(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5952839号
(P5952839)
(45)発行日　平成28年7月13日(2016.7.13)　(24)登録日　平成28年6月17日(2016.6.17)

(51)Int.Cl.　　F I
G06F 21/33 (2013.01)　　G06F 21/33
H04L 9/32 (2006.01)　　H04L 9/00 675B

請求項の数 18　(全 16 頁)

(21)出願番号　特願2013-554563(P2013-554563)
(86)(22)出願日　平成24年2月15日(2012.2.15)
(65)公表番号　特表2014-510967(P2014-510967A)
(43)公表日　平成26年5月1日(2014.5.1)
(86)国際出願番号　PCT/US2012/025172
(87)国際公開番号　WO2012/112640
(87)国際公開日　平成24年8月23日(2012.8.23)
審査請求日　平成27年2月6日(2015.2.6)
(31)優先権主張番号　61/444,753
(32)優先日　平成23年2月20日(2011.2.20)
(33)優先権主張国　米国(US)
(31)優先権主張番号　13/372,613
(32)優先日　平成24年2月14日(2012.2.14)
(33)優先権主張国　米国(US)

(73)特許権者　512004567
カーン，ロバート，エス.
ＣＡＨＮ，Ｒｏｂｅｒｔ，Ｓ.
アメリカ合衆国　ニューヨーク州　１０５１２，カーメル，ジプシートレイルロード　６０７，ジプシートレイルクラブ
(74)代理人　110001302
特許業務法人北青山インターナショナル
(72)発明者　カーン，ロバート，エス.
アメリカ合衆国　ニューヨーク州　１０５１２，カーメル，ジプシートレイルロード　６０７，ジプシートレイルクラブ

審査官　脇岡　剛

最終頁に続く

(54)【発明の名称】関連付けられた組織証明書を利用するオンラインメンバシップ検証

(57)【特許請求の範囲】
【請求項１】
意図されるメンバのウェブサイトに提示されるメンバシップ証明書を検証するコンピュータ実施方法において、
前記メンバシップ証明書をアクティブ化するステップであって、前記メンバシップ証明書は、当該メンバシップ証明書の発行組織を識別するフィールドと、特定のフィールドタグにより構造化される、前記発行組織が前記メンバシップ証明書に含めることが許された前記意図されるメンバに関する特定の情報を含むペイロード部分と、を含むステップと、
前記メンバシップ証明書を作成した組織に関連付けられた組織証明書を検索するステップであって、前記組織証明書が、特定の種類の組織のみに関連付けられて前記メンバシップを定義する所定の情報要素セットであって、前記組織証明書およびメンバシップ証明書において識別される固定のフィールドのセットにより制御される情報要素セットを含む、検索ステップと、
前記メンバシップ証明書に提示される前記要素を前記組織証明書と比較するステップと、
前記メンバシップ証明書に提示される特定の固定のフィールドのセットが、前記識別された組織により定義されているように、前記組織証明書内に構成された所定の固定のフィールドのセットに一致する場合且つその場合に限り、前記メンバシップ証明書を証明するステップと、
を含むことを特徴とする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において、
前記組織証明書が、正規の証明機関（ＣＡ）により作成され、前記方法が、前記証明機関に関して前記組織証明書を認証するステップを含むことを特徴とす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において、
前記方法を実行するローカルコンピュータが、有効組織証明書のキャッシュを含むことを特徴とするコンピュータ実施方法。
【請求項４】
請求項１に記載のコンピュータ実施方法において、
前記方法を実行するローカルコンピュータが、ネットワークデータベースから現在有効な組織証明書のリストを取得することを特徴とする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において、
前記メンバシップ証明書の特定のフィールドと前記組織証明書の所定の固定のフィールドとの比較は、各特定のフィールド内の必要情報の包含についてのチェックを含むことを特徴とする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において、
前記メンバシップ証明書の特定のフィールドと前記組織証明書の所定の固定のフィールドとの比較は、複数のエントリが許可されていないものとして定義される所定の特定のフィールドについて、情報要素の存在が１つのみであることのチェックを含むことを特徴とする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において、
前記方法が、前記組織証明書が適宜署名され、期限切れしていないことを検証するステップを含むことを特徴とす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において、
前記方法が、前記メンバシップ証明書が期限切れしていないことを検証するステップを含むことを特徴とす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において、
前記組織証明書及び前記メンバシップ証明書は、結合証明書として提示され、前記組織証明書が最初に検証され、次に前記メンバシップ証明書が検証されることを特徴とするコンピュータ実施方法。
【請求項１０】
意図されるメンバのウェブサイトに提示されるメンバシップ証明書を検証するシステムにおいて、
前記メンバシップ証明書をアクティブ化するコンピュータ使用可能コード手段であって、前記メンバシップ証明書は、当該メンバシップ証明書の発行組織を識別するフィールドと、特定のフィールドタグにより構造化される、前記発行組織が前記メンバシップ証明書に含めることが許された前記意図されるメンバに関する特定の情報を含むペイロード部分とを含む、アクティブ化するコード手段と、
前記メンバシップ証明書を作成した組織に関連付けられた組織証明書を検索するコンピュータ使用可能コード手段であって、前記組織証明書が、特定の種類の組織のみに関連付けられて前記メンバシップを定義する所定の情報要素セットであって、前記組織証明書およびメンバシップ証明書において識別される固定のフィールドのセットにより制御される情報要素セットを含む、検索するコンピュータ使用可能コード手段と、

