(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6533292号
(P6533292)

(45)発行日　令和1年6月19日(2019.6.19)　(24)登録日　令和1年5月31日(2019.5.31)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601F
H04L	9/32	(2006.01)	H04L	9/00	675B
G09C	1/00	(2006.01)	G09C	1/00	640E

請求項の数 14　(全 30 頁)

(21)出願番号	特願2017-529776 (P2017-529776)
(86)(22)出願日	平成27年12月14日 (2015.12.14)
(65)公表番号	特表2017-537548 (P2017-537548A)
(43)公表日	平成29年12月14日 (2017.12.14)
(86)国際出願番号	PCT/US2015/065634
(87)国際公開番号	WO2016/140724
(87)国際公開日	平成28年9月9日 (2016.9.9)
審査請求日	平成29年7月25日 (2017.7.25)
(31)優先権主張番号	14/570,867
(32)優先日	平成26年12月15日 (2014.12.15)
(33)優先権主張国	米国(US)

(73)特許権者　506223509
アマゾン・テクノロジーズ、インコーポレイテッド
アメリカ合衆国、９８１０８－１２２６
ワシントン州　シアトル　ピーオー　ボックス　８１２２６
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　ボウェン、ピーター　ザチャリー
アメリカ合衆国、ワシントン州　９８１０８、シアトル　ピー．オー．ボックス　８１２２６　アマゾン　テクノロジーズ、インコーポレイテッド内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】長期デジタル証明書の検証に基づく短期デジタル証明書の発行

(57)【特許請求の範囲】

【請求項１】

実行可能命令を含んで構成された一つ以上のコンピュータシステムの制御下で、

第一のデジタル証明書をカスタマに発行することと、ここで、前記第一のデジタル証明書が、前記カスタマの検証を証明機関サービスに可能にさせる重大な拡張子を規定し、前記第一のデジタル証明書が、

前記カスタマに特有の少なくとも一つのサブジェクトフィールドを規定し、

第一の公開暗号鍵を規定し、

第一の秘密暗号鍵に対応し、かつ

前記第一のデジタル証明書についての第一の有効期間を規定し、

前記カスタマから、第二のデジタル証明書を発行するためのリクエストを受信することと、ここで、前記リクエストが、前記第一のデジタル証明書及びデジタル署名を含み、前記第二のデジタル証明書が、前記カスタマのサーバを認証するために使用可能であり、

前記第一のデジタル証明書内の規定の有効期間及び前記第一の公開暗号鍵に基づいて、前記第二のデジタル証明書を発行するか否かを決定することと、及び

前記少なくとも一つのサブジェクトフィールド、及び前記第一の有効期間よりも短い第二の有効期間を有するように前記第二のデジタル証明書を発行することと、を含み、

前記第二のデジタル証明書は、前記第一の公開暗号鍵を含む、

コンピュータ実施方法。

【請求項２】

前記カスタマの検証を証明機関サービスに可能にさせる前記重大な拡張子が、さらに、前記カスタマの前記サーバを認証するために前記第一のデジタル証明書が使用されることを阻止する、請求項１に記載のコンピュータ実施方法。

【請求項３】

前記重大な拡張子が、前記第一のデジタル証明書の発行よりも前の、前記証明機関サービスによる前記カスタマの検証の日付、前記カスタマを検証するために前記証明機関サービスによって利用される一つ以上の基準、及び前記カスタマに対応する識別子を規定する、請求項１または請求項２に記載のコンピュータ実施方法。

【請求項４】

一つ以上のサービスを実施するように構成された少なくとも一つのコンピューティングデバイスを備えたシステムであって、前記一つ以上のサービスが、

第一のデジタル証明書をカスタマに発行し、ここで、前記第一のデジタル証明書が、

前記カスタマの検証を前記一つ以上のサービスに可能にさせ、かつ

前記カスタマに特有の少なくとも一つのサブジェクトフィールドを規定し、

前記カスタマから、第二のデジタル証明書を発行するためのリクエストを受信し、ここで、前記リクエストが、前記カスタマを認証するために使用可能な前記第一のデジタル証明書及び前記第二のデジタル証明書を含み、

前記第一のデジタル証明書内の規定の情報に基づいて、前記第二のデジタル証明書を発行するか否かを決定し、かつ

前記第一のデジタル証明書内の規定の前記情報に基づく情報、及び前記カスタマに特有の前記少なくとも一つのサブジェクトフィールドを有するように前記第二のデジタル証明書を発行するように構成された、前記システム。

【請求項５】

前記第二のデジタル証明書を発行するための前記リクエストがデジタル署名を含み、かつ

前記一つ以上のサービスが、さらに、前記第一のデジタル証明書内の規定の公開暗号鍵を使用して前記デジタル署名を確認するように構成された、請求項４に記載のシステム。

【請求項６】

前記第一のデジタル証明書内の規定の前記情報が、前記第一のデジタル証明書についての有効期間を含み、かつ

前記一つ以上のサービスが、さらに、前記第一のデジタル証明書についての前記有効期間を利用して、前記第一のデジタル証明書が満期になってなく、かつ前記第二のデジタル証明書を発行するために利用できることを確認するように構成された、請求項４または請求項５に記載のシステム。

【請求項７】

前記第二のデジタル証明書の前記情報が、前記第一のデジタル証明書についての前記有効期間よりも短い有効期間を規定する、請求項６に記載のシステム。

【請求項８】

前記第二のデジタル証明書に含まれる前記情報が、さらに、前記第二のデジタル証明書を発行するための前記リクエスト内の、前記カスタマによって規定された有効期間に基づく、請求項４から請求項７の何れか一項に記載のシステム。

【請求項９】

前記第二のデジタル証明書が、さらに、前記第一のデジタル証明書内に含まれない一つ以上の追加のサブジェクトフィールドを有するように発行された、請求項４から請求項８の何れか一項に記載のシステム。

【請求項１０】

前記第一のデジタル証明書が、前記第一のデジタル証明書を認証のために使用すべきでないことを表す重大な拡張子を規定する、請求項４から請求項９の何れか一項に記載のシステム。

【請求項１１】

前記重大な拡張子が、前記第一のデジタル証明書の発行よりも前の、前記一つ以上のサービスによる前記カスタマの検証の日付、前記カスタマを検証するために前記一つ以上のサービスによって利用される一つ以上の基準、及び前記カスタマに対応する識別子を含む、請求項１０に記載のシステム。

【請求項１２】

一つ以上のサービスを実施するように構成された少なくとも一つのコンピューティングデバイスを備えたシステムであって、前記一つ以上のサービスが、

カスタマから、前記カスタマを認証するために使用可能なデジタル証明書を発行するためのリクエストを受信し、ここで、前記リクエストが、証明機関サービスが前記カスタマを検証し、かつ前記カスタマに特有の少なくとも一つのサブジェクトフィールドを規定するのに使用可能な以前に発行されたデジタル証明書を含み、

前記以前に発行されたデジタル証明書内の規定の情報に基づいて、前記デジタル証明書を発行するか否かを決定し、かつ

前記以前に発行されたデジタル証明書内の規定の前記情報に基づく情報、及び前記カスタマに特有の前記少なくとも一つのサブジェクトフィールドを有する前記デジタル証明書を発行するように構成され、

前記デジタル証明書は、前記以前に発行されたデジタル証明書内に規定されたものと同じ公開暗号鍵を含む、

前記システム。

【請求項１３】

前記システムに、前記リクエスト内の前記カスタマによって規定された所望の有効期間を取得させて、第二のデジタル証明書を発行するか否かを決定させる命令を含む、請求項１２に記載のシステム。

【請求項１４】

前記以前に発行されたデジタル証明書が、さらに、秘密暗号鍵に対応する公開暗号鍵を規定し、

前記以前に発行されたデジタル証明書内の規定の前記情報が、前記以前に発行されたデジタル証明書についての有効期間を含み、

前記システムに、前記有効期間を利用させて、前記以前に発行されたデジタル証明書が満期になってなく、かつ前記デジタル証明書を発行するために利用できることを確認させる命令を含み、かつ

前記デジタル証明書を発行するための前記リクエストが、前記公開暗号鍵に対応する前記秘密暗号鍵を利用して前記カスタマによってデジタル署名された、請求項１２に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

［関連出願の相互参照］

本願は、２０１４年１２月１５日に出願された「ＳＨＯＲＴ－ＤＵＲＡＴＩＯＮ ＤＩＧＩＴＡＬ ＣＥＲＴＩＦＩＣＡＴＥ ＩＳＳＵＡＮＣＥ ＢＡＳＥＤ ＯＮ ＬＯＮＧ－ＤＵＲＡＴＩＯＮ ＤＩＧＩＴＡＬ ＣＥＲＴＩＦＩＣＡＴＥ ＶＡＬＩＤＡＴＩＯＮ」と題された同時係属の米国特許出願第１４／５７０，８６７号からの優先権を主張し、その内容全体を参照により本明細書に組み込む。

【背景技術】

【０００２】

証明機関は、通常、カスタマが他のエンティティとの安全な通信を確立でき、かつこれらの他のエンティティがこれらのカスタマを認証できるデジタル証明書をカスタマに発行する。デジタル証明書をカスタマに発行するために、証明機関は、政府データベース、第三者データベース及びサービスを調査するならびに他のカスタマ技術によって、カスタマに関する情報を検証する必要があり得る。カスタマに関する情報を証明機関が検証できる

場合には、証明機関は、デジタル証明書を生成してカスタマに発行することができる。しかしながら、そのような検証技術は、時間及び資源について大規模な活動であり得る。故に、複数のデジタル証明書についてのリクエストは、これらのデジタル証明書を取得するのに必要な費用及び時間が相当量になり得るので、望ましくない場合がある。

【０００３】

本開示に従うさまざまな実施形態を、図面を参照して記載する。

【図面の簡単な説明】

【０００４】

【図１】さまざまな実施形態を実施できる環境の例証となる実施例を示す。

【図２】少なくとも一つの実施形態に従う、証明機関サービスのさまざまな構成要素が集合的に長期デジタル証明書及び短期デジタル証明書をカスタマに発行するように構成された環境の例証となる実施例を示す。

【図３】少なくとも一つの実施形態に従う、証明機関サービスが有効な長期デジタル証明書の受信時に短期デジタル証明書をカスタマに発行する環境の例証となる実施例を示す。

【図４】少なくとも一つの実施形態に従う、ユーザクライアントがカスタマサーバから受信した長期デジタル証明書を拒否する環境の例証となる実施例を示す。

【図５】少なくとも一つの実施形態に従う、ユーザクライアントがカスタマサーバから受信した短期デジタル証明書を利用してカスタマサーバを認証できる環境の例証となる実施例を示す。

【図６】少なくとも一つの実施形態に従う、長期デジタル証明書及び短期デジタル証明書を証明機関サービスから受信するためのプロセスの例証となる実施例を示す。

【図７】少なくとも一つの実施形態に従う、長期デジタル証明書を発行するためのカスタマリクエストに応答して、長期デジタル証明書を生成して発行するためのプロセスの例証となる実施例を示す。

【図８】少なくとも一つの実施形態に従う、カスタマリクエストに応答して、長期デジタル証明書を利用してカスタマを認証して一つ以上の短期デジタル証明書を発行するためのプロセスの例証となる実施例を示す。

【図９】少なくとも一つの実施形態に従う、デジタル証明書を利用してカスタマサーバを認証するためのプロセスの例証となる実施例を示す。

【図１０】さまざまな実施形態を実施できる環境の例証となる実施例を示す。

【発明を実施するための形態】

【０００５】

以下の記載においてさまざまな実施形態を記載する。説明を目的として、実施形態の徹底的な理解を提供するために、具体的な構成及び詳細を説明する。しかしながら、具体的な詳細がなくても実施形態を実践できることも当業者に明らかである。さらに、記載されている実施形態を曖昧にしないために、周知の特徴は省略または簡略化することがある。

【０００６】

本明細書に記載及び提案される技術は、サーバ認証のための短期デジタル証明書をリクエスト及び取得するのに利用できる長期証明書の発行に関する。実施形態において、エンティティ（例えば、組織のコンピューティングデバイス）は、長期デジタル証明書の発行をリクエストするために、サービスを対象とする一つ以上のアプリケーションプログラミングインターフェース（ＡＰＩ）コールなどを通じて、証明機関サービスと通信する。エンティティは、さまざまなカスタマが他のエンティティとの安全な通信チャネルを確立でき、かつこれらの他のエンティティが発行されたデジタル証明書の使用を通じてこれらのさまざまなカスタマを認証できるデジタル証明書をこれらのさまざまなカスタマに発行するように構成できる証明機関サービスのこれらのカスタマに関連付くことができる。長期デジタル証明書は、（例えば、１年以上の）長い有効期間をもって発行でき、そして重大としてマークできる拡張子を含むことができる。この重大な拡張子は、ユーザクライアントが重大な拡張子を認識できないように構成されるまたはこの重大な拡張子を拒否するように構成できるので、これらのユーザクライアント（例えば、ユーザコンピューティング

デバイスにインストールされたブラウザアプリケーション）がこの長期デジタル証明書を承認することを阻止することができる。

【０００７】

証明機関サービスがエンティティを検証して長期デジタル証明書をエンティティに発行できることを保証すると、証明機関サービスは、この長期証明書をエンティティまたはエンティティのサーバに発行することができる。エンティティは、長期デジタル証明書の受信時に、ユーザクライアントとの安全な通信チャネルを確立するのに利用できる短期デジタル証明書をリクエストすることができる。例として、実施形態において、証明機関サービスは、エンティティから、長期デジタル証明書、及び短期デジタル証明書を発行するためのリクエストを受信する。証明機関サービスは、エンティティを認証するために長期デジタル証明書内の規定の情報を確認し、確認すると、短期デジタル証明書をエンティティに発行することができる。短期デジタル証明書は、長期デジタル証明書よりも短い有効期間（例えば、数日、数カ月など）を有することができる。さらに、証明機関サービスは、長期デジタル証明書の残存有効期間に基づいてこの有効期間を決定することができる。例えば、長期デジタル証明書についての残存有効期間が３カ月である場合には、証明機関サービスは、３カ月を超えない有効期間をもつ短期デジタル証明書を発行することができる。

