

(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
2014 年 10 月 2 日(02.10.2014)



(10) 国際公開番号
WO 2014/156328 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01) G09C 1/00 (2006.01)
G06F 21/64 (2013.01)
- (21) 国際出願番号: PCT/JP2014/052904
- (22) 国際出願日: 2014 年 2 月 7 日(07.02.2014)
- (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 2013-070945 2013 年 3 月 29 日(29.03.2013) JP
- (71) 出願人: 日立オートモティブシステムズ株式会社 (HITACHI AUTOMOTIVE SYSTEMS, LTD.)
[JP/JP]; 〒3128503 茨城県ひたちなか市高場 2 5
2 0 番地 Ibaraki (JP).
- (72) 発明者: 京増 司(KYOSO Tsukasa); 〒1008280 東京
都千代田区丸の内一丁目 6 番 6 号 株式会社
日立製作所内 Tokyo (JP). 成沢 文雄(NARISAWA
Fumio); 〒1008280 東京都千代田区丸の内一丁目
6 番 6 号 株式会社日立製作所内 Tokyo (JP). 大塚
敏史(OTSUKA Satoshi); 〒1008280 東京都千代
田区丸の内一丁目 6 番 6 号 株式会社日立製作
所内 Tokyo (JP).

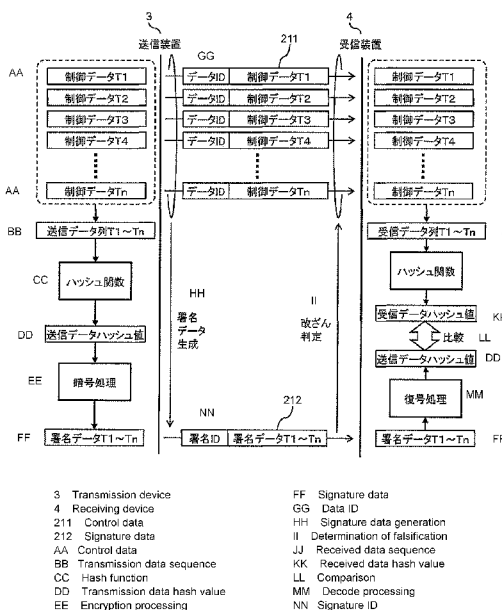
- (74) 代理人: 平木 祐輔, 外(HIRAKI Yusuke et al.); 〒
1056232 東京都港区愛宕 2 丁目 5 番 1 号 愛宕
グリーンヒルズMORIタワー 3 2 階 Tokyo
(JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保
護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA,
BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN,
CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES,
FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN,
IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS,
LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX,
MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH,
PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK,
SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保
護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW,
MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシ
ア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ
(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR,
GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT,
NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML,
MR, NE, SN, TD, TG).

[続葉有]

(54) Title: CAR ONBOARD COMMUNICATION SYSTEM AND COMMUNICATION DEVICE

(54) 発明の名称: 車載通信システム及び通信装置

[図2]



(57) Abstract: The present invention enables effective detection of fraud without requiring alteration of the format of a communication frame. A communication system for performing communication of packet communication data comprises: a transmission device provided with a transmission data generation unit for generating a plurality of transmission data packets, and a signature data generation unit for generating a signature data packet including authentication data in which verification information for a transmitted plurality of transmission data packets is encrypted, the transmission device further having a transmission means for transmitting the transmission data packets and the signature data packet; and a receiving means having a verification unit for generating verification information with regard to a received plurality of transmission data packets, and comparing the generated information with verification information obtained from the authentication data included in the received signature data packet to verify the validity of the received data.

(57) 要約: 本発明は、通信フレームの形式の変更を必要とせずに、効果的に不正の検出を可能とする。パケット通信データの通信を行う通信システムは、複数の送信データパケットを生成する送信データ生成部と、送信した複数の送信データパケットの検証情報を暗号化した認証データを含む署名データパケットを生成する署名データ生成部とを備え、送信データパケットと署名データパケットを送信する送信手段とを有する送信装置と、受信した複数の送信データパケットについて検証情報を生成し、受信した署名データパケットに含まれる認証データから求めた検証情報と比較して受信データの正当性を検証する検証部を有する受信手段からなる。

WO 2014/156328 A1



添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：車載通信システム及び通信装置

技術分野

[0001] 本発明は、電子署名を利用した通信システム及び通信装置に関する。

背景技術

[0002] 本技術分野の背景技術として、特開平 10-13403（特許文献 1）がある。この広報では、ネットワーク間で扱われる情報データに改ざんがないかどうかを検証するデータ管理システムを提供することを課題として、送信装置と受信装置に共通の暗号化手段を備えさせ、送信装置は情報データに上記暗号化手段により該情報データを暗号化した署名データを付加して送信し、受信装置は受信した情報データを暗号化手段により暗号化した署名データと、受信した上記署名データを比較することにより、上記情報データの検証を行う、と記載されている。

[0003] また、特開 2011-229075（特許文献 2）がある。この広報では、特許文献 1 で記載されている電子署名による通信データの正当性検証を自動車通信システムに適用する際に、署名データを付加することによる通信データのスループットの低下を抑制可能な通信システムを提供することを課題とし、送信側となる車載装置は、M 回分の通信データからなる単位データごとに、署名データを生成すると共に、その署名データを M 分割した分割署名データから生成した付加データを、通信データに付加して順次送信する、ことを特徴としており、通信データを検証するために各通信フレームに付加するデータのデータ量を少なく抑えることができる。

先行技術文献

特許文献

[0004] 特許文献 1：特開平 10-13403 号公報

特許文献 2：特開 2011-229075 号公報

発明の概要

発明が解決しようとする課題

- [0005] 本発明は、車載ネットワークなどのシステムにおいて、不正なデータを侵入させて誤動作させる攻撃に対して、送信装置によるデータの署名を利用し不正を検知、又は防御することが考えられる。
- [0006] しかし、特許文献 1 に記載の技術では、署名データを保護する対象の情報データに付加して送信するため、署名データを利用しない場合に通信装置間で送受信されるデータの形式と異なり、データ形式の互換性に劣る。
- [0007] また特許文献 2 に記載の技術では、各通信フレームに対して署名データを付加しており、署名データを利用しない場合に比べ、通信フレームの形式が異なるため、やはりフレーム形式の互換性に劣る。
- [0008] 本発明は、通信フレームの形式の変更を必要とせずに、効果的に不正の検出を可能とする。

課題を解決するための手段

- [0009] 上記課題を解決するために、パケット通信データの通信を行う通信システムは、複数の送信データパケットを生成する送信データ生成部と、送信した複数の送信データパケットの検証情報を暗号化した署名データを含む署名データパケットを生成する署名データ生成部とを備え、送信データパケットと署名データパケットを送信する送信手段とを有する送信装置と、受信した複数の送信データパケットについて検証情報を生成し、受信した署名データパケットに含まれる署名データから求めた検証情報と比較して受信データの正当性を検証する検証部を有する受信手段から構成される。

発明の効果

- [0010] 本発明によれば、なりすまし攻撃のようなネットワーク上で不正な攻撃が発生した場合に、検知して通知、又はフェールセーフ、不正転送防止、データの破棄、状態の記録、ユーザー又は他システムへの警告通知、等の各種対応する動作を行い不正に対処することが可能となる。
- [0011] また不正検知時の誤検知低減、データ確認時の負荷低減、についても可能になる。

図面の簡単な説明

[0012] [図1]ネットワークシステムの例である。

[図2]通信装置間で送受信されるパケット通信データによる署名データの生成と改ざん検出の手順を示す例である。

[図3]改ざんの有無の判定するフローチャートの例である。

[図4]送信データ生成部の構成を示す図。

[図5]送信データ署名付与部の構成を示す図。

[図6]署名付与対象送信データ識別子データを示す図。

[図7]送信データ判定部の処理を示すフローチャート。

[図8]署名データ生成部の構成を示す図。

[図9]受信データ検証部の構成を示す図。

[図10]受信データ判定部の処理を示すフローチャート。

[図11]改ざん判定部の構成を示す図。

[図12]改ざん判定部の処理を示すフローチャート。

[図13]改ざん判定部の処理を示すフローチャート。

[図14]他の実施例におけるネットワークシステムの構成を示す図。

[図15]他の実施例におけるネットワークシステムの構成を示す図。

[図16]他の実施例における通信装置間で送受信されるパケット通信データの構成を示す図。

発明を実施するための形態

[0013] 以下、本発明に好適な実施形態の例を図面を用いて説明する。ただし、本実施例は、主には車載ネットワークなどの周期的なデータ送受信を行うネットワークにおける装置及びシステムの動作を例にして説明しており、車載ネットワーク装置及び車載ネットワークにおけるデータ送受信システムの実施に好適であるが、ネットワーク装置及びデータ送受信システム以外への適用を妨げるものではない。

実施例 1

[0014] 図1は、本発明による車載通信システム1の構成の一例を示す図である。

送信装置 3 と受信装置 4 の間のパケット通信データの送受信は、本発明による送信データ署名付与部 3 2 による署名データパケットにより、受信データ検証部 4 2 によって不正を検出することが出来る。一方、受信装置 5 は、受信データ検証部 4 2 を備えておらず、本発明による署名データパケットに対応していない従来の ECU であるが、改ざんを検出できない一方で、パケット通信データは、受信して処理することができる。即ち、本発明が適用された装置と、適用されていない装置を同一の車載通信システムに混在させることができる。

[0015] 図 2 は、送信装置 3 から送信され、通信バス 2 を介して受信装置 4 に転送されるパケット通信データの構成の一例を示す図である。送信装置 3 は、受信装置 4 における制御で使用する制御データを含む、送信データパケット 2 1 1 を周期的に送信し、さらに N 個の送信データパケット 2 1 1 に対して 1 つの割合で、制御データからハッシュ値を求めて署名データを生成し、署名データパケット 2 1 2 を送信する。また、受信装置 4 は、受信した署名データのハッシュ値によりよりそれ以前に受信していた N 個の制御データの改ざんを検出する。

