はＳａａＳ事業者の持つ資源上のデータベースやファイルシステムに保存され、秘密情報はアクセス制限や暗号化による秘匿処理により保護する必要がある。さらに、ＳａａＳの利用において、サービス連携によって二次的なＳａａＳ事業者によってテナントの秘密情報が管理される場合が増えることが予想されている。そのような、二次的なＳａａＳ事業者が扱うテナントの秘密情報は、秘密情報の所有者であるテナントの意思が反映された形で、開示や秘匿などのアクセス制御のポリシー管理が行われることが望ましい。たとえば、テナント企業が開示を許した期間だけ、二次的なＳａａＳ事業者がテナントの秘密情報にアクセスできるようにしたり、サービス連携の契約期間が終了した場合には二次的なＳａａＳ事業者に付託した秘密情報の秘匿が保障され、サービス連携を再開する場合には迅速に秘密情報が開示されるようにしたりすることが望ましい。
【０００４】
データベースに格納された秘密情報の漏洩や不正なアクセスを防止する技術としては、データベース利用者に対してアクセス制限を付与することによって機密情報に対するアクセスを制限する技術、及び、機密情報自体を暗号化する技術が開示されている。
【０００５】
アクセス権限とは、データベースの表、又は列などの資源にアクセスする利用者に対して、データを参照したり更新したりする権限を付与し、与えられたＩＤやパスワードによって認証を行うことにより、適切なアクセス権限を認証し、資源へのアクセスを許可する技術である。特開２００６－１３４０１９号公報には、ユーザ認証処理によって認証されたユーザにのみ秘密情報を提供する情報処理システムが開示されている。
【０００６】
秘密情報の秘匿化には、データベースに格納される情報自体を暗号化する手法もある。しかし、全ての秘密情報に暗号化を行うとデータアクセスの効率が低下してしまう。特開平１１－２７２６８１号公報には、秘密情報を部分的に暗号化することによって復号処理の効率化を図る個人情報の記録方法が開示されている。
【０００７】
また、特表２００２－５１７８５４号公報（対応米国特許６２７９１１１（Ｂ１））には、複数のデータベース利用者が存在する場合、暗号化によるデータベースの秘匿化につ

いて、アクセス権を有するデータベース利用者に対して暗号鍵を与える方法が開示されている。

【０００８】

また、暗号鍵を与えることによってアクセス権を設定する場合、アクセス権を有するものが二次的に復号化されたデータベースを作成すると秘密情報が漏洩してしまう。しかし、特開２００８－１２４８３７号公報には、二次的にデータベースが公開される場合であっても、鍵管理サーバによって秘密情報の漏洩を防ぐデータ管理システムが開示されている。すなわち、そのデータ管理システムは、データベースサーバと鍵管理サーバとを含んで構成される。鍵管理サーバは、クライアント端末から、データベースサーバのデータベースを、データベースサーバへ登録するための登録要求を、当該データベースの利用許諾条件及び登録許諾条件を示す情報と共に受信するデータベース利用／登録請求入力ポートと、利用許諾条件及び登録許諾条件が、取得元のデータベースの登録許諾条件を満たすか否かを判断するデータベース登録条件可否判断モジュールと、登録許諾条件を満たすと判断された場合、データベースをデータベースサーバへの登録のために暗号化する登録用暗号鍵を生成して送信する暗号鍵生成モジュールとを備える。ただし、このデータ管理システムでは、暗号鍵を定期的に更新していない。

【０００９】

関連する技術として、特開平８－３０５６６２号公報（対応米国特許５７８４４６４（Ａ））にクライアント認証システムおよび方法が開示されている。このクライアント認証システムは、データを保持するデータ供給装置とそこから配送されるデータを受信するクライアントからなるデータ配送システム用である。データ供給装置は、クライアントに対応する第１の鍵を出力する鍵出力部、クライアントからのアクセス要求に応じて乱数を発生する乱数発生手段、鍵出力部において出力された第１の鍵によって乱数を暗号化することによって第１の認証子を出力する第１の暗号化手段、クライアントに乱数を送信する第１の送信手段、クライアントから第２の認証子を受信する第１の受信手段、及び第１の認証子と第２の認証子とを比較して両者が一致している場合に当該クライアントからのアクセス要求であると認証する比較手段を備える。クライアントは、データ供給装置にアクセス要求を行うアクセス要求手段、データ供給装置から送信された乱数を受信する第２の受信手段、第１の鍵と同一の第２の鍵を保持する鍵保持手段、第２の鍵によって乱数を暗号化することによって第２の認証子を出力する第２の暗号化手段、及びデータ供給装置に第２の認証子を送信する第２の送信手段を備える。

【００１０】

特表２００３－５１０９８７号公報（対応米国特許６７６３１１２（Ｂ１））にユニバーサル携帯電話サービスにおけるセキュリティ手順が開示されている。このセキュリティ手順は、無線アクセスネットワーク領域にわたって無線有効範囲をそれぞれ提供すると共にそれぞれ無線ネットワーク制御装置と基地局とを有する複数の無線アクセスネットワークに接続されたコアネットワークを有する移動通信システムにおける移動通信サービスと共に使用される。セキュリティ手順は、（ａ）移動局が位置する無線アクセスネットワーク領域内の無線有効範囲を制御する無線ネットワーク制御装置と移動局との間の通信障害を検出するステップ、（ｂ）移動局の認証を行うために無線ネットワーク制御装置からの要求をコアネットワークに送信するステップ、及び（ｃ）コアネットワークと移動局との間で移動局認証手順を行うステップを備える。

【００１１】

特表２００７－５０３１３６号公報（対応国際公開ＷＯ２００５０２０００２（Ａ２））にデジタル通信を容易にするためのシステム、方法、装置およびコンピュータプログラムが開示されている。この方法は、ネットワークを通じてクライアントからコンピュータに安全にアクセスするための、コンピュータに実装される。この方法は：・ユーザからユーザIDおよびパスワードを含む信用情報を受け取り、・信用情報を暗号化プロセスを用いて暗号化し、・暗号化された信用情報を含んだ、コンピュータへのアクセスの要求メッセージを生成し、・要求メッセージをネットワークを通じて送信し、・コンピュータへのア

クセスが認められたという検証メッセージを受信し、・コンピュータにアクセスする、ことを含んでおり、ユーザIDおよびユーザーパスワードがネットワークを通じて送信される際に暗号化されたままである。

【先行技術文献】

【特許文献】

【００１２】

【特許文献１】特開２００６－１３４０１９号公報

【特許文献２】特開平１１－２７２６８１号公報

【特許文献３】特表２００２－５１７８５４号公報

【特許文献４】特開２００８－１２４８３７号公報

【特許文献５】特開平８－３０５６６２号公報

【特許文献６】特表２００３－５１０９８７号公報

【特許文献７】特表２００７－５０３１３６号公報

【発明の概要】

【発明が解決しようとする課題】

【００１３】

特許文献１に開示された技術では、秘密情報へのアクセス制御は、二次的なＳａａＳ事業者に対して二次的なＳａａＳ事業者自身が持つデータベースへの資源管理として行われる。したがって、そこには秘密データを付託する秘密データ所有者が秘密情報の制御を行うことは考慮されていない。また、特許文献２で開示された技術では、暗号鍵が漏洩してしまった場合、秘密データを預託する側の秘密情報の秘匿性が守られなくなる恐れがある。特許文献３で開示された技術では、複数の暗号鍵を用意してアクセス制御を行っているが、秘密情報の預託側の開示や秘匿のポリシーの反映を考慮することをしていない。また、特許文献４で開示された技術では、二次的に利用されるデータベースをアクセスする場合、ネットワークによる通信によってアクセス制御の許諾条件を確認して、復号化と再暗号化によって二次的に蓄積されるデータベースの秘匿化を実現しているが、秘密データを預託する側の開示や秘匿のポリシーは考慮されていない。

【００１４】

本発明は、預託された秘密情報を二次的に利用するＳａａＳ事業者などの利用者に対し、秘密情報を預託した側のポリシーで設定されるアクセス制御を実現し、秘密情報の秘匿制御を預託側で制御することを目的とする。

