(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7196174号
(P7196174)

(45)発行日　令和4年12月26日(2022.12.26)

(24)登録日　令和4年12月16日(2022.12.16)

(51)国際特許分類

Ｇ０６Ｆ　21/33　(2013.01)		Ｇ０６Ｆ	21/33
Ｇ０６Ｆ　21/41　(2013.01)		Ｇ０６Ｆ	21/41

ＦＩ

請求項の数　20　（全33頁）

(21)出願番号　特願2020-527823(P2020-527823)
(86)(22)出願日　平成30年11月19日(2018.11.19)
(65)公表番号　特表2021-503667(P2021-503667A)
(43)公表日　令和3年2月12日(2021.2.12)
(86)国際出願番号　PCT/EP2018/081710
(87)国際公開番号　WO2019/097046
(87)国際公開日　令和1年5月23日(2019.5.23)
審査請求日　令和3年4月23日(2021.4.23)
(31)優先権主張番号　15/817,424
(32)優先日　平成29年11月20日(2017.11.20)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
Ｎｅｗ　Ｏｒｃｈａｒｄ　Ｒｏａｄ，　Ａｒｍｏｎｋ，　Ｎｅｗ　Ｙｏｒｋ　１０５０４，　Ｕｎｉｔｅｄ　Ｓｔａｔｅｓ　ｏｆ　Ａｍｅｒｉｃａ
(74)代理人　100112690
弁理士　太佐 種一

最終頁に続く

(54)【発明の名称】　委任アイデンティティを使用した認証方法、システム、プログラム

(57)【特許請求の範囲】

【請求項１】

暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のためのコンピュータ実装方法であって、

暗号化によりセキュリティ保護された前記レジスタは、ユーザのルート・アイデンティティを含み、前記ルート・アイデンティティは、ルート識別子と、前記ユーザを認証するために前記ルート識別子に割り当てられたクレデンシャルとを含み、暗号化によりセキュリティ保護された前記レジスタは、前記ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含み、前記委任アイデンティティのそれぞれが、委任識別子を含み、認証コンテキストに割り当てられ、

前記方法は、コンピュータが、

アイデンティティ・プロバイダとして前記ユーザを認証することを求める認証要求を受け取ることと、

前記ユーザの前記ルート・アイデンティティを使用して前記ユーザを認証することであって、成功裏の認証が前記ユーザの前記ルート・アイデンティティの前記ルート識別子に割り当てられた前記クレデンシャルを受け取ることを求める、前記認証することと、

要求された前記認証の認証コンテキストを識別することと、

前記ユーザの前記ルート・アイデンティティに割り当てられ、識別された前記認証コンテキストに割り当てられた、前記１つまたは複数の委任アイデンティティのうちの１つを、暗号化によりセキュリティ保護された前記レジスタを使用して識別することと、

前記ルート・アイデンティティを使用した前記ユーザの成功裏の認証に応答して、前記成功裏のユーザ認証を証明するとともに識別された前記委任アイデンティティの前記委任識別子によって成功裏に認証された前記ユーザを識別する認証トークンを発行することと
を実行する、コンピュータ実装方法。
【請求項２】
暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のためのコンピュータ実装方法であって、
暗号化によりセキュリティ保護された前記レジスタは、ユーザのルート・アイデンティティを含み、前記ルート・アイデンティティは、ルート識別子と、前記ユーザを認証するために前記ルート識別子に割り当てられたクレデンシャルとを含み、暗号化によりセキュリティ保護された前記レジスタは、前記ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含み、前記委任アイデンティティのそれぞれが、委任識別子を含み、認証コンテキストに割り当てられ、
前記方法は、コンピュータが、
前記ユーザを認証することを求める認証要求を受け取ることと、
前記ユーザの前記ルート・アイデンティティを使用して前記ユーザを認証することであって、成功裏の認証が前記ユーザの前記ルート・アイデンティティの前記ルート識別子に割り当てられた前記クレデンシャルを受け取ることを求める、前記認証することと、
要求された前記認証の認証コンテキストを識別することと、
前記ユーザの前記ルート・アイデンティティに割り当てられ、識別された前記認証コンテキストに割り当てられた、前記１つまたは複数の委任アイデンティティのうちの１つを、暗号化によりセキュリティ保護された前記レジスタを使用して識別することと、
前記ルート・アイデンティティを使用した前記ユーザの成功裏の認証に応答して、前記成功裏のユーザ認証を確認するとともに識別された前記委任アイデンティティの前記委任識別子によって認証された前記ユーザを識別する、認証トークンを発行することと
を実行し、前記ルート・アイデンティティは、前記ルート・アイデンティティに割り当てられた複数の委任アイデンティティを含み、前記複数の委任アイデンティティは、前記複数の委任アイデンティティのうちの少なくとも第１の１つの委任アイデンティティが前記複数の委任アイデンティティのうちの少なくとも第２の１つの委任アイデンティティを介して前記ルート・アイデンティティに割り当てられた、木構造の形態で、前記ルート・アイデンティティに割り当てられる、コンピュータ実装方法。
【請求項３】
前記方法は、コンピュータが、前記ユーザの前記ルート・アイデンティティを使用して、各自の前記ルート・アイデンティティに割り当てられたすべての委任アイデンティティについてシングル・サイン・オンを行う、請求項１または２に記載の方法。
【請求項４】
暗号化によりセキュリティ保護された前記レジスタは、コンピュータ可読プログラム・コードを含み、認証側コンピュータ・システムのプロセッサによる前記コンピュータ可読プログラム・コードの実行が、前記ユーザ認証の実行と前記認証トークンの発行とを行うように前記プロセッサに前記認証側コンピュータ・システムを制御させる、請求項１ないし３のいずれかに記載の方法。
【請求項５】
前記レジスタの暗号化によるセキュリティは、格納された前記ルート・アイデンティティおよび格納された前記１つまたは複数の委任アイデンティティの少なくとも一部のハッシュ化と、署名と、暗号化とのうちの１つまたは複数を含む、請求項１ないし４のいずれかに記載の方法。
【請求項６】
暗号化によりセキュリティ保護された前記レジスタは分散レジスタであり、前記分散レジスタのコピーが複数のコンピュータ・システムに分散される、請求項１ないし５のいずれかに記載の方法。

【請求項７】
前記分散レジスタの暗号化によるセキュリティは、前記ルート・アイデンティティと前記１つまたは複数の委任アイデンティティとを、前記分散レジスタの各コピーに含まれる、ブロックチェーンの複数のブロックに格納することを含む、請求項６に記載の方法。
【請求項８】
暗号化によりセキュリティ保護された前記レジスタが中央データベースによって提供される、請求項１ないし５のいずれかに記載の方法。
【請求項９】
前記認証に使用された前記ルート・アイデンティティまたは識別された前記委任アイデンティティが無効な場合、前記認証トークンの前記発行が拒否される、請求項１ないし８のいずれかに記載の方法。
【請求項１０】
前記認証要求は、認証に使用される前記ルート・アイデンティティの前記ルート識別子を含むか、または、前記ユーザの認証に使用される前記ルート・アイデンティティに割り当てられ、識別された前記認証コンテキストに割り当てられた前記委任識別子を含む、請求項１ないし９のいずれかに記載の方法。
【請求項１１】
前記認証要求は、暗号化によりセキュリティ保護された前記レジスタにアクセスすることができるアイデンティティ・プロバイダ・コンピュータ・システムによって受け取られ、前記アイデンティティ・プロバイダ・コンピュータ・システムは、前記ユーザの前記認証と、識別された前記委任アイデンティティの前記委任識別子によって成功裏に認証された前記ユーザを識別する前記認証トークンの前記発行とを行う、請求項１ないし１０のいずれかに記載の方法。
【請求項１２】
前記認証要求は、サービス・プロバイダ・コンピュータ・システムから受け取られ、前記ユーザを認証するために使用される前記クレデンシャルはユーザ・コンピュータ・システムから受け取られる、請求項１１に記載の方法。
【請求項１３】
前記１つまたは複数の委任アイデンティティは、それぞれ、前記それぞれの委任アイデンティティの有効性が満了する有効期限日を示す標識を含む、請求項１ないし１２のいずれかに記載の方法。
【請求項１４】
前記それぞれの委任アイデンティティが、前記認証のために使用される前記ルート・アイデンティティに割り当てられており、識別された前記認証コンテキストに割り当てられていると識別された前記委任アイデンティティである場合、前記１つまたは複数の委任アイデンティティのうちの少なくとも１つが、成功裏の認証のための追加の認証要件を含む、請求項１ないし１３のいずれかに記載の方法。
【請求項１５】
コンピュータが、
第１のアイデンティティ要求者から、前記ルート・アイデンティティに割り当てられたすべての委任アイデンティティを提供することを求める要求を受け取ることと、
前記第１のアイデンティティ要求者が各自の前記ルート・アイデンティティを使用して成功裏に認証された場合、前記ルート・アイデンティティに割り当てられた前記１つまたは複数の委任アイデンティティをすべて提供することと
をさらに実行する、請求項１ないし１４のいずれかに記載の方法。
【請求項１６】
前記ルート・アイデンティティに追加の委任アイデンティティを割り当てることをさらに含み、前記追加の委任アイデンティティは、追加の委任識別子を含み、追加の認証コンテキストに割り当てられ、前記追加の認証コンテキストは、さらなるルート・アイデンティティに依存し、前記割り当てることは、コンピュータが、

前記追加の委任アイデンティティを割り当てることを求める要求を受け取ることと、
前記追加の委任アイデンティティの前記追加の認証コンテキストを調べることと、
前記追加の認証コンテキストが前記さらなるルート・アイデンティティに依存する場合、前記追加の認証コンテキストが依存する前記さらなるルート・アイデンティティを使用して成功裏に認証されたさらなるユーザから前記追加の委任アイデンティティの承認を受け取ることに応答して、前記ルート・アイデンティティに割り当てられた前記追加の委任アイデンティティを、暗号化によりセキュリティ保護された前記レジスタに格納することとを含む、請求項１ないし１５のいずれかに記載の方法。

【請求項１７】

コンピュータ可読プログラム・コードが実現されたコンピュータ・プログラムであって、前記コンピュータ可読プログラム・コードは、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のための方法を実装するように構成され、暗号化によりセキュリティ保護された前記レジスタは、ユーザのルート・アイデンティティを含み、前記ルート・アイデンティティは、ルート識別子と前記ユーザを認証するために前記ルート識別子に割り当てられたクレデンシャルとを含み、暗号化によりセキュリティ保護された前記レジスタは、前記ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含み、前記委任アイデンティティのそれぞれが、委任識別子を含み、認証コンテキストに割り当てられ、
前記コンピュータ・プログラムは、コンピュータに、
アイデンティティ・プロバイダとして前記ユーザを認証することを求める認証要求を受け取ることと、
前記ユーザの前記ルート・アイデンティティを使用して前記ユーザを認証することであって、成功裏の認証が前記ユーザの前記ルート・アイデンティティの前記ルート識別子に割り当てられた前記クレデンシャルを受け取ることを求める、前記認証することと、
要求された前記認証の認証コンテキストを識別することと、
前記ユーザの前記ルート・アイデンティティに割り当てられ、識別された前記認証コンテキストに割り当てられた、前記１つまたは複数の委任アイデンティティのうちの１つを、暗号化によりセキュリティ保護された前記レジスタを使用して識別することと、
前記ルート・アイデンティティを使用した前記ユーザの成功裏の認証に応答して、前記成功裏のユーザ認証を証明するとともに識別された前記委任アイデンティティの前記委任識別子によって成功裏に認証された前記ユーザを識別する認証トークンを発行することと
を実行させるためのコンピュータ・プログラム。

【請求項１８】

コンピュータ可読プログラム・コードが実現されたコンピュータ・プログラムであって、前記コンピュータ可読プログラム・コードは、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のための方法を実装するように構成され、暗号化によりセキュリティ保護された前記レジスタは、ユーザのルート・アイデンティティを含み、前記ルート・アイデンティティは、ルート識別子と前記ユーザを認証するために前記ルート識別子に割り当てられたクレデンシャルとを含み、暗号化によりセキュリティ保護された前記レジスタは、前記ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含み、前記委任アイデンティティのそれぞれが、委任識別子を含み、認証コンテキストに割り当てられ、
前記コンピュータ・プログラムは、コンピュータに、
前記ユーザを認証することを求める認証要求を受け取ることと、
前記ユーザの前記ルート・アイデンティティを使用して前記ユーザを認証することであって、成功裏の認証が前記ユーザの前記ルート・アイデンティティの前記ルート識別子に割り当てられた前記クレデンシャルを受け取ることを求める、前記認証することと、
要求された前記認証の認証コンテキストを識別することと、
前記ユーザの前記ルート・アイデンティティに割り当てられ、識別された前記認証コンテキストに割り当てられた、前記１つまたは複数の委任アイデンティティのうちの１つを

、暗号化によりセキュリティ保護された前記レジスタを使用して識別することと、
前記ルート・アイデンティティを使用した前記ユーザの成功裏の認証に応答して、前記成功裏のユーザ認証を確認するとともに識別された前記委任アイデンティティの前記委任識別子によって認証された前記ユーザを識別する、認証トークンを発行することと
を実行させるためのコンピュータ・プログラムであって、前記ルート・アイデンティティは、前記ルート・アイデンティティに割り当てられた複数の委任アイデンティティを含み、前記複数の委任アイデンティティは、前記複数の委任アイデンティティのうちの少なくとも第１の１つの委任アイデンティティが前記複数の委任アイデンティティのうちの少なくとも第２の１つの委任アイデンティティを介して前記ルート・アイデンティティに割り当てられた、木構造の形態で、前記ルート・アイデンティティに割り当てられる、コンピュータ・プログラム。

【請求項１９】

暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のためのコンピュータ・システムであって、暗号化によりセキュリティ保護された前記レジスタは、ユーザのルート・アイデンティティを含み、前記ルート・アイデンティティは、ルート識別子と前記ユーザを認証するために前記ルート識別子に割り当てられたクレデンシャルとを含み、暗号化によりセキュリティ保護された前記レジスタは、前記ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含み、前記委任アイデンティティのそれぞれが、委任識別子を含み、認証コンテキストに割り当てられ、

