

(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
2020年5月7日(07.05.2020)



(10) 国際公開番号

WO 2020/090088 A1

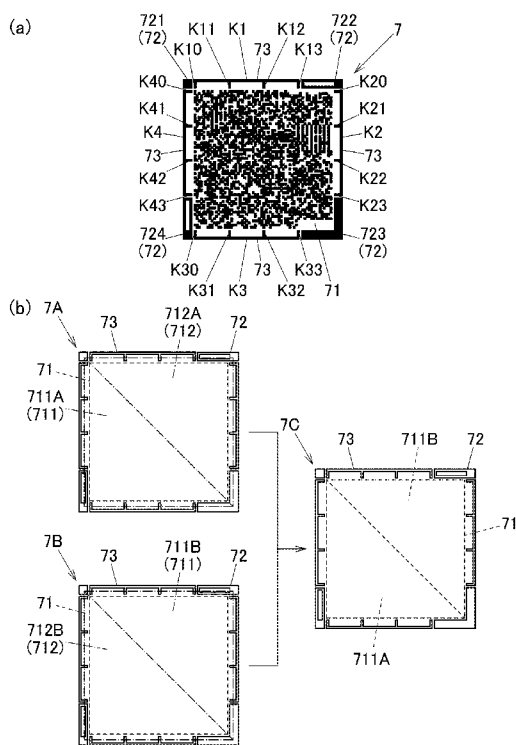
- (51) 国際特許分類:
G06K 19/06 (2006.01) G06K 7/14 (2006.01)
G06K 1/12 (2006.01)
- (21) 国際出願番号: PCT/JP2018/040733
- (22) 国際出願日: 2018年11月1日(01.11.2018)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (72) 発明者; および
- (71) 出願人: 溝口 ▲さとし▼(MIZOGUCHI Satoshi)
[JP/JP]; 〒1610035 東京都新宿区中井 2丁目10番8号ニの坂シティハウス108 Tokyo (JP).
- (74) 代理人: 特許業務法人コスモ国際特許事務所 (COSMO INTERNATIONAL PATENT FIRM); 〒1030006 東京都中央区日本橋富沢町10-14 日本橋BSビル3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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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).

(54) Title: ENCODING METHOD, DECODING METHOD, ENCODER, AND DECODER

(54) 発明の名称: エンコード方法、デコード方法、エンコーダ及びデコーダ



(57) Abstract: [Problem] To provide an encoding method, a decoding method, an encoder, and a decoder capable of secure secret sharing with a simple configuration. [Solution] Provided is an encoding method of two-dimensional code by an encoder, the encoder generating a first two-dimensional tally code that has a first effective area that includes first distributed information, and a first dummy area, and generating a second two-dimensional tally code that has a second effective area that includes second distributed information and that is arranged at the position of the first dummy area, and a second dummy area that is arranged at the position of the first effective area, according to a predetermined area allocation policy.

(57) 要約: 【課題】簡易な構成で安全な秘密分散が可能なエンコード方法、デコード方法、エンコーダ及びデコーダを提供すること。【解決手段】エンコーダによる二次元コードのエンコード方法は、該エンコーダが、予め定めた領域割当ポリシーに従って、第1分散情報を含む第1有効領域と、第1ダミー領域とを有する第1二次元割符コードを生成し、第2分散情報を含み第1ダミー領域の位置に配置される第2有効領域と、第1有効領域の位置に配置される第2ダミー領域とを有する第2二次元割符コードを生成する。

WO 2020/090088 A1

添付公開書類：

- 一 国際調査報告（条約第21条(3)）

明 細 書

発明の名称：

エンコード方法、デコード方法、エンコーダ及びデコーダ

技術分野

[0001] 本発明は、エンコード方法、デコード方法、エンコーダ及びデコーダに関する。

背景技術

[0002] 従来から、QRコード（登録商標）等の二次元コードに情報を埋め込んで、カメラを備えた情報処理装置に情報を伝達する技術が提案されている。例えば、特許文献1には、ユーザの携帯端末のディスプレイに表示された、取引IDを含む二次元コード及び第1の割符パターンを読み取る手段と、その取引IDに関連付けられた第2の割符パターンを記憶手段から抽出する手段と、第1の割符パターンと第2の割符パターンを重ね合わせて個性化電子証明書データの二次元コードを復元する手段と、を備える認証システムが記載されている。この認証システムは、個性化電子証明書データを確認して、ユーザが選択した商品の交付指令を出力することができる。

先行技術文献

特許文献

[0003] 特許文献1：特許第4268575号

発明の概要

発明が解決しようとする課題

[0004] 特許文献1の認証システムでは、割符パターンの生成において、データセルの部分に対して正マスクパターン適用処理及び副マスクパターン適用処理を施すことにより正割符パターンと副割符パターンを生成した後、割符コード生成部により各正割符パターン及び副割符パターンに調整パターンの追加処理が行われる。また、QRコードの復元は、調整済み正割符パターンと調整済み副割符パターンに対して、排他的論理和で演算処理を施すことにより

行われる。そのため、二次元コードの秘密分散処理及びその復元処理が複雑でシステムへの負荷が大きい。

[0005] 本発明は、以上の点に鑑み、簡易な構成で安全な秘密分散が可能なエンコード方法、デコード方法、エンコーダ及びデコーダ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

[0006] 本発明に係るエンコード方法は、エンコーダによる二次元コードのエンコード方法であって、前記エンコーダが、予め定めた領域割当ポリシーに従って、第1分散情報を含む第1有効領域と、第1ダミー領域とを有する第1二次元割符コードを生成し、第2分散情報を含み前記第1ダミー領域の位置に配置される第2有効領域と、前記第1有効領域の位置に配置される第2ダミー領域とを有する第2二次元割符コードを生成する、ことを特徴とする。

[0007] 本発明に係るデコード方法は、デコーダによる二次元コードのデコード方法であって、前記デコーダが、予め定めた領域割当ポリシーに従って生成された、第1分散情報を含む第1有効領域と、第1ダミー領域とを有する第1二次元割符コードを取得し、第2分散情報を含み前記第1ダミー領域の位置に配置される第2有効領域と、前記第1有効領域の位置に配置される第2ダミー領域とを有する第2二次元割符コードを取得し、前記領域割当ポリシーに従って前記第1有効領域及び前記第2有効領域を切り出し、前記第1有効領域及び前記第2有効領域を切り出し前の位置と対応する位置に配置して前記二次元コードのデータ領域として結合する、ことを特徴とする。

[0008] 本発明に係るエンコーダは、予め定めた領域割当ポリシーに従って、第1分散情報を含む第1有効領域と、第1ダミー領域とを有する第1二次元割符コードを生成し、第2分散情報を含み前記第1ダミー領域の位置に配置される第2有効領域と、前記第1有効領域の位置に配置される第2ダミー領域とを有する第2二次元割符コードを生成する、ことを特徴とする。