【課題を解決するための手段】

【００１５】

本発明のデータ管理システムは、データベースと、データベース管理装置と、暗号鍵管理装置とを具備する。データベースは、預託者が預託し、第１暗号鍵で暗号化された秘密情報を保持する。データベース管理装置は、前記第１暗号鍵を保持しているとき、アプリケーションプログラムの要求に応答して、前記データベースの前記秘密情報を前記第１暗号鍵で復号化して提供する。暗号鍵管理装置は、前記預託者による前記秘密情報の開示に関するポリシーに基づいて、第２暗号鍵を生成して前記データベース管理装置に配信する。前記データベース管理装置は、前記データベースの前記秘密情報を前記第１暗号鍵で復号化し、前記第２暗号鍵で再暗号化して前記データベースに格納する。前記データベース管理装置は、前記第２暗号鍵で前記秘密情報が再暗号化された後、前記第１暗号鍵を削除し、前記第２暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記第２暗号鍵を秘匿する。

【００１６】

本発明のデータベース管理装置は、預託者が預託し、暗号鍵で暗号化された秘密情報を保持するデータベースを管理する。このデータベース管理装置は、暗号鍵制御装置と、データベース接続装置と、定期的暗号化更新装置とを備える。暗号鍵制御装置は、秘密情報の暗号化に用いた第１暗号鍵を保持する。データベース接続装置は、アプリケーションプログラムの要求に応答して、前記データベースの前記秘密情報を前記第１暗号鍵で復号化

して提供する。定期的暗号化更新装置は、前記データベースの前記秘密情報を前記第１暗号鍵で復号化し、その後、前記預託者による前記秘密情報の開示に関するポリシーに基づいて暗号鍵管理装置が生成した第２暗号鍵で、復号化された前記秘密情報を再暗号化して、前記データベースに格納する。前記暗号鍵制御装置は、前記第２暗号鍵で前記秘密情報が再暗号化された後、前記第１暗号鍵を削除し、前記第２暗号鍵を保持しないか、又は、前記データベース接続装置に対して前記第２暗号鍵を秘匿する。

【００１７】

本発明のデータ管理方法は、預預託者が預託し、第１暗号鍵で暗号化された秘密情報をデータベースに保持するステップと、アプリケーションプログラムの要求に応答して、前記データベースの前記秘密情報を前記第１暗号鍵で復号化するステップと、前記預託者による前記秘密情報の開示に関するポリシーに基づいて、第２暗号鍵を生成するステップと、前記データベースの前記秘密情報を前記第１暗号鍵で復号化し、前記第２暗号鍵で再暗号化するステップと、再暗号化された前記秘密情報を前記データベースに格納するステップと、前記第２暗号鍵で前記秘密情報が再暗号化された後、前記第１暗号鍵を削除し、前記第２暗号鍵を保持しないか、又は、前記アプリケーションプログラムに対して前記第２暗号鍵を秘匿するステップとを具備する。

【００１８】

本発明のプログラムは、預託者が預託し、暗号鍵で暗号化された秘密情報を保持するデータベースを管理するデータベース管理方法をコンピュータに実行させるプログラムである。そのプログラムは、秘密情報の暗号化に用いた第１前記暗号鍵を保持するステップと、アプリケーションプログラムの要求に応答して、前記データベースの前記秘密情報を前記第１暗号鍵で復号化して提供するステップと、前記データベースの前記秘密情報を前記第１暗号鍵で復号化し、その後、前記預託者による前記秘密情報の開示に関するポリシーに基づいて暗号鍵管理装置が生成した第２暗号鍵で、復号化された前記秘密情報を再暗号化するステップと、再暗号化された前記秘密情報を前記データベースに格納するステップと、前記第２暗号鍵で前記秘密情報が再暗号化された後、前記第１暗号鍵を削除し、前記第２暗号鍵を保持しないか、又は、前記データベース接続装置に対して前記第２暗号鍵を秘匿するステップとを具備するデータベース管理方法をコンピュータに実行させる。

【発明の効果】

【００１９】

本発明により、預託された秘密情報を二次的に利用するＳａａＳ事業者などの利用者に対し、秘密情報を預託した側のポリシーで設定されるアクセス制御を実現でき、秘密情報の秘匿制御を預託側で制御することができる。

【図面の簡単な説明】

【００２０】

【図１】図１は、本発明の実施の形態に係るデータベース管理システムの構成を示すブロック図である。

【図２】図２は、図１におけるデータベースの一例を示すテーブルである。

【図３】図３は、図１における暗号鍵制御装置の構成を示すブロック図である。

【図４】図４は、図３における暗号鍵保持装置が保持する暗号鍵保持テーブルの一例を示すテーブルである。

【図５】図５は、図１における属性情報格納装置の暗号化対象フィールド指定テーブルの一例を示すテーブルである。

【図６Ａ】図６Ａは、本発明の実施の形態に係るデータベース管理システムの動作を示すフローチャートである。

【図６Ｂ】図６Ｂは、本発明の実施の形態に係るデータベース管理システムの動作を示すフローチャートである。

【図７Ａ】図７Ａは、本発明の実施の形態に係るデータベース管理システムの他の動作を示すフローチャートである。

【図７Ｂ】図７Ｂは、本発明の実施の形態に係るデータベース管理システムの他の動作を

示すフローチャートである。
【発明を実施するための形態】
【００２１】
以下、本発明のデータベース管理システム及びデータベース管理方法の実施の形態に関して、添付図面を参照して説明する。本実施の形態では、秘密情報を提供する預託者（主体者）はＳａａＳを利用する企業、すなわちテナントであるとして説明する。ただし、本発明はその例に限定されるものではない。
【００２２】
まず、本発明の実施の形態に係るデータベース管理システムの構成について説明する。図１は、本発明の実施の形態に係るデータベース管理システムの構成を示すブロック図である。データベース管理システム１は、ＳａａＳを提供する業者に属し、暗号鍵管理装置１０と、データベース管理装置２０と、データベース３０とを具備する。
【００２３】
暗号鍵管理装置１０は、コンピュータに例示される情報処理装置であり、インターネットに例示される通信ネットワーク５０を介してデータベース管理装置２０と双方向通信可能に接続されている。暗号鍵管理装置１０は、所定のポリシーに基づく暗号鍵の生成を行う。暗号鍵管理装置１０は、ポリシー管理装置１２と、暗号鍵配信サーバ１１とを備えている。
【００２４】
ポリシー管理装置１２は、秘密情報を預託したテナントが定める、秘密情報に関するポリシーを管理する。そのポリシーは、秘密情報の開示及び秘匿を行う時限や、秘密鍵の更新頻度のような秘密情報の秘匿に関するアクセス制御の条件を示している。ポリシーには、例えば、テナントを識別する情報（例示：テナントＩＤ）、暗号鍵の更新頻度（例示：１週間毎に更新、不定期のスケジュールに基づいて更新など）、テナントが預託した秘密情報の提供を中止する条件（例示：所定期間内に許可が無ければ提供中止、２週間後に提供中止など）、暗号鍵を配信しない条件（例示：１週間に２回以上配信しない、予め設定した特定のアプリケーションプログラムや情報取得の依頼元（例示：事前に安全確認を行ったプログラムや依頼元など）などを除いて配信しないなど）、等を含んでいる。テナントは、ポリシー管理装置１２に随時アクセスしてポリシーを変更することができる。それにより、技術動向の変化や事業計画の変更等により秘密情報の開示条件を変更したい場合、自在に対応することができる。
【００２５】
暗号鍵配信サーバ１１は、データベース管理装置２０又はポリシー管理装置１２からの要求に基づいて、ポリシー管理装置１２に登録されたポリシーに従って暗号鍵を生成する。そして、生成された暗号鍵をデータベース管理装置２０に配信する。暗号鍵配信サーバ１１及びポリシー管理装置１２（暗号鍵管理装置１０）は、秘密情報の預託者（テナント）から信頼されるサーバであり、他の装置に比較して極めて高いセキュリティが施されていることが好ましい。例えば、ＳＳＬ（ｓｅｃｕｒｅ　ｓｏｃｋｅｔｓ　ｌａｙｅｒ）プロトコルに用いられるサーバ証明書のような技術を用いて通信のセキュリティを高める方法に例示される。
【００２６】
データベース３０は、コンピュータに例示される情報処理装置であり、データベース管理装置２０と双方向通信可能に接続されている。データベース３０は、複数のテナントが提供（預託）する複数の秘密情報を保持している。そして、テナントの識別情報と提供（預託）された秘密情報とを関連付けて格納している。例えば、データベース３０がテーブルで管理されるデータベースの場合、テーブルには、秘密情報を預託したテナントの識別情報のフィールドと、その秘密情報のフィールドとが含まれている。
【００２７】
図２は、図１におけるデータベース３０の一例を示すテーブルである。データベース３０には、データベース名“ＭＡＳＴＥＲＴＢＬ”のテーブル５００を構成するフィールド

