(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7620974号
(P7620974)

(45)発行日　令和7年1月24日(2025.1.24)

(24)登録日　令和7年1月16日(2025.1.16)

(51)国際特許分類

| | | | | |
|---|---|---|---|---|
| *Ｇ０９Ｃ* | *5/00 (2006.01)* | Ｇ０９Ｃ | 5/00 | |
| *Ｈ０４Ｌ* | *9/32 (2006.01)* | Ｈ０４Ｌ | 9/32 | ２００Ｚ |

請求項の数　15　（全23頁）

(21)出願番号　特願2020-565027(P2020-565027)
(86)(22)出願日　平成31年1月20日(2019.1.20)
(65)公表番号　特表2021-514493(P2021-514493A)
(43)公表日　令和3年6月10日(2021.6.10)
(86)国際出願番号　PCT/IB2019/050466
(87)国際公開番号　WO2019/155309
(87)国際公開日　令和1年8月15日(2019.8.15)
審査請求日　令和4年1月20日(2022.1.20)
審判番号　不服2023-22287(P2023-22287/J1)
審判請求日　令和5年12月28日(2023.12.28)
(31)優先権主張番号　62/627,207
(32)優先日　平成30年2月7日(2018.2.7)
(33)優先権主張国・地域又は機関
最終頁に続く

(73)特許権者　520296417
クリプト リンクス リミテッド
イスラエル，９７５５７ エルサレム，ウリ・ベン・アリ ４
(74)代理人　100109896
弁理士　森 友宏
(72)発明者　ベレステッキー，ナウム
イスラエル，９７５５０８５ エルサレム，ウリ・ベン・アリ ４／５
(72)発明者　シャケド，エミル
イスラエル，７１７００ モディアン，エメック・アフラ ４２／１
合議体
審判長　須田 勝巳
審判官　脇岡 剛
最終頁に続く

(54)【発明の名称】　署名方法、システム、及び／又はデバイス

(57)【特許請求の範囲】

【請求項１】

物理的な紙文書に署名するための携帯型の署名デバイス（SD）であって、

前記SDは、署名イベントに関する情報を収集し、前記収集された情報から一意なコード（UC）を前記SDにより生成し、前記SDにより前記物理的な紙文書上に前記UCを付与するために構成されており、

前記UCの付与は、前記一意なコード（UC）を前記物理的な紙文書上に物理的に押印することによりなされ、

前記UCの生成は暗号手法を含み、

前記UCは、前記UCに関連付けられたURLに位置するデータ／情報に論理的に関連付けられており、

前記データ／情報は、前記収集された情報、又は、前記収集された情報から生成された情報であり、

前記一意なコード（UC）を形成するための前記収集された情報は、署名される前記文書の少なくとも一部の情報であって、OCR機能により前記紙文書から抽出されたテキストを含んでおり、

前記UCの生成のための前記暗号手法は、前記紙文書から抽出された前記テキストに秘密鍵とともにハッシュ関数を適用して暗号化データを生成し、前記暗号化データを用いて前記UCを生成することを含む、

署名デバイス（SD）。

【請求項２】
前記一意なコード（UC）は、デジタル署名によりさらに保証又は実施される電子的署名である、請求項１の署名デバイス（SD）。
【請求項３】
前記URLは、クラウドベースのウェブページ上に位置する前記データ／情報を指し示している、請求項１又は２の署名デバイス（SD）。
【請求項４】
一意なコード（UC）を形成することを前記SDの正規ユーザ（AU）に対してのみ許可するように構成される、請求項１から３のいずれか一項の署名デバイス（SD）。
【請求項５】
前記文書上に前記一意なコード（UC）の少なくとも一部を付与することは、通常の条件下で目に見えるマーキングを利用する、請求項１から４のいずれか一項の署名デバイス（SD）。
【請求項６】
前記文書上に前記一意なコード（UC）の少なくとも一部を付与することは、通常の条件下で目に見えないマーキングを利用する、請求項１から５のいずれか一項の署名デバイス（SD）。
【請求項７】
物理的な紙文書に署名する方法であって、
携帯型の署名デバイス（SD）を用意するステップと、
署名がなされる物理的な紙文書を用意するステップと、
署名イベントに関する情報を収集するステップと、
前記SDを用いて一意なコード（UC）を生成し、前記UCを物理的に押印することにより前記紙文書上に前記UCを付与するステップと
を有し、
前記UCの生成は、
暗号手法を含み、
前記UCに論理的に関連付けられたデータ／情報が位置しているURLを形成し、
前記データ／情報は、前記収集された情報、又は、前記収集された情報から生成された情報であり、
前記一意なコード（UC）は、前記収集された情報の少なくとも一部からなる、さらに／あるいは、前記収集された情報の少なくとも一部を含み、前記収集された情報は、GPS位置情報、WIFI情報、WIFI位置情報、キャリア情報、キャリア位置情報、IMEI、前記SDの正規ユーザ（AU）の電子メール及び／又は前記AUに関連付けられたデバイスの電子メールのうち少なくとも１つであり、
前記収集された情報は、OCR機能により前記紙文書から抽出されたテキストを含み、
前記UCの生成のための前記暗号手法は、前記紙文書から抽出された前記テキストに秘密鍵とともにハッシュ関数を適用して暗号化データを生成し、前記暗号化データを用いて前記UCを生成することを含み、
前記SDが位置している場所とは離れた場所にいる前記SDの前記AUによる遠隔署名処理を行うように構成され、
前記遠隔署名処理は、
生体認証により前記正規ユーザ（AU）を認証することと、
前記遠隔署名処理は、署名される前記紙文書の少なくとも１つのイメージを前記AUに送信することと
を含む、
方法。
【請求項８】
前記一意なコード（UC）を付与することは、前記SDの正規ユーザ（AU）によってのみ行われる、請求項７の方法。

【請求項９】
前記収集された情報は、前記署名デバイス（SD）により、前記SDに含まれるマイクロプロセッサ及び／又はメモリに格納される、請求項７又は８の方法。
【請求項１０】
前記一意なコード（UC）は、署名される前記文書の少なくとも一部からなる情報を含む、請求項７から９のいずれか一項の方法。
【請求項１１】
前記署名デバイス（SD）は、異なる署名イベント（EV）において使用されるように構成され、それぞれの署名イベント（EV）において、前記SDは、１以上の一意なコード（UC）を形成可能であり、あるEVにおけるすべての一意なコード（UC）は同一である、請求項７から10のいずれか一項の方法。
【請求項１２】
異なる署名イベント（EV）の一意なコード（UC）は、異なっている、請求項11の方法。
【請求項１３】
それぞれの署名イベント（EV）は、１つの前記URLを有している、請求項11又は12の方法。
【請求項１４】
前記データ／情報が前記SD上にローカルに格納されるオフライン動作モードにおいて使用されるように構成される、請求項７から13のいずれか一項の方法。
【請求項１５】
前記SDが外部デバイス／外部手段と通信するオンライン動作モードにおいても使用されるように構成され、前記オフライン動作モード中に前記SDに格納される前記データ／情報の少なくとも一部は、前記オンライン動作モード中に前記外部デバイス／前記外部手段にアップロードされるように構成される、請求項14の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、電子的形態の他のデータに論理的に関連付けられた署名を形成するための署名方法、システム及び／又はデバイスに関するものである。
【背景】
【０００２】
電子的署名は、手書きの署名と同一の法的地位を持つことができる方法により異なる種類の文書が真正なものであることを証明するために、そのような文書に署名するために使用され、電子的形態のデータの典型的な一例であり、これは電子的形態の他のデータに論理的に関連付けられている。
【０００３】
デジタル署名は、例えば文書が真正なものであることを証明し、電子的署名が基礎としている暗号化／復号化技術を用いてその文書の信憑性に対する確信をそのような文書の受取人に与えるためのスキームのさらなる一例である。デジタル署名は、電子的署名を行うために使用され得るが、すべての電子的署名がデジタル署名を用いているというわけではない。
【０００４】
文書及び署名を捏造し、偽造文書を作成したり、既存の文書を改変したり、あるいは未認証の署名を作成したりするための方法がいくつか知られている。紙の文書のような文書に署名する際には、例えば、本物の署名の上に偽物の文書を挿入したり、あるいは、法的契約書などのような文書に単にコピーした署名を貼り付けたりすることによる不正行為がなされやすい。この種の不正行為により、例えば、紙に署名する際に署名の上には何も記載されておらず、あるいは、例えば、署名の上には元々別の文が記載されていたが、それが消去されるか削除されるなどして、不正な文書に本物の署名がある場合には、その不正

