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

特許第6951329号
(P6951329)

(45)発行日　令和3年10月20日(2021.10.20)　(24)登録日　令和3年9月28日(2021.9.28)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675Z
G06F 21/64	(2013.01)	G06F	21/64	
G06F 21/62	(2013.01)	G06F	21/62	345
G06Q 10/06	(2012.01)	G06Q	10/06	326

請求項の数 30　(全 42 頁)

(21)出願番号　特願2018-519754 (P2018-519754)
(86)(22)出願日　平成28年10月14日 (2016.10.14)
(65)公表番号　特表2018-537022 (P2018-537022A)
(43)公表日　平成30年12月13日 (2018.12.13)
(86)国際出願番号　PCT/US2016/057232
(87)国際公開番号　WO2017/066715
(87)国際公開日　平成29年4月20日 (2017.4.20)
審査請求日　令和1年10月11日 (2019.10.11)
(31)優先権主張番号　62/241,436
(32)優先日　平成27年10月14日 (2015.10.14)
(33)優先権主張国・地域又は機関
米国 (US)
(31)優先権主張番号　62/264,418
(32)優先日　平成27年12月8日 (2015.12.8)
(33)優先権主張国・地域又は機関
米国 (US)

(73)特許権者　518126742
ケンブリッジ　ブロックチェーン，エルエルシー
アメリカ合衆国，マサチューセッツ州　02142，ケンブリッジ，ブロードウェイ　1，ケンブリッジ　イノベーション　センター
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦
(74)代理人　100134120
弁理士　内藤　和彦

最終頁に続く

(54)【発明の名称】デジタルアイデンティティを管理するためのシステム及び方法

(57)【特許請求の範囲】
【請求項１】
コンピュータシステムにより実行されるコンピュータ実施方法であって、
ポインタを用いて、分散台帳システムから、アイデンティティ所有者の少なくとも１つの属性について、少なくとも１つの証明にアクセスすることであって、前記少なくとも１つの証明は、前記少なくとも１つの証明の状態の表示とともに、前記分散台帳システムに記録されており、前記少なくとも１つの証明の前記状態は、少なくとも２つの状態から選択され、前記少なくとも２つの状態は、ＶＥＲＩＦＩＥＤ状態を含み、前記ＶＥＲＩＦＩＥＤ状態は、前記アイデンティティ所有者の前記少なくとも１つの属性の値が検証済みであることを示し、前記少なくとも１つの証明は、前記アイデンティティ所有者の前記少なくとも１つの属性の前記値に暗号学的一方向関数を少なくとも部分的に適用することにより得られる暗号学的証明を含む、ことと、
前記少なくとも１つの属性に対応する値を受信することと、
前記少なくとも１つの属性についての前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるか否かを、前記分散台帳システムに記録されている前記表示に基づいて、判断することと、
前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体を信用するかどうかを、信用済み実体のリストに基づいて、判断することと、
前記少なくとも１つの証明における前記暗号学的証明が前記少なくとも一つの属性に対応する前記受信した値の有効な証明であるか否かを、前記少なくとも一つの属性に対応す

る前記受信した値に前記暗号学的一方向関数を適用した結果に対して前記暗号学的証明を少なくとも部分的に比較することにより、判断することと、
前記少なくとも１つの証明が前記少なくとも１つの証明を照合する責任を持つ実体により電子署名されているか否かを判断することと、
（ａ）前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあること、（ｂ）前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体は信用されるべきものであること、（ｃ）前記暗号学的証明は、前記受信した値の有効な証明であること、及び（ｄ）前記少なくとも１つの証明が、前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体により電子署名されていることを判断することに応答して、前記アイデンティティ所有者と取引を進めることと、
を含むコンピュータ実施方法。
【請求項２】
請求項１に記載のコンピュータ実施方法であって、前記分散台帳システムは、少なくとも１つのブロックチェーンを用いて実装される、コンピュータ実施方法。
【請求項３】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明は、前記アイデンティティ所有者に関連するバッジに格納され、前記ポインタは、前記バッジへの参照を含む、コンピュータ実施方法。
【請求項４】
請求項３に記載のコンピュータ実施方法であって、前記バッジは、バッジについての複数のスキーマから選択されたスキーマに従って生成され、前記スキーマは、複数の属性を含み、前記複数の属性は、前記少なくとも１つの属性を含む、コンピュータ実施方法。
【請求項５】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＰＥＮＤＩＮＧ状態を含み、
前記コンピュータ実施方法は、前記実体が前記値の照合に成功することに応答して、前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体により、前記少なくとも１つの証明を前記ＰＥＮＤＩＮＧ状態から前記ＶＥＲＩＦＩＥＤ状態に遷移させることを更に含む、コンピュータ実施方法。
【請求項６】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＥＸＰＩＲＥＤ状態を含み、
前記コンピュータ実施方法は、前記少なくとも一つの属性の前記値が、前記値を照合する責任を持つ実体により、最後に照合されたときに設定されたタイマーの期限切れ後に、前記少なくとも１つの証明を前記ＶＥＲＩＦＩＥＤ状態から前記ＥＸＰＩＲＥＤ状態に遷移させることを更に含む、コンピュータ実施方法。
【請求項７】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるときに限り、前記少なくとも１つの証明における前記暗号学的証明へのアクセスが許可される、コンピュータ実施方法。
【請求項８】
請求項１に記載のコンピュータ実施方法であって、前記アイデンティティ所有者は、ユーザである、コンピュータ実施方法。
【請求項９】
請求項１に記載のコンピュータ実施方法であって、前記少なくとも１つの証明は、前記分散台帳システムに格納されているデジタルアイデンティティ表現からアクセスされ、前記デジタルアイデンティティ表現は、前記アイデンティティ所有者に関連し、且つ、前記少なくとも１つの証明の前記少なくとも２つの状態の間の遷移を管理する規則を実装するプログラムコードを含む、コンピュータ実施方法。
【請求項１０】

請求項１に記載のコンピュータ実施方法であって、前記少なくとも一つの属性に対応する前記値は、前記分散台帳システムの外部のチャンネルを介して受信される、コンピュータ実施方法。

【請求項１１】

システムであって、

少なくとも１つのプロセッサと、

少なくとも１つの非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つのプロセッサによって実行されたときに、前記少なくとも１つのプロセッサに、

ポインタを用いて、分散台帳システムから、アイデンティティ所有者の少なくとも１つの属性について、少なくとも１つの証明にアクセスすることであって、前記少なくとも１つの証明は、前記少なくとも１つの証明の状態の表示とともに、前記分散台帳システムに記録されており、前記少なくとも１つの証明の前記状態は、少なくとも２つの状態から選択され、前記少なくとも２つの状態は、ＶＥＲＩＦＩＥＤ状態を含み、前記ＶＥＲＩＦＩＥＤ状態は、前記アイデンティティ所有者の前記少なくとも１つの属性の値が検証済みであることを示し、前記少なくとも１つの証明は、前記アイデンティティ所有者の前記少なくとも１つの属性の前記値に暗号学的一方向関数を少なくとも部分的に適用することにより得られる暗号学的証明を含む、ことと、

前記少なくとも１つの属性に対応する値を受信することと、

前記少なくとも１つの属性についての前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるか否かを、前記分散台帳システムに記録されている前記表示に基づいて、判断することと、

前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体を信用するかどうかを、信用済み実体のリストに基づいて、判断することと、

前記少なくとも１つの証明における前記暗号学的証明が前記少なくとも一つの属性に対応する前記受信した値の有効な証明であるか否かを、前記少なくとも一つの属性に対応する前記受信した値に前記暗号学的一方向関数を適用した結果に対して前記暗号学的証明を少なくとも部分的に比較することにより、判断することと、

前記少なくとも１つの証明が前記少なくとも１つの証明を照合する責任を持つ実体により電子署名されているか否かを判断することと、

（ａ）前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあること、（ｂ）前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体は信用されるべきものであること、（ｃ）前記暗号学的証明は、前記受信した値の有効な証明であること、及び（ｄ）前記少なくとも１つの証明が、前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体により電子署名されていることを判断することに応答して、前記アイデンティティ所有者と取引を進めることと、

を実行させる複数の命令を記憶している、少なくとも１つの非一時的なコンピュータ読み取り可能な媒体と、

を備えるシステム。

【請求項１２】

請求項１１に記載のシステムであって、前記分散台帳システムは、少なくとも１つのブロックチェーンを用いて実装される、システム。

【請求項１３】

請求項１１に記載のシステムであって、前記少なくとも１つの証明は、前記アイデンティティ所有者に関連するバッジに格納され、前記ポインタは、前記バッジへの参照を含む、システム。

【請求項１４】

請求項１３に記載のシステムであって、前記バッジは、バッジについての複数のスキーマから選択されたスキーマに従って生成され、前記スキーマは、複数の属性を含み、前記複数の属性は、前記少なくとも１つの属性を含む、システム。

【請求項１５】

請求項１１に記載のシステムであって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＰＥＮＤＩＮＧ状態を含み、

前記複数の命令は、前記少なくとも１つのプロセッサによって実行されたときに、前記少なくとも１つのプロセッサに、前記実体が前記値の照合に成功することに応答して、前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体により、前記少なくとも１つの証明を前記ＰＥＮＤＩＮＧ状態から前記ＶＥＲＩＦＩＥＤ状態に遷移させることを更に実行させる、システム。

【請求項１６】

請求項１１に記載のシステムであって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＥＸＰＩＲＥＤ状態を含み、

前記複数の命令は、前記少なくとも１つのプロセッサによって実行されたときに、前記少なくとも１つのプロセッサに、前記少なくとも一つの属性の前記値が、前記値を照合する責任を持つ実体により、最後に照合されたときに設定されたタイマーの期限切れ後に、前記少なくとも１つの証明を前記ＶＥＲＩＦＩＥＤ状態から前記ＥＸＰＩＲＥＤ状態に遷移させることを更に実行させる、システム。

【請求項１７】

請求項１１に記載のシステムであって、前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるときに限り、前記少なくとも１つの証明における前記暗号学的証明へのアクセスが許可される、システム。

【請求項１８】

請求項１１に記載のシステムであって、前記アイデンティティ所有者は、ユーザである、システム。

【請求項１９】

請求項１１に記載のシステムであって、前記少なくとも１つの証明は、前記分散台帳システムに格納されているデジタルアイデンティティ表現からアクセスされ、前記デジタルアイデンティティ表現は、前記アイデンティティ所有者に関連し、且つ、前記少なくとも１つの証明の前記少なくとも２つの状態の間の遷移を管理する規則を実装するプログラムコードを含む、システム。

【請求項２０】

請求項１１に記載のシステムであって、前記少なくとも一つの属性に対応する前記値は、前記分散台帳システムの外部のチャンネルを介して受信される、システム。

【請求項２１】

少なくとも１つのプロセッサにより実行されたときに、方法を実行する複数の命令が符号化された非一時的なコンピュータ読み取り可能な媒体であって、前記方法は、

ポインタを用いて、分散台帳システムから、アイデンティティ所有者の少なくとも１つの属性について、少なくとも１つの証明にアクセスすることであって、前記少なくとも１つの証明は、前記少なくとも１つの証明の状態の表示とともに、前記分散台帳システムに記録されており、前記少なくとも１つの証明の前記状態は、少なくとも２つの状態から選択され、前記少なくとも２つの状態は、ＶＥＲＩＦＩＥＤ状態を含み、前記ＶＥＲＩＦＩＥＤ状態は、前記アイデンティティ所有者の前記少なくとも１つの属性の値が検証済みであることを示し、前記少なくとも１つの証明は、前記アイデンティティ所有者の前記少なくとも１つの属性の前記値に暗号学的一方向関数を少なくとも部分的に適用することにより得られる暗号学的証明を含む、ことと、

前記少なくとも１つの属性に対応する値を受信することと、

前記少なくとも１つの属性についての前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるか否かを、前記分散台帳システムに記録されている前記表示に基づいて、判断することと、

前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体を信用するかどうかを、信用済み実体のリストに基づいて、判断することと、

前記少なくとも１つの証明における前記暗号学的証明が前記少なくとも一つの属性に対

応する前記受信した値の有効な証明であるか否かを、前記少なくとも一つの属性に対応する前記受信した値に前記暗号学的一方向関数を適用した結果に対して前記暗号学的証明を少なくとも部分的に比較することにより、判断することと、
前記少なくとも１つの証明が前記少なくとも１つの証明を照合する責任を持つ実体により電子署名されているか否かを判断することと、
（ａ）前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあること、（ｂ）前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体は信用されるべきものであること、（ｃ）前記暗号学的証明は、前記受信した値の有効な証明であること、及び（ｄ）前記少なくとも１つの証明が、前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体により電子署名されていることを判断することに応答して、前記アイデンティティ所有者と取引を進めることと、
を含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２２】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記分散台帳システムは、少なくとも１つのブロックチェーンを用いて実装される、非一時的なコンピュータ読み取り可能な媒体。
【請求項２３】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つの証明は、前記アイデンティティ所有者に関連するバッジに格納され、前記ポインタは、前記バッジへの参照を含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２４】
請求項２３に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記バッジは、バッジについての複数のスキーマから選択されたスキーマに従って生成され、前記スキーマは、複数の属性を含み、前記複数の属性は、前記少なくとも１つの属性を含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２５】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＰＥＮＤＩＮＧ状態を含み、
前記方法は、前記実体が前記値の照合に成功することに応答して、前記アイデンティティ所有者の前記少なくとも１つの属性の前記値を照合する責任を持つ実体により、前記少なくとも１つの証明を前記ＰＥＮＤＩＮＧ状態から前記ＶＥＲＩＦＩＥＤ状態に遷移させることを更に含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２６】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つの証明の前記少なくとも２つの状態は、ＥＸＰＩＲＥＤ状態を含み、
前記方法は、前記少なくとも一つの属性の前記値が、前記値を照合する責任を持つ実体により、最後に照合されたときに設定されたタイマーの期限切れ後に、前記少なくとも１つの証明を前記ＶＥＲＩＦＩＥＤ状態から前記ＥＸＰＩＲＥＤ状態に遷移させることを更に含む、非一時的なコンピュータ読み取り可能な媒体。
【請求項２７】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つの証明が前記ＶＥＲＩＦＩＥＤ状態にあるときに限り、前記少なくとも１つの証明における前記暗号学的証明へのアクセスが許可される、非一時的なコンピュータ読み取り可能な媒体。
【請求項２８】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記アイデンティティ所有者は、ユーザである、非一時的なコンピュータ読み取り可能な媒体。
【請求項２９】
請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも１つの証明は、前記分散台帳システムに格納されているデジタルアイデンティティ表

現からアクセスされ、前記デジタルアイデンティティ表現は、前記アイデンティティ所有者に関連し、且つ、前記少なくとも１つの証明の前記少なくとも２つの状態の間の遷移を管理する規則を実装するプログラムコードを含む、非一時的なコンピュータ読み取り可能な媒体。

【請求項３０】

請求項２１に記載の非一時的なコンピュータ読み取り可能な媒体であって、前記少なくとも一つの属性に対応する前記値は、前記分散台帳システムの外部のチャンネルを介して受信される、非一時的なコンピュータ読み取り可能な媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願

本出願は、米国特許法１１９条（ｅ）に基づき、２０１６年８月２８日に出願された米国仮出願番号６２／３８０，４６７「強固なデジタルアイデンティティへの取り組み（ＡＮ ＡＰＰＲＯＡＣＨ ＦＯＲ ＳＴＲＯＮＧ ＤＩＧＩＴＡＬ ＩＤＥＮＴＩＴＩＥＳ）」と題する発明の優先権を主張し、当該出願の全体が本明細書に参照により組み込まれる。本出願は、米国特許法１１９条（ｅ）に基づき、２０１６年４月２１日に出願された米国仮出願番号６２／３２５，８８０「ブロックチェーンエコシステムの文脈における相手方照合（ＣＯＵＮＴＥＲＰＡＲＴＹ ＣＨＥＣＫＳ ＩＮ ＴＨＥ ＣＯＮＴＥＸＴ ＯＦ Ａ ＢＬＯＣＫＣＨＡＩＮ ＥＣＯＳＹＳＴＥＭ）」と題する発明の優先権を主張し、当該出願の全体が本明細書に参照により組み込まれる。本出願は、米国特許法１１９条（ｅ）に基づき、２０１５年１２月８日に出願された米国仮出願番号６２／２６４，４１８「選択的情報共有プラットフォーム（ＳＥＬＥＣＴＩＶＥ ＩＮＦＯＲＭＡＴＩＯＮ ＳＨＡＲＩＮＧ ＰＬＡＴＦＯＲＭ」と題する発明の優先権を主張し、当該出願の全体が本明細書に参照により組み込まれる。本出願は、米国特許法１１９条（ｅ）に基づき、２０１５年１０月１４日に出願された米国仮出願番号６２／２４１，４３６「マルチブロックチェーンアプローチによるアイデンティティ管理（“ＩＤＥＮＴＩＴＹ ＭＡＮＡＧＥＭＥＮＴ ＷＩＴＨ Ａ ＭＵＬＴＩ－ＢＬＯＣＫＣＨＡＩＮ ＡＰＰＲＯＡＣＨ）」と題する発明の優先権を主張し、当該出願の全体が本明細書に参照により組み込まれる。

