(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
2017 年 5 月 11 日(11.05.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/077868 A1

(51) 国際特許分類:
H04L 9/36 (2006.01) *G09C 1/00* (2006.01)
G06F 21/64 (2013.01)

(21) 国際出願番号: PCT/JP2016/081082

(22) 国際出願日: 2016 年 10 月 20 日(20.10.2016)

(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 2015-218336 2015 年 11 月 6 日(06.11.2015) 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２５２０番地 Ibaraki (JP).

(72) 発明者: 森田 伸義 (MORITA, Nobuyoshi); 〒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). 萱島 信 (KAYASHIMA, Makoto); 〒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). 井手口 恒太 (IDEGUCHI, Kouta); 〒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). 大和田 徹 (OWADA, Toru); 〒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: 永井 冬紀 (NAGAI, Fuyuki); 〒1080075 東京都港区港南一丁目６番４１号 品川クリスタルスクエア ９０１ 永井特許事務所 Tokyo (JP).

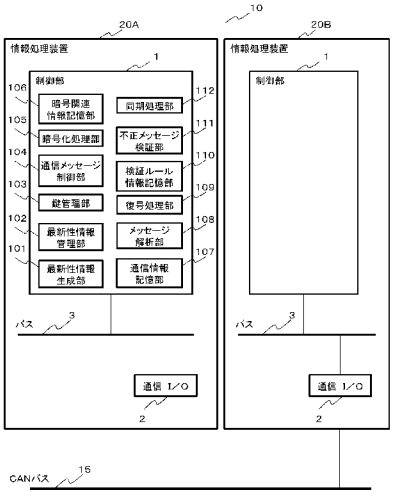
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK,

[続葉有]

(54) **Title**: INFORMATION PROCESSING DEVICE AND UNAUTHORIZED MESSAGE DETECTION METHOD

(54) 発明の名称 : 情報処理装置および不正メッセージ検知方法

[図1]



1 Control unit
2 Communication I/O
3 Bus
15 CAN bus
20A, 20B Information processing device
101 Recency information generation unit
102 Recency information management unit
103 Key management unit
104 Communication message control unit
105 Encryption processing unit
106 Encryption related information storage unit
107 Communication information storage unit
108 Message analysis unit
109 Decryption processing unit
110 Verification rule information storage unit
111 Unauthorized message verification unit
112 Synchronization processing unit

(57) **Abstract**: An information processing device receives a communication message generated on the basis of recency information and control data from another information processing device. The information processing device is provided with: a recency information generation unit that generates recency information; and a recency information management unit that extracts the recency information from the received communication message.

(57) 要約: 情報処理装置は、最新性情報と制御データとに基づいて生成された通信メッセージを他の情報処理装置から受信する情報処理装置であって、最新性情報を生成する最新性情報生成部と、受信した通信メッセージから最新性情報を抽出する最新性情報管理部と、を備える。

WO 2017/077868 A1

SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

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 ： 情報処理装置および不正メッセージ検知方法

技術分野

[0001] 本発明は、情報処理装置及び不正メッセージ検知方法に関する。

背景技術

[0002] 自動車の車載ネットワークにおける代表的な標準プロトコルとしてＣＡＮ（Ｃｏｎｔｒｏｌｌｅｒ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）が普及している。このような車載ネットワークでは、ＯＢＤ２（Ｏｎ－Ｂｏａｒｄ－Ｄｉａｇｎｏｓｔｉｃｓ　２）ポートのような車載ネットワークに直接繋がっているインタフェースに不正な機器が接続され、この不正な機器からリプレイ攻撃が行なわれることが想定される。ここで、リプレイ攻撃とは、通信路上を流れるメッセージを盗聴して事前に取得し、取得したメッセージを再送することで不正な動作を引き起こす攻撃である。また、車外のシステムと連携する情報処理装置がマルウェアに感染することも想定される。

[0003] 通常、これらの脅威に対しては、各情報処理装置間を流れるメッセージに対して、改ざん検知符号としてＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）を用いたメッセージ認証を実施することが有効とされている。例えば、特開２０１３－０９８７１９（特許文献１）には、車載ネットワークにおけるメッセージにＭＡＣを埋め込む通信システムが開示されている。特許文献１に記載の通信システムでは、各情報処理装置において、メッセージＩＤごとにメッセージが送信された回数をカウントする。送信側の情報処理装置は、データ、送信回数、メッセージＩＤからＭＡＣを生成する。受信側の情報処理装置は、受信したメッセージにおける、データ、送信回数、メッセージＩＤをもとにＭＡＣを算出し、別途受信したＭＡＣと比較する。受信側の情報処理装置は、算出したＭＡＣと受信したＭＡＣとが異なっている場合は、以降そのＩＤのメッセージを受け付けなくすることで、リプレイ攻撃やマルウェアによる感染に対処している。

先行技術文献

特許文献

[0004] 特許文献1：日本国特開２０１３－０９８７１９号公報

発明の概要

発明が解決しようとする課題

[0005] しかし、特許文献１に記載の通信システムでは、ＭＡＣを含むメッセージと制御用データを含むメッセージの２つのメッセージを送信するため、メッセージ数が増加するという課題がある。

課題を解決するための手段

[0006] 本発明の第１の態様によると、最新性情報と制御データとに基づいて生成された通信メッセージを他の情報処理装置から受信する情報処理装置は、最新性情報を生成する最新性情報生成部と、受信した通信メッセージから最新性情報を抽出する最新性情報管理部と、を備える。

本発明の第２の態様によると、不正メッセージ検知方法は、最新性情報と制御データとに基づいて一の情報処理装置で生成された通信メッセージが不正メッセージであるか否かを他の情報処理装置において検知する方法であって、一の情報処理装置のプロセッサは最新性情報を生成し、他の情報処理装置のプロセッサは通信メッセージから最新性情報を抽出する。

発明の効果

[0007] 本発明によれば、メッセージ数を増加させずに通信メッセージの検証を行うことができる。

図面の簡単な説明

[0008] [図1]制御ユニットの構成例を示すブロック図。

[図2]制御ユニットにおける処理の一例を示すフローチャート。

[図3]情報処理装置における最新性情報の生成処理の一例を示すフローチャート。

[図4]情報処理装置における通信メッセージ送信時の処理の一例を示すフロー

チャート。

[図5]通信メッセージのデータ構造の一例を示す図。

[図6]情報処理装置における通信メッセージ受信時の処理の一例を示すフローチャート。

[図7]情報処理装置における不正メッセージ判定処理の一例を示すフローチャート。

[図8]検証ルール情報のテーブル構成の一例を示す図。

発明を実施するための形態

[0009] （第１の実施の形態）

本実施の形態の情報処理装置２０は、車載用の情報処理装置２０である。この情報処理装置２０は、各情報処理装置２０でのみ共有する最新性情報により暗号化した暗号メッセージを、所定の検証ルールに従って復号する。ここで、最新性情報とは、通信メッセージの新しさに関する情報であり、例えば、シーケンス番号列やカウント値、時刻情報などである。情報処理装置２０は、復号されたメッセージが予め規定されたデータ構造に復元されるかどうかを検証することにより、受信したメッセージが不正なメッセージなのかどうかを判別する。ただし、本発明の技術的思想は、この例に限定されるものではない。なお、各情報処理装置２０で利用する暗号用の鍵及びシードは、安全に配布、管理、更新されていればよく、エンジン起動時／停止時、製品開発時、メンテナンス時などの任意のタイミングで配布や更新が行なわれてもよい。

[0010] 図１は、制御ユニット１０の構成例を示すブロック図である。制御ユニット１０は、複数の情報処理装置２０Ａ、２０Ｂを備える。情報処理装置２０Ａ、２０Ｂは、ＣＡＮバス１５を介して互いに接続されている。以下、情報処理装置２０Ａ、２０Ｂを代表して符号２０として説明することもある。情報処理装置２０は、互いにバス３で接続された制御部１および通信Ｉ／Ｏ２を備えている。なお、３以上の情報処理装置２０を備える制御ユニット１０にも本発明を適用できる。

[0011] 制御部１は、ＣＰＵやＦＰＧＡなどのプロセッサ、記憶装置であるＲＯＭおよびＲＡＭ、その他の周辺回路などを有する演算処理装置を含んで構成されている。プロセッサは、記憶装置に格納されているプログラムを実行することにより、装置内の各ハードウェアを制御する。各プログラムは、あらかじめ、情報処理装置内の記憶装置に格納されていてもよいし、入出力インタフェースを情報処理装置２０に具備しておき、必要なときに、入出力インタフェースと情報処理装置２０が利用可能な媒体を介して、他の装置から記憶装置に導入されてもよい。ここで、媒体とは、例えば入出力インタフェースに着脱可能な記憶媒体、または通信媒体（すなわち有線、無線、光などのネットワーク、または当該ネットワークを伝搬する搬送波やディジタル信号）を指す。