[0009] 本発明に係るデコーダは、予め定めた領域割当ポリシーに従って生成された、第1分散情報を含む第1有効領域と、第1ダミー領域とを有する第1二

次元割符コードを取得し、第2分散情報を含み前記第1ダミー領域の位置に配置される第2有効領域と、前記第1有効領域の位置に配置される第2ダミー領域とを有する第2二次元割符コードを取得し、前記領域割当ポリシーに従って前記第1有効領域及び前記第2有効領域を切り出し、前記第1有効領域及び前記第2有効領域を切り出し前の位置と対応する位置に配置して二次元コードのデータ領域として結合する、ことを特徴とする。

発明の効果

[0010] 本発明によれば、簡易な構成で安全な秘密分散が可能なエンコード方法、デコード方法、エンコーダ及びデコーダを提供することができる。

図面の簡単な説明

[0011] [図1]本発明の実施形態1に係るシステムの全体図である。

[図2]本発明の実施形態1に係る二次元コードを示す図であり、(a)は二次元コードの構成を示し、(b)は二次元割符コード及び復号した二次元コードの模式図を示す。

[図3]本発明の実施形態1に係るシステムのシーケンス図である。

[図4]本発明の実施形態2に係る二次元割符コードの適用例を示す図である。

[図5]本発明の実施形態3に係る二次元割符コードの適用例を示す図である。

発明を実施するための形態

[0012] (実施形態1)

以下、本発明の実施形態について、図を用いて説明する。図1は、実施形態1に係るシステム1の全体図である。本実施形態のシステム1では、使用者2が端末3を使用して認証装置4により認証を受け、認証装置4が端末3を所持する使用者2に各種のサービスを提供する。ここでは、認証装置4が現金自動預払機である場合に、使用者2が認証装置4から預貯金等のサービスを受ける例について説明する。また、端末3を使用する使用者2が真正か否かは、サーバ5から端末3及び認証装置4に対して配布される認証情報を認証装置4が取得することにより判定される。

[0013] 端末3は、携帯電話、スマートフォン、PDA、PC等の使用者2に紐付

いた装置である。端末3は、情報を表示可能な表示部31と、サーバ5との間でデータの送受信を行う送受信部32と、各種のデータを記憶する記憶部33とを有する。

[0014] 端末3は、パスワードによる認証や生体認証等により使用者2にログインさせてその機能を使用可能となるように構成される。また、端末3は、使用者2が保有する識別情報（ID）とパスワード等の認証情報によりサーバ5から認証を受けて、サーバ5とセキュアな通信を行うことができる。

[0015] サーバ5は、電子割符化した二次元コードを生成（エンコード）するエンコーダとしての機能を有し、その電子割符化した二次元コード（後述の二次元割符コード）を端末3及び認証装置4に対して配布する。二次元コードには、端末3が認証装置4から認証を受ける際に使用される認証情報が含まれる。また、サーバ5は、電子割符化した二次元コードの生成（エンコード）に使用する領域割当ポリシーを記憶する記憶部51を有する。

[0016] 認証装置4は、銀行サーバ6等と接続されており、預貯金等のサービスを提供するために必要な情報の送受信を銀行サーバ6との間で行うことができる。認証装置4とサーバ5の間にもセキュアな通信が確立している。認証装置4は、端末3、サーバ5及び銀行サーバ6から受信した二次元コード等のデータを記憶する記憶部41を備えている。また、認証装置4は、端末3やサーバ5から取得する電子割符化した二次元コードを復号（デコード）するデコーダとしての機能を有する。記憶部41にも、その二次元コードの復号に使用する領域割当ポリシーが記憶される。

[0017] 図2（a）は、本実施形態で使用される二次元コード7の構成を示す図である。二次元コード7は、二値化したデータが正形状の単位セルの形態でマトリクス状に格納されたデータ領域71と、データ領域71の4隅の外側に設置された画像切出パターン72（721～724）と、データ領域71を囲むようにデータ領域71の各辺の外側に配置された4本のスキニングガイド部73と、を備える。二次元コード7は全体が略正形状に形成される。

- [0018] スキャニングガイド部73は、データ領域71を四方から囲う線分K1～K4と、線分K1～K4からデータ領域71側へ向けて垂直な実線状に延設した突起部K10～K13、K20～K23、K30～K33、K40～K43を有する。突起部K10～K13、K20～K23、K30～K33、K40～K43は、各々略同じ長さに形成され、データ領域71のデータ密度或いはデータ領域71の面積に応じて増減させることができる。
- [0019] 画像切出パターン721は、一辺の長さが突起部K10～K13、K40～K43の長さと同じ正方形となるように形成され、黒く塗りつぶされている。画像切出パターン722は、左右端の短辺の長さが突起部K10～K13の長さと同じ長方形となるように形成される。また、画像切出パターン722の右端には1辺の長さを突起部K10～K13、K20～K23の長さと同じになるように黒く塗りつぶした正方形のパターンが配置される。
- [0020] 画像切出パターン723は、黒く塗りつぶされたL字状に形成される。画像切出パターン723の左下側端部及び右上側端部の短辺は、突起部K20～K23、K30～K33の長さと同じになるように形成される。画像切出パターン724は、上下端の短辺の長さが突起部K40～K43の長さと同じ長方形となるように形成される。また、画像切出パターン724の下端には1辺の長さを突起部K30～K33、K40～K43の長さと同じになるように黒く塗りつぶした正方形のパターンが配置される。
- [0021] データ領域71のセルの検出は、突起部K10～K13、K20～K23、K30～K33、K40～K43を基準に走査用のガイドラインを仮想的に形成して走査方向の補正をした後に、その走査方向データ領域71内を走査することによって行うことができる。
- [0022] 図2(b)は、二次元割符コード7A、7B及び復号した二次元コード7Cを模式的に示す図である。なお、本図ではデータ領域71、画像切出パターン72及びスキャニングガイド部73の明暗パターンの図示を省略しており、実線の枠は画像切出パターン72及びスキャニングガイド部73の外形線を示し、破線の枠はデータ領域71の外形線を示している。二次元割符コ

ード7 A, 7 Bは、データ領域7 1として一点鎖線で示す有効領域7 1 1及びダミー領域7 1 2を含む。

[0023] 二次元割符コード7 A（第1二次元割符コード）は図1のサーバ5により生成されて、端末3に送信されるコードである。二次元割符コード7 Aでは、データ領域7 1の左下の略直角二等辺三角形形状に形成された領域に有効領域7 1 1 A（第1有効領域）が形成され、データ領域7 1の右上の略直角二等辺三角形形状に形成された領域にダミー領域7 1 2 A（第1ダミー領域）が形成される。有効領域7 1 1 Aには、識別情報（例えば、端末3や使用者に紐付いた識別情報、認証装置4の取引識別情報、等）や認証情報（パスワード等）などの伝達情報が第1分散情報として電子割符化されて含まれる。第1分散情報には、タイムスタンプ及び端末3の位置情報等を含めてもよい。

