

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6846706号
(P6846706)

(45) 発行日 令和3年3月24日 (2021.3.24)

(24) 登録日 令和3年3月4日 (2021.3.4)

(51) Int.Cl. F I
H O 4 L 12/28 (2006.01) H O 4 L 12/28 2 O O M

請求項の数 22 (全 33 頁)

(21) 出願番号	特願2017-56570 (P2017-56570)	(73) 特許権者	314012076
(22) 出願日	平成29年3月22日 (2017.3.22)		パナソニック I P マネジメント株式会社
(65) 公開番号	特開2018-160786 (P2018-160786A)		大阪府大阪市中央区城見2丁目1番61号
(43) 公開日	平成30年10月11日 (2018.10.11)	(74) 代理人	100123102
審査請求日	令和1年12月16日 (2019.12.16)		弁理士 宗田 悟志
		(72) 発明者	安齋 潤
			大阪府門真市大字門真1006番地 パナ
			ソニック株式会社内
		(72) 発明者	芳賀 智之
			大阪府門真市大字門真1006番地 パナ
			ソニック株式会社内
		審査官	宮島 郁美
最終頁に続く			

(54) 【発明の名称】 監視装置、監視方法およびコンピュータプログラム

(57) 【特許請求の範囲】

【請求項1】

通信網からフレームを受信する受信部と、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定とを行い、前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理部と、

を備え、

前記第1判定により判定対象フレームが正当と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合、前記処理部は、前記判定対象フレームに関する情報を通報する優先度を、他の通信より高い優先度に設定する、

監視装置。

【請求項2】

通信網からフレームを受信する受信部と、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定とを行い、前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理部と、

10

20

を備え、

前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合、前記処理部は、前記判定対象フレームに関する情報を通報する優先度を、他の通信より低い優先度に設定する、

監視装置。

【請求項3】

通信網からフレームを受信する受信部と、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定とを行い、前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理部と、

を備え、

前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対象フレームが正当と判定された場合、前記処理部は、前記判定対象フレームに関する情報を通報する優先度を、前記第1判定により判定対象フレームが正当と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合より低い優先度であり、かつ、前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合より高い優先度に設定する、

監視装置。

【請求項4】

前記第1判定により判定対象フレームが正当と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合、前記処理部は、少なくとも前記判定対象フレームに含まれるコマンドの情報および前記判定対象フレームの送信元装置の情報を通報する、

請求項1に記載の監視装置。

【請求項5】

前記第1判定により判定対象フレームが正当と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合であって、かつ、前記判定対象フレームと同じIDのフレームの受信頻度が所定値を超える場合、前記処理部は、少なくとも前記判定対象フレームに含まれるコマンドの情報を通報する、

請求項1に記載の監視装置。

【請求項6】

前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合、前記処理部は、少なくとも前記判定対象フレームに含まれるコマンドの情報を通報する、

請求項1または2に記載の監視装置。

【請求項7】

前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対象フレームが正当と判定された場合、前記処理部は、少なくとも前記判定対象フレームに含まれるコマンドの情報および当該コマンドに関連する他のコマンドの情報を通報する、

請求項1から3のいずれかに記載の監視装置。

【請求項8】

通信網からフレームを受信する受信部と、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定とを行い、前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理部と、

を備え、

前記第 1 判定の対象外となったフレームが前記第 2 判定により不正と判定された場合であって、かつ、前記フレームと同じ I D のフレームの受信頻度が所定値に整合する場合、前記処理部は、他の通信より低い優先度で、少なくとも前記フレームに含まれるコマンドの情報および前記フレームの送信元装置の情報を通報する、

監視装置。

【請求項 9】

通信網からフレームを受信する受信部と、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第 1 判定と、前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第 2 判定とを行い、前記第 1 判定の結果と前記第 2 判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理部と、

を備え、

前記第 1 判定の対象外となったフレームが前記第 2 判定により不正と判定された場合であって、かつ、前記フレームと同じ I D のフレームの受信頻度が所定値を超える場合、前記処理部は、他の通信より低い優先度で、少なくとも前記フレームに含まれるコマンドの情報を通報する、

監視装置。

【請求項 10】

通信網からフレームを受信する受信部と、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第 1 判定と、前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第 2 判定とを行い、前記第 1 判定の結果と前記第 2 判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理部と、

を備え、

前記処理部は、判定対象フレームの態様と、予め定められた複数のルールとに基づいて、複数の中間判定を実行し、複数の中間判定の結果に応じて前記第 2 判定の結果を導出し、

前記処理部は、前記複数の中間判定の結果の中にルールに不適合であることを示す結果が存在する場合、前記複数の中間判定の結果を外部装置へ通報し、前記ルールに不適合であることを示す結果の数に応じて、通報の優先度を変更する、

監視装置。

【請求項 11】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第 1 判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第 2 判定と、を行い、

前記第 1 判定の結果と前記第 2 判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータが実行し、

前記第 1 判定により判定対象フレームが正当と判定され、前記第 2 判定により前記判定対象フレームが不正と判定された場合、前記処理は、前記判定対象フレームに関する情報を通報する優先度を、他の通信より高い優先度に設定する処理を含む、

監視方法。

【請求項 12】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第 1 判定と、

10

20

30

40

50

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータが実行し、

前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合、前記処理は、前記判定対象フレームに関する情報を通報する優先度を、他の通信より低い優先度に設定する処理を含む、

監視方法。

【請求項13】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータが実行し、

前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対象フレームが正当と判定された場合、前記処理は、前記判定対象フレームに関する情報を通報する優先度を、前記第1判定により判定対象フレームが正当と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合より低い優先度であり、かつ、前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合より高い優先度に設定する処理を含む、

監視方法。

【請求項14】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータが実行し、

前記第1判定の対象外となったフレームが前記第2判定により不正と判定された場合であって、かつ、前記フレームと同じIDのフレームの受信頻度が所定値に整合する場合、前記処理は、他の通信より低い優先度で、少なくとも前記フレームに含まれるコマンドの情報および前記フレームの送信元装置の情報を通報する処理を含む、

監視方法。

【請求項15】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータが実行し、

前記第1判定の対象外となったフレームが前記第2判定により不正と判定された場合であって、かつ、前記フレームと同じIDのフレームの受信頻度が所定値を超える場合、前

10

20

30

40

50

記処理は、他の通信より低い優先度で、少なくとも前記フレームに含まれるコマンドの情報を通報する処理を含む、

監視方法。

【請求項 16】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータが実行し、

前記処理は、判定対象フレームの態様と、予め定められた複数のルールとに基づいて、複数の中間判定を実行し、複数の中間判定の結果に応じて前記第2判定の結果を導出する処理を含み、

前記処理は、前記複数の中間判定の結果の中にルールに不適合であることを示す結果が存在する場合、前記複数の中間判定の結果を外部装置へ通報し、前記ルールに不適合であることを示す結果の数に応じて、通報の優先度を変更する処理をさらに含む、

監視方法。

【請求項 17】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータに実行させ、

前記第1判定により判定対象フレームが正当と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合、前記処理は、前記判定対象フレームに関する情報を通報する優先度を、他の通信より高い優先度に設定する処理を含む、

コンピュータプログラム。

【請求項 18】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータに実行させ、

前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対象フレームが不正と判定された場合、前記処理は、前記判定対象フレームに関する情報を通報する優先度を、他の通信より低い優先度に設定する処理を含む、

コンピュータプログラム。

【請求項 19】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定

10

20

30

40

50

する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報する
内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータに実行させ、

前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定
対象フレームが正当と判定された場合、前記処理は、前記判定対象フレームに関する情報
を通報する優先度を、前記第1判定により判定対象フレームが正当と判定され、前記第2
判定により前記判定対象フレームが不正と判定された場合より低い優先度であり、かつ、
前記第1判定により判定対象フレームが不正と判定され、前記第2判定により前記判定対
象フレームが不正と判定された場合より高い優先度に設定する処理を含む、

10

コンピュータプログラム。

【請求項20】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定す
る第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定
する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報す
る内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータに実行させ、

20

前記第1判定の対象外となったフレームが前記第2判定により不正と判定された場合で
あって、かつ、前記フレームと同じIDのフレームの受信頻度が所定値に整合する場合、
前記処理は、他の通信より低い優先度で、少なくとも前記フレームに含まれるコマンドの
情報および前記フレームの送信元装置の情報を通報する処理を含む、

コンピュータプログラム。

【請求項21】

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定す
る第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定
する第2判定と、を行い、

30

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報す
る内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータに実行させ、

前記第1判定の対象外となったフレームが前記第2判定により不正と判定された場合で
あって、かつ、前記フレームと同じIDのフレームの受信頻度が所定値を超える場合、前
記処理は、他の通信より低い優先度で、少なくとも前記フレームに含まれるコマンドの情
報を通報する処理を含む、

コンピュータプログラム。

【請求項22】

40

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定す
る第1判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定
する第2判定と、を行い、

前記第1判定の結果と前記第2判定の結果との組み合わせに応じて、外部装置へ通報す
る内容または通報の優先度の少なくとも一方を変更する処理、

をコンピュータに実行させ、

前記処理は、判定対象フレームの態様と、予め定められた複数のルールとに基づいて、
複数の中間判定を実行し、複数の中間判定の結果に応じて前記第2判定の結果を導出する

50

処理を含み、

前記処理は、前記複数の中間判定の結果の中にルールに不適合であることを示す結果が存在する場合、前記複数の中間判定の結果を外部装置へ通報し、前記ルールに不適合であることを示す結果の数に応じて、通報の優先度を変更する処理をさらに含む、

コンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明はデータ処理技術に関し、特に監視装置、監視方法およびコンピュータプログラムに関する。

10

【背景技術】

【0002】

近年、自動車には、多数の電子制御ユニット（Electronic Control Unit、以下「ECU」と呼ぶ。）が搭載されている。これらのECUを繋ぐネットワークは車載ネットワークと呼ばれる。車載ネットワークには多数の規格が存在するが、広く普及した規格としてCAN（Controller Area Network）がある。

【0003】

自動車の電動化に伴い、車載ネットワーク経由でステアリング等のアクチュエータを制御することが可能である。一方で、車載ネットワークで不正コマンドが伝送されることによるアクチュエータの不正操作等を防止するため、メッセージ認証コード（Message Authentication Code、以下「MAC」と呼ぶ。）を用いたメッセージ認証が実行されることがある（例えば特許文献1参照）。

20

【先行技術文献】

【特許文献】

【0004】

【特許文献1】国際公開第2013/065689号

【発明の概要】

【発明が解決しようとする課題】

【0005】

今後、インターネットへ常時接続される車両の普及に伴い、インターネットを介して車両と接続された装置群（以下「クラウド」とも呼ぶ。）が、車両のセキュリティ状態を常時監視することが考えられる。このようなクラウドサービスを利用する車両は、自車のセキュリティ状態をクラウドへ通報する必要があるが、通信量が過度に増加することは好ましくない。

30

【0006】

本願発明は上記課題に鑑みたもので、1つの目的は、自装置のセキュリティ状態に応じた適切な内容またはタイミングで、外部装置への通報を実現することである。

【課題を解決するための手段】

【0007】

上記課題を解決するために、本発明のある態様の監視装置は、通信網からフレームを受信する受信部と、フレームに対するメッセージ認証の結果に基づいてフレームが不正かを判定する第1判定と、フレームの態様と予め定められたルールとに基づいてフレームが不正かを判定する第2判定とを行い、第1判定の結果と第2判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理部と、を備える。

40

【0008】

本発明の別の態様は、監視方法である。この方法は、通信網からフレームを受信し、フレームに対するメッセージ認証の結果に基づいてフレームが不正かを判定する第1判定と、フレームの態様と予め定められたルールとに基づいてフレームが不正かを判定する第2判定と、を行い、第1判定の結果と第2判定の結果との組み合わせに応じて、外部装置へ

50

通報する内容または通報の優先度の少なくとも一方を変更する、ことをコンピュータが実行する。

【0009】

なお、以上の構成要素の任意の組合せ、本発明の表現を、コンピュータプログラム、コンピュータプログラムを記録した記録媒体、本装置を搭載した車両などの間で変換したものもまた、本発明の態様として有効である。

【発明の効果】

【0010】

本発明によれば、自装置のセキュリティ状態に応じた適切な内容またはタイミングで、外部装置への通報を実現することができる。

10

【図面の簡単な説明】

【0011】

【図1】第1実施例の車載ネットワークシステムの構成を示す図である。

【図2】図1のCGWの機能構成を示すブロック図である。

【図3】図1のECUの機能構成を示すブロック図である。

【図4】不正検出パターン別の不正対策を示す図である。

【図5】図1のCGWの動作を示すフローチャートである。

【図6】図1のECUの動作を示すフローチャートである。

【図7】変形例のCGWのハードウェア構成を示す図である。

【図8】第2実施例の車載ネットワークシステムの構成を示す図である。

20

【図9】図8のECUの機能構成を示すブロック図である。

【図10】不正検出パターンを示す図である。

【図11】図8のECUの動作を示すフローチャートである。

【発明を実施するための形態】

【0012】

[第1実施例]