【背景技術】

【０００２】

実質的に全ての組織（例：官庁、健康管理施設、金融機関、小売業者、ソーシャルネットワーキングサービス提供者、雇用主等）は個人データの収集、保持を行う。銀行業や保険業などの、特定の管理の厳しい産業においては、顧客のアイデンティティ検証を行うために、厳格な「顧客確認」プロセスを確立することが組織に要求される。これらのプロセスはアイデンティティの盗難、金融詐欺、マネーロンダリング、及びテロ資金調達を防ぐ為に重要である。

【０００３】

このような埋蔵個人データは頻繁に金融、政治、又は他の理由により悪用される。多くの政府は市民を守るために組織による個人データの取扱い方法について規制を導入している。

【発明の概要】

【０００４】

いくつかの実施形態では、コンピューターに実装された方法であり：ユーザーから取得した複数の計測値を使用してユーザーの識別子を生成し、前述の識別子は前述の複数の計測値の暗号学的証明を含み；前述のユーザー識別子に関連付けられたデジタルアイデンティティ表現を生成し、前述のデジタルアイデンティティ表現は認証のための規則を実装するプログラムコードを含み；デジタルアイデンティティ表現の電子署名を生成し；そしてデジタルアイデンティティ表現及び電子署名を分散台帳システムに発行する、動作を含む方法が提供される。

【０００５】
いくつかの実施形態では、コンピューターに実装された方法であり、バッジ中の複数のスキーマからスキーマを選択し、前述のスキーマは複数の属性を含み；前述のスキーマによりユーザーのアイデンティティを認証するために使用するバッジを生成し、前述の生成動作は：複数の値を識別し、各値はスキーマ中の前述の複数の属性のうちのある属性に関連し；前述の複数の値のうち各値に対して少なくとも一つの暗号学的証明を生成し；そして前述の複数の値を検証するために信用済み実体を識別し；そして前述のバッジを分散台帳システムへ発行する動作を含む方法が提供される。
【０００６】
いくつかの実施形態では、コンピューターに実装された方法であり、分散台帳システムを介してバッジを検証する要求を受信し、前述のバッジは、それぞれがユーザーの複数の属性に関連する複数の属性証明を含み、各属性に対して、関連する属性証明は暗号学的証明を含み；分散台帳システムの外部のチャンネルを介してそれぞれが前述の複数の属性に関連する複数の値を受信し；前述の複数の属性の少なくとも一つの属性に対して：前述の少なくとも一つの属性に関連する前述の値はユーザーの前述の少なくとも一つの属性の正しい値であるのかを検証し；そして前述の少なくとも一つの属性に関連する前述の値が前述のユーザーの前述の少なくとも一つの属性の正しい値であるかどうかの照合に応答し、前述の分散台帳システムを介して、前述の少なくとも一つの属性に関連する前述の属性証明がＶＥＲＩＦＩＥＤ状態に変更する方法が提供される。
【０００７】
いくつかの実施形態では、コンピューターに実装された方法であり、分散台帳システムを介して、第一のバッジを検証する要求を受信し、前述の第一のバッジはそれぞれがユーザーの複数の属性に関連する複数の属性証明を含み、各属性に対して、関連する属性証明は暗号学的証明を含み；分散台帳システムの外部のチャンネルを介して、それぞれが前述の複数の属性に関連する複数の値を受信し；前述の複数の属性のうち少なくとも一つの属性に対して：前述の第一のバッジから、前述の少なくとも一つの属性に関連する第一の属性証明を識別し、前述の第一の属性証明は第一の暗号学的証明を含み；前述の第一の属性証明から、第二のバッジへのポインタを識別し；前述のポインタを使用して前述の第二のバッジへ前述の分散台帳からアクセスし；前述の第二のバッジから前述の第二のバッジを照合する責任を持つ実体及び前述の少なくとも一つの属性への第二の属性証明を識別し；前述の第二のバッジを照合する責任を持つ実体を信用するかどうかを判断し；前述の第二のバッジを信用するかの照合に責任を持つ前述の実体を信用するかどうかの判断に応答して：（１）第二の属性証明がＶＥＲＩＦＩＥＤ状態であり、（２）第二の暗号学的証明は前述の少なくとも一つの属性に関する値の有効な証明であり、（３）第二の属性証明は第二のバッジを検証する責任を持つ実体により電子署名されているかどうか、をチェックする方法が提供される。
【０００８】
いくつかの実施形態に基づき、実行された時に少なくとも一つのプロセッサが上記の方法のうち任意のものを実行するようプログラムする命令を記憶した、少なくとも一つのプロセッサ及び少なくとも一つのコンピューターにより読み取り可能な記憶メディアを含むシステムが提供される。
【０００９】
いくつかの実施形態に基づき、実行された時に少なくとも一つのプロセッサが上記少なくとも一つの方法を実行するようプログラムする命令を記憶したコンピューターにより読み取り可能な記憶メディア。
【図面の簡単な説明】
【００１０】
【図１】図１はいくつかの実施形態に基づくアイデンティティ管理システム１００の説明図である。
【図２】図２はいくつかの実施形態に基づく個人データサービス（ＰＤＳ）２００の説明

図である。
【図３】図３はいくつかの実施形態に基づくデジタルアイデンティティ表現（ＤＩＲ）３００の説明図である。
【図４】図４はいくつかの実施形態に基づく、属性証明の異なる状態の間の遷移を管轄する状態マシン４００の説明図である。
【図５】図５はいくつかの実施形態に基づく認証プロセス５００の説明図である。
【図６】図６はいくつかの実施形態に基づく信用構造６００の説明図である。
【図７】図７はいくつかの実施形態に基づく相手方照合プロセス７００の説明図である。
【図８】図８は、いくつかの実施形態に基づいた、プライバシー層要素（例：ＰＤＳ）におけるデータ変化、及びその結果としての信用層（例：ＤＩＲ）における状態変化のプロセス８００の説明図である。
【図９】図９はいくつかの実施形態に基づくネットワーク中の分散台帳発見機構９００の説明図である。
【図１０】図１０は本開示の任意の態様が実装され得るコンピューター１００００を模式的に表した説明図である。
【発明を実施するための形態】
【００１１】
本開示の態様はデジタルアイデンティティを管理するシステム及び方法に関する。
【００１２】
個人データの共有を制限するプライバシー規制に従うため、多くの組織は独自のデジタルアイデンティティ管理システムを実装している。発明者らはそのような取り組みは不十分だと認識し理解した。例えば、あるユーザーが、銀行口座、仲介口座、保険講座、退職金口座、医療保険講座、事業用口座等、作成しようとする口座のそれぞれについて別個のアイデンティティ検証プロセスを完了することを要求され得る。同様に、あるユーザーが、オフィスビル、学校のキャンパス、レクリエーションエリア等への立ち入り許可を得るために別個のアイデンティティ検証プロセスを完了することを要求され得る。各アイデンティティ検証の中で、ユーザーは同じ個人データ（例：名、姓、運転免許証番号、誕生日、社会保障番号等）の提供を要求され得る。ユーザーの負担となるアイデンティティ検証プロセスにおいては相互作用が遅延したり、及び／又はユーザーが相互作用を完了することをあきらめたりすることが起こり得る。従って、いくつかの実施形態では、アイデンティティ検証プロセスを単純化し、結果的にユーザー体験を向上させる技術が提供されている。
【００１３】
発明者らは組織の観点から見ても非効率性が存在することを認識し理解した。例えば、ある顧客が合衆国内のＡ銀行に既に口座を持っていて、ドイツのＡ銀行に口座を作成することを要求し得る。このような場合、Ａ銀行は合衆国内の口座を作成した時に既に顧客のアイデンティティが検証されたにもかかわらず、再度アイデンティティ検証を実行し得る。結果、冗長なプロセスが実行され、重複した記録が維持され、時間と資源（例：プロセッササイクル、記憶装置等）が無駄にされ得る。したがって、いくつかの実施形態では、適切なセキュリティレベルを維持しながら冗長性を削減する技術が提供されている。
【００１４】
Ｉ．　個人データサービス
いくつかの実施形態においては、ユーザーが一つ以上の項目の個人識別情報（ＰＩＩ）及び／又は他の個人データがある実体（例：別のユーザーまたは組織）とどのように共有されるのかを制御できるような、所有者中心のアイデンティティ管理アプローチが提供される。例えば、個人データサービス（ＰＤＳ）は個人データを記憶するために使用され、ユーザーが個人データ（例：一つ以上の項目の追加、削除、及び／又は変更）を管理するためのユーザーインターフェースを提供し得る。加えて、又は代わりに、ＰＤＳはモバイル又はウェブアプリケーション等のソフトウエアアプリケーションに呼び出される一つ以上のアプリケーションプログラミングインターフェース（ＡＰＩ）を提供し得る。例えば、

ユーザーがアプリをダウンロードし、口座を開こうとしたとき、アプリはアイデンティティ検証プロセスを開始するＰＤＳのＡＰＩを呼び出し得る。アプリはＰＤＳにどの実体が検証を要求しているのか、そして／又は個人データのどの項目が検証されるのかを通知し得る。

【００１５】

いくつかの実施形態では、例えばＰＤＳに記憶された個人データへのアクセスを制限するなど、プライバシーを防御するようプログラムされていることがあり得る。例えば、個人データを閲覧又は変更するためにＰＤＳにログインしようとしているユーザーを認証するには一つ以上の証明書が要求され得る。加えて、又は代わりに、ＰＤＳは、認証済みのユーザーに指示された場合にのみ、個人データの一つ以上の項目を実体と共有し得る。

【００１６】

いくつかの実施形態では、ＰＤＳは、ユーザーインターフェース、アプリケーションプログラミングインターフェース、データ管理、信用管理及び／又は他の機能だけでなく、ランタイム環境（例：ライブラリ、構成ファイル等）を含む仮想コンテナとして実装される。発明者らはＰＤＳをコンテナとして実装することにより異なるプラットフォームへの展開が容易になり得ることを認識し理解した。しかしながら、本開示の態様はＰＤＳをコンテナとして実装することに限定されず、他の実装もまた適切とされてもよいことは理解されるべきである。

【００１７】

ＩＩ．　信用構造

いくつかの実施形態では、認証（例：アイデンティティ認証）が可能になり、また複数の実体から信頼され、結果的に冗長性を削減するために信用構造が提供され得る。例えば、あるユーザーが第一の組織（例：車両管理局（ＤＭＶ）のような官庁）へのアイデンティティ検証プロセスを完了し、第二の組織（例：公益事業会社）での口座開設を行おうとしているとき、第二の組織へのアイデンティティ検証プロセスは、第二の組織が第一の組織を信用している限り大幅に単純化され得る。従って、いくつかの実施形態では、ある組織によって、個人データのある項目が別の組織により検証済かどうかを、その項目を再び検証せずとも単純にチェックできるようにする信用構造を実装する技術が提供される。

【００１８】

いくつかの実施形態では、信用構造は、個人データのどの項目がどの実体と共有及び／又は証明されるのかをユーザーが正確に特定できるよう提供されてもよい。例えば、第一の組織（例：ＤＭＶ）が個人データの複数の項目（例：誕生日、社会保障番号等）を検証したとき、各項目に対してそれぞれ別の証明が提供されてもよい。このように、ユーザーは後に第一の項目の証明（例：２１歳を超えている）を、第二の項目（例：社会保障番号、現住所、厳密な誕生日）の証拠を提出せずに第二の組織（例：アルコールを提供するバー）へ提出するかを、後から決定してもよい。

【００１９】

ＩＩＩ．　分散台帳

２００９年に導入されたビットコインプロトコルは、手形交換所が存在しなくてもデジタル通貨の提供を可能とするためにブロックチェーンを使用する。ブロックチェーンはネットワーク中の複数のノードで共有され、暗号学的に安全な方法で取引を記録しチェックするために使用される。例えば、新たな取引がブロックチェーンに結び付けられるが、過去の取引は暗号学的証明のチェーンを破らない限り代替されない。

【００２０】

ビットコインプロトコルは特定のルールを施行するためにブロックチェーンの改ざん防止プロパティを使用する。例えば、第一の実体がビットコインを第二の実体に送り、取引の記録がネットワークを通じて伝搬すれば、攻撃者がネットワーク中の処理能力の半分より多くをコントロールしない限り取引は覆すことができない。このように、第一の実体が既にビットコインを所有していないことを第三の実体が即座に発見するので、第一の実体はビットコインを二重に消費することはできない。

【００２１】
発明者らはブロックチェーンのような分散台帳がデジタル通貨以外のアプリケーションに使用できることを認識し理解した。例えば分散台帳は、認証（例：アイデンティティ認証）が複数の実体に渡って依存される信用構造を実装するために使われてもよい。いくつかの実施形態では、分散台帳は信用された実体による認証を記録し、結果的に他の実体が独立して認証の事実を検証する必要がなくなるために使用されてもよい。
【００２２】
ＩＶ．　アイデンティティ管理プロトコル
発明者らはデジタルアイデンティティ管理における様々な競合する懸念を認識し理解した。例えば、ユーザーのプライバシーを守るためにはユーザーの個人データへのアクセスが制限されること（例：個人データをユーザーが制御する仮想コンテナに記憶することにより）が理想的である。一方、攻撃者が容易に認証を偽装できないようにするためには認証を記録する透明な機構を使用する（例：ネットワーク中の複数のノードで再現される、公的に利用可能なデータ構造へ認証を記録する）ことが理想的である。従って、いくつかの実施形態では、ユーザーが、認証の透明度を維持すると同時にどの程度の個人データを共有するかを制御できる技術が提供されている。このように、信用構造は個人データを過剰に共有せずとも実装され得る。
【００２３】
いくつかの実施形態では、認証を記録する透明な機構上にプライバシー保護を実装することを可能にするアイデンティティ管理プロトコルが提供され得る。例えば信用層、プライバシー層、及びアプリケーション層の３つの層を含むプロトコルスタックが提供され得る。信用層は認証を記憶するための分散台帳を含み、プライバシー層は各ユーザーが制御する仮想コンテナを含み、アプリケーション層はアイデンティティ管理プロトコルをアイデンティティ及び／又は他の個人データの検証に使用する一つ以上のアプリケーションを含み得る。
【００２４】
いくつかの実施形態では、アイデンティティ管理プロトコルの異なる層において異なる型のデータが交換されてもよい。例えば、機密データ（例：ＰＩＩの項目及び／又は他の個人データ）はプライバシー層で（例：暗号通信を介して）交換され、一方非機密データ（例：ＰＩＩの項目の暗号学的証明及び／又は他の個人データ）は信用層で交換されてもよい。このようにして、信用層においてはプライバシーを妥協せずに高レベルの透明さが提供され得る。
【００２５】
いくつかの実施形態では、ユーザーが、組織に相対して、ＰＩＩの項目及び／又は他の個人データが他の実体とどのように共有されるかを制御でき、同時に信用された実体がＰＩＩ及び／又は他の個人データの正確性を証明する、アイデンティティ管理プロトコルが提供され得る。このようにして、あるユーザーは、個人データの一つ以上の項目の内どれが別の実体（例：別のユーザー）と共有されるかを正確に決定することが可能であってもよく、また該別の実体は該個人データの一つ以上の項目が一つ以上の信用できる実体（例：一つ以上の官庁及び／又は雇用主）により検証済みかどうかを、負担となる検証プロセス（例：パスポート、社会保障カード、給与明細表を物理的に確認する）を行うことなくチェックしてもよい。
【００２６】
上に紹介し以下詳細に議論する技術は任意の数多くの方法により実装されてもよく、技術は特定の実装方法に限定されないということは認められなければならない。実装の詳細例は説明のみを目的としてここに提供する。さらに、開示する技術は単独又は任意の組み合わせにより使用してもよく、本開示の態様は特定の技術や技術の組み合わせに限定されない。
【００２７】
Ｖ．　例示的実施形態の詳細な説明

図１はいくつかの実施形態に基づくアイデンティティ管理システム１００の説明図である。本例では、アイデンティティ管理システム１００は３つの層を持つアイデンティティ管理プロトコルスタックを含む。例えば、認証（例：アイデンティティ認証）を記憶する分散台帳１０２を持つ信用層があってもよい。加えて、又は代わりに、複数の個人データサービス（ＰＤＳ）１０５Ａ、１０５Ｂ、１０５Ｃ・・・を含むプライバシー層、及び／又は複数のアプリケーション１１５Ａ、１１５Ｂ、１１５Ｃ・・・を備えるアプリケーション層を含んでもよい。ＰＤＳはアプリケーションを介した取引（例：口座開設、購入等）に関わる各ユーザーの個人データを記憶してもよい。

【００２８】

いくつかの実施形態では、ＰＤＳはＰＩＩ及び／又は個人データを管理するソフトウエアプログラムを含んでもよい。例えば、ＰＤＳは、ソフトウエアプログラムが任意の環境で一貫して動作できるよう、ソフトウエアプログラムをファイルシステム中に内包する仮想コンテナとしてとして実装されてもよい。例えば、ファイルシステムはランタイムシステム、一つ以上のシステムツール、一つ以上のシステムライブラリ等を含んでもよい。しかしながら、本開示の態様は以上のようには限定されないことは認められなければならない。代わりに、又は加えて、ＰＤＳは単に、ファイルシステムは含まず、個人データ管理用ソフトウエアプログラムを含んでもよい。