前記コンピュータ・システムは、

アイデンティティ・プロバイダとして前記ユーザを認証することを求める認証要求を受け取り、

前記ユーザの前記ルート・アイデンティティを使用して前記ユーザを認証することであって、成功裏の認証が前記ユーザの前記ルート・アイデンティティの前記ルート識別子に割り当てられた前記クレデンシャルを受け取ることを求める、前記認証を行い、

要求された前記認証の認証コンテキストを識別し、

前記ユーザの前記ルート・アイデンティティに割り当てられ、識別された前記認証コンテキストに割り当てられた、前記１つまたは複数の委任アイデンティティのうちの１つを、暗号化によりセキュリティ保護された前記レジスタを使用して識別し、

前記ルート・アイデンティティを使用した前記ユーザの成功裏の認証に応答して、前記成功裏のユーザ認証を証明するとともに識別された前記委任アイデンティティの前記委任識別子によって成功裏に認証された前記ユーザを識別する認証トークンを発行するように構成された、コンピュータ・システム。

【請求項２０】

暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のためのコンピュータ・システムであって、暗号化によりセキュリティ保護された前記レジスタは、ユーザのルート・アイデンティティを含み、前記ルート・アイデンティティは、ルート識別子と前記ユーザを認証するために前記ルート識別子に割り当てられたクレデンシャルとを含み、暗号化によりセキュリティ保護された前記レジスタは、前記ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含み、前記委任アイデンティティのそれぞれが、委任識別子を含み、認証コンテキストに割り当てられ、

前記コンピュータ・システムは、

前記ユーザを認証することを求める認証要求を受け取り、

前記ユーザの前記ルート・アイデンティティを使用して前記ユーザを認証することであって、成功裏の認証が前記ユーザの前記ルート・アイデンティティの前記ルート識別子に割り当てられた前記クレデンシャルを受け取ることを求める、前記認証を行い、

要求された前記認証の認証コンテキストを識別し、

前記ユーザの前記ルート・アイデンティティに割り当てられ、識別された前記認証コンテキストに割り当てられた、前記１つまたは複数の委任アイデンティティのうちの１つを、暗号化によりセキュリティ保護された前記レジスタを使用して識別し、

前記ルート・アイデンティティを使用した前記ユーザの成功裏の認証に応答して、前記成功裏のユーザ認証を確認するとともに識別された前記委任アイデンティティの前記委任識別子によって認証された前記ユーザを識別する、認証トークンを発行するように構成され、前記ルート・アイデンティティは、前記ルート・アイデンティティに割り当てられた複数の委任アイデンティティを含み、前記複数の委任アイデンティティは、前記複数の委任アイデンティティのうちの少なくとも第１の１つの委任アイデンティティが前記複数の委任アイデンティティのうちの少なくとも第２の１つの委任アイデンティティを介して前記ルート・アイデンティティに割り当てられた、木構造の形態で、前記ルート・アイデンティティに割り当てられる、コンピュータ・システム。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、電子データ処理の分野に関し、より具体的には、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のためのコンピュータ実装方法に関する。

【背景技術】

【０００２】

認証は、コンピュータ・システムやコンピュータ・システムよって提供される資源へのアクセス制御の基本構成要素である。許可されたユーザだけがアクセスすることができるように保証するために、それぞれのアイデンティティのために設定された特権を認めるようにある程度の信用度でユーザのアイデンティティ確認を行うための認証手続きが必要である。

【０００３】

しかし、ネットワークを介した認証手続きは、ネットワークを介してユーザのアイデンティティの信用を遠隔で確立し、提示する必要があるため、技術的な課題を生じさせる可能性がある。これは、共用コンピュータ・システムおよびそれらのシステムによって提供される資源へのユビキタス・アクセスを可能にすることを意図したネットワークの環境では特にそうなる可能性がある。ユーザは、複数の独立したコンピュータ・システムまたは、それらのシステムによって提供されるアプリケーションなどの独立した資源に認証を受ける必要に直面することがある。このようなコンピュータ・システムまたはアプリケーションのそれぞれの認証を受けるために、ユーザは、コンピュータ・システムまたはアプリケーションの認証を受けるための個々の認証データを使用することがある。しかし、コンピュータ・システムまたはソフトウェア・システムの数が増大し続けているため、個々のレベルでのそのような認証手法は、ますます実際的ではなくなる可能性がある。

【０００４】

関連はしているが独立している複数のソフトウェア・システムまたはハードウェア・システムのための認証を容易にするために、シングル・サイン・オン（single sign-on：ＳＳＯ）を実装することができる。ＳＳＯを使用すると、ユーザは、異なる認証データを使用することなく、単一の認証データのセットを使用して接続システムまたは複数の接続システムに認証を受けることができるようになる。ＳＳＯは、当事者間で認証データをやり取りするためのオープン・スタンダードであるＳＡＭＬ（Security Assertion Markup Language（セキュリティ・アサーション・マークアップ・ランゲージ））を使用して実装可能である。ＳＡＭＬの仕様は、プリンシパルと、アイデンティティ・プロバイダと、サービス・プロバイダという３つの役割を定義している。プリンシパルがサービス・プロバイダにサービスを要求すると、サービス・プロバイダは、アイデンティティ・プロバイダに認証アサーションを要求する。アイデンティティ・プロバイダは、プリンシパルを認証し、サービス・プロバイダに認証アサーションを与える。このアサーションに基づいて、サービス・プロバイダはアクセス制御の決定を行うこと、すなわち、接続されているプリンシパルのために何らかのサービスを行うか否かを決定することができる。

【０００５】

シングル・サイン・オンは、アイデンティティ・プロバイダとサービス・プロバイダと

の間の信用関係を保証する１つのセキュリティ領域内で行うのは比較的容易であるが、ＳＳＯを複数のセキュリティ領域にわたって拡張するのは難しくなる。したがって、ユーザ認証の性能を向上させることの絶えない要望がある。

【発明の概要】

【０００６】

種々の実施形態が、独立請求項の主題によって説明されているように、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証方法と、その方法を実行するためのコンピュータ・プログラム製品とコンピュータ・システムとを提供する。有利な実施形態が従属請求項に記載されている。本発明の実施形態は、それらの実施形態が互いに排反しない場合、互いに自由に組み合わせることができる。

【０００７】

一態様では、本発明は、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のためのコンピュータ実装方法に関する。暗号化によりセキュリティ保護されたレジスタは、ユーザのルート・アイデンティティを含む。ルート・アイデンティティは、ルート識別子と、ユーザを認証するためにそのルート識別子に割り当てられたクレデンシャルとを含む。暗号化によりセキュリティ保護されたレジスタは、ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含む。委任アイデンティティのそれぞれは、委任識別子を含み、認証コンテキストに割り当てられる。

【０００８】

この方法は以下を含む。ユーザを認証することを求める認証要求が受け取られる。ユーザは、そのユーザのルート・アイデンティティを使用して認証される。成功裏の認証には、ユーザのルート・アイデンティティのルート識別子に割り当てられたクレデンシャルを受け取ることが求められる。要求された認証の認証コンテキストが識別される。ユーザのルート・アイデンティティに割り当てられ、識別された認証コンテキストに割り当てられた、１つまたは複数の委任アイデンティティのうちの１つの委任アイデンティティが、暗号化によりセキュリティ保護されたレジスタを使用して識別される。ルート・アイデンティティを使用したユーザの成功裏の認証に応答して、認証トークンが発行され、それによって成功裏のユーザ認証を確認し、識別された委任アイデンティティの委任識別子によって成功裏に認証されたユーザを識別する。

【０００９】

他の態様では、本発明は、ルート・アイデンティティに追加の委任アイデンティティを割り当てることをさらに含む方法に関する。追加の委任アイデンティティは、追加の委任識別子を含み、追加の認証コンテキストに割り当てられる。追加の認証コンテキストは、さらなるルート・アイデンティティに依存する。割り当ては、追加の委任アイデンティティを割り当てることを求める要求を受け取ることを含む。追加の委任アイデンティティの追加の認証コンテキストが調べられる。追加の認証コンテキストが上記さらなるルート・アイデンティティに依存する場合、ルート・アイデンティティに割り当てられた追加の委任アイデンティティは、上記追加の認証コンテキストが依存する上記さらなるルート・アイデンティティを使用して認証に成功したさらなるユーザから追加の委任アイデンティティの承認を受け取ることに応答して、暗号化によりセキュリティ保護されたレジスタに格納される。

【００１０】

他の態様では、本発明は、コンピュータ可読プログラム・コードが実現されている不揮発性コンピュータ可読記憶媒体を含むコンピュータ・プログラム製品に関する。コンピュータ可読プログラム・コードは、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証方法を実装するように構成される。暗号化によりセキュリティ保護されたレジスタは、ユーザのルート・アイデンティティを含む。ルート・アイデンティティは、ルート識別子と、ユーザを認証するためのそのルート識別子に割り当てられたクレデンシャルとを含む。暗号化によりセキュリティ保護されたレジスタは、ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含む。委任アイデン

ティティのそれぞれは、委任識別子を含み、認証コンテキストに割り当てられる。
【００１１】
コンピュータ可読プログラム・コードによって実装される方法は、以下を含む。ユーザを認証することを求める認証要求が受け取られる。ユーザは、そのユーザのルート・アイデンティティを使用して認証される。成功裏な認証には、ユーザのルート・アイデンティティのルート識別子に割り当てられたクレデンシャルを受け取ることが求められる。要求された認証の認証コンテキストが識別される。ユーザのルート・アイデンティティに割り当てられ、識別された認証コンテキストに割り当てられた、１つまたは複数の委任アイデンティティのうちの１つの委任アイデンティティが、暗号化によりセキュリティ保護されたレジスタを使用して識別される。ルート・アイデンティティを使用したユーザの成功裏の認証に応答して、認証トークンが発行され、それによって成功裏のユーザ認証を確認し、識別された委任アイデンティティの委任識別子によって成功裏に認証されたユーザを識別する。
【００１２】
他の態様では、本発明は、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のためのコンピュータ・システムに関する。暗号化によりセキュリティ保護されたレジスタは、ユーザのルート・アイデンティティを含む。ルート・アイデンティティは、ルート識別子と、ユーザを認証するためにそのルート識別子に割り当てられたクレデンシャルとを含む。暗号化によりセキュリティ保護されたレジスタは、ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含む。委任アイデンティティのそれぞれは、委任識別子を含み、認証コンテキストに割り当てられる。
【００１３】
コンピュータ・システムは、以下を実行するように構成される。ユーザを認証することを求める認証要求が受け取られる。ユーザは、そのユーザのルート・アイデンティティを使用して認証される。成功裏な認証には、ユーザのルート・アイデンティティのルート識別子に割り当てられたクレデンシャルを受け取ることが求められる。要求された認証の認証コンテキストが識別される。ユーザのルート・アイデンティティに割り当てられ、識別された認証コンテキストに割り当てられた、１つまたは複数の委任アイデンティティのうちの１つの委任アイデンティティが、暗号化によりセキュリティ保護されたレジスタを使用して識別される。ルート・アイデンティティを使用したユーザの成功裏の認証に応答して、認証トークンが発行され、それによって成功裏のユーザ認証を確定し、識別された委任アイデンティティの委任識別子によって成功裏に認証されたユーザを識別する。
【００１４】
以下では、図面を参照しながら例示としてのみ本発明の実施形態について詳細に説明する。
【図面の簡単な説明】
【００１５】
【図１】ユーザ認証を実装するのに適する第１の例示のコンピュータ・システムを示す図である。
【図２】ユーザ認証を実装するのに適する第２の例示のコンピュータ・システムを示す図である。
【図３】ユーザ認証を実装する概略インフラストラクチャを示す図である。
【図４】委任アイデンティティの例示の割り当ての概略図を示す図である。
【図５】委任アイデンティティの例示の依存関係の概略図を示す図である。
【図６】例示のユーザ認証の概略流れ図を示す図である。
【図７】例示のブロックチェーンの概略図を示す図である。
【発明を実施するための形態】
【００１６】
本発明の様々な実施形態の説明を、例示を目的として示すが、網羅的であること、または開示されている実施形態に限定されることを意図しない。記載されている実施形態の範

囲および思想から逸脱することなく、当業者には多くの変更および変形が明らかであろう。本明細書で使用されている用語は、実施形態の原理、実際の適用、市場に見られる技術に優る技術的改良を最もよく説明するため、または当業者が本明細書で開示されている実施形態を理解することができるように選定された。

【００１７】

実施形態は、１つまたは複数の委任アイデンティティが提供されるという有利な効果を有し得る。委任アイデンティティのそれぞれが、特定の認証コンテキストに割り当てられる。認証コンテキストは、例えば、ユーザがアクセスを試みる資源が割り当てられているプロジェクトまたは組織に依存し得る。アクセスの許可はそれぞれのユーザの成功裏な認証に依存する。個別の認証コンテキストのそれぞれについて、ユーザは認証のために常に自分のルート・アイデンティティを使用することができる。これは、各自のルート・アイデンティティに割り当てられたすべての委任アイデンティティについて、ユーザのルート・アイデンティティを使用するシングル・サイン・オンに相当する。ユーザは、ルート識別子と、ルート・アイデンティティに含まれるクレデンシャルとを覚えておき、提供するだけで済む。ルート識別子は、例えばユーザ名の形態で提供することができ、クレデンシャルは例えばパスワードの形態で提供することができる。

【００１８】

クレデンシャルとは、暗号クレデンシャル、すなわち、通信に対する当事者のアイデンティティ確認を行うために使用される情報を指す。この情報は、特定の実際の個人または団体にとってのみ利用可能であるものとする。暗号クレデンシャルは、例えば機械可読暗号鍵、バイオメトリクス（例えば指紋、音声認識、網膜スキャン）の形態、またはパスワードの形態、あるいはこれらの組合せで提供することができる。クレデンシャルは、自己発行されるか、または信用のある第三者によって発行されてもよく、多くの場合、発行の唯一の基準は、クレデンシャルが特定の実際の個人または団体に一義的に関連付けられていることである。クレデンシャルは、一定期間後に満了するように構成されてもよい。ｘ．５０９証明書のような証明書が、クレデンシャルの他の例である。

