(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6226689号
(P6226689)
(45)発行日　平成29年11月8日(2017.11.8)　(24)登録日　平成29年10月20日(2017.10.20)

(51)Int.Cl.　F I
G06F 21/41 (2013.01)　G06F 21/41

請求項の数 10　(全 13 頁)

(21)出願番号　特願2013-215822(P2013-215822)
(22)出願日　平成25年10月16日(2013.10.16)
(65)公開番号　特開2015-79343(P2015-79343A)
(43)公開日　平成27年4月23日(2015.4.23)
審査請求日　平成28年10月13日(2016.10.13)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】情報処理システム、情報処理方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
ユーザー認証処理を行う異なる情報処理システムとシングルサインオン連携を行う情報処理システムであって、
前記異なる情報処理システムにより発行されシングルサインオン連携を行うために用いられる第一のグループに関する電子証明書に基づいて、当該第一のグループに属するユーザーにサービスを提供する提供手段と、
前記第一のグループに関する電子証明書と、前記第一のグループに属するユーザーが前記サービスを利用できるよう管理する役割を有する第二のグループに属するユーザーの通知先情報とを関連づけて管理する管理手段と、
前記電子証明書の有効期限までの残りの期間が所定の値を下回ったことに応じて、前記管理手段にて管理されている通知先情報の中から前記電子証明書に関連づけられた前記第二のグループに属するユーザーの通知先情報を特定し、当該特定された通知先情報に基づいて前記電子証明書の更新に関連する通知を行う通知手段と、
を有することを特徴とする情報処理システム。
【請求項２】
前記管理手段は、前記提供手段が提供するサービスの種類ごとに、サービスを利用できるように管理する役割を有する前記第二のグループに属するユーザーを関連づけて管理することを特徴とする請求項１に記載の情報処理システム。
【請求項３】

前記管理手段は、前記提供手段が提供するサービスの種類ごとに、ユーザー認証処理を行う情報処理システムを関連づけて管理することを特徴とする請求項１または２に記載の情報処理システム。
【請求項４】
前記管理手段は更に、ユーザー認証処理を行う情報処理システムごとに、前記通知手段による通知方法を関連づけて管理し、
前記通知手段は、前記通知方法に従って、通知を行うことを特徴とする請求項３に記載の情報処理システム。
【請求項５】
前記管理手段は更に、前記第一および第二のグループに属するユーザーそれぞれの役割と通知先情報とを関連づけて管理し、
前記通知手段は、前記第一および第二のグループに属するユーザーのうち、所定の役割を有するユーザーの通知先情報を特定し、当該特定された通知先情報に基づいて前記電子証明書の更新に関する通知を行うことを特徴とする請求項１乃至４のいずれか一項に記載の情報処理システム。
【請求項６】
前記所定の値として複数の値が設定されることを特徴とする請求項１乃至５のいずれか一項に記載の情報処理システム。
【請求項７】
前記通知先情報は、メールアドレスであり、
前記通知手段による通知は、前記メールアドレスを用いたメール送信により行われることを特徴とする請求項１乃至６のいずれか一項に記載の情報処理システム。
【請求項８】
前記通知手段は、電子証明書を発行する異なる情報処理システムの情報、電子証明書の有効期限、および第一のグループの情報のうちの少なくともいずれかを通知に含めることを特徴とする請求項１乃至７のいずれか一項に記載の情報処理システム。
【請求項９】
ユーザー認証処理を行う異なる情報処理システムとシングルサインオン連携を行う情報処理システムにおける情報処理方法であって、
前記異なる情報処理システムにより発行されシングルサインオン連携を行うために用いられる第一のグループに関する電子証明書に基づいて、当該第一のグループに属するユーザーにサービスを提供する提供工程と、
前記第一のグループに関する電子証明書と、前記第一のグループに属するユーザーが前記サービスを利用できるよう管理する役割を有する第二のグループに属するユーザーの通知先情報とを関連づけて管理する管理工程と、
前記電子証明書の有効期限までの残りの期間が所定の値を下回ったことに応じて、前記管理工程にて管理されている通知先情報の中から前記電子証明書に関連づけられた前記第二のグループに属するユーザーの通知先情報を特定し、当該特定された通知先情報に基づいて前記電子証明書の更新に関連する通知を行う通知工程と、
を有することを特徴とする情報処理方法。
【請求項１０】
コンピューターを、
ユーザー認証処理を行う異なる情報処理システムにより発行されシングルサインオン連携を行うために用いられる第一のグループに関する電子証明書に基づいて、当該第一のグループに属するユーザーにサービスを提供する提供手段、
前記第一のグループに関する電子証明書と、前記第一のグループに属するユーザーが前記サービスを利用できるよう管理する役割を有する第二のグループに属するユーザーの通知先情報とを関連づけて管理する管理手段、
前記電子証明書の有効期限までの残りの期間が所定の値を下回ったことに応じて、前記管理手段にて管理されている通知先情報の中から前記電子証明書に関連づけられた前記第