な文書が真正なものであると考えられることがある。
【０００５】
米国特許出願公開第20060265590号は、デジタル署名の物理的表現又はハードコピー文書又は対象物に添付する公開鍵の物理的表現としてのハードコピー真正文書について述べている。この方法は、デジタル署名の物理的表現をハードコピー文書に添付し、これを電子的デジタル署名に変換することを含んでいる。この電子的デジタル署名は、公開鍵と比較され、ハードコピー文書が真正なものであるかが証明される。
【概要】
【０００６】
以下の実施形態及びその態様は、例示的で説明的なシステム、ツール及び方法に関連して述べられ、図示されるものであって、範囲を限定することを意図しているものではない。
【０００７】
本発明の少なくともある態様は、例えばユニフォームリソースロケータリンク（URL）を介してサーバに対するアクセスを付与することに関連する。そのようなサーバにおいてデータを格納してもよく、データは、本発明の少なくともある署名デバイス（SD）の実施形態及び／又は本発明の署名方法により署名された文書に論理的に関連付けられている。
【０００８】
ある実施形態においては、文書の署名は、おそらくデジタル署名によりさらに保証又は実施される電子的署名の形態における一意なコード（UC）を生成し得る署名デバイス（SD）、おそらく携帯型SDを用いることにより構成され得る。本発明の少なくともある実施形態による一意なコード（UC）は、文書、おそらく紙の文書上に付与され得る。上述したURLに格納及び／又はアップロードされたデータは、一意なコード（UC）に論理的に関連付けられ得る。
【０００９】
ある場合においては、署名デバイス（SD）を介して文書に割り当てられたUCが分析された後に、そのようなURLが形成され得る。UCに関連付けられた格納データを閲覧するために、ユーザにURLが提供され得る。一実施形態においては、URLは、クラウドベースのウェブページ上に位置する文書及び／又は情報を指し示していてもよい。
【００１０】
URLにおけるデータ／情報へのアクセスは、場合によっては、ログインアクセス許可を要求するものであってもよいが、場合によっては、そのようなデータは公開されていると考えてもよく、情報の少なくとも一部が公開されたものと考えてもよい。拘束力のない一例においては、公開される情報は、署名者の名前、日付、場所、署名者の電子メール、電話（及びこれらに類似するもの）を含み得る。一例においては、ある情報、例えば署名者の電話番号、個人ID、署名された文書自体（及びこれらに類似するもの）は、秘密のままにしてよい。ある場合においては、一部の情報、例えば署名行為が行われた職場の部署、会社内の正当な署名者の役職、職場の場所（及びこれらに類似するもの）をユーザ制限のあるものとしてもよい。
【００１１】
ある場合においては、制限のある文書／情報を指し示しているURLは、ログイン／サインインを要求してもよい。ユーザがアクセスを取得した後に、「署名された」文書に関連する少なくとも一部の情報が明らかにされてもよい。明らかにされる情報は、データにアクセスしているユーザに関連するものであってもよく、例えばその人の電子メール（又はこれに類似するもの）のような特徴的な詳細により決定してもよい。
【００１２】
本発明の一実施形態においては、署名デバイス（SD）を介して一意なコード（UC）を付与することは、概して、文書に適用されるスタンプ動作及び／又はエンコード動作によるものであり得る。
【００１３】
少なくともある署名デバイス（SD）の実施形態は、通常の条件（例えば、日中の直接的

な日光及び間接的な日光の組み合わせを含む通常の「自然光」の条件）下で「目に見える」一意なコード（UC）を形成するように構成されていてもよい。例えば、そのような目に見えるUCは、文書上に一意なコード（UC）を付与するための着色液体及び／又は糊（例えばインク）を用いて形成してもよい。

【００１４】

少なくともある署名デバイス（SD）の実施形態は、通常の条件（例えば、通常の「自然光」の条件）下で「目に見えない」一意なコード（UC）を形成するように構成されていてもよい。例えば、そのような「目に見えない」UCは、例えばUCを形成するための蛍光物質を用いることによる発光を用いて形成してもよい。

【００１５】

ある実施形態においては、さらにSDにより署名されたUCの改竄を回避して、偽造文書の形成を防止（又はその可能性を低減）すべく、一意なコード（UC）を形成するために「目に見えない」マーキングを「目に見える」マーキングと組み合わせて用いてもよい。

【００１６】

「目に見えない」マーキングと「目に見える」マーキングとのそのような組み合わせは、より複雑な認証及び追跡のために署名された例えば紙の文書に「目に見えない」永続的なタグを用いてマーキングするために、ドーピング（すなわち「目に見える」タイプの物質と一緒に「目に見えない」タイプの物質を意図的に導入すること）や「目に見えない」タイプ（例えば蛍光タイプ）の元素や粒子を選択的に分布させることにより実現することができる。

【００１７】

ある場合においては、一意なコード（UC）を形成するための「目に見えない」マーキングと「目に見える」マーキングとの組み合わせは、「目に見えない」マーキングが「目に見える」マーキング中に懸濁していると考えられるコロイドの形態であるものとして定義され得る。そのような懸濁物質は、流体又は液体（ここでは「目に見える」マーキングを形成する物質）に固体又は液体の微粒子（ここでは「目に見えない」マーキングを形成する粒子）を分散させたものとして定義され得る。ある場合においては、そのような組み合わせは、「目に見えない」マーキングを形成する粒子を浮力により支持することによりさらに定義され得る。

【００１８】

少なくともあるSDの実施形態を介してUCを付与することは、認証プロセス、おそらく署名デバイス（SD）を操作する者がSDの正規ユーザ（AU）であると決定するための認証の初期段階を行うことを必要とし得る。

【００１９】

そのような認証は、生体認証を介して、例えばSDを操作する者の指紋認証を介して行われ得る。この認証は、署名デバイス（SD）の実施形態に統合され得るローカルスキャナ、例えば指紋認証の場合は指紋スキャナを介して、あるいは、SDに近接したデバイス、例えば有線又は（Bluetoothなどの）無線接続を介してSDとおそらく通信する携帯デバイスを介して行ってもよい。

【００２０】

おそらく、署名デバイス（SD）を操作するユーザの認証は、正規ユーザ（AU）に英数字からなるコードのようなパスワードの入力を要求することにより行ってもよい。少なくともある実施形態においては、正規ユーザ（AU）は、最初、生体認証を行い、これが失敗した場合に、考えられる１以上の追加の生体認証を行うことを要求され得る。ある場合においては、そのような最初の生体認証が失敗すると、ユーザは、英数字からなるコードを入力するなど、他の手段／方法により追加の認証の試行を行うように指示されてもよい。本発明の様々な実施形態の生体認証方法は、音声分析、声帯又は虹彩分析、顔分析（など）の少なくとも１つを含み得る。

【００２１】

ある実施形態においては、署名デバイス（SD）内で、光センサ、容量センサ、熱センサ

、圧力センサ、超音波及びRFセンサなどの様々な生体（例えば指紋）センサを用いてもよい。ある実施形態においては、所定の時点における特定の文書に署名するユーザの生理的又は精神的状態を分析するために、おそらく生体（例えば指紋）検出デバイスに組み込まれるバイオフィードバック（皮膚電気抵抗、サーモメータ、心拍数）を認証方法として用いてもよい。

【００２２】

場合によっては、正規ユーザ（AU）は、AUに関連付けられている署名デバイス（SD）が実際に位置している場所とは異なる場所にいてもよい。そのような異なる位置は、物理的に異なる位置及び／又は考えられる遠隔の異なる領域、例えば異なる職場、街、国などであってもよい。そのような場合には、遠隔認証処理を最初に実行し、実際の「署名」（すなわち物理的にUCを付与すること）は、正規ユーザ（AU）を補助する他の者により実行されてもよい。

【００２３】

そのような遠隔「署名」プロセスは、「署名された」文書に関連付けられているデータが位置している／アップロードされているURLの形成に先立って遠隔的に付与されたUCが真正なものであること及び／又は正当なものであることを確認するために、（UCにより）「署名された」文書のスキャン又は画像をAUに提供することを含み得る。

【００２４】

ある場合においては、本発明の少なくともある実施形態による署名方法は、最初のステップにおいて情報の収集を含み得る。この情報は、後のステップにおいて、一意なコード（UC）を生成するために使用され得る。そのような収集された情報は、ユーザのID、日付、場所、及び例えば、署名デバイス（SD）を使用している正規ユーザ（AU）の携帯デバイスからおそらく集められた様々なビット情報を含み得る。