【００１９】

ルート・アイデンティティを使用するユーザの認証が成功した場合に発行される認証トークンは、識別された委任アイデンティティの委任識別子にのみ関係し得る。認証トークンは、例えば、その真正性を証明するために署名されてもよい。基礎にあるルート・アイデンティティに関する詳細は開示されない。それぞれの認証トークンは、ユーザが成功裏の認証を証明するために使用することができる。認証トークンの受領者は、ユーザの委任識別子のみを知る。したがって、受領者の観点から見ると、ユーザは、委任アイデンティティによって成功裏に認証される。認証トークンの正当性とその保全性とを証明するために、例えばアイデンティティ・プロバイダ・システムのような認証トークンの発行者が認証トークンに署名してもよい。認証トークンに署名するために、アイデンティティ・プロバイダ・コンピュータ・システムが、アイデンティティ・プロバイダに割り当てられた秘密暗号鍵を使用してもよい。

【００２０】

実施形態は、複数の異なる認証コンテキスト、例えば、異なる組織の異なるプロジェクトのために、それらの認証コンテキストのそれぞれのためのユーザの個々の委任アイデンティティを提供するという有効な効果を有し得る。認証コンテキストは、例えば、認証要求を出すために使用されるＵＲＬなど、コンテキスト標識を使用して識別することができる。

【００２１】

サービス・プロバイダ・コンピュータ・システムが、異なる組織にサービスを提供することができる。それぞれのサービスは、同じであってもよく、または組織固有であってもよい。サービスは、例えばクラウド・サービスであってもよい。サービス・プロバイダによって提供されるサービスにアクセスするために、ユーザは、例えば、組織固有のＵＲＬを使用することができる。あるいは、ユーザは、汎用ＵＲＬを使用し、また、ユーザがそ

のためにサービス・プロバイダのサービスにアクセスを試みる組織またはユーザがその一員である組織を示す標識を入力することによって、認証コンテキストを提供してもよい。それぞれの標識は、例えば、組織名の形態で提供されてもよい。

【００２２】

それぞれの追加の委任アイデンティティの追加の認証コンテキストが依存するさらなるユーザからの追加の委任アイデンティティの承認を必要とすることは、効率的なテスト手続きが実装されるという有利な効果を有し得る。したがって、追加の委任アイデンティティを成功裏に割り当てることにより、それぞれの追加の委任アイデンティティの依存関係を証明し得る。したがって、委任アイデンティティは、さらなるルート・アイデンティティに依存し得る。各自のさらなるルート・アイデンティティは、例えば追加の委任アイデンティティが使用されるコンテキストにおける人物または組織のルート・アイデンティティであってよい。追加の委任アイデンティティは、例えば、そのさらなるルート・アイデンティティを有する組織のメンバーのアイデンティティとすることができる。したがって、追加の委任アイデンティティは、それぞれの組織がその追加のメンバーの追加の委任アイデンティティを承認する場合にのみ割り当てられ得る。

【００２３】

実施形態によると、この方法は、ユーザのルート・アイデンティティを使用して、各自のルート・アイデンティティに割り当てられたすべての委任アイデンティティについてシングル・サイン・オンを行う。実施形態は、複数の異なるコンテキストのために異なる委任アイデンティティを使用することができるという有利な効果を有し得る。ユーザは、これらのコンテキストのそれぞれにおいて自分のルート・アイデンティティを使用して認証することができるようになる一方、ルート・アイデンティティは、認証トークンの受領者、例えばユーザが認証を受けるサービス・プロバイダに開示されない。

【００２４】

実施形態によると、ルート・アイデンティティは、そのルート・アイデンティティに割り当てられた複数の委任アイデンティティを含む。複数の委任アイデンティティは、複数の委任アイデンティティのうちの少なくとも第１の１つの委任アイデンティティが、複数の委任アイデンティティのうちの少なくとも第２の１つの委任アイデンティティを介してルート・アイデンティティに割り当てられた、木構造の形態で、ルート・アイデンティティに割り当てられる。

【００２５】

実施形態は、委任アイデンティティがすべて、ルート・アイデンティティへのその委任アイデンティティの割り当てに依存するという有利な効果を有し得る。ルート・アイデンティティが失効させられた場合、各自のルート・アイデンティティに割り当てられたすべての委任アイデンティティも無効になる。木状構造は、さらに、委任アイデンティティのうちの１つまたは複数の委任アイデンティティを、委任アイデンティティのうちの他の委任アイデンティティを介してルート・アイデンティティに割り当てることができるという有利な効果も有し得る。例えば、ユーザに、認証コンテキストとしての特定の組織に割り当てられた委任識別子を含む委任アイデンティティを与えることができる。それぞれの組織は、１つまたは複数の下位組織または系列組織を含み得る。それぞれの下位組織または系列組織の全部またはそのうちの選択された組織のために、ユーザに、それぞれの組織の委任アイデンティティに割り当てられたさらなる委任アイデンティティを与えることができる。したがって、ユーザがそのために認証を受けることを意図している下位組織に応じて、ユーザは、認証コンテキストとして、そのそれぞれの下位組織に割り当てられた委任識別子を含む個別委任アイデンティティを使用することができる。

【００２６】

実施形態によると、暗号化によりセキュリティ保護されたレジスタは、コンピュータ可読プログラム・コードを含む。認証側コンピュータ・システムのプロセッサによるコンピュータ可読プログラム・コードの実行によって、ユーザ認証を実行し、認証トークンを発行するように、プロセッサに認証側コンピュータ・システムを制御させる。

【００２７】
実施形態は、暗号化によりセキュリティ保護されたレジスタによって提供されるコンピュータ可読プログラム・コードを使用して、認証側コンピュータ・システムによって、認証を実行することができるという有利な効果を有し得る。したがって、認証に使用されるコンピュータ・システム、すなわち認証側コンピュータ・システムは、ユーザ認証を実行することができるようにするために特定のコンピュータ可読プログラム・コードを含む必要がない。そうではなく、それぞれのコンピュータ可読プログラム・コードは、暗号化によりセキュリティ保護されたレジスタによって与えられる。認証側コンピュータ・システムは、例えば、アイデンティティ・プロバイダ・コンピュータ・システムであってもよい。実施形態は、さらに、暗号化によりセキュリティ保護されたレジスタによってそれぞれのコンピュータ可読プログラム・コードを提供することによって、認証が不正操作によって破損されないように保証することができるという有利な効果を有し得る。また、認証は、任意の汎用コンピュータ・システムによって実行可能であり、汎用コンピュータ・システムは暗号化によりセキュリティ保護されたレジスタにアクセスできるだけでよい。分散ブロックチェーンのような分散レジスタの場合、暗号化によりセキュリティ保護されたレジスタの最新のコピーに容易にアクセスすることができる。
【００２８】
実施形態によると、レジスタの暗号化によるセキュリティは、格納されたルート・アイデンティティおよび格納された１つまたは複数の委任アイデンティティの少なくとも一部のハッシュ化と、署名と、暗号化とのうちの１つまたは複数を含む。
【００２９】
実施形態は、それぞれのレジスタに格納されたアイデンティティ、すなわち、ルート・アイデンティティおよびそれぞれのルート・アイデンティティに割り当てられた委任アイデンティティを、不正操作から有効に保護することができるという有利な効果を有し得る。例えば、レジスタは、それぞれの暗号化によりセキュリティ保護されたレジスタに格納されたアイデンティティのそれぞれのハッシュを含むことができる。また、格納されたアイデンティティは、レジスタにそれぞれのアイデンティティを生成または追加あるいはその両方を行ったユーザまたは団体の署名鍵、すなわち暗号秘密鍵によって署名されてもよい。
【００３０】
例えば、レジスタは、１つまたは複数の管理者コンピュータ・システムによって管理されてもよい。管理者コンピュータ・システムのそれぞれに、例えばルート・アイデンティティまたは委任アイデンティティを含むレジスタのエントリに署名するための暗号秘密鍵を割り当ててもよい。また、レジスタに格納されているアイデンティティを暗号化してもよい。アイデンティティは、例えば、対称暗号鍵によって、または暗号公開鍵によって暗号化することができる。したがって、これらのアイデンティティを復号するのに必要なのは、それぞれの暗号公開鍵に割り当てられた対称暗号鍵または秘密暗号鍵のみである。アイデンティティは、例えばすべて同じ暗号鍵で暗号化されてもよい。他の実施形態によると、アイデンティティは、個別の暗号鍵または異なる暗号鍵あるいはその両方によって暗号化されてもよい。例えば、同じ認証コンテキストに割り当てられたすべての委任アイデンティティが同じ暗号鍵で暗号化されてもよい。実施形態によると、同じルート・アイデンティティに割り当てられたすべての委任アイデンティティが同じ暗号鍵で暗号化されてもよい。
【００３１】
実施形態によると、暗号化によりセキュリティ保護されたレジスタは、分散レジスタであり、そのコピーが複数のコンピュータ・システムに分散される。実施形態は、分散レジスタを使用することによって、レジスタの障害の危険を低減することができるという有利な効果を有し得る。特に、単一点障害を防止することができる。レジスタの他のコピーが損なわれていない限り、レジスタを復旧させることができる。また、レジスタの管理または維持あるいはその両方のワークロードをそれぞれの複数のコンピュータ・システムに分

散させることができる。

【００３２】

実施形態によると、分散レジスタの暗号化によるセキュリティは、ルート・アイデンティティと、１つまたは複数の委任アイデンティティとを、分散レジスタの各コピーに含まれる、ブロックチェーンの複数のブロックに格納することを含む。実施形態は、改ざん防止と、アイデンティティを管理するための共用インフラストラクチャとを提供するという有利な効果を有する。これは、格納されたアイデンティティの不正操作に対抗する有効な手段を提供することができる。

【００３３】

ブロックチェーンとは、連結され、暗号を使用してセキュリティ保護されたレコード、いわゆるブロックのリストを含むレジスタを指す。各ブロックは、前のブロックへのリンクとしてのハッシュ・ポインタと、それぞれのブロックの生成時刻を識別するタイムスタンプと、それぞれのブロックに格納されたデータとを含むことができる。ブロックチェーンは、ブロックに格納されているデータの変更に対して本質的に耐性を有し得る設計になっている。ブロックチェーンは、データを効率的かつ検証可能な永続的な方式で記録することができる開放された分散データベースとして機能することができる。分散レジスタとして使用する場合、ブロックチェーンは、例えば、ブロックチェーンに追加される追加のブロックを検証するためのプロトコルに集合的に準拠するピア・ツー・ピア・ネットワークによって管理される。記録された後は、どのブロック内のデータも、ネットワークの大多数が結託することを必要とするそれ以降のすべてのブロックの変更がない限り、遡って変更することができない。

【００３４】

ブロックチェーン・データベースは、格納データとブロックの２種類のレコードからなり得る。ブロックは、ハッシュ化されて、例えばマークル木としてコード化された、格納データを保持する。各ブロックは、ブロックチェーン内の直前のブロックのハッシュを含むことができ、ハッシュはこれら２つのブロックを連結する。連結されたブロックは、チェーンを形成することができる。この相互作用的プロセスにより、ブロックチェーンの最初のブロックである、いわゆるジェネシス・ブロックまで遡って前のブロックの保全性を確定することができる。

【００３５】

ブロックチェーンのブロックは、スマート・コントラクトとも呼ばれる実行可能プログラム命令も含むことができる。それぞれのプログラム命令は、ブロックチェーンに追加のエントリを追加するために、または、ブロックチェーンに格納されている情報にアクセスするために、または、ブロックチェーンによって定義されている他の何らかのタスクを行うために、コンピュータ・システムのプロセッサによって実行可能である。ブロックチェーンを使用して実行可能プログラム命令を提供することは、実行可能プログラム命令を、不正操作に対して暗号化によってセキュリティ保護することができるという有利な効果を有し得る。また、分散ブロックチェーンは、それぞれのプログラム命令を分散させる効率的な方法を提供し得る。実行可能プログラム命令は、検証可能とすることができ、署名され、プログラミング言語でコード化することができる。

【００３６】

ブロックチェーンは、意図的にセキュリティ保護されるようにすることができ、非集中型コンセンサスを実現する高いビザンチン・フォールト・トレラント性を備えた分散コンピューティング・システムを提供することができる。

【００３７】

実施形態によると、ブロックチェーンは、異なる識別プロバイダ間で共用することができる。ブロックチェーンは、参加者のそれぞれがブロックチェーンのコピーを有するように複製することができる。これは、ブロックチェーンに追加される追加ブロックを検証するためのプロトコルに集合的に準拠するピア・ツー・ピア・ネットワークによって管理することができる。したがって、ブロックチェーンは、改ざん防止と共用インフラストラク

チャとを提供するという有利な効果を有し得る。

【００３８】

ブロックチェーンに追加のエントリを追加するには、参加者のコンセンサスが必要であってもよい。ピア・ツー・ピア・ネットワークを介して、すべての参加者がそのエントリに合意し、そのエントリを検証することができる。実施形態によると、エントリを検証するための規則を設定することができる。これらの規則は、例えば、ブロックチェーン自体に含まれる実行可能プログラム命令によって実装可能である。実施形態は、トラステッドである参加者とトラストレスな参加者とに基づく低ワークロードなコミットメントを可能にするという有利な効果を有し得る。エントリは、暗号化し、ハッシュ化し、検証ノードのネットワークに送信することができる。

【００３９】

実施形態によると、暗号化によりセキュリティ保護されたレジスタを中央データベースによって提供することができる。実施形態は、中央データベースの形態で、レジスタの簡易で信頼性のある実装形態を提供することができるという有利な効果を有し得る。実施形態によると、中央データベースは、暗号化によりセキュリティ保護され、監査可能な共通データベースとすることができる。すべてのアイデンティティを含む中央データベースは、任意の委任識別子を、例えば組織などの異なるコンテキストに連結することを可能にし得る。

