

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005 年 11 月 10 日 (10.11.2005)

PCT

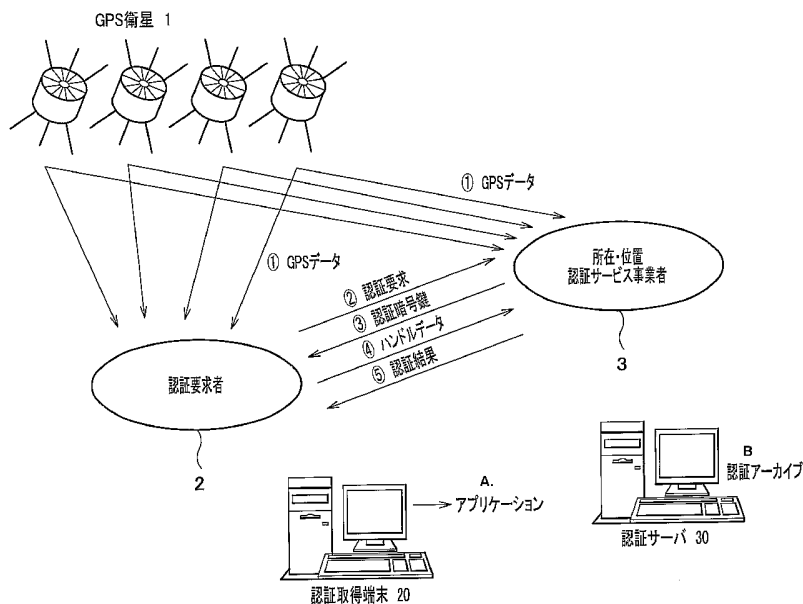
(10) 国際公開番号
WO 2005/107147 A1

- (51) 国際特許分類: H04L 9/32, 9/08, (72) 発明者; および
H04N 5/232, 5/225, 5/92, G06F 17/60 (75) 発明者/出願人 (米国についての): 山田 進一 (YAMADA, Shinichi) [JP/JP]; 〒1018010 東京都千代田区
(21) 国際出願番号: PCT/JP2004/006222 神田駿河台四丁目6番地 株式会社日立製作所 トータルソリューション事業部内 Tokyo (JP). 升山 義弘 (MASUYAMA, Yoshihiro) [JP/JP]; 〒1018010 東京都千代田区神田駿河台四丁目6番地 株式会社日立製作所 トータルソリューション事業部内 Tokyo (JP).
(22) 国際出願日: 2004 年 4 月 28 日 (28.04.2004)
(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 (米国を除く全ての指定国について): 株式会社日立製作所 (HITACHI, LTD.) [JP/JP]; 〒100-8280 東京都千代田区丸の内一丁目6番6号 Tokyo (JP). (74) 代理人: 磯野 道造 (ISONO, Michizo); 〒1020093 東京都千代田区平河町2丁目7番4号 砂防会館別館内 磯野国際特許商標事務所気付 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, AT, AU, AZ, BA, BB, BG, BR,

[続葉有]

(54) Title: AUTHENTICATION SYSTEM, AUTHENTICATION ACQUISITION DEVICE, AND AUTHENTICATION METHOD

(54) 発明の名称: 認証システムおよび認証取得装置ならびに認証方法



- 1.. GPS SATELLITE
(1).. GPS DATA
(2).. AUTHENTICATION REQUEST
(3).. AUTHENTICATION ENCRYPTION KEY
(4).. HANDLE DATA
(5).. AUTHENTICATION RESULT
2.. PERSON WHO REQUESTS AUTHENTICATION
3.. UBIETY/POSITION AUTHENTICATION SERVICE COMPANY
A.. APPLICATION
20.. AUTHENTICATION ACQUISITION TERMINAL
B.. AUTHENTICATION ARCHIVE
30.. AUTHENTICATION SERVER

(57) Abstract: An authentication system includes: an authentication acquisition device (digital camera (40)) for acquiring the current position data on the object-to-be-positioned received from electronic positioning means and the time data and generating unified data made from these data and an authentication encryption key received from an authentication device (authentication server (30)) when an authentication request is issued; and the authentication device (authentication server (30)) for acquiring the unified data from the authentication acquisition device (digital camera (40)) and performing authentication of the position information and the time information by using the authentication encryption key.

(57) 要約: 電子的な位置測位手段から受信した測位対象の現在位置データ、および時刻データを取り込み、これらデータと、認証要求発行時、認証装置(認証サーバ30)から受信した認証暗号鍵とを一体化したデータを生成する認証取得装置(デジタルカメラ40)と、認証取得装置(デジ

タルカメラ40)から前記一体化したデータを取得し、認証暗号化鍵を用いて前記位置情報と時刻情報の認証を行う認証装置(認証サーバ30)と、

[続葉有]



BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

(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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG,

2 文字コード及び他の略語については、定期発行される各 *PCT* ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

1

明 細 書

認証システムおよび認証取得装置ならびに認証方法

技術分野

- 5 本発明は、GPS等、電子的な位置測位手段によって得られる位置情報や時刻情報を認証して各種アプリケーションに引き渡す、認証システムおよび認証取得装置ならびに認証方法に関する。

背景技術

- 10 所在位置確認の対象となる物体等の現在位置をGPS（Global Positioning System）等、電子的な位置測位手段を介して取得し、そのデータを公的に認証する技術について、従来から多数提案され、出願されている。

- 例えば、デジタルカメラやパソコン等の可搬性電子機器に関し、GPSから位置と時刻情報を得、これらをセンタへ送信し、センタがコピーガードされた場所
15 と時間データを要求のあった電子機器へ送信する技術（特開2001-33537号公報）、入力した地点を特定する位置情報と時間情報を生成し、認証情報として入力データに付加すると共に、認証局へ送信してデジタル署名を付加する技術（特開2001-100632号公報）が知られている。

- いずれもデータの客観性を確保することにより、交通事故等の際の保険請求を
20 はじめ、警察、消防等の現場検証に広く実施可能であり、証拠としての証明力を向上させるための手段として大きな効果が得られる。しかしながら、いずれも認証局等のセンタ処理が中心であるため、センタ負荷が大きく、このため、現場での所在確認に時間を要していた。また、デジタルカメラによって撮影されたデジタル画像は改竄が容易であり、その保管の仕方によっては証拠能力に疑問が残り、
25 依然として客観性に乏しいものであった。

従って本発明の第1の課題は、センタの認証装置と現場の認証取得端末間で適

2

当に負荷分散することにより、現場での所在確認を容易とした、認証システムおよび認証取得装置ならびに認証方法を提供することにある。また、本発明の第2の課題は、デジタルカメラ等により撮影された画像についてもその真性を維持し、撮影から記録まで一貫したセキュリティを実現する、認証システムおよび認証取得装置ならびに認証方法を提供することにある。

発明の開示

前記した課題を解決するために、本発明の認証システムは、認証取得装置が、GPS等の電子的な位置測位手段から受信した測位対象の現在位置データ、および時刻データと、認証要求発行時に認証装置から受信した認証暗号鍵とを一体化したデータを生成する。そしてこの一体化したデータを、ネットワークを介して接続される認証装置へ送信し、認証装置が認証暗号化鍵を用いて位置情報と時刻情報の認証を行い、認証要求のあった認証取得装置へ返信する。

このことにより、センタの認証サーバと現場の認証取得装置間で負荷が分散され、現場での所在確認を容易とした認証システムを提供することができる。

また、撮像装置を含む認証取得装置が、現在時刻に同期した撮像素子の駆動タイミング信号を生成し、当該駆動タイミング信号に、認証装置から送信される認証暗号鍵情報、ならびに位置測位手段から取得した測位対象の現在位置情報を重畳してセキュリティマーキング信号を生成する。そして、撮像装置から出力される画像情報を、セキュリティマーキング情報を含む暗号化情報として追記型記録媒体に記録する。このことにより、デジタルカメラ等により撮影された画像についてもその真性を維持し、撮影から記録まで一貫したセキュリティを実現することができる。

25 図面の簡単な説明

第1図は、本発明の位置認証方法とその利用主体を説明するために引用した図

である。

第2図は、本発明の認証システムの全体動作を説明するために引用した動作シーケンス図である。

第3図は、本発明の認証取得装置の動作を示すフローチャートである。

5 第4図は、本発明の認証システムの動作を示すフローチャートである。

第5図は、本発明の認証取得装置の内部構成を機能展開して示したブロック図である。

第6図は、本発明の認証システムの内部構成を機能展開して示したブロック図である。

10 第7図は、本発明の認証取得装置の応用例を概念的に示した図である。

第8図は、第7図に示す画像真性処理部の内部構成を示すブロック図である。

第9図は、第8図に示す画像真性処理部の動作を示すフローチャートである。

第10図は、第8図に示す画像真性処理部のうち、色補正処理に係わる部分を抽出して示したブロック図である。

15

発明を実施するための最良の形態

以下、本発明の実施形態について図面を参照しながら詳細に説明する。第1図は、本発明の位置認証方法とその利用主体を説明するために引用した図である。

20 第1図において、符号1はGPS衛星であり、3以上のGPS衛星1から発せられる電波を受信することにより三角測量の原理で距離を測定し、緯度、経度、高度からなる現在位置情報ならびに標準時間を測定する電子的な測位手段として用いられる。なお、電子的な測位手段としては、他に、FM (Frequency Modulation) 電波によるもの等で代替可能である。また、符号2は認証要求者、