[0012] 制御部１は、各情報処理装置間２０で共有する最新性情報を生成する最新性情報生成部１０１、情報処理装置間を流れるメッセージ数或いはメッセージの種類に応じて最新性情報を更新する最新性情報管理部１０２、暗号化／復号処理や最新性情報を生成するための鍵データを管理する鍵管理部１０３、送信時におけるメッセージを生成する通信メッセージ制御部１０４、メッセージを暗号化する暗号化処理部１０５、暗号化／復号処理時における初期値や鍵データ、最新性情報等の暗号活用技術に関連する情報を記憶する暗号関連情報記憶部１０６、および通信路を流れるメッセージのカウンタ値等のメッセージ送受信処理に必要となる情報を記憶する通信情報記憶部１０７を機能的に備える。

[0013] 制御部１は、さらに、受信したメッセージのデータ構造を解析するメッセージ解析部１０８、メッセージ解析部１０８で分解したデータ構造をもとにメッセージを復号する復号処理部１０９、予め定められたルールを定義した検証ルール情報記憶部１１０、検証ルール情報記憶部１１０から取得したルールに基づいて復号したメッセージの完全性を検証する不正メッセージ検証部１１１、および各情報処理装置間における最新性情報の同期を行なう同期処理部１１２を機能的に備える。

[0014] 通信Ｉ／Ｏ２は、通信路を介して、他の情報処理装置２０からの送信メッセージを受信し、何らかの物理的な動作を行う。また、通信Ｉ／Ｏ２は、通信路を介して、他の情報処理装置２０に対し、何らかのメッセージを送信する。通信路は、例えば、ＣＡＮバス１５である。

[0015] 図２は、制御ユニット１０における処理の一例を示すフローチャートである。ここでは、情報処理装置２０Ａを送信用情報処理装置２１とし、情報処理装置２０Ｂを受信用情報処理装置２２として説明する。したがって、このフローチャートは、送信用情報処理装置２１と受信用情報処理装置２２との間における不正メッセージ検知処理シーケンスを示す。なお、送信用情報処理装置２１と受信用情報処理装置２２は、複数の情報処理装置２０の中から、メッセージを送信する情報処理装置とメッセージを受信する情報処理装置の例として挙げたものである。

[0016] ステップ２１１では、通信メッセージ制御部１０４は、送信用情報処理装置２１が送信する制御データを取得する。ステップ２１２では、最新性情報管理部１０２は、暗号関連情報記憶部１０６から最新性情報生成部１０１が生成した最新性情報を取得し、ステップ２１１で取得した制御データに所定のルールに基づいて最新性情報を付与する。ステップ２１３では、暗号化処理部１０５は、鍵管理部１０３から暗号用鍵を取得し、ステップ２１２で最新性情報を付与された制御データを暗号化する。

[0017] ステップ２１４では、通信メッセージ制御部１０４は、ステップ２１３で暗号化された制御データに、ＣＡＮ－ＩＤ等のヘッダ情報およびフッタ情報を付与し、通信メッセージを生成する。ステップ２１５では、通信メッセージ制御部１０４は、ステップ２１４で生成した通信メッセージを受信用情報処理装置２２に送信する。

[0018] ステップ２２１では、通信メッセージ制御部１０４は、ＣＡＮの通信プロトコルで定義されているＣＲＣ検証を行ない、ＣＲＣ検証において誤りを検知した場合は受信した通信メッセージを破棄し、所定のエラー処理を行なう。ステップ２２２では、復号処理部１０９は、鍵管理部１０３から復号処理

に用いる鍵を取得し、ステップ２２１におけるＣＲＣ検証で誤りが無いと判断されたメッセージを復号する。

[0019] ステップ２２３では、最新性情報管理部１０２は、ステップ２２２で復号されたメッセージに対して、通信メッセージの種類ごとに付与されるＩＤに紐付けた所定の検証ルールに基づいた処理を行なう。ステップ２２４では、不正メッセージ検証部１１１は、ステップ２２３の処理で得たメッセージに対して、検証ルール情報記憶部１１０から通信メッセージの種類ごとに付与されるＩＤに緋付けて定められた検証ルールを取得する。不正メッセージ検証部１１１は、検証ルールに従った判定処理を行ない、検証ルールを逸脱した場合は所定のエラー処理を行なう。ステップ２２５では、通信メッセージ制御部１０４は、ステップ２２４で検証ルールを遵守していると判断された場合、通常の制御処理を実行する。

[0020] 以上のステップにより、送信用情報処理装置２１は受信用情報処理装置２２にメッセージを送信し、受信用情報処理装置２２は受信したメッセージが不正なメッセージなのかどうかを判定できる。

[0021] 図３は、情報処理装置２０における最新性情報の生成処理の一例を示すフローチャートである。図３では、エンジン起動時、情報処理装置間での通信の直前、或いは情報処理装置間での通信の合間において、情報処理装置２０が生成する最新性情報の一例として、擬似乱数生成器を用いてシーケンス番号を生成する概要処理フローを示す。

[0022] ステップ３０１では、最新性情報管理部１０２は、擬似乱数生成器のシード、擬似乱数を生成するための補助情報、または擬似乱数生成器の内部状態を取得する。これらは、シーケンス番号を生成するために必要な付随情報の参照先を示す情報を用いて暗号関連情報記憶部１０６からシーケンス番号を生成するために必要な付随情報である。ここで、擬似乱数を生成するための補助情報とは、例えば、擬似乱数生成器の入力の一つである初期値（ＩＶ）である。また、擬似乱数生成器の内部状態とは、出力済みの乱数の次以降の乱数を生成するために必要な情報を指す。

[0023] ステップ３０２では、最新性情報生成部１０１は、ステップ３０１で取得したシード、または補助情報、または内部状態を用いて擬似乱数列を生成する。ステップ３０３では、最新性情報生成部１０１は、ステップ３０２で生成された擬似乱数列から、予め定められた方法でシーケンス番号列を作成する。ステップ３０４では、最新性情報管理部１０２は、ステップ３０３で生成したシーケンス番号列を最新性情報として暗号関連情報記憶部１０６に格納する。なお、最新性情報は、メモリ上に格納されてもよく、２次記憶装置に格納されてもよい。

[0024] ステップ３０５では、最新性情報管理部１０２は、シーケンス番号の生成が必要か否かを判断するための情報を更新し、終了する。ここで、シーケンス番号の生成が必要か否かを判断するための情報とは、例えば、シーケンス番号で使用するために生成した擬似乱数列の個数、および未使用の擬似乱数の先頭アドレスに相当する情報である。例えば、シーケンス番号のデータサイズがｂビットであり、ｂ×ｍビット分の擬似乱数を生成している場合、擬似乱数列の個数はｍである。また、最新性情報としてシーケンス番号を取得する際、ｂビットの擬似乱数を取得した場合は、擬似乱数列の個数をｍからｍ－１に更新し、先頭アドレスは次のｂビットの擬似乱数の先頭アドレスに更新する。

[0025] なお、ステップ３０２の擬似乱数生成処理では、予め定められた数を各情報処理装置２０が事前に共有しておき、１つのシードから生成された擬似乱数列のバイト長が予め定められた数に到達する度にシードの更新を行ってもよい。シードの更新は、例えば、ある情報処理装置において、１つのシードから生成された擬似乱数列のバイト長が予め定められた数に到達するとシードを生成し、更新用のシードを平文として暗号化を行って、他の情報処理装置２０に送信するようにすればよいが、実現可能な方法であればよく、上記の方法に限定されない。シードの更新などを実施することにより、シードを把握していない第三者はシーケンス番号の予測がさらに困難になる、という効果がある。

[0026] 以上のステップにより、情報処理装置２０は、各情報処理装置間で共有する最新性情報を生成することができる。

[0027] 図４は、情報処理装置２１における通信メッセージ送信時の処理の一例を示すフローチャートである。図４では、図２のステップ２１１からステップ２１５までの、送信用情報処理装置２１が不正なメッセージを判別するためのメッセージを生成し、そのメッセージを送信する時の概要処理フローを示す。図４の処理フローを開始する前に、図３で示したステップ３０１からステップ３０５を処理してもよい。このとき、最新性情報管理部１０２は、暗号関連情報記憶部１０６に格納されているシーケンス番号の生成が必要か否かを判断するための情報を参照し、シーケンス番号の生成の必要がある場合には、暗号関連情報記憶部１０６に格納されているシーケンス番号を生成するために必要な付随情報を用いてシーケンス番号列の生成処理を行い、シーケンス番号の生成が不要な場合は本処理をスキップする。

[0028] ステップ４１では、通信メッセージ制御部１０４は、車両の走行制御に用いる制御パラメータ情報を、例えば送信用情報処理装置２１に備わるセンサ機器等から取得する。ステップ４２では、通信メッセージ制御部１０４は、ステップ４１で取得した制御データの種類ごとに定められているＣＡＮ－ＩＤをチェックし、処理タイプを判定する。

[0029] 図８は、検証ルール情報８１のテーブル構成の一例を示す図である。すなわち、図８に示すテーブル構成は、ステップ４２で参照される検証ルール情報記憶部１１０に格納される検証ルール情報８１の一例である。ＣＡＮ－ＩＤ８１１は、メッセージに付与する制御データを識別する情報すなわちメッセージのＩＤ情報を示す。図８では、ＣＡＮ－ＩＤをメッセージに付与する制御データを識別する情報の例とし、ＣＡＮ－ＩＤ８１１としたが、メッセージに付与する制御データを識別可能な情報であればＣＡＮ－ＩＤ以外の情報を用いてもよい。