として、テナントの識別情報としてのテナントＩＤ（ＴＩＤ）と、秘密情報としての顧客名（ＣＵＮＡＭＥ）及び住所（ＣＡＤＲＳ）とが定義されている。すなわち、テナントＩＤ（ＴＩＤ）と、秘密情報（ＣＵＮＡＭＥ、ＣＡＤＲＳ）とが関連付けられている。

【００２８】

データベース管理装置２０は、コンピュータに例示される情報処理装置であり、アプリケーションプログラム（ＡＰプログラム）４０と双方向通信可能である。データベース管理装置２０は、アプリケーションプログラム４０からデータベース３０への参照、更新、削除のリクエストを受診し、データベース３０と交信して、処理を行う。データベース管理装置２０は、定期的暗号化更新装置２１と、暗号鍵制御装置２２と、データベース接続装置２３と、通信障害時暗号化装置２４と、属性情報格納装置２５とを備えている。

【００２９】

暗号鍵制御装置２２は、暗号鍵配信サーバ１１から暗号鍵を取得し、保持している。そして、定期的暗号化更新装置２１やデータベース接続装置２３の要求に応答して、保持している暗号鍵をそれらの定期的暗号化更新装置２１やデータベース接続装置２３に出力する。暗号鍵を保持していない場合、必要に応じて暗号鍵配信サーバ１１に暗号鍵を要求し、取得し、保持する。図３は、図１における暗号鍵制御装置２２の構成を示すブロック図である。暗号鍵制御装置２２は、更新暗号鍵受信装置２０１と、暗号鍵要求装置２０２と、再暗号化要求装置２０３と、暗号鍵配信装置２０４と、暗号鍵保持装置２０５とを備えている。

【００３０】

暗号鍵保持装置２０５は、テナントごとに暗号鍵を保持している。図４は、図３における暗号鍵保持装置２０５が保持する暗号鍵保持テーブル３００の一例を示すテーブルである。暗号鍵保持テーブル３００は、テナントを識別するテナントＩＤ３０１と、当該テナントの秘密情報の復号に用いる暗号鍵３０２と、当該暗号鍵の有効期限３０３とを含み、これらを互いに関連付けて格納している。暗号鍵保持装置２０５は、この暗号鍵保持テーブル３００をメモリ上など、クラッキングなどの脅威に対してセキュリティレベルの高い場所に保持する。

【００３１】

更新暗号鍵受信装置２０１は、暗号鍵配信サーバ１１から、ポリシーに基づいて更新された暗号鍵である更新暗号鍵と対応するテナントＩＤとを受信し、再暗号化要求装置２０３へ出力する。

【００３２】

再暗号化要求装置２０３は、更新暗号鍵受信装置２０１から更新暗号鍵とテナントＩＤとを受信する。そして、暗号鍵保持装置２０５の暗号鍵保持テーブル３００を参照して、受信したテナントＩＤに対応する暗号鍵（現在当該テナントが預託している秘密情報を暗号化している暗号鍵。以下、現暗号鍵ともいう）を取得する。そして、更新暗号鍵、テナントＩＤ、現暗号鍵を定期的暗号化更新装置２１に出力し、テナントＩＤに対応するデータベース３０内の秘密情報について、復号化処理及び再暗号化処理の依頼を行う。ただし、定期的暗号化更新装置２１に復号化処理及び再暗号化処理の依頼を行う場合、例えば、深夜時間帯や週末など、バッチ処理として実行する機能を備えてもよい。

【００３３】

暗号鍵配信装置２０４は、データベース接続装置２３から、秘密情報の開示を要求されたテナントＩＤを受信する。そして、暗号鍵保持装置２０５の暗号鍵保持テーブル３００を参照して、受信したテナントＩＤに対応する暗号鍵を取得する。又は、暗号鍵要求装置２０２を介して暗号鍵配信サーバ１１から暗号鍵を取得する。そして、取得した暗号鍵をデータベース接続装置２３へ出力する。

【００３４】

暗号鍵要求装置２０２は、暗号鍵配信装置２０４がテナントＩＤに対応する暗号鍵を取得できない場合、暗号鍵配信サーバ１１へ、そのテナントＩＤに対応する暗号鍵の配信を要求する。そして、暗号鍵配信サーバ１１から取得した暗号鍵を暗号鍵配信装置２０４へ

出力する。それと共に、その取得した暗号鍵を暗号鍵保持装置２０５に格納する。

【００３５】

属性情報格納装置２５は、データベース３０において、どのテーブルのどのフィールドに対して暗号化が行われているかの情報を示す暗号化対象フィールド指定テーブル６００を保持している。この暗号化フィールド指定テーブル６００は、テナントのポリシー設定によって暗号鍵配信サーバ１１から暗号鍵の暗号化対象として配信され、属性情報格納装置２５に格納される。図５は、図１における属性情報格納装置２５の暗号化対象フィールド指定テーブル６００の一例を示すテーブルである。暗号化対象フィールド指定テーブル６００は、テーブルの情報（データベース・テーブル名）と、情報の暗号化が行われているフィールド（秘匿フィールド）と、テナントＩＤが既述されているフィールド（識別ＩＤフィールド）とを関連付けている。すなわち、データベース・テーブル名に示されるテーブルにおいて、識別ＩＤフィールドに示されるフィールドに記述されたテナントＩＤから提供された情報のうち、秘匿フィールドに示されるフィールドに既述された情報（秘密情報）に対して暗号化が行われている。

【００３６】

定期的暗号化更新装置２１は、再暗号化要求装置２０３から復号化処理及び再暗号化処理の要求があった場合、更新暗号鍵、テナントＩＤ、現暗号鍵を受信する。次に、属性情報格納装置２５からテナントＩＤに対応するデータベース３０内の秘密情報のテーブル及びフィールドを取得する。続いて、データベース３０にアクセスして、当該テーブル及びフィールド、テナントＩＤに対応する秘密情報を取得する。そして、現暗号鍵で暗号化されている秘密情報について、現暗号鍵で復号化した後、更新暗号鍵で再暗号化する。そして、データベース３０に当該秘密情報を再び格納する。

【００３７】

定期的暗号化更新装置２１は、暗号化対象フィールド指定テーブル６００を参照して、暗号化対象フィールドと対象レコードを判別する。図５の例においては、暗号化対象フィールド指定テーブル６００を参照して、テナントＩＤと比較する対象がＴＩＤフィールドであること、秘密情報がＣＡＲＤＳフィールドに格納されていること、データベース・テーブル名がＭＡＳＴＥＲＴＢＬであることを抽出する。定期的暗号化更新装置２１は、データベース３０から、再暗号化要求装置２０３から送られたテナントＩＤと一致するレコード（秘密情報を含む）を読み出す。そして、読み出したレコードのうちの秘密情報を、現暗号鍵（暗号鍵保存装置２０５から得られた一世代前の暗号鍵）を用いて復号化し、更新暗号鍵（新しく暗号鍵配信サーバ１１から送信された暗号鍵）により再暗号化を行う。

