(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2012-519339
(P2012-519339A)
(43)公表日　平成24年8月23日(2012.8.23)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 13/00	(2006.01)	G06F	13/00	520D	5B084
G06F 21/20	(2006.01)	G06F	21/20	131A	

審査請求 有　予備審査請求 未請求　（全 20 頁）

(21)出願番号	特願2011-552367 (P2011-552367)
(86)(22)出願日	平成22年3月12日 (2010.3.12)
(85)翻訳文提出日	平成23年9月2日 (2011.9.2)
(86)国際出願番号	PCT/EP2010/001587
(87)国際公開番号	WO2010/102834
(87)国際公開日	平成22年9月16日 (2010.9.16)
(31)優先権主張番号	09003600.5
(32)優先日	平成21年3月12日 (2009.3.12)
(33)優先権主張国	欧州特許庁 (EP)

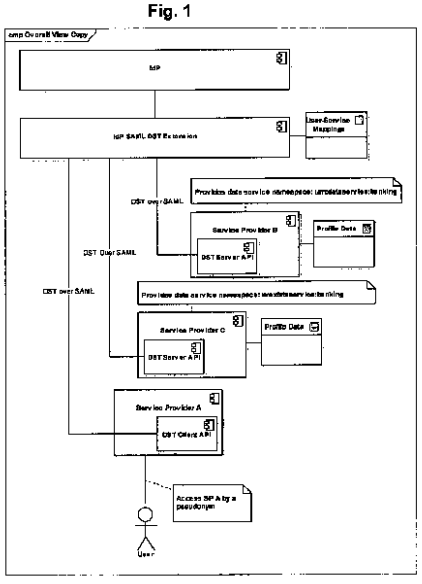
(71)出願人　508342183
エヌイーシー　ヨーロッパ　リミテッド
ＮＥＣ　ＥＵＲＯＰＥ　ＬＴＤ.
ドイツ連邦共和国、６９１１５　ハイデルベルク、クアフュルステン・アンラーゲ　３６
(74)代理人　100097157
弁理士　桂木　雄二
(72)発明者　ヴィンクラー、フローリアン
ドイツ連邦共和国　６９１２６　ハイデルベルク、アム　ヴァルトラント　１０
(72)発明者　ジラオ、ジョアオ
ドイツ連邦共和国　６７０６３　ルードヴィッヒスハーフェン、ザイラーシュトラーセ　２３

最終頁に続く

(54)【発明の名称】ユーザまたはエンティティの分散データの管理および交換をサポートする方法

(57)【要約】
ユーザまたはエンティティの分散データ、特にユーザプロファイル情報データの管理および交換をサポートする方法を提供する。ＳＡＭＬ（Security Assertion Markup Language）をベアラプロトコルとして使用するプロトコルが提供される。ＳＡＭＬメッセージは、ＳＡＭＬ
ＤＳＴメッセージを作成するために、ＤＳＴ（Data Services Template）またはＤＳＴライクなメッセージのためのコンテナとして機能する。ＤＳＴまたはＤＳＴライクなメッセージはデータ処理情報を含み、ＤＳＴまたはＤＳＴライクなメッセージに対して、統一されたプロトコル名前空間が、プロトコル固有の名前空間として定義される。

Fig. 1



【特許請求の範囲】
【請求項１】
ユーザまたはエンティティの分散データ、特にユーザプロファイル情報データの管理および交換をサポートする方法において、
ＳＡＭＬ（Security Assertion Markup Language）をベアラプロトコルとして使用するプロトコルが提供され、ＳＡＭＬメッセージは、ＳＡＭＬ　ＤＳＴメッセージを作成するために、ＤＳＴ（Data Services Template）またはＤＳＴライクなメッセージのためのコンテナとして機能し、前記ＤＳＴまたはＤＳＴライクなメッセージはデータ処理情報を含み、前記ＤＳＴまたはＤＳＴライクなメッセージに対して、統一されたプロトコル名前空間が、プロトコル固有の名前空間として定義されることを特徴とする、ユーザまたはエンティティの分散データの管理および交換をサポートする方法。
【請求項２】
前記ＳＡＭＬ　ＤＳＴメッセージが、単一のＤＳＴまたはＤＳＴライクなメッセージを伝達するためのコンテナとして機能する要素すなわちコンテナ要素を含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記ＳＡＭＬ　ＤＳＴメッセージが、ＳＡＭＬ　ＤＳＴ要求メッセージまたはＳＡＭＬ　ＤＳＴ応答メッセージを含むことを特徴とする請求項１または２に記載の方法。
【請求項４】
前記ＳＡＭＬ　ＤＳＴ要求メッセージが、ＳＡＭＬ　ＤＳＴ応答メッセージに含まれるＤＳＴまたはＤＳＴライクな応答によって応答されるＤＳＴまたはＤＳＴライクな要求を含むことを特徴とする請求項３に記載の方法。
【請求項５】
前記ＳＡＭＬ　ＤＳＴ要求メッセージが、前記ＳＡＭＬ　ＤＳＴ要求メッセージに含まれるＤＳＴまたはＤＳＴライクなメッセージで指定されるＤＳＴ処理の対象となるデータを有するユーザまたはエンティティを識別するためのサブジェクトフィールドとして機能する要素を含むことを特徴とする請求項３または４に記載の方法。
【請求項６】
前記ＳＡＭＬ　ＤＳＴ要求メッセージが、前記ＳＡＭＬ　ＤＳＴ要求メッセージの発信者を識別するための発行者フィールドとして機能する要素を含むことを特徴とする請求項３ないし５のいずれか１項に記載の方法。
【請求項７】
前記ＳＡＭＬ　ＤＳＴ要求メッセージが、前記ＳＡＭＬ　ＤＳＴ要求メッセージを特定の宛先、特に特定のデータサービスへ送信するための受信者フィールドとして機能する要素を含むことを特徴とする請求項３ないし６のいずれか１項に記載の方法。
【請求項８】
前記ＳＡＭＬ　ＤＳＴ要求メッセージのそれぞれが、前記ＤＳＴまたはＤＳＴライクな要求を構成する１つのコンテナ要素を含むことを特徴とする請求項４ないし７のいずれか１項に記載の方法。
【請求項９】
前記ＤＳＴまたはＤＳＴライクな要求が、前記分散データの作成、変更、削除または問合せに関するデータ処理情報を伝達することを特徴とする請求項４ないし７のいずれか１項に記載の方法。
【請求項１０】
前記作成および／または削除処理に関する前記ＤＳＴまたはＤＳＴライクな要求のセマンティクスは、前記要求の効果が、データレコード内のデータの作成および／または削除のみに限定されるように構成されることを特徴とする請求項４ないし９のいずれか１項に記載の方法。
【請求項１１】
前記ＤＳＴまたはＤＳＴライクな要求のそれぞれがselect文を含み、該select文は、前

