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

特許第5458888号
(P5458888)

(45)発行日　平成26年4月2日(2014.4.2)　(24)登録日　平成26年1月24日(2014.1.24)

(51)Int.Cl.		F I		
G06F 21/33	(2013.01)	G06F	21/20	133
G06F 21/31	(2013.01)	G06F	21/20	131A
H04L 9/32	(2006.01)	H04L	9/00	675D

請求項の数 16　(全 43 頁)

(21)出願番号　特願2009-534291 (P2009-534291)
(86)(22)出願日　平成20年9月17日(2008.9.17)
(86)国際出願番号　PCT/JP2008/066715
(87)国際公開番号　WO2009/041319
(87)国際公開日　平成21年4月2日(2009.4.2)
審査請求日　平成23年8月12日(2011.8.12)
(31)優先権主張番号　特願2007-247597 (P2007-247597)
(32)優先日　平成19年9月25日(2007.9.25)
(33)優先権主張国　日本国(JP)

(73)特許権者　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　100123788
弁理士　宮崎　昭夫
(74)代理人　100106138
弁理士　石橋　政幸
(74)代理人　100127454
弁理士　緒方　雅昭
(72)発明者　五味　秀仁
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　畠山　誠
東京都港区芝五丁目７番１号　日本電気株式会社内

最終頁に続く

(54)【発明の名称】証明書生成配布システム、証明書生成配布方法およびプログラム

(57)【特許請求の範囲】
【請求項１】
利用者を認証する認証装置と、サービスを提供するサービス提供装置と、前記サービス提供装置によるサービス提供を仲介するサービス仲介装置とを備えた証明書生成配布システムであって、
前記認証装置は、前記サービス仲介装置において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともに前記サービス仲介装置に送信するトークン送信手段を含み、
前記サービス仲介装置は、前記トークン送信手段が送信した証明書生成要求トークンを受信し、前記サービス提供装置に転送する仲介装置トークン転送手段を含み、
前記サービス提供装置は、前記仲介装置トークン転送手段が送信した証明書生成要求トークンを受信し、当該サービス提供装置において有効な第２の証明書を要求する際に前記証明書生成要求トークンを前記認証装置に送信する証明書要求手段を含み、
前記認証装置は、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証明書を、前記証明書要求手段による第２の証明書の要求に応じて前記サービス提供装置に送信する証明書送信手段を含む、証明書生成配布システム。
【請求項２】
証明書送信手段は、第２の証明書とともに、当該第２の証明書に対応付けた情報である証明書生成要求トークンをサービス提供装置に送信し、
サービス提供装置は、前記証明書送信手段が送信した証明書生成要求トークンを他のサ

ービス提供装置に転送する提供装置トークン転送手段を含む、請求項１に記載の証明書生成配布システム。
【請求項３】
サービス仲介装置は、認証装置に第１の証明書を要求する要求手段を含み、
前記要求手段は、第１の証明書を要求する際に、所定のサービス提供装置を示す情報を前記認証装置に送信し、
証明書送信手段は、受信した所定のサービス提供装置を示す情報に基づいて、第２の証明書を送信するか否かを判断する、請求項１または２に記載の証明書生成配布システム。
【請求項４】
認証装置は、証明書生成要求トークンを生成する認証装置トークン生成手段を含み、
トークン送信手段は、前記認証装置トークン生成手段が生成した証明書生成要求トークンをサービス仲介装置に送信する、請求項１から３のうちのいずれか１項に記載の証明書生成配布システム。
【請求項５】
サービス仲介装置は、証明書生成要求トークンを生成する仲介装置トークン生成手段を含み、
トークン送信手段は、前記仲介装置トークン生成手段が生成した証明書生成要求トークンを受信し、第１の証明書に対応付けてサービス仲介装置に送信する、請求項１から３のうちのいずれか１項に記載の証明書生成配布システム。
【請求項６】
サービスを提供するサービス提供装置と、前記サービス提供装置によるサービス提供を仲介するサービス仲介装置のそれぞれと接続され、利用者を認証する認証装置であって、
前記サービス仲介装置において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともに前記サービス仲介装置に送信するトークン送信手段と、
前記サービス仲介装置から転送された前記証明書生成要求トークンを受信した前記サービス提供装置から、該サービス提供装置において有効な第２の証明書の要求および前記証明書生成要求トークンを受信すると、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証明書を前記サービス提供装置に送信する証明書送信手段と、
を有する認証装置。
【請求項７】
証明書送信手段は、第２の証明書とともに、当該第２の証明書に対応付けた情報である証明書生成要求トークンをサービス提供装置に送信する、請求項６に記載の認証装置。
【請求項８】
証明書送信手段は、サービス仲介装置から所定のサービス提供装置を示す情報を受信し、受信した情報に基づいて、第２の証明書を送信するか否かを判断する、請求項６または７に記載の認証装置。
【請求項９】
認証装置は、証明書生成要求トークンを生成する認証装置トークン生成手段を備え、
トークン送信手段は、前記認証装置トークン生成手段が生成した証明書生成要求トークンをサービス仲介装置に送信する、請求項６から８のうちのいずれか１項に記載の認証装置。
【請求項１０】
トークン送信手段は、サービス仲介装置が生成した証明書生成要求トークンを受信し、第１の証明書に対応付けてサービス仲介装置に送信する、請求項６から８のうちのいずれか１項に記載の認証装置。
【請求項１１】
利用者を認証する認証装置が、サービスを提供するサービス提供装置および前記サービス提供装置によるサービス提供を仲介するサービス仲介装置に、証明書を配布する証明書

生成配布方法であって、
前記認証装置が、前記サービス仲介装置において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともに前記サービス仲介装置に送信するトークン送信ステップを含み、
前記サービス仲介装置が、前記トークン送信ステップで送信した証明書生成要求トークンを受信し、前記サービス提供装置に転送する仲介装置トークン転送ステップを含み、
前記サービス提供装置が、前記仲介装置トークン転送ステップで送信した証明書生成要求トークンを受信し、当該サービス提供装置において有効な第２の証明書を要求する際に前記証明書生成要求トークンを前記認証装置に送信する証明書要求ステップを含み、
前記認証装置が、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証明書を、前記証明書要求ステップにおける第２の証明書の要求に応じて前記サービス提供装置に送信する証明書送信ステップを含む、証明書生成配布方法。
【請求項１２】
認証装置が、証明書送信ステップで、第２の証明書とともに、当該第２の証明書に対応付けた情報である証明書生成要求トークンをサービス提供装置に送信し、
サービス提供装置が、前記証明書送信ステップで送信した証明書生成要求トークンを他のサービス提供装置に転送する提供装置トークン転送ステップを含む、請求項１１に記載の証明書生成配布方法。
【請求項１３】
サービス仲介装置が、認証装置に第１の証明書を要求する要求ステップを含み、
前記要求ステップで、第１の証明書を要求する際に、所定のサービス提供装置を示す情報を前記認証装置に送信し、
前記認証装置が、証明書送信ステップで、受信した所定のサービス提供装置を示す情報に基づいて、第２の証明書を送信するか否かを判断する、請求項１１または１２に記載の証明書生成配布方法。
【請求項１４】
認証装置が、証明書生成要求トークンを生成する認証装置トークン生成ステップを含み、
前記認証装置が、トークン送信ステップで、前記認証装置トークン生成ステップで生成した証明書生成要求トークンをサービス仲介装置に送信する、請求項１１から１３のうちのいずれか１項に記載の証明書生成配布方法。
【請求項１５】
サービス仲介装置が、証明書生成要求トークンを生成する仲介装置トークン生成ステップを含み、
認証装置が、トークン送信ステップで、前記仲介装置トークン生成ステップで生成した証明書生成要求トークンを受信し、第１の証明書に対応付けてサービス仲介装置に送信する、請求項１１から１３のうちのいずれか１項に記載の証明書生成配布方法。
【請求項１６】
利用者を認証する認証装置が、サービスを提供するサービス提供装置および前記サービス提供装置によるサービス提供を仲介するサービス仲介装置に、証明書を配布するための証明書生成配布処理のうち、前記認証装置の処理をコンピュータに実行させるためのプログラムであって、
前記コンピュータに、
前記サービス仲介装置において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともに前記サービス仲介装置に送信するトークン送信処理と、
前記サービス仲介装置から転送された前記証明書生成要求トークンを受信した前記サービス提供装置から、該サービス提供装置において有効な第２の証明書の要求および前記証明書生成要求トークンを受信すると、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証明書を前記サービス提供装置に送信する証明書送信

処理と、
を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、証明書生成配布システム、証明書生成配布方法および証明書生成配布用プログラムに関し、特に、証明書を動的、かつ、効率的に生成し配布することを可能とする証明書生成配布システム、証明書生成配布方法、及び証明書生成配布用プログラムに関する。また、本発明は、証明書生成配布システムが備える認証装置、サービス仲介装置、サービス提供装置に関する。また、本発明は、サービス仲介装置証明書生成配布プログラムおよびサービス提供装置証明書生成配布プログラムに関する。
【背景技術】
【０００２】
近年、ネットワークを介して様々なサービスを公開する分散システムが増えている。それに伴い、ネットワーク上のサービス事業者にとって、ネットワークを通じてアクセスする利用者の認証や認可は重要な課題となってきている。所定の利用者のみに限定してそれらのサービスへのアクセスを許可したい場合には、利用者に関する認証結果などを記載した証明書を、サービス事業者が提供するサービスシステムに配布し、利用者のアクセスを可能にしていることが多い。
【０００３】
上記の技術として、標準化団体ＯＡＳＩＳで策定された、ネットワーク上の各事業者間で利用者に関する認証情報を連携するための標準技術仕様ＳＡＭＬ（Security Assertion Markup Language）がある。ＳＡＭＬを利用した証明書生成配布システムの一例が、非特許文献１に記載されている。図１は、非特許文献１に記載されている証明書生成配布システムの例を示す説明図である。図２は、非特許文献１に記載されている証明書生成配布システムを適用して代理アクセス処理を行う場合の例を説明するための説明図である。
【０００４】
非特許文献１に記載された証明書生成配布システムは、ＩｄＰ（アイデンティティプロバイダ）１００と、ＳＰ（サービスプロバイダ）１０１と、ユーザエージェント（利用者端末のソフトウェア）１０２とを備える。ＩｄＰ１００、ＳＰ１０１およびユーザエージェント１０２は、インターネット等のネットワークを介して接続される。
【０００５】
このような構成を有する非特許文献１に記載された証明書生成配布システムの典型的な動作として、Ｗｅｂ　ＳＳＯプロトコルのアーティファクトプロファイルを用いて認証証明書の作成と配布によってシングルサインオンを実現する際に、ＩｄＰとＳＰ間で行われる手順を以下において説明する。
【０００６】
図１に示す例では、前提として、利用者は、ＩｄＰ１００の利用者情報１０３とＳＰ１０１の利用者情報１０４のそれぞれに、アカウントを保有している。また、両アカウントは事前に連携されている。すなわち、両アカウントは関連付けて記憶されている。例えば、ＩｄＰ１００は、利用者を認証すると、ＳＰ１０１に認証結果情報を送信する。ＳＰ１０１は、受信した認証結果情報に基づいて利用者が認証されていると判断し、サービスを提供する（シングルサインオン）。
【０００７】
図１に示すように、利用者は、ユーザエージェント１０２を用いて、ＩｄＰ１００の認証を受け、ログインする（ステップＳ１）。その後、利用者（ユーザエージェント１０２）は、ＳＰ１０１が提供する利用制限のあるサービスを利用するために、ＳＰ１０１にアクセスする（ステップＳ２）。
【０００８】
ＳＰ１０１は、利用者の認証のために、ユーザエージェント１０２に対して認証要求メ

ッセージを送付する（ステップＳ３－ａ）、ユーザエージェント１０２は、ＳＰ１０１からの認証要求メッセージをＩｄＰ１００にリダイレクト（転送）する（ステップＳ３－ｂ）。ＩｄＰ１００は、先にステップＳ１において利用者を認証していることを確認し、利用者が認証済みであることを証明するＸＭＬ記述の認証証明書（認証アサーション）を作成する（ステップＳ４）。

【０００９】

さらに、ＩｄＰ１００は、認証アサーションに対応するチケットの役割を担うアーティファクトを作成し、ユーザエージェント１０２に返信する（ステップＳ５－ａ）。ユーザエージェント１０２は、アーティファクトをＳＰ１０１に対してリダイレクトする（ステップＳ５－ｂ）。ＳＰ１０１は、アーティファクトを受信し、ＩｄＰ１００に送付して、対応する認証アサーションを要求する（ステップＳ６）。ＩｄＰ１００は、ＳＰ１０１から受け取ったアーティファクトを確認し、対応する認証アサーションをＳＰ１０１に対して返信する（ステップＳ７）。ＳＰ１０１は、ＩｄＰ１００から受信した認証アサーションの正当性を確認し、利用者のサービスへのアクセス要求に対して許可を与えるか否かをＳＰ１０１のセキュリティポリシを用いて検証する。許可を与える場合には、ＳＰ１０１は、ユーザエージェント１０２にサービスの提供を開始する（ステップＳ８）。

【００１０】

以上に説明したように、ＩｄＰ１００は、利用者に関する証明書を作成し、それをＳＰ１０１に対して配布する。ここで、ＩｄＰ１００が配布する証明書には、上述したように、ＩｄＰ１００とＳＰ１０１のそれぞれにおける利用者のアカウントを関連付ける情報として、ＩｄＰ１００とＳＰ１０１との間でのみ有効な仮名情報や、証明書の有効範囲（配布されて有効となる対象の事業者）情報や、その他利用者に関する機密情報などを記載することが可能となっている。すなわち、ＩｄＰ１００が配布する証明書は、セキュリティ情報の所定の対象以外への漏洩を防止する機能を備えている。なお、非特許文献１は、以下に示す文献である。

【非特許文献１】著者：ＯＡＳＩＳ、表題：”Ａｓｓｅｒｔｉｏｎｓ ａｎｄ Ｐｒｏｔｏｃｏｌ ｆｏｒ ｔｈｅ ＯＡＳＩＳ Ｓｅｃｕｒｉｔｙ Ａｓｓｅｒｔｉｏｎ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ（ＳＡＭＬ） Ｖ２．０”、媒体のタイプ：online、掲載年月日：２００５年3月１５日、検索日：２００７年5月３０日、情報源：インターネット＜ＵＲＬ：http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf＞

【発明の開示】

【００１１】

ＩｄＰで認証を受け、第１のＳＰのサービスにアクセスしている利用者に関して、第１のＳＰが、第１のＳＰとは異なる第２のＳＰに利用者の代理アクセスを試みる際に、第２のＳＰは、ＩｄＰからの利用者に関する証明書の配布を必要とする。この場合に、非特許文献１に記載されている証明書生成配布システムでは、証明書の作成と配布に必要となる通信が非効率的となるという問題がある。

【００１２】

その理由は、非特許文献１に記載されている方式では、ＳＰ間（第１のＳＰと第２のＳＰとの間）で、利用者に関する利用者情報または証明書情報を交換する手段がなく、第１のＳＰにユーザエージェントの機能がない場合、第２のＳＰは、ユーザエージェントを介して、証明書の要求及び配布を受ける必要があるからである。すなわち、第１のＳＰがユーザエージェント１０２を介した認証処理（ステップＳ３－ａ～Ｓ７）を既に行っているにも関わらず、第２のＳＰは、第１のＳＰおよびユーザエージェント１０２を介して同じ処理（ステップＳ３－ａ～Ｓ７）を行わなければならないため、第２のＳＰとＩｄＰとの間の通信が非効率的になるという問題がある。

【００１３】

本発明の目的は、上述した課題を解決する証明書生成配布システム、認証装置、サービス仲介装置、サービス提供装置、証明書生成配布方法、証明書生成配布用プログラム、サービス仲介装置証明書生成配布プログラム、およびサービス提供装置証明書生成配布プロ

グラムを提供することにある。

【００１４】

本発明による証明書生成配布システムは、利用者を認証する認証装置と、サービスを提供するサービス提供装置と、サービス提供装置によるサービス提供を仲介するサービス仲介装置とを備えた証明書生成配布システムであって、認証装置は、サービス仲介装置において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともにサービス仲介装置に送信するトークン送信手段を含み、サービス仲介装置は、トークン送信手段が送信した証明書生成要求トークンを受信し、サービス提供装置に転送する仲介装置トークン転送手段を含み、サービス提供装置は、仲介装置トークン転送手段が送信した証明書生成要求トークンを受信し、サービス提供装置において有効な第２の証明書を要求する際に証明書生成要求トークンを認証装置に送信する証明書要求手段を含み、認証装置は、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証明書を、証明書要求手段による第２の証明書の要求に応じてサービス提供装置に送信する証明書送信手段を含む。

【００１５】

本発明による認証装置は、サービスを提供するサービス提供装置と、サービス提供装置によるサービス提供を仲介するサービス仲介装置のそれぞれと接続され、利用者を認証する認証装置であって、サービス仲介装置において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともに前記サービス仲介装置に送信するトークン送信手段と、サービス仲介装置から転送された証明書生成要求トークンを受信したサービス提供装置から、サービス提供装置において有効な第２の証明書の要求および証明書生成要求トークンを受信すると、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証明書をサービス提供装置に送信する証明書送信手段と、を備えている。

【００１８】

本発明による証明書生成配布方法は、利用者を認証する認証装置が、サービスを提供するサービス提供装置およびサービス提供装置によるサービス提供を仲介するサービス仲介装置に、証明書を配布する証明書生成配布方法であって、認証装置が、サービス仲介装置において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともにサービス仲介装置に送信するトークン送信ステップを含み、サービス仲介装置が、トークン送信ステップで送信した証明書生成要求トークンを受信し、サービス提供装置に転送する仲介装置トークン転送ステップを含み、サービス提供装置が、仲介装置トークン転送ステップで送信した証明書生成要求トークンを受信し、サービス提供装置において有効な第２の証明書を要求する際に認証装置に送信する証明書要求ステップを含み、認証装置が、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証明書を、証明書要求ステップにおける第２の証明書の要求に応じてサービス提供装置に送信する証明書送信ステップを含む。

【００１９】

本発明によるプログラムは、利用者を認証する認証装置が、サービスを提供するサービス提供装置およびサービス提供装置によるサービス提供を仲介するサービス仲介装置に、証明書を配布するための証明書生成配布処理のうち、認証装置の処理をコンピュータに実行させるためのプログラムであって、コンピュータに、サービス仲介装置において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともにサービス仲介装置に送信するトークン送信処理と、サービス仲介装置から転送された証明書生成要求トークンを受信したサービス提供装置から、サービス提供装置において有効な第２の証明書の要求および証明書生成要求トークンを受信すると、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証明書をサービス提供装置に送信する証明書送信処理と、を実行させるものである。