【０００８】

実施形態において、エンティティが証明機関サービスから短期デジタル証明書を取得すると、エンティティは、安全な通信チャネルを確立するためのこの短期デジタル証明書をユーザクライアントに提供することができる。ユーザクライアントは、短期デジタル証明書の受信時に、短期デジタル証明書の評価を通じてエンティティの身元を確認し、そして証明機関サービスから取得した公開暗号鍵の使用を通じて短期デジタル証明書内に含まれるデジタル署名を確認することができる。これによりユーザクライアントは、短期デジタル証明書が、証明機関サービスによって発行されたものであり、故に、有効であることを確認することができる。この短期デジタル証明書の利用によって、ユーザクライアントは、エンティティの公開暗号鍵を取得し、この公開暗号鍵を利用して、データを暗号化して安全な通信チャネルを通じてエンティティに伝送することができる。

【０００９】

このようにして、エンティティは、各短期デジタル証明書の発行前に実行される大規模な検証プロセスの必要なく、以前に発行された長期デジタル証明書に基づいて、証明機関サービスから複数の短期デジタル証明書を取得することができる。加えて、本明細書に記載及び提案される技術は、追加の技術的利点を促進する。例えば、いくつかの実施形態では、ユーザクライアントが認識できないか、かつ／またはユーザクライアントに長期デジタル証明書を拒否させる拡張子を長期デジタル証明書が含むので、長期デジタル証明書が信用できないとされた事象時に、エンティティが新規の長期デジタル証明書の発行を無効及びリクエストする必要をもはやなくすことができる。さらに、短期デジタル証明書が信用できないとされた場合に、エンティティは、この短期デジタル証明書を無効にし、検証プロセス全体をもう一度行う必要なく、発行された長期デジタル証明書を利用して証明機関サービスから新規の短期デジタル証明書を取得することができる。

【００１０】

図１は、さまざまな実施形態を実施できる環境１００の例証となる実施例を示す。環境１００において、証明機関サービス１０２は、カスタマによる公開暗号鍵（例えば、デジタル証明書内で識別されるような、名付けられたサブジェクト）の所有を証明できる一つ以上のデジタル証明書の発行を証明機関サービス１０２のカスタマがリクエストできる証明機関システムを提供できる。これらの一つ以上のデジタル証明書によって、ユーザクライアント１０６などの他のエンティティ（例えば、ブラウザアプリケーション）が、カスタマの身元を確認し、カスタマとの安全な通信チャネルを確立することによって暗号化された及び暗号化されていないデータを伝送することができる。実施形態において、証明機関サービス１０２は、長期デジタル証明書が未だ有効である限り、後に短期デジタル証明

書を発行するために利用できる長期デジタル証明書についてのリクエストをカスタマから受信する。

【００１１】

証明機関サービス１０２は、長期証明書を発行するためのリクエストをカスタマから受信すると、カスタマが信用でき、かつ証明機関サービス１０２からデジタル証明書を取得する権限をカスタマに与えることを保証するための一つ以上の検証プロセスを実行することができる。例として、証明機関サービス１０２は、一つ以上の政府機関、第三者データベースまたは任意の他の信用がある情報リポジトリにアクセスしてカスタマを評価し、カスタマがそう称する者であり、かつカスタマがデジタル証明書について適切に吟味されたことを保証することができる。カスタマが証明機関サービス１０２によって適切に吟味された場合には、証明機関サービス１０２は、より短い期限の短期デジタル証明書を取得するのに使用される長期デジタル証明書をカスタマに発行することができる。いくつかの実施形態では、長期デジタル証明書は、デジタル証明書の発行者、証明書についての有効期間、サブジェクト（例えば、カスタマ）、サブジェクトの公開暗号鍵、及び証明機関サービス１０２のデジタル署名を規定できるＸ．５０９証明書である。しかしながら、この長期デジタル証明書は、さらに、長期デジタル証明書が検証目的のみのために利用されることを表すことができる重大な拡張子を規定することができる。この重大な拡張子は、いくつかのユーザクライアント１０６には認識されず、結果として、これらのユーザクライアント１０６によって自動的に拒否され得る。あるいは、ユーザクライアント１０６は、この重大な拡張子を含むあらゆるデジタル証明書を拒否するように構成できる。

【００１２】

カスタマがこの長期デジタル証明書を証明機関サービス１０２から受信すると、カスタマは、一つ以上のカスタマサーバ１０４を通じて、ユーザクライアント１０６との安全な通信チャネルを確立するのに使用可能であり、かつユーザクライアント１０６がカスタマサーバ１０４を認証できる一つ以上の短期デジタル証明書を取得するためのリクエストを証明機関サービス１０２に提示することができる。証明機関サービス１０２へのリクエストは、前述の長期デジタル証明書を含むことができる。一つ以上のカスタマサーバ１０４からリクエストを受信すると、証明機関サービス１０２は、長期デジタル証明書を評価して、カスタマの身元を確認し、長期デジタル証明書が未だ有効であることを保証できる。実施形態において、リクエストは、証明機関サービス１０２が長期デジタル証明書を最初に発行したのと同じエンティティに証明機関サービス１０２が一つ以上の短期デジタル証明書を発行していることを確実にするために、長期デジタル証明書内に規定された公開暗号鍵に対応するカスタマの秘密暗号鍵を使用してデジタル署名されたものであっても良い。証明機関サービス１０２は、長期デジタル証明書の公開暗号鍵を使用してデジタル署名を確認することができる。

【００１３】

証明機関サービス１０２は、リクエストを提供したカスタマの身元を確認すると、長期デジタル証明書を評価して、このデジタル証明書についての残存有効期間を決定することができる。証明機関サービス１０２は、この情報を利用して、一つ以上の短期デジタル証明書内に規定であり得る有効期間を確立することができる。例として、長期デジタル証明書についての残存有効期間が３カ月である場合には、証明機関サービス１０２は、長期デジタル証明書において規定された残存３カ月期間を超えない有効期間を有する短期デジタル証明書を発行することができる。あるいは、カスタマは、リクエストを通じて、提供された長期デジタル証明書の残存有効期間を所望の有効期間が超えない限り、短期デジタル証明書についての所望の有効期間を指定することができる。

【００１４】

証明機関サービス１０２は、長期デジタル証明書内に規定されたのと同じ公開暗号鍵を含むように短期デジタル証明書を生成することもできる。これにより短期デジタル証明書が長期デジタル証明書についてのプロキシとしての機能を果たし、ユーザクライアント１０６または他のエンティティにアクセスできるようにすることができる。例として、長期

デジタル証明書は、スマートカード、バッジ、または長期デジタル証明書内に格納できた他のデバイスなどの物理的実装を通じてカスタマに発行することができる。カスタマは、リモート位置において、コンピューティングデバイスを通じてスマートカード、バッジまたは他のデバイスを証明機関サービス１０２に提示することができる。スマートカードまたは他のデバイス内の長期デジタル証明書の解析に少なくともある程度基づいて、より短い期間有効であり得る短期デジタル証明書をカスタマに発行することができる。これによりカスタマは、リモート位置において自身の時間の間のみ有効であり得る、この新規に発行された短期デジタル証明書を利用してこのリモート位置においてアクセスすることができる。代替的な実施形態において、短期デジタル証明書は、さらに、長期デジタル証明書内に規定されたものとは異なるカスタマ暗号鍵を規定することができる。これによりカスタマは、長期デジタル証明書内の規定のカスタマ暗号鍵を公開することなく、信用できない場合に短期デジタル証明書を無効にすることができる。

【００１５】

カスタマが一つ以上のカスタマサーバ１０４を通じて一つ以上の短期デジタル証明書を証明機関サービス１０２から受信すると、カスタマサーバ１０４は、ここで、受信した一つ以上の短期デジタル証明書とともにデータを一つ以上のユーザクライアント１０６に伝送することができる。ユーザクライアント１０６は、一つ以上の短期デジタル証明書内の規定の証明機関サービス１０２のデジタル署名を確認するのに使用できる暗号鍵ペアの公開暗号鍵を証明機関サービス１０２から取得することができる。証明機関サービス１０２のデジタル署名が本物であると確認された場合には、ユーザクライアント１０６は、一つ以上の短期デジタル証明書が有効であることを決定し、故に、これらを使用して一つ以上のカスタマサーバ１０４の身元を確認し、確認された場合に、短期デジタル証明書内の規定のカスタマの公開暗号鍵を利用することができる。例として、デジタル署名された（例えば、カスタマの秘密暗号鍵を利用した）データをユーザクライアント１０６に伝送するのにカスタマサーバ１０４が利用される場合には、ユーザクライアント１０６は、短期デジタル証明書内に規定されたものとしてカスタマの公開暗号鍵を利用して、カスタマのデジタル署名を確認して、伝送されたデータが有効であるか否かを決定することができる。故に、ユーザクライアント１０６は、カスタマサーバ１０４に安全に情報を伝送するのに利用できる。

【００１６】

前述したように、カスタマは、証明機関サービスと通信して、短期デジタル証明書の取得において検証目的に利用できる長期デジタル証明書の発行をリクエストすることができる。さらに、カスタマは、一つ以上のカスタマサーバを通じて、証明機関サービスから、その後にユーザクライアントが一つ以上のカスタマサーバを認証するのに使用できるこれらの短期デジタル証明書をリクエストすることができる。これらの短期デジタル証明書についてのリクエストは、証明機関サービスがカスタマを認証するのに利用できる長期デジタル証明書を含むことができる。それに応じて、図２は、少なくとも一つの実施形態に従う、証明機関サービス２０２のさまざまな構成要素が集合的に長期デジタル証明書及び短期デジタル証明書をカスタマ２１２に発行するように構成された環境２００の例証となる実施例を示す。

【００１７】

証明機関サービス２０２は、カスタマ２１２が証明機関サービス２０２にアクセスできるインターフェース２０４をこれらのカスタマ２１２に提供することができる。カスタマ２１２は、インターネットなどの一つ以上の通信ネットワークを通じてインターフェース２０４を利用することができる。インターフェース２０４は、カスタマ２１２が証明機関サービス２０２にアクセスする権限を有することを保証する特定のセキュリティセーフガードを含むことができる。例として、証明機関サービス２０２にアクセスするために、カスタマは、インターフェース２０４を使用するときにユーザ名及び対応するパスワードまたはエンクリプションキーを提供する必要があり得る。加えて、インターフェース２０４に提示されたリクエスト（例えば、ＡＰＩコール）は、権限付与システム（図示せず）な

どの証明機関サービス２０２によって電子署名を確認可能なように、暗号鍵を使用して生成された電子署名を要求する場合がある。

【００１８】

インターフェース２０４を通じて、カスタマ２１２は、長期デジタル証明書を発行するためのリクエストを一つ以上のカスタマ２１２サーバに提示することができる。前述したように、後に、証明機関サービス２０２が、カスタマ２１２を認証し、短期デジタル証明書をカスタマ２１２サーバに発行できる長期デジタル証明書を利用することができる。長期デジタル証明書を発行するためのリクエストは、例えば、カスタマ２１２の名前、住所、収入情報などのカスタマ２１２に関する情報を含むことができる。さらに、インターフェース２０４を通じて、カスタマ２１２は、その後長期デジタル証明書内に規定され得る、長期デジタル証明書についての有効期間を規定することができる。

【００１９】

長期デジタル証明書を発行するためのカスタマ２１２のリクエストを証明機関サービス２０２が受信すると、インターフェース２０４は、リクエストを処理し、カスタマ２１２に長期デジタル証明書が発行できるか否かを決定するように構成できる管理サブシステム２０６にリクエストを伝送することができる。例として、管理サブシステム２０６は、政府機関データベース及び他の第三者データベースにアクセスして、リクエストとともに提供されたカスタマ２１２情報に少なくともある程度基づいて、カスタマ２１２に長期デジタル証明書が発行できるか否かを決定するように構成できる。例えば、管理サブシステム２０６が第三者データベース内の規定の情報に少なくともある程度基づいてカスタマ２１２が信用できないことを決定した場合には、管理サブシステム２０６は、長期デジタル証明書についてのカスタマ２１２のリクエストを拒絶することができる。カスタマ２１２に長期デジタル証明書を発行できることを管理サブシステム２０６が決定した場合には、管理サブシステム２０６は、カスタマ２１２の情報をカスタマプロファイルリポジトリ２１０内に保存することができる。さらに、管理サブシステム２０６は、証明書データストア２０８にアクセスして、長期デジタル証明書を生成するのに利用できる証明書テンプレートを取得することができる。例として、管理サブシステム２０６は、証明書データストア２０８からＸ．５０９デジタル証明書テンプレートを取得し、このテンプレートを利用してカスタマ２１２についての長期Ｘ．５０９デジタル証明書を生成することができる。管理サブシステム２０６は、インターフェース２０４を通じて、新規に生成された長期デジタル証明書をカスタマ２１２に提供することができる。

