(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6534913号
(P6534913)
(45)発行日　令和1年6月26日(2019.6.26)　(24)登録日　令和1年6月7日(2019.6.7)

(51)Int.Cl.		F I		
H04L 9/36	(2006.01)	H04L	9/00	685
G06F 21/64	(2013.01)	G06F	21/64	
G09C 1/00	(2006.01)	G09C	1/00	640D

請求項の数 8　(全 15 頁)

(21)出願番号　特願2015-218336(P2015-218336)
(22)出願日　平成27年11月6日(2015.11.6)
(65)公開番号　特開2017-92634(P2017-92634A)
(43)公開日　平成29年5月25日(2017.5.25)
審査請求日　平成30年4月24日(2018.4.24)

(73)特許権者　509186579
日立オートモティブシステムズ株式会社
茨城県ひたちなか市高場２５２０番地
(74)代理人　110002365
特許業務法人サンネクスト国際特許事務所
(72)発明者　森田　伸義
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
(72)発明者　萱島　信
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
(72)発明者　井手口　恒太
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

最終頁に続く

(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

(57)【特許請求の範囲】
【請求項１】
通信メッセージの新しさに関する情報である最新性情報を算出可能な情報を予め共有し相互に通信を行う情報処理装置であって、
前記最新性情報と制御データとの排他的論理和の演算結果を用いて前記通信メッセージを生成する通信メッセージ制御部と、
他の前記情報処理装置から受信した前記通信メッセージに基づく情報と前記最新性情報との排他的論理和の演算結果である評価対象を用いて前記通信メッセージが不正か否かを判断する不正メッセージ検証部とを備え、
前記通信メッセージには、前記制御データの種類を示す情報が含まれ、
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をさらに備え、
前記不正メッセージ検証部は、受信した前記通信メッセージに含まれる前記制御データの種類を特定し、特定した前記制御データの種類および前記検証ルールに基づいて前記評価対象の特定のビットを検証する情報処理装置。
【請求項２】
請求項１に記載の情報処理装置において、
前記不正メッセージ検証部は、前記検証ルールとして、前記評価対象の特定のビットの最小値および最大値を用いた検証、前記評価対象の特定のビットの値が予め決められた値との一致を判断する検証、前記評価対象の特定のビット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、前記通信メッセージが不正か否かを判断する情報処理装置。
【請求項３】
請求項２に記載の情報処理装置において、
前記通信メッセージを受信するたびに前記最新性情報を更新する最新性情報管理部と、
前記不正メッセージ検証部により前記通信メッセージが不正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とをさらに備える情報処理装置。
【請求項４】
請求項２に記載の情報処理装置において、
前記通信メッセージを受信するたびに前記最新性情報を更新する最新性情報管理部と、
前記不正メッセージ検証部による判断結果に関わらず、更新した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とをさらに備える情報処理装置。
【請求項５】
通信メッセージの新しさに関する情報である最新性情報を算出可能な情報を予め共有し相互に通信を行う情報処理装置が実行する不正メッセージ検知方法であって、
前記最新性情報と制御データとの排他的論理和の演算結果を用いて前記通信メッセージを生成することと、
他の前記情報処理装置から受信した前記通信メッセージに基づく情報と前記最新性情報との排他的論理和の演算結果である評価対象を用いて前記通信メッセージが不正か否かを判断することとを含み、
前記通信メッセージには、前記制御データの種類を示す情報が含まれ、
それぞれの情報処理装置は、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をさらに備え、
受信した前記通信メッセージに含まれる前記制御データの種類を特定し、特定した前記制御データの種類および前記検証ルールに基づいて前記評価対象の特定のビットを検証する不正メッセージ検知方法。
【請求項６】
請求項５に記載の不正メッセージ検知方法において、
前記検証ルールとして、前記評価対象の特定のビットの最小値および最大値を用いた検証、前記評価対象の特定のビットの値が予め決められた値との一致を判断する検証、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ことをさらに含む不正メッセージ検知方法。
【請求項７】
請求項６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を受信するたびに前記最新性情報を更新することと、
前記制御データが正当なデータでないと判定する場合に、更新した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ことをさらに含む不正メッセージ検知方法。
【請求項８】
請求項６に記載の不正メッセージ検知方法において、
所定の周期で前記最新性情報を更新することと、
前記通信メッセージが不正か否かの判断結果に関わらず、更新した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こととをさらに含む不正メッセージ検知方法。
【発明の詳細な説明】
【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】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の態様による情報処理装置は、通信メッセージの新しさに関する情報である最新性情報を算出可能な情報を予め共有し相互に通信を行う情報処理装置であって、前記最新性情報と制御データとの排他的論理和の演算結果を用いて前記通信メッセージを生成する通信メッセージ制御部と、他の前記情報処理装置から受信した前記通信メッセージに基づく情報と前記最新性情報との排他的論理和の演算結果である評価対象を用いて前記通信メッセージが不正か否かを判断する不正メッセージ検証部とを備え、前記通信メッセージには、前記制御データの種類を示す情報が含まれ、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をさらに備え、前記不正メッセージ検証部は、受信した前記通信メッセージに含まれる前記制御データの種類を特定し、特定した前記制御データの種類および前記検証ルールに基づいて前記評価対象の特定のビットを検証する。