【図面の簡単な説明】

【００２３】

【図１】図１は非特許文献１に記載されている証明書生成配布システムの例を示す説明図である。
【図２】図２は非特許文献１に記載されている証明書生成配布システムにおける代理アクセス処理の例を説明するための説明図である。
【図３】図３は本発明による証明書生成配布システムの最小の構成例を示すブロック図である。
【図４】図４は本発明による証明書生成配布システムの構成例を示すブロック図である。
【図５】図５は認証装置の構成の一例を示すブロック図である。
【図６】図６はサービス仲介装置の構成の一例を示すブロック図である。
【図７】図７は証明書管理部の構成の一例を示すブロック図である。
【図８】図８はサービス提供装置の構成の一例を示すブロック図である。
【図９】図９はサービス提供装置用証明書管理部の構成の一例を示すブロック図である。
【図１０】図１０はサービス管理部の構成の一例を示すブロック図である。
【図１１】図１１は認証装置がサービス仲介装置からの証明書配布要求を受信する場合の処理の例を示す流れ図である。
【図１２】図１２は認証装置がサービス提供装置からの証明書生成要求を受信する場合の処理の例を示す流れ図である。
【図１３】図１３はサービス提供装置が、サービスのアクセス要求を受ける場合の処理の例を示す流れ図である。
【図１４】図１４はサービス仲介装置がサービス提供装置へのアクセスを仲介する処理の例を示す流れ図である。
【図１５】図１５はサービス仲介装置が認証装置から証明書を受信する場合の処理の例を示す流れ図である。
【図１６】図１６はサービス提供装置が認証装置に証明書を要求して受信する場合の処理の例を示す流れ図である。
【図１７】図１７は第２の実施形態におけるサービス仲介装置の構成の一例を示すブロック図である。
【図１８】図１８は、サービス仲介装置が、サービス要求を仲介し、さらに他の装置や利用者に対してサービスを提供する場合の処理の例を示す流れ図である。
【図１９】図１９は第３の実施形態における認証装置の構成の一例を示すブロック図である。
【図２０】図２０は第３の実施形態におけるサービス仲介装置の構成の一例を示すブロック図である。
【図２１】図２１は、サービス仲介装置が、認証装置に対して証明書配布要求を行う場合の処理の例を示す流れ図である。
【図２２】図２２は認証装置がサービス仲介装置からの証明書配布要求を受信する場合の処理の例を示す流れ図である。
【図２３】図２３は第４の実施形態におけるサービス仲介装置の構成の一例を示すブロック図である。
【図２４】図２４はサービス仲介装置が、認証装置に対して証明書配布要求を行う場合の処理の例を示す流れ図である。
【図２５】図２５は認証装置がサービス仲介装置からの証明書配布要求を受信する場合の処理の例を示す流れ図である。
【図２６】図２６は本発明による証明書生成配布システムの第１の実施例を説明するための説明図である。
【図２７】図２７はアカウント対応管理表の登録例を示す説明図である。
【図２８】図２８は第１の実施例における証明書生成配布システムの動作の例を示すシーケンス図である。
【図２９】図２９は認証証明書の記載内容の一例を示す説明図である。
【図３０】図３０は証明書配布要求に対する返信メッセージの一例を示す説明図である。

【図３１】図３１は証明書生成トークンと認証証明書識別子の対応管理表の一例を示す説明図である。
【図３２】図３２はサービス提供装置向け認証証明書の一例を示す説明図である。
【図３３】図３３はレンタカー予約要求メッセージの一例を示す説明図である。
【図３４】図３４は証明書生成要求メッセージの一例を示す説明図である。
【図３５】図３５は本発明による証明書生成配布システムの第２の実施例を説明するための説明図である。
【図３６】図３６は属性証明書の生成要求メッセージの一例を示す説明図である。
【図３７】図３７は属性証明書の一例を示す説明図である。
【図３８】図３８は本発明による証明書生成配布システムの第３の実施例を説明するための説明図である。
【図３９】図３９は本発明による証明書生成配布システムの第４の実施例を説明するための説明図である。
【図４０】図４０はアカウント対応管理表の登録例を示す説明図である。
【符号の説明】
【００２４】
９００　認証装置
９０１　トークン送信手段
９０２　証明書送信手段
９１０　サービス仲介装置
９１１　仲介装置トークン転送手段
９２０　サービス提供装置
９２１　証明書要求手段
【発明を実施するための最良の形態】
【００２５】
まず、本発明の概要について図面を参照して説明する。図３は、本発明による証明書生成配布システムの最小の構成例を示すブロック図である。図３に例示する証明書生成配布システムは、認証装置９００と、サービス仲介装置９１０と、サービス提供装置９２０とを備える。
【００２６】
認証装置９００は、トークン送信手段９０１と、証明書送信手段９０２とを含む。サービス仲介装置９１０は、仲介装置トークン転送手段９１１を含む。サービス提供装置９２０は、証明書要求手段９２１を含む。
【００２７】
トークン送信手段９０１は、サービス仲介装置９１０において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともにサービス仲介装置９１０に送信する。
【００２８】
仲介装置トークン転送手段９１１は、トークン送信手段９０１が送信した証明書生成要求トークンを受信し、サービス提供装置９２０に転送する。
【００２９】
証明書要求手段９２１は、仲介装置トークン転送手段９１１が送信した証明書生成要求トークンを受信し、サービス提供装置９２０において有効な第２の証明書を要求する際に証明書生成要求トークンを認証装置９００に送信する。
【００３０】
証明書送信手段９０２は、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証明書を、証明書要求手段９２１による第２の証明書の要求に応じて、サービス提供装置９２０に送信する。
【００３１】
図３に示すように構成すれば、サービス仲介装置からの代理アクセスに応じてサービス

を提供するサービス提供装置に証明書を配布する場合に、証明書の配布に要する通信を効率化することができる。

【００３２】

（第１の実施形態）

次に、本発明の第１の実施形態を図面を参照して説明する。図４は、本発明による証明書生成配布システムの構成例を示すブロック図である。図４に示す証明書生成配布システムは、認証装置１と、サービス仲介装置２と、サービス提供装置３と、端末装置４とを備える。認証装置１、サービス仲介装置２、サービス提供装置３および端末装置４は、ネットワーク５を介して接続される。

【００３３】

認証装置１、サービス仲介装置２、サービス提供装置３および端末装置４は、それぞれ、複数存在してよい。利用者は、端末装置４を用いて、認証装置１やサービス仲介装置２に対してアクセスを行う。本発明における利用者は、個人であっても、複数の個人で構成される組織であってもよい。

【００３４】

図５は、認証装置１の構成の一例を示すブロック図である。図５に示すように、認証装置１は、利用者認証手段１０と、利用者情報管理手段１１と、証明書生成要求受付手段１２と、証明書生成要求トークン管理手段１３と、証明書生成手段１４と、証明書配布要求受付手段１５と、証明書管理手段１６と、利用者情報格納部２０と、アクセス制御ポリシ格納部２１と、証明書生成要求トークン格納部２２と、装置情報格納部２３と、証明書情報格納部２４とを含む。

【００３５】

利用者認証手段１０は、認証装置１を利用する利用者を、所定の認証方式によって認証する手段である。

【００３６】

利用者情報管理手段１１は、利用者情報格納部２０において格納される利用者に関する情報を管理する手段である。

【００３７】

利用者認証手段１０は、利用者を認証する際に、所定の認証方式に応じたクレデンシャル情報（例えば、パスワードなどの認証情報）の提示を利用者（端末装置４）に求める。利用者認証手段１０は、利用者（端末装置４）が提示した情報と、利用者情報管理手段１１を介して利用者情報格納部２０から得られる利用者の識別子と関連付けられて管理されるクレデンシャル情報とを比較照合して、認証を行う。

【００３８】

利用者認証手段１０が利用者を認証後、利用者情報管理手段１１は、利用者の認証結果情報を含むセッション情報を利用者情報格納部２０に格納する。セッション情報は、利用者の認証について認証装置１と端末装置４との間で確立したセッションを一意に識別することが可能なセッション識別子をキーとして関連付けられている情報である。利用者情報管理手段１１は、セッション識別子を用いて、利用者情報格納部２０を検索し、関連付けられるセッション情報を取得できる。

【００３９】

利用者情報格納部２０は、認証装置１を利用する利用者に関する情報を格納する。利用者情報格納部２０は、例えば、利用者の識別子情報、その属性情報、利用者認証手段１０から認証を求められた際に提示するパスワードなどのクレデンシャル情報、また、利用者認証手段１０が認証した利用者についてのセッション情報を格納する。

【００４０】

証明書生成要求受付手段１２は、サービス提供装置３からの、利用者に関する証明書の生成要求を受け付ける手段である。証明書とは、例えば、後述する図２９、図３２に例示しているＳＡＭＬが規定している認証アサーションや、図３７に例示しているＳＡＭＬが規定している属性アサーション（属性証明書）だけでなく、Ｘ．５０９の証明書などであ

る。
【００４１】
証明書要求受付手段１２は、サービス提供装置３から、利用者に関する証明書の生成要求メッセージを受けると、証明書生成要求メッセージの内容を確認して、アクセス制御ポリシ格納部２１に格納されるアクセス制御ポリシを参照して、証明書生成要求を受け付けて良いか否かの認可判断を行う機能を備える。また、証明書要求受付手段１２は、生成するべき証明書に記載可能な情報を、要求するサービス提供装置３に応じて適切な情報に変換または制限する機能を備える。
【００４２】
証明書要求受付手段１２が、判断結果として、証明書生成要求を受け付けて良いという判断をする場合、証明書生成手段１４は、要求された証明書を作成する。証明書要求受付手段１２は、証明書生成手段１４が生成した証明書を添付した応答メッセージを作成して、サービス提供装置３に対して返信する。
【００４３】
一方、判断結果として、証明書生成要求を受け付けてはいけないという判断をする場合には、証明書要求受付手段１２は、証明書生成要求を受け付けられないというエラー内容を含めた応答メッセージを作成して、サービス提供装置３に対して返信する。
【００４４】
アクセス制御ポリシ格納部２１は、証明書生成要求受付手段１２が、証明書の生成を行うための認可判断を決定するためのアクセス制御ポリシを格納する。アクセス制御ポリシは、ある情報の内容に関する条件に対して、証明書生成要求受付手段１２が取るべき動作が規定されている情報である。アクセス制御ポリシは、例えば、証明書生成要求受付手段１２がサービス提供装置３からの証明書の生成要求を受け付けた時刻が、利用者のセッション情報に含まれている所定のセッションの有効期間内であれば証明書の生成を許可する旨の規定や、証明書の生成要求を送付したサービス提供装置３が、装置情報格納部２３内のサービス提供装置に関する情報に含まれていなければ、該当する証明書の生成を許可しない旨の規定などである。アクセス制御ポリシに規定される条件及び動作は、所定のポリシ記述言語によって記述される。証明書生成要求受付手段１２は、アクセス制御ポリシを自動的に読み取ることができる。
【００４５】
証明書生成要求トークン管理手段１３は、サービス提供装置３が所定の証明書の生成を要求するために利用するトークンを管理する手段である。
【００４６】
証明書生成要求トークン管理手段１３は、利用者認証手段１０が認証し、利用者情報管理手段１１が管理する利用者のセッション情報と関連づけたセッション識別子を生成する。証明書生成要求トークン管理手段１３は、生成したセッション識別子と、認証装置１を一意に識別可能な認証装置識別子とを連接することによって、証明書生成要求トークンを生成する。
【００４７】
証明書生成要求トークン管理手段１３は、利用者やセッション情報が導出するに足る情報が含まれず、ランダムな値となるように、セッション識別子を生成する。
【００４８】
認証生成要求トークンは、例えば、非特許文献１で挙げたＳＡＭＬが規定するアーティファクトを用いて実現できる。認証生成要求トークンは、証明書と一意に対応付けられるランダムな文字列（セッション識別子）ならば、何でもよい。また、証明書生成要求トークン管理手段１３は、生成した証明書生成要求トークンを、証明書管理手段１６において管理される既に配布済みの証明書の識別子と関連付けて、証明書生成要求トークン格納部２２に格納し、後に参照可能となるように管理する。
【００４９】
証明書生成手段１４は、装置情報格納部２３が格納する装置情報を基にして、利用者に

関する認証結果情報、属性情報、権限情報などを記載した証明書を生成し、発行する手段である。証明書生成手段１４は、必要に応じて、ディジタル署名などの技術を用いて、生成する証明書に署名を付与することができる。それによって、証明書の配布先の装置は、受け取った該証明書が改ざんされていないことを検証することができる。また、証明書生成手段１４は、生成した証明書を証明書情報格納部２４に格納する。

【００５０】

装置情報格納部２３は、ビジネス上の契約などにより信頼関係を持つサービス仲介装置２またはサービス提供装置３に関する装置情報を格納し、管理する。

【００５１】

証明書配布要求受付手段１５は、サービス仲介装置２からの証明書配布要求に応じて、証明書管理手段１６を通じて、必要とする証明書を取得し、サービス仲介装置２に対して返信する手段である。

【００５２】

証明書管理手段１６は、証明書情報格納部２４に格納される証明書を管理する手段である。証明書管理手段１６は、何らかの検索キーを用いて、証明書情報格納部２４に格納される証明書から、該当する証明書を検索して参照し、所定の証明書を更新、あるいは、削除する機能を有する。

【００５３】

認証装置１がコンピュータで実現される場合には、利用者認証手段１０、利用者情報管理手段１１、証明書生成要求受付手段１２、証明書生成要求トークン管理手段１３、証明書生成手段１４、証明書配布要求受付手段１５および証明書管理手段１６は、認証装置１に搭載されるＣＰＵが、それらの機能を実現するためのプログラムを実行することによって実現される。

【００５４】

図６は、サービス仲介装置２の構成の一例を示すブロック図である。図６に示すように、サービス仲介装置２は、サービスアクセス仲介手段５０と、証明書配布要求手段５１と、証明書管理部６とを含む。

【００５５】

サービスアクセス仲介手段５０は、利用者の端末装置４またはサービス仲介装置２とは異なるサービス仲介装置（第２のサービス仲介装置）からのサービスアクセス要求（第１のサービスアクセス要求）を受けた後、第２のサービスアクセス要求をサービス提供装置３に対して行う手段である。サービスアクセス仲介手段５０は、第１のサービスアクセス要求を行った利用者に関連して、第１のサービスアクセス要求とは異なるサービスアクセス要求（第２のサービスアクセス要求）を、所定の通信プロトコルを用いて、サービス提供装置３に対して行う。

【００５６】

サービスアクセス仲介手段５０は、証明書管理部６（後述する図７を参照）内の証明書検証手段６２が管理する利用者に関して認証装置１から配布された証明書を、利用者の利用者識別子を基に取得（抽出）する。

【００５７】

また、サービスアクセス仲介手段５０は、後述する証明書生成要求トークン取得手段６１が管理する証明書に関連付けられる証明書生成要求トークンを取得し、サービス提供装置３への第２のサービスアクセス要求のメッセージに、証明書生成要求トークンを添付して、サービス提供装置３にサービスアクセス要求を行う。

【００５８】

証明書配布要求手段５１は、認証装置１に対して、所定の通信プロトコルを用いて、既に生成されている証明書の配布要求を行う手段である。

【００５９】

証明書配布要求手段５１は、証明書の配布要求を行う際に、認証装置情報管理手段６０を用いて、配布要求を送付すべき認証装置１のネットワーク上のアドレスなどの詳細情報

を取得する。また、証明書配布要求手段５１は、要求した証明書を認証装置１から受信した際、証明書にディジタル署名が施されている場合、証明書管理部６の証明書検証手段６２を用いて、証明書の検証を行うことができる。

【００６０】

さらに、証明書配布要求手段５１は、認証装置１から返信される証明書を含んだメッセージに、証明書生成要求トークンも添付されていれば、証明書管理部６の証明書生成要求トークン取得手段６１を用いて、返信メッセージから証明書生成要求トークンを取得（抽出）して解析する。

【００６１】

図７は、証明書管理部６の構成の一例を示すブロック図である。図７に示すように、証明書管理部６は、認証装置情報管理手段６０と、証明書生成要求トークン取得手段６１と、証明書検証手段６２と、認証装置情報格納部６３と、証明書情報格納部６５とを有する。

【００６２】

認証装置情報管理手段６０は、認証装置情報格納部６３が格納する認証装置１に関する情報を管理する手段である。認証装置情報管理手段６０は、証明書生成要求トークンに記載される認証装置識別子を基にして、ネットワーク上の位置情報（ＩＰ　Ａｄｄｒｅｓｓ）などの認証装置に関する詳細情報を取得する機能を持つ。

【００６３】

証明書生成要求トークン取得手段６１は、証明書配布要求手段５１が受信したメッセージから証明書生成要求トークンを取得する。

【００６４】

証明書検証手段６２は、認証装置１から受信した証明書に記載される情報の形式や内容を検証する手段である。証明書に、例えば、ディジタル署名などの署名技術による署名が付与されている場合、証明書検証手段６２は、署名の検証を行い、改ざんがされていないか検出できる。証明書検証手段６２は、証明書の検証が完了した後、検証した証明書を、適切な証明書として、証明書情報格納部６５に格納して管理する。証明書検証手段６２は、証明書の識別子や利用者の識別子などの、所定の検索キーを用いて、該当する証明書を取得する機能を持つ。

【００６５】

サービス仲介装置２がコンピュータで実現される場合には、サービスアクセス仲介手段５０、証明書配布要求手段５１、認証装置情報管理手段６０、証明書生成要求トークン取得手段６１および証明書検証手段６２は、サービス仲介装置２に搭載されるＣＰＵが、それらの機能を実現するためのプログラムを実行することによって実現される。

【００６６】

図８は、サービス提供装置３の構成の一例を示すブロック図である。図８に示すように、サービス提供装置３は、証明書生成要求手段８０と、サービス提供装置用証明書管理部６６と、サービス管理部７とを含む。

【００６７】

図９は、サービス提供装置用証明書管理部６６の構成の一例を示すブロック図である。図９に示すように、サービス提供装置用証明書管理部６６は、認証装置情報管理手段６０と、証明書生成要求トークン解析手段６６１と、証明書検証手段６２と、認証装置情報格納部６３と、証明書情報格納部６５とを有する。

【００６８】

サービス提供装置用証明書管理部６６は、サービス仲介装置２の証明書管理部６（図７を参照）における証明書要求トークン取得手段６１の代わりに、証明書生成要求トークン解析手段６６１を有する管理部である。

【００６９】

証明書生成要求トークン解析手段６６１は、サービス仲介装置２から受信した証明書生成要求トークンを解析し、そのトークンに含まれる認証装置識別子と、セッション識別子

を取得（抽出）する機能を持つ。証明書生成要求トークン解析手段６６１は、証明書生成要求トークンを管理する。

【００７０】

証明書生成要求手段８０は、証明書生成要求トークンを発行した認証装置１に対して、証明書生成要求を行うためのメッセージを、証明書生成要求トークンを添付した上で作成し、送付する手段である。