【００２９】

いくつかの実施形態では、ＰＤＳは分散台帳１０２中のデジタルアイデンティティ表現（ＤＩＲ）と関連付けられてもよい。例えば、ＰＤＳ１０５Ａ、１０５Ｂ、１０５Ｃ・・・はＤＩＲ１１０Ａ、１１０Ｂ、１１０Ｃ・・・とそれぞれ関連付けられてもよい。いくつかの実施形態では、各個人はＰＤＳ及び関連するＤＩＲを制御してもよい。ＰＤＳは機密データ（例：ＰＩＩの項目、及び／又は他の個人データ）を記憶し、一方関連ＤＩＲは非機密データ（例：ＰＩＩ項目の暗号学的証明及び／又は他の個人データ）を記憶していてもよい。ＰＤＳ間は互いに通信し、機密データを安全な方法で共有し、一方、ＤＩＲは分散台帳１０２内に非機密データ（例：ＰＩＩ項目の暗号学的証明及び／又は他の個人データ）を記録してもよい。

【００３０】

いくつかの実施形態では、暗号学的証明は個人データの項目から既知の方法で求められ、該個人データの項目の正確性検証を行った、信用済み実体によって署名されてもよい。ユーザーが個人データの項目（例：社会保障番号）の共有を行った相手である実体は、申し立てられた暗号学的証明が該個人データの項目から実際に求められたかどうか、また暗号学的証明が信用済み実体（例：官庁または雇用主）により実際に署名されたかどうかを直ちにチェックしてもよい。しかし、他の実体が暗号学的証明のみから個人データの項目を再構成することは計算機的に実現不可能であり得る。このようにして、プライバシーと透明性という競合する目的が同時に達成され得る。

【００３１】

いくつかの実施形態では、分散台帳１０２はピアツーピアネットワーク内の複数のノード間で再現されるデジタル記録を含んでもよい。ノードは、同期プロトコルを実行してもよく、同期プロトコルでは、あるノードにおいてデジタル記録のローカルコピーに変更が行われ、デジタル記録はネットワークを通して伝搬し、伝搬に従って他のノードはそれぞれの持つ同じデジタル記録のコピーをアップデートする。

【００３２】

いくつかの実施形態では、分散台帳はブロックチェーンを使用して実装されてもよい。ブロックチェーンは、複数のブロックを含んでもよく、各ブロックは複数の取引を含んでもよい。いくつかの実施形態では、複数の取引が、例えば時間順に命令されてもよい。加えて、又は代わりに、複数のブロックは、各新規追加されたブロックが最新の直前のブロックと連結されるような順番に並べられてもよい。このような構造は改ざんへの耐性があり、従って、いくつかの実施形態では、与えられた取引が実際に行われたかどうか、及び／又はいつ行われたかを確かめるために使用されてもよい。例えばネットワーク中の、ブ

ロックチェーンを実装する全てのノード（又は充分な計算能力を持つノードのサブセット）が合意した場合にのみ、あるブロックがブロックチェーンへ追加されてもよい。

【００３３】

いくつかの実施形態では、ノード（時折マイナーと称される）を生成するブロックは、直前の最新のブロックに連結する新しいブロックの生成に計算能力を注ぎ込んでもよい。計算集約的数学パズル（例：特定の数のゼロが先頭に付加されたハッシュの原像を識別する）を最も速く解くことができるノードは内部デジタルアセット（例：ビットコイン）により報酬が与えられる。ある時点においてネットワーク内で提供可能な計算能力に従った複雑さの数学パズルが使用されてもよい。このようにして、ブロックは選択された時間窓において生成され、衝突が削減され得る。

【００３４】

本開示の態様は上に説明された例のようなプルーフ・オブ・ワーク・アプローチの使用に限定されないことは認められなければならない。いくつかの実施形態では、分散合意形成を実現するためにプルーフ・オブ・ステーク・アプローチが使用されてもよい。さらに、信用層を提供するために、イーサリアムやＨｙｐｅｒｌｅｄｇｅｒ　Ｆａｂｒｉｃを限定せず含む、任意の適切なブロックチェーン実装が使用されてもよい。

【００３５】

図２はいくつかの実施形態に基づくＰＤＳ２００の説明図である。例えば、ＰＤＳ２００は、図１に示すプライバシー層の説明図中のＰＤＳ１０５ＡからＣのうちの一つであってもよい。いくつかの実施形態では、ＰＤＳ２００は個人のユーザーにより、ユーザーのデジタルアイデンティティを管理するために使用されてもよい。一つの例として、ユーザーは会社の従業員であり、ユーザーの年間収入に対する暗号学的証明に対して、会社に署名を要求するためにＰＤＳ２００を使用してもよい。加えて、又は代わりに、会社は、暗号学的証明に署名するためにＰＤＳ２００に類似したＰＤＳを使用し、署名を分散台帳（例：図１に説明的に示した分散台帳１０２）へ発行してもよい。

【００３６】

別の例として、ユーザーは自動車販売業者の顧客であってもよく、ＰＤＳ２００をユーザーの年間収入を証明するために使用してもよい。加えて、又は代わりに、自動車販売業者は分散台帳から、ユーザーにより提供された、申し立てられた年間収入の暗号学的証明及び、申し立てられた暗号学的署名の申し立てられた署名を分散台帳（例：図１に説明的に示した分散台帳１０２）から探索するためにＰＤＳ２００に類似したＰＤＳを使用してもよい。自動車販売業者のＰＤＳは申し立てられた暗号学的証明がユーザーから提供された年間収入値から実際に求められたかどうか、また暗号学的証明が実際にユーザーの雇用主によって署名されたかどうかをチェックする。

【００３７】

いくつかの実施形態では、ＰＤＳ２００はユーザーインターフェース２０２及び個人データ管理要素２０８を含んでもよい。ユーザーインターフェース２０２及び個人データ管理要素２０８により、ユーザーがＰＩＩ及び／又は他の個人データを記憶させ、記憶データを管理（例：追加、削除、変更、共有等）することが可能になってもよい。いくつかの実施形態では、ユーザーインターフェース２０２は、記憶データ及びＰＤＳ２００の様々な機能へのアクセスを制限するために多要素認証機構を使用してもよい。

【００３８】

いくつかの実施形態では、個人データ管理要素２０８はユーザーインターフェース２０２を介して行われた動作の一部または全ての監査証跡を維持してもよい。これによりユーザーは任意の認可されていない動作（例：ユーザーから盗まれた証明書を使用した攻撃者による）を特定することが可能になり得る。加えて、又は代わりに、監査証跡は捜査員によりユーザーが不正行為に関わっていないかどうかを判断するために使用されてもよい。

【００３９】

いくつかの実施形態では、ユーザーインターフェース２０２及び個人データ管理要素２０８により、ユーザーが個人データの一つ以上の項目を特定し、そして／又は別の実体と

の共有を承認することが可能になってもよい。加えて、又は代わりに、個人データ管理要素２０８は、個人データの一つ以上の項目を別の実体と共有を管理するための一つ以上の規則を適用してもよい。例えば、ある規則は、一つ以上の条件を特定し、そして該一つ以上の条件が現在の文脈において満たされた時にトリガされてもよい。規則はさらに共有する個人データの一つ以上の項目、及び／又は個人データの一つ以上の項目が共有される一つ以上の実体を特定してもよい。いくつかの実施形態では、ユーザーはある規則がトリガされる時に毎回通知を受け、そしてユーザーの合意があった場合のみ提示された個人データの共有が実行されてもよい。しかし、いくつかの実施形態ではユーザーは個人データの共有を、特定の規則のもとに事前に承認してもよいため、上記は必要がない。

【００４０】

いくつかの実施形態では、ユーザーによってある規則が特定され、又はユーザーの行動及び／又はユーザーの行動が観察される文脈から時間と共に学習されてもよい（例：一つ以上の機械学習アルゴリズムを使用）。加えて、又は代わりに、一つ以上の個人データの項目に適切な規則は、該一つ以上の個人データの項目の正確性を認証する責任を持つ信用済み実体から引き出される。

【００４１】

図２に戻り、いくつかの実施形態においてＰＤＳ２００はＰＤＳ２００が一つ以上のアプリケーション（例：図１に説明用に示されたアプリケーション層内のアプリケーション１１５ＡからＣ）と相互作用を行うためのＡＰＩ２０６を含んでもよい。一つの例として、ＰＤＳ２００はユーザーの年間収入の証明を要求するために雇用主の給与管理アプリケーションと相互作用してもよい。別の例として、ＰＤＳ２００はユーザーの年間収入を証明するために自動車販売業者の融資事務アプリケーションと相互作用し得る。アプリケーションのその他の例は、契約への署名、教育状況の検証、クレジットスコアの検証、デジタルアクセス制御、物理アクセス制御等を限定せず含む。

【００４２】

いくつかの実施形態においてＰＤＳ２００は、ＰＤＳ２００が一つ以上のＰＤＳと通信を行い得るための通信管理要素２１０を含んでもよい（例：図１に説明用に示されたプライバシー層内のＰＤＳ１０５ＡからＣ）。一つの例として、ユーザーの年間収入の暗号学的証明への署名を雇用主へ要求するために、ＰＤＳ２００はユーザーの雇用主のＰＤＳと通信してもよい。別の例としては、ユーザーの年間収入を証明し、ユーザーが自動車ローンを獲得するために、ＰＤＳ２００は自動車販売業者のＰＤＳと通信を行ってもよい。

【００４３】

いくつかの実施形態においてＰＤＳ２００は、分散台帳（例：図１に説明用に示された分散台帳１０２）内に、ＰＤＳ２００がＤＩＲを管理し得るための信用管理要素２１２を含んでもよい（例：図１に説明用に示された信用層内のＤＩＲ１１０ＡからＣのうちの１つ）。例えば、信用管理要素２１２はＤＩＲを文脈情報（例：どのアプリケーションがＰＤＳ２００を呼び出しているか）に基づいて管理するためのプログラムロジックを含んでもよい。プログラムロジックは、例えば、ユーザーからユーザーインターフェース２０２を介して受けとった命令、ＡＰＩ２０６を介したアプリケーションからの入力、通信要素２１０を介して別のＰＤＳから受け取ったオフレジャー通信等に基づいて、ＤＩＲの状態変化を起こしてもよい。

【００４４】

いくつかの実施形態では、ＰＤＳ２００は一つ以上の分散台帳（例：図１に示された説明用分散台帳１０２）の直接参加者であってもよい。加えて、又は代わりに、ＰＤＳ２００は、ＰＤＳ２００に代わって一つ以上の分散台帳を管理する信用済み実体と相互作用してもよい。いくつかの実施形態では、ＰＤＳ２００が、システムの導入及び／又は適用の検討を限定せず含み、直接又は間接的に参加またはその双方が行われているかどうかを判断するために、一つ以上の判断基準が使用されてもよい。

【００４５】

ＰＤＳの実装の詳細を図２に示し、上に議論を行ったが、本開示の態様は特定の構成要

素、または構成要素の組み合わせ、または任意の構成要素の特定の配置に限定されないことは認められるべきである。例えば、いくつかの実施形態では、ローカルに記憶されたデータを管理するコアに基づいて動的に拡張可能な機能をサポートするようなＰＤＳが提供されてもよい。例えば、ＰＤＳは変化する要求（例：新しいユースケース及び／又はプロセスフロー）に直ちに順応することができるよう、モジュールアーキテクチャ（例：マイクロサービスアーキテクチャ）が使用されてもよい。

【００４６】

図３はいくつかの実施形態に基づくＤＩＲ３００の説明図である。例えば、ＤＩＲ３００は、図１に示す信用層の説明図中のＤＩＲ１１０ＡからＣのうちの一つであってもよい。いくつかの実施形態では、ＤＩＲ３００はＰＤＳ（例：図２に説明用に示されたＰＤＳ２００）によって制御されてもよい。

【００４７】

いくつかの実施形態では、ＤＩＲ３００は分散台帳（例：図１に説明用に示された分散台帳１０２）内に実装されてもよく、分散台帳内のＤＩＲ３００を参照するために識別子が使用されてもよい。図３に示した例では、ＤＩＲ３００はグローバルにユニークなアイデンティティ識別子（ＧＵＩＩ）３０２を使用して参照され、そのため分散台帳内の二つのＤＩＲが同じ識別子を共有することはない。いくつかの実施形態では、各ＤＩＲはＰＤＳによって制御され、ＤＩＲ用のＧＵＩＩは、ＰＤＳに関連したユーザーの一つ以上のメトリクスに基づいて生成される。メトリクスの組み合わせは、ある与えられた二人のユーザーのＤＩＲが同じＧＵＩＩを持つ可能性が非常に低く、そのため二人のユーザーが一つより多いＤＩＲを作成することが困難であるように選択されてもよい。メトリクスの例は、バイオメトリクス（例：指紋スキャン、網膜スキャン、声紋等）、行動メトリクス（例：位置履歴、歩行パターン、睡眠パターン等）等を限定せず含む。

【００４８】

いくつかの実施形態では、一つ以上の基礎となるメトリック値からＧＵＩＩを生成するために、暗号学的一方向関数が使用されてもよく、そのためにＧＵＩＩが公的に入手可能になっても、該一つ以上の値はプライベートなままとなってもよい。基礎となるメトリック値は、基礎となるメトリック値からのＧＵＩＩの生成に使用される一つ以上のアルゴリズムを指し示すメタデータと共に、関連するＰＤＳにより安全に記憶されてもよい。基礎となるメトリック値には高いレベルのセキュリティが課されてもよい。例えば、基礎となるメトリック値は他の実体と共有されなくてもよい。

【００４９】

いくつかの実施形態では、ＤＩＲは、非機密データへ関わる公的なデータリポジトリとしてふるまい、そのようなデータへのアクセスを管轄するロジックを含んでもよい。例えば、図３に示した例では、ＤＩＲ３００は一つ以上のバッジ３０６内に配置された非機密データと、ＤＩＲ３００を介して行われ得る動作を特定する動作及びイベント仕様３０４、及び／又はＤＩＲ３００の変化をトリガとし得るイベントを含む。例えば、透明性を提供するために、分散台帳を維持するステークホルダーは、ＤＩＲ３００に変更が行われたらその都度通知を受けてもよい。

【００５０】

いくつかの実施形態では、ＤＩＲ３００は、任意の時点で、複数の状態のうちの一つをとってもよい。例えば、ＤＩＲ３００中のバッジ３０６は、一つ以上の属性証明３１０を含み、ある属性証明はいくつかの状態のうち一つをとってもよい（例：ペンディング（PENDING）、検証済み（VERIFIED)、無効（INVALID）、期限切れ（EXPIRED）等）。ＤＩＲ３００の全体的な状態は、ＤＩＲ３００中の構成要素である属性証明の状態のうちいくつか、又は全てに依存してもよい。

【００５１】

いくつかの実施形態では、ＤＩＲ３００の第一の状態から第二の状態への変化は分散台帳内の取引を介して起こってもよい。取引が、分散台帳を維持するステークホルダーのうち多数によって一旦確認されれば、ＤＩＲ３００は別の取引が確認されるまで第二の状態

に留まってもよい。いくつかの実施形態では、ＤＩＲ３００の全ての状態変化は分散台帳に記録され、ステークホルダーから可視であってもよく、結果、透明な監査証跡となる。

【００５２】

いくつかの実施形態では、ＤＩＲ３００は状態遷移がトリガされる条件及び／又はどの実体がどの遷移をトリガするかを管轄する規則を含んでもよい。例えば、そのような規則はＤＩＲ３００の動作及びイベント仕様３０４によって獲得されてもよい。ＤＩＲ３００が設定され分散台帳を介して一旦展開されれば動作及びイベント仕様３０４中のプログラムロジックはもはや変更されず、分散台帳はＤＩＲ３００の状態変化が動作及びイベント仕様３０４へ合致することを保証してもよい。

【００５３】

いくつかの実施形態では、一つ以上の認可済みの実体のみが、ＤＩＲ３００の状態変化が起こる取引の作成を許可されてもよい。各取引は取引を作成する実体により署名されてもよい。このように、ＤＩＲ３００の状態変化は監査可能であってもよい。いくつかの実施形態では、複数の実体が状態変化に関わってもよい。全てまたは少なくとも閾値の数の実体が、ある時間間隔において署名を求められてもよく、さもなければ状態変化は確認されなくてもよい。

【００５４】

いくつかの実施形態では、ある属性が個人データの項目、個人データの項目の名前、及び／又は関連するメタデータを含んでもよい。例えば、直接属性は、名、姓、誕生日、出生地、パスポート番号、運転免許証番号、社会保障番号、住所、電話番号、保険識別番号、指紋スキャン、網膜スキャン、声紋等のＰＩＩのような項目を含んでもよい。間接属性は所有財産（例：車、不動産等）、財産の状態等のような他の個人データを含んでもよい。加えて、又は代わりに、間接属性（例：少なくとも２１歳）は直接属性（例：誕生日）から求められてもよい。

【００５５】

発明者らは属性値の正確性は、中央手形交換所に頼らずにプライバシーを守る方法で証明され得ることを認識し理解した。例えば、いくつかの実施形態では、属性値そのものに代わって属性値の偽名が、分散台帳に記憶されてもよい。このように、属性値に対する偽名は、属性値そのものをさらすことなくネットワーク中に複製されてもよい。

【００５６】

いくつかの実施形態では、属性値の偽名は暗号学的一方向関数を使用して計算される。例えば、図３の例を参照し、ＤＩＲ３００（例：図２に説明用に示された個人データ管理要素２０８）を制御するＰＤＳによって維持される一つ以上の属性は、データ源３１２に記憶される。いくつかの実施形態では、データ源３１２から属性が引き出され、属性値に暗号学的一方向関数を適用して属性値の証明を求める。証明及び／又は関連メタデータ（例：証明が生成された時刻を示すタイムスタンプ）は属性証明３１０に含まれてもよいが、値そのものは含まれない。このように、属性証明３１０は、属性の値をさらすことなく分散台帳に発行されてもよい。

