

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004 年 12 月 9 日 (09.12.2004)

PCT

(10) 国際公開番号
WO 2004/107063 A1

(51) 国際特許分類: G04G 5/00, G06F 1/14

(21) 国際出願番号: PCT/JP2003/006669

(22) 国際出願日: 2003 年 5 月 28 日 (28.05.2003)

(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): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県 川崎市 中原区 上小田中 4 丁目 1 番 1 号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 秋山 良太 (AKIYAMA, Ryota) [JP/JP]; 〒211-8588 神奈川県 川崎

市 中原区 上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP). 石橋 正路 (ISHIBASHI, Masamichi) [JP/JP]; 〒211-8588 神奈川県 川崎市 中原区 上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP).

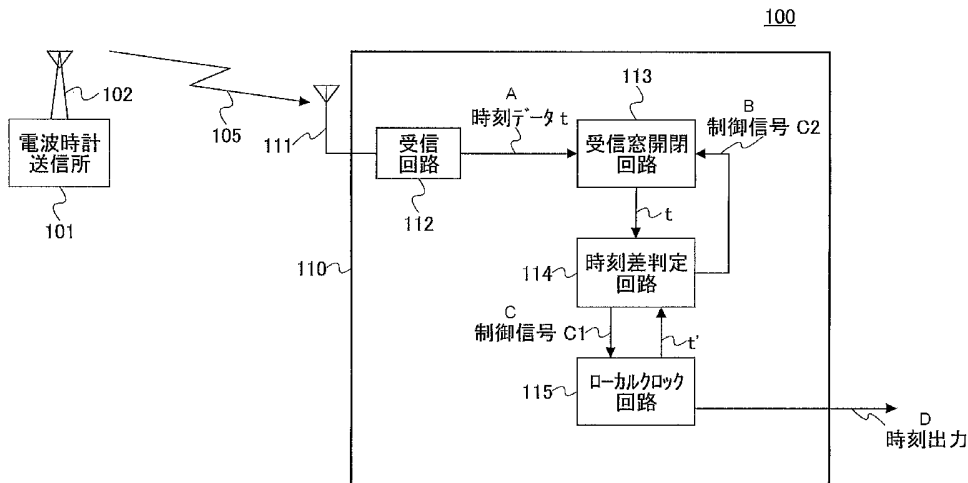
(74) 代理人: 伊東 忠彦 (ITO, Tadahiko); 〒150-6032 東京都 渋谷区 恵比寿 4 丁目 20 番 3 号 恵比寿ガーデンプレイスタワー 32 階 Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

/ 続葉有 /

(54) Title: TIME MANAGER AND TIME MANAGEMENT METHOD

(54) 発明の名称: 時刻管理装置及び時刻管理方法



101...RADIO WAVE CLOCK TRANSMISSION STATION
112...RECEPTION CIRCUIT
A...TIME DATA t
113...RECEPTION WINDOW OPEN/CLOSE CIRCUIT
B...CONTROL SIGNAL C2

114...TIME DIFFERENCE DETERMINATION CIRCUIT
C...CONTROL CIRCUIT C1
115...LOCAL CLOCKING CIRCUIT
D...TIME OUTPUT

(57) Abstract: A time manager for reducing the opportunity of intentional time falsification by a third party, and a time management method. This time manager is characterized by having an external time acquiring means which acquires an external time within a predetermined time width, a local clocking means which outputs a self-running time, and a time difference determining means which calculates the difference between the external time acquired by the external time acquiring means and the self-running time outputted by the local clocking means, sets the external time in the local clocking means when the difference is smaller than a predetermined value, but does not set the external time in the local clocking means when the difference is more than the predetermined value.

(57) 要約: 本発明は、第三者による意図的な時刻改ざんの機会を減らす時刻管理装置及び時刻管理方法を提供することを目的とする。この目的を達成するために、本発明は、予め定められた時間幅内で外部時刻を取り込む外部時刻取込手段と、自

/ 続葉有 /

WO 2004/107063 A1



(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (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

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。

走時刻を出力するローカル時計手段と、前記外部時刻取込手段により取り込んだ前記外部時刻と、前記ローカル時計手段の出力する前記自走時刻との差を計算し、前記差が予め定められた値より小さい場合には前記外部時刻を前記ローカル時計手段に設定し、そして、前記差が予め定められた値以上の場合には前記外部時刻を前記ローカル時計手段に設定しない、時刻差判定手段とを有することを特徴とする、時刻管理装置により構成する。

明 細 書

時刻管理装置及び時刻管理方法

5 技術分野

本発明は、時刻管理方式に関連し、特に、第三者による意図的な時刻の改ざんの機会を減少させた、時刻管理装置及び時刻管理方法に関連する。

背景技術

- 10 現在では、コンピュータで使用するファイルが作成されたときの時刻を保証して、セキュリティを確保するために、タイムスタンプが使用されている。このタイムスタンプは、理想的には、例えば、時刻管理装置として、誤差のない時計をコンピュータ等の内部に保持し、この時計により供給されるのが最良である。

- 15 しかし、実際には、コンピュータの内部に装備する時計は、誤差を生じる。従って、規準となる時計により、定期的に、補正を行うことが要求される。このような補正を行うための規準となる時計の一例としては、電波時計がある。

- 従来の技術では、電波時計から電波により送信される外部時刻情報が、時刻管理装置により受信可能である場合には、時刻管理装置は、その送信される外部時刻情報を用いて較正し、一方、外部時刻情報が受信が不可能な場合は、内蔵する
20 ローカル時計の時刻情報を較正せずに採用する。そして、この時刻管理装置の出力する時刻情報を、タイムスタンプとして使用していた。

しかしこの場合、偽の電波時計発信機を使って自由にローカル時計の示す時刻の改ざんが可能なために、電波時計から電波により送信される公的な時刻情報を、デジタル署名のタイムスタンプとして活用できないという問題があった。

- 25 更に、従来の技術では、時刻管理装置の示すローカルな時刻が、外部より供給される外部時刻よりも進んでいる場合には、外部より供給される外部時刻情報を、時刻管理装置内に取り込むと、時刻管理装置の出力する時間が、僅かに過去の時点の時刻へ戻ることになる。このような場合には、この過去の時点の時刻を示す時間帯の時刻署名は、信頼性がなくなることとなる。

また、更に、下記の文献には、本願と関連する技術が記載されている。

(特許文献1) 特開平6-258460号公報

(特許文献2) 特開2002-4876号公報

(特許文献3) 特開2002-236187号公報

5 (特許文献4) 特開2002-63614号公報

発明の開示

本発明は上記の点に鑑みてなされたもので、第三者による意図的な時刻の改ざんの機会を減らす時刻管理装置及び時刻管理装置方法を提供することを目的とする。

- 10 この目的を達成するために、本発明の時刻管理装置は、
予め定められた時間幅内で外部時刻を取り込む外部時刻取込手段と、
自走時刻を出力するローカル時計手段と、
前記外部時刻取込手段により取り込んだ前記外部時刻と、
前記ローカル時計手段の出力する前記自走時刻との差を計算し、前記差が予め定
15 められた値より小さい場合には前記外部時刻を前記ローカル時計手段に設定し、
そして、前記差が予め定められた値以上の場合には前記外部時刻を前記ローカル
時計手段に設定しない、時刻差判定手段とを有することを特徴とする。

- 本発明によれば、従来のように、単に外部時刻情報が受信可能か否かでローカル
時計に外部時刻情報を設定するか又は自走させるかを切り替えるのではなく、外部よ
20 り供給される時刻情報を定期的にあるいはランダムに、或る一定の時間帯の間に取り
込み、装置内のローカルな時刻情報との時間誤差を求め、その値の大小に応じて外部
時刻を設定しまたはローカル時刻をそのまま自走させて出力する。これにより、第三
者による意図的な時刻の改ざんの機会を減らす時刻管理装置及び時刻管理方法を提
供できる。

- 25 また、この目的を達成するために、本発明の時刻管理装置は、
予め定められた時間幅内で外部時刻を取り込む外部時刻取込手段と、
自走時刻を出力するローカル時計手段と、
前記外部時刻取込手段により取り込んだ前記外部時刻と、前記ローカル時計手
段の出力する前記自走時刻との差を計算し、

前記差が予め定められた値より小さい場合には前記外部時刻を前記ローカル時計手段に設定し、そして、前記差が予め定められた値以上の場合には前記外部時刻を前記ローカル時計手段に設定しない、時刻差判定手段と、

- 前記ローカル時計手段に設定された前記外部時刻が、前記外部時刻を前記ローカル時計手段に設定する直前に前記ローカル時計手段が出力した時刻よりも、前の時刻に等しい場合には、前記ローカル時計手段が出力する時刻が、前記外部時刻を前記ローカル時計手段に設定する直前に前記ローカル時計手段が出力した時刻に達するまで、前記ローカル時計手段の出力する時刻を出力することを阻止する時刻出力阻止手段と、を有することを特徴とする。
- 10 本発明によれば、時刻管理装置及び時刻管理方法の出力する時刻が、過去の時刻に戻ることはないので、意図的な時刻の改ざんの機会を減らす時刻管理装置及び時刻管理方法を提供できる。

図面の簡単な説明

- 15 本発明の他の目的、特徴及び利点は、添付の図面を参照しながら以下の詳細な説明を読むことにより一層明瞭となるであろう。
- 図1は、本発明の原理を示す第1の実施例を示す図である。
- 図2は、本発明の第2の実施例の構成を示す図である。
- 図3は、本発明の第2の実施例のメモリの構成を示す図である。
- 20 図4は、本発明の第2の実施例の動作のフローチャートを示す図である。
- 図5は、本発明の第2の実施例の動作のタイムチャートの第1の例を示す図である。
- 図6は、本発明の第2の実施例の動作のタイムチャートの第2の例を示す図である。
- 25 図7は、本発明の第2の実施例の動作のタイムチャートの第3の例を示す図である。
- 図8は、本発明の原理を示す第3の実施例を示す図である。
- 図9は、本発明の第4の実施例の構成を示す図である。
- 図10は、本発明の第4の実施例の動作のフローチャートを示す図である。