記分散データのどの部分が処理されるべきかを指示するＸＰＡＴＨ式を含むことを特徴とする請求項４ないし１０のいずれか１項に記載の方法。
【請求項１２】
前記ＸＰＡＴＨ式が、前記ＤＳＴまたはＤＳＴライクな要求の予想される受信者に渡されることを特徴とする請求項１１に記載の方法。
【請求項１３】
前記ＤＳＴまたはＤＳＴライクな要求で定義され、前記プロトコル固有の名前空間の１つではない名前空間が、前記分散データの要素を参照するための前記ＸＰＡＴＨ式内で使用されることを特徴とする請求項１１または１２に記載の方法。
【請求項１４】
前記ＳＡＭＬ　ＤＳＴ応答メッセージが、前記ＳＡＭＬ　ＤＳＴ応答メッセージのステータスを示すステータスフィールドとして機能する要素を含むことを特徴とする請求項３ないし１３のいずれか１項に記載の方法。
【請求項１５】
前記ＳＡＭＬ　ＤＳＴ応答メッセージが、再試行要求内で使用されるサブジェクト名に関する情報を保持するための再試行サブジェクトフィールドとして機能する要素を含むことを特徴とする請求項３ないし１４のいずれか１項に記載の方法。
【請求項１６】
前記ＳＡＭＬ　ＤＳＴ応答メッセージのそれぞれが、前記ＤＳＴまたはＤＳＴライクな応答を含む１つ以上のコンテナ要素を含むことを特徴とする請求項４ないし１５のいずれか１項に記載の方法。
【請求項１７】
前記ＳＡＭＬ　ＤＳＴ応答メッセージに含まれる前記１つ以上のコンテナ要素が、ＤＳＴまたはＤＳＴライクな応答の発行者を参照するために使用される識別子を含むことを特徴とする請求項１６に記載の方法。
【請求項１８】
前記ＳＡＭＬ　ＤＳＴメッセージが、前記ＳＡＭＬ　ＤＳＴメッセージに署名した結果を含む署名要素を含むことを特徴とする請求項１ないし１７のいずれか１項に記載の方法。
【請求項１９】
前記ＳＡＭＬ　ＤＳＴメッセージが、前記ユーザまたは前記エンティティの前記分散データを管理するために、要求側とサービス提供側のサービスプロバイダ間で交換されることを特徴とする請求項１ないし１８のいずれか１項に記載の方法。
【請求項２０】
アイデンティティプロバイダが、要求側とサービス提供側のサービスプロバイダ間での前記ＳＡＭＬ　ＤＳＴメッセージの交換に関与することを特徴とする請求項１ないし１９のいずれか１項に記載の方法。
【請求項２１】
前記ユーザまたは前記エンティティが、仮名識別子によってサービスプロバイダにアクセスし、前記アイデンティティプロバイダが、前記仮名識別子を解決するため、および／またはそれをローカルユーザアカウントにマッピングするために、サービスプロバイダによって使用されることを特徴とする請求項２０に記載の方法。
【請求項２２】
要求側サービスプロバイダが、前記ユーザまたは前記エンティティの前記仮名識別子をサブジェクトとして含むとともにＤＳＴまたはＤＳＴライクなメッセージを含むＳＡＭＬ　ＤＳＴ要求メッセージを前記アイデンティティプロバイダへ送信することを特徴とする請求項２０または２１に記載の方法。
【請求項２３】
前記アイデンティティプロバイダが、前記要求側および前記サービス提供側の両方のサービスプロバイダにおいて有効な一時的仮名識別子を作成することを特徴とする請求項２

０ないし２２のいずれか１項に記載の方法。
【請求項２４】
前記アイデンティティプロバイダが、前記一時的仮名識別子を示すＳＡＭＬ　ＤＳＴ再試行メッセージによって、前記要求側サービスプロバイダに応答することを特徴とする請求項２３に記載の方法。
【請求項２５】
前記アイデンティティプロバイダが、前記ＳＡＭＬ　ＤＳＴメッセージ内の前記一時的仮名識別子の代わりに前記仮名識別子を使用することを特徴とする請求項２３または２４に記載の方法。
【請求項２６】
前記要求側サービスプロバイダが、前記一時的仮名をサブジェクトとして含むとともに前記ＤＳＴまたはＤＳＴライクなメッセージを含む新しいＳＡＭＬ　ＤＳＴ要求メッセージを前記アイデンティティプロバイダへ送信することを特徴とする請求項２３ないし２５のいずれか１項に記載の方法。
【請求項２７】
前記アイデンティティプロバイダが、前記ＤＳＴまたはＤＳＴライクな要求で指定される前記分散データ、特にユーザプロファイル情報データの型に影響を及ぼす前記ＤＳＴまたはＤＳＴライクな要求にサービス提供できるのはどのサービスプロバイダであるかを検索し、前記ＳＡＭＬ　ＤＳＴ要求メッセージを該サービス提供側サービスプロバイダへ転送することを特徴とする請求項２０ないし２６のいずれか１項に記載の方法。
【請求項２８】
前記サービス提供側サービスプロバイダが、ＳＡＭＬ　ＤＳＴ応答メッセージによって前記アイデンティティプロバイダに応答し、前記アイデンティティプロバイダが、前記サービス提供側サービスプロバイダの前記ＳＡＭＬ　ＤＳＴ応答メッセージに含まれる前記ＤＳＴまたはＤＳＴライクな応答を集積し、該集積されたＤＳＴまたはＤＳＴライクな応答を含むＳＡＭＬ　ＤＳＴ応答メッセージを前記要求側サービスプロバイダに返すことを特徴とする請求項２０ないし２７のいずれか１項に記載の方法。
【請求項２９】
前記アイデンティティプロバイダは、要求側サービスプロバイダがサービス提供側サービスプロバイダを発見するための発見サーバとして使用され、
前記アイデンティティプロバイダが、前記要求側サービスプロバイダから送信されたＳＡＭＬ　ＤＳＴ要求メッセージの署名をチェックし、
前記アイデンティティプロバイダが、前記ＤＳＴまたはＤＳＴライクな要求で指定される前記分散データ、特にユーザプロファイル情報データの型に影響を及ぼす前記ＤＳＴまたはＤＳＴライクな要求にサービス提供できるのはどのサービスプロバイダであるかを検索し、
前記アイデンティティプロバイダが、一時的仮名識別子を作成し、
前記アイデンティティプロバイダが、前記一時的仮名の代わりに前記ＳＡＭＬ　ＤＳＴ要求メッセージすなわち変更された要求内のサブジェクトを使用し、
前記アイデンティティプロバイダが、前記変更された要求に署名し、
前記アイデンティティプロバイダが、前記変更された要求および前記検索したサービス提供側サービスプロバイダのUniform Resource Identifierを含むＳＡＭＬ　ＤＳＴ応答メッセージを前記要求側サービスプロバイダへ送信する
ことを特徴とする請求項２０ないし２８のいずれか１項に記載の方法。
【請求項３０】
前記要求側サービスプロバイダが、前記変更された要求に再署名し、該再署名した変更された要求を、前記検索したサービス提供側サービスプロバイダへ送信することを特徴とする請求項２９に記載の方法。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、ユーザまたはエンティティの分散データ、特にユーザプロファイル情報データの管理および交換をサポートする方法に関する。
【背景技術】
【０００２】
現在および将来のインターネット上で利用可能なサービスが増大し、各サービスがユーザプロファイルデータのアカウント作成、認証および保存を必要とするのに伴い、ユーザは、自己のプロファイルがさまざまなサービスプロバイダ、例えば銀行、書店、あるいはYouTubeやFacebookのようなコミュニティサービスにわたって分散するという事実に直面している。
【０００３】
アイデンティティ管理（Identity Management，ＩｄＭ）の目標は、シングルサインオン（single sign on，ＳＳＯ）を実現するとともに、サービスプロバイダ（Service Provider，ＳＰ）とアイデンティティプロバイダ（Identity Provider，ＩｄＰ）との間でセキュアでプライバシーに配慮した形でユーザ（プロファイル）情報を交換することである。ユーザの情報は、アイデンティティプロバイダによって保存されることも、またはいわゆる属性機関（Attribute Authority）に保存されることも可能である。属性機関は、アイデンティティプロバイダからユーザデータに関する問合せを受け、そのデータを要求側ＳＰに渡すことができる。
【０００４】
また、ほとんどのサービスプロバイダは現在、サービス定義の一部であるプロファイルデータを独自フォーマットで保存している。独自フォーマットでは、各データフィールドが、独自の名称と、関連するセマンティクスとを有する。すなわち、たとえアイデンティティ管理がさまざまな属性機関から分散データを読み出す手段を提供しても、データ識別子および／またはセマンティクスをサービスプロバイダドメイン間でマッピングする必要が常に存在するということである。これは面倒で、しばしば不可能であり、もしこれが行われなければ、プロファイルデータ利用者と、それを提供する機関との間が強く結びついてしまう。
【０００５】
アイデンティティ管理ソリューションを利用したいユーザは、自己の分散したプロファイルデータを制御したいと考え、それを簡便に管理する手段を必要とするであろう。これは、変更および問合せだけでなく、アクセス制御ポリシーによる保護と、どの個人データがどこに保存されるかに関する明確な全体像を有する能力をも含むであろう。
【０００６】
さらに、ユーザが分散したプロファイルおよびデータを管理することに関心を有するだけでなく、ＳＰもまた、このような操作を含むサービスを提供することに関心を有するであろう。しかし同時に、ユーザプロファイルデータを提供するＳＰは、それに対する制御を放棄したくはないであろう。このため、次のようなソリューションが必要となる。すなわち、ＳＰが、要求者を確認／アサートし、データを渡す前または操作を許可する前に自己のアクセス制御を施行することを可能にするソリューションである。
【０００７】
最後に、分散したユーザプロファイルの管理をサポートするインフラストラクチャは、さまざまなサービスプロバイダドメインのユーザ識別子間のマッピングを提供することにより、あるＳＰのドメインで識別され特定のプロファイルにリンクされるユーザが、別のＳＰのドメインで（おそらくは）別の名称によって識別されることができることを保証しなければならない。これは、今日のアイデンティティ管理ソリューションの本質的部分となる性質であり、プライバシー保護の基礎のひとつである。
【０００８】
ＳＡＭＬ２．０は、ＯＡＳＩＳコンソーシアムによって策定されたＸＭＬベースのマークアップ言語である。これは、相異なるセキュリティドメインにわたるシングルサインオ