前記メンバシップ証明書に提示される前記要素を前記組織証明書と比較するコンピュータ使用可能コード手段と、
前記メンバシップ証明書に提示される特定の固定のフィールドのセットが、前記識別された組織により定義されているように、前記組織証明書内に構成された所定の固定のフィールドのセットに一致する場合且つその場合に限り、前記メンバシップ証明書を証明するコンピュータ使用可能コード手段と、
を含むことを特徴とするシステム。
【請求項１１】
請求項１０に記載のシステムにおいて、
前記組織証明書が、正規の証明機関（ＣＡ）により作成され、前記証明機関に関して前記組織証明書を認証するコンピュータ使用可能プログラムコード手段ことを特徴とするシステム。
【請求項１２】
請求項１０に記載のシステムにおいて、
前記コンピュータ使用可能プログラムコード手段が、有効組織証明書のローカルキャッシュを検索するステップを実行することを特徴とするシステム。
【請求項１３】
請求項１０に記載のシステムにおいて、
前記コンピュータ使用可能プログラムコード手段が、ネットワークデータベースから有効組織証明書を検索するステップを実行することを特徴とするシステム。
【請求項１４】
請求項１０に記載のシステムにおいて、
前記コンピュータ使用可能プログラムコードが、各特定のフィールド内の必要情報の包含について前記メンバシップ証明書の特定のフィールドをチェックするステップを実行することを特徴とするシステム。
【請求項１５】
請求項１０に記載のシステムにおいて、
前記コンピュータ使用可能プログラムコード手段が、複数のエントリが許可されていないものとして定義される所定の特定のフィールドについて、情報要素の存在が１つのみであることをチェックするステップを実行することを特徴とするシステム。
【請求項１６】
請求項１０に記載のシステムにおいて、
前記コンピュータ使用可能プログラムコード手段が、前記組織証明書が適宜署名され、期限切れしていないことを検証するステップを実行することを特徴とするシステム。
【請求項１７】
請求項１０に記載のシステムにおいて、
前記組織証明書及び前記メンバシップ証明書は、結合証明書として提示され、前記コンピュータ使用可能プログラムコード手段が、前記組織証明書部分の検証を最初に実行し、次に前記メンバシップ証明書部分の検証を実行することを特徴とするシステム。
【請求項１８】
請求項１０に記載のシステムにおいて、
前記コンピュータ使用可能プログラムコード手段が、前記メンバシップ証明書が期限切れしていないことを検証するステップを実行することを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本願は、２０１１年２月２０日に出願された米国仮特許出願第６１／４４４，７５３号明細書の利益を主張するものであり、この仮特許出願を参照により本明細書に援用する。
【０００２】

本発明は、公認組織から指定され制限された認証情報の、第２のサイトの認証を必要としないオンライン検証を提供するシステム及び方法に関する。

【背景技術】

【０００３】

オンライン身元識別の問題は、数年にわたり、積極的な研究分野であった。人物又は組織が、自分達が主張している人物又は組織であるか否かの問題は、いくつかのウェブに基づく革新を生み出した。オンライン小売業者に関連付けられることが多いように、ウェブサイトは、オンライン小売業者の信憑性を「検証」することを意図する別のサイトへのリンクを含み得る。そのリンクをクリックすることにより、ユーザ（見込み客等）は、オンライン小売業者の「証明書」を表示している別のウェブページにリダイレクトされる。一般に、これらのシステムは「第２サイト認証」と呼ばれ、偽造が比較的容易であることが分かっている（残念ながら）。悪質な個人は、信頼できる「検証サービス」と比較的似ているドメイン名を購入し得、次に、「偽の」証明書を作成し、特定の製品又はサービスの検証を求めている不用心な第三者に提示し得る。簡単に言えば、良質なサイトは、認証のためにユーザを他の良質なサイトに送り、悪質なサイトはユーザを他の悪質なサイトに送る。更に、第２サイト認証の市場での悪質サイトの蔓延も問題のままである。いくつかのブラウザアドオンは、ユーザに対して「悪質サイト」を警告し得るが、この解決策は、新しい悪質サイトを作成する悪人と、アドオンを管理し、悪質サイトの識別情報を常時更新する作業を有する人々との競争を生じさせる。実際には、この手法は、インターネットに基づく性的題材を警告するペアレンタルコントロールツールにより使用されるものと同じである。従って、経験から、競争が決して終わらないことが分かっており、有害な情報にアクセスする方法が常に存在することになる。

【０００４】

これらの問題のいくつかに対処する従来技術による１つの試みは、２００９年７月９日にＰａｕｌ　Ｌ．Ｏｌｓｏｎに発行された米国特許出願公開第２００９／０１７７６９４号明細書に開示されている。この開示では、全ての認証済み認証情報を記憶する中央リポジトリが作成され、各認証情報は、チェックサムを含むように形成される。次に、特定の認証情報の精査に関心を有する個人は、リポジトリにアクセスし、所望の認証情報を検索し、チェックサムが計算され、検証のために提示される。従って、一致する場合、個人への認証情報の証明であると見なされる。

【０００５】

より一般的な第２サイト認証プロセスを超える進歩があるものの、それでもやはり、誰かがＯｌｓｏｎのシステムを実施して、同様にして偽の認証情報を保持する「偽造サイト」をセットアップし維持することが可能である。これが可能なことの１つの理由は、発端である組織（例えば、職業団体、大学、ライセンシング組織等）が証明書の制御を保持せず、リポジトリに渡すためである。更に、証明書のいかなる種類の期限切れも、リポジトリに記憶されるデータと共に含まれることも示されていない。

【０００６】

２０１０年７月２日に出願され、参照により本明細書に援用される米国特許出願第１２／８２９，５５０号明細書において実施される、本発明者による先行研究は、従来技術の欠点の多くに対処する。しかし、以下において詳細に考察するように、従来のシステムは、証明書に含まれると考えることができる情報の「種類」を制限していなかった。

【０００７】

例えば、認証組織がイェール大学である場合、イェール大学が個人に認めた学位を証明することは問題ない。しかし、イェールは、職務経歴、兵役、又は市民権の好ましい情報源であるとは見なされない。従って、認証組織が検証する情報の種類も制御する仕組みが未だに必要とされている。

【発明の概要】

【０００８】

従来技術のこれら及び他の制限は、本発明により対処され、本発明は、公認組織から指

定され制限された認証情報の、第２のサイトの認証を必要としないオンライン検証を提供するシステム及び方法に関する。

【０００９】

特に、本発明は、「組織証明書」（ＯＣ）を「メンバシップ証明書」（ＭＣ）と組み合わせて利用して、独立した人物（第三者、即ち、意図されるメンバのウェブサイトのユーザ）に、指定された認証情報の検証を提供するシステム及び方法を記載し、ＯＣのフィールド構造は、発行組織が証明することができる情報の種類を制限する。

【００１０】

証明機関（ＣＡ）により発行される規格Ｘ．５０９証明書と同様に、本発明の方法論で使用されるＯＣも、組織をまず入念に調べ、その公開鍵を検証するＣＡにより組織に発行される。

【００１１】

本発明によれば、ＣＡにより制御され、ＭＣに含まれる情報が信用できることを保証する所定のフィールドセットを利用する組織証明書（以下、「ＯＣ」）が提案される。ＯＣ内のフィールドセットは、特定の種類の組織に関連付けられるものとして定義され、いかなる無関係情報も、正当なメンバシップ証明書（以下、「ＭＣ」）の一部をなすことが許されない。特定のフィールド記述の使用は、ＯＣにおいて対応する＜フィールド＞タグを有さないＭＣに見られるいかなるフィールドも、検証プロセス中、ユーザのブラウザ拡張機能により無効としてフラグ付けられると想定する。