【００４０】

実施形態によると、認証に使用されたルート・アイデンティティまたは識別された委任アイデンティティが無効な場合は、認証トークンの発行が拒否される。

【００４１】

実施形態は、それぞれの委任アイデンティティが割り当てられたルート・アイデンティティを無効にすることによって委任アイデンティティのいずれかを使用する認証を容易に防止することができるという有利な効果を有し得る。無効化は、例えば失効させることよって行うことができる。また、例えば、ユーザが、それぞれの委任アイデンティティの認証コンテキストを与える組織にもはや勤務していない場合に、個別委任アイデンティティを失効させてもよい。また、委任アイデンティティが無効な場合、そのそれぞれの委任アイデンティティに割り当てられているすべての委任アイデンティティ、すなわち、そのそれぞれの委任アイデンティティを介してルート・アイデンティティに割り当てられたすべての委任アイデンティティも無効にすることができる。言い換えると、識別された委任アイデンティティが、無効な委任アイデンティティを介してルート・アイデンティティに割り当てられている場合、認証トークンの発行を拒否することができる。実施形態は、ある人物が特定の組織にもはや勤務していない場合、その人物のアイデンティティのすべてがそのそれぞれの組織のコンテキストで使用されるわけではなく、すなわち、そのそれぞれの組織の下位組織に勤務している場合、同じ認証コンテキスト、すなわちそのそれぞれの組織を使用する他のすべての委任アイデンティティが割り当てられている委任アイデンティティを無効化、例えば失効させれば足りるという有利な効果を有し得る。

【００４２】

実施形態によると、要求は認証に使用されるルート・アイデンティティのルート識別子を含む。実施形態は、ユーザがそれぞれの認証コンテキストに割り当てられた実際の委任アイデンティティとは独立して、認証ごとにルート・アイデンティティを提供することができるという有利な効果を有し得る。

【００４３】

実施形態によると、要求は、ユーザを認証するために使用されるルート・アイデンティティに割り当てられ、識別された認証コンテキストに割り当てられた委任識別子を含む。実施形態は、要求がそれ自体で委任識別子を提供することができるという有利な効果を有し得る。したがって、例えば委任アイデンティティを、それぞれの要求によって提供される委任識別子を使用して識別することができる。

【００４４】

実施形態によると、認証要求は、暗号化によりセキュリティ保護されたレジスタにアクセス可能なアイデンティティ・プロバイダ・コンピュータ・システムによって受け取られる。アイデンティティ・プロバイダ・コンピュータ・システムは、ユーザの認証と、識別された委任アイデンティティの委任識別子によって成功裏に認証されたユーザを識別する認証トークンの発行とを行う。

【００４５】

実施形態は、ユーザの認証をアイデンティティ・プロバイダ・コンピュータ・システムによって効率的に行うことができるという有利な効果を有し得る。それぞれのアイデンティティ・プロバイダ・コンピュータ・システムによって発行された認証トークンに基づいて、ユーザに、そのそれぞれの認証トークンに含まれる委任識別子の委任アイデンティティが与えられる。

【００４６】

実施形態によると、認証要求は、サービス・プロバイダ・コンピュータ・システムから受け取る。ユーザを認証するために使用されるクレデンシャルは、ユーザ・コンピュータ・システムから受け取る。

【００４７】

実施形態は、例えば、サービス・プロバイダ・コンピュータ・システムから要求を受け取ることができるという有利な効果を有し得る。例えば、要求はユーザ・コンピュータ・システムを介してサービス・プロバイダ・コンピュータ・システムから転送されてもよい。例えば、ユーザ・コンピュータ・システムは、サービス・プロバイダ・コンピュータ・システムによって提供されるサービスにアクセスを試みることができ、サービス・プロバイダ・コンピュータ・システムは、ユーザ・コンピュータ・システム、例えばユーザ・コンピュータ・システムのブラウザを、アイデンティティ・プロバイダ・コンピュータ・システムにリダイレクトすることができる。成功裏の認証を行うために、ユーザ・コンピュータ・システムは、さらに、そのそれぞれのユーザ・コンピュータ・システムを使用してユーザのルート・アイデンティティのクレデンシャルを提供してもよい。さらに、ユーザ・コンピュータ・システムは、ユーザが認証を受けようとしている認証コンテキストに割り当てられたルート識別子または委任識別子あるいはその両方を提供することができる。

【００４８】

実施形態によると、１つまたは複数の委任アイデンティティは、それぞれ、個々の委任アイデンティティの有効性が満了する有効期限日を示す標識を含む。実施形態は、それぞれの委任アイデンティティの有効性を時間的に制限することができるという有利な効果を有し得る。これにより、この方法の、特に委任アイデンティティのセキュリティをさらに強化することができる。

【００４９】

実施形態によると、それぞれの委任アイデンティティが、認証に使用されるルート・アイデンティティに割り当てられており、識別された認証コンテキストに割り当てられていると識別された委任アイデンティティである場合、１つまたは複数の委任アイデンティティのうちの少なくとも１つが認証の成功のための追加の認証要件を含む。

【００５０】

実施形態は、委任アイデンティティが追加の認証要件を含むことができるという有利な効果を有し得る。このような追加の認証要件は、追加のパスワードまたは多元認証あるいはその両方を含み得る。例えば、それぞれの委任アイデンティティのセキュリティ・レベルは、他の委任アイデンティティよりも高くてもよい。成功裏に認証するために追加の手段を必要とすることによってセキュリティを向上させることができる。それぞれの手段は、例えば、証明書に含まれるそれぞれの暗号公開鍵に割り当てられた暗号秘密鍵を使用して生成された署名の有効性を証明するように構成された暗号公開鍵を含む、証明書を提供することを含み得る。

【００５１】

実施形態によると、さらに、ルート・アイデンティティに割り当てられたすべての委任

アイデンティティの提供を求める要求を、第１のアイデンティティ要求者から受け取る。第１のアイデンティティ要求者がそれぞれのルート・アイデンティティを使用して成功裏に認証された場合、そのルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティのすべてが提供される。

【００５２】

実施形態は、ルート・アイデンティティに割り当てられた委任アイデンティティの全体が、ルート・アイデンティティ、すなわちそれぞれのルート・アイデンティティによって認証するユーザにのみ見えるという有利な効果を有し得る。他のすべての参加者、特に認証トークンの受領者は、それぞれの当事者によって提供される特定の認証コンテキストに割り当てられた委任アイデンティティのみを知ることができる。

【００５３】

実施形態によると、追加の認証コンテキストは、さらなるルート・アイデンティティに割り当てられた１つまたは複数のさらなる委任アイデンティティを介してそのさらなるルート・アイデンティティに依存する。実施形態は、委任アイデンティティが、例えば、さらなるルート・アイデンティティの組織の下位組織のさらなる委任アイデンティティに依存することができるという有利な効果を有し得る。

【００５４】

実施形態によると、追加の委任アイデンティティの依存関係は、さらなるルート・アイデンティティのさらなるルート識別子または、さらなるルート・アイデンティティに割り当てられたさらなる委任アイデンティティのさらなる委任識別子を含む、その追加の委任アイデンティティの認証コンテキストによって実装される。実施形態は、それぞれの追加の委任アイデンティティがそれぞれ依存する、それぞれ、ルート・アイデンティティまたは委任アイデンティティのルート識別子または委任識別子の形態で提供可能な認証コンテキストによって、依存関係を実装することができるという有利な効果を有し得る。

【００５５】

実施形態によると、アイデンティティは、さらに、それぞれのアイデンティティを定義する追加の属性を含むことができる。例えば、属性は、それぞれのアイデンティティが人物のアイデンティティであるか組織のアイデンティティであるかを定義することができる。また、属性はそれぞれのアイデンティティの役割を定義することができる。

【００５６】

実施形態によると、さらに、さらなるルート・アイデンティティに依存するすべての委任アイデンティティの提供を求める要求を、第２のアイデンティティ要求者から受け取る。第２のアイデンティティ要求者がそのさらなるルート・アイデンティティを使用して成功裏に認証された場合、そのさらなるルート・アイデンティティに依存するすべての委任アイデンティティが提供される。

【００５７】

実施形態は、依存側の委任アイデンティティの全体が、委任アイデンティティの依存する各自のさらなるルート・アイデンティティにのみ見えるという有利な効果を有し得る。各自のさらなるルート・アイデンティティに割り当てられ、１つまたは複数の委任アイデンティティが依存する委任アイデンティティの場合、依存側の委任アイデンティティのみが見える。

【００５８】

実施形態によると、暗号化によりセキュリティ保護されたレジスタは、さらなるコンピュータ可読プログラム・コードを含む。割り当て側コンピュータ・システムのプロセッサによるこのさらなるコンピュータ可読プログラム・コードの実行によって、プロセッサは、ルート・アイデンティティへの追加の委任アイデンティティの割り当てを実行するように、割り当て側コンピュータ・システムを制御する。

【００５９】

実施形態は、ルート・アイデンティティに追加の委任アイデンティティを割り当てるためのコンピュータ可読プログラム・コードが、暗号化によりセキュリティ保護されたレジ

スタによって提供され、追加の委任アイデンティティを割り当てるために使用されるコンピュータ・システムによって提供される必要がないという有利な効果を有し得る。言い換えるとそれぞれの追加の委任アイデンティティは、汎用コンピュータ・システムを使用して割り当てることができ、汎用コンピュータ・システムは、そのそれぞれのレジスタにアクセスすることができるだけでよい。

【００６０】

実施形態によると、さらに、割り当てられた追加の委任アイデンティティは失効により無効にされる。失効は、失効要求者から追加の委任アイデンティティの失効を求める要求を受け取ることを含む。失効要求者は認証される。失効要求者が、追加の認証コンテキストが依存するさらなるルート・アイデンティティを使用して認証を受けることに成功したさらなるユーザである場合、追加の委任アイデンティティの失効を示す失効標識が、暗号化によりセキュリティ保護されたレジスタに追加される。

【００６１】

実施形態は、追加の委任アイデンティティをその委任アイデンティティが依存するルート・アイデンティティによって失効させることができるという有利な効果を有し得る。例えば、各自のルート・アイデンティティは、追加の委任アイデンティティの組織のルート・アイデンティティであってもよい。したがって、各自の組織は、例えばメンバーがその組織を離れる場合に追加の委任アイデンティティを失効させることが可能となる。

【００６２】

実施形態は、ユーザのアイデンティティを維持し、ＳＳＯに関与するすべての当事者間の相互の信用の輪を必要とせずに、会社間ＳＳＯ、すなわち、セキュリティ領域間ＳＳＯを可能にすることができる。ユーザは自分の認証の詳細を、暗号化によりセキュリティ保護されたレジスタ、例えばブロックチェーンによって裏打ちされたアイデンティティ・プロバイダにのみ送信すればよいため、自分の実際のアイデンティティ、すなわちルート識別子を、認証を受けたいサービス・プロバイダＳＰに明かす必要がない。

【００６３】

ルート・アイデンティティに割り当てられた委任アイデンティティのフル・セットは、ルート・アイデンティティの所有者のみに見えるようにすることができる。可用性の高い認証インフラストラクチャを稼働させる負担を複数の当事者間で分散させるために、分散レジスタ、すなわちブロックチェーンに格納されたアイデンティティを暗号化によりセキュリティ保護することができ、ブロックチェーンを通して監査することができる。

【００６４】

実施形態によると、各アイデンティティは、一意のアイデンティティ、例えばパスポートによって与えられる。したがって、パスポートを所有する各市民にルート・アイデンティティが与えられる。ルート・アイデンティティは、ルート識別子、例えばその市民の実名と、そのルート識別子に割り当てられたパスワードとを含んでもよい。その市民が認証を希望する場合、その市民はこのルート識別子、すなわち実名を明らかにしなくても済む。ルート・アイデンティティは、その代わりに、この市民が委任識別子を使用してシングル・サイン・オンを行うことができるようにする。

【００６５】

実施形態によると、委任アイデンティティの認証および識別は、単一の独立したアイデンティティ・プロバイダが実行することができる。実施形態によると、委任アイデンティティの認証と識別を実行するアイデンティティ・プロバイダは、例えば認証コンテキストに基づいて複数のアイデンティティ・プロバイダから選択することができる。

【００６６】

実施形態によると、単一のブロックチェーンが提供される。実施形態によると、複数のブロックチェーンが提供されてもよい。例えば、ブロックチェーンのそれぞれが特定の認証コンテキストのために提供されてもよい。アイデンティティ・プロバイダは、会社間ＳＳＯが確立されるように、複数のブロックチェーンを信用してもよい。例えば、ブロックチェーンは、会社固有のブロックチェーンであってもよい。

