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

特許第5479111号
(P5479111)

(45)発行日　平成26年4月23日(2014.4.23)　(24)登録日　平成26年2月21日(2014.2.21)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/20	131A
G06F 21/33	(2013.01)	G06F	21/20	133
H04L 9/32	(2006.01)	H04L	9/00	673A
		H04L	9/00	673E

請求項の数 3　(全 18 頁)

(21)出願番号	特願2009-547403 (P2009-547403)
(86)(22)出願日	平成20年1月23日 (2008.1.23)
(65)公表番号	特表2010-517176 (P2010-517176A)
(43)公表日	平成22年5月20日 (2010.5.20)
(86)国際出願番号	PCT/US2008/051814
(87)国際公開番号	WO2009/029286
(87)国際公開日	平成21年3月5日 (2009.3.5)
審査請求日	平成22年12月6日 (2010.12.6)
(31)優先権主張番号	60/886,894
(32)優先日	平成19年1月26日 (2007.1.26)
(33)優先権主張国	米国(US)
(31)優先権主張番号	11/952,890
(32)優先日	平成19年12月7日 (2007.12.7)
(33)優先権主張国	米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100101373
弁理士　竹内　茂雄
(74)代理人　100118902
弁理士　山本　修
(74)代理人　100153028
弁理士　上田　忠

最終頁に続く

(54)【発明の名称】デジタルＩＤ提示の配布および使用のコントロール

(57)【特許請求の範囲】

【請求項１】

デジタルＩＤ表現を使用する方法であって、

ＩＤトークンを求める要求を依拠当事者から受信するステップと、

前記デジタルＩＤ表現を獲得する第２のデバイスからの要求を第１のデバイスに送信するステップと、

前記第２のデバイスにおいて、本人についての少なくとも第１の主張を説明するメタデータを含む前記デジタルＩＤ表現を受信するステップと、

前記デジタルＩＤ表現を使用する要求を前記第２のデバイスから送信するステップと、

前記第２のデバイスにおいて、前記デジタルＩＤ表現を使用する許可を受信するステップと、

前記デジタルＩＤ表現を使用して、前記ＩＤトークンを要求するステップと、

前記ＩＤトークンを受信するステップと、

前記ＩＤトークンを前記依拠当事者に供給するステップと

を含むことを特徴とする方法。

【請求項２】

前記デジタルＩＤ表現を使用する前記要求が、前記本人以外の個人によってコントロールされるデバイスに送信されることを特徴とする請求項１に記載の方法。

【請求項３】

前記デジタルＩＤ表現を使用する前記要求は、前記依拠当事者を識別する情報を含むこ

とを特徴とする請求項１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、「ＤＩＲ」（デジタルＩＤ表現）の配布（分配、ｄｉｓｔｒｉｂｕｔｉｏｎ）および使用をコントロールするためのシステムに関する。
【背景技術】
【０００２】
特にデジタルの文脈において、個人ＩＤ情報がどのように配布させられ、使用されるかに対するより大きいコントロールを個人に与えるさらなる取り組みが、行われている。例えば、とりわけ、ワシントン州レッドモンド所在のマイクロソフトコーポレーションが、ときとして、Ｉｎｆｏｒｍａｔｉｏｎ Ｃａｒｄ Ｓｅｌｅｃｔｏｒと呼ばれるシステムを提案しており、マイクロソフトによるインスタンス化は、一般に、Ｗｉｎｄｏｗｓ ＣａｒｄＳｐａｃｅと呼ばれる。Ｗｉｎｄｏｗｓ ＣａｒｄＳｐａｃｅシステムにおいて、本人が、ときとして、情報カードと呼ばれる、１つまたは複数のデジタルＩＤ表現を獲得する。本人が、本人について行われる主張のセットを要求するリソース（「依拠当事者」）にアクセスしようと試みる場合、本人は、デジタルＩＤ表現（以降、「ＤＩＲ」と呼ばれる）を使用して、それらの主張を表明することができるＩＤプロバイダとの通信を開始する。一部の事例では、ＩＤプロバイダは、本人によってコントロールされ、本人自らのマシン上で実行されることが可能である。他の事例では、ＩＤプロバイダは、第三者によってコントロールすることが可能である。ＩＤプロバイダは、要求された主張情報を含む「ＩＤトークン」を戻す。
【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】Web Services Security Specifications
【発明の概要】
【発明が解決しようとする課題】
【０００４】
ＤＩＲは、とりわけ、ＩＤトークンを求める依拠当事者要求に応じるという文脈において役立つ。ＤＩＲの容易でセキュリティで保護された使用を提供することが、そのような依拠当事者へのアクセスを求める本人に有利である。
【課題を解決するための手段】
【０００５】
この概要は、詳細な説明において後段でさらに説明される選定された概念を、簡略化された形態で概説するように与えられる。この概要は、主張される主題の重要な特徴、または不可欠な特徴を特定することは意図しておらず、主張される主題の範囲を確定する助けとして使用されることも意図していない。
【０００６】
一態様は、ＤＩＲの配布をコントロールするための方法に関する。第１のデバイスが、ＤＩＲを求める要求を受信する。第１のデバイスのユーザが、この要求を受け付ける、または拒否するように促される。この要求が受け付けられた場合、ＤＩＲが提供される。実施形態において、第１のデバイスのユーザは、ＤＩＲが主張を規定するところの本人である。他の実施形態において、第１のデバイスのユーザは、本人ではない。実施形態において、第１のデバイスは、時間認識（ｓｅｎｓｅ ｏｆ ｔｉｍｅ）を有さず、ＤＩＲは、第２のデバイスからのＤＩＲを求める要求の中で与えられるタイムスタンプに基づく使用制限を含む。さらなる実施形態において、第１のデバイスは、ＩＤプロバイダを含み、ＤＩＲが第２のデバイスに供給されるのに先立って、ＤＩＲの中のＩＤプロバイダに関するアドレスが、第１のデバイスの、外部からアクセス可能なアドレスに変更される。
【０００７】

別の態様は、ＤＩＲの使用をコントロールするためのコンピュータプログラム製品に関する。第１のデバイスが、ＤＩＲを使用する要求を第２のデバイスから受信する。第１のデバイスのユーザが、この要求を受け付ける、または拒否するように促される。この要求が受け付けられた場合、ＤＩＲを使用する許可が、与えられる。この場合も、実施形態において、第１のデバイスのユーザは、ＤＩＲが主張を含むところの本人であっても、本人でなくてもよい。

【０００８】

さらに別の態様は、ＤＩＲを使用するための方法に関する。ＩＤトークンを求める要求が、依拠当事者から受信される。ＤＩＲを獲得する要求が、第２のデバイスから第１のデバイスに送信される。デジタルＩＤ表現は、本人についての少なくとも第１の主張を記述するメタデータを含み、ＤＩＲは、第２のデバイスにおいて受信される。ＤＩＲを使用する要求が、第２のデバイスから送信される。第２のデバイスは、ＤＩＲを使用する許可を受信し、すると、ＤＩＲは、ＩＤトークンを獲得するのに使用される。ＩＤトークンは、依拠当事者に送信される。

【図面の簡単な説明】

【０００９】

【図１】例示的なＤＩＲ配布－使用システムを示す図である。

【図２】ＤＩＲの配布をコントロールするための例示的な方法を示す図である。

【図３】ＤＩＲを供給するための例示的な方法を示す図である。

【図４】ＤＩＲの使用をコントロールするための例示的な方法を示す図である。

【図５】ＤＩＲを入手し、使用するための例示的な方法を示す図である。

【図６】ＤＩＲを入手し、使用するための別の例示的な方法を示す図である。

【図７】汎用コンピューティングデバイスを示す図である。

【発明を実施するための形態】

【００１０】

次に、例示的な実施形態を、添付の図面を参照して以下により完全に説明する。全体にわたって同様の符号が、同様の要素を指す。

【００１１】

本明細書で開示される例示的な実施形態は、一般に、本人と関係するＩＤおよび／または情報を認証するのに本人、ＩＤプロバイダ、および依拠当事者の間で交換されることが可能なＩＤトークンの生成のために通信を開始する際に使用されるＤＩＲを含むＩＤシステムに関する。本明細書の例示的な実施形態において、本人は、自然人または複数の自然人、コンピュータ、ネットワーク、または他の任意のエンティティであることが可能である。依拠当事者は、本人がアクセスする、さらに／または獲得することを所望する品物、サービス、または他の情報を有する。例示的な実施形態において、依拠当事者は、入る、アクセスする、または使用するのにセキュリティポリシを要求する任意のリソース、特権、またはサービスであることが可能である。例えば、依拠当事者は、コンピュータ、コンピュータネットワーク、データ、データベース、建造物、スタッフ、サービス、会社、組織、物理的ロケーション、電子デバイス、または他の任意のタイプのリソースの１つまたは複数を含むことが可能である。