[0016] 図 3 は、車載通信システム 1 における、パケット通信データへの改ざんを検出する手順を示すフローチャートである。受信装置 4 の受信データ検証部 4 2 では、ステップ S 1 1 1 1 で制御データを受信する間、ステップ S 1 1 1 1 2 にて予め設定されている数（この例の場合 n 個）の受信した制御データからハッシュ値を算出する。ステップ S 1 1 1 3 で、署名データパケットにより署名データを受信したら、ステップ S 1 1 1 4 にて署名データを復号処理しハッシュ値を抽出する。ステップ S 1 1 1 5 で両者のハッシュ値を比較し、一致すれば改ざんは行われていないものとし（S 1 1 1 6）、一致しなければ制御データに改ざんが行われていると判定する（S 1 1 1 7）。

[0017] 図 4 は、送信装置 3 の送信データ生成部 3 1 の構成を示す図である。データ算出部 3 1 1 は、受信装置 4 の側における制御に必要なデータを算出し、送信データパケット生成部 3 1 2 は、算出したデータの種別に応じた送信デ

ータ識別子 3 1 3 を付加し、送信データパケット 2 1 1 を生成し、送信データ署名付与部 3 2 を介して生成した送信データパケット 2 1 1 を通信部 3 3 に送る。

[0018] 図 5 は、送信装置 3 の送信データ署名付与部 3 2 の構成を示す図である。送信データ判定部 3 2 2 では、送信データパケット 2 1 1 に含まれる送信データ識別子 3 1 3 と、署名付与対象送信データ識別子データ 3 2 1 を参照して、送信データパケット 2 1 1 を、通信部 3 3 と署名データ生成部 3 2 3 に振り分ける。署名データ生成部 3 2 3 は、所定個数の振り分けられてきた送信データパケット 2 1 1 から署名データパケット 2 1 2 を生成し、通信部 3 3 を介して送信する。

[0019] 図 6 は、署名付与対象データ識別子データ 3 2 1 に含まれるデータの例を示す図である。送信データ識別子に対応付けられた署名データ識別子が格納されている。

[0020] 図 7 は、送信データ判定部 3 2 2 の処理を示すフローチャートである。ステップ S 3 2 2 2 にて送信データ生成部 3 1 から送信データパケット 2 1 1 が入力される。ステップ S 3 2 3 では、署名付与対象データ識別子データ 3 2 1 を参照して、送信データパケット 2 1 1 の識別子が署名を付与する対象かどうかを調べる。対象であると判定された場合、ステップ S 3 2 2 4 に進み、署名付与対象データ識別子データ 3 2 1 に格納されている対応する署名データ識別子と送信データパケット 2 1 1 を署名データ生成部 3 2 3 に入力する。そしてステップ S 3 2 2 5 で、送信データパケットを通信部 3 3 へ入力する。またステップ S 3 2 2 3 で、対象データで無いと判定された場合、ステップ S 3 2 2 5 を実行する。

[0021] 図 8 は、署名データ生成部 3 2 3 の構成を示す図である。送信済みデータ記憶部 3 2 3 1 には、送信データ判定部 3 2 2 から送信データパケット 2 1 1 と署名データ識別子 3 2 1 3 が入力され、署名データ識別子 3 2 1 3 の種類ごとに送信データパケット 2 1 1 に含まれる制御データを、すでに送信済みの制御データを連結した送信データ列に連結し、記憶する。ハッシュ値生

成部は 3 2 3 2、送信済みデータ記憶部 3 2 3 1 に記憶されている送信データ列からハッシュ値を生成する。暗号処理部 3 2 3 3 は、予め定められている暗号化手順によりハッシュ値を暗号化し署名データを生成する。署名パケット生成部 3 2 3 4 は、署名データに署名データ識別子 3 2 1 3 を付加し、署名データパケット 2 1 2 を生成する。

[0022] 図 9 は、受信装置 4 の受信データ検証部 4 2 の構成を示す図である。受信データ判定部 4 2 3 は、署名付与対象受信データ識別子データ 4 2 1 と署名データ識別子データ 4 2 2 を参照し、通信部 4 3 から入力される受信データパケット 2 1 4 を、制御部 4 1 と改ざん判定部 4 2 4 に振り分ける。改ざん判定部 4 2 4 は、受信データパケット 2 1 4 と署名データパケット 2 1 2 を入力され、改ざんを検出した場合に制御部 4 1 に通知する。

[0023] 図 10 は、受信データ判定部 4 2 3 の処理を示すフローチャートである。ステップ S 4 2 3 2 で受信したパケットを、ステップ S 4 2 3 3 でまず署名データであるかどうかを調べる。署名データである場合は、ステップ S 4 2 3 5 で受信データパケットを改ざん判定部 4 2 4 に入力し、ステップ S 4 2 3 8 でそのまま終了する。ステップ S 4 2 3 3 の判定で、署名データで無いと判定された場合は、ステップ S 4 2 3 4 に進み、署名付与される対象であるかどうか調べる。対象データである場合は、ステップ S 4 2 3 6 で、受信データパケットと署名付与対象受信データ識別子データ 4 2 1 に格納されている対応する署名データ識別子を、改ざん判定部 4 2 4 に入力する。ステップ S 4 2 3 4 で対象でなかった場合は、ステップ S 4 2 3 7 をそのまま実行し、ステップ S 4 2 3 8 で処理を終了する。

[0024] 図 11 は、改ざん判定部 4 2 4 の構成を示す図である。署名データ識別子 4 2 1 3 の種類ごとに、受信データパケット 2 1 4 に含まれる制御データを、すでに受信済みの制御データを連結した受信データ列に連結し、記憶する受信済みデータ記憶部 4 2 4 1 と、記憶した受信データ列からハッシュ値を生成するハッシュ値生成部 4 2 4 2 がある。また署名データパケット 2 1 2 を復号し、送信装置から送信されたハッシュ値を抽出する復号処理部 4 2 4

4と、両ハッシュ値を比較し改ざんの有無を検出するデータ比較部4243から構成される。

[0025] 図12は、受信済みデータ記憶部4241の処理を示すフローチャートである。ステップS42412で入力された、署名データ識別子4213の種類ごとに、ステップS42413では受信データパケット214に含まれる制御データを記憶する。

[0026] 図13は、改ざん判定部424による改ざん判定の処理を示すフローチャートである。改ざん判定処理は、ステップS42422における署名データパケットの入力をトリガに行われる。ステップS42423では、入力された署名データパケットの識別子を参照し、受信済みデータ記憶部4241に記憶されている受信データ列を読み出す。ステップS42424では、ハッシュ値生成部4242にて、読み出した受信データ列のハッシュ値を算出する。ステップS42425では、受信した署名データを復号処理部4244で復号し、送信装置3から送信されたハッシュ値を抽出する。ステップS42436では、ステップS42424とステップS42425で算出した二つのハッシュが一致するか比較を行う。一致している場合、改ざんが行われていないとし、ステップS42428でそのまま処理を終了する。またステップS42426で一致しない場合は、ステップS42427に進み、制御部41に改ざんが行われている事を通知し、ステップS42428で処理を終了する。

[0027] このように、本実施の形態によれば、改ざん検出の対象となるパケット通信データに変更を加えなくとも、別途送信する署名データを検証することで、受信したパケット通信データに改ざんが行われているかどうかを検証することができる。受信したパケット通信データと署名の整合性が取れない場合、また署名データ自体が受信できない場合は、通信システムに不正があったことが判明するため、速やかに安全処置に移行することができる。

実施例 2

[0028] 次に本発明の他の実施の形態について、これまで説明した実施例との差異

点を中心に説明する。

[0029] 図14は、本実施の形態におけるネットワークシステムの構成を示す図である。送信装置61及び受信装置5は、従来と同様のECUである。署名生成アダプタ62は、送信装置61と通信バス2の間に設けられ、送信装置61から送信されるパケット通信データを入力され、パケット通信データを通信バス2に転送すると共に、署名付与対象データに対して署名データパケットを送信する。送信データ署名付与部621の構成及び処理は、実施例1と同様である。

[0030] また署名検証アダプタ72は、受信装置5と通信バス2の間に設けられ、通信バス2から受信したパケット通信データを受信装置5に転送すると共に、署名付与対象データに対して、別途受信する署名データパケットを用いて、正当性の検証を行う。受信データ検証部721の構成及び処理は、実施例1の場合と同様である。

[0031] 本実施例の形態によれば、送信装置と受信装置に従来のECUを用いて、通信バスとの間に備え付けられるアダプタの形態で、パケット通信データの正当性を検証することができる。

実施例 3

[0032] 更に、本発明の他の実施の形態について、これまで説明した実施例との差異点を中心に説明する。

[0033] 図15は、本実施の形態におけるネットワークシステムの構成を示す図である。データ転送装置8は、情報系通信バス21から受信したパケット通信データを、制御系通信バス22へ転送すると共に、送信データ署名付与部82により、転送したパケット通信データに対応する署名データパケットを生成し制御系通信バス22へ送信する。

[0034] また転送データ検証装置9は、データ転送装置8が転送するパケット通信データと、署名データパケットを受信し、受信データ検証部92によって情報系通信バス21から転送されるデータの正当性を検証する。転送データ検証装置9は、転送されたデータの改ざんを検出した場合、制御系通信バス2

2へ改ざんを通知するパケット通信データを送信する。

[0035] 送信データ署名付与部82、及び受信データ検証部92は、実施例1における送信データ署名付与部32、及び受信データ検証部42と同様の構成で実現される。

[0036] 本実施の形態によれば、不正が生じやすい情報系通信バス21から転送されるデータに着目し、転送装置と検証装置によりデータの検証を行うことで、他の通信装置は本発明が適用されていない、従来のECUを使用することができる。

