(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2015 年 1 月 8 日(08.01.2015)

WIPO | PCT

(10) 国際公開番号
WO 2015/001637 A1

(51) 国際特許分類:
G06F 21/44 (2013.01) *G09C 1/00* (2006.01)
G06K 7/00 (2006.01)

(21) 国際出願番号: PCT/JP2013/068295

(22) 国際出願日: 2013 年 7 月 3 日(03.07.2013)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: Ａ・Ｔコミュニケーションズ株式会社 **(A.T COMMUNICATIONS CO., LTD.)** [JP/JP]; 〒1100014 東京都台東区北上野一丁目９番１０号 Tokyo (JP).

(72) 発明者: 豊泉　博**(TOYOIZUMI Hiroshi)**; 〒1100014 東京都台東区北上野一丁目９番１０号　Ａ・Ｔコミュニケーションズ株式会社内 Tokyo (JP). 東陽一**(AZUMA Youichi)**; 〒1100014 東京都台東区北上野一丁目９番１０号　Ａ・Ｔコミュニケーションズ株式会社内 Tokyo (JP).

(74) 代理人: 木村　満**(KIMURA Mitsuru)**; 〒1010054 東京都千代田区神田錦町二丁目７番地　協販ビル２階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

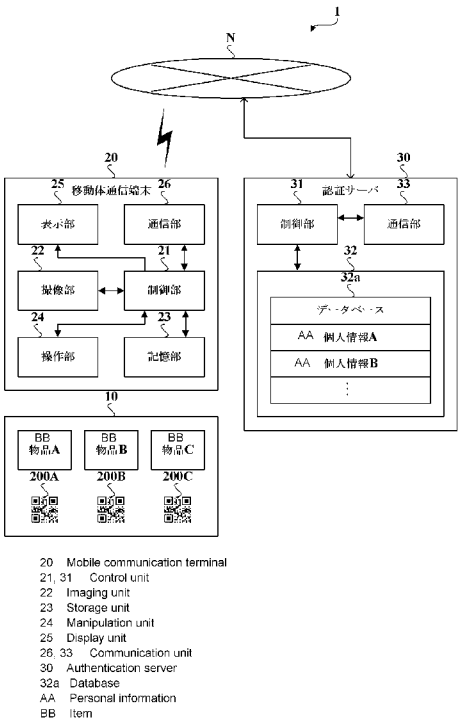
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

WO 2015/001637 A1

(54) Title: AUTHENTICATION SERVER, AUTHENTICATION SYSTEM, AUTHENTICATION METHOD, AND PROGRAM

(54) 発明の名称 : 認証サーバ、認証システム、認証方法、及びプログラム



20 Mobile communication terminal
21, 31 Control unit
22 Imaging unit
23 Storage unit
24 Manipulation unit
25 Display unit
26, 33 Communication unit
30 Authentication server
32a Database
AA Personal information
BB Item

(57) Abstract: In an authentication system (1), a mobile communication terminal (20) transmits, to an authentication server (30), a bit signal including both an imaged bit string, which is obtained by imaging a self-authentication two-dimensional code (200) having authentication information embedded in a correction area thereof, and a number bit string, which indicates the serial number of an authentication application program stored in a storage unit (23), and the authentication server (30) authenticates the user of the mobile communication terminal (20) and the self-authentication two-dimensional code (200). The authentication server (30) then transmits, to the mobile communication terminal (20), predetermined information expressed by the self-authentication two-dimensional code (200), on the condition that the authentication of the user and the self-authentication two-dimensional code (200) is successful. This enables the mobile communication terminal (20) to obtain the predetermined information expressed by the self-authentication two-dimensional code (200).

(57) 要約:　認証システム１では、移動体通信端末２０が、訂正領域に認証情報が埋め込まれた自己認証型二次元コード２００を撮像して得られた撮像ビット列と、記憶部２３に記憶されている認証アプリケーションプログラムにシリアル番号を示す番号ビット列と、を含むビット信号を認証サーバ３０に送信し、認証サーバ３０が、移動体通信端末２０の利用者及び自己認証型二次元コード２００の認証を行う。そして、認証サーバ３０は、利用者及び自己認証型二次元コード２００の認証に成功したことを条件に、自己認証型二次元コード２００が表現する所定の情報を移動体通信端末２０に送信する。これにより、移動体通信端末２０は、自己認証型二次元コード２００が表現する所定の情報を取得することができる。

明　細　書

発明の名称 ：

認証サーバ、認証システム、認証方法、及びプログラム

技術分野

[0001] 本発明は、認証サーバ、認証システム、認証方法、及びプログラム、特に二次元コードの偽造を検出できる認証サーバ、認証システム、認証方法、及びプログラムに関する。

背景技術

[0002] 所定の情報を容易に取得するためのものとして、ＱＲ（Quick Response）コード（登録商標）等の二次元コードが様々な分野で利用されている。特に、携帯電話やスマートフォン等の移動体通信端末を使用する消費者等に対して、企業の広告が掲載されたウェブサイト等、所望のウェブサイトへ誘導する手段として、例えば、下記特許文献１に開示される情報配信システムが知られている。なお、本明細書中に特許文献１の明細書、特許請求の範囲、図面全体を参考として取り込むものとする。

先行技術文献

特許文献

[0003] 特許文献1：特開２００８－２３４５３０号公報

発明の概要

発明が解決しようとする課題

[0004] このシステムでは、対象のウェブサイトのＵＲＬ（Uniform Resource Locator）をコード化した二次元コードを移動体通信端末で読み取ることでＵＲＬを取得でき、このような方法は広く普及している。これに伴い、各移動体通信端末では、二次元コードを光学的に読み取るためのプログラム（アプリケーション）が予めインストールされて構成されるかインターネット等を介してインストール可能に構成されており、誰でもが二次元コードを読取可能な読取装置を所持し得る環境となっている。

[0005] ところで、二次元コードを読み取ることで取得したＵＲＬが不正に改ざん等されている場合、このＵＲＬが安全であるか否かを確認する方法がないと、所望のウェブサイトと異なるウェブサイトに接続されてしまう。この場合、ウィルスやマルウェアが仕込まれた悪意のあるウェブサイト等に接続してしまうと、その移動体通信端末がウィルスやマルウェア感染してしまうといった被害が発生するという問題がある。

[0006] このような問題は、ＵＲＬに限らず、情報が不正に改ざん等された二次元コードを読み取る場合、すなわち、二次元コードに関する不正がある場合には、その不正を確認する方法がないと、不正な二次元コードを読み取ったことに起因する被害が発生するという問題がある。

[0007] 本発明は、上記の課題を解決するためになされたものであり、二次元コードの偽造を検出できる認証サーバ、認証システム、認証方法、及びプログラムを提供することを目的とする。

課題を解決するための手段

[0008] 上記目的を達成するため、本発明の第１の観点に係る認証サーバは、

所定の情報をセルの分布パターンによって表現する情報領域と、誤りを訂正するための訂正情報をセルの分布パターンによって表現する訂正領域と、を備え、該訂正領域の一部が、該一部から生成された第１訂正ビット列と該訂正領域のうち該一部とは異なる部分から生成された第２訂正ビット列との排他的論理和に置き換えられた二次元コードを撮像してビット信号を生成する通信端末とネットワークを介して接続され、

前記通信端末から前記ネットワークを介して送信される前記ビット信号を受信するビット信号受信手段と、

前記ビット信号受信手段によって受信した前記ビット信号をデコードして、前記所定の情報と前記訂正情報とを取得するデコード手段と、

前記デコード手段によって取得した前記訂正情報を用いて、前記第１訂正ビット列と前記第２訂正ビット列との排他的論理和を誤りとして検出する誤り検出手段と、

前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手段によって検出した誤りとの排他的論理和が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否か判別することにより、前記二次元コードの認証を行う二次元コード認証手段と、

前記二次元コード認証手段によって両者が合致するとの認証結果が得られた場合、前記デコード手段によって取得した前記所定の情報を前記ネットワークを介して前記通信端末に送信する情報送信手段と、

を備えることを特徴とする。

[0009] 上記の認証サーバにおいて、

前記ビット信号受信手段は、前記訂正領域の一部が、前記第１訂正ビット列と前記第２訂正ビット列を暗号化して得られた暗号ビット列との排他的論理和に置き換えられた前記二次元コードの前記ビット信号を受信し、

前記二次元コード認証手段は、前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手段によって検出した誤りとの排他的論理和を前記暗号化に対応する方式で復号化して得られた復号ビット列が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否かを判別することにより、前記二次元コードの認証を行う、

ようにしてもよい。

[0010] 上記の認証サーバにおいて、

前記ビット信号受信手段は、前記訂正領域の一部が、前記第１訂正ビット列と前記第２訂正ビット列を非対称暗号化方式で暗号化して得られた暗号ビット列との排他的論理和に置き換えられた前記二次元コードの前記ビット信号を受信し、

前記二次元コード認証手段は、前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手段によって検出した誤りとの排他的論理和を前記非対称暗号化方式に対応する方式で復号化して得られた復号ビット列が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否かを判別することにより、前記二次元コードの認証を行う、

ようにしてもよい。

[0011] 上記の認証サーバにおいて、

前記ビット信号受信手段は、前記訂正領域の一部が、前記第１訂正ビット列と前記第２訂正ビット列を楕円曲線暗号方式で暗号化して得られた暗号ビット列との排他的論理和に置き換えられた前記二次元コードの前記ビット信号を受信し、