【００３８】

データベース接続装置２３は、アプリケーションプログラム４０からデータベース３０の秘密情報の要求（データベース・テーブル名、秘匿フィールドを含む）を受けて、属性情報格納装置２５から当該秘密情報の識別ＩＤフィールドを取得し、暗号鍵制御装置２２から当該テナントＩＤの暗号鍵を取得し、当該暗号鍵を用いてデータベース３０から取得した秘密情報を復号化し、アプリケーションプログラム４０へ通知する。なお、データベース接続装置２３は、定期的暗号化更新装置２１や暗号鍵制御装置２２が行う暗号鍵の更新とは独立して、アプリケーションプログラム４０からの要求に基づいてデータベース３０から秘密情報を取得している。したがって、それらとは独立した装置と考えることができ、別体として設けて、ネットワークで接続するようにしても良い。

【００３９】

通信障害時暗号化装置２４は、暗号鍵制御装置２２（暗号鍵要求装置２０２）が暗号鍵配信サーバ１１に接続できない場合のように通信回線が途絶した場合に備えて、各テナントの公開鍵が予め登録されている。そして、通信回線が途絶した場合、予め登録されたテナントの公開鍵によって、該当するテナントＩＤの秘密情報の暗号化処理を行う。これにより、通信から切り離された場合の情報の秘匿性を保障することができる。

【００４０】

図６Ａ及び図６Ｂは、本発明の実施の形態に係るデータベース管理システムの動作（デ

ーベース管理方法）の一例を示すフローチャートである。ここでは、ポリシーに基づいて暗号鍵を配信する処理について説明する。

ここでは、一例として以下の前提条件に基づいて動作を説明する。すなわち、まず、ポリシー管理装置１２は、予め、テナントが設定したポリシーに関する情報を保持している。そのポリシーはテナントであれば随時変更（更新）可能である。また、データベース３０は、予め、テナントが預託した秘密情報をテーブル５００に保持している。更に、暗号鍵保持装置２０５は、属性情報格納装置２５は、予め、暗号鍵配信サーバ１１がテナントに対して設定した暗号鍵を暗号鍵保持テーブル３００に保持している。加えて、属性情報格納装置２５は、予め、テーブル５００における暗号化が行われているフィールドの情報を暗号化対象フィールド指定テーブル６００に保持している。

【００４１】

上記前提条件は、例えば以下のようにして設定することができる。

それぞれのテナントは、異なったポリシーにより時限的な預託した秘密情報の管理を行う。テナントが、２次的なＳａａＳ事業者のデータベースに秘密情報を預託する場合を考える。まず、テナントは、ポリシー管理装置１２に、ポリシーに関する情報（秘匿化項目と開示期限を含む）を設定すると共に、預託する秘密情報を入力する。次に、ポリシー管理装置１２は、暗号鍵配信サーバ１１に、テナントを識別するＩＤ、鍵生成要求及び預託する情報（秘密情報を含む）を出力する。続いて、暗号鍵配信サーバ１１は、ポリシー管理装置１２からの鍵生成要求に基づいて、新しい暗号鍵を生成する。そして、暗号鍵及びテナントＩＤと共に、預託先のデータベース３０の暗号化対象となるフィールド及び預託する情報（秘密情報を含む）を暗号鍵制御装置２２に配信する。その後、暗号鍵制御装置２２は、暗号鍵とテナントＩＤとを関連付けて暗号鍵保存装置２０５の暗号鍵保持テーブル３００に保存する。また、暗号化対象フィールドと、暗号鍵と、情報（秘密情報を含む）と、テナントＩＤとを定期的暗号化更新装置２１へ出力する。次に、定期的暗号化更新装置２１は、暗号化対象フィールド情報に対応する秘密情報を、暗号鍵で暗号化する。そして、暗号化された秘密情報を含む預託情報とテナントＩＤとを関連付けて、データベース３０のテーブル５００に格納する。また、テナントＩＤのフィールドである識別ＩＤフィールド、暗号化対象フィールド、データベース・テーブル名を属性情報格納装置２５へ出力する。そして、属性情報格納装置２５は、暗号化対象フィールドと識別ＩＤフィールドとデータベース・テーブル名とを関連付けて暗号化対象フィールド指定テーブル６００に格納する。

【００４２】

ポリシーに基づいて暗号鍵を配信する処理は以下のようになる。

まず、ポリシー管理装置１２は、個別のテナントがデータベース３０へ預託した秘密情報に関して、自身のタイマにより一定時間待機する。この一定時間は、ポリシーで定めた期間よりも十分小さく設定する。たとえば、一週間ごとに再暗号化を実施するポリシーであれば、１日や１時間など、十分小さい間隔とする（ステップＳ０１）。

【００４３】

次に、ポリシー管理装置１２は、ポリシーに基づき２次的なＳａａＳ事業者（２次提供先）に秘密情報を利用することを許可する場合、前回又は初回での預託した秘密情報の再暗号化からポリシーにより設定された期間が経過したか否か、及び、ポリシーに基づき秘密情報の提供を中止する場合であるか否か、を判定する（ステップＳ０２）。

【００４４】

秘密情報の２次提供先での利用を中止して既にデータベース接続装置２３に公開されない暗号鍵で秘密情報が暗号化されている場合や、ポリシーにより設定された期間に達していない場合（ステップＳ０２：Ｎｏ）、ステップＳ０１に戻り待機を行う。この期間、後述するが、このテナントの秘密情報を開示する暗号鍵が暗号鍵制御装置２２の暗号鍵保持装置２０５に保持されるため、データベース管理装置２０では、このテナントの秘密情報は開示されている状態になっている。

【００４５】

ステップＳ０２で、ポリシーにより設定された期間が過ぎている場合や、ポリシーにより秘密情報の提供を中止する場合（ステップＳ０２：Ｙｅｓ）、ポリシー管理装置１２は、暗号鍵配信サーバ１１に、暗号鍵の更新を要求する更新暗号鍵要求情報（ポリシーによる条件として、例えば有効期限を含んでいてもよい）と、テナントの識別情報として例えばテナントＩＤとを出力する（ステップＳ０３）。

【００４６】

暗号鍵配信サーバ１１は、更新要求情報とテナントＩＤとに基づいて、更新用の新しい暗号鍵である更新暗号鍵を生成する（ステップＳ０４）。このとき、暗号鍵配信サーバ１１は、テナントＩＤと更新暗号鍵と有効期限とを関連付けて保持する。そして、その更新暗号鍵（有効期限を含んでいてもよい）とテナントＩＤとをデータベース管理装置２０の暗号鍵制御装置２２の更新暗号鍵受信装置２０１へ配信する（ステップＳ０５）。

【００４７】

ただし、ポリシー管理装置１２は、テナントの要求に応じて、即座にデータベース３０に預託している秘密情報に対して暗号化を更新し、データベース３０の秘密情報を秘匿することも可能である。

【００４８】

更新鍵受信装置２０１は、更新暗号鍵とテナントＩＤとを受信する。そして、受信した更新暗号鍵とテナントＩＤとを、暗号鍵制御装置２２の再暗号化要求装置２０３に送信する（ステップＳ０６）。

【００４９】

再暗号化要求装置２０３は、送信されたテナントＩＤに基づいて、暗号鍵保持装置２０５における暗号鍵保持テーブル３００を参照して、当該テナントＩＤの秘密情報を暗号化している現時点での暗号鍵（以下、現暗号鍵ともいう）を取得する（ステップＳ０７）。そして、再暗号化要求装置２０３は、暗号鍵保持装置２０５の暗号鍵保持テーブル３００において、現暗号鍵及びその有効期限をクリアする（ステップＳ０８）。その後、取得した現暗号鍵と、テナントＩＤと、更新暗号鍵とを定期的暗号化更新装置２１に送信する（ステップＳ０９）。

