

(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
2010年9月10日(10.09.2010)

PCT

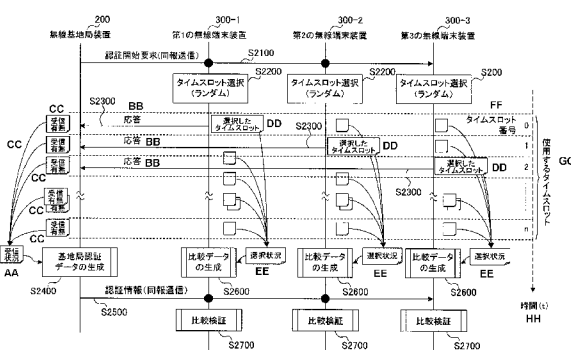
(10) 国際公開番号
WO 2010/100838 A1

- (51) 国際特許分類:
H04W 12/06 (2009.01) H04W 72/04 (2009.01)
G06K 17/00 (2006.01) H04W 84/10 (2009.01)
G06K 19/07 (2006.01)
- (21) 国際出願番号: PCT/JP2010/000951
- (22) 国際出願日: 2010年2月16日(16.02.2010)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2009-051319 2009年3月4日(04.03.2009) JP
- (71) 出願人(米国を除く全ての指定国について): パナソニック株式会社(PANASONIC CORPORATION) [JP/JP]; 〒5718501 大阪府門真市大字門真1006番地 Osaka (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 稲富康朗 (INATOMI, Yasuaki), 伊藤快(ITO, Hayashi).
- (74) 代理人: 鷺田 公一(WASHIDA, Kimihito); 〒2060034 東京都多摩市鶴牧1丁目24-1 新都市センタービル5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, 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, KE, KG, KM, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, 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, 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, SE, SI, SK, SM, 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(条約第21条(3))

(54) Title: WIRELESS BASE STATION APPARATUS, WIRELESS TERMINAL APPARATUS, AND BASE STATION AUTHENTICATION METHOD

(54) 発明の名称: 無線基地局装置、無線端末装置、および基地局認証方法

[図5]



200 WIRELESS BASE STATION APPARATUS
300-1 FIRST WIRELESS TERMINAL APPARATUS
300-2 SECOND WIRELESS TERMINAL APPARATUS
300-3 THIRD WIRELESS TERMINAL APPARATUS
S2100 AUTHENTICATION START REQUEST (BROADCAST COMMUNICATION)
S2200 TIMESLOT SELECTION (RANDOM)
S2300 RESPONSE
AA RECEPTION STATUS
BB RESPONSE
CC RECEIVED, Y/N?
DD SELECTED TIMESLOT
EE SELECTION STATUS
S2400 GENERATION OF BASE STATION AUTHENTICATION DATA
S2500 AUTHENTICATION INFORMATION (BROADCAST COMMUNICATION)
S2600 GENERATION OF COMPARISON DATA
S2700 COMPARISON VERIFICATION
GG USED TIMESLOT
HH TIME(T)
FF TIMESLOT NUMBER

(57) Abstract: A base station authentication method which allows base station authentication to be performed by more wireless terminal apparatuses within a fixed period of time. This method is a base station authentication method for TDMA wireless communication and comprises: a step in which wireless terminal apparatuses (300) select timeslots (S2200) and use the selected timeslots to transmit, to a wireless base station apparatus (200), responses indicating the start of base station authentication (S2300); a step in which the wireless base station apparatus (200) generates base station authentication data summarizing information indicating whether there has been a response for each timeslot, for the plurality of timeslots (S2400), and transmits the generated base station authentication data to the wireless terminal apparatuses (300) (S2500); and a step in which the wireless terminal apparatuses (300) perform base station authentication on the transmission origin of the base station authentication data, based on whether the received base station authentication data indicates that there were responses at the selected timeslots (S2700).

(57) 要約:

[続葉有]

WO 2010/100838 A1



一定時間内でより多くの無線端末装置が基地局認証を行うことができる基地局認証方法。この方法は、時分割多元接続の無線通信における基地局認証方法であって、無線端末装置（３００）が、タイムスロットを選択し（Ｓ２２００）、選択したタイムスロットを用いて、基地局認証を開始することを示す応答を無線基地局装置（３００）に送信するステップ（Ｓ２３００）と、無線基地局装置（２００）が、タイムスロット毎の応答の有無を示す情報を複数のタイムスロットについて集約した基地局認証データを生成し（Ｓ２４００）、生成した基地局認証データを無線端末装置（３００）に送信するステップ（Ｓ２５００）と、無線端末装置（３００）が、受信した基地局認証データが、選択したタイムスロットにおいて応答が有ったことを示すか否かに基づいて、基地局認証データの送信元に対する基地局認証を行うステップ（Ｓ２７００）とを有する。

明 細 書

発明の名称：

無線基地局装置、無線端末装置、および基地局認証方法

技術分野

[0001] 本発明は、時分割多元接続により無線通信を行う無線基地局装置、無線端末装置、および基地局認証方法に係り、特に、複数の無線端末装置が無線基地局装置に対して認証を行う無線通信システムにおける無線基地局装置、無線端末装置、および基地局認証方法に関する。

背景技術

[0002] 従来、多くの無線通信システムにおいて、無線通信装置間で重要なデータの送受信（以下「データ通信」という）を行うときに、通信相手が真正な相手であるかどうかを確認するための認証が行われている。

[0003] 無線通信装置間の認証は、通常、認証通信と認証処理という２段階の手順を踏む。認証通信は、通信相手の認証を行うために、無線通信装置の装置ＩＤ（identifier）やパスワード等の識別情報を含む認証情報を送受信する通信である。認証処理は、認証通信によって相手から受信した認証情報を検証することにより、相手の正当性（真正な相手であるか否か）を確認する処理である。

[0004] 無線通信装置は、相手が真正であることが確認できた場合にのみ、相手とのデータ通信を開始する。これにより、真正ではない相手とのデータ通信を防ぐことができ、第三者への情報の漏えいを防ぐことができる。

[0005] 相手の正当性を確認するためには、２つの事項について確認する必要がある。

[0006] １つ目は、受信した認証情報の内容が、真正の無線通信装置が作成したものであるか否かである。この事項の確認には、一般的には、電子署名や電子認証の技術が広く用いられている。

[0007] ２つ目は、受信した認証情報が、現に認証通信を行っている相手が作成し

たものであるか否かである。すなわち、受信した認証情報が、「第三者による、真正の無線通信装置が送信した認証情報に対する不正傍受と、その認証情報の再送信」が行われた結果であるか否かである。このような、不正傍受した認証情報の再送信による成りすまし行為は、一般的に、「リプレイアタック (replay attack)」と呼ばれている。

[0008] 2つ目の事項の確認には、一般的には、チャレンジ／レスポンス認証が広く用いられている。チャレンジ／レスポンス認証は、その時々によって値が異なるランダム値を用いることにより、リプレイアタックにより送られてきた情報を排除する技術である。

[0009] この技術では、まず、一方の無線通信装置が、例えばランダムに値を選択し、選択した値を、真正の相手先である無線通信装置に送信する。ランダム値を受信した無線通信装置は、事前に共有した秘密情報を用いて、受信したランダム値に署名を付与して、認証情報に含めて返信する。

[0010] 認証情報を受信した無線通信装置は、署名の正当性を確認するとともに、認証情報に含まれるランダム値と送信したランダム値とが一致するか否かを確認する。そして、無線通信装置は、これらの値が一致した場合にのみ、受信した認証情報の送信元が真正の相手であると判断する。これにより、無線通信装置は、リプレイアタックを排除することができる。

[0011] チャレンジ／レスポンス認証は、ランダム値を送信するための送信時間を必要とする。一方で、例えば、ある1つの無線基地局の無線通信エリアを通過する不特定多数の無線通信装置のそれぞれが、無線通信装置に対して認証を行うような場合、できるだけ短時間で個々の認証処理が行われることが望ましい。

[0012] そこで、時分割多元接続方式 (time division multiple access system、以下「TDMA方式」という) の無線通信システムにおいて個々の認証処理を短縮する技術が、例えば特許文献1に記載されている。以下、説明の便宜上、認証を行う側の無線通信装置を、「無線端末装置」といい、認証される側の無線通信装置を、「無線基地局装置」という。また、無線端末装置が、

通信相手が真正の無線基地局装置であることを確認するための認証を、「基地局認証」という。

[0013] 図1は、TDMA方式を説明するための模式図である。

[0014] 図1に示すように、TDMA方式では、同一周波数の電波上の通信路が、固定長のフレームという概念によって時間分割される。また、各フレームは、固定長のタイムスロットという概念によって更に分割される。

[0015] 複数の無線端末装置30-1～30-3には、認証通信を開始する毎に、タイムスロットがランダムにそれぞれ割り当てられる。各無線端末装置30は、割り当てられたタイムスロットを使用して、無線基地局装置20との間で通信を行う。これにより、TDMA方式は、複数の無線端末装置30-1～30-3の間での通信の電波的な干渉が発生することを防ぎ、1対多数の個別通信を可能にしている。

[0016] 各フレームおよび各タイムスロットは、それぞれに付与された番号によって識別される。また、フレーム番号およびタイムスロット番号は、時間とともに変化する。フレームの番号とタイムスロットの番号とを組み合わせた値は、その時々によって異なる値である。また、タイムスロット番号の選択は、ランダムに行われる。したがって、フレームの番号とタイムスロットの番号とを組み合わせた値は、ランダム性を有する。

[0017] そこで、特許文献1に記載された技術は、この組み合わせ値を、チャレンジ/レスポンス認証におけるランダム値として利用する。

[0018] 図2は、タイムスロットの番号をランダム値として利用した無線通信システムの全体動作を示すシーケンス図である。

[0019] 図2に示すように、例えば、まず、第1の無線端末装置30-1が、フレーム番号Mのフレームのタイムスロット番号Nのタイムスロットを用いて、無線基地局装置20に対して認証要求を送信する(S41)。すると、無線基地局装置20は、値M、Nから、事前に第1の無線端末装置30-1との間で共有する共有関数を用いて、認証データを生成し(S42)、生成した認証データを、第1の無線端末装置30-1へ送信する(S43)。第1の

無線端末装置 30-1 は、同様に、値 M、N から共有関数を用いて認証データを生成し、生成した認証データと無線基地局装置から受信した認証データとが一致するか否かを確認する（S 44）。2つのデータが一致する場合には、第1の無線端末装置 30-1 は、無線基地局装置 20 とのデータ通信を開始する（S 45）。続いて、次のタイムスロット番号 N+1 のタイムスロットにおいて、例えば、第2の無線端末装置 30-2 が、同様に認証要求を送信する。

[0020] このように、特許文献 1 記載の技術は、ランダム値を別途送信する必要がなく、基地局認証をより短時間で行うことができる。

先行技術文献

特許文献

[0021] 特許文献1：特開 2007-282086 号公報

発明の概要

発明が解決しようとする課題

[0022] ところで、一定時間内でより多くの無線端末装置が基地局認証を行うためには、タイムスロットの時間長（以降タイムスロット長）を短くする必要がある。しかし、特許文献 1 に記載された技術では、タイムスロット長を効果的に短くすることができず、一定の時間内において基地局認証を行うことができる無線端末装置の数が限られるという問題がある。その理由は以下の通りである。

[0023] 図 2 から明らかなように、認証通信には、少なくとも、無線基地局装置が認証要求を受信するための受信時間 51、認証データを演算するための演算時間 52、および認証データを送信するための送信時間 53 が掛かる。したがって、特許文献 1 に記載された技術では、それぞれのタイムスロット長を、これらの時間 51、52、53 を加算した時間よりも短くすることはできない。

[0024] 本発明の目的は、一定時間内でより多くの無線端末装置が基地局認証を行

うことができる無線基地局装置、無線端末装置、および基地局認証方法を提供することである。

課題を解決するための手段

- [0025] 本発明の無線基地局装置は、複数の無線端末装置と時分割多元接続により無線通信を行う無線基地局装置であって、前記無線端末装置から、基地局認証を開始することを示す応答情報を受信する応答情報受信部と、タイムスロット毎の前記応答情報の受信の有無を示す情報を集約した基地局認証データを生成する基地局認証データ生成部と、生成された前記基地局認証データを、前記無線端末装置に送信する基地局認証データ送信部とを有する。
- [0026] 本発明の無線端末装置は、無線基地局装置と時分割多元接続により無線通信を行う複数の無線端末装置のうちの1つであって、タイムスロットを選択するタイムスロット選択部と、選択された前記タイムスロットを用いて、基地局認証を開始することを示す応答情報を、前記無線基地局装置に送信する応答情報送信部と、送信された前記応答情報に対応して、基地局認証データを受信する基地局認証データ受信部と、受信した前記基地局認証データが、選択された前記タイムスロットにおいて前記応答情報の受信があったことを示すか否かに基づいて、前記基地局認証データの送信元に対する基地局認証を行う基地局認証部とを有する。
- [0027] 本発明の基地局認証方法は、無線基地局装置と、この無線基地局と時分割多元接続により無線通信を行う複数の無線端末装置との間で行われる基地局認証方法であって、前記無線端末装置が、タイムスロットを選択し、選択したタイムスロットを用いて、基地局認証を開始することを示す応答情報を前記無線基地局装置に送信するステップと、前記無線基地局装置が、タイムスロット毎の前記応答情報の受信の有無を示す情報を複数のタイムスロットについて集約した基地局認証データを生成し、生成した前記基地局認証データを前記無線端末装置に送信するステップと、前記無線端末装置が、受信した前記基地局認証データが、選択した前記タイムスロットにおいて前記応答情報の受信があったことを示すか否かに基づいて、前記基地局認証データの送

信元に対する基地局認証を行うステップとを有する。

発明の効果

[0028] 本発明によれば、各無線端末装置への処理をまとめることにより、一定時間内でより多くの無線端末装置が基地局認証を行うことができる。

図面の簡単な説明

[0029] [図1] T D M A方式を説明するための模式図

[図2]従来技術を採用した無線通信システムの全体動作を示すシーケンス図

[図3]本発明の実施の形態1に係る無線通信システムの構成の一例を示すシステム構成図

[図4]実施の形態1に係る無線通信システムが適用される環境の一例を示す模式図

[図5]実施の形態1に係る無線通信システムの全体動作の一例を示すシーケンス図

[図6]実施の形態1における認証開始要求および応答のデータ構成の一例を示す図

[図7]実施の形態1における基地局認証データを含む認証情報のデータ構成の一例を示す図

[図8]実施の形態1における基地局認証データのデータ生成ルールの一例を示す模式図

[図9]実施の形態1における比較データのデータ生成ルールの一例を示す模式図

[図10]実施の形態1における基地局認証データと比較データとの関係の一例を示す模式図

[図11]実施の形態1に係るタイムスロット番号の重複選択の様子の一列を示す模式図

[図12]実施の形態1に係る無線基地局装置の構成の一例を示すブロック図

[図13]実施の形態1に係る無線端末装置の構成の一例を示すブロック図

[図14]実施の形態1に係る無線基地局装置の通信制御部の動作の一例を示す

フローチャート

[図15]実施の形態1に係る無線基地局装置の送信部の動作の一例を示すフローチャート

[図16]実施の形態1に係る無線基地局装置のタイムスロット管理部の動作の一例を示すフローチャート

[図17]実施の形態1に係る無線基地局装置の受信部の動作の一例を示すフローチャート

[図18]実施の形態1に係る無線基地局装置の受信状況管理部の動作の一例を示すフローチャート

[図19]実施の形態1に係る無線基地局装置の基地局認証データ生成部の動作の一例を示すフローチャート

[図20]実施の形態1に係る無線端末装置の通信制御部の動作の一例を示すフローチャート

[図21]実施の形態1に係る無線端末装置の受信部の動作の一例を示すフローチャート

[図22]実施の形態1に係る無線端末装置のタイムスロット選択部の動作の一例を示すフローチャート

[図23]実施の形態1に係る無線端末装置の選択状況管理部の動作の一例を示すフローチャート

[図24]実施の形態1に係る無線端末装置のタイムスロット管理部の動作の一例を示すフローチャート

[図25]実施の形態1に係る無線端末装置の送信部の動作の一例を示すフローチャート

[図26]実施の形態1に係る無線端末装置の比較データ生成部の動作の一例を示すフローチャート

[図27]実施の形態1に係る無線端末装置の基地局認証部の動作の一例を示すフローチャート

[図28]本発明の実施の形態2に係る無線基地局装置の構成の一例を示すブ

ツク図

[図29]実施の形態2における乱数値が埋め込まれた応答のデータ構成の一例を示す図

[図30]実施の形態2に係る無線基地局装置の構成の一例を示すブロック図

[図31]実施の形態2に係る無線通信システムの全体動作の一例を示すシーケンス図

[図32]実施の形態2における基地局認証データのデータ生成ルールの一例を示す模式図

[図33]実施の形態2における無線端末装置による比較データのデータ生成ルールの一例を示す模式図

[図34]実施の形態2に係る無線基地局装置の受信部の動作の一例を示すフローチャート

[図35]実施の形態2に係る無線基地局装置の受信状況管理部の動作の一例を示すフローチャート

[図36]実施の形態2に係る無線端末装置のタイムスロット選択部の動作の一例を示すフローチャート

[図37]実施の形態2に係る無線端末装置の選択状況管理部の動作の一例を示すフローチャート

[図38]実施の形態2に係る無線端末装置のタイムスロット管理部の動作の一例を示すフローチャート

[図39]実施の形態2に係る無線端末装置の送信部の動作の一例を示すフローチャート

発明を実施するための形態

[0030] 以下、本発明の各実施の形態について、図面を参照して詳細に説明する。
なお、本発明は、以下に説明する実施の形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施し得る。

[0031] (実施の形態1)

図3は、本発明の実施の形態1に係る無線通信システムの構成の一例を示

すシステム構成図である。

[0032] 図3において、本実施の形態に係る無線通信システム100は、無線基地局装置200と、無線基地局装置200の通信エリアに位置する第1～第3の無線端末装置300-1～300-3とを有する。第1～第3の無線端末装置300-1～300-3は同一の構成を有する。以下、適宜、第1～第3の無線端末装置300-1～300-3を、無線端末装置300と総称して説明する。

[0033] 無線基地局装置200は、第1～第3の無線端末装置300-1～300-3と、TDMA方式による無線通信を行う。

[0034] 図4は、無線通信システム100が適用される環境の一例を示す模式図である。

[0035] 図4に示すように、無線基地局装置200の通信エリア400を通過する不特定多数の歩行者410は、それぞれ無線端末装置300を携帯している。無線端末装置300は、例えば、RFID（radio frequency identification）の一種であるアクティブタグである。無線基地局装置200は、例えば、アクティブタグのリーダ／ライタである。

[0036] また、通信エリア400内に同時に位置する無線端末装置300の数は変動する。例えば、図3に示すように、無線基地局装置200は、第4の無線端末装置300-4が通信エリアに移動してきたときには、第4の無線端末装置300-4ともTDMA方式による無線通信を行う。

[0037] 具体的には、無線通信システム100は、例えば、児童見守りサービスに適用される。児童見守りサービスの一例は、児童が校門を通過する際に、児童の登下校時間や登下校の有無を検知し、異常がある場合にはその旨を教師や保護者に通報するサービスである。この場合、無線基地局装置200は、学校の校門に設置され、無線端末装置300は、児童に携帯される。学校における登下校の際は、多数の児童が短時間の間に通過することが予想される。

[0038] また、無線通信システム100は、例えば、車両接近通知サービスに適用

される。車両接近通知サービスの一例は、車両にとって死角となり易い曲がり角の付近を歩行者が通行しているときに、その旨を検知して周囲の車両に通知するサービスである。この場合、無線基地局装置 200 は、曲がり角に設置され、無線端末装置 300 は、歩行者に携帯される。

[0039] 無線端末装置 300 は、その無線端末装置 300 に割り当てられたタイムスロットを用いて、無線基地局装置 200 とそれぞれ個別のデータ通信を行う。無線端末装置を携帯するユーザは、この個別のデータ通信により、通過記録や情報提供等のサービスを受ける。

[0040] ところが、どの無線端末装置 300 がいつ通信エリア 400 を通過するかは、事前に特定することができない。したがって、事前に各無線端末装置 300 にタイムスロットを割り当てておくことは難しい。

[0041] そこで、本実施の形態では、無線端末装置 300 が、通信に使用するタイムスロットをランダムに選択し、選択したタイムスロットを使用して、どのタイムスロットを選択したかを無線基地局装置 200 に対して通知する。

[0042] タイムスロットの識別は、タイムスロット番号を用いて行われる。また、タイムスロットの同期は、例えば、無線基地局装置 200 が、後述の認証開始要求の送信によってフレーム開始位置を各無線端末装置 300 に対して通知することにより、行われる。

[0043] また、各無線端末装置 300 は、データ通信を開始しようとする相手の正当性（ここでは、無線基地局装置 200 であるか否か）を判断するために、データ通信に先立ち、通信の相手先に対して基地局認証を行う。

[0044] また、各無線端末装置 300 は、この認証において、受信した認証情報がリプレイアタックによるものでないことを確認する。第三者が、無線基地局装置 200 に成りすまして、不正目的で無線端末装置 300 とのデータ通信開始を試みる可能性があるからである。

[0045] 更に、本実施の形態に係る無線通信システム 100 は、従来とは異なる内容で基地局認証を行うことにより、一定時間内でより多くの無線端末装置 300 が基地局認証を行うことを可能にする。以下、無線通信システム 100

の構成および動作のうち、基地局認証に関する部分に着目して、説明を行う。

[0046] ここで、基地局認証において無線基地局装置 200 と無線端末装置 300 との間で共有して使用される情報（以下「共有情報」という）は、各装置の出荷時点に、予め各装置に設定されているものとする。共有情報は、後述の、無線データの形式およびコマンドコード、基地局認証データを生成するためのデータ生成ルール、および後述の比較データを生成するためのデータ生成ルール、スロットの数およびスロット間隔等を含む。

[0047] なお、これらの共有情報は、基地局認証を行う毎に、無線基地局装置 200 から無線端末装置 300 へと送信されるようにしても良い。例えば、無線基地局装置 200 は、共有情報を、認証開始要求または基地局認証データに付加する。そして、無線端末装置 300 は、共有情報を、送信する認証開始要求または基地局認証データから取得する。

[0048] まず、無線通信システム 100 の全体動作の概要について、図 5 ～図 11 を参照して説明する。

[0049] 図 5 は、無線通信システム 100 の全体動作の一例を示すシーケンス図である

[0050] まず、無線基地局装置 200 は、通信エリア 400 に位置する無線端末装置 300 に対し、認証通信の開始の指示である認証開始要求を、所定の間隔で定期的に同報送信する（S2100）。ここで、後述の基地局認証は、認証開始要求を無線端末装置 300 が受信する毎に実行されることを前提とする。

[0051] 上述の所定の間隔は、無線端末装置 300 の通信エリア通過時間に収まる長さが望ましい。この通信エリア通過時間は、通信エリア 400 の大きさと無線端末装置 300 を携帯するユーザの平均移動速度とから計算することができる。また、上述の所定の間隔は、基地局認証用のタイムスロットやデータ通信用のタイムスロットを包含するような長さであることが望ましい。

[0052] 通信エリア 400 内に位置する無線端末装置 300 に対する同報送信を、

以下、単に「同報送信」という。ここでは、第1～第3の無線端末装置300-1～300-3が、図4に示すような通信エリア400内に存在するものとする。

[0053] 認証開始要求を受信した第1～第3の無線端末装置300-1～300-3は、それぞれ、受信した認証開始要求に対応して、例えば、ランダムに、タイムスロットを少なくとも1つ選択する(S2200)。

[0054] そして、第1～第3の無線端末装置300-1～300-3は、選択したタイムスロットを用いて、基地局認証を開始することを示す応答を無線基地局装置200にそれぞれ送信する(S2300)。

[0055] ここで、無線基地局装置200が送信する認証開始要求、および、この認証開始要求に対して無線端末装置300が返信する応答の構成について、説明する。

[0056] 図6は、認証開始要求および応答のデータ構成の一例を示す図である。

[0057] 図6に示すように、無線データ510は、同期コード511、Length512、コマンドコード513、およびチェックサム514をこの順に並べて構成される。同期コード511は、無線データの開始を示す所定のコードを記述する。Length512は、後続のデータの長さ(ここでは、コマンドコード513およびチェックサム514の合計長さ)を例えばバイト(byte)長で記述する。コマンドコード513は、当該無線データの種類を示すコマンドコードを記述する。チェックサム514は、当該無線データの誤り検出符号を記述する。

[0058] 無線基地局装置200は、コマンドコード513に、当該無線データ510が認証開始要求であることを示す所定のコマンドコードを記述して、認証開始要求の無線データを生成する。無線端末装置300は、同期コード511に基づいて、無線データの開始を検出し、Length512に基づいて、コマンドコード513およびチェックサム514を抽出する。そして、無線端末装置300は、コマンドコード513に上述の所定のコマンドコードが記述されているとき、当該無線データ510が認証開始要求であると判定