[0024] 二次元割符コード7 B（第2二次元割符コード）は図1のサーバ5により生成されて、認証装置4に送信される情報である。二次元割符コード7 Bでは、データ領域7 1の右上の略直角二等辺三角形形状に形成された領域に有効領域7 1 1 B（第2有効領域）が形成され、データ領域7 1の左下の略直角二等辺三角形形状に形成された領域にダミー領域7 1 2 B（第2ダミー領域）が形成される。また、二次元割符コード7 Bの例でも、識別情報（例えば、端末3や使用者に紐付いた識別情報、認証装置4の取引識別情報、等）や認証情報（パスワード等）などの伝達情報が前述の第1分散情報と対応する第2分散情報として電子割符化されて含まれる。第2分散情報にも、タイムスタンプ及び端末3の位置情報等を含めてもよい。二次元割符コード7 Bの有効領域7 1 1 Bは、二次元割符コード7 Aのダミー領域7 1 2 Aに対応する位置に配置され、二次元割符コード7 Bのダミー領域7 1 2 Bは二次元割符コード7 Aの有効領域7 1 1 Aに対応する位置に配置される。従って、本実施形態では、第1有効領域7 1 1 Aと第1ダミー領域7 1 2 Aの合計セル数と、第2有効領域7 1 1 Bと第2ダミー領域7 1 2 Bの合計セル数とは同じである。

[0025] ダミー領域7 1 2 A, 7 1 2 Bには、例えば、有効領域7 1 1 A, 7 1 1

Bとの視別が困難なランダムな明暗パターンを配置することができる。図2 (b) の二次元割符コード7 A及び二次元割符コード7 Bでは、第1有効領域7 1 1 A、第1ダミー領域7 1 2 A、第2有効領域7 1 1 B及び第2ダミー領域7 1 2 Bが、各々集合した略直角二等辺三角形形状の領域である。

[0026] また、二次元コード7 Cは、図2 (b) に示した二次元割符コード7 Aの有効領域7 1 1 Aと二次元割符コード7 Bの有効領域7 1 1 Bとを切り出して、有効領域7 1 1 A及び有効領域7 1 1 Bを切り出し前の二次元割符コード7 A、7 Bにおける位置と対応する位置に配置して、データ領域7 1の画像として結合することにより生成される。二次元コード7 Cには、2つの有効領域7 1 1 A、7 1 1 Bが結合されたデータ領域7 1に認証情報等が含まれており、認証装置4は二次元コード7 Cを撮影してデコーダによりデコードすると、データ領域7 1内の認証情報等を取得することができる。

[0027] 次に、本実施形態の認証処理の方法について説明する。図3はシステム1のシーケンス図である。ステップS 3 1の初期設定として、端末3は、使用者2を認証して操作を許可し、サーバ5からもログイン等の認証を受けてサーバ5との通信を可能とする処理を予め行う。

[0028] ステップS 3 2で、端末3は、認証情報の取得要求T 1をサーバ5に対して送信する。取得要求T 1には、端末3の位置情報を含めて送信することができる。

[0029] ステップS 5 1で、サーバ5は、認証情報等の一部を第1分散情報として有効領域7 1 1 Aに含めた二次元割符コード7 Aを生成（エンコード）して、端末3に送信する（T 2）。有効領域7 1 1 Aの形状及び位置は、サーバ5の記憶部5 1内に予め設定された領域割当ポリシーに従って割り当てられ、本実施形態では図5 (b) に示すようにデータ領域7 1の左下側に配置される。また、二次元割符コード7 Aの有効領域7 1 1 Aには、前述の第1分散情報が含まれる。端末3は、サーバ5から二次元割符コード7 Aを受信すると、ステップS 3 3で二次元割符コード7 Aを端末3の記憶部3 3内に記憶する。

- [0030] 一方、サーバ5は、ステップS52で、二次元割符コード7Bを生成（エンコード）して端末3に送信する（T3）。二次元割符コード7Bの有効領域711Bには、前述の第2分散情報が含まれる。認証装置4は、サーバ5から二次元割符コード7Bを受信すると、ステップS41で二次元割符コード7Bを記憶部41に記憶する。
- [0031] ステップS34で、端末3は、二次元割符コード7Aを表示部31に表示する。ステップS42で、使用者2の操作等により画像の読取を可能とさせた認証装置4は、端末3が表示した二次元割符コード7Aを撮像する。認証装置4は、表示部31に表示された二次元割符コード7Aを読取り、記憶部41に記憶する。
- [0032] ステップS43で、認証装置4は、記憶部41内に予め記憶されている領域割当ポリシーに従って、二次元割符コード7Aから有効領域711Aの画像を切り出すとともに、二次元割符コード7Bから有効領域711Bの画像を切り出す。そして、図2（b）に示すように、認証装置4は、有効領域711Aと有効領域711Bとを合成したデータ領域71を有する復号した二次元コード7Cを生成することができる。これにより、有効領域711Aに含まれていた第1分散情報と、有効領域711Bに含まれていた第2分散情報とが、画像結合され、認証装置4が復号されたデータ領域71のデータを取得可能な状態となる。
- [0033] 認証装置4は、復号した二次元コード7Cのデータ領域71に含まれる認証情報が、記憶部41等に記憶した認証条件を満たすか判定する。そして、認証装置4は、データ領域71の復号された認証情報が認証条件を満たす場合にステップS44の処理に進むことができる。また、認証装置4は、二次元コード7Cのデータ領域71に含まれるタイムスタンプの時刻と現在時刻との差分が予め定めた閾値以内である場合にステップS44の処理に進むように処理してもよいし、二次元コード7Cの有効領域711に含まれる位置情報の位置と、認証装置4の位置とが予め定めた閾値以内である場合にステップS44の処理に進むように処理してもよい。すなわち、認証装置4は、

認証のタイミングや端末3の位置によって、使用者2に対するサービスの提供可否を定めることができる。

[0034] ステップS44で、認証装置4は、端末3を所持した使用者2に対してサービスの提供を行う。例えば、認証装置4は、適宜銀行サーバ6から預貯金データ等を参照して、現金の預け払い処理を行うことができる。

[0035] 以上示したサーバ5のエンコード方法及び認証装置4のデコード方法によれば、使用者2は端末3に表示させた二次元コードをかざして認証装置4への認証操作を容易に行うことができる。また、二次元コードの画像データが端末3への送信中に盗聴されても、他方の二次元割符コード7Bが配布されていない認証装置に意図せず認証されることを防止できる。また、端末3が取得した二次元割符コード7Aをスクリーンショットや紙媒体に印刷しても、タイムスタンプにより認証可能な期間を時限設定することが可能であるため、認証装置4へのアクセス制限を容易に行うことができる。

[0036] なお、認証装置4は、ステップS45において、サーバ5から二次元割符コード7Bと共に領域割当ポリシーを受信する構成としてもよい。また、ステップS51においてサーバ5が端末3に領域割当ポリシーを送信して、端末3が予め搭載したエンコーダにより二次元割符コード7Aを生成する構成としてもよい。