図 1 1 は、本発明の第 4 の実施例の動作のタイムチャートを示す図である。

図 1 2 は、本発明の第 4 の実施例を利用した署名システムの動作のフローチャートを示す図である。

5 発明を実施するための最良の形態

以下に、本発明を実施するための実施の形態について、図面を用いて説明する。

図 1 は、本発明の原理を示す第 1 の実施例の時刻管理システム 1 0 0 を示す図である。図 1 において、時刻管理システム 1 0 0 は、主に、電波時計送信所 1 0 1 と時刻管理装置 1 1 0 により構成される。電波時計送信所 1 0 1 は、送信アンテナ 1 0 2 から外部時刻情報 1 0 5 を送信する。図 1 の時刻管理装置 1 1 0 は、主に、受信アンテナ 1 1 1、受信回路 1 1 2、受信窓開閉回路 1 1 3、時刻差判定回路 1 1 4 及びローカルクロック回路 1 1 5 より構成される。

図 1 の時刻管理装置 1 1 0 の受信回路 1 1 2 は、電波時計送信所 1 0 1 からの外部時刻情報 1 0 5 を、アンテナ 1 1 1 を介して受信し、そして、時刻データ t として受信窓開閉回路 1 1 3 へ供給する。外部時刻情報 1 0 5 の形式については、図 5 を用いて後述する。

ローカルクロック回路 1 1 5 は、一旦初期値に設定された後に、自走して時刻データ t' を出力する。

受信窓開閉回路 1 1 3 は、時刻差判定回路 1 1 4 から供給される制御信号 $C 2$ に従って、受信窓を開き、この間に入力される時刻データ t を、時刻差判定回路 1 1 4 へ送る。

一方、ローカルクロック回路 1 1 5 も、時刻データ t' を、時刻差判定回路 1 1 4 へ供給する。

時刻差判定回路 1 1 4 は、時刻データ t と時刻データ t' の間の差の絶対値 δt を計算する。そして、この絶対値 δt が、予め定められた設定値 σ より小さい場合には、時刻差判定回路 1 1 4 は、時刻データ t を、時刻設定制御信号 $C 1$ を介して、ローカルクロック回路 1 1 5 に設定するように制御する。一方、この絶対値 δt が、予め定められた設定値 σ 以上の場合には、時刻差判定回路 1 1 4 は、ローカルクロック回路 1 1 5 をそのまま自走するように制御信号 $C 1$ を介して制

御する。

次に、ローカルクロック回路 1 1 5 が、制御信号 C 1 により、時刻データ t が設定されて再起動される又は自走するように制御されると、時刻差判定回路 1 1 4 は、制御信号 C 2 により、受信窓開閉回路 1 1 3 の受信窓を閉じる。これにより、受信回路 1 1 2 から受信窓開閉回路 1 1 3 へ入力する時刻データ t は、時刻差判定回路 1 1 4 に供給されないため、ローカルクロック回路 1 1 5 は、自走する。

時刻差判定回路 1 1 4 は、予め定められた時刻 T に達したときに、再び制御信号 C 2 を受信窓開閉回路 1 1 3 に送り、受信窓を開くように制御する。これにより、上述の動作を繰り返す。

以上により、時刻の改ざんに強く、且つ、長期間にわたって高精度な時刻を提供できる時刻管理システム 1 1 0 を実現できる。

次に、図 2、3、4、5、6 及び 7 を使用して、本発明の第 2 の実施例をさらに詳しく説明する。

図 2 は、本発明の第 2 の実施例の時刻管理システムの構成を示す図である。図 2 に示された時刻管理システム 1 0 0 は、主に、電波時計送信所 1 0 1 と時刻管理装置 1 1 0 により構成される。図 2 の時刻管理システム 1 0 0 において、図 1 と同一番号を付した構成要素は、同一の構成要素を示す。図 2 の時刻管理装置 1 1 0 の時刻差判定回路 1 1 4 は、主に、マイクロプロセッサ (CPU) 2 0 1 とメモリ 2 0 2 により構成される。

図 3 は、本発明の第 2 の実施例のメモリ 2 0 2 の構成を示す図である。メモリ 2 0 2 の領域 3 0 1 は、定期的に、時刻データ t を、ローカルクロック回路 1 1 5 に設定するか、又は、ランダムな時間間隔で時刻データ t を、ローカルクロック回路 1 1 5 に設定するかを示す情報を格納する。本実施例の場合には、定期的に、時刻データ t を、ローカルクロック回路 1 1 5 に設定する場合には、“0”を、また、ランダムな時間間隔で時刻データ t を、ローカルクロック回路 1 1 5 に設定する場合には、“1”を格納する。メモリ 2 0 2 の領域 3 0 2 は、ランダムな時間間隔で時刻データ t を、ローカルクロック回路 1 1 5 に設定する場合の時間間隔値であるランダム生成値を格納する。メモリ 2 0 2 の領域 3 0 3 は、前述の絶

対値 δt を判断する規準となる、予め定められた設定値 σ を格納する。メモリ 202 の領域 304 は、定期的に、時刻データ t を、ローカルクロック回路 115 に設定する場合の時間間隔値 T_1 を格納する。また、メモリ 202 の領域 305 は、時刻データ t を、ローカルクロック回路 115 に次に設定する時刻 T を格納する。

図 4 は、本発明の第 2 の実施例の動作のフローチャートを示す図である。次に、本発明の第 2 の実施例の動作を、図 4 に示すフローチャートを使用して説明する。

本発明の第 2 の実施例の動作は、ステップ 401 で開始する。

次に、ステップ 402 で、図 3 のメモリ 202 の各領域 301 から 304 へ、
10 図 3 を参照して前述したパラメータを設定する。領域 301 には、定期 (0) / ランダム (1) ビット、領域 302 には、ランダム生成値、領域 303 には、設定値 σ として、領域 304 には、時間間隔値 T_1 の、領域 305 には、時刻データ t を、ローカルクロック回路 115 に次に設定する時刻 T のそれぞれの初期値が設定される。

15 次に、ステップ 403 では、CPU 201 は、受信回路 112 に対して制御信号 210 により時刻データ t の受信を指示し且つ、受信窓開閉回路 113 へ制御信号 (C2) 211 により、受信窓を開くように指示する。

次に、ステップ 404 では、CPU 201 は、ローカルクロック回路 115 から、信号 212 を使用して、時刻データ t' を、CPU 201 上で実行される時刻誤差計算プログラムへ、ロードする。
20

次に、ステップ 405 では、CPU 201 は、受信窓開閉回路 113 から、信号 213 を使用して、時刻データ t を、CPU 201 上で実行される時刻誤差計算プログラムへ、ロードする。

次に、ステップ 406 では、CPU 201 により、時刻データ t と時刻データ
25 t' の時間差の絶対値 $\delta t = |t - t'|$ を計算する。そして、時間差の絶対値 δt が、予め定められた設定値 σ より小さいかどうか判断される。時間差の絶対値 δt が、予め定められた設定値 σ より小さいと判断された場合には、ステップ 407 へ進む。

ステップ 407 では、CPU 201 は、制御信号 (C1) 214 により制御し

て、受信窓開閉回路113から供給される時刻データ t を、信号212を介して、ローカルクロック回路115へ設定し、そして、ローカルクロック回路115を再起動する。

次にステップ408で、CPU201は、制御信号(C2)211により、受信窓開閉回路113の受信窓を閉じるように制御する。そして、ステップ409へ進む。

ステップ409では、CPU201は、ローカルクロック回路115の時刻データ t' と、時刻データ t を、ローカルクロック回路115に次に設定する時刻 T が比較される。

10 ステップ410では、時刻データ t' と T が等しい場合には、ステップ411へ進む。一方、時刻データ t' と T が等しくない場合には、ステップ409へ進み、ステップ409と410を繰り返す。

ステップ411では、メモリ202のビット301の値が”1”を有するか又は、”0”を有するかが判断される。メモリ202のビット301の値が”1”を有する場合には、ランダムな時間間隔で時刻データ t を、ローカルクロック回路115に設定することを示し、処理は、ステップ412へ進む。

ステップ412では、CPU201は、メモリ202の領域304の時間間隔値 T_1 へ、領域302に格納されたランダム生成値をロードする。

次にステップ413では、CPU201は、新たなランダム生成値を発生する。

20 次にステップ414では、CPU201は、ステップ413で発生した新たなランダム生成値を、メモリ202の領域302へ格納する。そして、処理は、ステップ416へ進む。

一方、ステップ411で、メモリ202のビット301の値が”0”を有する場合には、定期的に、時刻データ t を、ローカルクロック回路115に設定する場合することを示し、処理は、ステップ415へ進む。

25 ステップ415では、メモリ202の領域304の時間間隔値 T_1 へ、値”1”をロードする。そして、処理はステップ416へ進む。

ステップ416では、時刻データ t を、ローカルクロック回路115に次に設定する時刻 T を、更新するために、メモリ202の領域305へ($T+T_1$)を

書きこむ。そして処理は、ステップ403に進み、上述の処理を繰り返す。

一方、ステップ406で、時間差の絶対値 δt が、予め定められた設定値 σ 以上であると判断された場合には、ステップ417へ進む。

5 ステップ417では、CPU201は、ローカルクロック回路115を自走させるように、制御信号(C1)214を介して制御する。そして、制御信号(C2)211により受信窓開閉回路113を制御して、受信窓を閉める。

次にステップ418では、ローカルクロック回路115は、新たな時刻($T+T_1$)まで、自走したかが判断される。ローカルクロック回路115が、時刻($T+T_1$)まで、自走したと判断される場合には、処理はステップ403に進み、
10 上述の処理を繰り返す。一方、ローカルクロック回路115はまだ、時刻($T+T_1$)まで、自走していないと判断される場合には、処理はステップ417に進み、ステップ417とステップ418を繰り返す。

以上により、図2の時刻管理装置110のローカルクロック回路115より、時刻データ t 又は、時刻データ t' が出力される。

15 図5は、本発明の第2の実施例の動作のタイムチャートの第1の例を示す図である。図5(1)は、電波時計送信所101から送信される時刻データ t の時間を「秒」で示したものであり、ゼロ秒から次のゼロ秒までが、同一の分に対応する。