する。更に、無線端末装置 300 は、チェックサム 514 に基づいて、当該無線データ 510 に誤りが存在するか否かを判定する。

[0059] また、無線端末装置 300 は、コマンドコード 513 に、所定のコマンドコード (ACKnowledgement : ACK) を記述して、応答の無線データを生成する。この所定のコマンドコードは、当該無線データ 510 が認証開始要求に対する応答であることを示す情報である。無線基地局装置 200 は、同期コード 511 に基づいて、無線データの開始を検出し、Length 512 に基づいて、コマンドコード 513 およびチェックサム 514 を抽出する。そして、無線基地局装置 200 は、コマンドコード 513 に上述の所定のコマンドコードが記述されているとき、当該無線データ 510 が応答であると判定する。更に、無線基地局装置 200 は、チェックサム 514 に基づいて、当該無線データ 510 に誤りが存在するか否かを判定する。

[0060] 無線基地局装置 200 は、第 1 ～ 第 3 の無線端末装置 300-1 ～ 300-3 から応答を受信する。そして、無線基地局装置 200 は、タイムスロット毎の受信の有無を表す受信状況に基づいて、基地局認証データを生成する (図 5 の S2400)。基地局認証データは、タイムスロット毎の、認証開始要求に対する応答の有無を、複数のタイムスロットについて集約したデータである。基地局認証データの詳細については後述する。

[0061] そして、無線基地局装置 200 は、認証情報を、第 1 ～ 第 3 の無線端末装置 300-1 ～ 300-3 に対して同報送信する (S2500)。認証情報は、無線基地局装置 200 が生成した基地局認証データと、装置 ID やパスワード等の識別情報とを含む。

[0062] 認証情報は、認証開始要求や応答と同様の形式の無線データに格納されて、送受信される。

[0063] 図 7 は、基地局認証データを含む認証情報のデータ構成の一例を示す図であり、図 6 に対応するものである。図 6 と同一部分には同一符号を付す。

[0064] 図 7 に示すように、認証情報の無線データ 520 は、同期コード 511、Length 512、コマンドコード 513、基地局認証データ 521、識

別情報 522、およびチェックサム 514 を、この順に並べて構成される。
Length 512 は、ここでは、コマンドコード 513、基地局認証データ 521、識別情報 522、およびチェックサム 514 の合計長さを記述する。

- [0065] 無線基地局装置 200 は、コマンドコード 513 に、当該無線データ 520 が認証情報であることを示す所定のコマンドコードを記述して、認証情報の無線データ 520 を生成する。無線端末装置 300 は、コマンドコード 513 に上述の所定のコマンドコードが記述されているとき、基地局認証データ 521 および識別情報 522 を抽出する。なお、チェックサム 514 は、電子署名としても良い。
- [0066] 無線基地局装置 200 は、このような無線データ 520 を生成して送信することにより、基地局認証データを含む認証情報の送信を行う。
- [0067] 一方、第 1～第 3 の無線端末装置 300-1～300-3 は、どのタイムスロットを選択したかに基づいて、比較データをそれぞれ生成する（図 5 の S2600）。比較データは、タイムスロットのそれぞれに対して選択の有無を示す識別子を対応付けたデータである。比較データの詳細については後述する。
- [0068] そして、第 1～第 3 の無線端末装置 300-1～300-3 は、無線基地局装置 200 から受信した認証情報に含まれる基地局認証データと、生成した比較データとに基づいて、基地局認証を行う（S2700）。具体的には、第 1～第 3 の無線端末装置 300-1～300-3 は、基地局認証データと比較データとを比較し、これらのデータが整合しているか否かを判断する。基地局認証データと比較データとが整合している状態とは、比較データによって示される選択されたタイムスロットの全てが、基地局認証データによって応答があったことが示されるタイムスロットに、包含されている状態である。基地局認証データと比較データとの整合の判断の詳細については後述する。
- [0069] 第 1～第 3 の無線端末装置 300-1～300-3 は、基地局認証データ

と比較データとが整合する場合には、認証情報の送信元が真正の相手（ここでは無線基地局装置 200）であると判定し、通信を継続して、データ通信を行う。具体的には、無線端末装置 300 は、基地局認証に成功した旨の通知を無線基地局装置 200 に対して送信する。更に、無線端末装置 300 は、基地局認証用のタイムスロットの後に配置した、データ通信用のタイムスロットを用いて、無線基地局装置 200 との間でデータ通信を行う。

[0070] また、第 1～第 3 の無線端末装置 300-1～300-3 は、基地局認証データと比較データとが整合しない場合は、認証情報の送信元が真正の相手ではない（例えばリプレイアタックを行った無線端末装置）と判定し、データ通信を行わない。

[0071] なお、無線基地局装置 200 は、送信する認証情報の改ざんを防ぐ目的で、上述の通り、認証情報に署名を付与することが望ましい。この場合、無線端末装置 300 は、認証情報に真正の署名が付与されているか否かの検証を、基地局認証において行う。

[0072] 図 8 は、無線基地局装置 200 による基地局認証データを生成するためのデータ生成ルールの一例を示す模式図である。

[0073] ここで、基地局認証に使用されるフレームの最後のタイムスロットの番号（以下、「既定のタイムスロット番号」という）は「n」であるものとする。また、第 1～第 3 の無線端末装置 300-1～300-3 は、それぞれ順に、タイムスロット番号「0」、「2」、「n」のタイムスロットを選択したものとする。また、無線基地局装置 200 は、無線端末装置 300 からの応答が有ったタイムスロットであることを示す識別子は「1」とし、応答が無かったタイムスロットであることを示す識別子は「0」とする。

[0074] この場合、無線基地局装置 200 は、受信有りのタイムスロット番号「0」、「2」、「n」に対応する識別子の値を「1」とし、その他の全てのタイムスロット番号に対応する識別子の値を「0」とする情報を、受信状況として保持する。すなわち、受信状況は、タイムスロット毎の応答の有無を表す情報である。

- [0075] ここでは、基地局認証データのデータ生成ルールは、応答の有無を示す上記識別子を、タイムスロット番号の昇順で並べる内容であるものとする。この場合、図8に示す例のように、無線基地局装置200が生成する基地局認証データは、「1、0、1、0、・・・、1」となる。
- [0076] 一方、図5において、第1～第3の無線端末装置300-1～300-3は、それぞれ、タイムスロット毎の選択の有無を表す選択状況に基づいて、比較データを生成する（S2400）。
- [0077] 図9は、無線端末装置300による比較データを生成するためのデータ生成ルールの一例を示す模式図である。ここでは、第1の無線端末装置300-1による比較データの生成の概要を例示する。
- [0078] 上述のように、第1の無線端末装置300-1は、タイムスロット番号「0」を選択している。ここで、第1の無線端末装置300-1は、選択した（応答を行った）タイムスロットであることを示す識別子を「1」とし、選択しなかった（応答を行わなかった）タイムスロットであることを示す識別子を「0」とする。この場合、図9に示すように、第1の無線端末装置300-1におけるタイムスロットの選択状況は、タイムスロット番号「0」に対応する識別子の値が「1」であり、その他のタイムスロット番号に対応する識別子の値が「0」である。
- [0079] 本実施の形態では、比較データのデータ生成ルールは、選択の有無を示す上記識別子を、タイムスロット番号の昇順で並べる内容であり、基地局認証データのデータ生成ルールと同一であるものとする。この場合、図9に示す例のように、無線基地局装置200が生成する比較データは、「1、0、0、0、・・・、0」となる。
- [0080] 図10は、図8および図9に示す例における、各無線端末装置300における基地局認証データと比較データとの関係を示す模式図である。
- [0081] 無線端末装置300により生成される基地局認証データは、「1、0、1、0、・・・、1」となる。これに対し、第1～第3の無線端末装置300-1～300-3により生成される比較データは、順に、「1、0、0、0

、・・・、0」、「0、0、1、0、・・・、0」、「0、0、0、0、・・・、1」となる。

[0082] すなわち、基地局認証データを構成するビットパターンのうち、各比較データの値「1」となるビット位置は、値「1」となっている。これは、無線基地局装置200と各無線端末装置300との間で、応答の送受信の有無および応答の送受信が行われたタイムスロットが一致しているからである。また、基地局認証データのデータ生成ルールと比較データのデータ生成ルールとが、タイムスロット番号の昇順に識別子を並べるという同一の内容となっているためである。

[0083] 基地局認証データを構成するビットパターンのうち、各比較データの値「1」となるビット位置が値「1」となることは、1つの無線端末装置300が、複数のタイムスロット番号を使用する場合においても同様である。つまり、無線端末装置300が複数のタイムスロットを選択して応答を送信する場合も同様である。

[0084] 基地局認証データのうち、比較データの値が「1」となっているビット位置が、値「1」となっていることは、基地局認証データと比較データとが整合していることを示す。このような基地局認証データと比較データとの整合性は、例えば、基地局認証データと比較データとの論理積の結果が比較データと一致するか否かを判定することによって行うことができる。

[0085] どのタイムスロット番号を使用して応答を行うかは、上述の通り、ランダムに選択される。これにより、基地局認証データおよび比較データは、高いランダム性を有する。

[0086] また、タイムスロット番号の選択は、各無線端末装置300において独立して行われるため、複数の無線端末装置300が同一のタイムスロット番号を選択してしまうことがある。図11は、複数の無線端末装置300が同一のタイムスロット番号を選択する様子の一例を示す模式図である。

[0087] しかし、このようなタイムスロット番号の重複選択の可能性は、更に基地局認証の信頼性を向上させる。選択されるタイムスロット番号の重複は、ラ

ンダムに発生し、基地局認証データのうち値が「1」となるビットの数は、応答を送信した無線端末装置300の数の範囲内で変動するからである。

[0088] なお、各無線端末装置300は、応答の送信の前に、選択したタイムスロットにおいてキャリアセンスを行う。各無線端末装置300は、選択したタイムスロットにおいて他の無線端末装置300が先に応答を行っていることを検知した場合には、実際には応答を送信せずに、応答を送信したものとして処理を行うことが望ましい。これにより、タイムスロット番号の重複選択があった場合でも、コリジョンを防止しつつ、単独で選択した場合と同様に基地局認証を行うことができる。なお、基地局認証の後に実際のデータ通信を行うに際しては、重複が無いように、使用タイムスロットの調整が改めて行われる。

[0089] なお、本発明の仕組み上、基地局認証データに値「1」のビットが多いときには、基地局認証の信頼性が低下することが考えられる。例えば、全てのビットが値「1」となっている基地局認証データが生成されたときは、この基地局認証データを用いてリプレイアタックが行われると、全ての無線端末装置300において基地局認証が成功してしまう。

[0090] このような事態を防ぐため、無線基地局装置200は、基地局認証データ生成の際に値「1」となるビットの総数を監視することが望ましい。この場合、無線基地局装置200は、値「1」となるビットの総数、つまり応答を受信したタイムスロットの数が所定の閾値を超えたときは、基地局認証データの送信をせずに処理を中止し、所定の間隔後に再度認証開始要求を送信する。このとき、無線基地局装置200は、スロット数を更新して、認証開始要求を送信しても良い。

[0091] ここでは、本実施の形態に係る無線通信システム100の優位性を示すために、図5に示す本実施の形態のシーケンス図と、図2に示す従来の無線通信システムのシーケンス図とを比較する。

[0092] 従来の無線通信システムでは、タイムスロット毎に基地局認証データの生成と送信とを完了させなければならない。また、例えば、無線基地局装置の

通信エリア内に３つの無線端末装置が位置する場合、少なくとも基地局認証データの生成と送信が３回ずつ行われることになる。

[0093] これに対し、本実施の形態では、図４に示す通信エリア４００内に３つの無線端末装置３００－１～３００－３が位置しているが、基地局認証データの生成と送信は少なくとも１回ずつで済む。

[0094] すなわち、本実施の形態に係る無線通信システム１００は、個々のタイムスロットの長さを、基地局認証データの生成と送信とに要する時間の分だけ短縮することができる。一方で、本実施の形態に係る無線通信システム１００は、認証開始要求に対する応答に用いるタイムスロットとは別に、認証開始要求の送信と、基地局認証データの生成と、基地局認証データの送信とに要する時間を必要とする。しかし、いずれも１回ずつであるため、その増加される時間は、削減される時間の総計よりも少なく抑えることができる。また、基地局認証データに対して署名付与を行う場合には、１回の署名付与で済む。

[0095] したがって、本実施の形態に係る無線通信システム１００は、一定時間に対して配置することが可能なタイムスロットの個数を増やすことができ、一定時間内でより多くの無線端末装置３００が基地局認証を行うことができる。

[0096] 次に、各装置の構成および動作について説明する。

[0097] 図１２は、無線基地局装置２００の構成の一例を示すブロック図である。

[0098] 図１２において、無線基地局装置２００は、通信制御部２１０、送信部２２０、タイムスロット管理部２３０、受信部２４０、受信状況管理部２５０、および基地局認証データ生成部２６０を有する。

[0099] 通信制御部２１０は、無線基地局装置２００全体の動作を制御する。通信制御部２１０には、送信部２２０、タイムスロット管理部２３０、受信部２４０、および基地局認証データ生成部２６０が接続されている。

[0100] 送信部２２０は、認証開始要求を生成し、生成した認証開始要求の同報送信を行う。また、送信部２２０は、基地局認証データ生成部２６０が生成し

た基地局認証データを含む認証情報の同報送信を行う。

[0101] タイムスロット管理部 230 は、既定のスロット番号および既定のタイムスロット間隔（タイムスロット長）を予め保持する。タイムスロット管理部 230 は、送信部 220 および受信部 240 に接続している。そして、タイムスロット管理部 230 は、少なくとも送信部 220 が認証開始要求を同報送信した後、通信エリア 400 内に位置する無線端末装置 300 との間で共有されるタイムスロットを管理する。

[0102] 受信部 240 は、無線端末装置 300 から送信される、認証開始要求に対する応答をタイムスロット毎に受信し、受信したタイムスロット毎の応答の有無を、受信状況管理部 250 に通知する。なお、各無線端末装置 300 におけるこの応答の送信は、その無線端末装置 300 が選択したタイムスロットを用いて行われる。

[0103] 受信状況管理部 250 は、受信部 240 に接続されている。そして、受信状況管理部 250 は、受信部 240 におけるタイムスロット毎の応答の有無を表す受信状況を管理する。

[0104] 基地局認証データ生成部 260 は、基地局認証データのデータ生成ルールを予め保持する。基地局認証データ生成部 260 は、受信状況管理部 250 に接続されている。そして、基地局認証データ生成部 260 は、受信状況管理部 250 で管理される受信状況に基づき、保持するデータ生成ルールに従って、基地局認証データを生成する。

[0105] また、無線基地局装置 200 は、例えば、CPU（central processing unit）、制御プログラムを格納したROM（read only memory）等の記憶媒体、およびRAM（random access memory）等の作業用メモリを有する。この場合、上記各部の機能は、CPUが制御プログラムを実行することにより実現される。

[0106] 図 13 は、無線端末装置 300 の構成の一例を示すブロック図である。

[0107] 図 13 において、無線端末装置 300 は、通信制御部 310、受信部 320、タイムスロット選択部 330、選択状況管理部 340、タイムスロット

管理部 350、送信部 360、比較データ生成部 370、および基地局認証部 380を有する。

[0108] 通信制御部 310は、無線端末装置 300全体の動作を制御する。通信制御部 310には、受信部 320、タイムスロット選択部 330、タイムスロット管理部 350、送信部 360、比較データ生成部 370、および基地局認証部 380が接続されている。

[0109] 受信部 320は、無線基地局装置 200から送信される、認証開始要求と、基地局認証データを含む認証情報とを、それぞれ受信する。

[0110] タイムスロット選択部 330は、タイムスロット管理部 350が管理するタイムスロットの中から、認証開始要求に対する応答に用いるタイムスロットを、ランダムに選択する。

[0111] 選択状況管理部 340は、タイムスロット選択部 330に接続されている。そして、選択状況管理部 340は、タイムスロット選択部 330におけるタイムスロット毎の選択の有無を表す選択状況を管理する。

[0112] タイムスロット管理部 350は、既定のスロット番号および既定のタイムスロット間隔（タイムスロット長）を予め保持する。タイムスロット管理部 350は、受信部 320および送信部 360に接続している。そして、タイムスロット管理部 350は、少なくともタイムスロット選択部 330がタイムスロットを選択した後、無線基地局装置 200との間で共有されるタイムスロットを管理する。

[0113] 送信部 360は、無線基地局装置 200に対し、タイムスロット選択部 330が選択したタイムスロットを用いて、認証開始要求に対する応答を送信する。

[0114] 比較データ生成部 370は、比較データのデータ生成ルールを予め保持する。比較データ生成部 370は、選択状況管理部 340に接続されている。そして、比較データ生成部 370は、選択状況管理部 340で管理される選択状況に基づき、予め保持したデータ生成ルールに従って、比較データを生成する。

- [0115] 基地局認証部 380 は、受信した基地局認証データと比較データ生成部 370 が生成した比較データとが整合するか否かに基づいて、基地局認証を行う。
- [0116] また、無線基地局装置 200 は、例えば、CPU、制御プログラムを格納した ROM 等の記憶媒体、および等の作業用メモリを有する。この場合、上記各部の機能は、CPU が制御プログラムを実行することにより実現される。
- [0117] 以下、無線基地局装置 200 の各部および無線端末装置 300 の各部の動作について、詳細に説明する。図 5 ～ 図 11 において説明した無線基地局装置 200 の動作および無線端末装置 300 の動作は、例えば、これらの装置を構成する各部が以下に動作をそれぞれ行うことにより、実現される。
- [0118] まず、無線基地局装置 200 の各部の動作について説明する。
- [0119] 図 14 は、無線基地局装置 200 の通信制御部 210 の動作の一例を示すフローチャートである。
- [0120] まず、通信制御部 210 は、送信部 220 に対して、認証開始要求の同報送信を指示し（S3101）、その後、送信部 220 から処理を戻される。なお、通信制御部 210 は、時間を管理し、例えば、任意の時間間隔で、認証開始要求の同報送信を送信部 220 に指示する。次に、通信制御部 210 は、タイムスロット管理部 230 に対して、タイムスロットの管理の開始を指示する（S3102）。そして、通信制御部 210 は、タイムスロット管理部 230 から処理を戻されると、基地局認証データ生成部 260 に対して、基地局認証データの生成を指示する（S3103）。
- [0121] そして、通信制御部 210 は、基地局認証データ生成部 260 から基地局認証データと共に処理を戻されると、送信部 220 に対して、基地局認証データを渡して、基地局認証データを含む認証情報の同報送信を指示する（S3104）。そして、通信制御部 210 は、オペレータ操作などにより基地局認証に関する処理の終了を指示されたか否かを判断し、終了を指示されていない間は、上述の処理を繰り返す（S3105）。

[0122] 図 15 は、無線基地局装置 200 の送信部 220 の動作の一例を示すフローチャートである。

[0123] 送信部 220 は、通信制御部 210 から認証開始要求の同報送信の指示を受け付け、指示を受け取る毎に（S3201：YES）、認証開始要求を同報送信し（S3202）、送信が完了すると、通信制御部 210 へ処理を戻す（S3203）。また、送信部 220 は、通信制御部 210 からの基地局認証データを含む認証情報の同報送信の指示を受け付ける。そして、送信部 220 は、指示を受け取る毎に（S3204：YES）、基地局認証データを含む認証情報を同報送信し（S3205）、送信が完了すると、通信制御部 210 へ処理を戻す（S3203）。

[0124] 図 16 は、無線基地局装置 200 のタイムスロット管理部 230 の動作の一例を示すフローチャートである。

[0125] タイムスロット管理部 230 は、通信制御部 210 からタイムスロットの管理開始の指示を受け付け、指示を受取る毎に（S3301：YES）、タイムスロットの管理を行う（S3302～S3305）。

[0126] より具体的には、タイムスロット管理部 230 は、まず、タイムスロット番号を初期値「0」に設定する（S3302）。次に、タイムスロット管理部 230 は、既定のタイムスロット間隔に基づいて、タイムスロット番号が既定のタイムスロット番号に到達するまでタイムスロット番号をインクリメントする（S3305）。その間、タイムスロット管理部 230 は、受信部 240 に対して、各タイムスロット番号と既定のタイムスロット間隔とを渡し、応答の受信を指示する（S3303～S3305）。

[0127] そして、タイムスロット管理部 230 は、インクリメントするタイムスロット番号が、既定のタイムスロット番号 n に到達した場合には（S3304：YES）、通信制御部 210 に処理を戻す（S3306）。

[0128] 図 17 は、無線基地局装置 200 の受信部 240 の動作の一例を示すフローチャートである。

[0129] 受信部 240 は、タイムスロット管理部 230 から、タイムスロット番号

およびタイムスロット間隔の指定と、受信指示とを受け付ける。次に、受信部 240 は、指示を受け取る毎に（S 3401 : YES）、指定されたタイムスロット間隔を単位として、無線端末装置 300 からの応答を待機する（S 3402 ~ S 3406）。

[0130] より具体的には、受信部 240 は、まず、時間計測を開始し（S 3402）、既定のスロット間隔に到達するまでに無線端末装置 300 から応答を受信したか否かを判断する（S 3403）。そして、受信部 240 は、応答を受信した場合には（S 3403 : YES、S 3405 : YES）、受信状況管理部 250 に対し、タイムスロット番号と、応答を受信したことを示す情報である受信通知とを渡す（S 3407）。また、受信部 240 は、応答を受信しなかった場合には（S 3403 : NO、S 3406 : YES）、受信状況管理部 250 に対し、タイムスロット番号と、応答を受信しなかったことを示す情報である未受信通知とを渡す（S 3408）。

[0131] そして、受信部 240 は、受信通知または未受信通知を受信状況管理部 250 に渡した後、受信状況管理部 250 から処理を戻されると、タイムスロット管理部 230 に処理を戻す。

[0132] 図 18 は、無線基地局装置 200 の受信状況管理部 250 の動作の一例を示すフローチャートである。

[0133] 受信状況管理部 250 は、受信部 240 からタイムスロット番号と受信通知または未受信通知とを受け付ける。次に、受信状況管理部 250 は、通知を受け取る毎に（S 3501 : YES）、受け取ったタイムスロット番号と通知内容に対応する識別子とを関連付けた受信状況を管理する（S 3502 ~ 3505）。

[0134] より具体的には、受信状況管理部 250 は、まず、タイムスロット番号を初期値「0」に設定する（S 3502）。次に、受信状況管理部 250 は、タイムスロット番号が既定のタイムスロット番号 n に到達するまでタイムスロット番号をインクリメントしながら、各タイムスロット番号に対応して受信通知を受け取ったか否かを判断する。受信状況管理部 250 は、受信通知

を受け取った場合には（Ｓ３５０３：ＹＥＳ）、そのタイムスロット番号と受信を示す識別子とを関連付けて管理する（Ｓ３５０４）。また、受信状況管理部２５０は、受信通知を受け取っていない（未受信通知を受け取った）場合には（Ｓ３５０３：ＮＯ）、そのタイムスロット番号と未受信を示す識別子とを関連付けて管理する（Ｓ３５０５）。

[0135] そして、受信状況管理部２５０は、インクリメントするタイムスロット番号が既定のタイムスロット番号 n に到達した場合には（Ｓ３５０６：ＹＥＳ）、受信部２４０に処理を戻す（Ｓ３５０８）。

[0136] 図１９は、無線基地局装置２００の基地局認証データ生成部２６０の動作の一例を示すフローチャートである。

[0137] 基地局認証データ生成部２６０は、通信制御部２１０から基地局認証データの生成の指示を受け付ける。そして、基地局認証データ生成部２６０は、基地局認証データの生成の指示を受け取る毎に（Ｓ３６０１：ＹＥＳ）、受信状況管理部２５０から受信状況を取得する（Ｓ３６０２）。

[0138] そして、基地局認証データ生成部２６０は、既定のデータ生成ルールに従って、基地局認証データを生成する（Ｓ３６０３）。そして、基地局認証データ生成部２６０は、通信制御部２１０に対して、生成した基地局認証データを渡し、処理を戻す（Ｓ３６０４）。ここでは、基地局認証データ生成部２６０は、図８で説明したデータ生成ルールにより、基地局認証データを生成するものとする。すなわち、基地局認証データ生成部２６０は、受信状況において各タイムスロット番号に対応付けられた情報を、タイムスロット番号の昇順に並べ替えることにより、基地局認証データを生成する。

[0139] 次に、無線端末装置３００の各部の動作について説明する。

[0140] 図２０は、無線端末装置３００の通信制御部３１０の動作の一例を示すフローチャートである。

[0141] まず、通信制御部３１０は、受信部３２０に対して、認証開始要求の受信を指示する（Ｓ４１０１）。通信制御部３１０は、受信部３２０から処理を戻されると、次に、タイムスロット選択部３３０に対し、認証開始要求に応

答するためのタイムスロット番号の選択を指示する（Ｓ４１０２）。通信制御部３１０は、タイムスロット選択部３３０からタイムスロット番号と共に処理を戻される。次に、通信制御部３１０は、タイムスロット管理部３５０に対して、タイムスロット選択部３３０から受け取ったタイムスロット番号を渡し、タイムスロットの管理の開始を指示する（Ｓ４１０３）。

[0142] 通信制御部３１０は、タイムスロット管理部３５０から処理を戻されると、比較データ生成部３７０に対して、比較データの生成を指示する（Ｓ４１０４）。通信制御部３１０は、比較データ生成部３７０から比較データと共に処理を戻されると、受信部３２０に対して、無線基地局装置２００からの、基地局認証データを含む認証情報の受信を指示する（Ｓ４１０５）。