25 符号3は所在位置認証サービス事業者であり、それぞれ、認証取得装置としての認証取得端末20、認証装置としての認証サーバ30を所持管理している。認証

取得端末 20 と認証サーバ 30 とは、図示せぬネットワークを介して接続されている。

前記したシステム構成において概略動作の流れを説明すれば以下のようになる。
すなわち、認証取得端末 20 は、内蔵の GPS レシーバにより GPS データ（緯
5 度、経度、高度、時間）を受信すると共に、認証サーバ 30 に対して受信した GPS
データの認証暗号鍵取得要求を発行する。これを受けた認証サーバ 30 は、
要求のあった認証取得端末 20 に対して認証暗号鍵情報を発行し、認証取得端末
20 は、GPS データとこの認証暗号鍵情報とを一体化したバンドルデータを生成
10 して認証サーバ 30 に対して認証要求を発行する。認証サーバ 30 は、認証し
た結果を認証取得端末 20 に送信し、これを受けた認証取得端末 20 は、認証デ
ータのアプリケーションへの引渡しを行う。このように、認証取得端末 20 と認
証サーバ 30 との間で適度な負荷分散を行うことができ、このため、認証要求者
2 は現場で迅速な回答結果を得ることができ、認証サーバ 30 の負担軽減がはか
れる。以下に詳細な説明を行う。

15 第 2 図は、本発明の認証システムの全体動作を説明するために引用した動作シ
ーケンス図である。ここでは、GPS 衛星 1 と認証取得端末 20 と認証サーバ 3
0 間の動作シーケンスが示されている。まず、認証取得端末 20 は、GPS 衛星
1 から電波を受信し、測位処理を実施する（S 2 1…第 2 図の矢印を修正します。）。
なお、GPS 衛星 1 からの電波は、認証サーバ 30 にも届けられ、認証サーバ 3
20 0 においても同様の処理が行なわれる（S 2 2）。続いて、認証取得端末 20 は、
認証サーバ 30 にタイムスタンプの要求を発行し（S 2 3）、これを受信した認
証サーバ 30 は、同期用のタイムスタンプを送信する（S 2 4）。このタイムス
タンプ受信と前後して認証取得端末 20 は、認証サーバ 30 に対して認証暗号鍵
取得要求を発行しており（S 2 5）、測位データとタイムスタンプならびに受信
25 した認証暗号鍵情報をバンドルして認証要求を発行する（S 2 6、S 2 7）。続
いて認証サーバ 30 から認証結果が送信され、認証取得端末 20 は、その認証デ

ータをアプリケーションへ引き渡す。

以下に具体的な実施形態について説明するが、本発明の認証システムによれば、処理負荷を認証取得端末20に負担させる方法と、認証サーバ30に負担させる方法の二通りある。まず、前者から説明する。第3図に、その場合の認証取得端
5 末20における動作の流れがフローチャートで示されている。

(第1の実施形態)

第3図において、認証取得端末20は、最初にGPS衛星1の電波を取り込み
(S31)、測位処理を実行して、緯度、経度、高度から成る認証取得端末20
の現在位置情報を入手する(S32)。そして、認証サーバ30から同期を取る
10 ためのタイムスタンプを受信して認証暗号鍵の発行要求を送信する(S33、S
34)。続いて、認証サーバ30から認証暗号鍵の発行を待ち(S35)、当該
受信した認証暗号鍵と、測位データおよびタイムスタンプとのバンドルデータを
生成し、認証サーバ30へ送信する(S36)。続いて、認証サーバ30からの
認証データの送信を待ち、結果をアプリケーションへ引き渡す(S37、S3
15 8)。

前記した本実施形態によれば、認証取得端末20での端末処理が中心となるた
め、現場での所在確認が容易になる。なお、アプリケーションとして、前記した
事故等の保険請求、警察、消防等の現場検証のほかに、RFID(Radio
Frequency Identification)タグと組み合わせることによる危険物や貴重品の物流
20 トラッキング等が考えられる。

具体的に、危険物、毒物、可燃物、放射性物質、爆発物、刀剣、銃、火気、爆
薬、汚染物質等に関する製造保管、使用、搬送に関する公的監督管理は、現在複
数の法律と官公庁に跨り、また、様式は個々に異なっており、データ収蔵の形態も
異なっており、一元管理がなされていない。また、現在における所在把握の方法
25 の多くは、届出や報告書によるものであり、電子化されておらず、また、リアル
タイムにその所在が把握されていない。このため、例えば、これら危険物、ある

6

いはその容器に脱着不能な I D タグを組み込み、前記した測位認証管理と組み合わせることで、これらの所在位置データを取得し、収蔵し、求めに応じて認証データとして提供することができる。物的防護建屋に保管された危険物に関しても同様、R F I D タグとの連携をはかり、室内外で測位管理することによる輸送を含む移動管理も可能である。このことにより、平時は勿論のこと、大規模災害発生時における危険物の所在の把握、および所在位置に関する報告を自動的、かつ、正確に把握できる。

(第 2 の実施形態)

第 4 図に、認証サーバを中心に処理負荷を分担させる場合の動作の流れがフローチャートで示されている。

第 4 図において、認証サーバ 3 0 は、まず、認証取得端末 2 0 から認証暗号鍵取得要求を受信する (S 4 1)。このことにより、認証サーバ 3 0 は、タイムスタンプに同期した認証用の連続暗号行列データ (認証暗号鍵情報) を生成し、要求のあった認証取得端末 2 0 へ送信する (S 4 2)。

そして、認証取得端末要求時刻データ、ならびに認証取得端末 2 0 による簡易測位結果データを取り込み (S 4 3、S 4 4)、自身が G P S 衛星 1 から取得した信号に基づき測位演算を行って得られる測位データと比較して簡易測位結果の確認を行う (S 4 5)。なお、確認は、以下に示す演算式 (測位方程式) を求めて得られる測位データに対し、特定の関数によって生成される認証暗証鍵情報を付加し、当該認証暗号鍵情報に基づき暗号化された測位演算データを、共有する関数を用いて復号化 (逆算) して得られる測位演算結果との比較により行われる。

[測位方程式]

$$(X_i - X_u)^2 + (Y_i - Y_u)^2 + (Z_i - Z_u)^2 = (R_i - C_{Bu})^2$$

但し、 i ($i = 1, 2, 3, 4$) : 測位に使用する衛星、 X_i 、 Y_i 、 Z_i : 既知の衛星位置、 X_u 、 Y_u 、 Z_u : 未知の受信機位置、 R_i : 既知の擬似距離 (受信信号から計算される衛星-G P S レシーバ間の実距離、時計誤差、伝播遅延、受

信機雑音を含む。このうち、衛星時計誤差と伝播遅延は解く前に補正される）、

C_{Bu} ：受信機時計誤差。

続いて前記と同様の認証処理を実行し（S 4 6）、結果を追記型の記録媒体から成る認証アーカイブ 3 6 に記録し（S 4 7）、同時に要求のあった認証取得端

5 末 2 0 へ結果を送信する（S 4 8）。

本発明実施形態によれば、認証サーバ 3 0 が測位計算を行う分、認証取得端末 2 0 にかかる負担が軽減され、また、認証サーバ 3 0 に認証データがアーカイブされるため、外部での改竄が困難であるといった効果が生じる。なお、認証取得

10 プラットフォームを利用して行われる。

なお、前記した本発明実施形態において、真なる測定位置で真なる測位データを取得したことを認証するためには、取得したデータそのものの一つに可逆的に真であることを証明できるデータが含まれている必要がある。しかしながら、受信した通常の G P S 信号には、可逆的に唯一の真なる信号であるという証明がな

15 されておらず、このため、本発明実施形態では、認証サーバ 3 0 から可逆的に真なる信号であることが証明できる認証暗号鍵情報を認証取得端末 2 0 に渡している。但し、これだけでは、受信した G P S 信号が全て真なる信号を受信していることの証明にはならないため、真なる位置で受信した全ての信号を復号化して認証サーバ 3 0 へ即時転送し、逆算や検算等合理性を検証して真性を確保している。