第1実施例の詳細な構成を説明する前にまず概要を述べる。実施例の車載ネットワークシステムでは、MACを用いたメッセージ認証（以下「MAC検証」とも呼ぶ。）と、車載ネットワークを流れるフレーム（言い換えればコマンド）に対する振る舞い検証を併用する。振る舞い検証は、振る舞い検知技術と言え、侵入検知技術とも言える。振る舞い検証には、例えば「特開2014-146868号公報」に記載された技術を適用してもよい。実施例の車載ネットワークシステムでは、MAC検証の結果と、振る舞い検証の結果の両方を総合的に判断して、不正対策アクション（言い換えれば防御アクション）を実行する。

30

【0013】

図1は、第1実施例の車載ネットワークシステムの構成を示す。実施例の車載ネットワークシステム12は、車両10に構築された通信システムであり、車載ネットワークにおける不正検知システムとしての機能を備える。車載ネットワークシステム12は、ECU14で総称されるECU14a、ECU14b、ECU14c、ECU14d、IVI装置16、OBDアダプタ18、CGW20、CMI22を備える。これらの装置はCAN24を介して接続される。

40

【0014】

複数のECU14のそれぞれは、不図示のセンサまたはアクチュエータに接続され、センサによる検知内容を示すフレームをCAN24へ送信し、または、CAN24から受信したフレームが示すコマンドに基づいてアクチュエータを制御する。CAN24の複数のバスのうちパワートレインバス26aに接続されるECU14aは、例えばエンジンECUである。また、運転支援バス26bに接続されるECU14bは、例えばステアリングECUである。また、シャーシバス26cに接続されるECU14cは、例えばサスペンションECUである。また、ボディバス26dに接続されるECU14dは、例えばパワーウィンドウECUである。

50

【0015】

I V I (In-Vehicle Infotainment) 装置 16 は、様々な情報を乗員へ提示する情報機器であり、例えばカーナビゲーション装置である。I V I 装置 16 は、車両 10 外部の通信網 (インターネット等) である外部通信網 28 と接続される。車両 10 は、外部通信網 28 を介してルール生成装置 29 と接続される。ルール生成装置 29 は、後述の振る舞いルールを生成するサーバである。O B D アダプタ 18 は、C A N 24 を流れる様々な情報、例えば車両 10 の動作状態を示す情報を外部装置へ出力するアダプタである。I V I 装置 16 および O B D アダプタ 18 は、C A N 24 の複数のバスのうち外部バス 26 e に接続される。外部バス 26 e は、E C U 14 以外の装置から送信されたフレームが流れるバスである。外部バス 26 e を流れるフレームは、例えば、外部通信網 28 側の装置から送信されたフレーム、および、O B D アダプタ 18 に接続された装置から送信されたフレームを含む。

10

【0016】

C G W (Central GateWay) 20 は、C A N 24 の複数のバスに接続され、バス間でのフレームの中継処理およびルーティング処理を実行するゲートウェイ E C U である。C M I (Centralized Monitoring and Interceptor) 22 は、C A N 24 の複数のバスに接続され、各バスを流れるフレームを監視する E C U である。変形例として、C M I 22 が C A N 24 に非接続の構成であってもよく、言い換えれば、車載ネットワークシステム 12 は、C M I 22 を備えなくてもよい。

20

【0017】

実施例では、M A C を用いたメッセージ認証に対応する複数の装置に監視モジュールが導入される。具体的には、C G W 20 と一部の E C U 14 に監視モジュールが導入される。監視モジュールが導入された C G W 20 と E C U 14 は、C A N 24 を流れる不正フレーム (言い換えれば不正コマンド) を監視し、不正対策を実行する監視装置として機能する。変形例として、(1) C G W 20 にのみ監視モジュールを導入する構成でもよく、(2) C M I 22 にのみ監視モジュールを導入する構成でもよく、(3) M A C を用いたメッセージ認証に対応する E C U 14 にのみ監視モジュールを導入する構成でもよい。

20

【0018】

図 2 は、図 1 の C G W 20 の機能構成を示すブロック図である。C G W 20 は、フレーム受信部 30、フレーム送信部 32、M A C 検証部 34、振る舞い検証部 36、不正対策部 38 を備える。なお、図 1 の C M I 22 が監視モジュールを備える場合、C M I 22 の機能構成は図 2 と同様になる。また、M A C 検証部 34、振る舞い検証部 36、不正対策部 38 を含めて、監視モジュールとして 1 つの処理部を構成してもよい。

30

【0019】

本明細書のブロック図において示される各ブロックは、ハードウェア的には、コンピュータの C P U ・メモリをはじめとする素子や機械装置で実現でき、ソフトウェア的にはコンピュータプログラム等によって実現されるが、ここでは、それらの連携によって実現される機能ブロックを描いている。これらの機能ブロックはハードウェア、ソフトウェアの組合せによっていろいろなかたちで実現できることは、当業者には理解されるところである。例えば、図 2 の各ブロックに対応するモジュールを含むコンピュータプログラムが C G W 20 のメモリに格納されてもよい。C G W 20 の C P U は、そのコンピュータプログラムを適宜読み出して実行することにより、各ブロックの機能を発揮してもよい。

40

【0020】

フレーム受信部 30 は、C A N 24 の各バスからフレームを受信する。フレーム受信部 30 は、受信したフレームのデータを、当該フレームを受信したバスの識別情報とともに M A C 検証部 34、振る舞い検証部 36 を経て、不正対策部 38 へ入力する。フレーム送信部 32 は、C A N 24 の各バスへフレームを送信する。例えば、フレーム送信部 32 は、あるバスから受信したフレームを、そのバスを除く他のバスへ転送する。

【0021】

M A C 検証部 34 は、フレーム受信部 30 により受信されたフレーム (以下「対象フレ

50

ーム」とも呼ぶ。)に対するメッセージ認証を実行する。例えば、MAC検証部34は、予め定められたメッセージ認証用の共通鍵(以下「MAC鍵」と呼ぶ。)に基づいてMACを生成する。MAC検証部34は、生成したMACと、予め送信元装置(例えばECU14)が対象フレームに付加したMACとを比較する。MAC検証部34は、両者のMACが一致する場合、メッセージ認証に成功したと判定し、両者のMACが不一致の場合、メッセージ認証に失敗したと判定する。MAC検証部34は、メッセージ認証に成功した場合、対象フレームを正当と判定し、メッセージ認証に失敗した場合、対象フレームを不正と判定する。

【0022】

振る舞い検証部36は、振る舞い検証処理として、対象フレームの態様と予め定められた振る舞いルールとに基づいて、対象フレームが不正か否かを判定する。振る舞い検証部36は、ルール生成装置29から提供された振る舞いルールを所定の記憶領域に保持する。振る舞いルールは、フレーム(言い換えればメッセージ)のフォーマットに関する規定を含む。フォーマットに関する規定は、具体的には、ID・DLC(データ長コード)・ペイロード等における固定値の規定を含む。例えば、振る舞いルールは、フレームの所定位置に特定の固定値が設定されることを規定してもよい。

【0023】

また、振る舞いルールは、フレームの振る舞いに関する規定を含む。振る舞いに関する規定は、具体的には、周期・頻度・ペイロードに関する可変値の規定を含む。例えば、振る舞いルールは、複数のID(フレームIDとも言え、CAN-IDとも言える)のそれぞれについて、前回のフレーム受信から今回のフレーム受信までの時間間隔の範囲または差分の規定を含んでもよい。また、振る舞いルールは、フレームIDごとに、ペイロードの所定位置に設定されたデータ項目、または、ペイロード内の所定名称のデータ項目について、前回受信したフレームからの差分の制限(許容する範囲等)を含んでもよい。

【0024】

なお、振る舞いルールは、ブラックリストとホワイトリストのいずれも含みうる。振る舞い検証部36は、対象フレームがブラックリストとしてのルールを充足する場合、対象フレームを不正と判定する。また、振る舞い検証部36は、対象フレームがホワイトリストとしてのルールから逸脱する場合、対象フレームを不正と判定する。

【0025】

不正対策部38は、MAC検証部34による不正判定結果と、振る舞い検証部36による不正判定結果との組み合わせに応じて、対象フレームに関する処理(「コマンド対策」とも呼ぶ。)と、フレームの送信元装置に関する処理(「ECU対策」とも呼ぶ。)の少なくとも一方を実行する。なお、不正対策部38は、MAC検証と振る舞い検証の両方で対象フレームが正当と判定された場合、対象フレームをフレーム送信部32に渡してCAN24へ送信させる。

【0026】

不正対策部38は、無効化部40、受信フレーム記憶部42、ログ保存部44、ルール更新部46、構成情報記憶部48、対象検出部50、プログラム更新部52、鍵更新部54を含む。

【0027】

無効化部40は、対象フレームの無効化処理として、CAN24のバス上に存在する対象フレームを消去する処理を実行する。具体的には、無効化部40は、対象フレームに対するエラーフレームを生成し、フレーム送信部32からCAN24へエラーフレームを出力させる。これにより、CAN24上の他の装置(ECU14等)における対象フレームも無効にする。フレームの無効化処理には、非特許文献「T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi, "A Method of Preventing Unauthorized Data Transmission in Controller Area Network," Vehicular Technology Conference, 2012.」に記載の技術を適用してもよい。実施例のCGW20は、不正なフレームに対して無効化処理を実行するが、後述のECU14と同様に、不正なフレームに対して破棄処理(言い換

10

20

30

40

50

えればフィルタ処理)を実行してもよい。

【0028】

受信フレーム記憶部42は、フレーム受信部30により受信された複数のフレームを所定の記憶領域に記憶させ、蓄積する。受信フレーム記憶部42は、受信されてから所定時間(30分等)が経過したフレームを記憶領域から順次消去しても良い。受信フレーム記憶部42は、フレームのデータと、そのフレームに対するMAC検証部34による判定結果と振る舞い検証部36による判定結果を対応付けて蓄積してもよい。

【0029】

ログ保存部44は、MAC検証部34により対象フレームが不正と判定され、振る舞い検証部36により対象フレームが正当と判定された場合に、少なくとも対象フレームに関するログデータを保存する。そして、オフライン上で(例えばディーラーでのメンテナンスにおいて)、保存されたログデータを収集し、上記判定結果をルール生成装置29へ送信する。これにより、ルール生成装置29は、振る舞い検証において対象フレームが不正と判断されるように、振る舞いルールを更新する。具体的には、ログ保存部44は、受信フレーム記憶部42に保持されたフレームのうち対象フレームとIDが一致する過去のフレームと、対象フレームとを含むルール更新指示データをログデータとして保存する。例えば、対象フレームと過去のフレームはともに、ステアリングの制御コマンドを指定し、かつ、ステアリングの回動角度を指定するものであってもよい。

【0030】

過去のフレームは、MAC検証部34による判定結果と振る舞い検証部36による判定結果の組み合わせが対象フレームとは異なるフレームであってもよい。そのため、過去のフレームを含めてルール生成装置29へ提供することにより、ルール生成装置29による振る舞いルール更新を支援できる。また、ログ保存部44は、過去のフレームと対象フレームそれぞれの、MAC検証部34による判定結果と振る舞い検証部36による判定結果を、ログデータとしてルール更新指示データに含めてもよい。また、対象フレームより後に受信されたフレームのうち対象フレームとIDが一致するフレームをルール更新データに含めてもよい。

【0031】

ルール生成装置29は、生成または更新した振る舞いルールを外部通信網28を介して車両10へ配信する。ルール更新部46は、ルール生成装置29から提供された振る舞いルールをCAN24を介して取得する。そしてルール更新部46は、取得した振る舞いルールを振る舞い検証部36に渡し、振る舞い検証部36が保持する振る舞いルールを更新させる。

【0032】

構成情報記憶部48は、CAN24の様々な構成要素に関する属性情報(ここでは「構成情報」と呼ぶ。)を記憶する。実施例の構成情報は、複数のECU14のそれぞれが接続されたバスの識別情報と、複数のECU14のそれぞれが送信するフレームのIDとを含む。

【0033】

対象検出部50は、複数のECU14から送信された複数のフレームにおける不正有無に基づいて、複数のECU14の中から不正対策の対象となるECU(以下「対象ECU」と呼ぶ。)を検出する。対象検出部50は、各ECU14から送信されたフレームの不正率または不正回数に基づいて、対象ECUを検出してもよい。対象ECUは、不正なECUともいえ、不正者により乗っ取られたECUとも言える。

【0034】

実施例の対象検出部50は、MAC検証と振る舞い検証の少なくとも一方で不正と判定されたフレームについて、IDごとの不正判定回数を蓄積する。対象検出部50は、不正判定回数が予め定められた閾値(例えば5回)以上になったIDを検出し、構成情報記憶部48を参照して、そのIDのフレームを送信するECU14を対象ECUとして検出する。