[0037] (実施形態2)

次に実施形態2について説明する。図4は、野菜や果物などの生産物を小売店等に配送する流通システム8を示す図である。本実施形態は、3つ以上の二次元割符コード7D~7Gの全てを読み込むことで復元可能な二次元コード7Hの例について説明する。なお、実施形態1と同様の構成についてはその説明を簡略化又は省略する。

[0038] 流通システム8は、各工程S81~S84に対応したエンコーダとしての装置8D~8Gを備えている。装置8D~8Gは予め設定された領域割当ポリシーに従って有効領域711D~711Gを配置した二次元割符コード7D~7Gを生成(エンコード)して生産物の包装等に付して、二次元割符コ

ード7D～7Gと生産物に紐づけることができる。

[0039] 第一工程S81では、生産物が生産されて出荷前検査及び包装がされ、生産地から第一中間卸し等の第二工程S82に向けて配送される。また、第一工程S81では、二次元割符コード7Dが生成されて生産物の包装等に付加される。二次元割符コード7Dの有効領域711Dには、例えば、生産者、生産地及び生産方法等の生産物情報、生産物の検査情報、出荷履歴、及び生産時や出荷時のタイムスタンプが伝達情報として含まれる。また、有効領域711Dには認証情報を分散情報として含めることができる。

[0040] 第二工程S82では、第一工程S81から集荷された生産物が第二中間卸し等の第三工程S83に向けて配送される。第二工程S82では流通経路の中間履歴として流通識別番号や記号等が採番される。第二工程S82では、二次元割符コード7Eが生成されて生産物の包装等に付加される。二次元割符コード7Eの有効領域711Eには、例えば、流通経路の中間履歴として流通識別情報、及び集荷時や出荷時のタイムスタンプが伝達情報として含まれる。有効領域711Eにも認証情報を分散情報として含めることができる。

[0041] 第三工程S83では、第二工程S82から集荷された生産物を第三中間卸し等の第四工程S84に向けて配送される。第三工程S83においても流通経路や単位ロットの容量等に応じて、ロット分割等が行われて、流通の中間履歴として流通識別番号や記号などが採番される。第三工程S83では、二次元割符コード7Fが生成されて生産物の包装等に付加される。二次元割符コード7Fの有効領域711Fには、例えば、包装情報、流通識別番号、及びタイムスタンプを伝達情報として含めることができる。ここでいう包装情報としては、例えば、生産物が流通過程で分割された包装単位ごとに設定された再包装ラベルの分割包装番号や小売りパックの番号とすることができる。また、有効領域711Fにも認証情報を分散情報として含めることができる。

[0042] 第四工程S84では、第三工程S83から集荷された生産物に対し流通経

路や小売りの単位に応じたロット分割等が行われて小売店等に配送される。第四工程 S 8 4 では、二次元割符コード 7 G が生成されて生産物の包装等に付加される。二次元割符コード 7 G の有効領域 7 1 1 G には、例えば、包装情報及び集荷時や出荷時等のタイムスタンプが伝達情報として含まれる。また、有効領域 7 1 1 にも認証情報を分散情報として含めることができる。

[0043] 本実施形態では、デコーダを備えた装置 8 H により二次元割符コード 7 D ~ 7 G が撮像されて読み込まれる。装置 8 H は、予め定めた領域割当ポリシーに従って各二次元割符コード 7 D ~ 7 G から各有効領域 7 1 1 D ~ 7 1 1 G を切り出して、有効領域 7 1 1 D ~ 7 1 1 G を切り出し前の二次元割符コード 7 D ~ 7 G における位置と対応する位置に配置して、二次元コード 7 H のデータ領域 7 1 の画像として結合する。したがって、装置 8 H は、各有効領域 7 1 1 D ~ 7 1 1 G に含まれていた分散情報から合成された認証情報を取得することができ、例えば、その認証情報が認証条件を満たす場合に、各工程 S 8 1 ~ S 8 4 で付加された伝達情報を取得することができる。

[0044] 以上、本実施形態のエンコード方法及びデコード方法では、各工程 S 8 1 ~ S 8 4 において二次元割符コード 7 D ~ 7 G の有効領域に個別に工程情報を付加することを可能としながら、各工程情報の複数の二次元割符コード 7 D ~ 7 G が全て揃うと取得可能とすることができる。よって、情報の取得が可能となるタイミングを予め設定することができ、簡易な構成で安全な情報伝達を行うことができる。

[0045] (実施形態 3)

次に実施形態 3 について説明する。実施形態 1 及び実施形態 2 では、配布される二次元割符コードの数である分割数と、読取可能な二次元コードの復号に必要な二次元割符コードの数である閾値とが、同じである場合について説明したが、本実施形態では分割数が閾値よりも大きくなるように二次元割符コードを生成して配布する例について説明する。

[0046] 図 5 は、二次元割符コードの適用例を示す図である。図 5 には、二次元割符コード 7 I ~ 7 K と二次元コード 7 L とを模式的に示している。

- [0047] 例えば、3つの二次元割符コード7 I ~ 7 Kを適宜のエンコーダによりエンコードして任意の媒体に分散保有させる。そして、例えば分散情報として、二次元割符コード7 Iの有効領域7 1 1にはデータ「A」、 「B」が含まれ、二次元割符コード7 Jの有効領域7 1 1にはデータ「B」、 「C」が含まれ、二次元割符コード7 Kの有効領域7 1 1にはデータ「C」、 「A」が含まれるように構成する。
- [0048] 従って、情報の取得手段である図示しないデコーダは、いずれかの2つの二次元割符コード（例えば、二次元割符コード7 Iと二次元割符コード7 K）を取得すれば、元の情報である「A」、 「B」、 「C」を含む二次元コード7 Lを復号（デコード）することができる。なお、二次元コード7 Lにおいて分散情報が配置されない余剰領域7 1 a, 7 1 bには二次元コード7 Lの読み取り可否に影響を与えない任意のパターンを表示させることができる。本実施形態のエンコード方法及びデコード方法により、情報伝達の冗長性を確保することができる。
- [0049] 以上、各実施形態に示したエンコード方法及びデコード方法では、二次元割符コードにおいて有効領域7 1 1とダミー領域7 1 2とが、視別困難であるため、単独でデコード可能な二次元コードであるのか、或いはどの二次元割符コードと組み合わせて復号可能なのかを客観的に判定することができない。よって、簡易な構成で安全に秘密分散を行うことができる。
- [0050] なお、各二次元割符コードの有効領域に含まれるデータとして、一方の二次元割符コードの有効領域7 1 1には暗号化した情報を埋め込み、他方の二次元割符コードの有効領域7 1 1には暗号鍵を含めるように構成してもよい。
- [0051] また、図2（b）の二次元割符コード7 A及び二次元割符コード7 Bの例において、第1有効領域7 1 1 A、第1ダミー領域7 1 2 A、第2有効領域7 1 1 B及び第2ダミー領域7 1 2 Bは、各々2つ以上の島を有して離散配置させる構成としてもよい。実施形態2及び実施形態3においても同様に有効領域とダミー領域を各々離散配置させてもよい。