[0143] そして、通信制御部３１０は、受信部３２０から基地局認証データと共に処理を戻される。次に、通信制御部３１０は、基地局認証部３８０に対して、受信部３２０から受け取った基地局認証データと、比較データ生成部３７０から受け取った比較データとを渡し、基地局認証を指示する（Ｓ４１０６）。通信制御部３１０は、基地局認証部３８０から認証結果と共に処理を戻される。次に、通信制御部３１０は、受け取った認証結果が「ＯＫ」である場合には（Ｓ４１０７：ＹＥＳ）、通信処理を継続する（Ｓ４１０８）。また、通信制御部３１０は、受け取った認証結果が「ＮＧ」である場合には（Ｓ４１０７：ＮＯ）、通信処理を終了する（Ｓ４１０９）。そして、通信制御部３１０は、ユーザ操作などにより基地局認証に関する処理の終了を指示されたか否かを判断し、終了を指示されていない間は、上述の処理を繰り返す（Ｓ４１１０）。

[0144] 図２１は、無線端末装置３００の受信部３２０の動作の一例を示すフローチャートである。

[0145] 受信部３２０は、通信制御部３１０から認証開始要求の受信の指示を受け付け、指示を受け取る毎に（Ｓ４２０１：ＹＥＳ）、認証開始要求の受信を待機する。そして、受信部３２０は、無線基地局装置２００から認証開始要求を受信すると（Ｓ４２０２：ＹＥＳ）、通信制御部３１０へ処理を戻す。

- [0146] また、受信部 320 は、通信制御部 310 から基地局認証データを含む認証情報の受信の指示を受け付け、指示を受ける毎に（S4204：YES）、認証情報の受信を待機する。そして、受信部 320 は、無線基地局装置 200 から基地局認証データを含む認証情報を受信すると（S4205：YES）、通信制御部 310 に対して、受信した基地局認証データを渡し、処理を戻す（S4203）。
- [0147] 図 22 は、無線端末装置 300 のタイムスロット選択部 330 の動作の一例を示すフローチャートである。
- [0148] タイムスロット選択部 330 は、通信制御部 310 からタイムスロットの選択の指示を受け付ける。次に、タイムスロット選択部 330 は、指示を受け取る毎に（S4301：YES）、既定のタイムスロット番号の範囲内で、ランダムに、タイムスロット番号を少なくとも 1 つ選択する（S4302）。
- [0149] タイムスロット選択部 330 は、選択したタイムスロット番号を、選択状況管理部 340 に対して通知する（S4303）。そして、タイムスロット選択部 330 は、選択状況管理部 340 から、選択したタイムスロット番号と共に処理を戻されると、通信制御部 310 に対して、そのタイムスロット番号を渡し、処理を戻す（S4304）。
- [0150] 図 23 は、無線端末装置 300 の選択状況管理部 340 の動作の一例を示すフローチャートである。
- [0151] 選択状況管理部 340 は、タイムスロット選択部 330 からタイムスロット番号を受け付ける。次に、選択状況管理部 340 は、タイムスロット番号を受け取る毎に（S4401：YES）、受け取ったタイムスロット番号と、選択されたことを示す識別子とを関連付けた、選択状況を管理する（S4402）。そして、選択状況管理部 340 は、受け取ったタイムスロット番号以外のタイムスロット番号と、選択されていないことを示す識別子とを関連付けた選択状況を管理し（S4403）、タイムスロット選択部 330 へ処理を戻す（S4404）。

[0152] 図24は、無線端末装置300のタイムスロット管理部350の動作の一例を示すフローチャートである。

[0153] タイムスロット管理部350は、通信制御部310から、タイムスロット番号およびタイムスロット管理の開始の指示を受け付ける。そして、タイムスロット管理部350は、タイムスロット番号およびタイムスロット管理の開始の指示を受け取る毎に（S4501：YES）、タイムスロットの管理を行う（S4502～S4506）。

[0154] より具体的には、タイムスロット管理部350は、まず、タイムスロット番号を初期値「0」に設定する（S4502）。次に、タイムスロット管理部350は、既定のタイムスロット間隔に基づいて、タイムスロット番号が既定のタイムスロット番号に到達するまでタイムスロット番号をインクリメントする（S4506）。その間、タイムスロット管理部350は、インクリメントされるタイムスロット番号が、通信制御部310から受け取ったタイムスロット番号と一致するか否かを判断する。

[0155] タイムスロット管理部350は、これらのタイムスロット番号が一致するとき（S4503：YES）、送信部360に対して、既定のタイムスロット間隔を渡し、認証開始要求に対する応答の送信を指示する（S4504）。そして、タイムスロット管理部350は、インクリメントするタイムスロット番号が既定のタイムスロット番号に到達した場合には（S4505：YES）、通信制御部310に処理を戻す（S4507）。

[0156] 図25は、無線端末装置300の送信部360の動作の一例を示すフローチャートである。

[0157] 送信部360は、タイムスロット管理部350から、タイムスロット間隔と認証開始要求に対する応答送信の指示とを受け付ける。次に、送信部360は、指示を受け取る毎に（S4601：YES）、指定されたタイムスロット間隔内に認証開始要求に対する応答を生成して送信する（S4602、4603）。

[0158] より具体的には、送信部360は、まず、時間計測を開始し（S4602

）、無線基地局装置 200 に対して応答を送信する（S4603）。次に、送信部 360 は、計測を開始してから指定されたタイムスロット間隔が経過すると（S4604：YES）、タイムスロット管理部 350 に処理を戻す（S4605）。

[0159] 図 26 は、無線端末装置 300 の比較データ生成部 370 の動作の一例を示すフローチャートである。

[0160] 比較データ生成部 370 は、通信制御部 310 から比較データの生成の指示を受け付ける。そして、比較データ生成部 370 は、比較データの生成の指示を受け取る毎に（S4701：YES）、選択状況管理部 340 から選択状況を取得する（S4702）。

[0161] そして、比較データ生成部 370 は、既定のデータ生成ルールに従って、比較データを生成する（S4703）。そして、比較データ生成部 370 は、通信処理部 1107 に対して、生成した比較データを渡し、処理を戻す（S4704）。ここでは、比較データ生成部 370 は、図 9 で説明したデータ生成ルールにより、比較データを生成するものとする。すなわち、比較データ生成部 370 は、選択状況において各タイムスロット番号に対応付けられた情報を、タイムスロット番号の昇順に並べ替えることにより、比較データを生成する。

[0162] 図 27 は、無線端末装置 300 の基地局認証部 380 の動作の一例を示すフローチャートである。

[0163] 基地局認証部 380 は、通信制御部 310 から、基地局認証データおよび比較データと、基地局認証の指示とを受け付ける。そして、基地局認証部 380 は、基地局認証の指示を受け取る毎に（S4801：YES）、基地局認証データと比較データの論理積（AND）を計算する（S4802）。そして、基地局認証部 380 は、計算結果が、比較データと一致するか否かを判定する。なお、基地局認証部 380 は、比較データのビットパターンのうち、値が「1」となっているビット位置と、基地局認証データのビットパターンの対応するビット位置とで、値が一致するか否か（両方とも「1」）を

判定しても良い。

[0164] 基地局認証部 380 は、計算結果と比較データとが一致する場合には（S4803：YES）、受信した基地局認証データがリプレイアタックによるものではないと判断する。そして、基地局認証部 380 は、通信制御部 310 に対して、「認証OK」とする識別子を渡し、処理を戻す（S4804）。

[0165] 一方、基地局認証部 380 は、計算結果と比較データとが一致しない場合には（S4803：NO）、受信した基地局認証データがリプレイアタックによるものであると判断する。そして、基地局認証部 380 は、通信制御部 310 に対して、「認証NG」とする識別子を渡し、処理を戻す（S4805）。

[0166] 以上のような各部の動作により、図5～図11で説明した、無線基地局装置 200 の動作、無線端末装置 300 の動作、および無線通信システム 100 の動作が実現される。

[0167] 以上説明したように、本実施の形態に係る無線通信システム 100 は、複数の無線端末装置 300 におけるリプレイアタックに対する防御に関して有効な、共通の基地局認証データを生成し、これを利用することができる。したがって、本実施の形態に係る無線通信システム 100 は、基地局認証データの生成回数や、基地局認証データに対する署名付与の回数を減らすことができる。また、本実施の形態に係る無線通信システム 100 は、同報送信を行うことにより、基地局認証データの送信回数を減らすことができる。

[0168] したがって、本実施の形態に係る無線通信システム 100 は、個々の無線端末装置 300 においてリプレイアタックを排除しつつ、従来必要であった無線端末装置 300 毎の基地局認証データの演算時間および送信時間を削減することができる。そして、これにより、本実施の形態に係る無線通信システム 100 は、タイムスロット長の短縮を実現し、一定時間内でより多くの無線端末装置 300 が基地局認証を行うことを可能にする。

[0169] また、本実施の形態に係る無線通信システム 100 は、基地局認証データ

の生成に、「個々の無線端末装置 300 が選択するタイムスロット」、「選択されるタイムスロットの数」という、変動する情報を組み合わせて用いる。これにより、第三者が、無線基地局装置 200 から過去に送信された基地局認証データを用いてリプレイアタックを試みても、その基地局認証データと現在の比較データとが整合しない。したがって、本実施の形態に係る無線通信システム 100 は、認証の安全度を向上させることができる。

[0170] なお、1つの基地局認証データの生成の対象となる無線端末装置 300 の数は、上述の数に限定されるものではない。また、基地局認証データおよび比較データのデータ生成ルールも、上述の内容に限定されるものではなく、タイムスロットの番号の降順で並べる内容や、タイムスロットの番号に対する他の各種並べ替え関数を採用することができる。

[0171] また、基地局認証データの作成および比較データの作成は、フレーム単位で行うのではなく、フレームを構成する複数のタイムスロットのうちの一部のタイムスロットを単位として行っても良い。すなわち、既定のタイムスロット番号 n は、認証開始要求に対する応答が行われるフレームのタイムスロットの数よりも小さくても良い。この場合、1つのフレームに対して、複数の基地局認証データが生成および送信されることになる。これにより、基地局認証データおよび比較データのデータ生成ルールによっては、個々のデータの生成時間、送信時間、および照合時間を、更に短縮することができる。

[0172] (実施の形態 2)

本発明の実施の形態 2 は、認証開始要求に対する応答に、無線端末装置が生成した乱数値を付加し、この乱数値を基地局認証データおよび比較データの生成に用いることにより、これらのデータのランダム性を更に向上させる。

[0173] 図 28 は、本実施の形態に係る無線端末装置 300 a の構成の一例を示すブロック図であり、実施の形態 1 の図 13 に対応するものである。図 13 と同一または対応する部分には同一符号を付し、これについての説明を省略する。

- [0174] 図28において、無線端末装置300aは、図13に示す構成とは異なるタイムスロット選択部330a、選択状況管理部340a、タイムスロット管理部350a、および送信部360aを有する。更に、無線端末装置300aは、乱数生成部390aを新たに有する。乱数生成部390aは、例えば、タイムスロット選択部330aに配置される。
- [0175] 乱数生成部390aは、例えば既知の擬似乱数生成法を用いて、乱数値を生成する。但し、乱数生成部390aは、未受信および未選択を示す識別子である「0」以外であって、かつ応答に埋め込むことが可能な大きさの範囲で、乱数値を生成する。
- [0176] タイムスロット選択部330aは、乱数生成部390aを用いて、選択したタイムスロット毎に乱数値を生成する。そして、タイムスロット選択部330aは、生成した乱数値を、選択状況管理部340aおよび通信制御部310に渡す。
- [0177] 選択状況管理部340aは、タイムスロット選択部330aから乱数値を受け取ったとき、タイムスロット番号と乱数値とを関連付けた選択状況を管理する。
- [0178] タイムスロット管理部350aは、タイムスロット選択部330aから乱数値を受け取ったとき、送信部360aに対し、応答として乱数値を埋め込んだ応答を送信することを指示する。
- [0179] 送信部360aは、タイムスロット管理部350aから応答送信の指示と乱数値とを受け取る。そして、送信部360aは、受け取った乱数値を埋め込んだ応答を生成し、認証開始要求に対する応答として、選択したスロットを使用して送信する。
- [0180] 図29は、乱数値が埋め込まれた応答のデータ構成の一例を示す図であり、実施の形態1の図6に対応するものである。図6と同一部分には同一符号を付す。
- [0181] 図29に示すように、乱数値が埋め込まれた応答の無線データ530は、同期コード511、Length512、コマンドコード513、乱数値5

3 1、およびチェックサム 5 1 4 を、この順に並べて構成される。Length 5 1 2 は、ここでは、コマンドコード 5 1 3、乱数値 5 3 1、およびチェックサム 5 1 4 の合計長さを記述する。

[0182] 無線端末装置 3 0 0 は、コマンドコード 5 1 3 に、当該無線データ 5 3 0 が応答であって乱数を格納していることを示す所定のコマンドコードを記述する。また、無線端末装置 3 0 0 は、乱数値 5 3 1 に、生成した乱数値を記述して、乱数値が埋め込まれた応答の無線データ 5 3 0 を生成する。無線基地局装置 2 0 0 は、コマンドコード 5 1 3 に上述の所定のコマンドコードが記述されているとき、当該無線データ 5 1 0 が応答であると判定し、かつ、乱数値 5 3 1 を抽出する。

[0183] このような無線端末装置 3 0 0 a は、生成した乱数値を応答として無線基地局装置 2 0 0 a に送信し、乱数値と未選択を示す識別子とがタイムスロット番号の昇順に並べられたデータを、比較データとして生成することができる。そして、無線端末装置 3 0 0 a は、無線基地局装置 2 0 0 a より送られる基地局認証データに、選択したタイムスロット番号に選択した乱数値が対応付けられているか否かに基づいて、基地局認証を行うことができる。

[0184] 図 3 0 は、本実施の形態に係る無線基地局装置 2 0 0 a の構成の一例を示すブロック図であり、実施の形態 1 の図 1 2 に対応するものである。図 1 2 と同一または対応する部分には同一符号を付し、これについての説明を省略する。

[0185] 図 3 0 において、無線基地局装置 2 0 0 a は、図 1 2 に示す受信部 2 4 0 および受信状況管理部 2 5 0 に代えて、これらとは異なる受信部 2 4 0 a および受信状況管理部 2 5 0 a を有する。

[0186] 受信部 2 4 0 a は、認証開始要求に対する応答を受信したとき、受信通知ではなく、応答として送られてきた ACK メッセージに埋め込まれた乱数値を、受信状況管理部 2 5 0 a に渡す。

[0187] 受信状況管理部 2 5 0 a は、受信部 2 4 0 a から乱数値を受け取ったとき、タイムスロット番号と乱数値とを関連付けた受信状況を管理する。

- [0188] このような無線基地局装置 200a は、受信した乱数値と未受信を示す識別子とがタイムスロット番号の昇順に並べられたデータを、基地局認証データとして生成することができる。
- [0189] 以下、本実施の形態に係る無線通信システムの動作のうち、実施の形態 1 と異なる部分について説明する。各図において、実施の形態 1 の対応する図面の同一または対応する部分には同ステップ番号を付し、これについての説明を省略する。
- [0190] 図 31 は、無線基地局装置 200a および無線端末装置 300a を有する無線通信システムの全体動作の一例を示すシーケンス図であり、実施の形態 1 の図 5 に対応するものである。図 32 は、無線基地局装置 200a による基地局認証データのデータ生成ルールの一例を示す模式図であり、実施の形態 1 の図 8 に対応するものである。図 33 は、無線端末装置 300a による比較データのデータ生成ルールの一例を示す模式図であり、実施の形態 1 の図 9 に対応するものである。
- [0191] 図 31 に示すように、各無線端末装置 300a は、生成した乱数値を、無線基地局装置 200a への応答と、選択状況とのそれぞれに含める。また、無線基地局装置 200a は、受信した乱数値を含む受信状況を管理する。この結果、図 32 および図 33 に示すように、基地局認証データと比較データのうち、実施の形態 1 においては基地局認証に使用されたタイムスロットを示す識別子が記述された部分に、本実施の形態においては乱数値が記述されることになる。
- [0192] 図 34 は、無線基地局装置 200a の受信部 240a の動作の一例を示すフローチャートであり、実施の形態 1 の図 17 に対応するものである。
- [0193] 受信部 240a は、無線端末装置 300a から応答を受信したとき（S3403：YES、S3405：YES）、受信状況管理部 250a に対し、タイムスロット番号と、応答に含まれていた乱数値とを渡す（S3407a）。
- [0194] 図 35 は、無線基地局装置 200a の受信状況管理部 250a の動作の一

例を示すフローチャートであり、実施の形態 1 の図 18 に対応するものである。

[0195] 受信状況管理部 250a は、受信部 240a から乱数値を通知されたタイムスロットについては (S3503a: YES)、タイムスロット番号と乱数値とを関連付けて管理する (S3504a)。

[0196] この結果、図 32 に示すように、乱数値が組み込まれた基地局認証データが生成され、同報送信される。

[0197] 図 36 は、無線端末装置 300a のタイムスロット選択部 330a の動作の一例を示すフローチャートであり、実施の形態 1 の図 22 に対応するものである。

[0198] タイムスロット選択部 330a は、選択したタイムスロット毎に、乱数生成部 390a を使用して乱数値を生成する (S4302a)。そして、タイムスロット選択部 330a は、選択状況管理部 340a に対し、選択したタイムスロット番号と、タイムスロット番号に対応する乱数値とを通知し (S4303a)、選択状況管理部 340a から処理を戻される。次に、タイムスロット選択部 330a は、通信制御部 310 に対し、選択したタイムスロット番号とタイムスロット番号に対応する乱数値とを渡し、処理を戻す (S4304a)。

[0199] 図 37 は、無線端末装置 300a の選択状況管理部 340a の動作の一例を示すフローチャートであり、実施の形態 1 の図 23 に対応するものである。

[0200] 選択状況管理部 340a は、タイムスロット選択部 330a からタイムスロット番号と、タイムスロット番号に対応する乱数値とを受け取る (S4401a: YES)。次に、選択状況管理部 340a は、受け取ったタイムスロット番号と乱数値とを関連付けて管理する (S4402a)。

[0201] 図 38 は、無線端末装置 300a のタイムスロット管理部 350a の動作の一例を示すフローチャートであり、実施の形態 1 の図 24 に対応するものである。

- [0202] タイムスロット管理部 350a は、通信制御部 310 から、タイムスロット番号とタイムスロット番号に対応する乱数値とを受け取り、タイムスロットの管理の開始を指示される（S4501a：YES）。次に、タイムスロット管理部 350a は、タイムスロット番号のインクリメントを開始する。そして、タイムスロット管理部 350a は、受け取ったタイムスロット番号のタイムスロットが到来すると（S4503：YES）、送信部 360a に対し、タイムスロット間隔とタイムスロット番号に対応する乱数値とを渡す。そして、タイムスロット管理部 350a は、認証開始要求に対する応答を指示する（S4504a）。
- [0203] 図 39 は、無線端末装置 300a の送信部 360a の動作の一例を示すフローチャートであり、実施の形態 1 の図 25 に対応するものである。
- [0204] 送信部 360a は、タイムスロット管理部 350a から、タイムスロット間隔とタイムスロット番号に対応する乱数値とを受け取る（S4601a：YES）。次に、送信部 360a は、現在のタイムスロットを用いて、認証開始要求に対する応答として、受け取った乱数値を無線基地局装置 200a に送信する（S4603a）。
- [0205] この結果、図 33 に示すように、乱数値が組み込まれた比較データが生成され、無線基地局装置 200a に送信される。
- [0206] 応答先と基地局認証データの送り元が同一である場合には、基地局認証データのうち比較データの乱数値が記述されたデータ位置に、比較データの乱数値と同一の乱数値が記述されていることになる。
- [0207] したがって、無線端末装置 300a の基地局認証部 380 は、例えば、2進数データとした上で論理積を取り、論理積の結果が比較データと一致するか否かによって、基地局認証データと比較データとが整合するか否かを判定すれば良い。
- [0208] このように、本実施形態に係る無線端末装置 300a は、基地局認証データの生成の際に、実施の形態 1 で説明した 3 つの変動する値に加えて、乱数値を組み合わせて用いる。したがって、本実施形態に係る無線端末装置 30

0 a は、更に安全度の高い認証を実現することができる。

[0209] なお、本実施の形態では、複数の無線端末装置 300 a が同一のタイムスロットを選択した場合、基地局認証データと比較データとで対応する乱数値が一致しないことになる。このような場合、他の無線端末装置 300 a との重複により応答を送信しない無線端末装置 300 a は、乱数値の一致不一致ではなく、応答を受信したスロットか否かに基づいて、データの整合を判断することが望ましい。すなわち、無線端末装置 300 a のデータの整合の判断は、基地局認証データのうち選択したタイムスロットに対応する位置の値が「0」か否かに基づいて、データの整合を判断することになる。

[0210] また、以上説明した各実施の形態では、認証される側の無線通信装置である無線基地局装置が固定設置され、認証を行う側の無線通信装置である無線端末装置が移動する場合について説明したが、本発明はこれに限定されない。複数の無線端末装置の全てまたは一部が固定設置され、無線基地局装置が移動しても良いし、複数の無線端末装置と無線基地局装置との両方が移動しても良い。

[0211] また、無線基地局装置は、その無線基地局装置が保持する基地局認証データに対応する比較データのデータ生成ルールを、共有情報として、認証開始要求または基地局認証データに付加するようにしても良い。この場合、比較データ生成部は、認証開始要求または基地局認証データに付加された共有情報から、比較データの生成ルールを取得する。これにより、無線基地局装置ごとに基地局認証データのデータ生成ルールが異なる場合でも、無線端末装置は、常に、通信中の無線基地局装置に対応するデータ生成ルールを用いて、比較データを生成することができる。

[0212] また、無線基地局装置および各無線端末装置は、互いの間で使用する基地局認証データおよび比較データのデータ生成ルールを、基地局認証毎に切り替えても良い。基地局認証毎にデータ生成ルールを切り替える場合は、データ生成ルールの実行順序を予め設定しておいても良いし、どのデータ生成ルールを使用するかを示す情報を、基地局認証を開始する毎に交換しても良い。

。

[0213] また、基地局認証データは、必ずしもタイムスロット毎の識別子を並べたデータである必要ではなく、タイムスロット毎の応答の有無を複数のタイムスロットについて集約したデータであって、無線端末装置側で解析可能なデータであれば良い。例えば、応答があったタイムスロットのタイムスロット番号を記述したデータが考えられる。

[0214] 2009年3月4日出願の特願2009-51319の日本出願に含まれる明細書、図面および要約書の開示内容は、すべて本願に援用される。

産業上の利用可能性

[0215] 本発明に係る無線基地局装置、無線端末装置、および基地局認証方法は、一定時間内でより多くの無線端末装置が基地局認証を行うことができる無線基地局装置、無線端末装置、および基地局認証方法として有用である。

符号の説明

[0216] 100 無線通信システム
200、200a 無線基地局装置
210、310 通信制御部
220、360、360a 送信部
230 タイムスロット管理部
240、240a、320 受信部
250、250a 受信状況管理部
260 基地局認証データ生成部
300、300a 無線端末装置
330、330a タイムスロット選択部
340、340a 選択状況管理部
350、350a タイムスロット管理部
370 比較データ生成部
380 基地局認証部
390a 乱数生成部

請求の範囲

- [請求項1] 複数の無線端末装置と時分割多元接続により無線通信を行う無線基地局装置であって、
- 前記無線端末装置から、基地局認証を開始することを示す応答情報を受信する応答情報受信部と、
- タイムスロット毎の前記応答情報の受信の有無を示す情報を集約した基地局認証データを生成する基地局認証データ生成部と、
- 生成された前記基地局認証データを、前記無線端末装置に送信する基地局認証データ送信部と、
- を有する無線基地局装置。
- [請求項2] 前記無線端末装置に対して、前記基地局認証の開始を要求する認証開始要求を送信する要求送信部、を更に有し、
- 前記応答情報は、前記認証開始要求に対する応答として前記無線端末装置から受信する、
- 請求項 1 記載の無線基地局装置。
- [請求項3] 前記基地局認証データは、前記タイムスロットのそれぞれに対して、前記応答情報受信部が前記応答情報を受信したか否かを示す識別子を対応付けた情報である、
- 請求項 2 記載の無線基地局装置。
- [請求項4] 前記基地局認証データは、前記タイムスロットの番号に応じた所定の順序で前記識別子を並べた情報である、
- 請求項 3 記載の無線基地局装置。
- [請求項5] 前記所定の順序を、共有情報として前記認証開始要求または前記基地局認証データに付加する共有情報通知部、を更に有する、
- 請求項 4 記載の無線基地局装置。
- [請求項6] 前記基地局認証データ送信部は、
- 前記応答情報を受信した前記タイムスロットの数が所定の閾値を超えるとき、前記基地局認証データを送信しない、

請求項 1 記載の無線基地局装置。

[請求項7]

無線基地局装置と時分割多元接続により無線通信を行う複数の無線端末装置のうちの 1 つであって、

タイムスロットを選択するタイムスロット選択部と、

選択された前記タイムスロットを用いて、基地局認証を開始することを示す応答情報を、前記無線基地局装置に送信する応答情報送信部と、

送信された前記応答情報に対応して、基地局認証データを受信する基地局認証データ受信部と、

受信した前記基地局認証データが、選択された前記タイムスロットにおいて前記応答情報の受信があったことを示すか否かに基づいて、前記基地局認証データの送信元に対する基地局認証を行う基地局認証部と、