【００２０】

実施形態において、管理サブシステム２０６は、長期デジタル証明書内に、ユーザクライアントが認識できないまたはユーザクライアントによって拒否され得る重大な拡張子を規定する。例として、重大な拡張子は、カスタマ２１２を認証するためにデジタル証明書を利用できないことをユーザクライアントに信号で送ることができる「検証のみ」拡張子であっても良い。この重大な拡張子は、検証を実行した日付、カスタマ２１２検証に使用された基準もしくは要件、及び／または検証が実行された、証明機関サービス２０２のカスタマ２１２の識別子などのカスタマ２１２を認証するために実行された一つ以上の検証についての情報を含むことができる。

【００２１】

後に、カスタマ２１２は、一つ以上のカスタマ２１２サーバを通じて、インターフェース２０４に再度アクセスし、ユーザクライアントとの安全な通信チャネルを確立し、かつユーザクライアントがカスタマ２１２を認証するのに使用できる一つ以上の短期デジタル証明書の作製をリクエストすることができる。リクエストは、カスタマ２１２に以前に発行された長期デジタル証明書を含むことができる。さらに、いくつかの実施形態では、リクエストは、最初の長期デジタル証明書内の規定の公開暗号鍵に対応し得る、カスタマ２１２の秘密暗号鍵を使用してカスタマ２１２によってデジタル署名することができる。リクエストの受信時に、管理サブシステム２０６は、長期デジタル証明書を評価して、長期デジタル証明書についての残存有効期間を決定することができる。例として、長期デジタ

ル証明書は、長期デジタル証明書についての開始日及び満期日を規定する有効期間フィールドを含むことができる。指定の満期日に少なくともある程度基づいて、管理サブシステム２０６は、長期デジタル証明書についての残存有効期間を計算することができる。

【００２２】

加えて、リクエストがカスタマ２１２によってデジタル署名されている場合には、管理サブシステム２０６は、カスタマプロファイルリポジトリ２１０にアクセスして、リクエストに含まれるデジタル署名を確認し、受信したリクエストが有効であることを保証するのに使用できる、この特定のカスタマ２１２に対応する暗号鍵を取得することができる。管理サブシステム２０６が長期デジタル証明書内の規定の情報に少なくともある程度基づいてカスタマ２１２がそう称する者であることを決定した場合には、管理サブシステム２０６は、証明書データストア２０８にアクセスして、リクエストされた一つ以上の短期デジタル証明書を生成するのに使用できるデジタル証明書テンプレートを取得することができる。一つ以上の短期デジタル証明書は、特定の規定の情報を除いて、長期デジタル証明書と同様のものであっても良い。例として、短期デジタル証明書は、長期デジタル証明書についての残存有効期間以下の有効期間を指定することができる。例として、長期デジタル証明書についての残存有効期間が３カ月である場合には、管理サブシステム２０６は、短期デジタル証明書内において、短期デジタル証明書についての有効期間を３カ月以下の任意の値に指定することができる。故に、短期デジタル証明書についての満期日は、長期デジタル証明書の満期日と一致しても良いし、長期デジタル証明書の満期日より早くても良い。

【００２３】

さらに、短期デジタル証明書は、長期デジタル証明書内の規定の重大な拡張子を含まなくても良い。これによりユーザクライアントは、短期デジタル証明書を利用してカスタマ２１２を認証し、かつユーザクライアントは、カスタマ２１２と安全に通信することができる。いくつかの実施形態では、管理サブシステム２０６は、最初の、長期デジタル証明書内の規定の暗号鍵の代わりとなるカスタマ２１２暗号鍵を規定する短期デジタル証明書を生成することができる。これは、長期デジタル証明書、故に、最初のカスタマ２１２暗号鍵が、短期デジタル証明書の違反の結果として信用できなくなり得る可能性の減少を支援することができる。

【００２４】

管理サブシステム２０６がカスタマ２１２リクエストに応答して一つ以上の短期デジタル証明書を生成すると、管理サブシステム２０６は、カスタマプロファイルリポジトリ２１０内のカスタマ２１２のプロファイルにアクセスして、発行された短期デジタル証明書の数、対応するカスタマ２１２暗号鍵、及び後にカスタマ２１２に代わってデジタル証明書を生成するのに有用となり得る任意の他の情報を特定することができる。管理サブシステム２０６は、インターフェース２０４を通じて、これらの短期デジタル証明書をユーザクライアントに提供できるカスタマ２１２にこれらの短期デジタル証明書を発行し、これによりこれらのユーザクライアントは、カスタマ２１２を認証し、安全な通信チャネルを通じてデータを安全にカスタマ２１２に伝送できる。さらに、これらの短期デジタル証明書によって、カスタマ２１２は、自身のデータをデジタル署名し、ユーザクライアントに伝送されるデータを暗号化することができる。

【００２５】

前述したように、カスタマは、以前に発行された長期デジタル証明書を含むリクエストを証明機関サービスに伝送して、ユーザクライアントが短期デジタル証明書を利用してカスタマを認証できるような、これらのユーザクライアントに伝送できる一つ以上の短期デジタル証明書を取得することができる。それに応じて、図３は、少なくとも一つの実施形態に従う、証明機関サービス３０４が有効な長期デジタル証明書３０６の受信時に短期デジタル証明書３０８をカスタマ３０２に発行する環境３００の例証となる実施例を示す。環境３００において、カスタマ３０２は、一つ以上の短期デジタル証明書３０８を発行するための証明機関サービス３０４へのリクエストの一部として、証明機関サービス３０４

によってカスタマ３０２に以前に発行された長期デジタル証明書３０６を提供することができる。前述したように、長期デジタル証明書３０６は、開始日（例えば、図３に例証するような「以後」フィールド）、及び満期日（例えば、図３に例証するような「以前」フィールド）を含むことができる有効期間を規定することができる。この有効期間は、長期デジタル証明書３０６が有効である継続期間を規定することができる。さらに、この有効期間によって、証明機関サービス３０４は、長期デジタル証明書３０６についての残存有効期間を決定できる。例として、証明機関サービス３０４は、満期日ならびに当日の日付及び時刻を利用して、長期デジタル証明書３０６についての残存有効期間を計算することができる。

【００２６】

長期デジタル証明書３０６は、ユーザクライアントがカスタマ３０２を認証するために長期デジタル証明書３０６を使用することを阻止するために利用できる重大な拡張子も含むことができる。例として、図３に例証するように、長期デジタル証明書３０６は、識別子「検証のみ　タイプ－１．０１」をもつ拡張子を規定することができる。この特定の拡張子は、ユーザクライアントが、重大な拡張子を認識しない場合に、長期デジタル証明書３０６を拒否しなければならないことを意味する重大としてマークすることができる。さらに、ユーザクライアントがこの重大な拡張子を認識するように更新されるときには、ユーザクライアントは、この重大な拡張子を含む任意の長期デジタル証明書３０６を承認しないように構成できる。故に、カスタマ３０２は、その身元を、この長期デジタル証明書３０６を簡単に利用するユーザクライアントにアサートすることはできない。

【００２７】

前述したように、一つ以上の短期デジタル証明書３０８を取得するためのリクエストをカスタマ３０２が証明機関サービス３０４に提示するときには、カスタマ３０２は、以前に発行された長期デジタル証明書３０６を証明機関サービス３０４に提供することができる。証明機関サービス３０４は、長期デジタル証明書３０６を評価して、長期デジタル証明書３０６が未だ有効であることを保証することができる。さらに、証明機関サービス３０４は、一つ以上のサブジェクトフィールド（図示せず）を評価して、カスタマ３０２がそう称する者であることを確認することができる。例として、一つ以上のサブジェクトフィールドは、カスタマ３０２の所与の名及び姓、カスタマ３０２の組織名及び／または部署、組織が位置し得る州、省及び国、カスタマ３０２についてのコモンネーム（例えば、ＵＲＬ）、または他のエンティティなどを規定することができる。実施形態において、カスタマ３０２は、短期デジタル証明書３０８が、長期デジタル証明書３０６を発行したのと同じカスタマ３０２に発行することを確実にするために、長期デジタル証明書３０６内に含まれる暗号鍵を利用して証明機関サービス３０４へのリクエストをデジタル署名する。

【００２８】

証明機関サービス３０４が長期デジタル証明書３０６の使用を通じてカスタマ３０２を認証すると、証明機関サービス３０４は、一つ以上の短期デジタル証明書３０８を生成してカスタマ３０２に発行することができる。これらの一つ以上の短期デジタル証明書３０８は、少しの代わりのエントリを除いて、長期デジタル証明書３０６と同様のものであっても良い。例として、図３に例証するように、短期デジタル証明書３０８についての有効期間は、長期デジタル証明書３０６内の規定の有効期間よりも短い。例えば、証明機関サービス３０４は、短期デジタル証明書３０８が生成された日付と等しい開始日を規定することができる。あるいは、短期デジタル証明書３０８についての開始日は、カスタマ３０２への短期デジタル証明書３０８の発行の日付よりも遅く、かつ長期デジタル証明書３０６内の規定の満期日よりも前の日付として規定することができる。

【００２９】

実施形態において、短期デジタル証明書３０８は、カスタマ３０２または長期デジタル証明書３０６の同じサブジェクトフィールド内の規定の他のエンティティに特有の少なくとも一つのサブジェクトフィールドを含むように生成される。例として、短期デジタル証

明書３０８は、長期デジタル証明書３０６内の規定のものとして、同じ組織名、組織位置（例えば、州、省、国）、及びコモンネーム（例えば、ＵＲＬ）を規定することができる。いくつかの実施形態では、短期デジタル証明書３０８は、さらに、長期デジタル証明書３０６内に規定されていない追加のサブジェクトフィールドを含むことができる。例として、短期デジタル証明書３０８は、これらの追加のサブジェクトフィールドの一つ以上を通じて、短期デジタル証明書３０８が生成されたカスタマ３０２に関連付けられた委託されたエンティティの身元を特定することができる。加えて、短期デジタル証明書３０８内に含まれる一つ以上の追加のサブジェクトフィールドは、短期デジタル証明書３０８を利用できる第二の位置（例えば、州、省、国）を規定することができる。

【００３０】

短期デジタル証明書３０８の満期日は、長期デジタル証明書３０６内の規定の満期日及び／またはカスタマ３０２リクエストに少なくともある程度基づいて、証明機関サービス３０４によって規定することができる。例として、図３に例証するように、短期デジタル証明書３０８内の規定の満期日は、長期デジタル証明書３０６内の規定の満期データよりも早い。短期デジタル証明書３０８についての有効期間は、短期デジタル証明書３０８についての有効期間が長期デジタル証明書３０６についての残存有効期間を超えない限り、証明機関サービス３０４またはリクエストを通じてカスタマ３０２によって規定することができる。

【００３１】

短期デジタル証明書３０８は、ユーザクライアントによるデジタル証明書の使用を阻止する、長期デジタル証明書３０６内に含まれる重大な拡張子を含まなくても良い。例として、図３に例証するように、短期デジタル証明書３０８は、拡張子「検証のみ　タイプ－１．０１」を含まない。代わりに、短期デジタル証明書３０８内の規定の拡張子によって、ユーザクライアントは、カスタマ３０２を認証する及び他の目的（例えば、データ検証、データ復号など）のために、短期デジタル証明書３０８を利用することができる。短期デジタル証明書３０８が満期になるときに、カスタマ３０２は、長期デジタル証明書３０６とともにリクエストを証明機関サービス３０４に再度提示して、新規の短期デジタル証明書３０６を取得することができる。

【００３２】

前述したように、証明機関サービスによってカスタマに発行された長期デジタル証明書は、自身の身元のカスタマのアサーションの信頼性の確認に利用することができない。例として、長期デジタル証明書は、一つ以上のユーザクライアントが認識できないまたはカスタマ認証のために長期デジタル証明書を承認できないことをこれらの一つ以上のユーザクライアントに指し示すことができる重大な拡張子を含むことができる。それに応じて、図４は、少なくとも一つの実施形態に従う、ユーザクライアント４０４がカスタマサーバ４０２から受信した長期デジタル証明書４０６を拒否する環境４００の例証となる実施例を示す。

【００３３】

長期デジタル証明書４０６は、正規のデジタル証明書に含まれるのと同様のフィールドの多くを含むことができる。例として、長期デジタル証明書４０６は、証明書についての有効期間、長期デジタル証明書４０６が発行されたカスタマ、カスタマ暗号鍵、及び長期デジタル証明書４０６が有効であることを確認するのに使用できる証明機関サービスデジタル署名を規定することができる。しかしながら、長期デジタル証明書４０６は、長期デジタル証明書４０６が検証のみのためであることを規定するのに利用できる一つ以上の重大な拡張子を含むことができる。例として、図４に例証するように、長期デジタル証明書４０６は、識別子「検証のみ　タイプ－１．０１」をもつ拡張子を規定することができる。この特定の拡張子は、ユーザクライアント４０４が、重大な拡張子を認識しない場合に、長期デジタル証明書４０６を拒否しなければならないことを意味する重大としてマークすることができる。さらに、ユーザクライアント４０４がこの重大な拡張子を認識するように更新されるときには、ユーザクライアント４０４は、この重大な拡張子を含む任意の

長期デジタル証明書４０６を承認しないように構成できる。

【００３４】

ユーザクライアント４０４がカスタマサーバ４０２からこの長期デジタル証明書４０６を受信する場合には、ユーザクライアント４０４は、カスタマサーバ４０２から受信したデータを破棄し、カスタマサーバ４０２との通信チャネルを終了させることができる。故に、カスタマは、証明機関サービスと連動して、検証目的のみのために長期デジタル証明書４０６を利用することが可能になる。さらに、これは、長期デジタル証明書４０６の広範な聴衆への公開を限定することによって、長期デジタル証明書４０６、それ故に、カスタマの公開暗号鍵が信用できないことがあるという潜在的なリスクを減少することができる。