前記二次元コード認証手段は、前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手段によって検出した誤りとの排他的論理和を前記楕円曲線暗号方式に対応する方式で復号化して得られた復号ビット列が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否かを判別することにより、前記二次元コードの認証を行う、

ようにしてもよい。

[0012] 上記の認証サーバにおいて、

前記通信端末の利用者を特定可能な識別情報を登録する識別情報登録手段と、

前記識別情報登録手段に、前記通信端末から前記ビット信号に含めて送信される前記識別情報と合致するものが登録されているか否かを判別することにより、前記利用者の認証を行う利用者認証手段と、

をさらに備え、

前記情報送信手段は、前記二次元コード認証手段によって両者が合致するとの認証結果が得られるとともに、前記利用者認証手段によって識別情報が登録されているとの認証結果が得られる場合、前記デコード手段によって取得した前記所定の情報を前記ネットワークを介して前記通信端末に送信する、

ようにしてもよい。

[0013] 上記目的を達成するため、本発明の第２の観点に係る認証システムは、

上記の認証サーバと、該認証サーバと前記ネットワークを介して接続された前記通信端末と、を備え、

前記通信端末は、

前記二次元コードを撮像して前記ビット信号を生成するビット信号生成手段と、

前記ビット信号生成手段によって生成した前記ビット信号を前記ネットワークを介して前記認証サーバに送信するビット信号送信手段と、

前記情報送信手段によって送信された前記所定の情報を受信することにより、前記二次元コードが表現する該所定の情報を取得する情報受信手段と、

を備えることを特徴とする。

[0014] 上記目的を達成するため、本発明の第３の観点に係る認証方法は、

所定の情報をセルの分布パターンによって表現する情報領域と、誤りを訂正するための訂正情報をセルの分布パターンによって表現する訂正領域と、を備え、該訂正領域の一部が、該一部から生成された第１訂正ビット列と該訂正領域のうち該一部とは異なる部分から生成された第２訂正ビット列との排他的論理和に置き換えられた二次元コードを撮像してビット信号を生成する通信端末とネットワークを介して接続された認証サーバによる認証方法であって、

前記通信端末から前記ネットワークを介して送信される前記ビット信号を受信するビット信号受信ステップと、

前記ビット信号受信ステップによって受信した前記ビット信号をデコードして、前記所定の情報と前記訂正情報とを取得するデコードステップと、

前記デコードステップによって取得した前記訂正情報を用いて、前記第１訂正ビット列と前記第２訂正ビット列との排他的論理和を誤りとして検出する誤り検出ステップと、

前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出ステップによって検出した誤りとの排他的論理和が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否か判別することにより、前記二次元コードの認証を行う二次元コード認証ステップと、

前記二次元コード認証ステップによって両者が合致するとの認証結果が得

られた場合、前記デコードステップによって取得した前記所定の情報を前記ネットワークを介して前記通信端末に送信する情報送信ステップと、

を備えることを特徴とする。

[0015] 上記目的を達成するため、本発明の第４の観点に係るプログラムは、

所定の情報をセルの分布パターンによって表現する情報領域と、誤りを訂正するための訂正情報をセルの分布パターンによって表現する訂正領域と、を備え、該訂正領域の一部が、該一部から生成された第１訂正ビット列と該訂正領域のうち該一部とは異なる部分から生成された第２訂正ビット列との排他的論理和に置き換えられた二次元コードを撮像してビット信号を生成する通信端末とネットワークを介して接続された認証サーバのコンピュータに、

前記通信端末から前記ネットワークを介して送信される前記ビット信号を受信するビット信号受信手順と、

前記ビット信号受信手順によって受信した前記ビット信号をデコードして、前記所定の情報と前記訂正情報とを取得するデコード手順と、

前記デコード手順によって取得した前記訂正情報を用いて、前記第１訂正ビット列と前記第２訂正ビット列との排他的論理和を誤りとして検出する誤り検出手順と、

前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手順によって検出した誤りとの排他的論理和が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否か判別することにより、前記二次元コードの認証を行う二次元コード認証手順と、

前記二次元コード認証手順によって両者が合致するとの認証結果が得られた場合、前記デコード手順によって取得した前記所定の情報を前記ネットワークを介して前記通信端末に送信する情報送信手順と、

を実行させる。

発明の効果

[0016] 本発明によれば、二次元コードの偽造を検出できる認証サーバ、認証シス

テム、認証方法、及びプログラムを提供することができる。

図面の簡単な説明

[0017] [図1]認証システムの構成例を示すブロック図である。

[図2]二次元コードの構成例を示す図である。

[図3]認証情報の埋込手順を説明するための模式図である。

[図4]登録処理の詳細を示すフローチャートである。

[図5]認証処理の詳細を示すフローチャートである。

[図6]認証処理の詳細を示すフローチャートである。

発明を実施するための形態

[0018] 以下、本発明の実施形態に係る認証システムについて図を参照して説明する。

[0019] 図１は、実施形態に係る認証システムの構成例を示す図である。認証システム１は、図１に示すように、仮想自動販売機１０と、移動体通信端末２０と、認証サーバ３０と、を備えている。

[0020] 仮想自動販売機１０は、例えばポスタや内照式パネル等から構成され、物品を特定可能な物品情報（図１に示す例では物品Ａ、物品Ｂ、及び物品Ｃなど）と、埋込対象の二次元コード１００に認証情報を埋め込んだ自己認証型二次元コード２００（図１に示す例では自己認証型二次元コード２００Ａ、２００Ｂ，及び２００Ｃ）と、を対応付けて表示する。

[0021] なお、仮想自動販売機１０は、物品情報と自己認証型二次元コード２００とを対応付けて表示可能なものであれば任意であり、例えば紙媒体、金属、プラスティック、ビニル、ゴム、布等から構成されるものであってもよい。具体的に、仮想自動販売機１０が紙媒体から構成されるポスタである場合には、物品情報と自己認証型二次元コード２００とを紙媒体上に印刷するようにすればよい。また、仮想自動販売機１０が布製のものである場合には、刺繍などによって物品情報と自己認証型二次元コード２００とを表示するようにすればよい。仮想自動販売機１０が金属製やプラスティック製のものである場合には、その表面をプレスして凹凸或いは空孔などを形成することによ

り、物品情報と自己認証型二次元コード２００とを表示するようにすればよい。

[0022] 本実施形態において、自己認証型二次元コード２００Ａ、２００Ｂ，及び２００Ｃは、それぞれ物品Ａ、物品Ｂ、及び物品Ｃの購入サイトのＵＲＬ（Uniform Resource Locator）を表現する。

[0023] 図２は、本実施の形態における埋込対象の二次元コードの構成例を示す図である。

[0024] 二次元コード１００は、いわゆるＱＲ（Quick Response）コード（登録商標、以下同様）の規格（ＪＩＳ　Ｘ　０５１０）を満たすものであって、図２に示すように、３つの位置決め用シンボル１０４Ａ，１０４Ｂ，１０４Ｃ、情報コード記録領域１０６、タイミングセル１０８及びフォーマットコード１０９などを備えている。

[0025] ３つの位置決め用シンボル１０４Ａ，１０４Ｂ，１０４Ｃは、矩形状をなす二次元コード１００の４つの頂点のうち、３つの頂点にそれぞれ配置されている。

[0026] タイミングセル１０８は、位置決め用シンボル１０４Ａ，１０４Ｂ，１０４Ｃ間に、白と黒とが交互に組み合わせられた直線状の基準パターンとして配置されている。このタイミングセル１０８は、各データセル位置の指標として用いられる。

[0027] フォーマットコード１０９は、位置決め用シンボル１０４Ａの近傍に配置されており、情報コード記録領域１０６内に記録された情報コードのフォーマットについて、予め規定されたバージョン情報を示すものである。二次元コード（ＱＲコード（登録商標））の規格におけるバージョン情報は、１～４０のバージョンと、各バージョンについて４つの誤り訂正レベルＬ，Ｍ，Ｑ，Ｈ（ＬからＨへと順に高くなる）と、の組み合わせで構成されている。

[0028] バージョン１～４０は、主に、８ビットに対応した８つのセルで構成されるシンボルの総数に対応している。また、誤り訂正レベル（Ｌ，Ｍ，Ｑ，Ｈ）は、全シンボルのうち読取れないシンボルを許容する割合の高さ、すなわ

ち許容欠損率の高さに対応している。それぞれのレベルの許容欠損率は、誤り訂正レベルＨが約３０％、誤り訂正レベルＱが約２５％、誤り訂正レベルＭが約１５％、誤り訂正レベルＬが約７％である。本実施の形態では、シンボルの総数が１３４のバージョン５で誤り訂正レベルＨの二次元コード１００を用いており、そのバージョン情報は、「５－Ｈ」と表される。なお、本発明はこれに限定されるものではなく、二次元コードのバージョン及び誤り訂正レベルは任意であり、バージョン１～４０のいずれであってもよく、また誤り訂正レベルはＬ，Ｍ，Ｑ，Ｈのいずれであってもよい。

[0029] 情報コード記録領域１０６は、光学的特性の異なる２種類のセル（白黒パターンを省略）から構成されており、情報コード（情報領域）Ｃｄとこれに対応するＲＳ（リード・ソロモン）コード（訂正領域）Ｃｅと、のコード対を含んでいる。情報コードＣｄは、所定の情報をコード化したもので、情報コードＣｄに含まれるセルの分布パターン（セルパターン）によって、所定の情報を表現している。また、ＲＳコードＣｅは、所定の情報をＲＳ（リード・ソロモン）を用いて符号化した訂正用情報をコード化したもので、ＲＳコードに含まれるセルパターンによって、誤りを訂正するための訂正用情報を表現している。