を有する無線端末装置。

[請求項8]

前記無線基地局装置から、前記基地局認証の開始を要求する認証開始要求を受信する要求受信部、を更に有し、

前記応答情報は、前記認証開始要求に対する応答として受信する、請求項 7 記載の無線端末装置。

[請求項9]

前記タイムスロットのそれぞれに対して、前記タイムスロット選択部の選択の有無を示す識別子を対応付けた比較データを生成する比較データ生成部、を更に有し、

前記基地局認証部は、

生成された前記比較データと受信された前記基地局認証データとを比較することにより、前記基地局認証を行う、

請求項 8 記載の無線端末装置。

[請求項10]

前記比較データは、前記タイムスロットの番号に応じた所定の順序で前記識別子を並べた情報である、

請求項 9 記載の無線端末装置。

[請求項11] 前記所定の順序を、前記認証開始要求または前記基地局認証データに付加された共有情報から取得する共有情報取得部、を更に有する、請求項10記載の無線端末装置。

[請求項12] 無線基地局装置と、この無線基地局と時分割多元接続により無線通信を行う複数の無線端末装置との間で行われる基地局認証方法であって、

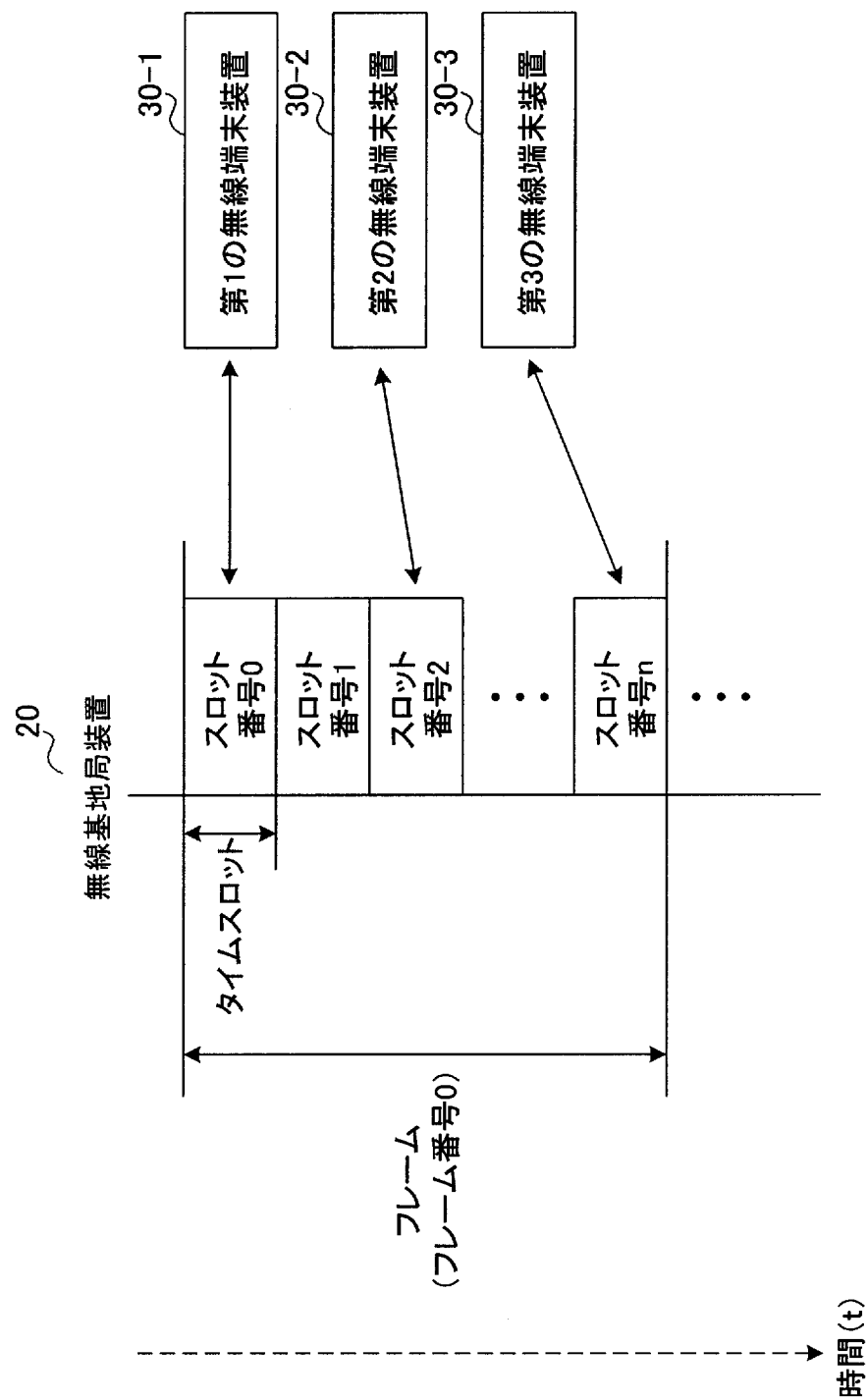
前記無線端末装置が、タイムスロットを選択し、選択したタイムスロットを用いて、基地局認証を開始することを示す応答情報を前記無線基地局装置に送信するステップと、

前記無線基地局装置が、タイムスロット毎の前記応答情報の受信の有無を示す情報を複数のタイムスロットについて集約した基地局認証データを生成し、生成した前記基地局認証データを前記無線端末装置に送信するステップと、

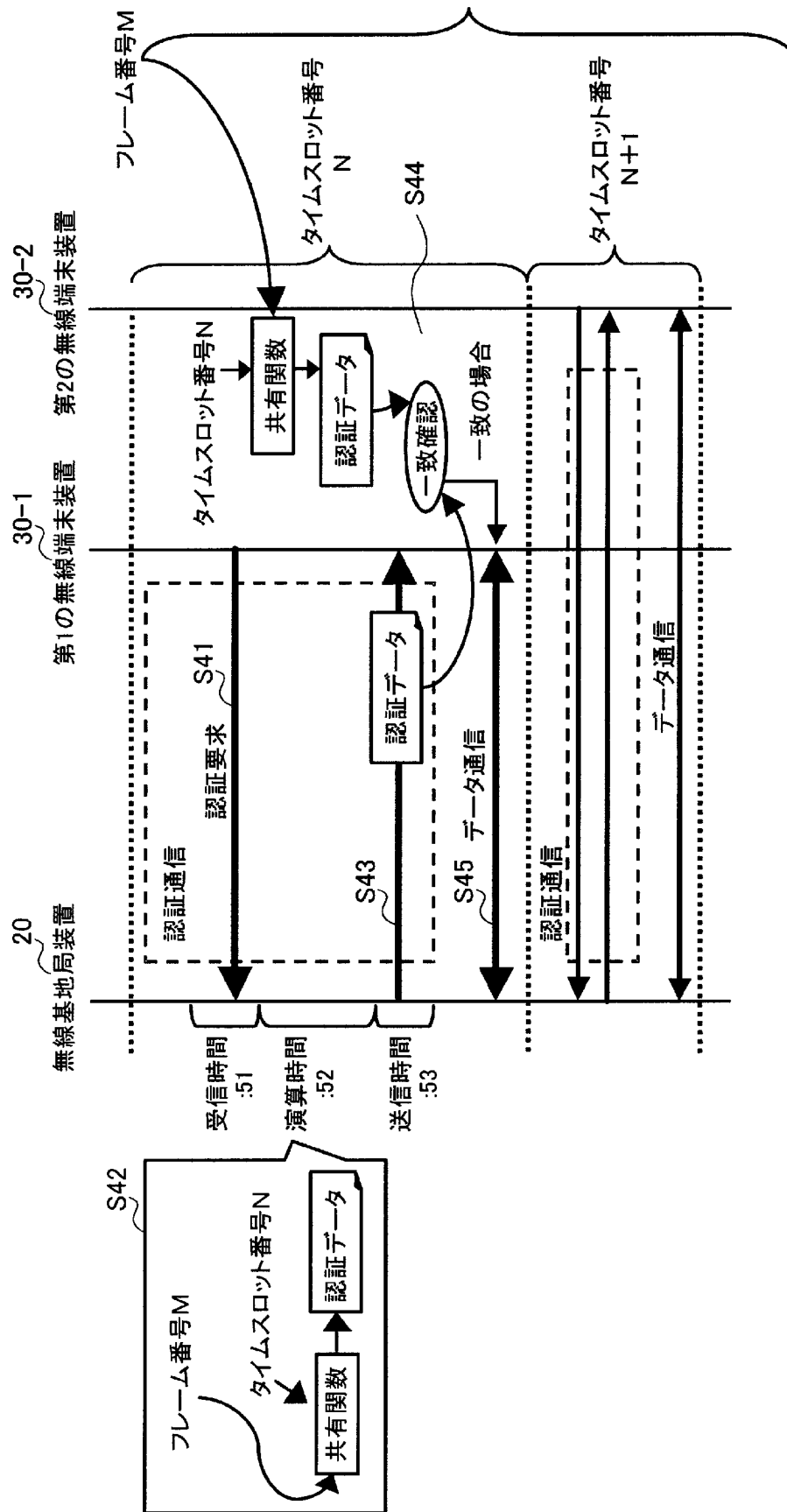
前記無線端末装置が、受信した前記基地局認証データが、選択した前記タイムスロットにおいて前記応答情報の受信があったことを示すか否かに基づいて、前記基地局認証データの送信元に対する基地局認証を行うステップと、

を有する基地局認証方法。

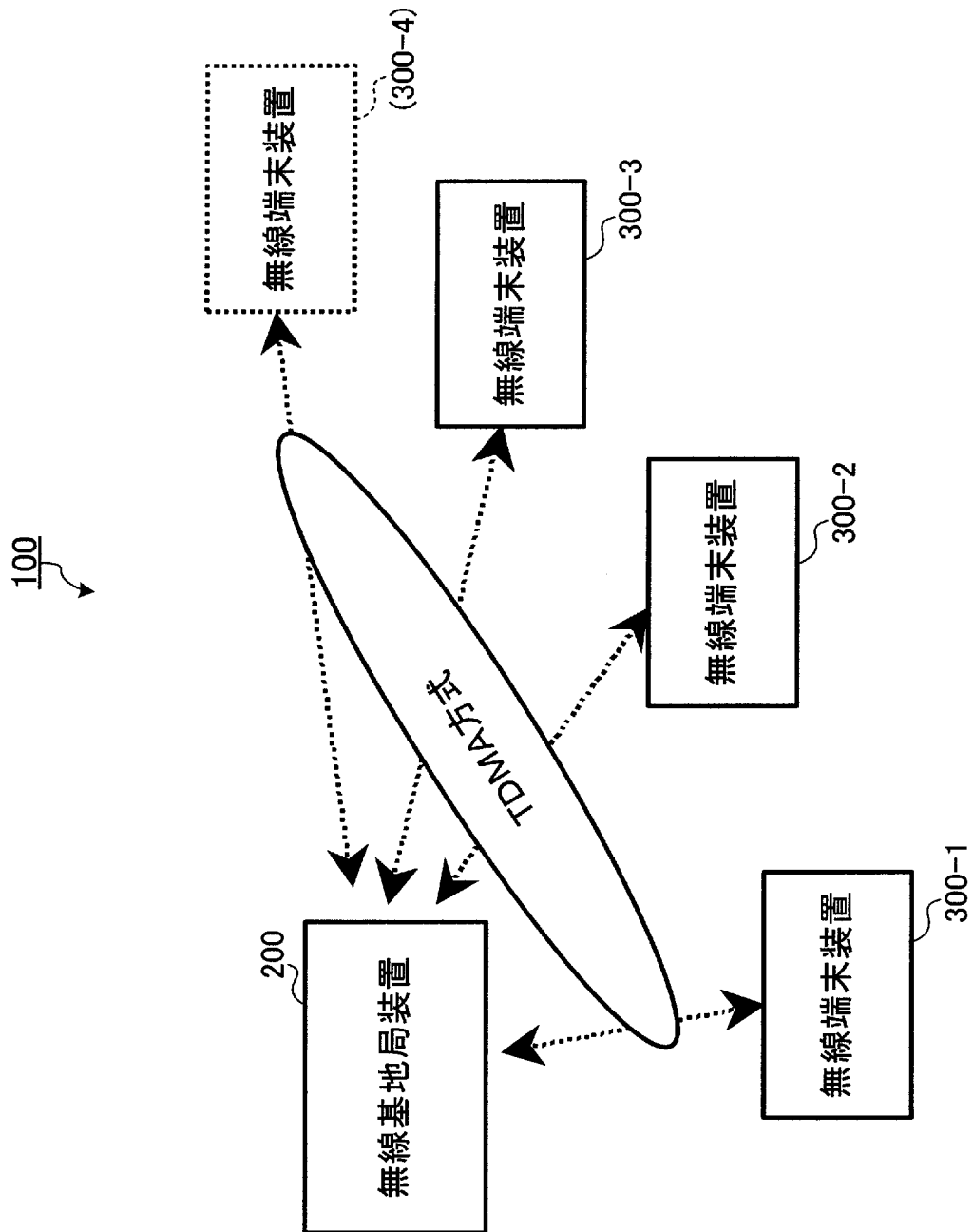
[図1]



[図2]



[図3]



[図4]

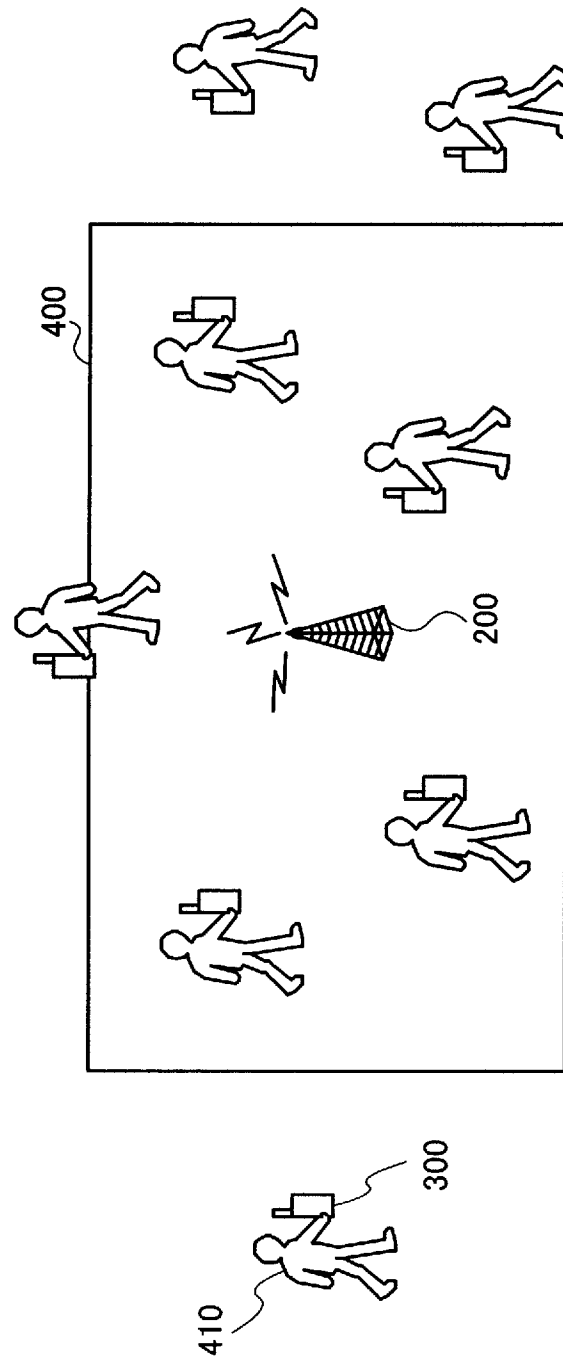
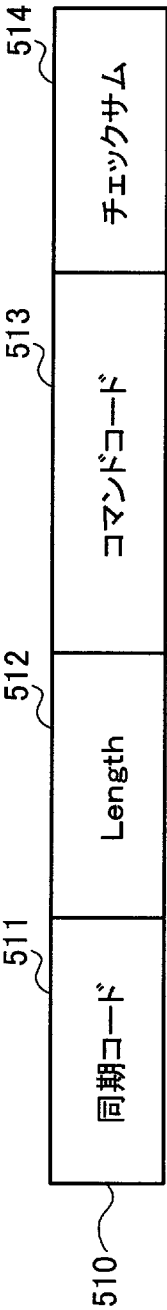


Figure 1 is a sequence diagram illustrating a radio base station authentication method. The diagram shows the interaction between a radio base station (200) and three wireless terminal devices (300-1, 300-2, 300-3) over time (t).

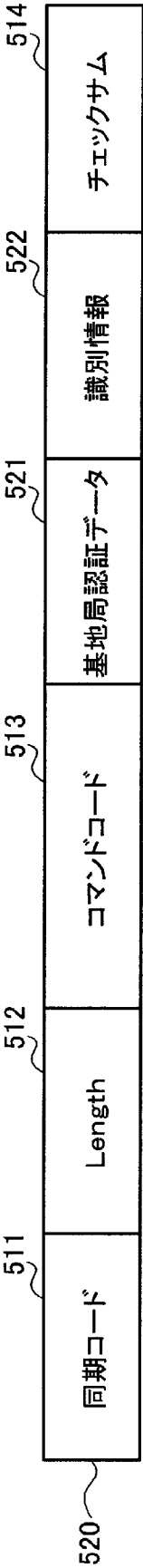
The process begins with the radio base station (200) sending an authentication start request (S2100) to the wireless terminal devices (300-1, 300-2, 300-3). Each terminal device then performs a random time slot selection (S2200). The radio base station (200) then generates comparison data (S2300) for each terminal device. The terminal devices then generate comparison data (S2600) and perform a comparison check (S2700). The radio base station (200) also generates comparison data (S2400) and performs a comparison check (S2500).

The diagram includes a timeline for time slots (0, 1, 2, ..., n) and a timeline for time (t). The time slots are used to schedule the authentication process for each terminal device. The time (t) axis shows the sequence of events, including the request, selection, generation, and checking of comparison data.

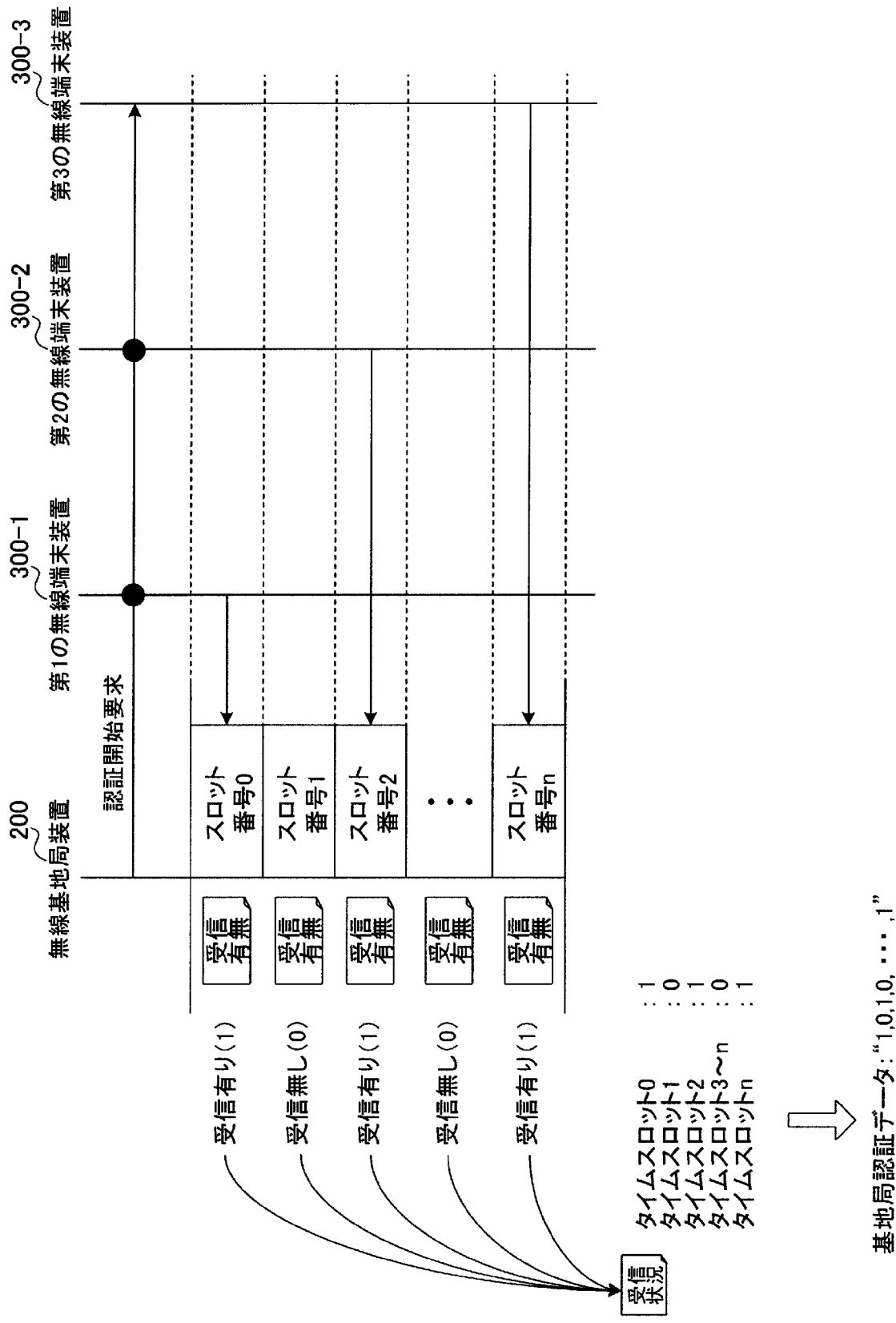
[図6]



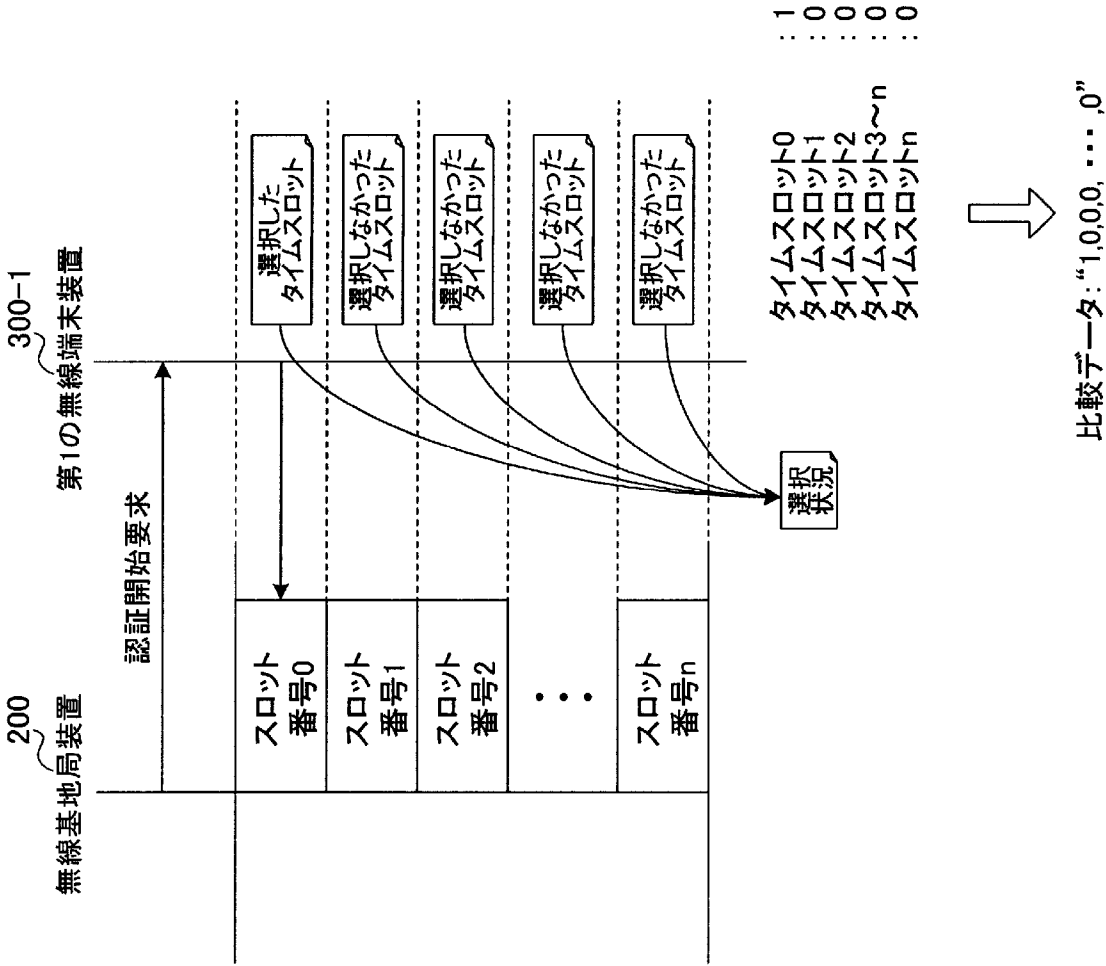
[図7]