ン、分散トランザクション、およびアサーションベースの認可をサポートする。いくつかのプロトコルバインディングが定義されており、これによりＳＡＭＬは、単純なＨＴＴＰサービスとともに、例えばＳＯＡＰ（Simple Object Access Protocol）やＳＩＰ（Session Initiation Protocol）上のウェブサービスでも使用可能となる。

【０００９】

ＳＳＯに対するＳＡＭＬの使用を３ＧＰＰのＩＰマルチメディアサブシステム（IP Multimedia Subsystem, ＩＭＳ）と組み合わせることが、非特許文献１で提案された。さらに、リバティアライアンス（Liberty Alliance）は、ＩｄＭソリューションとしてＳＡＭＬを採用した。このように、ＳＡＭＬは、エンタープライズ環境においてＩｄＭ関連情報を交換するためのデファクト標準となっている。

【００１０】

ＳＡＭＬは、いくつかの要求および応答の型を定義している。例えば、アイデンティティ属性を問い合わせるためのものや、要求者および応答者に関するアサーションを交換するためのものがある。また、ＳＡＭＬメッセージは、仮想ユーザアイデンティティの識別子を伝達することができる。本明細書においては、それらの識別子を仮名（pseudonym）と称する。というのは、それらはユーザの実際のアイデンティティを隠蔽するために使用可能だからである。なお、注意すべき重要な点であるが、仮名はドメイン固有とすることができる。すなわち、同一ユーザが、異なるサービスプロバイダドメインでは異なる仮名によって識別されることが可能である。

【００１１】

ＳＡＭＬは、読み出し専用アクセスのためのものであり、ユーザにも、アイデンティティプロバイダやＳＰにも、いかなる形でもプロファイル情報の管理すなわち書き込みや変更を許可しない。

【００１２】

もう１つの可能なメッセージフォーマットとして、リバティアライアンスのデータサービステンプレート（Data Services Template, ＤＳＴ）があり、非特許文献２で規定されている。ＤＳＴは、プロファイルデータの管理（作成、削除、変更および問合せ）のための情報を伝達するＸＭＬベースのメッセージの構造体を定義したプロトコルテンプレートの仕様である。ＤＳＴは、プロファイルデータがＸＭＬ構造体でアクセス可能であることを仮定しており、ＸＰＡＴＨ式を用いて、処理対象のプロファイルデータのノードを選択する。

【００１３】

その名称が示唆するように、ＤＳＴはプロトコルではなくプロトコルメッセージのテンプレートである。仕様に記載されているように、そのテンプレートは、各データサービスによって個別に実装されることになっている。実装は、ＤＳＴで管理されるべきプロトコルメッセージおよびデータの両方に対する、データサービスに依存した名前空間の定義を含む。しかし、このため、ＤＳＴは、それを実装するプロファイルデータサービスに完全に依存することになる。これは、ＤＳＴのクライアントとサーバとを統合するものでもなく、分離もできなくなる。実際、ＤＳＴは、プロトコルテンプレートのインスタンスをデータサービスにバインドする。

【００１４】

現在、セキュアでプライバシーに配慮した形で、分散したプロファイルデータの管理および変更を行う手段は存在しない。すなわち、ユーザは、個別のサービスにアクセスして、自己のプロファイル情報の一部を更新しなければならない。

【先行技術文献】

【非特許文献】

【００１５】

【非特許文献１】"Identity Management for IMS-based IPTV", IEEE Globecom 2008

【非特許文献２】https://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_data_services_template_v2_0_specifications

【発明の概要】
【発明が解決しようとする課題】
【００１６】
したがって、本発明の目的は、頭書のようなユーザまたはエンティティの分散データ、特にユーザプロファイル情報データの管理および交換をサポートする方法において、実施の容易なメカニズムを使用することにより、ユーザまたはエンティティが、セキュアでプライバシーに配慮した形で、自己の分散データの管理および／または変更が可能となるような改良およびさらなる展開を行うことである。
【課題を解決するための手段】
【００１７】
本発明によれば、上記の目的は、請求項１の構成を備えた方法によって達成される。この請求項に記載の通り、本方法は、以下のことを特徴とする。すなわち、ＳＡＭＬ（Security Assertion Markup Language）をベアラプロトコルとして使用するプロトコルが次のように提供される。ＳＡＭＬメッセージは、ＳＡＭＬ　ＤＳＴメッセージを作成するために、ＤＳＴ（Data Services Template）またはＤＳＴライクなメッセージのためのコンテナとして機能する。前記ＤＳＴまたはＤＳＴライクなメッセージはデータ処理情報を含む。前記ＤＳＴまたはＤＳＴライクなメッセージに対して、統一されたプロトコル名前空間が、プロトコル固有の名前空間として定義される。
【００１８】
本発明によって初めて認識されたこととして、セキュアでプライバシーおよびアイデンティティに配慮した形で、分散したユーザデータの管理および交換を提供する場合、ＳＡＭＬとＤＳＴを特定の方法で組み合わせることにより、顕著な改善を達成することができる。ＳＡＭＬとＤＳＴの組合せは、次のようにして、ＳＡＭＬをベアラプロトコルとして使用するプロトコルを提供することによって実現される。すなわち、ＳＡＭＬメッセージは、ＳＡＭＬ　ＤＳＴメッセージを作成するために、ＤＳＴまたはＤＳＴライクなメッセージのためのコンテナとして機能する。ＤＳＴまたはＤＳＴライクなメッセージは、ユーザまたはエンティティの分散データを管理するためのデータ処理情報を含む。また、認識されたこととして、提供されるプロトコルは、ＤＳＴまたはＤＳＴライクなメッセージに対して、統一されたプロトコル名前空間をプロトコル固有の名前空間として定義することによって、管理されるデータから独立とすることができる。このため、これらの名前空間は、プロトコルメッセージ自体にバインドされ、改変すなわち変更および／または管理される実際の分散データの要素を参照するために使用されるようなＤＳＴメッセージ内の他の名前空間宣言から区別される。こうして、本発明による方法は、セキュアでプライバシーに配慮した形でユーザまたはエンティティによる分散データの管理および変更を可能にする。
【００１９】
好ましい実施形態によれば、ＳＡＭＬ　ＤＳＴメッセージは、単一のＤＳＴまたはＤＳＴライクなメッセージを伝達するためのコンテナとして機能する要素（コンテナ要素）を含んでもよい。これにより、既存の抽象ＳＡＭＬメッセージ型から派生し、ＳＡＭＬのすべての特徴を継承するが、さらにＤＳＴまたはＤＳＴライクなメッセージのためのコンテナとして作用することができる新しいＳＡＭＬメッセージ型を定義することが可能となる。なお、既存のＳＡＭＬメッセージも、ＤＳＴまたはＤＳＴライクなメッセージのためのコンテナとして機能するベアラプロトコルとして再利用可能である。
【００２０】
好ましい実施形態によれば、ＳＡＭＬ　ＤＳＴメッセージは、ＳＡＭＬ　ＤＳＴ要求メッセージまたはＳＡＭＬ　ＤＳＴ応答メッセージを含んでもよい。
【００２１】
有利な態様として、ＳＡＭＬ　ＤＳＴ要求メッセージは、ＳＡＭＬ　ＤＳＴ応答メッセージに含まれるＤＳＴまたはＤＳＴライクな応答によって応答されるＤＳＴまたはＤＳＴライクな要求を含んでもよい。