【００７１】

証明書生成要求メッセージの送付先となる認証装置１のネットワーク上のアドレスなどの詳細情報は、証明書生成要求トークン解析手段６６１および認証装置情報管理手段６０によって抽出される。証明書生成要求トークン解析手段６６１は、証明書生成要求トークンを解析し、認証装置１の認証装置識別子を抽出して認証装置情報管理手段６０に出力する。認証装置情報管理手段６０は、出力された認証装置識別子に該当する認証装置１の情報の参照要求を認証装置情報格納部６３に行うことによって、認証装置１の詳細情報を抽出する。

【００７２】

図１０は、サービス管理部７の構成の一例を示すブロック図である。図１０に示すように、サービス管理部７は、サービスアクセス受付手段７０と、サービス情報管理手段７１と、アクセス制御ポリシ格納部７２と、サービス情報格納部７３とを含む。

【００７３】

サービスアクセス受付手段７０は、サービス情報管理手段７１がサービス情報格納部７３において管理するサービス情報を利用して、所定のアプリケーションサービスを公開する。また、サービスアクセス受付手段７０は、利用者からのサービスに対するアクセスに応じ、アクセス制御ポリシ格納部７２に格納されるアクセス制御ポリシを利用して、所定の利用者からのアクセスのみ許可するように制御して、サービスを提供する手段である。

【００７４】

また、サービスアクセス受付手段７０は、サービス提供装置３以外のサービス提供装置から、所定の通信プロトコルを利用して証明書生成要求トークンを受信する機能を備える。

【００７５】

アクセス制御ポリシ格納部７２には、サービスアクセス受付手段７０が提供するサービスの提供方法を、所定の利用者や状況に応じて制御するためのアクセス制御ポリシを格納する。アクセス制御ポリシは、ある情報に関する条件に対して、サービスアクセス受付手段７０の取るべき動作が規定されている情報である。例えば、アクセス制御ポリシは、所定の属性情報を保有する利用者に対してのみ、サービスへのアクセスを許可する旨の規定や、所定の時間帯においてのみ、所定の利用者のサービスへのアクセスを許可しない旨の規定などである。アクセス制御ポリシに規定される条件及び動作は、所定のポリシ記述言語によって記述される。サービスアクセス受付手段７０は、アクセス制御ポリシを自動的に読み取ることができる。

【００７６】

サービス情報管理手段７１は、サービス情報格納部７３が格納する所定のサービス固有の情報を管理する手段である。また、サービス情報管理手段７１は、サービスの内容に合わせて、サービス情報格納部７３が格納する利用者に関する情報を管理する。

【００７７】

サービス提供装置３がコンピュータで実現される場合には、証明書生成要求手段８０、認証装置情報管理手段６０、証明書生成要求トークン解析手段６６１、証明書検証手段６２、サービスアクセス受付手段７０およびサービス情報管理手段７１は、サービス提供装置３に搭載されるＣＰＵが、それらの機能を実現するためのプログラムを実行することによって実現される。

【００７８】

端末装置４は、利用者が直接に操作し、認証装置１の利用者認証手段１０が利用者を認

証するために要求するクレデンシャル情報を送信し、サービス仲介装置２の提供するサービスを利用するための通信機能を備える。

【００７９】

上記の認証装置１、サービス仲介装置２、サービス提供装置３および端末装置４は、それぞれ通信手段（図示せず。）を備える。認証装置１、サービス仲介装置２、サービス提供装置３および端末装置４における各通信手段は、互いに通信する場合には、ＳＳＬ（Secure Sockets Layer）やＴＬＳ（Transport Layer Security）などの機構、または、それらに相当する、送受信するメッセージの第３者による傍受を防止する機構を備えている。また、認証装置１、サービス仲介装置２、サービス提供装置３および端末装置４は、互いに送受信するメッセージの内容を所定の通信相手にのみ通知し、意図した通信相手に露呈することを防止するための暗号化機能を備え、その暗号化情報を受け取った場合に解読するための複合化機能を備えている。

【００８０】

次に、図１１～図１６を参照して第１の実施形態の動作について説明する。

【００８１】

まず、図１１および図１２を参照して、認証装置１の動作について説明する。認証装置１は、利用者やサービス提供装置３から送付される所定の要求メッセージを受信可能な状態にある。認証装置１は、アクセス要求を解析した上で、その要求内容に応じた動作処理を行う。以下、認証装置１が端末装置４の利用者を認証して認証証明書を生成した後の、本発明における特徴的な動作を説明する。

【００８２】

認証装置１が、サービス仲介装置２からの証明書配布要求を受信する場合の動作に関して、図１１を参照して説明する。図１１は、認証装置１がサービス仲介装置２からの証明書配布要求を受信する場合の処理の例を示す流れ図である。

【００８３】

認証装置１が、サービス仲介装置２からの証明書配布要求を受信すると（ステップＳ１１０１）、証明書配布要求受付手段１５は、証明書配布要求メッセージを解析し、証明書配布要求メッセージから、証明を要求する対象の利用者、証明書を要求したサービス仲介装置２および要求する証明書の種類や内容などの情報を取得（抽出）する（ステップＳ１１０２）。

【００８４】

次に、証明書配布要求受付手段１５は、ステップＳ１１０２で取得した証明書配布要求の内容情報を参照し、アクセス制御ポリシ格納部２１が格納するアクセス制御ポリシと照合して、証明書配布要求を許可するか否かの認可判断を決定する（ステップＳ１１０３）。

【００８５】

ステップＳ１１０３において、証明書配布要求を許可しない場合（Ｎｏ）、証明書配布要求受付手段１５は、証明書配布要求を認可しない旨のエラーメッセージを作成して（ステップＳ１１０９）、サービス仲介装置２に対して返信する（ステップＳ１１０８）。

【００８６】

一方、ステップＳ１１０３において、証明書配布要求を許可する場合（Ｙｅｓ）、証明書管理手段１６は、証明書配布要求の内容情報に基づいて、証明書情報格納部２４から、該当する証明書を検索して取得し（ステップＳ１１０４）、証明書配布要求受付手段１５に送付する。次に、証明書配布要求受付手段１５は、取得した証明書を、証明書生成要求トークン管理手段１３に送付する。

【００８７】

証明書生成要求トークン管理手段１３は、サービス提供装置３が証明書生成要求を行うための証明書生成要求トークンを、乱数を発生させることによって生成する（ステップＳ１１０５）。そして、証明書生成要求トークン管理手段１３は、生成した証明書生成要求トークンを、受け取った証明書と関連付けて管理する（ステップＳ１１０６）。例えば、

証明書生成要求トークン管理手段１３は、証明書識別子と証明書生成要求トークンとを関連付けて、証明書生成要求トークン格納部２２に記憶させる。そして、証明書生成要求トークン管理手段１３は、生成した証明書生成要求トークンを、証明書配布要求受付手段１５に返信する。

【００８８】

次に、証明書配布要求受付手段１５は、証明書生成要求トークン管理手段１３から受け取った証明書生成要求トークンとステップＳ１１０５において取得した証明書とを添付した、証明書配布要求に対する返信メッセージを作成して（ステップＳ１１０７）、サービス仲介装置２に対して返信する（ステップＳ１１０８）。

【００８９】

なお、上記のステップＳ１１０１からステップＳ１１０８の動作においては、認証装置１がサービス仲介装置２からの証明書配布要求を受信する場合を説明したが、サービス仲介装置２からの証明書配布要求が端末装置４を経由して行われる場合、すなわち、認証装置１が端末装置４から証明書配布要求を受信する場合もありうる。この場合には、上記ステップＳ１１０１からステップＳ１１０８の動作において、サービス仲介装置２を端末装置４と読み替えてよい。

【００９０】

次に、認証装置１が、あるサービス提供装置３からの証明書生成要求を受信する場合の認証装置１の動作に関して、図１２を参照して説明する。図１２は、認証装置１がサービス提供装置３からの証明書生成要求を受信する場合の処理の例を示す流れ図である。

【００９１】

認証装置１が、あるサービス提供装置３からの証明書生成要求を受信すると（ステップＳ１２０１）、証明書生成要求受付手段１２は、証明書作成要求メッセージを解析し、証明書作成要求メッセージから、作成するべき証明書の種類と内容を特定して証明書生成要求トークンを抽出する（ステップＳ１２０２）。

【００９２】

次に、証明書生成要求受付手段１２は、サービス提供装置３からの証明書作成要求の受付を許可するか否かの認可判断を、アクセス制御ポリシ格納部２１が格納するセキュリティポリシを参照することによって行う（ステップＳ１２０３）。証明書生成要求を許可しないと判断した場合（Ｎｏ）、証明書生成要求受付手段１２は、エラーメッセージを作成して（ステップＳ１２０４）、サービス提供装置３に対して返信する（ステップＳ１２１１）。

【００９３】

一方、ステップＳ１２０３において、証明書生成要求を許可するという認可判断に至った場合（Ｙｅｓ）、証明書生成要求受付手段１２は、抽出した証明書生成要求トークンを証明書生成要求トークン管理手段１３に送付する。

【００９４】

証明書生成要求トークン管理手段１３は、証明書生成要求トークン格納部２２から、受け取った証明書生成要求トークンと関連付けられた証明書識別子を取得する。証明書生成要求トークン管理手段１３は、証明書識別子を証明書管理手段１６に送付する。

【００９５】

証明書管理手段１６は、証明書識別子を基に、証明書情報格納部２４から該当する証明書を取得し（ステップＳ１２０５）、証明書生成要求受付手段１２に返信する。

【００９６】

証明書生成要求受付手段１２は、証明書に記載されている情報から、証明書に関連する利用者識別子とそのセッション識別子を取得し、サービス提供装置３に関する情報と合わせて、利用者情報管理手段１１に送付する。

【００９７】

利用者情報管理手段１１は、利用者識別子とセッション識別子とサービス提供装置３に関する情報とを基に、利用者情報格納部２０から、サービス提供装置３と関連付けられた

利用者に関する情報及びセッション情報を取得し（ステップＳ１２０６）、証明書生成要求受付手段１２に送付する。

【００９８】

次に、証明書生成要求受付手段１２は、証明書生成手段１４に対して、サービス提供装置３と関連付けられた利用者に関する情報及びそのセッション情報を添付した証明書生成要求を行う。

【００９９】

証明書生成手段１４は、サービス提供装置３に関する情報として必要な情報を装置情報格納部２３から取得した上で、利用者に関する情報及びそのセッション情報を利用し、要求された証明書を生成し（ステップＳ１２０７）、証明書生成要求受付手段１２に出力する。証明書生成要求受付手段１２は、新規作成された証明書を証明書生成要求トークン管理手段１３に送付する。

【０１００】

以降のステップＳ１２０８～Ｓ１２１０の処理は、図１１のステップＳ１１０５～Ｓ１１０７の処理内容とほぼ同様である。証明書生成要求トークン管理手段１３は、サービス提供装置３以外のサービス提供装置が証明書生成要求を行うための証明書生成要求トークンを、乱数を発生させることによって生成し（ステップＳ１２０８）、証明書生成要求トークンを受け取った証明書と関連付けて管理する（ステップＳ１２０９）。そして、証明書生成要求トークン生成手段１３は、生成した証明書生成要求トークンを、証明書生成要求受付手段１２に送付する。

【０１０１】

証明書生成要求受付手段１２は、証明書生成要求トークン管理手段１３から受け取った証明書生成要求トークンと、ステップＳ１２０８において取得した証明書とを添付した、証明書配布要求に対する返信メッセージを作成して（ステップＳ１２１０）、サービス提供装置３に対して返信する（ステップＳ１２１１）。

【０１０２】

なお、上記の説明では、サービス提供装置３がサービス仲介装置として動作し他のサービス提供装置を仲介する場合をも考慮して説明したが、サービス提供装置３がサービス仲介装置として動作しない場合には、サービス提供装置２は、ステップＳ１２０８～Ｓ１２０９の処理を実行しない。そして、サービス提供装置２は、ステップＳ１０において、証明書のみを添付した証明書配布要求に対する返信メッセージを作成する。

【０１０３】

次に、図１３～図１６を参照して、サービス仲介装置２またはサービス提供装置３の動作について説明する。

【０１０４】

サービス提供装置３が、サービスのアクセス要求を受ける場合の動作に関して、図１３を参照して説明する。図１３は、サービス提供装置３が、サービスのアクセス要求を受ける場合の処理の例を示す流れ図である。

【０１０５】

サービス提供装置３は、利用者（端末装置４）やサービス仲介装置２から送付される所定の要求メッセージを受信可能な状態にある。また、サービス提供装置３は、認証装置１に対して所定の要求メッセージを送信可能な状態にある。

【０１０６】

サービス提供装置３は、アクセス要求を受信した場合、そのメッセージを解析した上で、その要求内容に応じた動作処理を行う。また、サービス提供装置３は、所定のイベントをきっかけとして、要求メッセージを作成するなどの動作処理を行う。以下、本発明における特徴的な動作である、サービス提供装置３が代理アクセスを受け付ける処理について説明する。

【０１０７】

サービス提供装置３が、利用者（端末装置４）またはサービス仲介装置２から、サービ

ス提供装置３の公開するサービスに対するアクセス要求を受信する場合の動作に関して、図１３を参照して説明する。

【０１０８】

サービス提供装置３は、所定のサービスを公開している。サービス提供装置３のサービス管理部７におけるサービスアクセス受付手段７０は、利用者（端末装置４）またはサービス仲介装置２からの公開サービスへのアクセス要求を受信すると（ステップＳ１３０１）、アクセス要求に関する利用者の認証が必要か否かを確認する（ステップＳ１３０２）。公開サービスに関して認証が不要であるか、または、アクセス要求に、セッション識別子や証明書が含まれているなどして、利用者を認証可能で、新たに認証処理が不要である場合（Ｎｏ）、サービス情報管理手段７１が公開サービスを提供する旨の返信メッセージを作成し（ステップＳ１３０９）、サービスアクセス受付手段７０は、アクセス要求の要求者に対して返信する（ステップＳ１３１０）。

【０１０９】

一方、アクセス要求に関する利用者の認証が必要である場合（Ｙｅｓ）、サービスアクセス受付手段７０は、アクセス要求を解析して証明書生成要求トークンを取得（抽出）し、認証装置を特定する（ステップＳ１３０３）。

【０１１０】

次に、サービスアクセス受付手段７０は、サービス情報管理手段７１から、サービスアクセスを受け付けるために必要とする証明書の種類を取得し（ステップＳ１３０４）、証明書生成要求トークンと共に、証明書生成要求手段８０に送付する。後述するステップＳ１６０１からステップＳ１６１１の処理で、証明書生成要求手段８０は、証明書生成要求トークンを発行した認証装置１から、要求する証明書を受信し、サービスアクセス受付手段７０に送付する。また、証明書検証手段６２は、受信した証明書を検証する（ステップＳ１３０５）。

【０１１１】

次に、サービスアクセス受付手段７０は、証明書の検証結果の内容を確認する（ステップＳ１３０６）。証明書の検証結果が正で、適切な証明書ならば（Ｙｅｓ）、証明書の記載内容、あるいは、サービス情報管理手段７１で管理する利用者に関する情報を、アクセス制御ポリシ格納部７２に格納するセキュリティポリシと照合する（ステップＳ１３０７）。

【０１１２】

照合の結果を確認し（ステップＳ１３０８）、サービスアクセスを許可する場合は（Ｙｅｓ）、サービス情報管理手段７１は、サービスを提供する返信メッセージを作成する（ステップＳ１３０９）。一方、照合の結果、サービスアクセスを許可しない場合（Ｎｏ）、サービス情報管理手段７１は、サービスアクセスを受け付けないという旨のエラーメッセージを作成し（ステップＳ１３１１）、サービスアクセス受付手段７０は、アクセス要求の要求者に対して返信する（ステップＳ１３１０）。

【０１１３】

一方、ステップＳ１３０６において、証明書の検証結果が不正ならば（Ｎｏ）、サービス情報管理手段７１は、サービスアクセスを受け付けないという旨のエラーメッセージを作成し（ステップＳ１３１１）、サービスアクセス受付手段７０は、アクセス要求の要求者に対して返信する（ステップＳ１３１０）。

【０１１４】

次に、サービス仲介装置２が、サービス提供装置３に対して、サービスのアクセスを仲介する場合の動作に関して、図１４を参照して説明する。図１４は、サービス仲介装置２がサービス提供装置３へのアクセスを仲介する処理の例を示す流れ図である。

【０１１５】

サービス仲介装置２のサービスアクセス仲介手段５０は、サービス提供装置３が提供するサービスへの、利用者（端末装置４）からのサービスアクセス要求を受ける（ステップＳ１４０１）。

【０１１６】
その後、サービス仲介装置２は、認証装置1に対する証明書生成要求トークンを要求するメッセージを作成し、認証装置１へ送付する（ステップＳ１４０２）。
【０１１７】
次に、サービス仲介装置２は、認証装置１が図１１に示す動作で作成したサービスアクセス要求の利用者に関する証明書生成要求トークンが添付された返信メッセージを、認証装置１から受け取る（ステップＳ１４０３）。
【０１１８】
次に、証明書生成要求トークン取得手段６１は、証明書配布要求に対する返信メッセージから証明書生成要求トークンを抽出する（ステップＳ１４０４）。そして、サービスアクセス仲介手段５０は、サービス提供装置３が公開するサービスに対するサービスアクセス要求メッセージを所定のプロトコルを利用して作成し（ステップＳ１４０５）、証明書生成要求トークンを添付して（ステップＳ１４０６）、サービス提供装置３に送付する（ステップＳ１４０７）。
【０１１９】
次に、サービスアクセス仲介手段５０は、サービス提供装置３からの返信メッセージを受け取り（ステップＳ１４０８）、返信メッセージの内容を基にして、サービス提供装置３へのサービス仲介結果内容を、端末装置４に送付する（ステップＳ１４０９）。
【０１２０】
サービス仲介装置２が、認証装置１からの証明書の配布を受ける場合の動作に関して、図１５を参照して説明する。図１５は、サービス仲介装置２が認証装置１から証明書を受信する場合の処理の例を示す流れ図である。
【０１２１】
サービス仲介装置２の証明書配布要求手段５１は、所定の通信プロトコルを用いて、証明書配布要求メッセージを作成する（ステップＳ１５０１）。この際、証明書配布要求メッセージには、所定のプロトコルに応じた、配布要求する証明書を識別可能な情報を格納する。そして、証明書配布要求手段５１は、所定の認証装置１の証明書配布要求受付手段１５に対して、証明書配布要求メッセージを送付する（ステップＳ１５０２）。
【０１２２】
次に、証明書配布要求手段５１は、通信待ちの状態の後、認証装置１の証明書配布要求受付手段１５から、証明書配布要求に対する返信メッセージを受信する（ステップＳ１５０３）。
【０１２３】
次に、証明書配布要求手段５１は、返信メッセージを解析し（ステップＳ１５０４）、証明書を抽出して（ステップＳ１５０５）、証明書検証手段６２に送付する。証明書検証手段６２は、証明書を検証して、その内容に改ざんがなく、認証装置１が記載したものであるか否かを確認する（ステップＳ１５０６）。証明書が不正なものであると確認した場合（Ｎｏ）、直ちに処理を終了する。
【０１２４】
一方、証明書が適切なものであることが確認できた場合（Ｙｅｓ）、証明書配布要求手段５１は、返信メッセージを解析し、証明書生成要求トークンが含まれているか否かを調べる（ステップＳ１５０７）。
【０１２５】
ステップＳ１５０７において、証明書配布要求手段５１が、証明書生成要求トークンが含まれていると判断した場合（Ｙｅｓ）、証明書配布要求手段５１は、証明書生成要求トークンを証明書生成要求トークン取得手段６１に送付する。また、証明書生成要求トークン取得手段６１は、証明書生成要求トークンを解析し、（ステップＳ１５０８）、証明書検証手段６２は、証明書を証明書情報格納部６５において保管する（ステップＳ１５０９）。
【０１２６】