【００５７】

発明者らは属性証明を粒度の細かい方法で管理する方法を提供することが望ましいと認識し理解した。したがって、いくつかの実施形態では、属性証明は、別々に管理される一つ以上のバッジ（例：図６に説明用に示したバッジ３０６）として配置される。

【００５８】

いくつかの実施形態では、ユーザーは、信用済み実体をバッジに責任を持つよう指定してもよい。バッジ中の各属性に対して、信用済み実体は、使用者から属性に対して提供される値の正確性検証を行い、バッジ中へ属性に対して提供される証明が実際にユーザーから提供された値から計算されたかどうかをチェックし、そして／又は証明への署名を行う。上に説明されたように、証明はバッジに含まれ、分散台帳に発行されるが、値そのものは発行されなくてもよい。官庁、雇用主、金融機関、教育機関など、任意の実体が信用済み実体となってもよい。

【００５９】
いくつかの実施形態では、バッジは複数のフィールドを持つデータ構造であってもよい。バッジの非限定例を以下に示す。

【表１】

```
{
      label:              “信用済み銀行による KYC”
      trustedParty:       “trusted_party_identifier”
      proofAlgo:          “PBKDF2_SHA256_100000_3”
      salt:               “081627c0583380...83d51cdfdb1c8”
      schemaURI:          “http://schemas.example.org/strictKYCSchema”
      attributes:        [
            {
                  label:              “名”
                  proof:              “db74c940d447e877d...cbc319bcfaeab97a”
                  state:              “PENDING”
                  confirmedAt:        “1469633204”
                  references:        [
                      {
                         badgeLabel:         “バッジＸ”
                         attributeLabel:     “名”
                         state:              “ACTIVE”
                      }
                  ]
             }
             {
                  label:              “姓”
                  proof:              “55b5c51f867018...187e39a768aa8231ac”
                  state:              “PENDING”
                  confirmedAt:        “1469633204”
                  references:        [
                      {
                         badgeLabel:         “badgeX”
                         attributeLabel:     “姓”
                         state:              “ACTIVE”
                      }
                  ]
             }
             {
                  label:              “ssn”
                  proof:              “efa5ff7eefcfbe4...e15edbb2095934aa0e0”
                  state:              “PENDING”
                  expiryPeriod:       “1_YEAR”
                  confirmedAt:        “1469633204”
             }
             { /* 属性定義が続く */ }
      ]
}
```

【００６０】

上の例において、バッジは「ｌａｂｅｌ」、「ｔｒｕｓｔｅｄＰａｒｔｙ」、「ｐｒｏ

ｏｆＡｌｇｏ」「ｓａｌｔ」、「ｓｃｈｅｍａＵＲＩ」、そして「ａｔｔｒｉｂｕｔｅｓ」等のフィールドを持つデータ構造である。いくつかの実施形態では、「ｌａｂｅｌ」フィールドはＤＩＲ中のバッジを一意的に指定してもよい。このようなフィールドはＤＩＲ内の異なるバッジに単にアクセスしてもよい。

【００６１】

いくつかの実施形態では、「ｔｒｕｓｔｅｄＰａｒｔｙ」フィールドは信用済み実体への参照を含んでもよい。いくつかの実施形態では、参照された信用済み実体はバッジへのアクセスを与えられ、参照された信用済み実体のみがバッジ内の属性証明の状態変更を行う認可をされてもよい。

【００６２】

いくつかの実施形態では、「ｐｒｏｏｆＡｌｇ」フィールドはバッジ内に記憶された一つ以上の暗号学的証明の計算に使用されたアルゴリズムを識別してもよい。アルゴリズムはハッシュ関数などの暗号学的一方向関数を活用してもよい。例として、例えば選択した疑似乱数の関数（例：ＳＨＡ２５６）、選択した数の議事乱数の関数の繰り返し（例：１０，０００回）、及び／又は選択した数の出力バイト数（例：３２）によりパスワードに基づいた鍵導出関数２（ＰＢＫＤＦ２）が使用されてもよい。しかし、本開示の態様は、暗号学的証明を計算するための如何なる特定のアルゴリズムの使用に限定されないことは認められなければならない。

【００６３】

いくつかの実施形態では「ｓａｌｔ」フィールドは暗号学的証明の計算時に暗号学的一方向関数への入力として使用するランダム値を格納してもよい。

【００６４】

いくつかの実施形態では「ｓｃｈｅｍａＵＲＩ」フィールドはバッジを作成するためのスキーマへの参照を含んでもよい。スキーマの非限定例を以下に示す。

【００６５】

いくつかの実施形態では、「ａｔｔｒｉｂｕｔｅｓ」フィールドは一つ以上の属性証明を含み、各属性証明はそれ自体が一つ以上のフィールドを持つデータ構造であってもよい。例えば、属性証明は「ｌａｂｅｌ」、「ｐｒｏｏｆ」、「ｓｔａｔｅ」、「ｅｘｐｉｒｙＰｅｒｉｏｄ」、「ｃｏｎｆｉｒｍｅｄＡｔ」、そして「ｒｅｆｅｒｅｎｃｅｓ」のようなフィールドを持っていてもよい。

【００６６】

いくつかの実施形態では、「ｌａｂｅｌ」フィールドはバッジ内の属性証明を一意的に指定することに使用されてもよい。

【００６７】

いくつかの実施形態では、「ｐｒｏｏｆ」フィールドは、認証中の属性の値の暗号学的証明を記憶していてもよい。例えば、「ｐｒｏｏｆＡｌｇ」フィールドで指定されたアルゴリズムを使用して、「ｓａｌｔ」フィールドに記憶されたランダム値を追加入力として暗号学的証明が計算されてもよい。

【００６８】

いくつかの実施形態では、「ｓｔａｔｅ」フィールドは属性証明の現在の状態を記憶してもよい。たとえば、任意の時点において、属性証明は以下のPENDING、VERIFIED、INVALID、またはEXPIRED、の状態のうちの一つをとってもよい。これらの状態の遷移を管轄する説明用の状態マシンを図４に示し、以下に説明する。

【００６９】

いくつかの実施形態では、「ｃｏｎｆｉｒｍｅｄＡｔ」フィールドはバッジが分散台帳に最後に確認された時間を示してもよい。

【００７０】

いくつかの実施形態では、「ｅｘｐｉｒｙＰｅｒｉｏｄ」フィールドは属性証明がＶＥＲＩＦＩＥＤ状態をとることができる時間の長さを示してもよい。例えば期限の日時はｅｘｐｉｒｙＤａｔｅ＝ｃｏｎｆｉｒｍｅｄＡｔ＋ｅｘｐｉｒｙＰｅｒｉｏｄにより計算さ

れてもよい。期限に到達したら、内部遷移がトリガされ、属性証明はＶＥＲＩＦＩＥＤからＩＮＶＡＬＩＤ状態へ移動してもよい。

【００７１】

いくつかの実施形態では、「ｒｅｆｅｒｅｎｃｅｓ」フィールドは別のバッジ中の関連する属性証明への参照を含んでもよい。例えば、「ｒｅｆｅｒｅｎｃｅｓ」フィールドは他のバッジのラベルを記憶する「ｂａｄｇｅＬａｂｅｌ」フィールド、他のバッジの参照された属性証明を記憶する「ａｔｔｒｉｂｕｔｅＬａｂｅｌ」フィールド、参照された属性証明の状態を示す「ｓｔａｔｅ」フィールド（例：ＡＣＴＩＶＥ、ＩＮＶＡＬＩＤＡＴＥＤ、ＥＸＰＩＲＥＤ等）を含んでもよい。

【００７２】

発明者らは、第一のバッジ中のある属性証明から、同じＤＩＲ中にある第二のバッジ中の関連する属性証明へ参照を行うことにより、第一のバッジに責任を持つ信用済み実体が第二のバッジ中の関連属性証明を信頼することが可能になることを認識し理解した。例えば、上の例では、ユーザーが「ｔｒｕｓｔｅｄＰａｒｔｙ」フィールドで指定される信用済み実体に属性証明中の「ｆｉｒｓｔｎａｍｅ」とラベル付けされた値（例：ジョン）を検証するよう要求したとき、信用済み実体は別のバッジ（例：「ｂａｄｇｅＸ」とラベル付けされたバッジ中の「ｆｉｒｓｔｎａｍｅ」とラベル付けされた属性）中の関連属性証明をチェックしてもよい。チェックが成功すれば、信用済み実体は、負担となる検証プロセス（例：ユーザーの名が本当にジョンであるかを確かめるためにパスポートを確認する）を行うことなく「ｆｉｒｓｔｎａｍｅ」とラベル付けされた属性証明中の「ｐｒｏｏｆ」フィールドに記憶された証明に署名してもよい。

【００７３】

いくつかの実施形態では、他のバッジ中の関連する属性証明をチェックするために、信用済み実体は「ｂａｄｇｅＬａｂｅｌ」フィールド（例：ｂａｄｇｅＸ）に記憶されたラベルを、該他のバッジを探索するために使用し、「ａｔｔｒｉｂｕｔｅＬａｂｅｌ」フィールド（例：「ｆｉｒｓｔｎａｍｅ」）に記憶されたラベルを該他のバッジ中の関連する属性証明を探索するために使用する。該信用済み実体は関連する属性が「ＶＡＬＩＤ」状態であることをチェックし、該他のバッジにおいて「ｐｒｏｏｆＡｌｇｏ」フィールドで示されたアルゴリズムをユーザーにより提供された属性値（例：ジョン）へ適用し、該他のバッジ中の「ｓａｌｔ」フィールドに記憶されたソルトを使用して関連属性証明中の「ｐｒｏｏｆ」フィールドに記憶された証明が実際に属性値と該ソルトに該アルゴリズムを適用して生成されたかを確認する。

【００７４】

いくつかの実施形態では、信用済み実体は、該信用済み実体が該他のバッジ内の「ｔｒｕｓｔｅｄＰａｒｔｙ」フィールドで指定された実体を信頼する場合のみ該他のバッジ中の関連属性証明を信頼してもよい。例えば、他のバッジ中の「ｔｒｕｓｔｅｄＰａｒｔｙ」フィールドで指定されたバッジが官庁である場合、信用済み実体は認証を信頼することを決定してもよく、一方他のバッジ中の「ｔｒｕｓｔｅｄＰａｒｔｙ」フィールドが個人や信用済み実体にとって未知の組織の場合、認証を信頼することを決定しなくてもよい。

【００７５】

発明者らは、属性証明をバッジへと編成することによる様々な利点を認識し理解したが、本開示の態様はここに提供される特定の例、またはバッジの用途に限定されないことは認められなければならない。いくつかの実施形態では、属性証明は異なる方法で編成され、または独立して管理されてもよい。

【００７６】

いくつかの実施形態では、パブリックなソルト及び／又は一つ以上のプライベートなソルトと組み合わせて、暗号学的一方向関数が使われてもよい。例えば、パブリックソルトは、バッジ内の全ての属性証明により共有されるランダム値であり、バッジの作成中に計算され、分散台帳へと発行されてもよい。そのようなパブリックソルトはバッジへの結合値として使用されてもよい。

【００７７】
対照的に、いくつかの実施形態では、プライベートソルトは、属性値が検証される度に、各属性に対して独立に計算されるランダム値であり、分散台帳へ発行されなくてもよい。信用済み実体が属性値を検証できるようにするためには、該属性に対して計算されたプライベートソルト及び該特定の検証結果は、属性値と共に安全なオフレジャーチャンネルを介して信用済み実体と共有されてもよい。
【００７８】
いくつかの実施形態では、属性値の暗号学的証明は以下のように計算されてもよい。
（１）public_salt = random(X)
ここで関数ｒａｎｄｏｍ（）に対するＸの入力により長さＸのランダムバイトシーケンスが出力される。
（２）private_salt = random(Y)
ここで関数ｒａｎｄｏｍ（）に対するＹの入力により長さＹのランダムバイトシーケンスが出力される。
（３）proof = HASH(public_salt || private_salt || attribute_value)
ここで||はバイトシーケンス連結関数である。
【００７９】
いくつかの実施形態では、ＨＡＳＨ（）関数は単純な暗号学的ハッシュ関数よりも複雑な一方向関数であってもよい。例えば、潜在的な攻撃者を減速させブルートフォース攻撃への抵抗力を高めるために、ＰＢＫＤＦ２アルゴリズムが強固なハッシュ関数（例：ＳＨＡ２５６）、十分に大きい積分（例：１０，０００）、及び／又は充分に大きい出力バイト数（例：３２）と組み合わせて使用されてもよい。しかし、本開示の態様は、特定の証明アルゴリズムの使用に限定されないことは認められなければならない。いくつかの実施形態では、同じＤＩＲ内においてさえも、異なる証明アルゴリズムが異なるバッジに使用されてもよい。
【００８０】
いくつかの実施形態では、安全性を向上させるため、ソルト値は少なくともＨＡＳＨ（）関数の出力と同じ数のビット数を持つように選択されてもよい。そのようなソルトはＰＤＳ内で独立して計算されてもよい。例えば、パブリックソルトはバッジにおいて再利用されず、プライベートソルトは属性証明において再利用されなくてもよい。
【００８１】
発明者らは、プライベートソルトを使用することにより、属性値が変更されなくても現存する認証の無効化が可能になり得ると認識し理解した。例えば、認証を行う実体（例：信用調査機関）は、新しいプライベートソルトを使用して同じ属性値の新たな証明を生成することにより、以前の証明を新しい証明で置き換えてもよい。しかしながら、本開示の態様はプライベートソルトの用途に限定されず、いくつかの実施形態においては、プライベートソルトが使用されず、結果全ての以前の証明が有効であり続けてもよい。また、本開示の態様はパブリックソルトの用途に限定されない。例えば、いくつかの実施形態では、プライベートソルトをパブリックソルトの代わりに使用してもよい。
【００８２】
いくつかの実施形態では、バッジスキーマ（バッジ中の「ｓｃｈｅｍａ」フィールドにて参照される）に基づいてバッジが作成されてもよい。バッジスキーマはどのデータがバッジに記憶されるか、データがどのように編成されるか、データ間の意味論的な関係、及び／又はデータがどのように管理されるかを管轄する規則を記述してもよい。いくつかの実施形態では、バッジスキーマはＷ３Ｃウェブ・オントロジー言語（ＯＷＬ）又はリソース・ディスクリプション・フレームワーク・スキーマ（ＲＤＦＳ）のような意味論的言語を用いて記述されてもよい。しかし、上記はいくつかの実施形態では、ＸＭＬのようなマークアップ言語も使用されるため要求はされない。バッジスキーマの非限定例を以下に示す。

【表２】

```
{
    Id: “http://schemas.example.org/strictKYCSchema”
    schemaType: “001 - 個人用のKYC”
    riskProfile: “低”
    description: “以下のスキーマは低リスクな個人の顧客確認（KYC）チェックに必要な属性を定義する。”
    attributes: [
        {
            label: “名”
            description: “特定された人物の名である。”
            required: true
            validationCriteria: “政府により発行された写真付き身分証明書の名と一致しなければならない。対面で、または安全なデジタルチャンネルを介して送信された写真付き身分証明書の高品質スキャンをもってチェック済み。”
            enhancedPrivacy: “ラベルは、『firstname』ラベルに対して関連する一方向でソルトされたハッシュにて置き換えることにより保護可能である。”
            storageLocation: “PDS”
            dataType: “String”
            format: “平文またはハッシュ化済み”
        }
        {
            label: “姓”
            required: true
            validationCriteria: “名をチェックするために使用された政府により発行された写真付き身分証明書の姓と一致しなければならない。対面で、または安全なデジタルチャンネルを介して送信された写真付き身分証明書の高品質スキャンをもってチェック済み。”
            enhancedPrivacy: “ラベルは、『姓』ラベルを関連する一方向でソルト値が付与されたハッシュにて置き換えることにより保護可能である。”
            storageLocation: “PDS”
            dataType: “String”
            format: “平文またはハッシュ化済み”
        }
        {
            label: “ssn”
            required: true
            validationCriteria: “社会保障番号は名と姓のチェックに使用された政府により発行された写真付き身分証明書と一致しなければならない。”
            enhancedPrivacy: “ラベルは、『ssn』ラベルを関連する一方向でソ
```

```
                    ルトされたハッシュにて置き換えることにより保護可能である。”
                    dataType: “String”
                    storageLocation: “PDS”
                    format: “平文またはハッシュ化済み”
                }
                { /* 属性定義が続く */ }
        ]
}
```