[0030] 処理タイプ８１２は、ＣＡＮ－ＩＤ８１１の値を使用するメッセージに対する最新性情報を付与する処理方法を示す。処理タイプが「挿入」の場合は

、データフィールドの空き領域に最新性情報を挿入する、すなわち制御データに最新性情報を追加することを示す。処理タイプが「ＸＯＲ」の場合は、制御データと最新性情報の排他的論理和（ＸＯＲ）処理を行なうことを示す。例えば、最新性情報を挿入する箇所として、後述する検証対象ビット８１４を用いてもよいし、予め決められたビット数に挿入してもよい。このようにして、最新性情報は、予め定められたデータ長の範囲内で制御データに付与される。

[0031] ルール種別８１３は、ステップ２２４における不正メッセージの判定処理において、ＣＡＮ－ＩＤ８１１の値を使用するメッセージに対する検証方法を識別するための情報を示す。検証対象ビット８１４は、ＣＡＮ－ＩＤ８１１の値を使用するメッセージに対する検証において、検証対象となるビット値を示す。

[0032] ステップ４３では、通信メッセージ制御部１０４は、ステップ４２で取得したＣＡＮ－ＩＤ８１１に対応する処理タイプ８１２が「ＸＯＲ」の場合はステップ４４に進み、処理タイプ８１２が「挿入」の場合はステップ４５に進む。ステップ４４では、最新性情報管理部１０２は、ステップ３０３で生成した最新性情報を暗号関連情報記憶部１０６から取得し、ステップ４１で取得した制御データとの排他的論理和処理を行なう。ステップ４５では、最新性情報管理部１０２は、ステップ３０３で生成した最新性情報を暗号関連情報記憶部１０６から取得し、データフィールドの空き領域に最新性情報を追加する。

[0033] ステップ４６では、暗号化処理部１０５は鍵管理部１０３より暗号用鍵を取得し、ステップ４４、或いはステップ４５において最新性情報が付与された制御データの暗号化を行なう。ステップ４７では、通信メッセージ制御部１０４は、ステップ４６で暗号化された制御データに、ＣＡＮ－ＩＤ等のヘッダ情報およびフッタ情報を付与し、通信メッセージを生成する。

[0034] 図５は、通信メッセージのデータ構造の一例を示す図である。通信メッセージは、ヘッダ情報５１１、データフィールド５１２、フッタ情報５１５か

ら構成される。ヘッダ情報５１１は、ＣＡＮ－ＩＤ等の情報から成る。データフィールド５１２は、ペイロード長となっており、制御データが付与される。フッタ情報５１５は、ＣＲＣ（Ｃｙｃｌｉｃ　Ｒｅｄｕｎｄａｎｃｙ　Ｃｈｅｃｋ）等のプロトコルで定められた情報から成る。

[0035] データフィールド５１２は、ステップ４４で制御データと最新性情報との排他的論理和を算出した場合は、「制御データＸＯＲ　最新性情報５１７」となり、ステップ４６において暗号化された際に、「Ｅｎｃ（制御データＸＯＲ　最新性情報）５１８」となる。データフィールド５１２は、ステップ４５で制御データに最新性情報を付与する場合は、制御データ５１３と最新性情報５１４の組み合わせとなり、ステップ４６において暗号化された際に、「Ｅｎｃ（制御データ、最新性情報）５１６」となる。ステップ４８では、通信メッセージ制御部１０４は、ステップ４７で生成した通信メッセージを通信Ｉ／Ｏ２を介して送信する。

[0036] 以上のステップにより、送信用情報処理装置２１は、不正なメッセージを判別するためのメッセージを生成し、そのメッセージを受信用情報処理装置２２に送信できる。なお、上記ステップでは処理を軽くするために、最新性情報として擬似乱数のような特定できない情報のみを利用し、ステップ４６を省略してもよい。

[0037] 図６は、情報処理装置２０における通信メッセージ受信時の処理の一例を示すフローチャートである。図６では、図２のステップ２２１からステップ２２５における、受信用情報処理装置２２における制御部１が、図５に示したデータ構造のメッセージを受信したときに、メッセージ解析部１０８を用いて受信メッセージのデータ構造を解析し、受信メッセージが不正なメッセージなのかどうかを判別するための概要処理フローを示す。

[0038] ステップ６０１では、通信メッセージ制御部１０４は、通信Ｉ／Ｏ２を介して、他の情報処理装置から送信されたメッセージを受信する。ステップ６０２では、通信メッセージ制御部１０４は、メッセージ解析部１０８を用いて、所定の検証対象から算出するＣＲＣの値と、フッタ情報５１５に付与さ

れたＣＲＣの値が一致するかどうかを検証する。ステップ６０３では、ステップ６０２で検証したＣＲＣに誤りが無い場合はステップ６０４に進み、誤りがある場合は処理を終了し、ＣＡＮで規定されている所定のエラー処理を実行する。ステップ６０４では、復号処理部１０９は、鍵管理部１０３から復号用鍵を取得し、ステップ６０３でＣＲＣに誤りが無いと判断されたメッセージを復号する。

[0039] ステップ６０５では、通信メッセージ制御部１０４は、メッセージ解析部１０８を用いて、受信したメッセージのヘッダ情報５１１に含まれるＣＡＮ－ＩＤを取得し、検証ルール情報記憶部１１０を参照して、ＣＡＮ－ＩＤの処理タイプ８１２を取得する。ステップ６０６では、通信メッセージ制御部１０４は、ステップ６０５で取得した処理タイプ８１２が「ＸＯＲ」の場合はステップ６０７に進み、処理タイプ８１２が「挿入」の場合はステップ６０８に進む。ステップ６０７では、最新性情報管理部１０２は、メッセージ解析部１０８を用いてデータフィールド５１２を取得し、通信情報記憶部１０７から各情報処理装置２０で共有される最新性情報を取得し、データフィールド５１２と最新性情報との排他的論理和処理を行なう。

[0040] ステップ６０８では、不正メッセージ検証部１１１は、ステップ６０１で受信メッセージから抽出したデータフィールド５１２、或いはステップ６０７でデータフィールド５１２と最新性情報との排他的論理和処理の出力データに基づいて、受信メッセージの不正を判断するための不正メッセージ判定処理を行う。不正メッセージ判定処理の具体的な内容は、後で図７のフローチャートを参照して説明する。ステップ６０９では、不正メッセージ検証部１１１は、ステップ６０８で不正なメッセージと判定した場合はステップ６１２に進み、不正なメッセージでないと判定した場合はステップ６１０に進む。

[0041] ステップ６１０では、通信メッセージ制御部１０４は、同期処理部１１２を用いて同期処理を行なうタイミングかどうかを検証する。例えば、ＣＡＮ－ＩＤごとに通信メッセージ数に応じて同期処理を行なうように閾値を設定

しておき、通信メッセージの受信ごとに更新するカウンタ数と閾値を比較し、閾値と一致した場合に同期処理を行なうタイミングと判定する。勿論、通信回数の代わりに時刻情報等を用いてもよい。ステップ６１１では、通信メッセージ制御部１０４は、同期処理部１１２を用いて同期処理のタイミングであると判定した場合はステップ６１２に進み、同期処理のタイミングでないと判定した場合はステップ６１４に進む。

[0042] ステップ６１２では、通信メッセージ制御部１０４は、同期処理部１１２を用いて同期用のメッセージを生成する。例えば、同期用のＣＡＮ－ＩＤと最新性情報を含むメッセージを生成する。さらに、最新性情報の完全性を証明するためにＭＡＣ等の符号を付与してもよい。ステップ６１３では、通信メッセージ制御部１０４は、ステップ６１２で生成した同期用メッセージを通信Ｉ／Ｏ２を介して送信する。ステップ６１４では、通信メッセージ制御部１０４は、ステップ６０９で不正でないと判定された受信メッセージに基づいて、所定の制御処理を実行する。

[0043] 送信用情報処理装置２１は、ステップ６１３で出力された同期用メッセージを通信Ｉ／Ｏ２を介して受信する。送信用情報処理装置２１は、同期用メッセージに含まれる受信用情報処理装置２２が付与した最新性情報と、送信用情報処理装置２１が保持する最新性情報とが一致しているか否かを判定する。送信用情報処理装置２１は、最新性情報が一致しない場合は、例えば、同期用メッセージに含まれる最新性情報に基づいて、送信用情報処理装置２１の最新性情報管理部１０２により最新性情報を更新させる。送信用情報処理装置２１は、送信用情報処理装置２１が使用する最新性情報を、同期用メッセージに含まれる最新性情報と同一にすることで、情報処理装置間で最新性情報を同期させることができる。

[0044] 以上のステップにより、受信用情報処理装置２２における制御部１が、他の情報処理装置から図５に示したデータ構造のメッセージを受信したときに、メッセージ解析部１０８を用いて受信メッセージのデータ構造を解析し、受信メッセージが不正なメッセージなのかどうかを判別できる。