【００５０】

定期的暗号化更新装置２１は、現暗号鍵と、テナントＩＤと、更新暗号鍵とを受信する。そして、定期的暗号化装置２１は、テナントＩＤをデータベース３０に送信する（ステップＳ１０）。データベース３０は、テナントＩＤに基づいて、当該テナントＩＤに対応するデータベースのテーブル５００のデータベース・テーブル名及びその情報（秘密情報を含む）を読み出し、定期的暗号化装置２１へ出力する。定期的暗号化装置２１は、データベース・テーブル名及びその情報（秘密情報を含む）を取得する（ステップＳ１１）。

【００５１】

定期的暗号化更新装置２１は、データベース・テーブル名を、属性情報格納装置２５へ送信する（ステップＳ１２）。属性情報格納装置２５は、データベース・テーブル名に基づいて、暗号化対象フィールド指定テーブル６００を参照して、当該データベース・テーブル名における暗号化対象フィールドを読み出して、定期的暗号化更新装置２１に出力する。定期的暗号化更新装置２１は、暗号化対象フィールドを取得する（ステップＳ１３）。

【００５２】

定期的暗号化装置２１は、取得した情報（秘密情報を含む）のうち、暗号化対象フィールドの対象レコード（秘密情報）を、現暗号鍵で復号化する（ステップＳ１４）。その後、復号化された秘密情報を更新暗号鍵で再暗号化する（ステップＳ１５）。そして、再暗号化された秘密情報を含む情報と、テナントＩＤと、データベース・テーブル名とをデータベース３０へ出力する（ステップＳ１６）。データベース３０は、受信したテナントＩＤ及び情報（再暗号化された秘密情報を含む）を、データベース３０のテーブル５００に格納する（ステップＳ１７）。

【００５３】

以上の処理により、ポリシーで定められた期間が終了するたびに、新しく更新された暗号鍵でデータベース３０の当該テナントの秘密情報を暗号化することができる。

【００５４】

なお、この時点では、暗号鍵保持装置２０５が保持する暗号鍵保持テーブル３００には、更新暗号鍵は登録されていない（秘匿されている）。そのため、データベース接続装置２３がデータベース３０のテナントの暗号化された秘密情報を復号化できない状態となっている。ただし、更新暗号鍵は、データベース接続装置２３（又はアプリケーションプログラム４０）に対して秘匿されていれば、例えばステップＳ０８において、暗号鍵保持装置２０５内に、テナントＩＤと有効期限と共に格納されていても良い。

【００５５】

なお、ステップＳ０７において、暗号鍵保持装置２０５に現暗号鍵が登録されていない場合（更新暗号鍵は登録されないため場合があるため）、再暗号化要求装置２０３は、暗号鍵配信サーバ１１にテナントＩＤを引数として現暗号鍵を問い合わせてもよい。又は、ステップＳ０５において暗号鍵配信サーバ１１が更新暗号鍵とテナントＩＤとを更新暗号鍵受信装置２０１へ配信するとき、現暗号鍵も併せて配信しても良い。これにより、ステップＳ１４において定期的暗号化装置２１は、確実に秘密情報を現暗号鍵で復号化することができる。

【００５６】

以上の処理により、テナントのポリシーによって、テナントが２次的なＳａａＳ事業者のデータベース３０に預託した、秘密情報が、定期的に更新された暗号鍵によって暗号化される。

【００５７】

図７Ａ及び図７Ｂは、本発明の実施の形態に係るデータベース管理システムの他の動作（デーベース管理方法）の一例を示すフローチャートである。ここでは、アプリケーションプログラム４０がデータベース３０をアクセスして読み取り、更新などを行う処理について説明する。本実施の形態では、一例としてデータベース接続装置２３がＪＤＢＣ（Ｊａｖａ（登録商標）　ＤａｔａＢａｓｅ　Ｃｏｎｎｅｃｔｉｖｉｔｙ）などのようなデータベース接続ライブラリとして説明するが、より高度な働きをするライブラリ、たとえば、Ｏ／Ｒ（Ｏｂｊｅｃｔ／ＲＤＢ（Ｒｅｌａｔｉｏｎａｌ　ＤａｔａＢａｓｅ））マッピングライブラリであってもよい。

【００５８】

一例として、アプリケーションプログラム４０が、データベース接続装置２３に、例えばＳＱＬ文として、次のＳＱＬ文を発行したとして、動作を説明する。

“ＳＥＬＥＣＴ　ＣＵＮＡＭＥ　ＣＡＤＲＳ　ＦＲＯＭ　ＭＡＳＴＥＲＴＢＬ；”

このとき、データベース接続装置２３は、アプリケーションプログラム４０から呼び出され、データベース３０へのクエリを発行し、データを取得する。

【００５９】

アプリケーションプログラム４０は、データベース接続装置２３に、データを要求する命令として、上記のＳＱＬ文を発行する。このデータ要求命令は、検索対象となるデータベース・テーブルの名称（ＭＡＳＴＥＲＴＢＬ）と、抽出対象となるフィールドの名称（ＣＵＮＡＭＥ　ＣＡＤＲＳ）とを含んでいる。ただし、データベース・テーブルの名称は、データベース３０に格納された複数のテーブル５００のうちのいずれかの名称（識別子：データベース・テーブル名を含む）を示している。フィールドの名称は、テーブル５００の複数のフィールドのうちのいずれかの名称（識別子：秘匿フィールドを含む）を示している。データベース接続装置２３は、そのデータを要求する命令（ＳＱＬ文）を受信する（ステップＳ４１）。なお、データ要求命令は、テナントＩＤや、アプリケーションプログラムや情報要求の依頼元の情報を含んでいても良い。

【００６０】

データベース接続装置２３は、データベース・テーブルの名称とフィールドの名称とをデータベース３０に送信する（ステップＳ４２）。データベース３０は、データベース・

テーブルの名称に対応するデータベースのテーブル５００から、フィールドの名称に対応する情報（秘密情報を含む場合あり）を抽出して、テナントＩＤと共にデータベース接続装置２３へ出力する。データベース接続装置２３は、その情報（秘密情報を含む場合あり）及びテナントＩＤを取得する（ステップＳ４３）。なお、データ要求命令にテナントＩＤが含まれている場合には、フィールドの名称に対応する情報のうち、そのテナントＩＤに対応する情報を抽出して出力する。

【００６１】

データベース接続装置２３は、属性情報格納装置２５へ暗号化対象フィールド指定テーブル６００を読み出す命令を出力する（ステップＳ４４）。属性情報格納装置２５は、読み出し命令に応答して、暗号化対象フィールド指定テーブル６００をデータベース接続装置２３へ出力する（ステップＳ４５）。データベース接続装置２３は、読み出された暗号化対象フィールド指定テーブル６００を参照して、データ要求命令における検索対象のデータベース・テーブルの名称と一致するデータベース・テーブル名のレコードを抽出し、当該レコードから秘匿フィールドを取得する。そして、上記ＳＥＬＥＣＴ文で抽出した情報（秘密情報を含む場合あり）のフィールドの中に、秘匿フィールドが含まれているか否かを判定する（ステップＳ４６）。そのような秘匿フィールドが含まれていない場合（ステップＳ４６：Ｎｏ）、データベース接続装置２３はアプリケーションプログラム４０へ、取得した情報（秘密情報なし）を出力して処理を終了する（ステップＳ４７）。一方、そのような秘匿フィールドが含まれている場合（ステップＳ４６：Ｙｅｓ）、データベース接続装置２３は、暗号化対象フィールド指定テーブル６００で指定された識別ＩＤフィールドがテナントＩＤであることに基づいて、取得したテナントＩＤを暗号鍵制御装置２２へ出力する（ステップＳ４８）。

【００６２】

暗号鍵制御装置２２の暗号鍵配信装置２０４は、テナントＩＤを受信する。そして、暗号鍵保持装置２０５の暗号鍵保持テーブル３００からテナントＩＤに対応した暗号鍵を有効期限と共に取得する（ステップＳ４９）。そして、有効期限内の暗号鍵を取得できた場合（ステップＳ５０：Ｙｅｓ）、暗号鍵配信装置２０４は取得された暗号鍵をデータベース接続装置２３へ送信する（ステップＳ６０）。