[0030] 本実施の形態では、最適例としてＲＳ符号を用いて符号化するものを例示しているが、本発明はこれに限定されるものではなく、他の符号化方式であってもよい。例えばＢＣＨ符号などは本発明に好適に適用可能である。また、ゴレイ符号、アダマール符号、リード・マラー符号、低密度パリティ検査符号、ゴッパ符号や、ファイア符号、畳込み符号、ターボ符号、巡回ハミングとＲＳ符号との連接符なども本発明に適用可能である。

[0031] 情報コード記録領域１０６は、情報コードＣｄを構成する４４個の情報シンボルと、ＲＳコードＣｅを構成する９０個のＲＳシンボルと、の計１３４個のシンボルからなっている。情報コード記録領域１０６は、４つのブロックＢ１～Ｂ４に分けられており、このうち２つのブロックＢ１及びＢ２は、１１個の情報シンボルとこれに対応する２２個のＲＳシンボルとの計３３個

のシンボルから構成され、残りの２つのブロックＢ３及びＢ４は、１１個の情報シンボルとこれに対応する２３個のＲＳシンボルとの計３４個のシンボルから構成されている。

[0032] 次に、図２に示す二次元コード１００の訂正領域に認証情報を埋め込んで、自己認証型二次元コード２００を生成する方法について、図３に示す模式図を用いて説明する。

[0033] まず、二次元コード１００の各ブロックを、所定のコード配置規則に従ってデコードして行くことにより、各ブロックから１１個の情報シンボルからなる情報ビット列と２２又は２３個のＲＳシンボルからなるＲＳビット列とを取得する。

[0034] 次に、各ブロックのＲＳビット列の予め定められた位置から１２個のＲＳシンボルを抽出する。続いて、抽出した１２個のＲＳシンボルのうちから、予め定められた６シンボルを選択し、全４ブロックで計２４個のＲＳシンボルからなるビット長１９２のビット列ｍを取得する。

[0035] そして、ビット列ｍを楕円曲線暗号（ECC: Elliptic Curve Cryptography）を用いて暗号化してビット列ｃを取得する。楕円曲線暗号は、楕円曲線上の離散対数問題(ＥＣＤＬＰ)という数学の困難さに依存しており、ＥＣＤＬＰを効率的に解くアルゴリズムは現存しないことから、暗号的に強い。また、楕円曲線暗号では、ＲＳＡの１０２４ビットの鍵長の暗号強度を、僅か１６０ビットで実現でき、かつ処理に要する時間も短い。このため、楕円曲線暗号を用いて暗号化するのが最も好ましい。

[0036] なお、本実施の形態では、最適例として、楕円曲線暗号を用いてビット列を暗号化するものを例示しているが、本発明はこれに限定されるものではなく、他の暗号化方式であってもよい。例えばＲＳＡ（Rivest-Shamir-Adleman）暗号やエルガマル暗号などの非対称暗号（公開鍵暗号）は、本発明に好適に適用可能である。また、ＡＥＳ（Advanced Encryption Standard）暗号やＤＥＳ（Data Encryption Standard）暗号なども本発明に適用可能である。

[0037] 続いて、ビット列ｃをブロック数に合わせて４分割してビット列ｃｉ（ｉ

＝１～４）を生成する。また、ビット列ｃｉ（ｉ＝１～４）と各ブロックから抽出した１２個のＲＳシンボルのうち、残りの６シンボルからなるビット列Ｉｉ（ｉ＝１～４）との排他的論理和をそれぞれ算出してビット列ｃｉ（ｉ＝１～４）を生成する。そして、例えば図３（Ａ）及び（Ｂ）に示すように、ビット列Ｉｉをそれぞれビット列ｃｉに置換することにより、ビット列ｃを認証情報として埋め込む。

[0038] 続いて、情報ビット列と、認証情報が埋め込まれたＲＳビット列と、を元の二次元コード１００のコード配置規則に従って配置することにより、訂正領域に認証情報を埋め込んだ自己認証型二次元コード２００を生成する。

[0039] 次に、図１に示す移動体通信端末２０の構成について説明する。

[0040] 移動体通信端末２０は、例えば、カメラ機能を有する携帯電話やスマートフォンなどに、後述する認証アプリケーションプログラムをインストールすることで二値化処理の実施が可能となる。移動体通信端末２０は、自己認証型二次元コード２００を光学的に読み取り可能な光学的情報読取装置として構成される端末である。この移動体通信端末２０は、制御部２１と、撮像部２２と、記憶部２３と、操作部２４と、表示部２５と、通信部２６と、を備えている。

[0041] 制御部２１は、携帯電話としての通常の通信処理に加えて、カメラ機能を有する撮像部２２からの画素信号に基づいて撮像された画像データを処理可能なものである。制御部２１は、マイコンを主体として構成されるものであり、ＣＰＵ（Central Processing Unit）、システムバス、入出力インターフェース等を有している。制御部２１は、記憶部２３とともに情報処理装置として機能している。

[0042] 記憶部２３は、ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）、不揮発性メモリなどの公知の半導体メモリなどによって構成されている。この記憶部２３には、上述した通話機能や通信機能を実現するための所定プログラム等が予め格納されているとともに、認証サーバ３０からダウンロードした認証アプリケーションプログラムが格納される。これにより、当

該移動体通信端末２０は、画像データに含まれる自己認証型二次元コード２００を二値化する装置として構成される。また、記憶部２３には、認証アプリケーションプログラムのシリアル番号が格納されている。

[0043] 操作部２４は、複数のキー等により構成されている。操作部２４は、制御部２１に対してキー操作に応じた情報を入力する機能を有するものである。

[0044] 表示部２５は、液晶表示器等から構成されている。表示部２５は、制御部２１により制御されて、自己認証型二次元コード２００によって表現される物品の購入サイトのＵＲＬ等を表示する機能を有するものである。

[0045] 通信部２６は、制御部２１により制御されて、インターネット等のネットワークＮを介して認証サーバ３０等と通信を行う機能を有するものである。

[0046] 次に、認証サーバ３０の構成について説明する。

[0047] 認証サーバ３０は、ネットワークＮを介して１または複数の移動体通信端末２０と通信可能なサーバとして機能する装置である。認証サーバ３０は、主に、制御部３１と、記憶部３２と、通信部３３と、を備えている。

[0048] 制御部３１は、記憶部３２及び通信部３３を統括的に制御するものである。制御部３１は、マイコンを主体として構成されるものであり、ＣＰＵ、システムバス、入出力インターフェース等を有している。制御部３１は、記憶部３２とともに情報処理装置として機能している。

[0049] 記憶部３２は、ＲＯＭ、ＲＡＭ、不揮発性メモリなどの公知の半導体メモリなどによって構成されている。この記憶部３２には、データベース３２ａと、後述する認証処理を実行するためのアプリケーションプログラムと、が予め格納されている。また、記憶部３２には、認証アプリケーションプログラムのダウンロードデータが格納されている。

[0050] データベース３２ａは、認証アプリケーションプログラムのシリアル番号と、認証アプリケーションプログラムをダウンロードした移動体通信端末２０の利用者の個人情報と、を対応付けて登録する。個人情報には、利用者の名前や、住所、メールアドレスなどが含まれている。

[0051] 通信部３３は、ネットワークＮ等を介した通信を可能とするものである。

通信部３３は、制御部３１により制御されて、ネットワークＮを介して、１または２以上の移動体通信端末２０等と通信を行う機能を有するものである。

[0052] 次に、このように構成される認証システム１において、利用者の個人情報を登録するために実施される登録処理と、移動体通信端末２０及び自己認証型二次元コード２００を認証するために実施される認証処理と、について、図４～図６を参照して説明する。図４は、本実施形態に係る認証システムにおける登録処理の流れを例示するフローチャートである。図５及び図６は、本実施形態に係る認証システムにおける認証処理の流れを例示するフローチャートである。

[0053] まず、認証システム１にて実施される登録処理について、図４に示すフローチャートを用いて詳細に説明する。

[0054] 利用者による操作部２４の操作によって認証アプリケーションプログラムのダウンロードが指示されたことに応答して、移動体通信端末２０は、図４に示す登録処理を開始する。

[0055] 登録処理において、制御部２１は、まず、ダウンロード処理を実行して、認証アプリケーションプログラムを認証サーバ３０からネットワークＮを介してダウンロードするとともに（ステップＳ１）、個人情報入力画面を表示部２５に表示する（ステップＳ２）。

[0056] その後、制御部２１は、利用者による操作部２４の操作によって個人情報が個人情報入力画面に入力されて認証サーバ３０への送信が指示されたか否かを判別し（ステップＳ３）、個人情報が入力されて送信の指示がされたと判別するまで（ステップＳ３；Ｎｏ）、ループして待つ。

[0057] そして、個人情報が入力されて送信の指示がされたと判別した場合（ステップＳ３；Ｙｅｓ）、制御部２１は、個人情報入力画面に入力された個人情報を、通信部２６からネットワークＮを介して認証サーバ３０に送信する（ステップＳ４）。

[0058] 一方、認証サーバ３０では、制御部３１が、移動体通信端末２０からネッ

トワークＮを介して送信された個人情報を通信部３３で受信したことに応答して（ステップＳ５）、移動体通信端末２０によってダウンロードされた認証アプリケーションプログラムにシリアル番号を付与する（ステップＳ６）。