[0045] 図７は、情報処理装置２０における不正メッセージ判定処理の一例を示すフローチャートである。図７では、図６のステップ６０８で実行される不正メッセージ判定処理の概要処理フローを示す。

[0046] ステップ７１では、不正メッセージ検証部１１１は、検証ルール情報記憶部１１０より受信メッセージのＣＡＮ－ＩＤに該当するルール種別８１３を取得する。ステップ７２では、不正メッセージ検証部１１１は、検証ルール情報記憶部１１０より受信メッセージのＣＡＮ－ＩＤに該当する検証対象ビット８１４を取得する。ステップ７３では、不正メッセージ検証部１１１は、ステップ７１とステップ７２で取得した、ルール種別および検証対象ビットに基づいて不正メッセージかどうかを検証する。

[0047] 例えば、ルール種別が「カウンタ」の場合は、検証対象ビット８１４に挿入される最新性情報と、受信用情報処理装置が保持する最新性情報と一致しているかを検証する。ルール種別が「固定」の場合は、検証対象ビット８１４に記載されるビットの値が、予め決められた値から変化していないかを検証する。ルール種別が「レンジ」の場合は、検証対象ビット８１４に記載されるビットの値が、予め決められた最小値から最大値の範囲内かどうかを検証する。ルール種別が「チェックサム」の場合は、検証対象ビット８１４に記載されるビットの値が、所定のチェックサム算出手法を用いて算出したチェックサムの値と一致しているかを検証する。なお、このようなルール種別として、一つのＣＡＮ－ＩＤに複数のルールが適用されてもよい。

[0048] ステップ７４では、不正メッセージ検証部１１１は、ステップ７３で検証ルールを逸脱したと判定した場合にステップ７６に進み、検証ルールを逸脱していないと判定した場合にステップ７５に進む。ステップ７５では、不正メッセージ検証部１１１は、検証ルール逸脱フラグを「ＯＦＦ」とし、ステップ６０９で当該フラグに基づいてステップ６１０に進む。ステップ７６では、不正メッセージ検証部１１１は、検証ルール逸脱フラグを「ＯＮ」とし、ステップ６０９で当該フラグに基づいてステップ６１２に進む。

[0049] 以上のステップにより、受信用情報処理装置２２は、受信したメッセージ

が不正メッセージなのかどうかを判定できる。

[0050] 上述した実施の形態によれば、次の作用効果が得られる。

（１）情報処理装置２０は、最新性情報と制御データとに基づいて生成された通信メッセージを、他の情報処理装置から受信する。情報処理装置２０は、最新性情報を生成する最新性情報生成部１０１と、受信した通信メッセージから最新性情報を抽出する最新性情報管理部１０２と、を備える。本実施の形態では、最新性情報と制御データとに基づいて生成された通信メッセージを受信し、受信した通信メッセージから最新性情報を抽出する。したがって、メッセージ数を増加させずに通信メッセージの検証を行うことができる。

（２）最新性情報は、同期用通信メッセージに応じて更新される。このため、メッセージを盗聴して事前に取得しメッセージを再送するリプレイ攻撃が行われても、再送されたメッセージは不正メッセージと検知することができる。すなわち、リプレイ攻撃に使用される再送された通信メッセージは、受信側の情報処理装置が通信メッセージを復号する時点よりも旧い時点の最新性情報を含んでいる。そのため、リプレイ攻撃を防御することができる。

[0051] （３）最新性情報管理部１０２は、通信メッセージに応じて最新性情報を更新し、最新性情報を含む同期用の通信メッセージに基づいて、最新性情報管理部１０２が更新する最新性情報を他の情報処理装置が更新する最新性情報と同期させる。このようにしたので、最新性情報と制御データとに基づいて生成された通信メッセージを受信した受信側の情報処理装置は送信側の情報処理装置の最新性情報と同期をとることができる。すなわち、各情報処理装置２０で更新される最新性情報を同一にすることができる。

（４）通信メッセージは、予め定められたデータ長の範囲内で制御データに最新性情報を付与して生成される。このようにしたので、メッセージ数を増加させずに不正なメッセージを検知することができる。メッセージ数を増加させないため、メッセージ数の増加による通信負荷の増大を回避することができる。また、制御データのデータフィールドに、挿入あるいは排他的論理

和により最新性情報を付与するため、通信プロトコルを変更せずに不正メッセージの検証を行うことができる。

[0052] （５）情報処理装置２０は、制御データの種類に応じた検証ルールを記憶する検証ルール情報記憶部１１０と、検証ルールに基づいて、制御データの正誤を検証する不正メッセージ検証部１１１と、をさらに備える。本実施の形態では、制御データの種類ごとに付与されるＣＡＮ－ＩＤに応じた検証ルールが記憶され、検証ルールに基づいて不正メッセージの検知を行う。このようにしたので、制御データの種類に応じて検証ルールを変更させることができる。検証ルールはネットワーク上を伝送しないため、検証ルールが不正に取得されることを防止することができる。

（６）検証ルール情報記憶部１１０には、制御データの種類とデータ検証領域とが対応付けられて記憶されており、不正メッセージ検証部１１１は、データ検証領域のデータに基づいて、制御データの正誤を検証する。このようにしたので、制御データの種類に応じてデータ検証領域を変更させることができる。データ検証領域はネットワーク上を伝送しないため、データ検証領域が不正に取得されることを防止することができる。

[0053] （７）不正メッセージ検証部１１１は、検証ルールとして、制御データの最小値および最大値を用いた検証、制御データの所定領域を用いた検証、制御データのチェックサムを用いた検証の少なくとも一つに基づいて、制御データの正誤を検証する。このようにしたので、制御データの種類に応じてデータ検証方法を変更させることができる。

（８）情報処理装置２０は、不正メッセージ検証部１１１により制御データが正当なデータでないと判定された場合に、最新性情報管理部１０２が更新する最新性情報を含む同期用の通信メッセージを生成して、他の情報処理装置に送信する同期処理部１１２をさらに備える。このようにしたので、不正メッセージを受信した場合において、各情報処理装置間の最新性情報の同期を行うことができる。

[0054] （９）同期処理部１１２は、不正メッセージ検証部１１１による検証の結果

に関わらず、所定の周期で同期用の通信メッセージを生成して、他の情報処理装置に送信する。このようにしたので、所定の周期で各情報処理装置間の最新性情報の同期を行うことができる。

（１０）最新性情報管理部１０２は、受信した通信メッセージと最新性情報の排他的論理和を算出して、受信した通信メッセージから最新性情報を抽出する。このようにしたので、メッセージ数を増加させずに、制御データに最新性情報を付与することができる。

[0055] 次のような変形も本発明の範囲内であり、変形例の一つ、もしくは複数を上述の実施形

態と組み合わせることも可能である。

[0056]（変形例１）

上述した実施の形態および変形例では、通信規格としてＣＡＮを例に説明したが、本発明はこれに限定されず、たとえば、ＣＡＮ－ＦＤやＥｔｈｅｒｎｅｔ（登録商標）に適用してもよい。ＣＡＮのデータ長が８バイトの固定長に対して、ＣＡＮ－ＦＤのデータ長は８バイト～６４バイトの可変長となっており、ＣＡＮ－ＩＤごとにデータ長が決まっている。このため、ＣＡＮ－ＩＤのデータフィールドが６４バイトすべてを使用していない場合、データフィールド内の空き領域に最新性情報を埋め込む方法を追加してもよい。Ｅｔｈｅｒｎｅｔの場合は、ＣＡＮ－ＩＤの代わりに、送信元アドレス等を用いて適用するルールを選択するようにしてもよい。

[0057]（変形例２）

上述した実施の形態および変形例では、車載ネットワークを対象に説明しているが、本情報処理装置はこれに限定するものではなく、制御系システムや情報系システムにおける装置にも適用可能である。

[0058] 上記では、種々の実施の形態および変形例を説明したが、本発明はこれらの内容に限定されるものではない。本発明の技術的思想の範囲内で考えられるその他の態様も本発明の範囲内に含まれる。

たとえば、最新性情報と制御データとに基づいて生成された通信メッセー

ジを他の情報処理装置から受信する情報処理装置であって、最新性情報を生成する最新性情報生成部と、受信した通信メッセージから最新性情報を抽出する最新性情報管理部とを備える種々の情報処理装置に本発明を適用できる。

また、最新性情報と制御データとに基づいて一の情報処理装置で生成された通信メッセージが不正メッセージであるか否かを他の情報処理装置において検知する方法であって、一の情報処理装置のプロセッサは最新性情報を生成し、他の情報処理装置のプロセッサは通信メッセージから最新性情報を抽出する不正メッセージ検知方法に本発明を適用できる。