一方、ステップＳ１５０７において、証明書配布要求手段５１が、返信メッセージに証明書生成要求トークンが含まれていないと判断した場合（Ｎｏ）、証明書検証手段６２は、証明書を証明書情報格納部６５において保管し（ステップＳ１５０９）、処理を終了する。

【０１２７】

次に、サービス提供装置３が、認証装置１に対して証明書の生成を要求した上で、要求した証明書の配布を受ける場合の動作に関して、図１６を参照して説明する。図１６は、サービス提供装置３が認証装置１に証明書を要求して受信する場合の処理の例を示す流れ図である。

【０１２８】

サービス提供装置３のサービス管理部７におけるサービスアクセス受付手段７０は、サービス仲介装置２のサービスアクセス仲介手段５０が送付するサービスアクセス要求とともに、証明書生成要求トークンを受信する（ステップＳ１６０１）。

【０１２９】

その後、サービス提供装置３のサービス提供装置用証明書管理部６６における証明書生成要求トークン解析手段６６１は、証明書生成要求トークンを解析する（ステップＳ１６０２）。証明書生成要求トークン解析手段６６１は、解析の結果、証明書生成要求トークンに含まれる、それを発行した認証装置１の識別子情報を取得し、認証装置情報管理手段６０に送付する。

【０１３０】

認証装置情報管理手段６０は、認証装置１の識別子情報から、認証装置１のネットワーク上のアドレスなどの詳細情報を取得し（ステップＳ１６０３）、証明書生成要求手段８０に送付する。

【０１３１】

証明書生成要求手段８０は、認証装置１に関する詳細情報から、所定の通信プロトコルを用いて、認証装置１に対する、サービス提供装置３用の証明書生成要求メッセージを作成し（ステップＳ１６０４）、証明書生成要求トークンを添付し（ステップＳ１６０５）、認証装置１の証明書生成要求受付手段１２に対して送付する（ステップＳ１６０６）。

【０１３２】

その後、証明書生成要求手段８０は、通信待ちの状態に移行後、認証装置１の証明書生成要求受付手段１２からの返信メッセージを受信し（ステップＳ１６０７）、ステップＳ１５０６～Ｓ１５０９の処理と同様に、返信メッセージに含まれる証明書を検証し、格納する（ステップＳ１６０８～Ｓ１６１１）。

【０１３３】

上記の第１の実施形態の動作では、代理アクセス先装置（サービス提供装置３）向けの証明書の発行のタイミングは、認証装置１が証明書生成要求メッセージを受信したときになっていたが、認証装置１がサービス提供装置３向けに証明書生成要求トークンを発行した際に、サービス提供装置３向けの証明書を発行してもよい。その場合は、証明書生成要求トークンを生成した際に、証明書を生成し、証明書情報格納部２４に登録する。さらに、認証装置１が、サービス提供装置３が送信する証明書生成要求メッセージを受信したときには、証明書生成要求受付手段１２は、証明書管理手段１６を用いて、証明書情報格納部２４を検索し、証明書を取得して、サービス提供装置３へ応答する。なお、例えば、サービス提供装置３向けの証明書とは、サービス提供装置３において有効な証明書を意味する。

【０１３４】

第１の実施形態では、利用者に関する証明書の生成と配信が、端末装置を経由せずに、認証装置とサービス提供装置間の直接の通信によって行われる。そのため、端末装置を介したリダイレクトの回数が減り、通信回数が少なくなることから、通信を効率化することができる。

【０１３５】

例えば、仮に、第１のＳＰにユーザエージェントの機能を追加することによって、非特許文献１に記載されている技術を利用してユーザエージェントを介さずに第２のＳＰへの代理アクセスを実現しようとしても、通信が非効率になる。

【０１３６】

非特許文献１に記載されている証明書生成配布システムを適用して、ＩｄＰ１００で認証を受け、第１のＳＰのサービスにアクセスしている利用者に関して、第１のＳＰが、第１のＳＰとは異なる第２のＳＰに利用者の代理アクセスを試みる場合について説明する。この場合、第２のＳＰは、ＩｄＰ１００からの利用者に関する証明書の配布を必要とする。

【０１３７】

仮に、第１のＳＰにユーザエージェントの機能を追加することによって、非特許文献１に記載されている技術を利用してユーザエージェントを介さずに第２のＳＰへの代理アクセスを実現する場合について説明する。図２を参照して、ユーザエージェントを介さずに代理アクセスを実現する処理の流れの例を説明する。

【０１３８】

図２は、非特許文献１に記載されている証明書生成配布システムを適用して代理アクセス処理を行う場合の例を説明するための説明図である。図２に示す証明書生成配布システムは、図１に示すＳＰ１０１に代えて、ＳＰ１２１（第１のＳＰ）が設けられている。また、図２に示す証明書生成配布システムは、図１に示すシステムには設けられていないＳＰ１２２（第２のＳＰ）が設けられている。図２には、最初に利用者がＳＰ１２１にアクセスし、次にＳＰ１２１がユーザの代わりにＳＰ１２２にアクセスする例を示す。

【０１３９】

図２に示す証明書生成配布システムは、利用者がＳＰ１２１にアクセスするまで（ステップＳ１からステップＳ７まで）は、図１に示す関連技術と同じ処理を実行する。ステップＳ８以降の処理は、図１に示す処理においてユーザエージェント１０２がＳＰ１０１にアクセスしてＳＰ１０１がサービスを提供する処理の代わりに、ＳＰ１２１がサービス（ＳＰ１２２）にアクセスしてＳＰ１２２がサービスを提供する処理になる。

【０１４０】

まず、ＳＰ１２１が利用者の認証アサーションを取得すると、ＳＰ１２１は、ユーザエージェントとしてＳＰ１２２に代理アクセスする（ステップＳ８）。ＳＰ１２２は、アクセスしてきたエンティティを認証するために、ＩｄＰ１００に対して認証要求メッセージを送付し（ステップＳ９－ａ）、ＳＰ１２１は、ＳＰ１２２からの認証要求メッセージをＩｄＰ１００にリダイレクトする（ステップＳ９－ｂ）。

【０１４１】

ＩｄＰ１００は、先にステップＳ１において利用者を認証していることを確認し、利用者を認証済みであることを証明するＸＭＬ記述の認証証明書（認証アサーション）を作成する（ステップＳ１０）。この認証証明書は、ＳＰ１２２向けに発行されるものであり、ステップＳ４で作成されたＳＰ１２１向けの認証証明書とは異なる。

【０１４２】

さらに、ＩｄＰ１００は、作成した認証アサーションに対応するチケットの役割を担うアーティファクトを作成し、ＳＰ１２１に返信する（ステップＳ１１－ａ）。ＳＰ１２１は、受信したアーティファクトをＳＰ１２２に対してリダイレクトする（ステップＳ１１－ｂ）。ＳＰ１２２は、アーティファクトを受信し、受信したアーティファクトをＩｄＰ１００に送付して、対応する認証アサーションを要求する（ステップＳ１２）。

【０１４３】

ＩｄＰ１００は、ＳＰ１２２から受け取ったアーティファクトを確認し、対応する認証アサーションをＳＰ１２２に対して返信する（ステップＳ１３）。ＳＰ１２２は、ＩｄＰ１００から受信した認証アサーションの正当性を確認し、利用者のサービスへのアクセス要求に対して許可を与えるか否かをＳＰ１２２のセキュリティポリシを用いて検証し、許可を与える場合にはＳＰ１２１にサービスの提供を開始する（ステップＳ１４）。これに

より、ＳＰ１２１の代理アクセスが完了し、最終的にＳＰ１２１がユーザエージェントにサービスを提供する（ステップＳ１５）。

【０１４４】

以上に説明したように、仮に、第１のＳＰにユーザエージェントの機能を追加することによって、非特許文献１に記載されている技術を利用してユーザエージェントを介さずに第２のＳＰへの代理アクセスを実現しようとしても、第１のＳＰが既に行った認証処理（ステップＳ３－ａ～Ｓ７）と同じ認証処理（ステップＳ９－ａ～Ｓ１３）を、第２のＳＰが第１のＳＰを介して行う必要がある。そのため、処理が複雑になり、通信が非効率になる。これに対して、本実施形態によれば、利用者に関する証明書の生成と配信が、認証装置とサービス提供装置間の直接の通信によって行われるので、端末装置を介したリダイレクトの回数が減り、通信回数が少なくなることから、通信を効率化することができる。

【０１４５】

また、第１の実施形態では、サービス仲介装置にユーザエージェントの機能を追加してサービス提供装置への代理アクセスを実現する場合と比較しても、サービス仲介装置を介したリダイレクトの回数が減り、通信回数が少なくなることから、通信を効率化することができる。

【０１４６】

また、サービス仲介装置とサービス提供装置間では、証明書自体ではなく、証明書よりも少ない情報量の証明書生成要求トークンを交換する。このため、証明書の配信に伴う通信回数と通信量が削減し、効率性が向上する。

【０１４７】

また、第１の実施形態では、証明書生成要求トークンを受け取ったサービス提供装置は、証明書生成要求トークンを利用して、証明書生成要求を認証装置に対して行い、認証装置は、証明書生成要求を受けた時点で証明書を生成する。このため、認証装置は、利用されるか否かわからない証明書を事前に生成して管理したり、不要な証明書を生成したりする必要がなく、証明書生成に伴う処理コストや管理コストを低減できる。

【０１４８】

また、第１の実施形態では、サービス仲介装置とサービス提供装置間で、利用者に関する証明書の生成要求を行うための証明書生成要求トークンを交換する。証明書生成要求トークン自体には、利用者を特定するに足る情報は含まれていない。このため、証明書生成及び配布に伴う処理動作における機密情報の漏洩を防止し、プライバシを保護することができる。

【０１４９】

（第２の実施形態）

次に、本発明の第２の実施形態について図面を参照して説明する。

【０１５０】

図１７は、第２の実施形態におけるサービス仲介装置３０の構成の一例を示すブロック図である。図１７に示すように、第２の実施形態は、サービス仲介装置３０が、図６に示す第１の実施形態におけるサービス仲介装置２の構成に加えて、サービス管理部７と、証明書生成要求手段８０と、サービス提供装置用証明書管理部６６とを有する点で、第１の実施形態と異なる。なお、第１の実施形態におけるサービス仲介装置２と同様の構成部については、図６と同一の符号を付し、説明を省略する。

【０１５１】

第２の実施形態の証明書生成配布システムの好ましい一態様は、例えば、図４に示す認証装置１と、サービス仲介装置２と、サービス提供装置３と、端末装置４とを備える。認証装置１、サービス仲介装置２、サービス提供装置３および端末装置４は、相互にネットワーク５で接続されている。

【０１５２】

第２の実施形態の証明書生成配布システムの認証装置１は、図５に示すように、利用者情報管理手段１１が利用者情報格納部２０で管理する利用者情報を参照し、所定の認証方

式を用いて、利用者の認証を行う利用者認証手段１０を備え、他のサービス提供装置からの証明書生成要求を受け付け、証明書生成要求に含まれた要求する証明書の種類と証明書生成要求トークンに応じて、アクセス制御ポリシ格納部２１で管理されるセキュリティポリシを参照しつつ、証明書要求を許可するか否かの認可判断を行ったうえで、要求された証明書を、証明書生成手段１４を通じて生成し、配布する証明書生成要求受付手段１２と、他のサービス提供装置から、既に生成された証明書配布要求を受け付け、証明書配布要求を基にして、証明書管理手段１６を通じて、配布要求された証明書を取得し配布する証明書配布要求受付手段１５と、他のサービス提供装置からの証明書生成要求を受け付けるために、生成要求される証明書と関連付けた識別子である証明書生成要求トークンを発行し、証明書生成要求トークン格納部２２において、証明書生成要求トークンを管理する証明書生成要求トークン管理手段１３と、他のサービス提供装置からの、証明書生成要求に含まれる証明書生成トークンに関連付けた利用者に関連し、装置情報格納部２３に格納するサービス提供装置情報を基にして生成要求された証明書を生成し、証明書情報格納部２４において管理する証明書生成手段１４と証明書生成手段が生成した証明書を、その証明書の識別子と関連付けて、証明書情報格納部において管理する証明書管理手段１６とを備える。

【０１５３】

第２の実施形態の証明書生成配布システムのサービス仲介装置３０は、図１０および図１７に示すように、サービス管理部７のサービス情報格納部７３において格納され、サービス情報管理手段７１が管理するサービス情報を用いて所定のサービスを公開し、サービスへの利用者からのアクセス要求に対して、アクセス制御ポリシ格納部７２で管理するセキュリティポリシを参照の上、所定の利用者に対してのみアクセスを許可するサービスアクセス受付手段７０と、利用者、あるいは、該サービス仲介装置とは異なるサービス仲介装置からのサービスアクセス要求からの、サービスアクセス要求（第１のサービスアクセス要求）を受けた後、該サービスアクセス要求を行った利用者に関連して、サービスアクセス要求とは異なるサービスアクセス要求（第２のサービスアクセス要求）を、所定の通信プロトコルを用いて、証明書生成要求トークンを含めたうえで、サービス提供装置に対して行うサービスアクセス仲介手段５０と、証明書の検証、証明書生成要求トークンの解析、認証装置情報の管理機能を備えた証明書管理部６とを備える。

【０１５４】

第２の実施形態の証明書生成配布システムのサービス提供装置３は、図８、図９および図１０に示すように、サービス管理部７のサービス情報格納部７３において格納され、サービス情報管理手段７１が管理するサービス情報を用いて所定のサービスを公開し、サービスへの利用者からのアクセス要求に対して、アクセス制御ポリシ格納部７２で管理するセキュリティポリシを参照の上、所定の利用者に対してのみアクセスを許可するサービスアクセス受付手段７０と、サービス提供装置用証明書管理部６６で管理される証明書生成要求トークンと認証装置情報を基にして、認証装置に対して、証明書生成要求を行うためのメッセージを、証明書生成要求トークンを添付した上で作成し、送付する証明書生成要求手段８０とを備える。

【０１５５】

第２の実施形態の証明書管理部６は、図７に示すように、ランダムな変数を生成して、該変数を証明書生成要求トークンとして、証明書と関連付けて管理する証明書生成要求トークン取得手段６１と、認証装置識別子情報と認証装置情報の詳細情報とを関連付けて、認証装置情報格納部６３において管理する認証装置情報管理手段６０と、認証装置に対して、所定の通信プロトコルを用いて、既に生成されている証明書の配布要求を、認証装置情報管理手段の関する認証装置情報を基にして送付し、認証装置から配布を受けた証明書を検証し、証明書が適切であった場合に、証明書情報格納部６５において格納し、管理する証明書検証手段６２とを備える。

【０１５６】

上記のような構成を採用し、サービス仲介装置とサービス提供装置の間で、証明書生成

要求トークンを交換し、また、証明書生成要求トークンを受け取ったサービス提供装置が、証明書生成要求トークンを利用して、認証装置向けに動的に該証明書生成要求トークンを以って、サービス提供装置に対する新たな証明書を要求し、認証装置が証明書を動的に作成し、サービス提供装置に対して配布することによって、本発明の目的を達成することができる。

【０１５７】

次に、図１８を参照して、第２の実施形態の動作について説明する。図１８は、サービス仲介装置３０が、サービス要求を仲介し、さらに他の装置や利用者に対してサービスを提供する場合の処理の例を示す流れ図である。図１８に示す例では、図１３のステップＳ１３０３の代わりにステップＳ１３１２の処理が行われ、さらにステップＳ１３１３，Ｓ１３１４およびＳ１３１５の処理が追加されている。なお、図１８におけるステップＳ１３０１，Ｓ１３０２，Ｓ１３０４～Ｓ１３１０の処理は、実施形態１における処理（図１３を参照）と同様であるため、説明を省略する。

【０１５８】

ステップＳ１３１２で、証明書配布要求手段５１は、サービス仲介装置３０へのサービスアクセス要求メッセージに証明書生成要求トークンが含まれているか否か判断する。含まれていると判断した場合は（Ｙｅｓ）、第１の実施形態のサービス提供装置３と同じ処理（ステップＳ１３０４，Ｓ１３０５）を行い、ステップＳ１３１５に移行する。

【０１５９】

ステップＳ１３１２で、証明書生成要求トークンが含まれていないと判断した場合（Ｎｏ）、サービス仲介装置３０は、認証装置１に対して認証要求メッセージを送付する（ステップＳ１３１３）。そして、図１５に示すサービス仲介装置２の処理（ステップＳ１５０１～Ｓ１５０９）と同じ処理を行い、証明書を取得する（ステップＳ１３１４）。

【０１６０】

証明書を取得した後、さらにサービス管理部７が代理アクセスを実行するか否かを判断して、必要に応じて代理アクセスを実行する（ステップＳ１３１５）。その後、ステップＳ１３０６～Ｓ１３１０の処理を実行する。

【０１６１】

第２の実施形態では、サービス提供装置（サービス仲介装置）が、さらに別のサービス提供装置に対して代理アクセスできるようになる。これにより、サービスへの代理アクセスを何度も繰り返し実行できるため、サービス提供装置や認証装置間の通信量を削減することができる。

【０１６２】

（第３の実施形態）

次に、本発明の第３の実施形態について図面を参照して説明する。

【０１６３】

図１９は、第３の実施形態における認証装置８の構成の一例を示すブロック図である。図１９に示すように、第３の実施形態では、認証装置８が、図５に示す第１の実施形態における認証装置１の構成に加えて、証明書配布範囲制限手段８５を有する。

【０１６４】

図２０は、第３の実施形態におけるサービス仲介装置９の構成の一例を示すブロック図である。図２０に示すように、第３の実施形態では、サービス仲介装置９が、図６に示す第１の実施形態におけるサービス仲介装置２の構成に加え、サービス管理部７と、証明書配布範囲指定手段８６とを有する点で異なる。なお、サービス管理部７の構成は、実施形態２（図１７を参照）における構成と同様であるため、説明を省略する。

【０１６５】

図２０に示すサービス仲介装置９における証明書配布範囲指定手段８６は、証明書配布要求手段５１が認証装置８に対して送信する証明書配布要求メッセージに、証明書の配布範囲を指定するための情報を追加する。証明書の配布範囲を指定するための情報とは、例えば、認証装置８から返信されるべき証明書生成要求トークンを配布して有効とするサー