二のグループに属するユーザーの通知先情報を特定し、当該特定された通知先情報に基づいて前記電子証明書の更新に関連する通知を行う通知手段、
として機能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、情報処理システム、情報処理方法、及びプログラムに関し、特にクラウドサービスにおいて、シングルサインオン連携に関する電子証明書の有効期限を管理する処理に関する。
【背景技術】
【０００２】
近年、クラウド型サービスを始めとする、インターネット上に設置されたサーバーを利用し顧客にサービスを提供するビジネスが多く存在する。このようなビジネスでは複数の異なるサービスが提供され、顧客はそれらサービスの中から自身が利用したいものを選択し、必要なサービスに関する契約だけを結ぶといった契約形態が取られる。
【０００３】
このようなサービスでは、ある顧客企業にサービスを提供する場合、サービス提供側はテナントを新規に作成しその顧客企業に割り当てる。また新規作成したテナントを顧客企業側で管理するための初期ユーザーが作成され、テナントに登録される。そして、顧客企業側の管理者は、作成された初期ユーザーとしてサービスにログインし、割り当てられたテナントにユーザーを追加するほか、必要な設定を行うことで、顧客企業はサービスの利用を開始できる。
【０００４】
また、従来、異なるドメイン下に存在する複数のサーバー間で認証を連携させる技術として、Ｓｅｃｕｒｉｔｙ Ａｓｓｅｒｔｉｏｎ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（以下、ＳＡＭＬ）によるシングルサインオン（以下、ＳＳＯ）の仕組みが知られている。ＳＡＭＬを実現するシステムは、認証機能を提供するサーバー群（Ｉｄｅｎｔｉｔｙ Ｐｒｏｖｉｄｅｒ、以下、ＩｄＰ）を含む。またＩｄＰの認証結果（アサーション）を信頼して機能を提供する少なくとも一つ以上のサーバー群（Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ、以下、ＳＰ）も含む。
【０００５】
ＳＡＭＬのＳＳＯは、ＩｄＰとＳＰとの間の信頼関係によって成り立っており、そのため、ＳＳＯを実現する前に、事前にＩｄＰとＳＰとの間で信頼関係を結んでいる必要がある。この信頼関係は、ＳＡＭＬプロトコルで規定されたどの方式でＳＳＯを行うのかを記述したメタデータと、電子証明書の登録をＳＰに登録することで成立する。なお、クラウド型システムではテナント毎に上述したメタデータと電子証明書を登録する場合が一般的であり、顧客企業ごとの設定が必要となる。
【０００６】
前述の電子証明書には有効期限があり定期的に設定を更新しなければならない。この電子証明書の有効期限は２年程度とある程度長めの有効期限を設定されていることが多く、顧客企業側の設定者は更新時期において忘れずに作業することが難しい。また、本設定は作業の難易度が高いこともあり、顧客にライセンスを提供している販売店が作業を代行している場合が多い。この場合には、有効期限切れの際、販売店側から顧客に再登録の代行作業に関する確認を行いたいという要望がある。
【０００７】
従来、各顧客企業の担当者のメールアドレスを事前に登録しておき、そのメールアドレスに連絡を通知する方法が提案されている（例えば、特許文献１参照）。
【先行技術文献】
【特許文献】
【０００８】

【特許文献１】特開２００２－２２２３０６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００９】
従来の方法では以下のような課題がある。例えば、電子証明書の有効期限が長いため、顧客ごとの販売店の担当者が変わる場合がある。よって、担当者が変更される都度、通知先の設定をメンテナンスし続ける必要があるため、手間がかかる。また、通知先の設定変更を忘れると、実際に通知を要する段階ですでに担当者がおらず、通知が届かないということが生じる恐れもある。また、販売店を設定しておき、その販売店のユーザー全てに通知するという方法も考えられるが、複数サービスを扱うクラウドサービスの販売店のユーザーの中には、ＳＳＯに関係ないサービスを扱う担当者も存在するため、無駄な通知が発生してしまう。
【課題を解決するための手段】
【００１０】
上記課題を解決するために本願発明は以下の構成を有する。すなわち、ユーザー認証処理を行う異なる情報処理システムとシングルサインオン連携を行う情報処理システムであって、前記異なる情報処理システムにより発行されシングルサインオン連携を行うために用いられる第一のグループに関する電子証明書に基づいて、当該第一のグループに属するユーザーにサービスを提供する提供手段と、前記第一のグループに関する電子証明書と、前記第一のグループに属するユーザーが前記サービスを利用できるよう管理する役割を有する第二のグループに属するユーザーの通知先情報とを関連づけて管理する管理手段と、前記電子証明書の有効期限までの残りの期間が所定の値を下回ったことに応じて、前記管理手段にて管理されている通知先情報の中から前記電子証明書に関連づけられた前記第二のグループに属するユーザーの通知先情報を特定し、当該特定された通知先情報に基づいて前記電子証明書の更新に関連する通知を行う通知手段とを有する。
【発明の効果】
【００１１】
本発明によれば、電子証明書の有効期限を通知するシステムにおいて、通知先の設定を都度変更する作業を軽減し、変更忘れによる通知失敗を防止することができる。
【図面の簡単な説明】
【００１２】
【図１】システム構成例を示す図。
【図２】各装置のハードウェア構成例を示す図。
【図３】各装置のソフトウェア構成例を示す図。
【図４】本実施形態に係るテーブル構造とデータの一例を示す図。
【図５】本実施形態に係る通知先を決定し、通知を実施する処理を示すフローチャート。
【図６】通知されるメールの内容の一例を示す図。
【発明を実施するための形態】
【００１３】
以下、本発明を実施するための形態について図面を用いて説明する。
【００１４】
［システム構成］
まず、本実施形態においては、以下のサービスが、インターネット上のサーバーに設置され、提供されていることを前提として説明を行う。
・インターネット上で帳票を生成する帳票サービス
・生成した帳票を画像形成装置にて印刷するための印刷サービス
・オフィスの印刷環境を管理する管理サービス
以降、上記サービスのように、インターネット上で機能を提供しているサービスを、「リソースサービス」と呼ぶ。なお、提供されるリソースサービスはこれに限定するものではなく、他のサービスであってもよい。