【００２５】

そのような収集されると考えられる情報は、（例えばBluetooth接続を介して）無線で取得されてもよく、GPS位置情報、WIFI情報、WIFI位置情報、キャリア情報、キャリア位置情報、IMEI、電子メール（及びこれらに類似するもの）を含み得る。一実施形態においては、署名デバイス（SD）により情報が収集され、さらに／あるいは、例えばSDに含まれるマイクロプロセッサ及び／又はメモリなどの手段により保存されてもよい。

【００２６】

一実施形態においては、一意なコード（UC）（例えば電子的に署名されたUC）の生成は、UCを生成するために収集された情報のすべて、そのほとんど、あるいはその少なくとも一部をまるで「混ぜる」又は「利用する」ような機能を適用することを含んでいてもよい。そのような一意なコード（UC）は、電子型のUCであってもよく、例えば署名された文書（又はその一部）の画像を含むようにコンパイルされている場合にはデジタル型のUCであることも考えられる。また、そのような一意なコードは、UCに関連付けられているデータが位置している又はアップロードされている場所に対するURLリンクを含むように構成され得る。一意なコード（UC）は、場合によっては、UCが形成される元となった情報の少なくとも一部から形成されたURLにリンクされていてもよい。また、URLは、ランダムに形成されるものであってもよい。

【００２７】

拘束力のない一例においては、一意なコード（UC）は、現在の日付を表す数値を積算し（例えば、2017年10月９日という日付を表す数値091017に積算関数を適用し）、その後、例えば、その結果にユーザID（など）で乗算して、得られた結果を表す一意なコード（UC）を生成することにより形成してもよい。本発明の少なくともある一意なコード（UC）を形成するために、暗号法及び／又は暗号ハッシュ関数のようなセキュアな情報／通信のための他の手法を用いてもよい。例えば、UCを形成するための手法として、ラビン暗号方式、SHA-256アルゴリズム、SHA-512ハッシュ関数、及びこれに類似するもののうち少なくとも１つを含む手法を用いてもよい。一意なコード（UC）が形成されると、正規ユーザ（AU）が一意なコード（UC）を用いて、署名デバイス（SD）により文書にUCを付

与するいわゆる「署名」イベント（EV）を構成してもよい。

【００２８】

本発明の少なくともある署名方法の実施形態は、類似する一意なコード（UC）を複数回（例えば、スタンプ／印刷／署名により）同一の文書に（例えば、文書のある領域又はあるページに）付与すること又は互いに関連する複数の文書（例えば、類似する法律事項に関連する複数の契約）に付与することなどを含む署名イベント（EV）の実行を含み得る。

【００２９】

おそらく、署名イベント（EV）において複数回使用されるそのような類似するUCは、UCに関連付けられたデータが格納される単一のURLを有していてもよい。また、署名イベント（EV）は、ある一意なコード（UC）を（例えばスタンプにより）１回だけ付与する、例えば単一のページにUCを１回スタンプすることを含み得る。

【００３０】

本発明のある態様においては、１以上の署名イベント（EV）に関する情報は、EVを適用するために使用される署名デバイス（SD）の実施形態に一時的に格納されてもよい。したがって、そのような署名イベント（EV）は、一意なコード（UC）を生成するために集められたデータ／情報をそれぞれ含んでいてもよく、UCは、EVとUCに関連付けられたデータが格納されるURLとにおいて使用されてもよい。

【００３１】

少なくともある実施形態においては、１以上の署名イベント（EV）のデータ／情報は、EVを実行する署名デバイス（SD）が「オフライン」モードのとき、SD上に一時的に格納され得る。その後、署名デバイス（SD）とウェブとの間でセキュアな接続が確立されたときに、そのようなデータ／情報を上記EVに関連付けられたURLにアップロードしてもよい。

【００３２】

接続を確立した時点で（あるいはその少し後に）、（おそらく専用サーバ上の）クラウドにおいてそれぞれの実際のリンクが生成されてもよい。SD上に格納されたEVのそれぞれに対して、URLリンク（例えば、https://lynx.io/W5h67r）が形成され得る。URL／リンクの生成時又は生成後に、このリンクに関連付けられたEVの情報が現在存在しているURLにアップロードされ得る。

【００３３】

一実施形態においては、遠隔「署名」処理は、以下のステップを含み得る。文書が存在する場所にいるユーザが、文書の「署名」するページの画像を遠隔承認／署名のために離れた場所にいる正規ユーザ（AU）に送信する。その後、正規ユーザ（AU）は、文書を検証し、承認する場合には、生体手段（例えば指紋スキャナ）を介して自分自身を認証してもよい。この認証を含むプロセスは、例えば、正規ユーザ（AU）の携帯デバイスのような携帯デバイス上で実行される専用携帯アプリケーションなどの計算手段を介しておそらく実行され得る。

【００３４】

その後、そのような計算手段は、セキュアな通信を介して、ローカルなユーザ及びローカルなユーザが所有する署名デバイス（SD）に対して確認を送信し得る。ここで、一意なコード（UC）及びURLが、これから行うスタンプ処理（例えばEV）のために形成されてもよい。

【００３５】

一実施形態においては、一意なコード（UC）は、マトリクスバーコード、例えばQRコード（とりわけ、ここで述べられている態様はQRコードのみに限られるものではない）のような様々な他の形態で実現され得る。そのようなQRコード型のUCに含まれるメッセージの内容は、例えばe18f415ae8fef102d57e69d6d316d59ef6d30e85のようなハッシュ結果を形成することによりさらにハッシュ化されていてもよい。このハッシュ化された結果を公開鍵とともに通信してデジタル署名を形成してもよい。

【００３６】

メッセージ内容の暗号化は、メッセージ内容にZipイメージ化を適用することを含み得る。メッセージハッシュ値とメッセージのZipイメージ化に加えて、署名者のID、日付、場所、Bluetooth接続された電話からの情報（GPS位置情報、WIFI情報、WIFI一情報、キャリア情報、キャリア位置情報、IMEI、メールアドレス）などの追加の情報を収集してもよい。

【００３７】

一実施形態においては、サーバ上で形成されたURL（例えば、https://lynx.io/W5h67r）のような情報や「メッセージを読むには次のステップに従ってください・・・」のような暗号化されていないメッセージを考慮して、QRコード型の一意なコード（UC）を確立してもよい。

【００３８】

少なくともある実施形態におけるQRエンコード処理は、メッセージとハッシュ関数を考慮してなされる場合がある。例えば、秘密鍵とともにハッシュ結果e18f415ae8fef102d57e69d6d316d59ef6d30e85を考慮して、デジタル署名された一意なコード（UC）を生成してもよい。

【００３９】

一意なコード（UC）により真正なものであるとされたハードコピー文書の場合、OCR機能を適用して文書からテキストと数字を抽出してもよい（より良いOCR結果を得るためにはコンマ、点、及び他の小さな記号は無視され得るが）。OCRが成功し、文字と数字が抽出された（上コンマ又は下コンマ、点、及び他の小さな記号はおそらく除去される）後、秘密鍵とともにハッシュ関数を適用してデジタル型UC署名を生成するなどの次のステップを続けてもよい。

【００４０】

本発明のある実施形態においては、ユーザは、メッセージの手動認証を行ってもよい。これは、詐欺の疑いがあり、自動処理のような他の処理では署名済み文書の真正性に対して要求される確実性が得られない場合に行われ得る。

【００４１】

例えば専用ソフトウェアを使うことによって先の署名済み文書が真正なものである（例えば改竄されていない）ことを確かめたい正規ユーザ（AU）は、「認証」又は「不審」のオプションを選択するように指示され得る。「不審」を選択すると、正規ユーザ（AU）又はAUに関連付けられた者には、「コンマ」やアラビア数字などの追加のような文書の改竄がなされたかもしれないか否かを検査する文書のzipイメージ又はスキャンのような、署名済み文書及び／又はそのUCに関連付けられた内容が提供され得る。とりわけ、「コンマ」などの情報を追加することは、異なるハッシュ値を生成することになるので、認証プロセスにおいてエラーが生じ得る。

【００４２】

QRコード型の一意なコード（UC）の場合、そのようなQRコード中のメッセージがQRコードにzipイメージ化されている場合、zipイメージを抽出して解凍し、そのメッセージを表示してもよい。

【００４３】

ある場合においては、ソフトコピーをウェブ上、例えばEVに関するデータ／情報を格納する専用サーバ上に格納してもよい。例えば、詐欺の疑いがあった場合に、ソフトコピーをEVに関連付けられたURLに格納してもよい。最初に署名した文書がユーザによりあるいは自動で既にそのURLにアップロードされている場合には、以前に署名した文書のソフトコピーに切り替えることが考えられる。