ビス提供装置３のリストである。

【０１６６】

第３の実施形態において、証明書配布要求受付手段１５は、サービス仲介装置９から証明書配布要求メッセージを受信する。証明書配布要求メッセージは、新規に証明書を生成して配布可能なサービス提供装置３のリスト情報を含む。

【０１６７】

図１９に示す認証装置８における証明書配布範囲制限手段８５は、証明書配布要求メッセージにおいて指定されたサービス提供装置３のリスト情報を基に、サービス提供装置３のリストに対して証明書作成配布することに問題ないか否かを判断する。証明書配布範囲制限手段８５は、問題ないと判断した場合において、新たに生成する証明書生成トークンを以って、その後、サービス提供装置３から証明書生成要求を受けた際に、サービス提供装置３のリストに含まれるサービス提供装置３に対してのみ証明書生成を受け付けるようにする。具体的には、証明書配布要求受付手段１５が証明書配布要求を受けた際に、証明書配布範囲制限手段８５は、リストに含まれるサービス提供装置３に対して証明書生成要求を許可する旨のポリシを生成し、アクセス制御ポリシ格納部２１に追加する。

【０１６８】

次に、第３の実施形態の動作について説明する。

【０１６９】

図２１を参照し、サービス仲介装置９が、認証装置８に対して証明書配布要求を行う場合の処理を説明する。図２１は、サービス仲介装置９が、認証装置８に対して証明書配布要求を行う場合の処理の例を示す流れ図である。図２１に示す例では、図１５のステップＳ１５０１とステップＳ１５０２との間に、ステップＳ１５１０の処理が追加されている。なお、図２１におけるステップＳ１５０１，Ｓ１５０２～Ｓ１５０９の処理は、実施形態１における処理（図１５を参照）と同様であるため、説明を省略する。

【０１７０】

ステップＳ１５１０において、証明書配布範囲指定手段８６は、ステップＳ１５０１で証明書配布要求手段５１が作成した証明書配布要求メッセージに対して、証明書を配布してもよいとみなすサービス要求装置３のリスト情報を追加する。

【０１７１】

次に、図２２を参照し、認証装置８が、サービス仲介装置９からの証明書配布要求を受け取った場合の処理を説明する。図２２は、認証装置８がサービス仲介装置９からの証明書配布要求を受信する場合の処理の例を示す流れ図である。

【０１７２】

図２２に示す例では、図８のステップＳ１１０６とステップＳ１１０７との間に、ステップＳ１１１０の処理が追加されている。なお、図２２におけるステップＳ１１０１～Ｓ１１０６，Ｓ１１０７～Ｓ１１０９の処理は、実施形態１における処理（図１１を参照）と同様であるため、説明を省略する。

【０１７３】

ステップＳ１１１０において、証明書配布範囲制限手段８５は、ステップＳ１１０１で受け取った証明書配布要求メッセージに含まれるリスト情報を抽出する。リスト情報は、サービス仲介装置９が指定する、新規に生成する証明書を配布可能なサービス提供装置３を示す情報である。

【０１７４】

証明書配布範囲制限手段８５は、抽出したリストに含まれるサービス提供装置３に対して、新規に証明を生成し、配布してよいか否かを確認の上、生成・配布してよい場合には、証明書生成要求を許可するポリシを生成し、アクセス制御ポリシ格納部２１に登録する。証明書配布範囲制限手段８５が生成するポリシは、サービス提供装置３からステップＳ１１０５で生成した証明書生成要求トークンに関連する証明書生成要求を受けた場合に、証明書生成要求を許可する旨のポリシである。

【０１７５】

第３の実施形態では、証明書生成要求トークンが有効となる範囲を、サービス仲介装置が指定する。例えば、証明書を送信するサービス提供装置をサービス仲介装置が指定することができる。それに伴って、認証装置は、証明書配布を限定的にすることができる。これにより、証明書情報の漏洩の防止を強化することができる。

【０１７６】

（第４の実施形態）

次に、本発明の第４の実施形態について図面を参照して説明する。

【０１７７】

図２３は、第４の実施形態におけるサービス仲介装置４０の構成の一例を示すブロック図である。図２３に示すように、第４の実施形態は、サービス仲介装置４０が、図６に示す第１の実施形態におけるサービス仲介装置２の構成に加えて、証明書生成要求トークン発行手段４１を有する点で、第１の実施形態と異なる。なお、第１の実施形態におけるサービス仲介装置２と同様の構成部については、図６と同一の符号を付し、説明を省略する。

【０１７８】

図２３に示すサービス仲介装置４０における証明書生成要求トークン発行手段４１は、認証装置１が証明書を発行するためのトークンを生成する。サービス仲介装置４０が発行するトークンは、第１の実施形態における認証装置１が発行するトークンと同じ構造である。

【０１７９】

次に、図２４を参照し、第４の実施形態の動作について説明する。図２４は、サービス仲介装置４０が、認証装置１に対して証明書配布要求を行う場合の処理の例を示す流れ図である。図２４に示す例では、図１４のステップＳ１４０１とステップＳ１４０２との間に、ステップＳ１４１０の処理が追加されている。なお、図２４におけるステップＳ１４０１，Ｓ１４０２～Ｓ１４０９の処理は、実施形態１における処理（図１４を参照）と同様であるため、説明を省略する。

【０１８０】

ステップＳ１４１０において、サービス仲介装置４０は、証明書生成要求トークンを発行する。次に、ステップＳ１４０２において、サービス仲介装置４０は、証明書生成要求トークンを要求するメッセージを作成するときに、作成メッセージ中に証明書生成要求トークンを含める。これ以降の処理は、第１の実施形態における動作と同じである。

【０１８１】

次に、図２５を参照し、認証装置１が、サービス仲介装置４０からの証明書配布要求を受け取った場合の処理を説明する。図２５は、認証装置１がサービス仲介装置４０からの証明書配布要求を受信する場合の処理の例を示す流れ図である。

【０１８２】

図２５に示す例では、図１１のステップＳ１１０４とステップＳ１１０６の間にある証明書生成要求トークンの作成処理（ステップＳ１１０５）が削除されている。認証装置１は、自身で証明書生成要求トークンを発行するのではなく、サービス仲介装置４０が送信した証明書生成要求トークンを利用する。証明書生成要求トークンと証明書の関連付け処理（ステップＳ１１０６）以降の処理は、第１の実施形態における動作と同じである。

【０１８３】

第４の実施形態では、証明書生成要求トークン発行機能を、認証装置１からサービス仲介装置４０へと移行できる。これにより、認証装置１のメッセージ処理の負荷を軽減することができる。

【実施例１】

【０１８４】

次に、本発明の第１の実施例を、図面を参照して説明する。かかる実施例は本発明の第２の実施形態に対応するものである。

【０１８５】

図２６は、本発明による証明書生成配布システムの第１の実施例を説明するための説明図である。図２６に示す証明書生成配布システムは、認証装置２００と、サービス仲介装置２０１と、サービス提供装置２０２と、端末装置２０３とを備える。認証装置２００、サービス仲介装置２０１、サービス提供装置２０２および端末装置２０３は、それぞれ第２の実施形態で示した機能を備える。

【０１８６】

第１の実施例において、認証装置２００は、インターネット上で、認証サービスを所定の利用者に対して公開する。サービス仲介装置２０１は、旅行ポータルサイトとしてのサービスを所定の利用者に公開している。サービス提供装置２０２は、レンタカー予約サイトとしてのサービスを所定の利用者に対して公開する。端末装置２０３は、汎用的なＷｅｂブラウザの機能を持ち、利用者によって操作される。認証装置２００、サービス仲介装置２０１、サービス提供装置２０２および端末装置２０３は、それぞれインターネット等の通信ネットワークに接続されている。

【０１８７】

サービス仲介装置２０１は、パッケージ旅行を利用者に代わって一括予約が可能なサイトを実現する装置である。サービス仲介装置２０１は、利用者からの旅行予約要求に応じて、提携しているレンタカー予約サイトを実現する装置であるサービス提供装置２０２にアクセスし、必要に応じて、利用者の代理として利用者のレンタカー予約を行う。

【０１８８】

認証装置２００と、サービス仲介装置２０１と、サービス提供装置２０２と、端末装置２０３とは、例えば、いずれもＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｐｏｒｔ　Ｐｒｏｔｏｃｏｌ）の規定する通信プロトコルで互いに通信する機能を備える。

【０１８９】

利用者Ａｌｉｃｅは、事前に認証装置２００を管理する通信事業者に加入しており、アカウントを保有している（アカウント名は、Alice200）。また、Ａｌｉｃｅは、旅行ポータルサイトとレンタカー予約サイトにも加入しており、やはり、それぞれ、アカウントを保有している（アカウント名は、aabbcc、xxyyzz）。旅行ポータルサイトとレンタカー予約サイトにおける両アカウントは、通信事業者のアカウントと、それぞれ、関連付けられて管理されている。

【０１９０】

図２７は、認証装置２００の利用者情報管理手段１１が管理するアカウント対応管理表の登録例を示す説明図である。図２７には、Ａｌｉｃｅに関する装置毎のアカウント名（仮名）の対応管理表の一例を示す。図２７に示す例では、それぞれの装置において管理されるＡｌｉｃｅのアカウント名（仮名）が、装置名に関連付けられて管理されている。

【０１９１】

当初、Ａｌｉｃｅは、認証装置２００に認証されておらず、認証装置２００、サービス仲介装置２０１およびサービス提供装置２０２のいずれにも、Ａｌｉｃｅに関するセッションは確立していない。

【０１９２】

図２８は、第１の実施例における証明書生成配布システムの動作の例を示すシーケンス図である。以下、図２６および図２８を参照して、第１の実施例における証明書生成配布システムの動作について説明する。

【０１９３】

Ａｌｉｃｅは、端末装置２０３を利用して、通信事業者の認証装置２００にアクセスし、認証を受ける（ステップＳ３００）。Ａｌｉｃｅの認証後、認証装置２００は、Ａｌｉｃｅに対するセッションを確立し、Ａｌｉｃｅの端末装置２０３に対して、セッションの識別子に相当する情報（例えば、セッションクッキー）を送付し、端末装置２０３は、セッション識別子情報を受け取る。

【０１９４】

次に、Ａｌｉｃｅは、旅行ポータルサイトのサービス仲介装置２０１に対して、旅行予

約のサービスアクセス要求を送付する（ステップＳ３０１）。サービス仲介装置２０１は、端末装置２０３からのサービスアクセス要求を受けて、認証装置２００に対して利用者の認証を依頼する認証要求メッセージを送付する（ステップＳ３０２）。認証要求に関しては、例えば、非特許文献１記載のＳＡＭＬのアーティファクトプロファイルによる方法を取る。認証要求メッセージは、Ａｌｉｃｅの端末装置２０３を経由して、認証装置２００に送付される。

【０１９５】

認証要求を受け取った認証装置２００は、Ａｌｉｃｅが既に認証済みであることをセッションの存在から確認し、Ａｌｉｃｅに関して、認証が完了している旨を表す認証証明書と、認証証明書に対応するアーティファクトとを生成する（ステップＳ３０３）。そして、認証装置２００は、アーティファクトをサービス仲介装置２０１に対して、端末装置２０３を経由して返信する（ステップＳ３０４）。

【０１９６】

図２９は、認証証明書の記載内容の一例を示す説明図である。図２９に例示する認証証明書は、サービス仲介装置２０１において利用されるＡｌｉｃｅに関する仮名（aabbcc）を含む。また、証明書を配布する有効範囲を、サービス仲介装置２０１だけに規定している。

【０１９７】

アーティファクトを受け取ったサービス仲介装置２０１は、アーティファクトを添付した証明書配布要求メッセージを作成し、認証装置２００に送付する（ステップＳ３０５）。

【０１９８】

証明書配布要求を受け取った認証装置２００は、アーティファクトに基づいて、Ａｌｉｃｅに関する認証証明書を取得（抽出）する。認証装置２００は、サービス提供装置２０２向け認証証明書と証明書生成要求トークンとを作成し、認証証明書と証明書生成要求トークンとを関連付けて管理する（ステップＳ３０６）。次に、認証装置２００は、認証証明書と証明書生成要求トークンとを添付して、証明書配布要求に対する返信メッセージを作成して、サービス仲介装置２０１に対して返信する（ステップＳ３０７）。

【０１９９】

図３０は、証明書配布要求に対する返信メッセージの一例を示す説明図である。図３０に例示する認証証明書には、ＨＴＴＰ上のＳＯＡＰ（Simple Object Access Protocol）のプロトコルに従い、ＳＯＡＰ Ｈｅａｄｅｒ部において、証明書生成要求トークンが<cert-req-token>タグに格納されている。また、ＳＯＡＰ Ｂｏｄｙ部において、ＳＡＭＬ Ｒｅｓｐｏｎｓｅプロトコルに対応させて、<Response>タグの配下に、図２９に例示する認証証明書が格納されている。

【０２００】

また、図３１は、認証装置２００の証明書生成要求トークン管理手段１３が管理する証明書生成トークンと認証証明書識別子の対応管理表の一例を示す説明図である。証明書生成要求トークン管理手段１３は、証明書生成要求トークンと認証証明書の識別子と利用者識別子とを関連付けて、図３１に例示する対応管理表として、証明書生成要求トークン格納部２２のデータベース上で管理している。

【０２０１】

図３２は、サービス提供装置２０２向け認証証明書の一例を示す説明図である。サービス提供装置２０２向け認証証明書は、図２９に例示する認証証明書と比較すると、利用者Ａｌｉｃｅに関して認証装置２００が生成し、Ａｌｉｃｅの認証結果情報を証明するという点では同じであるが、記載内容に違いがある。例えば、図３２に例示する認証証明書は、利用者情報として、サービス提供装置２０２におけるＡｌｉｃｅの仮名（xxyyzz）を用いている点や、認証証明書の配布範囲を、サービス提供装置２０２だけに規定している点が異なる。

【０２０２】

認証証明書と証明書生成要求トークンを受信したサービス仲介装置２０１は、認証証明書を検証し、格納する。

【０２０３】

次に、サービス仲介装置２０１は、サービス提供装置２０２に対するレンタカー予約要求メッセージを作成し、証明書生成要求トークンを添付して、送付する（ステップＳ３０８）。

【０２０４】

図３３は、レンタカー予約要求メッセージの一例を示す説明図である。レンタカー予約要求メッセージには、ＨＴＴＰ上のＳＯＡＰに基づいて、ＳＯＡＰ　Ｈｅａｄｅｒ部に証明書生成要求トークンが格納され、ＳＯＡＰ　Ｂｏｄｙ部にレンタカー予約のための詳細情報が記載されている。

【０２０５】

レンタカー予約要求メッセージを受け取ったサービス提供装置２０２は、証明書生成要求トークンを抽出し、解析する。そして、認証装置２００が発行した証明書生成要求トークンであることを確認する。また、レンタカー予約には利用者の認証証明書が必要であることから、利用者の認証証明書に関する証明書生成要求メッセージを作成し、証明書生成要求トークンを添付して、認証装置２００に対して送付する（ステップＳ３０９）。

【０２０６】

図３４は、証明書生成要求メッセージの一例を示す説明図である。証明書生成要求メッセージは、ＨＴＴＰ上のＳＯＡＰを利用したメッセージであり、ＳＯＡＰ　Ｈｅａｄｅｒ部に、証明書生成要求トークンが格納され、ＳＯＡＰ　Ｂｏｄｙ部に、要求する証明書の種類（ここでは、認証証明書）などの証明書生成要求の詳細が記載されている。

【０２０７】

証明書生成要求メッセージを受け取った認証装置２００は、添付されている証明書生成要求トークンを取得（抽出）する。そして、サービス提供装置２０２に対する、管理するセキュリティポリシを参照の上、利用者に関する認証証明書配布の認可判断を行う（ステップＳ３１０）。

【０２０８】

次に、認証装置２００は、証明書生成要求トークンの内容を解析して、証明書生成要求トークンに関連づけられた証明書識別子を取得（抽出）し、証明書に記載されている利用者Ａｌｉｃｅを示す情報と、証明書生成要求トークンに対応するサービス提供装置２０２向け認証証明書とを取得する（ステップＳ３１１）。

【０２０９】

次に、認証装置２００は、サービス提供装置２０２に対する認証証明書を添付した、証明書生成要求に対する返信メッセージを作成し、サービス提供装置２０２に対して送付する（ステップＳ３１２）。

【０２１０】

証明書を受け取ったサービス提供装置２０２は、証明書を検証の上、記載情報から、Ａｌｉｃｅが認証されていることを確認し、Ａｌｉｃｅに対するレンタカー予約のアクションに対する認可判断を行う。認可判断の結果、アクションを許可してよいならば、Ａｌｉｃｅに対する所定のレンタカー予約を行う（ステップＳ３１３）。そして、サービス提供装置２０２は、サービス仲介装置２０１に対して、レンタカー予約要求に対する返信メッセージを作成し、送付する（ステップＳ３１４）。

【０２１１】

レンタカー予約返信メッセージを受け取ったサービス仲介装置２０１は、そのレンタカー予約情報を確認の上、Ａｌｉｃｅに対する旅行予約に関する全ての処理を完了させる（ステップＳ３１５）。そして、サービス仲介装置２０１は、Ａｌｉｃｅの端末装置２０３に対して、旅行予約が完了した旨の返信メッセージを作成し、送付する（ステップＳ３１６）。