10

20

30

40

50

【0035】

以下、ECU対策のための4種類の構成を説明するが、実際にはいずれか1つの対策が実行されてもよく、2つ以上の対策の組み合わせが実行されてもよい。

【0036】

(1)無効化部40は、構成情報記憶部48を参照して、対象ECUから送信されうる全てのIDのフレームを無効化する処理を実行する。(2)無効化部40は、構成情報記憶部48を参照して、対象ECUが接続されたCAN24のバスを識別し、識別したバスからフレーム受信部30が受信した全てのフレームを無効化する処理を実行する。

【0037】

(3)プログラム更新部52は、対象ECUのROMに格納されたコンピュータプログラムを更新させるための処理(すなわちリプログラミング)を実行する。例えば、CGW20は、個々のECU14ごとの正規のプログラムを予め保持し、プログラム更新部52は、対象ECU用の正規のプログラムを、対象ECUのROMに上書き保存してもよい。また、プログラム更新部52は、対象ECU用の正規のプログラムを、外部通信網28を介して外部のサーバから取得し、対象ECUのROMに上書き保存してもよい。

【0038】

(4)鍵更新部54は、複数のECU14に亘り使用される共通鍵であるMAC鍵を更新する。鍵更新部54は、更新したMAC鍵を複数のECU14へ配布する。後述するように、MAC検証の結果と振る舞い検証の結果の組み合わせに応じて、鍵更新部54は、全てのECU14へ更新したMAC鍵を送信して、全てのECU14が使用するMAC鍵を変更させる。または、鍵更新部54は、対象ECUを除く残りのECU14へ更新したMAC鍵を送信して、対象ECU以外のECU14が使用するMAC鍵を変更させる。なお、鍵更新部54は、予め定められたEUCごとに異なる鍵(MAC鍵とは異なる鍵)を使用して暗号化したMAC鍵を各ECUへ配布してもよい。

【0039】

実施例では、鍵更新部54は、MAC検証部34により対象フレームが正当と判定され、振る舞い検証部36により対象フレームが不正と判定された場合であり、かつ、対象フレームが、ECU14以外から送信されたフレームが流れるバス(実施例では外部バス26e)から受信されたものであるとき、全てのECU14が使用するMAC鍵を更新する。この判定の場合、MAC検証は成功したため、MAC鍵が漏洩している可能性がある。また、不正フレームは外部から注入されたものである。そこで、全てのECU14が使用するMAC鍵を更新することで、MAC鍵の漏洩リスクを解消し、セキュリティを向上させる。

【0040】

その一方、不正フレームが外部バス26e以外のバス(パワートレインバス26a等)から受信された場合、対象ECUが不正者により乗っ取られ、さらにMAC鍵を不正者が使用可能である状況が想定される。そこで、不正フレームが外部バス26e以外のバスから受信された場合、鍵更新部54は、対象ECU以外のECU14が使用するMAC鍵を更新する。

【0041】

図3は、図1のECU14の機能構成を示すブロック図である。図3では、図1の複数のECU14のうちMACを用いたメッセージ認証に対応するECU14の機能構成を示している。また、図3では、図2で説明したCGW20の機能ブロックと同一または対応する機能ブロックに同一の符号を付している。以下、図2に関連して説明済みの内容は適宜省略する。

【0042】

ECU14は、フレーム受信部30、フレーム送信部32、MAC検証部34、振る舞い検証部36、不正対策部38、コマンド実行部56、フレーム生成部58を備える。コマンド実行部56は、フレームで指定されたコマンドを実行する。例えば、コマンド実行部56は、自ECUに接続されたアクチュエータをコマンドにしたがって制御する。フレ

10

20

30

40

50

ーム生成部 58 は、外部装置（例えば他の ECU 14）に対するコマンドを指定したフレームを生成し、生成したフレームをフレーム送信部 32 に渡して送信させる。

【0043】

ECU 14 の不正対策部 38 は、受信フレーム記憶部 42、ログ保存部 44、ルール更新部 46、構成情報記憶部 48、対象検出部 50、プログラム更新部 52、鍵更新部 54、フィルタ部 60、モード切替部 62 を含む。フィルタ部 60 は、CGW 20 における無効化部 40 に対応し、ECU 14 のコマンド対策を実行する。具体的には、フィルタ部 60 は、不正と判定された対象フレームを破棄し、言い換えれば、対象フレームで指定されたコマンドを破棄する。例えば、フィルタ部 60 は、対象フレームのデータを ECU 14 内部のメモリ（不図示）から消去してもよい。

10

【0044】

また、ECU 14 は、既述した ECU 対策を実行する。ただし、実施例の CGW 20 における ECU 対策（1）（2）ではフレームの無効化処理を実行したが、ECU 14 における ECU 対策（1）（2）ではフレームの廃棄処理、言い換えればフィルタ処理を実行する。ECU 対策（3）（4）は CGW 20 と同様である。

【0045】

モード切替部 62 は、CGW 20 を経由して伝送されたフレームが振る舞い検証で不正と判定された場合、複数のバスに接続して車載ネットワークの要である CGW 20 のセキュリティ機能が突破されている状態であると判断し、車両 10 の自動運転のモードをフェイルセーフモードへ切り替える。例えば、モード切替部 62 は、構成情報記憶部 48 を参照して、不正と判定された対象フレームの ID に基づいて送信元の ECU 14 を特定してもよい。そして、送信元の ECU 14 が、自 ECU が接続されたバスとは異なるバスに接続されたものである場合に、モード切替部 62 は、対象フレームが CGW 20 により中継されたと判定してもよい。また、フェイルセーフモードは、自動運転制御（言い換えれば電動による運転支援処理）をオフにした状態であってもよい。

20

【0046】

CGW 20 を経由して伝送されたフレームが不正であることは、CGW 20 が不正者に乗っ取られた可能性が高いことを意味する。CAN 24 における CGW 20 は、複数の ECU 14 間の通信の基盤であり、CGW 20 が乗っ取られたことはセキュリティ上、重大な問題である。そこで、実施例のモード切替部 62 は、CGW 20 を経由して伝送されたフレームが不正である場合に自動運転をフェイルセーフモードへ移行させることで、車両運転の安全性を一層高める。なお、CMI 22 に監視モジュールが導入される場合、CMI 22 は、モード切替部 62 を備えてもよい。

30

【0047】

変形例として、CGW 20 を経由して伝送されたフレームが不正である場合に限らず、車載ネットワークシステム 12 のセキュリティの根幹装置から送信されたフレームが不正である場合に、モード切替部 62 は、車両 10 の自動運転のモードをフェイルセーフモードへ切り替えてもよい。セキュリティの根幹装置は、例えば、個々の ECU 14 ごとの鍵を保持し、ECU ごとの鍵で暗号化した MAC 鍵を各 ECU 14 へ配布する装置（CGW 20、ECU 14 等）が該当する。モード切替部 62 は、構成情報記憶部 48 を参照して、不正と判定された対象フレームの ID に基づいて、対象フレームの送信元がセキュリティの根幹装置かを判定してもよい。

40

【0048】

図 4 は、不正検出パターン別の不正対策を示す。ここでは、監視モジュールが導入される装置（ECU 14、CGW 20、CMI 22）を総称して「監視装置」と呼ぶ。図 4 のコマンド対策欄では、監視装置が ECU 14、CGW 20、CMI 22 の場合の処理をそれぞれ示している。

【0049】

MAC 検証で対象フレームが正当と判定され、振る舞い検証で対象フレームが不正と判定された場合（パターン 1 およびパターン 5）、または、MAC 検証で対象フレームが不正

50

正と判定され、振る舞い検証で対象フレームが不正と判定された場合（パターン2）、監視装置の不正対策部38は、コマンド対策として、対象フレームを破棄または無効化する。なお、パターン2において、ECU14でのコマンド対策が「なし」であるのは、メッセージ認証に対応するECU14では、通常、MAC検証のNGに伴いエラー処理が実行されるからである。また、パターン2において、CGW20のコマンド対策が無効化であるのは、DoS攻撃（Denial of Service attack）への対策として有効だからである。

【0050】

パターン1およびパターン2の場合、不正対策部38は、4種類のEUC対策のうち1つまたは複数を実行する。パターン5の場合、不正対策部38は、EUC対策として、全てのECU14のMAC鍵を更新する。

10

【0051】

MAC検証で対象フレームが不正と判定され、振る舞い検証で対象フレームが正当と判定された場合（パターン6）、監視装置の不正対策部38は、対象フレームとその前後のフレームを含むルール更新指示データをログデータとして保存することにより、ルール生成装置29に対象フレームとその前後のフレームに基づいて振る舞いルールを更新させる。例えば、ルール生成装置29は、監視装置が再度対象フレームを受け付けた場合、振る舞い検証において不正を検出するように振る舞いルールを更新する。

【0052】

図4のパターン3とパターン4は、MACを用いたメッセージ認証に対応しないECU14から送信されたフレームが不正であるパターンである。すなわち、フレームにMACが付加されないためMAC検証はできず、振る舞い検証にて不正が検出されたパターンである。なお、パターン3は、不正と判定された対象フレームがECU14から送信されたパターンであり、パターン4は、不正と判定された対象フレームが外部から注入された（言い換えれば外部バス26eから受信された）パターンである。

20

【0053】

パターン3とパターン4のいずれでも、監視装置の不正対策部38は、コマンド対策として、対象フレームを破棄または無効化する。パターン4は、不正フレームが外部注入された状況であり、MAC鍵の漏洩はないため、EUC対策は実行しない。その一方、パターン3では対象ECUが乗っ取られた可能性が高いため、不正対策部38は、パターン1等と同様のEUC対策を実行する。

30

【0054】

以上の構成による車載ネットワークシステム12の動作を説明する。図5は、図1のCGW20の動作を示すフローチャートである。フレーム受信部30は、CAN24からフレームを受信する（S10）。MAC検証部34は、受信された対象フレームに対するMAC検証を実行して、対象フレームが正当か不正かを判定する（S12）。振る舞い検証部36は、受信された対象フレームに対する振る舞い検証を実行して、対象フレームが正当か不正かを判定する（S14）。なお、S12とS14の実行順序に制限はなく、並行して実行してもよい。

【0055】

MAC検証と振る舞い検証の両方で対象フレームが正当と判定された場合（S16のY）、不正対策部38は、対象フレームをフレーム送信部32に渡し、フレーム送信部32は、フレームID、転送元バス、転送先バスを対応付けたルーティングテーブルにしたがって、対象フレームを転送する（S18）。MAC検証で対象フレームが不正と判定され、振る舞い検証で対象フレームが正当と判定された場合（S16のN、S20のY）、不正対策部38は、ルール生成装置29に振る舞いルールを更新させるためのログデータであり、対象フレームとその前後のフレームを含むログデータを保存する（S22）。MAC検証結果が不正かつ振る舞い検証結果が不正となった場合、または、MAC検証結果が正当かつ振る舞い検証結果が不正となった場合（S20のN）、不正対策部38は、図4に示したコマンド対策を実行する（S24）。

40

【0056】

50

不正検出パターン（図４）にしたがってＥＣＵ対策が必要な場合（Ｓ２６のＹ）、不正対策部３８は、乗っ取られた可能性が高い対象ＥＣＵを特定する（Ｓ２８）。不正対策部３８は、対象ＥＣＵおよび／または他のＥＣＵ１４に関するＥＣＵ対策を実行する（Ｓ３０）。ＥＣＵ対策が不要であれば（Ｓ２６のＮ）、Ｓ２８、Ｓ３０をスキップする。

【００５７】

図６は、図１のＥＣＵ１４の動作を示すフローチャートである。Ｓ４０～Ｓ４４の処理は図５のＳ１０～Ｓ１４と同じであるため説明を省略する。ＭＡＣ検証と振る舞い検証の両方で対象フレームが正当と判定された場合（Ｓ４６のＹ）、不正対策部３８は、対象フレームをコマンド実行部５６に渡し、コマンド実行部５６は、対象フレームで指定されたコマンドにしたがいデータ処理を実行する（Ｓ４８）。対象フレームがＣＧＷ２０経由のフレームであり、かつ、少なくとも振る舞い検証により不正と判定された場合（Ｓ４６のＮ、Ｓ５０のＹ）、不正対策部３８は、車両１０の自動運転をフェイルセーフモードへ移行させる（Ｓ５２）。Ｓ５０のＮ以降、Ｓ５４～Ｓ６４の処理は図５のＳ２０～Ｓ３０と同じであるため説明を省略する。