【００４４】

ウェブ上に格納した文書のソフトコピーに関して改竄が疑われる署名済み文書（例えば法的契約書）の認証は、以下のように行うことができる。

【００４５】

考えられる最初のステップにおいては、疑いのある文書のOCRを行い、OCRに基づくハ

ッシュ関数を得てもよい。そして、おそらく自動的に、両方のメッセージのハッシュ（現在疑いのある文書のものとサーバに格納されたソフトコピーのもの）を表示してマッチングしてもよい。比較により、マッチングスコアのパーセンテージを提供して、おそらく不整合／不一致を例えば赤色でハイライトすることにより表示し得る。また、ユーザは、不整合／不一致を１つ１つ確認して、それぞれハイライトされている相違点を無効であると確認又はマークすることを求められ得る。そして、最後に考えられるステップにおいて、認証の概要と結果が表示され得る。

【００４６】

さらなる例においては（おそらく先の例と組み合わせられるか、あるいは独立している）、正当性を確認するために署名から情報を抽出してもよい。最初のステップにおいては、スタンプされた一意なコード（UC）がスキャンされ、認識されて、例えばQRコード型のUCがQRコードスキャナによりスキャンされ得る。一例においては、所定の制限の下でUCに関連付けられた情報にアクセス可能なウェブサーバ／クラウドを指し示すリンクをスキャンから抽出してもよい。

【００４７】

QRコード型のUCのようにより多くの情報がUCにエンコードされる場合、さらなる参照を抽出してもよい。QRコードのようなUCは、ユーザ情報、URL（例えば、https://lynx.io/W5h67r）、暗号化されていないメッセージ（例えば、「メッセージを読むには次のステップに従ってください・・・」）、文書ハッシュ値、zipイメージ化されたメッセージ、公開鍵、デジタル署名（及びこれらに類似するもの）を含み得る。

【００４８】

ある場合においては、署名済み文書の真正性を確認するための方法を２つ以上一度に適用してもよい。

【００４９】

上述した例示的な態様及び実施形態に加えて、図面を参照することにより、また、以下の詳細な説明を検討することにより、さらなる態様及び実施形態が明らかになるであろう。

【図面の簡単な説明】

【００５０】

参照される図面において例示的な実施形態が示されている。本明細書に開示されている実施形態及び図面は、限定的なものではなく、説明的なものであると考えられることが意図されている。しかしながら、本発明は、組織及び動作方法の両方に関して、その目的、特徴、及び効果とともに、添付図面とともに以下の詳細な説明を参照することにより最も理解され得る。

【００５１】

【図１Ａ】図1Aは、本発明の様々な方法により署名される、紙の文書の表紙のような表面上にスタンプ／署名状態で置かれた本発明の署名デバイス（SD）の実施形態を模式的に示すものである。

【００５２】

【図１Ｂ】図1Bは、図1Aの署名デバイスと略同一の署名デバイスであって、表面から取り除かれた署名デバイスの実施形態を模式的に示すものであり、表面に印刷／スタンプされたか、あるいは表面に付着したままの考えられるあるタイプの一意なコード（UC）を示すものである。

【００５３】

【図２Ａ－２Ｂ】図2A及び図2Bは、図１の署名デバイスと略同一の署名デバイス（SD）の実施形態のそれぞれ上方斜視図及び下方斜視図を模式的に示すものである。

【００５４】

【図３】図３は、本発明の方法の実施形態に含まれると考えられるステップを模式的に示すものであり、おそらく図１及び図２の署名デバイスと略同一の署名デバイス（SD）を用い、SDにより付与された一意なコード（UC）に関連付けられたURLの形成を示すものである。

【００５５】
【図４】図４は、本発明の少なくともある実施形態による一意なコードを形成するために行われると考えられる一連の動作を模式的に示すものである。
【００５６】
【図５Ａ－５Ｅ】図5Aから図5Eは、本発明の少なくともある実施形態による一意なコード（UC）及び／又はそのようなUCに関連付けられたデータ又は情報を模式的に示すものである。
【００５７】
【図６】図６は、本発明の方法の実施形態に含まれると考えられるステップ、すなわち本発明の少なくともある署名デバイスの実施形態により行われる署名動作のいわゆる遠隔承認を模式的に示すものである。
【００５８】
【図７Ａ－７Ｄ】図7Aから図7Dは、本発明の様々な実施形態を理解するのに有用なフローチャートを模式的に示すものである。
【００５９】
説明の簡略化と理解を容易にするため、図に示されている要素は、必ずしも縮尺通りに描かれているとは限らないことは理解できよう。例えば、理解を容易にするため、一部の要素の寸法は、他の要素に対して誇張されている場合がある。さらに、適切であると考えられる場合には、同様の要素を示すために参照数字が図中で繰り返されることがある。
【詳細な説明】
【００６０】
まず、本発明の署名デバイス（SD）10の実施形態を示す図1A及び図1Bに注目する。本発明の一態様においては、図示された文書12のような物理的な文書に署名するために署名デバイス（SD）10を用いることができる。ここでは、「ゴム印スタンプ」のような形態の署名デバイス（SD）が、文書に一意なコード（UC）14を形成する／押印するものとして図示されている。
【００６１】
さらに、署名デバイス（SD）10の１つの考えられる実施形態の上方斜視図及び下方斜視図をそれぞれ示している図2A及び図2Bに注目する。この例におけるSD10は、SDを操作しようとするユーザの生体的特徴を検出するように構成された認証装置16、ここでは考えられる生体認証装置を備えている。
【００６２】
この例では、認証装置16は、指紋認証装置であり得る。図示された署名デバイス（SD）を用いて文書に署名を行うことを考えているユーザは、最初の初期ステップにおいて、ユーザとして認識されるために、認証装置16上で認証のために使用される指を置くように指示／要求され得る。他の実施形態（図示せず）においては、認証装置は、声、網膜、虹彩（又はこれに類似するもの）のような他の種類の生体的特徴を特定するように構成されていてもよい。
【００６３】
図示された例においては、署名デバイス（SD）10は、その下部に押印手段140を含んでいるものとして示されてる。この押印手段140は、署名する文書上に一意なコード（UC）14を形成するように構成されている。この例における押印手段140は、複数のマーカ（この例では５つのマーカ）141-145を含んでいる。
【００６４】
この例におけるマーカは、SDが一意なコード（UC）を形成するために使用される際に、マーキング（この例では比較的短い線分のマーキング）を形成するように構成される突起部170に向かって下方に傾斜する形態を有している。一例では、少なくともある署名デバイス（SD）の実施形態は、例えば、この選択的な例においては、インクを浸した後、マーカの突起部にインクを付け、これをSDが押しつけられる面に写してUCを付与することにより、通常の条件（例えば、通常の「自然光」の条件）では「目に見える」タイプのマ

ーキングを形成するように構成されていてもよい。

【００６５】

ある署名デバイス（SD）の実施形態は、「目に見える」タイプのマーキングに代えて、あるいはこれに加えて、通常の条件（例えば、通常の「自然光」の条件）では「目に見えない」タイプのマーキングを形成する一意なコード（UC14又はUC100など）を形成するように構成されていてもよい。そのような「目に見えない」タイプのマーキングは、例えば、蛍光物質を用いることによる発光を用いて形成することができ、「目に見える」タイプのマーキングと組み合わされる場合には、例えばドーピングや選択的分布（あるいはこれに類似するもの）によって「目に見える」タイプのマーキングの内部に配置され得る。「目に見えない」マーキングと「目に見える」マーキングとの組み合わせは、「目に見えない」マーキングが「目に見える」マーキングの全体におそらく懸濁しているようなコロイドの形態として定義され得る。

【００６６】

再び図1Bに注目すると、一意なコード（UC）14における短いマーキング17は、押印手段140の突起部と概して類似する手段により形成し得る。

【００６７】

本発明の様々な実施形態において、少なくともあるSDの実施形態は、ローカルカメラ型スキャナ（図示せず）を備えていてもよい。このスキャナがSDに組み込まれることにより、SDがより自律的になり、スマートフォンのような外部カメラ／スキャナデバイスとは独立したものとなり、安全性の高いものとなり得る。このカメラ／スキャナは、例えば本明細書で議論され得る認証のために、署名の前及び／又は署名の後に文書をスキャンするために使用され得る。

【００６８】

デバイス10のような署名デバイス（SD）は、少なくともある実施形態においては、１以上の正規ユーザ（AU）による操作のために構成され得る。SDを操作しようとするユーザが正規ユーザであることの認証は、図7Aに示される認証プロセス200を含み得る。