【００２２】
好ましい実施形態によれば、ＳＡＭＬ　ＤＳＴ要求メッセージは、ＳＡＭＬ　ＤＳＴ要求メッセージに含まれるＤＳＴまたはＤＳＴライクなメッセージで指定されるＤＳＴ処理の対象となるデータを有するユーザまたはエンティティを識別するためのサブジェクト（subject）フィールドとして機能する要素を含む。これにより、サブジェクトフィールドは、ユーザを識別するために使用されることが可能である。例えばアイデンティティプロバイダ経由でユーザに関する情報を取得しようとしてＤＳＴを使用する要求側サービスは、どのユーザに対する情報をフェッチしようとしているかをアイデンティティプロバイダに対して指定するためにサブジェクトフィールドを使用してもよい。このサブジェクト識別子は、要求側サービスにおいて使用される仮名であることも可能である。

【００２３】
有利な態様として、ＳＡＭＬ　ＤＳＴ要求メッセージは、ＳＡＭＬ　ＤＳＴ要求メッセージの発信者を識別するための発行者（issuer）フィールドとして機能する要素を含んでもよい。

【００２４】
また、ＳＡＭＬ　ＤＳＴ要求メッセージは、ＳＡＭＬ　ＤＳＴ要求メッセージを特定の宛先、特に特定のデータサービスへ送信するための受信者（recipient）フィールドとして機能する要素を含んでもよい。例えば、受信者フィールドは、受信者サービスプロバイダＩＤのために使用されてもよい。このＩＤは、エンドポイントＵＲＬ（Uniform Resource Locator）であることも、アイデンティティプロバイダによって解決可能なサービスプロバイダ仮名であることも可能である。

【００２５】
各ＳＡＭＬ　ＤＳＴ要求メッセージは、ＤＳＴまたはＤＳＴライクな要求を構成するただ１つのコンテナ要素を含んでもよい。

【００２６】
ＤＳＴ処理に関して、ＤＳＴまたはＤＳＴライクな要求は、分散データの作成、変更、削除または問合せに関する、特にＸＭＬベースのデータ処理情報を伝達してもよい。ＤＳＴ処理の型は、特定のメッセージフィールドとしては与えられない。この型は、ＤＳＴ仕様によって定義されるRequestTypeから推論することができる。これは、ModifyRequest、CreateRequest、DeleteRequestまたはQueryRequestのいずれかであってもよい。

【００２７】
有利な態様として、作成および／または削除処理に関するＤＳＴまたはＤＳＴライクな要求のセマンティクスは、要求の効果が、ユーザまたはエンティティの分散データのデータレコード内、例えばユーザプロファイル内のデータの作成および／または削除のみに限定されるように構成される。

【００２８】
各ＤＳＴまたはＤＳＴライクな要求は、select文を含んでもよい。select文は、分散データのどの部分が処理されるべきかを指示するＸＰＡＴＨ式を含む。

【００２９】
ＸＰＡＴＨ式は、ＤＳＴまたはＤＳＴライクな要求の予想される受信者、特に、ＸＰＡＴＨ式（例えばＸＰＡＴＨ問合せ）に基づいて情報を返すことになっているデータサービスに渡されてもよい。

【００３０】
有利な態様として、ＤＳＴまたはＤＳＴライクな要求で定義され、プロトコル固有の名前空間の１つではない名前空間が、分散データの要素を参照するためのＸＰＡＴＨ式内で使用されるようにしてもよい。この名前空間は、アイデンティティプロバイダによって、どの種類の情報がユーザに対して要求されようとしているか、および、どのサービスプロバイダに連絡をとるべきかを区別するために使用されてもよい。例えば、アイデンティティプロバイダは、プロファイルデータサービスの名前空間から、このサービスが提供するプロファイルデータ（すなわち型）の名前空間へのマッピングを保持してもよい。このマ

ッピングは、各ユーザごとに保持してもよい。

【００３１】

また、ＳＡＭＬ　ＤＳＴ応答メッセージは、ＳＡＭＬ　ＤＳＴ応答メッセージのステータスを示すステータスフィールドとして機能する要素を含んでもよい。

【００３２】

有利な態様として、ＳＡＭＬ　ＤＳＴ応答メッセージは、再試行要求内で使用されるサブジェクト名に関する情報を保持するための再試行（retry）サブジェクトフィールドとして機能する要素を含んでもよい。これは、サブジェクト識別子がアイデンティティプロバイダによって、ドメイン間でアドホックな形でマッピングされる場合に必要とされる。

【００３３】

各ＳＡＭＬ　ＤＳＴ応答メッセージは、ＤＳＴまたはＤＳＴライクな応答を含む１つ以上のコンテナ要素を含んでもよい。ＳＡＭＬ　ＤＳＴ応答内に複数のコンテナ要素を含む必要がある場合として、アイデンティティプロバイダが複数のＤＳＴまたはＤＳＴライクな応答を単一のＳＡＭＬ　ＤＳＴ応答内に集積することができるという潜在的要件によるものが挙げられる。

【００３４】

ＳＡＭＬ　ＤＳＴ応答メッセージに含まれる１つ以上のコンテナ要素は、ＤＳＴ応答の発行者を参照するために使用される識別子を含んでもよい。この識別子は、例えば、不成功の応答または期待されない応答の場合に、特定のサービス提供側サービスプロバイダと連絡をとるために、要求側サービスプロバイダによって使用されることが可能である。特定のＤＳＴ応答が失敗を示す場合、要求側クライアントは、ＤＳＴメッセージが失敗した当該サービスプロバイダのみに別の要求を送信することができる。この識別子はさらに、どのサービスプロバイダがどのように（例えば、分散ユーザプロファイル管理ユーザインタフェースにおいて）応答したかをユーザに示すために使用可能である。

【００３５】

有利な態様として、ＳＡＭＬ　ＤＳＴメッセージは、ＳＡＭＬ　ＤＳＴメッセージに署名した結果を含む署名（signature）要素を含んでもよい。

【００３６】

ＳＡＭＬ　ＤＳＴメッセージは、ユーザまたはエンティティの分散データを管理するために、要求側とサービス提供側のサービスプロバイダ間で交換されてもよい。

【００３７】

また、アイデンティティプロバイダが、要求側とサービス提供側のサービスプロバイダ間でのＳＡＭＬ　ＤＳＴメッセージの交換に関与してもよい。

【００３８】

有利な態様として、ユーザまたはエンティティは、仮名識別子によってサービスプロバイダにアクセスしてもよい。この場合、アイデンティティプロバイダは、仮名識別子を解決するため、および／またはそれをローカルユーザアカウントにマッピングするために、サービスプロバイダによって使用される。

【００３９】

要求側サービスプロバイダは、ユーザまたはエンティティの仮名識別子をサブジェクトとして含むとともにＤＳＴまたはＤＳＴライクなメッセージを含むＳＡＭＬ　ＤＳＴ要求メッセージをアイデンティティプロバイダへ送信してもよい。