【００３５】

前述したように、カスタマは、一つ以上のカスタマサーバを通じて、証明機関サービスから一つ以上の短期デジタル証明書をリクエストすることができる。リクエストは、証明機関サービスが、カスタマを認証し、かつ長期デジタル証明書内の規定の情報を利用して、カスタマに発行される一つ以上の短期デジタル証明書についての有効期間を規定することができる長期デジタル証明書を含むことができる。これらの一つ以上の短期デジタル証明書は、自身の身元をユーザクライアントにアサートし、ユーザクライアントがカスタマを認証できるようにカスタマによって利用することができる。それに応じて、図５は、少なくとも一つの実施形態に従う、ユーザクライアント５０４がカスタマサーバ５０２から受信した短期デジタル証明書５０６を利用してカスタマサーバ５０２を認証できる環境５００の例証となる実施例を示す。ユーザクライアント５０４及びカスタマサーバ５０２は、図４に例証したユーザクライアント及びカスタマサーバと同様のものであっても良い。

【００３６】

環境５００において、カスタマサーバ５０２は、データ及び短期デジタル証明書５０６をユーザクライアント５０４に伝送することができる。ユーザクライアント５０４は、ユーザが相互作用してカスタマサーバ５０２にアクセスできるブラウザアプリケーションであっても良い。ユーザクライアント５０４がカスタマサーバ５０２との通信を開始したときに、カスタマサーバ５０２は、特定のデータ及び短期デジタル証明書５０６をユーザクライアント５０４に提供することによって応答することができる。短期デジタル証明書５０６は、カスタマの身元、短期デジタル証明書５０６についての有効期間、カスタマ公開暗号鍵、及びカスタマサーバ５０２に短期デジタル証明書を発行した証明機関サービスデジタル署名を規定することができる。この情報に加えて、短期デジタル証明書５０６は、短期デジタル証明書５０６が特定の目的のために利用され得ることを規定するのに使用できる一つ以上の拡張子を規定することができる。例として、図５に例証するように、短期デジタル証明書５０６は、証明書チェーンについての経路長を制限するのに使用できる「基本制約」拡張子を含むことができる。「基本制約」拡張子が例証目的のために本開示の全体を通じて広く使用されるが、追加の及び／または代替的な拡張子を短期デジタル証明書５０６内に規定することができる。

【００３７】

しかしながら、図４に例証した長期デジタル証明書とは対照的に、短期デジタル証明書５０６は、図４に例証した長期デジタル証明書内の規定の「検証のみ　タイプ－１．０１」拡張子などの重大な「検証のみ」拡張子を規定しなくても良い。故に、短期デジタル証明書５０６は、ユーザクライアント５０４によって認識でき、ユーザクライアント５０４は、短期デジタル証明書５０６を利用してカスタマサーバ５０２を認証し、証明機関サービスの公開暗号鍵の使用を通じて、短期デジタル証明書５０６内の規定の証明機関サービスデジタル署名を検証することができる。故に、ユーザクライアント５０４が、カスタマサーバ５０２を認証し、短期デジタル証明書５０６が有効であることを確認できる場合には、ユーザクライアント５０４は、安全な通信チャネルを通じたカスタマサーバ５０２とのさらなる通信に携わることができる。

【００３８】

前述したように、カスタマは、カスタマと証明機関サービスとの間の検証目的のみのために利用できる長期デジタル証明書の発行をリクエストするためのリクエストを証明機関サービスに提示することができる。さらに、長期デジタル証明書がカスタマに発行されると、カスタマは、カスタマを認証してカスタマとこれらのユーザクライアントとの間の安全な通信を可能にするためにユーザクライアントによって使用できる一つ以上の短期デジタル証明書を発行するための新規のリクエストを証明機関サービスに提示することができる。一つ以上の短期デジタル証明書を発行するための新規のリクエストは、前述の証明機関サービスが、カスタマを認証し、かつ短期デジタル証明書のパラメータを規定するのに必須の情報を取得するのに利用できる長期デジタル証明書を含むことができる。それに応じて、図６は、少なくとも一つの実施形態に従う、長期デジタル証明書及び短期デジタル証明書を証明機関サービスから受信するためのプロセス６００の例証となる実施例を示す。プロセス６００は、カスタマと証明機関サービスとの間の通信を可能にするように構成できる一つ以上のカスタマサーバを通じて、カスタマによって実行することができる。

【００３９】

長期デジタル証明書をカスタマが取得するために、カスタマは、証明機関サービスが、それを利用して、長期デジタル証明書を委託できる信用できるエンティティとしてカスタマを適切に吟味できる特定の情報を証明機関サービスに提供する必要があり得る。例として、証明機関サービスは、政府機関、信用がある第三者データベース及び他の信用がある情報リポジトリによって維持される一つ以上のデータベースにアクセスし、カスタマが信用できるか否かを決定することができる。故に、カスタマは、長期証明書を取得するために、一つ以上の証明機関サービス検証要件を満たす必要があり得る（６０２）。

【００４０】

カスタマが証明機関サービス検証要件を満たすことができる場合には、証明機関サービスは、長期デジタル証明書を生成することができる。この長期デジタル証明書は、長い有効期間（例えば、１年以上）及び長期デジタル証明書が証明機関サービスによって検証目的のみに使用できることを規定できる特定の重大な拡張子を規定することができる。故に、長期デジタル証明書は、この特定の重大な拡張子を認識するように構成されたユーザクライアントによって承認することはできない。あるいは、ユーザクライアントに長期デジタル証明書を拒否させることができる重大な拡張子は、ユーザクライアントによって認識できない。長期デジタル証明書の有効期間は、証明機関サービスまたはサービスへの自身のリクエストを通じてカスタマによって規定することができる。長期デジタル証明書が生成されると、証明機関サービスは、長期デジタル証明書をカスタマに使用のために発行することができる。故に、カスタマは、証明機関サービスから長期デジタル証明書を受信することができる（６０４）。

【００４１】

証明機関サービスから長期デジタル証明書を受信した後のいつでも、カスタマは、一つ以上のユーザクライアントと通信するときに認証目的のために利用できる一つ以上の短期デジタル証明書を発行するためのリクエストを証明機関サービスに提示することができる（６０６）。リクエストは、証明機関サービスが、カスタマの身元を確認しかつリクエストされた一つ以上の短期デジタル証明書を取得するための権限をカスタマに与えることを保証するために利用できる前述の長期デジタル証明書を含むことができる。実施形態において、証明機関サービスに提示されたリクエストは、長期デジタル証明書内に規定された公開暗号鍵に対応するカスタマの秘密暗号鍵を利用することによって、カスタマによってデジタル署名される。証明機関サービスは、長期証明書の公開鍵を使用してデジタル署名を確認することができる。これにより証明機関サービスは、短期デジタル証明書が、長期デジタル証明書が以前に発行されたのと同じエンティティに発行されることを保証することができる。

【００４２】

証明機関サービスが長期デジタル証明書の使用を通じてカスタマを検証すると、証明機関サービスは、カスタマに発行できる一つ以上の短期デジタル証明書を生成することがで

きる。これらの短期デジタル証明書は、長期デジタル証明書よりも短い継続期間または有効期間を有することができる。例として、証明機関サービスは、長期デジタル証明書についての残存有効期間に少なくともある程度基づいて、短期デジタル証明書についての有効期間を規定することができる。あるいは、カスタマは、有効期間が長期デジタル証明書についての残存有効期間以下である限り、これらの短期デジタル証明書についての特定の有効期間をリクエストすることができる。これにより、証明機関サービスが、長期デジタル証明書の満期日よりも遅い満期日を有する短期デジタル証明書を発行することを阻止できる。短期デジタル証明書は、長期デジタル証明書内の規定の重大な拡張子を除外することもできる。これによりこれらの短期デジタル証明書が、カスタマを認証するためにユーザクライアントによって利用されることが可能になる。短期デジタル証明書が生成されると、カスタマは、これらの短期デジタル証明書を証明機関サービスから受信することができる（６０８）。

【００４３】

カスタマが証明機関サービスから一つ以上の短期デジタル証明書を受信すると、カスタマは、認証目的のためにこれらの一つ以上の短期デジタル証明書を利用することができる（６１０）。例として、カスタマのカスタマサーバは、例として、権限を与えられたサーバと通信して短期デジタル証明書の規定のドメイン名に代わって動作していることをユーザクライアントが決定できる短期デジタル証明書のコピーをユーザクライアントに提供できる。短期デジタル証明書は、証明機関サービスから取得し、例えば、信用がある証明書のためのデータ保存位置においてユーザクライアントによって維持された公開暗号鍵の使用を通じてユーザクライアントによって検証できる証明機関サービスデジタル署名を含むことができる。デジタル署名が検証された場合には、ユーザクライアントは、短期デジタル証明書が本物であり、それを使用してカスタマがそう称する者であることを保証することを決定できる。

【００４４】

前述したように、証明機関サービスは、長期デジタル証明書を発行するためのリクエストをカスタマから受信することができる。この長期デジタル証明書は、カスタマと証明機関サービスとの間の検証目的のために利用することができる。例として、長期デジタル証明書は、カスタマまたは任意の他のエンティティによってユーザクライアントに提供された場合にユーザクライアントにデジタル証明書を拒否させることができる重大な拡張子を規定することができる。しかしながら、証明機関サービスは、この長期デジタル証明書を利用して、カスタマを検証し、リクエスト時に認証のために使用できる短期デジタル証明書を発行することができる。それに応じて、図７は、少なくとも一つの実施形態に従う、長期デジタル証明書を発行するためのカスタマリクエストに応答して、長期デジタル証明書を生成して発行するプロセス７００の例証となる実施例を示す。プロセス７００は、カスタマに長期デジタル証明書を委託できるか否かを決定するために、カスタマからのリクエストを受信し、他のエンティティと通信するように構成できる前述の証明機関サービスによって実行することができる。さらに、証明機関サービスは、カスタマのリクエストならびに既知のデジタル証明書フォーマット及び基準に少なくともある程度基づいて、これらの長期デジタル証明書を生成するように構成できる。

【００４５】

カスタマは、証明機関サービスと通信して、カスタマと証明機関サービスとの間の検証目的のために利用することができる長期デジタル証明書の発行をリクエストすることができる。カスタマは、ビジネス中にさまざまなユーザクライアントと通信するのに利用できる一つ以上のサーバを動作させることができる。これらの一つ以上のサーバがこれらのユーザクライアントによって認証され、これらの一つ以上のサーバとユーザクライアントとの間の安全な通信を可能にするために、カスタマは、カスタマがそう称する者であることをこれらのユーザクライアントに確信させるために、一つ以上のデジタル証明書を獲得する必要があり得る。前述したように、長期デジタル証明書は、検証目的のために利用される。加えて、この長期デジタル証明書は、ユーザクライアントによってサーバ認証のため

に利用できる短期デジタル証明書を取得するために必要となり得る。故に、証明機関サービスは、長期デジタル証明書を発行するためのリクエストをカスタマから受信することができる７０２。

【００４６】

カスタマからのリクエストは、カスタマのビジネスオペレーションに関する情報を含むことができる。例として、カスタマは、名前、住所、Ｅメールアドレス、ユニフォームリソースロケータ（ＵＲＬ）、財務記録などをレビューのために証明機関サービスに提供することができる。この情報は、カスタマに一つ以上の長期デジタル証明書を委託できるか否かを決定するのに必須であり得る。故に、証明機関サービスは、カスタマを吟味するための徹底的な検証プロセスを実行するための、カスタマから必須の情報を受信したか否かを決定することができる７０４。証明機関サービスによって要求されるようなこの必須の情報をカスタマが供給しなかった場合には、証明機関サービスは、長期デジタル証明書を発行するためのカスタマのリクエストを拒絶することができる７０６。

【００４７】

カスタマを検証するのに必要な必須の情報をカスタマが証明機関サービスに供給した場合には、証明機関サービスは、リクエスタ（例えば、カスタマ）を確認及び検証するための一つ以上のエンティティ及びドメイン検証プロセスを実行することができる７０８。例として、いくつかの実施形態では、証明機関サービスは、カスタマのドメインに管理的に関与するものとして既知のアドレスに一つ以上の電子メール（Ｅメール）メッセージを送信することができる。証明機関サービスは、例えば、カスタマドメインを識別するための「ＷＨＯＩＳ」クエリを使用して、カスタマの「ＷＨＯＩＳ」エントリに含まれる規定の連絡アドレスに認証リンクを伝送することができる。追加的にまたは代替的に、証明機関サービスは、さまざまな政府機関データベース及び他の第三者データベースにアクセスし、提供された情報に少なくともある程度基づいて、カスタマに長期デジタル証明書を委託できるか否かを決定することができる。

【００４８】

証明機関サービスがエンティティ及びドメイン検証プロセスを実行すると、証明機関サービスは、これらのプロセスが満たされたか否かを決定することができる（７１０）。例として、証明機関サービスが、政府機関データベース及び他の第三者データベース内の規定のカスタマ情報の解析に基づいて、カスタマに長期デジタル証明書を委託できないことを決定した場合には、証明機関サービスは、カスタマのリクエストを拒絶することができる（７０６）。しかしながら、検証プロセスが満たされた場合には、証明機関サービスは、証明機関サービスとカスタマとの間の検証目的に利用できる長期デジタル証明書を生成することができる（７１２）。

【００４９】

長期デジタル証明書は、デジタル証明書の発行者、証明書についての有効期間、サブジェクト（例えば、カスタマ）、サブジェクトの公開暗号鍵、及び証明機関サービスデジタル署名を規定することができる。長期デジタル証明書は、さらに、長期デジタル証明書が検証目的のみのために利用されることを表すことができる重大な拡張子を規定することができる。この重大な拡張子は、いくつかのユーザクライアントには認識されず、結果として、これらのユーザクライアントによって自動的に拒否され得る。あるいは、ユーザクライアントは、この重大な拡張子を含むあらゆるデジタル証明書を拒否するように構成できる。証明機関サービスがこの長期デジタル証明書を生成すると、証明機関サービスは、この証明書をカスタマに発行することができる（７１４）。故に、カスタマは、ここで、検証目的のために及びリクエストの一部としてこの長期デジタル証明書を利用して、一つ以上のユーザクライアントと通信するための短期デジタル証明書を取得することができる。