20 また、認証用信号である認証暗号鍵情報に時系列的な真性判定可能な配列（認証用の暗号行列データ）を持たせることや、付与のための通信方法の中に認証位置の合理性を検証できるような通過ルートの確認機能を付与する等の配慮も必要になる。更に、合理性検証にかかわる関数については一定のものではなく、認証サーバ 3 0 や認証取得端末 2 0 の双方で同期して動的に変化させる等の配慮も必要

25 である。

第 5 図は、前記した認証取得端末、第 6 図は、認証サーバの内部構成を機能展

開して示したブロック図である。

第5図において、認証取得端末20は、GPSデータ取込み部21と、認証暗号鍵受信部22と、バンドルデータ生成部23と、位置認証結果受信部24で構成される。GPSデータ取込み部21は、GPS衛星1から測位対象の現在位置データ、および時刻データを取り込み、バンドルデータ生成部23へ供給する。バンドルデータ生成部23には、他に、認証サーバ30から送信される認証暗号鍵情報が認証暗号鍵受信部22を介して供給されており、ここで、これらデータを一体化したバンドルデータ（測位データ+タイムスタンプ+認証暗号鍵情報）を生成し、位置認証結果受信部24を起動する。

10 一方、認証サーバ30は、認証取得端末20から前記したバンドルデータを取得し、自身が生成した認証暗号化鍵情報（認証用連続暗号行列データ）を用いて位置情報と時刻情報の認証を行い、要求のあった認証取得端末20へ送信する。位置認証結果受信部24は、認証サーバ30から位置認証の結果を受信してアプリケーションへ引き渡す。

15 第6図において、認証サーバ30は、GPSデータ取込み部31と、認証要求受信部32と、簡易測位結果受信部33と、認証暗号鍵生成送信部34と、測位処理部35と、認証アーカイブ36と、認証結果送信部37で構成される。

GPSデータ取込み部31は、GPS衛星1から測位対象の現在位置データ、および時刻データを取り込み、測位処理部35へ供給する。測位処理部35へは、
20 他に、簡易測位結果受信部33からの出力、ならびに認証暗号鍵生成送信部34からの出力が供給されている。簡易測位結果受信部33は、認証取得端末20により生成される簡易測位演算（GPSデータ、時刻データ、認証暗号鍵情報に基づく）の結果を受信し、認証暗号鍵生成送信部34は、認証取得端末20から認証要求を、認証要求受信部32を介して受信したときにGPS衛星1から受信した時刻データに基づく現在時刻に同期した認証暗号鍵情報を生成する。
25

測位処理部35は、認証取得端末20からの認証要求と同時に発せられる認証

暗号鍵取得要求に基づき、GPSデータ取込み部31を介して取り込まれる測位対象の現在位置データを、先に生成した認証暗号鍵情報を用いて認証し、認証取得端末20から送信される簡易測位の結果を確認する。そして、その結果を追記型の記録媒体で構成される認証アーカイブ36へ記録すると共に、認証結果送信部37を介して要求のあった認証取得端末20へ送信して回答する。

(第3の実施形態)

第7図は、本発明の認証システムを撮像装置（例えば、デジタルカメラ）に応用した場合の動作概念図を示す。

ここでは、デジタルカメラ40が本発明の認証取得端末20として動作する。

- 10 デジタルカメラ40は、通信モジュール49を介して所在・位置認証サービス事業者3の認証サーバ30に接続される。ここでは、前記した所在・位置認証の他に、映像・データ保管、時刻認証も行われる。

- デジタルカメラ40は、図示せぬカメラ本体部の他に、GPS衛星1からGPSレシーバ41を介して得られる測位入力（FM電波によるデファレンシャル入力も含む）、方位ジャイロ42、地磁気センサ43による方位入力、温度、気圧、湿度等、環境センサ44による周辺環境データ入力、指紋等の生体情報入力による操作者ID確認部45、ならびにタグリーダ部46を入力デバイスとして備えている。第7図において、操作者ID確認部45の下の大きな2重丸は、指紋センサといったような操作者ID確認部45の受け台である。（…第7図の符号45の位置を修正します） これら入力データは、制御中枢となるCPU47（ここでは、画像真性処理部）に提供され、処理される。
- 15
- 20

- なお、撮影データは、これら入力データと関連付けられて暗号化され、デジタルカメラ40に内蔵された追記型の記録媒体48（以下、暗号化記録メディア）に記録される。また、認証サーバ30の追記型記録媒体36（認証アーカイブ）にも同様に記録される。
- 25

ところで、現場の状況記録のための写真撮影は、工事前後、あるいは交通事故

等の際の保険請求をはじめ、警察、および消防の現場検証等で広く実施されている。ここでは、これらの映像記録において、撮影された日時とともに、撮影された方向、場所を同時に真性映像データとして記録し、収蔵する。また、要求に応じて真性映像データを再現し、提供するまでの一貫したシステムを提供するものである。

このとき、撮影された映像データは、撮像素子（以下、イメージセンサという）の光／電気変換以降の処理は改竄不可能なものであることが必須とされ、映像データは、先の入力データと共に、デジタルカメラ40ならびに認証サーバ30の認証アーカイブ36等の複数の追記型記録媒体に同時に収蔵される。また、
10 接続される通信回線については高セキュア性を有するものとする。更に、センタ側の認証アーカイブ36については、必要な立ち入り管理が行なわれ、改竄防止機能、および物理的防護機能を持つこととする。

第8図に、映像の真性を確保し、認証可能な映像を保存するために必須となる画像真性処理部の構成例が、第9図に、その処理手順がフローチャートで示されている。

第8図において、符号472は、CCD（Charge Coupled Device）等により構成されるイメージセンサ部であり、イメージセンサ駆動タイミング部471により生成されるタイミング信号により駆動される（S91）。また、セキュリティマーキング生成部483は、認証暗号鍵受信部476を介して取り込まれる認証
20 サーバ30によって生成された認証暗号鍵情報、ならびに、外部信号受信部473、同期時刻受信部474、位置認証処理部475を介して得られる、それぞれ時刻情報と現在位置情報を重畳してセキュリティマーキング信号を生成してセキュリティマーキング処理部485へ供給する（S92）。セキュリティマーキング処理部485には、他に、前記した駆動タイミング信号、A/D処理部482
25 を介して入力されるイメージセンサ出力信号が供給されており、ここでセキュリティマーキング信号と合成され、映像生成基礎データとして出力バッフ484を

經由してカメラ信号処理部 4 8 9 へ供給される (S 9 3)。

カメラ信号処理部 4 8 9 は、前記映像生成基礎データをカメラ入力信号として処理を行い、セキュリティマーキング信号を含む映像暗号化データを生成して出力する。この映像暗号化データは、セキュア回線 4 8 7 を介して認証サーバ 3 0
5 の認証アーカイブ (追記型記録媒体 3 6) へリアルタイムに伝送され、記録される。このとき、必要に応じて、同期時刻スタンプ (同期時刻受信部 4 7 4)、測位位置データ (位置認証処理部 4 7 5)、周囲環境センサデータ (各種センサ 4 4 1、4 4 2)、操作者 ID (操作者 ID 受信部 4 7 7) をリンクして記録しても良い。なお、前記した各信号、同期時刻スタンプ信号 (同期時刻受信部 4 7
10 4)、測位位置信号 (位置認証処理部 4 7 5)、周囲環境センサデータ (各種センサ 4 4 1、4 4 2)、操作者 ID データ (操作者 ID 受信部 4 7 7) は、全て受信した時点で映像信号と共に、暗号化記録メディア 4 8 にも記録される (S 9 4)。

このように、認証情報を同時に異なった記録媒体へ異なった形式で記録することにより、複数記録媒体に跨って異なる形式の映像データを同時に改竄しない限り
15 目的を持った第三者による故意の改竄は不可能になる。

また、この映像暗号化データを再生するには (S 9 5)、セキュリティマーキング信号によって駆動される復調アルゴリズムを用いて映像以外の付与データを含む信号から真の映像データを抽出する必要がある (S 9 6)。

20 なお、前記した本発明実施形態によれば、イメージセンサによる光/電気信号変換タイミング以降を改竄不可能なものとする処理について述べたが、露光調節等、光/電気信号変換の前段階にある光学的な入力を制限する機械式または電気式シャッターの起動タイミングについても同様に考慮する必要がある。例えば、デジタルカメラであっても、CCD (光/電気変換素子) といったようなイメージ
25 ジセンサ部 4 7 2 の前に光学的な入力を制限 (露光調節) するための機械式または電子式シャッターが存在するものがある。これが存在する理由は高速で動く被

写体を撮影する際の光／電気変換素子のON／OFFによるシャッターよりも、機械式または電子式シャッターの方が低コストなことや電子的な回路の煩雑さが解消され、従来の写真技術的な操作（絞り×シャッタースピード×焦点）が可能であるからといわれている。このように、光／電気変換素子のON／OFFによるシャッターの場合でも、機械式または電子式シャッターの場合でも本発明を適用でき、タイミングは適宜設定できるものとする。なお、シャッター速度（スリットなどの移動速度）を考慮して、時刻を設定することもできる。