【００５８】

実施例の監視装置（例えばＥＣＵ１４、ＣＧＷ２０）によると、メッセージ認証の結果と振る舞い検証の結果との組み合わせに基づいて、セキュリティの脅威の種類をきめ細かに認識し、脅威の種類に応じた適切なコマンド対策およびＥＣＵ対策を自動実行する。これにより、車載ネットワークシステム１２のセキュリティを担保できる。例えば、ＭＡＣ鍵の漏洩、および、ＭＡＣ対応ＥＣＵの乗っ取りを検知し、ＭＡＣ鍵の更新およびＥＣＵのリプログラミングを適切に実行できる。また、車載ネットワークシステム１２内にＭＡＣ未対応のＥＣＵ１４が存在し、ＭＡＣ未対応のＥＣＵ１４が脅威にさらされた場合も、セキュリティを担保しやすくなる。

【００５９】

以上、本発明を第１実施例をもとに説明した。この実施例は例示であり、それらの各構成要素あるいは各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【００６０】

第１変形例を説明する。実施例の振る舞い検証部３６は、対象フレームを正当または不正に分類したが、変形例として、振る舞い検証部３６は、対象フレームの態様と振る舞いルールとの乖離の度合い（もしくは一致の度合い）に応じて、対象フレームを正当、不正、グレーのいずれかに分類してもよい。不正対策部３８のログ保存部４４は、対象フレームがグレーに分類された場合、対象フレームと、同じＩＤの過去のフレームとを含むルール更新指示データをログデータとして保存する。既述したように、ルール更新指示データは、対象フレームより後に受信された同ＩＤのフレームを含んでもよい。これにより、保存されたログデータはオフライン上で収集されてルール生成装置２９に通知され、ルール生成装置２９は、例えば対象フレームを不正と判定するように振る舞いルール更新する。

【００６１】

具体例として、振る舞い検証部３６は、検知パラメータＡ～Ｅのそれぞれで対象フレームを評価し、各検知パラメータによる中間判定結果Ａ～Ｅを生成し、４つ以上の中間判定結果が不正となった場合に最終判定結果を不正としてもよい。また、不正となった中間判定結果の個数が３個以下であれば最終判定結果を正当としてもよい。この構成において、振る舞い検証部３６は、各フレームで指定されるフレームＩＤ（コマンドＩＤでもよい）ごとに中間判定結果が不正となった回数を累計していく。振る舞い検証部３６は、中間判定結果が不正となった累計数が所定の閾値（例えば１０回等）を超えたＩＤのフレームをグレーと判定する。

【００６２】

また、振る舞い検証部３６は、フレームＩＤ（コマンドＩＤ）で区別せずに全てのフレームを母集団として、中間判定結果が不正となった回数を累計してもよい。振る舞い検証部３６は、中間判定結果が不正となった累計数が所定の閾値（例えば１０回等）を超えた

場合にグレーと判定してもよい。この場合、ログ保存部44は、過去の一定期間に受信した全フレームを含むルール更新指示データをログデータとして保存してもよい。

【0063】

フレームの正当性がグレーと判定されることは本来望ましくないが、第1変形例によると、振る舞いルールを適切に更新し、車載ネットワークシステム12のセキュリティを向上させることができる。なお、振る舞い検証部36は、対象フレームの振る舞い検証において、対象フレームのIDに紐付く不正判定累計数が所定の閾値を超過した場合、対象フレームの最終判定結果を「不正」としてもよい。この態様によると、グレー判定となったフレームに基づいてコマンド対策およびECU対策が実行され、車載ネットワークシステム12のセキュリティを一層高めることができる。

10

【0064】

第2変形例を説明する。図7は、変形例のCGW20のハードウェア構成を示す。CGW20は、CPU70、監視モジュール72、LANコントローラ74、LANコントローラ76を備える。LANコントローラ74およびLANコントローラ76は、CAN24の各バスに接続される。CPU70は、CGW20全体の動作を制御するとともに、図2に示した各機能ブロックの機能を実行する。

【0065】

監視モジュール72は、CPU70と物理的に異なるLSIであり、言い換えれば、CPU70と物理的に分離または独立して実装されたLSIである。監視モジュール72は、図2に示した機能ブロックのうちMAC検証部34、振る舞い検証部36、不正対策部38の機能を実行する。監視モジュール72が備える不正対策部38の機能は、図4に示したパターン別のコマンド対策およびECU対策を決定する機能を少なくとも含む。

20

【0066】

CPU70と監視モジュール72は、互いに並行して、同じ対象フレームに対する不正判定処理を実行する。監視モジュール72は、不正判定処理の結果と、CPU70におけるフレーム処理の内容に基づいて、CPU70が正常か否かを判定する。例えば、監視モジュール72は、MAC検証と振る舞い検証の少なくとも一方で対象フレームが不正と判定された場合であって、かつ、CPU70が対象フレームをCAN24へ送信した場合に、CPU70（特にCPU70のルーティング機能）が異常と判定する。また、監視モジュール72は、MAC検証と振る舞い検証の両方で対象フレームが正当と判定された場合であって、かつ、CPU70が対象フレームを破棄または無効化した場合に、CPU70が異常と判定する。

30

【0067】

CPU70が異常と判定した場合、監視モジュール72は、所定のエラー処理、リカバリ処理、乗員または外部の人等への通知処理のうち少なくとも1つを実行してもよい。第2変形例によると、CGW20のCPU70が不正者により乗っ取られた場合も、その事実を監視モジュール72により検出して、セキュリティの脅威を解消するための処理を実行可能になる。なお、CPU70と監視モジュール72は、仮想的または論理的に分離して実装されてもよい。また、ここではCGW20の例を示したが、監視装置として動作するECU14においても本変形例の構成を適用可能である。

40

【0068】

第3変形例を説明する。上記実施例では、車載ネットワークをCANとしたが、変形例として、車載ネットワークをイーサネット（登録商標）にしてもよく、この場合も、ECU14およびCGW20には実施例と同様の構成を適用できる。

【0069】

第4変形例を説明する。第3変形例に関連して、車載ネットワークにおいてCANとイーサネットが混在してもよい。監視装置としてのCGW20は、CANとイーサネットを接続し、CANのフレームとイーサネットフレームとを相互に変換する機能をさらに備えてもよい。CGW20は、MAC検証と振る舞い検証の少なくとも一方で不正と判定されたCANフレームをイーサネットフレームへ変換することを抑制する。同様に、上記不正

50

と判定されたイーサネットフレームをCANフレームへ変換することを抑制する。

【0070】

また、CGW20は、CANの複数のバスと、イーサネットの複数のバスに接続されてもよい。この場合に、或るフレームがMAC検証と振る舞い検証の少なくとも一方で不正と判定された場合、CGW20は、そのフレームが流れるバスから他のバスへの、全フレームの変換および中継を抑制してもよい。さらにまた、CGW20は、不正と判定されたフレームが流れるバスへの他のバスからの、全フレームの変換および中継を抑制してもよい。

【0071】

さらにまた、CGW20は、イーサネットにおけるセキュリティ機能（例えばファイアウォール機能、MACアドレスフィルタ等）を備えてもよい。CGW20は、イーサネットにおけるセキュリティ機能とMAC検証との少なくとも一方で対象フレームが不正と判定されたことを、実施例においてMAC検証で不正と判定した場合と同等に取り扱ってもよい。なお、CGW20は、イーサネットにおけるセキュリティ機能とMAC検証の両方で対象フレームが不正と判定された場合、不正の確度が高いと判定して、コマンド対策およびECU対策の実行に代えて、もしくはコマンド対策およびECU対策の実行とともに、車両10の自動運転のモードをフェイルセーフモードへ移行させてもよい。なお、第4変形例は、CGW20に限らず、異なる種類のネットワークを接続する装置全般に適用可能である。

【0072】

第5変形例を説明する。車載ネットワークシステム12のECU14、CGW20には、自装置の改ざん有無を判定するセキュリティチップ（Trusted Platform Module、以下「TPM」と呼ぶ。）が搭載されてもよい。監視装置（例えばCGW20、ECU14）の対象検出部50は、少なくとも振る舞い検証で不正と判定されたフレームを送信したECUのTPMに対して改ざん有無を問い合わせてもよい（Attestation）。なお、第2変形例との組み合わせ時、対象検出部50は、CGW20のSOC（System on Chip）に対して改ざん有無を問い合わせてもよい。対象検出部50は、問い合わせの結果が改ざんありを示す場合、問い合わせ先の装置（例えばCGW20、ECU14）を不正と判定し、言い換えれば、不正対策の対象装置と判定する。

【0073】

第1実施例および変形例に記載の技術は、以下の項目によって特定されてもよい。

[項目1]

通信網からフレームを受信する受信部と、フレームに対するメッセージ認証の結果に基づいてフレームが不正かを判定する第1判定と、フレームの態様と予め定められたルールとに基づいてフレームが不正かを判定する第2判定とを行い、第1判定の結果と第2判定の結果との組み合わせに応じて、フレームに関する処理とフレームの送信元装置に関する処理の少なくとも一方を実行する処理部と、を備える監視装置。

この監視装置によると、通信システムのセキュリティを向上させることができる。

[項目2]

第1判定により判定対象フレームが正当と判定され、第2判定により判定対象フレームが不正と判定された場合、または、第1判定により判定対象フレームが不正と判定され、第2判定により判定対象フレームが不正と判定された場合、処理部は、判定対象フレームを破棄または無効化する処理を実行してもよい。

この態様によると、不正なフレームによるセキュリティのリスクを低減できる。

[項目3]

第1判定により判定対象フレームが正当と判定され、第2判定により判定対象フレームが不正と判定された場合、または、第1判定により判定対象フレームが不正と判定され、第2判定により判定対象フレームが不正と判定された場合に、複数の送信元装置から送信された複数のフレームにおける不正有無に基づいて、複数の送信元装置の中から不正対策の対象装置を検出し、（1）対象装置から送信されるフレームを破棄または無効化する処

10

20

30

40

50

理、(2)対象装置におけるコンピュータプログラムを更新する処理、(3)対象装置以外の送信元装置におけるメッセージ認証の鍵を更新する処理、(4)対象装置が接続された通信網のバスから受信されたフレームを破棄または無効化する処理、のうち少なくとも1つを実行してもよい。

この態様によると、不正なフレームの検出に基づいて、フレームの送信元装置に関する不正対策を実施できる。

[項目4]

第1判定により判定対象フレームが正当と判定され、第2判定により判定対象フレームが不正と判定された場合であり、かつ、判定対象フレームが、所定の送信元装置以外から送信されたフレームが流れるバスから受信されたものであるとき、処理部は、所定の送信元装置におけるメッセージ認証の鍵を更新する処理を実行してもよい。

10

この態様によると、外部から不正なフレームが注入され、メッセージ認証の鍵が漏洩している可能性がある場合に、メッセージ認証の鍵を更新し、セキュリティのリスクを低減できる。

[項目5]

第1判定により判定対象フレームが不正と判定され、第2判定により判定対象フレームが正当と判定された場合に、処理部は、少なくとも判定対象フレームに関するログデータを保存してもよい。

この態様によると、第2判定のためのルールが不完全であることが想定される場合に、ルールの改善を支援できる。

20

[項目6]

処理部は、判定対象フレームの態様とルールとの乖離の度合いに応じて、判定対象フレームを正当、不正、グレーのいずれかに分類し、判定対象フレームがグレーに分類された場合、少なくとも判定対象フレームに関するログデータを保存してもよい。

この態様によると、本来望ましくないグレー判定に伴い、第2判定のためのルールの改善を支援できる。

[項目7]

監視装置は、車両に搭載された電子制御ユニットであってもよい。処理部は、車載ネットワークにおける所定のゲートウェイ装置を経由して伝送されたフレームが第2判定により不正と判定された場合、車両の自動運転のモードをフェイルセーフモードへ切り替えてもよい。

30

この態様によると、車両運転の安全性を一層高めることができる。

[項目8]

通信網からフレームを受信し、受信されたフレームに対するメッセージ認証の結果に基づいてフレームが不正かを判定する第1判定と、受信されたフレームの態様と予め定められたルールとに基づいてフレームが不正かを判定する第2判定と、を行い、第1判定の結果と第2判定の結果との組み合わせに応じて、受信されたフレームに関する処理と受信されたフレームの送信元装置に関する処理の少なくとも一方を実行する、ことをコンピュータが実行する監視方法。

この監視方法によると、通信システムのセキュリティを向上させることができる。

40

[項目9]

通信網からフレームを受信し、受信されたフレームに対するメッセージ認証の結果に基づいてフレームが不正かを判定する第1判定と、受信されたフレームの態様と予め定められたルールとに基づいてフレームが不正かを判定する第2判定と、を行い、第1判定の結果と第2判定の結果との組み合わせに応じて、受信されたフレームに関する処理と受信されたフレームの送信元装置に関する処理の少なくとも一方を実行する、ことをコンピュータに実行させるためのコンピュータプログラム。