【００５０】

前述したように、証明機関サービスは、一つ以上の短期デジタル証明書を発行するためのカスタマからのリクエストを受信することができる。これらの一つ以上の短期デジタル証明書は、以前に発行された長期デジタル証明書とは対照的に、カスタマを認証してカス

タマとこれらのユーザクライアントとの間の安全な通信を可能にするために、ユーザクライアントによって利用することができる。カスタマからのリクエストは、カスタマを検証し、リクエストされた短期デジタル証明書を生成するのに必須の情報を取得するために証明機関サービスによって利用できる以前に発行された長期デジタル証明書を含むことができる。それに応じて、図８は、少なくとも一つの実施形態に従う、カスタマリクエストに応答して、長期デジタル証明書を利用してカスタマを認証して一つ以上の短期デジタル証明書を発行するためのプロセス８００の例証となる実施例を示す。

【００５１】

前述のプロセス７００と同様に、カスタマは、証明機関サービスと通信して、カスタマによってユーザクライアントに提供され、これらのユーザクライアントがカスタマを認証して安全な通信をカスタマに伝送できる短期デジタル証明書の発行をリクエストすることができる。リクエストは、証明機関サービスによってカスタマに以前に発行され、カスタマと証明機関サービスとの間の検証目的のみに使用可能な長期デジタル証明書を含むことができる。いくつかの実施形態では、短期デジタル証明書を発行するためのリクエストは、短期デジタル証明書がカスタマに発行されることを証明機関サービスに確信させるために、長期デジタル証明書内に含まれるカスタマの秘密暗号鍵を使用してデジタル署名することができる。証明機関サービスは、長期デジタル証明書の公開暗号鍵を使用してデジタル署名を確認することができる。故に、証明機関サービスは、一つ以上の短期デジタル証明書を発行するためのリクエストを受信することができる（８０２）。

【００５２】

一つ以上の短期デジタル証明書を発行するためのリクエストを証明機関サービスがカスタマから受信すると、証明機関サービスは、長期デジタル証明書内に含まれる情報を調査して（８０４）、証明書が有効であるか否かを決定することができる（８０６）。例として、証明機関サービスは、長期デジタル証明書内のサブジェクトフィールドを評価して、リクエストを提示したエンティティが長期デジタル証明書内の規定のサブジェクトとマッチするか否かを決定することができる。さらに、証明機関サービスは、含まれている証明機関サービスデジタル署名を利用することによって長期デジタル証明書が改ざんされたか否かを決定し、証明書の有効性を決定することができる。長期デジタル証明書が有効でないことを証明機関サービスが決定した場合には、証明機関サービスは、短期デジタル証明書を発行するためのカスタマのリクエストを拒絶することができる（８０８）。

【００５３】

実施形態において、長期デジタル証明書は、短期デジタル証明書をカスタマに発行するように構成された証明機関サービスとは異なる証明機関サービスによって発行することができる。長期デジタル証明書は、この異なる証明機関サービスに対応する証明機関サービスデジタル署名を含むことができる。それに応じて、証明機関サービスは、最初にこの異なる証明機関サービスからの公開暗号鍵を有するか否かを決定し、有する場合には、この公開暗号鍵を利用して、長期デジタル証明書内の規定のデジタル署名を確認し、長期デジタル証明書を検証することができる。長期デジタル証明書が有効である場合には、証明機関サービスは、長期デジタル証明書の調査を継続し、リクエストされた短期デジタル証明書をカスタマに発行できるか否かを決定することができる。

【００５４】

長期デジタル証明書が確かに有効であることを証明機関サービスが決定した場合には、証明機関サービスは、長期デジタル証明書が、短期デジタル証明書を発行するための十分な残存有効期間を未だ有するか否かを決定することができる（８１０）。例として、証明機関サービスは、証明機関サービスが長期デジタル証明書に基づいて任意の短期デジタル証明書を発行するために、３カ月超の残存有効期間を長期デジタル証明書が有することを要求する場合がある。同様に、証明機関サービスは、特定の有効期間をもつ短期デジタル証明書のみを発行するように構成できる。この特定の有効期間が長期デジタル証明書の残存有効期間を超える場合には、証明機関サービスは、リクエストされた一つ以上の短期デジタル証明書を生成することができない。故に、長期デジタル証明書が十分な残存有効期

間を有さないことを証明機関サービスが決定した場合には、証明機関サービスは、カスタマのリクエストを拒絶することができる（８０８）。

【００５５】

リクエストされた一つ以上の短期デジタル証明書を発行するための十分な残存有効期間を長期デジタル証明書が有することを証明機関サービスが決定すると、証明機関サービスは、発行される短期デジタル証明書の有効期間を決定することができる８１２。前述したように、証明機関サービスは、設定された有効期間をもつ短期デジタル証明書を生成するように構成できる。故に、これらの短期デジタル証明書は、この特定の有効期間を規定することができる。他の実施形態では、カスタマは、リクエストを通じて、短期デジタル証明書についての所望の有効期間を規定することができる。所望の有効期間が長期デジタル証明書についての残存有効期間を超えない場合には、証明機関サービスは、この所望の有効期間を利用して、リクエストされた一つ以上の短期デジタル証明書の開始日及び満期日を計算することができる。

【００５６】

証明機関サービスは、短期デジタル証明書の決定された有効期間及び長期デジタル証明書から集めた情報を利用して、一つ以上の短期デジタル証明書を生成することができる。その後、証明機関サービスは、カスタマ自身のリクエストに応答してカスタマに一つ以上の短期デジタル証明書を発行することができる（８１４）。これによりカスタマは、これらの一つ以上の短期デジタル証明書をさまざまなユーザクライアントに提供でき、そしてこれらのユーザクライアントは、カスタマを認証してカスタマと安全に通信することができる。

【００５７】

前述したように、長期デジタル証明書は、ユーザクライアントによって認識できない、またはユーザクライアントに、この拡張子の検出及び認識時に長期デジタル証明書を承認させない重大な拡張子を含むことができる。故に、カスタマが長期デジタル証明書をユーザクライアントに提供した場合には、ユーザクライアントは、カスタマを認証することができず、故に、さらに、カスタマと通信することができない。それに応じて、図９は、少なくとも一つの実施形態に従う、デジタル証明書を利用してカスタマサーバを認証するためのプロセス９００の例証となる実施例を示す。プロセス９００は、ユーザのコンピューティングデバイスにインストールされたブラウザアプリケーションなどの任意のユーザクライアントによって実行することができる。

【００５８】

ユーザクライアントがカスタマサーバとの通信チャネルを確立するときに、カスタマサーバは、カスタマサーバの身元を確立するために、一つ以上のデジタル証明書をユーザクライアントに伝送することができる。これらのデジタル証明書は、カスタマサーバがそう称する者であるか否かを決定するのに使用できるさまざまなフィールドを含むことができる。例として、デジタル証明書は、カスタマ及び関連付けられたカスタマサーバの名前、アドレス及びドメインを規定できるサブジェクトフィールドを含むことができる。さらに、デジタル証明書は、信用がある証明機関サービスによってデジタル証明書が発行され、デジタル証明書が有効であることをユーザクライアントが確認するのに利用できる証明機関サービスデジタル署名を含むことができる。さらに、デジタル証明書は、ユーザクライアントによってデジタル証明書をどのように処理すべきかを規定できるさまざまな拡張子を含むことができる。故に、カスタマサーバとの通信の確立時に、ユーザクライアントは、このカスタマサーバからデジタル証明書を受信し（９０２）、さらに、デジタル証明書内の規定の任意の拡張子を識別することができる（９０４）。

【００５９】

前述したように、長期デジタル証明書は、カスタマサーバと発行している証明機関サービスとの間の検証目的のみに長期デジタル証明書を利用できることを規定できる重大な拡張子を含むことができる。この重大な拡張子は、特定のユーザクライアントには認識されず、結果として、これらのユーザクライアントに長期デジタル証明書を拒否させることが

できる。あるいは、いくつかの実施形態では、ユーザクライアントは、この重大な拡張子を認識し、結果として、カスタマサーバからの長期デジタル証明書を承認させないように構成できる。故に、ユーザクライアントは、受信したデジタル証明書がこの「検証のみ」の重大な拡張子を含むか否かを決定することができる（９０６）。デジタル証明書がこの重大な拡張子を含む場合には、ユーザクライアントは、ユーザクライアントがカスタマを認証できないように、ユーザクライアントとカスタマとの間の通信チャネルを終了することができる（９０８）。しかしながら、重大な拡張子が存在しない場合には、ユーザクライアントは、カスタマサーバを認証するためのデジタル証明書の処理を継続することができる（９１０）。

【００６０】

図１０は、さまざまな実施形態に従う、態様を実施するための例示的な環境１０００の態様を例証する。認識されるように、説明を目的としてウェブベースの環境を使用したが、必要に応じて、さまざまな実施形態を実施するための種々の環境を使用することができる。環境は、適切なネットワーク１００４を通じてリクエスト、メッセージまたは情報を送信及び／または受信する、そしていくつかの実施形態ではデバイスのユーザに情報を戻すように伝達するように動作可能な任意の適切なデバイスを含むことができる電子クライアントデバイス１００２を含む。そのようなクライアントデバイスの実施例は、パーソナルコンピュータ、携帯電話、ハンドヘルドメッセージングデバイス、ラップトップコンピュータ、タブレットコンピュータ、セットトップボックス、パーソナルデータアシスタント、組み込み型コンピュータシステム、電子ブックリーダなどを含む。ネットワークは、イントラネット、インターネット、セルラーネットワーク、ローカルエリアネットワーク、衛星ネットワークもしくは任意の他のそのようなネットワーク、及び／またはそれらの組み合わせを含む任意の適切なネットワークを含むことができる。そのようなシステムに使用される構成要素は、選択されたネットワーク及び／または環境のタイプに少なくともある程度応じて決めることができる。そのようなネットワークを通じて通信するためのプロトコル及び構成要素は、公知であり、本明細書に詳細には論じない。ネットワークを通じた通信は、有線または無線接続及びそれらの組み合わせによって可能になる。他のネットワークでは、当業者に明らかであろうような、同様の目的を果たす代替的なデバイスであるが、この実施例では、リクエストを受信し、それに応答してコンテンツをサーブするためのウェブサーバ１００６を環境が含むので、ネットワークは、インターネットを含む。

【００６１】

例証となる環境は、少なくとも一つのアプリケーションサーバ１００８及びデータストア１０１０を含む。相互作用して適切なデータストアからデータを取得するなどのタスクを実行できる鎖状または別な様に構成できるいくつかのアプリケーションサーバ、層もしくは他の要素、プロセスまたは構成要素が存在し得ることを理解すべきである。本明細書に使用されるようなサーバは、ハードウェアデバイスまたは仮想コンピュータシステムなどのさまざまな様式において実装することができる。いくつかの文脈において、サーバは、コンピュータシステムにおいて実行されるプログラミングモジュールを指しても良い。文脈から別な様に明記しないまたは明確にしない限り、本明細書に使用されるような「データストア」という用語は、データを保存、それにアクセス及びそれを検索できる任意のデバイスまたはデバイスの組み合わせを指し、任意の標準、分散、仮想またはクラスタ化環境における、データサーバ、データベース、データ記憶デバイス及びデータ記憶媒体の任意の組み合わせ及び数を含むことができる。アプリケーションサーバは、アプリケーションのためのデータアクセス及びビジネスロジックのいくつかまたはすべてを処理する、クライアントデバイスのための一つ以上のアプリケーションの態様を実行するのに必要なような、データストアと統合するための任意の適切なハードウェア、ソフトウェア及びファームウェアを含むことができる。アプリケーションサーバは、データストアと協働してアクセス制御サービスを提供し、これらに限定されないが、テキスト、グラフィックス、音声、映像及び／またはハイパーテキストマークアップ言語（「ＨＴＭＬ」）、拡張マー

クアップ言語（「ＸＭＬ」）、ジャバスクリプト、カスケーディングスタイルシート（「ＣＳＳ」）、もしくは他の適切なクライアント側構造化言語の形態において、ウェブサーバによってユーザにサーブすることができる、ユーザに提供されて使用可能な他のコンテンツを含むコンテンツを生成できる。クライアントデバイスに転送されるコンテンツは、これらに限定されないが、ユーザが、音声的に、視覚的にならびに／または触覚、味覚及び／もしくは嗅覚を含む他の感覚を通じて知覚可能な形態を含む一つ以上の形態においてコンテンツを提供するようにクライアントデバイスによって処理することができる。すべてのリクエスト及び応答の処理、ならびにクライアントデバイス１００２とアプリケーションサーバ１００８との間のコンテンツの送達は、この実施例では、ＰＨＰ、ハイパーテキストプリプロセッサ（「ＰＨＰ」）、Ｐｙｔｈｏｎ、Ｒｕｂｙ、Ｐｅｒｌ、Ｊａｖａ、ＨＴＭＬ、ＸＭＬまたは別の適切なサーバ側構造化言語を使用してウェブサーバによって処理することができる。本明細書に論じる構造的コードを本明細書の他の箇所に論じるような任意の適切なデバイスまたはホストマシンにおいて実行できるので、ウェブ及びアプリケーションサーバが必須ではなく、単なる例示的な構成要素であることを理解すべきである。さらに、単一デバイスによって実行するように本明細書に記載する動作は、文脈から別な様に明確でない限り、分散及び／または仮想システムを形成できる複数のデバイスによって集合的に実行できる。