また、より高度なセキュリティ応用カメラにおいては、光入力をハーフミラー等により二重系により処理を行い、個別に暗号化記録メディア48に（データ収蔵アーカイブ）に同時に登録することが考えられる。更に、色彩平準化のために、送受信側で同じ基準に基づいた補正色彩が再現できる相互誤差差分補正処理を行うこともできる（S97）。

以下、前記した相互誤差差分補正処理について説明する。第10図は、相互誤差差分補正処理を汎用的に説明するために引用した図であり、送受信側として、撮影側サブシステム100と表示側サブシステム200を例示している。

撮影側サブシステム100に前記したデジタルカメラ40の要部構成が示されている。なお、第10図中、第8図と同一番号が付されたブロックは、第8図に示すそれと同じとする。

ネットワークを介して送受信される色彩情報は、個々の表示装置の色彩表現誤差により、若干異なって表現される。ここでは、ある標準に対して色彩表現誤差の無いデータをやりとりすることにより、真なる色彩ではないもののシステムの両端にある送受信側のマンマシンインタフェース上での誤差を最小とすることで色彩を含むデータの流通を目的としている。

具体的に、標準色彩テンプレート（TP）を用意し、標準テンプレート色彩データ生成部501により生成された撮影画像のそれぞれの標準色成分について生成出力する。標準色彩差分処理部502は、撮影画像の色成分と、それぞれの標

準色成分との差分を演算し、入力色彩データ補正信号を生成し、撮影された映像信号と共に表示側サブシステム200へ送信する。表示側サブシステム200では、再現時、受信した入力色彩データ補正信号（差分信号）を誤差信号として除外するための演算を行い、表示する。このことにより、真なる色彩ではないものの、システムの両端にある送受信側のマンマシンインタフェース上での色彩誤差を最小とすることができる。

以上説明のように本発明は、認証取得装置が、GPS等の電子的な位置測位手段から受信した測位対象の現在位置データ、および時刻データと、認証要求発行時に認証装置から受信した認証暗号鍵とを一体化したデータを生成し、この一体化したデータを、ネットワークを介して接続される認証装置へ送信し、認証装置が認証暗号化鍵を用いて位置情報と時刻情報の認証を行い、認証要求のあった認証取得装置へ返信するものであり、このことにより、センタの認証サーバと現場の認証取得装置間で負荷分散され、現場での所在確認を容易とした認証システムを提供することができる。

また、撮像装置を含む認証取得装置が、現在時刻に同期した撮像素子の駆動タイミング信号を生成し、当該駆動タイミング信号に、認証装置から送信される認証暗号鍵情報、ならびに位置測位手段から取得した測位対象の現在位置情報を重畳してセキュリティマーキング信号を生成し、撮像装置から出力される画像情報を、セキュリティマーキング情報を含む暗号化情報として追記型の記録媒体に記録することで、デジタルカメラ等により撮影された画像についてもその真性を維持するものである。撮影から記録まで一貫したセキュリティを実現するものである。

更に、撮影画像のそれぞれの標準色成分について、あらかじめ用意されたそれぞれの標準色成分との差分を演算し、入力色彩データ補正信号として撮影された映像信号と共に表示側サブシステムへ送信し、表示側サブシステムでは、再現時、受信した入力色彩データ補正信号を誤差信号として除外するための処理を行うこ

とで色彩の真性を担保するものである。以上により、撮影から記録まで一貫したセキュリティを実現することができる。

15

請求の範囲

1. 測位対象の位置認証を行う認証装置と、前記認証装置とはネットワークを介して接続される認証取得装置から成る認証システムであって、

- 5 電子的な位置測位手段から受信した前記測位対象の現在位置データ、および時刻データを取り込み、これらデータと、認証要求発行時、前記認証装置から受信した認証暗号鍵とを一体化したデータを生成する前記認証取得装置と、

前記認証取得装置から前記一体化したデータを取得し、前記認証暗号化鍵を用いて前記位置情報と時刻情報の認証を行う前記認証装置と、

- 10 を具備することを特徴とする認証システム。

2. 請求項1に記載の認証システムにおいて、前記認証装置は、

前記認証取得装置からの認証要求を受信し、前記電子的な位置測位手段から受信した時刻データに基づく現在時刻に同期した認証暗号鍵を生成し返信する手段と、

- 15 前記認証取得装置からの前記認証要求と同時に発せられる認証暗号鍵取得要求に基づき、前記電子的な位置測位手段から取り込まれる測位対象の現在位置データを、前記生成した認証暗号鍵を用いて認証し、前記認証取得装置から送信される簡易測位の結果を確認する手段とを具備することを特徴とする。

3. 請求項1に記載の認証システムにおいて、前記認証装置は、

- 20 測位演算式を計算して得られる測位データに対して特定の関数によって生成される認証暗証鍵を付加して暗号化した測位データを生成する手段と、前記暗号化された測位演算データを、前記関数を用いて復号化して前記測位演算結果を得る手段を具備することを特徴とする。

4. 測位対象を含む撮影画像の認証を行う認証装置とはネットワークを介して接

- 25 続される撮像装置を備えた認証取得装置であって、

現在時刻に同期した撮像素子の駆動タイミング信号を生成し、当該駆動タイミ

ング信号に、前記認証装置から送信される認証暗号鍵情報、ならびに前記位置測位手段から取得した測位対象の現在位置情報を重畳してセキュリティマーキング信号を生成する手段と、

前記撮像装置から出力される画像情報を、前記セキュリティマーキング情報を
5 含む暗号化情報として追記型の記録媒体に記録する手段と、

を具備することを特徴とする認証取得装置。

5. 請求項4に記載の認証取得装置であって、

前記撮影画像のそれぞれの色成分について、それぞれの標準色成分との差分を演算し、再現時、前記差分を誤差信号として除外する手段を具備することを特徴
10 とする。

6. 請求項4に記載の認証取得装置であって、

光入力を分光し、それぞれから得られる撮影画像に前記セキュリティマーキング情報ならびに現在位置情報を重畳してセキュリティマーキング信号を生成し、それぞれに用意される追記型の記録媒体に記録することを特徴とする。

15 7. 請求項4に記載の認証取得装置であって、

撮影者固有の生体情報を取得して得られる撮影者情報、撮影方位情報を含む前記現在位置情報、環境情報の少なくとも一つを前記セキュリティマーキング信号と関連付けて前記追記型の記録媒体に記録することを特徴とする。

8. 認証取得装置とネットワークを介して接続される認証装置が測位対象の位置
20 認証を行う認証方法であって、

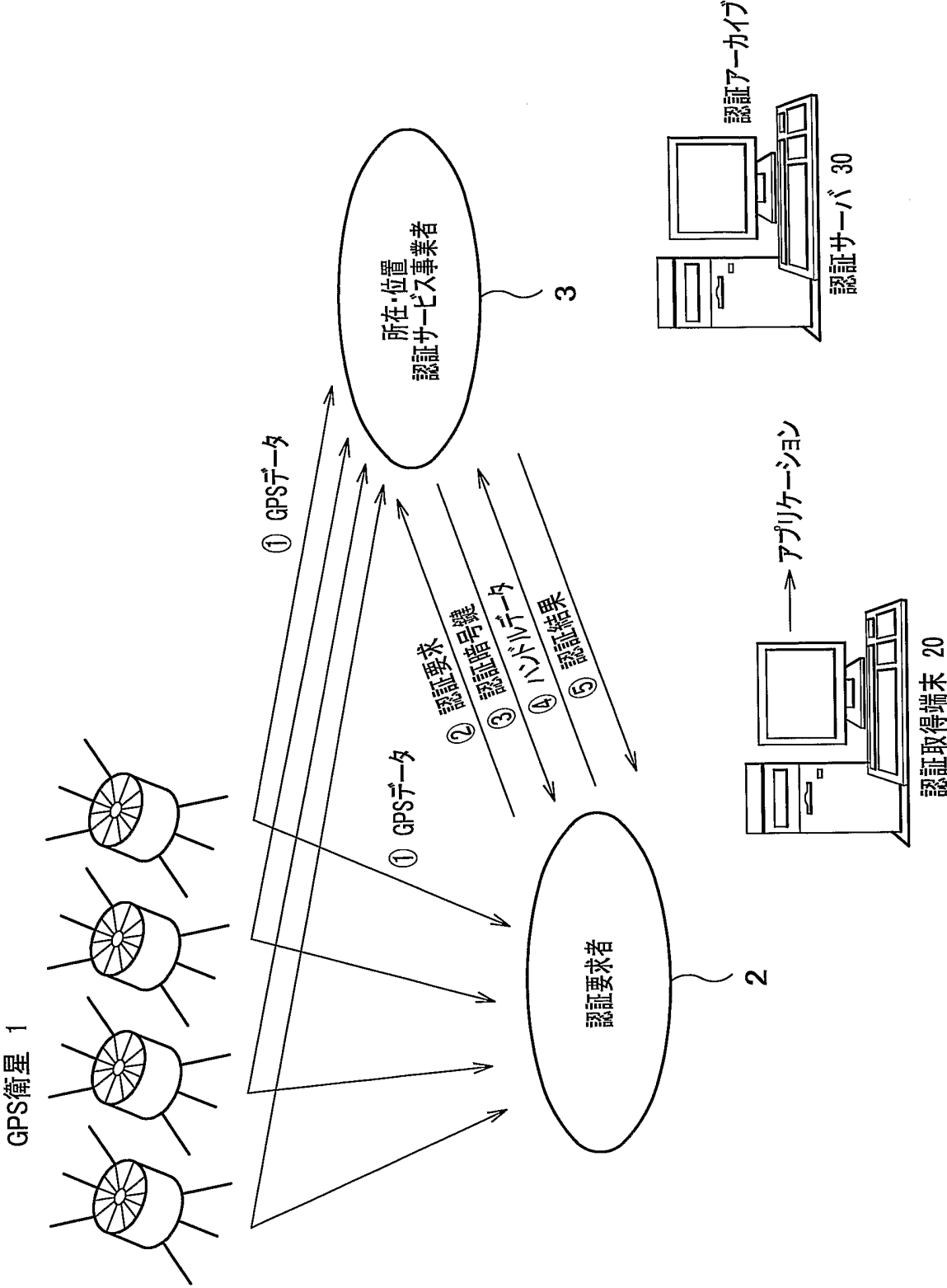
前記認証取得装置が電子的な位置測位手段から受信した前記測位対象の現在位置データ、および時刻データを取得するステップと、