【００１５】
本実施形態に係る情報処理システムは、例えば、図１に示すような構成のネットワーク上に実現される。ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）１００は、本発明ではＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）システムが構築されている。ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）１０１は各構成要素を接続する。
【００１６】
認証サーバー１１０は、認証情報を用いてユーザーの認証を行う。リソースサーバー１２０には、本実施形態では上述した帳票サービスや印刷サービス、管理サービスが設置されている。なお１台のリソースサーバーに設置されるリソースサービスは１つでもよいし、複数でもよい。また、本実施形態において各サーバーは１台ずつ設置されているが複数台で構成されていても良く、例えば、認証サーバーシステムとして提供されても良い。
【００１７】
バッチサーバー１３０は、各顧客に関するテナント情報の管理や期限切れ通知を行う。ここでテナントとは、クラウドサービスにおいて、サービスの提供の単位（グループ）を示し、例えば、１のテナントに対し、１または複数のユーザーが属することとなる。なお、本実施形態において、顧客テナントを第一のグループ、販社テナントを第二のグループとも記載する。
【００１８】
クライアント端末１５０は、Ｗｅｂブラウザ３５０がインストールされており、例えば各サーバーが提供するウェブサイトを表示することができる。ＩｄＰ（Ｉｄｅｎｔｉｔｙ　Ｐｒｏｖｉｄｅｒ）１８０は、認証サーバー１１０とは別に提供される、認証機能を備えた認証サーバーである。また、認証サーバー１１０、リソースサーバー１２０、バッチサーバー１３０、クライアント端末１５０、およびＩｄＰ１８０はそれぞれ、ＷＡＮ１００およびＬＡＮ１０１を介して接続されている。なお認証サーバー１１０、リソースサーバー１２０、バッチサーバー１３０、クライアント端末１５０、およびＩｄＰ１８０はそれぞれ、別個のＬＡＮ上に構成されていてもよいし同一のＬＡＮ上に構成されていてもよい。また認証サーバー１１０、リソースサーバー１２０、およびバッチサーバー１３０は、同一の装置上に構成されていてもよい。
【００１９】
なお、ここでの情報処理システムとは、ユーザー認証処理を行う少なくとも１台のログイン制御サーバーと、ログイン制御サーバーによるユーザー認証処理が成功したことに応じてサービスを提供するサーバーとを含むシステムを指す。しかしながら、それらのサーバーを１台に集約した形態も想定されるため、情報処理システムと称する場合、必ずしも複数台のサーバーから構成されるとは限らない。また、情報処理システムは、ログイン制御サーバーのみから構成されていても良い。
【００２０】
［ハードウェア構成］
図２は、本実施形態に係る認証サーバー１１０、リソースサーバー１２０、バッチサーバー１３０、クライアント端末１５０、およびＩｄＰ１８０のハードウェア構成例を示す図である。尚、図２に示されるハードウェア構成図は一般的な情報処理装置のハードウェアブロック図に相当するものとし、本実施形態のコンピューターには一般的な情報処理装置のハードウェア構成を適用できるものとする。
【００２１】
図２において、ＣＰＵ２３１は、ＲＯＭ２３３のプログラム用ＲＯＭに記憶された、或いはハードディスク（ＨＤ）等の外部メモリ２４１からＲＡＭ２３２にロードされたＯＳやアプリケーション等のプログラムを実行する。またＣＰＵ２３１は、システムバス２３４に接続される各ブロックを制御する。ここでＯＳとはコンピューター２００上で稼動するオペレーティングシステムの略語である。後述する各シーケンスの処理は、このプログラムの実行により実現できる。
【００２２】

ＲＡＭ２３２は、ＣＰＵ２３１の主メモリ、ワークエリア等として機能する。キーボードコントローラ（ＫＢＣ）２３５は、キーボード２３９やポインティングデバイス（不図示）からのキー入力を制御する。ＣＲＴコントローラ（ＣＲＴＣ）２３６は、ＣＲＴディスプレイ２４０の表示を制御する。ディスクコントローラ（ＤＫＣ）２３７は、各種データを記憶するハードディスク（ＨＤ）等の外部メモリ２４１におけるデータアクセスを制御する。ネットワークコントローラ（ＮＣ）２３８は、ＷＡＮ１００もしくはＬＡＮ１０１を介して接続されたコンピューターや他の機器との通信制御処理を実行する。

【００２３】

尚、後述の全ての説明においては、特に断りのない限りサーバーにおける実行のハードウェア上の主体はＣＰＵ２３１であり、ソフトウェア上の主体は外部メモリ２４１にインストールされたアプリケーションプログラムである。

【００２４】

［ソフトウェア構成］

図３は、本実施形態に係る認証サーバー１１０、リソースサーバー１２０、バッチサーバー１３０、クライアント端末１５０、およびＩｄＰ１８０それぞれのソフトウェア構成例を示す図である。なお、ここでは、本実施形態に関係するモジュールのみを示しており、他のソフトウェアモジュールを含んでいても良い。