[0059] そして、制御部３１は、ステップＳ５で受信した個人情報とステップＳ６で付与したシリアル番号とを対応付けて記憶部３２のデータベース３２ａに記憶するとともに（ステップＳ７）、ステップＳ６で付与したシリアル番号を通信部３３からネットワークＮを介して移動体通信端末２０に送信する（ステップＳ８）。

[0060] 一方、移動体通信端末２０では、制御部２１が、認証サーバ３０からネットワークＮを介して送信されたシリアル番号を通信部２６で受信したことに応答して（ステップＳ９）、インストール処理を実行して、ステップＳ１でダウンロードした認証プログラムアプリケーションを記憶部２３にインストールするとともに（ステップＳ１０）、ステップＳ９で受信したシリアル番号を記憶部２３に記憶して（ステップＳ１１）、登録処理を終了する。

[0061] 次に、認証システム１にて実施される認証処理について、図５に示すフローチャートを用いて詳細に説明する。

[0062] 移動体通信端末２０は、撮像部２２で自己認証型二次元コード２００を撮像したことに応答して、図５及び図６に示す認証処理を開始する。認証処理において、制御部２１は、まず、撮像部２２で自己認証型二次元コード２００を撮像して得られた撮像ビット列と、記憶部２３に記憶されている認証アプリケーションプログラムにシリアル番号を示す番号ビット列と、を含むビット信号を生成して（図５のステップＳ２１）、通信部２６からネットワークＮを介して認証サーバ３０に送信する（ステップＳ２２）。

[0063] 一方、認証サーバ３０では、制御部３１が、移動体通信端末２０からネットワークＮを介して送信されるビット信号を通信部３３で受信したことに応答して（ステップＳ２３）、ビット信号から撮像ビット列と番号ビット列とを抽出する（ステップＳ２４）。そして、制御部３１は、ステップＳ２４で

抽出した番号ビット列が示すシリアル番号に一致するものが、データベース３２ａに登録されているか否かを判別することにより、利用者の認証を行う（ステップＳ２５）。

[0064] 制御部３１は、認証の結果、一致するシリアル番号が登録されていると判別した場合（ステップＳ２５；Ｙｅｓ）、ステップＳ２４で抽出した撮像ビット列を、上述のコード配置規則に従ってデコードして行くことにより、自己認証型二次元コード２００の各ブロックから１１個の情報シンボルからなる情報ビット列と２２又は２３個のＲＳシンボルからなるＲＳビット列とを取得する（ステップＳ２６）。

[0065] 次に、制御部３１は、撮像ビット列と、情報ビット列及びＲＳビット列と、の排他的論理和を求めることにより、２４個のＲＳシンボルからなるビット列ｃ’を誤りとして検出する（ステップＳ２７）。

[0066] 続いて、制御部３１は、ＲＳビット列に含まれるビット列Ｉと、誤りとして検出したビット列ｃ’と、の排他的論理和を算出することにより、認証情報として埋め込まれたビット列ｃ’を取得する（ステップＳ２８）。

[0067] また、制御部３１は、暗号化に対応する復号キーを利用して、ビット列ｃ’を復号化することにより、ビット列ｍｄを取得する（ステップＳ２９）。

[0068] そして、制御部３１は、復号化したビット列ｍｄが、ＲＳビット列に含まれるビット列ｍと合致しているか否かを判別することにより、自己認証型二次元コード２００の認証を行う（図６のステップＳ３０）。

[0069] 制御部３１は、認証の結果、両ビット列が合致しているとの認証結果が得られた場合（ステップＳ３０；Ｙｅｓ）、利用者の個人情報が登録され、自己認証型二次元コード２００が改ざんされていないとして、利用者及び自己認証型二次元コード２００の認証に成功した旨を示す認証成功通知とともに、ステップＳ２６で取得した計４４個の情報シンボルから構成される情報コードＣｄが表現する所定の情報（本実施形態では物品の購入サイトのＵＲＬ）を通信部３３からネットワークＮを介して移動体通信端末２０に送信する（ステップＳ３１）。

[0070] 一方、移動体通信端末２０では、制御部２１が、認証サーバ３０からネットワークＮを介して送信される認証成功通知及び所定の情報を受信したことに応答して（ステップＳ３２）、移動体通信端末２０及び自己認証型二次元コード２００の認証に成功した旨を表示部２５に表示するとともに（ステップＳ３３）、所定の情報（本実施形態では物品の購入サイトのＵＲＬ）を表示部２５に表示して購入サイトへのアクセスを可能にする（ステップＳ３４）。

[0071] これに対して、制御部３１は、認証の結果、一致するシリアル番号が登録されていないと判別した場合（ステップＳ２５；Ｎｏ）、利用者の個人情報が登録されていないとして、また、両ビット列が合致しているとの認証結果が得られた場合（ステップＳ３０；Ｎｏ）、自己認証型二次元コード２００が改ざんされているとして、利用者及び／又は自己認証型二次元コード２００の認証に失敗した旨を示す認証失敗通知を通信部３３からネットワークＮを介して移動体通信端末２０に送信する（ステップＳ３５）。

[0072] 一方、移動体通信端末２０では、制御部２１が、認証サーバ３０からネットワークＮを介して送信される認証失敗通知を受信したことに応答して（ステップＳ３６）、利用者及び／又は自己認証型二次元コード２００の認証に失敗した旨のみを表示部２５に表示する（ステップＳ３７）。

[0073] 以上説明したように、本実施形態に係る認証システム１では、移動体通信端末２０が、訂正領域に認証情報が埋め込まれた自己認証型二次元コード２００を撮像して得られた撮像ビット列と、記憶部２３に記憶されている認証アプリケーションプログラムにシリアル番号を示す番号ビット列と、を含むビット信号を認証サーバ３０に送信し、認証サーバ３０が、移動体通信端末２０の利用者及び自己認証型二次元コード２００の認証を行う。そして、認証サーバ３０は、利用者及び自己認証型二次元コード２００の認証に成功したことを条件に、自己認証型二次元コード２００が表現する所定の情報を移動体通信端末２０に送信する。これにより、移動体通信端末２０は、自己認証型二次元コード２００が表現する所定の情報を取得することができる。

[0074] ここで、自己認証型二次元コード２００は、ＲＳコードＣｅの一部から生成されるビット列ｍを暗号化したビット列ｃと、ＲＳコードＣｅのうち上記一部とは異なる部分から生成されるビット列Ｉと、の排他的論理和を求めてビット列ｃを取得し、ビット列Ｉをビット列ｃに置き換えることで、ビット列ｃを認証情報としてＲＳコードＣｅに埋め込むことにより生成される。

[0075] これにより、自己認証型二次元コード２００が改ざんされた場合、認証サーバ３０は、ビット列ｃとビット列Ｉとの排他的論理和を誤りとして検出できなくなるため、自己認証型二次元コード２００の偽造を検出することができる。

[0076] また、ＲＳコードＣｅに認証情報を埋め込むことで、所定の情報を表現する情報コードＣｄに何ら変更を加える必要が無くなるため、自己認証型二次元コード２００によって表現される情報のデータ量が削減されることを防止することができる。

[0077] さらに、ビット列ｍを暗号化したビット列ｃを認証情報としてＲＳコードＣｅに埋め込むことで、自己認証型二次元コード２００の偽造をより効果的に防止することができる。

[0078] また、移動体通信端末２０は、自己認証型二次元コード２００のデコード及び認証を行わず、自己認証型二次元コード２００を撮像して得られた撮像ビット列と、記憶部２３に記憶されている認証アプリケーションプログラムにシリアル番号を示す番号ビット列と、を含むビット信号を送信するため、認証サーバ３０以外は、ビット信号を解読して所定の情報を取得することができないため、安全性を高めることができる。

[0079] さらに、移動体通信端末２０は、認証サーバ３０で利用者及び自己認証型二次元コード２００の認証に成功したことを条件に、自己認証型二次元コード２００が表現する所定の情報を取得することができるため、危険なウェブサイトへのアクセスを防止することができる。

[0080] また、移動体通信端末２０の利用者の認証には、利用者の個人情報の登録時に付与される認証アプリケーションのシリアル番号が用いられ、ＩＤ（Ide

ntity Document）やパスワード等を認証サーバ３０に送信する必要がないため、ＩＤやパスワード等の流出を防止することができる。

[0081] なお、本発明は、上記実施形態に限定されず、種々の変形、応用が可能である。以下、本発明に適用可能な上記実施形態の変形態様について、説明する。

[0082] 上記実施形態では、利用者及び自己認証型二次元コード２００の認証の用途として、物品の購入の際に行われるものを例に説明したが、本発明はこれに限定されるものでなく、役所等で住民票や印鑑証明を請求する際等、その用途は任意である。

[0083] 上記実施形態では、自己認証型二次元コード２００が所定の情報として物品の購入サイトを表現するものとして説明したが、本発明はこれに限定されるものではなく、自己認証型二次元コード２００が表現する情報は任意であり、役所等で住民票や印鑑証明を請求する旨等、如何なる情報であっても構わない。

[0084] 上記実施形態では、利用者及び自己認証型二次元コード２００の認証に成功した場合、その旨が表示部２５に表示されるとともに、自己認証型二次元コード２００が表現する所定の情報が表示されるものとして説明した。しかしながら、本発明はこれに限定されるものではなく、利用者及び自己認証型二次元コード２００の認証に成功した場合における表示は、任意であり、例えば利用者及び自己認証型二次元コード２００の認証に成功した旨の表示が行われ、自己認証型二次元コード２００が表現する所定の情報が表示されないものであってもよい。