【００８３】
上の例では、バッジスキーマは、属性への証明がバッジ内に含まれるような属性の組を定義する。各属性証明はバッジが作成された時に配置されてもよく、または後にバッジに追加されてもよい。いくつかの実施形態では、バッジスキーマはどのように属性証明が管理されるかを管轄する一つ以上の規則を定義してもよい。例えば、規則により属性証明の期限は５年から１０年の間でなければならないと定義してもよい。
【００８４】
発明者らはバッジスキーマによりバッジが標準化された方法で作成されることを認識し理解した。これにより異なる目的のために作成されたバッジ間のマッピングを単純化し、同じ縦断関係（例：異なる金融機関）内または異なる縦断関係（例：乗客のアイデンティティを検証するために顧客確認またはＫＹＣスキーマを使用するＴＳＡのような官庁）にある異なるシステムの相互運用性を向上させ得る。しかし、本開示の態様は、バッジを作成するためのバッジスキーマの使用法に限定されないことは認められなければならない。
【００８５】
図４はいくつかの実施形態に基づく、属性証明の異なる状態の間の遷移を管轄する状態マシン４００の説明図である。例えば、状態マシン４００は、図３に示された一つ以上の説明用バッジ３０６中の属性証明の状態遷移を管轄してもよい。
【００８６】
いくつかの実施形態では、属性証明を使用してバッジが作成されたとき（または存在するバッジに属性証明が追加されたとき）、属性証明はＰＥＮＤＩＮＧ状態に初期化されてもよい。この状態では、属性証明は有効でも無効でもなくてよい。
【００８７】
いくつかの実施形態では、バッジが作成された対象であるユーザーは、バッジに関連付けられた信用済み実体へ、属性値の検証を要求してもよい。信用済み実体が属性値を検証すれば、信用済み実体は属性証明をＶＥＲＩＦＩＥＤ状態へと変更させてもよい。信用済み実体が属性値を拒否すれば、信用済み実体は属性証明をＩＮＶＡＬＩＤ状態へと変更させてもよい。
【００８８】
いくつかの実施形態では、属性証明はＶＥＲＩＦＩＥＤ状態、ＥＸＰＩＲＥＤ状態、またはＩＮＶＡＬＩＤ状態である時に、ユーザーが属性を異なる値に変更すれば、属性証明はＰＥＮＤＩＮＧ状態に戻ってもよい。
【００８９】
いくつかの実施形態では、属性証明がＶＥＲＩＦＩＥＤ状態であり、信用済み実体が以前の検証を取り消したら、信用済み実体は属性証明をＩＮＶＡＬＩＤ状態に変更してもよい。
【００９０】
いくつかの実施形態では、属性証明がＶＥＲＩＦＩＥＤ状態であり、有効期間が過ぎたら、属性証明はＥＸＰＩＲＥＤ状態へ変化し、属性証明は信用済み実体が再度属性値を検証するまでＥＸＰＩＲＥＤ状態に留まる。
【００９１】

状態マシン４００を図４中に示し、上に説明したが、説明のみを目的とし、本開示の態様は特定の状態及び／又は遷移に限定されないことは認められるべきである。

【００９２】

いくつかの実施形態では、参照先の属性証明の状態は、参照元の属性証明の状態と同期されてもよい。しかし、いくつかの実施形態においては、参照先の属性証明は参照元の属性証明の状態遷移と独立していてもよい。

【００９３】

上に議論されたように、ＤＩＲには状態変化がトリガされる条件及び／又はどの実体がどの遷移をトリガするかを管轄する規則が含まれてもよい。例えば、そのような規則は動作及びイベント仕様（例：図３に示す動作及びイベント仕様３０４）により獲得されてもよい。ＤＩＲを介して行われる動作（例：状態変化及び／又は証明のアップデート）の非限定例を下の表に示す。

【表３】

動作	入力／出力	属性状態	副作用
createBadge	入力 (1) バッジラベル (2) 信用済み実体 出力：なし	なし	「バッジ作成済イベント」がトリガされた
setAttribute	(1) バッジラベル (2) 属性ラベル (3) 属性証明	PENDING	「属性設定イベント」がトリガされた
submitVerificationRequest	入力 (1) バッジラベル 出力：なし	なし	「検証要求イベント」がトリガされた
changeAttributeState	入力 (1) バッジラベル (2) 属性ラベル (3) 属性状態 出力：なし	PENDING から VERIFIED 又は INVALID	「属性状態変更イベント」がトリガされた

【００９４】

いくつかの実施形態では、「ｃｒｅａｔｅＢａｄｇｅ」動作は、バッジラベル及び識別子を信用済み実体へ入力することとして実行されもよい。「ｃｒｅａｔｅＢａｄｇｅ」の動作を実行するユーザーのＤＩＲの結果として、「ｌａｂｅｌ」フィールドに入力バッジラベルを持ち「ｔｒｕｓｔｅｄＰａｒｔｙ」フィールドに信用済み実体の識別子を持つバッジが作成されてもよい。加えて、又は代わりに、新しく作成されたバッジを分散台帳へ発行する「Ｂａｄｇｅ　Ｃｒｅａｔｅｄ」イベントがトリガされてもよい。

【００９５】

いくつかの実施形態では、「ｓｅｔＡｔｔｒｉｂｕｔｅ」動作は、バッジラベル、属性ラベル、属性証明の入力となってもよい。ユーザーのＤＩＲが「ｓｅｔＡｔｔｒｉｂｕｔｅ」動作を実行した結果として、入力バッジラベルにより識別されるバッジの「ａｔｔｒｉｂｕｔｅｓ」フィールドがアップデートされてもよい。例えば、入力属性ラベルによって識別される属性証明は、「ｐｒｏｏｆ」フィールド中の入力属性証明をもって、追加及び／又は変更される。加えて、又は代わりに、属性証明の状態はＰＥＮＤＩＮＧに設定され、及び／又は分散台帳へ属性証明を発行する「Ａｔｔｒｉｂｕｔｅ　Ｓｅｔ」イベントがトリガされる。

【００９６】

いくつかの実施形態では、「ｓｕｂｍｉｔＶｅｒｉｆｉｃａｔｉｏｎＲｅｑｕｅｓｔ」動作は、バッジラベルの入力となってもよい。ユーザーのＤＩＲが「ｓｅｔＡｔｔｒｉｂｕｔｅ」の動作を実行すると、「Ｖｅｒｉｆｉｃａｔｉｏｎ　Ｒｅｑｕｅｓｔ」イベントがトリガされ、入力バッジラベルにより識別されるバッジへの責任を持つ信用済み実体のＤＩＲへと検証要求が送信される。

【００９７】

いくつかの実施形態では、「ｃｈａｎｇｅＡｔｔｒｉｂｕｔｅＳｔａｔｅ」動作は、バッジラベル、属性ラベル、属性状態（例：ＶＥＲＩＦＩＥＤまたはＩＮＶＡＬＩＤ）の入力となってもよい。信用済み実体のＤＩＲが「ｃｈａｎｇｅＡｔｔｒｉｂｕｔｅＳｔａｔｅ」動作を実行した結果として、入力バッジラベルにより識別されるバッジの「ａｔｔｒｉｂｕｔｅｓ」フィールドがアップデートされてもよい。例えば、入力属性ラベルによって識別される属性証明は、「ｓｔａｔｅ」フィールド中の入力属性状態（例：ＶＥＲＩＦＩＥＤ又はＩＮＶＡＬＩＤ）をもって変更される。加えて、又は代わりに、上記属性証明への変更を分散台帳へ発行する「Ａｔｔｒｉｂｕｔｅ　Ｓｔａｔｅ　Ｃｈａｎｇｅ」イベントがトリガされてもよい。

【００９８】

「Ｂａｄｇｅ　Ｃｒｅａｔｅｄ」「Ａｔｔｒｉｂｕｔｅ　Ｓｅｔ」「Ｖｅｒｉｆｉｃａｔｉｏｎ　Ｒｅｑｕｅｓｔ」及び「Ａｔｔｒｉｂｕｔｅ　Ｓｔａｔｅ　Ｃｈａｎｇｅ」イベントの非限定例を下の表に示す。

【表４】

Badge Created イベント		
フィールド	**コール元**	本イベントをトリガした実体の GUII
	バッジ	作成されたバッジのラベル
	信用済み団体	属性値を検証する責任を持ち同値の正確性を証明する信用済み実体の GUII
Verification Request イベントの例		
フィールド	**コール元**	本イベントを作成した実体の GUII
	バッジ	検証されるべきバッジのラベル
Attribute Set イベントの例		
フィールド	**コール元**	本イベントを作成した実体の GUII
	バッジ	属性値が設定されたバッジのラベル
	属性鍵	値が設定された属性のラベル
	属性値	属性値への一つ以上の暗号学的証明
Attribute State Change イベントの例		
フィールド	**コール元**	本イベントを作成した実体の GUII
	バッジ	内部で属性証明が状態変更するバッジのラベル
	属性鍵	状態変更している属性証明のラベル
	古い状態	状態遷移前の属性証明の状態
	新しい状態	状態遷移後の属性証明の状態

【００９９】

いくつかの実施形態では、属性値は、官庁（例：旅券当局）、雇用主、金融機関などの信用済み実体によって検証されてもよい。例えば物理的な書類（例：出生証明書、運転免許証、社会保障カード、給与明細表）を確認したり、そして／または対面でユーザーに聞き取りを行ったりすることにより信用済み実体が属性の値を検証してもよい。検証が成功すると、信用済み実体は関係する属性証明をＶＥＲＩＦＩＥＤ状態にする。問題があれば、信用済み実体は関係する属性証明をＩＮＶＡＬＩＤ状態にする。

【０１００】

図５は、いくつかの実施形態に基づく、信用済み実体による認証プロセス５００の説明図である。例えば、プロセス５００はユーザーと金融機関の間で、顧客確認（ＫＹＣ）チェックの中で実施される。

【０１０１】
いくつかの実施形態では、プロセス５００を開始する前に、ユーザーは信用済み実体とアプリケーション層（例：図１の例示的アプリケーション層）中の一つ以上のオフレジャーインターフェースを介して通信してもよい。例えば、ユーザーは信用済み実体のウェブサイトを訪れ、及び／又は信用済みのアプリをダウンロードして起動してもよい。アプリケーション層中におけるこのような通信によりユーザーのＰＤＳまたは信用済み実体のＰＤＳが、動作５０５において、プライバシー層におけるハンドシェイク（例：図１に示す例示的プライバシー層）を開始させる。このハンドシェイクにより、信用済み実体のＰＤＳは、信用済み実体が一つ以上の属性値を検証する責任を持つことを確認してもよい。加えて、又は代わりに、信用済み実体のＰＤＳはユーザーのＰＤＳへと、信用済み実体のＧＵＩＩ及び／又は一つ以上の属性証明（例：ＫＹＣプロセスに関連するもの）を用いてバッジを作成するスキーマを送信してもよい。
【０１０２】
動作５１０にて、ユーザーのＰＤＳはバッジ（例：信用済み実体のＧＵＩＩを使用して、及び／又は信用済み実体のＰＤＳにより提供されたスキーマに基づいて）を作成してもよく、バッジを信用層（例：図１に示された例示的信用層）中の分散岩棚へ発行してもよい。次に、ユーザーのＰＤＳは、動作５１５において、信用済み実体のＰＤＳへ、オフレジャー通信を介して、ユーザーのＤＩＲへの参照を、一つ以上の検証対象の属性値と共に送信してもよい。いくつかの実施形態では、ユーザーのＤＩＲは、信用済み実体のＤＩＲに通知するために、オンレジャーイベント（例：「Ｖｅｒｉｆｉｃａｔｉｏｎ　Ｒｅｑｕｅｓｔ」イベント）をトリガしてもよい。
【０１０３】
動作５２０において、信用済み実体のＤＩＲは動作５１５において受信した参照を使用して分散台帳からバッジを探索する。バッジ中の各属性証明に対して、信用済み実体のＤＩＲはバッジ中の暗号学的証明が受信した属性値からバッジ中で指定されたアルゴリズムを使用して生成されたかどうかをチェックしてもよい。次に信用済み実体のＤＩＲは受信した属性値（例：参照バッジを介して間接的に、又は信用済み実体により直接的に）を検証してもよい。
【０１０４】
例えば、与えられた属性証明に対して、信用済み実体のＤＩＲは、別のバッジへの参照があるかどうかをチェックしてもよい。もしあれば、信用済み実体のＤＩＲは分散台帳から該別のバッジを探索し、一つ以上のチェックを実行してもよい。例えば、信用済み実体は、別のバッジを検証した実体が信用できるかどうか、別のバッジ中の暗号学的証明が受信した属性値から別のバッジで指定されたアルゴリズムを用いて生成されたかどうか、及び／又は別のバッジが検証実体により署名されたかどうか、をチェックしてもよい。本開示の態様は限定されていないため、任意の適切な電子署名スキームが使用されてもよい。
【０１０５】
加えて、又は代わりに、信用済み実体は、例えば、物理的な書類を点検したり、そして／又はユーザーに対面で聞き取りを行ったり、といったように、受信した属性値を直接検証してもよい。
【０１０６】
問題がなければ、信用済み実体のＤＩＲはバッジに署名し、バッジ中の各属性証明をＶＥＲＩＦＩＥＤ状態にさせる。問題のある属性証明が一つ以上あれば、信用済み実体のＤＩＲは問題のある属性証明をＩＮＶＡＬＩＤ状態にする。
【０１０７】
いくつかの実施形態では、実体は信用構造を形成し、その中では実体が一つ以上の他の実体を信用し、該一つ以上の信用済み実体（例：図５に関連して上に議論されたように）のうち任意のものにより署名された属性証明を信頼してもよい。このように、ある実体は、物理的な検証をせずとも属性証明を検証可能であってもよい。
【０１０８】

信用構造は実体間における任意の適切な信用関係を伴う任意の適切な数の実体を含んでもよい。さらに、信用構造のメンバーシップは、現存のメンバーが去り、新しいメンバーが加わり、及び／又は信用構造が変化することで、時間と共に進化してもよい。

【０１０９】

図６は、いくつかの実施形態に基づく、信用構造６００の説明図である。本例にて、ＤＩＲ中には６０５ＡからＤの４つのバッジが存在する。バッジ６０５ＡからＤは信用済み実体ＡからＤと関連してもよい。バッジ６０５Ａは次の属性証明を含んでもよい。「名」、「姓」、「社会保障番号」及び「現住所」であり、全てが実体Ａ（例：銀行）によって直接検証済みであってもよい。

【０１１０】

いくつかの実施形態では、バッジ６０５Ｃは次の属性証明を含んでもよい。「現住所」、「名」、「姓」及び「電子メールアドレス」である。これらの属性証明は、属性証明「現住所」はバッジ６０５Ａへの参照を含み、「現住所」属性証明に関して実体Ｃが実体Ａを信頼していることを示していることを除いては、それぞれが実体Ｃ（例：オンラインマーチャント）により直接検証済みであってもよい。これにより実体Ｃがバッジ６０５Ａ内の「現住所」属性証明の状態を見ることが可能になる。

【０１１１】

いくつかの実施形態では、バッジ６０５Ｄは次の属性証明を含んでもよい。「現住所」、「姓名」、「社会保障番号」及び「交際状況」である。これらの属性証明は、属性証明「現住所」はバッジ６０５Ａへの参照を含んでいて「現住所」属性証明に関して実体Ｄが実体Ａを信用していることを示していることを除いては、それぞれが実体Ｄ（例：ソーシャルネットワーキング提供者）により直接検証済みであってもよい。これにより実体Ｄがバッジ６０５Ａ内の「現住所」属性証明の状態を見ることが可能になる。

【０１１２】

いくつかの実施形態では、バッジ６０５Ｂは次の属性証明を含んでもよい。「姓」、「名」、「パスポート番号」及び「電話番号」である。これらの属性証明は、属性証明「姓」はバッジ６０５Ａへの参照とバッジ６０５Ｃへの参照を含んでいて、実体Ｂは実体Ａと実体Ｃが直接、独立に「姓」の属性値を検証した場合のみ属性証明「姓」に署名し得ることを示していることを除いては、属性証明のそれぞれが実体Ｂ（例：旅行業者）により直接検証済みであってもよい。これにより実体ＢがバッジＡ内の「姓」属性証明の状態及びバッジ６０５Ｃ内の「姓」属性証明の状態を見ることが可能になる。

【０１１３】

従って、図６に示す例では、「現住所」属性証明は３つの実体Ａ、Ｃ及びＤを含む信用の輪を持っていてもよく、実体Ａは勤勉にも直接「姓」の属性値の検証を済ませており、実体ＣとＤは、「現住所」に関して実体Ａによる証明に頼っている。一方、属性証明「姓」は３つの実体Ａ、Ｂ及びＣを含む信用の輪を持っていてもよく、実体Ａ及びＣは勤勉にも独立して「姓」の属性値の検証を済ませており、実体Ｂは「現住所」に関して実体Ａによる認証に頼っていた。

【０１１４】

図７は、いくつかの実施形態に基づく、相手方照合プロセス７００の説明図である。本例では、ユーザーＡがユーザーＢと相互作用してもよい。例えば、ユーザーＡは不動産取引における購入者であり、ユーザーＢは売主であってもよい。プロセス７００はユーザーＡまたはＢどちらにより開始されてもよい。

【０１１５】

いくつかの実施形態では、プロセス７００の前にユーザーＡ及びＢは一つ以上のオフレジャーチャンネルを介して通信してもよい。例えば、ユーザーＡ及びＢは間接的に（例：一人以上のブローカーを介して）又は直接（例：電子メールを介して）通信してもよい。このような通信により、動作７０５において、ユーザーＡのＰＤＳが、ユーザーＢのＰＤＳとの、または逆の、プライバシー層におけるハンドシェイク（例：図１に示す例示的プライバシー層）の開始を命令してもよい。