【００２５】

認証サーバー１１０は、ユーザーがログイン処理を行うためのログインＵＩモジュール３１０、およびユーザー認証処理を行う認証モジュール３１１を備える。リソースサーバー１２０は、各種サービスを提供するリソースサーバーモジュール３２０を備える。バッチサーバー１３０は、有効期限切れ通知モジュール３３０を備える。有効期限切れ通知モジュール３３０の詳細な処理に関しては、図５を用いて説明する。クライアント端末１５０は、ＷＷＷを利用するためのユーザーエージェントであるＷｅｂブラウザ３５０を備える。ＩｄＰ１８０は、認証サーバー１１０と同様にログインＵＩモジュール３８０と認証モジュール３８１を備える。なお、認証サーバー１１０とＩｄＰ１８０との認証方法は、同じでなくてもよく、また、従来における認証処理の方法（例えば、ユーザーＩＤとパスワードの組による認証）を適用できるものとする。

【００２６】

［データ構成］

図４は、各情報を関連付け、認証サーバー１１０の外部メモリ２４１に記憶されるデータテーブルである。これらデータテーブルは、認証サーバー１１０とバッチサーバー１３０のそれぞれからアクセス可能であるとする。なお、各データテーブルは、外部メモリ２４１ではなく、ＬＡＮ１０１を介して通信可能に構成された別のサーバーに記憶するよう構成してもよい。

【００２７】

図４（ａ）は、顧客テナント管理テーブル４００の構成例を示し、顧客テナント管理テーブル４００は、顧客の１契約ごとに１顧客テナントを利用するよう顧客のテナントを管理している。顧客テナント管理テーブル４００は、顧客テナントを一意に識別するための顧客テナントＩＤ４０１、各テナントの名称を示すテナント名４０２、テナントがどのＩｄＰを利用しているのかを特定するためのＩｄＰ　ＩＤ４０３を管理する。さらには、顧客テナント管理テーブル４００は、ＩｄＰとＳＳＯ連携（シングルサインオン連携）をするための電子証明書データを示す電子証明書４０４、および電子証明書４０４の証明書有効期限４０５を含む。

【００２８】

図４（ｂ）は、ＩｄＰ管理テーブル４１０の構成例を示す。ＩｄＰ管理テーブル４１０は、ＩｄＰを一意に識別するためのＩｄＰ　ＩＤ４１１、通知（ここでは、電子証明書の期限切れの通知）を行う方法を示す通知方法４１２、および関連ライセンス４１３を含む。関連ライセンス４１３は、ＩｄＰ　ＩＤで示されるＩｄＰがどのサービス種類のライセンスに関連しているかを示す。ＩｄＰ　ＩＤ４１１には、「Ｌｏｃａｌ」もしくは各種Ｉ

ｄＰに対応した任意のＩＤ（識別情報）の値が登録される。「Ｌｏｃａｌ」の値が設定されている場合は、認証サーバー１１０自身でログイン処理を行い、情報処理システムを利用することを示し、ＳＳＯ連携していない場合に設定される。いずれかのＩｄＰに対応するＩｄＰ＿ＩＤが設定されている場合は、ＩｄＰ１８０側でログインしＳＳＯ連携により情報処理システムを利用することを示す。

【００２９】

通知方法４１２には、「テナント」もしくは「運用者」の値が設定される。「テナント」の値が設定されている場合は、電子証明書を登録している顧客テナントと、その顧客テナントにサービスを利用するためのライセンスを発行している販社テナントに対し、通知を行うことを示す。「運用者」の場合はシステムの運用者権限を持つユーザーに通知することを示す。なお、ここで示す通知方法は一例であり、ＩｄＰの管理者に通知する方法や、特定のメールアドレスに通知する方法等、その他の通知方法を適用してもよい。関連ライセンス４１３では、「Ｆｏｒｍ」「Ｐｒｉｎｔ」「ＭＤＳ」といったシステムに存在するサービスに対応するライセンスの値が設定される。本実施形態においては例えば、帳票サービスの場合は「Ｆｏｒｍ」、印刷サービスの場合は「Ｐｒｉｎｔ」、管理サービスの場合は「ＭＤＳ」がそれぞれ設定される。設定が無い場合には、ライセンスに関係なく通知を行うことを意味する。

【００３０】

図４（ｃ）は、ライセンス管理テーブル４２０の構成例を示し、ライセンス管理テーブル４２０は販売店が利用する販社テナントが、どの顧客テナントに対し、いずれのライセンスを付与しているかを管理する。ライセンスは、リソースサービスごとに存在しており、帳票サービスは「Ｆｏｒｍ」、印刷サービスは「Ｐｒｉｎｔ」、管理サービスは「ＭＤＳ」のライセンスとして管理される。

【００３１】

ライセンス管理テーブル４２０は、ライセンスを発行している販社を一意に識別するための販社テナントＩＤ４２１、ライセンスを付与されている顧客を一意に識別するための顧客テナントＩＤ４２２、発行／付与されたライセンス種類を示すライセンス４２３を含む。