【００６９】

初期ステップ201においてなされる、署名デバイス（SD）を操作しているユーザが正規ユーザであるという肯定的な認証によって、SDにより押印される一意なコード（UC）を生成するための次のステップ203において後で使用され得る情報を集めるステップ202が開始され得る。ステップ201で行われる認証は、認証装置16上でユーザが指を置くことによって行われてもよい。

【００７０】

そのような情報には、認証される正規ユーザ（AU）に関連付けられたIDナンバー、日付、場所、及び例えば、認証される正規ユーザ（AU）の携帯端末から集められ得る追加の情報が含まれ得る。

【００７１】

一実施形態においては、ある正規ユーザに使用されている間に、署名デバイス（SD）により押印される一意なコード（UC）を生成する際に、AUについて収集された情報の少なくとも一部を表すUC用の形状／構造を得てもよい。例えば、収集された情報のすべて、又はその大部分、又はその少なくとも一部に対して、UCの形状／構造により表され得る何らかの「スコア」を生じる関数を適用してもよい。

【００７２】

図示されている例では、算出された「スコア」を表す、いわゆる「マーカコンビネーション」を形成するためにマーカ141-145の位置を変更することにより、結果的に得られる一意なコード（UC）の形状／構造がさらなるステップ204において形成され得る。この例では、署名デバイス（SD）は、一意なコード（UC）の必要とされる構造を形成するためにマーカの位置を変更するための１以上の内部アクチュエータ（図示せず）を含み得る。

【００７３】

一意なコード（UC）の生成に加えて、ステップ205においては、UCに関連する情報が

格納され得る一意なURLを形成してもよい。このURLは、署名デバイス（SD）と通信及び／又は協働するサーバによって、あるいは、署名デバイス（SD）自体によって（例えばSD上で作動しているプロセッサによって）割り当てられ得る。

【００７４】

様々な署名デバイス（SD）の実施形態（図示せず）は、異なる機械的形態又は他の形態を有していてもよく、ステップ204において、図1B及び図2Bに示されたものとは異なる形状／形態の一意なコード（UC）を形成するように構成されていてもよい。例えば、少なくともある署名デバイス（SD）の実施形態は、QRコードのような様々なタイプの一意なコード（UC）を形成するように構成され得る。

【００７５】

例えば、本発明の少なくともある実施形態における携帯型署名デバイス（SD）は、例えば署名される文書上に一意なコード（UC）を付与／スタンプするためのコード（QRコードであり得る）生成手段（例えばインクジェットプリンタのような印刷手段）を備えていてもよい。そのようにして署名される面上にUCを付与する際に、まずSDを当該面に配置し、その後、その面に沿って横にSDを引きずってUCを付与してもよい。

【００７６】

少なくともある署名デバイス（SD）の実施形態は、インターネットのような外部環境との通信が存在しないことがある「オフライン」動作用に構成されていてもよい。そのような署名デバイス（SD）の実施形態は、そのような「オフライン」期間中に、１以上の署名動作を行うために使用され得る。それぞれの署名動作は、例えば、それが正規ユーザ（AU）異なること、署名が行われる時点が異なること、署名された文書が異なること（又はこれに類似すること）のうち少なくとも１つに関係する場合には、別個の署名イベント（EV）として特徴付けられ得る。

【００７７】

ある実施形態においては、情報が異なる署名イベント（EV）に関連することが、外部通信が可能になるまで、さらに／あるいは外部通信が再開されるまで、署名デバイス（SD）上に記憶され、サーバ、おそらく署名デバイス（SD）と協働するように構成される専用サーバにアップロードされ得る。

【００７８】

署名デバイス（SD）10からサーバ20、おそらくクラウドサーバへのそのようなアップロード処理プロセスを示す図３に注目する。異なる署名イベント（EV）は専用のURLにおいて記憶され得る。ここでは、専用のURLは、その「オフライン」期間中に実行された後、署名デバイス（SD）上に記憶されたn個の署名イベント（EV）に対してURL(1)から(n)としてマークされる。

【００７９】

少なくともある実施形態の署名デバイス（SD）により押印／スタンプされる一意なコード（UC）を生成する１つの考えられる例を示している図４に注目する。この図の上部から始めて、一意なコード（UC）の形成において考慮される情報を収集する考えられる最初のステップ101が図示されている。

【００８０】

この任意的な例においては、収集される情報には、現在の日付（この例では2017年11月6日）、SDを使用しようとするユーザの個人ID、SDを操作するユーザによっておそらく入力される、行われようとしている署名イベント（EV）を表す数、及び使用されるSDのシリアル番号（及びこれに類似するもの）が含まれる。

【００８１】

次のステップ102において、これらの情報は、入力された情報の値を用いて「出力」34を形成するように構成された「生成器」32に通信で伝達され得る。生成器32は、例えば暗号手法及び／又は暗号ハッシュ関数（及びこれに類似するもの）のような出力34を形成するための安全な情報／通信のための様々な手法を実施し得る。例えば、「生成器」32によって実施され得る手法には、ラビン暗号、SHA-256アルゴリズム、SHA-512ハッシュ

関数（及びこれに類似するもの）のうち少なくとも１つが含まれ得る。一意なコード（UC）の生成のプロセス中に秘密鍵のような鍵を利用して／用いてもよい。

【００８２】

この例における出力34は、ここでは数字と文字を含む複数の「タグ」からなる「メッセージ」を含んでいる。「メッセージ」内に埋め込まれた内容（例えば、「メッセージ」内の「タグ」のグループ及び／又は組み合わせ）は、例えば、行われようとしている署名イベント（EV）（この例ではEV 00013）においてSDによって使用される一意なコード（UC）を決定するために使用され得る。

【００８３】

示された例は、「メッセージ」から複数の数値（この例では５つの値）を形成することを示している。この例では、これらの値はX1からX5として示されている。値X1からX5のそれぞれは、所定の範囲に入るように正規化されていてもよく、この例では必要に応じて「０」から「315」の間の範囲に入るようになっている。出力34の「メッセージ」を値X1からX5に変換することが、両側矢印により「出力」34の右側に示されており、X1からX5のそれぞれの値は、上記所定の範囲内のそれぞれの対応する位置に示されている。

【００８４】

少なくともある実施形態においては、署名デバイス（SD）10が、X1からX5の値に応じてそのマーカ141から145のそれぞれの相対的な位置を設定するように構成されていてもよい。例えば、X1の値によりマーカ141の位置を設定し、X2の値によりマーカ142の位置を設定し、X3の値によりマーカ143の位置を設定し、X4の値によりマーカ144の位置を設定し、X5の値によりマーカ145の位置を設定してもよい。それぞれの位置に到達したマーカは、その後、署名デバイス（SD）による一意なコード（UC）を形成するために署名動作において使用されてもよい。

【００８５】

上述したUCの形成のステップとともに、UC14を得るためのプロセスについての図示した任意的な例は、UCを配布するための本質的内部統制手法が必要とされ得る組織により好適であり得るUCのタイプを表している。拘束力のない一例においては、そのようなUCのタイプは、署名認証の内部基準が強制され得る政府機関（例えば税関）のような組織の場合に好ましいと考えられ得る。

【００８６】

より開放的なUCのタイプは、例えばQRコードタイプのUCを含み得る。図5A及び図5Dに注目すると、そのようなQRコードのタイプの一意なコード（UC）100が、本発明の少なくともある実施形態においてそのようなUCを生成し（図5A及び図5B）、UC内に埋め込まれる情報を読み取る（図5C及び図5D）ために行われ得る一連の考えられるステップとともに述べられる。

【００８７】

図5Aにおいて、「暗号化データ」を形成する第１のステップ1001が示されており、この第１のステップ1001は、この例では、（例えば、正規ユーザの携帯デバイス上で実行されているアプリケーションを用いて）文書の一部の署名された文書の「OCRデータ」を取得し、その後、「秘密鍵」を用いて「暗号化データ」を形成することを含んでいる。ステップ1001は、正規ユーザ（AU）の携帯端末（又はこれに類似するもの）で実行される専用アプリケーション（APP）上で少なくとも部分的に実行され得る。

【００８８】

考えられる第２のステップ1002においては、UC100のようなUC内に埋め込まれるデータの例が示され得る。UC100内に埋め込まれた第１のセットのデータ36は、先のステップで生成された「暗号化データ」をZIPイメージ化することにより形成され得る。この例ではZIPイメージ化された「暗号化メッセージ」を開くために使用され得る「公開鍵」をデータ38としてUC100内に埋め込んでもよい。UC内に埋め込んでもよい情報としてさらに考えられるものは、「メッセージ」と「リンク」である。