図5(2)は、電波時計送信所101から送信される時刻データ t の値のフォーマットを示す。この例では、最初の10秒間は「分」の値が送信され、次の10秒間は「時」の値が送信され、次の20秒間は「通算日」が送信され、次の10秒間は「年」の値が送信され、そして、最後の10秒間は「曜日」が送信される。
20

図5(3)は、受信窓開閉回路113の受信窓を示し、受信窓は、ローカルクロック回路115の出力する時刻データ t' と電波時計送信所101から送信される時刻データ t の値のずれにより、 ΔT だけ0秒からずれた時点TAで、CPU201により開かれる。一方、CPU201によりローカルクロック回路115に時刻データ t が設定された後に、時刻TCでCPU201により閉じられる。
25

図5(4)は、時刻差判定回路114による、時刻データ t の取り込みのタイ

ミングTBを示す。タイミングTBで、時刻データt1が、時刻差判定回路114に取りこまれる。

図5(5)は、時刻差判定回路114による、ローカルクロック回路115からの時刻データt1'の取りこみのタイミングTBを示す。上述のタイミングTBで、時刻データt1'も、時刻差判定回路114に取りこまれる。

図5(6)は、時刻差判定回路114による、時刻データtと時刻データt'の時間差の絶対値 $\delta t = |t - t'|$ を計算するタイミングを示す。

図5(7)は、時刻差判定回路114による、ローカルクロック回路115へ、新時刻データt1を設定するタイミングを示す。

図5(8)は、時刻差判定回路114により新時刻データt1を設定するタイミングに1秒程度の遅延がある場合の、ローカルクロック回路115へ、新時刻データt1を設定するタイミングを示す。このように遅延がある場合でも、図5(1)に示すように、電波時計送信所101から送信される時刻データt1の時間は秒で検出されることが可能であるので、設定時に1秒ずらすことにより、電波時計送信所101から送信される時刻データt1の時間に正確にローカルクロック回路115に時刻データt1を設定することができる。

最後に、図5(9)は、新たに時刻データt1が設定された後の、ローカルクロック回路115の出力する時刻データを示す。

図6は、本発明の第2の実施例の動作のタイムチャートの第2の例を示す図である。図6は、「日」単位で、受信窓開閉回路113の受信窓を開く構成を示す。

図6(1)は、電波時計送信所101から送信される時刻データtの時間を「時」単位で示したものであり、ゼロ時から次のゼロ時までが、同一の日に対応する。図6(2)は、受信窓開閉回路113の受信窓を示し、タイミングTAで開かれる。そして、時刻データtがローカルクロック回路115へ設定できたタイミングTBで、受信窓開閉回路113の受信窓が閉じられる。また、この日の終了のタイミングTCまで、時刻データtがローカルクロック回路115へ設定できない場合には、タイミングTCで受信窓開閉回路113の受信窓は閉じられる。

図7は、本発明の第2の実施例の動作のタイムチャートの第3の例を示す図である。図7は、「月」単位で、受信窓開閉回路113の受信窓を開く構成を示す。

図7(1)は、電波時計送信所101から送信される時刻データ t の時間を「日」単位で示したものであり、1日目から次の1日目までが、同一の月に対応する。

図7(2)は、受信窓開閉回路113の受信窓を開閉するタイミングを示す。

- 5 1日目の最初のタイミングTAで受信窓開閉回路113の受信窓が開かれる。そして、時刻データ t がローカルクロック回路115へ設定できたタイミングTBで、受信窓開閉回路113の受信窓が閉じられる。この図7(2)のタイミングTAからタイミングTBの動作は、図7で説明した動作と同一である。

- 図7(3)は、第1日目で、時刻データ t がローカルクロック回路115へ設定できなかった場合を示す。この場合には、例えば、2日目まで受信窓開閉回路113の受信窓が開かれ、図7で説明したのと同じ動作が実行される。図7(4)は、第1日目及び第2日目ともに、時刻データ t がローカルクロック回路115へ設定できなかった場合を示す。この場合には、例えば、3日目まで受信窓開閉回路113の受信窓が開かれ、図7で説明したのと同じ動作が実行される。

- 15 次に本発明の第3の実施例について説明する。

- 図8は、本発明の原理を示す第3の実施例の時刻管理システム100を示す図である。本実施例は、時刻管理装置110のローカルクロック回路115の示すローカルな時刻が、外部より供給される外部時刻情報105よりも進んでいる場合の実施例である。図8において、図1と同一番号の構成要素は、同一の構成要素を示す。図8に示された第3の実施例と、図1に示された第1の実施例の間の異なる点は、図8に示された第3の実施例は、クロックカウンタ801とゲート部802を有することである。

- クロックカウンタ801は、時刻差判定回路114により計算される、時刻データ t と時刻データ t' の間の差の絶対値 δt と、ローカルクロック回路115より出力されるクロックCLKを入力とし、ゲート部802へゲートの開閉信号803を送る。

ゲート部802は、クロックカウンタ801より出力される、開閉信号803に従って、ローカルクロック回路115よりゲート部802に供給される時刻データを、時刻管理装置110から出力するかどうかを制御する。

図8の時刻管理装置110の受信回路112は、電波時計送信所101からの外部時刻情報105を、受信し、そして、時刻データ t として受信窓開閉回路113へ供給する。外部時刻情報105の形式については、図5を用いて後述する。

ローカルクロック回路115は、一旦初期値に設定された後に、自走して時刻データ t' を出力する。

受信窓開閉回路113は、時刻差判定回路114から供給される制御信号C2に従って、受信窓を開き、この間に入力される時刻データ t を、時刻差判定回路114へ送る。

一方、ローカルクロック回路115も、時刻データ t' を、時刻差判定回路114へ供給する。

時刻差判定回路114は、時刻データ t と時刻データ t' の間の差の絶対値 δt を計算する。そして、この絶対値 δt が、予め定められた設定値 σ より小さい場合には、時刻差判定回路114は、時刻データ t を、時刻設定制御信号C1を介して、ローカルクロック回路115に設定するように制御する。一方、この絶対値 δt が、予め定められた設定値 σ 以上の場合には、時刻差判定回路114は、ローカルクロック回路115をそのまま自走するように制御信号C1を介して制御する。

ここで、時刻管理装置110のローカルクロック回路115の示すローカルな時刻が、外部より供給される外部時刻情報105よりも進んでいる場合には、外部より供給される外部時刻情報105を、時刻管理装置110内に取り込むと、時刻管理装置110の出力する時間が、僅かに過去の時点の時刻へ戻ることになる。

第3の実施例では、時刻差判定回路114が、時刻データ t を、時刻設定制御信号C1を介して、ローカルクロック回路115に設定するように制御する場合に、絶対値 δt を、クロックカウンタ801に設定する。そして、クロックカウンタ801は、開閉信号803により、ゲート部802を閉じるように制御する。そして、次に、クロックカウンタ801が、クロックCLKによりカウントアップされ、そして、設定された絶対値 δt にカウント値が達すると、開閉信号803により、ゲート部802を開くように制御する。このようにすることにより、

時刻管理装置 110 の出力する時間が、過去の時点の時刻へ戻ることを防止できる。

次に、ローカルクロック回路 115 が、制御信号 C1 により、時刻データ t が設定されて再起動される又は自走するように制御されると、時刻差判定回路 114 は、制御信号 C2 により、受信窓開閉回路 113 の受信窓を閉じる。これにより、受信回路 112 から受信窓開閉回路 113 へ入力する時刻データ t は、時刻差判定回路 114 に供給されないので、ローカルクロック回路 115 は、自走する。

時刻差判定回路 114 は、予め定められた時刻 T に達したときに、再び制御信号 C2 を受信窓開閉回路 113 に送り、受信窓を開くように制御する。これにより、上述の動作を繰返す。

以上により、時刻の改ざんに強く、且つ、長期間にわたって高精度な時刻を提供できる時刻管理装置 110 を実現できかつ、時刻管理装置 110 から出力する時刻がこの時点の時刻に戻ることはない、信頼性ある時刻を出力できる。

次に、図 9、10、11 及び 12 を使用して、本発明の第 2 の実施例をさら詳しく説明する。

図 9 は、本発明の第 4 の実施例の構成を示す図である。本実施例は、時刻管理装置 110 のローカルクロック回路 115 の示すローカルな時刻が、外部より供給される外部時刻情報 105 よりも進んでいる場合の実施例である。図 9 において、図 2 と同一番号の構成要素は、同一の構成要素を示す。図 9 に示された第 4 の実施例と、図 2 に示された第 2 の実施例の間の異なる点は、図 9 に示された第 3 の実施例は、CPU 201 が、クロックカウンタの機能を含むことと、ゲート部 802 を有することである。

クロックカウンタの機能及びゲート部 802 の動作は、図 8 を参照して接続された第 3 の実施例と同一である。

図 10 は、本発明の第 4 の実施例の動作のフローチャートを示す図である。図 10 において、図 4 と同一番号を付したステップは、同一のステップを示すものとする。

図 10 に示す本発明の第 4 の実施例の動作のフローチャートと図 4 に示す本発

明の第2の実施例の動作のフローチャートの相違点は、図4のステップ407と408が、図10のステップ1001と置き換えられたことである。

図10のステップ406では、CPU201により、時刻データ t と時刻データ t' の時間差の絶対値 $\delta t = |t - t'|$ を計算する。そして、時間差の絶対値 δt が、予め定められた設定値 σ より小さいかどうか決定される。時間差の絶対値 δt が、予め定められた設定値 σ より小さいと判断された場合には、ステップ1001へ進む。

ステップ1001では、CPU201は、時刻データ t を、時刻設定制御信号C1を介して、ローカルクロック回路115に設定するように制御する。この場合には、CPU201から開閉信号803が出力され、これにより、ゲート部802を閉じるように制御する。そして、次に、CPU201内のクロックカウンタ機能が、クロックCLKによりカウントアップされ、そして、設定された絶対値 δt にカウント値が達すると、開閉信号803により、ゲート部802を開くように制御する。このようにすることにより、時刻管理装置110の出力する時間が、過去の時点の時刻へ戻ることを防止できる。