【００１２】

次に図１を参照すると、第１のデバイス１０５、第１のユーザ１０６、本人１１０、第２のデバイス１１１、第３のデバイス１１７、第３のユーザ１１８、および依拠当事者１２０を含む例示的なＤＩＲシステム１００が、示されている。第１のデバイス１０５は、第１のユーザ１０６によって少なくとも一時的にコントロールされるコンピュータシステムを含む。第２のデバイス１１１は、本人１１０によって少なくとも一時的にコントロールされるコンピュータシステムを含む。第３のデバイス１１７は、第３のユーザ１１８によって少なくとも一時的にコントロールされるコンピュータシステムを含む。本明細書で説明されるとおり、第１のユーザ１０６、本人１１０、および第３のユーザ１１８は、３つの異なる人々またはエンティティを含むことが可能であり、あるいは、実施形態におい

て、同一の人々またはエンティティを含むことが可能である。依拠当事者１２０は、コンピュータシステムを含むことも可能である。システム１００は、ＩＤプロバイダ１１５およびＩＤプロバイダ１０７を含むことも可能であり、プロバイダ１１５およびプロバイダ１０７のそれぞれは、後段でさらに説明され、コンピュータシステムを含む、またはコンピュータシステムの一部であることが可能である。

【００１３】

第１のデバイス１０５、第２のデバイス１１１、第３のデバイス１１７、ＩＤプロバイダ１１５、および依拠当事者１２０は、インターネットなどの１つまたは複数のネットワークを介して、あるいは電話通信、または他の形態の有線通信もしくは無線通信を介して互いに通信することができる。例示的な実施形態において、本人１１０は、第２のデバイス１１１を使用して、依拠当事者１２０から品物、サービス、情報、特権、または他のアクセスを要求することができる。依拠当事者１２０は、要求されたアクセスを本人１１０に与える前に、または与えるのに当たって、本人１１０のＩＤ、または本人１１０についての情報の認証を要求することができる。

【００１４】

やはり図１に示されているのが、例示的なＩＤプロバイダ１１５である。ＩＤプロバイダ１１５は、コンピュータシステムを含む。例示的な実施形態において、ＩＤプロバイダ１１５は、主張トランスフォーマ１３０および主張権限１４０を含む。主張トランスフォーマ１３０は、ときとして、「セキュリティトークンサービス」と呼ばれる。図示される実施例において、ＩＤプロバイダ１１５は、本人１１０についての１つまたは複数の主張を供給することができる。主張は、場合により、例えば、名前、アドレス、社会保障番号、年齢、信用履歴、取引要件などの、本人についての情報を含む、本人について行われる言明または表明である。後段でさらに説明されるとおり、ＩＤプロバイダ１１５は、デジタル署名されたＩＤトークンの形態で依拠当事者１２０に主張を供給することができる。例示的な実施形態において、ＩＤプロバイダ１１５は、依拠当事者１２０と信頼関係にあり、したがって、依拠当事者１２０は、ＩＤプロバイダ１１５からの署名されたＩＤトークンの中の主張を信頼する。実施形態において、ＩＤプロバイダ１０７は、ＩＤプロバイダ１１５と同一、または同様であることが可能であるが、別個にコントロールされるコンピュータシステムではなく、第１のデバイス１０５の一部であることが可能である。

【００１５】

ＩＤプロバイダ１１５の主張トランスフォーマ１３０と主張権限１４０は、図１に別々のエンティティとして示されるものの、代替の実施形態において、主張トランスフォーマ１３０と主張権限１４０は、同一のエンティティであることも、異なるエンティティもしくはシステムであることも可能である。ＩＤプロバイダ１１５は、一部の例示的な実施形態においてセキュリティトークンサービスの形態をとることが可能である。同様に、第１のデバイス１０５、第２のデバイス１１１、および第３のデバイス１１７は、同一のエンティティもしくはシステムであっても、異なるエンティティもしくはシステムであってもよい。

【００１６】

本明細書で説明されるコンピュータシステムは、限定なしに、パーソナルコンピュータ、サーバコンピュータ、ハンドヘルドデバイスもしくはラップトップデバイス、マイクロプロセッサシステム、マイクロプロセッサベースのシステム、プログラマブル家庭用電子機器、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、スマートカード、電話機、移動通信デバイスもしくはセルラー通信デバイス、パーソナルデータアシスタント、以上のシステムもしくはデバイスのいずれかを含む分散コンピューティング環境などを含む。本明細書で説明される一部のコンピュータシステムは、ポータブルコンピューティングデバイスを含むことが可能である。ポータブルコンピューティングデバイスは、ユーザによって物理的に携帯されるように設計された任意のコンピュータシステムである。各コンピュータシステムは、限定なしに、キーボード、マウス、カメラ、Ｗｅｂカメラ、ビデオカメラ、指紋スキャナ、虹彩スキャナ、モニタなどのディスプレイデバイス

、マイク、またはスピーカを含む、１つまたは複数の周辺装置を含むことも可能である。「コンピュータシステム」という用語は、本明細書で「デバイス」と互換的に使用される。

【００１７】

各コンピュータシステムは、（限定なしに）マイクロソフトコーポレーションからのＷＩＮＤＯＷＳオペレーティングシステムなどのオペレーティングシステム、およびコンピュータ可読媒体上に格納された１つまたは複数のプログラムを含む。また、各コンピュータシステムは、ユーザがコンピュータシステムと通信することを可能にするとともに、コンピュータシステムが他のデバイスと通信することも可能にする１つまたは複数の入力通信デバイスおよび出力通信デバイスを含むことも可能である。図１のコンピュータシステム（例えば、第１のデバイス１０５、第２のデバイス１１１、第３のデバイス１１７、ＩＤプロバイダ１１５、および依拠当事者１２０間の通信は、限定なしに、インターネット、ワイドエリアネットワーク、イントラネット、イーサネット、直接配線パス、衛星、赤外線スキャン、Ｂｌｕｅｔｏｏｔｈ、セルラー通信、あるいは他の任意のタイプの有線通信または無線通信を含む、任意のタイプの通信リンクを使用して実施されることが可能である。

【００１８】

本明細書で開示される一部の例示的な実施形態において、システム１００は、少なくとも部分的に、ワシントン州レッドモンド所在のマイクロソフトコーポレーションによって開発された．ＮＥＴ３．０フレームワークにおいて提供されるＩｎｆｏｒｍａｔｉｏｎ Ｃａｒｄシステムとして実施される。Ｉｎｆｏｒｍａｔｉｏｎ Ｃａｒｄシステムは、ユーザが、様々なＩＤプロバイダからの複数のＤＩＲを管理することを可能にする。第１のデバイス１０５、第２のデバイス１１１、および第３のデバイス１１７のそれぞれが、ワシントン州レッドモンド所在のマイクロソフトコーポレーションからのＷｉｎｄｏｗｓ ＣａｒｄＳｐａｃｅなどのＩＤセレクタを含むことが可能である。

【００１９】

Ｉｎｆｏｒｍａｔｉｏｎ Ｃａｒｄシステムは、．ＮＥＴ３．０フレームワークにおけるＷｉｎｄｏｗｓ Ｃｏｍｍｕｎｉｃａｔｉｏｎ ＦｒａｍｅｗｏｒｋなどのＷｅｂサービスプラットフォームを利用する。さらに、Ｉｎｆｏｒｍａｔｉｏｎ Ｃａｒｄシステムは、少なくとも一部にはワシントン州レッドモンド所在のマイクロソフトコーポレーションによって広められる非特許文献１を使用して構築される。これらの仕様は、メッセージセキュリティモデル、ＷＳ－Ｓｅｃｕｒｉｔｙ、エンドポイントポリシ、ＷＳ－ＳｅｃｕｒｉｔｙＰｏｌｉｃｙ、メタデータ交換、ＷＳ－ＭｅｔａｄａｔａＥｘｃｈａｎｇｅ、および信頼モデル、ＷＳ－Ｔｒｕｓｔを含む。一般に、ＷＳ－Ｓｅｃｕｒｉｔｙモデルは、ＩＤトークンをメッセージにどのように添付すべきかを説明する。ＷＳ－ＳｅｃｕｒｉｔｙＰｏｌｉｃｙモデルは、要求されるＩＤトークンやサポートされる暗号化アルゴリズムなどのエンドポイントポリシ要件を説明する。そのようなポリシ要件は、ＷＳ－ＭｅｔａｄａｔａＥｘｃｈａｎｇｅによって定義されるメタデータプロトコルを使用して伝えられ、ネゴシエートされることが可能である。ＷＳ－Ｔｒｕｓｔモデルは、異なるＷｅｂサービスが相互運用されることを可能にする信頼モデルのためのフレームワークを説明する。本明細書で説明される一部の例示的な実施形態は、前述した非特許文献１を参照する。代替の実施形態では、他の１つまたは複数の仕様を使用して、システム１００内の様々なサブシステム間の通信が円滑にされることが可能である。