【００３２】

図４（ｄ）は、ユーザー管理テーブル４３０の構成例を示し、ユーザー管理テーブル４３０は、本システムに存在する全てのユーザー情報を管理する。ユーザー管理テーブル４３０は、ユーザーを一意に識別するためのユーザーＩＤ４３１、ユーザーが所属するテナントを一意に識別するためのテナントＩＤ４３２、ユーザーのメールアドレス４３３、およびユーザーのシステム上の役割を管理するロール４３４を含む。ロール４３４には、以下のような値を保持する。

・システム運用者を表す「運用者」
・販社テナントにて管理者か一般ユーザーかを表す「販社テナント管理者」、「販社ユーザー」
・販社テナントにて各ライセンスを取り扱えることを表す「Ｆｏｒｍ販売者」「Ｐｒｉｎｔ販売者」「ＭＤＳ販売者」
・顧客テナントにて管理者か一般ユーザーかを表す「顧客テナント管理者」「顧客ユーザー」
・顧客テナントにてリソースサービスの管理者か利用者かを表す「Ｆｏｒｍ利用者」「Ｆｏｒｍ管理者」「Ｐｒｉｎｔ管理者」「Ｐｒｉｎｔ利用者」「ＭＤＳ管理者」「ＭＤＳ利用者」

【００３３】

なお、ロール４３４には、上記に示した値を１または複数設定できる。また、ロール４３４に設定される役割は上記に示したものに限定するものではない。また、本実施形態では、通知方法としてメール送信により通知を行う。そのため、通知先情報としてメールアドレスが管理されている。しかし、他の通知方法を用いても構わない。

【００３４】
図４（ｅ）は、日時管理テーブル４４０の構成例を示す。日時管理テーブル４４０は、管理する対象の日時を一意に識別するためのＩＤ４４１、日時を示す日時４４２を含む。ＩＤ４４１には例えば「証明書期限切れチェック」といった値が含まれ、システムで管理したい日時単位ごとに日時４４２を保存する。
【００３５】
［処理フロー］
図５は、電子証明書の期限切れ通知を行う際に通知先を決定し、メール通知を実施する処理を示すフローチャートである。本処理は、バッチサーバー１３０の有効期限切れ通知モジュール３３０にて実行され、１日１回定期的に実行する処理であるとして説明する。なお、実行するタイミングはこれに限定するものではなく、管理者等により設定された間隔にて定期的に実行するようにしてよい。
【００３６】
Ｓ５０１にて、バッチサーバー１３０は、各種日時の情報を取得する。まず、バッチサーバー１３０は、日時管理テーブル４４０より、前回の証明書期限切れチェックの実施日時（Ｔ１）を取得する。次に、バッチサーバー１３０は、現在の日時（Ｔ２）を取得する。そして、バッチサーバー１３０は、外部メモリ２４１で保持している期限切れ通知タイミング（ＴＩ）を取得する。通知タイミング（ＴＩ）は、例えば「３０日前」といった設定がなされ、期限までの残り期間に対する閾値として記憶部に保持されているものとする。本設定は複数持ってもよく、その場合は、Ｓ５０２～Ｓ５１２の処理をその設定数分実施することとなる。これにより、例えば、３０日前、７日前、１日前として設定された所定の閾値に対し、残りの期間が下回ったタイミングで期限切れ通知を複数回にわたって行うことが可能となる。
【００３７】
Ｓ５０２にて、バッチサーバー１３０は、期限切れ通知対象となる電子証明書を取得する。バッチサーバー１３０は、前回チェック日時（Ｔ１）＋通知タイミング（ＴＩ）の日時から、現在の日時（Ｔ２）＋通知タイミング（ＴＩ）の日時の間に有効期限が切れる電子証明書を検索する。本処理は、顧客テナント管理テーブル４００の証明書有効期限４０５を対象として検索することで実現する。
【００３８】
例えば、前回チェック日時（Ｔ１）が「２０１３／９／７　０：００」であるとする。また、現在実行日時（Ｔ２）が「２０１３／９／８／　０：００」であるとする。そして、期限切れ通知タイミング（ＴＩ）が「３０日」であるとする。以上により、
Ｔ１＋ＴＩ＝２０１３／１０／７　０：００
Ｔ２＋ＴＩ＝２０１３／１０／８　０：００
となる。したがって、バッチサーバー１３０は、２０１３／１０／７　０：００　～　２０１３／１０／８　０：００の間に期限切れとなる電子証明書を検索する。本例の場合、図４（ａ）の顧客テナント管理テーブル４００にて対象となるのは、証明書有効期限４０５が「２０１３／１０／７　１１：５３」である、顧客テナントＩＤ「１００１ＡＡ」に対応するテナントの電子証明書が合致する。よって、顧客テナントＩＤ「１００１ＡＡ」に対応するテナントに通知することが決定される。
【００３９】
Ｓ５０３は、顧客テナント分のループ処理を示す。先ほどの例では顧客テナントＩＤ「１００１ＡＡ」に対応するテナントのみが合致するとして検出されているため、顧客テナントＩＤ「１００１ＡＡ」に対応するテナントに対してＳ５０４～Ｓ５１２の処理を行うだけとなる。一方、Ｓ５０２にて複数の期限切れ通知対象テナントが検出された場合には、バッチサーバー１３０は、そのテナント数分、Ｓ５０４～Ｓ５１２の処理を繰り返すこととなる。
【００４０】
Ｓ５０４にて、バッチサーバー１３０は、ＩｄＰに対応した通知処理を判別する。図４