図11は、本発明の第4の実施例の動作のタイムチャートを示す図である。図11の横軸は、電波時計送信所101より送られる外部時刻情報105による時間の経過を示し、一方、図11の縦軸は、ローカルクロック回路115の自走クロックによる時間の経過を示す。

外部時刻情報105の時間とローカルクロック回路115の自走クロックによる時間の経過速度が一致している場合には、増加角度 45° の直線1101が示すように、外部時刻情報105による時間の経過とローカルクロック回路115の自走クロックによる時間の経過が一致する。一方、ローカルクロック回路115の自走クロックによる時間の経過速度の方が外部時刻情報105による時間の経過速度よりも速い場合には、直線1102のように、ローカルクロック回路115の自走クロックが進む。ローカルクロック回路115の自走クロックによる時間の経過速度の方が外部時刻情報105による時間の経過速度よりも遅い場合には、直線1103のように、ローカルクロック回路115の自走クロックが遅れる。

ここで、直線1102に示されたように、ローカルクロック回路115の自走クロックが進む場合において、時刻Tでローカルクロック回路115が外部時刻情報105による時刻データtに設定されると、時刻Tでは、ローカルクロック回路115はその出力する時刻が、過去にローカルクロック回路115が出力した時刻に戻ることであり、時刻署名の信頼性が低下する。

そこで、ローカルクロック回路115の出力する時刻が、時刻Tにおいて外部時刻情報105による時刻データtに設定された後に、時刻データtと時刻データt'の時間差の絶対値 δt の間だけ、ゲート部802により、時刻管理装置110から出力するのを禁止する。これは、時刻TからT'の間は、時刻管理装置110からの時刻出力を停止することに想到する。そして、この期間の経過後に、即ち、時刻T'から、時刻の出力を開始することにより、以前にローカルクロック回路115が出力した時刻に戻ることを防止できる。

尚、ローカルクロック回路115の出力するローカルクロック時刻の方が遅れているときは、外部時刻情報105に一致させても過去の時刻へ戻ることがないので、 δt の期間、出力を阻止する必要はない。

図12は、本発明の第4の実施例を利用した署名システムの動作のフローチャートを示す図である。例えば、本発明を利用した、署名システムのソフトウェア等により実行される。

ステップ1201で本署名システムの動作は開始する。

次にステップ1202で、署名システムのソフトウェアは、図9の開閉信号803が、オンかオフかを判断する。ここで、開閉信号803がオンの場合には、図9のゲート部802は、ローカルクロック回路115の出力するローカルクロック804を時刻管理装置110から出力する。開閉信号803がオフの場合には、ステップ1202を繰り返す。

次にステップ1203では、署名システムのソフトウェアは、時刻管理装置110より出力される時刻が、全て0又は、全て1でないかを判断する。いずれかの場合には、処理はステップ1202へ戻り、上述の処理を繰り返す、正規に時刻が出力されるまで待つ。いずれでもない場合には、処理はステップ1204へ進む。

ステップ1204では、署名システムのソフトウェアは、ローカルクロック回路からゲートを通して送られてくる時刻出力を入手する。

ステップ1205では、署名システムのソフトウェアは、署名する入力データを取得する。

- 5 次にステップ1206では、署名システムのソフトウェアは、keyを取得する。

そして、ステップ1207で、署名システムのソフトウェアは、入力データと時刻出力とkeyを用いて時刻署名付きデータを作成する。

- そして、ステップ1208で、署名システムのソフトウェアは、作成した時刻
10 署名付きデータを記憶装置に格納する。

最後にステップ1209で、署名システムのソフトウェアの処理は終了する。

以上のように、本発明を利用した、署名システムのソフトウェア等により、時刻署名付きデータを作成できる。

請 求 の 範 囲

1. 予め定められた時間幅内で外部時刻を取り込む外部時刻取込ステップと、
自走時刻を出力するローカル時計ステップと、
- 5 前記外部時刻取込ステップにより取り込んだ前記外部時刻と、前記ローカル時計
ステップの出力する前記自走時刻との差を計算し、前記差が予め定められた値よ
り小さい場合には前記外部時刻を前記ローカル時計ステップに設定し、そして、
前記差が予め定められた値以上の場合には前記外部時刻を前記ローカル時計ステ
ップに設定しない、時刻差判定ステップとを有することを特徴とする、時刻管理
10 方法。
2. 前記外部時刻取込ステップによる前記外部時刻の取り込みは、一定の時間間隔
で実行されることを特徴とする、請求項1に記載の時刻管理方法。
- 15 3. 前記外部時刻取込ステップによる前記外部時刻の取り込みは、ランダムな時間
間隔で実行されることを特徴とする、請求項1に記載の時刻管理方法。
4. 前記予め定められた時間幅内で、前記外部時刻取込ステップにより、前記外
部時刻が取り込めない場合には、前記予め定められた時間幅を拡張して、前記外
20 部時刻取込ステップによる前記外部時刻の取り込みを継続する、請求項2に記載の
時刻管理方法。
5. 前記予め定められた時間幅内で、前記外部時刻取込ステップにより、前記外
部時刻が取り込めない場合には、前記予め定められた時間幅を拡張して、前記外
25 部時刻取込ステップによる前記外部時刻の取り込みを継続する、請求項3に記載の
時刻管理方法。
6. 予め定められた時間幅内で外部時刻を取り込む外部時刻取込手段と、
自走時刻を出力するローカル時計手段と、

前記外部時刻取込手段により取り込んだ前記外部時刻と、前記ローカル時計手段の出力する前記自走時刻との差を計算し、前記差が予め定められた値より小さい場合には前記外部時刻を前記ローカル時計手段に設定し、そして、前記差が予め定められた値以上の場合には前記外部時刻を前記ローカル時計手段に設定しない、時刻差判定手段とを有することを特徴とする、時刻管理装置。

7. 前記外部時刻取込手段による前記外部時刻の取り込みは、一定の時間間隔で実行されることを特徴とする、請求項6に記載の時刻管理装置。

10 8. 前記外部時刻取込手段による前記外部時刻の取り込みは、ランダムな時間間隔で実行されることを特徴とする、請求項6に記載の時刻管理装置。

9. 前記予め定められた時間幅内で、前記外部時刻取込手段により、前記外部時刻が取り込めない場合には、前記予め定められた時間幅を拡張して、前記外部時刻取込手段による前記外部時刻の取り込みを継続する、請求項7に記載の時刻管理装置。

10. 前記予め定められた時間幅内で、前記外部時刻取込手段により、前記外部時刻が取り込めない場合には、前記予め定められた時間幅を拡張して、前記外部時刻取込手段による前記外部時刻の取り込みを継続する、請求項8に記載の時刻管理装置。

11. 予め定められた時間幅内で外部時刻を取り込む外部時刻取込ステップと、自走時刻を出力するローカル時計ステップと、

25 前記外部時刻取込ステップにより取り込んだ前記外部時刻と、前記ローカル時計ステップの出力する前記自走時刻との差を計算し、前記差が予め定められた値より小さい場合には前記外部時刻を前記ローカル時計ステップに設定し、そして、前記差が予め定められた値以上の場合には前記外部時刻を前記ローカル時計ステップに設定しない、時刻差判定ステップと、

- 前記ローカル時計ステップに設定された前記外部時刻が、前記外部時刻を前記ローカル時計ステップに設定する直前に前記ローカル時計ステップが出力した時刻よりも、過去の時刻に等しい場合には、前記ローカル時計ステップが出力する時刻が、前記外部時刻を前記ローカル時計ステップに設定する直前に前記ローカル時計ステップが出力した前記過去の時刻に達するまで、前記ローカル時計ステップの出力する時刻を出力することを阻止する時刻出力阻止ステップと、を有することを特徴とする、時刻管理方法。
- 5
- 1 2. 前記外部時刻取込ステップによる前記外部時刻の取り込みは、一定の時間間隔で実行されることを特徴とする、請求項 1 1 に記載の時刻管理方法。
- 10
- 1 3. 前記外部時刻取込ステップによる前記外部時刻の取り込みは、ランダムな時間間隔で実行されることを特徴とする、請求項 1 1 に記載の時刻管理方法。
- 15
- 1 4. 前記予め定められた時間幅内で、前記外部時刻取込ステップにより、前記外部時刻が取り込めない場合には、前記予め定められた時間幅を拡張して、前記外部時刻取込ステップによる前記外部時刻の取り込みを継続する、請求項 1 2 に記載の時刻管理方法。
- 20
- 1 5. 前記予め定められた時間幅内で、前記外部時刻取込ステップにより、前記外部時刻が取り込めない場合には、前記予め定められた時間幅を拡張して、前記外部時刻取込ステップによる前記外部時刻の取り込みを継続する、請求項 1 3 に記載の時刻管理方法。
- 25
- 1 6. 予め定められた時間幅内で外部時刻を取り込む外部時刻取込手段と、
自走時刻を出力するローカル時計手段と、
前記外部時刻取込手段により取り込んだ前記外部時刻と、前記ローカル時計手段の出力する前記自走時刻との差を計算し、前記差が予め定められた値より小さい場合には前記外部時刻を前記ローカル時計手段に設定し、そして、前記差が予

め定められた値以上の場合には前記外部時刻を前記ローカル時計手段に設定しない、時刻差判定手段と、

- 前記ローカル時計手段に設定された前記外部時刻が、前記外部時刻を前記ローカル時計手段に設定する直前に前記ローカル時計手段が出力した時刻よりも、過去
- 5 去の時刻に等しい場合には、前記ローカル時計手段が出力する時刻が、前記外部時刻を前記ローカル時計手段に設定する直前に前記ローカル時計手段が出力した前記過去の時刻に達するまで、前記ローカル時計手段の出力する時刻を出力することを阻止する時刻出力阻止手段と、を有することを特徴とする、時刻管理装置。