実施例 4

[0037] また、本発明の他の実施の形態についてこれまで説明した実施例との差異点を中心に説明する。

[0038] 図16は、本実施の形態における通信バスを介して送受信されるパケット通信データの構成を示す図である。ネットワーク通信においては、不正な改ざんのみならず、通信経路の不具合などにより必ずしも全てのデータの通信に成功する保証が無い。特に車載通信ネットワークでは、短い周期で繰り返しデータの送受信を行うため、一部のデータの受信に失敗しても再送信の要求を行わない。この場合、不正によらず、送信装置3が送信したデータと、受信装置4が受信したデータの間に差異が生じる。

[0039] そこで本実施の形態では、受信装置4が受信に成功した送信データパケット211についてのみ、署名データの生成を要求する署名要求パケット213を、受信装置4から送信装置3に送信する。送信装置3は、署名要求パケット213で要求されている、送信済みデータから署名データを生成し、署名データパケット212を、受信装置4へ送信する。

[0040] 本実施の形態によれば、不正によらない受信済みデータと署名データの不一致を、改ざんと誤検知することを回避し、システム処理の効率を向上させることができる。

符号の説明

[0041] 2…通信バス

3…送信装置
4, 5…受信装置
8…データ転送装置
9…転送データ検証装置
2 1 1…送信データパケット
2 1 2…署名データパケット
2 1 4…受信データパケット
3 1, 6 1 1…送信データ生成部
3 2, 6 2 1, 8 2…送信データ署名付与部
3 3, 4 3, 8 3, 8 4, 6 1 2, 6 2 2, 7 2 2, 9 3…通信部
2 1…情報系通信バス
2 2…制御系通信バス
4 1…制御部
4 2, 7 2 1, 9 2…受信データ検証部
3 1 1…データ算出部
3 1 2…送信データパケット生成部
3 1 3…送信データ識別子
3 2 1…署名付与対象送信データ識別子データ
3 2 2…送信データ判定部
3 2 3…署名データ生成部
3 2 1 3, 4 2 1 3…署名データ識別子
3 2 3 1…送信済みデータ記憶部
3 2 3 2, 4 2 4 2…ハッシュ値生成部
3 2 3 3…暗号処理部
3 2 3 4…署名パケット生成部
4 2 1…署名付与対象受信データ識別子データ
4 2 2…署名データ識別子データ
4 2 3…受信データ判定部

- 4 2 4 …改ざん判定部
- 4 2 4 1 …受信済みデータ記憶部
- 4 2 4 3 …データ比較部
- 4 2 4 4 …復号処理部
- 6 2 …署名生成アダプタ
- 7 2 …署名検証アダプタ

請求の範囲

- [請求項1] パケット通信データの通信を行う送信装置と受信装置からなる通信システムにおいて、
- 前記送信装置は、
- 少なくとも2つ以上の第1のパケット通信データを生成する送信データ生成部と、
- 送信した複数の前記第1のパケット通信データの検証情報を暗号化した認証データを含む第2のパケット通信データを生成する署名データ生成部と、
- 前記第1と第2のパケット通信データを送信する送信手段と、
- を有し、
- 前記受信手段は、
- 前記第1と第2のパケット通信データを受信する受信部と、
- 受信した前記複数の第1のパケット通信データについて検証情報を生成し、受信した前記第2のパケット通信データに含まれる認証データから求めた検証情報と比較して受信データの正当性を検証する検証部を有する
- ことを特徴とする通信システム。
- [請求項2] 請求項1に記載の通信システムにおいて、
- 前記受信装置は、受信した少なくとも2つ以上の第1のパケット通信データを指定する情報である第3のパケット通信データを前記送信装置へ送信し、
- 前記送信装置は、前記第3のパケット通信データを受信した後、当該第3のパケット通信データで指定されている少なくとも2つ以上の第1のパケット通信データの検証情報を暗号化した認証データを含む第2のパケット通信データを生成して送信すること、
- を特徴とする通信システム。
- [請求項3] 請求項2に記載の通信システムにおいて、

前記第 1 及び第 2 及び第 3 パケット通信データは、パケット通信データの種類を特定するパケット識別子と、伝送対象のデータを配置したデータ領域を含むこと、
を特徴とする通信システム。

[請求項 4]

請求項 1 に記載の通信システムにおいて、

前記第 1 のパケット通信データは、データ領域に含んでいるデータに応じて、パケット識別子を持つこと、を特徴とする通信システム。

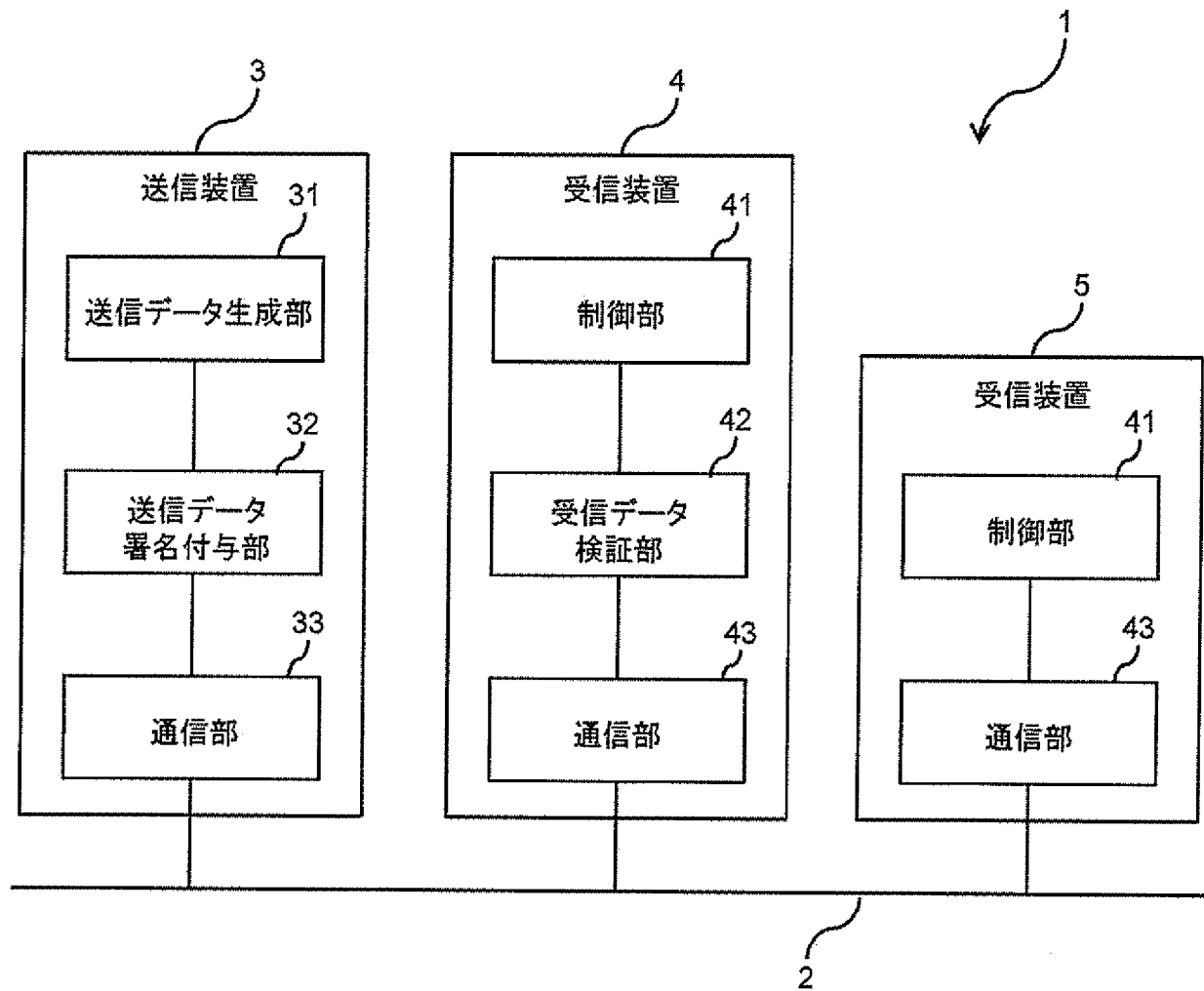
[請求項 5]