【００６３】

しかし、取得しようとしたテナントＩＤに対応する暗号鍵について、暗号鍵保持テーブル３００の有効期限３０３が既に過ぎている場合、暗号鍵配信装置２０４は、取得した暗号鍵の有効期限が過ぎているので、有効な暗号鍵を取得できない（ステップＳ５０：Ｎｏ）。あるいは、取得しようとしたテナントＩＤに対応する暗号鍵が再暗号化要求装置２０３により更新されていた場合（ステップＳ１５：図６Ｂ）、再暗号化要求装置２０３が暗号鍵保持テーブル３００のテナントＩＤに対応する暗号鍵をクリアするため（ステップＳ０８：図６Ａ）、暗号鍵保持テーブル３００に暗号鍵は存在しない。すなわち、暗号鍵を取得できない（ステップＳ５０：Ｎｏ）。これらの場合、暗号鍵配信装置２０４は、暗号鍵要求装置２０２に、暗号鍵を習得しようとしたテナントＩＤについて、暗号鍵配信サーバ１１への暗号鍵の取得要求を発行する（ステップＳ５１）。

【００６４】

暗号鍵要求装置２０２は、取得したいテナントＩＤを引数として、暗号鍵配信サーバ１１に暗号鍵配信要求を行う（ステップＳ５２）。この暗号鍵配信要求に、アプリケーションプログラム４０から取得したアプリケーションプログラムや情報要求の依頼元の情報を含ませても良い。暗号鍵配信サーバ１１は、暗号鍵配信要求に応答して、ポリシー管理装置１２にそのテナントＩＤのポリシーを問い合せる（ステップＳ５３）。ポリシー管理装置１２は、そのテナントＩＤのポリシーを暗号鍵配信サーバ１１へ出力する（ステップＳ５４）。暗号鍵配信サーバ１１は、そのテナントＩＤのポリシーによって暗号鍵の配信が許されるか否かを判断する（ステップＳ５５）。例えば、ポリシーにおける、テナントが預託した秘密情報の提供を中止する条件に該当するか否かや、暗号鍵を配信しない条件に該当するか否かなどを判断する。そして、暗号鍵の配信が許されない場合（ステップＳ５

５：Ｎｏ）、暗号鍵配信サーバ１１は暗号鍵配信不可通知を、暗号鍵要求装置２０２を介してデータベース接続装置２３へ送信する（ステップＳ５６）。データベース接続装置２３は、アプリケーションプログラム４０へエラーを発行して処理を終了する（ステップＳ５７）。一方、暗号鍵の配信が許される場合（ステップＳ５５：Ｙｅｓ）、暗号鍵配信サーバ１１は、そのテナントＩＤに基づいて、秘密情報を暗号化した現在（最新）の暗号鍵を抽出する（ステップＳ５８）。ただし、現在（最新）の暗号鍵は、テナントＩＤ及びポリシーで決まる有効期限と関連付けられて暗号鍵配信サーバ１１に格納されている。そして、抽出された暗号鍵を、ポリシーで決まる有効期限と共に、暗号鍵要求装置２０２に通知する（ステップＳ５９）。暗号鍵配信装置２０４は取得された暗号鍵をデータベース接続装置２３へ送信する（ステップＳ６０）。暗号鍵要求装置２０２は、暗号鍵要求装置２０２自身によって要求して取得した暗号鍵及び有効期限を暗号鍵保持装置２０５の暗号鍵保持テーブル３００にも記録する（ステップＳ６１）。

【００６５】

データベース接続装置２３は、取得した情報（秘密情報あり）のうちの秘匿フィールドの秘密情報を取得した暗号鍵で復号化する（ステップＳ６２）。そして、データベース接続装置２３は、取得した情報（復号化された秘密情報を含む）をアプリケーションプログラム４０へ出力する（ステップＳ６３）。

【００６６】

以上の動作により、データベース接続装置２３は、テナントのポリシーによって暗号鍵を取得することが許されている場合にのみ、データベース３０に保持された暗号化された秘密情報を復号してアプリケーションプログラム４０に供給することができる。

【００６７】

また、一度暗号鍵要求装置２０２が取得した暗号鍵は、暗号鍵保持装置２０５に保持されるため、暗号鍵はテナントのポリシーが許す間、暗号鍵保持装置２０５にキャッシュされることになる。

【００６８】

また、上記動作において、上記暗号鍵要求装置２０２が、暗号鍵配信サーバに接続できないなど、通信回線が途絶した場合、通信障害時暗号化装置２４にあらかじめ登録されたテナントの公開鍵によって、該当するテナントＩＤの秘密情報の暗号化処理を行う。これにより、通信から切り離された場合の情報の秘匿性を保障することができる。

【００６９】

なお、上記実施の形態では、暗号鍵管理装置１０が一台であったが、本発明はこの例に限定されるものではなく、暗号鍵管理装置１０が複数台あってもよい。また、データベース３０はリレーショナルデータベースに限定されるものではなく、他のデータベースやファイルシステムであってもよい。更に、データベース管理装置２０及びデータベース３０は、一体に構成されていても良い。例えば一台のコンピュータで構成されていても良い。

【００７０】

本実施の形態では、暗号鍵管理装置１０により定期的に暗号鍵が更新され、暗号鍵制御装置２２及び定期的暗号化更新装置２１により当該更新された暗号鍵により定期的にデータベース３０の情報が暗号化される（図６Ａ及び図６Ｂなど）。これらは、アプリケーションプログラム４０等によるデータベース３０へのアクセスとは全く独立に行われている。すなわち、アプリケーションプログラム４０等の都合に関わらず、テナントの設定した（及び更新された）ポリシーに基づいて、独立に暗号鍵を更新し、情報を暗号化することができる。また、ポリシーの設定は随時テナントの希望時に変更できる。それにより、テナントの希望を適切に反映したポリシーに基づく情報開示を行うことができる。すなわち、秘密情報を預託した側のポリシーで設定されるアクセス制御を実現し、秘密情報の秘匿制御を預託側で制御することができる。そして、テナントの満足の行く秘匿制御を行うことができる。

【００７１】

また、本実施の形態では、アプリケーションプログラム４０等によるデータベース３０

へのアクセスに対して、ポリシー管理装置１２に格納された随時更新可能なポリシー（例示：アクセスの時期や回数、アクセスするアプリケーションプログラム４０や依頼元）に基づいて、暗号鍵を付与するか否かを決定することができる。それにより、当該ポリシーに基づいて、テナントの希望を適切に反映したアクセス制御、秘匿制御を実現することができる。テナントの納得可能なセキュリティを実現することができる。

【００７２】

また、本実施の形態では、アプリケーションプログラム４０等によるデータベース３０へのアクセスの度に暗号鍵管理装置１０が暗号鍵の付与を行うとすると、通信負荷や情報処理負荷が非常に重くなり実用的ではない。本実施の形態では、暗号鍵を付与するときに、有効期限等の条件を決めて暗号鍵を付与する。そのため、その有効期限等の条件内であれば、暗号鍵管理装置１０による暗号鍵の付与を受けることなく、既に付与された暗号鍵を用いてデータベース３０へアクセスすることができる。すなわち、暗号鍵の有効期限内において、通信負荷や情報処理負荷を低く抑えたアクセスが可能となる。それにより、通信負荷や情報処理負荷の増大を抑制し、アプリケーションプログラム４０等によるアクセスの利便性を確保しつつ、テナントの希望を適切に反映したアクセス制御、秘匿制御を実現することができる。

【００７３】

以上のように本発明の代表的な一形態では、データベース管理装置と、暗号鍵管理装置とを具備する。データベース管理装置は、プロセッサと、プロセッサに接続されるメモリと、データベースが格納される記憶装置と、暗号鍵データベースの秘密情報を部分的に新しい暗号鍵で再暗号化する定期的暗号化更新装置と、アプリケーションプログラムからデータベースにアクセスを行うデータベース接続装置と、暗号鍵制御装置と、データベースを部分的に暗号化する際に利用する属性情報格納装置と、ネットワーク接続装置とを備える。暗号鍵管理装置は、このデータベース管理装置とネットワークで接続され、秘密情報提供者（預託者、テナントともいう）の開示ポリシーを格納するポリシー管理装置と、秘密情報提供者から信頼されるサーバであり開示ポリシーで決められる間隔で新しい暗号鍵を生成しデータベース管理装置に供給する暗号鍵配信サーバとを備える。