- 10 17. 前記外部時刻取込手段による前記外部時刻の取り込みは、一定の時間間隔で実行されることを特徴とする、請求項16に記載の時刻管理装置。

18. 前記外部時刻取込手段による前記外部時刻の取り込みは、ランダムな時間間隔で実行されることを特徴とする、請求項16に記載の時刻管理装置。

15

19. 前記予め定められた時間幅内で、前記外部時刻取込手段により、前記外部時刻が取り込めない場合には、前記予め定められた時間幅を拡張して、前記外部時刻取込手段による前記外部時刻の取り込みを継続する、請求項17に記載の時刻管理装置。

20

20. 前記予め定められた時間幅内で、前記外部時刻取込手段により、前記外部時刻が取り込めない場合には、前記予め定められた時間幅を拡張して、前記外部時刻取込手段による前記外部時刻の取り込みを継続する、請求項18に記載の時刻管理装置。

25

FIG.1

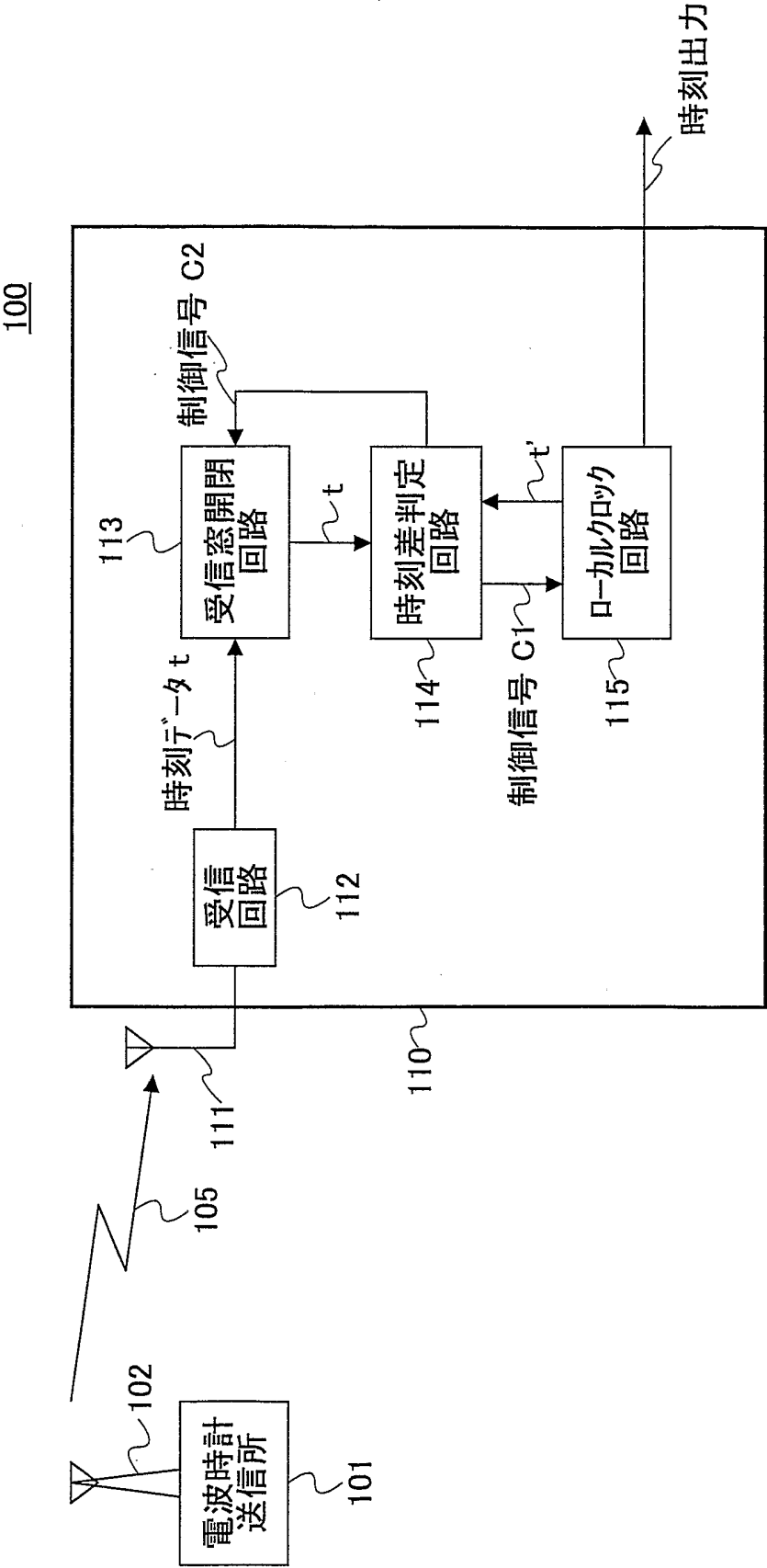


FIG. 2

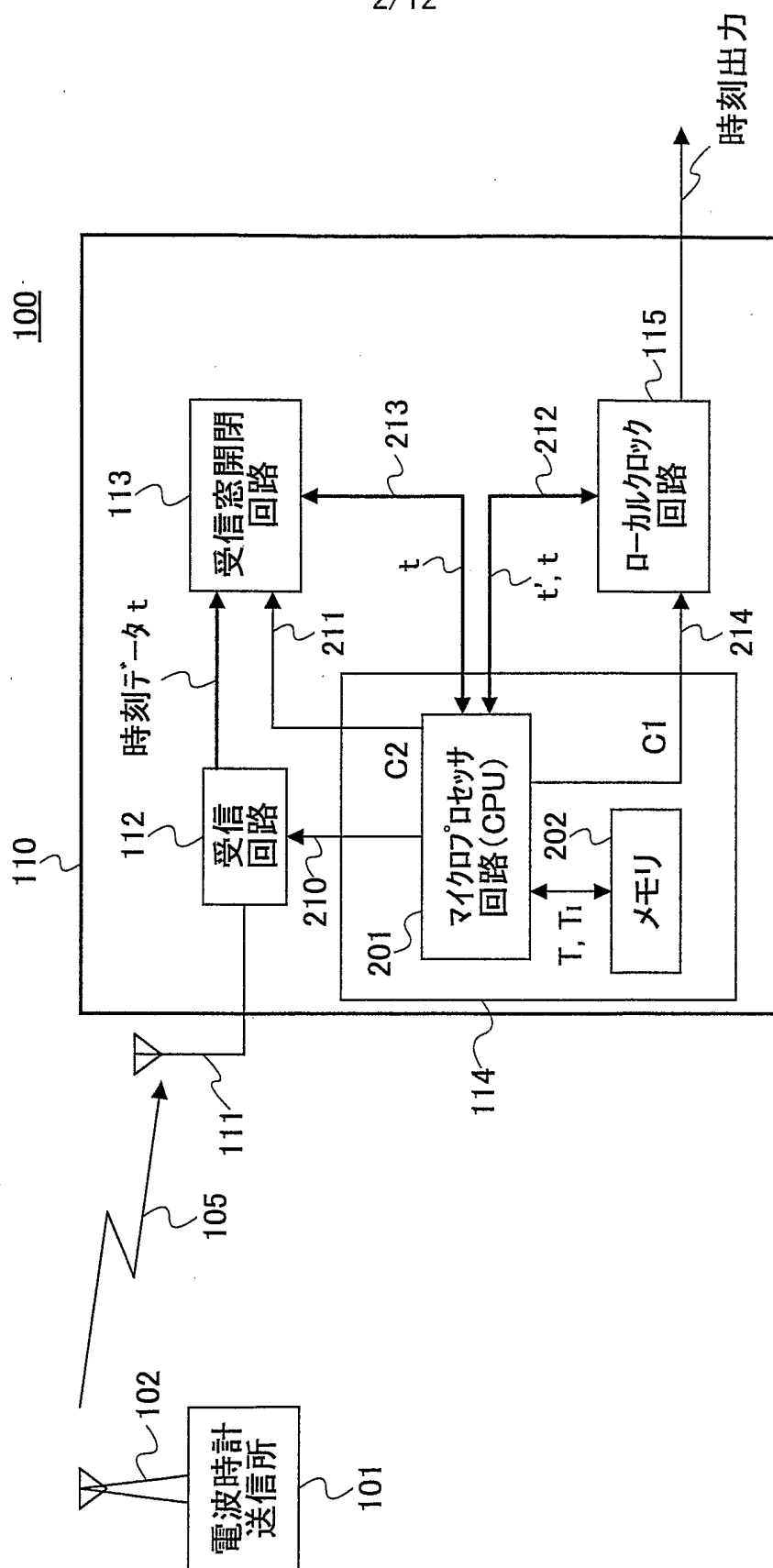
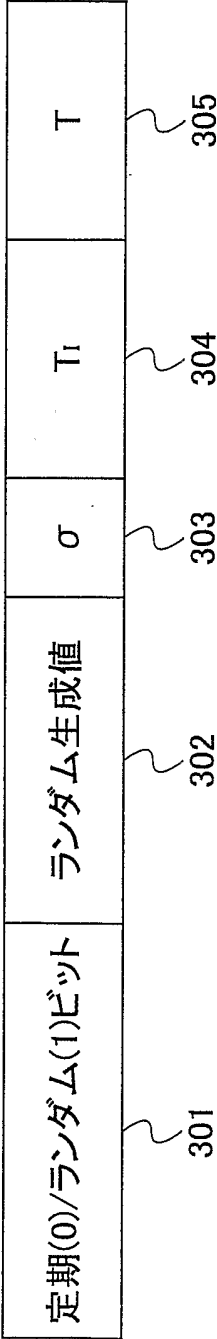