【００６７】
実施形態によると、暗号化によりセキュリティ保護されたレジスタは、不揮発性コンピュータ可読記憶媒体によって実現化され、コンピュータ可読プログラム・コードは、暗号化によりセキュリティ保護されたレジスタに含まれる。実施形態によると、コンピュータ可読プログラム・コードは、さらに、本明細書に記載の暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のための方法の実施形態のいずれかを実装するように構成される。
【００６８】
実施形態によると、コンピュータ・システムは、さらに、本明細書に記載の暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のための方法の実施形態のいずれかを実行するように構成される。
【００６９】
図１に、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のための方法を実装するのに適したコンピュータ・システム１００を示す。本明細書に記載の方法は、少なくとも部分的に非対話式であり、サーバまたは組み込みシステムなどのコンピュータ化システムによって自動化されることはわかるであろう。ただし、例示の実施形態では、本明細書に記載の方法は、（部分的に）対話式で実装可能である。これらの方法は、さらに、ソフトウェア１１２、１２２（ファームウェア１２２を含む）、ハードウェア（プロセッサ）１０５、またはこれらの組合せで実装可能である。例示の実施形態では、本明細書に記載の方法は、実行可能プログラムとしてソフトウェアで実装され、パーソナル・コンピュータ、ワークステーション、ミニコンピュータ、またはメインフレーム・コンピュータなどの特殊目的または汎用デジタル・コンピュータによって実行される。したがって、最も汎用的なシステム１００は汎用コンピュータ１０１を含む。
【００７０】
例示の実施形態では、図１に示すように、ハードウェア・アーキテクチャの観点からは、コンピュータ１０１は、プロセッサ１０５と、メモリ・コントローラ１１５に結合されたメモリ（メイン・メモリ）１１０と、ローカル入力／出力コントローラ１３５を介して通信可能に結合された１つまたは複数の入力または出力あるいはその両方の（Ｉ／Ｏ）デバイス（または周辺装置）１０、１４５とを含む。入力／出力コントローラ１３５は、当技術分野で知られているように１つまたは複数のバスまたはその他の有線または無線接続とすることができるが、これらには限定されない。図を簡単にするために省略されているが、入力／出力コントローラ１３５は、通信を可能にするために、コントローラ、バッファ（キャッシュ）、ドライバ、リピータおよび受信器など、追加の要素を含んでもよい。また、ローカル・インターフェースは、上記の構成要素間の適切な通信を可能にするために、アドレス接続、制御接続またはデータ接続あるいはこれらの組合せを含むことができる。本明細書に記載のように、Ｉ／Ｏデバイス１０、１４５は、一般に、当技術分野で知られている任意の汎用型暗号カードまたはスマート・カードを含み得る。
【００７１】
プロセッサ１０５は、ソフトウェア、具体的にはメモリ１１０に記憶されているソフトウェアを実行するためのハードウェア・デバイスである。プロセッサ１０５は、任意の特注または市販のプロセッサ、中央処理装置（ＣＰＵ）、コンピュータ１０１に付随するいくつかのプロセッサのうちの補助プロセッサ、半導体ベースの（マイクロチップまたはチップ・セットの形態の）マイクロプロセッサ、マクロプロセッサ、または一般に、ソフトウェア命令を実行するための任意のデバイスとすることができる。
【００７２】
メモリ１１０は、揮発性記憶素子（例えば、ランダム・アクセス・メモリ（ＤＲＡＭ、ＳＲＡＭ、ＳＤＲＡＭなどのＲＡＭ））、および不揮発性記憶素子（例えば、ＲＯＭ、消去可能プログラマブル読み取り専用メモリ（ＥＰＲＯＭ）、電気的消去可能プログラマブル読み取り専用メモリ（ＥＥＰＲＯＭ）、プログラマブル読み取り専用メモリ（ＰＲＯＭ））のうちのいずれか１つまたはいずれかの組合せを含み得る。なお、メモリ１１０は、

様々な構成要素が互いに遠隔に位置するがプロセッサ１０５によってアクセス可能な分散アーキテクチャを有することができる。

【００７３】

メモリ１１０内のソフトウェアは、それぞれが論理機能、特に本発明の実施形態に関わる機能を実装するための実行可能命令の順序付けられたリストを含む、１つまたは複数の別個のプログラムを含み得る。図１の例では、メモリ１１０内のソフトウェアは、例えば暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証を実装するように構成された、命令またはソフトウェア１１２を含む。

【００７４】

メモリ１１０内のソフトウェアは、典型的には適切なオペレーティング・システム（ＯＳ）１１１も含む必要がある。ＯＳ１１１は、基本的に、場合により本明細書に記載のように方法を実装するためのソフトウェア１１２などの他のコンピュータ・プログラムの実行を制御する。

【００７５】

本明細書に記載の方法は、ソース・プログラム１１２、実行可能プログラム１１２（オブジェクト・コード）、スクリプト、または、実行される１組の命令１１２を含む任意の他の実体の形態を取り得る。ソフトウェア１１２は、例えば、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証を実装することができる。ソース・プログラムの場合、プログラムはコンパイラ、アセンブラ、インタプリタなどにより変換される必要があり、これらは、ＯＳ１１１と連関して正常に動作するように、メモリ１１０内に含まれても含まれていなくてもよい。また、方法は、データおよびメソッドのクラスを有するオブジェクト指向プログラミング言語として、または、ルーチン、サブルーチンまたは関数あるいはその組合せを有する手続き型プログラミング言語として記述することも可能である。

【００７６】

例示の実施形態では、従来型キーボード１５０とマウス１５５とを入力／出力コントローラ１３５に結合することができる。Ｉ／Ｏデバイス１４５などのその他の出力デバイスは、入力デバイス、例えば、プリンタ、スキャナ、マイクロフォンなどであるがこれらには限定されない入力デバイスを含み得る。最後に、Ｉ／Ｏデバイス１０、１４５は、さらに、入力と出力の両方を伝達するデバイス、例えば、（他のファイル、デバイス、システムまたはネットワークにアクセスするための）ネットワーク・インターフェース・カード（ＮＩＣ）または変調器／復調器、無線周波数（ＲＦ）またはその他の送受信器、電話インターフェース、ブリッジ、ルータなどであるがこれらには限定されないデバイスを含み得る。Ｉ／Ｏデバイス１０、１４５は、当技術分野で知られている任意の汎用型暗号カードまたはスマート・カードであってもよい。システム１００は、ディスプレイ１３０に結合されたディスプレイ・コントローラ１２５をさらに含み得る。例示の実施形態では、システム１００は、ネットワーク１６５への結合のためのネットワーク・インターフェースをさらに含むことができる。ネットワーク１６５は、ブロードバンド接続を介したコンピュータ１０１と任意の外部サーバ、クライアントなどとの間の通信のためのＩＰベースのネットワークとすることができる。ネットワーク１６５は、コンピュータ１０１と、本明細書に記載の方法のステップの一部または全部を行うために関与し得る外部システム３０との間でデータを送受信する。例示の実施形態では、ネットワーク１６５は、サービス・プロバイダによって管理されるマネージドＩＰネットワークとすることができる。ネットワーク１６５は、例えば、ＷｉＦｉ（登録商標）、ＷｉＭａｘ（登録商標）などの無線プロトコルおよび技術を使用して無線方式で実装されてもよい。ネットワーク１６５は、ローカル・エリア・ネットワーク、ワイド・エリア・ネットワーク、メトロポリタン・エリア・ネットワーク、インターネット・ネットワーク、またはその他の類似の種類のネットワーク環境などのパケット交換網とすることもできる。ネットワーク１６５は、固定無線ネットワーク、無線ローカル・エリア・ネットワーク（ＬＡＮ）、無線ワイド・エリア・ネットワーク（ＷＡＮ）、パーソナル・エリア・ネットワーク（ＰＡＮ）、仮想プライベ

ート・ネットワーク（ＶＰＮ）、イントラネット、またはその他の適切なネットワーク・システムであってもよく、信号を受信し、送信するための装置を含む。

【００７７】

コンピュータ１０１が、ＰＣ、ワークステーション、インテリジェント・デバイスなどである場合、メモリ１１０内のソフトウェアは、ベーシック・インプット・アウトプット・システム（ＢＩＯＳ）１２２をさらに含むことができる。ＢＩＯＳは、スタートアップ時にハードウェアを初期設定し、テストし、ＯＳ１１１を始動させ、ハードウェア・デバイス間のデータの伝送をサポートする１組の基本ソフトウェア・ルーチンである。ＢＩＯＳは、コンピュータ１０１の起動時にＢＩＯＳを実行することができるようにＲＯＭに格納される。

【００７８】

コンピュータ１０１の動作時、プロセッサ１０５がメモリ１１０内に格納されているソフトウェア１１２を実行し、メモリ１１０との間でデータを伝達し、ソフトウェアに従ってコンピュータ１０１の動作を全般的に制御するように構成される。本明細書に記載の方法およびＯＳ１１１は、全体または一部、典型的には後者が、プロセッサ１０５によって読み出され、場合によってはプロセッサ１０５内でバッファリングされてから、実行される。

【００７９】

本明細書に記載のシステムおよび方法が図１に示すようにソフトウェア１１２で実装される場合、方法は、任意のコンピュータ関連システムまたは方法によって、またはそれらと連携して使用するために、ストレージ１２０などの任意のコンピュータ可読媒体に記憶することができる。ストレージ１２０は、ＨＤＤストレージなどのディスク・ストレージを含み得る。

【００８０】

暗号化によりセキュリティ保護されたレジスタは、中央データベース４５、１４５によって提供されてもよい。中央データベースは、コンピュータ１０１に通信可能に接続されたデータベース１４５であってもよい。あるいは、中央データベース４５は、例えば、ネットワーク１６５を介してアクセス可能な外部システム３０によって提供されてもよい。

【００８１】

図２に、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のための方法を実装するのに適したコンピュータ・システム１００の別の実施形態を示す。図２による実施形態では、暗号化によりセキュリティ保護されたレジスタは、ブロックチェーンを含む分散レジスタである。ブロックチェーンのコピー１２７がストレージ１２０に含まれてもよい。レジスタは、複数のコンピュータ・システム３０、１００に分散させることができる。例えば、外部システム３０もブロックチェーンのコピーを含むことができる。実施形態によると、ネットワーク１６５は、ブロックチェーンを管理するため、例えばブロックチェーンに追加のブロックを追加するために、使用することができる。実施形態によると、ネットワーク１６５は、例えば、ブロックチェーンの追加のブロックを検証するためのプロトコルに集合的に準拠する、ピア・ツー・ピア・ネットワークを含み得る。

【００８２】

図３に、実施形態によるユーザ認証のための方法の例示の参加者の概略図を示す。例示のために、以下の例を考えることができる。すなわち、ユーザ１（２０２）が第１の組織Ａ２０４のメンバーである。組織Ａ２０４は、組織Ａのメンバーを認証するためのアイデンティティ・プロバイダ２０６を含み得る。また、第２の組織Ｂ２０８と第３の組織Ｃ２１２も存在する。組織Ｂ２０８と組織Ｃ２１２の両方は、それぞれ、アイデンティティ・プロバイダ、すなわち、それぞれアイデンティティ・プロバイダＢ２１０およびアイデンティティ・プロバイダＣ２１４を含み得る。それぞれのアイデンティティ・プロバイダ２１０、２１４は、それぞれ組織Ｂ２０８、組織Ｃ２１２のメンバーを認証するように構成することができる。また、ポータル２１８を含むサービス・プロバイダＳＰ２１６があり、そのポータル２１８を介してそれぞれのサービス・プロバイダＳＰ２１６によって提供

されるサービスにアクセスすることができる。ポータル２１８は、例えば、それぞれのネットワークを介してサービス・プロバイダ２１６と通信するためのネットワーク・インターフェースとすることができる。

【００８３】

例示のために、組織Ａが例えば外部サプライヤであるものとする。組織Ａは、ユーザ１がメンバーである第１のプロジェクトＰＡＢの一員としての組織Ｂの請負業者であってもよい。組織Ａは、さらに、やはりユーザ１がメンバーである第２のプロジェクトＰＡＣの一員としての組織Ｃの請負業者であってもよい。両方の組織ＢおよびＣは、それぞれのプロジェクトを管理するために、サービス・プロバイダＳＰによって提供されるサービス・ポータル２１８を使用することができる。

【００８４】

実施形態は、ユーザ１が自分の組織Ａのクレデンシャルを使用して、組織ＢのプロジェクトＰＡＢの一員として、および、組織ＣのプロジェクトＰＡＣの一員として、サービス・プロバイダＳＰによって提供されるサービスにＳＳＯすることを可能にすることができる。したがって、異なるアイデンティティ間、すなわちサービス・プロバイダＳＰと組織Ｂまたは組織Ｃとの間に、相互の信用の輪を構築する必要がない。相互の信用の輪の場合、組織Ｂのすべての従業員が組織Ｂとサービス・プロバイダＳＰとの間でのＳＳＯを行うことができるようにするために、サービス・プロバイダＳＰと組織Ｂとは、組織Ｂのアイデンティティ・プロバイダＢとサービス・プロバイダＳＰとの間で信用関係を形成することになる。また、サービス・プロバイダＳＰと組織Ｃとは、組織Ｃとサービス・プロバイダＳＰとの間でのＳＳＯを行うための要件を実現するために、組織Ｃのアイデンティティ・プロバイダＣとサービス・プロバイダＳＰとの間で信用関係を形成する必要が生じることになる。

【００８５】

本発明の方法を使用して組織Ａの従業員、例えばユーザ１などが、サービス・プロバイダＳＰによって提供されるサービスにアクセスすることができるようにすることで、サービス・プロバイダＳＰと組織Ｂとの間、および、サービス・プロバイダＳＰと組織Ｃとの間の信用関係による相互の信用の輪と比較して、いくつかの難点を回避することができる。

【００８６】

組織Ａの従業員が、組織Ａとプロバイダ ＳＰによって提供されるサービスとの間でＳＳＯを行うことができるようにするために、サービス・プロバイダＳＰと組織Ａとが組織Ａのアイデンティティ・プロバイダＡとサービス・プロバイダＳＰとの間に信用関係を形成することを考えてみる。しかし、サービス・プロバイダＳＰは、一方で組織Ｂとともにプロジェクト ＰＡＢの一員として仕事をするユーザ１と、他方で組織ＣとともにプロジェクトＰＡＣの一員として仕事をするユーザ１とを区別することができるようにはなされない。ユーザ１が組織ＢとのプロジェクトＰＡＢに関連するデータにアクセスする許可と、ユーザ１が組織ＣとのプロジェクトＰＡＣに関連するデータにアクする許可とは、プロジェクトＰＡＢとプロジェクトＰＡＣのそれぞれのデータを扱うサービス・プロバイダＳＰのサービスに格納される必要があることになる。したがって、サービス・プロバイダＳＰはそれぞれの許可を扱うことができる必要がある。

【００８７】

ユーザ１は、組織ＢとのプロジェクトＰＡＢのためのサービス・プロバイダＳＰとの第１の追加のローカル・アイデンティティと、第１の追加のローカル・アイデンティティとは異なる、組織ＣとのプロジェクトＰＡＣのための第２の追加のローカル・アイデンティティとを作成することができる。ローカル・アイデンティティとは、それぞれのプロジェクトに限定されたプロジェクト固有のアイデンティティを指す。それぞれのローカル・アイデンティティは、ユーザ１が組織Ａに関連するデータにアクセスすることができるようにする組織Ａの従業員としてのユーザ１のアイデンティティに加えて作成される。