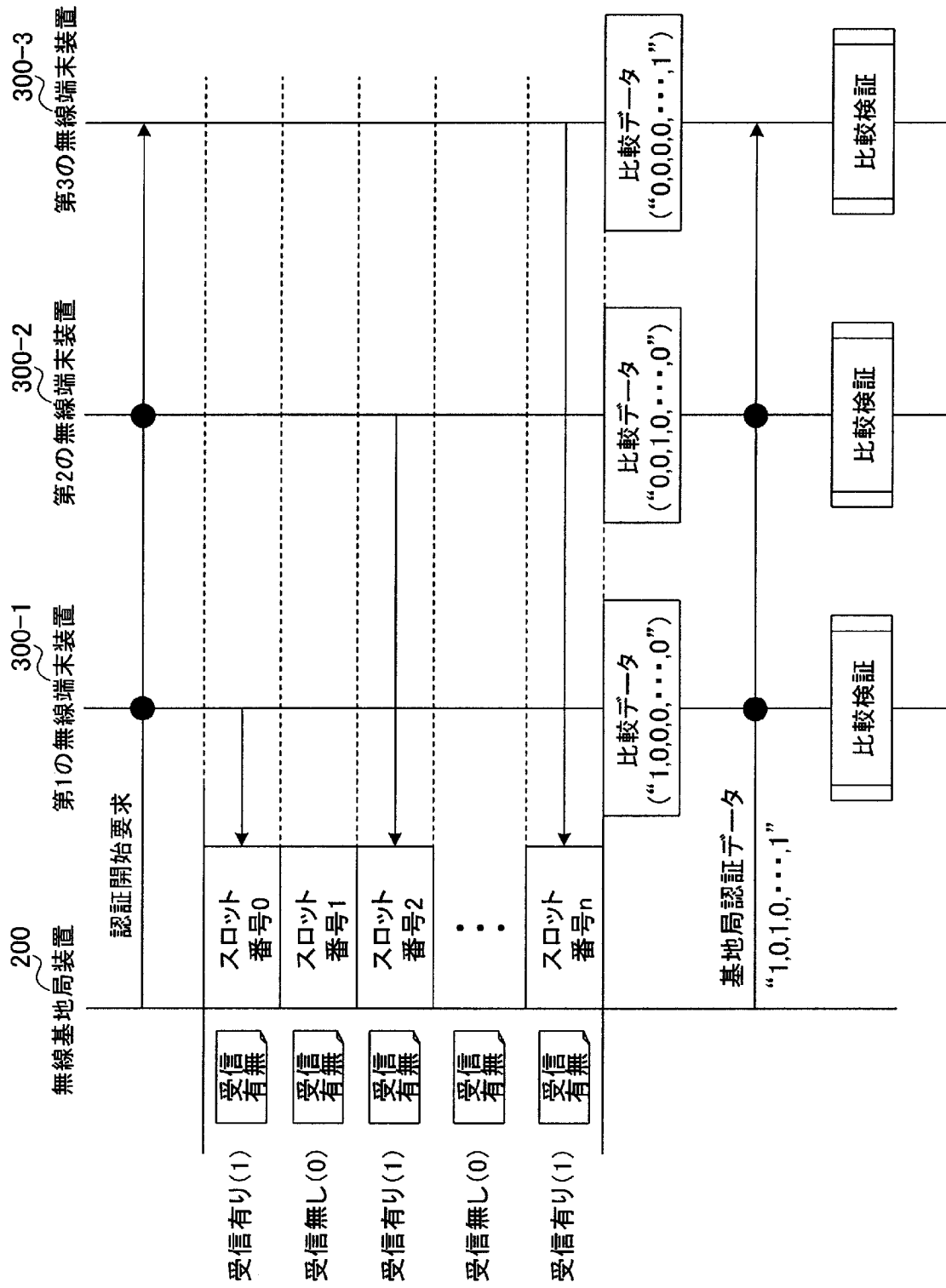
[図8]



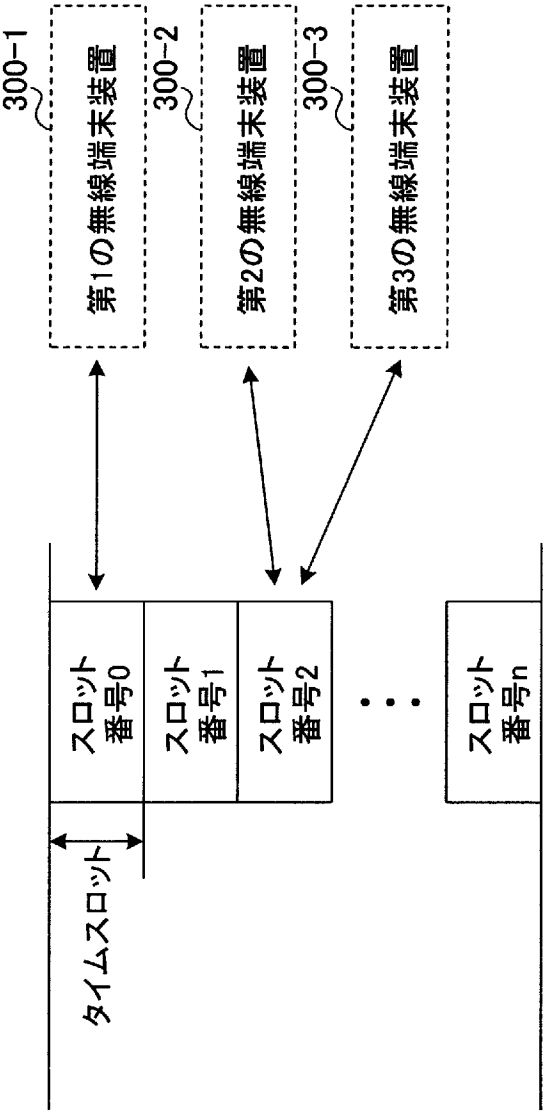
[図9]



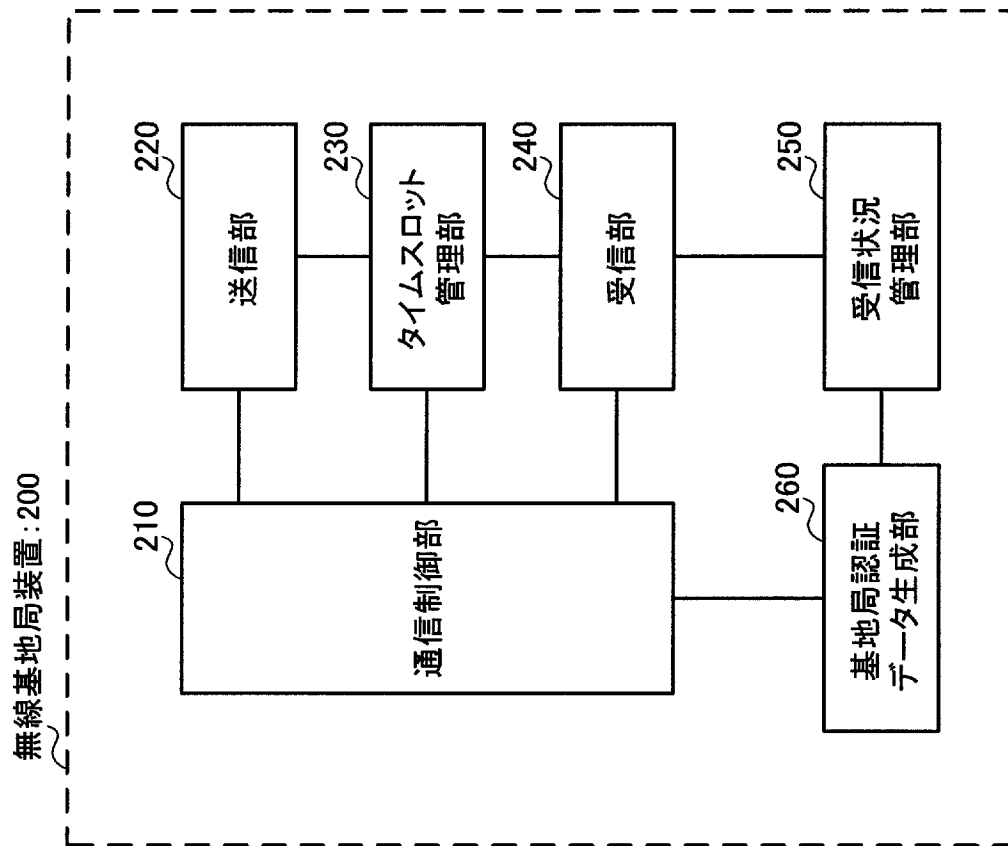
[図10]



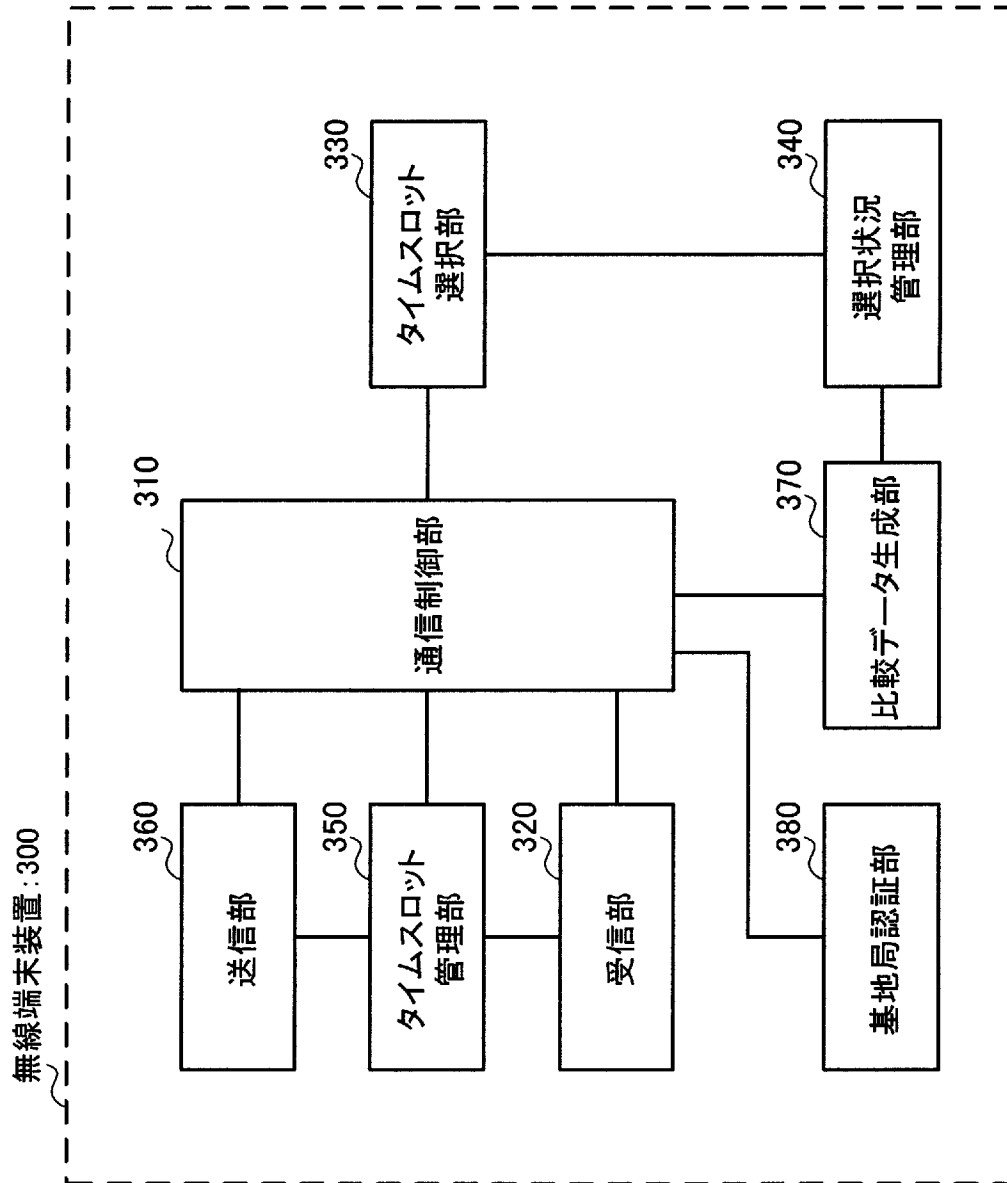
[図11]



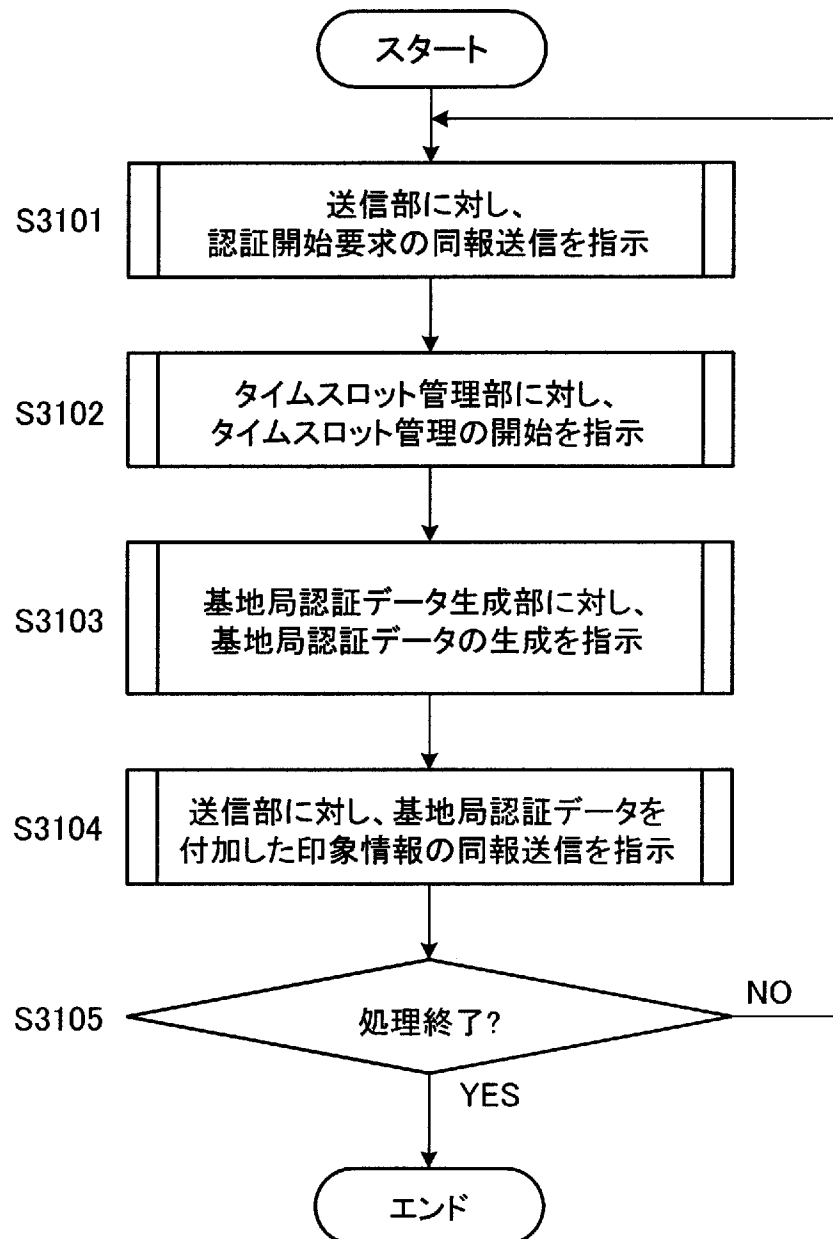
[図12]



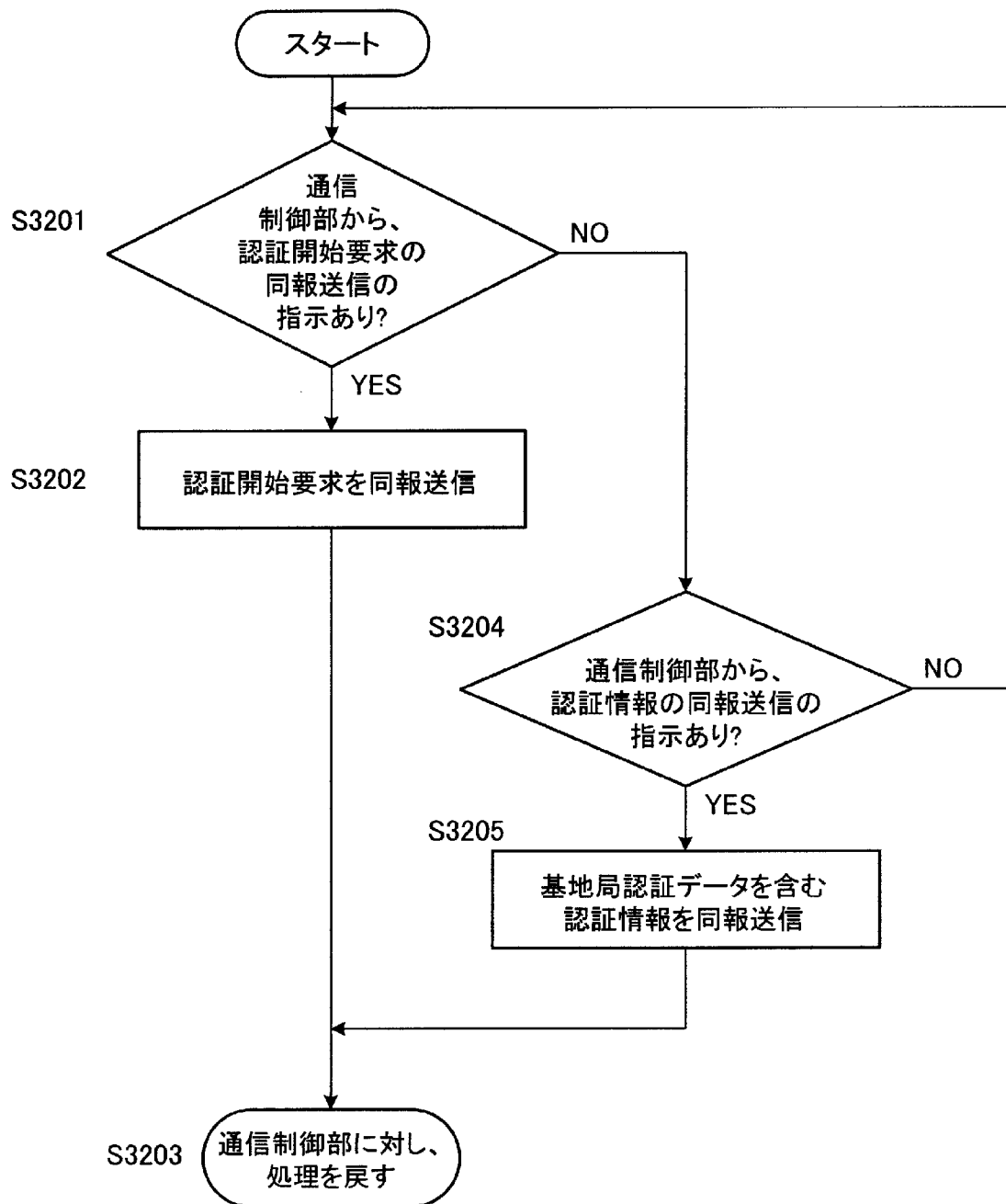
[図13]



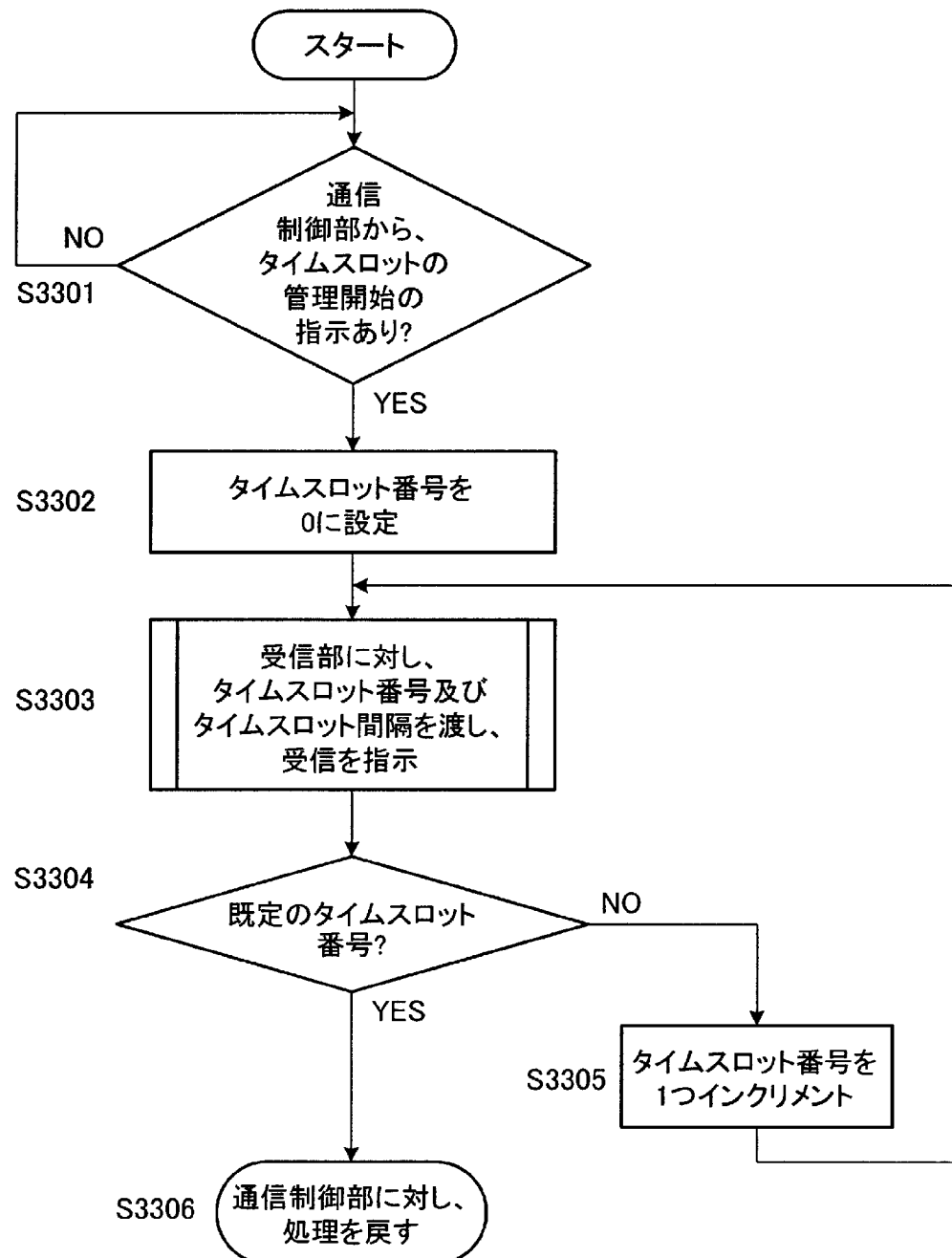
[図14]



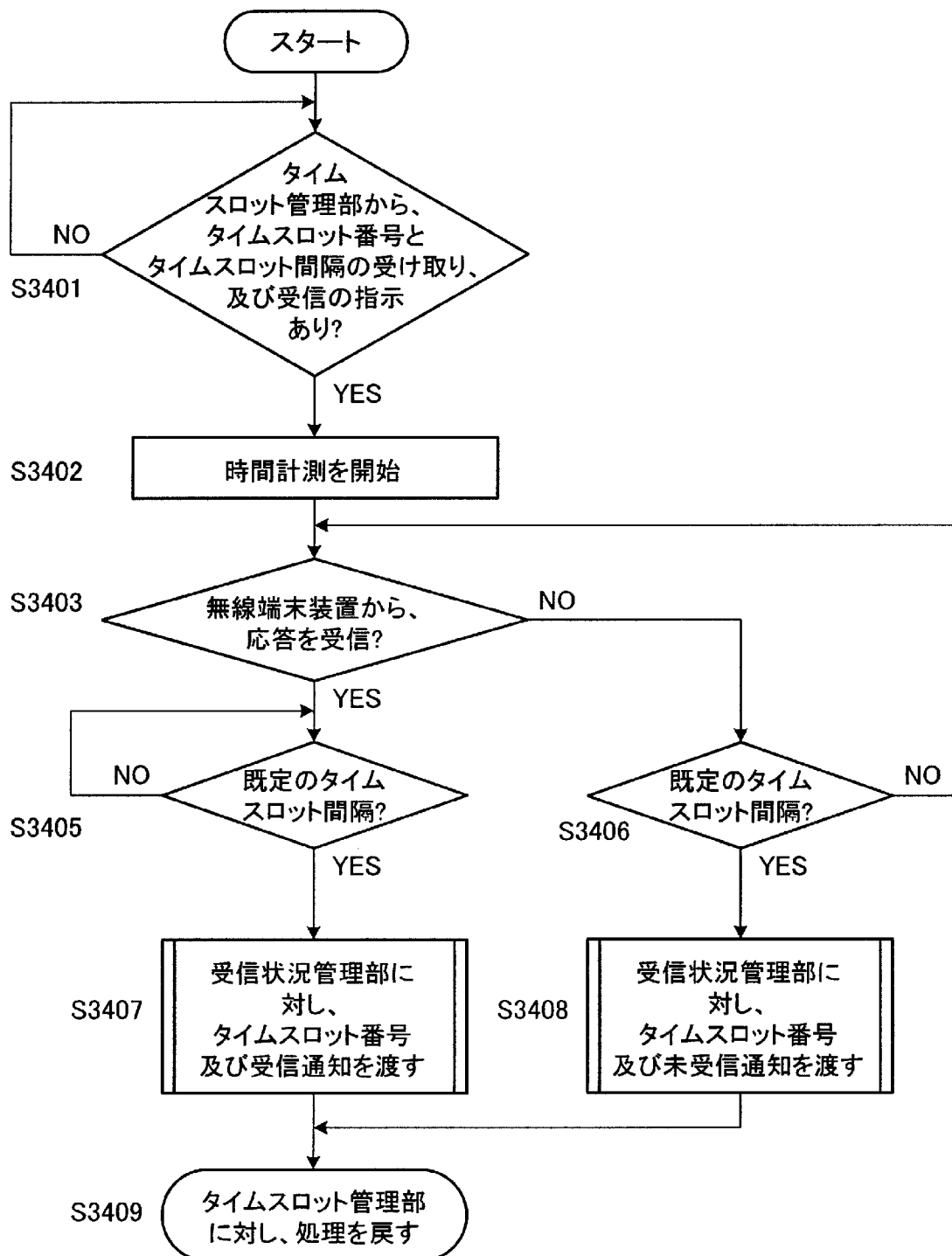
[図15]