[0059] 次の優先権基礎出願の開示内容は引用文としてここに組み込まれる。

日本国特許出願２０１５年第２１８３３６号（２０１５年１１月６日出願）

符号の説明

[0060] １　制御部

２　通信Ｉ／Ｏ

３　バス

２０　情報処理装置

１０１　最新性情報生成部

１０２　最新性情報管理部

１１０　検証ルール情報記憶部

１１１　不正メッセージ検証部

１１２　同期処理部

請求の範囲

[請求項1] 最新性情報と制御データとに基づいて生成された通信メッセージを他の情報処理装置から受信する情報処理装置であって、

前記最新性情報を生成する最新性情報生成部と、

前記受信した通信メッセージから前記最新性情報を抽出する最新性情報管理部と、

を備える情報処理装置。

[請求項2] 請求項１に記載の情報処理装置において、

前記最新性情報管理部は、前記通信メッセージに応じて前記最新性情報を更新し、前記最新性情報を含む同期用の通信メッセージに基づいて、前記最新性情報管理部が更新する前記最新性情報を前記他の情報処理装置が更新する前記最新性情報と同期させる情報処理装置。

[請求項3] 請求項１または２に記載の情報処理装置において、

前記通信メッセージは、予め定められたデータ長の範囲内で前記制御データに前記最新性情報を付与して生成される情報処理装置。

[請求項4] 請求項１～３のいずれか一項に記載の情報処理装置において、

前記制御データの種類に応じた検証ルールを記憶する検証ルール情報記憶部と、

前記検証ルールに基づいて、前記制御データの正誤を検証する不正メッセージ検証部と、をさらに備える情報処理装置。

[請求項5] 請求項４に記載の情報処理装置において、

前記検証ルール情報記憶部には、前記制御データの種類とデータ検証領域とが対応付けられて記憶されており、

前記不正メッセージ検証部は、前記データ検証領域のデータに基づいて、前記制御データの正誤を検証する情報処理装置。

[請求項6] 請求項４または５に記載の情報処理装置において、

前記不正メッセージ検証部は、前記検証ルールとして、前記制御データの最小値および最大値を用いた検証、前記制御データの所定領域

を用いた検証、前記制御データのチェックサムを用いた検証の少なくとも一つに基づいて、前記制御データの正誤を検証する情報処理装置。

[請求項7] 請求項４～６のいずれか一項に記載の情報処理装置において、

前記不正メッセージ検証部により前記制御データが正当なデータでないと判定された場合に、前記最新性情報管理部が更新する前記最新性情報を含む同期用の通信メッセージを生成して、前記他の情報処理装置に送信する同期処理部をさらに備える情報処理装置。

[請求項8] 請求項４～６のいずれか一項に記載の情報処理装置において、

前記最新性情報管理部が更新する前記最新性情報を含む同期用の通信メッセージを生成して、前記他の情報処理装置に送信する同期処理部をさらに備え、

前記同期処理部は、前記不正メッセージ検証部による前記検証の結果に関わらず、所定の周期で前記同期用の通信メッセージを生成して、前記他の情報処理装置に送信する情報処理装置。

[請求項9] 請求項１～８のいずれか一項に記載の情報処理装置において、

前記最新性情報管理部は、前記受信した通信メッセージと前記最新性情報の排他的論理和を算出して、前記受信した通信メッセージから前記最新性情報を抽出する情報処理装置。

[請求項10] 最新性情報と制御データとに基づいて一の情報処理装置で生成された通信メッセージが不正メッセージであるか否かを他の情報処理装置において検知する方法であって、