【００８８】

しかし、ユーザ１の３つのアイデンティティは切り離されることになる。したがって、

ユーザ１は、ＳＳＯを行うことができないことになる。また、セキュリティ・ポリシーが確実に一貫して適用され、監査が統一性のある方法で行われ、適切なときにアクセス権が失効させられるようにすることが困難になる可能性がある。

【００８９】

なお、一般に、組織Ｂまたは組織Ｃに、ユーザ１をその組織に連合させる組織Ａに対する信用関係を形成させることは不可能であることに留意されたい。ユーザ１のみ、すなわち、ユーザ１の１つの識別子を有する１つのアイデンティティのみがそれぞれ残ることになるため、サービス・プロバイダＳＰは、どのアイデンティティ・プロバイダ、すなわち、組織Ｂのアイデンティティ・プロバイダＢか組織Ｃのアイデンティティ・プロバイダＣのどちらがこのユーザを認証する責任を担うことができるかを区別することができないことになる。したがって、どちらの識別子に認証要求を送信すべきかを決定することができないことになる。

【００９０】

それに対して、本開示による実施形態は、知られているＳＳＯ解決策で必要とされている信用の輪を異なる機構に置き換えるための有効な手法を提供することができる。ユーザ１は、組織Ａのコンピュータ・システムを介して、または組織Ａに関連するポータル２１８にアクセスするためのＵＲＬを介して、サービス・プロバイダ・ポータル２１８にアクセスすることができる。いずれの場合も、ユーザ１は、認証のためにルート・アイデンティティを使用することができる。認証は、アイデンティティ・プロバイダＡが暗号化によりセキュリティ保護されたレジスタにアクセスすることによって実行することができる。暗号化によりセキュリティ保護されたレジスタは、例えば、ブロックチェーンとして実装することができ、ブロックチェーンの第１のコピーがアイデンティティ・プロバイダＡに含まれてもよい。例えば、認証に成功した場合、ユーザ１を組織Ａのメンバーであると識別する委任アイデンティティＡの委任識別子を含む認証トークンが提供される。したがって、ユーザ１は組織Ａのために発行された認証トークンを使用して認証を行うことが可能となる。

【００９１】

あるいは、ユーザ１は、組織Ｂのコンピュータ・システムを介して、または組織Ｂに関連するポータル２１８にアクセスするためのＵＲＬを介して、サービス・プロバイダ・ポータル２１８にアクセスすることができる。これは、プロジェクトＰＡＢのメンバーとしての作業を行うために行うことができる。この場合も、ユーザ１は、認証のためにルート・アイデンティティを使用することができる。この場合は、認証は、アイデンティティ・プロバイダＢがアイデンティティ・プロバイダＢに含まれるブロックチェーンの第２のコピーにアクセスすることによって行うことができる。例えば、認証が成功した場合、ユーザ１を組織Ｂのメンバーとして識別する委任アイデンティティＢの委任識別子を含む認証トークンが提供される。したがって、ユーザ１は組織Ｂのために発行された認証トークンを使用して認証を行うことが可能になる。

【００９２】

また、ユーザ１は、組織Ｃのコンピュータ・システムを介して、または組織Ｃに関連するポータル２１８にアクセスするためのＵＲＬを介して、サービス・プロバイダ・ポータル２１８にアクセスすることができる。これは、プロジェクトＰＡＣのメンバーとしての作業を行うために行うことができる。この場合も、ユーザ１は、認証のためにルート・アイデンティティを使用することができる。この場合は、認証はアイデンティティ・プロバイダＣがアイデンティティ・プロバイダＣに含まれるブロックチェーンの第３のコピーにアクセスすることによって行うことができる。暗号化によりセキュリティ保護されたレジスタは、例えばブロックチェーンとして実装することができ、ブロックチェーンのコピーがアイデンティティ・プロバイダＣに含まれてもよい。例えば、認証が成功した場合、ユーザ１を組織Ｃのメンバーとして識別する委任アイデンティティＣの委任識別子を含む認証トークンが提供される。したがって、ユーザ１は組織Ｃのために発行された認証トークンを使用して認証を行うことが可能になる。

【００９３】
ユーザ１がポータル２１８にアクセスを試みるために用いるホームページに応じて、またはユーザ１がどのサービス・アカウントにアクセスしようとしているかに応じて、アイデンティティ・プロバイダＢまたはアイデンティティ・プロバイダＣにユーザ１を認証するように要求することができる。
【００９４】
図４に、図３の例による、ルート・アイデンティティ２０２に割り当てられた委任アイデンティティ２２０、２２２、２２４の木状構造の概略図を示す。ルート・アイデンティティ２０２は、ルート識別子「ｕｓｅｒ１＠ｏｒｇ＿ａ．ｃｏｍ」とパスワード「ｓｅｃｒｅｔ１２３」とを含む。委任アイデンティティ２２０は、認証コンテキストとしての組織Ａに割り当てられた委任識別子「５７２ｆ７ｂｆ８ｄ８９３５０」を含む。委任アイデンティティ２２２および２２４は、委任アイデンティティ２２０を介してルート・アイデンティティ２０２に割り当てられる。委任アイデンティティ２２２は、認証コンテキストとしての組織Ｂに割り当てられた委任識別子「６ｂｅｂｆｂｅ９７４８８０１」を含む。委任アイデンティティ２２４は、認証コンテキストとしての組織Ｃに割り当てられた識別子「９ｆｅｅ６７ｅ２ａ２ｃａ７９」を含む。
【００９５】
図３の例を考えると、プライバシーおよびコンテキスト依存性によってさらなる問題が生じる可能性がある。職務と許可と管理範囲の分離を確実にするために、組織Ｂのコンテキスト、すなわちプロジェクトＰＡＢでプロバイダＳＰによって提供されるサービスにアクセスするユーザ１は、組織Ｃのコンテキスト、すなわちプロジェクトＰＡＣでプロバイダＳＰのサービスにアクセスするユーザ１とは異なる識別子を使用する必要がある。したがって、図４に示すように、認証のためにルート・アイデンティティ２０２が使用される異なるコンテキストのために、それぞれがそれらのコンテキストのうちの１つのコンテキストに固有である、異なる委任アイデンティティ２２０～２２４が使用される。したがって、ルート・アイデンティティは、ＳＳＯのために委任アイデンティティ２２０ないし２２４の委任識別子を利用するすべてのシステムに知られないままである。
【００９６】
ルート・アイデンティティ２０２は、ユーザ１がいずれかのＳＳＯログインで使用するログインのための識別子とパスワードとを含む。ＳＳＯログインはアクセスを要求するアプリケーションの領域のコンテキストで実行されるため、ＳＳＯログインは、ユーザ１が組織Ｂのコンテキスト、すなわちプロジェクトＰＡＢでログインしようとしているのか、または組織Ｃのコンテキスト、すなわちプロジェクトＰＡＣでログインしようとしているのかを判断することができる。ルート・アイデンティティ２０２を使用してユーザ１を成功裏に認証し、ユーザ１の組織Ｂアイデンティティ２２２「ユーザ１［組織Ｂ］」またはユーザ１の組織Ｃアイデンティティ２２４「ユーザ１［組織Ｃ］」の委任識別子を見つけるかまたは作成した後、組織Ｂアイデンティティ２２２または組織Ｃアイデンティティ２２４のそれぞれの識別子がサービス・プロバイダＳＰに返される。
【００９７】
サービス・プロバイダＳＰにとって、組織Ｂアイデンティティ２２２の識別子と組織Ｃアイデンティティ２２４の識別子との間には何の関係もない。両方の識別子は、それぞれがそれぞれの領域、組織Ｂまたは組織Ｃの一員である、２人の異なるユーザの異なる識別子を指しているように見える。
【００９８】
図５に、ルート・アイデンティティまたはルート・アイデンティティに割り当てられた委任アイデンティティとすることができる、組織Ｂのアイデンティティ２０８を示す。アイデンティティ２０８は、識別子「ｃｂ１０２１２９９６ｅ７」と属性「種類：組織」とを含む。属性は、アイデンティティ２０８が何らかの組織に属することを示す。複数の委任アイデンティティ２２２、２３０、２４０が組織Ｂのルート・アイデンティティ２０８に依存し得る。委任アイデンティティ２２２、２３０および２４０の依存関係は、組織Ｂ

によって例えば識別子の形態で与えられるそれぞれの委任アイデンティティ２２２、２３０、２４０の認証コンテキストによって実装することができる。委任アイデンティティ２２２、２３０、２４０の認証コンテキストは、例えば「ｃｂ１０２１２９９６ｅ７」である。委任アイデンティティ２２２、２３０、２４０のそれぞれが委任識別子を含むことができる。

【００９９】

組織Ｂのために提供されるサービス・プロバイダＳＰのサービスへのユーザ１のログイン時、ＳＳＯサービスは、ユーザ１がアクセスしようとしている領域、すなわち組織Ｂのメンバーとして認証されているか否かを判断する必要がある。ユーザ２（２３０）とユーザ３（２４０）が組織Ｂに直接勤務し、組織Ａには関係がない、すなわち組織Ａのアイデンティティがないものと考えてみる。ユーザ１は、組織Ｂのための委任識別子「６ｂｅｂｆｂｅ９７４８８０１」を使用して委任アイデンティティ２２２を作成する。組織Ｂの識別子「ｃｂ１０２１２９９６ｅ７」によって提供するかまたはこの識別子にリンクさせる認証コンテキストを選択することによって、委任アイデンティティ２２２と組織Ｂのアイデンティティ２０８との間の依存関係を（提供することができる）。サービス・プロバイダＳＰは、組織のアイデンティティ、すなわち識別子をそれぞれのプロジェクトＰＡＢに結合することによって、組織Ｂの領域に割り当てられたすべてのユーザがログオンをすることを許可する。

【０１００】

したがって、ユーザ１は、常に自分の組織Ａ識別子とパスワードとを使用して、サービス・プロバイダＳＰによって提供されるサービスにログインすることができる一方、ユーザのアイデンティティは、ユーザ１がログインしようとしているコンテキストに応じて、正しくサービス・プロバイダＳＰのサービスに対して明らかにされることになる。サービス・プロバイダＳＰの観点からは２つの異なるユーザ１アイデンティティが存在するため、プロバイダＳＰのサービスにおける無用な複雑さが回避される。組織Ｂと組織Ｃはそれぞれ独立して、それぞれのディレクトリ内でユーザ１がサービス・プロバイダＳＰのサービスの部分にログインすることができるか否かを制御し、ユーザ１がそれぞれ組織Ｂと組織Ｃの実際の従業員であるかのように同じ原則を適用する。

【０１０１】

図６に、クライアント、例えばユーザ・コンピュータ・システムによって実行されるウェブ・ブラウザと、資源サーバ、例えばサービス・プロバイダ・コンピュータ・システムと、許可サーバ、例えばアイデンティティ・プロバイダ・コンピュータ・システムとの間の例示の通信プロセスの概略図を示す。ステップＡで、クライアントがクライアント上で稼働しているアプリケーションにおいてＵＲＬにアクセスする。ＵＲＬは、組織Ｂのためにサービス・プロバイダによって提供されるサービスを参照することができる。それぞれのＵＲＬにアクセスするとき、アプリケーションは認証要求を生成する。クライアントのユーザを認証することを求める認証要求は、例えばＨＴＴＰポストを使用して許可サーバに送信される。認証要求は、許可サーバに渡され、検証される。ステップＣで、許可サーバがクライアントを認証サーバのログイン・ページにリダイレクトする。ユーザは、自分のルート・アイデンティティを使用してログインを行う。認証サーバは、ユーザを認証し、暗号化によりセキュリティ保護されたレジスタを使用して、認証コンテキスト、すなわち組織Ｂに割り当てられた委任アイデンティティを識別する。例えば、認証コンテキストは、ユーザがアプリケーションにおいてアクセスするＵＲＬに依存する。ステップＤで、ユーザの委任アイデンティティのために、認証トークンが例えばＳＡＭＬトークンの形態で生成される。ステップＤで、認証トークンとともにアプリケーションが資源サーバにリダイレクトされる。ステップＥで、認証トークンがその認証トークンによって識別された委任アイデンティティの有効な認証を確認することにより、ユーザが資源サーバにログインされる。したがって、ユーザは組織Ｂの資源サーバによって提供されるサービスにアクセスすることができる。

【０１０２】

暗号化によりセキュリティ保護されたレジスタは、ブロックチェーンのブロックに格納された、例えばユーザのルート・アイデンティティ、委任アイデンティティ、および組織のアイデンティティなどすべてのアイデンティティを含む、ブロックチェーンの形態で実装することができる。アイデンティティ・プロバイダは、やはりブロックチェーンに格納されたコンピュータ可読プログラム・コードを実行することができる。それぞれのコンピュータ可読プログラム・コードの実行により、パスワードが正しく、アイデンティティがアクセスを許可される場合は、対象認証コンテキストの委任アイデンティティを返すことができる。例えば、コンピュータ可読プログラム・コードは、delegatedIdentity=getIdentity（authentication context, rootID, root password）を定義することができる。

【０１０３】

別の実施形態によると、サービス・プロバイダＳＰは、ブロックチェーンに接続され、例えば組織Ｃおよび組織Ｂのような、サービス・プロバイダＳＰによって提供される資源を有するすべての領域のためにユーザ・ログインを認可する役割を担う、単一のアイデンティティ・プロバイダを稼働させることができる。別の実施形態によると、ブロックチェーンに接続され、例えば組織Ｃおよび組織Ｂのような、サービス・プロバイダＳＰによって提供される資源を有するすべての領域のためのユーザ・ログインを認可する役割を担う、単一の独立したアイデンティティ・プロバイダを提供することができる。