【００２０】

図１を再び参照すると、本人１１０が、品物、サービス、または他の情報へのアクセスを求める要求を、第２のデバイス１１１を介して依拠当事者１２０に送信することができる。例えば、一実施形態では、第２のデバイス１１１が、オンライン購入を完了するなどの、依拠当事者１２０において或る操作を実行する要求を、依拠当事者１２０に送信する。第２のデバイス１１１によって送信される、この要求は、例えば、ＷＳ－ＭｅｔａｄａｔａＥｘｃｈａｎｇｅにおいて提供される機構を使用して、依拠当事者１２０の認証要件

を求める要求を含むことが可能である。

【００２１】

この要求に応答して、依拠当事者１２０は、依拠当事者１２０が、本人のＩＤ、または本人１１０についての他の情報を認証する要件を第２のデバイス１１１に送信することが可能である。認証を求める依拠当事者１２０の、これらの要件は、本明細書でセキュリティポリシと呼ばれる。セキュリティポリシは、依拠当事者１２０が本人１１０を認証するのに、本人１１０が依拠当事者１２０に供給しなければならない、信頼されるＩＤプロバイダ１１５もしくはＩＤプロバイダ１１７からの主張のセットの最小限の定義を行う。セキュリティポリシは、個人的特徴（年齢などの）、ＩＤ、財務状況などに関する証明の要件を含むことが可能である。また、セキュリティポリシは、証明の申し出（例えば、或る特定のＩＤプロバイダからのデジタル署名）を認証するのに要求される検証および認証のレベルに関する規則を含むことも可能である。

【００２２】

一実施例では、依拠当事者１２０は、依拠当事者１２０によって要求される主張要件と、ＩＤトークンのタイプの両方を含め、依拠当事者１２０のセキュリティポリシを、ＷＳ－ＳｅｃｕｒｉｔｙＰｏｌｉｃｙを使用して指定する。主張のタイプの例には、限定なしに、以下が含まれる。すなわち、ファーストネーム、ラストネーム、電子メールアドレス、番地、地域名または都市、州または県、郵便番号、国、電話番号、社会保障番号、生年月日、性別、個人識別番号、信用度、財務状況、法的地位などである。

【００２３】

また、このセキュリティポリシを使用して、依拠当事者１２０によって要求されるＩＤトークンのタイプが指定されることも可能であり、あるいはＩＤプロバイダによって決定されるとおりのデフォルトのタイプが、使用されることが可能である。要求される主張およびトークンタイプを指定することに加えて、セキュリティポリシは、依拠当事者によって要求される特定のＩＤプロバイダを指定することができる。代替として、ポリシは、この要素を省略して、適切なＩＤプロバイダの決定を本人１１０に任せることもできる。例えば、要求されるセキュリティトークンの鮮度などの、他の要素が、セキュリティポリシの中で指定されることも可能である。

【００２４】

一部の実施形態において、本人１１０は、後段で説明されるとおり、依拠当事者１２０が、第２のデバイス１１１に自らの身元を明らかにして、本人１１０が、依拠当事者１２０のセキュリティポリシを満たすか否かを判定することができるようにすることを要求することができる。一実施例では、依拠当事者１２０は、Ｘ５０９証明書を使用して自らの身元を明らかにする。他の実施形態において、依拠当事者１２０は、例えば、「ＳＳＬ」（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）サーバ証明書などの他の機構を使用して、自らの身元を明らかにすることができる。

【００２５】

第２のデバイス１１１は、本人１１０に関する１つまたは複数のＤＩＲ１１２を含むことが可能である。これらのＤＩＲ１１２（ワシントン州レッドモンド所在のマイクロソフトコーポレーションによって開発された．ＮＥＴ３．０フレームワークにおいて提供されるＷｉｎｄｏｗｓ　ＣａｒｄＳｐａｃｅシステムにおいて、ときとして、「Ｉｎｆｏｒｍａｔｉｏｎ　Ｃａｒｄ」と呼ばれる）は、本人１１０と、ＩＤプロバイダ１１５などの或る特定のＩＤプロバイダとの間のトークン発行関係を表す人工物（ａｒｔｉｆａｃｔ）である。各ＤＩＲは、或る特定のＩＤプロバイダに対応することが可能であり、さらに本人１１０は、同一のＩＤプロバイダ、または異なるＩＤプロバイダからの複数のＤＩＲ１１２を有することが可能である。

【００２６】

ＤＩＲ１１２は、他の情報も含むが、とりわけ、発行されることが可能なトークンのタイプ、ＩＤプロバイダが権限を有する主張タイプ、および／またはＩＤトークンを要求する場合に認証のために使用すべき資格証明を含め、ＩＤトークンに関するＩＤプロバイダ

の発行ポリシを含むことが可能である。ＤＩＲ１１２は、ＩＤプロバイダ１１５またはＤＩＲ生成システムによって発行され、第２のデバイス１１１、第１のデバイス１０５、および／または第３のデバイス１１７などの記憶装置上に格納されるＸＭＬ文書として表されることが可能である。図１の様々なデバイスの中に表されるＤＩＲ１１２は、本明細書でさらに説明されるとおり、同一のＤＩＲの異なるコピーであること、異なるＤＩＲであること、あるいは同一の主張を有するが、異なるデバイスにおいて使用されるように適合されたＤＩＲであることが可能である。

【００２７】

説明されるとおり、第２のデバイス１１１は、ＩＤセレクタを含むことも可能である。一般に、ＩＤセレクタは、本人１１０が、第２のデバイス１１１上で本人１１０の１つまたは複数のＤＩＲ１１２の間で選択を行うことを許すコンピュータプログラムおよびユーザインタフェースである。ＤＩＲ１１２は、次にＩＤプロバイダ１１５などの１つまたは複数のＩＤプロバイダからＩＤトークンを要求し、獲得するのに使用されることが可能である。例えば、依拠当事者１２０からのセキュリティポリシが、第２のデバイス１１１によって受信された場合、ＩＤセレクタは、ＤＩＲ１１２の中の情報を使用して、このセキュリティポリシによって要求される主張の１つまたは複数を満たす１つまたは複数のＤＩＲ１１２を識別するようにプログラミングされることが可能である。本人１１０が、依拠当事者１２０からセキュリティポリシを受信すると、本人１１０は、１つまたは複数のＩＤプロバイダと通信して（例えば、第２のデバイス１１１を使用して）、このポリシによって要求される主張を収集することができる。

【００２８】

例示的な実施形態において、本人が、第２のデバイス１１１上の適切なＤＩＲにアクセスした場合、本人１１０は、このＤＩＲ１１２を使用して、ＷＳ－Ｔｒｕｓｔにおいて説明される発行機構を使用するＩＤプロバイダ１１５から１つまたは複数のＩＤトークンを要求する。依拠当事者１２０のＩＤは、本人１１０によってＩＤプロバイダ１１５に送信される要求の中で指定されることが可能であるが、指定されなくてもよい。この要求は、ディスプレイトークンを求める要求などの、他の要件も含むことが可能である。

【００２９】

一般に、ＩＤプロバイダ１１５の主張権限１４０は、依拠当事者１２０からのセキュリティポリシによって要求される主張の１つまたは複数を供給することができる。ＩＤプロバイダ１１５の主張トランスフォーマ１３０は、これらの主張を変形し、さらに本人１１０と関係する主張を含む１つまたは複数の署名されたＩＤトークン１５０を生成するようにプログラミングされる。