請求項 1 に記載の通信システムにおいて、

前記第 2 のパケット通信データは、検証対象とする第 1 のパケット通信データに対応するパケット識別子を持つこと、を特徴とする通信システム。

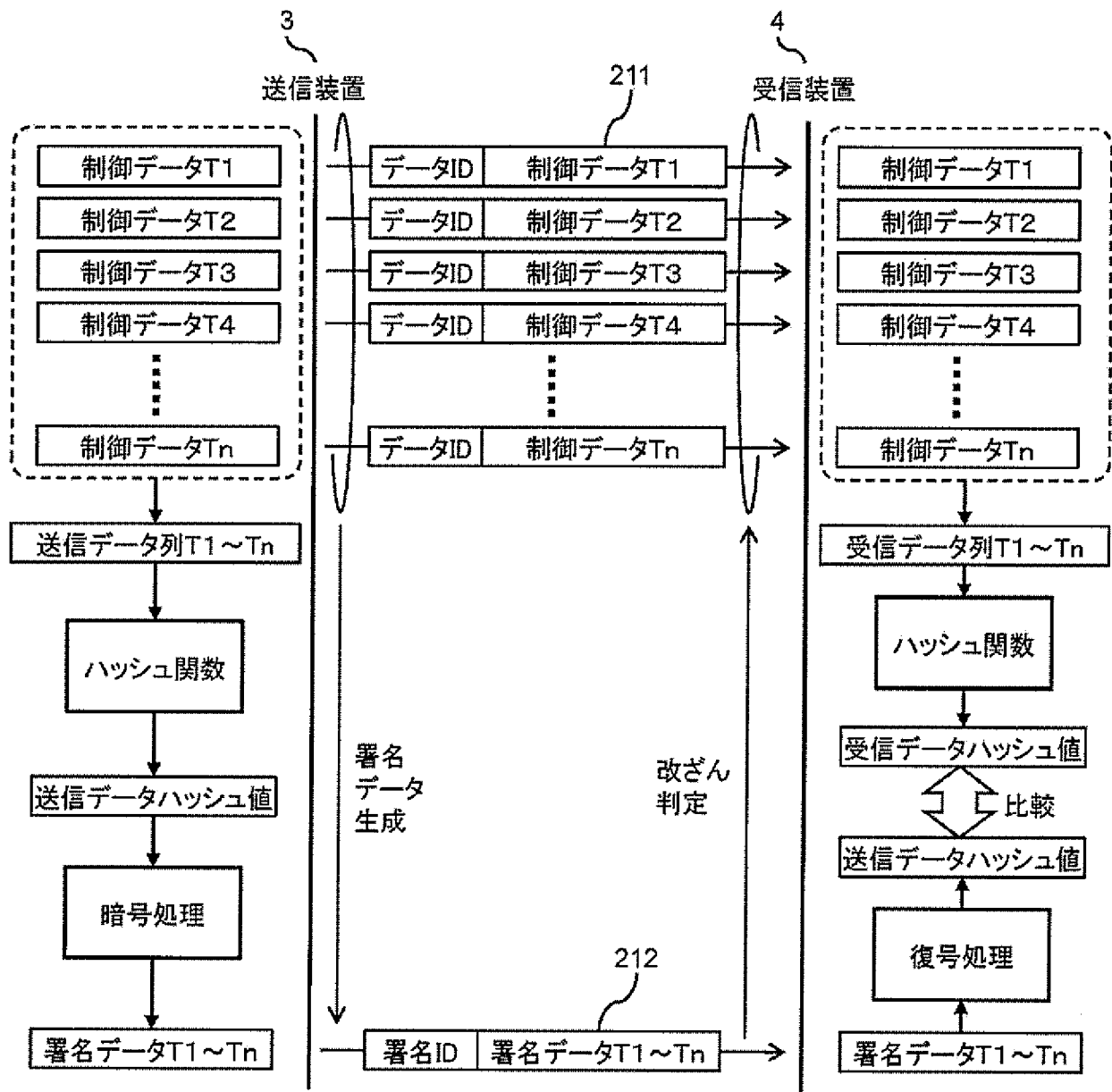
[図1]

図 1



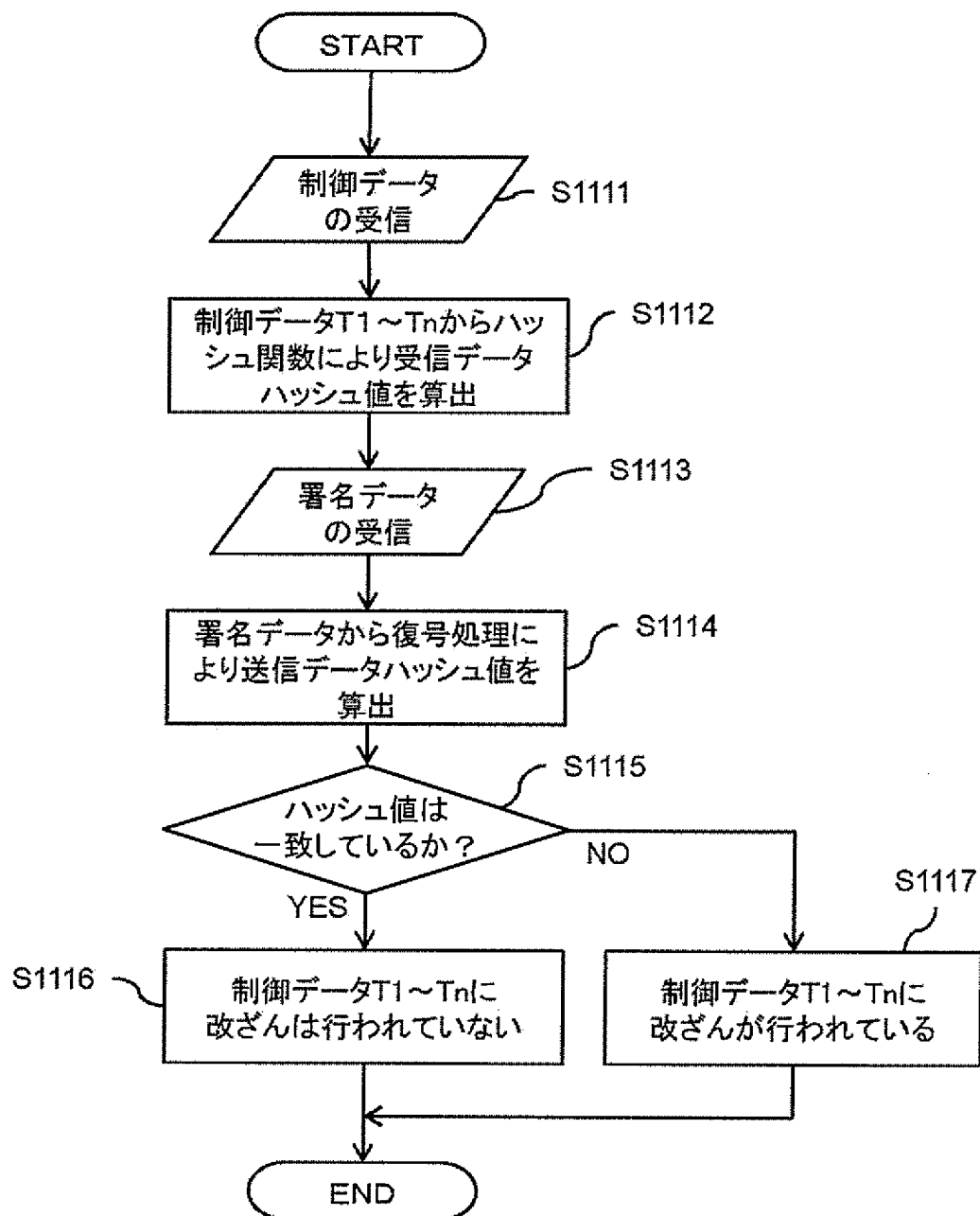
[図2]

図 2



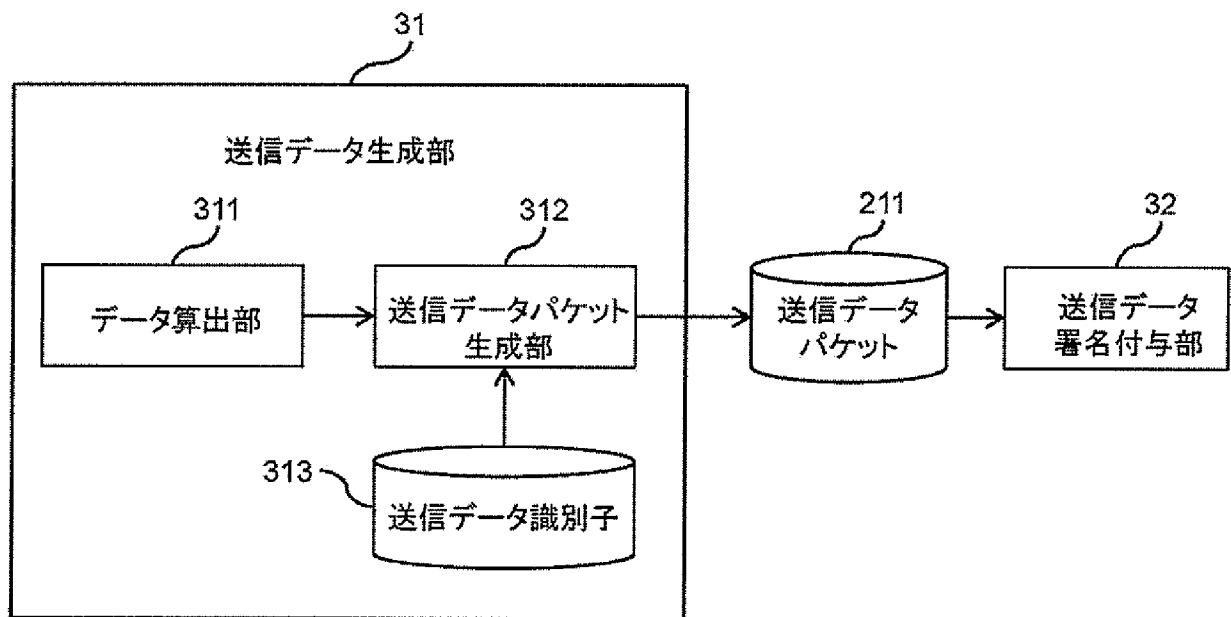
[図3]