前記取得した各データと、認証要求発行時に前記認証装置から受信した認証暗号鍵とを一体化したデータを生成し、前記認証装置へ送信するステップと、

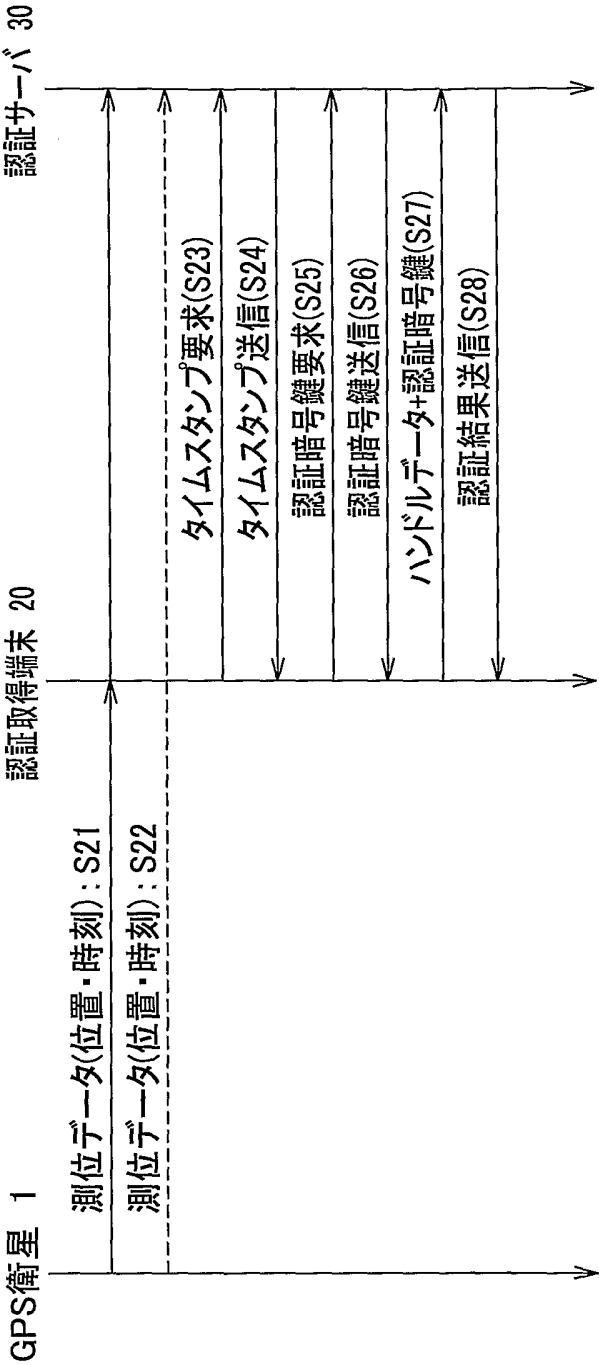
25 前記一体化したデータを受信した認証装置が前記認証暗号化鍵を用いて前記位置情報と時刻情報の認証を行うステップと、