【００４０】

さらに、アイデンティティプロバイダは、要求側およびサービス提供側の両方のサービスプロバイダにおいて有効な一時的仮名識別子を作成してもよい。

【００４１】

有利な態様として、アイデンティティプロバイダは、一時的仮名識別子を示すＳＡＭＬ　ＤＳＴ再試行メッセージによって、要求側サービスプロバイダに応答してもよい。

【００４２】

これに加えて、または別法として、アイデンティティプロバイダは、ＳＡＭＬ　ＤＳＴ

メッセージ内の一時的仮名識別子の代わりに仮名識別子を使用してもよい。

【００４３】

要求側サービスプロバイダは、一時的仮名をサブジェクトとして含むとともにＤＳＴまたはＤＳＴライクなメッセージを含む新しいＳＡＭＬ　ＤＳＴ要求メッセージをアイデンティティプロバイダへ送信してもよい。

【００４４】

有利な態様として、アイデンティティプロバイダは、ＤＳＴまたはＤＳＴライクな要求で指定される分散データ、特にユーザプロファイル情報データの型に影響を及ぼすＤＳＴまたはＤＳＴライクな要求にサービス提供できるのはどのサービスプロバイダであるかを検索し、ＳＡＭＬ　ＤＳＴ要求メッセージをそのサービス提供側サービスプロバイダへ転送してもよい。

【００４５】

サービス提供側サービスプロバイダは、ＳＡＭＬ　ＤＳＴ応答メッセージによってアイデンティティプロバイダに応答してもよい。この場合、アイデンティティプロバイダは、サービス提供側サービスプロバイダのＳＡＭＬ　ＤＳＴ応答メッセージに含まれるＤＳＴまたはＤＳＴライクな応答を集積し、集積されたＤＳＴまたはＤＳＴライクな応答を含むＳＡＭＬ　ＤＳＴ応答メッセージを要求側サービスプロバイダに返す。

【００４６】

好ましい実施形態において、アイデンティティプロバイダは、要求側サービスプロバイダがサービス提供側サービスプロバイダを発見するための発見サーバとして使用されてもよい。アイデンティティプロバイダは、要求側サービスプロバイダから送信されたＳＡＭＬ　ＤＳＴ要求メッセージの署名をチェックしてもよい。その後、アイデンティティプロバイダは、ＤＳＴまたはＤＳＴライクな要求で指定される分散データ、特にユーザプロファイル情報データの型に影響を及ぼすＤＳＴまたはＤＳＴライクな要求にサービス提供できるのはどのサービスプロバイダであるかを検索してもよい。アイデンティティプロバイダは、一時的仮名識別子を作成し、一時的仮名の代わりにＳＡＭＬ　ＤＳＴ要求メッセージ（変更された要求）内のサブジェクトを使用してもよい。最後に、アイデンティティプロバイダは、変更された要求に署名し、変更された要求および検索したサービス提供側サービスプロバイダのUniform Resource Identifierを含むＳＡＭＬ　ＤＳＴ応答メッセージを要求側サービスプロバイダへ送信する。

【００４７】

有利な態様として、要求側サービスプロバイダは、変更された要求に再署名し、再署名した変更された要求を、検索したサービス提供側サービスプロバイダへ送信してもよい。

【００４８】

本発明を好ましい態様で実施するにはいくつもの可能性がある。このためには、一方で請求項１に従属する諸請求項を参照しつつ、他方で図面により例示された本発明の好ましい実施形態についての以下の説明を参照されたい。図面を用いて本発明の好ましい実施形態を説明する際には、本発明の教示による好ましい実施形態一般およびその変形例について説明する。

【図面の簡単な説明】

【００４９】

【図１】本発明による方法の適用場面の一例を示す模式的なＳＡＭＬ　ＤＳＴインフラストラクチャの概略図である。

【図２】本発明の一実施形態によるＳＡＭＬ　ＤＳＴ要求メッセージを例示する模式図である。

【図３】本発明の一実施形態によるＳＡＭＬ　ＤＳＴ応答メッセージを例示する模式図である。

【図４】ＳＡＭＬ　ＤＳＴプロキシとしてアイデンティティプロバイダが作用する場合のメッセージフローを例示するシーケンス図である。

【図５】可能なサービス提供側サービスプロバイダを要求側サービスプロバイダが発見す

るための発見サーバとしてアイデンティティプロバイダが作用する場合のメッセージフローを例示するシーケンス図である。

【発明を実施するための形態】

【００５０】

図１は、分散したユーザプロファイルおよびＩｄＭ関連データの管理を可能にするために、本発明による方法に対して想定されるインフラストラクチャおよびコンポーネントの概略を示している。ユーザは、ＩｄＭにおいて一般的であるように、与えられた仮名によってサービスプロバイダにアクセスする。アイデンティティプロバイダを利用して、仮名は、例えばシングルサインオンを提供するために、ＳＰによって解決され、ローカルユーザアカウントにマッピングされることが可能である。サービスプロバイダが、ローカルに利用可能でないユーザのプロファイル情報に対するアクセスおよび／または操作を必要とするときには、サービスプロバイダは、アイデンティティプロバイダの拡張ポイントへＳＡＭＬ　ＤＳＴ要求を送信する。ＳＡＭＬ　ＤＳＴ要求は、サービスプロバイダ自身を要求の発行者として含み、ユーザの仮名をメッセージのサブジェクトとして含むとともに、どの種類のプロファイルデータが影響を受けるかの指示を含む。

【００５１】

アイデンティティプロバイダは、ＳＡＭＬ　ＤＳＴプロキシとして作用するが、与えられたユーザに対する要求された種類のプロファイル情報を扱うＳＰを識別すること、および、要求側ＳＰにおけるユーザの仮名とサービス提供側ＳＰにおいて使用されるユーザ識別子との間のマッピングを作成することを担当する。これを実行した後、アイデンティティプロバイダは、ユーザに対する要求にサービス提供可能なすべてのＳＰへ要求を転送する。ユーザのプロファイル情報を保有するサービス提供側ＳＰは、アイデンティティプロバイダの署名およびアサーションを含む要求の有効性をチェックした後、ＳＡＭＬメッセージ内で送信されたＤＳＴ要求を処理することができる。

【００５２】

要求の処理は、各個別ＳＰに独自なアクセスおよびセキュリティポリシーの施行を含むことができる。これは、プロファイルデータの操作および提供が許可されることを保証するためである。処理後、各サービス提供側ＳＰは、どのＳＰがどの応答を送信しているかに関する情報を含む結果を単一のＳＡＭＬ　ＤＳＴ応答内に集積したＳＡＭＬ　ＤＳＴ応答をアイデンティティプロバイダへ返送する。そして、集積された応答は、要求側ＳＰへ返送される。

【００５３】

図１の適用場面に記載されているようなインフラストラクチャを提供するため、ＤＳＴが変更される。ＤＳＴの変更については以下でさらに詳細に説明するが、ＤＳＴを変更したものをＤＳＴライクなメッセージと称する。なお、一般的に、ＤＳＴはテンプレートであって、プロトコルではなく、通常は、名前空間によって、ＤＳＴをインタフェースとして提供するデータサービスにバインドされる。ＤＳＴの実装は、３つの名前空間の定義を必要とする。すなわち、ユーティリティＸＭＬ要素に対する名前空間、ＸＭＬ　ＤＳＴベースメッセージに対する名前空間、およびＤＳＴ参照実装スキーマに対する名前空間である。

【００５４】

独自の、したがってバインドしている名前空間の限界を克服するため、統一されたプロトコル名前空間がＤＳＴメッセージに対して次のように定義される。

１）urn:eu:neclab:nw:util:2009-02　ユーティリティ要素に対して

２）urn:eu:neclab:nw:dst:2009-02　ＤＳＴベースメッセージに対して

３）urn:eu:neclab:nw:dst:2009-02:ref　ＤＳＴ参照実装スキーマに対して

【００５５】

これらをプロトコル固有の名前空間として定義することにより、これらを他の名前空間宣言から区別することが可能となり、それらの宣言は、ＤＳＴ処理の対象となる種々のプロファイルデータ型を示すために使用可能となる。