【００３０】

本人１１０は、依拠当事者１２０からの要件に基づいて、ＩＤプロバイダ１１５への本人１１０の要求の中で或るフォーマットのＩＤトークンを要求することができる。主張トランスフォーマ１３０は、限定なしに、Ｘ５０９、ケルベロス、ＳＡＭＬ（バージョン１．０および２．０）、「ＳＸＩＰ」（Ｓｉｍｐｌｅ　ｅＸｔｅｎｓｉｂｌｅ　Ｉｄｅｎｔｉｔｙ　Ｐｒｏｔｏｃｏｌ）などを含む複数のフォーマットの１つでＩＤトークンを生成するようにプログラミングされることが可能である。そのような要件は、ＤＩＲの中に含められることが可能である。

【００３１】

例示的な実施形態において、主張トランスフォーマ１３０は、ＷＳ－Ｔｒｕｓｔにおいて説明される応答機構を使用して、ＩＤトークン１５０を本人１１０に転送する。一実施形態では、主張トランスフォーマ１３０は、セキュリティトークンサービス（ときとして、「ＳＴＳ」と呼ばれる）を含む。或る例示的な実施形態では、本人１１０は、ＷＳ－Ｓｅｃｕｒｉｔｙの中で説明されるセキュリティ結合機構を使用してＩＤトークン１５０をアプリケーションメッセージに結合することによって、ＩＤトークン１５０を依拠当事者１２０に転送する。他の実施形態では、ＩＤトークン１５０は、ＩＤプロバイダ１１５から依拠当事者１２０に直接に送信されることが可能である。

【００３２】
依拠当事者１２０が、ＩＤトークン１５０を受信すると、依拠当事者１２０は、署名されたＩＤトークン１５０の出所を検証する（例えば、ＩＤトークン１５０を復号すること、または解読することによって）ことができる。また、依拠当事者１２０は、依拠当事者１２０のセキュリティポリシを満たすようにＩＤトークン１５０の中の主張を利用して、本人１１０を認証し、要求される操作を本人１１０が完了することを許すこともできる。
【００３３】
しかし、実施形態において、第２のデバイス１１１は、ローカルストレージの中に、依拠当事者１２０のセキュリティポリシによって要求される主張を参照する適切なＤＩＲ１１２を有さない。例えば、時々、本人１１０は、公共アクセス可能である第２のデバイス１１１（例えば、公共図書館、空港キオスク、保護されていないコンピュータ端末装置など）を使用して、依拠当事者１２０にアクセスしよう、または依拠当事者１２０において操作を実行しようと試みることが可能である。この事例において、本人１１０は、第１のデバイス１０５または第３のデバイス１１７などの別のデバイス上に格納されたＤＩＲ１１２を使用することを所望する可能性がある。次に、そのような遠隔で格納されたＤＩＲ１１２の使用が、より詳細に説明される。
【００３４】
時々、本人１１０は、依拠当事者１２０などの依拠当事者にアクセスしようと試みるのに本人１１０が使用するデバイスとは異なるデバイスを使用して、ＤＩＲ１１２を格納することが可能である。例えば、本人１１０は、セルラー電話機などの移動デバイスを使用して、ＤＩＲ１１２を格納することが可能であるが、依拠当事者と対話するのに、「ＰＣ」（パーソナルコンピュータ）などの、より豊かなユーザインタフェースを有するデバイスを使用することを所望する可能性がある。実施形態において、本人１１０は、依拠当事者１２０にアクセスする際に使用するために、ＤＩＲ１１２が第１のデバイス１０５から第２のデバイス１１１に供給されることを要求する。第１のユーザ１０６は、第２のデバイス１１１へのＤＩＲ１１２の解放を承認するように促され、さらに、実施形態において、要求されたＤＩＲ１１２は、そのような承認が受け取られるまで、第２のデバイス１１１に送信されない。他の実施形態では、ＤＩＲ１１２は、第３のデバイス１１７上に格納されるが、第３のデバイス１１７が、ＤＩＲ１１２を第２のデバイス１１１に解放するのに先立って、第２のデバイス１１１へのＤＩＲ１１２の解放の、第１のユーザ１０６からの承認が、要求される。
【００３５】
実施形態において、第１のユーザ１０６と本人１１０は、同一の個人である。例えば、移動電話機上にＤＩＲ１１２を格納し、ＤＩＲ１１２が存在していない第２のデバイス１１１（例えば、ＰＣ）においてＤＩＲを使用することを所望する本人１１０が、（ａ）第２のデバイス１１１上でＤＩＲ１１２を要求すること、および（ｂ）第１のデバイス１０５（例えば、本人の移動電話機）から第２のデバイス１１１へのＤＩＲ１１２の解放を承認することをともに行うことが可能である。他の実施形態では、第２のデバイス１１１へのＤＩＲの解放は、本人１１０と同一ではない第１のユーザ１０６および／または第３のユーザ１１８によって承認されなければならない。
【００３６】
実施形態において、第１のデバイス１０５上に格納されたＤＩＲ１１２は、第１のデバイス１０５上のサービスであることが可能なＩＤプロバイダ１０７をポイントする内部アドレスを含む。例えば、ＤＩＲ１１２が、第１のデバイス１０５によって「自己発行」された（例えば、第１のデバイスが、ＤＩＲ１１２を作成しており、さらにＤＩＲ１１２の使用によって作成されたＩＤトークンを発行する）場合、このＤＩＲ１１２は、ＩＤプロバイダ１０７への内部ポインタを含む。このことは、ＩＤプロバイダ１１５などの第三者ＩＤプロバイダのアドレスを含む「管理されたＤＩＲ」と対照的である。ＩＤプロバイダ１０７は、ＩＤプロバイダ１１５に関連して説明された主張トランスフォーマおよび主張権限を含むことが可能である。

【００３７】
第１のデバイス１０５によって「自己発行」されたＤＩＲ１１２の事例において、第２のデバイス１１１が、第１のデバイス１０５からＤＩＲ１１２を要求した場合、第１のデバイスは、ＩＤプロバイダ１０７のアドレスを内部アドレスから、外部からアクセス可能なアドレスに変更する。このことは、第２のデバイス１１１が、ＤＩＲ１１２を使用してＩＤトークン１５０を獲得しようと最終的に試みた場合に、ＩＤプロバイダ１０７を見出すことを許す。例えば、第２のデバイス１１１からのＤＩＲ１１２を求める要求が、Ｂｌｕｅｔｏｏｔｈ通信を介して行われた場合、ＩＤプロバイダ１０７のアドレスは、Ｂｌｕｅｔｏｏｔｈ識別子に変更されることが可能である。第２のデバイスと第１のデバイスの間の接続が、ＧＰＲＳを介して行われる場合、ＩＤプロバイダ１０７の電話番号が、ＤＩＲ１１２の中に挿入されることが可能である。同様に、ＩＰアドレスとポート番号、ＵＲＬパス名、または他のいくつものアドレス指定機構が、第１のデバイス１０５と第２のデバイス１１１の間の利用可能な通信スタックに応じて、使用されることが可能である。同様に、自己発行されたＤＩＲ１１２が、第３のデバイス１１７からアクセスされる場合、第３のデバイス１１７は、同様の変更を行って、第３のデバイス１１７の中に含まれるＩＤプロバイダの外部からアクセス可能なアドレスをもたらすことができる。
【００３８】
実施形態において、ＤＩＲ１１２は、使用制限を含むことが可能である。例えば、ＤＩＲ１１２は、ＤＩＲ１１２が解放される（第２のデバイス１１１などに）と、ＤＩＲ１１２は、１回だけ、または「以後１０分」以内だけ使用されることが可能であるという命令を含むようにプログラミングされることが可能である。説明されるとおり、時々、本人１１０は、セキュリティで保護されていない第２のデバイス１１１（例えば、公共図書館、キオスクなど）を介して依拠当事者１２０と対話していることが可能である。したがって、実施形態は、ＤＩＲ１１２の許可のない使用を別の仕方で防止すること（例えば、パスワード保護など）が可能であるものの、使用制限は、本人１１０が第２のデバイス１１１をもはやコントロールしなくなった後に、許可のない使用からの別の層の保護をもたらす。
【００３９】
実施形態において、第１のデバイス１０５と第３のデバイス１１７は、互いと比べて、さらに第２のデバイス１１１と比べて、異なる計算能力を有することが可能である。例えば、第１のデバイス１０５と第３のデバイス１１７のいずれか、または両方が、内部クロック、または他の独立した時間認識を欠いている可能性がある。このことは、第１のデバイス１０５または第３のデバイス１１７が、ＤＩＲ１１２を第２のデバイス１１１に解放するのに先立って、ユーザ制限をＤＩＲ１１２の中に符号化することを困難にする。実施形態において、第２のデバイス１１１は、ＤＩＲ１１２を求めるデバイス１１１の要求の中に、第２のデバイス１１１のタイミング機構に基づくタイムスタンプを含める。独自のタイミング機構が無い状態で、第１のデバイス１０５または第３のデバイス１１７は、第２のデバイス１１１からの要求の中のタイムスタンプに依拠して、第２のデバイス１１１にＤＩＲ１１２を解放するのに先立って、ＤＩＲ１１２の中に任意の時間ベースの使用制限を符号化することができる。例えば、ＤＩＲ１１２が、第２のデバイス１１１にダウンロードされた後、１０分間だけ使用可能であるという制限を、ＤＩＲ１１２が要求する、または本人１１０が要求する場合、第１のデバイス１０５は、第２のデバイス１１１からの要求の中のタイムスタンプを使用して現在時刻を決定し、この時刻に１０分を加え、第２のデバイス１１１に送信されるＤＩＲ１１２のコピーの中に適切な有効期限時刻を設定する。
【００４０】
図２は、ＤＩＲの配布をコントロールするための方法２００の実施形態を示す。方法２００は、本人が、或る依拠当事者にアクセスしようと試みることに応答して、あるいはＤＩＲを使用しようとする試みの特定の文脈以外で、行われることが可能である。ステップ２１０で、ＤＩＲを入手する要求が、第２のデバイスから第１のデバイスにおいて受信さ