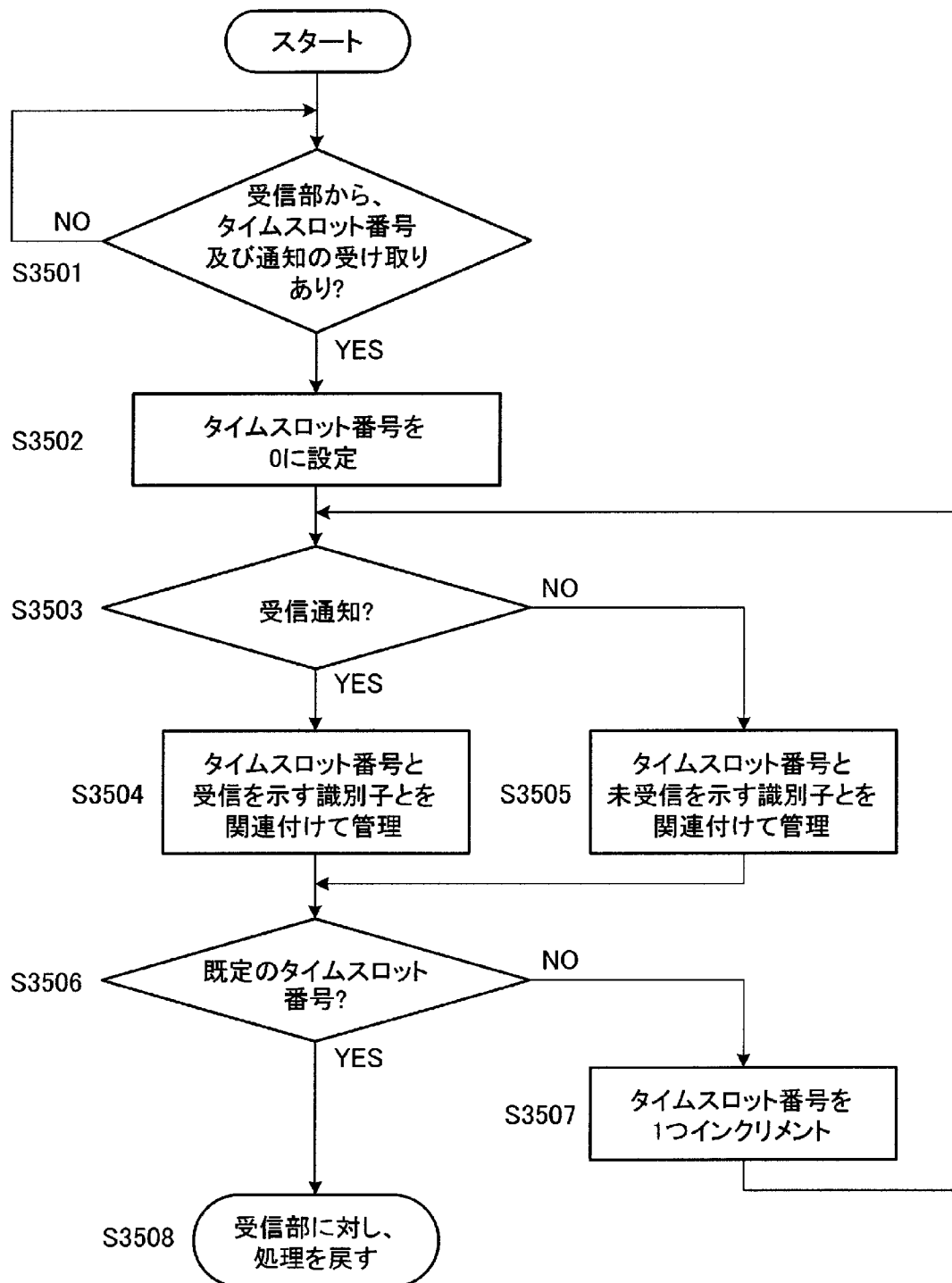
[図16]



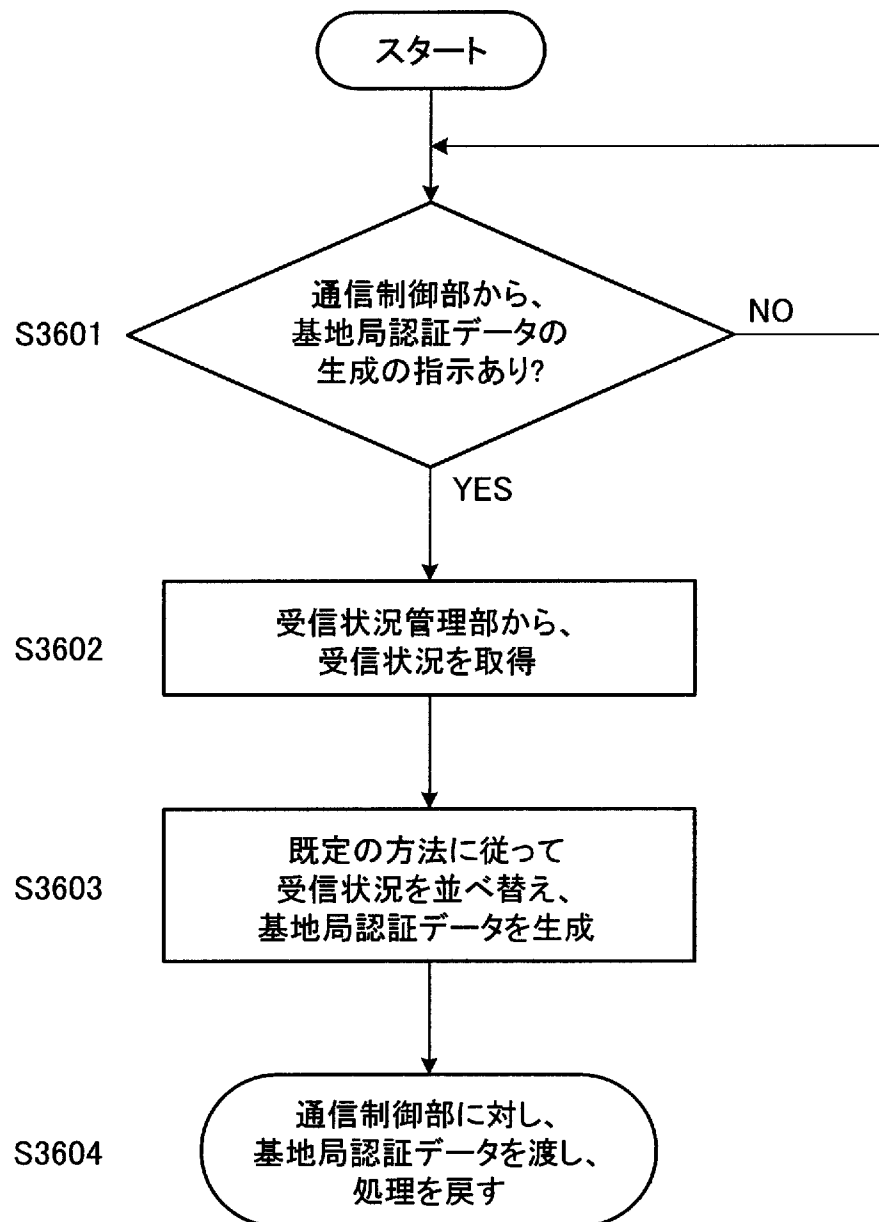
[図17]



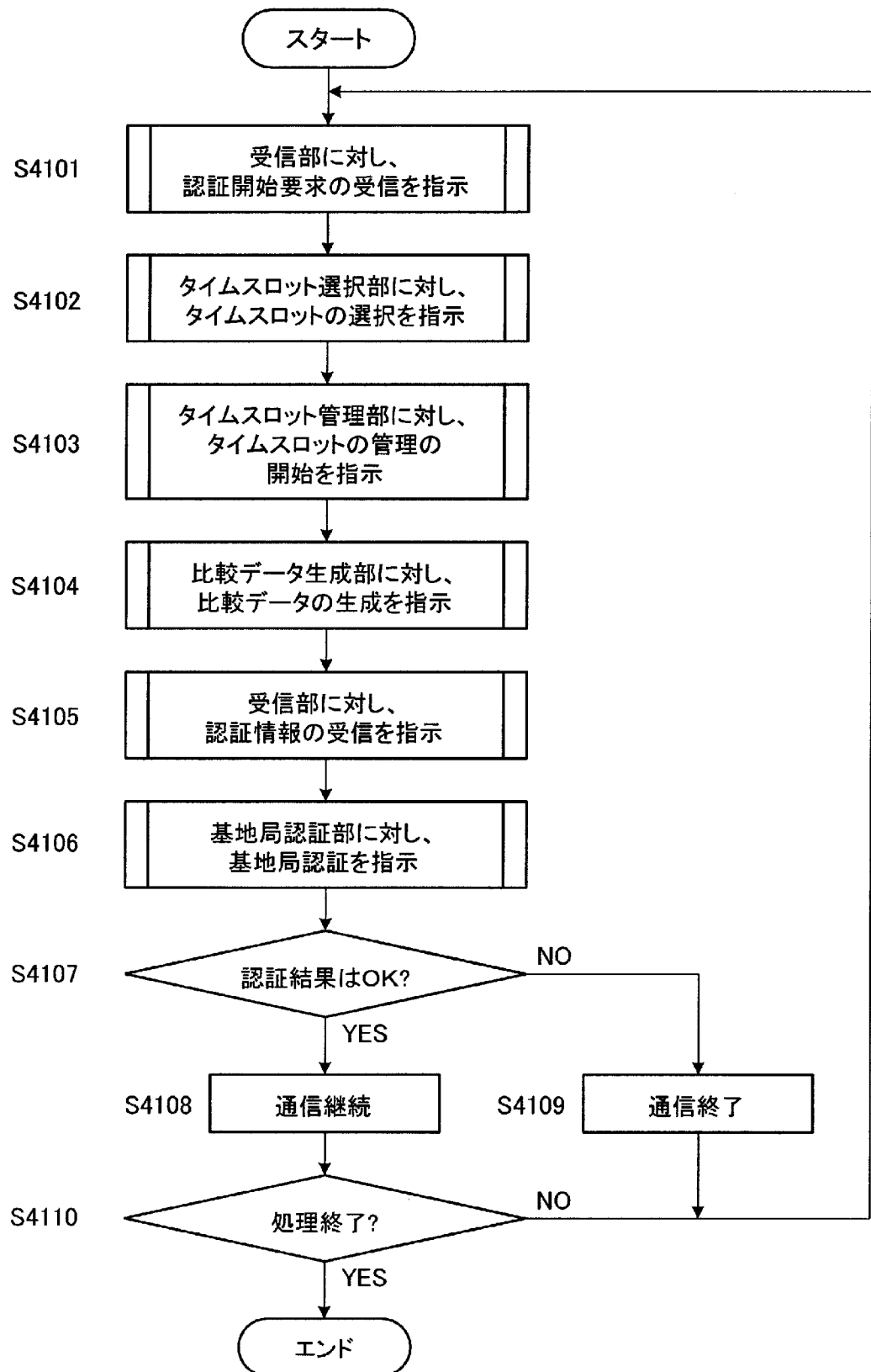
[図18]



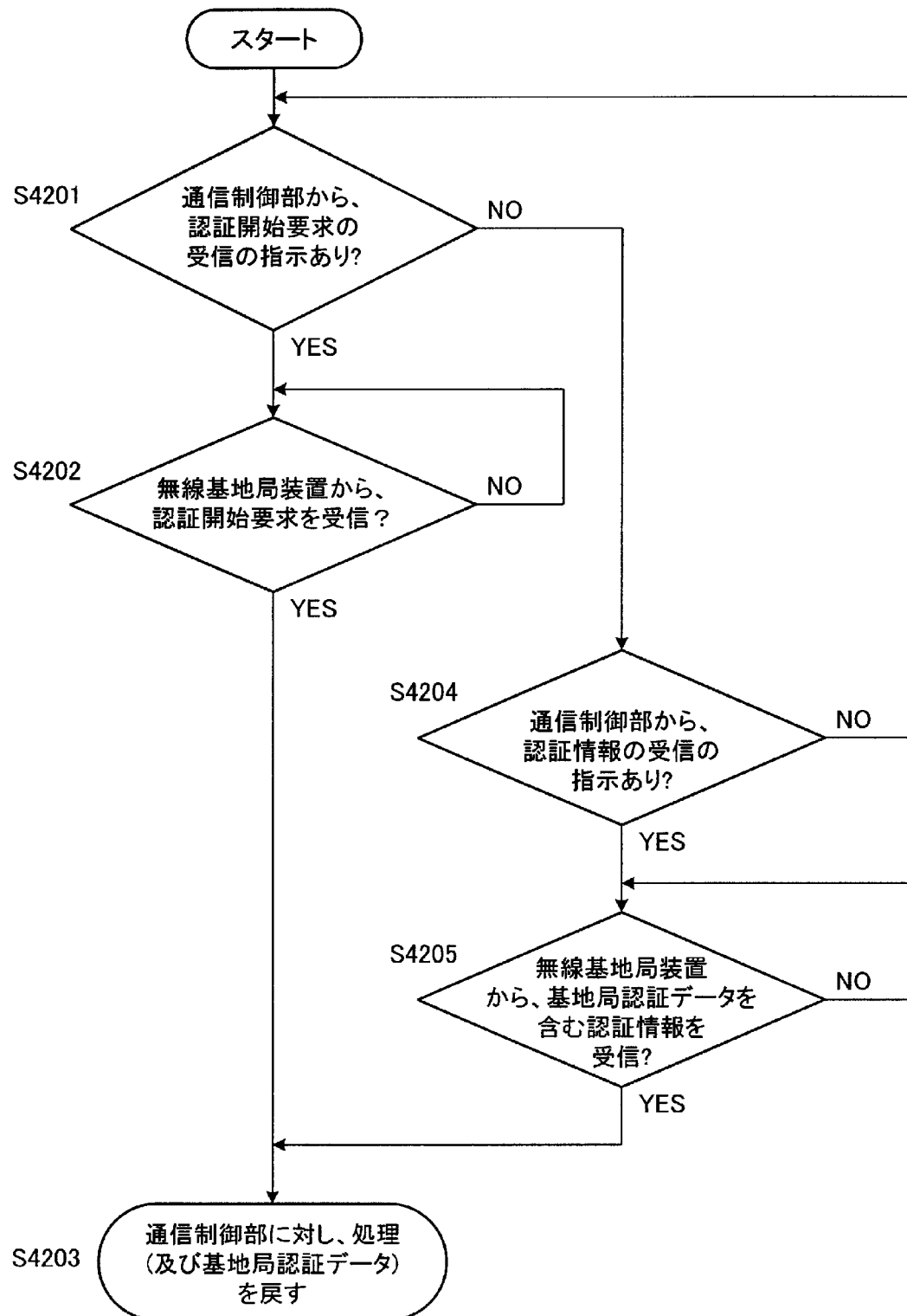
[図19]



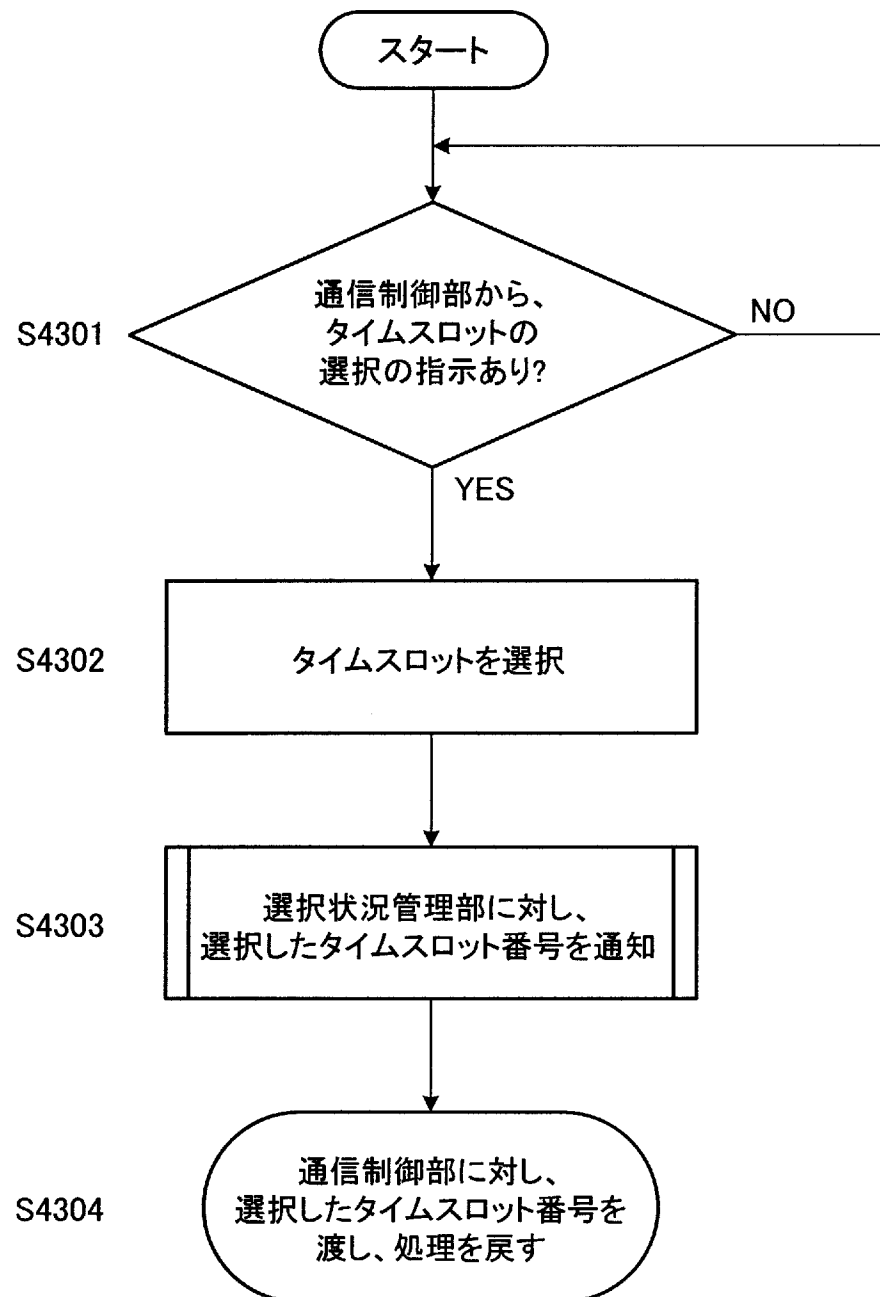
[図20]



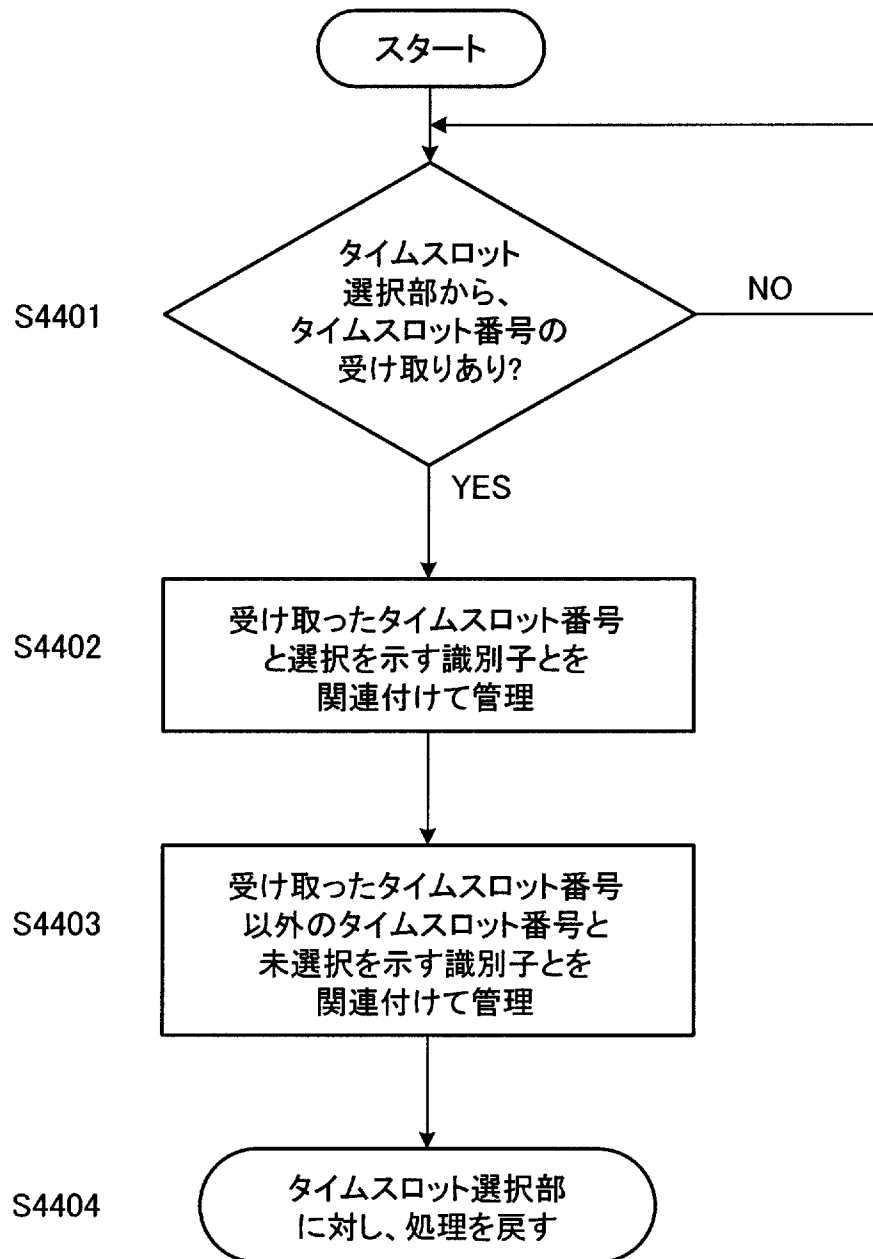
[図21]



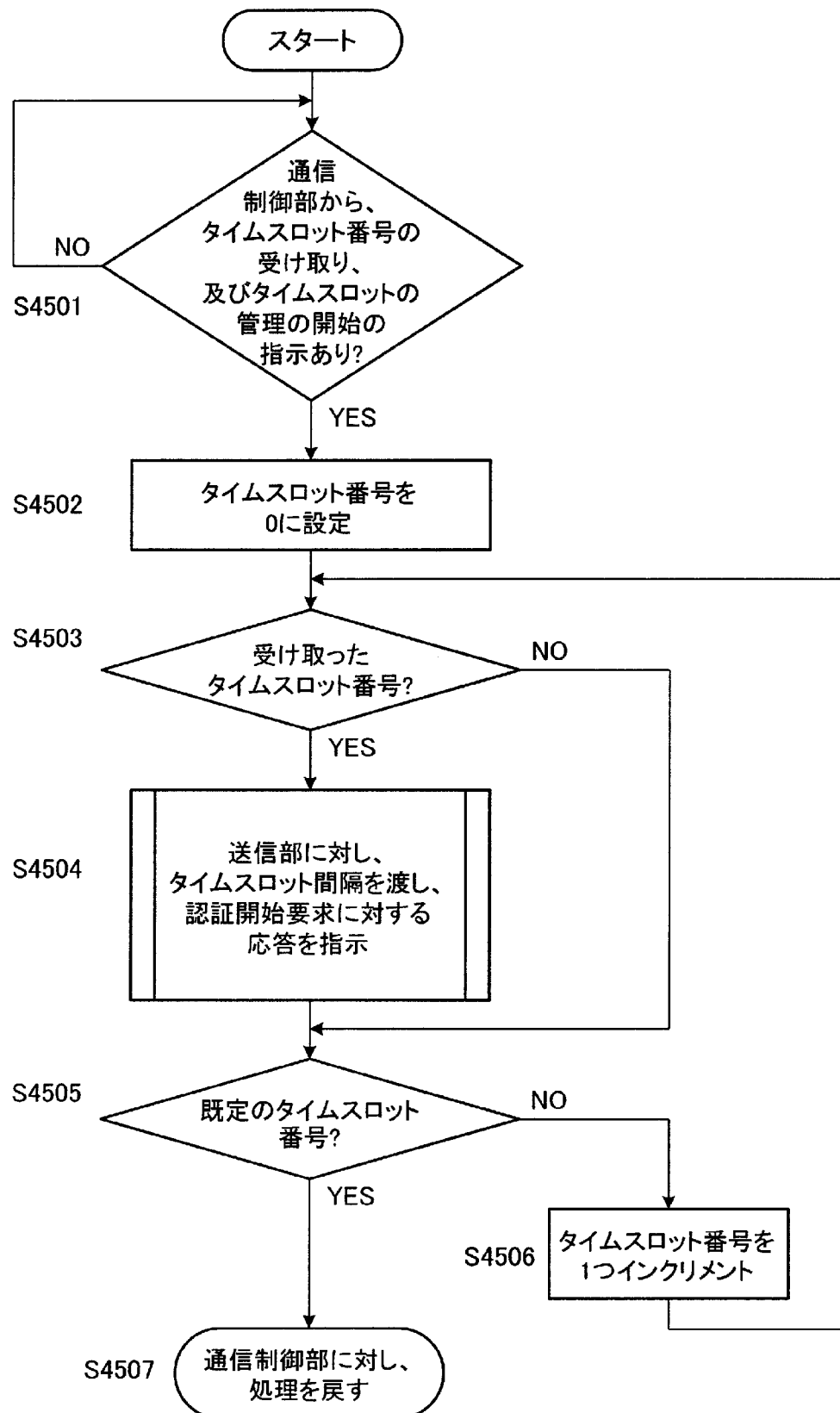
[図22]