【実施例２】

【０２１２】
次に、本発明の第２の実施例を、図面を参照して説明する。かかる実施例は本発明の第１の実施形態に対応するものである。
【０２１３】
図３５は、本発明による証明書生成配布システムの第２の実施例を説明するための説明図である。図３５に示す証明書生成配布システムは、認証装置２００と、サービス仲介装置２０１と、サービス提供装置２０４と、端末装置２０３とを備える。認証装置２００、サービス仲介装置２０１、サービス提供装置２０４および端末装置２０３は、それぞれ第１の実施形態における機能を含む。
【０２１４】
第２の実施例では、図３５に示すように、第１の実施例の構成（図２６を参照）におけるレンタカーサイト（サービス提供装置２０２）の代わりに、購買サイトとしてインターネット上で購買サービスを公開しているサービス提供装置２０４が追加されている。
【０２１５】
購買サイト（サービス提供装置２０４）は、利用者情報を管理しておらず、第１の実施例における旅行ポータルサイト（サービス仲介装置２０１）に対して課金処理の代行を依頼している。購買サイトは、認証装置２００が配布した、利用者に関する所定の属性情報を記載した属性証明書があれば、利用者に関する、旅行ポータルサイトからの購買要求を受け入れることができる。購買サイトのサービス提供装置２０４も、ＨＴＴＰに対応した通信機能を備える。
【０２１６】
Ａｌｉｃｅは、第１の実施例のステップＳ３１６が完了後、すなわち、既に、認証装置２００で認証済みでセッションが確立している状態で、端末装置２０３を利用して、旅行ポータルのサービス仲介装置２０１に対して、旅行関連グッズの購買要求を行う（ステップＳ３１７）。
【０２１７】
購買要求を受けたサービス仲介装置２０１は、第１の実施例のステップＳ３０７において受信し、格納したＡｌｉｃｅに関する証明書生成要求トークンを抽出して、購買サイトのサービス提供装置２０４に対する旅行関連グッズの購買要求メッセージを作成し、証明書生成要求トークンを添付して、サービス提供装置２０４に送付する（ステップＳ３１８）。
【０２１８】
購買要求メッセージを受けたサービス提供装置２０４は、受け取ったメッセージに含まれる証明書生成要求トークンを取得する。そして、サービス提供装置２０４は、認証装置２００に対する、証明書生成要求トークンに関連付けられた利用者の属性証明書の生成要求メッセージを作成し、証明書生成要求トークンを添付して、送付する（ステップＳ３１９）。
【０２１９】
例えば、本実施例では、要求する属性証明書に記載する属性情報として、郵便番号、年齢、支払い能力を規定する。図３６は、属性証明書の生成要求メッセージの一例を示す説明図である。生成要求メッセージは、ＨＴＴＰのＳＯＡＰを利用したメッセージであり、ＳＯＡＰ　Ｂｏｄｙ部において、生成要求する証明書の種類として、利用者の属性証明書が規定され、要求する属性情報の種類として、郵便番号（zip-code）、年齢（age）、支払い能力（rate-for-payment）が規定されている。
【０２２０】
認証装置２００は、証明書生成要求を受け取って、証明書生成要求トークンを取得し、解析する。そして、証明書生成要求トークンと関連付けられたＡｌｉｃｅの認証証明書を取得し、Ａｌｉｃｅに関して、郵便番号、年齢、支払い能力を含めた属性証明書を新規に生成する（ステップＳ３２０）。
【０２２１】

そして、認証装置２００は、属性証明書をサービス提供装置２０４に対して返信する（ステップＳ３２１）。図３７は、属性証明書の一例を示す説明図である。属性証明書には、利用者Ａｌｉｃｅの郵便番号（zip-code）、年齢（age）、支払い能力（rate-for-payment）の属性情報が記載されているが、利用者Ａｌｉｃｅの認証情報や、Ａｌｉｃｅを特定するに足る情報は記載されていない。

【０２２２】

属性証明書を受け取ったサービス提供装置２０４は、属性証明書を検証し、属性証明書に記載される情報を確認の上、購買要求を許可するか否かの認可判断を行う（ステップＳ３２２）。そして、購買要求を許可する場合、サービス提供装置２０４は、要求された旅行関連グッズの購買処理を行い、その結果をサービス仲介装置２０１に対して返信する（ステップＳ３２３）。

【０２２３】

購買要求に対する結果情報を受け取ったサービス仲介装置２０１は、その内容を確認の上、ステップＳ３１７におけるＡｌｉｃｅからの購買要求に対する返信メッセージを作成し、送付する（ステップＳ３２４）。

【０２２４】

その後、課金情報に関して、サービス仲介装置２０１とサービス提供装置２０４の間で情報交換が行われるが、ここでは省略する。

【実施例３】

【０２２５】

次に、本発明の第３の実施例を、図面を参照して説明する。かかる実施例は本発明の第１の実施形態に対応するものである。

【０２２６】

図３８は、本発明による証明書生成配布システムの第３の実施例を説明するための説明図である。図３８に示す証明書生成配布システムは、認証装置４００と、サービス仲介装置４０１と、サービス提供装置４０２と、端末装置４０３と、端末装置４０４とを備える。認証装置４００、サービス仲介装置４０１、サービス提供装置４０２、端末装置４０３および端末装置４０４は、それぞれ第１の実施形態における機能を含み、ＳＩＰ（Ｓｅｓｓｉｏｎ　Ｉｎｉｔｉａｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）に従った通信を互いに行うことができる。

【０２２７】

サービス仲介装置４０１は、ＳＩＰプロキシの機能を備えている。また、認証装置４００とサービス提供装置４０２とは、ＳＩＰサーバの機能を備えている。端末装置４０３と端末装置４０４とは、共にＳＩＰのメッセージを送受信できる携帯端末である。利用者ＡｌｉｃｅとＢｏｂは、共に、認証装置４００の運営する通信キャリアにアカウントを保有しており、それぞれ端末装置４０３と端末装置４０４とを用いて、ＳＩＰに対応したＶｏＩＰ（Ｖｏｉｃｅ　ｏｖｅｒ　ＩＰ）通信を行うことができる。

【０２２８】

Ａｌｉｃｅは、端末装置４０３を操作することにより、認証装置４００から所定の認証方式で認証を受ける（ステップＳ３３０）。この際、認証装置４００は、Ａｌｉｃｅに関するセッション情報と認証証明書とを生成する。次に、Ａｌｉｃｅは、Ｂｏｂに対してＶｏＩＰで通話しようと、端末装置４０３を用いて、サービス仲介装置４０１にＳＩＰ　ＩＮＶＩＴＥメッセージを送付する（ステップＳ３３１）。

【０２２９】

次に、ＳＩＰ　ＩＮＶＩＴＥメッセージを受け取ったサービス仲介装置４０１は、ＳＩＰ　ＩＮＶＩＴＥメッセージに関連する利用者の認証状態を確認するため、所定の通信プロトコルを用いて、認証装置４００に対して、利用者に関する認証証明書の配布要求を行う（ステップＳ３３２）。証明書配布要求のメッセージには、例えば、端末装置４０３の識別子情報が格納されている。

【０２３０】

証明書配布要求を受信した認証装置４００は、端末装置４０３の識別子情報を確認し、端末識別子情報を基にして、認証要求がＡｌｉｃｅに関連していることを確認し、Ａｌｉｃｅのセッション情報と認証証明書とを確認する。次に、認証装置４００は、証明書生成要求トークンを生成して、Ａｌｉｃｅの認証証明書と関連付けて管理した上で（ステップＳ３３３）、証明書生成要求トークンと認証証明書を添付して、サービス仲介装置４０１に返信する（ステップＳ３３４）。

【０２３１】

証明書生成要求に対する返信を受け取ったサービス仲介装置４０１は、証明書生成要求トークンを取得して、サービス提供装置４０２に対する新たなＳＩＰ　ＩＮＶＩＴＥメッセージを作成し、証明書生成要求トークンを添付した上で、サービス提供装置４０２に送付する（ステップＳ３３５）。

【０２３２】

サービス仲介装置４０１からのＳＩＰ　ＩＮＶＩＴＥメッセージを受け取ったサービス提供装置４０２は、受け取った証明書生成要求トークンを添付した、認証証明書の証明書生成要求メッセージを作成し、認証装置４００に対して、送付する（ステップＳ３３６）。

【０２３３】

証明書生成要求メッセージを受け取った認証装置４００は、証明書生成要求トークンを取得し、Ａｌｉｃｅに関する認証証明書の生成要求であることを確認する。そして、認証装置４００は、Ａｌｉｃｅに関する認証証明書を生成し、サービス提供装置４０２に対して返信する（ステップＳ３３７）。

【０２３４】

証明書生成要求に対する応答メッセージを受け取ったサービス提供装置４０２は、認証証明書を取得して検証し、利用者Ａｌｉｃｅからの要求であることを確認する。そして、サービス提供装置４０２は、Ａｌｉｃｅの契約状態などを含むセキュリティポリシを確認のうえ、Ｂｏｂに対するＳＩＰ　ＩＮＶＩＴＥの転送の認可判断を行う（ステップＳ３３８）。次に、サービス提供装置４０２は、Ｂｏｂに対するＡｌｉｃｅからの ＳＩＰ　ＩＮＶＩＴＥメッセージを作成し、Ｂｏｂの端末装置４０４に対して送付する（ステップＳ３３９）。

【０２３５】

サービス提供装置４０２からのＳＩＰ　ＩＮＶＩＴＥメッセージを端末装置４０４において受け取ったＢｏｂは、端末装置４０４の示す呼に反応し、通話を許可する。ここで、端末装置４０４は、ＳＩＰ　ＩＮＶＩＴＥメッセージに対するＡＣＫを返信する（ステップＳ３４０）。

【０２３６】

サービス提供装置４０２は、端末装置４０４からのＡＣＫを受信し、サービス仲介装置４０１に対して、ＡＣＫを返信する（ステップＳ３４１）。さらに、サービス仲介装置４０１は、Ａｌｉｃｅの端末装置４０３に対して、ＡＣＫを返信する（ステップＳ３４２）。以上の処理によって、Ａｌｉｃｅは、Ｂｏｂとの通話を開始することができる。

【実施例４】

【０２３７】

次に、本発明の第４の実施例を、図面を参照して説明する。かかる実施例は本発明の第２の実施形態に対応するものである。

【０２３８】

図３９は、本発明による証明書生成配布システムの第４の実施例を説明するための説明図である。図３９に示す証明書生成配布システムは、認証装置２００と、サービス仲介装置２０１と、端末装置２０３と、サービス仲介装置６０１と、サービス提供装置６００とを備える。認証装置２００、サービス仲介装置２０１、端末装置２０３、サービス仲介装置６０１およびサービス提供装置６００は、それぞれ第２の実施形態における機能を含む。

【０２３９】
図３９に示す第４の実施例では、第１の実施例の構成（図２６を参照）に加えて、レンタカー予約サイトを提供するサービス仲介装置６０１と、自動車保険サービスを提供するサービス提供装置６００とが、インターネット等の通信ネットワークを介して接続されている。なお、サービス仲介装置６０１は、第１の実施例におけるサービス提供装置２０２に対応する。
【０２４０】
サービス提供装置６００は、レンタカー予約サイト（サービス仲介装置６０１）からの自動車保険サービス要求に応じて、利用者向けの自動車保険を提供する。
【０２４１】
また、第４の実施例におけるレンタカー予約サイトであるサービス仲介装置６０１は、第１の実施例のサービス提供装置２０２の機能に加え、ユーザの代わりに自動車保険を要求するサービスを仲介する機能も併せ持つ。第４の実施例におけるレンタカー予約サイト（サービス仲介装置６０１）は、レンタカー予約処理を完了する前に、自動車保険サイト（サービス提供装置６００）にアクセスし、自動車保険に加入するための処理を実行してから、レンタカー予約処理を完了し、ユーザに通知する。
【０２４２】
認証サービスを所定の利用者に対して公開する認証装置２００と、旅行ポータルサイトとしてのサービスを所定の利用者に公開しているサービス仲介装置２０１と、汎用的なＷｅｂブラウザの機能を持つ利用者の端末装置２０３とは、第１の実施例と同じ機能を持つ。すべての装置は、ＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｐｏｒｔ　Ｐｒｏｔｏｃｏｌ）の規定する通信プロトコルで互いに通信する機能を備える。
【０２４３】
利用者Ａｌｉｃｅは、事前に認証装置２００を管理する通信事業者に加入しており、アカウントを保有している（アカウント名は、Alice200）。また、Ａｌｉｃｅは、旅行ポータルサイトとレンタカー予約サイト、自動車保険サイトにも加入しており、やはり、それぞれ、アカウントを保有している（アカウント名は、Alice201、Alice601、Alice600）。旅行ポータルサイト、レンタカー予約サイト、自動車保険サイトにおけるそれぞれのアカウントは、通信事業者のアカウントと関連付けられて管理されている。
【０２４４】
図４０は、認証装置２００の利用者情報管理手段１１が管理するアカウント対応管理表の登録例を示す説明図である。図４０には、Ａｌｉｃｅに関する装置毎のアカウント名（仮名）の対応管理表の一例を示す。図４０に示す例では、それぞれの装置において管理されるＡｌｉｃｅのアカウント名（仮名）が、装置名に関連付けられて管理されている。
【０２４５】
当初、Ａｌｉｃｅは、認証装置２００に認証されておらず、認証装置２００、サービス仲介装置２０１、サービス仲介装置６０１およびサービス提供装置６００のいずれにも、Ａｌｉｃｅに関するセッションは確立していない。この状態から、レンタカー予約サイト（サービス仲介装置６０１）が証明書生成要求トークンをサービス仲介装置２０１から取得するまでは、第１の実施例のステップＳ３００からステップＳ３０８までと、同じ処理を行う。以下、ステップＳ３０８以降の処理について説明する。
【０２４６】
ステップＳ３０８において、レンタカー予約サイトを運営するサービス仲介装置６０１が、サービス仲介装置２０１から証明書生成要求トークンを取得すると、第４の実施例では、サービス応答を返すのではなく、自動車保険サイトを運営するサービス提供装置６００にアクセスする。まず、サービス仲介装置６０１は、証明書生成要求トークン（サービス仲介装置６０１向け）を添付した証明書配布要求メッセージを作成し、認証装置２００に送付する（ステップＳ４００）。
【０２４７】
証明書生成要求を受取った認証装置２００は、添付されている証明書生成要求トークン

を取得（抽出）する。そして、サービス仲介装置６０１に対する、管理するセキュリティポリシを参照の上、利用者に関する認証証明書配布の認可判断を行う（ステップＳ４０１）。

【０２４８】

次に、認証装置２００は、証明書生成要求トークンの内容を解析して、証明書生成要求トークンに関連づけられた証明書識別子を取得（抽出）し、証明書に記載されている利用者Ａｌｉｃｅを示す情報をその認証結果情報を元に取得する。

【０２４９】

そして、認証装置２００は、証明書記載の情報を基にして、サービス仲介装置６０１に対して関連づけられたＡｌｉｃｅの利用者識別子（図４０に示す例では、xxyyzz）と、証明書の配布範囲（この例では、サービス仲介装置６０１）の情報を更新したＡｌｉｃｅに関する認証証明書（サービス仲介装置６０１向け）を新規に生成する。

【０２５０】

さらに、認証装置２００は、認証証明書（サービス仲介装置６０１向け）に基づいて、新たにサービス提供装置６００向けの認証証明書を発行し、認証証明書と関連する証明書要求トークン（サービス提供装置６００向け）を生成し、関連付けて管理する（ステップＳ４０２）。

【０２５１】

次に、認証装置２００は、認証証明書（サービス仲介装置６０１向け）と証明書生成要求トークン（サービス提供装置６００向け）を添付して、証明書配布要求に対する返信メッセージを作成して、サービス仲介装置６０１に対して返信する（ステップＳ４０３）。

【０２５２】

認証証明書と証明書生成要求トークンを受信したサービス仲介装置６０１は、認証証明書を検証し、格納する。次に、サービス仲介装置６０１は、サービス提供装置６００に対する自動車保険加入要求メッセージを作成し、証明書生成要求トークン（サービス提供装置６００向け）を添付して、サービス提供装置６００に送付する（ステップＳ４０４）

自動車保険加入要求を受け取ったサービス提供装置６００は、証明書生成要求トークンを取り出し、解析する。そして、認証装置２００が発行した証明書生成要求トークンであることを確認する。また、自動車保険加入には利用者の認証証明書（サービス提供装置６００向け）が必要であることから、利用者の認証証明書に関する証明書生成要求メッセージを作成し、証明書生成要求トークン（サービス提供装置６００向け）を添付して、認証装置２００に対して送付する（ステップＳ４０５）。

【０２５３】

証明書生成要求メッセージを受け取った認証装置２００は、添付されている証明書生成要求トークンを取得し、サービス提供装置６００に対する、管理するセキュリティポリシを参照の上、利用者に関する認証証明書の生成及び配布の認可判断を行う（ステップＳ４０６）。

【０２５４】

次に、認証装置２００は、証明書生成要求トークンの内容を解析して、証明書生成要求トークンに関連づけられた証明書識別子を取得（抽出）し、証明書に記載されている利用者Ａｌｉｃｅを示す情報をその認証結果情報を元に取得する。

【０２５５】

そして、認証装置２００は、証明書記載の情報を基にして、サービス提供装置６００に対して関連づけられた利用者識別子（図４０に示す例では、qwertyに相当）と、証明書の配布範囲（この例では、サービス提供装置６００に相当）の情報を更新したＡｌｉｃｅに関する認証証明書（サービス提供装置６００向け）を取得する（ステップＳ４０７）。

【０２５６】

次に、認証装置２００は、サービス提供装置６００に対する認証証明書を添付した、証明書生成要求に対する返信メッセージを作成し、サービス提供装置６００に対して送付する（ステップＳ４０８）。

【０２５７】
証明書を受け取ったサービス提供装置６００は、証明書を検証の上、記載情報から、Ａｌｉｃｅが認証されていることを確認し、Ａｌｉｃｅに対する自動車保険加入のアクションに対する認可判断を行う。認可判断の結果、アクションを許可してよいならば、Ａｌｉｃｅに対する自動車保険加入手続きを実行する（ステップＳ４０９）。そして、サービス提供装置６００は、サービス仲介装置６０１に対して、自動車保険加入要求に対する返信メッセージを作成し、送付する（ステップＳ４１０）。
【０２５８】
自動車保険加入応答メッセージを受け取ったサービス仲介装置６０１は、ステップＳ４０４において取得した証明書を検証の上、記載情報から、Ａｌｉｃｅが認証されていることを確認し、Ａｌｉｃｅに対するレンタカー予約のアクションに対する認可判断を行う。認可判断の結果、アクションを許可してよいならば、Ａｌｉｃｅに対する所定のレンタカー予約を行う（ステップＳ４１１）。以降の処理は、第１の実施例におけるステップＳ３１４～Ｓ３１６と同じである。
【０２５９】
以下、本発明による効果について説明する。第１の効果は、証明書の作成と配布に関して行われる装置間の通信を効率化できることにある。その理由は、ユーザエージェントを介さずに、かつ簡単な処理でサービス装置から認証装置への証明書作成・配布を行うことができるからである。
【０２６０】
第２の効果は、機密情報の漏洩を防止できることにある。その理由は、サービス装置間で交換する証明書生成配布要求トークン自体には、利用者を特定する情報が含まれていないからである。
【０２６１】
第３の効果は、認証装置は、証明書記載の情報の漏洩を防止できることにある。その理由は、認証装置は、証明書の有効範囲を厳密に規定し、証明書に記載した有効範囲と配布対象となるサービス提供装置とが一致するように、証明書の生成及び配布を行うことができるからである。
【０２６２】
第４の効果は、認証装置は、証明書を配布したサービス提供装置を監査できることにある。その理由は、認証装置は、証明書を配布したサービス提供装置を全て把握し、記録することができるからである。なお、サービス提供装置を監査するとは、サービス提供装置に対するアクセスログを管理し、サービス提供装置への不正アクセスが無いことを確認する処理を実行することである。
【０２６３】
なお、上記に示した実施形態では、以下の（１）～（５）に示すような特徴的構成を備えた証明書生成配布システムが示されている。
【０２６４】
（１）証明書生成配布システムは、利用者を認証する認証装置と、サービスを提供するサービス提供装置と、サービス提供装置によるサービス提供を仲介するサービス仲介装置とを備えた証明書生成配布システムであって、認証装置は、サービス仲介装置において有効な第１の証明書に対応付けた情報である証明書生成要求トークンを、第１の証明書とともにサービス仲介装置に送信するトークン送信手段（例えば、証明書配布要求受付手段１５で実現される）を含み、サービス仲介装置は、トークン送信手段が送信した証明書生成要求トークンを受信し、サービス提供装置に転送する仲介装置トークン転送手段（例えば、サービスアクセス仲介手段５０で実現される）を含み、サービス提供装置は、仲介装置トークン転送手段が送信した証明書生成要求トークンを受信し、当該サービス提供装置において有効な第２の証明書を要求する際に証明書生成要求トークンを認証装置に送信する証明書要求手段（例えば、証明書生成要求手段８０で実現される）を含み、認証装置は、受信した証明書生成要求トークンに対応する第１の証明書に基づいて生成された第２の証