（ａ）に示す顧客テナント管理テーブル４００のＩｄＰ　ＩＤ４０３に基づき、ＩｄＰを特定する。本例では顧客テナントＩＤ「１００１ＡＡ」に対応するＩｄＰ　ＩＤは「ＩｄＰ－Ａ」となる。次に、図４（ｂ）に示すＩｄＰ管理テーブル４１０からＩｄＰ　ＩＤ「ＩｄＰ－Ａ」に対応する通知方法を検索し、通知方法を特定する。本例では、顧客テナントＩＤ「１００１ＡＡ」に対応する顧客テナントに対して「ＩｄＰ－Ａ」が設定されており、通知方法は「テナント」となる。Ｓ５０４にて通知方法が「テナント」である場合、Ｓ５０７の処理へ進む。

【００４１】

Ｓ５０７にて、バッチサーバー１３０は、図４（ｂ）に示すＩｄＰ管理テーブル４１０の関連ライセンス４１３より通知対象となるライセンスの取得を行う。特定のライセンスが設定されている場合はそのライセンスに関連しているとして扱い、何も設定されていない場合には、全てのライセンスに関連しているとして扱う。なお、本例では、ＩｄＰ　ＩＤ「ＩｄＰ－Ａ」の関連ライセンスは「Ｆｏｒｍ」となる。

【００４２】

Ｓ５０８にて、バッチサーバー１３０は、顧客テナントにライセンスを付与している販社テナントと、そのライセンスの種類を取得する。図４（ｃ）に示すライセンス管理テーブル４２０の顧客テナントＩＤ４２２に基づき、顧客テナントに対してライセンスを付与している販社テナントＩＤ４２１とライセンス４２３を取得する。本例では、顧客テナントＩＤ「１００１ＡＡ」に対応する顧客テナントに対し、販社テナントＩＤ「１０１ＡＡ」に対応する販社テナントが「Ｆｏｒｍ」ライセンスを付与している。また、販社テナントＩＤ「１０２ＡＡ」に対応する販社テナントが「ＭＤＳ」ライセンスを付与している。

【００４３】

Ｓ５０９にて、バッチサーバー１３０は、Ｓ５０８で取得した販社テナントとライセンスの情報に基づき、Ｓ５０７で取得した関連ライセンスを販売している販社テナントを特定し、期限切れ対象通知を行う販社テナントを決定する。本例では、「Ｆｏｒｍ」ライセンスを付与しているのは販社テナントＩＤ「１０１ＡＡ」に対応する販社テナントとなる。一方、販社テナントＩＤ「１０２ＡＡ」に対応する販社テナントが販売した「ＭＤＳ」ライセンスは関連ライセンスと異なるため、ここでは対象外となる。

【００４４】

Ｓ５０９にて、バッチサーバー１３０は、対象となる販社テナントが有るか否かを判定する。対象となる販社テナントがある場合には（Ｓ５０９にてＹＥＳ）、Ｓ５１０へ進み、無い場合には（Ｓ５０９にてＮＯ）Ｓ５１１へ進む。

【００４５】

Ｓ５１０にて、バッチサーバー１３０は、販社テナント内のユーザーのうち、Ｓ５０７で取得したライセンスを取り扱えるユーザーを特定する。本処理により、担当外のユーザーに不要な通知が行われるのを防止する。バッチサーバー１３０は、図４（ｄ）に示すユーザー管理テーブル４３０より、テナントＩＤ４３２がＳ５０９にて特定した販社テナントであり、かつ、ロール４３４にＳ５０７にて取得したライセンスを取り扱えるロールを持つユーザーを全て取得する。本例では、テナントＩＤ４３２が「１０１ＡＡ」であり、かつ、ロール４３４が「Ｆｏｒｍ販売者」であるユーザーを取得することになり、ユーザーＩＤ「ｕｓｅｒ０１@１０１ＡＡ」が通知対象ユーザーとして特定される。

【００４６】

Ｓ５１１にて、バッチサーバー１３０は、期限切れ証明書を登録している顧客テナントの管理者ユーザーを特定する。図４（ｄ）に示すユーザー管理テーブル４３０より、テナントＩＤ４３２がＳ５０２にて取得したテナントＩＤであり、かつ、ロール４３４が「顧客テナント管理者」であるユーザーを全て取得する。本例では、テナントＩＤ４３２が「１００１ＡＡ」であるユーザーＩＤ「ａｄｍｉｎ@１００１ＡＡ」が通知対象ユーザーとして特定される。

【００４７】

Ｓ５１２にて、バッチサーバー１３０は、Ｓ５１０およびＳ５１１で特定した通知ユー

ザーに対してメール通知を行う。まず、バッチサーバー１３０は、特定したユーザーＩＤに基づいて、図４（ｄ）に示すユーザー管理テーブル４３０のメールアドレス４３３よりメールアドレスを取得する。本例では、ユーザーＩＤ「ｕｓｅｒ０１@１０１ＡＡ」のメールアドレス「ｕｓｅｒ１@ａ．ａｓｌｅｓ．ｃｏ．ｊｐ」およびユーザーＩＤ「ａｄｍｉｎ@１００１ＡＡ」のメールアドレス「ａｄｍｉｎ@ｘ．ｃｕｓｔｏｍｅｒ．ｃｏ．ｊｐ」が取得される。次に、バッチサーバー１３０は、取得したメールアドレスにメールを送信する。