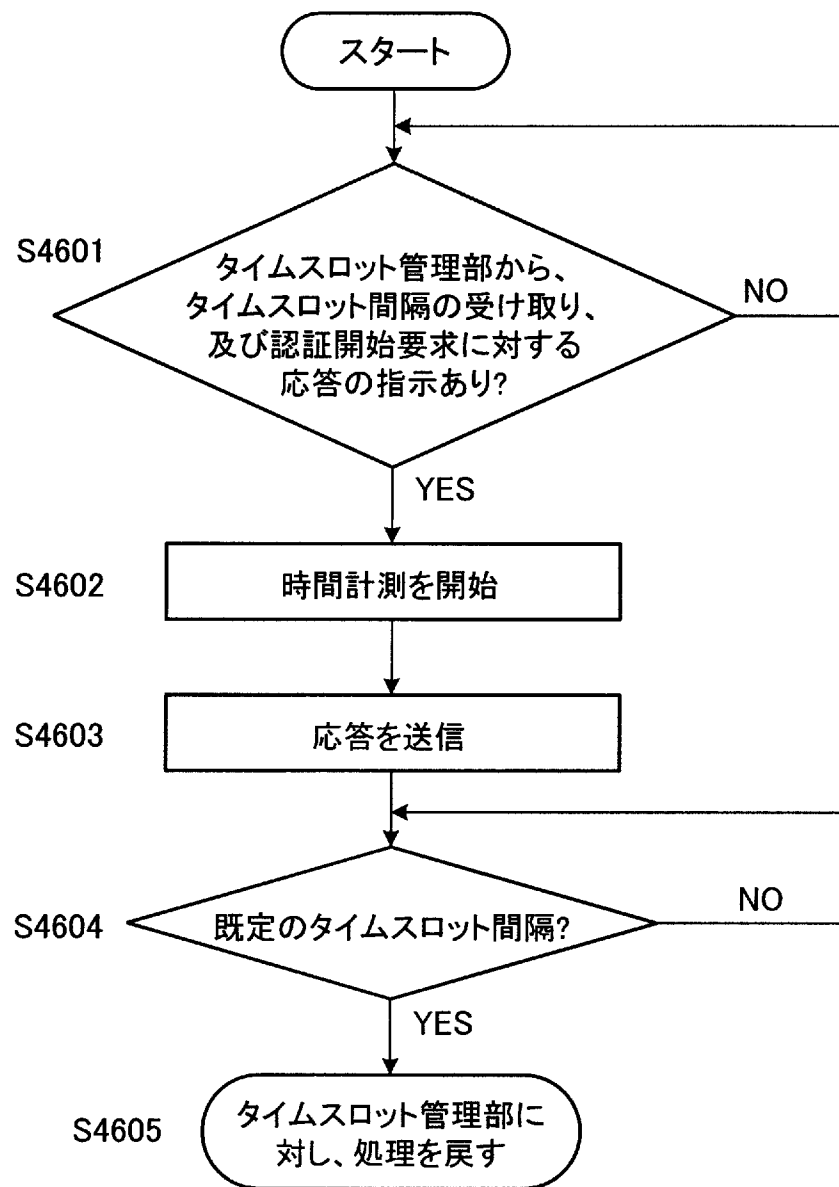
[図23]



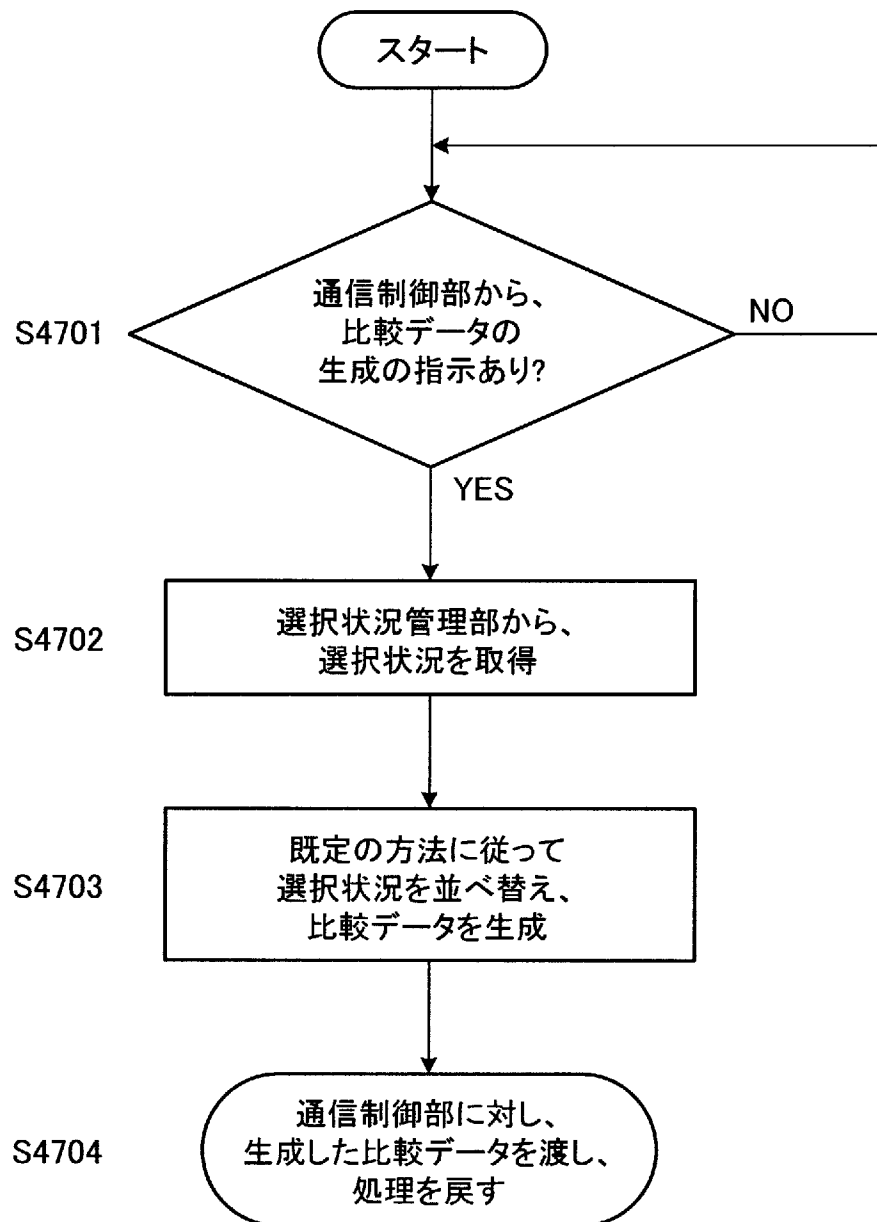
[図24]



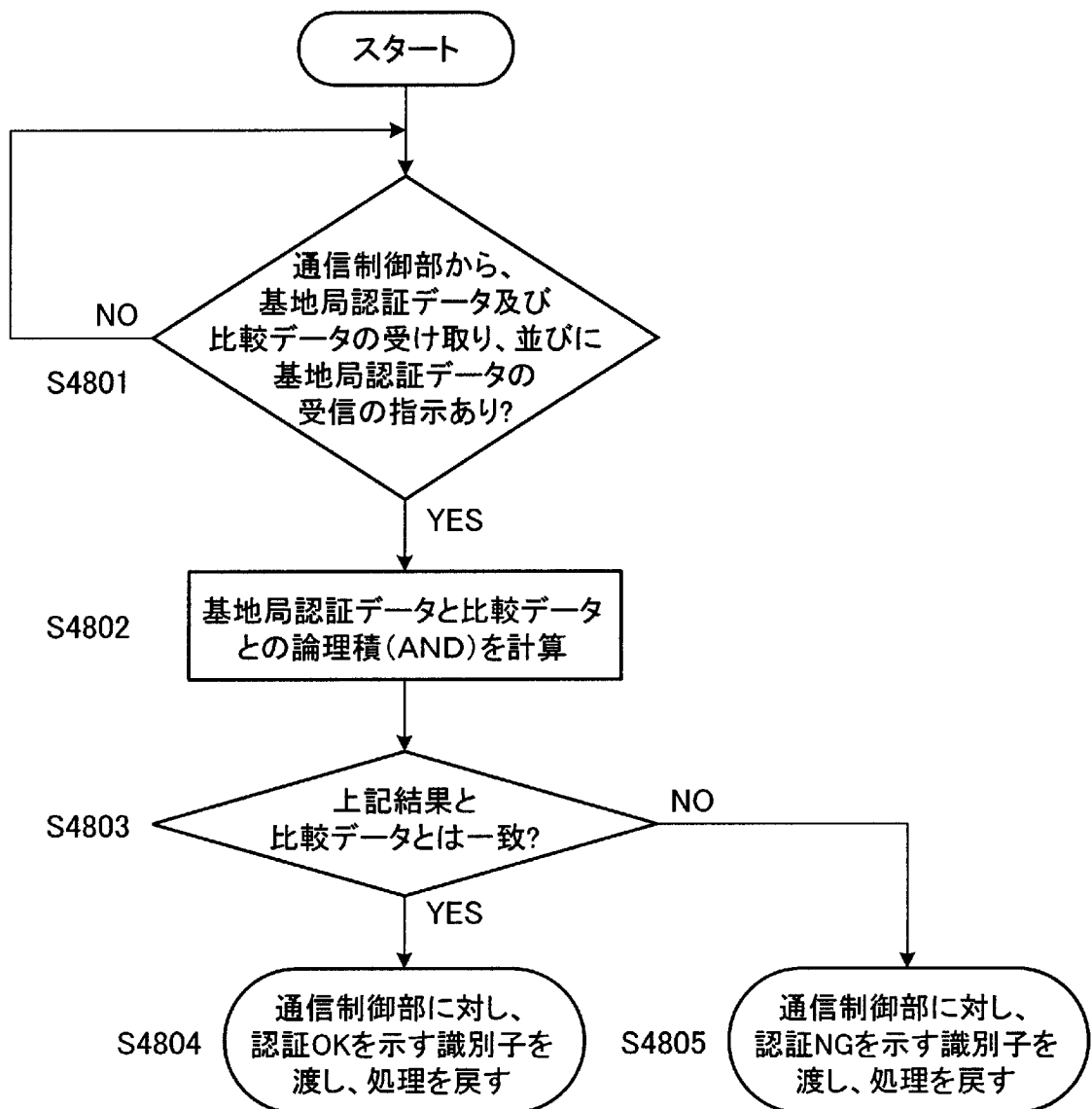
[図25]



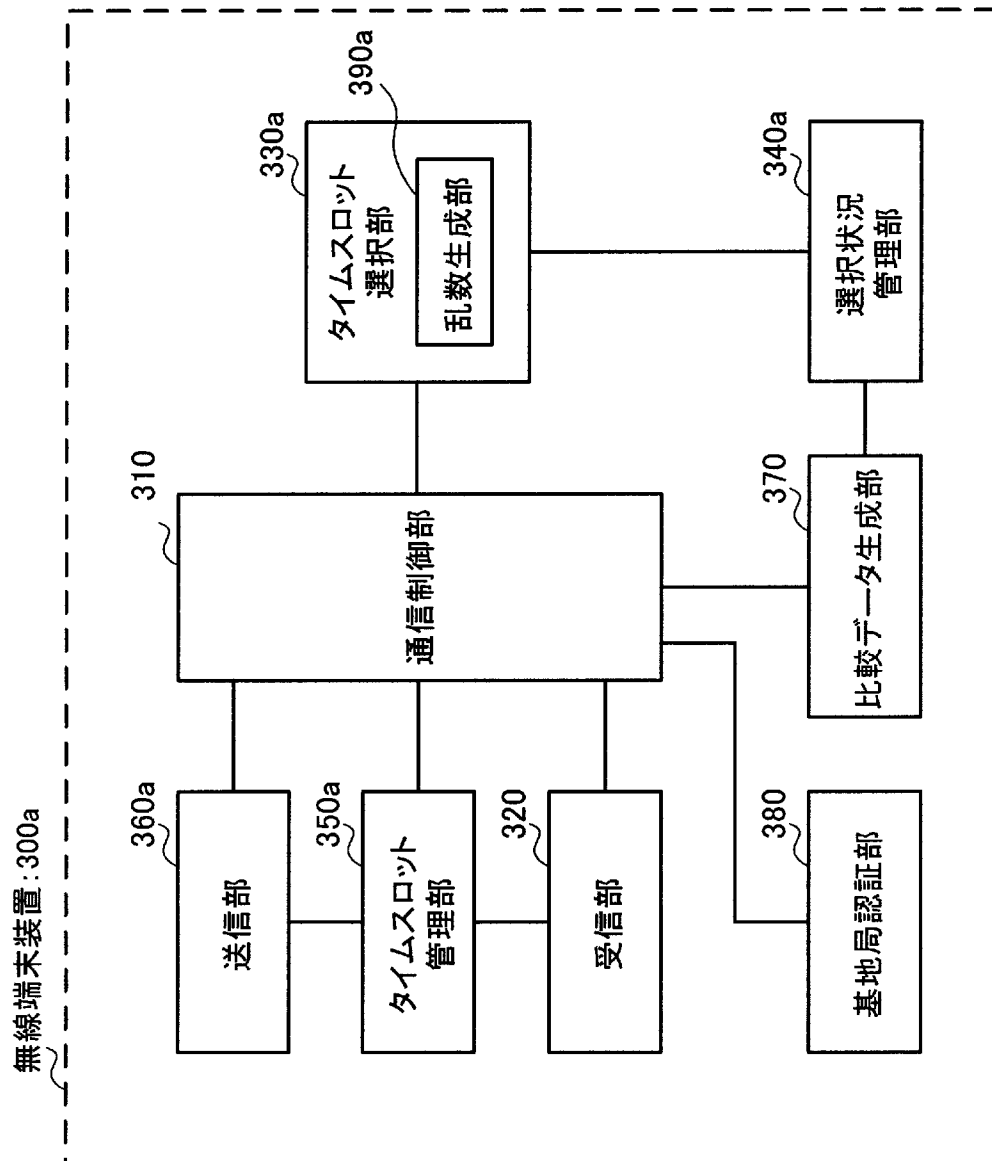
[図26]



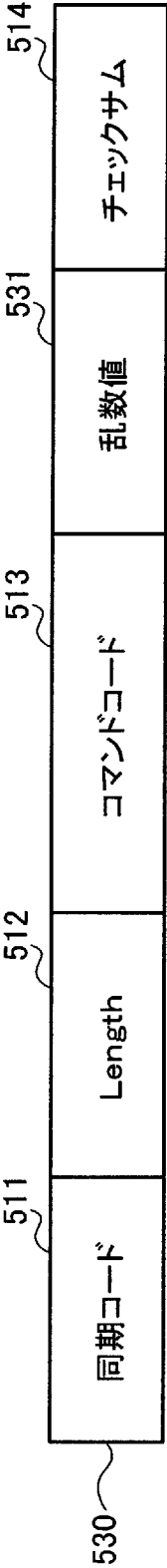
[図27]



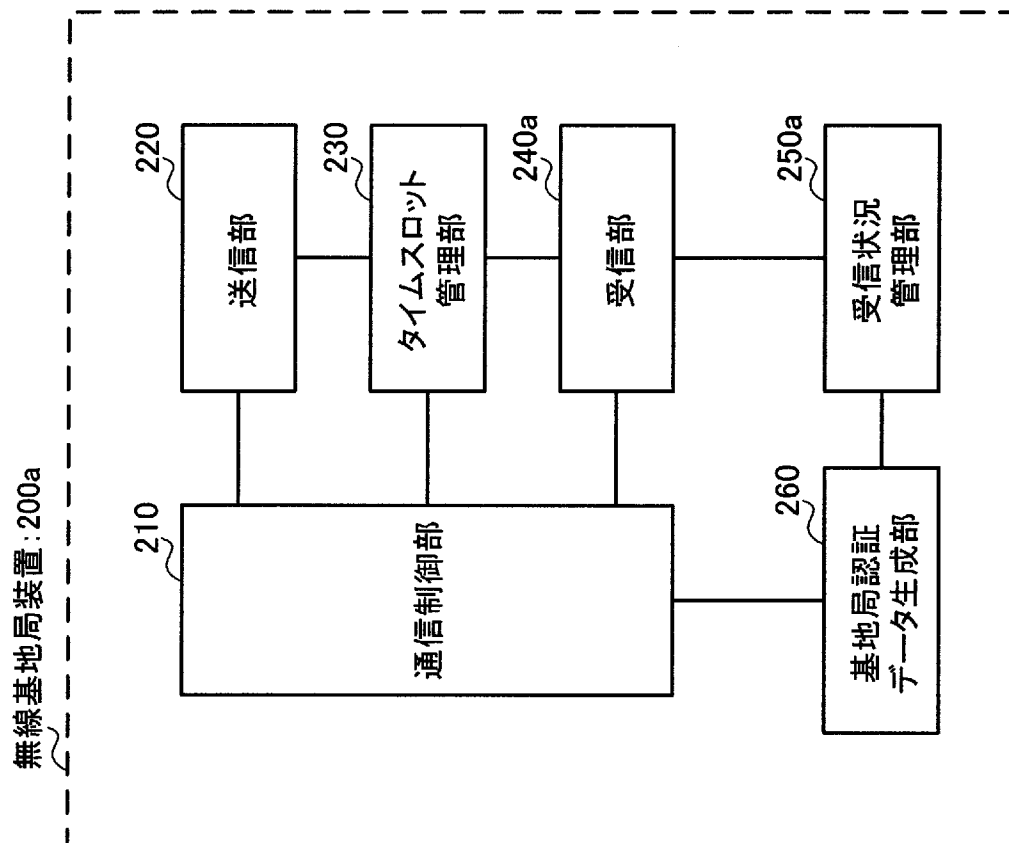
[図28]



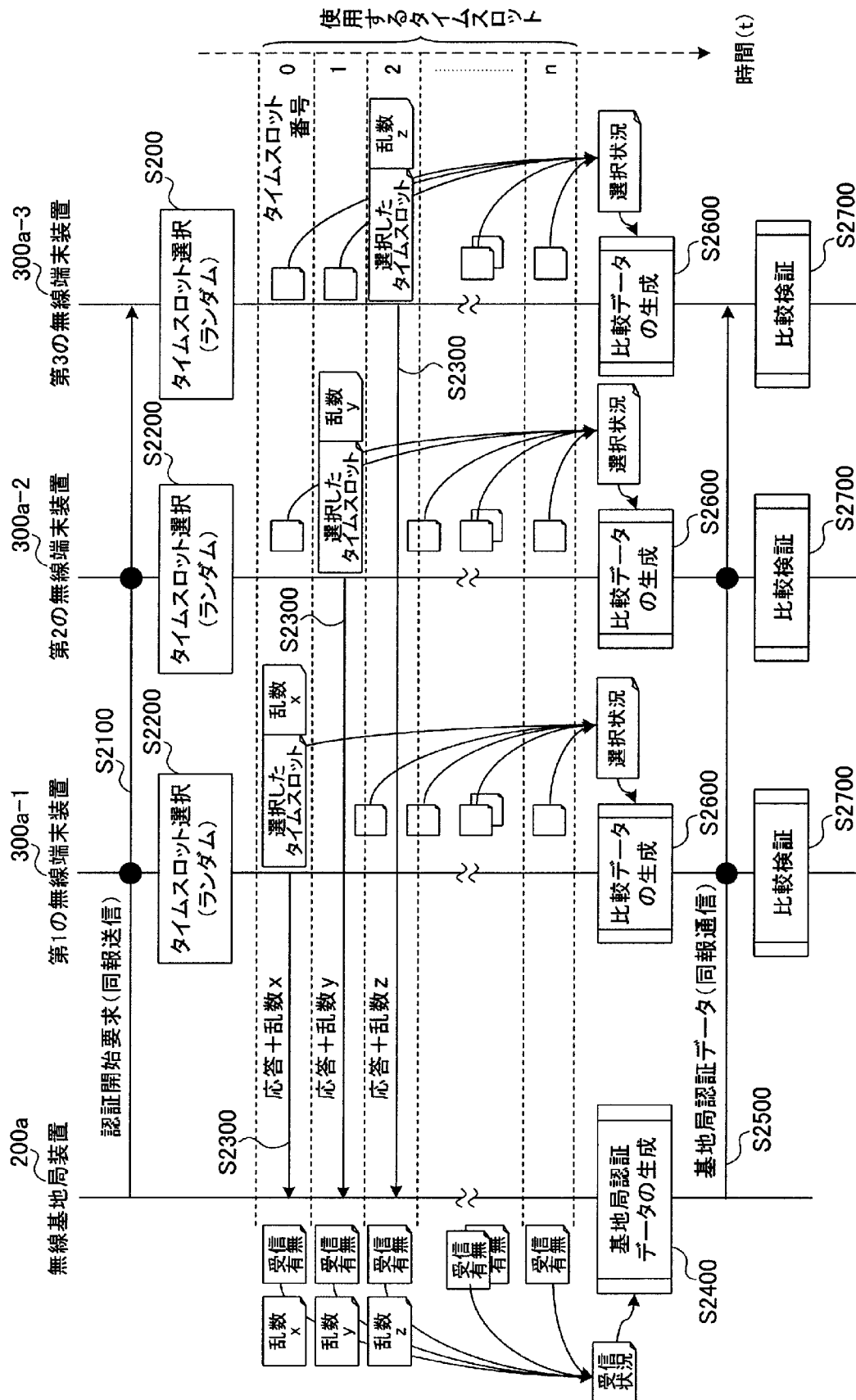
[図29]



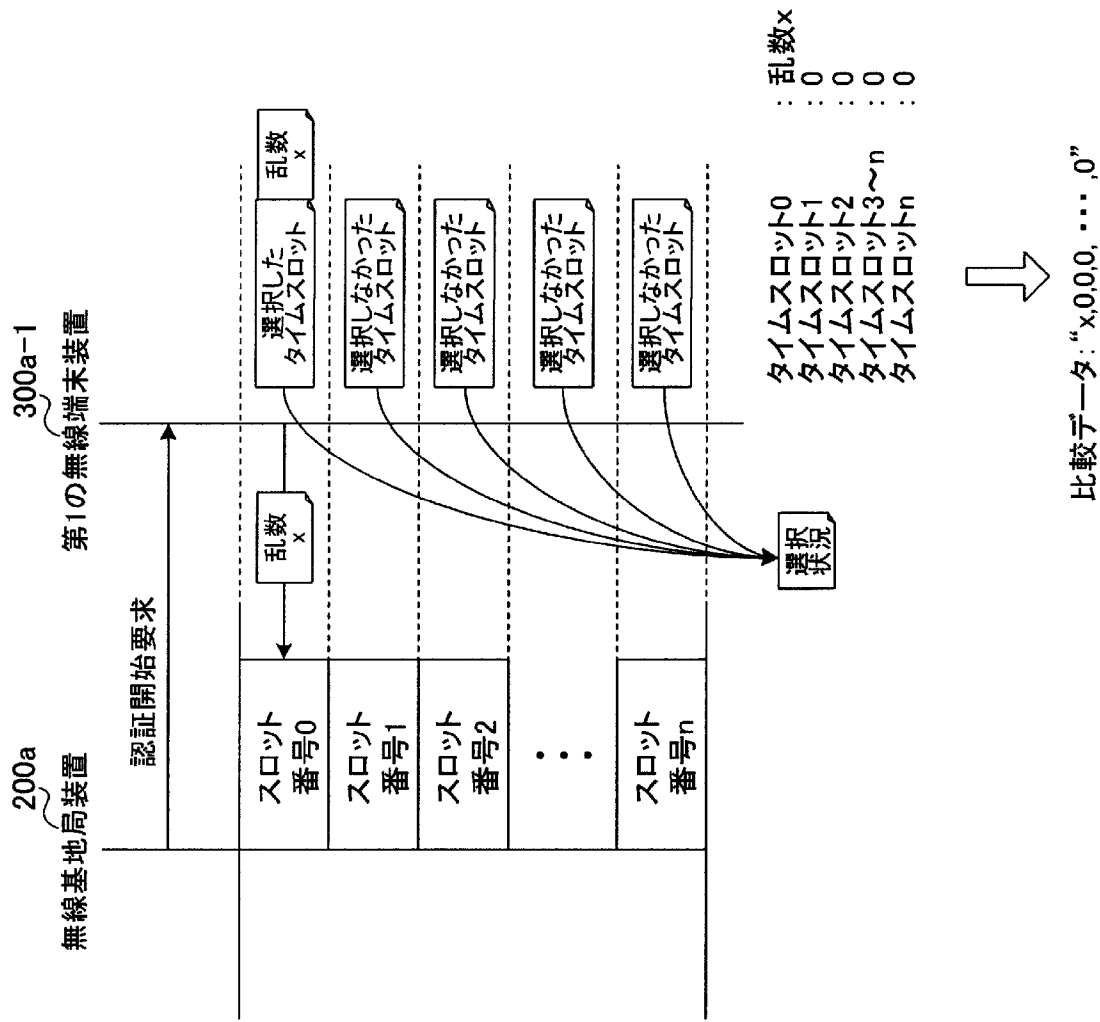
[図30]