このコンピュータプログラムによると、通信システムのセキュリティを向上させることができる。

【0074】

50

〔第2実施例〕

第2実施例の詳細な構成を説明する前にまず概要を述べる。コネクテッドカー等、インターネットへ常時接続される車両の普及に伴い、クラウド側で車両を常時監視し、クラウドから適切なサービスを車両へ提供することが考えられる。このようなクラウドサービスを利用する車両は、自車のセキュリティ状態をリアルタイムにクラウドへ伝える必要があるが、リアルタイム性を重視するほど通信量は増大する。そのため車両には、セキュリティ状態の検知結果に応じた適切な通信が求められる。

【0075】

第2実施例では、MAC検証の結果と、振る舞い検証の結果とに基づいて、車両のセキュリティ状態を判定し、車両のセキュリティ状態に応じて、適切なタイミングで、かつ、適切な内容をクラウドへ送信する車載ネットワークシステムを説明する。以下の図面において、第1実施例と同一または対応するブロックには、第1実施例と同一の符号を付している。また、第1実施例で説明済みの内容は適宜省略し、主に、第1実施例と異なる構成を説明する。

【0076】

図8は、第2実施例の車載ネットワークシステムの構成を示す。車載ネットワークシステム12のハードウェア構成は第1実施例と同様である。第2実施例では、車両10は、外部通信網28を介して車両監視サーバ100と接続される。

【0077】

車両監視サーバ100は、車両10のセキュリティ状態に応じたサービスを提供する。車両監視サーバ100は、第1実施例においてCGW20、ECU14等を実装された不正対策部38に対応する機能を備えてもよい。例えば、車両監視サーバ100は、車両10から通報された車両10のセキュリティ状態に応じて、ECU14のリプログラミングまたは鍵更新を車両10に指示してもよい。なお、車両監視サーバ100は、第1実施例のルール生成装置29の機能を含む。

【0078】

第2実施例の車載ネットワークシステム12では、MACを用いたメッセージ認証に対応するECU14に監視モジュールが導入される。監視モジュールが導入されたECU14は、CAN24を流れる不正フレーム（言い換えれば不正コマンド）を監視し、その監視結果を車両監視サーバ100へ通報する監視装置として機能する。変形例として、（1）CGW20にのみ監視モジュールを導入する構成でもよく、（2）CMI22にのみ監視モジュールを導入する構成でもよく、（3）CGW20と、MACを用いたメッセージ認証に対応するECU14とに監視モジュールを導入する構成でもよい。

【0079】

図9は、図8のECU14の機能構成を示すブロック図である。ECU14は、フレーム受信部30、フレーム送信部32、MAC検証部34、振る舞い検証部36、ルール更新部46、コマンド実行部56、フレーム生成部58、通報部114を備える。図8のCGW20またはCMI22が監視モジュールを備える場合も、図9と同様の構成になる。

【0080】

図9のMAC検証部34、振る舞い検証部36、ルール更新部46、通報要否判定部112、通報部114は、監視モジュールとして処理部110を構成してもよい。また、図9のフレーム受信部30、フレーム送信部32、MAC検証部34、振る舞い検証部36、ルール更新部46、コマンド実行部56、フレーム生成部58は、第1実施例と同じ機能であるため説明を省略する。

【0081】

通報部114は、CAN24から受信されたフレーム（以下「対象フレーム」とも呼ぶ。）をフレーム受信部30から受信する。また、通報部114は、対象フレームに対するMAC検証の結果をMAC検証部34から取得し、対象フレームに対する振る舞い検証の結果を振る舞い検証部36から取得する。通報部114は、対象フレームに対するMAC検証の結果と振る舞い検証の結果の組み合わせに基づいて、車両監視サーバ100へ通報

する内容または通報の優先度を設定し、また、複数の対象フレーム間で、車両監視サーバ100へ通報する内容または通報の優先度を変更する。実施例では、通報する内容と通報の優先度の両方を変更する。

【0082】

通報部114は、受信フレーム記憶部42、構成情報記憶部48、解析部120、メッセージ生成部122、メッセージ出力部124を含む。

【0083】

受信フレーム記憶部42は、フレーム受信部30により受信された複数のフレームを所定の記憶領域に記憶し、蓄積する。受信フレーム記憶部42は、受信されてから所定時間が経過したフレームを記憶領域から順次消去しても良い。受信フレーム記憶部42は、フ

10

【0084】

構成情報記憶部48は、CAN24の様々な構成要素に関する属性情報（ここでは「構成情報」と呼ぶ。）を記憶する。実施例の構成情報は、複数のECU14のIDと、複数のECU14のそれぞれが送信するフレームに含まれるコマンドのIDを含む。なお、構成情報は、コマンドのIDに代えて、フレームID（言い換えればCAN-ID）を含んでもよい。もしくは、構成情報は、コマンドのIDとともに、フレームのID（CAN-ID）を含んでもよい。

【0085】

20

また、実施例の構成情報は、複数のコマンドのIDと、各コマンドの送信頻度とを対応付けた情報を含む。コマンドの送信頻度は、送信元のECUが当該コマンドを含むフレームを送信する頻度（例えば単位時間あたりの送信個数）であってもよい。また、実施例の構成情報は、複数のコマンドのIDと、各コマンドに関連する他のコマンドのIDとを対応付けた情報を含む。特定のコマンドに関連する他のコマンドは、特定のコマンドと依存関係を有する他のコマンドでもよく、特定のコマンドと対になって送信される他のコマンドでもよい。例えば、車速制御コマンドに関連する他のコマンドは、ブレーキアクチュエータ制御コマンドでもよい。

【0086】

解析部120は、対象フレームに対するMAC検証の結果と振る舞い検証の結果との組み合わせに基づいて、対象フレームの不正検出パターンを識別する。図10は、不正検出パターンを示す。解析部120は、対象フレームの不正検出パターンとして、図10に示す7つの不正検出パターンのうちいずれかを特定する。

30

【0087】

パターン1とパターン5の識別方法を説明する。解析部120は、あるコマンドID（フレームIDでもよい）を含むフレームに対するMAC検証結果が正当（図10における「OK」）を示すと共に、振る舞い検証結果が不正（図10における「NG」）を示す場合、受信フレーム記憶部42を参照して、そのコマンドIDを含むフレームの受信頻度を特定する。特定した受信頻度が、構成情報記憶部48に記憶された当該コマンドIDの送信頻度と整合する（例えば、特定した受信頻度と当該コマンドIDの送信頻度との差異が

40

【0088】

このように識別する理由は、ECUが乗っ取られた場合（パターン1）は、送信頻度が変わらないが、不正コマンドが外部注入された場合（パターン5）は、正常なECUが送信するコマンドと外部注入されたコマンドの両方が存在することで受信頻度が高くなるからである。

【0089】

パターン3とパターン4の識別方法を説明する。パターン3またはパターン4に分類さ

50

れうる対象フレームは、M A Cのコード値が付加されていないフレームであり、言い換えれば、M A C検証部34によるM A C検証の対象外となるフレームである。解析部120は、あるコマンドID（フレームIDでもよい）を含むフレームに対するM A C検証結果がなく（図10における「n/a」）、振る舞い検証結果が不正（図10における「NG」）を示す場合、受信フレーム記憶部42を参照して、そのコマンドIDを含むフレームの受信頻度を特定する。特定した受信頻度が、構成情報記憶部48に記憶された当該コマンドIDの送信頻度と整合する場合、パターン3と識別する。その一方、特定した受信頻度が、送信頻度を上回る場合、パターン4と識別する。

【0090】

解析部120は、対象フレームの不正検出パターンとしてパターン1またはパターン3を識別した場合、乗っ取られた可能性があるE C UのIDを特定する。例えば、解析部120は、構成情報記憶部48を参照して、対象フレームが示すコマンドIDに対応づけられたE C Uを、乗っ取られた可能性があるE C Uとして特定する。なお、E C Uが乗っ取られていることは、当該E C Uで想定外のプログラムが実行されていることを含む。

【0091】

図9に戻り、メッセージ生成部122は、解析部120により識別された対象フレームの不正検出パターンに応じて、対象フレームに関する情報を車両監視サーバ100へ通報するためのメッセージを生成する。このメッセージは、車両10のセキュリティ状態を示す。メッセージ生成部122は、対象フレームの不正検出パターンに該当する図10の通報内容および付加情報をメッセージに含める。

【0092】

メッセージ生成部122は、上記メッセージをペイロードに設定したフレームであり、車両10のセキュリティ状態（具体的には不正検出状態）を車両監視サーバ100へ通報するための通報フレームを生成する。メッセージ生成部122は、上記メッセージを複数に分割し、分割後のメッセージをそれぞれ含む複数の通報フレームを生成してもよい。メッセージ出力部124は、メッセージ生成部122により生成された通報フレームをフレーム送信部32へ出力し、フレーム送信部32からCAN24へ出力させる。通報フレームは、CAN24～外部バス26e～外部通信網28を介して車両監視サーバ100へ伝送される。

【0093】

メッセージ内容の設定処理の詳細を説明する。対象フレームの不正検出パターンがパターン1であるとき、メッセージ生成部122は、図10のパターン1の通報内容をメッセージに含める。また、メッセージ生成部122は、付加情報（A）（B）（C）をメッセージに含める。なお、いずれのパターンにおいても、図10の「通報内容」欄の文章に代えて、図10の「想定される脅威」欄の文章をメッセージに含めてもよい。

【0094】

具体的には、メッセージ生成部122は、M A C検証と振る舞い検証の結果を付加情報（A）としてメッセージに含める。また、メッセージ生成部122は、対象フレームが含むコマンドIDを付加情報（B）としてメッセージに含める。また、メッセージ生成部122は、解析部120により特定されたE C U（ここでは「不正E C U」と呼ぶ。）のIDを付加情報（C）としてメッセージに含める。また、メッセージ生成部122は、構成情報記憶部48を参照して、不正E C Uに対応づけられたコマンドIDであり、すなわち、不正E C Uが送信するコマンドIDを特定し、そのコマンドIDを付加情報（C）としてメッセージに含める。

【0095】

対象フレームの不正検出パターンがパターン2であるとき、メッセージ生成部122は、付加情報として（A）（B）のみをメッセージに含める。この理由は、M A C検証と振る舞い検証のいずれも機能しており、パターン1の場合よりも問題が小さいからである（つまり、この場合、付加情報を減らすことによって、通信量の削減効果を高めている）。変形例として、パターン1と同様の付加情報（すなわち（A）～（C））をメッセージに

10

20

30

40

50

含めてもよい。

【0096】

次に、対象フレームの不正検出パターンがパターン6であるときの、メッセージ生成部122の処理を説明する。第1実施例でも言及したように、パターン6は、振る舞い検証が本来NGになるべきところがOKになった可能性があり、すなわち、振る舞い検証ルールが不完全の可能性がある。メッセージ生成部122は、図10のパターン6の通報内容をメッセージに含める。また、メッセージ生成部122は、付加情報(A)(B)(D)(E)をメッセージに含める。

【0097】

具体的には、メッセージ生成部122は、受信フレーム記憶部42を参照して、対象フレームのフレームIDと同じIDが設定されたフレームであり、対象フレームより前に受信された所定個数(例えば10個)のフレームを特定する。また、メッセージ生成部122は、受信フレーム記憶部42を参照して、対象フレームのフレームIDと同じIDが設定されたフレームであり、対象フレームより後に受信された所定個数(例えば10個)のフレームを特定する。メッセージ生成部122は、特定した各フレームに含まれるコマンドIDを付加情報(D)としてメッセージに含める。変形例として、メッセージ生成部122は、付加情報(D)として、対象フレームの前後で受信した所定個数のフレームの全体データをメッセージに含めてもよい。

10

【0098】

また、メッセージ生成部122は、構成情報記憶部48を参照して、対象フレームに含まれるコマンドに関連する他のコマンドのIDを特定し、他のコマンドのIDを付加情報(E)としてメッセージに含める。変形例として、メッセージ生成部122は、付加情報(E)として、上記他のコマンドのIDを含む所定個数のフレームの全体データをメッセージに含めてもよい。

20

【0099】

なお、メッセージ生成部122は、通報内容および付加情報(A)(B)を含む第1メッセージと、付加情報(D)(E)を含む第2メッセージとを別個に生成する。このように生成する理由は、後述するように、第1メッセージの通報タイミングと、第2メッセージの通報タイミングとが異なるからである。

【0100】

メッセージ生成部122は、対象フレームの不正検出パターンがパターン7であるとき、フレームを生成しない。ただし、不正検出パターンがパターン7である状態が所定時間以上継続する場合、メッセージ生成部122は、セキュリティに異常がないことを示すフレームを定期的(例えば1分経過毎に)に生成してもよい。

30

【0101】

次に、通報の優先度の設定処理の詳細を説明する。メッセージ生成部122は、対象フレームの不正検出パターンに応じた優先度(図10)を通報フレームに設定する。メッセージ生成部122は、対象フレームの不正検出パターンがパターン1または5の場合、優先度を高に設定し、すなわち、通報フレーム以外の他の通信より高い優先度を通報フレームに設定する。この理由は、パターン1または5は、MAC鍵が漏洩もしくはECUが乗っ取られている可能性が高いため、早急に対処すべきだからである。