FIG.3

202



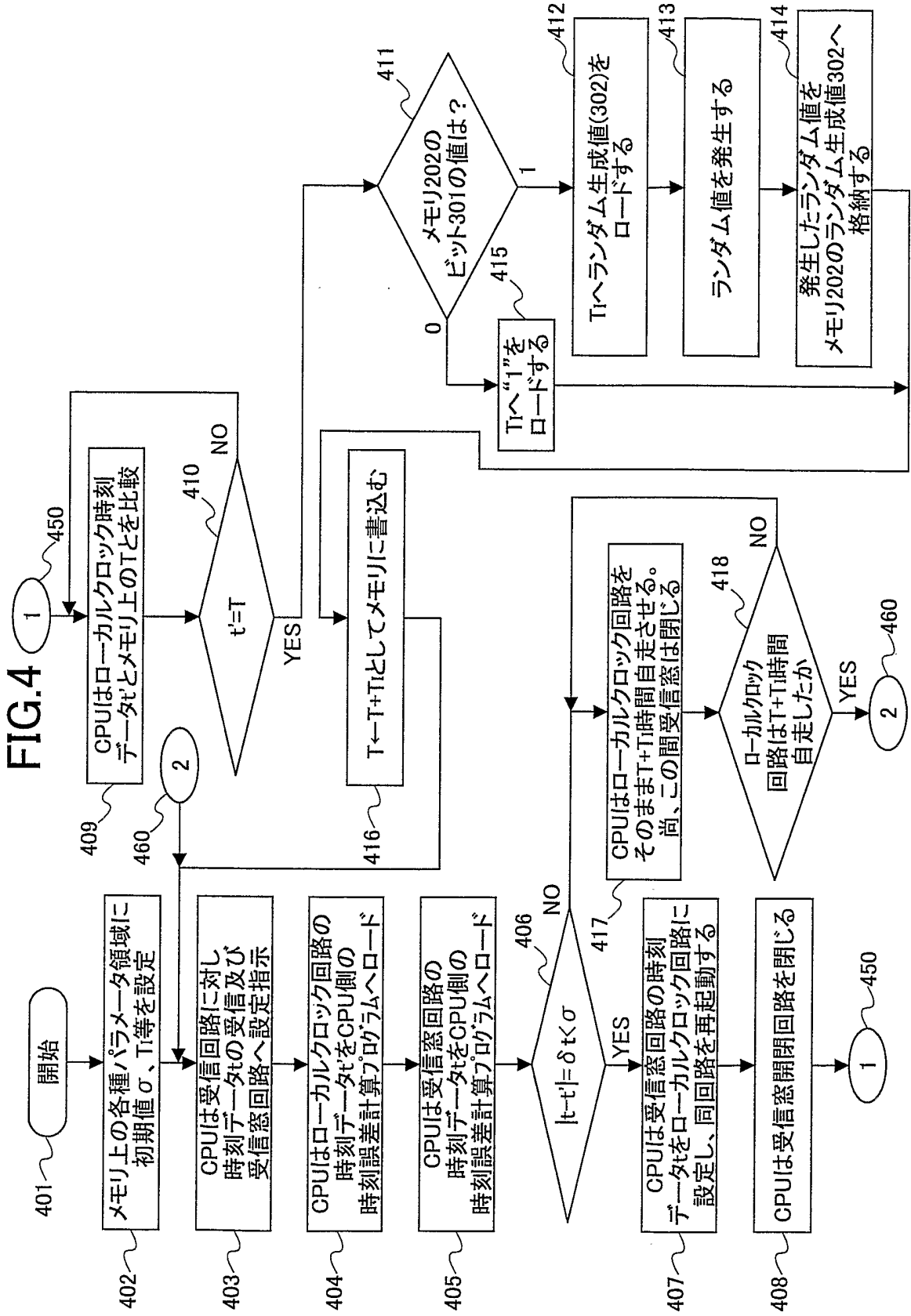


FIG.5

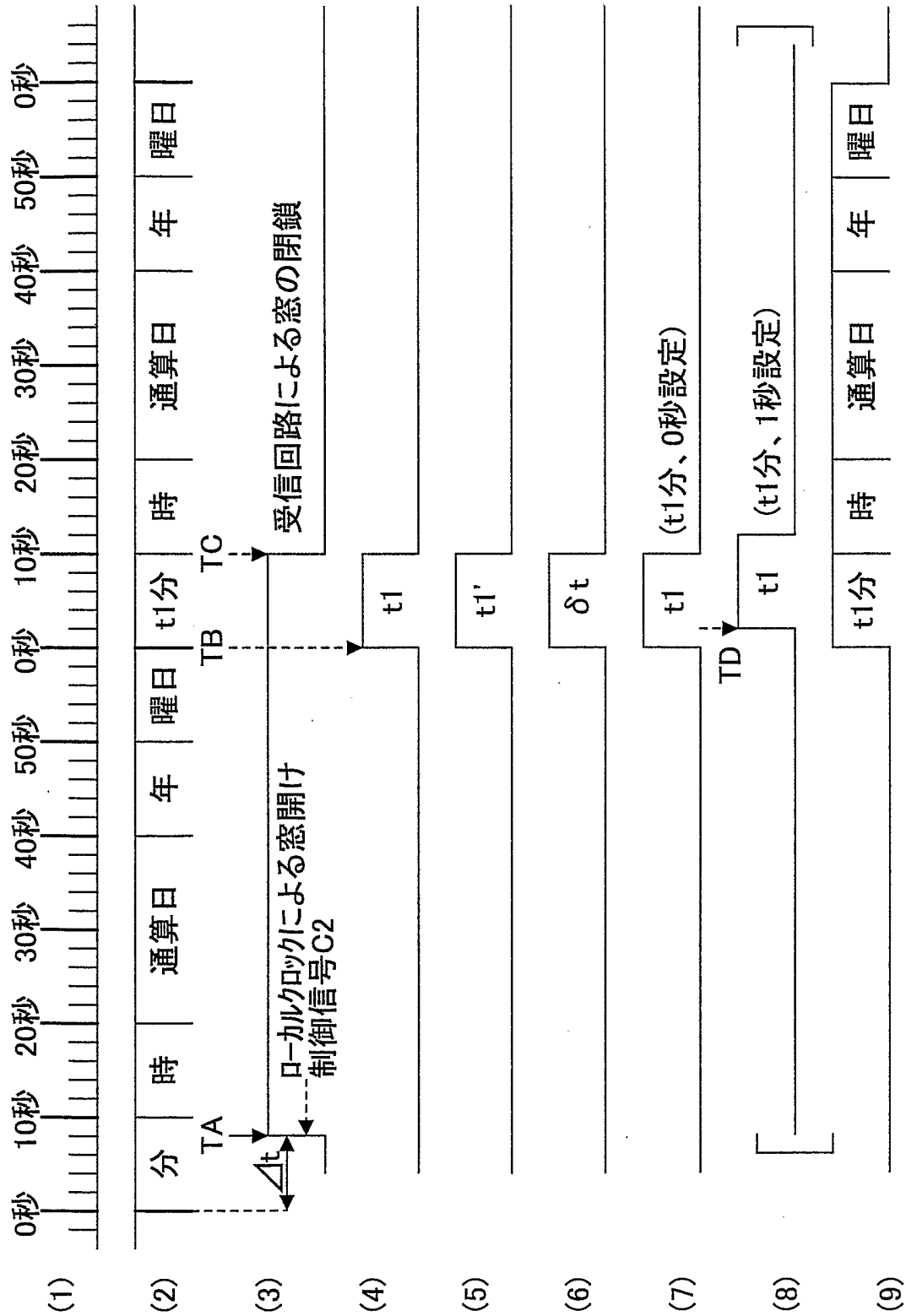


FIG.6



FIG.7