【００１２】

本発明の更なる実施形態では、各フィールドに関連付けられたチェックの数は、１つ又は複数の特定のフィールドの属性を検証するために拡張することができる。更に、本発明により、ＭＣを検証するプロセスにおいて精査される「無効化された」ＯＣのリストを含むことが可能である。

【００１３】

本発明によれば、プロトコル及び暗号化を利用して、ウェブサイトと組み合わせて身元識別情報の信用できる証明を提示することができる人物（又は組織）と取引することを顧客（以下、全般的に「ユーザ」と称される）に保証するシステム及び方法が提供される。このシステムは、ユーザのブラウザから直接起動され、それにより、証明書検証プロセスは、別の（恐らくは悪質な）ウェブサイトを開き、そこから情報を得る必要なく、「ローカル」に実行される。期限切れ日が、好ましくは、ＯＣ及びＭＣの両方に含まれて、いずれの証明書も「古」くないことを保証するとともに、証明書が期限切れする固定日が作成される。

【００１４】

システム及び方法により提供される組織証明書及びメンバシップ証明書が、偽造又は盗難が難しいことが、本発明の態様である。知識（即ち、コンピュータの知識）が豊富なユーザが、証明書の信憑性を手動で検証することが可能であるが、本発明によるシステムの好ましい実施形態は、ユーザのブラウザを利用し、発端となる証明機関（ＣＡ）の公開鍵と組み合わせて認証組織に関連付けられた公開鍵を利用する新しいＭＩＭＥ（即ち、多目的インターネットメール拡張機能）型の作成に基づく。従来技術とは異なり、認証組織はメンバシップ証明の制御を保持する。

【００１５】

一実施形態では、本発明は、意図されるメンバのウェブサイト上にアイコン又はハイパーリンクとして提示される、メンバシップ証明書を検証するコンピュータ実施方法を含み、この方法は、メンバシップ証明書アイコンをアクティブ化するステップと、メンバシップ証明書を作成した組織に関連付けられた組織証明書（組織証明書はメンバシップを定義する所定の情報要素セットを含む）を検索するステップと、メンバシップ証明書に提示される要素を組織証明書と比較するステップと、メンバシップ証明書に提示される要素が、組織証明書内の所定の情報要素セットに一致する場合且つその場合に限り、メンバシップ証明書を証明するステップと、次に、メンバシップ証明書の署名を、組織証明書において

公開された公開鍵と突き合わせて検証するステップと、を含む。
【００１６】
別の実施形態では、本発明は、意図されるメンバのウェブサイト上にアイコンとして提示されるメンバシップ証明書を検証するコンピュータ使用可能コードを含むコンピュータ使用可能媒体を含むコンピュータ使用可能製品を定義し、コンピュータ使用可能媒体は、メンバシップ証明書アイコンをアクティブ化するコンピュータ使用可能コードと、メンバシップ証明書を作成した組織に関連付けられた組織証明書（組織証明書は、メンバシップを定義する所定の情報要素セットを含む）を検索するコンピュータ使用可能コードと、メンバシップ証明書に提示される要素を組織証明書と比較するコンピュータ使用可能コードと、メンバシップ証明書に提示される要素が、組織証明書内の所定の情報要素セットに一致する場合且つその場合に限り、メンバシップ証明書を証明し、次に、メンバシップ証明書の署名を、組織証明書において公開された公開鍵と突き合わせて検証する、メンバシップ証明書を証明するコンピュータ使用可能コードと、を含む。
【００１７】
更なる実施形態では、本発明は、意図されるメンバのウェブサイト上のアイコンとして提示される、メンバシップ証明書を検証するシステムを開示し、このシステムは、メンバシップ証明書アイコンをアクティブ化するコンピュータ使用可能コード手段と、メンバシップ証明書を作成した組織に関連付けられた組織証明書（組織証明書は、メンバシップを定義する所定の情報要素セットを含む）を検索するコンピュータ使用可能コード手段と、メンバシップ証明書に提示される要素を組織証明書と比較するコンピュータ使用可能コード手段と、メンバシップ証明書に提示される要素が、組織証明書内の所定の情報要素セットに一致する場合且つその場合に限り、メンバシップ証明書を証明するコンピュータ使用可能コード手段と、を含む。
【００１８】
本発明の他及び更なる態様及び実施形態が、以下の考察及び添付図面への参照の過程において明白になるだろう。
【図面の簡単な説明】
【００１９】
【図１】図１は、本発明により形成されるメンバシップ証明書（ＭＣ）の基本図である。
【図２】図２は、例示的なＭＣのリストを含む。
【図３】図３は、本発明により形成される組織証明書（ＯＣ）及び関連付けられたフィールド識別テーブルの基本図である。
【図４】図４は、例示的なＯＣの証明機関部分のリストを含む。
【図５】図５は、例示的なＯＣの組織識別部分のリストを含む。
【図６】図６は、本発明のプロセスにおいて使用し得る拡張型のフィールド識別テーブルを示す。
【図７】図７は、ＯＣ及びＭＣの両方を実施する結合証明書（ＣＣ）の基本図である。
【図８】図８は、本発明により提示されるＭＣを検証する例示的なプロセスのフローチャートである。
【発明を実施するための形態】
【００２０】
詳細に後述するように、本発明は、組織証明書（ＯＣ）を利用して、メンバシップ証明書（ＭＣ）を作成し、後に、第三者がメンバシップ証明書にアクセスして、「メンバ」（個人、ビジネス、企業等）が参加（認証）組織（即ち、大学、ライセンシング組織、職業団体）に合法的に関連付けられていることを検証することができる。特に、ＯＣは、ＭＣ内に含めることができる情報の種類を、発行組織に関連する情報のみに制限するように構造化される。
【００２１】
特定の個人又はビジネスのウェブサイトを開く場合、特定の個人又はビジネス（又は任意の他の種類のエンティティ）の信憑性を検証するために、本発明が公衆により利用され

ることが意図される。ウェブサイトは、リアルタイムでアクティブ化して、検証プロセスを始動するために使用することができるＭＣアイコン（又はハイパーリンク）を含む。従って、ウェブサイトを開く個人（以下、「ユーザ」として定義される）は、「メンバシップ」アイコン／ハイパーリンクを見て、その位置をクリックして、検証プロセスを実行する。成功の場合、プロセスは、ユーザによる視覚的確認のために検証された証明書を表示し、プロセスが何らかの理由により失敗する場合、エラー／失敗メッセージがユーザに表示される。ユーザのブラウザは恐らく、全ての有効ＯＣの識別情報を含め、検証プロセスを実行するために必要なアドオンを含むように構成され、ユーザが利用するシステムの詳細については、本出願人の同時係属中の出願第１２／８２９，５５０号明細書に詳細に説明されており、この出願を参照により本明細書に援用する。