れる。第１のデバイスのユーザが、ＤＩＲを求める、この要求を受け付ける、または拒否するように促される（２２０）。実施形態において、第１のデバイスのユーザは、第１のデバイスのユーザインタフェースを介して促される。第１のデバイスのユーザは、ＤＩＲを求める、この要求を受け付ける、または拒否することを許されるのに先立って、ユーザ自身を認証するよう求められることが可能である。認証方法は、パスワード、生体認証、スマートカードなどを含め、様々な認証プロトコルのいずれかを含むことが可能である。

【００４１】

ステップ２３０で、第１のデバイスのユーザが、この要求が受け付けられたかどうかを第１のデバイスに示す。受け付けの表示は、プロンプトに応答した第１のデバイスにおけるキーボード入力を含め、様々な仕方で行われることが可能である。ＤＩＲを求める要求が、受け付けられない場合、要求が拒否されたというメッセージが、送信される（２４０）。例えば、第１のデバイスのユーザが、この要求を拒否した場合、または要求がタイムアウトした場合、第１のデバイスは、第２のデバイスが第２のデバイスのユーザに表示することができるメッセージを送信することが可能である。説明されるとおり、第１のデバイスのユーザは、第２のデバイスのユーザと同一であっても、異なっていてもよい。ＤＩＲを求める要求が受け付けられた場合、要求されたＤＩＲが、供給される（２５０）。

【００４２】

図３は、供給ステップ２５０を一部の実施形態において含む方法３００を示す。ステップ３１０で、要求されたＤＩＲが、第１のデバイス上にローカルで格納されているかどうかの判定が、行われる。格納されていない場合、第３のデバイスが、要求されたＤＩＲを供給するように命令される（３２０）。この実施形態において、第３のデバイスは、この図３の残りのステップのいずれか、またはすべてを実行することができる。

【００４３】

ステップ３３０で、ＤＩＲが、ローカルで格納されている場合、要求されたＤＩＲの中に含まれるＩＤプロバイダアドレスが、ローカルサービスまたはローカルプロセスをポイントするかどうかの判定が、行われる。ポイントする場合、供給されるべきＤＩＲのコピーの中のＩＤプロバイダアドレスが、外部からアクセス可能なアドレスに変更される（３４０）。図１に関連して説明されるとおり、外部からアクセス可能なＩＤプロバイダアドレスの選択は、ＤＩＲを要求するのに使用される通信スタックのタイプに依存することが可能である。例えば、第２のデバイスが、インターネット接続を使用して、第１のデバイスからＤＩＲを要求した場合、第１のデバイスにローカルのＩＤプロバイダのアドレスは、第２のデバイスによってアクセス可能なＵＲＬアドレスに変更されることが可能である。

【００４４】

ステップ３５０で、時間ベースの使用制限がＤＩＲの中に含められるべきかどうかの判定が、行われる。実施形態において、ＤＩＲは、別のデバイスに転送される場合、ＤＩＲのそのコピーの使用が制限されなければならない（例えば、「１０分間有効」、「１回限りの使用」など）という命令を含む。他の実施形態では、第２のデバイスにおける本人が、ＤＩＲを求める本人の要求の中に使用制限を含めることができる。例えば、公共コンピュータを使用して依拠当事者にアクセスしている本人が、本人の移動電話機からＤＩＲが公共コンピュータにダウンロードされるように要求することが可能である。しかし、本人は、ＤＩＲが、１０分間だけ有効であることを要求することもでき、このことは、本人が、依拠当事者において或る操作を完了することを可能にするが、ＤＩＲは、その公共コンピュータに後にログインする誰かによって使用可能ではない。第１のデバイスが、ＤＩＲの中に使用制限を含める場合、第１のデバイスは、第２のデバイスが、この使用制限を順守することを信用して頼りにする。例えば、第２のデバイスにおける「ＩＤセレクタ」または他のユーザインタフェースが、使用制限に従って有効期限が切れていない、またはそれ以外で使用不可になっていないカードだけをユーザに提示するようにプログラミングされることが可能である。

【００４５】

時間ベースの使用制限が、第２のデバイスに供給されるＤＩＲコピーの中に含められるべき場合、このＤＩＲを供給するデバイスは、内部クロックを使用して、使用制限をプログラミングすることが可能である。図３に示される実施形態において、デバイス（例えば、第１のデバイス）は、内部タイミング機構を欠いており、前述した仕方で第２のデバイスの要求の中のタイムスタンプに基づいて使用制限を設定する（３６０）。

【００４６】

ステップ３７０で、要求されるＤＩＲを裏付けるデータを含めるかどうかの決定が、行われる。裏付けデータを含めるかどうかは、本人からの要求に基づいて、またはそれ以外で決定されることが可能である。裏付けデータには、依拠当事者によって要求される主張を含む実際のデータが含まれる。例えば、ＤＩＲは、或る特定の依拠当事者に関するＩＤトークンの中に含められることが要求される主張のタイプ（例えば、社会保障番号、電話番号などに関するフィールド）をリストアップするメタデータを含むことが可能である。裏付けデータは、ＤＩＲを受信したことに応答して、ＩＤプロバイダによってＩＤトークンの中に符号化される実際の社会保障番号、電話番号などを含む。

【００４７】

通常、裏付けデータは、裏付けデータがセンシティブな個人情報であるため、ＤＩＲと一緒に供給されず、ＤＩＲを使用して、ＩＤプロバイダからのセキュリティで保護されたＩＤトークンの中で利用可能な裏付けデータが表される。このことは、裏付けデータが不必要に格納される、または転送されることを防ぐ。しかし、実施形態において、第１のデバイスは、ＩＤトークンを生成する、または暗号化する計算能力を欠いている可能性があり、さらに本人が、ＩＤプロバイダ（必要なＩＤトークンのプロバイダ）の役割をすることができる第２のデバイスに、ＤＩＲと、ＤＩＲの裏付けデータの両方を転送することを所望する可能性がある。

【００４８】

裏付けデータが、ＤＩＲと一緒に付けられるべきでない場合、ＤＩＲが、供給される（３８０）。実施形態において、ステップ３８０は、第１のデバイスから第２のデバイスにＤＩＲを送信することを含む。他の実施形態では、ステップ３８０は、第２のデバイスにＤＩＲを送信するよう第３のデバイスに指示すること、または第２のデバイスに、第３のデバイス上に格納されたＤＩＲへのポインタまたは参照を供給することを含む。裏付けデータがＤＩＲと一緒に付けられるべき場合、ＤＩＲと裏付けデータが、同様に供給される（３９０）。