前記一の情報処理装置のプロセッサは前記最新性情報を生成し、

前記他の情報処理装置のプロセッサは前記通信メッセージから前記最新性情報を抽出する不正メッセージ検知方法。

[請求項11] 請求項１０に記載の不正メッセージ検知方法において、

前記他の情報処理装置のプロセッサは、前記最新性情報を含む同期用の通信メッセージに基づいて、前記一の情報処理装置が更新する前

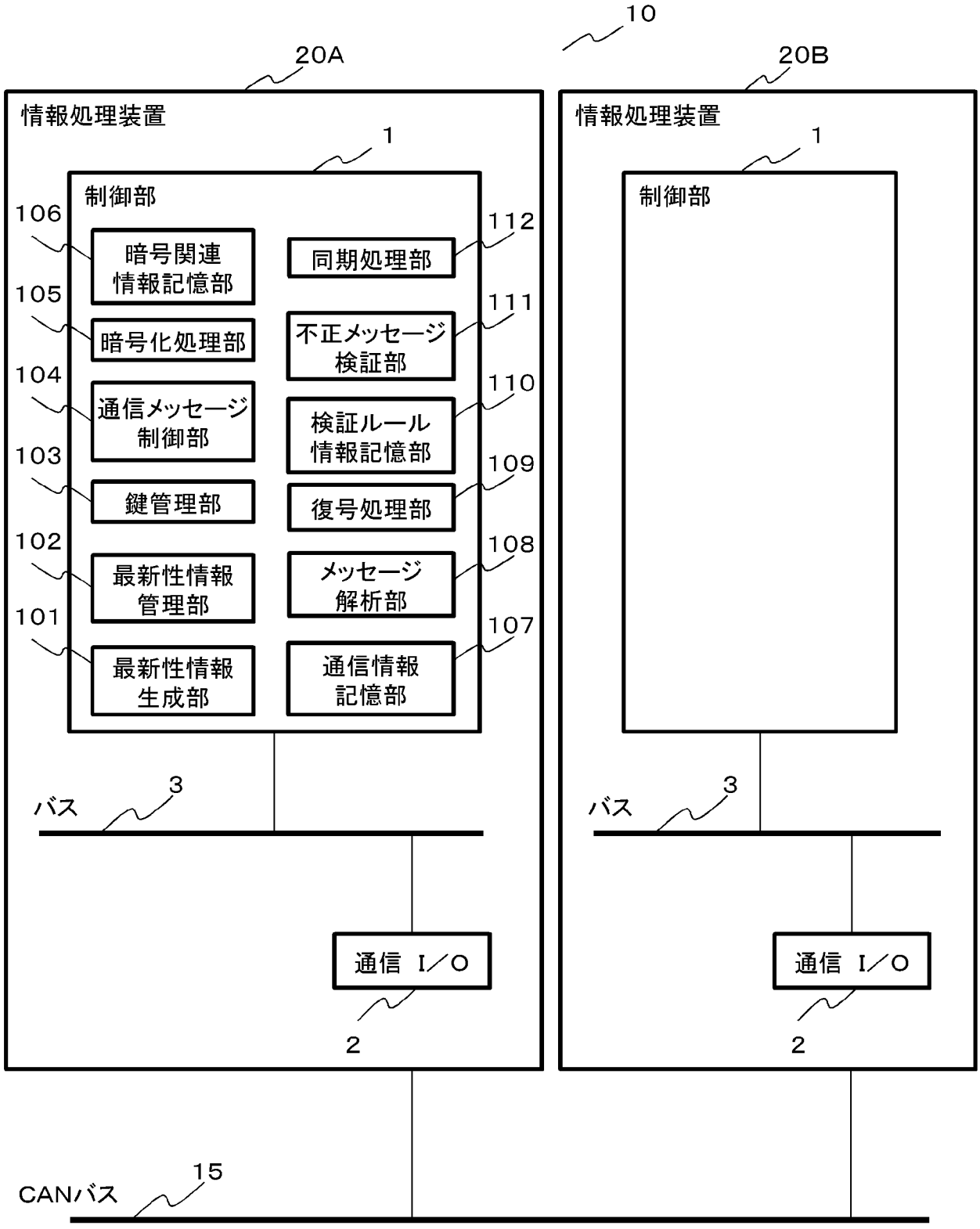
記最新性情報と同期させて前記最新性情報を更新する不正メッセージ検知方法。

[請求項12] 請求項１０または１１に記載の不正メッセージ検知方法において、

前記通信メッセージは、予め定められたデータ長の範囲内で前記制御データに前記最新性情報を付与して生成される不正メッセージ検知方法。

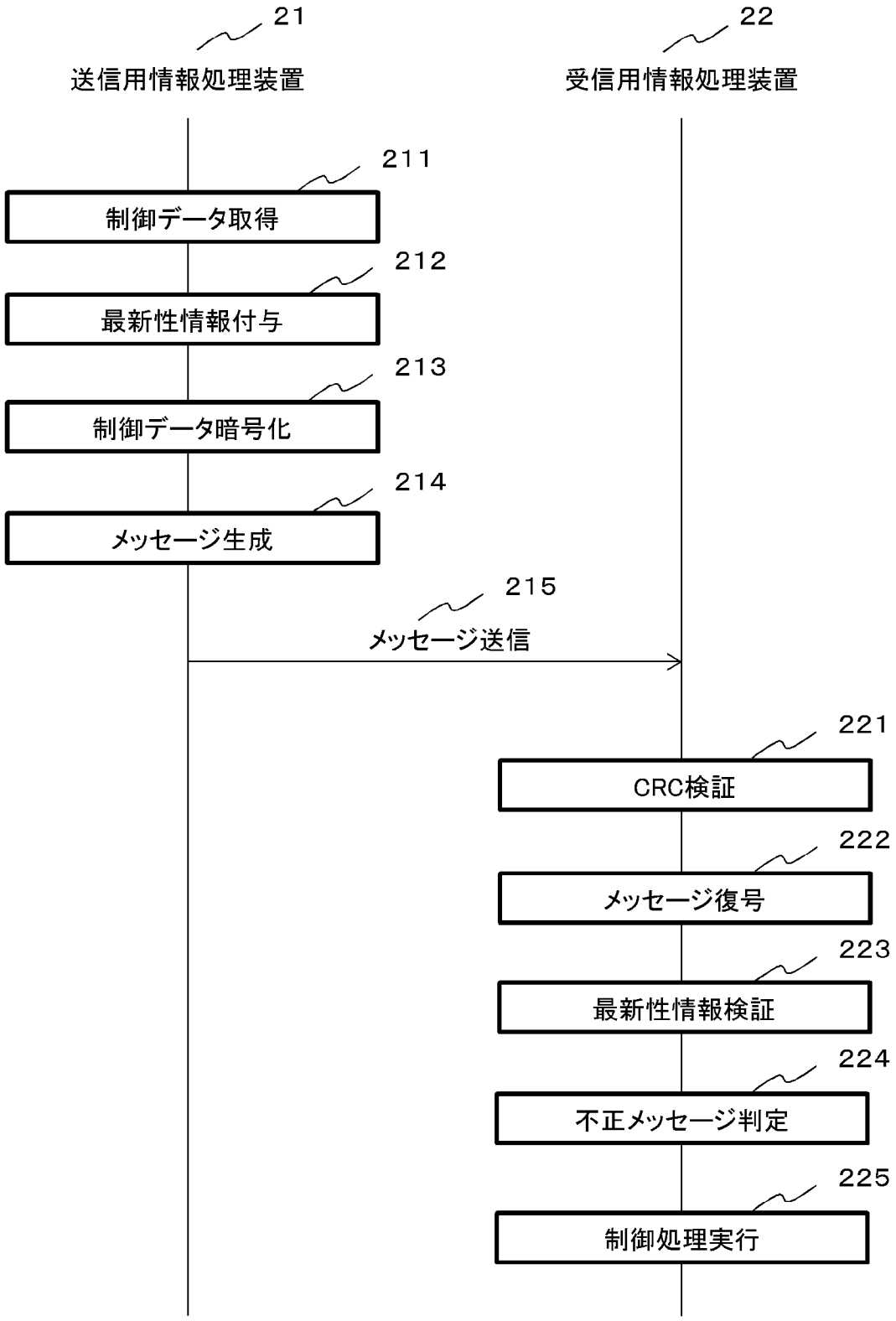
[図1]

【図1】


10
20A
20B
情報処理装置
情報処理装置
1
1
制御部
制御部
106
暗号関連
情報記憶部
105
暗号化処理部
104
通信メッセージ
制御部
103
鍵管理部
102
最新性情報
管理部
101
最新性情報
生成部
112
同期処理部
111
不正メッセージ
検証部
110
検証ルール
情報記憶部
109
復号処理部
108
メッセージ
解析部
107
通信情報
記憶部
バス
3
バス
3
通信 I／O
通信 I／O
2
2
CANバス
15

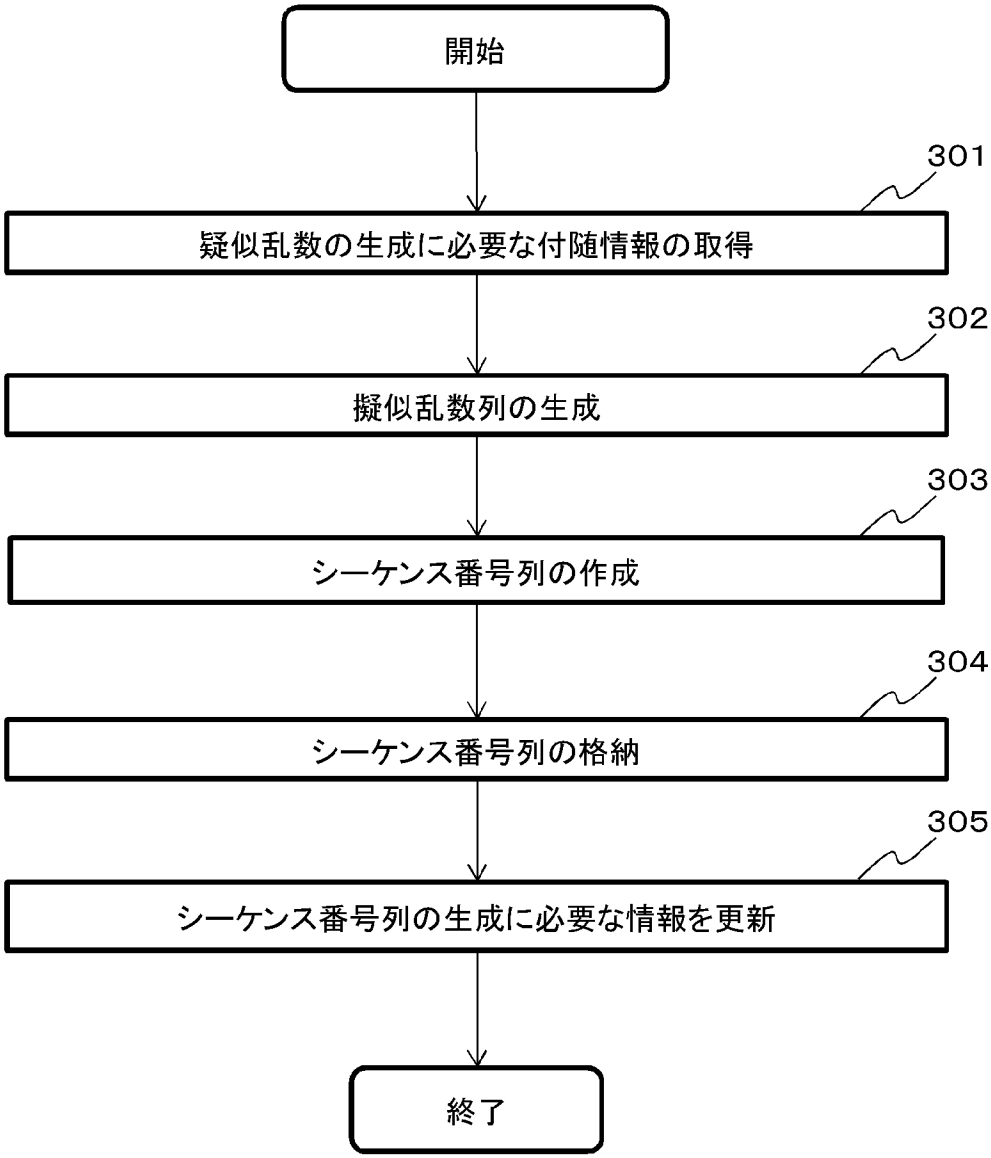
[図2]

【図2】


21
送信用情報処理装置
22
受信用情報処理装置
211
制御データ取得
212
最新性情報付与
213
制御データ暗号化
214
メッセージ生成
215
メッセージ送信
221
CRC検証
222
メッセージ復号
223
最新性情報検証
224
不正メッセージ判定
225
制御処理実行

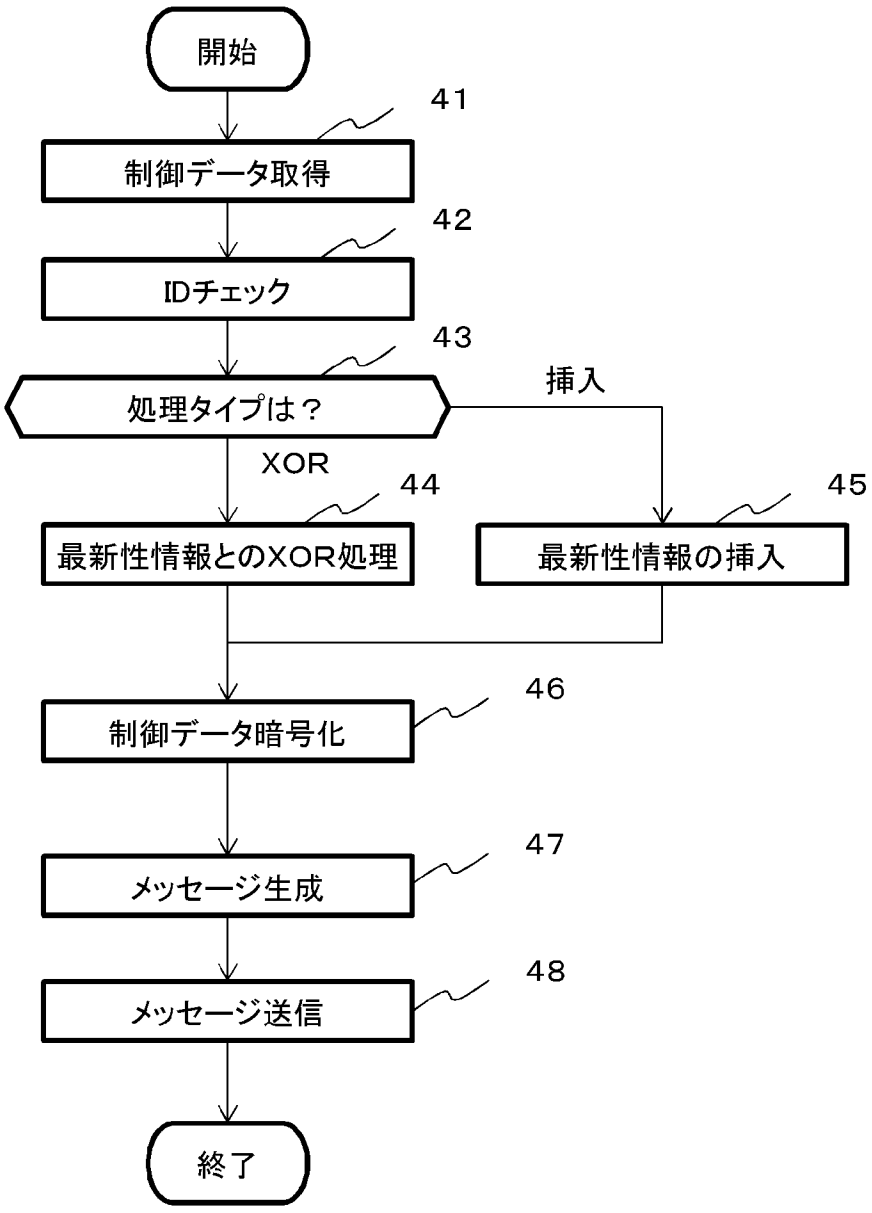
[図3]