【００２２】

図１は、ここではＭＣ１０として定義される、例示的なメンバシップ証明書内に含まれる情報の種類を高レベル図形式で示す。ＭＣ１０の要素の順序は重要ではなく、本発明の範囲を限定するものとして見なされるべきではない。示されるように、ＭＣ１０はウェブサイト識別要素１２を含み、この要素１２は、この特定のＭＣに関連付けられたウェブサイトを定義する。ウェブサイト情報の包含により、悪質な個人がＭＣを「盗」み、別のウェブサイトで再公開しないようにする。ＭＣ１０は組織識別要素１４も含み、この要素１４は、組織証明書（ＯＣ）を最初に承認した証明機関（ＣＡ）により提供される「証明」シリアル番号を含め、ＭＣを発行する組織を定義する情報を含む。後で手短に考察し、且つ本出願人の同時係属中の出願に詳述されるように、ＣＡは、「要求側組織」が実際に意図される組織であることを確認する提示ドキュメントである。次に、この情報は入念に調べられ（多かれ少なかれ、状況に応じて）、確認後、ＣＡは、一意のシリアル番号を有するＯＣを要求側組織に発行し、要求側組織において、その番号が次に、要求側組織のＯＣ及び発行されるあらゆるＭＣに含められる。ＭＣ１０に関連付けられた特定の「メンバ」（ユーザが開いているウェブサイトの個人／企業）の識別情報が、メンバ要素１６としてＭＣ１０に含まれる。図１に示されるように、ＭＣ１０のペイロード部分１８は、特定のフィールドタグにより構造化される、発行組織がＭＣに含めることが許された、個人に関連する特定の情報を含む。

【００２３】

図２は、１行目がウェブサイト識別要素１２に対応する、ＭＣ１０の例示的なリストを含む。重要なことには、リストの２行目はこの特定のＭＣの期限切れ日を含み、上述したように、ＭＣ内の情報が「古く」ならず、期限切れ日が含まれて、証明された情報の信憑性を更に保証することが重要である。続く２行が、発行組織の名称（ここでは、イェール大学）及び監督ＣＡによりイェール大学に発行された特定の一意のシリアル番号の両方を含む組織識別要素１４を具現する。リストの５行目は、図１の図では要素１６として含まれる、ＭＣ１０に関連付けられた特定の「メンバ」の識別されたを含む。

【００２４】

本発明によれば、図２のリスト内の残りのフィールドは特にタグ付けされ、発行組織により供給されることが許された詳細情報（即ち、ＭＣ１０の「ペイロード」部分１８）を含む。詳細に後述するように、異なるフィールドは異なる属性を有し、「単一」のみの情報を含むものもあれば、「複数」の情報を含むものもある。更に、フィールドによっては「必須」であるものもあれば、「任意」であるものもある。明らかなことに、これらの属性は発行されているＭＣの種類に固有であり、大学は１組のフィールド及び属性を有し、ＡＭＡ等のライセンシング組織は別の組のフィールド及び属性を有する。実際には、発行組織がＭＣにおいて供給する情報の種類が、ＯＣ及びＭＣにおいて識別される固定のフィールドセットにより制御されることは、本発明の重要な態様である。

【００２５】

同時係属中の出願番号第１２／８２９，５５０号明細書に記載されるような本出願人の前の仕組みと比較して、ＯＣは、組織の検証に関連付けられた署名付きＧＰＧ鍵又は署名付きＸ．５０９証明書に取って代わる。一般に、ＯＣは大まかにＸ．５０９に基づくが、

いくつかの主な違いがある。ＯＣは、標準Ｘ．５０９証明書に含まれるよりも、組織について多くの情報を含む。後述するように、ＯＣはまた、Ｘ．５０９証明書で許されているように証明機関（ＣＡ）からＣＡに「連鎖」させることができず、「ルート」ＣＡに戻る全ての組織により署名する必要がある。

【００２６】

より詳細には、本発明のＯＣは、（１）証明機関の識別情報、（２）組織の識別情報、（３）組織により提供される特定の情報を定義するフィールド識別情報、（４）組織の公開鍵、及び（５）ＯＣの有効期間（即ち、期限切れ日）を含む選択された要素セット（別様に実施し得る）を必要とする。図３は、これらの要素を含む例示的なＯＣ２０を示し、ＯＣ２０は、意図される「メンバ」のウェブサイトを見ているユーザによる検証のために提示されるＭＣを有効化（又は場合によっては無効化）するために使用される。

【００２７】

図３に示されるように、ＯＣ２０は上述した要素を指定するいくつかの別個のフィールドを含む。特に、ＯＣ２０は、ＯＣを発行した「証明機関」（ＣＡ）及び組織に割り当てられた一意のシリアル番号を定義する第１のフィールド２２を含む。ＯＣ２０内の次のフィールド２４は、この証明書が作成された特定の組織を識別する。フィールド識別ポインタ２６は、図３に示されるように、プロセスを別個のフィールド識別テーブル３０に向けるためにＯＣ２０内に含まれ、使用される。詳細に後述するように、フィールド識別テーブル３０は、ＭＣを作成する場合、組織が追加入力する特定のタグ付けフィールドを含む。最後に、ＯＣ２０は、発行組織の公開鍵と、好ましくは、ＯＣ２０の期限切れ日と、を含む検証フィールド２８を含む。

【００２８】

ＭＣにより生まれるライセンシング及び収益を適宜統制するために、ＯＣには、ルートＣＡに戻る連鎖内の全ての発行者が署名する必要がある。あるいは、ＯＣには、発端となったＣＡ（即ち、連鎖中、ＯＣに「最も近い」ＣＡ）及びルートＣＡにより署名することができる。この態様を利用して、様々なＣＡ間での商業関係を施行することができる。

【００２９】

これは、例として示すことができる。ＣＡ１がルートＣＡであり、世界中で生成される全てのＯＣに署名するものと仮定される。ＣＡ１は、ＣＡ２と商業関係になり、カナダ国の組織証明書を発行する。そして、ＣＡ２はＣＡ３と関係になり、オンタリオ州の証明書を発行する。