本発明の第２の態様による不正メッセージ検知方法は、通信メッセージの新しさに関する情報である最新性情報を算出可能な情報を予め共有し相互に通信を行う情報処理装置が実行する不正メッセージ検知方法であって、前記最新性情報と制御データとの排他的論理和の演算結果を用いて前記通信メッセージを生成することと、他の前記情報処理装置から受信した前記通信メッセージに基づく情報と前記最新性情報との排他的論理和の演算結果である評価対象を用いて前記通信メッセージが不正か否かを判断することとを含み、前記

通信メッセージには、前記制御データの種類を示す情報が含まれ、それぞれの情報処理装置は、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をさらに備え、受信した前記通信メッセージに含まれる前記制御データの種類を特定し、特定した前記制御データの種類および前記検証ルールに基づいて前記評価対象の特定のビットを検証する。

【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。

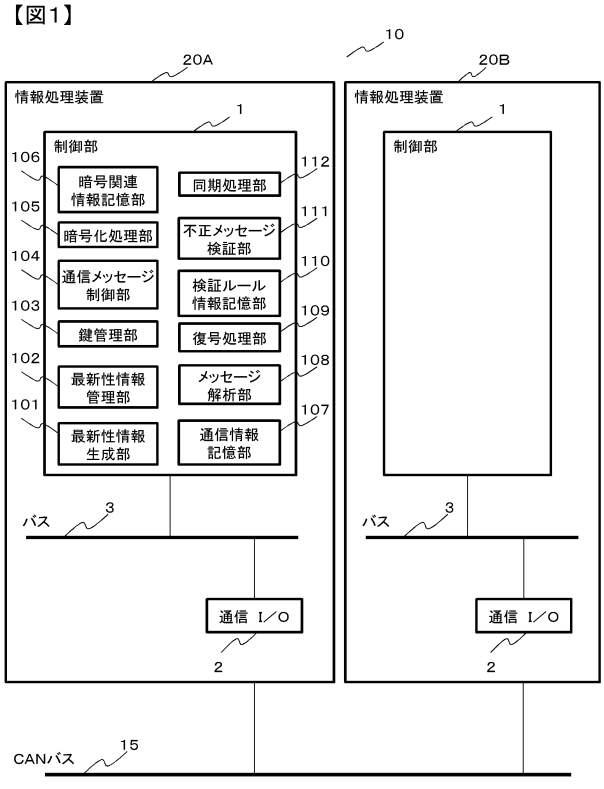
【符号の説明】

【００５９】

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

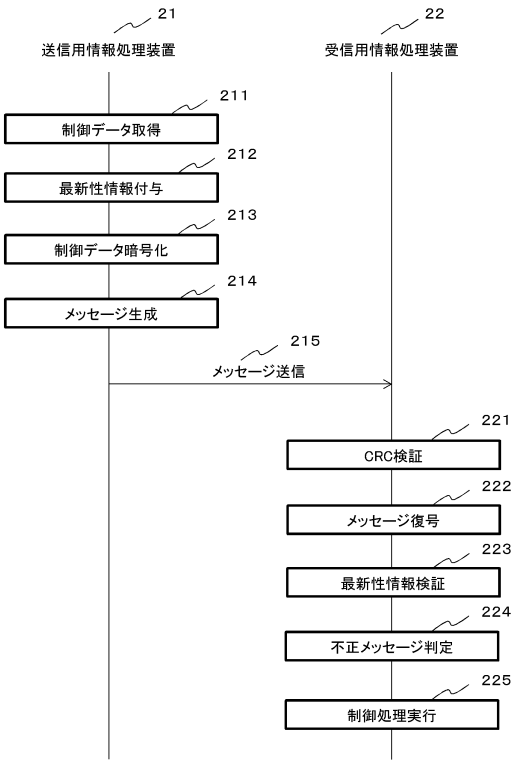
【図１】

【図1】