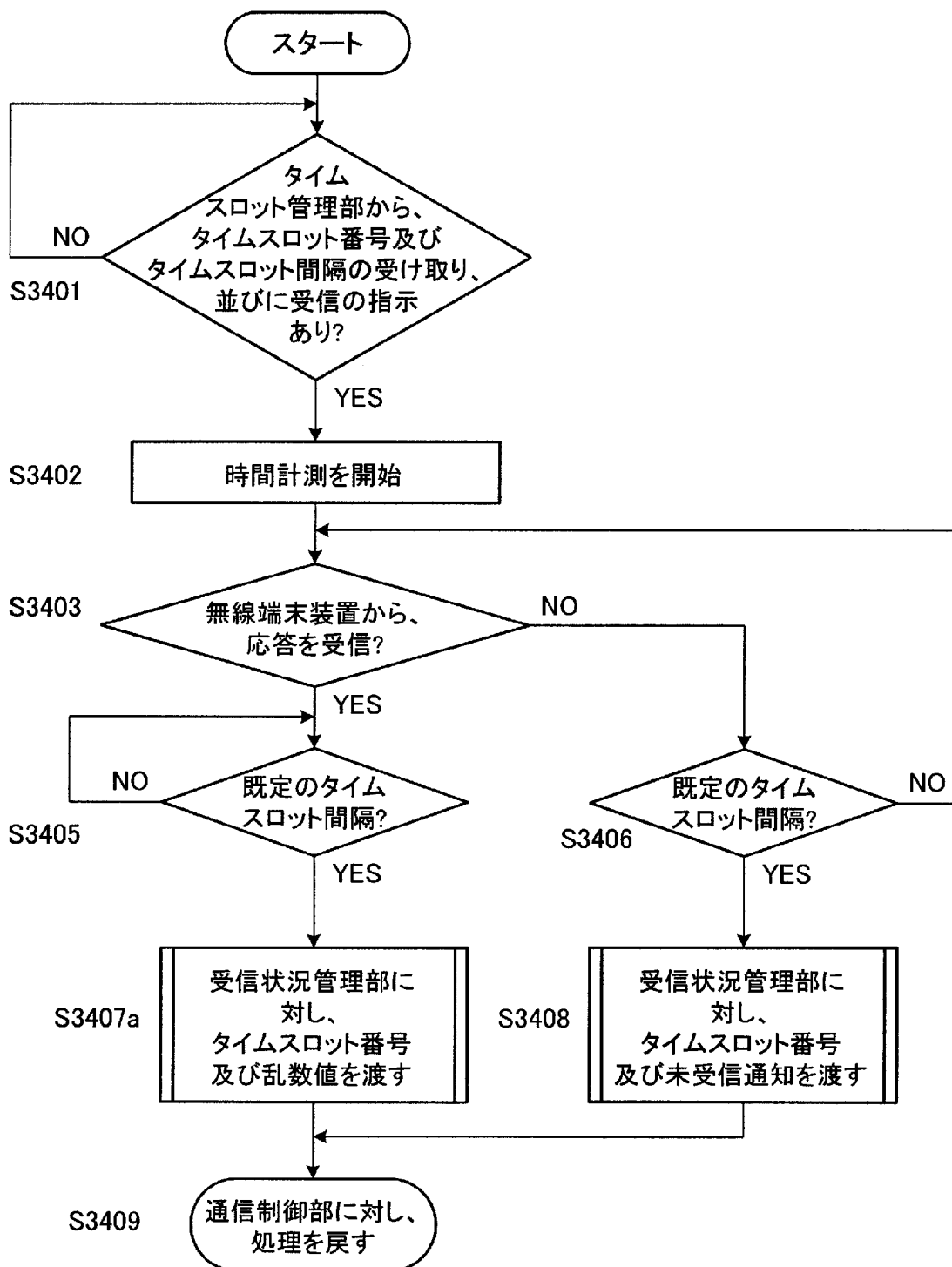
[図31]



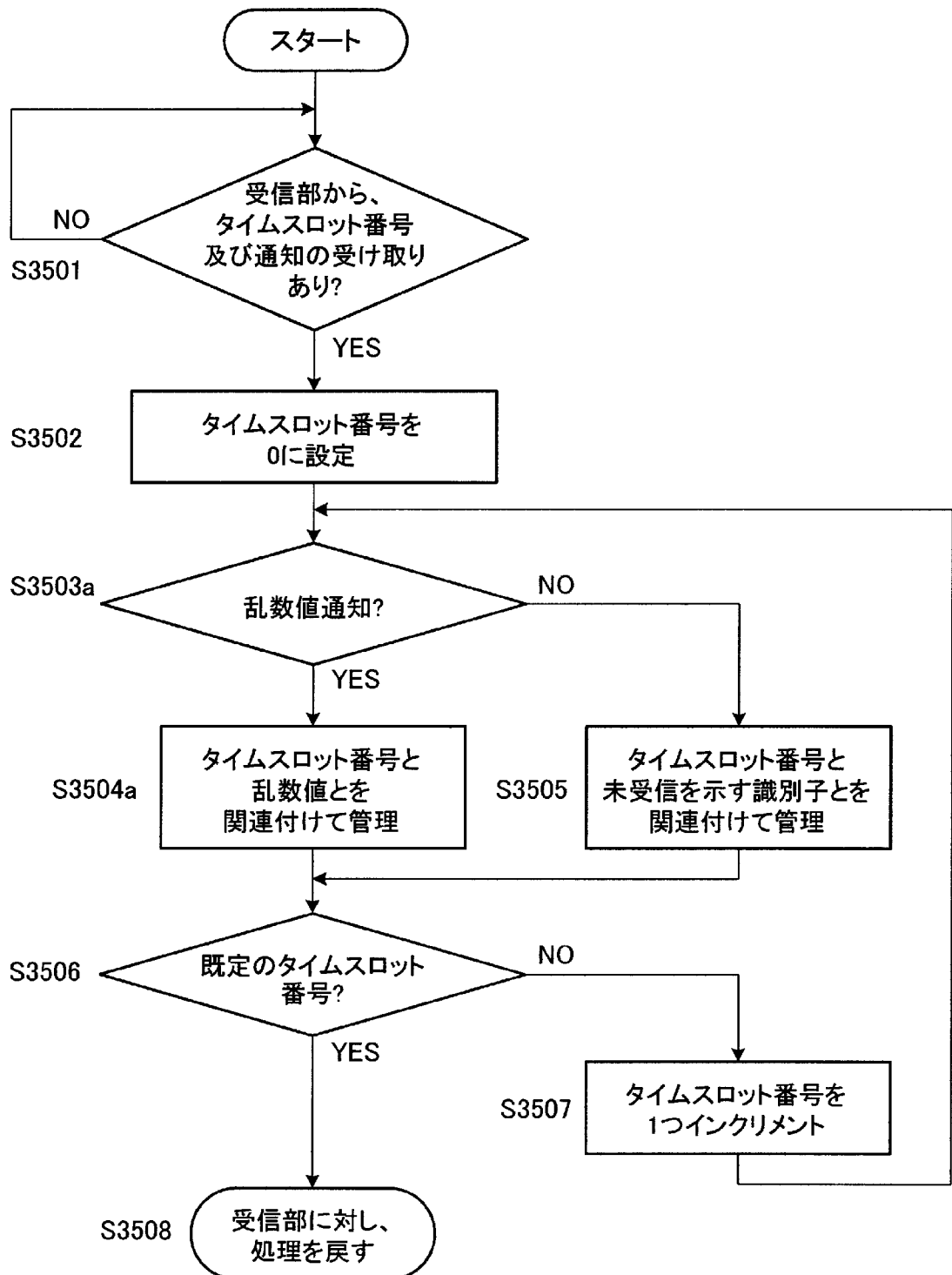
[図33]



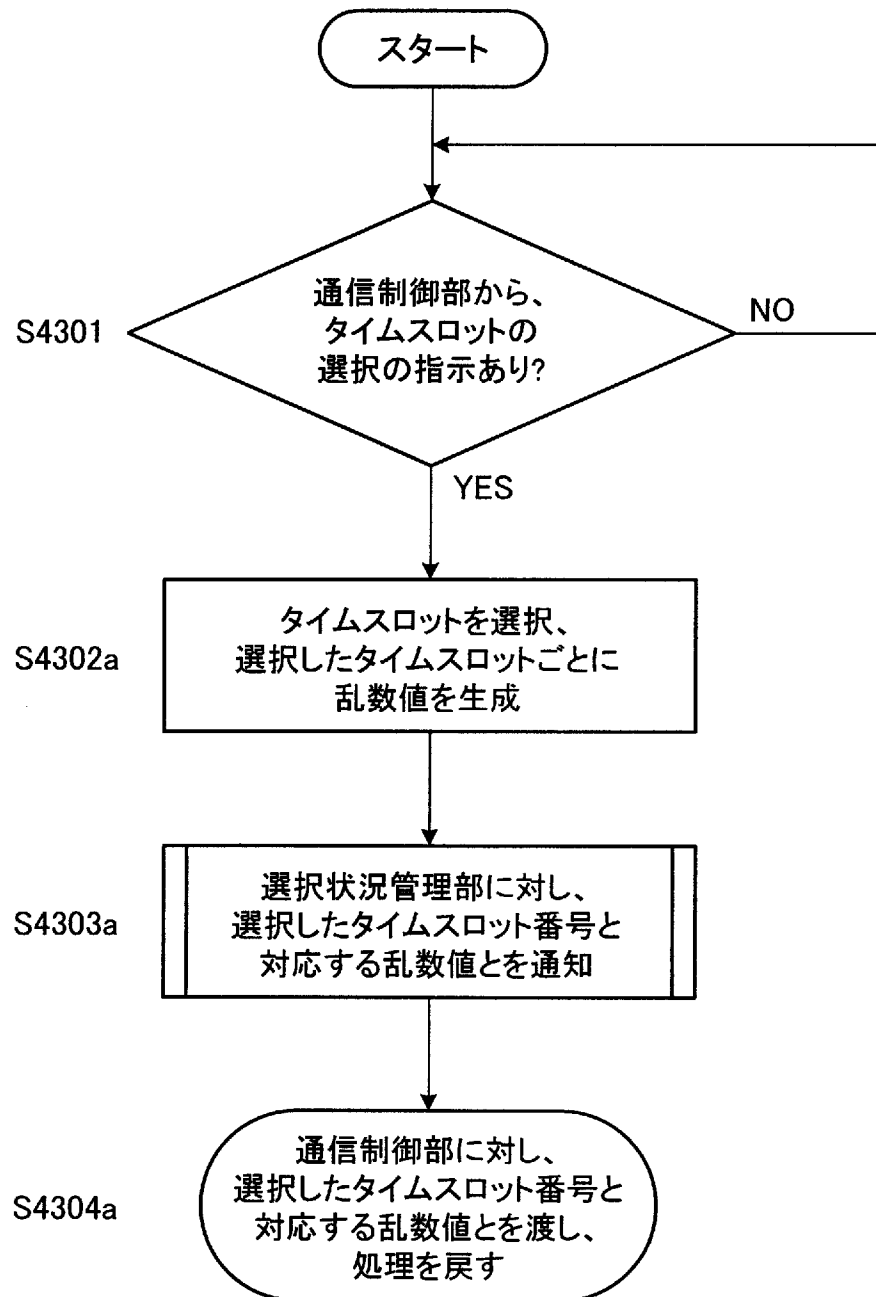
[図34]



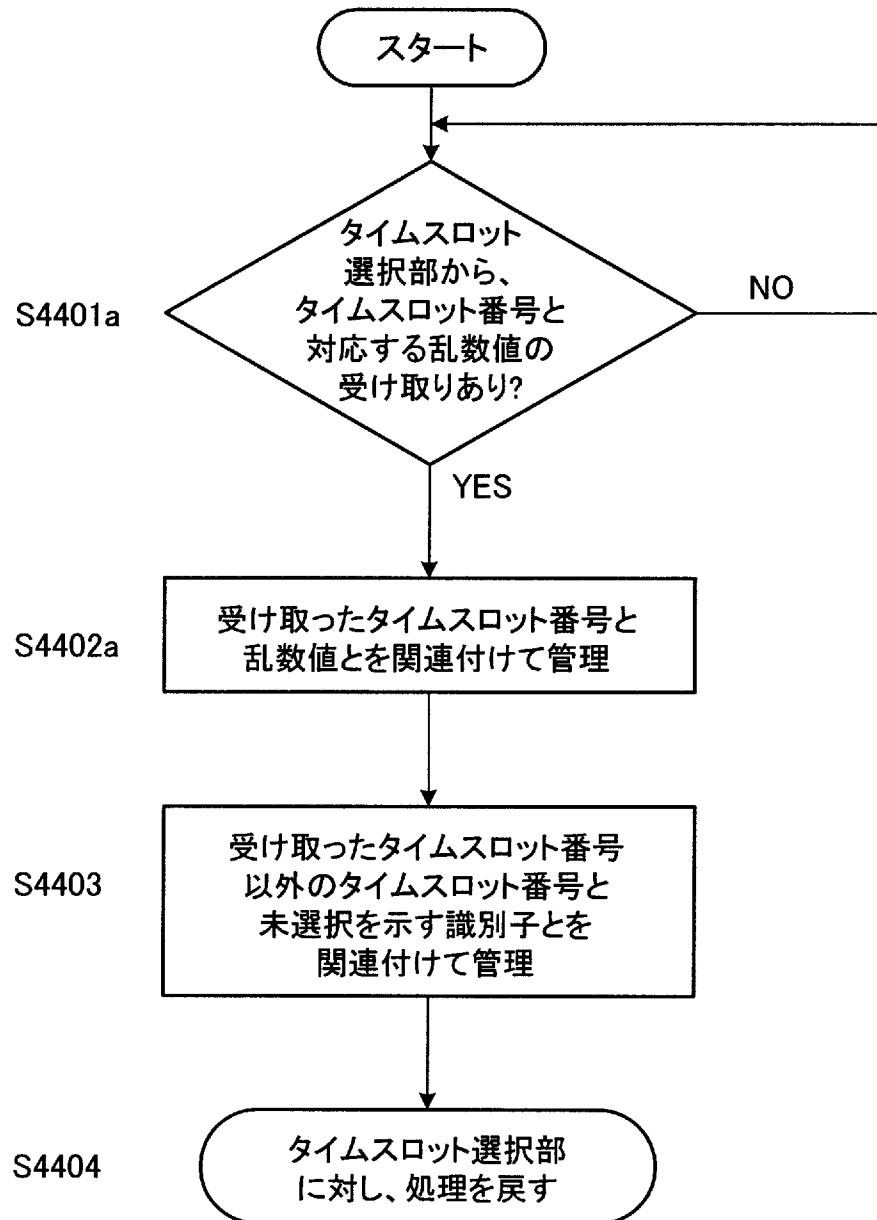
[図35]



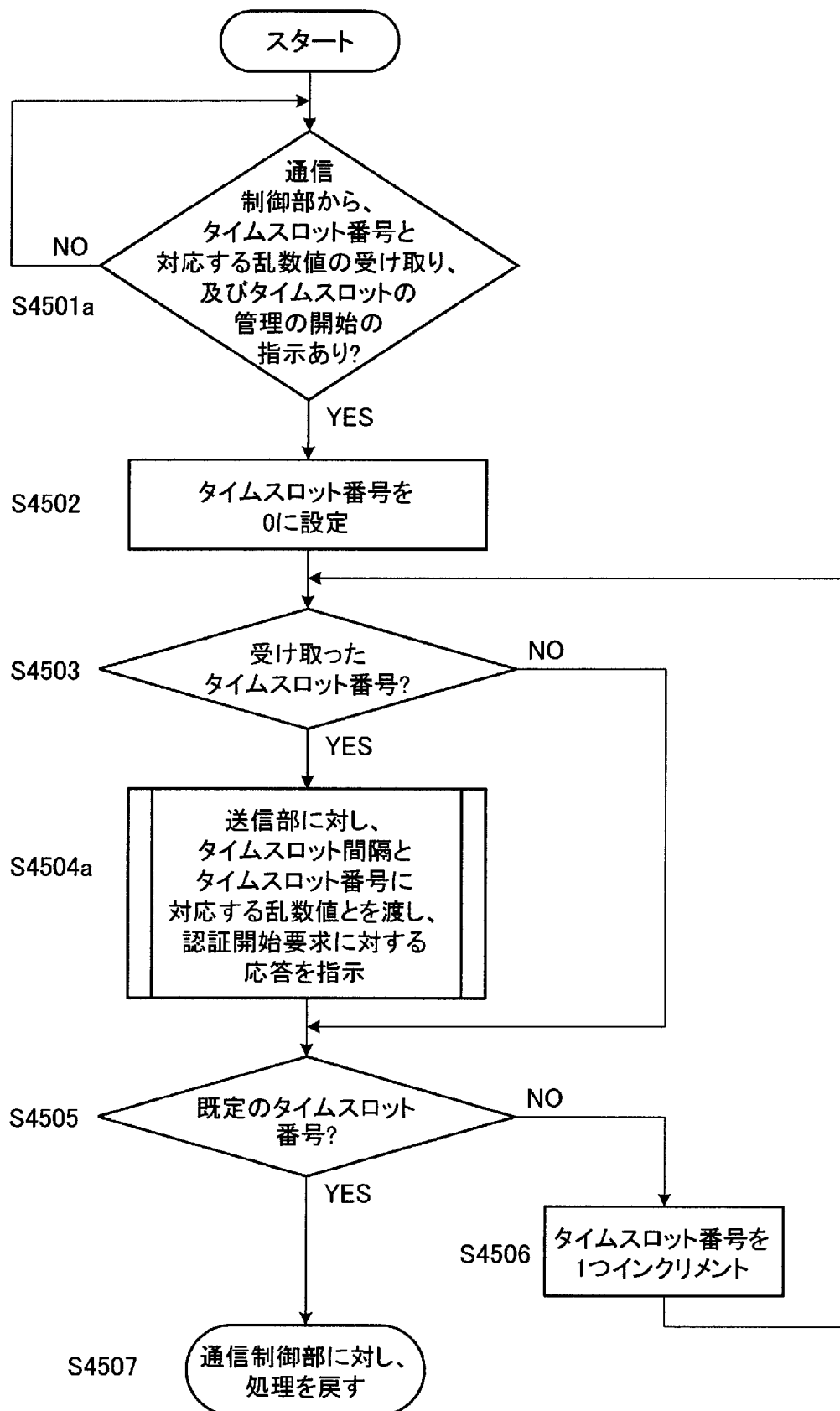
[図36]



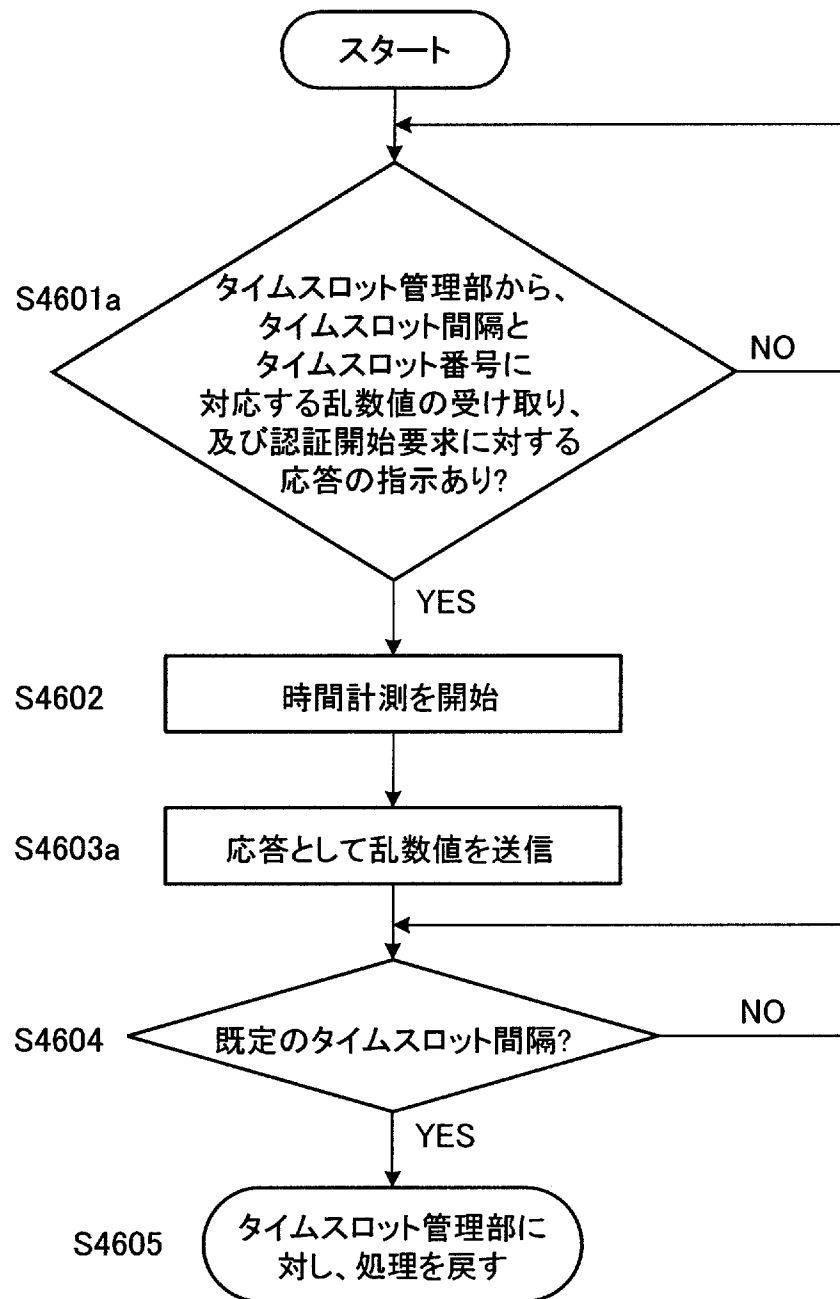
[図37]



[図38]



[図39]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/000951

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/06(2009.01)i, G06K17/00(2006.01)i, G06K19/07(2006.01)i, H04W72/04(2009.01)i, H04W84/10(2009.01)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)

H04B7/24-7/26, H04W4/00-99/00, G06K17/00, G06K19/07

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	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

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 A	JP 2000-3420 A (Toshiba Corp.), 07 January 2000 (07.01.2000), paragraphs [0087] to [0112]; fig. 1 to 3, 14, 16 (Family: none)	1-4, 7-10, 12 5, 6, 11
A	JP 2006-99343 A (Saxa, Inc.), 13 April 2006 (13.04.2006), fig. 3, 4 (Family: none)	1-12
A	JP 2009-38588 A (Panasonic Corp.), 19 February 2009 (19.02.2009), paragraph [0023]; fig. 2 & WO 2009/016818 A1	1-12



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
21 April, 2010 (21.04.10)

Date of mailing of the international search report
11 May, 2010 (11.05.10)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. H04W12/06(2009.01)i, G06K17/00(2006.01)i, G06K19/07(2006.01)i, H04W72/04(2009.01)i,
H04W84/10(2009.01)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 (I P C))

Int.Cl. H04B 7/24-7/26, H04W 4/00-99/00, G06K17/00, G06K19/07

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 0 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 0 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 0 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
X	JP 2000-3420 A (株式会社東芝) 2000.01.07, 第 87-112 段落、第 1-3, 14, 16 図 (ファミリーなし)	1-4, 7-10, 12
A		5, 6, 11
A	JP 2006-99343 A (サクサ株式会社) 2006.04.13, 第 3, 4 図 (ファミリーなし)	1-12

☒ 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

2 1 . 0 4 . 2 0 1 0

国際調査報告の発送日

1 1 . 0 5 . 2 0 1 0

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

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)

桑原 聡一

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 3 4

5 J

3 9 8 4

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 2009-38588 A (パナソニック株式会社) 2009. 02. 19, 第 23 段落、第 2 図 & WO 2009/016818 A1	1-12