【００３０】

トロント大学は、ＭＣを卒業生に発行するためにＯＣを取得したい場合、ＣＡ３と交信するように指示される。続けて、ＣＡ３は、トロント大学を確認するために必要な適正評価を実行し、大学のＯＣに署名する。トロント大学は次に、署名付きＯＣ及び関係書類を、署名のためにＣＡ２に転送し、ＣＡ２において、パッケージは次に、最後の署名のためにＣＡ１に転送される。このプロセスは、商業関係のために、組織及び秩序だった会計を入念に調べる一貫したプロセスがあることを保証する。

【００３１】

ＯＣを処理するブラウザ拡張機能が、ＣＡ１による「外部」署名を検証する必要があるだけであり、ＣＡ２及びＣＡ３による「内部」署名を恐らくは無視することができることを理解されたい（仮定は、前の機関がＯＣを精査し承認した場合のみ、ＣＡ１が見つけられるというものである）。あるいは、ブラウザ拡張機能は、全てのＣＡ公開鍵のデータベースを保持し、ＣＡに含まれる署名のそれぞれ１つを検証することができる。

【００３２】

図４は、ＯＣ２０内に含まれる例示的なＣＡフィールド２２のリストであり、ＯＣ２０のこの部分が、Ｘ．５０９証明書内のフィールドに類似することが分かる。この場合、「Ｖｅｒｉｆｙ　Ｍｅｍｂｅｒｓｈｉｐ，Ｉｎｃ．」が、証明機関としてリストの５行目に示される。図４の２行目に示されるシリアル番号は、ＣＡの識別番号で開始される。この特定の実施形態では、番号００：００が示され、「ｉｓｓｕｅｒ＿ｐａｒｅｎｔ」と同じ

であるため、「ルート」として定義される。本発明の検証システムは、企業判断及び動作効率により支配されるように、単一のルート機関を利用してもよく、又は複数のルートを利用してもよい。図４に示されるように、ＣＡは、ＯＣ２０のこの部分に詳細な交信情報を含み、それにより、特定のＭＣの検証に関わるユーザは、必要な全ての情報にアクセスすることができる。図４に示される特定の実施形態では、「検証レベル」の表示は、ＯＣ２０のこの部分の１０行目に含められ、組織の識別情報及び組織の履歴を特定するためにＣＡが実行する入念な検査の程度を指す。この「レベル」情報の包含により、ＭＣにおいて組織により最終的に供給される情報の信用レベルを高く及び低くすることができる。

【００３３】

図５は、「組織」イェール大学（例示のみを目的とする）である場合の、ＯＣ２０の組織識別フィールド２４の例示的なリストを含む。このリストが、住所、電話番号、及びウェブサイト情報等のイェール大学についての様々な詳細を含むことが分かる。上述したように、本発明により構成される特定のＯＣは、標準Ｘ．５０９証明書よりも詳細に発行組織を識別する。その結果、特定のＭＣを精査しているユーザは、最初にＭＣを発行する組織に関連付けられた必要なあらゆる背景情報に精通することにもなる。

【００３４】

本発明の重要な態様は、特定の組織が「証明」することができる情報の種類の制御である。教育機関のこの場合、情報の種類は、入学許可日及び卒業日、授与された学位、賞与等に限定される。この制御を、ＭＣにおいて組織が「証明」することができる情報の種類に提供するために、ＯＣは、図３に示されるように、フィールド識別テーブル３０を利用し、フィールド識別テーブル３０は、組織が発行するＭＣに含み得る特定の制限された記述子セットを含む。明らかなことに、提示されたＭＣの認証過程中に精査されている特定のテーブルが、名称が示されていない任意のフィールドを含む場合、ＯＣ２０は無効として拒絶される。

【００３５】

図３を参照すると、フィールド識別テーブル３０が大学（又は任意の種類の教育機関）に関連付けられた情報を含むことが明らかである。本発明により、他の種類の組織が、テーブルにおいて、その組織でのメンバシップを認めることに関連する情報を定義する異なる特定のフィールドセットを利用することを理解されたい。例えば、米国赤十字に関連付けられたＯＣは、「メンバ」の血液型及び恐らくはメンバが献血した最新日のみを確認するフィールドリスト識別テーブルを利用し得る。

【００３６】

これよりテーブル３０を参照すると、いくつかの特定のフィールドが示され、各フィールドはそのフィールドを定義する特定の属性セットも含む。示されるように、第１のフィールド３２は、このテーブルへの問い合わせ元の特定のＯＣに関連付けられた特定の「組織」を定義する。この場合、「内容属性」３４は「イェール大学」として示される（この場合、明らかなことに、これが、発端となったＯＣでの組織定義に一致しない場合、プロセスは中止され、ＯＣは無効と考えられる）。このフィールドは、好ましくは、テーブルにおいて、「固定」エントリとして定義され、常に必要とされ、テーブルで１回のみ出現することができるフィールドである。明らかなことに、証明組織の識別情報はこの種の情報である。

【００３７】

続けて、フィールド識別テーブル３０内のメンバフィールド４０は、ＭＣを要求している特定の「メンバ」を識別する。メンバフィールド４０は、「必要／任意」インジケータ３６及び「単一／複数」インジケータ３８を含むものとして定義される２つの属性を含む。インジケータ３６での「必要」表示は、発行されるＭＣに含まなければならない情報を定義し、ＭＣの検証中にこれが「欠落（ｍｉｓｓｉｎｇ）」の場合、ユーザのブラウザはエラーメッセージを作成する（そして、その場合、ユーザは、提供されたＭＣが偽物であるか、歪められたものであると想定する）。同様に、インジケータ３８での「単一」表示は、この特定のフィールドの１つのみのインスタンスをＭＣに含むことができることを意

味する（ここで、「単一」では、「必要」としても定義されない場合、このフィールドは「欠落（ｍｉｓｓｉｎｇ）」してもよい）。複数のエントリを含む場合、証明書プロセスを実行中のユーザのブラウザはここでも、エラーメッセージを発行する。明らかなことに、ＭＣに関連付けられた「メンバ」の識別情報は必要且つ単一でなければならない。メンバの氏名（この例では、「Ｊａｍｅｓ　Ｔｈｏｍａｓ」として示される）が、フィールドの内容部分に含まれる。

【００３８】

証明書期限がフィールド４２に含まれ（ここでも「必要」、「単一」）、ＭＣが表示されるウェブサイトがフィールド４４に含まれる（「必要」、「単一」）。組織の種類に関係なく、これらの最初の４つのフィールドが、発行される大半の証明書に含まれると仮定すべきである（恐らくはテーブル内において異なる位置及び異なる順序で）。