【図３】


開始
301
疑似乱数の生成に必要な付随情報の取得
302
擬似乱数列の生成
303
シーケンス番号列の作成
304
シーケンス番号列の格納
305
シーケンス番号列の生成に必要な情報を更新
終了

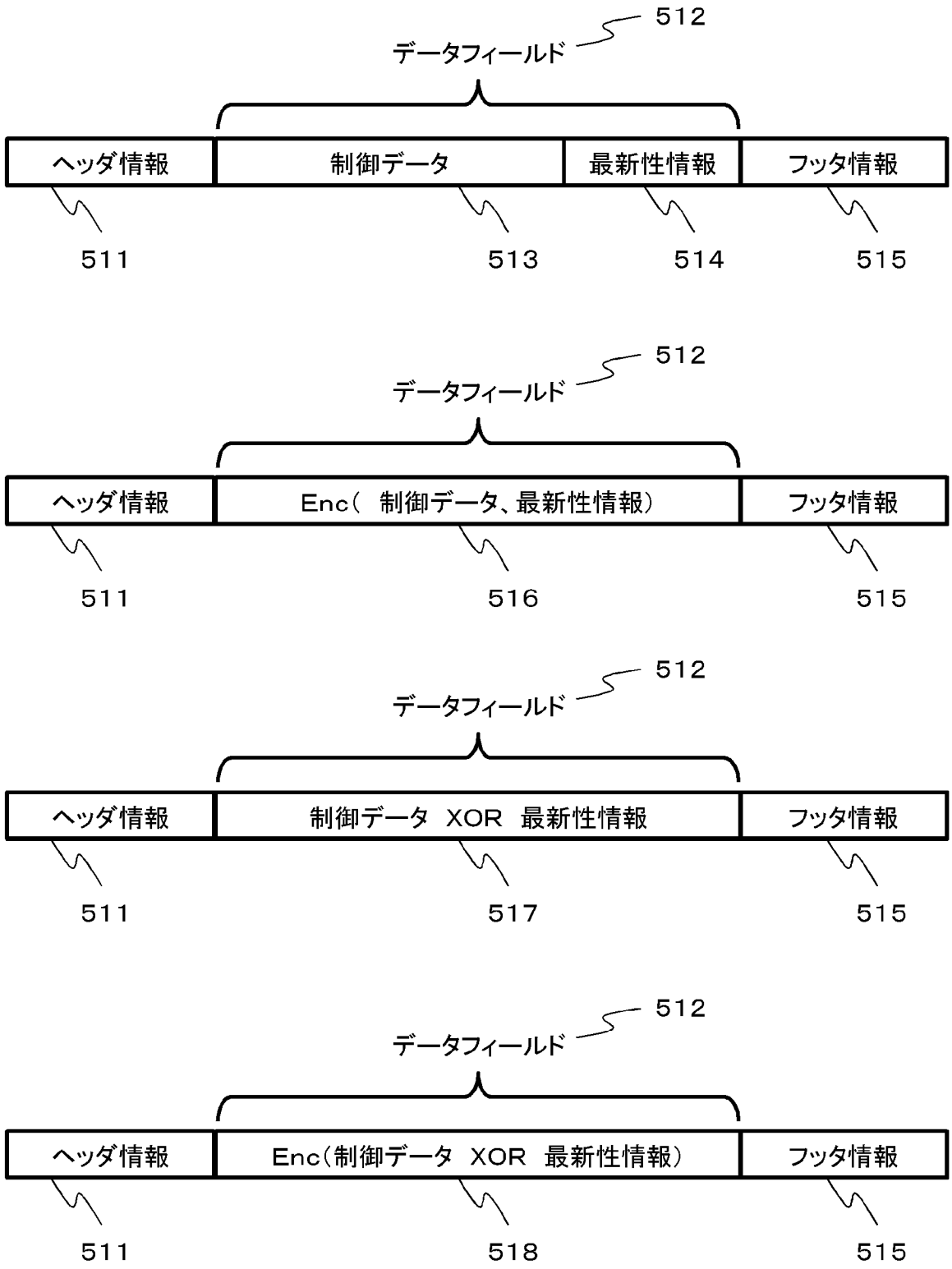
[図4]

【図4】


開始
41
制御データ取得
42
IDチェック
43
処理タイプは？
挿入
XOR
44
45
最新性情報とのXOR処理
最新性情報の挿入
46
制御データ暗号化
47
メッセージ生成
48
メッセージ送信
終了

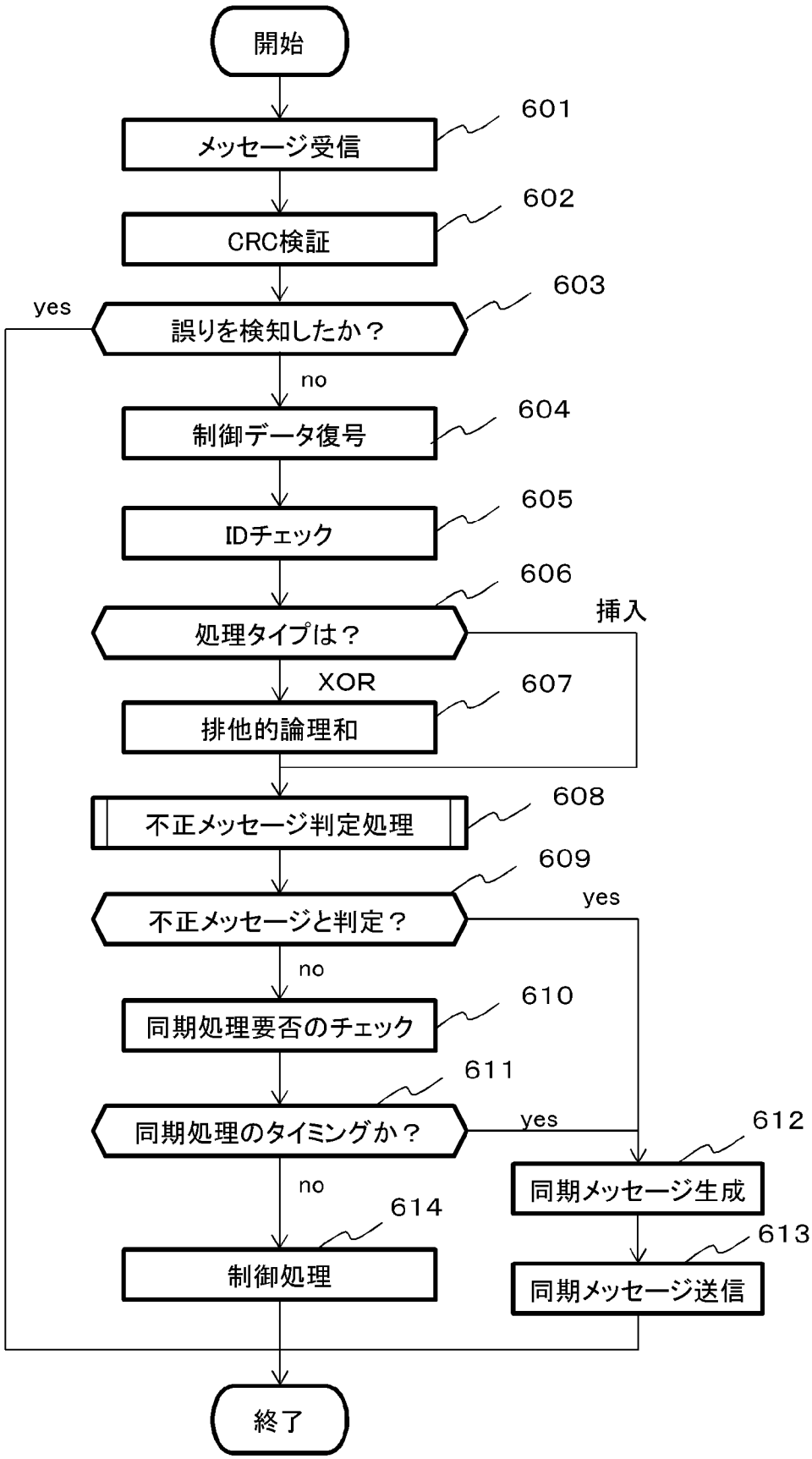
[図5]