【００６２】

データストア１０１０は、本開示の特定の態様に関するデータを保存するためのいくつかの別個のデータ表、データベース、データドキュメント、動的データストレージスキームならびに／または他のデータストレージ機構及び媒体を含むことができる。例えば、例証したデータストアは、生産側にコンテンツをサーブするのに使用できるプロダクションデータ１０１２及びユーザ情報１０１６を保存するための機構を含むことができる。データストアは、報告、解析または他のそのような目的のために使用できるログデータ１０１４を保存するための機構を含むようにも示される。必要に応じて前にリストした機構またはデータストア１０１０における追加の機構のいずれかに保存できる、ページイメージ情報及びアクセス権情報などのデータストアに保存する必要があり得る多くの他の態様が存在し得ることを理解すべきである。データストア１０１０は、それに関連付けられたロジックを通じて、アプリケーションサーバ１００８からの命令を受信し、それに応答してデータを取得、更新または別な様に処理するように動作可能である。アプリケーションサーバ１００８は、受信した命令に応答して、静的データ、動的データまたは静的データと動的データとの組み合わせを提供することができる。ウェブログ（ブログ）、ショッピングアプリケーション、ニュースサービス及び他のそのようなアプリケーションに使用されるデータなどの動的データは、本明細書に記載するようなサーバ側構造化言語によって生成できる、またはアプリケーションサーバにおいてもしくはその制御下で動作するコンテンツ管理システム（「ＣＭＳ」）によって提供することができる。一実施例において、ユーザは、ユーザによって操作されるデバイスを通じて、特定のタイプのアイテムについての検索リクエストを提示することができる。この場合では、データストアは、ユーザ情報にアクセスしてユーザの身元を確認し、そしてカタログ詳細情報にアクセスしてそのタイプのアイテムについての情報を取得することができる。その後、ユーザがユーザデバイス１００２におけるブラウザを通じて見ることができるウェブページにリストされている結果などの情報をユーザに戻すことができる。関心のある特定のアイテムについての情報は、ブラウザの専用ページまたはウィンドウにおいて見ることができる。しかしながら、本開示のその実施形態が、必ずしもウェブページの文脈に限定されず、リクエストが必ずしもコンテンツについてのリクエストではない場合に、通例、リクエストの処理により広く適用可能であり得ることに留意すべきである。

【００６３】

各サーバは、通常、そのサーバの全般的な管理及び動作のための実行可能プログラム命令を提供するオペレーティングシステム、及び通常、サーバのプロセッサによって実行されたときに、サーバにその意図する機能を実行させる命令を保存するコンピュータ可読記

憶媒体（例えば、ハードディスク、ランダムアクセスメモリ、リードオンリーメモリなど）を含む。サーバのオペレーティングシステム及び全般的な機能性の適切な実施態様は、既知または市販されており、特に、本明細書の開示に照らした当業者によって容易に実施される。

【００６４】

一実施形態において、環境は、一つ以上のコンピュータネットワークまたは直接接続を使用して、通信リンクを通じて相互接続されたいくつかのコンピュータシステム及び構成要素を利用する分散及び／または仮想コンピューティング環境である。しかしながら、そのようなシステムが、図１０に例証するよりも少ないまたは多い数の構成要素を有するシステムにおいて等しく良好に動作できることが当業者によって認識される。故に、図１０のシステム１０００の描写は、事実上例証として解釈され、本開示の範囲を限定しないはずである。

【００６５】

さまざまな実施形態は、さらに、場合によっては多数のアプリケーションのいずれかを動作させるのに使用できる、一つ以上のユーザコンピュータ、コンピューティングデバイスまたはプロセッシングデバイスを含むことができる広範な様々な動作環境において実施することができる。ユーザまたはクライアントデバイスは、標準オペレーティングシステムを実行するデスクトップ、ラップトップまたはタブレットコンピュータ、ならびにモバイルソフトウェアを実行し、多数のネットワーキング及びメッセージングプロトコルをサポートできるセルラー、無線及びハンドヘルドデバイスなどの多数の汎用パーソナルコンピュータのいずれかを含むことができる。そのようなシステムは、開発及びデータベース管理などの目的のための様々な市販のオペレーティングシステム及び他の既知のアプリケーションのいずれかを実行する多数のワークステーションも含むことができる。これらのデバイスは、ダミーターミナル、シンクライアント、ゲーミングシステム、及びネットワークを通じて通信できる他のデバイスなどの他の電子デバイスも含むことができる。これらのデバイスは、ネットワークを通じて通信できる仮想マシン、ハイパーバイザ及び他の仮想デバイスなどの仮想デバイスも含むことができる。

【００６６】

本開示のさまざまな実施形態は、伝送制御プロトコル／インターネットプロトコル（「ＴＣＰ／ＩＰ」）、ユーザデータグラムプロトコル（「ＵＤＰ」）、オープンシステムインターコネクション（「ＯＳＩ」）モデルのさまざまな層において動作するプロトコル、ファイル転送プロトコル（「ＦＴＰ」）、ユニバーサルプラグアンドプレイ（「ＵｐｎＰ」）、ネットワークファイルシステム（「ＮＦＳ」）、共通インターネットファイルシステム（「ＣＩＦＳ」）、及びアップルトークなどの様々な市販のプロトコルのいずれかを使用して通信をサポートするための、当業者によく知られている少なくとも一つのネットワークを利用する。ネットワークは、例えば、ローカルエリアネットワーク、広域ネットワーク、仮想プライベートネットワーク、インターネット、イントラネット、エクストラネット、公衆交換電話網、赤外線ネットワーク、無線ネットワーク、衛星ネットワーク、及びそれらの任意の組み合わせであっても良い。

【００６７】

ウェブサーバを利用する実施形態では、ウェブサーバは、ハイパーテキスト転送プロトコル（「ＨＴＴＰ」）サーバ、ＦＴＰサーバ、共通ゲートウェイインターフェース（「ＣＧＩ」）サーバ、データサーバ、Ｊａｖａサーバ、アパッチサーバ、及びビジネスアプリケーションサーバを含む様々なサーバまたは中間層アプリケーションのいずれかを実行することができる。サーバ（複数可）は、Ｊａｖａ（登録商標）、Ｃ、Ｃ＃もしくは Ｃ＋＋などの任意のプログラミング言語、またはＲｕｂｙ、ＰＨＰ、Ｐｅｒｌ、ＰｙｔｈｏｎもしくはＴＣＬなどの任意のスクリプト言語、及びそれらの組み合わせにおいて書き込まれた一つ以上のスクリプトまたはプログラムとして実施できる一つ以上のウェブアプリケーションを実行することなどによって、ユーザデバイスからのリクエストに応答してプログラムまたはスクリプトも実行することができる。サーバ（複数可）は、制限なく、Ｏｒａ

ｃｌｅ（登録商標）、Ｍｉｃｒｏｓｏｆｔ（登録商標）、Ｓｙｂａｓｅ（登録商標）及びＩＢＭ（登録商標）から市販されているもの、ならびにＭｙＳＱＬ、Ｐｏｓｔｇｒｅｓ、ＳＱＬｉｔｅ、ＭｏｎｇｏＤＢなどのオープンソースサーバ、及び構造化または非構造化データに保存、それを検索及びそれにアクセスできる任意の他のサーバを含むデータベースサーバも含むことができる。データベースサーバは、タブレットベースのサーバ、ドキュメントベースのサーバ、非構造化サーバ、リレーショナルサーバ、非リレーショナルサーバもしくはこれらの組み合わせ、及び／または他のデータベースサーバを含むことができる。

【００６８】

環境は、前述のような様々なデータストア、ならびに他のメモリ及び記憶媒体を含むことができる。これらは、コンピュータの一つ以上にローカル（かつ／またはそこに存在する）、またはネットワークにわたるコンピュータのいずれかまたはすべてからリモートの記憶媒体などの様々な位置に存在することができる。特定の一連の実施形態では、情報は、当業者によく知られているストレージエリアネットワーク（「ＳＡＮ」）に存在することができる。同様に、コンピュータ、サーバまたは他のネットワークデバイスに属する機能を実行するための任意の必須のファイルを、必要に応じて、ローカルに及び／またはリモートに保存することができる。コンピュータ化されたデバイスをシステムが含む場合には、各々のそのようなデバイスは、バスを通じて電気的に連結できるハードウェア要素を含むことができる。この要素は、例えば、少なくとも一つの中央処理装置（「ＣＰＵ」または「プロセッサ」）、少なくとも一つの入力デバイス（例えば、マウス、キーボード、コントローラ、タッチスクリーンまたはキーパッド）、及び少なくとも一つの出力デバイス（例えば、表示デバイス、プリンタまたはスピーカ）を含む。そのようなシステムは、ディスクドライブ、光記憶デバイス、及びランダムアクセスメモリ（「ＲＡＭ」）またはリードオンリーメモリ（「ＲＯＭ」）などの固体記憶デバイスなどの一つ以上の記憶デバイス、ならびにリムーバブル媒体デバイス、メモリカード、フラッシュカードなども含むことができる。

【００６９】

そのようなデバイスは、前述のようなコンピュータ可読記憶媒体リーダ、通信デバイス（例えば、モデム、ネットワークカード（無線または有線）、赤外線通信デバイスなど）、及びワーキングメモリも含むことができる。コンピュータ可読記憶媒体リーダは、コンピュータ可読記憶媒体、相当するリモート、ローカル、固定及び／またはリムーバブル記憶デバイス、ならびにコンピュータ可読情報を一時的に及び／またはより恒久的に含有、保存、伝送及び検索するための記憶媒体に接続できるまたはそれらを受け入れるように構成できる。システム及びさまざまなデバイスは、通常、クライアントアプリケーションまたはウェブブラウザなどのオペレーティングシステム及びアプリケーションプログラムを含む、少なくとも一つのワーキングメモリデバイス内に位置する多数のソフトウェアアプリケーション、モジュール、サービスまたは他の要素も含む。代替的な実施形態が前述からの数々のバリエーションを有することができることを認識すべきである。例えば、カスタマイズされたハードウェアも使用でき、かつ／または特定の要素をハードウェア、（アプレットなどの高移植性ソフトウェアを含む）ソフトウェアまたはその両方において実装することができる。さらに、ネットワーク入力／出力デバイスなどの他のコンピューティングデバイスとの接続を用いることができる。

【００７０】

コードまたはコードの一部を含有するための記憶媒体及びコンピュータ可読媒体は、これらに限定されないが、ＲＡＭ、ＲＯＭ、電気的消去可能プログラマブルリードオンリーメモリ（「ＥＥＰＲＯＭ」）、フラッシュメモリまたは他のメモリ技術を含む、コンピュータ可読命令、データ構造、プログラムモジュールまたは他のデータなどの情報を保存及び／または伝送するための任意の方法または技術において実装される揮発性の及び不揮発性の、リムーバブル及び非リムーバブル媒体、コンパクトディスク読出し専用メモリ（「ＣＤ－ＲＯＭ」）、デジタル多用途ディスク（ＤＶＤ）または他の光ストレージ、磁気カ

セット、磁気テープ、磁気ディスクストレージまたは他の磁気記憶デバイス、または所望の情報を保存するのに使用できる及びシステムデバイスによってアクセスできる任意の他の媒体などの記憶媒体及び通信媒体を含む、当業界において公知のまたは使用されている任意の適切な媒体を含むことができる。本開示及び本明細書に提供される教示に基づいて、当業者は、さまざまな実施形態を実施する他の様式及び／または方法を認識する。

【００７１】

それに応じて、明細書及び図面は、限定的意味ではなく例証とみなされる。しかしながら、特許請求の範囲に説明されているような本発明のより広範な精神及び範囲から逸脱することなく、本発明にさまざまな修正及び変更を為せることが明白である。

【００７２】

他のバリエーションも本開示の精神内にある。故に、開示した技術はさまざまな修正及び代替的な構造を受け入れることができるが、その特定の例証である実施形態を、図面に示し、詳細に前述した。しかしながら、開示した具体的な一つ以上の形態に本発明を限定する意図はなく、それどころか、その意図が、すべての修正、代替的な構造、及び添付の特許請求の範囲に定義されるような本発明の精神及び範囲内に収まる均等物を含むことを理解すべきである。

【００７３】

開示した実施形態を記載する文脈における（とりわけ、以下の特許請求の範囲の文脈における）、「ａ」及び「ａｎ」ならびに「ｔｈｅ」という用語、ならびに同様の指示対象の使用は、本明細書において別な様に示さない限りまたは文脈において明確に矛盾しない限り、単数形及び複数形の両方を含むように解釈されるべきである。「ｃｏｍｐｒｉｓｉｎｇ（を備える）」、「ｈａｖｉｎｇ（を有する）」「ｉｎｃｌｕｄｉｎｇ（を含む）」、及び「ｃｏｎｔａｉｎｉｎｇ（を含有する）」という用語は、別な様に留意されていない限り、オープンエンド用語（すなわち、「ｉｎｃｌｕｄｉｎｇ，ｂｕｔ ｎｏｔ ｌｉｍｉｔｅｄ ｔｏ（を含むが、これに限定されない）」を意味する）として解釈されるべきである。「ｃｏｎｎｅｃｔｅｄ（接続された）」という用語は、修正されていなく、物理的接続を指すときには、何らかの介在物が存在する場合でさえも、共に取り付けられたまたは接合された、その内部に部分的または全体的に収容されていると解釈されるべきである。本明細書の値の範囲の列挙は、本明細書において別な様に示さない限り、単に、範囲内に収まる各々の別個の値を個々に指す簡単な方法として役立つように意図され、各々の別個の値は、本明細書に個々に列挙されるように本明細書に組み込まれる。「ｓｅｔ（セット）」（例えば、「ａ ｓｅｔ ｏｆ ｉｔｅｍｓ」（アイテムのセット）または「ｓｕｂｓｅｔ（サブセット）」という用語の使用は、別な様に留意されていない限りまたは文脈において矛盾しない限り、一つ以上の部材を備えた空でない集合として解釈されるべきである。さらに、別な様に留意されていない限りまたは文脈において矛盾しない限り、対応するセットの「ｓｕｂｓｅｔ（サブセット）」という用語は、必ずしも対応するセットの適切なサブセットを意味せず、むしろ、サブセットと、対応するセットとは等しい場合がある。