【００４９】

図４は、ＤＩＲの使用をコントロールする方法４００を示す。ステップ４１０で、ＤＩＲを使用する要求が、受信される。実施形態において、第１のデバイスのユーザが、ＤＩＲを使用する要求を受信する。第１のデバイスのユーザは、この要求を行うデバイスのユーザと異なっていても、同一であってもよい。例えば、或る子供が、或る依拠当事者において特定の操作を実行するのにＤＩＲを使用する許可を、親から得ることを要求される可能性がある。ＤＩＲを使用する要求は、本人によってコントロールされるデバイスからであること、またはＩＤトークンを獲得しようと試みてＤＩＲを受信したＩＤプロバイダからであることが可能である。

【００５０】

ＤＩＲは、ＩＤプロバイダにＤＩＲを送信しようと試みているデバイスがまず、或る特定の個人、または或る特定のデバイスから許可を得ることを要求するようにプログラミングされることが可能である。例えば、本人によって、依拠当事者と対話するのに使用されているデバイスが、或るＩＤプロバイダにＤＩＲを送信するのに先立って、そのＤＩＲを使用する許可を求めるよう要求されることが可能である。また、ＤＩＲは、ＤＩＲを受信するＩＤプロバイダに、そのＤＩＲを使用する許可が、或る特定の個人、または或る特定のデバイスから得られてからでないと、ＩＤプロバイダは、要求するデバイスにＩＤトークンを供給することを許可されないと通知するようにプログラミングされることも可能である。許可を求める要求は、許可を与える（パスワードを介して、生体認証を介して、ま

たはそれ以外で）ように目標に定められたユーザをまず、認証することを含むことが可能であり、あるいは誰であれ、許可を求める要求が送信されるデバイスを、その時点でコントロールしている人からの承認の表示だけしか要求しないことも可能である。

【００５１】

実施形態において、ＤＩＲを使用する（ＩＤトークンを獲得するように）要求を受信するデバイスのユーザが、ＤＩＲの意図される使用と関係する情報を要求することが可能である（４２０）。例えば、ＤＩＲを使用する要求を承認するように求められるユーザは、本人によって或る操作を実行することが試みられている依拠当事者の名前、その要求される操作が何であるか、ならびにその操作と関係する他の情報を知ることを所望する可能性がある。ステップ４３０で、ＤＩＲの意図される使用と関係する情報が、受信される。排他的でない例として、この情報には、オンライン商店主の名前（依拠当事者）、試みられる購入（操作）、および意図される取引の価格／費用（操作固有のパラメータ）が含まれることが可能である。また、この情報には、ＤＩＲの説明的な名前（例えば、「Ｍｏｍ’ｓ　Ｖｉｓａ　Ｃａｒｄ」）が含まれることも可能である。この情報は、ユーザが、その要求を受け付けるかどうかを決定する（４４０）のを助けることが可能である。受け付けない場合、その要求を拒否するメッセージが、供給される（４４５）。受け付ける場合、そのＤＩＲを使用する許可が、供給される（４５０）。ステップ４４５における要求の拒否、またはステップ４５０における要求の許可は、要求するデバイスに、またはＩＤプロバイダに（直接に、または要求するデバイスを介して）供給されることが可能である。

【００５２】

図５は、ＤＩＲを獲得して、使用するための方法５００を示す。この実施形態において、方法は、依拠当事者にアクセスする要求から始まる（５１０）。アクセスする要求は、依拠当事者のセキュリティで保護された領域（セキュリティで保護されたＷｅｂページなどの）に入る要求、または依拠当事者において或る特定の操作を実行する要求であることが可能である。ステップ５２０で、ＩＤトークンを求める要求が、受信される。例えば、依拠当事者は、依拠当事者へのアクセスを要求したデバイスに、最小の主張セットを含むＩＤトークンを求める要求を含む、依拠当事者に関するセキュリティポリシで応答することが可能である。

【００５３】

ステップ５３０で、ＤＩＲを求める要求が、行われる。ＤＩＲを求める要求は、実施形態において、或る特定のＤＩＲを求める要求、または依拠当事者のセキュリティポリシによって要求される最小の主張セットを満たすＤＩＲを求める要求であることが可能である。このＤＩＲが、ステップ５４０で受信され、このＤＩＲを使用する要求が、ステップ５５０で送信される。ステップ５５０における、このＤＩＲを使用する要求は、このＤＩＲを獲得する要求とは異なるデバイスもしくはエンティティに対して行われることが可能である。例えば、本人が、本人の移動電話機上にＤＩＲを格納し、或るＤＩＲが、使用のために公共ＰＣにダウンロードされることを要求することが可能である。しかし、このＤＩＲは、このＤＩＲが、ＩＤトークンを獲得するのに使用されることが可能であるのに先立って、別のデバイスの別の個人もしくはユーザの許可を要求するようにプログラミングされることが可能である。

【００５４】

ステップ５６０で、このＤＩＲを使用する許可が、受信される。図５に示される実施形態では、このＤＩＲを使用する許可は、ＤＩＲが、ステップ５７０でＩＤプロバイダに送信されるのに先立って、受信される（５６０）。他の実施形態では、ＤＩＲは、ＩＤプロバイダに送信され、ＩＤプロバイダは、ＩＤトークンを供給するのに先立って、このＤＩＲを使用する許可を要求し、受信する。ステップ５８０で、ＩＤトークンが、依拠当事者に供給される。実施形態において、ＩＤトークンは、ＩＤプロバイダによって依拠当事者に直接に供給される。他の実施形態では、ＩＤトークンは、依拠当事者へのアクセスを要求するデバイスに供給され、このデバイスが、そのＩＤトークンを依拠当事者に転送する。さらに、本明細書で使用される「ＩＤトークンを供給する」には、依拠当事者が、ＩＤ

プロバイダまたは他のデバイスからＩＤトークンを得るのに使用することができる、ＩＤトークンへのポインタまたは参照を供給することが含まれる。実施形態において、ＩＤプロバイダと依拠当事者の間の通信パスは、要求するデバイス経由で依拠当事者に至るパスと比べて、より信頼できる、またはより堅牢であることが可能である。

【００５５】

さらに、実施形態において、ＤＩＲを獲得する要求とＤＩＲを使用する要求は、単一のデバイスに対して同時に行われてもよい。例えば、本人が、依拠当事者へのアクセスを得ることを求め、或るＤＩＲを獲得して、使用する要求を第１のデバイスに送信した場合、第１のデバイスは、そのＤＩＲを獲得する要求、およびそのＤＩＲを使用する要求が受け付けられたかどうかをユーザに指示することができる。受け付けられ、さらにそのＤＩＲが、自己発行される場合、第１のデバイスは、本人によって使用されているデバイスに、依拠当事者のセキュリティポリシを満たすＩＤトークンで応答することができる。他の実施形態では、このことは、そのＤＩＲを開放するかどうかの決定に対する、そのＤＩＲが、ＩＤトークンを獲得するのに使用されることが可能であるかどうかの決定に、異なるユーザ、または異なるデバイスが関与するため、該当しない。

【００５６】

ステップ５９０で、依拠当事者へのアクセスが、獲得される。例えば、依拠当事者のセキュリティポリシを満たす或るＩＤトークンが、ステップ５８０で供給された場合、本人は、依拠当事者において、要求される操作を実行することを許される。

【００５７】

図６は、ＤＩＲが、或る特定の文脈において獲得されて、使用される方法６００の実施形態を示す。ステップ６１０で、本人が、ＰＣから、依拠当事者Ｗｅｂサイトにおける支払いサイトへのアクセスを要求する。ステップ６２０で、依拠当事者が、本人と関係する最小主張セットを有するＩＤトークンを要求する。本人は、ＰＣを使用して、本人が、本人の移動デバイス上に格納している、この依拠当事者のためのＤＩＲを要求する（６３０）。本人は、本人の移動デバイス上で、このＤＩＲを求める要求に関して指示され（６４０）、本人は、この要求を受け付ける。すると、本人の移動デバイスは、本人によって、その時点で使用されているＰＣに、要求されたＤＩＲを送信する（６５０）。