[0052] また、以上説明した実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の趣旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これらの実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

符号の説明

[0053]	1	システム	2	使用者
	3	端末	4	認証装置
	5	サーバ	6	銀行サーバ
	7, 7 C, 7 H, 7 L	二次元コード		
	7 A, 7 B, 7 D~7 G, 7 I~7 K	二次元割符コード		
	8	流通システム	8 D~8 H	装置
	3 1	表示部	3 2	送受信部
	3 3	記憶部	4 1	記憶部
	5 1	記憶部	7 1	データ領域
	7 1 a	余剰領域	7 1 b	余剰領域
	7 2	画像切出パターン	7 3	スキャニングガイド部
	7 1 1	有効領域	7 1 1 A	第1有効領域
	7 1 1 B	第2有効領域	7 1 1 D	有効領域
	7 1 1 E	有効領域	7 1 1 F	有効領域
	7 1 1 G	有効領域	7 1 2	ダミー領域
	7 1 2 A	第1ダミー領域	7 1 2 B	第2ダミー領域
	7 2 1	画像切出パターン	7 2 2	画像切出パターン
	7 2 3	画像切出パターン	7 2 4	画像切出パターン
	K 1~K 4	線分	K 1 0~K 1 3	突起部
	K 2 0~K 2 3	突起部	K 3 0~K 3 3	突起部
	K 4 0~K 4 3	突起部		

請求の範囲

- [請求項1] エンコーダによる二次元コードのエンコード方法であって、
前記エンコーダが、
予め定めた領域割当ポリシーに従って、第1分散情報を含む第1有効領域と、第1ダミー領域とを有する第1二次元割符コードを生成し、
第2分散情報を含み前記第1ダミー領域の位置に配置される第2有効領域と、前記第1有効領域の位置に配置される第2ダミー領域とを有する第2二次元割符コードを生成する、
ことを特徴とするエンコード方法。
- [請求項2] 前記第1分散情報及び前記第2分散情報は、伝達情報として認証情報を含むことを特徴とする請求項1に記載のエンコード方法。
- [請求項3] 前記第1分散情報及び前記第2分散情報は、タイムスタンプ及び／又は位置情報と、前記タイムスタンプ及び／又は前記位置情報が予め定めた閾値を満たす場合にデコーダによりデコードされる伝達情報と、を含むことを特徴とする請求項1又は請求項2に記載のエンコード方法。
- [請求項4] 前記第1有効領域と前記第1ダミー領域の合計セル数と、前記第2有効領域と前記第2ダミー領域の合計セル数とは同じであることを特徴とする請求項1乃至請求項3の何れかに記載のエンコード方法。
- [請求項5] 前記第1有効領域、前記第1ダミー領域、前記第2有効領域及び前記第2ダミー領域は、各々集合した領域であることを特徴とする請求項1乃至請求項4の何れかに記載のエンコード方法。
- [請求項6] デコーダによる二次元コードのデコード方法であって、
前記デコーダが、
予め定めた領域割当ポリシーに従って生成された、第1分散情報を含む第1有効領域と、第1ダミー領域とを有する第1二次元割符コードを取得し、

第2分散情報を含み前記第1ダミー領域の位置に配置される第2有効領域と、前記第1有効領域の位置に配置される第2ダミー領域とを有する第2二次元割符コードを取得し、

前記領域割当ポリシーに従って前記第1有効領域及び前記第2有効領域を切り出し、

前記第1有効領域及び前記第2有効領域を切り出し前の位置と対応する位置に配置して前記二次元コードのデータ領域として結合する、ことを特徴とするデコード方法。

[請求項7]

予め定めた領域割当ポリシーに従って、第1分散情報を含む第1有効領域と、第1ダミー領域とを有する第1二次元割符コードを生成し、

第2分散情報を含み前記第1ダミー領域の位置に配置される第2有効領域と、前記第1有効領域の位置に配置される第2ダミー領域とを有する第2二次元割符コードを生成する、

ことを特徴とする二次元コードのエンコーダ。

[請求項8]

予め定めた領域割当ポリシーに従って生成された、第1分散情報を含む第1有効領域と、第1ダミー領域とを有する第1二次元割符コードを取得し、

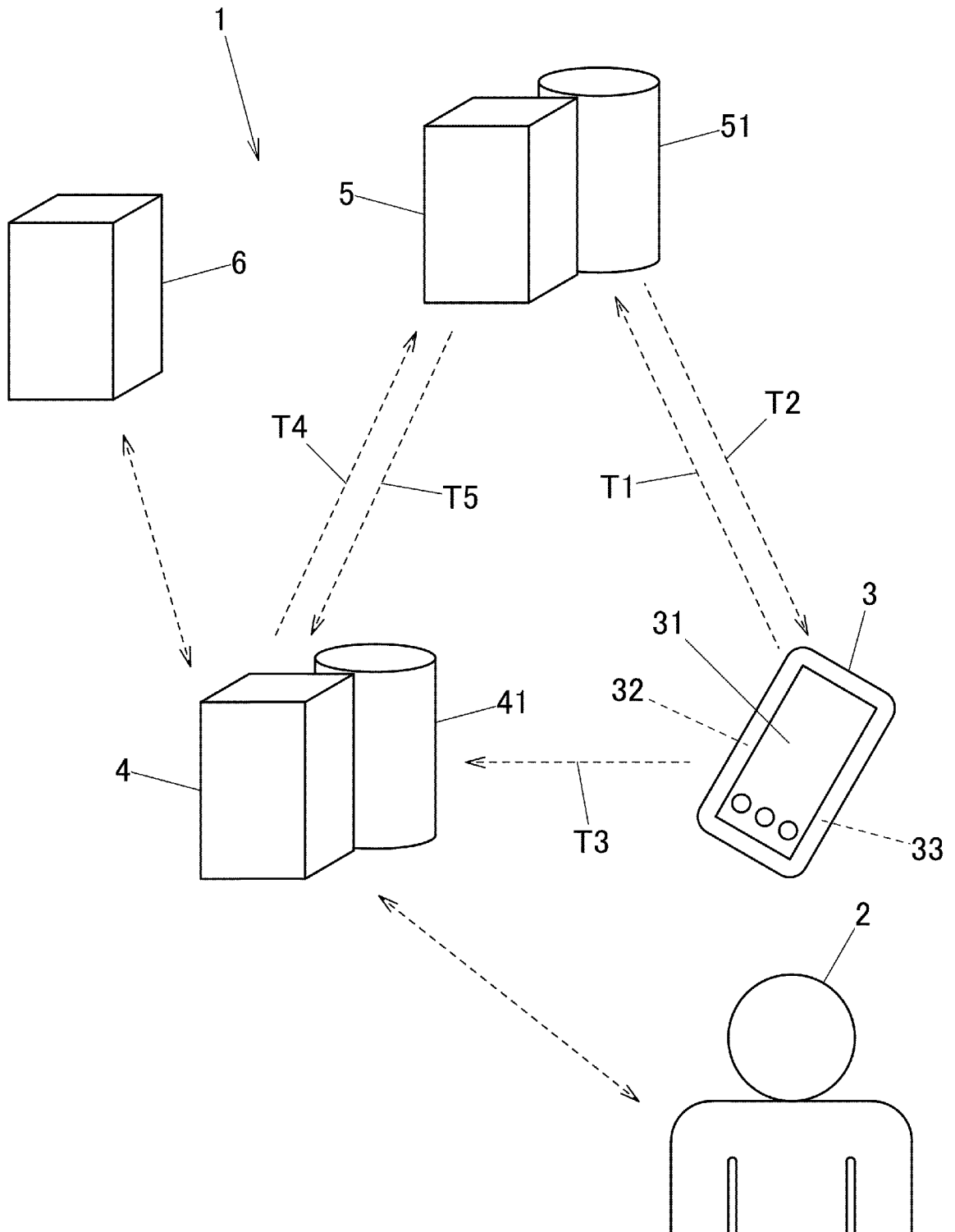
第2分散情報を含み前記第1ダミー領域の位置に配置される第2有効領域と、前記第1有効領域の位置に配置される第2ダミー領域とを有する第2二次元割符コードを取得し、