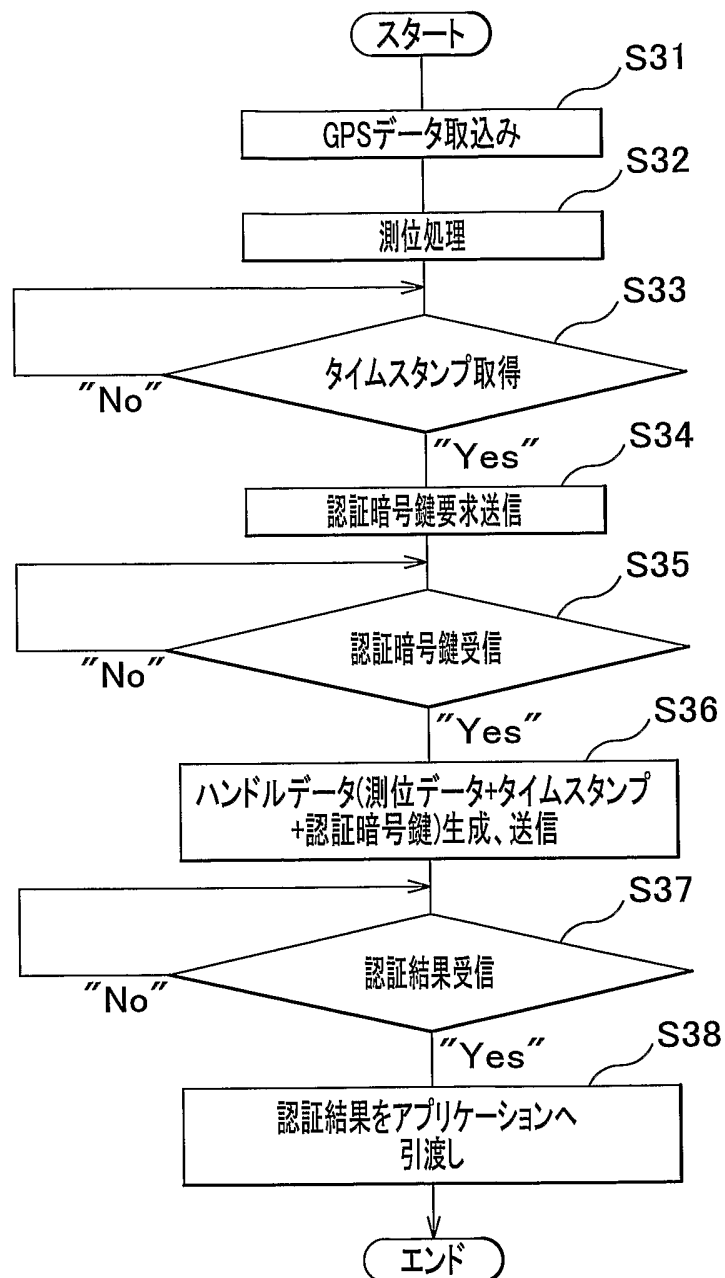
を有することを特徴とする認証方法。

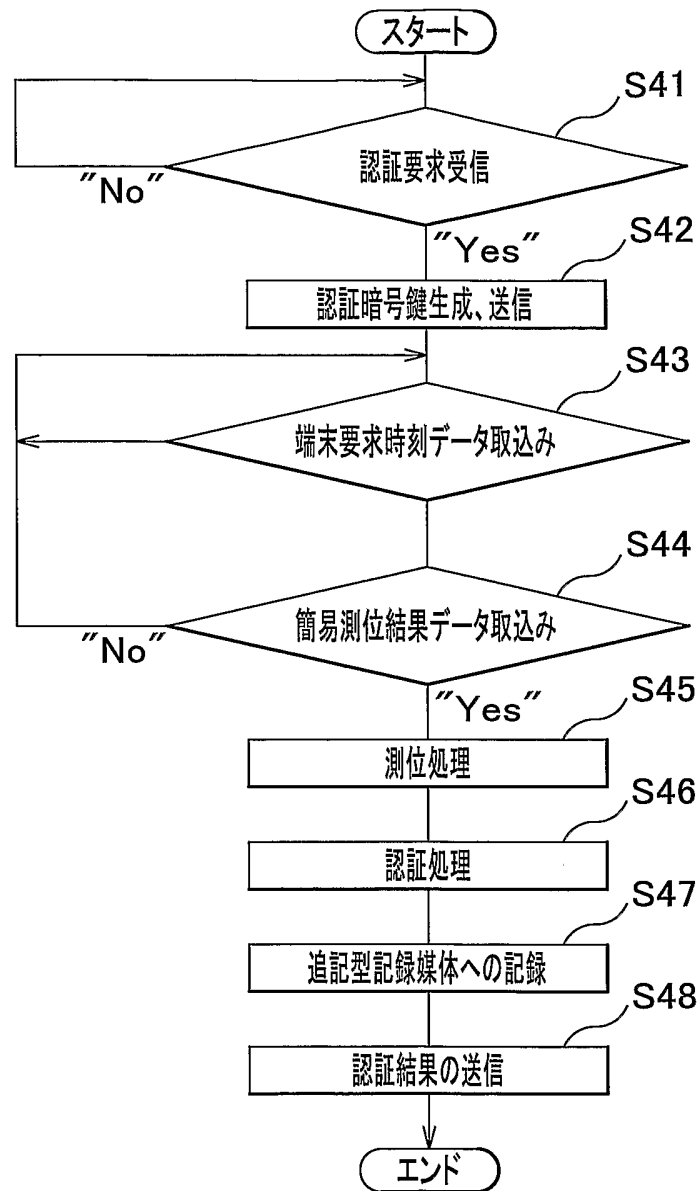
第1図



第2図

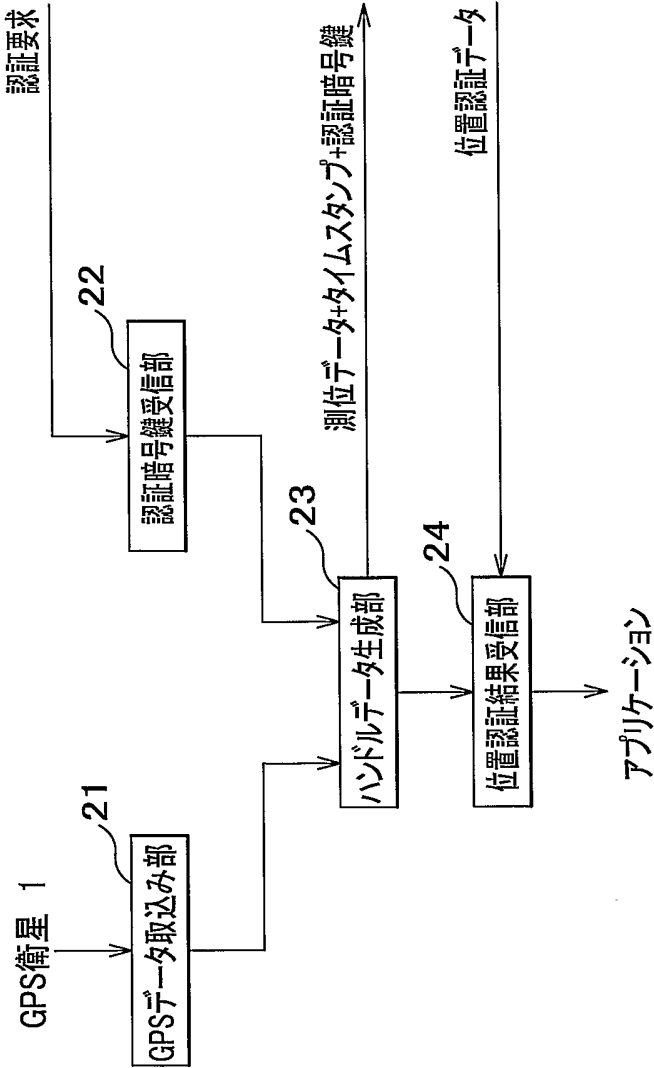




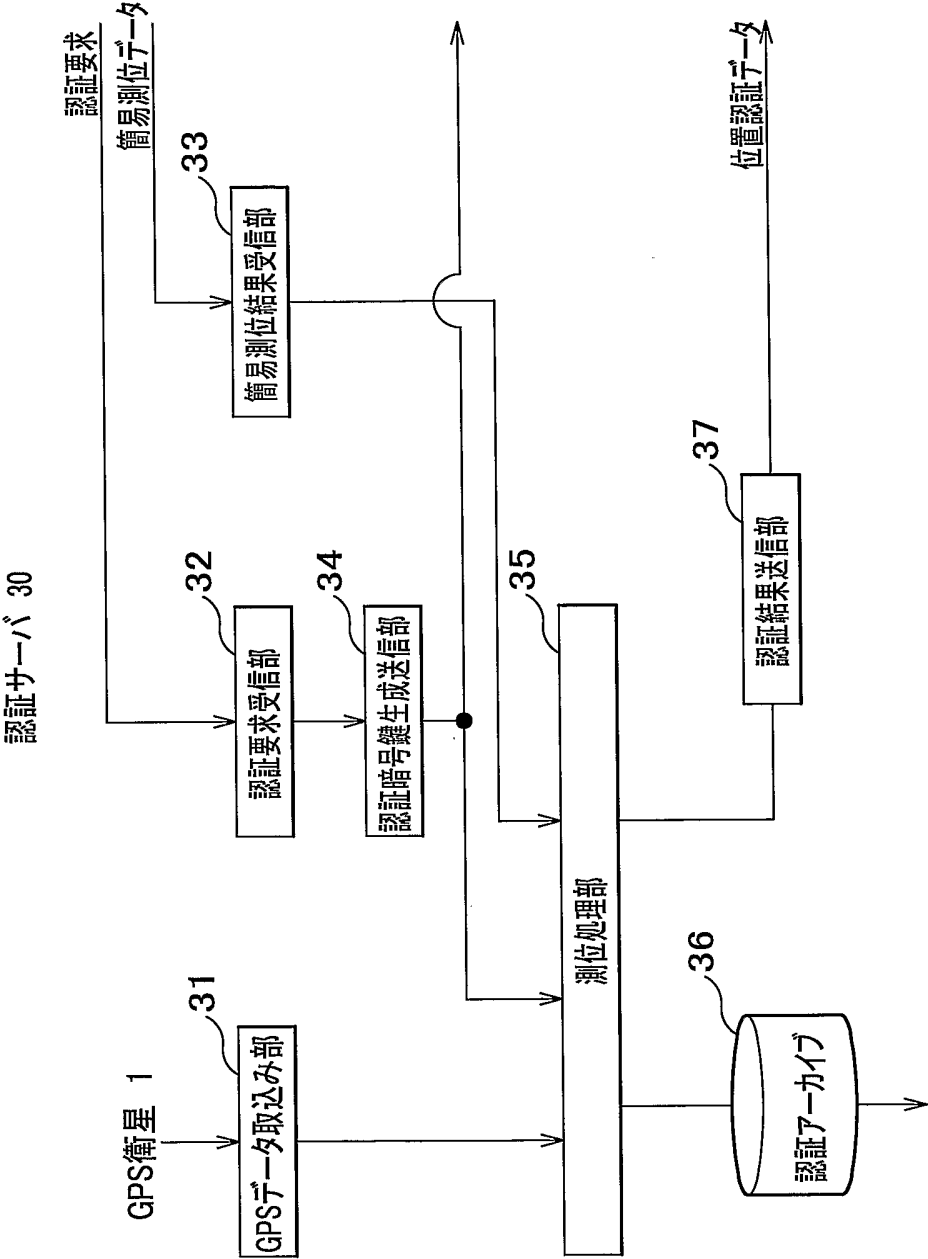