定期的暗号化更新装置は、再暗号化のために新しい暗号鍵が配信された場合、テナントの秘密情報を以前の暗号鍵で復号し配信された新しい暗号鍵で再暗号化する。その際、新しい暗号鍵は暗号鍵制御装置には格納されない。データベース接続装置は、アプリケーションからの接続要請に応じてデータベースに対して参照を行う。

その際、データベース接続装置は、テナントを識別するＩＤ情報を元に、暗号化されているテーブルおよびフィールド情報を属性情報格納装置から取得し、該当フィールドに対してテナント固有の配信された暗号鍵を暗号鍵制御装置から取得して復号を行い、アプリケーションプログラムに結果を返す。

このとき、データベース接続装置は、定期的暗号化更新装置によって再暗号化されて暗号鍵制御装置に当該テナントの暗号鍵が保持されていない場合、暗号鍵配信サーバに暗号鍵を要求し、テナントのポリシーが許可すれば暗号鍵は暗号鍵制御装置に配信され、アプリケーションプログラムに配信された暗号鍵を用いて秘密情報を復号し平文で情報を戻す。

暗号鍵配信サーバは、テナントごとにテナントの秘密情報を開示する期間などのポリシーをポリシー管理装置から取得し、データベース管理装置の暗号鍵制御装置から暗号鍵の配信要求があった場合、ポリシーで開示が認められる場合は、現在データベースを暗号化している暗号鍵を配信する。

通信障害時暗号化装置は、通信障害が暗号鍵制御装置で検出された場合、テナントごとにあらかじめ配信され保存されている公開鍵を用いてデータベース上のテナントの秘密情報の暗号化を行う。

【００７４】

本実施の形態によれば、テナントが２次的なＳａａＳサービス事業者に秘密情報を預託する場合、以下のことをテナントに保障することが可能となる。すなわち、データベース

管理装置２０に、信用のおける暗号鍵配信サーバ１１から、テナントのポリシーにしたがって定期的に暗号鍵を配信し、定期的に新しい暗号鍵でデータベース３０の秘密情報を暗号化する。そして、データベース接続装置２３が、データベース３０の秘密情報を復号する際、テナントが時限的なアクセスを許すポリシーで認められた範囲で、暗号鍵制御装置２２を通して暗号鍵を付与して、２次的に保持しているテナントから預託されたデータベース３０の秘密情報を復号する。これにより、テナントが時限的に、秘密情報の開示秘匿を、暗号鍵配信サーバ１１を信頼することによって実現することができる。

【００７５】

本発明の実施の形態によれば、ＳａａＳのサービス連携時のように、ＳａａＳの利用企業であるテナントの秘密情報が二次的な事業者（ＳａａＳ事業者）が所有するデータベースに渡される場合、暗号鍵を定期的に更新し、定期的に更新された暗号鍵によって秘密情報を再暗号化することにより、時限的なアクセス制御をテナントごとに決めるポリシーにしたがって行うことができる。また、ポリシーによる開示可能の確認は通信によって行われるが、通信が断絶した場合、あらかじめ配備しておいたテナントの公開鍵によって暗号化を行うため、秘密情報の漏洩の防止を保障することができる。また、秘密情報をテナントが管理し、必要になった場合に通信によりアプリケーションに供給するモデルと比べて、通信量を下げることができる。また、本発明ではポリシーにより再暗号化の暗号鍵を配信するため、再暗号化の時間間隔を変えることにより、再暗号化処理にかかる処理時間を減少させることができる。さらに、暗号化された秘密情報を消去しなくても、暗号鍵の配信停止、再配信の処理だけで、再度秘密データなどアプリケーションが必要なデータを再転送することなく、二次的なサービスでの秘密情報の利用の再開が情報漏洩を心配せず可能となる。

【００７６】

本発明の動作に用いられるプログラム、データ構造は、コンピュータ読取可能な記憶媒体に記録され、その記憶媒体から情報処理装置に読み込まれても良い。

【００７７】

本発明は上記各実施の形態に限定されず、本発明の技術思想の範囲内において、各実施の形態は適宜変形又は変更され得ることは明らかである。

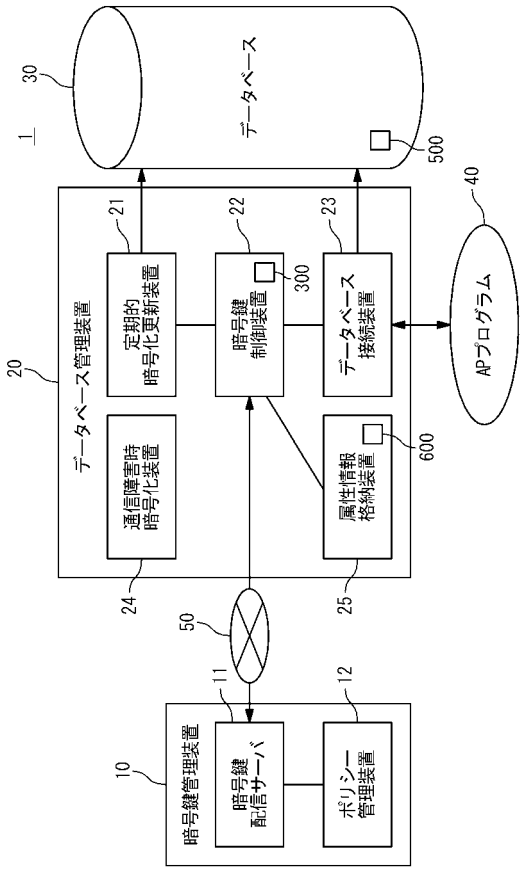
【符号の説明】

【００７８】

１　　データベース管理システム
１０　暗号鍵管理装置
１１　暗号鍵配信サーバ
１２　ポリシー管理装置
２０　データベース管理装置
２１　定期的暗号化更新装置
２２　暗号鍵制御装置
２３　データベース接続装置
２４　通信障害時暗号化装置
２５　属性情報格納装置
３０　データベース
４０　アプリケーションプログラム
５０　ネットワーク
２０１　更新暗号鍵受信装置
２０２　暗号鍵要求装置
２０３　再暗号化要求装置
２０４　暗号鍵配信装置
２０５　暗号鍵保持装置
３００　暗号鍵保持テーブル
３０１　テナントＩＤ

３０２　暗号鍵
３０３　有効期限
５００　データベース・テーブル
６００　暗号化対象フィールド指定テーブル

【図１】

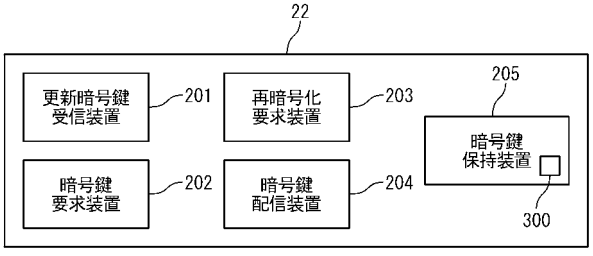


【図２】

500

テナントID	顧客名	住所
TID	CUNAME	CADRS
34859	西山庄吉	東京都目黒区洗足
49898	西山勝利	神戸市西区玉津町
34859	西山真紀子	東京都豊島区西池袋