40

【0102】

また、対象フレームの不正検出パターンがパターン2~4の場合、メッセージ生成部122は、優先度を低に設定し、すなわち、通報フレーム以外の他の通信より低い優先度を通報フレームに設定する。この理由は、パターン2~4では、不正コマンドを問題なく検出できているからである。また、この理由は、パターン3および4の判定対象フレームにはMACが付与されず、MACが付与されない判定対象フレームは、運転上重要性が低いからである。

【0103】

また、対象フレームの不正検出パターンがパターン6の場合、メッセージ生成部122

50

は、通報内容および付加情報（Ａ）（Ｂ）を含む第１メッセージのフレームの優先度を中に設定する。すなわち、通報フレーム以外の他の通信と同程度の優先度を通報フレームに設定する。この理由は、ＭＡＣ検証がＮＧであるため、不正コマンドによる被害は回避できているが、振る舞い検証ではＯＫとなっているため、振る舞い検証のルールを改善すべきだからである。また、メッセージ生成部１２２は、付加情報（Ｄ）（Ｅ）を含む第２メッセージのフレームの優先度を低に設定する。この理由は、付加情報（Ｄ）（Ｅ）はデータ量が多いからである。ただし、ＣＡＮ２４などの通信量が空いている場合には、付加情報（Ｄ）（Ｅ）を含む第２メッセージのフレームの優先度を中に設定してもよい。

【０１０４】

メッセージ生成部１２２は、優先度高に設定された通報フレームに、ＣＡＮ２４で優先的に伝送されるＩＤを付与してもよい。メッセージ出力部１２４は、優先度高に設定された通報フレームを、他のフレームが送信中か否かに関わらず、即時にＣＡＮ２４へ出力してもよい。また、メッセージ生成部１２２は、外部通信網２８と接続されたＩＶＩ装置１６に対して、優先度高に設定され通報フレームを、他の通信に優先して送信するように指示するデータを付与してもよい。他の通信は、車両１０の自動運転に必要な情報の送受信を含んでもよく、例えば、ダイナミックマップや標識情報のアップロードおよびダウンロードを含んでもよい。

10

【０１０５】

メッセージ生成部１２２は、優先度中に設定された通報フレームに、ＣＡＮ２４で他の種類のフレームと同等の優先度で扱われるＩＤを付与してもよい。メッセージ出力部１２４は、優先度中に設定された通報フレームを、他のフレームが送信されていない間にＣＡＮ２４へ出力してもよい。また、メッセージ生成部１２２は、優先度中に設定された通報フレームに、他の通信と同等に扱って送信する（例えば早い者勝ちで送信する）ようにＩＶＩ装置１６に指示するデータを付与してもよい。

20

【０１０６】

メッセージ生成部１２２は、優先度低に設定された通報フレームに、ＣＡＮ２４で他の種類のフレームより低い優先度で扱われるＩＤを付与してもよい。メッセージ出力部１２４は、優先度低に設定された通報を、イグニッションオフまたは電源オフ等、通信の空き時間にＣＡＮ２４へ出力してもよい。また、メッセージ生成部１２２は、優先度低に設定された通報フレームに、他の通信より低い優先度で送信するようにＩＶＩ装置１６指示するデータを付与してもよい。例えば、メッセージ生成部１２２は、優先度低に設定された通報フレームに、通信処理のアイドル中に車両監視サーバ１００へ送信するようにＩＶＩ装置１６に指示するデータを付与してもよい。

30

【０１０７】

なお、メッセージ生成部１２２は、優先度が高以外に設定された通報フレームを、第１実施例と同様に、ログとして不揮発メモリに保存してもよい。メッセージ出力部１２４は、ＣＡＮ２４が空いた場合等、通報フレームの送信が可能になった場合に、不揮発メモリに保存された通報フレームを読み出し、通報フレームをＣＡＮ２４へ出力してもよい。

【０１０８】

車両１０が複数種類の通信網に接続されるケースを説明する。例えば、車両１０は、複数の通信装置を備えてもよく、例えば、ＩＶＩ装置１６、ＴＣＵ（Telematics. Communication Unit）（不図示）、緊急通信ユニット（不図示）を備えてもよい。ＩＶＩ装置１６は、ＷｉＦｉ（登録商標）に接続されてもよい。また、ＴＣＵは、４Ｇ／ＬＴＥ（Long Term Evolution）（登録商標）ネットワークに接続されてもよい。また、緊急通信ユニットは、３Ｇネットワークに接続されてもよい。上述に挙げた通信網および各装置との組合せは一例であり、その他にも組み合わせることが可能であることは、当業者にとっては理解されよう。

40

【０１０９】

このような車両１０において、通報の優先度が高の場合、緊急通信ユニットを使用して通報処理を実行してもよい。また、通報の優先度が中の場合、ＴＣＵを使用して通報処理

50

を実行してもよい。また、通報の優先度が低の場合、I V I 装置 1 6 を使用して通報処理を実行してもよい。あるいは、通報の優先度が低の場合、複数種類の通信網のうち空いている通信網を選択して通報処理を実行してもよい。その一方、通報の優先度が高の場合、他の通信による高速な通信網の使用を中止させ、その高速な通信網を使用して通報処理を実行してもよい。上述に挙げた優先度の設定および各処理との組合せは一例であり、その他にも組み合わせることが可能であることは、当業者にとっては理解されよう。

【0110】

以上の構成による E C U 1 4 の動作を説明する。図 1 1 は、図 8 の E C U 1 4 の動作を示すフローチャートである。フレーム受信部 3 0 は、C A N 2 4 からフレームを受信する (S 7 0) 。 M A C 検証部 3 4 は、受信された対象フレームに対する M A C 検証を実行して、対象フレームが正当か不正かを判定する (S 7 2) 。振る舞い検証部 3 6 は、受信された対象フレームに対する振る舞い検証を実行して、対象フレームが正当か不正かを判定する (S 7 4) 。

10

【0111】

M A C 検証と振る舞い検証の両方で対象フレームが正当と判定された場合 (S 7 6 の Y) 、通報部 1 1 4 のメッセージ出力部 1 2 4 は、対象フレームをコマンド実行部 5 6 に渡す。コマンド実行部 5 6 は、対象フレームで指定されたコマンドにしたがいデータ処理を実行する (S 7 8) 。

【0112】

また、M A C 検証と振る舞い検証の両方で対象フレームが正当と判定される状態が継続する場合、メッセージ生成部 1 2 2 は、車両 1 0 のセキュリティ状態が正常であることを示すフレームを定期的に生成する。メッセージ出力部 1 2 4 は、当該フレームを車両監視サーバ 1 0 0 へ送信する。

20

【0113】

M A C 検証と振る舞い検証の少なくとも一方で対象フレームが不正と判定された場合 (S 7 6 の N) 、通報部 1 1 4 の解析部 1 2 0 は、対象フレームの不正検出パターンとして、図 1 0 の 7 つのパターンの中から 1 つのパターンを特定する (S 8 0) 。メッセージ生成部 1 2 2 は、特定された対象フレームの不正検出パターンにしたがって、車両監視サーバ 1 0 0 へ通報するメッセージと、通報の優先度を設定する (S 8 2) 。メッセージ出力部 1 2 4 は、メッセージ生成部 1 2 2 により生成されたメッセージを含む通報フレームを、メッセージ生成部 1 2 2 により設定された優先度にしたがって車両監視サーバ 1 0 0 へ送信する (S 8 4) 。このように、通報部 1 1 4 は、不正が検出されたフレームごとに、その不正検出パターンに応じて、通報フレームの内容および優先度を変更する。

30

【0114】

対象フレームの不正検出パターンがパターン 1 または 5 の場合 (優先度高) 、車両 1 0 の通信部 (不図示) は、自動運転のためのダイナミックマップのダウンロードおよびアップロード (以下「他の通信」と呼ぶ。) より優先して通報フレームを処理し、通報フレームを車両監視サーバ 1 0 0 へ送信してもよい。また、対象フレームの不正検出パターンがパターン 6 の場合、上記通信部は、他の通信と同程度の優先度 (例えば早い者勝ち) で通報フレームを処理してもよい。また、対象フレームの不正検出パターンがパターン 2 ~ 4 の場合、上記通信部は、他の通信を処理中であれば、通報フレームの処理を後回しにしてもよい。

40

【0115】

第 2 実施例の E C U 1 4 によると、車両 1 0 (言い換えれば車載ネットワークシステム 1 2 内の各装置) のセキュリティ状態に応じた適切なタイミングで、かつ、適切な内容を車両監視サーバ 1 0 0 へ通報することができる。

【0116】

以上、本発明を第 2 実施例をもとに説明した。この実施例は例示であり、それらの各構成要素あるいは各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

50

【0117】

第1変形例を説明する。本変形例は、第1実施例の第1変形例に対応する。振る舞い検証部36は、対象フレームの態様と、予め定められた複数のルールとに基づいて、複数の中間判定を実行し、複数の中間判定の結果に応じて、振る舞い検証の結果を導出する。振る舞い検証部36は、振る舞い検証の結果とともに、複数の中間判定の結果を通報部114へ出力する。メッセージ生成部122は、複数の中間判定結果の中にルールに不適合であることを示す結果が存在する場合、複数の中間判定結果を含む通報フレームを生成する。メッセージ出力部124は、上記の通報フレームを車両監視サーバ100へ送信する。また、メッセージ生成部122は、ルールに不適合であることを示す中間判定結果の数に応じて、通報の優先度を変更する。

10

【0118】

具体例として、振る舞い検証部36は、1つの対象フレームのデータを、複数の検知パラメータA～Eのそれぞれで評価し、各検知パラメータによる中間判定結果（ルールに適合するか否かの判定結果）を生成してもよい。振る舞い検証部36は、複数の中間判定結果のうちNGとなった中間判定結果の個数が3以上であれば、対象フレームの最終判定結果を不正としてもよい。NGとは、例えば、判定対象フレームのデータが、個々の中間判定のルールに不適合であることを含む。

【0119】

1) フレーム単位での通報処理を説明する。メッセージ生成部122は、複数の中間判定結果の中にルール不適合を示す結果が1つ以上存在する場合、全ての中間判定結果を含む通報フレームを生成してもよい。中間判定結果は、中間判定で使用されたパラメータの情報を含んでよく、また、中間判定で正否が判定されたフレームのデータを含んでもよい。また、メッセージ生成部122は、中間判定結果がNGになった数に応じて、車両監視サーバ100への通報の優先度を変更してもよい。例えば、5つの中間判定が行われる場合、中間判定結果のNG数が1または2であれば実施例の優先度低を設定してもよい。また、中間判定結果のNG数が3または4であれば実施例の優先度中を設定し、中間判定結果のNG数が5であれば優先度高を設定してもよい。

20

【0120】

次に、2) コマンド単位での通報処理を説明する。メッセージ生成部122は、コマンドIDごと（もしくはフレームIDごと）に、振る舞い検証部36による中間判定結果のNG数の累計値（ここでは「コマンド別中間NG累計数」と呼ぶ。）を記憶してもよい。メッセージ生成部122は、コマンド別中間NG累計数が第1閾値（例えば20回）を超えた場合に、コマンド別中間NG累計数が第1閾値を超えた旨の情報とコマンドIDとを含む通報フレームを生成し、通報の優先度を低に設定してもよい。また、メッセージ生成部122は、コマンド別中間NG累計数が第2閾値（例えば40回）を超えた場合に、コマンド別中間NG累計数が第2閾値を超えた旨の情報とコマンドIDとを含む通報フレームを生成し、通報の優先度を中に設定してもよい。

30

【0121】

次に、3) 車両10全体としての通報処理を説明する。メッセージ生成部122は、コマンドIDに関係なく、複数のコマンド（複数の対象フレーム）について振る舞い検証部36から入力された中間判定結果のNG数の累計値（ここでは「全体中間NG累計数」と呼ぶ。）を記憶してもよい。メッセージ生成部122は、全体中間NG累計数が第1閾値（例えば100回）を超えた場合に、全体中間NG累計数が第1閾値を超えた旨の情報をを含む通報フレームを生成し、通報の優先度を低に設定してもよい。また、メッセージ生成部122は、全体中間NG累計数が第2閾値（例えば200回）を超えた場合に、全体中間NG累計数が第2閾値を超えた旨の情報をを含む通報フレームを生成し、通報の優先度を中に設定してもよい。