【００８９】

「メッセージ」は、例えばUC100内のデータにアクセスする方法を説明するもの（・・・へ行って「APP」をダウンロードなどのようなもの）であってもよい。「リンク」は、UCに関連付けられたデータが格納され得る専用サーバ上の位置に対するものであり得る。ある実施形態においては、ステップ1001及び1002は、署名された文書の少なくとも一部をイメージ化した後に専用APPにより自動的に実行され得る。この結果、署名された文書上に例えば押印されることになるUC（例えばUC100）が出力される。

【００９０】

ある実施形態においては、ステップ1001，1002は、様々な形態で実行され得る。例えば、クラウドベースのアプリケーションにおいて実行してもよく、その後例えば署名のために例えばSDと通信されてもよく、あるいは、UCを押印するように構成されたSD上でローカルにて実行されることも考えられる。

【００９１】

UC100のようなUC内に埋め込まれたデータを読み取るのに考えられるプロセスを示している図5C及び図5Dに注目する。考えられる最初のステップ1003においては、符号化されたデータを取得するためにUC100内に埋め込まれたデータが特定され得る。この例では、このデータは、０と１とを含む２値データとして示されている。この例では、UC100を読み取るために使用されるAPPは、UCの領域40及び42内のデータのようなデータの一部を特定し得る。このデータの一部は、例えば、UCを読み取るための専用APPをダウンロードする場所を説明するメッセージと、UCに関連付けられたデータが格納され得る場所へのリンクのようなものである。

【００９２】

領域38内に埋め込まれた公開鍵の存在も特定され得る。また、例えば領域40内に含まれるテキストが、領域36内に埋め込まれた暗号化データの復号化方法をユーザに教えるものであってもよい。ある実施形態においては、領域42内のデータにおいて提供されるリンクで「ログイン」を行った後にのみ、UC100の読取を補助するための公開鍵へのアクセスが許可されるようにしてもよい。

【００９３】

したがって、一意なコード（UC）100は、異なる領域内に埋め込まれ得る符号化されたデータを異なる領域内に含み得る。図5B及び図5Cに図示される例においては、簡略化のため、そのような異なる領域が別個の隣接する矩形領域であるものとして示されているが、UC100のような一意なコード内に情報を埋め込むことは、UCの点在する部分／領域内（など）のように、UCの全体にわたって行われていてもよい。

【００９４】

少なくともある実施形態によれば、UCに関連するデータ／情報が格納され得る場所へのリンク（URL）は、「自由にアクセス可能」又は「アクセス制限あり」としてカテゴリ分けされていてもよい。図5Eに注目すると、そのようなカテゴリが示されており、いわゆる「自由にアクセス可能」のリンク（URL）は、（この図の左側に示されているように）パスワードなどを必要とすることなく、そこにある情報（おそらくは公開情報）の表示を許可し得る。（この図の右側に示されているような）いわゆる「アクセス制限あり」のリンクは、このリンクに到達したユーザに「エントリ」動作を要求し得る。この「エントリ」動作は、ログイン処理を行い、（そのようなリンクに到達したユーザに対して既存のアカウントがない場合には）アカウントを作成することを含み得る。「エントリ」後、ユーザは、リンク内の情報への完全なアクセス又は部分的なアクセスを得るか、あるいはアクセスが拒否され得る。

【００９５】

さらに図7Bに注目すると、UC100内の情報をデコードする／取得するステップとして考えられるステップを示しているフローチャートが示されている。考えられる最初のステップ301においては、UC100を読み取るために公知のQRコードリーダ又はスキャナを用いることができる。（図５に関連して示されているような）UC100に埋め込まれた情報の少なくとも一部は、公知のQRコードスキャナによって少なくとも読み取ることができ、こ

のためステップ302において明らかにできるように構成され得る。そのような情報は、UC100に関連付けられたデータが格納され得るURLを規定する領域42を含み得る。

【００９６】

公知のスキャナにより読み取ることができ、ステップ303において明らかにできるものとして考えられる追加の情報は、したがって、例えば領域40内に埋め込まれていてもよく、一意なコード（UC）100内に埋め込まれた追加の情報を読み取ることが可能な専用QRコードリーダをダウンロードする場所に関する表示（例えばメッセージ）を含み得る。読み取られない場合には、この情報は、明らかにされないか、理解されないままとなり得る。例えば、メッセージとしては「完全なコードを読み取るには・・・をダウンロード」のようなものが考えられる。先に述べたように、領域40のようなUCの領域は、必ずしも図示された矩形状のものでなくてもよく、UC内の周囲に散在するように広がっていてもよい（あるいはこれに類似するようなものでもよい）。

【００９７】

したがって、領域36は、当初UC100により署名されていた文書（又はその一部）の真正な内容のZIPイメージを含んでいてもよい。また、ある領域においては、文書のハッシュ又は文書の一部のハッシュを埋め込んでもよい。少なくともいくつかの場合において、ZIP及び／又はハッシュは、一意なコード（UC）100を文書に付与する前に、署名する文書をスキャンすることにより形成してもよい。

【００９８】

「オリジナル」の署名済み文書上に一意なコード（UC）の少なくとも一部を形成するために（通常の条件、例えば「自然の光」の条件で）「目に見えない」マーキングが使用されていた実施形態においては、そのような「目に見えない」マーキングを実質的に無視するように（例えば取得しないように）そのような「オリジナル」の文書のスキャンを調整してもよい。これにより、例えば、そのようなマーキングが「オリジナル」の文書の内容に対する障害になる、さらに／あるいは干渉を引き起こすことを避けることが容易になり得る。

【００９９】

ある場合においては、「目に見えない」タイプのマーキング（例えば蛍光インク）である一意なコード（UC）及び／又はそのようなマーキングを含む一意なコード（UC）のスキャンは、UCにおいて使用されたそのような「目に見えない」物質を取得するように構成されたスキャナによって行ってもよい。

【０１００】

ある場合においては、元々「目に見えない」マーキングを含んでいたことが知られているUC付署名済み文書の正当性を確かめたいと考えるユーザ又は者は、「目に見えない」物質が現れるように設計された適切な照明条件下でそのようなUCを目で見て視覚的に検査してもよい。そのような「目に見えない」マーキングがないことは、UCの捏造の可能性及び／又はそのようなUCが付された文書内の内容の捏造の可能性を暗示し得るものとなる。

【０１０１】

ステップ304においてこの文書に対するアクセスを提供するためにオリジナルの署名済み文書のZIPイメージは、領域42内で明らかにされたURLからおそらくダウンロードされる専用QRコードリーダ及び／又は専用アプリケーションを用いて解凍され得る。そのような専用アプリケーションは、携帯端末上で実行されている携帯アプリであり得る。オリジナルの署名済み文書のハッシュもステップ305において専用アプリケーション／リーダによって明らかにしてもよい。

【０１０２】

元々UC100により署名した実際の文書を見たり、その文書にアクセスしたりすることにより、UC100が付された現在の文書の内容と元々署名されたオリジナルの文書とを比較する手段が提供され得る。そのような比較により、その元々の署名から現在の検査までの間で元々署名された文書が変更又は改竄されていないことを証明することが可能となる。

【０１０３】

一実施形態においては、おそらく現在検査されている文書のハッシュとオリジナルの署名済み文書になされたハッシュとの間で比較308を行うために、初期ステップ306において、現在の文書をスキャンし、そのスキャンにOCRを適用し、その後、続くステップ307でOCRされたスキャンにハッシュ関数を適用することにより、オリジナルの署名済み文書と現在検査されている署名済み文書との間で比較を行ってもよい。

【０１０４】

ハッシュが一致しない場合には、現在の文書の信憑性の疑いが生じ得る。例えば、オリジナルの署名済み文書は、合計100万ドルについて言及した法的契約書であり得る。最初に署名された後に文書に対して改竄を行うことは、1000万ドルを示すようにこの合計を変更することを含み得る。したがって、議論された契約書の基礎となるこの金額の変更は、現在の文書のハッシュ値とオリジナルの文書のハッシュ値とを比較することで明らかになる場合がある。