[0085] 上記実施形態では、利用者及び自己認証型二次元コード２００の双方の認証を行うものとして説明したが、本発明はこれに限定されるものではなく、例えば利用者の認証のみを行うものであってもよいし、自己認証型二次元コード２０の認証のみを行うものであってもよい。

[0086] 上記実施形態において、利用者の認証に認証アプリケーションプログラムのシリアル番号が使用されるものとして説明したが、本発明はこれに限定さ

れるものではなく、利用者の認証に使用される識別番号は任意であり、例えば移動体通信端末２０の個体識別番号等であってもよい。

[0087] 上記実施形態において、認証アプリケーションプログラムのシリアル番号は、個人情報の入力後、認証アプリケーションプログラムのインストール前に付与される者として説明した。しかしながら、本発明はこれに限定されるものではなく、認証アプリケーションプログラムのシリアル番号の付与タイミングは任意であり、認証アプリケーションプログラムのダウンロード時に付与されてもよいし、認証アプリケーションプログラムのインストール後に付与されてもよい。

[0088] 上記実施形態では、ビット列ｍを暗号化してビット列ｃを生成し、ビット列ｃとビット列ｌとの排他的論理和を算出するものとして説明した。しかしながら、本発明はこれに限定されるものではなく、ビット列ｍを暗号化することなく、ビット列ｍとビット列ｌとの排他的論理和を算出してもよい。この場合、自己認証型二次元コード２００は、ビット列ｍを４分割したビット列ｍｉとビット列ｌｉとの排他的論理和をそれぞれ算出してビット列ｍｉを生成し、ビット列ｌｉをビット列ｍｉに置き換えてビット列ｍを認証情報としてＲＳコードＣｅに埋め込むことにより生成されればよい。

[0089] そして、認証サーバ３０では、制御部３１が、ＲＳビット列を用いて、ビット列ｍ’を誤りとして検出する。次に、制御部３１は、ＲＳビット列に含まれるビット列ｌと誤りとして検出したビット列ｍ’との排他的論理和を算出してビット列ｍ’を取得し、取得したビット列ｍ’が、ＲＳビット列に含まれるビット列ｍと合致するか否か判別することにより、自己認証型二次元コード２００の認証を行えばよい。

[0090] 上記実施形態では、二次元コード１００及び自己認証型二次元コード２００が白色のセルと黒色のセルとから構成されるものとして説明した。しかしながら、本発明はこれに限定されるものではなく、汎用の二次元コードリーダによって“０”と認識される光学的特性の一又は複数の色と、“１”と認識される光学的特性の一又は複数の色と、を用いて所定の情報を表現するも

のであれば任意に適用可能であり、例えば二次元コードに視認可能なロゴマークを重ね合わせたロゴ付き二次元コードであってもよい。例えば、所定明度未満（汎用の二次元コードリーダによって“０”と認識される明度）のロゴマークに、所定明度以上（汎用の二次元コードリーダによって“１”と認識される明度）のセルを重ね合わせ、ロゴマークのうちセルが重ね合わされていない部分とセルとの分布パターンによって所定の情報を表現するものであってもよい（例えば特開２００７－２８７００４号公報参照）。

[0091] あるいは、「ロゴマークのうち所定明度以上の部分には、所定明度未満のセルドットを重ね合わせる一方で、ロゴマークのうち所定明度未満の部分には、所定明度以上のセルドットを重ね合わせ、所定明度以上のセルドット及びロゴマークのうち所定明度以上の部分と、所定明度未満のセルドット及びロゴマークのうち所定明度未満の部分と、の分布パターンによって所定の情報を表現するものであってもよい（例えば特開２００８－１５６４２号公報参照）。なお、本明細書中に特開２００７－２８７００４号公報及び特開２００８－１５６４２号公報の明細書、特許請求の範囲、図面全体を参考として取り込むものとする。

[0092] 上記実施形態では、二次元コードとしてＱＲコード（登録商標）を例示して説明したが、本発明はこれに限定されるものではなく、二次元コードは、データマトリクス、アズテックコード、コードワン、アレイタグ、ボックス図形コード、マキシコード、ペリコード、ソフトストリップ、ＣＰコード、カルラコード、ウルトラコードなどといった他のマトリクス式の二次元コードであってもよい。あるいは、ＰＤＦ４１７、コード４９、コード１６ｋ、コーダブロックなどといった一次元バーコードを縦に積み重ねたスタック式の二次元コードであっても構わない。

[0093] 上記実施形態において、認証サーバ３０のＣＰＵが実行するプログラムは、予めＲＯＭ等に記憶されるものとして説明したが、本発明はこれに限定されるものではなく、上述の処理を実行させるためのプログラムを、既存の汎用コンピュータに適用することで、上記実施形態に係る認証サーバ３０とし

て機能させてもよい。

[0094] このようなプログラムの提供方法は任意であり、例えばコンピュータが読取可能な記録媒体（フレキシブルディスク、ＣＤ（Compact Disc）－ＲＯＭ、ＤＶＤ（Digital Versatile Disc）－ＲＯＭ等）に格納して配布してもよいし、インターネット等のネットワーク上のストレージにプログラムを格納しておき、これをダウンロードさせることにより提供してもよい。

[0095] さらに、上記の処理をＯＳとアプリケーションプログラムとの分担、又はＯＳとアプリケーションプログラムとの協働によって実行する場合には、アプリケーションプログラムのみを記録媒体やストレージに格納してもよい。また、搬送波にプログラムを重畳し、ネットワークを介して配信することも可能である。例えば、ネットワーク上の掲示板（ＢＢＳ：Bulletin Board System）に上記プログラムを掲示し、ネットワークを介してプログラムを配信してもよい。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケーションプログラムと同様に実行することにより、上記の処理を実行できるように構成してもよい。

[0096] なお、本発明は、本発明の広義の精神と範囲を逸脱することなく、様々な実施の形態及び変形が可能とされるものである。また、上述した実施の形態は、本発明の一実施例を説明するためのものであり、本発明の範囲を限定するものではない。

符号の説明

[0097]

１ 認証システム

１０ 仮想自動販売機

２０ 移動体通信端末

２１ 制御部

２２ 撮像部

２３ 記憶部

２４ 操作部

２５ 表示部

２６　通信部

３０　認証サーバ

３１　制御部

３２　記憶部

３３　通信部

１００　二次元コード

２００　自己認証型二次元コード

請求の範囲

［請求項1］ 所定の情報をセルの分布パターンによって表現する情報領域と、誤りを訂正するための訂正情報をセルの分布パターンによって表現する訂正領域と、を備え、該訂正領域の一部が、該一部から生成された第１訂正ビット列と該訂正領域のうち該一部とは異なる部分から生成された第２訂正ビット列との排他的論理和に置き換えられた二次元コードを撮像してビット信号を生成する通信端末とネットワークを介して接続され、

前記通信端末から前記ネットワークを介して送信される前記ビット信号を受信するビット信号受信手段と、

前記ビット信号受信手段によって受信した前記ビット信号をデコードして、前記所定の情報と前記訂正情報とを取得するデコード手段と、

前記デコード手段によって取得した前記訂正情報を用いて、前記第１訂正ビット列と前記第２訂正ビット列との排他的論理和を誤りとして検出する誤り検出手段と、

前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手段によって検出した誤りとの排他的論理和が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否か判別することにより、前記二次元コードの認証を行う二次元コード認証手段と、

前記二次元コード認証手段によって両者が合致するとの認証結果が得られた場合、前記デコード手段によって取得した前記所定の情報を前記ネットワークを介して前記通信端末に送信する情報送信手段と、

を備えることを特徴とする認証サーバ。

［請求項2］ 前記ビット信号受信手段は、前記訂正領域の一部が、前記第１訂正ビット列と前記第２訂正ビット列を暗号化して得られた暗号ビット列との排他的論理和に置き換えられた前記二次元コードの前記ビット信号を受信し、

前記二次元コード認証手段は、前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手段によって検出した誤りとの排他的論理和を前記暗号化に対応する方式で復号化して得られた復号ビット列が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否かを判別することにより、前記二次元コードの認証を行う、

ことを特徴とする請求項１に記載の認証サーバ。

［請求項3］ 前記ビット信号受信手段は、前記訂正領域の一部が、前記第１訂正ビット列と前記第２訂正ビット列を非対称暗号化方式で暗号化して得られた暗号ビット列との排他的論理和に置き換えられた前記二次元コードの前記ビット信号を受信し、

前記二次元コード認証手段は、前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手段によって検出した誤りとの排他的論理和を前記非対称暗号化方式に対応する方式で復号化して得られた復号ビット列が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否かを判別することにより、前記二次元コードの認証を行う、

ことを特徴とする請求項２に記載の認証サーバ。

［請求項4］ 前記ビット信号受信手段は、前記訂正領域の一部が、前記第１訂正ビット列と前記第２訂正ビット列を楕円曲線暗号方式で暗号化して得られた暗号ビット列との排他的論理和に置き換えられた前記二次元コードの前記ビット信号を受信し、

前記二次元コード認証手段は、前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手段によって検出した誤りとの排他的論理和を前記楕円曲線暗号方式に対応する方式で復号化して得られた復号ビット列が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否かを判別することにより、前記二次元コードの認証を行う、