図 3



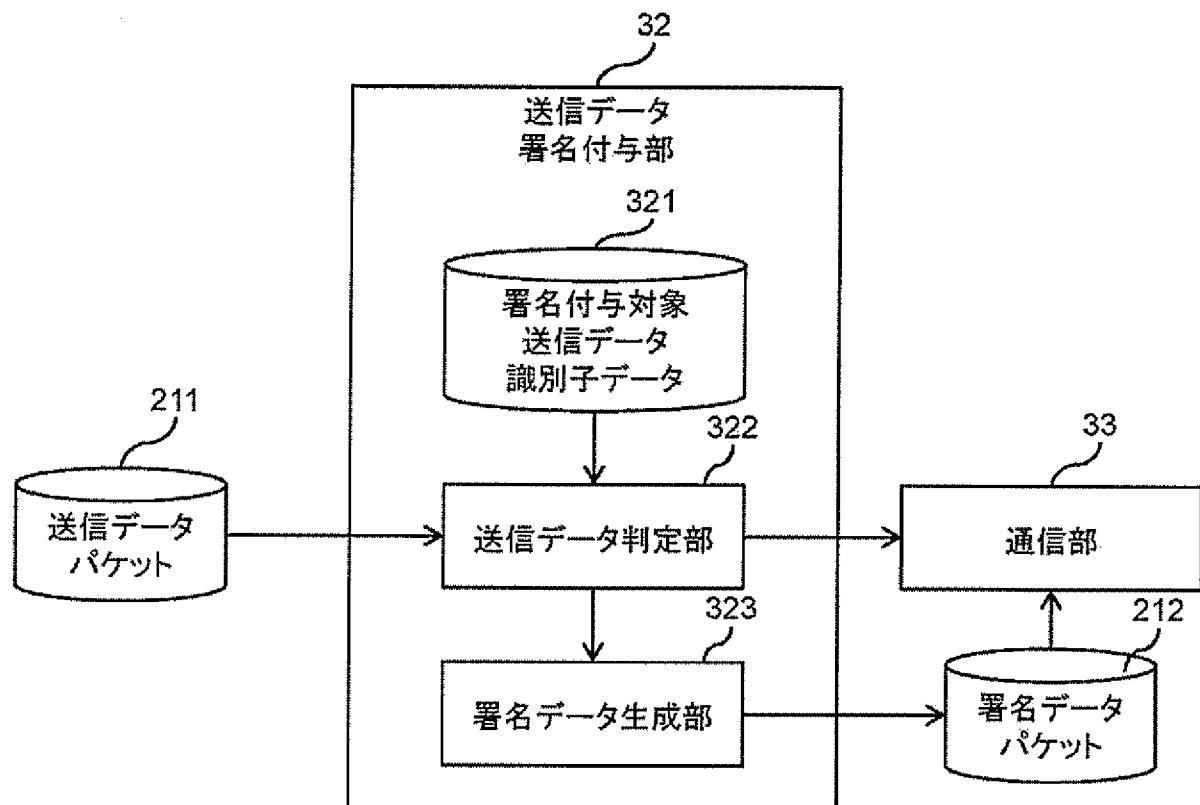
[図4]

図 4



[図5]

図 5



[図6]

図 6

Diagram illustrating a table structure with two columns and multiple rows. The table is labeled with reference numerals 3211, 3212, and 3213.

3211 points to the entire table structure.

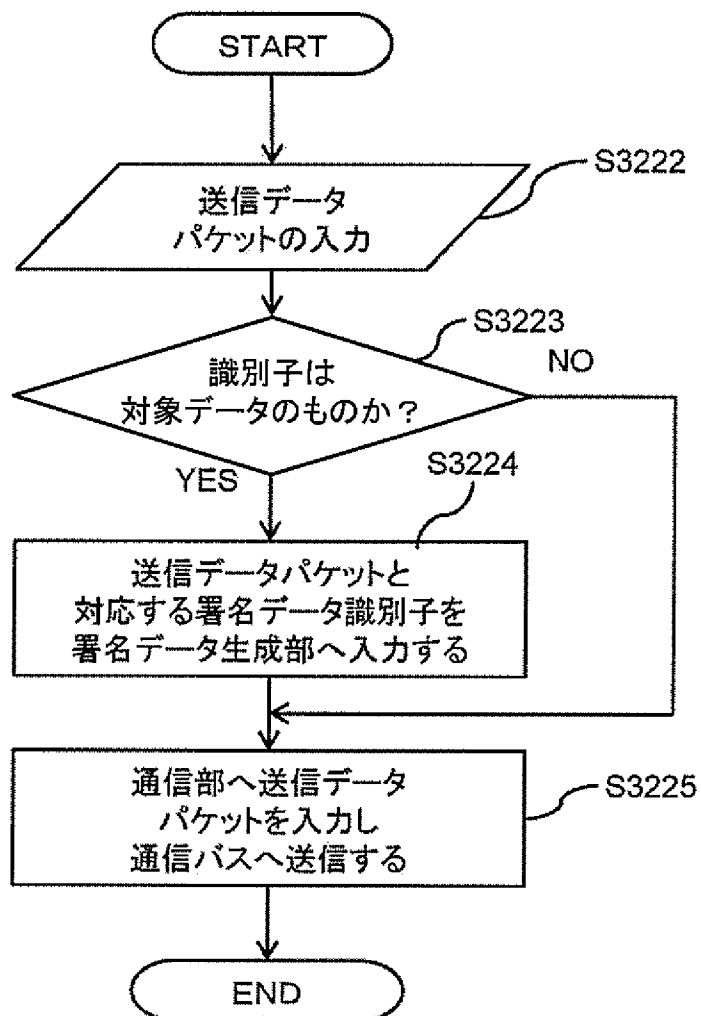
3212 points to the first column header, "送信データ識別子" (Transmitted Data Identifier).

3213 points to the second column header, "署名データ識別子" (Signature Data Identifier).

送信データ識別子	署名データ識別子
#0001	#1001
#0002	#1002
#0005	#2001
#0006	#2001
#0123	#1030

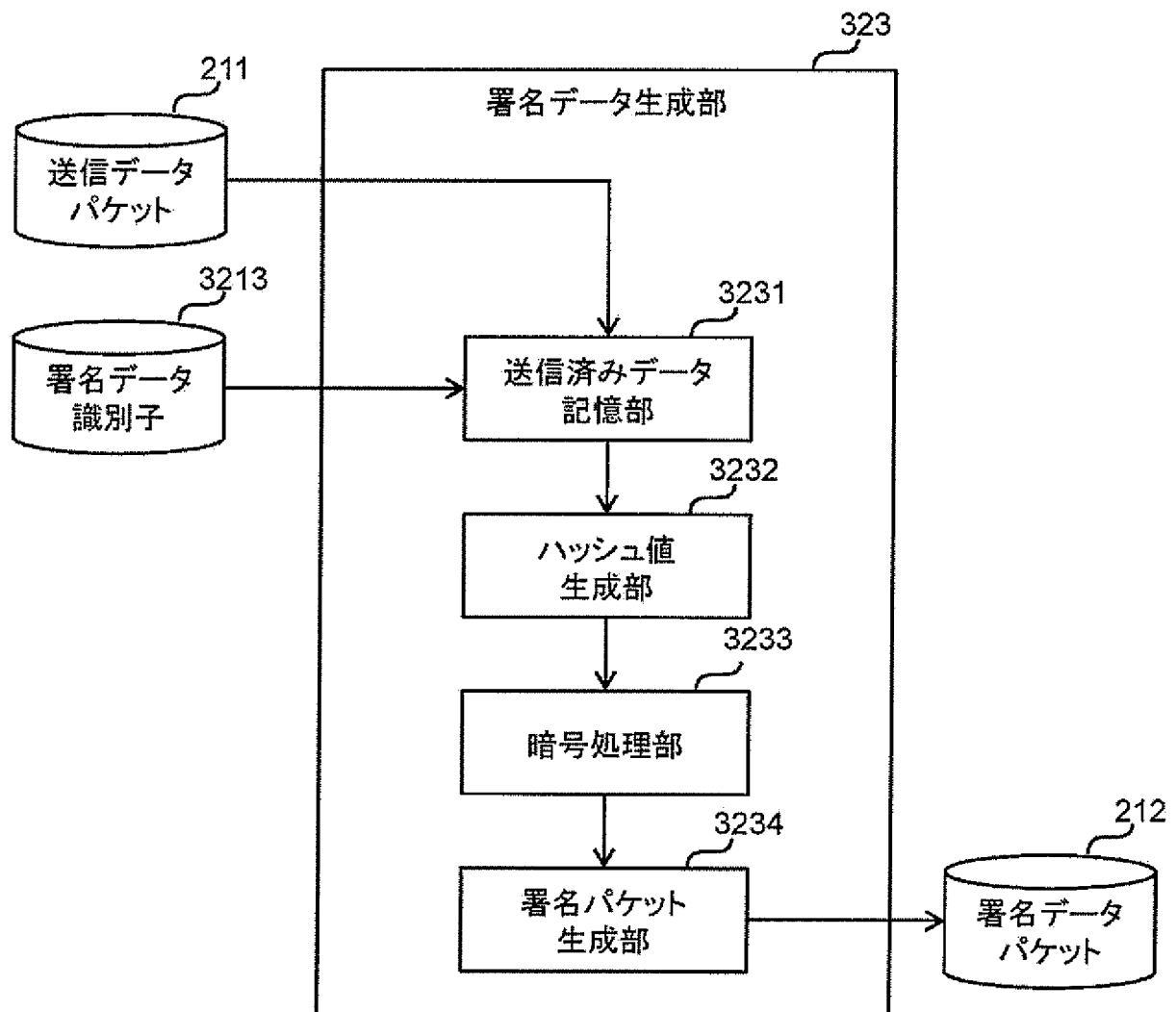
[図7]