【００４８】

図６は、通知するメールの一例を示す。通知メール６０１は、顧客の管理者ユーザー（ロールが「顧客テナント管理者」に対応）が受け取るメールの一例である。また、通知メール６０２は、販社の担当者（ロールが「～販売者」に対応）が受け取るメールの一例である。通知メール６０１では、受信者である顧客のテナント管理者が所属する顧客テナントのＩｄＰ設定、およびそのＩｄＰの電子証明書の有効期限が記載され、電子証明書の更新を促す。通知メール６０２では、対象となる顧客のテナントＩＤやテナント名、電子証明書の有効期限が記載される。なお、上記内容に限定するものではなく、例えば、図４の各テーブルにて管理されている情報を含めるようにしてもよい。

【００４９】

一方、Ｓ５０４にて通知方法４１２が「運用者」である場合には、Ｓ５０５へ進む。Ｓ５０５にて、バッチサーバー１３０は、図４（ｄ）に示すユーザー管理テーブル４３０から、ロール４３４が「運用者」であるユーザーを特定する。本例では、ユーザーＩＤ「ｏｐｅｒａｔｏｒ@１１ＡＡ」のユーザーが特定される。

【００５０】

Ｓ５０６にて、バッチサーバー１３０は、Ｓ５０５で特定したユーザーに対してメール通知する。ここでバッチサーバー１３０は、特定したユーザーＩＤに基づいて、ユーザー管理テーブル４３０のメールアドレス４３３より対応するメールアドレスを取得し、送信する。本例では、ユーザーＩＤ「ｏｐｅｒａｔｏｒ@１１ＡＡ」のメールアドレス「ｏｐｅｒａｔｏｒ@ｓａｍｐｌｅ．ｃｏｍ」が取得され、バッチサーバー１３０は、そのアドレスにメール通知する。

【００５１】

また、Ｓ５０４にて通知方法の設定がない場合には、次の顧客テナントに対する処理に移る。

【００５２】

全て顧客テナントに対し処理が終了したら、Ｓ５１３にて、バッチサーバー１３０は、実行日時の更新を行う。具体的には、バッチサーバー１３０は、日時管理テーブル４４０の証明書期限切れチェックの日時４４２をＳ５０１で取得した現在実行日時（Ｔ２）で更新する。本処理により一度期限切れ通知した電子証明書は次回期限切れ通知から除外される。

【００５３】

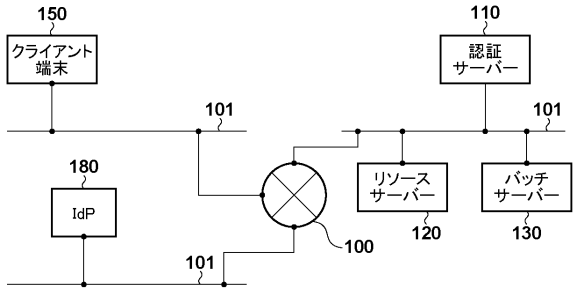
以上、本発明によれば、電子証明書の有効期限を通知するシステムにおいて、通知先の設定を都度変更する作業を軽減し、変更忘れによる通知失敗を防止することができる。また、電子証明書の期限切れ通知を適切な担当者に送信することが可能となる。

【００５４】

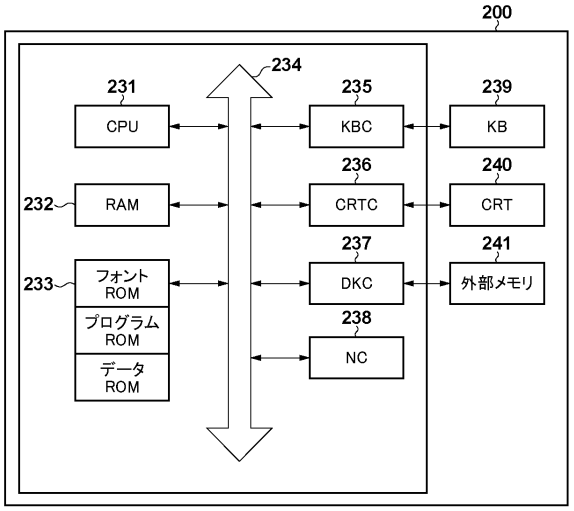
＜その他の実施形態＞

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

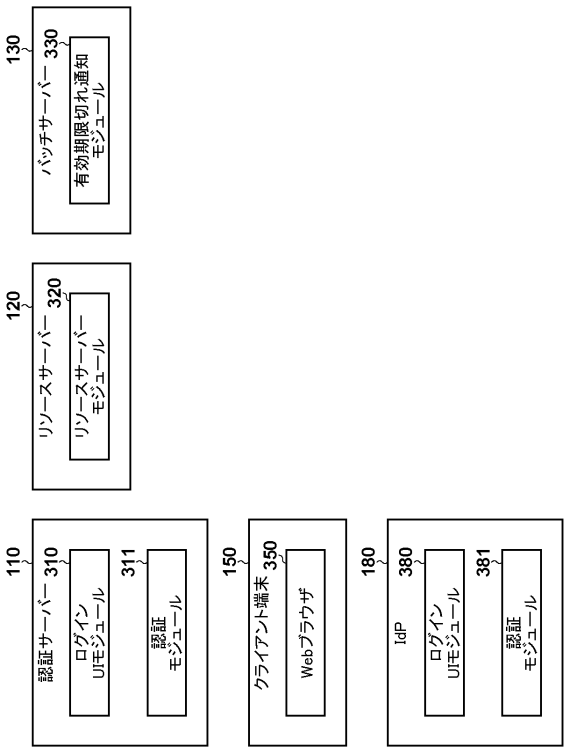
【図１】



【図２】



【図３】



【図４】

(a)