ことを特徴とする請求項３に記載の認証サーバ。

［請求項5］ 前記通信端末の利用者を特定可能な識別情報を登録する識別情報登録手段と、

前記識別情報登録手段に、前記通信端末から前記ビット信号に含めて送信される前記識別情報と合致するものが登録されているか否かを判別することにより、前記利用者の認証を行う利用者認証手段と、

をさらに備え、

前記情報送信手段は、前記二次元コード認証手段によって両者が合致するとの認証結果が得られるとともに、前記利用者認証手段によって識別情報が登録されているとの認証結果が得られる場合、前記デコード手段によって取得した前記所定の情報を前記ネットワークを介して前記通信端末に送信する、

ことを特徴とする請求項１～４のいずれか１項に記載の認証サーバ。

[請求項6] 請求項１～５のいずれか１項に記載の認証サーバと、該認証サーバと前記ネットワークを介して接続された前記通信端末と、を備え、

前記通信端末は、

前記二次元コードを撮像して前記ビット信号を生成するビット信号生成手段と、

前記ビット信号生成手段によって生成した前記ビット信号を前記ネットワークを介して前記認証サーバに送信するビット信号送信手段と、

前記情報送信手段によって送信された前記所定の情報を受信することにより、前記二次元コードが表現する該所定の情報を取得する情報受信手段と、

を備えることを特徴とする認証システム。

[請求項7] 所定の情報をセルの分布パターンによって表現する情報領域と、誤りを訂正するための訂正情報をセルの分布パターンによって表現する訂正領域と、を備え、該訂正領域の一部が、該一部から生成された第１訂正ビット列と該訂正領域のうち該一部とは異なる部分から生成された第２訂正ビット列との排他的論理和に置き換えられた二次元コー

ドを撮像してビット信号を生成する通信端末とネットワークを介して接続された認証サーバによる認証方法であって、

前記通信端末から前記ネットワークを介して送信される前記ビット信号を受信するビット信号受信ステップと、

前記ビット信号受信ステップによって受信した前記ビット信号をデコードして、前記所定の情報と前記訂正情報とを取得するデコードステップと、

前記デコードステップによって取得した前記訂正情報を用いて、前記第１訂正ビット列と前記第２訂正ビット列との排他的論理和を誤りとして検出する誤り検出ステップと、

前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出ステップによって検出した誤りとの排他的論理和が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否か判別することにより、前記二次元コードの認証を行う二次元コード認証ステップと、

前記二次元コード認証ステップによって両者が合致するとの認証結果が得られた場合、前記デコードステップによって取得した前記所定の情報を前記ネットワークを介して前記通信端末に送信する情報送信ステップと、

を備えることを特徴とする認証方法。

［請求項8］ 所定の情報をセルの分布パターンによって表現する情報領域と、誤りを訂正するための訂正情報をセルの分布パターンによって表現する訂正領域と、を備え、該訂正領域の一部が、該一部から生成された第１訂正ビット列と該訂正領域のうち該一部とは異なる部分から生成された第２訂正ビット列との排他的論理和に置き換えられた二次元コードを撮像してビット信号を生成する通信端末とネットワークを介して接続された認証サーバのコンピュータに、

前記通信端末から前記ネットワークを介して送信される前記ビット信号を受信するビット信号受信手順と、

前記ビット信号受信手順によって受信した前記ビット信号をデコードして、前記所定の情報と前記訂正情報とを取得するデコード手順と、

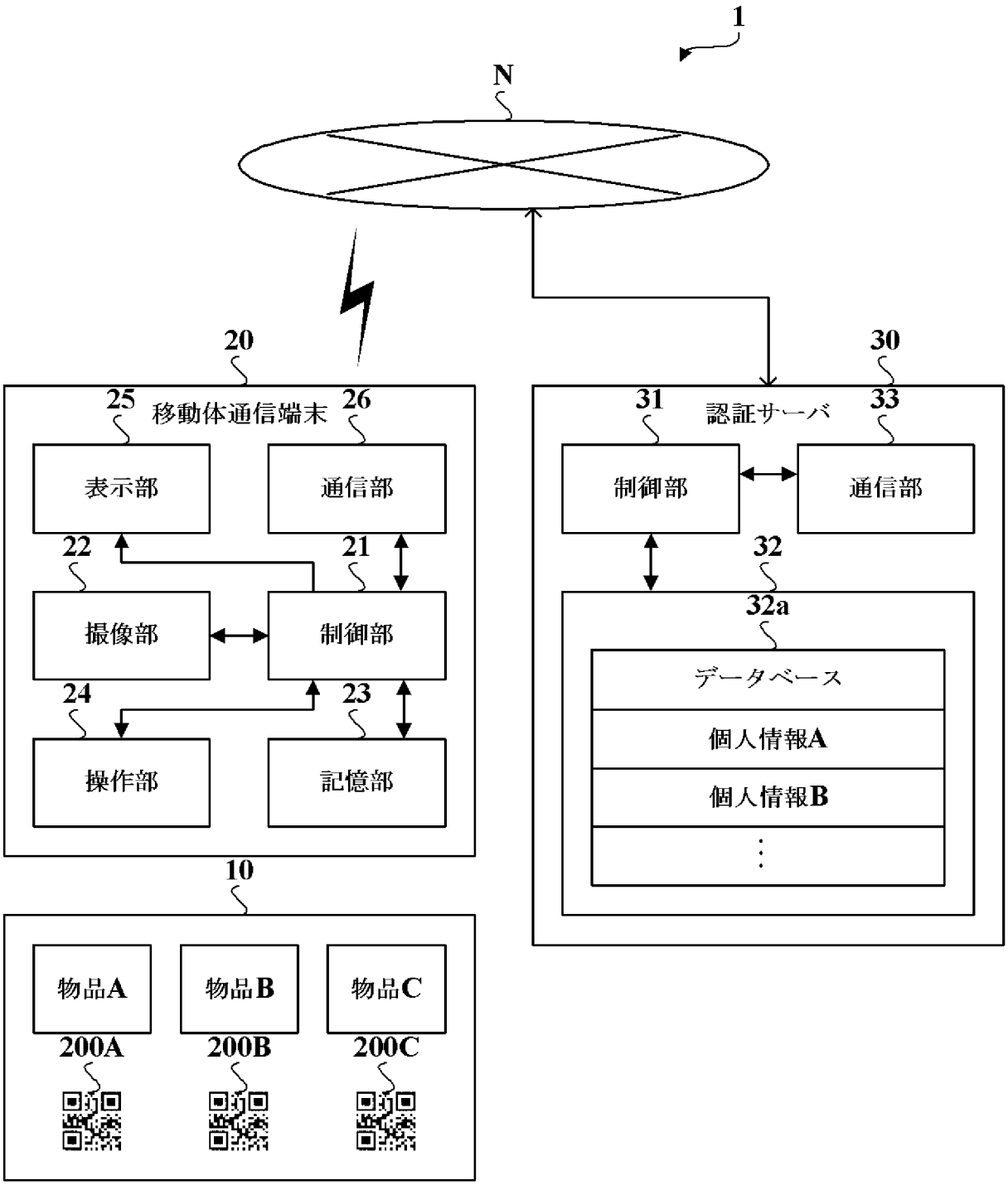
前記デコード手順によって取得した前記訂正情報を用いて、前記第１訂正ビット列と前記第２訂正ビット列との排他的論理和を誤りとして検出する誤り検出手順と、

前記訂正情報に含まれる前記第１訂正ビット列と前記誤り検出手順によって検出した誤りとの排他的論理和が、該訂正情報に含まれる前記第２訂正ビット列と合致するか否か判別することにより、前記二次元コードの認証を行う二次元コード認証手順と、

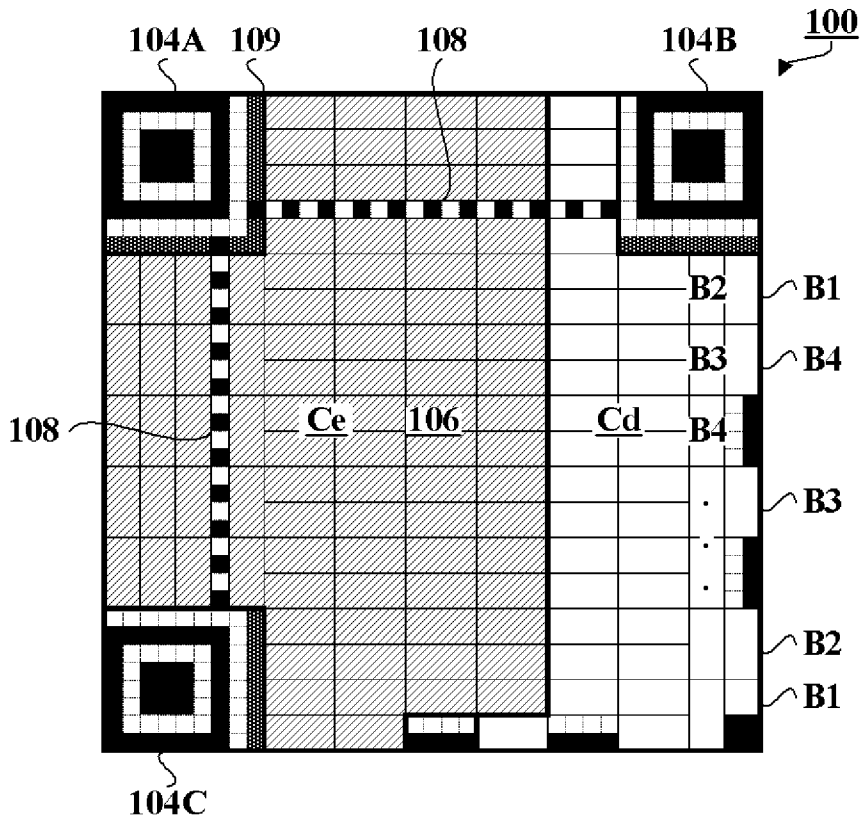
前記二次元コード認証手順によって両者が合致するとの認証結果が得られた場合、前記デコード手順によって取得した前記所定の情報を前記ネットワークを介して前記通信端末に送信する情報送信手順と、