明書を、証明書要求手段による第２の証明書の要求に応じてサービス提供装置に送信する証明書送信手段（例えば、証明書生成要求受付手段１２で実現される）を含む。

【０２６５】

（２）上記（１）の証明書生成配布システムにおいて、証明書送信手段は、第２の証明書とともに、当該第２の証明書に対応付けた情報である証明書生成要求トークンをサービス提供装置に送信し、サービス提供装置は、証明書送信手段が送信した証明書生成要求トークンを他のサービス提供装置に転送する提供装置トークン転送手段（例えば、サービスアクセス仲介手段５０で実現される）を含んでもよい。そのように構成された証明書生成配布システムは、サービス提供装置が、さらに別のサービス提供装置に代理アクセスすることができる。

【０２６６】

（３）上記（１）の証明書生成配布システムにおいて、サービス仲介装置は、認証装置に第１の証明書を要求する要求手段（例えば、証明書配布要求手段５１で実現される）を含み、要求手段は、第１の証明書を要求する際に、所定のサービス提供装置を示す情報（例えば、リスト情報で実現される）を認証装置に送信し、証明書送信手段は、受信した所定のサービス提供装置を示す情報に基づいて、第２の証明書を送信するか否かを判断してもよい。そのように構成された証明書生成配布システムは、サービス仲介装置が指定したサービス提供装置に証明書を送信することができる。

【０２６７】

（４）上記（１）の証明書生成配布システムにおいて、認証装置は、証明書生成要求トークンを生成する認証装置トークン生成手段を含み、トークン送信手段は、認証装置トークン生成手段が生成した証明書生成要求トークンをサービス仲介装置に送信してもよい。そのように構成された証明書生成配布システムは、認証装置が生成した証明書生成要求トークンを利用することができる。

【０２６８】

（５）上記（１）の証明書生成配布システムにおいて、サービス仲介装置は、証明書生成要求トークンを生成する仲介装置トークン生成手段を含み、トークン送信手段は、仲介装置トークン生成手段が生成した証明書生成要求トークンを受信し、第１の証明書に対応付けてサービス仲介装置に送信してもよい。そのように構成された証明書生成配布システムは、サービス仲介装置が生成した証明書生成要求トークンを利用することができる。

【産業上の利用可能性】

【０２６９】

本発明によれば、インターネット上サービス、企業内システム、企業間システム、キャリアシステムなどのネットワーク上で構築される分散システムにおける証明書生成配布システムや、証明書生成配布システムをコンピュータに実現するためのプログラム等の用途に適用できる。

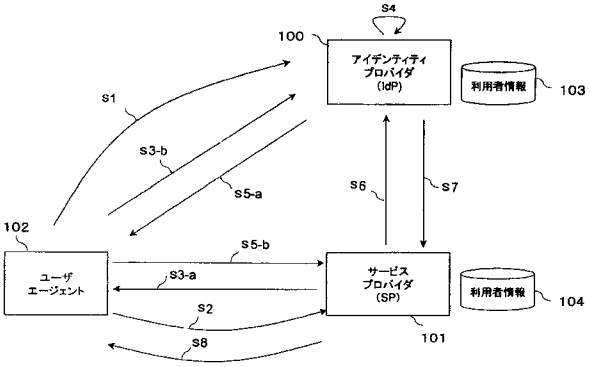
【０２７０】

以上、実施形態および実施例を参照して本願発明を説明したが、本願発明は上記実施形態および実施例に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

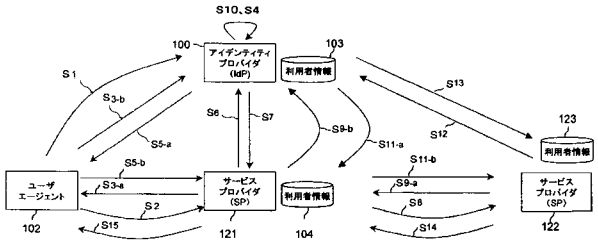
【０２７１】

この出願は、２００７年９月２５日に出願された日本出願の特願２００７－２４７５９７の内容が全て取り込まれており、この日本出願を基礎として優先権を主張するものである。