【０１０４】

図７に、アイデンティティを格納するために使用される例示のブロックチェーン４００の概略図を示す。格納されるアイデンティティには、ルート・アイデンティティと委任アイデンティティとが含まれ得る。実施形態によると、例えば人物と団体のアイデンティティなどの、アイデンティティのカテゴリがあってもよい。ブロックチェーン４００は、複数のブロックＢ１～ＢＮ（４０２～４１０）を含む。各ブロックＢ２～ＢＮ（４０４～４１０）は、ブロックチェーン４００内の直前のブロックＢ１～ＢＮ－１（４０２～４０８）のハッシュを含み、それによってそれら２つのブロックを連結する。ブロックＢ１～ＢＮ（４０２～４１０）のうちの１つのブロックを修正するには、それ以降のすべてのブロックのハッシュも修正する必要がある。ブロックチェーン４００に追加のデータが格納される場合は、その追加のデータを含む追加のブロックＢＮ＋１（４１２）が生成され、そのブロックを最後のブロックＢＮ４１０に連結することによってブロックチェーン４００に追加される。ブロックＢＮ＋１（４１２）をブロックＢＮ４１０に連結することは、ブロックＢＮ４１０のハッシュをブロックＢＮ＋１（４１２）に追加することを含む。ブロックＢ１～ＢＮ（４０２～４１０）、具体的にはブロックチェーン４００の最初の数ブロックは、コンピュータ可読プログラム・コードを含み得る。電子データ処理手段の１つによるコンピュータ可読プログラム・コードの実行によって、ブロックチェーンに格納されたアイデンティティを使用するユーザ認証の実行と、認証トークンの発行が行われる。コンピュータ可読プログラム・コードは、具体的には、ユーザのルート・アイデンティティと認証要求のために識別された認証コンテキストとに割り当てられた委任アイデンティティを識別するように構成することができる。

【０１０５】

同じブロックチェーン４００に含まれる異なるアイデンティティの機密性は、ブロックチェーン４００のブロックＢ１～ＢＮ（４０２～４１０）に格納されたデータへの読み取りアクセスを制限することによって実装することができる。このような読み取りアクセスの制限は、例えば、異なる暗号鍵を使用してブロックチェーン４００に格納されたデータを暗号化することによって実装することができる。

【０１０６】

本明細書では、本発明の態様について、本発明の実施形態による方法、装置（システム）、およびコンピュータ・プログラム製品を示すフローチャート図またはブロック図あるいはその両方を参照しながら説明している。フローチャート図またはブロック図あるいはその両方の図の各ブロックおよび、フローチャート図またはブロック図あるいはその両方の図のブロックの組合せは、コンピュータ可読プログラム命令によって実装可能であるこ

とはわかるであろう。

【０１０７】

本発明は、システム、方法またはコンピュータ・プログラム製品あるいはその組合せとすることができる。コンピュータ・プログラム製品は、プロセッサに本発明の態様を実施させるためのコンピュータ可読プログラム命令を有するコンピュータ可読記憶媒体（または複数の媒体）を含み得る。

【０１０８】

コンピュータ可読記憶媒体は、命令実行デバイスによって使用されるための命令を保持し、記憶することができる有形のデバイスとすることができる。コンピュータ可読記憶媒体は、例えば、電子ストレージ・デバイス、磁気ストレージ・デバイス、光学式ストレージ・デバイス、電磁気ストレージ・デバイス、半導体ストレージ・デバイス、またはこれらの任意の適合する組合せであってよいが、これらには限定されない。コンピュータ可読記憶媒体のより具体的な例の非網羅的なリストには以下のものが含まれる。すなわち、可搬コンピュータ・ディスケット、ハードディスク、ランダム・アクセス・メモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、消去可能プログラマブル読み取り専用メモリ（ＥＰＲＯＭまたはフラッシュ・メモリ）、スタティック・ランダム・アクセス・メモリ（ＳＲＡＭ）、可搬コンパクト・ディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、デジタル・バーサタイル・ディスク（ＤＶＤ）、メモリ・スティック、フロッピィ・ディスク、パンチカードまたは命令が記録された溝内の隆起構造などの機械的に符号化されたデバイス、およびこれらの任意の適合する組合せが含まれる。本明細書で使用されるコンピュータ可読記憶媒体とは、電波またはその他の自由に伝播する電磁波、導波路またはその他の伝送媒体を伝播する電磁波（例えば光ファイバ・ケーブルを通る光パルス）、または電線を介して伝送される電気信号などの、一過性の信号自体であると解釈すべきではない。

【０１０９】

本明細書に記載のコンピュータ可読プログラム命令は、コンピュータ可読記憶媒体からそれぞれのコンピューティング／処理デバイスに、または、ネットワーク、例えばインターネット、ローカル・エリア・ネットワーク、ワイド・エリア・ネットワーク、または無線ネットワークあるいはこれらの組合せを介して外部コンピュータまたは外部記憶デバイスにダウンロードすることができる。ネットワークは、銅伝送ケーブル、光伝送ファイバ、無線伝送、ルータ、ファイアウォール、交換機、ゲートウェイ・コンピュータ、またはエッジ・サーバあるいはこれらの組合せを含み得る。各コンピューティング／処理デバイスにおけるネットワーク・アダプタ・カードまたはネットワーク・インターフェースが、ネットワークからコンピュータ可読プログラム命令を受信し、それらのコンピュータ可読プログラム命令を、それぞれのコンピューティング／処理デバイス内のコンピュータ可読記憶媒体への記憶のために転送する。

【０１１０】

本発明の動作を実行するためのコンピュータ可読プログラム命令は、アセンブラ命令、インストラクション・セット・アーキテクチャ（ＩＳＡ）命令、マシン命令、マシン依存命令、マイクロコード、ファームウェア命令、状態設定データ、または、Ｓｍａｌｌｔａｌｋ、Ｃ＋＋などのオブジェクト指向プログラミング言語、および「Ｃ」プログラミング言語、または同様のプログラム言語などの従来型の手続き型プログラミング言語を含む、１つまたは複数のプログラミング言語の任意の組合せで書かれたソース・コードまたはオブジェクト・コードとすることができる。コンピュータ可読プログラム命令は、スタンドアロン・ソフトウェア・パッケージとして全体がユーザ・コンピュータ・システムのコンピュータ上でまたは一部がユーザ・コンピュータ・システムのコンピュータ上で、または一部がユーザ・コンピュータ・システムのコンピュータ上で一部がリモート・コンピュータ上で、または全体がリモート・コンピュータまたはサーバ上で実行されてもよい。後者の場合、リモート・コンピュータは、ローカル・エリア・ネットワーク（ＬＡＮ）またはワイド・エリア・ネットワーク（ＷＡＮ）を含む、任意の種類のネットワークを介してユーザ・コンピュータ・システムのコンピュータに接続することができ、または接続は（例

えば、インターネット・サービス・プロバイダを使用してインターネットを介して）外部コンピュータに対して行ってもよい。実施形態によっては、本発明の態様を実行するために、例えばプログラマブル・ロジック回路、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、またはプログラマブル・ロジック・アレイ（ＰＬＡ）を含む電子回路が、コンピュータ可読プログラム命令の状態情報を使用して電子回路をパーソナライズすることにより、コンピュータ可読プログラム命令を実行することができる。

【０１１１】

本明細書では、本発明の態様について、本発明の実施形態による方法、装置（システム）、およびコンピュータ・プログラム製品を示すフローチャート図またはブロック図あるいはその両方を参照しながら説明している。フローチャート図またはブロック図あるいはその両方の図の各ブロックおよび、フローチャート図またはブロック図あるいはその両方の図のブロックの組合せは、コンピュータ可読プログラム命令によって実装可能であることはわかるであろう。

【０１１２】

これらのコンピュータ可読プログラム命令は、コンピュータまたはその他のプログラマブル・データ処理装置のプロセッサにより実行される命令が、フローチャートまたはブロック図あるいはその両方のブロックで規定されている機能／動作を実装する手段を形成するようなマシンを実現するように、汎用コンピュータ、特殊目的コンピュータ、またはその他のプログラマブル・データ処理装置のプロセッサに供給することができる。これらのコンピュータ可読プログラム命令は、命令が記憶されたコンピュータ可読記憶媒体が、フローチャートまたはブロック図あるいはその両方のブロックで規定されている機能／動作の態様を実装する命令を含む製造品を含むように、コンピュータ、プログラマブル・データ処理装置、またはその他のデバイスあるいはこれらの組合せに対して特定の方式で機能するように指示することができるコンピュータ可読記憶媒体に記憶することもできる。

【０１１３】

コンピュータ可読プログラム命令は、コンピュータ、その他のプログラマブル装置またはその他のデバイス上で実行される命令がフローチャートまたはブロック図あるいはその両方のブロックで規定されている機能／動作を実装するように、コンピュータ実装プロセスを生成するために、コンピュータ、その他のプログラマブル装置、またはその他のデバイス上で一連の動作ステップが実行されるようにするために、コンピュータ、その他のプログラマブル・データ処理装置、またはその他のデバイスにロードされてもよい。

【０１１４】

図面中のフローチャートおよびブロック図は、本発明の様々な実施形態によるシステム、方法およびコンピュータ・プログラム製品の可能な実装形態のアーキテクチャ、機能および動作を示す。なお、フローチャートまたはブロック図の各ブロックは、規定されている論理機能を実装するための１つまたは複数の実行可能命令を含む、命令のモジュール、セグメント、または部分を表すことがある。別の実装形態によっては、ブロックに記載されている機能は、図に記載されている順序とは異なる順序で行われてもよい。例えば、連続して示されている２つのブロックは、関与する機能に応じて、実際には実質的に並行して実行されてよく、またはそれらのブロックは場合によっては逆の順序で実行されてもよい。また、ブロック図またはフローチャート図あるいはその両方の図の各ブロック、およびブロック図またはフローチャート図あるいはその両方の図のブロックの組合せは、規定されている機能または動作を実行する特殊目的ハードウェア・ベースのシステムによって実装可能であるか、または特殊目的ハードウェアとコンピュータ命令との組合せを実施することができることも留意されたい。

【０１１５】

上記の特徴の可能な組合せは以下の通りとすることができる。

１．暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のためのコンピュータ実装方法であって、暗号化によりセキュリティ保護された上記レジスタは、ユーザのルート・アイデンティティを含み、上記ルート・アイデンティティは、ルート識別子と

上記ユーザを認証するために上記ルート識別子に割り当てられたクレデンシャルとを含み、暗号化によりセキュリティ保護された上記レジスタは、上記ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含み、上記委任アイデンティティのそれぞれが、委任識別子を含み、認証コンテキストに割り当てられ、上記方法は、

・上記ユーザを認証することを求める認証要求を受け取ることと、

・上記ユーザの上記ルート・アイデンティティを使用して上記ユーザを認証することであって、成功裏の認証が上記ユーザの上記ルート・アイデンティティの上記ルート識別子に割り当てられた上記クレデンシャルを受け取ることを求める、上記認証することと、

・要求された上記認証の認証コンテキストを識別することと、

・上記ユーザの上記ルート・アイデンティティに割り当てられ、識別された上記認証コンテキストに割り当てられた、上記１つまたは複数の委任アイデンティティのうちの１つを、暗号化によりセキュリティ保護された上記レジスタを使用して識別することと、

・上記ルート・アイデンティティを使用した上記ユーザの成功裏の認証に応答して、上記成功裏のユーザ認証を確認するとともに識別された上記委任アイデンティティの上記委任識別子によって上記成功裏に認証されたユーザを識別する、認証トークンを発行することとを含む、コンピュータ実装方法。

２．上記方法は、上記ユーザの上記ルート・アイデンティティを使用して、各自の上記ルート・アイデンティティに割り当てられたすべての委任アイデンティティについてシングル・サイン・オンを行う、項目１に記載の方法。

３．上記ルート・アイデンティティは上記ルート・アイデンティティに割り当てられた複数の委任アイデンティティを含み、上記複数の委任アイデンティティは、上記複数の委任アイデンティティのうちの少なくとも第１の１つの委任アイデンティティが上記複数の委任アイデンティティのうちの少なくとも第２の１つの委任アイデンティティを介して上記ルート・アイデンティティに割り当てられた、木構造の形態で、て上記ルート・アイデンティティに割り当てられる、上記項目のいずれかに記載の方法。

４．暗号化によりセキュリティ保護された上記レジスタは、コンピュータ可読プログラム・コードを含み、認証側コンピュータ・システムのプロセッサによる上記コンピュータ可読プログラム・コードの実行が、上記ユーザ認証の実行と上記認証トークンの発行とを行うように上記プロセッサに上記認証側コンピュータ・システムを制御させる、上記項目のいずれかに記載の方法。

５．上記レジスタの暗号化によるセキュリティは、格納された上記ルート・アイデンティティおよび格納された上記１つまたは複数の委任アイデンティティの少なくとも一部のハッシュ化と、署名と、暗号化とのうちの１つまたは複数を含む、上記項目のいずれかに記載の方法。

６．暗号化によりセキュリティ保護された上記レジスタは分散レジスタであり、上記分散レジスタのコピーが複数のコンピュータ・システムに分散される、上記項目のいずれかに記載の方法。

７．上記分散レジスタの暗号化による上記セキュリティは、上記ルート・アイデンティティと上記１つまたは複数の委任アイデンティティとを、上記分散レジスタの各コピーに含まれる、ブロックチェーンの複数のブロックに格納することを含む、項目６に記載の方法。

８．暗号化によりセキュリティ保護された上記レジスタが中央データベースによって提供される、項目１ないし５のいずれかに記載の方法。

９．上記認証に使用された上記ルート・アイデンティティまたは識別された上記委任アイデンティティが無効な場合、上記認証トークンの上記発行が拒否される、上記項目のいずれかに記載の方法。