を実行させるためのプログラム。

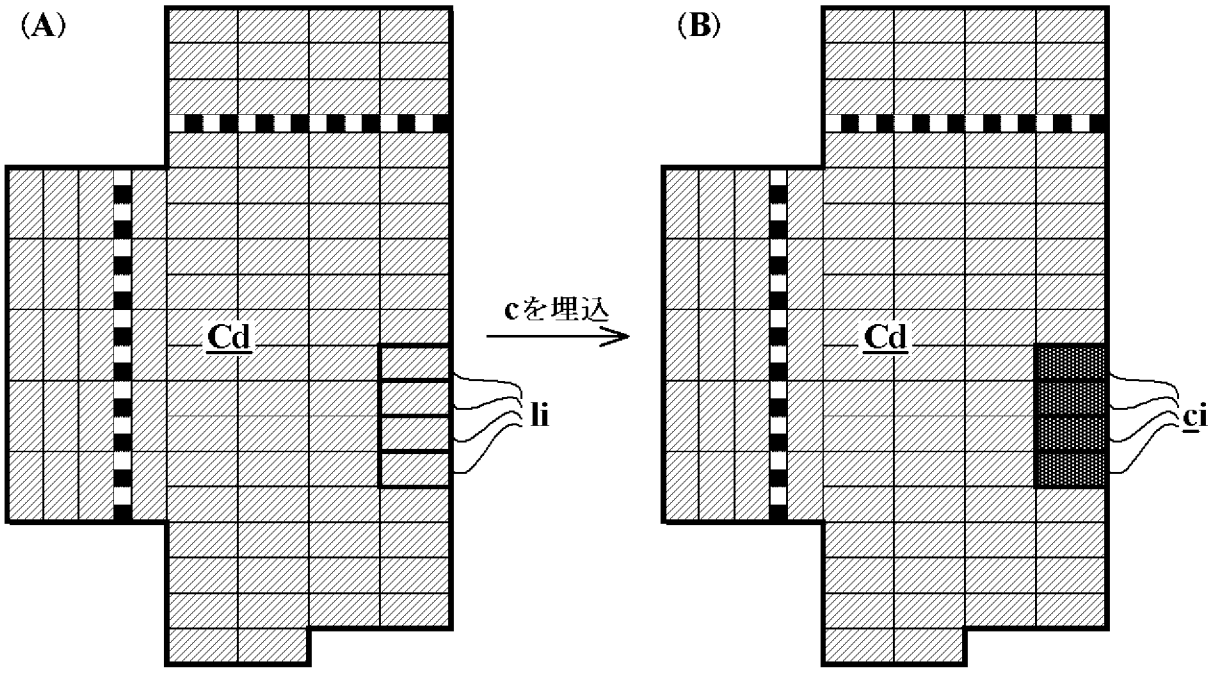
[図1]


1
N
20
30
25
移動体通信端末
26
31
認証サーバ
33
表示部
通信部
制御部
通信部
22
21
32
32a
撮像部
制御部
データベース
個人情報A
個人情報B
24
23
操作部
記憶部
10
物品A
物品B
物品C
200A
200B
200C

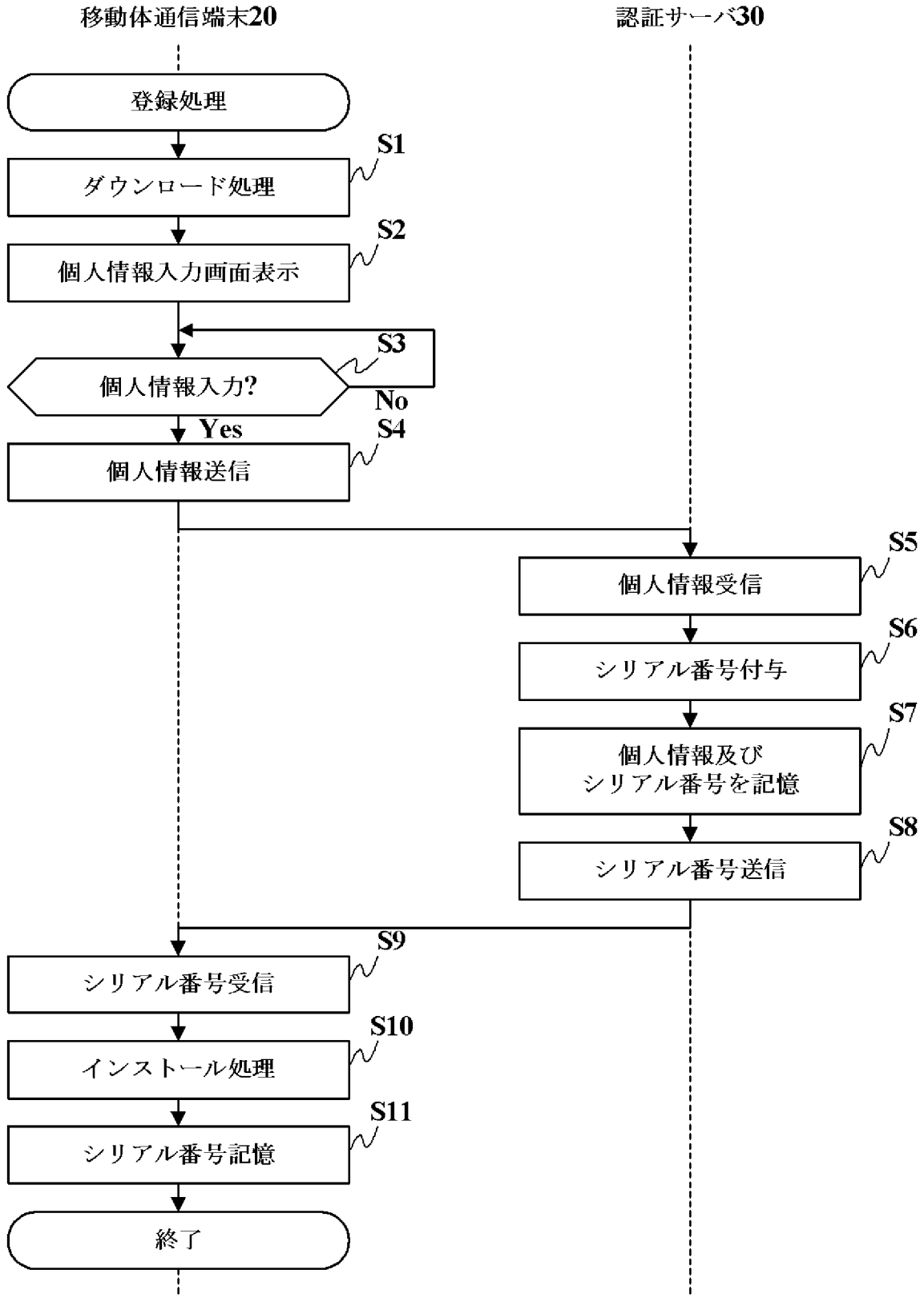
[図2]