【００７４】

「ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ，Ｂ，ａｎｄ Ｃ（Ａ、Ｂの少なくとも一つ及びＣ）」または「ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ，Ｂ ａｎｄ Ｃ（Ａ、Ｂ及びＣの少なくとも一つ）」の形態の慣用句などの接続的な言葉は、別な様に具体的に示されていない限りまたはさもなければ文脈において明確に矛盾しない限り、通例、アイテム、用語などが、ＡまたはＢまたはＣ、またはＡ及びＢ及びＣのセットの任意の空でないサブセットのいずれかであり得ることを提示するのに利用されるように文脈においてさもなければ理解される。例として、３つの部材を有するセットの例証となる実施例では、「ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ，Ｂ，ａｎｄ Ｃ（Ａ、Ｂの少なくとも一つ及びＣ）」及び「ａｔ ｌｅａｓｔ ｏｎｅ ｏｆ Ａ，Ｂ ａｎｄ Ｃ（Ａ、Ｂ及びＣの少なくとも一つ）」という接続的な慣用句は、以下のセット、すなわち、｛Ａ｝、｛Ｂ｝、｛Ｃ｝、｛Ａ，Ｂ｝、｛Ａ，Ｃ｝、｛Ｂ，Ｃ｝、｛Ａ，Ｂ，Ｃ｝のいずれかを指す。故に、そのよ

うな接続的な言葉は、通常、特定の実施形態が、各々が存在し得る、Ａの少なくとも一つ、Ｂの少なくとも一つ、Ｃの少なくとも一つを必要とすることを示唆することは意図しない。

【００７５】

本明細書に記載するプロセスの動作は、本明細書において別な様に示さない限りまたはさもなければ文脈において明確に矛盾しない限り、任意の適切な順序で実行することができる。本明細書に記載するプロセス（または、それらのバリエーション及び／または組み合わせ）は、実行可能命令を含んで構成された一つ以上のコンピュータシステムの制御下で実行することができる、及びハードウェアまたはそれらの組み合わせによって一つ以上のプロセッサにおいて集合的に実行するコード（例えば、実行可能命令、一つ以上のコンピュータプログラムまたは一つ以上のアプリケーション）として実装することができる。コードは、例えば、一つ以上のプロセッサによって実行可能な複数個の命令を含むコンピュータプログラムの形態において、コンピュータ可読記憶媒体に保存することができる。コンピュータ可読記憶媒体は、非一時的であっても良い。

【００７６】

本明細書に提供される任意の及びすべての実施例または例示の言葉（例えば、「ｓｕｃｈ　ａｓ（などの）」）の使用は、別な様に主張されない限り、単に、本発明の実施形態の理解を容易にすることが意図され、本発明の範囲を制限しない。明細書中の言葉はすべて、本発明の実践に絶対不可欠なものとして任意の主張しない要素を示唆しないものとして解釈される。

【００７７】

本開示の実施形態は、本発明を実行するための発明者らに既知の最良の形態を含んで本明細書に記載される。それらの実施形態のバリエーションは、先の記載を読んだ当業者に明らかになる。発明者らは、当業者が必要に応じてそのようなバリエーションを用いることを期待し、そして発明者らは、本開示の実施形態が本明細書に具体的に記載するのとは別な様に実践されることを意図する。それに応じて、本開示の範囲は、適用法によって許可されるようなこの文書に添付した特許請求の範囲に列挙した主題のすべての修正及び均等物を含む。その上、そのすべての可能なバリエーションにおける前述の要素の任意の組み合わせは、本明細書において別な様に示さない限りまたはさもなければ文脈において明確に矛盾しない限り、本開示の範囲に包含される。

【００７８】

本明細書に引用された公開物、特許出願及び特許品を含むすべての参考文献は、各参考文献が個々にかつ具体的に表されるように参照により組み込まれ、かつ本明細書全体において説明されるのと同じ範囲において本文書に参照により組み込まれる。

【００７９】

本開示の実施形態は、以下の条項を考慮して記載することができる。

【００８０】

１．

実行可能命令を含んで構成された一つ以上のコンピュータシステムの制御下で、

第一のデジタル証明書をエンティティに発行することと、ここで、前記第一のデジタル証明書が、前記エンティティの検証を証明機関サービスに可能にさせる重大な拡張子を規定し、前記第一のデジタル証明書が、

前記エンティティに特有の少なくとも一つのサブジェクトフィールドを規定し、

第一の公開暗号鍵を規定し、

第一の秘密暗号鍵に対応し、かつ

前記第一のデジタル証明書についての第一の有効期間を規定し、

前記エンティティから、第二のデジタル証明書を発行するためのリクエストを受信することと、ここで、前記リクエストが、前記第一のデジタル証明書及びデジタル署名を含み、前記第二のデジタル証明書が、前記エンティティのサーバを認証するために使用可能であり、

前記第一のデジタル証明書内の規定の有効期間及び前記第一の公開暗号鍵に少なくともある程度基づいて、前記第二のデジタル証明書を発行するか否かを決定することと、及び
前記少なくとも一つのサブジェクトフィールド、及び前記第一の有効期間よりも短い第二の有効期間を有するように前記第二のデジタル証明書を発行することと、を含む、コンピュータ実施方法。

【００８１】

２．

前記エンティティの検証を証明機関サービスに可能にさせる前記重大な拡張子が、さらに、前記エンティティの前記サーバを認証するために前記第一のデジタル証明書が使用されることを阻止する、条項１に記載のコンピュータ実施方法。

【００８２】

３．

前記重大な拡張子が、前記第一のデジタル証明書の発行よりも前の、前記証明機関サービスによる前記エンティティの検証の日付、前記エンティティを検証するために前記証明機関サービスによって利用される一つ以上の基準、及び前記エンティティに対応する識別子を規定する、条項１または２に記載のコンピュータ実施方法。

【００８３】

４．

前記第二のデジタル証明書が、さらに、前記第一のデジタル証明書に規定された前記第一の公開暗号鍵とは異なる第二の公開暗号鍵を含む、条項１～３のいずれか１項に記載のコンピュータ実施方法。

【００８４】

５．

一つ以上のサービスを実施するように構成された少なくとも一つのコンピューティングデバイスを備えたシステムであって、前記一つ以上のサービスが、
第一のデジタル証明書をエンティティに発行し、ここで、前記第一のデジタル証明書が、
前記エンティティの検証を前記一つ以上のサービスに可能にさせ、かつ
前記エンティティに特有の少なくとも一つのサブジェクトフィールドを規定し、
前記エンティティから、第二のデジタル証明書を発行するためのリクエストを受信し、ここで、前記リクエストが、前記エンティティを認証するために使用可能な前記第一のデジタル証明書及び前記第二のデジタル証明書を含み、
前記第一のデジタル証明書内の規定の情報に少なくともある程度基づいて、前記第二のデジタル証明書を発行するか否かを決定し、かつ
前記第一のデジタル証明書内の規定の前記情報に少なくともある程度基づく情報、及び前記エンティティに特有の前記少なくとも一つのサブジェクトフィールドを有するように前記第二のデジタル証明書を発行するように構成された、前記システム。

【００８５】

６．

前記第二のデジタル証明書を発行するための前記リクエストがデジタル署名を含み、かつ
前記一つ以上のサービスが、さらに、前記第一のデジタル証明書内の規定の公開暗号鍵を使用して前記デジタル署名を確認するように構成された、条項５に記載のシステム。

【００８６】

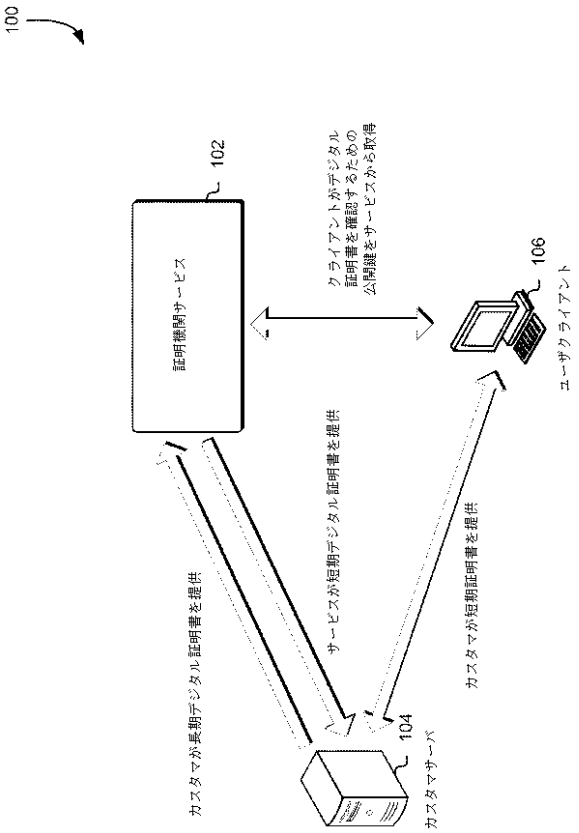
７．

前記第一のデジタル証明書内の規定の前記情報が、前記第一のデジタル証明書についての有効期間を含み、かつ
前記一つ以上のサービスが、さらに、前記第一のデジタル証明書についての前記有効期間を利用して、前記第一のデジタル証明書が満期になってなく、かつ前記第二のデジタル証明書を発行するために利用できることを確認するように構成された、条項５または６に

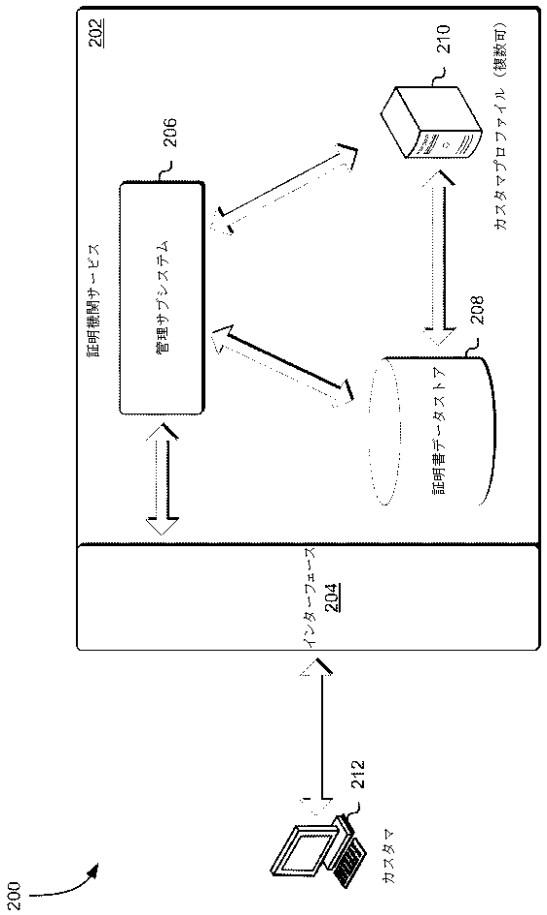
記載のシステム。
【００８７】
８．
前記第二のデジタル証明書の前記情報が、前記第一のデジタル証明書についての前記有効期間よりも短い有効期間を規定する、条項７に記載のシステム。
【００８８】
９．
前記第二のデジタル証明書に含まれる前記情報が、さらに、前記第二のデジタル証明書を発行するための前記リクエスト内の、前記エンティティによって規定された有効期間に少なくともある程度基づく、条項５～８のいずれか１項に記載のシステム。
【００８９】
１０．
前記第二のデジタル証明書が、さらに、前記第一のデジタル証明書内に含まれない一つ以上の追加のサブジェクトフィールドを有するように発行された、条項５～９のいずれか１項に記載のシステム。
【００９０】
１１．
前記第一のデジタル証明書が、前記第一のデジタル証明書を認証のために使用すべきでないことを表す重大な拡張子を規定する、条項５～１０のいずれか１項に記載のシステム。
【００９１】
１２．
前記重大な拡張子が、前記第一のデジタル証明書の発行よりも前の、前記一つ以上のサービスによる前記エンティティの検証の日付、前記エンティティを検証するために前記一つ以上のサービスによって利用される一つ以上の基準、及び前記エンティティに対応する識別子を含む、条項１１に記載のシステム。
【００９２】
１３．
コンピュータシステムの一つ以上のプロセッサによって実行されたときに、前記コンピュータシステムに、少なくとも、
エンティティから、前記エンティティを認証するために使用可能なデジタル証明書を発行するためのリクエストを受信させる、ここで、前記リクエストが、証明機関サービスが前記エンティティを検証し、かつ前記エンティティに特有の少なくとも一つのサブジェクトフィールドを規定するのに使用可能な以前に発行されたデジタル証明書を含み、
前記以前に発行されたデジタル証明書内の規定の情報に少なくともある程度基づいて、前記デジタル証明書を発行するか否かを決定させる、及び
前記以前に発行されたデジタル証明書内の規定の前記情報に少なくともある程度基づく情報、及び前記エンティティに特有の前記少なくとも一つのサブジェクトフィールドを有する前記デジタル証明書を発行させる、実行可能命令をそこに保存した非一時的コンピュータ可読記憶媒体。
【００９３】
１４．
前記命令が、さらに、前記コンピュータシステムの前記一つ以上のプロセッサによって実行されたときに、前記コンピュータシステムに、前記リクエスト内の前記エンティティによって規定された所望の有効期間を取得させて、前記第二のデジタル証明書を発行するか否かを決定させる命令を含む、条項１３に記載の非一時的コンピュータ可読記憶媒体。
【００９４】
１５．
前記以前に発行されたデジタル証明書が、前記以前に発行されたデジタル証明書を発行するための、前記エンティティからのリクエストに応答して、前記コンピュータシステム