【００５８】

ステップ６５５で、ＰＣは、そのＤＩＲを、そのＤＩＲの中で指定されたＩＤプロバイダに送信する。この例示的な実施形態において、ＩＤプロバイダは、第三者ＩＤプロバイダであり、ＤＩＲは、「管理されたＤＩＲ」である。ＩＤプロバイダは、ＩＤトークンを獲得するのに、そのＤＩＲを使用する許可の証明を本人から要求する（６６０）。ＰＣは、使用する許可の証明を求める要求を、そのＤＩＲの中で指定された第三者デバイスに転送する（６６５）。この例示的な実施形態では、本人は、ティーンエージャであり、ＤＩＲは、本人の母親のセルラー電話機上で母親からの許可を求めるようＩＤプロバイダに指示する。本人の母親は、母親のセルラー電話機を使用して、そのＤＩＲの意図される使用に関するさらなる情報を要求する（６７０）。

【００５９】

ステップ６７５で、ＰＣは、要求された情報を、本人の母親によってコントロールされる第三者デバイスに供給する。この実施例では、ＰＣは、依拠当事者の名前、予期される操作（例えば、品物の代金の支払い）、操作固有のパラメータ（例えば、品物の価格）を提供する。ステップ６８０で、本人の母親が、母親のセル電話機を使用して、そのＤＩＲを使用する要求を受け付け、さらにその趣旨のメッセージを、ＰＣを介してＩＤプロバイダに送信する。すると、ＩＤプロバイダは、依拠当事者にＩＤトークンを供給し（６８５）、さらに本人が、依拠当事者において、要求される操作を完了することを許される（６９０）。

【００６０】

図７は、本明細書で説明される実施形態を実施するのに使用されることが可能な汎用コンピューティングデバイス７００（本明細書でデバイス、コンピュータ、またはコンピュ

ータシステムとも呼ばれる）を示す。コンピューティングデバイス７００は、コンピューティング環境の一例に過ぎず、コンピュータアーキテクチャおよびネットワークアーキテクチャの用法または機能の範囲について何ら限定を示唆することも意図していない。また、コンピューティングデバイス７００が、例示的なコンピューティングデバイス７００に示される構成要素のいずれの１つ、または組み合わせと関係する依存関係または要件を有すると解釈されるべきでもない。実施形態において、コンピューティングデバイス７００は、図１に関連して前述したとおり、例えば、第１のデバイス１０５として、第２のデバイス１１１として、第３のデバイス１１７として、ＩＤプロバイダ１１５として、または依拠当事者１２０として使用されることが可能である。

【００６１】

最も基本的な構成において、コンピューティングデバイス７００は、通常、少なくとも１つの処理装置７０２、およびメモリ７０４を含む。コンピューティングデバイスの厳密な構成およびタイプに応じて、メモリ７０４は、揮発性（ＲＡＭなどの）、不揮発性（ＲＯＭ、フラッシュメモリなどの）、またはこの２つの何らかの組み合わせであることが可能である。この最も基本的な構成が、図７に破線７０６で示される。システムメモリ７０４は、コンピューティングデバイス７００上で実行されているアプリケーションを格納する。アプリケーションに加えて、メモリ７０４は、図１～図６に関連して説明されるとおり、ＤＩＲ使用要求７１０および／またはＤＩＲ入手要求７１１などの、コンピューティングデバイス７００によって実行されている、動作中に使用されている情報を格納することもできる。

【００６２】

さらに、コンピューティングデバイス７００は、さらなるフィーチャ／機能を有することも可能である。例えば、コンピューティングデバイス７００は、磁気ディスクもしくは磁気テープ、または光ディスクまたは光テープを含むが、以上には限定されない追加のストレージ７０８（リムーバブルなストレージおよび／またはリムーバブルでないストレージ）を含むことも可能である。そのような追加のストレージが、図７にストレージ７０８によって示される。コンピュータ記憶媒体には、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの情報を格納するために任意の方法、または任意の技術で実施された揮発性媒体および不揮発性媒体、リムーバブルな媒体およびリムーバブルでない媒体が含まれる。メモリ７０４およびストレージ７０８が、コンピュータ記憶媒体の例である。コンピュータ記憶媒体には、ＲＡＭ、ＲＯＭ，ＥＥＰＲＯＭ、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、ＤＶＤ（デジタルバーサタイルディスク）または他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージまたは他の磁気記憶装置、あるいは所望される情報を格納するのに使用されることが可能であり、コンピューティングデバイス７００によってアクセスされることが可能な他の任意の媒体が含まれるが、以上には限定されない。任意のそのようなコンピュータ記憶媒体が、コンピューティングデバイス７００の一部であることが可能である。

【００６３】

当業者には認識されるとおり、ストレージ７０８は、様々な情報を格納することができる。他のタイプの情報もあるなかで、とりわけ、ストレージ７０８は、デジタルＩＤ表現７３０またはＩＤトークン７４５を格納することができる。

【００６４】

また、コンピューティングデバイス７００は、システムが、他のデバイスと通信することを可能にする通信接続７１２を含むことも可能である。通信接続７１２は、通信媒体の例である。通信媒体は、通常、搬送波などの変調されたデータ信号、または他のトランスポート機構で、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータを実体化し、あらゆる情報配信媒体を含む。「変調されたデータ信号」という用語は、信号内に情報を符号化するように特性の１つまたは複数が設定または変更された信号を意味する。例として、限定としてではなく、通信媒体には、有線ネットワークまたは直接有線接続などの有線媒体、ならびに音響媒体、ＲＦ媒体、赤外線媒体、およびその他の

無線媒体などの無線媒体が含まれる。本明細書で使用されるコンピュータ可読媒体という用語には、記憶媒体と通信媒体がともに含まれる。

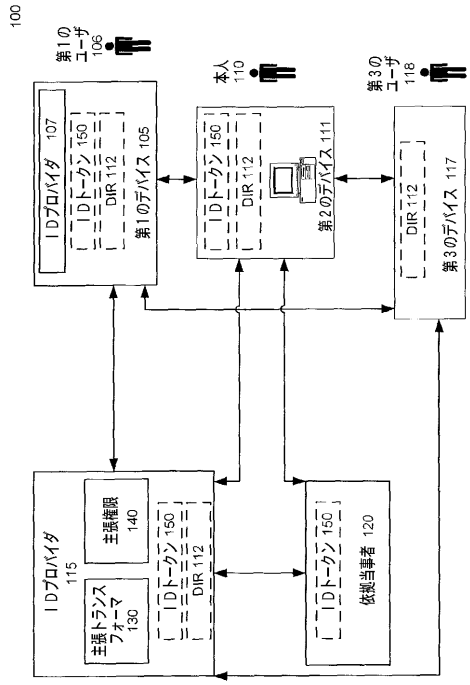
【００６５】

コンピューティングデバイス７００は、キーボード、マウス、ペン、音声入力デバイス、タッチ入力デバイスなどの入力デバイス７１４を有することも可能である。また、ディスプレイ、スピーカ、プリンタなどの出力デバイス７１６が、含まれることも可能である。これらすべてのデバイスは、当技術分野でよく知られており、本明細書で詳細に説明される必要はない。

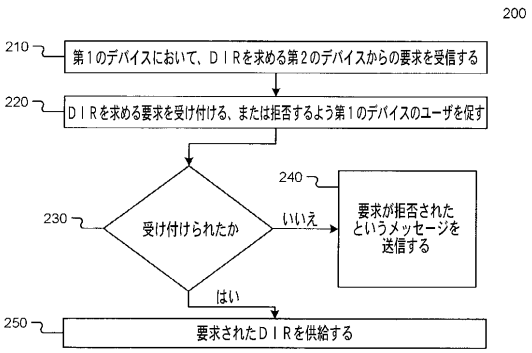
【００６６】

前述した様々な実施形態は、単に例として与えられ、限定するものと解釈されるべきではない。本開示、または添付の特許請求の範囲の真の趣旨および範囲を逸脱することなく、前述した実施形態に行われることが可能である様々な変形および変更が、当業者には容易に認識されよう。