4 / 10
第4図

第5図

認証要求端末 20



第6図



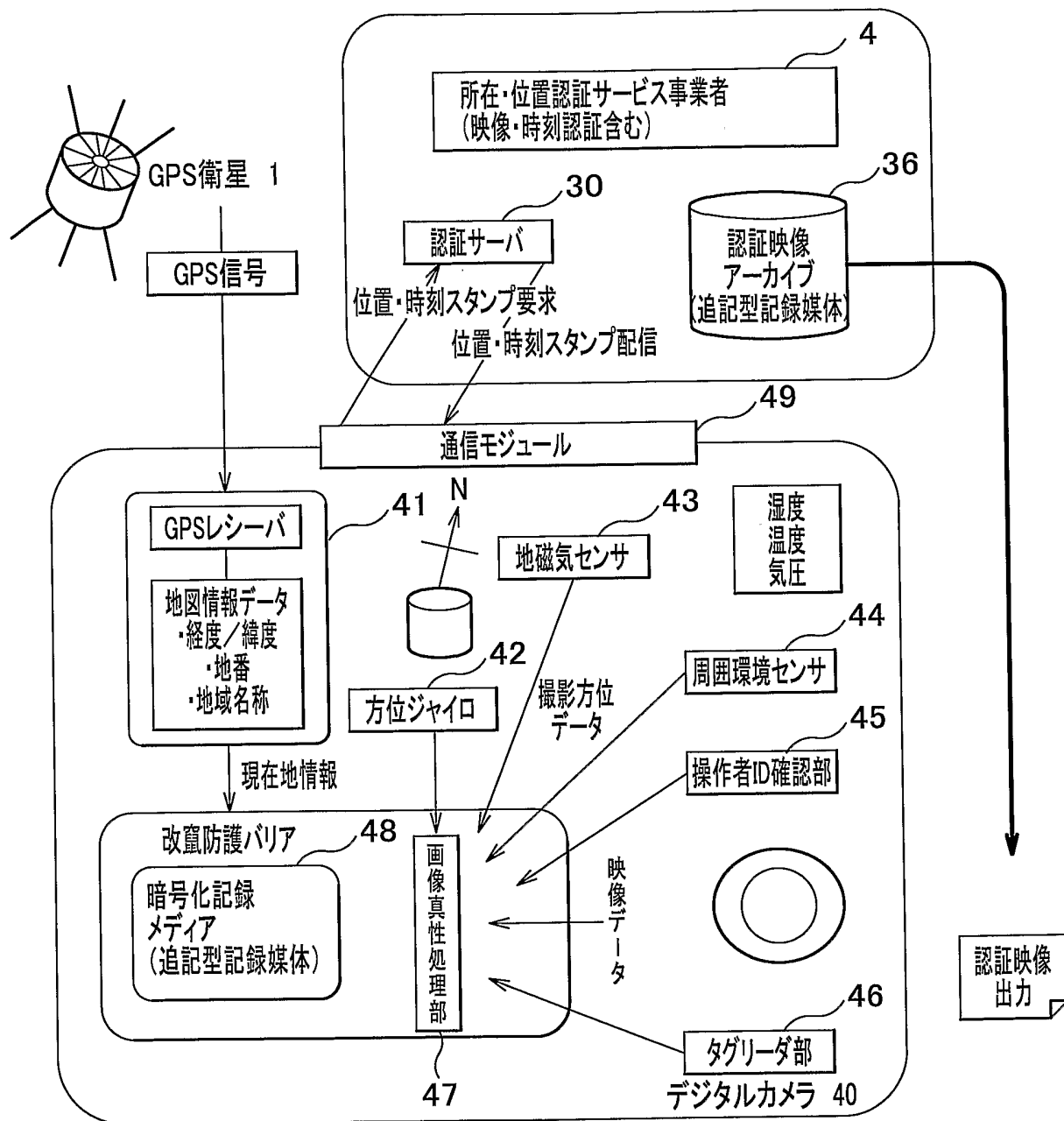
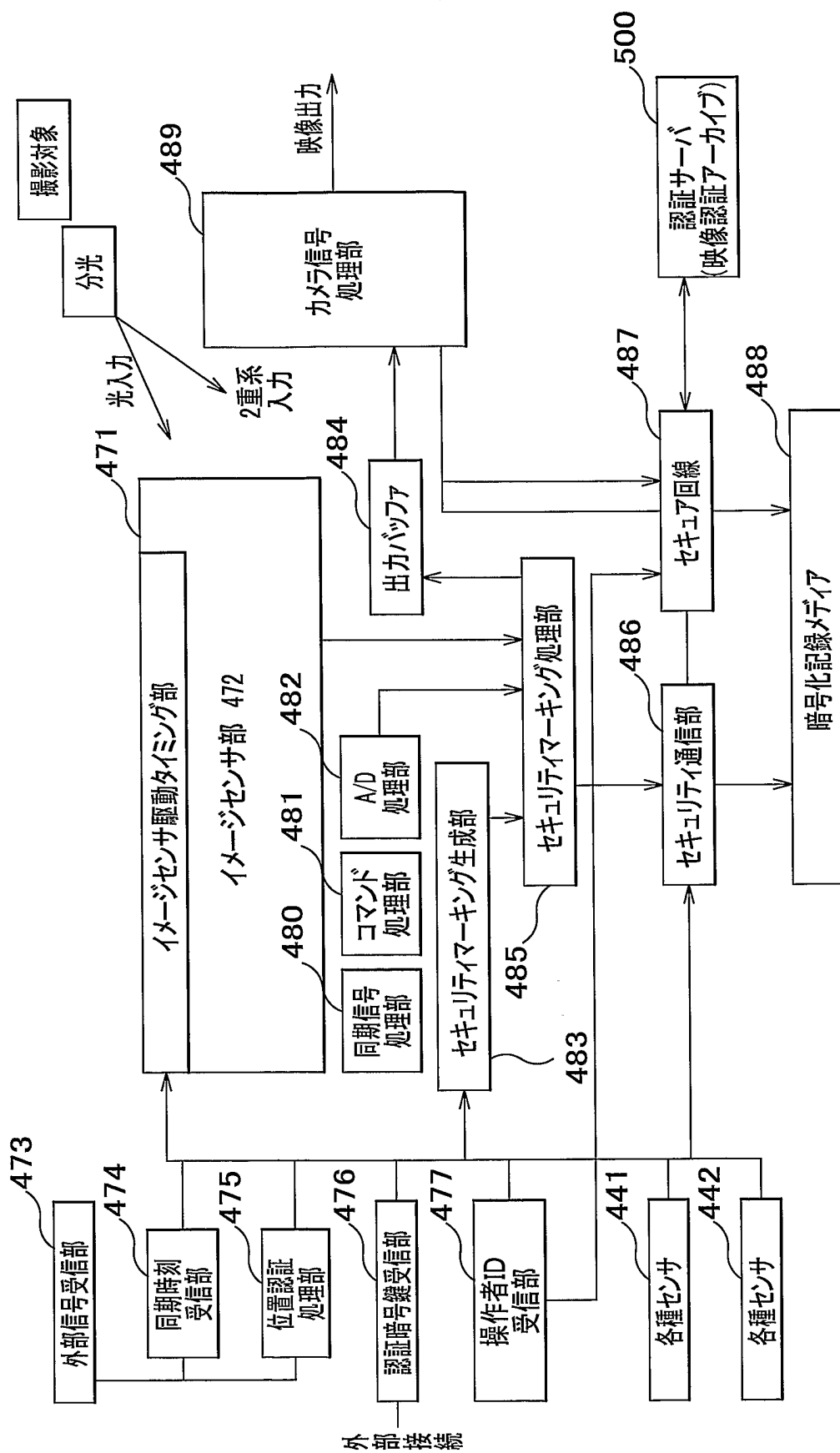
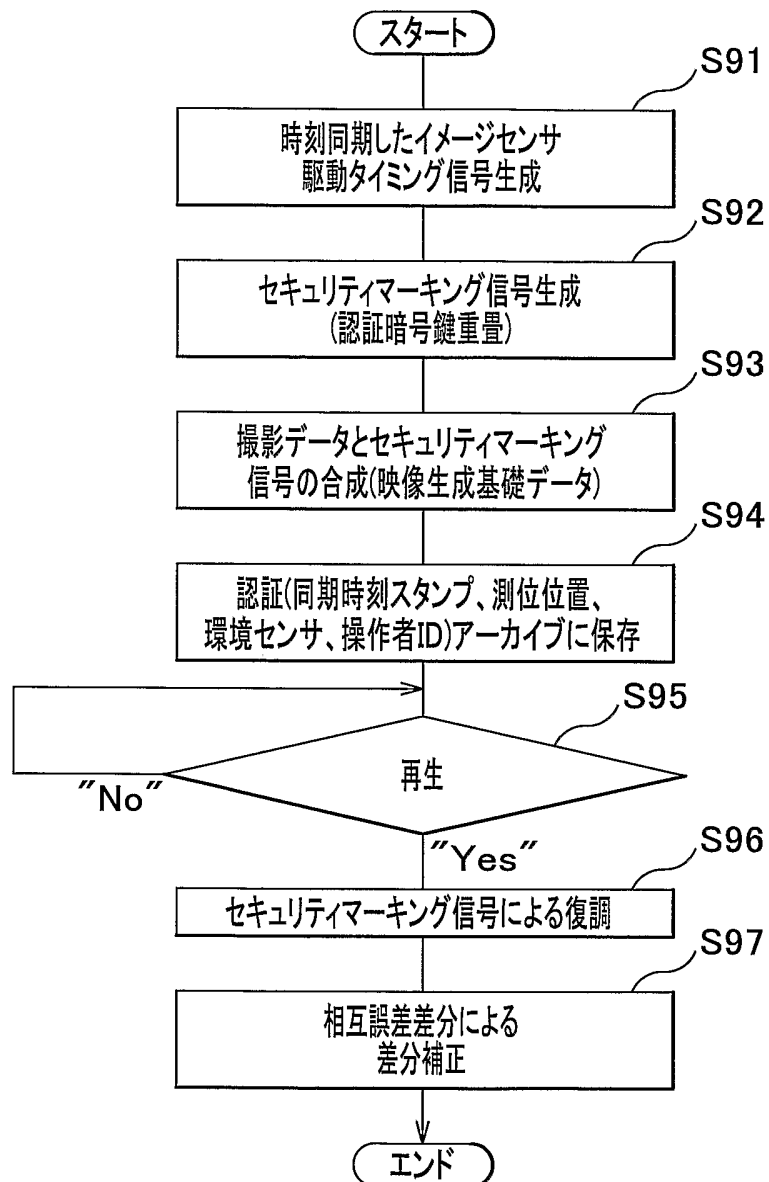
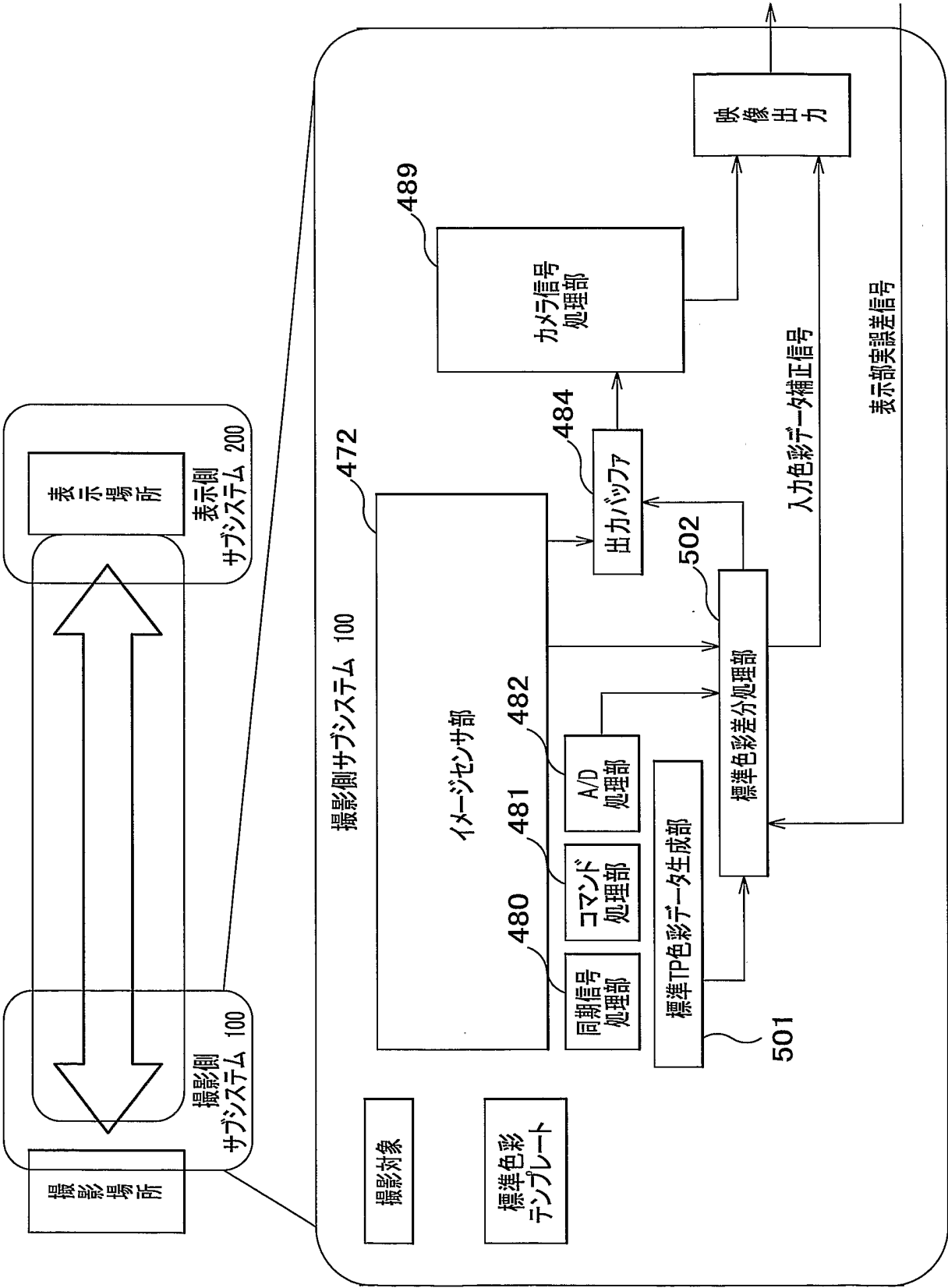