【０１１６】
加えて、又は代わりに、ユーザーＡ及びＢは、アプリケーション層（例：図１の例示的アプリケーション層）内の一つ以上のオフレジャーインターフェースを介して通信してもよい。アプリケーション層中におけるこのような通信の結果として、ユーザーＡのＰＤＳまたはユーザーＢのＰＤＳが、動作７０５において、プライバシー層におけるハンドシェイク（例：図１に示す例示的プライバシー層）を開始してもよい。
【０１１７】
動作７１０において、ユーザーＡのＰＤＳ及びユーザーＢのＰＤＳは個人データ（例：姓名、現住所、電子メールアドレス、等）及び／又は各ＤＩＲへの参照を交換してもよい。属性証明の編成にバッジが使用されるならば、各バッジのラベルもまた交換されてもよい。いくつかの実施形態では、同じ組の個人データがどちらの側から提供されてもよい。しかし、ユーザーＡがユーザーＢからの情報を要求し、同じ情報をユーザーＢはユーザーＡに要求していなく、またはその反対もあり得るため、上記は必須ではない。
【０１１８】
いくつかの実施形態では、ユーザーＡのＤＩＲはユーザーＢから受信した情報を使用して分散台帳から属性証明を探索し、一つ以上のチェックを実施してもよい。例えば、ユーザーＡのＤＩＲは属性証明を検証した実体が信用できるかどうか、属性証明がＶＥＲＩＦＩＥＤ状態かどうか、属性証明を含むバッジにより指定されたアルゴリズムを使用してユーザーＢから受信した関連属性値から属性証明中の暗号学的証明が生成されているかどうか、及び／又は、属性証明が検証を行う実体により署名されたかどうかをチェックしてもよい。ユーザーＢのＤＩＲは同様のチェックを行ってもよい。
【０１１９】
発明者らはプライバシー層要素（例：ＰＤＳ）をホストする環境の安全性を高めることが望ましいと認識し理解した。加えて、又は代わりに、プライバシー層及び／又は信用層のアクセス制御を向上させることが望ましい。
【０１２０】
いくつかの実施形態では、ホスト環境の安全性はプライバシー層要素（例：ＰＤＳ）により取り扱われるデータを暗号化することにより向上し、その結果ホストする実体（例：パブリッククラウドプロバイダ）は、データが物理的または仮想ディスクに書かれているためにアクセスできなくなってもよい。このような暗号化は仮想環境（例：仮想マシンあたりに一つのＰＤＳ、しかし物理マシンに対して複数のＰＤＳ）又は専用環境（例：物理マシンあたり一つのＰＤＳ）のプライバシー層要素を実装することに加えて行われてもよい。しかしながら、本開示の態様はそのようなデータの暗号化に限定されないことは認められなければならない。
【０１２１】
いくつかの実施形態では、一つ以上の暗号化鍵がプライバシー層要素（例：ＰＤＳ）の外部に記憶され、そのためホスト実体は該一つ以上の暗号化鍵にアクセスできなくなってもよい。任意の適切な鍵管理スキームが使用されてよい。例えば、プライバシー層要素のユーザーにより鍵が維持されてもよい。
【０１２２】
いくつかの実施形態では、プライバシー層におけるデータ変更及び／又は信用層における状態変更に対してアクセスコントロールが課されてもよい。図８は、いくつかの実施形態に基づく、プライバシー層要素（例：ＰＤＳ）におけるデータ変化、及び結果としての信用層要素（例：ＤＩＲ）における状態変化のプロセス８００の説明図である。
【０１２３】
図８に示した例では、プロセス８００はプライバシー層に記憶された個人データの項目を変更しようとするユーザーによって開始され、結果、プライバシー層のアクセス制御チェックがトリガされてもよい。いくつかの実施形態では、プライバシー層のアクセス制御機構は、ユーザーにより要求された動作の型に応じた厳しさを持つ認証及び／又は認可プロセスを含んでもよい。例えば、重大なデータ（例：パスポート番号）を変更しようとす

る試みにより、重大でないデータ（例：電子メールアドレス）を変更しようとする時よりも、より厳しい認証プロセス（例：多要素認証）がトリガされ得る。従って、要求されたデータ変更の機密の度合いによって、より強固な安全性が粒度の細かい方法で提供され得る。

【０１２４】

いくつかの実施形態では、プライバシー層における認証及び／又は認可が成功することでユーザーがプライバシー層要素において行おうとしたデータ変更を完了できるようになってもよい。加えて、又は代わりに、プライバシー層要素は、認証及び／又は認可の成功を受けて、信用層にアクセスするために使用する一つ以上の信用層鍵を引き出してもよい。例えば、信用層鍵は信用層要素に一つ以上の動作を行わせる権限を証明するために提示される暗号鍵であってもよい。

【０１２５】

いくつかの実施形態では、異なる型の動作を実行する権限を証明するために異なる信用層鍵が提示されてもよい。例えば、重大でないデータ（例：電子メールアドレス）の変更と比較して、重大データ（例：パスポート番号）の変更のためにはより高レベルの権限に関連付けられた鍵が提示されてもよい。いくつかの実施形態では、信用層要素は、適切な認可（例：一つ以上の適切な鍵を提示）が得られた場合のみ、一つ以上の動作（例：状態変更）を実行するよう命令されてもよい。

【０１２６】

加えて、又は代わりに、文脈に応じた動的アクセス制御ができるよう一つ以上のアクセス規則が提供されてもよい。このように、アクセスは要求された動作の性質だけでなく一つ以上の外的条件にも依存してもよく、そのために安全性が向上する。例えば、進行中の攻撃がある場合厳しいアクセス規則が強制される。

【０１２７】

いくつかの実施形態では、ある実体（例：ユーザーまたは組織）が複数の暗号鍵と関連付けられてもよい。発明者らは安全性と使いやすさの間にトレードオフがあり得ると認識し理解した。従って、いくつかの実施形態では、所望の安全性と使いやすさのバランスを達成するために、ある実体が適切な数の鍵を選択できるようなシステムが提供されてもよい。図３の例を参照して、いくつかの実施形態において鍵管理要素３０８は、ＤＩＲを制御する実体に関連する複数の公開暗号鍵に追従するために提供される。そのような要素は基礎を成す公開鍵基盤（ＰＫＩ）を提供してもよい。このように、ユーザー及び／又はアプリケーション層のアプリケーションは、基礎となる暗号鍵と直接相互作用せず、それぞれのＰＤＳを介してＤＩＲのみと相互作用してもよい。

【０１２８】

いくつかの実施形態では、鍵管理要素３０８はロールベースアクセス制御を行ってもよい。例えば、認証者とアイデンティティ所有者という少なくとも二つのロールがあってもよい。鍵管理要素３０８はあるバッジに割り当てられたれた信用済み実体のみに対して、該バッジ中の属性証明の状態変更を許可してもよい。

【０１２９】

上に議論されたように、発明者らは、パスポート情報のような特定の属性に対してより高度なセキュリティを課すことが望ましいと認識し理解した。いくつかの実施形態では、このことは一つ以上の認証及び／又は認可の測定を通して実現できる。例えば、認証プロセスの信頼性を向上させるために一つ以上の生体マーカーが使用されてもよい。加えて、又は代わりに、一つ以上の生体マーカーが、ユーザーが複数のＤＩＲを作成することを防ぐＧＵＩＩを生成するために使用されてもよい。いくつかの実施形態では、このような生体マーカーは高機密情報として扱われ、他の実体と共有されなくてもよい。

【０１３０】

加えて、又は代わりに、一つ以上の行動メトリクス（例：位置履歴、歩行パターン、睡眠パターン、旅行パターン等）が、認証プロセスにおける信頼度を向上させるために使用されてもよい。

【０１３１】
いくつかの実施形態では、機密属性値（例：パスポート番号）は複数鍵認証を用いて保護される。例えば、あるユーザーが認証時に複数の鍵を提示することで属性値を変更する認可を得ようとし得る。いくつかの実施形態では、各鍵は異なる機器と関連づけられていてもよい。例えば、あるユーザーがノートＰＣ用に第一の鍵、スマートフォン用の第二の鍵、スマートウォッチ用に第三の鍵を持っていてもよい。属性値を変更する例示的プロセスは以下のステップを含んでもよい。
【０１３２】
１）ユーザーはＰＤＳのインターフェース（例：ウェブインターフェース）にアクセスし、変更動作をトリガする。
【０１３３】
２）ユーザーからの追加の確認が必要であることの示唆と共に、変更動作がペンディング動作として記録される。
【０１３４】
３）ユーザーが変更動作を少なくとも一つの追加の個人用機器を用いて確認する。例えば、変更動作は、登録済のスマートフォン及び登録済みの生体署名を用いて指紋認証を介して確認されてもよい。
【０１３５】
いくつかの実施形態では、ユーザーはＭ個の鍵を持ち、少なくともＮ個の鍵（Ｎ＜＝Ｍ）が特定の動作（例：属性値の変更）を実行するために使用される。このように、安全性のレベルが向上し、ユーザーを偽装することがより困難となってもよい。いくつかの実施形態では、Ｍはユーザーに対して登録された機器の数と同じでもよい。
【０１３６】
加えて、又は代わりに、スマートウォッチ、スマートフォン、ノートＰＣ等のような二つ以上の個人機器が互いに特定の距離（例：１０メートル）内にある場合のみに認可されてもよい。加えて、又は代わりに、個人機器が特定の場所（例：ＧＰＳデータに基づいて決定される）にある場合のみに認可されてもよい。
【０１３７】
いくつかの実施形態では、鍵が危殆化されたら（例：機器が盗難に遭う）、危殆化された鍵は取り消され、新しい鍵で置換されてもよい。これにより安全性が向上し、例えば動作を要求する実体がＰＤＳとＤＩＲに関係する実際のユーザーであるという確率が高くなり得る。
【０１３８】
発明者らは、複数の鍵が使用されれば、危殆化された認証鍵は取り消されて置換され、一方ユーザーのＰＤＳ及びＤＩＲへのその間におけるアクセス能力が維持されることを認識し理解した。いくつかの実施形態では、一つ以上の鍵は、一つ以上のアクセス権と共に、分散岩棚を通して伝搬され、結果該一つ以上の鍵及び一つ以上のアクセス権は改ざんへの耐性を得て、任意の実体から証明可能となる。上に議論されたように、いくつかの実施形態では、暗号学的一方向関数を使用して機密データの証明を求めることによりプライバシー保護が実現されてもよい。元の機密データを証明から求めることは計算機的に困難であり得る。共有された分散台帳内に非機密証明のみを含むことにより、高度なプライバシーを実現できる。元の機密情報を共有するために、実体間の安全なオフレジャー通信チャンネルが使用されてもよい。加えて、又は代わりに、さらにプライバシーを向上させる粒度の細かい属性の構造を提供するためにスキーマが使用されてもよい。例えば、不必要な情報（例：現住所又は実際の誕生日）を共有する代わりに、特定の文脈（例：アルコールの購入目的においては２１歳を超えている）に関する情報のみを他の実体と共有してもよい。さらにプライバシーを向上させるため、ある実体は、いくつかの実施形態において、異なるバッジ内の異なる識別子を用いて識別されてもよい。このようにして、実体に戻って相互作用を辿ることは攻撃者にとってより困難となってもよい。
【０１３９】

発明者らはユーザーが、特定の分散台帳を管理するノードを発見する機構を提供することが望ましいと認識し理解した。ある状況においては、分散台帳を管理するノードはカスタマイズされた発見機構、一つ以上のＨＴＴＰリクエスト、及び／又はＤＮＳ解決プロセスを介して発見されてもよい。いくつかの実施形態では、インターネットスケールのネットワーク内で分散台帳の発見可能性を満足するプロパティの組を含むＵＲＩスキームが提供されてもよい。ある状況では、ノードは分散台帳に加入及び／又は脱退してもよい。このために要求した実体に返されるノードのリストが最新であることが望ましい。

【０１４０】

いくつかの実施形態では、一つより多い分散台帳（例：一つ以上のブロックチェーン）が使用されてもよい。そのような構造では、複数の分散台帳を通してノードを発見するために発見メカニズムが提供される。単一分散台帳の構造と比較して、複数分散台帳を持つ構造では通信オーバーヘッドが小さくなり、分散台帳識別子を特定する要求をただ一つのみ含んでもよい。応答には、要求された分散台帳を現在管理するノードのリストが含まれてもよい。いくつかの実施形態では、基礎となるデータ構造は分散ハッシュテーブル（ＤＨＴ）であってもよい。ノードは、分散台帳の管理を開始する度に、ネットワークに対して動作をアナウンスしてもよい。ノードはまた分散台帳の管理を終了したときにもアナウンスを行ってもよい。

【０１４１】

図９は、いくつかの実施形態に基づく、ネットワーク９００における分散台帳発見機構の例である。動作１においては、ノード２はノード１からのブロックチェーンＸへのアクセスを要求してもよい。応答としては、動作２でノード１はノード２へ許可を与えてもよい。動作３では、ノード２がブロックチェーンＸに対してブロックチェーンＸの管理を現在行っていることをアナウンスしてもよい。動作３では、ノード３もまたブロックチェーンＸへのアクセスをノード１に要求してもよい。応答としては、動作４でノード１はノード３へ許可を与えてもよい。動作５では、ノード３が現在ブロックチェーンＸへ現在管理していることをアナウンスしてもよい。動作６では、ノード２はブロックチェーンＸを脱退することを決断し、ブロックチェーンＸへ脱退をアナウンスしてもよい。動作７では、ノード４はどのノードがブロックチェーンＸを管理しているかを探索してもよい。動作８ではブロックチェーンはアップデート済みの管理中ノードのリストを返してもよい。

【０１４２】

ここに説明される任意の一つ以上の技術は、個人データの検証を単純化するために様々な設定で使用されてもよい。例えば、いくつかの実施形態では、関連するユースケースに関する全ての属性を含む、カスタマイズされたバッジスキーマが、各ユースケースに対して提供されてもよい。このように、スキーマに基づいて生成されたバッジは全ての関連データを含み、バッジを管理するＰＤＳはデータを最新に保ってもよい。

【０１４３】

以下にユースケースの非限定例を説明する。

Ｉ．　顧客確認（ＫＹＣ）

そのようなアプリケーションの一つが顧客確認（ＫＹＣ）チェックであり、銀行のような金融機関によって実行されてもよい。ユーザー（例：銀行の顧客）のアイデンティティは、ユーザーにより提出された一つ以上の属性値を信用済み実体（例：銀行）が検証するプロセスを通じて有効性検証がなされてもよい。該プロセスは本明細書において説明される一つ以上の技術を用いて実行されてもよい。一つ以上の属性値の有効性検証が行われたら、信用済み実体は一つ以上の属性証明に署名し、続いて、以前の信用済み実体及び後の信用済み実体が信用構造の一部である限り認証は別の信用済み実体によって信頼されるようになってもよい。

【０１４４】

金融機関は顧客が誰であるかを検証するために厳しい規則や規制に従わなければならなくてもよい。一方、金融機関は顧客の記録を維持するよう要求されていてもよい。一方、金融機関はデータをプライベートで安全に維持するよう要求されていてもよい。ユーザー

（例：銀行顧客）が自身のデータを制御できるようにし、ユーザーがデータを管理し共有できるプラットフォームを提供することで、結果としてのＫＹＣチェックはより著しく効率的となりデータ重複が削減され得る。ユーザーの観点からは、データはＰＤＳが作成された時点で、続いては属性が変更になった時点でのみ入力されてもよい。このように、同様の情報を複数回入力する負担が制限され得る。金融機関の観点からは、データの正確性が著しく向上し得る。なぜならば、例えば、アップデートが関連する全ての信用済み実体へ伝搬し得るためである。

【０１４５】

ＩＩ．　従業員認証

ＫＹＣチェックと比較すると、従業員の認証はそれほど規制されていない。それにもかかわらず、雇用主は本明細書内で説明された任意の一つ以上の技術を使用してアイデンティティ及び／又は従業員の他の情報を認証してもよい。このような認証は認証及び／又は認可のみを目的として内部で使用され、加えて、または代わりにパートナー及び／又はステークホルダーと安全に情報を共有するために外部で使用されてもよい。このようにして、主張されるアイデンティティに関して保証を行うことが確証されてもよい。いくつかの実施形態では、雇用主に代わって特定の仕事を行う認可を従業員に与えるプロセスが著しく簡潔になり得る。理由はすべての信頼済みステークホルダーへ属性が伝搬し、所望の認可レベルがいつでも最新であるからである。

【０１４６】

ＩＩＩ．　セキュリティチェック

開示される任意の一つ以上の技術はセキュリティチェック（例：空港で実行されるセキュリティチェック、立ち入り禁止区域やビルへの立ち入り許可を与えるセキュリティチェック）の加速を可能にする。例えば、身分証明書（ＩＤ）又は他の識別情報を手でチェックする代わりに、セキュリティチェックが自動化され得る。

いくつかの実施形態では、自動化されたセキュリティチェックは、適切な信用済み実体により証明された犯罪履歴（例：過去６か月以内にアップデート）のリアルタイムでの引き出しを含んでもよい。

【０１４７】

ＩＶ．　運輸保安庁（ＴＳＡ）

一例として、ある旅行者がＰＤＳ及び属性証明の組を含む関連ＤＩＲを持っていてもよい。ＤＩＲはＴＳＡチェックに適切なスキーマを含んでもよい。このように、ＴＳＡ代理人により空港で行われるセキュリティチェックは相手方照合を行うことにより実行されてもよい。このような相手方照合の一例は次のようなステップを含んでもよい。

１）　旅行者が空港にてＴＳＡセキュリティチェックポイントへ接近してもよい。

２）　旅行者の携帯機器が属性値をＴＳＡシステムへ共有してもよい。

３）　ＴＳＡシステムは共有された属性値を受信したことを確認してもよい。

４）　ＴＳＡ代理人は共有された属性値を開き旅行者と視覚的に比較する。加えて、又は代わりに、旅行者は指紋及び／又は他の生体特徴をスキャンしてもよい。このような特徴は共有された属性値に含まれる関連した特徴と比較されてもよい。