【０１０５】

ある場合においては、UC100の領域のうちの１つに埋め込まれたハッシュは、文書全体にわたって行われることも考えられるが、UC100の領域36に埋め込まれた署名済み文書のZIPイメージは、署名済み文書の一部のみを含んでいてもよい。例えば、署名済み文書は10ページを含んでいてもよく、これらの10ページすべての情報を含むZIPイメージを形成し、標準サイズのQRコードタイプのUCの領域36に埋め込むことは、領域36内にはそのような大容量のZIP圧縮の情報を収容するためのスペースが不十分であるために、現実的ではない場合がある。他方、10ページのハッシュは、実質的に、標準サイズのQRコードの１つの領域内に簡単に配置することができる「１行の」情報となる。

【０１０６】

本発明の少なくともある実施形態の一態様は、ZIPイメージとハッシュにより提供される二重のセキュリティにより、UCにより署名される検査文書の信憑性に対する信頼性を向上させる。例えば、ハッシュだけを用いた場合には、一方で、文書内のある情報を改竄（100万ドルを1000万ドルへ変更するなど）した後、文書の別の部分を変更してオリジナルの改竄されていない文書のハッシュに類似するように見えるハッシュを得る（試行錯誤によることが考えられる）ことにより、文書の詐欺が可能となる可能性が生じ得る。

【０１０７】

（例えば上述したもののように）所定のUCが押印された「オリジナル」の内容とそのような所定のUCが付された「現在」の内容とを一致させようとした後に行い得るステップとして考えられるステップを図示した図7Dに注目する。「オリジナル」の内容と「現在」の内容との間で自動的に比較／認証することにより、例えば、これらの内容が肯定的に一致したり、これらの内容の間で、例えば「オリジナル」の内容のハッシュと「現在」の内容のハッシュとの間で不一致を特定できたりすることにつながる。

【０１０８】

（図7Dの上部に「NO」で示されるように）そのような自動的検証／認証が失敗した場合には、そのような検証を行おうとするユーザは、そのような否定的な結果を引き起こしている不一致を手動で検査するように指示されてもよい。ユーザは、「オリジナル」の内容と認証される「現在」の内容とを有していてもよく、この任意的な例においては、両方の内容を分割したスクリーン上に表示させてもよい。その後、ユーザは、２つの内容の間の不一致を手動で検査するために、内容中の不一致箇所に誘導されてもよい。

【０１０９】

そのような検査中に、ユーザが、ある特定された不一致が（例えば内容に対してなされたOCRにおける誤りのために）間違ったものであり、「偽アラーム」であると判断した場合には、ユーザは、この不一致を訂正／無視する選択をしてもよく、以前に行われた自動認証において失敗を引き起こしたすべての不一致が検査されるまで、（図7Dでマークされた「次」の矩形で示されるように）さらに考えられる不一致に誘導されてもよい。

【０１１０】

すべての不一致が「偽アラーム」であると判明した場合には、そのようなマニュアル検

査は、自動処理中になされた前回の否定的な結果を無視し得る肯定的なマニュアル認証になり得る。他方、マニュアル検証処理が以前に行われた否定的な結果と同じ結果になった場合には、二重の検証（最初の自動検証とその後のマニュアル検証）により、「現在」の検査中の内容が真正なものではないことをより確実に決定することができる。内容の真正な「オリジナル」のコピーは、例えばUCに関連付けられたURLに保存されていてもよい。

【０１１１】

【０１１２】

遠隔署名処理における少なくともある署名デバイス（SD）の実施形態10の使用を模式的に示している図６に注目する。同時に注目される図7Cは、そのような遠隔署名中に行われ得るステップを示したフローチャートを提供するものである。そのような遠隔署名処理においては、正規ユーザ30は、署名デバイス（SD）が実際に位置している場所から離れた場所にいる場合があり、SDによる署名の実行を承認するために遠隔認証及び確認処理が行われ得る。

【０１１３】

考えられる最初のステップ401においては、署名される文書又は文書ページ120の写真又はスキャンが、離れた場所にいる正規ユーザ30に送信され得る。次のステップ402においては、離れた場所にいるユーザは、文書のスキャンされたデータを受信し、おそらく携帯電話のようなデバイス上で実行される専用アプリケーション上でそのデータにアクセスし得る。

【０１１４】

離れた場所にいるユーザは、ステップ403において、その文書を読み、おそらくそのアプリケーションにより実行されている指紋スキャナに自分の指紋を付けることにより遠隔署名を行うために文書の確認を行うことができる。これによって、署名される文書が存在している場所にいるローカルユーザにセキュアな確認404を送ることになり得る。次のステップ405においては、文書120の署名が、署名の承認を離れた場所にいる正規ユーザ30が行うことを補助するローカルユーザによって行われ得る。

【０１１５】

本出願の明細書及び特許請求の範囲においては、「備える」、「含む」、「有する」という動詞及びそれと同語源の語は、それぞれ、動詞の目的語が、その動詞の主語の構成部材、構成要素、要素、又は部品を完全に列挙しているものでは必ずしもないことを示すために使用されている。

【０１１６】

さらに、図面及びこれまでの説明において本発明又は本技術が詳細に図示され、述べられてきたが、そのような図示及び説明は、説明的又は例示的なものであり、非制限的なものであると考えるべきである。したがって、本技術は、開示された実施形態に限定されるものではない。当業者であれば、開示された実施形態の変形例を理解及び実現することができ、図面、本技術、及び添付した特許請求の範囲の検討から、特許請求の範囲に記載された技術を実施することができる。

【０１１７】

特許請求の範囲において、「備え」という語は、他の要素又はステップを排除するものではなく、「a」や「an」といった不定冠詞は、複数形を排除するものではない。単一のプロセッサや他のユニットが、特許請求の範囲において記載された複数の項目の機能を実現することがある。単にある手段が互いに異なる従属請求項に記載されているということは、これらの手段の組み合わせが利点のあるように使用することができないということを示すものではない。

【０１１８】

また、本技術は、用語、特徴、数値又は数値範囲などが「約」、「およそ」、「実質的に」、「概して」、「少なくとも」などの用語に関連して述べられている場合には、その用語、特徴、数値又は数値範囲そのものを包含するものと理解される。換言すれば、「約３」は「３」も含むものとし、「実質的に垂直」は「垂直」も含むものとする。特許請求