１０．上記要求は認証に使用される上記ルート・アイデンティティの上記ルート識別子を含む、上記項目のいずれかに記載の方法。

１１．上記要求は、上記ユーザの認証に使用される上記ルート・アイデンティティに割り当てられ、識別された上記認証コンテキストに割り当てられた上記委任識別子を含む、項

目１ないし９のいずれかに記載の方法。
１２．上記認証要求は、暗号化によりセキュリティ保護された上記レジスタにアクセスすることができるアイデンティティ・プロバイダ・コンピュータ・システムによって受け取られ、上記アイデンティティ・プロバイダ・コンピュータ・システムは、上記ユーザの上記認証と、識別された上記委任アイデンティティの上記委任識別子によって成功裏に認証された上記ユーザを識別する上記認証トークンの発行とを行う、上記項目のいずれかに記載の方法。
１３．上記認証要求は、サービス・プロバイダ・コンピュータ・システムから受け取られ、上記ユーザを認証するために使用される上記クレデンシャルはユーザ・コンピュータ・システムから受け取られる、項目１２に記載の方法。
１４．上記１つまたは複数の委任アイデンティティは、それぞれ、上記それぞれの委任アイデンティティの有効性が満了する有効期限日を示す標識を含む、上記項目のいずれかに記載の方法。
１５．上記それぞれの委任アイデンティティが上記認証のために使用される上記ルート・アイデンティティに割り当てられており、識別された上記認証コンテキストに割り当てられていると識別された上記委任アイデンティティである場合、上記１つまたは複数の委任アイデンティティのうちの少なくとも１つが、成功裏の認証のための追加の認証要件を含む、上記項目のいずれかに記載の方法。
１６．・第１のアイデンティティ要求者から、上記ルート・アイデンティティに割り当てられたすべての委任アイデンティティを提供することを求める要求を受け取ることと、
・上記第１のアイデンティティ要求者が各自の上記ルート・アイデンティティを使用して成功裏に認証された場合、上記ルート・アイデンティティに割り当てられた上記１つまたは複数の委任アイデンティティをすべて提供することとをさらに含む、上記項目のいずれかに記載の方法。
１７．上記ルート・アイデンティティに追加の委任アイデンティティを割り当てることをさらに含み、上記追加の委任アイデンティティは、追加の委任識別子を含み、追加の認証コンテキストに割り当てられ、上記追加の認証コンテキストは、さらなるルート・アイデンティティに依存し、上記割り当てることは、
・上記追加の委任アイデンティティを割り当てることを求める要求を受け取ることと、
・上記追加の委任アイデンティティの上記追加の認証コンテキストを調べることと、
・上記追加の認証コンテキストが上記さらなるルート・アイデンティティに依存する場合、上記追加の認証コンテキストが依存する上記さらなるルート・アイデンティティを使用して成功裏に認証されたさらなるユーザから上記追加の委任アイデンティティの承認を受け取ることに応答して、上記ルート・アイデンティティに割り当てられた上記追加の委任アイデンティティを、暗号化によりセキュリティ保護された上記レジスタに格納することとを含む、上記項目のいずれかに記載の方法。
１８．上記追加の認証コンテキストは、さらなるルート・アイデンティティに割り当てられた１つまたは複数のさらなる委任アイデンティティを介して上記さらなるルート・アイデンティティに依存する、項目１７に記載の方法。
１９．上記追加の委任アイデンティティの依存関係は、上記さらなるルート・アイデンティティの上記さらなるルート識別子または上記さらなるルート・アイデンティティに割り当てられたさらなる委任アイデンティティのさらなる委任識別子を含む上記追加の委任アイデンティティの上記認証コンテキストによって実装される、項目１７および１８のいずれかに記載の方法。
２０．・上記さらなるルート・アイデンティティに依存するすべての委任アイデンティティの提供を求める要求を第２のアイデンティティ要求者から受け取ることと、
・上記第２のアイデンティティ要求者が上記さらなるルート・アイデンティティを使用して成功裏に認証された場合、上記さらなるルート・アイデンティティに依存するすべての委任アイデンティティを提供することと、
をさらに含む、項目１７ないし１９のいずれかに記載の方法。

２１．暗号化によりセキュリティ保護された上記レジスタが、さらなるコンピュータ可読プログラム・コードを含み、割り当て側コンピュータ・システムのプロセッサによる上記さらなるコンピュータ可読プログラム・コードの実行によって、上記ルート・アイデンティティへの上記追加の委任アイデンティティの割り当てを実行するように上記プロセッサに上記割り当て側コンピュータ・システムを制御させる、項目１７ないし２０のいずれかに記載の方法。
２２．失効により、割り当てられた上記追加の委任アイデンティティを無効にすることをさらに含み、上記失効は、
・失効要求者から上記追加の委任アイデンティティの失効を求める要求を受け取ることと、
・上記失効要求者を認証することと、
・上記失効要求者が、上記追加の認証コンテキストが依存する上記さらなるルート・アイデンティティを使用して成功裏に認証された上記さらなるユーザである場合、暗号化によりセキュリティ保護された上記レジスタに、上記追加の委任アイデンティティの上記失効を示す失効標識を追加することとを含む、項目１７ないし２１のいずれかに記載の方法。
２３．コンピュータ可読プログラム・コードが実現された不揮発性コンピュータ可読記憶媒体を含むコンピュータ・プログラム製品であって、上記コンピュータ可読プログラム・コードは、暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のための方法を実装するように構成され、暗号化によりセキュリティ保護された上記レジスタは、ユーザのルート・アイデンティティを含み、上記ルート・アイデンティティは、ルート識別子と上記ユーザを認証するために上記ルート識別子に割り当てられたクレデンシャルとを含み、暗号化によりセキュリティ保護された上記レジスタは、上記ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含み、上記委任アイデンティティのそれぞれが、委任識別子を含み、認証コンテキストに割り当てられ、上記方法は、
・上記ユーザを認証することを求める認証要求を受け取ることと、
・上記ユーザの上記ルート・アイデンティティを使用して上記ユーザを認証することであって、成功裏の認証が上記ユーザの上記ルート・アイデンティティの上記ルート識別子に割り当てられた上記クレデンシャルを受け取ることを求める、上記認証することと、
・要求された上記認証の認証コンテキストを識別することと、
・上記ユーザの上記ルート・アイデンティティに割り当てられ、識別された上記認証コンテキストに割り当てられた、上記１つまたは複数の委任アイデンティティのうちの１つを、暗号化によりセキュリティ保護された上記レジスタを使用して識別することと、
・上記ルート・アイデンティティを使用した上記ユーザの成功裏の認証に応答して、上記成功裏のユーザ認証を確認するとともに識別された上記委任アイデンティティの上記委任識別子によって上記成功裏に認証されたユーザを識別する、認証トークンを発行することとを含む、コンピュータ・プログラム製品。
２４．暗号化によりセキュリティ保護された上記レジスタは、不揮発性コンピュータ可読記憶媒体を使用して実現され、上記コンピュータ可読プログラム・コードは、暗号化によりセキュリティ保護された上記レジスタに含まれる、項目２３に記載のコンピュータ・プログラム製品。
２５．暗号化によりセキュリティ保護されたレジスタを使用するユーザ認証のためのコンピュータ・システムであって、暗号化によりセキュリティ保護された上記レジスタは、ユーザのルート・アイデンティティを含み、上記ルート・アイデンティティは、ルート識別子と上記ユーザを認証するために上記ルート識別子に割り当てられたクレデンシャルとを含み、暗号化によりセキュリティ保護された上記レジスタは、上記ルート・アイデンティティに割り当てられた１つまたは複数の委任アイデンティティをさらに含み、上記委任アイデンティティのそれぞれが、委任識別子を含み、認証コンテキストに割り当てられ、上記コンピュータ・システムは、
・上記ユーザを認証することを求める認証要求を受け取り、

・上記ユーザの上記ルート・アイデンティティを使用して上記ユーザを認証することであって、成功裏の認証が上記ユーザの上記ルート・アイデンティティの上記ルート識別子に割り当てられた上記クレデンシャルを受け取ることを求める、上記認証を行い、

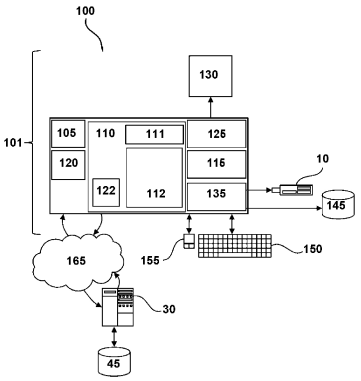
・要求された上記認証の認証コンテキストを識別し、

・上記ユーザの上記ルート・アイデンティティに割り当てられ、識別された上記認証コンテキストに割り当てられた、上記１つまたは複数の委任アイデンティティのうちの１つを、暗号化によりセキュリティ保護された上記レジスタを使用して識別し、

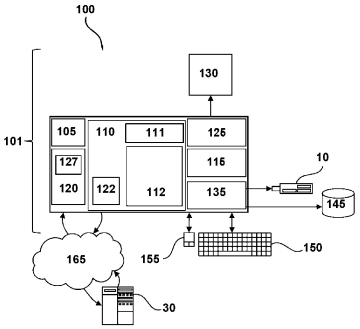
・上記ルート・アイデンティティを使用した上記ユーザの成功裏の認証に応答して、上記成功裏のユーザ認証を確認するとともに識別された上記委任アイデンティティの上記委任識別子によって上記成功裏に認証されたユーザを識別する、認証トークンを発行するように構成された、コンピュータ・システム。

【図面】

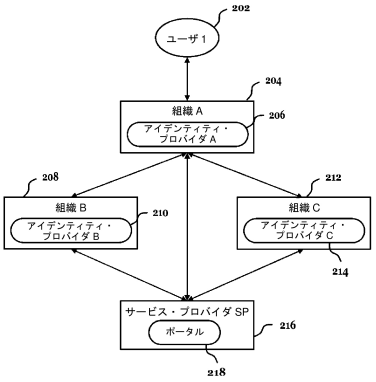
【図１】



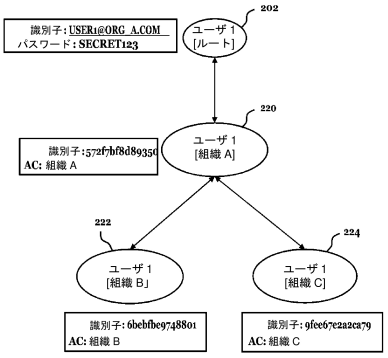
【図２】



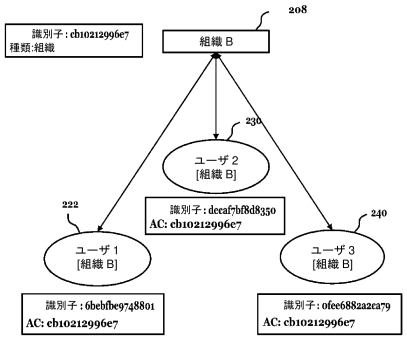
【図３】


202
ユーザ１
204
組織 A
206
アイデンティティ・プロバイダ A
208
組織 B
210
アイデンティティ・プロバイダ B
212
組織 C
アイデンティティ・プロバイダ C
214
サービス・プロバイダ SP
ポータル
216
218

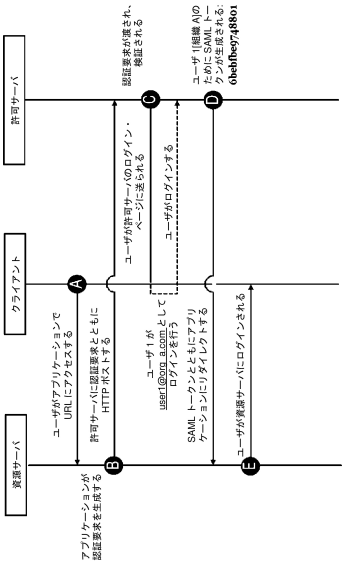
【図４】


識別子：USER1@ORG_A.COM
パスワード：SECRET123
202
ユーザ１
[ルート]
220
識別子：572f7bf8d89350
AC: 組織 A
ユーザ１
[組織 A]
222
224
ユーザ１
[組織 B]
ユーザ１
[組織 C]
識別子：6bebfbe9748801
AC: 組織 B
識別子：9fec67e2a2ca79
AC: 組織 C

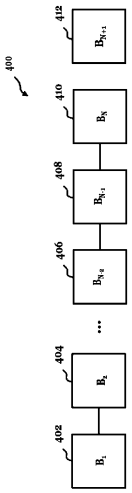
【図５】


識別子：cb10212996e7
種類:組織
208
組織 B
230
ユーザ２
[組織 B]
識別子：dceaf7bf8d8350
AC: cb10212996e7
222
240
ユーザ１
[組織 B]
ユーザ３
[組織 B]
識別子：6bebfbe9748801
AC: cb10212996e7
識別子：0fec6882a2ca79
AC: cb10212996e7

【図６】


許可サーバ
クライアント
資源サーバ
認証要求が渡され、検証される
ユーザ１(組織 A)のためにSAMLトークンが発行される
6bebfbe9748801
ユーザがアプリケーションでURLにアクセスする
許可サーバに認証要求とともにHTTP POSTする
ユーザが許可サーバへのログイン・ページに送られる
ユーザがログインする
ユーザ１が user1@org_a.com として ログインを行う
SAML トークンとともにアプリケーションにリダイレクトする
ユーザが資源サーバにログインされる
アプリケーションが認証要求を生成する
A
B
C
D
E

【図７】



フロントページの続き

(74)復代理人　110000420
弁理士法人ＭＩＰ
(72)発明者　ホフマン、フィリップ
ドイツ　７１０３２　ベーブリンゲン　シェーナイヒャー・シュトラーセ　２２０
(72)発明者　ピットナー、ダニエル
ドイツ　７１０３２　ベーブリンゲン　シェーナイヒャー・シュトラーセ　２２０
(72)発明者　ウェンルトペ、ムハメット
ドイツ　７１０３２　ベーブリンゲン　シェーナイヒャー・シュトラーセ　２２０
(72)発明者　ルブトッシュ、デビッド
ドイツ　７１０３２　ベーブリンゲン　シェーナイヒャー・シュトラーセ　２２０
(72)発明者　オーバーホーファー、マーティン
ドイツ　７１０３２　ベーブリンゲン　シェーナイヒャー・シュトラーセ　２２０

審査官　平井　誠
(56)参考文献　米国特許出願公開第２００３／０００５２９９（ＵＳ，Ａ１）
米国特許出願公開第２００７／０２３４４１７（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－８８