５）　ＴＳＡシステムは：署名を行う信用済み実体がＴＳＡにより信用済みか確認すると同時に受信した属性値が正当であるかを分散台帳に対してチェックすることによりチェックし；一つ以上の属性値を外部リスト（例：飛行禁止又はテロ監視リスト）に対してクロスチェックし；そして／又は顔認識を実行又は受信した写真付証明書をリアルタイムビデオストリームに対してクロスチェックしてもよい。

【０１４８】

上記全てのチェックを通過すれば、旅行者は信用済みとしてマークされてもよい。従って、ＴＳＡにおいてはもはや大きなデータベースを維持する必要がなくなり得る。加えて、本アプローチは物理パスポートチェックと他のバックグラウンドチェックを一つの簡単なステップへ連結させ得る。このように、バックグラウンドチェックは遭遇のたびに簡単に実行されてもよい。

【０１４９】
Ｖ．　チェックイン
チェックイン時、顧客は列で待たされることが多い。そのような待ち時間は本明細書において説明される一つ以上の技術を用いて著しく短縮され得る。例えば、顧客がＰＤＳ及び関連ＤＩＲを持ち、アイデンティティ及び／又は他の関連データが、属性の参照をチェックすることにより、認証組織（例：ホテル、レンタカー等）により認証されてもよい。予約時には、顧客はＰＤＳを使用して関連情報を組織と共有してもよい。個人情報を手入力する代わりに、組織のシステムから顧客にどの属性値が必要かを通知してもよい。チェックイン時には、顧客はホテルの部屋、車等に対して、代理人に会ったり個人情報を提供したりすることなく支配権を得てもよい。いくつかの実施形態では、顧客は、彼／彼女が予約時に使用したデジタルアイデンティティ表現へのアクセスを得ていることを提示することにより、ホテルの部屋または車を開錠してもよい。例えば、顧客はＰＤＳを制御できる携帯機器を使用してもよい。
【０１５０】
ＶＩ．　年齢制限のある会場
バーなどの特定の会場は顧客には特定の年齢より上であることの証明を提供することが求められ得る。年齢の証明を提供するためには、顧客は関連情報を会場に共有するためのバッジを作成してもよい。バッジは特定のスキーマを使用して形成され、顧客の年齢、又は顧客の年齢と名前のみを含んでもよい。携帯機器を使用して情報の共有が実行されてもよい。年齢が他の信用済み団体により証明されていれば、該会場は顧客により提供された年齢情報が実際に正しいということを結論付けてもよい。
【０１５１】
いくつかの実施形態では、有利な技術的効果が分散され保護された記憶場所を介して提供され、機密及び（高度に）攻撃を受けやすいユーザー情報が、暗号学的一方向関数を適用することにより保護された方法で記憶される。さらに、互いを信用する独立した実体間において、各要求に対して状態情報（例：属性値が検証されたかどうか）を共有することにより、（ユーザー）情報の正確性を確認するための検証手続きの冗長性が簡単に削減され得る。時間だけでなく他の資源、例えば、不要なワークフローを避ける（結果ネットワークトラフィックが削減される）ことによる個人データの組の複製（結果コンピューター記憶領域）、互換なデータベースをいかなる状況下でも常に利用可能にしておくための中央手形交換所のような中央記憶装置及び管理システムのための高額なインフラストラクチャ、も保全され得る。従って、データ管理における効率性の向上は、例えば、インフラストラクチャと必要な計算力の削減、及び／又は応答時間の削減をももたらし得る。
【０１５２】
いくつかの実施形態では、（ユーザー）情報を保護された方法で共有することにより、例えば、有利なハッシュアルゴリズムを使用することにより、機密（ユーザー）情報さえも、互いを信頼し得る複数の異なる実体で構成されるネットワーク環境内において、外来の信頼済みでない実体による盗難や承認不可能な又は詐欺行為の変更等の危険を冒すことなくアクセス可能な場所に維持してもよい。
【０１５３】
本開示の態様の例を以下に説明する。複数の実体のうち少なくとも一つの個人アイデンティティ表現をデジタルアイデンティティ表現（ＤＩＲ）と考え、複数の実体のうち少なくとも一つのユーザーデータ構造を個人データサービス（ＰＤＳ）と考える。
【０１５４】
１．　コンピューターに実装した方法であり
ユーザーより取得した複数の計測値を使用して前述のユーザーの識別子を生成し、前述の識別子は前述の複数の計測値の暗号学的証明を含み、
前述のユーザーの識別子と関連したデジタルアイデンティティ表現を生成し、前述のデジタルアイデンティティ表現は認証の規則を実装するプログラムコードを含み、
前述のデジタルアイデンティティ表現に対する電子署名を生成し、

前述のデジタルアイデンティティ表現及び電子署名を分散台帳システムへ発行する動作を含む、方法。

【０１５５】

２．　態様１のコンピューターに実装された方法であり、前述の複数の計測値は少なくとも一つの生体計測値及び少なくとも一つの行動計測値を含む、方法。

【０１５６】

３．　態様１のコンピューターに実装された方法であり、さらに

分散台帳システムから、デジタルアイデンティティ表現の記録が作成されたことを示す確認を受信する動作を含む、方法。

【０１５７】

４．　態様３のコンピューターに実装された方法であり、前述の分散台帳システムは少なくとも一つのブロックチェーンを使用して実装されている、方法。

【０１５８】

５．　態様１のコンピューターに実装された方法であり、さらに

分散台帳システムを介して信用済み実体へバッジを検証する要求を送信し、前述のバッジはそれぞれが複数の属性に関連する複数の暗号学的証明を含み、各暗号学的証明は前述の暗号学的証明に関連する前述の属性の値に基づいて生成され、

前述の複数の属性の前述の複数の値を分散台帳システムの外部のチャンネルを介して前述の信用済み実体へ送信する動作を含む、方法。

【０１５９】

６．　態様１のコンピューターに実装された方法であり、さらに

バッジへのポインタを受信し、

前述の分散台帳システムから前述のバッジにアクセスするために前述のポインタを使用し、前述のバッジは、前述のバッジはそれぞれが前述の複数の属性に関連する複数の属性証明を含み、各属性に対して、前述の関連する属性証明は暗号学的証明を含み、

分散台帳システムの外部のチャンネルを介して前述の複数の属性にそれぞれ関連する複数の値を受信し、

前述のバッジから前述のバッジを検証する責任を持つ実体を識別し、

前述のバッジを検証する責任を持つ前述の実体を信用するかどうかを決定し、

前述のバッジを検証する責任を持つ前述の実体を信用するかどうかの決定に応答して、前述の複数の属性証明中の各属性証明に対して、

前述の属性証明がＶＥＲＩＦＩＥＤ状態かどうか、

前述の属性証明中の前述の暗号学的証明は受信した前述の属性に関連する値の有効な証明かどうか、

前述の属性証明は前述のバッジを検証する責任を持つ実体により実体により電子的に署名されているかどうか、のチェックを行う、方法。

【０１６０】

７．　コンピューターに実装された方法であり、

バッジに対する複数のスキーマからスキーマを選択し、前述のスキーマは複数の属性を含み、

前述のスキーマに基づき、ユーザーのアイデンティティを認証するために使用するバッジを生成し、前述の生成動作は、

各値が前述のスキーマ中の前述の属性に関連する複数の値を識別し、

前述の複数の値中の各値に対して少なくとも一つの暗号学的証明を生成し、

前述の複数の値を検証する信用済み実体を識別し、

前述のバッジを分散台帳システムへ発行する動作を含む、方法。

【０１６１】

８．　態様７のコンピューターに実装された方法であり、前述の分散台帳システムはユーザーの識別子に関連付けられたデジタルアイデンティティ表現を含み、前述のデジタルアイデンティティ表現は認証のための規則を実装するプログラムコードを含む、方法。

【０１６２】
９．　態様８のコンピューターに実装された方法であり、さらに
前述の複数の属性中の各属性に対して、前述のバッジは該属性に対する属性証明を含み、
前述の属性証明は関連する属性値に対する少なくとも一つの暗号学的証明を含み、
前述のプログラムコードは、少なくとも一つのプロセッサにより実行された時、前述の複数の属性中の各属性証明の状態情報を維持する、方法。
【０１６３】
１０．　態様９のコンピューターに実装された方法であり、少なくとも一つの属性証明は以下の、ＰＥＮＤＩＮＧ、ＶＥＲＩＦＩＥＤ、ＥＸＰＩＲＥＤ、及びＩＮＶＡＬＩＤ、から成るグループから選択した状態をとる、方法。
【０１６４】
１１．　態様１０のコンピューターに実装された方法であり、前述のプログラムコードは、少なくとも一つのプロセッサにより実行された時、関連する属性値が前述の信用済み実体により検証されたことが前述の信用済み実体から通知されたことに応答してのみ、前述の少なくとも一つの属性証明をＰＥＮＤＩＮＧ状態からＶＥＲＩＦＩＥＤ状態へ遷移させる、方法。
【０１６５】
１２．　態様１０のコンピューターに実装された方法であり、前述のプログラムコードは、少なくとも一つのプロセッサにより実行された時、関連する属性値が直前に検証された時点で設定されたタイマーが期限切れとなるときに、前述の少なくとも一つの属性証明をＶＥＲＩＦＩＥＤ状態からＥＸＰＩＲＥＤ状態へ遷移させる、方法。
【０１６６】
１３．　態様１０のコンピューターに実装された方法であり、前述のプログラムコードは、前述の少なくとも一つのプロセッサにより実行された時、前述の少なくとも一つの属性証明がＶＥＲＩＦＩＥＤ状態であるとき、関連する属性値の暗号学的証明のアクセスを可能にする、方法。
【０１６７】
１４．　コンピューターに実装された方法であり
分散台帳システムを介しての、バッジを検証する要求を受信し、前述のバッジはそれぞれがユーザーの複数の属性へ関連する複数の属性証明を含み、各属性に対して、前述の関連する属性証明は暗号学的証明を含み、
分散台帳システムの外部のチャンネルを介して前述の複数の属性にそれぞれ関連する複数の値を受信し、
前述の複数の属性のうち少なくとも一つの属性に対して、
前述の少なくとも一つの属性に対する前述の値が前述のユーザーの前述の少なくとも一つの属性の正しい値であるかを検証し、
前述の少なくとも一つの属性に関する前述の値が前述のユーザーの前述の少なくとも一つの属性の正しい値であるかの検証に応答して、前述の分散台帳システムを介して、前述の少なくとも一つの属性に関する前述の属性証明をＶＥＲＩＦＩＥＤ状態にさせる、方法。
【０１６８】
１５．　コンピューターに実装された方法であり
分散台帳システムを介しての、第一のバッジを検証する要求を受信し、前述の第一のバッジはそれぞれがユーザーの複数の属性へ関連する複数の属性証明を含み、各属性に対して、前述の関連する属性証明は暗号学的証明を含み、
分散台帳システムの外部のチャンネルを介して前述の複数の属性にそれぞれ関連する複数の値を受信し、
前述の複数の属性のうち少なくとも一つの属性に対して、
前述の第一のバッジから、前述の少なくとも一つの属性に関連する第一の属性証明を識別し、前述の第一の属性証明は第一の暗号学的証明を含み、
前述の第一の属性証明から、第二のバッジへのポインタを識別し、

前述のポインタを使用して分散台帳から前述の第二のバッジへアクセスし、
前述の第二のバッジから、前述の第二のバッジ及び前述の少なくとも一つの属性に関連する第二の属性証明を検証することに責任を持つ実体を識別し、
前述の第二のバッジを検証する責任を持つ前述の実体を信用するかどうかを決定し、
前述の第二のバッジを検証する責任を持つ前述の実体を信用するかどうかの判断に対して、
（１）前述の第二の属性証明がＶＥＲＩＦＩＥＤ状態かどうか、
（２）前述の第二の暗号学的証明が、前述の少なくとも一つの属性に関連する前述の受信した値の有効な証明であるかどうか、そして
（３）前述の第二の属性証明は前述の第二のバッジを検証する責任を持つ実体により電子的に署名されているかどうか、のチェックを行う、方法。

【０１６９】

１６．　態様１５の方法であり、さらに
（４）前述の第一の暗号学的証明が、前述の少なくとも一つの属性に関連する前述の受信した値の有効な証明であるかどうかのチェック動作を含む、方法。

【０１７０】

１７．　態様１６の方法であり、さらに（１）から（４）が満足されたことをチェックしたことへの応答として、さらに
前述の第一の属性証明へ電子的に署名し、
前述の第一の属性証明をＶＥＲＩＦＩＥＤ状態へ遷移させる動作を含む、方法。

【０１７１】

図１０は本開示の任意の態様が実装され得るコンピューター１００００を模式的に表した説明図である。図１０に示されるいくつかの実施形態では、コンピューター１００００は、一つ以上のプロセッサを持つ処理装置１０００１、及び、揮発性及び／又は不揮発性メモリを含み得る非一時的なコンピューターによって読み取り可能な記憶メディア１０００２を含む。メモリ１０００２は、処理装置１０００１が本明細書に記載される任意の機能を実行するようプログラムする一つ以上の命令を記憶してもよい。コンピューター１００００はまた、システムメモリ１０００２に加えて記憶装置１０００５（例：一つ以上のディスクドライブ）のような異なる型の非一時的なコンピューターによって読み取り可能なメディアを含んでもよい。記憶装置１０００５は一つ以上のアプリケーションプログラム及び／又は、記憶装置１０００２にロードされアプリケーションプログラムにより使用される外部構成要素（例：ソフトウエアライブラリ）を記憶してもよい。

【０１７２】

コンピューター１００００は図１０に示される機器１０００６、１０００７のような一つ以上の入力装置及び／又は出力装置を持っていてもよい。これらの機器は他の物の中でも、ユーザーインターフェースを提示するために使用されてもよい。ユーザーインターフェースを提供する出力装置の例は、出力の視覚的な提示を行うためのプリンターまたはディスプレイ画面、そして出力の音声提示のためのスピーカーまたは他の音発生装置を含む。ユーザーインターフェースとして使用できる入力装置の例はキーボード及びマウス、タッチパッド、及びディ自体逗葉タブレットのようなポインティングデバイスを含む。別の例として、入力装置１０００７は音声信号を獲得するマイクを含んでもよく、そして出力装置１０００６は認識した文字を視覚的に提示するディスプレイ画面及び／又は音声で提示するスピーカーを含んでもよい。

【０１７３】

図１０に示されるように、コンピューター１００００は、様々なネットワーク（例：ネットワーク１００２０）を介した通信を可能にする一つ以上のネットワークインターフェース（例：ネットワークインターフェース１００１０）を含んでもよい。ネットワークの例は企業ネットワークまたはインターネットなどのローカルエリアネットワーク又はワイドエリアネットワークを含む。そのようなネットワークは任意の適切な技術に基づいていてもよく、任意の適切なプロトコルにより動作してもよく、無線ネットワーク、有線ネッ

トワーク又は光ファイバーネットワークを含んでもよい。

【０１７４】

少なくとも一つの実施形態の幾つかの態様について説明を行ったが、当業者に様々な改変、変更、及び改善が起こることは認められなければならない。そのような改変、変更及び改善は本開示の精神及び範疇内であることを意図している。従って、行ってきた説明及び図は例示のみを目的とする。

【０１７５】

上に説明された本開示の実施形態は任意の数々の方法で改善されてもよい。例えば、実施形態はハードウエア、ソフトウエア及びその組み合わせにより実装されてもよい。ソフトウエアに実装された時は、単一のコンピューター内又は複数のコンピューターに分散して提供されても、ソフトウエアのコードは任意のプロセッサ又はプロセッサの集合により実行されることができる。

【０１７６】

また、本明細書中に概説した様々な方法又はプロセスはソフトウエアとしてコード化でき、様々なオペレーティングシステムのうち一つ以上を用いる一つ以上のプロセッサで実行可能である。加えて、そのようなソフトウエアは数々の適切なプログラミング言語及び／又はプログラミング又はスクリプティングツールのうち任意の物を使用して記述されてもよく、そして実行可能な機械言語コード又はフレームワーク又は仮想マシンで実行可能な中間言語コードへコンパイルされてもよい。

【０１７７】

この点で、本明細書中で開示されるコンセプトは、一つ以上のコンピューター又は他のプロセッサにより実行された時、上に議論された本開示の様々な実施形態を実施する一つ以上のプログラムを以てコード化された、非一時的なコンピューターによって読み取り可能なメディア（又は複数のコンピューターによって読み取り可能なメディア）（例：コンピューターのメモリ、一つ以上のフロッピーディスク、コンパクトディスク、光ディスク、磁気テープ、フラッシュメモリ、フィールドプログラマブルゲートアレイの回路構成又は他の半導体デバイス、又は他の非一過性の夕景の記憶メディア）により実施されてもよい。コンピューターにより読み取り可能なメディアは可搬であってもよく、そのためプログラムまたはメディア上に記憶されたプログラムは一つ以上の異なるコンピューター又はプロセッサ上にロードされ、上に議論された本開示の様々な態様を実装することができる。

【０１７８】

「プログラム」又は「ソフトウエア」の語は、本明細書内にて、上に議論した本開示の様々な態様を実装するようコンピューターをプログラムするために用いられる任意のコンピューターコード又はコンピューターにより実行可能な命令の組を参照するよう使用される。加えて、本実施形態の一つの態様によれば、実行時に本開示の方法を実行する一つ以上のコンピュータープログラムは一つのコンピューターまたはプロセッサ上に存在する必要はなく、本開示の様々な態様を実装するために数々の異なるコンピューター又はプロセッサにモジュール化された方法で分散されてもよいことは認められなければならない。