【００３９】

テーブル３０に示される続くフィールドは、大学をＯＣとして有することの詳細に関する。示されるように、フィールド４６は、個人の入学日を指定し（「必要」、「単一」）、続くフィールド４８は個人の卒業日を指定する。機関に入学したあらゆる人が卒業するわけではないため、このフィールドは、識別子４６で示されるように、「任意」である（識別子４８に「単一」表示が保たれる間）。この特定のテーブル内の別個のフィールド５０は、表示「中退」を有し、この情報を証明書に含められるようにする。フィールド５２は、授与された学位（「任意」、「複数」）を定義し、「任意」及び「複数」としてそれぞれインジケータ５６及び５８により定義されるフィールド５４（「賞与」を有する）に示される任意の特定の賞与。

【００４０】

フィールド識別テーブル３０に示されるフィールドのこのリストが、単なる例示であり、他を含んでもよいことを理解されたい。しかし、教育機関は、「雇用形態」、「市民権」、兵役記録」等の特定の種類の情報を検証することが決して許されず、これらの特定の種類の情報は全て、異なる組織により、よりよく検証される。従って、本発明によれば、イェール大学等により発行されるＭＣは、個人の教育認証情報のみに関連付けられた情報を含むように制限される。同様に、企業等のＯＣにより発行されるＭＣは、職務経歴のみに制限され、米国空軍等のＯＣにより発行されるＭＣは、兵役等のみに制限される。ＣＡを入念に調べるプロセスの一部は、組織と協働して、ＭＣに含めるべき特定のフィールドを決定することを含むものと意図内。このプロセスの採用が普及する場合、単科大学及び総合大学が学位の認可を確認するために発行されるＭＣにおけるフィールドの標準リストについて合意し、それにより、更に自動化された処理を実施可能なことが予期される。

【００４１】

本発明によれば、内容を検証する、テーブル３０に内蔵される追加のチェックがあり得る。例えば、テーブル３０の特定の構成では、「卒業」及び「中退」フィールド４８及び５０の両方が「真」であるべきではなく、一方のみが存在する場合、任意であることが意図される。意味論チェックを適用して、この種のエラーがテーブルに入力されることを回避することができる。追加又は代替として、「最終形態」として定義される別のフィールドを含むことができる－値は、ｗｉｔｈｄｒｅｗ（中退）、ｔｒａｎｓｆｅｒｒｅｄ（転出）、ｇｒａｄｕａｔｅｄ（卒業）、ｅｘｐｅｌｌｅｄ（退学処分）、ｃｕｒｒｅｎｔ＿ｓｔｕｄｅｎｔ（現在生徒）という値のドロップダウンメニューから選択される。

【００４２】

再び図２に示されるＭＣ１０に関連付けられた特定のリストを参照すると、ＭＣ１０が、＜入学許可２＞及び＜卒業２＞に加えて、任意フィールドとして＜学位２＞を含むことが分かる。これにより、＜学位２＞フィールドに何も入力せずに、＜入学許可２＞フィールドに情報を含むＭＣ－意味のない種類の証明書－を作成可能なことが明らかである。この問題を回避するために、フィールド識別テーブルは、２つの追加のインジケーター「必要」及び「生成」を含むように増補することができる。図６は、これらのインジケータを利用して、供給された情報が無効であることを保証する例示的なフィールド識別テーブル

５０の部分を含む。

【００４３】

書かれているように、テーブル５０は冗長である。テーブル５０は、＜学位２＞が＜入学許可２＞及び＜卒業２＞の両方についての情報を生成することを示し、これは＜入学許可２＞が＜学位２＞を必要とすることに等しい。簡潔にするために、テーブルは、第２のフィールドが「必要／任意」、「単一／複数」であるかどうかに関わらず、別のフィールドを必要とするフィールドを許容可能であるように編成することができる。ＭＣを確認するブラウザ拡張機能は単に、第２のフィールドに直面した場合、第１のフィールドのインスタンスが証明書にあることをチェックする。これは、証明書の２回の読み取りを必要とし得る。第１のパスは、証明書中のフィールドを識別し、第２のパスは、必要インジケータ及び生成インジケータにより指定される条件が満たされることを検証する。

【００４４】

各ＯＣは、発行組織及びＣＡの両方の交信情報を含むため、任意のエラーに対するデフォルト対策は、対応するＭＣの確認である（そして、そのＯＣにより署名された全てのＭＣを拒絶させる）。処理ソフトウェア、大概はブラウザ拡張機能は、ＯＣのユーザがこれらのエンティティのうちの１つ又は複数と交信することを示唆し得る。典型的なエラーとしては、期限切れ通知キー、不良署名、開始タグと終了タグとの不一致、必須タグの欠落、示されたタグがフィールド記述子に含まれていない、及び「単一」として定義されるフィールド内の「複数」の種類のデータの包含が挙げられるが、これらに限定されない。

【００４５】

ウェブサイトがＭＣを含む場合、ＭＣを検証しようとする個人は対応するＯＣも取得する必要がある。これに対する一解決策は、全ての現在のＯＣを記憶するウェブサイトを維持することである。次に、ユーザ機のブラウザ拡張機能又はプラグインは、アンチウィルスプログラムが定期的に規則正しくウィルスシグネチャをダウンロードするのと略同じように、ＯＣウェブサイトにアクセスすることができる。

【００４６】

あるいは、ＯＣ及びＭＣを、結合証明書（ＣＣ）と称される単一のパッケージに組み合わせることができ、ＣＣはメンバのウェブサイトに配置される。図７は例示的なＣＣ６０を示し、ＣＣ６０は、ＯＣ２０とＭＣ１０との境界を示すために使用される特定の区切り文字を含む。示されるように、ＣＣ６０は組織の秘密鍵で署名され、ＯＣ２０はＣＡの秘密鍵で署名される。

【００４７】

図７に示される特定のＣＣを使用するＭＣのアクセス及び検証に関連付けられた特定のプロセスフローが、図８のフローチャートに含まれる。一般に、プロセスはＣＣ６０内のＯＣ２０をまず分離することに進み、次に、ＭＣ１０を抽出し、ＯＣ２０に関してその内容を検証する。