圖
8
錄





第10図



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006222

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/32, H04L9/08, H04N5/232, H04N5/225, H04N5/92, G06F17/60

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.Cl⁷ H04L9/32, H04L9/08, H04N5/232, H04N5/225, H04N5/92, G06F17/60

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

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

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.
X	JP 2001-33537 A (NEC Corp.), 09 February, 2001 (09.02.01), Full text; Figs. 1 to 7	1, 3, 8
Y	Full text; Figs. 1 to 7 (Family: none)	2, 4-7
Y	JP 1-100586 A (NEC Corp.), 18 April, 1989 (18.04.89), Page 2, upper right column, line 19 to lower right column, line 21 (Family: none)	2
Y	JP 2000-50193 A (Fuji Photo Film Co., Ltd.), 18 February, 2000 (18.02.00), Par. Nos. [0014] to [0015] (Family: none)	4, 6

☒ 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
08 October, 2004 (08.10.04)

Date of mailing of the international search report
26 October, 2004 (26.10.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006222

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 63-76687 A (NEC Corp.), 18 March, 1987 (18.03.87), Full text; Figs. 1, 2 (Family: none)	5
Y	JP 2003-157241 A (Fuji Photo Film Co., Ltd.), 30 May, 2003 (30.05.03), Par. No. [0037]; Fig. 4 (Family: none)	7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006222

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-3 disclose an authentication system for performing data authentication according to the object-to-be-positioned current position data and the time data transmitted from the authentication acquisition device and the invention of claim 8 discloses the authentication method.

The inventions of claims 4-7 disclose an authentication acquisition device for image-processing the image information and recording it while correlating it with an imaging person and an imaging environment. However, these inventions do not have any definition of the data authentication processing according to the position data and the time data which are the technical features of the inventions of claims 1-3, 8. (Continued to extra sheet)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
- ☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006222

Continuation of Box No.III of continuation of first sheet (2)

Accordingly, the inventions of these claims have different concepts of invention.

A. 発明の属する分野の分類 (国際特許分類 (IPC))			
Int. Cl ⁷ H04L9/32, H04L9/08, H04N5/232, H04N5/225, H04N5/92, G06F17/60			
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 ⁷ H04L9/32, H04L9/08, H04N5/232, H04N5/225, H04N5/92, G06F17/60			
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		1971-2004年	
日本国登録実用新案公報		1994-2004年	
日本国実用新案登録公報		1996-2004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 請求の範囲の番号
X Y	JP 2001-33537 A (日本電気株式会社) 2001.02.09 全文, 図1-7 全文, 図1-7 (ファミリーなし)		1, 3, 8 2, 4-7
Y	JP 1-100586 A (日本電気株式会社) 1989.04.18 第2頁右上欄第19行-同頁右下欄第21行 (ファミリーなし)		2
☒ 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 08.10.2004		国際調査報告の発送日 26.10.2004	
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) 青木 重徳	5M 4229
		電話番号 03-3581-1101 内線 3597	

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 請求の範囲の番号
Y	J P 2000-50193 A (富士写真フイルム株式会社) 2000.02.18 第【0014】-【0015】段落 (ファミリーなし)	4, 6
Y	J P 63-76687 A (日本電気株式会社) 1987.03.18 全文, 第1, 2図 (ファミリーなし)	5
Y	J P 2003-157241 A (富士写真フイルム株式会社) 2003.05.30 第【0037】段落, 図4 (ファミリーなし)	7

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見（第1ページの2の続き）

法第8条第3項（PCT17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲1－3には、認証取得装置から送られてくる測位対象の現在位置データや時刻データに基づくデータの認証をおこなう認証システムが、請求の範囲8には、その認証方法が記載されている。

これに対し、請求の範囲4－7には、画像情報を画像処理し、撮影者や撮影環境に関連付けて記録する認証取得装置が記載されているものの、請求の範囲1－3、8に係る発明の技術的な特徴である位置データや時刻データに基づくデータの認証処理については何ら定義していないことから、これら請求の範囲に記載されている発明概念は、それぞれ相違するものである。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。