前記領域割当ポリシーに従って前記第1有効領域及び前記第2有効領域を切り出し、

前記第1有効領域及び前記第2有効領域を切り出し前の位置と対応する位置に配置して二次元コードのデータ領域として結合する、

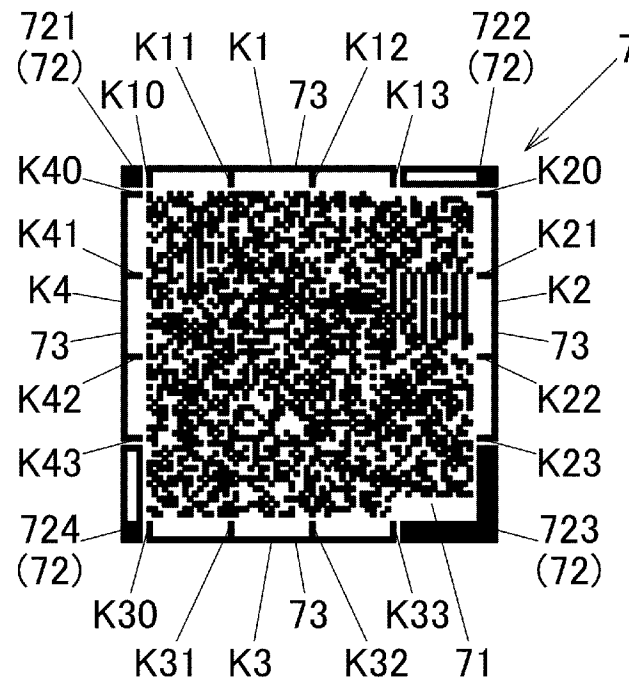
ことを特徴とする二次元コードのデコーダ。

[図1]

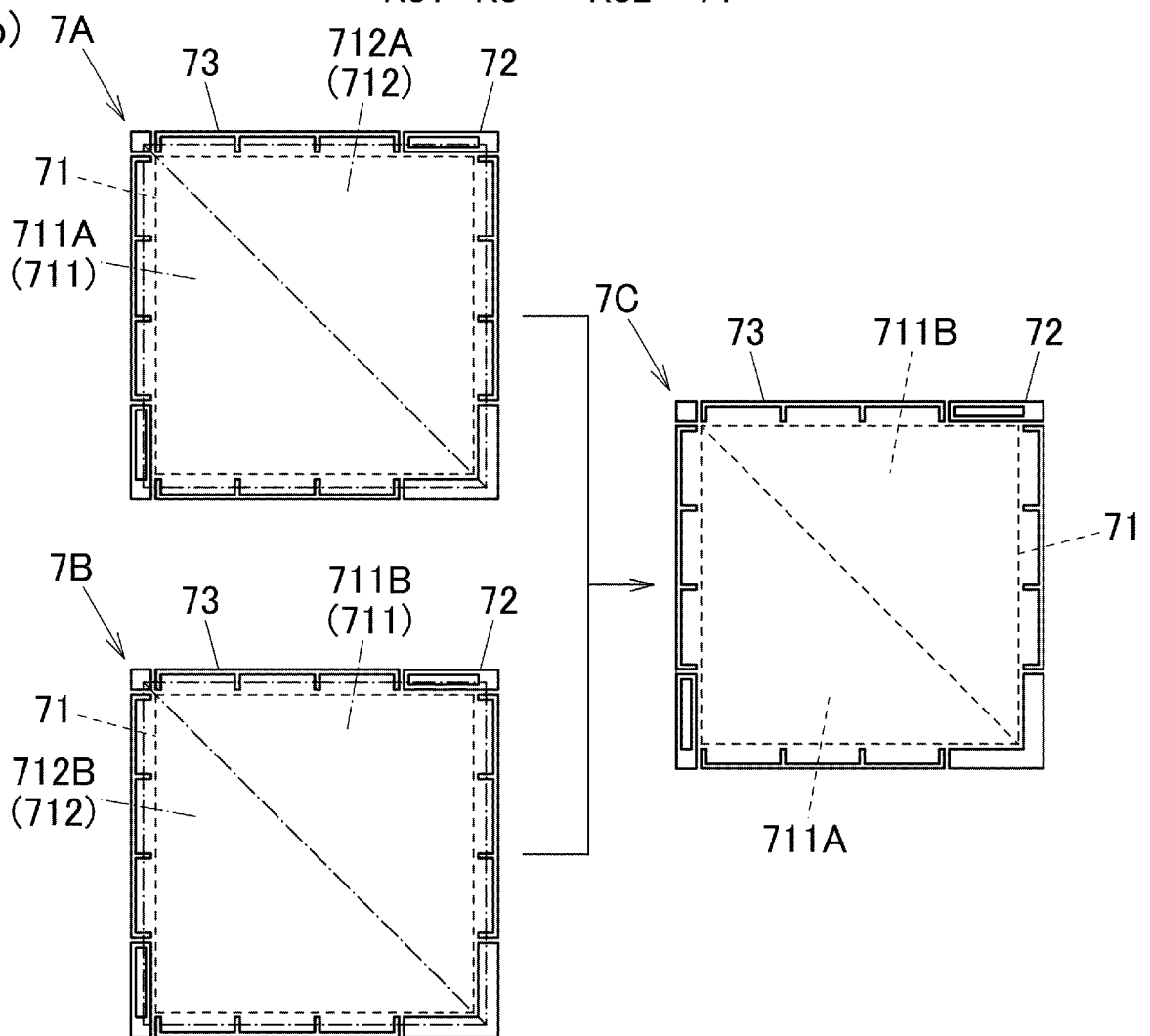


[図2]