図 7



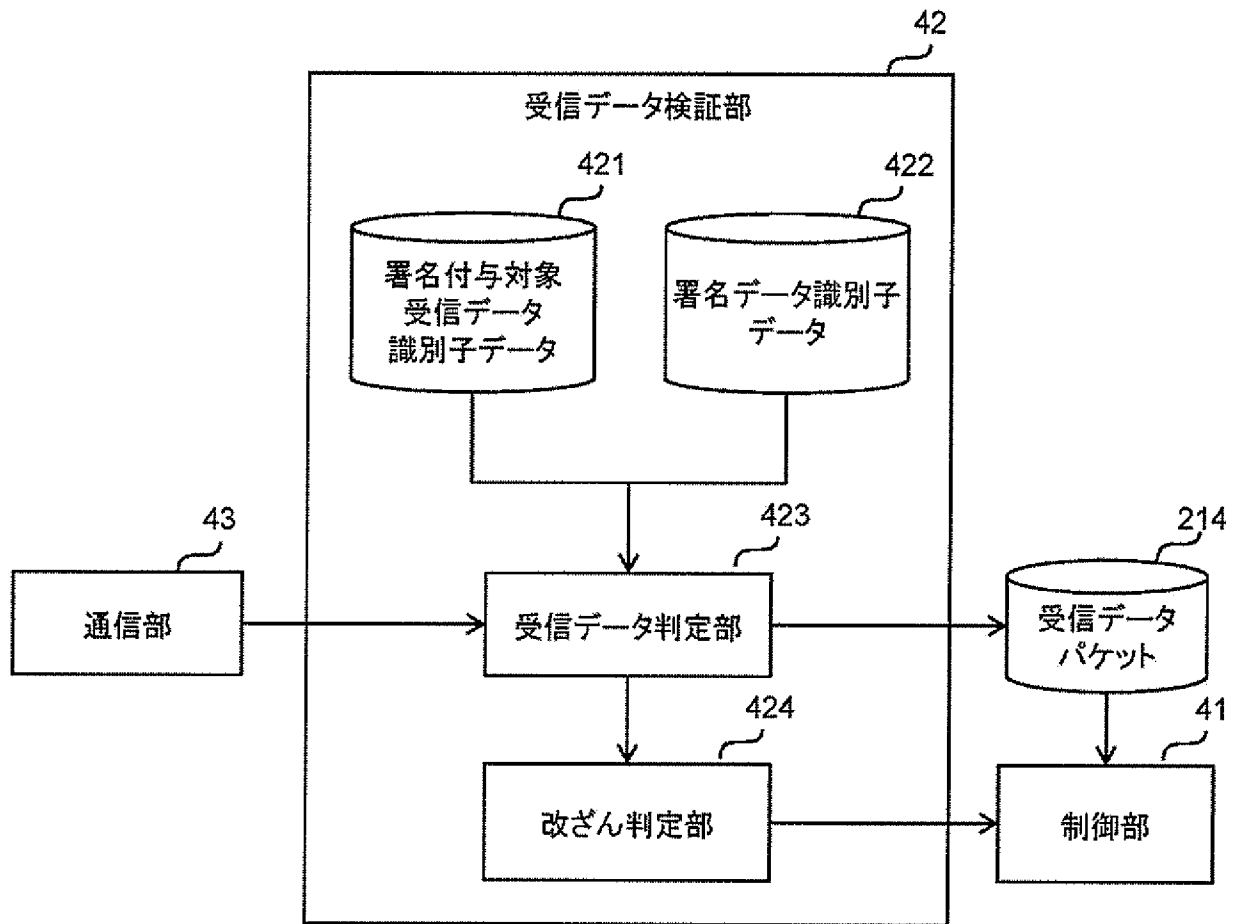
[図8]

図 8



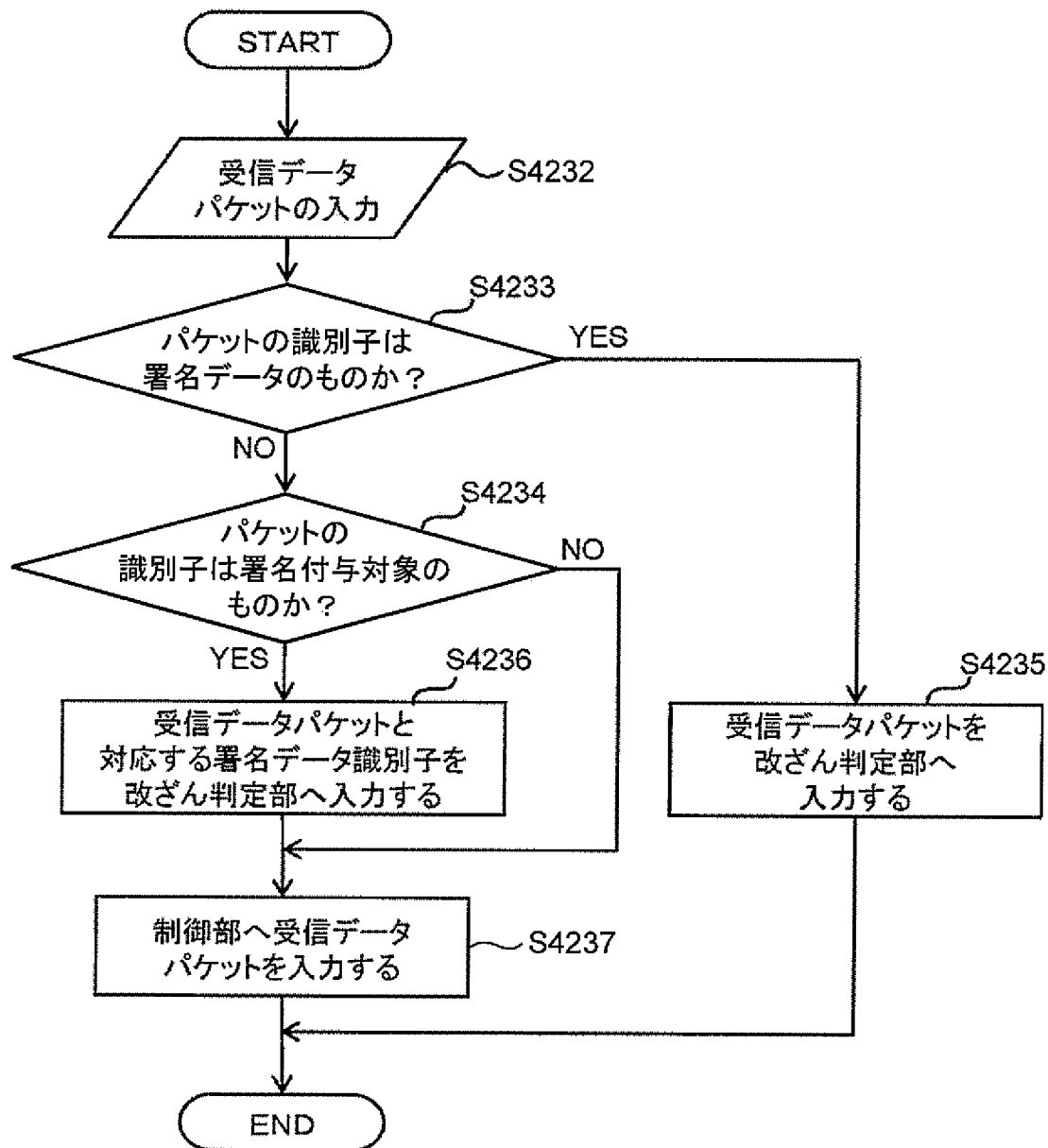
[図9]

図 9



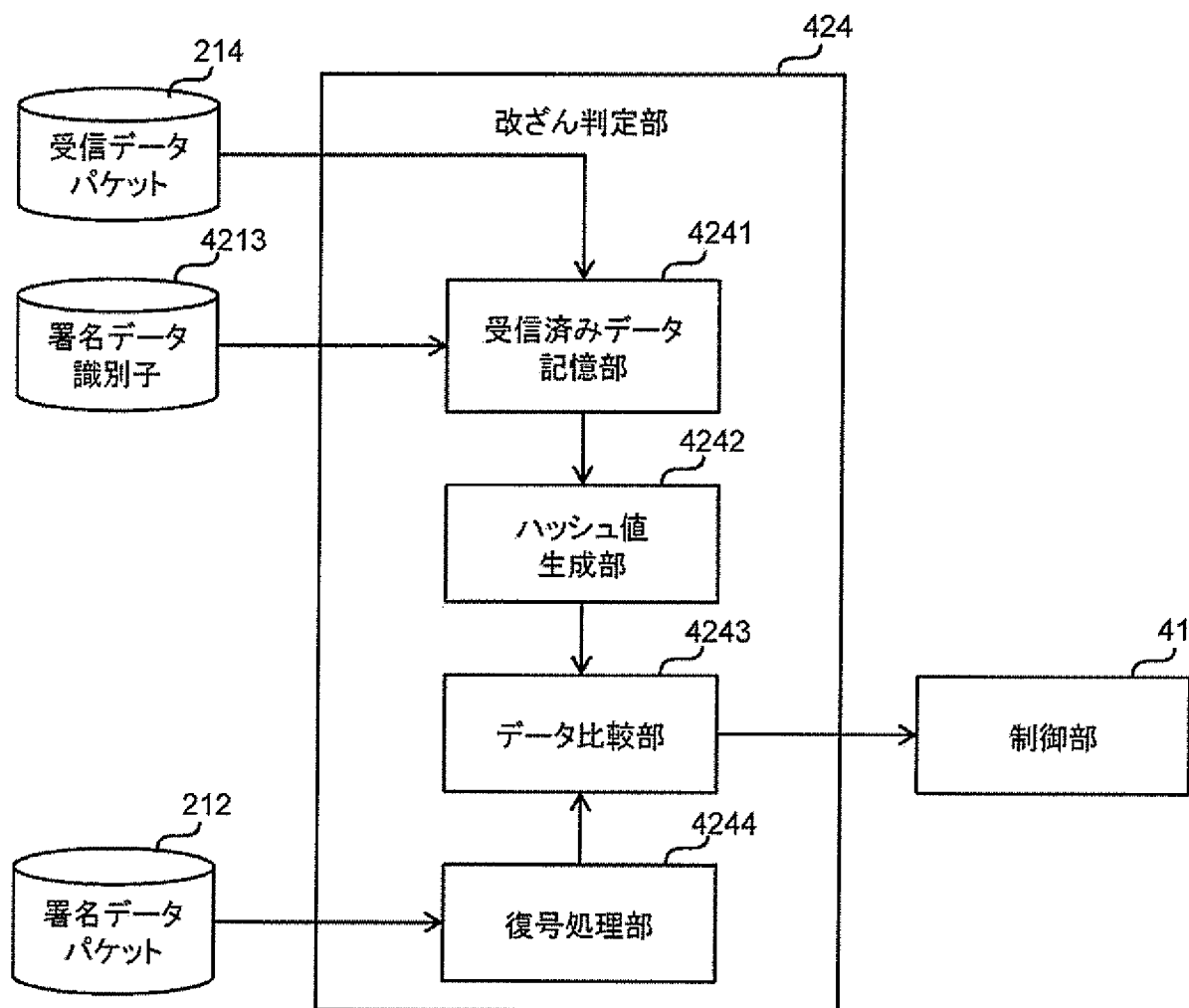
[図10]