によって発行された、条項１３または１４に記載の非一時的コンピュータ可読記憶媒体。
【００９５】
１６．
前記以前に発行されたデジタル証明書が、さらに、秘密暗号鍵に対応する公開暗号鍵を規定し、
前記以前に発行されたデジタル証明書内の規定の前記情報が、前記以前に発行されたデジタル証明書についての有効期間を含み、かつ
前記命令が、さらに、前記一つ以上のプロセッサによって実行されたときに、前記コンピュータシステムに、前記有効期間を利用させて、前記以前に発行されたデジタル証明書が満期になってなく、かつ前記デジタル証明書を発行するために利用できることを確認させる命令を含む、条項１３～１５のいずれか１項に記載の非一時的コンピュータ可読記憶媒体。
【００９６】
１７．
前記発行されたデジタル証明書内に含まれる前記情報が、前記以前に発行されたデジタル証明書についての前記有効期間よりも短い有効期間を規定する、条項１６に記載の非一時的コンピュータ可読記憶媒体。
【００９７】
１８．
前記デジタル証明書を発行するための前記リクエストが、前記公開暗号に対応する前記秘密暗号鍵を利用して前記エンティティによってデジタル署名された、条項１６または１７に記載の非一時的コンピュータ可読記憶媒体。
【００９８】
１９．
前記以前に発行されたデジタル証明書が、前記エンティティを検証するために利用される一つ以上の基準を含む重大な拡張子を規定する、条項１３～１８のいずれか１項に記載の非一時的コンピュータ可読記憶媒体。
【００９９】
２０．
前記重大な拡張子が、さらに、前記以前に発行されたデジタル証明書を認証のために使用すべきでないことを表す、条項１９に記載の非一時的コンピュータ可読記憶媒体。

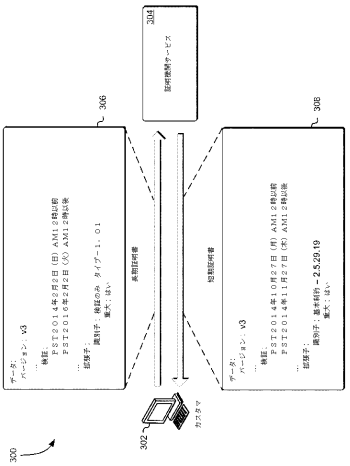
【図１】


100
102
証明機関サービス
クライアントがデジタル証明書を確認するための公開鍵をサービスから取得
106
ユーザクライアント
サービスが短期デジタル証明書を提供
カスタマが長期デジタル証明書を提供
カスタマが短期証明書を提供
104
カスタマサーバ

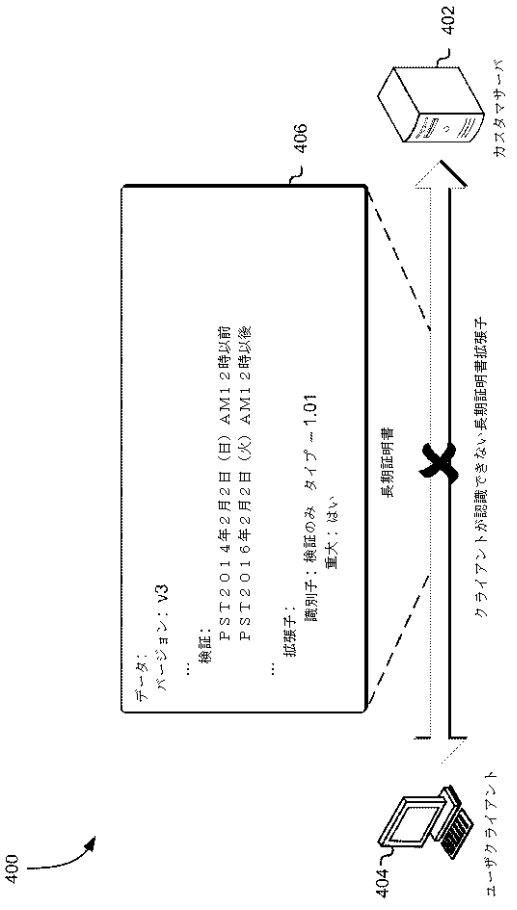
【図２】


202
証明機関サービス
206
管理サブシステム
210
カスタマプロファイル（複数可）
208
証明書データストア
インターフェース
204
212
カスタマ
200

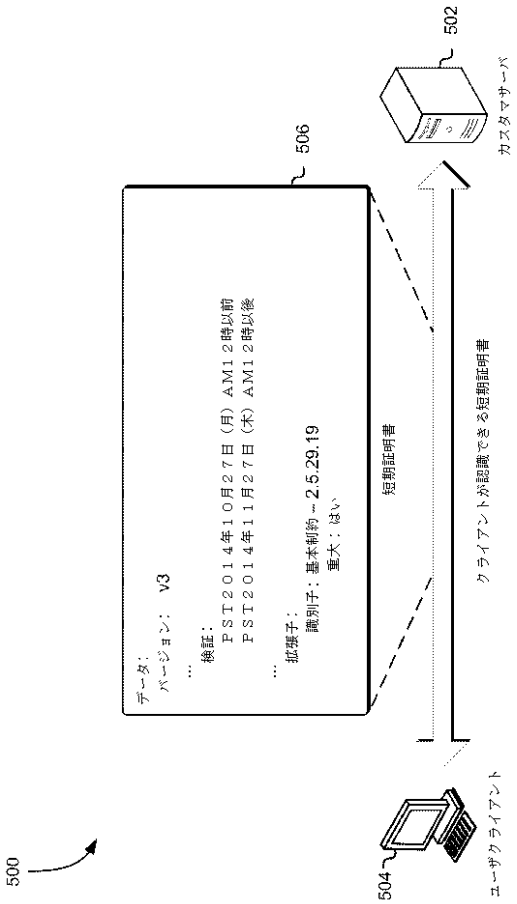
【図３】


304
306
308
302
300

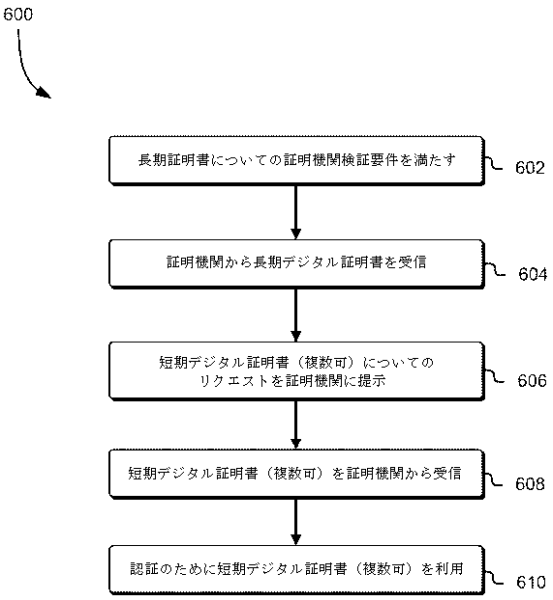
【図４】


402
カスタマサーバ
406
データ:
バージョン：v3
...
検証:
PST2014年2月2日（日）AM12時以前
PST2016年2月2日（火）AM12時以後
...
拡張子:
識別子：検証のみ タイプ＝1.01
重大：はい
長期証明書
クライアントが認識できない長期証明書拡張子
404
ユーザクライアント
400

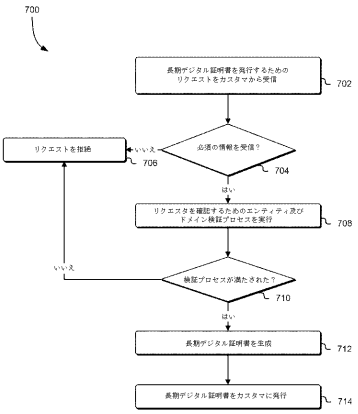
【図５】


502
カスタマサーバ
506
データ：
バージョン：v3
…
検証：
ＰＳＴ２０１４年１０月２７日（月）ＡＭ１２時以前
ＰＳＴ２０１４年１１月２７日（木）ＡＭ１２時以後
…
拡張子：
識別子：基本制約 – 2.5.29.19
重大：はい
短期証明書
クライアントが認識できる短期証明書
504
ユーザクライアント
500

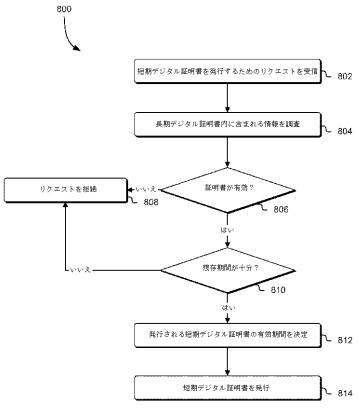
【図６】


600
長期証明書についての証明機関検証要件を満たす
602
証明機関から長期デジタル証明書を受信
604
短期デジタル証明書（複数可）についての
リクエストを証明機関に提示
606
短期デジタル証明書（複数可）を証明機関から受信
608
認証のために短期デジタル証明書（複数可）を利用
610

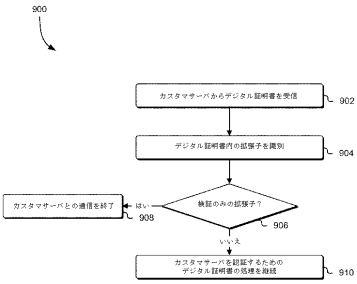
【図７】


700
長期デジタル証明書を発行するための
リクエストをカスタマから受信
702
必須の情報を受信？
704
いいえ
リクエストを拒絶
706
はい
リクエスタを確認するためのエンティティ及び
ドメイン検証プロセスを実行
708
検証プロセスが満たされた？
710
いいえ
はい
長期デジタル証明書を生成
712
長期デジタル証明書をカスタマに発行
714

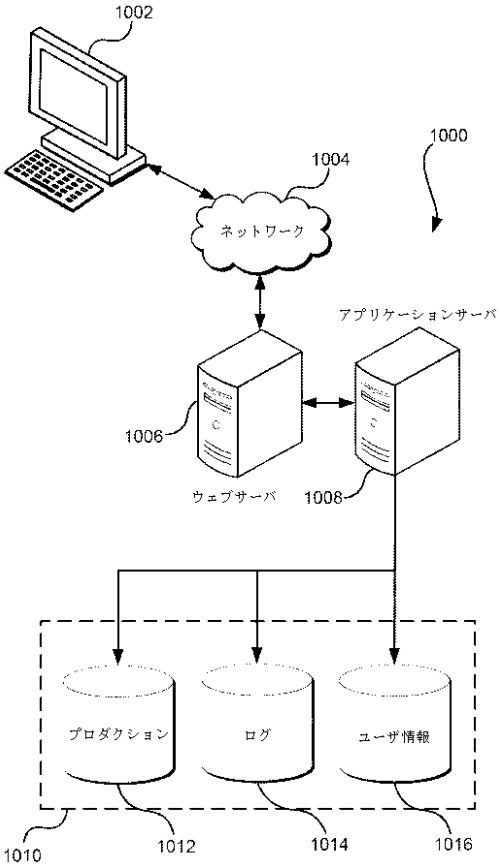
【図８】


800
短期デジタル証明書を発行するためのリクエストを受信
802
長期デジタル証明書内に含まれる情報を調査
804
証明書が有効？
806
いいえ
リクエストを拒絶
808
はい
残存期間が十分？
810
いいえ
はい
発行される短期デジタル証明書の有効期間を決定
812
短期デジタル証明書を発行
814

【図９】


900
カスタマサーバからデジタル証明書を受信
902
デジタル証明書内の拡張子を識別
904
検証のみの拡張子？
906
はい
カスタマサーバとの通信を終了
908
いいえ
カスタマサーバを認証するための
デジタル証明書の処理を継続
910

【図１０】


1002
1000
1004
ネットワーク
アプリケーションサーバ
1006
ウェブサーバ
1008
プロダクション
ログ
ユーザ情報
1010
1012
1014
1016

フロントページの続き

(56)参考文献 米国特許出願公開第２０１３／０２７５７５０（ＵＳ，Ａ１）
米国特許出願公開第２０１２／０２１０１２３（ＵＳ，Ａ１）
特開２００５－１３０４４７（ＪＰ，Ａ）
米国特許出願公開第２０１３／０１４５１５５（ＵＳ，Ａ１）
米国特許出願公開第２０１０／０２６８９４２（ＵＳ，Ａ１）
H. Housley, et al., Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Net Work Working Group Request for Comments: 2459, ［オンライン］, １９９９年 １月, Category: Standards Track, Page 1, Page 15 - Page 42, ＵＲＬ, <https://tools.ietf.org/pdf/rfc2459.pdf>
ｚ／ＯＳ Ｓｅｃｕｒｉｔｙ Ｓｅｒｖｅｒ ＰＫＩサービス ガイドおよび解説書, 日本アイ・ビー・エム株式会社, ２００２年１２月, 第1刷, ｐｐ．１５７，３６５－３６６

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／３２