【００５６】

```
<ns3:Query xmlns:ns1="urn:eu:neclab:nw:util:2009-02"
    xmlns:ns2="urn:eu:neclab:nw:dst:2009-02"
    xmlns:ns3="urn:eu:neclab:nw:dst:2009-02:ref"
    xmlns:bp="urn:banking:profile:service">
  <ns3:QueryItem>
    <ns3:Select>/bp:Banking/bp:Accounts</ns3:Select>
  </ns3:QueryItem>
</ns3:Query>
```

【００５７】

例えば、上記のＸＭＬサンプルは、ユーザのすべての銀行口座を取得する単純なＤＳＴ問合せ要求を示している。なお、Select文は、名前空間を用いたＸＰＡＴＨ問合せを含むが、この名前空間は、プロトコル名前空間ではなく、問合せ対象のユーザプロファイルの型を示すために追加的に定義された名前空間であることに注意すべきである。元のＤＳＴでは、これは予測されていない。上記のサンプルにおける名前空間urn:banking:profile:serviceは、スキーマ定義されたbankingプロファイルを参照している。リバティアライアンスによってすでに開始されているように、例えばバンキングデータ、個人プロファイルデータ等に対して、明確に定義された要素名および定義されたデータセマンティクスを有する、より標準化されたプロファイルスキーマが存在するであろうと仮定される。それらの各プロファイル型は、明確に定義され、与えられた構造に従い、どのデータがその仕様のプロファイル内に含まれるかを指定するであろう。これにより、定義されたセマンティクスで、標準化された方法により、特定の種類の情報を取得することが可能となる。本発明による方法は、操作され得るプロファイルの型とは独立であるので、ＳＰ間の広範な相互運用性を可能にする。

【００５８】

また、ＤＳＴのCreate（作成）およびDelete（削除）メッセージのセマンティクスが若干変更される。リバティアライアンスのData Services Template仕様では、CreateおよびDeleteメッセージは、データレコード全体、すなわち本発明による用語法では、プロファイルまたはアカウント全体の作成および削除のために使用される。プロファイル内のデータの作成または削除のためには、Modify（変更）要求が使用される。それらのセマンティクスは、CreateおよびDeleteメッセージの効果を特定のプロファイル内のデータの作成および削除のみに制限することによって変更される。これが行われる理由は、ＳＰはプロファイル／アカウント全体の作成および削除を完全に制御すべきであり、それによってプロトコルをより容易かつ簡明にするためである。セマンティクスにおけるこの改変は、CreateメッセージにSelect文を追加することにより、ＸＰＡＴＨ式で、プロファイル内のどこに新しいデータが作成されるべきかを示すことを必要とする。

【００５９】

プロファイルデータ、あるいはＤＳＴにおける呼称でデータサービスは、ＸＭＬ構造体として表現されることになっている。これは、ＤＳＴ処理のためのデータはＸＭＬ構造化データに限られるという意味ではなく、本発明による方法によって処理されるべきどのデータに対しても、それがＸＭＬ構造化されているかのようにデータを公開する抽象化レイヤが存在しなければならない、という意味である。

【００６０】

ＤＳＴメッセージは、要求によって影響を受けるプロファイルデータを有するユーザ（サブジェクト）を知らない。また、ＤＳＴメッセージは、要求者をアサートしたり、メッセージの完全性を検証したりするために使用可能ないかなる情報も伝達しない。最後に、ＤＳＴメッセージ内には、アイデンティティ管理を提供する手段は存在しない。その機能は、ベアラプロトコル、すなわち、ＤＳＴメッセージを伝達するプロトコルによって提供されなければならない。ＳＡＭＬ２．０は、エンタープライズＩｄＭソリューションに対するデファクト標準である。ＳＡＭＬ２．０は、よく理解されたプロトコルであり、すで

に広く使用されている。既存の技術に影響を及ぼさないために、新しい要求および応答の型を定義することによってＳＡＭＬプロトコルを拡張することが選択される。

【００６１】

図２は、本発明の一実施形態によるＳＡＭＬ　ＤＳＴ要求メッセージを例示する模式図である。例示したＳＡＭＬ　ＤＳＴ要求は、ＳＡＭＬのSubjectQueryAbstractTypeから派生された新しい型である。既存の要求型から派生することによって、アイデンティティ管理に必要とされるＳＡＭＬメッセージの利益およびプロパティ、例えばメッセージ署名、セキュリティ、サブジェクト等が保持されることが保証される。これにより、ＳＡＭＬ　ＤＳＴ要求は、ユーザを識別するサブジェクトフィールド、要求の発信者を識別するために使用可能な発行者フィールド、およびメッセージ署名の結果を含む署名要素を含む。

【００６２】

図２に例示したように、ＤＳＴ要求を含む新しい要素が追加的に定義される。ＳＡＭＬ　ＤＳＴを用いて、要求側ＳＰは、どのユーザプロファイル（サブジェクトによって与えられる）がＳＡＭＬメッセージ内で送信されるＤＳＴ要求によって影響を受けるかを正確に指定することができる。さらに、ＳＡＭＬは識別子マッピングメッセージの交換をサポートするので、サブジェクト識別子がユーザの仮名であることが可能であり、それにより、ユーザの実際のアイデンティティを隠蔽するだけでなく、サービスプロバイダドメイン間でのユーザ識別子マッピングも可能となる。これは、真のクロスドメイン適用可能性の前提条件のひとつである。

【００６３】

図３は、本発明の一実施形態によるＳＡＭＬ　ＤＳＴ応答メッセージを例示する模式図を示している。これは、ＳＡＭＬ　ＤＳＴ要求に対する応答である。図３に例示したＳＡＭＬ　ＤＳＴ応答は、周知のＳＡＭＬ応答型（StatusResponseType）から派生されており、応答がステータス、署名等を含むことができることを保証する。

【００６４】

ＳＡＭＬ　ＤＳＴ応答は、再試行要求内で使用されるべきサブジェクト名に関する情報を保持する要素を含む。これは、サブジェクト識別子がアイデンティティプロバイダによって、ドメイン間でアドホックな形でマッピングされる場合に必要とされる。さらに、ＳＡＭＬ　ＤＳＴ応答内で複数のＤＳＴコンテナ（DSTContainer）要素を宣言する可能性が追加される。

【００６５】

各DSTContainer要素は、ＤＳＴ要求に対する応答とともに、ＤＳＴを発行したサービスプロバイダを参照するために使用可能な識別子を含む。この識別子は、例えば、不成功の応答または期待されない応答の場合に、特定のサービス提供側ＳＰと連絡をとるために、要求側ＳＰによって使用されることが可能である。また、この識別子は、どのＳＰがどのように（例えば、分散ユーザプロファイル管理ユーザインタフェースにおいて）応答したかをユーザに示すために使用可能である。

【００６６】

なお、各サービス提供側ＳＰは、DSTContainer要素内でただ１つのＤＳＴ応答によって応答する。というのは、ＳＡＭＬ　ＤＳＴ要求はただ１つのＤＳＴ要求を含むからである。ＳＡＭＬ　ＤＳＴ応答内に複数のDSTContainer要素を有する必要性は、アイデンティティプロバイダ側で複数のＤＳＴ応答を１つのＳＡＭＬ　ＤＳＴ応答内に集積させるという要件による。ただし、この要件は、図４に例示するプロキシモードの場合のみである。

【００６７】

図４は、ＳＡＭＬ　ＤＳＴプロキシとしてアイデンティティプロバイダが作用する場合のメッセージフローを例示するシーケンス図である。ＳＡＭＬ　ＤＳＴメッセージは、要求側とサービス提供側のＳＰ間で直接に使用される。しかし、要求者と応答者を分離し、ユーザのプライバシーを尊重するクロスドメインプロファイルデータ管理を提供するため、アイデンティティプロバイダが、ＳＡＭＬ　ＤＳＴメッセージの交換に関与する。したがって、アイデンティティプロバイダに対する拡張が実装され、それがメッセージフロー