【図３】



【図４】

300

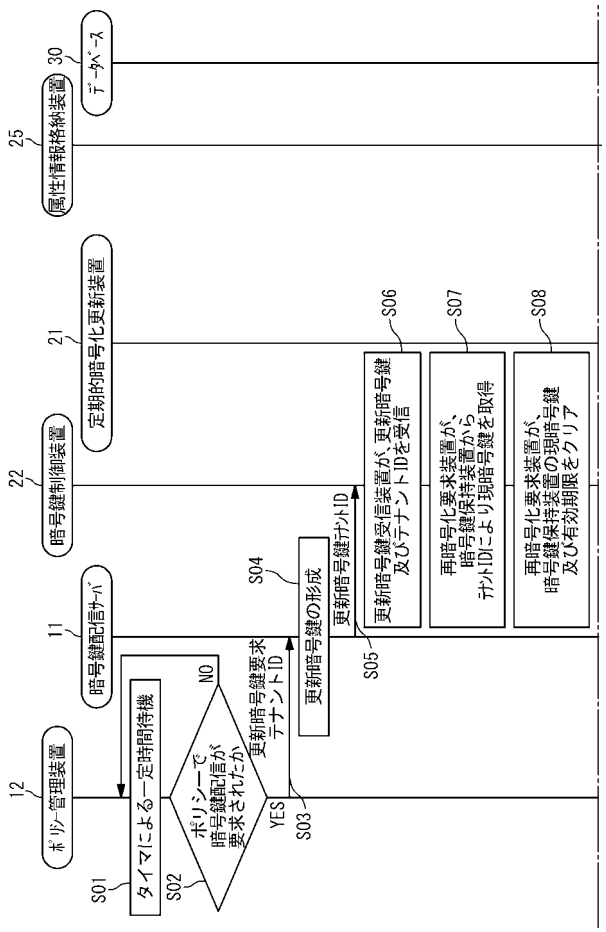
301 テナントID	302 暗号鍵	303 有効期限
242419	kdjfk4n69fcl23k2130flkvm	201210101200
34859	dg9948kjKKJK94o9tj	201210201200
49898	Dfku4tkjgpi-tOh90kl54jkth9g	201211101200

【図５】

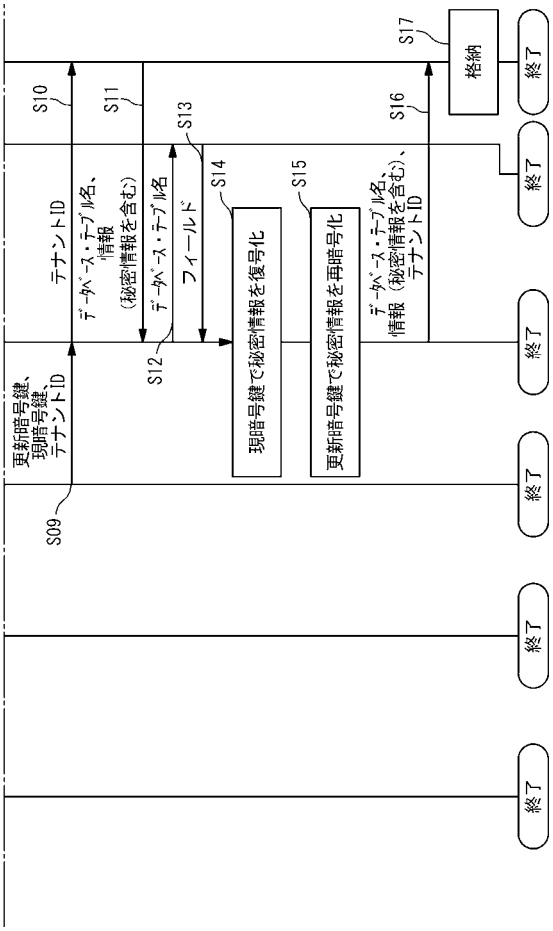
600

データベース・テーブル名	秘匿フィールド	識別IDフィールド
MASTERTBL	CADRS	TID
…	…	…
…	…	…

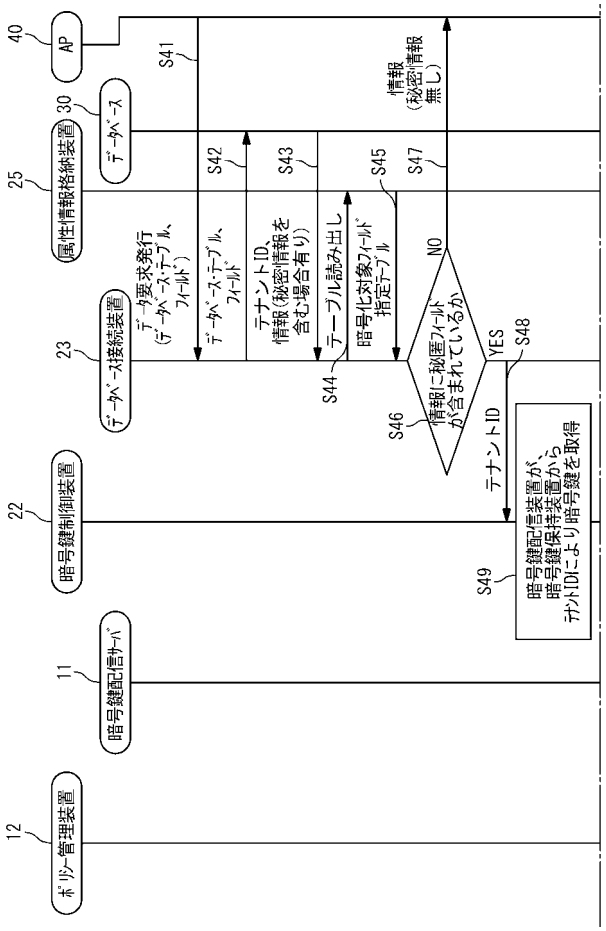
【図６Ａ】



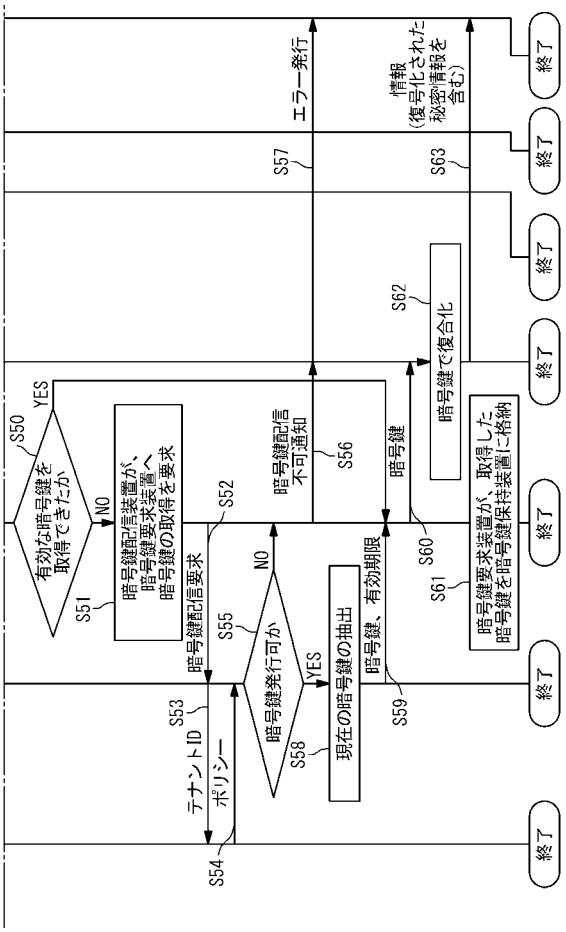
【図６Ｂ】



【図７Ａ】



【図７Ｂ】


S50
有効な暗号鍵を取得できたか
YES
NO
S51
暗号鍵配信装置が、暗号鍵要求装置へ暗号鍵の取得を要求
S52
暗号鍵配信要求
S53
テナントID
ポリシー
S54
S55
暗号鍵発行可か
NO
YES
S56
暗号鍵配信不可通知
S57
エラー発行
S58
現在の暗号鍵の抽出
S59
暗号鍵、有効期限
S60
暗号鍵
S61
暗号鍵要求装置が、取得した暗号鍵を暗号鍵保持装置に格納
S62
暗号鍵で復合化
S63
情報（復号化された秘密情報を含む）
終了
終了
終了
終了
終了
終了
終了

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	H04L 9/00 601B	