【００４８】

図８のフローチャートを参照すると、プロセスは、ＯＣ２０の署名の検証で開始される（ステップ１００）。ブラウザ拡張機能が、ＯＣ２０の署名の検証に使用することができる初期ＣＡ公開鍵セットを含むものと仮定される。ＣＡ署名がこれらの鍵の１つと突き合わせて正しい場合、ＯＣ２０は有効であると見なされ、組織公開鍵がＯＣ２０から抽出される（ステップ１１０）。その他の場合、ユーザのブラウザにより処理は停止し、「エラー」が報告される（ステップ１２０）。エラーが報告されると、ＯＣ２０及びＭＣ１０の両方内に含まれる情報は無効であると見なされ、ウェブブラウザによりユーザに表示されない。その代わり、ユーザには、ＣＡ鍵に伴う問題の結果、ＣＣ６０が有効ではないことが通知される。正しいＣＡ公開鍵を発見することができない場合、ＣＡ公開鍵のキャッシュへの更新の遠隔検索を始動する（ステップ１３０）ことが可能であり、見つかった場合、プロセスはステップ１４０に進む。

【００４９】

いずれの場合でも、ＯＣ公開鍵が抽出されると、ＯＣ２０の期限切れ日が、現在日時と

突き合わせてチェックされる（ステップ１４０）。時間期間が過ぎている（又はまだ開始されていない）場合、エラーが報告され（ステップ１５０）、処理は中止され、エラーメッセージ以外の情報はユーザに表示されない。公開鍵が有効であると仮定すると、公開鍵を使用して、ＣＣ６０の署名を検証する（ステップ１６０）。ここでも、証明されない場合、プロセスは、エラーメッセージを伴って中止される（ステップ１７０）。ＣＣ６０の署名が有効であると仮定すると、プロセスの次のステップ（ステップ１８０）は、ＣＣ６０からのＭＣ１０の抽出に進み、＜ウェブサイト＞がＣＣ６０に示されるロケーション（ＵＲＬ）と突き合わせてチェックされる（ステップ１９０）。一致しない場合、プロセスは終了する（ステップ２００）。この時点で、悪質な個人が、別の個人向けに作成されたメンバシップ証明書を使用しようとしていることを組織に通知することができる。

【００５０】

＜ウェブサイト＞がＣＣと一致すると仮定すると、ＯＣ２０のポインタ２６を使用して、ＭＣ１０内のフィールドにアクセスし（ステップ２１０）、ＭＣ内のフィールドは、フィールド識別テーブル３０と突き合わせてチェックされ（ステップ２２０）、ステップ２３０において、比較動作を実行する。フィールドが適宜入力されていない場合（例えば、「必要」フィールドが欠落している、「単一」フィールドが「複数」表示を有する）、又は意味論チェックが「真」ではない場合、又はＭＣがテーブル３０において指定されない情報を含むように試みる場合、プロセスは終了し（ステップ２４０）、ユーザは、精査中のＭＣが有効ではないことが「警告」される。その他の場合、プロセスは、ＣＣ６０自体の期限切れデータのチェック（ステップ２５０）に進む。

【００５１】

後述する他のチェック（ステップ２６０）をプロセスに追加して、ＭＣ１０の有効性を更に保証し得る。全てのテストが完了すると、ＭＣ１０の内容は、ユーザによる閲覧のために表示され（ステップ２７０）、証明書の特定の属性の視覚的確認（例えば、ウェブサイトの所有者がイェール大学の卒業生であることの証明書）を提供する。

【００５２】

特に、ユーザのブラウザが「履歴」照会をサポートする場合、「前のページ」がＭＣに含まれる＜ウェブサイト＞に対応することのチェックを行うことができる。ＭＣの信憑性を更に制御するために、「再生攻撃」を回避するために使用され、ユーザのブラウザにローカルな、ローカルに選択される（即ち、「秘密の」）色のローカルで既知（即ち、「秘密」）のセキュリティフレーズを含むように構成し得る。従って、「秘密のフレーズ」－「秘密の色」でプリントされる－が、証明書チェックプロセスで出現しない場合、ユーザは、誰かが偽の証明書をユーザに提示しようとしていることを知る。

【００５３】

検証プロセス中、無効化されたＯＣの「チェック」を含むことも可能である。例えば、ＣＡは、特定の組織のＯＣを無効化したいことがある。その場合、ＣＡは、「不良」組織により発行された全てのＭＣが無効であることを保証したい。この場合、ユーザのブラウザ拡張機能は、証明書無効化リスト（ＣＲＬ）についてＣＡを照会する。ＯＣが、初期／発行ＣＡからルートまでＣＡの連鎖（複数のＣＡが存在する場合）を遡ることによりチェックされるかもしれない。これにより、「不良」ＣＡにより発行された全てのＯＣを一度に無効化することができる。

【００５４】

現在のプロセスに関連付けられた特定のＯＣがリストにない場合、拡張機能は組織自体を照会して、特定のＭＣが無効化されたか否かを判断することができる。これは、Ｘ．５０９証明書のように、一意のＩＤを有するＭＣを発行する必要がある。いずれの場合でも、ブラウザ拡張機能は、エラー報告メカニズムを使用して、無効化されたＣＣ（ＭＣに基づく）の使用を発行組織に報告し得る。これにより、発行組織は、ウェブサイトの所有者を追跡し、ＣＣの除去を求める。

【００５５】

上述したブロック図内の構成要素及びフローチャート内のステップは、単なる例示とし

て説明される。構成要素及びステップは、説明の明確性をために選択されており、例示的な実施形態を限定しない。例えば、特定の実施態様は、例示的な実施形態の範囲から逸脱せずに、任意の構成要素又はステップの結合、省略、更なる細分、変更、強化、低減、又は代替の実施を行い得る。更に、上述したプロセスのステップは、例示的な実施形態の範囲内で異なる順序で実行し得る。

【００５６】

従って、コンピュータ実施方法、装置、及びコンピュータプログラム製品が、本発明による組織証明書及びメンバ証明書の使用を検証し施行する例示的な実施形態において提供される。本発明は、全体的にハードウェア実施形態、全体的なソフトウェア実施形態、又はハードウェア要素及びソフトウェア要素を含む実施形態の形態をとることができる。好ましい実施形態では、本発明は、ファームウェア、常駐ソフトウェア、及びマイクロコードを含むが、これらに限定されないソフトウェアで実施される。

【００５７】

更に、本発明は、コンピュータ若しくは任意の命令実行システムにより使用されるか、又はこれ（ら）と併せて使用されるプログラムコードを提供するコンピュータ使用可能又はコンピュータ可読媒体からアクセス可能なコンピュータプログラム製品の形態をとることができる。この説明では、コンピュータ使用可能又はコンピュータ可読媒体は、命令実行システム、装置、若しくはデバイスにより使用されるか、又はこれ（ら）と併せて使用されるプログラムの包含、記憶、通信、伝播、又は輸送を行うことができる任意の有形装置であることができる。