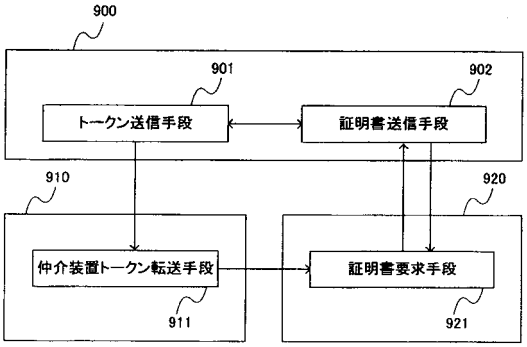
【図１】



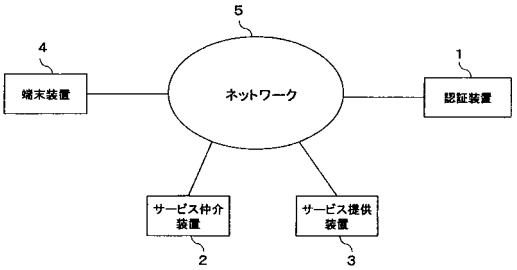
【図２】



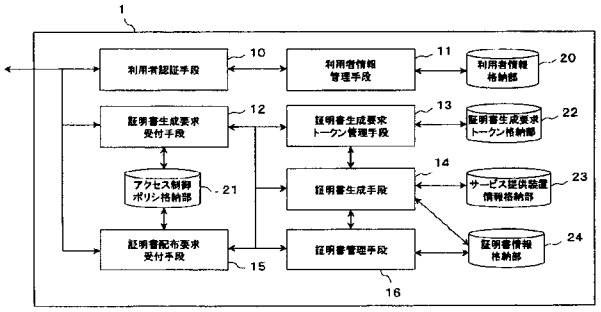
【図３】



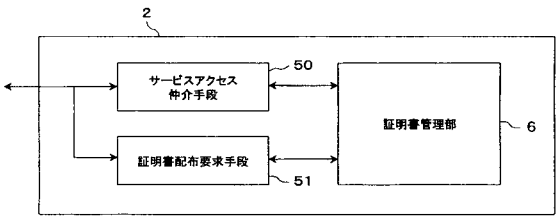
【図４】



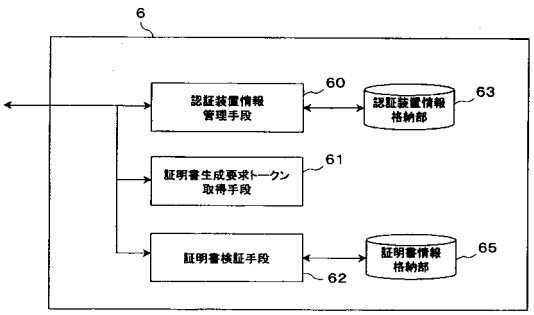
【図５】



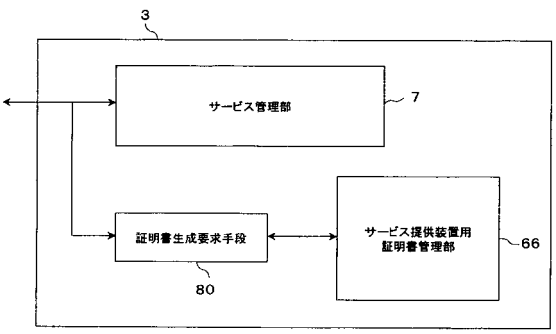
【図６】



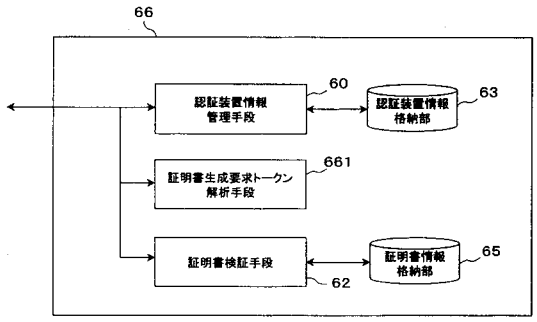
【図７】



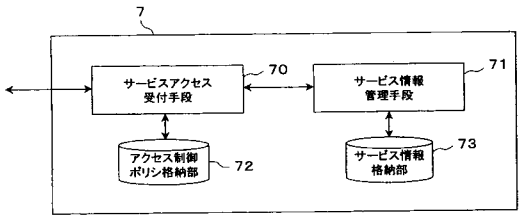
【図８】



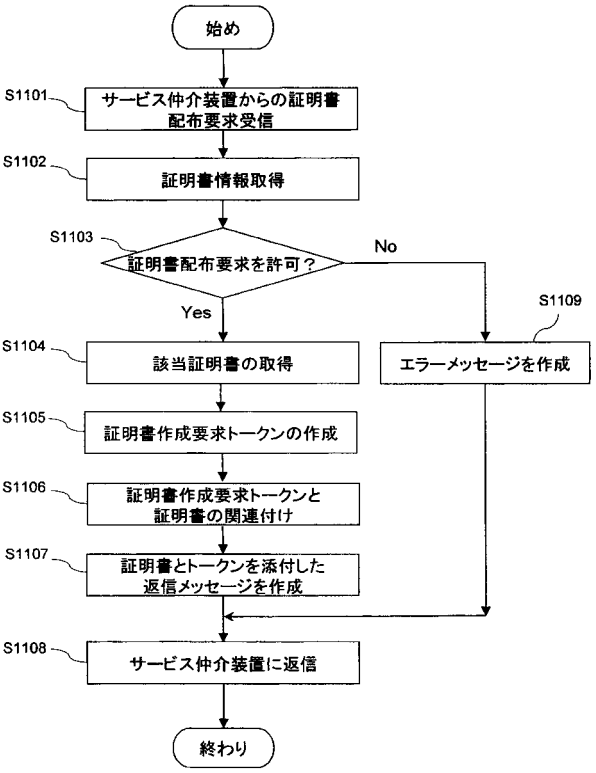
【図９】



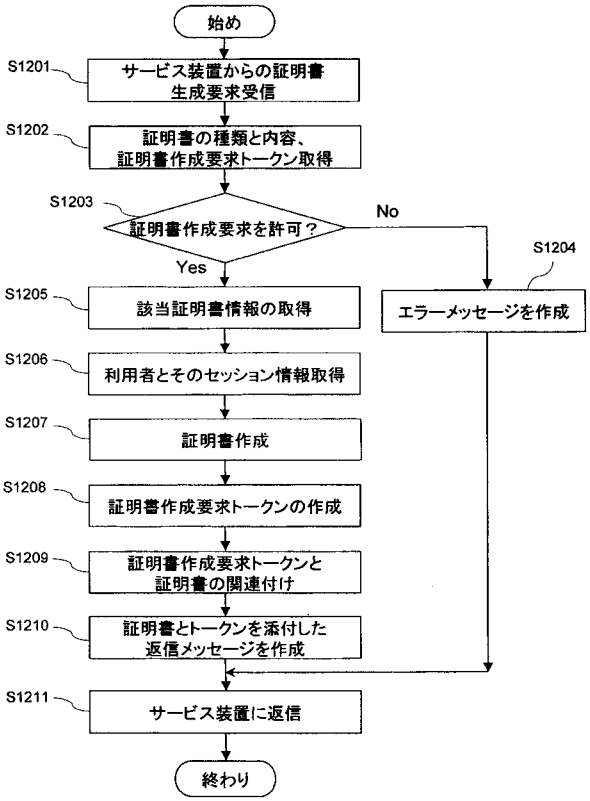
【図１０】



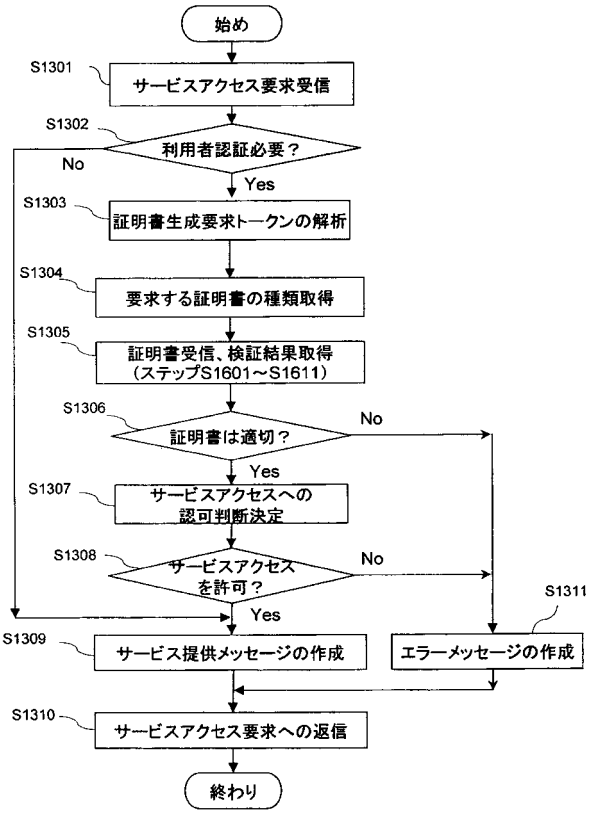
【図１１】



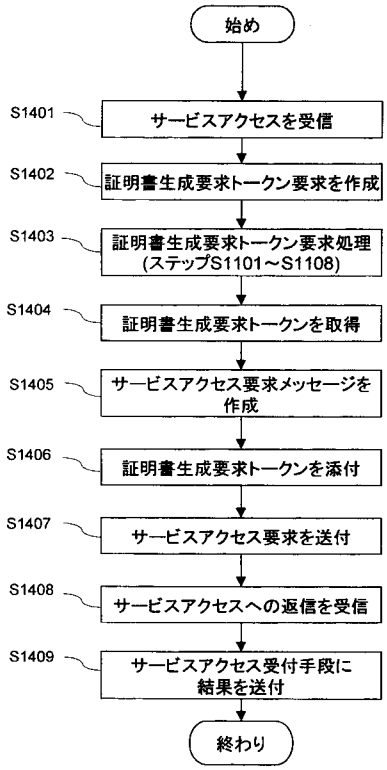
【図１２】



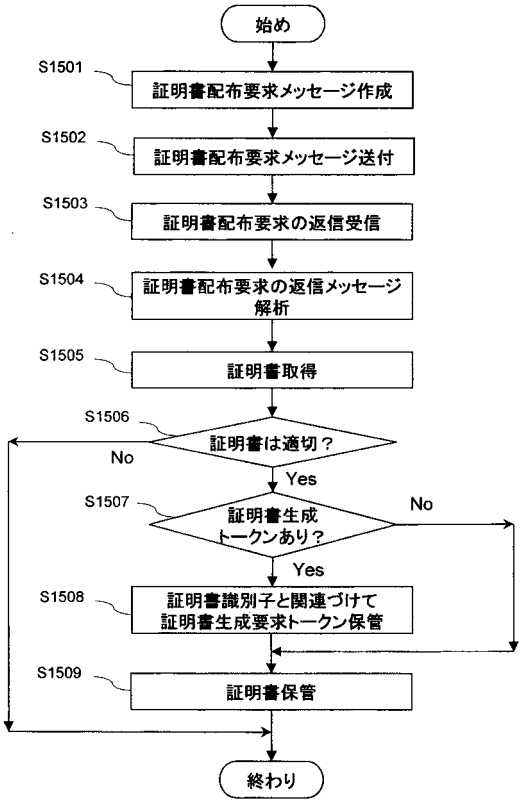
【図１３】



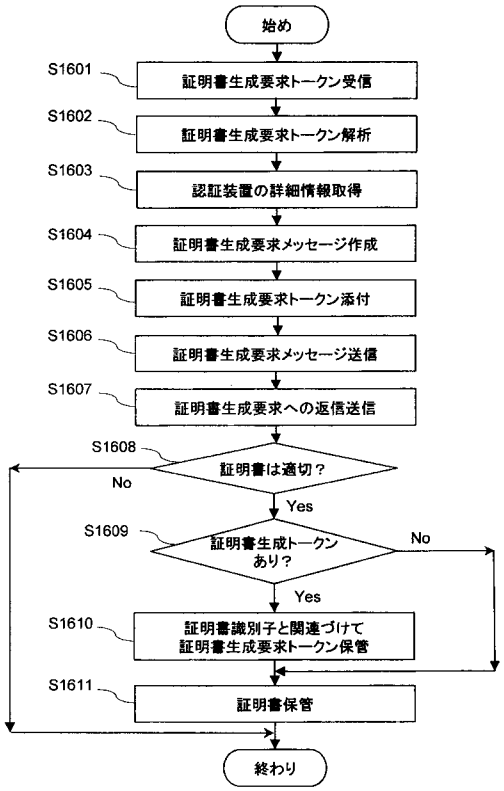
【図１４】



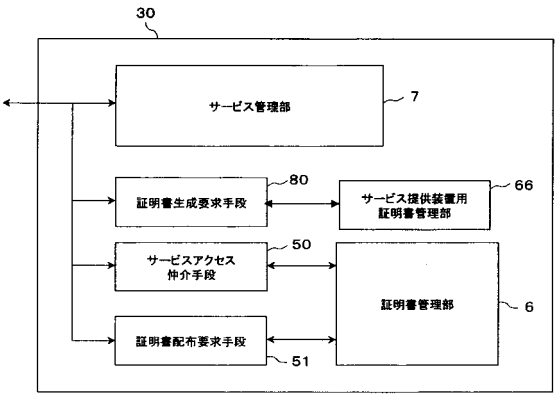
【図１５】



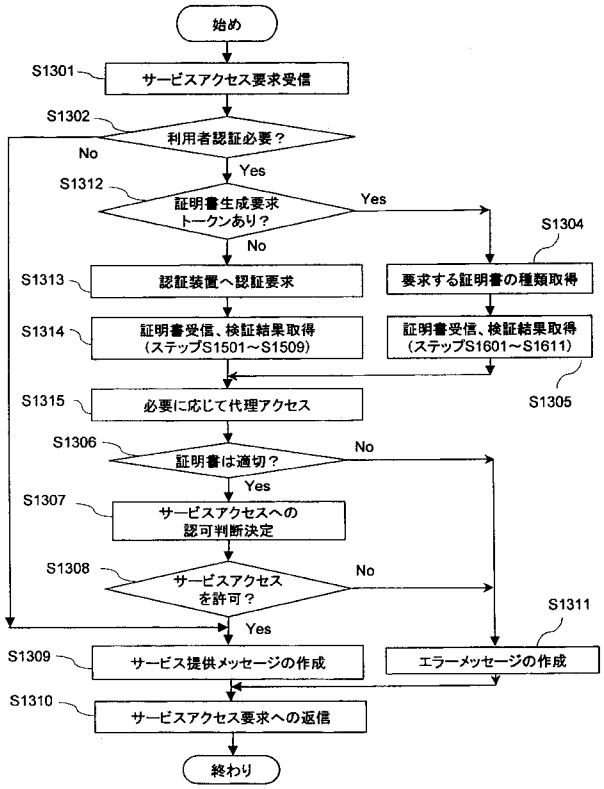
【図１６】



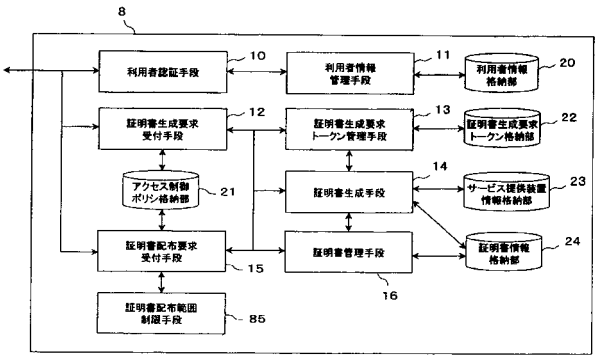
【図１７】



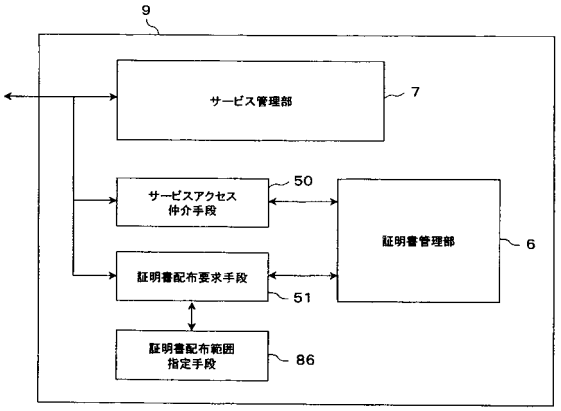
【図１８】



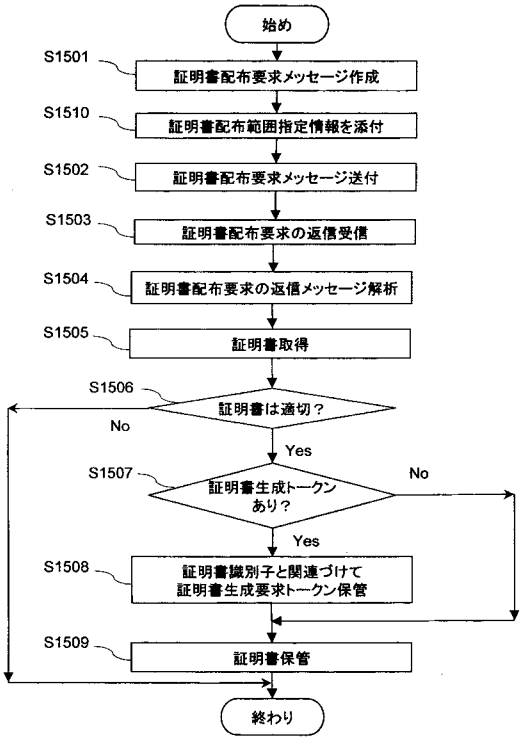
【図１９】



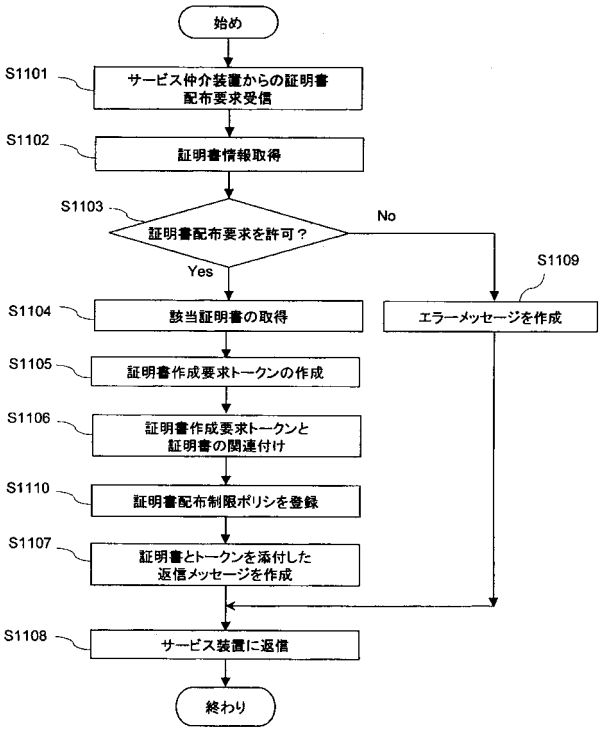
【図２０】



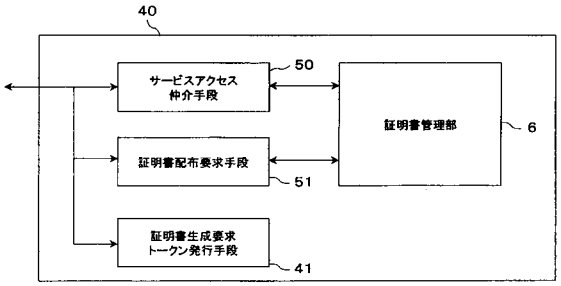
【図２１】



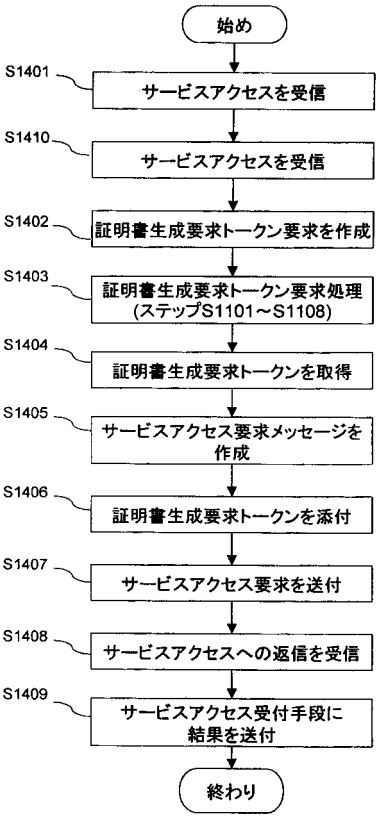
【図２２】



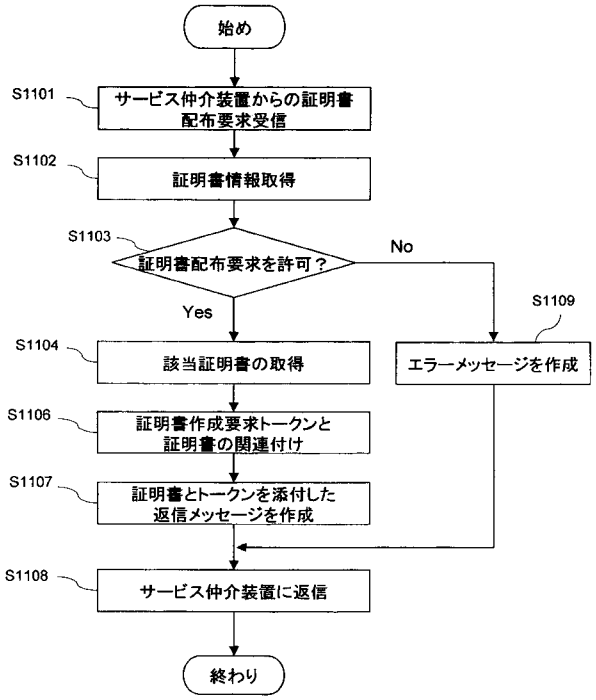
【図２３】



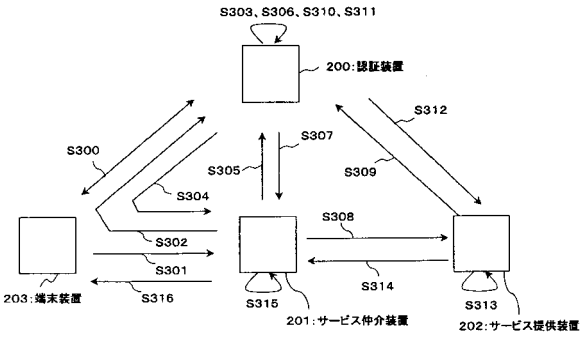
【図２４】



【図２５】



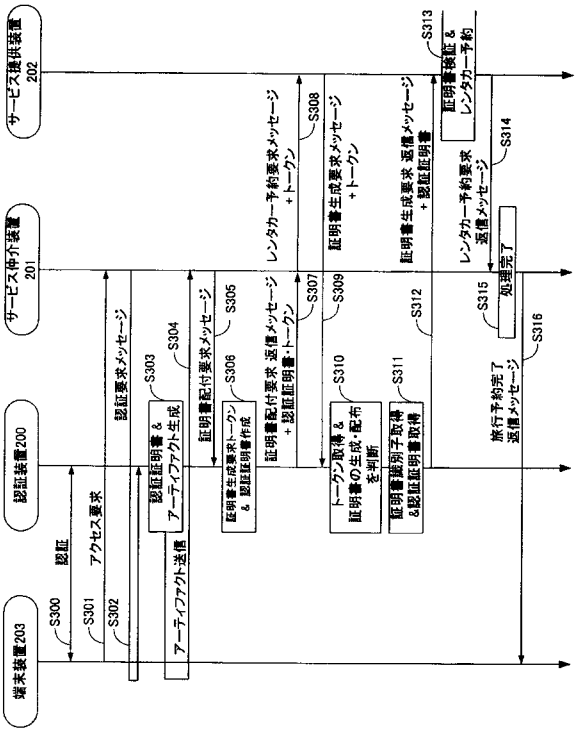
【図２６】



【図２７】

装置名	アカウント名(仮名)	ドメイン
認証装置200	Alice200	authn200.com
サービス仲介装置201	aabbcc	sp-proxy201.com
サービス提供装置202	xxyyzz	sp202.com

【図２８】



【図２９】

```
<Assertion ID="assertion-12345678910" IssueInstant="2005-07-01T00:20:02Z" Version="2.0">
  <Issuer> https://authn200.com </Issuer>
  <ds:Signature> signature by authn200 goes here </ds:Signature>
  <Subject>
    <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:persistent>
      aabbcc
    </NameID>
  </Subject>
  <Conditions NotBefore="2005-07-01T00:20:02Z" NotOnOrAfter="2005-07-01T00:25:02Z">
    <AudienceRestriction>
      <Audience>http://sp-proxy201.com</Audience>
    </AudienceRestriction>
  </Conditions>
  <AuthnStatement AuthnInstant="2005-07-01T00:20:02Z" NotONOrAfter="2005-07-01T00:25:02Z">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0.ac:classes:PasswordProtectedTransport
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </AuthnStatement>
</Assertion>
```

【図３０】

```
HTTP1.1 200 OK
Content-Type: text/xmi
Content-Length: 13455
<soap-env:Envelope>
  <soap-env:Header>
    <cert-req-token>
      9df234tr5234rig3485289
    </cert-req-token>
  </soap-env:Header>
  <soap-env:Body>
    <samlp:Response>
      <saml:Issuer> https://authn200.com </saml:Issuer>
      <ds:Signature> ..... </ds:Signature>
      <Status>
        <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
      </Status>
      <Assertion ID="assertion-12345678910" IssueInstant="2005-07-01T00:20:02Z" Version="2.0">
        <Issuer> https://authn200.com</Issuer>
        <ds:Signature> signature by authn200 goes here </ds:Signature>
        <Subject>
          <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:persistent>
            aabbcc
          </NameID>
        </Subject>
        ...
      </Assertion>
    </samlp:Response>
  </soap-env:Body>
</soap-env:Envelope>
```

【図３１】

証明書生成要求トークン	証明書識別子	利用者識別子
9df234tr5234rig3485289	assertion-12345678910	Alice200

【図３２】

```
<Assertion ID="assertion-789012255" IssueInstant="2005-07-01T00:23:02Z" Version="2.0">
  <Issuer> https://authn200.com </Issuer>
  <ds:Signature> signature by authn200 goes here </ds:Signature>
  <Subject>
    <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:persistent>
      xxyyzz
    </NameID>
  </Subject>
  <Conditions NotBefore="2005-07-01T00:20:02Z" NotOnOrAfter="2005-07-01T00:20:02Z">
    <AudienceRestriction>
      <Audience>http://sp202.com</Audience>
    </AudienceRestriction>
  </Conditions>
  <AuthnStatement AuthnInstant="2005-07-01T00:20:02Z" NotONOrAfter="2005-07-01T00:25:02Z">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </AuthnStatement>
</Assertion>
```

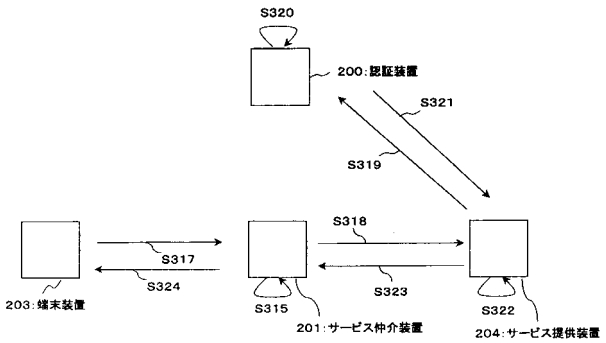
【図３３】

```
POST /rent-car-service HTTP/1.1
HOST: sp-proxy201.com
Content-Type: text/xml
Content-Length: 555
<soap-env:Envelope>
  <soap-env:Header>
    <cert-req-token>
      9df234tr5234rig3485289
    </cert-req-token>
  </soap-env:Header>
  <soap-env:Body>
    <rent-a-car-req>
      <date> 2007-06-25 </date>
      <car-type> medium </car-type>
      ...
    </rent-a-car-req>
  </soap-env:Body>
</soap-env:Envelope>
```

【図３４】

```
POST /cert-generating-service HTTP/1.1
HOST: sp202.com
Content-Type: text/xml
Content-Length: 444
<soap-env:Envelope>
  <soap-env:Header>
    <cert-req-token>
      9df234tr5234rig3485289
    </cert-req-token>
  </soap-env:Header>
  <soap-env:Body>
    <cert-generation-req>
      <cert-type> authentication </cert-type>
      ...
    </cert-generation-req>
  </soap-env:Body>
</soap-env:Envelope>
```

【図３５】



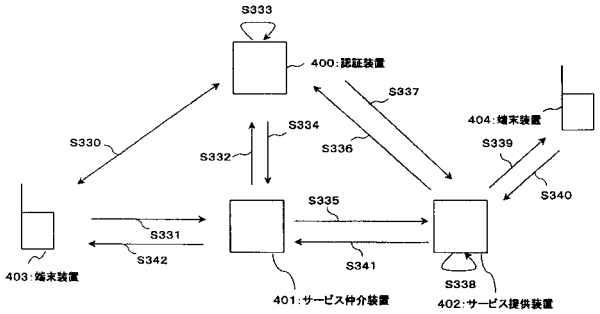
【図３６】

```
POST /cert-generating-service HTTP/1.1
HOST: sp204.com
Content-Type: text/xml
Content-Length: 777
<soap-env:Envelope>
  <soap-env:Header>
    <cert-req-token>
       sdfasdfasjkdfa90323
    </cert-req-token>
  </soap-env:Header>
  <soap-env:Body>
     <cert-generation-req>
        <cert-type> attributes </cert-type>
        <req-attributes>
           <zip-code/>
           <age/>
            <rate-for-payment/>
        </req-attributes>
    </cert-generation-req>
  </soap-env:Body>
</soap-env:Envelope>
```

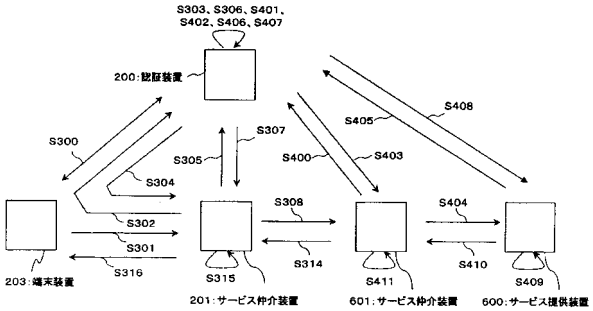
【図３７】

```
<Assertion ID="assertion-789012255" IssueInstant="2005-07-01T00:30:02Z" Version="2.0">
  <Issuer> https://authn200.com </Issuer>
  <ds:Signature> signature by authn200 goes here </ds:Signature>
  <Conditions NotBefore="2005-07-01T00:50:02Z" NotOnOrAfter="2005-07-01T00:50:02Z">
    <AudienceRestriction>
      <Audience>http://sp204.com</Audience>
    </AudienceRestriction>
  </Conditions>
  <AttributeStatement>
     <saml:Attribute Name="zip-code">
       <saml:AttributeValue xsi:type="xs:string"> 211-8666 </saml:AttributeValue>
     </saml:Attribute>
     <saml:Attribute Name="age">
       <saml:AttributeValue xsi:type="xs:string"> 40 </saml:AttributeValue>
     </saml:Attribute>
     <saml:Attribute Name="rate-for-payment">
       <saml:AttributeValue xsi:type="xs:string"> AAA </saml:AttributeValue>
     </saml:Attribute>
  </AttributeStatement>
</Assertion>
```

【図３８】



【図３９】



【図４０】

装置名	アカウント名（仮名）	ドメイン
認証装置200	Alice200	authn200.com
サービス仲介装置201	aabbcc	sp-proxy201.com
サービス提供装置601	xxyyzz	sp202.com
サービス提供装置600	qwerty	sp600. insurance. com

フロントページの続き

審査官　林　毅

(56)参考文献　特開２００７－２３３７０５（ＪＰ，Ａ）
特開２００７－１４９０１０（ＪＰ，Ａ）
国際公開第２００４／０５９４１５（WO，Ａ１）
国際公開第２００４／０５９４７８（WO，Ａ１）
米国特許出願公開第２００６／００２１０１８（ＵＳ，Ａ１）
Assertions and Protocols for the OASIS Security Assertion Markup Language(SAML) v2.0, OASIS，２００５年　3月１５日，ＵＲＬ，http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３３
Ｇ０６Ｆ　２１／３１
Ｈ０４Ｌ　９／３２