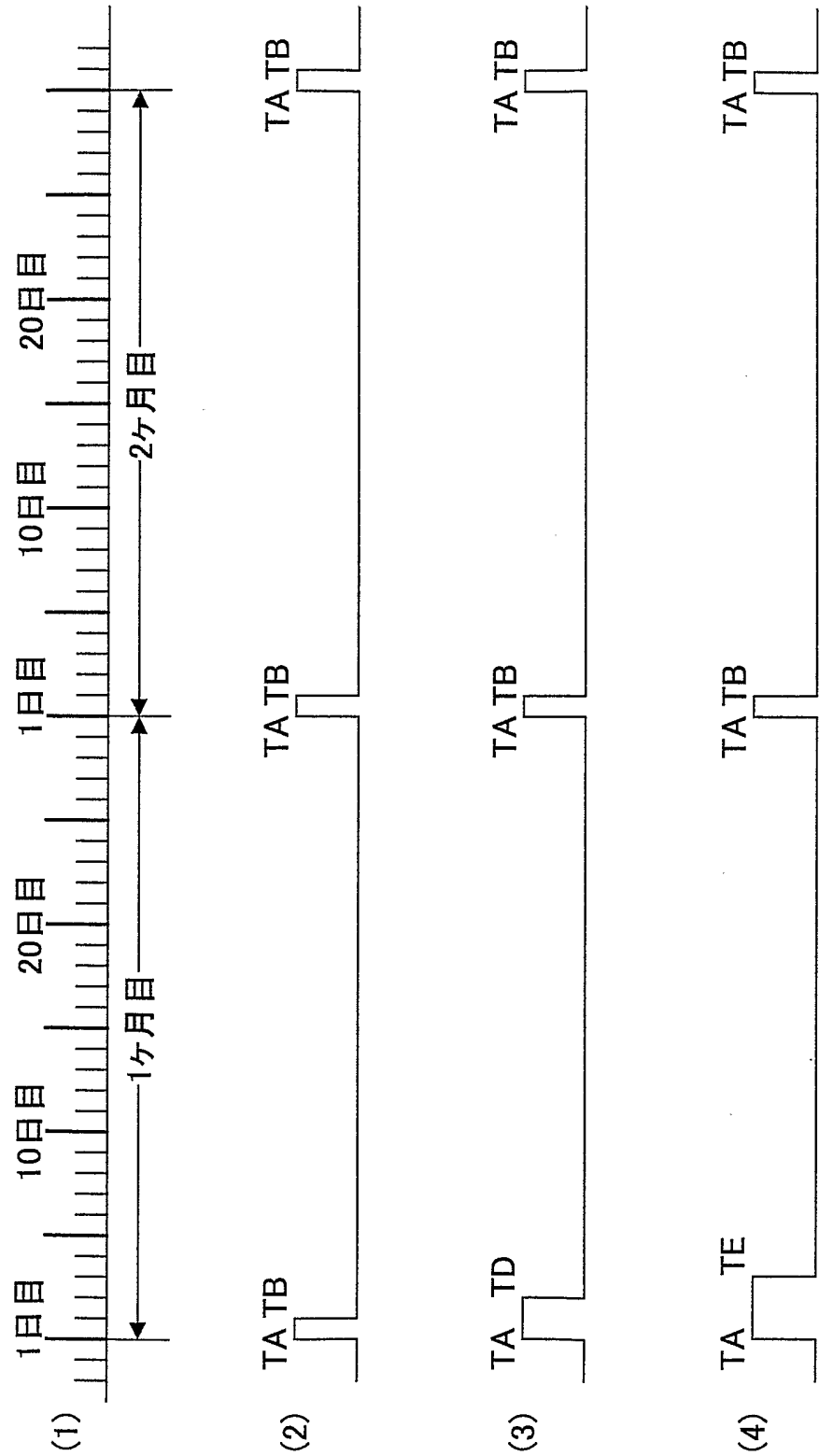


FIG.8

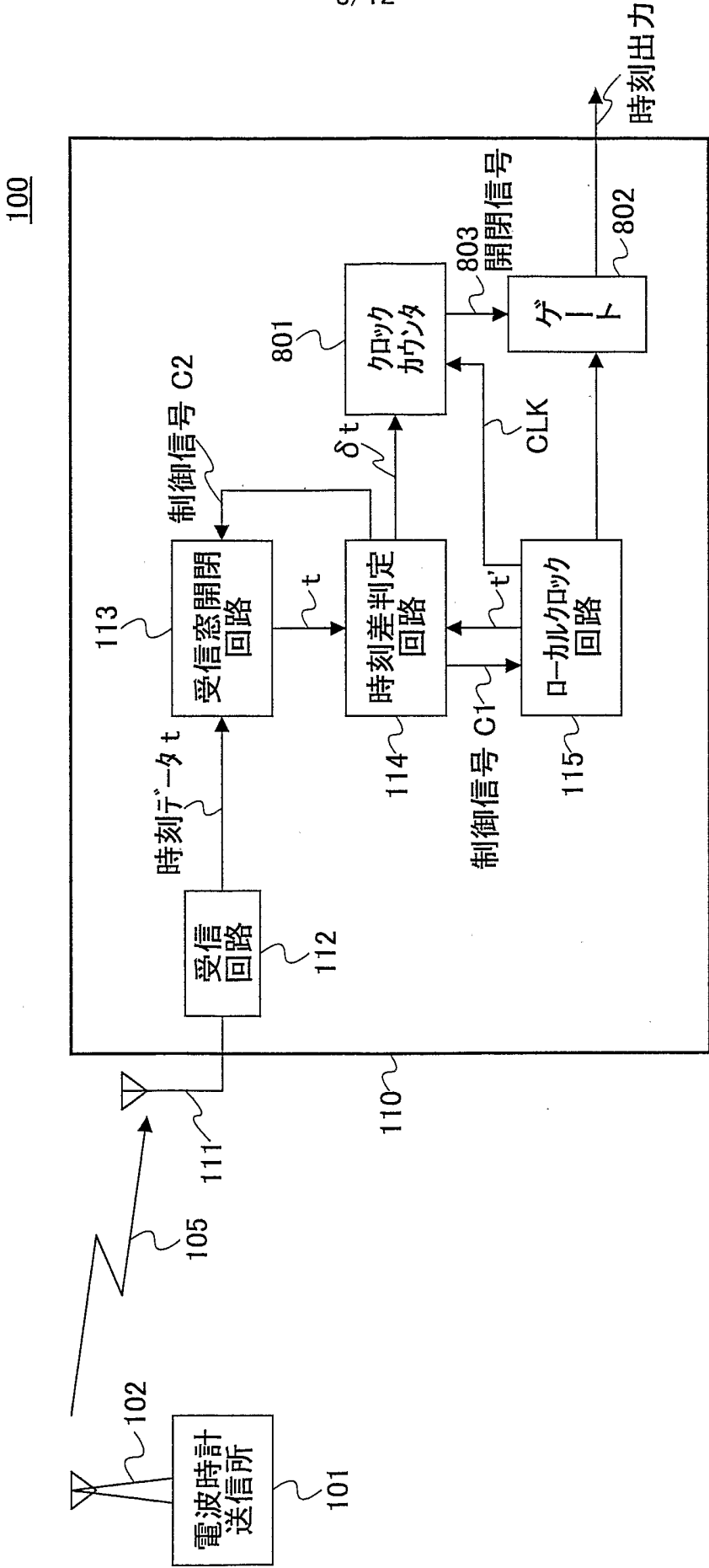
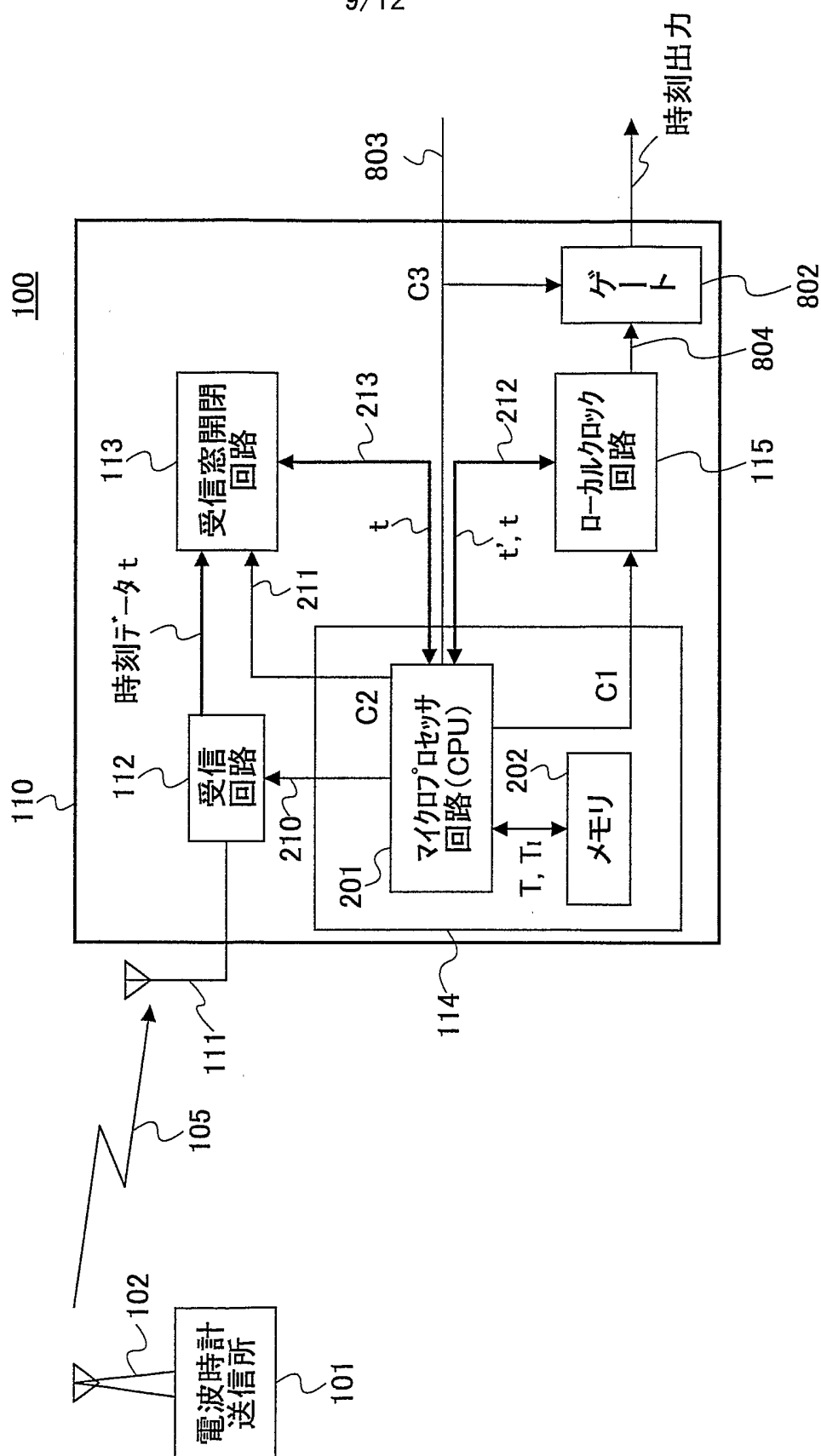