顧客テナント管理テーブル

顧客テナントID	テナント名	IdP ID	電子証明書	証明書有効期限
1001AA	X株式会社	IdP-A	Xaeigaovhio…	2013/10/7 11:53
1002AA	Y株式会社	IdP-B	ekthopqc…	2015/3/28 19:24
1003AA	Z株式会社	Local		

(b)

IdP管理テーブル

IdP ID	通知方法	関連ライセンス
Local		
IdP-A	テナント	Form
IdP-B	運用者	

ライセンス管理テーブル

販社テナントID	顧客テナントID	ライセンス
101AA	1001AA	Form
102AA	1001AA	MDS
102AA	1002AA	MDS
103AA	1003AA	MDS

(c)

ユーザー管理テーブル

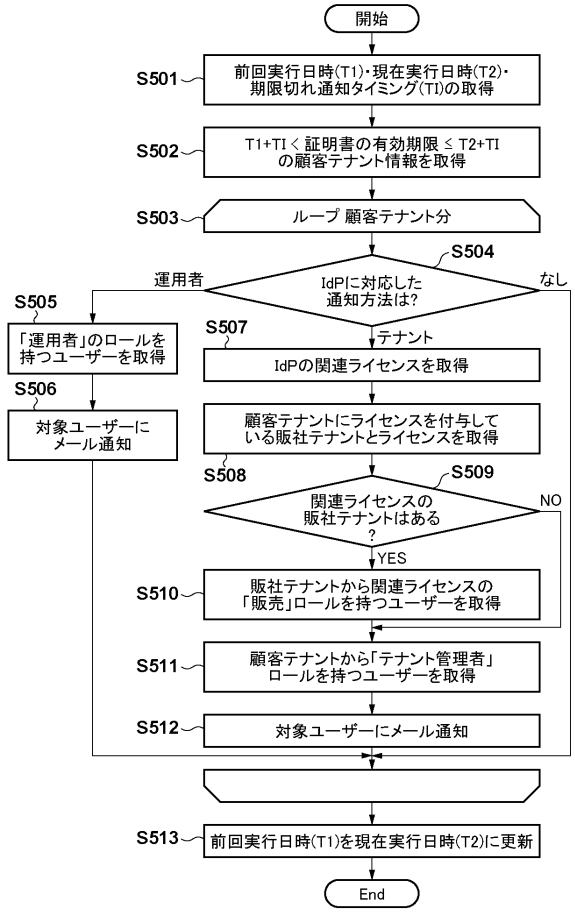
ユーザーID	テナントID	メールアドレス	ロール
operator@11AA	11AA	operator@sample.com	運用者
admin@101AA	101AA	admin@a.sales.co.jp	販社テナント管理者
user1@101AA	101AA	user1@a.sales.co.jp	販社ユーザー、Form販売者
user2@101AA	101AA	user2@a.sales.co.jp	販社ユーザー、MDS販売者
admin@102AA	102AA	admin@b.sales.co.jp	販社テナント管理者、MDS販売者
admin@103AA	103AA	admin@c.sales.co.jp	販社テナント管理者、MDS販売者
admin@1001AA	1001AA	admin@x.customer.cojp	顧客テナント管理者、Form管理者
user1@1001AA	1001AA	user1@x.customer.cojp	顧客ユーザー、Form利用者
admin@1002AA	1002AA	admin@y.customer.cojp	顧客テナント管理者
user1@1002AA	1002AA	user1@y.customer.cojp	顧客ユーザー、MDS管理者
admin@1003AA	1003AA	admin@z.customer.cojp	顧客テナント管理者
user1@1003AA	1003AA	user1@z.customer.cojp	顧客ユーザー、MDS管理者

(d)

日時管理テーブル

ID	日時
証明書期限切れチェック	2013/9/7 0:00

【図５】



【図６】

601

■件名
証明書の有効期限が近づいています

■本文
(このメールは、システムより自動送信しています。)

メニュー/機能：IDプロバイダーの登録と管理

IDプロバイダーの証明書の有効期限が近づいています。
有効期限が切れる前に、証明書ファイルを更新してください。

設定状況の詳細は、以下のURLからご確認ください。
https:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

対象のIDプロバイダー：
IDプロバイダー名：IdP-A

証明書の情報：
有効期限：2013/10/07 11:53

602

■件名
証明書の有効期限が近づいています

■本文
(このメールは、システムより自動送信しています。)

メニュー/機能：IDプロバイダーの登録と管理

お客様のIDプロバイダーの証明書の有効期限が近づいています。

対象の顧客テナント：
顧客のテナントID：1001AA
顧客の表示名：X株式会社

証明書の情報：
有効期限：2013/10/07 11:53

フロントページの続き

(72)発明者　三原　誠
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　宮司　卓佳

(56)参考文献　特開平１０－２７６１８６（ＪＰ，Ａ）
特開２００４－１７１５２５（ＪＰ，Ａ）
特開２０１１－１９２０６１（ＪＰ，Ａ）
特開２０１３－００８２２９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４１
Ｈ０４Ｌ　９／３２