の範囲におけるいずれの参照符号もその範囲を限定するものと解釈されるべきではない。

【０１１９】

本実施形態が、ある程度詳細に述べられてきたが、以下に規定される本発明の範囲から逸脱することなく、様々な変更や変形をなすことができることは理解されるべきである。

【図面】

【図１Ａ】

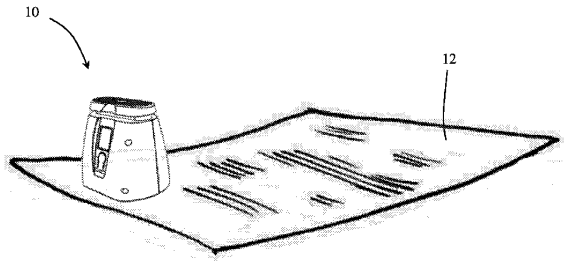



Fig. 1A

【図１Ｂ】

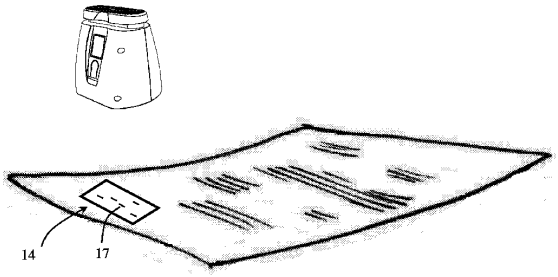



Fig. 1B

【図２Ａ】

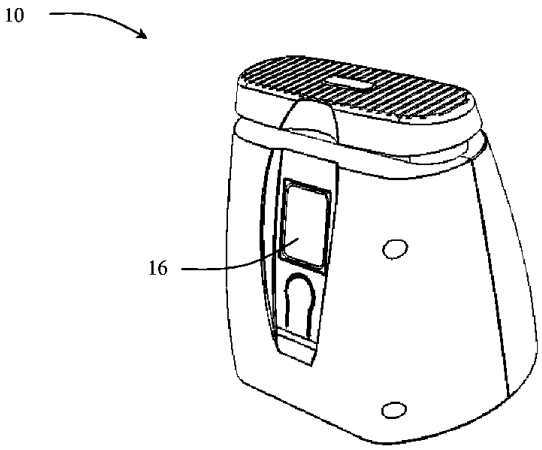



Fig. 2A

【図２Ｂ】

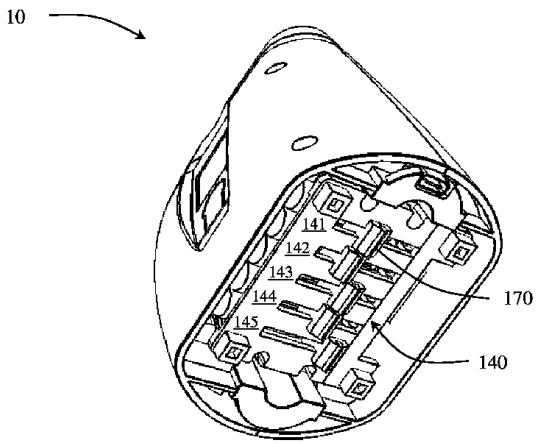



Fig. 2B

【図３】

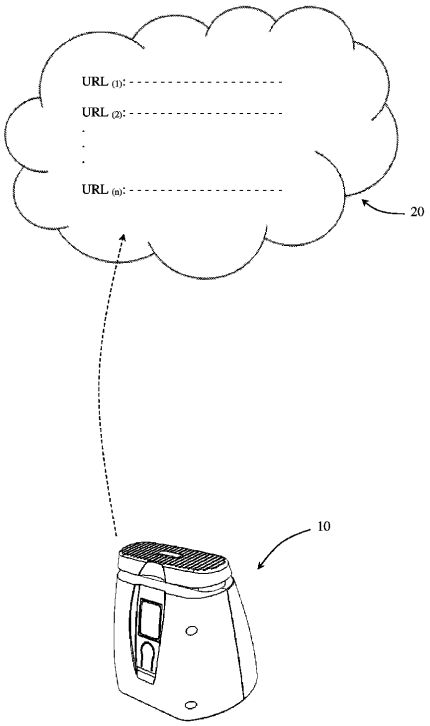
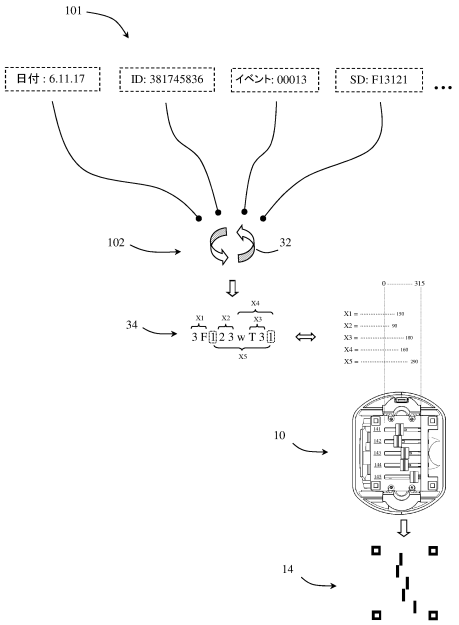
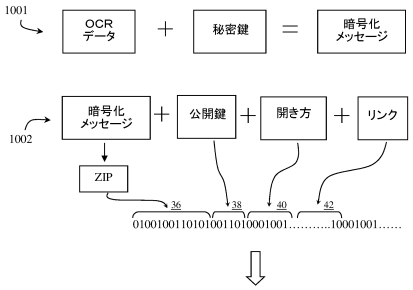



Fig. 3

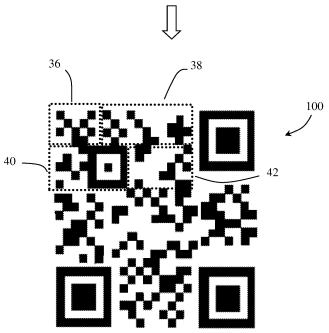
【図４】



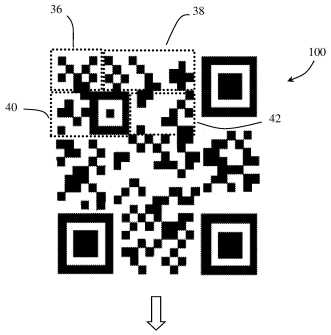

【図５Ａ】



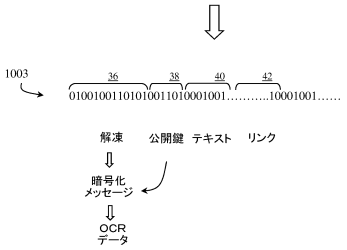

【図５Ｂ】



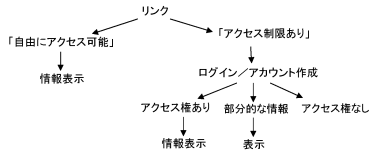
【図５Ｃ】




【図５Ｄ】




【図５Ｅ】




【図６】

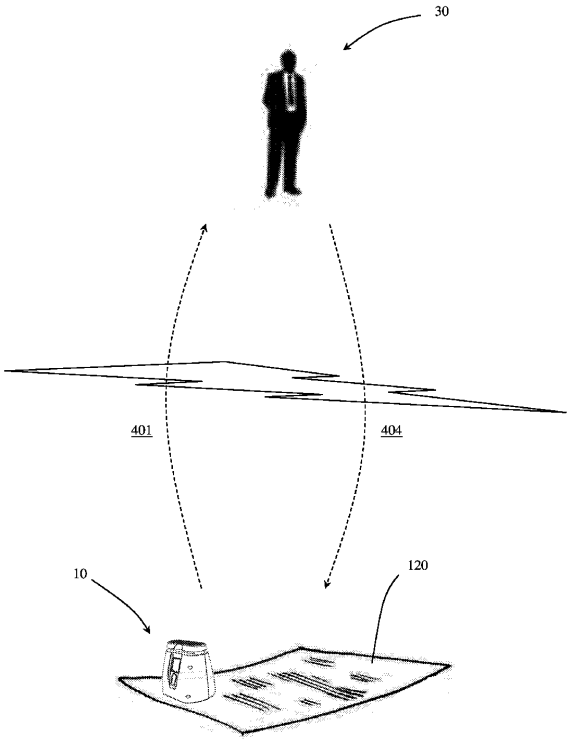
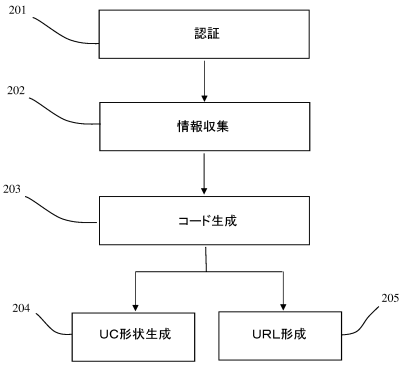
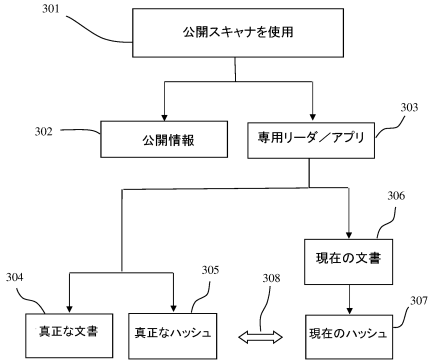



Fig. 6

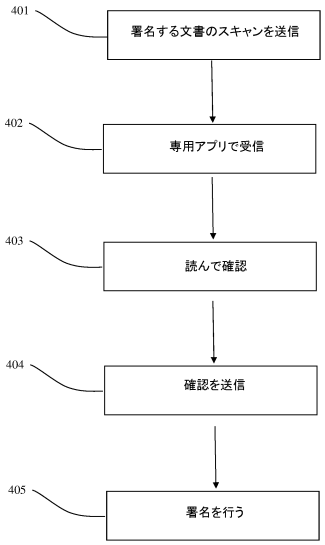
【図７Ａ】



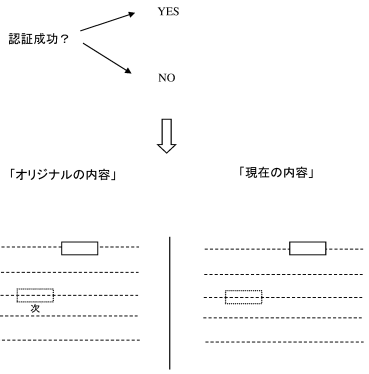

【図７Ｂ】




【図７Ｃ】




【図７Ｄ】



フロントページの続き

米国(US)

審判官　山崎 慎一

(56)参考文献　特開平４－２９４１６７（ＪＰ，Ａ）
特開平２００５－１１９１０９（ＪＰ，Ａ）
特開平２００４－３４８７０６（ＪＰ，Ａ）
特開平２００３－０２９６２９（ＪＰ，Ａ）
特開平２０１２－１２０１０２（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ１／００－５／００
Ｈ０４Ｋ１／００－３／００
Ｈ０４Ｌ９／０６－９／４０