104A
109
108
104B
100
B2
B1
B3
B4
108
Ce
106
Cd
B4
B3
B2
B1
104C

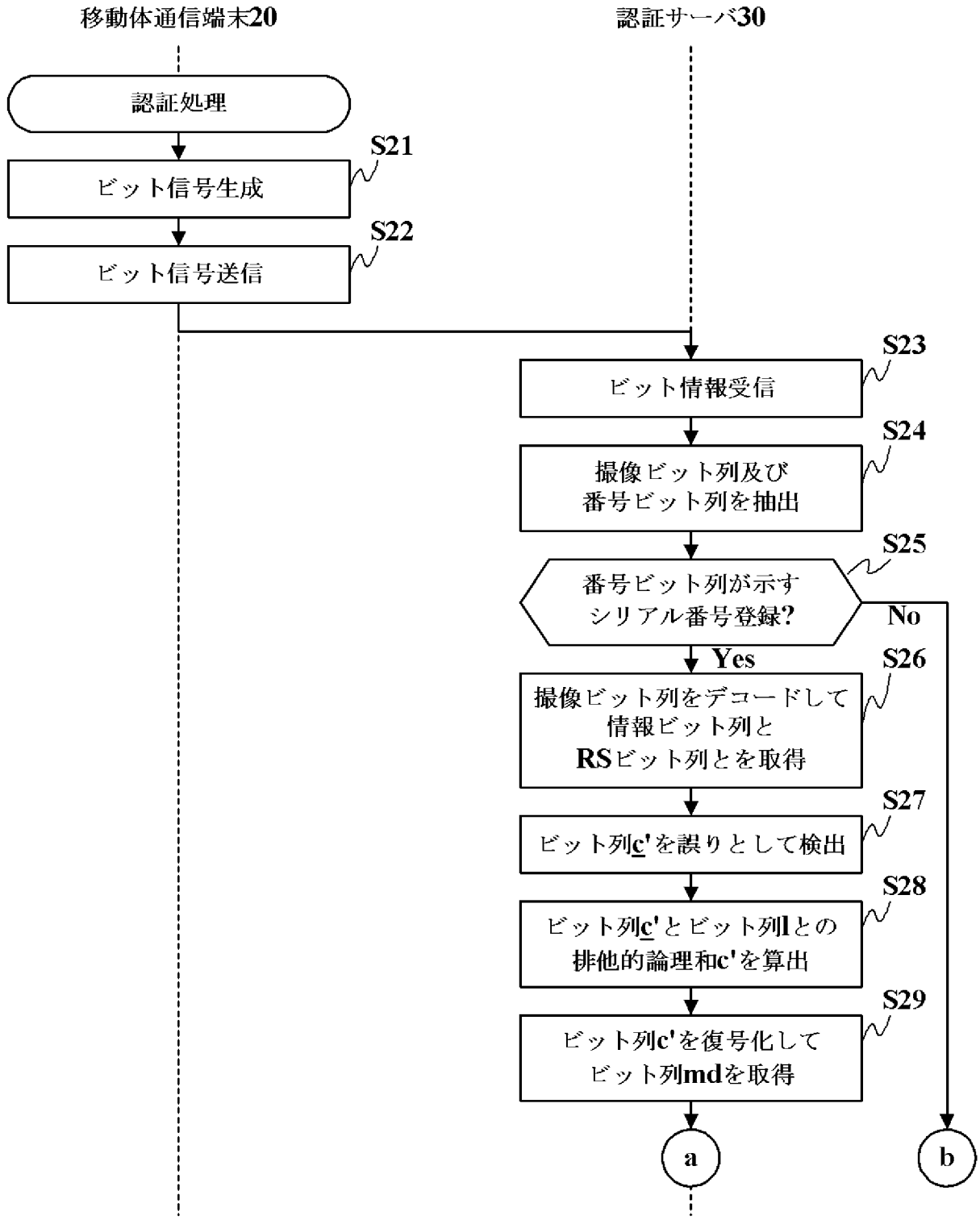
[図3]


(A)
(B)
Cd
cを埋込
li
Cd
ci

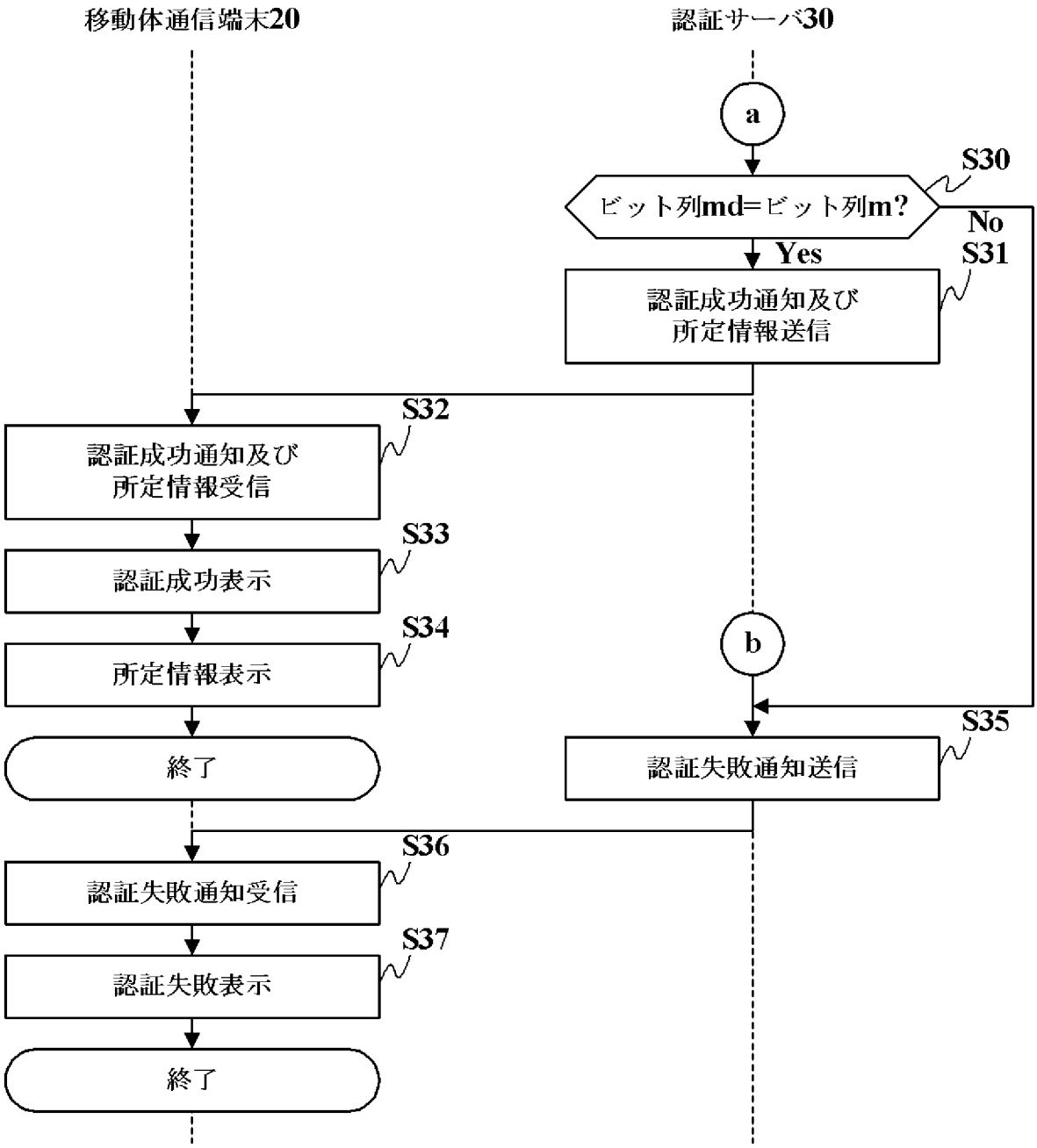
[図4]


移動体通信端末20
認証サーバ30
登録処理
S1
ダウンロード処理
S2
個人情報入力画面表示
S3
個人情報入力?
No
Yes
S4
個人情報送信
S5
個人情報受信
S6
シリアル番号付与
S7
個人情報及び
シリアル番号を記憶
S8
シリアル番号送信
S9
シリアル番号受信
S10
インストール処理
S11
シリアル番号記憶
終了

[図5]


移動体通信端末20
認証サーバ30
認証処理
S21
ビット信号生成
S22
ビット信号送信
S23
ビット情報受信
S24
撮像ビット列及び
番号ビット列を抽出
S25
番号ビット列が示す
シリアル番号登録?
No
Yes
S26
撮像ビット列をデコードして
情報ビット列と
RSビット列とを取得
S27
ビット列c'を誤りとして検出
S28
ビット列c'とビット列Iとの
排他的論理和c'を算出
S29
ビット列c'を復号化して
ビット列mdを取得
a
b

[図6]


移動体通信端末20
認証サーバ30
a
S30
ビット列md=ビット列m?
No
Yes
S31
認証成功通知及び
所定情報送信
S32
認証成功通知及び
所定情報受信
S33
認証成功表示
S34
所定情報表示
終了
b
S35
認証失敗通知送信
S36
認証失敗通知受信
S37
認証失敗表示
終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/068295

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/44(2013.01)i, *G06K7/00*(2006.01)i, *G09C1/00*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/44, G06K7/00, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2013
Kokai Jitsuyo Shinan Koho	1971-2013	Toroku Jitsuyo Shinan Koho	1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2012-181645 A (Nippon Hoso Kyokai), 20 September 2012 (20.09.2012), paragraphs [0036] to [0129]; fig. 1 to 10 (Family: none)	1-8
A	JP 7-254037 A (Nippondenso Co., Ltd., Toyota Central Research and Development Laboratories, Inc.), 03 October 1995 (03.10.1995), paragraphs [0025] to [0069]; fig. 1 to 18 & JP 2938338 B2 & US 5726435 A & EP 672994 A1	1-8

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 October, 2013 (02.10.13)	15 October, 2013 (15.10.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/068295

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-53851 A (Nomura Research Institute, Ltd.), 03 February 2006 (03.02.2006), paragraphs [0023] to [0064]; fig. 2 to 10 (Family: none)	1-8
A	JP 2011-28314 A (Fujitsu Ltd.), 10 February 2011 (10.02.2011), paragraphs [0011] to [0086]; fig. 10 (Family: none)	1-8

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１３／０６８２９５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/44(2013.01)i, G06K7/00(2006.01)i, G09C1/00(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/44, G06K7/00, G09C1/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2012-181645 A（日本放送協会） 2012.09.20, 段落００３６－０１２９, 図１－１０ （ファミリーなし）	1-8
A	JP 7-254037 A（日本電装株式会社, 株式会社豊田中央研究所） 1995.10.03, 段落００２５－００６９, 図１－１８ & JP 2938338 B2 & US 5726435 A & EP 672994 A1	1-8

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０２．１０．２０１３	１５．１０．２０１３

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　４０９２
木村　励
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2006-53851 A (株式会社野村総合研究所) 2006.02.03, 段落００２３－００６４，図２－１０ (ファミリーなし)	1-8
A	JP 2011-28314 A (富士通株式会社) 2011.02.10, 段落００１１－００８６，図１０（ファミリーなし）	1-8