【０１７９】

コンピューターにより実行可能な命令は、一つ以上のコンピューターまたは他の機器により実行されるプログラムモジュールのような多くの形であってもよい。一般的に、プログラムモジュールは、特定のタスクを実行または特定の型の抽象データを実装するための、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造等を含む。典型的にはプログラムモジュールの機能性は、様々な実施形態で説明されたように連結または分散されてもよい。

【０１８０】

また、データ構造はコンピューターにより読み取り可能なメディアに任意の適切な方法で記憶されてもよい。説明の簡便さのためにデータ構造は、データ構造上の位置に関連するフィールドを持つよう示されてもよい。そのような関係は、コンピューターにより読み

取り可能なメディア内に、フィールド間の関係を伝えるフィールドに対して記憶装置内の場所を割り当てることで同様に達成されてもよい。しかし、データ構造のフィールド内の情報の関係を樹立するために、ポインタや、データ要素間の関係を樹立するタグ又は他の機構の使用を通じることを含み、任意の適切な機構が使用されてよい。

【０１８１】

本開示の様々な機能や態様は単独で使用されてもよく、二つ以上を任意に組み合わせて使用されてもよく、また上に説明された実施形態内で特に議論されていなく、そしてそのために上述の説明または図中の説明で明らかにされた内容により細部の応用と説明済みの構成要素の配置に限定されないような様々な配置により使用されてもよい。例えば、一つの実施形態に説明された態様は任意の方法で他の実施形態にて説明された態様に結合させてもよい。

【０１８２】

また、本明細書中にて開示されたコンセプトは、例が提供された方法として実施されてもよい。方法の一部として実行された動作は任意の適切な方法で順序立てられてもよい。従って、例示的な実施形態では連続した動作として示された幾つかの動作を同時に行ったりすることも含め、説明された順序とは違う順序で動作が実行されるような実施形態が構成されてもよい。

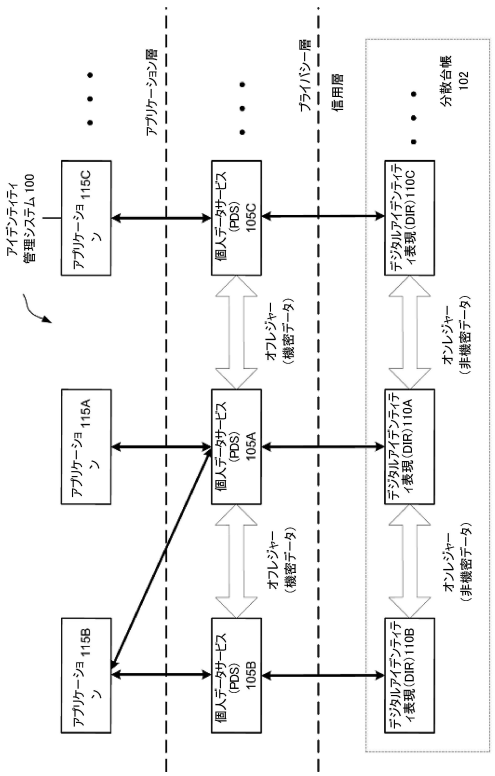
【０１８３】

請求項中にて請求項の要素を修飾するために使用される順序を示す語「第一の」「第二の」「第三の」等は、それ自体により優先度、時間的な先行、又は一つの請求項要素の他の要素に対しての順番、又は方法の動作が実行される一時的な順番を含蓄せず、一つの特定の名前を持つ請求項要素を別の同じ名前を持つ要素と区別する目的のみに用いられる。

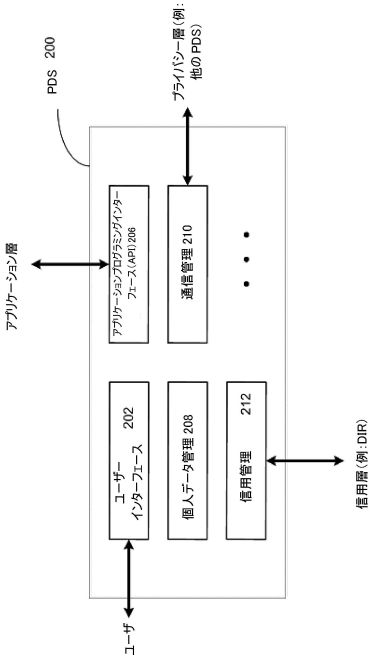
【０１８４】

また、本明細書中の表現法や用語法は説明を目的とし、限定的と理解されてはならない。本明細書中の「含む」「備える」「持つ」「内包する」「関わる」及びそれらのバリエーションは、追加項目に加えて、その前に挙げる項目及びその同等な項目を内包することを意図している。

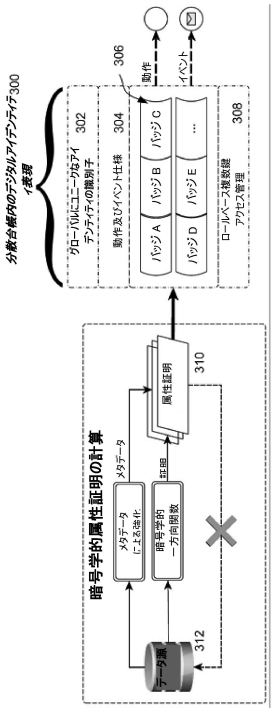
【図１】


アイデンティティ管理システム 100
アプリケーション層
プライバシー層
信用層
分散台帳 102
アプリケーション 115C
アプリケーション 115A
アプリケーション 115B
個人データサービス (PDS) 105C
個人データサービス (PDS) 105A
個人データサービス (PDS) 105B
デジタルアイデンティティ表現(DIR) 110C
デジタルアイデンティティ表現(DIR) 110A
デジタルアイデンティティ表現(DIR) 110B
オフレジャー（機密データ）
オンレジャー（非機密データ）
オフレジャー（機密データ）
オンレジャー（非機密データ）

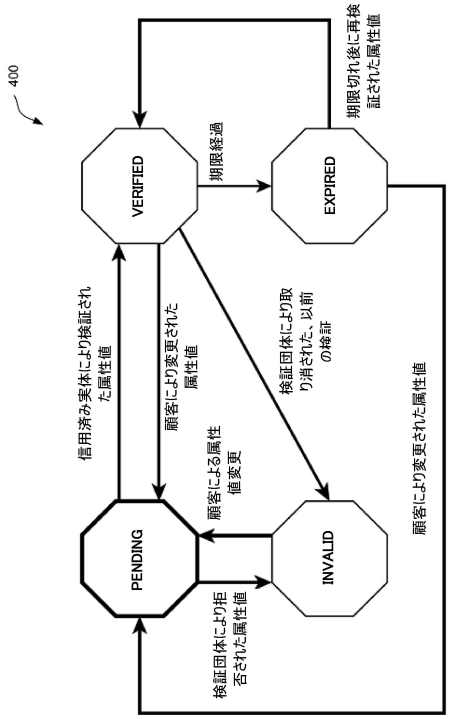
【図２】


PDS 200
プライバシー層（例：他のPDS）
アプリケーション層
アプリケーションプログラミングインターフェース(API) 206
通信管理 210
ユーザーインターフェース 202
個人データ管理 208
信用管理 212
信用層（例：DIR）
ユーザ

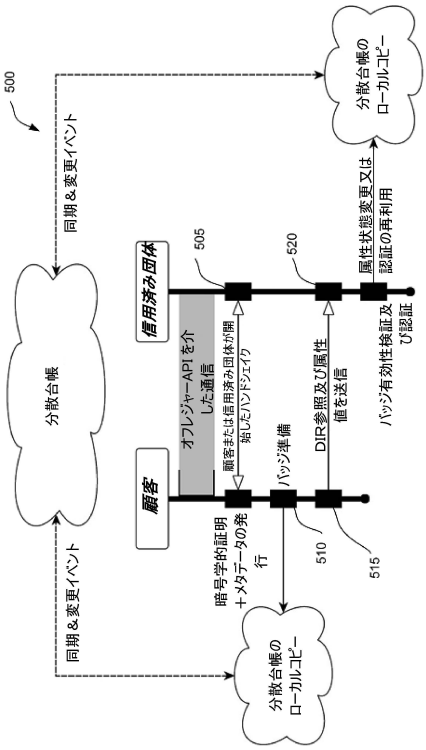
【図３】


分散台帳内のデジタルアイデンティティ表現 300
グローバルにユニークなアイデンティティの識別子 302
動作及びイベント仕様 304
306
動作
イベント
バッジA
バッジB
バッジC
バッジD
バッジE
...
ローカルベース属性値アクセス管理 308
暗号学的属性証明の計算
メタデータ
メタデータによる改ざん
暗号学的一方向関数
証明
属性証明
310
データ源
312

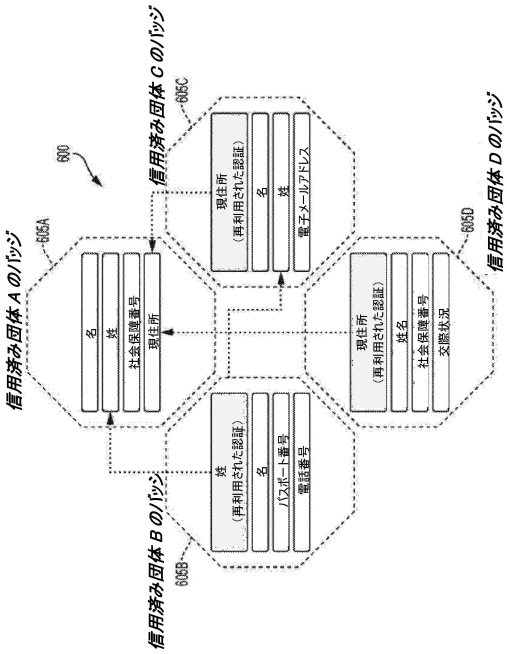
【図４】


400
VERIFIED
EXPIRED
PENDING
INVALID
期限経過
期限切れ後に再検証された属性値
信用済み実体により検証された属性値
顧客により変更された属性値
検証団体により取り消された、以前の検証
顧客による属性値変更
検証団体により拒否された属性値
顧客により変更された属性値

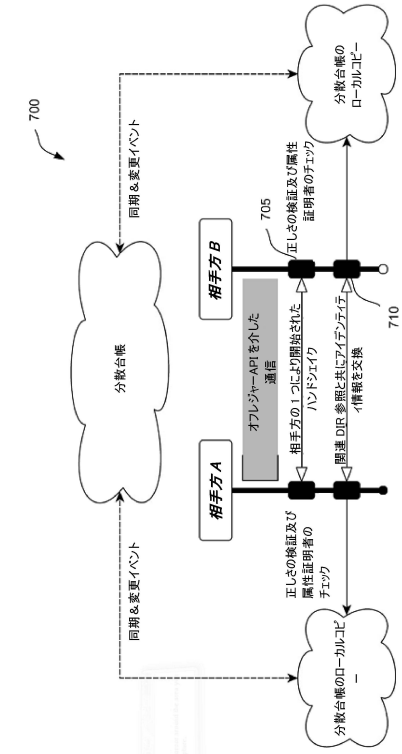
【図５】


500
同期＆変更イベント
分散台帳
同期＆変更イベント
分散台帳のローカルコピー
分散台帳のローカルコピー
信用済み団体
顧客
505
520
オフレジャーAPIを介した通信
顧客または信用済み団体が開始したハンドシェイク
バッジ準備
DIR参照及び属性値を送信
属性状態変更又は認証の再利用
バッジ有効性検証及び認証
暗号学的証明＋メタデータの発行
510
515

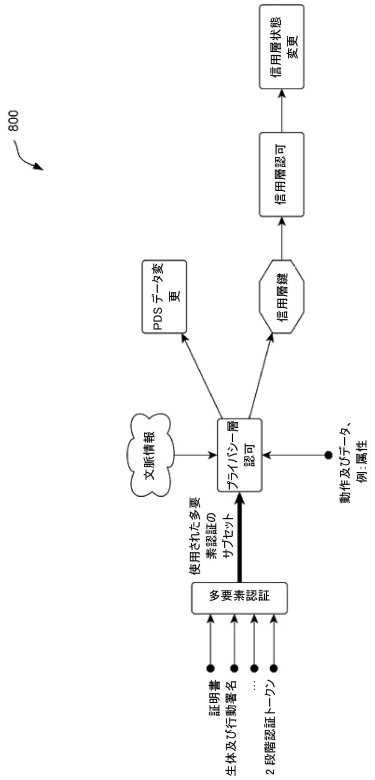
【図６】


600
信用済み団体Aのバッジ
605A
名
姓
社会保障番号
現住所
信用済み団体Cのバッジ
605C
現住所
（再利用された認証）
名
姓
電子メールアドレス
信用済み団体Bのバッジ
605B
姓
（再利用された認証）
名
パスポート番号
電話番号
信用済み団体Dのバッジ
605D
現住所
（再利用された認証）
姓名
社会保障番号
交際状況

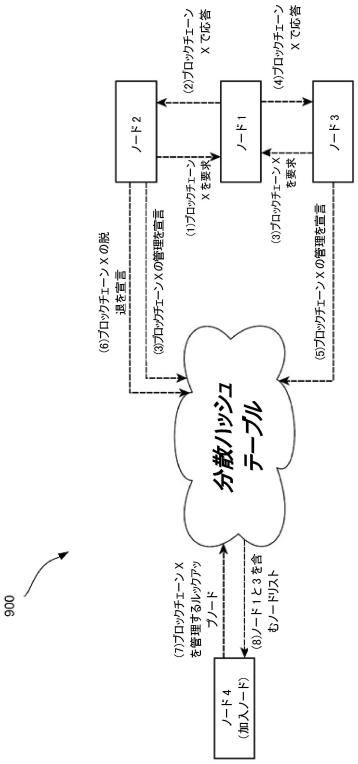
【図７】


700
同期＆変更イベント
分散台帳
同期＆変更イベント
分散台帳のローカルコピー
分散台帳のローカルコピー
相手方B
相手方A
705
710
オフレジャーAPIを介した通信
相手方の1つにより開始されたハンドシェイク
正しさの検証及び属性証明者のチェック
関連DIR参照と共にアイデンティティ情報を交換
正しさの検証及び属性証明者のチェック

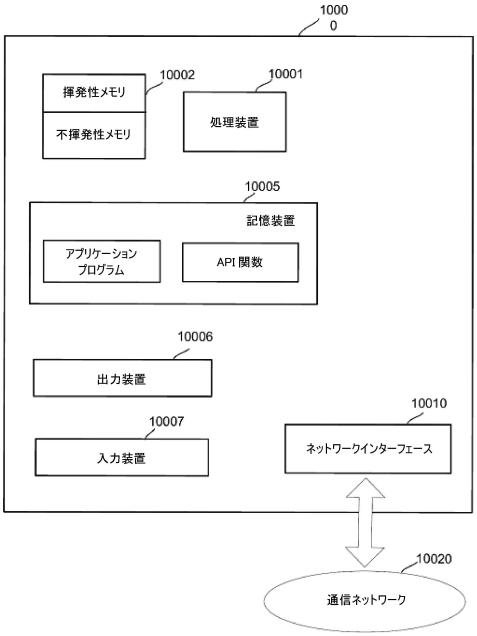
【図８】


800
信用層状態変更
信用層認可
信用層鍵
PDSデータ変更
文脈情報
プライバシー層認可
動作及びデータ、例：属性
使用された多要素認証のサブセット
多要素認証
証明書
生体及び行動署名
2段階認証トークン

【図９】


900
ノード２
ノード１
ノード３
ノード４
（加入ノード）
分散ハッシュテーブル
(1)ブロックチェーンXを要求
(2)ブロックチェーンXで応答
(3)ブロックチェーンXを要求
(4)ブロックチェーンXで応答
(5)ブロックチェーンXの管理を宣言
(6)ブロックチェーンXの脱退を宣言
(3)ブロックチェーンXの管理を宣言
(7)ブロックチェーンXを管理するルックアップノード
(8)ノード１と３を含むノードリスト

【図１０】


10000
揮発性メモリ
不揮発性メモリ
10002
処理装置
10001
記憶装置
10005
アプリケーションプログラム
API 関数
出力装置
10006
入力装置
10007
ネットワークインターフェース
10010
通信ネットワーク
10020

フロントページの続き

(31)優先権主張番号 62/325,880
(32)優先日 平成28年4月21日(2016.4.21)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 62/380,467
(32)優先日 平成28年8月28日(2016.8.28)
(33)優先権主張国・地域又は機関
米国(US)

(72)発明者 バルガヴァ，アロック
アメリカ合衆国，マサチューセッツ州 ０２４５９，ニュートン，ボンテンポ ロード ３３
(72)発明者 オーバーハウサー，アレックス
アメリカ合衆国，マサチューセッツ州 ０２１５５，メドフォード，フレデリック アベニュー １０
(72)発明者 コモンズ，マシュー
アメリカ合衆国，マサチューセッツ州 ０２１４０，ケンブリッジ，リッチデール アベニュー １，ユニット １０

審査官 行田 悦資

(56)参考文献 特開２００６－１６５８８１（ＪＰ，Ａ）
特開２００３－３４８０７７（ＪＰ，Ａ）
特開２００４－２１３４６１（ＪＰ，Ａ）
米国特許出願公開第２０１５／０２４４６９０（ＵＳ，Ａ１）
特開２００５－２５２６２１（ＪＰ，Ａ）
特開２０１３－１３７５８８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／６４
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｑ １０／０６