40

【0122】

第2変形例を説明する。第1実施例の任意の構成要素と第2実施例の任意の構成要素の組み合わせが可能である。例えば、第1実施例に記載したように、車両10のCGW20

50

は、MAC 検証および振る舞い検証により不正と判定したフレームを破棄または無効化する機能を備えてもよい。上記第 2 実施例では、ECU 14 の構成情報記憶部 48 は、コマンド ID と、そのコマンドを送信する ECU-ID とを対応付けた構成情報を記憶する。変形例として、構成情報記憶部 48 は、自機とは異なる CAN 24 のバスに接続された ECU が送信するコマンドについて、そのコマンド ID と CGW 20 の ID とを対応付けた構成情報を記憶してもよい。この理由は、自機とは異なる CAN 24 のバスに接続された ECU から送信されるフレームは、CGW 20 により中継されるからである。

【0123】

第 2 変形例の解析部 120 は、対象フレームの不正検出パターンがパターン 1 またはパターン 3 であり、かつ、その対象フレームが CGW 20 を経由して受信されたものである場合、乗っ取られた可能性がある ECU として、CGW 20 の ID を特定する。具体的には、構成情報記憶部 48 の構成情報は、当該対象フレームに含まれるコマンド ID と CGW 20 の ID とを対応付けている。解析部 120 は、その構成情報を参照することにより、対象フレームが CGW 20 を経由して受信されたものである場合、CGW 20 の ID を特定する。メッセージ生成部 122 は、CGW 20 が乗っ取られた可能性があることを示す通報フレームを生成する。

10

【0124】

既述したように、CGW 20 が正常に動作していれば、不正フレームを破棄または無効化する。そのため、CGW 20 により中継されたフレームの不正が ECU 14 で検出された場合、CGW 20 の動作が異常であり、乗っ取られた可能性がある。本変形例の態様によると、CGW 20 の異常を精度よく検出して、車両監視サーバ 100 へ通報することができる。なお、第 2 変形例の構成は、CMI 22 に監視モジュールが導入される場合も適用可能である。

20

【0125】

第 2 実施例および変形例に記載の技術は、以下の項目によって特定されてもよい。

[項目 1]

通信網からフレームを受信する受信部と、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第 1 判定と、前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第 2 判定とを行い、前記第 1 判定の結果と前記第 2 判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する処理部と、

30

を備える監視装置。

この監視装置によると、自装置のセキュリティ状態に応じた適切な内容またはタイミングで、外部装置への通報を実行することができる。

[項目 2]

前記第 1 判定により判定対象フレームが正当と判定され、前記第 2 判定により前記判定対象フレームが不正と判定された場合、前記処理部は、前記判定対象フレームに関する情報を通報する優先度を、他の通信より高い優先度に設定する、

40

項目 1 に記載の監視装置。

この態様によると、メッセージ認証の鍵が漏洩している危険がある場合に、外部装置への通報を迅速に実行することができる。

[項目 3]

前記第 1 判定により判定対象フレームが不正と判定され、前記第 2 判定により前記判定対象フレームが不正と判定された場合、前記処理部は、前記判定対象フレームに関する情報を通報する優先度を、他の通信より低い優先度に設定する、

項目 1 または 2 に記載の監視装置。

この態様によると、第 1 判定と第 2 判定のいずれでも判定対象フレームが不正と判定された場合、不正フレームによる被害は回避できているため、他の通信を阻害してしまうことを抑制した通報を実現できる。

50

[項目 4]

前記第 1 判定により判定対象フレームが不正と判定され、前記第 2 判定により前記判定対象フレームが正当と判定された場合、前記処理部は、前記判定対象フレームに関する情報を通報する優先度を、前記第 1 判定により判定対象フレームが正当と判定され、前記第 2 判定により前記判定対象フレームが不正と判定された場合より低い優先度であり、かつ、前記第 1 判定により判定対象フレームが不正と判定され、前記第 2 判定により前記判定対象フレームが不正と判定された場合より高い優先度に設定する、

項目 1 から 3 のいずれかに記載の監視装置。

この態様によると、第 1 判定により不正が検出されることで、不正フレームによる被害は回避できているが、第 2 判定のルールが不完全である可能性があるため、中程度の優先度での通報を実現できる。

10

[項目 5]

前記第 1 判定により判定対象フレームが正当と判定され、前記第 2 判定により前記判定対象フレームが不正と判定された場合、前記処理部は、少なくとも前記判定対象フレームに含まれるコマンドの情報および前記判定対象フレームの送信元装置の情報を通報する、

項目 1 または 2 に記載の監視装置。

この態様によると、不正が検出されたコマンドに加えて、乗っ取られた可能性がある ECU の情報を外部装置へ通報することにより、外部装置側での適切なデータ処理を支援することができる。

20

[項目 6]

前記第 1 判定により判定対象フレームが正当と判定され、前記第 2 判定により前記判定対象フレームが不正と判定された場合であって、かつ、前記判定対象フレームと同じ ID のフレームの受信頻度が所定値を超える場合、前記処理部は、少なくとも前記判定対象フレームに含まれるコマンドの情報を通報する、

項目 1 または 2 に記載の監視装置。

この態様によると、不正なフレームが外部から注入されたことを検出して、適切な内容を通報することができる。

[項目 7]

前記第 1 判定により判定対象フレームが不正と判定され、前記第 2 判定により前記判定対象フレームが不正と判定された場合、前記処理部は、少なくとも前記判定対象フレームに含まれるコマンドの情報を通報する、

30

項目 1 から 3 のいずれかに記載の監視装置。

この態様によると、監視装置では判定対象フレームの不正を正しく検知できているため、通報内容を不正が検出されたコマンドの情報に抑えることで、通信トラフィックの増加を抑制することができる。

[項目 8]

前記第 1 判定により判定対象フレームが不正と判定され、前記第 2 判定により前記判定対象フレームが正当と判定された場合、前記処理部は、少なくとも前記判定対象フレームに含まれるコマンドの情報および当該コマンドに関連する他のコマンドの情報を通報する、

40

項目 1 から 4 のいずれかに記載の監視装置。

この態様によると、ルールが不完全である可能性がある場合に、ルールの改善を支援することができる。

[項目 9]

前記第 1 判定の対象外となったフレームが前記第 2 判定により不正と判定された場合であって、かつ、前記フレームと同じ ID のフレームの受信頻度が所定値に整合する場合、前記処理部は、他の通信より低い優先度で、少なくとも前記フレームに含まれるコマンドの情報および前記フレームの送信元装置の情報を通報する、

項目 1 から 4 のいずれかに記載の監視装置。

この態様によると、メッセージ認証用の鍵を有しない電子機器が乗っ取られたことを検

50

出して、適切な優先度で適切な内容を通報することができる。

[項目 10]

前記第 1 判定の対象外となったフレームが前記第 2 判定により不正と判定された場合であって、かつ、前記フレームと同じ ID のフレームの受信頻度が所定値を超える場合、前記処理部は、他の通信より低い優先度で、少なくとも前記フレームに含まれるコマンドの情報を通報する、

項目 1 から 4 のいずれかに記載の監視装置。

この態様によると、メッセージ認証用のコードを持たないフレームであり、不正なフレームが外部から注入されたことを検出して、適切な優先度で適切な内容を通報することができる。

10

[項目 11]

前記処理部は、判定対象フレームの態様と、予め定められた複数のルールとに基づいて、複数の中間判定を実行し、複数の中間判定の結果に応じて前記第 2 判定の結果を導出し、

前記処理部は、前記複数の中間判定の結果の中にルールに不適合であることを示す結果が存在する場合、前記複数の中間判定の結果を外部装置へ通報し、前記ルールに不適合であることを示す結果の数に応じて、通報の優先度を変更する、

項目 1 から 10 のいずれかに記載の監視装置。

この監視装置によると、振る舞い検証によるセキュリティの強度を高めることができる。

20

[項目 12]

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第 1 判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第 2 判定と、を行い、

前記第 1 判定の結果と前記第 2 判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する、

ことをコンピュータが実行する監視方法。

この監視方法によると、自装置のセキュリティ状態に応じた適切な内容またはタイミングで、外部装置への通報を実行することができる。

30

[項目 13]

通信網からフレームを受信し、

前記フレームに対するメッセージ認証の結果に基づいて前記フレームが不正かを判定する第 1 判定と、

前記フレームの態様と予め定められたルールとに基づいて前記フレームが不正かを判定する第 2 判定と、を行い、

前記第 1 判定の結果と前記第 2 判定の結果との組み合わせに応じて、外部装置へ通報する内容または通報の優先度の少なくとも一方を変更する、

ことをコンピュータに実行させるためのコンピュータプログラム。

40

このコンピュータプログラムによると、自装置のセキュリティ状態に応じた適切な内容またはタイミングで、外部装置への通報を実行することができる。

【0126】

上述した実施例および変形例の任意の組み合わせもまた本発明の実施の形態として有用である。組み合わせによって生じる新たな実施の形態は、組み合わせられる実施例および変形例それぞれの効果をあわせもつ。また、請求項に記載の各構成要件が果たすべき機能は、実施例および変形例において示された各構成要素の単体もしくはそれらの連携によって実現されることも当業者には理解されるところである。

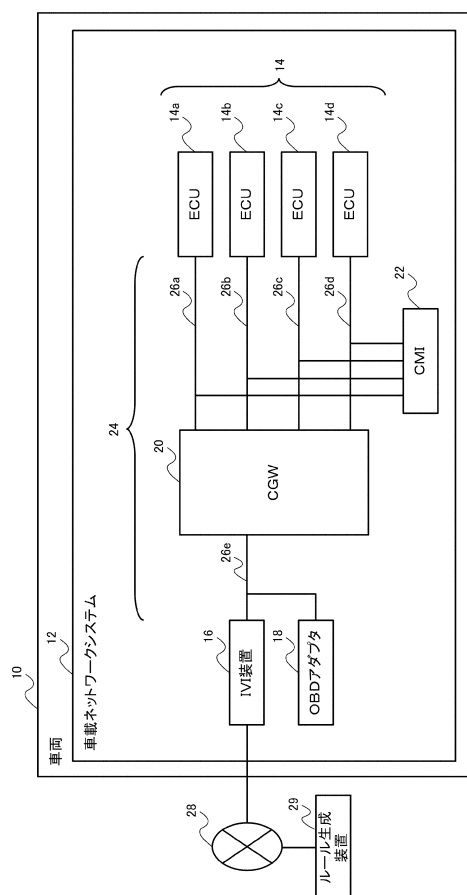
【符号の説明】

【0127】

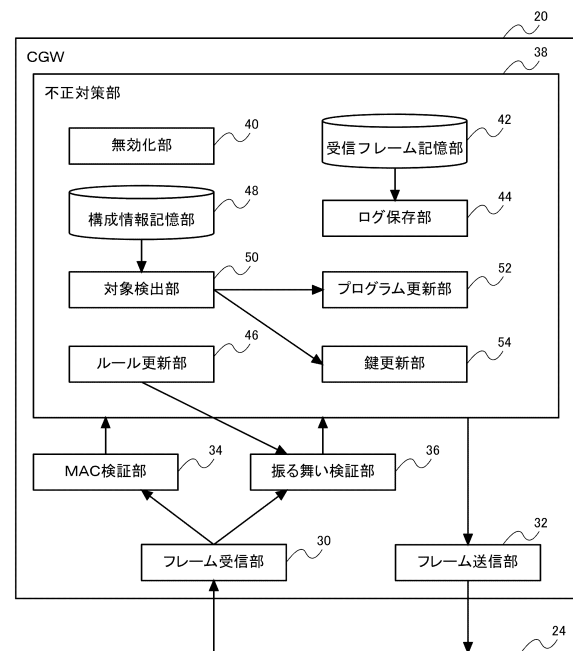
50

10 車両、 12 車載ネットワークシステム、 14 ECU、 24 CAN、
 30 フレーム受信部、 100 車両監視サーバ、 110 処理部、 114 通
 報部、 120 解析部、 122 メッセージ生成部、 124 メッセージ出力部。