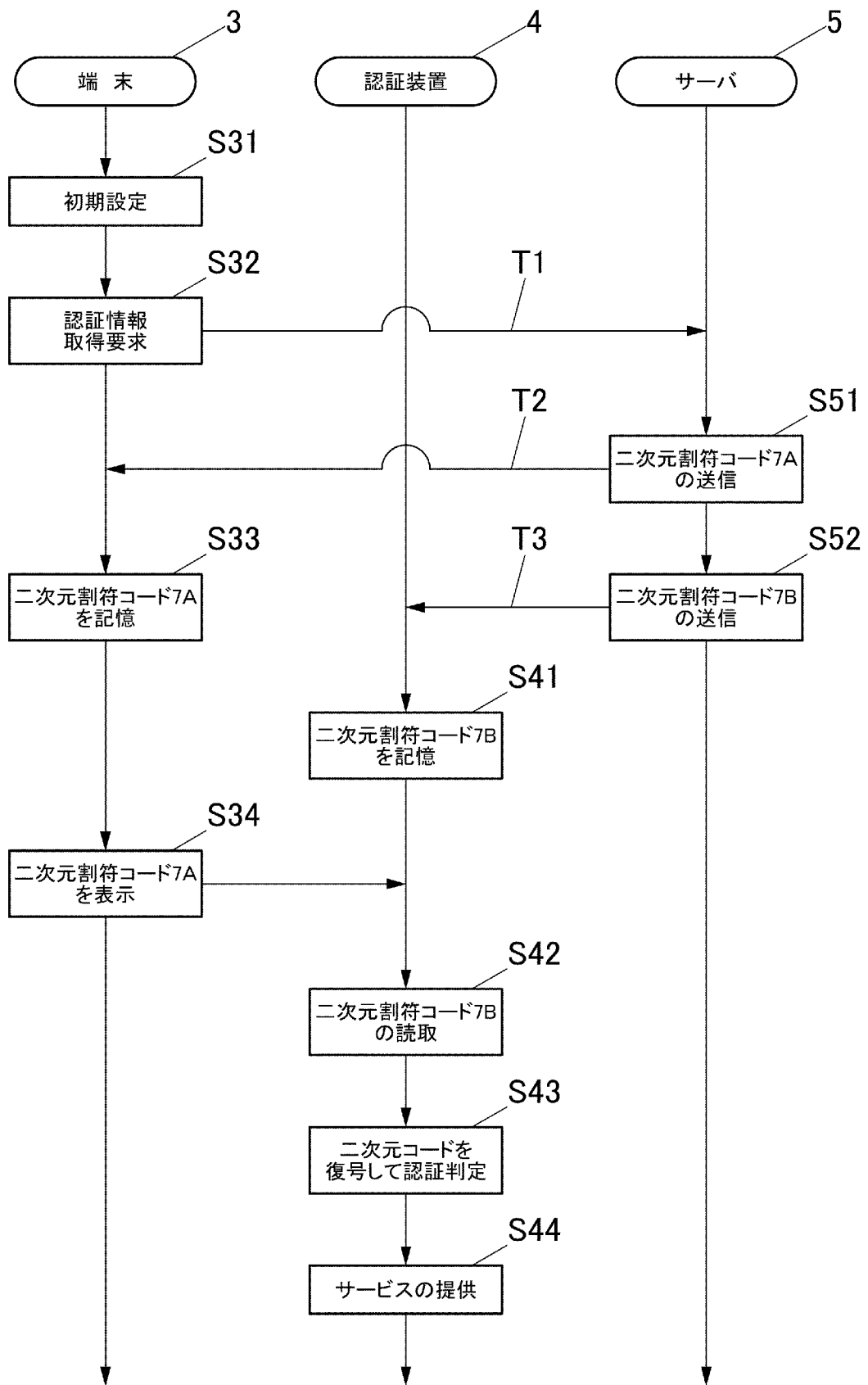
(a)



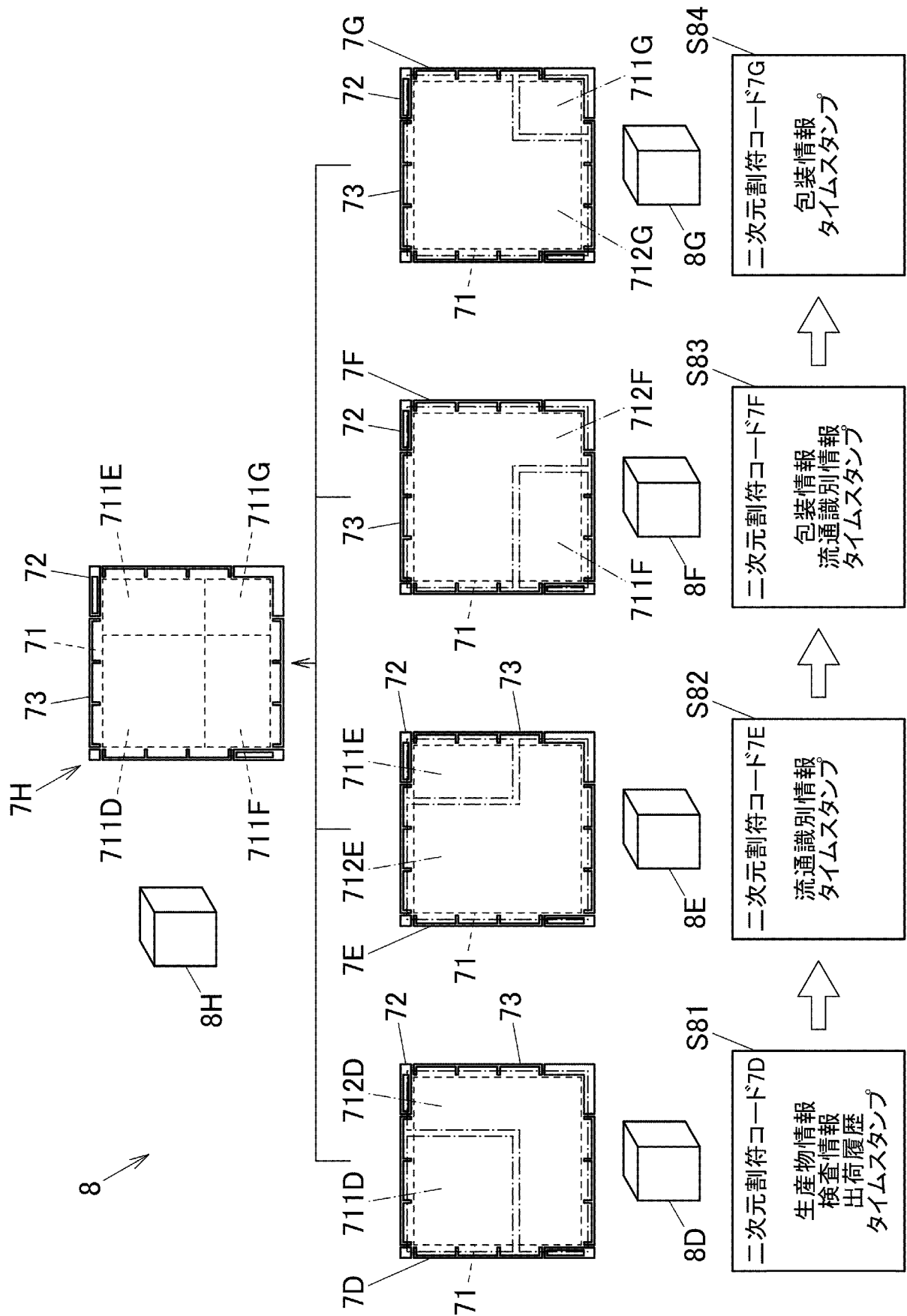
(b)