に統合される。

【００６８】

図４のステップ１．０に例示するように、ユーザは、与えられた仮名によってＳＰ－Ａにアクセスする。ユーザのプロファイルに対する問合せまたは操作のため、ＳＰ－Ａは、ＳＡＭＬ　ＤＳＴメッセージを作成する。ＳＡＭＬ　ＤＳＴメッセージは、ユーザの仮名をサブジェクトとし、ユーザの特定のデータに影響を及ぼすＤＳＴメッセージを含む。ステップ１．２で、ＳＰ－Ａは、ＳＡＭＬ　ＤＳＴメッセージをアイデンティティプロバイダへ送信する。ユーザの仮名はＳＰ－Ａのドメイン内でのみ有効なので、アイデンティティプロバイダは、要求側およびサービス提供側の両方のＳＰで有効となる一時的仮名を作成する。そして、アイデンティティプロバイダは、問合せで使用されるべき一時的仮名を示すＳＡＭＬ　ＤＳＴ再試行メッセージによって応答する。これは、ＳＰ－Ａのメッセージ署名が元のまま保持されなければならない場合に必要である。より容易な方式として、アイデンティティプロバイダがＳＡＭＬ　ＤＳＴメッセージ内で仮名を交換することも考えられるが、これはＳＰ－Ａの署名を破壊してしまう。その場合、サービス提供側ＳＰは、アイデンティティプロバイダの署名を検証できるだけで、発信側ＳＰのものは検証できなくなる。これは必ずしも欠点ではなく、ＳＰ間の信頼およびビジネス関係に依存する。

【００６９】

図４のステップ１．５で、ＳＰ－Ａは、一時的仮名をサブジェクトとする新しいＳＡＭＬ　ＤＳＴメッセージを送信する。ステップ１．６で、アイデンティティプロバイダは、受信した要求で指定されるプロファイル型に影響を及ぼすＤＳＴ要求をどのＳＰが処理できるかを検索する。例えば、ＤＳＴ要求が型urn:banking:profile:dataのプロファイルに影響を及ぼす場合、アイデンティティプロバイダは、ユーザが契約しているすべての銀行を検索する。この情報は、アイデンティティプロバイダに利用可能でなければならず、これは通常、事前のアカウント連合（account federation）ステップによって確立される。

【００７０】

図４のステップ１．７で、アイデンティティプロバイダは、要求を第１のサービス提供側ＳＰ（ＳＰ－Ｂ）へ転送する。ＳＰ－Ｂは、まず、要求の一時的仮名をローカルユーザＩＤへと解決しようと試みる。これはユーザのプロファイルを識別することになる。アイデンティティプロバイダは、ＩｄＭの場合に通例となっているように、一時的ＩＤを解決する。その後、ＳＰ－ＢはＤＳＴ要求を処理し、ＤＳＴ要求に対する応答を示すＳＡＭＬ　ＤＳＴ応答によって応答する（ステップ１．１１）。

【００７１】

アイデンティティプロバイダは、この手続きをすべての利用可能なＳＰについて繰り返し、各サービス提供側ＳＰの応答を集積する。最後に、（ステップ１．１８）アイデンティティプロバイダは、サービス提供側ＳＰからのすべてのＤＳＴ応答を含むＳＡＭＬ　ＤＳＴ応答を返す。これに加えて、ＳＡＭＬ　ＤＳＴ応答は、各ＤＳＴ応答ごとに、それぞれのＤＳＴ応答者、すなわちサービス提供側ＳＰを識別するＩＤを含む。

【００７２】

プロセス全体の間に、アイデンティティプロバイダは、ユーザによって定義されたアクセス制御ポリシーに従って、特定のプロファイル情報またはサービス提供側ＳＰへのアクセスを拒否することができる。さらに、各サービス提供側ＳＰは、保存しているプロファイル情報へのアクセスおよび変更に対する完全な制御を有する。したがって、各ＳＰは、限定されたサブセットのみにアクセス可能であること、またはどの情報にもアクセス不可能であることを保証することができる。

【００７３】

ＳＰによって公開されるメタデータを利用することにより（これは、リバティアライアンスのＩｄＭソリューションにおける共通の概念である）、アイデンティティプロバイダまたは要求側ＳＰは、ＳＰがサポートするのはどのプロファイルデータ型であるかを発見することが可能となる。サービス提供側ＳＰは、公開されたメタデータ内のユーザプロファイルのサポートされた型を指定するだけでよい。プロファイル型は、固有のプロファイ

ルスキーマ名前空間によって簡単に識別することができる。プロファイルスキーマ名前空間もまた、ＳＡＭＬ　ＤＳＴメッセージ内でプロファイル型を識別するために使用される。

【００７４】

図５は、可能なサービス提供側サービスプロバイダを要求側サービスプロバイダが発見するための発見サーバとしてアイデンティティプロバイダが作用する場合のメッセージフローを例示するシーケンス図を示している。前提条件として、アイデンティティプロバイダ、要求側ＳＰおよびサービス提供側データＳＰは連合を有する。特に、サービス提供側データＳＰは、ユーザ情報のリポジトリ（アカウント）を有し、そのアカウントについてアイデンティティプロバイダとの間で連合している。すなわち、アイデンティティプロバイダには、サービス提供側データＳＰがローカルユーザデータアカウントを識別するために使用可能なアカウントマッピング識別子が存在する。

【００７５】

図５のステップ１．０で、要求側ＳＰは、ユーザの仮名をサブジェクトとして含むＳＡＭＬ　ＤＳＴ要求をアイデンティティプロバイダへ送信する。アイデンティティプロバイダは、署名をチェックして、要求が有効であることを確認し（ステップ１．１）、どのプロファイル型がＤＳＴ処理を受けるかを見出し（ステップ１．２および１．３）、この特定ユーザに対してこの種類の要求にサービス提供できるＳＰを見つけ（ステップ１．４および１．５）、ユーザを識別するためにサービス提供側ＳＰによって使用されることが可能な一時的仮名を作成することができる。これは、nameIDマッピングによって確立される。

【００７６】

そして、アイデンティティプロバイダは、ＳＡＭＬ　ＤＳＴメッセージのサブジェクトを一時的仮名と交換し、自己の署名によりメッセージに署名する。要求の変更は要求側ＳＰの署名を破壊するので、アイデンティティプロバイダは、変更した要求およびサービス提供側ＳＰのエンドポイントＵＲＬ（Uniform Resource Locator）を含むＳＡＭＬ　ＤＳＴ応答を要求側ＳＰへ送信する。このサービス提供側ＳＰは、その変更された要求にサービス提供することができるとともに、一時的仮名に対する確立されたnameＩＤマッピングを有する（ステップ１．９）。アイデンティティプロバイダは、アクセスポリシーを施行し、例えばＵＲＬのリストからある特定のＳＰを除外してもよい。

【００７７】

そして、要求側ＳＰは、ＳＡＭＬ　ＤＳＴ要求に再署名し（これを行う理由は、アイデンティティプロバイダを信頼しているためである）、要求側ＳＰがコンタクトＵＲＬを取得した１つまたは複数のＳＰへ要求を送信する。こうして、各サービス提供側ＳＰは、アイデンティティプロバイダおよび要求側ＳＰの両方の署名をチェックすることができる。サービス提供側ＳＰは、仮名をローカルユーザＩＤへと解決し、ＤＳＴ要求にサービス提供し、要求側ＳＰに対してＳＡＭＬ　ＤＳＴ応答により応答する。

【００７８】

これにより、アイデンティティプロバイダ上の負荷が低減され、ＳＰ間の対話がより直接的になる。他方、アイデンティティプロバイダはメッセージループから除外されるので、そのアクセス権を施行する能力を低減させる。また、サービス提供側ＳＡＭＬ　ＤＳＴＳＰのエンドポイントＵＲＩを渡すことにより、要求側ＳＰは、ユーザがどこにアカウントを有するかを見出すことができる。要求側ＳＰは仮名によってのみ（すなわちユーザの実際のアイデンティティによってではなく）ユーザを識別するかもしれないが、これはユーザのプライバシーを損なわない。