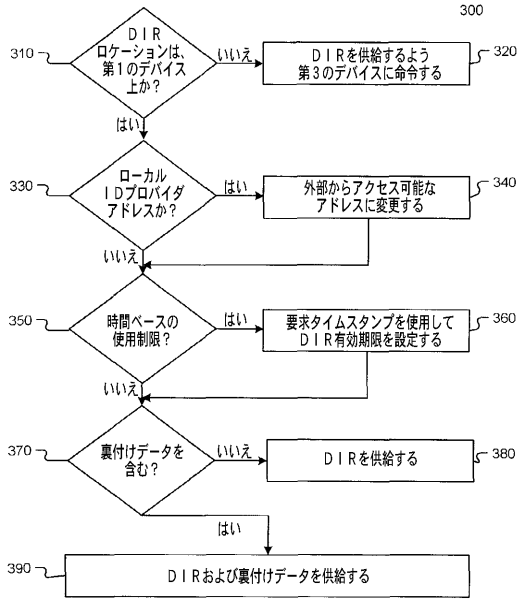
【図１】



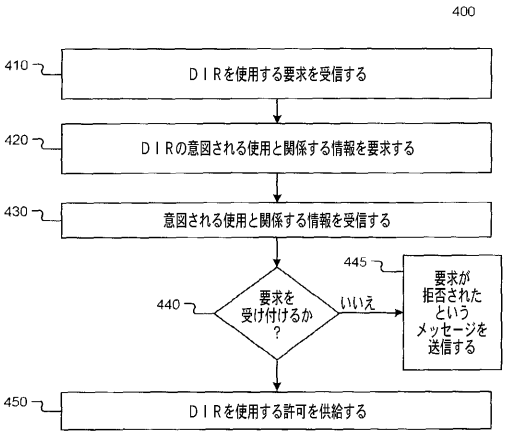
【図２】



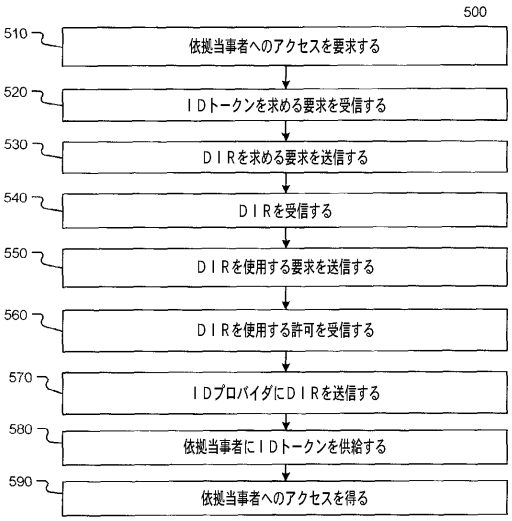
【図３】


300
310
ＤＩＲロケーションは、第１のデバイス上か？
いいえ
ＤＩＲを供給するよう第３のデバイスに命令する
320
はい
330
ローカルＩＤプロバイダアドレスか？
はい
外部からアクセス可能なアドレスに変更する
340
いいえ
350
時間ベースの使用制限？
はい
要求タイムスタンプを使用してＤＩＲ有効期限を設定する
360
いいえ
370
裏付けデータを含む？
いいえ
ＤＩＲを供給する
380
はい
390
ＤＩＲおよび裏付けデータを供給する

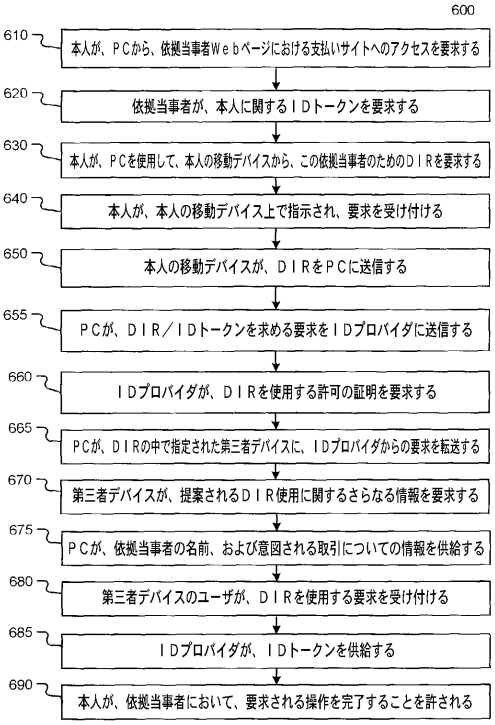
【図４】


400
410
ＤＩＲを使用する要求を受信する
420
ＤＩＲの意図される使用と関係する情報を要求する
430
意図される使用と関係する情報を受信する
445
要求が拒否されたというメッセージを送信する
440
要求を受け付けるか？
いいえ
450
ＤＩＲを使用する許可を供給する

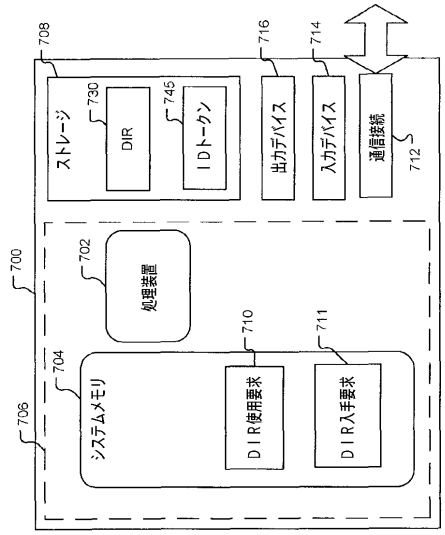
【図５】


500
510
依拠当事者へのアクセスを要求する
520
ＩＤトークンを求める要求を受信する
530
ＤＩＲを求める要求を送信する
540
ＤＩＲを受信する
550
ＤＩＲを使用する要求を送信する
560
ＤＩＲを使用する許可を受信する
570
ＩＤプロバイダにＤＩＲを送信する
580
依拠当事者にＩＤトークンを供給する
590
依拠当事者へのアクセスを得る

【図６】


600
610
本人が、ＰＣから、依拠当事者Ｗｅｂページにおける支払いサイトへのアクセスを要求する
620
依拠当事者が、本人に関するＩＤトークンを要求する
630
本人が、ＰＣを使用して、本人の移動デバイスから、この依拠当事者のためのＤＩＲを要求する
640
本人が、本人の移動デバイス上で指示され、要求を受け付ける
650
本人の移動デバイスが、ＤＩＲをＰＣに送信する
655
ＰＣが、ＤＩＲ／ＩＤトークンを求める要求をＩＤプロバイダに送信する
660
ＩＤプロバイダが、ＤＩＲを使用する許可の証明を要求する
665
ＰＣが、ＤＩＲの中で指定された第三者デバイスに、ＩＤプロバイダからの要求を転送する
670
第三者デバイスが、提案されるＤＩＲ使用に関するさらなる情報を要求する
675
ＰＣが、依拠当事者の名前、および意図される取引についての情報を供給する
680
第三者デバイスのユーザが、ＤＩＲを使用する要求を受け付ける
685
ＩＤプロバイダが、ＩＤトークンを供給する
690
本人が、依拠当事者において、要求される操作を完了することを許される

【図７】


708
716
714
ストレージ
730
DIR
745
IDトークン
出力デバイス
入力デバイス
通信接続
712
700
702
処理装置
710
711
704
システムメモリ
DIR使用要求
DIR入手要求
706

フロントページの続き

(74)代理人 100120112
弁理士 中西 基晴
(74)代理人 100147991
弁理士 鳥居 健一
(74)代理人 100119781
弁理士 中村 彰吾
(74)代理人 100162846
弁理士 大牧 綾子
(74)代理人 100173565
弁理士 末松 亮太
(74)代理人 100138759
弁理士 大房 直樹
(74)代理人 100091063
弁理士 田中 英夫
(72)発明者 ジョン シェウチュク
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション インターナショナル パテンツ内
(72)発明者 キム キャメロン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション インターナショナル パテンツ内
(72)発明者 アラン ナンダ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション インターナショナル パテンツ内
(72)発明者 ジャオ ジー
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション インターナショナル パテンツ内

審査官 平井 誠

(56)参考文献 特開２００３－３４６０５５（ＪＰ，Ａ）
特開２００４－３５６８１６（ＪＰ，Ａ）
特開２００６－２４４４７４（ＪＰ，Ａ）
特開２００２－０４１４６７（ＪＰ，Ａ）
特開２００３－３３７８０２（ＪＰ，Ａ）
特開２００１－２８２６２５（ＪＰ，Ａ）
特開２００２－２４５００６（ＪＰ，Ａ）
特開平１１－２５９７３３（ＪＰ，Ａ）
特開平０３－１５４１３７（ＪＰ，Ａ）
米国特許第０７３５６８３７（ＵＳ，Ｂ１）
Martin Goldack, Lesson learned: From MS Passport to CardSpace, ２００６年 7月 9日, p.1-13, internet:http://nds.hgi.rub.de/lehre/seminar/SS06/Goldack_PassportCardSpace.pdf(検索日2012年12月13日)

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｆ ２１