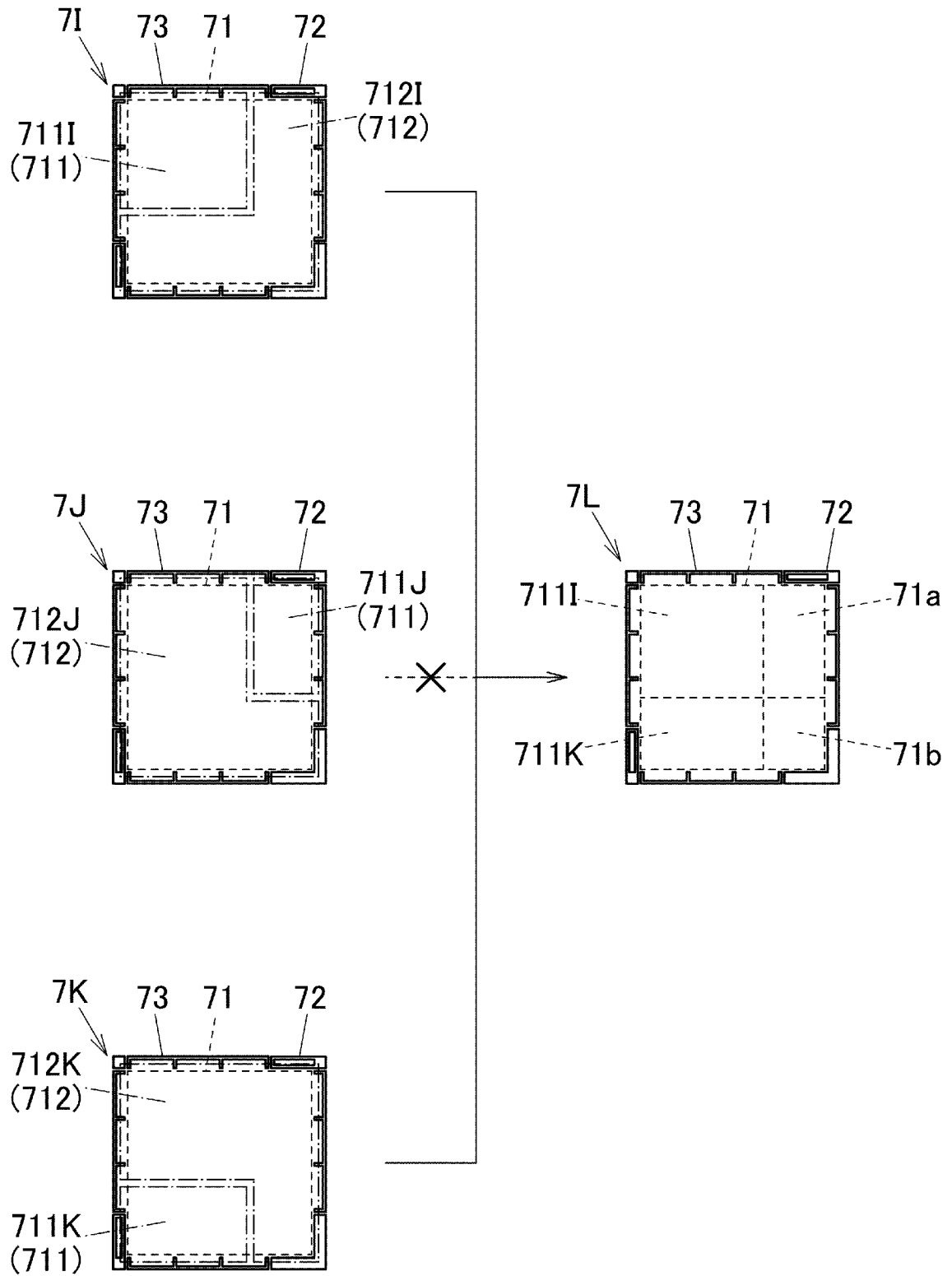
[図3]



[図4]



[図5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2018/040733

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. G06K19/06(2006.01) i, G06K1/12(2006.01) i, G06K7/14(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)

Int. Cl. G06K19/06, G06K1/12, G06K7/14

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

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2019
 Registered utility model specifications of Japan 1996-2019
 Published registered utility model applications of Japan 1994-2019

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.
Y	JP 2006-195912 A (DENSO WAVE INC.) 27 July 2006, paragraphs [0021]-[0056], fig. 1-14 (Family: none)	1-8
Y	JP 2016-178495 A (FUJITSU FRONTECH LTD.) 06 October 2016, paragraphs [0065]-[0071], fig. 9, 10 (Family: none)	1-8
Y	JP 2017-199110 A (MICE ONE CORP.) 02 November 2017, paragraphs [0051]-[0066], fig. 9-11 (Family: none)	3
A	JP 3145609 U (MATSUYAMA SEAL INSATSU CORP.) 24 September 2008, entire text, all drawings (Family: none)	1-8

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	"I" 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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search
04.01.2019

Date of mailing of the international search report
15.01.2019

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））
 Int.Cl. G06K19/06(2006.01)i, G06K1/12(2006.01)i, G06K7/14(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. G06K19/06, G06K1/12, G06K7/14

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	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019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
Y	JP 2006-195912 A（株式会社デンソーウェーブ）2006.07.27, [0021] - [0056] 及び図1-14（ファミリーなし）	1-8
Y	JP 2016-178495 A（富士通フロンテック株式会社）2016.10.06, [0065] - [0071] 及び図9, 10（ファミリーなし）	1-8
Y	JP 2017-199110 A（株式会社マイス・ワン）2017.11.02, [0051] - [0066] 及び図9-11（ファミリーなし）	3

☑ 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	の日の後に公表された文献
「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	「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
「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	「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
「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）	「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
「O」口頭による開示、使用、展示等に言及する文献	「&」同一パテントファミリー文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願	

国際調査を完了した日 04.01.2019	国際調査報告の発送日 15.01.2019
国際調査機関の名称及びあて先 日本国特許庁（ISA/J P） 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） 境 周一 電話番号 03-3581-1101 内線 3586

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 3145609 U (有限会社松山シール印刷) 2008.09.24, 全文及び全 図面 (ファミリーなし)	1-8