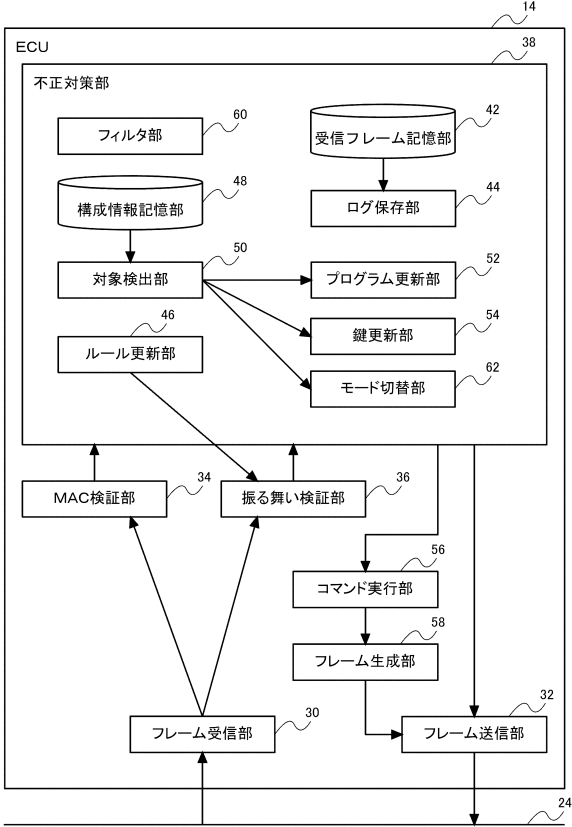
【図 1】



【図 2】



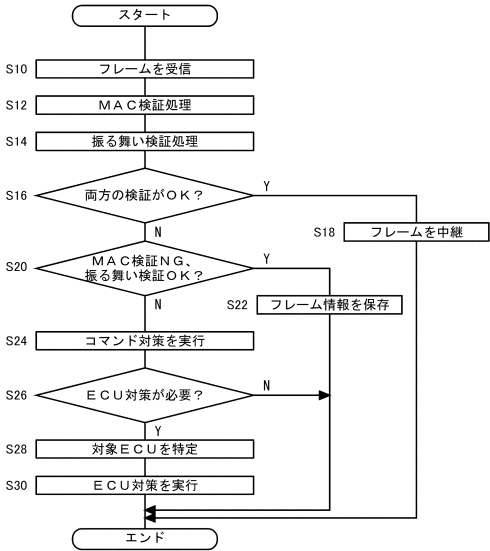
【図 3】



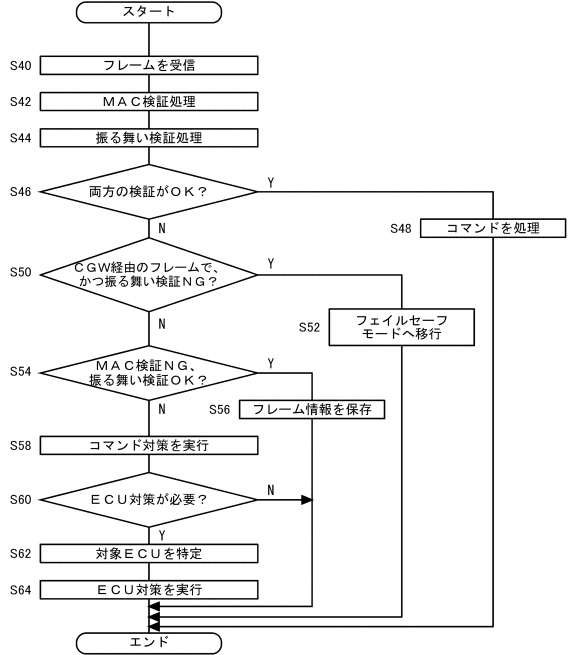
【図 4】

ECU対策	コマンド対策	想定される脅威	追加条件	振る舞い検証	MAC検証	
対象ECUを特定し、以下の1つまたは複数を実施する (1) 対象ECUから送信された他のフレーム(コマンド)にも上記コマンドを実行し、他のECUに送信されたコマンド(コマンド)を注ぎ、他のECUに送信されたコマンド(コマンド)にも上記コマンド対策を実施する (2) 対象ECUのプログラムを更新する (3) 対象ECUを除く全てのECUのMAC鍵を再算(リボーン)	CGW:フィルタまたは無効化 ECU:フィルタ CMI:無効化	MAC鍵を有するECUが完全に壊れた (MAC鍵使用可能)	なし	NG	OK	パターン1
対象ECUを特定し、以下の1つまたは複数を実施する (1) 対象ECUから送信された他のフレーム(コマンド)にも上記コマンドを実行し、他のECUに送信されたコマンド(コマンド)を注ぎ、他のECUに送信されたコマンド(コマンド)にも上記コマンド対策を実施する (2) 対象ECUのプログラムを更新する (3) 対象ECUを除く全てのECUのMAC鍵を再算(リボーン)	CGW:無効化 ECU:なし CMI:無効化	MAC鍵を有するECUの一部壊れた (MAC鍵使用困難)	なし	NG	NG	パターン2
対象ECUを特定し、以下の1つまたは複数を実施する (1) 対象ECUから送信された他のフレーム(コマンド)にも上記コマンドを実行し、他のECUに送信されたコマンド(コマンド)を注ぎ、他のECUに送信されたコマンド(コマンド)にも上記コマンド対策を実施する (2) 対象ECUのプログラムを更新する (3) 対象ECUを除く全てのECUのMAC鍵を再算(リボーン)	CGW:フィルタまたは無効化 ECU:なし CMI:無効化	MAC鍵を有しないECUが壊れた	なし	NG	n/a	パターン3
対象ECUを特定し、以下の1つまたは複数を実施する (1) 対象ECUから送信された他のフレーム(コマンド)にも上記コマンドを実行し、他のECUに送信されたコマンド(コマンド)を注ぎ、他のECUに送信されたコマンド(コマンド)にも上記コマンド対策を実施する (2) 対象ECUのプログラムを更新する (3) 対象ECUを除く全てのECUのMAC鍵を再算(リボーン)	CGW:フィルタまたは無効化 ECU:なし CMI:無効化	MACなし不正フレームの外注注入(不正ECU接続を含む)	外部バスから受信	NG	n/a	パターン4
対象ECUを特定し、以下の1つまたは複数を実施する (1) 対象ECUから送信された他のフレーム(コマンド)にも上記コマンドを実行し、他のECUに送信されたコマンド(コマンド)を注ぎ、他のECUに送信されたコマンド(コマンド)にも上記コマンド対策を実施する (2) 対象ECUのプログラムを更新する (3) 対象ECUを除く全てのECUのMAC鍵を再算(リボーン)	CGW:フィルタまたは無効化 ECU:なし CMI:無効化	MAC有り不正フレームの外注注入(MAC鍵無効)	外部バスから受信	NG	OK	パターン5
対象ECUを特定し、以下の1つまたは複数を実施する (1) 対象ECUから送信された他のフレーム(コマンド)にも上記コマンドを実行し、他のECUに送信されたコマンド(コマンド)を注ぎ、他のECUに送信されたコマンド(コマンド)にも上記コマンド対策を実施する (2) 対象ECUのプログラムを更新する (3) 対象ECUを除く全てのECUのMAC鍵を再算(リボーン)	なし	振る舞い検証ルールが不完全	なし	OK	NG	パターン6

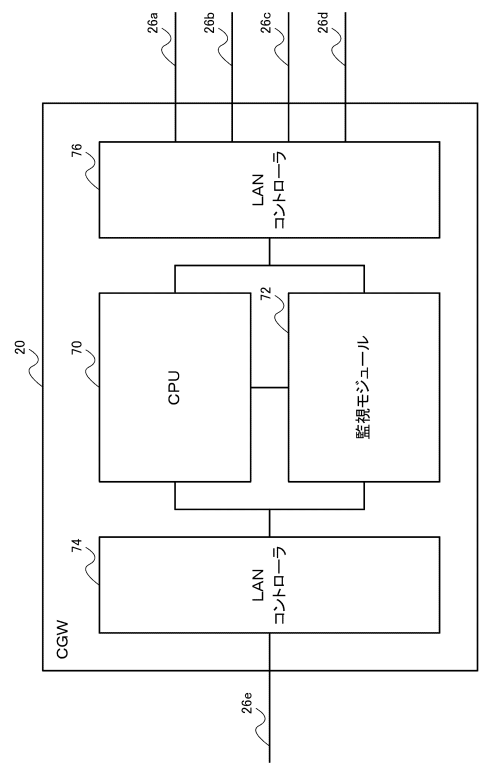
【図 5】



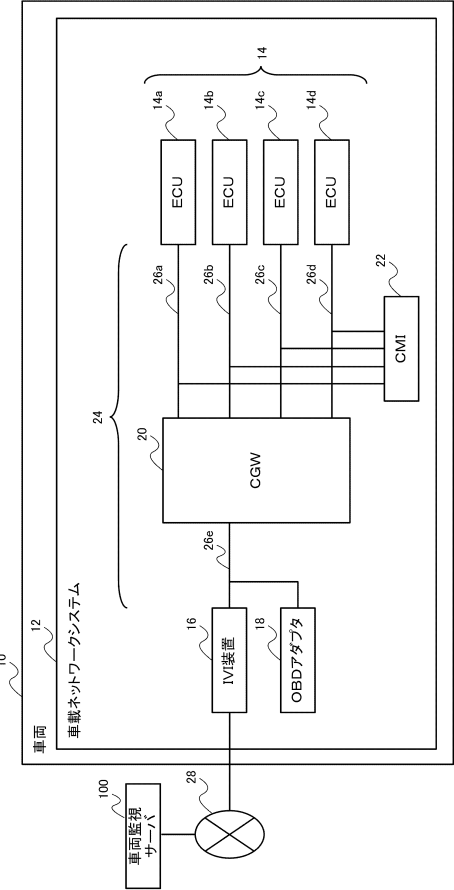
【図 6】



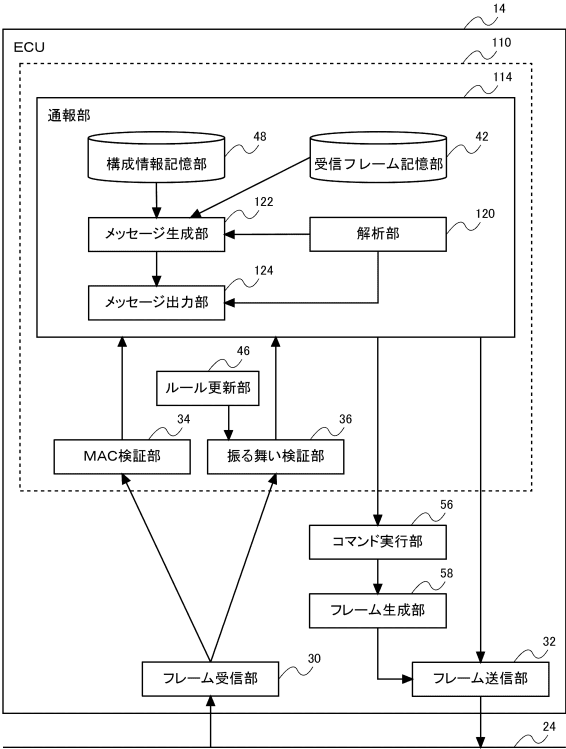
【図 7】



【図 8】



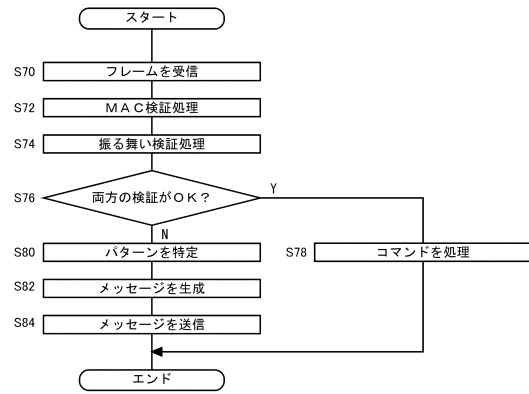
【図 9】



【図 10】

	MAC検証	振る舞い検証	想定される脅威	優先度	通報内容	付加情報
パターン1	OK	NG	MAC鍵を有するECUが完全に取られた (MAC鍵使用可能)	高	MAC鍵漏洩もしくは対象ECU乗っ取りの可能性あり	(A) MAC検証と振る舞い検証の結果一致しない可能性あり (B) 不正コマンドの注入の可能性あり (C) 不正コマンドの注入の可能性あり (D) 不正コマンドの注入の可能性あり (E) 不正コマンドの注入の可能性あり
パターン2	NG	NG	MAC鍵を有するECUが一部乗っ取られた (MAC鍵使用可能)	低	対象ECU乗っ取りの可能性あり	上記の(A) (B)
パターン3	n/a	NG	MAC鍵を有しないECUが乗っ取られた	低	対象ECU乗っ取りもしくは不正コマンド外部注入の可能性あり	上記の(A) (B) (C)
パターン4	n/a	NG	MACなし不正フレームの外部注入 (不正ECU接続を含む)	低	対象ECU乗っ取りもしくは不正コマンド外部注入の可能性あり	上記の(A) (B)
パターン5	OK	NG	MAC有/不正フレームの外部注入 (MAC鍵漏洩)	高	MAC鍵漏洩もしくは対象ECU乗っ取りの可能性あり	上記の(A) (B)
パターン6	NG	OK	振る舞い検証ルールが不完全	中	振る舞い検証ルールが不完全の可能性あり	不正コマンドの前後のコマンド不正コマンドに関連するコマンド
パターン7	OK	OK	安全なケース	-	セキュリティ異常なし	

【図 11】



フロントページの続き

(56)参考文献 国際公開第2015/170451 (WO, A1)

特開2001-358774 (JP, A)

特開2015-114907 (JP, A)

特開2005-343430 (JP, A)

(58)調査した分野(Int.Cl., DB名)

H04L12/00-12/955