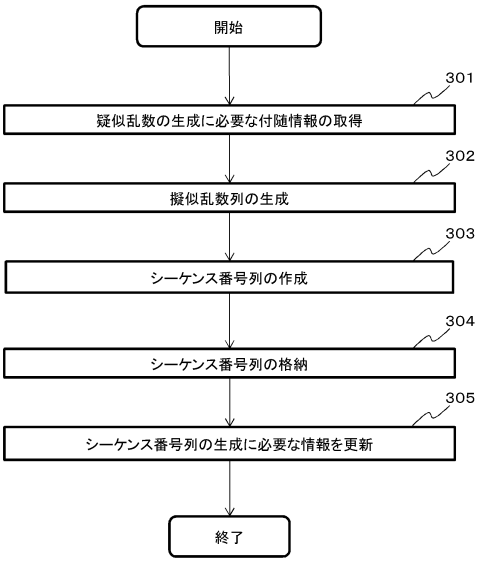
【図２】

【図2】



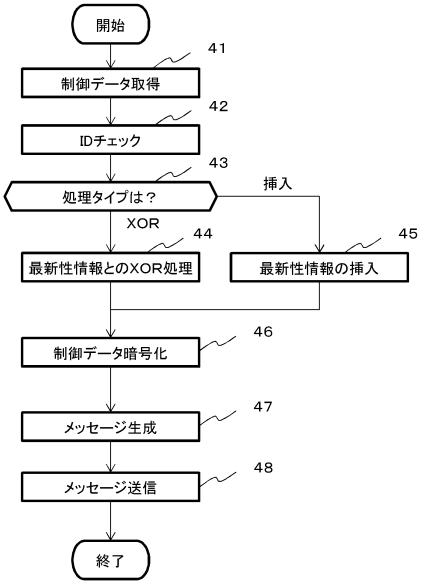
【図３】

【図3】



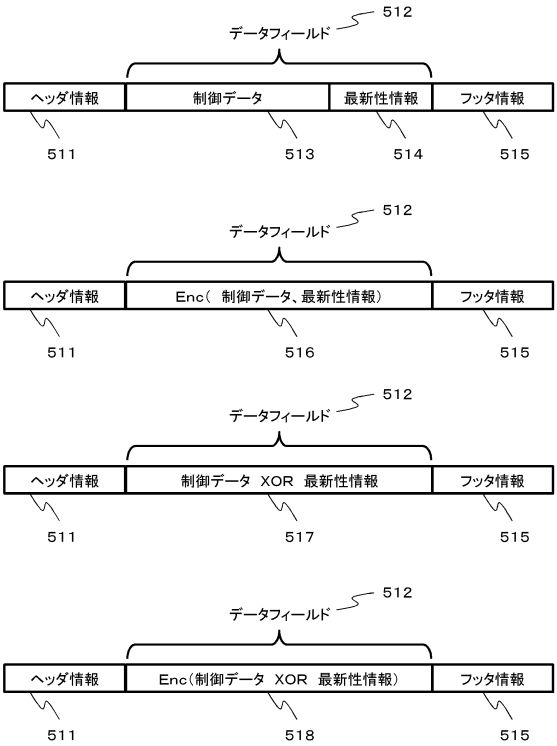
【図４】

【図4】



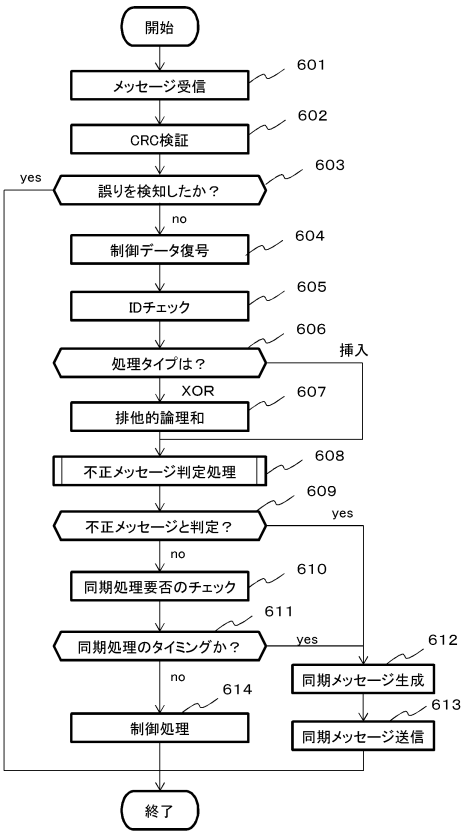
【図５】

【図5】



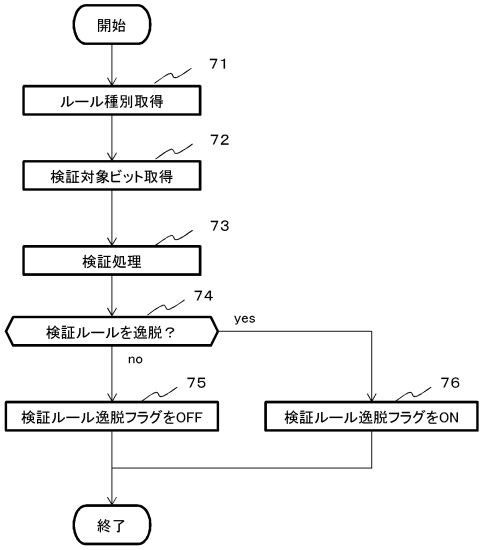
【図６】

【図6】



【図７】

【図7】



【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}
･･･		･･･	･･･

フロントページの続き

(72)発明者　大和田　徹
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

審査官　行田　悦資

(56)参考文献　特開２０１３－０４８３７４（ＪＰ，Ａ）
特開平１０－１９０６５１（ＪＰ，Ａ）
特開２０１６－０２１７００（ＪＰ，Ａ）
特表２０００－５１４６２５（ＪＰ，Ａ）
特開２０１２－２４９１０７（ＪＰ，Ａ）
特開２００９－１６４６９５（ＪＰ，Ａ）
特表２００９－５０８３９０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３６
Ｇ０６Ｆ　２１／６４
Ｇ０９Ｃ　　１／００