【図5】


512
データフィールド
ヘッダ情報
制御データ
最新性情報
フッタ情報
511
513
514
515
512
データフィールド
ヘッダ情報
Enc(制御データ、最新性情報)
フッタ情報
511
516
515
512
データフィールド
ヘッダ情報
制御データ XOR 最新性情報
フッタ情報
511
517
515
512
データフィールド
ヘッダ情報
Enc(制御データ XOR 最新性情報)
フッタ情報
511
518
515

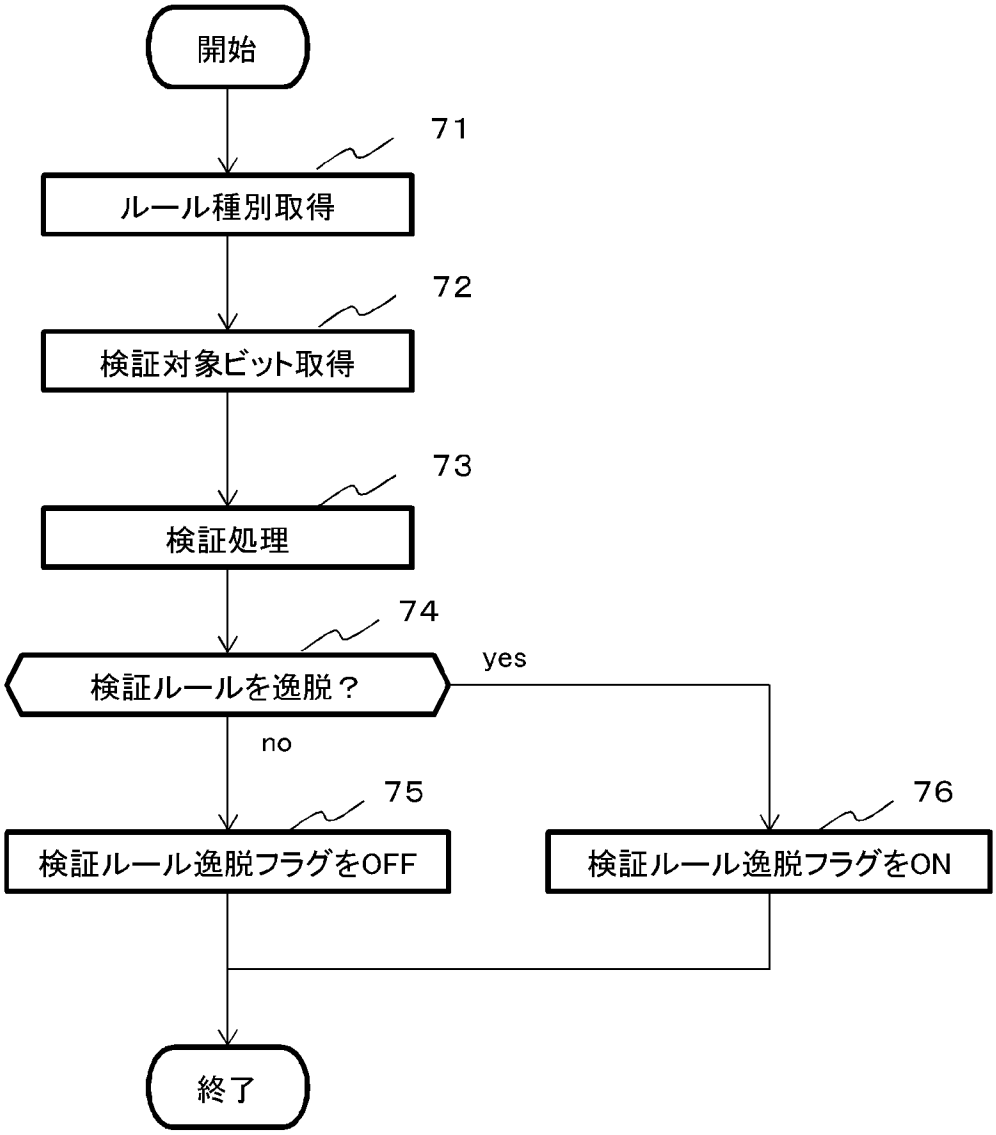
[図6]

【図6】


開始
601
メッセージ受信
602
CRC検証
603
yes
誤りを検知したか？
no
604
制御データ復号
605
IDチェック
606
処理タイプは？
挿入
XOR
607
排他的論理和
608
不正メッセージ判定処理
609
yes
不正メッセージと判定？
no
610
同期処理要否のチェック
611
同期処理のタイミングか？
yes
612
同期メッセージ生成
613
同期メッセージ送信
no
614
制御処理
終了

[図7]

【図7】


開始
71
ルール種別取得
72
検証対象ビット取得
73
検証処理
74
検証ルールを逸脱？
yes
no
75
検証ルール逸脱フラグをOFF
76
検証ルール逸脱フラグをON
終了

[図8]

【図8】

81

検証ルール情報

811 CAN－ID	812 処理タイプ	813 ルール種別	814 検証対象ビット
0x2D1	挿入	カウンタ	{30、・・・、63}
0x401	挿入	カウンタ	{0、・・・、15}
0x601	XOR	固定	{36、・・・、52}
0xD02	XOR	レンジ	{0、623343}
0xEE1	XOR	チェックサム	{56、・・・、63}
・・・		・・・	・・・

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/081082

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/36(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)
H04L9/36, 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	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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 2000-514625 A (Gemplus S.C.A.), 31 October 2000 (31.10.2000), pages 10 to 33; fig. 1 to 4 & US 6367014 B1 columns 1 to 18; fig. 1 to 4 & WO 1998/003026 A1 & EP 910923 A1 & CA 2259287 A & AU 721223 B & CN 1230324 A	1-3,10-12 4,6-8 5,9
Y A	JP 2012-249107 A (Toshiba Corp.), 13 December 2012 (13.12.2012), paragraphs [0107] to [0124] (Family: none)	4,6-8 5,9

☒ 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	Date of mailing of the international search report
16 November 2016 (16.11.16)	29 November 2016 (29.11.16)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/081082

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2009-164695 A (Fujitsu Ltd.), 23 July 2009 (23.07.2009), paragraphs [0046] to [0062]; fig. 4 & US 2009/0169009 A1 paragraphs [0109] to [0125]; fig. 4 & EP 2076072 A2	7 5,9
Y A	JP 2009-508390 A (Telefonaktiebolaget LM Ericsson (publ)), 26 February 2009 (26.02.2009), paragraphs [0015] to [0024] & US 2007/0113085 A1 paragraphs [0017] to [0026] & WO 2007/030074 A1 & EP 1922836 A1 & DE 602006008487 D & CA 2616153 A & CN 101258706 A & AT 439711 T & BR PI0615628 A	8 5,9
P,X	JP 2016-21700 A (Hitachi, Ltd.), 04 February 2016 (04.02.2016), paragraphs [0028], [0049], [0125] (Family: none)	1,10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０８１０８２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/36(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（ＩＰＣ））

Int.Cl.　H04L9/36, 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	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１６年
日本国実用新案登録公報	１９９６－２０１６年
日本国登録実用新案公報	１９９４－２０１６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 Y A	JP 2000-514625 A (ジェムプリュス　エス．セー．アー．) 2000.10.31, 10－33頁, 図1－4 & US 6367014 B1, 1-18欄, FIG.1-4 & WO 1998/003026 A1 & EP 910923 A1 & CA 2259287 A & AU 721223 B & CN 1230324 A	1-3, 10-12 4, 6-8 5, 9
Y A	JP 2012-249107 A (株式会社東芝) 2012.12.13, 段落［0107］－［0124］ (ファミリーなし)	4, 6-8 5, 9

☑　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	国際調査報告の発送日
１６．１１．２０１６	２９．１１．２０１６

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）　５Ｓ　６３０４
青木　重徳
電話番号　０３－３５８１－１１０１　内線　３５４６

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
Y A	JP 2009-164695 A (富士通株式会社) 2009.07.23, 段落 [0046] － [0062], 図 4 & US 2009/0169009 A1, 段落 [0109] － [0125], FIG.4 & EP 2076072 A2	7 5, 9
Y A	JP 2009-508390 A (テレフオンアクチーボラゲット　エル　エム　エリクソン（パブル）) 2009.02.26, 段落 [0015] － [0024] & US 2007/0113085 A1, 段落 [0017] － [0026] & WO 2007/030074 A1 & EP 1922836 A1 & DE 602006008487 D & CA 2616153 A & CN 101258706 A & AT 439711 T & BR PI0615628 A	8 5, 9
P, X	JP 2016-21700 A (株式会社日立製作所) 2016.02.04, 段落 [0028], [0049], [0125] (ファミリーなし)	1, 10