【００７９】

上記の説明および添付図面の記載に基づいて、当業者は本発明の多くの変形例および他の実施形態に想到し得るであろう。したがって、本発明は、開示した具体的実施形態に限定されるものではなく、変形例および他の実施形態も、添付の特許請求の範囲内に含まれるものと解すべきである。本明細書では特定の用語を用いているが、それらは総称的・説

明的意味でのみ用いられており、限定を目的としたものではない。

【図１】

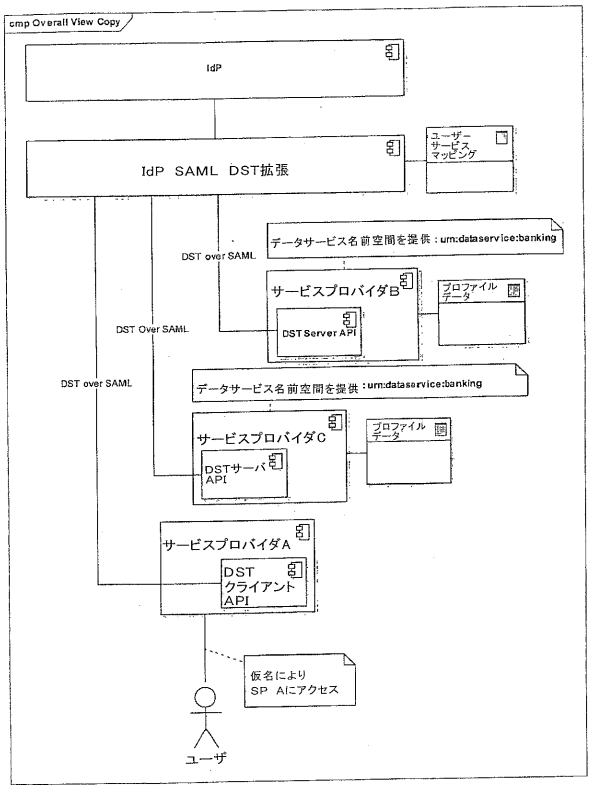


Fig. 1

【図２】

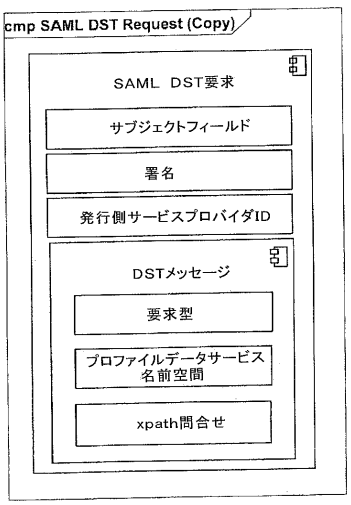


Fig. 2

【図３】

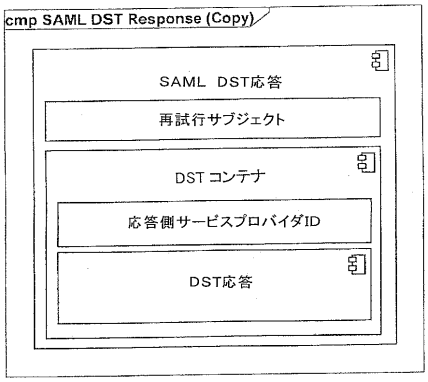


Fig. 3

【図４】

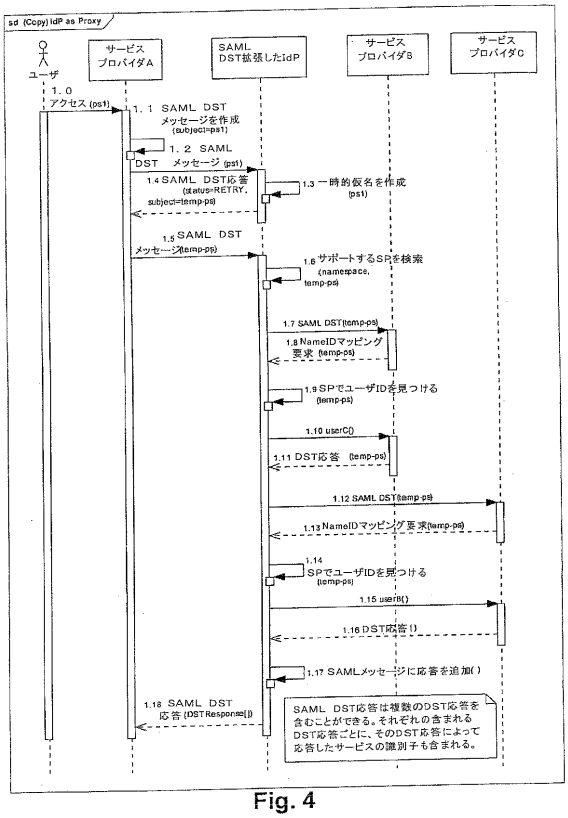


Fig. 4

【図５】

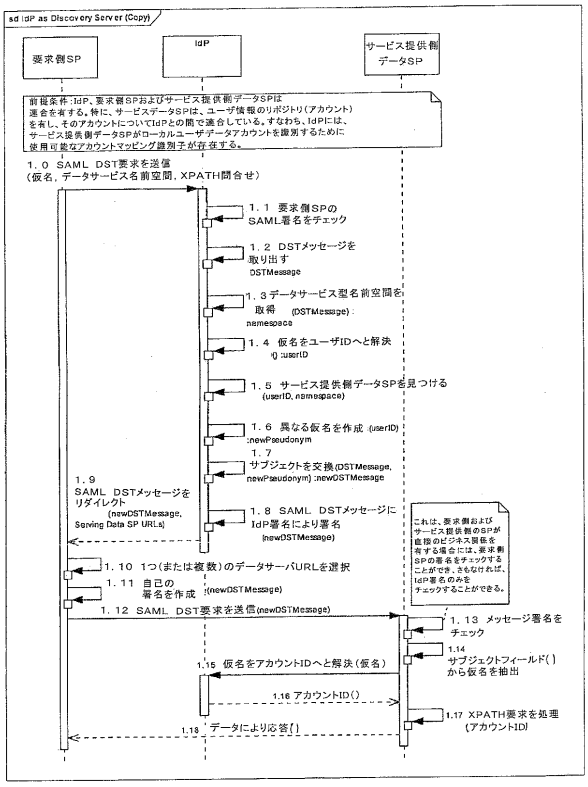


Fig. 5

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/001587

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Generic User Profile (GUP); Stage 3; Network (Release 8)" 3GPP STANDARD; 3GPP TS 29.240, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE, no. V8.0.0, 1 December 2008 (2008-12-01), pages 1-73, XP050372722	1-12, 14-30
A	sections 1,4 sections 5-7 section 10	13

-/--

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 June 2010	12/07/2010

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schossmaier, Klaus

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2010/001587

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"SAML XPath Attribute Profile" OASIS 30 August 2005 (2005-08-30), pages 1-9, XP002588047 Retrieved from the Internet: URL:http://www.oasis-open.org/committees/download.php/16112 [retrieved on 2010-06-21] section 2	1-30
A	S. SAKLIKAR, S. SAHA: "User Privacy-preserving Identity Data Dependencies" ACM, 2 PENN PLAZA, SUITE 701 - NEW YORK USA, 3 November 2006 (2006-11-03), pages 45-54, XP040050487 * abstract; figures 1,4,6 sections 2.1, 2.2, 3.3, 4.3	1-30

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 サントス、フーゴ
ドイツ連邦共和国 ６９１１５ ハイデルベルク、フェーレンツシュトラーセ ６
(72)発明者 ダ シルバ、ジョアオ
ドイツ連邦共和国 ６９１２１ ハイデルベルク、カペレンベック ２０

Ｆターム(参考) 5B084 AA26 AB36 BB16 CD22