図 10



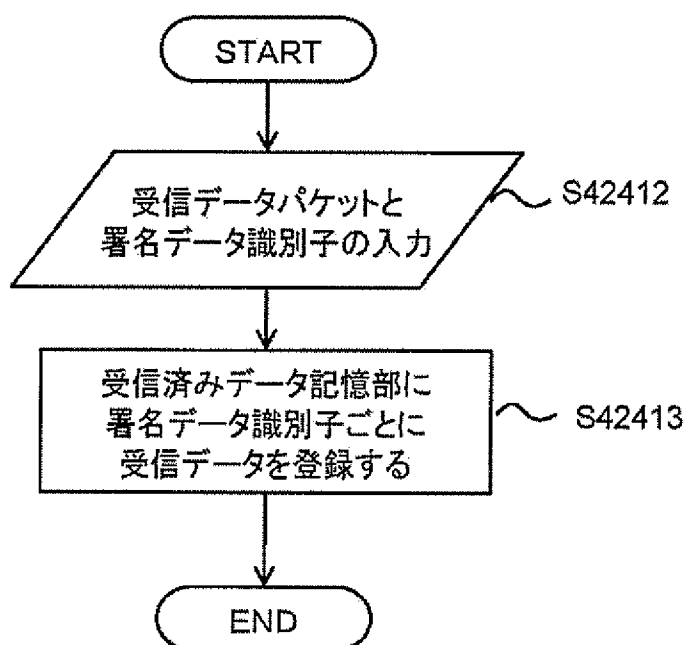
[図11]

図 1 1



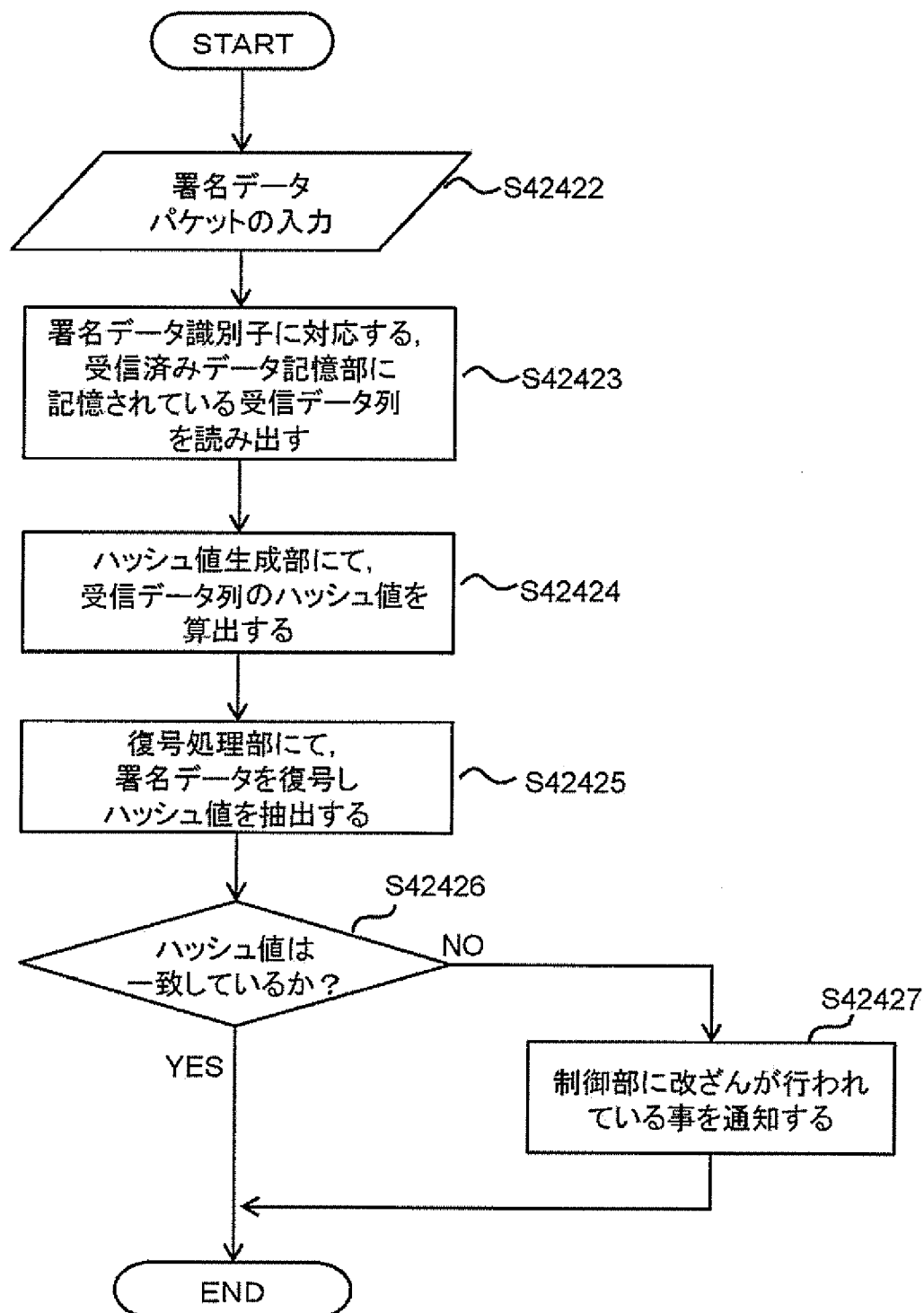
[図12]

図 1 2



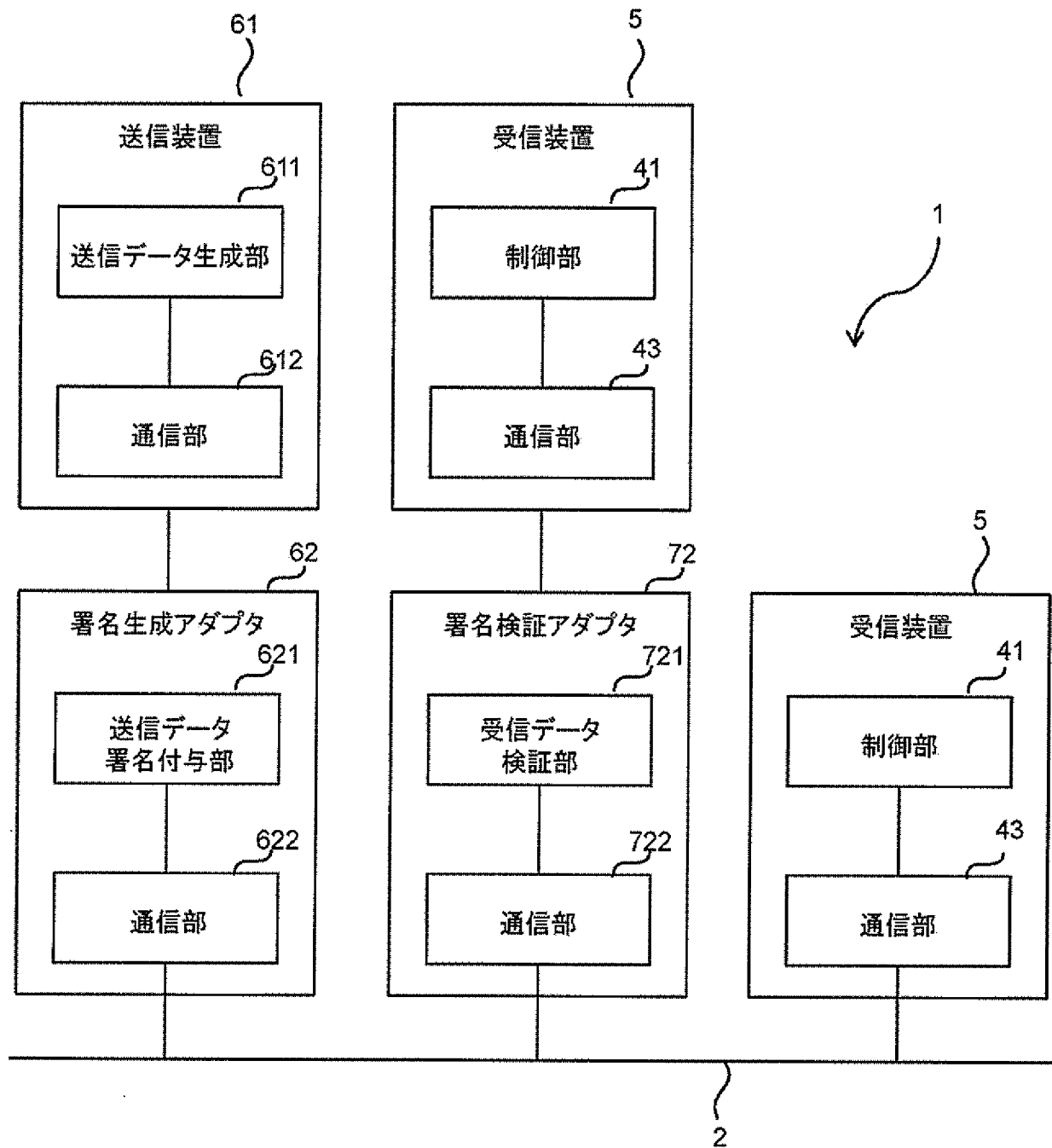
[図13]