【００５８】

媒体は、電子システム、磁気システム、光学システム、電磁システム、赤外線システム、又は半導体システム（又は装置、又はデバイス）であることができる。半導体又は固体状態メンバ、磁気テープ、ランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、剛性磁気ディスク、及び光ディスクを含むコンピュータ可読媒体の例。光ディスクの現在の例としては、コンパクトディスク読み取り専用メモリ（ＣＤ－ＲＯＭ）、コンパクトディスク－読み取り／書き込み（ＣＤ－Ｒ／Ｗ）、及びＤＶＤが挙げられる。

【００５９】

更に、コンピュータ記憶媒体は、コンピュータ可読プログラムコードがコンピュータで実行される場合、このコンピュータ可読プログラムコードの実行により、コンピュータに、通信リンクを介して他のコンピュータ可読プログラムコードを送信させるようなコンピュータ可読プログラムコードを含むか、又は記憶し得る。この通信リンクは、例えば、限定ではなく物理的に、又は無線である媒体を使用し得る。

【００６０】

本発明の説明は、例示及び説明のために提示されており、網羅的である、即ち、本発明を開示された形態に限定する意図はない。多くの変更及び変形が当業者には明らかになるだろう。実施形態は、本発明の原理及び実際用途を説明するため、且つ意図される特定の用途に適する様々な変更を行った様々な実施形態で本発明を他の当業者が理解できるように選ばれ説明された。

【図１】

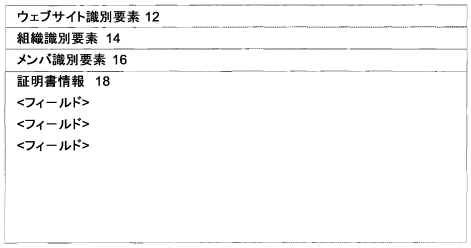


図１

【図２】

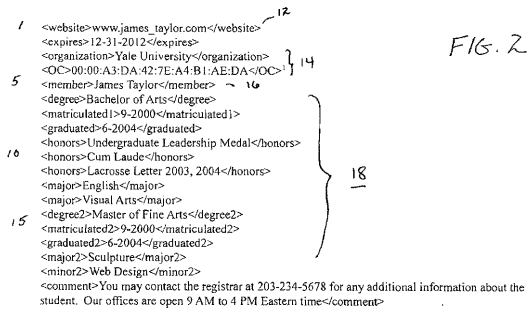
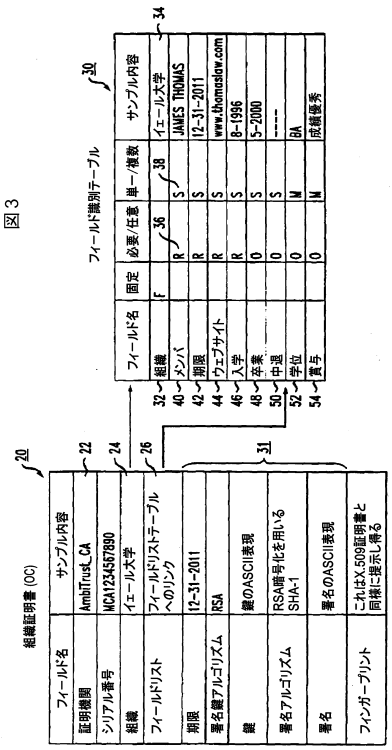


FIG. 2

【図３】



【図４】

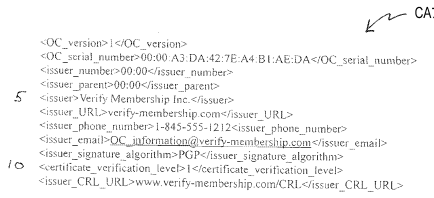


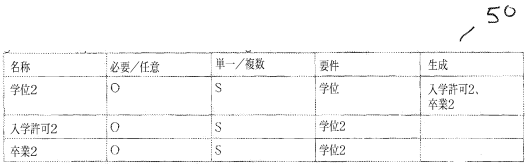
図4

FIG. 4

【図５】

FIG. 5

【図６】


50

名称	必要／任意	単一／複数	要件	生成
学位2	O	S	学位	入学許可2、卒業2
入学許可2	O	S	学位2	
卒業2	O	S	学位2	

図6

【図７】

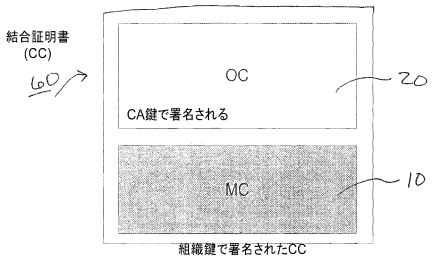


図7

【図８】

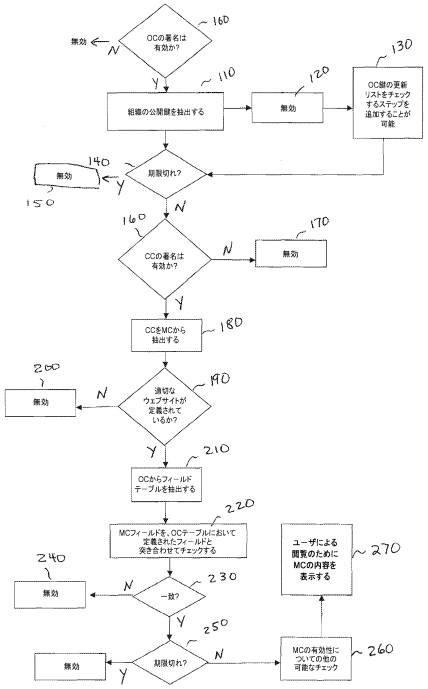

160
OCの署名は有効か?
無効
N
Y
110
組織の公開鍵を抽出する
120
無効
130
OC側の更新リストをチェックするステップを追加することが可能
140
無効
150
期限切れ?
Y
N
160
CCの署名は有効か?
N
170
無効
Y
CCをMCから抽出する
180
200
無効
N
適切なウェブサイトが定義されているか?
190
Y
210
OCからフィールドテーブルを抽出する
220
MCフィールドを、OCテーブルにおいて定義されたフィールドと突き合わせてチェックする
240
無効
N
一致?
230
Y
250
無効
Y
期限切れ?
N
MCの有効性についての他の可能なチェック
260
ユーザによる閲覧のためにMCの内容を表示する
270

図８

フロントページの続き

(56)参考文献　米国特許出願公開第２０１１／００１０５５３（ＵＳ，Ａ１）
特開２００６－０６７５１５（ＪＰ，Ａ）
国際公開第２００８／０５０７９２（WO，Ａ１）

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