FIG. 9



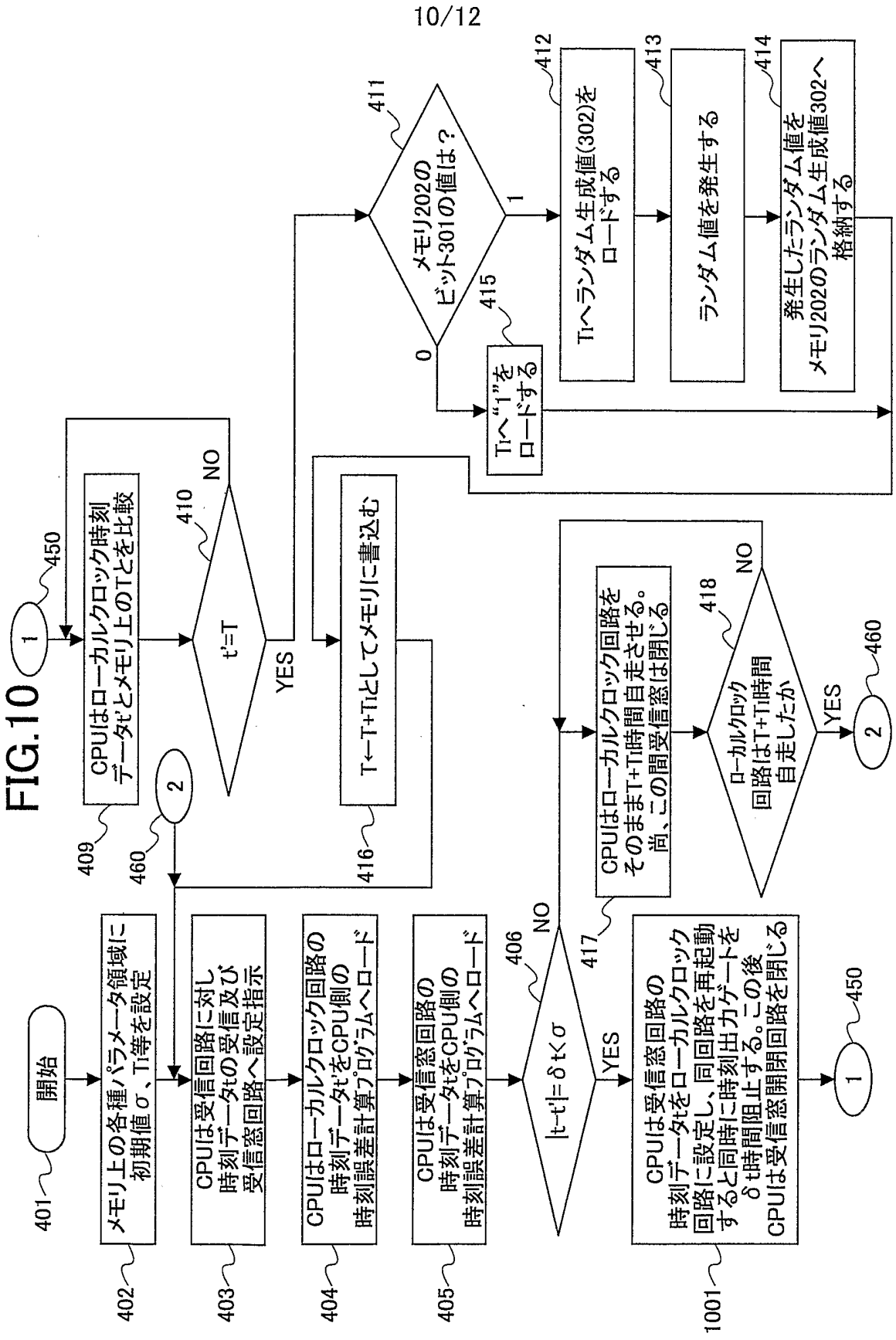
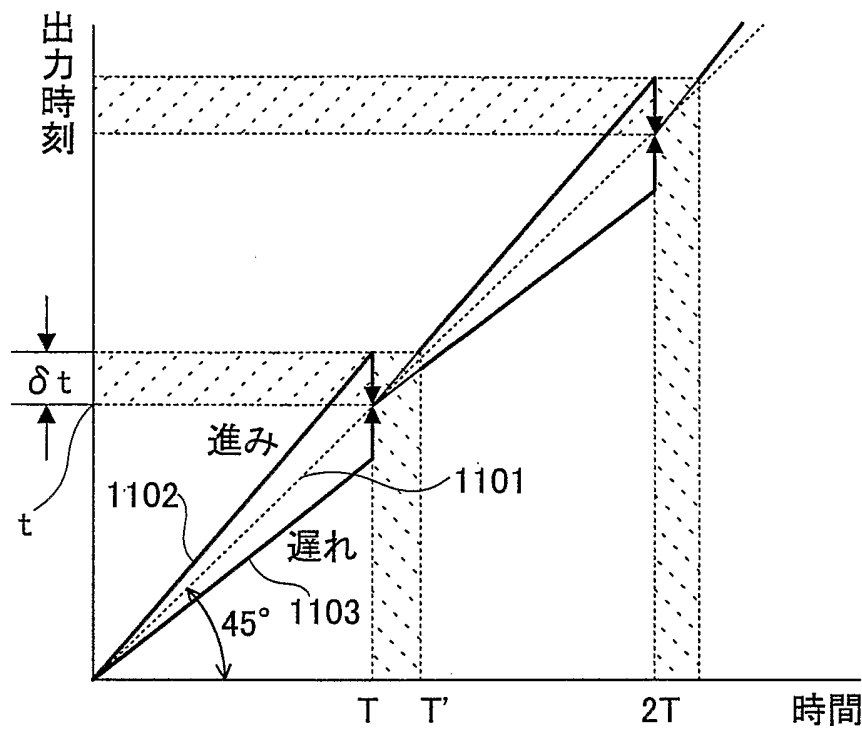
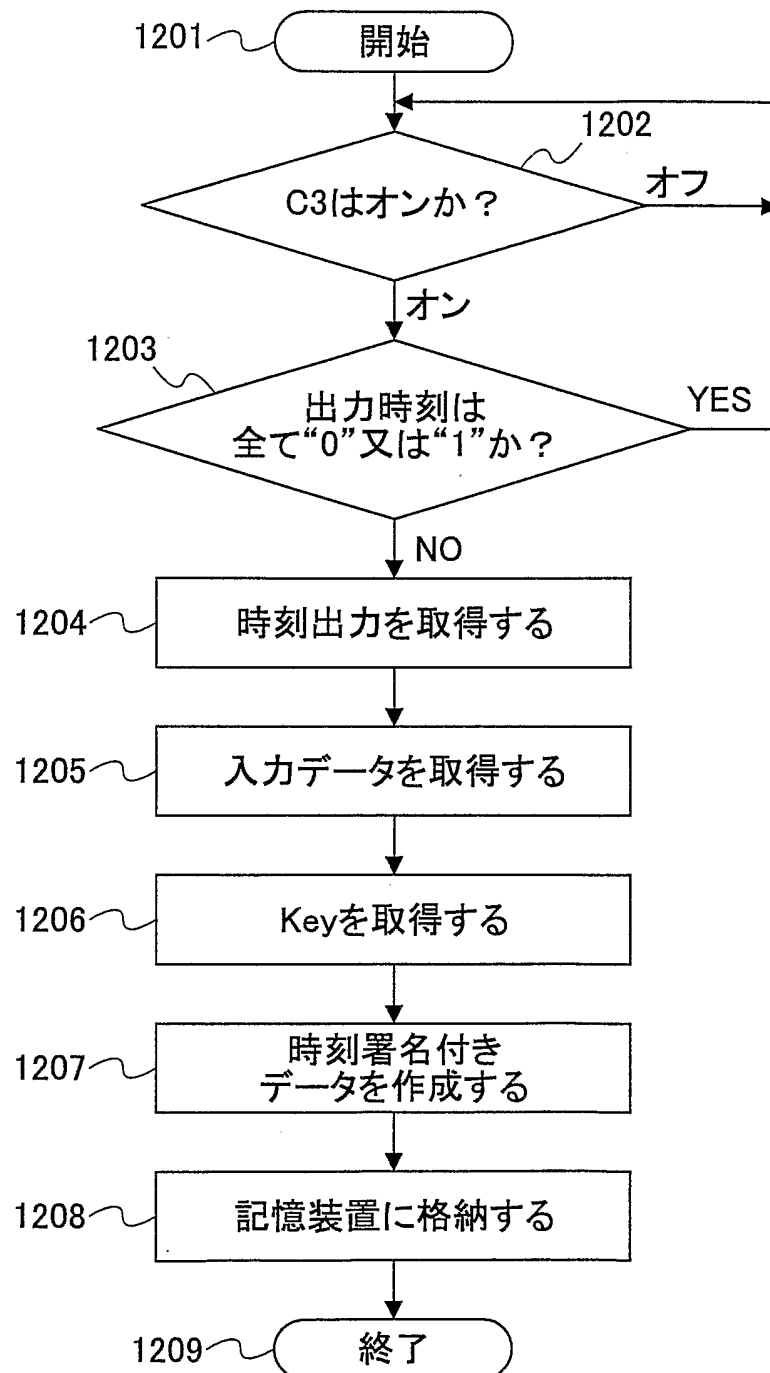


FIG.11



12/12

FIG.12



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/06669

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G04G5/00, G06F1/14

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 G04G5/00, G04G7/00, G06F1/14

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	1996-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Toroku Jitsuyo Shinan Koho	1994-2003

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 Y A	JP 2002-22863 A (Toyo Communication Equipment Co., Ltd.), 23 January, 2002 (23.01.02), Full text; all drawings (Family: none)	1, 2, 6, 7 4, 9 3, 5, 8, 10, 11-20
X Y A	JP 2002-374473 A (Sharp Corp.), 26 December, 2002 (26.12.02), Full text; all drawings (Family: none)	1, 2, 6, 7 4, 9 3, 5, 8, 10, 11-20
Y A	JP 10-170667 A (Sharp Corp.), 26 June, 1998 (26.06.98), Claims (Family: none)	4, 9 5, 10, 14, 15, 19, 20

☒ 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 document 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
11 July, 2003 (11.07.03)

Date of mailing of the international search report
29 July, 2003 (29.07.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/06669

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 58-182582 A (NEC Corp.), 25 October, 1983 (25.10.83), Full text; all drawings (Family: none)	11-20
A	JP 2000-65966 A (Nippon Telegraph And Telephone Corp.), 03 March, 2000 (03.03.00), Full text; all drawings (Family: none)	1-20

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl⁷ G04G 5/00, G06F 1/14

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. Cl⁷ G04G 5/00, G04G 7/00, G06F 1/14

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 1971-2003年
日本国実用新案登録公報 1996-2003年
日本国登録実用新案公報 1994-2003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	JP 2002-22863 A (東洋通信機株式会社) 2002.01.23, 全文, 全図 (ファミリーなし)	1, 2, 6, 7
Y		4, 9
A		3, 5, 8, 10, 11-20

☒ 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
11.07.03

国際調査報告の発送日
29.07.03

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)
五関 統一郎



2F 2904

電話番号 03-3581-1101 内線 3216

C (続き) . 関連すると認められる文献

引用文献の カテゴリ*	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	J P 2002-374473 A (シャープ株式会社) 2002. 12. 26, 全文, 全図 (ファミリーなし)	1, 2, 6, 7
Y		4, 9
A		3, 5, 8, 10, 11-20
Y	J P 10-170667 A (シャープ株式会社) 1998. 06. 26, 【特許請求の範囲】 (ファミリーなし)	4, 9
A		5, 10, 14, 15, 19, 20
A	J P 58-182582 A (日本電気株式会社) 1983. 10. 25, 全文, 全図 (ファミリーなし)	11-20
A	J P 2000-65966 A (日本電信電話株式会社) 2000. 03. 03, 全文, 全図 (ファミリーなし)	1-20