図 1 3



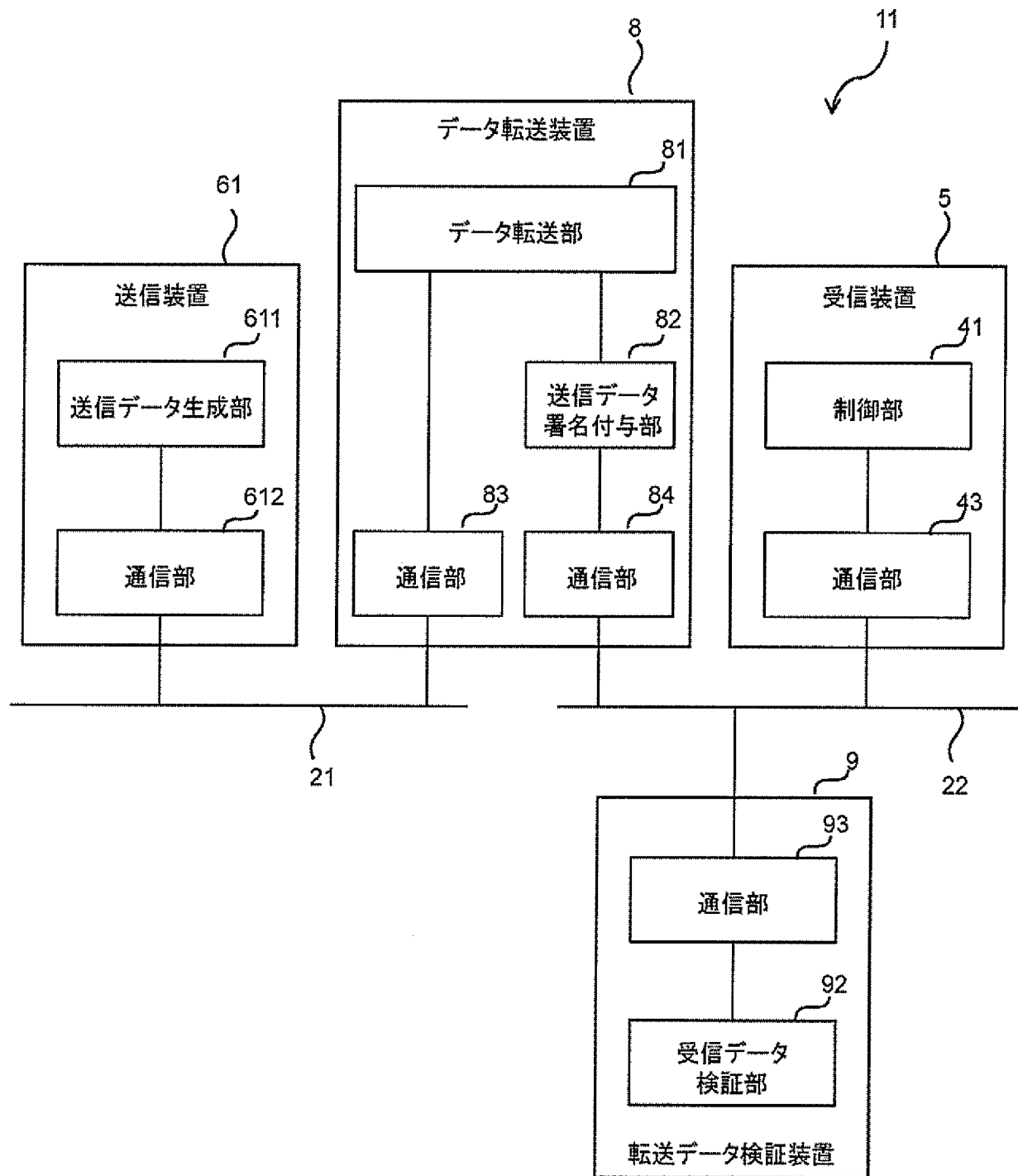
[図14]

図 1 4



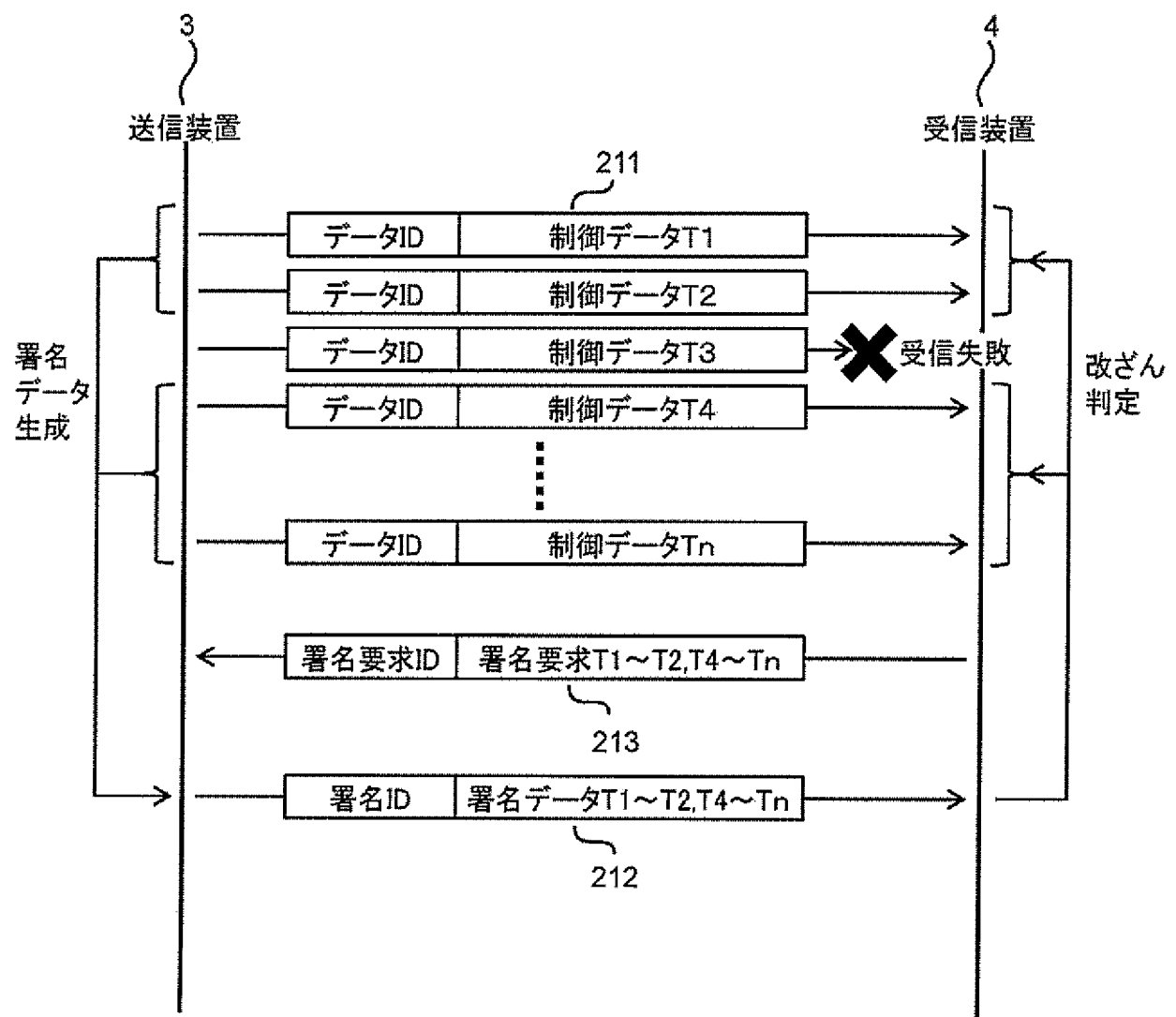
[図15]

図 1 5



[図16]

図 1 6



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/052904

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32(2006.01)i, G06F21/64(2013.01)i, G09C1/00(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/32, G06F21/64, G09C1/00

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2009-81549 A (Kyocera Corp. et al.), 16 April 2009 (16.04.2009), paragraphs [0020] to [0048] (Family: none)	1, 4, 5 2, 3
Y A	WO 2011/105350 A1 (Renesas Electronics Corp.), 01 September 2011 (01.09.2011), paragraphs [0004] to [0008] & US 2012/0311340 A1 & EP 2541829 A1 & CN 102771078 A	1, 4, 5 2, 3
A	JP 2008-60809 A (Toyota InfoTechnology Center, Co., Ltd. et al.), 13 March 2008 (13.03.2008), entire text; all drawings (Family: none)	1-5



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
26 February, 2014 (26.02.14)

Date of mailing of the international search report
11 March, 2014 (11.03.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/052904

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 2011-229075 A (Denso Corp.), 10 November 2011 (10.11.2011), entire text; all drawings & US 2011/0261890 A1 & DE 102011007857 A & FR 2959377 A & CA 2737841 A1	1-5

A. 発明の属する分野の分類（国際特許分類（I P C）） Int.Cl. H04L9/32(2006.01)i, G06F21/64(2013.01)i, G09C1/00(2006.01)i			
B. 調査を行った分野 調査を行った最小限資料（国際特許分類（I P C）） Int.Cl. H04L9/32, G06F21/64, G09C1/00			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 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 4 年 日本国実用新案登録公報 1 9 9 6 - 2 0 1 4 年 日本国登録実用新案公報 1 9 9 4 - 2 0 1 4 年			
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号	
Y A	JP 2009-81549 A（京セラ株式会社，他） 2009.04.16，段落 0020-0048 （ファミリーなし）	1, 4, 5 2, 3	
Y A	WO 2011/105350 A1（ルネサスエレクトロニクス株式会社） 2011.09.01，段落 0004-0008 & US 2012/0311340 A1 & EP 2541829 A1 & CN 102771078 A	1, 4, 5 2, 3	
☒ C 欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー 「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 2 6 . 0 2 . 2 0 1 4		国際調査報告の発送日 1 1 . 0 3 . 2 0 1 4	
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） 金沢 史明 電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6	5 S 4 5 3 8

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 請求項の番号
A	JP 2008-60809 A (株式会社トヨタ I T 開発センター, 他) 2008.03.13, 全文, 全図 (ファミリーなし)	1-5
A	JP 2011-229075 A (株式会社デンソー) 2011.11.10, 全文, 全図 & US 2011/0261890 A1 & DE 102011007857 A & FR 2959377 A & CA 2737841 A1	1-5